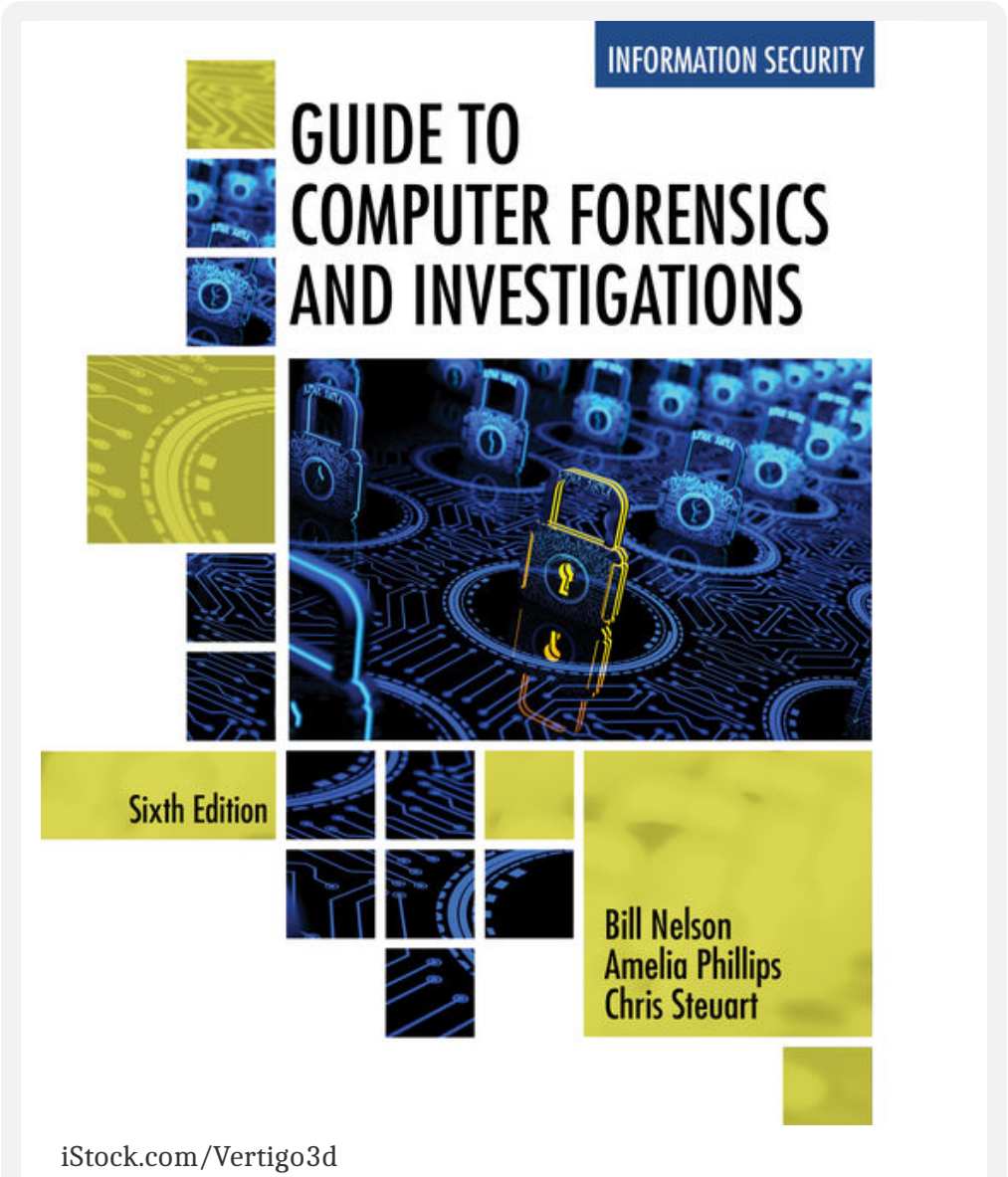
INFORMATION SECURITY

GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS

Sixth Edition

Bill Nelson
Amelia Phillips
Chris Steuart

Guide to Computer Forensics and Investigations: Processing Digital Evidence



iStock.com/Vertigo3d

Guide to Computer Forensics and Investigations: Processing Digital Evidence

6th Edition

Bill Nelson

Amelia Phillips

Christopher Steuart

Jonathan Lau *SVP, GM Skills*

Lauren Murphy *Product Director*

Kristin McNary *Product Team Manager*

Amy Savino *Product Manager*

Jake Toth *Product Assistant*

Marah Bellegarde *Executive Director, Content Design*

Leigh Hefferon *Director, Learning Design*

Natalie Onderdonk *Learning Designer*

Lisa M. Lord *Development Editor*

Michele McTighe *Sr. Marketing Director*

Cassie Cloutier *Assoc. Marketing Manager*

Patty Stephan *Director, Content Delivery*

Brooke Greenhouse *Senior Content Manager*

Jim Vaughey *Digital Delivery Lead*

Diana H. Graham *Senior Designer*

SPi Global *Production Service/Composition*

Copyright Statement
Guide to Computer Forensics and Investigations: Processing Digital Evidence

COPYRIGHT © 2019, 2016 Cengage Learning, Inc.

ALL RIGHTS RESERVED. No part of this work covered by the copyright herein may be reproduced or distributed in any form or by any means, except as permitted by U.S. copyright law, without the prior written permission of the copyright owner.

For product information and technology assistance, contact us at **Cengage Customer & Sales Support, 1-800-354-9706** or **support.cengage.com**.

For permission to use material from this text or product, submit all requests online at www.cengage.com/permissions.

SOURCE FOR ILLUSTRATIONS: Copyright © Cengage.

, Microsoft® is a registered trademark of the Microsoft Corporation.

Library of Congress Control Number: 2018936389

ISBN: 978-1-337-56894-4

Cengage

20 Channel Center Street

Boston MA 02210

USA

Cengage is a leading provider of customized learning solutions with employees residing in nearly 40 different countries and sales in more than 125 countries around the world. Find your local representative at www.cengage.com.

Cengage products are represented in Canada by Nelson Education, Ltd.

To learn more about Cengage platforms and services, visit www.cengage.com.

To register or access your online learning solution or purchase materials for your course, visit www.cengagebrain.com.

Notice to the Reader
Publisher does not warrant or guarantee any of the products described herein or perform any independent analysis in connection with any of the product information contained herein. Publisher does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instructions contained herein, the reader willingly assumes all risks in connection with such instructions. The publisher makes no representations or warranties of any kind, including but not limited to, the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and the publisher takes no responsibility with respect to such material. The publisher shall not be liable for any special, consequential, or exemplary damages resulting, in whole or part, from the readers' use of, or reliance upon, this material.

Preface

Guide to Computer Forensics and Investigations is now in its sixth edition. As digital technology and cyberspace have evolved from their early roots as basic communication platforms into the hyper-connected world we live in today, so has the demand for people who have the knowledge and skills to investigate legal and technical issues involving computers and digital technology. My sincere compliments to the authors and publishing staff who have made this textbook such a remarkable resource for thousands of students and practitioners worldwide.

Computers, the Internet, and the world's digital ecosystem are all instrumental in how we conduct our daily lives. When the founding fathers of the modern computing era were designing the digital infrastructure as we know it today, security and temporal accountability issues were not at the top of their list of things to do. The technological advancement of these systems over the past 10 years has changed the way we learn, socialize, and conduct business. Finding digital data that can be used as evidence to incriminate or exonerate a suspect accused in a legal or administrative proceeding is not an easy task.

Cyberthreats have become pervasive in modern society. They range from simple computer viruses to complex ransomware and cyber extortion schemes. The ability to conduct sophisticated digital forensics investigations has become a requirement in both the government and commercial sectors. Currently, the organizations and agencies whose job it is to investigate both criminal and civil matters involving the use of rapidly developing digital technology often struggle to keep up with the ever-changing digital landscape. Additionally, finding trained and qualified people to conduct these types of inquiries has been challenging.

Today, an entire industry has evolved for the purpose of investigating events occurring in cyberspace to include incidents involving international and corporate espionage, massive data breaches, and even cyberterrorism. The opportunities for employment in this field are expanding every day. Professionals in this exciting field of endeavor are now in high demand and are expected to have multiple skill sets in areas such as malware analysis, cloud computing, social media, and mobile device forensics.

Guide to Computer Forensics and Investigations can now be found in both academic and professional environments as a reliable source of current technical information and practical exercises concerning investigations involving the latest digital technologies. It's my belief that this book, combined with an enthusiastic and knowledgeable facilitator, makes for a fascinating course of instruction.

As I have stated to many of my students in the past, it's not just laptop computers and servers that harbor the binary code of ones and zeros, but an infinite array of digital devices. If one of these devices retains evidence of a crime, it's up to newly trained and educated digital detectives to find the evidence in a forensically sound manner. This book will assist both students and practitioners in accomplishing this goal.

Respectfully,

John A. Sgromolo

As a Senior Special Agent, John was one of the founding members of the NCIS Computer Crime Investigations Group. John left government service to run his own company, Digital Forensics, Inc., and has taught hundreds of law enforcement and corporate students nationwide in the art and science of digital forensics investigations. Currently, he serves as a

senior consultant for Verizon's Global Security Services, where he helps manage the Threat Intel Response Service.

Introduction

Computer forensics, now most commonly called "digital forensics," has been a professional field for many years, but most well-established experts in the field have been self-taught. The growth of the Internet and the worldwide proliferation of computers have increased the need for digital investigations. Computers can be used to commit crimes, and crimes can be recorded on computers, including company policy violations, embezzlement, e-mail harassment, murder, leaks of proprietary information, and even terrorism. Law enforcement, network administrators, attorneys, and private investigators now rely on the skills of professional digital forensics experts to investigate criminal and civil cases.

This book is not intended to provide comprehensive training in digital forensics. It does, however, give you a solid foundation by introducing digital forensics to those who are new to the field. Other books on digital forensics are targeted to experts; this book is intended for novices who have a thorough grounding in computer and networking basics.

The new generation of digital forensics experts needs more initial training because operating systems, computer and mobile device hardware, and forensics software tools are changing more quickly. This book covers current and past operating systems and a range of hardware, from basic workstations and high-end network servers to a wide array of mobile devices. Although this book focuses on a few forensics software tools, it also reviews and discusses other currently available tools.

The purpose of this book is to guide you toward becoming a skilled digital forensics investigator. A secondary goal is to help you pass related certification exams. As the field of digital forensics and investigations matures, keep in mind that certifications will change. You can find more information on certifications in **Chapter 2** and Appendix A.

Intended Audience

Although this book can be used by people with a wide range of backgrounds, it's intended for those with A+ and Network+ certifications or the equivalent. A networking background is necessary so that you understand how computers operate in a networked environment and can work with a network administrator when needed. In addition, you must know how to use a computer from the command line and how to use common operating systems, including Windows, Linux, and macOS, and their related hardware.

This book can be used at any educational level, from technical high schools and community colleges to graduate students. Current professionals in the public and private sectors can also use this book. Each group will approach investigative problems from a different perspective, but all will benefit from the coverage.

What's New in This Edition

The chapter flow of this book is organized so that you're first exposed to what happens in a forensics lab and how to set one up before you get into the nuts and bolts. Coverage of several GUI tools has been added to give you a familiarity with some widely used software. In addition, **Chapter 11** has additional coverage of social media forensics, Chapter 12 has been expanded to include more information on smartphones and tablets, and Chapter 13 on forensics procedures for information stored in the cloud has been updated. Corrections have been made to this edition based on feedback from users, and all software tools and Web sites have been updated to reflect what's current at the time of publication. Finally, a new digital lab manual is being offered in *MindTap for Guide to Computer Forensics and Investigations*to go with the sixth edition textbook.

Chapter Descriptions

Here is a summary of the topics covered in each chapter of this book:

Chapter 1 , "Understanding the Digital Forensics Profession and Investigations," introduces you to the history of digital forensics and explains how the use of electronic evidence developed. It also reviews legal issues and compares public and private sector cases. This chapter also explains how to take a systematic approach to preparing a digital investigation, describes how to conduct an investigation, and summarizes requirements for workstations and software.

Chapter 2 , "The Investigator's Office and Laboratory," outlines physical requirements and equipment for digital forensics labs, from small private investigators' labs to the regional FBI lab. It also covers certifications for digital investigators and building a business case for a forensics lab.

Chapter 3 , "Data Acquisition," explains how to prepare to acquire data from a suspect's drive and discusses available Linux and GUI acquisition tools. This chapter also discusses acquiring data from RAID systems and gives you an overview of tools for remote acquisitions.

Chapter 4 , "Processing Crime and Incident Scenes," explains search warrants and the nature of a typical digital forensics case. It discusses when to use outside professionals, how to assemble a team, and how to evaluate a case and explains the correct procedures for searching and seizing evidence. This chapter also introduces you to calculating hashes to verify data you collect.

Chapter 5 , "Working with Windows and CLI Systems," discusses the most common operating systems. You learn what happens and what files are altered during computer startup and how file systems deal with deleted and slack space. In addition, this chapter covers some options for decrypting drives encrypted with whole disk encryption and explains the purpose of using virtual machines.

Chapter 6 , "Current Digital Forensics Tools," explores current digital forensics software and hardware tools, including those that might not be readily available, and evaluates their strengths and weaknesses.

Chapter 7 , "Linux and Macintosh File Systems," continues the operating system discussion from Chapter 5 by examining Macintosh and Linux OSs and file systems. It also gives you practice in using Linux forensics tools.

Chapter 8 , "Recovering Graphics Files," explains how to recover graphics files and examines data compression, carving data, reconstructing file fragments, and steganography and copyright issues.

Chapter 9 , "Digital Forensics Analysis and Validation," covers determining what data to collect and analyze and refining investigation plans. It also explains validation with hex editors and forensics software and data-hiding techniques.

Chapter 10 , "Virtual Machine Forensics, Live Acquisitions, and Network Forensics," covers tools and methods for conducting forensic analysis of virtual machines, performing live acquisitions, reviewing network logs for evidence, and using network-monitoring tools to detect unauthorized access. It also examines using Linux tools and the Honeynet Project's resources.

Chapter 11 , "E-mail and Social Media Investigations," examines e-mail crimes and violations and reviews some specialized e-mail and social media forensics tools. It also explains how to approach investigating social media communications and handling the challenges this content poses.

Chapter 12 , "Mobile Device Forensics and The Internet of Anything," covers investigation techniques and acquisition procedures for smartphones, other mobile devices, Internet of Anything devices, and sensors. You learn where data might be stored or backed up and what tools are available for these investigations.

Chapter 13 , "Cloud Forensics," summarizes the legal and technical challenges in conducting cloud forensics. It also describes how to acquire cloud data and explains how remote acquisition tools can be used in cloud investigations.

Chapter 14 , "Report Writing for High-Tech Investigations," discusses the importance of report writing in digital forensics examinations; offers guidelines on report content, structure, and presentation; and explains how to generate report findings with forensics software tools.

Chapter 15 , "Expert Testimony in Digital Investigations," explores the role of an expert witness or a fact witness, including developing a curriculum vitae, understanding the trial process, and preparing forensics evidence for testimony. It also offers guidelines for testifying in court and at depositions and hearings.

Chapter 16 , "Ethics for the Expert Witness," provides guidance in the principles and practice of ethics for digital forensics investigators and examines other professional organizations' codes of ethics.

Appendix A , "Certification Test References," provides information on the National Institute of Standards and Technology (NIST) testing processes for validating digital forensics tools and covers digital forensics certifications and training programs.

Appendix B , "Digital Forensics References," lists recommended books, journals, e-mail lists, and Web sites for additional information and further study. It also covers the latest ISO 27000 standards that apply to digital forensics.

Appendix C , "Digital Forensics Lab Considerations," provides more information on considerations for forensics labs, including certifications, ergonomics, structural design, and communication and fire-suppression systems. It also covers applicable ISO standards.

Appendix D , "Legacy File System and Forensics Tools," reviews FAT file system basics and Mac legacy file systems and explains using DOS forensics tools, creating forensic boot media, and using scripts. It also has an overview of the hexadecimal numbering system and how it's applied to digital information.

Features

To help you fully understand digital forensics, this book includes many features designed to enhance your learning experience:

- *Chapter objectives*—Each chapter begins with a detailed list of the concepts to be mastered in that chapter. This list gives you a quick reference to the chapter's contents and is a useful study aid.
- *Figures and tables*—Screenshots are used as guidelines for stepping through commands and forensics tools. For tools not included with the book or that aren't offered in free demo versions, figures have been added when possible to illustrate the tool's interface. Tables are used throughout the book to present information in an organized, easy-to-grasp manner.
- *Chapter summaries*—Each chapter's material is followed by a summary of the concepts introduced in that chapter. These summaries are a helpful way to review the ideas covered in each chapter.
- *Key terms*—Following the chapter summary, all new terms introduced in the chapter with boldfaced text are gathered together in the Key Terms list. This list encourages a more thorough understanding of the chapter's key concepts and is a useful reference.
- *Review questions*—The end-of-chapter assessment begins with a set of review questions that reinforce the main concepts in each chapter. These questions help you evaluate and apply the material you have learned.

- *Hands-on projects*—Although understanding the theory behind digital technology is important, nothing can improve on real-world experience. To this end, each chapter offers several hands-on projects with software supplied as free downloads on the student companion site and in MindTap. You can explore a variety of ways to acquire and even hide evidence. For the conceptual chapters, research projects are supplied.
- *Case projects*—At the end of each chapter are case projects. To do these projects, you must draw on real-world common sense as well as your knowledge of the technical topics covered to that point in the book. Your goal for each project is to come up with answers to problems similar to those you'll face as a working digital forensics investigator.
- *Software and student data files*—Student data files are available for download from the student companion site and the MindTap for this book and are used for activities and projects in the chapters. Demo and freeware software used in this book can be downloaded from the Web sites specified in activities and projects or in "Digital Forensics Software" later in this introduction.
- *Student companion site*—To access the student companion site, go to *www.cengagebrain.com* and search for the sixth edition by entering the title, author's name, or ISBN. On the product page, click the Free Materials tab, and then click Save to MyHome. Then you can sign in as a returning student or choose to create a new account. After you've logged on, you can begin accessing your free study tools.

Text and Graphic Conventions

When appropriate, additional information and exercises have been added to this book to help you better understand the topic at hand. The following icons used in this book alert you to additional materials:

Note

The Note icon draws your attention to additional helpful material related to the subject being covered.

Tip

Tips based on the authors' experiences offer extra information about how to attack a problem or what to do in real-world situations.

Caution

The Caution icon warns you about potential mistakes or problems and explains how to avoid them.

Hands-On Projects

The hands-on icon indicates that the projects following it give you a chance to practice using software tools and get hands-on experience.

Case Projects

This icon marks the start of projects that require you to apply common sense and knowledge to solving problems involving that chapter's concepts.

Student Resources

MindTap for Guide to Computer Forensics and Investigations helps you learn on your terms.

- Instant access in your pocket: Take advantage of the MindTap Mobile App to learn on your terms. Read or listen to textbooks and study with the aid of instructor notifications, flashcards, and practice quizzes.
- MindTap helps you create your own potential. Gear up for ultimate success: Track your scores and stay motivated toward your goals. Whether you have more work to do or are ahead of the curve, you'll know where you need to focus your efforts. The MindTap Green Dot will charge your confidence along the way.
- MindTap helps you own your progress. Make your textbook yours; no one knows what works for you better than you. Highlight key text, add notes, and create custom flashcards. When it's time to study, everything you've flagged or noted can be gathered into a guide you can organize.

Lab Manual

A new digital lab manual is being offered in the *MindTap for Guide to Computer Forensics and Investigations* to give you additional hands-on experience.

Lab Requirements

The hands-on projects in this book help you apply what you have learned about digital forensics techniques. The following sections list the minimum requirements for completing all the projects in this book. In addition to the items listed, you must be able to download and install demo versions of software.

Note

Magnet AXIOM has a 30-day trial for download. If you aren't purchasing its academic license or are planning to do the labs at home, it's recommended that you wait until **Chapter 11** to begin using this tool so that your trial doesn't expire before you finish the projects. In addition, wait until Chapter 11 before doing Hands-On Project 6–5, installing Magnet AXIOM.

Note

OSForensics from PassMark Software also has a 30-day trial for download. If you aren't purchasing its license or are planning to do the labs at home, it's recommended that you wait until **Chapter 4** to begin using this tool so that your trial doesn't expire before you finish the projects.

Minimum Lab Requirements

- Lab computers that boot to Windows 7, 8, 8.1, or 10
- An external USB, FireWire, or SATA drive larger than a typical 1 TB USB drive

The projects in this book are designed with the following hardware and software requirements in mind. The labs in which most of the work takes place should be typical network training labs with a variety of operating systems and computers available.

Operating Systems and Hardware

Windows 7, 8, 8.1, or 10

Use a standard installation of Windows. The computer running Windows should be a fairly current model that meets the following minimum requirements:

- USB ports
- CD-ROM/DVD-ROM drive
- VGA or higher monitor
- Hard disk partition of 500 GB or more
- Mouse or other pointing device
- Keyboard
- At least 6 GB RAM (more is recommended)

Linux

For this book, it's assumed you're using an Ubuntu 16.04 or later standard installation, although other Linux distributions will work with minor modifications. Also, some projects use specialized "live" Linux distributions, such as Kali Linux.

- Hard disk partition of 6 GB or more reserved for Linux
- Other hardware requirements are the same as those listed for Windows computers

Digital Forensics Software

This book includes projects using the following software, most of which can be downloaded from the Internet as freeware, shareware, or demo versions:

Note

Because Web site addresses change frequently, search online to find the following software if URLs are no longer valid. Efforts have been made to provide information that's current at the time of writing, but things change constantly on the Web. Learning how to use search tools to find what you need is a valuable skill you'll use as a digital forensics investigator. Demoware tools typically have limited functions and strict time limits on their use. See their licensing information for restrictions when using vendors' demoware tools.

Vendor	Tool	Version	License	Download Link
AccessData	FTK Imager Lite	3.1.1	Demoware	https://accessdata.com/product-download/ftk-imager-lite-version-3.1.1
AccessData	Registry Viewer	1.8.0.5	Demoware	https://accessdata.com/product-download/registry-viewer-1-8-0-5
Aid4Mail	Aid4Mail	N/A	Demoware	www.aid4mail.com/download-free-trial
BreakPoint Software	Hex Workshop	6.8.0	Demoware	www.bpsoft.com/downloads/
Cellebrite	UFED Reader	3.2	Demoware	www.cfreds.nist.gov/
Citrix	XenServer	7.2	Demoware	https://xenserver.org/open-source-virtualization-download.html
Deft Linux	DEFT Zero	2017.1	Open-source	www.deftlinux.net/download/
Kali.org	Kali	2017.3	Open-source	www.kali.org/downloads/
PassMark	OSForensics	4.0.1002	Demoware	www.osforensics.com/download.html

Vendor	Tool	Version	License	Download Link
Santoku	Santoku Linux	0.5	Open-source	http://santoku-linux.com/download/
Sleuthkit.org	Autopsy	4.3.0	Open-source	https://sourceforge.net/projects/autopsy/files/autopsy/4.3.0/
S-Tools	S-Tools4	N/A	Open-source	https://packetstormsecurity.com/files/21688/s-tools4.zip.html
Ubuntu	Ubuntu Linux	17.10	Open-source	www.ubuntu.com/download
VirtualBox	VirtualBox	5.2.4	Open-source	www.virtualbox.org/wiki/Downloads
VMware	VMware Workstation Player	14.0.0	Demoware	https://my.vmware.com/en/web/vmware/free#desktop_end_user_compu
X-Ways	WinHex	19.5	Demoware	www.x-ways.net/winhex/

In addition, you use Microsoft Office Word (or other word processing software) and Excel (or other spreadsheet software) as well as a Web browser.

About the Authors

Bill Nelson has worked for more than 32 years for two global Fortune 100 companies in information technologies, with more than 20 years in corporate digital forensics and information security. In addition, he has been an instructor of digital forensics classes at the City University of Seattle and the University of Washington's Professional and Continuing Education Department for 10 years. His previous experience includes Automated Fingerprint Identification System software engineering and reserve police work. Bill has served as president and vice president for Computer Technology Investigators Northwest. He routinely lectures at several colleges and universities in the Pacific Northwest.

Amelia Phillips is a graduate of the Massachusetts Institute of Technology with B.S. degrees in astronautical engineering and archaeology and an MBA in technology management. She also holds an interdisciplinary Ph.D. in computer security from the University of Alaska, Fairbanks. After serving as an engineer at the Jet Propulsion Lab, she worked with e-commerce Web sites and began her training in computer forensics to prevent stealing credit card numbers from sensitive e-commerce databases. She has designed certificate and AAS programs for community colleges in e-commerce, network security, computer forensics, and data recovery. She also designed the Bachelor of Applied Science program in cybersecurity and forensics at Highline College and was instrumental in its becoming a National Center of Academic Excellence in Cyber Defense. Amelia has served as the Regional Director of the Pacific Rim Collegiate Cyber Defense Competition for many years and is the PI for the International Collegiate Cyber Defense Invitational. She is tenured at Highline College in Seattle, Washington. Amelia is a Fulbright

Scholar who taught at Polytechnic of Namibia (now Namibia University of Science and Technology) in 2005 and 2006 and is currently a Fulbright Ambassador for the 2017–2019 term. She continues her work with developing nations and travels there frequently.

Christopher K. Steuart is a practicing attorney maintaining a general litigation practice, with experience in information systems security for a Fortune 50 company and the U.S. Army. He is also an honorary life member and the former general counsel for Computer Investigators Northwest. He has presented computer forensics seminars in regional and national forums, including the American Society for Industrial Security, Agora, Northwest Computer Technology Crime Analysis Seminar, and Computer Investigators Northwest. He is currently vice president and general counsel for IT Forensics, Inc.

Acknowledgments

The team would like to thank the entire editorial and production staff for their dedication and fortitude during this project, including Natalie Onderdonk, Learning Designer, and Brooke Greenhouse, Senior Content Manager. Our special thanks go to Lisa Lord, the development editor. We also appreciate the careful reading and thoughtful suggestions of the technical editor, Danielle Shaw. We would like to thank the reviewers: Henry Felch, University of Maine, Augusta; Eddie Horton, Northeastern State University; Todd Koonts, Central Piedmont Community College; and Tenette Prevatte, Fayetteville Technical Community College. We would also like to thank our colleagues in professional groups in Washington State and Mike Lacey for his photos.

Bill Nelson

I want to express my appreciation to my wife, Tricia, for her support during the long hours spent writing. I would also like to express appreciation to my co-authors along with our editor, Lisa Lord; technical editor, Danielle Shaw; and book reviewers for the team effort in producing this book. Special thanks for the support and encouragement from my digital forensics colleagues: Franklin Clark, retired investigator for the Pierce County Prosecutor's Office, Tacoma, Washington; John Sgromolo of Verizon; Stefan Fleischmann of X-Ways; Gordon Ross, formerly of Net Nanny; and Gordon Mitchell of Future Focus, Inc. In addition, special thanks to colleagues Troy Larson of Microsoft and Brett Shavers.

Amelia Phillips

My deepest gratitude goes to my co-author Bill Nelson. I want to reiterate the thanks to Lisa Lord for her patience and support and to all the people who have helped us in the past, including Teresa Mobley, Ron Godfrey, Deb Buser, and Detective Melissa Rogers. Acknowledgments go to my many past and present students who have helped with research on what's happening in the field of digital forensics. Special thanks go to Jens Kircher at X-Ways, who contributed to the Macintosh and Linux chapter, for his insight into these OSs. Thanks to my friends in Namibia, without whom I would not have such a thorough understanding of the different laws on digital evidence and privacy, and special thanks to Dr. Jack Bermingham (President Emeritus of Highline College), Dr. Jeff Wagnitz, Alice Madsen, and Dr. Rolita Ezeonu, who have funded and supported me as I experienced what it means to get a Ph.D., write two textbooks, create a bachelor's program, and work full time. Thanks go to my friends and family members for their support, and the most special thanks go to my aunties, who were all at some point in their lives great teachers and set an excellent example for me. Without them, this would not be possible.

Christopher K. Steuart

I would like to express my appreciation to my wife, Josephine, son, Alexander, and daughter, Isobel, for their enthusiastic support of my commitment to this book, even as it consumed time and energy that they deserved. I also want to express my thanks to my parents, William and Mary, for their support of my education and development of the skills needed for this project. I thank my co-authors for inviting me to join them in this project. I would like to express my appreciation to the Boy Scouts of America for providing me with the first of many leadership

opportunities in my life. I want to recognize Lieutenant General (then Captain) Edward Soriano for seeing the potential in me as a young soldier and encouraging me in learning the skills required to administer, communicate with, and command an organization within the structure of law, regulation, and personal commitment. I must also thank the faculty of Drake University Law School, particularly Professor James A. Albert, for encouraging me to think and write creatively about the law. I also note the contribution of Diane Gagon and the staff of the Church of Scientology in Seattle, Washington, in supporting my better understanding of commitment to myself and others.

Chapter 1. Understanding the Digital Forensics Profession and Investigations

After reading this chapter and completing the exercises, you will be able to:

- Describe the field of digital forensics
- Explain how to prepare for computer investigations and summarize the difference between public-sector and private-sector investigations
- Explain the importance of maintaining professional conduct
- Describe how to prepare a digital forensics investigation by taking a systematic approach
- Describe procedures for private-sector digital investigations
- Explain requirements for data recovery workstations and software
- Summarize how to conduct an investigation, including critiquing a case

In the past several years, the field of computer forensics has developed significantly, including new terminology. This chapter introduces you to computer forensics or, as it's now typically called, digital forensics and discusses issues of importance in the industry. This book blends traditional investigative methods with classic systems analysis problem-solving techniques and applies them to investigations involving computers and other digital media and systems. Understanding these disciplines combined with the use of the forensics tools will make you a skilled digital forensics examiner.

This chapter also gives you an overview of how to manage a digital investigation and use standard problem-solving techniques. You learn about the problems and challenges forensics examiners face when preparing and processing investigations, including the ideas and questions they must consider. To perform the activities and projects in this chapter, you work with forensic disk images from small USB drives and then can apply the same techniques to a large disk.

An Overview of Digital Forensics

As the world has become more of a level playing field, with more people online who have access to the same information (Thomas L. Freidman, *The World Is Flat*, Farrar, Straus, and Giroux, 2005), the need to standardize digital forensics processes has become more urgent. The definition of **digital forensics** has also evolved over the years from simply involving securing and analyzing digital information stored on a computer for use as evidence in civil, criminal, or administrative cases. The former director of the Defense Computer Forensics Laboratory, Ken Zatyko, wrote a treatise on the many specialties including computer forensics, network forensics, video forensics, and a host of others. He defined it as "[t]he application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence (information of probative value that is stored or transmitted in binary form) after proper search authority, chain of custody, validation with mathematics (hash function), use of validated tools, repeatability, reporting and possible expert presentation" ("Commentary: Defining Digital Forensics," *Forensic Magazine*, 2007).

The field of digital forensics can also encompass items such as research and incident response. With incident response, most organizations are concerned with protecting their assets and containing the situation, not necessarily prosecuting or finding the person responsible. Research in digital forensics also isn't concerned with prosecution or validity of evidence. This book is intended for digital forensics investigators and examiners at the civil, criminal, and administrative levels. Other facets of digital forensics are beyond the scope of this book. Keep in mind that depending on the jurisdiction and situation, forensic investigators and examiners might be the same or different personnel. In this book, the terms are used interchangeably.

Note

For a more in-depth discussion of what the term "digital forensics" means, see "Digital Forensic Evidence Examination" (Fred Cohen, www.fredcohen.net/Books/2013-DFE-Examination.pdf, 2012).

Many groups have tried to create digital forensics certifications that could be recognized worldwide but have failed in this attempt. However, they have created certifications for specific categories of practitioners, such as government investigators. With the ubiquitous access to mobile devices now, digital evidence is everywhere, so the need for a global standardized method is even more critical so that companies and governments can share and use digital evidence. In October 2012, an International Organization for Standardization (ISO) standard for digital forensics was ratified. This standard, ISO 27037 "Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence" (see www.iso.org/standard/44381.html), defines the personnel and methods for acquiring and preserving digital evidence. To address the multinational cases that continue to emerge, agencies in every country should develop policies and procedures that meet this standard.

The Federal Rules of Evidence (FRE), signed into law in 1973, was created to ensure consistency in federal proceedings, but many states' rules map to the FRE, too. In another attempt to standardize procedures, the FBI Computer Analysis and Response Team (CART) was formed in 1984 to handle the increase in cases involving digital evidence. By the late 1990s, CART had teamed up with the Department of Defense Computer Forensics Laboratory (DCFL) for research and training. Much of the early curriculum in this field came from the DCFL. For more information on the FBI's cybercrime investigation services, see www.fbi.gov/investigate/cyber.

Files maintained on a computer are covered by different rules, depending on the nature of the documents. Many court cases in state and federal courts have developed and clarified how the rules apply to digital evidence. The **Fourth Amendment** to the U.S. Constitution (and each state's constitution) protects everyone's right to be secure in their person, residence, and property from search and seizure. Continuing development of the jurisprudence of this amendment has played a role in determining whether the search for digital evidence has established a different precedent, so separate **search warrants** might not be necessary. However, when preparing to search for evidence in a criminal case, many investigators still include the suspect's computer and its components in the search warrant to avoid later admissibility problems.

In an important case involving these issues, the Pennsylvania Supreme Court addressed expectations of privacy and whether evidence is admissible (see *Commonwealth v. Copenhefer*, 587 A.2d 1353, 526 Pa. 555 [1991]). Initial investigations by the FBI, state police, and local police resulted in discovering computer-generated notes and instructions—some of which had been deleted—that had been concealed in hiding places around Corry, Pennsylvania. The investigation also produced several possible suspects, including David Copenhefer, who owned a nearby bookstore and apparently had bad relationships with the victim and her husband. Examination of trash discarded from Copenhefer's store revealed drafts of the ransom note and directions. Subsequent search warrants resulted in seizure of evidence against him. Copenhefer's computer contained several drafts and amendments of the text of phone calls to the victim and the victim's husband the next day, the ransom note, the series of hidden notes, and a plan for the entire kidnapping scheme (*Copenhefer*, p. 559).

On direct appeal, the Pennsylvania Supreme Court concluded that the physical evidence, including the digital forensics evidence, was sufficient to support the bookstore owner's conviction. Copenhefer's argument was that "[E]ven though his computer was validly seized

pursuant to a warrant, his attempted deletion of the documents in question created an expectation of privacy protected by the Fourth Amendment. Thus, he claims, under *Katz v. United States*, 389 U.S. 347, 357, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967), and its progeny, Agent Johnson's retrieval of the documents, without first obtaining another search warrant, was unreasonable under the Fourth Amendment and the documents thus seized should have been suppressed" (*Copenhefer*, p. 561).

The Pennsylvania Supreme Court rejected this argument, stating, "A defendant's attempt to secrete evidence of a crime is not synonymous with a legally cognizable expectation of privacy. A mere hope for secrecy is not a legally protected expectation. If it were, search warrants would be required in a vast number of cases where warrants are clearly not necessary" (*Copenhefer*, p. 562).

Every U.S. jurisdiction has case law related to the admissibility of evidence recovered from computers and other digital devices. As you learn in this book, however, the laws on digital evidence vary between states as well as between provinces and countries.

Note

The U.S. Department of Justice offers a useful guide to search and seizure procedures for computers and computer evidence at https://pdfs.semanticscholar.org/aabb/8b0caf982a0aa211f932252af38d4c9376fb.pdf.

Digital Forensics and Other Related Disciplines

According to DIBS USA, Inc., a privately owned corporation specializing in digital forensics since the 1990s (www.dibsforensics.com), digital forensics involves scientifically examining and analyzing data from computer storage media so that it can be used as evidence in court. In the National Institute of Standards and Technology (NIST) document "Guide to Integrating Forensic Techniques into Incident Response" (http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf, 2006), digital forensics is defined as "the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data." Typically, investigating digital devices includes collecting data securely, examining suspect data to determine details such as origin and content, presenting digital information to courts, and applying laws to digital device practices.

In general, digital forensics is used to investigate data that can be retrieved from a computer's hard drive or other storage media. Like an archaeologist excavating a site, digital forensics examiners retrieve information from a computer or its components. The information retrieved might already be on the drive, but it might not be easy to find or decipher. On the other hand, network forensics yields information about how attackers gain access to a network along with files they might have copied, examined, or tampered with. Network forensics examiners use log files to determine when users logged on and determine which URLs users accessed, how they logged on to the network, and from what location. Network forensics also tries to determine what tracks or new files were left behind on a victim's computer and what changes were made. In **Chapter 10**, you explore when and how network forensics should be used in an investigation.

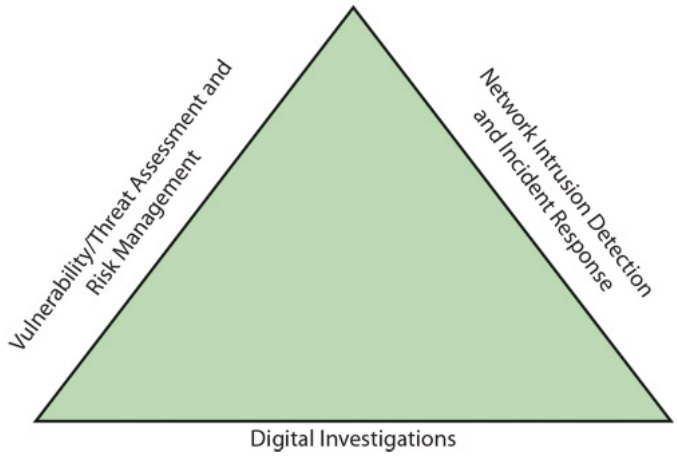
Digital forensics is also different from **data recovery** , which involves retrieving information that was deleted by mistake or lost during a power surge or server crash, for example. In data recovery, typically you know what you're looking for. Digital forensics is the task of recovering data that users have hidden or deleted, with the goal of ensuring that the recovered data is valid so that it can be used as evidence. In this regard, digital forensics differs from other types of evidence recovered from a scene. When investigators in a crime scene unit retrieve blood or

hair or bullets, they can identify what it is. When a laptop, smartphone, or other digital device is retrieved, its contents are unknown and pose a challenge to the examiner. The evidence can be **inculpatory evidence** (in criminal cases, the expression is "incriminating") or **exculpatory evidence** , meaning it tends to clear the suspect. Examiners often approach a digital device not knowing whether it contains evidence. They must search storage media and piece together any data they find. Forensics software tools can be used for most cases. In extreme cases, examiners can use electron microscopes and other sophisticated equipment to retrieve information from machines that have been damaged or reformatted purposefully. This method is usually cost prohibitive, so it's not normally used.

Forensics investigators often work as part of a team to secure an organization's computers and networks. The digital investigation function can be viewed as part of a triad that makes up computing security. Rapid progress in technology has resulted in an expansion of the skills needed and varies depending on the organization using practitioners in this field. **Figure 1-1** shows the investigations triad made up of these functions:

- Vulnerability/threat assessment and risk management
- Network intrusion detection and incident response
- Digital investigations

Figure 1-1.



The investigations triad

Each side of the triad in **Figure 1-1** represents a group or department responsible for performing the associated tasks. Although each function operates independently, all three groups draw from one another when a large-scale digital investigation is being conducted. By combining these three groups into a team, all aspects of a digital technology investigation can be addressed without calling in outside specialists. In smaller companies, one group might perform all the tasks shown in the investigations triad, or a small company might contract with service providers to perform these tasks.

When you work in the **vulnerability/threat assessment and risk management** group, you test and verify the integrity of stand-alone workstations and network servers. This integrity check covers the physical security of systems and the security of operating systems (OSs) and applications. People working in this group (often known as penetration testers) test for vulnerabilities of OSs and applications used in the network and conduct authorized attacks on the network to assess vulnerabilities. Typically, people performing this task have several years of experience in system administration. Their job is to poke holes in the network to help an organization be better prepared for a real attack.

Professionals in the vulnerability assessment and risk management group also need skills in **network intrusion detection and incident response** . This group detects intruder attacks by using automated tools and monitoring network firewall logs. When an external attack is detected, the response team tracks, locates, and identifies the intrusion method and denies further access to the network. If an intruder launches an attack that causes damage or potential damage, this team collects the necessary evidence, which can be used for civil or criminal litigation against the intruder and to prevent future intrusions. If an internal user is engaged in illegal acts or policy violations, the network intrusion detection and incident response group might assist in locating the user. For example, someone at a community college sends e-mails containing a worm to other users on the network. The network team realizes the e-mails are coming from a node on the internal network, and the security team focuses on that node. The **digital investigations** group manages investigations and conducts forensics analysis of systems suspected of containing evidence related to an incident or a crime. For complex casework, this group draws on resources from personnel in vulnerability assessment, risk management, and network intrusion detection and incident response. However, the digital investigations group typically resolves or terminates case investigations.

A Brief History of Digital Forensics

Fifty years ago, few people imagined that computers would be an integral part of everyday life. Now computer technology is commonplace, as are crimes in which a digital device is the instrument of the crime, the target of the crime, and, by its nature, the location where evidence is stored.

By the 1970s, electronic crimes were increasing, especially in the financial sector. Most computers in that era were mainframes, used by trained people with specialized skills who worked in finance, engineering, and academia. White-collar fraud began when people in these industries saw a way to make money by manipulating computer data. One of the most well-known crimes of the mainframe era is the one-half cent crime. Banks commonly tracked money in accounts to the third decimal place or more. They used and still use the rounding-up accounting method when paying interest. If the interest applied to an account resulted in a fraction of a cent, that fraction was used in the calculation for the next account until the total resulted in a whole cent. It was assumed that eventually every customer would benefit from this averaging. Some computer programmers corrupted this method by opening an account for themselves and writing programs that diverted all the fractional monies into their accounts. In small banks, this practice amounted to only a few hundred dollars a month. In large banks with millions of accounts, however, the amount could reach hundreds of thousands of dollars.

During this time, most law enforcement officers didn't know enough about computers to ask the right questions or to preserve evidence for trial. Many began to attend Federal Law Enforcement Training Center (FLETC) programs designed to train law enforcement in handling digital data.

As PCs gained popularity and began to replace mainframe computers in the 1980s, many different OSs emerged. Apple released the Apple IIe in 1983 and then the Macintosh in 1984. Computers such as the TRS-80 and Commodore 64 were the machines of the day. CP/M machines, such as the Kaypro and Zenith, were also in demand.

Disk Operating System (DOS) was available in many varieties, including PC-DOS, QDOS, DR-DOS, IBM-DOS, and MS-DOS. Forensics tools at that time were simple, and most were generated by government agencies, such as the Royal Canadian Mounted Police (RCMP, which had its own investigative tools) and the U.S. Internal Revenue Service (IRS). Most tools were written in C and assembly language and weren't available to the general public.

In the mid-1980s, a new tool, Xtree Gold, appeared on the market. It recognized file types and retrieved lost or deleted files. Norton DiskEdit soon followed and became the preferred tool for finding and recovering deleted files. You could use these tools on the most powerful PCs of

that time; IBM-compatible computers had hard disks of 10 to 40 MB and two floppy drives, as shown in **Figure 1-2**.

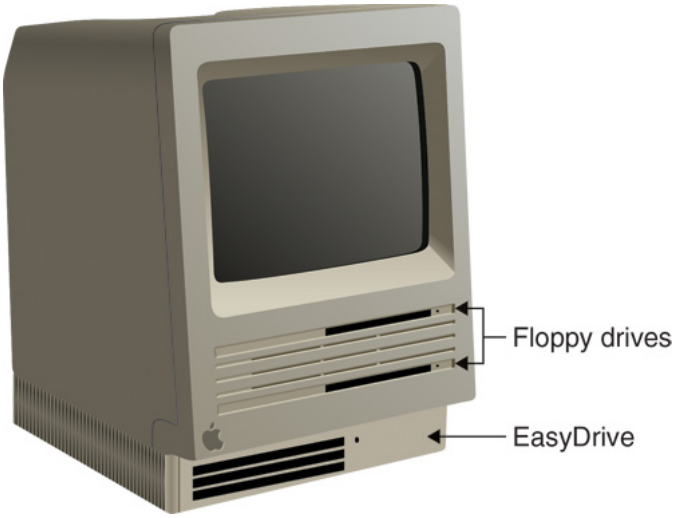
Figure 1-2.

© iStock.com/Maxiphoto

An 8088 computer

In 1987, Apple produced the Mac SE, a Macintosh with an external EasyDrive hard disk with 60 MB of storage (see **Figure 1-3**). At this time, the popular Commodore 64 still used standard audiotapes to record data, so the Mac SE represented an important advance in computer technology.

Figure 1-3.



A Mac SE with an external EasyDrive hard disk

By the early 1990s, specialized tools for digital forensics were available. The **International Association of Computer Investigative Specialists (IACIS)** introduced training on software for digital forensics examinations, and the IRS created search-warrant programs. However, no commercial GUI software for digital forensics was available until ASR Data created Expert Witness for Macintosh. This software could recover deleted files and fragments of deleted files. One of the ASR Data partners later left and developed EnCase, which became a popular digital forensics tool.

As computer technology continued to evolve, more digital forensics software was developed. The introduction of large hard disks posed new problems for investigators. Most DOS-based software didn't recognize a hard disk larger than 8 GB. Because contemporary computers have hard disks of 500 GB and often much larger, changes in forensics software were needed. Later in this book, you explore the challenges of examining older software and hardware.

Other tools, such as ILook, which is currently maintained by the IRS Criminal Investigation Division and limited to law enforcement, can analyze and read special files that are copies of a disk. AccessData Forensic Toolkit (FTK) has become a popular commercial product that performs similar tasks in the law enforcement and civilian markets.

As software companies become savvier about digital forensics and investigations, they are producing more forensics tools to keep pace with technology. This book describes several tools but by no means all available tools. You should refer to trade publications, e-zines, and Web sites to stay current.

Understanding Case Law

Existing laws and statutes simply can't keep up with the rate of technological change. Therefore, when statutes or regulations don't exist, case law is used. In common law nations, such as the United States, case law allows legal counsel to apply previous similar cases to current ones in an effort to address ambiguity in laws. Examiners must be familiar with recent court rulings on search and seizure in the electronic environment to avoid mistakes such as exceeding a search warrant's authority. Recent events involving privacy incursions by government agencies have resulted in new laws and policies. Developments in technology have changed how everyday events are viewed. For example, what should be considered private conversations? Which devices are actually protected?

Although law enforcement can certainly confiscate anything an arrested person is carrying and log that a device, such as a smartphone, was on the person, they don't necessarily have the right or authority to search the device. These actions are being challenged in courts constantly. Remaining vigilant in keeping up with changing case law is critical to being an effective digital forensics investigator.

Developing Digital Forensics Resources

To be a successful digital forensics investigator, you must be familiar with more than one computing platform. In addition to older platforms, such as DOS, Windows 9x, and Windows XP, you should be familiar with Linux, macOS, and current Windows platforms. However, no one can be an expert in every aspect of computing. Likewise, you can't know everything about the technology you're investigating. To supplement your knowledge, you should develop and maintain contact with digital, network, and investigative professionals.

Join computer user groups in both the public and private sectors. In the Pacific Northwest, for example, **Computer Technology Investigators Network (CTIN)** meets to discuss problems that digital forensics examiners encounter. This nonprofit organization also conducts training. IACIS is an excellent group for law enforcement personnel but doesn't have local chapters. However, groups such as the High Technology Crime Investigation Association, International Information Systems Security Certification Consortium $(ISC)^2$, and InfraGard have local chapters open to professionals in most major cities. Build your own network of digital forensics experts, and keep in touch through e-mail. Cultivate professional relationships with people who specialize in technical areas different from your own specialty. If you're a Windows expert, for example, maintain contact with experts in Linux, UNIX, and macOS. If you're using social media to interact with experts, exercise caution and good judgment when communicating with people you haven't met in person or whose backgrounds you don't know.

User groups can be especially helpful when you need information about obscure OSs. For example, a user group helped convict a child molester in Pierce County, Washington, in 1996.

The suspect installed video cameras throughout his house, served alcohol to young women to intoxicate them, and secretly filmed them playing strip poker. When he was accused of molesting a child, police seized his computers and other physical evidence. The investigator discovered that the computers used CoCo DOS, an OS that had been out of use for years. The investigator contacted a local user group, which supplied the standard commands and other information needed to access the system. On the suspect's computer, the investigator found a diary detailing the suspect's actions over 15 years, including the molestation of more than 400 young women. As a result, the suspect received a longer sentence than if he had been convicted of molesting only one child.

Outside experts can also give you detailed information you need to retrieve digital evidence. For example, a recent murder case involved a husband and wife who owned a Macintosh store. When the wife was discovered dead, apparently murdered, investigators found that she had wanted to leave her husband but didn't because of her religious beliefs. The police got a search warrant and confiscated the home and office computers. When the detective on the case examined the home system, he found that the hard drive had been compressed and erased. He contacted a Macintosh engineer, who determined the two software programs used to compress the drive. With this knowledge, the detective could retrieve information from the hard drive, including text files indicating that the husband spent $35,000 in business funds to purchase cocaine and prostitution services. This evidence proved crucial in making it possible to convict the husband of murder.

Preparing for Digital Investigations

Digital investigations can be categorized several ways. For the purposes of this discussion, however, they fall into two categories: public-sector investigations and private-sector investigations (see **Figure 1-4**).

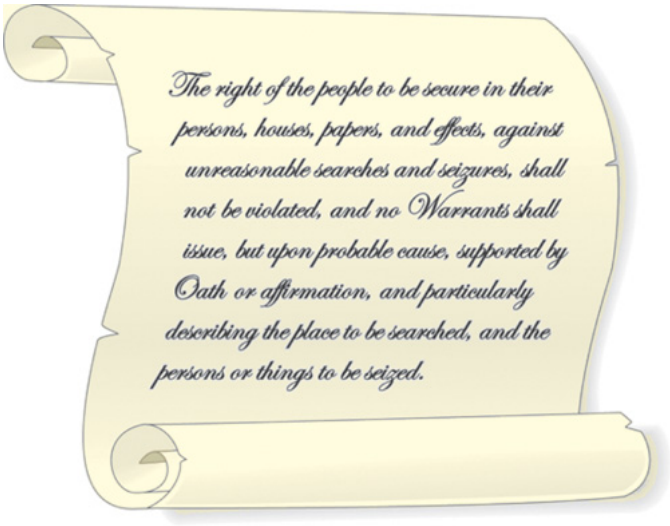
Figure 1-4.

iStock.com/RobinsonBecquart, iStock.com/buzbuzzer

Public-sector and private-sector investigations

In general, public-sector investigations involve government agencies responsible for criminal investigations and prosecution. Government agencies range from municipal, county, and state or provincial police departments to federal law enforcement agencies. These organizations must observe legal guidelines of their jurisdictions, such as Article 8 in the Charter of Rights of Canada and the Fourth Amendment to the U.S. Constitution restricting government **search and seizure** (see Figure 1-5). The law of search and seizure in the United States protects the rights of people, including people suspected of crimes; as a digital forensics examiner, you must follow these laws. The Department of Justice (DOJ) updates information on computer search and seizure regularly.

Figure 1-5.



The Fourth Amendment

Private-sector investigations focus more on policy violations, such as not adhering to Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations. However, criminal acts, such as corporate espionage, can also occur. So although private-sector investigations often start as civil cases, they can develop into criminal cases; likewise, a criminal case can have implications leading to a civil case. If you follow good forensics procedures, the evidence found in your examinations can make the transition between civil and criminal cases.

Understanding Law Enforcement Agency Investigations

When conducting public-sector investigations, you must understand laws on computer-related crimes, including standard legal processes, guidelines on search and seizure, and how to build a criminal case. In a criminal case, a suspect is charged with a criminal offense, such as burglary, murder, molestation, or fraud. To determine whether there was a computer crime, an investigator asks questions such as the following: What was the tool used to commit the crime? Was it a simple trespass? Was it a theft or vandalism? Did the perpetrator infringe on someone else's rights by cyberstalking or e-mail harassment?

Note

Laws, including procedural rules, vary by jurisdiction. Therefore, this book points out when items accepted in U.S. courts don't stand up in other courts. Lately, a major issue has been that European Union (EU) privacy laws are more stringent than U.S. privacy laws. Issues related to international companies are still being defined. Over the past few decades, more companies have been consolidating into global entities. As a result, internal company investigations can involve laws of multiple countries. For example, a company has a subsidiary operating in Australia. An employee at that subsidiary is suspected of fraud, and as part of your investigation, you need to seize his cell phone. Under U.S. law, you can if he used it on company property and synchronized it with the company network. Under Australian law, you can't.

Computers and networks might be only tools used to commit crimes and are, therefore, analogous to the lockpick a burglar uses to break into a house. For this reason, many states have added specific language to criminal codes to define crimes involving computers. States such as Alabama have wording such as "willfully or without authorization" and specify what

dollar amount qualifies as a misdemeanor or a felony. For example, they have expanded the definition of laws for crimes such as theft to include taking data from a computer without the owner's permission, so computer theft is now on a par with shoplifting or car theft. States have also enacted specific criminal statutes that address computer-related crimes but typically don't include digital issues in standard trespass, theft, vandalism, or burglary laws. The Computer Fraud and Abuse Act was passed in 1986, but specific state laws were generally developed later.

Note

For information on how each state defines and addresses computer-related crimes, see http://statelaws.findlaw.com/criminal-laws/computer-crimes.html.

Many serious crimes involve computers, smartphones, and other digital devices. The most notorious are those involving sexual exploitation of minors. Digital images are stored on hard disks, flash drives, removable hard drives, and the cloud and are circulated on the Internet. Other computer crimes concern missing children and adults because information about missing people is often found on computers. Drug dealers, car theft rings, and other criminals often keep information about transactions on their computers, laptops, smartphones, and other devices.

Following Legal Processes

When conducting a computer investigation for potential criminal violations of the law, the legal processes you follow depend on local custom, legislative standards, and rules of evidence. In general, however, a criminal case follows three stages: the complaint, the investigation, and the prosecution. Someone files a complaint, and then a specialist investigates the complaint and, with the help of a prosecutor, collects evidence and builds a case. If the evidence is sufficient, the case might proceed to trial.

A criminal investigation generally begins when someone finds evidence of or witnesses an illegal act. The witness or victim makes an **allegation** to the police, an accusation of fact that a crime has been committed.

A police officer interviews the complainant and writes a report about the crime. The law enforcement agency processes the report, and management decides to start an investigation or log the information into a police blotter, which provides a record of information about crimes that have been committed previously. Criminals often repeat actions in their illegal activities, and these patterns can be discovered by examining police blotters. This historical knowledge is useful when conducting investigations, especially in high-technology crimes. Blotters now are generally electronic files, often structured as databases, so they can be searched more easily than the old paper blotters.

Tip

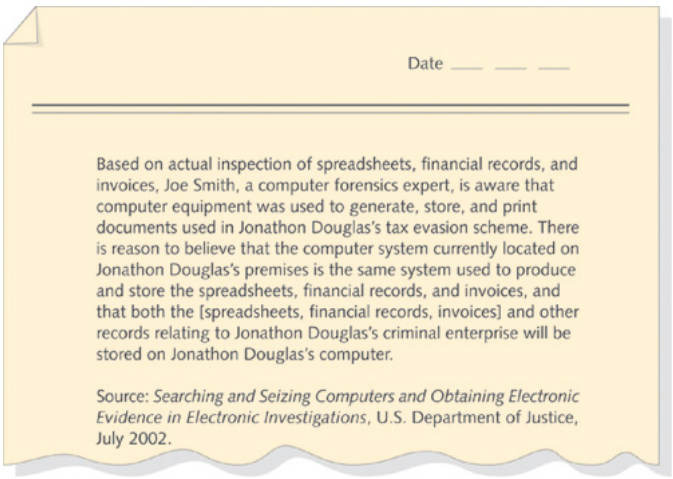
To see an example of a police blotter, go to http://spdblotter.seattle.gov.

Not every police officer is a computer expert. Some are computer novices; others might be trained to recognize what they can retrieve from a computer disk. To differentiate the training and experience officers have, ISO standard 27037 (www.iso.org/standard/44381.html) defines two categories. A **Digital Evidence First Responder (DEFR)** has the skill and training to arrive on an incident scene, assess the situation, and take precautions to acquire and preserve evidence. A **Digital Evidence Specialist (DES)** has the skill to analyze the data and determine when another specialist should be called in to assist with the analysis.

If you're an examiner assigned to a case, recognize the level of expertise of police officers and others involved in the case. You should have DES training to conduct the examination of systems and manage the digital forensics aspects of the case. You start by assessing the scope of the case, which includes the device's OS, hardware, and peripheral devices. You then determine whether resources are available to process all the evidence. Determine whether you have the right tools to collect and analyze evidence and whether you need to call on other specialists to assist in collecting and processing evidence. After you have gathered the resources you need, your role is to delegate, collect, and process the information related to the complaint. After you build a case, the information is turned over to the prosecutor. As an investigator, you must then present the collected evidence with a report to the government's attorney. Depending on the community and the nature of the crime, the prosecutor's title varies by jurisdiction.

In a criminal or public-sector case, if the police officer or investigator has sufficient cause to support a search warrant, the prosecuting attorney might direct him or her to submit an **affidavit** (also called a "declaration"). This sworn statement of support of facts about or evidence of a crime is submitted to a judge with the request for a search warrant before seizing evidence. Figure 1-6 shows a typical affidavit. It's your responsibility to write the affidavit, which must include **exhibits** (evidence) that support the allegation to justify the warrant. You must then have the affidavit notarized under sworn oath to verify that the information in the affidavit is true. (You learn more about affidavits and declarations in Chapter 14.)

Figure 1-6.



Date ___ ___ ___

Based on actual inspection of spreadsheets, financial records, and invoices, Joe Smith, a computer forensics expert, is aware that computer equipment was used to generate, store, and print documents used in Jonathon Douglas's tax evasion scheme. There is reason to believe that the computer system currently located on Jonathon Douglas's premises is the same system used to produce and store the spreadsheets, financial records, and invoices, and that both the [spreadsheets, financial records, invoices] and other records relating to Jonathon Douglas's criminal enterprise will be stored on Jonathon Douglas's computer.

Source: *Searching and Seizing Computers and Obtaining Electronic Evidence in Electronic Investigations*, U.S. Department of Justice, July 2002.

Typical affidavit language

In general, after a judge approves and signs a search warrant, it's ready to be executed, meaning a DEFR can collect evidence as defined by the warrant. After you collect the evidence, you process and analyze it to determine whether a crime actually occurred. The evidence can then be presented in court in a hearing or trial. A judge or an administrative law judge then renders a judgment, or a jury hands down a **verdict** (after which a judge can enter a judgment).

Understanding Private-Sector Investigations

Private-sector investigations involve private companies and lawyers who address company policy violations and litigation disputes, such as wrongful termination. When conducting an investigation for a private company, remember that business must continue with minimal interruption from your investigation. Because businesses usually focus on continuing their usual operations and making profits, many in a private-sector environment consider your

investigation and apprehension of a suspect secondary to stopping the violation and minimizing damage or loss to the business. Businesses also strive to minimize or eliminate litigation, which is an expensive way to address criminal or civil issues. Private-sector computer crimes can involve e-mail harassment; gender and age discrimination; **white-collar crimes** (defined by the FBI, www.fbi.gov/investigate/white-collar-crime), such as falsification of data, embezzlement, and sabotage; and **industrial espionage** , which involves selling sensitive or confidential company information to a competitor. Anyone with access to a computer can commit these crimes.

Establishing Company Policies

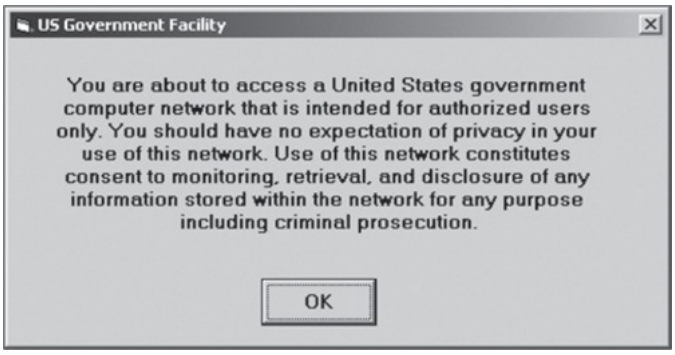
One way that businesses can reduce the risk of litigation is to publish and maintain policies that employees find easy to read and follow. In addition, these policies can make internal investigations go more smoothly. The most important policies are those defining rules for using the company's computers and networks; this type of policy is commonly known as an "acceptable use policy." Organizations should have all employees sign this acceptable use agreement. Published company policies also provide a **line of authority** for conducting internal investigations; it states who has the legal right to initiate an investigation, who can take possession of evidence, and who can have access to evidence.

Well-defined policies give computer investigators and forensics examiners the authority to conduct an investigation. Policies also demonstrate that an organization intends to be fair-minded and objective about how it treats employees and state that the organization will follow due process for all investigations. ("Due process" refers to fairness under the law and is meant to protect all.) Without defined policies, a business risks exposing itself to litigation from current or former employees. The person or committee in charge of maintaining company policies must also stay current with applicable laws, which can vary depending on the city, state, and country. In addition, training and updates on standards and policies should be scheduled regularly to keep employees informed of what should and shouldn't be done on the organization's network.

Displaying Warning Banners

Another way a private or public organization can avoid litigation is to display a warning banner on computer screens. A **warning banner** usually appears when a computer starts or connects to the company intranet, network, or virtual private network (VPN) and informs end users that the organization reserves the right to inspect computer systems and network traffic at will. (An end user is a person using a computer to perform routine tasks other than system administration.) If this right isn't stated explicitly, employees might have an assumed right of privacy when using a company's computer systems and network accesses. Figure 1-7 shows a sample warning banner.

Figure 1-7.



A sample warning banner

A warning banner asserts the right to conduct an investigation and notifies the user. By displaying a strong, well-worded warning banner, an organization owning computer equipment doesn't need a search warrant or court order as required under Fourth Amendment search-and-seizure rules to seize the equipment. In a company with a well-defined policy, this right to inspect or search at will applies to both criminal activity and company policy violations. Keep in mind, however, that your country's laws might differ. For example, in some countries, even though the company has the right to seize computers at any time, if employees are suspected of a criminal act, they must be informed at that time.

The following list recommends phrases to include in warning banners. Before using these warnings, consult with the organization's legal department for other required legal notices for your work area or department. Depending on the type of organization, the following text can be used in internal warning banners:

- Access to this system and network is restricted.
- Use of this system and network is for official business only.
- Systems and networks are subject to monitoring at any time by the owner.
- Using this system implies consent to monitoring by the owner.
- Unauthorized or illegal users of this system or network will be subject to discipline or prosecution.
- Users of this system agree that they have no expectation of privacy relating to all activity performed on this system.

Tip

The DOJ document at www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf has several examples of warning banners.

An organization such as a community college might simply state that systems and networks are subject to observation and monitoring at any time because members of the local community who aren't staff or students might use the facilities. A for-profit organization, on the other hand, could have proprietary information on its network and use all the phrases suggested in the preceding list. Guests, such as employees of business partners, might be allowed to use the system. The text that's displayed when a guest attempts to log on can include warnings similar to the following:

- This system is the property of Company X.
- This system is for authorized use only; unauthorized access is a violation of law and violators will be prosecuted.
- All activity, software, network traffic, and communications are subject to monitoring.

As a private-sector digital investigator, make sure a company displays a clearly worded warning banner. Without a banner, your authority to inspect might conflict with the user's expectation of privacy, and a court might have to determine the issue of authority to inspect. State laws vary on the expectation of privacy, but all states accept the concept of a waiver of the expectation of privacy. Additionally, the EU and its member nations impose substantial penalties for personal information that crosses national boundaries without the person's consent. For example, if your company is conducting an investigation at its subsidiary in the EU, you might not be able to acquire a network drive without notifying certain parties or making sure consent documents are in place.

Some might argue that written policies are all that are necessary. However, in the actual prosecution of cases, warning banners have been critical in determining that a user didn't have an expectation of privacy for information stored on the system. A warning banner has the additional advantage of being easier to present in trial as an exhibit than a policy manual. Government agencies, such as the Department of Energy, NASA, Lawrence Livermore Labs, and even public libraries, now require warning banners on all computer terminals on their systems. Many corporations also require warning banners as part of the logon/startup process.

Designating an Authorized Requester

As mentioned, investigations must establish a line of authority. In addition to using warning banners that state a company's rights of computer ownership, businesses are advised to specify an **authorized requester** who has the power to initiate investigations. Executive management should define a policy to avoid conflicts from competing interests in organizations. In large organizations, competition for funding or management support can become so fierce that people might create false allegations of misconduct to prevent competing departments from delivering a proposal for the same source of funds.

To avoid inappropriate investigations, executive management must also define and limit who's authorized to request a computer investigation and forensics analysis. Generally, the fewer groups with authority to request a computer investigation, the better. Examples of groups with this authority in a private-sector environment include the following:

- Corporate security investigations
- Corporate ethics office
- Corporate equal employment opportunity office
- Internal auditing
- The general counsel or legal department

All other groups should coordinate their requests through the corporate security investigations group. This policy separates the investigative process from the process of employee discipline.

Conducting Security Investigations

Conducting a digital investigation in the private sector is not much different from conducting one in the public sector. During public investigations, you search for evidence to support criminal allegations. During private investigations, you search for evidence to support allegations of violations of a company's rules or an attack on its assets. Three types of situations are common in private-sector environments:

- Abuse or misuse of digital assets
- E-mail abuse
- Internet abuse

Most digital investigations in the private sector involve misuse of digital assets. Typically, this misuse is referred to as "company rules violation." Digital abuse complaints often center on e-mail and Internet misuse by employees but could involve other digital resources, such as using company software to produce a product for personal profit. The scope of an e-mail investigation ranges from excessive use of a company's e-mail system for personal use to making threats or harassing others via e-mail. Some common e-mail abuses involve transmitting offensive messages. These types of messages can create a **hostile work environment** that can result in an employee's civil lawsuit against a company that does nothing to prevent or respond to it (in other words, implicitly condones the e-mail abuse).

Digital investigators also examine Internet abuse. Employees' abuse of Internet privileges ranges from excessive use, such as spending all day Web surfing, to viewing pornographic pictures on the Internet while at work. An extreme instance of Internet abuse is viewing contraband (illegal) pornographic images, such as child pornography. Viewing contraband images is a criminal act in most jurisdictions, and digital investigators must handle this situation with the highest level of professionalism and notify law enforcement. By enforcing policies consistently, a company minimizes its liability exposure. The role of a digital forensics examiner is to give management personnel complete and accurate information so that they can verify and correct abuse problems in an organization. (In later chapters, you learn the procedures for conducting these types of investigations.)

Actions that seem related to internal abuse could also have criminal or civil liability. Because any civil investigation can become a criminal investigation, you must treat all evidence you collect with the highest level of security and accountability. Later in this book, you learn the Federal Rules of Evidence (processes to ensure the chain of custody) and how to apply them to digital investigations.

Similarly, your private-sector investigation might seem to involve a civil, noncriminal matter, but as you progress through your analysis, you might identify a criminal matter, too. Because of this possibility, always remember that your work can come under the scrutiny of the civil or criminal legal system. The Federal Rules of Evidence are the same for civil and criminal matters. By applying the rules to all investigations uniformly, you eliminate any concerns about the admissibility of the evidence you develop. These standards are emphasized throughout this book.

Note

The silver-platter doctrine used to allow a civilian or private-sector investigative agent to deliver evidence obtained in a manner that violated the Fourth Amendment to a law enforcement agency. However, this doctrine was ruled unconstitutional in 1960 (see *Elkins v. United States*, 1960).

Remember that a police officer is a law enforcement agent. A private-sector investigator's job is to minimize risk to the company. After you turn over evidence to law enforcement and begin working under their direction, you become an agent of law enforcement, subject to the same restrictions on search and seizure as a law enforcement agent. A law enforcement agent can't ask you, as a private citizen, to obtain evidence that requires a warrant. The rules controlling the use of evidence collected by private citizens vary by jurisdiction, so check the law if you're investigating a case outside the United States.

Litigation is costly, so after you have assembled evidence, offending employees are usually disciplined. However, when you discover that a criminal act involving a third-party victim has been committed, you might have a legal and moral obligation to turn the information over to law enforcement. In the next section, you learn about situations in which criminal evidence must be separated from any company proprietary information.

Distinguishing Personal and Company Property

Many company policies distinguish between personal and company computer property; however, making this distinction can be difficult with cell phones, smartphones, personal notebooks, and tablet computers. For example, an employee brings her personal tablet to work and connects it to the company's wireless network. As the employee synchronizes information on the tablet with information in the company network, she copies some data in the tablet to the company network. During the synchronization, data on the company computer or network might be placed on the tablet, too. In this case, at least one question is "Does the information on the tablet belong to the company or the employee?"

Now suppose the company gave the employee the tablet as a holiday bonus. Can the company claim rights to this device? Similar issues come up when an employee brings in a smartphone and connects it to the company network. What rules apply? Because digital devices are part of daily life, you'll encounter these issues often. These questions are still being debated, however, and companies are establishing their own policies to handle them. In today's bring your own device (BYOD) environment, more companies are forced to address the issue of personal devices accessing the company network. Some companies simply state that if you connect a personal device to the business network, it falls under the same rules as company property.

Note

BYOD is a major challenge in company security, digital investigations, and compliance with regulations, including company policies.

Maintaining Professional Conduct

Your professional conduct as a digital investigator is critical because it determines your credibility. **Professional conduct** , discussed in more detail in Chapters 15 and 16, includes ethics, morals, and standards of behavior. As a professional, you must exhibit the highest level of professional behavior at all times. To do so, you must maintain objectivity and confidentiality during an investigation, expand your technical knowledge constantly, and conduct yourself with integrity. Maintaining objectivity means you form opinions based on your education, training, experience, and the evidence in your cases. Avoid making conclusions about your findings until you have exhausted all reasonable leads and considered the available facts. Your ultimate responsibility is to find relevant digital evidence. You must avoid prejudice or bias to maintain the integrity of your fact-finding in all investigations. For example, if you're employed by an attorney, don't allow the attorney's agenda to dictate the outcome of your investigation. Your reputation depends on maintaining your objectivity.

You must also maintain an investigation's credibility by maintaining confidentiality. Discuss the case only with people who need to know about it, such as other investigators involved in the case or someone in the line of authority. If you need advice from other professionals, discuss only the general terms and facts about the case without mentioning specifics. All investigations you conduct must be kept confidential, until you're designated as a witness or required by the attorney or court to release a report.

In the private-sector environment, confidentiality is critical, especially when dealing with employees who have been terminated. The agreement between the company and the employee might have been to represent the termination as a layoff or resignation in exchange for no bad references. If you give case details and the employee's name to others, your company could be liable for breach of contract.

In some instances, a civil case might become a criminal case, and it could be years before the case finally goes to trial or is settled. If an investigator talks about evidence with unauthorized people, the case could be damaged. When working for an attorney on an investigation, the attorney-work-product rule applies to all communications. This means you can discuss the case only with the attorney or other members of the team working with the attorney. All communication about the case to other people requires the attorney's approval.

In addition to maintaining objectivity and confidentiality, you can enhance your professional conduct by continuing your training. The field of digital investigations and forensics is changing constantly. You should stay current with the latest technical changes in computer hardware and software, networking, and forensic tools. You should also learn about the latest investigation techniques you can use in your cases. To continue your professional training, you should attend workshops, conferences, and vendor courses. You might also need to continue or enhance your formal education, such as pursuing certifications. You improve your

professional standing if you have at least an undergraduate degree in computing or a related field. If you don't have an advanced degree, consider graduate-level studies in a complementary area of study, such as business law or e-commerce. Several colleges and universities now offer associate's, bachelor's, and master's degrees and certificate programs in digital forensics. Many companies are willing to assist with employee education expenses because it's to their advantage that employees remain current in their knowledge.

In addition to education and training, membership in professional organizations adds to your credentials. These organizations often sponsor training and publications on the latest technical improvements and trends in digital forensic examinations. Also, keep up to date with the most current publications on digital forensics examination tools and techniques.

As a digital investigator and forensics professional, you're expected to maintain honesty and integrity. You must conduct yourself with the highest levels of integrity in all aspects of your life. Any indiscreet actions can embarrass you and give opposing attorneys opportunities to discredit you during your testimony in court or in depositions.

Preparing a Digital Forensics Investigation

Your role as a digital forensics professional is to gather data from a suspect's computer and determine whether there's evidence that a crime was committed or company policies or industry regulations have been violated. If the evidence suggests that a crime or policy violation has been committed, you begin to prepare a case, which is a collection of evidence you can offer in court or at a private-sector inquiry. This process involves investigating the suspect's computer and then preserving the evidence on a different computer. Before you begin investigating, however, you must follow an accepted procedure to prepare a case. By approaching each case methodically, you can evaluate the evidence thoroughly and document the **chain of custody** , which is the route evidence takes from the time you find it until the case is closed or goes to court.

The following sections present two sample cases—one involving a computer crime and another involving a company policy violation. Each example describes the typical steps of a forensics investigation, including gathering evidence, preparing a case, and preserving the evidence.

An Overview of a Computer Crime

Law enforcement officers often find computers, smartphones, and other devices as they're investigating crimes, gathering other evidence, or making arrests. These devices can contain information that helps law enforcement officers determine the chain of events leading to a crime or information providing evidence that's more likely to lead to a conviction. As an example of a case in which computers were involved in a crime, the police raided a suspected drug dealer's home and found a desktop computer, several USB drives (also called "flash drives" or "thumb drives"), a tablet computer, and a cell phone in a bedroom (see Figure 1-8). The computer was "bagged and tagged," meaning it was placed in evidence bags along with the storage media and then labeled with tags as part of the search and seizure.

Figure 1-8.

The crime scene

The lead detective on the case wants you to examine the computer and cell phone to find and organize data that could be evidence of a crime, such as files containing names of the drug dealer's contacts, text messages, and photos. The acquisitions officer gives you documentation of items the investigating officers collected with the computer, including a list of other storage media, such as removable disks and flash drives. The acquisitions officer also notes that the computer is a Windows 8 system, and the machine was running when it was discovered. Before shutting down the computer, the acquisitions officer photographs all open windows on the Windows desktop, including one showing File Explorer, and gives you the photos. (Before shutting down the computer, a live acquisition should be done to capture RAM, too. This procedure is discussed in **Chapter 10**.)

As a digital forensics investigator, you're grateful the officers followed proper procedure when acquiring the evidence. With digital evidence, it's important to realize how easily key data, such as the last access date, can be altered by an overeager investigator who's first on the scene. The U.S. DOJ has a document you can download that reviews the correct acquisition of electronic evidence, "Prosecuting Computer Crimes" (www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf, 2009). If this link has changed because of site updates, use the search feature.

In your preliminary assessment, you assume that the hard disk and storage media include intact files, such as e-mail messages, deleted files, and hidden files. A range of software is available for use in your investigation; your office uses the tool Autopsy from Sleuth Kit.

Note

This chapter introduces you to the principles applied to digital forensics. In **Chapter 6**, you learn the strengths and weaknesses of several software packages.

Tip

Because some cases involve computers running legacy OSs, older versions of tools often need to be used in forensics investigations. For example, the tool Norton DiskEdit was last available on the Norton System Works 2000 CD.

After your preliminary assessment, you identify the potential challenges in this case. Later, you perform the steps needed to investigate the case, including how to address risks and obstacles. Then you can begin the actual investigation and data retrieval.

An Overview of a Company Policy Violation

Companies often establish policies for employee use of computers. Employees surfing the Internet, sending personal e-mail, or using company computers for personal tasks during work hours can waste company time. Because lost time can cost companies millions of dollars, digital forensics specialists are often used to investigate policy violations. The following example describes a company policy violation.

Manager Steve Billings has been receiving complaints from customers about the job performance of one of his sales representatives, George Montgomery. George has worked as a representative for several years. He's been absent from work for two days but hasn't called in sick or told anyone why he wouldn't be at work. Another employee, Martha, is also missing and hasn't informed anyone of the reason for her absence. Steve asks the IT Department to confiscate George's hard drive and all storage media in his work area. He wants to know whether any information on George's computer and storage media might offer a clue to his whereabouts and job performance concerns. To help determine George's and Martha's whereabouts, you must take a systematic approach, described in the following section, to examining and analyzing the data found on George's desk.

Taking a Systematic Approach

When preparing a case, you can apply standard systems analysis steps, explained in the following list, to problem solving. Later in this chapter, you apply these steps to cases.

- *Make an initial assessment about the type of case you're investigating*—To assess the type of case you're handling, talk to others involved in the case and ask questions about the incident. Have law enforcement or company security officers already seized the computer, disks, peripherals, and other components? Do you need to visit an office or another location? Was the computer used to commit a crime, or does it contain evidence about another crime?
- *Determine a preliminary design or approach to the case*—Outline the general steps you need to follow to investigate the case. If the suspect is an employee and you need to acquire his or her system, determine whether you can seize the computer during work hours or have to wait until evening or weekend hours. If you're preparing a criminal case, determine what information law enforcement officers have already gathered.
- *Create a detailed checklist*—Refine the general outline by creating a detailed checklist of steps and an estimated amount of time for each step. This outline helps you stay on track during the investigation.
- *Determine the resources you need*—Based on the OS of the computer you're investigating, list the software you plan to use for the investigation, noting any other software, tools, or expert assistance you might need.
- *Obtain and copy an evidence drive*—In some cases, you might be seizing multiple computers along with CDs, DVDs, USB drives, mobile devices, and other removable media. (For the examples in this chapter, you're using only USB drives.) Make a forensic copy of the disk.
- *Identify the risks*—List the problems you normally expect in the type of case you're handling. This list is known as a standard risk assessment. For example, if the suspect seems knowledgeable about computers, he or she might have set up a logon scheme that shuts down the computer or overwrites data on the hard disk when someone tries to change the logon password.

- *Mitigate or minimize the risks*—Identify how you can minimize the risks. For example, if you're working with a computer on which the suspect has likely password-protected the hard drive, you can make multiple copies of the original media before starting. Then if you destroy a copy during the process of retrieving information from the disk, you have additional copies.
- *Test the design*—Review the decisions you've made and the steps you've completed. If you have already copied the original media, a standard part of testing the design involves comparing hash values (discussed in Chapters 3 and 4) to ensure that you copied the original media correctly.
- *Analyze and recover the digital evidence*—Using the software tools and other resources you've gathered, and making sure you've addressed any risks and obstacles, examine the disk to find digital evidence.
- *Investigate the data you recover*—View the information recovered from the disk, including existing files, deleted files, e-mail, and Web history, and organize the files to help find information relevant to the case.
- *Complete the case report*—Write a complete report detailing what you did and what you found.
- *Critique the case*—Self-evaluation and peer review are essential parts of professional growth. After you complete a case, review it to identify successful decisions and actions and determine how you could have improved your performance.

The amount of time and effort you put into each step varies, depending on the nature of the investigation. For example, in most cases, you need to create a simple investigation plan so that you don't overlook any steps. However, if a case involves many computers with complex issues to identify and examine, a detailed plan with periodic review and updates is essential. A systematic approach helps you discover the information you need for your case, and you should gather as much information as possible.

For all digital investigations, you must be prepared for the unexpected, so you should always have a contingency plan for the investigation. A contingency plan can consist of anything to help you complete the investigation, from alternative software and hardware tools to other methods of approaching the investigation.

Assessing the Case

As mentioned, identifying case requirements involves determining the type of case you're investigating. Doing so means you should outline the case details systematically, including the nature of the case, the type of evidence available, and the location of evidence.

In the company-policy violation case, you have been asked to investigate George Montgomery. Steve Billings had the IT Department confiscate George's storage media that might contain information about his whereabouts. After talking to George's co-workers, Steve learned that George has been conducting a personal business on the side using company computers. Therefore, the focus of the case has shifted to include possible employee abuse of company resources. You can begin assessing this case as follows:

- *Situation*—Employee abuse of resources.
- *Nature of the case*—Side business conducted on the company computer.
- *Specifics of the case*—The employee is reportedly conducting a side business on his company computer that involves registering domain names for clients and setting up their Web sites at local ISPs. Co-workers have complained that he's been spending too much time on his own business and not performing his assigned work duties. Company policy states that all company-owned digital assets are subject to inspection by company

management at any time. Employees have no expectation of privacy when operating company computer systems.

- *Type of evidence*—Small-capacity USB drive connected to a company computer.
- *Known disk format*—NTFS.
- *Location of evidence*—One USB drive recovered from the employee's assigned computer.

Based on these details, you can determine the case requirements. You now know that the nature of the case involves employee abuse of company resources, and you're looking for evidence that an employee was conducting a side business using his employer's computers. On the USB drive retrieved from George's computer, you're looking for any information related to Web sites, ISPs, or domain names. You know that the USB drive uses the NTFS file system. To duplicate the USB drive and find deleted and hidden files, you need a reliable digital forensics tool. Because the USB drive has already been retrieved, you don't need to seize the drive yourself. You call this case Montgomery_72018 (because the case opened on July 20, 2018) and determine that your task is to gather data from the storage media seized to confirm or deny the allegation that George is conducting a side business on company time and computers. Remember that he's suspected only of resource abuse, and the evidence you obtain might be exculpatory—meaning it could prove his innocence. You must always maintain an unbiased perspective and be objective in your fact-findings. If you are systematic and thorough, you're more likely to produce consistently reliable results.

Planning Your Investigation

Now that you have identified the requirements of the Montgomery_72018 case, you can plan your investigation. You have already determined the kind of evidence you need; now you can identify the specific steps to gather the evidence, establish a chain of custody, and perform the forensic analysis. These steps become the basic plan for your investigation and indicate what you should do and when. To investigate the Montgomery_72018 case, you should perform the following general steps. Most of these steps are explained in more detail in the following sections.

1. Acquire the USB drive from the IT Department, which bagged and tagged the evidence.
2. Complete an evidence form and establish a chain of custody.
3. Transport the evidence to your digital forensics lab.
4. Place the evidence in an **approved secure container** .
5. Prepare your forensic workstation.
6. Retrieve the evidence from the secure container.
7. Make a forensic copy of the evidence drive (in this case, the USB drive).
8. Return the evidence drive to the secure container.
9. Process the copied evidence drive with your digital forensics tools.

Tip

The approved secure container you need in **Step 4** should be a locked, fireproof locker or cabinet that has limited access. Limited access means that only you and other authorized personnel can open the secure container.

The first rule for all investigations is to preserve the evidence, which means it shouldn't be tampered with or contaminated. Because the IT Department staff confiscated the storage media, you need to go to them for the evidence. The IT Department manager confirms that the

storage media has been locked in a secure cabinet since it was retrieved from George's desk. Keep in mind that even though this case is a company policy matter, many cases are thrown out because the chain of custody can't be proved or has been broken. When this happens, there's the possibility that the evidence has been compromised.

To document the evidence, you record details about the media, including who recovered the evidence and when and who possessed it and when. Use an **evidence custody form** , also called a chain-of-evidence form, which helps you document what has and has not been done with the original evidence and forensic copies of the evidence. Depending on whether you're working in law enforcement or private security, you can create an evidence custody form to fit your environment. This form should be easy to read and use. It can contain information for one or several pieces of evidence. Consider creating a **single-evidence form** (which lists each piece of evidence on a separate page) and a **multi-evidence form** (see Figure 1-9), depending on the administrative needs of your investigation.

Figure 1-9.

Organization X
Security Investigations
This form is to be used for one to ten pieces of evidence

Case No.:		Investigating Organization:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

	Description of evidence:	Vendor Name	Model No./Serial No.
Item #1			
Item #2			
Item #3			
Item #4			
Item #5			
Item #6			
Item #7			
Item #8			
Item #9			
Item #10			

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Item #	Evidence Processed by	Disposition of Evidence	Date/Time
			Page __ of ___

A sample multi-evidence form used in a private-sector environment

If necessary, document how to use your evidence custody form. Clear instructions help users remain consistent when completing the form and ensure that everyone uses the same definitions for collected items. Standardization helps maintain consistent quality for all investigations and prevent confusion and mistakes about the evidence you collect. An evidence custody form usually contains the following information:

- *Case number*—The number your organization assigns when an investigation is initiated.
- *Investigating organization*—The name of your organization. In large corporations with global facilities, several organizations might be conducting investigations in different geographic areas.
- *Investigator*—The name of the investigator assigned to the case. If many investigators are assigned, specify the lead investigator's name.
- *Nature of case*—A short description of the case. For example, in the private-sector environment, it might be "data recovery for corporate litigation" or "employee policy violation case."
- *Location evidence was obtained*—The exact location where the evidence was collected. If you're using multi-evidence forms, a new form should be created for each location.

- *Description of evidence*—A list of the evidence items, such as "hard drive, 250 GB" or "one USB drive, 8 GB." On a multi-evidence form, write a description for each item of evidence you acquire and possibly include photos.
- *Vendor name*—The name of the manufacturer of the computer component. List a 250 GB hard drive, for example, as a "Maxtor 250 GB hard drive," or describe a USB drive as a "SanDisk 8 GB USB drive." In later chapters, you see how differences among manufacturers can affect data recovery.
- *Model number or serial number*—List the model number or serial number (if available) of the computer component. Many computer components, including hard drives, memory chips, and expansion slot cards, have model numbers but not serial numbers.
- *Evidence recovered by*—The name of the investigator who recovered the evidence. The chain of custody for evidence starts with this information. If you insert your name, for example, you're declaring that you have taken control of the evidence. It's now your responsibility to ensure that nothing damages the evidence and no one tampers with it. The person placing his or her name on this line is responsible for preserving, transporting, and securing the evidence.
- *Date and time*—The date and time the evidence was taken into custody. This information establishes exactly when the chain of custody starts.
- *Evidence placed in locker*—Specifies which approved secure container is used to store evidence and when the evidence was placed in the container.
- *Item #/Evidence processed by/Disposition of evidence/Date/Time*—When you or another authorized investigator retrieves evidence from the evidence locker for processing and analysis, list the item number and your name, and then describe what was done to the evidence.
- *Page*—The forms used to catalog all evidence for each location should have page numbers. List the page number, and indicate the total number of pages for this group of evidence. For example, if you collected 15 pieces of evidence at one location and your form has only 10 lines, you need to fill out two multi-evidence forms. The first form is noted as "Page 1 of 2," and the second page is noted as "Page 2 of 2."

Figure 1-10 shows a single-evidence form, which lists only one piece of evidence per page. This form gives you more flexibility in tracking separate pieces of evidence for your chain-of-custody log. It also has more space for descriptions, which is helpful when finalizing the investigation and creating a case report. With this form, you can accurately account for what was done to the evidence and what was found. Use evidence forms as a reference for all actions taken during your investigative analysis.

Figure 1-10.

Metropolis Police Bureau
High-tech Investigations Unit
This form is to be used for only one piece of evidence.
Fill out a separate form for each piece of evidence.

Case No.:		Unit Number:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

Item # ID	Description of evidence:	Vendor Name	Model No./Serial No.

Evidence Recovered by:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Evidence Processed by	Disposition of Evidence	Date/Time
		Page __ of ___

A single-evidence form

You can use both multi-evidence and single-evidence forms in your investigation. By using two forms, you can keep the single-evidence form with the evidence and the multi-evidence form in your report file. Two forms also provide redundancy that can be used as a quality control for evidence.

Securing Your Evidence

Digital investigations demand that you adjust your procedures to suit the case. For example, if the evidence for a case includes an entire computer system and associated storage media, such as flash drives and large external hard drives, you must be flexible when you account for all these items. Some evidence is small enough to fit into an evidence bag. Other items, such as CPU cabinets, monitors, keyboards, and printers, are too large.

To secure and catalog the evidence contained in large computer components, you can use large **evidence bags** , tape, tags, labels, and other products available from police supply vendors or office supply stores. When gathering products to secure your computer evidence, make sure they are safe and effective to use on computer components. Be cautious when handling any computer component to avoid damaging the component or coming into contact with static electricity, which can destroy digital data. For this reason, make sure you use antistatic bags when collecting computer evidence. Consider using an antistatic pad with an attached wrist strap, too. Both help prevent damage to computer evidence.

Note

This section focuses on securing computers and related hardware. Devices such as smartphones and cell phones are covered later in **Chapter 12**.

Be sure to place computer evidence in a well-padded container. Padding prevents damage to the evidence as you transport it to your secure evidence locker, evidence room, or computer lab. Save discarded hard drive boxes, antistatic bags, and packing material for computer hardware when you or others acquire computer devices.

Because you might not have everything needed to secure your evidence, you have to improvise. Securing evidence often requires building secure containers. If the computer component is large and contained in its own casing, you can use evidence tape to seal all

openings on the cabinet. Placing evidence tape over drive bays, insertion slots for power supply cords and USB cables, and any other openings ensures the security of evidence. As a standard practice, you should write your initials on the tape before applying it to the evidence. This practice makes it possible to prove later in court that the evidence hasn't been tampered with because the casing couldn't have been opened nor could power have been supplied to the closed casing with this tape in place. If the tape had been replaced, your initials wouldn't be present, which would indicate tampering. If you transport a computer, place new disks in disk drives to reduce possible drive damage while you're moving it.

Computer components require specific temperature and humidity ranges. If it's too cold, hot, or wet, computer components and magnetic media can be damaged. Even heated car seats can damage digital media, and placing a computer on top of a two-way car radio in the trunk can damage magnetic media. When collecting computer evidence, make sure you have a safe environment for transporting and storing it until a secure evidence container is available.

Procedures for Private-Sector High-Tech Investigations

As an investigator, you need to develop formal procedures and informal checklists to cover all issues important to high-tech investigations. These procedures are necessary to ensure that correct techniques are used in an investigation. Use informal checklists to be certain that all evidence is collected and processed correctly. This section lists some sample procedures that digital investigators commonly use in private-sector high-tech investigations.

Employee Termination Cases

Most investigative work for termination cases involves employee abuse of company resources. Incidents that create a hostile work environment, such as viewing pornography in the workplace and sending inappropriate e-mails, are the predominant types of cases investigated. The following sections describe key points for conducting an investigation that might lead to an employee's termination. Consulting with your organization's general counsel and Human Resources Department for specific directions on how to handle these investigations is recommended. Your organization must have appropriate policies in place, as described previously in this chapter.

Internet Abuse Investigations

The information in this section applies to an organization's internal private network, not a public ISP. Consult with your organization's general counsel after reviewing this list, and make changes according to their directions to build your own procedures. To conduct an investigation involving Internet abuse, you need the following:

- The organization's Internet proxy server logs
- Suspect computer's IP address obtained from your organization's network administrator
- Suspect computer's disk drive
- Your preferred digital forensics analysis tool

The following steps outline the recommended processing of an Internet abuse case:

1. Use the standard forensic analysis techniques and procedures described in this book for the disk drive examination.
2. Search for and extract all Web page URLs and other associated information.
3. Contact the network firewall administrator and request a proxy server log, if it's available, of the suspect computer's network device name or IP address for the dates of interest. Consult with your organization's network administrator to confirm that these logs

are maintained and how long the time to live (TTL) is set for the network's IP address assignments using Dynamic Host Configuration Protocol (DHCP).

4. Compare the data recovered from forensics analysis with the network server log data to confirm that they match.

5. If the URL data matches the network server log and the forensic disk examination, continue analyzing the suspect computer's drive data, and collect any relevant photos or Web pages that support the allegation. If there are no matches between the network server logs, and the forensic examination shows no contributing evidence, report that the allegation is unsubstantiated.

Before investigating an Internet abuse case, research your state or country's privacy laws. Many countries have unique privacy laws that restrict the use of computer log data, such as network server logs or disk drive cache files, for any type of investigation. Some state or federal laws might supersede your organization's employee policies. Always consult with your organization's attorney. For companies with international business operations, jurisdiction is a problem; what's legal in the United States, such as examining and investigating a network server log, might not be legal in Germany, for example.

For investigations in which the network server log doesn't match the forensics analysis that found inappropriate data, continue the examination of the suspect computer's disk drive. Determine when inappropriate data was downloaded to the computer and whether it was through an organization's intranet connection to the Internet. Employees might have used their employer's laptop computers to connect to their own ISPs to download inappropriate Web content. For these situations, you need to consult your organization's employee policy guidelines for what's considered appropriate use of the organization's digital resources.

E-mail Abuse Investigations

E-mail investigations typically include spam, inappropriate and offensive message content, and harassment or threats. E-mail is subject to the same restrictions as other computer evidence data, in that an organization must have a defined policy, as described previously. The following list is what you need for an investigation involving e-mail abuse:

- An electronic copy of the offending e-mail that contains message header data; consult with your e-mail server administrator
- If available, e-mail server log records; consult with your e-mail server administrator to see whether they are available
- For e-mail systems that store users' messages on a central server, access to the server; consult with your e-mail server administrator
- For e-mail systems that store users' messages on a computer as an Outlook .pst or .ost file, for example, access to the computer so that you can perform a forensic analysis on it
- Your preferred digital forensics analysis tool

The following steps outline the recommended procedure for e-mail investigations:

1. For computer-based e-mail data files, such as Outlook .pst or .ost files, use the standard forensics analysis techniques and procedures described in this book for the drive examination.

2. For server-based e-mail data files, contact the e-mail server administrator and obtain an electronic copy of the suspect's and victim's e-mail folder or data.

3. For Web-based e-mail (Gmail, for example) investigations, search for Internet keywords to extract all related e-mail address information.

Examine header data of all messages of interest to the investigation.

4. Attorney-Client Privilege Investigations

When conducting a digital forensics analysis under **attorney-client privilege (ACP)** rules for an attorney, you must keep all findings confidential. The attorney you're working for is the ultimate authority over the investigation. For investigations of this nature, attorneys typically request that you extract all data from drives. It's your responsibility to comply with the attorney's directions. Because of the large quantities of data a drive can contain, the attorney will want to know about everything of interest on the drives.

Many attorneys like to have printouts of the data you have recovered, but printouts can pose problems when you have log files with several thousand pages of data or CAD drawing programs that can be read only by proprietary programs. You need to persuade and educate many attorneys on how digital evidence can be viewed electronically. In addition, learn how to teach attorneys and paralegals to sort through files so that you can help them efficiently analyze the huge amount of data a forensic examination produces.

You can also encounter problems if you find data in the form of binary files, such as CAD drawings. Examining these files requires using the CAD program that created them. In addition, engineering companies often have specialized drafting programs. Discovery demands for lawsuits involving a product that caused injury or death requires extracting design plans for attorneys and expert witnesses to review. You're responsible for locating the programs for these design plans so that attorneys and expert witnesses can view the evidence files.

The following list shows the basic steps for conducting an ACP case:

1. Request a memo from the attorney directing you to start the investigation. The memorandum must state that the investigation is privileged communication and list your name and any other associates' names assigned to the case.
2. Request a list of keywords of interest to the investigation.
3. After you have received the memorandum, initiate the investigation and analysis. Any findings you made before receiving the memorandum are subject to discovery by the opposing attorney.
4. For drive examinations, make two bit-stream images (discussed later in this chapter) of the drive, using a different tool for each image. This approach is advisable because every tool has its strengths and weaknesses. If you have large enough storage drives, make each bit-stream image uncompressed (refer to **Chapter 3**) so that if it becomes corrupt, you can still examine uncorrupted areas with your preferred forensics analysis tool.
5. Verify the hash values on all files on the original and re-created disks or its image file.
6. Methodically examine every portion of the drive (both allocated and unallocated data areas) and extract all data.
7. Run keyword searches on allocated and unallocated disk space. Follow up the searches to determine whether the results contain information that supports the case.
8. For Windows OSs, use specialty tools to analyze and extract data from the Registry, such as AccessData Registry Viewer or a Registry viewer program (discussed in more detail in **Chapter 5**). Use the Edit, Find menu option in Registry Editor, for example, to search for keywords of interest to the investigation.
9. For binary files, such as CAD drawings, find the correct program and, if possible, make printouts of the binary file content. If the files are too large, load the specialty program on a separate workstation with the recovered binary files so that the attorney can view them.
10. For unallocated data recovery, use a tool that removes or replaces nonprintable data.

11. Consolidate all recovered data from the evidence bit-stream image into well-organized folders and subfolders. Store the recovered data output, using a logical and easy-to-follow storage method for the attorney or paralegal.

Here are some other guidelines to remember for ACP cases:

- Minimize all written communication with the attorney; use the telephone when you need to ask questions or provide information related to the case.
- Any documentation written to the attorney must contain a header stating that it's "Privileged Legal Communication—Confidential Work Product," as defined under the attorney-work-product rule.
- Assist the attorney and paralegal in analyzing the data.

If you have difficulty complying with the directions or don't understand the directives in the memo, contact the attorney and explain the problem. Always keep an open line of verbal communication with the attorney during these types of investigations. If you're communicating via e-mail, use encryption or another secure e-mail service for all messages.

Industrial Espionage Investigations

Industrial espionage cases can be time consuming and are subject to scope creep problems (meaning the investigation's focus widens and becomes more time consuming). This section offers some guidelines on how to deal with industrial espionage investigations. Be aware that cases dealing with foreign nationals might be violations of International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR). For more information on ITAR, see the U.S. Department of State's Web site (www.state.gov; substitute the actual state name or a shortened version for state) or do an Internet search for "International Traffic in Arms Regulations." For EAR information, see the U.S. Department of Commerce Web site (www.doc.gov) or do an Internet search for "Export Administration Regulations."

Unlike the other private-sector investigations covered in this section, all suspected industrial espionage cases should be treated as criminal investigations. The techniques described here are for private network environments and internal investigations that haven't yet been reported to law enforcement officials. Make sure you don't become an agent of law enforcement by filing a complaint of a suspected espionage case before substantiating the allegation. The following list includes staff you might need when planning an industrial espionage investigation. This list isn't exhaustive, so use your knowledge to improve on these recommendations:

- The digital investigator who's responsible for disk forensic examinations
- The technology specialist who is knowledgeable about the suspected compromised technical data
- The network specialist who can perform log analysis and set up network monitors to trap network communication of possible suspects
- The threat assessment specialist (typically an attorney) who's familiar with federal and state laws and regulations related to ITAR or EAR and industrial espionage

Tip

The International Competition Network has established guidelines (available at www.internationalcompetitionnetwork.org/uploads/library/doc627.pdf) for digital evidence gathering in private-sector settings; they're used by more than 90 jurisdictions.

In addition, consider the following guidelines when initiating an international espionage investigation:

- Determine whether this investigation involves a possible industrial espionage incident, and then determine whether it falls under ITAR or EAR.
- Consult with corporate attorneys and upper management if the investigations must be conducted discreetly.
- Determine what information is needed to substantiate the allegation of industrial espionage.
- Generate a list of keywords for disk forensics and network monitoring.
- List and collect resources needed for the investigation.
- Determine the goal and scope of the investigation; consult with management and the company's attorneys on how much work you should do.
- Initiate the investigation after approval from management, and make regular reports of your activities and findings.

The following are planning considerations for industrial espionage investigations:

- Examine all e-mail of suspected employees, both company-provided e-mail and free Web-based services.
- Search Internet forums or blogs for any postings related to the incident.
- Initiate physical surveillance with cameras on people or things of interest to the investigation.
- If available, examine all facility physical access logs for sensitive areas, which might include secure areas where smart badges or video surveillance recordings are used.
- If there's a suspect, determine his or her location in relation to the vulnerable resource that was compromised.
- Study the suspect's work habits.
- Collect all incoming and outgoing phone logs to see whether any unique or unusual places were called.

When conducting an industrial espionage case, follow these basic steps:

1. Gather all personnel assigned to the investigation and brief them on the plan and any concerns.
2. Gather the resources needed to conduct the investigation.
3. Start the investigation by placing surveillance systems, such as cameras and network monitors, at key locations.
4. Discreetly gather any additional evidence, such as the suspect's computer drive, and make a bit-stream image for follow-up examination.
5. Collect all log data from networks and e-mail servers, and examine them for unique items that might relate to the investigation.
6. Report regularly to management and corporate attorneys on your investigation's status and current findings.
7. Review the investigation's scope with management and corporate attorneys to determine whether it needs to be expanded and more resources added.

Interviews and Interrogations in High-Tech Investigations

Becoming a skilled interviewer and interrogator can take many years of experience. Typically, a private-sector digital investigator is a technical person acquiring the evidence for an investigation. Many large organizations have full-time security investigators with years of training and experience in criminal and civil investigations and interviewing techniques. Few of these investigators have any computing or network technical skills, so you might be asked to assist in interviewing or interrogating a suspect when you have performed a forensic disk analysis on that suspect's machine.

An interrogation is different from an interview. An **interview** is usually conducted to collect information from a witness or suspect about specific facts related to an investigation. An **interrogation** is the process of trying to get a suspect to confess to a specific incident or crime. An investigator might change from an interview to an interrogation when talking to a witness or suspect. The more experience and training investigators have in the art of interviewing and interrogating, the more easily they can determine whether a witness is credible and possibly a suspect.

Your role as a digital investigator is to instruct the investigator conducting the interview on what questions to ask and what the answers should be. As you build rapport with the investigator, he or she might ask you to question the suspect. Watching a skilled interrogator is a learning experience in human relations skills. If you're asked to assist in an interview or interrogation, prepare yourself by answering the following questions:

- What questions do I need to ask the suspect to get the vital information about the case?
- Do I know what I'm talking about, or will I have to research the topic or technology related to the investigation?
- Do I need additional questions to cover other indirect issues related to the investigation?

Common interview and interrogation errors include being unprepared for the interview or interrogation and not having the right questions or enough questions to increase your depth of knowledge. Make sure you don't run out of conversation topics; you need to keep the conversation friendly to gain the suspect's confidence. Avoid doubting your own skills, which might show the suspect you lack confidence in your ability. The ingredients for a successful interview or interrogation include the following:

- Being patient throughout the session
- Repeating or rephrasing questions to zero in on specific facts from a reluctant witness or suspect
- Being tenacious

Understanding Data Recovery Workstations and Software

Now you know what's involved in acquiring and documenting evidence. In **Chapter 2**, you examine a complete setup of a digital forensics lab, which is where you conduct your investigations and where most of your equipment and software are located, including secure evidence containers. Be aware that some companies that perform digital investigations also do data recovery, e-discovery, and other related investigations.

Remember the difference between data recovery and digital forensics. In data recovery, typically, the customer or your company just wants the data back. The other key difference is that in data recovery, you usually know what you're trying to retrieve. In digital forensics, you might have an idea of what you're searching for, but not necessarily.

To conduct your investigation and analysis, you must have a specially configured PC known as a **forensic workstation** , which is a computer loaded with additional bays and forensics

software. Depending on your needs, a forensic workstation can use the following operating systems:

- MS-DOS 6.22
- Windows 95, 98, or Me
- Windows NT 3.5 or 4.0
- Windows 2000, XP, Vista, 7, 8, or 10
- Linux
- Mac OS X and macOS

Tip

Chapters 2 and 6 cover the software resources you need and the forensics lab and workstation in detail. Visit www.digitalintelligence.com to examine the specifications of the Forensic Recovery of Evidence Device (F.R.E.D.) unit or www.forensiccomputers.com to look at current products.

If you start any operating system while you're examining a hard disk, the OS alters the evidence disk by writing data to the Recycle Bin and corrupts the quality and integrity of the evidence you're trying to preserve. **Chapter 5** covers which files Windows updates automatically at startup. Newer Windows OSs also record the serial numbers of hard drives and CPUs in a file, which can be difficult to recover.

Of all the Microsoft OSs, the least intrusive (in terms of changing data) to disks is MS-DOS 6.22. With the continued evolution of Microsoft OSs, it's not always practical to use older MS-DOS platforms, however. Many older digital forensics acquisition tools work in the MS-DOS environment. These tools can operate from an MS-DOS window in Windows 98 or from the command prompt in Windows 2000 and later. Some of their functions are disabled or generate error messages when run in these OSs, however.

Newer file system formats, such as NTFS, are accessible—that is, readable—only from Windows NT and later or any Linux OS. You can use one of several write-blockers that enable you to boot to Windows without writing data to the evidence drive. In Chapter 3, you learn more about write-blockers and some inexpensive alternatives for preserving data during an acquisition.

Many hardware write-blockers that connect to USB or FireWire ports are on the market. Several vendors sell write-blockers, including Digital Intelligence Ultra-Kit, UltraBlock, FireFly, FireChief 800, and USB Write Blocker; WiebeTECH Forensic DriveDock; Guidance Software FastBloc; Paralan's SCSI Write Blockers; Tableu UltraBlock SAS Write Blocker; and Intelligent Computer Solutions (www.ics-iq.com) Image LinkMASSter Forensics Hard Case.

Software write-blockers are available, too. Typically, these write-blockers require a bootable DVD or USB drive that runs an independent OS in a suspect computer's RAM. For more information on software write-blockers, see http://forensicsoft.com. Windows products are being developed that make performing disk forensics easier. However, because Windows has limitations in performing disk forensics, you need to develop skills in acquiring data with Linux. In later chapters, you learn more about using these other tools. Keep in mind that no single digital forensics tool can recover everything. Each tool and OS has its own strengths and weaknesses, so develop skills with as many tools as possible to become an effective digital investigator. Appendix D has additional information on how to use MS-DOS for data acquisitions.

Setting Up Your Workstation for Digital Forensics

With current digital forensics hardware and software, configuring a computer workstation or laptop as a forensic workstation is simple. All that's required are the following:

- A workstation running Windows 7 or later
- A write-blocker device
- Digital forensics acquisition tool
- Digital forensics analysis tool
- A target drive to receive the source or suspect disk data
- Spare PATA and SATA ports
- USB ports

Additional useful items include the following:

- Network interface card (NIC)
- Extra USB ports
- FireWire 400/800 ports
- SCSI card
- Disk editor tool
- Text editor tool
- Graphics viewer program
- Other specialized viewing tools

In **Chapter 2**, you learn more about setting up and configuring a computer to be a forensic workstation.

Conducting an Investigation

Now you're ready to return to the Montgomery_72018 case. You have created a plan for the investigation, set up your forensic workstation, and installed the necessary forensics analysis software you need to examine the evidence. The type of software to install includes your preferred analysis tool, such as OSForensics, Forensic Explorer, EnCase, FTK, or X-Ways Forensics; an office suite, such as LibreOffice; and a graphics viewer, such as IrfanView. To begin conducting an investigation, you start by copying the evidence, using a variety of methods. No single method retrieves all data from a disk, so using several tools to retrieve and analyze data is a good idea. Start by gathering the resources you identified in your investigation plan. You need the following items:

- Original storage media
- Evidence custody form
- Evidence container for the storage media, such as an evidence bag
- Bit-stream imaging tool; in this case, FTK Imager Lite
- Forensic workstation to copy and examine the evidence
- Secure evidence locker, cabinet, or safe

Gathering the Evidence

Now you're ready to gather evidence for the Montgomery_72018 case. Remember that you need antistatic bags and pads with wrist straps to prevent static electricity from damaging

digital evidence. To acquire George Montgomery's storage media from the IT Department and then secure the evidence, you perform the following steps:

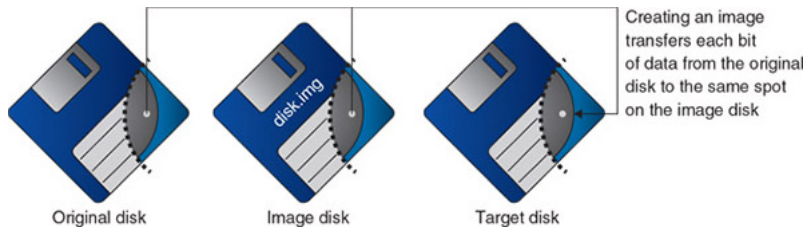
1. Arrange to meet the IT manager to interview him and pick up the storage media.
2. After interviewing the IT manager, fill out the evidence form, have him sign it, and then sign it yourself.
3. Store the storage media in an evidence bag, and then transport it to your forensic facility.
4. Carry the evidence to a secure container, such as a locker, cabinet, or safe.
5. Complete the evidence custody form. As mentioned, if you're using a multi-evidence form, you can store the form in the file folder for the case. If you're also using single-evidence forms, store them in the secure container with the evidence. Reduce the risk of tampering by limiting access to the forms.
6. Secure the evidence by locking the container.

Understanding Bit-stream Copies

A **bit-stream copy** is a bit-by-bit copy (also known as a "forensic copy") of the original drive or storage medium and is an exact duplicate. The more exact the copy, the better chance you have of retrieving the evidence you need from the disk. This process is usually referred to as "acquiring an image" or "making an image" of a suspect drive. A bit-stream copy is different from a simple backup copy of a disk. Backup software can copy or compress only files that are stored in a folder or are of a known file type. Backup software can't copy deleted files and e-mails or recover file fragments.

A **bit-stream image** is the file containing the bit-stream copy of all data on a disk or disk partition. For simplicity, it's usually referred to as an "image," "image save," or "image file." To create an exact image of an evidence disk, copying the image to a target disk that's identical to the evidence disk is preferable (Figure 1-11). The target disk's manufacturer and model, in general, should be the same as the original disk's manufacturer and model. If the target disk is identical to the original, the size in bytes and sectors of both disks should also be the same. Some image acquisition tools can accommodate a target disk that's a different size than the original. These imaging tools are discussed in Chapter 3. Older digital forensics tools designed for MS-DOS work only on a copied disk. Current GUI tools can work on both a disk drive and copied data sets that many manufacturers refer to as "image saves."

Figure 1-11.



Transfer of data from original to image to target

Tip

Occasionally, the track and sector maps on the original and target disks don't match, even if you use disks of exactly the same size that are different makes or models. Tools such as Guidance EnCase and NTI SafeBack adjust for the target drive's geometry. One other tool, X-Ways WinHex Specialist Edition, can copy sector by sector to equal-size or larger disks without needing to force changes in the target disk's geometry.

Acquiring an Image of Evidence Media

After you retrieve and secure the evidence, you're ready to copy the evidence media and analyze the data. The first rule of digital forensics is to preserve the original evidence. Then conduct your analysis only on a copy of the data—the image of the original medium. Several vendors offer Windows and Linux acquisition tools. These tools, however, require a write-blocking device (discussed in Chapter 3) when acquiring data from disks and USB drives; you also learn about acquiring forensic images in this chapter.

Analyzing Your Digital Evidence

When you analyze digital evidence, your job is to recover the data. If users have deleted or overwritten files on a disk, the disk contains deleted files and file fragments in addition to existing files. Remember that as files are deleted, the space they occupied becomes free space—meaning it can be used for new files that are saved or files that expand as data is added to them. The files that were deleted are still on the disk until a new file is saved to the same physical location, overwriting the original file. In the meantime, those files can still be retrieved. Forensics tools such as Autopsy can retrieve deleted files for use as evidence.

Note

Before doing the next activity, you need to download Autopsy for Windows, a free forensics tool from Sleuth Kit. The version used throughout this book is 4.3.0. Download Autopsy from https://sourceforge.net/projects/autopsy/files/autopsy/4.3.0/, and then install it. For detailed information on using Autopsy, see http://sleuthkit.org/autopsy/docs/user-docs/4.3/. For an explanation of the user interface, see http://sleuthkit.org/autopsy/docs/user-docs/4.3/uilayout_page.html.

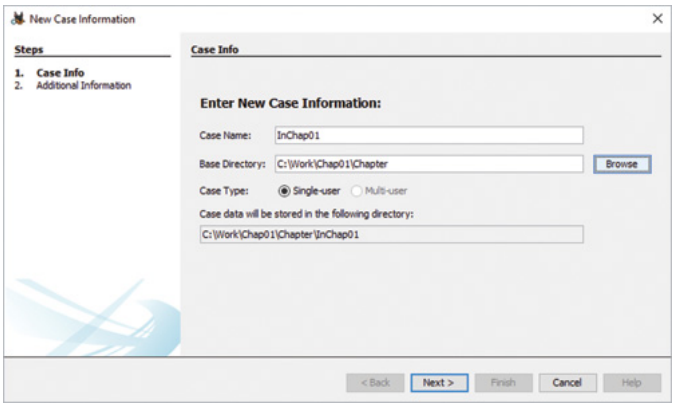
In the following steps, you analyze George Montgomery's USB drive. The first task is to configure Autopsy for a new case and analyze the image file of George Montgomery's USB drive. To perform the analysis, follow these steps:

Note

Before beginning this activity, create a C:\Work\Chap01\Chapter folder (referred to as your "work folder" in steps). Download to this work folder the Ch01InChap01.exe file from this chapter's downloads section on the student companion site for this book.

1. Double-click the **Ch01InChap01.exe** file in File Explorer to uncompress it into InChap01.dd. Start Autopsy for Windows.
2. In Autopsy's main window, click the **Create New Case** button. In the New Case Information window, enter **InChap01** in the Case Name text box (see Figure 1-12), and click **Browse** next to the Base Directory text box. Navigate to and click your work folder. Make sure the **Single-user** option button is selected for Case Type, and then click **Next**.

Figure 1-12.

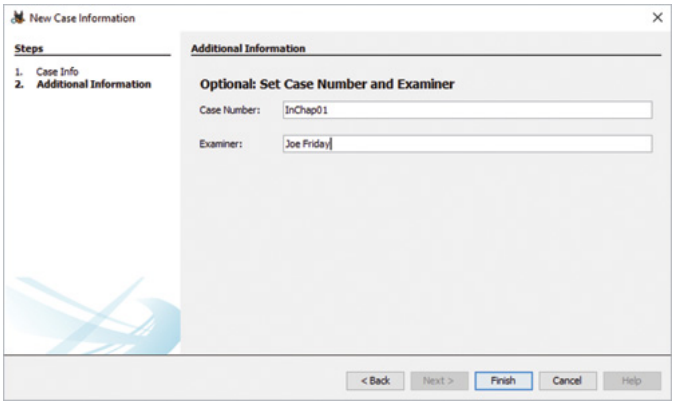


Source: www.sleuthkit.org

The New Case Information window

3. In the Additional Information window, type **InChap01** in the Case Number text box and your name in the Examiner text box (see Figure 1-13), and then click **Finish** to start the Add Data Source Wizard.

Figure 1-13.

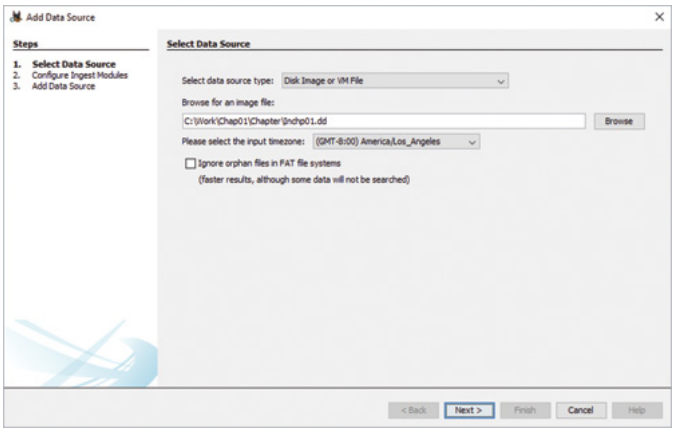


Source: www.sleuthkit.org

Adding more information for the case

4. In the Select Data Source window (see **Figure 1-14**), click the **Select data source type** list arrow, and click **Disk Image or VM file**. Click the **Browse** button next to the "Browse for an image file" text box, navigate to and click your work folder and the **Ch01InChap01.dd** file, and then click **Open**. Click **Next**.

Figure 1-14.



Source: www.sleuthkit.org

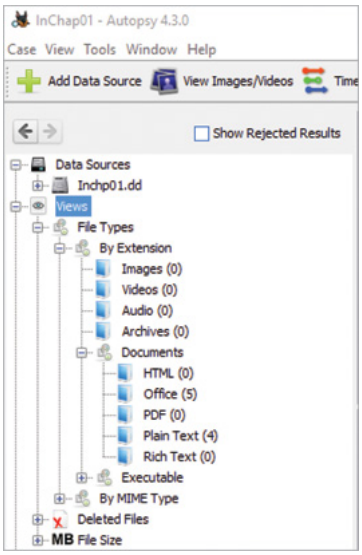
The Select Data Source window

5. Keep the default settings in the Configure Ingest Modules window. Click **Next** and then **Finish**.

Next, follow these steps to display the contents of the acquired data:

1. In the Tree Viewer pane on the left, click to expand **Views**, **File Types**, **By Extension**, and **Documents** (see Figure 1-15).

Figure 1-15.



Source: www.sleuthkit.org

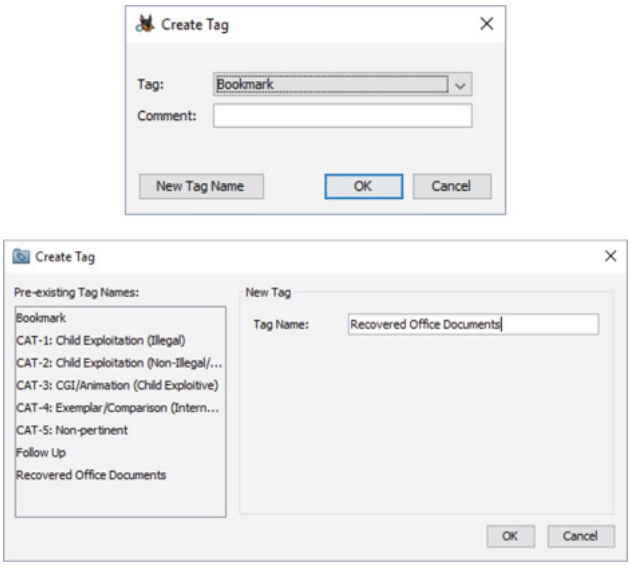
Autopsy's Tree Viewer pane

2. Under Documents, click **Office**. In the Result Viewer (upper-right pane), click the first file, **Billing Letter.doc** , to display its contents in the Content Viewer (lower-right pane).

3. Right-click **Billing Letter.doc** , point to **Tag File**, and click **Tag and Comment**.

4. In the Create Tag dialog box, click the **New Tag Name** button shown in Figure 1-16. In the New Tag section, type **Recovered Office Documents** in the Tag Name text box, click **OK**, and then click **OK** again.

Figure 1-16.

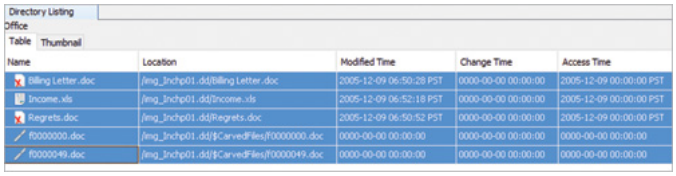


Source: www.sleuthkit.org

The Create Tag dialog boxes

5. In the Result Viewer pane, Ctrl+click **Billing Letter.doc** , **Income.xls** , **Regrets.doc** , **f0000000.doc** , and **f0000049.doc** to select these files, and then release the Ctrl key. Right-click the highlighted files shown in Figure 1-17, point to **Tag File** and then **Quick Tag**, and then click **Recovered Office Documents**.

Figure 1-17.



Source: www.sleuthkit.org

Selecting multiple files for tagging

6. Under Documents in the Tree Viewer pane, click **Plain Text** to display more recovered files.

7. In the Result Viewer pane, select the files listed in **Step 5** again, right-click the selection, point to **Tag File** and then **Quick Tag**, and then click **Follow Up**. Leave Autopsy running for the next activity.

The next step is analyzing the data and searching for information related to the complaint. Data analysis can be the most time-consuming task, even when you know exactly what to look for in the evidence. The method for locating evidentiary artifacts is to search for specific known data values. Data values can be unique words or nonprintable characters, such as hexadecimal codes. There are also printable character codes that can't be generated from a keyboard, such as the copyright (©) or registered trademark (™) symbols. Many digital forensics programs can search for character strings (letters and numbers) and hexadecimal values, such as 0xA9 for the copyright symbol or 0xAE for the registered trademark symbol. All these searchable data values are referred to as "keywords."

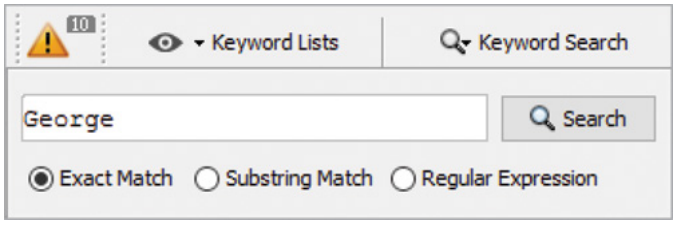
Note

Hexadecimal values are typically preceded with a zero and the letter x to clearly identify what they represent.

With Autopsy, you can search for keywords of interest in the case. For this case, you need to find any files associated with George Montgomery. Follow these steps to search for any reference to the name "George":

1. Click the **Keyword Search** button at the far upper right, type **George** in the text box (see Figure 1-18), and then click **Search**.

Figure 1-18.

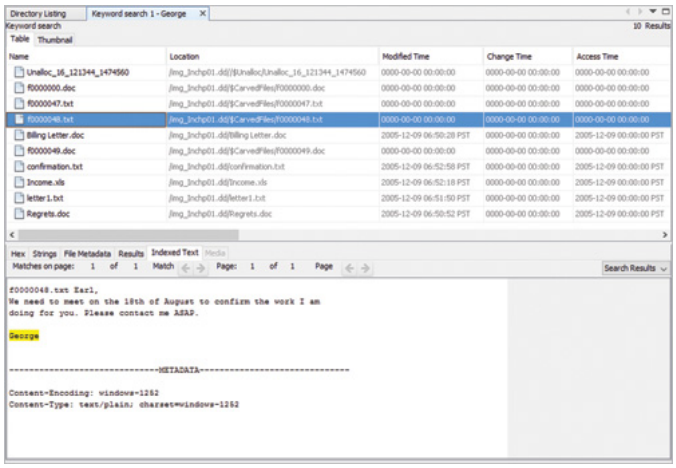


Source: www.sleuthkit.org

Entering a keyword search term

2. In the Result Viewer pane, a new tab named Keyword search 1 opens. Click each file to view its contents in the Content Viewer (see **Figure 1-19**). Look for files containing the name "George."

Figure 1-19.



Source: www.sleuthkit.org

Viewing the results of searching for the keyword "George"

3. Click the **Keyword Lists** button at the far upper right, click the **Email Addresses** check box, and then click **Search**.

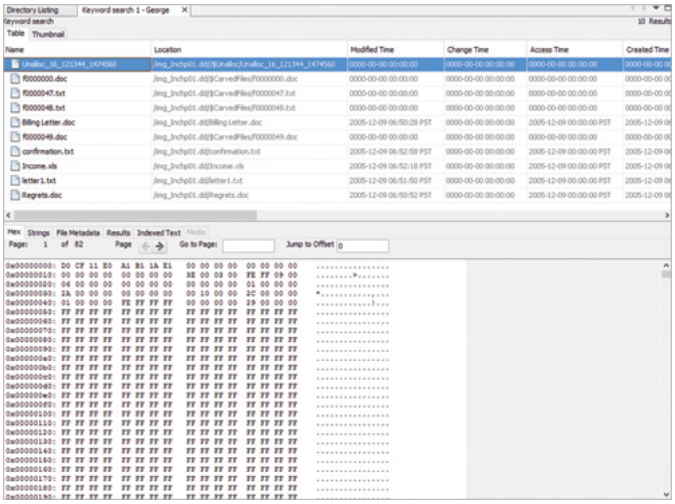
4. In the Result Viewer pane, a new tab named Keyword search 2 opens. Click each file to view its contents in the Content Viewer pane and examine all e-mail addresses found in the search. Leave Autopsy running so that you can learn about more of its features in the next section.

Some Additional Features of Autopsy

If you find a file of interest that displays binary (nonprintable) data in the Content Viewer, there are six available viewing options in Autopsy: Hex, Strings, File Metadata, Results, Indexed

Text, and Media. To view an unallocated sector for its hexadecimal values, click the Hex tab in the Content Viewer, as shown in **Figure 1-20**.

Figure 1-20.



Source: www.sleuthkit.org

Viewing search results found in unallocated drive space

If you want to examine an Office file, such as an Excel spreadsheet, right-click the file and click Open in External Viewer. To use this option, you must have the external viewer's software installed on your computer. To export a file from Autopsy, select it, and then right-click the file and click Extract File. In the Save dialog box that opens, you can copy the file to a work folder.

In the next section, you learn how to complete the case. In later chapters, you learn how to apply more search and analysis techniques.

Completing the Case

After analyzing the disk, you can retrieve deleted files, e-mail, and items that have been purposefully hidden, which you do in **Chapters 8**, 9, and 11. The files on George's USB drive indicate that he was conducting a side business on his company computer. Now that you have retrieved and analyzed the evidence, you need to find the answers to the following questions to write the final report:

- How did George's manager acquire the disk?
- Did George perform the work on a laptop, which is his own property? If so, did he conduct business transactions on his break or during his lunch hour?
- At what times of the day was George using the non-work-related files? How did you retrieve this information?
- Which company policies apply?
- Are there any other items that need to be considered?

When you write your report, state what you did and what you found. The report you generate with a forensics tool gives an account of the steps you took. As part of your final report, depending on guidance from management or legal counsel, include this report file to document your work. In any digital investigation, you should be able to repeat the steps you took and produce the same results. This capability is referred to as **repeatable findings** ; without it, your work product has no value as evidence.

In addition to writing a report, keep a written journal of everything you do. Your notes can be used in court, so be mindful of what you write or e-mail, even to a fellow investigator. Often these journals start out as handwritten notes, but you can transcribe them to electronic format periodically.

Basic report writing involves answering the six Ws: who, what, when, where, why, and how. In addition to these basic facts, you must also explain computer and network processes. Typically, your reader is a senior personnel manager, a lawyer, or occasionally a judge who might have little computer knowledge. Identify your reader and write the report for that person. Provide explanations for processes and how systems and their components work.

Your organization might have templates to use when writing reports. Depending on your organization's needs and requirements, your report must describe the findings from your analysis. The reports generated by forensics tools generally list your examination and data recovery findings. Some digital forensics tools also generate a log file of all actions taken during your examination and analysis. Integrating a log file from these other tools can enhance your final report. When describing the findings, consider writing your narrative first and then placing the log file at the end of the report, with references to it in the main narrative. **Chapter 14** covers writing final reports for investigations in more detail.

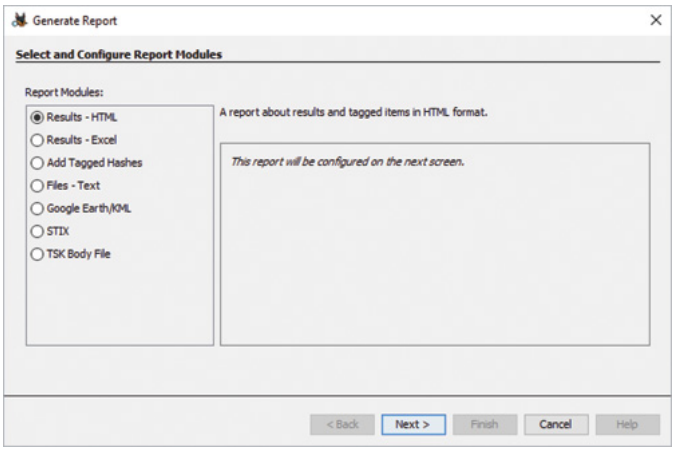
In the Montgomery_72018 case, you want to show what evidence exists proving that George had his own business registering domain names. You should include a list of his clients' names, his income from this business, and any correspondence he wrote to clients about their accounts. The time and date stamps on the files are during work hours, so you should include this information, too. Eventually, you hand the evidence file to your supervisor or to Steve, George's manager, who then decides on a course of action.

Autopsy's Report Generator

Autopsy has several styles of reports, including a plain text file, an HTML Web page with links to artifacts, and an Excel spreadsheet. To generate a report, you can follow this general procedure:

1. If you exited Autopsy, start it again, and click **Open Recent Case**. Click **InChap01** and then click **Open** in the Recent Case window. In Autopsy's main window, click the **Generate Report** button at the top.
2. In the Generate Report window, select the report format you want in the Report Modules section (see **Figure 1-21**). The Results - HTML option, for example, produces a linkable Web page with tagged artifacts, and the Files - Text option creates a plain text output file. When you're finished, click **Next**.

Figure 1-21.



Source: www.sleuthkit.org

The Generate Report window

3. If you select Results - HTML, the Configure Artifacts Report window opens, where you can select what data to add to the report. After you make your selections, click **Finish** to generate the report.

4. After the report is generated, Autopsy displays the Report Generation Progress window. Click the link to open the report, and then click **Close** after you've reviewed it.

Critiquing the Case

After you close the case and make your final report, you need to meet with your department or a group of fellow investigators and critique the case in an effort to improve your work. Ask yourself assessment questions such as the following:

- How could you improve your performance in the case?
- Did you expect the results you found? Did the case develop in ways you did not expect?
- Was the documentation as thorough as it could have been?
- What feedback has been received from the requesting source?
- Did you discover any new problems? If so, what are they?
- Did you use new techniques during the case or during research?

Make notes to yourself in your journal about techniques or processes that might need to be changed or addressed in future investigations. Then store your journal in a secure place.

Chapter Summary

- Digital forensics applies forensics procedures to digital evidence. This process involves systematically accumulating and analyzing digital information for use as evidence in civil, criminal, and administrative cases. Digital forensics differs from network forensics and data recovery in scope, technique, and objective.
- Laws relating to digital evidence were established in the 1970s.
- To be a successful digital forensics investigator, you must be familiar with more than one computing platform. To supplement your knowledge, develop and maintain contact with computer, network, and investigative professionals.
- Investigators need specialized workstations to examine digital evidence, including additional bays for evidence drives, forensics software, and write blockers.
- Public-sector and private-sector investigations differ, in that public-sector investigations typically require a search warrant before seizing digital evidence. The Fourth Amendment to the U.S. Constitution and similar legislation in other countries apply to government search and seizure. During public-sector investigations, you search for evidence to support criminal allegations. During private-sector investigations, you search for evidence to support allegations of policy violations, abuse of assets, and, in some cases, criminal complaints.
- Warning banners should be used to remind employees and visitors of company policy on computer, e-mail, and Internet use.
- Companies should define and limit the number of authorized requesters who can start an investigation.
- Digital forensics investigators must maintain professional conduct to protect their credibility.
- Always use a systematic approach to your investigations. Follow the checklist in this chapter as a guideline for your case.
- When planning a case, take into account the nature of the case, instructions from the requester, what additional tools and expertise you might need, and how you will acquire the evidence.
- Criminal cases and company-policy violations should be handled in much the same manner to ensure that quality evidence is presented. Both criminal cases and company-policy violations can go to court.
- When you begin a case, there might be unanticipated challenges that weren't obvious when applying a systematic approach to your investigation plan. For all investigations, you need to plan for contingencies for any unexpected problems you might encounter.
- You should create a standard evidence custody form to track the chain of custody of evidence for your case. There are two types of forms: a multi-evidence form and a single-evidence form.
- Internet abuse investigations require examining server log data.
- For attorney-client privilege cases, all written communication should have a header label stating that it's privileged communication and a confidential work product.
- A bit-stream copy is a bit-by-bit duplicate of the original disk. You should use the duplicate, whenever possible, when analyzing evidence.
- Always maintain a journal to keep notes on exactly what you did when handling evidence.

- You should always critique your own work to determine what improvements you made during each case, what could have been done differently, and how to apply those lessons to future cases.

Key Terms

affidavit
allegation
approved secure container
attorney-client privilege (ACP)
authorized requester
bit-stream copy
bit-stream image
chain of custody
Computer Technology Investigators Network (CTIN)
data recovery
Digital Evidence First Responder (DEFR)
Digital Evidence Specialist (DES)
digital forensics
digital investigations
evidence bags
evidence custody form
exculpatory evidence
exhibits
forensic workstation
Fourth Amendment
hostile work environment
inculpatory evidence
industrial espionage
International Association of Computer Investigative Specialists (IACIS)
interrogation
interview
line of authority
multi-evidence form
network intrusion detection and incident response
professional conduct
repeatable findings
search and seizure
search warrants
single-evidence form
verdict
vulnerability/threat assessment and risk management
warning banner
white-collar crimes

Review Questions

1. Digital forensics and data recovery refer to the activities. True or False?
2. Police in the United States must use procedures that adhere to which of the following?
    a. Third Amendment
    b. Fourth Amendment
    c. First Amendment
    d. None of the above
3. The triad of computing security includes which of the following?
    a. Detection, response, and monitoring
    b. Vulnerability assessment, detection, and monitoring
    c. Vulnerability/threat assessment and risk management, network intrusion detection and incident response, and digital investigation
    d. Vulnerability assessment, intrusion response, and monitoring
4. What's the purpose of maintaining a network of digital forensics specialists?
5. Policies can address rules for which of the following?
    a. When you can log on to a company network from home
    b. The Internet sites you can or can't access
    c. The amount of personal e-mail you can send
    d. Any of the above
6. List two items that should appear on a warning banner.
7. Under normal circumstances, a private-sector investigator is considered an agent of law enforcement. True or False?
8. List two types of digital investigations typically conducted in a business environment.
9. What is professional conduct, and why is it important?
10. What's the purpose of an affidavit?
11. What are the necessary components of a search warrant?
12. What are some ways to determine the resources needed for an investigation?
13. List three items that should be on an evidence custody form.
14. Why should you do a standard risk assessment to prepare for an investigation?
15. You should always prove the allegations made by the person who hired you. True or False?
16. For digital evidence, an evidence bag is typically made of antistatic material. True or False?
17. Why should evidence media be write-protected?
18. List three items that should be in your case report.
19. Why should you critique your case after it's finished?
20. What do you call a list of people who have had physical possession of the evidence?
21. Data collected before an attorney issues a memo for an attorney-client privilege case is protected under the confidential work product rule. True or False?

Hands-On Projects

Create a Chap01\Projects folder under your work folder. Then download the Ch01ProjDataFiles.exe file from the downloads section for this chapter (on the student companion site for this book) to this work subfolder. Double-click this file in File Explorer to uncompress its contents.

Hands-On Project 1-1.

The case in this project involves a suspicious death. Joshua Zarkan found his girlfriend's dead body in her apartment and reported it. The first responding law enforcement officer seized a USB drive. A crime scene evidence technician skilled in data acquisition made an image of the USB drive with FTK Imager and named it C1Prj01.E01. Following the acquisition, the technician transported and secured the USB drive and placed it in a secure evidence locker at the police station. You have received the image file from the detective assigned to this case. He directs you to examine it and identify any evidentiary artifacts that might relate to this case. To process this case, follow these steps to evaluate what's on the image of the USB drive:

1. Start Autopsy for Windows, and click the **Create New Case** icon. In the New Case Information window, enter **C1Prj01** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**.
2. In the Additional Information window, type **C1Prj01** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.
3. In the Select Data Source window, click the **Select data source type** list arrow, and click **Disk Image or VM file**. Click the **Browse** button next to the "Browse for an image file" text box, navigate to and click your work folder and the **C1Prj01.E01** file, and then click **Open**. Click **Next**.
4. In the Configure Ingest Modules window, click **Select All**. Click **Next** and then **Finish**.
5. In the Tree Viewer pane, expand **Views**, **File Types**, **By Extension**, and **Documents**.
6. Examine each subfolder under Documents. Determine which folder might contain files of interest to this case.
7. If you found any files related to the case, select the files as a group, right-click the selection, and click **Extract File(s)**. In the Save dialog box, click **Save** to save the files automatically in Autopsy's case subfolder: *Work*\Chap01\Projects\C1Prj01\Export.
8. Write a short report of no more than two paragraphs, including facts from any contents you found. When you're finished, leave Autopsy running if you're continuing to the next project.

Hands-On Project 1-2.

In this project, you work for a large corporation's IT Security Department. Your duties include conducting internal digital investigations and forensics examinations on company computing systems. A paralegal from the Law Department, Ms. Jones, asks you to examine a USB drive belonging to an employee who left the company and now works for a competitor. The Law Department is concerned that the former employee might possess sensitive company data. Ms. Jones wants to know whether the USB drive contains anything relevant.

In addition, she tells you that the former employee might have had access to confidential documents because a co-worker saw him accessing his manager's computer on his last day of work. These documents consist of nine files containing the word "confidential." She wants to know whether the USB's bit-stream image file has these documents.

To process this case, make sure the C1Prj02.001 file has been extracted to your work folder, and then follow these steps:

1.

Start Autopsy for Windows, if you exited it at the end of the previous project. If the previous project is open, click **Case**, **Close Case** from the menu. Click the **Create New Case** icon. In the New Case Information window, enter **C1Prj02** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**.

2. In the Additional Information window, type **C1Prj02** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

3. In the Select Data Source window, click the **Select data source type** list arrow, and click **Disk Image or VM file**. Click the **Browse** button next to the "Browse for an image file" text box, navigate to and click your work folder and the **C1Prj02.001** file, and then click **Open**. Click **Next**.

4. In the Configure Ingest Modules window, click **Select All**. Click **Next** and then **Finish**.

5. Click the **Keyword Search** button at the far upper right, type confidential in the text box, and then click **Search**.

6. In the Result Viewer pane, a new tab named Keyword search 1 opens. Click each file to view its contents in the Content Viewer pane.

7. Ctrl+click to select the files in the Keyword search 1 tab. Right-click this selection, point to **Tag File**, and click **Tag and Comment**. In the Create Tag dialog box, click the **New Tag Name** button, type **Recovered Office Documents** in the Tag Name text box, and then click **OK**.

8. Click **Generate Report** at the top. In the Generate Report window, click the **Results - Excel** option button in the Report Modules section, and then click **Next**.

9. In the Configure Artifacts Report window, click the **Tagged Results** button, click the **Recovered Office Documents** check box, and then click **Finish**.

10. In the Report Generation Progress Complete window, click the **Results - Excel** pathname to open the Excel report. This Excel file should have several tabs of information about the files you tagged for this project.

11. In the Report Generation Progress Complete window, click **Close**, and then exit Autopsy. Write a memo to Ms. Jones listing the filenames where you found a hit for the keyword. List the cluster numbers for hits that occurred in unallocated space. Include the Excel spreadsheet with the report.

Hands-On Project 1-3.

You're an IT security specialist for Superior Sailmakers, a company making sails for sloops and yawls. It sells rigging and sails to many sailboat makers who are competing against one another. Ms. Olsen in the Human Resources Department notifies you that she got an anonymous letter with an old USB drive. The letter states that a former employee, Ralph Williams, had photos belonging to ACE Sailboats that contained trade secrets from April 2006. The letter also states that after Mr. Williams ended his employment at Superior Sailmakers in January 2007, he used the photos on the USB drive to get hired by Smith Sloop Boats, a competitor of ACE Sailboats. Both sailboat manufacturers are customers of Superior Sailmakers.

Ms. Olsen tells you that another specialist has already made an image of the USB drive in the Expert Witness format (with an .E01 extension). She wants you to examine its contents for any photograph files to determine whether the anonymous complaint is true. After your examination, you need to generate a report that Ms. Olsen will send to the Legal Department. The Legal Department will then determine whether any violations of trade secret or intellectual property laws might have occurred.

Follow these steps:

1. Start Autopsy for Windows, and click the **Create New Case** icon. In the New Case Information window, enter **C1Prj03** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**.
2. In the Additional Information window, type **C1Prj03** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.
3. In the Select Data Source window, click the **Select data source type** list arrow, and click **Disk Image or VM file**. Click the **Browse** button next to the "Browse for an image file" text box, navigate to your work folder and click the **C1Prj03.E01** file, and then click **Open**. Click **Next**.
4. In the Configure Ingest Modules window, click **Select All**. Click **Next** and then **Finish**.

Because you're looking for photos of sailboats that were copied to the USB drive sometime during April 2006, perform the following steps.

1. In the Tree Viewer pane, expand **Views**, **File Types**, **By Extension**, and **Images**.
2. In the Result Viewer pane, scroll to the right, if necessary, until the Modified Time column is in view. Sort the column by clicking the **Modified Time** header.
3. Scroll down until you find the first file with a starting month of April 2006, and then click the file to view it in the Content Viewer. Press the **down arrow** on the keyboard to view all files created or modified in April 2006.
4. Ctrl+click every file that has a photo of a boat or part of a boat. Right-click this selection, point to **Tag File** and then **Quick Tag**, and click **Follow Up**.
5. In the Tree Viewer pane, scroll down and expand **Tags**, **Follow Up**, and **File Tags**.
6. In the Result Viewer pane, click the **Thumbnail** tab to view the tagged photos.
7. To create a report, click Generate Report at the top. In the **Generate Report** window, click the **Results - HTML** option button in the Report Modules section, and then click **Next**.
8. In the Configure Artifacts Report window, click the **Tagged Results** button, click the **Follow Up** check box, and then click **Finish**.
9. In the Report Generation Progress window, click the **Results - HTML** pathname to view the report. When viewing the report, click the links to examine the tagged files. When you're finished, click **Close** in the Report Generation Progress window.
10. Exit Autopsy, and write a short memo to summarize your findings.

Tip

When doing string searches, it's a good practice to examine graphics files that might contain documents. The search functions in forensics tools ignore graphics files because text in a graphics file is stored as part of a picture, not as plain text.

Hands-On Project 1-4.

Sometimes discovery demands from law firms require you to recover only allocated data from a disk. This project shows you how to extract just the files that haven't been deleted (that is, the allocated files) from an image.

1. Start Autopsy for Windows. Click the **Create New Case** icon. In the New Case Information window, enter **C1Prj04** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**.

2. In the Additional Information window, type **C1Prj04** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

3. In the Select Data Source window, click the **Select data source type** list arrow, and click **Disk Image or VM file**. Click the **Browse** button next to the "Browse for an image" text box, navigate to your work folder and click the **C1Prj04.E01** file, and then click **Open**. Click **Next**.

4. In the Configure Ingest Modules dialog box, click **Select All**. Click **Next** and then **Finish**.

5. In the Tree Viewer pane, expand **Views**, **File Types**, and **By Extension**. Under By Extension are several subfolders representing file types, as you've seen in previous projects. Next to each file type subfolder is a number enclosed in parentheses, which shows the number of files of this type Autopsy found. Click subfolders with numbers greater than zero to view the files.

6. In the Result Viewer pane, scroll to the right, if necessary until the Flags(Meta) column is in view. Sort the column by clicking the **Flags(Meta)** header, which displays all allocated files to the top of the list.

Note

In the Result Viewer pane, allocated (not deleted) files have a paper sheet icon to the left of the filename. Deleted (unallocated) files have a red X over the paper sheet icon, and unallocated files that have been corrupted and recovered by the OS have a diagonal broken bar icon.

7. Scroll to the left until the Name column is visible. If there are allocated files, they will be at the top of this list. Ctrl+click each allocated file, right-click this selection, and then click **Extract File(s)**.

8. In the Save dialog box, click Save to save the files automatically in Autopsy's case subfolder: *Work*\Chap01\Projects\C1Prj04\Export.

9. Write a brief memo that lists all the files you exported. Leave Autopsy running for the next project.

Hands-On Project 1-5.

This project is a continuation from the previous project. You create a report listing all the unallocated (deleted) files Autopsy finds.

1. Start Autopsy for Windows and click the **Open Recent Case** icon, if necessary.
2. In the Tree Viewer pane, expand **Views**, **File Types**, **Deleted Files**, and All.
3. In the Result Viewer pane, Ctrl+click all files in the All subfolder. Right-click this selection, point to **Tag File** and then **Quick Tag**, and click **Follow Up**.
4. Click **Generate Report** at the top. In the Generate Report window, click the **Results - Excel** option button in the Report Modules section, and then click **Next**.
5. In the Configure Artifacts Report window, click the **Tagged Results** button, click the **Follow Up** check box, and then click **Finish**.
6. In the Report Generation Progress Complete window, click the **Results - Excel** pathname to open the Excel report. When you're finished, click **Close** in the Report Generation Progress window.
7.

Write a brief memo listing all the deleted files on your report spreadsheet. Exit Autopsy.

Hands-On Project 1-6.

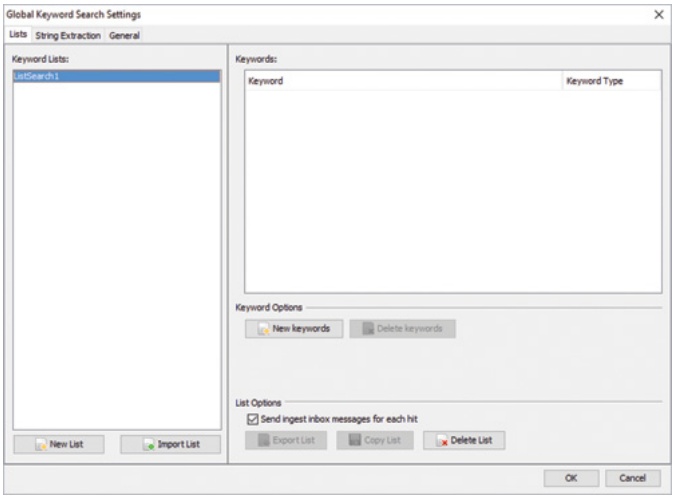
In this project, another investigator asks you to examine an image and search for all occurrences of the following keywords:

- ANTONIO
- HUGH EVANS
- HORATIO

After you complete these searches, the investigator wants a short report listing which files contain these names.

1. Start Autopsy for Windows. Click the **Create New Case** icon. In the New Case Information window, enter **C1Prj06** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**.
2. In the Additional Information window, type **C1Prj06** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.
3. In the Select Data Source window, click the **Select data source type** list arrow, and click **Disk Image or VM file**. Click the **Browse** button next to the "Browse for an image" text box, navigate to your work folder and click the **C1Prj06.E01** file, and then click **Open**. Click **Next**.
4. In the Configure Ingest Modules dialog box, click **Select All**. Click **Next** and then **Finish**.
5. Click the **Keyword Lists** button at the far upper right, and then click **Manage List**.
6. In the Global Keyword Search Settings dialog box, click the **New List** button. In the New Keyword List dialog box, type **ListSearch1** in the "New keyword list" text box, and then click **OK**.
7. In the Keyword Lists section, click **ListSearch1**, as shown in Figure 1-22, and then click the **New keywords** button under the Keyword Options heading.

Figure 1-22.



Source: www.sleuthkit.org

The Global Keyword Search Settings dialog box

8.

In the New keywords dialog box, type **ANTONIO** in the "Enter keywords (one per line) below" text box and press **Enter**, type **HUGH EVANS** and press **Enter**, and then type **HORATIO** and click **OK**. Click **OK** again.

9. In Autopsy's main window, click **Keyword List** again, click the **ListSearch1** check box, and then click **Search**.

10. Inspect each file to see whether it contains the word "confidential." If so, right-click the file, point to **Tag Files** and then **Quick Tag**, and then click **Follow Up**.

Note

If the search results don't display the keyword in the Content Viewer, the keyword might be obscured. For example, if a keyword is in unallocated disk space that's commingled with a graphics file, the Content Viewer automatically displays the graphics file. If this occurs and you want to examine the unallocated area, click the Content Viewer's Hex, String, or Indexed Text tabs to see what additional information might be revealed.

11. Click **Generate Report** at the top. In the Generate Report window, click the **Results - HTML** option button in the Report Modules section, and then click **Next**.

12. In the Configure Artifacts Report window, click the **Tagged Results** button, click the **Follow Up** check box, and then click **Finish**.

13. In the Report Generation Progress window, click the **Results - HTML** pathname to view the report. When you're finished, click **Close** and then exit Autopsy. Write a memo to the investigator with the following information from the report:

- Keyword
- File's pathname and filename
- Modified date and time
- Create date and time
- File size

Case Projects

Case Project 1-1.

An insurance company has asked your digital forensics firm to review a case for an arson investigation. The suspected arsonist has already been arrested, but the insurance company wants to determine whether there's any contributory negligence on the part of the victims. Two files were extracted to your work folder for this project. The first, Chap01_CasePrj01a.doc, is a memo about the case from the police department. The second, Chap01_CasePrj01b.doc, is a letter from the insurance company explaining what should be investigated. Review these files, and decide the course of action your firm needs to take. Write an outline for how your firm should approach the case.

Case Project 1-2.

Jonathan Simpson owns a construction company. One day a subcontractor calls him, saying that he needs a replacement check for the job he completed at 1437 West Maple Avenue. Jonathan looks up the job on his accounting program and agrees to reissue the check for $12,750. The subcontractor says that the original check was for only $10,750. Jonathan looks around the office but can't find the company checkbook or ledger. Only one other person has access to the accounting program. Jonathan calls you to investigate. How would you proceed?

Write a one-page report detailing the steps Jonathan needs to take to gather the necessary evidence and protect his company.

Case Project 1-3.

You are the digital forensics investigator for a law firm. The firm acquired a new client, a young woman who was fired from her job for inappropriate files discovered on her computer. She swears she never accessed the files. What questions should you ask and how should you proceed? Write a one- to two-page report describing the computer the client used, who else had access to it, and any other relevant facts that should be investigated.

Case Project 1-4.

A desperate employee calls because she has accidentally deleted crucial files from her hard drive and can't retrieve them from the Recycle Bin. What are your options? Write one to two pages explaining your capabilities and listing the questions you need to ask her about her system.

Chapter 2. The Investigator's Office and Laboratory

After reading this chapter and completing the exercises, you will be able to:

- Describe certification requirements for digital forensics labs
- List physical requirements for a digital forensics lab
- Explain the criteria for selecting a basic forensic workstation
- Describe components used to build a business case for developing a forensics lab

This chapter explains some options for setting up an effective digital forensics laboratory. Each digital forensics investigator in a lab should also have a private office where he or she can manage cases, conduct interviews, and communicate without eavesdropping concerns. Whether you're new to digital forensics or are an experienced examiner, your goal is to make your office and lab work smoothly and efficiently for all casework.

Digital forensics investigators must remember to consider budget and time when updating their labs to keep pace with computer technology changes. The workflow and processes you establish directly affect the quality of evidence you discover. You must balance cost, quality, and reliability when determining the kind of equipment, software, and other items you need to add to your lab. This chapter provides a foundation for organizing, controlling, and managing a safe, efficient forensics laboratory.

Understanding Forensics Lab Accreditation Requirements

A **digital forensics lab** is where you conduct investigations, store evidence, and do most of your work. You use the lab to house your instruments, current and legacy software, and forensic workstations. In general, you need a variety of digital forensics hardware and software to do your work.

You also need to make sure you have defined policies, processes, and prescribed procedures before beginning any casework to ensure the integrity of an analysis and its results. A number of organizations have created guidelines for devising your own processes and procedures. What's most important is that you follow the policies and procedures you have created to ensure consistency in your output. Checklists are a good way to ensure consistent methods of operations for staff.

Caution ⚠

Be sure to research accrediting bodies thoroughly before pursuing any accreditation. Many accreditations are offered by software vendors; others are specific for law enforcement or started by local groups.

The **ANSI-ASQ National Accreditation Board (ANAB)** (www.anab.org), a wholly owned subsidiary of ANSI (American National Standards Institute) and ASQ (American Society for Quality), provides accreditation of crime and forensics labs worldwide. This accreditation includes forensics labs that analyze digital evidence. For a lab to be accredited, ANAB audits the lab's tasks and functions to ensure correct and consistent results for all cases. These audits are done on subscribing members' forensics labs to ensure the quality and integrity of their work. The following sections discuss several key guidelines from the ANAB program that you can apply to managing, configuring, and auditing your forensics lab. For additional information on how ANAB conforms to an international standard, see www.anab.org/forensics-accreditation/iso-iec-17025-forensic-labs.

Identifying Duties of the Lab Manager and Staff

The ANAB states that each lab should have specific objectives that a parent organization and the lab's director or manager have determined. The lab manager sets up processes for managing cases and reviews them regularly. Besides performing general management tasks, such as promoting group consensus in decision making, maintaining fiscal responsibility for lab needs, and enforcing ethical standards (covered in **Chapters 15** and 16) among staff members, the lab manager plans updates for the lab, such as new hardware and software purchases.

The lab manager also establishes and promotes quality assurance processes for the lab's staff to follow, such as outlining what to do when a case arrives, logging evidence, specifying who can enter the lab, and establishing guidelines for filing reports. To ensure the lab's efficiency, the lab manager also sets reasonable production schedules for processing work.

A typical investigation involves seizing a hard disk and other media, such as USB drives; making forensic copies of them; evaluating evidence; and filing a report. A forensics analysis of a 6 TB disk, for example, can take several days or weeks and often involves running imaging software overnight and on weekends. This means one of the forensic workstations in the lab is occupied for that time, which can be 20 hours or more. Based on past experience, the lab manager can estimate how many cases each investigator can handle and when to expect a preliminary and final report for each case.

The lab manager creates and monitors lab policies for staff and provides a safe and secure workplace for staff and evidence. Above all, the lab manager accounts for all activities the lab's staff conducts to complete its work. Tracking cases such as e-mail abuse, Internet misuse, and illicit activities can justify the funds spent on a lab.

Staff members in a forensics lab should have enough training to perform their tasks. Necessary skills include hardware and software knowledge, including OSs and file types, and deductive reasoning. Their work is reviewed regularly by the lab manager and their peers to ensure quality. Staff members are also responsible for continuing technical training to update their investigative and computer skills and maintaining a record of the training they have completed. Many vendors and organizations hold annual or quarterly training seminars that offer certification exams.

The ANAB Web site summarizes the requirements of managing a digital forensics lab, handling and preserving evidence, performing laboratory procedures, setting personnel requirements, and encouraging professional development. The site also provides a user license for printed and online manuals of lab management guidelines. ANAB stresses that each lab should maintain an up-to-date library of resources in its field. For digital forensics, these resources include software, hardware information, and technical journals.

Lab Budget Planning

To conduct a professional digital investigation, you need to understand the cost of your lab operation. Lab costs can be broken down into monthly, quarterly, and annual expenses. The better you understand these expenses, the better you can delegate resources for each investigation. Using a spreadsheet program helps you keep track of past investigation expenses so that you can extrapolate expected future costs. Remember that expenses include purchasing computer hardware and software, renting facility space, and training personnel.

When creating a budget, start by estimating the number of cases your lab expects to examine and identifying the types of computers you're likely to examine, such as Windows PCs, Apple systems, or Linux workstations. For example, suppose you work for a state police agency that's planning to provide digital investigation services for the entire state. You could start by collecting state crime statistics for the current year and several previous years to determine types of computers or other devices associated with these crimes. Criminal behavior often reflects sales trends for certain computing systems. Because most consumers use Intel and AMD PCs, and most of these computers run Windows, the same is likely true of computers

used in crimes. Verify this trend by determining how often each type of system is used in a crime. List the number of crimes committed that involve Windows, Linux/UNIX, and Apple computers. In addition to estimating resources for digital investigations, you should also determine what resources will be needed to examine mobile devices, such as smartphones and tablets.

If you can't find detailed information on the types of computers and OSs used in digital crimes, gather enough information to make an educated guess. Your goal is to build a baseline for the types and numbers of systems you can expect to investigate. In addition to the historical data you compile, identify any future trends that could affect your lab, such as a new version of an OS or an increase in the number of computers involved in crime.

Next, estimate how many investigations you might conduct involving computer systems used less often to help determine how many tools you need to examine these systems. For example, if you learn that on average, one Macintosh is involved in a criminal investigation each month, you probably need only one or two software tools to conduct a forensic analysis on Macintosh file systems.

Figure 2-1 shows a table of statistics from a **Uniform Crime Report** that identifies the number of hard disk types, such as SATA or SCSI, and the OS used to commit crimes. Annual Uniform Crime Reports are generated at the federal, state, and local levels to show the types and frequency of crimes committed. For federal reports, see https://ucr.fbi.gov/ucr-publications, and for a summary of crimes committed at different levels, see www.bjs.gov.

Figure 2-1.

Crime Statistics For 2016	HDD	Windows OS	Linux	OS X & 9	Other H/W	Mobile Devices	Total Systems Examined
Arson	5	3	1	1	0	0	5
Bribery	6	3	0	1	0	0	4
Burglary	6	0	0	0	0	0	0
Child Porn	29	14	2	7	0	23	46
Counterfeit & Forgery	6	6	0	0	0	1	7
Drug Narcotic	20	7	0	3	0	54	64
Embezzlement	9	9	0	1	1	0	11
Extortion & Blackmail	5	3	2	0	0	1	6
Fraud	13	4	0	7	0	41	52
Gambling	10	7	2	0	0	5	14
Homicide	13	5	0	0	0	3	8
Kidnapping & Abduction	0	0	0	0	0	1	1
Larceny Theft	2	1	0	2	0	0	3
Robbery	1	0	0	1	0	0	1
Sex Offense Forcible	6	4	0	0	0	0	4
Sex Offense Non-Forcible	8	8	0	0	0	8	16
Stalking	15	9	0	5	0	28	42
Stolen Property Offenses	1	1	0	0	0	0	1
Weapons Violations	2	2	0	0	0	0	2
Totals	157	86	7	28	1	165	287

Uniform Crime Report statistics

You can also identify specialized software used with certain crimes. For example, if you find a check-writing software tool used in several counterfeiting cases, you should consider adding this specialized software to your inventory.

If you're preparing to set up a forensics lab for a private company, you can determine your needs more easily because you're working in a contained environment. Start by getting an inventory of all known computing systems and applications used in the business. For example, an insurance company often has a network of Intel PCs and servers and specialized insurance software using a database for data storage. A large manufacturing company might use Intel

PCs, UNIX workstations running a computer-aided design (CAD) system, super minicomputers, and mainframes. A publishing company might have a combination of Intel PCs and Macintosh systems and a variety of word processing, imaging, and composition packages. Many other organizations use cloud-based storage or supervisory control and data acquisition (SCADA) systems for data and applications.

Next, check with your Management, Human Resource, and Security departments to determine the types of complaints and problems reported in the past year. Most companies using Internet connections, for example, get complaints about employees accessing the Web excessively or for personal use, which generate investigations of Web misuse. Be sure to distinguish investigations of excessive Web use from inappropriate Web site access and e-mail harassment.

Your budget should also take future developments in digital technology into account because drive storage capabilities improve constantly. When examining a disk, you need a target disk to copy evidence data to. This disk should be at least one and a half times the size of the evidence (suspect) disk. For example, a lab equipped with 4 TB disks can effectively analyze disks up to 3 TB. If your company upgrades its computers to 3 TB disks, however, you need disks that are 6 TB or more or a central secure server with at least 100 TB or more of storage. One forensic server, the Digital Intelligence FREDC (www.digitalintelligence.com/products/fredc/), includes a private cloud that starts at 96 TB, with options for installing more storage. Many businesses replace their desktop computers every 18 months to three years. You must be informed of computer upgrades and other changes in the computing environment so that you can prepare and submit your budget for needed resources.

When considering a central forensic server, such as the FREDC, your network should be designed to support higher speeds. The faster the network, the faster data can be transferred to and from the forensic server and workstations. This increase in speed reduces the time needed to process cases.

An alternative to digital forensics data storage is cloud storage. The cost savings are considerably higher than you get when purchasing storage hardware; however, you need to consider the throughput speeds of retrieving data and the levels of security. For more information on cloud security, see the Cloud Security Alliance (CSA) Security as a Service (SecaaS) Working Group (https://cloudsecurityalliance.org/group/security-as-a-service/#_downloads), which offers several papers and implementation guides.

Like hardware, OSs change periodically. If your current digital forensics tool doesn't work with the next release of an OS or a file system, you must upgrade your software tools. You should also monitor or contact vendor product development teams to learn about upgrades. File systems change, too. Forensics tools had their birth in DOS, and over the years, Windows hard disks used a variety of file systems, including FAT16, FAT32, New Technology File System (NTFS), Resilient File System (ReFS), and others. Most DOS-based tools can't read NTFS disks. In addition, the popularity and prevalence of the Xbox requires investigators to be familiar with the FATX file system.

Time management is a major factor when choosing software and hardware to purchase. For example, you've decided to purchase eight machines for your lab. Many commercial forensics software packages require a USB dongle to operate or have a site license of five concurrent users. You or the budget manager must decide whether you're using all the machines or need only two licensed copies of each software package. Your choices depend on what tools you have verified and what's needed for your casework.

Another option for viewing file systems is to use a Linux Live CD or WinFE (modified version of WinPE, the automated installation kit), which are CD or DVD disk acquisition tools discussed in **Chapter 3**. These tools don't mount the hard drive automatically and, therefore, don't write to the drive. (A hardware write-blocker is still recommended to prevent errors

caused by the forensics technician, if nothing else.) Examining tablets, USB drives, and smartphones is routine now in cases from criminal investigations to civil litigation discovery demands. Digital investigators must be prepared to deal with constant change in these devices and know what tools are available to extract data from them safely for an investigation. In Chapter 12, you learn how to acquire data from these devices.

Acquiring Certification and Training

To continue a career in digital investigations and forensic analysis, you need to upgrade your skills through training. Several organizations have developed certification programs for digital forensics that usually test you after you have completed one or more training sessions successfully. Certifying organizations range from nonprofit associations to vendor-sponsored groups. All these programs charge fees for certification, and some require candidates to take vendor-sponsored or organization-sponsored training to qualify for the certification. Some U.S. state legislatures now require digital forensics examiners working in a private practice or business to have a private investigator's license. These states typically require some level of training and certification in both digital forensics and investigations before you apply for a license.

Before enlisting in a certification program, thoroughly research the requirements, cost, and acceptability in your area of employment. Most certification programs require continuing education credits or reexamination of candidates' skills, which can become costly.

International Association of Computer Investigative Specialists

Created by police officers who wanted to formalize credentials in digital investigations, the International Association of Computer Investigative Specialists (IACIS) is one of the oldest professional digital forensics organizations. For more information about IACIS, visit its Web site (www.iacis.com) to verify the current membership requirements.

Candidates who complete the IACIS test successfully are designated as a **Certified Forensic Computer Examiner (CFCE)** . The CFCE process changes as technology changes. The description here is current as of this writing. IACIS requires recertification every three years to demonstrate continuing work in the field of digital forensics. Recertification is less intense than the original certification but does test examiners to make sure they're continuing their education and are still active in the field of digital forensics. For the latest information about the CFCE certification, or IACIS membership, visit the IACIS Web site.

In addition to the CFCE, IACIS has two specialized certification programs: Certified Advanced Windows Forensic Examiner (CAWFE) and the IACIS Certified Mobile Device Examiner (ICMDE).

ISC^2 Certified Cyber Forensics Professional

The **Certified Cyber Forensics Professional (CCFP)** program, sponsored by ISC^2, requires knowledge of digital forensics, malware analysis, incident response, e-discovery, and other disciplines related to cyber investigations. The CCFP Web site (www.isc2.org/ccfp/default.aspx) lists requirements and processes needed for this certification.

High Tech Crime Network

The **High Tech Crime Network (HTCN)** also offers several levels of certification. Unlike IACIS, however, HTCN requires a review of all related training, including training in one of its approved courses, and a review of the candidate's work history. HTCN certification is open to anyone meeting the criteria in the profession of computing investigations. At the time of this writing, the HTCN Web site (www.htcn.org) specifies requirements for the certification levels discussed in the following paragraphs. Requirements are updated without notice, so make sure you check the site periodically.

Certified Computer Crime Investigator, Basic

- Candidates must have three years of experience directly related to investigating computer-related incidents or crimes.
- Candidates have successfully completed 40 hours of training from an approved agency, organization, or training company.
- Candidates must provide documentation of at least 10 cases in which they participated.

Certified Computer Crime Investigator, Advanced

- Candidates must have five years of experience directly related to investigating computer-related incidents or crimes.
- Candidates have successfully completed 80 hours of training from an approved agency, organization, or company.
- Candidates have served as lead investigator in at least 20 cases during the past three years and were involved in at least 40 other cases as a lead investigator or supervisor or in a supportive capacity. Candidates have at least 60 hours of involvement in cases in the past three years.

Certified Computer Forensic Technician, Basic

- Candidates must have three years of experience in computing investigations for law enforcement or corporate cases.
- Candidates must have completed 40 hours of computer forensics training from an approved organization.
- Candidates must provide documentation of at least 10 computing investigations.

Certified Computer Forensic Technician, Advanced

- Candidates must have five years of hands-on experience in computer forensics investigations for law enforcement or corporate cases.
- Candidates must have completed 80 hours of computer forensics training from an approved organization.
- Candidates must provide documentation of at least 15 computing investigations.
- Candidates must have been the lead computer forensics investigator in 20 or more investigations in the past three years and in 40 or more additional computing investigations as lead computer forensics technician, supervisor, or contributor. The candidate must have completed at least 60 investigations in the past three years.

EnCase Certified Examiner Certification

Guidance Software, the creator of EnCase, sponsors the EnCase Certified Examiner (EnCE) certification program. EnCE certification is open to the public and private sectors and is specific to use and mastery of EnCase forensics analysis. Requirements for taking the EnCE certification exam don't depend on taking the Guidance Software EnCase training courses. Candidates for this certification are required to have a licensed copy of EnCase. For more information on EnCE certification requirements, visit www.guidancesoftware.com/training/certifications?cmpid=nav_r. Additional certifications offered by Guidance Software are Certified Forensic Security Responder (CFSR) and EnCase Certified eDiscovery Practitioner (EnCEP).

AccessData Certified Examiner

AccessData sponsors the AccessData Certified Examiner (ACE) certification program. ACE certification is open to the public and private sectors and is specific to use and mastery of AccessData Ultimate Toolkit. To help prepare for the ACE exam, applicants can attend the AccessData BootCamp and advanced FTK courses. The exam has a knowledge base component and a practical skills component. For more information on this certification, visit www.syntricate.com/computer-forensics-certification.html.

Other Training and Certifications

The following are other organizations to consider for certification or training:

- EC-Council, www.eccouncil.org/Certification
- SysAdmin, Audit, Network, Security (SANS) Institute, www.sans.org or https://digital-forensics.sans.org/certification
- Defense Cyber Investigations Training Academy (DCITA), www.dcita.edu
- International Society of Forensic Computer Examiners (ISFCE, www.isfce.com) for the **Certified Computer Examiner (CCE)** certification
- Computer Technology Investigators Network (CTIN), www.ctin.org
- Digital Forensics Certification Board (DFCB), www.dfcb.org/certification.html
- Cloud Security Alliance (CSA), https://cloudsecurityalliance.org/education/

Organizations that offer training and certification for law enforcement personnel or qualified civilian government personnel include the following:

- Federal Law Enforcement Training Centers (FLETC), www.fletc.gov
- National White Collar Crime Center (NW3C), www.nw3c.org

Determining the Physical Requirements for a Digital Forensics Lab

After you have the training to become a digital forensics investigator, you conduct most of your investigations in a lab. This section discusses the physical requirements for a forensics lab. Addressing these requirements can make a lab safer, more secure, and more productive.

Your lab facility must be physically secure so that evidence isn't lost, corrupted, or destroyed. As with hardware and software costs, you must consider what's needed to maintain a safe and secure environment when determining physical lab expenses. You must also use inventory control methods to track your computing assets, which means you should maintain a complete and up-to-date inventory of all major hardware and software items in the lab. For consumable items, such as cables and storage media, maintain an inventory so that you know when to order more supplies.

Identifying Lab Security Needs

All digital forensics labs need an enclosed room where a forensic workstation can be set up. You shouldn't use an open cubicle because it allows easy access to your evidence. You need a room you can lock to control your evidence and attest to its integrity. In particular, your lab should be secure during data analysis, even if it takes several weeks to analyze a disk drive. To preserve the integrity of evidence, your lab should function as an evidence locker or safe, making it a **secure facility** or a secure storage safe.

The following are the minimum requirements for a digital forensics lab of any size:

- Small room with true floor-to-ceiling walls

- Door access with a locking mechanism (limited to authorized users, including cleaning crews), which can be a regular key lock, combination lock, or an electronic lock capable of logging who accessed it
- Secure container, such as a safe or heavy-duty file cabinet with a quality padlock that prevents drawers from opening
- Visitor's log with legible entries listing all people who have accessed the lab and showing the date, time in, and time out

For daily work production, several examiners can work together in a large open area, as long as they all have the same level of authority and access need. This area should also have floor-to-ceiling walls and a locking door. In many public and private organizations, several investigators share a door to the lab that requires an ID card and entry code.

Digital investigators and forensics examiners must be briefed on the lab's security policy. Share information about a case investigation only with other examiners and personnel who need to know about the investigation.

Conducting High-Risk Investigations

High-risk investigations, such as those involving national security or murder, demand more security than the minimum lab requirements provide. As technology improves and information circulates among computer attackers, keeping an investigation secure can be more difficult. For example, detecting computer eavesdropping is difficult and expensive, but sophisticated criminals and intelligence services in foreign countries can use equipment that detects network transmissions, wireless devices, phone conversations, and the use of computer equipment. Instructions for building a sniffing device that can collect computer emanations illegally can be found online and, therefore, are available to anyone. These devices can pick up anything you type on your computer.

Most electronic devices emit electromagnetic radiation (EMR). Certain kinds of equipment can intercept EMR, which can be used to determine the data the device is transmitting or displaying. The EMR from a computer monitor can be picked up as far away as a half mile.

During the Cold War, defense contractors were required to shield sensitive computing systems and prevent electronic eavesdropping of any computer emissions. The U.S. Department of Defense calls this special computer-emission shielding **TEMPEST** . (For a brief description of TEMPEST, see the National Industrial Security Program Operating Manual [NISPOM]. DoD 5220.22-M, Chapter 11, Section 1, TEMPEST, www.dss.mil/documents/odaa/nispom2006-5220.pdf or SANS Institute, InfoSec Reading Room's article "An Introduction to TEMPEST," www.sans.org/reading-room/whitepapers/privacy/introduction-tempest-981. Another site listing reliable sources is www.jammed.com/~jwa/tempest.html.)

To protect your investigations, you might consider constructing a TEMPEST-qualified lab, which requires lining the walls, ceiling, floor, and doors with specially grounded conductive metal sheets. Typically, copper sheeting is used because it conducts electricity well. TEMPEST facilities must include special filters for electrical power that prevent power cables from transmitting computer emanations. All heating and ventilation ducts must have special baffles to trap emanations. Likewise, telephones inside the TEMPEST facility must have special line filters. A TEMPEST facility usually has two doors separated by dead space. The first exterior door must be shut before opening the interior door. Each door also has special copper molding to enhance electricity conduction.

Because a TEMPEST-qualified lab facility is expensive and requires routine inspection and testing, it should be considered only for large regional digital forensics labs that demand absolute security from illegal eavesdropping. To avoid these costs, some vendors have built low-emanating workstations instead of TEMPEST facilities. These workstations are more expensive than average workstations but less expensive than a TEMPEST lab.

Using Evidence Containers

Evidence storage containers, also known as evidence lockers, must be secure so that no unauthorized person can access your evidence easily. You must use high-quality locks, such as padlocks, with limited duplicate-key distribution. Also, inspect the contents of evidence storage containers routinely to make sure only current evidence is stored. The evidence custody forms should indicate what's still in the locker. Evidence for closed cases should be moved to a secure off-site facility.

Chapter 5, Section 3, of the NISPOM (www.dss.mil/documents/odaa/nispom2006-5220.pdf) describes the characteristics of a safe storage container. Consult with facility management or legal counsel, such as corporate or prosecuting attorneys, to determine what your lab should do to maintain evidence integrity. The following are recommendations for securing storage containers:

- The evidence container should be located in a restricted area that's accessible only to lab personnel.
- The number of people authorized to open the evidence container should be kept to a minimum. Maintain records on who's authorized to access each container.
- All evidence containers should remain locked when they aren't under the direct supervision of an authorized person.

If a combination locking system is used for your evidence container, follow these practices:

- Provide the same level of security for the combination as for the container's contents. Store the combination in another equally secure container.
- Destroy any previous combinations after setting up a new combination.
- Allow only authorized personnel to change lock combinations.
- Change the combination every six months, when any authorized personnel leave the organization, and immediately after finding an unsecured container—that is, one that's open and unattended.

If you're using a keyed padlock, follow these practices:

- Appoint a key custodian who's responsible for distributing keys.
- Stamp sequential numbers on each duplicate key.
- Maintain a registry listing which key is assigned to which authorized person.
- Conduct a monthly audit to ensure that no authorized person has lost a key.
- Take an inventory of all keys when the custodian changes.
- Place keys in a lockable container accessible only to the lab manager and designated key custodian.
- Maintain the same level of security for keys as for evidence containers.
- Change locks and keys annually; if a key is missing, replace all associated locks and the key.
- Do not use a master key for several locks.

The storage container or cabinet should be made of steel and include an internal cabinet lock or external padlock. If possible, purchase a safe, which provides superior security and protects your evidence from fire damage. Look for specialized safes, called "media safes," designed to

protect electronic media. Media safes are rated by the number of hours it takes before fire damages the contents. The higher the rating, the better the safe protects evidence.

An evidence storage room is also convenient, especially if it's part of your forensics lab. Security for an evidence room must integrate the same construction and securing devices as the general lab does. Large digital forensics operations also need an evidence custodian and a service counter with a securable metal roll-up window to control evidence. With a secure evidence room, you can store large computer components, such as computers, monitors, and other peripheral devices.

Be sure to maintain a log listing every time an evidence container is opened and closed. Each time the container is accessed, the log should indicate the date it was opened and the initials of the authorized person. These records should be maintained for at least three years or longer, as prescribed by your prosecuting or corporate attorneys. Logs are discussed in more detail in **Chapter 4**.

Overseeing Facility Maintenance

Your lab should be maintained at all times to ensure the safety and health of lab personnel. Any damage to the floor, walls, ceilings, or furniture should be repaired immediately. Also, be sure to escort cleaning crews into the facility and monitor them as they work.

Because static electricity is a major problem when handling computer parts, placing antistatic pads around electronic workbenches and workstations is recommended. In addition, floors and carpets should be cleaned at least once a week to help minimize dust that can cause static electricity.

Maintain two separate trash containers, one to store items unrelated to an investigation, such as discarded CDs, and the other for sensitive material that requires special handling to make sure it's destroyed. Using separate trash containers maintains the integrity of criminal investigation processes and protects trade secrets and attorney-client privileged communication in a private company. Several commercially bonded firms specialize in disposing of sensitive materials, and you should hire one to help maintain the integrity of your investigations.

Considering Physical Security Needs

In addition to your lab's physical design and construction, you need to enhance security by setting security policies. How much physical security you implement depends on the nature of your lab. A regional computer crime lab has high physical security needs because of the risks of losing, corrupting, or damaging evidence. The physical security needs of a large corporation are probably not as high because the risk of evidence loss or compromise is much lower. Determining the risk for your organization dictates how much security you integrate into your digital forensics lab.

Note

When considering digital security needs, many companies neglect physical security.

Regardless of the security risk to your lab, maintain a paper or electronic sign-in log for all visitors. The log should list the visitor's name, date and time of arrival and departure, employer's name, purpose of the visit, and name of the lab member receiving the visitor. Consider anyone who's not assigned to the lab to be a visitor, including cleaning crews, facility maintenance personnel, friends, and family. All visitors should be escorted by an assigned authorized staff member throughout their visit to the lab to ensure that they don't accidentally or intentionally tamper with an investigation or evidence. As an added precaution, use a visible or audible alarm, such as a visitor badge, to let all investigators know that a visitor is in

the area. If possible, hire a security guard or have an intrusion alarm system with a guard to ensure your lab's security. Alarm systems with guards can also be used after business hours to monitor your lab.

Auditing a Digital Forensics Lab

To make sure security policies and practices are followed, conduct routine inspections to audit your lab and evidence storage containers. Audits should include, but aren't limited to, the following facility components and practices:

- Inspect the lab's ceiling, floor, roof, and exterior walls at least once a month, looking for anything unusual or new.
- Inspect doors to make sure they close and lock correctly.
- Check locks to see whether they need to be replaced or changed.
- Review visitor logs to see whether they're being used properly.
- Review log sheets for evidence containers to determine when they have been opened and closed.
- At the end of every workday, secure any evidence that's not being processed on a forensic workstation.

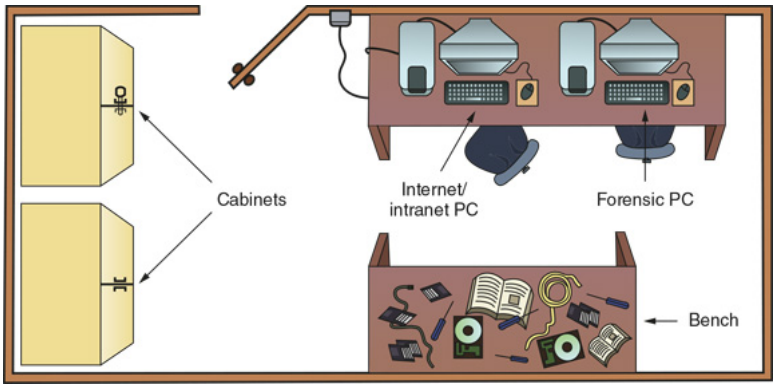
Determining Floor Plans for Digital Forensics Labs

How you configure the work area for your digital forensics lab depends on your budget, the amount of available floor space, and the number of computers you assign to each computing investigator. For a small operation handling two or three cases a month, one forensic workstation should be enough to handle the workload. One workstation requires only the space an average desk takes up. If you're handling many more cases per month, you can probably process two or three investigations at a time, which requires more than one workstation. The ideal configuration for multiple workstations is to have two forensic workstations plus one non-forensic workstation with Internet access.

Because you need plenty of room around each workstation, a work area containing three workstations requires approximately 150 square feet of space, meaning the work area should be about 10 feet by 15 feet. This amount of space allows for two chairs so that the digital investigator can brief another investigator, paralegal, or attorney on the case.

Small labs usually consist of one or two forensic workstations, a research computer with Internet access, a workbench (if space allows), and storage cabinets, as shown in **Figure 2-2**.

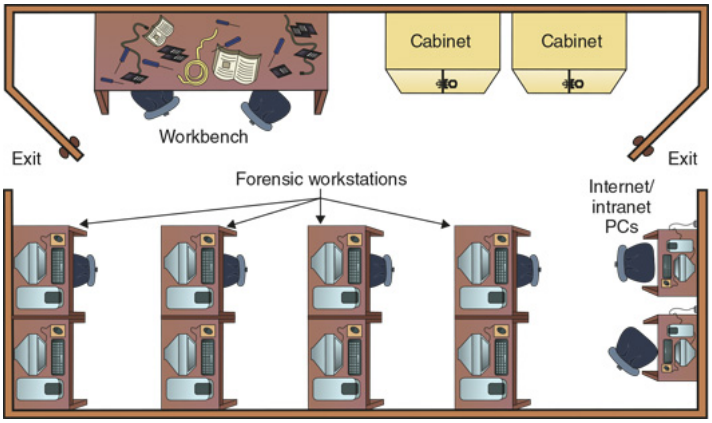
Figure 2-2.



Small or home-based lab

Mid-size digital forensics labs, such as those in a private business, have more workstations. For safety reasons, the lab should have at least two exits, as shown in **Figure 2-3**. If possible, cubicles or even separate offices should be part of the layout to reinforce the need-to-know policy. These labs usually have more library space for software and hardware storage.

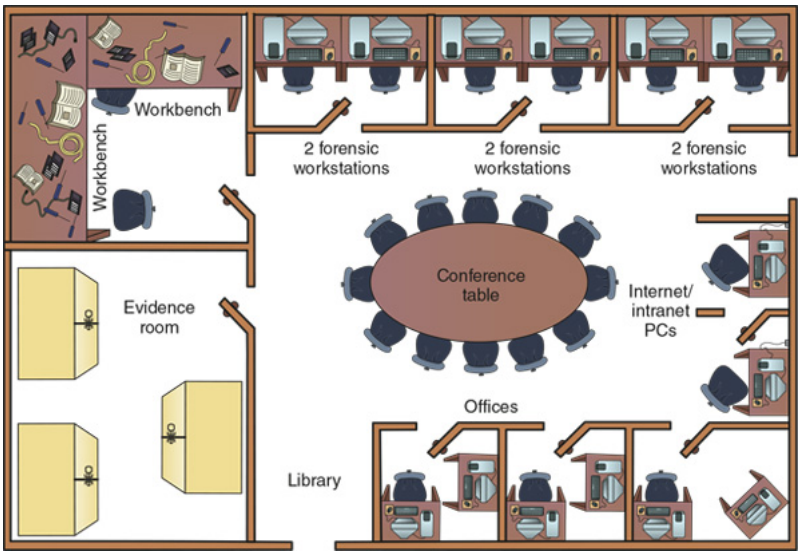
Figure 2-3.



Mid-size digital forensics lab

State law enforcement or the FBI usually runs most large or regional digital forensics labs. As shown in **Figure 2-4**, these labs have a separate evidence room, which is typical in police investigations, except this room is limited to digital evidence. One or more custodians might be assigned to manage and control traffic in and out of the evidence room.

Figure 2-4.



Regional digital forensics lab

As discussed, the evidence room needs to be secure. The lab should have at least two controlled exits and no windows. Separate offices for supervisors and cubicles for investigators are more practical in this configuration. Remember that forensic workstations are connected to an isolated local area network (LAN), and only a few machines are connected to an organization's intranet or the Internet.

Selecting a Basic Forensic Workstation

The workstation you use as a forensics analysis system depends on your budget and specific needs. You can find many well-designed forensic workstations that can handle most digital investigation needs. When acquiring a workstation, try to get the most powerful processor and the most RAM and disk storage available to improve the productivity of digital examinations. When you start processing a case, you use a workstation for the duration of the examination. Use less powerful workstations for mundane tasks and multipurpose workstations for resource-heavy analysis tasks.

Selecting Workstations for a Lab

If you're managing a lab for a police department in a major city, you probably have the most diverse needs for digital investigation tools because the communities it serves use a wide assortment of computing systems. Not all computer users have the latest technology, so a lab might need legacy systems and software, such as computers running CP/M or Minix, to match what's used in the community. For small, local police departments, however, most work involves Windows PCs, Macintosh systems, and mobile devices. A small police department's digital forensics lab could be limited to one multipurpose forensic workstation with one or two basic workstations or high-end laptops.

One way to investigate older and unusual computing systems is to keep track of forums and blogs that you can find through an online search. These groups can be a valuable source of support for recovering and analyzing uncommon systems. Entering "computer forensics" or "digital forensics" as a search keyword produces several links you can follow to further your knowledge in this profession. You can also coordinate with or subcontract to larger forensics labs. Like large police departments, a regional digital forensics lab must have diverse systems to serve its community and often receives work from smaller labs involving unusual computers or OSs.

Computing systems in a lab should be able to process typical cases in a timely manner. The time it takes to process a case usually depends on the size and type of industries in the region. For example, suppose your lab is located in a region with a large manufacturing firm that employs 50,000 people. Based on crime reports you've consulted, 1% of those employees might be involved in criminal behavior, meaning 500 employees will commit crimes such as fraud, embezzlement, and so on. These statistics can help you estimate how much time is involved in processing these types of cases.

Improvements in hardware technology offer more flexibility in digital forensics. You can now use a laptop system with USB 3.0 or SATA hard disks to create a lightweight, mobile forensic workstation. Improved throughput speeds of data transfer on laptops also make it easier to create images of suspect drives, especially in the field.

Another consideration is the need to perform password cracking to access a suspect's encrypted data. For this task, desktop computers that can use multiple graphics processing units (GPUs) are helpful. For the latest information on password recovery, search online for "password cracking systems and clusters."

For white papers about password clusters, consult the following resources:

- http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.70.2420&rep=rep1&type=pdf
- www.emc.com/collateral/software/white-papers/h5936-recoverpoint-cluster-enabler-wp.pdf
- www.whitehatsec.com/blog/cracking-aes-256-dmgs-and-epic-self-pwnage/
- www.picocomputing.com/pdf/Pico_White_Paper_Crypto_Nov_09.pdf
- www.blackhat.com/docs/us-15/materials/us-15-Morris-CrackLord-Maximizing-Password-Cracking-wp.pdf

Selecting Workstations for Private-Sector Labs

For the private sector, such as a business conducting internal investigations or a commercial business providing digital forensics services to private parties, equipment resources are generally easy to determine.

Commercial businesses providing forensics analysis for other companies can tailor their services to specific markets. They can specialize in one or two platforms, such as an Intel PC running a Microsoft OS. They can also gather a variety of tools to meet a wider market. The type of equipment they need depends on their specialty, if any. For general digital forensics facilities, a multipurpose forensic workstation is enough.

Private companies conducting their own internal digital investigations can determine the type of forensic workstation they need based on the types of computers they use. If a company uses only Windows PCs, internal investigators don't need a wide variety of specialized equipment. If a company uses many kinds of computers, its internal investigators need systems and equipment that support the same types of computers. With some digital forensics programs, you can work from a Windows PC and examine both Windows and Macintosh disk drives.

Stocking Hardware Peripherals

In addition to workstations and software, all labs should have a wide assortment of cables and spare expansion slot cards. Consider stocking your forensics lab with the following peripheral devices:

- A digital camera capable of still and motion recording
- Assorted antistatic bags
- An external CD/DVD drive
- 40-pin 18-inch and 36-inch IDE cables, both ATA-33 and ATA-100 or faster
- Ribbon cables for floppy disks
- Extra USB 3.0 or newer cables and SATA cards and associated cables
- Extra SCSI cards, preferably ultrawide
- Graphics cards, both Peripheral Component Interconnect (PCI) and Accelerated Graphics Port (AGP)
- Assorted FireWire and USB adapters
- A variety of hard drives and USB drives (as many as you can afford and in as wide a variety as possible)
- At least two 2.5-inch adapters from notebook IDE hard drives to standard IDE/ATA drives, SATA drives, and so on
- Computer hand tools, such as Phillips and flathead screwdrivers, a socket wrench, any vendor-specific tools, a small flashlight, and an antistatic wrist strap

Maintaining Operating Systems and Software Inventories

Operating systems are an essential part of your lab's inventory. You should maintain licensed copies of as many legacy OSs as possible to handle cases involving unusual systems. Microsoft OSs should include, in addition to the most current OS, Windows 10, 8.0 and 8.1, 7, Vista, XP, 2000, NT 4.0, NT 3.5, 9x, 3.11, and DOS 6.22. Macintosh OSs should include macOS, Mac OS X, 9.x, and 8 or older. Linux OSs can include Linux Mint, DeftZ, Fedora, Ubuntu, Slackware, and Debian.

Although most high-end digital forensics tools can open or display data files created with commonly used programs, they don't support all programs. Your software inventory should

include current and older versions of the following programs. If you deal with Windows PCs, Macintosh systems, and Linux systems, you should have programs for all these OSs.

- Microsoft Office (including current and older versions)
- Hexadecimal editor, such as WinHex or Hex Workshop
- Programming languages, such as Visual Studio, Perl, or Python
- Specialized image viewers, such as Quick View, ACDSee, ThumbsPlus, and IrfanView
- WPS Office, WordPerfect, and a third-party or open-source office suite
- Accounting applications, such as Quicken and QuickBooks

Using a Disaster Recovery Plan

Besides planning for equipment needs, you need to plan for disasters, such as hard disk crashes, lightning strikes, power outages, floods, earthquakes, and so forth. A disaster recovery plan ensures that you can restore your workstations and file servers to their original condition or a lab-like building if a catastrophic failure occurs.

A disaster recovery plan also specifies how to rebuild a forensic workstation after it has been severely contaminated by a virus from a drive you're analyzing. Central to any disaster recovery plan is a system for backing up investigation computers. Tools such as Norton Ghost are useful for restoring files directly. As a general precaution, you should back up your workstation once a week. You can restore programs from the original disks, USB drives, CDs/DVDs, or the cloud, but recovering lost data without up-to-date backups is difficult.

Store your system backups where they are easily accessible. You should have at least one copy of backups on site and a duplicate or a previous copy of backups stored in a safe off-site facility. Off-site backups are usually rotated on a schedule that varies according to your needs, such as every day, week, or month.

In addition, record all updates you make to your workstation by using a process called **configuration management** . Some companies log updates in a configuration management database to maintain compliance with lab policy. Every time you add or update software on your workstation, enter the change in the database or in a simple notebook with handwritten entries to document the change. A useful tool to run regularly is Belarc Advisor (www.belarc.com/free_download.html), which inventories applications, hardware, and system configurations.

A disaster recovery plan can also address how to restore a workstation you reconfigured for a specific investigation. For example, if you install a suite of applications, you might not have enough disk space for normal processing needs, so you could encounter problems during reconfigurations or even simple upgrades. The disaster recovery plan should outline how to uninstall software and delete any files the uninstall program hasn't removed so that you can restore your system to its original configuration.

For labs using high-end RAID servers or a private cloud (such as a Dell PowerEdge or Digital Intelligence FREDC), you need methods for restoring large data sets. These servers must have adequate data backup systems in case of a major failure of more than one drive. When planning a recovery procedure for RAID servers, consider whether the amount of downtime it takes to restore backup data is acceptable to the lab operation.

Planning for Equipment Upgrades

Risk management involves determining how much risk is acceptable for any process or operation, such as replacing equipment. Identify the equipment your lab depends on, and create a schedule to replace this equipment. Also, identify equipment that you can replace when it fails.

Computing components are designed to last 18 to 36 months in normal business operations, and new versions of OSs and applications that take up more disk space are released frequently. Therefore, systems periodically need more RAM, disk space, and processing speed. To keep your lab current with updates in hardware technology, schedule hardware replacements at least every 18 months and preferably every 12 months.

Building a Business Case for Developing a Forensics Lab

Before you can set up a digital forensics lab, you must enlist the support of managers and other team members. To do so, you build a **business case** , a plan you can use to sell your services to management or clients. In the business case, you justify acquiring newer and better resources to investigate digital forensics cases.

How you develop a business case depends on the organization you support. If you're the sole proprietor, creating a business case is fairly simple. If you need money to buy tools, you can save your money for the purchase or negotiate with your bank for a loan. For a public entity such as a police department, business requirements can change drastically because budgets are planned a year or more in advance. Public agency department managers present their budget proposals to upper management. If the proposal is approved, upper management makes money available to acquire resources outlined in the budget. Some public organizations might have other funds available that can be spent immediately for special needs. Managers can divert these funds for emergency or unforeseen needs.

Note

Like private-sector companies, police departments usually have to justify expenses to upper management. The important difference is that police departments don't always have to show cost recovery for the additional capabilities new resources and equipment offer.

Keep in mind that a private-sector business, especially a large corporation, is motivated by the need to make money. A business case should demonstrate how digital investigations could save money and avoid risks that can damage profits, such as by preventing litigation involving the company. For example, court decisions have defined viewing pornographic images in the workplace as creating a hostile environment for other employees, which is related to employee harassment and computer misuse. An employer is responsible for preventing and investigating harassment of employees and nonemployees associated with the workplace. A company is also liable if it doesn't actively prevent creating a hostile workplace by providing employee training and investigating allegations of computer misuse. A lawsuit, regardless of who wins, can cost an employer several hundred thousand dollars. In your business case, compare the cost of training and conducting digital investigations with the cost of a lawsuit.

The Internet makes it difficult for employers to provide a safe and secure environment for employees. In particular, employees can misuse free Web-based e-mail services. These free services give senders anonymity, making it possible for employees to send inappropriate e-mails, often in the form of sexual harassment. Because training rarely prevents this type of behavior, an employer needs to institute an investigation program that involves collecting network logs, such as proxy server logs, and examining computer disks to locate traces of message evidence. **Chapter 11** discusses e-mail abuse and using e-mail server and network logs.

Your business case should also show how digital investigations can improve profits, such as by protecting intellectual property, trade secrets, and future business plans. For example, when employees leave one company for a competing company, they can reveal vital competitive information to their new employers. Suppose a company called Skateboard International (SI) has invested research and development funds into a new product that improves the stability of

skateboards. Its main competitor is Better Skateboard; this company contacts Gwen Smith, a disgruntled SI employee, via e-mail and offers her a job. When Gwen leaves SI, she takes with her the plans for the new product. A few months later, Better Skateboard introduces a product similar to the skateboard Gwen had been researching at SI. SI recognizes that the new, improved skateboard is similar to the one Gwen had been developing and consults the noncompete agreement Gwen signed when she was hired. SI thinks that Better Skateboard might have gotten its new product from Gwen and suspects that Better Skateboard stole its trade secret and intellectual property.

SI could sue Better Skateboard and demand discovery on internal documents. Because Gwen and Better Skateboard corresponded via e-mail, a digital investigator needs to find data related to hiring and research engineering at Better Skateboard. Better Skateboard can also demand discovery on SI's research records to determine whether any discrepancies in product design could disprove the lawsuit. In this example, digital investigations can allow one company to generate revenue from a new product and prevent the other company from doing so. Information related to profit and loss makes a persuasive argument in a business case.

Preparing a Business Case for a Digital Forensics Lab

It's important to understand the need for planning in the creation and continued maintenance of a forensics lab. The reason is the constant cost-cutting efforts of upper management. Because of organizations' tendencies to look for ways to reduce costs, you must plan ahead to ensure that money is available for facilities, tools, supplies, and training for your forensics lab. The following sections describe some key elements for creating a digital forensics business case. It's a good idea to maintain a business case with annual updates.

Justification

Before you can start, you need to justify to the person controlling the budget the reason a lab is needed. This justification step requires asking the following questions:

- What type of digital investigation service is needed for your organization?
- Who are the potential customers for this service, and how will it be budgeted—as an internal operation (police department or company security department, for instance) or an external operation (a for-profit business venture)?
- How will you advertise your services to customers?
- What time-management techniques will you use?
- Where will the initial and sustaining budget for business operations come from?

No matter what type of organization you work for—a public agency or a private business—operating a digital forensics lab successfully requires constant efforts to market the lab's services to previous, current, and future customers and clients. By using marketing to attract new customers or clients, you can justify future budgets for the lab's operation and staff.

Budget Development

The budget needs to include all items described in the following sections. You must be as exact as possible when determining the true cost of these items. Making a mistake could cause delays and possible loss of the opportunity to start or improve your lab.

Facility Cost

For a new forensics lab, startup costs might take most of the budget. Depending on how large the lab is, you must determine first how much floor space is needed. As mentioned, a good rule of thumb is 150 square feet per person. This amount of space might seem a bit larger than necessary, but you need to factor in how much storage space is needed to preserve evidence and to have enough supplies in stock. Check with your organization's facility manager on per-

square-foot costs for your area or building. Here are some sample questions to get you started on calculating a budget:

- How many digital forensics examiners do you need?
- How much training does each examiner require per year, and what are the estimated costs?
- Do you need more than one lab?
- How many digital forensics examiners are going to use each lab? Is there a need to accommodate other nonexaminers temporarily to inspect recovered evidence?
- What are the costs to construct a secure lab?
- Is there a suitable room that can be converted into a lab?
- Does the designated room have enough electrical power and heating, ventilation, and air-conditioning (HVAC) systems?
- Does the designated room have existing phone lines and network cables? If not, how much would it cost to install these items?
- Is there an adequate lock on the designated room's door?
- What are the furniture costs?
- Do you need to install an alarm system?
- Are there any other facility costs, such as fees for janitorial services and facility maintenance services?
- If IT support is needed, how many hours of support are estimated?

Hardware Requirements

Determining the types of investigations and data that will be analyzed in your forensics lab dictates what hardware equipment you need. If your organization is using Intel-based PCs with Windows 10 or later, for instance, your forensic workstation should be a high-end Intel-based PC, too. For a small police department, determining the types of computers the public uses is more difficult. The diversity of a community's computer systems requires a police department to be more versatile in the tools needed to conduct investigations. To determine hardware budget needs, here are some questions to consider in your planning:

- What types of investigations and data recovery will be performed in the lab?
- How many investigations can be expected per month of operation?
- Are there any time-sensitive investigations that demand rapid analysis of disk data?
- How many drives (and what sizes) are needed to support a typical investigation?
- Do you need a high-speed backup system, such as tape backup or DVD burners?
- What's the predominant type of computer system you will investigate?
- What will you use to store digital evidence? How long do you need to store it?

Software Requirements

In the past few years, many more digital forensics tools have become available. For the private sector, the cost for these tools is about $1100 and up. For the public sector, many forensics software vendors offer discounts. However, just as you select hardware for your digital forensics lab to fit specific needs, you must determine what type of OSs and applications will be investigated and then make purchases accordingly. Keep in mind that the more you spend

on a forensics software package, the more function and flexibility you'll have. To determine software budget needs, here are some questions to consider in your planning:

- What types of OSs will be examined?
- For less popular, uncommon, or older OSs (such as Mac OS 9.x, OS/2, and CP/M), how often is there a need to investigate them?
- What are the minimum needs for forensics software tools? For example, how many copies of each tool are needed? How often is each tool used in an average week?
- What types of OSs are needed to conduct routine examinations?
- Is there a need for specialized software, such as QuickBooks, FreshBooks, Xero, or Sage 50c?
- Is there a budget to purchase more than one forensics software tool?
- Which disk-editing tool should be selected for general data analysis?

Miscellaneous Budget Needs

For this section of the budget, you need to brainstorm on other items, tools, and supplies to consider purchasing for the lab, from general office supplies to specific needs for daily operations. To determine miscellaneous budget needs, here are some questions to consider in your planning:

- Is there a need for errors and omission insurance for the lab's operation and staff?
- Do you need a budget for office supplies?

Approval and Acquisition

The approval and acquisition phase for a digital forensics lab is a management function. It's your responsibility to create a business case with a budget to present to upper management for approval. As part of the approval process, you should include a risk analysis describing how the lab will minimize the risk of litigation, which is a persuasive argument for supporting the lab. You also need to make an educated guess of how many investigations are anticipated and how long they will take on average. Remember that part of the approval process requires using negotiation skills to justify the business case. You might need to revise your case to get approval.

As part of the business case, acquisition planning requires researching different products to determine which one is the best and most cost effective. You need to contact several vendors' sales staff and design engineers to learn more about each product and service. Another factor to investigate is annual maintenance costs. You need to budget for this expense, too, so that you can get support if you run into problems during an investigation. An additional item to research from others in the profession is the vendor's maintenance history. Do other forensics labs use the same product, and have they had any problems getting support for problems they encounter?

Another consideration is vendors' pricing structures. Vendor pricing isn't based on the cost of creating CDs and DVDs and packaging them. Product prices are based on cost for development, testing, documentation support, shipping, and research and development for future improvements. In addition, vendors are for-profit organizations; they have investors to pay, too. Keep in mind that for vendors to be around next year to provide products and services for you, they need to make money.

Implementation

After approval and acquisition, you need to plan the implementation of facilities and tools. As part of your business case, describe how you plan to incorporate and install all approved

items. A timeline showing expected delivery or installation dates and expected completion dates must be included. You should also have a coordination plan for delivery dates and times for materials and tools. Include inspection of facility construction, equipment (including furniture and benches), and software tools in the schedule. Make sure you schedule inspection dates, too, to ensure that what you ordered arrived and is functional.

Acceptance Testing

Following the implementation scheduling and inspection, you need to develop an acceptance test plan for the digital forensics lab to make sure everything works correctly. When writing the acceptance test plan, make sure you include the following tasks:

- Inspect the facility to see whether it meets the security criteria for containing and controlling digital evidence.
- Test all communications, such as phone and network connections, to make sure they work as expected.
- Test all hardware to verify that it operates correctly; for example, test a computer to make sure it boots to Windows.
- Install and start all software tools; make sure all software can run on the computers and OSs you have in the lab.

Correction for Acceptance

The better you plan for your lab, the less likely you'll have problems. However, any lab operation has some problems during startup. Your business case must anticipate problems that can cause delays in lab production. In the business case, you need to develop contingencies to deal with system or facility failures. For example, devise workarounds for problems such as the wrong locks being installed on lab doors or electrical power needing additional filtering.

Production

After all essential corrections have been made, your digital forensics lab can then go into production. At this time, you carry out the lab operations and procedures that have been described in this chapter.

Tip

For additional information on how to write a business case, see www.sba.gov/tools/sba-learning-center/training/how-write-business-plan.

Chapter Summary

- A digital forensics lab is where you conduct investigations, store evidence, and do most of your work. You use the lab to house your instruments, current and legacy software, and forensic workstations. In general, you need a variety of digital forensics hardware and software.
- To continue a career in digital investigations and forensics analysis, you need to upgrade your skills through training. Several organizations offer training and certification programs for digital forensics that test you after you have successfully completed training. Some state and federal government agencies have also established certification programs that address the minimum skills needed to conduct digital investigations at different levels.
- Your lab facility must be physically secure so that evidence is not lost, corrupted, or destroyed.
- Police departments in major cities need a wide assortment of computing systems, including older, outdated technology. Most digital investigations in small, local police departments involve Windows PCs, Macintosh systems, and mobile devices. As a general rule, there should be at least one law enforcement digital investigator for every 250,000 people in a geographic region. Commercial services providing forensics analysis for other businesses can tailor their services to specific markets.
- A forensic workstation needs to have adequate memory, storage, and ports to deal with the common types of cases that come through your lab.
- Before you can set up a digital forensics lab, you must enlist the support of your managers and other team members by building a business case, a plan you can use to sell your services to management or clients. In the business case, you justify acquiring newer and better resources to investigate digital forensics cases.

Key Terms

ANSI-ASQ National Accreditation Board (ANAB)
business case
Certified Computer Examiner (CCE)
Certified Cyber Forensics Professional (CCFP)
Certified Forensic Computer Examiner (CFCE)
configuration management
digital forensics lab
High Tech Crime Network (HTCN)
risk management
secure facility
TEMPEST
Uniform Crime Report

Review Questions

1. An employer can be held liable for e-mail harassment. True or False?
2. Building a business case can involve which of the following?
   a. Procedures for gathering evidence
   b. Testing software

c. Protecting trade secrets

d. All of the above

3. The ANAB mandates the procedures established for a digital forensics lab. True or False?

4. The manager of a digital forensics lab is responsible for which of the following? (Choose all that apply.)

a. Making necessary changes in lab procedures and software

b. Ensuring that staff members have enough training to do the job

c. Knowing the lab objectives

d. None of the above

5. To determine the types of operating systems needed in your lab, list two sources of information you could use.

6. What items should your business plan include?

7. List two popular certification programs for digital forensics.

8. Why is physical security so critical for digital forensics labs?

9. If a visitor to your digital forensics lab is a personal friend, it's not necessary to have him or her sign the visitor's log. True or False?

10. What three items should you research before enlisting in a certification program?

11. Large digital forensics labs should have at least ___ exits.

12. Typically, a(n) ___ lab has a separate storage area or room for evidence.

13. Digital forensics facilities always have windows. True or False?

14. Evidence storage containers should have several master keys. True or False?

15. A forensic workstation should always have a direct broadband connection to the Internet. True or False?

16. Which organization provides good information on safe storage containers?

17. Which organization has guidelines on how to operate a digital forensics lab?

18. What term refers to labs constructed to shield EMR emissions?

Hands-On Projects

Hands-On Project 2-1.

You have just been hired to perform digital investigations and forensics analysis for a company. You find that no policies, processes, or procedures are currently in place. Do an Internet search to find information, and then create a policy and processes document to provide the structure necessary for your lab environment. Be sure to cite your online sources.

Hands-On Project 2-2.

As mentioned, new forensics certifications are offered constantly. Research certifications online and find one not discussed in this chapter. Write a short paper stating what organization offers the certification, who endorses the certification, how long the organization has been in business, and so forth.

Hands-On Project 2-3.

Physical security of a lab must always be maintained. In your classroom lab, get permission to make observations at different times of the day when classes are and aren't in session. Record how many people go in and out during a period. Do you know all the people or can you identify them? Are they all students or faculty? Who monitors the lab when classes aren't in session? Are the rooms locked? How often are things stolen from the labs? Write one to two pages about your observations. If it were a digital forensics lab, what changes would you have to make?

Hands-On Project 2-4.

Write a disaster recovery plan of not more than three pages for a fictitious company's digital forensics lab. Include backup schedules, note the programs and OS installed on each machine, and list other information you would have to recover after a disaster. You should also note where the original disks and backups are located.

Hands-On Project 2-5.

A law firm has hired you to assist with digital evidence cases involving divorces. The main evidence consists of e-mail, spreadsheets, and documents. Before hiring you, the firm used an outside group to conduct investigations. You have to decide what equipment and software to purchase. What would you do to build a business plan that would be approved?

Case Projects

Case Project 2-1.

Your manager informs you that she needs to prepare for next year's budget and wants you to create a list of hardware and software for two new workstations and one laptop, all Windows computers. Conduct Internet research, and create a spreadsheet listing hardware and software for each computer with estimated costs. For the computers, include specifications such as processor speeds, RAM, internal disk storage, and type of monitor. For software, include an OS, an office suite, and two digital forensics tools.

Case Project 2-2.

A new version of Windows has been released. What do you need to do to be ready in 6 to 10 months when you encounter cases involving the new OS? Include research, user groups, and others you need to contact. Write a one-page paper on the procedures you should use.

Case Project 2-3.

Research your state, province, or neighboring states and provinces to determine whether digital forensics examiners require licenses. Write a one-page summary of the licensing requirements in the region you selected. If your region doesn't have any licensing requirements, research one of the following states: Michigan, Texas, or Georgia.

Case Project 2-4.

Your manager informs you that your company is going to have a new digital forensics lab built. It will have space for additional computers to perform password cracking. You're asked to research hardware and software requirements for this task and write a one-page memo describing recommendations for a password-cracking computer running multiple GPUs in a cluster of other systems with multiple GPUs. State what OS is recommended for these clusters' systems.

Chapter 3. Data Acquisition

After reading this chapter and completing the exercises, you will be able to:

- List digital evidence storage formats
- Explain ways to determine the best acquisition method
- Describe contingency planning for data acquisitions
- Explain how to use acquisition tools
- Describe how to validate data acquisitions
- Describe RAID acquisition methods
- Explain how to use remote network acquisition tools
- List other forensics tools available for data acquisitions

Data acquisition is the process of copying data. For digital forensics, it's the task of collecting digital evidence from electronic media. There are two types of data acquisition: static acquisitions and live acquisitions. In this chapter, you learn how to perform static acquisitions from magnetic disk media and flash drives. In **Chapter 12**, you learn how to forensically acquire digital evidence from solid-state devices, typically found in smartphones and tablets.

Because of the use of whole disk encryption, data acquisitions are shifting toward live acquisitions with newer operating systems (OSs). In addition to encryption concerns, collecting any data that's active in a suspect's computer RAM is becoming more important to digital investigations. Techniques for acquiring live disk and RAM data are covered in **Chapter 10**. The processes and data integrity requirements for static and live acquisitions are similar, in that static acquisitions capture data that's not accessed by other processes that can change. With live acquisitions, file metadata, such as date and time values, changes when read by an acquisition tool. With static acquisitions, if you have preserved the original media, making a second static acquisition should produce the same results. The data on the original disk isn't altered, no matter how many times an acquisition is done. Making a second live acquisition while a computer is running collects new data because of dynamic changes in the OS.

Your goal when acquiring data for a static acquisition is to preserve the digital evidence. Many times, you have only one chance to create a reliable copy of disk evidence with a data acquisition tool. Although these tools are generally dependable, you should still take steps to make sure you acquire an image that can be verified. In addition, failures can and do occur, so you should learn how to use several acquisition tools and methods; you work with a few different tools in this chapter. Other data acquisition tools that work in Windows, MS-DOS 6.22, and Linux are described briefly in the last section, but the list of vendors and methods is by no means conclusive. You should always search for newer and better tools to ensure the integrity of your forensics acquisitions.

Note

For additional information on older acquisition methods and tools, see Appendix D. You can perform most digital evidence acquisitions for your investigations with a combination of the tools discussed in this chapter.

Understanding Storage Formats for Digital Evidence

The data a forensics acquisition tool collects is stored as an image file, typically in an open-source or proprietary format. Each vendor has unique features, so several different proprietary formats are available. Depending on the proprietary format, many forensics analysis tools can read other vendors' formatted acquisitions. Many acquisition tools create a disk-to-image file in an older open-source format, known as raw, as well as their own proprietary formats. The new open-source format, Advanced Forensic Format (AFF), is gaining recognition from some forensics examiners.

Each data acquisition format has unique features along with advantages and disadvantages. The following sections summarize each format to help you choose which one to use.

Note

For additional information on digital evidence handling and documenting, see ISO/IEC 27037: 2012, www.iso.org/iso/catalogue_detail?csnumber=44381. Downloading ISO documents requires paying a fee, so you might check with a college or public library about getting a copy.

Raw Format

In the past, there was only one practical way of copying data for the purpose of evidence preservation and examination. Examiners performed a bit-by-bit copy from one disk to another disk the same size or larger. As a practical way to preserve digital evidence, vendors (and some OS utilities, such as the Linux/UNIX dd command) made it possible to write bit-stream data to files. This copy technique creates simple sequential flat files of a suspect drive or data set. The output of these flat files is referred to as a **raw format** . This format has unique advantages and disadvantages to consider when selecting an acquisition format.

The advantages of the raw format are fast data transfers and the capability to ignore minor data read errors on the source drive. In addition, most forensics tools can read the raw format, making it a universal acquisition format for most tools. One disadvantage of the raw format is that it requires as much storage space as the original disk or data set. Another disadvantage is that some raw format tools, typically freeware versions, might not collect marginal (bad) sectors on the source drive, meaning they have a low threshold of retry reads on weak media spots on a drive. Many commercial tools have a much higher threshold of retry reads to ensure that all data is collected.

Several commercial acquisition tools can produce raw format acquisitions and typically perform a validation check by using Cyclic Redundancy Check (CRC32), Message Digest 5 (MD5), and Secure Hash Algorithm (SHA-1 or later) hashing functions. These validation checks, however, usually create a separate file containing the hash value.

Proprietary Formats

Most commercial forensics tools have their own formats for collecting digital evidence. Proprietary formats typically offer several features that complement the vendor's analysis tool, such as the following:

- The option to compress or not compress image files of a suspect drive, thus saving space on the target drive
- The capability to split an image into smaller segmented files for archiving purposes, such as to CDs or DVDs, with data integrity checks integrated into each segment
- The capability to integrate metadata into the image file, such as date and time of the acquisition, hash value (for self-authentication) of the original disk or medium, investigator or examiner name, and comments or case details

Note

Forensics examiners have several ways of referring to copying evidence data to files: bit-stream copy, bit-stream image, image, mirror, and sector copy, to name a few. For the purposes of this book, "image" is generally used to refer to all forensics acquisitions saved to a data file.

One major disadvantage of proprietary format acquisitions is the inability to share an image between different vendors' computer forensics analysis tools. For example, the ILookIX imaging tool IXImager (www.perlustro.com/solutions/e-forensics/iximager) produces three proprietary formats—IDIF, IRBF, and IEIF—that can be read only by ILookIX (see www.perlustro.com for additional information on ILookIX).

Another problem with proprietary and raw formats is a file size limitation for each segmented volume. Typically, proprietary format tools produce a segmented file of 650 MB. The file size can be adjusted up or down, with a maximum file size per segment of no more than 2 GB. Most proprietary format tools go up to only 2 GB because many examiners use target drives formatted as FAT, which has a file size limit of 2 GB.

Of all the proprietary formats for image acquisitions, the Expert Witness Compression format is currently the unofficial standard. This format, the default for Guidance Software EnCase, produces both compressed and uncompressed image files. These files (or volumes) write an extension starting with .e01 and increment it for each additional segmented image volume.

Several forensics analysis tools can generate generic versions of the Expert Witness Compression format and analyze it, including X-Ways Forensics, AccessData Forensic Toolkit (FTK), Belkasoft, and SMART. For more information on the Expert Witness Compression format, see http://asrdata.com/E01-format.html.

Advanced Forensic Format

Dr. Simson L. Garfinkel developed an open-source acquisition format called **Advanced Forensic Format (AFF)** . This format has the following design goals:

- Capable of producing compressed or uncompressed image files
- No size restriction for disk-to-image files
- Space in the image file or segmented files for metadata
- Simple design with extensibility
- Open source for multiple computing platforms and OSs
- Internal consistency checks for self-authentication

File extensions include .afd for segmented image files and .afm for AFF metadata. Because AFF is open source, digital forensics vendors have no implementation restrictions on this format. For more information on AFF, see www.afflib.sourceforge.net and www.basistech.com/wp-content/uploads/datasheets/Digital-Forensics-Toolsets-EN.pdf.

Tip

For more information on forensics acquisition file formats, see www.sleuthkit.org/informer, issues #19 and #23.

Determining the Best Acquisition Method

As mentioned, there are two types of acquisitions: **static acquisitions** and **live acquisitions** . Typically, a static acquisition is done on a computer seized during a police raid, for example. If the computer has an encrypted drive, a live acquisition is done if the password or passphrase is available—meaning the computer is powered on and has been logged on to by the suspect. Static acquisitions are always the preferred way to collect digital evidence. However, they do have limitations in some situations, such as an encrypted drive that's readable only when the computer is powered on or a computer that's accessible only over a network. Some solutions can help decrypt a drive that has been encrypted with whole disk encryption, such as Elcomsoft Forensic Disk Decryptor (www.elcomsoft.com/efdd.html).

Note

In **Chapter 11**, you learn how to perform live acquisitions, including data collection of digital media and dynamic/volatile memory (RAM) on a computing system.

For both types of acquisitions, data can be collected with four methods: creating a disk-to-image file, creating a disk-to-disk copy, creating a logical disk-to-disk or disk-to-data file, or creating a sparse copy of a folder or file. Determining the best acquisition method depends on the circumstances of the investigation.

Note

See ISO/IEC 27037: 2012 (section 5.4.4 Acquisition and section 6.5 Use reasonable care) for additional discussions on when to perform sparse acquisitions.

Creating a disk-to-image file is the most common method and offers the most flexibility for your investigation. With this method, you can make one or many copies of a suspect drive. These copies are bit-for-bit replications of the original drive. In addition, you can use many commercial forensics tools to read the most common types of disk-to-image files you create. These programs read the disk-to-image file as though it were the original disk. Older MS-DOS tools can only read data from a drive. To use MS-DOS tools, you have to duplicate the original drive to perform the analysis. GUI programs save time and disk resources because they can read and interpret directly from the disk-to-image file of a copied drive.

Sometimes you can't make a disk-to-image file because of hardware or software errors or incompatibilities. This problem is more common when you have to acquire older drives. For these drives, you might have to create a disk-to-disk copy of the suspect drive. Several imaging tools can copy data exactly from an older disk to a newer disk. These programs can adjust the target disk's geometry (its cylinder, head, and track configuration) so that the copied data matches the original suspect drive. These imaging tools include EnCase and X-Ways Forensics. See the vendors' manuals for instructions on using these tools for disk-to-disk copying.

Tip

For more information on current and older drives, see www.t13.org.

Collecting evidence from a large drive can take several hours. If your time is limited, consider using a logical acquisition or sparse acquisition data copy method. A **logical acquisition** captures only specific files of interest to the case or specific types of files. A **sparse acquisition** is similar but also collects fragments of unallocated (deleted) data; use this method only when you don't need to examine the entire drive. An example of a logical acquisition is an e-mail investigation that requires collecting only Outlook .pst or .ost files. Another example is collecting only specific records from a large RAID server. If you have to recover data from a RAID or storage area network (SAN) server with several exabytes (EB) or more of data storage, the logical method might be the only way you can acquire the evidence. In e-discovery for the purpose of litigation, a logical acquisition is becoming the preferred method, especially with large data storage systems.

To determine which acquisition method to use for an investigation, consider the size of the source (suspect) disk, whether you can retain the source disk as evidence or must return it to the owner, how much time you have to perform the acquisition, and where the evidence is located.

If the source disk is very large, such as 4 terabytes (TB) or more, make sure you have a target disk that can store a disk-to-image file of the large disk. If you don't have a target disk of comparable size, review alternatives for reducing the size of data to create a verifiable copy of the suspect drive. Older Microsoft disk compression tools, such as DoubleSpace or DriveSpace, eliminate only slack disk space between files. Other compression methods use an algorithm to reduce file size. Popular archiving tools, such as PKZip, WinZip, and WinRAR, use an algorithm referred to as "lossless compression." Compression algorithms for graphics files use what's called "lossy compression," which can change data. For example, lossy compression is used with .jpeg files to reduce file size and doesn't affect image quality when the file is restored and viewed. Because lossy compression alters original data, however, it isn't used for forensics acquisitions. Both compression methods are discussed in more detail in Chapter 8.

Most imaging tools have an option to use lossless compression to save disk space, which means the target drive doesn't have to be as large as the suspect drive. For example, if you're examining a 3 TB SATA drive, you might be able to use lossless compression to create the disk-to-image file on a 2 TB target drive. Image files can be reduced by as much as 50% of the original. If the suspect drive already contains several zip files, however, the imaging tool can't compress them any further. This is because zip files have already been compressed, so any additional compression results in very little size reduction. For additional information on lossless compression, see www.data-compression.com/lossless.shtml or www.cise.ufl.edu/~sahni/papers/encycloimage.pdf.

An easy way to test lossless compression is to perform an MD5 or SHA-1 hash on a file before and after it's compressed. If the compression is done correctly, both versions have the same hash value. If the hashes don't match, that means something corrupted the compressed file, such as a hardware or software error. As an added precaution, perform two separate hashes with different algorithms, such as MD5 and SHA-1. This step isn't mandatory; however, it's a good way to establish that nothing has changed during data processing.

If you can't retain the original evidence drive and must return it to the owner, as in a discovery demand for a civil litigation case, check with the requester (your lawyer or supervisor, for example), and ask whether a logical acquisition is acceptable. If not, you have to refer the matter back to the requester. When performing an acquisition under these conditions, make sure you have a good copy because most discovery demands give you only one chance to capture data. In addition, make sure you have a reliable forensics tool that you know how to use.

Contingency Planning for Image Acquisitions

Because you're working with digital evidence, you must take precautions to protect it from loss. You should also make contingency plans in case software or hardware doesn't work or you encounter a failure during an acquisition. The most common and time-consuming technique for preserving evidence is creating a duplicate of your disk-to-image file. Many digital investigators don't make duplicates of their evidence because they don't have enough time or resources to make a second image. However, if the first copy doesn't work correctly, having a duplicate is worth the effort and resources. Be sure you take steps to minimize the risk of failure in your investigation.

As a standard practice, make at least two images of the digital evidence you collect. If you have more than one imaging tool, such as FTK Imager Lite and X-Ways Forensics, make the first copy with one tool and the second copy with the other tool. Different acquisition tools use different methods to copy data, and one tool might, for example, make more attempts to copy corrupted areas of a drive. So using more than one tool can be helpful in making sure data has been copied correctly.

If you have only one tool, however, consider making two images of the drive with the same tool, especially for critical investigations. With many tools, you can make one copy with no

compression and compress the other copy. Remember that Murphy's Law applies to digital forensics, too: If anything can go wrong, it will.

Some acquisition tools don't copy data in the **host protected area (HPA)** of a disk drive. Check the vendor's documentation to see whether its tool can copy a drive's HPA. If not, consider using a hardware acquisition tool that can access the drive at the BIOS level, such as Belkasoft or ILookIX IXImager, with a write-blocker, Image MASSter Solo, or X-Ways Replica. These tools can read a disk's HPA.

Microsoft has added **whole disk encryption** with BitLocker to its newer operating systems, such as Windows Vista, 7, 8, and 10, which makes performing static acquisitions more difficult. (Several other third-party whole disk encryption tools are available, and you should be familiar with as many as possible.) As part of contingency planning, you must be prepared to deal with encrypted drives. A static acquisition on most whole disk—encrypted drives currently involves decrypting the drives, which requires the user's cooperation in providing the decryption key. Most whole disk encryption tools at least have a manual process for decrypting data, which is converting the encrypted disk to an unencrypted disk. This process can take several hours, depending on the disk size. One good thing about encryption is that data isn't altered, in that free and slack space aren't changed. The biggest concern with whole disk encryption is getting the decryption key—that is, the password or code used to access encrypted data. If you can recover the whole disk key with tools such as Elcomsoft Forensic Disk Decryptor, mentioned previously, you need to learn how to use it to decrypt the drive. In criminal investigations, this might be impossible because if a disk contains evidence supporting the crime, a suspect has a strong motivation not to supply the decryption key.

Note

Researchers at Princeton University have produced a technique to recover passwords and passphrases from RAM; for more information, see www.usenix.org/legacy/event/sec08/tech/full_papers/halderman/halderman.pdf or https://jhalderm.com/pub/papers/coldboot-cacm09.pdf.

Using Acquisition Tools

Many forensics software vendors have developed acquisition tools that run in Windows. These tools make acquiring evidence from a suspect drive more convenient, especially when you use them with hot-swappable devices, such as USB-3, FireWire 1394A and 1394B, or SATA, to connect disks to your workstation.

Using acquisition tools with current OSs, such as Windows and Linux, has some drawbacks, however. Because Windows and Linux can easily contaminate an evidence drive when it's mounted, you must protect it with a well-tested write-blocking hardware device. The automatic mounting process updates boot files by changing metadata, such as the most recent access time. (**Chapter 6** discusses write-blocking devices in more detail.) In addition, some countries haven't yet accepted the use of write-blocking devices for data acquisitions. Check with your legal counsel for evidence standards in your community or country.

Note

Although many digital forensics vendors have improved their acquisition tools, some older Windows and Linux tools (such as the dd or dcfldd commands) can't acquire data from a disk's HPA.

Mini-WinFE Boot CDs and USB Drives

Accessing a disk drive directly might not be practical for a forensics acquisition. For example, a laptop's design could make removing the disk drive to mount it on a write-blocker difficult, or you might not have the right connector for a drive. In these situations, a forensic boot CD/DVD or USB drive gives you a way to acquire data from a suspect computer and write-protect the disk drive. These forensic boot discs or drives can be Windows or Linux.

One forensically sound Windows boot utility is Mini-WinFE. It enables you to build a Windows forensic boot CD/DVD or USB drive with a modification in its Windows Registry file so that connected drives are mounted as read-only. Before booting a suspect's computer with Mini-WinFE, you need to connect your target drive, such as a USB drive. After Mini-WinFE is booted, you can list all connected drives and alter your target USB drive to read-write mode so that you can run an acquisition program.

To create your own Mini-WinFE boot CD or USB drive, review the documentation and download the software from the following Web sites:

- For an overview of WinFE, see http://brettshavers.cc/index.php/brettsblog/tags/tag/winfe. For the latest information and instructions, review the Downloads and Using WinFE menus.
- For download instructions on Mini-WinFE, see http://brettshavers.cc/index.php/brettsblog/entry/mini-winfe-and-xwf.
- Another download site for Mini-WinFE is http://reboot.pro/files/file/375-mini-winfe.
- For complete instructions on Mini-WinFE, see www.forensicfocus.com/downloads/WinFE.pdf.

In addition, you need a Windows installation DVD (version 8 or later) and FTK Imager Lite or X-Ways Forensics installed on your workstation. Follow the instructions in the preceding Web sites to create the Mini-WinFE ISO file and then burn it to CD or transfer it to a USB drive. If you want to use a USB drive, you need a tool to transfer an ISO image to a USB drive. A freeware tool called ISO to USB is available at www.isotousb.com.

Acquiring Data with a Linux Boot CD

The Linux OS has many features that are applicable to digital forensics, especially data acquisitions. One unique feature of older Linux versions is that it can access a drive that isn't mounted. Physical access for the purpose of reading data can be done on a connected media device, such as a disk drive, a USB drive, or other storage devices. In Windows OSs and newer Linux kernels, when you connect a drive via USB, FireWire, external SATA, or even internal PATA or SATA controllers, both OSs automatically mount and access the drive. On Windows drives, an acquisition workstation can access and alter data in the Recycle Bin; on Linux drives, the workstation most likely alters metadata, such as mount point configurations for an Ext3 or later drive. If you need to acquire a USB drive that doesn't have a write-lock switch, use one of the forensic Linux Live CDs (discussed in the next section) to access the device.

Caution ⚠

Use caution when working with newer Linux distributions with KDE or Gnome GUIs. Many newer distributions mount most media devices automatically. If you're using a nonforensic Linux distribution, you should test it before using it on actual evidence to see how it handles attached storage devices. If in doubt, always use a physical write-blocker for an acquisition from Linux.

Using Linux Live CD Distributions

Several Linux distributions, such as Ubuntu, openSUSE, Arch Linux, Fedora, and Slackware, provide ISO images that can be burned to a CD or DVD. They're called "Linux Live CDs." Most of these Linux distributions are for Linux OS recovery, not for digital forensics acquisition and analysis. For a list of the most current Linux Live CDs, see https://livecdlist.com/.

A few Linux ISO images are designed specifically for digital forensics, however. These images contain additional utilities that aren't typically installed in normal Linux distributions. They're also configured not to mount, or to mount as read-only, any connected storage media, such as USB drives. This feature protects the media's integrity for the purpose of acquiring and analyzing data. To access media, you have to give specific instructions to the Live CD boot session through a GUI utility or a shell command prompt. Mounting drives from a shell gives you more control over them. See the man page for the mount command (by typing man mount at the shell prompt) to learn what options are available for your Linux distribution.

Tip

The man command displays pages from the online help manual for information on Linux commands and their options.

Linux can read data from a physical device without having to mount it. As a usual practice, don't mount a suspect media device as a precaution against any writes to it. Later in this section, you learn how to make a forensics acquisition in Linux without mounting the device.

The following are some well-designed Linux Live CDs for digital forensics:

- Penguin Sleuth Kit (www.linux-forensics.com or https://sourceforge.net/projects/psk/?source=directory)
- CAINE (www.caine-live.net)
- Deft (www.deftlinux.net)
- Kali Linux (www.kali.org), previously known as BackTrack (www.backtrack-linux.org/wiki/index.php/Forensics_Boot)
- Knoppix (www.knopper.net/knoppix/index-en.html)
- SANS Investigate Forensic Toolkit (SIFT; http://computer-forensics.sans.org/community/downloads)

You can download these ISO images to any computer, including a Windows system, and then burn them to CD/DVD with burner software, such as Roxio or Nero. Creating a bootable image from an ISO file is different from copying data or music files to a CD or DVD. If you aren't familiar with how to do it, see the Help menu in your burner software for instructions on creating a bootable CD or DVD. For example, Roxio Creator Classic and Nero Express have a Bootable CD or DVD option. An alternative is using a USB drive instead of a CD or DVD. For this option, you need a tool such as ISO to USB, mentioned previously (or another tool for transferring an ISO image to a USB drive).

Note

For an alternative Windows-based USB boot drive, see http://osforensics.com/tools/write-usb-images.html.

After creating a Linux Live CD, test it on your workstation. Remember to check your workstation's BIOS to see whether it boots first from the CD or DVD on the system. To test the Live CD, simply place it in the CD or DVD drive and reboot your system. If successful, Linux loads into your computer's memory, and a common GUI for Linux is displayed. If you have

problems with the video display on your workstation, try another computer with a different video card. No one Live CD distribution has all video drivers. Linux Live CDs load the OS into a computer's RAM, so performance can be affected when you're using GUI tools. The following sections explain how to use Linux to make forensically sound data acquisitions.

Preparing a Target Drive for Acquisition in Linux

The Linux OS has many tools you can use to modify non-Linux file systems. Current Linux distributions can create Microsoft FAT and NTFS partition tables. Linux kernel version 2.6.17.7 and earlier can format and read only the FAT file system, although an NTFS driver, NTFS-3G, is available that allows Linux to mount and write data only to NTFS partitions. You can download this driver from http://sourceforge.net/projects/ntfs-3g, where you can also find information about NTFS and instructions for installing the driver. For information on macOS file systems and acquisitions, see Chapter 7.

In this section, you learn how to partition and format a Microsoft FAT drive from Linux so that you don't have to switch OSs or computers to prepare a FAT target disk. If you have a previously used target drive, you can use the following procedure to format it as a FAT32 drive. After you make the acquisition, you can then transfer the FAT disk to a Windows system to use a Windows analysis tool.

Note

When preparing a drive to be used on a Linux system for forensics acquisition or analysis, do it in a separate boot session with no suspect drive attached.

Tip

Linux/UNIX commands are case sensitive, so make sure you type commands exactly as shown in this section's steps.

Assuming you have a functioning Linux computer or one running with a Linux Live CD, perform the following steps from a shell prompt:

Note

Depending on which version and distribution of Linux you use, your screen prompts might be slightly different from those shown in this section.

1. First, boot Linux on your computer.
2. Connect the USB, FireWire, or SATA external drive to the Linux computer and power it on.
3. If a shell window isn't already open, start one.
4. At the shell prompt, type **su** and press **Enter** to log in as the superuser (root). Then type the root password and press **Enter**.

   Note

   If you're using one of the Live CDs listed previously, these distributions are typically already in superuser (root) mode, so there's no need to use the su command. Other Linux Live CDs might have no password set and simply require pressing Enter.

5. To list the current disk devices connected to the computer, type **fdisk -l** (lowercase L) and press **Enter**. You should see output similar to the following:

Note

Linux lists all IDE (also known as PATA) drives as hda, hdb, and so on. All SCSI, SATA, FireWire, and USB-connected drives are listed as sda, sdb, and so forth.

```
Disk /dev/hda: 40.0 GB, 40007761920 bytes
255 heads, 63 sectors/track, 4864 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Device Boot    Start    End     Blocks    Id  System
/dev/hda1  *     1      13     104391     83  Linux
/dev/hda2       14     4864   38965657+  8e  Linux LVM
Disk /dev/sda: 6448 MB, 6448619520 bytes
199 heads, 62 sectors/track, 1020 cylinders
Units = cylinders of 12338 * 512 = 6317056 bytes
Disk /dev/sda doesn't contain a valid partition table
```

Note

In the preceding output, the /dev/sda device has no partition listed. These steps show how to create a Microsoft FAT partition on this disk. If there's a partition on this drive, it can be deleted with the Linux fdisk utility. For additional information on fdisk, refer to the man page.

6. Type **fdisk/dev/sda** and press **Enter** to partition the disk drive as a FAT file system. You should see output similar to the following:

```
Welcome to fdisk (util-linux 2.21.2).
Changes will remain in memory only, until you decide
to write them.
Be careful before using the write command.
Command (m for help): m
```

7. Display fdisk menu options by typing **m** and pressing **Enter**. You should see output similar to the following:

```
Command action
a   toggle a bootable flag
b   edit bsd disklabel
c   toggle the dos compatibility flag
d   delete a partition
l   list known partition types
m   print this menu
n   add a new partition
o   create a new empty DOS partition table
p   print the partition table
q   quit without saving changes
s   create a new empty Sun disk label
t   change a partition's system id
u   change display/entry units
v   verify the partition table
w   write table to disk and exit
x   extra functionality (experts only)
```

8. Determine whether there are any partitions on /dev/sda by typing **p** and pressing **Enter**. You should see output similar to the following:

```
Disk /dev/sda: 6448 MB, 6448619520 bytes
199 heads, 62 sectors/track, 1020 cylinders
Units = cylinders of 12338 * 512 = 6317056 bytes

Device Boot  Start End   Blocks  Id  System
/dev/sda1    1     1020  6292349 b   W95 FAT32
```

Note

In this example, the disk has no previously configured partitions. If it did, there would be data under each column heading describing each partition's configuration.

9. Next, you create a new primary partition on /dev/sda. To use the defaults and select the entire drive, type **n** and press **Enter**. To create a primary partition table, type **p** and press **Enter**, and then type **1** (the numeral) to select the first partition and press **Enter**. At the remaining prompts, press **Enter**. Your output should be similar to the following:

```
Command action
e   extended
p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-1020, default 1):
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-1020,
default 1020):
Using default value 1020
```

Note

In Linux, the first logical partition created after the primary and extended partitions is numbered 5; any additional logical partitions are numbered 6, 7, and so on. For example, the C partition is typically /dev/hda1, and the D partition is /dev/hda2.

10. List the newly defined partitions by typing **p** and pressing **Enter**, which produces the following output:

```
Disk /dev/sda: 6448 MB, 6448619520 bytes
199 heads, 62 sectors/track, 1020 cylinders
Units = cylinders of 12338 * 512 = 6317056 bytes

Device Boot     Start     End     Blocks     Id  System
/dev/sda1         1       1020    6292349    83  Linux
```

11. To list the menu again so that you can select the change partition ID, type **m** and press **Enter**. You should see output similar to the following:

```
Command action
a   toggle a bootable flag
b   edit bsd disk label
c   toggle the dos compatibility flag
d   delete a partition
l   list known partition types
m   print this menu
n   add a new partition
o   create a new empty DOS partition table
p   print the partition table
q   quit without saving changes
s   create a new empty Sun disk label
t   change a partition's system id
u   change display/entry units
v   verify the partition table
w   write table to disk and exit
x   extra functionality (experts only)
```

12. To change the newly created partition to the Windows 95 FAT32 file system, first type **t** and press **Enter**, which produces the following output:

```
Selected partition 1
Hex code (type L to list codes):
```

13. List available file systems and their code values by typing **l** (lowercase L) and pressing **Enter**. You should see output similar to what's shown in Figure 3-1.

Figure 3-1.

```
Command (m for help): l

 0 Empty            24 NEC DOS         81 Minix / old Lin    bf Solaris
 1 FAT12            27 Hidden NTFS Win 82 Linux swap / So    c1 DRDOS/sec (FAT-
 2 XENIX root       39 Plan 9          83 Linux              c4 DRDOS/sec (FAT-
 3 XENIX usr        3c PartitionMagic  84 OS/2 hidden C:     c6 DRDOS/sec (FAT-
 4 FAT16 <32M       40 Venix 80286     85 Linux extended     c7 Syrinx
 5 Extended         41 PPC PReP Boot   86 NTFS volume set    da Non-FS data
 6 FAT16            42 SFS             87 NTFS volume set    db CP/M / CTOS / .
 7 HPFS/NTFS/exFAT  4d QNX4.x          88 Linux plaintext    de Dell Utility
 8 AIX              4e QNX4.x 2nd part 8e Linux LVM          df BootIt
 9 AIX bootable     4f QNX4.x 3rd part 93 Amoeba             e1 DOS access
 a OS/2 Boot Manag  50 OnTrack DM      94 Amoeba BBT         e3 DOS R/O
 b W95 FAT32        51 OnTrack DM6 Aux 9f BSD/OS             e4 SpeedStor
 c W95 FAT32 (LBA)  52 CP/M            a0 IBM Thinkpad hi    eb BeOS fs
 e W95 FAT16 (LBA)  53 OnTrack DM6 Aux a5 FreeBSD            ee GPT
 f W95 Ext'd (LBA)  54 OnTrackDM6      a6 OpenBSD            ef EFI (FAT-12/16/
10 OPUS             55 EZ-Drive        a7 NeXTSTEP           f0 Linux/PA-RISC b
11 Hidden FAT12     56 Golden Bow      a8 Darwin UFS         f1 SpeedStor
12 Compaq diagnost  5c Priam Edisk     a9 NetBSD             f4 SpeedStor
14 Hidden FAT16 <3  61 SpeedStor       ab Darwin boot        f2 DOS secondary
16 Hidden FAT16     63 GNU HURD or Sys af HFS / HFS+         fb VMware VMFS
17 Hidden HPFS/NTF  64 Novell Netware  b7 BSDI fs            fc VMware VMKCORE
18 AST SmartSleep   65 Novell Netware  b8 BSDI swap          fd Linux raid auto
1b Hidden W95 FAT3  70 DiskSecure Mult bb Boot Wizard hid    fe LANstep
1c Hidden W95 FAT3  75 PC/IX           be Solaris boot       ff BBT
1e Hidden W95 FAT1  80 Old Minix

Command (m for help):
```

Source: Linux Foundation.

Listing code values for available file systems

14. Change the newly created partition to the Windows 95 FAT32 file system by typing **c** and pressing **Enter**. Your output should look similar to the following:

```
Changed system type of partition 1 to c (W95 FAT32 (LBA))
```

15. To display partitions of the newly changed drive, type **p** and press **Enter**, which produces the following output:

```
Disk /dev/sda: 6448 MB, 6448619520 bytes
199 heads, 62 sectors/track, 1020 cylinders
Units = cylinders of 12338 * 512 = 6317056 bytes

Device Boot    Start       End    Blocks   Id  System
/dev/sda1        1         1020   6292349   c  W95 FAT32 (LBA)
```

16. Save (write) the newly created partition to the /dev/sda drive by typing **w** and pressing **Enter**. Your output should look similar to the following:

```
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: If you have created or modified any DOS 6.x partitions,
please see the fdisk manual page for additional information.
```

Note

Fdisk exits back to the shell prompt after updating the partition table on the /dev/sda drive.

17. Show the known drives connected to your computer by typing **fdisk -l** and pressing **Enter**, which produces the following output:

```
Disk /dev/hda: 40.0 GB, 40007761920 bytes
255 heads, 63 sectors/track, 4864 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

Device Boot    Start    End    Blocks     Id   System
/dev/hda1   *    1       13    104391     83   Linux
/dev/hda2       14     4864   38965657+  8e   Linux LVM

Disk /dev/sda: 6448 MB, 6448619520 bytes
199 heads, 62 sectors/track, 1020 cylinders
Units = cylinders of 12338 * 512 = 6317056 bytes

Device Boot    Start   End    Blocks   Id   System
/dev/sda1        1     1020  6292349   b   W95 FAT32
```

18. To format a FAT file system from Linux, type **mkfs.msdos -vF32 /dev/sda1** and press **Enter**, which produces the following output:

Note

If your Linux distribution is missing the mkfs.msdos command, download and install your distribution's dosfstools package. To find these files, search for mkfs.msdos Fedora or dostools Debian, for example.

```
mkfs.msdos 2.8 (28 Feb 2001)
Selecting 8 sectors per cluster
/dev/sde1 has 33 heads and 61 sectors per track,
logical sector size is 512,
using 0xf8 media descriptor, with 2047966 sectors;
file system has 2 32-bit FATs and 8 sectors per cluster.
FAT size is 1997 sectors, and provides 255492 clusters.
Volume ID is 420781ea, no volume label.
```

Note

Newer Linux distributions automatically sync a newly created partition and format the drive. The sync feature eliminates the need to reboot the computer, unlike with Microsoft OSs.

19. Close the shell window for this session by typing **exit** and pressing **Enter**. This drive can now be mounted and used to receive an image of a suspect drive. Later in this section, you learn how to mount and write to this Microsoft FAT target drive.

Acquiring Data with dd in Linux

A unique feature of a forensics Linux Live CD is that it can mount and read most drives. To perform a data acquisition on a suspect computer, all you need are the following:

- A forensics Linux Live CD
- A USB, FireWire, or SATA external drive with cables
- Knowledge of how to alter the suspect computer's BIOS to boot from the Linux Live CD
- Knowledge of which shell commands to use for the data acquisition

Tip

If you want to learn more about Linux and shell commands, review a Linux tutorial, such as Nix Tutor at www.nixtutor.com/linux/all-the-best-linux-cheat-sheets.

The dd command, available on all UNIX and Linux distributions, means "data dump." This command, which has many functions and switches, can be used to read and write data from a media device and a data file. The dd command isn't bound by a logical file system's data structures, meaning the drive doesn't have to be mounted for dd to access it. For example, if you list a physical device name, the dd command copies the entire device—all data files, slack space, and free space (unallocated data) on the device. The dd command creates a raw format file that most forensics analysis tools can read, which makes it useful for data acquisitions.

Caution

Use extreme caution with the dd command. Make sure you know which drives are the suspect drive and target drive. Although you might not have mounted the suspect drive, if you reverse the input field (if=) of the suspect and target drives with the output field (of=), data is written to the wrong drive, thus destroying the original evidence drive.

As powerful as this command is, it does have some shortcomings. One major problem is that it requires more advanced skills than the average computer user might have. Also, because it

doesn't compress data, the target drive needs to be equal to or larger than the suspect drive. It's possible to divide the output to other drives if a large enough target drive isn't available, but this process can be cumbersome and prone to mistakes when you're trying to keep track of which data blocks to copy to which target drive.

The dd command combined with the split command segments output into separate volumes. Use the split command with the -b switch to adjust the size of segmented volumes the dd command creates. As a standard practice for archiving purposes, create segmented volumes that fit on a CD or DVD. For additional information on dd and split, see their man pages. Follow these steps to make an image of an NTFS disk on a FAT32 disk by using the dd command:

1. Assuming that your workstation is the suspect computer and is booted from a Linux Live CD, connect the USB, FireWire, or SATA external drive containing the FAT32 target drive, and turn the external drive on.
2. If you're not at a shell prompt, start a shell window, switch to superuser (su) mode, type the root password, and press **Enter**.
3. At the shell prompt, list all drives connected to the computer by typing **fdisk -l** and pressing **Enter**, which produces the following output:

```
Disk /dev/hda: 40.0 GB, 40007761920 bytes
255 heads, 63 sectors/track, 4864 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

Device Boot    Start     End      Blocks    Id   System
/dev/hda1   *    1        13      104391    83   Linux
/dev/hda2       14      4864    38965657+   8e   Linux LVM

Disk /dev/sda: 163.9 GB, 163928605184 bytes
255 heads, 63 sectors/track, 19929 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

Device Boot    Start     End      Blocks    Id  System
/dev/sda1        1      12000    96389968+   b  W95 FAT32
/dev/sda2    12001      19929    63689692+   5  Extended
/dev/sda5    12001      19929    63689661    c  W95 FAT32 (LBA)

Disk /dev/sdb: 6448 MB, 6448619520 bytes
199 heads, 62 sectors/track, 1020 cylinders
Units = cylinders of 12338 * 512 = 6317056 bytes

Device Boot    Start    End    Blocks   Id   System
/dev/sdb1        1     1020   6292349    7   HPFS/NTFS
```

4. To create a mount point for the USB, FireWire, or SATA external drive and partition, make a directory in /mnt by typing **mkdir /mnt/sda5** and pressing **Enter**.
5. To mount the target drive partition, type **mount -t vfat /dev/sda5 /mnt/sda5** and press **Enter**.
6. To change your default directory to the target drive, type **cd /mnt/sda5** and press **Enter**.
7. List the contents of the target drive's root level by typing **ls -al** and pressing **Enter**. Your output should be similar to the following:

```
total 40
drwxr-xr-x  2 root root 32768 Dec 31  1969 .
drwxr-xr-x  5 root root  4096 Feb  6 17:22 ..
```

8. To make a target directory to receive image saves of the suspect drive, type **mkdir case01** and press **Enter**.

9. To change to the newly created target directory, type **cd case01** and press **Enter**. Don't close the shell window.

Next, you perform a raw format image of the entire suspect drive to the target directory. To do this, you use the split command with the dd command. The split command creates a two-letter extension for each segmented volume. The -d switch creates numeric rather than letter extensions. As a general rule, if you plan to use a Windows forensics tool to examine a dd image file created with this switch, the segmented volumes shouldn't exceed 2 GB each because of FAT32 file size limits. This 2 GB limit allows you to copy only up to 198 GB of a suspect's disk. If you need to use the dd command, it's better to use the split command's default of incremented letter extensions and make smaller segments. To adjust the segmented volume size, change the value for the -b switch from the 650 MB used in the following example to 2000 MB.

1. Type **dd if=/dev/sdb | split -b 650m - image_sdb**. and press **Enter**. You should see output similar to the following:

```
12594960+0 records in
12594960+0 records out
```

Tip

When using the split command, type a period at the end of the filename as shown, with no space between it and the filename. Otherwise, the extension is appended to the filename with no "." delimiter.

2. List the raw images that have been created from the dd and split commands by typing **ls -l** and pressing **Enter**. You should see output similar to the following:

```
total 6297504
-rwxr-xr-x  1 root root 681574400 Feb  6 17:26 image_sdb.aa
-rwxr-xr-x  1 root root 681574400 Feb  6 17:28 image_sdb.ab
-rwxr-xr-x  1 root root 681574400 Feb  6 17:29 image_sdb.ac
-rwxr-xr-x  1 root root 681574400 Feb  6 17:30 image_sdb.ad
-rwxr-xr-x  1 root root 681574400 Feb  6 17:32 image_sdb.ae
-rwxr-xr-x  1 root root 681574400 Feb  6 17:33 image_sdb.af
-rwxr-xr-x  1 root root 681574400 Feb  6 17:34 image_sdb.ag
-rwxr-xr-x  1 root root 681574400 Feb  6 17:36 image_sdb.ah
-rwxr-xr-x  1 root root 681574400 Feb  6 17:37 image_sdb.ai
-rwxr-xr-x  1 root root 314449920 Feb  6 17:37 image_sdb.aj
```

3. To complete this acquisition, dismount the target drive by typing **umount /dev/sda5** and pressing **Enter**.

Depending on the Windows forensics analysis tool you're using, renaming each segmented volume's extension with incremented numbers instead of letters might be necessary. For example, rename image_sdb.aa as image_sdb.01, and so on. Several Windows forensics tools can read only disk-to-image segmented files that have numeric extensions. Most Linux forensics tools can read segments with numeric or lettered extensions.

Acquiring a specific partition on a drive works the same way as acquiring the entire drive. Instead of typing /dev/sdb as you would for the entire drive, add the partition number to the device name, such as /dev/sdb1. For drives with additional partitions, use the number that

would be listed in the fdisk -l output. For example, to copy only the partition of the previous NTFS drive, you use the following dd command:

```
dd if=/dev/sdb1 | split -b 650m - image_sdb1
```

Remember to use caution with the dd command in your forensics data acquisitions.

Acquiring Data with dcfldd in Linux

The dd command is intended as a data management tool; it's not designed for forensics acquisitions. Because of these shortcomings, Nicholas Harbour of the Defense Computer Forensics Laboratory (DCFL) developed a tool that can be added to most UNIX/Linux OSs. This tool, the dcfldd command, works similarly to the dd command but has many features designed for forensics acquisitions. The following are important functions dcfldd offers that aren't possible with dd:

- Specify hexadecimal patterns or text for clearing disk space.
- Log errors to an output file for analysis and review.
- Use the hashing options MD5, SHA-1, SHA-256, SHA-384, and SHA-512 with logging and the option of specifying the number of bytes to hash, such as specific blocks or sectors.
- Refer to a status display indicating the acquisition's progress in bytes.
- Split data acquisitions into segmented volumes with numeric extensions (unlike dd's limit of 99).
- Verify the acquired data with the original disk or media data.

When using dcfldd, you should follow the same precautions as with dd. The dcfldd command can also write to the wrong device, if you aren't careful.

The following examples show how to use the dcfldd command to acquire data from a 64 MB USB drive, although you can use the command on a larger media device. All commands need to be run from a privileged root shell session. To acquire an entire media device in one image file, type the following command at the shell prompt:

```
dcfldd if=/dev/sda of=usbimg.dat
```

If the suspect media or disk needs to be segmented, use the dcfldd command with the split command, placing split before the output file field (of=), as shown here:

```
dcfldd if=/dev/sda hash=md5 md5log=usbimgmd5.txt bs=512
  conv=noerror,sync split=2M of=usbimg
```

This command creates segmented volumes of 2 MB each. To create segmented volumes that fit on a CD of 650 MB, change the split=2M to split=650M. This command also saves the MD5 value of the acquired data in a text file named usbimgmd5.txt.

Tip

For additional information on the dcfldd command, see http://dcfldd.sourceforge.net. Information on how to download and install dcfldd is available for many UNIX, Linux, and Macintosh OSs. You can also use the man page to find more information on dcfldd features and switches.

Capturing an Image with AccessData FTK Imager Lite

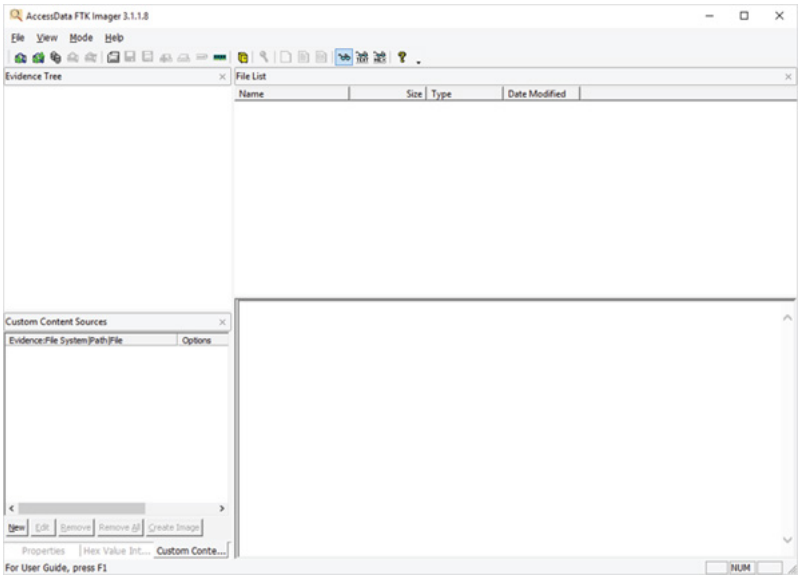
The following activity assumes you have removed the suspect drive and connected it to a USB or FireWire write-blocker device connected to your forensic workstation. The acquisition is written to a work folder on your C drive, assuming it has enough free space for the acquired data. Follow these steps to perform the first task of connecting the suspect's drive to your workstation:

1. Document the chain of evidence for the drive you plan to acquire.
2. Remove the drive from the suspect's computer.
3. For IDE drives, configure the suspect drive's jumpers as needed. (*Note*: This step doesn't apply to SATA or USB drives.)
4. Connect the suspect drive to the USB or FireWire write-blocker device.
5. Create a storage folder on the target drive. For this activity, you use your work folder (C:*Work*\Chap03\Chapter), but in real life, you'd use a folder name such as C:\Evidence.

FTK Imager is a data acquisition tool included with a licensed copy of AccessData Forensic Toolkit. Like most Windows data acquisition tools, it requires using a USB dongle for licensing. FTK Imager Lite, Debian and Ubuntu x64 command-line interfaces, and macOS 10.5 and 10.6x command-line interfaces are free and require no dongle license. To download FTK Imager Lite, see http://accessdata.com/product-download/digital-forensics/ftk-imager-lite-version-3.1.1. To download Debian and Ubuntu x64, see http://accessdata.com/product-download/digital-forensics/debian-and-ubuntu-x64-3.1.1#release-information. To download macOS 10.5 and 10.6x, see http://accessdata.com/product-download/digital-forensics/mac-os-10.5-and-10.6x-version-3.1.1.

FTK Imager is designed for viewing evidence disks and disk-to-image files created from other proprietary formats. It can read AccessData .ad1, Expert Witness Compression (EnCase) .e01, SMART .s01, Advanced Forensic Format (AFF), and raw format files. In addition to disk media, FTK Imager can read CD and DVD file systems. This program shows a view of a disk partition or an image file as though it's a mounted partition, with additional panes showing the contents of the selected file (see Figure 3-2).

Figure 3-2.



Source: AccessData Group, Inc., www.accessdata.com

The FTK Imager main window

FTK Imager can make disk-to-image copies of evidence drives and enables you to acquire an evidence drive from a logical partition level or a physical drive level. You can also define the size of each disk-to-image file volume, allowing you to segment the image into one or many split volumes. For example, you can specify 650 MB volume segments if you plan to store volumes on 650 MB CD-Rs or 2.0 GB volume segments so that you can record volumes on DVD-/+Rs. An additional feature of FTK Imager is that it can image RAM on a live computer. The evidence drive you're acquiring data from must have a hardware write-blocking device or run from a Live CD, such as Mini-WinFE.

FTK Imager can't acquire a drive's HPA and device configuration overlay (DCO), however. In other words, if the drive's specifications indicate it has 11,000,000 sectors and the BIOS display indicates 9,000,000, a host protected area of 2,000,000 sectors might be assigned to the drive. If you suspect an evidence drive has a host protected area, you must use an advanced acquisition tool to include this area when copying data. With older MS-DOS tools, you might have to define the exact sector count to make sure you include more than what the BIOS shows as the number of known sectors on a drive. Review vendors' manuals to determine how to account for a drive's host protected area.

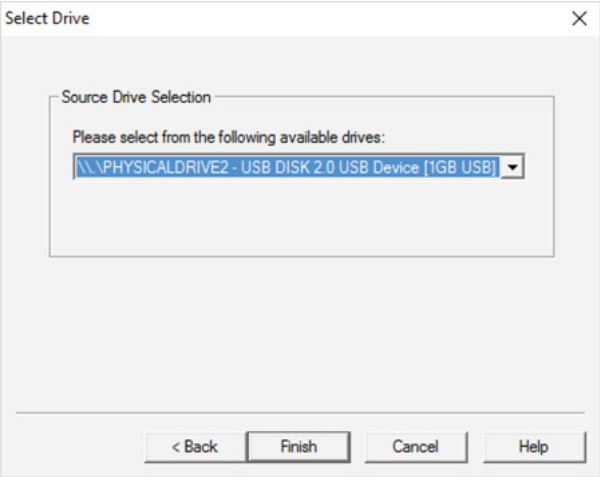
In the following activity, you use FTK Imager Lite to make an image file. (If you haven't installed it already, do so now. You download it at http://accessdata.com/product-download/digital-forensics/ftk-imager-lite-version-3.1.1.) Use a write-blocking device to protect the suspect drive, and then follow these steps:

Note

Before starting this activity, create a work folder named *Work*\Chap03\Chapter. Note that work folder names might differ slightly in screenshots.

1. Boot your forensic workstation to Windows, using an installed write-blocker.
2. Connect the evidence drive to a write-blocking device or USB device.
3. Connect the target drive to a USB external drive, if you're using a write-blocker.
4. Start FTK Imager Lite. If prompted by the User Account Control message box, click **Yes**.
5. In the FTK Imager main window, click **File**, **Create Disk Image** from the menu.
6. In the Select Source dialog box, click the **Physical Drive** option button, if necessary, and then click **Next**.
7. In the Select Drive dialog box, click the **Source Drive Selection** list arrow (see Figure 3-3), click the suspect drive, and then click **Finish**.

Figure 3-3.

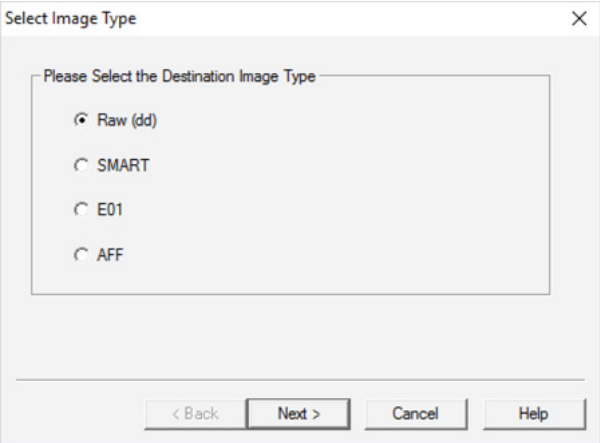


Source: AccessData Group, Inc., www.accessdata.com

The Select Drive dialog box

8. In the Create Image dialog box, click to select the **Verify images after they are created** check box, if necessary, and then click **Add**. In the Select Image Type dialog box that opens (see Figure 3-4), click the **Raw (dd)** option button, if necessary, and then click **Next**.

Figure 3-4.

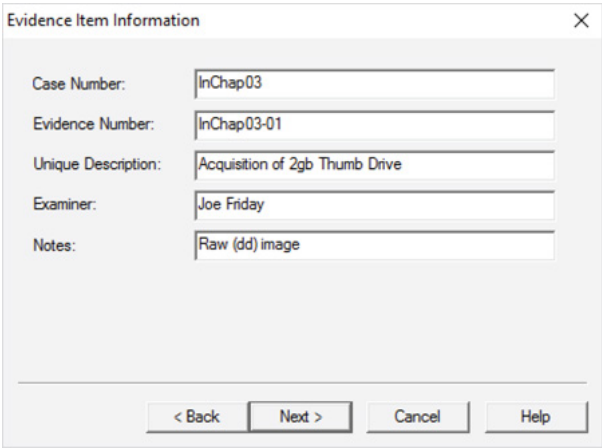


Source: AccessData Group, Inc., www.accessdata.com

The Select Image Type dialog box

9. In the Evidence Item Information dialog box, complete the case information, as shown in **Figure 3-5**, and then click **Next**.

Figure 3-5.

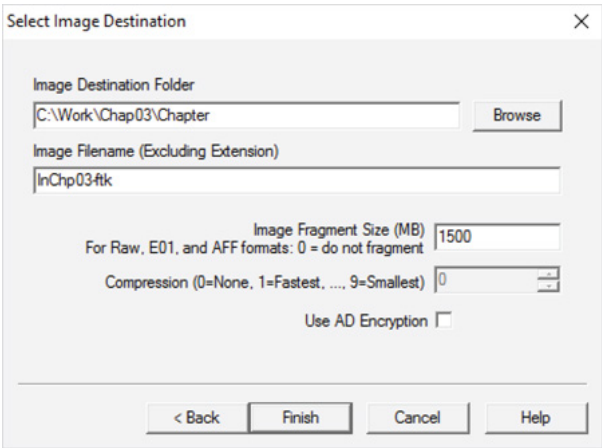


Source: AccessData Group, Inc., www.accessdata.com

The Evidence Item Information dialog box

10. In the Select Image Destination dialog box (see **Figure 3-6**), click **Browse**, navigate to the location for the image file (your work folder), and click to clear the **Use AD Encryption** check box, if necessary.

Figure 3-6.



Source: AccessData Group, Inc., www.accessdata.com

Selecting where to save the image file

Note

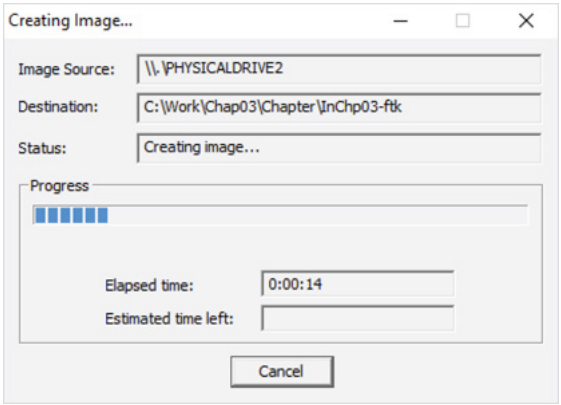
You can adjust the amount in the Image Fragment Size text box, but for this activity, leave the default value of 1500 MB.

11. In the Image Filename (Excluding Extension) text box, type **InChp03-ftk**, and then click **Finish**.

12. Next, in the Create Image dialog box, click **Start** to initiate the acquisition.

13. When FTK Imager finishes the acquisition, review the information in the Drive/Image Verify Results dialog box, and then click **Close**. Click **Close** again in the Creating Image dialog box (see Figure 3-7).

Figure 3-7.



Source: AccessData Group, Inc., www.accessdata.com

An image save in progress

14. Exit FTK Imager Lite by clicking **File**, **Exit** from the menu.

Note

For additional information, see the Help menu in FTK Imager Lite to learn more about its many features.

Validating Data Acquisitions

Probably the most critical aspect of computer forensics is validating digital evidence. The weakest point of any digital investigation is the integrity of the data you collect, so validation is essential. In this section, you learn how to use several tools to validate data acquisitions.

Validating digital evidence requires using a hashing algorithm utility, which is designed to create a binary or hexadecimal number that represents the uniqueness of a data set, such as a file or disk drive. This unique number is referred to as a "digital fingerprint." With a few exceptions, making any alteration in one of the files—even changing one letter from uppercase to lowercase—produces a completely different hash value.

These exceptions, known as "collisions," have been found to occur in a small number of files with MD5, and SHA-1 might also be subject to collisions. For forensic examinations of data files on a disk drive, however, collisions are of little concern. If two files with different content have the same MD5 hash value, a comparison of each byte of a file can be done to see the differences. Currently, several tools can do a byte-by-byte comparison of files. Programs such as X-Ways Forensics, X-Ways WinHex, and IDM Computing Solution's UltraCompare can analyze and compare data files. For more information on MD5 collisions, see www.x-ways.net/md5collision.html or www.mscs.dal.ca/~selinger/md5collision/. Chapter 4 discusses methods of using MD5 and SHA-1.

For imaging an evidence drive, many tools offer validation techniques ranging from CRC-32, MD5, and SHA-1 to SHA-512. These hashing algorithm utilities are available as stand-alone programs or are integrated into many acquisition tools. The following sections discuss how to perform validation with some currently available acquisition programs.

Linux Validation Methods

Linux is rich in commands and functions. The two Linux shell commands shown earlier in this chapter, dd and dcfldd, have several options that can be combined with other commands to validate data. The dcfldd command has other options that validate data collected from an

acquisition. Validating acquired data with the dd command requires using other shell commands.

Current distributions of Linux include two hashing algorithm utilities: md5sum and sha1sum. Both utilities can compute hashes of a single file, multiple files, individual or multiple disk partitions, or an entire disk drive.

Validating dd-Acquired Data

As shown earlier, the following command produces segmented volumes of the /dev/sdb drive, with each segmented volume named image_sdb and an incrementing extension of .aa, .ab, .ac, and so on:

```
dd if=/dev/sdb | split -b 650m image_sdb
```

To validate all segmented volumes of a suspect drive with the md5sum utility, you use the Linux shell commands shown in the following steps. For the saved images, remember to change to the directory where the data was saved, or list the exact path for the saved images. To use sha1sum instead of md5sum, just replace all md5sum references in commands with sha1sum. The drive should still be connected to your acquisition workstation.

1. If necessary, start Linux, open a shell window, and navigate to the directory where image files are saved. To calculate the hash value of the original drive, type **md5sum/dev/sdb > md5_sdb.txt** and press **Enter**.

   Note

   The redirect (>) option saves the computed MD5 hash value in the md5_sdb.txt file. This file should be saved with image files as validation of the evidence.

2. To compute the MD5 hash value for the segmented volumes and append the output to the md5_sdb.txt file, type **cat image_sdb.*| md5sum >> md5_sdb.txt** and press **Enter**.

   Note

   By using the cat (concatenate) command with an asterisk (*) as the extension value, all segmented volumes are read sequentially as one big contiguous file, as though they were the original drive or partition. The pipe (|) function outputs the cat command read data to the input of the md5sum command. The >> option adds the md5sum hash results to the end of the md5_sdb.txt file's content.

3. Examine the md5_sdb.txt file to see whether both hashes match by typing **cat md5_sdb.txt** and pressing **Enter**. If the data acquisition is successful, the two hash numbers should be identical. If not, the acquisition didn't work correctly. You should see output similar to the following:

   ```
   34963884a4bc5810b130018b00da9de1  /dev/sdb
   34963884a4bc5810b130018b00da9de1
   ```

4. Close the Linux shell window by typing **exit** and pressing **Enter**.

With the dd command, the md5sum or sha1sum utilities should be run on all suspect disks and volumes or segmented volumes.

Validating dcfldd-Acquired Data

Because dcfldd is designed for forensics data acquisition, it has validation options integrated: hash and hashlog. You use the hash option to designate a hashing algorithm of md5, sha1, sha256, sha384, or sha512. The hashlog option outputs hash results to a text file that can be stored with image files. To create an MD5 hash output file during a dcfldd acquisition, you enter the following command (in one line) at the shell prompt:

```
dcfldd if=/dev/sda split=2M of=usbimg hash=md5
  hashlog=usbhash.log
```

To see the results of files generated with the split command, you enter the list directory (ls) command at the shell prompt. You should see the following output:

```
usbhash.logusbimg.004 usbimg.010 usbimg.016 usbimg.022 usbimg.028
usbseghash.logusbimg.005 usbimg.011 usbimg.017 usbimg.023 usbimg.029
usbimg.000 usbimg.006 usbimg.012 usbimg.018 usbimg.024 usbimg.030
usbimg.001 usbimg.007 usbimg.013 usbimg.019 usbimg.025
usbimg.002 usbimg.008 usbimg.014 usbimg.020 usbimg.026
usbimg.003 usbimg.009 usbimg.015 usbimg.021 usbimg.027
```

Note that the first segmented volume has the extension .000 rather than .001. Some Windows forensics tools might not be able to read segmented file extensions starting with .000. They're typically looking for .001. If your forensics tool requires starting with an .001 extension, the files need to be renamed incrementally. So segmented file .000 should be renamed .001, .001 should be renamed .002, and so on.

Another useful dcfldd option is vf (verify file), which compares the image file with the original medium, such as a partition or drive. The vf option applies only to a nonsegmented image file. To validate segmented files from dcfldd, use the md5sum or sha1sum command described previously. To use the vf option, you enter the following command at the shell prompt:

```
dcfldd if=/dev/sda vf=sda_hash.img
```

For additional information on dcfldd, see the man page.

Windows Validation Methods

Unlike Linux, Windows has no built-in hashing algorithm tools for digital forensics. However, many Windows third-party programs do have a variety of built-in tools. These third-party programs range from hexadecimal editors, such as X-Ways WinHex or Breakpoint Software Hex Workshop, to forensics programs, such as OSForensics, Autopsy, EnCase, and FTK. In **Chapter 9**, you learn how to hash specific data by using a hexadecimal editor to locate and verify groups of data that have no file association or are sections within a file.

Commercial forensics programs also have built-in validation features. Each program has its own validation technique used with acquisition data in its proprietary format. For example, Autopsy uses MD5 to validate an image. It reads the metadata in Expert Witness Compression or AFF image files to get the original hash. If the hashes don't match, Autopsy notifies you that the acquisition is corrupt and can't be considered reliable evidence.

In Autopsy and many other forensics tools, however, raw format image files don't contain metadata. As mentioned, a separate manual validation is recommended for all raw acquisitions at the time of analysis. The previously generated validation file for raw format acquisitions is essential to the integrity of digital evidence. The saved validation file can be used later to check whether the acquisition file is still good.

In FTK Imager Lite, when you select the Expert Witness Compression (.e01) or the SMART (.s01) format, additional options for validation are displayed. This validation report also lists the MD5 and SHA-1 hash values. The MD5 hash value is added to the proprietary format image

or segmented files. When this image is loaded into FTK, SMART, or X-Ways Forensics (which can read only .e01 and raw files), the MD5 hash is read and compared with the image to verify whether the acquisition is correct.

You can find other open-source hashing tools online; just search for "windows open source hash" to find the latest available Windows hashing tools. For example, a recent search turned up SourceForge md5deep at http://md5deep.sourceforge.net and Software Informer at http://softwaresolution.informer.com/Hash-Tool.

Performing RAID Data Acquisitions

Acquisitions of RAID drives can be challenging and frustrating for digital forensics examiners because of how RAID systems are designed, configured, and sized. Size is the biggest concern because many RAID systems are now pushing into exabytes or more of data. The following sections review common RAID configurations and discuss ways to acquire data on these large storage devices.

Understanding RAID

Redundant array of independent disks (RAID) is a computer configuration involving two or more physical disks. Originally, RAID was developed as a data-redundancy measure to minimize data loss caused by a disk failure. As technology improved, RAID also provided increased storage capabilities.

Several levels of RAID can be implemented through software (known as "software RAID") or special hardware controllers (known as "hardware RAID"). Software RAID is typically implemented from the host computer's OS. Hardware RAID uses its own controller as well as a processor and memory connected to the host computer. For more information on RAID configurations, see www.adaptec.com/nr/rdonlyres/14b2fd84-f7a0-4ac5-a07a-214123ea3dd6/0/4423_sw_hwraid_10.pdf.

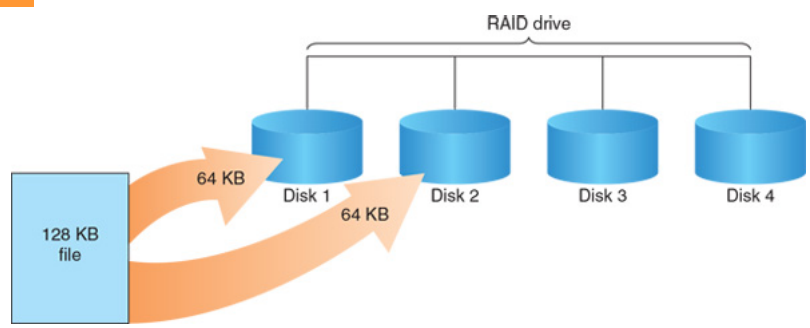
For Windows XP, 2000, and NT servers and workstations, RAID 0 or 1 is available. For a high-end data-processing environment, RAID 5 is common and is often based in special RAID towers. These high-end RAID systems usually have integrated controllers that connect to high-end servers or mainframes. These systems provide redundancy and high-speed data access and can make many small disks appear as one very large drive.

Note

Other variations of RAID besides 0, 1, and 5 are specific to their vendor or application.

RAID 0 provides rapid access and increased data storage (see **Figure 3-8**). In RAID 0, two or more disk drives become one large volume, so the computer views the disks as a single disk. The tracks of data on this mode of storage cross over to each disk. The logical addressing scheme makes it seem as though each track of data is continuous throughout all disks. If you have two disks configured as RAID 0, track one starts on the first physical disk and continues to the second physical disk. When viewed from a booted OS, such as Windows XP or later, the two disks appear as one large disk. The advantage of RAID 0 is increased speed and data storage capability spread over two or more disks that can be one large disk partition. Its biggest disadvantage is lack of redundancy; if a disk fails, data isn't continuously available.

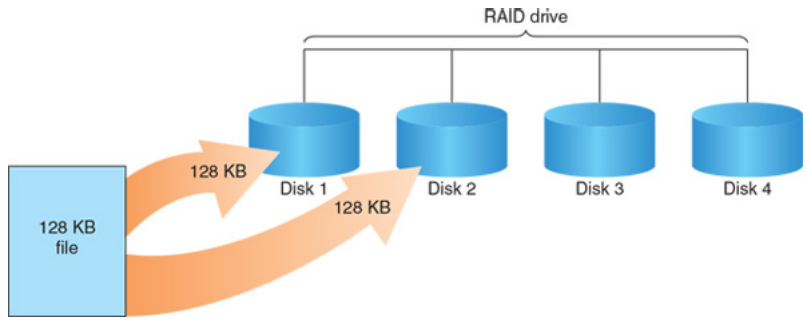
Figure 3-8.



RAID 0: Striping

RAID 1, shown in **Figure 3-9**, is made up of two disks for each volume and is designed for data recovery in the event of a disk failure. The contents of the two disks in RAID 1 are identical. When data is written to a volume, the OS writes the data twice—once to each disk at the same time. If one drive fails, the OS switches to the other disk.

Figure 3-9.



RAID 1: Mirroring

RAID 1 ensures that data isn't lost and helps prevent computer downtime. The main disadvantage of RAID 1 is that it takes two disks for each volume, which doubles the cost of disk storage.

Like RAID 1, RAID 2 (see **Figure 3-10**) provides rapid access and increased storage by configuring two or more disks as one large volume. The difference with RAID 2 is that data is written to disks on a bit level. An error-correcting code (ECC) is used to verify whether the write is successful. RAID 2, therefore, has better data integrity checking than RAID 0. Because of the bit-level writes and the ECC, however, RAID 2 is slower than RAID 0.

Figure 3-10.

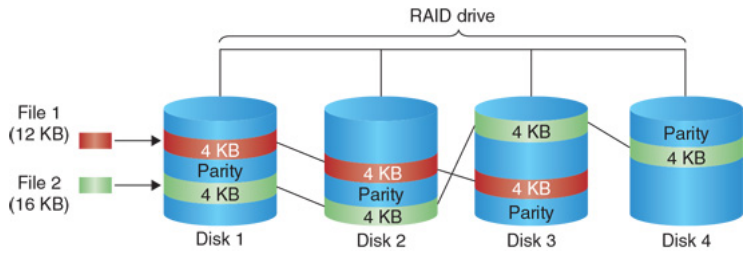
RAID 2: Striping (bit level)

RAID 3 uses data striping and dedicated parity and requires at least three disks. Similar to RAID 0, RAID 3 stripes tracks across all disks that make up one volume. RAID 3 also

implements dedicated parity of data to ensure recovery if data is corrupted. Dedicated parity is stored on one disk in the RAID 3 array. Like RAID 3, RAID 4 uses data striping and dedicated parity (block writing), except data is written in blocks rather than bytes.

RAID 5 (see **Figure 3-11**) is similar to RAID 0 and RAID 3 in that it uses distributed data and distributed parity and stripes data tracks across all disks in the RAID array. Unlike RAID 3, however, RAID 5 places parity data on each disk. If a disk in a RAID array has a data failure, the parity on other disks rebuilds the corrupt data automatically when the failed drive is replaced.

Figure 3-11.



RAID 5: Block-level striping with distributed parity

In RAID 6, distributed data and distributed parity (double parity) function the same way as RAID 5, except each disk in the RAID array has redundant parity. The advantage of RAID 6 over RAID 5 is that it recovers any two disks that fail because of the additional parity stored on each disk.

RAID 10, or mirrored striping, also known as RAID 1+0, is a combination of RAID 1 and RAID 0. It provides fast access and redundancy of data storage. RAID 15, or mirrored striping with parity, also known as RAID 1+5, is a combination of RAID 1 and RAID 5. It offers the most robust data recovery capability and speed of access of all RAID configurations and is also more costly.

Acquiring RAID Disks

There's no simple method for getting an image of a RAID server's disks. You need to address the following concerns:

- How much data storage is needed to acquire all data for a forensics image?
- What type of RAID is used? Is it Windows RAID 0 or 1 or an integrated hardware-firmware vendor's RAID 5, 10, or 15? Is it another unknown configuration or OS?
- If it's a RAID 1, 10, or 15 server, do you need to have all drives connected so that the OS sees their contents? Some older RAID 1 systems required connecting both drives to make the data readable, which might also apply to RAID 10 and 15.
- Do you have an acquisition tool capable of copying the data correctly?
- Can the tool read a forensic copy of a RAID image?
- Can the tool read split data saves of each RAID disk, and then combine all images of each disk into one RAID virtual drive for analysis?

With the larger disks now available, copying small RAID systems to one large disk is possible, similar to the way non-RAID suspect drives are copied. For example, a small server running eight 36 GB SCSI drives in a RAID 0 tower requires about a 300 GB SATA or IDE (PATA) drive. Less data storage is needed if a proprietary format acquisition is used with compression applied. All forensics analysis tools can analyze an image because they see the acquired data as one large drive, not eight separate drives.

Several forensics vendors have added RAID recovery features. These vendors typically specialize in one or two types of RAID formats. The following are some vendors offering RAID acquisition functions:

- Guidance Software EnCase
- X-Ways Forensics
- AccessData FTK
- Runtime Software
- R-Tools Technologies

You should know which vendor supports which RAID format and keep up to date on the latest improvements in these products.

Being able to separate each physical disk into smaller save sets eliminates the need to have one large drive for storing acquired data. Acquiring RAID data requires only similar-size drives that match each disk in the RAID array. For example, with a RAID 0 array of three 2 TB disks, all you need are three target drives of the same size. If each acquisition is compressed, you might be able to get by with slightly smaller target drives.

Tools such as Runtime Software (www.runtime.org) and R-Tools Technologies (www.r-tt.com) are designed as data recovery tools. Although not intended as forensics acquisition tools, they have unique features that can aid in recovering corrupted RAID data and can perform raw format acquisitions and repair broken RAID 0 and 5 systems. The Runtime RAID Reconstructor tool copies the original RAID to a raw format file, which must then be restored on another RAID-configured system where repairs can be performed. It also scans and corrects errors on the newly copied RAID. R-Tools R-Studio creates a virtual volume of the RAID image file. All repairs are made on the virtual volume, which can then be restored to the original RAID.

Occasionally, a RAID system is too large for a static acquisition. Under ideal circumstances, your goal is to collect a complete image of evidence drives. Because RAID systems can have dozens or more terabytes of data storage, copying all data isn't always practical. For these occasions, retrieving only the data relevant to the investigation with the sparse or logical acquisition method is the only practical solution. When dealing with very large RAID servers, consult with the forensics vendor to determine how to best capture RAID data. Another possible solution is renting a portable RAIDBank for your acquisition.

Using Remote Network Acquisition Tools

Recent improvements in forensics tools include the capability to acquire disk data or data fragments (sparse or logical) remotely. With this feature, you can connect to a suspect computer remotely via a network connection and copy data from it. Remote acquisition tools vary in configurations and capabilities. Some require manual intervention on remote suspect computers to initiate the data copy. Others can acquire data surreptitiously through an encrypted link by pushing a remote access program to the suspect's computer. From an investigation perspective, being able to connect to a suspect's computer remotely to perform an acquisition has tremendous appeal. It saves time because you don't have to go to a suspect's computer, and it minimizes the chances of a suspect discovering that an investigation is taking place. Most remote acquisitions have to be done as live acquisitions, not static acquisitions. When performing remote acquisitions, advanced privileges are required to push agent applications to the remote system.

There are some drawbacks to consider, such as antivirus, antispyware, and firewall tools. Most of these security programs can be configured to ignore remote access programs. However, if

suspects have administrator rights on their computers, they could easily install their own security tools that trigger an alarm to notify them of remote access intrusions.

The following sections describe methods used by digital forensics tools that have the capability to perform remote acquisitions. An older version of ProDiscover is used as an example to show how remote acquisitions work. Other vendors' remote acquisition functions work similarly. **Chapter 10** covers other resources for data copying and explains how to perform a live forensics acquisition.

Remote Acquisition with ProDiscover

ProDiscover Incident Response is designed to be integrated as a network intrusion analysis tool and is useful for performing remote acquisitions. When connected to a remote computer, it uses the same ProDiscover acquisition method described previously. After the connection is established, the remote computer is displayed in the Capture Image dialog box. This tool offers all the functions and features of other tools in the ProDiscover suite plus the following:

- Capture volatile system state information.
- Analyze current running processes on a remote system.
- Locate unseen files and processes on a remote system that might be running malware or spyware.
- Remotely view and listen to IP ports on a compromised system.
- Run hash comparisons on a remote system to search for known Trojans and rootkits.
- Create a hash inventory of all files on a system remotely (a negative hash search capability) to establish a baseline if it gets attacked.

The ProDiscover utility for remote access is the PDServer remote agent, which must be loaded on the suspect computer before ProDiscover Incident Response can access it. This remote agent can be installed in three different ways:

- *Trusted CD*—For this manual installation method, ProDiscover can create a special CD/DVD or USB drive containing the PDServer remote agent. It's used to load PDServer manually on the suspect computer.
- *Preinstallation*—For networks with a configured OS, the PDServer remote agent can be added to the standard installation of high-risk computers, which enables network security administrators to respond to network attacks and malware contaminations quickly. Any network management tool, such as DameWare (www.dameware.com) or Hyena (www.systemtools.com/hyena/), can be used to initiate a connection with ProDiscover. This is a remote method of installing the remote acquisition tool.
- *Pushing out and running remotely*—Downloading PDServer to a remote computer helps investigators respond quickly to incidents. Data is collected in real time when using this function. This is a remote method of installing the remote acquisition tool.

With PDServer, you have the option of running it in a stealth mode to hide it from the suspect. Note that Windows Task Manager lists the process as PDServer. To disguise it, you can change the process name so that it appears to be an OS function in the suspect computer's Task Manager. In addition, the following security features are available for remote connections:

- *Password protection*—PDServer on the target computer is password-protected, and the password is encrypted at all times.
- *Encryption*—All communication between PDServer on the suspect's and investigator's computers can be encrypted. ProDiscover provides 256-bit Advanced Encryption Standard (AES) or Twofish encryption for the connection.

- *Secure communication protocol*—All connections between the suspect's and examiner's computers have globally unique identifiers (GUIDs) to prevent inserting packets in the data stream.
- *Write-protected trusted binaries*—PDServer can run from a write-protected device, such as a CD.
- *Digital signatures*—PDServer and its removal device driver, PARemoval.sys, are digitally signed to verify that they haven't been tampered with before and during the remote connection.

Note

For more information on ProDiscover, see www.arcgroupny.com.

Remote Acquisition with EnCase Enterprise

Guidance Software was the first forensics vendor to develop a remote acquisition and analysis tool based on its desktop tool EnCase. This remote tool, EnCase Endpoint Investigator, can perform the following functions:

- Search and collect internal and external network systems over a wide geographical area
- Support multiple OSs and file systems
- Triage to help determine systems' relevance to an investigation
- Perform simultaneous searches of up to five systems at a time

For more information, see www.guidancesoftware.com/docs/default-source/document-library/product-brief/encase-endpoint-investigator-product-overview.pdf.

Remote Acquisition with R-Tools R-Studio

The R-Tools suite of software is designed for data recovery. As part of this recovery capability, the R-Studio network edition can remotely access networked computer systems. Data acquired with R-Studio network edition creates raw format acquisitions, and it's capable of recovering many different file systems, including ReFS. For more information on R-Studio, see www.r-studio.com.

Remote Acquisition with WetStone US-LATT PRO

US-LATT PRO, part of a suite of tools developed by WetStone, can connect to a networked computer remotely and perform a live acquisition of all drives connected to it. For more information on this tool, see www.wetstonetech.com/product/us-latt/.

Remote Acquisition with F-Response

F-Response is a vendor-neutral specialty remote access utility designed to work with any digital forensics program. When installed on a remote computer, it sets up a security read-only connection that allows forensics examiners to access it. With F-Response, examiners can access remote drives at the physical level and view raw data. After the F-Response connection has been set up, any forensics acquisition tool can be used to collect digital evidence.

F-Response is sold in four different versions: Enterprise Edition, Consultant + Convert Edition, Consultant Edition, and TACTICAL Edition. For the latest information on F-Response, see www.f-response.com.

Using Other Forensics Acquisition Tools

In addition to the tools you've learned about already, you can use other commercial acquisition tools, described in the following sections. Prices for some tools are discounted for law enforcement officers working in digital forensics.

PassMark Software ImageUSB

PassMark Software has an acquisition tool called ImageUSB for its OSForensics analysis product. To create a bootable flash drive, you need Windows XP or later and ImageUSB downloaded from the OSForensics Web site. For more information on ImageUSB, see www.osforensics.com/tools/write-usb-images.html.

ASR Data SMART

ASR Data SMART is a Linux forensics analysis tool that can make image files of a suspect drive. SMART can produce proprietary or raw format images and includes the following capabilities:

- Robust data reading of bad sectors on drives
- Mounting suspect drives in write-protected mode
- Mounting target drives, including NTFS drives, in read/write mode
- Optional compression schemes to speed up acquisition or reduce the amount of storage needed for acquired digital evidence

For more information on SMART, see www.asrdata.com.

Runtime Software

In addition to RAID Reconstructor, Runtime Software offers several compact shareware programs for data acquisition and recovery, including DiskExplorer for FAT and DiskExplorer for NTFS. Runtime has designed its tools to be file system specific, so DiskExplorer versions for both FAT and NTFS are available. These tools offer the following features for acquisition needs:

- Create a raw format image file.
- Segment the raw format or compressed image for archiving purposes.
- Access network computers' drives.

For more information on Runtime Software, see www.runtime.org/raid.htm.

ILookIX IXImager

IXImager runs from a bootable thumb drive or CD/DVD. It's a stand-alone proprietary format acquisition tool designed to work only with ILookIX. It can acquire single drives and RAID drives. It supports IDE (PATA), SCSI, USB, and FireWire devices. The IXImager proprietary format can be converted to a raw format if other analysis tools are used. For more information on IXImager, see www.perlustro.com/solutions/e-forensics/iximager.

SourceForge

SourceForge provides several applications for security, analysis, and investigations. For a listing of its current tools, see https://sourceforge.net/directory/os:windows/. SourceForge also offers a Windows version of dcfldd; for updates, go to https://sourceforge.net/projects/dcfldd/?source=typ_redirect.

Chapter Summary

- Forensics data acquisitions are stored in three different formats: raw, proprietary, and AFF. Most proprietary formats and AFF store metadata about the acquired data in the image file.
- The four methods of acquiring data for forensics analysis are disk-to-image file, disk-to-disk copy, logical disk-to-disk or disk-to-data file, and sparse data copy of a folder or file.
- Lossless compression for forensics acquisitions doesn't alter the data when it's restored, unlike lossy compression. Lossless compression can compress up to 50% for most data. If data is already compressed on a drive, lossless compression might not save much more space.
- If there are time restrictions or too much data to acquire from large drives or RAID drives, a logical or sparse acquisition might be necessary. Consult with your lead attorney or supervisor first to let them know that collecting all the data might not be possible.
- You should have a contingency plan to ensure that you have a forensically sound acquisition and make two acquisitions if you have enough data storage. The first acquisition should be compressed, and the second should be uncompressed. If one acquisition becomes corrupt, the other one is available for analysis.
- Write-blocking devices or utilities must be used with GUI acquisition tools in both Windows and Linux. Practice with a test drive rather than suspect drive, and use a hashing tool on the test drive to verify that no data was altered.
- Always validate your acquisition with built-in tools from a forensics acquisition program, a hexadecimal editor with MD5 or SHA-1 hashing functions, or the Linux md5sum or sha1sum commands.
- A Linux Live CD, such as Ubuntu, openSUSE, Arch Linux, Fedora, or Slackware provides many useful tools for digital forensics acquisitions.
- The preferred Linux acquisition tool is dcfldd instead of dd because it was designed for forensics acquisition. The dcfldd tool is also available for Windows. Always validate the acquisition with the hashing features of dcfldd and md5sum or sha1sum.
- When using the Linux dd or dcfldd commands, remember that reversing the output field (of=) and input field (if=) of suspect and target drives could write data to the wrong drive, thus destroying your evidence. If available, you should always use a physical write-blocker device for acquisitions.
- To acquire RAID disks, you need to determine the type of RAID and which acquisition tool to use. With a firmware-hardware RAID, acquiring data directly from the RAID server might be necessary.
- Remote network acquisition tools require installing a remote agent on the suspect computer. The remote agent can be detected if suspects install their own security programs, such as a firewall.

Key Terms

Advanced Forensic Format (AFF)
host protected area (HPA)
live acquisitions
logical acquisition
raw format
redundant array of independent disks (RAID)

sparse acquisition
static acquisitions
whole disk encryption

Review Questions

1. What's the main goal of a static acquisition?
2. Name the three formats for digital forensics data acquisitions.
3. What are two advantages and disadvantages of the raw format?
4. List two features common with proprietary format acquisition files.
5. Of all the proprietary formats, which one is the unofficial standard?
6. Name two commercial tools that can make a forensic sector-by-sector copy of a drive to a larger drive.
7. What does a logical acquisition collect for an investigation?
8. What does a sparse acquisition collect for an investigation?
9. What should you consider when determining which data acquisition method to use?
10. Why is it a good practice to make two images of a suspect drive in a critical investigation?
11. When you perform an acquisition at a remote location, what should you consider to prepare for this task?
12. With newer Linux kernel distributions, what happens if you connect a hot-swappable device, such a USB drive, containing evidence?
13. In Linux, the fdisk -l command lists the suspect drive as /dev/hda1. Is the following dcfldd command correct?

```
dcfldd if=image_file.img
  of=/dev/hda1
```

14. What's the most critical aspect of digital evidence?
15. What's a hashing algorithm?
16. In the Linux dcfldd command, which three options are used for validating data?
17. What's the maximum file size when writing data to a FAT32 drive?
18. What are two concerns when acquiring data from a RAID server?
19. With remote acquisitions, what problems should you be aware of? (Choose all that apply.)
    a. Data transfer speeds
    b. Access permissions over the network
    c. Antivirus, antispyware, and firewall programs
    d. The password of the remote computer's user
20. Which forensics tools can connect to a suspect's remote computer and run surreptitiously?
21. EnCase, FTK, SMART, and ILookIX treat an image file as though it were the original disk. True or False?
22. FTK Imager can acquire data in a drive's host protected area. True or False?

Hands-On Projects

Create a Chap03\Projects folder under your work folder. Then copy the data files from the downloads section for this chapter (on the student companion site for this book) to this work

subfolder. If necessary, extract any compressed files to this subfolder.

Hands-On Project 3-1.

In this project, you prepare a drive and create a FAT32 disk partition using Linux. You need the following:

- A Linux distribution or Linux Live CD
- A disk drive
- A method of connecting a disk drive to your workstation, such as USB, FireWire, external SATA, or internal connections, such as PATA or SATA
- A review of the steps in the "Preparing a Target Drive for Acquisition in Linux" sectionA disk drive

To format a drive as FAT32 in Linux, follow these steps:

1. Connect the target drive to be partitioned and formatted as FAT32 to your workstation.
2. Start your workstation, and log on or boot the Linux Live CD.
3. Follow the steps in the "Preparing a Target Disk for Acquisition in Linux" section.
4. When you've finished formatting the target drive, leave it connected for the next project.

Hands-On Project 3-2.

In this project, you use the Linux dd command to make an acquisition split into 30 MB segmented volumes. Then you validate the data by using the Linux md5sum command on the original drive and the image files. The output for md5sum is then redirected to a data file kept with the image files. For this project, you need the following:

- A Linux distribution or Linux Live CD
- The FAT32 drive partitioned and formatted in **Hands-On Project 3-1**
- A method of connecting the FAT32 drive and the drive created in **Hands-On Project 3-1** to your workstation, such as USB, FireWire, external SATA, or internal connections, such as PATA or SATA
- A review of the "Acquiring Data with dd in Linux" and "Validating dd-Acquired Data" sections

Follow these steps:

1. Make sure you've connected the drive you prepared in **Hands-On Project 3-1** to your Linux workstation.
2. Start your workstation, if necessary, and log on to Linux or boot the Linux Live CD.
3. Reboot the Linux system, and make the dd acquisition, following the steps in "Acquiring Data with dd in Linux." For the split -b command, make the segmented size 30m, and use the -d switch to create numeric extensions for each segmented file.
4. When the acquisition is finished, do a validation of the suspect drive and the acquired image files. Follow the steps in the "Validating dd-Acquired Data" section. When you're finished, keep the terminal window open, and keep Linux running for the next project.

Hands-On Project 3-3.

Digital forensics examiners are sometimes asked to restore an image file to a disk drive. In this project, you learn how to perform this task. To prepare for this project, you need the following

items:

- Two USB drives formatted as FAT16 or FAT32 that can hold up to 120 MB

> **Note**
>
> Both USB drives should be formatted as FAT16 or FAT32. Your version of Linux might not be able to read or write data to USB media formatted as NTFS.

- A Linux distribution, Linux Live CD, or a computer running Linux with at least two USB ports
- The **GCFI-datacarve-FAT.dd** data file (extracted from CH03ProjDataFiles.exe to your work folder)

Data-Loading Procedure in Linux

First, you transfer data from the GCFI-datacarve-FAT.dd file to the target drive. Second, you restore the image file to another USB drive. Follow these steps:

1. On your Windows computer, copy the **GCFI-datacarve-FAT.dd** file to one of your USB drives.
2. Start your Linux workstation, if necessary. If you're using your Windows computer with a Linux Live CD, connect the second USB drive to the computer to serve as the target drive. If you're using a computer running Linux, connect both USB drives to it.
3. In Linux, open a terminal window, if necessary. To switch to the superuser account, type **su** and press **Enter**, and at the password prompt, type the root password and press **Enter**.
4. Type **df** and press **Enter** to list all attached devices to the computer, as shown in Figure 3-12. This output identifies the Linux-assigned pathnames.

Figure 3-12.

```
GCFI6e-01 Joe # df
Filesystem  1k-blocks      Used      Available  Use%  Mounted on
udev          4061368         0        4061368    0%  /dev
tmpfs          916548      9900         806648    2%  /run
/dev/sda1    69069427   8821436     4878744860  16%  /
...
/dev/sdh1     7847904    102804        7745100    2%  /media/joe/FC11-3D2E
/dev/sdi1      978672        48         978624    1%  /media/Joe/UDISK
```

Source: Linux Foundation.

Displaying a disk's file system

> **Note**
>
> Different distributions of Linux display slightly different names, as shown in **Figure 3-13**. For example, note that the /media directory in LinuxMint lists a joe subdirectory and an oem subdirectory. DeftZ Linux shows the /media directory's subdirectories as cdrom and root. Subdirectory names vary depending on the Linux distribution you're using. Remember to substitute the correct directory names for commands in this and other projects.

Figure 3-13.

```
GCFI6e-01 Joe # ls /media/joe/FC11-3D2E
GCFI-datacarve-FAT.dd  System Volume Information
GCFI6e-01 Joe # ls /media/joe/UDISK
System Volume Information
```

Source: Linux Foundation.

Examples of how different Linux distributions display the / media directory

Note

The following steps were performed in LinuxMint. These commands work the same in other Linux distributions and most Linux Live CDs. If necessary, replace the subdirectory name joe with the correct name for your distribution.

5. To determine which USB drive contains the image file GCFI-datacarve-FAT.dd and which one is empty of any data, type **ls /media/joe/FC11-3D2E** and press **Enter**, and then type **ls /media/joe/UDISK** (see Figure 3-14) and press **Enter**.

Note

Some USB drives have a hexadecimal number or a vendor-assigned name, such as the FC11-3D2E shown in **Figure 3-14**. Substitute the subdirectory names displayed with the commands in Step 5.

Figure 3-14.

```
GCFI6e ~ # dd if=/media/joe/FC11-3D2E/GCFI-datacarve-FAT.dd of=/dev/sdh1 bs=64
conv=noerror,sync status=progress
104262208 bytes (104 MB, 99 MiB) copied, 99.0001 s, 1.1 MB/s
1644552+0 records in
1644552+0 records out
105251328 bytes (105 MB, 100 MiB) copied, 99.7624 s, 1.1 MB/s
GCFI6E ~ #
```

Source: Linux Foundation.

Showing the contents of subdirectories in the /media/joe directory

Note

For this example, the UDISK subdirectory shows only the FAT System Volume Information file. The FC11-3D2E subdirectory shows the GCFI-datacarve-FAT.dd file, which will be restored from FC11-3D2E to UDISK.

6. Type **dd if=/media/joe/FC11-3D2E/GCFI-datacarve-FAT.dd of=/dev/sdh1 bs=64 conv=noerror,sync status=progress** and press **Enter**. Figure 3-15 shows the output.

Figure 3-15.

Example 1, from a LinuxMint distro

```
GCFI6e-01 Joe # ls /media
joe  oem
```

Example 2, from DeftZ Linux Live CD

```
[SH:2][DeftZ]: ls /media
cdrom  root
```

Source: Linux Foundation.

The dd command for restoring an image to a disk drive

7. When the data has finished copying, continue to the next project. If you're not continuing, close the terminal window and log off Linux.

Hands-On Project 3-4.

For this project, you use the dd command to make segmented image files of the restored USB drive created in Hands-On Project 3-3. To prepare, you need the following:

- One USB drive containing the restored image GCFI-datacarve-FAT.dd from Hands-On Project 3-3
- One USB drive formatted as FAT16 or FAT32 that can hold up to 120 MB
- A Linux distribution, Linux Live CD, or a computer running Linux with at least two USB ports

To make this acquisition, follow these steps:

1. If necessary, connect the two USB drives and boot the system to Linux, and then open a terminal window.
2. Type **su** and press **Enter**, and then type the root password, if necessary, and press **Enter**.
3. Type **df -h** and press **Enter** to list all devices attached to the computer and see the assigned pathnames.
4. Change your current working directory to the USB drive containing the GCFI-datacarve-FAT.dd file by typing **cd /media/*root*/*usbdrive*** and pressing **Enter**.

Note

Replace /root/*usbdrive* with the path listed in the df -h command output.

5. Examine the output of the df -h command from Step 3 to see how much space (under the Avail column) is available on the USB drive, /media/root/usbdrive. If there's less than 120 MB, type **rm GCFI-datacarve-FAT.dd** and press **Enter** to delete the file and make space for writing the segmented image files.

Note

Replace sdb with the USB drive that received the image file created in Hands-On Project 3-3. To reduce the number of segmented files, change the 50m to 650m or larger.

6. Type **dd if=/dev/sdb | split -b 50m - GCFI-datacarve-FAT. -d** and press **Enter**.

7. When the acquisition is finished, type **ls -l** and press **Enter** to see how many segmented files were produced.
8. Shut down the acquisition workstation, remove the USB drives, and remove the Linux Live CD, if necessary.

Case Projects

Case Project 3-1.

Your supervisor has asked you to research current acquisition tools. Using your preferred Internet search engine and the vendors listed in this chapter, prepare a report containing the following information for each tool and stating which tool you would prefer to use:

- Forensics vendor name
- Acquisition tool name and latest version number
- Features of the vendor's product

With this data collected, prepare a spreadsheet listing vendors in the rows. For the column headings, list the following features:

- Raw format
- Proprietary format
- AFF format
- Other proprietary formats the tool can read
- Compression of image files
- Remote network acquisition capabilities
- Method used to validate (MD5, SHA-1, and so on)

Case Project 3-2.

At a murder scene, you have started making an image of a computer's drive. You're in the back bedroom of the house, and a small fire has started in the kitchen. If the fire can't be extinguished, you have only a few minutes to acquire data from a 10 GB hard disk. Write one to two pages outlining your options for preserving the data.

Case Project 3-3.

You need to acquire an image of a disk on a computer that can't be removed from the scene, and you discover that it's a Linux computer. What are your options for acquiring the image? Write a brief paper specifying the hardware and software you would use.

Case Project 3-4.

A bank has hired your firm to investigate employee fraud. The bank uses four 20 TB machines on a LAN. You're permitted to talk to the network administrator, who is familiar with where the data is stored. What diplomatic strategies should you use? Which acquisition method should you use? Write a two-page report outlining the problems you expect to encounter, explaining how to rectify them, and describing your solution. Be sure to address any customer privacy issues.

Case Project 3-5.

You're investigating a case involving a 2 GB drive that you need to copy at the scene. Write one to two pages describing the three types of acquisitions—physical, logical, and sparse—you can use to copy the drive accurately. Be sure to include your software and media choices.

Case Project 3-6.

Your supervisor has asked you to list the acquisition tools available on a forensic Linux Live CD. Download the current ISO version of Deft (www.deftlinux.net), CAINE (www.caine-live.net), Kali Linux (www.kali.org), or Penguin Sleuth (www.linux-forensics.com), and then create a bootable CD or DVD of it. Start it on your workstation and survey its tools. Then write a one- to two-page report containing a brief description of each acquisition utility on the CD or DVD.

Chapter 4. Processing Crime and Incident Scenes

After reading this chapter and completing the exercises, you will be able to:

- Explain the rules for controlling digital evidence
- Describe how to collect evidence at private-sector incident scenes
- Explain guidelines for processing law enforcement crime scenes
- List the steps in preparing for an evidence search
- Describe how to secure a computer incident or crime scene
- Explain guidelines for seizing digital evidence at the scene
- List procedures for storing digital evidence
- Explain how to obtain a digital hash
- Review a case to identify requirements and plan your investigation

In this chapter, you learn how to process a digital investigation scene. Because this chapter focuses on investigation needs for computing systems and digital devices, you should supplement your training by studying police science or U.S. Department of Justice (DOJ) procedures to understand field-of-evidence recovery tasks. If you're in another country, be aware of laws relating to privacy, searches, and the rules of evidence for your region. In addition, consult local authorities, and refer to the excellent guidelines in ISO standard 27037 (introduced in **Chapter 1**).

Evidence rules are critical, whether you're on a civil or a criminal case. As you'll see, a civil case can quickly become a criminal case, and a criminal case can have civil implications larger than the criminal case. This chapter examines rules of evidence in the United States, but similar procedures apply in most courts worldwide. This chapter also describes differences between a business (private entity) and a law enforcement organization (public entity) in needs and concerns and discusses incident-scene processing for both types of investigations. Private-sector security officers often begin investigating private-sector digital crimes and then coordinate with law enforcement as they complete the investigation. Law enforcement investigators should, therefore, know how to process and manage incident scenes. Because public agencies usually don't have the funding to train officers continuously in technology advances, they must learn to work with private-sector investigators, whose employers can often afford to maintain their investigators' computing skills.

This chapter also discusses how the Fourth Amendment relates to private-sector and law enforcement digital investigations in the United States. Many countries have similar statutes or charters. As the world becomes more global or "flat" in nature, you need to be aware of how laws are interpreted in other countries. In addition, laws must be applied consistently as more countries establish e-laws and more cases go to court. Cases of fraud and money laundering are becoming more global issues, and crimes against consumers can originate from anywhere in the world. Computers and digital evidence seized in one jurisdiction might affect a case that's worldwide in scope.

To address these issues, this chapter explains how to apply standard crime scene practices and rules for handling evidence to private-sector and law enforcement digital investigations. You must handle digital evidence systematically so that you don't inadvertently alter or lose data. In addition, you should apply the same security controls to evidence for a civil lawsuit as evidence for a major crime. Federal and state rules of evidence govern both civil and criminal cases. However, the restrictions on how the government can proceed, as opposed to a private company, are much stricter. For example, as long as a policy exists, a company doesn't need a search warrant to examine a machine it owns; however, the government does. These rules are similar in English-speaking countries because they have a common ancestor in English common law (judge-made law), dating back to the late Middle Ages. However, laws in only 40% of the world are based on English or Dutch common law.

Identifying Digital Evidence

Digital evidence can be any information stored or transmitted in digital form. Because you can't see or touch digital data directly, it's difficult to explain and describe. Is digital evidence real or virtual? Does data on a disk or other storage medium physically exist, or does it merely represent real information? U.S. courts accept digital evidence as physical evidence, which means digital data is treated as a tangible object, such as a weapon, paper document, or visible injury, that's related to a criminal or civil incident. In addition, ISO standard 27037 gives guidance on what procedures countries should have in place for digital evidence. However, each country has its own interpretation of what can or can't be presented in court or accepted as evidence. Some countries used to require that all digital evidence be printed to be presented in court, and this requirement, at one time, was true for many U.S. states. Groups such as the **Scientific Working Group on Digital Evidence** (**SWGDE** ; www.swgde.org) set standards for recovering, preserving, and examining digital evidence.

Note

For more information on digital evidence, read "Electronic Crime Scene Investigation: A Guide for First Responders, 2nd edition," available at www.ncjrs.gov/pdffiles1/nij/219941.pdf. It has guidelines for U.S. law enforcement and other responders who protect an electronic crime scene and search for, collect, and preserve electronic evidence.

Following are the general tasks investigators perform when working with digital evidence:

- Identify digital information or artifacts that can be used as evidence.
- Collect, preserve, and document evidence.
- Analyze, identify, and organize evidence.
- Rebuild evidence or repeat a situation to verify that the results can be reproduced reliably.

Collecting digital devices while processing a crime or incident scene must be done systematically. To minimize confusion, reduce the risk of losing evidence, and avoid damaging evidence, only one team should collect and catalog digital evidence at a crime scene or lab, if practical. If there's too much evidence or too many systems to make it practical for one team to perform these tasks, all examiners must follow the same established operating procedures, and a lead or managing examiner should control collecting and cataloging evidence. You should also use standardized forms (discussed later in "**Documenting Evidence**") for tracking evidence to ensure that you consistently handle evidence in a safe, secure manner.

An important challenge investigators face is establishing recognized standards for digital evidence. For example, there are cases involving police raids being conducted simultaneously in many countries as well as anti-cartel investigations taking place in several locations around the world. As a result, hundreds of pieces of digital evidence, including hard drives, cell phones, and other storage devices, are seized in multiple sites. If law enforcement and civil organizations in these countries have agreed on proper procedures (generally, the highest control standard should be applied to evidence collection in all jurisdictions), the evidence can be presented in any jurisdiction confidently. Evidence collection is now even more complicated as mobile devices and cloud storage become the norm.

Understanding Rules of Evidence

Consistent practices help verify your work and enhance your credibility, so you must handle all evidence consistently. Apply the same security and accountability controls for evidence in a

civil lawsuit as in a major crime to comply with your state's rules of evidence or with the Federal Rules of Evidence (FRE). Also, keep in mind that evidence admitted in a criminal case might also be used in a civil suit, and vice versa. For example, suppose someone is charged with murder and acquitted at the criminal trial because the jury isn't convinced beyond a reasonable doubt of the person's guilt. If enough evidence shows that the accused's negligence contributed to a wrongful death, however, the victim's relatives can use the evidence in a civil lawsuit to recover damages.

Tip

You can review the Federal Rules of Evidence at www.uscourts.gov/uscourts/rules/rules-evidence.pdf.

As part of your professional growth, keep current on the latest rulings and directives on collecting, processing, storing, and admitting digital evidence. The following sections discuss some key concepts of digital evidence. You can find additional information at the U.S. Department of Justice Web site (www.usdoj.gov) and by searching the Internet for "digital evidence," "best evidence rule," "hearsay," and other relevant keywords. Consult with your prosecuting attorney, Crown attorney, corporate general counsel, or the attorney who retained you to learn more about managing evidence for your investigation.

In **Chapter 3**, you learned how to make an image of a disk as part of the process of gathering digital evidence. The data you discover from a forensic examination falls under your state's rules of evidence or the FRE. However, digital evidence is unlike other physical evidence because it can be changed more easily. The only way to detect these changes is to compare the original data with a duplicate. Furthermore, distinguishing a duplicate from the original electronically is challenging, so digital evidence requires special legal consideration.

Tip

If you're working in a country outside the United States, you need to verify its rules of evidence for electronic evidence. One resource is "An Investigation of Digital Forensics Concepts in an International Environment" (https://scholarworks.alaska.edu/handle/11122/4615), and you can also learn more about data and privacy laws by country at www.dlapiperdataprotection.com.

Another concern when dealing with digital records is the concept of hearsay, which is a statement made while testifying at a hearing by someone other than an actual witness to the event. For example, a rumor has been circulating around an office about an incident, or a friend mentioned it to the person being questioned; both situations are considered hearsay. The determination of what is or isn't hearsay can become particularly challenging when examining the contents of documents, text messages, e-mails, and other electronic files. The existence of these electronic files can't be disputed; however, their contents require eyewitness testimony or corroborating evidence. The definition of hearsay isn't difficult to understand, but it can be confusing when considering all the exceptions to the general rule against hearsay.

Like most common law nations, the United States excludes hearsay as spelled out in FRE Article VIII, Rule 802. Rules 803 and 804 cite more than 20 exceptions for when hearsay can be used. The following are some that apply to digital forensics investigations:

- Business records, including those of a public agency
- Certain public records and reports
- Evidence of the absence of a business record or entry

- Learned treatises used to question an expert witness
- Statements of the absence of a public record or entry

Tip

To see more exceptions to the hearsay rule, consult sources such as www.FindLaw.com.

The business-record exception, for example, allows "records of regularly conducted activity," such as business memos, reports, records, or data compilations. Business records are authenticated by verifying that they were created "at or near the time by, or from information transmitted by, a person with knowledge …" and are admissible "if the record was kept in the course of a regularly conducted business activity, and it was the regular practice of that business activity to make the record" (FRE, 803(6); see Section V, Evidence, in "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf).

In early 2017, changes were proposed to Rule 803 and are expected to be accepted into law by December 2017. Currently, if documents are older than 20 years (referred to as "ancient documents"), no testimony of their authenticity is needed. Because of e-mails and potential advances in technology, only documents created before 1998 will fall into this category. Updates to the FRE are also being made to address topics such as hash values.

Tip

For further discussion of the topic, go to www.discoveryadvocate.com/2017/01/17/ancient-data-and-documents-prepare-for-federal-changes-to-a-long-standing-hearsay-exception/.

In other common law countries, a distinction is made between "real computer evidence" and "hearsay computer evidence." A simplified explanation of this distinction states that you can, for example, prove an e-mail was sent and perhaps opened by a logged-in user. However, you can't necessarily verify the e-mail's contents. Generally, digital records are considered admissible if they qualify as a business record.

Another way of categorizing digital records is by dividing them into computer-generated records and computer-stored records. **Computer-generated records** are data the system maintains, such as system log files and proxy server logs. They are output generated from a computer process or algorithm, not usually data a person creates. **Computer-stored records** , however, are electronic data that a person creates and saves on a computer or digital device, such as a spreadsheet or word processing document. Some records combine computer-generated and computer-stored evidence, such as a spreadsheet containing mathematical operations (computer-generated records) generated from a person's input (computer-stored records).

Computer-generated and computer-stored records must also be shown to be authentic and trustworthy to be admitted into evidence. Computer-generated records are considered authentic if the program that created the output is functioning correctly. These records are usually considered exceptions to the hearsay rule. For computer-stored records to be admitted into court, they must also satisfy an exception to the hearsay rule, usually the business-record exception, so they must be authentic records of regularly conducted business activity. To show that computer-stored records are authentic, the person offering the records must demonstrate that a person created the data and the data is reliable and trustworthy—in other words, it wasn't altered when it was acquired or afterward.

Collecting evidence according to approved steps of evidence control helps ensure that the computer evidence is authentic, as does using established forensics software tools. Courts have consistently ruled that forensics investigators don't have to be subject matter experts on the tools they use. In *United States v. Salgado* (250 F.3d 438, 453, 6th Cir., 2001), the court stated, "It is not necessary that the computer programmer testify in order to authenticate computer-generated records." In other words, the witness must have first-hand knowledge only of facts relevant to the case. If you have to testify about your role in acquiring, preserving, and analyzing evidence, you don't have to know the inner workings of the tools you use, but you should understand their purpose and operation. For example, Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1) tools use complex algorithms. During a cross-examination, an opposing attorney might ask you to describe how these forensics tools work. You can safely testify that you don't know how the MD5 hashing algorithm works, but you can describe the steps for using the MD5 function in a specific tool, for instance.

Note

Even though research has forced collisions (meaning duplicate values) of the MD5 hash, it's still useful for forensic validation. Keep in mind that you can't generate the source string from the hash value. In addition, the probability of collisions affecting a case is remote.

When attorneys challenge digital evidence, often they raise the issue of whether computer-generated records were altered or damaged after they were created. In the case of *American Express v. Vinhnee* (9th Cir. Bk. App. Panel, 2005), the judge determined that American Express hadn't established that the records presented in court were authentic and the same as the original bill sent to Mr. Vinhnee. The company lost on appeal, too.

Attorneys might also question the authenticity of computer-generated records by challenging the program that created them. FRE 902, for example, refers to self-authenticating evidence, which includes public documents that are sealed and signed or certified. It also includes publications such as newspapers. Proposed changes to FRE 902 (b) are attempting to put an end to challenges based on computer-generated records being unreliable or having been tampered with. (For more information, see www.jdsupra.com/legalnews/new-amendments-to-federal-rule-of-22539/.)

To date, courts have been skeptical of unsupported claims about digital evidence. Asserting that the data changed without specific evidence isn't sufficient grounds to discredit the digital evidence's authenticity. Most federal courts that evaluate digital evidence from computer-generated records assume that the records contain hearsay. Federal courts then apply the business-records exception to hearsay as it relates to digital evidence.

As mentioned, one test to prove that computer-stored records are authentic is to demonstrate that a specific person created the records. Establishing who created digital evidence can be difficult, however, because records recovered from slack space or unallocated disk space usually don't identify the author. The same is true for other records, such as anonymous e-mails or text messages. To establish authorship of digital evidence in these cases, attorneys can use circumstantial evidence, which requires finding other clues associated with the suspect's computer or location. The circumstantial evidence might be that the computer has a password consistent with the password the suspect used on other systems, a witness saw the suspect at the computer at the time the offense occurred, or additional trace evidence associates the suspect with the computer at the time of the incident. In a recent case, the attorney chose not to use the digital evidence because although it could be proved that a particular camera was used to create the suspect's movies, CDs, and DVDs, there was no way to prove that the suspect was the person using the camera. Therefore, there was no circumstantial or corroborating evidence to prove that the suspect was guilty.

Although some files might not contain the author's name, in the arrest of the BTK strangler, the author of a Microsoft Word document was identified by using file metadata. In February 2005, the man claiming to be the BTK strangler sent a floppy disk to FOX News in Wichita. The police he had been taunting told him that they wouldn't be able to trace him via the floppy disk. Forensic examination of the disk came back with the name of the church and a user named Dennis, who turned out to be Dennis Rader, president of the congregation. The police had enough physical evidence to link him to the crimes. They arrested him, and he confessed to murdering 10 people over the course of 30 years. He was sentenced to 10 life terms. (For the full story, see the *ABA Journal* article at www.abajournal.com/magazine/article/how_the_cops_caught_btk/.)

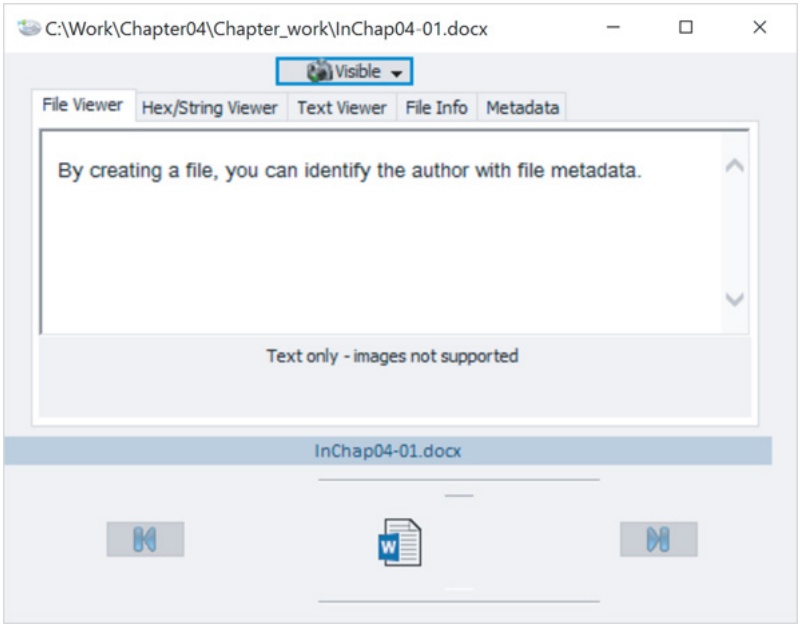
The following activity shows an easy way to identify this file metadata. Before starting this activity, go to www.osforensics.com/download.html and download the trial version of OSForensics. At the time of this writing, version 4.0.1002 is current. When you're finished, install the program, and then follow these steps.

Note

Before starting, create a *Work*\Chap04\Chapter folder on your system; it's referred to as your "work folder" in steps.

1. Start Microsoft Word, and in a new document, type **By creating a file, you can identify the author with file metadata**. Save it in your work folder as **InChap04-01.docx** (or **InChap04-01.doc** in earlier Word versions), and then exit Microsoft Word.
2. Start OSForensics by clicking **Start, OSForensics**. If Windows prompts you to confirm that you trust this program, click **OK** or **Yes**. Click **Continue Using Trial Version**, if prompted.
3. If you see a message asking whether you want to upgrade to the professional version, click the **Continue Using Trial Version** button.
4. In the OSForensics main window, notice the Viewers section in the right pane. Click **File** and **Hex Viewer**. In the "Select a file to open" dialog box that opens, navigate to your work folder and double-click the file you created in Step 1.
5. The dialog box that opens (see **Figure 4-1**) has five tabs. Click the **File Info** tab. You can see where the file is located along with the date and time it was created. Notice that the file size and its size on the disk are different.

Figure 4-1.

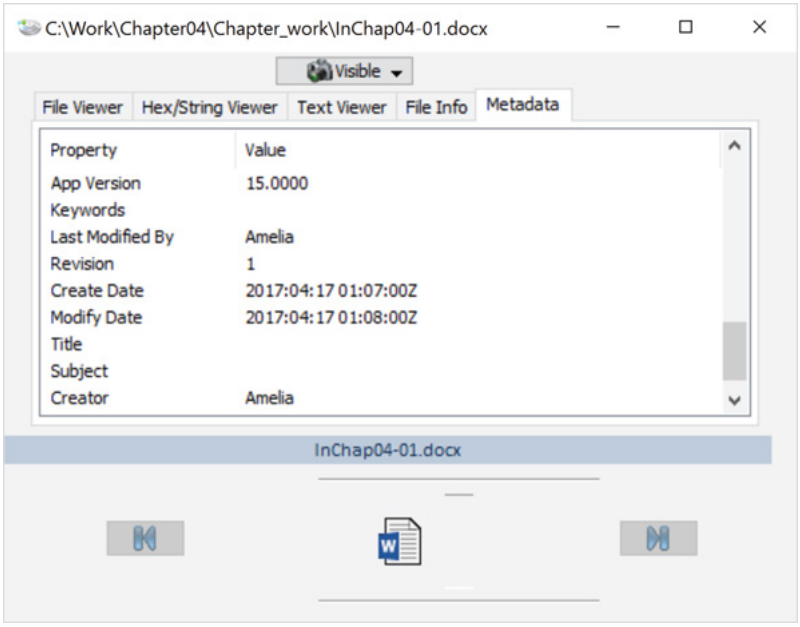


Source: PassMark Software, www.osforensics.com

Examining a file in OSForensics

6. Click the **Metadata** tab. The information in this tab includes file permissions, file type, file size, and other items. Scroll to the bottom of this tab, where you can see who created the file and who last modified the file (see Figure 4-2).

Figure 4-2.



Source: PassMark Software, www.osforensics.com

Viewing file metadata

7. Close the dialog box, and exit OSForensics by scrolling to the bottom of the left pane and clicking the **Exit** button.

In addition to revealing the author, computer-stored records must be proved authentic, which is the most difficult requirement when you're trying to qualify evidence as an exception to the

hearsay rule. The process of establishing digital evidence's trustworthiness originated with written documents and the "best evidence rule," which states that to prove the content of a written document, a recording, or a photograph, ordinarily the original file is required (as stated in Article X, Rule 1001, of the FRE). In addition, the original of a document is preferred to a duplicate. The best evidence, therefore, is the document created and saved on a computer's hard disk. However, Rule 1001, section (e), defines a duplicate done in a manner, including electronic, that "accurately reproduces the original." Moreover, Rule 1003 states that the duplicate can be used unless the original's authenticity is challenged.

Agents and prosecutors occasionally express concern that a printout of a computer-stored electronic file might not qualify as an original document, according to the best evidence rule. In its most fundamental form, the original file is a collection of 0s and 1s; in contrast, the printout is the result of manipulating the file through a complicated series of electronic and mechanical processes (FRE, 803(6); see "Searching and Seizing from Computers and Obtaining Electronic Evidence in Criminal Investigations," 2009). To address this concern about original evidence, the FRE states: "[I]f data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'" Instead of producing hard disks in court, attorneys can submit printed copies of files as evidence. In contrast, some countries and even some U.S. states used to allow only the printed version to be presented in court, not hard disks.

In addition, the FRE allows duplicates instead of originals when the duplicate is "produced by the same impression as the original … by mechanical or electronic re-recording … or by other equivalent techniques which accurately reproduce the original." Therefore, as long as bit-stream copies of data are created and maintained correctly, the copies can be admitted in court, although they aren't considered best evidence. The copied evidence can be a reliable working copy, but it's not considered the original. Courts understand that the original evidence might not be available, however. For example, you could make one image of the evidence drive successfully but lose access to the original drive because it has a head crash when you attempt to make a backup image. Your first successful copy then becomes secondary evidence. The attorney must be able to explain to the judge that circumstances beyond the examiner's control resulted in loss of the original evidence; in this case, the hard drive is no longer available to be examined or imaged. Mishaps with evidence happen routinely in all aspects of evidence recovery; the majority are caused by user error. Adhering to approved procedures can help prevent these mishaps.

Another example of not being able to use original evidence is investigations involving network servers. Removing a server from the network to acquire evidence data could cause harm to a business or its owner, who might be an innocent bystander to a crime or civil wrong. For example, Steve Jackson Games was the innocent party in a case in which evidence of criminal activity had been stored in e-mail on company computers. The network administrator had reported evidence of a crime committed by users of the company's bulletin board system (BBS) to the Secret Service. Secret Service agents seized all the computers at Steve Jackson Games and effectively put the company out of business. Steve Jackson Games sued the Secret Service, which was found liable for damages under the Privacy Protection Act and Title II of the Electronic Communications Privacy Act. For more information, see *Steve Jackson Games v. United States Secret Service and United States of America* (36 F.3d 457, USCA 5, 1994). (You can read about it at https://w2.eff.org/legal/cases/SJG/.) This case set the precedent for not resorting to such drastic measures, and as a result, they are no longer used. In this situation, you might not have the authority to create an image or remove the original drive. Instead, make your best effort to acquire the digital evidence with a less intrusive or disruptive method. In this context, the recovered materials become the best evidence because of the circumstances.

In summary, computer-generated records, such as system logs or the results of a mathematical formula in a spreadsheet, aren't hearsay. Computer-stored records that a person generates are

subject to rules governing hearsay, however. For the evidence to qualify as a business record exception to the hearsay rule, a person must have created the computer-stored records, and the records must be original. The FRE treats images and printouts of digital files as original evidence.

Collecting Evidence in Private-Sector Incident Scenes

Private-sector organizations include small to medium businesses, large corporations, and non-government organizations (NGOs), which might get funding from the government or other agencies. In the United States, NGOs and similar agencies must comply with state public disclosure and federal Freedom of Information Act (FOIA) laws and make certain documents available as public records. State public disclosure laws define state public records as open and available for inspection. For example, divorces recorded in a public office, such as a courthouse, become matters of public record unless a judge orders the documents sealed. Anyone can request a copy of a public divorce decree. **Figure 4-3** shows an excerpt of a public disclosure law for the state of Idaho.

Figure 4-3.

9-338. PUBLIC RECORDS -- RIGHT TO EXAMINE.

(1) Every person has a right to examine and take a copy of any public record of this state and there is a presumption that all public records in Idaho are open at all reasonable times for inspection except as otherwise expressly provided by statute.

(2) The right to copy public records shall include the right to make photographs or photographic or other copies while the records are in the possession of the custodian of the records using equipment provided by the public agency or independent public body corporate and politic or using equipment designated by the custodian.

(4) The custodian shall make no inquiry of any person who applies for a public record, except to verify the identity of a person requesting a record in accordance with section 9-342, Idaho Code, to ensure that the requested record or information will not be used for purposes of a mailing or telephone list prohibited by section 9-348, Idaho Code, or as otherwise provided by law. The person may be required to make a written request and provide their name, a mailing address and telephone number. [The custodian shall make no inquiry of any person who applies for a public record, except that the person may be required to make a written request and provide a mailing address and telephone number, and except as required for purposes of protecting personal information from disclosure under chapter 2, title 49, Idaho Code, and federal law.]

(5) The custodian shall not review, examine or scrutinize any copy, photograph or memoranda in the possession of any such person and shall extend to the person all reasonable comfort and facility for the full exercise of the right granted under this act.

Idaho public disclosure law

State public disclosure laws apply to state records, but the FOIA allows citizens to request copies of public documents created by federal agencies. The FOIA was originally enacted in the 1960s, and several subsequent amendments have broadened its laws. Some Web sites now provide copies of publicly accessible records for a fee.

ISPs and other communication companies make up a special category of private-sector businesses. ISPs can investigate computer abuse committed by their employees but not by customers. They must preserve customer privacy, especially when dealing with e-mail. However, federal regulations related to the Homeland Security Act and the PATRIOT Act of 2001 have redefined how ISPs and large organizations operate and maintain their records. ISPs and other communication companies can be called on to investigate customers' activities that are deemed to create an emergency situation. An emergency situation under the PATRIOT

Act is defined as the immediate risk of death or personal injury, such as finding a bomb threat in an e-mail.

As recent events have shown, the government monitors e-mails for the occurrence of keywords. Incidents such as the Edward Snowden case have made public the amount of electronic surveillance done by the U.S. government and the governments of other countries. Some provisions of these federal regulations have been revised over the past few years, so you should stay abreast of their implications. For example, in March 2017, the U.S. Congress voted to allow ISPs to sell customers' browsing histories without their explicit permission. (See www.congress.gov/bill/115th-congress/senate-joint-resolution/34 for more details.)

Investigating and controlling computer incident scenes in private-sector environments is much easier than in crime scenes. In the private sector, the incident scene is often a workplace, such as a contained office or manufacturing area, where a policy violation is being investigated. Everything from the computers used to violate a company policy to the surrounding facility is under a controlled authority—that is, company management. Typically, businesses have inventory databases of computer hardware and software. Having access to these databases and knowing what applications are on suspected computers help identify the forensics tools needed to analyze a policy violation and the best way to conduct the analysis. For example, companies might have a preferred Web browser, such as Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, or Google Chrome. Knowing which browser a suspect used helps you develop standard examination procedures to identify data downloaded to the suspect's workstation.

To investigate employees suspected of improper use of company digital assets, a company policy statement about misuse of digital assets allows private-sector investigators to conduct covert surveillance with little or no cause and access company computer systems and digital devices without a warrant, which is an advantage. Law enforcement investigators can't do the same, however, without sufficient reason for a warrant.

However, if a company doesn't display a warning banner or publish a policy stating that it reserves the right to inspect digital assets at will, employees have an expectation of privacy (as explained in **Chapter 1**). When an employee is being investigated, this expected privacy prevents the employer from legally conducting an intrusive investigation. A well-defined company policy, therefore, should state that an employer has the right to examine, inspect, or access any company-owned digital assets. If a company issues a policy statement to all employees, the employer can investigate digital assets at will without any privacy right restrictions; this practice might violate the privacy laws of countries in the EU, for example. As a standard practice, companies should use both warning banners and policy statements. For example, if an incident is escalated to a criminal complaint, prosecutors prefer showing juries warning banners instead of policy manuals. A warning banner leaves a much stronger impression on a jury.

In addition to making sure a company has a policy statement or a warning banner, private-sector investigators should know under what circumstances they can examine an employee's computer. With a policy statement, an employer can freely initiate any inquiry necessary to protect the company or organization. However, organizations must also have a well-defined process describing when an investigation can be initiated. At a minimum, most company policies require that employers have a "reasonable suspicion" that a law or policy is being violated. For example, if a policy states that employees can't use company computers for outside business and a supervisor notices a change in work behavior that could indicate an employee is violating this rule, generally it's enough to warrant an investigation. However, some countries require notifying employees that they're being investigated if they're suspected of criminal behavior at work.

If a private-sector investigator finds that an employee is committing or has committed a crime, the employer can file a criminal complaint with the police. Some businesses, such as banks,

have a regulatory requirement to report crimes. In the United States, the employer must turn over all evidence to the police for prosecution. If this evidence had been collected by a law enforcement officer, it would require a warrant, which would be difficult to get without sufficient probable cause. In “Processing Law Enforcement Crime Scenes” later in this chapter, you learn more about probable cause and how it applies to a criminal investigation.

Employers are usually interested in enforcing company policy, not seeking out and prosecuting employees, so typically they approve digital investigations only to identify employees who are misusing company assets. Private-sector investigators are, therefore, concerned mainly with protecting company assets, such as intellectual property. Finding evidence of a criminal act during an investigation escalates the investigation from an internal civil matter to an external criminal complaint. In some situations, such as the discovery of child pornography, the company or its agents must notify law enforcement immediately.

If you discover evidence of a crime during a company policy investigation, first determine whether the incident meets the elements of criminal law. You might have to consult with your organization’s attorney to determine whether the situation is a potential crime. Next, inform management of the incident; they might have other concerns, such as protecting confidential business data that could be included with the criminal evidence (called “commingled data”). In this case, coordinate with management and the organization’s attorney to determine the best way to protect commingled data. After you submit evidence containing sensitive information to the police, it becomes public record. Public record laws do include exceptions for protecting sensitive company information; ultimately, however, a judge decides what to protect.

After you discover illegal activity and document and report the crime, stop your investigation to make sure you don’t violate Fourth Amendment restrictions on obtaining evidence. If the information you supply is specific enough to meet the criteria for a search warrant, the police are responsible for obtaining a warrant that requests any new evidence. If you follow police instructions to gather additional evidence without a search warrant after you have reported the crime, you run the risk of becoming an agent of law enforcement. Instead, consult with your organization’s attorney on how to respond to a police request for information. The police and prosecutor should issue a subpoena for any additional new evidence, which minimizes your exposure to potential civil liability. In addition, you should keep all documentation of evidence collected to investigate an internal company policy violation. Later in this section, you learn more about using affidavits in an internal investigation.

One example of a company policy violation involves employees observing another employee accessing pornographic Web sites. If your organization’s policy requires you to determine whether any evidence supports this accusation, you could start by extracting log file data from the proxy server (used to connect a company LAN to the Internet) and conducting a forensic examination of the subject’s computer. Suppose that during your examination, you find adult and child pornography. Further examination of the subject’s hard disk reveals that the employee has been collecting child pornography in separate folders on his workstation’s hard drive. In the United States, possessing child pornography is a crime under federal and state criminal statutes. These situations aren’t uncommon and make life difficult for investigators who don’t want to be guilty of possession of this contraband on their forensic workstations.

You survey the remaining content of the subject’s drive and find that he’s a lead engineer for the team developing your company’s latest high-tech bicycle. He placed the child pornography images in a subfolder where the bicycle plans are stored. By doing so, he has commingled contraband with the company’s confidential design plans for the bicycle. Your discovery poses two problems in dealing with this contraband evidence. First, you must report the crime to the police; all U.S. states and most countries have legal and moral codes when evidence of sexual exploitation of children is found. Second, you must also protect sensitive company information. Letting the high-tech bicycle plans become part of the criminal evidence might make it public record, and the design work will then be available to competitors. Your first step

is to ask your organization's attorney how to deal with the commingled contraband data and sensitive design plans.

Your next step is to work with the attorney to write an affidavit confirming your findings. The attorney should indicate in the affidavit that the evidence is commingled with company secrets, and releasing the information will be detrimental to the company's financial health. When the affidavit is completed, you sign it before a notary, and then deliver the affidavit and the recovered evidence with log files to the police, where you make a criminal complaint. At the same time, the attorney goes to court and requests that all evidence recovered from the hard disk that's not related to the complaint and is a company trade secret be protected from public viewing. You and the attorney have reported the crime and taken steps to protect the sensitive data.

Now suppose the detective assigned to the case calls you. In the evidence you've turned over to the police, the detective notices that the suspect is collecting most of his contraband from e-mail attachments. The prosecutor needs you to collect more evidence to determine whether the suspect is transmitting contraband pictures to other potential suspects. The detective realizes that collecting more evidence might make you an agent of law enforcement and violate the employee's Fourth Amendment rights, so she writes an affidavit for a search warrant, ensuring that any subsequent instructions to you are legal. Before collecting any additional information, you wait until you or your organization's attorney gets a subpoena, search warrant, or other court order.

Processing Law Enforcement Crime Scenes

To process a crime scene correctly, you must be familiar with criminal rules of search and seizure. You should also understand how a search warrant works and what to do when you process one. For all criminal investigations in the United States, the Fourth Amendment limits how governments search and seize evidence. A law enforcement officer can search for and seize criminal evidence only with probable cause. **Probable cause** is the standard specifying whether a police officer has the right to make an arrest, conduct a personal or property search, or obtain a warrant for arrest. With probable cause, a police officer can obtain a search warrant from a judge to authorize a search and the seizure of specific evidence related to the criminal complaint.

The Fourth Amendment states that only warrants "particularly describing the place to be searched and the persons or things to be seized" can be issued. Note that this excerpt uses the word "particularly." The courts have determined that it means a warrant can authorize a search only of a specific place for a specific thing. Without *specific* evidence and the description of a particular location, a warrant might be weak and create problems later during prosecution. For example, stating that the evidence is in a house on Elm Avenue between Broadway and Main Street is too general, unless only one house fits that description, because several houses might be located in this area. Instead, provide specific information, such as "123 Elm Avenue." Most courts have allowed more general wording for digital evidence, however. For example, you can state that you want to seize a "computer and all associated parts" instead of specifying a "Dell Optiplex GXA." The DOJ document "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" (www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf, 2009) has an example of a search warrant affidavit for computer searches on the premises.

Although several court cases have allowed latitude when searching and seizing digital evidence, making your warrant as specific as possible to avoid challenges from defense attorneys is a good practice. Often a warrant is written and issued in haste because of the nature of the investigation. Law enforcement officers might not have the time to research the correct language for stating the nature of the complaint to meet probable cause requirements. However, because a judge can exclude evidence obtained from a poorly worded warrant, you should review these issues with your local prosecutor before investigating a case.

Understanding Concepts and Terms Used in Warrants

You should be familiar with warrant terminology governing the type of evidence that can be seized. Many digital investigations involve large amounts of data you must sort through to find evidence; the Enron case, for example, involved terabytes of information. Unrelated information (referred to as **innocent information**) is often included with the evidence you're trying to recover. It might be personal records of innocent people or confidential business information, for example. When you find commingled evidence, judges often issue a **limiting phrase** to the warrant, which allows the police to separate innocent information from evidence. The warrant must list which items can be seized.

When approaching or investigating a crime scene, you might find evidence related to the crime but not in the location the warrant specifies. You might also find evidence of another unrelated crime. In these situations, this evidence is subject to the plain view doctrine. The **plain view doctrine** states that objects falling in the direct sight of an officer who has the right to be in a location are subject to seizure without a warrant and can be introduced into evidence. For the plain view doctrine to apply, three criteria must be met:

- The officer is where he or she has a legal right to be.
- Ordinary senses must not be enhanced by advanced technology in any way, such as with binoculars.
- Any discovery must be by chance.

For the officer to seize the item, he or she must have probable cause to believe the item is evidence of a crime or is contraband. In addition, the police aren't permitted to move objects to get a better view. In *Arizona v. Hicks* (480 U.S. 321, 1987), the officer was found to have acted unlawfully because he moved stereo equipment, without probable cause, to record the serial numbers. The plain view doctrine has also been expanded to include the subdoctrines of plain feel, plain smell, and plain hearing.

In *Horton v. California* (496 U.S. 128, 1990), the court eliminated the requirement that the discovery of evidence in plain view be inadvertent. Previously, "inadvertent discovery" was required, which led to difficulties in defining this term. The three-prong Horton test requires the following:

- The officer must be lawfully present at the place where the evidence can be plainly viewed.
- The officer must have a lawful right of access to the object.
- The incriminating character of the object must be "immediately apparent."

Note

The plain view doctrine doesn't extend to supporting a general exploratory search from one object to another unless something incriminating is found (*Coolidge v. New Hampshire*, 403 U.S. 443, 466, 1971).

However, the plain view doctrine's applicability in the digital forensics world is being rejected. The U.S. Court of Appeals for the Ninth Circuit has directly addressed this doctrine and used it to give wide latitude to law enforcement (*United States v. Wong*, 334 F.3d 831, 9th Cir., 2003). Other circuit courts have been less willing to address applying the doctrine to computer searches. For example, police investigating a case have a search warrant authorizing the search of a computer for evidence related to illegal drug trafficking; during the search, the examiner observes an .avi file, opens it, and sees that it's child pornography. At that point, she must get

an additional warrant or an expansion of the existing warrant to continue the search for child pornography. This approach is consistent with rulings in *United States v. Carey* (172 F.3d 1268, 10th Cir., 1999) and *United States v. Walser* (275 F.3d 981, 10th Cir., 2001). In a more recent case that went to the Ninth Circuit Court of Appeals, the original search warrant was for 10 major league baseball players suspected of steroid use (*United States v. Comprehensive Drug Testing*, 2010). During the examination of files and e-mails, 200 more players were implicated. Forensics investigators see many files when they're searching for evidence, so in this case, their opinion was that the data was in plain view. However, the court disagreed. As with the example of discovering child pornography, a separate warrant for all other players should have been issued.

Preparing for a Search

Preparing for search and seizure of computers or digital devices is probably the most important step in digital investigations. The better you prepare, the smoother your investigation will be. The following sections discuss the tasks you should perform before you search for evidence. For these tasks, you might need to get answers from the victim (the complainant) and an informant, who could be a police detective assigned to the case, a law enforcement witness, or a manager or co-worker of the **person of interest** to the investigation.

Identifying the Nature of the Case

Recall from **Chapter 1** that when you're assigned a digital investigation case, you start by identifying the nature of the case, including whether it involves the private or public sector. For example, a private-sector investigation might involve an employee abusing Internet privileges by surfing the Web excessively or an employee who has filed an equal employment opportunity (EEO), e-mail harassment, or other ethics complaint. Serious cases might involve an employee abusing company digital assets to acquire or deliver contraband. Law enforcement cases could range from a check fraud ring to a homicide. The nature of the case dictates how you proceed and what types of assets or resources you need to use in the investigation (discussed in more detail in "Determining the Tools You Need" later in this chapter).

Identifying the Type of OS or Digital Device

Next, determine the type of OSs involved in the investigation. For law enforcement, this step might be difficult because the crime scene isn't controlled. You might not know what kinds of digital devices were used to commit a crime or how or where they were used. In this case, you must draw on your skills, creativity, and sources of knowledge, such as the Uniform Crime Report discussed in **Chapter 2**, to deal with the unknown.

If you can identify the OS or device, estimate the size of the storage device on suspect computers and determine how many digital devices you have to process at the scene. Also, determine what hardware might be involved, such as PCs or mobile devices, including smartphones, tablets, Fitbits, and laptops. Then you need to determine the OS: Microsoft, Linux, macOS, Apple iOS, Android, and so forth. For private-sector investigators, configuration management databases (discussed in **Chapter 2**) make this step easier. Consultants to the private sector or law enforcement officers might have to investigate more thoroughly to determine these details. You also need to consider cloud storage, which has become more widespread. Most smartphones, for example, are automatically backed up to the cloud, and people often store their files, music, and pictures in the cloud. You might need a separate warrant or subpoena to access this information.

Determining Whether You Can Seize Computers and Digital Devices

Generally, the ideal situation for incident or crime scenes is seizing computers and digital devices and taking them to your lab for further processing. However, the type of case and location of the evidence determine whether you can remove digital equipment from the scene. Law enforcement investigators need a warrant to remove computers from a crime scene and transport them to a lab. If removing the computers will irreparably harm a business, the computers shouldn't be taken offsite, unless you have disclosed the effect of the seizure to the judge. An additional complication is files stored offsite that are accessed remotely. You must decide whether the drives containing these files need to be examined. Another consideration is the availability of cloud storage, which essentially can't be located physically. The data is stored on drives where data from many other subscribers might be stored.

If you aren't allowed to take the computers and digital devices to your lab, determine the resources you need to acquire digital evidence and which tools can speed data acquisition. With large drives, such as a terabyte or more, acquisition times can increase to several hours. In **Chapter 3**, you examined data acquisition software and learned which tools meet needs for acquiring disk images. Some software compresses data while making forensic images. For large drives, this compression might be necessary.

Getting a Detailed Description of the Location

The more information you have about the location of a digital crime, the more efficiently you can gather evidence from the crime scene. Environmental and safety issues are the main concerns during this process. Before arriving at incident or crime scenes, identify potential hazards to your safety as well as that of other examiners.

Some cases involve dangerous settings, such as a drug bust of a methamphetamine lab or a terrorist attack using biological, chemical, or nuclear contaminants. For these types of investigations, you must rely on the skills of **hazardous materials (HAZMAT)** teams to recover evidence from the scene. The recovery process might include decontaminating digital components needed for the investigation, if possible. If the decontamination procedure might destroy electronic evidence, a HAZMAT specialist or an investigator in HAZMAT gear should make an image of a suspect's drive. If you have to rely on a HAZMAT specialist to acquire data, coach the specialist on how to connect cables and how to run the software. You must be exact and articulate in your instructions. Ambiguous or incorrect instructions could destroy evidence. Ideally, a digital forensics investigator trained in dealing with HAZMAT environments should acquire drive images. However, not all organizations have funds available for this training.

Whether you or a HAZMAT technician is the one acquiring an image, you should keep some guidelines in mind. Before acquiring the data, a HAZMAT technician might suggest that you put the target drive in a special HAZMAT bag, leaving the data and power cables out of the bag but creating an airtight seal around the cables to prevent any contaminants from entering the bag and affecting the target drive. When the data acquisition is finished, power down the computer and then disconnect the data and power cables from the target drive. The HAZMAT technician can then decontaminate the bag. When dealing with extreme conditions, such as biological or chemical hazardous contaminants, you might have to sacrifice equipment, such as data and power cables, to perform a task. In certain instances, such as a methamphetamine lab bust, the contaminants might be so toxic that hazards to the safety of others prohibit acquiring any digital evidence.

In addition, if the temperature in the contaminated room is higher than 80 degrees, you should take measures to avoid damage to the drive from overheating. In a dry desert region, consider cooling the target drive by using sealed ice packs or double-wrapped bags of ice so that moisture doesn't leak out and damage the drive. In extreme conditions, consider the risks to evidence and your equipment. You'll need to brainstorm for solutions to overcome these problems. Moving the equipment to a controlled environment is ideal; however, doing so isn't always possible.

Determining Who Is in Charge

As discussed in **Chapter 1**, a company needs an established line of authority to specify who can instigate or authorize an investigation. Private-sector investigations usually require only one person to respond to an incident or crime scene. Processing evidence usually involves acquiring an image of a suspect's drive. In law enforcement, however, many investigations need additional staff to collect all evidence quickly. For large-scale investigations, a crime or incident scene leader should be designated. Anyone assigned to a large-scale investigation scene should cooperate with the designated leader to ensure that the team addresses all details when collecting evidence.

Using Additional Technical Expertise

After you collect evidence data, determine whether you need specialized help to process the incident or crime scene. For example, suppose you're assigned to process a crime scene at a data center running Windows servers with several RAID drives and high-end Linux servers. If you're the lead on this investigation, you must identify the additional skills needed to process the crime scene, such as enlisting help with a high-end server OS. Other concerns are how to acquire data from RAID drives and how much data you can acquire. RAID servers typically process several terabytes of data, and standard imaging tools might not be able to handle such large data sets.

When working at high-end computing facilities, identify the applications the suspect uses, such as Oracle databases. You might need to recruit an Oracle specialist or site support staff to help extract data for the investigation. In addition, mobile devices (covered in **Chapter 12**) are found at most incident scenes, so having someone on hand who knows how to handle them is essential. Finding the right person with the necessary technical expertise can be an even bigger challenge than conducting the investigation.

If you do need to recruit a specialist who's not an investigator, develop a training program to educate the specialist in investigative techniques. This advice also applies to specialists you plan to supervise during search-and-seizure tasks. When dealing with digital evidence, an untrained specialist could destroy evidence unintentionally, no matter how careful you are in giving instructions and monitoring his or her activities.

Determining the Tools You Need

After you have gathered as much information as possible about the incident or crime scene, you can start listing what you need at the scene. Being overprepared is better than being underprepared, especially when you determine that you can't transfer the computer to your lab for processing.

To manage your tools, consider creating an initial-response field kit and an extensive-response field kit. Using the right kit makes processing an incident or crime scene much easier and minimizes how much you have to carry from your vehicle to the scene.

Your **initial-response field kit** should be lightweight and easy to transport. With this kit, you can arrive at a scene, acquire the data you need, and return to the lab as quickly as possible. Figure 4-4 shows some items you might need, and Table 4-1 lists the tools you might need in an initial-response field kit.

Figure 4-4.

Items in an initial-response field kit

Table 4-1. Tools in an Initial-Response Field Kit

Number needed	Tools
1	Small computer toolkit
1	Large-capacity drive
1	Set of Japanese Industrial Standard (JIS) screwdrivers
1	Set of ANSI screwdrivers
2	Antistatic wrist bands
1	IDE ribbon cable (ATA-33 or ATA-100)
1	SATA cables
1	Forensic boot media containing an acquisition utility
1	Laptop IDE 40- to 44-pin adapter, other adapter cables
1	Laptop or tablet computer
1	FireWire or USB dual write-protect external bay
1	Flashlight
1	Digital camera with extra batteries or 35mm camera with film and flash
10	Evidence log forms
1	Notebook or digital dictation recorder
10	Computer evidence bags (antistatic bags)
20	Evidence labels, tape, and tags
1	Permanent ink marker
10	USB drives (or a portable hard drive)

An **extensive-response field kit** should include all the tools you can afford to take to the field. When you arrive at the scene, you should extract only those items you need to acquire evidence. Doing so protects your equipment and minimizes how many items you have to keep

track of at the scene. Table 4-2 lists the tools you might need in an extensive-response field kit, including external USB drives.

Table 4-2. Tools in an Extensive-Response Field Kit

Number needed	Tools
Varies	Assorted technical manuals, ranging from OS references to forensic analysis guides
1	Initial-response field kit
1	Laptop or tablet with cables and connectors
2	Electrical power strips
1	Additional hand tools, including bolt cutters, pry bar, and hacksaw
1	Leather gloves and disposable latex gloves (assorted sizes)
1	Set of JIS screwdrivers
1	Set of ANSI screwdrivers
2	Antistatic wristbands
1	Hand truck and luggage cart
10	Large garbage bags and large cardboard boxes with packaging tape
1	Rubber bands of assorted sizes
1	Magnifying glass
1	Ream of printer paper
1	Small brush for cleaning dust from digital devices
10	USB drives of varying sizes
2	External hard drives (1 TB or larger) with power cables
Assorted	Converter cables
5	Additional assorted hard drives or USB drives for data acquisition

When deciding what items to include in initial-response and extensive-response field kits, you should also analyze needs specific to your region or organization. Refer to **Tables 4-1** and 4-2 for guidelines.

Preparing the Investigation Team

Before you initiate the search and seizure of digital evidence at incident or crime scenes, you must review all the available facts, plans, and objectives with the investigation team you have assembled. The goal of scene processing is to collect and secure digital evidence successfully. The better prepared you are, the fewer problems you encounter when you carry out the plan to collect data.

Keep in mind that digital evidence is volatile. Develop the skills to assess the facts quickly, make your plan, gather the needed resources, and collect data from the incident or crime scene. In some digital investigations, responding slowly might result in the loss of important evidence for the case.

Securing a Digital Incident or Crime Scene

Investigators secure an incident or crime scene to preserve the evidence and to keep information about the incident or crime confidential. Information made public could jeopardize the investigation. If you're in charge of securing a digital incident or crime scene, use barrier tape to prevent bystanders from entering the scene accidentally, and ask police officers or security guards to prevent others from entering the scene or taking photos and videos with smartphones and other digital devices. Legal authority for an incident scene includes trespassing violations; for a crime scene, it includes obstructing justice or failing to comply with a police officer. Access to the scene should be restricted to only those people who

have a specific reason to be there. The reason for the standard practice of securing an incident or a crime scene is to expand the area of control beyond the scene's immediate location. In this way, you avoid overlooking an area that might be part of the scene. Shrinking the scene's perimeter is easier than expanding it.

For major crime scenes, digital investigators aren't usually responsible for defining a scene's security perimeter. These cases involve other specialists and detectives who are collecting physical evidence and recording the scene. For incidents involving mostly computers, the computers can be a crime scene within a crime scene or a secondary crime scene, containing evidence to be processed. The evidence is in the computer, but the courts consider it physical evidence. Computers and other digital devices can also contain actual physical evidence, such as DNA evidence or fingerprints on keyboards. Crime labs can use special vacuums to extract DNA residue from a keyboard to compare with other DNA samples. In a major crime scene, law enforcement usually retains the keyboard and other peripherals.

Evidence is commonly lost or corrupted because of **professional curiosity** , which involves the presence of police officers and other professionals who aren't part of the crime scene–processing team. They just have a compelling interest in seeing what happened, but their presence could contaminate the scene directly or indirectly. Keep in mind that even those authorized and trained to search crime scenes can alter the scene or evidence inadvertently.

For example, during one homicide investigation, the lead detective collected a good latent fingerprint from the crime scene. He compared it with the victim's fingerprints and those of others who knew the victim, but he couldn't find a matching fingerprint. The detective suspected he had the murderer's fingerprint and kept it on file for several years until his police department purchased an **Automated Fingerprint Identification System (AFIS)** computer. During acceptance testing, the software vendor processed sample fingerprints to see how quickly and accurately the system could match fingerprints in the database. The detective asked the testing team to run the fingerprint he found at the homicide scene. He believed the suspect's fingerprints were in the AFIS database. The testing team complied and within minutes, AFIS found a near-perfect match of the latent fingerprint: It belonged to the detective.

Always remember that professional curiosity can destroy or corrupt evidence, including digital evidence. When working at an incident or crime scene, be aware of what you're doing and what you have touched, physically or virtually. A police detective can take elimination prints of everyone who had access to the crime scene to identify the fingerprints of known people; digital evidence doesn't have an equivalent elimination process. You must protect all digital evidence, so make sure no one examines a suspect's computer before you can capture and preserve an image of the hard disk. For example, starting a computer without forensic boot media alters important data, such as the date and timestamps of last access to certain files.

Seizing Digital Evidence at the Scene

With proper search warrants, law enforcement can seize all digital systems and peripherals. In private-sector investigations, you might have similar authority; however, you might have the authority only to make an image of the suspect's drive. Depending on company policies, private-sector investigators rarely have the authority to seize all computers and peripherals.

When seizing digital evidence in criminal investigations, follow the U.S. DOJ standards for seizing digital data (described later in this chapter, or see www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf). Another good source for both criminal and civil procedures is ISO standard 27037, which sets international standards for identifying, collecting, acquiring, and preserving digital evidence (www.iso27001security.com/html/27037.html). For civil investigations, you follow the same rules of evidence as for criminal investigations. You might be looking for specific evidence, such as a particular e-mail or spreadsheet. In a criminal matter, investigators seize entire

drives to preserve as much information as possible and make sure no evidence is overlooked. If you have any questions, doubts, or concerns, consult with your attorney for additional guidance.

Preparing to Acquire Digital Evidence

The evidence you acquire at the scene depends on the nature of the case and the alleged crime or violation. For a criminal case involving a drug dealer's computer, for example, you need to take the entire computer along with any peripherals and media in the area, including smartphones, USB devices, CDs/DVDs, printers, cameras, and scanners. You might also need to seize smart TVs, gaming systems, and other devices attached to the network. Seizing peripherals and other media ensures that you leave no necessary system components behind, but predicting what components might be critical to the system's operation is often difficult. On the other hand, if you're investigating employee misconduct, you might need only a few specific items.

Before you collect digital evidence, ask your supervisor or senior forensics examiner in the organization the following questions:

- Do you need to take the entire computer and all peripherals and media in the immediate area? How are you going to protect the computer and media while transporting them to your lab? This precaution includes blocking devices from accessing wireless networks while in transport.
- Is the computer powered on when you arrive? (This question is discussed in more detail later in "**Processing Incident or Crime Scenes** .")
- Is the suspect you're investigating in the immediate area of the computer? Is it possible the suspect damaged or destroyed the computer, peripherals, or media? Will you have to separate the suspect from the computer?

For example, suppose an employee, Edward Braun, is suspected of using a company computer at his desk to write a book. You suspect that Edward is saving personal files on the computer's hard drive. Using imaging software, you can copy the hard drive onto another drive, install the duplicate hard drive in the computer, and take the original drive to your forensics lab for examination. This procedure doesn't create a bit-for-bit copy; you're creating a working copy for continued business operations and taking the original for examination.

Because Edward's supervisors don't want him to know he's being investigated, you must create the working copy when he's not at his desk and isn't expected to return. Because most people notice when something is out of order on their desks, you should photograph the scene, measure the height of his chair, and record the position of items on his desk you need to move before removing the hard drive. (The following section has more tips on photographing and documenting the scene.) After you create an image of his hard drive and substitute the copy, return Edward's belongings to their original locations.

Processing Incident or Crime Scenes

The following guidelines offer suggestions on how to process incident or crime scenes. As you gain experience in performing searches and seizures, you can add to or modify these guidelines to meet the needs of specific cases. Use your judgment to determine what steps to take when processing a civil or criminal investigation. For any difficult issues, seek out legal counsel or other technical experts.

Keep a journal to document your activities. Include the date and time you arrive on the scene, the people you encounter, and notes on every important task you perform. Update the journal as you process the scene. With mobile devices, you can easily record a log of what you're doing; just be sure to check who has access to your mobile device.

To secure the scene, use whatever is practical to make sure only authorized people can access the area. Remove anyone who isn't investigating the scene unless you need his or her help to process the scene. For example, the company's network administrator might need to help you collect and recover data. As mentioned, you should secure a wider scene perimeter than necessary. Make sure nothing in this area, including digital evidence, moves until you have had time to record it. Be professional and courteous to any curious onlookers, but don't offer information about the investigation or incident or answer questions. Refer journalists to a public information officer or the organization's public relations manager.

Take video and still recordings of the area around the computer or digital device. Start by recording the overall scene, and then record details with close-up shots, including the back of all computers. Before recording the back of each computer, place numbered or lettered labels on each cable to help identify which cable is connected to which plug, in case you need to reassemble components at the lab. Make sure you take close-ups of all cable connections, including keyloggers (devices used to record keystrokes) and dongle devices used with software as part of the licensing agreement. Record the area around the computer, including the floor and ceiling, and all access points to the computer, such as doors and windows. Be sure to look under any tables or desks for anything taped to the underside of a table or desk drawer or on the floor out of view. If the area has ceiling panels—false ceiling tiles—remove them and record that area, too. Slowly pan or zoom the camera to prevent blurring in the video image, and maintain a camera log for all shots you take.

When you finish videotaping or photographing the scene, sketch the incident or crime scene. This sketch is usually a rough draft with notes on objects' dimensions and distances between fixed objects. For example, a note might read "The suspect's computer is on the south wall, three meters from the southeast corner of the room." When you prepare your report, you can make a clean, detailed drawing from your sketch, preferably using drawing software so that the sketch is in electronic form.

Because digital data is volatile, check the state of each computer or device at the scene as soon as possible. Determine whether the computer is powered on or off or in hibernation or sleep mode. If it's off, leave it off. If it's on, use your professional judgment on what to do next. Standard digital forensics practice has been to kill the computer's power to make sure data doesn't become corrupt through covert means. Typically, this procedure is still acceptable on older Windows and MS-DOS systems because turning off the power usually preserves data. On most Windows, UNIX, and Linux computers, generally you should do an orderly shutdown first. Every shutdown process has inherent risks, however; to avoid data loss, you or your supervisor might have to determine the best shutdown procedure.

In addition, there are many urban legends about criminals placing self-destruct mechanisms—both hardware and software devices—in computers. Many years ago, a common trick was altering the DOS program command.com by changing the dir (directory) command to the deltree (delete the directory tree) command. When an investigator entered the dir command on a suspect's computer, he would inadvertently start the deltree command, which deletes all files and folders and their contents. More advanced criminals have been known to create similar command-altering methods that overwrite a drive's contents. In addition, computer owners who suspect someone will investigate their computers might set the computer to delete the hard drive's contents if the correct screensaver password isn't entered.

As a general rule, don't cut electrical power to a running system unless it's an older Windows or MS-DOS system. However, it's a judgment call because of recent trends in digital crimes. More digital investigations now revolve around network and Internet-related cases, which rely heavily on log file data. Certain files, such as the Event log and Security log in Windows, might lose essential network activity records if power is terminated without a proper shutdown. Some government agencies, however, still teach investigators to "pull the plug"; it's the Digital Evidence First Responder's (DEFR's) judgment call.

If you're working on a network or Internet investigation and the computer is on, save data in any current applications as safely as possible and record all active windows or shell sessions. Don't examine folders or network connections or press any keys unless it's necessary. For systems that are powered on and running, photograph the screens. If windows are open but minimized, expanding them so that you can photograph them is safe. As a precaution, write down each window's contents.

As you're copying data on a live suspect computer, make notes in your journal about everything you do so that you can explain your actions in your formal report to prosecutors and other attorneys. When you've finished recording screen contents, save them to external media. For example, if one screen shows a Word file, save it to an external drive. Keep in mind that the suspect might have changed the file since last using the Save command. If another screen is a Web browser, take a screenshot or save the Web page to a USB drive or an external hard drive. If the suspect computer has an active connection to a network server with enough storage, you can save large files to a folder on the server. To do so, you need the network administrator's cooperation to direct you to the correct server and folder for storing the file.

If you can't save an open application to external media, save it to the suspect drive with a new filename. Changing the filename avoids overwriting an existing file that might not have been updated already. This method isn't ideal and should be done only in extreme emergency conditions. Remember that your goal is to preserve as much evidence in as good a condition as is practical.

After you have saved all active files on the suspect computer, you can close all applications. If an application prompts you to save before closing, don't save the files. When all applications are closed, perform an orderly shutdown. If you're not familiar with the correct shutdown method for the system you're examining, consult someone who has expertise in this procedure.

After you record the scene, shut down the system, and bag and tag the evidence, follow these steps:

1. Assign one person, if possible, to collect and log all evidence. Minimize the number of people handling evidence to ensure its integrity.
2. Tag all the evidence you collect with the current date and time, serial numbers or unique features, make and model, and name of the person who collected it.
3. Maintain two separate logs of collected evidence to be reconciled for audit control purposes and to verify everything you have collected.
4. Maintain constant control of the collected evidence and the crime or incident scene.

If the nature of the case doesn't permit you to seize the computer or digital device, create an image of the hard drive, as you learned in **Chapter 3**. Be sure to use critical investigative methods and look for other physical drives, and verify that the image you created corresponds to the device's physical size.

Note

In **Chapter 10**, you learn how to use forensics tools to acquire RAM. Many studies are being conducted on how to analyze RAM systematically, in an effort to find relevant information in what seems to look like random garbage data.

During the data acquisition or immediately after collecting the evidence, look for information related to the investigation, such as passwords, passphrases, personal identification numbers (PINs), and bank account numbers (particularly offshore bank accounts, often used to hide evidence of financial transactions). This information might be in plain view or out of sight in a

drawer or trashcan. At the scene, collect as much personal information as possible about the suspect or victim. Collect all information related to facts about the crime or incident, particularly anything that connects the suspect to the victim.

To finish your analysis and processing of a scene, collect all documentation and media related to the investigation, including the following material:

- Hardware, including mobile and peripheral devices
- Software, including OSs and applications
- All media, such as USB drives, backup tapes, and disks
- All documentation, manuals, printouts, and handwritten notes

Processing Data Centers with RAID Systems

Digital investigators sometimes perform forensics analysis on RAID systems or server farms, which are rooms filled with extremely large disk systems and are typical of large business data centers, such as banks, insurance companies, and ISPs. As you learned in **Chapter 3**, one technique for extracting evidence from large systems is sparse acquisition. This technique extracts only data related to evidence for your case from allocated files and minimizes how much data you need to analyze. A drawback of this technique is that it doesn't recover data in free or slack space. If you have a digital forensics tool that accesses unallocated space on a RAID system, work with the tool on a test system first to make sure it doesn't corrupt the RAID system.

Using a Technical Advisor

When working with advanced technologies, recruit a technical advisor who can help you list the tools you need to process the incident or crime scene. At large data centers, the technical advisor is the person guiding you about where to locate data and helping you extract log records or other evidence from large RAID servers. In law enforcement cases, the technical advisor can help create the search warrant by itemizing what you need for the warrant. If you use a technical advisor for this purpose, you should list his or her name in the warrant. At the scene, a technical advisor can help direct other investigators to collect evidence correctly. Technical advisors have the following responsibilities:

- Know all aspects of the system being seized and searched.
- Direct investigators on how to handle sensitive media and systems to prevent damage.
- Help ensure security of the scene.
- Help document the planning strategy for the search and seizure.
- Conduct ad hoc training for investigators on the technologies and components being seized and searched.
- Document activities during the search and seizure.
- Help conduct the search and seizure.

Documenting Evidence in the Lab

After you collect digital evidence at the scene, you transport it to a forensics lab, which should be a controlled environment that ensures the security and integrity of digital evidence. In any investigative work, be sure to record your activities and findings as you work. To do so, you can maintain a journal to record the steps you take as you process evidence. Your goal is to be able to reproduce the same results when you or another investigator repeat the steps you took to collect evidence.

If you get different results when you repeat the steps, the credibility of your evidence becomes questionable. At best, the evidence's value is compromised; at worst, the evidence will be disqualified. Because of the nature of electronic components, failures do occur. For example, you might not be able to repeat a data recovery because of a hardware failure, such as a disk drive head crash. Be sure to report all facts and events as they occur.

Besides verifying your work, a journal serves as a reference that documents the methods you used to process digital evidence. You and others can use it for training and guidance on other investigations.

Processing and Handling Digital Evidence

You must maintain the integrity of digital evidence in the lab as you do when collecting it in the field. Your first task is to preserve the disk data. If you have a suspect computer that hasn't been copied with an imaging tool, you must create a copy. When you do, be sure to make the suspect drive read-only (typically by using a write-blocking device), and document this step. If the disk has been copied with an imaging tool, you must preserve the image files. With most imaging tools, you can create smaller, compressed volume sets to make archiving your data easier.

In **Chapter 3**, you learned how to use imaging tools, and in Chapter 1, you examined the steps for preserving digital evidence with chain-of-custody controls. You use the following steps to create image files:

1. Copy all image files to a terabyte drive or a storage area network (SAN). Most forensics labs have several machines set up with disk-imaging software and multiple hard drives that can be exchanged as needed for your cases. You can use these resources to copy image files to large drives. Some might be equipped with large network storage devices for ongoing cases.
2. Start your forensics tool to access and open the image files.
3. Run an MD5 or SHA-1 hashing algorithm on the image files to get a digital hash. Later in "Obtaining a Digital Hash," you learn how to compare MD5 or SHA-1 hashes to make sure the evidence hasn't changed.
4. When you finish copying image files to a larger drive, secure the original media in an evidence locker. Don't work with the original media; it should be stored in a locker that has an evidence custody form. Be sure to fill out the form and date it.

Storing Digital Evidence

With digital evidence, you need to consider how and on what type of media to save it and what type of storage device is recommended to secure it. The choice of media for storing digital evidence usually depends on how long you need to keep it. If you investigate criminal matters, store the evidence as long as you can. The ideal storage media for digital data used to be CDs and DVDs. (CDs from the 1980s could last up to 5 years. The expected lifespan of CDs and DVDs is now 2 to 5 years.) The optimum choice now is solid-state USB drives. Although they're more expensive than CDs and DVDs, they're more durable.

You can also use magnetic tape to preserve evidence data. The 4-mm DAT magnetic tapes store from 40 to 72 GB or more of data, but they're slow at reading and writing data. If you're using these tapes, test stored data by copying the contents from the tape back to a disk drive. Then verify that the data is good by examining it with forensics tools or doing an MD5 hash comparison of the original data and the newly restored data.

Evidence is routinely kept for long periods. In the United States, for example, tens of thousands of rape kits kept in storage have never been processed, and as you've probably heard, cold cases from 20, 30, or even 50 years ago are now being solved because of advances in technology. You never know when a case might be solved or go to trial, so you need to make

sure evidence is preserved for the long term. If a 30-year lifespan for data storage is acceptable for your digital evidence, older DLT magnetic tape cartridge systems are a good choice. Keep in mind that you never know how long it will take for a case to go to trial. DLT systems have been used with mainframe computers for several decades and are reliable data-archiving systems. Depending on the size of the DLT cartridge, one cartridge can store up to 80 GB of data in compressed mode. Speed of data transfer from a hard drive to a DLT tape is also faster than transferring data to a CD or DVD. The only major drawback of a DLT drive and tapes is cost. A drive can cost from $400 to $800, and each tape is about $40. However, with the current large disk drives, the DLT system does offer substantial labor savings over other systems.

Manufacturers such as Quantum Corp. introduced a high-speed, high-capacity tape cartridge drive system called Super Digital Linear Tape (Super-DLT or SDLT). These systems are specifically designed for large RAID data backups and can store more than 1 TB of data. Smaller external SDLT drives can connect to a workstation through a SCSI card. In addition, many external USB drives can hold 1 or more TB of information. Reliable offsite storage and encrypted cloud storage are other options.

Don't rely on one media storage method to preserve your evidence, however. Be sure to make two copies of every image to prevent data loss. Also, if practical, use different tools to create the two images because every tool has strengths and weaknesses. For example, you can use the Linux dd command to create the first image and FTK Imager Lite to create the second image.

Evidence Retention and Media Storage Needs

To help maintain the chain of custody for digital evidence so that it's accepted in court or by arbitration, restrict access to your lab and evidence storage area. When your lab is open for operations, authorized personnel must keep these areas under constant supervision. When your lab is closed, at least two security workers should guard evidence storage cabinets and lab facilities.

As a good security practice, your lab should have a sign-in roster for all visitors. Most labs use a manual log system that an authorized technician maintains when an evidence storage container is opened and closed. Some facilities have upgraded to electronic systems that meet statutes, but many prefer the tried-and-true manual logs. These logs should be maintained for a period based on legal requirements, including the statute of limitations, the maximum sentence, and expiration of appeal periods. Make the logs available for management to inspect. The evidence custody form should contain an entry for every person who handles the evidence (see **Figure 4-5**).

Figure 4-5.

Item description:				
Item tag number:				
Person	Date logged out	Time logged out	Date logged in	Time logged in

A sample log file

If you're supporting a law enforcement agency, you might need to retain evidence indefinitely, depending on the type of crime. Check with your local prosecuting attorney's office or state laws to make sure you're in compliance. For the private sector, check with the organization's legal department (the general counsel), which is responsible for setting standards for evidence retention. Cases in which child pornography is discovered are the exception: The evidence must be examined by law enforcement. As a private-sector investigator, you aren't allowed to examine these files. You have to stop what you're doing and call federal investigators. This material is contraband and must not be stored by any person or organization other than a law enforcement agency.

Documenting Evidence

To document evidence, create or use an evidence custody form (shown in **Chapter 1**). Because of constant changes in technologies and methods for acquiring data, create an electronic evidence custody form that you can modify as needed. An evidence custody form serves the following functions:

- Identifies the evidence
- Identifies who has handled the evidence
- Lists dates and times the evidence was handled

After you have established these pieces of information, you can add others to your form, such as a section listing MD5 and SHA-1 hash values. Include any detailed information you might need to reference.

Evidence bags also include labels or evidence forms you can use to document your evidence. Commercial companies offer a variety of sizes and styles of paper and plastic evidence bags. Be sure to write on the bag when it's empty, not when it contains digital evidence, to make sure your writing is legible and to avoid damaging the evidence. You should use antistatic bags for electronic components.

Obtaining a Digital Hash

To verify data integrity, different methods of obtaining a unique identity for file data have been developed. One of the first methods was the **Cyclic Redundancy Check (CRC)** , a mathematical algorithm that determines whether a file's contents have changed. The most recent version is CRC-32. CRC, however, is not considered a forensic hashing algorithm. The first algorithm used for digital forensics was **Message Digest 5 (MD5)** . Like CRC, MD5 is a mathematical formula that generates a hexadecimal code, or **hash value** , based on the contents of a file, a folder, or an entire drive. If a bit or byte in the file changes, it alters the hash value, a unique hexadecimal value that can be used to verify that a file or drive hasn't changed or been tampered with. Before you process or analyze a file, you can use a software tool to calculate its hash value. After you process the file, you produce another digital hash. If it's the same as the original one, you can verify the integrity of your digital evidence with mathematical proof that the file didn't change.

According to work done by Wang Xiaoyun and her associates from Beijing's Tsinghua University and Shandong University of Technology, there are three rules for forensic hashes:

- You can't predict the hash value of a file or device.
- No two hash values can be the same. (Note that collisions have occurred in research using supercomputers.)
- If anything changes in the file or device, the hash value must change.

Another hashing algorithm is **Secure Hash Algorithm version 1 (SHA-1)** , developed by the **National Institute of Standards and Technology (NIST)** . SHA-1 has slowly replaced MD5

and CRC-32, although MD5 is still widely used. (For more information on SHA-1, see http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf.) In both MD5 and SHA-1, collisions have occurred, meaning two different files have the same hash value. Collisions are rare, however, and despite flaws in MD5 and SHA-1, both are still used for validating digital evidence collected from files and storage media. If a collision is suspected, you can do a byte-by-byte comparison to verify that all bytes are identical. Byte-by-byte comparisons can be done with the MS-DOS comp command or the Linux/UNIX diff command. New developments in this field happen constantly, however, so staying current by investigating the NIST Web site and reading related journals is a good idea. New versions, such as SHA 256, are already being used.

Most digital forensics hashing needs can be satisfied with a **nonkeyed hash set** , which is a unique hash number generated by a software tool, such as the Linux md5sum command. The advantage of this type of hash is that it can identify known files, such as executable programs or viruses, that hide themselves by changing their names. For example, many people who view or transmit pornographic material change filenames and extensions to obscure the nature of the contents. However, even if a file's name and extension change, the hash value doesn't.

The alternative to a nonkeyed hash is a **keyed hash set** , which is created by an encryption utility's secret key. You can use the secret key to create a unique hash value for a file. Although a keyed hash set can't identify files as nonkeyed hash methods can, it can produce a unique hash set for digital evidence.

You can use the MD5 function in FTK Imager to obtain the digital signature of a file or an entire drive. In the following activity, you use a USB drive, although you often work with hard drives in actual investigations. First, you create a test file and then generate an MD5 hash value for it. Then you change the file and produce another MD5 hash value, this time noting the change in the hash value. You need a blank, formatted USB drive and a Windows computer for the following steps:

1. Power on your forensic workstation, booting it to Windows.
2. Insert a blank, formatted USB drive into your computer.
3. Start Notepad. In a new text file, type **This is a test to see how an MD5 digital hash works**.
4. Click **File**, **Save As** from the menu. In the File name text box, type **InChap04.txt** . Navigate to your USB drive, and then click **Save**.
5. Exit Notepad.

Next, you use FTK Imager Lite to determine the MD5 and SHA-1 hash values:

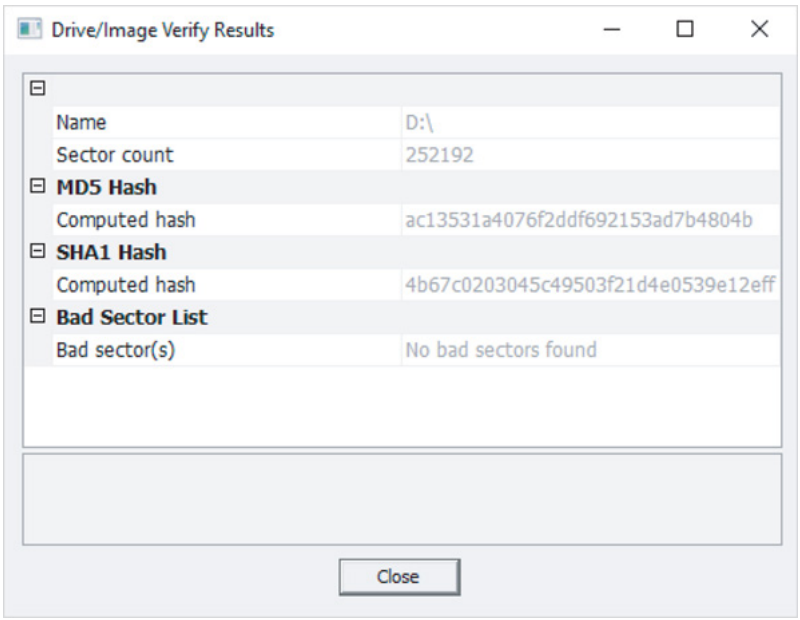
Note

If you didn't install FTK Imager Lite in **Chapter 3**, do so before performing these steps.

1. Start FTK Imager Lite. Click **Yes** in the UAC message box, if necessary.
2. Click **File**, **Add Evidence Item** from the menu. In the Select Source dialog box, click the **Logical Drive** option button, and then click **Next**.
3. In the Select Drive dialog box, click the **Source Drive Selection** list arrow, click your USB drive in the drop-down list, and then click **Finish**.
4. Right-click the USB drive at the upper left and click **Verify Drive/Image**. The verification process takes a few minutes. When it finishes, you should see a dialog box similar to Figure 4-6. Copy the MD5 and SHA-1 hash values for this file to a text file in

Notepad, and then click **Close**. Click **Save**, and save the text file in your work folder with a filename of your choosing. Close the Drive/Image Verify Results dialog box.

Figure 4-6.



Source: AccessData Group, Inc., www.accessdata.com

Using FTK Imager Lite to verify hash values

5. In FTK Imager, click **File**, **Remove Evidence Item** from the menu. (You're about to make changes to the file and don't want it open in FTK Imager while you do so.) Leave FTK Imager running for the next set of steps.

Now you change the text file:

1. Start Notepad, and open the **InChap04.txt** file.
2. Delete one word from the sentence. Click **File**, **Save**, and save the file with the same filename.
3. Repeat the previous activity's steps in FTK Imager to generate MD5 and SHA-1 hash values. Open the file containing the original hash values from **Step 4** in the preceding activity to compare the hash values. They should be different from the original hash values you found for this file. When you're finished, exit FTK Imager.

Reviewing a Case

Chapter 1 introduced tasks for planning your investigation, some of which are repeated in the following list. Later in this section, you apply each task to a hypothetical investigation to create a preparation plan for searching incident or crime scenes. The following are the general tasks you perform in any digital forensics case:

- Identify the case requirements.
- Plan your investigation.
- Conduct the investigation.
- Complete the case report.
- Critique the case.

The following sections give you an example of civil and criminal investigations, and then you review how to perform some of these general tasks in a case involving a hypothetical company.

Sample Civil Investigation

Most cases in the private sector are considered **low-level investigations** , or noncriminal cases. This doesn't mean private-sector investigations are less important; it means they require less effort than a major criminal case. The example of a low-level civil investigation in this section is an e-mail investigation that resulted in a lawsuit between two businesses. An investigation of this nature requires examining only e-mail messages, not a complete disk forensics analysis.

Mr. Jones at Company A claims to have received an order for $200,000 in widgets from the purchasing manager, Mr. Smith, at Company B. Company A manufactures the widgets and notifies Company B that they're ready for shipment. Mr. Smith at Company B replies that they didn't order any widgets and won't pay for them. Company A locates an e-mail requesting the widgets that appears to be from Mr. Smith and informs Company B about the e-mail. Company B tells Company A that the e-mail didn't originate from its e-mail server, and it won't pay for the widgets.

Company A files a lawsuit against Company B based on the widget order in Mr. Smith's e-mail. The lawyers for Company A contact the lawyers for Company B and discuss the lawsuit. Company A's lawyers make discovery demands to conduct a digital forensics analysis on Mr. Smith's computer in hopes of finding the original message that caused the problem. At the same time, Company B's lawyers demand discovery on Mr. Jones's computer because they believe the e-mail is a fake.

You're a digital investigator and get a call from your boss asking you to fulfill the discovery demands from Company B's lawyers to find the e-mail message on Mr. Jones's computer and determine whether it's real or fake. Because it's an e-mail investigation, not a major crime involving computers, you're dispatched to Company A. When you get there, you find Mr. Jones's computer powered on and running Microsoft Outlook. The discovery order authorizes you to recover only Mr. Jones's Outlook e-mail folder, the .pst file. You aren't authorized to do anything else. In this situation, you take the following steps:

1. Exit the Outlook program on Mr. Jones's computer.
2. Use File Explorer to find the Outlook .pst file containing his business e-mail. You might need to use the Windows Search feature to find files with a .pst extension.
3. Determine how large the .pst file is and connect a suitable storage device, such as a USB drive, to Mr. Jones's computer.
4. Copy the .pst file to the USB drive, and then remove the USB drive.
5. Fill out your evidence form, stating where on Mr. Jones's disk you found the .pst file, along with the date and time you performed this task.
6. Leave Company A and return to your forensics lab. Place the USB drive in your evidence safe.

For most civil investigations, you collect only specific items that have been determined germane by lawyers or the Human Resources Department.

Another activity common in the private sector is **covert surveillance** of employees who are abusing their computing and network privileges. The use of covert surveillance of employees must be well defined in company policy before it can be carried out. If a company doesn't have a policy that informs employees they have no privacy rights when using company computers and digital devices, no surveillance can be conducted without exposing the company to civil or even criminal liability. If no policy exists, the company must create a policy and notify all

employees about the new rules. The Legal Department should create policy language appropriate for your state or country and define the rights and authority the company has in conducting surveillance of employees according to provincial, state, or country privacy laws.

For covert surveillance, you set up monitoring tools that record a suspect's activity in real time. Real-time surveillance requires **sniffing** data transmissions between a suspect's computer and a network server. Network sniffer tools, such as Wireshark, allow network administrators and others to determine what data is being transmitted over the network. Other data-collecting tools (called keylogger programs—Spector and TrueActive Software, for example) are screen capture programs that collect most or all screens and keystrokes on a suspect's computer. Most of these tools run on Windows and usually collect data through remote network connections. The tools are hidden or disguised as other programs in Windows Task Manager and process logs.

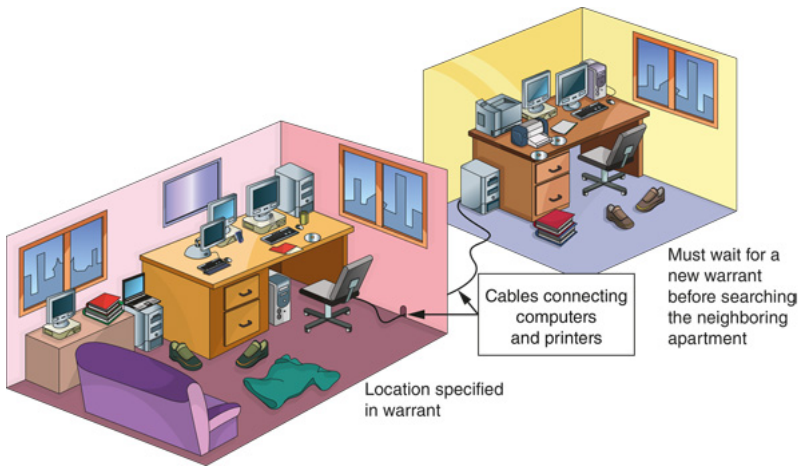
Another covert surveillance product is Guidance Software EnCase Enterprise Edition (EEE), which is a centrally located server with specialized software that can activate servlets over a network to remote workstations. Digital investigators can perform forensics examinations in real time through this remote connection to a suspect's computer.

An Example of a Criminal Investigation

Crime scenes involving computers range from fraud cases to homicides. Because high-quality printers are now available, one of the most common computer-related crimes is check fraud. Many check fraud cases also involve making and selling false ID cards, such as driver's licenses.

In one case, the police received a tip that a check-forging operation was active in an apartment building. After the detective contacted a reliable informant, he had enough information for a search warrant and asked the patrol division to assist him in serving the warrant. When the detective entered the suspect's apartment and conducted a preliminary search, he found a network of six high-end workstations with cables connected to devices in the adjacent apartment through a hole in the wall (see **Figure 4-7**). Unfortunately, the warrant specified a search of only one apartment.

Figure 4-7.



Search warrant limits

The detective contacted the deputy prosecutor, who instructed him to stand guard at both apartments until she could have a judge issue an additional warrant for the neighboring apartment. When he received the second search warrant, the detective entered the adjoining apartment and continued his search, finding more computers, high-quality color laser printers, checks, and stolen blank driver's licenses. The outcome of the investigation revealed that the perpetrators were three enterprising high school students who were selling fake IDs

to fellow students. The check fraud scheme was a new sideline they were developing to improve their cash flow.

Reviewing Background Information for a Case

In some activities and projects in this book, you use data files from the hypothetical M57 Patents case. These files were developed with a National Science Foundation (NSF) grant for digital forensics students; they are full images of drives with Microsoft proprietary information redacted. A hypothetical startup company, M57 Patents, was in business for about a month, doing art patent searches. Later, a computer sold on Craigslist was discovered to contain "kitty" porn. It was traced back to M57 Patents, and an employee is suspected of downloading the porn.

Note

For more details of the case, read the PDF files (M57-Patents Parts 1, 2, and 3) that are in this chapter's downloads section of the student companion site for this book.

Planning the Investigation

In this case, the main players are the CEO, Pat McGoo; the IT person, Terry; and the patent researchers, Jo and Charlie. The police seized the digital evidence at the scene and made forensic copies of the following evidence:

- The image of the computer sold on Craigslist
- The images of five other machines found at the M57 Patents office
- The images of four USB drives found at M57 Patents
- RAM from the imaged machines
- Network data from the M57 Patents servers

Conducting the Investigation: Acquiring Evidence with OSForensics

In the following activity, you use OSForensics to analyze an image file. In **Chapters 1** and 3, you learned how to acquire an image of a drive. To prepare OSForensics for analyzing the image of a suspect USB drive, follow these steps:

Note

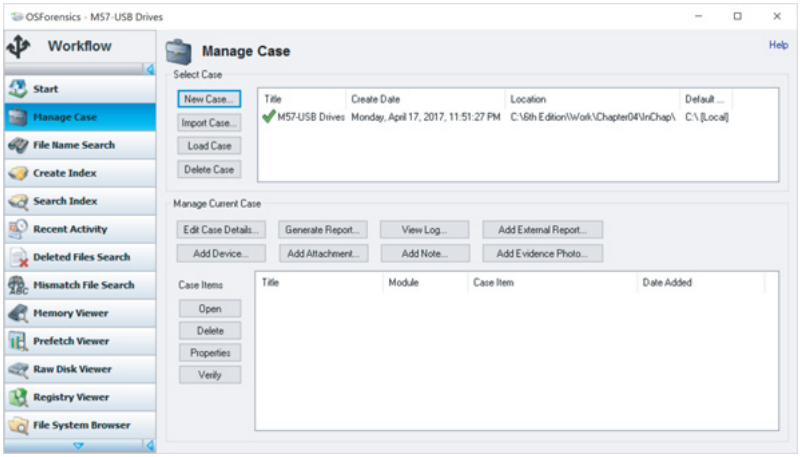
If you haven't already done so, create a subfolder of your work folder called Chapter so that the path is *Work*\Chap04\Chapter.

1. Go to the student companion site for this book. Scroll to the downloads section for this chapter, and download all four USB drive images to your work folder. Some are used in later activities and projects. (If you haven't done so already, download the PDF files, too, for background information on this case.)
2. Start OSForensics. If prompted to allow the program to make changes to your computer, click **OK** or **Yes**. In the OSForensics message box, click **Continue Using Trial Version**.
3. Click **Start** in the left pane, if necessary. In the right pane, click **Create Case**.
4. In the New Case dialog box, enter your name. For the case name, type **M57-USB drives**. Fill in the contact details and the organization, and then click **Investigate**

Disk(s) from Another Machine.

5. Click **Custom Location** for the case folder. Click the **Browse** button on the lower right, navigate to and click your work folder, and then click **OK** twice. You should see the Manage Case window (see Figure 4-8).

Figure 4-8.



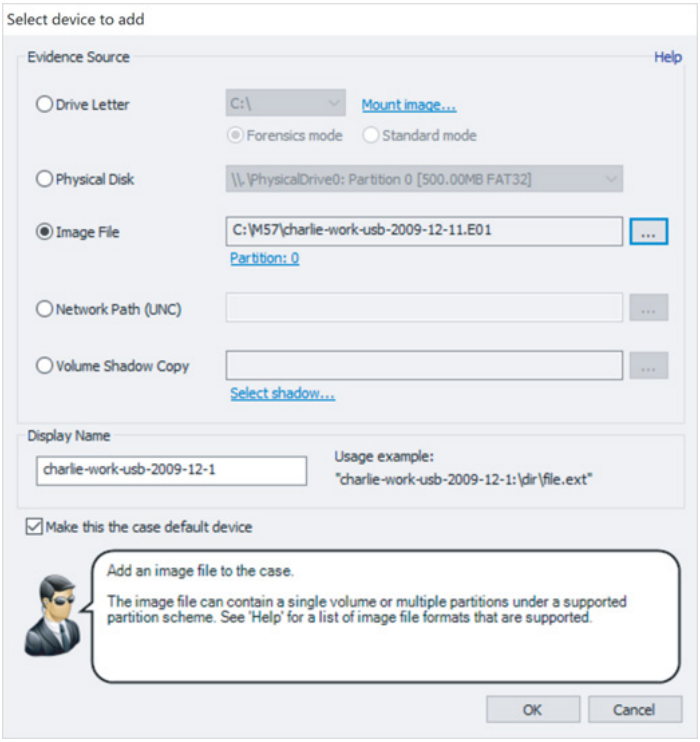
Source: PassMark Software, www.osforensics.com

The Manage Case window

6. Click the **Add Device** button to open the "Select device to add" dialog box, and then click the **Image File** option button. Click the browse button, navigate to your work folder where you copied the USB drive images, click **charlie-work-usb-2009-12-11.E01** , and click **Open**.

7. In the message box asking which partition to use, click **Partition 0**, and then click **OK**. The completed "Select device to add" dialog box should be similar to Figure 4-9. Click **OK**.

Figure 4-9.

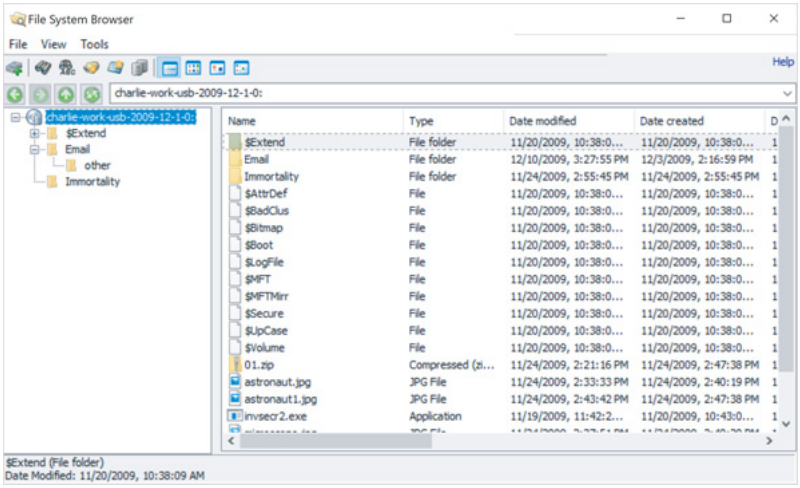


Source: PassMark Software, www.osforensics.com

The "Select device to add" dialog box

8. Click the **charlie-work-usb-2009-12-11.E01** filename in the bottom pane on the right, and then click the **Open** button to the left to open the File System Browser window shown in Figure 4-10. Although viewing the files on a USB drive in this window is fairly easy, tools to search for specific files are available. Close the window.

Figure 4-10.



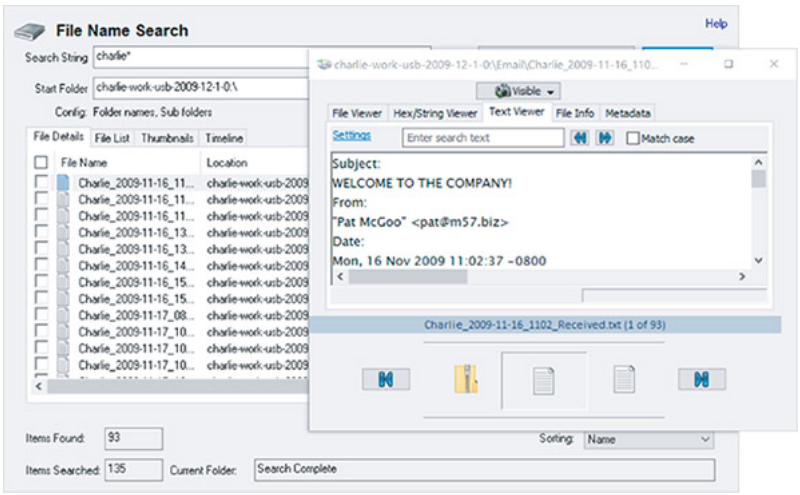
Source: PassMark Software, www.osforensics.com

The File System Browser window

9. Click the **File Name Search** button in the left pane of the main window. Type **charlie*** in the Search String text box. Verify that the Start Folder specifies Charlie's USB image file. On the far right, click the **Search** button. Then double-click any of the listed files. The

results should be similar to Figure 4-11. You can use the tabs at the top of the search results to see thumbnails of files and the timeline for files on the device.

Figure 4-11.

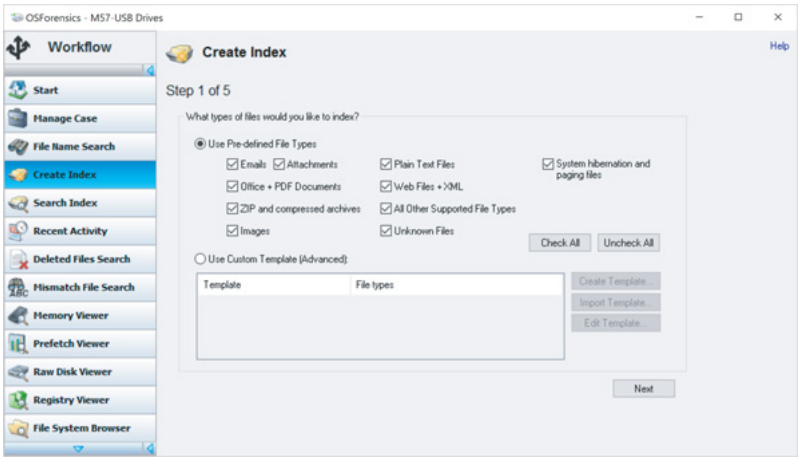


Source: PassMark Software, www.osforensics.com

The File Name Search window

10. Next, click the **Create Index** button in the left pane to start the Create Index Wizard. In the Step 1 of 5 window, click the **Use Pre-defined File Types** option button, if necessary. Click all the file types listed (see Figure 4-12), and then click **Next**.

Figure 4-12.



Source: PassMark Software, www.osforensics.com

Specifying the file types to index

11. In the **Step 2** of 5 window, click the **Add** button, click the **charlie-work-usb-2009-12-11.E01** file, click **OK**, and then click **Next**.

12. In the **Step 3** of 5 window, type **Index all file types** in the Index Title text box, and then click **Start Indexing**. The Step 4 of 5 window flashes by quickly, and then the Step 5 of 5 window shows the files processing. When the indexing is finished, click **OK** in the message box informing you that some errors might have occurred in the indexing process.

13. Click the **Open Log** button at the lower right of the Step 5 of 5 window. The window that opens shows you the files that were indexed, any errors that occurred, and a

summary of what was done. After examining the summary, close the window.

14. Click the **Manage Case** button in the left pane. Notice that the index is now listed in the bottom pane on the right. Scroll to the bottom of the left pane, and click the **Exit** button.

This activity has given you a chance to see how indexing is done in the OSForensics tool you use throughout the book. You should now be able to create a case, add it to your inventory, scan the files, and perform indexing, which will be useful later for searching.

Chapter Summary

- Digital evidence is anything stored or transmitted on electronic or optical media. It's extremely fragile and easily altered.
- In the private sector, an incident scene is often a place of work, such as a contained office or manufacturing area. Because everything from the computers used to violate a company policy to the surrounding facility is under a controlled authority, investigating and controlling the scene are easier than at a crime scene.
- Companies should publish policies stating that they reserve the right to inspect digital assets at will; otherwise, employees' expectation of privacy prevents an employer from legally conducting an intrusive investigation or covert surveillance. A well-defined company policy states that an employer has the right to examine, inspect, or access any company-owned digital asset.
- Approved procedures must be followed, even in private-sector investigations, because civil cases can easily become criminal cases. If a private-sector case is turned over to law enforcement because of criminal activity, the investigator must avoid becoming an agent of law enforcement.
- Criminal cases require a correctly executed and well-defined search warrant. A specific crime and location must be spelled out in the warrant. For all criminal investigations in the United States, the Fourth Amendment specifies that a law enforcement officer can search for and seize criminal evidence only with probable cause, which is facts or circumstances that lead a reasonable person to believe a crime has been committed or is about to be committed.
- The plain view doctrine applies when investigators find evidentiary items that aren't specified in a warrant or under probable cause.
- When preparing for a case, describe the nature of the case, identify the type of OS, determine whether you can seize the computer or digital device, and get a description of the location. Keep in mind that with mobile devices, you might have to get a warrant or subpoena for evidence stored on a cloud server, an ISP's server, or a telecommunications provider's server.
- If you deal with situations involving hazardous materials often, you might need to get HAZMAT certification or have someone else with this certification collect the evidence.
- Always take pictures or use a video camera to document the scene. Prevent professional curiosity from contaminating evidence by limiting who enters the scene.
- As you collect digital evidence, guard against physically destroying or contaminating it. Take precautions to prevent static electricity discharge to electronic devices. If possible, bag or box digital evidence and any hardware you collect from the scene. As you collect hardware, sketch the equipment, including exact markings of where components are located. Tag and number each cable, port, and other connection and record its number and description in a log.
- Selecting a medium for storing digital evidence usually depends on how long you need to keep the evidence. The ideal storage media are CDs, DVDs, USB drives, external solid-state devices, or offsite storage. You can also use magnetic tape, such as 4-mm DAT and DLT magnetic tapes.
- Forensic hash values are used to verify that data or storage media haven't been altered. The two most common hashing algorithms for forensics purposes are

currently MD5 and SHA-1. A forensic hash can't be predicted, each file produces a unique hash value, and if the file changes, the hash value must change.

- To analyze digital forensics data, learn to use more than one vendor tool. Vendors offer different methods for recovering data from digital media.
- You must handle all evidence the same way every time you handle it. Apply the same security and accountability controls for evidence in a civil lawsuit as for evidence from a crime scene to comply with state or federal rules of evidence.
- After you determine that an incident scene or a crime scene has digital data or devices, identify the information or artifacts that can be used as evidence. Next, catalog or document the evidence you find. Your goal is to preserve evidence integrity, which means you must not modify the evidence as you collect and catalog it. The scene should be photographed and sketched, and then each item labeled and put in an evidence bag. Collect, preserve, document, analyze, identify, and organize the evidence. Then rebuild evidence or repeat a situation to verify that you get the same results every time.

Key Terms

Automated Fingerprint Identification System (AFIS)
computer-generated records
computer-stored records
covert surveillance
Cyclic Redundancy Check (CRC)
digital evidence
extensive-response field kit
hash value
hazardous materials (HAZMAT)
initial-response field kit
innocent information
keyed hash set
limiting phrase
low-level investigations
Message Digest 5 (MD5)
National Institute of Standards and Technology (NIST)
nonkeyed hash set
person of interest
plain view doctrine
probable cause
professional curiosity
Scientific Working Group on Digital Evidence (SWGDE)
Secure Hash Algorithm version 1 (SHA-1)
sniffing

Review Questions

1. Private-sector investigations are typically easier than law enforcement investigations for which of the following reasons?

a. Most companies keep inventory databases of all hardware and software used.

b. The investigator doesn't have to get a warrant.

c. The investigator has to get a warrant.

d. Users can load whatever they want on their machines.

2. In the United States, if a company publishes a policy stating that it reserves the right to inspect computing assets at will, a private-sector investigator can conduct covert surveillance on an employee with little cause. True or False?

3. If you discover a criminal act while investigating a company policy abuse, the case becomes a criminal investigation and should be referred to law enforcement. True or False?

4. As a private-sector investigator, you can become an agent of law enforcement when which of the following happens?

a. You begin to take orders from a police detective without a warrant or subpoena.

b. Your internal investigation has concluded, and you have filed a criminal complaint and turned over the evidence to law enforcement.

c. Your internal investigation begins.

d. None of the above.

5. The plain view doctrine in computer searches is well-established law. True or False?

6. If a suspect's computer is found in an area that might have toxic chemicals, you must do which of the following?

a. Coordinate with the HAZMAT team.

b. Determine a way to obtain the suspect's computer.

c. Assume the suspect's computer is contaminated.

d. Do not enter alone.

7. What are the three rules for a forensic hash?

8. In forensic hashes, when does a collision occur?

9. List three items that should be in an initial-response field kit.

10. When you arrive at the scene, why should you extract only those items you need to acquire evidence?

11. Computer peripherals or attachments can contain DNA evidence. True or False?

12. If a suspect computer is running Windows 10, which of the following can you perform safely?

a. Browsing open applications

b. Disconnecting power

c. Either of the above

d. None of the above

13. Describe what should be videotaped or sketched at a digital crime scene.

14. Which of the following techniques might be used in covert surveillance?

a. Keylogging

b. Data sniffing

c. Network logs

d. None of the above

15. Commingling evidence means what in a private-sector setting?

16. List two hashing algorithms commonly used for forensic purposes. True or False?

17. Small companies rarely need investigators. True or False?

18. If a company doesn't distribute a computing use policy stating an employer's right to inspect employees' computers freely, including e-mail and Web use, employees have an expectation of privacy. True or False?

19. You have been called to the scene of a fatal car crash where a laptop computer is still running. What type of field kit should you take with you?

20. You should always answer questions from onlookers at a crime scene. True or False?

Hands-On Projects

Create a *Work*\Chap04\Projects folder on your system before starting these projects; it's referred to as your "work folder" in steps. Copy the drive images for the M57 Patents case to your workstation, if you haven't done so already. (You can find them in the downloads section for this chapter on the student companion site for this book.) In addition, download the PDF files containing detective reports as well as a warrant and an affidavit.

Hands-On Project 4-1.

Read the four detective reports and the combined affidavit and warrant for the M57 Patents case. Write a one- to two-page paper describing the evidence the police found and explaining whether they had enough information for the search warrant. Did the information justify taking all the computers and USB drives? Why or why not?

Hands-On Project 4-2.

You're investigating an internal policy violation when you find an e-mail about a serious assault for which a police report needs to be filed. What should you do? Write a two-page paper specifying who in your company you need to talk to first and what evidence must be turned over to the police.

Hands-On Project 4-3.

In this project, you examine a USB drive belonging to Terry, the IT person for M57 Patents. Your job is to ascertain whether Terry is involved in anything illicit or against company policy.

1. Start OSForensics. If necessary, click **OK** or **Yes** in the UAC message box. In the OSForensics message box, click **Continue Using Trial Version**.
2. Click **Start** in the left pane, if necessary. In the right pane, click **Create Case**.
3. In the New Case dialog box, enter your name in the Investigator text box. In the Case Name text box, type **M57-Terrys USB drive**. Fill in the contact details and the organization, and then click **Investigate Disk(s) from Another Machine**.
4. Click **Custom Location** for the case folder. Click the **Browse** button on the lower right, navigate to and click your work folder, and then click **OK** twice. You should see the Manage Case window.
5. Click the **Add Device** button to open the "Select device to add" dialog box, and then click the **Image File** option button. Click the browse button, navigate to the folder you copied images to, and click **terry-work-usb-2009-12-11.E01** . Click **Open**.
6. In the message box asking which partition to use, leave the default setting for using the entire image file, and then click **OK**. Click **OK** to close the "Select device to add" dialog box.

7. Click the **terry-work-usb-2009-12-11.E01** filename at the lower right, and then click the **Open** button to the left to open the File System Browser window.

8. Click the **File Name Search** icon in the File System Browser window or the left pane of the main window. In the Search String text box, type **kitty***. On the far right, click the **Search** button. Notice that the "kitty porn" isn't on his USB drive.

9. Click the **Create Index** button in the left pane. (*Note*: You might have to click New Index if the window is showing the results from the index of Charlie's USB drive.) In the Step 1 of 5 window, click the **Use Pre-defined File Types** option button, click all the file types listed, and then click **Next**.

10. In the **Step 2** of 5 window, click **Charlie's USB image** and click **Remove** to delete it from the list box, if necessary. Click **Add**, click **terry-work-usb-2009-12-11.E01** , click **OK**, and then click **Next**.

11. In the **Step 3** of 5 window, type **Index all file types** in the Index Title text box, and then click **Start Indexing**. When the indexing is finished, which might take up to an hour, click **OK** in the message box.

12. Click the **Open Log** button at the lower right, and examine the log. Notice whether any errors were reported and the number of files processed, and then close the log.

13. Click the **Manage Case** button in the left pane. In the lower-right pane, double-click **Terrys USB** under the Devices heading, open any text or picture files, and examine them.

14. Scroll to the bottom of the left pane, and click the **Exit** button. Write a one- to two-page paper explaining the importance of the files you examined. How might they affect a patent case? When you're finished, exit OSForensics.

Hands-On Project 4-1.

In this project, you create a file on a USB drive and calculate its hash value in FTK Imager Lite. Then you change the file and calculate the hash value again to compare the files. You need a Windows computer and a USB drive.

1. Create a folder called **C4Prj04** on your USB drive, and then start Notepad.
2. In a new text file, type **This is a test of hash values. One definition of a forensic hash is that if the file changes, the hash value changes**.
3. Save the file as **hash1.txt** in the C4Prj04 folder on your USB drive, and then exit Notepad.
4. Start FTK Imager Lite (clicking **OK** or **Yes** in the UAC message box, if necessary), and click **File**, **Add Evidence Item** from the menu. In the Select Source dialog box, click the **Logical Drive** option button, and then click **Next**.
5. In the Select Drive dialog box, click the **Source Drive Selection** list arrow, click to select your USB drive, and then click **Finish**.
6. In the upper-left pane, click to expand the USB drive and continue expanding until you can click the **C4Prj04** folder. In the upper-right pane, you should see the hash1.txt file you created.
7. Right-click the file and click **Export File Hash List**. Save the file as **original hash** in the C4Prj04 folder on your USB drive. FTK Imager Lite saves it as a .csv file. Exit FTK Imager Lite, and start Notepad.
8. Open **hash1.txt** in Notepad. Add one letter to the end of the file, save it, and exit Notepad.
9.

Start FTK Imager Lite again. Repeat **Steps 4**, 5, 6 and 7 (but without starting Notepad), but this time when you export the file hash list, save the file as **changed hash** .

10. Open the **original hash** and **changed hash** files on your USB drive in Excel or another spreadsheet program. Compare the hash values in both files to see whether they're different, and then exit Excel and FTK Imager Lite.

Hands-On Project 4-5.

In this project, you create a file on your USB drive and calculate its hash values in FTK Imager Lite. Then you change the filename and extension and calculate the hash values again to compare them. You need a Windows computer and a USB drive.

1. Create a folder called **C4Prj05** on your USB drive, and then start Notepad.
2. In a new text file, type **This project shows that the file, not the filename, has to change for the hash value to change**.
3. Click **File**, **Save As** from the menu, and save the file as **testhash.txt** in the C4Prj05 folder on your USB drive. Exit Notepad, and start FTK Imager Lite (clicking **OK** or
4. Click **File**, **Add Evidence Item** from the menu. In the Select Source dialog box, click the **Logical Drive** option button, and then click **Next**.
5. In the Select Drive dialog box, click the **Source Drive Selection** list arrow, click to select your USB drive, and then click **Finish**.
6. In the upper-left pane, click to expand your USB drive and continue expanding until you can click the **C4Prj05** folder. In the upper-right pane, you should see the testhash.txt file you created.
7. Right-click the file and click **Export File Hash List**. Save the file as **original hash value** in the C4Prj05 folder on your USB drive. FTK Imager Lite saves it as a .csv file.
8. Click to select your USB drive in the upper-left pane, if necessary, and then click **File**, **Remove Evidence** Item from the menu. Exit FTK Imager Lite.
9. Open File Explorer. Right-click the **testhash.txt** file on your USB drive, and rename it as **testhash.doc** . In the warning message about the change in extension, click **Yes**.
10. Start FTK Imager Lite. Follow **Steps 4**, 5, 6 and 7, but this time when you export the file hash list, save the file as **changed hash value** . Exit FTK Imager Lite.
11. Open **original hash value** and **changed hash value** in Excel or another spreadsheet program. Compare the hash values in both files to see whether they're different, and then exit Excel.

Case Projects

Case Project 4-1.

You're a detective for the local police. Thomas Brown, the primary suspect in a murder investigation, works at a large local firm and is reported to have two computers at work in addition to one at home. What do you need to do to gather evidence from these computers, and what obstacles can you expect to encounter during this process? Write a two- to three-page report stating what you would do if the company had its own Digital Forensics and Investigations Department and what you would do if the company did not.

Case Project 4-2.

A murder in a downtown office building has been widely publicized. You're a police detective and receive a phone call from a digital forensics investigator employed by the police department. His name is Gary Owens, and he says he has information that might relate to the murder case. Gary says he ran across a few files while investigating another case at a company

in the same office building. Considering the plain view doctrine, what procedures might you and he, as public officials, have to follow? Write a one-page paper detailing what you might do.

Case Project 4-3.

Your spouse works at a middle school and reports rumors of a teacher, Zane Wilkens, molesting some students and taking illicit pictures of them. Zane allegedly viewed these pictures in his office. Your spouse wants you to take a disk image of Zane's computer and find out whether the rumors are true. Write a one- to two-page paper outlining how you would tell your spouse and school administrators to proceed. Also, explain why walking into Zane's office to acquire a disk image wouldn't preserve the integrity of the evidence.

Case Project 4-4.

As a digital investigator for your local sheriff's department, you have been asked to go with a detective to a local school that got a bomb threat in an anonymous e-mail. The detective already has information from a subpoena sent to the last known ISP where the anonymous e-mail originated, and the message was sent from a residence in the school's neighborhood. The detective tells you the school principal also stated that the school's Web server had been defaced by an unknown attacker. The detective has just obtained a warrant for the search and seizure of a computer at the residence the ISP identified. Prepare a list of what items should be included in an initial-response field kit to ensure the preservation of digital evidence when the warrant is carried out.

Chapter 5. Working with Windows and CLI Systems

After reading this chapter and completing the exercises, you will be able to:

- Explain the purpose and structure of file systems
- Describe Microsoft file structures
- Explain the structure of NTFS disks
- List some options for decrypting drives encrypted with whole disk encryption
- Explain how the Windows Registry works
- Describe Microsoft startup tasks
- Explain the purpose of a virtual machine

This chapter and Chapter 7 **give you an overview of digital data and drives. In this** chapter, you review how data is stored and managed in Microsoft OSs, including Windows and command-line interface (CLI) OSs. To become proficient in recovering data for digital investigations, you should understand file systems and their OSs, including legacy (MS-DOS, Windows 9x, and Windows Me, for example) and current OSs. In this chapter, you examine the tasks an OS performs when it starts so that you can avoid altering evidence when you examine data on a drive. You also learn how to use a virtual environment to further analyze Windows digital evidence. Chapter 7 discusses Linux and Macintosh file systems and covers hardware devices, such as CDs/DVDs and SCSI, IDE, and SATA drives.

Understanding File Systems

To investigate digital evidence effectively, you must understand how the most commonly used OSs work and how they store files. In addition to this section on file systems, you should review books on Computer Technology Industry Association (CompTIA) A+ certifications in hardware and firmware startup tasks and operations. A **file system** gives an OS a road map to data on a disk. The type of file system an OS uses determines how data is stored on the disk. When you need to access a suspect's computer to acquire or inspect data related to your investigation, you should be familiar with both the computer's OS and file system so that you can access and modify system settings when necessary. This chapter examines Windows and CLI OSs in detail; Chapter 7 covers information on Linux and Macintosh. For other OSs, consult system administrators and vendor manuals.

Understanding the Boot Sequence

This section explains the boot sequence for desktop and laptop computers. For tablets and smartphones, it's best to review vendors' documentation. To ensure that you don't contaminate or alter data on a suspect's system, you must know how to access and modify Complementary Metal Oxide Semiconductor (CMOS), BIOS, Extensible Firmware Interface (EFI), and Unified Extensible Firmware Interface (UEFI) settings. A computer stores system configuration and date and time information in the CMOS when power to the system is off. The system BIOS or EFI contains programs that perform input and output at the hardware level. BIOS is designed for x86 computers and typically used on disk drives with Master Boot Records (MBRs). EFI is designed for x64 computers and uses GUID Partition Table (GPT)–formatted disks. BIOS and EFI are designed for specific firmware. In an effort to reduce the relationship with firmware, Intel developed UEFI, which defines the interface between a computer's firmware and the OS. (For more information on Windows boot processes, see "Overview of Boot Options in Windows Vista and Later" (https://msdn.microsoft.com/en-us/windows/hardware/drivers/devtest/boot-options-in-windows-vista-and-later.)

Note

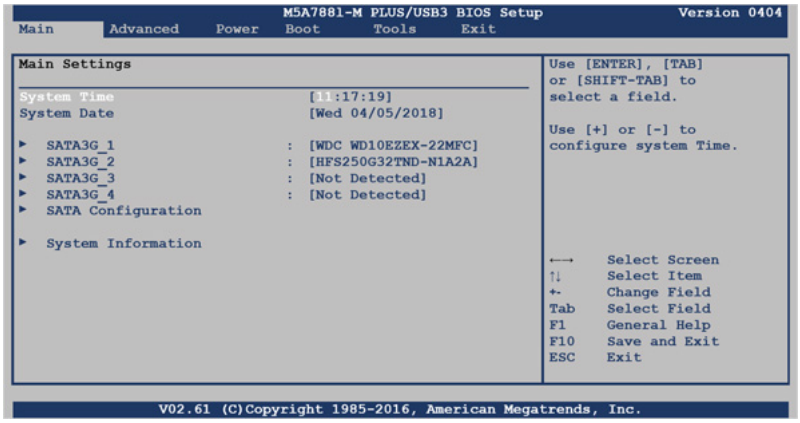
The following paragraph describes how a BIOS boot works. For more information on the differences in these boot utilities, see www.cs.rutgers.edu/~pxk/416/notes/02-

boot.html.

When a subject's computer starts, you must make sure it boots to a forensically configured CD, DVD, or USB drive, as described in **Chapters 1** and 3, because booting to the hard disk overwrites and changes evidentiary data. To do this, you access the CMOS setup by monitoring the computer during the bootstrap process to identify the correct key or keys to use. The **bootstrap process** , which is contained in ROM, tells the computer how to proceed. As the computer starts, the screen usually displays the key or keys, such as the Delete key, you press to open the CMOS setup screen. You can also try unhooking the keyboard to force the system to tell you what keys to use. The key you press to access CMOS depends on the computer's BIOS. Many BIOS manufacturers use the Delete key to access CMOS; other manufacturers use Ctrl+Alt+Insert, Ctrl+A, Ctrl+S, or Ctrl+F1, F2, or F10. A safe method for verifying the BIOS is removing all hard drives from the computer, which enables you to start the computer to verify its BIOS date and time without accessing the disk drive.

Figure 5-1 shows a typical CMOS setup screen, where you check a computer's boot sequence. If necessary, you can change the boot sequence so that the OS accesses the CD/DVD drive, for example, before any other boot device. Each BIOS vendor's screen is different, but you can refer to the vendor's documentation or Web site for instructions on changing the boot sequence.

Figure 5-1.



Source: American Megatrends, Inc., https://ami.com/en/

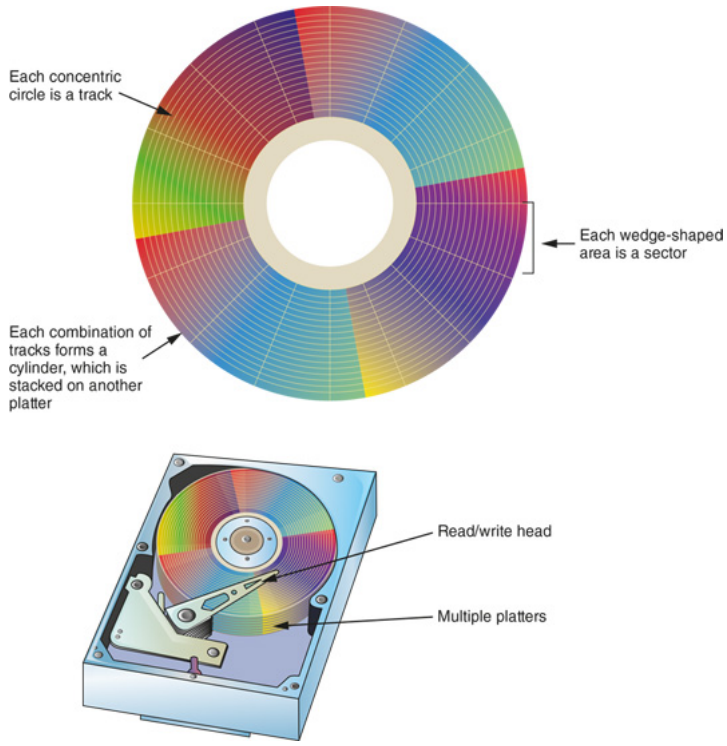
A Typical CMOS Setup Screen

Understanding Disk Drives

You should be familiar with disk drives and how data is organized on a disk so that you can find data effectively. Disk drives are made up of one or more platters coated with magnetic material, and data is stored on platters in a particular way. The following disk drive components are illustrated in **Figure 5-2**:

- *Geometry*— **Geometry** refers to a disk's logical structure of platters, tracks, and sectors.
- *Head*—The **head** is the device that reads and writes data to a drive. There are two heads per platter that read and write the top and bottom sides.
- *Tracks*— **Tracks** are concentric circles on a disk platter where data is located.
- *Cylinders*—A **cylinder** is a column of tracks on two or more disk platters. Typically, each platter has two surfaces: top and bottom.
- *Sectors*—A **sector** is a section on a track, usually made up of 512 bytes.

Figure 5-2.



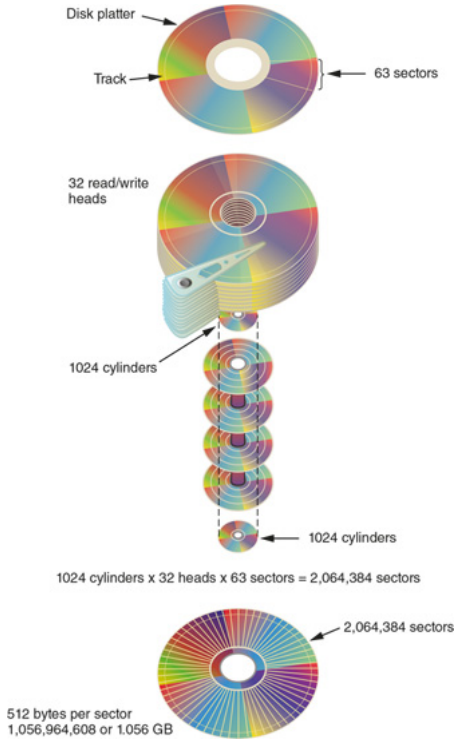
Components of a Disk Drive

Tip

For more information on disk drive configurations, see www.storagereview.com/guide2000/ref/hdd/index.html.

The manufacturer engineers a disk to have a certain number of sectors per track, and a typical disk drive stores 512 bytes per sector. (For an update on Advanced Format [4K] disk compatibility, see https://msdn.microsoft.com/windows/compatibility/advanced-format-disk-compatibility-update.) To determine the total number of addressable bytes on a disk, multiply the number of cylinders by the number of heads (actually tracks) and by the number of sectors (groups of 512 or more bytes), as shown in Figure 5-3. Disk drive vendors refer to this formula as a "cylinder, head, and sector (CHS) calculation." Tracks also follow a numbering scheme starting from 0, which is the first value in computing. If a disk lists 79 tracks, you actually have 80 tracks from 0 to 79.

Figure 5-3.



CHS Calculation

Other disk properties, such as **zone bit recording (ZBR)** , **track density** , **areal density** , and **head and cylinder skew** , are handled at the drive's hardware or firmware level. ZBR is how most manufacturers deal with a platter's inner tracks having a smaller circumference (and, therefore, less space to store data) than its outer tracks. Grouping tracks by zones ensures that all tracks hold the same amount of data.

Track density is the space between each track. As with old vinyl records, the smaller the space between each track, the more tracks you can place on the platter.

Areal density is the number of bits in one square inch of a disk platter. This number includes the unused space between tracks. Head and cylinder skew are used to improve disk performance. As the read-write head moves from one track to another, starting sectors are offset to minimize lag time.

Solid-State Storage Devices

Flash memory storage devices used in USB drives, laptops, tablets, and cell phones can be a challenge for digital forensics examiners because if deleted data isn't recovered immediately, it might be lost forever. The reason is a feature all flash memory devices have: **wear-leveling** .

When data is deleted on a hard drive, only the references to it are removed, which leaves the original data in unallocated disk space. With forensics recovery tools, recovering data from magnetic media is fairly easy; you just copy the unallocated space. USB drives and other solid-state drive systems are different, in that memory cells shift data at the physical level to other cells that have had fewer reads and writes continuously. The purpose of shifting (or rotating) data from one memory cell to another is to make sure all memory cells on the flash drive wear evenly. Memory cells are designed to perform only 10,000 to 100,000 reads/writes, depending on the manufacturer's design. When they reach their defined limits, they can no longer retain data. When you attempt to connect to the device, you get an access failure message. This process is controlled on the flash device's firmware.

In addition, when data is rotated to another memory cell, the old memory cell addresses are listed in a firmware file called a "garbage collector." At some point, the flash drive's firmware erases data in unallocated cells by overwriting the value of 1 in all cells listed in the garbage collector file.

When dealing with solid-state devices, making a full forensic copy as soon as possible is crucial in case you need to recover data from unallocated disk space. You can test this feature with a USB drive easily by copying data to it, deleting it, and then making a forensic acquisition with any acquisition tool, such as OSForensics or X-Ways Forensics, immediately after the data is deleted. The first acquisition produces recoverable artifacts. If you let the USB drive sit and write no additional data to it, wear-leveling automatically overwrites the unallocated space. All solid-state drives have an internal power source for memory cells (both allocated and unallocated) so that they can preserve data. If you make another acquisition of the USB drive a day or more later, it reveals that the previously recoverable deleted data no longer exists. For mobile device forensics, this feature is extremely important, especially if a suspect deleted relevant messages, for example, just before the device was seized and taken into evidence.

Depending on your jurisdiction and country's laws on search and seizure, there might be some limitations on when an acquisition can take place in criminal cases. For criminal investigations, you should get guidance from your local prosecutor's office on how to handle this type of evidence.

Exploring Microsoft File Structures

Because most PCs use Microsoft software products, you should understand Microsoft file systems so that you know how Windows and DOS computers store files. In particular, you need to understand clusters, File Allocation Table (FAT), and NT File System (NTFS). The method an OS uses to store files determines where data can be hidden. When you examine a computer for forensic evidence, you need to explore these hiding places to determine whether they contain files or parts of files that might be evidence of a crime or policy violation.

In Microsoft file structures, sectors are grouped to form **clusters** , which are storage allocation units of one or more sectors. Clusters range from 512 bytes up to 32,000 bytes each. Combining sectors minimizes the overhead of writing or reading files to a disk. The OS groups one or more sectors into a cluster. The number of sectors in a cluster varies according to the disk size. For example, a double-sided floppy disk has one sector per cluster; a hard disk has four or more sectors per cluster.

Clusters are numbered sequentially, starting at 0 in NTFS and 2 in FAT. The first sector of all disks contains a system area, the boot record, and a file structure database. The OS assigns these cluster numbers, referred to as **logical addresses** . They point to relative cluster positions; for example, cluster address 100 is 98 clusters from cluster address 2. Sector numbers, however, are referred to as **physical addresses** because they reside at the hardware or firmware level and go from address 0 (the first sector on the disk) to the last sector on the disk. Clusters and their addresses are specific to a logical disk drive, which is a disk partition.

Disk Partitions

Many hard disks are partitioned, or divided, into two or more sections. A **partition** is a logical drive. Windows OSs can have three primary partitions followed by an extended partition that can contain one or more logical drives. Someone who wants to hide data on a hard disk can create hidden partitions or voids—large unused gaps between partitions on a disk drive. For example, partitions containing unused space can be created between the primary partitions or logical partitions. This unused space between partitions is called the **partition gap** . It's possible to create a partition, add data to it, and then remove references to the partition so that it can be hidden in Windows. If data is hidden in this partition gap, a disk editor utility could be used to access it. Another technique is to hide incriminating digital evidence at the

end of a disk by declaring a smaller number of bytes than the actual drive size. With disk-editing tools, however, you can access these hidden or empty areas of the disk.

One way to examine a partition's physical level is to use a disk editor, such as WinHex or Hex Workshop. These tools enable you to view file headers and other critical parts of a file. Both tasks involve analyzing the key hexadecimal codes the OS uses to identify and maintain the file system. **Table 5-1** lists the hexadecimal codes in a partition table and identifies some common file system structures.

Tip

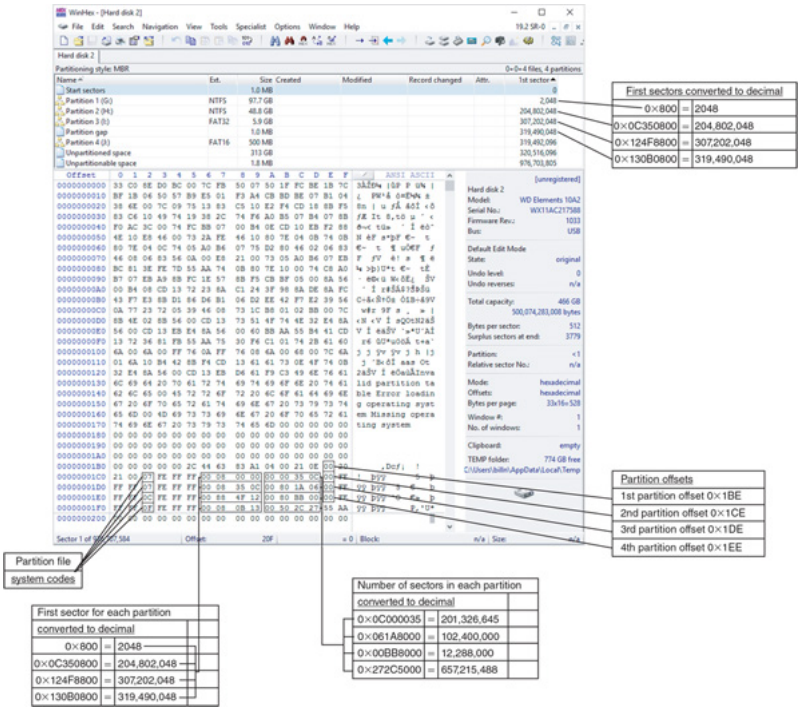
To understand hexadecimal numbering better, see www.i-programmer.info/babbages-bag/478-hexadecimal.html.

Table 5-1. Hexadecimal Codes in the Partition Table

Hexadecimal code	File system
01	DOS 12-bit FAT (floppy disks)
04	DOS 16-bit FAT for partitions smaller than 32 MB
05	Extended partition
06	DOS 16-bit FAT for partitions larger than 32 MB
07	NTFS and exFAT
08	AIX bootable partition
09	AIX data partition
0B	DOS 32-bit FAT
0C	DOS 32-bit FAT for interrupt 13 support
0F	Extended Partition with Logical Block Address (LBA)
17	Hidden NTFS partition (XP and earlier)
1B	Hidden FAT32 partition
1E	Hidden VFAT partition
3C	Partition Magic recovery partition
66–69	Novell partitions
81	Linux
82	Linux swap partition (can also be associated with Solaris partitions)
83	Linux native file systems (Ext2, Ext3, Ext4, Reiser, Xiafs)
86	FAT16 volume/stripe set (Windows NT)
87	High Performance File System (HPFS) fault-tolerant mirrored partition or NTFS volume/stripe set
A5	FreeBSD and BSD/386
A6	OpenBSD
A9	NetBSD
C7	Typical of a corrupted NTFS volume/stripe set
EB	BeOS

The partition table is in the **Master Boot Record (MBR)** , located at sector 0 of the disk drive. In a hexadecimal editor, such as WinHex, you can find the first partition starting at offset 0x1BE. The second partition starts at 0x1CE, the third partition starts at 0x1DE, and the fourth partition starts at 0x1EE (see Figure 5-4).

Figure 5-4.



Source: X-Ways AG, www.x-ways.net

The Partition Table in a Hexadecimal Editor

Tip

For more information on the Master Boot Record, see https://technet.microsoft.com/en-us/library/cc976786.aspx.

The file system's hexadecimal code is offset 3 bytes from 0x1BE for the first partition. The sector address of where this partition starts on the drive is offset 8 bytes from 0x1BE. The number of sectors assigned to the partition are offset 12 bytes for position 0x1BE. These offsets are duplicated for any additional partitions created on the disk, as shown in **Figure 5-4**. For the extended part of the drive, all partitions are logical partitions. In the first logical partition's boot sector, there's a partition table similar to the MBR.

In some instances, you might need to identify the OS on an unknown disk. You can use WinHex or another hexadecimal editor, such as Hex Workshop, for this task. The following steps show you how to determine a disk's OS by using WinHex:

Note

Before beginning the following activity, create a *Work*\Chap05\Chapter work folder on your system.

1. Start a Web browser, and go to http://x-ways.net. Under the Software Products heading, click **WinHex**. Download and install this program, after checking with your instructor about where to install it on your computer.

2. Insert a USB drive into a USB port.

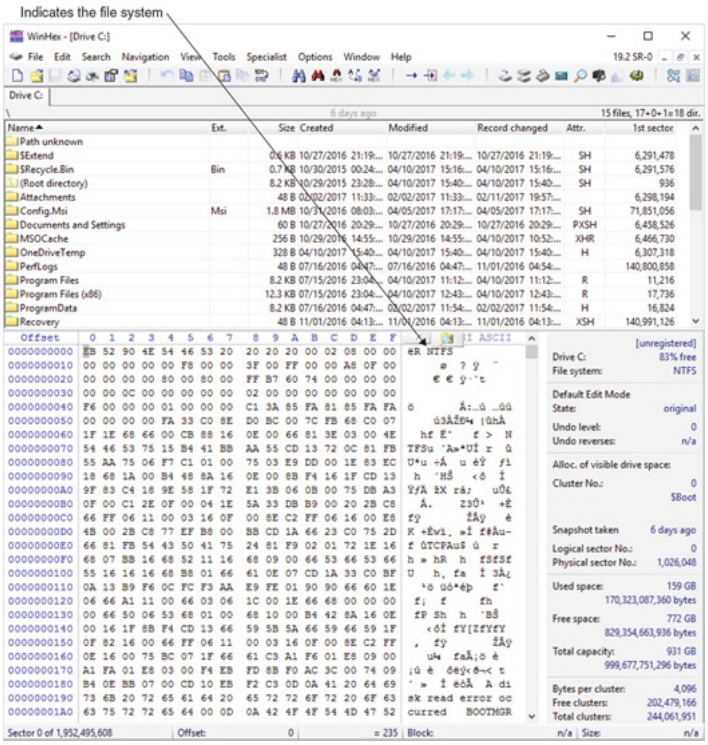
3. Right-click the **WinHex** desktop icon and click **Run as administrator**. If necessary, click **Continue** or **Yes** in the UAC message box.

Tip

In Windows 10 or later, it's recommended that you create a desktop shortcut in File Explorer for the WinHex.exe file, which is usually in the C:\Program Files\WinHex folder. In older Windows versions, the path might be C:\Program Files (x86)\Winhex. To start the program, you right-click the WinHex desktop icon and click "Run as administrator."

4. Click **Tools, Open Disk** from the menu to see a list of logical drives. Click the **C** drive (or your working drive), and click **OK**. Figure 5-5 shows a typical hard disk in the WinHex window. If an error message is displayed, you can ignore it because it won't affect your analysis for this activity.

Figure 5-5.



Source: X-Ways AG, www.x-ways.net

WinHex Identifying the File System

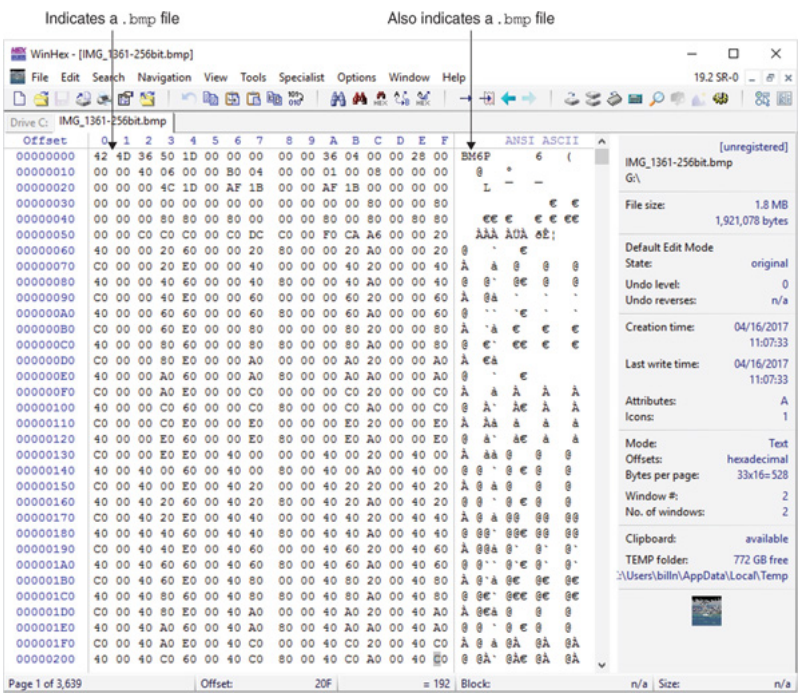
5. Click **Tools, Open Disk** again, but this time, click your USB drive in the Edit Disk list, and then click **OK**. Compare the file system label for this drive with the one you saw in Step 4. Leave WinHex open for the next activity.

With tools such as WinHex, you can also identify file headers to determine the file types, with or without an extension. Before performing the following steps in WinHex, use File Explorer to find a bitmap (.bmp) file and a Word document (.docx). (In the Hands-On Projects, you apply these techniques to other file types.) Then follow these steps:

1. To open a bitmap file on your computer, click **File, Open** from the WinHex menu (the main menu, not the File item in the Case Data menu). In the Open Files dialog box, navigate to a folder containing a bitmap file, and then double-click the .bmp file. If you get a WinHex evaluation warning message, click **OK** to continue.

2. As shown in **Figure 5-6**, the WinHex window identifies the file type for the graphic. For .bmp files, it shows “BM6,” “BM,” or “BMF.” As shown in the figure, “42 4D” is also displayed to indicate a BMP file signature.

Figure 5-6.



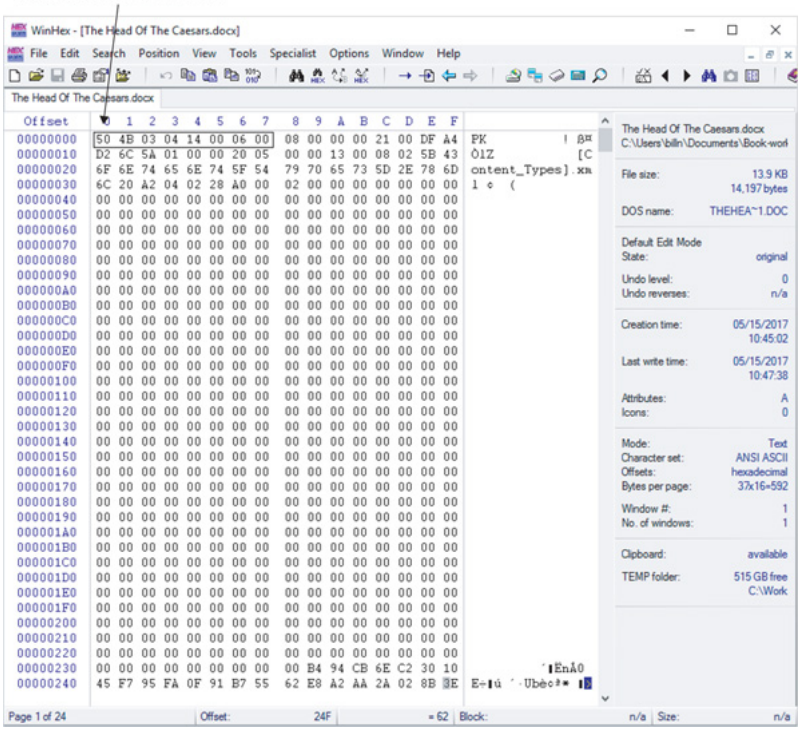
Source: X-Ways AG, www.x-ways.net

WinHex Indicating a .bmp File

3. To open a Word document, click **File, Open** from the menu. Navigate to a folder containing a Word document, and then double-click the .docx file. As shown in Figure 5-7, the first line contains the hexadecimal values “50 4B 03 04 14 00 06 00,” which identify the file as a Microsoft Office 2010 or later document. The same file header is displayed for an Excel or a PowerPoint file but doesn’t apply to Access databases. For Microsoft Office 2007 and earlier, the first eight hexadecimal values are “D0 CF 11 E0 A1 B1 1A E1.”

Figure 5-7.

Indicates a Microsoft Office file



Source: X-Ways AG, www.x-ways.net

WinHex Indicating a Microsoft Office File

4. Exit WinHex.

Tip

Depending on the hexadecimal editor, hex values can be grouped in sets of two or four digits. For more information on file header hexadecimal information, see www.garykessler.net/library/file_sigs.html.

Examining FAT Disks

File Allocation Table (FAT) is the file structure database that Microsoft designed for floppy disks. It's used to organize files on a disk so that the OS can find the files it needs. Since its development, other OSs, such as Linux and Macintosh, can format, read, and write to FAT storage devices such as USB drives and SD cards. The FAT database is typically written to a disk's outermost track and contains filenames, directory names, date and time stamps, the starting cluster number, and file attributes (archive, hidden, system, and read-only).

There are three current versions of FAT—FAT16, FAT32, and exFAT (used for mobile personal storage devices)—and three older FAT formats, which are FATX, Virtual FAT (VFAT), and FAT12. The FAT version in Microsoft DOS 6.22 had a limitation of eight characters for filenames and three characters for extensions. The following list summarizes the evolution of FAT versions:

- *FAT12*—This version is used specifically for floppy disks, so it has a limited amount of storage space. It was originally designed for MS-DOS 1.0, the first Microsoft OS, used for floppy disk drives and drives up to 16 MB.
- *FAT16*—To handle larger disks, Microsoft developed FAT16, which is still used on older Microsoft OSs, such as MS-DOS 3.0 through 6.22, Windows 95 (first release), and

Windows NT 3.5 and 4.0. FAT16 supports disk partitions with a maximum storage capacity of 4 GB.

- *FAT32*—When disk technology improved and disks larger than 2 GB were developed, Microsoft released FAT32, which can access larger drives.
- *exFAT*—Developed for mobile personal storage devices, such as flash memory devices, secure digital eXtended capacity (SDCX), and memory sticks. The exFAT file system can store very large files, such as digital images, video, and audio files.
- *VFAT*—Developed to handle files with more than eight-character filenames and three-character extensions; introduced with Windows 95. VFAT is an extension of other FAT file systems.

Tip

For additional information on the specifications for FAT, exFAT, and NTFS, see www.ntfs.com/ntfs_vs_fat.htm.

Cluster sizes vary according to the hard disk size and file system. **Table 5-2** lists the number of sectors and bytes assigned to a cluster on FAT16 disk according to hard disk size. For FAT32 file systems, cluster sizes are determined by the OS. Clusters can range from 1 sector consisting of 512 bytes to 128 sectors of 64 KB.

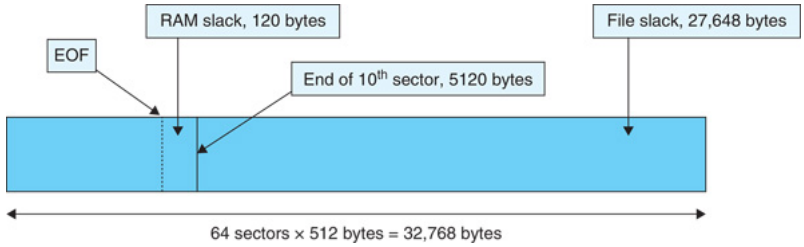
Table 5-2. Sectors and Bytes per Cluster

Drive size	Sectors per cluster	FAT16
8–32 MB	1	512 bytes
32–64 MB	2	1 KB
64–128 MB	4	2 KB
128–256 MB	8	4 KB
256–512 MB	16	8 KB
512–1024 MB	32	16 KB
1024–2048 MB	64	32 KB
2048–4096 MB	128	64 KB

Microsoft OSs allocate disk space for files by clusters. This practice results in **drive slack**, composed of the unused space in a cluster between the end of an active file's content and the end of the cluster. Drive slack includes **RAM slack** (found mainly in older Microsoft OSs) and **file slack**. In newer Windows OSs, when data is written to disk, the remaining RAM slack is zeroed out and contains no RAM data.

For example, suppose you create a text document containing 5000 characters—that is, 5000 bytes of data. If you save this file on a FAT16 1.6 GB disk, a Microsoft OS reserves one cluster for it automatically. For a 1.6 GB disk, the OS allocates about 32,000 bytes, or 64 sectors (512 bytes per sector), for your file. The unused space, 27,000 bytes, is the file slack (see **Figure 5-8**). That is, RAM slack is the portion of the last sector used in the last assigned cluster, and the remaining sectors are referred to as "file slack." The 5000-byte text document uses up 10 sectors, or 5120 bytes, so 120 bytes of a sector aren't used; however, DOS must write in full 512-byte chunks of data (sectors). The data to fill the 120-byte void is pulled from RAM and placed in the area between the end of the file (EOF) and the end of the last sector used by the active file in the cluster. Any information in RAM at that point, such as logon IDs or passwords, is placed in RAM slack on older Microsoft OSs when you save a file. File fragments, deleted e-mails, and passwords are often found in RAM and file slack.

Figure 5-8.

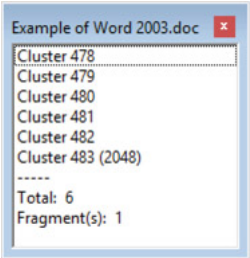


File Slack Space

An unintentional side effect of FAT16 allowing large clusters was that it reduced fragmentation as cluster size increased. The OS added extra data to the end of the file and allowed the file to expand to this assigned cluster until it consumed the remaining reserved 27,000 bytes. This increased cluster size resulted in inefficient use of disk space. Because of this inefficient allocation of sectors to clusters, when nearly full FAT16 drives were converted to FAT32, users discovered they had a lot of extra free disk space because the files wasted less space.

When you run out of room for an allocated cluster, the OS allocates another cluster for your file. As files grow and require more disk space, assigned clusters are chained together. Typically, chained clusters are contiguous on the disk. However, as some files are created and deleted and other files are expanded, the chain can be broken or fragmented. With a tool such as WinHex, you can view the cluster-chaining sequence and see how FAT addresses linking clusters to one another (see **Figure 5-9**).

Figure 5-9.



Source: X-Ways AG, www.x-ways.net

Chained Sectors Associated with Clusters as a Result of Increasing File Size

When the OS stores data in a FAT file system, it assigns a starting cluster position to a file. Data for the file is written to the first sector of the first assigned cluster. When this first assigned cluster is filled and runs out of room, FAT assigns the next available cluster to the file. If the next available cluster isn't contiguous to the current cluster, the file becomes fragmented. In the FAT for each cluster on the volume (the partitioned disk), the OS writes the address of the next assigned cluster. Think of clusters as buckets that can hold a specific number of bytes. When a cluster (or bucket) fills up, the OS allocates another cluster to collect the extra data.

On rare occasions, such as a system failure or sabotage, these cluster chains can break. If they do, data can be lost because it's no longer associated with the previous chained cluster. FAT looks forward for the next cluster assignment but doesn't provide pointers to the previous cluster. Rebuilding these broken chains can be difficult.

Note

Many disk forensics tools have automated much of the file-rebuilding process. These improved features make recovering data easier.

Deleting FAT Files

When a file is deleted in Windows Explorer or with the MS-DOS delete command, the OS inserts a HEX E5 (0xE5) in the filename's first letter position in the associated directory entry. This value tells the OS that the file is no longer available and a new file can be written to the same cluster location.

In the FAT file system, when a file is deleted, the only modifications made are that the directory entry is marked as a deleted file, with the HEX E5 character replacing the first letter of the filename, and the FAT chain for that file is set to 0. The data in the file remains on the disk drive. The area of the disk where the deleted file resides becomes **unallocated disk space** (also called "free disk space"). The unallocated disk space is now available to receive new data from newly created files or other files needing more space as they grow. Most forensics tools can recover data still residing in this area.

Examining NTFS Disks

NT File System (NTFS) was introduced when Microsoft created Windows NT and is still the main file system in Windows 10. Each generation of Windows since NT has included minor changes in NTFS configuration and features. The NTFS design was partially based on, and incorporated many features from, Microsoft's project for IBM with the OS/2 operating system; in this OS, the file system was **High Performance File System (HPFS)** . When Microsoft created Windows NT, it provided backward-compatibility so that NT could read OS/2 HPFS disk drives. Since the release of Windows 2000, this backward-compatibility is no longer available. For a detailed explanation of NTFS structures, see www.ntfs.com/ntfs.htm.

NTFS offers substantial improvements over FAT file systems. It provides more information about a file, including security features, file ownership, and other file attributes. With NTFS, you also have more control over files and folders (directories) than with FAT file systems.

NTFS was Microsoft's move toward a journaling file system. The system keeps track of transactions such as file deleting or saving. This journaling feature is helpful because it records a transaction before the system carries it out. That way, in a power failure or other interruption, the system can complete the transaction or go back to the last good setting.

In NTFS, everything written to the disk is considered a file. On an NTFS disk, the first data set is the **Partition Boot Sector** , which starts at sector [0] of the disk and can expand to 16 sectors. Immediately after the Partition Boot Sector is the **Master File Table (MFT)** . The MFT, similar to FAT in earlier Microsoft OSs, is the first file on the disk. An MFT file is created at the same time a disk partition is formatted as an NTFS volume and usually consumes about 12.5% of the disk when it's created. As data is added, the MFT can expand to take up 50% of the disk. (The MFT is covered in more detail in "NTFS System Files.")

An important advantage of NTFS over FAT is that it results in much less file slack space. Compare the cluster sizes in **Table 5-3** with Table 5-2, which showed FAT cluster sizes. Clusters are smaller for smaller disk drives. This feature saves more space on all disks using NTFS.

Table 5-3. Cluster Sizes in an NTFS Disk

Drive size	Sectors per cluster	Cluster size
7–512 MB	8	4 KB
512 MB–1 GB	8	4 KB
1–2 GB	8	4 KB
2 GB–2 TB	8	4 KB
2–16 TB	8	4 KB
16–32 TB	16	8 KB

Drive size	Sectors per cluster	Cluster size
32–64 TB	32	16 KB
64–128 TB	64	32 KB
128–256 TB	128	64 KB

Tip

For more information on Microsoft file system sizes, see http://support.microsoft.com/kb/140365.

NTFS (and VFAT for long filenames) also uses **Unicode** , an international data format. Unlike the **American Standard Code for Information Interchange (ASCII)** 8-bit configuration, Unicode uses an 8-bit, a 16-bit, or a 32-bit configuration. These configurations are known as **UTF-8 (Unicode Transformation Format)** , UTF-16, and UTF-32. For Western-language alphabetic characters, UTF-8 is identical to ASCII (see www.unicode.org/versions for more details). Knowing this feature of Unicode comes in handy when you perform keyword searches for evidence on a disk drive. (This feature is discussed in more detail in Chapter 9.) Because NTFS offers many more features than FAT, more utilities are used to manage it.

NTFS System Files

Because everything on an NTFS disk is a file, the first file, the MFT, contains information about all files on the disk, including the system files the OS uses. In the MFT, the first 15 records are reserved for system files. Records in the MFT are called **metadata** . Table 5-4 lists the first 16 metadata records you find in the MFT.

Table 5-4. Metadata records in the MFT

Filename	System file	Record position	Description
$Mft	MFT	0	Base file record for each folder on the NTFS volume; other record positions in the MFT are allocated if more space is needed.
$MftMirr	MFT 2	1	The first four records of the MFT are saved in this position. If a single sector fails in the first MFT, the records can be restored, allowing recovery of the MFT.
$LogFile	Log file	2	Previous transactions are stored here to allow recovery after a system failure in the NTFS volume.
$Volume	Volume	3	Information specific to the volume, such as label and version, is stored here.
$AttrDef	Attribute definitions	4	A table listing attribute names, numbers, and definitions.
$	Root filename index	5	This is the root folder on the NTFS volume.
$Bitmap	Boot sector	6	A map of the NTFS partition shows which clusters are in use and which are available.
$Boot	Boot sector	7	Used to mount the NTFS volume during the bootstrap process; additional code is listed here if it's the boot drive for the system.
$BadClus	Bad cluster file	8	For clusters that have unrecoverable errors, an entry of the cluster location is made in this file.
$Secure	Security file	9	Unique security descriptors for the volume are listed in this file. It's where the access control list (ACL) is maintained for all files and folders on the NTFS volume.
$Upcase	Upcase table	10	Converts all lowercase characters to uppercase Unicode characters for the NTFS volume.
$Extend	NTFS extension file	11	Optional extensions are listed here, such as quotas, object identifiers, and reparse point data.
		12–15	Reserved for future use.

MFT and File Attributes

When Microsoft introduced NTFS, the way the OS stores data on disks changed substantially. In the NTFS MFT, all files and folders are stored in separate records of 1024 bytes each. Each record contains file or folder information. This information is divided into record fields containing metadata about the file or folder and the file's data or links to the file's data. A record field is referred to as an **attribute ID** .

File or folder information is typically stored in one of two ways in an MFT record: resident and nonresident. For very small files, about 512 bytes or less, all file metadata and data are stored in the MFT record. These types of records are called resident files because all their information is stored in the MFT record.

Files larger than 512 bytes are stored outside the MFT. The file or folder's MFT record provides cluster addresses where the file is stored on the drive's partition. These cluster addresses are called **data runs** . This type of MFT record is referred to as "nonresident" because the file's data is stored in its own separate file outside the MFT.

Each MFT record starts with a header identifying it as a resident or nonresident attribute. The first 4 bytes (characters) for all MFT records are FILE. The header information contains additional data specifying where the first attribute ID starts, which is typically at offset 0x14 from the beginning of the record. Each attribute ID has a length value in hexadecimal defining where it ends and where the next attribute starts. The length value is located 4 bytes from the attribute ID.

Table 5-5 lists the types of attributes in an MFT record. For more details on how the MFT is configured, search on MFT and NTFS at http://technet.microsoft.com/en-us/library/cc781134.aspx.

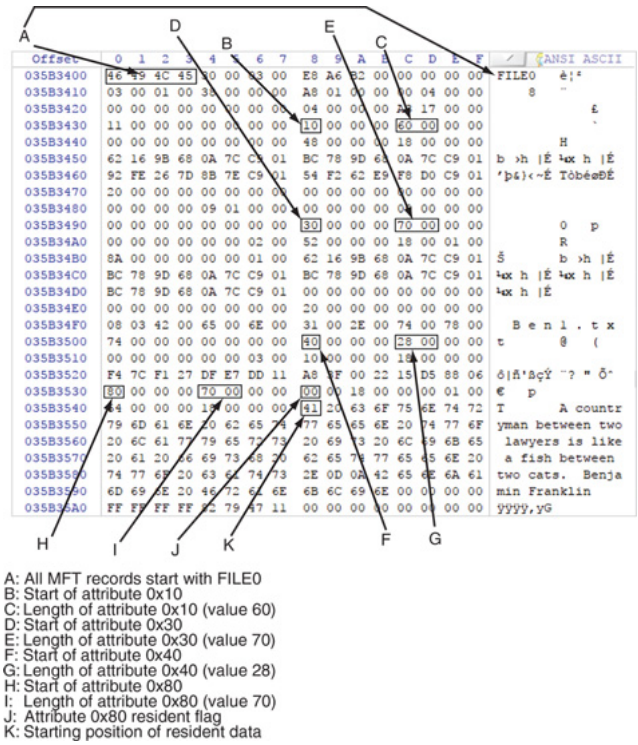
Table 5-5. Attributes in the MFT

Attribute ID	Purpose
0x10	$Standard Information This field contains data on file creation, alterations, MFT changes, read dates and times, and DOS file permissions.
0x20	$Attribute_List Attributes that don't fit in the MFT (nonresident attributes) are listed here along with their locations.
0x30	$File_Name The long and short names for a file are contained here. Up to 255 Unicode bytes are available for long filenames. For POSIX requirements, additional names or hard links can also be listed. Files with short filenames have only one attribute ID 0x30. In older Windows OSs, long filenames have two ID 0x30s in the MFT record: one for the short name and one for the long name. In Windows 10, there's only one 0x30 that combines the short and long filenames.
0x40	$Object_ID ($Volume_Version in Windows NT) Ownership and who has access rights to the file or folder are listed here. Every MFT record is assigned a unique GUID. Depending on your NTFS setup, some file records might not contain this attribute ID.
0x50	$Security_Descriptor Contains the access control list (ACL) for the file.
0x60	$Volume_Name The volume-unique file identifier is listed here. Not all files need this unique identifier.

Attribute ID	Purpose
0x70	$Volume_Information This field indicates the version and state of the volume.
0x80	$Data File data for resident files or data runs for nonresident files.
0x90	$Index_Root Implemented for use of folders and indexes.
0xA0	$Index_Allocation Implemented for use of folders and indexes.
0xB0	$Bitmap A bitmap indicating cluster status, such as which clusters are in use and which are available.
0xC0	$Reparse_Point This field is used for volume mount points and Installable File System (IFS) filter drivers. For the IFS, it marks specific files used by drivers.
0xD0	$EA_Information For use with OS/2 HPFS.
0xE0	For use with OS/2 HPFS.
0x100	$Logged_Utility_Stream This field is used by Encrypting File System (EFS) in Windows 2000 and later .

Figure 5-10 is an MFT record showing the resident attributes of a small file viewed in a hexadecimal editor. Note that on line 035B3530 near the bottom, there's text data in the right pane. In Figure 5-11, the bottom half of the hexadecimal editor window shows the remaining portion of this resident file's MFT record.

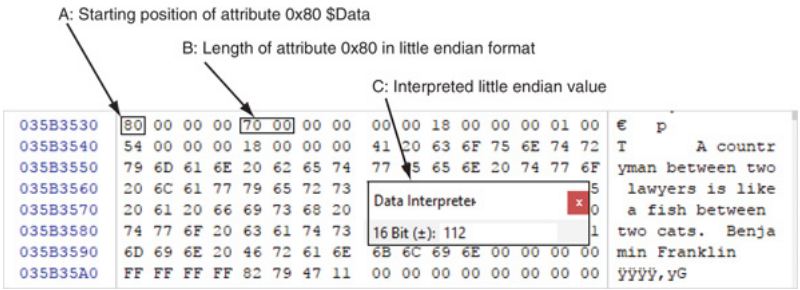
Figure 5-10.



Source: X-Ways AG, www.x-ways.net

Resident File in an MFT Record

Figure 5-11.

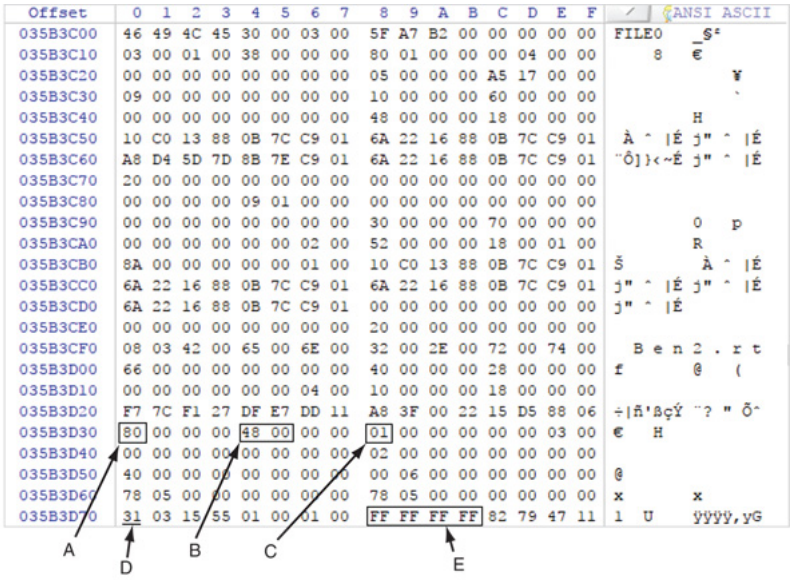


Source: X-Ways AG, www.x-ways.net

File Data for a Resident File

Figure 5-12 is an example of a nonresident file's hexadecimal view. Notice that on line 35B3D50 near the bottom, there's no text data. This file is a longer version of the file shown in Figure 5-10. Current forensics tools, such as OSForensics, EnCase, Forensic Explorer, FTK, and X-Ways Forensics, can interpret the MFT from an image file.

Figure 5-12.



A: Start of nonresident attribute 0x80
B: Length of nonresident attribute 0x80
C: Attribute 0x80 nonresident flag
D: Starting point of data run
E: End-of-record marker (FF FF FF FF) for the MFT record

Source: X-Ways AG, www.x-ways.net

Nonresident File in an MFT Record

To understand how data runs are assigned for nonresident MFT records, you should know that when a disk is created as an NTFS file structure, the OS assigns logical clusters to the entire disk partition. These assigned clusters, called **logical cluster numbers (LCNs)** , are sequentially numbered from the beginning of the disk partition, starting with the value 0. LCNs become the addresses that allow the MFT to link to nonresident files (files outside the MFT) on the disk's partition.

When data is first written to nonresident files, an LCN address is assigned to the file in the attribute 0x80 field of the MFT. This LCN becomes the file's **virtual cluster number (VCN)** , which is listed as zero: VCN(0). If there's not enough space at VCN(0)'s location because of excessive disk fragmentation, another data run is added. More VCNs are added as needed, and each additional VCN is sequentially numbered as VCN(1), VCN(2), and so on until all data is written to the drive.

The value in VCN(0) is the first cluster for the file; this value is the cluster's actual LCN. VCN(1) and other VCNs are the offset of the cluster's number from the previous VCN cluster position in the data run. For example, to determine the next data run location for VCN(0) for a fragmented file, simply add VCN(0)'s LCN value to the next VCN's offset value. So if VCN(0)'s LCN is 10000 and VCN(1) is 120, add VCN(1)'s 120 to VCN(0)'s LCN value of 10000 to get the starting LCN cluster for VCN(1), which is the LCN address 10120. If the file is fragmented more and there's a VCN(2), add VCN(1)'s LCN value to VCN(2)'s LCN value. This process is repeated for any additional VCNs assigned to a file.

VCNs are also signed integers so that if the next largest unused disk space is at a lower address than the previous VCN, the lower value address can be computed by simply adding a negative number to the VCN. For example, if the previous VCN data run is at offset 3000000 and the next available open area to receive data is at LCN 2900000, the VCN is $-100000\ (3000000 + [-100000] = 2900000)$.

The following two sections explain the basic configuration of resident and nonresident files managed by the MFT. By learning how data is stored in the MFT, a forensics examiner can manually reconstruct any residual data on NTFS-formatted disk media. You need to understand how these offsets are calculated for activities in **Chapter 16**.

The following descriptions of the values and functions of NTFS and the MFT aren't exhaustive, and future Windows updates could change these configurations. This discussion should be used as a quick reference for locating and interpreting data artifacts where you might find residual fragments from partially overwritten MFT records.

MFT Structures for File Data

When you're viewing an MFT record with a hexadecimal editor, the data is displayed in little endian format, meaning it's read from right to left. For example, the hexadecimal value 400 is displayed as 00 04 00 00, and the number 0x40000 is displayed as 00 00 04 00.

The first section of an MFT record is the header that defines the size and starting position of the first attribute. Following the header are attributes that are specific for the file type, such as an application file or a data file. MFT records for directories and system files have additional attributes that don't appear in a file MFT record. The following sections explain how data files are configured in the MFT. In **Chapter 16**, you see how these fields apply to data recovery.

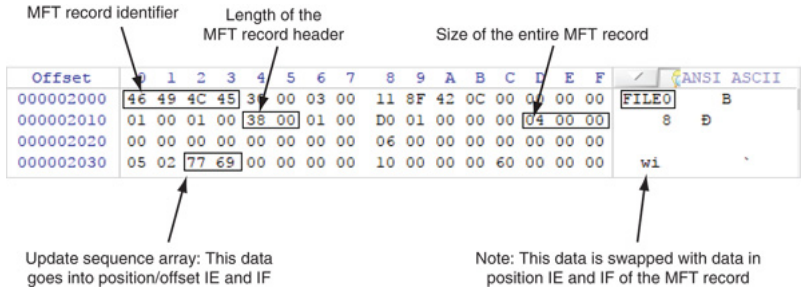
MFT Header Fields

For the header of all MFT records, the record fields of interest are as follows:

- *At offset 0x00*—The MFT record identifier FILE; the letter F is at offset 0.
- *At offset 0x1C to 0x1F*—Size of the MFT record; the default is 0x400 (1024) bytes, or two sectors.
- *At offset 0x14*—Length of the header, which indicates where the next attribute starts; it's typically 0x38 bytes.
- *At offset 0x32 and 0x33*—The update sequence array, which stores the last 2 bytes of the first sector of the MFT record. It's used only when MFT data exceeds 512 bytes. The update sequence array is used as a checksum for record integrity validation.

Figure 5-13 shows these fields and their relationships in the MFT record.

Figure 5-13.



Source: X-Ways AG, www.x-ways.net

An MFT Header

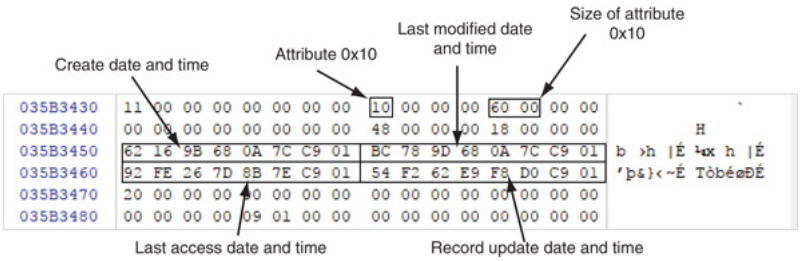
Attribute 0x10: Standard Information

Following the MFT header for a data file is the Standard Information attribute, 0x10, which has the following fields (see **Figure 5-14**):

- *At offset 0x38 from the beginning of the MFT record*—The start of attribute 0x10.

- *At offset 0x04 and 0x05 from the beginning of attribute 0x10*—Size of the 0x10 attribute.
- *At offset 0x18 to 0x1F*—The file's create date and time; all dates and times are stored in the Win32 Filetime format.
- *At offset 0x20 to 0x27*—The last modified date and time for the file.
- *At offset 0x28 to 0x2F*—The last access date and time.
- *At offset 0x30 to 0x2F*—The record access date and time.

Figure 5-14.



Source: X-Ways AG, www.x-ways.net

Attribute 0x10: Standard Information

Attribute 0x30: File Name

For files with filenames of eight or fewer characters, the MFT record has only one attribute 0x30. If a filename is longer than eight characters, there are two attribute 0x30s. The following description shows an MFT record with a short and long filename in attribute 0x30. The fields of interest for the short filename attribute 0x30 are as follows:

- *At offset 0x04 and 0x05 from the beginning of attribute 0x30*—The size of attribute 0x30.
- *At offset 0x5A from the 0x30 attribute's starting position*—The short filename; note that it's in Unicode.
- *At offset 0x20 to 0x27*—The file's create date and time; all dates and times are stored in Win32 Filetime format.
- *At offset 0x28 to 0x2F*—The last modified date and time for the file.
- *At offset 0x30 to 0x37*—The last access date and time.
- *At offset 0x38 to 0x3F*—The record update date and time.

Note

The date and time values in attribute 0x30 are usually the same as in attribute 0x10. On occasion, depending how data is copied to a disk and the Windows OS version, these values might differ substantially.

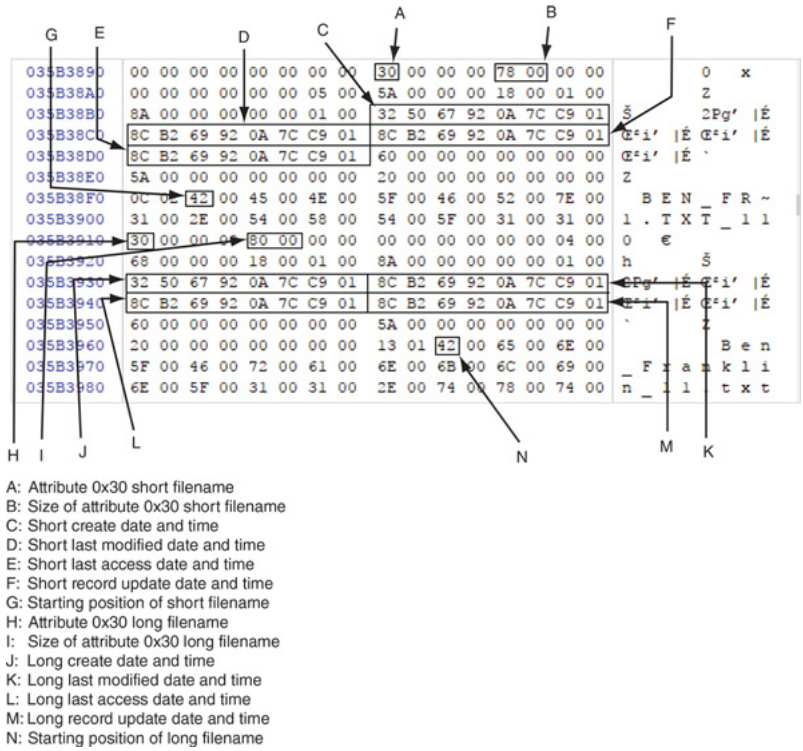
The following are fields of interest for the long filename attribute 0x30:

- *At offset 0x04 and 0x05 from the beginning of attribute 0x30*—The size of attribute 0x30.
- *At offset 0x5A from the 0x30 attribute's starting position*—The long filename; note that it's in Unicode.
- *At offset 0x20 to 0x27*—The file's create date and time; all dates and times are stored in Win32 Filetime format.

- *At offset 0x28 to 0x2F*—The last modified date and time for the file.
- *At offset 0x30 to 0x37*—The last access date and time.
- *At offset 0x38 to 0x3F*—The record update date and time.

Figure 5-15 shows these fields and their relationships in the MFT record.

Figure 5-15.



Source: X-Ways AG, www.x-ways.net

Attribute 0x30: Short and Long Filenames

Attribute 0x40: Object_ID

Depending on the Windows version, sometimes attribute 0x40 is listed in the MFT. This attribute contains file ownership and access control information and has the following fields:

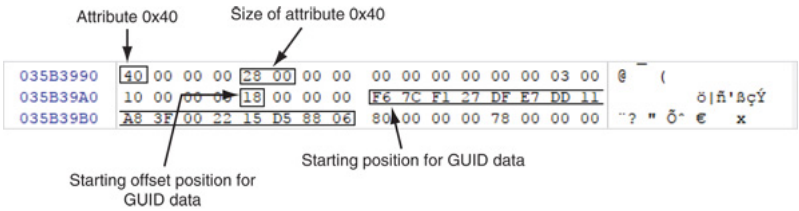
- *At offset 0x04 and 0x05 from the beginning of attribute 0x40*—The size of attribute 0x40
- *At offset 0x14*—Starting offset position for GUID data
- *At offset 0x18 to 0x27*—Starting position for GUID Object_ID data

In this example, only the GUID Object_ID is listed. In large enterprise systems, typically additional information is listed, such as the following:

- GUID Birth Volume ID
- GUID Birth Object ID
- GUID Birth Domain ID

Figure 5-16 shows these fields and their relationships in the MFT record.

Figure 5-16.



Source: X-Ways AG, www.x-ways.net

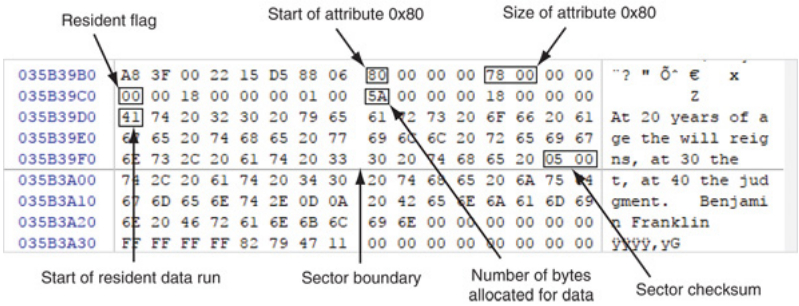
Attribute 0x40: Object_ID

Attribute 0x80: Data for a Resident File

For a resident file's attribute 0x80, the fields of interest are as follows (see **Figure 5-17**):

- *At offset 0x04 and 0x05 from the beginning of attribute 0x80*—Size of the attribute.
- *At offset 0x08*—The resident/nonresident flag; for resident data, it's set to 0x00.
- *At offset 0x10*—Number of bytes in the data run.
- *At offset 0x18*—Start of the resident data run.
- *At offset 0x1E and 0x1F from the beginning of the MFT header*—The sector checksum value, used to validate the first 512 bytes of the MFT record. The break between the first and second sectors is referred to as the sector boundary. The 2 bytes at positions 0x32 and 0x33 of the MFT header in the update sequence array field are where the actual values for these bytes are stored.

Figure 5-17.



Source: X-Ways AG, www.x-ways.net

Attribute 0x80: Data for a Resident File

The end of the MFT record is indicated by the hexadecimal values FF FF FF FF at the end of the record.

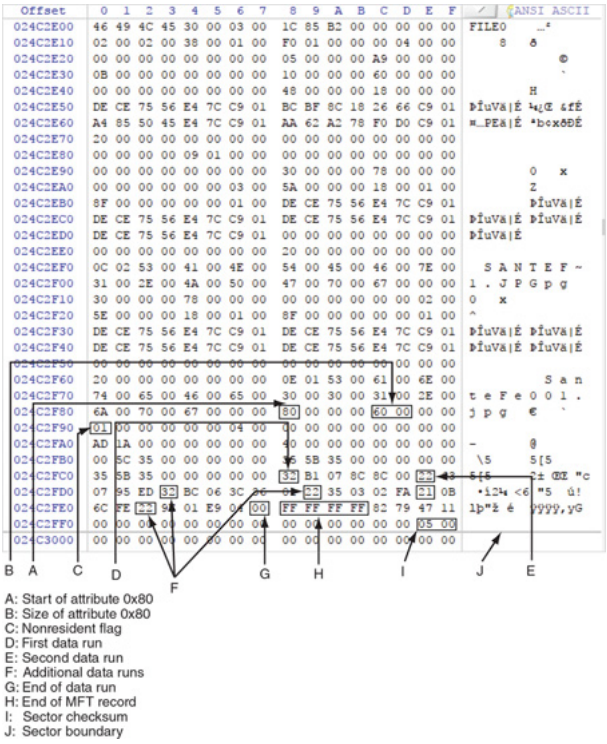
Attribute 0x80: Data for a Nonresident File

For a nonresident file, the fields of interest for attribute 0x80 are as follows:

- *At offset 0x04 and 0x05 from the beginning of attribute 0x80*—Size of the attribute.
- *At offset 0x08*—The resident/nonresident flag; for nonresident data, it's set to 0x01.
- *At offset 0x40*—The start of the data run. The first run is the LCN; if the file is fragmented, additional data runs follow, as shown in Figure 5-18. In this example, there are a total of six data runs, which means this file has several fragments.

Following the last data run, the value 0x00 indicates the end of the Data attribute. **Figure 5-18** shows these fields and their relationships in the MFT record.

Figure 5-18.



Source: X-Ways AG, www.x-ways.net

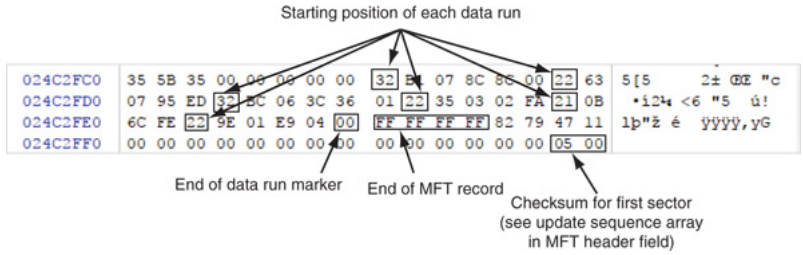
Attribute 0x80: Data for a Nonresident File

Interpreting a Data Run

As discussed, the first data run for a nonresident attribute 0x80 field starts at offset 0x40 from the beginning of the attribute. In this discussion, a file called SanteFe001.jpg is used as an example of how data runs are interpreted. Data runs have three components: The first component declares how many bytes in the attribute field are needed to store the values for the second and third components. The second component stores the number of clusters assigned to the data run, and the third component contains the starting cluster address value (the LCN or the VCN). This discussion uses a file with six fragments (data runs).

For the first component—the 32 shown in **Figure 5-19** as the data run's starting position—the second digit, 2, means that the next 2 bytes contain the number of clusters assigned to this data run. The first digit, 3, means that the next 3 bytes (after the number of clusters assigned) contain the cluster address value VCN(0); for the first data run, this value is the LCN.

Figure 5-19.

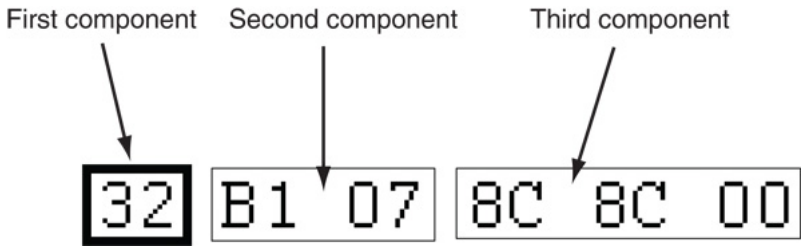


Source: X-Ways AG, www.x-ways.net

Multiple Data Runs

In **Figure 5-20**, the second component shows the 2 bytes needed to store the hexadecimal value (in little endian) for the number of clusters assigned to this data run. The number of clusters assigned to this data run is 7B1 (hexadecimal) or 1969 in decimal.

Figure 5-20.

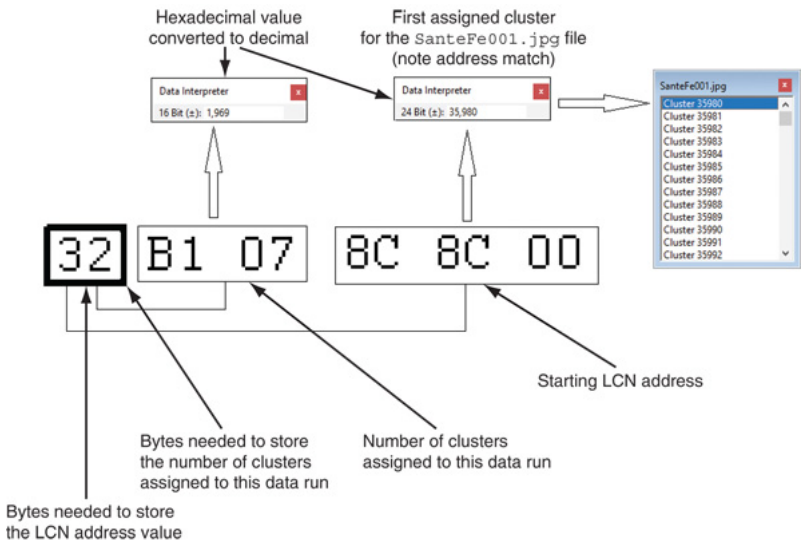


Source: X-Ways AG, www.x-ways.net

Data Run Components

As shown in **Figure 5-21**, for the third component, the starting assigned cluster address is 0x8C8C (hexadecimal), or 35980 in decimal. Because it's the first data run of the file, this address is the LCN.

Figure 5-21.

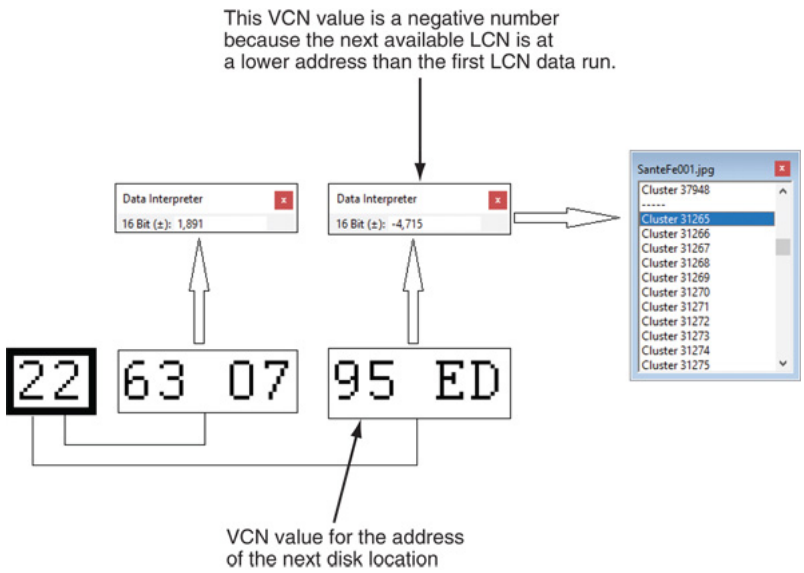


Source: X-Ways AG, www.x-ways.net

First Data Run with an LCN Address

Figures 5-22 and 5-23 show the second and third data runs for the SanteFe001.jpg file. For the second and all other data runs, the third component is a signed integer; for example, in Figure 5-22, this value is converted from a hexadecimal number to a negative decimal number. In NTFS, if the next available open area of a highly fragmented disk is at a lower address, a negative number is assigned as the VCN value. The way NTFS navigates to this second open area is by adding the VCN to the previous LCN. For example, the first data run has the LCN address 35980, and the second data run has the value -4715. The OS adds the two numbers, but because the second data run has a negative number, they're actually subtracted: $35980 + (-4715) = 31265$.

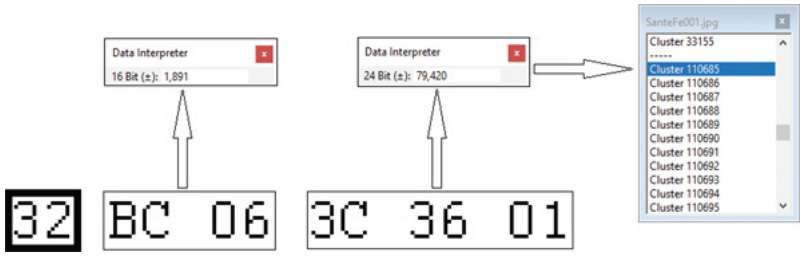
Figure 5-22.



Source: X-Ways AG, www.x-ways.net

Second Data Run with a VCN Address

Figure 5-23.



Source: X-Ways AG, www.x-ways.net

Third Data Run with a VCN Address

As you can see in the assigned cluster lists in **Figure 5-23**, the second fragment has a starting cluster number (an LCN) of 31265. In the third data run, the VCN value is a positive number.

Tip

For additional information on NTFS and its design, see http://dubeyko.com/development/FileSystems/NTFS/ntfsdoc.pdf or http://download.paragon-software.com/doc/manual_NTFS-HFS_for_Linux_8.1_User_Manual.pdf.

NTFS Alternate Data Streams

Of particular interest when you're examining NTFS disks are **alternate data streams** , which are ways data can be appended to existing files. When you're examining a disk, be aware that alternate data streams can obscure valuable evidentiary data, intentionally or by coincidence.

In NTFS, an alternate data stream becomes an additional file attribute and allows the file to be associated with different applications. As a result, it remains one data unit. You can also store information about a file in an alternate data stream. In its resource documentation Web page, Microsoft states: "For example, a graphics program can store a thumbnail image of a bitmap in a named data stream within the NTFS file containing the image." At a command prompt in Windows NT and later, you can create an alternate data stream with this DOS command:

```
C:\echo text_string > myfile.txt:stream_name
```

You can also use the following type command to redirect the contents of a small file to an alternate data stream:

```
C:\type textfile.txt > myfile.txt:stream1
```

In these commands, the alternate data stream is defined in the MFT by the colon between the file extension and the stream label. To display an alternate data stream's content as a simple text string, use this command:

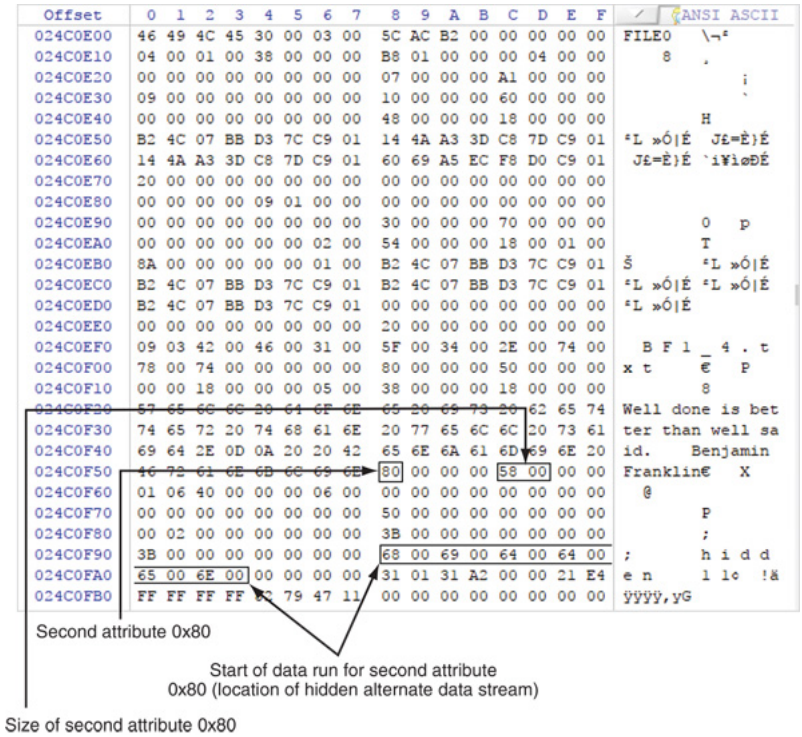
```
C:\more > myfile.txt:stream1
```

Note

If you save a file with alternate data streams attached to a FAT volume, the alternate data streams aren't transferred.

If you perform a keyword search and retrieve a file associated with a keyword, you might not be able to open the alternate data stream. An alternate data stream isn't displayed when you open a file in a text editor. The only way you can tell whether a file has an alternate data stream attached is by examining the file's MFT record entry. **Figure 5-24** shows the MFT record of a file containing a text alternate data stream. Note that there are two attribute 0x80 fields.

Figure 5-24.

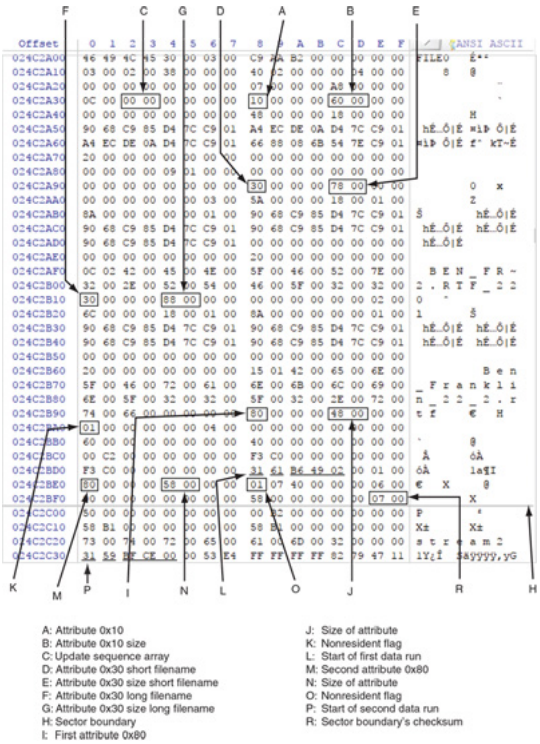


Source: X-Ways AG, www.x-ways.net

A Text Alternate Data Stream

Figure 5-25 shows what larger nonresident files look like in an MFT record. Note that the sector boundary's checksum value (item R) must be swapped with the update sequence array's value (item C).

Figure 5-25.



Source: X-Ways AG, www.x-ways.net

A Nonresident Alternate Data Stream

Tip

For more information on alternate data streams, see "Dissecting NTFS Hidden Streams" at www.forensicfocus.com/dissecting-ntfs-hidden-streams.

NTFS Compressed Files

To improve data storage on disk drives, NTFS provides compression similar to FAT DriveSpace 3, a Windows 98 compression utility. With NTFS, you can compress files, folders, or entire volumes. With FAT16, you can compress only a volume. On a Windows NT or later system, compressed data is displayed normally when you view it in Windows Explorer or applications such as Microsoft Word.

During an investigation, typically you work from an image of a compressed disk, folder, or file. Most forensics tools can uncompress and analyze compressed Windows data, including data compressed with the Lempel-Ziv-Huffman (LZH) algorithm and in formats such as PKZip, WinZip, and GNU gzip. However, forensics tools might have difficulty with third-party compression utilities, such as the .rar format. If you identify third-party compressed data, you need to uncompress it with the utility that created it.

NTFS Encrypting File System

When Microsoft introduced Windows 2000, it added optional built-in encryption to NTFS called **Encrypting File System (EFS)** . EFS uses **public key** and **private key** methods of encrypting files, folders, or disk volumes (partitions). Only the owner or user who encrypted the data can access encrypted files. The owner holds the private key, and the public key is held

by a certification authority, such as a global registry, network server, or company such as VeriSign.

When EFS is used in Windows 2000 and later, a **recovery certificate** is generated and sent to the local Windows administrator account. The purpose of the recovery certificate is to provide a mechanism for recovering files encrypted with EFS if there's a problem with the user's original private key. The recovery key is stored in one of two places. When a network user initiates EFS, the recovery key is sent to the local domain server's administrator account. On a stand-alone workstation, the recovery key is sent to the local administrator account.

Users can apply EFS to files stored on their local workstations or a remote server. Windows 2000 and later decrypt the data automatically when a user or an application accesses an EFS file, folder, or disk volume. In Windows Server 2003 and later, users can grant other users access to their EFS data. If a user copies a file encrypted with EFS to a folder that isn't encrypted, the copied data is saved in unencrypted format.

EFS Recovery Key Agent

The Recovery Key Agent implements the recovery certificate, which is in the Windows administrator account. Windows administrators can recover a key in two ways: through Windows or from a command prompt. These two commands are available from a command prompt: cipher and copy.

For information on how to use these commands, enter the question mark switch after each command. For example, type cipher /? and press Enter. Encrypted files aren't part of the FAT12, FAT16, or FAT32 file systems, so cipher works only on NTFS systems running Windows 2000 Professional or later. The copy command, however, works in both FAT and NTFS.

Note

In Vista Business Edition and later, Microsoft has added features to the cipher command that aren't available when encrypting data in Windows Explorer or File Explorer. One is the /w switch that overwrites all deleted files, making them impossible to recover with data recovery or forensics carving tools.

Tip

If you copy an encrypted file from an EFS-enabled NTFS disk or folder to a non-EFS storage media or folder, it's unencrypted automatically.

To recover an encrypted EFS file, a user can e-mail it or copy the file to the administrator, who can then run the Recovery Key Agent function to restore the file. For additional information, see "How It Works" (https://technet.microsoft.com/en-us/library/cc962103.aspx) and "The Encrypting File System" (https://technet.microsoft.com/en-us/library/cc700811.aspx).

Deleting NTFS Files

Typically, you use File Explorer to delete files from a disk. When a file is deleted in Windows NT and later, the OS renames it and moves it to the Recycle Bin. Another method is using the del (delete) MS-DOS command. This method doesn't rename and move the file to the Recycle Bin, but it eliminates the file from the MFT listing in the same way FAT does.

When you delete a file in Windows or File Explorer, you can restore it from the Recycle Bin. The OS takes the following steps when you delete a file or a folder in Windows or File Explorer:

1.

Windows changes the filename and moves the file to a subdirectory with a unique identity in the Recycle Bin.

2. Windows stores information about the original path and filename in the **Info2 file** , which is the control file for the Recycle Bin. It contains ASCII data, Unicode data, and the date and time of deletion for each file or folder.

NTFS files deleted at a command prompt function much like FAT files. (The following steps also apply when a user empties the Recycle Bin.) The OS performs the following tasks:

1. The associated clusters are designated as free—that is, marked as available for new data.
2. The $Bitmap file attribute in the MFT is updated to reflect the file's deletion, showing that this space is available.
3. The file's record in the MFT is marked as being available.
4. VCN/LCN cluster locations linked to deleted nonresident files are then removed from the original MFT record.
5. A run list is maintained in the MFT of all cluster locations on the disk for nonresident files. When the list of links is deleted, any reference to the links is lost.

Note

NTFS is more efficient than FAT at reclaiming deleted space. Deleted files are overwritten more quickly.

Resilient File System

With the release of Windows Server 2012, Microsoft created a new file system: **Resilient File System (ReFS)** . ReFS is designed to address very large data storage needs, such as the cloud. The following features are incorporated into ReFS's design:

- Maximized data availability
- Improved data integrity
- Designed for scalability

ReFS is an outgrowth of NTFS designed to provide a large-scale data storage access capability. It's intended only for data storage, so as of this writing, it can't be used as a boot drive. Windows 8/8.1 and later and Windows Server 2012 and later are the only Windows OSs that can access ReFS disk drives.

ReFS uses disk structures similar to the MFT in NTFS. Its storage engine uses a B+-tree sort method for fast access to large data sets. It also uses a method called "allocate-on-write" that copies updates of data files to new locations; similar to shadow paging, it prevents overwriting the original data files. The purpose of writing updates to new locations is to ensure that the original data can be recovered easily if a failure occurs in the update write to disk.

Tip

For more information on ReFS and other storage methods, see http://msdn.microsoft.com/en-us/library/windows/desktop/hh848060(v=vs.85).aspx or https://technet.microsoft.com/en-us/windows-server-docs/storage/refs/refs-overview.

Understanding Whole Disk Encryption

Loss of **personal identity information (PII)** and trade secrets caused by computer theft has become more of a concern. Company PII might consist of employees' full names, home addresses, and Social Security numbers. With this information, criminals could easily apply for credit card accounts in these employees' names. Trade secrets are any information a business keeps confidential because it provides a competitive edge over other companies. The inadvertent public release of this information could devastate a business's competitive edge.

Of particular concern is the theft of laptops and handheld devices, such as smartphones. If data on these devices isn't secured correctly, the owners could be liable for any damages incurred, such as stolen identities, credit card fraud, or loss of business caused by the release of trade secrets to the competition. Because of the PII problem, many states have enacted laws requiring any person or business to notify potential victims of the loss as soon as possible. To help prevent loss of information, software vendors, including Microsoft, now provide whole disk encryption (WDE, introduced in **Chapter 3**). This feature creates new challenges in examining and recovering data from drives.

Whole disk encryption tools offer the following features that forensics examiners should be aware of:

- Preboot authentication, such as a single sign-on password, fingerprint scan, or token (USB device)
- Full or partial disk encryption with secure hibernation, such as activating a password-protected screen saver
- Advanced encryption algorithms, such as Advanced Encryption Standard (AES) and International Data Encryption Algorithm (IDEA)
- Key management function that uses a challenge-and-response method to reset passwords or passphrases

WDE tools encrypt each sector of a drive separately. Many of these tools encrypt the drive's boot sector to prevent any efforts to bypass the secured drive's partition. To examine an encrypted drive, you must decrypt it first. An encryption tool's key management function typically uses a challenge-and-response method for decryption, which means you must run a vendor-specific program to decrypt the drive. Many vendors use a bootable CD or USB drive that prompts for a **one-time passphrase** generated by the key management function. If you need to decrypt the same computer a second time, you need a new one-time passphrase.

The biggest drawback to decrypting a drive is the several hours required to read, decrypt, and write each sector. The larger the drive, the longer decryption takes. After you've decrypted the drive, however, you can use standard acquisition methods to retrieve data.

Examining Microsoft BitLocker

BitLocker, introduced briefly in **Chapter 3**, is Microsoft's utility for protecting drive data. It's available in Windows Vista Enterprise and Ultimate editions, Windows 7, 8, and 10 Professional and Enterprise editions, and Windows Server 2008 and later. Guidance Software Encase can decrypt BitLocker drives, although the process can take a lot of time. BitLocker's current hardware and software requirements are as follows:

- A computer capable of running Windows Vista or later (non-home editions)
- The Trusted Platform Module (TPM) microchip, version 1.2 or newer
- A computer BIOS compliant with Trusted Computing Group (TCG)
- Two NTFS partitions for the OS and an active system volume with available space

- The BIOS configured so that the hard drive boots first before checking the CD/DVD drive or other bootable peripherals

Tip

For more information on BitLocker, see http://technet.microsoft.com/en-us/library/cc732774.aspx or go to http://technet.microsoft.com and search on "BitLocker."

Examining Third-Party Disk Encryption Tools

Several vendors offer third-party WDE utilities that often have more features than BitLocker. For example, BitLocker can encrypt only NTFS drives. If you want to encrypt a FAT drive, you need a third-party solution. Decrypting with third-party utilities typically follows the same process as in BitLocker, with some exceptions. Before using one of these utilities, make sure you investigate its features thoroughly. The following list describes some available third-party WDE utilities:

- Endpoint Encryption (www.symantec.com/products/endpoint-encryption) can be used on PCs, laptops, and removable media to secure an entire disk volume. This tool works in Windows Server 2008 and later and Windows 7 and later.
- Voltage SecureFile (www.voltage.com/products/data-security/hpe-securefile/) is designed for an enterprise computing environment.
- Jetico BestCrypt Volume Encryption (www.jetico.com/products/personal-privacy/bestcrypt-volume-encryption) provides WDE for older MS-DOS and current Windows systems.

With improved encryption methods, extracting digital evidence will become more difficult. Because of these challenges, you need to know how to make remote live acquisitions, discussed in **Chapter 10**.

Understanding the Windows Registry

When Microsoft created Windows 95, it consolidated initialization (.ini) files into the **Registry**, a database that stores hardware and software configuration information, network connections, user preferences (including usernames and passwords), and setup information. The Registry has been updated and is still used in Windows Vista and later.

For investigative purposes, the Registry can contain valuable evidence. To view the Registry, you can use the Regedit (Registry Editor) program for Windows 9x and Regedt32 for Windows 2000, XP, and Vista. For Windows 7 and 8, both Regedit and Regedt32 are available.

Tip

For more information on using Regedit and Regedt32, see the Windows Resource Kit documentation for the OS version. You can find it at https://support.microsoft.com/en-us/help/141377/differences-between-regedit.exe-and-regedt32.exe.

In general, you can use the Edit, Find menu command in Registry Editor to locate entries that might contain trace evidence, such as information identifying the last person who logged on to the computer, which is usually stored in user account information. You can also use the Registry to determine the most recently accessed files and peripheral devices. In addition, all installed programs store information in the Registry, such as Web sites accessed, recent files, and even chat rooms accessed.

As a digital forensics investigator, you should explore the Registry of all Windows systems. On a live system, be careful not to alter any Registry setting to avoid corrupting the system and possibly making it unbootable.

Note

Several third-party tools, such as FTK Registry Viewer, are also available for accessing the Registry.

Exploring the Organization of the Windows Registry

The Windows Registry is organized in a specific way that has changed slightly with each new version of Windows. However, the major Registry sections have been consistent, with some minor changes, since Windows 2000; they're slightly different in Windows 9x/Me. Before proceeding, review the following list of Registry terminology:

- *Registry*—A hierarchical database containing system and user information.
- *Registry Editor*—A Windows utility for viewing and modifying data in the Registry. There are two Registry Editors: Regedit and Regedt32 (introduced in Windows 2000).
- *HKEY*—Windows splits the Registry into categories with the prefix HKEY_. Windows 9x systems have six HKEY categories and Windows 2000 and later have five. Windows programmers refer to the "H" as the handle for the key.
- *Key*—Each HKEY contains folders referred to as keys. Keys can contain other key folders or values.
- *Subkey*—A key displayed under another key is a subkey, similar to a subfolder in Windows or File Explorer.
- *Branch*—A key and its contents, including subkeys, make up a branch in the Registry.
- *Value*—A name and value in a key; it's similar to a file and its data content.
- *Default value*—All keys have a default value that may or may not contain data.
- *Hives*—Hives are specific branches in HKEY_USER and HKEY_LOCAL_MACHINE. Hive branches in HKEY_LOCAL_MACHINE\Software are SAM, Security, Components, and System. For HKEY_USER, each user account has its own hive link to Ntuser.dat.

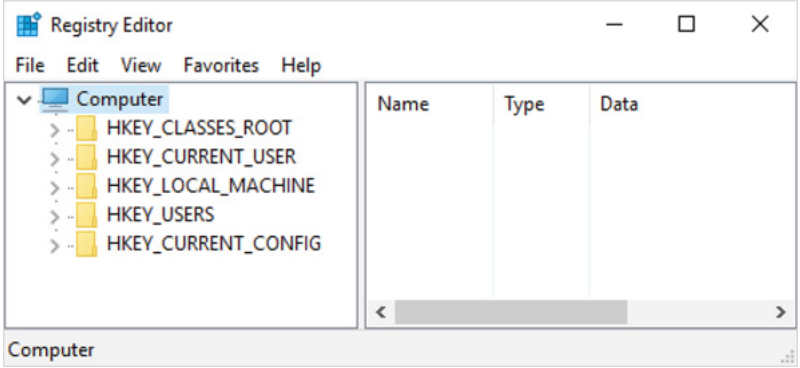
The next piece of the puzzle is learning where data files that the Registry reads are located. The number of files the Registry uses depends on the Windows version. In Windows 9x/Me, it uses only two files, User.dat and System.dat. In Windows NT and later, there are six files: Ntuser.dat, System.dat, SAM.dat, Software.dat, Security.dat, and Default.dat. When examining Registry data from a suspect drive after you have made an acquisition and are reviewing it in a forensics tool, you need to know the location of these files. Table 5-6 shows how Registry data files are organized and explains these files' purposes in Windows Vista and later. For information on older Windows Registry files, see http://support.microsoft.com/kb/250410.

Table 5-6. Registry file locations and purposes

Filename and location	Purpose of file
Users*user-account*\Ntuser.dat	User-protected storage area; contains the list of most recently used files and desktop configuration settings
Windows\system32\config\Default.dat	Contains the computer's system settings
Windows\system32\config\SAM.dat	Contains user account management and security settings
Windows\system32\config\Security.dat	Contains the computer's security settings
Windows\system32\config\Software.dat	Contains installed programs' settings and associated usernames and passwords

Filename and location	Purpose of file
Windows\system32\config\System.dat	Contains additional computer system settings
Windows\system32\config\systemprofile	Contains additional NTUSER information

Figure 5-26.



Viewing HKEYs in Registry Editor

When viewing the Registry with Registry Editor, you can see the HKEYs used in Windows (see **Figure 5-26**).

Table 5-7 describes the functions of Registry HKEYs.

Table 5-7. Registry HKEYs and their functions

HKEY	Function
HKEY_CLASSES_ROOT	A symbolic link to HKEY_LOCAL_MACHINE\SOFTWARE\Classes; provides file type and file extension information, URL protocol prefixes, and so forth
HKEY_CURRENT_USER	A symbolic link to HKEY_USERS; stores settings for the currently logged-on user
HKEY_LOCAL_MACHINE	Contains information about installed hardware and software
HKEY_USERS	Stores information for the currently logged-on user; only one key in this HKEY is linked to HKEY_CURRENT_USER
HKEY_CURRENT_CONFIG	A symbolic link to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware ProfileVxxxx (with xxxx representing the current hardware profile); contains hardware configuration settings
HKEY_DYN_DATA	Used only in Windows 9x/Me systems; stores hardware configuration settings

Examining the Windows Registry

Some forensics tools, such as X-Ways Forensics, OSForensics, Forensic Explorer, and FTK, have built-in or add-on Registry viewers. For this next activity, your company's Legal Department has asked you to search for any references to any e-mail addresses containing the name Denise or Robinson with the domain name outlook.com. A paralegal gives you a raw (dd) image file containing InCh05.img, a forensic image of a Windows 8 computer's hard drive used by Superior Bicycle employee Denise Robinson.

For this activity, you use OSForensics to examine Denise Robinson's NTUser.dat file. If you find any items of interest, add them to an OSForensics case report that you can give to the paralegal. The following steps explain how to generate a case report in OSForensics.

Note

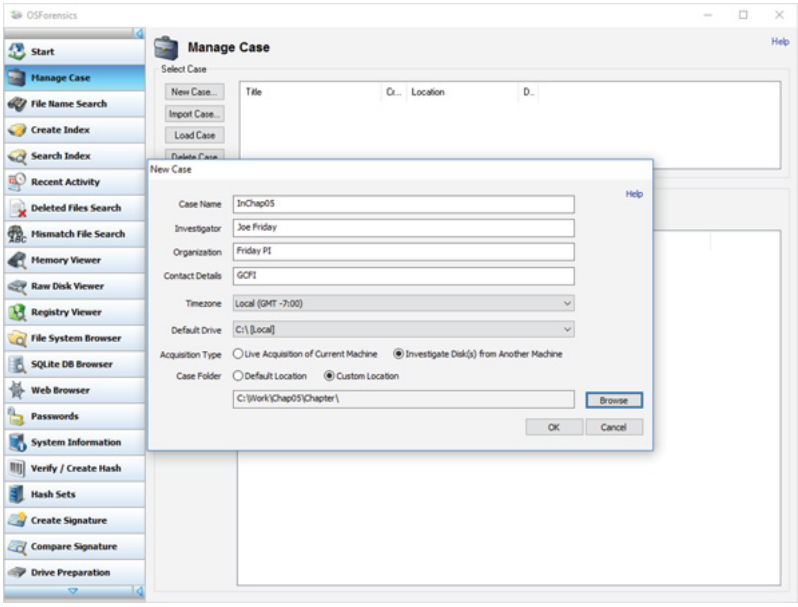
Before beginning this activity, download the zipped file in the downloads section for this chapter on the student companion site to your *Work*\Chap05\Chapter folder. When the download is finished, double-click the zipped file in File Explorer to extract the InChap05.img file. The work folder pathname you see in screenshots might differ.

To examine Registry files with OSForensics, follow these steps:

1. Start OSForensics with the **Run as administrator** option, and click **Continue Using Trial Version**.

2. In the left pane, click **Manage Case**, if necessary. In the Manage Case pane on the right, click the **New Case** button. In the New Case dialog box, type **InChap05** in the Case Name text box and your name in the Investigator text box. For the Acquisition Type setting, click the **Investigate Disk(s) from Another Machine** option button (see Figure 5-27). Click **Custom Location** for the Case Folder option. Click the **Browse** button on the lower right, navigate to and click your work folder, and then click OK twice.

Figure 5-27.



Source: PassMark Software, *www.osforensics.com*

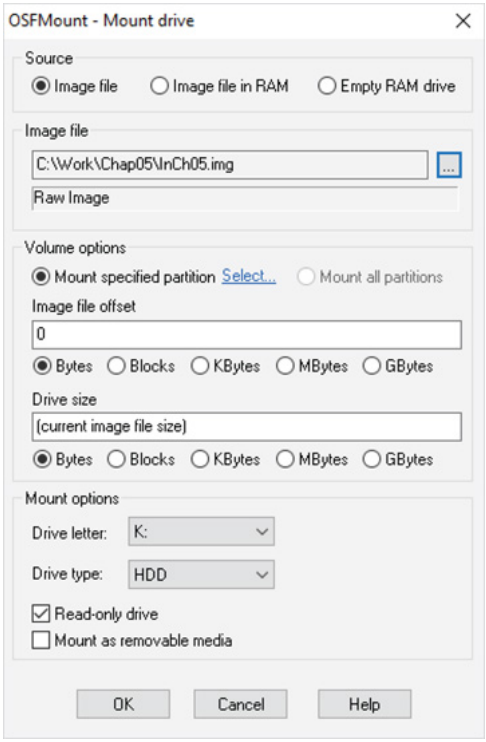
The New Case Dialog Box

Tip

Notice the drive letter in the OSFMount - Mount drive dialog box, which you use in **Step 3**. This image is mounted as read-only as an attached drive on your computer and becomes accessible to OSForensics.

3. Copy the **InChap05.img** file to the ***Work* \Chap05\Chapter** folder, if necessary. To mount this disk image, scroll down the navigation bar on the left, and click **Mount Drive Image**. In the Mounted virtual disks window, click the **Mount new** button. In the OSFMount - Mount drive dialog box that opens (see Figure 5-28), click the ... button next to the Image file text box, navigate to your work folder, click **InCh05.img** , click **Open**, and then click **OK**.

Figure 5-28.

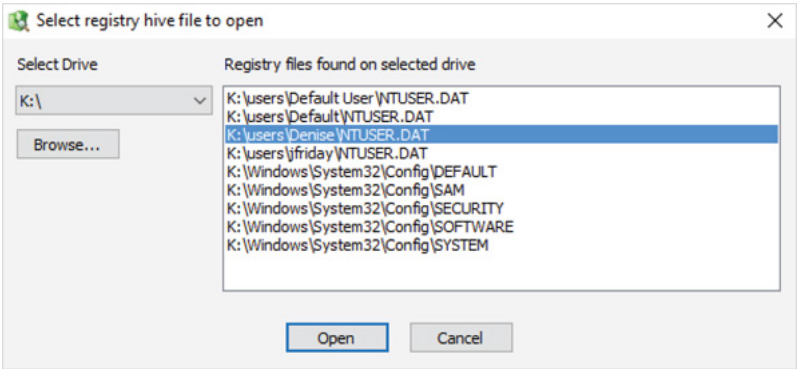


Source: PassMark Software, *www.osforensics.com*

Mounting a Drive in OSForensics

4. In the navigation bar on the left, click **Registry Viewer**. In the "Select registry hive file to open" dialog box, click the **Select Drive** list arrow, and then click the drive letter that was shown in Step 3 (see Figure 5-29). The drive letter on your system is likely to be different. In the list of files on the right, click ***DriveLetter* \users\Denise\NTUSER.DAT**, and then click **Open**.

Figure 5-29.

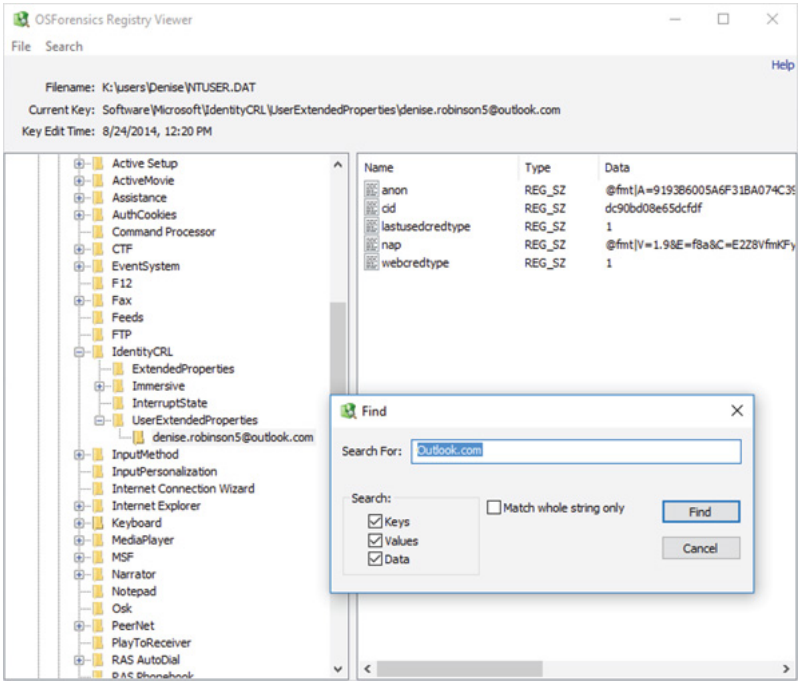


Source: PassMark Software, www.osforensics.com

The "Select Registry Hive File to Open" Dialog Box

5. In the OSForensics Registry Viewer, click **Search, Find** from the menu to open the Find dialog box. In the Search For text box, type **Outlook.com** (see Figure 5-30), and then click the **Find** button.

Figure 5-30.



Source: PassMark Software, *www.osforensics.com*

Entering a Search Term

6. In the Registry Viewer pane on the right, right-click the first search hit and click **Add to Case** to open the Please Enter New Case Item Details dialog box. In the Title text box, type **Outlook e-mail address for Denise Robinson**, and then click **OK**.

7. In the Find dialog box, click **Find** again. Right-click the next search hit and click **Add to Case**. Type **Outlook e-mail Web site** in the Title text box, and then click **OK**.

8. In the Find dialog box, click **Find** again. Right-click the next search hit and click **Add to Case**. Type **Denise Robinson's e-mail address** in the Title text box, and then click **OK**. Exit Registry Viewer.

9. In the main OSForensics window, click **Manage Case** in the navigation bar on the left. In the Manage Current Case pane on the right, click the **Generate Report** button. In the Export Report window, click **Browse** next to the Output Location text box, navigate to your work folder, and click **OK** to open the report in your Web browser. Scroll to the bottom of the navigation bar and click **Exit**. In the "Mounted virtual disks" window, click the **Dismount all & Exit** button. Click **Yes** in the OSMount warning message, and then click **OK** again to exit OSMount.

10. Review the contents of your report, and then exit your Web browser.

An extensive amount of information is stored in the Registry. With Registry data, you can ascertain when users went online, when they accessed a printer, and many other events. A lot of the information in the Registry is beyond the scope of this book, so you're encouraged to expand your knowledge by attending training sessions or classes.

Understanding Microsoft Startup Tasks

You should have a good understanding of what happens to disk data at startup. In some investigations, you must preserve data on the disk exactly as the suspect last used it. Any access to a computer system after it was used for illicit purposes alters your disk evidence. As you learned in **Chapter 3**, altering disk data lessens its evidentiary quality considerably. In

some instances, accessing a suspect computer incorrectly could make the digital evidence corrupt and less credible for litigation.

In the following sections, you learn what files are accessed when Windows starts. This information helps you determine when a suspect's computer was last accessed, which is particularly important with computers that might have been used after an incident was reported.

Startup in Windows 7, Windows 8, and Windows 10

Since Windows Vista, Microsoft has changed its approach to OS boot processes. In addition, Windows 8 and 10 are multiplatform OSs that can run on desktops, laptops, tablets, and smartphones. This discussion covers desktop and laptop computers running Windows 10, although Windows Vista, 7, and 8 are very similar.

All Windows 8 and 10 boot processes are designed to run on multiple devices, ranging from desktop or laptop systems to tablets and smartphones. In Windows Vista and later, the boot process uses a boot configuration data (BCD) store. For desktops and laptops (BIOS-designed systems), a BCD Registry file in the \Boot\Bcd folder is maintained to control the boot process. To access this file, you use the BCD Editor; Regedit and Regedt32 aren't associated with this file.

In Windows 8 and 10, the BCD contains the boot loader that initiates the system's bootstrap process when Windows starts. To access the Advanced Boot Options menu during the bootstrap process, press F8 or F12 when the system is starting. This menu enables you to choose between Safe Mode (or Enable Safe Mode, in Windows 8 and 10), Enable boot logging, or Disable Driver Signature Enforcement.

To access the computer's firmware to modify the boot priority order, press F2 or Delete. Follow the onscreen instructions to save the updates and reboot the computer. For additional information on Windows boot processes, refer to "Insight of Operating System booting process – Windows 10" (Vinit Pandey, https://vinitpandey.wordpress.com/2016/10/21/insight-of-operating-system-booting-process-windows-10/). For information on IBM-compatible laptop and desktop computers, see "The BIOS/MBR Boot Process" (https://neosmart.net/wiki/mbr-boot-process/). To learn more about changing the boot order of a Windows OS, see "Computer Boot Order: How to change computer boot order for booting from a CD/DVD, USB disk or floppy" (Margus Saluste, www.winhelp.us/computer-boot-order.html).

Startup in Windows NT and Later

Although Windows NT is much different from Windows 95 and 98, the startup method for the NT OSs—NT, 2000, and XP—is about the same. There are some minor differences in how certain system start files function, but they accomplish the same orderly startup.

Any computer using NTFS performs the following steps when the computer is turned on:

- Power-on self test (POST)
- Initial startup
- Boot loader
- Hardware detection and configuration
- Kernel loading
- User logon

Windows OSs use the files discussed in the following sections to start. These files can be located on the system partition or boot partition.

Startup Files for Windows Vista

When Microsoft developed Vista, it updated the boot process to use the new Extensible Firmware Interface (EFI) as well as the older BIOS system. The EFI boot firmware is designed to provide better protection against malware than BIOS does. EFI Vista's boot processes have also changed since Windows XP. The Ntldr program in Windows XP used to load the OS has been replaced with these three boot utilities:

- Bootmgr.exe—The Windows Boot Manager program controls boot flow and allows booting multiple OSs, such as booting Vista along with XP.
- Winload.exe—The Windows Vista OS loader installs the kernel and the Hardware Abstraction Layer (HAL) and loads memory with the necessary boot drivers.
- Winresume.exe—This tool restarts Vista after the OS goes into hibernation mode.

Windows Vista also includes the BCD editor for modifying boot options and updating the BCD registry file. The BCD store replaces the Windows XP Boot.ini file. For additional information on the BCD, see https://msdn.microsoft.com/en-us/library/windows/hardware/dn653287(v=vs.85).aspx.

Startup Files for Windows XP

Unless otherwise specified, most startup files for Windows XP are in the root folder of the system partition. **NT Loader (Ntldr)** loads the OS. When the system is powered on, Ntldr reads the **Boot.ini** file, which displays a boot menu. After you select the mode to boot to, Boot.ini runs Ntoskrnl.exe and reads Bootvid.dll, Hal.dll, and startup device drivers. Boot.ini specifies the Windows XP path installation and contains options for selecting the Windows version.

If a system has multiple boot OSs, including older ones such as Windows 9x or DOS, Ntldr reads **BootSect.dos** (a hidden file), which contains the address (boot sector location) of each OS.

When the boot selection is made, Ntldr runs **NTDetect.com** , a 16-bit real-mode program that queries the system for device and configuration data, and then passes its findings to Ntldr. This program identifies components and values on the computer system, such as the following:

- CMOS time and date value
- Buses attached to the motherboard, such as Industry Standard Architecture (ISA) or Peripheral Component Interconnect (PCI)
- Disk drives connected to the system
- Mouse input devices connected to the system
- Parallel ports connected to the system

NTBootdd.sys is the device driver that allows the OS to communicate with SCSI or ATA drives that aren't related to the BIOS. (On some workstations, a SCSI disk is used as the primary boot disk.) Controllers that don't use Interrupt 13 (INT-13) use NTBootdd.sys. It runs in privileged processor mode with direct access to hardware and system data.

Ntoskrnl.exe is the Windows XP OS kernel, located in the *systemroot*\Windows\System32 folder.

Hal.dll is the Hardware Abstraction Layer (HAL) dynamic link library, located in the systemroot\Windows\System32 folder. The HAL allows the OS kernel to communicate with the computer's hardware.

At startup, data and instruction code are moved in and out of the **Pagefile.sys** file to optimize the amount of physical RAM available.

The HKEY_LOCAL_MACHINE\SYSTEM Registry key contains information the OS requires to start system services and devices. This system Registry file is located in the *systemroot*\Windows\System32\Config\System folder.

Device drivers contain instructions for the OS for hardware devices, such as the keyboard, mouse, and video card, and are stored in the *systemroot*\Windows\System32\Drivers folder.

Note

To identify the specific path for *systemroot* at a DOS prompt, type set with no switches or parameters and press Enter. This command displays all current *systemroot* paths.

Windows XP System Files

Next, you need to examine the core OS files that Windows XP, 2000, and NT use, usually located in *systemroot*\Windows\System32 or *systemroot*\Winnt\System32. Table 5-8 lists the system files Windows XP uses. Although a few of these files are repeats of previous table entries, you should be aware of their key roles.

Table 5-8. Windows XP system files

Filename	Description
Ntoskrnl.exe	The XP executable and kernel
Ntkrnlpa.exe	The physical address support program for accessing more than 4 GB of physical RAM
Hal.dll	The Hardware Abstraction Layer (described earlier)
Win32k.sys	The kernel-mode portion of the Win32 subsystem
Ntdll.dll	System service dispatch stubs to executable functions and internal support functions
Kernel32.dll	Core Win32 subsystem DLL file
Advapi32.dll	Core Win32 subsystem DLL file
User32.dll	Core Win32 subsystem DLL file
Gdi32.dll	Core Win32 subsystem DLL file

Contamination Concerns with Windows XP

When you start a Windows XP NTFS workstation, several files are accessed immediately. When any of these or other related OS files are accessed at startup, the last access date and time stamp for the files changes to the current date and time. This change destroys any potential evidence that shows when a Windows XP workstation was last used. For this reason, you should have a strong working knowledge of the startup process.

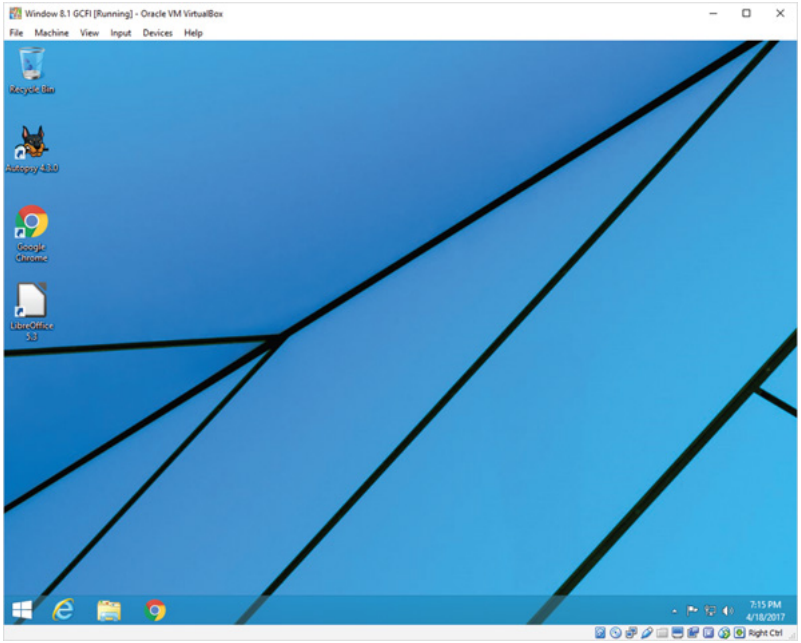
Understanding Virtual Machines

New versions of OSs and applications are released frequently, but older versions are still widely used. As an investigator, you'll face the challenge of having enough resources to support the variety of software you're likely to encounter. More companies are turning to virtualization to reduce the cost of hardware purchases, so the number of investigations involving virtual machines will increase as this practice continues.

As an investigator, you might need a virtual server to view legacy systems, and you might need to forensically examine suspects' virtual machines. **Virtual machines** enable you to run another OS on an existing physical computer (known as the host computer) by emulating a computer's hardware environment. Figure 5-31 shows an Oracle VM VirtualBox virtual machine running Windows 8.1 on the desktop of a host computer. Typically, a virtual machine consists of several files. The two main files are the configuration file containing hardware settings, such as RAM, network configurations, port settings, and so on, and the virtual hard

disk file, which contains the boot loader program, OS files, and users' data files. (Depending on the virtualization software, these files might be organized differently.)

Figure 5-31.



Source: Oracle VirtualBox, www.virtualbox.org

A Virtual Machine Running on the Host Computer's Desktop

Another reason for using a virtual machine in an investigation is to emulate actions taken by a suspect or even by malware. Several forensics analysis tools can convert a forensic image to an **ISO image** or a **virtual hard disk (VHD)** file, which enables you to run a suspect's computer in a virtual environment. This feature is useful for analyzing malware to see how it behaves without corrupting or contaminating your workstation.

A virtual machine acts like any other computer but with a twist: It performs all the tasks the OS running on the physical computer can, up to a certain point. The virtual machine recognizes hardware components of the host computer it's loaded on, such as the mouse, keyboard, and CD/DVD drive. However, the guest OS (the one running on a virtual machine) is limited by the host computer's OS, which might block certain operations. For example, most virtual machines recognize a CD/DVD drive because the host computer defaults to autodetect. Some virtual machines don't recognize a USB drive; this capability varies with the virtualization software. Although networking capabilities are beyond the scope of this book, be aware that virtual machines can use bridged, Network Address Translation (NAT), or other network configurations to determine how they access the Internet and communicate with systems on the local network.

Say your company has upgraded to Windows 10, but you still have a few applications that require Windows XP. Not a problem! Choose your virtualization software, install the Windows XP OS and the applications you want to run, and you're ready to go. Depending on the host computer's hard drive size and amount of RAM, you can have an entire virtual network running on one physical computer. One advantage is that if you're running several virtual machines, you can pause some of the guest OSs to keep them from consuming CPU cycles and then resume them when needed.

In digital forensics, virtual machines make it possible to restore a suspect drive on a virtual machine and run nonstandard software the suspect might have loaded, for example. You can

browse through the drive's contents, and then go back to the forensic image and test the items you found. Remember that in forensics, everything should be reproducible. Therefore, anything you found in the virtual machine re-creation of the suspect drive should exist in the forensic image, too.

From a network forensics standpoint, you need to be aware of some potential issues, such as a virtual machine used to attack another system or network. The technology is still developing, so it's unclear how much of the physical drive is represented in the virtual disk file. File slack, unallocated space, and so forth don't exist on a virtual machine, so many standard items don't work on virtual drives.

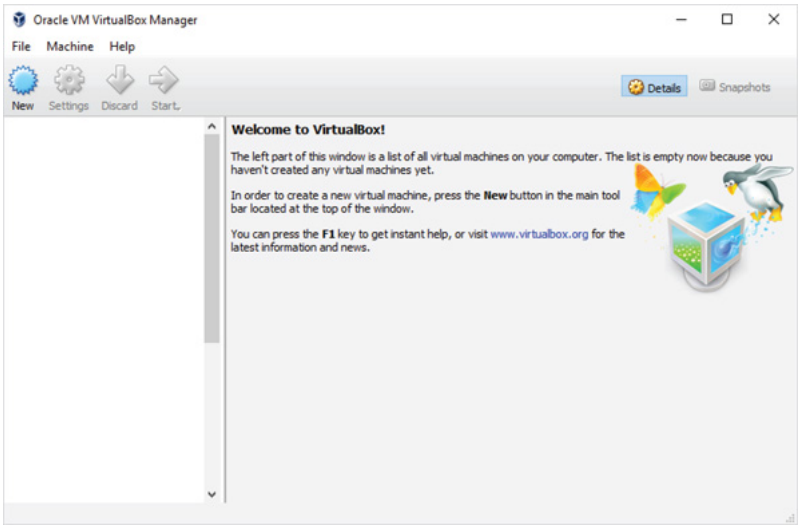
Creating a Virtual Machine

Some common applications for creating virtual machines are VMware Server, VMware Player and VMware Workstation, Oracle VM VirtualBox, Microsoft Virtual PC, and Microsoft HyperV, available in current versions of Windows Server. VirtualBox is an open-source program that can be downloaded from www.virtualbox.org.

Consult with your instructor before doing the following activity, which shows you how to create a virtual machine in VirtualBox and install Windows 7 as the virtual OS. You can use these steps to install other legacy and current OSs.

1. Start a Web browser, and go to www.virtualbox.org. Download and install VirtualBox.
2. Start VirtualBox. In the Oracle VM VirtualBox Manager, click the New icon at the upper left (see Figure 5-32) to start the Create Virtual Machine Wizard.

Figure 5-32.

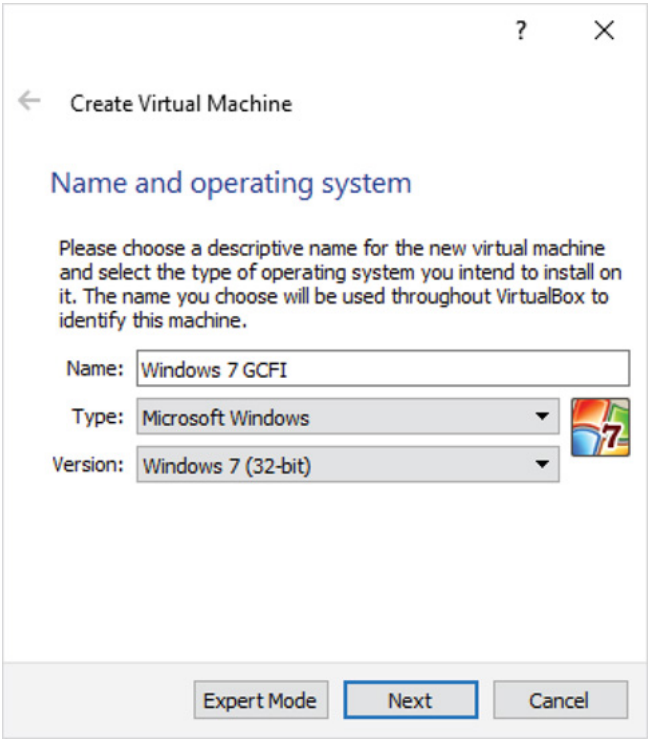


Source: Oracle VirtualBox, www.virtualbox.org

The Oracle VM VirtualBox Manager

3. In the "Name and operating system" window, type **Windows 7 GCFI** for the virtual machine name (see Figure 5-33). If necessary, click the **Type** list arrow, and click **Microsoft Windows**; then click the **Version** list arrow, and click **Windows 7 (32-bit)**. (If you have another version of Windows, click that version.) Click **Next**.

Figure 5-33.



Source: Oracle VirtualBox, www.virtualbox.org

Entering a Virtual Machine Name

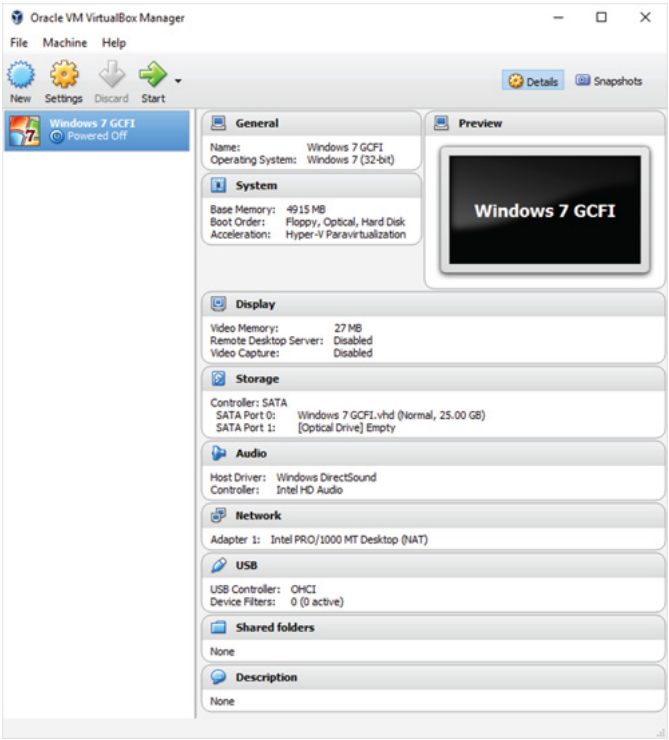
4. In the "Memory size" window, adjust the allocated memory to about 50% of your workstation's total amount of RAM, and then click **Next**.
5. In the "Hard drive" window, click **Create a virtual drive now**, and then click **Create**.
6. In the "Hard drive file type" window, click **VHD (Virtual Hard Disk)**, and then click **Next**

Note

VirtualBox offers versatility in its virtual hard disk file options. By selecting the VHD option, you can load the virtual hard disk file into other virtualization programs, such as VMware.

7. In the "Storage on physical hard drive" window, click **Dynamically allocated**, and then click **Next**.
8. In the File location and size window, expand the default 25 GB if you think you need more storage space allocated, and then click **Create**. When VirtualBox finishes creating the virtual machine, the window shown in Figure 5-34 is displayed. Leave VirtualBox running for the next activity.

Figure 5-34.



Source: Oracle VirtualBox, www.virtualbox.org

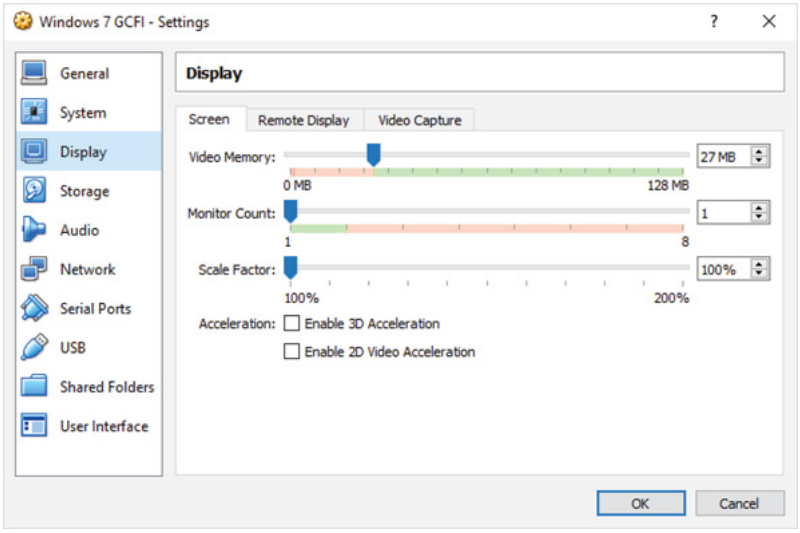
Displaying a Created Virtual Machine

In the following activity, you use an ISO image that your instructor will provide for installing Windows 7 as a guest OS. (You can also install other Windows OSs and most Linux distributions as guest OSs.) For any guest OS, you must have a valid product key to install it. You can get the product key from your instructor.

1. In the Oracle VM VirtualBox Manager, click the **Settings** icon. In the Windows 7 Settings dialog box, click **System** in the left pane, and click to clear the **Floppy** check box for the boot order (leaving the CD/DVD and Hard Disk check boxes selected).

2. Next, click **Display** in the left pane, and click the **Screen** tab, if necessary. Adjust the **Video Memory** slider to at least 27 MB (see Figure 5-35).

Figure 5-35.



Source: Oracle VirtualBox, www.virtualbox.org

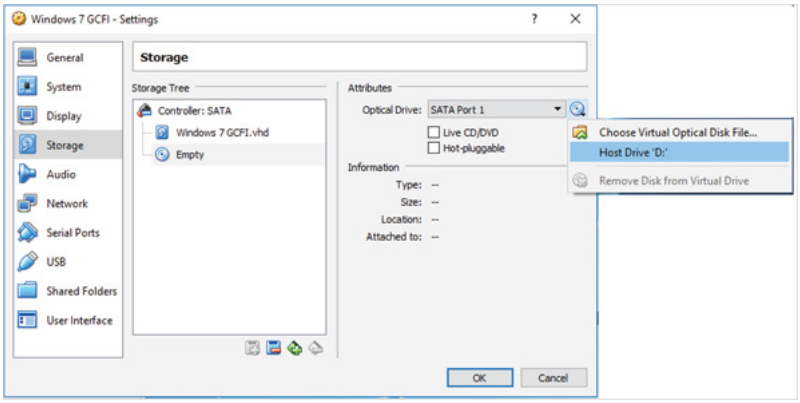
Adjusting the Video Memory

Note

Depending on the amount of video memory on your workstation, you might need to adjust it so that your monitor can display the virtual session correctly. For more information on this setting and other VirtualBox features, see www.virtualbox.org/wiki/Documentation.

3. Click **Storage** in the left pane, click **Empty** in the Storage Tree section, and then click the down arrow with the disk icon in the Attributes section, as shown in Figure 5-36. If you have a Windows ISO file, click **Choose Virtual Optical Disk File**, click an ISO image to install, and then click **OK**. If you have a Windows installation DVD, click **Host Drive 'D:'**, and then click **OK**. In the Oracle VM VirtualBox Manager, click **Start**.

Figure 5-36.



Source: Oracle VirtualBox, www.virtualbox.org

Selecting a Source Drive

Note

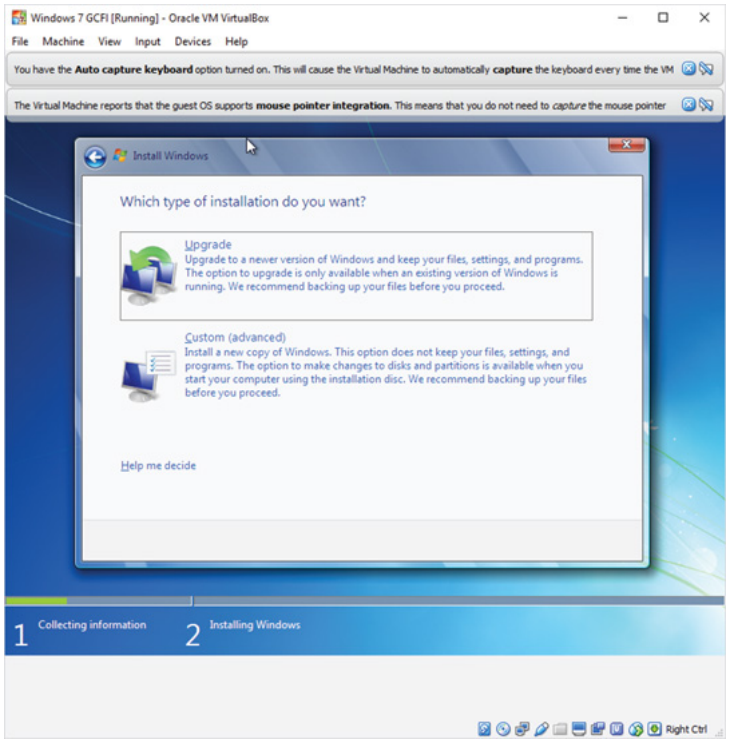
In this example, the installation disc for the source OS, Windows 7, is in the DVD drive, lettered D. Your workstation might show a different drive letter, such as E, if your hard drive has only one partition.

Tip

If VirtualBox displays the error message "Failed to open a session for the virtual machine," restart your computer, access the BIOS or UEFI firmware, and enable virtualization. For instructions, see your computer's hardware documentation. For additional information on BIOS, see "How to Enable Intel Virtualization Technology (VT-x) and AMD-V in BIOS on a Laptop or Desktop" (Dinesh, www.sysprobs.com/disable-enable-virtualization-technology-bios). For information on UEFI, see "How to Enable Intel VT-x in Your Computer's BIOS or UEFI Firmware" (Chris Hoffman, www.howtogeek.com/213795/how-to-enable-intel-vt-x-in-your-computers-bios-or-uefi-firmware/).

4. Follow the prompts to continue installing Windows 7 as a guest OS on your virtual machine. If the "Which type of installation do you want?" window is displayed, click **Custom (advanced)**, as shown in Figure 5-37. Exit VirtualBox.

Figure 5-37.



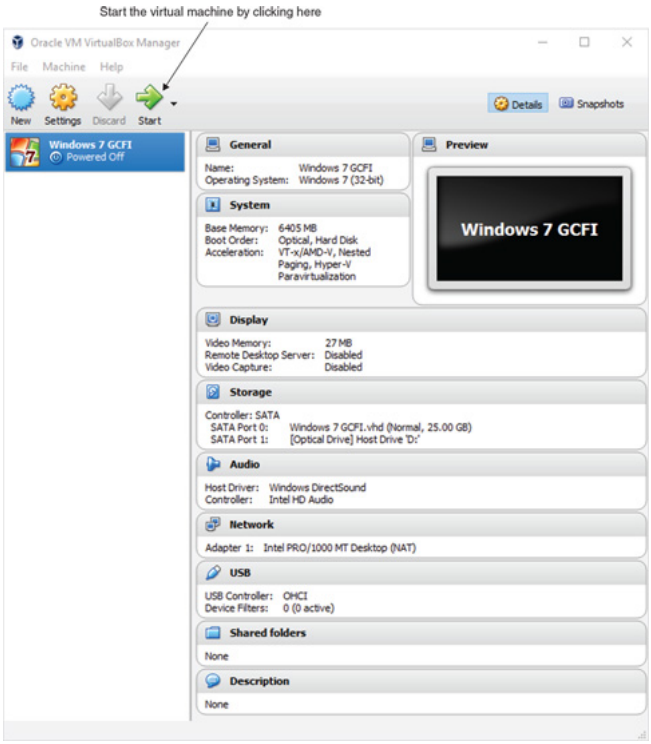
Source: Oracle VirtualBox, www.virtualbox.org

Selecting a Windows Installation Option

To start a virtual session in VirtualBox, select a virtual machine you created, and then click the Start icon (see **Figure 5-38**). You see standard boot prompts for the logon name and password you defined during the OS installation. The guest OS works as though it were running on a stand-alone workstation. You can add other applications to this virtual environment to

perform tasks as needed. To terminate the session, simply perform the usual Windows shutdown procedure.

Figure 5-38.



Source: Oracle VirtualBox, www.virtualbox.org

Starting a Virtual Machine Session

Be aware that as you install software and perform other tasks, you might encounter problems with recognition of the CD/DVD drive, for example. Virtual machines present some challenges because they are limited by the host computer they're loaded on. For this reason, many legal issues need to be addressed before these systems are accepted for use in court.

Chapter Summary

- When starting a suspect's computer, using boot media (such as forensic boot CDs or USB drives) is important to ensure that disk evidence isn't altered. You should access a suspect computer's BIOS to configure the computer to boot to these CDs or USB drives.
- The Master Boot Record (MBR) stores information about partitions on a disk.
- Microsoft used FAT12 and FAT16 on older operating systems, such as MS-DOS, Windows 3.x, and Windows 9x. The maximum partition size is 2 GB. Newer systems use FAT32. FAT12 is now used mainly on floppy disks and small USB drives. VFAT, created for Windows 95, allows filenames longer than eight characters.
- To find a hard disk's capacity, use the cylinders, heads, and sectors (CHS) calculation. To find a disk's byte capacity, multiply the number of heads, cylinders, and sectors.
- Sectors are grouped into clusters and clusters are chained because the OS can track only a given number of allocation units (65,536 in FAT16 and 4,294,967,296 in FAT32).
- Solid-state drives use wear-leveling to ensure even use of memory cells. It transfers data to unused memory cells so that all cells have an equal amount of reads and writes. The previously assigned memory cells are listed as unallocated space. After a predetermined time, the unallocated memory cells are overwritten with binary 1s.
- When files are deleted in a FAT file system, the hexadecimal value 0x05 is inserted in the first character of the filename in the directory.
- NTFS is more versatile because it uses the Master File Table (MFT) to track file information. Approximately the first 512 bytes of data for small files (called resident files) are stored in the MFT. Data for larger files (called nonresident files) is stored outside the MFT and linked by using cluster addresses.
- Records in the MFT contain attribute IDs that store metadata about files.
- In NTFS, alternate data streams can obscure information that might be of evidentiary value to an investigation.
- File slack, RAM slack (in older Windows OSs), and drive slack are areas in which valuable information, such as downloaded files, swap files, passwords, and logon IDs, can reside on a drive.
- NTFS can encrypt data with Encrypting File System (EFS) and BitLocker. Decrypting data with these methods requires using recovery certificates. BitLocker is Microsoft's whole disk encryption (WDE) utility that can be decrypted by using a one-time passphrase.
- The Resilient File System (ReFS), available only in Windows 8 and later and Windows Server 2012 and later, provides access to large disk storage systems.
- With a hexadecimal editor, you can determine information such as file type and OS configurations.
- NTFS can compress files, folders, or an entire volume. FAT16 can compress only entire volumes.
- The Registry in Windows keeps a record of attached hardware, user preferences, network connections, and installed software. It also contains information such as passwords in two binary files: System.dat and User.dat.

- Every user with an account on a Windows computer has his or her own Ntuser.dat file. Windows 9x user information is stored in User.dat.
- Virtualization software enables you to run other OSs on a host computer. Virtual machines are beneficial if, for example, you need to run a previous OS to test old software that won't run on newer OSs.
- Preserving data exactly as it was when a system was last used by a suspect is crucial. Accessing a suspect's disk without a write-blocking device alters the evidence.

Key Terms

alternate data streams
American Standard Code for Information Interchange (ASCII)
areal density
attribute ID
Boot.ini
BootSect.dos
bootstrap process
clusters
cylinder
data runs
device drivers
drive slack
Encrypting File System (EFS)
File Allocation Table (FAT)
file slack
file system
geometry
Hal.dll
head
head and cylinder skew
High Performance File System (HPFS)
Info2 file
ISO image
logical addresses
logical cluster numbers (LCNs)
Master Boot Record (MBR)
Master File Table (MFT)
metadata
NTBootdd.sys
NTDetect.com
NT File System (NTFS)
NT Loader (Ntldr)
Ntoskrnl.exe
one-time passphrase

Pagefile.sys
partition
Partition Boot Sector
partition gap
personal identity information (PII)
physical addresses
private key
public key
RAM slack
recovery certificate
Registry
Resilient File System (ReFS)
sector
track density
tracks
unallocated disk space
Unicode
UTF-8 (Unicode Transformation Format)
virtual cluster number (VCN)
virtual hard disk (VHD)
virtual machines
wear-leveling
zone bit recording (ZBR)

Review Questions

1. On a Windows system, sectors typically contain how many bytes?
    a. 256
    b. 512
    c. 1024
    d. 2048
2. What does CHS stand for?
3. Zone bit recording is how disk manufacturers ensure that a platter's outer tracks store as much data as possible. True or False?
4. Areal density refers to which of the following?
    a. Number of bits per disk
    b. Number of bits per partition
    c. Number of bits per square inch of a disk platter
    d. Number of bits per platter
5. Clusters in Windows always begin numbering at what number?
6. How many sectors are typically in a cluster on a disk drive?
    a. 1

   b. 2 or more
   c. 4 or more
   d. 8 or more

7. List three items stored in the FAT database.
8. What does the Ntuser.dat file contain?
9. In FAT32, a 123 KB file uses how many sectors?
10. What is the space on a drive called when a file is deleted? (Choose all that apply.)
    a. Disk space
    b. Unallocated space
    c. Drive space
    d. Free space
11. List two features NTFS has that FAT does not.
12. What does MFT stand for?
13. In NTFS, files smaller than 512 bytes are stored in the MFT. True or False?
14. In Windows 7 and later, how much data from RAM is loaded into RAM slack on a disk drive?
15. What's a virtual cluster number?
16. Why was EFI boot firmware developed?
17. Device drivers contain what kind of information?
18. Which of the following Windows 8 files contains user-specific information?
    a. User.dat
    b. Ntuser.dat
    c. System.dat
    d. SAM.dat
19. Virtual machines have which of the following limitations when running on a host computer?
    a. Internet connectivity is restricted to virtual Web sites.
    b. Applications can be run on the virtual machine only if they're resident on the physical machine.
    c. Virtual machines are limited to the host computer's peripheral configurations, such as mouse, keyboard, CD/DVD drives, and other devices.
    d. Virtual machines can run only OSs that are older than the physical machine's OS.
20. An image of a suspect drive can be loaded on a virtual machine. True or False?
21. EFS can encrypt which of the following?
    a. Files, folders, and volumes
    b. Certificates and private keys
    c. The global Registry
    d. Network servers
22. What happens when you copy an encrypted file from an EFS-enabled NTFS disk to a non-EFS disk or folder?

a. The file can no longer be encrypted.

b. EFS protection is maintained on the file.

c. The file is unencrypted automatically.

d. Only the owner of the file can continue to access it.

Hands-On Projects

There are no data files to download for this chapter's projects, but create a *Work*\Chap05\Projects folder on your system before starting the projects.

Hands-On Project 5-1.

In this project, you compare two files created in Microsoft Office to determine whether the files are different at the hexadecimal level. Keep a log of what you find. Follow these steps:

1. Start Word, and in a new document, type **This is a test**.
2. Save the file as **Mywordnew.docx** in your work folder, using **Word Document (*.docx)** as the file type. Exit Word.
3. Start Excel, and in a new workbook, enter a few random numbers. Save the file in your work folder as **Myworkbook.xlsx** , using **Excel Workbook (*.xlsx)** as the file type.
4. Exit Excel, and start WinHex (running it as an Administrator).
5. Click **File, Open** from the menu. In the Open dialog box, navigate to your work folder and double-click **Mywordnew.docx** .
6. Notice the file hexadecimal header 50 4B 03 04 14 00 06 00 starting at offset 0. Click **Edit, Copy All** from the menu, and then click **Editor Display**.
7. Start Notepad, and in a new document, press **Ctrl+V** to paste the copied data. Leave this window open.
8. Click **File, Open** from the WinHex menu. In the Open dialog box, navigate to your work folder and double-click **Myworkbook.xlsx** .
9. Repeat **Step 6**.
10. Paste the data you just copied under the Word document header information you pasted previously.
11. In the Notepad window, add your observations about the two files' header data. Save this file as C5Prj01.txt and turn it in to your instructor. Exit WinHex.

Hands-On Project 5-2.

In this project, you explore the MFT and learn how to locate date and time values in the metadata of a file you create. These steps help you identify previously deleted fragments of MFT records that you might find in unallocated disk space or in residual data in Pagefile.sys. You need the following for this project:

- A system running Windows with the C drive formatted as NTFS
- Notepad to create a small text file
- WinHex (downloaded from http://x-ways.net and installed, if you haven't done so already) to analyze the metadata in the MFT

1. Start Notepad, and create a text file with one or more of the following lines:
   - A countryman between two lawyers is like a fish between two cats.
   - A slip of the foot you may soon recover, but a slip of the tongue you may never get over.

- An investment in knowledge always pays the best interest.
- Drive thy business or it will drive thee.

2. Save the file in your work folder as **C5Prj02.txt** , and exit Notepad. (If your work folder isn't on the C drive, make sure you save the file on your C drive to have it entered in the $MFT files you copy later.)

3. Next, review the material in "MFT and File Attributes," paying particular attention to attributes 0x10 and 0x30 for file dates and times. The following charts show the offset byte count starting at position FILE of the file's MFT record for the date and time stamps:

Note

The offsets listed in the following charts are from the first byte of the MFT record, not the starting position of the specific attributes 0x10 and 0x30.

0x10 $Standard Information (data starts at offset 0x18)

Description of field	Offset position	Byte size
C Time (file creation)	0x50	8
A Time (file altered)	0x58	8
L Time (Last accessed)	0x60	8

0x30 $File_Name (data starts at offset 0x18)

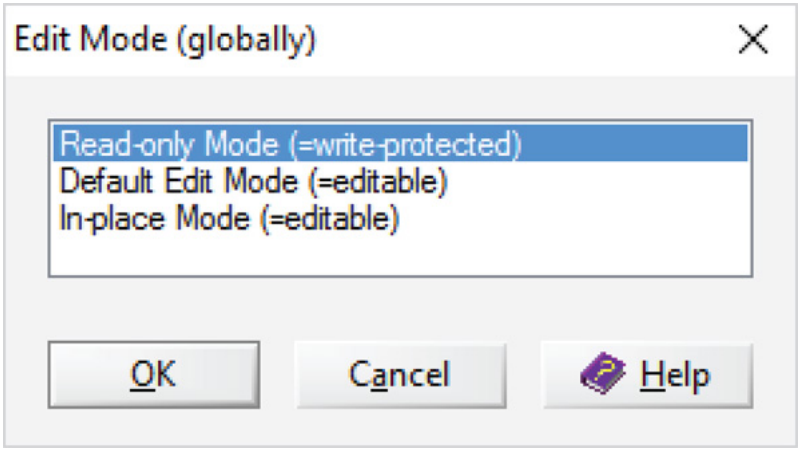
Description of field	Offset position	Byte size
C Time (file creation)	0xB8	8
A Time (file altered)	0xC0	8
R Time (file read)	0xC8	8
M Time (MFT change)	0xD0	8

Next, you examine the metadata of the C5Prj02.txt file stored in the $MFT file. Follow these steps:

1. Start WinHex with the **Run as administrator** option. If you see an evaluation warning message, click **OK**.

2. As a safety precaution, click **Options, Edit Mode** from the menu. In the Select Mode (globally) dialog box, click **Read-only Mode (=write protected)**, as shown in Figure 5-39, and then click **OK**.

Figure 5-39.



Source: X-Ways AG, www.x-ways.net

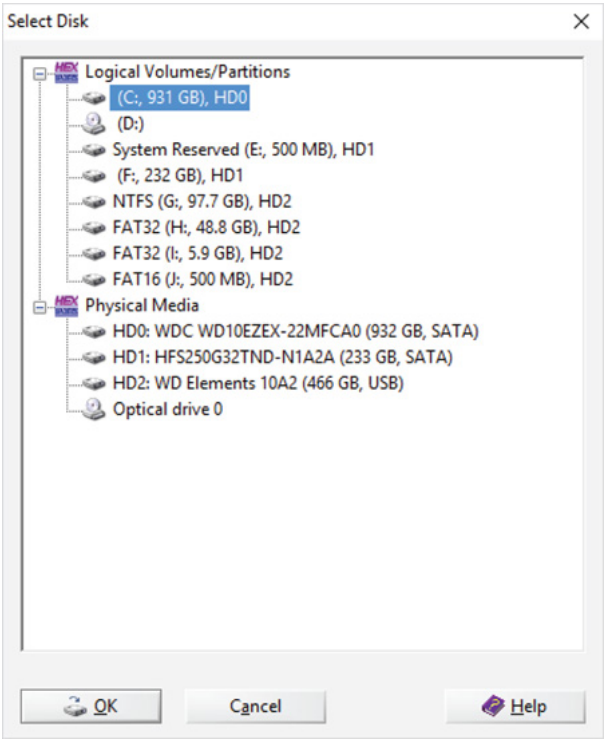
Changing WinHex to Read-Only Mode

Note

WinHex defaults to an editable mode, which means you can alter data in important system files and possibly corrupt them. When using a disk editor such as WinHex, always set it to read-only mode, unless you need to make specific modifications to data.

3. Click **Tools, Open Disk** from the menu. In the View Disk dialog box, click the **C:** drive (or the drive where you saved C5Prj02.txt), as shown in Figure 5-40, and then click **OK**. If you're prompted to take a new snapshot, click **Take new one**. Depending on the size and quantity of data on your disk, it might take several minutes for WinHex to traverse all the files and paths on your disk drive.

Figure 5-40.



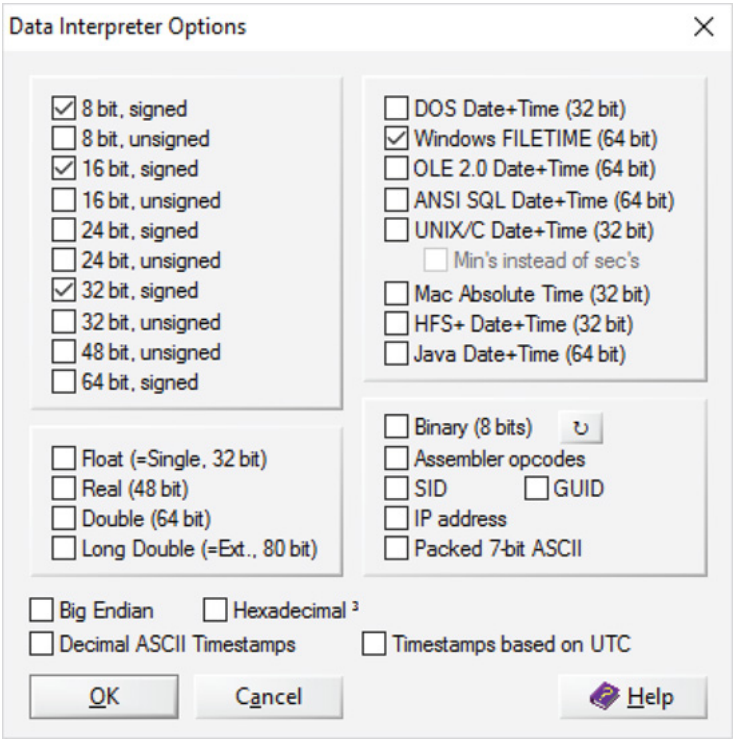
Source: X-Ways AG, www.x-ways.net

Selecting the Drive in WinHex

Note By default, WinHex displays a floating Data Interpreter window that converts hex values to decimal values and can also convert date and time codes. If you don't see this window, activate it by clicking View, pointing to Show, and clicking Data Interpreter.

4. Click **Options, Data Interpreter** from the menu. In the Data Interpreter Options dialog box, click the **Windows FILETIME (64 bit)** check box, shown in Figure 5-41, and then click **OK**. The Data Interpreter should then have FILETIME as an additional display item.

Figure 5-41.

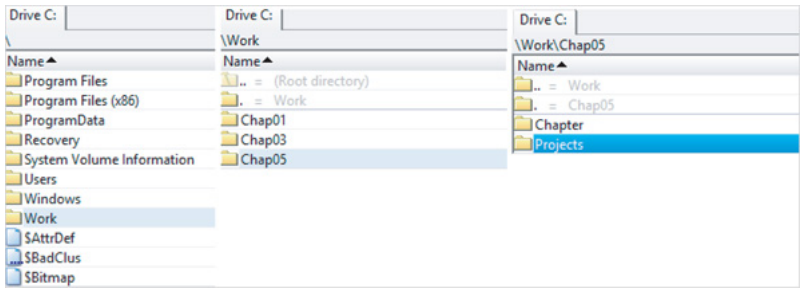


Source: X-Ways AG, www.x-ways.net

The Data Interpreter Options Dialog Box

5. Now you need to navigate to your work folder (C:*Work*\Chap05\Projects) in WinHex. In the upper-right pane of WinHex, scroll down until you see your work folder. Double-click each folder in the path (see Figure 5-42), and then click the **C5Prj02.txt** file.

Figure 5-42.

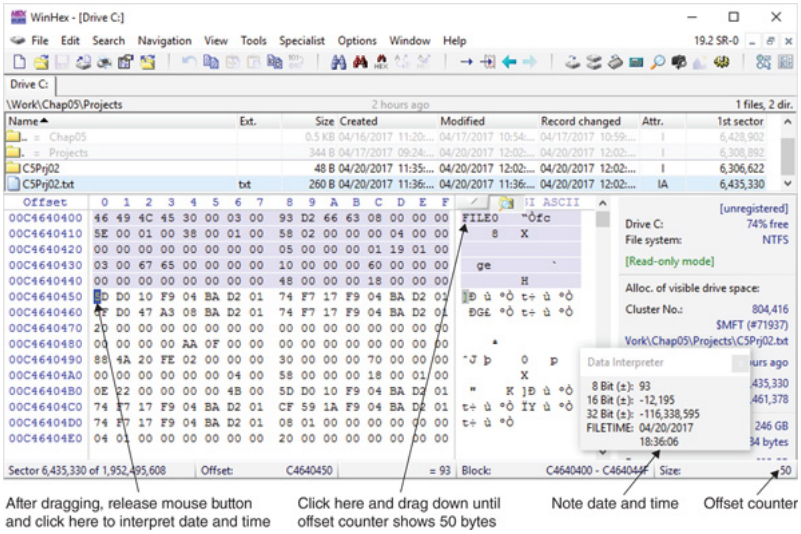


Source: X-Ways AG, www.x-ways.net

Navigating Through Folders in WinHex

6. Drag from the beginning of the record, on the letter **F** in FILE, and then down and to the right while you monitor the hexadecimal counter in the lower-right corner. (*Note*: 50 hexadecimal bytes is the "position" for the first date and time stamp for this record, as described in the previous charts for 0x10 $Standard Information.) When the counter reaches 50 (see Figure 5-43), release the mouse button.

Figure 5-43.



Source: X-Ways AG, www.x-ways.net

Locating the Date and Time Value in the MFT Record

7. Move the cursor one position to the next byte (down one line and to the left), and record the date and time of the Data Interpreter's FILETIME values.

8. Reposition the mouse cursor on the remaining offsets listed in the previous charts, and record their values.

9. When you're finished, exit WinHex and hand in the date and time values you recorded.

Hands-On Project 5-3.

In this project, you use WinHex to become familiar with different file types. Follow these steps:

1. Locate or create Microsoft Excel (.xlsx), Microsoft Word (.docx), .gif, .jpg, and .mp3 files. If you're creating a Word document or an Excel spreadsheet, save it as a Word or Excel file.

2. Start WinHex.

3. Open each file type in WinHex. Record the hexadecimal codes for each file in a text editor, such as Notepad or WordPad. For example, for the Word document, record **Word Header: 50 4B 03 04**.

4. Save the file, and then print it to give to your instructor.

Hands-On Project 5-4.

This project is a continuation of the in-chapter activity done with OSForensics. The paralegal has asked you to see whether any passwords are listed in the image of Denise Robinson's computer. Follow these steps:

1. Start OSForensics. If prompted to allow the program to make changes to your computer, click **OK** or **Yes**. In the OSForensics message box, click **Continue Using Trial Version**.

2. Copy the **InCh05.img** file to your work folder. Mount the **InCh05.img** file as described in the in-chapter activity.

3. In the main window, click **Manage Case** in the navigation bar on the left, if necessary. In the Select Case pane on the right, double-click **InChap05** if a green checkmark isn't displayed next to it.

4. In the navigation bar on the left, click **Passwords**. In the pane on the right, click the **Find Browser Passwords** tab, if necessary. Click the **Scan Drive** button, and then click the drive letter for the InCh05.img mounted virtual drive.

5. In the navigation bar on the left, click **Retrieve Passwords**. In the pane on the right, right-click the first item and click **Export List to Case**. In the Title text box, type **Denise Robinson's additional e-mail and password**, and then click **OK**. Repeat this step for all browser passwords that were recovered.

6. In the Passwords window, click the **Windows Login Passwords** tab. Click the **Scan Drive** button, and then click the drive letter for the InCh05.img mounted virtual drive.

7. Click **Retrieve Hashes**, and then click **Save to File**. In the Save to dialog box, navigate to your work folder, type **Denise-Robinson-Win-Passwords** in the File name text box, and then click **Save**.

8. In the navigation bar on the left, click **Manage Case**. In the Manage Current Case pane on the right, click the **Add Attachment** button. Navigate to and click the **Denise-Robinson-Win-Passwords** file, and click **Open**. In the Export Title text box, type **Denise-Robinson-Win-Passwords**, and then click **Add**.

9. In the navigation bar at the top, click **Generate Report**. In the Export Report dialog box, click **OK**. If you get a warning message that the report already exists, click **Yes** to overwrite the previous report.

10. Exit OSForensics, and print the report displayed in your Web browser. Turn the report in to your instructor.

Case Projects

Case Project 5-1.

Using the information you gathered in **Hands-On Project 5-4**, write a one-page memo to the paralegal, Ms. D. K. Jones, explaining the process you used to find the e-mail and password data.

Case Project 5-2.

An employee suspects that his password has been compromised. He changed it two days ago, yet it seems someone has used it again. What might be going on?

Case Project 5-3.

Sometimes you need to see how an application works and behaves on a booted suspect's computer. For this project, write a short guideline of two to three pages on how to use VirtualBox to start and run applications from a suspect's disk image. Your research should start with the VirtualBox user guide at www.virtualbox.org. For more information, search for terms such as "VirtualBox convert RAW image to VDI" or "convert raw to vmdk."

Chapter 6. Current Digital Forensics Tools

After reading this chapter and completing the exercises, you will be able to:

- Explain how to evaluate needs for digital forensics tools
- Describe available digital forensics software tools
- List some considerations for digital forensics hardware tools
- Describe methods for validating and testing forensics tools

Chapter 2 outlined how to set up a forensics laboratory. This chapter explores many software and hardware tools used during digital forensics investigations. No specific tools are recommended; instead, the goal is to explain how to select tools for digital investigations based on specific criteria.

Forensics tools are constantly being developed, updated, patched, revised, and discontinued. Therefore, checking vendors' Web sites routinely to look for new features and improvements is important. These improvements might address a difficult problem you're having in an investigation.

Before purchasing any forensics tools, consider whether the tool can save you time during investigations and whether that time savings affects the reliability of data you recover. Many GUI forensics tools require a lot of resources and demand computers with more memory and faster processor speeds or more processors. Sometimes they require more resources than a typical workstation has because of other applications, such as antivirus programs, running in the background. These background programs compete for resources with a digital forensics program, and a forensics program or the OS can stop running or hang, causing delays in your investigation.

Finally, when planning purchases for your forensics lab, determine what a new forensics tool can do better than one you're currently using. In particular, assess how well the software performs in validation tests, and then verify the integrity of the tool's results.

Note

As software continues to develop and investigators have new needs, vendors will address these needs. The tools listed in this chapter are in no way a complete list of tools available for Windows, Linux, or macOS.

Evaluating Digital Forensics Tool Needs

As described in **Chapter 2**, you need to develop a business plan to justify the acquisition of digital forensics hardware and software. When researching options, consider open-source tools, which sometimes include technical support. The goal is to find the best value for as many features as possible. Some questions to ask when evaluating tools include the following:

- On which OS does the forensics tool run? Does the tool run on multiple OSs?
- Is the tool versatile? For example, does it work in both Windows and Linux? Does it work in macOS?
- Can the tool analyze more than one file system, such as FAT, NTFS, and Ext4?
- Can a scripting language be used with the tool to automate repetitive functions and tasks?
- Does the tool have any automated features that can help reduce the time needed to analyze data?
- What's the vendor's reputation for providing product support? For open-source tools, how good are the support forums?

As you learn more about digital investigations, you'll have more questions about tools for conducting these investigations. When you search for tools, keep in mind what OSs and file types you'll be analyzing. For example, if you need to analyze Microsoft Access or SQL Server databases, look for a product designed to read these files. If you're analyzing e-mail messages, look for a forensics tool that specializes in reading e-mail content.

When you're selecting tools for your lab, keep an open mind, and compare platforms and applications for different tasks. Although many investigators are most comfortable using Windows tools, check into other options, such as Linux and macOS platforms (covered in Chapter 7).

Types of Digital Forensics Tools

Digital forensics tools are divided into two major categories: hardware and software. Each category has subcategories discussed in more depth later in this chapter. The following sections outline basic features required and expected of most digital forensics tools.

Note

Two trends will no doubt have an effect on your future choice of forensics tools. The field of digital forensics is predicted to grow at 11% per year between now and 2020 (www.marketsandmarkets.com/PressReleases/digital-forensics.asp), and the variety of tools available will probably grow to match this trend. In addition, with the growth of the Internet of Things (IoT), investigations are going to get more challenging, and more specialized tools might become essential.

Hardware Forensics Tools

Hardware forensics tools range from simple, single-purpose components to complete computer systems and servers. For example, the Tableau T35es-R2 SATA/IDE eSATA bridge is a single-purpose component that makes it possible to access a SATA or an IDE drive with one device. Some examples of complete systems are Digital Intelligence F.R.E.D. systems (www.digitalintelligence.com/forensichardware.php), DIBS Advanced Forensic Workstations (www.dibsforensics.com/index.html), Forensic Computers' Forensic Examination Stations and portable units (www.forensic-computers.com), and Ace Laboratory systems (www.acelaboratory.com/catalog/), designed for data recovery of failed drives, a feature that comes in handy in many situations.

Software Forensics Tools

Software forensics tools are grouped into command-line applications and GUI applications. Some tools are specialized to perform one task. For example, SafeBack, from New Technologies, Inc. (NTI), was designed as a command-line disk acquisition tool. It's no longer supported, but you can still find it distributed online. However, it's used more as a reliable fallback when all else fails than a primary tool. Other tools are designed to perform many different tasks. For example, PassMark Software OSForensics, X-Ways Forensics, Guidance Software EnCase, Magnet Forensics AXIOM, and AccessData FTK are GUI tools designed to perform most forensics acquisition and analysis functions.

Note

Another widely used GUI tool, Technology Pathways ProDiscover Forensics Edition, has been acquired by ARC Group, a cybersecurity company. At the time of this writing, the tool was being incorporated into a new product that hasn't been announced yet (www.arcgroupny.com/products/prodiscover-forensic-edition/). As the digital forensics field continues to grow, these kinds of mergers will continue to occur.

Software forensics tools are commonly used to copy data from a suspect's drive to an image file. Many GUI acquisition tools can read all structures in an image file as though the image were the original drive and have the capability to analyze image files. In **Chapter 5**, you learned how some of these tools are used to acquire data from suspects' drives.

Tasks Performed by Digital Forensics Tools

All digital forensics tools, both hardware and software, perform specific functions. When you're testing new tools, you might find it helpful to follow guidelines set up by NIST's **Computer Forensics Tool Testing (CFTT)** program, ASTM International's (formerly the American Society of Testing and Materials) E2678 standard, and the International Organization on Computer Evidence (IOCE). In addition, ISO standard 27037 (www.iso.org/standard/44381.html) states that Digital Evidence First Responders (DEFRs) should use validated tools. The following categories of functions are meant as guidelines for evaluating digital forensics tools, with subfunctions for refining data analysis and recovery and ensuring data quality:

- Acquisition
- Validation and verification
- Extraction
- Reconstruction
- Reporting

NIST's CFTT and other groups include additional functions, such as data acquisition, data extraction from mobile devices, file reconstruction, and string searching, that aren't included in these guidelines ("Verification of Digital Forensics Tools," Jim Lyle, May 2010, Montana Supreme Court Spring Training Conference). In the following sections, you learn how these functions and subfunctions apply to digital investigations.

Acquisition

Acquisition , the first task in digital forensics investigations, is making a copy of the original drive. As described in Chapter 3, this procedure preserves the original drive to make sure it doesn't become corrupt and damage the digital evidence. Subfunctions in the acquisition category include the following:

- Physical data copy
- Logical data copy
- Data acquisition format
- Command-line acquisition
- GUI acquisition
- Remote, live, and memory acquisitions

ISO standard 27037 states that the most important factors in data acquisition are the DEFR's competency and the use of validated tools, and it includes guidelines on how to approach acquisition in different situations. What's most important is documenting what was done and why. For example, if you're acquiring data at a scene with hazardous materials, clearly speed is critical, so you might decide to forgo acquiring RAM and focus on collecting devices. You can also find decision-making flowcharts on whether to copy an entire physical disk or concentrate on only a partition or folder, for instance. Section 7 of the standard addresses acquiring volatile memory, an important part of live acquisitions. Other situations that affect acquisitions include encrypted devices or mission-critical systems that can't be turned off.

Some digital forensics software suites, such as AccessData FTK, have separate tools for acquiring an image. Magnet AXIOM, for example, enables you to acquire the forensic image and process it in the same step. However, some investigators opt to use hardware devices, such as Tableau TD2, Logicube Talon, VOOM HardCopy 3P, or Image MASSter Solo-4 Forensic unit from Intelligent Computer Solutions, Inc., for acquiring an image. These hardware devices have built-in software for data acquisition. No other device or program is needed to make a duplicate drive; however, you still need forensics software to analyze the data.

Note

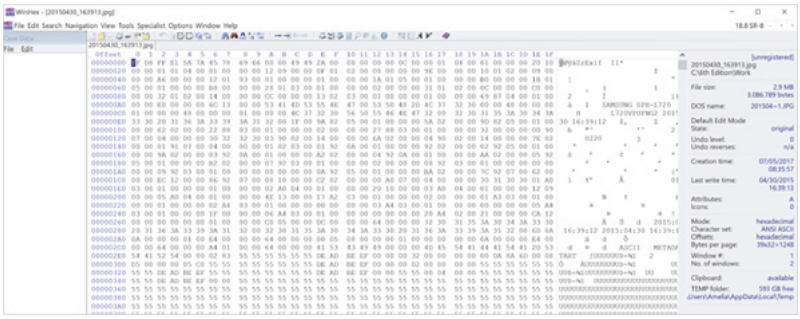
To see specifications for the Logicube Talon, go to www.logicube.com/shop/talon-ultimate/. To see the Image MASSter Solo-4 unit, search at www.ics-iq.com. To see VOOM HardCopy 3, search at www.voomtech.com.

Other acquisition tools require combining hardware devices and software programs to make disk acquisitions. For example, many software tools mount drives as read-only, and others might require a physical write-blocker. Any tool that has a built-in software write-blocker should be verified to make sure evidence hasn't been altered.

Two types of data-copying methods are used in software acquisitions: physical copying of the entire drive and logical copying of a disk partition. Most software acquisition tools include the option of imaging an entire physical drive or just a logical partition. Usually, the situation dictates whether you make a physical or logical acquisition. One reason to choose a logical acquisition is drive encryption. With the increasing emphasis on data security, drive encryption is used more commonly now. As mentioned in Chapter 5, making a physical acquisition of a drive with whole disk encryption can result in unreadable data. With a logical acquisition, however, you can still read and analyze the files. Of course, this method requires a live acquisition (covered in Chapter 10) because you need to log on to the system.

Disk acquisition formats vary from raw data to vendor-specific proprietary, as you learned in **Chapter 5**. The raw data format, typically created with the Linux dd command, is a simple bit-for-bit copy of a data file, a disk partition, or an entire drive. A raw-format imaging tool can copy data from one drive to another disk or to segmented files. Because it's a true unaltered copy, you can view a raw image file's contents with any hexadecimal editor, such as Hex Workshop or WinHex. These tools give you a hexadecimal view (see Figure 6-1) or a plaintext view of the data.

Figure 6-1.



Source: X-Ways AG, www.x-ways.net

Viewing data in WinHex

Creating smaller segmented files is a typical feature in vendor acquisition tools. Their purpose is to make it easier to store acquired data on smaller media, such as CDs and USB drives.

Remote acquisition of files is common in larger organizations. Enterprise-level companies are geographically diverse, so investigators might not be able to get physical access to systems without traveling long distances. Popular tools, such as AccessData and EnCase, can do remote acquisitions of forensic drive images on a network, and these acquisitions can also be done with a dd command.

Validation and Verification

Validation and verification functions work hand in hand. **Validation** is a way to confirm that a tool is functioning as intended, and **verification** proves that two sets of data are identical by calculating hash values or using another similar method. Another related process is filtering, which involves sorting and searching through investigation findings to separate good data and suspicious data. Validating tools and verifying data are what allow filtering.

To validate a tool, you can use forensic images that have been created for desktop and mobile devices; these files are posted on Web sites such as NIST's CFTT or the Scientific Working Group on Digital Evidence (SWGDE) and tell you what the tool should find as evidence on the drives. They can also give you ranges of results so that you can determine, for example, that a tool works well for acquiring Linux images but has problems with older Windows versions. These groups also publish the results of testing hardware acquisition tools. After validating a tool, you must also make sure all forensic copies of a particular device have the same hash value.

All forensics acquisition tools have a method for verification of the data-copying process that compares the original drive with the image. For example, EnCase prompts you to calculate the MD5 hash value of acquired data, and FTK validates MD5 and SHA-1 hash sets during data acquisition. Hardware acquisition tools, such as Image MASSter Solo-4, can perform simultaneous MD5 and CRC-32 hashing during data acquisition. Whether you choose a software or hardware solution for acquisition, make sure the tool has a hashing function for verification purposes. How data hashing is used depends on the investigation, but using a hashing algorithm on the entire suspect drive and all its files is a standard practice. This method produces a unique hexadecimal value for ensuring that the original data hasn't changed and copies are of the same unchanged data or image.

When performing filtering, you separate good data from suspicious data. Good data consists of known files, such as OS files, common applications (Microsoft Word, for example), and standard files used in a company's day-to-day business. You can also use hash values to create a known good hash value list of a fresh installation of an OS, all applications, and known good images and documents (spreadsheets, text files, and so on). With this information, an investigator could ignore all files on this known good list and focus on other files that aren't on this list. Filtering can also be used to find data for evidence in criminal investigations or to build a case for terminating an employee. The **National Software Reference Library (NSRL)** has compiled a list of known file hashes for a variety of OSs, applications, and images that you can download (see Figure 6-2). It's also adding hash values for mobile apps, specifically iOS and Android. You learn more about the NSRL in "Validating and Testing Forensics Software" later in this chapter.

Figure 6-2.

Source: *www.nsrl.nist.gov*

The home page of the National Software Reference Library

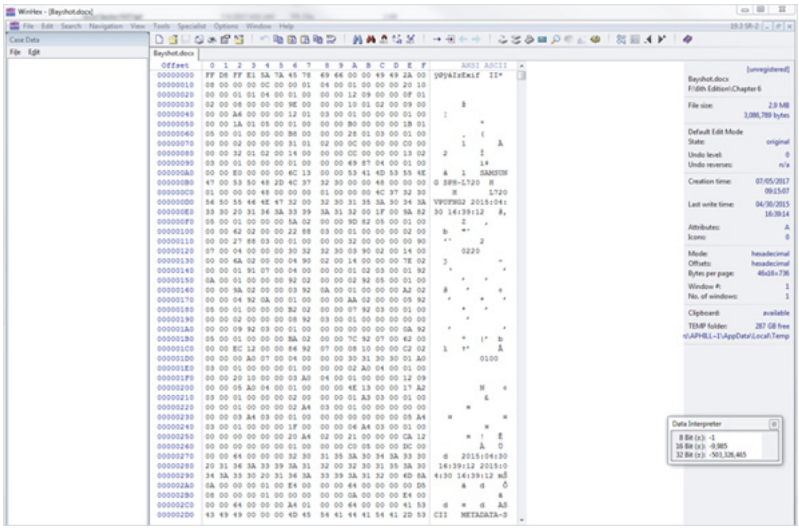
Note

Organizations such as the National Center for Missing and Exploited Children maintain hash sets of photos of known victims. These files are sorted into the “suspicious” or known bad category.

Several digital forensics tools can integrate known good file hash sets and compare them with file hashes from a suspect drive to see whether they match. With this process, you can eliminate large amounts of data quickly so that you can focus your evidence analysis. You can also begin building your own hash sets. Another feature to consider is hashing and comparing sectors of data. It’s useful for identifying fragments of data in slack and free disk space that might be partially overwritten.

Another way to filter data is analyzing and verifying header values for known file types. Each file type has a header value associated with a file extension, and many forensics tools include a list of common file headers. To view these file headers, you use a hexadecimal editor, which can tell you whether a file extension is incorrect for the file type. Renaming file extensions is often done to disguise or hide data, and you could miss pertinent data if you don’t check file headers. A standard indicator for graphics files is the hex value “FF D8,” shown in the first line of output in the Bayshot.docx file shown in Figure 6-3. (You examine graphics files in more detail in Chapter 8.) After some practice in viewing file headers, you’ll learn to recognize common header values.

Figure 6-3.

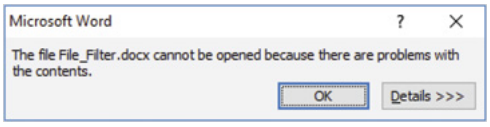


Source: X-Ways AG, www.x-ways.net

The file header indicates a .jpeg file

Because the Bayshot.docx file has “FF D8” in the header, it’s a .jpeg image, not a .docx file. If you try to open this file in Microsoft Word, you see the error message shown in Figure 6-4, if you’re using Windows 7 or 8.1. Windows 10, however, automatically detects that the file is a JPEG and adds the correct extension.

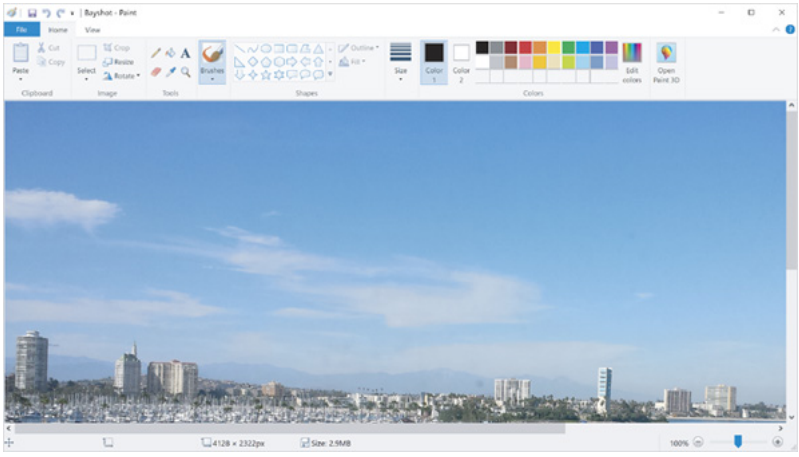
Figure 6-4.



Error message displayed when trying to open a .jpeg file in Word

If you open the file with an image viewer, such as Microsoft Paint, you see the image shown in **Figure 6-5**.

Figure 6-5.



Bayshot.docx opened in Paint

Searching and comparing file headers rather than file extensions improves filtering. With this feature, you can locate files that might have been altered intentionally. In **Chapters 8** and 9, you see how to use this feature to locate hidden data.

Extraction

The **extraction** function is the recovery task in a digital investigation and is the most challenging of all tasks to master. In Chapter 1, you learned how system analysis applies to an investigation. Recovering data is the first step in analyzing an investigation's data. The following subfunctions of extraction are used in investigations:

- Data viewing
- Keyword searching
- Decompressing or uncompressing
- Carving
- Decrypting
- Bookmarking or tagging

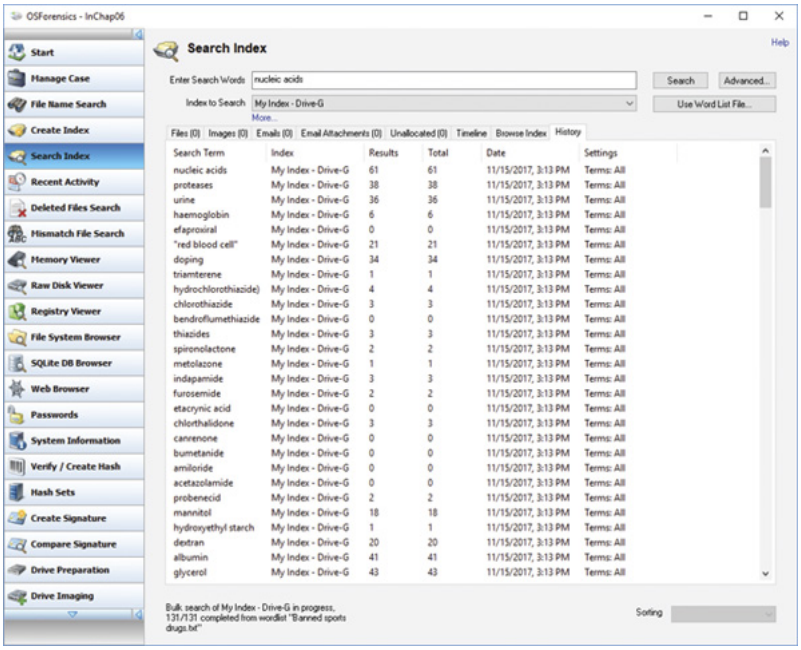
Note

Mobile devices have added some complexity to forensic extraction because so much data can be retrieved from them: call records, URLs, GPS data, SMS and text messages, and more. You explore mobile device forensics in **Chapter 12**.

Many digital forensics tools include a data-viewing mechanism for digital evidence and offer several ways to view data, including logical drive structures, such as folders and files. These tools also display allocated file data and unallocated disk areas with special file and disk viewers. Being able to view this data in its normal form makes analyzing and collecting clues for the investigation easier.

A common task in digital investigations is searching for and recovering relevant data. Forensics tools have functions for searching for keywords of interest to the investigation. Using a **keyword search** speeds up the analysis process, if used correctly; however, a poor selection of keywords generates too much information. Another way to narrow down a search is by using word lists created for a specific case. Figure 6-6 shows an OSForensics built-in file called "banned sports drugs" used to do an indexed search for the keyword "nucleic acids" in Charlie's hard drive (from the M57 Patents case).

Figure 6-6.



Source: PassMark Software, *www.osforensics.com*

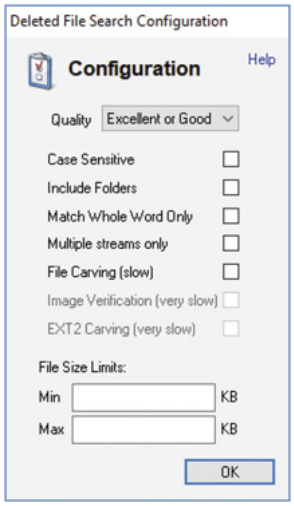
Using a word list to search in OSForensics

With some tools, you can set filters to select file types to search, such as searching only PDF files. Another function in some forensics tools, such as X-Ways Forensics and OSForensics, is indexing all words on a drive. These features speed up keyword searches, which speeds up analysis.

Another feature to consider for extraction is the format the forensics tool can read. For example, OSForensics has a feature for reading and indexing data from Microsoft .pst and .ost files, and EnCase has a third-party add-on that indexes and analyzes Microsoft .pst files. In addition, EnCase and X-Ways Forensics enable you to create scripts for extracting data, but older versions of FTK don't have this feature. Often you have to use a combination of tools to retrieve and report on evidence from digital devices accurately.

The investigation process also involves reconstructing fragments of files that have been deleted from a suspect drive. In North America, this reconstruction is called "carving"; in Europe, it's called "salvaging." (Carving is covered in more depth in **Chapters 8** and 16.) Investigators often need to be able to extract data from unallocated disk space. Locating file header information, as mentioned in "Validation and Verification," is a reliable method for carving data. Most forensics tools analyze unallocated areas of a drive or a forensic image and locate fragments or entire file structures that can be carved and copied into a newly reconstructed file. Some investigators prefer carving fragmented data manually with a command-line tool, but advanced GUI tools with built-in carving functions are more common now. Figure 6-7 shows the data-carving feature in OSForensics.

Figure 6-7.



Source: PassMark Software, *www.osforensics.com*

Data-carving options in OS Forensics

Some tools, such as Simple Carver Suite (www.simplecarver.com) and DataLifter (http://downloads.informer.com/datalifter-with-file-extractor-pro/), are specifically designed to carve known data types from exported unallocated disk space. DataLifter includes a feature that enables you to add other header values.

There are many compression or zip utilities, such as WinZip, 7Zip, and pzip. When a forensics tool encounters a compressed file or zip archive as part of a forensic image, it applies the correct algorithm for uncompressing the files. For example, uncompressing Windows files is done with the Lempel-Ziv algorithm, Lz32.dll. Other OSs and compression utilities use other algorithms.

A major challenge in digital investigations is analyzing, recovering, and decrypting data from encrypted files or systems. Encryption can be used on a drive, disk partition, or file. Many e-mail services, such as Microsoft Outlook, provide encryption protection for .pst folders and messages. Encryption can be platform specific, such as Windows Encrypting File System (EFS) and BitLocker, or done with third-party tools, such as Pretty Good Privacy (PGP) and GnuPG.

From an investigation perspective, encrypted files and systems are a problem. Many password recovery tools have a feature for generating potential password lists for a **password dictionary attack** . Passwords are typically stored as hash values, not in plaintext, and are meant to be one-way hashes, meaning you can't apply an algorithm to break them. Password lists give you a starting point for guessing passwords; in addition, you can try words related to a suspect's profession and hobbies. Passwords are sometimes written to a temporary file or system file, such as Pagefile.sys, so examining these files is a useful technique, too. OSForensics, like many forensics tools, has a built-in password cracker. First, it attempts to retrieve browser and OS passwords, especially if you're examining a live system. Next, it generates rainbow tables (files containing password hash values; explained in Chapter 9) and compares hash values to see whether it can find a match with the password. If it fails, the next step is to run a **brute-force attack** on the encrypted file. OSForensics, for example, attempts to recover Windows logon passwords and has additional features, such as recovering browser passwords. With the proliferation of mobile devices, the ability to access passwords depends on how secure users' passphrases are. After you get into a smartphone, most apps open automatically.

After finding the evidence, the next task is to bookmark or tag it so that you can refer to it later when needed. Many forensics tools use bookmarks to insert digital evidence into a report generator, which produces a technical report in HTML or RTF format of the examination's findings. When the report generator is started, bookmarks are loaded into the report.

Reconstruction

The purpose of having a **reconstruction** function in a forensics tool is to re-create a suspect drive to show what happened during a crime or an incident. Another reason for duplicating a suspect drive is to create a copy for other digital investigators, who might need a fully functional copy of the drive so that they can perform their own acquisition, test, and analysis of the evidence. Reconstruction is also done if a drive has been compromised by malware or a suspect's actions. The following are methods of reconstruction:

- Disk-to-disk copy
- Partition-to-partition copy
- Image-to-disk copy
- Image-to-partition copy
- Disk-to-image copy
- Rebuilding files from data runs and carving

There are several ways to re-create an image of a suspect drive. A decade ago, the ideal method was using the same make and model disk as the suspect disk, as discussed in **Chapter 3**, but disk-to-disk copies are rarely used now. (A partition-to-partition copy is very similar, but you use partitions instead of disks.) Typically, you copy an image to another location, such as a partition, a physical disk, or a virtual machine (covered in Chapter 10). The simplest method of duplicating a drive is using a tool that makes a direct disk-to-image copy from the suspect disk to the target location. Many tools can perform this task. One free tool is the Linux dd command, but it has a major disadvantage: It produces a flat, uncompressed file that's the same size as the source drive.

Some tools have proprietary formats that can be restored only by the same application that created them. For example, a ProDiscover image (.eve format) can be restored only by using ProDiscover. Most tools, however, can convert files to the .E01 or .001 format so that you can use files in a variety of tools to take advantage of their different strengths.

Forensics analysis is often complicated by time-critical cases, such as those involving kidnapping or homicides, but shadowing drives is a useful technique in these situations. It requires a hardware device, such as Voom Technologies Shadow Drive, that connects a suspect's drive to a read-only IDE port and another drive to a read-write port that's called a "shadow drive." When the Voom device is connected to a computer, you can access and run applications on the suspect's drive. All data that would normally be written to the suspect's drive is redirected to the shadow drive ("Voom Technologies' Shadow 3 said to provide a quick way to investigate computers without compromising evidence," *Government Security News*, February 2014). This tool has been used in court so that expert witnesses could easily show evidence on a drive and how a suspect could have used the information.

Reporting

To perform a forensics disk analysis and examination, you need to create a report. Before Windows forensics tools were available, this process required copying data from a suspect drive and extracting the digital evidence manually. The investigator then copied the evidence to a separate program, such as a word processor, to create a report. File data that couldn't be read in a word processor—databases, spreadsheets, and graphics, for example—made it difficult to insert nonprintable characters, such as binary data, into a report. Typically, these

reports weren't stored electronically because investigators had to collect printouts from several different applications to consolidate everything into one large paper report.

Newer forensics tools can produce electronic reports in a variety of formats, such as word-processing documents, HTML Web pages, and Acrobat PDF files. The following are subfunctions of the reporting function:

- Bookmarking or tagging
- Log reports
- Timelines
- Report generator

As part of the validation process, often you need to document the steps you took to acquire data from a suspect drive. Many forensics tools can produce a log report that records an investigator's activities and incorporates evidence that was bookmarked or tagged during extraction. Then a built-in report generator is used to create a report in a variety of formats. Some tools with report generators that display bookmarked evidence are EnCase, FTK, OSForensics, ILookIX, and X-Ways Forensics.

You can add a log report to your final report as documentation of the steps you took during the examination, which can be useful if repeating the examination is necessary. For a case that requires peer review, log reports confirm what activities were performed and what results were found in the original analysis and examination. Keep in mind that reports generated by forensics tools are no substitute for an investigator's report. Investigators need to be able to explain their decisions and the output in more detail than a tool-generated report can produce.

Tool Comparisons

To help determine which forensics tool to purchase, a comparison table of functions, subfunctions, and vendor products is useful. Cross-referencing functions and subfunctions with vendor products makes it easier to identify the forensics tool that best meets your needs. **Table 6-1** is an example of how to compare forensics vendors' tools. Your needs might differ from the functions and subfunctions listed in this table. When developing your own table, add other functions and subfunctions you think are necessary to determine which tools you should acquire for an investigation.

Table 6-1. Comparison of Forensics Tool Functions

Function	Magnet Forensics AXIOM, demo version	OSForensics, demo version	AccessData FTK	Guidance Software EnCase
Acquisition				
Physical data copy	✓	✓	✓	✓
Logical data copy	✓	✓	✓	
Data acquisition formats	✓	✓	✓	✓
Command-line processes				✓
GUI processes	✓	✓	✓	✓
Remote acquisition		✓	✓	✓
Validation and verification				
Hashing	✓	✓	✓	✓
Verification	✓	✓	✓	✓
Filtering	✓	✓	✓	✓
Analyzing file headers	✓	✓	✓	✓
Extraction				
Data viewing	✓	✓	✓	✓

Function	Magnet Forensics AXIOM, demo version	OSForensics, demo version	AccessData FTK	Guidance Software EnCase
Keyword searching	✓	✓	✓	✓
Decompressing	✓		✓	✓
Carving	✓	✓	✓	✓
Decrypting	✓	✓	✓	
Bookmarking	✓	✓	✓	✓
Reconstruction				
Disk-to-disk copy	✓	✓	✓	✓
Partition-to-partition copy	✓	✓	✓	✓
Image-to-disk copy	✓	✓	✓	✓
Image-to-partition copy	✓	✓	✓	✓
Disk-to-image copy	✓	✓	✓	✓
Rebuilding files	✓	✓	✓	✓
Reporting				
Bookmarking/tagging	✓	✓	✓	✓
Log reports	✓	✓	✓	✓
Timeline	✓	✓	✓	✓
Report generator	✓	✓	✓	✓
Automation and other features				
Scripting language				✓
Mount virtual machines		✓	✓	✓
E-discovery		✓	✓	✓

Other Considerations for Tools

As part of the business planning for your lab, you should determine which tools offer the most flexibility, reliability, and future expandability. The software tools you select should be compatible with the next generation of OSs; for example, Windows 7 and later added features for compatibility with mobile devices. As an investigator, it's your responsibility to find information on changes in new hardware or software releases and changes planned for the next release. Because OS vendors don't always supply adequate information about future file system upgrades, you must research and prepare for these changes and develop resources for finding new specifications if the vendor fails to provide them. For example, when NTFS was introduced with Windows NT, forensics software vendors revised their products for this new file system, but addressing the file system changes took some time. Therefore, investigators had to look for alternatives to getting the data they needed, such as consulting Microsoft resource kits for Windows NT. Similar compatibility issues have occurred as people have moved from Windows 8.1 to Windows 10 and Windows Server 2012 to 2016.

Another consideration when maintaining a forensics lab is creating a software library containing older versions of forensics utilities, OSs, and other programs. When purchasing newer and more versatile tools, you should also ensure that your lab maintains older versions of software and OSs. If a new software version fixes one bug but introduces another, you can use the previous version to overcome problems caused by the new bug.

Digital Forensics Software Tools

Whether you use a suite of tools or a task-specific tool, you have the option of selecting one that enables you to analyze digital evidence through the command line or in a GUI. The following sections explore some options for command-line and GUI tools in both Windows and Linux.

Note

Macintosh has made a comeback, and more people are using it. Installing Windows on Apple machines is fairly easy, so you can use most forensics tools in macOS.

Command-Line Forensics Tools

As mentioned in **Chapter 1**, computers used several OSs before Windows and MS-DOS dominated the market. During this time, digital forensics wasn't a major concern. After people started using PCs, however, they figured out how to use them for illegal and destructive purposes and to commit crimes and civil infractions with them. Software developers began releasing forensics tools to help private-sector and public-sector investigators examine PCs. The first tools that analyzed and extracted data from floppy disks and hard disks were MS-DOS tools for IBM PC file systems.

One of the first MS-DOS tools used for digital investigations was Norton DiskEdit. This tool used manual processes that required investigators to spend considerable time on a typical 500 MB drive. Eventually, programs designed for digital forensics were developed for DOS, Windows, Apple, NetWare, and UNIX systems. Some of these early programs could extract data from slack and free disk space; others were capable only of retrieving deleted files. Current programs are more powerful and can search for specific words or characters, import a keyword list to search, calculate hash values, recover deleted items, conduct physical and logical analyses, and more.

One advantage of using command-line tools for an investigation is that they require few system resources because they're designed to run in minimal configurations. In fact, most tools fit on bootable media (USB drives, CDs, and DVDs). Conducting an initial inquiry or a complete investigation with bootable media can save time and effort. Most tools also produce a text report that fits on a USB drive or other removable media.

Some command-line forensics tools are created specifically for Windows command-line interface (CLI) platforms; others are created for macOS and Linux. Because there are many different versions of UNIX and Linux, these OSs are often referred to as "Linux platforms." In **Chapter 5**, you were introduced to using some command-line tools in Linux, such as the dd and dcfldd commands. For Windows platforms, a number of companies, such as NTI, Digital Intelligence, Maresware, DataLifter, and ByteBack, are recognized for their work in command-line forensics tools.

Some tools that are readily available in the command line are often overlooked. For example, in Windows 2000 and later, the dir command shows you the file owner if you have multiple users on the system or network. Try it by following these steps:

1. Open a command prompt window.
2. At the command prompt, type **cd /** and press **Enter** to take you to the root directory. Create a work folder for this chapter by typing **md *Work* \Chap06\Chapter** (replacing *Work* with the name of your work folder) and pressing **Enter**.
3. Make sure you're at the root directory, and type **dir /q > C:\ *Work* \Chap06\Chapter\Fileowner.txt** and press **Enter**.
4. In any text editor, open **Fileowner.txt** to see the results. You should see your file structure and whether the files were generated by the system or by a user. When you're finished, exit the text editor and close the command prompt window.

Linux Forensics Tools

Although UNIX has been around for many decades, it's been mostly replaced by Linux; however, you might still encounter systems running UNIX. Linux platforms have become more common, and the GUIs that are readily available with them make them increasingly popular with home and business users. Because most are free, they're widely used in developing and emerging nations. This newfound popularity and the staggering number of versions give investigators more challenges, such as learning the Linux command line and investigating the Linux environment. In **Chapter 7**, you learn more about several Linux tools for forensics analysis, such as Kali Linux and DEFT.

Note

This book isn't geared toward the Linux platform for forensics analysis, but using a Linux tool for the processes described in this book works as well as on a Microsoft platform. Also, keep in mind that Linux tools work well on Windows systems, as you see in **Chapter 7**.

Smart

SMART is designed to be installed on numerous Linux versions, including Gentoo, Fedora, SUSE, Debian, Knoppix, Ubuntu, and Slackware. You can analyze a variety of file systems with SMART; for a list of file systems or to download an evaluation ISO image for SMART and SMART Linux, go to www.asrdata.com/forensic-software/software-download/.

SMART includes several plug-in utilities. This modular approach makes it possible to upgrade SMART components easily and quickly. SMART can also take advantage of multithreading capabilities in OSs and hardware, a feature lacking in other forensics utilities. This tool is one of the few that can mount different file systems, such as journaling file systems, in a read-only format.

Another useful option in SMART is the hex viewer, which color-codes hex values to make it easier to see where a file begins and ends. SMART also offers a reporting feature. Everything you do during your investigation with SMART is logged, so you can select what you want to include in a report, such as bookmarks.

Helix 3

One of the easiest suites to use is Helix because of its user interface. Although Helix is no longer a free package, you can go to www.e-fense.com/products.php to learn more about it. What's unique about Helix is that you can load it on a live Windows system, and it loads as a bootable Linux OS from a cold boot. Its Windows component is used for live acquisitions. Be aware, however, that some international courts haven't accepted live acquisitions as a valid forensics practice.

During private-sector investigations, often you need to retrieve RAM and other data, such as the suspect's user profile, from a workstation or server that can't be seized or turned off. This data is extracted while the system is running and captured in its state at the time of extraction. Make sure to keep a journal to record what you're doing, however. To do a live acquisition, insert the Helix DVD into the suspect's machine.

Kali Linux

Kali Linux, formerly known as BackTrack, is another Linux Live product used by many security professionals and forensics investigators. It includes a variety of tools and has an easy-to-use KDE interface. You can download the ISO image from www.kali.org. Kali includes several tools, such as Autopsy and Sleuth Kit (discussed next), ophcrack, dcfldd, MemFetch, and MBoxGrep.

Autopsy and Sleuth Kit

Sleuth Kit was designed as a Linux forensics tool, and Autopsy was the browser interface for accessing Sleuth Kit's command-line tools. The Linux version hasn't been updated in several years, but a version for Windows is available and has the most current updates. **Chapter 7** explains how to use the Linux version, but if you're accessing these tools from Kali, for example, shut down your Windows computer with the Kali disc in the CD/DVD drive or with a Kali installation on a USB drive, making sure your system is set to boot from the CD/DVD or USB drive before the hard drive. Then do a hard boot to the computer. In the options that are displayed, select Expert Mode, which is a forensically sound mode. If you're booting from a laptop, you might have display issues. You can click Scan to have Kali find the correct settings. (If Kali fails to find these settings, experiment until you find a setting that works.) After the correct display setting is applied, a GUI is displayed. If prompted, specify whether to load SCSI modules or additional modules from a floppy disk.

On your desktop, you should see what drives have been detected. For example, you see /dev/sda1 and /dev/sda2 displayed at the upper left. If you click the Kali button, which is similar to the Start button in Windows, you see the GUI selection. When you select Forensic Tools, the Autopsy option is displayed. From here, you can open an existing case or start a new case. For more information on these tools, visit www.sleuthkit.org.

Forcepoint Threat Protection

Forcepoint Threat Protection, formerly known as Second Look, is a Linux memory analysis tool that was developed under a grant from the Air Force Research Lab for Pikewerks Corporation. It was designed to do both onsite and remote (enterprise) memory acquisitions to determine whether malware is present. You can find this tool at www.forcepoint.com/product/cloud-security/forcepoint-threat-protection-for-linux (hosted by Raytheon). Products such as this one show that the fields of digital forensics and network security are merging.

Other GUI Forensics Tools

Several software vendors have introduced forensics tools that work in Windows. Because GUI forensics tools don't require the same understanding of the Windows CLI and file systems that command-line tools do, they can simplify digital forensics investigations. These GUI tools have also simplified training for beginning examiners; however, you should continue to learn about and use command-line tools because some GUI tools might miss critical evidence.

Most GUI tools are put together as suites of tools. For example, the largest GUI tool vendors—AccessData and Guidance Software—offer tools that perform most of the tasks discussed in this chapter. Another example is Magnet AXIOM, which is designed to work with FTK, EnCase, X-Ways Forensics, and NUIX and has hundreds of Samsung mobile frameworks to assist in acquiring mobile devices. It also offers features for working with IoT devices, social media, and cloud services. (You have a chance to see how these features work in **Chapter 12**.) As with all software, each suite has its strengths and weaknesses.

GUI tools have several advantages, such as ease of use, the capability to perform multiple tasks, and no requirement to learn older OSs. Their disadvantages range from excessive resource requirements (needing large amounts of RAM, for example) and producing inconsistent results because of the type of OS used. Another concern with using GUI tools is that they create investigators' dependence on using only one tool. In some situations, GUI tools don't work and a command-line tool is required, so it's essential for investigators to be familiar with more than one type of tool.

Digital Forensics Hardware Tools

This section discusses computer hardware used for forensics investigations. Technology changes rapidly, and hardware manufacturers have designed most computer components to last about 18 months between failures. Whether hardware is a rack-mounted server or a

forensic workstation, eventually it fails. For this reason, you should schedule equipment replacements periodically—ideally, every 18 months if you use the hardware full time. Most digital forensics operations use a workstation 24 hours a day for a week or longer between complete shutdowns.

You should plan your hardware needs carefully, especially if you have budget limitations. Include the amount of time you expect the forensic workstation to be running, how often you expect hardware failures, consultant and vendor fees to support the hardware, and how often to anticipate replacing forensic workstations. The longer you expect the forensic workstation to be running, the more you need to anticipate physical equipment failure and the expense of replacement equipment.

Forensic Workstations

Many hardware vendors offer a wide range of forensic workstations that you can tailor to meet your investigation needs. The more diverse your investigation environment, the more options you need. In general, forensic workstations can be divided into the following categories:

- *Stationary workstation*—A tower with several bays and many peripheral devices
- *Portable workstation*—A laptop computer with almost as many bays and peripherals as a stationary workstation
- *Lightweight workstation*—Usually a laptop computer built into a carrying case with a small selection of peripheral options

When considering options to add to a basic workstation, keep in mind that PCs have limitations on how many peripherals they can handle. The more peripherals you add, the more potential problems you might have, especially if you're using an older version of Windows. You must learn to balance what you actually need with what your system can handle. In addition, remember that RAM and storage need updating as technology advances.

If you're operating a digital forensics lab for a police agency, you need as many options as possible to handle any investigation. If possible, use two or three hardware configurations to handle diverse investigations. You should also keep a hardware inventory in addition to your software library. In the private sector, however, consider streamlining your workstation to meet the needs of only the types of systems used in your business.

Building Your Own Workstation

To decide whether you want to build your own workstation, first ask "How much do I have to spend?" Building a forensic workstation isn't as difficult as it sounds but can quickly become expensive if you aren't careful. If you have the time and skill to build your own forensic workstation, you can customize it to your needs and save money, although you might have trouble finding support for problems that develop. For example, peripheral devices might conflict with one another, or components might fail. If you build your own forensic workstation, you should be able to support the hardware. You also need to identify what you intend to analyze. If you're analyzing SPARC disks from workstations in a company network, for example, you need to include a SPARC drive with a write-protector on your forensic workstation. (SPARC disks are commonly used with Sun Solaris systems.)

If you decide that building a forensic workstation is beyond your skills, some vendors still offer workstations designed for digital forensics, such as the F.R.E.D. unit from Digital Intelligence or hardware mounts from ForensicPC that convert a standard server or PC into a forensic workstation. Having a vendor-supplied workstation has its advantages. If you aren't skilled in hardware maintenance and repair, having vendor support can save you time and frustration when you have problems. Of course, you can always mix and match components to get the capabilities you need for your forensic workstation.

Note

If you don't have the skills to build and support a PC, you might want to consider taking an A+ certification course.

Using a Write-Blocker

The first item you should consider for a forensic workstation is a **write-blocker** . Write-blockers protect evidence disks by preventing data from being written to them. Software and hardware write-blockers perform the same function but in a different fashion.

Software write-blockers, such as PDBlock from Digital Intelligence, typically run in a shell mode (such as a Windows CLI). PDBlock changes interrupt-13 of a workstation's BIOS to prevent writing to the specified drive. If you attempt to write data to the blocked drive, an alarm sounds, advising that no writes have occurred. PDBlock can run only in a true DOS mode, however, not in a Windows CLI.

With hardware write-blockers, you can connect the evidence drive to your workstation and start the OS as usual. Hardware write-blockers, which act as a bridge between the suspect drive and the forensic workstation, are ideal for GUI forensics tools. They prevent Windows or Linux from writing data to the blocked drive.

In the Windows environment, when a write-blocker is installed on an attached drive, the drive appears as any other attached disk. You can navigate to the blocked drive with any Windows application, such as File Explorer, to view files or use Word to read files. When you copy data to the blocked drive or write updates to a file with Word, Windows shows that the data copy is successful. However, the write-blocker actually discards the written data—in other words, data is written to null. When you restart the workstation and examine the blocked drive, you won't see the data or files you copied to it previously.

Many vendors have developed write-blocking devices that connect to a computer through FireWire, USB 2.0 and 3.0, SATA, PATA, and SCSI controllers. Most of these write-blockers enable you to remove and reconnect drives without having to shut down your workstation, which saves time in processing the evidence drive. For more information on write-blocker specifications, visit www.cftt.nist.gov. The following vendors offer write-blocking devices:

- www.digitalintelligence.com
- www.forensicpc.com
- www.guidancesoftware.com
- www.voomtech.com
- www.mykeytech.com
- www.lc-tech.com
- www.logicube.com
- www.forensic-computers.com
- www.cru-inc.com
- www.paraben.com
- www.usbgear.com/USB-FORENSIC.html

Recommendations for a Forensic Workstation

Before you purchase or build a forensic workstation, determine where your data acquisitions will take place. If you acquire data in the field, consider streamlining the tools you use. With

the newer FireWire and USB write-blocking devices, you can acquire data easily with Digital Intelligence FireChief and a laptop, for example. If you want to reduce the hardware you carry, consider a product such as the WiebeTech Forensic DriveDock with its regular DriveDock FireWire bridge or the Logicube Talon.

When choosing a computer as a stationary or lightweight forensic workstation, you want a full tower to allow for expansion devices, such as a 2.5-inch drive converter to analyze a laptop hard drive on a 3.5-inch IDE write-protected drive controller. You want as much memory and processor power as your budget allows and different sizes of hard drives. In addition, consider a 400-watt or better power supply with battery backup, extra power and data cables, a SCSI controller card, external FireWire and USB ports, an assortment of drive adapter bridges to connect SATA to IDE (PATA) drives, an ergonomic keyboard and mouse, and a good video card with at least a 17-inch monitor. If you plan to conduct many investigations, a high-end video card and dual monitors are recommended. If you have a limited budget, one option for outfitting your lab is to use high-end game PCs from a local computer store. With some minor modifications and additions of hardware components, these systems perform extremely well.

As with any technology, what your forensic workstation includes is often a matter of preference. Whatever vendor you choose, make sure the devices you select perform the functions you expect to need as an investigator.

Validating and Testing Forensics Software

Now that you have selected some tools to use, you need to make sure the evidence you recover and analyze can be admitted in court. To do this, you must test and validate your software. The following sections discuss validation tools available at the time of this writing and how to develop your own validation protocols.

Using National Institute of Standards and Technology Tools

The National Institute of Standards and Technology (NIST) publishes articles, provides tools, and creates procedures for testing and validating computer forensics software. Software should be verified to improve evidence admissibility in judicial proceedings. NIST sponsors the CFTT project to manage research on forensics tools. For additional information on this testing project, visit www.cftt.nist.gov. The Computer Forensic Reference Data Sets (CFReDS; www.cfreds.nist.gov) has been created recently to provide data sets for tools, training, and hardware testing.

NIST also created criteria for testing forensics tools, which are included in the article "General Test Methodology for Computer Forensic Tools" (version 1.9, November 7, 2001), available at www.cftt.nist.gov/testdocs.html. This article addresses the lack of specifications for what forensics tools should do and the importance of tools meeting judicial scrutiny. The criteria are based on standard testing methods and ISO 17025 criteria for testing when no current standards are available. Your lab must meet the following criteria and keep accurate records so that when new software and hardware become available, testing standards are in place for your lab:

- *Establish categories for digital forensics tools*—Group digital forensics software according to categories, such as forensics tools designed to retrieve and trace e-mail.
- *Identify forensics category requirements*—For each category, describe the technical features or functions a forensics tool must have.
- *Develop test assertions*—Based on the requirements, create tests that prove or disprove the tool's capability to meet the requirements.
- *Identify test cases*—Find or create types of cases to investigate with the forensics tool, and identify information to retrieve from a sample drive or other media. For example, use the

image of a closed case file created with a trusted forensics tool to test a new tool in the same category and see whether it produces the same results.

- *Establish a test method*—Considering the tool's purpose and design, specify how to test it.
- *Report test results*—Describe the test results in a report that complies with ISO 17025, which requires accurate, clear, unambiguous, and objective test reports.

Another standards document, ISO 5725, demands accuracy for all aspects of the testing process, so results must be repeatable and reproducible. "Repeatable results" means that if you work in the same lab on the same machine, you generate the same results. "Reproducible results" means that if you're in a different lab working on a different machine, the tool still retrieves the same information.

Note

NIST has also developed several tools for evaluating drive-imaging tools. These tools are posted on the CFTT Web site at *www.cftt.nist.gov/disk_imaging.htm.*

In addition, NIST created the NSRL project (www.nsrl.nist.gov) with the goal of collecting all known hash values for commercial software and OS files. The primary hash NSRL uses is SHA-1, which generates known digital signatures called the Reference Data Set (RDS). SHA-1 has better accuracy than other hashing methods, such as MD5. The purpose of collecting known hash values is to reduce the number of known files, such as OS or program files, included in a forensics examination of a drive so that only unknown files are left. You can also use the RDS to locate and identify known bad files, such as illegal images and malware, on a suspect drive.

Using Validation Protocols

After retrieving and examining evidence data with one tool, you should verify your results by performing the same tasks with other similar forensics tools. For example, after you use one forensics tool to retrieve disk data, you use another to see whether you retrieve the same information. Although this step might seem unnecessary, you might be asked "How did you verify your results?" on the witness stand. To satisfy the need for verification, you need at least two tools to validate software or hardware upgrades. The tool you use to validate the results should be well tested and documented. A hands-on project at the end of this chapter gives you a chance to validate tools.

Investigators must be confident in a tool's capability to produce consistent and accurate findings during analysis. Understanding how the tool works is equally important, as you might not have vendor support in a courtroom. One way to compare results and verify a new tool is by using a disk editor, such as Hex Workshop or WinHex, to view data on a disk in its raw format. Disk editors typically show files, file headers, file slack, and other data on the physical disk. Although disk editors aren't known for their flashy interfaces, they're reliable and capable of accessing sectors of the digital evidence to verify your findings.

Note

Although a disk editor gives you the most flexibility in testing, it might not be capable of examining a compressed file's contents, such as a .zip file or an Outlook .pst file. This is another reason that testing and validating your tools' capabilities are essential.

If you decide to use a GUI forensics tool, use the recommended steps in the following sections to validate your findings.

Digital Forensics Examination Protocol

1. First, conduct your investigation of the digital evidence with one GUI tool.
2. Then perform the same investigation with a disk editor to verify that the GUI tool is seeing the same digital evidence in the same places on the test or suspect drive's image.
3. If a file is recovered, obtain the hash value with the GUI tool and the disk editor, and then compare the results to verify whether the file has the same value in both tools.

Many investigators in both the public and private sectors use FTK and EnCase as their choice of "flagship" forensics software suites, but they don't rely on them solely; investigators' software libraries often include other forensics utilities to supplement these tools' capabilities.

Digital Forensics Tool Upgrade Protocol

In addition to verifying your results by using two disk-analysis tools, you should test all new releases and OS patches and upgrades to make sure they're reliable and don't corrupt evidence data. New releases and OS upgrades and patches can affect the way your forensics tools perform. If you determine that a patch or upgrade isn't reliable, don't use it on your forensic workstation until the problem has been fixed. If you have a problem, such as not being able to read old image files with the new release or the disk editor generating errors after you apply the latest service pack, you can file an error report with the vendor. In most cases, the vendor addresses the problem and provides a new patch, which you should check with another round of validation testing.

One of the best ways to test patches and upgrades is to build a test hard disk to store data in unused space allocated for a file, also known as file slack. You can then use a forensics tool to retrieve it. If you can retrieve the data with that tool and verify your findings with a second tool, you know the tool is reliable.

As digital forensics tools continue to evolve, you should check the Web for new editions, updates, patches, and validation tests for your tools. Always validate what the hardware or software tool is doing as opposed to what it's supposed to be doing, and remember to test and document why a tool does or doesn't work the way it's supposed to.

Chapter Summary

- Consult your business plan to get the best hardware and software solution for your digital investigation needs.
- The functions required for digital forensics tools are acquisition, validation and verification, extraction, reconstruction, and reporting.
- For your forensics lab, you should create a software library for older versions of forensics utilities, OSs, and applications and maintain older versions of software you have used and retired, such as previous versions of Windows and Linux. In addition, vendors merge or go out of business, so maintaining a backup copy of their tools might come in handy.
- Some forensics tools run in a command-line interface, including those that can find file slack and free space, recover data, and search by keyword. They're designed to run in minimal configurations and can fit on a bootable disk.
- Hardware required for digital forensics includes workstations and devices, such as write-blockers, to prevent contamination of evidence. Before you purchase or build a forensic workstation, consider where you acquire data, which determines the hardware configuration you need.
- Tools that run in Windows and other GUI environments don't require the same level of computing expertise as command-line tools and can simplify training and investigations.
- Before upgrading to a new version of a forensics tool, run a validation test on the new version. The National Institute of Standards and Technology has standard guidelines for verifying forensics tools.

Key Terms

acquisition
brute-force attack
Computer Forensics Tool Testing (CFTT)
extraction
keyword search
National Software Reference Library (NSRL)
password dictionary attack
reconstruction
validation
verification
write-blocker

Review Questions

1. Forensics software tools are grouped into ___ and ___ applications.

2. According to ISO standard 27037, which of the following is an important factor in data acquisition? (Choose all that apply.)

   a. The DEFR's competency

   b. The DEFR's skills in using the command line

   c. Use of validated tools

d. Conditions at the acquisition setting

An encrypted drive is one reason to choose a logical acquisition. True or False?

4. Hashing, filtering, and file header analysis make up which function of digital forensics tools?

a. Validation and verification

b. Acquisition

c. Extraction

d. Reconstruction

Hardware acquisition tools typically have built-in software for data analysis. True or False?

6. The reconstruction function is needed for which of the following purposes? (Choose all that apply.)

a. Re-create a suspect drive to show what happened.

b. Create a copy of a drive for other investigators.

c. Recover file headers.

d. Re-create a drive compromised by malware.

7. List three subfunctions of the extraction function.

Data can't be written to disk with a command-line tool. True or False?

9. Hash values are used for which of the following purposes? (Choose all that apply.)

a. Determining file size

b. Filtering known good files from potentially suspicious data

c. Reconstructing file fragments

d. Validating that the original data hasn't changed

In testing tools, the term "reproducible results" means that if you work in the same lab on the same machine, you generate the same results. True or False?

11. The verification function does which of the following?

a. Proves that a tool performs as intended

b. Creates segmented files

c. Proves that two sets of data are identical via hash values

d. Verifies hex editors

12. What's the advantage of a write-blocking device that connects to a computer through a FireWire or USB controller?

Building a forensic workstation is more expensive than purchasing one. True or False?

A live acquisition can be replicated. True or False?

15. Which of the following is true of most drive-imaging tools? (Choose all that apply.)

a. They perform the same function as a backup.

b. They ensure that the original drive doesn't become corrupt and damage the digital evidence.

c. They create a copy of the original drive.

d. They must be run from the command line.

16. The standards for testing forensics tools are based on which criteria?

a. U.S. Title 18

b. ASTD 1975

c. ISO 17025

d. All of the above

17. A log report in forensics tools does which of the following?

a. Tracks file types

b. Monitors network intrusion attempts

c. Records an investigator's actions in examining a case

d. Lists known good files

18. When validating the results of a forensic analysis, you should do which of the following? (Choose all that apply.)

a. Calculate the hash value with two different tools.

b. Use a different tool to compare the results of evidence you find.

c. Repeat the steps used to obtain the digital evidence, using the same tool, and recalculate the hash value to verify the results.

d. Use a command-line tool and then a GUI tool.

The primary hashing algorithm the NSRL project uses is SHA-1. True or False?

Hands-On Projects

Before starting these projects, create a *Work*\Chap06\Projects folder on your system; it's referred to as your "work folder" in steps. Copy the drive image charlie-2009-12-07.E01 from the M57 Patents case to your work folder, if you haven't done so already. (You can find this file in the downloads section for this chapter on the student companion site for this book.)

Hands-On Project 6-1.

In this project, you create and delete Word and Excel files on a USB drive (or small disk partition, if you don't have a USB drive), and then use OSForensics to examine the drive. Follow these steps:

1. Create a **C6Prj01** folder on your USB drive.
2. Open a new document in Word, and type **This is to test deleting files and then wiping them**. Save the file in the C6Prj01 folder as **Test 6-1.docx** , and exit Word.
3. Open a new workbook in Excel. Type a few numbers, and then save the workbook in the C6Prj01 folder as **Test 6-2.xlsx** . Exit Excel.
4. Use File Explorer to delete both files from the USB drive.
5. Start OSForensics, and start a new case. Type **C6Prj01** for the case name, and enter your name for the investigator. Leave the Acquisition Type option as **Live Acquisition of Current Machine**, and specify the work folder you created for this chapter. Create a subfolder called **C6Prj01**, and click **OK**.
6. If necessary, click **Manage Case** in the left pane, and then click the **Add Device** button in the right pane. Click the drive letter of your USB device, make sure the **Forensics mode** option button is selected, and click **OK**.
7. Make sure the case you just created has a green check mark next to it; if not, double-click the case name, and then click **Start** in the left pane. Using the scroll bar on the far

right, scroll down and click the **Deleted Files & Data Carving** icon. In the Deleted Files Search window, click the **Disk** list arrow, and then click the USB drive in the list of options. Click the **Search** button. Because you're searching for deleted files, you don't need to enter a file string or filter.

8. Double-click the **Test 6-1.docx** file in the lower pane to view its contents. You can also click the **File Info** tab to verify the file's MAC time. Repeat this process with the **Test 6-2.xlsx** file.

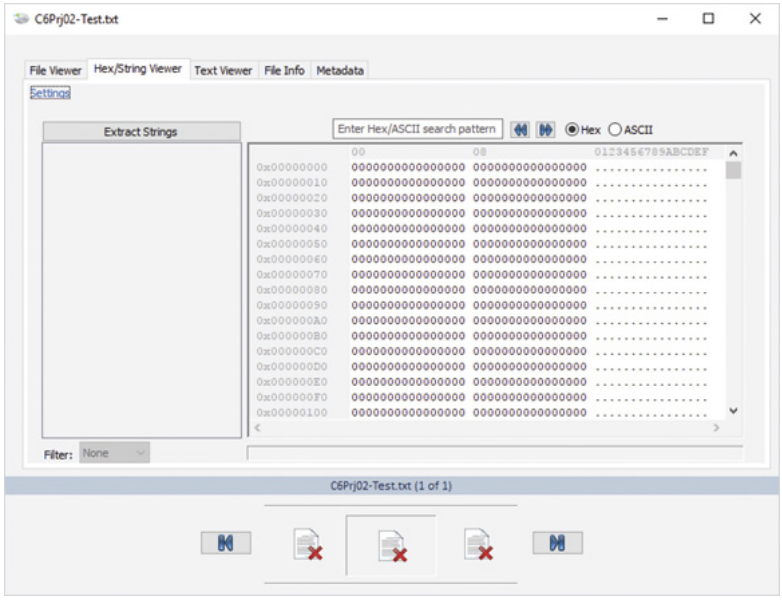
9. Close all open windows, and exit OSForensics.

Hands-On Project 6-2.

In this project, you research and download a disk-cleaning and wiping tool and verify that it works. Make sure you aren't on a production machine. Do an Internet search for disk-cleaning and wiping software, and download and install at least one tool. Then follow these steps:

1. Create a **C6Prj02** folder on your USB drive. Start the tool you just installed.
2. Select your USB drive. Following instructions in the software documentation, wipe the drive.
3. Start OSForensics, and start a new case. Type your name for the investigator's name, type **C6Prj02** for the case name, and enter your work folder as the case path. Create a subfolder called **C6Prj02**, and click **OK**.
4. Click the **Add Device** button. Click the **Drive Letter** option button, if necessary, and in the drop-down list box, click the drive letter for your USB drive. Click **OK**.
5. Click **Start** in the left pane, if necessary, and click the **Deleted Files Search** button on the left. (*Note*: This is another way to open the Deleted Files Search window.)
6. Click the **Disk** list arrow, and then click the USB drive in the list of options. Click the **Search** button. Because you're searching for deleted files, you don't need to enter a file string.
7. Double-click any file in the lower pane to open it.
8. If necessary, click the **Hex/String Viewer** tab (see Figure 6-8). It should show hexadecimal 0 values, which verifies that the disk wipe worked. Take a screenshot, and then exit OSForensics. Write a short report on the tool's effectiveness, and turn it in to your instructor with the screenshot.

Figure 6-8.



Source: PassMark Software, *www.osforensics.com*

The Hex/String Viewer tab

Hands-On Project 6-3.

In this project, you create a test drive by planting evidence in the file slack space on a USB drive or small disk partition. Then you use Hex Workshop to verify that the drive contains evidence. Follow these steps:

1. To format the drive in File Explorer, right-click the drive icon and click **Format**, click to clear the **Quick Format** check box, if necessary, and then click **Start**. If you see a warning message, click **OK** to continue, and then click **OK** in the Format Complete message box.
2. Create a **C6Prj03** folder on the USB drive. *Warning*: This drive should contain data you no longer need.
3. Open a new document in Word, and type **Testing for string Millennium**. Save the file in the C6Prj03 folder as **C6Prj03a.docx** .
4. Close the file, start a new Word document, and type **Testing for string XYZX**. Save the file in the C6Prj03 folder as **C6Prj03b.docx** . Exit Word.

Next, you use Hex Workshop to hide information in file slack space:

1. Start a Web browser, and go to www.hexworkshop.com. Download Hex Workshop, and install it with the default settings.
2. Start Hex Workshop. On a sheet of paper, create a chart with two columns. Label the columns **Item** and **Sector**.
3. In Hex Workshop, click **Disk**, **Open Drive** from the menu. (*Note*: Whenever you see the UAC message box, click **Yes**.) Make sure the USB or disk drive is selected, and then click **OK**.
4. Click **File**, **Open** from the menu. Navigate to and double-click **C6Prj03a.docx** . Scroll down until you see "Testing for string Millennium."
5. Click the tab corresponding to your USB drive, and then click at the beginning of the right column. Click **Edit**, **Find** from the menu. In the Find dialog box, make sure **Text**

String is selected in the Type list box. Type **Millennium** in the Value text box, and then click **OK**. (If Hex Workshop doesn't find "Millennium" the first time, repeat this step.)

6. In the Item column on your chart, write **C6Prj03a.docx.** In the Sector column, write the sector number containing the search text, as shown on the Hex Workshop title bar.

7. Scroll to the bottom of the sector, if necessary. Type **Murder She Wrote** *near* the end of the sector in the right pane, and then click the **Save** toolbar button. (*Note*: If you're asked to enable Insert mode, click **OK**, press **Insert**, click to select the **Disable notification message** check box, and click **OK**, if necessary.)

8. Click the **C6Prj03a.docx** tab. Click **Edit**, **Find** from the menu, make sure **Text String** is selected in the Type list box, type **Murder** in the Value text box, and then click **OK**. Hex Workshop can't find this text in C6Prj03a.docx. Click **Edit**, **Find** from the menu, and then click **OK** to verify that Hex Workshop doesn't find "Murder" in the document. Close the file by clicking the lower **Close** button in the upper-right corner.

9. Click **File**, **Open** from the menu. Navigate to and double-click **C6Prj03b.docx** . Scroll down, if needed, until you see the "Testing for string XYZX" text you entered earlier. (*Hint*: You might need to use the Find command more than once to find this text.)

10. Click the tab for your USB drive, if necessary, and then click at the beginning of the right column. Click **Edit**, **Find** from the menu, type **XYZX** as the value you want to find, and then click **OK**. On your chart, write **C6Prj03b.docx** as the filename in the Item column, and in the Sector column, write the sector number containing the search text, as shown on the Hex Workshop title bar.

11. In the tab for your USB drive, type **I Spy** *near* the end of the sector in the right pane, in the slack space, and then click the **Save** toolbar button.

12. Verify that "I Spy" doesn't appear as part of the file by clicking the **C6Prj03b.docx** tab and searching for this string twice.

13. Close the **C6Prj03b.docx** file, and exit Hex Workshop.

Note

In a forensics lab, you would generate the drive's MD5, SHA-1, or other hash value with a tool such as md5sum, and then generate a copy with one of the GUI tools covered in this chapter.

Hands-On Project 6-4.

You should test new or updated digital forensics tools to make sure they're performing correctly. When complex software applications are updated, they might create new problems and function failures the vendor wasn't aware of. In this project, you test two competing digital forensics analysis tools to see how they compare in locating and recovering data. Keep in mind that even though tools have different strengths, they should yield similar results. To compare OSForensics and Autopsy for Windows, you need the following:

- Autopsy for Windows installed on your workstation (version 4.3.0 used at the time of this writing)
- OSForensics installed on your workstation
- The charlie-2009-12-07.E01 drive image from the M57 Patents case

First, you use Autopsy for Windows to examine the file:

1.

If necessary, install Autopsy for Windows on your workstation, following the instructions in **Chapter 1**. You can also go to www.sleuthkit.org/autopsy/ , click **Download Now**, and install it. (*Note*: If you install a different version from the one used in these steps, you might see a slightly different interface and options.)

2. Start Autopsy for Windows. To begin your analysis, click the **Create New Case** button. In the New Case Information window, type **C6Prj04PD** for the case name. Click the **Browse** button next to the Base Directory text box, navigate to and click your work folder, click **OK**, and then click **Next**. In the Additional Information window, type **001** in the Case Number text box and your name in the Examiner text box. Click **Finish**.

3. In the Add Data Source window, click **Disk Image or VM file** in the Select Type of Data Source to Add section, and then click **Next**. In the Select Data Source window, click the **Browse** button, navigate to your work folder, click **charlie-2009-12-07.E01** , and then click **Open**. Then click **Next**.

4. In the Configure Ingest Modules window, click **Next**. In the Add Data Source window, click **Finish**. A status bar in the lower-right corner shows the file intake. When it's finished, Autopsy then analyzes the files, which might take up to 30 minutes, depending on the amount of RAM in your workstation.

5. Click the **Keyword Search** down arrow at the upper right. In the Search for the pattern(s) text box, type **project2400**, and then click **Search**. If you get an error message stating that the procedure isn't complete, click **Ignore**.

6. In the Search tab, Ctrl+click to select all the files. Right-click the selection, point to **Tag Files**, and click **Tag and Comment**. In the Comment text box, type the search term.

7. Repeat **Steps 5** and 6 for the search term **craiglist**.

8. Click the **Generate Report** button at the top. Click the **Results - HTML** option button for the report format, and then examine the report. When you're finished, exit Autopsy for Windows.

Next, you perform the same searches in OSForensics:

Note

Before starting this part of the project, create a subfolder of your work folder called C6Prj04.

1. Start OSForensics. Click **Start** in the left pane, if necessary, and in the right pane, click **Create Case**.

2. In the New Case dialog box, enter your name for the investigator, type **C6Prj04** for the case name, and click the **Investigate Disk(s) from Another Machine** option button for the acquisition type. Click **Custom Location** for the case folder, click the **Browse** button, navigate to and click your ***Work*\C6Prj04** folder, and then click **OK** twice.

3. Click the **Add Device** button. Click the **Image File** option button, and then browse to your work folder, click the **charlie-2009-12-07.E01** image file, and click **Open**. Click **OK** twice.

4. Click the **Create Index** button in the left pane. In the Step 1 of 5 window, click the **Use Pre-defined File Types** option button, click all the file types listed, and then click **Next**. In the Step 2 of 5 window, click the **Add** button, click **charlie-2009-12-07.E01** , click **OK**, and then click **Next**. In the Step 3 of 5 window, type **Index all file types** in the Index Title text box, and then click **Start Indexing**.

5. When OSForensics finishes indexing the image file, click **OK** in the message box.

Caution

Indexing might take an hour or more, so make sure you allow enough time.

6. Click the **Search Index** button in the left pane. In the Enter Search Words text box, type **project2400**, and then click **Search** in the right pane. Right-click each file in the results, point to **Bookmark**, and click **Red**.

7. In the Enter Search Words text box, type **craigslist**, and then click **Search** in the right pane. Right-click each file in the results, point to **Bookmark**, and click **Yellow**. Repeat this procedure with the search terms **kitty** and **kitten**, assigning the bookmark color red to "kitty" and the bookmark color yellow to "kitten."

8. When you're done, click the **Start** button, and then click the **Generate Report** button. Accept the default settings, and click **OK**. In the report, notice your bookmarked files toward the bottom.

9. Compare the files you found with those found in Autopsy for Windows, and note any discrepancies. Write a two- to three-page report, including screenshots, to submit to your instructor. Explain which tool you prefer to use and why.

10. Exit your Web browser, and exit OSForensics.

Hands-On Project 6-5.

In this project, you use Magnet AXIOM to examine the same file you did in **Hands-On Project 6-4**. Go to www.magnetforensics.com, and request a 30-day free trial. After getting your 30-day license key, follow Magnet's instructions to download and install AXIOM.

Note

You use this tool in **Chapters 11** and 12, too, so your instructor might ask you to do this project later when you get to those chapters.

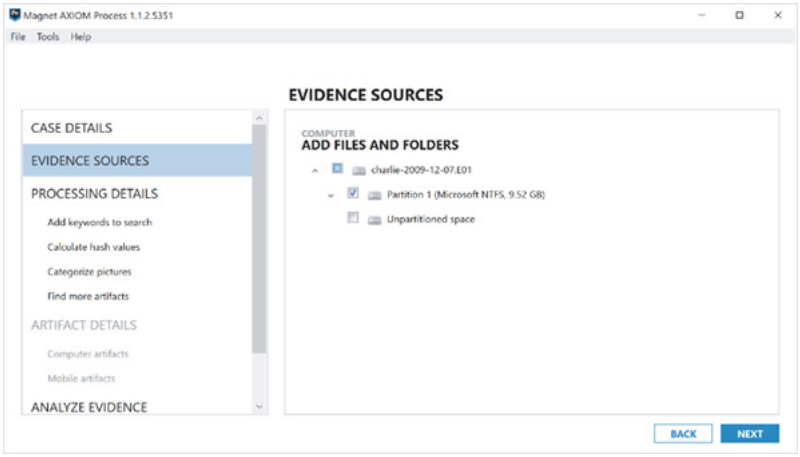
1. Start Magnet AXIOM Process, and click the **CREATE NEW CASE** button. In the CASE DETAILS window, type **001** in the case number text box. In the LOCATION FOR CASE FILES section, type **Hands-On Project 6-5** in the Folder name text box. Click the **BROWSE** button next to the File path text box, navigate to and click your work folder, and click **Select Folder**.

2. Enter the folder name **Hands-On Project 6-5** in the Location of Acquired Evidence text box, and then click **GO TO EVIDENCE SOURCES** in the lower-right corner.

3. In the EVIDENCE SOURCES window, you can choose COMPUTER, MOBILE, or CLOUD in the SELECT EVIDENCE SOURCE section. Click the **COMPUTER** icon. In the next window, click **LOAD EVIDENCE**, and then click **NEXT** . (At this stage, you could actually do a forensic acquisition.)

4. In the SELECT EVIDENCE SOURCE window, click **IMAGE**, browse to and click the **charlie-2009-12-07.E01** file, and click **OK**. In the EVIDENCE SOURCES window, click to clear the **Unpartitioned space** check box (see Figure 6-9), and then click **NEXT**.

Figure 6-9.



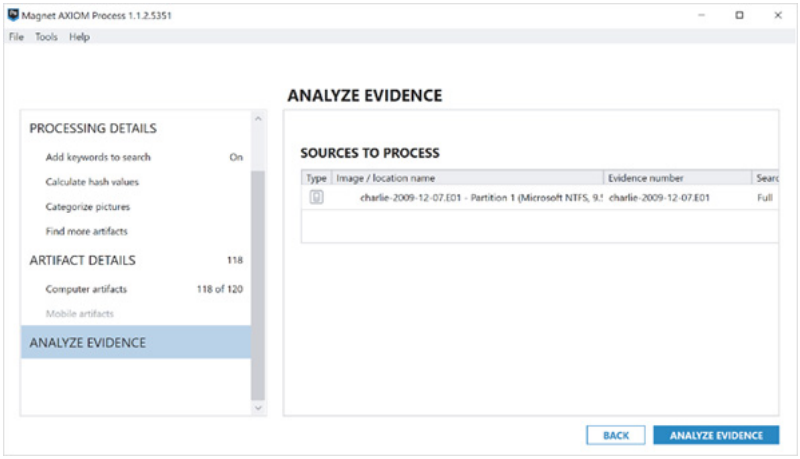
Source: Magnet Forensics, www.magnetforensics.com

The EVIDENCE SOURCES window

5. Accept the default setting **Full**, and click **NEXT**. Then click **GO TO PROCESSING DETAILS**.

6. Click **ADD KEYWORDS TO SEARCH**, scroll to the bottom, and click the **Add Keyword** button. Type **project2400**, **craigslist**, **kitty**, and **kitten**. In the left pane, scroll down, if necessary, and click **ANALYZE EVIDENCE**. Then click the **ANALYZE EVIDENCE** button at the lower right, shown in Figure 6-10.

Figure 6-10.



Source: Magnet Forensics, www.magnetforensics.com

The ANALYZE EVIDENCE window

7. The Magnet AXIOM Examine tool opens and starts running. When it's finished, click **RESULTS** in the left pane and examine the findings.

8. Compare your results with your findings in Autopsy for Windows or OSForensics, and note any discrepancies. Write a two- to three-page report, including screenshots, to submit to your instructor. Explain which tool you prefer to use and why.

Case Projects

Case Project 6-1.

Do online research on two widely used GUI tools, Guidance Software EnCase and AccessData FTK, and compare their features with other products, such as NUIX (www.nuix.com) and

Ontrack EasyRecover Professional (www.ontrack.com/easyrecoveryprofessional). Create a chart outlining each tool's current capabilities (using Table 6-1 as a guide, if you want), and write a one- to two-page report on the features you found most beneficial for your lab.

Case Project 6-2.

Research hex editors available for macOS and Linux. Based on the documentation, how easy would validating these tools be? Select at least two hex editors for each OS, and write a one- to two-page paper describing what you would do to validate them, based on what you have learned in this chapter.

Case Project 6-3.

You need to establish a procedure for your organization on how to validate a new forensics software package. Write two to three pages outlining the procedure you plan to use in your lab. Be sure to cite references, such as the ISO standard or NIST, to support your procedure.

Chapter 7. Linux and Macintosh File Systems

After reading this chapter and completing the exercises, you will be able to:

- Describe Linux file structures
- Describe Macintosh file structures
- Use Linux forensics tools

In Chapter 5, **you explored Microsoft OSs and file systems. Because digital forensics** investigators must understand how OSs store and manage data, this chapter continues this exploration by examining Linux and macOS file structures. You see how they differ from Windows file structures and how information is stored. In addition, this chapter gives you an overview of basic Linux commands. Because many freeware and shareware tools are Linux based, understanding how these commands work is important. You also explore hard links, soft links, and keychains. With iPhones and iPads becoming such popular mobile devices, you need to understand where information is stored in the macOS and how to retrieve it, and this chapter gives you an introduction to this topic. In addition, this chapter introduces some hands-on approaches to identifying Linux file structures with tools such as X-Ways Forensics, OSForensics, Autopsy, and WinHex.

Examining Linux File Structures

UNIX was created in the early 1970s to be a multiuser, multithreaded, secure OS, and many UNIX-based OSs followed. They came in many "flavors" (the term often used for different distributions), but the Open Group was created as a neutral standards consortium that determines and certifies when an OS meets UNIX requirements. For more information, see www.unix.org/online.html.

Some notable UNIX distributions included Silicon Graphics, Inc. (SGI) IRIX, Santa Cruz Operation (SCO) UnixWare, Sun Solaris, IBM AIX, and HP-UX. Most are no longer available, however. Referring to Linux as a "UNIX system" or "UNIX variety" isn't technically correct, as it isn't UNIX certified. However, it's available in even more flavors than UNIX had in its heyday. In addition, the Linux kernel is usually packaged with other software components, such as a GUI and applications, so that users don't have to combine several open-source elements to create a working environment.

The most widely used distributions include Ubuntu, CentOS, Mint, Fedora, and Gentoo. The term "kernel" is often used when discussing Linux because technically, Linux is only the core of the OS. Linus Torvalds, the inventor of Linux, maintains the official kernel. All other tools, graphical interfaces, and so forth are maintained and developed by others. Despite the association of the word "kernel" with Linux terminology, all UNIX-like OSs have a kernel, and so do all Windows OSs.

Note

Ubuntu 16.04 is a long-term support (LTS) version of Ubuntu, meaning it will be supported for the next five years. In some activities in this book, Ubuntu 14.04 is used; it's also an LTS version.

Note

In Ubuntu 15.x and later, the upstart init (initialization) system (/sbin/init) was replaced with the systemd init system (/sbin/upstart). This new init system affects keywords and services but not the location of files. For a full list of comparisons between init systems, see https://wiki.ubuntu.com/SystemdForUpstartUsers.

Table 7-1 lists several Linux system files containing information about users and their activities, and Table 7-2 lists important top-level directories in Linux.

Table 7-1. Linux System Files

System file	Contents
/etc/exports	File systems exported to remote hosts; might include remote drive mappings
/etc/fstab	File system table of devices and mount points
/var/log/lastlog	User's last logon
/var/log/wtmp	Logon and logoff history information
/var/run/utmp	Current user's logon information
/var/log/dmesg	System messages log
/var/log/syslog	System log, occasionally called system.log or kernel.log
/etc/shadow	Master password file, containing hashed passwords for the local system
/etc/group	Group memberships for the local system
/etc/passwd	Account information for the local system

Table 7-2. Core Top-Level Directories of a Linux System

Directory	Contents
/usr	Most applications and commands are in this directory or its subdirectories bin (stands for "binary" and contains binary files required at boot time) and sbin (which requires superuser permission to run the binaries in it).
/etc	Most system configuration files are stored in this directory.
/home	The home directories for all users, usually named after their usernames.
/root	The home directory for the root user (superuser), which is kept separate from other user home directories.
/dev	Device files that act as stand-ins for the devices they represent, as described in **Chapter 3**; for example, /dev/sda is the first non-IDE disk drive on the system, usually the main hard drive.
/var	Subdirectories such as log (often useful for investigations), mail (storing e-mail accounts), and spool (where print jobs are spooled).

Note

Before beginning this activity, create a C:*Work*\Chap07\Chapter folder (referred to as your "work folder" in steps). Download to this work folder any files in this chapter's downloads section on the student companion site for this book.

Chapter 3 covered Linux commands for acquiring images. In this section, you use standard commands to find information about your Linux system. Most of the commands used in this activity work the same in all UNIX-like OSs, including Mac OSs. Remember that UNIX and Linux commands are case sensitive. The wrong capitalization can mean your commands are rejected as incorrect or interpreted as something different. If you don't have Ubuntu 16.04 installed, follow these steps to create a virtual machine for running it.

1. Start VirtualBox, and click the **New** icon at the upper left to start the Create Virtual Machine Wizard.
2. In the Name and operating system window, type **Ubuntu 16.04** for the virtual machine name. Accept the default settings, and click **Next**.

In the Memory size window, increase the setting to **1024**, and then click **Next**.

3 4 In the Hard drive window, click **Create a virtual hard drive now**, and then click **Create**. In the Hard drive file type window, click **Virtual Machine Disk (VMDK)**, and then click **Next**. In the "Storage on physical hard drive" window, click the **Dynamically allocated** option button, and then click **Next**.

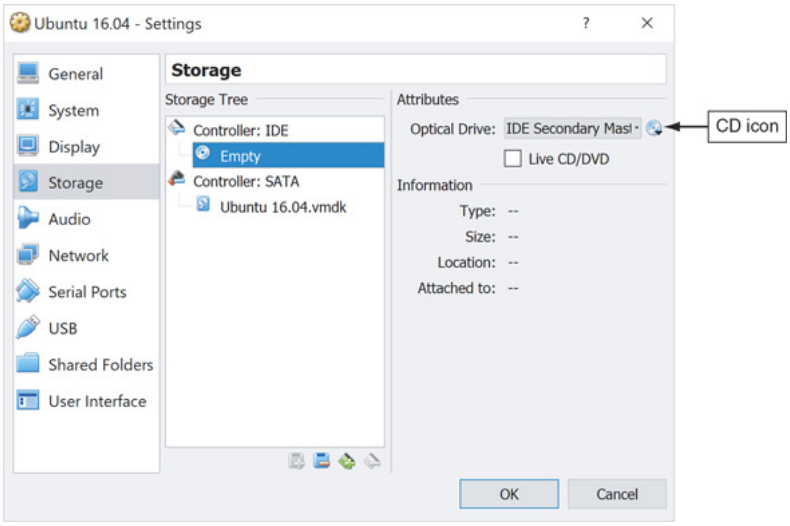
5 In the File location and size window, increase the setting to **20 GB**, and then click **Create**. Leave VirtualBox open.

6 Start a Web browser, go to www.ubuntu.com/download/desktop, and download the ISO image for Ubuntu 16.04.

7 In the Oracle VM VirtualBox Manager, click the **Settings** icon.

8 Click **Storage** in the left pane. In the Storage Tree section, click **Empty** under Controller: IDE. In the Attributes section on the right, click the CD icon (see Figure 7-1). Click **Choose Virtual Optical Disk File**. Navigate to the folder where the ISO file is stored, double-click the ISO file, and then click **OK**.

Figure 7-1.



Source: Oracle VirtualBox, *www.virtualbox.org*

Selecting the source for an ISO file

9 In the Oracle VM VirtualBox Manager, click the **Ubuntu 16.04** virtual machine, and then click the **Start** icon. The VM should follow a standard OS installation. Accept the default settings. Leave the virtual machine running for the next activity.

Before moving on to working with Linux forensics tools, the following activity gives you a chance to review some commands. For example, being able to find a machine's name is always useful; the uname command is used for this task. Displaying file listings and permissions is also useful for investigators. To help with these tasks, you can use the > character to redirect the output of the command preceding it to a file you specify. If the file exists, it's overwritten with a new one; if the file doesn't exist, it's created. The double >> adds output at the *end* of a specified file, if it already exists.

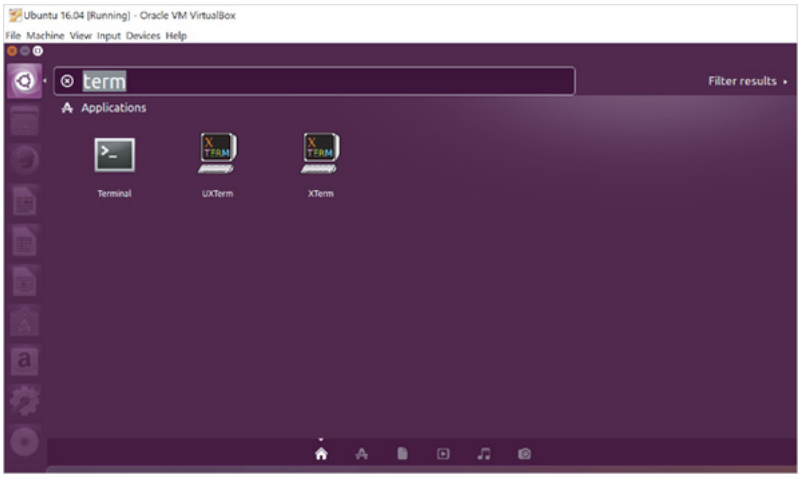
For all the commands in the following activity, you can see their output in the terminal window or add the output to your log file by entering >> ~/my.log at the end of each command. (The ~ character specifies the current user's home directory.) Use the echo command to add notes or headings in the log, and add blank lines to make the contents easier to read. Just don't forget that a single > character replaces the entire file instead of appending to it. You aren't prompted that you're overwriting the file.

As you've learned, Linux commands use options to create variations of a command. There's no difference between grouping letter arguments (such as l and a) or entering them separately. Therefore, ls -la functions the same as ls -l -a. Arguments consisting of multiple letters must be preceded by two — characters instead of one and can't be grouped together, as in ls —all.

As you've learned in previous chapters, the pipe (|) character also redirects the output of the command preceding it. Unlike the > character, however, it redirects output as input for the following command. As you see in this activity, the output of the cat command (which would have displayed the entire file in the terminal window) is sent to the grep command to search for occurrences of your username. The grep command then displays only lines matching search criteria.

1. Start Ubuntu 16.04, if necessary. On the left side of the desktop are icons for different categories of applications. You can use these desktop icons to select an application, or click the Ubuntu icon and start typing the name of the application you want to have the system make a suggestion (see **Figure 7-2**). Type **term** (in this case, to suggest opening the terminal window), and click the **Terminal** icon.

Figure 7-2.



Source: www.ubuntu.com

Opening the terminal window

2. To find the name of your computer and the Linux kernel revision number, type **uname -a** and press **Enter**. To record the results in a file, type **uname -a > ~/my.log** and press **Enter**. Nothing is displayed in the terminal window, but a file called my.log is created in your user profile folder, and the output of the uname -a command is redirected to it.

3. To identify your current path, type **pwd** (which stands for "print working directory") and press **Enter**. In a new terminal window, it's likely the user's home directory.

4. To see a list of the directory's contents, type **ls** and press **Enter**. For comparison, try typing **ls -l** and pressing **Enter**, and then typing **ls -la** and pressing **Enter**. (*Note*: In listings, all files beginning with the . character are usually omitted, unless you add the a option, which stands for "all.")

5. To record the full listing in the same log file you created earlier, type **echo "" >> ~/my.log** and press **Enter**, and then type **echo "Full listing:" >> ~/my.log** and press **Enter**. Finally, type **ls -la >> ~/my.log** and press **Enter**. These commands add a blank line, followed by the heading Full listing:, and finally the listing of the directory's contents in your log file.

6. To see the updated contents of your log file, type **cat ~/my.log** and press **Enter**.

Tip

In current versions of Gnome, which is the Ubuntu desktop, the terminal window's scrollbar doesn't show, but you can display it by moving your mouse pointer to where a scrollbar is usually placed.

7. Type **ifconfig** and press **Enter** to see your network interfaces: wired, wireless, FireWire, lo (the loopback device), and so forth. They're displayed with their MAC addresses (in the "HWaddr" column) and currently assigned IP addresses (in the "inet addr" column). Try the same command with **-a** , and observe the difference in the output. Append the output of this command to your log file.

8. Navigate to the root directory by typing **cd /** and pressing **Enter**. Confirm that you're at the top of the directory tree by typing **pwd** and pressing **Enter**.

9. To identify the username you're currently using, type **whoami** and press **Enter**.

10. To see a listing of all user accounts configured on the system, type **sudo cat/etc/passwd** and press **Enter**, and then type the password and press **Enter**. The output displays the contents of the user account configuration file, passwd. It contains the superuser account "root," the regular user account you're currently using, and a long list of system accounts for system services, such as lp, sys, daemon, and sync. For each account, you see the username, numeric user and group IDs, possibly a formatted display name, the home directory (which is /root for the superuser), and the standard command shell, which is usually /bin/bash for regular and root users.

11. To see just the information for your user account, type **cat /etc/passwd | grep user** (replacing *user* with your own username) and press **Enter**.

12. Append the /etc/passwd file to your log file by typing **cat /etc/passwd >> ~/my.log** and pressing **Enter**. The /etc/passwd file doesn't contain user passwords, although it used to store hashed passwords. Because everyone can read this file, storing even hashed passwords was considered a security risk, so they were moved to the /etc/shadow file, which can be accessed only by the root user.

13. To get a detailed listing of the /etc/shadow file, type **ls -l /etc/shadow** and press **Enter**. If permission is denied, repeat this command preceded by **sudo** .

14. Type **sudo cat /etc/shadow** and press **Enter**, and then type the password and press **Enter**. The file's contents are shown, but only regular user accounts contain a password hash. You should see this information for your user account.

15. To append just the entry for your user account to your log file, type **sudo cat/etc/shadow | grep *user* >> ~/my.log** (replacing *user* with your username) and press **Enter**. This command redirects the output of cat as input to grep, which leaves only the line containing your username, and then appends it to your log file. You can have multiple | pipes in a single command but only one redirection to a file (using > or >>) because the file is a like a dead end—there can be no output after it's redirected to a file.

16. Close the terminal window by typing **exit** and pressing **Enter**, and leave Ubuntu running for the next activity.

Next, you examine deconstructing password hash values in the etc/shadow file. The entries in /etc/shadow are separated by colons. The first field is the username, and the second is the password hash, if available. (For more details, see www.cyberciti.biz/faq/understanding-etcshadow-file/.) The remaining fields are numeric settings, including the maximum time before a password must be changed. Take a look at a typical password hash field:

```
$digit$ShortHashString$LongHashString
```

It begins with a $ symbol, followed by a digit representing the hashing algorithm (which is 6 for SHA-512). Next is another $ symbol followed by a short hash string, which is the password salt, used to make password hashes different even if two users have the same password. Finally, there's another $ symbol followed by a long hash string, which is the salted password hash. Even though passwords aren't stored in plaintext, two users having the same password normally results in identical hashes, which could make cracking passwords easier. In addition, without password salting, it's possible for others to create rainbow tables (discussed in more detail in Chapter 9) to look up passwords.

The salt and hash are stored in an encoded format with letters, numbers, dots, and slashes that's similar to base-64 encoding. Assuming the password hash field starts with 6, meaning SHA-512 is being used, you can use the following command to find a salted password hash, replacing *ShortHashString* and *password* with the information from your own entry in the /etc/shadow file:

```
mkpasswd --method=sha-512 --salt=ShortHashString password
```

This command returns the salted password hash and is used internally by the OS to check whether the correct password was entered. However, knowing how password hash values are created is helpful in case you need to attempt cracking passwords.

File Structures in Ext4

Linux supports a wide range of file systems. The early standard was **Second Extended File System (Ext2)** , and then **Third Extended File System (Ext3)** replaced Ext2 in most Linux distributions. Its major difference from Ext2 was being a journaling file system, which has a built-in file recovery mechanism used after a crash.

A few years later, **Fourth Extended File System (Ext4)** was introduced. Among other features, it added support for partitions larger than 16 TB, improved management of large files, and offered a more flexible approach to adding file system features. Because these changes affected the way the Linux kernel interacts with the file system, adoption of Ext4 was slower in some Linux distributions, but it's now considered the standard file system for most distributions. The Ubuntu version you used previously, for example, has an Ext4 partition at its core, unless you select another file system during installation.

In UNIX and Linux, everything is considered a file, including disk drives, monitors, tape drives, network interface cards, system memory, and directories. UNIX files are defined as objects, which means a file, like an object in an object-oriented programming language, has properties and methods (actions such as writing, deleting, and reading) that can be performed on it.

UNIX/Linux has four components defining the file system: boot block, superblock, inode block, and data block. A block is the smallest disk allocation unit in the UNIX/Linux file system and can be 512 bytes and up; block size depends on how the disk volume is initiated. The **boot block** contains the bootstrap code—instructions for startup. A UNIX/Linux computer has only one boot block, on the main hard disk.

The **superblock** contains vital information about the system and is considered part of the metadata. It specifies the disk geometry and available space and keeps track of all inodes (discussed in more detail in the following section). The superblock also manages the file system, including configuration information, such as block size for the drive, file system names, blocks reserved for inodes, and volume name. Multiple copies of the superblock are kept in different locations on the disk to prevent losing such important information.

Inode blocks contain the first data after the superblock. An inode is assigned to every file allocation unit. As files or directories are created or deleted, inodes are also created or deleted. The link between inodes associated with files and directories controls access to those files or directories.

The **data block** is where directories and files are stored on a disk drive. This location is linked directly to inodes. As in Microsoft file systems, the Linux file system on a PC has 512-byte sectors. A data block is equivalent to a cluster of disk sectors on a FAT or NTFS volume. Blocks range from 1024 to 4096 bytes each on a Linux volume.

Inodes

Inodes contain file and directory metadata and provide a mechanism for linking data stored in data blocks. When a file or directory is created on a Linux file system, an inode is assigned that contains the following information:

- The mode and type of the file or directory
- The number of links to a file or directory
- The UID and GID of the file's or directory's owner
- The number of bytes in the file or directory
- The file's or directory's last access time and last modified time
- The inode's last file status change time
- The block address for the file data
- The indirect, double-indirect, and triple-indirect block addresses for the file data
- Current usage status of the inode
- The number of actual blocks assigned to a file
- File generation number and version number
- The continuation inode's link

The only pieces of metadata not in an inode are the filename and path. Inodes contain modification, access, and creation (MAC) times, not filenames. An assigned inode has 13 pointers that link to data blocks and other pointers where files are stored. Pointers 1 through 10 link directly to data storage blocks in the disk's data block and contain block addresses indicating where data is stored on the disk. These pointers are direct pointers because each one is associated with one block of data storage.

As a file grows, the OS provides up to three layers of additional inode pointers. In a file's inode, the first 10 pointers are called **indirect pointers** . The pointers in the second layer are called **double-indirect pointers** , and the pointers in the last or third layer are called **triple-indirect pointers** .

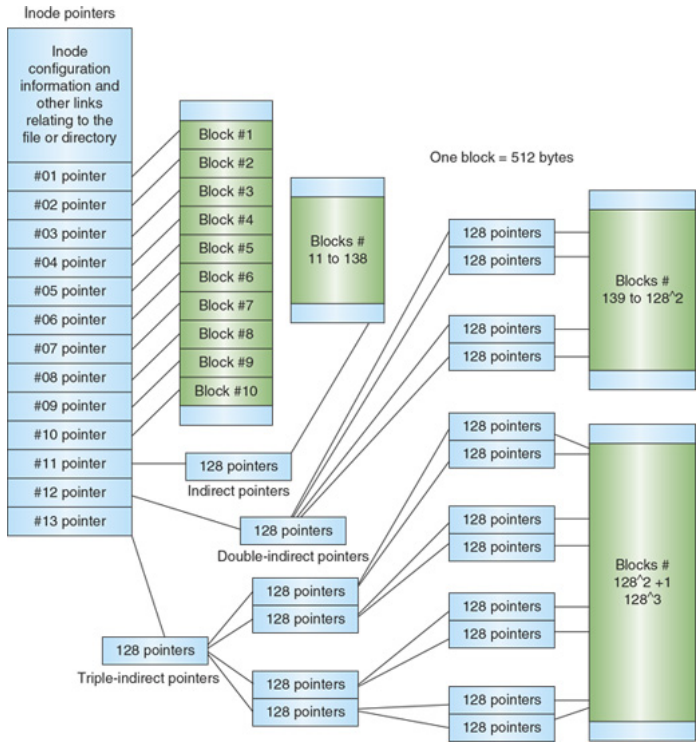
To expand storage allocation, the OS initiates the original inode's 11th pointer, which links to 128 pointer inodes. Each pointer links directly to 128 blocks located in the drive's data block. If all 10 pointers in the original inode are consumed with file data, the 11th pointer links to another 128 pointers. The first pointer in this indirect group of inodes points to the 11th block. The last block of these 128 inodes is block 138.

Note

The term "indirect inode" refers to the 11th pointer in the original inode, which points to another group of inode pointers. In other words, it's linked indirectly to the original inode.

If more storage is needed, the 12th pointer of the original inode is used to link to another 128 inode pointers. From each of these pointers, another 128 pointers are created. This second layer of inode pointers is then linked directly to blocks in the drive's data block. The first block these double-indirect pointers point to is block 139. If more storage is needed, the 13th pointer links to 128 pointer inodes, each pointing to another 128 pointers, and each pointer in this second layer points to a third layer of 128 pointers. File data is stored in these data blocks, as shown in **Figure 7-3**.

Figure 7-3.



Inode pointers in the Linux file system

All disks have more storage capacity than the manufacturer states. For example, a 240 GB disk might actually have 240.5 GB free space because disks always have bad sectors. Windows doesn't keep track of bad sectors, but Linux does in an inode called the **bad block inode** . The root inode is inode 2, and the bad block inode is inode 1. Some forensics tools ignore inode 1 and fail to recover valuable data for cases. Someone trying to mislead an investigator can access the bad block inode, list good sectors in it, and then hide information in these supposedly "bad" sectors.

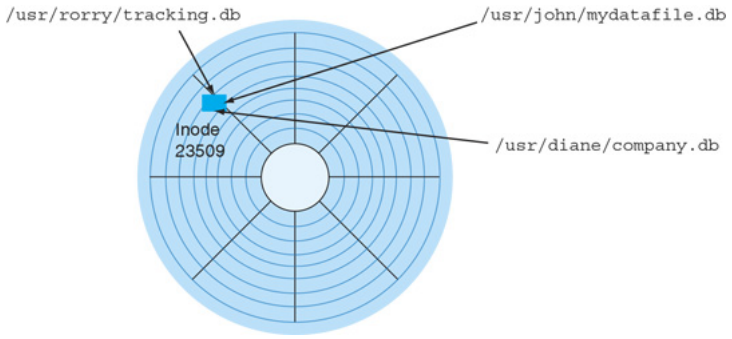
To find bad blocks on your Linux computer, you can use the badblocks command, although you must log in as root to do so. Linux includes two other commands that supply bad block information: mke2fs and e2fsck. The badblocks command can destroy valuable data, but the mke2fs and e2fsck commands include safeguards that prevent them from overwriting important information.

Hard Links and Symbolic Links

A **hard link** is a pointer that allows accessing the same file by different filenames (Rute-Users-Guide/Linux Dictionary V 0.16, www.tldp.org/LDP/Linux-Dictionary/html/index.html). The filenames refer to the same inode and physical location on a drive. Originally, hard links were used so that people with different logins could access the same physical file. If one person changed the file, the changes would be apparent when another user opened the file.

Figure 7-4 shows three hard-linked files pointing to the same inode: 23509. You use the *ln* command to create a hard link. The main requirement is that all files pointing to the same inode have to be on the same physical drive, not on another volume.

Figure 7-4.

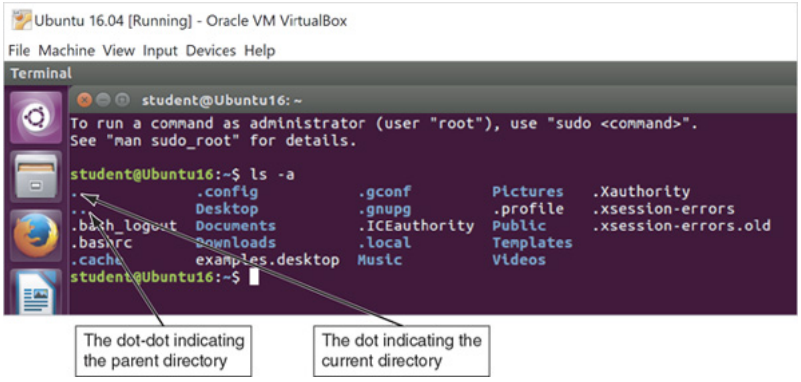


Hard-linked files with different filenames

To see files and their inode numbers, you use the ls -ia command. Inside each inode is a field called **link count** that specifies the number of hard links. The link count for directories is higher than for other file types. If two files have the same inode number, the link count is two. If one file is deleted, the link count drops by one. When the hard link count drops to zero, the file is effectively deleted. Most forensics tools, however, can retrieve these files.

To see the contents of a directory, you use the ls -a command. The first two items are . (called "dot"), which refers to the directory, and .. (called "dot-dot"), which refers to the parent directory (see Figure 7-5). Both dot and dot-dot count as links, so most directories have at least two hard links. Every subdirectory has a dot-dot reference to the corresponding parent directory; therefore, each one adds to the parent directory's link count.

Figure 7-5.



Source: www.ubuntu.com

The ls -a command showing the dot and dot-dot notation

Symbolic links (also known as "soft links" or "symlinks") are simply pointers to other files and aren't included in the link count. Unlike hard links, they can point to items on other drives or other parts of the network; they simply need an absolute path. Symbolic links have an inode of their own, which isn't the same as the inode of the item they're pointing to. Unlike hard links, they depend on the continued existence of the destination they're pointing to, and they're easier to identify on a running Linux system than hard links are. Unlike hard links, which point to their destination with an inode number, symbolic links identify their

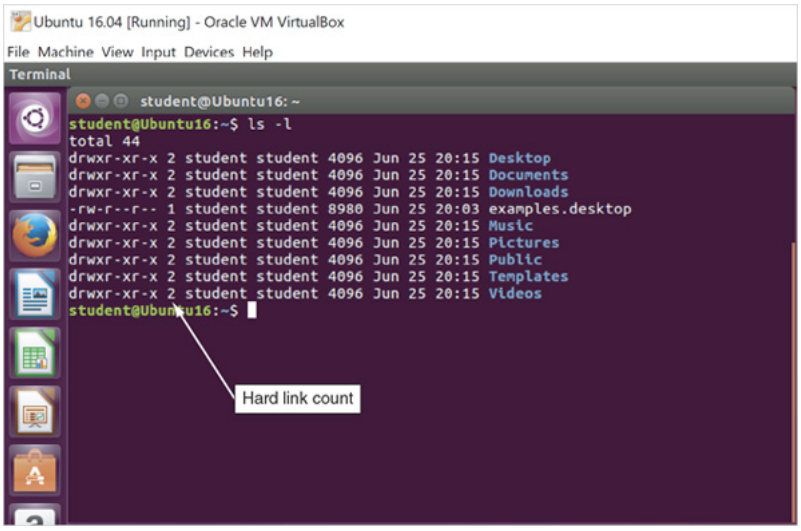
destination by name and path. If a name and path no longer exist, the symbolic link stops working. You create symbolic links with the ln -s command.

To see how hard and symbolic links work, follow these steps:

1. Start Ubuntu, if necessary, and open a terminal window. Type **ls -l** and press **Enter**.
2. The number in the second column shows the hard link count (see **Figure 7-6**). Notice the number of hard links for the Music directory. Type **cd Music** and press **Enter**.

Create a subdirectory called PopTunes by typing **mkdir PopTunes** and pressing **Enter**.

Figure 7-6.

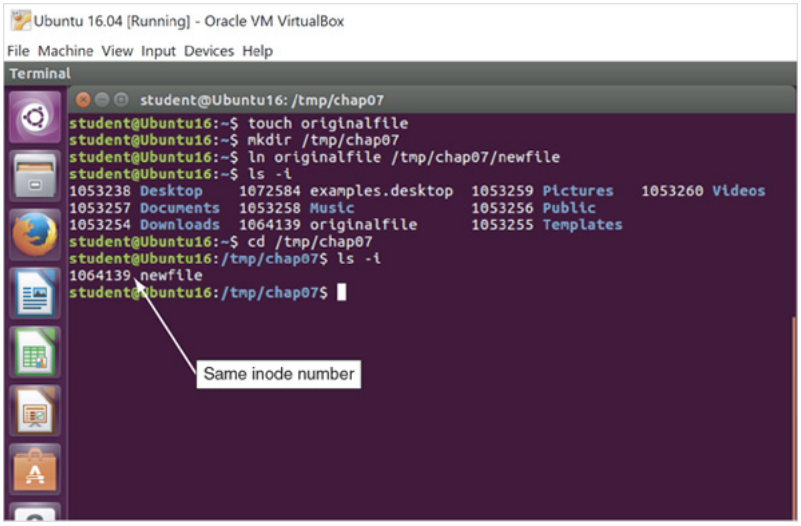


Source: www.ubuntu.com

The ls -l command showing the hard link count

3. Return to your home directory by typing **cd** and pressing **Enter**. Next, type **ls -l** and press **Enter**, and notice that the link count for the Music directory has increased.
4. To create a hard link, first create a new file by typing **touch originalfile** and pressing **Enter**. Then create a new subdirectory in the /tmp directory by typing **mkdir /tmp/chap07** and pressing **Enter**. Switch to your home directory again, if necessary, and type **ln originalfile /tmp/chap07/newfile** and press **Enter**.
5. Type **ls -i** and press **Enter** to see originalfile's inode number. Change to the **/tmp/chap07** directory and repeat this command. Newfile should have the same inode number as originalfile (see Figure 7-7).

Figure 7-7.



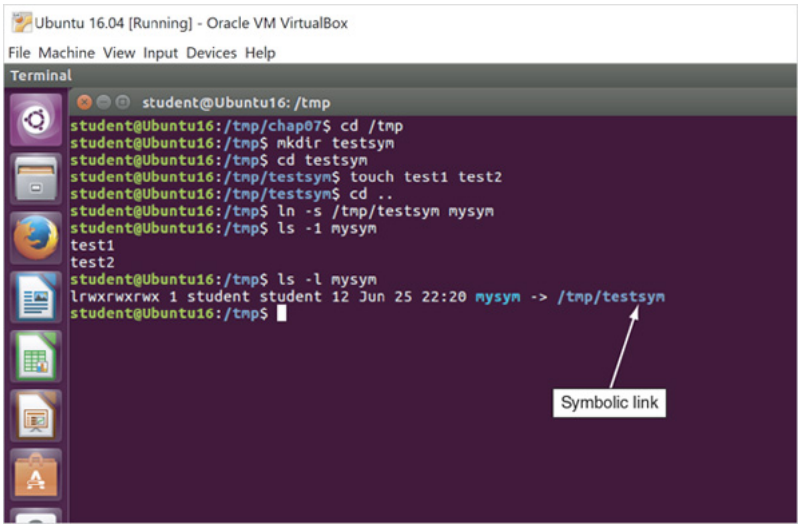
Source: www.ubuntu.com

Comparing inode numbers for a hard link

6. To create a symbolic link, switch to the **/tmp** directory, and type **mkdir testsym** and press **Enter** to create a new subdirectory. Switch to this subdirectory, and create two files by typing **touch test1 test2** and pressing **Enter**. If necessary, type **cd ..** and press **Enter** to return to the /tmp directory. Finally, create the symbolic link by typing **ln -s /tmp/testsym mysym** and pressing **Enter**.

7. Type **ls -1 mysym** (using the numeral one, not a lowercase L, for the option after the hyphen) and press **Enter**. The files you created in the testsym directory are also in mysym. Finally, type **ls -l mysym** and press **Enter**. An arrow points from mysym to the testsym directory, as shown in Figure 7-8, to indicate the symbolic link.

Figure 7-8.



Source: www.ubuntu.com

Creating a symbolic link

8. Leave Ubuntu running and the terminal window open for the next activity.

Understanding Macintosh File Structures

The current Macintosh OS is macOS, version 10.13, code-named High Sierra. Other versions still in use include 10.12.5 (Sierra), 10.11 (El Capitan), 10.9 (Yosemite), 10.6 (Snow Leopard), 10.7 (Lion), and 10.8 (Mountain Lion). macOS is built with the new Apple File System (APFS). The current version offers better security, encryption, and performance speeds, and users can still mount HFS+ drives. Apple's OSs have been developing since 1984 with the introduction of Apple System 1. In 1997, Apple introduced Mac OS 8, followed by Mac OS 9 and then OS X. With OS X, Macintosh moved to the Intel processor and became UNIX based.

Note

Version 10.13 is also known as just "macOS" to conform with names such as iPod, tvOS, and so forth. You can find updated information on it at www.macworld.co.uk/news/mac-software/macos-sierra-latest-version-updates-beta-features-3630374/.

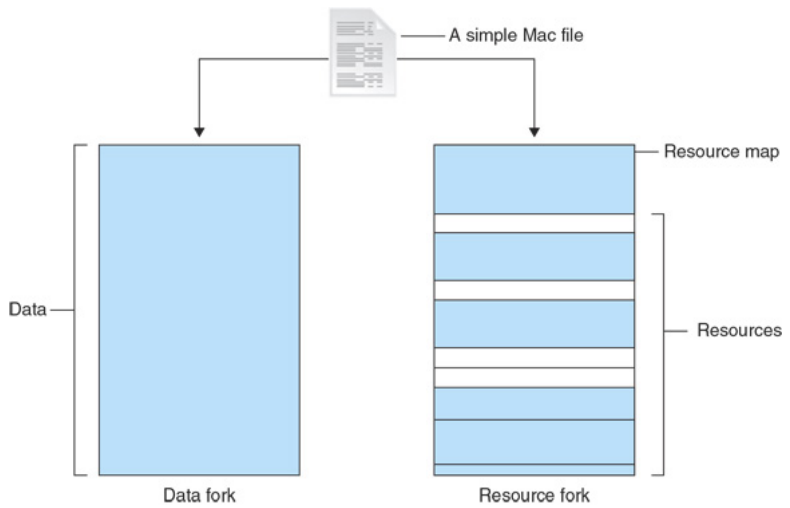
Before OS X, the **Hierarchical File System (HFS)** was used, in which files are stored in directories (folders) that can be nested in other directories. With Mac OS 8.1, Apple introduced **Extended Format File System (HFS+)** . The main difference between HFS and HFS+ is that HFS was limited to 65,536 blocks (512 bytes per block) per volume, and HFS+ raised the number of blocks to more than 4 billion. Consequently, HFS+ supports smaller file sizes on larger volumes, resulting in more efficient disk use. macOS High Sierra also supports the Unix File System (UFS), which isn't covered in this book. In macOS High Sierra, the **Apple File System (APFS)** was introduced. It differs from many file systems in that when data is written to a device, the metadata is also copied to help with crash protection.

An Overview of Mac File Structures

In macOS, a file consists of two parts: a **data fork** , where data is stored, and a **resource fork** , where file metadata and application information are stored (see Figure 7-9). Both forks contain the following essential information for each file:

- Resource map
- Resource header information for each file
- Window locations
- Icons

Figure 7-9.



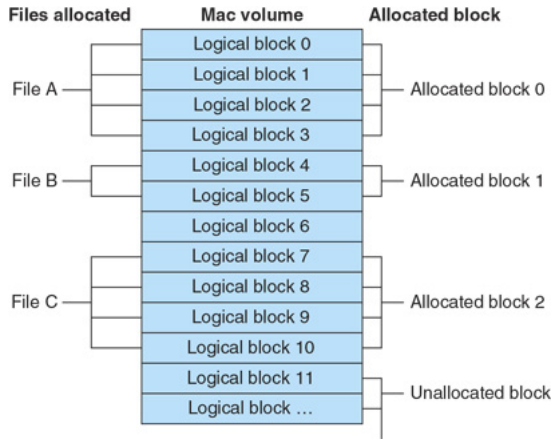
The resource fork and data fork in a macOS file

The data fork typically contains data the user creates, such as text or spreadsheets. Applications, such as Microsoft Word or Excel, also read and write to the data fork. When you're working with an application file, the resource fork contains additional information, such as menus, dialog boxes, icons, executable code, and controls. In macOS, the resource or data fork can be empty.

A volume is any storage medium used to store files. It can be all or part of the storage media for hard disks; however, in Mac OS 9 and earlier, a volume on a floppy disk was always the entire floppy. With larger disks, the user or administrator now defines a volume.

Volumes have allocation blocks and logical blocks. A **logical block** is a collection of data that can't exceed 512 bytes. When you save a file, it's assigned to an **allocation block** , which is a group of consecutive logical blocks. As volumes increase in size, one allocation block might be composed of three or more logical blocks. Figure 7-10 shows the relationship between these two types of blocks. If a file contains information, it always occupies one allocation block. For example, if a data fork contains only 11 bytes of data, it occupies one allocation block (512 bytes) on a disk, which leaves more than 500 bytes empty in the data fork.

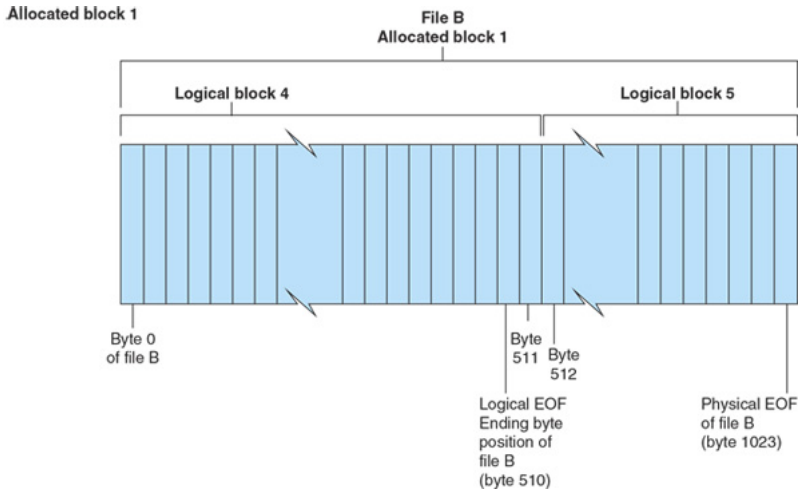
Figure 7-10.



Logical and allocation block structures

The HFS and HFS+ file systems have two descriptors for the end of a file (EOF)—the logical EOF and the physical EOF. The **logical EOF** is the actual ending of a file's data, so if file B has 510 bytes of data, byte 510 is the logical EOF. The **physical EOF** is the number of bytes allotted on the volume for a file, so for file B, it's byte 1023, as shown in Figure 7-11.

Figure 7-11.



Logical EOF and physical EOF

In macOS, file fragmentation is reduced by using **clumps** , which are groups of contiguous allocation blocks. As a file increases in size, it occupies more of the clump. Volume fragmentation is kept to a minimum by adding more clumps to larger files.

For older HFS-formatted drives, the first two logical blocks, 0 and 1, on the volume (or disk) are the boot blocks containing system startup instructions. Optional executable code for system files can also be placed in boot blocks.

Older Mac OSs use the **Master Directory Block (MDB)** for HFS, which is the Volume Information Block (VIB) in HFS+. All information about a volume is stored in the MDB and written to it when the volume is initialized. A copy of the MDB is also written to the next-to-last block on the volume to support disk utility functions. When the OS mounts a volume, some information from the MDB is written to a **Volume Control Block (VCB)** , stored in system memory. When a user no longer needs the volume and unmounts it, the VCB is removed.

The copy of the MDB is updated when the extents overflow file or catalog increases in size. The **extents overflow file** is used to store any file information not in the MDB or a VCB. The **catalog** is the listing of all files and directories on the volume and is used to maintain relationships between files and directories on a volume.

Volume Bitmap, a system application, tracks each block on a volume to determine which blocks are in use and which ones are available to receive data. It has information about the blocks' use but not about their content. Volume Bitmap's size depends on the number of allocated blocks for the volume.

File-mapping information is stored in two locations: the extents overflow file and the file's catalog entry. In earlier Mac versions, the **B*-tree** file system is also used to organize the directory hierarchy and file block mapping. In this file system, files are nodes (records or objects) containing file data. Each node is 512 bytes. The nodes containing actual file data are called leaf nodes; they're the bottom level of the B*-tree. The B*-tree also has the following nodes that handle file information:

- The **header node** stores information about the B*-tree file.
- The **index node** stores link information to previous and next nodes.
- The **map node** stores a node descriptor and map record.

Tip

For more information on HFS and HFS+, see http://wiki.sleuthkit.org/index.php?title=HFS and https://developer.apple.com/library/mac/documentation/Darwin/Reference/Manpages/man1/RezWack.1.html.

Forensics Procedures in Mac

Although understanding Linux file structures can help you learn about macOS file structures, there *are* some differences between the Linux and macOS file systems. For example, Linux has the /home/username and /root directories. In macOS, the corresponding folders are /users/username and /private/var/root. The /home directory exists in macOS, but it's empty. In addition, macOS users have limited access to other user accounts' files, and the guest account is disabled by default. If it's enabled, it has no password, and guest files are deleted at logout.

For forensics procedures in macOS, you must know where file system components are located and how both files and file components are stored. Application settings are in three formats: plaintext, plist files (which include plain XML plists and binary plists, which are condensed XML), and the SQLite database. Plaintext files, of course, can be viewed in any text editor.

Plist files are preference files for installed applications on a system, usually stored in /Library/Preferences. To view them, you use special editors, such as the one available at the Apple Developer Web site (https://developer.apple.com) or PlistEdit Pro (www.macupdate.com/app/mac/14363/plistedit-pro).

To view the SQLite database, use the SQLite Database Browser (http://sqlitebrowser.org). You can also use the new macOS feature called **unified logging** , which is located in /var/db/diagnostics (where log files are stored) and /var/db/uuid.text. It includes three new utilities—log, log collect, and log show—that a forensics examiner can use. For more details, see https://developer.apple.com/videos/play/wwdc2016/721/.

Other files that might contain information useful for an investigation include the following:

- /System/Library/CoreServices/SystemVersion.plist—Contains the OS version.
- /Library/Preferences/SystemConfiguration/NetworkInterfaces.plist—Shows all existing network interfaces. If an interface has been used recently, it's listed in the /private/var/db/dhcpclient/leases directory.
- /private/var/db/DirectoryService/flatfile.db—A list of users on a system; used before Mac OS X v10.7 and is similar to the Linux/UNIX /etc/passwd file.
- /private/var/db/dslocal/nodes/Default/users—Contains users' plist files in Mac OS X after v10.7.
- /private/var/db/shadow/hash—Contains account passwords.

FileVault, introduced with version 10.3, is used to encrypt and decrypt a user's /users directory. It has master keys and recovery keys, which research later proved could be retrieved from RAM and used to crack encryption. In response to these security vulnerabilities, the improved FileVault2 was introduced, which encrypts the whole disk with 128-bit AES encryption.

Other encrypted information you're likely to find during an investigation is passwords. Since Mac OS 8.6, **keychains** have been used to manage passwords for applications, Web sites, and other system files (www.macworld.com/article/2013756/how-to-manage-passwords-with-keychain-access.html). You can find keychain files in a variety of places, including /System/Library/Keychains and /Library/Keychains, and they can be useful to show what

applications and files require passwords. The Mac application Keychain Access enables you to restore passwords.

You need to find deleted files in most investigations, too. In macOS, deleted files are in the Trash folder. If a file is deleted at the command line, however, it doesn't show up in the trash, which is similar to the Recycle Bin in Windows.

Note

Unlike Windows, macOS files retain their filenames in the trash. In addition, when you copy a file in Windows, the timestamp is reset. In macOS, the creation time is copied, so the timestamps are more accurate.

Several vendors have software for examining the macOS file system. In the following section, you look at BlackBag Technologies (www.blackbagtech.com/software-products.html).

Another product for Mac forensics is SubRosaSoft MacForensicsLab (www.macforensicslab.com). Other vendors have added the capability to analyze macOS file systems, such as ProDiscover Forensic Edition and the freeware tools Sleuth Kit and Autopsy (www.sleuthkit.org). Sleuth Kit is discussed in "Using Linux Forensics Tools" later in this chapter.

Acquisition Methods in macOS

To examine a computer running macOS, you need to make an image of the drive, using the same techniques described in **Chapter 5**. You should be aware of some exceptions, however, caused by Apple design and engineering. (In addition, removing the drive from a Mac Mini case is difficult, and attempting to do so without Apple factory training could damage the computer. A MacBook Air poses similar problems, as you need special Apple screwdrivers to open the case.) You need a macOS-compatible forensic boot CD/DVD to make an image, which then must be written to an external drive, such as a FireWire or USB drive. Larger macOS systems are constructed much like desktop PCs, making removal of the hard drive easier.

BlackBag Technologies sells acquisition tools for OS 9 and OS X and offers a forensic boot CD called MacQuisition for making a drive image (see www.blackbagtech.com/software-products/macquisition-2/macquisition.html). It also offers some free tools for forensics examiners (www.blackbagtech.com/resources/freetools.html).

After making an acquisition, the next step is examining the image of the file system with a forensics tool. The tool you use depends on the image file's format. For example, if you used EnCase, FTK, or X-Ways Forensics to create an Expert Witness (.e01) image, you must use one of these tools to analyze the image. If you made a raw format image, you can use any of the following tools:

- BlackBag Technologies Macintosh Forensic Software (OS X only)
- SubRosaSoft MacForensicsLab (OS X only)
- Guidance Software EnCase
- Recon Mac OS X Forensics with Palladin (https://sumuri.com/software/recon/)
- X-Ways Forensics
- AccessData FTK

BlackBag Technologies Macintosh Forensic Software and SubRosaSoft MacForensicsLab have a function for disabling and enabling Disk Arbitration, which is a macOS feature for disabling and enabling automatic mounting when a drive is connected via a USB or FireWire device (see

www.appleexaminer.com). Being able to turn off the mount function in macOS allows you to connect a suspect drive to a Mac without a write-blocking device.

Using Linux Forensics Tools

Learning how to use Linux forensics tools can come in handy when Windows tools don't work or you're having trouble getting a Windows machine to boot. Several commercial and freeware tools are available for analyzing UNIX and Linux file systems. Most commercial forensics tools, such as OSForensics, X-Ways Forensics, Guidance Software EnCase, and AccessData FTK, can analyze Linux Ext2, Ext3, Ext4, ReiserFS, and Reiser4 file systems.

Freeware tools include Sleuth Kit and its Web browser interface, Autopsy Forensic Browser, maintained by Brian Carrier (see www.sleuthkit.org). Sleuth Kit, previously called TASK, is partially based on The Coroner's Toolset (TCT) by Dan Farmer and Wietse Venema and designed as a network analysis tool for investigating attackers.

The U.S. Air Force Office of Special Investigations and the Center for Information Systems Security Studies and Research developed another specialized freeware tool called Foremost (see http://foremost.sourceforge.net). Foremost is a carving tool that can read many image file formats, such as raw and Expert Witness. It has a configuration file, foremost.conf, listing the most common file headers, footers, and data structures. If a file format isn't included in this file, it can be added by using a hex editor to determine the new format's header and footer values and a text editor to update the file. This file is typically in the /usr/local/etc directory and contains instructions on updating it. If your installation is different, read the makefile script in the Foremost tarball to see how the current version is installed. A **tarball** is a highly compressed data file containing one or more files or directories and their contents. It's similar to Windows zip utilities and typically has a .tar or .gz extension.

Installing Sleuth Kit and Autopsy

In **Chapter 1**, you installed Autopsy for Windows. Version 2 can be installed in Linux or macOS. You can find current and past versions of Sleuth Kit and Autopsy Forensic Browser at www.sleuthkit.org.

Note

Older versions of Sleuth Kit and Autopsy are available at Web sites listed on Sleuth Kit's main page. The RPM Package Manager utility makes installing these tools in Red Hat and Fedora Linux much easier. Several other Linux distributions have tools for installing RPM packages. Check their documentation to see how they handle RPM packages.

Caution

In Linux, Sleuth Kit must be installed before Autopsy Forensic Browser, or Autopsy isn't installed correctly. In Windows, however, you just need to install Autopsy. In addition, when you're running Autopsy Forensic Browser in Mac or Linux, you must preface all commands with sudo.

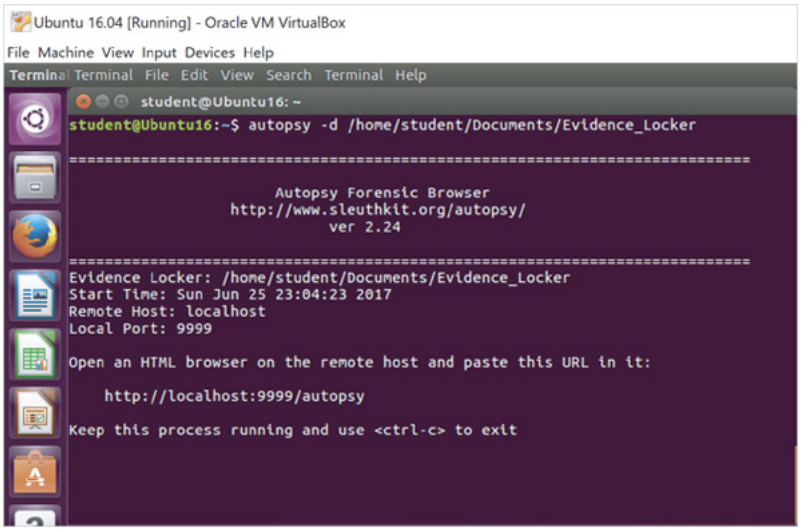
To install Sleuth Kit and Autopsy Forensic Browser in Ubuntu 16.04, you need root user privileges. Follow these steps:

1. If necessary, start Ubuntu and open a terminal window.
2. To install Sleuth Kit, type **sudo apt-get install sleuthkit** and press **Enter**, and then install Autopsy by typing **sudo apt-get install autopsy** and pressing **Enter**.
3.

To confirm that you're in your home directory, type **pwd** and press **Enter**. Next, create the evidence locker for storing files by typing **mkdir Documents/Evidence_Locker** and pressing **Enter**.

4. To start Autopsy and let it know where to store files, type **autopsy -d /home/username/Documents/Evidence_Locker** (see Figure 7-12) and press **Enter**.

Figure 7-12.

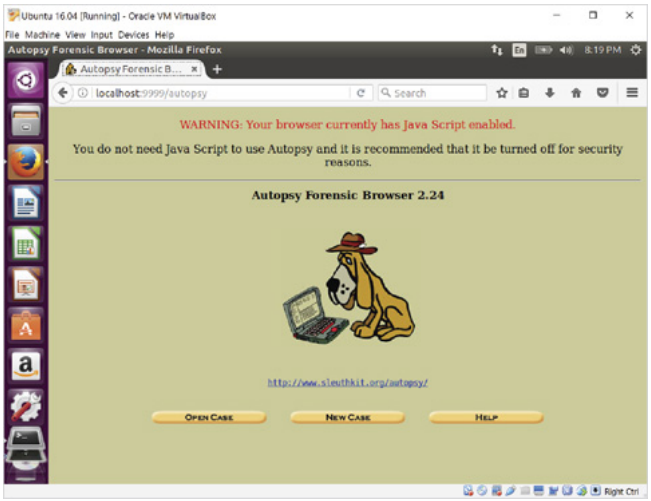


Source: www.sleuthkit.org

Starting Autopsy in Linux

5. Right-click the URL http://localhost:9999/autopsy shown in the terminal window and click **Open Link**. Figure 7-13 shows the Autopsy main window.

Figure 7-13.



Source: www.sleuthkit.org

The Autopsy main window

Tip

If you see a warning message at the top stating that JavaScript is enabled, you have to reconfigure your browser to disable it. After reconfiguring the browser, you might have to exit and restart. If the Autopsy terminal session is still running, simply paste the Autopsy URL into the Address text box again.

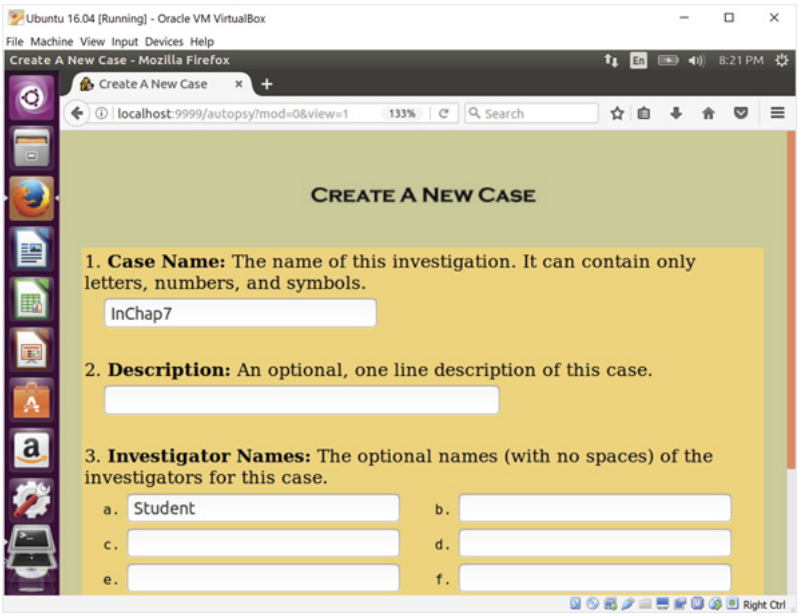
6. Leave Autopsy running and your Web browser open for the next activity.

Examining a Case with Sleuth Kit and Autopsy

In this section, you use Sleuth Kit and Autopsy Forensic Browser to examine an older Linux file system. In digital forensics, sometimes you have to reevaluate cases that are several years old, and this activity gives you a chance to do that. Before starting the examination, copy the GCFI-LX.00n (with *n* representing a number from 1 to 5) image files from your work folder to the evidence locker you set up in the previous activity. Autopsy uses the evidence locker to save results from examinations. To start the examination, follow these steps:

1. In Autopsy's main window, click the **New Case** button shown previously in Figure 7-13. When the Create a New Case dialog box opens, enter **InChap7** for the case name (see Figure 7-14), a description (optional), and your name, and then click the **New Case** button to continue.

Figure 7-14.

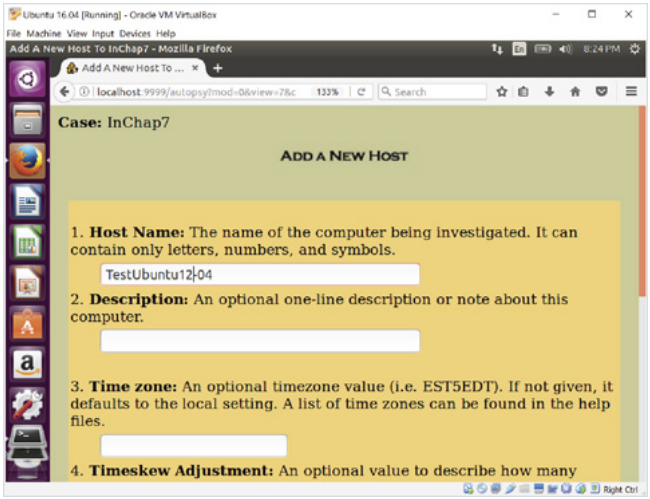


Source: www.sleuthkit.org

The Create a New Case dialog box

2. In the Creating Case dialog box, click **Add Host** to continue. In the Add a New Host dialog box, enter **TestUbuntu12-04** for the hostname (see Figure 7-15), and then click **Add Host**.

Figure 7-15.



Source: www.sleuthkit.org

The Add a New Host dialog box

3 In the Adding host dialog box, click **Add Image** to continue. In the Open Image dialog box, click **Add Image File**.

Note

If you don't click Partition in **Step 4**, the image is read as raw data, and file and directory structures aren't visible to Autopsy.

4 In the Add a New Image dialog box, type the complete path to the evidence locker in the Location text box, click the **Partition** and **Move** option buttons, and then click **Next**. (Remember that Linux commands are case sensitive. If you enter a lowercase filename and the filename is uppercase, Autopsy can't find and load the file.)

Note

If you have multiple segment volumes that are sequentially numbered or lettered (the dd command with the split option without the -d switch), use an asterisk as the extension (for example, GCFI-LX.*) so that all segments are read sequentially.

5 In the Split Image Confirmation dialog box, verify that all images are correctly loaded; if they are, click **Next**. If not, click **Cancel**. (If this data is incorrect, it's probably caused by an error in the pathname to the evidence locker or image files.)

6 In the Image File Details section, click the **Calculate the hash value for this image** option button, and then click **Add**. In the Calculating MD5 message box, click **OK**.

7 In the "Select a volume to analyze or add a new image file" dialog box, click **Analyze** and then **Keyword Search** to start a search for keywords of interest to the investigation.

8 In the Keyword Search of Allocated and Unallocated Space dialog box, type the name **martha** in the text box, and then click **Search**.

9 When the search is finished, Autopsy displays a summary of the search results. To see detailed search results, click the link to results link at the upper left.

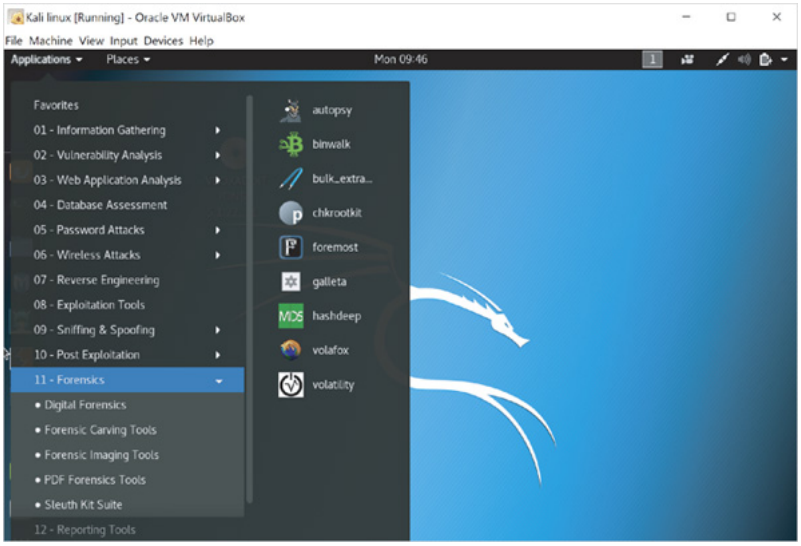
10

Examine the search results by scrolling through the left pane, and then click the **Fragment 236019 "Ascii"** link to view details of the search. Repeat this examination by clicking other ASCII and Hex links for the remaining hits. When you're finished examining the search hits, close the Searching for ASCII and Searching for Unicode dialog box to return to the "Select a volume to analyze or add a new image file" dialog box. Exit Autopsy, and log off Ubuntu.

Kali Linux has several forensics tools in its arsenal. For the full list of these tools, see https://tools.kali.org/tools-listing. Many are command-line tools. You can find the GUI tools in the Kali menu. To explore some of Kali's tools, follow these steps:

1. Start a Web browser, and go to www.kali.org/downloads/. Download the Kali ISO image.
2. Start Virtual Box, and create a VM named **Kali**. Allow at least 2 GB of RAM and increase the storage to **20** GB.
3. Install Kali, accepting the defaults. Set the password to **password**. (Remember that in the real world, you would set a more complex password for security reasons.)
4. Restart Kali, and enter **root** for the username and **password** for the password.
5. Click the **Applications** down arrow, and click **Forensics** (see Figure 7-16). Notice that Autopsy is listed first.

Figure 7-16.

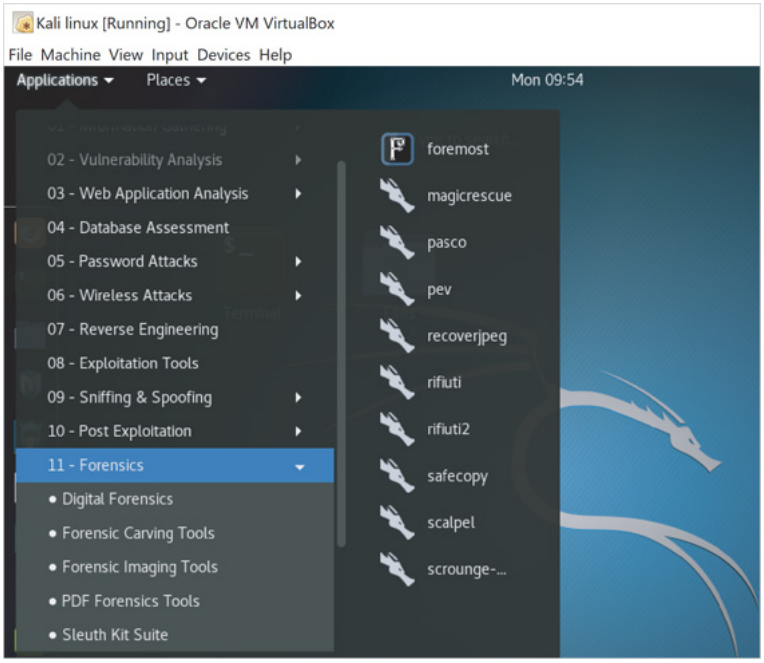


Source: www.kali.org

The forensics tools in Kali Linux

6. Next, click the **Forensic Carving Tools** category, and see the available tools (see Figure 7-17). They tend to be command-line tools; building GUI commercial tool suites requires a lot of work.

Figure 7-17.



Source: www.kali.org

Tools in the Forensic Carving Tools category

7 Exit Kali, and power off the VM.

You have the chance to research and use some of these tools in the hands-on projects.

Chapter Summary

- UNIX was created to be a multiuser, multithreaded, secure OS. The Open Group was formed as a neutral standards consortium that determines and certifies when an OS meets UNIX requirements.
- The Linux kernel is usually packaged with other software components, such as a GUI and applications. The most widely used distributions include Ubuntu, Mint, Fedora, CentOS, and Gentoo.
- Linux supports a wide range of file systems. The most recent, Ext4, added support for partitions larger than 16 TB, improved management of large files, and offered a more flexible approach to adding file system features.
- UNIX and Linux have four components defining the file system: boot block, superblock, inode block, and data block. In addition, an inode is assigned to each file allocation unit that contains file and directory metadata (except the filename and path) and provides a mechanism for linking data stored in data blocks.
- In the Linux file system, a hard link is a pointer that allows accessing the same file by different filenames, which refer to the same inode and physical location on the drive. Symbolic links are pointers to other files; they can point to items on other drives or other parts of the network and don't affect the link count.
- Before macOS, the file systems HFS and HFS+ were used. The main difference is that HFS+ raised the number of blocks to more than 4 billion. Consequently, HFS+ supports smaller file sizes on larger volumes, resulting in more efficient disk use. With the advent of macOS High Sierra, the Apple File System was introduced and provides better security, encryption, and performance speeds.
- In older versions of macOS, a file consists of two parts: a data fork, where data is stored, and a resource fork, where file metadata and application information are stored.
- A volume is any storage medium used to store files. Volumes have allocation blocks and logical blocks. When you save a file, it's assigned to an allocation block, which is a group of consecutive logical blocks. macOS reduces file fragmentation by using clumps, which are groups of contiguous allocation blocks.
- Plist files, which are preference files for installed applications on a system running macOS, can be useful sources of information for a forensics investigation.
- In macOS, unified logging has been added for recording log files and includes new utilities to help forensics examiners.
- The biggest challenge in acquiring images from macOS systems is often physical access to the drive. With many macOS devices, special tools and training from Apple are needed.
- Linux forensics tools are often freeware, so forensics investigators can use them to help keep costs down. Tools such as Autopsy are commonly used.

Key Terms

allocation block

Apple File System (APFS)

B*-tree

bad block inode

boot block

catalog
clumps
data block
data fork
double-indirect pointers
Extended Format File System (HFS+)
extents overflow file
Fourth Extended File System (Ext4)
hard link
header node
Hierarchical File System (HFS)
index node
indirect pointers
inode blocks
inodes
keychains
link count
logical block
logical EOF
map node
Master Directory Block (MDB)
physical EOF
plist files
resource fork
Second Extended File System (Ext2)
superblock
symbolic links
tarball
Third Extended File System (Ext3)
triple-indirect pointers
unified logging
Volume Control Block (VCB)

Review Questions

1. Explain the differences in resource and data forks used in macOS.

2. Which of the following is the main challenge in acquiring an image of a system running macOS? (Choose all that apply.)

   a. Most commercial software doesn't support macOS.

   b. Vendor training is needed.

   c. The macOS is incompatible with most write-blockers.

   d. You need special tools to remove drives from a system running macOS or open its case.

3. To recover a password in macOS, which tool do you use?

a. Finder

b. PRTK

c. Keychain Access

d. Password Access

4. What are the major improvements in the Linux Ext4 file system?

5. How does macOS reduce file fragmentation?

6. Linux is the only OS that has a kernel. True or False?

7. Hard links work in only one partition or volume. True or False?

8. Which of the following Linux system files contains hashed passwords for the local system?

a. /var/log/dmesg

b. /etc/passwd

c. /var/log/syslog

d. /etc/shadow

9. Which of the following describes the superblock's function in the Linux file system? (Choose all that apply.)

a. Stores bootstrap code

b. Specifies the disk geometry and available space

c. Manages the file system, including configuration information

d. Contains links between inodes

10. What's the Disk Arbitration feature used for in macOS?

11. In Linux, which of the following is the home directory for the superuser?

a. home

b. root

c. super

d. /home/superuser

12. Which of the following certifies when an OS meets UNIX requirements?

a. IEEE

b. UNIX Users Group

c. The Open Group

d. SUSE Group

13. On most Linux systems, current user login information is in which of the following locations?

a. /var/log/dmesg

b. /var/log/wmtp

c. /var/log/usr

d. /var/log/utmp

14. Hard links are associated with which of the following?

a. Dot notation

b. A specific inode

c. An absolute path to a file

d. Hidden files

15. Which of the following describes plist files? (Choose all that apply.)

a. You must have a special editor to view them.

b. They're found only in Linux file systems.

c. They're preference files for applications.

d. They require special installers.

16. Data blocks contain actual files and directories and are linked directly to inodes. True or False?

17. Which of the following is a new file added in macOS? (Choose all that apply).

a. /private/var/db

b. /private/db

c. /var/db/diagnostics

d. /var/db/uuid.text

Hands-On Projects

Create a *Work*\Chap07\Projects folder on your system before starting the projects; it's referred to as your "work folder" in steps. All the data files you use in these projects are from previous chapters.

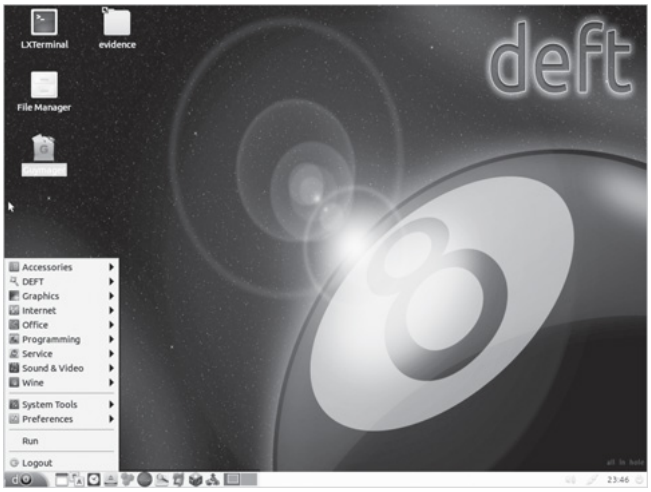
Hands-On Project 7-1.

In this project, you explore another free Linux forensics tool. The Digital Evidence and Forensics Toolkit (DEFT) was created at the University of Bologna, Italy.

1. Start a Web browser, if necessary, and go to www.deftlinux.net. Download the DEFT ISO file and the user's manual. Use the ISO file to create a bootable DVD. (You aren't installing it on your hard drive. You might need to change the BIOS to boot from the CD/DVD drive.)

2. Start DEFT. The opening window should look similar to **Figure 7-18**. Click **Start**, **DEFT**.

Figure 7-18.



Source: www.deftlinux.net

The opening window in DEFT

3. Open the **MountManager** tool, and take a screenshot of this window for your report. In the DEFT 8 Warning! message box, click **I know what I'm doing**. Next, click **Start**, DEFT. Point to **Hashing**, and click **Dhash2**. Make a note of the types of hashes that are available, and then close this tool.

4. Click the **Autopsy** icon to open the Autopsy Forensic Browser window and the text interface. Take a screenshot of these windows, and then exit both.

5. Click the **Digital Forensics Framework (DFF)** icon. Examine its interface to get an idea of what functions it has. If you have time, go to its Web site to learn more about it.

6. Finally, click the **GHex** icon. This tool is a simple hex and binary editor. Examine its interface, and take a screenshot.

7. Write a one- to three-page paper explaining how this tool could be used in the field, and include your screenshots.

Hands-On Project 7-2.

The purpose of this project is to become more familiar with the Linux version of Sleuth Kit and Autopsy. The best way to learn a tool, especially one that isn't well documented, is to explore its functions. You're encouraged to work in teams for this project and share your findings with other students. In this project, you use the image file GCFI-datacarve-FAT.dd from Chapter 3 and analyze it with Sleuth Kit and Autopsy. You need a system with a Linux virtual machine and Sleuth Kit and Autopsy installed. Follow these steps:

1. Copy the **GCFI-datacarve-FAT.dd** file to your Linux virtual machine with Sleuth Kit and Autopsy installed. Start Sleuth Kit and Autopsy. In the main window, click **New Case**. In the Create a New Case dialog box, fill in your information (using **GCFI-datacarve-FAT** for the case name), and then click **New Case**.

2. In the Creating Case dialog box, click **Add Host**, and in the Add a New Host dialog box, enter your information, and click **Add Host**.

3. In the Adding host dialog box, click **Add Image** to continue. In the Open Image dialog box, click **Add Image File**. In the Add a New Image dialog box, type the full pathname and the **GCFI-datacarve-FAT.dd** image filename in the Location text box, click the **Partition** option button, click the **Copy** option button for the import method, and then click **Next**.

4. In the Image File Details section, click **Add**, and in the Testing partitions dialog box, click **OK**. In the "Select a volume to analyze or add a new image file" dialog box, click the **Analyze** button.

5. In the Analysis dialog box, click **File Analysis**, and then click **Generate MD5 List of Files**. In the MD5 results window, save the list as **GCFI-datacarve-FAT-MD5.txt** in your work folder, and close the MD5 results window.

6. Next, in the Analysis dialog box, click **File Type**, click **Sort Files by Type**, and then click **OK**. When the analysis is finished, print the Results Summary frame of the Web page.

7. Click **Image Details**, and in the General File System Details dialog box, print the frame containing the results.

8. Write a report describing the information each function asks for and what information it produces so that you can begin building your own user manual for this tool.

Hands-On Project 7-3.

In this project, you explore the command-line forensics tools in Kali Linux. Go to https://tools.kali.org/tools-listing, and in the Applications menu, scroll down to the Forensics

option. Select three tools, and research their functions and syntax. Start Kali Linux, and use the three tools you selected on the charlie-work-usb-2009-12-11.E01 file or another file you have already worked with. Write a one- to two-page paper comparing the stand-alone tools with OS Forensics or WinHex.

Case Projects

Case Project 7-1.

Research and compare forensics tools that can examine Mac, iPod, and iPhone devices. Create a table listing the features they have in common, differences in functions, and price. Write a short paper stating which one you would choose if you were an investigator for a small firm, and explain why.

Case Project 7-2.

This chapter introduced Autopsy for Windows, which is freeware. Compare it with OSForensics and another free tool of your choice. Describe how each tool performs in Linux based on research you do using blogs, user groups, and user manuals.

Chapter 8. Recovering Graphics Files

After reading this chapter and completing the exercises, you will be able to:

- Describe types of graphics file formats
- Explain types of data compression
- Explain how to locate and recover graphics files
- Describe how to identify unknown file formats
- Explain copyright issues with graphics

Many digital forensics investigations involve graphics, especially those downloaded from the Web and circulated via e-mail. To examine and recover graphics files, you need to understand the basics of computer graphics, including file characteristics, common file formats, and compression methods for reducing file size. This chapter begins with an overview of computer graphics and data compression, and then explains how to locate and recover graphics files based on information stored in file headers. You learn how to identify and reconstruct graphics file fragments, analyze graphics file headers, and repair damaged file headers.

This chapter also explores tools for viewing graphics files you recover and discusses two issues related to computer graphics: steganography and copyrights. Steganography involves hiding data, including images, in files. Copyrights determine the ownership of media, such as images downloaded from a Web site, and the right to use media.

Recognizing a Graphics File

Graphics files contain digital photographs, line art, three-dimensional images, text data converted to images, and scanned replicas of printed pictures. You might have used a graphics program, such as Microsoft Paint, Adobe Photoshop, or Gnome GIMP, to create or edit an image. A graphics program creates one of three types of graphics files: bitmap, vector, and metafile. **Bitmap images** are collections of dots, or pixels, in a grid format that form a graphic. **Vector graphics** are based on mathematical instructions that define lines, curves, text, ovals, and other geometric shapes. **Metafile graphics** are combinations of bitmap and vector images.

You can use two types of programs to work with graphics files: graphics editors and image viewers. You use graphics editors to create, modify, and save bitmap, vector, and metafile graphics. You use image viewers to open and view graphics files, but you can't change their contents. When you use a graphics editor or an image viewer, you can open a file in one of many graphics file formats, such as BMP, GIF, and JPEG. Each format has different qualities, including the amount of color and compression it uses. If you open a graphics file in a graphics editor that supports multiple file formats, you can save the file in another file format. However, converting graphics files in this way can change the image quality, as you see in a hands-on project at the end of this chapter.

Understanding Bitmap and Raster Images

Bitmap images store graphics information as grids of **pixels** , short for "picture elements." **Raster images** are also collections of pixels, but they store pixels in rows to make images easy to print. In most cases, printing an image converts (rasterizes) it to print pixels line by line instead of processing the complete collection of pixels.

A bitmap's image quality on a monitor is governed by **resolution** , which determines the amount of detail that's displayed. Resolution is related to the density of pixels onscreen and depends on a combination of hardware and software. Monitors can display a range of resolutions; the higher the resolution, the sharper the image. Computers also use a video card containing a certain amount of memory for displaying images. The more advanced the video card's electronics and the more memory it has, the more detailed instructions it can accept, resulting in higher-quality images.

For example, the monitor and video card on a Windows computer might support a 4096 × 2160 resolution, which means displaying 4096 pixels horizontally and 2160 pixels vertically. Because a bitmap image is defined by pixel size, high-resolution images use smaller pixels than low-resolution images do.

Software also contributes to image quality. Software includes drivers, which are coded instructions that set a video card's display parameters, and programs used to create, modify, and view images. With some programs, such as IrfanView (www.irfanview.com), you can view many types of images; with other programs, you can view or work with only the graphics files they create. Digital graphics professionals use programs that support high resolutions to have more control over the display of bitmap images. However, bitmaps, especially those with low resolution, usually lose quality when you enlarge them.

Another setting that affects image quality is the number of colors the monitor displays. Graphics files can have different amounts of color per pixel, but each file must support colors with bits of space. The following list shows the number of bits per colored pixel:

- 1 bit = 2 colors
- 4 bits = 16 colors
- 8 bits = 256 colors
- 16 bits = 65,536 colors
- 24 bits = 16,777,216 colors
- 32 bits = 4,294,967,296 colors

Bitmap and raster files use as much of the color palette as possible. However, when you save a bitmap or raster file, the resolution and color might change, depending on the colors in the original file and whether the file format supports these colors.

Understanding Vector Graphics

Vector graphics, unlike bitmap and raster images, use lines instead of dots to make up an image. A vector file stores only the calculations for drawing lines and shapes; a graphics program converts these calculations into an image. Because vector files store calculations, not images, they are generally smaller than bitmap files, thereby saving disk space. You can also enlarge a vector graphic without affecting image quality—to make an image twice as large, a vector graphics program, such as CorelDRAW and Adobe Illustrator, computes the image mathematically.

Understanding Metafile Graphics

Metafile graphics combine raster and vector graphics and can have the characteristics of both file types. For example, if you scan a photograph (a bitmap image) and then add text or arrows (vector drawings), you create a metafile graphic. Although metafile graphics have the features of both bitmap and vector files, they share the limitations of both. For example, if you enlarge a metafile graphic, the area created with a bitmap loses some resolution, but the vector-formatted area remains sharp and clear.

Understanding Graphics File Formats

Graphics files are created and saved in a graphics editor, such as Microsoft Paint, Adobe Freehand MX, Adobe Photoshop, or Gnome GIMP. Some graphics editors, such as Freehand MX, work only with vector graphics, and some programs, such as Photoshop, work with both.

Most graphics editors enable you to create and save files in one or more of the **standard graphics file formats** . Standard bitmap file formats include Portable Network Graphic (.png), Graphics Interchange Format (.gif), Joint Photographic Experts Group (.jpg or .jpeg), Tagged

Image File Format (.tif or .tiff), and Windows Bitmap (.bmp). Standard vector file formats include Hewlett-Packard Graphics Language (.hpgl) and AutoCad (.dxf).

Nonstandard graphics file formats include less common formats, such as Targa (.tga) and Raster Transfer Language (.rtl); proprietary formats, such as Photoshop (.psd), Illustrator (.ai), and Freehand (.fh11); newer formats, such as Scalable Vector Graphics (.svg); and old or obsolete formats, such as Paintbrush (.pcx). Because you can open standard graphics files in most or all graphics programs, they are easier to work with in a digital forensics investigation. If you encounter files in nonstandard formats, you might need to rely on your investigative skills to identify the file as a graphics file, and then find the right tools for viewing it.

To determine whether a file is a graphics file and to find a program for viewing a nonstandard graphics file, you can search the Web or consult a dictionary Web site. For example, suppose you find a file with a .tga extension during an investigation. None of the programs on your forensic workstation can open the file, and you suspect it could provide crucial evidence. To learn more about this file format, see www.garykessler.net/library/file_sigs.html, or follow these steps:

1. Start your Web browser, and go to www.webopedia.com.
2. Type **tga** in the "Enter a term" text box, and click **Search**. Webopedia lists links to additional Web pages describing the .tga file format.
3. In the Webopedia search results Web page, click the **Data Formats and File Extensions: T Web** link, which is www.webopedia.com/quick_ref/graphics_formats.asp.
4. Scroll down until you find a definition of this format, and write it down. When you're finished, exit your Web browser.

Understanding Digital Photograph File Formats

Digital photographs have had an impact on digital forensics; witnesses or suspects can create them easily with smartphones, digital cameras and closed-circuit television surveillance. As a digital forensics investigator, you might need to examine a digital photo created by a witness to an accident, for example. Crimes such as child pornography might involve hundreds of digital photos of alleged victims, and knowing how to analyze the data structures of graphics files can give you additional evidence for a case. In addition, knowing how digital photos are created and how they store unique information can contribute to your credibility when presenting evidence. Most, if not all, digital cameras produce digital photos in raw or Exif format, described in the following sections.

Examining the Raw File Format

Referred to as a digital negative, the **raw file format** is typically used on many higher-end digital cameras. A camera performs no enhancement processing—hence the term "raw" for this format. Sensors in a digital camera simply record pixels on the memory card. One advantage of this format is that it maintains the best picture quality.

From a digital forensics perspective, the biggest disadvantage of the raw file format is that it's proprietary, and not all image viewers can display these formats. To view a raw graphics file, you might need to get the viewing and conversion software from the camera manufacturer. Each manufacturer has its own program with an algorithm to convert raw data to other standard formats, such as JPEG or TIF. The process of converting raw picture data to another format is called **demosaicing** .

Note

For more information on raw format images, see http://helpx.adobe.com/photoshop/digital-negative.html.

Examining the Exchangeable Image File Format

Most digital photographs are stored in the **Exchangeable Image File (Exif)** format. The Japan Electronics and Information Technology Industries Association (JEITA) developed it as a standard for storing metadata in JPEG and TIF files (see http://home.jeita.or.jp/tsc/std-pdf/CP3451C.pdf). When a digital photo is taken, information about the device (such as model, make, and serial number) and settings (such as shutter speed, focal length, resolution, date, and time) are stored in the graphics file. Most digital devices store graphics files as Exif JPEG files. In addition, if the device has GPS capability, the latitude and longitude location data might be recorded in the Exif section of the file. Location data stored in digital images is discussed in more detail in Chapter 12.

Because the Exif format collects metadata, investigators can learn more about the type of digital device and the environment in which photos were taken. Viewing an Exif JPEG file's metadata requires special programs, such as Exif Reader (www.takenet.or.jp/~ryuuji/minisoft/exifread/english/), IrfanView (www.irfanview.com), or Magnet Forensics AXIOM (www.magnetforensics.com), which has a built-in Exif viewer.

Originally, JPEG and TIF formats were designed to store only digital photo data. Exif is an enhancement of these formats that modifies the beginning of a JPEG or TIF file so that metadata can be inserted. In the similar photos in **Figure 8-1**, the one on the left is an Exif JPEG file, and the one on the right is a standard JPEG file.

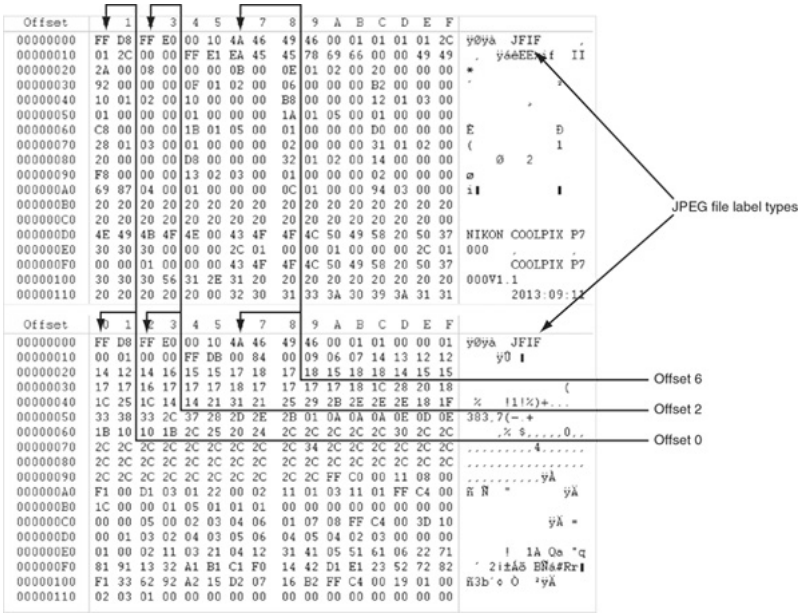
Figure 8-1.

Exif picture file JPEG picture file

Similar Exif and JPEG photos

Figure 8-2 shows the differences between file headers in Exif and standard JPEG files. Sawtoothmt.jpg is an Exif file, and Sawtoothmtn.jpg is a standard JPEG file. The first 160 (hexadecimal 0x9F) bytes are displayed for both files.

Figure 8-2.

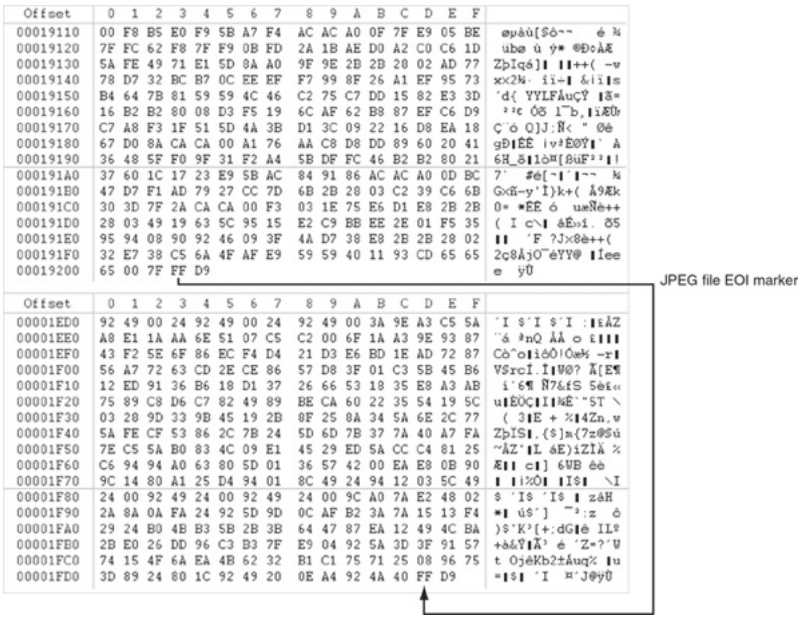


Source: X-Ways AG, www.x-ways.net

Differences in Exif and JPEG file header information

All JPEG files, including Exif, start from offset 0 (the first byte of a file) with hexadecimal FFD8. The current standard header for regular JPEG files is JPEG File Interchange Format (JFIF), which has the hexadecimal value FFE0 starting at offset 2. For Exif JPEG files, the hexadecimal value starting at offset 2 is FFE1. In addition, the hexadecimal values at offset 6 specify the label name (refer to **Figure 8-2**). For all JPEG files, the ending hexadecimal marker, also known as the end of image (EOI), is FFD9 (see Figure 8-3).

Figure 8-3.

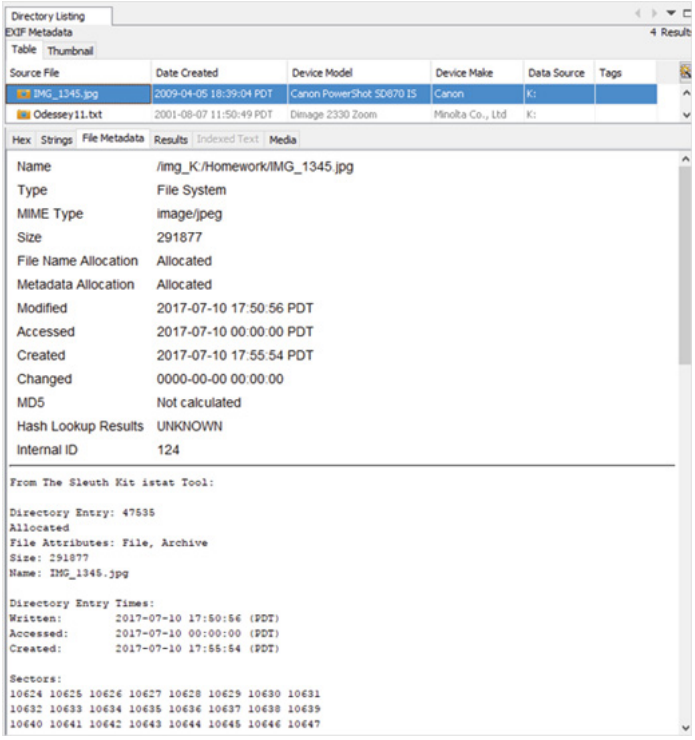


Source: X-Ways AG, www.x-ways.net

EOI marker FFD9 for all JPEG files

With tools such as Autopsy and Exif Reader, you can extract metadata as evidence for your case. As you can see in **Figure 8-4**, Autopsy shows that the picture was taken on July 10, 2017, at 5:50 p.m. PDT.

Figure 8-4.



Source: www.sleuthkit.org

Autopsy displaying metadata from an Exif JPEG file

As in any digital forensics investigation, determining date and time for a file is important. Getting this information might not be possible, however, for a variety of reasons, such as suspects losing cameras after transferring photo files to their computers. You should list this type of evidence as subjective in your report because intentional and unintentional acts make date and time difficult to confirm. For example, suspects could alter a camera's clock intentionally to record an incorrect date and time when a picture is taken. An unintentional act could be the battery or camera's electronics failing, for example, which causes an incorrect date and time to be recorded. When you're dealing with date and time values in Exif metadata, always look for corroborating information, such as where the picture was taken or whether the device is set to Coordinated Universal Time (abbreviated as UTC), to help support what you find in metadata.

For example, the photograph in **Figure 8-1** was taken in Sante Fe, New Mexico, on September 10, 2013. If the camera's date and time had been set to UTC, you would need to adjust for local time. In September, Sante Fe's local time is mountain daylight saving (MDT), which is -6 hours from UTC time. So the actual local time might be 7:09 p.m. MDT. Because 7:09 p.m. is early evening, you should determine when sunset occurred on that date by using online tools, such as Time and Date (www.timeanddate.com/worldclock/sunrise.html) or SunriseSunset (www.sunrisesunset.com/sun.html). The Time and Date Web site shows that sunset for this location and time happened at 7:18 p.m. If the camera is set to 7:09 p.m. local time, you might assume sunlight would cast long shadows. Because the shadows look short, the date and time might not be accurate. In addition, if latitude and longitude values are available in the Exif file,

you could approximate the time of day based on the length and angle of shadows to the sun. Of course, this calculation applies only to photos taken outside on sunny days.

Understanding Data Compression

Most graphics file formats, including GIF and JPEG, compress data to save disk space and reduce the file's transmission time. Other formats, such as BMP, rarely compress data or do so inefficiently. In this case, you can use compression tools to compact data and reduce file size. **Data compression** is the process of coding data from a larger form to a smaller form. Graphics files and most compression tools use one of two data compression schemes: lossless or lossy. You need to understand how compression schemes work to know what happens when an image is altered.

Lossless and Lossy Compression

This section describes how lossless and lossy compression work, explains their advantages and disadvantages, and discusses what they mean in terms of digital forensics.

Lossless compression techniques reduce file size without removing data. When you uncompress a file that uses lossless compression, you restore all its information. GIF and Portable Network Graphics (PNG) file formats reduce file size with lossless compression, which saves file space by using mathematical formulas to represent data in a file. These formulas generally use one of two algorithms: Huffman or Lempel-Ziv-Welch (LZW) coding. Each algorithm uses a code to represent redundant bits of data. For example, if a graphics file contains a large red area, the algorithm can set 1 byte to red and set another byte to specify 200 red bytes instead of having to store 200 red bytes. Therefore, only 2 bytes are used.

Lossy compression is much different because it compresses data by permanently discarding bits of information in the file. Some discarded bits are redundant, but others are not. When you uncompress a graphics file that uses lossy compression, you lose information, although most people don't notice the difference unless they print the image on a high-resolution printer or increase the image size. In either case, the removed bits of information reduce image quality. The JPEG format is one that uses lossy compression. If you open a JPEG file in a graphics program, for example, and save it as a JPEG file with a different name, lossy compression is reapplied automatically, which removes more bits of data and, therefore, reduces image quality. If you simply rename a file by using File Explorer or the command line, however, the file doesn't lose any more data.

Another form of lossy compression, **vector quantization (VQ)** , uses complex algorithms to determine what data to discard based on vectors in the graphics file. In simple terms, VQ discards bits in much the same way rounding off decimal values discards numbers.

Some widely used lossless compression utilities include WinZip, PKZip, Stuffit, and FreeZip. Lzip is a lossy compression utility. You use compression tools to compact folders and files for data storage and transmission. Remember that the difference between lossless and lossy compression is the way data is represented after it has been uncompressed. Lossless compression produces an exact replica of the original data after it has been uncompressed; lossy compression typically produces an altered replica of the data.

Locating and Recovering Graphics Files

In a digital forensics investigation involving graphics files, you need to locate and recover all graphics files on the suspect drive and determine which ones are pertinent to your case. Because images aren't always stored in standard graphics file formats, you should examine all files your forensics tools find, even if they aren't identified as graphics files.

Some OSs have built-in tools for recovering graphics files, but they're time consuming, and the results are difficult to verify. Instead, you can use digital forensics tools dedicated to analyzing graphics files. As you work with these tools and built-in OS tools, develop standard procedures

for your organization and continue to refine them so that other investigators can benefit from your experience. You should also follow standard procedures for each case to make sure your analysis is thorough.

As discussed earlier in "**Examining the Exchangeable Image File Format**," you can use digital forensics tools to analyze images based on information in graphics files. Each graphics file contains a header with instructions for displaying the image; this header information helps you identify the file format. The header is complex and difficult to remember, however; instead of memorizing header information, you can compare a known good file header with that of a suspected file. For example, if you find an image that you suspect is a JPEG file but can't display it with a bitmap graphics program, compare its file header with a known JPEG file header to determine whether the header has been altered. You could then use the information in the known JPEG file header to supply instructions for displaying the image. In other words, you use the known JPEG header information to create a baseline analysis.

Before you can examine a graphics file header, often you need to reconstruct a fragmented graphics file. To do so, you need to identify the data patterns the graphics file uses. If part of the file header has been overwritten with other data, you might also need to repair the damaged header. By rebuilding the file header, you can then perform a forensics analysis on the graphics file. These techniques are described in the following sections.

Identifying Graphics File Fragments

If a graphics file is fragmented across areas on a disk, you must recover all the fragments before re-creating the file. Recovering any type of file fragments is called **carving** , also known as **salvaging** outside North America. To carve a graphics file's data from file slack space and free space, you should be familiar with the data patterns of known graphics file types. Many digital forensics programs, such as X-Ways Forensics, OSForensics, EnCase, and FTK, can recognize these data patterns and carve the graphics files from slack and free space automatically, however. After you recover fragments of a graphics file, you restore them to continue your examination. You use Autopsy and WinHex later in this chapter to copy known data patterns from files you recover, and then restore this information to view the graphics file.

Repairing Damaged Headers

When you're examining recovered fragments from files in slack or free space, you might find data that appears to be a header for a common graphics file type. If you locate header data that's partially overwritten, you must reconstruct the header to make it readable by comparing the hexadecimal values of known graphics file formats with the pattern of the file header you found.

Each graphics file type has a unique header value. As you become familiar with these header values, you can spot data from partially overwritten headers in file slack or free space. For example, a JPEG file has the hexadecimal header value FFD8, followed by the label JFIF for a standard JPEG or Exif file at offset 6.

Suppose you're investigating a possible intellectual property theft by a new employee of Superior Bicycles, Inc. This employee, Tom Johnson, is the cousin of Jim Shu, an employee who had been terminated. Bob Aspen is an external contractor and investor who gets a strange e-mail from Terry Sadler about Jim Shu's new project, as shown in **Figure 8-5**. Bob forwards the e-mail to Chris Robinson (the president of Superior Bicycles) to inquire about any special projects that might need capital investments. Chris forwards the e-mail to the general counsel, Ralph Benson, asking him to look into it. He also forwards it to Bob Swartz, asking him to have IT look for any e-mails with attachments. After a little investigation, Bob Swartz forwards an e-mail IT found with the subject "You might be interested" to Chris Robinson (see Figure 8-6).

Figure 8-5.

Chris Robinson

From: Bob Aspen <b_aspen@aol.com>
Sent: Monday, July 10, 2017 3:32 PM
To: cr-superior@outlook.com
Subject: FW: More info

Chris,
I got cc'd this odd message from Terry Sadler.
Do you have any projects that might need some capital investment?
Bob

-----Original Message-----
From: Terry Sadler [mailto:t_sadler@zoho.com]
Sent: Monday, July 10, 2017 3:28 PM
To: Jim Shu
Subject: Re: More info

Do you have a name for the project?

On 7/10/2017 3:04 PM, Jim Shu wrote:
> Terry,
>
> Here a few more photos from Tom.
>
> How much you willing to pay for these?
>
> Jim
>

An e-mail from Terry Sadler

Figure 8-6.

Chris Robinson

From: Tom Johnson <1060waddisonst@gmx.us>
Sent: Monday, July 10, 2017 2:40 PM
To: Jim Shu
Subject: You might be interested

Jim,

I had a tour of the new kayak factory. I think we can run with this to the other party interested in competing. I smuggled these files out, they are JPEG files I edited with my hex editor so that the email monitor won't pick up on them. So to view them you have to re-edit each file to the proper JPEG header of offset 0x FF D8 FF E0 and offset 6 of 4A. Then you have to rename them to a .jpg extension to view them.

Tom

The e-mail with attachments IT found

For this examination, you need to search for all possible places data might be hidden. To do this, in the next section you use Autopsy's search function with hexadecimal search strings to look for known data.

Searching for and Carving Data from Unallocated Space

At this time, you have to think about what to look for in the e-mails and on the mail servers. You need to ask some basic questions and make some assumptions based on available information to proceed in your search for information.

The message from t_sadler@zoho.com is addressed to b_aspen@aol.com, which matches the contractor's name, Bob Aspen. Next, look at the time and date stamps in this message. The date and time are July 10, 2017 3:32 PM, and farther down is a header from Terry Sadler with a time and date stamp of July 10, 2017, 3:28 PM. Therefore, it seems Jim Shu sent the original message to the t_sadler@zoho.com account.

Now examine the second e-mail, which contains the following pieces of information:

- Jim Shu had a tour of the new kayak factory.
- Another party might be interested in competing in manufacturing kayaks.

- Jim Shu smuggled out JPEG photos he modified with a hexadecimal editor so that they wouldn't be detected by any Web or e-mail filters.
- Jim Shu provides instructions on how to reedit the digital photos and add the .jpg extension so that they can be viewed.

With these collected facts and your knowledge of JPEG file structures, you can use the steps in the following sections to determine whether these allegations are true.

Planning Your Examination

In the e-mail from Tom Johnson to Jim Shu, Tom states, "So to view them you have to re-edit each file to the proper JPEG header of offset 0x FF D8 FF E0 and offset 6 of 4A." From this statement, you can assume that any kayak photographs from the e-mail or on the drive contain unknown characters in the first four bytes and the sixth byte. Because this is all Tom said about the JPEG files, you need to assume that the seventh, eighth, and ninth bytes have the original correct information for the JPEG file.

In "**Examining the Exchangeable Image File Format**," you learned the difference between a standard JFIF JPEG and an Exif JPEG file: The JFIF format has 0x FFD8 FFE0 in the first four bytes, and the Exif format has 0x FFD8 FFE1. In the sixth byte, the JPEG label is listed as JFIF or Exif. In the second e-mail, Jim Shu mentions 0x FF D8 FF E0, which is a JFIF JPEG format. He also says to change the sixth byte to 0x 4A, which is the uppercase letter "J" in ASCII.

Because the files have been extracted from the mail server, you should be thorough in your examination and analysis. You need to search all sectors of the drive for deleted files, both allocated space (in case Bob didn't modify the files) and unallocated space. In the next section, you use Autopsy for Windows to search for and recover these JPEG files.

Searching for and Recovering Digital Photograph Evidence

In this section, you learn how to use Autopsy for Windows to search for and extract (recover) possible evidence of JPEG files from the USB drive the EMTS manager gave you. The search string to use for this examination is "FIF." Because it's part of the label name of the JFIF JPEG format, you might have several false hits if the USB drive contains several other JPEG files. These false hits, referred to as **false positives** , require examining each search hit to verify whether it's what you are looking for. In this activity, you see that Autopsy has an Exif parser.

Note

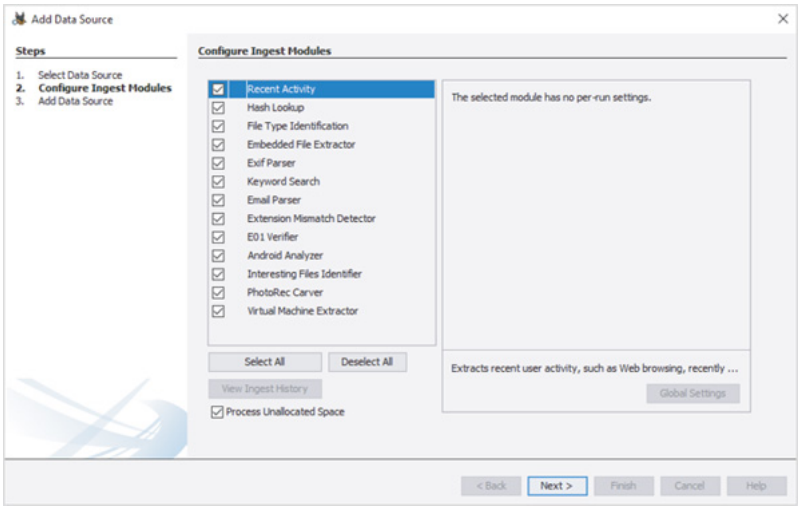
Before starting this activity, create the C:*Work*\Chap08\Chapter folder on your system (referred to as your "work folder" in steps). Then download the C08InChp.exe file in the downloads section for this chapter on the student companion site for this book. You should extract this file to your work folder.

To begin the examination, follow these steps to load the image file:

1. Start Autopsy for Windows, and click the **Create New Case** button. In the New Case Information window, type **C08InChp** for the case name, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**. In the Additional Information window, type **C08InChp** for the case number, enter your name for the examiner, and then click **Finish**.
2. In the Add Data Source window, leave the default selection **Disk Image or VM file** in the Type of Data Source to Add section, and then click **Next**.
3. In the Select Data Source window, click the **Browse** button, navigate to your work folder, click **C08InChp.dd** , and click **Open**. Then click **Next**.

4. In the Configure Ingest Modules window, you can select what type of processing you want, such as a hash lookup or an Exif parser (see **Figure 8-7**). Leave the default selections, click **Next**, and then click **Finish**.

Figure 8-7.

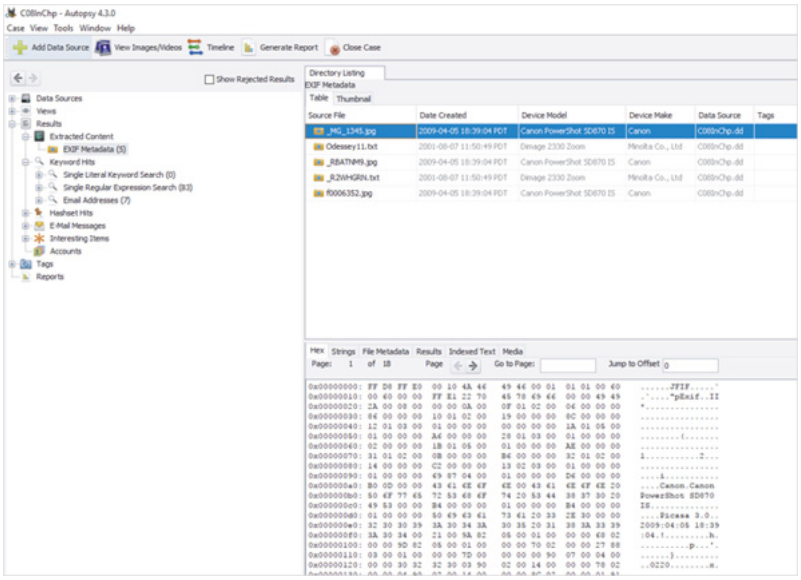


Source: www.sleuthkit.org

Processing options in the Configure Ingest Modules window

5. In the left pane of Autopsy's main window, click to expand **Extracted Content**, if necessary, and then click **EXIF Metadata**. Examine the files displayed in the upper-right pane (see Figure 8-8). As you scroll through these files, notice that the hexadecimal codes haven't been altered. (In the e-mail Tom Johnson sent, the JFIF code was supposedly altered.)

Figure 8-8.



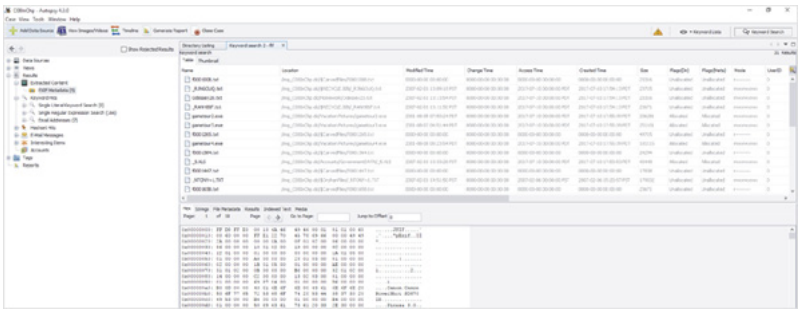
Source: www.sleuthkit.org

Parsing Exif metadata in Autopsy

6. Click the **Keyword Search** down arrow at the upper right. To verify that no other codes have been altered, you should check whether a change has been made to the FIF format. In the text box, type **FIF** (all uppercase letters), click the **Exact Match** option, and then click **Search**. There are no results. Next, type **fif** (all lowercase letters), click the

Substring Search option, and then click **Search**. Your results should be similar to what's shown in Figure 8-9.

Figure 8-9.



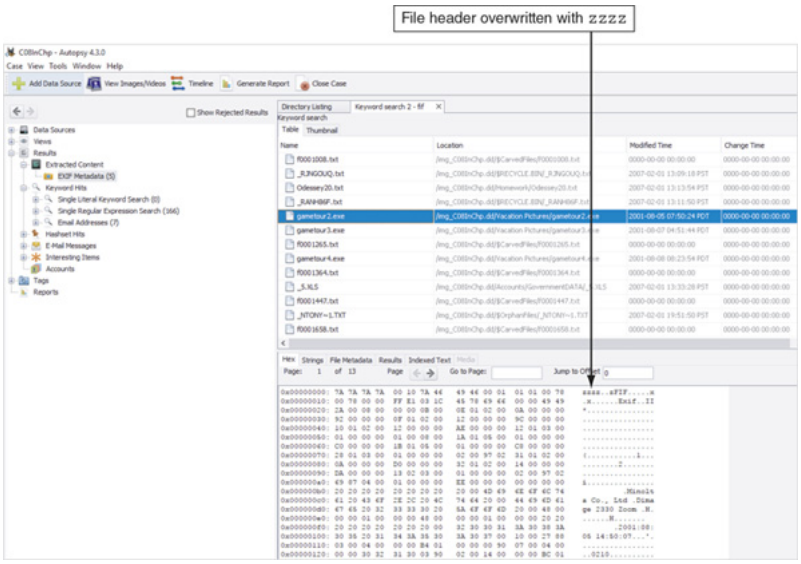
Source: www.sleuthkit.org

The results of searching for "fif"

Note

In **Figure 8-10**, the header for this JPEG file has been overwritten with zzzz. This unique header information might give you additional search values that could minimize false-positive hits in subsequent searches.

Figure 8-10.



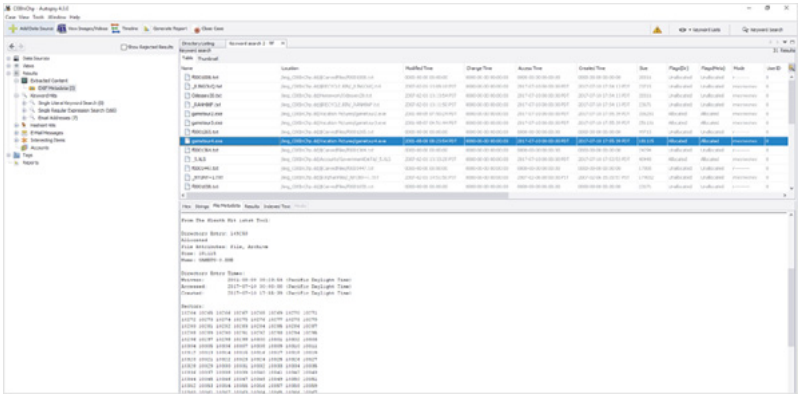
Source: www.sleuthkit.org

The altered file header

7. To view the changes made to the file header, you need to see the hexadecimal code. To do this, click the **Hex** tab in the lower-right pane, if necessary, and scroll down through the files until you see "zzzz" in the file header, as shown in Figure 8-10. You should be viewing the gametour2.exe file.

8. Click the **File Metadata** tab to view the written, accessed, and created dates and times along with the sectors used by the file (see Figure 8-11).

Figure 8-11.



Source: www.sleuthkit.org

Viewing all sectors used by the gametour2.exe file

9. In the search results, right-click the **gametour2.exe** file and click **Extract File(s)**. In the Save As dialog box, navigate to your work folder, type **Recover1.jpg** for the filename, and then click **Save**. Autopsy then creates an Export subfolder of your work folder to store this file. In the confirmation message box, click **OK**, and then exit Autopsy.

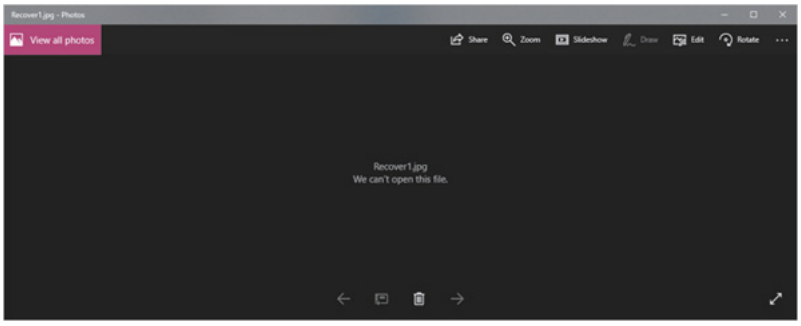
The next section shows you how to rebuild header data from this recovered file by using WinHex, although any hexadecimal editor has the capability to examine and repair damaged file headers. From a digital forensics view, this procedure can be considered corrupting the evidence, but knowing how to reconstruct data, as in the preceding example, is part of an investigator's job. When you change data as part of the recovery and analysis process, make sure you document each step as part of your reporting procedures. Your documentation should be detailed enough that other investigators could repeat the steps, which increases the credibility of your findings. When you're rebuilding a corrupted evidence image file, create a new file and leave the original file in its initial corrupt condition.

Rebuilding File Headers

Before attempting to edit a graphics file you have recovered, try to open it with an image viewer, such as the default Microsoft tool. To test whether you can view the image, double-click the recovered file in its current location in File Explorer. If you can open and view the image, you have recovered the graphics file successfully. If the image isn't displayed, you have to inspect and correct the header values manually.

If some of the data you recovered from the graphics file header is corrupt, you might need to recover more pieces of the file before you can view the image, as you'll see in the next section. Because the deleted file you recovered in the previous activity, Recoverl.jpg, was altered intentionally, you might see an error message similar to the one in Figure 8-12 when you attempt to open the file.

Figure 8-12.

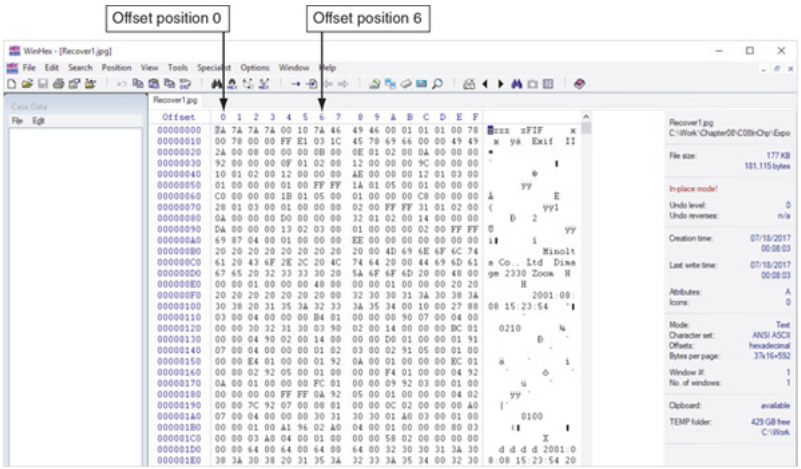


Error message indicating a damaged or an altered graphics file

If you can't open a graphics file in an image viewer, the next step is to examine the file's header data to see whether it matches the header in a good JPEG file. If the header doesn't match, you must insert the correct hexadecimal values manually with a hexadecimal editor. To inspect a file with WinHex, follow these steps:

1. Start WinHex, and click **File, Open** from the menu. Navigate to your work folder, and then double-click **Recover1.jpg** . If necessary, click **OK**. Figure 8-13 shows this file open in WinHex.

Figure 8-13.



Source: X-Ways AG, www.x-ways.net

Recover1.jpg open in WinHex

2. At the top of the WinHex window, notice that the hexadecimal values starting at the first byte position (offset 0) are 7A 7A 7A 7A, and the sixth position (offset 6) is also 7A. Leave WinHex open for the next activity.

As mentioned, a standard JFIF JPEG file has a header value of FF D8 FF E0 from offset 0 and the label name JFIF starting at offset 6. Using WinHex, you can correct this file header manually by following these steps:

1. In the center pane, click to the left of the first 7A hexadecimal value. Then type **FF D8 FF E0**, which are the correct hexadecimal values for the first 4 bytes of a JPEG file.
2. In the right pane at offset 6, click the **z**, and then type **J**, as shown in Figure 8-14.

Figure 8-14.

Source: X-Ways AG, www.x-ways.net

Inserting correct hexadecimal values for a JPEG file

Tip In WinHex, when you type a keyboard character in the right pane, the corresponding hexadecimal value appears in the center pane. So, for example, when you type J in the right pane, the hexadecimal value 4A appears in the center pane.

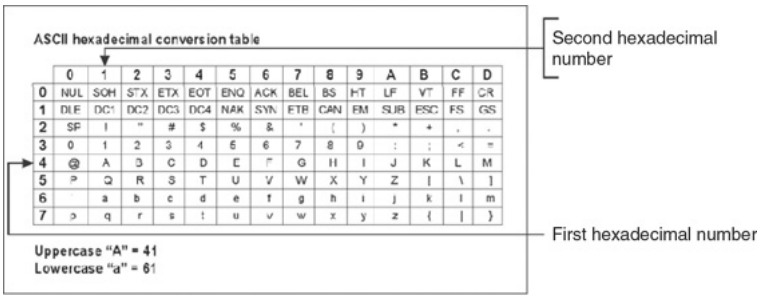
3. Click **File**, **Save As** from the menu. In the Save File As dialog box, navigate to your work folder, type **Fixed1.jpg** as the filename, and then click **Save**. If you're using the demo version of WinHex, you get an error message because of the file size. Exit WinHex.

Note

In WinHex Demo, you can save only up to 200 KB of data in a file.

Every two hexadecimal values you entered in the previous steps are equivalent to one ASCII character. For example, an uppercase "A" has the hexadecimal value 41, and a lowercase "a" has the hexadecimal value 61. Most disk editors have a reference chart for converting hexadecimal values to ASCII characters, such as in **Figure 8-15**.

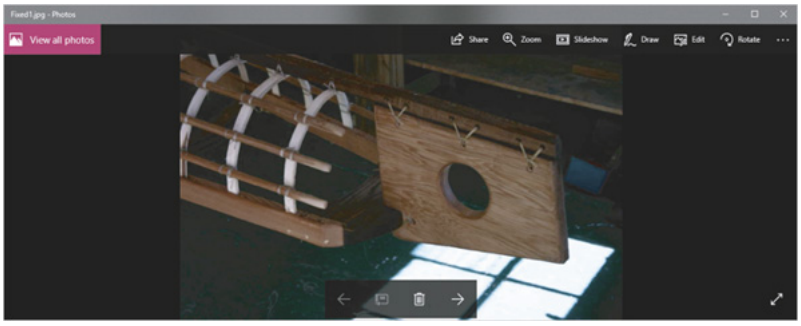
Figure 8-15.



ASCII equivalents of hexadecimal values

After you repair a graphics file header, you can test the updated file by opening it in an image viewer, such as Windows Photo Viewer, IrfanView, ThumbsPlus, QuickView, or ACDSee. If the file displays the image, as shown in **Figure 8-16**, you have performed the recovery correctly.

Figure 8-16.



Fixed1.jpg open in an image viewer

The process of repairing file headers isn't limited to JPEG files. You can apply the same technique to any file you can determine the header value for, including Microsoft Word, Excel, and PowerPoint documents and other image formats. You need to know only the correct header format for the type of file you're attempting to repair.

Reconstructing File Fragments

You might occasionally encounter corrupt data that prevents you from recovering data fragments for files. Whether the data corruption is accidental or intentional, you need to know how to examine a suspect drive and extract possible data fragments to reconstruct files for evidentiary purposes. In this section, you learn how to locate noncontiguous clusters that make up a deleted file. Current digital forensics tools can typically follow the links between clusters for FAT and NTFS file systems. However, sometimes the pointer information in a FAT or an NTFS Master File Table (MFT) file doesn't list this information.

The JPEG file you recovered in the previous activity was fragmented into several clusters. The following activity shows you how to recover a fragmented graphics file on a suspect drive. To perform this data-carving task, you need to locate the starting and ending sectors for each fragmented group of sectors. Here's an overview of the procedure:

1. Locate and export all sectors of the fragmented file.
2. Determine the starting and ending cluster numbers for each fragmented group of sectors.
3. Copy each fragmented group of sectors in their correct sequence to a recovery file.
4. Rebuild the file's header to make it readable in a graphics viewer.
5. Add a .txt extension on all the copied sectors.

To view and rebuild a file, you use the techniques described previously in "Rebuilding File Headers." (Remember to save the updated recovered data with a .jpg extension.) You should notice that it's the same data that enabled you to re-create Fixed1.jpg. Other JPEG files with altered header information, such as gametour4.exe, can be recovered by using the same techniques. Because gametour4.exe is larger than 200 KB, you would have to extract its data into two separate files if you were using WinHex. Next, you would repair the first file containing the overwritten data of zzzz, such as fragment1.txt, and then combine the two files into one file. To combine them, you can use the DOS command type fragment2.txt >> fragment1.txt, and then use the DOS command ren to rename fragment1.txt as Fixed2.jpg. Another disk editor you can use is Hex Workshop (www.hexworkshop.com), which has a 30-day use policy for a demo version and no file size limits.

Identifying Unknown File Formats

With the continuing changes in technology and digital graphics, eventually you'll encounter graphics file formats you're not familiar with. In addition, suspects might use older systems with programs that create files in uncommon or obsolete file formats. Therefore, you must research both old and new file types. Knowing the purpose of each format and how it stores data is part of the investigation process.

The Internet is the best source for learning more about file formats and their extensions. You have already used the Webopedia site to research the TGA file format. You can also use a search engine to search for "file type" or "file format" and find the latest list of Web sites with information on file extensions. If you still can't find a specific file extension, try refining your search by entering the file extension along with the words "file format" in a search engine. One nonstandard graphics file format is XIF. To search for information on this file format, follow these steps:

1. Start your Web browser, and go to www.google.com.
2. Type **XIF file format** in the text box and press **Enter**.
3. Click a few links in the search results to learn more about this file format. When you're finished, exit your Web browser.

Nuance PaperPort is a scanning program that produces images in the XIF (also referred to as XIFF) format, which is derived from the TIF file format. (It's not related to the Exif format.) Older versions of PaperPort had a free viewer utility for XIF files, but you can also use Solvusoft FileViewPro (www.solvusoft.com/en/file-extensions/file-extension-xif/) to view these files.

The following sites have information to help you analyze file formats. Keep in mind that information on the Web changes frequently; use a search engine to find graphics file information if you can't access these Web sites:

- www.fileformat.info/format/all.htm
- http://extension.informer.com/
- www.martinreddy.net/gfx/

Analyzing Graphics File Headers

You should analyze graphics file headers when you find new or unique file types that forensics tools don't recognize. The simplest way to access a file header is to use a hexadecimal editor, such as WinHex. You can then record the hexadecimal values in the header and use them to define a file type.

For example, suppose you encounter an XIF file. Because this format is so old, not much information on it is available. If you need to look for hidden or deleted XIF files, you must build your own header search string. To do this, you need a hexadecimal editor, such as WinHex. To see the differences between XIF and TIF, viewing and comparing header values for these file formats is good practice.

TIF is a well-established file format for transmitting faxes and for use in printed publications. All TIF files start at offset 0 with hexadecimal 49 49 2A. These hexadecimal values translate to the letters "II" in ASCII. **Figure 8-17** shows a sample TIF file open in WinHex.

Figure 8-17.

TIF file headers start with hexadecimal 49 49 2A, equivalent to ASCII II

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	49	49	2A	00	6E	EE	05	00	80	0B	4B	2A	07	F8	06	0C	II* ní ▌ K* ø
00000010	00	84	42	20	C0	10	03	FA	18	00	85	C2	62	50	88	2C	▌B À ú ▌ÅbP▌,
00000020	2A	0F	12	88	C6	20	EF	F8	98	08	01	05	01	C2	63	D1	* ▌Æ ïø▌ ÅcÑ
00000030	A8	7C	4E	4D	24	88	45	E4	F2	89	5C	1A	39	2B	96	4C	¨|NM$▌Eäò▌\ 9+▌L
00000040	26	53	39	A4	A6	4B	35	9A	C6	67	13	59	1C	EE	7D	16	&S9¤¦K5▌Æg Y î}
00000050	9B	CC	27	51	27	E4	7C	06	FE	8F	BF	DF	70	87	EC	51	▌Ì'Q'ä| þ ¿ßp▌ìQ
00000060	FF	1C	01	80	C0	C0	00	15	56	3F	0E	86	BF	A9	00	60	ÿ ÀÀ V? ▌¿© `
00000070	48	28	00	FD	B0	00	1F	6F	CA	2D	6A	91	58	9B	42	00	H(ý° oÊ-j´X▌B
00000080	51	C0	10	06	38	04	7D	D3	40	36	B8	80	00	09	5F	B9	QÀ 8 }Ó@6,▌ _¹
00000090	D2	61	8F	E0	14	86	DA	05	B5	43	29	F1	C8	BB	F9	F5	Òa à ▌Ú µC)ñÈ»ùõ
000000A0	4B	84	51	41	00	4C	03	F9	FE	FA	C4	D2	00	A0	7C	03	K▌QA L ùþúÄÒ |
000000B0	E6	C3	05	8F	48	24	51	F0	04	86	29	26	00	D1	61	00	æÃ H$Qð ▌)& Ña

Source: X-Ways AG, www.x-ways.net

A TIF file open in WinHex

The first 3 bytes of an XIF file are the same as a TIF file, followed by other hexadecimal values that distinguish it from a TIF file (see **Figure 8-18**). As you can see, the XIF header starts with hexadecimal 49 49 2A and has an offset of 4 bytes of 5C 01 00 00 20 65 58 74 65 6E 64 65 64 20 03. (Some values have been cut off in this figure to conserve space.) With this information, you can configure your forensics tool to detect an XIF file header. For more information on XIF, go to www.fileformat.info/info/mimetype/image/vnd.xiff/index.htm or www.vincent-net.com/luc/papers/99isdm_document_talk.pdf.

Figure 8-18.

XIF file header ASCII equivalent shows the same beginning values as a TIF extension

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	49	49	2A	00	5C	01	00	00	20	65	58	74	65	6E	64	65	II* \ eXtende
00000010	64	20	03	00	05	00	01	00	34	00	00	00	02	00	40	00	d 4 @
00000020	00	00	03	00	00	00	00	00	05	00	00	00	00	00	04	00	
00000030	00	00	00	00	01	00	20	00	01	00	B4	00	00	00	00	00	
00000040	6F	00	41	75	74	68	6F	72	00	58	65	72	6F	78	00	43	o Author Xerox C
00000050	6F	72	70	00	00	44	61	74	65	00	4A	75	6C	00	32	31	orp Date Jul 21
00000060	20	31	39	39	39	00	43	6F	70	79	72	69	67	68	74	00	1999 Copyright
00000070	43	6F	70	79	72	69	67	68	74	00	28	43	29	00	31	39	Copyright (C) 19
00000080	39	35	2D	31	39	39	36	00	58	65	72	6F	78	00	43	6F	95-1996 Xerox Co
00000090	72	70	6F	72	61	74	69	6F	6E	2C	20	41	6C	6C	20	52	rporation, All R
000000A0	69	67	68	74	73	20	52	65	73	65	72	76	65	64	00	00	ights Reserved
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Source: X-Ways AG, www.x-ways.net

An XIF file open in WinHex

Tools for Viewing Images

Throughout this chapter, you have been learning about recognizing file formats, using compression techniques, salvaging header information, recovering graphics files, and saving your modifications. After you recover a graphics file, you can use an image viewer to open and view it. Several hundred image viewers are available that can read many graphics file formats, although no one viewer program can read every file format. Therefore, having many different viewer programs for investigations is best.

Many viewer utilities are freeware or shareware programs that can be used to view a wide range of graphics file formats. Most GUI forensics tools include image viewers that display only

common image formats, especially GIF and JPEG, which are often found in Internet-related investigations. For less common file formats, such as PCX, integrated viewers often simply identify the data as a graphics file or might not recognize the data at all. Being unable to view all formats can prevent you from finding critical evidence for a case. Be sure that you analyze, identify, and inspect every unknown file on a drive.

Note

With many forensics tools, you can open files with external viewers.

Understanding Steganography in Graphics Files

When you open some graphics files in an image viewer, they might not seem to contain information related to your investigation. However, someone might have hidden information inside the image by using a data-hiding technique called steganography (discussed in more detail in **Chapter 9**), which uses a host file to cover the contents of a secret message.

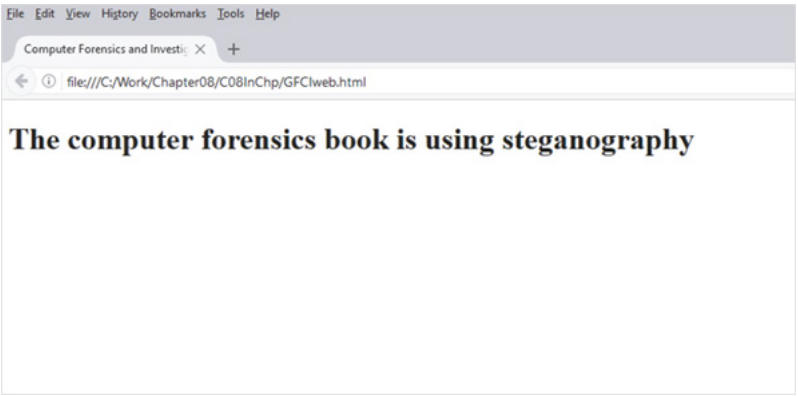
Steganography has been used since ancient times. Greek rulers used this technique to send covert messages to diplomats and troops via messengers. To hide messages, rulers shaved their messengers' heads and tattooed messages on their scalps. After the messengers' hair grew enough to cover the message, they left for their destinations, where they shaved their heads so that recipients could read the message. This method was a clever way to send and retrieve encrypted information, but it was inefficient because the messengers' hair took a long time to grow back, and only a limited amount of space was available to write messages. However, it enabled the Greeks to send secret messages until their enemies discovered this early form of steganography and began intercepting messengers.

Tip

Contemporary steganography has limits because a graphics file can hide only a certain amount of information before its size and structure change. However, it does allow someone to send covert information to a recipient, unless someone else detects the hidden data.

The two major forms of steganography are insertion and substitution. Insertion places data from the secret file into the host file. When you view the host file in its associated program, the inserted data is hidden unless you analyze the data structure carefully. For example, if you create a Web page with HTML, you can display images and text in a Web browser without revealing the HTML code. **Figure 8-19** shows a typical Web page intended to be viewed in a Web browser. It contains hidden text, which is shown in Figure 8-20 along with the source HTML code. To detect hidden text, you need to compare what the file displays and what the file contains. Depending on your skill level, this process can be difficult and time consuming.

Figure 8-19.



Source: Mozilla Corporation, www.mozilla.org

A simple Web page displayed in a Web browser

Figure 8-20.

Source: Mozilla Corporation, www.mozilla.org

The HTML code reveals hidden text

The second type of steganography, substitution, replaces bits of the host file with other bits of data. With a bitmap file, for example, you could replace bits used for pixels and colors with hidden data. To avoid detection, you substitute only those bits that result in the least amount of change.

For example, if you use an 8-bit graphics file, each pixel is represented by 8 bits of data containing information about the color each pixel displays onscreen. The bits are prioritized from left to right, such as 11101100. The first bit on the left is the **most significant bit (MSB)** , and the last bit on the right is the **least significant bit (LSB)** . As the names suggest, changing the MSB affects the pixel display more than changing the LSB does. Furthermore, you can usually change only the last two LSBs in an image without producing a noticeable change in the shade of color the pixel displays. To detect a change to the last two LSBs in a graphics file, you need to use a steganalysis tool, which is software designed to identify steganography techniques.

For example, if your secret message is converted to binary form to equal 01101100 and you want to embed this secret message into a picture, you alter the last 2 bits of four pixels. You break the binary form into sections of two, as in 01 10 11 00, and insert the bits into the last 2 bits of each pixel, as shown in **Table 8-1**.

Table 8-1. Bit Breakdown of a Secret Message

Original pixel	Altered pixel
1010 1010	1010 1001
1001 1101	1001 1110
1111 0000	1111 0011
0011 1111	0011 1100

The sequence of 2 bits is substituted for the last 2 bits of the pixel. This bit substitution can't be detected by the human eye, which can see only about 6 bits of color. **Figure 8-21** shows the original image on the left and the altered image on the right. The altered image contains the hidden message shown in Figure 8-22.

Figure 8-21.

Original and altered images

Figure 8-22.

```
My secret bank accounts:

Country        Bank                        Account No.    Passcode       Currency Amt.
Swiss          Swiss National SA           26845622       Y1115AQ        1.2 million CHF
Caymen Is.     Caribbean Intn. Bank Ltd.   5589999        SAMMM242       5.82 million KYD
Malta          Valletta Nat. Bank Limited  57896165       558TF558       2.3 million EUR
Hong Kong      Chan Wag Bank               A5AA59         665308888      8.9 million HKD
South Africa   Rand Bank of Cape Town      6982543        AAF8           0.53 million ZAL
```

A hidden message in the altered image

Whether insertion or substitution is used, you should inspect files for evidence of steganography, especially if your suspect is technically savvy or you see signs that steganography has been used. Clues to look for are duplicate files, such as images, with different hash values, or steganography programs installed on the suspect's drive.

Tip

Steganography can be used with file formats other than graphics files, such as MPEG and AVI files.

Using Steganalysis Tools

You can use several different steganalysis tools (also called "steg tools") to detect, decode, and record hidden data, even in files that have been renamed to protect their contents. A steganalysis tool can also detect variations of an image. If a graphics file has been renamed, a steganalysis tool can identify the file format from the file header and indicate whether the file contains an image. Although steganalysis tools can help identify hidden data, steganography is generally difficult to detect. In fact, if steganography is done correctly, in most cases you can't

detect the hidden data unless you can compare the altered file with the original file. Check to see whether the file size, image quality, or file extensions have changed. If so, you might be dealing with a steganography image. As an example of the difficulty of detecting the use of steganography, Niels Provos and Peter Honeyman at the University of Michigan conducted a study of more than two million images used in eBay auctions to see whether hidden data might have been placed in photos (see www2.sans.org/reading-room/whitepapers/stenganography/steganography-whats-real-risk-555). They were unable to determine whether any graphics files contained hidden messages.

Note

Steganography and steganalysis tools change as rapidly as some OSs. Current steg tools include Steg Suite from WetStone and Outguess StegDetect and StegBreak. For a list of other steg tools, do an Internet search on "steganography," "steganalysis," or "blind steganalysis."

Tip

For more information on steganography, read "Steganography: Hiding Data Within Data" at www.garykessler.net/library/steganography.html.

Understanding Copyright Issues with Graphics

Steganography has also been used to protect copyrighted material by inserting digital watermarks into a file. When working with graphics files, digital investigators need to be aware of copyright laws, especially in the corporate environment, where they often work closely with the legal department to guard against copyright violations. Investigators might also need to determine whether a photo is from a known copyrighted source, such as a news photo being posted on a Web page without permission.

The U.S. Copyright Office Web site defines precisely how copyright laws pertain to graphics (see www.copyright.gov for information on the 1976 Copyright Act). Copyright laws as they pertain to the Internet, however, aren't as clear. For example, a server in another country might host a Web site, which could mean it's regulated by copyright laws in that country. Because each country has its own copyright laws, enforcement can be difficult. Contrary to what some might believe, there's no international copyright law that applies to all countries, but there are international copyright treaties between several countries. Typically, enforcing international copyright treaties requires legal action in the country where the infringement occurred. For more information, see www.mondaq.com/unitedstates/x/171306/Copyright/International+Copyright+Protection+How+Does+It+Work or www.rightsdirect.com/international-copyright-basics/.

The U.S. Copyright Office (www.copyright.gov/circs/circ01.pdf) identifies what can and can't be covered under copyright law in the United States:

Copyright protects "original works of authorship" that are fixed in a tangible form of expression. The fixation need not be directly perceptible so long as it may be communicated with the aid of a machine or device. Copyrightable works include the following categories:

1. *literary works;*
2. *musical works, including any accompanying words;*
3. *dramatic works, including any accompanying music;*
4. *pantomimes and choreographic works;*

5. *pictorial, graphic, and sculptural works;*
6. *motion pictures and other audiovisual works;*
7. *sound recordings;*
8. *architectural works.*

These categories should be viewed broadly. For example, computer programs and most "compilations" may be registered as "literary works"; maps and architectural plans may be registered as "pictorial, graphic, and sculptural works."

Anything that would ordinarily be copyrighted through noncomputer means and is now being created on digital media is considered to be copyrighted, as long as the process for obtaining a copyright has been followed.

Digital watermarks can be visible or imperceptible in media such as digital photos and audio files. Visible watermarks are usually an image, such as the copyright symbol or a company logo, layered on top of a photo. Imperceptible watermarks don't change the appearance or sound quality of a copyrighted file. Methods used for imperceptible watermarks sometimes involve modifying a file's LSBs into a unique pattern.

Another guideline to consider is **fair use** . A short direct quote for news reporting or critiques is considered fair use, and the material's originator or owner doesn't have to be paid. Material used for noncommercial and educational purposes also falls under the fair use guideline. These distinctions can get complicated, however. For example, an instructor copying parts of a book to use as handouts in a class setting is operating within the fair use guideline. On the other hand, if the instructor sends the book to a printer to copy and pays the printer, a copyright violation has occurred because a commercial printer was paid to copy the book, even though the copies were to be used for educational purposes.

Chapter Summary

- A graphics file contains an image, such as a digital photo, line art, a three-dimensional image, or a scanned replica of a printed picture. A graphics program creates and saves one of three types of graphics files: bitmap, vector, and metafile. Bitmap images are collections of dots, or pixels, that form an image. Vector graphics are mathematical instructions that define lines, curves, text, and geometric shapes. Metafile graphics are combinations of bitmap and vector images.
- When you use a graphics editor or an image viewer, you can open a file in one of many graphics file formats. Each format has different qualities, including the amount of color and compression it uses. If you open a graphics file in a program that supports multiple file formats, you can save the file in a different file format. However, converting graphics files this way can change image quality.
- Bitmap images store graphics information as grids of pixels (short for "picture elements"). The quality of a bitmap image displayed onscreen is governed by resolution, which determines the amount of detail displayed. Vector graphics, unlike bitmap and raster files, use lines instead of dots. A vector graphic stores only the calculations for drawing lines and shapes; a graphics program converts these calculations into images. You can enlarge a vector graphic without affecting image quality. Metafile graphics combine bitmap and vector graphics and can have the characteristics of both image types.
- Most graphics editors enable you to create files in one or more of the standard graphics file formats, such as Graphic Interchange Format (.gif), Joint Photographic Experts Group (.jpeg or .jpg), Windows Bitmap (.bmp), and Tagged Image File Format (.tif or .tiff). Nonstandard graphics file formats include less common formats, such as Targa (.tga) and Raster Transfer Language (.rtl); proprietary formats, such as Photoshop (.psd); newer formats, such as Scalable Vector Graphics (.svg); and old or obsolete formats, such as Paintbrush (.pcx).
- Most graphics file formats, including GIF and JPEG, compress data to save disk space and reduce transmission time. Other formats, such as BMP, rarely compress data or do so inefficiently. You can use compression tools to compact data and reduce file size. Lossless compression saves file space by using mathematical formulas to represent data in a file. Lossy compression compresses data by permanently discarding bits of information in the file.
- Photos taken with digital cameras, smartphones, and other digital devices are typically in raw and Exif JPEG formats. The raw format is the proprietary format of a device's manufacturer. The Exif format is different from the standard JFIF JPEG format because it contains metadata about the device and picture, such as shutter speed and date and time a picture was taken.
- In a digital forensics investigation involving graphics files, you need to locate and recover all graphics files on a drive and determine which ones are pertinent to your case. Because these files aren't always stored in standard graphics file formats, you should examine all files your forensics tools find, even if they aren't identified as graphics files. A graphics file contains a header with instructions for displaying the image. Each type of graphics file has its own header that helps you identify the file format. Because the header is complex and difficult to remember, you can compare a known good file header with that of a suspect file.
- When you're examining recovered data remnants from files in slack or free space, you might find data that appears to be a header for a common graphics file type. If you locate header data that's partially overwritten, you must reconstruct the header to make it readable again by comparing the hexadecimal values of known graphics file formats to the

pattern of the file header you found. After you identify fragmented data, you can use a forensics tool to recover the fragmented file.

- If you can't open a graphics file in an image viewer, the next step is to examine the file header to see whether it matches the header in a known good file. If the header doesn't match, you must insert the correct hexadecimal values manually with a hex editor.
- The Internet is the best source for learning more about file formats and their extensions. You can search for "file type" or "file format" and find a list of Web sites with information on file extensions.
- You should analyze graphics file headers when you find new or unique file types that digital forensics tools don't recognize. The simplest way to do this is with a hex editor. You can record the hexadecimal values in the header for future reference.
- Many viewer utilities are freeware or shareware and enable you to view a wide range of graphics file formats. Most GUI forensics tools include image viewers that display common image formats, especially GIF and JPEG.
- Steganography is a method of hiding data by using a host file to cover the contents of a secret message. The two major techniques are insertion and substitution. Insertion places data from the secret file into the host file. When you view the host file in its associated program, the inserted data is hidden unless you analyze the data structure. Substitution replaces bits of the host file with other bits of data.
- Steganalysis tools can detect hidden data in graphics files, even in files that have been renamed to protect their contents. If the file has been renamed, steganalysis tools can use the file header to identify the file format and indicate whether the file contains an image. Steganalysis tools can also detect variations in a graphics file.
- Copyright law in the United States protects literary works, musical works, motion pictures, sound recordings and graphics. On the Internet, however, artists should take additional precautions. There's no "international" copyright law, so laws vary from country to country. There are, however, treaties and conventions that protect works on an international scale.
- Fair use allows using copyrighted material for noncommercial or educational purposes without having to compensate the material's originator or owner.

Key Terms

bitmap images
carving
data compression
demosaicing
Exchangeable Image File (Exif)
fair use
false positives
least significant bit (LSB)
lossless compression
lossy compression
metafile graphics
most significant bit (MSB)
nonstandard graphics file formats
pixels

raster images
raw file format
resolution
salvaging
standard graphics file formats
vector graphics
vector quantization (VQ)

Review Questions

1. Graphics files stored on a computer can't be recovered after they are deleted. True or False?

2. When you carve a graphics file, recovering the image depends on which of the following skills?

   a. Recovering the image from a tape backup

   b. Recognizing the pattern of the data content

   c. Recognizing the pattern of the file header content

   d. Recognizing the pattern of a corrupt file

3. Explain how to identify an unknown graphics file format that your digital forensics tool doesn't recognize.

4. What type of compression uses an algorithm that allows viewing the graphics file without losing any portion of the data?

5. When investigating graphics files, you should convert them into one standard format. True or False?

6. Digital pictures use data compression to accomplish which of the following goals? (Choose all that apply.)

   a. Save space on a hard drive.

   b. Provide a crisp and clear image.

   c. Eliminate redundant data.

   d. Produce a file that can be e-mailed or posted on the Internet.

7. The process of converting raw images to another format is called which of the following?

   a. Data conversion

   b. Transmogrification

   c. Transfiguring

   d. Demosaicing

8. In JPEG files, what's the starting offset position for the JFIF label?

   a. Offset 0

   b. Offset 2

   c. Offset 6

   d. Offset 4

9. Each type of graphics file has a unique header containing information that distinguishes it from other types of graphics files. True or False?

10. Copyright laws don't apply to Web sites. True or False?

11. When viewing a file header, you need to include hexadecimal information to view the image. True or False?

12. When recovering a file with ProDiscover, your first objective is to recover cluster values. True or False?

13. Bitmap (.bmp) files use which of the following types of compression?

    a. WinZip

    b. Lossy

    c. Lzip

    d. Lossless

14. A JPEG file uses which type of compression?

    a. WinZip

    b. Lossy

    c. Lzip

    d. Lossless

15. Only one file format can compress graphics files. True or False?

16. A JPEG file is an example of a vector graphic. True or False?

17. Which of the following is true about JPEG and TIF files?

    a. They have identical values for the first 2 bytes of their file headers.

    b. They have different values for the first 2 bytes of their file headers.

    c. They differ from other graphics files because their file headers contain more bits.

    d. They differ from other graphics files because their file headers contain fewer bits.

18. What methods do steganography programs use to hide data in graphics files? (Choose all that apply.)

    a. Insertion

    b. Substitution

    c. Masking

    d. Carving

19. Some clues left on a drive that might indicate steganography include which of the following? (Choose all that apply.)

    a. Multiple copies of a graphics file

    b. Graphics files with the same name but different file sizes

    c. Steganography programs in the suspect's All Programs list

    d. Graphics files with different timestamps

20. What methods are used for digital watermarking? (Choose all that apply.)

    a. Implanted subroutines that link to a central Web server automatically when the watermarked file is accessed

    b. Invisible modification of the LSBs in the file

    c. Layering visible symbols on top of the image

    d. Using a hex editor to alter the image data

Hands-On Projects

Create the C:*Work*\Chap08\Projects folder on your system before starting these projects. If necessary, copy all data files from the downloads section for this chapter (on the student companion site for this book) to your work folder.

Hands-On Project 8-1.

In this project, you use Autopsy for Windows to locate and extract JPEG files with altered extensions. Some of these files are embedded in files with non-JPEG extensions. Find the C08frag.dd file in your work folder, and then follow these steps:

1. Start Autopsy for Windows, and click the **Create New Case** button. In the New Case Information window, type **C08frag** in the Case Name text box, and click **Next**. Enter **C08Frag** for the case number and your name as the examiner, and then click **Finish**.
2. In Add Data Source window, click **Disk Image or VM file** in the Select Type of Data Source to Add section, if necessary, and then click **Next**. In the Select Data Source window, click the **Browse** button. In the Open dialog box, navigate to your work folder, and click **C08frag.dd** . Click **Open**, and then click **Next**. Accept all the default selections in the Configure Ingest Modules window, and click **Next** and then **Finish**.
3. Click the **Keyword Search** down arrow at the upper right. Type **jfif** in the text box, click the **Substring Match** option, and then click **Search**.
4. Click each file in the search results that doesn't have a .jpg extension. Then examine the contents of each file to find any occurrences of a JFIF label. Right-click a file with a JFIF label, point to **Tag Files**, and click **Tag and Comment**. In the Comment text box, type **Recovered hidden .jpg file**, and then click **OK**. Repeat this procedure for each file with a JFIF label.
5. Click **Generate Report**. Click the **Results - HTML** option button for the report format, and then click **Next**. Click **All Results**, and then click **Finish**. Click the report link, and examine your report in the browser window that opens.
6. Exit Autopsy for Windows, saving your project when prompted.

Hands-On Project 8-2.

In this project, you continue examining the files found by IT staff at Superior Bicycles. In the in-chapter activity, you recovered three files containing zzzz for the first 4 bytes of altered JPEG files. These altered files had different extensions to hide the fact that they're graphics files.

Find the C08carve.dd file in your work folder. This image file is a new drive acquisition the IT staff made. The CEO wants to know whether any similar files on this drive match the files you recovered from the first USB drive. Because you know that the files you recovered earlier have zzzz for the first 4 bytes, you can use it as your search string to see whether similar files are on this drive.

1. Start Autopsy for Windows, and click the **Create New Case** button. In the New Case Information window, type **C08carve** in the Case Name text box, and click **Next**. In the Additional Information window, type the date in the Case Number text box and your name in the Examiner text box. Click **Finish.**
2. In the Select Data Source window, click the **Browse** button, navigate to your work folder, click **c08carve.dd** , and then click **Open**. Then click **Next**.
3. Next, click the **Keyword Search** down arrow. In the text box, type **zzzz**, click the **Exact Match** option button, and then click **Search**.
4. Click each file in the search results to display its contents. If the file contains zzzz at the beginning of the sector, right-click the file, point to **Tag Files**, and click **Tag and**

Comment. In the Comment text box, type **Similar file**, and then click **OK**.

5. Click the **gametour5.exe** file. Ctrl+click to select **gametour1.exe** , **gametour2.exe** , **gametour3.exe** , **gametour4.exe** , and **gametour6.exe** . Right-click the selection, point to **Tag Files**, and click **Tag and Comment**. In the Comment text box, type **Additional similar files**, and then click **OK**.

6. Click **Generate Report**. Click the **Results - HTML** option button, and then click **Next**. Click **All Results**, and then click **Finish**. Examine the results in the browser window, and then exit Autopsy.

Hands-On Project 8-3.

In this project, you use IrfanView to open graphics files and save them in a compressed graphics format different from the original format. You should note any changes in image quality after converting files to a different format. Download IrfanView from www.irfanview.com and install it, and then follow these steps:

1. Start IrfanView. Click **File, Open** from the menu. In the Open dialog box, navigate to your work folder, and then double-click **SPIDER.bmp** to open the file.
2. Click **File, Save as** from the menu. Change the file type to **JPG** and save the file as **Spider.jpg** in the same location.
3. Save Spider.jpg as **Spider2.bmp** in the same location.
4. Open these three graphics files in new sessions of IrfanView and compare the files. Document any changes you notice.
5. Open **FLOWER.gif** from your work folder, and save it as **Flower.jpg** in the same location.

Tip

If your screen is cluttered with too many open IrfanView windows, close a few that you're no longer working with.

6. Save Flower.jpg as **Flower2.gif** in the same location.
7. Open these three graphics files in new sessions of IrfanView, and document any changes you see when comparing the files.
8. Open **Cartoon.bmp** from your work folder, and save it as **Cartoon.gif** in the same location.
9. Save Cartoon.gif as **Cartoon2.bmp** in the same location.
10. Open these three graphics files in new sessions of IrfanView, and document any changes you see when comparing the files.
11. Exit all instances of IrfanView. Summarize your conclusions in a brief report and submit it to your instructor.

Hands-On Project 8-4.

In this project, you use S-Tools4 to create a steganography file for hiding an image. Download S-Tools4 from http://packetstormsecurity.com/files/21688/s-tools4.zip.html or www.4shared.com/zip/q764vcPu/s-tools4.htm, install the program, and then follow these steps:

1. In File Explorer, navigate to where you installed S-Tools4, and start the program by double-clicking **S-Tools.exe** . If necessary, click **Run**, and then click **Continue**, if

necessary.

2. Drag **RUSHMORE.bmp** from your work folder to the S-Tools window.
3. To hide text in the RUSHMORE.bmp file, drag **Findme.txt** from your work folder to the **RUSHMORE.bmp** image.
4. In the Hiding dialog box, type **FREEDOM** in the Passphrase and Verify passphrase text boxes, and then click **OK**. A hidden data window opens in the S-Tools window.
5. Right-click the hidden data window and click **Save as**. Save the image as **Steg.bmp** in your work folder.
6. Close the Steg.bmp and RUSHMORE.bmp windows, but leave S-Tools open for the next project.

Hands-On Project 8-5.

In this project, you use S-Tools4 to create a secret message in a bitmap file and compare this steganography file with the original file by using the DOS comp command. You need S-Tools4 and the Mission.bmp and USDECINP.rtf files in your work folder. First, follow these steps to create a steganography file:

1. If you have exited S-Tools4, start it by double-clicking **S-Tools.exe** in File Explorer.
2. Drag **Mission.bmp** from your work folder to the S-Tools window.
3. Next, drag **USDECINP.rtf** from your work folder to the **Mission.bmp** image.
4. Type **hop08-5** in the Passphrase and Verify passphrase text boxes, and then click **OK**. A hidden data window opens in the S-Tools window.
5. Right-click the hidden data window and click **Save as**. Save the image as **Mission-steg.bmp** in your work folder. Exit S-Tools.

Next, you use the DOS comp command to compare these two files and redirect the output to a text file for further analysis:

1. To open a command prompt window in Windows, click the **Search** icon, type **cmd**, and then press **Enter**. (In earlier Windows versions, you can click **Start**, type **cmd** in the "Search for programs and files" text box, and then press **Enter**.)
2. Change to your work folder by typing **cd \ *Work* \Chap08\Projects** (substituting the path to your work folder) and pressing **Enter**.
3. Type **comp Mission.bmp Mission-steg.bmp > Mission-compare.txt** and press **Enter**, and then at the Compare more files (Y/N) ? prompt, type **n** and press **Enter**.
4. In File Explorer, navigate to your work folder, and open the **Mission-compare.txt** file to see what discrepancies were found. When you're finished, close the file, and exit the command prompt window by typing **exit** and pressing **Enter**.
5. To complete this project, write a one-page report on the number of mismatches and the deviation in each mismatch between the two files. In addition, state your observations of the differences in the two files, such as hexadecimal values and their patterns.

Case Projects

Case Projects 8-1.

Do an Internet search to find current steganography tools. Create a spreadsheet listing at least five steganography tools and their features. The spreadsheet should have the following columns: name of tool, vendor (with URL for purchasing or downloading the tool), cost (or note that it's freeware, if applicable), file formats of data that can be hidden, and Web site.

Case Project 8-2.

You're investigating a case involving an employee who's allegedly sending inappropriate photos via e-mail in attachments that have been compressed with a zip utility. As you examine the employee's hard disk, you find a file named Orkty.zip, which you suspect is a graphics file. When you try to open the file in an image viewer, a message is displayed indicating that the file is corrupt. Write a two- to three-page report explaining how to recover Orkty.zip for further investigation.

Case Project 8-3.

You work for a mid-size corporation known for its inventions that does a lot of copyright and patent work. You're investigating an employee suspected of selling and distributing animations created for your corporation. During your investigation of the suspect's drive, you find some files with the unfamiliar extension .xde. The network administrator mentions that other .xde files have been sent through an FTP server to another site. Describe your findings after conducting an Internet search for this file extension.

Chapter 9. Digital Forensics Analysis and Validation

After reading this chapter and completing the exercises, you will be able to:

- Determine what data to analyze in a digital forensics investigation
- Explain tools used to validate data
- Explain common data-hiding techniques

This chapter explains how to apply your forensics skills and techniques to a digital investigation. One of the most critical functions is validating evidence during the analysis process. In **Chapter 3**, you learned how data acquisitions are validated for Windows and Linux file systems; in Chapter 4, you were introduced to hashing algorithms; and in Chapter 6 you learned about validating forensics software tools. In this chapter, you learn more about using hashing algorithms in forensics analysis to validate data. You also learn how to refine and modify an investigation plan, use data analysis tools and practices to process digital evidence, determine whether data-hiding techniques have been used, and learn methods for performing a remote acquisition.

Determining What Data to Collect and Analyze

Examining and analyzing digital evidence depend on the nature of the investigation and the amount of data to process. Criminal investigations are limited to finding data defined in the search warrant, and civil investigations are often limited by court orders for discovery. Private-sector investigators might be searching for company policy violations that require examining only specific items, such as e-mail. Therefore, investigations often involve locating and recovering a few specific items, which simplifies and speeds processing.

In a private-sector environment, however, especially if litigation is involved or anticipated, the company attorney often directs the investigator to recover as much information as possible. Satisfying this demand becomes a major undertaking with many hours of tedious work. These types of investigations can also result in **scope creep** , in which an investigation expands beyond the original description because of unexpected evidence you find, prompting the attorney to ask you to examine other areas to recover more evidence. Scope creep increases the time and resources needed to extract, analyze, and present evidence. Be sure to document any requests for additional investigation, in case you must explain why the investigation took longer than planned, why the scope widened during the course of the investigation, and so forth.

One reason scope creep has become more common is that criminal investigations increasingly require more detailed examination of evidence just before trial to help prosecutors fend off attacks from defense attorneys. Because defense attorneys typically have the right of full discovery of digital evidence used against their clients, it's possible for new evidence to come to light while complying with the defense request for full discovery. However, this new evidence often isn't revealed to the prosecution; instead, the defense uses it to defend the accused. For this reason, it's become more important for prosecution teams to ensure that they have analyzed the evidence exhaustively before trial. (Note that the defense request for full discovery applies only to criminal cases in the United States; civil cases are handled differently.)

Approaching Digital Forensics Cases

Recall from **Chapter 1** that you begin a digital forensics case by creating an investigation plan that defines the investigation's goal and scope, the materials needed, and the tasks to perform. Although some basic principles apply to almost all digital forensics cases, the approach you take depends largely on the type of case you're investigating.

For example, gathering evidence for an e-mail harassment case might involve little more than accessing network logs and e-mail server backups to locate specific messages. Your approach,

however, depends on whether the case is an internal organizational investigation or a civil or criminal investigation carried out by law enforcement. In an internal investigation, evidence collection tends to be fairly easy and straightforward because private-sector investigators usually have ready access to the necessary records and files. In contrast, when investigating a criminal cyberstalking case, you need to contact the ISP and e-mail service. Some companies have systems set up to handle these situations, but others do not. Most organizations don't keep e-mail for longer than 90 days, and many keep it for far less time.

An investigation of an employee suspected of industrial espionage can require the most work. Before initiating this type of investigation, make sure the organization, whether it's a private company or a public agency, has set up rules of use and limitations of privacy rights, as described in **Chapter 1**. For these investigations, you might need to set up a surveillance camera to monitor the employee's activities in the office. You might also need to plant a software or hardware keylogger (for capturing keystrokes remotely), and you need to engage the network administrator's services to monitor Internet and network activities. In this situation, you might want to do a remote acquisition of the employee's drive, and then use another tool to determine what peripheral devices have been accessed.

As a standard practice, you should follow these basic steps for all digital forensics investigations:

Note

For more information on basic processes and recommendations, refer to **Chapter 2** for guidelines on setting up a forensic workstation.

1. For target drives, IACIS recommends using recently wiped media that have been reformatted and inspected for viruses. At the very least, media should be inspected and cleared of any possible malware before using them on a case. With advanced digital forensics tools that can access network storage media, apply standard network security practices, such as access restrictions (through an access control list), securely configured routers, and a firewall. With disk-to-disk forensic copying, the original drive reformats the target drive to the same configuration. If you need to wipe media, you can use several different tools, such as X-Ways Security, Digital Intelligence PDWipe, or WhiteCanyon SecureClean, to clean all data from the target media.

Note Some commercial tools can wipe only up to 2 TB. An alternative wiping method that has no limits is the Linux dd command's zero option. If your forensic workstation is a Windows system, boot a Linux Live CD as described in Chapter 7. Open a terminal window, identify the drive you want to wipe clean, enter the command sudo dd if=/dev/zero of=/dev/sdb, and press Enter. Use caution when selecting the of device drive; make sure you're wiping the correct drive.

2. Inventory the hardware on the suspect's computer, and note the condition of the computer when seized. Document all physical hardware components as part of your evidence acquisition process.

3. For static acquisitions, remove the original drive from the computer, if practical, and then check the date and time values in the system's CMOS.

4. Record how you acquired data from the suspect drive—note, for example, that you created a bit-stream image and which tool you used. The tool you use should also create an MD5 or SHA-1 hash for validating the image.

5.

When examining the image of the drive's contents, process the data methodically and logically.

6. List all folders and files on the image or drive. For example, Autopsy and other forensics tools can generate lists of all files and folders on a suspect's drive in Excel, HTML, and other data file formats. Note where specific evidence is found, and indicate how it's related to the investigation.

7. If possible, examine the contents of all data files in all folders, starting at the root directory of the volume partition. The exception is for cases with the defined scope of work stated in a search warrant or discovery demand. For these cases, you look for only the specific items listed in the warrant or discovery demand.

8. For all password-protected files that might be related to the investigation, make your best effort to recover file contents. You can use password-recovery tools for this purpose, such as OSForensics Password Recovery and Decryption, AccessData Password Recovery Toolkit (PRTK), or Passware Kit Enterprise.

9. Identify the function of every executable (binary or .exe) file that doesn't match known hash values. Make note of any system files or folders, such as the System32 folder or its content, that are out of place. If you can't find information on an executable file by using a disk editor, examine the file to see what it does and how it works.

10. Maintain control of all evidence and findings, and document everything as you progress through your examination.

Refining and Modifying the Investigation Plan

In civil and criminal cases, the scope is often defined by search warrants or subpoenas, which specify what data you can recover. However, private-sector cases, such as employee abuse investigations, might not specify limitations in recovering data. For these cases, it's important to refine the investigation plan as much as possible by trying to determine what the case requires. Generally, you want the investigation to be broad enough to encompass all relevant evidence yet not so wide-ranging that you waste time and resources analyzing data that's not going to help your case.

Of course, even if your initial plan is sound, at times you'll find you need to deviate from it and follow where the evidence leads you. Even in these cases, having a plan you revise deliberately along the way is much better than searching for evidence haphazardly.

Suppose, for example, an employee is accused of operating an online business using company resources during work hours. You use this timeframe to narrow the set of data you're searching, and because you're looking for unauthorized Internet use, you focus the search on temporary Internet files, Internet history, and e-mail communication. Knowing the types of data you're looking for at the outset helps you make the best use of your time and prevents you from casting too wide a net. However, in the course of reviewing e-mails related to the case, you might find references to spreadsheets or Word documents containing financial information related to the online business. In this case, it makes sense to broaden the range of data you're looking for to include these types of files. Again, the key is to start with a plan but remain flexible in the face of new evidence.

Using Autopsy to Validate Data

In previous chapters, you have used Autopsy for Windows, which can perform forensics analysis on the following file systems:

- Microsoft FAT, NTFS, ExFAT, UFS1, and UFS2
- ISO 9660 and YAFFS2
- Mac HFS+ and HFSX

- Linux Ext2fs, Ext3fs, and Ext4fs

In addition, it can analyze data from several sources, including image files from other vendors. Autopsy can handle many formats, including raw, Expert Witness, and virtual machine image files (.vdi and .vhd).

To enhance searching for and eliminating known OS and application files, Autopsy has an indexed version of the NIST National Software Reference Library (NSRL) of MD5 hashes, and you can import NSRL reference hashes into Autopsy. For more information on the NSRL, see **Chapter 6** or visit www.nsrl.nist.gov.

Installing NSRL Hashes in Autopsy

To install the indexed NSRL hashes in Autopsy, you need to download the latest version. Follow these steps:

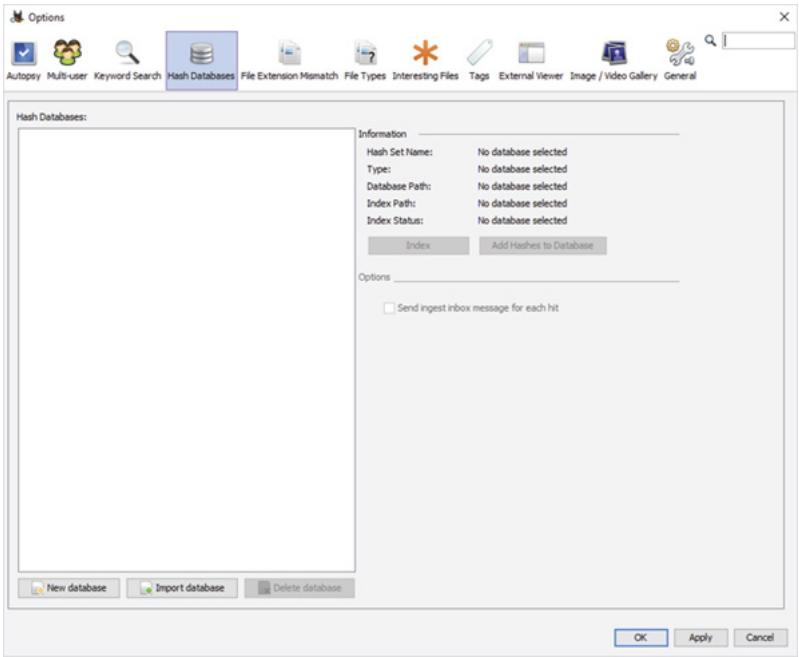
Note

Before beginning this activity, create a C:*Work*\Chap09\Chapter folder (referred to as your "work folder" in steps). Download to this work folder any files in this chapter's downloads section on the student companion site for this book.

1. Start a Web browser, go to https://sourceforge.net/projects/autopsy/files/NSRL/, and download the zip file containing the latest version of NSRL hashes. Unzip this file to your work folder, where you can access it from Autopsy.

2. Start Autopsy for Windows. In the Welcome window, click **Close**, and then click **Tools, Options** from the menu. In the Options window, click the **Hash Databases** icon to open the window shown in Figure 9-1.

Figure 9-1.



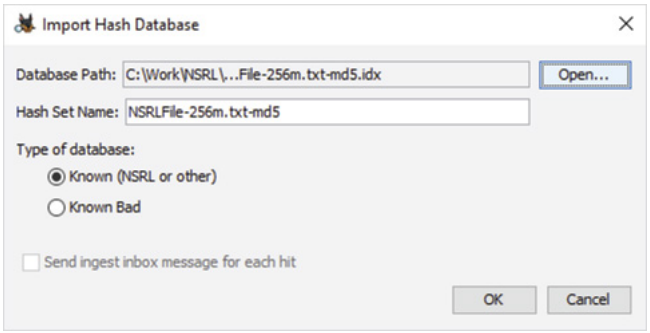
Source: www.sleuthkit.org

The Hash Databases options

3. Click the **Import database** button. In the Import Hash Database dialog box (see Figure 9-2), click **Open**, navigate to your work folder, click the NSRL file, and then click **Open**.

Click **OK**.

Figure 9-2.



Source: www.sleuthkit.org

The Import Hash Database dialog box

Note Each edition of the NSRL hash database contains a version number in its filename; in **Figure 9-2**, for example, the version number is 256. When installing this database, use the one with the highest version number in its filename.

4. In the Options window, click **OK** to finish the installation. Exit your Web browser, and leave Autopsy running for the next activity.

Later in this chapter, you learn how to use hash databases to find data on a suspect's disk or in an image file.

Collecting Hash Values in Autopsy

In the following activity, you learn how to get the MD5 hash value of files in Autopsy. You're looking for files named "Special Project-A" with a .jpg or .bmp extension. After you find these files, you collect their MD5 hash values in a spreadsheet. In the next activity, you create a hash database of known files of interest. To find files' hash values, follow these steps:

1. In File Explorer, double-click the **Ch09Inchp01.exe** file you downloaded to your work folder to uncompress the image file InChap09.dd, and then start Autopsy for Windows, if necessary.

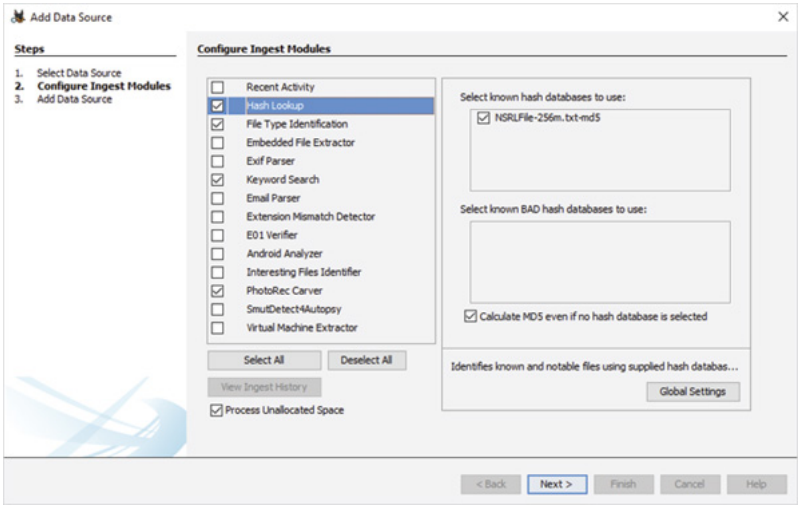
2. In the Welcome window, click the **Create New Case** button. In the New Case Information window, type **InChap09** for the case name. Click the **Browse** button next to the Base Directory text box, navigate to and click your work folder, click **OK**, and then click **Next**.

3. In the Additional Information window, type **InChap09** in the Case Number text box and your name in the Examiner text box. Click **Finish**.

4. In the Add Data Source window, click **Disk Image or VM file** in the Select Type of Data Source to Add section, and then click **Next**. In the Select Data Source window, click the **Browse** button, navigate to your work folder, click **InChap09.dd** , and then click **Open**. Then click **Next**.

5. In the Configure Ingest Modules window, click the **Hash Lookup** check box. In the "Select known hash databases to use" section, click the check box for the NSRL file you installed. On the left, click the **File Type Identification**, **Keyword Search**, and **PhotoRec Carver** check boxes, and then click to clear all other check boxes. At the lower left, click the **Process Unallocated Space** check box, as shown in Figure 9-3, and then click **Next** and **Finish**.

Figure 9-3.

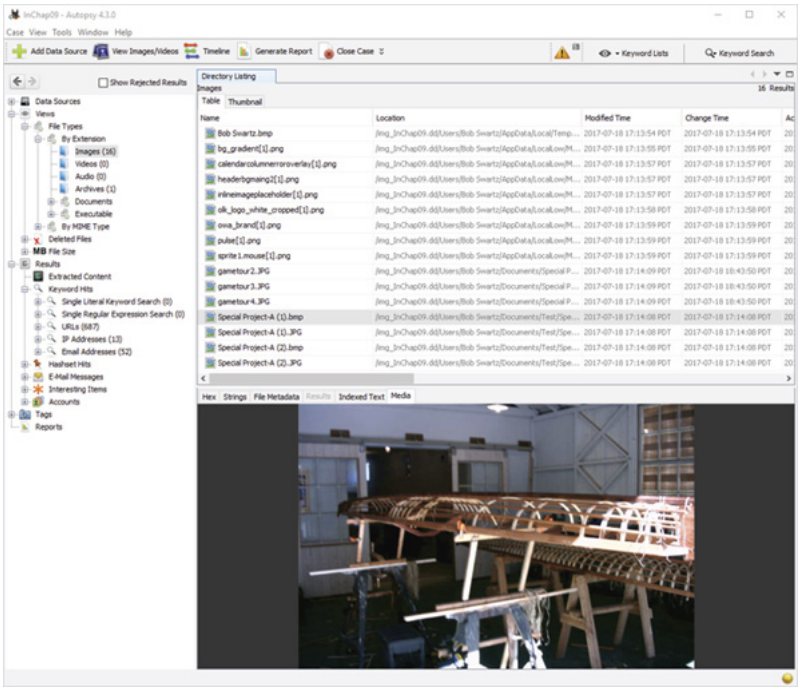


Source: www.sleuthkit.org

The Configure Ingest Modules window

6. When the ingest process is finished, in the Tree Viewer pane on the left, click to expand **Views**, **File Types**, **By Extension**, and **Images** (see Figure 9-4).

Figure 9-4.



Source: www.sleuthkit.org

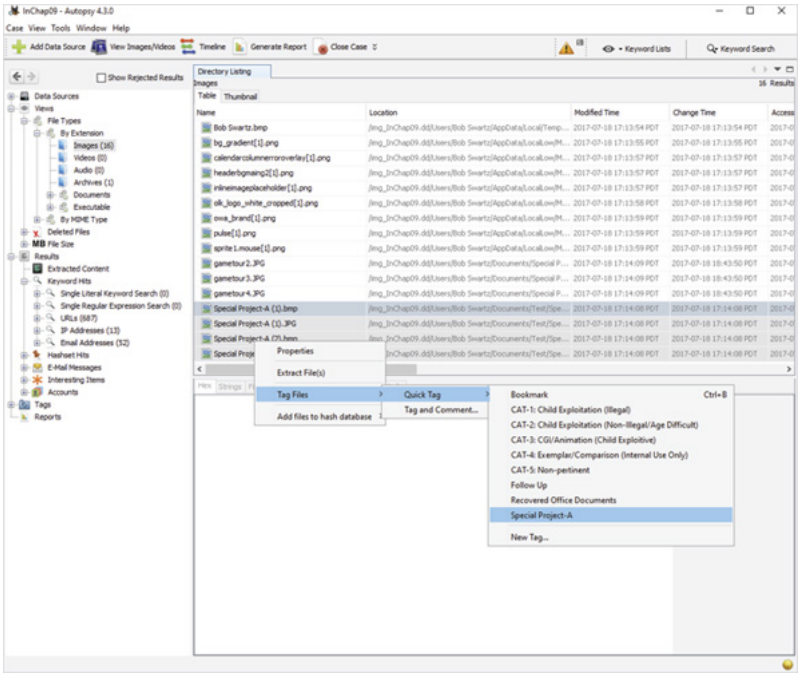
Viewing files with image file extensions

7. Right-click the **Special Project-A (1).bmp** file, point to **Tag File**, and click **Tag and Comment**. In the Create Tag dialog box, click the **New Tag Name** button. In the New Tag section, type **Special Project-A** in the Tag Name text box, click **OK**, and then click **OK** again.

8. In the Result Viewer pane, Ctrl+click **Special Project-A (1).JPG, Special Project-A (2).bmp** , and **Special Project-A (2).JPG** . Right-click this selection, point to **Tag File**

and then **Quick Tag**, and then click **Special Project-A** (see Figure 9-5).

Figure 9-5.

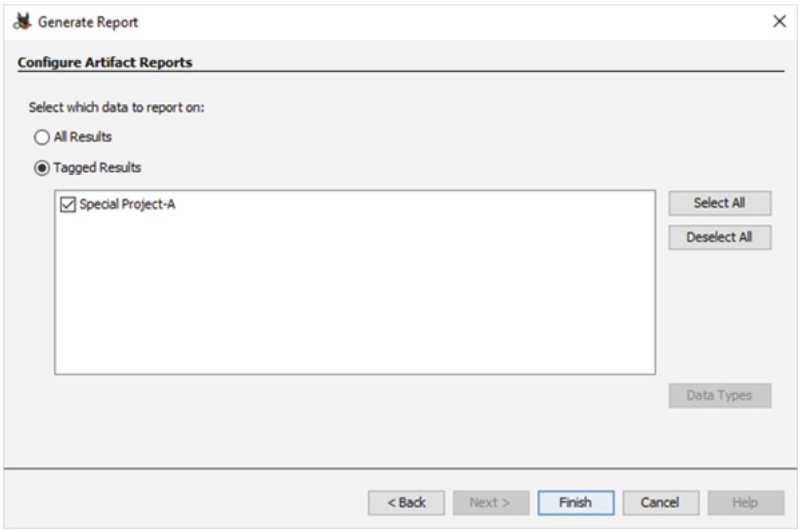


Source: www.sleuthkit.org

Tagging Special Project-A files

9. Click **Generate Report**, and in the Generate Report window, click the **Results - Excel** option button in the Report Modules section, and then click **Next**. In the Configure Artifact Reports window, click the **Tagged Results** option button, click the **Special Project-A** check box (see Figure 9-6), and then click **Finish**.

Figure 9-6.



Source: www.sleuthkit.org

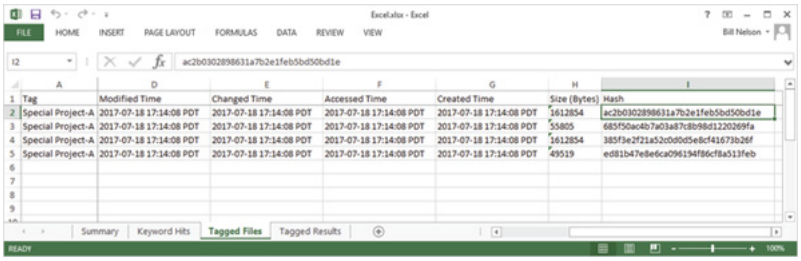
Configuring report options

10. In the Report Generation Progress window, click the **Results - Excel** pathname to examine the Excel report.

11.

In the Excel report, examine the contents of the Tagged Files sheet. Scroll to column I, labeled Hash (see **Figure 9-7**), and then save the Excel file as **InChap09-Report** in your work folder. Leave it open for the next activity.

Figure 9-7.

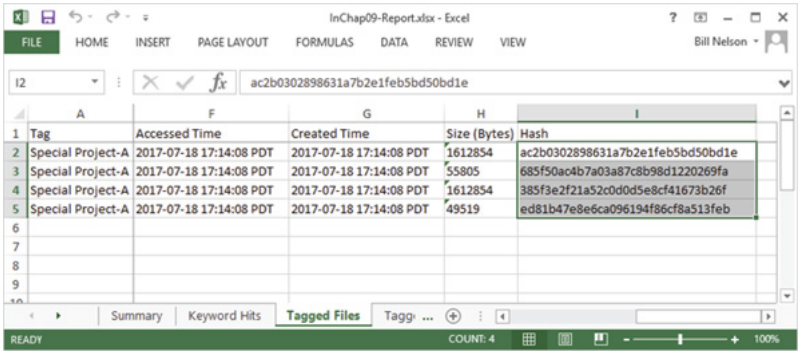


Hash values for Special Project files

The following activity shows you how to add the hash values you found to a new hash database that can be used in future forensics analysis on other drives. Follow these steps to create this database:

1. If you closed the Excel file created in the previous activity, open it and navigate to column I in the Tagged Files sheet. Copy the four MD5 hash values in rows 2 through 5, shown in **Figure 9-8**.

Figure 9-8.

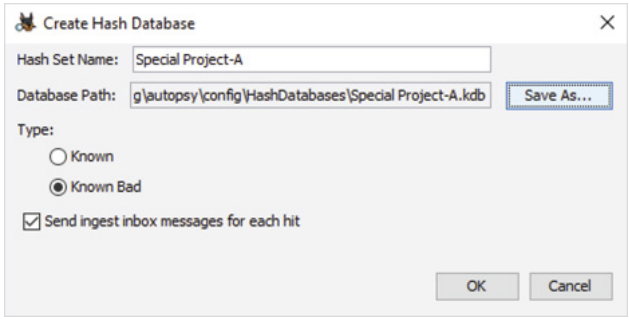


Hash values to copy from the Excel spreadsheet

2. In Autopsy, click **Tools, Options** from the menu, and in the Options window, click the **Hash Databases** icon.

3. Click the **New database** button to open the Create Hash Database dialog box. In the Hash Set Name text box, type **Special Project-A**, and then click **Save As**. In the Save dialog box, click **Save**. In the Create Hash Database dialog box, click the **Known Bad** option button (see Figure 9-9), and then click **OK**.

Figure 9-9.



Source: www.sleuthkit.org

Creating a known bad hash database

4. In the Hash Databases list box, click to select **Special Project-A**, and under the Information section, click the **Add Hashes to Database** button. In the "Paste MD5 hash value(s) (one per line) below" section, click **Paste From Clipboard**. Click **Add Hashes to Database**, and click **OK** twice.

5. Exit Autopsy and Excel.

Validating Forensic Data

One of the most critical aspects of digital forensics is validating digital evidence because ensuring the integrity of data you collect is essential for presenting evidence in court. **Chapter 4** introduced forensic hashing algorithms, and in this section, you learn more about validating an acquired image before you analyze it.

Most forensics tools offer a feature for hashing image files. Digital forensics tools have some limitations in performing hashing, however, so using advanced hexadecimal editors is necessary to ensure data integrity.

Validating with Hexadecimal Editors

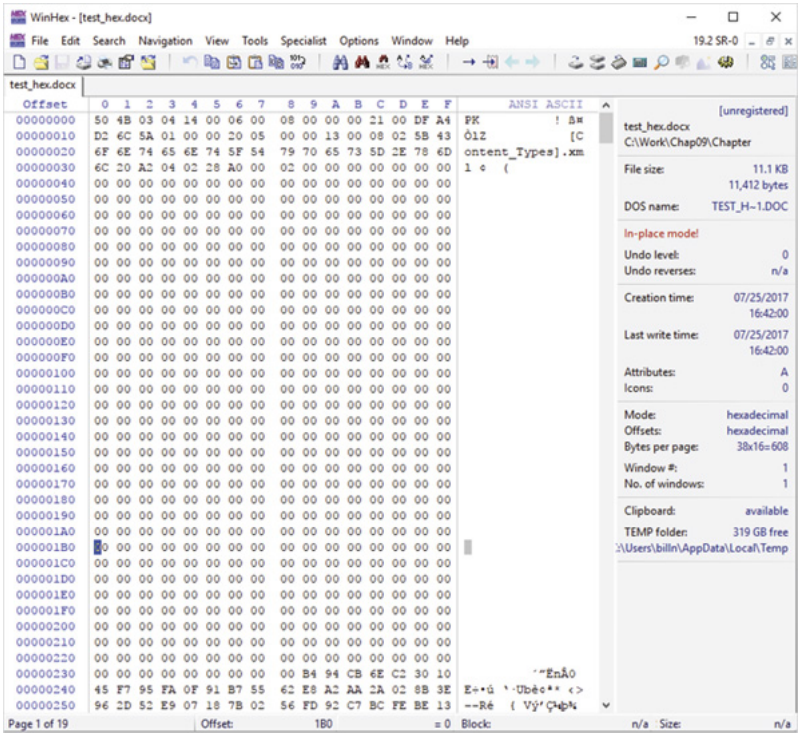
Advanced hexadecimal editors have many features not available in digital forensics tools, such as hashing specific files or sectors. Learning how to use these tools is important, especially when you need to find a particular file—for example, a known contraband image. With the hash value in hand, you can use a forensics tool to search for a suspicious file that might have had its name changed to look like an innocuous file. (Recall that two files with exactly the same content have the same hash value, even if they have different names.) Getting hash values with a full-featured hexadecimal editor can be faster and easier than with a digital forensics tool.

WinHex provides several hashing algorithms, such as MD5 and SHA-1. Sometimes you need the hash value of specific files or sectors to validate whether data or fragments (sectors) match the contents of a known file, or you need to verify data immediately after a sparse acquisition, for example. To use the hashing functions of WinHex, follow these steps:

1. Start Word, and in a new document, type a sentence or two, and save the file as **test_hex.docx** in your work folder. When you're finished, exit Word.

2. Start WinHex, using the **Run as administrator** option. (If necessary, when the UAC message box opens, click **Yes**.) Click **File, Open** from the main menu. In the Open dialog box, navigate to your work folder, click **test_hex.docx** , and click **Open**. Figure 9-10 shows the file open in WinHex.

Figure 9-10.

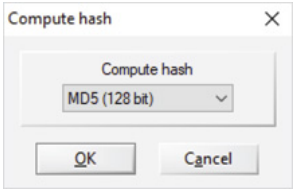


Source: X-Ways AG, www.x-ways.net

Viewing a file opened in WinHex

3. To compute an MD5 hash of this file, click **Tools, Compute Hash** from the menu to open the Compute hash dialog box (see Figure 9-11). Click the list arrow, click **MD5 (128 bit)**, if necessary, and then click **OK**.

Figure 9-11.

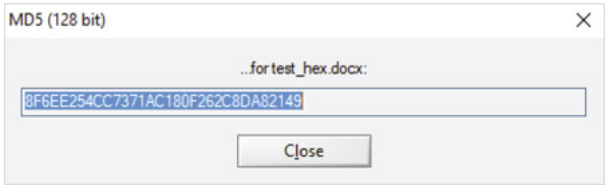


Source: X-Ways AG, www.x-ways.net

The Compute hash dialog box

4. In the MD5 (128 bit) dialog box, right-click the hash value (see **Figure 9-12**) and click **Copy**. Start Notepad, and paste the hash value into a new text document. Save the file as **test_hex_hashvalue.txt** in your work folder, exit Notepad, and then click **Close** in the MD5 (128 bit) dialog box. Leave WinHex running for the next activity.

Figure 9-12.



Source: X-Ways AG, www.x-ways.net

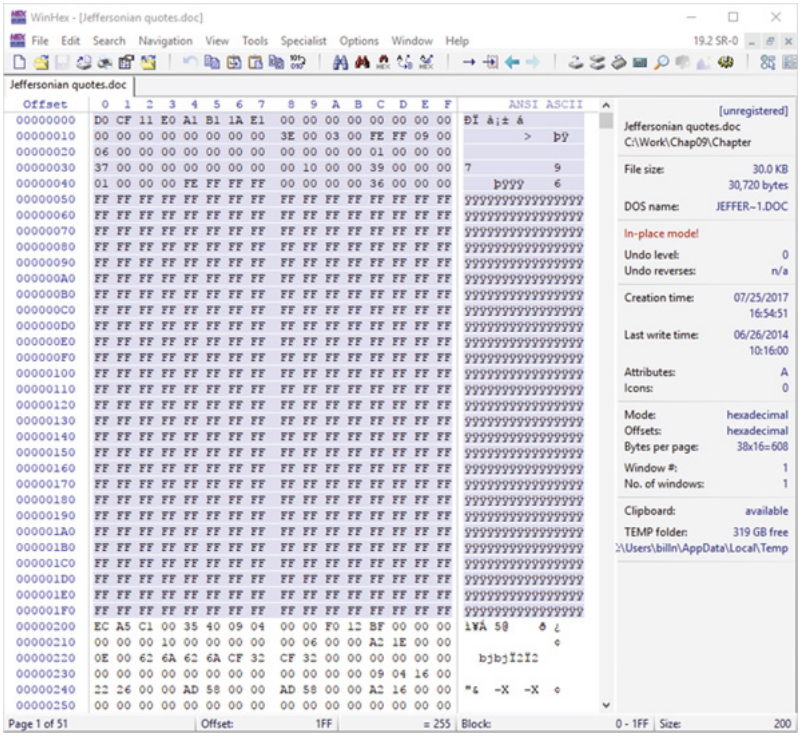
MD5 hash results

Another feature of WinHex generates the hash value of selected data in a file or any sector on a disk. To see how this feature works, follow these steps:

1. In WinHex, open the **Jeffersonian quotes.doc** file from your work folder.
2. Place the mouse pointer at the beginning of the byte address **00000000** ; the pointer should be positioned on the hexadecimal D0 because you're examining the first sector of the file.
3. Drag to select a complete sector (512 bytes or x200 bytes). To know when you've selected the sector, watch the Offset counter at the bottom in the status bar. It should display "Offset: 1FF" when you've highlighted the entire sector, as shown in **Figure 9-13**.

Tip As you drag the mouse, note that the offset counter increments or decrements according to the direction of the mouse's movement across the window. This counter defaults to hexadecimal but can be altered to decimal counting. To toggle the offset counter between hexadecimal and decimal, click anywhere in the Offset section of the status bar at the bottom.

Figure 9-13.



Source: X-Ways AG, www.x-ways.net

The first sector of Jeffersonian quotes.doc

4. Click **Tools, Compute Hash** from the menu to open the Compute hash dialog box. Click the list arrow, click **MD5 (128 bit)**, if necessary, and then click **OK**.

5. Right-click the hash value in the MD5 (128 bit) dialog box and click **Copy**. Start Notepad, and paste the hash value into a new text document. Save the file as **Quotes_hashvalue.txt** in your work folder, exit Notepad, and then click **Close** in the MD5 (128 bit) dialog box.

6. Exit Notepad and WinHex.

The advantage of recording hash values is that you can determine whether data has changed. As shown in the preceding steps, you can use this method for specific sectors or entire files. One advantage of using hashes of sectors is that you can look for known file fragments, a process called **block-wise hashing** . This process builds a data set of hashes of sectors from the original file, and then examines sectors on the suspect's drive to see whether any other sectors match. If an identical hash value is found, you have confirmed that the file was stored on the suspect's drive. For example, say you have a known Word document from a victim, and it was stored and then deleted on a suspect's computer. The attempted recovery of deleted files reveals no trace of the original file, but you can search for fragments of deleted files by using block-wise hashing. X-Ways Forensics and many other forensics tools offer this feature. For more information on how it detects data remnants, see www.x-ways.net/winhex/manual.pdf; for an example of how X-Ways Forensics performs this function, see www.xwaysclips.co.uk/2015/05/video-46-block-hashing-explained.html.

Using Hash Values to Discriminate Data

In **Chapter 6**, you learned about using the discrimination function to sort known good files from suspicious files. This function is useful in limiting the amount of data you have to examine, and many current digital forensics tools offer it. AccessData has its own hashing database, **Known File Filter (KFF)** , which is available only with FTK. KFF filters known

program files, such as winword.exe, from view and contains the hash values of known illegal files, such as child pornography. It then compares known file hash values with files on your evidence drive or image files to see whether they contain suspicious data. Periodically, AccessData updates these known hash values and posts an updated KFF. As mentioned in Chapter 6, the NIST National Software Reference Library (NSRL; www.nsrl.nist.gov/index.html) maintains a national database of updated file hash values for a variety of OSs, applications, and images; however, it doesn't list hash values of known illegal files. Other digital forensics tools, such as X-Ways Forensics, OSForensics, and Forensic Explorer, can import the NSRL database and run hash comparisons.

Validating with Digital Forensics Tools

As mentioned, commercial digital forensics tools have built-in validation features for image acquisitions. These tools generate MD5 and SHA-1 hash values for the data in image files.

For example, in AccessData FTK Imager, when you select the Expert Witness (.E01) or SMART (.S01) format, additional options are available for hashing all the data. FTK Imager then inserts a report into the .E01 or .S01 file that lists MD5 and SHA-1 hash values. Autopsy has a similar feature called E01 Verifier for verifying an Expert Witness image file.

When this image file is loaded in a forensics tool, another MD5 or SHA-1 hash is run on the copied data and then compared with the original hash value to verify whether the image file is correct. If the hashes don't match, the forensic tool produces an error message that the digital evidence has been corrupted. In this case, the digital forensics examiner needs to create a new forensic image of the original data. If the original drive is unavailable or if the image is from a RAM disk or a system memory dump, the examiner should list the mismatched hash values in a report, which should state that the findings might not be accurate because the hash values don't match.

Because raw data acquisitions, such as dd images, can't store the original image hash, many tools generate a separate text file containing additional information about an acquisition, including its hash value. In the following activity, you learn how to use WinHex to hash an image file and then compare it with the original hash value FTK Imager calculated. You use two files you extract from the Ch09Inchp01.exe file you downloaded before starting this chapter's activities. Follow these steps to verify the integrity of the InChap09.dd image:

1. In File Explorer, navigate to your work folder and double-click the **InChap09.exe** file to extract its contents. Then double-click the **InChap09.dd.txt** file to open it in Notepad, as shown in Figure 9-14.

Figure 9-14.

```
InChap09.dd.txt - Notepad
File  Edit  Format  View  Help
Created By AccessData® FTK® Imager 3.1.1.8

Case Information:
Acquired using: ADI3.1.1.8
Case Number: InChap09
Evidence Number: InChap09
Unique description: In chapter exercise
Examiner: Joe Friday
Notes: In chapter exercise on hashing raw image files

--------------------------------------------------------------

Information for C:\Work\Chap09\InChap09:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Logical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 3,074,048
[Physical Drive Information]
 Removable drive: False
 Source data size: 1501 MB
 Sector count:    3074048

ATTENTION:
The following sector(s) on the source drive could not be read:
        1960096 through 1960101
        2061632 through 2061635
The contents of these sectors were replaced with zeros in the image.

[Computed Hashes]
 MD5 checksum:    db945a7e3589743923237c0518ababe1
 SHA1 checksum:   6d87a3665d756b7e22de3d0b087c6ab9ec3f8bf7

Image Information:
 Acquisition started:   Thu Jul 27 15:36:30 2017
 Acquisition finished:  Thu Jul 27 15:38:03 2017
 Segment list:
  C:\Work\Chap09\InChap09.001
```

The FTK Imager case information file

2. Start WinHex, and click **File, Open** from the menu. Navigate to your work folder. Click the **InChap09.dd** file, and click **Open**. In the WinHex warning message box, click **OK**.

3. Click **Tools**, **Compute Hash** from the menu. In the Compute hash dialog box, click the list arrow, click **MD5 (128)**, if necessary, and then click **OK**.

4. Right-click the hash value in the MD5 (128) dialog box and click **Copy**. In the InChap09.dd.txt file you opened in Step 1, find the original MD5 hash value. Under it, type **Verified MD5:** and paste the MD5 hash value, as shown in Figure 9-15.

Figure 9-15.

```
[Computed Hashes]
 MD5 checksum:    db945a7e3589743923237c0518ababe1
 Verified MD5:    DB945A7E3589743923237C0518ABABE1
 SHA1 checksum:   6d87a3665d756b7e22de3d0b087c6ab9ec3f8bf7
```

Recording the MD5 hash value

5. In Notepad, save InChap09.dd.txt as **InChap09.dd-verified.txt** in your work folder, and exit Notepad.

6. In WinHex, click **Close** in the MD5 (128) dialog box, and exit WinHex.

Addressing Data-Hiding Techniques

Data hiding involves changing or manipulating a file to conceal information. Data-hiding techniques include hiding entire partitions, changing file extensions, setting file attributes to hidden, bit-shifting, using encryption, and setting up password protection. Some of these techniques are discussed in the following sections.

Hiding Files by Using the OS

One of the first techniques used to hide data was changing file extensions, as you learned in **Chapter 8**. For example, a suspect wanting to hide an Excel spreadsheet containing

incriminating evidence could change its extension from .xlsx to .jpg. An investigator who tries to open the file in Excel will get an error message stating that the file can't be opened. Advanced digital forensics tools, however, check file headers and compare the file extension to verify that it's correct. If there's a discrepancy, the tool flags the file as a possible altered file that requires more analysis.

Another hiding technique is selecting the Hidden attribute in a file's Properties dialog box, so an investigator who's trying to view files in File Explorer should select the option to view hidden files, folders, and drives. Digital forensics tools can identify hidden files for investigators, however.

Hiding Partitions

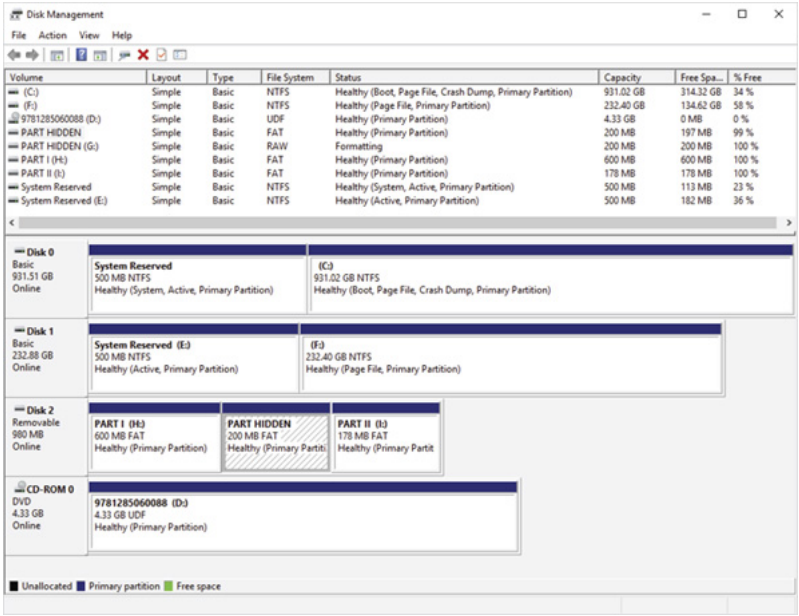
One way to hide partitions is with the Windows disk partition utility, diskpart. By using the diskpart remove *letter* command at the PowerShell prompt, you can unassign the partition's letter, which hides it from view in File Explorer. To unhide the partition, use the diskpart assign *letter* command. Other disk management tools, such as IM-Magic, EaseUS Partition Master, and Linux Grand Unified Bootloader (GRUB), are available, too. For more information on the diskpart command, see www.disk-partition.com/diskpart/assign-drive-letter-4125.html

Tip

To learn more about hiding and unhiding partitions, see www.isumsoft.com/windows-10/hide-or-unhide-hard-disk-partition-in-windows-10.html or https://datarecovery.wondershare.com/hide-partition-in-windows-10.html.

To detect whether this technique has been used, be sure to account for all disk space when you're examining an evidence drive. Analyze any disk areas containing space you can't account for so that you can determine whether they contain additional evidence. For example, in **Figure 9-16**, the Windows Disk Management tool shows two partitions for Disk 2, labeled H and I, with a 200 MB gap between them. For demonstration purposes, this gap has been labeled "PART HIDDEN" and has no assigned letter. Most digital forensics tools or hexadecimal editors can access these gaps. Gaps between partitions are typically 128 bytes in Windows Vista and later. In this example, the 200 MB gap between partitions H and I indicates you should examine this larger-than-normal gap to see whether it contains any relevant evidence.

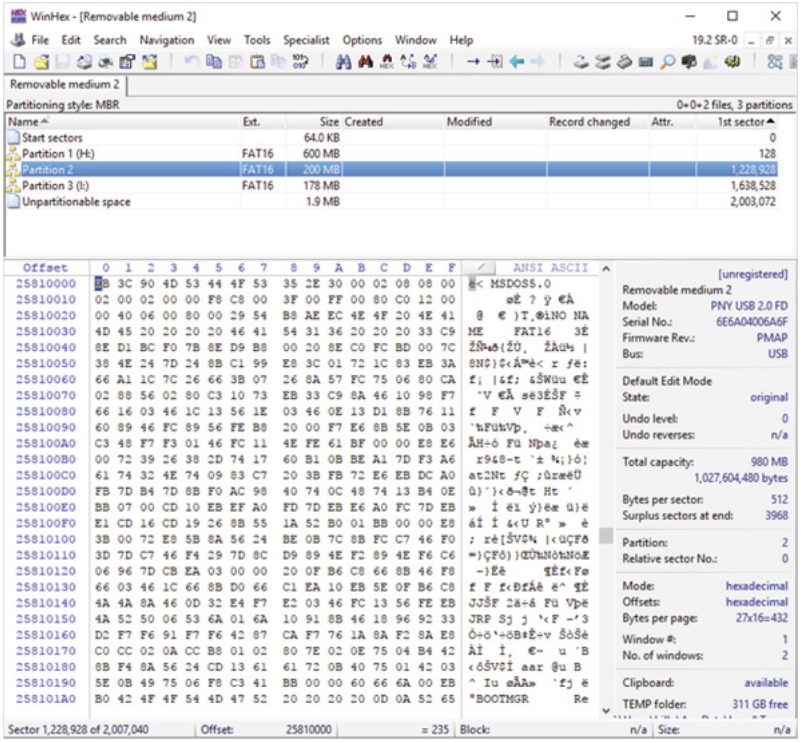
Figure 9-16.



The Disk Management window

Many digital forensics tools can detect and view a hidden partition. Both WinHex and Autopsy, for example, can show partitions and hidden partitions on a disk volume. In WinHex, you can also view all connected disks. Notice that partition 2 in **Figure 9-17** has no drive letter associated with it. The lack of a drive letter means it's a hidden partition. In addition, WinHex displays the boot partition as "Start sectors" and the unallocated area as "Unpartitionable space."

Figure 9-17.

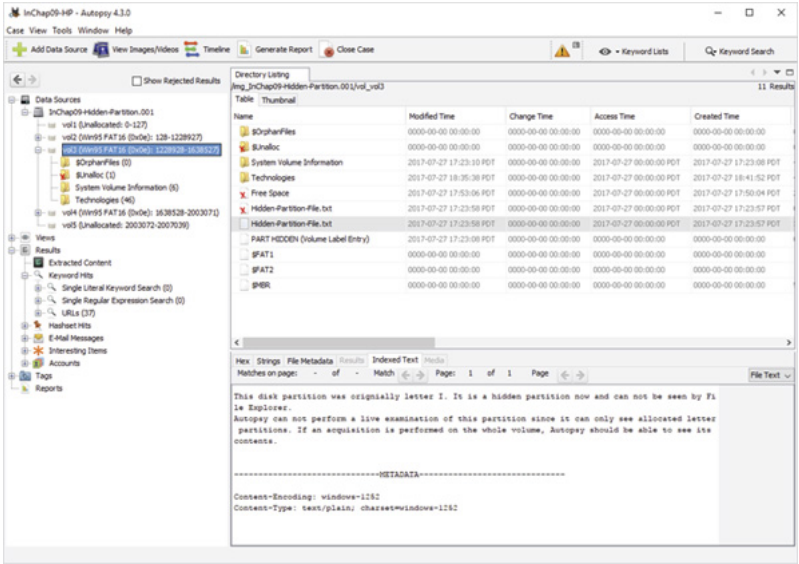


Source: X-Ways AG, www.x-ways.net

Viewing a hidden partition in WinHex

Figure 9-18 shows how Autopsy displays a forensic image of the same drive shown in Figure 9-17. Under Data Sources, Autopsy displays all partitions as volumes, including the boot partition and the unallocated volume. The hidden partition in WinHex, Partition 2, is displayed in Autopsy as vol3 (Win95 FAT16 (0x0e): 1228928-1638527). In Autopsy, hidden partitions are visible only when viewing a forensic disk image, not when viewing in live mode.

Figure 9-18.



Source: www.sleuthkit.org

Viewing a hidden partition in Autopsy

Marking Bad Clusters

Another data-hiding technique used in FAT file systems is placing sensitive or incriminating data in free or slack space on disk partition clusters. This technique, although not common now, involves using older utilities, such as Norton DiskEdit, developed by Symantec as part of its Norton Utilities suite. In Norton DiskEdit, you can mark good clusters as bad clusters in the FAT table. The OS then considers these clusters unusable. The only way they can be accessed from the OS is by changing them to good clusters with a disk editor.

To mark a good cluster as bad in Norton DiskEdit, you type the letter B in the FAT entry corresponding to that cluster when examining the FAT table. You can then use any DOS disk editor to write and read data to this cluster, which is effectively hidden because it appears as bad to the OS.

DiskEdit was last available in version 8.0 of Norton Utilities. It runs only in MS-DOS and can access only FAT-formatted disk media. You can't run it by using Windows command prompts. You can find Symantec Norton Utilities at Win World PC (https://winworldpc.com/product/norton-utilities/80). This download site provides one file in 7z compressed format. See the READ.ME text file for instructions on how to run this utility. For additional Norton DOS utilities, see http://vetusware.com/download/Norton%20Utilities%208.0/?id=3515.

Note

If a FAT partition containing clusters marked as bad is converted to an NTFS partition, the bad clusters remain marked as bad, so the conversion to NTFS doesn't affect the content of these clusters. Most GUI tools skip clusters marked as bad in FAT and NTFS, and these clusters might contain valuable evidence for your investigation.

Bit-Shifting

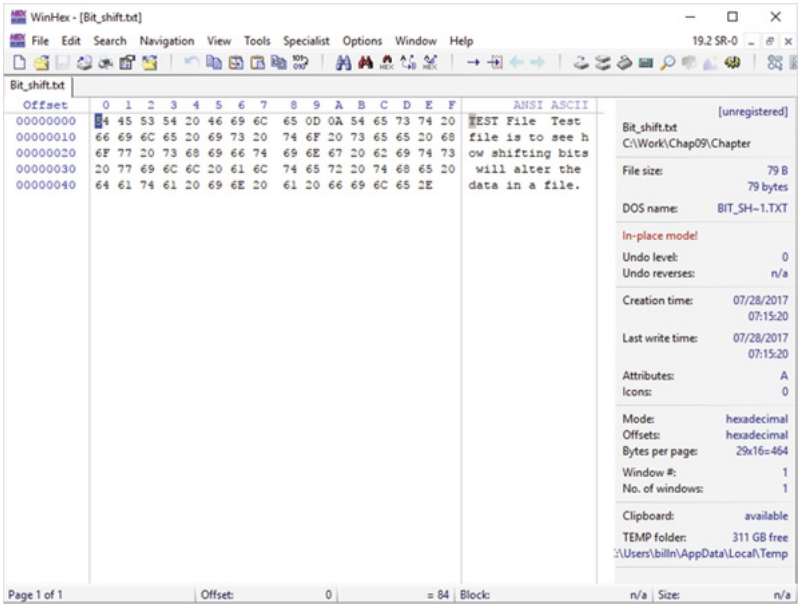
Some home computer users developed programming skills in computer manufacturers' assembly languages and learned how to create a low-level encryption program that changes

the order of binary data, making the altered data unreadable when accessed with a text editor or word processor. These programs rearrange bits for each byte in a file. To secure a file containing sensitive or incriminating information, these users run an assembler program (also called a "macro") on the file to scramble the bits. To access the file, they run another program that restores the scrambled bits to their original order. Some of these programs are still used today and can make it difficult for investigators to analyze data on a suspect drive. You should start by identifying any files you're not familiar with that might lead to new evidence. Training in assembly language—as well as higher-level programming languages, such as Visual Basic, Visual C++, or Perl—is also helpful.

A related, and well-known, technique for hiding data is shifting bit patterns to alter the byte values of data. **Bit-shifting** changes data from readable code to data that looks like binary executable code. WinHex and Hex Workshop include a feature for shifting bits and altering byte patterns of entire files or specified data. To shift bits in a text file, follow these steps:

1. Start Notepad, and in a text document, type **TEST FILE. Test file is to see how shifting bits will alter the data in a file**.
2. Save the file as **Bit_shift.txt** in your work folder, and exit Notepad.
3. Start WinHex, using the **Run as administrator** option. (If necessary, when the UAC message box opens, click **Yes**.) Click **File, Open** from the menu. Navigate to your work folder, and then double-click **Bit_shift.txt** . Figure 9-19 shows the file open in WinHex.

Figure 9-19.

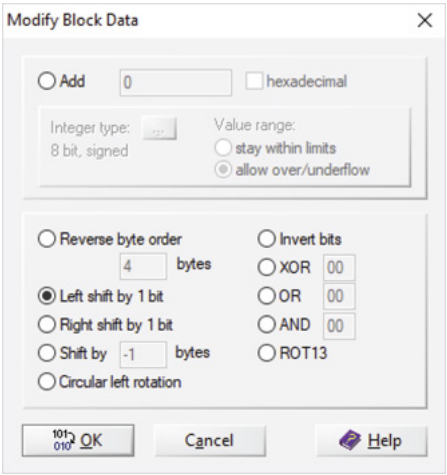


Source: X-Ways AG, www.x-ways.net

Bit_shift.txt open in WinHex

4. To set up WinHex for bit-shifting, click **Options**, **Edit Mode** from the menu. Click **Default Edit Mode (=editable)**, if necessary, and then click **OK**.
5. Highlight all the data in the file by clicking **Edit**, **Select All** from the menu.
6. Click **Edit**, **Modify Data** from the menu. In the Modify Block Data dialog box, click the **Left shift by 1** bit option button (see Figure 9-20), and then click **OK**.

Figure 9-20.

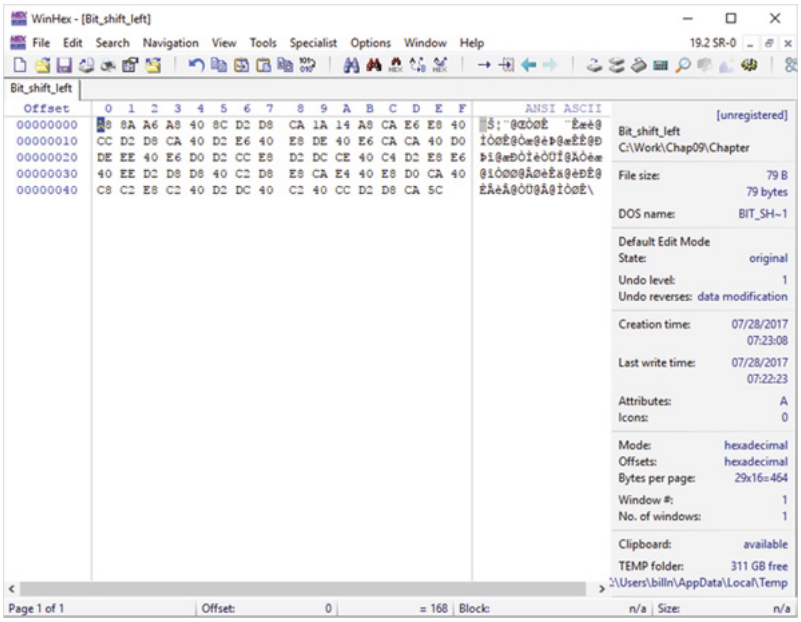


Source: X-Ways AG, www.x-ways.net

The Modify Block Data dialog box

7. Click **File**, **Save As** from the menu, and save the file as **Bit_shift_left.txt** in your work folder. As you can see in Figure 9-21, the text has changed to random values. Exit and then restart WinHex.

Figure 9-21.



Source: X-Ways AG, www.x-ways.net

Viewing the shifted bits

8. To return the file to its original configuration, you need to bit-shift it back to the right. Make sure the data is highlighted, and then click **Edit**, **Modify Data** from the menu. In the Modify Block Data dialog box, click **Right shift by 1 bit**, and then click **OK**.

9. Save the file as **Bit_shift_right.txt** in your work folder, and leave this file open in WinHex for the next activity.

Now you can use WinHex to find the MD5 hash values for these three files and determine whether Bit_shift.txt is different from Bit_shift_right.txt and Bit_shift_left.txt. To check the MD5 values in WinHex, follow these steps:

1. With Bit_shift_right.txt open in WinHex, click **File**, **Open** to open **Bit_shift.txt** , and then repeat to open **Bit_shift_left.txt** .
2. Click the **Bit_shift.txt** tab to make it the active file, and highlight the file's content by clicking **Edit**, **Select All**.
3. Click **Tools, Compute Hash** from the menu to open the Compute hash dialog box. In the list box, click **MD5 (128 bit)**, if necessary, and then click **OK**. Copy the MD5 hash value of Bit_shift.txt, and paste it in a new text document in Notepad. Click **Close** in the MD5 (128 bit) dialog box.
4. Repeat **Steps 2** and 3 for **Bit_shift_left.txt** and **Bit_shift_right.txt** , pasting their hash values in the same Notepad text file.
5. Compare the MD5 hash values to determine whether the files are different. When you're finished, exit WinHex. In Notepad, save the text file as **Bit_shift_recovery.txt** in your work folder, and exit Notepad. If your output is correct, the Bit_shift.txt and Bit_shift_right.txt files should have the same MD5 hash values. Exit WinHex and Notepad.

Typically, antivirus tools run hashes on potential malware files, but some advanced malware uses bit-shifting as a way to hide its malicious code from antivirus tools. With the bit-shifting functions in WinHex, however, you can inspect potential malicious code manually. In addition, some malware that attacks Microsoft Office files consists of executable code that's embedded at the end of document files and hidden with bit-shifting. When an Office document is opened, the malware reverses the bit-shifting on the executable code and then runs it.

Understanding Steganalysis Methods

As explained in **Chapter 8**, the term **steganography** comes from the Greek word for "hidden writing." It's defined as hiding messages in such a way that only the intended recipient knows the message is there. The term for detecting and analyzing steganography files is "steganalysis."

In addition to steganography, digital watermarking was developed as a way to protect file ownership. Some digital watermarks are designed to be visible—for example, to notify users that an image is copyrighted. The digital watermarks used for steganography aren't usually visible. For example, when viewing two files that look the same, but one has an invisible digital watermark, they appear to be the same file. Their file sizes might even be identical. However, if you run an MD5 or SHA-1 hash comparison on both files, you'll find that the hash values aren't equal. **Chapter 8** described a few steganography tools available for lossy graphics files. These tools insert data into the graphics file but often alter the original file in size and clarity.

One way to hide data is to use steganography tools, many of which are freeware or shareware, to insert information into a variety of files. If you encrypt a plaintext file with PGP and insert the encrypted text into a steganography file, for example, cracking the encrypted message is extremely difficult.

Neil F. Johnson and Sushil Jajodia, authors of the white paper "Steganalysis of Images Created Using Current Steganography Software" (1998, www.jjtc.com/ihws98/jjgmu.html), described these steganalysis methods ("attacks"):

- *Stego-only attack*—Used when only the file containing the possible steganography content is available for analysis; it's similar to a cyphertext attack. This attack is one of the most difficult to perform because all you have to analyze is the suspected steganography file.
- *Known cover attack*—Used when the **cover-media** , the original file with no hidden message, and the **stego-media** , the converted cover-media file that stores the hidden message, are available for analysis. By analyzing the original and steganography files,

further comparisons can be made to identify common patterns that might help decipher the message.

- *Known message attack*—Used when the hidden message is revealed later, allowing further analysis of new messages. Similar to the known cover attack, this method uses comparative analysis to decipher the message. Because the message is known, deciphering it takes less effort.
- *Chosen stego attack*—Used when a steganography tool and stego-media were used to hide the message content. Because this method uses a known steganography tool, the analyst applies password or passphrase recovery techniques to decipher the message.
- *Chosen message attack*—Used to identify corresponding patterns used in stego-media. This technique creates stego-media and then analyzes them to determine how data is configured in the file. The analyst then uses these known configuration patterns to compare with suspected stego-media to determine what the message might be.

Examining Encrypted Files

People who want to make data unreadable can use advanced encryption programs, such as PGP or BestCrypt. Encrypted files are encoded to prevent unauthorized access. To decode an encrypted file, users supply a password or passphrase. Without the passphrase, recovering the contents of encrypted files is difficult. Many commercial encryption programs use a technology called **key escrow** , which is designed to recover encrypted data if users forget their passphrases or if the user key is corrupted after a system failure. Forensics examiners can also use key escrow to attempt to recover encrypted data. Although some vendors have developed key recovery tools, the resources needed to crack encryption schemes are usually beyond what's available to small or medium organizations. If you do encounter encrypted data in an investigation, make an effort to persuade the suspect to reveal the encryption passphrase.

Some encryption schemes are so complex that the time to crack them can be measured in days, weeks, years, and even decades. Key sizes of 128 bits to 4096 bits make the job of breaking them with a brute-force attack nearly impossible with current technology. Quantum computing is progressing to make many current encryption schemes obsolete. Currently, there are some encryption schemes that will remain unbroken with commercially available tools.

Recovering Passwords

Password recovery is becoming more common in digital forensics analysis. Several password-cracking tools are available for handling password-protected data or systems. Some of these products are integrated into a digital forensics tool, such as OSForensics. Others, including the following, are stand-alone tools that typically require extracting password files or accessing a suspect's disk or image file directly:

- Last Bit (http://lastbit.com/password-recovery-methods.asp)
- AccessData PRTK (http://accessdata.com/product-download at the Decryption Products link)
- ophcrack (http://ophcrack.sourceforge.net)
- John the Ripper (www.openwall.com/john)
- Passware (www.lostpassword.com/kit-forensic.htm)

These tools use a dictionary attack or brute-force attack to crack passwords. Brute-force attacks use every possible letter, number, and character found on a keyboard. Eventually, a brute-force attack can crack any password; however, this method can require a lot of time and processing power, especially if the password is very long. In a dictionary attack, the program

uses common words found in the dictionary and tries them as passwords. Most password crackers have dictionaries in a variety of languages, including English, French, Russian, and even Swahili. With some password-cracking tools, you can import additional unique words extracted from evidence. In FTK, for example, you can export a word list to PRTK that can be added to the dictionary.

With many of these programs, you can build profiles of a suspect to help determine his or her password. These programs consider information such as names of relatives or pets, favorite colors, and schools attended. The principle behind these programs is that people have a habit of using things they're comfortable with, especially if it requires memorizing something secret, such as a password. This method of password cracking is known as a "hybrid attack."

Many password-protected OSs and applications store passwords in the form of MD5 or SHA hash values. Because of this storage method, a brute-force attack requires converting a dictionary password from plaintext to a hash value. This process requires additional CPU cycle time to process each attempt to match the dictionary password to the OS or application password.

Another method has been developed that hashes passwords in a dictionary. A **rainbow table** is a file containing the hash values for every possible password that can be generated from a computer's keyboard. Because rainbow tables already contain these hash values and no conversion is necessary, this method is much faster than a dictionary or brute-force attack. For more information on rainbow tables and where to download them, visit http://project-rainbowcrack.com and http://project-rainbowcrack.com/table.htm. As good as rainbow tables are for cracking passwords, however, a new scheme of protecting passwords has been developed that adds extra bits to a password and then hashes it. This technique, called **salting passwords** , alters hash values, which makes cracking passwords more difficult.

Tip

For more information on salting passwords, see http://web.cs.du.edu/~mitchell/forensics/information/pass_crack.html and https://crackstation.net/hashing-security.htm.

It should be noted that algorithms for password encryption vary from simple to complex. When attempting to crack a password, research the encryption method used by the application or OS. You might be able to identify known weaknesses that could help you determine the password.

Chapter Summary

- Examining and analyzing digital evidence depend on the nature of the investigation and the amount of data to process. You begin a forensics case by creating an investigation plan that defines the investigation's goal and scope, the materials needed, and the tasks to perform. Depending on the evidence you find, you might have to modify your investigation plan at some point.
- For most forensics investigations, you follow the same general procedures: Wipe and prepare target drives, document all hardware components on the suspect's computer, check date and time values in the suspect computer's CMOS, acquire data and document your steps, list all folders and files on the suspect system and examine their contents, attempt to open any password-protected files, determine the function of executable files, and document all your steps, making sure to follow evidence preservation procedures.
- Advanced digital forensics tools have features such as indexing text data that make keyword searches much faster. They also allow integrating the NIST National Software Resource Library (NSRL) to get MD5 and SHA-1 hash values for known OSs and applications.
- One of the most critical aspects of digital forensics is validating digital evidence because ensuring the integrity of data you collect is essential for presenting evidence in court. Forensics tools have built-in validation features, but hexadecimal editors offer more advanced features. All data needs to be validated before and during analysis because digital evidence can be corrupted easily. Use hash values such as MD5 and SHA-1 to verify that data hasn't changed.
- Data hiding involves changing or manipulating a file to conceal information. Data-hiding techniques include changing file extensions, setting file attributes to hidden, hiding partitions, bit-shifting, using steganography, and using encryption and password protection.
- There are three ways to recover passwords: dictionary attacks, brute-force attacks, and rainbow tables. Rainbow tables are the quickest method because they contain predefined hash values of all known passwords. If passwords have been salted, however, recovering them can take much longer, and some might not be recoverable at all.

Key Terms

bit-shifting
block-wise hashing
cover-media
key escrow
Known File Filter (KFF)
rainbow table
salting passwords
scope creep
steganography
stego-media

Review Questions

1. Which of the following represents known files you can eliminate from an investigation? (Choose all that apply.)
    a. Any graphics files
    b. Files associated with an application
    c. System files the OS uses
    d. Any files pertaining to the company
2. For which of the following reasons should you wipe a target drive?
    a. To ensure the quality of digital evidence you acquire
    b. To make sure unwanted data isn't retained on the drive
    c. Neither of the above
    d. Both a and b
3. The Known File Filter (KFF) can be used for which of the following purposes? (Choose all that apply.)
    a. Filter known program files from view.
    b. Calculate hash values of image files.
    c. Compare hash values of known files with evidence files.
    d. Filter out evidence that doesn't relate to your investigation.
4. Password recovery is included in all forensics tools. True or False?
5. After you shift a file's bits, the hash value remains the same. True or False?
6. Which forensic image file format creates or incorporates a validation hash value in the image file? (Choose all that apply.)
    a. Expert Witness
    b. SMART
    c. AFF
    d. dd
7. ___ happens when an investigation goes beyond the bounds of its original description.
8. Suppose you're investigating an e-mail harassment case. Generally, is collecting evidence for this type of case easier for an internal corporate investigation or a criminal investigation?
    a. Criminal investigation because subpoenas can be issued to acquire any needed evidence quickly
    b. Criminal investigation because law enforcement agencies have more resources at their disposal
    c. Internal corporate investigation because corporate investigators typically have ready access to company records
    d. Internal corporate investigation because ISPs almost always turn over e-mail and access logs when requested by a large corporation
9. You're using Disk Management to view primary and extended partitions on a suspect's drive. The program reports the extended partition's total size as larger than the sum of the sizes of logical partitions in this extended partition. What might you infer from this information?
    a. The disk is corrupted.
    b. There's a hidden partition.

c. Nothing; this is what you'd expect to see.

d. The drive is formatted incorrectly.

10. Commercial encryption programs often rely on ___ technology to recover files if a password or passphrase is lost.

11. Steganography is used for which of the following purposes?

    a. Validating data

    b. Hiding data

    c. Accessing remote computers

    d. Creating strong passwords

12. The National Software Reference Library provides what type of resource for digital forensics examiners?

    a. A list of digital forensics tools that make examinations easier

    b. A list of MD5 and SHA1 hash values for all known OSs and applications

    c. Reference books and materials for digital forensics

    d. A repository for software vendors to register their developed applications

13. In steganalysis, cover-media is which of the following?

    a. The content of a file used for a steganography message

    b. The type of steganographic method used to conceal a message

    c. The file a steganography tool uses to host a hidden message, such as a JPEG or an MP3 file

    d. A specific type of graphics file used only for hashing steganographic files

14. Rainbow tables serve what purpose for digital forensics examinations?

    a. Rainbow tables contain computed hashes of possible passwords that some password-recovery programs can use to crack passwords.

    b. Rainbow tables are a supplement to the NIST NSRL library of hash tables.

    c. Rainbow tables are designed to enhance the search capability of many digital forensics examination tools.

    d. Rainbow tables provide a scoring system for probable search terms.

15. The likelihood that a brute-force attack can succeed in cracking a password depends heavily on the password length. True or False?

16. If an application uses salting when creating passwords, what concerns should a forensics examiner have when attempting to recover passwords?

    a. There are no concerns because salting doesn't affect password-recovery tools.

    b. Salting can make password recovery extremely difficult and time consuming.

    c. Salting applies only to OS startup passwords, so there are no serious concerns for examiners.

    d. The effect on the computer's CMOS clock could alter files' date and time values.

17. Block-wise hashing has which of the following benefits for forensics examiners?

    a. Allows validating sector comparisons between known files

    b. Provides a faster way to shift bits in a block or sector of data

    c. Verifies the quality of OS files

d. Provides a method for hashing sectors of a known good file that can be used to search for data remnants on a suspect's drive

Hands-On Projects

Create a *Work*\Chap09\Projects folder on your system before starting these projects; it's referred to as your "work folder" in steps. Download to this work folder any files in this chapter's downloads section on the student companion site for this book.

Hands-On Project 9-1.

In this project, you perform bit-shifting on a file and verify that it can be restored.

1. Start Notepad and type the following in a new text document: **This document contains very sensitive information. We do not want the competition to be able to read it if they intercept the message**.
2. Save the file as **correspondence.txt** in your work folder, and then exit Notepad.
3. Start WinHex, using the **Run as administrator** option. (If necessary, when the UAC message box opens, click **Yes**.) Open the correspondence.txt file.
4. In the in-chapter activity, you used the left and right shift options. For this project, you use the Circular left rotation option in the Modify Block Data dialog box. (*Note*: Because this text file is ASCII, returning it to a readable state takes eight circular left rotations.) Click **Edit**, **Select All** from the menu.
5. Click **Edit**, **Modify Data** from the menu. In the Modify Block Data dialog box, click the **Circular left rotation** option button, and then click **OK**.
6. Save the file as **correspondence1.txt** , and exit WinHex.
7. Restart WinHex, and open **correspondence1.txt** . Click **Edit, Select All** from the menu.
8. With the file's contents highlighted, click **Edit, Modify Data** from the menu. In the Modify Block Data dialog box, click the **Circular left rotation** option button, if necessary, to rotate the bits, and then click **OK**. Repeat this step seven times to verify that you can recover the data.
9. When you have recovered the text to its readable state, save it as **correspondence2.txt** .
10. Write a short paper stating whether you think this method is a reliable one for encrypting. Leave WinHex running for the next project.

Hands-On Project 9-2.

As part of the validation process, a forensic image file should be analyzed to verify that it's a true copy, as you saw in the in-chapter activity in "Validating with Digital Forensics Tools." For image files created in the Expert Witness .E01 format, the original hash value is stored in the image file's header. In this project, you examine a recent copy of the hard drive from Bob Swartz's (the engineering manager at Superior Bicycles, Inc.) computer to calculate MD5 hashes of sensitive files. The purpose is to have the hash values available for examinations of other disks you might encounter in this investigation. You use the hash database created in the in-chapter activity for InChap09.dd. You perform the following tasks:

- Use Autopsy's E01 Verifier feature to verify the GCFI-bs01.E01 file.
- Identify Special Project-A files and add them to the Special Project-A hash database.

For this project, you need the Ch09ProjDataFiles.exe file, which you downloaded and copied to your work folder. In File Explorer, double-click this file to uncompress its contents. You use

GCFI-bs01.E01 for this project. Follow these steps:

1. Start Autopsy for Windows. Click the **Create New Case** button. In the New Case Information window, enter **Proj0902** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**. In the Additional Information window, type **Proj0902** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.
2. In the Select Data Source window, click the **Browse** button next to the "Browse for an image file" text box, navigate to your work folder and click the **GCFI-bs01.E01** file, and then click **Open**. Click **Next**.
3. In the Configure Ingest Modules window, click the **Hash Lookup** check box. In the "Select known hash databases to use" list box, click to clear the **NISTFile- *nnn* m.txt-md5** check box, and then click the **Special Project-A** check box. Under the Hash Lookup check box, click the **File Type Identification**, **Keyword Search**, **PhotoRec Carver**, and **E01 Verifier** check boxes. Click the **Calculate MD5 even if no hash database is selected** check box, and click **Next** and then **Finish**.
4. When Autopsy finishes its analysis, go to the Tree Viewer pane, and expand **Results**, **Hashset Hits** to see the matching files found in the GCFI-bs01.E01 image.
5. In the Result Viewer pane, Ctrl+click all files. Right-click this selection, point to **Tag Results** and **Quick Tag**, and click **Special Project-A**.
6. Click **Generate Report** at the top. In the Generate Report window, click the **Results - Excel** option button in the Report Modules section, and then click **Next**. In the Configure Artifact Reports window, click the **Tagged Results** option button, click the **Special Project-A** check box, and then click **Finish**.
7. When the report has been generated, click the **Results - Excel** pathname in the Report Generation Progress window. In the Excel file, examine the contents of the Tagged Files sheet. Scroll to column I, labeled Hash, and review the hash values. When you're finished, save the Excel file as **Proj0902-Report** in your work folder.
8. Click **Close Case**, and leave Autopsy running for the next project.

Hands-On Project 9-3.

For this project, you collect and add hash values from the GCFI-bs01.E01 image to the Special Project-A hash database. The files of interest are documents associated with special projects for Superior Bicycles, Inc. Follow these steps:

1. Start Autopsy for Windows. Click the **Create New Case** button. In the New Case Information window, enter **Proj0903** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**. In the Additional Information window, type **Proj0903** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.
2. In the Select Data Source window, click the **Browse** button next to the "Browse for an image file" text box, navigate to your work folder and click the **GCFI-bs01.E01** file, and then click **Open**. Click **Next**.
3. In the Configure Ingest Modules window, click the **Hash Lookup** check box. In the "Select known hash databases to use" list box, click to clear the **NISTFile- *nnn* m.txt-md5** check box, and then click the **Special Project-A** check box. Under the Hash Lookup check box, click the **File Type Identification**, **Keyword Search**, **PhotoRec Carver**, and **E01 Verifier** check boxes. Click the **Calculate MD5 even if no hash database is selected** check box, and click **Next** and then **Finish**.
4.

When Autopsy finishes its analysis, go to the Tree Viewer pane, expand **Data Sources**, and navigate to the path **GCFI-bs01.E01\Users\Bob Swartz\Documents\Special Project A\Design Specs**.

5. In the Result Viewer pane, Ctrl+click all Special Project A files with a .docx extension. (Ignore files beginning with the tilde (~) character or files with .tmp and .docx-slack extensions.) Right-click this selection, point to **Tag File** and **Quick Tag**, and click **Special Project-A**.

6. Click **Generate Report** at the top. In the Generate Report window, click the **Results - Excel** option button in the Report Modules section, and then click **Next**. In the Configure Artifact Reports window, click the **Tagged Results** option button, click the **Special Project-A** check box, and then click **Finish**.

7. When the report has been generated, click the **Results - Excel** pathname in the Report Generation Progress window, and then click **Close**. In the Excel file, examine the contents of the Tagged Files sheet. Scroll to column I, labeled Hash, and review the hash values. When you're finished, save the Excel file as **Proj0903-Report** in your work folder. Leave this file open for the next steps.

8. In column I in the Tagged Files sheet, copy the four MD5 hash values in rows 2 through 5.

9. Click **Tools, Options** from the Autopsy menu, and in the Options window, click the **Hash Databases** icon.

10. In the Hash Databases list box, click **Special Project-A**, and in the Hash Database Information section, click **Add Hashes to Database**. In the Add Hashes to Database dialog box, click **Paste From Clipboard**, click **Add Hashes to Database**, and click **OK** twice.

11. Exit Excel, click **Close Case** in Autopsy, and then leave Autopsy running for the next project.

Hands-On Project 9-4.

Similar to **Hands-On Projects 9-2** and 9-3, you collect and insert hash values from the forensic image file GCFI-dr01.E01 in a new hash database. The files of interest are document files containing personal identification information for Superior Bicycles, Inc. employees. Follow these steps:

1. Start Autopsy for Windows, if necessary. Click the **Create New Case** button. In the New Case Information window, enter **Proj0904** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**. In the Additional Information window, type **Proj0904** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

2. In the Select Data Source window, click the **Browse** button next to the "Browse for an image file" text box, navigate to and click your work folder and the **GCFI-dr01.E01** file, and then click **Open**. Click **Next**.

3. In the Configure Ingest Modules window, click the **Hash Lookup** check box. In the "Select known hash databases to use" section, click the **NISTFile- *nnn* m.txt-md5** check box, and then click to clear the **Special Project-A** check box. On the left, click the **File Type Identification**, **Keyword Search**, and **E01 Verifier** check boxes. Under "Select known BAD hash databases to use," click the **Calculate MD5 even if no hash database is selected** check box, and then click **Next** and **Finish**.

4. When Autopsy finishes its analysis, go to the Tree Viewer pane, and click to expand **Data Sources**. Navigate to the path **GCFI-dr01.E01\Users\Denise Robinson\Documents\Special Project A\Personnel Records**.

5. In the Personnel Records folder, examine the contents of the **Investigations** subfolder. In the Result Viewer pane, Ctrl+click any files with the extensions **.ods** , **.odt** , and **.pdf** . Ignore all files beginning with the tilde (~) character and those with the extensions .ods-slack, .odt-slack, and .pdf-slack.

6. Right-click the highlighted files, point to **Tag File**, and click **Tag and Comment**. In the Create Tag dialog box, click the **New Tag Name** button, type **Superior-Personnel-Records** in the Tag Name text box, and then click **OK** twice.

7. In the Personnel Records folder, examine the contents of the **Official Records** subfolder. In the Result Viewer pane, click to select any files with the extensions **.ods** , **.odt** , and **.pdf** . (Ignore all files beginning with the tilde (~) character and those with the extensions .ods-slack, .odt-slack, and .pdf-slack.)

8. Right-click the highlighted files, point to **Tag File** and then **Quick Tag**, and click **Superior-Personnel-Records**. Click **OK** twice.

9. Repeat **Steps 7** and 8 for the **Preliminary Records** subfolder.

10. Click **Generate Report** at the top. In the Generate Report window, click the **Results - Excel** option button in the Report Modules section, and then click **Next**. In the Configure Artifact Reports window, click the **Tagged Results** option button, click the **Superior-Personnel-Records** check box, and then click **Finish**.

11. In the Report Generation Progress Complete window, click the **Results - Excel** link to open the Excel report. Examine the contents of the Tagged Files sheet, scroll to column I labeled Hash, and then save the file as **Proj0904-Report** in your work folder. Leave this file open for the next steps.

12. Navigate to column I again, and copy the four MD5 hash values in rows 2 through 29.

13. Click **Tools, Options** from the Autopsy menu, and in the Options window, click the **Hash Databases** icon.

14. Under the Hash Databases list box, click the **New database** button. In the Create Hash Database dialog box, type **Superior-Personnel-Records** in the Hash Set Name text box, and click **Save as**. In the Save dialog box, click **Save**, and in the Create Hash Database dialog box, click **Known Bad**, and then click **OK**.

15. In the Hash Database Information section, click **Add Hashes to Database**. In the Add Hashes to Database dialog box, click **Paste From Clipboard**, click **Add Hashes to Database**, and click **OK** twice.

16. When the report has been generated, click the **Results - Excel** pathname in the Report Generation Progress window, then click **Close**. In the Excel file, examine the contents of the Tagged Files sheet. Scroll to column I, labeled Hash, and review the hash values. When you're finished, save the Excel file as **Proj0904-Report** in your work folder. Leave this file open for the next steps.

17. In column I in the Tagged Files sheet, copy the MD5 hash values in rows 2 through 29.

18. Click **Tools, Options** from the Autopsy menu, and in the Options window, click the **Hash Databases** icon.

19. In the Hash Databases list box, click **Superior-Personnel-Records**, and in the Hash Database Information section, click **Add Hashes to Database**. In the Add Hashes to Database dialog box, click **Paste From Clipboard**, click **Add Hashes to Database**, and click **OK** twice.

20. Exit Excel, and in Autopsy, click **Close Case**. Click **Close** again in the Welcome window, and then click **Case** and **Exit**.

Case Projects

Case Project 9-1.

As part of the duties of a digital forensics examiner, creating an investigation plan is a standard practice. Write a paper that describes how you would organize an investigation for a potential fraud case. In addition, list methods you plan to use to validate the data collected from drives and files, such as Word and Excel, with hashes. Specify the hash algorithm you plan to use, such as MD5 or SHA-1.

Case Project 9-2.

Several graphics files were transmitted via e-mail from an unknown source to a suspect in an ongoing investigation. The lead investigator gives you these graphics files and tells you that at least four messages should be embedded in them. Use your problem-solving and brainstorming skills to determine a procedure to follow. Write a short report outlining what to do.

Case Project 9-3.

A drive you're investigating contains several password-protected files and other files with headers that don't match the extension. Write a report describing the procedures for retrieving the evidence with some of the forensics tools and hexadecimal editors discussed in this chapter and **Chapter 8**. Explain how to identify the file headers and determine how their extensions are mismatched. Then discuss what techniques and tools you can use for recovering passwords from the protected files.

Case Project 9-4.

With improvements in cryptanalysis, quantum computing methods are now used. Review three to five current articles discussing the use of quantum computing for password cracking. Write a one-page to two-page report summarizing the advantages and possible limitations of quantum computing for this purpose.

Chapter 10. Virtual Machine Forensics, Live Acquisitions, and Network Forensics

After reading this chapter and completing the exercises, you will be able to:

- Explain standard procedures for conducting forensic analysis of virtual machines
- Describe the process of a live acquisition
- Explain network intrusions and unauthorized access
- Describe standard procedures in network forensics and network-monitoring tools

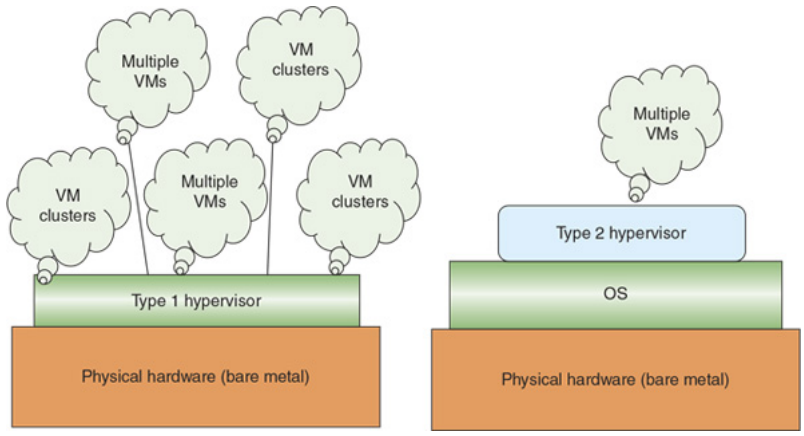
This chapter explores procedures for virtual machine forensics, live acquisitions, and network forensics. You learn about virtualization and virtual machine components and see how to detect that a virtual machine has been set up on a host computer and how to acquire an image of a virtual machine. Network forensics enable you to determine how an intruder gained access to a network's resources and information, and you use live acquisitions to capture an image while a machine is running, which is necessary in many situations, such as when you're concerned about losing data if a system is shut down. For these procedures, you need to understand how to analyze RAM and network traffic.

An Overview of Virtual Machine Forensics

Virtual machines are now common for both personal and business use, so forensics investigators need to know how to analyze them and use them to analyze suspect drives and systems containing malware. Later in this chapter, you use virtual machines installed on a USB drive to perform live acquisitions on suspect drives.

As you've learned, virtual machines (VMs) help offset hardware costs for companies; in many companies, even full networks are virtual, which reduces costs substantially. VMs are also handy when you want to run legacy or uncommon OSs and software along with the other software on your computer. The software that runs virtual machines is called a "hypervisor." There are two types of hypervisors: type 1 and type 2. A **type 1 hypervisor** runs on "bare metal," meaning it loads on physical hardware and doesn't require a separate OS, although many type 1 hypervisors incorporate Linux-based operating systems (explained later in "Working with Type 1 Hypervisors"). Literally thousands of VMs can be hosted on a single type 1 hypervisor and many more on a cluster of these hosts. A **type 2 hypervisor** rests on top of an existing OS, such as Windows, Linux, or macOS. Figure 10-1 illustrates the difference between the two.

Figure 10-1.



Type 1 and type 2 hypervisors

With rising hardware and software costs, companies have to pay careful attention to making the best investments for IT infrastructures. New versions of software require more RAM, hard drive space, and resources, and redeploying new versions of OSs and applications two or three times a year isn't cost effective. Enter virtual machines, which make it possible for one server to support an entire department or company. With virtual machines in use, a well-equipped workstation or reasonably priced server can take care of all a small company's needs. For all these reasons, virtual networks are now a standard part of doing business ("Virtual Forensics: A Discussion of Virtual Machines Related to Forensic Analysis," B. Shavers, 2008, www.forensicfocus.com/downloads/virtual-machines-forensics-analysis.pdf). Large companies might add rack servers that can host literally thousands of VMs. In Chapter 13, you see the challenge VMs pose in cloud forensics.

Type 2 hypervisors are usually the ones you find loaded on a suspect machine. Type 1 hypervisors are typically, but not exclusively, loaded on servers or workstations with a lot of RAM and storage. The next sections describe these hypervisors in more detail. Because users tend to be more familiar with type 2 hypervisors, you examine them first before moving on to type 1 hypervisors.

Type 2 Hypervisors

Type 2 hypervisors can be used on a laptop, a desktop, or even a tablet to simulate an OS environment, such as running a Windows Server 2016 VM on a Linux host. Companies often use these hypervisors to run legacy hardware that works only with a specific OS, such as Windows XP. Although VMs should be kept on a separate network, this setup can be a useful solution if hardware replacement costs are beyond a company's budget.

Before attempting to install a type 2 hypervisor, you need to enable virtualization in the BIOS before attempting to create a VM. Intel **Virtualization Technology (VT)** has responded to the need for security and performance by producing different CPU designs. With one design, you must go into the BIOS to enable virtualization (which is a hardware function, not an OS function). The other CPU design doesn't support virtualization. To determine whether your CPU supports virtualization, first look in Control Panel to find out what type of CPU your device has, and then do a search on this particular CPU at http://ark.intel.com/Products/VirtualizationTechnology. Instruction sets called **Virtual Machine Extensions (VMX)** are necessary to use virtualization; without these instruction sets, virtualization software doesn't work. (For a more detailed explanation, refer to www.intel.com/content/www/us/en/virtualization/virtualization-technology/intel-virtualization-technology.html.) Intel has also developed Virtualization Technology for memory virtualization, I/O virtualization, graphics virtualization, and virtualization of network and security functions. The following sections give you an overview of the most widely used type 2 hypervisors.

Note

As a result of the security risk of people using mobile devices to connect to company networks, a new approach to BYOD was needed. The original limitation on mobile devices and hypervisors was hardware. Most embedded devices and mobile devices used ARM technology, which didn't support virtualization. With advances in the underlying hardware, this is no longer the case, however. Both type 1 and type 2 hypervisors can be supported on mobile devices. Several approaches are possible, including a CPU virtualization model, an interrupt virtualization model, and a network virtualization model. For an in-depth discussion, see "A Survey of Mobile Device Virtualization: Taxonomy and State of the Art," *ACM Computing Surveys* 49:1, Article 1 (April 2016, Shuja J. et al).

Parallels Desktop

Parallels Desktop (www.parallels.com/products/desktop/) was created for Macintosh users who also use Windows applications. It runs both legacy and current Windows OSs as well as Linux. Unlike most type 2 hypervisors, it isn't free but is generally under US$100.

KVM

The KVM (Kernel-based Virtual Machine; www.linux-kvm.org/page/Main_Page) hypervisor is for the Linux OS. This open-source hypervisor enables you to choose between an Intel and an AMD CPU and to run Linux or Windows VMs. It's now included as part of most Linux kernels. Like many type 2 hypervisors, it supplies virtualized hardware, such as graphics cards and network adapters. The version from Red Hat deploys it as a type I hypervisor.

Microsoft Hyper-V

Microsoft began its venture into virtualization with Virtual PC, which allowed you to create VMs that could run non-Windows OSs. Its new hypervisor is built into Windows 10, and unlike most programs, it isn't downloaded. To install it, go to Windows PowerShell and enter Enable-WindowsOptionalFeature -Online -FeatureName:Microsoft-Hyper-V -All. (This command doesn't work in the Home Edition of Windows, however.) After it's installed, you can create virtual machines in Hyper-V Manager and create a network for VMs to access the Internet.

VMware Workstation and Workstation Player

VMware Workstation (www.vmware.com/products/workstation) is a solid workhorse, and although the standard version isn't free, a trial version is available. Take a look at some of its features:

- Can be installed on almost any device, including tablets
- Can install Microsoft Hyper-V Server on it
- Can create encrypted VMs
- Capable of supporting up to 16 CPUs, 8 TB of storage, and 20 virtual networks

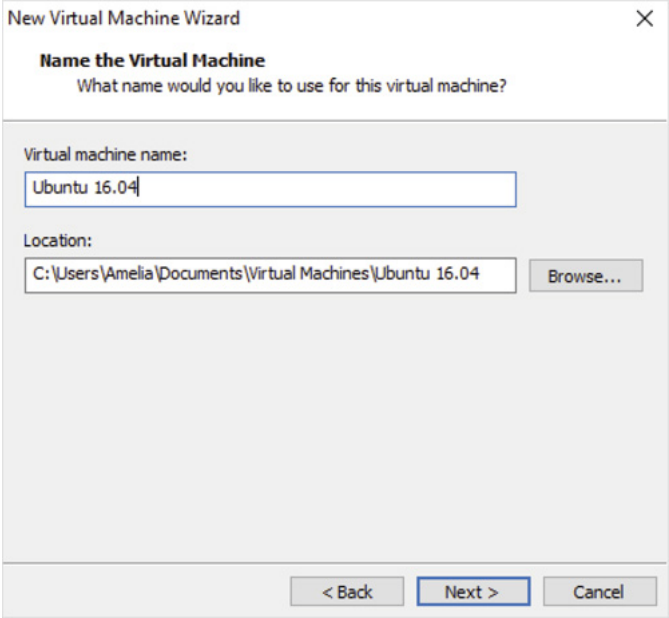
Note

Most current hypervisors can encrypt VMs to send sensitive information to clients. They can also be used to send new or proprietary software for testing to clients.

Older versions of VMware Player could run only VMs that had already been created. Newer versions, however, allow you to create and run VMs but not connect to other devices. You can download VMware Workstation and Workstation Player from the VMware Web site (www.vmware.com). When installing VMware Workstation Player, be sure to select the option for installing VMware Tools, which adds sharing folders with the host, dragging and dropping, and other features to make working with VMs easier.

Figure 10-2 shows the default location of files for a Windows installation of VMware Workstation Player. On a Linux installation, the files are in the /var/lib/vmware/virtual machines directory. Table 10-1 lists some files associated with VMware. For more information on VMware Workstation, go to www.vmware.com/products/workstation.html.

Figure 10-2.



Source: VMware, www.vmware.com

The default location of VMware Workstation Player files

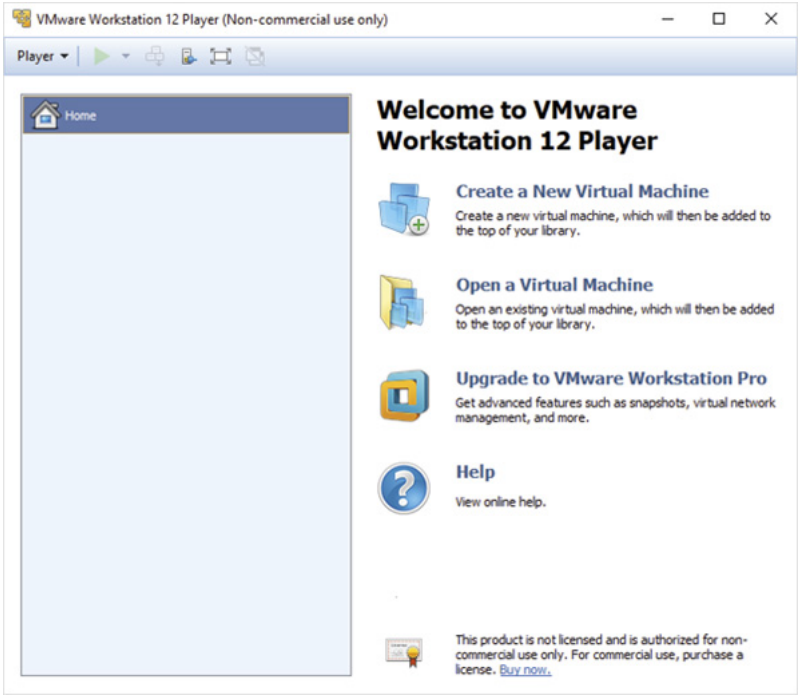
Table 10-1. Files Associated with VMware

File extension	Description
.vmx	Stores configuration files
.log	Contains logs of information such as when a VM was powered off, virtual appliances added, and so on
.nvram	Keeps track of the state of a VM's BIOS
.vmdk	Stores the virtual hard drive's contents
.vmem	Stores VM paging files, which serve as RAM
.vmsd	Contains information about snapshots

Source: "Using VMware Workstation - VMware Workstation 12," 2016, https://docs.vmware.com/en/VMware-Workstation-Player/12.0/workstation-player-12-windows-user-guide.pdf

After VMware Workstation Player is installed, you see the opening window shown in **Figure 10-3**. You can create a VM, open an existing VM, or upgrade to VMware Workstation.

Figure 10-3.



Source: VMware, www.vmware.com

The VMware Workstation Player opening window

VirtualBox

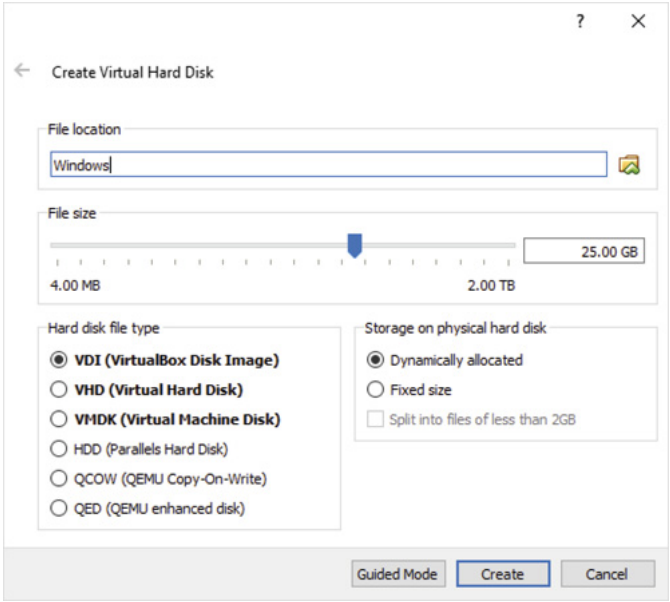
Oracle VirtualBox (www.virtualbox.org) supports all Windows and Linux OSs as well as Macintosh and Solaris. This shareware can be downloaded and installed on both Windows and Linux host systems. Table 10-2 shows the file types associated with VirtualBox.

Table 10-2. Files associated with VirtualBox

File extension	Description
.ova or .ovf	File used to create a virtual machine; OVF stands for "Open Virtualization Format"
.vdi	Disk image file
.r0	Default libraries
.vbox	Saved settings of virtual hard drives
.vbox-extpack	Plug-ins
.vbox-prev	Backups of VMs
.xml-prev	Backups of XML settings
.log	Log files containing information such as a VM being powered on and off, whether it's in hibernation mode, virtual appliances added, and so on

As with most other type 2 hypervisors, you can select different virtual hard drive types when you're creating a VM (see **Figure 10-4**). VirtualBox, in Expert Mode, even allows selecting types associated with other applications, such as the VMware VMDK type or the Parallels HDD type. Keep in mind, however, that virtual machines created with one type 2 hypervisor might not be able to be read by another. For example, VMware doesn't read the Parallels format. Later in the chapter, you learn that some virtual hard drive types can't be mounted as a virtual drive by forensics software, such as Autopsy, OSForensics, and FTK Imager.

Figure 10-4.

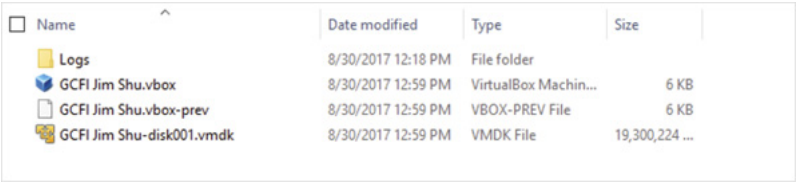


Source: Oracle VirtualBox, www.virtualbox.org

Types of virtual hard drives

Type 2 hypervisors also come with templates for different operating systems. For example, if the VM's filename includes the word "Ubuntu," the hypervisor assumes it's running a 64-bit Linux OS. After a VM has been created, several files are associated with it, as you've seen in **Tables 10-1** and 10-2. Figure 10-5 shows some files associated with a VM running Fedora Linux. The .vbox file stores settings for the virtual hard drive, the .vbox-prev file contains backups of the VM, and the .vhd file contains the VM's virtual hard drive. There's also a folder for log files.

Figure 10-5.



Name	Date modified	Type	Size
Logs	8/30/2017 12:18 PM	File folder	
GCFI Jim Shu.vbox	8/30/2017 12:59 PM	VirtualBox Machin...	6 KB
GCFI Jim Shu.vbox-prev	8/30/2017 12:59 PM	VBOX-PREV File	6 KB
GCFI Jim Shu-disk001.vmdk	8/30/2017 12:59 PM	VMDK File	19,300,224 ...

Source: Oracle VirtualBox, www.virtualbox.org

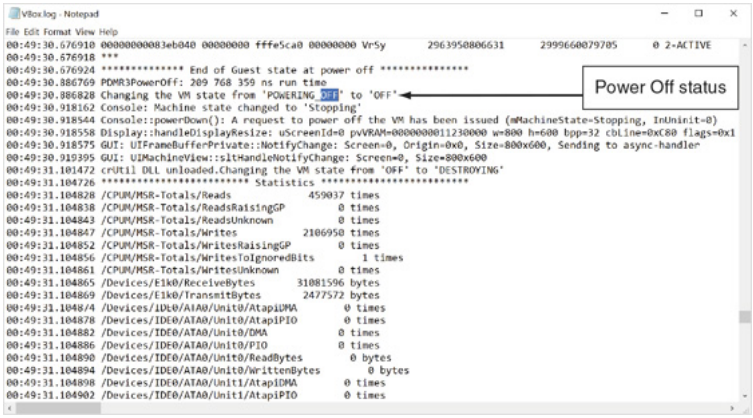
VM files in VirtualBox

Conducting an Investigation with Type 2 Hypervisors

On the surface, an investigation involving virtual machines doesn't differ much from a standard investigation. You begin by acquiring a forensic image of the host computer (the physical machine the VM runs on) as well as network logs. By linking the VM's IP address to log files, you might be able to determine what Web sites the VM accessed (assuming it's bridged with a separate IP from the host). After acquiring a forensic image of the host, export associated VM files, such as the ones listed in Tables **10-1** and 10-2. A VM shares the host's physical devices, such as DVD/CD players and USB drives, and can access files from peripheral devices and shared folders.

Detecting whether virtual machines are on a host computer can be challenging for digital investigators. On a Windows host, you usually look in the Users or Documents folder. On a Linux host, the files might be in /usr/bin/software-center or another folder in the /usr directory. Files associated with VMs, such as log files, should be extracted and examined to determine the crime or incident's timeline and to find relevant information, such as Web sites and network files that were accessed as well as downloads that occurred from the VM's IP address, which might include penetration-testing software or malware. Figure 10-6 shows part of a log file, including a VM powering off and other activities.

Figure 10-6.



Source: Oracle VirtualBox, www.virtualbox.org

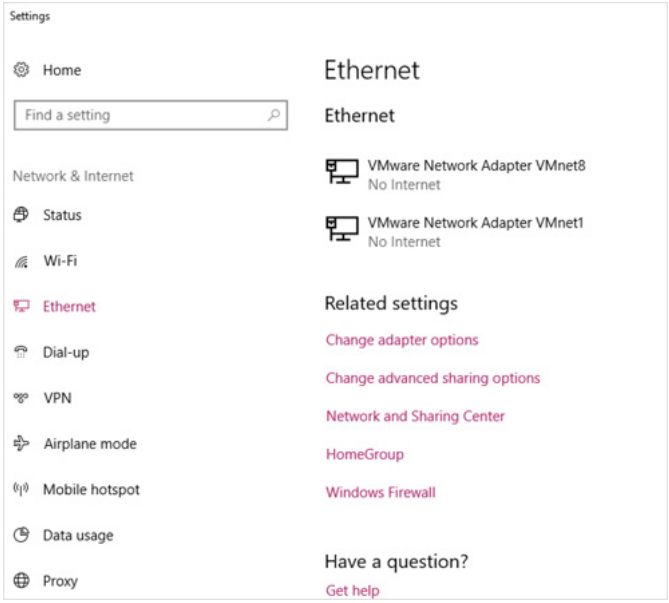
A VM log file

Note

Older OSs, such as Windows XP, often have a My Virtual Machines folder.

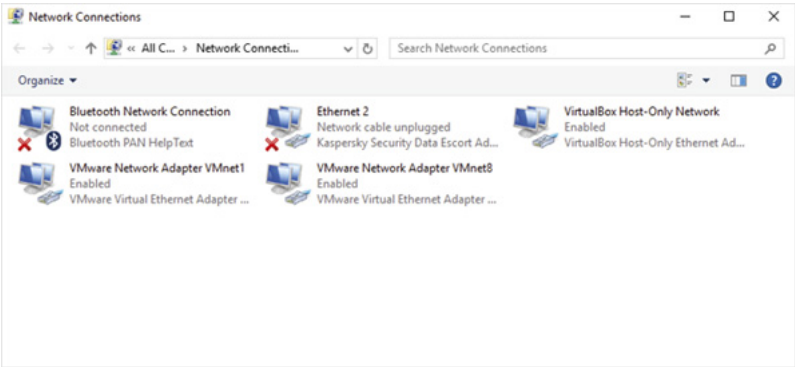
The next step is to check the host's Registry for clues that VMs have been installed or uninstalled. For example, the HKEY_CLASSES_ROOT Registry key contains associations for file extensions. If you see one of the file extensions listed in Tables **10-1** and 10-2, you know to search for a VM. Another clue to a VM being installed is the existence of a virtual network adapter. Figure 10-7 shows the Ethernet connections on a Windows 10 computer, which can be opened by clicking Start, Settings, Network & Internet. Clicking "Change adapter options" displays available network connections (see Figure 10-8). To see all network adapters on a system, you can also use the Windows ipconfig or Linux ifconfig command. In Windows PowerShell, you can also use the Get-VM cmdlet and pipe the output to the Get-VMNetworkAdapter cmdlet:

Figure 10-7.



Ethernet Connections on a Windows 10 computer

Figure 10-8.

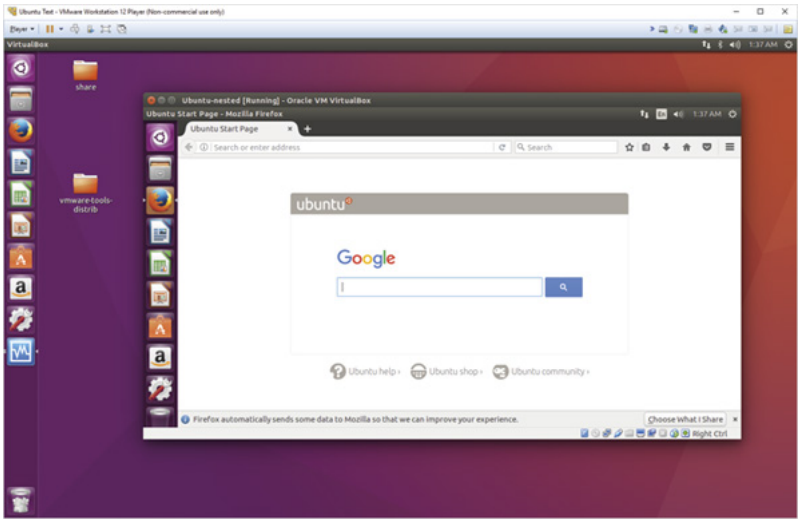


Viewing network connections

In VirtualBox, six types of virtual network adapters are possible, such as AMD and Intel Pro adapters. Refer to the user documentation for hypervisor software to find the names of virtual adapters to look for.

In addition to searching for network adapters, you need to determine whether USB drives have been attached to the host because they could have live VMs running on them. These VMs might have been used to access files and then disconnected without installing anything on the host. A VM can also be nested inside other VMs on the host machine or a USB drive (see **Figure 10-9**). Some newer Windows systems log when USB drives are attached, but there are other ways to determine whether this happened. After imaging the host's drive, search the Windows Registry or the system log files.

Figure 10-9.



Source: VMware, www.vmware.com

A VM nested inside another VM

Following a consistent procedure when you're conducting a forensic analysis of VMs is crucial. Here's an overview:

1. Image the host machine.
2. Locate the virtualization software and VMs, using the information you've learned about file extensions and network adapters.
3. Export from the host machine all files associated with VMs, including log files, virtual adapters, and snapshots.
4. Record the hash values of these associated files. Typically, forensics software can perform this task as part of the export function.
5. Next, you can open a VM as an image file in forensics software and create a forensic image of it or mount the VM as a drive and then image it or do a live search.

Live acquisitions of VMs are often necessary because they include all snapshots. A snapshot simply records the state of a VM at a particular moment. However, it's recording only changes in state; it's *not* a complete backup. Many network administrators depend on snapshots when working with VMs in case updates or software installations fail. When you're acquiring an image of a VM file, snapshots might not be included, depending on the software you're using. In this case, you have only the original VM, which might not have any of the changes made to it after it was created. Therefore, doing live acquisitions of VMs is important to make sure snapshots are incorporated.

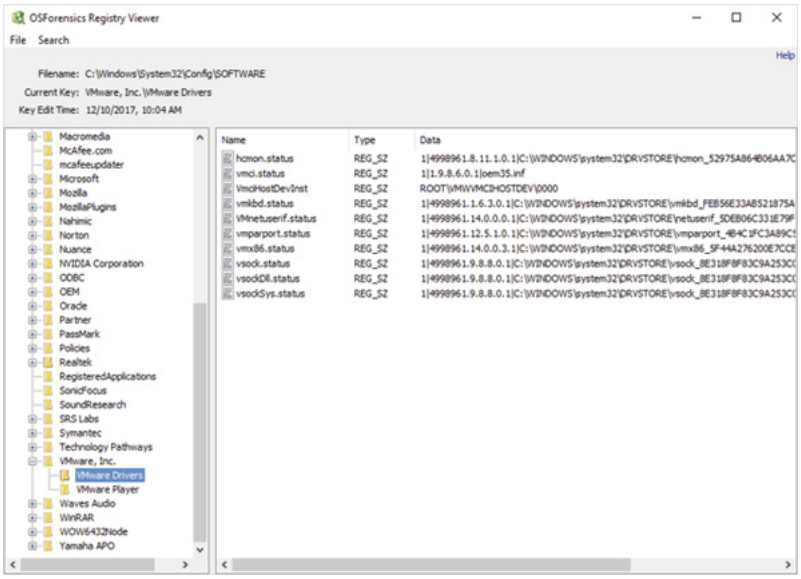
Note

Create a *Work*\Chap10\Chapter work folder on your system. The work folder path shown in screenshots might differ slightly from yours.

If necessary, download VMware Workstation Player from www.vmware.com/products/workstation-player/workstation-player-evaluation.html and install it. You also need FTK Imager Lite, which you installed in Chapter 3. In this activity, you examine your own system for evidence of a VM:

1. Start FTK Imager Lite, and click **File**, **Add Evidence Item** from the menu.
2. In the Select Source dialog box, click the **Logical Drive** option button, and then click **Next**.
3. In the Select Drive dialog box, click the **Source Drive Selection** list arrow, click the drive where you installed VMware Workstation Player, and then click **Finish**.
4. In the upper-left pane, expand the drive where VMware Workstation Player is installed until you see a folder with "[root]" next to it. Expand this folder, and navigate to the **Windows\System32** folder.
5. Right-click the **config** folder and click **Export Files**.
6. In the Browse For Folder dialog box, navigate to and click your work folder, and then click **OK**. Click **OK** in the Export Results dialog box, and then exit FTK Imager.
7. Start OSForensics, and start a new case. When you're prompted for a case folder, create one under your work folder called **InChap10-1**.
8. In the left pane, click **Registry Viewer**, which opens to a listing of Registry keys.
9. Click the **Software** folder in the right pane and click **Open**. In the left pane of the window that opens, expand the **SOFTWARE** node, scroll down, and then expand **C:/VMware, Inc.** and **VMware Drivers**. The drivers shown in Figure 10-10 are examples of what you might see in the Registry as evidence of a VM's presence on the system. Exit OSForensics.

Figure 10-10.



Source: PassMark Software, www.osforensics.com

Viewing VMware in the Registry

After determining that a VM was installed on the host, the next step is finding it. In VMware, you look for files with .vmdk, .vmsd, or .vmx extensions as well as nvram (virtual RAM) files. Next, you need to acquire an image of the VM. Follow these steps:

1. Start your Web browser, and go to www.ubuntu.com/download/desktop. Download an ISO image of Ubuntu Linux 16.04.
2. Start VirtualBox. Create a virtual machine named **Ubuntu 16.04**, and install Ubuntu 16.04 as the guest OS.
3. Start FTK Imager Lite, and click **File, Add Evidence Item** from the menu.

4. In the Select Source dialog box, click the **Image File** option button, and then click **Next**.

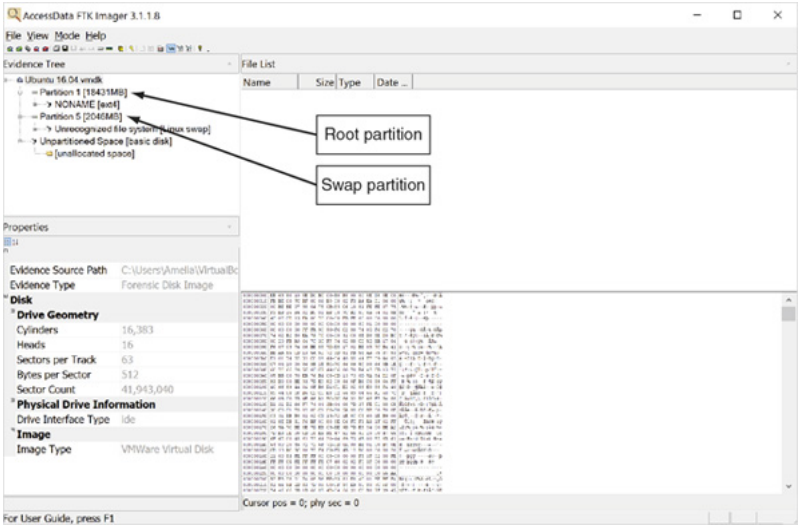
5. Click the **Browse** button, navigate to \users*username*\VirtualBox VMs\Ubuntu 16.04, click the Ubuntu 16.04 folder, and double-click the .vmdk file. Then click Finish.

6. Click to expand the Evidence Tree in the left pane. Typically, in an Ubuntu installation, three partitions are listed: partition 1, containing the root partition; partition 5, containing the swap partition (see **Figure 10-11**); and unallocated space.

Tip

In Linux, the swap partition can be set up as virtual memory. It serves as RAM and might contain important information, such as passwords.

Figure 10-11.



Source: AccessData Group, Inc., www.accessdata.com

Examining a virtual machine's root and swap partitions in FTK Imager Lite

7. Now that you have the virtual machine file open, acquire an image of it by clicking **File**, **Create Disk Image** from the menu.

8. In the Select Source dialog box, click the **Image File** option button, and then click **Next**.

9. In the Select File dialog box, click the **Browse** button, and then navigate to and double-click the **.vmdk** file. Click **Finish**.

10. In the Create Image dialog box, click the Add button in the Image Destination section.

11. In the Select Image Type dialog box, verify that **Raw (dd)** is selected for the image format, and then click **Next**.

12. In the Evidence Item Information dialog box, enter today's date for the evidence number, your name, and any other pertinent information, and then click **Next**.

13. In the Select Image Destination dialog box, click the **Browse** button, navigate to and click your work folder, and then click **OK**. In the Image Filename (Excluding Extension) text box, type **C10InChap-2**. In the Image Fragment Size (MB) text box, type **0** so that FTK Imager Lite doesn't attempt to break the image file into chunks that fit on a CD.

14.

Click **Finish**, and then click **Start** to begin the image acquisition. This process might take a few minutes. When it's finished, exit FTK Imager Lite. You can then examine the image with the tool of your choice.

Note

In this activity, an Ubuntu Linux 16.04 virtual machine is used. You should already have VirtualBox installed.

Other VM Examination Methods

In much the same way that Linux systems mount OSs or peripheral devices, forensics tools can mount VMs as an external drive. FTK Imager, Magnet AXIOM, and OSForensics, for example, have this feature built in. By mounting a VM as a drive, you can make it behave more like a physical computer, which means you can use the standard examination procedures for a static hard drive. Imaging the host machine enables you to retrieve and examine log files as well as associated VM files (for example, .vbox-prev files or .vmdk files) to determine what the VM was used for. You mount a VM as a drive in Hands-On Project 10-1.

Another method of examining a VM is making a copy of its forensic image and opening this copy while it's running—in other words, starting it as a live virtual machine. From a forensics standpoint, this method alters the evidence, so it might be considered a nonstandard approach. However, this method makes it possible to run forensics software on the image to search for clues, such as finding malware and penetration-testing tools. For example, typical users shouldn't have tools such as Metasploit, W3AF, PortSwigger, Cain and Abel, or Wireshark installed on their work machines. These tools can be used to monitor network traffic, conduct brute-force attacks on passwords, perform SQL injections, and so forth. Here are the basic steps for this method:

1. Acquire a forensic image of the VM, and make a copy of this image.
2. Verify the copy's hash value (as you learned in **Chapter 3**), and then start the VM from the copy and explore its contents.
3. Your objective is to find evidence you can extract with a forensics software tool. Look for malware or network-monitoring tools, as discussed previously. Document what you find.
4. Create a snapshot of the running VM, and then power off the VM and exit the virtualization software.
5. Now that you have documented what's on the VM by doing a live examination, follow standard forensics procedures to ensure that the evidence is admissible in court. Open the original forensic image of the VM, and find the malware or tools you discovered in the live analysis. Prepare a written report of your findings.

Using VMs as Forensics Tools

In addition to the many ways VMs can be used, investigators can use them to run forensics tools stored on USB drives. Being able to use a USB drive to acquire an image of a system is convenient. In this section, you set up two VMs on a USB drive, with one running Ubuntu 16.04 and the other running SANS Investigative Forensics Toolkit (SIFT), an open-source VMware appliance with guidelines and procedures for digital investigations. For these activities, you need a 16 GB or larger USB drive. You use VirtualBox because as of this writing, VMware has no portable version.

Note

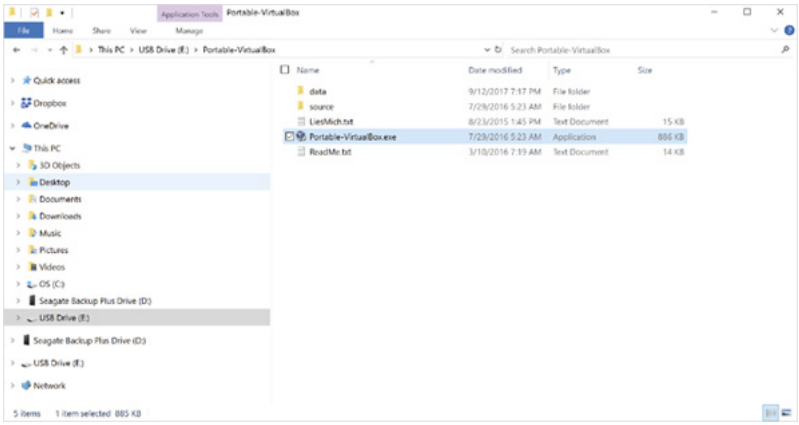
The SANS SIFT currently works only with Ubuntu 16.04, so in the next activity, you download and install this version.

1. Most USB drives still use FAT32, so first reformat the drive as NTFS: Insert the USB drive, open File Explorer, click the USB drive, and do a quick format to NTFS, making sure to set the cluster size to 8192.

2. Start a Web browser, and go to www.vbox.me. Click the **Portable-VirtualBox_v5.0.26-Starter-v6.4.10-Win_all.exe** link. Download the ***.exe** file, and install it on your USB drive.

3. In File Explorer, create a folder on your USB drive called **VirtualMachine VMs**. Next, navigate to your USB drive, and double-click the **Portable-VirtualBox.exe** file (see Figure 10-12). If necessary, click **Yes** in the UAC message box.

Figure 10-12.



Source: Oracle VirtualBox, www.virtualbox.org

Starting Portable-VirtualBox from the USB drive

4. In the main Portable-VirtualBox window, click **File**, **Preferences** from the menu to open the VirtualBox Settings dialog box. In the right pane, click the **Default Machine Folder** list arrow, click the **VirtualMachine VMs** folder you created, and click **OK**.

5. To facilitate the process, copy the **Sift-Workstation-Virtual-Machine-Distro version** folder to your USB drive. Click **File**, **Import Appliance** from the menu. Navigate to the folder you just copied, and click **SIFT3-Distro Version.ovf** . Click **Next** and then **Import**. (*Note*: At first, nothing seems to happen, and then a predicted time of around 13 hours is suggested. However, the process should finish in less than 30 minutes.)

6. In File Explorer, navigate to your USB drive, and open the **VirtualMachine VMs** folder you created. Then open the **vm** subfolder, which should contain .vmdk files. Delete the folder you copied from the hard drive to free up room on the USB drive, and then close File Explorer.

7. In the VirtualBox main window, click the **vm** virtual machine, and then click **Start**. When the virtual machine has started to the SANS SIFT login, type **forensics** for the password and press **Enter**. If you get a terminal window with an error message, simply type **exit** and press **Enter**.

8. You should now be at the main Linux window for SANS SIFT. Notice the available cheatsheets and posters, shown in **Figure 10-13**. Open a few and examine the information. When you're done, click the **Settings** button in the left pane, click **Shut Down**, and click the **Shutdown** button to exit the virtual machine.

Figure 10-13.

Source: Oracle VirtualBox, www.virtualbox.org

The SANS SIFT tools

Working with Type 1 Hypervisors

This section isn't intended as complete coverage of type 1 hypervisors and virtual networks; it's meant to help you understand the impact they have on forensic investigations. Having a good working relationship with network administrators and lead technicians can be extremely helpful in these investigations, particularly when you're a law enforcement officer or work for an outside company.

Type 1 hypervisors are installed directly on hardware, although for testing purposes, you can install them on a VM. Some are freeware, and some are proprietary and quite expensive. The capability of type 1 hypervisors is limited only by the amount of available RAM, storage, and throughput. Most type 1 hypervisors come in different levels, such as free, standard, and enterprise. Each type 1 hypervisor can host from a few to several hundred VMs per host, and the IBM hypervisor can even host thousands of VMs per host. The following are some common type 1 hypervisors:

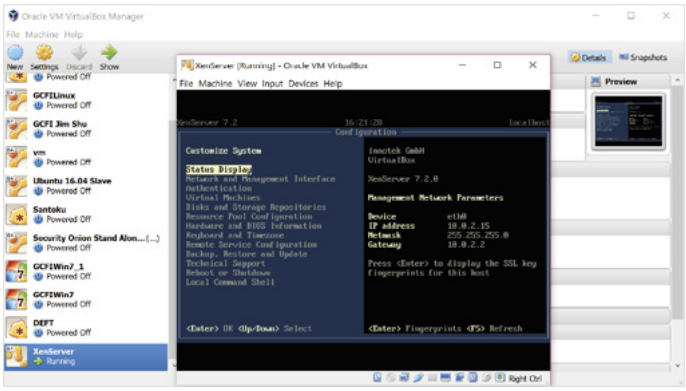
- VMware vSphere (www.vmware.com/products/vsphere.html) in Standard, Enterprise Plus, and Operations Management Enterprise Plus editions
- Microsoft Hyper-V Server 2016 (www.microsoft.com/en-us/evalcenter/evaluate-hyper-v-server-2016)
- XenProject XenServer in a free edition (https://xenserver.org/overview-xenserver-open-source-virtualization/download.html) and a commercial version designed for data centers with a free demo (www.citrix.com/downloads/xenserver/)
- IBM PowerVM (www-03.ibm.com/systems/power/software/virtualization/) in Introductory, Standard, and Enterprise editions
- Parallels Desktop for Mac (www.parallels.com/all-products/)

Training to use these products can be expensive; for example, one week of training on VMware vSphere 6.5 can cost thousands of dollars. To manage these products, you also need a thorough understanding of virtual networks, IP addressing, hardware, and security.

The two most readily available products are Citrix XenServer and VMware ESXi. In this activity, you install XenServer as a VM in VirtualBox:

1. Start your Web browser, and go to https://xenserver.org/overview-xenserver-open-source-virtualization/download.html. Download the free ISO image for XenServer, and make note of where you stored this file.
2. Start VirtualBox, and click the **New** icon. In the dialog box that opens, type **XenServer** for the virtual machine name.
3. Click the **Type** list arrow, and click **Other**. Click the **Version** list arrow, and click **Other/Unknown (64 bit)**. If you aren't using a 64-bit machine, click **Other**. Click **Next**.
4. For the memory size, specify **2048** (or higher, around 25% of your available RAM), and then click **Next**.
5. Click **Create**. The Create Virtual Hard Drive dialog box opens. For the hard drive type, click the **VMDK (Virtual Machine Disk)** option button, and then click **Next**.
6. In the next dialog box, accept the default setting **Dynamically allocated for the hard drive**, and click **Next**. In the File location and size window, change the file size to **46 GB** (or higher), and then click **Create**.
7. In the Oracle VM VirtualBox Manager window, click the **XenServer** VM you just created. Click the **Settings** icon at the top. On the left side, click **Storage**.
8. In the Storage Tree section, click the **CD** icon. On the right side, you should see a CD icon under Attributes to the right of the CD/DVD Drive label. Click the **CD** icon, and click **Choose a virtual CD/DVD disk file**.
9. Navigate to the folder where the XenServer ISO image is stored, click the XenServer-7.2.0-install-cd.iso file, click **Open**, and then click **OK**.
10. In the Oracle VM VirtualBox Manager window, click the **Start** icon, and follow the wizard to install XenServer.
11. If you're prompted to restart, press **Enter**, and wait for your system to finish restarting. Figure 10-14 shows the XenServer VM.

Figure 10-14.



Source: Oracle VirtualBox, www.virtualbox.com

The XenServer VM running in VirtualBox

12. Power off the XenServer VM, and exit VirtualBox.

Performing Live Acquisitions

As you learned in **Chapter 3**, live acquisitions are especially useful when you're dealing with active network intrusions and attacks or if you suspect employees are accessing network areas they shouldn't. Live acquisitions done before taking a system offline are also becoming a necessity because attacks might leave footprints only in running processes or RAM; for example, some malware disappears after a system is restarted. In addition, information in RAM is lost after you turn off a suspect system. However, after you do a live acquisition, information on the system has changed because your actions affect RAM and running processes, which also means the information can't be reproduced. Therefore, live acquisitions don't follow typical forensics procedures.

The problem investigators face is the **order of volatility (OOV)** , which determines how long a piece of information lasts on a system. Data such as RAM and running processes might exist for only milliseconds; other data, such as files stored on the hard drive, might last for years. The following steps show the general procedure for a live acquisition, although investigators differ on exact steps:

1. Create or download a bootable forensic CD or USB drive, and test it before using it on a suspect drive. If the suspect system is on your network and you can access it remotely, add the necessary network forensics tools to your workstation. If not, insert the bootable forensics CD/USB drive in the suspect system.
2. Make sure you keep a log of all your actions; documenting your actions and reasons for these actions is critical.
3. A network drive is ideal as a place to send the information you collect. If you don't have one available, connect an external drive to the suspect system for collecting data. Be sure to note this step in your log.
4. Next, copy the physical memory (RAM). WindowsScope (www.windowsscope.com), Magnet AXIOM, OSForensics, FTK Imager, and similar tools can copy the RAM for you.
5. The next step varies, depending on the incident you're investigating. With an intrusion, for example, you might want to see whether a rootkit exists by using tools such as Malwarebytes Anti-Rootkit (www.malwarebytes.com/antirootkit/) or PC Hunter (www.bleepingcomputer.com/download/pc-hunter/). You can also access the system's firmware to see whether it has changed, create an image of the drive over the network, or shut down the system and make a static acquisition later.
6. Be sure to get a forensically sound digital hash value of all files you recover during the live acquisition to make sure they aren't altered later.

Performing a Live Acquisition in Windows

Several tools are available for capturing RAM. For example, Mandiant Memoryze (www.fireeye.com/services/freeware/memoryze.html) lists all open network sockets, including those hidden by rootkits. It also works on both 32-bit and 64-bit systems. Belkasoft RamCapturer (https://belkasoft.com/ram-capturer) is available in 32-bit and 64-bit versions and can run from a USB drive. Another tool is Kali Linux, the updated version of BackTrack (covered in more detail in Chapter 7). It still has more than 300 tools, but outdated or obsolete ones have been eliminated. Kali Linux contains password crackers, network sniffers, and freeware forensics tools. For more details, go to www.kali.org/official-documentation/.

GUI tools are easy to use, but keep in mind that they often require a lot of system resources. In addition, some GUI tools might get false readings in Windows OSs, and command-line tools often give you more control. For these reasons, you should become familiar with some command-line forensics tools, such as Sleuth Kit, introduced in **Chapter 7**. Covering the more

than 300 available command-line tools is beyond the scope of this book, but investigating them on your own is highly recommended.

Network Forensics Overview

Network forensics is the process of collecting and analyzing raw network data and tracking network traffic systematically to ascertain how an attack was carried out or how an event occurred on a network. Because network attacks are on the rise, there's more focus on this field and an increasing demand for skilled technicians. Labor forecasts predict a shortfall of network forensics specialists in law enforcement, legal firms, companies, and universities.

When intruders break into a network, they leave a trail. Being able to spot variations in network traffic can help you track intrusions, so knowing your network's typical traffic patterns is important. For example, if a company's peak use is typically between 6 a.m. and 6 p.m., that's when you should expect spikes. If a usage spike occurs during the night, the network administrator should recognize it as unusual activity and take steps to investigate it.

Network forensics can also help you determine whether a network is truly under attack or a user has inadvertently installed an untested patch or custom program, for example. A lot of time and resources can be wasted determining that a bug in a custom program or an untested open-source program caused an "attack."

The Need for Established Procedures

Network forensics examiners must establish standard procedures for how to acquire data after an attack or intrusion incident. Typically, network administrators want to find compromised machines, get them offline, and restore them as quickly as possible to minimize downtime. However, taking the time to follow standard procedures is essential to ensure that all compromised systems have been found and to ascertain attack methods in an effort to prevent them from happening again.

Procedures must be based on an organization's needs and should complement the network infrastructure. The increase in cybercrimes has prompted many groups to begin compiling procedures and protocols to follow when a network intrusion occurs. Network administrators need to learn how to stop intruders and determine how they got in; what they copied, altered, or deleted; and whether they're still on the network. To address these needs, NIST created "Guide to Integrating Forensic Techniques into Incident Response" (http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf, 2006). In addition, the paper "Identifying Critical Features for Network Forensics Investigation Perspectives (Adeyemi, Razak, and Azhan, http://arxiv.org/ftp/arxiv/papers/1210/1210.1645.pdf, 2012) explores network investigations from the perspectives of the military, law enforcement, and industry. A group from India has also come up with a general framework for network forensics (www.ijcaonline.org/journal/number11/pxc387408.pdf, 2010). These approaches are discussed in more detail in "Developing Procedures for Network Forensics."

Securing a Network

Network forensics is used to determine how a security breach occurred; however, steps must be taken to harden networks before a security breach happens, particularly with recent increases in network attacks, viruses, and other security incidents. Hardening includes a range of tasks, from applying the latest patches to using a **layered network defense strategy** , which sets up layers of protection to hide the most valuable data at the innermost part of the network. It also ensures that the deeper into the network an attacker gets, the more difficult access becomes and the more safeguards are in place. The National Security Agency (NSA) developed a similar approach, called the **defense in depth (DiD)** strategy. DiD has three modes of protection:

- People

- Technology
- Operations

If one mode of protection fails, the others can be used to thwart the attack. Listing people as a mode of protection means organizations must hire well-qualified people and treat them well so that they have no reason to seek revenge. In addition, organizations should make sure employees are trained adequately in security procedures and are familiar with the organization's security policy. Physical and personnel security measures are included in this mode of protection.

The technology mode includes choosing a strong network architecture and using tested tools, such as intrusion detection systems (IDSs) and firewalls. Regular penetration testing coupled with risk assessment can help improve network security, too. Having systems in place that allow quick and thorough analysis when a security breach occurs is also part of the technology mode of protection.

Finally, the operations mode addresses day-to-day operations. Updating security patches, antivirus software, and OSs falls into this category, as does assessment and monitoring procedures and disaster recovery plans.

Tip

If you're interested in more information on DiD, visit www.nsa.gov/ia/_files/support/defenseindepth.pdf.

Testing networks is as important as testing servers. You need to be up to date on the latest methods intruders use to infiltrate networks as well as methods internal employees use to sabotage networks. In the early and mid-1990s, approximately 70% of network attacks were caused by employees. Since then, this problem has been compounded by contract employees, who often have the same level of network privileges as full-time employees.

In addition, small companies of fewer than 10 employees often don't consider security precautions against internal threats necessary, so they can be more susceptible to problems caused by employees revealing proprietary information to competitors. However, increasing use of the Internet has caused a sharp rise in external threats, so internal and external threats are currently about 50-50.

Developing Procedures for Network Forensics

As you have seen, log files are often examined along with forensic image files collected from devices. To get these files, you need to establish a good working relationship with network administrators and technicians. Network forensics can be a long, tedious process, and unfortunately, the trail can go cold quickly. A standard procedure often used in network forensics is as follows:

1. Always use a standard installation image for systems on a network. This image isn't a bit-stream image but an image containing all the standard applications used. You should also have MD5 and SHA-1 hash values of all application and OS files.
2. When an intrusion incident happens, make sure the vulnerability has been fixed to prevent other attacks from taking advantage of the opening.
3. Attempt to retrieve all volatile data, such as RAM and running processes, by doing a live acquisition before turning the system off.
4. Acquire the compromised drive and make a forensic image of it.

5. Compare files on the forensic image with the original installation image. Compare hash values of common files, such as Win.exe and standard dynamic link libraries (DLLs), and ascertain whether they have changed.

In digital forensics, you can work from the image to find most of the deleted or hidden files and partitions. Sometimes you restore the image to a physical drive so that you can run programs on the drive. In network forensics, you have to restore the drive to see how malware that attackers have installed on the system works. For example, intruders might have transmitted a Trojan program that gives them access to the system and then installed a rootkit, which is a collection of tools that can perform network reconnaissance tasks (using the ls or netstat command to collect information, for instance), keylogging, and other actions.

Reviewing Network Logs

Network logs record traffic in and out of a network. Network servers, routers, firewalls, and other devices record the activities and events that move through them. A common way of examining network traffic is running the tcpdump command-line program (www.tcpdump.org), which can produce hundreds or thousands of lines of records. A sample output is shown here:

```
TCP log from 2017-12-16:15:06:33 to 2017-12-16:15:06:34.
Fri Dec 15 15:06:33 2017; TCP; eth0; 1296 bytes; from
  204.146.114.10:1916 to 156.26.62.201:126
Fri Dec 15 15:06:33 2017; TCP; eth0; 625 bytes; from
  192.168.114.30:289 to 188.226.173.122:13
Fri Dec 15 15:06:33 2017; TCP; eth0; 2401 bytes; from
  192.168.5.41:529 to 188.226.173.122:31
Fri Dec 15 15:06:33 2017; TCP; eth0; 1296 bytes; from
  206.199.79.28:1280 to 10.253.170.210:168;first packet
```

The first line of the output is simply the header. The rest of the lines follow the format *time; protocol; interface; size; source and destination addresses*. Take another look at the second line from the previous output:

```
Fri Dec 15 15:06:33 2017; TCP; eth0; 1296 bytes; from
  204.146.114.10:1916 to 156.26.62.201:126
```

This line shows that data was transmitted on Saturday, December 16, 2017, at 15:06:33. It was a TCP packet sent via the Ethernet 0 interface of 1296 bytes. The packet was sent from 204.146.114.10:1916 to 156.26.62.201:126. In these IP addresses, the numbers after the colon represent the port number.

When viewing network logs, port information can give you clues to investigate. For example, you might notice that a particular IP address is coming in frequently on an unusual port. A receiving port above 1024, for example, should also raise a flag. You can check the Internet Assigned Numbers Authority Web site (www.iana.org/assignments/port-numbers) for a list of assigned port numbers.

Using a network analysis tool such as Wireshark (which you use later in this chapter), you could generate a list of the top 10 Web sites users in your network are visiting. As shown in the following output, the number of bytes being transferred is listed first, followed by the IP address of the site:

```
Top 10 External Sites Visited:
      4897 188.226.173.122
      2592 156.26.62.201
      4897 110.150.70.190
      4897 132.130.65.172
      4897 192.22.192.204
      4897 83.141.167.38
      1296 167.253.170.210
      1296 183.74.83.174
      625 6.234.186.83
      789 89.40.199.255
```

You could also generate a list of the top 10 internal users, as shown:

```
Top 10 Internal Users:
      4897 192.168.5.119
      4897 192.168.5.41
      4897 192.168.5.44
      4897 192.168.5.5
      2401 204.146.114.50
      1296 192.168.5.95
      1296 204.146.114.10
      1296 204.146.114.14
      1296 206.199.79.28
      625 192.168.5.72
```

These network logs can show you patterns, such as an employee transmitting data to or from a particular IP address frequently. Further investigation of the IP address could show that this employee is accessing an online shopping site during company time, for example.

Note

Automated software packages, such as Tripwire (www.tripwire.com), can tell you when suspicious network activity has occurred. Tripwire is an audit control program that detects anomalies in traffic and sends alerts automatically.

As with all investigations, keep preservation of evidence in mind. Your investigation might turn up other companies that have been compromised. In much the same way you wouldn't turn over proprietary company information to become public record, you shouldn't reveal information discovered about other companies. In these situations, the best course of action is to contact the companies and enlist their aid in tracking down network intruders. Depending on the situation, at some point you might have to report the incident to federal authorities.

Using Network Tools

A variety of tools are available for network administrators to perform remote shutdowns, monitor device use, and more. The tools covered in this chapter are a combination of freeware and enterprise software; some tools have free demo versions.

Tools such as Splunk (www.splunk.com), Spiceworks (www.spiceworks.com), Nagios (www.nagios.org), and Cacti (www.cacti.net) help you monitor your network efficiently and thoroughly. For example, you can consult records that the tool generates to prove an employee ran a program without permission. You can also monitor your network and shut down machines or processes that could be harmful.

Although these tools are helpful for network administrators, imagine what would happen if an attacker (or even an internal user) could get administrative rights to the network and start using these tools. For example, in a networking class, students had to install their own servers

and then harden their systems. One student was able to log on to another student's server and shut it down remotely because no password for the default user account had been created.

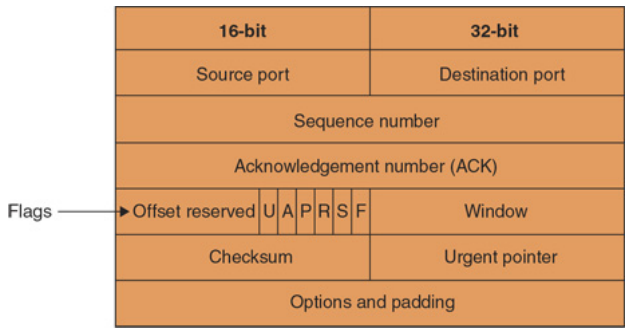
Using Packet Analyzers

Packet analyzers are devices or software placed on a network to monitor traffic. Most network administrators use them for increasing security and tracking bottlenecks. However, attackers can use them to get information covertly. Most packet analyzers work at Layer 2 or 3 of the OSI model. To understand what's happening on a network, often you have to look at the higher layers by using custom software that comes with switches and routers, however.

Some analyzers perform packet captures, some are used for analysis, and some handle both tasks. Your organization needs to have policies about using these tools to comply with new federal laws on digital evidence. Windows has many tools capable of capturing and analyzing packets, but you can't feed the data they collect directly into other tools. Most tools can read anything captured in Pcap (packet capture) format. (Libpcap is the version for Linux, and Winpcap is the version for Windows.) Programs such as tcpdump and Wireshark (www.wireshark.org) use the Pcap format, for example. To take advantage of the strengths in different tools, many investigators do a capture with tcpdump and then analyze the capture in Wireshark.

As a forensics expert, you must choose the tool that best suits your purposes. For example, if your network is being hit with SYN (the synchronize portion of the TCP handshake) flood attacks, you want to find packets with the SYN flag set. In a SYN flood attack, the attacker keeps asking your server to establish a connection. Although your server can handle thousands of connections, it can handle only a limited number of establishing connections. To find these packets, tcpdump and tethereal (a network protocol analyzer) can be programmed to examine TCP headers to find the SYN flag. Figure 10-15 shows a TCP header; the Flags area contains several flags, including the SYN flag (denoted as S in the figure).

Figure 10-15.



A TCP header

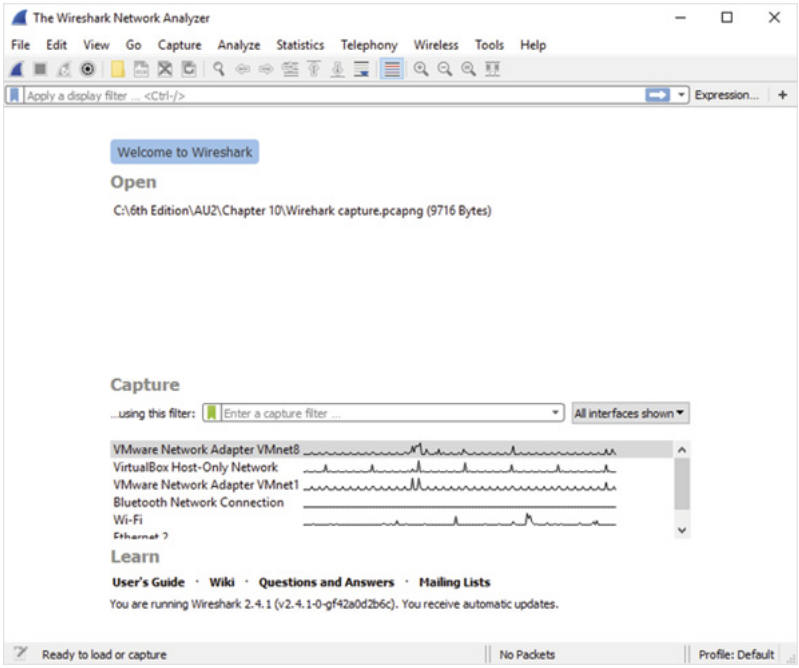
Tcpslice (http://sourceforge.net/projects/tcpslice/) is a good tool for extracting information from large Libpcap files; you simply specify the time frame you want to examine. It's also capable of combining files. A suite of tools called Tcpreplay (http://tcpreplay.appneta.com) can be used to replay network traffic recorded in Libpcap format; you use this information to test network devices, such as IDSs, switches, and routers.

Etherape (http://etherape.sourceforge.net) is a tool for viewing network traffic graphically. Another GUI tool, Netdude (http://netdude.sourceforge.net/), was designed as an easy-to-use interface for inspecting and analyzing large tcpdump files (sometimes several gigabytes). Argus (www.qosient.com/argus) is a session data probe, collector, and analysis tool. This real-time flow monitor can be used for security, accounting, and network management.

Wireshark can be used in a real-time environment to open saved trace files from packet captures. An important feature is its capability to rebuild sessions. To use this feature, right-click a frame in the upper pane and click Follow TCP Stream. Wireshark then traces the packets associated with an exploit. To see how this tool works, download the most recent version of Wireshark for Windows (www.wireshark.org/download.html) and install it on your workstation. Then follow these steps:

1. Start Wireshark, Notice the list of networks with traffic (see **Figure 10-16**).

Figure 10-16.



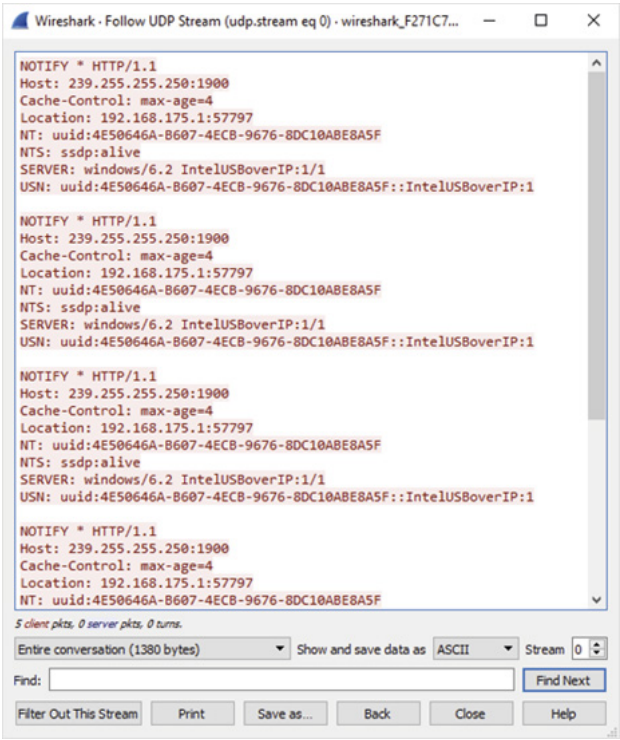
Source: Wireshark Foundation, www.wireshark.org

The opening window in Wireshark

2. Double-click a network that's showing activity. (If you're not on a live network, ping another student or yourself and visit some Web sites and download a file to generate traffic. Then start this activity again.)

3. After the trace has been loaded, scroll through the upper pane until you see a UDP frame or an SSOP frame. Right-click the frame, point to **Follow**, and click **UDP Stream**. You should see a window similar to Figure 10-17.

Figure 10-17.



Source: Wireshark Foundation, www.wireshark.org

Following a UDP stream

4. After several frames have been captured, click **Stop**.
5. Review the information in this window, and then exit Wireshark.

You can find information on network forensics tools at many of the Web sites mentioned in this chapter. If you're interested in learning even more about network forensics, the next section covers the Honeynet Project.

Investigating Virtual Networks

An article in the *Journal of Cybersecurity* explores how to modify the investigation approach that's used in physical networks so that it applies to virtual or logical networks (www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-1439_522.pdf). A virtual switch is a little different from a physical switch, in that there's no spanning tree between virtual switches. For example, say that 24 students each create a virtual network, using a 192.168.x.x network on the type 1 hypervisor, such as vSphere. The numbering isn't unique to their network, but the networks don't overlap because each has its own virtual switch. There's no way to connect the virtual switches, and they don't share the same physical adapters. If there were a physical adapter, the students would have to worry about subnets, which could cause problems, such as a server on Student A's network having the same IP address as one on Student B's network.

This feature of virtual switches grew out of people needing VMs on isolated networks but residing on the same physical rack server as other virtual networks. An additional complication is that hypervisors, including Xen Server, can assign MAC addresses to virtual devices, *and* devices can have the same MAC address on different virtual networks. So Student A's VM can have a virtual Ethernet adapter or virtual network interface card with the same IP address and same MAC address as an adapter on Student B's network and even Student C's network. Each student network can't detect other student networks because of the virtual switches, which enables each student to create large networks independent of other students

and is limited only by the allotted RAM and storage the student's login provides. In this setup, you could have 24 NICs with the same IP address and MAC address that are on different networks.

To take this to the next level, say you're dealing with a cloud service provider (CSP) that hosts networks for several to hundreds of companies. As stated in the *Journal of Cybersecurity* article cited at the beginning of this section, network forensics investigations in the cloud are hampered by the very qualities that make the cloud appealing—elasticity and flexibility. If needed (and it's allowed in the service level agreement), a new server can come online to deal with load balancing. In addition, automatic failovers are in place, which may or may not be in the same physical location as the server. Add to that hundreds or even thousands of NICs with the same IP address and MAC address, and you can see that traditional physical network forensics can't handle these arrangements.

Wireshark and Network Miner are two tools that are capable of analyzing virtual networks. As these networks become more complex, newer or updated tools will be needed.

Examining the Honeynet Project

The Honeynet Project (www.honeynet.org) was developed to make information widely available in an attempt to thwart Internet and network attackers. Many people participate in this worldwide project, which is now a nonprofit organization. The objectives are awareness, information, and tools. The first step is to make people and organizations aware that threats exist and they might be targets. The second is to provide information on how to protect against these threats, including how attackers operate, how they communicate, and what tactics they use. Finally, for people who want to do their own research, the Honeynet Project offers tools and methods.

A major threat is **distributed denial-of-service (DDoS)** attacks. A trace of a DDoS attack might go through other organizations' networks, not just yours or your ISP's. In DDoS attacks, hundreds or even thousands of machines can be used. These machines are known as **zombies** because they have unwittingly become part of the attack. When the first DDoS attacks began, the main concerns were the high monetary impact and the amount of time it took to track down these attacks.

Another major threat is **zero day attacks** . Attackers look for holes in networks and OSs and exploit these weaknesses before patches are available. Vendors usually aren't aware that these vulnerabilities exist, so they haven't developed and released patches for them. Penetration testers attempt to break into networks to find undiscovered vulnerabilities and then predict where the next onslaught of network attacks will come from.

In any organization, you have to determine the value of the data you're protecting and weigh it against the price of the defense system you plan to install. When an attack strikes, your first response is to stop it and prevent it from going further. Then you need to see what defense procedures worked and what additional procedures might be needed. Training and informing IT staff are critical.

The Honeynet Project was set up as a resource to help network administrators deal with DDoS and other attacks. It involves installing honeypots and honeywalls at different locations in the world. A **honeypot** is a computer set up to look like any other machine on your network; its purpose is to lure attackers to your network, but it contains no information of real value. You can take the honeypot offline to analyze it and not affect the running of your network. **Honeywalls** are computers set up to monitor what's happening to honeypots on your network and record what attackers are doing (see www.honeynet.org/papers/cdrom/). Honeypots and honeywalls are commonly used to attract intruders and see what they're attempting to do on a network.

Chapter Summary

- Virtual machines are used extensively in organizations and are a common part of forensic investigations. Investigators must be familiar with file extensions that indicate the existence of VMs.
- There are two types of hypervisors for running virtual machines. Type 1 hypervisors contain their own OSs and are loaded directly on physical hardware. Type 2 hypervisors are applications installed on top of an OS.
- Virtualization Technology is Intel's CPU design for security and performance enhancements that enable the BIOS to support virtualization. Virtual Machine Extensions (VMX) are instruction sets created for Intel processors to handle virtualization. Intel now has virtualization technology for memory, I/O, graphics, and security.
- Forensic procedures for VMs start by creating an image of the host machine, and then exporting files associated with a VM. Next, you create an image of the VM. Virtual machines can be imaged by using forensics software tools, mounting the VM as a drive, or doing a live acquisition.
- Live acquisitions are necessary to retrieve volatile items, such as RAM and running processes. They're also useful when taking systems offline would affect business functioning adversely. Investigators must be concerned with the order of volatility (OOV), which determines how long a piece of information lasts on a system.
- Network forensics is the process of collecting and analyzing raw network data and systematically tracking network traffic to ascertain how an attack took place. Organizations should develop standard procedures for network forensics.
- Steps must be taken to harden networks before a security breach happens, which includes applying layered defense strategies to the network architecture, installing the latest software patches, and making employees aware of security procedures.
- Being able to spot variations in network traffic can help you track intrusions, so knowing a network's typical traffic patterns is important.
- Several tools are available for monitoring network traffic, such as packet analyzers and honeypots. Tools such as tcpdump and Wireshark offer support groups and online training. Keep in mind that network tools can also be used by intruders who obtain administrative rights to attack networks from the inside.
- The Honeynet Project is designed to help people learn the latest intrusion techniques that attackers are using. The project disseminates information and provides tools for research.

Key Terms

defense in depth (DiD)
distributed denial-of-service (DDoS)
honeypot
honeywalls
layered network defense strategy
network forensics
order of volatility (OOV)
packet analyzers
type 1 hypervisor

type 2 hypervisor
Virtualization Technology (VT)
Virtual Machine Extensions (VMX)
zero day attacks
zombies

Review Questions

1. Virtual Machine Extensions (VMX) are part of which of the following?
   a. Type 1 hypervisors
   b. Type 2 hypervisors
   c. Intel Virtualized Technology
   d. AMD Virtualized Technology

2. You can expect to find a type 2 hypervisor on what type of device? (Choose all that apply.)
   a. Desktop
   b. Smartphone
   c. Tablet
   d. Network server

3. Which of the following file extensions are associated with VMware virtual machines?
   a. .vmx, .log, and .nvram
   b. .vdi, .ova, and .r0
   c. .vmx, .r0, and .xml-prev
   d. .vbox, .vdi, and .log

4. In VirtualBox, a(n) _____ file contains settings for virtual hard drives.
   a. .vbox-prev
   b. .ovf
   c. .vbox
   d. .log

5. The number of VMs that can be supported per host by a type 1 hypervisor is generally determined by the amount of
   _____
   _____
   and
   _____
   _____.

6. A forensic image of a VM includes all snapshots. True or False?

7. Which Registry key contains associations for file extensions?
   a. HFILE_CLASSES_ROOT
   b. HKEY_CLASSES_ROOT
   c. HFILE_EXTENSIONS

d. HKEY_CLASSES_FILE

8. Which of the following is a clue that a virtual machine has been installed on a host system?

a. Network logs

b. Virtual network adapter

c. Virtualization software

d. USB drive

9. To find network adapters, you use the

_____

_____

command in Windows and the

_____

_____

command in Linux.

10. What are the three modes of protection in the DiD strategy?

11. A layered network defense strategy puts the most valuable data where?

a. In the DMZ

b. In the outermost layer

c. In the innermost layer

d. None of the above

12. Tcpslice can be used to retrieve specific timeframes of packet captures. True or False?

13. Packet analyzers examine what layers of the OSI model?

a. Layers 2 and 4

b. Layers 4 through 7

c. Layers 2 and 3

d. All layers

14. When do zero day attacks occur? (Choose all that apply.)

a. On the day the application or OS is released

b. Before a patch is available

c. Before the vendor is aware of the vulnerability

d. On the day a patch is created

Hands-On Projects

The objective of these projects is to give you practice in mounting and imaging virtual machines. Before beginning, create a *Work*\Chap10\Projects folder on your system.

Hands-On Project 10-1.

In this project, you open a VM in Autopsy for Windows. As you'll see, Autopsy can't read .vmdk files.

1. Start Autopsy for Windows, and click the **Create New Case** button. In the New Case Information window, enter today's date in the Case Name text box, and click **Browse**

next to the Base Directory text box. Navigate to and click your work folder, create a subfolder called **Hands-On 10-1**, and then click **Select**.

2. In the Additional Information window, type today's date in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

3. In the Select Data Source window, click the **Browse** button next to the "Browse for an image file" text box, Navigate to the **/users/*username*/VirtualBox VMs/Ubuntu 16.04** folder you created in the in-chapter activity, click the **Ubuntu 16.04.vmdk** file, and then click **Open**. Click **Next**, leave the default settings in the Configure Ingest Modules window, and click **Next** again. You get an error message.

4. To convert the VM to a file type Autopsy can open, follow these steps. Start VirtualBox, and click **File**, **Virtual Media Manager** from the menu. In the Virtual Media Manager dialog box, click the **Hard Disks** tab, if necessary, and click the **Ubuntu 16.vmdk** file. Click the **Copy** icon in the upper-left corner, and then click **Next**. In the Copy Virtual Hard Disk window, verify that you selected the correct file, and then click **Next**. Click the **VHD** option button, and click **Next**. Click **Dynamically allocated**, click **Next** again, and then click **Copy**.

5. Click the **View Log** button. The log should show that Autopsy didn't recognize the data type. Take a screenshot of this log.

6. The conversion process takes about 10 to 20 minutes. When it's finished, repeat **Steps 1**, 2, 3, but click the **Ubuntu 16.04.vhd** file this time. Autopsy should recognize the file type. Take a screenshot of the results.

7. Write a brief report about your results. Consider the forensic implications of changing the file type, and explain in your report what must be proved for a converted file to be admissible as evidence in court.

Hands-On Project 10-2.

In this project, you examine a virtual machine nested inside another virtual machine. Keep in mind that the number of VMs you can nest depends on the host machine's hardware. For this project, you use both VMware Workstation Player and VirtualBox. (If you haven't installed VMware Workstation Player yet, go to www.vmware.com/products/workstation-player/workstation-player-evaluation.html to download it, and then install it.)

1. Create a folder called **shared** on your host system. Start VMware Workstation Player, create a VM called **Ubuntu-Primary**, and install Ubuntu 16.04 as a guest OS. In the main VMware Workstation Player window, click the **Ubuntu-Primary** VM, and then click **Edit virtual machine settings**. Click the **Options** tab, and click **Shared folders** on the left. On the right, click **Add** to start the Add Shared Folder Wizard. In the welcome window, click **Next**. In the Name the Shared Folder window, click **Browse**, navigate to and click the **shared** folder on your host system, and click **OK**. Click **Next** and then **Finish** to enable the share.

2. Start a Web browser, and go to www.ubuntu.com/downloads. Download a 32-bit version of Ubuntu 16.04 to the **shared** folder. Back in VMware Workstation Player, start the **Ubuntu-Primary** VM, and click the **Ubuntu** software icon so that you can install the software easily without having to download it. In the search area, type **VirtualBox**, and then select and install it.

3. Start VirtualBox on the Ubuntu-Primary VM, and create a VM called **Ubuntu-Nested**. In the Create Virtual Machine window, notice that only 32-bit versions of this OS are listed as choices. Continue creating the VM. Click the **VMDK (Virtual Machine Disk)** option button for the hard disk type, and leave the default settings in the remaining windows.

4.

With the VM powered off, click **Settings**, and then click **Storage**. Navigate to and click the **shared** folder, and click the 32-bit Ubuntu 16.04 version you downloaded earlier. (*Note*: You might need to install VMware Tools to make sharing work.) Be sure to adjust the RAM to approximately half that of the host VM, and confirm that you have at least 10 GB of storage on this one.) Start the **Ubuntu-Nested** VM, and install Ubuntu 16.04.

5. Take a screenshot of Ubuntu-Nested running inside Ubuntu-Primary. Navigate to where virtual machine files are stored on Ubuntu-Primary (referring to the chapter discussion, if needed), and take a screenshot showing where files for Ubuntu-Nested are located. When you're finished, power off Ubuntu-Nested.

6. Take a snapshot of the Ubuntu-Primary VM, and name it **SS_of_Ubuntu_Nested**. Add descriptive comments, if you like. Power off the **Ubuntu-Primary** VM, and exit VMware Player.

7. Write a short report on the problems caused by deleting the VM that another VM is nested inside, and state whether any trace of the primary VM would be left. As a challenge, you can try doing this same project in VirtualBox.

Hands-On Project 10-3.

For this project, you install and use a tool for capturing live RAM.

1. Start a Web browser, go to https://belkasoft.com/ram-capturer, and download Belkasoft Live RAM Capturer. Install this tool, accepting the defaults, and then start it.

2. Take a screenshot of the opening window. In the "Select output folder path" text box, type your work folder name, and then click **Capture!** When the capture is finished, click **Close**.

3. Using WinHex, the hex editor you've used in previous chapters, open the **testdump** file and examine its contents. Do a search for keywords you'd expect to find in a physical machine's RAM, such as Microsoft, From, To, Subject, and http. If you find other keywords, make note of them. Take screenshots of the search results.

4. Exit WinHex. Write a short paper on your findings, and describe the challenges and possibilities of using Belkasoft for capturing live RAM and WinHex for analysis in an actual investigation.

Hands-On Project 10-4.

This project gives you a chance to explore the SANS SIFT tools. If you didn't install it in the in-chapter activity, do so before starting this project.

1. Start Portable-VirtualBox, and start the **SANS SIFT** VM.

2. Open **sift-cheatsheet.pdf** . It gives instructions on how to mount drives and examine files and has resources for sample images. Take a screen capture of the VM with this file open.

3. Open **memory-forensics-cheatsheet.pdf** . One of the resources it lists is the volatility tool. Start a Web browser, go to https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples, and write down the resources this tool offers.

4. On the left, scroll down and click **DFF (Digital Forensics Framework)**. Click the second icon from the left to add a local device. Click the **VBOX Hard drive** device, and click **OK**. If anything had been loaded on the USB drive, this tool would enable you to search for terms and examine the contents. Click **File**, **Exit** from the menu.

5. Wireshark is another tool available in the SIFT toolkit. Click the **Wireshark** icon on the left. In the Capture Help section, click the **How to Capture** link.

6. You should see step-by-step instructions open in Firefox. Make note of the warnings, such as making sure you have permission before doing packet captures. Exit Firefox. Write a one- to two-page paper summarizing the information in the two cheatsheets you examined and listing warnings for using Wireshark.

Case Projects

Case Project 10-1.

As you have seen, some virtual machines can be loaded on a USB drive. Research which type 2 hypervisors can operate on a USB drive. Which OS and forensics tools could you load on this drive?

Case Project 10-2.

Your company wants to send a working VM to customers with a sample of its new software, but you're concerned about the security of the software and data. What precautions can you take?

Case Project 10-3.

You have acquired a forensic image of a suspect's laptop. After doing an examination, you discover at least one VM installed, and you think more data can be found, but you aren't sure. You decide to make a copy of the VM's files and mount the VM as an external drive. Write the best procedure for this situation.

Case Project 10-4.

Go to http://docs.kali.org/installation/kali-linux-live-usb-install and follow the instructions for installing Kali Linux on a USB drive. Try at least three of the tools it includes, and take screenshots of the tools you selected. Write a one- to two-page paper summarizing each tool's functions.

Chapter 11. E-mail and Social Media Investigations

After reading this chapter and completing the exercises, you will be able to:

- Explain the role of e-mail in investigations
- Describe client and server roles in e-mail
- Describe tasks in investigating e-mail crimes and violations
- Explain the use of e-mail server logs
- Describe some specialized e-mail forensics tools
- Explain how to apply digital forensics methods to investigating social media communications

This chapter explains how to trace, recover, and analyze e-mail messages by using forensics tools designed for investigating e-mail, and general-purpose tools, such as disk editors. E-mail is a major means of communication, and e-mail programs differ in how and where they store and track e-mail. Some are installed separately from the OS and require their own directories and information files on the local computer. Others take advantage of existing software, such as Web browsers, and install no additional software on the client computer. In addition, many people communicate through social media sites, such as LinkedIn, Facebook, and Twitter. Throughout this chapter, you see how e-mail programs on the server interact with e-mail programs on the client, and vice versa. You also learn how to recover deleted e-mail from a client computer, regardless of the e-mail program used, and how to trace an e-mail back to the sender. You also get an overview of the legal issues affecting social media communications.

Exploring the Role of E-mail in Investigations

E-mail evidence is an important part of any computing investigation, so digital forensics investigators must know how e-mail is processed to collect this essential evidence. In addition, with the increase in e-mail scams and fraud attempts with phishing or spoofing, investigators need to know how to examine and interpret the unique content of e-mail messages.

As a digital forensics investigator, you might be called on to examine a phishing e-mail to see whether it's authentic. Later, in "Tracing an E-mail Message," you learn about resources for looking up e-mail and Web addresses to verify whether they're associated with a spoofed message. The Internet links in a phishing e-mail often appear to be correct, such as the U.S. Internal Revenue Service's Web page, www.irs.gov. Typically, **phishing** e-mails contain links to text on a Web page. By using this technique, a phishing message attempts to get personal information by luring readers with false promises. When **pharming** is used, readers might go to the correct Web site address, but DNS poisoning takes them to a fake site. To determine whether redirection has been used, you need to view the message's HTML source code and check whether an Internet link is a label with a redirect to a different Web address.

Tip

For more information on phishing, see www.phishing.org/what-is-phishing.

One of the most noteworthy e-mail scams was 419, or the Nigerian Scam, which originated as chain letters from Nigeria, Africa, in the 1970s and 1980s before switching to fax machines and then e-mail. Fraudsters need only access to Internet e-mail to solicit victims, thus saving the costs of international mail and phone calls. Unlike newer, more sophisticated phishing e-mail frauds, 419 messages have certain characteristic ploys and a typical writing style. For example, the sender asks for access to your bank account so that he can transfer his money to it as a way to prevent corrupt government officials in his homeland from confiscating it. In a more current version, a woman says her husband has died and left her millions of dollars, but she wants to give the money to a church. The sender often promises to reward you financially

if you make a minor payment or allow access to your bank account. The messages are usually in uppercase letters and use poor grammar. Another common scam is a sender stating you have won a sweepstake and asking you to send money to claim the prize. You can find samples of 419 scam messages at www.hoax-slayer.com/nigerian-scam-list.shtml.

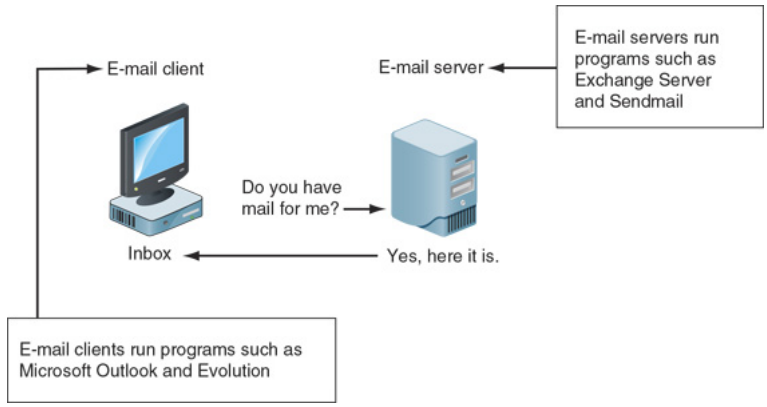
A landmark example of a lawsuit involving **spoofing** e-mail occurred in February 2001 in the Superior Court of Massachusetts: *Suni Munshani v. Signal Lake Venture Fund II, LP et al*. Suni Munshani claimed he received an e-mail from the CEO of Signal Lake Venture Fund instructing him to purchase options (financial warrants) for a total of $25 million. Signal Lake Venture Fund investigated its e-mail servers and didn't find the e-mail Munshani claimed he received.

In preparation for the trial, Signal Lake Venture Fund conducted a discovery demand for all of Munshani's e-mail. Because of the sensitive information Munshani had on his e-mail server, the court appointed an impartial discovery firm to examine the e-mail. The discovery firm found that Munshani had used a text editor to alter an e-mail the CEO of Signal Lake Venture Fund had sent. The clue to the e-mail being a fake was the **Enhanced/Extended Simple Mail Transfer Protocol (ESMTP)** number in the message's header, which is unique to each message an e-mail server transmits. The e-mail Munshani claimed was a legitimate message instructing him to purchase options had the same ESMTP value as the other message the CEO sent. This level of examination revealed that Munshani committed fraud. For more information on this case, see http://signallake.com/email_forensics_library/SMunshaniVsSL.pdf.

Exploring the Roles of the Client and Server in E-mail

You can send and receive e-mail in two environments: via the Internet or an intranet (an internal network). In both e-mail environments, messages are distributed from a central server to many connected client computers, a configuration called a **client/server architecture** . The server runs an e-mail server program, such as Microsoft Exchange Server, to provide e-mail services. Client computers use e-mail programs (also called e-mail clients), such as Microsoft Outlook, to contact the e-mail server and send and retrieve e-mail messages (see Figure 11-1).

Figure 11-1.



E-mail in a client/server architecture

Regardless of the OS or e-mail program, users access their e-mail based on permissions the e-mail server administrator grants. These permissions prevent users from accessing each other's e-mail. To retrieve messages from the e-mail server, users identify themselves to the server, as when logging on to the network. Then e-mails are delivered to their computers.

E-mail services on both the Internet and an intranet use a client/server architecture, but they differ in how client accounts are assigned, used, and managed and in how users access their e-mail. Overall, an intranet e-mail system is for the private use of network users, and Internet e-

mail systems are for public use. On an intranet, the e-mail server is generally part of the local network, and an administrator manages the server and its services. In most cases, an intranet e-mail system is specific to a company, used only by its employees, and regulated by its business practices, which usually include strict security and acceptable use policies. For example, network users can't create their own e-mail accounts, and usernames tend to follow a naming convention that the e-mail administrator determines. For example, for John Smith at Some Company, jsmith is the username, and it's followed by the company's domain name, somecompany.com, to create the e-mail address jsmith@somecompany.com.

Note

In an e-mail address, everything after the @ symbol represents the domain name. You need to know the domain information when you investigate e-mail to identify the point of contact at a domain, and you need the domain administrator's assistance to collect evidence.

In contrast, a company that provides public e-mail services, such as Google, GMX, or Yahoo!, owns the e-mail server and accepts everyone who signs up for the service by providing a username and password. E-mail companies also provide their own servers and administrators. After users sign up, they can access their e-mail from any computer connected to the Internet. In most cases, Internet e-mail users aren't required to follow a standardized naming convention for usernames. They can choose their own usernames (but not the domain name), as long as they aren't already in use.

For digital investigators, tracking intranet e-mail is easier because accounts use standard names the administrator establishes. For example, jane.smith@mycompany.com is easily recognized as the e-mail address for an employee named Jane Smith. Tracking Internet e-mail users is more difficult because these accounts don't always use standard naming schemes, and e-mail administrators aren't familiar with all the user accounts on their servers. Identifying the owner of an e-mail account with an address such as itty_bitty@gmail.com, for example, isn't easy.

With the expansion of cloud service providers, many companies are migrating their e-mail services to the cloud. This setup is convenient because employees can easily access their e-mail from anywhere in the world, but it adds a layer of complexity for investigations, depending on the service level agreement with the cloud provider (covered in **Chapter 13**).

Investigating E-mail Crimes and Violations

Investigating crimes or policy violations involving e-mail is similar to investigating other types of computer abuse and crimes. Your goal is to find out who's behind the crime or policy violation, collect the evidence, and present your findings to build a case for reprimands, prosecution, or arbitration. Make sure you know the applicable privacy laws for your jurisdiction; for example, in the United States, the **Electronic Communications Privacy Act (ECPA)** and the **Stored Communications Act (SCA)** apply to e-mail.

E-mail crimes and violations depend on the city, state, and country in which the e-mail originated. For example, in Washington State, sending unsolicited e-mail is illegal. However, in other states, it isn't considered a crime. Consult with an attorney for your organization to determine what constitutes an e-mail crime.

Committing crimes with e-mail is common, and more investigators are finding communications that link suspects to a crime or policy violation through e-mail. For example, some people use e-mail when committing crimes such as narcotics trafficking, extortion, sexual harassment, stalking, fraud, child abductions, terrorism, child pornography, and so on. Because e-mail is a major communication medium, any crime or policy violation can involve e-mail as well as text messages and social media communication.

Understanding Forensic Linguistics

A related field that has developed in the past few decades is **forensic linguistics** , which is where language and the law intersect. The International Association of Forensic Linguists (www.iafl.org/forensic.php) divides this field into four categories: language and law, language in the legal process, language as evidence, and research/teaching. For the purposes of this book, language as evidence is of the most importance. Think about getting e-mails from people you know. Based on the words that are used, you can almost picture the senders' facial expressions, such as smiles or frowns, and you can probably tell when the language doesn't sound like them, which might indicate they didn't write the e-mails.

Forensic linguistics goes a step further by training people to listen to voice recordings to determine who's speaking or read e-mail and other writings known to be by a certain person and determine whether that person wrote the e-mail or letter in question. Can you tell by looking at a string of e-mails whether they all came from the same person? Would you be able to tell if one had been spoofed? Keep in mind that as a forensic linguist, you might also have to analyze chats, voicemail, and text messages. Often in crime dramas and even crime reenactments, investigators were able to deduce that a missing person hadn't written an e-mail or text message because of differences in tone or style.

In the article "How forensic linguistics can aid investigations" (www.securityinfowatch.com/article/12078050/how-forensic-linguistics-can-aid-investigations), Liz Martinez explores what forensic linguistics can and can't do. What's most important is that it's accepted in many courts around the globe as a valid science. A linguist can determine a speaker's original dialect and sometimes even where a person is from based on the phrases he or she uses. It's been especially useful in determining whether suicide notes have been faked and can be used to examine text messages and social media communications, too. What forensic linguistics can't do yet is determine an author's veracity or gender.

Forensic linguistics encompasses civil cases, criminal cases, cyberterrorism cases, and other legal proceedings. The median income for a forensic linguist is approximately U.S. $65,000 per year. There are several bachelor's and master's degrees in this field.

Examining E-mail Messages

After you have determined that a crime has been committed involving e-mail, access the victim's computer or mobile device to recover the evidence on it. Using the victim's e-mail client, find and copy any potential evidence. It might be necessary to log on to the e-mail service and access any protected or encrypted files or folders. With a corporate investigation, be sure policies are in place for this action. For a criminal investigation, you need warrants to access or get copies of files on a server. When dealing with a stalker, if you can't actually sit down at the victim's computer, you might have to guide the victim on the phone to open and print a copy of an offending message, including the header. The header contains unique identifying numbers, such as the IP address of the server that sent the message. This information helps you trace the e-mail to the suspect.

Earlier in this chapter, you read about the Munshani case, which was solved by examining the e-mail header. As you probably know, an e-mail consists of the header, the e-mail, and the closing. The header contains the date and time, the sender, the recipient, the subject line, and information about the route the e-mail took through e-mail servers. In the Munshani case, Kenneth Shear was able to determine that the suspect e-mail was fake because its ESMTP ID was identical to one used for another e-mail sent earlier. UNIX servers assign unique codes to e-mails based on the precise date and time they're sent, so no two ESMTP IDs are the same. In addition, there was no record of the suspect e-mail on the company's e-mail server.

Investigators can use headers and the encoding at the beginning and ending of e-mails to trace the route e-mails take through servers. They can also use this information to determine who really sent an e-mail or at least pinpoint the sender's location, which can be especially useful in

cases when threats have been made. For a more in-depth examination of e-mail headers, see The E-mail Forensics GuideBook (www.freeviewer.org/email-forensics/).

Tip

Before you work with a victim on the phone, create written procedures for opening and printing an e-mail header and message text with a variety of e-mail programs, according to your state, county, or company's laws or policies. These steps help you give consistent instructions and can be useful when training new investigators.

In some cases, you might have to recover e-mail after a suspect has deleted it and tried to hide it. You see how to recover these messages later in "Using Magnet AXIOM to Recover E-mail." For now, you continue working with a victim's computer as a digital investigator.

Copying an E-mail Message

Before you start an e-mail investigation, you need to copy and print the e-mail involved in the crime or policy violation. You might also want to forward the message as an attachment to another e-mail address, depending on your organization's guidelines. This section gives procedures for different e-mail programs. You might not have access to all of them, but these procedures can serve as a guideline for when you encounter them in investigations.

The following activity shows you how to use Outlook, included with Microsoft Office, to copy an e-mail message to a USB drive. (*Note*: Depending on the Outlook version you use, the steps might vary slightly.) You use a similar procedure to copy messages in other e-mail programs. If Outlook or Outlook Express is installed on your computer, follow these steps:

1. Insert a USB drive into a USB port.
2. Open File Explorer, navigate to the USB drive, and leave this window open.
3. Start Outlook by going to the Start screen, typing **Outlook**, and pressing **Enter**.
4. In the Mail Folders pane, click the folder containing the message you want to copy. For example, click the **Inbox** folder. A list of messages in that folder is displayed in the pane in the middle. Click the message you want to copy.
5. Resize the Outlook window so that you can see the message you want to copy and the USB drive icon in File Explorer.
6. Drag the message from the Outlook window to the USB drive icon in File Explorer.
7. Click the **File** tab, and then click **Print** to open the Print pane. After printing the e-mail so that you have a copy to include in your final report, exit Outlook.

Tip

Instead of dragging, you can click a message in the Inbox, click the File tab, and click Save As. In the Save As dialog box, navigate to where you want to copy the message, making sure you select Outlook Message Format if you want to make a copy. (The Text Only format strips everything but the message contents, including formatting and attachments.) Finally, click the Save button.

With many GUI e-mail programs, you can copy an e-mail by dragging it to a storage medium, such as a folder or drive, or by saving it in a different location. For e-mail programs you run from the command line, however, open the message, and then use the option to copy it, usually located at the bottom of the screen. After you copy an e-mail, work only with the copy, not the original version, to avoid altering the original evidence by mistake.

Viewing E-mail Headers

After you copy and print a message, use the e-mail program that created it to find the e-mail header. This section includes instructions for viewing e-mail headers in a variety of e-mail programs, including Windows GUI clients and some common Web-based e-mail providers. After you open e-mail headers, copy and paste them into a text document so that you can read them with a text editor, such as Windows Notepad+, Linux vim, Nano (used with UNIX), or macOS TextEdit. You examine headers in the next section.

Whether you're working in a forensics lab or elsewhere, installing and becoming familiar with as many e-mail programs as possible is beneficial. Often more than one e-mail program is installed on a computer, and you need to find out which one the suspect is using. Keep in mind, too, that most people now have one or more Web-based e-mail accounts, such as Gmail and Yahoo!, so you need to look for evidence of these accounts.

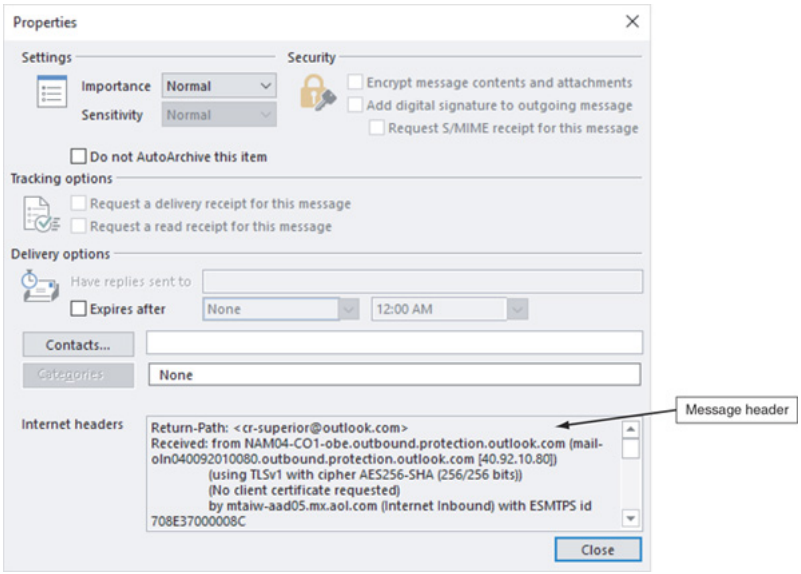
Note

Before beginning the next activity, create a *Work*\Chap11\Chapter work folder on your system. Download to this work folder any files in this chapter's downloads section on the student companion site for this book. The work folder path shown in screenshots might differ slightly from yours.

To retrieve an Outlook e-mail header, follow these steps:

1. Start Outlook, and then select the message you copied in the previous section.
2. Double-click the message, and then click **File, Properties**. The "Internet headers" text box at the bottom contains the message header, shown in Figure 11-2.

Figure 11-2.



An Outlook e-mail header

3. Select the message header text, and then press **Ctrl+C** to copy it to the Clipboard.
4. Start Notepad, and then press **Ctrl+V** in a new document window to paste the message header text.
5. Save the document as **Outlook header.txt** in your work folder. Then close the document and exit Outlook.

Some popular Web-based e-mail service providers are Gmail, Zoho, Outlook Online, and Yahoo!, and you work with a couple in the following activities. You can use any computer and most Internet-connected devices to send and receive e-mail, which makes Web-based e-mail messages more difficult to trace. To view Gmail Web e-mail headers, follow these steps:

1. Start your Web browser, and log on to Gmail.
2. Open an e-mail, click the down arrow next to the Reply circular arrow, and click **Show original**.
3. A new tab opens in your browser that shows basic information at the top, such as the message ID, from, to, and subject line. As you scroll down, you can see the header details along with the original message and encoding. Click the **Download Original** link to open the "Opening original_msg.txt" dialog box. Click **Open with Notepad (default)** and click **Okay**. Save the file in your work folder with the default name.

Follow these steps to view e-mail headers in Yahoo!:

1. Log on to your Yahoo! mail account, click **Inbox** to view a list of incoming e-mails, and then open an e-mail.
2. Above the message window, click the **More** list arrow, and click **View Raw Message** (see Figure 11-3).

Figure 11-3.

Source: Yahoo! Inc., www.yahoo.com

Viewing headers in Yahoo!

3. In the Full Header window, select all the text, press **Ctrl+C** to copy it, and then click **OK**.
4. Start Notepad, and then press **Ctrl+V** in a new document window to paste the message header text. Save the document as **Yahoo Header.txt** in your work folder. Log off Yahoo!, and exit your Web browser.

The e-mail programs reviewed in this section supply similar information in the message header. The methods for retrieving headers vary, but you can usually find information about displaying message headers in the program's Help files.

Examining E-mail Headers

The next step is examining the e-mail header you saved to gather information about the e-mail and track the suspect to the e-mail's originating location. The main piece of information you're looking for is the originating e-mail's domain address or an IP address. Other helpful

information includes the date and time the message was sent, filenames of any attachments, and unique message number, if it's supplied.

Note

For more detailed information on e-mail headers, see www.stopspam.org/index.php.

To open and examine an e-mail header, follow these steps:

1. Open File Explorer and navigate to your work folder.
2. Double-click a .txt file containing message header text, such as **Outlook header.txt** . The message header opens in Notepad.

Figure 11-4 shows a message header copied from an Outlook e-mail. (The e-mail addresses are not real addresses.) Line numbers have been added for reference.

Figure 11-4.

```
Outlook header.txt - Notepad
File  Edit  Format  View  Help
1.      Return-Path: <cr-superior@outlook.com>

2.      Received: from NAM04-CO1-obe.outbound.protection.outlook.com (mail-oln040092010080.outbound.protection.out
        (using TLSv1 with cipher AES256-SHA (256/256 bits))
        (No client certificate requested)
        by mtaiw-aad05.mx.aol.com (Internet Inbound) with ESMTPS id 708E37000008C
        for <b_aspen@aol.com>; Mon, 10 Jul 2017 18:33:12 -0400 (EDT)

3.      DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=outlook.com;
 s=selector1; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version;
 bh=lrZUozDUrSt47+5BKxEkYZkL84z9Xa5pdNS+eLR66fc=;
 b=galykGSNrAUEF2RXwl1P99hjSSA++U4ov0ar6361aUQ0ng2y66ARNrNonxnEWhJ1tKgLXdgpUofKBmH5UTZjYdRJx4q26nZWYoF8o1bQ7h30Gby

4.      Received: from SN1NAM04FT054.eop-NAM04.prod.protection.outlook.com
 (10.152.88.54) by SN1NAM04HT232.eop-NAM04.prod.protection.outlook.com
 (10.152.89.67) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384) id 15.1.1240.9; Mon, 10
 Jul 2017 22:33:04 +0000

5.      Received: from DM3PR14MB1033.namprd14.prod.outlook.com (10.152.88.60) by
 SN1NAM04FT054.mail.protection.outlook.com (10.152.89.2) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id
 15.1.1240.9 via Frontend Transport; Mon, 10 Jul 2017 22:33:04 +0000

6.      Received: from DM3PR14MB1033.namprd14.prod.outlook.com ([10.166.159.17]) by
 DM3PR14MB1033.namprd14.prod.outlook.com ([10.166.159.17]) with mapi id
 15.01.1240.020; Mon, 10 Jul 2017 22:33:03 +0000
```

An e-mail header with line numbers added

The e-mail header in **Figure 11-4** supplies useful information. Lines 1 and 2 show the servers the message passed through. Line 3 shows "DKIM-Signature," which stands for DomainKeys Identified Mail (www.dkim.org). It's a way to verify the names of domains a message is flowing through and was developed to help cut down on spam. Lines 4 through 6 show other servers the message passed through. Typically, these lines are followed by the From, To, Subject, and Date fields in the e-mail.

If there were an attachment, it would be listed in a later line. An attachment can be any type of file, from a program to a picture. If a message includes an attachment, investigate it as a supporting piece of evidence. If you're working with the victim, the attachment is usually still attached to the e-mail. If you're investigating a suspect's computer, remember to work with the copied version. On a suspect's computer or a forensic image, search for the attached file with a forensics tool or the OS's Search or Find feature to determine whether the file was saved and still exists on the drive. If you're investigating an e-mail attachment with an unfamiliar file extension, such as .mdf, you can search the Internet to find out what program creates a file of this type.

Tip

To search for specific files in e-mail headers, use a forensics tool. You can also use a forensics tool to search for unique header information, such as an ID number.

Examining Additional E-mail Files

E-mail programs save messages on the client computer or leave them on the server. How e-mails are stored depends on settings on the client and server. On the client computer, you could save all your e-mail in a separate folder for record-keeping purposes. For example, in Outlook, you can save sent, draft, deleted, and received e-mails in a .pst file, or you can save offline files in an .ost file. With these client files (.pst and .ost), users can access and read their e-mail offline (when their computers aren't connected to the central e-mail server). With many companies having their Exchange servers hosted in the cloud, you might find that only the .ost files are stored on a device, and the .pst files are kept on the server. In this case, you need to contact the network administrator to get access to the .pst files.

Most e-mail programs also include an address book of contacts, and many offer calendars, task lists, and memos. A suspect's address book, calendar, task list, and memos can contain valuable information that links e-mail crimes or abuse to other parties and reveal the suspect's physical address and even involvement in other crimes.

In Web-based e-mail, messages are displayed and saved as Web pages in the browser's cache folders. Many Web-based e-mail providers offer instant messaging (IM) services, such as Yahoo! Messenger and Google Talk, that can save message contents in proprietary and nonproprietary file formats. Facebook Messenger is an example of a social media site that provides an instant-messaging service. These files are usually stored in different folders than Internet data files are. For example, in Windows 8.1, you can find IM files and folders under Users*username*\AppData or under Program Files. IM and chat programs usually have their own folder names. Because some of these programs create proprietary files, you might need special tools to read their contents.

Some IM programs are configured to not save chat content unless users change the default setting, so you might need to search the suspect's Pagefile.sys file to find message fragments. Unlike Yahoo!'s proprietary file format, Windows Messenger stored messages in RTF format that most word processors could read. Although Microsoft no longer supports Windows Messenger, some vendor still distribute it, and as an investigator, you might still encounter it. When you're working on the victim's computer, these types of files can help you document corroborating evidence for the investigation.

Tracing an E-mail Message

As part of the investigation, you need to determine an e-mail's origin by further examining the header with one of many free Internet tools. Determining message origin is referred to as "tracing." In this section, you learn about some Internet lookup tools that can be used to trace where an e-mail originated.

For example, if a company is listed in an e-mail address, you can visit the company's site to find out who administers the domain. If the point of contact isn't listed on the Web site or the domain doesn't have a Web site, you need to use a registry site, such as those in the following list, to determine the point of contact:

- www.arin.net—Use the American Registry for Internet Numbers (ARIN) to map an IP address to a domain name and find the domain's point of contact.
- www.internic.com—Like www.arin.net, you use this site to find a domain's IP address and point of contact.
- www.google.com—Use this search engine and others to look for more information and additional postings on discussion boards.

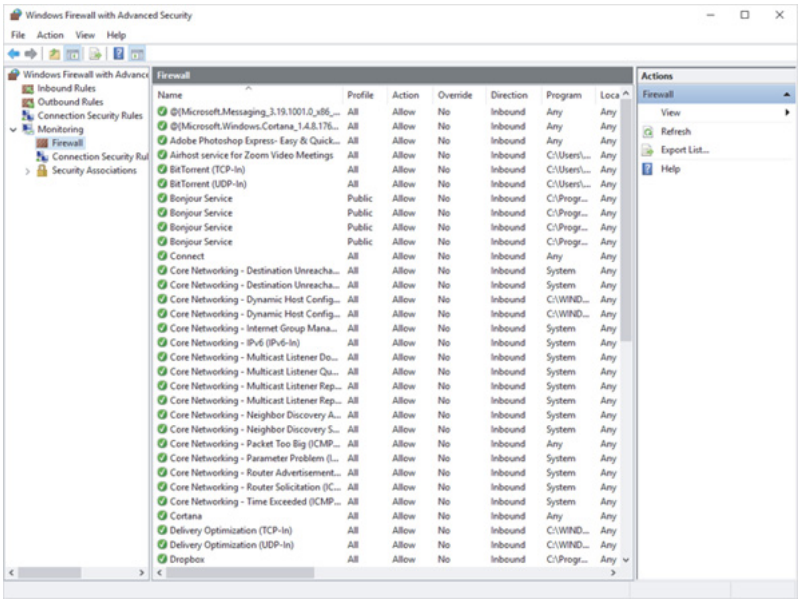
Using one of these Web sites, you can find the suspect's full e-mail address, such as jim.shu@superiorbicycles.biz, and contact information. Keep in mind that the suspect might

have posted false information, so verify your findings by checking network e-mail logs against e-mail addresses, as described in the next section.

Using Network E-mail Logs

Network administrators maintain logs of the inbound and outbound traffic routers handle. Routers have rules to allow or deny traffic based on source or destination IP address. In most cases, a router is set up to track all traffic flowing through its ports. Using these logs, you can determine the path a transmitted e-mail has taken. The network administrator who manages routers can supply the log files you need. Review the router logs to find the victim's (recipient's) e-mail, and look for the unique ID number. Network administrators also maintain logs for firewalls that filter Internet traffic; these logs can help verify whether an e-mail message passed through the firewall. Firewalls maintain log files that track Internet traffic destined for other networks or the network the firewall is protecting. When a network administrator provides firewall log files, you can open them in a text editor, such as Notepad in Windows or vim in Linux. (Some firewalls, however, require special programs to read their log files.) Figure 11-5 shows a typical Windows firewall log.

Figure 11-5.



A Windows firewall log

Understanding E-mail Servers

An e-mail server is loaded with software that uses e-mail protocols for its services and maintains logs you can examine and use in your investigation. As a digital forensics investigator, you can't know everything about e-mail servers. Your focus is not to learn how a particular e-mail server works but how to retrieve information about e-mails for an investigation. Usually, you must work closely with the network administrator or e-mail administrator, who is often willing to help you find the data or files you need and might even suggest new ways to find this information. If you can't work with an administrator, conduct research on the Internet or use the forensics tools discussed later in this chapter to investigate the e-mail server software.

To investigate e-mail abuse, you should know how an e-mail server records and handles the e-mail it receives. Some e-mail servers use databases that store users' e-mails, and others use a flat file system. All e-mail servers can maintain a log of e-mails that are processed. Some e-mail servers are set up to log e-mail transactions by default; others must be configured to do so.

Most e-mail administrators log system operations and message traffic for the following reasons:

- Recover e-mails in case of a disaster.
- Make sure the firewall and e-mail filters are working correctly.
- Enforce company policy.

However, the e-mail administrator can disable logging or use circular logging (also called "log rotation"), which overwrites the log file when it reaches a specified size or at the end of a specified time frame. It's similar to the standard backup rotations used for file servers. Circular logging saves valuable server space, but you can't recover a log after it's overwritten. For example, on Monday the e-mail server records traffic in the Mon.log file. For the next six days, the e-mail server uses a log for each day, such as Tues.log, Wed.log, and so forth. On Sunday at midnight, the e-mail server starts recording e-mail traffic in Mon.log, overwriting the information logged the previous Monday. The only way to access the log file information is from a backup file, which many e-mail administrators create before a log file is overwritten.

E-mail logs generally identify the e-mail messages an account received, the IP address from which they were sent, the time and date the e-mail server received them, the time and date the client computer accessed the e-mail, the e-mail contents, system-specific information, and any other information the e-mail administrator wants to track. These e-mail logs are usually formatted in plain text and can be read with a basic text editor, such as Notepad or vim.

Administrators usually set e-mail servers to continuous logging mode. They can also log all e-mail information in the same file, or use one log file to record, for example, date and time information, the size of the e-mail, and the IP address. These separate log files are extremely useful when you have an e-mail header with a date and time stamp and an IP address, and you want to filter or sort the log files to narrow your search.

After you have identified the source of the e-mail, contact the network or e-mail administrator of the suspect's network as soon as possible. Some e-mail providers, especially Internet e-mail providers, don't keep logs for more than 30 days (and some keep logs for less time), and their logs might contain key information for your investigation.

In addition to logging e-mail traffic, e-mail servers maintain copies of clients' e-mail, even if the users have deleted messages from their inboxes. Some e-mail servers don't completely delete messages until the system is backed up. Sometimes the e-mail administrator can recover deleted e-mail without restoring the entire e-mail server, but some e-mail servers require recovering the entire server to retrieve one deleted message.

This process is similar to deleting files on a hard drive; the file is marked for deletion, but it's not truly unrecoverable until another piece of data is written in the same place. E-mail servers wait to overwrite disk space until the server has been backed up. If you have a date and time stamp for an e-mail, the e-mail administrator should be able to recover it from backup media if the message is no longer on the e-mail server.

Examining UNIX E-mail Server Logs

More than a dozen UNIX e-mail server programs are available. Most produce log files similar to the ones discussed previously. Postfix and Sendmail are two common UNIX e-mail servers. Sendmail is the default for FreeBSD systems, such as CentOS.

Log files and configuration files can provide helpful information. The configuration file for Sendmail is /etc/mail/sendmail.cf, which can help you determine where log files are stored. Sendmail refers to the sendmail.cf file to find out what to do with an e-mail after it's received. For example, if the server receives an e-mail from an unsolicited site, a line in the sendmail.cf file can tell the Sendmail server to discard it.

Tip

Recall that the forward slash (/) is used in UNIX/Linux file paths, and the backslash (\) is used in Windows file paths.

Similar to the sendmail.cf file, the /etc/syslog.conf file includes e-mail logging instructions so that you can determine how Sendmail is set up to log e-mail events and which events are logged. The syslog.conf file's configuration in the /etc directory contains three pieces of information that tell you what happened to an e-mail when it was logged: the event, the priority level of concern, and the action taken when it was logged. By default, Sendmail can display an event message, log the event message to a log file, or send an event message to a remote log host. E-mail files are typically found at /var/mail.

Postfix is another common UNIX e-mail server. Similar to Sendmail, it has configuration files, master.cf and main.cf, in the /etc/postfix directory, and e-mails are stored in /var/spool/postfix.

Because a UNIX system has a variety of e-mail servers available, the syslog.conf file simply specifies where to save different types of e-mail log files. The first log file it configures is /var/log/maillog, which usually contains a record of **Simple Mail Transfer Protocol (SMTP)** communication between servers.

The IP address (10.0.1.1) and the timestamp in the maillog file are important information in an e-mail investigation. You can compare this information with the header of the e-mail the victim received to confirm the sender. The maillog file also contains information about **Post Office Protocol version 3 (POP3)** and **Internet Message Access Protocol 4 (IMAP4)** events. This information includes an IP address and a timestamp that you can compare with the e-mail the victim received.

Typically, UNIX systems are set to store log files in the /var/log directory. However, an administrator can change the log location, especially when an e-mail service specifies a different location. If you're examining a UNIX computer and don't find the e-mail logs in /var/log, you can use the find or locate command to find them. For example, type locate .log at a UNIX command prompt.

If you need more assistance to find where a file is created by default, you can use the UNIX man pages for the e-mail service running on the computer. A new directory —/home/*username*/mail—is created on the client computer when a user logs on for the first time and runs the e-mail program. If the server has been configured to deliver e-mail to client machines but not store copies of e-mails on the server, the only copy of the e-mail is on the client computer in the user's mail folder.

If the UNIX e-mail server is set to store all messages on the server, you can access them by requesting that the UNIX administrator create e-mail groups and add you to the same group as the suspect. UNIX e-mail servers don't usually use groups to prevent users from accidentally viewing e-mail that doesn't belong to them. However, e-mail groups can be useful for investigative purposes, as long as you have secured a warrant.

Examining Microsoft E-mail Server Logs

Exchange Server, generally called Exchange, is the Microsoft e-mail server software. Exchange uses an Exchange database and is based on the Microsoft Extensible Storage Engine (ESE), which uses several files in different combinations to provide e-mail service. The files most useful to an investigation are .edb database files, checkpoint files, and temporary files.

In older versions of Exchange, .edb files were the database files you needed. An .edb file is responsible for messages formatted with **Messaging Application Programming Interface (MAPI)** , a Microsoft system that enables different e-mail applications to work together. As a

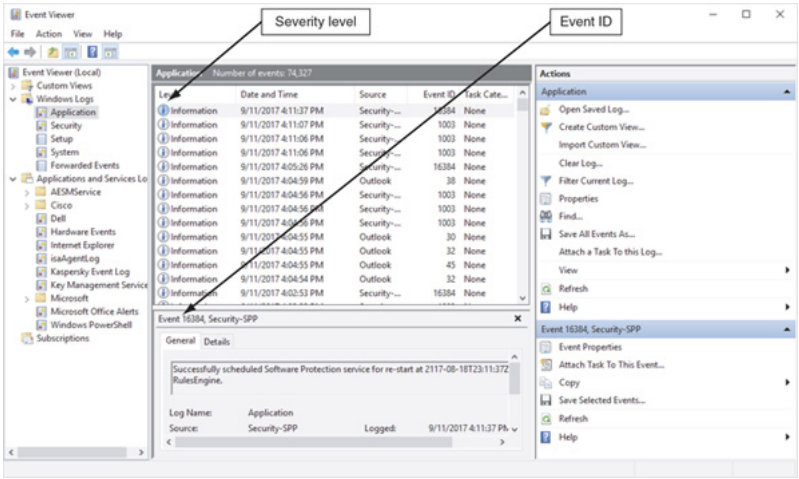
database server, Exchange logs information about changes to its data, also called transactions, in a transaction log. To prevent loss of data from the most recent backup, a checkpoint file, or marker, is inserted in the transaction log to mark the last point at which the database was written to disk. With these files, e-mail administrators can recover lost or deleted messages in the event of a disaster, such as a power failure. Exchange also creates .tmp (temporary) files to prevent loss when it's busy converting binary data to readable text.

Like UNIX e-mail servers, Exchange maintains logs to track e-mails. To retrieve them, you can use the Windows PowerShell cmdlet GetTransactionLogStats.ps1 -Gather (https://blogs.technet.microsoft.com/exchange/2017/01/31/analyzing-exchange-transaction-log-generation-statistics-revisited/).

Exchange servers can also maintain a log called Tracking.log that tracks messages. If the Message Tracking feature has been enabled and the e-mail administrator selects verbose (detailed) logging, you can see the timestamp, IP address of the sending computer, and the e-mail's contents or body. Except for special forensics tools, the message-tracking log in verbose mode provides the most information about messages sent and received in Exchange.

Another log used for troubleshooting and investigating the Exchange environment is the troubleshooting log. You can read this log, also known as a "diagnostic log," by using Windows Event Viewer, shown in **Figure 11-6**, which is available in Administrative Tools. Each event logged has an ID number and a severity level.

Figure 11-6.



Viewing a log in Event Viewer

To examine the details of an e-mail event, double-click the event to open its Event Properties dialog box. This dialog box shows date and time information that might be useful if, for example, you suspect the e-mail server has been tampered with to alter its contents.

Using Specialized E-mail Forensics Tools

For many e-mail investigations, you can rely on e-mail message files, e-mail headers, and e-mail server log files. However, if you can't find an e-mail administrator willing to help with the investigation, or you encounter a highly customized e-mail environment, you can use data recovery tools and forensics tools designed to recover e-mail files.

As technology has progressed in e-mail and other services, so have the tools for recovering information lost or deleted from a hard drive. In previous chapters, you have reviewed many tools for data recovery, such as Magnet AXIOM, Autopsy, and OSForensics. You can also use these tools to investigate and recover e-mail files. Other tools, such as the ones in the following

list, are specifically created for e-mail recovery, including recovering deleted attachments from a hard drive:

- DataNumen for Outlook and Outlook Express (www.datanumen.com/products.htm)
- FINALeMAIL for Outlook Express and Eudora (http://finalemail-1-2.en.softonic.com)
- Sawmill-Novell GroupWise for log analysis (www.sawmill.net/formats/groupwise_post_office_agent.html)
- MailXaminer for multiple e-mail formats and large data sets (www.mailxaminer.com/)
- Fookes Aid4Mail and MailBag Assistant for Outlook, Thunderbird, and Eudora (www.fookes.com)
- Paraben E-Mail Examiner, configured to recover several e-mail formats (www.paraben.com/products/e3-emx)
- AccessData FTK for Outlook and Outlook Express (www.accessdata.com)
- Ontrack EasyRecovery EmailRepair for Outlook and Outlook Express (www.ontrackdatarecovery.ie/data-recovery/email-recovery/)
- R-Tools R-Mail for Outlook and Outlook Express (www.r-tt.com/outlook_mail_recovery/)
- OfficeRecovery's MailRecovery for Outlook, Outlook Express, Exchange, Exchange Server, and IBM Notes (www.officerecovery.com)
- MXToolBox for decoding e-mail headers (https://mxtoolbox.com/EmailHeaders.aspx)
- FreeViewer with free tools for Outlook, Windows Live Mail, Thunderbird, and other servers (www.freeviewer.org/email-forensics/free-tools.html)

When you use a third-party tool to search for a .db file, for example, you can find where the administrator stores these files for the e-mail server; they could be on the server or in a remote location for backup. To find log files, use .log as the search criteria. You're likely to find at least two logs related to e-mail—one listing logged events for messages and the other listing logged events for accounts accessing e-mail.

Forensics tools enable you to find e-mail database files, personal e-mail files, offline storage files, and log files. With some tools, you use a special viewer to see messages and other files; others require using a text editor to compare information, such as the timestamp, username, domain, and message contents, to determine whether it matches what was found on the victim's computer.

One advantage of using data recovery tools is that you don't need to know how the e-mail server or e-mail client operates to extract data from these computers. Data recovery tools do the work for you and allow you to view evidence on the computer. However, if you're serving as an expert witness, you do need to understand the e-mail system's functions and be able to explain them to laypeople.

After you compare e-mail logs with the messages, you should verify the e-mail account, message ID, IP address, and date and time stamp to determine whether there's enough evidence for a warrant. If so, you can obtain and serve your warrant for the suspect's computer equipment. Remember to follow the evidence-handling rules and control measures your organization uses, as described in previous chapters.

Tip

When requesting a search warrant, consider whether you're looking for evidence of more than one crime. If you intend to investigate different crimes, make sure to include probable cause for each crime so that you need only a single warrant covering all areas of interest. Your investigation might require a second warrant, however. For example, if

you're investigating a drive for evidence of harassment and you come across e-mail suggesting that the suspect is also selling controlled substances over the Internet, you need a second warrant to investigate this crime.

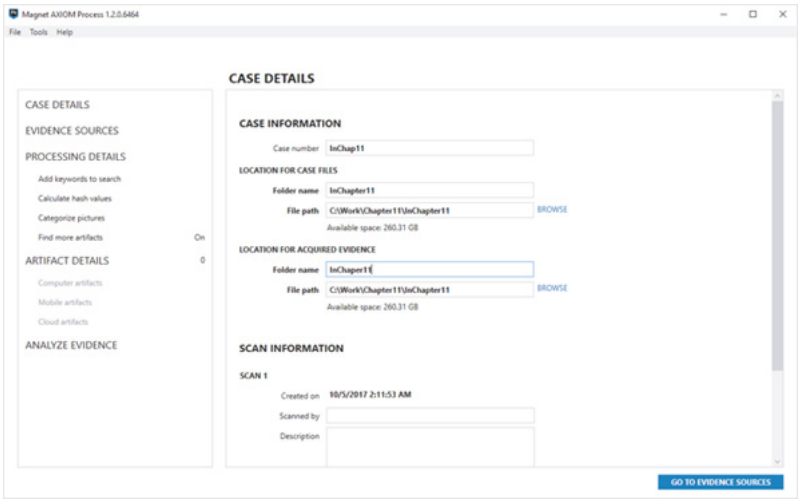
After collecting evidence, you begin copying it to another source for the examination while documenting everything you're doing. If you create an image, document the procedure and tool you use. If you're just collecting a specific folder, such as the .evolution directory, document the command you use to copy data. With some tools, you can scan e-mail database files on a suspect's Windows computer, locate any e-mails the suspect has deleted—these messages don't have data location information—and restore them to their original state. You can also search a computer for other files associated with e-mail, such as databases, and see whether any attachments were sent with an e-mail and view them.

Using Magnet AXIOM to Recover E-mail

Magnet AXIOM is designed to combine evidence retrieval from PCs, mobile devices, and the cloud. Many other tools are also moving in this direction. In this activity, you learn how to use Magnet AXIOM to recover e-mails. Magnet AXIOM has two modules: Process and Examine. You start Process first to enter the case details and add the evidence. When you finish these procedures, Magnet AXIOM Examine starts.

1. Start Magnet AXIOM Process, and click the **CREATE NEW CASE** button. On the left is the navigation pane to show where you are in processing a case, and on the right is where you enter or select details. In the Case number text box, type **InChap11**. In the LOCATION FOR CASE FILES section, type **InChapter11** in the Folder name text box, as shown in Figure 11-7. Click the **BROWSE** button next to the File path text box, navigate to and click your work folder, and click **Select Folder**. Click the **GO TO EVIDENCE SOURCES** button.

Figure 11-7.



Source: Magnet Forensics, www.magnetforensics.com

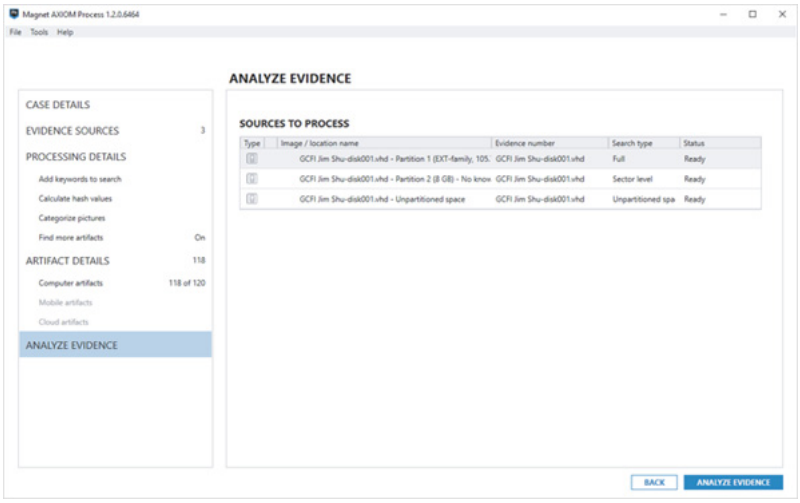
Entering information in the CASE DETAILS window

2. In the EVIDENCE SOURCES window, you can choose COMPUTER, MOBILE, or CLOUD in the SELECT EVIDENCE SOURCE section. Click the **COMPUTER** icon. In the next window, click the **LOAD EVIDENCE** icon, and then click **NEXT**. In the next window, you can specify loading a drive, an image, a file, or a volume shadow copy. Click **IMAGE**. Navigate to your work folder where you downloaded this chapter's data files, click the hard drive file **Jim Shu001.vhd** , and click **OK**.

3. In the Add Files and Folders window, notice the listed partitions, and then click **NEXT**. In the next window, you can select the search type: full, sector level, or unpartitioned space. Leave all these search types selected, and click **NEXT**. The next window shows you the evidence that has been added to the case. Click **GO TO PROCESSING DETAILS**, where you could add keyword lists, hash values, and other details to customize your case. For now, you're not adding anything else, so click **GO TO ARTIFACT DETAILS**. The MOBILE ARTIFACTS and CLOUD ARTIFACTS sections are grayed out because you haven't added any evidence from these sources.

4. Click **GO TO ANALYZE EVIDENCE**. This window shows the evidence sources to be processed (see Figure 11-8). **Click ANALYZE EVIDENCE** . This process takes around two hours, depending on your workstation. When it's finished, Magnet AXIOM Examine starts automatically.

Figure 11-8.

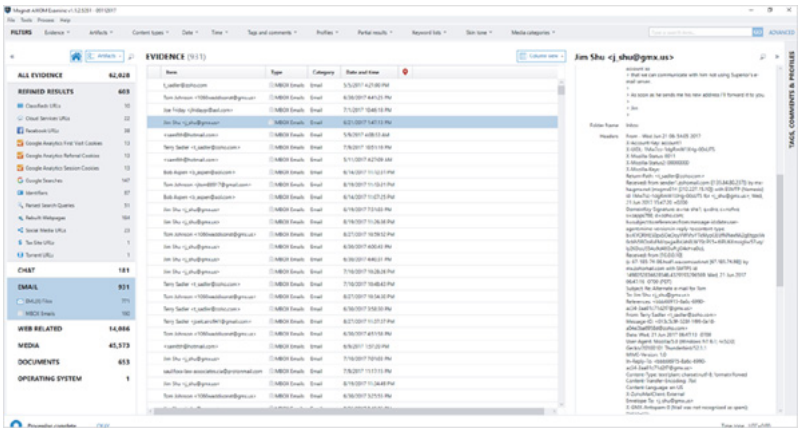


Source: Magnet Forensics, www.magnetforensics.com

Preparing to analyze evidence

5. On the left, click to expand **EMAIL**. Notice the two subfolders under it. Next, click an e-mail with the j_shu@gmx.us address in the EVIDENCE pane in the middle (see Figure 11-9). Copy the e-mail header in the pane on the far right.

Figure 11-9.



Source: Magnet Forensics, www.magnetforensics.com

Viewing e-mail headers in Magnet AXIOM

6. Start a Web browser, and go to https://mxtoolbox.com/EmailHeaders.aspx. Paste the e-mail header into the E-mail Header Analyzer text box, and click **Analyze Header**.

What information can you get from the MXToolBox tool? When you're finished examining the e-mail, exit Magnet AXIOM.

Using a Hex Editor to Carve E-mail Messages

Few vendors have products for analyzing e-mail in systems other than Microsoft, such as macOS Mail or Evolution. In this section, you learn about a method for acquiring Evolution e-mail directories and extracting messages with Hex Workshop. These techniques can be used with all e-mail systems that create flat plaintext files, known as an **mbox** format, to store messages. Vendor-unique e-mail file systems, such as Microsoft .pst or .ost, typically use **Multipurpose Internet Mail Extensions (MIME)** formatting, which can be difficult to read with a text or hexadecimal editor.

To carve e-mails from Evolution, you need to copy the .evolution directory, its subdirectories, and content to another storage medium that can be transported to your forensic workstation. One way is to export this directory and subdirectories from an image file to a target drive path you designate by using a forensics tool. For an e-mail recovery that requires extracting only e-mail data from a computer, the Linux tar command is easy to use. You can create a tarball of the entire .evolution directory and uncompress it so that a hexadecimal editor on any OS can read it.

For this case, you're acquiring the .evolution directory from Martha Dax's Linux computer to see whether you can find the same e-mail you found in the Jim_shu's.pst file. Then you compare the message headers of the two e-mails to detect any differences and perhaps discover e-mail addresses other than Terry Sadler's and Martha Dax's. The following steps explain how to make a tarball of the .evolution directory:

Note

Because you don't have an .evolution directory on your system, just read through these steps as an example of extracting this file to a USB drive.

1. Start Linux and open a terminal window.
2. Connect a USB drive to your computer and mount it, if it's not mounted automatically.
3. Navigate to the user's home directory. For example, type cd /home/martha and press Enter.
4. To determine whether the .evolution directory is in this location, type ls -a and press Enter. Examine the output. If you don't see an .evolution directory in the home directory, type ls -aR to list all subdirectories. When you have found the .evolution directory, use the cd command to navigate to the parent directory so that you can copy the .evolution directory and its subdirectories.
5. Type tar cf martha-evolution.tar .evolution and press Enter. If you get an error of insufficient authority, repeat the command, but precede it with sudo. When prompted, enter your password.
6. Using File Manager or another GUI utility, copy martha-evolution.tar to a USB drive.
7. Type exit and press Enter, and then log out of your Linux computer.

All mbox-formatted messages start with the word "From" followed by a space (the character 0x20). To carve e-mails from martha-evolution.tar (which you downloaded to your work folder earlier), follow these steps:

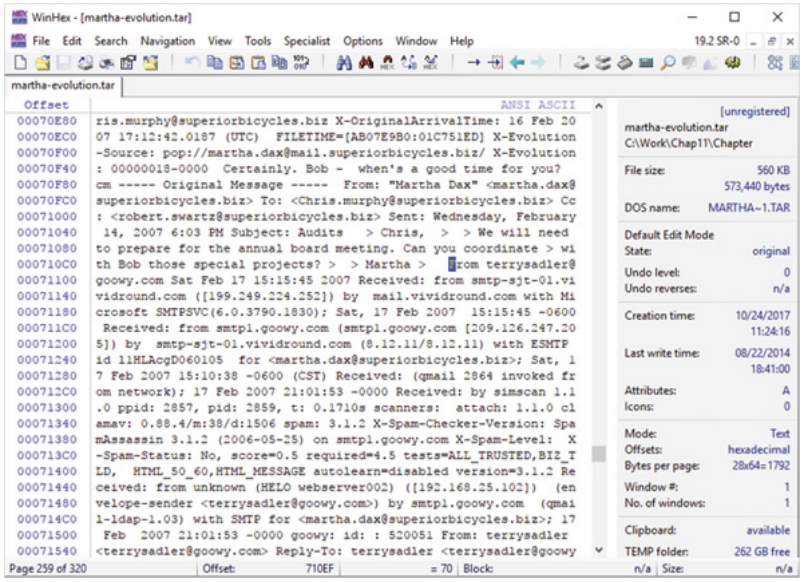
1. Start WinHex. Click **File, Open** from the menu, navigate to your work folder, click **martha-evolution.tar** , and then click **Open**. Click **View, Text Display Only** from the menu, and then click **View**, point to **Character Set**, and click **ANSI ASCII**.

2. To locate the e-mail from Terry Sadler, click **Search, Find Text** from the menu.

3. In the Find Text dialog box, type **terrysadler** in the "The following text string will be searched" text box, make sure **ASCII/Code page** is selected in the drop-down list, and then click **OK**. If necessary, click **OK** in the "Search complete" message box.

4. Place the cursor in front of the letter "F" in the word "From" (see the fifth line in **Figure 11-10**). Notice the offset byte count 710EF at the bottom.

Figure 11-10.

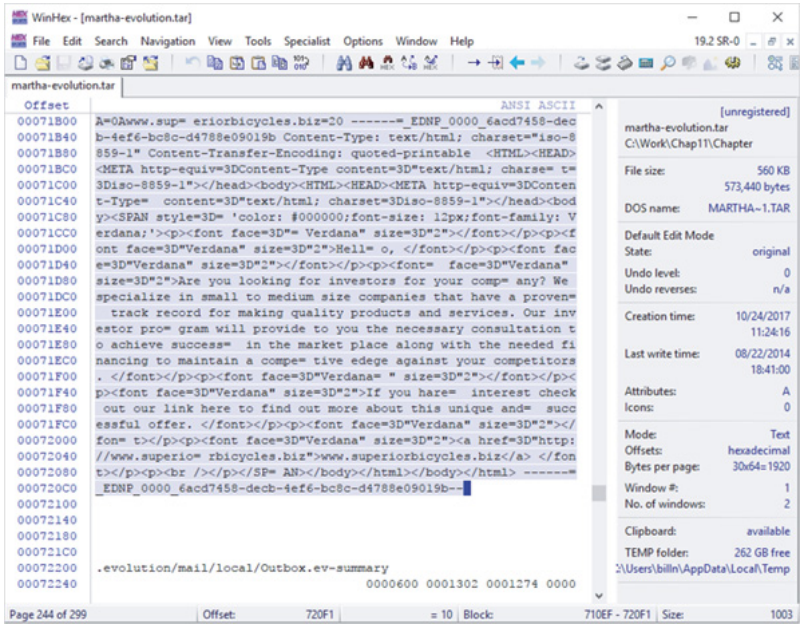


Source: X-Ways AG, www.x-ways.net

WinHex displaying the beginning of the e-mail from Terry Sadler

5. Click at offset **710EF** in the middle pane and drag down until you reach the end of the e-mail, as shown in Figure 11-11 (*Note*: Your screen might look a little different.)

Figure 11-11.



Source: X-Ways AG, www.x-ways.net

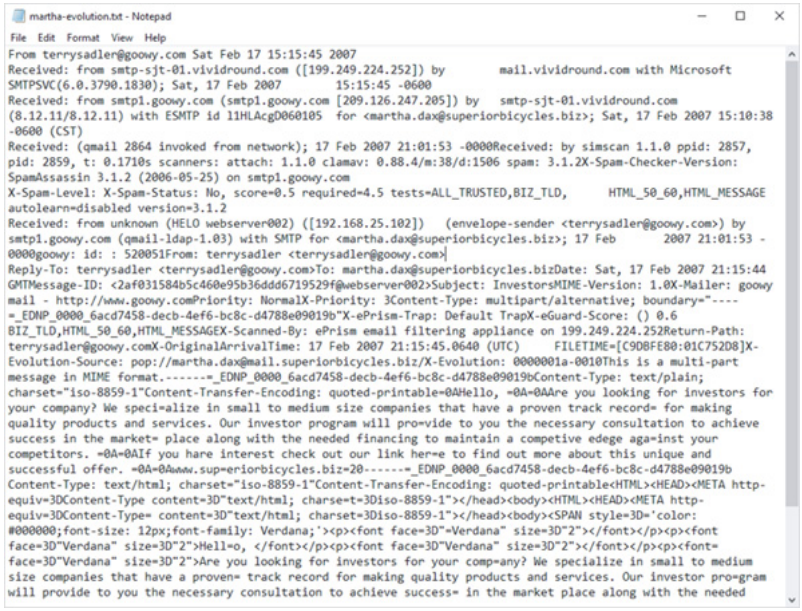
WinHex displaying the ending position of the e-mail from Terry Sadler

6. Right-click the highlighted text and click **Edit**, point to **Copy Block**, and click **Into New File**.

7. In the Save File As dialog box that opens, save the file as **Martha-evolution.txt** in your work folder, and exit Hex Workshop.

8. Start Notepad and open the **Martha-evolution.txt** file (see Figure 11-12) so that you can refer to it in the next few paragraphs, and then exit Notepad when you've finished reading this section.

Figure 11-12.



The Terry Sadler e-mail in Notepad

Note

The ending position of this message is at offset 720F1. With mbox-formatted files, typically you find the end of the message at the next "From_" occurrence. Because this message is the last in the inbox, it terminates with "0A, 0A, 0A."

After carving an e-mail message from a tarball .evolution file, you have a plaintext file with no line breaks. The text pasted into Notepad wraps, making it difficult to find reference points. To make this file's header and content readable, you need to enter line breaks at logical places, which can be tedious. The effort pays off, however, because you can find information of interest to your investigation more easily.

For example, you might notice that the only addresses visible are terrysadler@goowy.com and martha.dax@superiorbicycles.biz. The next step is to see whether you can find Jim Shu's e-mail. His e-mail address hasn't been listed in the results so far. By comparing these two messages from the Jim_shu's.pst file and Martha Dax's .evolution inbox, you determine that Terry Sadler blind-copied (bcc) Jim Shu. This information might be of interest to Martha Dax because it shows that Jim Shu and Terry Sadler have a relationship involving a business proposal. By further examining Jim Shu's e-mail and other Superior Bicycles employees' e-mail, you might be able to learn what the relationship is and whether it should be of concern to Martha Dax and Superior Bicycles.

Recovering Outlook Files

As a forensics examiner recovering e-mail messages from Outlook, you might need to reconstruct .pst files and messages. With many advanced forensics tools, such as Magnet AXIOM, OSForensics, X-Ways Forensics, AccessData FTK, and Guidance Software EnCase, deleted .pst files can be partially or completely recovered. Typically, additional effort is required to reconstruct these recovered files so that their content can be extracted as part of a data recovery or forensics examination.

The scanpst.exe recovery tool comes with Microsoft Office and can repair .ost files as well as .pst files. You can run this tool from File Explorer or a command prompt and use it with any data that looks like a .pst or an .ost file. It processes the data and rebuilds it into a .pst file that can be accessed with Outlook or other tools discussed in this chapter.

Tip

For more information on scanpst.exe, see http://office.microsoft.com/en-001/outlook-help/repair-outlook-data-files-pst-and-ost-HA010075831.aspx and www.slipstick.com/outlook/config/recover-deleted-messages-pst-files/.

Guidance Software uses the SysTools plug-in (www.guidancesoftware.com/app/SysTools-Outlook-Exporter-v-Demo-Version-) for Outlook e-mail through version 2013. SysTools extracts .pst files from EnCase Forensic for analysis. An advantage of this plug-in is that you don't have to install Outlook to examine Outlook e-mails.

Other recovery tools are designed to reconstruct e-mail data in Outlook and other e-mail formats. One tool that has been well tested is DataNumen Outlook Repair (www.datanumen.com/outlook-repair); it's one of the better e-mail recovery tools on the market. It can recover files from VMware and Virtual PC as well as ISO images and other types of file backups. You install and use it later in the hands-on projects.

E-mail Case Studies

Throughout this book, you have been using the M57 case, and in the hands-on projects, you work with some .pst files in this case. Another major case involving corporate e-mail is the Enron case, which required retrieving thousands of e-mails at a time when few policies for collecting this information existed. When the Electronic Discovery Reference Model (EDRM; www.edrm.net) group acquired the right to store and distribute these e-mails, it discovered how much personally identifiable information they contained. Another company worked with the EDRM to correct the problem by removing the personal information. In the end, more than 10,000 e-mails were collected (http://info.nuix.com/Enron.html). The following list gives you an idea of how much personal information these e-mails contained:

- 60 containing credit card numbers
- 572 containing thousands of Social Security or other identity numbers
- 292 containing birth dates
- 532 containing information of a highly personal nature, such as medical or legal matters

As a regular part of doing business, employees sent internal e-mails with spreadsheet attachments containing personal information about employees and customers. Now spreadsheets are typically password-protected or encrypted, but these documents weren't. In the hands-on projects, you download some .pst files of Enron employees and examine them with tools discussed in this chapter to get an idea of what kind of information can be found in corporate e-mails.

Applying Digital Forensics Methods to Social Media Communications

Social media sites, such as Twitter, Facebook, LinkedIn, and YouTube, aren't just a way of communicating with friends and family. These **online social networks (OSNs)** are also used to conduct business, brag about criminal activities, raise money, and have class discussions. You can also use OSNs to build a profile of a prospective client, a business partner, a suspect in a murder trial, and more.

Social media can contain a lot of information, including the following:

- Evidence of cyberbullying and witness tampering
- A company's position on an issue
- Whether intellectual property rights have been violated
- Who posted information and when

The number of cases involving social media is growing, and social media evidence often substantiates a party's claims. For example, in an early intellectual property case involving social media, evidence gathered from the public side of an employee's LinkedIn profile showed that she had copied thousands of records from her company laptop to a USB drive and started working at a competing company before quitting her job ("Elephant in the Room: Case Studies of Social Media in Civil and Criminal Cases," Mark Lanterman, https://blog.x1discovery.com/2014/06/10/elephant-in-the-room-case-studies-of-social-media-in-civil-and-criminal-cases/, June 2014). In his article on social media forensics (http://mashable.com/2012/02/13/social-media-forensics/), Todd Piett noted that 88% of the law enforcement groups surveyed use social media as a tool for doing background checks, corroborating data, verifying alibis, and finding suspects and witnesses. For example, in one case, a 19-year-old was accused of a crime, but police were able to use his Facebook posts as proof he was somewhere else when the crime occurred (http://edition.cnn.com/2009/CRIME/11/12/facebook.alibi/index.html, *2009*).

Note

In another case, police were able to arrest a gang member because one of his friends boasted about a murder on his MySpace page ("Police embrace social media as crime-fighting tool," www.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media/, 2012).

A challenge with using social media data in court is authenticating the author and the information. In this age of accusations of "fake news," investigators must be careful to verify their data. In "Authentication of Social Media Evidence: 2 Cases To Know" (www.law360.com/articles/897947/authentication-of-social-media-evidence-2-cases-to-know), Beth Rose examines what constitutes "discoverable" versus "admissible" by examining the case *U.S. v. Brown*, in which the prosecutor presented enough circumstantial evidence to prove that Facebook chats had been written by the defendant. The defendant claimed the chats couldn't be authenticated and, therefore, couldn't be used in court. However, Facebook could authenticate that the chats had taken place and gave a certificate of authenticity, as it was a normal business record. In addition, the other people involved in the case (who were minors) could testify as to the content of the chats and state they had met the defendant in person. Four of the five chats were allowed as admissible in court.

Digital investigators can mine social media sites to find information, too. The challenge is that even though much of YouTube and Facebook content is public, the data is spread over many servers, providers, and users. By January 2017, Facebook alone had two billion monthly users. The amount of data on social media sites is staggering: 250 million pictures and 200 million tweets a day, for example. There's so much information that analyzing it requires techniques referred to as "big data analytics," which is the study of dissimilar types of data in huge quantities. Investigators might have to sift through videos, pictures, GPS locations, text messages, e-mails, tweets, and posts in just one case, and trying to analyze so many types of data has an effect on what approach is used.

In addition, OSNs involve multiple jurisdictions that might even cross national boundaries, and social media vendors prohibit access to their servers. As an investigator, you're not allowed to physically touch or retrieve information from these machines. A warrant or subpoena is needed to get the information, and then vendors have to supply the information for you. In cases involving imminent danger, law enforcement can file for emergency requests; however. Facebook, SnapChat, and other OSNs usually have legal staff who evaluate these requests. SnapChat, for example, has a downloadable guide for law enforcement. Twitter vehemently opposes government requests and cites the U.S. Fourth Amendment to refuse all requests. Facebook, however, has begun accommodating international requests.

Facebook has two types of profiles: basic subscriber info and extended subscriber info (called Neoprint). Basic subscriber info simply tells you the last time a person logged on, his or her e-mail address and associated mobile number, and whether the account can be viewed publicly. The Neoprint profile includes friends, groups, video feeds, and undeleted photos ("U.S. Law Enforcement obtaining warrants to search Facebook Profiles," www.foxnews.com/tech/2011/07/12/us-law-enforcement-obtain-warrants-to-search-facebook-profiles/, 2011). Typically, this profile is given to law enforcement only with a warrant.

Note

Stroz-Freidburg, an established company specializing in e-discovery, digital forensics, and fraud accounting, has created procedures on how to approach social media forensics (www.strozfriedberg.com/how-we-help/capture-emerging-data-types/), such as

collecting and validating social media content, determining what data should be collected, and maintaining the chain of custody with evidence that's variable in nature.

Many types of cases involve social media. For example, a company selling illegal knock-offs might use social media to sell its merchandise. As an investigator, you need a big-picture perspective to determine what evidence might apply to a case and where to look for information. With the advent of social media and the cloud, locations to examine for evidence are no longer limited to physical devices, such as cell phones and laptops.

Social Media Forensics on Mobile Devices

In mid-2017, Facebook had 2 billion users worldwide. Of those, 1.74 billion, or 87%, were mobile users (www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/). Although Twitter has only 328 million monthly users, 80% of them are mobile users (www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/). A study in 2012 examined Facebook, Twitter, and MySpace use on BlackBerries, iPhones, and Android devices and discovered, for example, that physical acquisitions of iPhones required "jailbreaking," meaning they got root access to the device's OS to bypass the provider's codes for preventing users from switching to other providers and preventing unauthorized people from taking actions an investigator would take (Noora Al Mutawa, et al, "Forensic analysis of social networking applications on mobile devices," *Digital Investigation* 9, 2012, www.dfrws.org/2012/proceedings/DFRWS2012-3.pdf).

In addition, they found that evidence artifacts vary depending on the social media channel and the device. For example, on iPhones, a SQLite database for Facebook was found that lists friends, their ID numbers, and phone numbers as well as files that tracked all uploads, including pictures. Similar databases were found on Twitter. On Android devices, Facebook friends were found in the contacts list because these devices synchronized with Facebook. Forensic analysis also showed that iPhone and Android devices yielded the most information, and much of the data was stored in SQLite databases. Following standard procedures—doing a logical acquisition followed by a physical acquisition—can yield solid evidence, especially with devices that aren't locked.

Forensics Tools for Social Media Investigations

Software for social media forensics is being developed, but not many tools are available. A number of social media tools that were free or inexpensive have now been incorporated into forensics suites, such as FTK Social Analyzer, or offer only 14-day to 30-day trials. In addition, there are many questions about how the information these tools gather can be used in court or in arbitration. Investigators often run into the problem of finding information unrelated to a case, and sometimes they must stop to get another warrant or subpoena, such as investigating a claim of fraud and finding evidence of corporate espionage. Using social media forensics software might also require getting the permission of people whose information is being examined.

Many OSN tools use customized Web crawlers to find data, but they take too long to find information to make them efficient. A few helpful software packages are available, however. For example, X1 Social Discovery (www.x1.com/products/x1_social_discovery/) can be used in two modes in Facebook: a credentialed user account (which requires the username and password of the person under investigation) and a public account (created to examine the publicly accessible posts of people or groups). X1 also has tools for Twitter and YouTube. In addition, researchers created an open-source tool to target Facebook accounts (Huber, Mulazzani, et al, "Social Snapshots: Digital Forensics for Online Social Networks," ACSAC '11, Proceedings of the 27th Annual Computer Security Applications Conference, December 2011, www.sba-research.org/wp-content/uploads/publications/social_snapshots_preprint.pdf).

As with any investigation, you need a warrant or subpoena to ask an OSN to produce its records. There are other approaches you can take, however. If people are cooperating with your investigation, they might give you the usernames and passwords to their social media accounts. If not, you can access only their public profile or become friends with one of their friends, which might give you limited information. For this approach, there are a few steps you need to take:

1. Begin with a workstation that doesn't contain any of your personal information, or create a virtual machine with a bridged network (meaning it has a different IP address from the host computer).
2. Many people link their cell phone numbers to their Facebook accounts, so try looking up the suspect's cell phone number in Facebook, which shows you the person's username, too. People often use the same username in all platforms, including Twitter, Instagram, LinkedIn, and so forth.
3. Next, you should do a Google search on this username, making sure to use your investigation workstation. Disable Google's Safe Search feature and "instant results," which Google uses to guess what you're searching for. Last, but not least, turn off location-based searches so that Google doesn't use your location to filter results. For example, if you're searching for a restaurant serving pizza and you're in New York City, Google won't return search results for Miami—or any other city.
4. Collect as much information as possible on Google, and use it to find friends of the suspect and then attempt to friend these people. With some social media tools, you need to create a decoy account. Remember that it's against the law to use someone else's likeness as your own for a social media account, and operating within the law is crucial in any investigation.

Chapter Summary

- E-mail fraudsters use phishing, pharming, and spoofing scam techniques. Phishing e-mails typically lure users to sites or ask for sensitive information. Pharming e-mails redirect users to Web sites that look like legitimate businesses or official government Web sites and solicit personal identity information from victims.
- In both Internet and intranet e-mail environments, e-mail messages are distributed from one central server to connected client computers, a configuration called a client/server architecture. The server uses server e-mail software to provide e-mail services. Client computers use e-mail programs (also called e-mail clients) to contact the e-mail server and send and retrieve e-mails.
- Investigating crimes or policy violations involving e-mail is similar to investigating other types of computer abuse and crimes. Your goal is to find out who's behind the crime, collect the evidence, and build a case.
- Forensics linguistics is a field where language and the law intersect to determine the author of e-mails, text messages, and other online communications; it encompasses civil cases, criminal cases, cyberterrorism cases, and other legal proceedings. Evidence from forensic linguists is now accepted in many courts worldwide. Forensic linguists can determine, for example, whether a certain person actually wrote an e-mail, where he or she might be from, and in some cases, his or her original language or dialect.
- After determining that a crime has been committed involving e-mail, access the victim's computer, if possible, and then use the installed e-mail program to find the e-mail the victim received. Next, copy and print the e-mail. You might also want to forward the message to another e-mail address, depending on your organization's guidelines.
- Investigators use e-mail headers to trace the route e-mails take through servers. They can also use this information to determine who really sent an e-mail or pinpoint the sender's location.
- To find an e-mail header, investigators generally use the e-mail program that created the message. The header provides supporting evidence and can help track a suspect to an e-mail's originating location by finding the domain or IP address. Also helpful are the date and time a message was sent, the filenames of any attachments, and the unique ID number, if it's supplied. With the originating e-mail address, investigators can track a message to a suspect by doing reverse lookups.
- To investigate e-mail abuse, you should know how an e-mail server records and handles e-mail. Some e-mail servers use databases that store users' e-mails; others use a flat file system. E-mail servers also maintain a log (by default or through configuration settings) of all e-mails that are processed.
- For many e-mail investigations, you can rely on e-mail files, e-mail headers, and e-mail server log files. However, if the e-mail administrator isn't willing to turn over records and files, or you encounter a highly customized e-mail environment, you can use data recovery tools and forensics tools designed to recover e-mail files.
- For other e-mail applications that use the mbox format, a hexadecimal editor can be used to carve messages manually. This technique requires perseverance because it's tedious and time consuming.
- Social media, or online social networks (OSNs), can provide evidence in criminal and civil cases, so software for collecting OSN information is being developed.

Because of the variety and amount of data involved in OSN investigations, techniques of big data analytics are usually needed.

- The majority of people engaging in social media communications are mobile users. Almost all mobile devices store data in a SQLite database, but evidence artifacts vary depending on the social media channel and the device.
- Social media forensics tools have evolved with the technology, and many forensics suites have built-in social media tools. They're designed to access Facebook, Twitter, and other OSN user accounts and examine pictures, postings, videos, friend lists, and so forth. These tools can be used to find out which people users have been in touch with, when, and how often.

Key Terms

client/server architecture
Electronic Communications Privacy Act (ECPA)
Enhanced/Extended Simple Mail Transfer Protocol (ESMTP)
forensic linguistics
Internet Message Access Protocol 4 (IMAP4)
mbox
Messaging Application Programming Interface (MAPI)
Multipurpose Internet Mail Extensions (MIME)
online social networks (OSNs)
pharming
phishing
Post Office Protocol version 3 (POP3)
Simple Mail Transfer Protocol (SMTP)
spoofing
Stored Communications Act (SCA)

Review Questions

1. E-mail headers contain which of the following information?
   a. The sender and receiver e-mail addresses
   b. An ESMTP number or reference number
   c. The e-mail servers the message traveled through to reach its destination
   d. The IP address of the receiving server
   e. All of the above
2. What's the main piece of information you look for in an e-mail message you're investigating?
   a. Sender or receiver's e-mail address
   b. Originating e-mail domain or IP address
   c. Subject line content
   d. Message number
3. In Microsoft Outlook, e-mails are typically stored in which of the following?
   a. .pstand .ostfiles
   b. res1.log and res2.log files

c. PU020102.db file

d. .evolution file

4. When searching a victim's computer for a crime committed with a specific e-mail, which of the following provides information for determining the e-mail's originator?

   a. E-mail header

   b. Username and password

   c. Firewall log

   d. All of the above

5. Phishing does which of the following?

   a. Uses DNS poisoning

   b. Lures users with false promises

   c. Takes people to fake Web sites

   d. Uses DHCP

6. Which of the following is a current formatting standard for e-mail?

   a. SMTP

   b. MIME

   c. Outlook

   d. HTML

7 After examining e-mail headers to find an e-mail's originating address, investigators use forward lookups to track an e-mail to a suspect. True or False?

8. When you access your e-mail, what type of computer architecture are you using?

   a. Mainframe and minicomputers

   b. Domain

   c. Client/server

   d. None of the above

9. To trace an IP address in an e-mail header, what type of lookup service can you use?

   a. Intelius Inc.'s AnyWho online directory

   b. Verizon's http://superpages.com

   c. A domain lookup service, such as www.arin.net, www.internic.com, or www.whois.net

   d. Any Web search engine

10. Router logs can be used to verify what types of e-mail data?

    a. Message content

    b. Content of attached files

    c. Tracking flows through e-mail server ports

    d. Finding blind copies

11. Logging options on e-mail servers can be which of the following?

    a. Disabled by users

    b. Set up in a circular logging configuration

    c. Configured to a specified size before being overwritten

    d. Typically set to periodic logging mode

12. On a UNIX-like system, which file specifies where to save different types of e-mail log files?
    a. maillog
    b. /var/spool/log
    c. syslog.conf
    d. log
13. What information is *not* in an e-mail header?
    a. Blind copy (bcc) addresses
    b. Internet addresses
    c. Domain name
    d. Contents of the message
    e. Type of e-mail server used to send the e-mail
14. Which of the following types of files can provide useful information when you're examining an e-mail server?
    a. .dbf files
    b. .emx files
    c. .log files
    d. .slf files

15 E-mail accessed with a Web browser leaves files in temporary folders. True or False?

16. When confronted with an e-mail server that no longer contains a log with the date information you need for your investigation, and the client has deleted the e-mail, what should you do?
    a. Search available log files for any forwarded messages.
    b. Restore the e-mail server from a backup.
    c. Check the current database files for an existing copy of the e-mail.
    d. Do nothing because after the file has been deleted, it can no longer be recovered.

17 You can view e-mail headers in Notepad with all popular e-mail clients. True or False?

18 To analyze e-mail evidence, an investigator must be knowledgeable about an e-mail server's internal operations. True or False?

19. Sendmail uses which file for instructions on processing an e-mail message?
    a. sendmail.cf
    b. syslogd.conf
    c. mese.ese
    d. mapi.log

20 A forensic linguist can determine an author's gender by analyzing chat logs and social media communications.

Hands-On Projects

Create a *Work*\Chap11\Projects folder on your system for this chapter's projects. The data files you need for the first two projects are from the Enron case. For the third project, you use the case file from the in-chapter activity you did in Magnet AXIOM.

Note

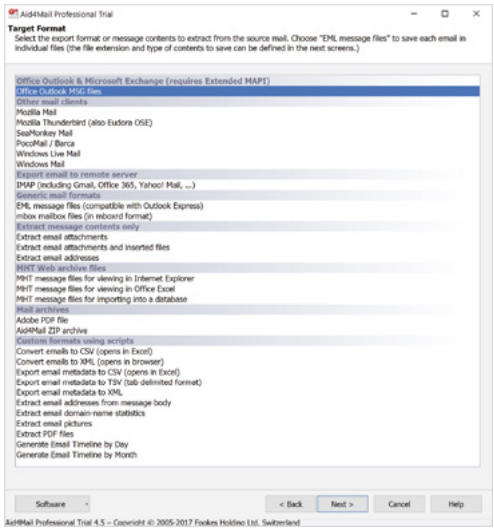
If your instructor hasn't already done so, go to http://info.nuix.com/Enron.html to register for the Enron data set and get information on downloading the cleansed Enron e-mail.

Hands-On Project 11-1

For this project, you use Aid4Mail to examine an Enron employee's e-mail.

1. First, create a subfolder of your work folder called **HandsOn11-1**. Then start your Web browser, and go to **www.aid4mail.com/download-free-trial**. Download and install Aid4Mail.
2. Go to the link you got for cleansed Enron e-mail. Download the complete Enron EDRM data set of 18 GB. Uncompress the file to your work folder, and copy the **eric_saibi.pst** file to your *Work*\Chap11\Projects folder.
3. Start Aid4Mail. Click **Next** in the Welcome window. Click **Office Outlook PST** file, and then click **Next**.
4. Navigate to and click the **eric_saibi.pst** file, and then click **Next**. In the Source MAPI Folders window, click **Next**.
5. In the Filter Options window, you can select a range of dates and words to search for. For now, leave the default settings, and click **Next**.
6. In the Target Format window, scroll to the bottom and examine the export options shown in **Figure 11-13**. You can export metadata in CSV or XML format, for example. Click **Convert e-mails to CSV**, and then click **Next**.

Figure 11-13.



Source: Fookes Software, www.aid4mail.com

Export options in Aid4Mail

7. In the Target Settings window, click the **HandsOn11-1** subfolder of your work folder, and enter the filename **Eric_Saibi.CSV**. Click **Next**, and then click **Start**.
8. After Aid4Mail has finished converting the e-mail to CSV format, open the file in Microsoft Excel (or any spreadsheet program), and exit Aid4Mail. Scroll through Eric Saibi's e-mail data and look for messages that might contain personal information or be

related to the Enron scandal. Go to the Aid4Mail Web site and read the user manual. What can be done to make viewing data easier? Write a short paper describing the options.

Hands-On Project 11-2

In this project, you use Autopsy for Windows to examine e-mail from the Enron case.

Note

Make sure you downloaded the cleansed Enron data set in **Hands-On Project 11-1**.

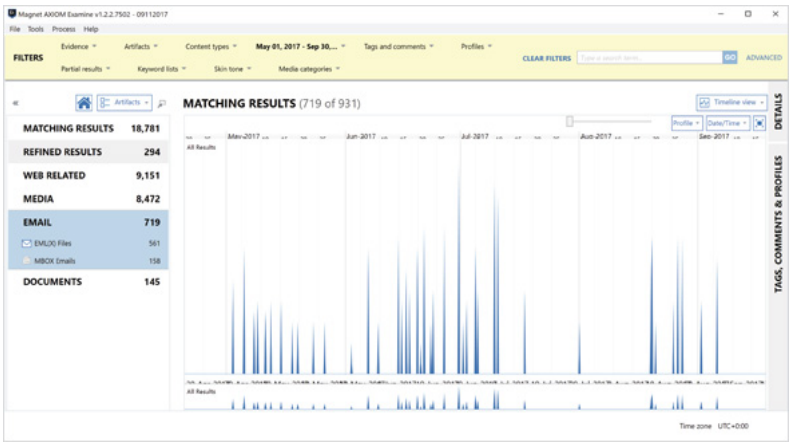
1. Start Autopsy for Windows, and click the **Create New Case** button. In the New Case Information window, enter **Enron** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**. In the Additional Information window, type today's date in the Case Number text box and your name in the Examiner text box, and then click **Finish**.
2. In the Select Data Source window, click the **Select data source type** list arrow, and click **Logical Files**. Click the **Browse** button next to the "Browse for an image file" text box, navigate to your work folder, click the Kenneth Lay **.pst** files, and then click **Open**. Click **Next**.
3. In the Configure Ingest Modules window, click **Next**, and then click **Finish**. When Autopsy has finished processing the ingest modules (about 20 minutes), click **Keyword Search** at the upper-right corner and enter the following search keywords: **trade, trading, stocks**, and **money**.
4. Research Kenneth Lay's role in the Enron scandal, and then examine his e-mails. What additional words would you add to the search terms? When you're finished, exit Autopsy for Windows.
5. Write a report describing your results. What evidence did you find about Kenneth Lay's part in the Enron case? What's your assessment of using Autopsy to examine e-mail?

Hands-On Project 11-3

In this project, you use Magnet AXIOM to create a timeline of the e-mails Jim Shu sent and received.

1. Start Magnet AXIOM Examine, and under the "Open a recent case" heading, click the **InChapter11** case. Click **EMAIL** in the pane on the left.
2. In the upper-right corner, click **Histogram view** in the drop-down list. What can you determine from this view?
3. Next, click **Timeline view** in the same drop-down list. The timeline shows a spike in 2017, which indicates increased activity. You should examine any e-mails sent or received during these spikes.
4. In the drop-down list under the view selection, click **Date**. A calendar drops down. For the start date, click the arrow button until you get to May, and then click **May 1**. For the end date, click **September 30**, and then click **OKAY**. The timeline in Figure 11-14 shows the e-mail activity in this date range, which helps you know where to look for e-mails.

Figure 11-14.



Source: Magnet Forensics, www.magnetforensics.com

The Magnet AXIOM timeline with a filter applied

5. Click **CLEAR FILTERS**, and then exit Magnet AXIOM Examine. Write a one- to two-page paper describing the information you found.

Case Projects

Case Project 11-1

You get a call from a high school student named Marco who claims he just received a Facebook message from another student who was threatening to commit suicide. Marco isn't sure where the student was when he sent the message. Write a brief report explaining how you should proceed, including what you should do first in this situation.

Case Project 11-2

A mother calls you to report that her 15-year-old daughter has run away from home. She has access to her daughter's e-mail account and says her daughter has e-mails in her inbox suggesting she has run away to be with a 35-year-old woman. Her daughter has also made related posts on Snapchat. Write a brief report explaining how you should proceed.

Case Project 11-3

X1 Social Discovery is a forensics package for OSNs. The orientation videos advise that investigators create a Facebook or similar OSN profile without friends, groups, or associates attached to it. Go to www.x1.com/products/x1_social_discovery/ and download the user information and 14-day free trial. Write a one- to two-page paper in which you support or argue against the safeguards that are recommended before you use this tool to gather information on a social media account.

Chapter 12. Mobile Device Forensics and the Internet of Anything

After reading this chapter and completing the exercises, you will be able to:

> - Explain the basic concepts of mobile device forensics
> - Describe procedures for acquiring data from mobile devices
> - Summarize the challenges of forensic acquisitions of data stored on Internet of Anything devices

This chapter explains how to retrieve information from a cell phone, smartphone, tablet, or other mobile device and explores social media content on mobile devices in more depth. Although some projects use free and demo software, the software and hardware discussed in this chapter are usually expensive and not supplied in this book's downloads on the student companion site. Check with your instructor to see whether any is available at your organization.

The field of mobile device forensics changes rapidly and poses challenges in trying to retrieve information. Unlike what you might see in television shows, you don't just start scrolling through contact lists or most recent calls. As with all digital investigations, you must follow the forensics procedures described in this chapter.

As more devices are now capable of accessing the Internet, the terminology to describe this phenomenon has changed from the Internet of Things to the Internet of Everything to the Internet of Anything. So many devices access the Internet; practically anything can be online and connected, which poses new challenges in investigations.

Understanding Mobile Device Forensics

People store a wealth of information on cell phones and smartphones, and the thought of losing your phone and, therefore, the information stored on it can be a frightening prospect. Despite this concern, not many people think about securing their phones, although they routinely lock and secure laptops or desktops. Depending on your phone's model, the following information might be stored on it:

- Incoming, outgoing, and missed calls
- Multimedia Message Service (MMS; text messages) and Short Message Service (SMS) messages
- E-mail accounts
- Instant messaging (IM) logs
- Web pages
- Photos, videos, and music files
- Calendars and address books
- Social media account information
- GPS data
- Voice recordings and voicemail
- Bank account logins
- Access to your home

Many people store more information on smartphones and tablets than on computers. When you consider that smartphones have the same computing power as desktops of a few years ago, the amount of information stored on them is often enough to piece together a case's facts.

Top-of-the-line smartphones are even comparable to current mid-range computers ("Computer vs. Smartphone," www.computerhope.com/issues/ch001398.htm). In many countries, phones are used to log in to bank accounts, make deposits, and transfer funds from one device to another, which provides even more potential evidence.

Note

The use of smartphones for illicit activities—such as identity theft, child pornography, and bank fraud—has become more prevalent.

Because mobile devices are seized at the time of arrest, police used to look through them as a routine matter. The Supreme Courts of Oregon and Ohio, however, ruled that a search warrant is needed to examine these devices because of all the information they can contain. In 2014, the U.S. Supreme Court ruled unanimously in *Riley v. California* that a search warrant is required before an arresting officer can begin examining a phone's contents (www.newrepublic.com/article/118396/supreme-court-cellphone-case-went-further-privacy-advocates-hoped, June 2014). Furthermore, because phones often contain private or sensitive information, any information that doesn't pertain to the case must be redacted from the public record. Despite the usefulness of these devices in providing clues for investigations, investigating smartphones and other mobile devices is a challenging task in digital forensics. No single standard exists for how and where phones store messages, although many phones use similar storage schemes. In addition, new phones come out about every six months, and they're rarely compatible with previous models. Therefore, the cables, software, and accessories used for forensics acquisitions can become obsolete in a short time.

Mobile Phone Basics

Mobile phone technology has advanced rapidly in the past few decades and developed far beyond what its inventors could have imagined. Gone are the days of two-pound cell phones that only the wealthy could afford. By the end of 2008, mobile phones had gone through three generations: analog, digital personal communications service (PCS), and **third-generation (3G)** . 3G introduced unheard-of capabilities, such as being able to download while you were walking or in a moving vehicle. Sprint Nextel introduced the **fourth-generation (4G)** network in 2009. Several technologies can be used for 4G networks and are discussed later in this section. **Fifth-generation (5G)** cellular networks, expected to be finalized in 2020, will incorporate emerging technologies, including the ever-expanding cloud and device-to-device networks.

Many digital networks are used in the mobile phone industry, and **Table 12-1** lists the main ones. Much of this table is taken from the National Institute of Standards and Technology (NIST) document "Guidelines on Mobile Device Forensics" (Special Publication [SP] 800-101, Revision 1, May 2014; http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf). You can download this document to learn more.

Table 12-1. Digital Networks

Digital network	Description
Code Division Multiple Access (CDMA)	Developed during World War II, this technology was patented by Qualcomm after the war. One of the most common digital networks, it uses the full radio frequency spectrum to define channels. In the United States, Sprint, U.S. Cellular, and Verizon, for example, use CDMA networks.
Global System for Mobile Communications (GSM)	Another common digital network, it's used by AT&T and T-Mobile in the United States and is the standard in Europe and Asia.
Time Division Multiple Access (TDMA)	This digital network uses the technique of dividing a radio frequency into time slots; GSM networks use this technique. It also refers to a specific cellular network standard covered by Interim Standard (IS) 136.
Integrated Digital Enhanced Network (iDEN)	This Motorola protocol combines several services, including data transmission, into one network.

Digital network	Description
Digital Advanced Mobile Phone Service (D-AMPS)	This network is a digital version of the original analog standard for cell phones.
Enhanced Data GSM Environment (EDGE)	This digital network, a faster version of GSM, is designed to deliver data.
Orthogonal Frequency Division Multiplexing (OFDM)	This technology for 4G networks uses energy more efficiently than 3G networks and is more immune to interference.

Most **Code Division Multiple Access (CDMA)** networks conform to IS-95, created by the **Telecommunications Industry Association (TIA)** . These systems are referred to as CDMAOne, and when they went to 3G services, they became CDMA2000.

Global System for Mobile Communications (GSM) uses the **Time Division Multiple Access (TDMA)** technique, in which multiple phones take turns sharing a channel on a round-robin basis. As noted in Table 12-1, TDMA also refers to the IS-136 standard, which introduced sleep mode to enhance battery life. TDMA can operate in the cell phone (800 to 1000 MHz) or personal communications service (PCS; 1900 MHz) frequency, so it's compatible with several cell phone networks.

The 3G standard was developed by the **International Telecommunication Union (ITU)** under the United Nations. It's compatible with CDMA, GSM, and TDMA. The **Enhanced Data GSM Environment (EDGE)** standard was developed specifically for 3G.

Note

GSM carriers, by definition, must accept any GSM phone. CDMA carriers have locked phones and don't have to accept any users who aren't subscribers. Until recently, users who traveled frequently between the United States, Africa, Europe, and parts of Asia needed separate phones for each place. With GSM phones, you simply pop in a SIM card for the country you're currently in.

In 2008, the International Telecommunication Union Radio (ITU-R) created the requirements for carriers to be considered 4G (www.whatsag.com/G/Understanding_4G.php). 4G networks can use the following technologies:

- *Orthogonal Frequency Division Multiplexing*—The **Orthogonal Frequency Division Multiplexing (OFDM)** technology uses numerous parallel carriers instead of a single broad carrier and is less susceptible to interference (http://bwrcs.eecs.berkeley.edu/Classes/EE225C/Lectures/Lec16_ofdm.pdf).
- *Mobile WiMAX*—This technology uses the IEEE 802.16e standard and Orthogonal Frequency Division Multiple Access (OFDMA) and supports transmission speeds of 12 Mbps. Sprint chose this technology for its 4G network, although some argue it's not true 4G.
- *Ultra Mobile Broadband (UMB)*—Also known as CDMA2000 EV-DO, this technology was used by CDMA network providers to switch to 4G and supports transmission speeds of 275 Mbps for downlinks and 75 Mbps for uplinks. It has been replaced by LTE (described later in this list).
- *Multiple Input Multiple Output (MIMO)*—This technology, developed by Airgo and acquired by Qualcomm, supports transmission speeds of 312 Mbps and is used by 4G, WiMAX, and other technologies.
- *Long Term Evolution (LTE)*—This technology, designed for GSM and Universal Mobile Telecommunications Systems (UMTS) technology, supports 45 Mbps to 144 Mbps transmission speeds. Commonly called "4G LTE."

Tip

As an investigator, you should research these technologies to make sure you stay up to date.

Although digital networks use different technologies, they operate on the same basic principles. Geographic areas are divided into cells resembling honeycombs. As described in NIST SP 800-101 (mentioned earlier in this section), three main components are used for communication with these cells:

- *Base transceiver station (BTS)*—This component is made up of radio transceiver equipment that defines cells and communicates with mobile phones; it's sometimes referred to as a "cell phone tower," although the tower is only one part of the BTS equipment.
- *Base station controller (BSC)*—This combination of hardware and software manages BTSs and assigns channels by connecting to the mobile switching center.
- *Mobile switching center (MSC)*—This component connects calls by routing digital packets for the network and relies on a database to support subscribers. This central database contains account data, location data, and other key information needed during an investigation. If you have to retrieve information from a carrier's central database, you usually need a warrant or subpoena.

Inside Mobile Devices

Mobile devices can range from simple phones to **smartphones** , tablets, and smartwatches. The hardware consists of a microprocessor, ROM, RAM, a digital signal processor, a radio module, a microphone and speaker, hardware interfaces (such as keypads, cameras, and GPS devices), and an LCD display. Many have removable memory cards and up to 64 GB of internal memory, and Bluetooth and Wi-Fi are included in most mobile devices ("Guidelines on Mobile Device Forensics," SP 800-101, Revision 1, May 2014; http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf).

Most basic phones have a proprietary OS, although smartphones use the same OSs as PCs (or stripped-down versions of them). These OSs include Windows Mobile, RIM OS, Android (based on Linux), Google OS, and iOS (for Apple devices). Typically, phones store system data in **electronically erasable programmable read-only memory (EEPROM)** , which enables service providers to reprogram phones without having to access memory chips physically. Many users take advantage of this capability by reprogramming their phones to add features or switch to different service providers. Although this reprogramming isn't supported officially by service providers, instructions on how to do so are readily available on the Internet.

The OS is stored in ROM, which is nonvolatile memory, so along with other data, it's available even if the phone loses power. Acquiring data from ROM is covered in more detail later in "Understanding Acquisition Procedures for Mobile Devices."

For personal use, personal digital assistants (PDAs) have been replaced by iPods, iPads, and other mobile devices. The use of PDAs has shifted to more specific markets, such as medical or industrial PDAs; they're now called "handhelds" and are still sold on sites such as Amazon and eBay. Palm Pilot and Microsoft Pocket PC were popular models when PDAs came on the market in the 1990s. HP purchased Palm and used the OS in its early touchpads. Similar to smartphones, PDAs housed a microprocessor, flash ROM, RAM, and other hardware components. As with smartphones, the amount of information on a PDA varied depending on the model. Usually, you could retrieve a user's calendar, address book, Web access, and other items.

A number of peripheral memory cards were used with PDAs:

- *Compact Flash (CF)*—CF cards were used for extra storage and work much the same way as PCMCIA cards.
- *MultiMediaCard (MMC)*—MMC cards were designed for mobile phones, but they can be used with PDAs to provide another storage area.
- *Secure Digital (SD)*—SD cards are similar to MMCs but have added security features to protect data; they're now used on smartphones.

Most PDAs were designed to synchronize with a computer, so they had built-in slots for that purpose (whether hard-wired or wireless synchronization). Although you're not likely to encounter one during an investigation, having some background information on PDAs is still useful.

SIM Cards

Subscriber identity module (SIM) cards are usually found in GSM devices and consist of a microprocessor and internal memory. SIM cards are similar to standard memory cards, except the connectors are aligned differently. iPhones and many Android phones have micro SIM and nano SIM slots. However, some can be accessed only if the phone has been unlocked.

GSM refers to mobile phones as "mobile stations" and divides a station into two parts: the SIM card and the mobile equipment (ME), which is the remainder of the phone. The SIM card is necessary for the ME to work and serves these additional purposes:

- Identifies the subscriber to the network
- Stores service-related information
- Can be used to back up the device

SIM cards come in three sizes: standard, micro, and nano. Portability of information is what makes SIM cards so versatile. By switching a SIM card between compatible phones, users can move their provider usage and other information to another phone automatically without having to notify the service provider. For example, if you travel between neighboring countries often, you could have a GSM phone and two SIM cards. When you travel to another country, you simply switch to the other SIM card. With phones on which this switching is allowed, information such as your contact list is stored on the phone, so when you switch to another carrier, all you have to do is change the SIM card. Another common practice is switching to another SIM card when you have used most of your monthly minutes on your main SIM card.

Note

Older CDMA phones don't use SIM cards; they incorporate the card's functions into the phone. Newer TDMA phones in North America do use SIM cards, however, and they are sealed so that users must contact the service provider when changing phones or providers.

As mentioned, many phones now include SD cards for external storage. Standard SD cards range from 16 GB to 64 GB and can be part of a mobile device or game console. Other sizes include miniSD and microSD cards. Note, however, that many Google Nexus devices don't have SD cards.

Understanding Acquisition Procedures for Mobile Devices

Search and seizure procedures for mobile devices are as important as procedures for computers. The main concerns are loss of power, synchronization with cloud services, and

remote wiping. All mobile devices have volatile memory, so making sure they don't lose power before you can retrieve RAM data is critical. At the investigation scene, determine whether the device is on or off. If it's off, leave it off, but find the charger and attach it as soon as possible. Note this step in your log if you can't determine whether the device was charged at the time of seizure. If the device is on, check the display for the battery's current charge level.

Because mobile devices are often designed to synchronize with applications on a user's laptop or tablet, any mobile device attached to a PC or tablet via a USB cable or micro USB cable should be disconnected immediately. Many people use their smartphones to get Internet access for tablets or laptops, so you might find these devices already connected to the Internet. Disconnecting them immediately helps prevent synchronization that might occur automatically on a preset schedule and overwrite data on the device. In addition, collect the laptop and any peripheral devices to determine whether the hard drive contains any information that's been transferred and then deleted from the mobile device, including pictures, videos, and other files that have been transferred and then deleted.

Depending on the warrant or subpoena, the time of seizure might be relevant. In addition, messages might be received on the mobile device after seizure that may or may not be admissible in court. If you determine that the device should be turned off to preserve battery power or prevent a possible attack, note the time and date when you take this step. The alternative is to isolate the device from incoming signals with one of the following options:

- Place the device in airplane mode, if this feature is available.
- Place the device in a paint can, preferably one that previously contained radio wave-blocking paint.
- Use a Faraday bag that conforms to Faraday wire cage standards. Many allow plugging a unit into a power source (http://faradaybag.com or www.disklabs.com/faraday-bags/).
- Turn the device off.

The drawback of using these isolating options is that the mobile device is put into roaming mode, which accelerates battery drainage. Most mobile devices shut themselves off or enter a "sleep state" after reaching a certain low battery level. In either case, a phone that's been seized for investigation must be isolated from incoming signals and from broadcasting.

Caution ⚠

Make sure you handle all components with care and protect them from environmental factors and sources of electromagnetic interference (EMI).

SANS DFIR (Digital Forensics and Incident Response) has a slightly different process that handles other possible problems (http://digital-forensics.sans.org/blog/2014/06/24/getting-the-most-out-of-smartphone-forensic-exams-sans-advanced-smartphone-forensics-poster-release). It lists three conditions: The device is on and unlocked, the device is on and locked, and the device is off. If it's on and unlocked, you must isolate it from the network, disable the screen lock, and remove the passcode, among other tasks. If the device is on and locked, what you can and can't do varies depending on the type of device, such as whether it's a BlackBerry, an iPhone, or an Android. If the device is off, you should attempt a physical static acquisition and then turn the device on, determine whether it's locked, and then follow the procedure for either a locked or unlocked condition. As devices become more sophisticated, turning them off means removing the battery.

When you're back in the forensics lab, you need to assess what can be retrieved. To determine whether you should do a logical acquisition or physical acquisition, you need to know where information is stored. As with laptops and desktops, a logical acquisition involves accessing

files and folders as you would see them when looking at them in File Explorer. A physical acquisition is a bit-by-bit acquisition done to find deleted files or folders. You should check the following locations for information, keeping in mind that with mobile devices, often you need manufacturers' tools:

- Internal memory
- SIM card
- Removable or external memory cards
- Network provider

Because of wiretap laws, checking providers' servers requires a search warrant or subpoena, so you need one if you want to check voicemail stored by the provider or another third party, for example. In addition, because most newer phones and phone plans store voicemail on the phone, you need a search warrant for the device, too. You might also need information from the service provider to determine where the suspect or victim was at the time of a call, to access backups of contacts, and more. In the past, you had to serve the provider with a warrant to have a triangulation of a cell tower done to determine location. This is still true if you're doing an ongoing investigation and don't have the device. If, however, you have the device, you can usually retrieve GPS data from it.

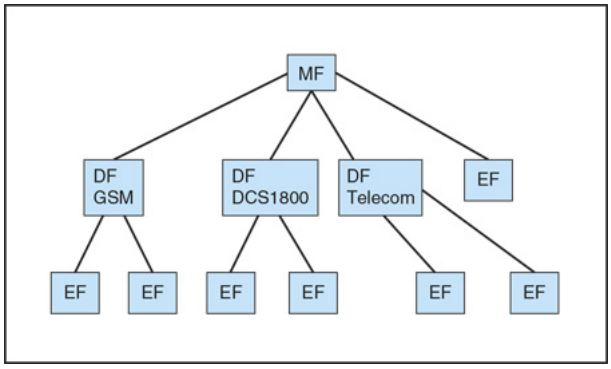
Checking with the service provider has been further complicated because backups might be stored in a cloud provided by the carrier or a third party. For iPods and iPads, syncing and backups tend to occur in the iCloud; other providers offer a similar cloud backup.

Given how crucial smartphones are now, people who lose them are concerned about the amount of sensitive information that can be gathered from them. Because of the growing problem of mobile devices being stolen, service providers have started using remote wiping to remove a user's personal information stored on a stolen device, and this procedure often results in the loss of valuable information for investigations. Remote wiping is usually done to remove an account so that a thief can't use the phone and rack up charges. It also erases all contacts, the calendar, and other personal information, such as photos and bank logins, stored on the device. In some instances, it restores the device to the original factory settings. Depending on the device and service provider, the device owner or the service provider can do the remote wipe. Remote wiping can be used by device owners trying to protect their information.

Memory storage on a mobile device is usually a combination of volatile and nonvolatile memory. Volatile memory requires power to maintain its contents, but nonvolatile memory doesn't. Although the locations of data vary from one phone model to the next, volatile memory usually contains data that changes frequently, such as missed calls, text messages, and sometimes even user files. Nonvolatile memory, on the other hand, contains OS files and stored user data, such as a personal information manager (PIM) and backed-up files.

As mentioned, memory resides in the phone and in the SIM card, if the device is equipped with one. The file system for a SIM card is a hierarchical structure (see **Figure 12-1**). This file structure begins with the root of the system (MF). The next level consists of directory files (DF), and under them are files containing elementary data (EF). In this figure, the EFs under the GSM and DCS1800 DFs contain network data on different frequency bands of operation. The EFs under the Telecom DF contain service-related data.

Figure 12-1.



SIM file structure

You can retrieve quite a bit of data from a SIM card, depending on whether the phone is GSM or CDMA. The information that can be retrieved falls into four categories:

- Service-related data, such as identifiers for the SIM card and subscriber
- Call data, such as numbers dialed
- Message information
- Location information

If power has been lost, you might need PINs or other access codes to view files. Typically, users keep the original PIN assigned to the SIM card, so when you're collecting evidence at the scene, look for users' manuals and other documentation that can help you access the SIM card. With most SIM cards, you have three attempts at entering an access code before the device is locked, which then requires calling the service provider to get the PIN unlock key (PUK) and waiting a certain amount of time before trying again. Common codes to try are 1-1-1-1 or 1-2-3-4.

Mobile Forensics Equipment

Mobile forensics is an evolving science, with the biggest challenge being constantly changing phone models. What works today might not work on a model that comes out tomorrow. This section gives you an overview of procedures for working with mobile forensics software, and specific tools are discussed in the following sections.

The first step is identifying the mobile device. Most users don't alter their devices, but some file off serial numbers, change the display to show misleading data, and so on. When attempting to identify a phone, you can make use of several online sources, such as www.phonescoop.com.

Next, make sure you have installed the mobile device forensics software. As mentioned, not all facilities are equipped with the necessary software because many tools are cost prohibitive. Some vendors offer tools that simply take pictures of screens as you scroll through them. Forensically, this approach isn't the best, but you can use it if no other alternatives are available.

The next step is to attach the phone to its power supply and connect the correct cables. Most phones now have a combination USB/power cable, and many are interchangeable. For older phones, often you have to rig cables together. Some vendors have toolkits with an array of cables you can use (discussed later in "**Using Mobile Forensics Tools**").

After you've connected the device, start the forensics software and begin downloading the available information. If your forensics software doesn't support the model you're

investigating, you might need to acquire other tools. Your main concern should be that the software is forensically sound.

SIM Card Readers

With GSM phones and many newer models of mobile devices, the next step is accessing the SIM card, which you can do by using a combination hardware/software device called a "SIM card reader." To use this device, you should be in a forensics lab equipped with antistatic devices. In addition, biological agents, such as fingerprints, might be present on the inside of the case, so you should consult the lead investigator when you're ready to proceed to this step. The general procedure is as follows:

1. Remove the device's back panel.
2. Remove the battery.
3. Remove the SIM card from its holder.
4. Insert the SIM card into the card reader, which you insert into your forensic workstation's USB port.

A variety of SIM card readers are available. Some are forensically sound and some are not; make sure you note this feature in your investigation log. Another problem with SIM card readers is dealing with text and SMS messages that haven't been read yet. After you view a message, the device shows the message as opened or read. For this reason, documenting messages that haven't been read is critical. Using a tool that takes pictures of each screen can be valuable because these screen captures can provide additional documentation.

Mobile Phone Forensics Tools and Methods

The best method of retrieving information, of course, is acquiring a forensic image, which enables you to recover deleted text messages and similar data. With Android devices, the process can be as simple as using AccessData FTK Imager to perform a logical acquisition and a low-level analysis ("How Avast recovered 'erased' data from used Android phones," July 2014, http://blog.avast.com/2014/07/09/android-foreniscs-pt-2-how-we-recovered-erased-data/).

iPhone acquisition procedures are similar, and several good tools are available, such as MacLockPick 3.0 (http://macforensicslab.com/product/maclockpick/), which is designed to deal with iPhones, iPads, iOS, and Mac OS X Lion (now macOS). It can also extract iPhoto information, handle plug-in apps, and pull the user's online history.

The NIST guidelines (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf) list six types of mobile forensics methods:

- *Manual extraction*—This method involves looking at the device's content page by page and taking pictures. It's used if investigators can't do a logical or physical extraction.
- *Logical extraction*—The mobile device is connected to a forensic workstation via a wired (USB cable, for example) or wireless (such as Bluetooth) connection, and then the file system information is extracted.
- *Physical extraction*—As with a logical extraction, the mobile device is attached to a forensic workstation. However, a forensic copy is made so that deleted files can be retrieved and other items decoded.
- *Hex dumping and Joint Test Action Group (JTAG) extraction*—Hex dumping involves using a modified boot loader to access the RAM for analysis (http://digital-forensics.sans.org/blog/2008/09/03/hex-dumping-flash-from-a-mobile). The JTAG extraction method gets information from the processor, flash memory, or other physical components. It's a highly invasive method.

- *Chip-off*—This method requires physically removing flash memory chip and gathering information at the binary level.
- *Micro read*—This method looks at logic gates with an electron microscope and can be used even when data has been overwritten on magnetic media. It's very expensive, however, so it's typically used only in cases involving national security.

Paraben Software (www.paraben.com), a vendor of mobile forensics software, offers several tools, such as E3:DS, for mobile device investigations. It examines Internet of Things (IoT) devices, has a bootloader for locked mobile devices, and can perform data parsing and cloud data capture. Paraben offers different packages for a variety of uses. Another tool, DataPilot (www.datapilot.com), has a collection of cables that can interface with phones made by Nokia, Motorola, Ericsson, Samsung, Audiovox, Sanyo, and others. Susteen Inc. (http://susteen.com) also has a tool for mobile forensics analysis called Secure View 3 (http://secureview.us).

BitPim (www.bitpim.org) is a tool used to view data on many CDMA phones, including LG, Samsung, Sanyo, and others. It offers versions for Windows, Linux, and macOS. It's not a forensics tool, but it can be used in read-only mode. In Windows, BitPim stores files in Documents\BitPim by default, so when you start a new case, make sure you move these files to another location first so that they're not overwritten (www.windowsuninstaller.org/winuninstall/how-to-remove-BitPim-1-0-7-guide-BitPim-1-0-7-uninstaller-info.html).

Caution ⚠

Keep in mind that you should validate any new tool and verify its claims with rigorous testing.

Cellebrite UFED Forensic System (www.cellebrite.com) works with smartphones, PDAs, tablets, and GPS devices. This kit comes with several hundred cables, includes handset support for phones from outside the United States, and handles multiple languages. The newer version can access a smart device via a USB cable. A lesser known tool used widely by government agencies is Micro Systemation XRY (www.msab.com), which retrieves data from smartphones, GPS devices, tablets, music players, and drones.

MOBILedit Forensic (www.mobiledit.com) is a forensics software tool containing a built-in write-blocker. It can connect to phones directly via Bluetooth, irDA, or a cable and can read SIM cards by using a SIM reader. It's notable for being very user friendly.

Software tools differ in the information they display and the level of detail, and some tools are designed for updating files, not retrieving data. In general, tools designed to edit information, although they are user friendly, usually aren't forensically sound. You might be able to view some data with one of these tools that you can't view with a forensics tool, but note this step in your log and state that the tool isn't typically used for forensics purposes. Every program has its idiosyncrasies, so be aware of the shortcomings of the tools you use, and document every step you take during an investigation.

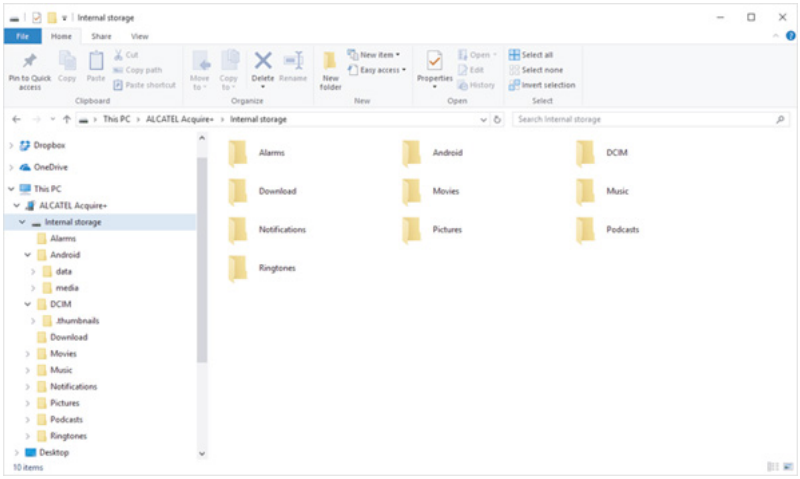
Using Mobile Forensics Tools

Now that you have a good idea of the types of tools and procedures needed for a mobile device investigation, you can learn about using some popular tools. Cellebrite (www.cellebrite.com) includes UFED Reader, a mobile forensics tool that's often used by law enforcement and the military. It also offers certifications with different training tracks. Its Universal Forensics Extraction Device (UFED) is a stand-alone portable device with software that can be loaded on a computer. This software has been tested on more than 19,000 devices. With this straightforward tool, you can determine a mobile device's make and model, learn what has to be done before connecting a mobile device to the UFED device, and then retrieve the data. You

have three options for data extraction: logical, file system, and physical. The logical extraction, however, doesn't collect FaceBook, Snapchat, or other social media files, and the physical extraction requires some reconstruction of data. In Hands-On Project 12-5, you download UFED Reader and look at some physical and logical extractions.

You can also simply connect a mobile device to a computer to browse the file system and examine and retrieve files. **Figure 12-2**, for example, shows the file system on an Android device connected by USB cable to a computer. To make an acquisition, you just need a USB write-blocker. This method isn't ideal, but you can use it to gather basic information.

Figure 12-2.



Viewing the Android file system

Note

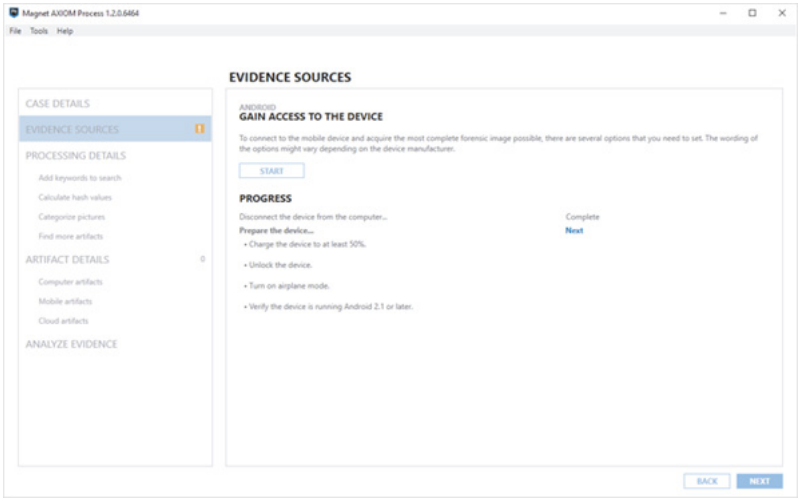
Create a *Work*\Chap12\Chapter folder on your system. The work folder path shown in screenshots might differ slightly from yours.

In this activity, you see how to use the Magnet AXIOM demo software for mobile forensics:

1. Start Magnet AXIOM Process, and click the **CREATE NEW CASE** button. In the Case number text box, type today's date followed by a hyphen and the number of the case you're working on that day, such as 02152018-1 for the first case of February 15, 2018. In the LOCATION FOR CASE FILES section, type **Chapter** in the Folder name text box. Click the **BROWSE** button next to the File path text box, navigate to and click your work folder, and click **Select Folder**. In the LOCATION FOR ACQUIRED EVIDENCE section, the folder name and file path should update automatically to be the same. If they don't, type **Chapter** for the folder name and select the path as described previously. (*Note*: For an actual case, you might want to have the acquired evidence in a separate location.) Click the **GO TO EVIDENCE SOURCES** button.
2. In the SELECT EVIDENCE SOURCE section, you can choose COMPUTER, MOBILE, or CLOUD. Click the **MOBILE** icon. In the next window, you select which type of device you're accessing: ANDROID, IOS, WINDOWS PHONE, KINDLE FIRE, or MEDIA DEVICE (MTP). In this case, click **ANDROID**. In the LOAD OR ACQUIRE window that opens automatically, click the **ACQUIRE EVIDENCE** icon, and then click **NEXT**. Finally, you specify whether the device is locked or unlocked. Click the **Unlocked** icon, and then click **NEXT**.
3. The SELECT DEVICE window displays a question mark to indicate an unknown device. Click **NEXT**.

4. In the GAIN ACCESS TO THE DEVICE window, click **START**. When prompted to disconnect the device from the computer, click **Next** in the PROGRESS list. Then you're prompted to verify that the device is charged to at least 50% and is in airplane mode, as shown in Figure 12-3.

Figure 12-3.

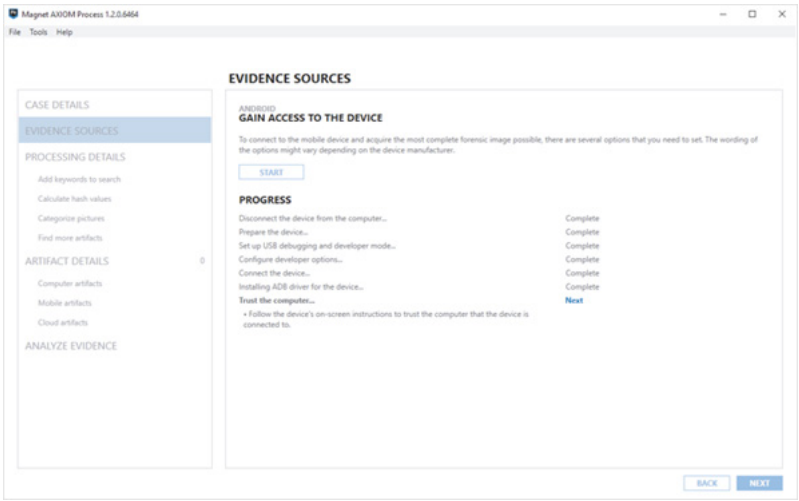


Source: Magnet Forensics, www.magnetforensics.com

Preliminary steps in accessing a mobile device

5. The program continues to prompt you through the remaining steps, such as setting up USB debugging and configuring developer options (see **Figure 12-4**). After it detects the device, as shown in Figure 12-5, click **NEXT**. Magnet AXIOM loads an agent (software) into RAM and starts accessing the mobile device.

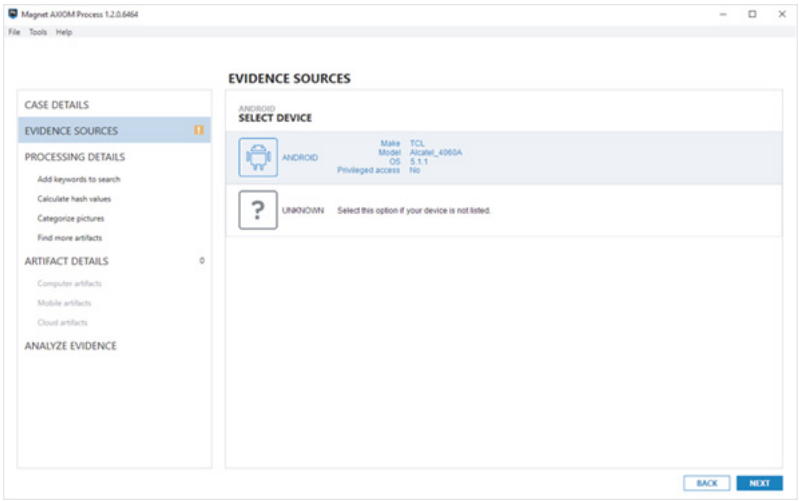
Figure 12-4.



Source: Magnet Forensics, www.magnetforensics.com

Additional steps in accessing a mobile device

Figure 12-5.



Source: Magnet Forensics, www.magnetforensics.com

The identified device

6. After Magnet AXIOM gains access to the device, you see a notification that the device is restarting, and you need to acknowledge access by the computer. If it gains privileged access, a physical acquisition is made; if not, a basic acquisition is made. After the acquisition is finished, Magnet AXIOM Examine starts. Exit the program after you're verified that the acquisition data is in the location you specified in **Step 1** for acquired evidence.

Many mobile forensics tools are available, but most aren't free. As the mobile forensics market continues to expand and mature, the methods and techniques for acquiring evidence will change. Subscribe to user groups and professional organizations to stay abreast of what's happening in the industry.

Understanding Forensics in the Internet of Anything

In 2010, both VMware and BlackBerry were thinking of developing type 2 hypervisors for mobile devices. They would be useful for security and protecting personal information but would add another layer of complexity to forensics investigations. In private-sector investigations, for example, you must take care to separate personal information from business-related data, and knowledge of privacy laws is especially crucial in this task. In the ensuing years, the idea of type 2 hypervisors for mobile devices has dropped by the wayside, but the issue of private or confidential data being on personal mobile devices still exists. Moreover, because bring your own device (BYOD) has become a business standard, investigators must consider how to keep employees' personal data separate from case evidence.

The Internet of Things (IoT) brings additional challenges to the field of mobile forensics. The number of devices connecting to the Internet is higher than the number of people, and this number is expected to reach 50 billion in the next few decades (www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/). Although jokes about "The fridge did it" are rampant, the concerns are real.

From a mobile device, you can turn on lights in your home, lock or unlock doors, adjust the thermostat, and more, and all these appliances and devices can be interconnected. LG offers a refrigerator that can order groceries for you, and it's connected to an established payment method, such as a digital wallet. So in an investigation, determining who actually ordered food

and unlocked the door when the delivery was made could be difficult. In the very near future, investigators will face these challenges and more.

As mentioned previously, the world has gone from the Internet of Things (IoT) to the Internet of Everything (IoE) to the Internet of Anything (IoA). The IoT includes the ever-growing number of physical devices connected on the Internet. The article "Smart Forensics in the Internet of Things (IoT)" explains that the IoT covers not only wired, wireless, and mobile devices but also radio frequency identification (RFID) sensors (https://securityintelligence.com/smart-forensics-for-the-internet-of-things-iot/). The IoE adds features that aren't tangible but are widespread on the Internet, such as the Google search engine and YouTube. The IoA includes cars, homes, pets, livestock, and applications for making all these things work together. The IoA makes people's lives more convenient, but this interconnectivity complicates tracking evidence.

In addition, the IoA will eventually include 5G smart devices, and 5G mobile networks are gaining momentum. In February 2017, the ITU began the final requirements for 5G networks with the International Mobile Telecommunications (IMT) working group, which is producing the document IMT-2020 (www.itu.int/en/mediacentre/Pages/2017-PR04.aspx). IMT-2020 will set the standards for 5G devices, which include smart homes, smart cars, smart cities, and more. Currently, the ITU has divided 5G into three categories:

- *enhanced Mobile BroadBand (eMBB)*—Provides more bandwidth to increase digital connectivity for users
- *Ultra-reliable and Low-latency Communications (uRLLC)*—Focuses on devices such as self-driving cars
- *massive Machine Type Communications (mMTC)*—Focuses on smart cities

These 5G devices introduce new challenges for digital forensics. Investigators will be dealing with people-to-device communications (P2D), device-to-device (D2D) communications, and device-to-cloud (D2C) communications. This variety of communication types complicates where they look for evidence. A recent demonstration on a news program showed a penetration tester breaking into a home's wireless network via the television, and then starting the smart coffeemaker and turning off the owner's laptop. If he had actually committed a crime, where would an investigator start to determine how he had gained access to the home's network?

You can now turn on a burglar alarm in your home, turn on the lights, start the coffeemaker, and even start your car from your mobile device, whether it's a smart phone or tablet. Smart refrigerators can order groceries for you and have them delivered and waiting in a cold storage box on your doorstep while you're at work. In addition, smart cities are becoming more of a reality, with traffic lights controlled to keep traffic moving or stop traffic for emergency vehicles. The iOS watch can tell you that you've been sitting too long and need to take a walk or that your heartrate is too high and you need to do some deep breathing to calm down. This information can be synchronized with your smartphone and stored in the cloud. All these new developments expand the task of collecting evidence for investigations.

Note

In their paper "Digital Evidence Challenges in the Internet of Things," Hegarty, Lamb, and Attwood emphasize that not all devices are created equal (Proceedings of the Ninth International Workshop on Digital Forensics and Incident Analysis, www.researchgate.net/publication/288660566_Digital_evidence_challenges_in_the_internet_of_things, 2014). Data from some devices might be reliable, but from other devices, it might not be. Also, the storage capacity on small devices might be limited, so data could be overwritten quickly.

Gaming consoles such as the Sony PlayStation and Xbox are other devices that can contain information hackers might try to intercept and collect, and information on how to retrieve this information is readily available on the Internet. Because of the graphics-heavy software these consoles run, many are more powerful than standard desktop or laptop computers and, therefore, might be a target of attacks.

Research on wearable computers has been conducted at MIT labs for more than a decade, and these computers are now moving into working reality. For example, workers in warehouses can wear rings to scan inventory, and Google Glass is available to access the Internet or take pictures while walking, for example. As mentioned, the iOS Watch and other smartwatches are becoming popular. However, the iOS Watch synchronizes to a smartphone via a magnetic device. There's no other way to get information from the watch, so this feature is one investigators must learn how to handle. In addition, IBM created a unique mobile phone as jewelry. Earrings are the speakers, a necklace is the microphone, a ring notifies you of incoming calls, and a bracelet identifies the caller (*http://electronics.howstuffworks.com/gadgets/home/digital-jewelry1.htm*). Collecting information from wearable computers poses many new challenges for investigators.

A new field is vehicle system forensics, which addresses the many parts that have sensors in cars. For example, your car can sense when another car is approaching perpendicular to your car as you back out or when your windshield wipers need to go faster. Many device-to-device sensors make decisions without the driver needing to do anything. A few years ago at an event sponsored by a car manufacturer, a 14-year-old with $20 of equipment purchased at RadioShack was able to hack into a car. As more devices are added to the Internet of Anything, investigations will become more complex. Many times, devices aren't designed with investigations or security in mind, so investigators will have to conduct research to find out how and where to access data on IoA devices and sensors, which can slow down or complicate the process of getting warrants to collect data.

Chapter Summary

- People store a wealth of information on smartphones, including calls, text messages, picture and music files, address books, and more. These files can give you a lot of information when investigating cases.
- Mobile devices have gone through four generations: analog, digital personal communications service (PCS), third-generation (3G), and fourth-generation (4G). Two major digital networks currently used in the United States are Code Division Multiple Access (CDMA) and Global System for Mobile Communications (GSM).
- 4G technology is the current generation of mobile phones. It has faster data transfer rates than previous generations.
- 5G standards are being negotiated and developed by the IMT 2020 working group of the International Telecommunications Union. They are in three categories: enhanced Mobile BroadBand (eMBB), Ultra-reliable and Low-latency Communications (uRLLC), and massive Machine Type Communications (mMTC).
- Mobile devices range from basic, inexpensive phones used primarily for phone calls to smartphones that integrate a phone, PDA, camera, music player, and more into one device.
- Data can be retrieved from several different places in phones, including volatile memory, nonvolatile memory, and Secure Digital, MultiMediaCard, and Compact Flash cards.
- The use of personal digital assistants (PDAs) has declined because smartphones incorporated all their features and added more. They're still used for specialized applications, such as medical and industrial PDAs.
- As you do with computers, you must follow correct search and seizure procedures for mobile devices. In particular, investigators must take care to ensure that mobile devices remain connected to a power source so that they don't lose data in volatile memory. Also, suspect devices should be disconnected from PCs as soon as possible to prevent any synchronization that might overwrite data on the device.
- To isolate a mobile device from incoming messages, you can put it in airplane mode, turn the device off, or place it in a specially treated paint can or evidence bag.
- SIM cards store data in a hierarchical file structure containing a system root, which holds directory files that store elementary data.
- Mobile device forensics is becoming more important as these devices grow in popularity. Accessing backup files from the cloud or SIM cards is the easiest way to retrieve information from these devices, but acquiring an image is more accurate and produces more detailed data.
- Many software tools are available for reading data stored in mobile devices. Typically, these devices connect to the phone wirelessly (through Bluetooth or irDA) or with a cable. Some also read SIM cards by using a SIM card reader, which is a combination hardware/software device.
- The Internet of Things (IoT) has resulted in yet another challenge for digital forensics investigators. The number of devices that connect to the Internet is expected to reach 50 billion in the next few decades. Because mobile devices and appliances are so interconnected, determining a timeline or who actually performed an action can be difficult. In addition, collecting information from wearable computers will pose many new challenges for investigators.

Key Terms

Code Division Multiple Access (CDMA)
electronically erasable programmable read-only memory (EEPROM)
Enhanced Data GSM Environment (EDGE)
fifth-generation (5G)
fourth-generation (4G)
Global System for Mobile Communications (GSM)
International Telecommunication Union (ITU)
Orthogonal Frequency Division Multiplexing (OFDM)
smartphones
subscriber identity module (SIM) cards
Telecommunications Industry Association (TIA)
third-generation (3G)
Time Division Multiple Access (TDMA)

Review Questions

1. List four places where mobile device information might be stored.

2. Typically, you need a search warrant to retrieve information from a service provider. True or False?

3. The term TDMA refers to which of the following? (Choose all that apply.)
   a. A technique of dividing a radio frequency so that multiple users share the same channel
   b. A proprietary protocol developed by Motorola
   c. A specific cellular network standard
   d. A technique of spreading the signal across many channels

4. What's the most commonly used cellular network worldwide?

5. Which of the following relies on a central database that tracks account data, location data, and subscriber information?
   a. BTS
   b. MSC
   c. BSC
   d. None of the above

6. GSM divides a mobile station into ___ and ___ .

7. SD cards have a capacity up to which of the following?
   a. 100 MB
   b. 4 MB
   c. 64 GB
   d. 500 MB

8. Describe two ways you can isolate a mobile device from incoming signals.

9. Which of the following categories of information is stored on a SIM card? (Choose all that apply.)
   a. Volatile memory

b. Call data

c. Service-related data

d. None of the above

10. Most SIM cards allow ___ access attempts before locking you out.

11. SIM card readers can alter evidence by showing that a message has been read when you view it. True or False?

12. The uRLLC 5G category focuses on communications in smart cities. True or False?

13. When acquiring a mobile device at an investigation scene, you should leave it connected to a laptop or tablet so that you can observe synchronization as it takes place. True or False?

14. Remote wiping of a mobile device can result in which of the following? (Choose all that apply.)

a. Removing account information

b. Enabling a GPS beacon to track the thief

c. Returning the phone to the original factory settings

d. Deleting contacts

15. In which of the following cases did the U.S. Supreme Court require using a search warrant to examine the contents of mobile devices?

a. *Miles v. North Dakota*

b. *Smith v. Oregon*

c. *Riley v. California*

d. *Dearborn v. Ohio*

16. The Internet of Things includes ___ as well as wired, wireless, and mobile devices.

17. Which of the following is a mobile forensics method listed in NIST guidelines? (Choose all that apply.)

a. Logical extraction

b. Bilateral read

c. Physical extraction

d. Hex dumping

18. According to SANS DFIR Forensics, which of the following tasks should you perform if a mobile device is on and unlocked? (Choose all that apply.)

a. Isolate the device from the network.

b. Disable the screen lock.

c. Remove the passcode.

d. Attempt to do a physical acquisition.

19. Which organization is setting standards for 5G devices?

Hands-On Projects

Create a *Work*\Chap12\Projects folder on your system before starting these projects; it's referred to as your "work folder" in steps. If necessary, copy all data files from the downloads section for this chapter (on the student companion site for this book) to your work folder.

Hands-On Project 12-1

In this project, you're using Magnet AXIOM to examine the image of Jim Shu's cell phone. (Assume someone else did the acquisition.)

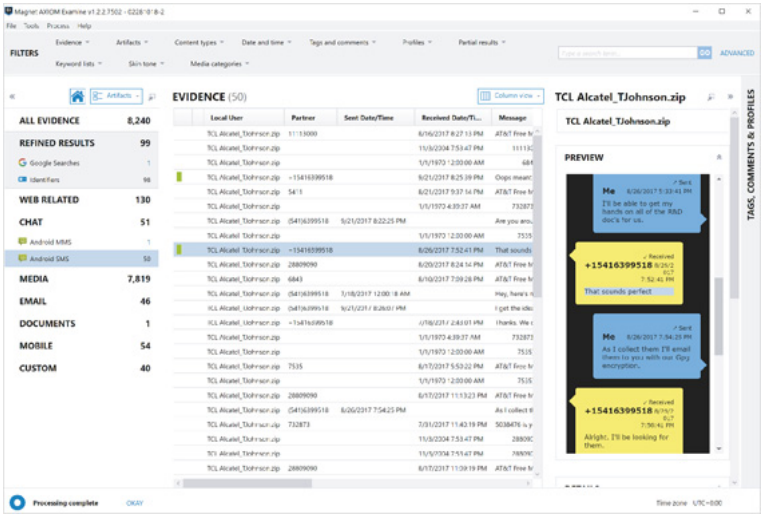
1. Start Magnet AXIOM Process, and click the **CREATE NEW CASE** button. In the Case number text box, type today's date followed by a hyphen and the number of the case you're working on that day. In both the LOCATION FOR CASE FILES and LOCATION FOR ACQUIRED EVIDENCE sections, type **Jim_Shu** in the Folder name text box. In both sections, click the **BROWSE** button next to the File path text box, navigate to and click your work folder, and click **Select Folder**. Click the **GO TO EVIDENCE SOURCES** button.
2. In the SELECT EVIDENCE SOURCE section, click the **MOBILE** icon. In the next window, click **ANDROID** to specify the type of device you're accessing, and then click **NEXT**. In the next window, click the **LOAD EVIDENCE** icon, and then click **IMAGE**. Browse to and click the TCL Alcatel_JShu.zip file, and then click **Open**. In the EVIDENCE SOURCES window, click **NEXT**.
3. Click **GO TO PROCESSING DETAILS**. In the following windows, click **GO TO ARTIFACT DETAILS, GO TO ANALYZE EVIDENCE**, and then **ANALYZE EVIDENCE** to start Magnet AXIOM Examine.
4. Click **REFINED RESULTS** in the left pane to see the recovered items. Notice that you can also examine evidence in the categories CHAT, EMAIL, WEB RELATED, and MOBILE. Examine the evidence in these categories to see who Jim Shu was in contact with.
5. Write a one- to two-page report summarizing your findings, and exit Magnet AXIOM Examine.

Hands-On Project 12-2

In this project, you use Magnet AXIOM to examine the image of Tom Johnson's cell phone. (Assume someone else did the acquisition.)

1. Start Magnet AXIOM Process, and click the **CREATE NEW CASE** button. In the Case number text box, type today's date followed by a hyphen and the number of the case you're working on that day. In both the LOCATION FOR CASE FILES and LOCATION FOR ACQUIRED EVIDENCE sections, type **Tom_Johnson** in the Folder name text box. In both sections, click the **BROWSE** button next to the File path text box, navigate to and click your work folder, and click **Select Folder**. Click the **GO TO EVIDENCE SOURCES** button.
2. In the SELECT EVIDENCE SOURCE section, click the **MOBILE** icon. In the next window, click **ANDROID** to specify the type of device you're accessing, and then click **NEXT**. In the next window, click the **LOAD EVIDENCE** icon, and then click **IMAGE**. Browse to and click the TCL Alcatel_TJohnson.zip file, and then click **Open**. In the EVIDENCE SOURCES window, click **NEXT**.
3. Click **GO TO PROCESSING DETAILS**. In the following windows, click **GO TO ARTIFACT DETAILS, GO TO ANALYZE EVIDENCE**, and then **ANALYZE EVIDENCE** to start Magnet AXIOM Examine. When you see a message that the processing is complete, click **OK**.
4. Click **REFINED RESULTS** to see the recovered items. Notice that you can examine evidence in the categories CHAT, EMAIL, WEB RELATED, and MOBILE.
5. Click to expand **CHAT**, and then click **Android MMS** and **Android SMS** to examine these chat messages (see Figure 12-6).

Figure 12-6.



Source: Magnet Forensics, www.magnetforensics.com

Reviewing chat messages on Tom Johnson's smartphone

6. Leave Magnet AXIOM Examine running for the next project. Write a one- to two-page report summarizing your findings.

Hands-On Project 12-3

This project requires completing Hands-On Project 12-2. In an actual case in which several hard drives or mobile devices have been seized as evidence, you would add devices to the case in Magnet AXIOM Process (or a similar function in other tools).

1. Start Magnet AXIOM Examine, if necessary, and open the Tom Johnson case. In the EVIDENCE pane in the middle, there's a drop-down list in the upper-right corner showing that the program is in Row view; click the list arrow and examine other views, such as Classic, Histogram, and Timeline.

2. Return to Row view. Notice the word "FILTERS" in the upper-left corner under the File menu and review the types of filters available, such as Evidence, Artifacts, Date, Time, Keyword Lists, and Skin Tone. Click the **Date** list arrow, and in the calendar window that opens, set the START DATE to **1 August 2017** and the END DATE to **30 September 2017**. The Filter area changes to yellow to let you know you're using a filter. Examine the visible information and take screenshots.

3. Close Tom Johnson's file, and open Jim Shu's case. Apply the same date range.

4. Compare the e-mails and chats in both cases. What can you conclude from this information?

5. Write a two- to three-page paper describing your findings and any conclusions you drew. Include your screenshots from **Step 2**. When you're finished, exit Magnet AXIOM.

Hands-On Project 12-4

In this project, you download Santoku Linux to create an Android virtual device and then gather data from it. This useful tool gives you a way to experiment with a variety of practice mobile devices.

1. Start a Web browser, go to http://santoku-linux.com/download/, and download the ISO file for Santoku Linux.

2.

Start VirtualBox, and create a virtual machine with at least 4 GB RAM and 30 GB of hard drive storage. Start Santoku Linux, and click the **Install Santoku 14.04** icon. When prompted, restart the VM.

3. When the installation is finished, click **Device, Insert Guest Additions CD Image** from the menu. When prompted to open the image in File Manager, click **OK**. Click **Start, Accessories, LXTerminal** to open a command prompt window. Type cd/media/username/VBOXADDITIONS_5.1.22_115126 and press **Enter**, and then type sudo sh ./VBoxLinuxAdditions.run and press Enter. You can then use scaled mode for window sizing to make viewing easier. Click **View, Scaled Mode** from the menu.

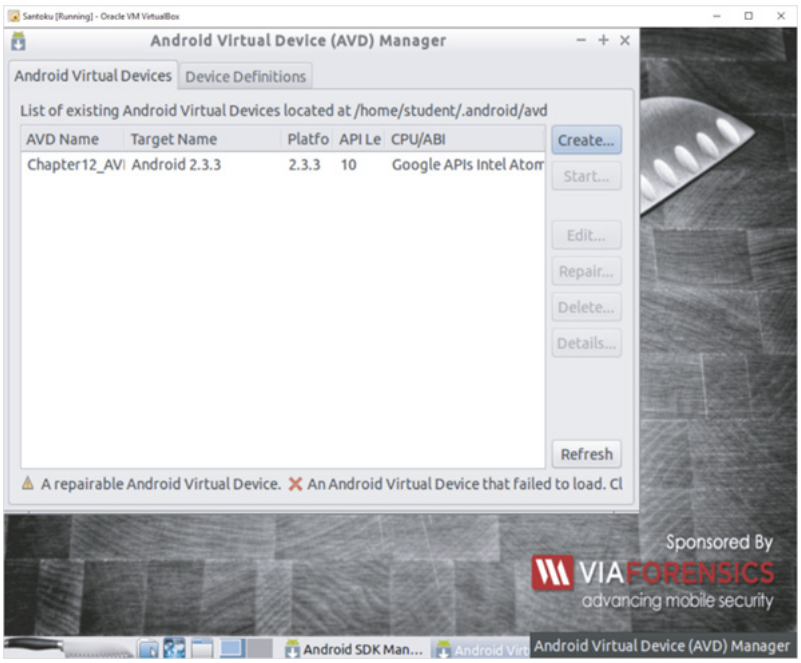
4. Next, you need to create an Android 2.3.3 virtual device (AVD) for making a forensic extraction. Click **Start, Santoku, Development Tools, SDK Manager**. Santoku downloads the development tools, which might take a few minutes.

5. In the window that opens, select all the bulleted items under Tools, and then scroll to Android 2.3.3 and select all the bulleted items for Android 2.3.3. At the lower right, click the **Install 17 packages** button. In the next window, click the **Accept License** option button and then the **Install** button. Click **OK**. Close SDK Manager and reopen it.

6. Click **Tools, Manage AVDs**from the menu, and then click the **Create** button at the upper right. For the name, type **Chapter12_AVD**, and for the device type, click **Nexus One**. Click the **CPU/ABI** list arrow, and click **Google APIs ARM**. For the skin type, click **WVGA 800**. Enter **100 GB** for the size of the SD card, and then click **OK**.

7. The next window shows the details of the new AVD. Click **OK** to open the window shown in Figure 12-7.

Figure 12-7.



Source: Santoku Linux, https://santoku-linux.com

Creating an AVD in Santoku Linux

8. Click to select the **Chapter12_AVD** virtual device, and then click the **Start** button. In the window that opens, click **Launch**. (*Note*: This window might take a few minutes to open.)

9. APK files contain source data for Android applications, To install one for collecting data from your AVD, go to https://github.com/nowsecure/android-forensics/downloads

and download the APLogical-OSE software to the VM.

10. In the VM's command prompt window, type adb install ~/Desktop/AFlogical-OSE_1.5.2.apkand press **Enter**. When you see the "Success" message, you know the APK was able to retrieve data from the Android virtual device.

11. Close the AVD and any other open windows, and exit Santoku.

Hands-On Project 12-5

In this project, you download UFED Reader from Cellebrite and compare a logical acquisition with a physical acquisition. The Web site you go to in **Step 1** contains logical and physical acquisitions performed by NIST to help you learn how to read these files.

1. Start a Web browser, go to www.cfreds.nist.gov, and scroll to the table at the bottom of the page. Click **Mobile Device Images**, and on the next page, click the **Cellebrite UFED** link.

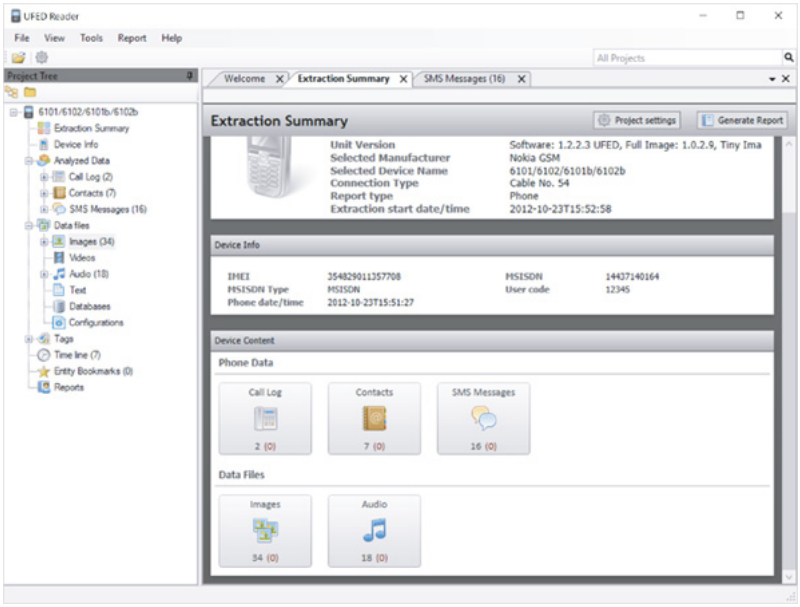
Note

UFED Reader can read the .ufdr files on this Web site, so although you're not doing the acquisitions, you can open the files created by actual acquisitions. As mentioned previously, many commercial tools have created readers so that other stakeholders in a case, such as lawyers, don't need to have a licensed version of the forensic tool to be able to examine the evidence.

2. Download the UFED Reader 3.2.exe file. In the table on the first page, find the entry with Nokia in the first column and Logical Acquisition in the second column. In the third column, click the **ufdr** link, and download Nokia-logical.ufdr. Go back to the table, find the entry with Nokia in the first column and Physical Acquisition in the second column. In the third column, click the **ufdr** link, and download Nokia-physical.ufdr.

3. Start UFED Reader. Click **File, Open** from the menu, and click Nokia-logical.ufdr (a logical acquisition). It should open to the Extraction Summary tab shown in Figure 12-8. On the left you can see the file structure, and on the right you can see the type of phone, SMS messages, contacts, the call log, and so forth. Examine the information acquired from the phone, and take screenshots of this information. When you're finished, click **File, Close** from the menu.

Figure 12-8.



Source: Cellebrite Mobile Synchronization LTD., www.cellebrite.com

Using UFED Reader

4. Next, open the Nokia-physical.ufdr file (a physical acquisition). Examine the information acquired from the phone, and take screenshots of this information.

5. Exit your Web browser and UFED Reader. Write a one- to two-page paper describing the differences between the logical and physical acquisitions you examined.

Case Projects

Case Project 12-1

Download the most current version of the NIST Mobile Device Forensics Guidelines at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf. Page 17 lists classifications of mobile device tools. For the tools covered in this chapter, determine what type each one is based on these NIST guidelines. Write a one- to two-page paper explaining the uses and limitations of each tool.

Case Project 12-2

For this project, you need access to a mobile forensics toolkit. Select a cell phone model for which you have no cable. After doing Internet research for possible options, write a plan for approaching the problem. Remember that you don't want to destroy data, so make sure you include a step to test the equipment before using it.

Chapter 13. Cloud Forensics

After reading this chapter and completing the exercises, you will be able to:

- Describe the main concepts of cloud computing
- Summarize the legal challenges in conducting cloud forensics
- Give an overview of the technical challenges with cloud forensics
- Describe how to acquire cloud data
- Explain how to conduct a cloud investigation
- Explain what remote access tools can be used for cloud investigations

This chapter explains how to apply forensics skills and techniques to a cloud environment. First, you get an overview of cloud computing so that you understand how clouds are configured and how they operate. Next, you review some of the legal and technical challenges in conducting cloud forensics and get an overview of some related issues with acquisitions and encryption.

This chapter also gives you guidance on creating a plan for conducting a cloud investigation and describes how to gather evidence from cloud service providers and customers. Because of rapid changes in cloud storage models and methods, you need to continue researching changes in cloud computing and how to apply digital forensics techniques to the cloud.

An Overview of Cloud Computing

The cloud has introduced ways of managing data that didn't exist a decade ago, such as companies migrating e-mail services to the cloud for employees anywhere in the world to access or smartphones syncing and backing up to the cloud. For these reasons, cloud investigations have some unique challenges. This section gives you background on cloud computing, including a brief history, cloud service levels and deployment methods, cloud vendors, and basic concepts of cloud forensics. You also learn about new standards being developed to improve security practices and incident responses in cloud environments.

History of the Cloud

The idea of cloud computing came from several people. Professor John McCarthy of MIT and Dr. J. C. R. Licklider, director at the U.S. Department of Defense Advanced Research Projects Agency (ARPA), are generally given credit for developing the concept (www.computerweekly.com/feature/A-history-of-cloud-computing). In 1961, McCarthy proposed selling computing resources (such as data processing) and software as a service through a public utility, similar to how water, sewer, and electrical power are made available to the public. This idea was based on hosting services and software on a mainframe computer. In an April 25, 1963, memo, "Members and Affiliates of the Intergalactic Computer Network," Dr. Licklider proposed interconnecting programs and data to share resources. In 1968, the ARPA Program Plan No. 723, Resource Sharing Computer Networks, was initiated to engineer a solution of sharing networked resources. It then developed into the Advanced Research Projects Agency Network (ARPANET), which later became the Internet (www.darpa.mil/about-us/timeline/modern-internet).

In 1999, Salesforce.com developed a customer relationship management (CRM) Web service that applied digital marketing research to business subscribers so that they could do their own market analysis; this service eventually led the way to the cloud. Amazon created Amazon Mechanical Turk in 2002, which provided storage, computations, and human intelligence, and then started its Elastic Compute Cloud (EC2) in 2006, a Web service aimed at supporting small businesses. It enabled people and small businesses to rent processing time to run their own applications from a centralized source. After Web 2.0 in 2009, other providers started their own cloud services, such as Google Apps, Apple iCloud, Microsoft OneDrive, and more.

Cloud Service Levels and Deployment Methods

The National Institute of Standards and Technology defines cloud computing in its NIST Special Publication 800-145 document "The NIST Definition of Cloud Computing" (http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, 2011) as a computing storage system that provides on-demand network access for multiple users and can allocate storage to users to keep up with changes in their needs. The cloud has three basic service levels:

- *SaaS*— **Software as a service (SaaS)** means applications are delivered via the Internet. A familiar one is Google Docs, which is similar to office suites such as Microsoft Office or LibreOffice. Data is stored in the cloud, and files can be accessed and shared with others.
- *PaaS*— **Platform as a service (PaaS)** means an OS has been installed on a cloud server. Users can then install their own applications, settings, and tools in the cloud environment. The cloud provider maintains just the hardware for customers, who are responsible for their own system administration and application support.
- *IaaS*— **Infrastructure as a service (IaaS)** means customers can rent hardware, such as servers and workstations, and install whatever OSs and applications they need. IaaS can come in handy when customers can't afford to purchase hardware or pay someone to maintain it but can afford to rent. In addition, this service level makes it easy to add hardware during peak business periods, such as tax season or end-of-year accounting, and then cut back on hardware when it's not needed during slow periods.

Note

NIST document 800-145 has only the three types of cloud services described in the preceding list. However, in June 2017, NIST document SP 500-322 was released for public comment and includes more than 75 services, such as backup as a service, security as a service, and Drupal as a service. The final document should be approved and released in the near future.

Table 13-1 describes where investigators find evidence of cloud access, depending on the type of cloud service level.

Table 13-1. Locations of evidence in different service levels

Service level	Locations of evidence
SaaS	Most likely stored on a desktop, laptop, tablet, or smartphone.
PaaS	Most likely found on a desktop or server, although it could also be stored on a company network or the remote service provider's infrastructure.
IaaS	Usually found on a desktop or server; infrastructure equipment can be owned by the company or the remote service provider.

For investigators, the location of evidence affects what you can get access to and what laws regulate your actions. If, for example, you're conducting a private-sector investigation and policies and procedures are in place, you can do a static acquisition of the device that accessed cloud data and a remote acquisition of files on the cloud server. If the organization has its own cloud server, the acquisition might be even more straightforward, particularly if the cloud server has built-in forensics and e-discovery tools. These tools speed up an investigation and reduce its costs. Having a forensics team or an incident response team with a digital forensics component in place is also important.

The deployment methods for a cloud are public, private, community, and hybrid. A **public cloud** is accessible to anyone, and typically, the only identification required is an e-mail address. This deployment method offers no security, but it's popular because of its ease of use. Next is a **private cloud** , which can be accessed only by people who have the necessary

credentials, such as logon names and passwords; sometimes location is used as a way to restrict access, too. Most companies have private clouds. A **community cloud** is a way to bring people together for a specific purpose. For example, say a city wants all small businesses to have access to the same documents and templates. By creating a community cloud, the city can make these files accessible to those who have a current business license. A **hybrid cloud** enables a company to keep some information private and designate other files as public or community information.

Cloud Vendors

Many **cloud service providers (CSPs)** and products are available. CSPs use a variety of approaches and systems to build their cloud systems, such as servers using distributive processing methods with data farms for storage or mainframes running OSs as virtual machines. The following are some CSPs and cloud applications:

- *Salesforce* (www.salesforce.com)—Offers a variety of cloud services, including automation and CRM, cloud application development, and Web site marketing
- *IBM Cloud* (www.ibm.com/cloud-computing/us/en/)—Provides cloud development and mobile applications for several platforms
- *Cisco Cloud Computing* (www.cisco.com/web/solutions/trends/cloud/index.html)—Has cloud applications for a wide assortment of businesses, ranging from enterprise and midsize businesses to resellers of cloud services
- *Amazon EC2* (http://aws.amazon.com/ec2/)—Offers a Web service run from the cloud that allows scalability
- *AT&T Synaptic* (www.synaptic.att.com/clouduser/)—Provides on-site data storage and the capability of a hybrid cloud system
- *Google Cloud Storage* (https://cloud.google.com/products/cloud-storage/)—Offers virtual machines with tools for analyzing large data sets
- *HP Helion* (www8.hp.com/us/en/cloud/helion-overview.html)—Provides a hybrid cloud environment with a wide range of products that can integrate into a business's storage needs
- *Microsoft Azure* (http://azure.microsoft.com/en-us/documentation/services/storage/)—Offers tiered support for large organizations, including file, disk, blob, and archive.
- *XenServer and XenCenter Windows Management Console* (http://xenserver.org/overview-xenserver-open-source-virtualization/download.html)—Has a freeware type 1 hypervisor used for public and private clouds (commercial support provided by Citrix Systems, Inc.)
- *Atlantic.Net* (www.atlantic.net)—Provides HIPAA-compliant storage and colocation, hybrid, and private hosting
- *Digital Ocean* (www.digitalocean.com)—Offers cloud storage for developers and businesses as well as support for deploying Hadoop and other cloud-based services
- *Rackspace* (www.rackspace.com/cloud)—Provides private, hybrid, and multi-cloud solutions along with management options
- *Oracle Cloud* (https://cloud.oracle.com/home)—Offers a variety of cloud platforms and more than 4000 vendor applications that integrate into its systems

Basic Concepts of Cloud Forensics

Cloud forensics procedures are needed in many situations, such as cyber criminals attacking a cloud, policy violations in accessing a cloud, data recovery, reports of suspicious activity, fraud,

and data breaches (Stephen Coty, AlertLogic, Inc., RSAConference, www.rsaconference.com/writable/presentations/file_upload/anf-t07a-computer-forensics-and-incident-response-in-the-cloud.pdf, 2014). Cloud forensics can be defined as simply as applying digital forensics to cloud computing and is considered a subset of network forensics (Keyun Ruan et al, "Cloud forensics: An overview," www.researchgate.net/publication/229021339_Cloud_forensics_An_overview, 2011). This article describes cloud forensics as having three dimensions: organizational, legal, and technical. The organizational dimension addresses the structure of the cloud, such as location of data storage and administration of services. The legal dimension covers service agreements and other jurisdictional matters because a cloud's data storage can be located anywhere in the world and even cross nations' boundaries. The technical dimension deals with procedures and specialized applications designed to perform forensics recovery and analysis in the cloud. The following are capabilities forensics tools should have to handle acquiring data from a cloud:

- *Forensic data collection*—Tools must be able to identify, label, record, and acquire data from the cloud.
- *Elastic, static, and live forensics*—To meet the elastic nature of clouds, tools must be able to expand and contract their data storage capabilities as the demand for services changes.
- *Evidence segregation*—Clouds are set up for **multitenancy** , meaning many different unrelated businesses and users share the same applications and storage space, so forensics tools must be able to separate each customer's data.
- *Investigations in virtualized environments*—Because cloud operations typically run in a virtual environment, forensics tools should have the capability to examine virtual systems.

Although most cloud architecture is composed of virtual machines, the actual cloud is much more complex. The failover capability is necessary in case a VM fails, and there are virtualized switches and routers along with multi-tenant and multi-cloud environments. Becoming proficient as a cloud manager on platforms such as vSphere takes a few years of experience maintaining these systems.

Legal Challenges in Cloud Forensics

Because cloud computing is a rapidly changing technology, laws haven't kept up with the implications of storing files and data in locations that aren't physically within reach. For this reason, when you're investigating a cloud system, you need to consider many factors involving a CSP's relationship with cloud users. This section explains a CSP's contract obligations with cloud users and how warrants and subpoenas are applied to CSPs and users. Understanding these legal issues can help you prepare for an investigation more effectively.

Service Level Agreements

Organizations that sell cloud services have **cloud service agreements (CSAs)** with their customers, which are also called "master service agreements" or "service level agreements (SLAs)." A CSA is a contract between a CSP and the customer that describes what services are being provided and at what level. It should also specify support options, penalties for services not provided, system performance (periods of downtime and uptime, for example), fees, provided software or hardware, and so forth. The Cloud Standards Customer Council has published guidelines to help customers understand their rights and responsibilities in Practical Guide to Cloud Service Agreements (www.cloud-council.org/deliverables/CSCC-(Practical-Guide-to-Cloud-Service-Agreements.pdf). It's important that CSAs define in detail the scope of services the CSP provides and what responsibilities are expected of the customer, including the following:

- Service hours

- Restrictions applied to the customer by the CSP
- Availability of the cloud to the customer
- Levels of support for the customer
- Response time for data transfers
- Throughput limitations
- Contingency plan for incident response
- Business continuity and disaster recovery plan
- Fees for the subscription to the cloud and fees for additional services as they occur
- Security measures
- Terminology of the cloud's systems and applications

Digital forensics examiners should be most concerned with restrictions applied to customers and security measures. These CSP components must state who is authorized to access data and what the limitations are in conducting acquisitions for an investigation. Because many cloud vendors spread data storage systems across multiple countries, the CSP should also address any multi-jurisdiction concerns and define how conflicts between laws of different countries will be resolved.

Caution

Even if a contract delineates access to data and processes for acquiring it, a country's laws might expand, limit, or even reject the rights specified in the contract's terms.

Policies, Standards, and Guidelines for CSPs

CSPs have policies, standards, and guidelines for their daily operations, and digital forensics investigators should review them carefully when preparing a cloud investigation plan. This section summarizes recommendations for these policies, standards, and guidelines from the SANS organization (www.sans.org/security-resources/policies/#name and www.sans.org/security-resources/policies/computer.php).

Policies are detailed rules for a CSP's internal operation and typically include personnel responsibilities, management structure, delegation authority, contracting authority, expectations of protecting data, and the authorization to distribute information. Standards give guidance to staff for unique operations, hardware, and software and describe their obligations in daily operations and security of the CSP's environment. Although guidelines aren't required, they describe best practices for cloud processes and give staff an example of what they should strive to achieve in their work.

Tip

For more information on policy, standards, and guidelines, see www.itmanagerdaily.com/cloud-computing-policy-template/ and https://cloudsecurityalliance.org.

CSP Processes and Procedures

Processes and procedures are detailed documents that define workflow and step-by-step instructions for CSP staff. They often include hardware configuration diagrams, network maps, and application processing flowcharts. Digital forensics examiners can use these documents to understand how data is stored, manipulated, secured, backed up, restored, and accessed by CSP staff and customers.

Additional documents of interest are the CSP's business continuity and disaster recovery plans, which can be helpful in recovering and analyzing data you need for your investigation. These documents are particularly useful if you have large quantities of data to collect and examine without adequate storage. If the CSP has a backup site designated in its business continuity plan, you might be able to use it for storing digital evidence you've collected and analyzing extremely large data sets.

Jurisdiction Issues

Although there are plans to revise current laws, many cross-jurisdiction legal issues haven't been resolved. No law ensures uniform access or required handling procedures for the cloud, so cases that encompass multiple jurisdictions as well as the cloud's multitenancy nature are concerns for any investigation. In addition, investigators should be concerned about cases involving data commingled with other customers' data that's unrelated to the investigation. In his white paper "Legal Issues of Cloud Forensics" (https://d12vzecr6ihe4p.cloudfront.net/media/965983/wp-legal-issues-of-cloud-forensics.pdf, 2013), attorney David White explores the issue from a legal perspective and concludes that cloud customers need to be prepared for an incident and know what's in their CSAs. If government regulations and agreements haven't been developed in other countries, investigators might be limited in what they can do to process a case. In their paper "Cloud Forensics Issues and Opportunities" (www.researchgate.net/publication/276010807_Cloud_Forensics_Issues_and_Opportunities, 2013), Aminnezhad et al conclude that global standards for cloud security and cloud forensics are necessary to ensure that data can move across borders and be accepted in courts.

Often simply figuring out what law controls data stored in the cloud is a challenge. Although the CSA or associated contracts and addenda can prescribe what laws are enforceable, they don't usually control privacy issues and criminal or civil procedures. (An addendum is used to add or change a contract without having to re-create it.) Many countries with legal systems derived from a common source, such as English common law, might have similar laws but vary in procedures. In addition, how privacy rights are defined in different jurisdictions is a major factor in problems with the right to access data. For example, EU Directive 95/46/EC (http://searchsecurity.techtarget.co.uk/definition/EU-Data-Protection-Directive) is more restrictive than rules in other countries, including the United States. This directive protects private information for all EU citizens, stating that EU citizens must be notified before their personal information is accessed, and this information can be accessed only with their consent. Updates to the EU Data Protection Rules are being made, with member countries expected to incorporate them by May 2018. These updates are of particular interest because they will affect transfer of data outside the EU, which will require that companies and organizations meet EU data protection standards (http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm, 2017).

Some problems are as fundamental as establishing definitions of terms and roles and determining which law is applicable. As mentioned, when data is stored in multiple countries, conflicts in laws can happen. For this reason, digital forensics examiners could be held liable when conducting an investigation involving cloud data. Consult with legal experts when conducting cloud examinations to make sure you're aware of possible restrictions in collecting evidence.

Accessing Evidence in the Cloud

Cloud forensics typically involves litigation of criminal or civil matters. When information or evidence is needed, warrants and subpoenas are used to get it from parties involved in the investigation or litigation. When evidence needs to be seized, warrants are used in criminal cases and issued by law enforcement. When only information is needed, subpoenas are typically issued for civil and criminal cases. In the United States, the Electronic

Communications Privacy Act (ECPA) describes five mechanisms the government can use to get electronic information from a provider: search warrants, subpoenas, subpoenas with prior notice to the subscriber or customer, court orders, and court orders with prior notice to the subscriber or customer. The following sections describe these mechanisms in more detail as they apply to cloud investigations.

Search Warrants

A search warrant can be used only in criminal cases, and it must be requested by a law enforcement officer who has evidence of probable cause that a crime was committed and evidence of it can be found at the location specified in the warrant. There has been a lot of litigation over the concept of "probable cause," but not much case law applies to searches conducted in the cloud.

Note

To get a search warrant, a government entity must show that there's probable cause to believe the contents of a wire communication, an electronic communication, or other records are relevant to an ongoing criminal investigation.

The law requires search warrants to contain specific descriptions of what's to be seized. For cloud environments, the property to be seized usually describes data rather than physical hardware, unless the CSP is a suspect. Generally, however, seizing hardware yields no benefit that seizing just data can't provide.

Seizing hardware can also be disruptive to other customers sharing it with the suspect. For example, FBI agents seized computers from a data center in Dallas, Texas, to gather evidence in an investigation of two men accused of defrauding telecommunication providers. Seizing these computers had the unintended consequence of disrupting the business operations of around 50 companies with data hosted on these systems. The FBI's main motivation in seizing these computers was that the CSP was also a suspect. As a result, however, Liquid Motors, a company providing inventory management services to car dealers, had to shut down its operations and filed a temporary restraining order (TRO) against the FBI the same day to get its data back. Although the TRO was denied, the FBI made mirror images of the data over the weekend to give to Liquid Motors (*Liquid Motors, Inc. v. Lynd*, No. 3:09-cv0611-N, N.D. Tex, April 3, 2009).

Search warrants must also describe the location of items to be seized. This step is straightforward when describing physical locations, but it's less clear when dealing with online data because servers are often dispersed across state or national borders. The near-instant **provisioning** and **deprovisioning** of resources pose a serious legal challenge in cloud forensics. Unless physical machines are seized or virtual machines are turned off, executing a warrant is unlikely to affect the data owner, but the trade-off is that the risk of **spoliation** (failing to preserve evidence) increases if the search is announced. The FBI faced this risk in the Liquid Motors case, which is why hardware was seized along with the data.

Finally, a search warrant must establish how it will be carried out. Safeguards in federal search warrants include specifying the date and time of day to minimize disruptions to people and business operations.

Subpoenas and Court Orders

Under the U.S. federal judicial system, there are government agency subpoenas, non-government and civil litigation subpoenas, and court orders:

- *Government agency subpoenas*—U.S. Code 18 states that customer communications and records can't be knowingly divulged to any person or entity, although it allows specific exceptions to government agencies. This type of subpoena is used to get information when it's believed there's a danger of death or serious physical injury or to get

information for the National Center for Missing and Exploited Children. U.S. federal courts interpret this as meaning that no Stored Communications Act provision permits disclosure for a civil discovery order unless the order comes from a government entity: "Subpoena may not be enforced consistent with the plain language of the Privacy Act because the exceptions enumerated in § 2702(b) do not include civil discovery subpoenas." Most courts have concluded that third parties can't be compelled to disclose electronic communications pursuant to a civil discovery subpoena (*Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 [C.D. Cal. 2010], and *Mintz v. Mark Bartelstein & Associates, Inc.*, 885 F. Supp. 2d 987, 991 [C.D. Cal. 2012]). The SCA doesn't contain an exception for civil discovery subpoenas. See www.law.cornell.edu/uscode/text/18/2702 for more information about this statute.

- *Non-government and civil litigation subpoenas*—These subpoenas are used to produce information from private parties for litigation. An example of how they apply to a CSP can be seen in *Flagg v. City of Detroit* (252 F.R.D. 346, E.D. Mich., 2008). A CSP received a civil subpoena for the production of electronically stored information (ESI) in the cloud, including text messages sent or received by city employees who used mobile devices supplied by SkyTel. Although the court determined that this data could be subject to discovery under the Federal Rules of Civil Procedure, it denied the subpoena because the evidence could have been acquired more easily by making an ESI discovery request to the cloud users. For more information on this case, see www.ca6.uscourts.gov/opinions.pdf/13a0119p-06.pdf and www.ediscoverylaw.com/2008/03/articles/case-summaries/court-sets-protocol-for-production-and-review-of-text-messages/.
- *Court orders*—Court orders are written by judges to compel someone to do or not do something, such as a CSP producing user logon activities. Under U.S. Code 18, court orders are available only to government agencies. In U.S. federal courts, it's interpreted as meaning that a court order can be issued by "any court that is a court of competent jurisdiction" only if the government agency "offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." When a state government agency is involved, a court order can't be issued if the laws of the state prohibit it. For more information, see www.law.cornell.edu/uscode/text/18/2703.

Note

The burden of proof (reasonable grounds) to get a court order is lower than the probable cause required for a search warrant.

Technical Challenges in Cloud Forensics

Cloud forensics procedures combine many computing and networking tasks, such as data recovery, network analysis to detect intrusions, database administration and security, software security, and international relations. In the following sections, you learn about some common technical concerns you'll encounter when performing cloud forensics.

The Cloud Security Alliance has developed the Cloud Forensics Capability Maturity Model (https://downloads.cloudsecurityalliance.org/assets/research/incident-management-and-forensics/CloudForensicsCapabilityModel.pdf), which explores the needs, processes, and responsibilities of both customers and the CSP during an incident response to a VM compromised in a cloud environment. In many instances, customers might simply notice that their VMs aren't functioning correctly or as expected. As with any incident response process, it's assumed that customers have their own incident response teams to identify the problem,

begin analyzing the extent of the problem, contain it, and begin remediation. Larger CSPs have their own incident response teams and work with the customer's team to, for example, get access to affected VMs along with their backups and snapshots. A CSP incident response team should have its own forensics tools to use. What's most important is that both parties should have procedures and resources in place to handle these events.

The NIST Cloud Computing Forensic Science Working Group developed the following list of challenges in conducting cloud forensics. Some of these challenges are discussed in more detail in the following sections:

- Architecture
- Data collection
- Analysis of cloud forensic data
- Anti-forensics
- Incident first responders
- Role management
- Legal issues
- Standards and training

Note

NIST is building standards for cloud forensics procedures. For the most current information, see www.nist.gov/programs-projects/nist-cloud-computing-forensic-science.

Architecture

Clouds vary in their architecture, so no two CSPs are configured in exactly the same way. Depending on the type of cloud architecture, customers' data might be commingled, making it difficult to sort through data to determine what's relevant to an investigation. Identifying data storage locations can be a problem, too, because most CSPs keep these locations secret for security reasons. In addition, differences in recording procedures or log keeping can make it difficult to determine data's origin and complicate an investigation's chain of evidence.

Analysis of Cloud Forensic Data

Analyzing digital evidence collected from a cloud requires verifying the data with other data and log records. You might need to reconstruct the data to determine what actually occurred during an incident and compare network records to make sure servers' internal clocks are synchronized correctly. Examining logs can be useful to compare the modified, last access, and create (MAC) dates and times for files. Metadata from affected files should be examined, too, to validate file accesses. All this information is used to build a timeline to show what happened when an incident occurred.

Anti-Forensics

Destroying ESI that's potential evidence is called "anti-forensics." Anti-forensics tactics are used in cloud environments as well as in other network environments. Hackers might obfuscate incriminating files or hide them by the simple technique of changing file extensions. Specialized malware for defeating evidence collection can add time to an investigation and result in the loss of valuable evidence. Additional methods for anti-forensics include inserting malware programs in other files, using encryption to obfuscate malware programs activated through other malware programs, and using data-hiding utilities that append malware to

existing files. Other techniques affect file metadata by changing the modify and last access times. Changing file timestamps can make it difficult to develop a timeline of a hacker's activities. Calculating hash values of files and comparing the results with known good files' hash values can help identify files that might have been altered. (For a reminder on hashing and using known good files, refer to **Chapter 6**.)

Incident First Responders

Typically, CSPs have personnel trained to respond to network incidents, such as system and network administrators who handle normal support services for the cloud. When a network intrusion occurs, they become first responders to the incident. If a CSP doesn't have an internal first responder team, the forensics examiner should organize CSP staff to handle these tasks. Some factors to address include the following:

- Will the CSP's operations staff be cooperative and follow directions, and will management issue orders stating that you're the leader of the investigation?
- Do you need to brief staff about operations security? For example, you might need to explain that they should talk only to others who have a need to know about the incident and the investigation's activities.
- Do you need to train staff in evidence collection procedures, including the chain of custody?

Role Management

Role management in the cloud covers data owners, identity protection, users, access controls (a list of access privileges and restrictions for each user), and so forth. As an investigator, you need to collect this information so that you can identify additional victims or suspects. Identity protection, for example, means you need to determine whether sensitive personally identifiable information (PII) was compromised, which broadens the investigation's scope. You might also need to determine whether a PII compromise was intentional or accidental, and knowing cloud users' access permissions can help with this task.

Standards and Training

As the cloud becomes more widely used, there's an effort to standardize cloud architectures for operating procedures, interoperability, testing, validation, and so on, and there should be common standards that all CSPs follow. The Cloud Security Alliance (CSA; https://cloudsecurityalliance.org) is one organization that has developed resource documentation for CSPs and their staff. It provides guidance for privacy agreements, security measures, questionnaires, and more.

Training in cloud security and cloud forensics is also continuing to develop. Cloud investigators should have an understanding of cloud architecture in addition to basic digital and network forensics skills. Some sources for cloud forensics training are (ISC)^2's Certified Cyber Forensics Professional (www.isc2.org/ccfp/Default.aspx), INFOSEC Institute (http://resources.infosecinstitute.com/overview-cloud-forensics/), SANS Cloud Forensics with F-Response (http://digital-forensics.sans.org/blog/2013/04/09/cloud-forensics-with-f-response), National Institute of Justice Digital Forensics Training (for law enforcement only; www.nij.gov/topics/forensics/evidence/digital/training/Pages/welcome.aspx), and University College Dublin Centre for Cybersecurity and Cybercrime Investigation (www.ucd.ie/cci/training.html).

Acquisitions in the Cloud

The methods used to collect evidence in cloud investigations depend on the nature of the case. For example, an incident involving a network penetration through a CSP's firewall requires collecting and examining firewall and server logs for attacker activities and ensuring that the

company's database hasn't been accessed or corrupted. Investigating an unauthorized database access, on the other hand, means focusing on transaction logs, too.

For e-discovery and investigations that require collecting specific files and recovering deleted artifacts, the standard acquisition methods discussed in previous chapters must be used, whether they're static or remote acquisitions. Recovering deleted data from cloud storage might be limited to the type of file system the CSP uses. For example, if a CSP uses a Microsoft NTFS RAID system, you can probably recover deleted data. This task might be more difficult if providers use Linux, UNIX, or another file system.

As you learned in **Chapter 3**, remote acquisitions are often more difficult because you're usually dealing with large volumes of data and can be limited by the network speed. You might need to negotiate with attorneys and the CSP about limiting the collection to specific files to prevent scope creep. You can also set up another cloud system dedicated to the investigation, which should grant access only to authorized users, such as digital forensics examiners and first responders. If external network connections are needed, make sure they're protected and monitored through a firewall to guard against unauthorized accesses.

With cloud systems running in a virtual environment, snapshots can give you valuable information before, during, and after an incident. Forensics examiners should re-create separate cloud servers from each snapshot, acquire an image of each server, and calculate an MD5 or SHA-1 hash for all files. They can then compare hash values, modified, MAC (modified, last accessed, and created) dates and times, and file access permission to see what changed between snapshots. With this information, they can determine what files were altered and a time range for when they were altered as well as what files need further inspection of their contents to see what was altered.

Note

To learn more about this technique, see "Forensic Acquisition and Analysis of VMware Hard Disk" (Manish Hirwani, Yin Pan, Bill Stackpole, and Daryl Johnson, Rochester Institue of Technology, July 5, 2012, http://scholarworks.rit.edu/other/297/).

Other factors add complexity to cloud investigations, such as physical servers in the cloud being able to host thousands of virtual networks with virtual switches that run through the same physical router. Unlike physical switches, the virtual switches can't "see" each other. With this setup, VMs can have the same IP address and MAC address on each virtual network that could be owned or rented by different companies. There are also backups and snapshots for each VM as well as logs that show when a failover for a VM was used, when snapshots occurred, and so forth. Therefore, a CSP's team must know how to isolate data that applies to the incident you're investigating.

Encryption in the Cloud

Many CSPs and third parties offer encryption services for cloud users as a security measure, so you should expect to encounter encrypted files in cloud investigations. Knowing how encryption is used in cloud computing helps you plan your investigation and data acquisition. Capturing encrypted data in the cloud is handled the same way as acquiring any encrypted digital evidence, as discussed in Chapter 5. You need assistance from the data owner (the cloud user) or the CSP to decrypt data with the right encryption key. If the data owner is uncooperative, you might need to turn to the attorneys handling the case or the data owner's management and have them direct the data owner to provide the information needed to access files.

Encrypted data in the cloud is in two states: data at rest (data that has been written to disk) and data in motion (data being transmitted over a network). Some systems also have encryption for data in use (data that's in RAM).

Note

Some public CSPs, such as Google Cloud Storage (https://cloud.google.com/storage/) and Microsoft OneDrive (https://onedrive.live.com/about/en-us/), provide encryption for data stored in the cloud and automatically decrypt it when data is accessed. Accessing data encrypted on these servers might require a live acquisition.

More CSPs and third-party vendors are offering cloud encryption tools for cloud customers. If you encounter encrypted data, you need to find out from the CSP what type of encryption was used and who knows how to recover this encrypted data. Some vendors that offer encryption services for cloud data are as follows:

- Atalla Cloud Encryption from Micro Focus (https://software.microfocus.com/en-us/software/data-security-encryption) provides trusted key management and data layer encryption that can encrypt virtual disks, databases, files, and more.
- Trend Micro SecureCloud (http://apac.trendmicro.com/apac/enterprise/cloud-solutions/secure-cloud/index.html) combines encryption with key management based on an organization's security policies. SecureCloud can also wipe data after it's deleted from cloud storage areas. Knowing about this feature is important when attempting to recover deleted data.
- Sophos SafeGuard Encryption and Sophos Mobile Control (www.sophos.com/en-us/products/safeguard-encryption.aspx) provide automatic encryption and decryption for users' uploads and downloads of data. Some public cloud services that can use these applications are Dropbox and OneDrive.

Craig Gentry of IBM, a cryptography researcher, invented an encryption method called "fully homomorphic encryption." Homomorphic encryption uses an "ideal lattice" mathematical formula to encrypt data. This formula uses abstract algebra's ring theory to make encryption more difficult to break. For an explanation of ideal lattices and their use, see "On Ideal Lattices and Learning with Errors over Rings" (Vadim Lyubashevsky et al, https://link.springer.com/chapter/10.1007/978-3-642-13190-5_1, 2010). IBM acquired the patent on homomorphic encryption in 2013 (http://talkcloudcomputing.com/ibms-fully-homomorphic-encryption-technology-gets-patent/).

Block chain technology, used by companies such as Bitcoin, is a way to trace your information while keeping it secure. It's defined as "an incorruptible ledger of economical transactions" (https://blockgeeks.com/guides/what-is-blockchain-technology/). At the time of this writing, all banks in Dubai are required to use block chains by 2020 (https://seekingalpha.com/article/4064985-dubai-globalization-blockchain-technology-fintech), which will have a major impact on the way digital forensics procedures work.

Note

For more information on homomorphic encryption, read about the work being done at Microsoft (www.microsoft.com/en-us/research/project/homomorphic-encryption/).

Conducting a Cloud Investigation

In **Chapter 1**, you learned about taking a systematic approach to digital forensics examinations, and you should use this same approach in investigating cloud incidents. The type of incident determines how to proceed with planning the investigation. For example, if a CSP is a victim of a cyberattack, the investigation should follow network forensics techniques

(covered in Chapters 9 and 10). If the investigation involves searching for and recovering data from cloud storage or cloud customers, review the tools described in Chapters 5 and 6.

Investigating CSPs

As mentioned, CSPs usually have incident response teams trained to handle events such as cyberattacks and responding to e-discovery demands. How much support they offer to forensics investigators is affected by the CSA with cloud customers. If a CSP has no team or limited staff to handle these tasks, investigators should ask the following questions to understand how the CSP is set up:

- Does the investigator have the authority to use cloud staff and resources to conduct an investigation?
- Is detailed knowledge of the cloud's topology, policies, data storage methods, and devices available?
- Are there any restrictions on collecting digital evidence from remote cloud storage?
- For e-discovery demands on multitenant cloud systems, is the data to collect commingled with other cloud customers' unrelated data? Is there a way to separate the data to prevent violating privacy rights or confidentiality agreements?
- Is the data of interest to the investigation local or remote? If it's in a remote location, can the CSP provide a forensically sound connection to it?

For additional guidance on cloud investigations, see "NIST Cloud Computing Forensic Science Challenges," Draft NISTIR 8006 (https://csrc.nist.gov/csrc/media/publications/nistir/8006/draft/documents/draft_nistir_8006.pdf, 2014). Also, refer to the Cloud Security Alliance's guidelines on estimating the amount of time these investigations might take and questions to ask when working with a CSP (see the previous discussion under "Technical Challenges in Cloud Forensics"). For example, if the CSP is giving you the digital evidence, how much time does a keyword search normally take? How many people need to be assigned to a task to meet the incident's requirements?

Investigating Cloud Customers

Cloud customers access CSPs through both computers and mobile devices, such as tablets and smartphones, and can do this through a Web site, an app, or other methods. What's more common now is that organizations such as iCloud, Samsung Cloud, and more are activated automatically unless users turn them off on their smart devices. If a cloud customer doesn't have the CSP's application installed, you might find cloud-related evidence in a Web browser's cache file. If the CSP's application is installed, you can find evidence of file transfers in the application's folder, usually under the user's account folder, such as C:\Users*username*. (If you're examining a mobile device, the location is different.) You can find more information about cloud application activities on a user's computer in the Windows Prefetch folder (C:\Windows\Prefetch). Prefetch files are important when an application synchronizes with a device, as you learn in the next section.

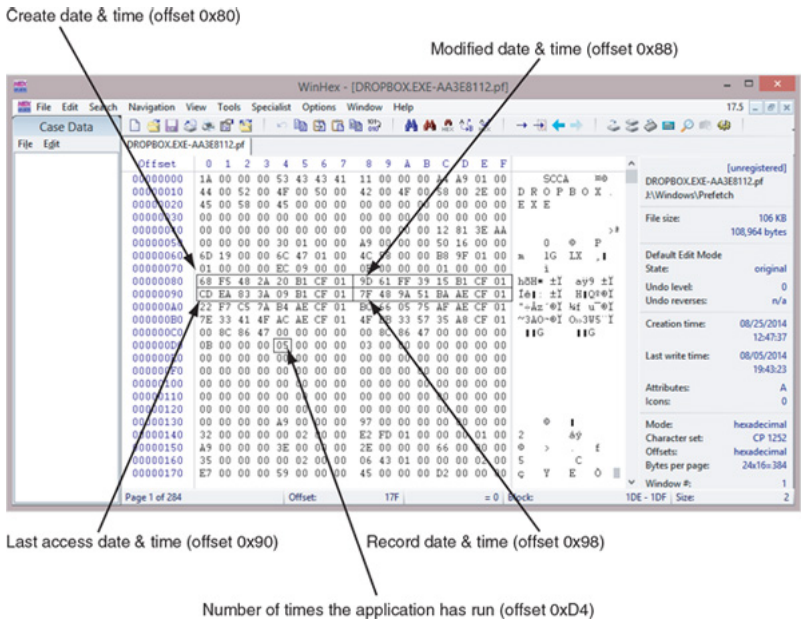
Understanding Prefetch Files

To reduce the time it takes to start applications, Microsoft has created prefetch files, which contain the DLL pathnames and metadata used by an application. They contain a log of prefetcher events along with the data and code accessed. The OS reads the associated prefetch file, which has a .pf extension, and loads its information into the computer's memory to speed an application's start time. This way, the OS can handle other tasks instead of waiting for an application to load the libraries it needs. Metadata in a prefetch file contains, for example, an application's MAC times in UTC format and a counter of how many times the application has

run since the prefetch file was created. If a prefetch file is deleted, Windows re-creates one that resets the MAC times and the counter.

In a prefetch file, the application's create date and time are at offset 0x80, the modified date and time are at offset 0x88, the last access date and time are at offset 0x90, and the record date and time are at offset 0x98. The counter listing the number of times the application has run since creating the prefetch file is at offset 0xD4, as shown in **Figure 13-1**. (See Chapter 5 for a review of how to interpret these dates and times.)

Figure 13-1.



Source: X-Ways AG, www.x-ways.net

Showing the offset positions for the counter and the dates and times for Dropbox.exe

Examining Stored Cloud Data on a PC

Several vendors offer cloud storage to the public. Three widely used services are Dropbox, Google Drive, and OneDrive. These services are free for storage up to 2 GB for Dropbox and up to 15 GB for Google Drive and OneDrive. Users can get more storage for a monthly subscription fee.

When Dropbox or Google Drive is installed on a computer, File Explorer shows it as a separate folder, and data can be copied from and to it. OneDrive is already installed with Windows and is shown as a folder in File Explorer when a user activates his or her OneDrive account. If a user's computer is offline, these services have storage on a user's computer, and when Internet connectivity is restored, they update cloud-stored files based on the user's stored files. If the user accesses the cloud service via the Web on the same computer or a different computer, updates to the original computer are made automatically when the Internet connection is reestablished.

The cloud services Dropbox, Google Drive, and OneDrive have Registry entries, so even if a suspect uninstalls a cloud application, you can usually find information to show it was installed previously. The following sections describe what data to look for in Windows 8.1 and 10 systems that reveals an association with one of these cloud services. The locations of this data might vary in older Windows versions. For other OSs, such as Linux and macOS, you might need to do more research to test how cloud services interact with them. For example, Dropbox should be located in the ~/Dropbox folder in Linux.

Because security is such an important issue with cloud storage, users must maintain control over access to their cloud accounts. An unscrupulous person who cracks a user's cloud password could upload illegal or compromising data to that user's cloud via the Web. The next time the unsuspecting user connects to the cloud, this data is downloaded automatically to his or her computer's synchronized folder. To determine whether this happened, you can review a CSP's Web-connected login records and compare them with date and time values for the suspected files.

Dropbox

In addition to providing secure online data storage, Dropbox (www.dropbox.com) offers third-party applications, such as e-mail, chat, Cisco WebEx, and other collaboration tools. Files that show use of Dropbox are usually in these folders in Windows 8.1:

- C:\Users*username*\Dropbox (contains the folders and files also stored in the Dropbox cloud)
- C:\Users*username*\AppData\Roaming\Dropbox (synchronizes files between the Dropbox cloud and the client workstation)

Note

In Windows 10, the file is in C:\Users*username*\AppData\Roaming\DropboxOEM.

Since 2012, Dropbox has used base-64 format to store the contents of these files, so reading them requires specialized software. Magnet Forensics has a tool called Internet Evidence Finder (IEF) designed for this purpose. It can read and interpret the Dropbox filecache.dbx file, which stores information on shared directories associated with a Dropbox user account and file transfers between Dropbox and the client's system. For more information on IEF features, see www.magnetforensics.com/magnet-ief/. Magnet Forensics also offers a free tool, Dropbox Decryptor (www.magnetforensics.com/free-tool-dropbox-decryptor/), that decrypts filecache.db and config.dbx.

Dropbox prefetch files also create several files: C:\Windows\Prefetch\DROPBOXDECRYPTOR-*nnnnnnnn*.pf, C:\Windows\Prefetch\DROPBOX.EXE-*nnnnnnnn*.pf, C:\Windows\Prefetch\DROPBOXDECRYPTORVnnnNSETUP.TMP-*nnnnnnnn*.pf, and C:\Windows\Prefetch\DROPBOXINSTALLER.EXE-*nnnnnnnn*.pf.

Google Drive

Gmail users have access to Google Drive (www.google.com/drive/download/) for cloud data storage and applications such as Google Docs (a word processor), Google Drawings (a graphics program for charts), Google Forms (an online form and survey tool), Google Sheets (a spreadsheet tool), Google Slides (a slide presentation tool), and PDFzen (a PDF viewer and editor). Users can access Gmail and Google Drive from any Internet-connected computer running Windows Vista or later, macOS, or Linux and smartphones running Android or iOS.

Google Drive is installed in C:\Program Files (x86)\Google\Drive. Each user has a configuration file, called a "user profile," stored in C:\Users*username*\AppData\Local\Google\Drive. If Google Drive has been installed, it creates a folder in the path C:\Users*username*\Google Drive. This folder contains the contents of what has been uploaded to Google Drive cloud storage.

The C:\Users*username*\AppData\Local\Google\Drive\user_default folder contains the synchronization file sync_config.db, which is an SQL database file with the Google Drive upgrade number, the highest application version number, the local synchronization root path, and other parameters. To view this file, extract it to a work folder from the disk or image and

use a SQL viewer program, such as the freeware SQLite Database Browser at SourceForge (http://sourceforge.net/projects/sqlitebrowser/).

Google Drive also creates a snapshot database in the C:\Users*username*\AppData\Local\Google\Drive\user_default folder that lists information about local cloud entries. The snapshot.db file contains information about each file accessed, the URL pathname, the modified and created dates and times in UNIX timestamp format, and the file's MD5 value and size. This file can be read by an SQL viewer, such as SQLite Database Browser. To decipher the UNIX times, see www.onlineconversion.com/unix_time.htm or http://unixtime-converter.com. When files are deleted, Google Drive removes all this information from the snapshot.db file.

The Google Drive file sync_log.log in C:\Users*username*\AppData\Local\Google\Drive\user_default has a detailed list of a user's cloud transactions. You can open this file with any text editor. The create, modify, and delete dates and times in this file are of special interest. Dates and times are formatted as UNIX timestamps. To find this information, search for these string values: RawEvent(CREATE, RawEvent(MODIFY, and RawEvent(DELETE.

If Google Drive has been uninstalled, search for the Web browser's cache and history, shadow volume restore points, Pagefile.sys, Hiberfile.sys, prefetch files, Registry keys of recent file activities, and shortcut files (link files with an .lnk extension).

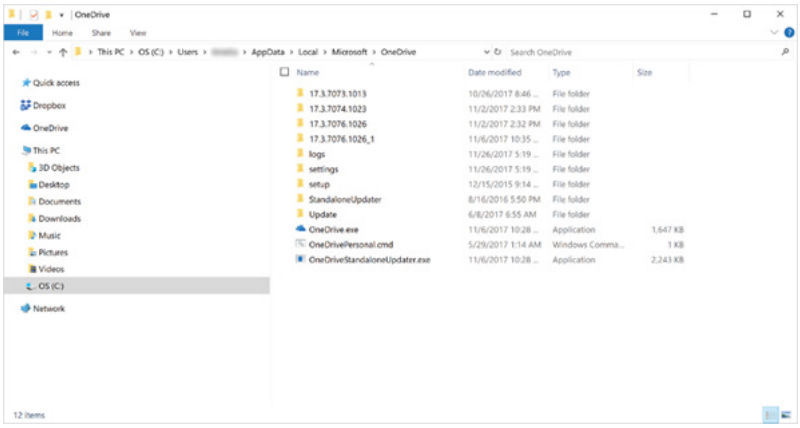
OneDrive

Microsoft created SkyDrive as a cloud service that later became OneDrive (https://onedrive.live.com/about/en-us/); it's available in Windows 8 and later. OneDrive is similar to Dropbox and Google Drive in function and features, such as handling many cloud storage tasks automatically for users. It also offers subscription services for Microsoft software, such as Microsoft Office.

OneDrive stores user profile data in the user's account path, and logs and synchronized files are stored in the following paths:

- Windows 10 log files are in C:\Users*username*\AppData\Local\Microsoft|OneDrive\logs (see Figure 13-2).

Figure 13-2.



The location of OneDrive log files in Windows 10

- Windows 8.1 log files are in C:\Users*username*\AppData\Local\Microsoft\Windows\SkyDrive\logs (or OneDrive\logs).
- Windows 8.1 synchronized files are in C:\Users*username*\AppData\SkyDrive\OneDrive.

- Windows 8 OneDrive prefetch files are named ONEDRIVEREBRAND.EXE-*nnnnnnnn* and stored in C:\Windows\Prefetch. In older versions of Windows, the Windows\Prefetch folder typically contains the prefetch filenames SKYDRIVE.EXE-*nnnnnnnn*.pf, SKYDRIVECONFIG.EXE-*nnnnnnnn*.pf, and SKYDRIVESETUP.EXE-*nnnnnnnn*.pf.

Tip

You might find OneDrive folders and files listed as SkyDrive when looking for the preceding files and paths. SkyDrive folders are typically found in older releases, such as Windows 7 and 8. In addition, some pathnames might vary with the Windows release. When you're looking for OneDrive log files, searching all folders is best.

Some Registry files of interest that Windows 8.1 and 10 use for OneDrive are as follows:

- SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions*nnnnnnnn-nnnn-nnnn-nnnn-nnnnnnnnnnnn*
- SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SyncRootManager\SkyDrive
- SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SyncRootManager\SkyDrive\UserSyncRoots
- SOFTWARE\Microsoft\Windows\CurrentVersion\Live\Roaming
- SOFTWARE\Microsoft\Windows\CurrentVersion\PushNotifications\Applications\MoSkyFileSync
- SOFTWARE\Microsoft\Windows\CurrentVersion\SettingSync\WindowsSettingHandlers\SkyDriveSettings
- SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks*nnnnnnnn-nnnn-nnnn-nnnn-nnnnnnnnnnnn*
- SOFTWARE\Microsoft\Windows Search\FileChangeClientConfigs*nnnnnnnn-nnnn-nnnn-nnnn-nnnnnnnnnnnn*
- NTUSER\Software\Microsoft\Windows\CurrentVersion\SkyDrive
- NTUSER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

Note

Most Registry entries are listed as SkyDrive, but in future Windows updates, this name might change to OneDrive.

You can find more information in the following Windows 8.1 log files, which are in the C:\Users*username*\AppData\Local\Microsoft\Windows\SkyDrive\logs folder:

- SyncEngine-*yyyy-mm-ddnn.nnn-n*.etl manages synchronization between OneDrive and a user's computer. It contains timestamps for activities that have been performed.
- SyncDiagnostics.log contains cid (client ID), clientType, clientVersion, device, deviceID, and timeUtc values. The cid, deviceID, and timeUtc values can be useful for confirming the relationship between OneDrive and a user's computer.

OneDrive is installed by default in Windows 10 in the path C:\Users*username*\AppData\Local\Microsoft\OneDrive. The "logs" folder contains the default subfolders Business1, Common, and Personal, with each containing the following files:

- SyncEngine-*yyyy-mm-dd.nnn,nnnnn.n*.odl also manages the synchronization between OneDrive and a user's computer. It contains timestamps for activities that have occurred.
- telemetryCache.otc.session keeps track of location and activity.
- TraceCurrent.*nnnn.nnnn*.etl deals with synchronization.

Windows Prefetch Artifacts

You can collect prefetch file artifacts with a disk editor or forensics tool. In the following activity, you use WinHex's Data Interpreter to find an application's MAC dates and times and the number of times Dropbox has run. You need WinHex, OSForensics, and the image file InCh05.img from Chapter 5. Follow these steps:

Note

Before beginning this activity, create a *Work*\Chap13\Chapter folder (referred to as your "work folder" in the following steps).

1. Copy **InCh05.img** from Chapter 5 to your work folder for this chapter. Start OSForensics with the **Run as administrator** option, and click **Continue Using Trial Version**. In the left pane, click **Manage Case**, if necessary. In the Manage Case pane on the right, click the **New Case** button. In the New Case dialog box, type **InChap13** in the Case Name text box and your name in the Investigator text box. For the Acquisition Type setting, click the **Investigate Disk(s) from Another Machine** option button, and click **Custom Location** for the Case Folder setting. Click the **Browse** button, navigate to and click your work folder, and then click **OK** twice.
2. To mount the disk image, scroll down the navigation pane on the left and click **Mount Drive Image**.
3. In the "Mounted virtual disks" window, click the **Mount new** button. In the OSFMount - Mount drive dialog box that opens, click the **...** button next to the Image file text box, navigate to your work folder, click **InCh05.img** , click **Open**, and then click **OK**.
4. Click **File Name Search** in the left pane, click the **...** button next to the Config button, navigate to and click the drive letter where you mounted InCh05.img, and then click **OK**. In the Search String text box, type **DROPBOX**, and then click **Search**.
5. When the search is finished, scroll through the list of results and find the DROPBOX.EXE-AA3E8112.pf file in the path C:\Windows\Prefetch (although your drive letter might differ). Right-click this file and click **Open With**.
6. In the How do you want to open this file? dialog box, click **Look for another app on this PC**. In the "Open with" window, navigate to **C:\Program Files \WinHex**(or the location where you installed WinHex), and click **WinHex.exe** .
7. In WinHex, click **View** from the menu, point to **Show**, and click **Data Interpreter**. Click **Options**, **Data Interpreter** from the menu to open the Data Interpreter Options dialog box. Click the **Win32 FILETIME (64 bit)** check box, if necessary, and then click **OK**.
8. Click offset **0x80**, and notice the date and time displayed in the Data Interpreter window. Repeat by clicking at offsets **0x88**, **0x90**, and **0x98** to view the other dates and times.
9. Click **Options**, **Data Interpreter** from the menu again, click to clear the **Win32 FILETIME (64 bit)** check box, click the **8 bit, unsigned** check box, and then click **OK**.
10. Move the cursor and click at offset **0xD4** to see how many times this application has been run. When you're finished, exit OSForensics and WinHex.

Tip

For more information on recovering evidence from computers with Dropbox, Google Drive, and OneDrive, review "Cloud Forensics" (Maegan Katz and Ryan Montelbano, www.champlain.edu/Documents/LCDI/CloudForensics.pdf, 2013) and "Cloud Storage Forensics" (Mattia Epifani, https://digital-forensics.sans.org/summit-archives/Prague_Summit/Cloud_Storage_Forensics_Mattia_Eppifani.pdf, 2013).

Tools for Cloud Forensics

In the early days of the cloud, very few tools designed for cloud forensics were available, but many digital, network, and e-discovery tools were used to handle collecting and analyzing data from the cloud. Some vendors with integrated tools that can be applied to cloud forensics include the following:

- Guidance Software EnCase eDiscovery and its incident response and EnCase Cybersecurity tools
- AccessData Digital Forensics Incident Response services and AD eDiscovery can collect cloud data from Office 365, SharePoint, and OneDrive for Business (http://accessdata.com/blog/3-challenges-to-data-collection-in-the-cloud, 2017)
- F-Response and its cloud server forensics utility

Forensic Open-Stack Tools

Forensic Open-Stack Tools (FROST) integrates with OpenStack running in IaaS cloud environments and adds forensics response capabilities for a CSP. OpenStack is an open-source computing platform intended for public and private cloud services, and FROST is the first known effort to provide a forensics response process for a cloud service. A feature of FROST is that it bypasses a virtual machine's hypervisor. Collected data is placed in the cloud's **management plane** , which is a tool with application programming interfaces (APIs) that allow reconfiguring a cloud on the fly; it's accessed through the application's Web interface. Because the hypervisor is bypassed, special malware can take control of the virtual session and deny or alter access. It can also prevent or interfere with forensic analysis and data collection.

For more information on FROST, see "Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform" (www.cisa.umbc.edu/papers/DFRWS2013_Dykstra_FROST.pdf).

F-Response for the Cloud

F-Response is a remote access tool introduced in **Chapter 3** that can be applied to cloud forensics. It uses USB forwarding techniques to allow non-remote-capable forensics tools, such as X-Ways Forensics, to access remote servers and their data storage. For remote access with F-Response, two tools are needed: F-Response Enterprise or Consultant (www.f-response.com) and KernelPro USB-Over-Ethernet (www.usb-over-ethernet.com). For information on using F-Response, see www.f-response.com/assets/pdfs/CloudForensicsWithF-Response.pdf.

Magnet AXIOM Cloud

Magnet AXIOM has created a Cloud module to go with its Process and Examine modules because most investigations now require collecting information from the cloud as well as from computers, files, and mobile devices. Magnet AXIOM Cloud can retrieve information from Facebook Messenger, Skype, Instagram, Twitter, iCloud, and many other cloud applications. To

access this information, however, you still need usernames and passwords, which you can usually get from victims or suspects.

Chapter Summary

- Three service levels are available for the cloud: software as a service, platform as a service, and infrastructure as a service. These services can be deployed as public clouds, private clouds, community clouds, or hybrid clouds. NIST document SP 500-322, soon to be approved, lists more than 75 cloud services such as backup as a service, security as a service, and Drupal as a service.
- Cloud service providers use servers on distributive networks or mainframes that allow elasticity of resources for customers.
- With multinational clouds, you should seek legal counsel before proceeding with an investigation to make sure you aren't violating another country's privacy laws and to identify all jurisdictions where data is stored. Updates to the EU Data Protection Rules proposed for implementation in May 2018 will affect transfer of data outside the EU.
- Cloud investigations are necessary in cases involving cyberattacks, policy violations, data recovery, and fraud complaints. Cloud forensics is considered a subset of network forensics.
- Before initiating a cloud investigation, you should review the CSA to identify any restrictions that might limit collecting and analyzing data. You should also review the CSP's policies and be aware of contract obligations between the CSP and cloud customers. Some CSPs have customers sharing resources that might cross international boundaries, which is a concern for digital forensics examiners.
- Law enforcement uses search warrants to acquire evidence in a criminal case. For criminal and civil cases, subpoenas and court orders are used to collect evidence. There are three types of subpoenas: government agency, non-government and civil litigation, and court orders.
- Five mechanisms are used to collect digital evidence under the U.S. Electronic Communications Privacy Act (ECPA): search warrants, subpoenas, subpoenas with prior notice to the subscriber or customer, court orders, and court orders with prior notice to the subscriber or customer. A search warrant can be used by law enforcement only when there's evidence of probable cause that a crime was committed and evidence can be found at a specific location.
- Technical challenges in cloud forensics involve cloud architecture, data collection, analysis of cloud forensic data, anti-forensics, incident first responders, role management, legal issues, and standards and training.
- Customer data at CSPs might be commingled, which can make separating it difficult for investigations of a specific customer. Data might also be stored in geographic locations other than where the investigation is taking place, making it difficult to collect evidence and even resulting in conflicts in privacy laws.
- Anti-forensics is an effort to alter log records as well as date and time values of important system files and install malware to hide hackers' activities.
- CSPs should have an incident response team ready to respond to network intrusions. In the absence of this team, it's up to the digital forensics examiner to develop a plan for responding to the incident.
- Role management defines the duties of CSP staff and customers, such as who's the data owner, who's in charge of identity protection, who are the users, and who allows user account access to the CSP. A digital forensics examiner needs this information to determine where data is stored and the impact of its loss to the CSP and customers.

- The Cloud Security Alliance has developed resources that guide CSPs in privacy agreements and security measures. Security and digital forensics training for clouds are sponsored by organizations such as SANS, ISC^2, the INFOSEC Institute, and the National Institute of Justice.
- Procedures for acquiring cloud evidence include examining network and firewall logs, performing disk acquisitions of a cloud system's OS, and examining data storage devices. Data in clouds can be encrypted in two states: at rest and in motion.
- When investigating a cloud incident, apply a systematic approach to planning and processing the case. CSPs typically have incident response teams consisting of system administrators, network administrators, and legal advisors.
- The cloud services Dropbox, Google Drive, and Microsoft OneDrive contain data on a user's computer or mobile device that can reveal what files were copied or accessed along with dates and times they were accessed.
- Prefetch files, which help speed applications' startups, contain metadata on the last date and time an application was run and how many times it has run since being installed. Interpreting this metadata requires a hex editor or forensics tool.
- Vendors offer tools that can be combined for cloud forensics. Specific forensics tools for the cloud are FROST for OpenStack cloud IaaS platforms, F-Response's cloud server utility, and Magnet AXIOM's Cloud module.

Key Terms

cloud service agreements (CSAs)
cloud service providers (CSPs)
community cloud
deprovisioning
hybrid cloud
infrastructure as a service (IaaS)
management plane
multitenancy
platform as a service (PaaS)
private cloud
provisioning
public cloud
software as a service (SaaS)
spoliation

Review Questions

1. Amazon was an early provider of Web-based services that eventually developed into the cloud concept. True or False?

2. What are the three levels of cloud services defined by NIST?

    a. CRC, DRAM, and IMAP

    b. OpenStack, FROST, and management plane

    c. SaaS, PaaS, and IaaS

    d. Hybrid, private, and community clouds

3. What capabilities should a forensics tool have to acquire data from a cloud?
    a. Identify and acquire data from the cloud.
    b. Expand and contract data storage capabilities as needed for service changes.
    c. Circumvent firewalls to access cloud data.
    d. Examine virtual systems.
4. Commingled data isn't a concern when acquiring cloud data. True or False?
5. A(n) ___ is a contract between a CSP and the customer that describes what services are being provided and at what level.
6. Which of the following is a mechanism the ECPA describes for the government to get electronic information from a provider?
    a. Subpoenas with prior notice
    b. Temporary restraining orders
    c. Search warrants
    d. Court orders
7. In which cloud service level can customers rent hardware and install whatever OSs and applications they need?
8. What are the two states of encrypted data in a secure cloud?
    a. RC4 and RC5
    b. CRC-32 and UTF-16
    c. Homomorphic and AES
    d. Data in motion and data at rest
9. Evidence of cloud access found on a smartphone usually means which cloud service level was in use?
    a. IaaS
    b. HaaS
    c. PaaS
    d. SaaS
10. Which of the following cloud deployment methods typically offers no security?
    a. Hybrid cloud
    b. Public cloud
    c. Community cloud
    d. Private cloud
11. The multitenancy nature of cloud environments means conflicts in privacy laws can occur. True or False?
12. To see Google Drive synchronization files, you need a SQL viewer. True or False?
13. A CSP's incident response team typically consists of which staff? List at least three positions.
14. The cloud services Dropbox, Google Drive, and OneDrive have Registry entries. True or False?
15. When should a temporary restraining order be requested for cloud environments?

a. When cloud customers need immediate access to their data

b. To enforce a court order

c. When anti-forensics techniques are suspected

d. When a search warrant requires seizing a CSP's hardware and software used by other parties not involved in the case

16. Updates to the EU Data Protection Rules will affect how data is moved during an investigation regardless of location. True or False?

17. NIST document SP 500-322 defines more than 75 cloud services, including which of the following?

    a. Backup as a service

    b. Security as a service

    c. Drupal as a service

    d. Intelligence as a service

18. Public cloud services such as Dropbox and OneDrive use what encryption applications?

Hands-On Projects

Create a *Work*\Chap13\Projects folder on your system before starting these projects; it's referred to as your "work folder" in steps. If you didn't do the in-chapter activity, copy the InCh05.img file from Chapter 5 to this work folder.

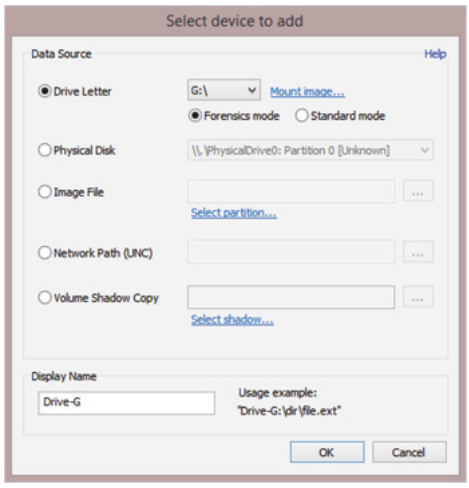
Hands-On Project 13-1.

1. Start OSForensics with the **Run as administrator** option, and click **Continue Using Trial Version**. If you dismounted the InCh05.img image file after the in-chapter activity, mount it again.

2. Click the **Manage Case** button, and verify that the InChap13 case has a green check mark next to it in the Select Case window. If not, right-click the case name and click **Open**. If the case isn't displayed, click **Import Case**, navigate to and click the case location folder, and then click **OK**.

3. You need to find Denise Robinson's account name listed in *drive*:\Users*username*\Dropbox. To find this information, click **File System Browser** in the left pane. In the "Select device to add" dialog box, click the **Drive Letter** option button, if necessary. Click the **Drive Letter** list arrow (see Figure 13-3), click the drive letter assigned to the InCh05.img file, and then click **OK**.

Figure 13-3.

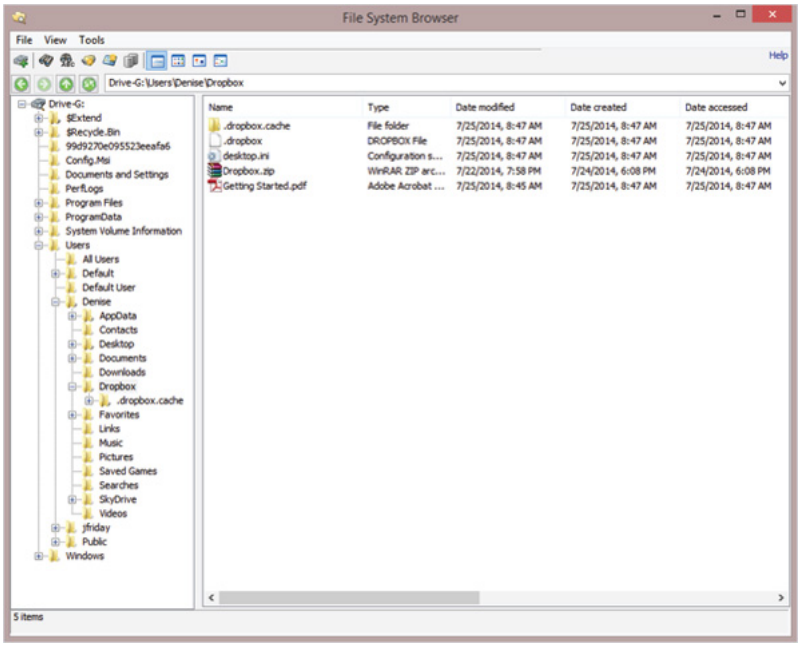


Source: PassMark Software, *www.osforensics.com*

The "Select device to add" dialog box

4. In the File System Browser window, navigate to ***drive*** \ ***Users*** (substituting the correct drive letter for drive) and expand the file listings. Click to expand the **Denise** user account folder, and then click the **Dropbox** subfolder, as shown in Figure 13-4.

Figure 13-4.

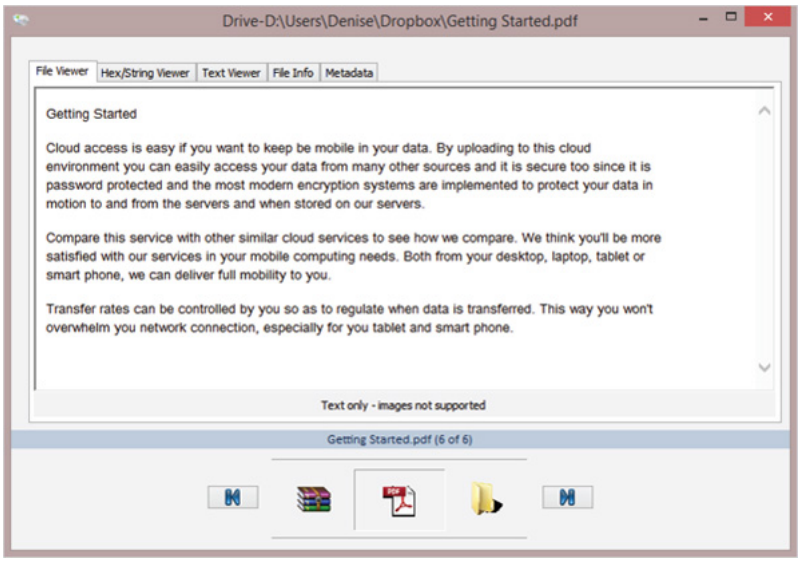


Source: PassMark Software, *www.osforensics.com*

The File System Browser window

5. Right-click the **Getting Started.pdf** file in the right pane and click **View with Internal Viewer** to display its contents. In the viewer window, click the **File Viewer** tab (see Figure 13-5), if necessary, and scroll through the document, which is a welcome notice from Dropbox. Close this viewer window, and repeat this step for other files in this folder to determine their contents.

Figure 13-5.



Source: PassMark Software, *www.osforensics.com*

Viewing the file's contents

6. In the File System Browser window, right-click the **Dropbox.zip** file and click **Save to disk**. In the "Save file as" dialog box, navigate to your work folder, click **Save**, and then click **OK**. Close the File System Browser window.

7. Open File Explorer, navigate to your work folder, and extract (unzip) **Dropbox.zip** . Examine the extracted data, and write a memo to the attorney stating that you recovered the Dropbox.zip file and describing its contents.

8. Leave the InChap13 case open and OSForensics running for the next project.

Hands-On Project 13-2.

The attorney managing the case discovered that Denise Robinson's computer contains the IMG_3646.png file that might have been uploaded to Google Drive. To determine whether it has, you need to examine the Google Drive file sync_log.log. For this project, you need a text editor (Notepad, WordPad, or any word processor), OSForensics, a Web browser, and the image file InCh05.img you saved in Hands-On Project 13-1. Follow these steps:

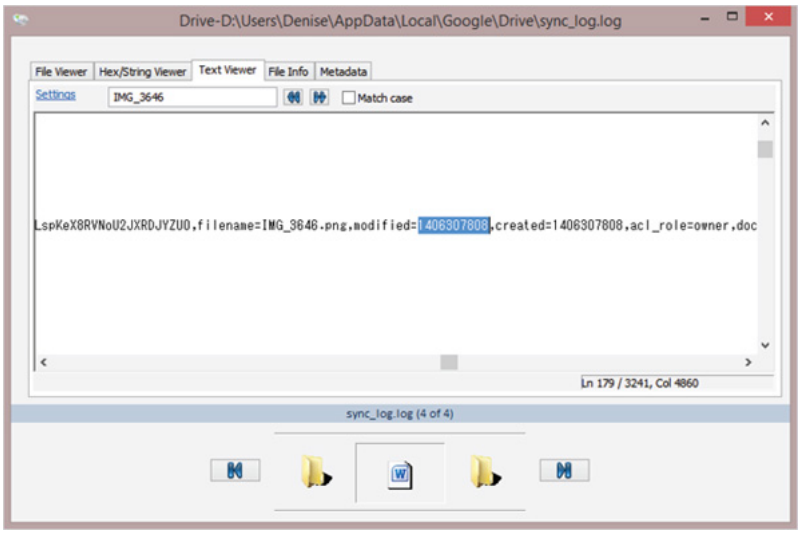
1. If you exited OSForensics, restart it, and open the **InChap13** case and the **InCh05.img** file.

2. Click **File System Browser** in the left pane and navigate to **C:\Users\Denise\AppData\Local\Google\Drive**. Right-click **sync_log.log** and click **View with Internal Viewer**.

3. In the viewer window, click the **Text Viewer** tab, if necessary. In the text box, type **IMG_3646**, and then click the >> button. Finding the file confirms that it was uploaded to Google Drive.

4. Scroll to the right to view the modified =1406307808 and created= 1406307808 values. Because both timestamp values are identical, you need to convert only one of them. Highlight the modified timestamp **1406307808**, as shown in Figure 13-6, and then right-click it and click **Copy**.

Figure 13-6.



Source: PassMark Software, www.osforensics.com

Searching for a file uploaded to Google Drive

5. Start a Web browser, go to http://unixtime-converter.com, paste the numbers into the UNIX TimeStamp text box, as shown in Figure 13-7, and click **Convert**. (*Note*: If you can't access this Web site, try www.onlineconversion.com/unix_time.htm.)

Figure 13-7.

Source: http://unixtime-converter.com

A UNIX timestamp converter

Note

In this book's examples, all date and time values are in the U.S. Pacific time zone, which is -0800 from UTC time for Pacific standard time or -0700 from UTC time for Pacific daylight time. Depending on the conversion utility you're using, these values might be converted to your local time zone. It's important to note the time zone where evidence was collected to make sure you have the correct local time for file activities.

6. In the Result text box, highlight the converted date and time value, and then right-click it and click **Copy**.

7. Start a text editor and type **IMG_3646.png** in the first line. Press **Enter** to add a blank line, and then press **Enter** again. Create two columns by typing **Last modified date**, pressing **Tab** eight times, and typing **Created date**. Place the cursor under the "Last modified date" column, and then right-click and click **Paste**. Repeat to paste the same date and time value under the "Created date" column.

8. Save the file as **Google Drive IMG_3646 date stamps.txt** . Exit the text editor, and turn this file in to your instructor. Leave OSForensics running for the next project.

Hands-On Project 13-3.

The case attorney asked you to examine the OneDrive synchronization folder for Denise Robinson to look for any e-mail correspondence. Follow these steps:

1. If you exited OSForensics, restart it, and open the **InChap13** case and **InCh05.img** file. In the left pane, click **File System Browser**.

2. In the File System Browser window, navigate to ***drive*** :**Users\Denise\SkyDrive\OneDrive\E-mails**. Extract all files with the extension .oxps by right-clicking each file and clicking **Save to disk**, and then clicking **OK** in the message box about saving the file successfully. Exit OSForensics.

3. Open File Explorer, navigate to your work folder, and open each file to view its contents. Write a one-page memo describing the contents of each file you recovered, and then close File Explorer. Turn the memo in to your instructor.

Hands-On Project 13-4.

The case attorney wants to know the last time Denise Robinson accessed Google Drive. To find this information, use the following steps. If you need help, refer to the in-chapter activity.

1. Start WinHex, and open the ***drive*:\Windows\Prefetch\GOOGLEDRIVESYNC(1).EXE-67B59A2.pf** file.

2. Find the Windows date and time at offset ox80 and the number of times this file has been run since it was installed at offset oxD4.

3. Write a memo stating the date, time, and number of times this program has been run. Turn the memo in to your instructor.

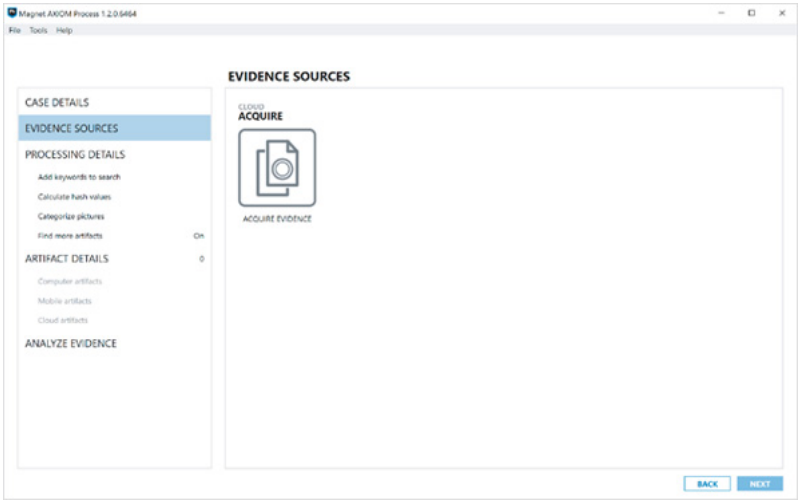
Hands-On Project 13-5.

Jim Shu has been using his phone to access his Facebook and Google Drive information. In this project, you use Magnet AXIOM to examine evidence stored in the cloud.

1. Start Magnet AXIOM Process, and click the **CREATE NEW CASE** button. In the Case number text box, type today's date followed by a hyphen and the number of the case you're working on that day. In the LOCATION FOR CASE FILES section, type **Hands-On Project 13-5** in the Folder name text box. Click the **BROWSE** button next to the File path text box, navigate to and click your work folder, and click **Select Folder**. In the LOCATION FOR ACQUIRED EVIDENCE section, the folder name and file path should update automatically to be the same. If they don't, type **Hands-On Project 13-5** for the folder name and select the path as described previously.

2. Click the **GO TO EVIDENCE SOURCES** button. In the SELECT EVIDENCE SOURCE section, click the **CLOUD** icon, and then click **NEXT**. In the EVIDENCE SOURCES window, click the **ACQUIRE EVIDENCE** icon (see Figure 13-8), and then click **NEXT**.

Figure 13-8.

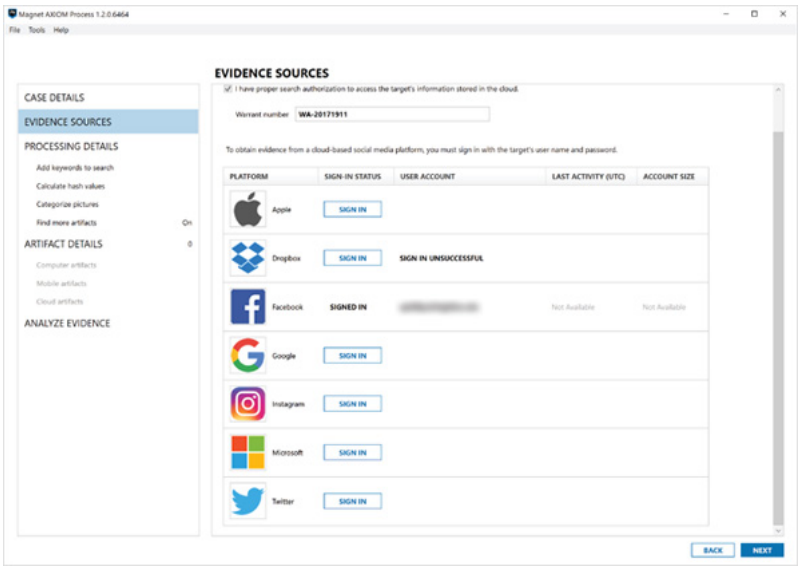


Source: Magnet Forensics, www.magnetforensics.com

Selecting the option to acquire evidence

3. In the next window, click the **I have proper search authorization to access the target's information stored in the cloud** check box. The window shown in Figure 13-9 opens automatically, where you specify which platforms you want to access. (*Note*: For an actual case, you must sign in with victim or suspect's username and password.) Click the **Facebook** icon. In the SIGN IN TO FACEBOOK window, you select a sign-in method as well as your username and password. If you have a Facebook account, enter your login information and attempt to sign in. If you're successful, the SELECT DATE RANGE window opens.

Figure 13-9.



Source: Magnet Forensics, www.magnetforensics.com

Selecting a cloud platform to access

4. Notice that you can set a date range or leave the default option, which is all dates. Your choice might depend on the warrant you have. Under it is the SELECT SERVICES AND CONTENT section with check boxes for Facebook Profile Info, Facebook Messenger Messages, and Facebook Timeline. All are selected by default, so leave them selected for

this project. Click **NEXT** to go to the PROCESSING DETAILS window, where you can add keywords or known hashes for media files, if needed. Click **Cloud Artifacts** on the left. Click **GO TO ANALYZE EVIDENCE**, and in the next window, click **ANALYZE EVIDENCE**.

5. When it's finished processing, start Magnet AXIOM Examine, if necessary. Review all the information on your Facebook account that's available, and take screenshots. In the center pane, click the **Column view** down arrow and click **Timeline view**. Write a one- to two-page paper explaining what information on a suspect or victim could be found. Include your screenshots, and submit them with the paper to your instructor. Exit Magnet AXIOM.

Case Projects

Case Project 13-1.

Privacy laws in other countries are an important concern when performing cloud forensics and investigations. You've been assigned a case involving PII data stored on a cloud in Australia. Before you start any data acquisition from this cloud, you need to research what you can access under Australian law. For this project, look for information on Australia's Privacy Principles (APP), particularly **Chapter 8**: APP 8–Cross-border disclosure of personal information. Write a one- to two-page paper summarizing disclosure requirements, steps for storing PII data in Australia, requirements for getting consent from data owners, and any exceptions allowed by this law.

Case Project 13-2.

As a digital forensics examiner, it's a good idea to build a list of references for information on privacy laws in other countries, which can be useful in cases involving cloud storage. Using the search term "world privacy laws," look for at least three Web sites with references to laws in other countries. Write a one-page paper listing the URL for each site, summarizing what kind of information it offers, and evaluating its ease of use.

Case Project 13-3.

A cloud customer has asked you to do a forensics analysis of data stored on a CSP's server. The customer's attorney explains that the CSP offers little support for data acquisition and analysis but will help with data collection for a fee. The attorney asks you to prepare a memo with detailed questions of what you need to know to perform this task. She plans to use this memo to negotiate for services you'll provide in collecting and analyzing evidence. Write a one- to two-page memo with questions to ask the CSP.

Case Project 13-4.

To examine a cloud environment, you must have the latest knowledge on cloud encryption. Conduct online research, and write a two-page report about current vendors and services for encrypting data stored in the cloud. List the vendors, their products, and what type of cloud service level each tool is intended for, such as PaaS, IaaS, or SaaS.

Chapter 14. Report Writing for High-Tech Investigations

After reading this chapter and completing the exercises, you will be able to:

- Explain the importance of reports
- Describe guidelines for writing reports
- Explain how to use forensics tools to generate reports

This chapter gives you guidelines on writing reports of your findings in digital forensics investigations. You learn about different types of reports and what to include in a typical report and examine how to generate report findings with forensics software tools.

Understanding the Importance of Reports

You write a report to communicate the results of your forensic examination of a computer, network system, or digital device. A forensic report presents evidence that might support further investigation and, in some situations, be admissible in court, at an administrative hearing, or as an affidavit to support issuing an arrest or a search warrant. A report can also provide justification for collecting more evidence and be used at a probable cause hearing, as evidence in a grand jury hearing, or at a motion hearing in civil or criminal cases. In addition, if an employer is investigating employee misconduct, a report might be the basis for disciplinary action. Besides presenting facts, reports can communicate expert opinion. You should look at your report as your first testimony in a case. You must expect to be examined and cross-examined about it. Opposing counsel will look for an opportunity to attack the facts you present, whether you determined them yourself or extracted them from other reports or the expected testimony of other witnesses. You need to know what facts affect your opinion and what facts don't.

For civil cases, including those involving digital forensics investigations, U.S. district courts require that expert witnesses submit written reports; state courts are also starting to require reports from expert witnesses, although the details of these requirements vary. Therefore, if you're a digital forensics examiner involved in a civil case, you must write a report explaining your investigation and findings. Specifically, Rule 26, Federal Rules of Civil Procedure (FRCP; see www.law.cornell.edu/rules/frcp/Rule26.htm), requires that parties who anticipate calling an expert witness to testify must provide a copy of the expert's written report that includes all opinions, the basis for the opinions, and the information considered in coming to those opinions. The report must also include related exhibits, such as photographs or diagrams, and the witness's curriculum vitae listing all publications he or she contributed to during the preceding 10 years. (These publications don't have to be relevant to the case.)

In addition, federal courts, as a matter of rule, require all fact or expert witnesses to provide a report before trial in civil cases. See FRCP 26 (a) (2); Federal Rules of Evidence (FRE) 702, 703, and 705; and the rule stated in *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, which is that testimony is based on sufficient facts or data, testimony is the product of reliable principles and methods, and the witness has applied the principles and methods reliably to the facts of the case. This rule is followed in more than half the states. The remaining states generally follow the rule established in *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923), which states that testimony is inadmissible unless it is "testimony deduced from a well-recognized scientific principle or discovery; the thing from which the deduction is made must be sufficiently established to have gained general acceptance in the particular field in which it belongs."

In addition to opinions and exhibits, the written report must specify fees paid for the expert's services and list all other civil or criminal cases in which the expert has testified (in trials and depositions) for the preceding 4 years. This list doesn't need to include cases in which the expert acted as a consulting expert and didn't provide expert testimony or cases in which the expert testified as a **lay witness** (a witness testifying to personally observed facts).

Although the requirements for information in reports aren't specific, you should keep a copy of any deposition notice or subpoena so that you can include the following information:

- Jurisdiction (for example, U.S. District Court for Eastern District of Washington)
- Style of the case (the format used for official court documents—for example, using a header such as *John Smith, Plaintiff v. Paul Jones, Defendant*)
- Cause number
- Date and location of the deposition
- Name of the deponent (the person testifying at deposition)

There are no requirements to include details of your previous testimony in a report, although you should summarize key points of your testimony for future reference and keep transcripts of your previous testimony, if available.

As an expert witness, you should be aware that lawyers use services called **deposition banks** (libraries), which store examples of expert witnesses' previous testimony. Some of these services have hundreds of thousands of depositions on file and might have several depositions for expert witnesses who testify regularly. After a case is resolved, a lawyer sends copies of the opposing expert witnesses' depositions to the bank to be stored. In preparation for a trial, when the opposing party has identified an expert witness, the attorney might request copies of this witness's previous testimony. Lawyers might also request transcripts of previous testimony by their own potential experts to ensure that the experts haven't testified previously to a contrary position. Lawyers who are members of associations also use electronic mailing lists to ask other members for copies of previous depositions by a specific expert witness.

Note

Attorneys can submit documents electronically in many courts; the standard format in U.S. federal courts and most state courts is Portable Document Format (PDF).

Limiting a Report to Specifics

The client (who might be an attorney, a detective, or an investigator) should define the investigation's goal or mission. All reports to the client should start by stating this mission or goal, which is usually to find information on a specific subject, recover certain important documents, or recover certain types of files or files with specific dates and times. Clearly defining the goals reduces the time and cost of the examination and is especially important with the increasing size of hard drives and complexity of networks.

Before you begin writing, identify your audience and the purpose of the report to help you focus on specifics. Remember that if the audience has little technical knowledge, you might have to dedicate part of the report to educating readers on technical issues. You can do this with a set of several stock paragraphs that you keep on hand, although you should update these stock definitions periodically.

Types of Reports

Digital forensics examiners are required to create different types of reports, such as a formal report consisting of facts from your findings, a preliminary written or verbal report to your attorney, and an examination plan for the attorney who has retained you.

An **examination plan** is a document that serves as a guideline for knowing what questions to expect when you're testifying (see Figure 14-1). Your attorney uses the examination plan as an outline and a guide for your testimony. You can propose changes to clarify or define information or to include substantive information the attorney might have omitted. You can

also use the examination plan to help your attorney learn the terms and functions used in digital forensics.

Figure 14-1.

WITNESS EXAMINATION PLAN
WITNES: Joseph Friday /Factors: Expert Digital Forensic Examiner.
Direct Examination: Expert Testimony Objective/Rule/
Testimony CV
Identity and Address Iowa Bureau of Criminal Investigations
Position (Current) Digital Forensic Examiner
Undergraduate Iowa State University summa cum laude 1990 BS Computer Science
Master's Degree Purdue University, 1992 MS Electrical Engineering
Summer Internship 1989 Des Moines Police Department
Academic Appointments
Lecturer, Dept. of Computer Science, University of Iowa 1998-Current
Instructor, Iowa Police Academy
Professional Society Certifications
P.E. 1990
CISSP 2001
Memberships
American Society of Industrial Security
Publications
Journal of the Iowa State Bar Association, May 1999, "Computer Forensics on RAID Servers-Testifying to Reasonable Certainty"
Experience
How many systems have you conducted forensic examinations on?
The Client
What is your relationship to the Plaintiff? Retained by his attorney to examine the hard drive of his computer for all financial records. I have never actually met or talked to Mr. Smith.
The Specific Examination
How long does it take you to conduct this examination?
What type of files were you looking for? Why those types of files? Where did you find those files?
What condition were the files in?
What is your opinion as to the cause of that condition?
Can you say for a reasonable certainty that the financial data files were deleted intentionally? Yes.
Are you able to state to a reasonable certainty who deleted the financial data files? Yes.
What is your fee for examining the hard drive, preparing a report and testifying?
Anticipated Cross Examination – Expert Testimony
How many times have you worked for Mr. Sawyer as an expert witness? I've done 16 contracts as a consultant expert or expert witness.
Have you ever previously testified that overwriting utilities are not 100% reliable? Yes, but that was in 1994 and utilities are so far as I can tell are 100% reliable today.

A sample examination plan

A verbal report is less structured than a written report. Typically, it takes place in an attorney's office, where the attorney requests the consultant's report. An expert hired as a trial consultant uses verbal reports often. Keep in mind that others can't force your attorney to repeat what you've told him or her in a verbal report. A verbal report is usually a preliminary report and addresses areas of investigation yet to be completed, such as the following:

- Tests that haven't been concluded
- Interrogatories that the lawyer might want to address to opposing parties
- Document production, either requests for production (to parties) or subpoenas (to nonparties, people who have information but aren't a named party in the case)
- Determining who should be deposed and the plan for deposing them

With preliminary reports, mention to your client that your factual statement and opinion are still tentative and subject to change as more information comes in. A written report is frequently an affidavit or a declaration. Because this type of report is sworn to under oath (and penalty of perjury or comparable false-swearing statute), it demands attention to detail, carefully limiting what you write, and thorough documentation and support of what you write. See the following section for more guidelines on written reports.

Guidelines for Writing Reports

The method for expressing an opinion is to have an attorney frame a hypothetical question based on available factual evidence. The law requires that an expert who doesn't have personal knowledge about the system or occurrence must state opinions by response to hypothetical questions, which ask the expert witness to express an opinion based on hypothetical facts

without referring to a particular system or situation. In this regard, you as a forensics investigator (an expert witness) differ from an ordinary witness. You didn't see or hear the incident in dispute; you're giving evidence as an opinion based on professional knowledge and experience, even if you might never have seen the system, data, or scene.

Although the rules of evidence have relaxed requirements on the way an expert renders an opinion, structuring hypothetical questions for your own use helps ensure that you're basing your opinion on facts expected to be supported by evidence. State the facts needed to answer the question, and don't include any unnecessary facts. You might want to address alternative facts, however, if they allow your opinion to remain the same. The expression "alternative facts" might seem contradictory, but it simply means competing facts. In a civil case, if there weren't alternative possible facts, the case wouldn't be at trial; it would have been decided at summary judgment.

Note

An expert's opinion is governed by FRE, Rule 705, and the corresponding rule in many states. For more information on Rule 705, visit www.law.cornell.edu/rules/fre/rule_705.

The following text from a court transcript illustrates an exchange using a hypothetical question between an attorney and a digital forensics expert. The word "presented" is used in this transcript to mean the attorney handed the expert something while asking a question.

> **Mr. Stiubhard:** Mr. Noriki, presented with a hard drive of 1 TB, an attached Maxtor manufacturer's data sheet indicating it was manufactured in May 2017, previous testimony by a detective that the notebook computer in which this drive was found was manufactured by Dell Computer Corporation in June 2017 and purchased by the owner in June 2017. Based on these facts testified to, do you have an opinion whether this is original equipment on this system?
>
> **Mr. Noriki:** Yes.
>
> **Mr. Stiubhard:** Mr. Noriki, what is your opinion on whether this hypothetical hard drive would be the original equipment with the system?
>
> **Mr. Noriki:** Based on facts you have provided, it's my professional opinion that the hard drive would…

Hypothetical questions can be abused and made so complex that the expert might not be able to remember enough of the question to evaluate the answer. Another abuse of the hypothetical question is that it effectively allows attorneys to recite their favored facts to the jury repeatedly and in the order and with the emphasis they want to use. As an expert witness, you can testify to an opinion or a conclusion if these basic conditions are met:

- The opinion, inferences, or conclusions depend on special knowledge, skill, or training not within the ordinary experience of lay witnesses or jurors.
- The witness must be shown to be qualified as a true expert in the field (which is why a curriculum vitae is important).
- The witness must testify to a reasonable degree of certainty (probability) about his or her opinion, inference, or conclusion.
- At minimum, expert witnesses must know the relevant data (facts) on which their opinion, inference, or conclusion is based, and they must be prepared to testify in response to a hypothetical question that sets forth the underlying evidence.

What to Include in Written Preliminary Reports

Remember that anything you write down as part of your examination for a report in a civil litigation case is subject to discovery from the opposing attorney, meaning what you write can or will be given to the opposing attorney. **Discovery** is the process of opposing attorneys seeking information from each other. Therefore, a written preliminary report, such as one created in a software tool before all the data analysis is complete, is considered a **high-risk document** because opposing counsel can demand discovery on it.

If the written preliminary report states a contrary or more equivocal position than you take in your final report or testimony, you should expect opposing counsel to try to discredit your testimony by using the written report. It's simply better if there's no written report to provide. If you must write a preliminary report, don't use words such as "preliminary copy," "draft copy," or "working draft." These words give opposing counsel an opening for discrediting you and make it seem as though the attorney who retained you contributed to what should be your independent professional judgment. In addition, if you do write a preliminary report, don't destroy it before a final resolution of the case or any discovery issue related to the report. Destroying the report could be considered destroying or concealing evidence; among lawyers, this action is called spoliation, and it could subject your client to monetary or evidentiary sanctions. If you've been identified on a witness list provided to the court and opposing counsel, all your work related to the case is potentially subject to discovery.

For written preliminary reports, therefore, include the same information you would supply in an informal verbal report. First, restate the assignment to confirm with your client that the work you have done is focused correctly. Next, summarize what has been accomplished. Identify the systems you have examined, what tools you have used, and what you have seen. State evidence preservation or protection processes you have used. (See **Chapters 3** and 9 for more information on these processes.) The following list shows additional items to include in your report:

- Summarize your billing to date and estimate costs to complete the effort.
- Identify the tentative conclusion (rather than the preliminary conclusion).
- Identify areas for further investigation and get confirmation from the attorney on the scope of your examination.

Report Structure

A report usually includes the sections shown in the following list, although the order varies depending on organizational guidelines or case requirements:

- Abstract (or summary)
- Table of contents
- Body of report
- Conclusion
- References
- Glossary
- Acknowledgments
- Appendixes

Each section should have a title indicating what you're discussing, so make sure it conveys the essential point of the section. For example, the body of your report might be titled "Investigation Findings for Superior Bicycles, Inc.: Intellectual Property Theft."

If the report is long and complex, you should include an abstract. Typically, more people read the abstract than the entire report, so writing one for your report is important. The abstract

and table of contents give readers an overview of the report and its points so that they can decide what parts they need to review. An abstract simply condenses the report's key points to focus on the essential information. It should be one or two paragraphs totaling about 150 to 200 words. Remember that the abstract should describe the examination or investigation and present the report's main ideas in a summarized form. Informative abstracts don't duplicate references or tables of results. As with any research paper, write the abstract last.

The body consists of the introduction and discussion sections. The introduction should state the report's purpose (the questions to be answered) and show that you're aware of its terms of reference. You should also state any methods used and any limitations and indicate how the report is structured. It's important to justify why you're writing the report, so make sure you answer the question "What is the problem?" You should also give readers a map of what you're delivering. Introduce the problem, moving from broader issues to the specific problem, finishing the introduction with the precise aims of the report (key questions). Craft this introduction carefully, setting up the processes you used to develop the information in logical order. Refer to *relevant* facts, ideas, and theories as well as related research by other authors. Organize discussion sections logically under headings to reflect how you classify information and to ensure that your information remains relevant to the investigation.

Two other main sections are the conclusion and supporting materials (references and appendixes). The conclusion starts by referring to the report's purpose, states the main points, draws conclusions, and possibly renders an opinion. References and appendixes list the supporting material to which your work refers. Follow a style manual's guidelines on format for presenting references, such as *Gregg Reference Manual: A Manual of Style, Grammar, Usage, and Formatting; The Chicago Manual of Style: The Essential Guide for Writers, Editors, and Publishers; or MLA Style Manual and Guide to Scholarly Publishing* from the Modern Language Association. Appendixes provide additional resource material not included in the body of the report.

Writing Reports Clearly

To produce clear, concise reports, you should assess the quality of your writing, using the following criteria:

- *Communicative quality*—Is it easy to read? Think of your readers and how to make the report appealing to them.
- *Ideas and organization*—Is the information relevant and clearly organized?
- *Grammar and vocabulary*—Is the language simple and direct so that the meaning is clear and the text isn't repetitive? However, technical terms should be used consistently; you shouldn't try to use variety for these terms. Using different words for the same thing might raise questions.
- *Punctuation and spelling*—Are they accurate and consistent?

Good expert reports share many of the qualities of other kinds of writing. To write is to think, so a report should lay out ideas in a logical order that facilitates logical thinking. Make each sentence follow from the previous one, building an argument piece by piece. Group related ideas and sentences into paragraphs, and group paragraphs into sections. Create a flow from the beginning of the report to the end.

The report should be grammatically sound, have correct spelling, and be free of writing errors. Avoid jargon, slang, or colloquial terms. Most lawyers, judges, and jurors aren't technically trained, so if technical terms must be used, define them in ordinary language (or refer readers to your glossary). Defining acronyms and any abbreviations not used as standard measurement units is particularly important; spell out all acronyms the first time they're used. If there's any possibility of misinterpreting an abbreviation, define it or use the full expression.

For example, “m” is used routinely in scientific and technical writing as an abbreviation for “meter,” but nontechnical readers (especially in the United States) might think it’s an abbreviation for “mile.”

Considering Writing Style

Style means the tone of language you use to address the reader. When writing a report, use a natural language style. For instance, talk about yourself in the first person, not the third person; don’t call yourself “your affiant” when “I” is appropriate and clearly more natural. (However, keep in mind that too many sentences containing “I” can become repetitive.) A natural language style helps keep readers interested in what you have to say. However, you should also follow formal writing guidelines, so pay attention to word usage, grammar, and spelling.

Be sure to avoid vague language and generalizations, as in “There was a problem.” Instead, state the problem specifically and describe what you or others did to solve it. Be careful about repetition, too; repeat only what’s necessary, such as key words or technical terms.

Most of the report describes what you did, so it should be in past tense, but use present or future tense as appropriate. Use active rather than passive voice to avoid boring writing and contorted phrases. For example, “The software recovered the following data” is more direct and, therefore, more interesting to read than “The following data was recovered by the software.”

Avoid including too many details and personal observations. Your only agenda should be finding the truth, so don’t think in terms of catching somebody or proving something. It’s not your job to win the case. Don’t become an advocate for anything other than the truth and your honest objective opinion.

A final caution in writing style: Project objectivity. You must communicate calm, detached observations in your report, so don’t become emotionally involved in the investigation. Always try to identify the flaws in your thinking or examination; it’s better to identify flaws than to allow opposing counsel to do it for you at an embarrassing moment.

Including Signposts

Another aspect of writing clearly is choosing language that gives your readers signposts to what you’re trying to communicate, draws their attention to a point, and shows them the sequence of a process. Signposts assist readers in scanning the text quickly by highlighting the main points and logical development of information.

For example, the first substantive section of your report could start with “This is the report of findings from the forensic examination of computer SN 123456.” The discussion of your examination procedures could be introduced with “The first step in this examination was,” “The second step in this examination was,” and so on. “First” and “second” are signposts that show the sequence of information or tasks. When you want to evaluate something, you might include a signpost such as “The problem with this is…” To show that you’re drawing a conclusion, introduce the point with “This means that …” or “The result shows that….”

Designing the Layout and Presentation of Reports

Layout and presentation involve many factors, including using clear titles and section headings. A numbering system is also part of the layout. Typically, report writers use one of two numbering systems: decimal numbering or legal-sequential numbering. After you choose a system, be sure to follow it consistently throughout the report.

A report using the decimal numbering system divides material into sections and restarts numbering with each main section, as shown in the following example. With this system, readers can scan the headings and understand how one part of the report relates to the other.

I. Abstract

1.1 This report includes a review of data found on hard drives on Computer A and Computer B. Both systems were Dell desktop computers. Computer A had no image files other than those that would have been found in routine office applications. Computer B had more than 2 TB of image data (approximately 120,000 JPG files with dates from January 30, 2017, to March 15, 2018).

II. Detailed Analysis Computer A

2.1. The hard drives of Computer A are designated drive C and drive D.

2.2. Both hard drives are 1 TB Maxtor drives.

2.3. Both hard drives are less than 20% full. Computer B

2.4 The hard drives of Computer B are designated drive C and drive D.

2.5. Both hard drives are 750 GB Seagate drives.

2.6. Both drives are more than 90% full.

The legal-sequential numbering system is often used in legal pleadings. Each Roman numeral represents a major aspect of the report, and each Arabic numeral is an important piece of supporting information, as shown in the following example. This system is meaningful to lawyers but might not be as effective with nonlawyers because the sequential numbering doesn't indicate a hierarchy that shows the relative importance of information in the report.

I. Abstract

1. This report includes a review of data found on hard drives on Computer A and Computer B. Both systems were Dell desktop computers. Computer A had no image files other than those that would have been found in routine office applications. Computer B had more than 2 TB of image data (approximately 120,000 JPG files with dates from January 30, 2017, to March 15, 2018).

II. Detailed Analysis Computer A

2. The hard drives of Computer A are designated drive C and drive D.
3. Both hard drives are 1 TB Maxtor drives.
4. Both hard drives are less than 20% full. Computer B
5. The hard drives of Computer B are designated drive C and drive D.
6. Both hard drives are 750 GB Seagate drives.
7. Both drives are more than 90% full.

Providing Supporting Material

Use supporting material such as figures, tables, data, and equations to help tell the story as it unfolds. Refer to this material in the text and integrate the points they make into your writing. Number figures and tables sequentially as they're introduced (for example, Figure 1, Figure 2, and so forth with another sequence for Table 1, Table 2, and so on).

Figure captions should supply descriptive information. In charts, label all axes and include units of measure. Insert a figure or table after the paragraph in which it's first mentioned, or gather all supporting material in one place after the references section (before any appendixes).

Formatting Consistently

How you format text is less important than being consistent in applying formatting. For example, if you indent paragraphs, be sure all are indented. Use fonts consistently, and use consistent heading styles throughout (for example, major headings in bold with initial capitals, minor headings in italics, and so forth). Follow the same guideline throughout for units of measure; for example, use "%" or "percent," but don't use both. In other words, establish a template and stick to it.

Explaining Examination and Data Collection Methods

Explain how you studied the problem, which should follow logically from the report's purpose. Depending on the kind of data, this section might contain subsections on examination

procedures, materials or equipment, data collection and sources, and analytical or statistical techniques. Supply enough detail for readers to understand what you did.

Data collection is a critical portion of the report. Without good data recording in a lab notebook or file, completing a report beyond this point is futile. If your data collection process becomes the subject of discovery or examination, presenting data in a well-organized manner is important. Use tables in your report to illustrate how data was handled and examined. As mentioned, tables should be labeled clearly as to their content and numbered for easy referral.

Including Calculations

In most cases, hashing algorithms are calculated in digital forensics investigations. If you use any hashing algorithms, be sure to give the common name, such as "Message Digest 5 (MD5) hash." Generally, you don't need to give examples of each type of hash if you're using standard tools; you explain generally what they do and cite the authority or policy you rely on for using the tool. For example, to explain why you're using the MD5 hash, you might cite the National Software Reference Library (NSRL; www.nsrl.nist.gov) as an authority. You could also cite a court case in which a tool's validity had been accepted previously.

Providing for Uncertainty and Error Analysis

In digital forensics, many results can be absolutely true if stated conservatively but might be a guess if you overreach. Therefore, a statement of limitations of knowledge and uncertainty is necessary to protect your credibility. For example, if you're using the timestamp for a file in a Windows OS to indicate that the file was created at a certain time, you need to acknowledge that a PC clock could be reset easily. In addition, you should state that there's no absolute assurance that a file's timestamp is a reflection of its creation time, but there might be other reliable indicators, such as timestamps of other files, creation timestamps for directories, creation order of certain files, and information in automatic backups.

Explaining Results and Conclusions

Explain your findings, using subheadings to divide the discussion into logical parts. Make comments on results as they're presented, discussing the importance of what you found in light of the overall report objectives. Take a step back from the details and synthesize what has (and has not) been learned about the problem and what the information means. Describe what you actually found, not what you hoped to find. Including this discussion as you present results can often improve clarity and readers' understanding.

Link your discussion to figures and tables as you present results, and describe and interpret what these supporting materials show. If you have many similar figures, select representative examples for the main report and put the rest in an appendix. Save broader generalizations and summaries for the report's conclusion. The conclusion should restate the objectives, aims, and key questions and summarize your findings with clear, concise statements. Keep the conclusion brief and to the point.

Providing References

When you write a report, you must cite references to all material you have used as sources for the content of your work. These citations are made wherever you quote, paraphrase, or summarize someone else's opinions, theories, or data. References can include books, periodicals, newspapers, Web sites, conference proceedings, personal communications, and interviews.

In the main section of your report, typically you cite references with the author's last name and year of publication enclosed in parentheses. (Sometimes page numbers are required, too; check the style manual you're following for guidance.) In the references section, you list sources alphabetically by author and provide publication information. Give enough detail so that someone else could track down the information. Follow a standard format, such as the one shown in the following examples, for use of italics, capitalization, volume and page

numbers, publisher address, and other style concerns. Many good style manuals are available, and having one handy is worthwhile.

The following examples show how different sources are presented in the references section; keep in mind that formatting might differ slightly depending on the style manual you follow:

Personal (unpublished) communications:

Cited in the text only, as in "x is recoverable by using tool A (Koenick, F., pers. comm.)."

Lecture notes:

Stiubhard, C. K. "The Curriculum Vitae." Lecture for CIS 411/511, CTIN and City University, Seattle, WA, May 1, 2018.

Web site:

Law Office of Christopher K. Stiubhard. ww w.stiubhardlaw.com, 2016.

Single-author journal article:

O'Herlighy, T. A. "Development of Relationships on the Internet." *Journal of the Advocate* 7, 2018, pp. 130–142.

Multiple-author journal article:

Noriki, H. W., C. K. Stiubhard, and M. D. Clay. "Investigation of Counterfeiting of Spare Parts—A Statistical Analysis." *The Frontline Journal of Aviation* 8, 2015, pp. 150–152.

Book:

Clark, F. and K. Diliberto. *Investigating Computer Crime*. CRC Press, New York, 2008.

Government or technical report:

U.S. Department of Justice. "The Examination of Computers." Report XYZ-001, Washington, DC, 2018.

Chapter in an edited volume:

Pellegrino, A. "Investigation of the Automated Backup Copies of Microsoft Application Files." In Noriki, H. W. et al, *Computer Forensics*. Learning Technology, Springfield, MA, 2017.

Including Appendixes

If necessary, you can include appendixes containing material such as raw data, figures not used in the body of the report, and anticipated exhibits. Arrange them in the order referred to in the report. They are considered additional material and might not be examined by readers. Some portions of appendixes might be considered optional, but others are required. For example, exhibits are required under FRCP, Rule 26, as is your curriculum vitae (unless bona fides are integrated into the report).

Tip

Whether you're working for a law firm, digital forensics company, research lab, or law enforcement agency, these organizations have established formats for reports. Be sure to get samples or templates from them before beginning your report.

Note

For an example of a report, see Vincenzo D. Crawford's report at www.academia.edu/12324822/Example_of_An_Expert_Witness_Digital_forensics_Report?auto=download. Another source is available at https://allegiantinvestigation.com/writing-a-forensics-expert-report/.

Generating Report Findings with Forensics Software Tools

With many forensics software tools, log files of analysis activities and reports can be created that provide information about the findings for a case. Although forensics software reports what was found and where, remember that it's your responsibility to explain the significance of the evidence you recover and, if necessary, define any limitations or uncertainty that applies to your findings. These reports and logs are typically in text, word processing, spreadsheet, or HTML format. In this section, you learn how to integrate a software-generated report into the official investigation report that you present to your attorney or client.

Using Autopsy to Generate Reports

Note

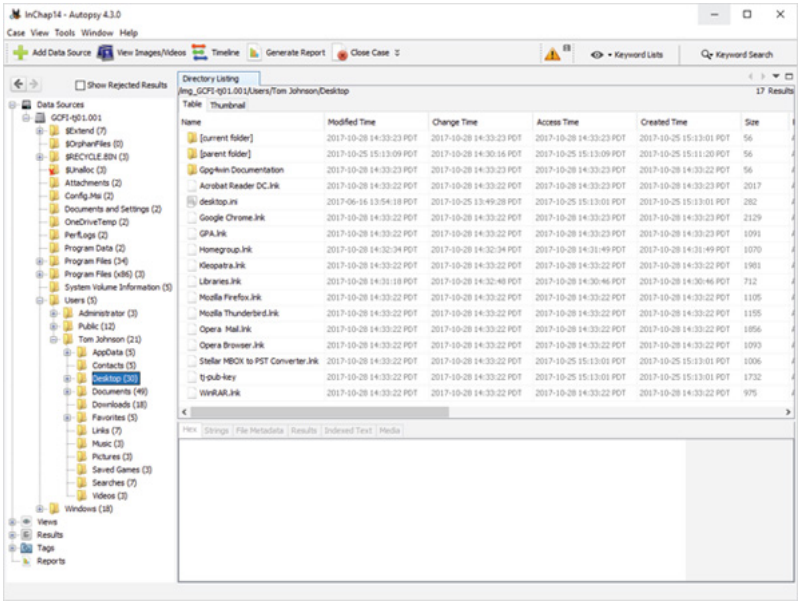
Before starting the activity, create a *Work*\Chap14\Chapter folder on your system (referred to as your "work folder" in steps). Your folder name will likely differ from what's shown in screenshots. Download to your work folder the Ch14Inchp01.exe file from this chapter's downloads section on the student companion site for this book.

For this activity, you do an inventory of software on Tom Johnson's computer. Management at Superior Bicycles, Inc., wants to know the authorized and unauthorized applications on his and several other employees' computer to make sure everyone is compliant with software licensing. In this activity, you use Autopsy for Windows to find the evidence and create a report of your findings.

In **Chapter 9**, you generated an Excel report listing hash values for Special Project-A. For this activity, you produce a similar report listing all application files on Tom Johnson's computer in HTML format for Harry Mudd, the IT manager at Superior Bicycles. The report should be divided into authorized applications (consisting of all Microsoft products) and unauthorized applications (that aren't Microsoft products). Follow these steps:

1. In File Explorer, double-click the **Ch14Inchp01.exe** file and click **Extract** to uncompress it into GCFI-tj01.001.
2. Start Autopsy for Windows, and click the **Create New Case** button. In the New Case Information window, enter **InChap14** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**.
3. In the Additional Information window, type **InChap14** in the Case Number text box and your name in the Examiner text box, and then click **Finish** to start the Add Data Source Wizard.
4. In the Select Data Source window, click the **Browse** button next to the "Browse for an image file" text box, navigate to your work folder, click the **GCFI-tj01.001** file, and click **Open**. Click **Next**.
5. In the Configure Ingest Modules window, click **Deselect All**, and click the **File Type Identification** check box. Click **Next** and then **Finish**.
6. When Autopsy finishes its analysis, go to the Tree Viewer pane. Click to expand **Data Sources**, **GCFI-tj01.001**, **Users**, and **Tom Johnson**, and then click **Desktop** to display its contents, as shown in Figure 14-2.

Figure 14-2.



Source: www.sleuthkit.org

Viewing the Desktop folder

.

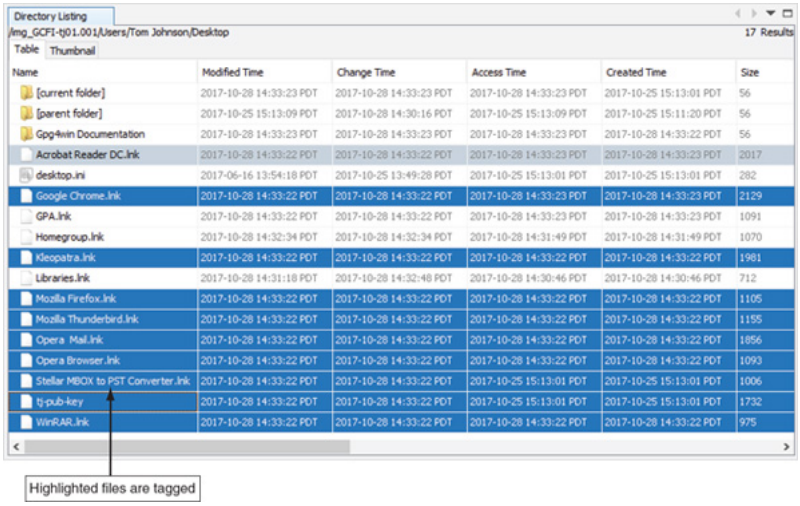
7. In the Result Viewer pane, right-click **Acrobat Reader DC.lnk** , point to **Tag File**, and click **Tag and Comment.** In the Create Tag dialog box, click the **New Tag Name button**, type **Unauthorized Applications** in the Tag Name text box, and then click **OK** twice.

8. Next, right-click **Google Chrome.lnk** , point to **Tag File** and **Quick Tag**, and then click **Unauthorized Applications**.

9. Repeat **Step 8** to tag the following files (see Figure 14-3):

- **GPA.lnk**
- **Kleopatra.lnk**
- **Mozilla Firefox.lnk**
- **Mozilla Thunderbird.lnk**
- **Opera Mail.lnk**
- **Opera Browser.lnk**
- **Stellar MBOX to PST Converter.lnk**
- **tj-pub-key**
- **WinRAR.lnk**

Figure 14-3.



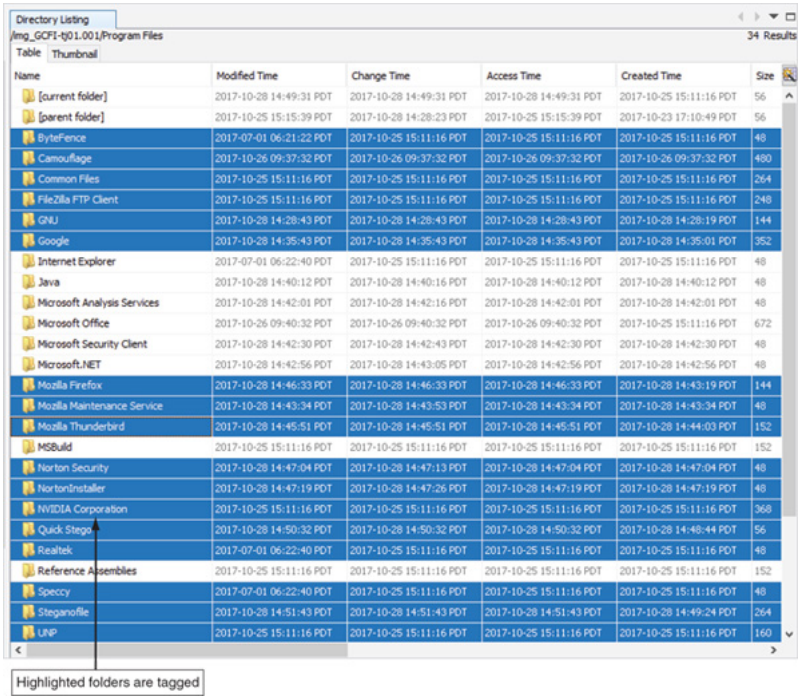
Source: www.sleuthkit.org

Tagged files in the Desktop folder

10. In the Tree Viewer pane, under GCFI-tj01.001, click to expand **Program Files**. In the Result Viewer pane, tag the following application folders as **Unauthorized Applications** (see Figure 14-4):

- **ByteFence**
- **Camouflage**
- **FileZilla FTP Client**
- **GNU**
- **Google**
- **Java**
- **Mozilla Firefox**
- **Mozilla Maintenance Service**
- **Mozilla Thunderbird**
- **Norton Security**
- **NortonInstaller**
- **NVIDIA Corporation**
- **Quick Stego**
- **Realtek**
- **Speccy**
- **Steganofile**
- **UNP**

Figure 14-4.



Source: www.sleuthkit.org

Tagged application folders under Program Files

11. Right-click **Internet Explorer** in the Result Viewer pane, point to **Tag File**, and click **Tag and Comment**. In the Create Tag dialog box, click the **New Tag Name** button, type **Authorized Applications** in the Tag Name text box, and then click **OK** twice.

12. Next, right-click **Microsoft Analysis Services**, point to **Tag File** and **Quick Tag**, and then click **Authorized Applications**.

13. Repeat **Step 12** to tag the following folders:

- **Microsoft Office**
- **Microsoft Security Client**
- **Microsoft.NET**
- **MSBuild**
- **Windows Defender**
- **Windows Mail**
- **Windows Media Player**
- **Windows NT**
- **Windows Photo Viewer**
- **Windows Security**
- **Windows PowerShell**

14. Click **Generate Report**. In the Generate Report window, click the **Results - HTML** option button in the Report Modules section, and then click **Next**.

15. In the Configure Artifact Reports window, click the **Tagged Results** button, click **Select All**, and then click **Finish**.

16. In the Report Generation Progress Complete window, click the **Results - HTML** link to open the report. With the report open in your Web browser, click the **Tagged Files** link and print the report in landscape mode to review its contents.

17. Click **Close**, and then exit Autopsy.

Chapter Summary

- All U.S. district courts and many state courts require expert witnesses to submit written reports.
- Rule 26 of the FRCP in the United States requires expert witnesses who anticipate that they will have to testify to submit written reports. The report must include the expert's opinion along with the basis for the opinion.
- Attorneys use deposition banks to research expert witnesses' previous testimony and to learn more about expert witnesses hired by opposing counsel.
- Reports should answer the questions you were retained to answer and keep information that doesn't support specific questions to a minimum.
- A well-defined report structure contributes to readers' ability to understand the information you're communicating. Make sure your report includes clearly labeled sections and follows a numbering scheme consistently. Ensure that supporting materials, such as figures and tables, are numbered and labeled clearly.
- Clarity of writing is critical to a report's success. Make sure to include signposts to give readers clues about the sequence of information, and avoid vague wording, jargon, and slang.
- Convey a tone of objectivity, and be detached in your observations. Synthesize what has (and has not) been learned about the problem and what the information means.

Key Terms

deposition banks
discovery
examination plan
high-risk document
lay witness

Review Questions

1. Which of the following rules or laws requires an expert to prepare and submit a report?
    a. FRCP 26
    b. FRE 801
    c. Neither
    d. Both
2. For what purpose have hypothetical questions traditionally been used in litigation?
    a. To frame the factual context of rendering an expert witness's opinion
    b. To define the case issues for the finder of fact to determine
    c. To stimulate discussion between a consulting expert and an expert witness
    d. To deter a witness from expanding the scope of his or her investigation beyond the case requirements
    e. All of the above

3. If you were a lay witness at a previous trial, you shouldn't list that case in your written report.

4. Which of the following is an example of a written report?

a. A search warrant

b. An affidavit

c. Voir dire

d. Any of the above

5. What is destroying a report before the final resolution of a case called?

6. An expert witness can give an opinion in which of the following situations?

a. The opinion, inferences, or conclusions depend on special knowledge, skills, or training not within the ordinary experience of laypeople.

b. The witness is shown to be qualified as a true expert in the field.

c. The witness testifies to a reasonable degree of certainty (probability) about his or her opinion, inference, or conclusion.

d. All of the above

7. Which of the following is the standard format for reports filed electronically in U.S. federal courts and most state courts?

a. Word

b. Excel

c. PDF

d. HTML

8. When writing a report, what's the most important aspect of formatting?

a. A neat appearance

b. Size of the font

c. Clear use of symbols and abbreviations

d. Consistency

9. Automated tools help you collect and report evidence, but you're responsible for doing which of the following?

a. Explaining your formatting choices

b. Explaining the significance of the evidence

c. Explaining in detail how the software works

d. All of the above

10. What can be included in report appendixes?

11. Which of the following statements about the legal-sequential numbering system in report writing is true?

a. It's favored because it's easy to organize and understand.

b. It's most effective for shorter reports.

c. It doesn't indicate the relative importance of information.

d. It's required for reports submitted in federal court.

12. What's a major advantage of automated forensics tools in report writing?

Hands-On Projects

At Superior Bicycles, Inc., there are strict guidelines on how to conduct investigations of employees to ensure that employees under investigation are treated fairly and to avoid any embarrassment to them and the company. There must be a series of inquiries and analysis of

information to justify a full forensics examination of an employee's computer. In the example used in the in-chapter activity, an audit for unauthorized applications was conducted on Tom Johnson's computer. The following projects require a systemic approach of collecting additional evidence to justify a full examination of Tom Johnson's computer.

In the first four projects, you examine data to determine whether a company policy violation has taken place. In the fifth project, you consolidate the information from the in-chapter activity and the first four projects into a report for the general counsel, Ralph Benson. Before starting these projects, create a *Work*\Chap14\Projects work folder.

Hands-On Project 14-1.

In the in-chapter activity, you examined Tom Johnson's computer and found several instances of unauthorized applications. Harry Mudd, the IT manager at Superior Bicycles, wants to know whether Mr. Johnson's computer contains any Special Project-A files. For this project, you use the Special Project-A hashes you created in **Chapter 9** and generate a report listing these files. Follow these steps:

1. Start Autopsy for Windows, and click the **Create New Case** button. In the New Case Information window, enter **Proj1401** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**.
2. In the Additional Information window, type **Proj1401** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.
3. In the Select Data Source window, click the **Browse** button next to the "Browse for an image file" text box, navigate to your work folder and click the **GCFI-tj01.001** file, and then click **Open**. Click **Next**.
4. In the Configure Ingest Modules window, click the **Deselect All** button, and in the pane above that button, click the **File Type Identification** and **PhotoRec Carver** check boxes.
5. Click the **Hash Lookup** check box, and in the "Select known hash databases to use" section, click the **NISTFile-*nnn*m.txt-md5** check box. In the "Select known BAD hash databases to use" section, click the **Special Project-A** and **Superior-Personnel Records** check boxes, and then click the **Calculate MD5 even if no hash database is selected** check box.
6. Click **Next** and then **Finish**. When Autopsy finishes its analysis, go to the Tree Viewer pane, and click to expand **Results**, **Hashset Hits** to examine Special Project-A files on Tom Johnson's computer.
7. In the Result Viewer pane, Ctrl+click all files. Right-click this selection, point to **Tag Results** and **Quick Tag**, and click **Special Project-A**.
8. In the Tree Viewer pane, click **Tags**, **Special Project-A**, and then **Result Tags**. In the Result Viewer pane, click the **Thumbnail** tab.
9. In the Thumbnail tab, right-click each photo and click **View in Window** to examine its contents. Note that all the photos appear to be the same: a kayak under construction.
10. Click **Generate Report** at the top. In the Generate Report window, click the **Results - Excel** option button in the Report Modules section, and then click **Next**. In the Configure Artifact Reports window, click the **Tagged Results** option button, click the **Special Project-A** check box, and then click **Finish**.
11. When the report has been generated, click the **Results - Excel** pathname in the Report Generation Progress window. In the Excel file, examine the contents of the

Tagged Files sheet. When you're finished, save the Excel file as **Proj1401-Report** in your work folder.

12. Click **Close Case**. Write a short memo to Harry Mudd describing the two photos you identified with the Special Project-A hashes. Include information about each file from the Excel spreadsheet. Turn the memo into your instructor, and leave Autopsy running for the next project.

Hands-On Project 14-2.

Harry Mudd forwarded your memo to his boss, Bob Swartz, the chief engineer for Superior Bicycles. Mr. Swartz asks Mr. Mudd to have you look for other potential photos and archive files on Mr. Johnson's computer related to Special Project-A and bicycle components. Follow these steps:

1. Start Autopsy for Windows, and click the **Create New Case** button. In the New Case Information window, enter **Proj1402** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**.

2. In the Additional Information window, type **Proj1402** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

3. In the Select Data Source window, click the **Browse** button next to the "Browse for an image file" text box, navigate to your work folder and click the **GCFI-tj01.001** file, and then click **Open**. Click **Next**.

4. In the Configure Ingest Modules window, click the **Deselect All** button, and in the pane above that button, click the **File Type Identification**, **Embedded File Extractor**, **PhotoRec Carver**, and **Exif Parser** check boxes.

5. Click the **Hash Lookup** check box, and in the "Select known hash databases to use" section, click the **NISTFile-*nnn*m.txt-md5** check box. In the "Select known BAD hash databases to use" section, click the **Special Project-A** and **Superior-Personnel Records** check boxes, and then click the **Calculate MD5 even if no hash database is selected** check box.

6. Click **Next** and then **Finish**. When Autopsy finishes its analysis, go to the Tree Viewer pane, and expand **Views, File Types, By Extension**, and **Images**. In the Result Viewer pane, click the **Thumbnail** tab and find photos of kayaks and bicycle components.

Tip

To see the thumbnails better, right-click a photo and click View in New Window to enlarge it.

7. Ctrl+click all photos of interest to highlight them. Right-click the selection, point to **Tag Files**, and click **Tag and Comment**. In the Create Tag dialog box, click the **New Tag Name** button. In the New Tag section, type **TJohnson-photos**, and then click **OK** twice.

8. In the Tree Viewer pane, expand **Views, File Types, By Extension**, and **Archives**. In the Result Viewer pane, click the **Table** tab, and find any Special Project-A files with a .zip or .cab extension.

9. Ctrl+click all files of interest to highlight them. Right-click the selection, point to **Tag Files**, and click **Tag and Comment**. In the Create Tag dialog box, click the **New Tag Name** button. In the New Tag section, type **TJohnson-archives**, and then click **OK** twice.

10. Click **Generate Report** at the top. In the Generate Report window, click the **Results - Excel** option button in the Report Modules section, and then click **Next**. In the

Configure Artifact Reports window, click the **Tagged Results** option button, click **Select All**, and then click **Finish**.

11. When the report has been generated, click the **Results - Excel** pathname in the Report Generation Progress window. In the Excel file, examine the contents of the Tagged Files sheet. When you're finished, save the report as **Proj1402-Report** in your work folder.

12. Click **Close Case**. Write a short memo to Harry Mudd describing the two photos you identified with the Special Project-A hashes, and include information about each file from the spreadsheet. Turn the memo in to your instructor, and leave Autopsy running for the next project.

Hands-On Project 14-3.

Mr. Mudd forwarded your latest memo to Mr. Swartz, who forwarded both memos to the CEO of Superior Bicycles, Chris Robinson. Mr. Robinson has consulted with the general counsel, Ralph Benson, for his opinion on what to do next. Mr. Benson sends you a memo asking you to look for more information. He wants to see some of the e-mails sent to Mr. Johnson and asks that all your correspondence and reports about this investigation include the headers "Attorney-Client Privilege" and "Attorney Work Product." For this project, examine all e-mails on Mr. Johnson's computer. Find and tag e-mails that might define Mr. Johnson's activities with people who aren't with Superior Bicycles. Follow these steps:

1. Start Autopsy for Windows, and click the **Create New Case** button. In the New Case Information window, enter **Proj1403** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**.

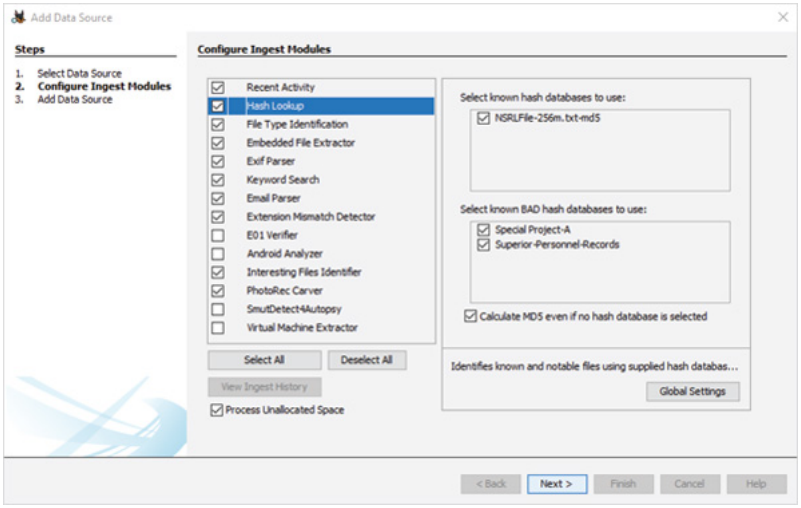
2. In the Additional Information window, type **Proj1403** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

3. In the Select Data Source window, click the **Browse** button next to the "Browse for an image file" text box, navigate to your work folder and click the **GCFI-tj01.001** file, and then click **Open**. Click **Next**.

4. In the Configure Ingest Modules window, click the **Deselect All** button, and in the pane above that button, click the **Recent Activity, File Type Identification, Embedded File Extractor, Exif Parser, Email Parser**, **Interesting Files Identifier**, and **PhotoRec Carver** check boxes.

5. In the list of ingest modules, click the **Hash Lookup** check box, and in the "Select known hash databases to use" section, click the **NISTFile-*nnn*m.txt-md5** check box. In the "Select known BAD hash databases to use" section, click the **Special Project-A** and **Superior-Personnel Records** check boxes, and then click the **Calculate MD5 even if no hash database is selected** check box, as shown in Figure 14-5.

Figure 14-5.



Source: www.sleuthkit.org

Selecting subfunctions for the Hash Lookup ingest module

6. In the list of ingest modules, click the **Keyword Search** check box, and in the "Select keyword lists to enable during ingest" section, click the check boxes for **Phone Numbers, IP Addresses, Email Addresses**, and **URLs**.

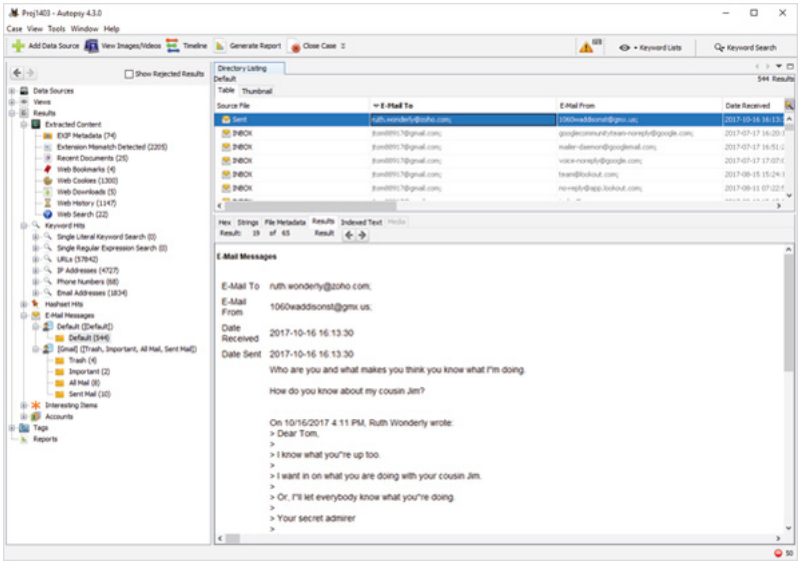
7. Click the **Extension Mismatch Detector** check box in the list of ingest modules, and then click the **Check all file types** option button, and the **Skip files without extensions** and **Skip known files** check boxes.

8. Click **Next** and then **Finish**. When Autopsy finishes its analysis, go to the Tree Viewer pane, and click to expand **E-Mail Messages, Default (Default)**, and **Default**.

9. In the Result Viewer pane, click the **E-Mail To** column twice to sort all sent e-mails in descending order.

10. In the Result Viewer pane, click the first e-mail from ruth.wonderly@zoho.com, and read it (see **Figure 14-6**). This message is to a person who doesn't work at Superior Bicycles and states, "I know what you"re up too. I want in on what you are doing with your cousin Jim."

Figure 14-6.



Source: www.sleuthkit.org

Reviewing the contents of the first e-mail in the Sent folder

11. Right-click this e-mail, point to **Tag Result**, and click **Tag and Comment**. In the Create Tag dialog box, click the **New Tag Name** button. In the New Tag section, type **Non-SB-Email-Address**, and then click **OK** twice.

12. Go through the e-mails in the E-Mail To column and tag the ones meeting the criteria, ignoring any redundant messages. To do this, right-click the e-mail, point to **Tag Result** and **Quick Tag**, and click **Non-SB-Email-Address**.

13. Click **Generate Report** at the top. In the Generate Report window, click the **Results - Excel** option button in the Report Modules section, and then click **Next**. In the Configure Artifact Reports window, click the **Tagged Results** option button, click **Select All**, and then click **Finish**.

14. When the report has been generated, click the **Results - Excel** pathname in the Report Generation Progress window. In the Excel file, examine the contents of the Tagged Files sheet. When you're finished, save the Excel file as **Proj1403-Report** in your work folder.

Tip

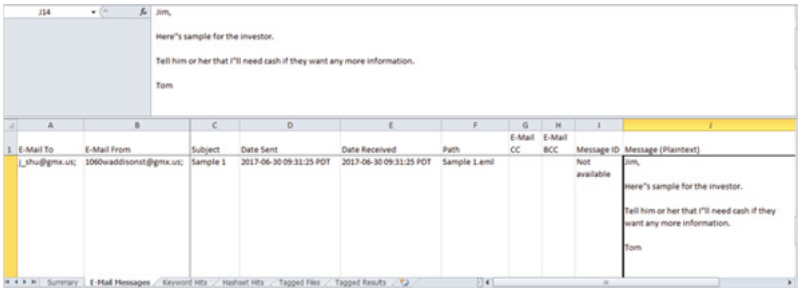
When you open the Excel report, if you get an error message stating that the file has unreadable content, click Yes to recover and view the workbook.

15. Write a short memo to Ralph Benson stating that you have found several e-mails to people who don't work at Superior Bicycles, and include the spreadsheet you generated. Turn the memo and spreadsheet in to your instructor, and leave Autopsy running for the next project.

Hands-On Project 14-4.

After submitting your report and spreadsheet from **Hands-On Project 14-3**, you get a message from Ralph Benson, asking you for a copy of the file attached to Mr. Johnson's e-mail (from his 1060waddisonst@gmx.us account), which was sent to j_shu@gmx.us and dated 2017-06-30 09:31:25 PDT, with the subject line "Sample 1" (see Figure 14-7).

Figure 14-7.



Source: www.sleuthkit.org

The Sample 1 e-mail in the spreadsheet

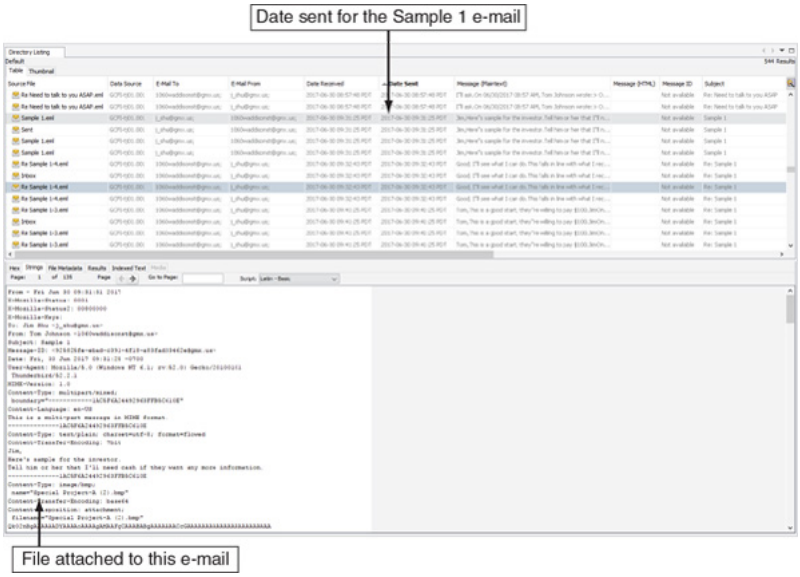
Note

Depending on how many files you tagged in **Hands-On Project 14-3**, your Excel spreadsheet might list this e-mail on a different line number. To find it, sort the spreadsheet's Date Sent column to find the date and time 2017-06-30 09:31:25 PDT.

To find and extract the attached file from this e-mail, follow these steps:

1. If you exited Autopsy, start Autopsy for Windows and open project **Proj1403**.
2. In the Tree Viewer pane, click to expand **E-Mail Messages**, **Default (Default)**, and **Default**. In the Result Viewer pane, click the **Date Sent** column once to sort its contents in ascending order, and then scroll down until you see the date 2017-06-30 09:31:25 PDT for Sample 1.eml. In the Content Viewer pane, click the **Strings** tab. Near the bottom, find the string filename="Special Project-A (2).bmp"(see Figure 14-8).

Figure 14-8.



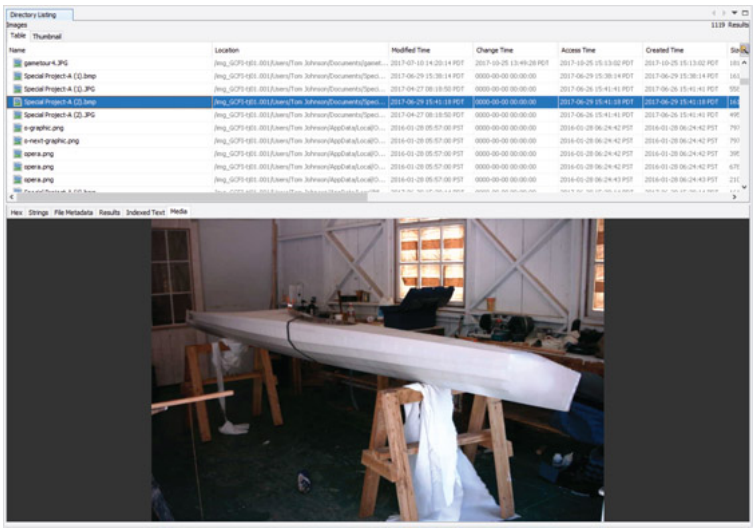
Source: www.sleuthkit.org

String content of the **Sample 1.eml** e-mail

3. To find this attached file, go to the Tree Viewer pane, and click to expand **Views, By Extension**, and **Images**. In the Result Viewer pane, click the **Table** tab, if necessary,

scroll down the Name column, and click the **Special Project-A (2).bmp** file (see Figure 14-9).

Figure 14-9.



Source: www.sleuthkit.org

The **Special Project-A (2).bmp** file

4. Right-click the **Special Project-A (2).bmp** file, point to **Tag Files**, and click **Tag and Comment**. In the Create Tag dialog box, click the **New Tag** Name button. In the New Tag section, type **Sample1-Attachment**, and then click **OK** twice.

5. Click **Generate Report** at the top. In the Generate Report window, click the **Results - HTML** option button in the Report Modules section, and then click **Next**. In the Configure Artifact Reports window, click the **Tagged Results** option button, click **Sample1-Attachment**, and then click **Finish**.

6. In the Result Viewer pane, right-click **Special Project-A (2).bmp** and click **Extract File(s)**. In the Save dialog box, navigate to and click your work folder, and then click **Save**.

7. Write a short memo to Ralph Benson stating that you have found the attached file for the Sample 1.eml e-mail. Attach the recovered file Special Project-A (2).bmp to your memo, turn the memo and attachment into your instructor, and leave Autopsy running for the next project.

Hands-On Project 14-5.

Ralph Benson says he also wants a copy of the legal notice that's displayed when Windows starts on Tom Johnson's computer. He needs this evidence to make sure that when Mr. Johnson logs on, he has been notified he has no right of privacy when using a Superior Bicycles computer. Mr. Benson wants this evidence added to a discovery request to get a forensics image of Jim Shu's computer. Mr. Johnson has been communicating with Mr. Shu, a former Superior Bicycles employee, about Special Project-A. To find and extract the Windows Registry Software folder in Autopsy, follow these steps:

1. Start a Web browser, go to http://accessdata.com/product-download/registry-viewer-1-8-0-5, and download the demo version of AccessData Registry Viewer. Install the software, and exit your Web browser. If you exited Autopsy, start Autopsy for Windows and open project **Proj1403**.

2. In the Tree Viewer pane, click to expand **Data Sources, GCFI-tj01.001, Windows, System32**, and **Config folder**. Scroll down, right-click the **SOFTWARE** file, and click

Extract File(s). In the Save dialog box, navigate to and click your work folder, and then click **Save**.

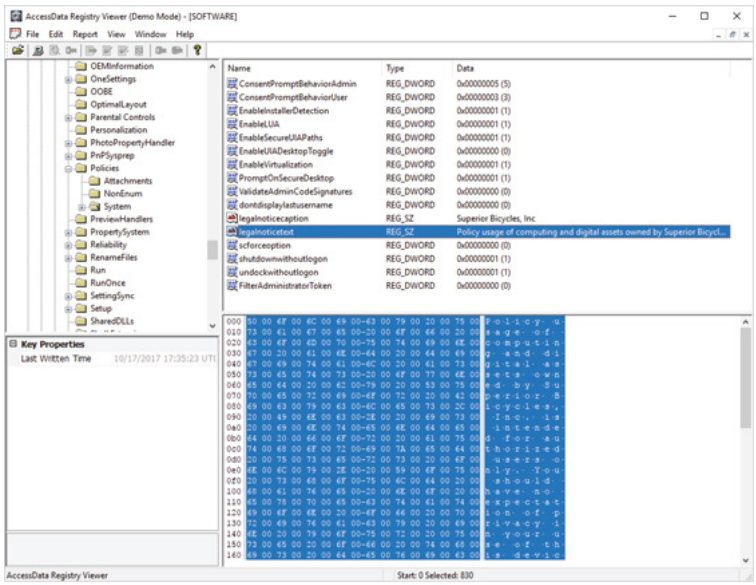
3. Click **Close Case**, and exit Autopsy.

To find and copy the legal notice in the Windows Registry SOFTWARE file, follow these steps:

1. Start AccessData Registry Viewer. If you get an error message, click **No** to run the program in demo mode, and click **OK** in the "No dongle found" message box. Click **File, Open** from the menu, navigate to your work folder, click **SOFTWARE**, and then click **Open**.

2. In the tree view on the left, scroll down and click to expand **Microsoft, Windows, CurrentVersion, Policies**, and **System**. In the Registry Key list at the upper right, click the **legalnoticetext** key (see Figure 14-10). Right-click the hexadecimal data at the lower right and click **Select All**. Next, right-click the highlighted hexadecimal data and click **Copy Hex**.

Figure 14-10.



Source: AccessData Group, Inc., www.accessdata.com

Viewing the content of the legalnoticetext key

3. In Windows, start a new document in Notepad, and click **Edit, Paste** from the menu. Click **File, Save As** from the menu, navigate to and click your work folder, and type **LegalNoticeText** in the File name text box. Click **Save**, and exit Notepad. Exit Registry Viewer.

4. After you've finished all the projects, write a formal report including all the memos you've written and the legal notice you found in this project. Address the report to Ralph Benson, General Counsel of Superior Bicycles, Inc., and include any observations about the contents of the e-mails. Submit the report to your instructor.

Case Projects

Case Project 14-1.

The county prosecutor has hired you to investigate a case in which the county treasurer has been accused of embezzlement. What additional resources, such as other experts, might you need to collect data for this investigation? Write a one-page paper outlining what resources you should consider to help you with the evidence collection process.

Case Project 14-2.

Your digital forensics company has been hired to verify the local police department's findings on a current case. Tension over the case is running high in the city. What do you need to ask the police investigator for, and what procedures should you follow? Consider what test you might use to validate the police department's findings. Write a one- to two-page report outlining what you need to do.

Case Project 14-3.

Your manager has asked you to research and recommend a writing guide that examiners in your digital forensics company can use for all official written reports. Conduct research on the Internet to find information about style manuals and technical and legal writing guides. You should also research writing guides from professional associations, such as the IEEE and the American Psychological Association. Write a two- to three-page report recommending a style manual or technical/legal writing guide for your company to use and explain the reasons for your recommendations. You might want to combine guidelines from different sources in coming up with recommendations for digital forensics reports.

Chapter 15. Expert Testimony in Digital Investigations

After reading this chapter and completing the exercises, you will be able to:

- Explain guidelines for giving testimony as a fact witness or an expert witness
- Describe guidelines for testifying in court
- Explain guidelines for testifying in depositions and hearings
- Describe procedures for preparing forensics evidence for testimony

This chapter explains the rules of evidence and procedure as they apply to testimony. You learn about the types of testimony—for trials, depositions, and hearings—and the difference between a fact witness and an expert witness. In addition, you learn how to avoid some common problems of testimony and learn some techniques you can use to increase the value of your testimony. This chapter also offers an example of how to prepare forensics evidence for testimony.

Preparing for Testimony

When cases go to trial or a hearing involving testimony, you as a forensics examiner can play one of two roles: a **fact witness** providing technical or scientific evidence or an **expert witness** . As a fact witness, you provide only the facts you have found in your investigation—any evidence that meets the relevance standard and is more probative than prejudicial. When you give technical or scientific testimony, you present this evidence and explain what it is and how it was obtained. You don't offer conclusions, only the facts and ordinary inferences based on that evidence. However, as an expert witness, you have opinions about what you have found or observed. You form these opinions from experience and deductive reasoning based on facts found during an investigation. In fact, it's your opinion that makes you an expert witness.

For either type of testimony, you need to prepare thoroughly. Establish communication early with your attorney. Before you start processing evidence, learn about the victim, the complainant, opposing experts or fact witnesses, and the opposing attorney as soon as possible. Learn the basic points of the dispute. As you learn about the case, take notes, but keep them in rough draft form and record only the facts, keeping your opinions to a minimum. (As explained in **Chapter 14**, any written material is subject to discovery, so use caution in what you put in written form.)

Note

Your attorney can give you specific guidelines in preparing for the case. Remember that as an expert witness, you work for the attorney, not the client (plaintiff or defendant), so if you discover negative findings, communicate them as soon as possible to your attorney.

As part of your preparation, you might want to review your own documentation and confirm your findings by corroborating them with other digital forensics professionals. Return to the notes you took during your investigation. If you're working with electronic notes, use care in storing them. In your analysis and reporting, develop and maintain a standard method of processing to minimize confusion and help you prepare for testimony later. Digital forensics is only now developing a peer review process. To get a peer review, often you have to search outside your region. Learn to take advantage of your professional network and request peer reviews to help support your findings.

You might also want to use the Internet to research opposing experts and try to find their strengths and weaknesses in previous testimony. Review their curriculum vitae, if possible, and see how they present themselves. To do otherwise is to go into battle without trying to know your opponent. Your attorney might be able to get copies of depositions they have given

in other cases, usually from the deposition banks mentioned in **Chapter 14**, but also from lectures, classes, and presentations that have been summarized or recorded and posted online. Some organizations of forensics investigators also maintain e-mail lists that you can use to query members about other expert witnesses.

Review the following questions when preparing your testimony:

- What's the client's overall theory of the case?
- What's my story of the case (the central facts relevant to my testimony)?
- What can I say with confidence?
- How does my opinion fit into the theory of the case?
- What's the scope of the case? Have I gone too far?
- Have I identified the client's needs for how my testimony fits into the overall theory of the case?

Documenting and Preparing Evidence

As emphasized in previous chapters, document your steps in gathering and preserving evidence to make sure they're repeatable, in case you're challenged. If your findings can't be repeated, they lose credibility as evidence. In addition, validate your tools and verify your evidence with hash algorithms to ensure its integrity. (Refer to **Chapter 9** for guidelines on using hash algorithms.) The following guidelines are also useful in ensuring the integrity of your evidence:

- If you need a checklist to analyze evidence, create it only for a specific case. Don't create a formal checklist of your procedures that's applied to all your cases or include such a checklist in your report. If opposing counsel gets this checklist through discovery, you might be challenged during cross-examination about inconsistencies in your performance if you deviated from the checklist.
- As a standard practice, collect evidence and record the tools you used in designated file folders or evidence containers. This method helps organize your evidence and tools. Follow a system to record where items are kept for each case and how documentation is stored.
- Remember that the chain of custody of evidence supports the integrity of your evidence; do whatever you can to prevent contamination of the evidence. You should also document any lapse or gap in evidence preservation or custody. Lapses and gaps don't necessarily result in evidence being inadmissible, but they might affect the weight given to the evidence.
- When collecting evidence, be careful not to get too little or too much information. For litigation, you're responsible for collecting only what's asked for, no more. In some circumstances, collecting and identifying evidence on facts unrelated to the case could cause problems for your attorney.
- Make sure you note the date and time of your forensic workstation when starting your analysis. If precise time is an issue, consider using an Internet clock, such as the one at www.time.gov or www.nist.gov/pml/div688/grp40/its.cfm (downloading nistime-32bit.exe), or an atomic clock to verify the accuracy of your workstation's clock. Many retailers, such as Walmart and Radio Shack, now sell atomic clocks.
- Keep only successful output when running analysis tools; don't keep previous runs, such as those missing necessary switch or output settings. Note that you used the tool, but it didn't generate results because of these missing settings.

- When searching for keyword results, rerun searches with well-defined keywords and search parameters. You might even want to state how they relate to the case, such as being business or personal names. Narrow the search to reduce false hits, and eliminate search results containing false-positive hits.
- When taking notes of your findings, keep them simple and specific to the investigation. You should avoid any personal comments so that you don't have to explain them to opposing counsel.
- When writing your report, list only the evidence that's relevant to the case; do not include unrelated findings.
- Define any procedures you use to conduct your analysis as scientific and conforming to your profession's standards. Listing textbooks, technical books, articles by recognized experts, and procedures from highly respected professional organizations that you relied on or referenced during your examination is a common way to prove your conformity with scientific and professional standards.

Reviewing Your Role as a Consulting Expert or an Expert Witness

Depending on your attorney's needs, you might give him or her just your opinion and technical expertise instead of testifying in court; this role is called a "consulting expert." If your role changes from consulting expert to expert witness later, however, your previous work as a consulting expert is subject to discovery by opposing counsel. For this reason, don't record conversations or phone calls.

When you appear in a federal court as an expert witness, Federal Rules of Civil Procedure (FRCP) 26 (2) (B) requires that you provide the following information:

- Other cases in which you have testified as an expert at a trial or in a deposition in the preceding four years
- Ten years of any published writings
- Previous compensation you received when giving testimony

In addition, the court can appoint its own expert witnesses. Court-appointed expert witnesses must be neutral in their opinions, and they must be knowledgeable in their field. As an expert hired by the defense or plaintiff, you need to evaluate the court's expert. Make sure you brief your attorney on your findings and opinion of the court's expert to help your attorney deal with any testimony the court-appointed expert provides.

Note

When approached to give expert testimony, find out whether you're the first one asked. If you aren't, find out why other experts might have been contacted but not retained.

Creating and Maintaining Your CV

Your **curriculum vitae (CV)** lists your education, training, and professional experience and is used to qualify your testimony. For forensics examiners, keeping this document updated and complete is crucial to supporting your role as an expert and showing that you're constantly enhancing your skills through training, teaching, and experience.

Your CV should describe tasks you've performed that define specific accomplishments and your basic and advanced skills. You should also list your general and professional education and professional training. If the list of training is extremely lengthy, use a heading such as "Selected Training Attended." Be sure to include coursework sponsored by government

agencies or organizations that train government agency personnel and courses sponsored or approved by professional associations, such as bar associations. Also, note any professional training you provided or contributed to. You must also include a testimony log that reflects every testimony you have given as an expert.

Make sure your CV reflects your professional background. Unlike a job resume, it should not be geared toward a specific trial. Most important, keep your CV current and date it for version control. If your CV is more than three months old, you probably need to update it to reflect new cases and additional training.

Note

Keep a separate list of books on your area of expertise that you've read, but don't include this list in your CV because it might suggest that you approve of everything written in these books.

Tip

For more information on how to write a CV, see www.testifyingtraining.com/write-curriculum-vitae-cv-expert-witness-work/ and www.academyofexperts.org/guidance/expert-witnesses/expert-witness-cv-template.

Preparing Technical Definitions

Before you testify in court, prepare definitions of technical concepts you can use when questioned by your attorney and the opposing attorney. Make sure you use your own words, and remember that you're explaining these concepts for a nontechnical audience. You might want to practice explaining your definitions and concepts with a person who has limited technical skills to confirm that your statements are understandable. You don't need to make the jury subject matter experts; you're simply explaining the general meaning of these terms. The following are examples of definitions to prepare ahead of time for your testimony:

- Digital forensics or computer forensics
- CRC-32, MD5, and SHA-1 hashing algorithms
- Image files and bit-stream copies
- File slack and unallocated (free) space
- File timestamps
- Computer log files
- Folder or directory
- Hardware
- Software
- Operating system

Preparing to Deal with the News Media

Some legal actions generate interest from the news media, but you should avoid contact with news media, especially during a case, for the following reasons:

- Your comments could harm the case and create a record that can be used against you.
- You have no control over the context of the information a journalist publishes.

- You can't rely on a journalist's promises of confidentiality. Journalists have been known to be aggressive in getting information, and their interests do not coincide with yours or your client's. Be on guard at all times because your comments could be interpreted in a manner that taints your impartiality in this case and future cases. Even after the case is resolved, avoid discussing details with the press.

If you're solicited for information or opinions by journalists (or anyone else), refrain from saying anything, and refer them to your client (the attorney who retained you). If you can't avoid a journalist, consult with your attorney and determine how to handle the situation. Plan to record any attempted interviews so that you have your own record of what occurred. (Note, however, that state laws on consent for recording vary.) This recording can be important if you're misquoted or quoted out of context. Reporters often look for a sensational sound bite or controversial quote.

Testifying in Court

Before you're called to testify in court, you should become familiar with the usual procedures followed during a trial. First, your attorney examines you about your qualifications to demonstrate to the court that you're competent as an expert witness or a fact witness. The opposing counsel might then cross-examine you on your qualifications (perhaps in an attempt to discredit you). Next, your attorney guides you through your testimony, and then opposing counsel can cross-examine you on your testimony. Your attorney might then have an opportunity for redirect examination of material addressed in cross-examination. After your testimony, you might be called back to update your testimony, or you might be called as a rebuttal witness.

Understanding the Trial Process

The typical order of trial proceedings, whether civil or criminal, is as follows:

- *Motion in limine*—A pretrial motion to exclude or limit the use of certain evidence because its potential to prejudice the jury would exceed its probative value. Effectively, this motion is a written list of objections to certain testimony or exhibits. It allows the judge to decide whether certain evidence should be admitted when the jury isn't present. Some evidence is so prejudicial that just the jury knowing it exists is enough to damage the case. In this situation, getting a ruling on the evidence before trial is crucial.
- *Impaneling the jury*—This process includes voir dire of venireman (questioning potential jurors to see whether they're qualified), strikes (rejecting potential jurors), and seating of jurors.
- *Opening statements*—Both attorneys provide an overview of the case, with the plaintiff's attorney going first.
- *Plaintiff*—The plaintiff's attorney presents the case.
- *Defense*—The defense's attorney presents the case.
- *Rebuttal*—Rebuttal from both the plaintiff's and defense's attorneys is an optional phase of the trial. Generally, it's allowed to cover an issue raised during cross-examination of a witness.
- *Closing arguments*—Statements that organize the evidence and state the applicable law. The plaintiff's attorney goes first and gets a rebuttal opportunity at the end, which should be limited to issues raised by the defense's attorney.
- *Jury instructions*—The attorneys propose instructions to the jury on how to consider the evidence, and then the judge approves or disapproves; if the instructions are approved, the judge reads them to the jury.

Providing Qualifications for Your Testimony

During the qualification phase of your testimony, your attorney asks questions to elicit the qualifications that make you an expert witness. This qualification phase is called **voir dire** (in French, literally "to see, to say"). Typically, your attorney guides you through your CV. The amount of detail in this examination depends on several factors, but they all relate to how much advantage the attorney sees in your qualifications. After your attorney has completed this examination, he or she asks the court to accept you as an expert on digital forensics. However, opposing counsel might object and is allowed to examine you, too; usually, cross-examination happens only if the opposing attorney thinks there's something to gain from it.

Tip

If you know that the opposing expert witness taught or took a course that used a publication you wrote or co-authored, tell your attorney about it. He could emphasize that you're the author and examine the opposing witness on this fact to give you more credibility as a recognized expert in the field.

The following example is a short direct-examination voir dire:

Q: Please state your name and spell your last name for the record.

A: Wilma Nokiki, N-O-K-I-K-I.

Q: What is your profession?

A: I am a digital forensics examiner.

Q: How long have you been a digital forensics examiner?

A: Twelve years.

Q: Where are you currently employed?

A: I am currently employed by IT Forensics, Incorporated, of Seattle, Washington.

Q: How long have you been with IT Forensics?

A: Eight years.

Q: What is your title with IT Forensics?

A: I am a senior case manager.

Q: What training have you received in digital forensics?

A: I have been trained at the Federal Law Enforcement Training Center in 2000, I trained with NTI in 1996, and I have received training from the International Association of Computer Investigative Specialists since 1999, most recently on large disk acquisitions and network monitoring. I have taken dozens of short courses with many different investigative training organizations over the past fifteen years.

Q: Where have you been an instructor?

A: I have taught classes on digital forensics at City College, Highline Community College, Bellevue Community College, and Lake Washington Technical College. I taught the digital forensics instructors for the state of Washington in 2012. I have made many shorter presentations, including continuing legal education programs approved by the Washington State Bar Association.

Q: Have you been published?

A: Yes, I am co-author of the college textbook Digital Investigations and Forensics.

Q: Have you testified previously?

A: Yes, I have most recently in United States versus Smith. A detailed list of occasions when I have testified is in my CV.

Plaintiff's Attorney: Your witness.

Defense Attorney: No questions for the witness.

Plaintiff's Attorney: Your Honor, Plaintiff would move that Ms. Nokiki be accepted as an expert witness on digital forensics.

Judge: Any objection, Ms. Defense Attorney?

Defense Attorney: No objection, Your Honor.

Judge: Ms. Nokiki is accepted as an expert witness on digital forensics. You may proceed, Mr. Plaintiff's Attorney.

If you have especially strong qualifications and have been qualified as an expert on several occasions, opposing counsel might offer to accept you as an expert without your qualifications being stated formally. Generally, your attorney bypasses that offer in favor of impressing the jury with your qualifications.

General Guidelines on Testifying

Whether you're serving as an expert witness or a fact witness, be professional and polite when presenting yourself to any attorney or the court. Before the trial, try to learn the jury, judge, and other attorneys' level of knowledge on and attitudes toward computers and technology. Talk to local attorneys to learn more about the type of people typically serving on local juries. With this knowledge, you can gauge your presentation to your audience's educational level, and incorporate appropriate analogies into your explanations. Remember that the judge is well educated but not necessarily in the field of digital evidence. Jurors typically average around 12 years of education and an eighth-grade reading level. The attorneys might have a thorough background in the field, but you're the expert with experience. You could also be dealing with an arbiter or mediator who may or may not have a background in digital forensics.

There are two responses you should be prepared to use often as a witness. First, if asked a question you can't answer, respond by saying, "That is beyond the scope of my expertise" or "I was not asked to investigate that." These statements make it clear that you understand your limitations. You won't seem less of an expert for knowing and expressing your limitations. If anything, acknowledging your limitations enhances your standing with a jury. Second, if you don't understand a question or find it confusing, simply say, "Can you please rephrase the question?" Typically, this response gets the attorney to reorganize the question and is one method you can use to control the pace and direction of the examination. If the question is stated awkwardly or you aren't sure of the intent, ask the attorney for clarification.

If opposing counsel tries to reframe your answer in a way that you don't believe is accurate, reject his restatement by saying "No, that isn't what I said," and then restate your position accurately, starting with "What I said was." Be respectful and even pleasant, but be firm.

Another aspect of acknowledging your limitations is making sure you avoid overstating opinions. Part of what you have to deliver to the jury is a person they can trust to help them figure out something that's beyond their expertise. Overstating an opinion creates the potential for the jury to mistrust or doubt you; like a teacher, you should admit your limitations and the limitations of your results.

Your delivery is an important part of how you answer questions and affects the impact you have on the jury. The following list offers some general guidelines on delivery and presentation:

- Always acknowledge the jury and direct your testimony to them, using an enthusiastic, sincere tone to keep the jury interested in what you have to say. When an attorney or the judge asks you a question, turn toward the questioner, and then turn back to the jury to give the answer.
- If a microphone is present, place it 6 to 8 inches from you, and remember to speak loudly and clearly so that the jury can hear and understand you.
- Use simple, direct language to help the jury understand you. For example, use "test" instead of "analyze," as in "I ran a test on the files I found." Also, make sure you use specific, articulate speech when speaking; for clarity, avoid contractions and slang, unless you're quoting a fact related to the case.
- Avoid humor. What one person thinks is funny, another won't. In addition, limit your responses to what you perceive as attempts at humor from anybody else.
- Build repetition into your explanations and descriptions for the jury.
- Use chronological order to describe events when testifying, and use hand gestures to help the audience understand what you're emphasizing. For example, point to graphics while talking. (Graphics are discussed more later in "Using Graphics During Testimony.")
- If you're using technical terms, identify and define these terms for the jury, using analogies and graphics as appropriate. List any important technical elements, showing how you verified and validated each element.
- When giving an opinion, cite the source of the evidence the opinion is based on. Then express your opinion and explain your methodology—how you arrived at your opinion.
- If the witness chair is adjustable, make sure the height is comfortable, and turn the chair so that it faces the jury.
- To enhance your image with the jury, dress in a manner conforming to the community's dress code for business professionals, or dress like the attorneys in the case. If your testimony is being videotaped, avoid fine stripes in suits or ties because they can generate a strobing effect in video recordings under artificial light. Men should wear conservative ties with a base color of red; women should wear suits in conservative colors or a dress that allows freedom of movement.
- Don't memorize your testimony; you should strive for a natural, extemporaneous tone. Also, make sure you have alternative ways to describe or explain key facts.
- For direct examinations, state your opinion, identify evidence to support your opinion, explain the method you used to arrive at your opinion from your analysis, and then restate your opinion.

As mentioned, have definitions and explanations aimed at a nontechnical audience ready for technical terms you must use in your testimony. Learn how to describe the tools you use as a standardized process for your work. Make sure you're knowledgeable about the fallibility of digital forensics so that you can resist counterattacks from opposing counsel. Lengthy explanations might be good for some jury cases but not for others, so seek your attorney's opinion.

Prepare your testimony with the attorney who hired you. The following are specific questions you should prepare for:

- How is data (or evidence) stored on a hard drive?

- What is an image or a bit-stream copy of a drive?
- How is deleted data recovered from a drive?
- What are Windows temporary files, and how are they related to data or evidence?
- What are system or network log files?

Using Graphics During Testimony

Graphical exhibits, such as charts and tables, illustrate and clarify your findings. As a general rule, memory retention is much weaker for audio material and stronger for visual material. Therefore, oral testimony supported by graphical presentations is an effective way to impart information and help your listeners retain it. Your exhibits must be clear and easy to understand. Graphics should be big, bold, and simple so that the jury can see them easily, and consider factors such as glare and adequate contrast to ensure easy visibility. If necessary, make smaller copies of graphics for jurors so that they can see details better.

The goal of using graphics is to provide information the jury needs to know (such as how hardware and software work), an explanation of your findings, and the role the evidence plays in the case. Make sure each graphic conveys only one concept or point; don't try to include too much information in a single graphic. If you're using graphics to explain a complex technical concept or procedure, use two or more graphics, with the first graphic providing an overview.

Note

Don't include vendor logos on your charts, and don't use charts created by someone else, unless you commissioned someone to create them or have documented permission to use them. In this way, you can avoid possible copyright issues. Another advantage of creating your own charts is you can make sure you're comfortable with—and can explain—their content.

Review all graphics with your attorney before trial, and make sure you've practiced using them so that you appear comfortable and confident. In most courts, you need at least three extra copies of your graphics: one for your attorney, one for the opposing attorney, and one for the judge. However, it's the attorney's responsibility to have graphical exhibits admitted into evidence.

Courtrooms are becoming more audiovisual capable, and you might be able to use a projector system. If one is available, discuss using it with your attorney. You might also talk about the possibility of giving jurors copies of your presentation on removable storage media, such as a CD or a USB drive.

Make sure the jury can see your graphics, and face the jury during your presentation. If your graphics haven't been placed near the jury box, ask the judge if you can move them so that the jury can see them better. When you're talking about specific areas of an illustration, use a pointer to direct jurors' attention to details. You can also use your hands to help emphasize certain information or direct attention to specific points. Make sure any gestures are above the waist so that the jury can see them. If an attorney asks you questions as you explain the graphics, face the jury and answer the questions in full sentences.

Tip

When you're standing in front of the jury, leave your jacket unbuttoned and keep your elbows bent to show that you're comfortable, confident, and at ease.

Avoiding Testimony Problems

Although you should recognize when conflict-of-interest issues apply to your case and discuss any concerns with the attorney who hires you, be aware of a practice called **conflicting out** . It's an attempt by opposing attorneys to prevent you from serving on an important case and is most common in the private sector when you work as an independent consultant. Opposing attorneys might call to discuss the case with you and then claim you can't testify because of a conflict of interest caused by you discussing the case with another attorney besides the one who hired you. As a result, you might be excluded from working for an attorney needing your services. (The issue of conflict is raised by motion after witness lists are exchanged.)

In addition, avoid agreeing to review a case unless you're under contract with that person. Also, avoid conversations with opposing attorneys—there's no such thing as an "off the record" conversation with opposing attorneys after you have been retained; refer them to the attorney who retained you. Have a fee agreement for your case review ready to e-mail or fax to opposing attorneys to protect yourself from this practice; this agreement serves as proof that they didn't want to retain you. If you aren't retained, you're in a better position to collect a fee for the service you did provide, and it deters them from attempting to manufacture a conflict issue to disqualify you later as an expert witness.

Early in direct examination, your attorney should ask whether you were hired to perform an analysis and testify. He or she might ask how much you charged for your services and whether you have already been paid; you should receive payment before testifying. If you haven't been paid, it might seem that you have a contingent interest in the litigation—that your payment depends on the resolution of the case. Fees and payment schedules are appropriate subjects for examination, although the judge might limit these questions. If your attorney doesn't ask you questions about payment, the opposing counsel could examine you on it in an effort to discredit you or lessen your credibility as a witness. However, the opposing counsel knows that this tactic might be used on his expert witnesses, too, so he might touch on the subject but not dwell on it, unless you say you haven't been paid completely.

When you're testifying, don't talk to anyone during court recess. If the opposing attorney sees you having a conversation with anyone, including the attorney who retained you, he or she could cross-examine you again and demand that you explain and repeat your conversation. However, be aware that your attorney might want to notify you of updates during breaks, so make sure you conduct any conferences in a private setting. If a juror approaches and says anything to you, decline to talk with him or her and promptly report the contact to the attorney who retained you. This event must be reported to the court.

Understanding Prosecutorial Misconduct

If you're working for a prosecutor in a criminal case and believe you have found exculpatory evidence (evidence that exonerates or diminishes the defendant's liability), you have an obligation to ensure that the evidence isn't concealed. Initially, you should report the evidence (emphasizing its exculpatory nature) to the prosecutor handling the case. Be sure you document communicating your concern to the prosecutor. If this information isn't disclosed to the defense attorney in a reasonable time, you can report it to the prosecutor's supervisor. Be sure to document this communication, too. Documentation of each attempt to induce disclosure and your reasoning is important to protect your reputation.

If these efforts still don't result in disclosure, you can report the lack of disclosure to the judge. Be sure you have documented your attempts to bring the matter to the prosecutor's attention before bringing it to the judge. Don't communicate directly with the defense attorney; reporting evidence to the judge fulfills your obligation. The rules that apply to defense expert witnesses are different.

Testifying During Direct Examination

You provide direct testimony when you answer questions from the attorney who hired you. This direct examination is the most important part of testimony at a trial. Cross-examination is

not as important, even if the opposing attorney is attempting to discredit you.

When preparing your testimony for direct examination, keep some guidelines and techniques in mind. You should work with your attorney to get the right language that communicates your message to the jury effectively. Also, your attorney might advise you to be wary of your inclination to be helpful. This trait is natural, but it can hurt your testimony. You shouldn't volunteer any information or be overly friendly (or hostile) to the opposing attorney.

Review the examination plan your attorney has prepared to see whether you can make any suggestions for improvement; this plan is structured to ensure that questions elicit relevant evidence during direct examination. Make sure you've prepared a clear overview of your findings and have a systematic and easy-to-follow plan for describing your evidence-collection methods. Practice testifying with your graphics so that you're comfortable using them.

Your attorney might also help you develop a theme to follow when presenting your testimony, but make sure you use your own words when answering questions. Generally, the best approach your attorney can take in direct examination is to ask you open-ended questions and let you give your testimony.

In addition, make sure you know the following terms before giving testimony because your attorney will likely use them during the direct examination:

- *Independent recollection*—Information you know about this case and others without being prompted
- *Customary practice*—Procedures that are traditionally followed in similar cases
- *Documentation of the case*—The written records you have maintained

When your attorney questions you about your background and qualifications, your answers should show why you are an expert able to give testimony. Give answers that emphasize your factual findings and opinions. Remember to tailor your language to the jury's educational level, and try to strike a balance between technical language and layperson language when describing complex matters.

Avoid vagueness in your wording choices, too. For example, don't use expressions such as "very large" or "a long time." The meaning of these expressions varies, depending on what they're compared with, and this comparison might be different for every juror. Use precise numbers and units of measurement, and if relevant, cite numbers' statistical position, relationship to the mean, or an expected value or range.

When you're using graphics in a presentation, keep in mind that you're instructing the jury in what you did to collect evidence, so follow some of the same guidelines teachers use in a classroom to make sure the jury understands your explanations.

Testifying During Cross-Examination

When answering questions from the opposing attorney, use your own words. Keep in mind that certain words have additional meanings that an opposing attorney can exploit. For example, the word "suspicious" is more value laden than the more neutral "concerned."

Be aware of leading questions from the opposing attorney, too. An ambiguous question—such as "Isn't it true that forensics experts always destroy their handwritten notes?,"—is an attempt to lead you to say something that could be construed as wrong. (The answer to that question should be "I don't know.") Leading questions call for yes or no answers and are sometimes referred to as "setup questions"—setting you up for a response that could be damaging to your client's case. They're often phrased in a complex structure, designed to limit your freedom in answering. Getting to the real question opposing counsel is asking might take many questions.

If opposing attorneys ask you a question such as "Did you use more than one tool to verify the evidence?" they're checking to make sure you validated the findings from one tool by using

another tool. Opposing attorneys often ask the following questions, too:

- What tools did you use, and what are their known problems or weaknesses?
- Are the tools you used reliable? Are they consistent, and do they produce the same results?
- Have other professionals called on you as a consultant on how to use tools?
- Do you keep up with the latest technologies used in digital forensics, such as by reading journal articles?

During examinations, lawyers aren't supposed to ask another question until you have finished answering the current question. However, the opposing counsel sometimes uses rapid-fire questions during cross-examination that are meant to throw you off. Taking a moment to turn toward the jury before you answer gives you more control over the timing and speed of the opposing attorney's examination. Even though your attorney should object by saying, "Counsel has not allowed the witness to answer the question," don't be afraid to regroup and restate your answers if you get confused during your testimony. Jurors will sympathize because often they're confused by the opposing attorney's questions, too.

If the opposing attorney declares that you aren't answering the questions, she could be making an attempt to get you to change your testimony. You aren't giving the answer she wants, or she's attempting to get you to say something that contradicts part of your previous testimony. Don't take this attempt personally, but think carefully about what the opposing attorney is trying to do.

During a jury trial, keep a comfortable level of eye contact with the jury. You might find yourself competing with the opposing attorney, but do your best to keep the jury's attention on you during your testimony. As the opposing attorney asks you questions, avoid strict yes or no answers, if possible; add facts to clarify your answer, when appropriate, before the opposing attorney can hit you with a "killer question." This type of question, contrived based on a change in a basic underlying fact, is one that you seemingly can't answer or deny. It can derail your testimony and your client's case; however, the judge will usually support you in stating conditions or limits. The most effective process for success in cross-examination is to establish the hypothetical facts that are the basis of your opinion. Hypothetical facts should be based on evidence presented at trial as well as stipulations and standard facts that all professional digital forensics examiners rely on, such as the fact that a kilobyte is composed of 1024 bytes.

On some occasions, you have to bring in another examiner or agency to collect more evidence because of the nature of the case. As an examiner working on a civil case, for example, sometimes you need to hand off evidence you have gathered to another company's security group or a government agency to develop the case further. Consult with your supervisor or the party who retained you to determine the correct procedure.

Sometimes opposing attorneys ask several questions inside one question; this practice is called a compound question, and your attorney should object to it. If your attorney doesn't, you can respond by saying, "Could you please break your last question into separate questions?" Another tactic opposing attorneys use in cross-examinations is to make a speech and phrase it as a question. You have no obligation to respond to statements by opposing counsel. The judge usually catches this error, and your attorney should also object. Other methods opposing attorneys use to challenge your credibility are putting words in your mouth and summarizing your testimony to fit their needs, creating assumptions or speculation, and controlling the pace of your testimony. Other tactics are stating minor inconsistencies that cause you to make conflicting statements and encouraging you to volunteer information.

Your response to cross-examination tactics should challenge the opposing attorney to be more sensible, a response that often plays well with juries. Take your time answering questions. Be

thoughtful, professional, and courteous in your responses. The more patient you are during cross-examination, the better you'll weather any possible attacks. If the opposing attorney becomes assertive or upset with your testimony, be as professional and courteous as possible. If he continues to lose control, staying calm and professional strengthens your image by comparison. Responding to a question with a sentence that communicates limitations or qualifications might be important, if a simple yes or no doesn't answer the question completely and accurately. If you need to have your attorney expand a line of questions on redirect, have an agreed-on expression you can use to signal him, such as "This question requires a more complex answer, but the short answer is yes (or no)."

In addition to direct examination and cross-examination, most jurisdictions now allow the judge and jurors to ask questions. These questions are subject to the same rules of evidence that any other question is. Attorneys can object to these questions but generally won't unless they are an especially serious breach of the rules, such as a question that was specifically excluded in a motion in limine. Answering a question from the judge or a juror should be viewed as an opportunity. As a witness, you usually have to guess at what's important to the judge and jury, but you don't when responding to a question directly from them.

Many factors contribute to your stress when testifying, including the judge, the attorneys, the jury, and the feeling of losing control. Don't think you're responsible for the outcome. If you make a mistake, correct it, and get back on track with your testimony. You should avoid showing that you have lost control, such as by the following behaviors:

- Being argumentative when being badgered by the opposing attorney or being nervous about testifying
- Having poor listening skills or defensive body language, such as crossing your arms
- Being too talkative or talking too fast when answering questions
- Being too technical for an ordinary juror to understand your testimony
- Acting surprised and unprepared to respond when presented with unknown or new information

Never have unrealistically high self-expectations when testifying; everyone makes mistakes. Who controls the testimony is the most important part for the attorney, in both direct examination and cross-examination. The key to successful cross-examination is to continue selling yourself to the jury, no matter how much the opposing attorney tries to discredit you or your testimony. In addition, remember that for every expert witness, there's a first time testifying. Good technical credentials and related experience are the most effective defense against cross-examination voir dire when testifying. You should also remember that the number of times you've testified isn't a condition of qualifying as an expert witness.

Preparing for a Deposition or Hearing

A **deposition** differs from trial testimony because there's no jury or judge. Both attorneys are present and ask you questions. (With current technology, the concept of "present" is expanding to include "virtually present.") The purpose of the deposition is for the opposing attorney to preview your testimony before trial. The attorney who requests a deposition usually establishes its location, which might be in his or her office or your forensics laboratory.

There are two types of depositions: discovery and testimony preservation. A **discovery deposition** is part of the discovery process for trial. The opposing attorney who requested the deposition often conducts the equivalent of a direct examination and a cross-examination. Your attorney usually asks only questions needed to clarify a point that could be subject to misinterpretation in your direct testimony. Although a discovery deposition can be video recorded, a written transcript is more common and is required in addition to the video

recording. If the deposition is video recorded, court rules generally require a longer notice period to schedule it than a stenographically recorded one.

A **testimony preservation deposition** is usually requested by your client to preserve your testimony in case of schedule conflicts or health problems. These depositions are often video recorded in addition to the written transcript, and your testimony is entered by playing the video recording for the jury. In some cases, you can set the deposition at your laboratory or have lab facilities available, which can make it easier to conduct demonstrations and produce better testimony. This deposition follows the pattern of trial testimony, with your attorney calling you as a witness and conducting a direct examination, opposing counsel conducting cross-examination, and the attorneys conducting redirect and recross examination, if necessary. The judge rules on objections and, based on objections that are sustained, decides which portions of the testimony are omitted from the copy presented to the jury.

Guidelines for Testifying at Depositions

Often attorneys are more combative during discovery depositions than they are during trial (or video-recorded depositions). For this reason, a deposition can be more stressful than trial testimony. Therefore, strive to stay calm and convey a relaxed, confident appearance during a deposition. For example, try to keep your hands on top of the table, and make sure your chair is at the right height to avoid sitting below the opposing attorney's eye level. Maintain a professional demeanor and try not to be influenced by the opposing attorney's tone, expression, or tactics. Learn the opposing attorney's name before the deposition and include it in your responses to project a sense of equality in position between you and the opposing attorney. Look the opposing attorney directly in the eyes, even if she attempts to avoid eye contact.

Remember that during a deposition, opposing attorneys use all the techniques available to them at trial, so keep the guidelines for testimony in mind when answering questions, and be assertive in your responses. If you're particularly concerned about the deposition, ask your attorney to record a practice session, and then evaluate your performance. Here are some general rules to follow during depositions:

- Be professional and polite.
- Use facts when describing your opinion.
- Understand that being deposed in a discovery deposition is an unnatural process; it's intended to get you to make mistakes.

If you prepared a written report, the opposing attorney might attempt to use it against you by leading you to testify contrary to what you had previously written. If the attorney is concealing the report or any other document from your view, ask to see the document. When the opposing attorney asks you about something specific in your written report, ask what page number he's referring to. If you don't have the report in your hands, you can ask to review it.

If your attorney objects to a question from the opposing attorney, pause and think of what direction your attorney might want you to go in your answer. Keep your answers short and simple. Strive for a relaxed, friendly demeanor, especially if you're being recorded. To gain time and control, ask the opposing attorney questions to clarify what he's asking for, such as asking him to repeat the question.

Be prepared at the end of a deposition to spell any specialized or technical words you used. To aid court reporters, give them a list of technical or scientific words you use often, including definitions and correct spellings.

Recognizing Deposition Problems

Discuss any potential problems with your attorney before the deposition. Identify anything that might affect your client negatively and could be used by opposing counsel. If you don't disclose this information, the opposing attorney might be aware of it and use it against you in court. Be prepared to defend yourself if there are problems. The following guidelines can also help you avoid problems during depositions:

- Avoid omitting information in your testimony; omissions can cause major problems. Although you don't have to volunteer more information than an attorney asks for, make sure you're telling the truth at all times.
- To respond to difficult questions that could jeopardize your client's case, pause before answering, allowing your attorney to object before you answer.
- To avoid having the opposing attorney box you into a corner or lead you to contradict previous statements, answer only the questions you're asked, using short answers that are narrow in scope when possible.
- Realize that excessively detailed questions from opposing counsel are an attempt to get you to contradict yourself. Avoid trying to educate the opposing attorney, especially if the questions seem to be beyond the scope of your expertise or the questions you were retained to answer. Feel free to give answers such as "I don't know" or "I don't understand."
- When asked whether you know about an opposing fact or expert witness, your response should be as professional as possible. A good standard answer is "I have heard Mr. Smith is a competent examiner, but I have not reviewed the body of his work." If you have specific and verifiable information that's damaging to the opposing expert's reputation, you can note it, but do it in an understated manner. This technique emphasizes your professional demeanor, especially if you have negative information about the opposing expert's skills or competency.
- Keep in mind that you can correct any minor errors you make during your examination by referring back to the error and correcting it. You also have an opportunity after the deposition, but you have to ask for it. You'll be asked at the end of the deposition if you waive signature; if you want to review the deposition, you shouldn't waive signature because you then get a chance to review, make corrections on the corrections page, and sign the deposition.
- Discovery deposition testimony generally doesn't make it to the jury, except for the purpose of showing previous inconsistent testimony by the witness. This process is called "publishing the deposition." The witness can then be examined about inconsistent testimony in the deposition.

Guidelines for Testifying at Hearings

Testifying at a hearing is generally comparable to testifying at a trial, so follow the same general guidelines you would for courtroom testimony. A hearing can be before an administrative agency or a legislative body or in a court (when it typically addresses specific issues). An administrative or legislative hearing generally addresses the agency's or committee's subject matter and seeks evidence in your testimony on a subject for which it's contemplating making a rule or legislation. A presiding officer or committee chairperson is present, and the format of questioning depends on the agency's or committee's rules and the purpose of the hearing. Often administrative or legislative hearings are related to events that previously resulted in litigation. Testifying at administrative hearings isn't as common as testifying in depositions or at trials.

Note

The federal government has thousands of administrative agencies, and states often have hundreds of administrative agencies.

A judicial hearing is held in court to determine the admissibility of certain evidence before trial. No jury is present, but evidentiary suppression hearings are usually held early in the case to determine whether a criminal case moves forward or is dismissed. Generally, they focus more on your procedure in obtaining and preserving evidence than on the substance of the evidence or your opinion. They can also include the basis or authority (warrant or probable cause) for you conducting the examination. In most criminal cases, the defense attorney seeks to suppress any evidence for which there's an arguable basis for rejection.

Note

For more information and examples of how to give expert witness testimony, see www.youtube.com/watch?v=yGughpPXbt4 for depositions and www.youtube.com/results?search_query=expert+witness+testimony+in+court for hearings.

Preparing Forensics Evidence for Testimony

In this section, you learn the steps for extracting information to be presented to a court. You also learn how to prepare to testify on digital evidence you have collected. You should be ready to answer specific questions from your attorney as well as opposing counsel.

Based on your analysis of Tom Johnson's computer in **Chapter 14**, Ralph Benson, the general counsel at Superior Bicycles, Inc., has obtained an electronic discovery demand and received a forensic disk image of former employee Jim Shu's personal computer. Mr. Benson sent you the forensic disk image and instructed you to search for all e-mails from Mr. Johnson. The e-mail accounts to look for are 1060waddisonst@gmx.com and jtom88917@gmail.com. After you have collected the e-mails, Mr. Benson wants you to prepare to testify at a deposition hearing about their contents. He also stated that you need to testify on how you extracted the e-mails and how the chain of custody was maintained. Another examiner has already created a forensic image of Mr. Shu's computer, and a paralegal gave you this file, ChInchp15-01.001.

Note

Before beginning the following activity, create a folder called *Work*\Chap15\Chapter folder (referred to as your "work folder" in steps).

To perform this task, you use Autopsy for Windows to extract and examine e-mails in the forensic image GCFI-js01.001. Follow these steps:

1. Download Ch15Proj01.exe from this chapter's downloads section of the student companion site for this book. In File Explorer, double-click this file and click **Extract** to extract it to your work folder.
2. Start Autopsy for Windows. Click the **Create New Case** button. In the New Case Information window, enter **InChap15** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**.
3. In the Additional Information window, type **InChap15** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.
4. In the Select Data Source window, click the **Browse** button next to the "Browse for an image file" text box, navigate to your work folder and click the GCFI-js01.001 file, and

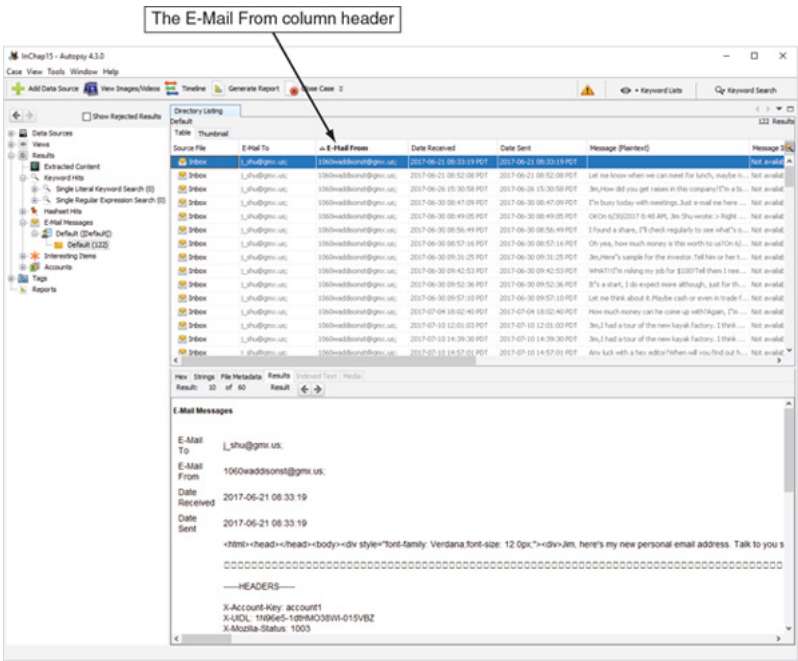
click **Open** and then **Next**.

5 In the Configure Ingest Modules window, click **Deselect All**, click the **Email Parser** check box, and click **Next** and then **Finish**.

6 When Autopsy finishes its analysis, go to the Tree Viewer pane, and click to expand **E-Mail Messages**, **Default (Default)**, and **Default**.

7 In the Result Viewer pane, click the **E-Mail From** column header to sort the e-messages by e-mail address in ascending order (see Figure 15-1).

Figure 15-1.



Source: www.sleuthkit.org

E-mails sorted by sender

8 In the Result Viewer pane, Ctrl+click all e-mails from **1060waddisonst@gmx.us** and **jtom88917@gmail.com**. Right-click this selection, point to **Tag Results**, and click **Tag and Comments**. In the Create Tag dialog box, click the **New Tag Name** button, type **Message-from-TJohnson** in the Tag Name text box, and click **OK** twice.

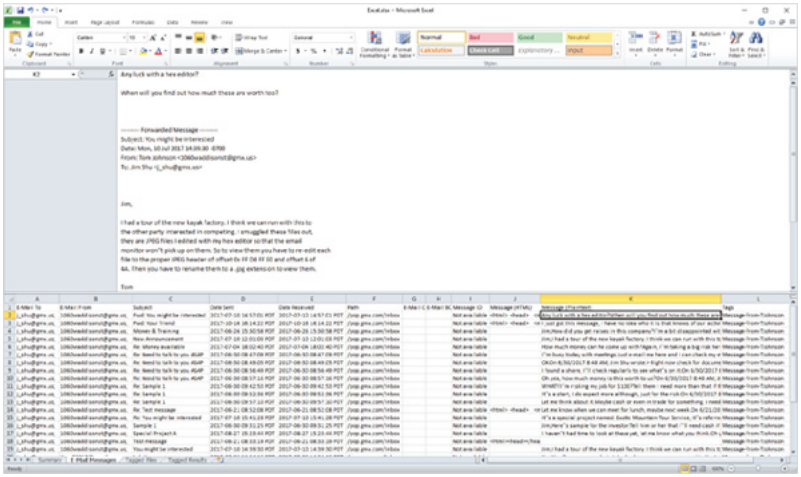
9 Click **Generate Report**. In the Generate Report window, click the **Results - Excel** option button in the Report Modules section, and then click **Next**. In the Configure Artifacts Report window, click the **Tagged Results** button, click **Select All**, and then click **Finish**.

10 In the Report Generation Progress Complete window, click the **Results - Excel** link to open the report. Leave Excel running for the next steps.

To examine the contents of the Excel report, follow these steps:

1 In Excel, click the **E-Mail Messages** tab, and then adjust the column widths and formula bar height so that you can view the cells' contents better (see Figure 15-2).

Figure 15-2.



The Excel spreadsheet of Jim Shu's e-mails

2. Click cells **K2** through **K27** and read the content of each e-mail.
3. After reading all e-mails, save this spreadsheet as **Ch15Inchp-TJohnson-msg.xlsx** , and exit Autopsy and Excel.

Preparing a Defense of Your Evidence-Collection Methods

To prepare for testimony, you should prepare answers for questions on what steps you took to extract e-mails from the image of Jim Shu's computer. You might also be asked to explain specific features of the computer, OS, and applications (such as Mozilla Thunderbird or Microsoft Outlook) and explain how these applications and digital forensics tools work.

Ms. Gallagher, from the law firm CR PLLC, plans to ask you the following questions when you're called to testify. Prepare your answers, referring to these examples as guidelines, so that you can answer the questions with confidence and professionalism.

Question 1: How did you find e-mails in the image of Mr. Shu's computer?

Answer 1: I used Sleuth Kit's Autopsy for Windows to access and search the GCFI-js01.001 image of Mr. Shu's computer.

Question 2: How did you search for e-mails on Mr. Shu's computer?

Answer 2: In Autopsy, I used the Email Parser ingest module to find all Mr. Shu's e-mails. I then sorted the received e-mails and found all from Mr. Johnson.

Question 3: After you found these e-mails, what did you do?

Answer 3: I used Autopsy to extract specific data items—in this case, e-mails—and copy them to a report. Then I used Autopsy to create an Excel spreadsheet of the extracted data.

Question 4: What's an image file?

Answer 4: An image file is a copy of a computer's disk drive. It copies all areas of a disk drive, including deleted files.

Question 5: When did you perform this examination?

Answer 5: I performed this examination on November 15, 2017, at about 2:00 p.m.

Question 6: How many e-mails on Mr. Shu's computer were from Mr. Johnson?

Answer 6: I found twenty-six e-mails.

Question 7: After finishing your examination, what did you do?

Answer 7: I sent the case report with the spreadsheet data to Mr. Benson, the general counsel. I then closed Autopsy and secured the external disk drive containing the forensic image of Mr. Shu's computer in the evidence locker.

Chapter Summary

- When cases go to trial, you as the forensics expert play one of two roles: a fact witness or an expert witness. As a fact witness, you're providing only the facts you discovered in your investigation. However, as an expert witness, you have opinions about what you have observed. In fact, it's your opinion that makes you an expert witness.
- If you're called as a fact witness or an expert witness in a digital forensics case, you need to prepare for your testimony thoroughly. Establish communication early with your attorney. Substantiate your findings with your own documentation and by collaborating with other digital forensics professionals.
- When you're called to testify in court, your attorney examines you on your qualifications to establish your competency as an expert witness or a fact witness. Opposing counsel might attempt to discredit you based on your past record. Your attorney then leads you through the evidence, followed by the opposing counsel cross-examining you. Redirect examinations and recross examinations of limited scope might follow.
- Make sure you're prepared for questions opposing counsel might use to discredit you, confuse you, or throw you off the track. Stay calm and project professionalism in your behavior and appearance.
- Know whether you're being called as a fact witness or an expert witness (or both) and whether you're being retained as a consulting expert or expert witness. Also, be familiar with the contents of your curriculum vitae.
- A deposition differs from a trial because there's no jury or judge. Both attorneys and a court reporter are present, and the attorney asks you questions. There are two types of depositions: discovery and testimony preservation. Testimony preservation depositions are often recorded.
- Hearings are typically administrative hearings or judicial hearings. Guidelines for testifying at depositions and hearings are much the same as the guidelines for courtroom testimony. Keep in mind that attorneys at discovery depositions might be more combative, so striving to maintain a calm, professional appearance can be critical. Discovery depositions are designed to elicit relevant evidence or testimony that might lead to relevant evidence, so the capacity to object effectively is very limited.
- Make sure you prepare answers for questions on what steps you took to collect and analyze evidence and questions on what tools you used and how they work.

Key Terms

conflicting out
curriculum vitae (CV)
deposition
discovery deposition
expert witness
fact witness
testimony preservation deposition
voir dire

Review Questions

1. Which of the following describes fact testimony?
    a. Scientific or technical testimony describing information recovered during an examination
    b. Testimony by law enforcement officers
    c. Testimony based on observations by lay witnesses
    d. None of the above
2. Which of the following describes expert witness testimony?
    a. Testimony designed to assist the jury in determining matters beyond the ordinary person's scope of knowledge
    b. Testimony that defines issues of the case for determination by the jury
    c. Testimony resulting in the expression of an opinion by a witness with scientific, technical, or other professional knowledge or experience
    d. Testimony designed to raise doubt about facts or witnesses' credibility
3. When using graphics while testifying, which of the following guidelines applies?
    a. Make sure the jury can see your graphics.
    b. Practice using charts for courtroom testimony.
    c. Your exhibits must be clear and easy to understand.
    d. Make sure you have plenty of extra graphics, in case you have to explain more complex or supporting issues.
4. What kind of information do fact witnesses provide during testimony?
    a. Their professional opinion on the significance of evidence
    b. Definitions of issues to be determined by the finder of fact
    c. Facts only
    d. Observations of the results of tests they performed
5. What expressions are acceptable to use in testimony to respond to a question for which you have no answer?
    a. No comment.
    b. That's beyond the scope of my expertise.
    c. I don't want to answer that question.
    d. I wasn't asked to investigate that.
    e. That's beyond the scope of my investigation.
6. What should you do if you realize you have made a mistake or misstatement during a deposition?
    a. If the deposition is still in session, refer back to the error and correct it.
    b. Decide whether the error is minor, and if so, ignore it.
    c. If the deposition is over, make the correction on the corrections page of the copy provided for your signature.
    d. Call the opposing attorney and inform him of your mistake or misstatement.
    e. Request an opportunity to make the correction at trial.

7. List two types of depositions.

8. At trial as a fact or expert witness, what must you always remember about your testimony?

a. You're responsible for the outcome of the case.

b. Your duty is to report your technical or scientific findings or render an honest opinion.

c. Avoid mentioning how much you were paid for your services.

d. All of the above

9. Before testifying, you should do which of the following?

a. Create an examination plan with your retaining attorney.

b. Make sure you've been paid for your services and the estimated fee for the deposition or trial.

c. Get a haircut.

d. Type all the draft notes you took during your investigation.

10. Voir dire is the process of qualifying a witness as an expert.

11. What is a motion in limine?

a. A motion to dismiss the case

b. The movement of molecules in a random fashion

c. A pretrial motion for the purpose of excluding certain evidence

d. A pretrial motion to revise the case schedule

12. During your cross-examination, you should do which of the following?

a. Maintain eye contact with the jury.

b. Pay close attention to what your attorney is objecting to.

c. Help the attorneys, judge, and jury in understanding the case, even if you have to go a bit beyond the scope of your expertise.

d. Pay close attention to opposing counsel's questions.

e. Answer opposing counsel's questions as briefly as is practical.

13. Your curriculum vitae is which of the following?

a. A necessary tool to be an expert witness

b. A generally required document to be made available before your testimony

c. A detailed record of your experience, education, and training

d. Focused on your skills as they apply to the current case

14. The most reliable way to ensure that jurors recall testimony is to do which of the following?

a. Present evidence using oral testimony supported by hand gestures and facial expressions.

b. Present evidence combining oral testimony and graphics that support the testimony.

c. Wear bright clothing to attract jurors' attention.

d. Emphasize your points with humorous anecdotes.

e. Memorize your testimony carefully.

15. If you're giving an answer that you think your attorney should follow up on, what should you do?

a. Change the tone of your voice.

b. Argue with the attorney who asked the question.

c. Use an agreed-on expression to alert the attorney to follow up on the question.

d. Try to include as much information in your answer as you can.

16. In answering a question about the size of a hard drive, which of the following responses is appropriate?

a. It's a very large hard drive.

b. The technical data sheet indicates it's a 3 terabyte hard drive.

c. It's a 3 terabyte hard drive configured with 2.78 terabytes of accessible storage.

d. I was unable to determine the drive size because it was so badly damaged.

17. List three items you should include in your CV.

18. When working for a prosecutor, what should you do if the evidence you found appears to be exculpatory and isn't being released to the defense?

a. Keep the information on file for later review.

b. Bring the information to the attention of the prosecutor, then his or her supervisor, and finally to the judge (the court).

c. Destroy the evidence.

d. Give the evidence to the defense attorney.

Hands-On Projects

For the following projects, you process an examination request from Mr. Benson, the general counsel at Superior Bicycles, Inc., and provide expert witness services by rendering opinions for each case. It's assumed you know how to retrieve data from an image file and document evidence as it's collected. For these projects, you need the GCFI-js01.001 file used in the in-chapter activity and the hash sets you created in Chapter 9. Before beginning, create a *Work*\Chap15\Projects folder, and move the image file to this subfolder.

Hands-On Project 15-1.

After reviewing the e-mails you recovered during the in-chapter activity, the general counsel, Mr. Benson, has found new information that Jim Shu is involved in collecting intellectual property information belonging to Superior Bicycles, Inc., from Tom Johnson. Mr. Benson also noticed in the spreadsheet that an e-mail from Mr. Johnson dated August 19, 2017 at 3:42 p.m. PDT was signed "Cousin Tom." Mr. Benson asks you to reexamine Mr. Shu's computer to see whether you can find any e-mails or files containing additional information to indicate that Mr. Shu and Mr. Johnson are related. For this project, you search allocated and unallocated space in the GCFI-js01.001 image for the word "cousin." Follow these steps:

1. Start Autopsy for Windows, and click the **Create New Case** button. In the New Case Information window, enter **Proj1501** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**.

2. In the Additional Information window, type **Proj1501** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

3. In the Select Data Source window, click the **Browse** button next to the "Browse for an image file" text box, navigate to your work folder and click the GCFI-js01.001 file, and click **Open** and then **Next**.

4. In the Configure Ingest Modules window, click the **Deselect All** button, and in the pane above that button, click the **Recent Activity, File Type Identification, Embedded File Extractor, Interesting Files Identifier**, and **PhotoRec Carver** check boxes.

5. Click the **Hash Lookup** check box, and in the "Select known hash databases to use" section, click the **NISTFile- *nnn* m.txt-md5** check box. In the "Select known BAD hash databases to use" section, click the **Special Project-A** and **Superior-Personnel Records**

check boxes, and then click the **Calculate MD5 even if no hash database is selected** check box.

6 In the list of ingest modules, click the **Keyword Search** check box, and in the "Select keyword lists to enable during ingest" section, click the check boxes for **Phone Numbers, IP Addresses, Email Addresses**, and **URLs**.

7 In the list of ingest modules, click the **Email Parser** check box, and the **Extension Mismatch Detector** check box, and then click the **Check all file types** option button and the **Skip files without extensions** and **Skip known files** check boxes.

8 Click **Next** and then **Finish**. When Autopsy finishes its analysis, click the **Keyword Search** down arrow at the upper right. In the text box, type **cousin**, and then click **Search**.

9 In the Result Viewer pane, click the **Keyword search 1 - cousin** tab to view the search results. Click the first file in the list, and review its contents in the Content Viewer pane.

10 In the Result Viewer pane, right-click the first file, point to **Tag Files**, and click **Tag and Comment**. In the Create Tag dialog box, click the **New Tag Name** button. In the New Tag section, type **Search 1 Cousin**, and then click **OK** twice.

11 Examine the contents of the remaining files. For all e-mails with information about the relationship between Mr. Shu and Mr. Johnson, right-click the e-mail, point to **Tag Result** and **Quick Tag**, and click **Search 1 Cousin**. Ignore any redundant files.

12 When you're finished, go to the Tree Viewer pane, and click to expand **Tags, Search 1 Cousin**, and **File Tags**.

13 In the Result Viewer pane, Ctrl+click all relevant files. Right-click this selection and click **Extract File(s)**. In the Save dialog box, click **Save**, and then click **OK** to extract these files to the Export subfolder.

14 Start Microsoft Word. Click **File**, **Open** from the menu. In the Open dialog box, navigate to the ***Work* \Chap15\Projects\Proj1501\Export** folder, click the first .eml file, and click **Open**. Print this e-mail.

Note

Microsoft Word, Outlook, and Mozilla Thunderbird can format and display .eml files correctly. In other word processing programs, such as LibreWriter, WordPad, or Notepad, the text-formatting information is displayed, which makes the contents difficult to read.

15 Repeat **Step 14** for all the e-mails you tagged. Close the case and exit Autopsy.

16 Write a memo to Mr. Benson stating that you have extracted several e-mails showing that Mr. Johnson is Mr. Shu's cousin, and you're ready to testify about the steps you took for this assignment. Submit this memo to your instructor.

Hands-On Project 15-2.

After reviewing your memo, Mr. Benson asks you to reexamine Mr. Shu's computer to look for any Superior Bicycles, Inc. documents. For this examination, you need to run the hashes created in **Chapter 9** on all data files in the image of Mr. Shu's computer. Follow these steps:

1 Start Autopsy for Windows, and click the **Create New Case** button. In the New Case Information window, enter **Proj1502** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**.

2 In the Additional Information window, type **Proj1502** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

3 In the Select Data Source window, click the **Browse** button next to the "Browse for an image file" text box, navigate to your work folder and click the GCFI-js01.001 file, and click **Open** and then **Next**.

4 In the Configure Ingest Modules window, click the **Deselect All** button, and in the pane above that button, click the **File Type Identification, Embedded File Extractor, Extension Mismatch Detector**, and **PhotoRec Carver** check boxes.

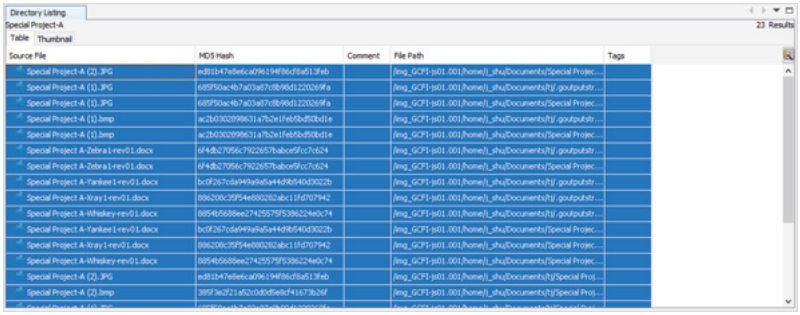
5 Click the **Hash Lookup** check box, and in the "Select known hash databases to use" section, click the **NISTFile- *nnn* m.txt-md5** check box. In the "Select known BAD hash databases to use" section, click the **Special Project-A** and **Superior-Personnel Records** check boxes, and then click the **Calculate MD5 even if no hash database is selected** check box.

6 In the list of ingest modules, click the **Keyword Search** check box, and in the "Select keyword lists to enable during ingest" section, click the check boxes for **Phone Numbers, IP Addresses, Email Addresses**, and **URLs**.

7 Click **Next** and then **Finish**. When Autopsy finishes its analysis, go to the Tree Viewer pane, and click to expand **Hash Hits** and **Special Project-A**.

8 In the Result Viewer pane, click the first file to display it in the Content Viewer pane, and press **Ctrl+A** to highlight all files (see Figure 15-3). Right-click this selection, point to **Tag Files**, and click **Tag and Comment**. In the Create Tag dialog box, click the **New Tag Name** button. In the New Tag section, type **Superior Bicycles data files**, and then click **OK** twice.

Figure 15-3.



Source: www.sleuthkit.org

Tagging all files in the Result Viewer pane

9 In the Result Viewer pane, click the first file and press **Ctrl+A**. Right-click this selection and click **Extract File(s)**. In the Save dialog box, click **Save**, and then **OK** to extract these files to the Export subfolder.

10 Click **Generate Report**. In the Generate Report window, click the **Results - Excel** option button in the Report Modules section, and then click **Next**. In the Configure Artifact Reports window, click the **Tagged Results** option button, click **Select All**, and then click **Finish**.

11 When the report has been generated, click the **Results - Excel** pathname in the Report Generation Progress window. Leave the report open for the next project, and exit Autopsy.

Hands-On Project 15-3.

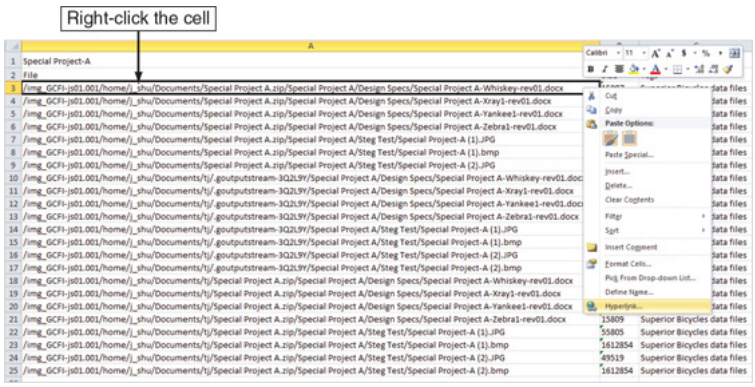
In this project, you finish the Excel report and write a memo about the data you found in **Hands-On Project 15-2**. You need to create hyperlinks to the Word documents listed in the Excel report.

Note

If you closed the Excel report, navigate to the *Work*\Chap15\Projects\Proj1502\Report\Proj1502 *mm-dd-yyyy-hh-mm-ss* folder and double-click the .xlsx file.

1 In the Excel report from **Hands-On Project 15-2**, click the **Hashset Hits** tab. Right-click the first file in cell **A3** and click **Hyperlink** (see Figure 15-4).

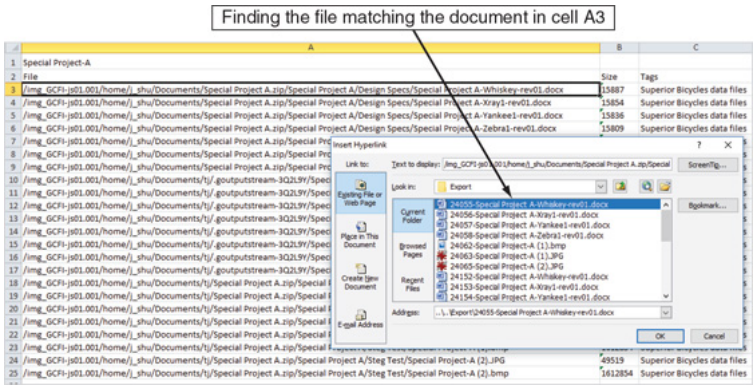
Figure 15-4.



Creating hyperlinks to Word documents

2 In the Insert Hyperlink dialog box, navigate to the ***Work*\Chap15\Projects\Proj1502\Export** folder and find the Word document matching the file listed in cell A3 (see Figure 15-5). Click the file in the list box and then click **OK** to link the file to the cell.

Figure 15-5.



The Insert Hyperlink dialog box

3 Repeat **Step 2** for all remaining files. When you're finished, save the spreadsheet and exit Excel.

4 To finish this project, write a memo to Mr. Benson stating that you have found Superior Bicycles documents in the image of Mr. Shu's computer. Attach your spreadsheet report, and turn the memo and report in to your instructor.

Hands-On Project 15-4.

After reviewing e-mails in the image of Mr. Shu's computer, Mr. Benson wants you to find and extract all e-mails to and from Terry Sadler. Follow these steps:

1 Start Autopsy for Windows. Click the **Create New Case** button. In the New Case Information window, enter **Proj1504** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**.

2 In the Additional Information window, type **Proj1504** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

3 In the Select Data Source window, click the **Browse** button next to the "Browse for an image file" text box, navigate to your work folder and click the GCFI-js01.001 file, and then click **Open** and then **Next**.

4 In the Configure Ingest Modules window, click the **Deselect All** button, and in the pane above that button, click the **File Type Identification, Embedded File Extractor, Exif Parser, Email Parser, Extension Mismatch Detector**, and **PhotoRec Carver** check boxes.

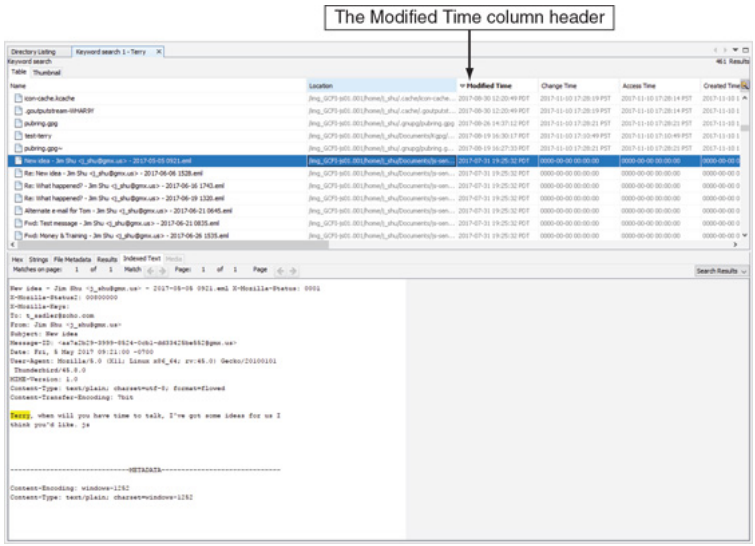
5 Click the **Hash Lookup** check box, and in the "Select known hash databases to use" section, click the **NISTFile- *nnn* m.txt-md5** check box. In the "Select known BAD hash databases to use" section, click the **Special Project-A** and **Superior-Personnel Records** check boxes, and then click the **Calculate MD5 even if no hash database is selected** check box.

6 In the list of ingest modules, click the **Keyword Search** check box, and in the "Select keyword lists to enable during ingest" section, click the check boxes for **Phone Numbers, IP Addresses, Email Addresses**, and **URLs**.

7 Click **Next** and then **Finish**. When Autopsy finishes its analysis, click the **Keyword Search** down arrow at the upper right. In the text box, type **Terry**, and then click **Search**.

8 In the Result Viewer pane, click the **Modified Time** column header twice to sort in descending order, then scroll down to find the first e-mail with an .eml extension in the Name column and click it, as shown in .Figure 15-6

Figure 15-6.

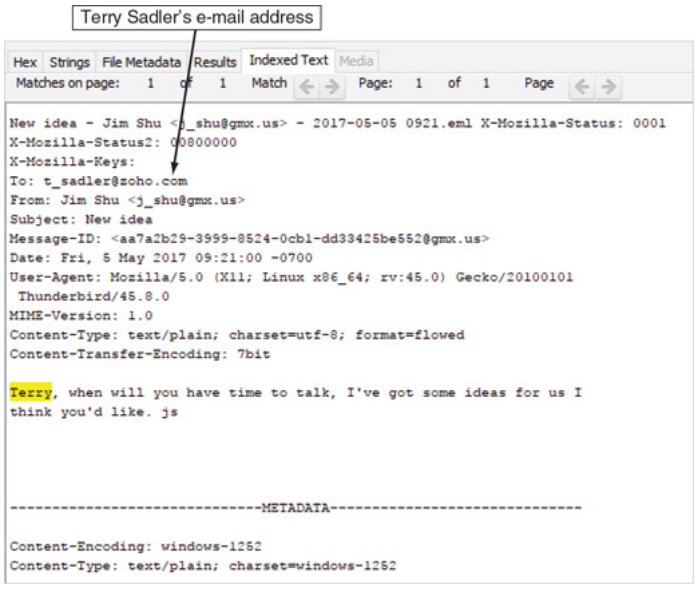


Source: www.sleuthkit.org

The keyword search results

9 Examine the contents of this e-mail in the Contents Viewer pane (see **Figure 15-7**) to determine the e-mail address Terry Sadler used.

Figure 15-7.



Source: www.sleuthkit.org

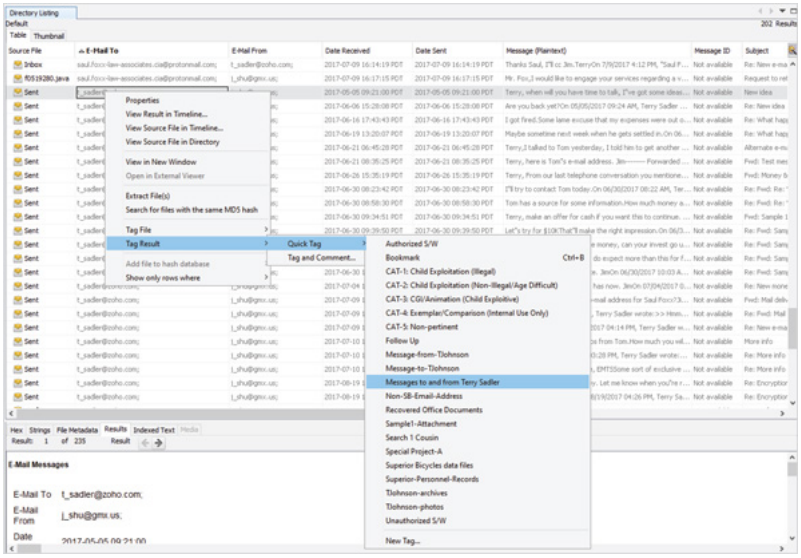
Viewing the contents of Terry Sadler's e-mails

10 In the Tree Viewer pane, click to expand **E-Mail Messages, Default (Default)**, and **Default**. In the Result Viewer pane, click the **E-Mail To** column header once to sort the e-mail addresses in alphabetical order.

11 Scroll down the list of e-mails and find the first occurrence of Terry Sadler's e-mail address, t_sadler@zoho.com. This e-mail and the following ones are in the Sent folder. Right-click the first message, point to **Tag Result**, and click **Tag and Comment**. In the Create Tag dialog box, click the **New Tag Name** button. In the New Tag section, type **Messages to and from Terry Sadler**, and then click **OK** twice.

12 Shift+click the next e-mail in the list, and then click the last e-mail with the address t_sadler@zoho.com in the Sent folder. Right-click this selection, point to **Tag Result** and **Quick Tag**, and click **Messages to and from Terry Sadler** (see Figure 15-8).

Figure 15-8.



Source: www.sleuthkit.org

Tagging e-mails in Terry Sadler's Sent folder

13 In the Result Viewer pane, click the **E-mail From** column header once to sort the e-mail addresses in alphabetical order by e-mail address, and then scroll down until you find the first occurrence of t_sadler@zoho.com. This e-mail and the following ones are shown in the Source File column as e-mails in the Inbox folder. Then highlight all the Terry Sadler e-mails that are associated with his Inbox folder and tag them as described previously.

14 In the Tree Viewer pane, click to expand **Tags, Messages to and from Terry Sadler**, and **Result Tags**. In the Result Viewer pane, highlight all the e-mails. Right-click this selection and click **Extract File(s)**. In the Save dialog box, click **Save**, and then click **OK** to extract these e-mails to the *Work*\Chap15\Projects\Proj1504\Export folder.

15 Click **Generate Report**. In the Generate Report window, click the **Results - HTML** option button in the Report Modules section, and then click **Next**. In the Configure Artifact Reports window, click the **Tagged Results** option button, click **Select All**, and then click **Finish**.

16 When the report has been generated, click the **Results - HTML** pathname in the Report Generation Progress window. Leave the report open for the next project, and exit Autopsy.

17 Write a memo to Mr. Benson with a link to your HTML report. Describe the steps you took to collect the evidence and the date and time you performed the analysis and extractions. Submit this memo to your instructor.

Hands-On Project 15-5.

Mr. Benson tells you that you need to present evidence at a hearing about Mr. Shu's activities. He wants you to prepare a presentation in Web page, Microsoft PowerPoint, or LibreOffice Impress format showing the evidence you recovered from the analysis done in the previous projects. The presentation should cover noteworthy e-mails and any files belonging to Superior Bicycles, Inc. To prepare material for your presentation, follow these steps:

1 Start Autopsy for Windows. Click the **Create New Case** button. In the New Case Information window, enter **Proj1505** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**.

2 In the Additional Information window, type **Proj1505** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

3 In the Select Data Source window, click the **Browse** button next to the "Browse for an image file" text box, navigate to your work folder, click the GCFI-js01.001 file, and click **Open** and then **Next**.

4 In the Configure Ingest Modules window, click the **Select All** button, and then click **Next** and **Finish**.

5 In the Tree Viewer pane, click to expand **Hashset Hits** and **Special Project-A**. In the Result Viewer pane, click the first file listed and then press **Ctrl+A** to select all files. Right-click this selection and click **Extract File(s)**. In the Save dialog box, click **Save**, and then click **OK** to extract these files to the *Work*\Chap15\Projects\Proj1505\Export folder.

6 In the Tree Viewer pane, click to expand **E-Mail Messages, Default (Default)**, and **Default**. In the Result Viewer pane, click the **E-mail From** header once to sort the addresses in alphabetical order. Shift+click the first e-mail in the Inbox folder from Tom Johnson (with the e-mail address 1060waddisonst@gmx.us and an .eml extension), and then click the last e-mail in the list from Tom Johnson. Right-click this selection, point to **Tag Result** and **Quick Tag**, and click **Messages-from-TJohnson**.

7 Scroll down until you find e-mails from Terry Sadler. Shift+click the first e-mail in the Inbox folder (with the e-mail address t_sadler@zoho.com and an .eml extension), and then click the last e-mail in the list from Terry Sadler. Right-click this selection, point to **Tag Result** and **Quick Tag**, and click **Messages to or from Terry Sadler**.

8 Scroll through the list of e-mails to find any others in the Email From column from other people who haven't been tagged, but omit Jim Shu's e-mails. Select these e-mails as a group, right-click the selection, point to **Tag Files** and **Quick Tag**, and click **Follow up**.

9 In the Result Viewer pane, click any e-mail and then press **Ctrl+A** to select all e-mails. Right-click this selection and click **Extract File(s)**. In the Save dialog box, click **Save**, and then click **OK** to extract these files to the *Work*\Chap15\Projects\Proj1505\Export folder.

10 Click **Generate Report**. In the Generate Report window, click the **Results - HTML** or **Results - Excel** option button in the Report Modules section, and then click **Next**. In the Configure Artifact Reports window, click the **All Results** option button, and then click **Finish**.

11 When the report has been generated, click the link in the Report Generation Progress window to open the report. Leave Excel or your Web browser open for the next project, and exit Autopsy.

After you have finished tagging the evidence and extracting e-mails and files, create a presentation in Microsoft PowerPoint, LibreOffice Impress, or Web page format to be used when presenting evidence in the hearing. You need to do the following:

- Review the tagged e-mails to determine the relationships between Jim Shu, Tom Johnson, and Terry Sadler.
- Based on the hash hits in the image of Mr. Shu's computer, identify and list documents and photos belonging to Superior Bicycles, Inc.
- Review the follow-up e-mails to discover how they might be related to Jim Shu.

Note

With the version of Autopsy used in this book, there are formatting limitations when you're viewing e-mails, which makes reading the content and accessing attachments

difficult. Several e-mail viewers for mbox-type e-mails and Outlook .pst files are available, however. For this project, you use BitRecover Thunderbird Viewer. For other recovery tools from BitRecover, see www.bitrecover.com/free/.

To view e-mails extracted from the forensic image, follow these steps:

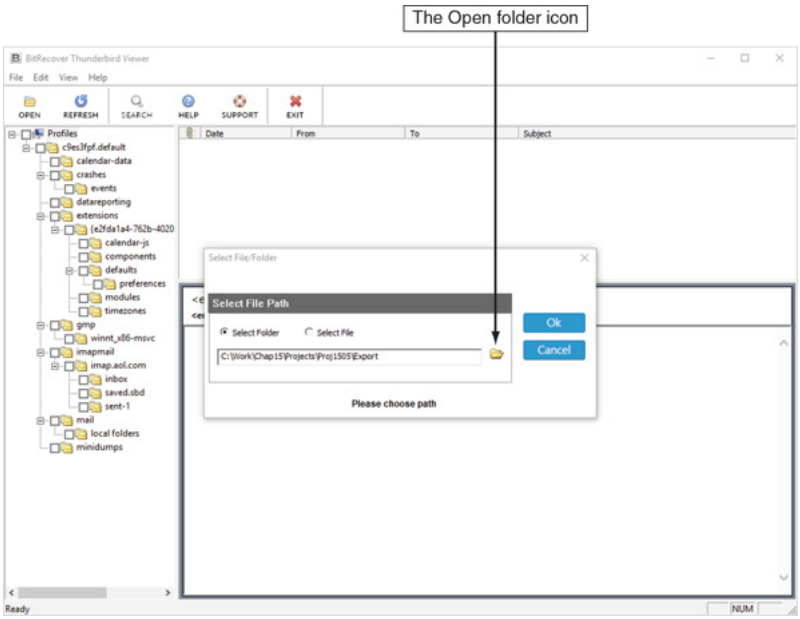
1. Start a Web browser, go to www.bitrecover.com/free/thunderbird-viewer/, and download and install the freeware version of BitRecover Thunderbird Viewer.
2. Start BitRecover Thunderbird Viewer, and click **File**, **Options** from the menu. In the Options dialog box, select a date format, such as mm/dd/yyyy, and click **OK**.

Note

When you start BitRecover Thunderbird Viewer, it automatically lists any Thunderbird e-mail data already on your workstation. For the purposes of this project, ignore the data in the left pane that displays your workstation's information. Proceed with **Step 3**, and when you open the Export folder, BitRecover Thunderbird Viewer replaces your information with the extracted e-mail folders from Autopsy.

3. Click the **OPEN** toolbar button. In the Select File/Folder dialog box, click the **Select Folder** option button (see Figure 15-9), click the **Open folder** icon, navigate to and click ***Work* \Chap15\Projects\Proj1505\Export**, and then click **OK** twice.

Figure 15-9.

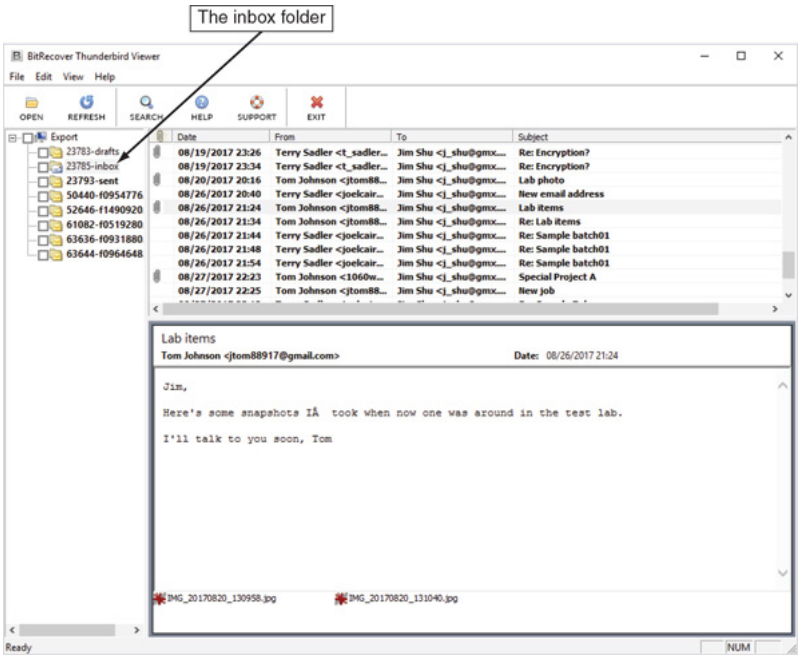


Source: BitRecover, www.bitrecover.com

Adding extracted Thunderbird e-mails

4. In the left pane, click the ***nnnnn* -inbox** folder. In the upper-right pane, click each e-mail and read its contents in the lower-right pane, as shown in .Figure 15-10

Figure 15-10.



Source: BitRecover, www.bitrecover.com

Reading Thunderbird e-mails

5 In **Figure 15-10**, two files attached to this e-mail are listed at the bottom. To view these files, double-click any image file icon or an e-mail in the upper-right pane to extract the e-mail contents and attachments. When you double-click an e-mail, BitRecover opens the folder in File Explorer containing the .eml or .txt file along with any attached files. In File Explorer, you can then open the e-mail or attachments.

6 Review all folders and any e-mails in them, along with their attachments to collect information for your presentation. When you're finished, exit BitRecover Thunderbird Viewer.

7 Based on the data you recovered, update your presentation report, created previously, and submit it to your instructor.

Case Projects

Case Project 15-1.

For this project, you create a brief outline of the steps you used for the in-chapter activity and hands-on projects. This project helps you review your work so that you can testify competently on your findings and the procedures you used. The outline doesn't need detailed steps; it serves as a way to trigger your memory about what you did.

Case Project 15-2.

You have been approached by an attorney who needs you as a fact witness and possibly an expert witness in a criminal case. The attorney has requested your curriculum vitae so that she can review it and prepare questions for you to answer during the pretrial qualifications. Prepare a draft of your CV and turn it in to your instructor for review. Your CV will be an ongoing project in your career.

Case Project 15-3

The attorney who retained you has given you a list of digital forensics terms and asked you to write definitions for these terms. These definitions will be given to the jury to help them better

understand the case's subject matter. Do research online to define the following terms, making sure you target your definitions to nontechnical readers:

- Hashes for Cyclic Redundancy Check, Message Digest, and Secure Hash Algorithm
- A drive image
- Static versus live data acquisition of drives
- Data carving
- Digital forensics tool validation

When you're finished, submit the definitions to your instructor.

Case Project 15-4.

The general counsel for Superior Bicycles has asked you to create a Microsoft PowerPoint, LibreOffice Impress, or Web page presentation on the work you've done for him (in the in-chapter activity and hands-on projects). Insert any evidence, such as e-mails, documents, and photographs. He plans to have you make this presentation to the jury during the trial. Integrate portions of your Autopsy reports and findings from e-mails that might be of use for testimony. When you're finished, submit the presentation's files to your instructor.

Chapter 16. Ethics for the Expert Witness

After reading this chapter and completing the exercises, you will be able to:

- Explain how ethics and codes apply to expert witnesses
- Explain how other organizations' codes of ethics apply to expert testimony
- Describe ethical difficulties in expert testimony
- Explain the process of carving data manually

For digital forensics examiners, maintaining the highest level of ethical behavior in their work is essential. In this chapter, you learn how digital forensics experts and other professionals apply ethics and codes of conduct to their work and to giving expert testimony. Forensics examiners are responsible for meeting the highest standards when conducting examinations, preparing reports, and giving testimony to ensure that evidence is accurate, reliable, and impartial. In addition, you must know when to disqualify yourself from an investigation. Knowing what to look for when taking a new case helps you avoid potential ethical problems.

Applying Ethics and Codes to Expert Witnesses

Ethics are the rules you internalize and use to measure your performance. The standards that others apply to you or that you're compelled to adhere to by external forces, such as licensing bodies, can be called ethics, but they're more accurately described as rules of conduct. Many professions now call these rules **codes of professional conduct or responsibility** . Both concepts of ethics are addressed in this chapter.

People need ethics to help maintain their balance, especially in difficult and contentious situations, and for guidance on their values. Ethics also help you maintain self-respect and the respect of those in your profession. Because forensics examiners don't have the same formal, detailed codes of conduct that professions such as medicine and the law have, relying on an internal code of ethics might be more critical. In addition, your internal standards, related to a philosophical, religious, or moral position, can be higher than standards established by codes of professional conduct. Laws governing codes of professional conduct or responsibility define the lowest level of action or performance required to avoid liability. Even with these low standards, there are still violations.

One of the most effective mechanisms for protecting yourself at a personal level and a legal level is to have nothing to hide. This ethical position allows people to be self-critical and critical of others. People who fear having their improper acts revealed feel as though they must protest the improper actions of others being revealed. Being able to engage in criticism of yourself or others, however, makes it possible to refine and strengthen personal codes of ethics or codes of professional responsibility.

Expert witnesses are expected to present unbiased, specialized, and technical evidence to a jury. However, experts, like the attorneys who hire them, have biases and other ethical failings. As a professional, you must control your biases, not allow them to control you. Ethics are a tool you can use to identify and control your biases or prejudices.

Currently, expert witnesses testify in more than 80% of trials, and in many trials, multiple expert witnesses testify. The courts are clearly aware of the importance of expert witnesses to the legal system and are concerned about expert witnesses' ethics and the challenges experts face in reconciling their ethical standards and court practice. Awareness of this challenge is evident in the following statement from *Kenneth C. v. Delonda R.* (814 N.Y.S.2d 562, 2006):

> … the topic of expert witness ethics and professionalism is largely undeveloped and there are few definitive statements about what exactly the expert witness's ethical obligations are and how they are to handle the subtle as well as the more blatant attempts to influence them. While some expert witnesses belong to professions that have an

> established code …, many experts come from professions that are not self-governing with a uniform code of ethics… . Even where professional associations have established ethical guidelines for conducting investigations, forming opinions … very few explain how the ethical boundaries imposed on judges and lawyers may bear on the performance of their role in the legal system.

Included in most professions' codes of professional conduct is an admonition to adhere to or comply with the law. The most important laws applying to attorneys and witnesses are the rules of evidence. As mentioned in **Chapter 15**, the Federal Rules of Evidence (FRE) prescribe the methods by which experts appear before the court. Codes of professional conduct or responsibility affect attorneys who hire experts, but experts are bound by their personal ethics and the ethics of their professional organizations. Professional organizations' guidelines are often vague and broad and might do little to enforce experts' ethical conduct, however. Finding examples of experts' ethically questionable behavior in court isn't difficult. For example, in an investigation of the West Virginia State Police Crime Lab (438 S.E.2d 501, W. Va. 1993), a former officer in the Serology Division was found to have falsified evidence in criminal prosecutions. In addition, the article "Erdmann Faces New Legal Woes: Pathologist indicted for perjury in Texas murder trial" (Geoffrey A. Campbell, *American Bar Association Journal*, November 1995) describes how a former Texas pathologist faked autopsies to aid in criminal trials. For a general discussion of expert witness ethics, see http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4332&context=flr.

In the United States, there's no state or national licensing body for digital forensics examiners. Some states have licensing requirements for private investigators and classify forensics examiners with private investigators, but the work private investigators usually do bears little resemblance to the work of forensics examiners. Therefore, your sources for ethical standards are your internal values (ethics), the codes of professional associations you belong to, the codes of certifying bodies that have granted you a certification, and your employer's rules of professional conduct. Most examiners rely on a combination of these standards and codes to construct their professional ethical codes.

A movement is underway to create a general code of ethics for expert witnesses. At least one proposal includes the topics of confidentiality, fees, ex parte communication, conflicts of interest, and professionalism. Generally, the positions advocated for in these proposals reflect the experience of other professional organizations, court rulings, and court rules but seek to consolidate these scattered resources into a codified system. For more information, see http://blogs.findlaw.com/strategist/2011/03/should-there-be-an-expert-witness-code-of-ethics.html.

Forensics Examiners' Roles in Testifying

As you learned in **Chapter 15**, forensics examiners have two roles in testifying: testifying to facts found during evidence recovery (fact witness) and rendering an opinion based on education, training, and experience (expert witness).

As an expert witness, you can testify even if you weren't present when the event occurred or didn't handle the data storage device personally. Because of an expert's important role in litigation, attorneys often shop for experts who can support their cases, and experts' fees might be only a secondary consideration. Criticism of expert witnesses is widespread in the legal community because it's possible to find and hire an expert to testify to almost any opinion on any topic. As a result, the impartiality of expert testimony and the potential for misconduct have become concerns.

If you're going to have a long and productive career as an expert witness, beware of attorneys' opinion shopping. An attorney might be willing to risk your career to improve the prospect of success in a case—and can always find another expert for the next case. The most effective way to prevent opinion shopping is to require that the attorney retaining your services send

you enough material on the case for you to make an evaluation. Distinguishing opinion shopping from the process of attempting to disqualify experts by creating conflicts can be difficult, however.

Conversely, attorneys should be cautious of expert witnesses who will tailor an opinion. If witnesses will tailor opinions for you, they might have tailored opinions for somebody else. When an expert witness is discredited, it can affect the attorney's credibility, too.

Considerations in Disqualification

One of the effects of violating court rules or laws is **disqualification** . This outcome isn't usually punitive, but it can be embarrassing for you as a professional and potentially for the attorney who retained you. A disqualification based on an ethical lapse could effectively be a death sentence for a career as an expert witness, as you can expect it to come up in any case you're involved in.

Opposing counsel might attempt to disqualify you based on any deviations from opinions you've given in previous cases. Any testimony you give at trials or depositions is on record and available to attorneys. (As mentioned in **Chapter 14**, attorneys search deposition banks for information on expert witnesses.) If there's a change in your position on a point, be sure to explain why you have changed it, such as recent developments in technology, new tools with new capabilities, or the facts of the current case differing from a previous case. An apparent change of position could be a subject for cross-examination, and you must be able to explain what appears to be contradictory opinions, or you'll be seen as tailoring testimony to your client's needs.

Some attorneys contact many experts as a ploy to disqualify them or prevent opposing counsel from hiring them; as explained in **Chapter 15**, this practice is called "conflicting out." Although attorneys might merely be scouting the field for information, you should always note calls from attorneys and the nature of the communication. Have a standard response, such as "Before we go beyond the general nature of the case and my expertise, you need to complete a client questionnaire and send me an investigation retainer." The retainer can be small, perhaps 2 to 8 hours of your usual billable rate for a simple case; the purpose of requesting the retainer is to deter attorneys from communicating with you solely for the purpose of disqualifying you. No explicit rule in the code of professional conduct prohibits attorneys from engaging in this process, but there are general prohibitions on engaging in actions designed to delay or be obstructive without legitimate purpose. These types of actions are unlikely to result in a bar association taking disciplinary action against attorneys, however.

Before allowing an attorney to describe any case details, determine who the parties are to reduce the possibility of a conflict. Although you aren't bound by the rigid rules on conflict of interest that bind attorneys, you might be working for an attorney on a case opposing the attorney who called you, and this conflict could reflect on the attorney.

When you're aware of a possible disqualification issue, bring it to the attention of the attorney who has retained you. The attorney then can get an early determination on the disqualification issue. There are rules to determine whether you can be disqualified from working on a case merely because you discussed general aspects of it. The rules for disqualification are derived from court decisions. Factors courts have used in determining whether to disqualify an expert include the following:

- Whether the attorney informed the expert that their discussions were confidential
- Whether the expert reviewed materials marked as confidential or attorney work product
- Whether the expert was asked to sign a confidentiality agreement
- Number of discussions held over a period of time
- The type of documents that were reviewed (publicly filed or confidential)

- The type of information conveyed to the expert—whether it included general or specific data or included confidential information, trial strategies, plans for method of proof, and so forth
- The amount of time involved in discussions or meetings between the expert and attorney
- Whether the expert provided the attorney with confidential information
- Whether the attorney formally retained the expert
- Whether the expert voiced concerns about being retained
- Whether the expert was requested to perform services for the attorney
- Whether the attorney compensated the expert

Numerous cases describe disqualification under the communication standards. For example, in *Wang Laboratories, Inc. v. Toshiba Corp.* (762 F. Supp. 1246 [E.D. Va. 1991]), the court summarized the process of determining whether an expert should be disqualified because of previous contact with an opposing party. The test is in two parts. First, was it objectively reasonable for the first party who claims to have previously retained the consultant to conclude that a confidential relationship existed? Second, was any confidential or privileged information disclosed by the first party to the consultant?

Similarly, there's extensive case law in which experts weren't disqualified and were allowed to testify over the objection of opposing counsel. For example, in *Hewlett-Packard Co. v. EMC Corp.* (330 F. Supp. 2d 1087 [N.D. Cal. 2004]) and *Tidemann v. Nadler Golf Car Sales, Inc.* (224 F.3d 719 [7th Cir. 2000]), the other side's lawyer merely served a subpoena on the expert to get factual testimony. If you don't know which standards for disqualification are being applied or how they are being applied in your jurisdiction, you should research the applicable state's court rulings on these issues. States often refer to already established rulings in other states or federal courts, and you can use an online search to find cases in the applicable jurisdiction. You might also want to have a standing relationship with an attorney who can advise you on these issues.

Traps for Unwary Experts

Expert witnesses should be cautious about the following potential traps, even though some aren't laid deliberately:

- What are some differences between the attorney's motives and the investigator's duty that might affect how the investigator acts, or is expected to act, as an expert witness?
- Is the function of the expert witness in conflict with the investigator's code of professional responsibility?
- Attorneys look at witnesses' codes of professional responsibility based on organizations they are members of. As an expert witness, you should anticipate that the opposing counsel will look at your organization memberships and those organizations' codes of professional responsibility.

Contingency fees aren't allowed except in certain limited circumstances; for example, consultants who don't testify can earn a contingency fee for finding testifying experts or investigative leads. However, an expert's activities leading to testimony can't be compensated on a contingent basis. Even the appearance of testimony on a contingent basis is dangerous. Therefore, experts should be paid in full for all previous work and for the anticipated time required for testimony.

It's unlikely you will encounter these situations, but if you do, it's wise to ask the hiring attorney to file a motion with the court requesting a ruling on disqualification. This process

protects you from future liability or ethical complaints. If the attorney doesn't want to follow this procedure, consider withdrawing from the employment.

In addition, avoid obvious ethical errors, such as the following:

- Don't alter data or present false data.
- Don't report work that wasn't done.
- Don't ignore available contradictory data.
- Don't do work beyond your expertise or competence.
- Don't allow the attorney who retained you to influence your opinion in an unauthorized way. (Keep in mind that there are authorized points of influence, such as the attorney framing a hypothetical question for you or asking you to answer specific questions.)
- Don't accept an assignment if it can't be done reasonably in the allowed time.
- Don't reach a conclusion before doing complete research.
- Don't fail to report possible conflicts of interest.

Determining Admissibility of Evidence

Although stating hypothetical questions during examination is no longer required in court, these questions can give you the factual structure to support and defend your opinion. You owe your client a full understanding of the facts relevant to your opinion, and you can ask him or her to establish that there's evidence supporting the facts your opinion is based on.

Although expert opinions can be presented without stating the underlying factual basis, the testimony isn't admissible if the facts on which the opinion is based are inadequate or there's not enough evidence to allow stating a legitimate opinion. FRE 702 (whether the expert is qualified and whether the expert opinion can be helpful) and FRE 703 (whether basis for the testimony is adequate) are considered in determining admissibility. If a question on admissibility arises under FRE 702 or 703, the court might require underlying facts or data to determine whether or to what extent the expert should be permitted to testify. Obviously, opposing counsel has an opportunity to explore and challenge the underlying facts and data on cross-examination. However, experts who provide explanations for how they reached their conclusions are far more persuasive to a judge or jury.

Organizations with Codes of Ethics

No single source offers a definitive code of ethics for expert witnesses, so you must draw on standards from other organizations to form your own ethical standards. This section discusses the effect that other organizations' ethical guidelines can have on expert testimony. Many professional organizations have rules to guide their members in areas such as interaction with patients and clients, objectivity, role in society, fees, solicitation, independence, and contractual relationships. The more restrictive and specific ethical rules are, the more effect they have in curbing unethical expert testimony.

International Society of Forensic Computer Examiners

The International Society of Forensic Computer Examiners (ISFCE) Code of Ethics and Professional Responsibility supplies guidelines for its members on how they are expected to perform their duties as forensics examiners. These guidelines include specific instructions on how members must maintain their professional standing and define what members must do and not do when performing their duties as forensics examiners. For example, the ISFCE code of ethics includes guidelines such as the following:

- Maintain the utmost objectivity in all forensic examinations and present findings accurately.

- Conduct examinations based on established, validated principles.
- Testify truthfully in all matters before any board, court, or proceeding.
- Avoid any action that would appear to be a conflict of interest.
- Never misrepresent training, credentials, or association membership.
- Never reveal any confidential matters or knowledge learned in an examination without an order from a court of competent jurisdiction or the client's express permission.

In addition, members are expected to maintain their integrity by reporting other members who violate the code of conduct to the ISFCE.

Note

The ISFCE also offers a Certified Computer Examiner (CCE) certification and includes ethical standards for examiners holding this certification. For more information on the ISFCE Code of Ethics and Professional Responsibility, see www.isfce.com/ethics2.htm.

International High Technology Crime Investigation Association

In its bylaws, the International High Technology Crime Investigation Association (HTCIA) provides a detailed Code of Ethics of Professional Standards Conduct for its members. HTCIA core values include the following requirements related to testifying:

- The HTCIA values the Truth uncovered within digital information and the effective techniques used to uncover that Truth, so that no one is wrongfully convicted.
- The HTCIA values the Integrity of its members and the evidence they expose through common investigative and digital forensics best practices, including specialized techniques used to gather digital evidence.

Note

For more information on the HTCIA code of ethics, see www.socalhtcia.com/about-htcia/.

International Association of Computer Investigative Specialists

The International Association of Computer Investigative Specialists (IACIS) provides a well-defined, simple guide for expected behavior of forensics examiners. These standards follow the principles defined by other professional organizations for investigations and testimony. The standards for IACIS members that apply to testifying include the following:

- Maintain the highest level of objectivity in all forensic examinations and accurately present the facts involved.
- Examine and analyze evidence in a case thoroughly.
- Conduct examinations based on established, validated principles.
- Render opinions having a basis that is demonstratively reasonable.
- Not withhold any findings, whether inculpatory or exculpatory, that would cause the facts of a case to be misrepresented or distorted.

Note

For more information on the IACIS code of ethics, see www.iacis.com/membership-2/membership-overview/.

American Bar Association

As a forensics examiner, you deal with attorneys, so you should be aware of the basic rules of professional conduct they must follow. The American Bar Association (ABA) is not a licensing body, but the ABA's Model Code of Professional Responsibility (Model Code) and its successor, the Model Rules of Professional Conduct (Model Rules), are the basis of state licensing bodies' codes. In the United States, attorneys are licensed by states.

Note

These codes are quite extensive, so only a few relevant sections are given here. To read the codes in their entirety, go to www.americanbar.org/content/dam/aba/migrated/cpr/mrpc/mcpr.authcheckdam.pdf for the Model Code and www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct.html for the Model Rules.

The ABA has stated that, unlike attorneys, expert witnesses do not owe a duty of loyalty to their clients. However, this doesn't absolve them of a duty to truth in facts they've observed or opinions they've rendered.

American Psychological Association

For psychologists, the broadly accepted guidelines governing their conduct as experts are the American Psychological Association's (APA's) Ethical Principles of Psychologists and Code of Conduct (commonly referred to as the "Ethics Code"). These guidelines offer comprehensive regulations, with an entire section devoted to forensics activities. The Ethics Code (www.apa.org/ethics/code/index.aspx) consists of standards that are enforceable rules for the conduct of psychologists and applies only to psychologists' activities in scientific and professional functions that are psychological in nature.

Ethical Difficulties in Expert Testimony

Despite the professional guidelines described in the previous section, problems still exist with expert witness testimony. There are inherent conflicts between the goals of attorneys and the goals of scientists or technicians (experts). Attorneys work in an adversarial system and look to sway the judge or jury with the most articulate, understandable expert, who is generally the most persuasive expert rather than the best scientist. In contrast, science requires experts to focus on the evidence without the influence of others' objectives.

As a result, *Daubert* and the APA's forensics guidelines can challenge experts to choose between complete impartiality and responsible advocacy. On one hand, an expert can appear in the role of impartial educator, whose purpose is to help the judge or jury understand a fact or an issue. According to *Daubert*, to provide reliable and valid testimony, the expert has the "ethical responsibility to present a complete and unbiased picture of the … research relevant to the case at hand." With an adversarial system, pressures from hiring attorneys, and a tendency to identify with the side you're working for, educating impartially is difficult. Therefore, experts should accept the position they have been placed in and act as responsible advocates. Ethical problems surface when experts decide to advocate for one side, as they must consider the line between using research to argue one side of an issue fairly and distorting and misrepresenting available research. *Daubert* cautions that if an expert falsifies,

distorts, or misrepresents the facts while advocating his or her position, opinion testimony will not be deemed reliable or valid.

Enforcing any professional organization's ethical guidelines is difficult. The principles can be enforced only against members of the organization, and if the expert chooses to withdraw from the organization, there's no effective mechanism to enforce the guidelines, unless the organization is a licensing agency. For forensics examiners testifying as experts, this means an organization has limited influence over examiners as witnesses in the form of peer pressure and reputation among peers. In addition, without a specific organization to oversee and comment on current expert testimony standards or transgressions, it's difficult to identify and investigate violations or to apprise an organization's members of acceptable methodologies and standards.

As a result, even the most specific guidelines, such as Section 7.0 of the APA Ethics Code, are as challenging to enforce as the broader restrictions the AMA has established. All guidelines rely primarily on internalization of the codes and witnesses' analysis of when and how they will participate in a case. The available guidelines also fail to ensure superior quality expert testimony because along with applicable laws, they set only a minimum level of acceptable performance or competence as the standard.

Ethical Responsibilities Owed to You

The attorney who has retained you, opposing counsel, and the court also owe you ethical responsibilities as an expert witness. Your attorney owes you a fair statement of the case or situation, adequate time to review evidence and prepare your report, and a reasonable opportunity to examine data, conduct testing, and investigate the matter before rendering an opinion. If the attorney wants you to render an opinion quickly and without adequate opportunity to review, be cautious. He might be trying to get you to commit based on inadequate information, or he's trying to rush you because he hasn't kept track of critical dates and is under pressure to meet a deadline. The attorney might also hold you under subpoena for an excessive amount of time waiting to testify. This might reflect difficulties in anticipating the amount of time required for other witnesses' testimony; however, you should be paid for the waiting time per the fee agreement. Making any portion of your fee dependent on a favorable report is inappropriate and should be a breach of the fee agreement. You are owed fair compensation for your time and work under the terms of the fee agreement.

Most attorneys, including opposing counsel, are competent, courteous professionals, but if they aren't, you can expect abuses that might include inquiry into your personal finances; unless this inquiry is about compensation terms for the current case, it's inappropriate. In addition, some opposing counsel attempt to make discovery depositions physically uncomfortable, such as using an excessively warm or cool room, having you face into the sun, or refusing to take comfort breaks. You don't need to endure the situation in silence, but you should be practical. Note the conditions to the attorney who set the deposition and ask him or her to correct the situation. If the situation is not corrected, you should note these conditions in the record, and continue noting them as long as the conditions persist.

After you have noted a problem in the record, you can refuse to continue with the deposition; however, these situations are rare and even more rare in court. Generally, you should consult with an attorney before taking that last step. If you think the behavior was serious enough that you can justify refusing to continue, you should also consider reporting the attorney to the state bar association. Other tactics include the attorney who set the deposition neglecting to have payment ready for you; you can refuse to attend the deposition if payment isn't tendered. An opposing attorney might also ask repetitive questions; the attorney who retained you should object to these techniques. For a testimony preservation deposition, however, you can expect that the attorney calling for your testimony will try to make you as comfortable as possible because he or she wants your best performance.

As a measure of protection, you might want to have your personal attorney attend the deposition; this attorney can't object to questions but is available to advise the attorney who retained you or to advise you during breaks. Whether this precaution is necessary depends on the issues involved, how confrontational opposing counsel is expected to be, and whether the retaining attorney might need immediate advice on questions. A less costly alternative is arranging to have your attorney available by phone during the deposition. In this case, you could bring your own recorder to the deposition and play back portions to your attorney, unless there's an order to the contrary. In most jurisdictions, attendees are allowed to record depositions, so unless somebody objects, record your testimony. A recording is also useful when you review your deposition testimony before signing the transcript.

Standard Forensics Tools and Tools You Create

The tools you use to recover, control, and track evidence are subject to review by opposing parties. If the court deems them unreliable, the evidence you recovered with them might not be admitted or might be admitted with a limiting instruction. If you use standard tools—commonly used tools or commercially available tools—you simplify the process of validating them.

Tools you've created, if they're designed for a specific purpose and have been tested adequately to validate their accuracy for that purpose, might have advantages you can demonstrate to a judge, who ultimately determines whether evidence is admissible. For example, a tool you've created could be more compact or run more efficiently than other comparable tools. You're still required to validate these personal tools, however, and might have to share their source code for analysis. Remember that "borrowing" code from other products or incorporating other tools into your own without acknowledgment or paying royalties could be a violation of copyright law and is considered theft. In addition, it can result in major embarrassment for you, could have serious criminal and civil liability implications, and could adversely affect the attorney who retained you. (For opinions related to the advisability of using your own tools, you can read about *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, at www.law.cornell.edu/supct/html/92-102.ZS.html.)

An Ethics Exercise

In any investigation, examination, or expert opinion, ethical issues can arise. For this final chapter, you're asked to analyze a forensic image from a computer that seems to have data corrupted by malware. This forensic image is of a disk drive on a second computer owned by Jim Shu, who's suspected of receiving the intellectual property data you found in **Chapter 15**. The general counsel of Superior Bicycles, Inc., Ralph Benson, wants you to determine whether the data was corrupted by malware or was damaged intentionally to hide evidence. Your task is to examine the forensic image to determine the direction of the case and provide an expert opinion on whether the data's corruption was caused by malware or intentional destruction.

Note

Before beginning these activities, refer to the information in the "**Examining NTFS Disks**" section of Chapter 5 on record field structures in the MFT record. Then create a *Work*\Chap16\Chapter folder on your system (referred to as your "work folder" in steps). Your folder name will likely differ from what's shown in screenshots.

Performing a Cursory Exam of a Forensic Image

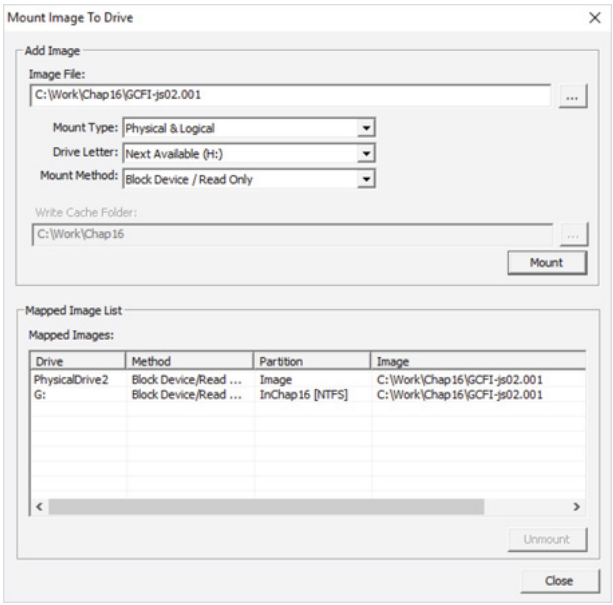
A forensics examiner's technical capability requires being able to work around problems and challenges when dealing with digital evidence. To begin examining the forensic image used for this activity, you need to check it for viruses first. To do this, you use FTK Imager Lite to mount

the image as a disk drive and run antivirus software to scan the drive. Follow these steps to mount a forensic image as a disk drive:

1. Download to your work folder the **Ch16Inchp01.exe** file from this chapter's downloads section on the student companion site for this book. In File Explorer, double-click the **Ch16Inchp01.exe** file and click **Extract** to uncompress it into GCFI-js02.001.

2. Start FTK Imager Lite, and click **File**, **Image Mounting** from the menu. In the Mount Image To Drive dialog box, click the ... button next to the Image File text box, navigate to your work folder, click **GCFI-js02.001** , and then click **Open** (see the results in Figure 16-1). Click the **Mount** button, and keep this dialog box open. Note the drive letter assigned to the mounted forensic image; your system might have assigned a different letter.

Figure 16-1.



The Mount Image to Drive Dialog Box

Caution

When you mount a forensic image with the Image Mounting function, it's mounted as a read-only drive. Don't change the Mount Method option to writeable because it corrupts the digital evidence.

Note

If you need to clear screen space, click Close and then Minimize in FTK Imager Lite. To open the Mount Image To Drive dialog box again, click File, Image Mounting from the menu. Exiting FTK Imager Lite unmounts the forensic image.

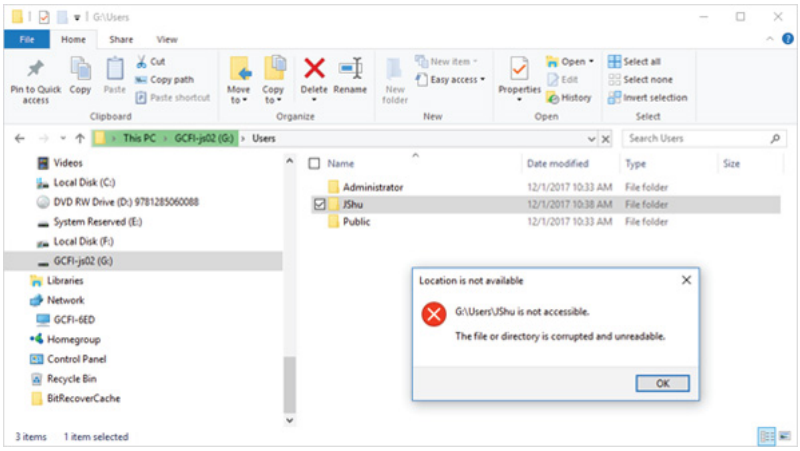
3. Run your antivirus software on the drive you mounted. When the scan is finished, note whether a virus was detected.

Note

If your antivirus software is Windows Defender, a scan could take several hours. For the purpose of this activity, choose the Quick Scan option to reduce the time. Some antivirus software, such as Norton Security Suite, enables you to select a specific drive to shorten the time needed to finish a scan.

4. To examine the contents of the mounted image, click the **Users** folder in File Explorer and then the **JShu** subfolder (see Figure 16-2). In the "Location is not available" error message, click **OK**.

Figure 16-2.



Viewing the Users Folder on Jim Shu's Computer

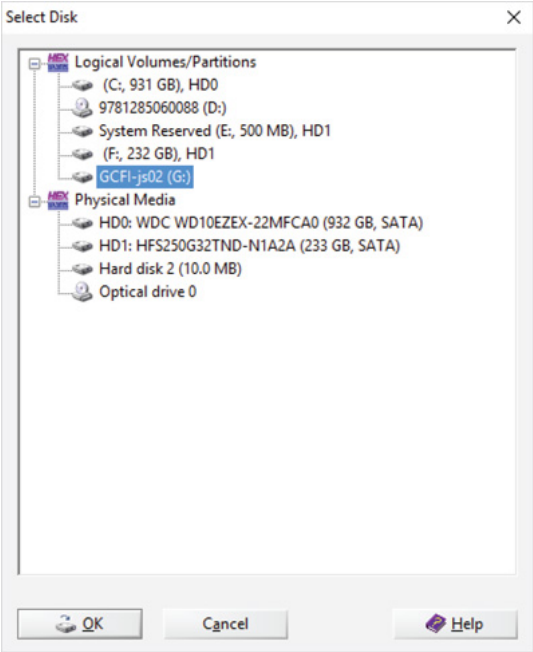
5. Leave FTK Imager Lite running for the next activity.

Performing a Detailed Exam of a Forensic Image

Because you weren't able to open the JShu folder in File Explorer, you need to make a detailed examination of the image in a different tool. For this examination, the first file to inspect is $MFT in the drive's root folder. This file contains the cluster addresses of where files are stored on a disk drive. Not being able to open the JShu folder in File Explorer means the OS can't read the folder's cluster address and might be corrupted in the $MFT file. For this activity, you need to determine whether data can be recovered and give an opinion of what might have caused the JShu folder to be inaccessible. To examine the GCFI-js02.001 image in WinHex, follow these steps:

1. Start WinHex and click **Tools**, **Open Disk** from the menu. In the Select Disk dialog box, click **GCFI-js02 (G:)**, as shown in Figure 16-3, and then click **OK**. (*Note*: Your drive letter might be different.)

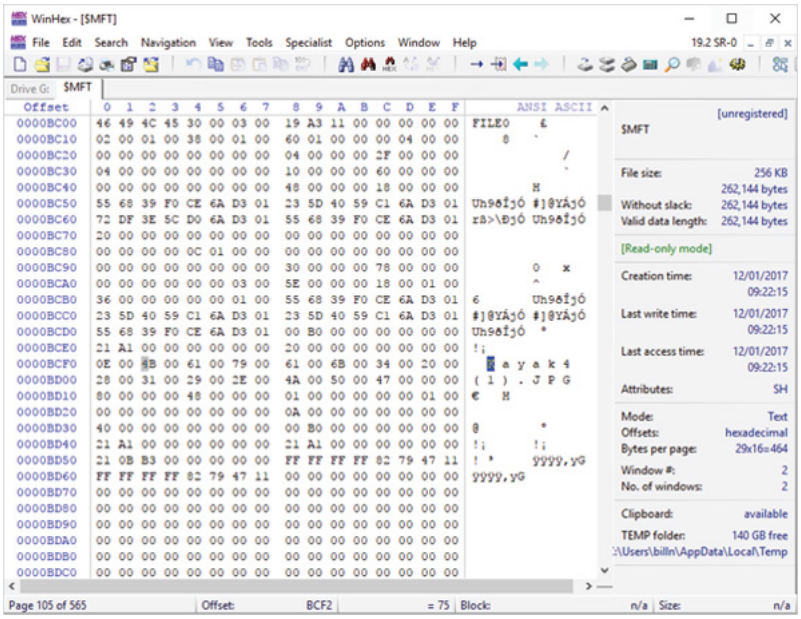
Figure 16-3.



Selecting the Disk Drive

2. In the list of folders and files in the upper pane, scroll down, and then right-click **$MFT** and click **Open**, at which time a new tab opens (see Figure 16-4).

Figure 16-4.



Opening the $MFT File

Note

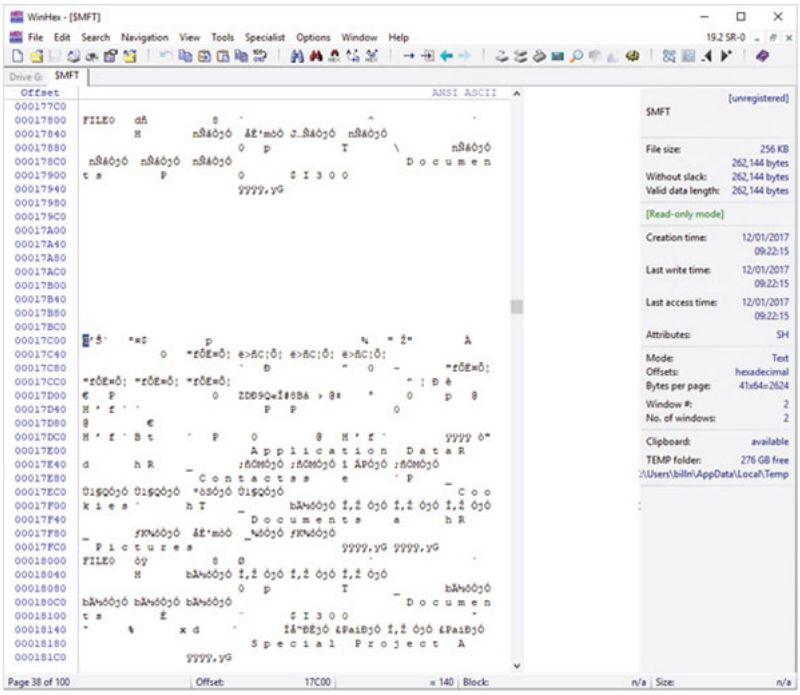
In the $MFT file, each record starts with the string FILE0 and is 0x400 (1024) bytes.

3.

To make viewing records easier, click **View**, **Text Display Only** from the menu to eliminate hexadecimal values in the display.

4. Scroll through each record to determine whether any start with characters other than FILE0. When you have found a record like this, note its offset position at the start of the record, such as the 17C00 shown at the bottom of **Figure 16-5**.

Figure 16-5.



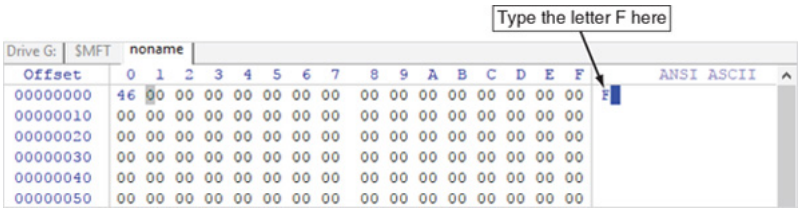
Finding a Corrupt Record in the $MFT File

5. Because the first 0x200 (512) bytes of the record at offset 17C00 are unreadable characters, click **View**, **Text Display Only** from the menu again to toggle the display of hexadecimal values.

Next, you need to look at the binary patterns of the first byte of this record to determine what might have happened to the data. To begin your analysis, determine the binary pattern for the uppercase letter F because the first 5 bytes in an MFT record should be FILE0. Follow these steps:

1. In WinHex, click **File**, **New** from the menu. In the Create New File dialog box, click **OK**. When the noname tab opens, click in the ANSI ASCII column at position **00000000**, and type the letter **F** (see Figure 16-6).

Figure 16-6.



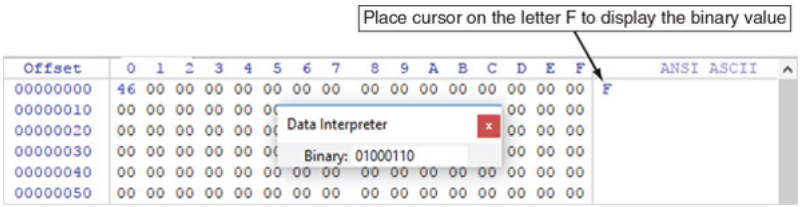
The Noname Tab Displaying the Hexadecimal Value of F

2. Click the letter **F**, and then click **Options**, **Data Interpreter** from the menu. In the Data Interpreter Options dialog box, click the **Binary (8 bits)** check box, and then click **OK**.

(To minimize the Data Interpreter window, click to clear all other check boxes.)

3. If the Data Interpreter window doesn't open, click **View** from the menu, point to **Show**, and click the **Data Interpreter** check box. Note the binary pattern 01000110 in the Data Interpreter window (see Figure 16-7).

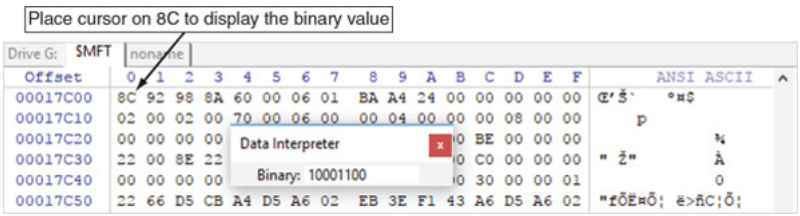
Figure 16-7.



The Data Interpreter Window Showing the Binary Value of F

4. Click the **$MFT** tab and click the first byte, **8C**, at offset 17C00 and note the binary pattern 10001100 (see Figure 16-8).

Figure 16-8.

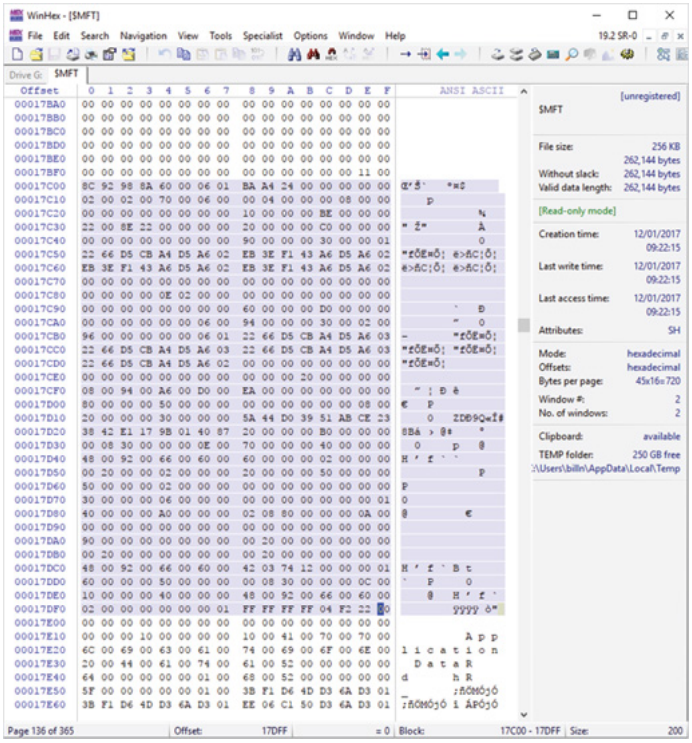


The Data Interpreter Window Showing the Binary Value of 8C

Based on this examination, it seems that the bits in the byte at offset 17C00 have shifted 1 bit to the left. As stated, all $MFT records start with the letter F. Because the first byte's binary bit pattern at offset 17C00 is 10001100 and the letter F binary pattern is 01000110, it appears the 0s and 1s moved one position to the left. To verify that all bytes have been shifted, follow these steps:

1. Select the range of bytes from offset **17C00** to offset **17DFF** (see Figure 16-9).

Figure 16-9.

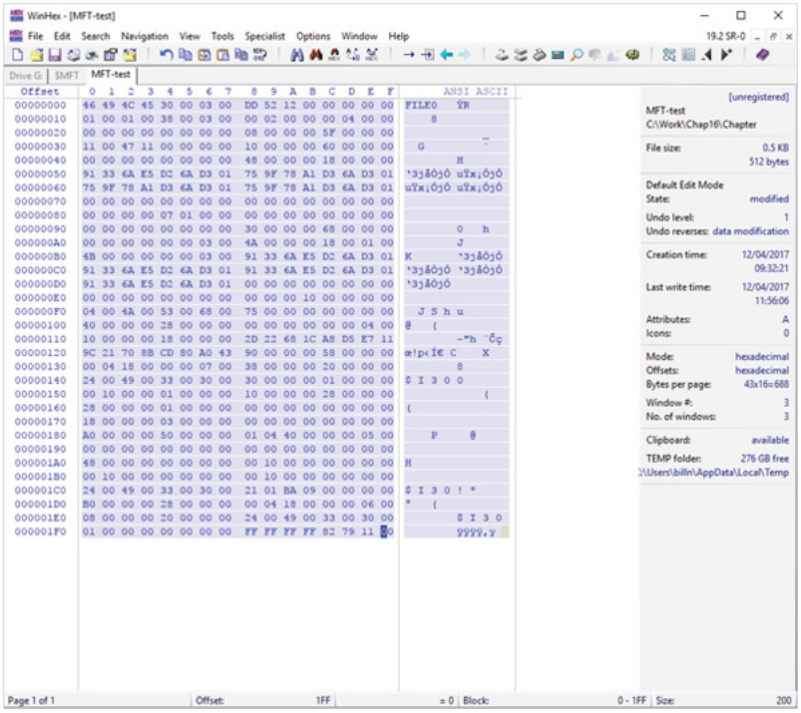


Highlighting the Corrupted MFT Record

2. Click **Edit** from the menu, point to **Copy Block**, and click **Into New File**. In the Save File As dialog box, navigate to and click your work folder, type **MFT-test** in the File name text box, and click **Save**.

3. When the new MFT-test tab opens, select all data from offset **00000000** to **000001FF** (see Figure 16-10), and then click **Edit**, **Modify Data** from the menu. In the Modify Block Data dialog box, click the **Right shift by 1 bit** option button, and then click **OK**. Click **File, Save As** from the menu. In the Save File As dialog box, type **MFT-recovered** in the File name text box, and then click **Save**. Leave WinHex running for the next activity.

Figure 16-10.



The Recovered MFT Record

This activity has shown you how to examine altered or corrupted data and then restore it. It's a simple example of how **bit-shifting** can obscure data. In an MFT record, the first 5 bytes should be FILE0. By examining the bit of the first byte and other bytes, you can easily see that bits have shifted to the left. Shifting the bits to the right restored this data to its original state.

More complex bit-shifting techniques might use a combination of methods, such as reverse byte order, shifting by a certain number of bytes, circular left rotation, inverting bits, and so on. Whatever method was used, you might need to apply combinations of methods in an attempt to restore data. Running through several combinations can take a long time and might result in scope creep. You need to determine how much effort to put into this task and what the likelihood of success is for the efforts.

For this case, you've been asked to give an expert opinion on whether the data was intentionally or unintentionally corrupted. Because the antivirus scan failed to show any known viruses, you should state in your report that offering a reason for how the data became corrupted is premature. To follow your ethical standards, you should analyze the data in more depth to see whether you can find anything to establish how the data was corrupted.

Performing the Exam

To maintain the highest possible ethical standards when conducting a forensics examination, you should develop a plan as described in **Chapter 1** and review it before starting your analysis. You need to be as thorough as possible during your examination to minimize any challenges an opposing attorney could make to discredit your report or testimony.

Preparing for an Examination

The planning stage should cover all possibilities, including giving an opinion of whether data was corrupted intentionally or unintentionally. To create a plan for examining Jim Shu's second computer, review the following questions and answers about the data. Be prepared to give answers to these types of questions in a report or as oral testimony.

Q: What's the purpose of the examination or inquiry?

A: To determine whether data was corrupted intentionally or by a virus.

Q: What's the scope of this examination?

A: To find corrupted files and recover them, if possible.

Q: What do you need to look for to determine whether the corruption was intentional or caused by a virus that an antivirus program failed to identify?

A: I look for any folders or files that the computer's operating system can't read.

Q: What programs do you use to look for corrupted data?

A: I use standard antivirus programs and a hexadecimal editor.

Q: What are the names of the programs you used to check for viruses?

A: I used Norton Security Suite.

Q: What is a hexadecimal editor?

A: It's a special tool that can display data's hexadecimal values.

Q: What does "hexadecimal" mean?

A: It's the numbering system used by computers and is called "base-16." Similar to the decimal numbering system, which is base-10 with values of 0 through 9, the hexadecimal system includes 0 through 9 plus the letters A, B, C, D, and F. The hexadecimal value of A is equal to the decimal value of 10, and the hexadecimal value of F is equal to the decimal value of 16.

Q: What's the name of the hexadecimal editor you used for this examination?

A: I used WinHex.

Q: How can data become corrupted on a computer?

A: Data corruption can be caused by a virus attack, unknown user mishandling, or unknown hardware failure, or it can be altered intentionally by someone.

Q: In the case of Mr. Shu's second computer, what corrupted data did you find?

A: I found that the JShu user folder and all its subfolders and files couldn't be accessed, and the data couldn't be read.

Q: What caused the JShu user folder to be inaccessible?

A: At this time, I don't know what caused the folder to be inaccessible.

Q: What is a Master File Table?

A: The Master File Table is a file containing the names and disk locations of files and folders. It functions like a table of contents for a book.

Q: Do you know what caused this data to be unreadable?

A: No, not at this time.

Q: Why not at this time?

A: Finding the reason requires more analysis of the entire disk drive to see what might have altered this data.

Q: Will you be able to determine whether the data was altered—that is, corrupted intentionally?

A: No.

Q: Why not?

A: In my examination of the Master File Table, the only altered data I found was the record for the JShu folder. All other records were unaltered. Furthermore, I determine from my analysis that the altered data was bit-shifted 1 bit to the left.

Q: What do you mean by bit-shifted?

A: Data such as letters are represented as bytes, each of which is 8 or 16 bits depending on the file system. For example, Windows 10 uses 16 bits for a byte. Bits are switches that are on, represented by 1s, or off, represented by 0s. The letter F has the bit pattern 01000110. When I examined the first byte of the corrupted record in the Master File Table, it should have been the letter F. However, the corrupted first byte has the bit pattern 0001100. By comparing the 1s and 0s of the letter F and the first byte of the corrupted record, I can see that that the byte seems to have been shifted 1 bit to the left. Therefore, I tested the first 512 bytes of the corrupted record by bit-shifting each byte 1 bit to the right. This test seemed to restore the data to its original state.

Q: Because you tested the forensic image of Mr. Shu's second computer for viruses and found nothing, can you say that this data was corrupted intentionally?

A: At this time, I can't determine whether the data was corrupted intentionally.

Interpreting Attribute 0x80 Data Runs

The next task is a detailed examination of attribute 0x80 of an MFT record in WinHex. Because the JShu folder has been corrupted, files and folders in its directory tree are no longer visible. For this examination, you search through the MFT record of GCFI-js02.001 for an **orphan file** (a file or folder that has lost its link to the parent folder) named Kayak4(1).jpg. Next, find its attribute 0x80 field and calculate the data run. Refer to Chapter 5 (in the "Interpreting a Data Run" section) for a refresher on how to find and compute data runs. After calculating the data run, you use WinHex to extract the orphaned file to a new file.

Finding Attribute 0x80 an MFT Record

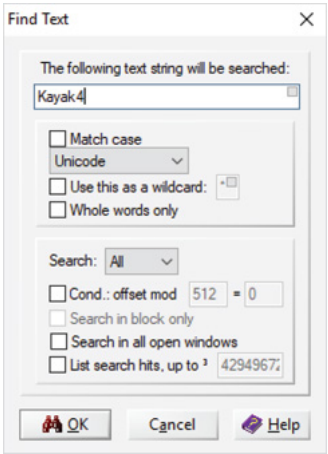
To find the attribute 0x80 field and its data run, first locate the starting and ending positions of attributes 0x10 and 0x30. The next attribute after attribute 0x30 is attribute 0x80. Follow these steps to find attribute 0x80:

Tip

All numeric values in these steps are hexadecimal. If the offset counter is in decimal mode, click anywhere in the Offset column once to change it to hexadecimal mode.

1. In WinHex, click **Search**, **Find Text** from the menu. In the Find Text dialog box, type **Kayak4** in the text box at the top. In the drop-down list box under the "Match case" check box, click **Unicode** (see Figure 16-11), and then click **OK**.

Figure 16-11.



The Find Text Dialog Box

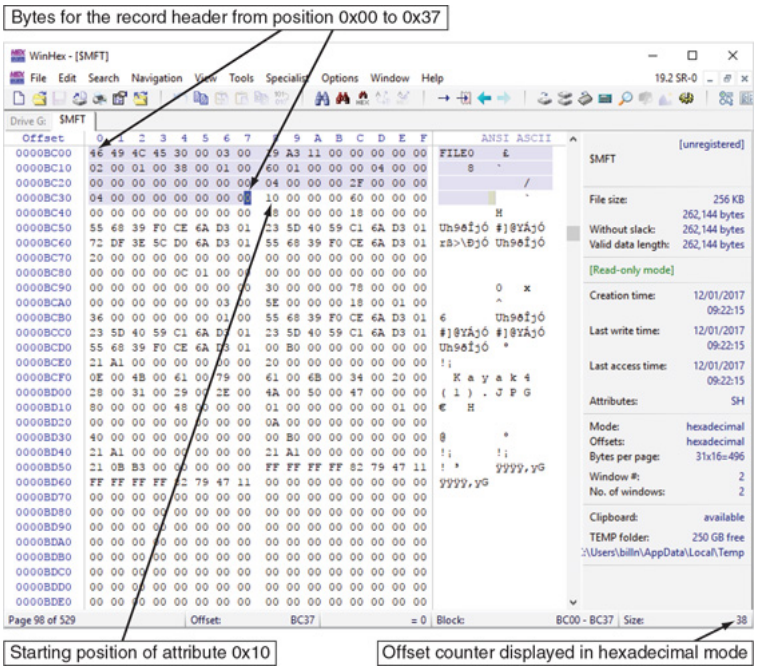
Note

When searching for specific record information, sometimes you see duplicate files with the same name that have different data runs, meaning the file was written to disk more than once on separate occasions. You need to examine all search results, compute their data run values, and attempt to recover the files. If your first effort doesn't produce successful results, continue searching for other occurrences.

2. In the main window, the cursor is in the right pane at the start of the first occurrence of the Unicode string Kayak4. From this position, scroll up until you see FILE0 and click the letter **F** at offset 0000BC00.

3. To find the starting position of attribute 0x10, drag down 38 hexadecimal bytes at offset 0000BC37 (see **Figure 16-12**), using the offset counter in the lower-right corner as a guide. Attribute 0x10 starts at offset 0000BC38.

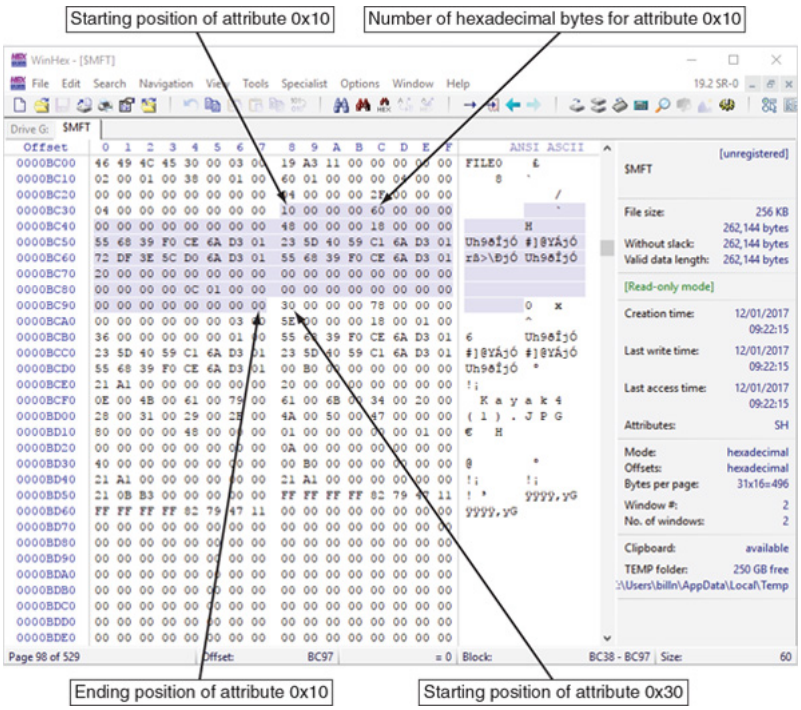
Figure 16-12.



Selecting an MFT Record Header

4. Next, place the cursor at the beginning of attribute 0x10 (at offset 0000BC38) and drag down 60 hexadecimal bytes until you reach the next attribute, 0x30 (see **Figure 16-13**). Attribute 0x30 starts at offset 0000BC98.

Figure 16-13.

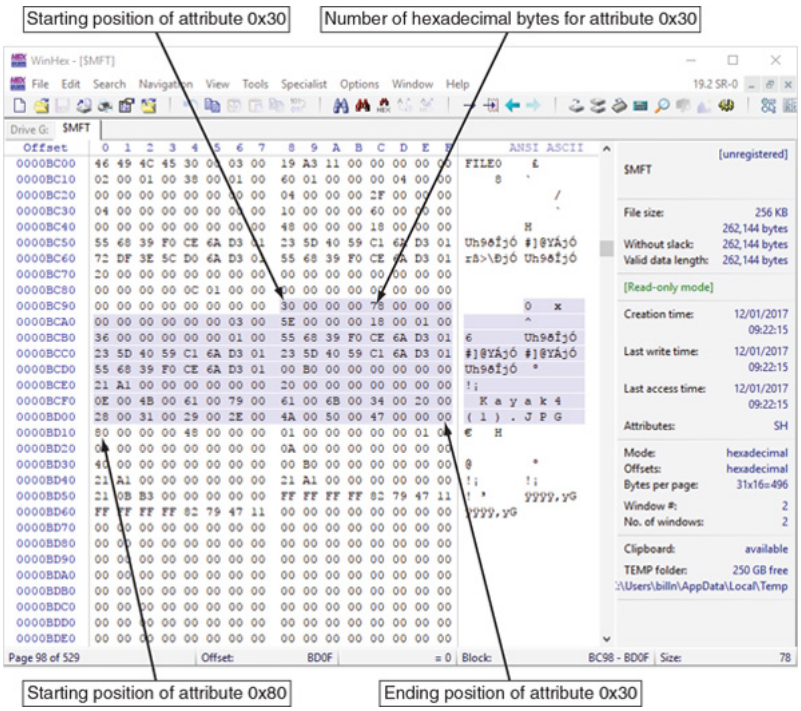


Selecting Attribute 0x10

5. Place the cursor at the beginning of attribute 0x30 (at offset 0000BC98) and drag down 78 hexadecimal bytes until you reach the next attribute, 0x80 (see **Figure 16-**

14). Attribute 0x80 starts at offset 0000BD10.

Figure 16-14.



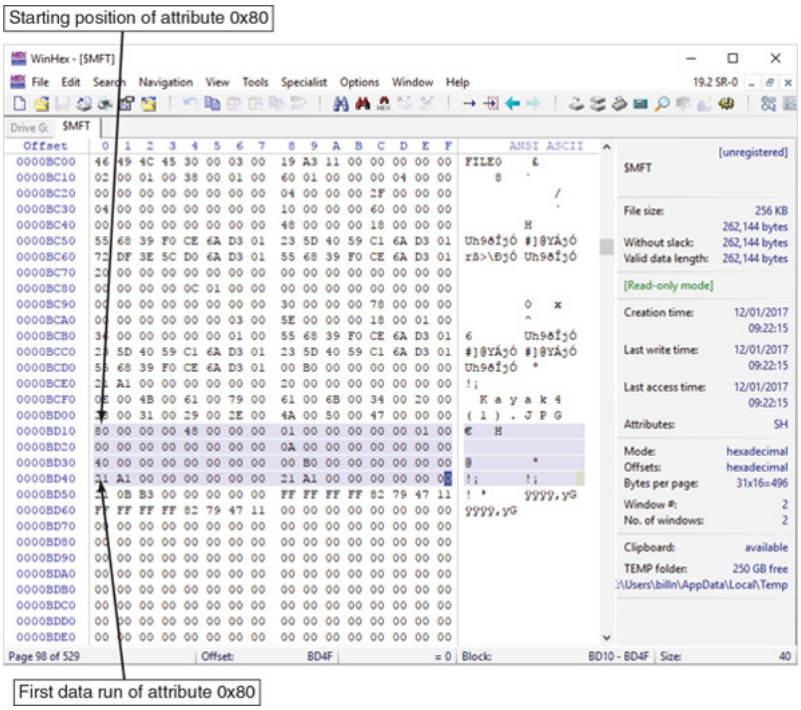
Attribute 0x30: Short Filename

Note

The forensic image for this activity is from an NTFS file system created in Windows 10. If you're examining a forensic NTFS image from a Windows 7 or older system, you'll see two attribute 0x30s: one for the short filename and one for the long filename. In that case, you must repeat **Step 5** to find the starting position of attribute 0x80.

6. From the starting position of attribute 0x80 (at offset 0000BD10), count 40 hexadecimal bytes to the beginning of the first data run at offset 0000BD50 (see **Figure 16-15**). Leave WinHex running for the next activity.

Figure 16-15.



Attribute 0x80: the Beginning of the First Data Run

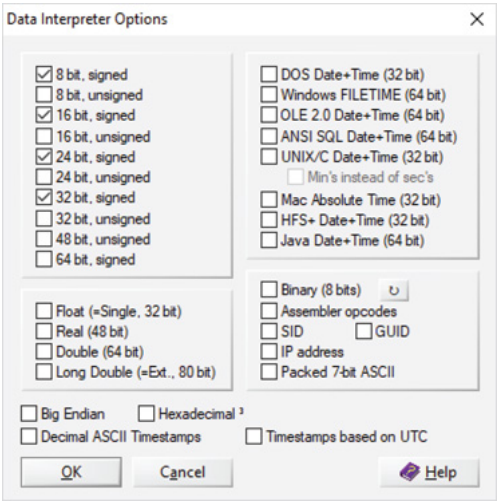
Now that you have found the data run's starting position, the next task is to calculate the starting and ending cluster positions of each data run fragment. (For more detailed information on calculating data runs, refer back to **Figures 5-19**, 5-20, 5-21, 5-22 and 5-23 in Chapter 5.)

Configuring Data Interpreter Options in WinHex

Typically, when WinHex starts, the Data Interpreter window opens, where you can convert data formats into easy-to-read values, such as converting hexadecimal values into decimal values. For the following activities, you need to know how to configure settings to perform data run calculations. Follow these steps:

1. Start WinHex, if necessary. If the Data Interpreter window doesn't open, click **View** from the menu, point to **Show**, and click the **Data Interpreter** check box.
2. Click **Options**, **Data Interpreter** from the menu to open the Data Interpreter Options dialog box. Click the **8 bit, signed**, **16 bit, signed**, **24 bit, signed**, and **32 bit, signed** check boxes (clearing any other check boxes that are selected), as shown in Figure 16-16, and then click **OK**. Leave WinHex running for the next activity.

Figure 16-16.



The Data Interpreter Options Dialog Box

Calculating Data Runs

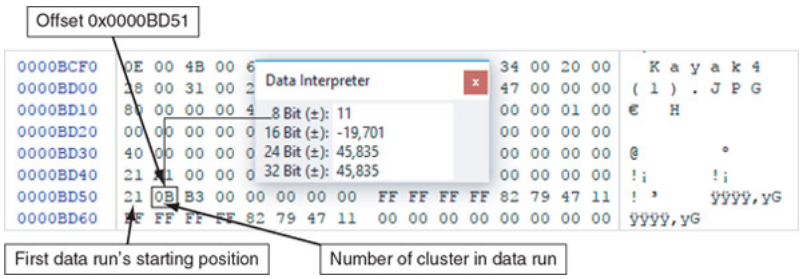
Next, determine the starting and ending cluster numbers for the MFT record's data run. The length of this MFT record is less than 512 bytes (0x200 hexadecimal), so the data run doesn't have an update sequence array value, as described in **Chapter 5** (refer to Figure 5-13). To calculate the data run for this example, follow these steps:

Tip

WinHex's Data Interpreter converts hexadecimal values into decimal values.

1. To determine the number of clusters for this data run, place the cursor at offset **0000BD51** (see Figure 16-17). Because it's only 1 byte long (8 bits), record the 8 Bit (±) value in the Data Interpreter window, which is 11.

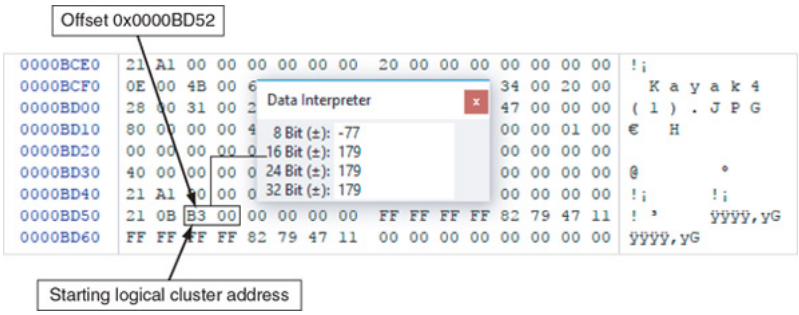
Figure 16-17.



Number of Clusters in the First Data Run

2. Next, you determine the starting logical cluster address (also called "logical cluster number," or LCN) for this data run. Place the cursor at offset **0000BD52** (see Figure 16-18). This logical cluster address is 2 bytes long (16 bits). Record the 16 Bit (±) value in the Data Interpreter window, which is 179.

Figure 16-18.



Starting Logical Cluster Address for the First Data Run

3. To compute the ending logical cluster address for this data run, add the number of clusters you found in **Step 1**, minus one cluster, to the starting logical cluster address you found in Step 2. For this example, it's starting logical cluster address plus (number of clusters minus one cluster) equals the last cluster of the data run, or $179 + (11 - 1) = 189$. Leave WinHex running for the next activity.

Caution

Remember to subtract one cluster from the number of clusters in a data run. If you don't, the correct ending cluster address will have one too many clusters that belong to another file. Later in Hands-On **Project 16-1**, you learn how to carve data runs into segmented files and then append them to restore a file.

The file used in this example has only one data run, so carving simply requires copying data from its starting cluster position of 179 (the logical cluster address) to its ending cluster position of 189. For files with multiple virtual cluster numbers (VCNs), additional data runs are listed in the file's MFT record.

Note

Typically, disk drives that haven't been defragmented have large files fragmented into one or more data runs.

Carving Data Run Clusters Manually

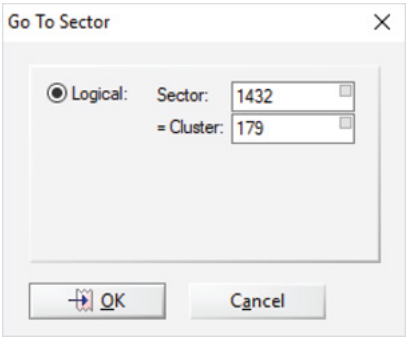
Now that you have calculated the starting and ending cluster positions for the Kayak4(1).jpg file, it's time to recover the fragments by using WinHex. To begin data carving, follow these steps:

Tip

The demo version of WinHex can save only files of less than 200 KB at a time. The licensed versions of WinHex and X-Ways Forensics have no limit on file sizes that can be saved.

1. In WinHex, click the **Drive G:** tab to access the entire drive, and then click **Navigation**, **Go To Sector** from the menu to open the Go To Sector dialog box. In the =Cluster text box, type **179** (see Figure 16-19), and then click **OK**.

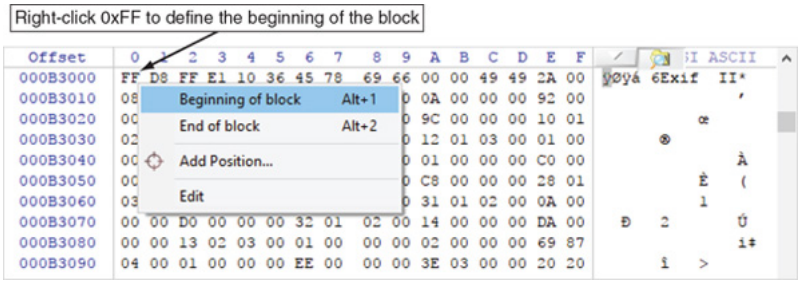
Figure 16-19.



The Go To Sector Dialog Box

2. In the hexadecimal pane, right-click the Kayak4(1).jpg file's first byte, at offset **000B3000**, and then click **Beginning of block** (see Figure 16-20) to mark the data run's starting position.

Figure 16-20.

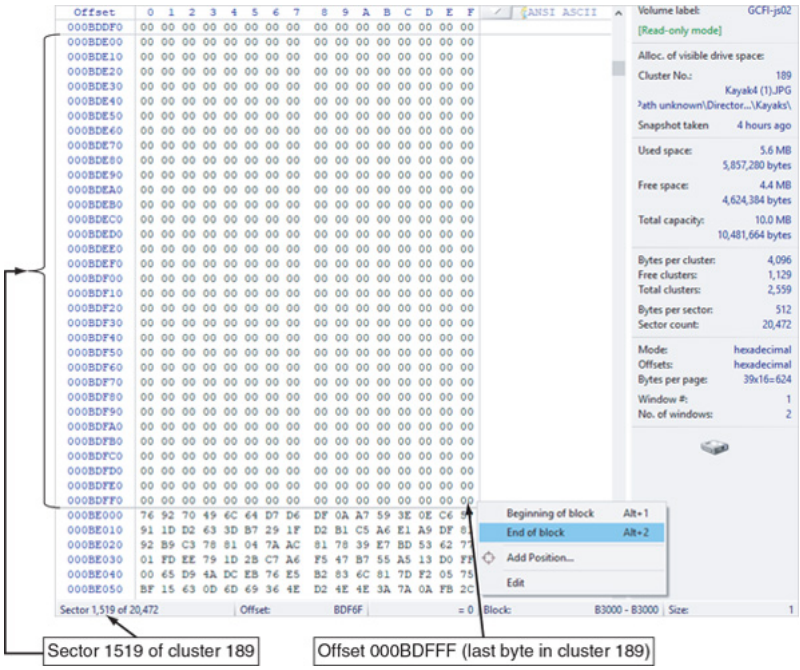


Marking the Beginning of the Block

3. Click **Navigation**, **Go to Sector** from the menu. In the =Cluster text box, type **189**, and then click **OK**.

4. **Step 3** positioned you at the beginning byte of the last cluster for this data run (offset 0000BD000). To mark the ending position for this data run, you need to include all the data in cluster 189. To do this, scroll down seven more sectors to offset 000BDFFF (the last byte in sector 1519). Right-click offset **000BDFFF** and click **End of block** (see Figure 16-21) to mark the data run's ending position.

Figure 16-21.



Marking the End of the Block

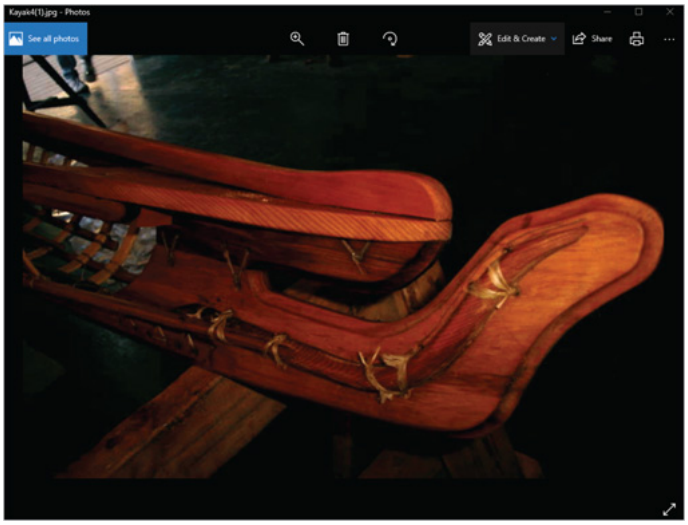
Note

In this forensic image, there are eight sectors per cluster. The last cluster of this data run starts at sector 1512 and ends at sector 1519.

5. Click **Edit** from the menu, point to **Copy Block**, and click **Into New File**. In the Save File As dialog box, navigate to and click your work folder, type **Kayak4(1).jpg** in the File name text box, and click **Save**.

6. To examine the carved Kayak4(1).jpg file, open it in File Explorer. Figure 16-22 shows the results. Exit WinHex.

Figure 16-22.



The Recovered Kayak4(1).jpg File

In your examination of Jim Shu's second disk drive, you found one folder that was bit-shifted. Based on your examination of the $MFT file, no other records seem to have been corrupted. Reviewing the files and folders listed show that there are no known applications, such as a hexadecimal editor, that could have altered data in the JShu folder. Without any evidence showing that the JShu folder was altered intentionally or by a virus, your report to Mr. Benson should state that the cause of the folder's corruption is unknown.

Chapter Summary

- Ethics can be defined as rules you internalize and use to measure your performance (internal standards) or standards that you're compelled to adhere to by external forces, such as licensing bodies (codes of professional conduct or responsibility). Laws governing codes of professional conduct or responsibility typically define the lowest level of action or performance required to avoid liability.
- Digital forensics examiners don't have the same formal, detailed codes of conduct that professions such as medicine and the law have, so relying on an internal code of ethics might be more critical. Additional sources include codes of professional associations you belong to, certifying bodies that have granted you a certification, and your employer's rules of professional conduct. Most examiners rely on a combination of these standards to construct their professional ethical codes.
- You owe your client a full understanding of the facts relevant to your opinion, and you can ask him or her to establish that there's evidence supporting the facts your opinion is based on.
- Be aware of attempts to disqualify you as an expert. Opposing counsel might attempt to disqualify you based on any deviations from opinions you've given in previous cases, so be prepared to explain the reason for any changes in your position. Some attorneys might contact you solely for the purpose of discrediting or disqualifying you (conflicting out). Always note calls from attorneys and the nature of the communication, and require that the attorney complete a client questionnaire and send you an investigation retainer.
- Courts use many factors in determining whether to disqualify an expert, such as whether an expert was formally retained and compensated, whether an expert was informed that discussions were confidential, and so on.
- Be aware of obvious ethical errors, such as ignoring contradictory data, performing work beyond your expertise or competence, allowing the attorney who hired you to influence your opinion improperly, and reaching a conclusion before completing your research.
- No single source offers a definitive code of ethics for expert witnesses, so you must draw on standards from other organizations to form your own ethical standards. Many professional organizations, such as the ABA and APA, have rules to guide their members in areas such as interaction with patients/clients, objectivity, role in society, fees, solicitation, independence, and contractual relationships.
- The International Society of Forensic Computer Examiners (ISFCE) Code of Ethics and Professional Responsibility provides guidelines for its members, and the International Association of Computer Investigative Specialists (IACIS) has a well-defined, simple guide for the expected behavior of forensics examiners.
- The inherent conflict between the needs of the justice system and your obligations for professional conduct can create ethical difficulties. With an adversarial legal system, pressures from hiring attorneys, and a tendency to identify with the side you're working for, maintaining impartiality can be difficult. Digital forensics examiners should consider their personal values, review the codes of conduct that apply to other professions, and develop a personal code of conduct that will protect them from ethical errors.
- The attorney who has retained you, opposing counsel, and the court owe you ethical responsibilities as an expert witness. For example, your attorney owes you a fair statement of the case or situation, adequate time to review evidence and prepare

your report, and a reasonable opportunity to examine data, conduct testing, and investigate the matter before rendering an opinion.

- As a forensics examiner, you deal with attorneys, so be aware of the basic rules of professional conduct they must follow. The American Bar Association is not a licensing body, but its Model Code of Professional Responsibility (Model Code) and its successor, the Model Rules of Professional Conduct (Model Rules), are the basis of state licensing bodies' codes.
- To give reliable and valid testimony, an expert has the ethical responsibility to present a complete, unbiased picture of the research related to the case. With an adversarial system, pressures from hiring attorneys, and a tendency to identify with the side you're working for, educating impartially is difficult.
- The attorney who has retained you, opposing counsel, and the court also owe you ethical responsibilities as an expert witness.
- The tools you use to recover, control, and track evidence are subject to review by opposing parties. If the court deems them unreliable, the evidence you recovered with those tools might not be admitted or be admitted with a limiting instruction. If you create tools for your own use, you must still validate them and submit them for review.
- After carving data artifacts, analyzing as much of the information as possible is critical. This information includes the create, modified, last access, and record timestamps in a recovered MFT record in addition to any recovered data runs. Collecting as many facts as possible provides more complete findings for your final report.

Key Terms

codes of professional conduct or responsibility
contingency fees
disqualification
ethics
orphan file

Review Questions

1. Describe two types of ethical standards.
2. Ethical obligations are duties that you owe only to others. True or False?
3. List three sound reasons for offering a different opinion from one you testified to in a previous case.
4. List three or more factors courts have used in determining whether to disqualify an expert.
5. All expert witnesses must be members of associations that license them. True or False?
6. Contingency fees can be used to compensate an expert under which circumstances?
    a. When the expert is too expensive to compensate at the hourly rate
    b. When the expert is willing to accept a contingency fee arrangement
    c. When the expert is acting only as a consultant, not a witness
    d. All of the above
7. List three organizations that have a code of ethics or conduct.

8. In the United States, no state or national licensing body specifically licenses forensics examiners. True or False?
9. When you begin a conversation with an attorney about a specific case, what should you do? (Choose all that apply.)
    a. Ask to meet with the attorney.
    b. Answer his or her questions in as much detail as possible.
    c. Ask who the parties in the case are.
    d. Refuse to discuss details until a retainer agreement is returned.
10. What purpose does making your own recording during a deposition serve?
    a. It shows the court reporter that you don't trust him or her.
    b. It assists you with reviewing the transcript of the deposition.
    c. It allows you to review your testimony with your attorney during breaks.
    d. It prevents opposing counsel from intimidating you.
11. Externally enforced ethical rules, with sanctions that can restrict a professional's practice, are more accurately described as which of the following?
    a. Laws
    b. Objectives
    c. A higher calling
    d. All of the above.
12. Describe an unethical technique opposing counsel might use to make a deposition difficult for you.
13. What are some risks of using tools you have created yourself?
    a. The tool might not perform reliably.
    b. The judge might be suspicious of the validity of results from the tool.
    c. You might have to share the tool's source code with opposing counsel for review.
    d. The tool doesn't generate reports in a standard format.
14. List four steps you should take, in the correct order, to handle a deposition in which physical circumstances are uncomfortable.
15. List three obvious ethical errors.
16. Codes of professional conduct or responsibility set the highest standards for professionals' expected performance. True or False?

Hands-On Projects

The following projects are a continuation of data carving from the in-chapter activity and case analysis of additional persons of interest developed from the **Chapters 14** and 15 projects. Before beginning these projects, create a *Work*\Chap16\Projects folder on your system (referred to as your "work folder" in steps). Download to this work folder all the files from this chapter's downloads section on the student companion site for this book.

Hands-On Project 16-1.

As you learned previously, Mr. Shu stated that a couple of JPG files with the name Kayak are on his second computer. For this project, you need the GCFI-js02.001 image you used in in-chapter activities. Follow these steps to carve the second orphan JPG file:

1. In File Explorer, double-click the **Ch16-Data-Carve.exe** file you downloaded and click **Extract** to extract the **Ch16-Data-Carve.xlsx** spreadsheet to your work folder.

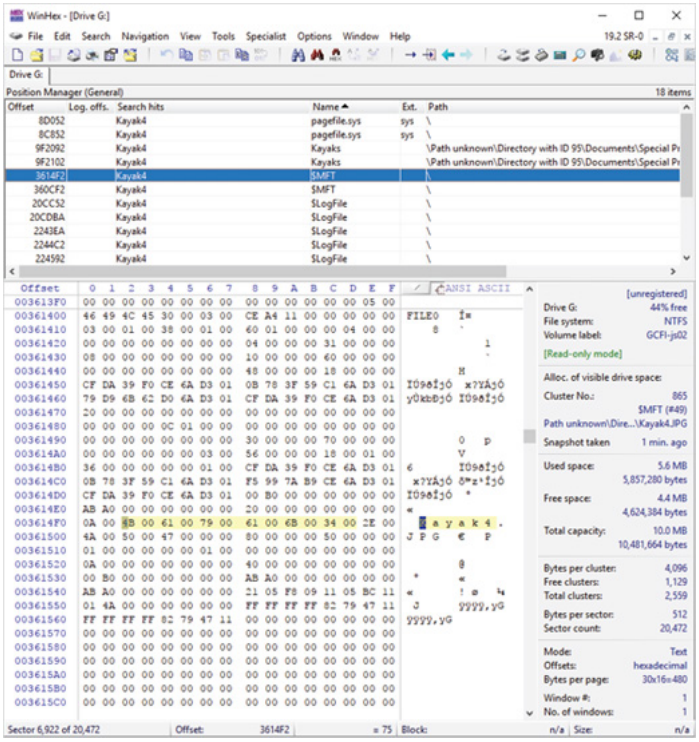
2. Start FTK Imager Lite, and click **File**, **Image Mounting** from the menu. In the Mount Image To Drive dialog box, click the **...** button next to the Image File text box, navigate to your work folder, click **GCFI-js02.001** , and then click **Open**. Click the **Mount** button, and keep this dialog box open. Remember to leave FTK Imager Lite running so that you can access this image as a mounted drive.

3. Start WinHex. Click **Tools**, **Open Disk** from the menu. In the Select Disk dialog box, click **GCFI-js02 (G:)**, and then click **OK**. (*Note*: Your drive letter might be different.)

4. Click **Search**, **Find Text** from the menu to open the Find Text dialog box. In the text box at the top, type **Kayak4**, click the **List search hits, up to** check box, and click **OK**. In the "Search complete" message box, click **OK**.

5. In the upper pane, click the **Name** column header once to sort alphabetically from A to Z, and then scroll down and click the row with the first occurrence of $MFT. Scroll up in the bottom pane to show FILE0 (see Figure 16-23).

Figure 16-23.



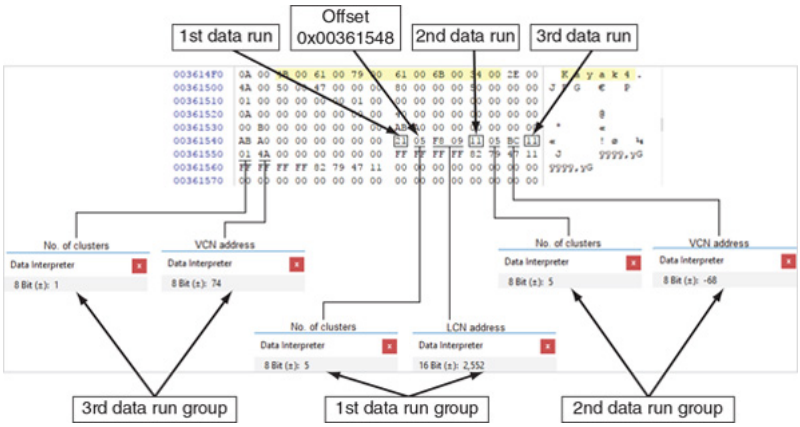
Search Results for the Keyword Kayak4

6. In the hexadecimal pane, start at the first byte of the record, offset **00361400**, and navigate to the last byte of the file header field, then the last byte of attribute 0x10, and then the last byte of attribute 0x30 to find the starting position for attribute 0x80 (offset 00361508). (For additional guidance on this step, see "Navigating Through an MFT Record" earlier in this chapter.)

7. Open the **Ch16-Data-Carve.xlsx** spreadsheet and enter the data run values.

8. In WinHex, find the first data run for this file (offset 00361548), and then place the cursor 1 byte to the right (offset **00361549**). Record the value shown for 8 Bit(±) in the Data Interpreter window. Figure 16-24 shows this file's data runs.

Figure 16-24.



The Data Run for the Kayak4.jpg File

9. In the **Ch16-Data-Carve.xlsx** spreadsheet, enter the LCN address **2552** in cell **B17**, and then type the first data run's number of clusters in cell **B18** (see Figure 16-25).

Figure 16-25.

	A	B	C	D	E
13					
14	HOP 16-1				
15	File:	Kayak4.jpg			
16		Cluster (Decimal Value)	Computed Logical Cluster Addresses	Navigate to Cluster	
17	LCN Address	2552	2552	2552	First Data Run Starting Cluster
18	No. of Clusters	5			
19	Last Cluster	2556	2556	2557	First Data Run Ending Cluster
20					
21	VCN Address		2552	2552	Second Data Run Starting Cluster
22	No. of Clusters				
23	Last Cluster		2551	2552	Second Data Run Ending Cluster
24					
25	VCN Address		2552	2552	Third Data Run Starting Cluster
26	No. of Clusters				
27	Last Cluster		2551	2552	Third Data Run Ending Cluster
28					

The Spreadsheet of the Data Run Cluster Addresses

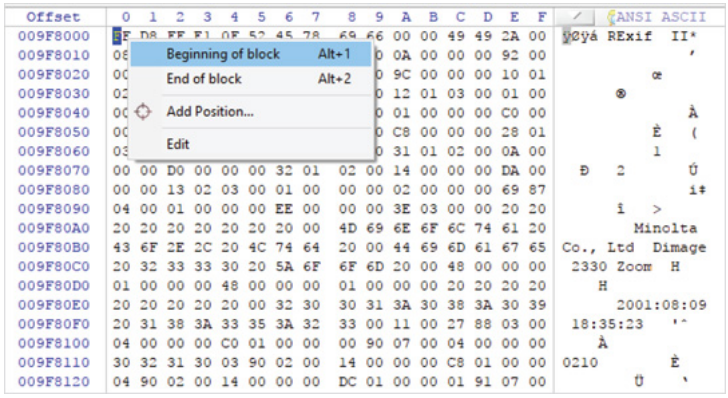
10. Repeat **Step 9** for the second and third data runs in cells **B21**, **B22**, **B25**, and **B26**.

Note

In this example, the second data run has the VCN value -68. When entering VCN values with minus signs in the Data Interpreter, be sure to include the minus sign in the spreadsheet cell to compute the correct starting cluster position.

11. In WinHex, click the **Drive G:** tab listing search results (substituting your drive letter, if needed), and then click **Navigation, Go To Sector** from the menu. In the Go To Sector dialog box, type the first data run's starting address, **2552** (listed in spreadsheet cell **D17**), in the =Cluster text box, and click **OK**. At the start of the cluster, right-click the first byte of the file header and click **Beginning of block** (see Figure 16-26).

Figure 16-26.

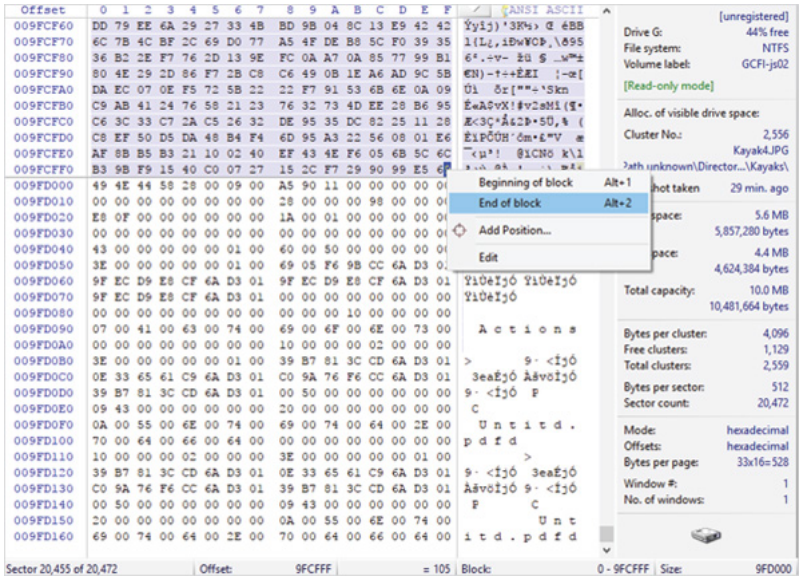


Source: X-Ways AG, www.x-ways.net

The Beginning Cluster Position for the Kayak4.jpg File

12. Click **Navigation, Go To Sector** from the menu. In the Go To Sector dialog box, type the first data run's ending address, **2557** (listed in spreadsheet cell **D19**), in the =Cluster text box, and click **OK**. To mark the ending block for the data run, scroll up one row in the lower pane, and then right-click offset **009FCFFF** and click **End of block** (see Figure 16-27).

Figure 16-27.



Source: X-Ways AG, www.x-ways.net

The Ending Cluster Position for the Kayak4.jpg File

13. Click **Edit** from the menu, point to **Copy Block**, and click **Into New File**. In the Save File As dialog box, navigate to and click your work folder, type **Kayak-dr1.jpg** in the File name text box, and click **Save**.

Caution ⚠

When marking the beginning and ending blocks, press the Esc key to avoid highlighting the entire image file after saving the data run.

14. Click the **Drive G:** tab listing search results (substituting your drive letter, if needed), and then click **Navigation, Go To Sector** from the menu. In the Go To Sector dialog box, type the second data run's starting address, **2484** (listed in spreadsheet cell **D21**), in the =Cluster text box, and click **OK**. At the beginning cluster, right-click the first byte of the file header and click **Beginning of block**.

15. Next, click **Navigation, Go To Sector** from the menu. In the Go To Sector dialog box, type the second data run's ending address, **2489** (listed in spreadsheet cell **D23**), in the =Cluster text box, and click **OK**. To mark the ending block for the data run, scroll up one row in the lower pane, and then right-click offset **009B8FFF** and click **End of block**.

16. Click **Edit** from the menu, point to **Copy Block**, and click **Into New File**. In the Save File As dialog box, navigate to and click your work folder, type **Kayak-dr2.jpg** in the File name text box, and click **Save**.

17. Click **Navigation, Go To Sector** from the menu. In the Go To Sector dialog box, type the third data run's starting address, **2558** (listed in spreadsheet cell **D25**), in the =Cluster text box, and click **OK**. At the beginning cluster, right-click the first byte of the file header and click **Beginning of block**.

18. Click **Navigation, Go To Sector** from the menu. In the Go To Sector dialog box, type the third data run's starting address, **2559** (listed in spreadsheet cell **D27**), in the =Cluster text box, and click **OK**. To mark the ending block for the data run, scroll up one row in the lower pane, and then right-click offset **009FE0FF** and click **End of block**.

19. Click **Edit** from the menu, point to **Copy Block**, and click **Into New File**. In the Save File As dialog box, navigate to and click your work folder, type **Kayak-dr3.jpg** in the File name text box, and click **Save**. Leave the spreadsheet open and WinHex running for the next steps.

Now that you've finished the first stage of carving orphan files from a disk drive, you can move on to the next stage of concatenating the data runs into one file. Follow these steps:

1. In WinHex, click **Tools** from the menu, point to **File Tools**, and click **Concatenate**. In the Select Destination File dialog box, navigate to and click your work folder, type **Kayak4.jpg**, and click **Save** to create the file where you're exporting data runs (the "target file").

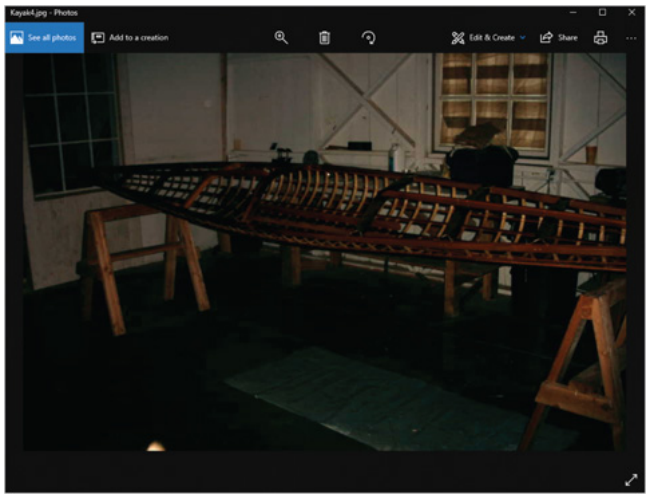
2. After you save the target file, the Choose Source File #1 dialog box opens. Click **Kayak4-dr1.jpg** and click the **Append** button to write the first data run to Kayak4.jpg, the target file.

3. Next, the Choose Source File #2 dialog box opens. Click **Kayak4-dr2.jpg** and click the **Append** button to add the second data run to the target file.

4. Next, the Choose Source File #3 dialog box opens. Click **Kayak4-dr3.jpg** and click the **Append** button to add the third data run to the target file. Click the **Done** button, and then click **OK** in the confirmation message box.

5. In File Explorer, navigate to your work folder and open **Kayak4.jpg** with your preferred graphics viewer to see whether the recovery was successful. Figure 16-28 shows the results you should get.

Figure 16-28.



The Recovered Kayak4.jpg File

6. Right-click the **Drive G:** tab and click Close, and then right-click the **$MFT** tab and click **Close**. Leave WinHex running for the next project.

7. Write a short memo to Mr. Benson stating that you used WinHex to recover the Kayak4.jpg file. Explain that this file had three data runs that were recovered successfully and added to a re-created file. Attach the recovered image to the memo, and submit both to your instructor.

Hands-On Project 16-2.

In Hands-On Project 16-1, you learned how to carve and recover the Kayak4.jpg file. For this project, you apply data-carving methods to another JPG file in the GCFI-js02.001 image: f003478.jpg. It's an orphan file, so you might not be able to recover it completely. Follow these steps:

1. Start WinHex, if necessary. Click **Tools, Open Disk** from the menu. In the Select Disk dialog box, click **GCFI-js02 (G:)**, and then click **OK**. (*Note*: Your drive letter might be different.) To find the $MFT record for the f003478.jpg file, click **Search, Find Text** from the menu to open the Find Text dialog box. In the text box at the top, type **f003478**, click the **List search hits, up to** check box, and then click **OK** twice.

2. In the search results, click **$MFT** and follow the same steps from Hands-On Project 16-1 to determine the data runs for attribute 0x80. Then open the **Ch16-Data-Carve.xlsx** spreadsheet to compute the data run's cluster addresses, starting at cell **B32** of the spreadsheet.

3. In WinHex, click **Navigation, Go To Sector** from the menu. In the Go To Sector dialog box, type the first data run's starting address (listed in spreadsheet cell D32) in the =Cluster text box, and click **OK**. At the start of the cluster, right-click the first byte of the file header and click **Beginning of block**.

4. Click **Navigation, Go To Sector** from the menu. In the Go To Sector dialog box, type the first data run's ending address (listed in spreadsheet cell D34) in the =Cluster text box, and click **OK**. To mark the ending block for the data run, scroll up one row in the lower pane, and then right-click the last byte of the cluster (listed in spreadsheet cell C34) and click **End of block**.

5. Click **Edit** from the menu, point to **Copy** Block, and click **Into New File**. In the Save File As dialog box, navigate to and click your work folder, type **f003478-dr1.jpg** in the File name text box, and click **Save**.

6. Repeat **Steps 3**, 4, and 5 for all remaining data runs listed in your spreadsheet; see cells D36 through D74 for starting and ending cluster addresses of each data run. For Step 5, increase the carved data run's filename by 1, such as f003478-dr2.jpg, f003478-dr3.jpg, and so on. When you have finished carving all data runs, save and close your spreadsheet.

After carving the orphan file f003478.jpg from the disk drive, concatenate the data runs into one file. Follow these steps:

1. Click **Tools** from the menu, point to **File Tools**, and click **Concatenate**. In the Select Destination File dialog box, navigate to and click your work folder, type **f003478.jpg** , and click **Save** to create the target file.
2. In the Choose Source File #1 dialog box, click **f003478-dr1.jpg** and click the **Append** button to add this data run to the target file.
3. Repeat **Step 2** to add the next six data runs to the target file. After you add the final data run, click **OK** in the warning message box about WinHex limitations. Click the **Done** button under the Append button, and then click **OK** in the confirmation message box.

Note

Remember to join the data runs in the same order they're listed in attribute 0x80.

4. In File Explorer, navigate to your work folder and open **f003478.jpg** with your preferred graphics viewer to see whether the recovery was successful. The photo has been only partially recovered because of the limitations in WinHex's demo version. Exit WinHex.
5. Write a short memo to Mr. Benson, stating that you used WinHex to recover the f003478.jpg file. Explain how many data runs are listed in the attribute 0x80 field and how many runs you were able to join. Attach the partially recovered photo and explain that the demo version of WinHex can recover only 200 KB of data. Submit the memo and attached photo to your instructor.

Hands-On Project 16-3.

In **Chapters 14** and 15, you examined Tom Johnson's and Jim Shu's forensic disk images. Information gathered from Jim Shu's e-mail indicates that he was selling intellectual property data to Terry Sadler. Ralph Benson, the general counsel for Superior Bicycles, Inc., has obtained through discovery a forensic image of Mr. Sadler's computer.

For this project, you use Autopsy to examine the forensic image of Mr. Sadler's computer and look at e-mails and any other files related to Superior Bicycles intellectual property. To view and export e-mails and attached files more easily, you use BitRecover Thunderbird Viewer, the tool you used in **Chapter 15**. After you've found and tagged all relevant files, use Autopsy's report generator to create an Excel spreadsheet listing your findings. Follow these steps:

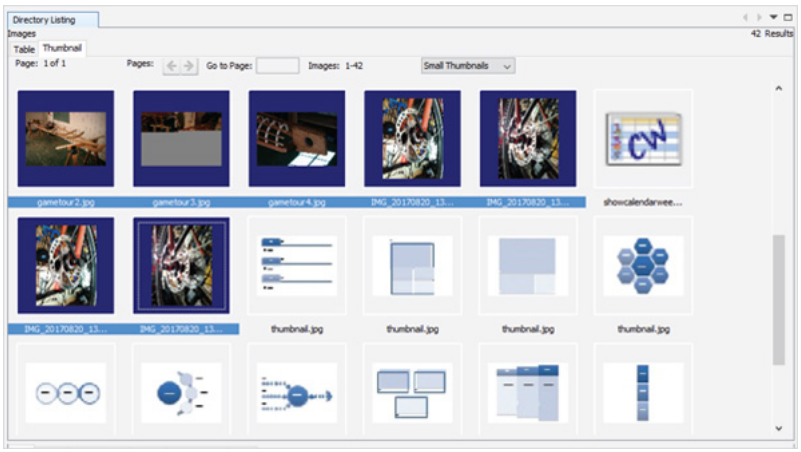
1. Download **Ch16Proj03.exe** from this chapter's downloads section on the student companion site for this book. In File Explorer, double-click the **Ch16Proj03.exe** file and click **Extract** to extract it to your work folder.
2. Start Autopsy for Windows, and click the **Create New Case** button. In the New Case Information window, enter **Proj1603** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**.
3. In the Additional Information window, type **Proj1603** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

4. In the Select Data Source window, click the **Browse** button next to the "Browse for an image file" text box, navigate to your work folder and click the **GCFI-ts01.001** file, and click **Open** and then **Next**.

5. In the Configure Ingest Modules window, click **Select All**. Click to clear the **SmutDetect4Autopsy** and **Virtual Machine Extractor** check boxes, click the **Process Unallocated Space** check box, and click **Next** and then **Finish**.

6. When Autopsy finishes its analysis, go to the Tree Viewer pane, click to expand **Views, File Types, By Extension,** and then click **Images**. In the Result Viewer pane, click the **Thumbnail** tab, scroll through the photos, and then Ctrl+click all whole or partial photos of bicycle components and kayaks (see Figure 16-29).

Figure 16-29.



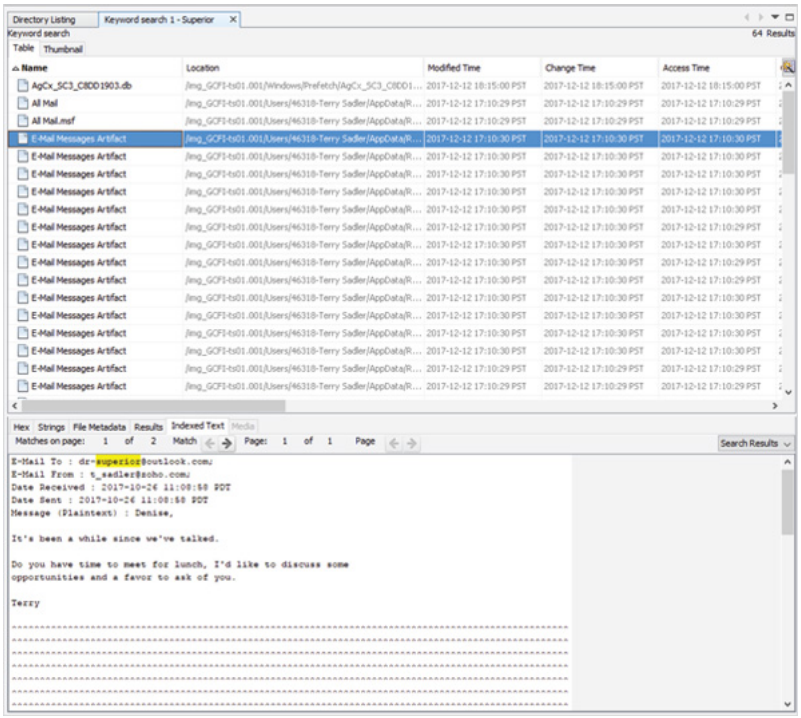
Tagging Bicycle and Kayak Photos

7. Right-click this selection, point to **Tag Files**, and click **Tag and Comment**. In the Create Tag dialog box, click the **New Tag Name** button, type **Possible Superior Bicycles evidence** in the Tag Name text box, and click **OK** twice.

8. In the Tree Viewer pane, click to expand **Results, Hash Hits,** and **Special Project-A**. In the Result Viewer pane, click the **Table** tab, then right-click the first **_S_p_e_c_i_a_l__P_r_o_j_e_c_t_-_A__(_2_)_._b_m_p_** file, point to **Tag Result** and **Quick Tag**, and click **Possible Superior Bicycles evidence**.

9. Click **Keyword Search**, type **Superior** in the text box, and then click **Search**. In the Result Viewer pane, click the **Keyword search 1 - Superior** tab, click the **Table** tab, and then click the **Name** column header to sort search results in alphabetical order (see Figure 16-30).

Figure 16-30.



The Keyword Search 1 - Superior Tab

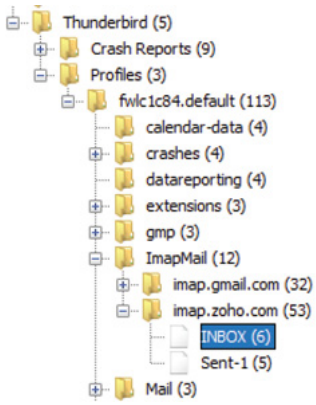
10. Read all e-mails with the name **E-mail Messages Artifact**. For e-mails in plaintext, right-click the e-mail, point to **Tag File** and **Quick Tag**, and click **Possible Superior Bicycles evidence**. Skip e-mails that are redundant or have no message body, such as coded HTML or message header data.

11. Click **Keyword Search**, type **Shu** in the text box, and then click **Search**. In the Result Viewer pane, click the **Keyword search 2 - Shu** tab, click the **Table** tab, and then click the **Name** column header to sort search results in an alphabetical order.

12. Read all e-mails with the name **E-mail Messages Artifact**. For all e-mails in plaintext, right-click the e-mail, point to **Tag File** and **Quick Tag**, and click **Possible Superior Bicycles evidence**. Skip e-mails that are redundant or have no message body, such as coded HTML or message header data.

13. In the Tree Viewer pane, click to expand **Tags**, **Possible Superior Bicycles evidence**, and **File Tags**. In the Result Viewer pane, right-click the first **Sent-1** and click **View File in Directory**. In the Tree Viewer pane, right-click the **INBOX** folder (see Figure 16-31) and click **Extract File(s)**. In the Save dialog box, click **Save**, and then click **OK**. Then right-click the **Sent-1** folder in the Tree Viewer pane and click **Extract File(s)**. In the Save dialog box, click **Save**, and then click **OK**.

Figure 16-31.



The INBOX Folder in the Tree Viewer

14. In the Tree Viewer pane, click to expand **imap.gmail.com** and **[Gmail].sdb**. In the Result Viewer pane, right-click **All Mail** and click **Extract File(s)**. In the Save dialog box, click **Save**, and then click **OK**.

15. Click **Generate Report**, and in the Generate Report window, click the **Results - Excel** option button in the Report Modules section, and then click **Next**. In the Configure Artifact Reports window, click the **Tagged Results** option button, click **Select All**, and then click **Finish**.

16. When the report has been generated, click the **Results - Excel** pathname in the Report Generation Progress window to view the report, and then exit Autopsy.

Next, you use BitRecover Thunderbird Viewer to find and copy all attachments from the e-mail folders you extracted in the previous steps. Follow these steps:

1. Start BitRecover Thunderbird Viewer. Click the **OPEN** toolbar button. In the Select File/Folder dialog box, click the **Select Folder** option button, click the **Open folder** icon, navigate to and click ***Work*\Chap16\Projects\Proj1603\Export**, and then click **OK** twice.

2. In the left pane, click the **all mail** folder. In the upper-right pane, scroll through the e-mails until you see one with a paper clip icon. Double-click that e-mail to open File Explorer.

3. In File Explorer, rename **message.eml** as **Attachment1-message.eml** , and then copy the contents of the **user\AppData\Local\Temp\bitrecovermbox** folder to your work folder's **Proj1603\Export** subfolder.

4. Repeat **Step 3** for each e-mail with a paper clip icon. Increment each new filename by 1, such as **Attachment2-message.eml** for the second message.eml file, **Attachment3-message.eml** for the third message.eml file and so on.

5. After extracting all relevant e-mails and attachments in the all mail folder, extract attachments from the inbox and sent-1 folders. When you're finished, exit BitRecover Thunder Viewer.

6. Examine the contents of each attachment and its associated e-mail, and then write a memo to Mr. Benson listing each e-mail and describing any attachments. Then submit the Autopsy report and memo to your instructor.

Hands-On Project 16-4.

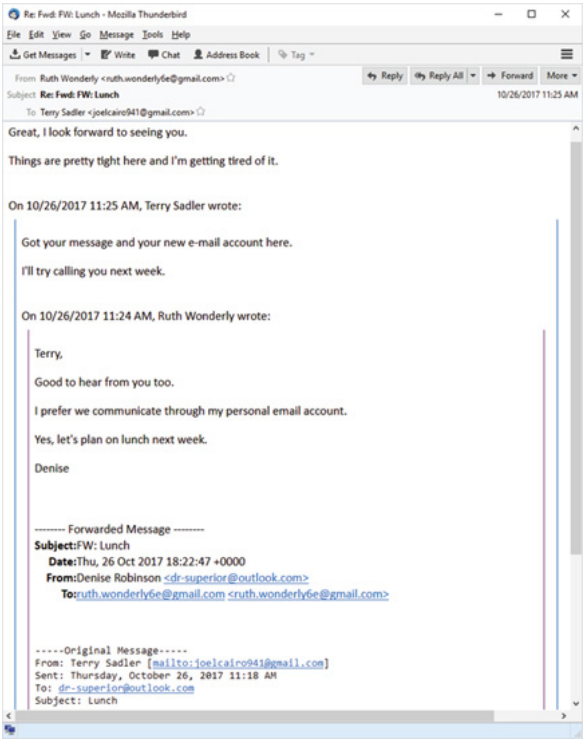
This project is a follow-up based on an e-mail found in the Excel report from Hands-On Project 16-3. Cell B66 of the report's E-Mail Messages worksheet lists an e-mail sent to Mr. Sadler from

the e-mail address dr-superior@outlook. com on October 27, 2017, at 11:59:52 a.m. PDT. This e-mail address belongs to Denise Robinson, the Human Resources manager at Superior Bicycles. Further examination of cell B77 shows another e-mail from ruth.wonderly6e@gmail. com that includes Denise Robinson's e-mail address in its contents. This e-mail was sent October 26, 2017, at 11:24:10 a.m. PDT.

Mr. Benson recalls seeing an e-mail from Ruth Wonderly on Tom Johnson's computer (see **Figure 14-6** or cell B140 of the Excel report for Hands-On Project 14-3). This e-mail was sent October 16, 2017, at 4:13 p.m. PDT. For this project, he wants you to confirm that the e-mails found in the forensic images of Mr. Johnson's and Mr. Sadler's computers are also in the forensic image of Denise Robinson's computer. Follow these steps:

1. Download **Ch16Proj04.exe** from this chapter's downloads section of the student companion site for this book. In File Explorer, double-click the **Ch16Proj04.exe** file and click **Extract** to extract it to your work folder.
2. Start Autopsy for Windows, and click the **Create New Case** button. In the New Case Information window, enter **Proj1604** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and then click **Next**.
3. In the Additional Information window, type **Proj1604** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.
4. In the Select Data Source window, click the **Browse** button next to the "Browse for an image file" text box, navigate to your work folder, click the **GCFI-dr01.001** file, and click **Open**. Click **Next**.
5. In the Configure Ingest Modules window, click **Deselect All**, and click the **Email Parser** check box. Click **Next** and then **Finish**.
6. In the Tree Viewer, click to expand **Results**, **E-Mail Messages**, **Default (Default)**, and **Default**. In the Result Viewer pane, click the **Date Sent** header once to sort e-mails from oldest to most recent. Scroll down and click the e-mail sent October 26, 2017, at or after 11:24 a.m. PDT from Terry Sadler to Denise Robinson's Ruth Wonderly account (see Figure 16-32).

Figure 16-32.



Terry Sadler's First E-mail to Denise Robinson

7. Right-click the e-mail, point to **Tag Results**, and click **Tag and Comment**. In the Create Tag dialog box, click the **New Tag Name** button, type **Recovered E-Mail** in the Tag Name text box, and click OK twice.

8. In the Result Viewer pane, click the **E-Mail From** header once to sort e-mails in alphabetical order. Scroll down and find all e-mails with the account name ruth.wonderly. Examine the contents of each e-mail. For all e-mails with the name Tom or Tom Johnson in the body of the message, right-click the e-mail, point to **Tag Results** and **Quick Tag**, and click **Recovered E-Mail**. Skip any redundant e-mails.

9. Click **Generate Report**. In the Generate Report window, click the **Results - Excel** option button in the Report Modules section, and then click **Next**. In the Configure Artifact Reports window, click the **Tagged Results** button, click **Select All**, and then click **Finish**.

10. When the report has been generated, click the **Results - Excel** pathname in the Report Generation Progress window to view the report, and then exit Autopsy. Turn the report in to your instructor.

Case Projects

Case Project 16-1.

Write a code of ethics for an organization you belong to or a school you attend, and explain the purpose of the code. Your code of ethics should have at least three items of expected ethical behavior.

Case Project 16-2.

Write a one- to two-page paper on the basic tenets of your personal ethical code and the sources your code is based on. It should be based on your personal experiences with ethical conflicts and how your understanding of ethics has played a part in your life.

Case Project 16-3.

Examine a code of ethics for a professional organization, business, or government agency, and write a critique of it. In your paper, determine the entity's priorities and whose interests the code serves.

Case Project 16-4.

Write an opinion paper of at least two pages describing your findings in the in-chapter activities and hands-on projects for Jim Shu's second computer. Review the contents of the files you extracted, and make your own conclusion as to whether the data was corrupted intentionally or by an unknown virus. Include the facts that support your opinion and explain how you arrived at this conclusion.

Lab Manual for Guide to Computer Forensics and Investigations

Introduction

The hands-on labs in this manual are designed to give you additional skills to reinforce the concepts covered in *Guide to Computer Forensics and Investigations, Sixth Edition*. Practicing these skills is necessary to become a digital forensics investigator. This book assumes a beginning to intermediate level of experience in operating systems and networking, and you should have experience in computer hardware equivalent to the coverage in the CompTIA A+ certification curriculum. If you don't have this background, reviewing a supplemental book, such as *A+ Guide to IT Tech Support,* by Jean Andrews, can help you understand the concepts and techniques in the labs.

Features

The labs feature step-by-step procedures with screenshots to illustrate many steps. They're designed to be finished within typical class periods. Each lab ends with challenging review questions that require you to analyze the evidence files. This lab manual works best in a classroom setting with an instructor or a facilitator to help guide you.

To help you understand digital forensics, this lab manual includes many features designed to enhance your learning experience:

- *Lab objectives*—Each lab has an introduction with background information, if needed, and a list of learning objectives.
- *Materials required*—Every lab includes information on hardware, software, and other materials you need to do the lab.
- *Completion times*—Every lab has an estimated completion time so that you can plan your activities more accurately.
- *Step-by-step instructions*—Logical step-by-step instructions guide you through the hands-on activities in each lab.
- *Review questions*—Questions help reinforce concepts covered in the lab.
- *Data files and software*—The data files available to be used in the labs are available for download. Several chapters include links to free and demo software to download for use with labs.

Additional Features

The following icons used in this book alert you to additional materials:

Note

The Note icon draws your attention to additional helpful material related to the subject being covered.

Tip

Tips based on the author's experience offer extra information about how to attack a problem or what to do in real-world situations.

Caution

The Caution icon warns you about potential mistakes or problems and explains how to avoid them.

Hardware Requirements

Use a standard installation of Windows 10. The computer running Windows should be a fairly current model that meets the following minimum requirements:

- USB ports
- CD-ROM/DVD-ROM drive
- VGA or higher monitor
- Hard disk partition of 500 GB or more
- Mouse or other pointing device
- Keyboard
- At least 6 GB RAM (more recommended)

For labs done in Linux, it's assumed you're using an Ubuntu 16.04 or later standard installation, although other Linux distributions will work with minor modifications. Some labs use specialized "live" Linux distributions, such as Kali Linux. The hardware requirements are as follows:

- A DVD or a USB drive of 6 GB or more
- Other hardware requirements are the same as those listed for Windows computers

Software Requirements

The following is a list of the freeware, shareware, and demo software used in this lab manual:

Note

Although efforts have been made to supply information that's current at the time of writing, Web site addresses change often, so search online to find the following software if URLs are no longer valid. Demoware tools typically have limited functions and strict time limits on their use. See their licensing information for restrictions.

Vendor	Tool	Version	License	Download Link
Igor Pavlov	7-Zip	18.04 beta	Freeware	www.7-zip.org
AccessData Group, Inc.	FTK Imager Lite	3.1.1	Demoware	https://accessdata.com/product-download/ftk-imager-lite-version-3.1.1
AccessData Group, Inc.	Registry Viewer	1.8.0.5	Demoware	https://accessdata.com/product-download/registry-viewer-1-8-0-5
Resin.io	Etcher	v1.4.4, 2018-04-24	Open-source	https://etcher.io/#downloads
mh-nexus	HxD	2.0 RC	Freeware	https://mh-nexus.de/en/downloads.php?product=HxD20
KRyLack Software	KRyLaCK Zip Password Recovery	3.70.69	Demoware	www.krylack.com/products/
Deft Linux	DEFT Zero	2017.1	Open-source	www.deftlinux.net/download/
Deft Linux	DART	v2-2014	Open-source	www.deftlinux.net/2014/04/16/deft-8-1-and-dart-2-2014/
Briggs Software	Directory Snoop	-	Demoware	www.briggsoft.com/
Kali.org	Kali	2017.3	Open-source	www.kali.org/downloads/

Vendor	Tool	Version	License	Download Link
PassMark	OSForensics	4.0.1002	Demoware (30-day free use limit)	www.osforensics.com/download.html
Reboot.pro	Mini-WinFE ISO	Mini-WinFE.2017.04.27	Freeware	http://reboot.pro/files/download/375-miniwinfe/
Sleuthkit.org	Autopsy	4.3.0	Open-source	https://sourceforge.net/projects/autopsy/files/autopsy/4.3.0/
Sleuthkit.org	Autopsy	4.7.0	Open-source	www.autopsy.com/download/
X-Ways	WinHex	19.5	Demoware	www.x-ways.net/winhex/
Mirek's Free Software	MWSnap 3.0.0.74	3.0.0.74	Freeware	www.tucows.com/preview/222629
Ted Smith	QuickHash	v3.0.2	Freeware	http://quickhash-gui.org/downloads/
Qt Company	SQL Lite	3.10.1	Freeware	http://sqlitebrowser.org
Parmavex Services	WinAudit	3.2.1	Freeware	www.parmavex.co.uk/winaudit.html

In addition, you use Microsoft Office Word, Notepad, and Excel (or open-source office software) and a Web browser.

Note

OSForensics from PassMark Software has a 30-day trial for download. If you aren't purchasing its license or are planning to do the labs at home, it's recommended that you wait until Chapter 8 or later to begin using this tool so that your trial doesn't expire before you finish the projects.

Classroom Setup Guidelines

This lab manual assumes Windows has been installed and doesn't require computers to be networked unless shared resources (such as printers), ExamView exams, or Internet access are needed. Lab managers can install the software in the preceding list ahead of time, if needed. As mentioned, some tools have time limits on their use, so plan lab assignments to make sure they can be done before licenses expire. Several labs use very large forensic images from 2 to 8 GB, and processing them might take up to 6 hours, depending on computer performance. Starting these labs before the end of the class day and allowing them to run overnight is the recommended method.

About the Author

Bill Nelson has worked for more than 32 years for two global Fortune 100 companies in information technologies, with more than 20 years in corporate digital forensics and information security. In addition, he has been an instructor of digital forensics classes at the City University of Seattle and the University of Washington's Professional and Continuing Education Department for 10 years. His previous experience includes Automated Fingerprint Identification System software engineering and reserve police work. Bill has served as president and vice president for Computer Technology Investigators Northwest. He routinely lectures at several colleges and universities in the Pacific Northwest.

Acknowledgments

I would like to thank the entire editorial and production staff for their dedication and fortitude during this project, including Natalie Onderdonk, Learning Designer, and Brooke Greenhouse, Content Manager. My special thanks go to Lisa Lord, the development editor, and I appreciate the careful testing of the technical editor, Danielle Shaw. I would also like to thank colleagues

in professional groups in Washington State, Mike Lacey for his photos, and the following digital forensics colleagues for their support and encouragement: Franklin Clark, retired investigator for the Pierce County Prosecutor's Office, Tacoma, Washington; John Sgromolo of Verizon; Stefan Fleischmann of X-Ways; Gordon Ross, formerly of Net Nanny; and Gordon Mitchell of Future Focus, Inc. In addition, my special thanks to colleagues Troy Larson of Microsoft and Brett Shavers. Finally, I want to express my appreciation to my wife, Tricia, for her support during the long hours spent writing.

Chapter 1. Understanding the Digital Forensics Profession and Investigations

Labs included in this chapter:

Lab 1.**1**. Installing Autopsy for Windows

Lab 1.**2**. Downloading FTK Imager Lite

Lab 1.**3**. Downloading WinHex

Lab 1.**4**. Using Autopsy for Windows

Note

Before starting this chapter, create a work folder for files you use in these labs, if you haven't done so already. You might want to name it "Lab" to differentiate it from your work folder for textbook projects. Then create a subfolder of your work folder named Ch01. In labs, you'll see it referred to as "*Work*" or "your work folder."

Lab 1.1. Installing Autopsy for Windows

Objectives

After completing this lab, you will be able to:

- Install Autopsy for Windows
- Explain Autopsy's features that help forensics investigators recover digital evidence

Investigating digital evidence takes time because of the large storage capacity of current hard disk drives. In addition, operating systems (OSs) and applications are typically large collections of files and executable programs that work together to form a user interface. Autopsy for Windows combines an extensive array of digital forensics tools into a single stand-alone software suite. It enables investigators to analyze storage devices; search for files, folders, e-mails, documents, pictures, and any remaining evidence that might have been deleted; and document their findings.

Forensics investigators need to search large volumes of data stored on different types of storage media, such as CDs and DVDs, USB drives, and hard disk drives, for potential digital evidence. In many criminal cases, the suspect might have attempted to delete a file or modify it in some way to prevent other users from seeing it. Autopsy can recover deleted or corrupted files and display the contents. Additional features, such as keyword searching, enable investigators to search for words related to the crime or number patterns that might reveal phone or credit card numbers. Autopsy also creates hash values for every file so that investigators can search for known file types, changed or altered files, malware, and legitimate application and OS files. File hashes are mathematically derived hexadecimal values that uniquely identify both known and unknown files. Hashing is an important feature because it preserves the chain of custody by making sure files haven't been altered or changed and recovered evidence doesn't change over time. Autopsy also enables you to import hash sets so that you can identify known files. One widely used hash set is the National Software Resource Library (NSRL), which contains known OS hash values. In this lab, you install Autopsy for Windows to begin investigating digital evidence.

Materials Required

This lab requires the following:

- The autopsy-4.3.0-64bit.msi file for 64-bit computers or the autopsy-4.3.0-32bit.msi file for 32-bit computers, downloaded in Step 1
- Windows

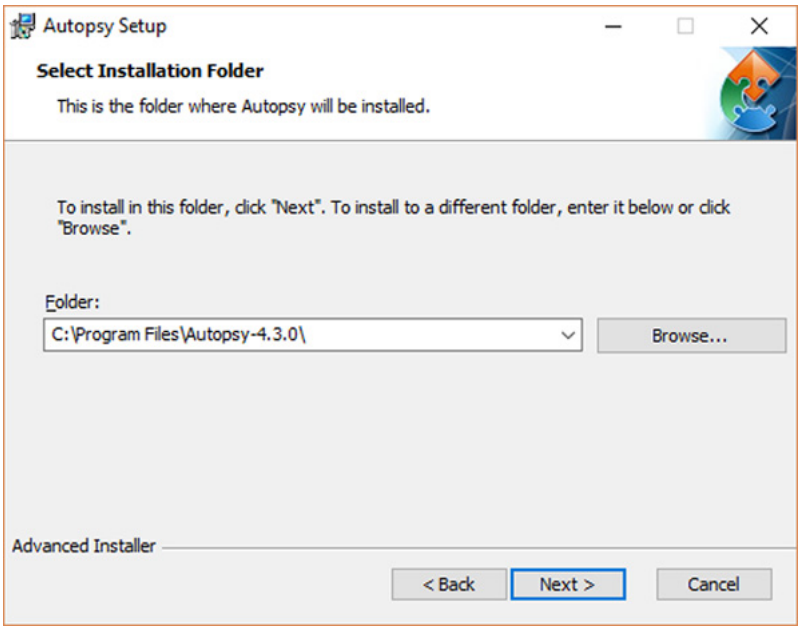
Estimated completion time: 10–15 minutes

Activity

In this lab, you install Autopsy for Windows:

1. Open File Explorer, and create a subfolder of your work folder called **Autopsy**. Start a Web browser, and go to https://sourceforge.net/projects/autopsy/files/autopsy/4.3.0/. Download the Autopsy installation file for your computer, listed in the "Materials Required" section, to your *Work*/Autopsy folder.
2. Open File Explorer, and navigate to your ***Work* /Autopsy** folder. Right-click **autopsy-4.3.0-*nn*bit.msi** (replacing *nn* with 32 or 64, depending on your computer) and click **Install** to begin the installation. If prompted with the User Account Control (UAC) message box, click **Yes** to continue.
3. Click **Next** in the Autopsy Setup Wizard welcome window.
4. In the Select Installation Folder window, shown in **Figure 1-1**, click **Next** to continue.

Figure 1-1.



Source: www.sleuthkit.org

The Select Installation Folder window

5. In the Ready to Install window, click **Install** to continue the installation.
6. In the Completing the Autopsy Setup Wizard window, click **Finish**, and then exit Autopsy.

Review Questions

1. Why is Autopsy an important forensics tool?

a. It can be used to troubleshoot a computer.

b. It can be used to test a computer's operability.

c. It can be used to help digital forensics investigators find potential evidence.

d. It can be used to recover human DNA.

2. Autopsy can search for which of the following types of files? (Choose all that apply.)

   a. E-mail

   b. Graphics

   c. Deleted files

   d. Registry files

3. What's a file hash?

   a. A hexadecimal value obtained mathematically from a file

   b. The name of a software program's vendor or manufacturer

   c. The size of a computer's hard disk

   d. The file size of potential evidence

4. Which of the following statements is true?

   a. File hash information can be found in File Explorer.

   b. File hashes can verify that the chain of custody has been maintained.

   c. File hashes can indicate that software has been purchased legally.

   d. File hashing values aren't important to a digital investigator.

5. Autopsy can't recover deleted or corrupted files and display their contents. True or False?

Lab 1.2. Downloading FTK Imager Lite

Objectives

After completing this lab, you will be able to:

> - Download FTK Imager Lite to your computer
> - Explain the purpose of using an imaging tool to copy digital evidence

Forensics investigators must protect the integrity of digital evidence from the time it's seized until the end of the trial. This task, known as "maintaining the chain of custody," ensures that the original data hasn't been changed during the investigation. They duplicate digital evidence by using a bit-stream process called "imaging," which preserves the original evidence along with other system files and duplicates a storage device with files intact to another lab storage device.

Imaging makes it possible to examine the duplicated storage device without the risk of damaging potential evidence. This bit-stream process makes an exact byte-for-byte copy of the original storage device that preserves the physical and logical file locations and any unpartitioned space. This process is important because remnants of deleted files still exist on a storage device until they're overwritten during computer operations. These file remnants can be searched and repaired to recover deleted files and make them readable. Imaging also generates file hashes that can be used to identify potential evidence and validate its integrity throughout the investigation process.

FTK Imager Lite is a compact version of AccessData's commercial tool FTK Imager. It's designed to be run from most small storage devices, such as a small USB drive, or on any Windows computer. It can preview digital files to determine whether evidentiary data exists before starting an extensive investigation. If potential forensic data is found, FTK Imager Lite

can then forensically duplicate the storage device to process the data safely. It supports the following file systems: Microsoft FAT12, FAT16, FAT32, exFAT, and NTFS; Linux/UNIX Ext2, Ext3, Ext4, and ReiserFS3; macOS Apple File System (AFS), HFS, and HFS+; and CDFS and VxFS (used for CDs and DVDs). It can produce hard disk image formats supported by FTK: AccessData Logical Image (AD1), EnCase 6.12, Expert Witness (.E01), Linux dd, Symantec Ghost, ICS, SMART, and Advanced Forensics Format (AFF). Although FTK Imager can copy encrypted files, it can't actually decrypt them. In this lab, you download FTK Imager Lite to your computer. In Chapter 3 of the textbook, you install this software.

Materials Required

This lab requires the following:

- FTK Imager Lite, version 3.1.1, downloaded in **Step 1**
- Windows

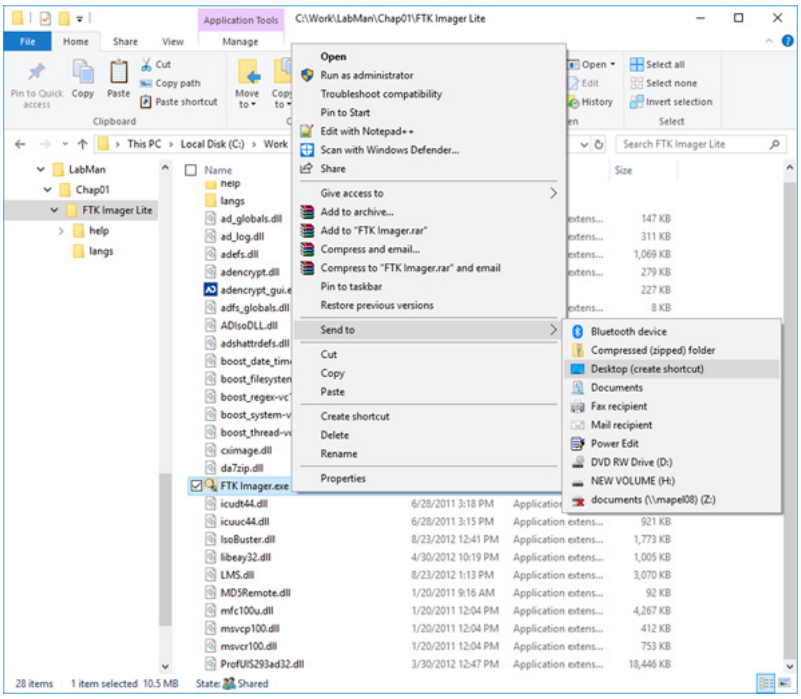
Estimated completion time: 10 minutes

Activity

In this lab, you download FTK Imager Lite from AccessData's Web site:

1. Start a Web browser, go to https://accessdata.com/product-download/ftk-imager-lite-version-3.1.1, and click **DOWNLOAD NOW**. Follow the instructions and fill out the registration form, including your personal e-mail address. Click the **Email Opt In** check box, and then click **Submit**.
2. In the e-mail from AccessData, click the **Download FTK Imager Lite 3.1.1** link to start the download. When the download is finished, navigate to your download folder in File Explorer. If necessary, copy or move **Imager_Lite_3.1.1.zip** to your work folder.
3. In File Explorer, create a subfolder of your work folder named **FTK_Imager_Lite**, and then extract the contents of the **Imager_Lite_3.1.1.zip** file to this subfolder.
4. Navigate to the **FTK_Imager_Lite** subfolder. Right-click the **FTK Imager.exe** file, point to **Send to**, and click **Desktop (create shortcut)**, as shown in Figure 1-2.

Figure 1-2.



Creating a desktop icon for FTK Imager Lite

5. Close File Explorer.

Review Questions

1. FTK Imager can be used to search all the following except what?
   a. Deleted files
   b. Documents
   c. Graphics
   d. Encrypted files
2. FTK Imager is used primarily to produce which of the following?
   a. Hard disk images that can be analyzed by forensics software
   b. Forensic evidence
   c. Device manufacturer information
   d. DNA evidence
3. Why do forensics investigators work with bit-stream images?
   a. Image files are smaller than the actual hard disk files.
   b. Only image files contain forensic evidence.
   c. An image file can be examined without damaging the original evidence.
   d. The original storage device can't be analyzed without the original computer.
4. FTK Imager can detect and view encrypted files. True or False?
5. Bit-stream imaging is the process of _____.
   a. Creating hash values from files on a storage device
   b. Extracting readable information from encrypted files

c. Duplicating data on storage devices for forensic analysis

d. Determining the forensic nature of digital evidence

Lab 1.3. Downloading WinHex

Objectives

After completing this lab, you will be able to:

- Download WinHex to your computer
- Explain the features of WinHex

Forensics investigators often use more than one forensics tool to analyze stored files and search for potential evidence. WinHex is a disk editor with several features that enable you to view and manipulate data at the byte and bit level. Although it isn't intended as a digital forensics tool, it offers advanced data interpretation and manipulation features. In this lab, you download WinHex, and you install it in **Chapter 5** of the textbook.

The licensed version of WinHex includes native support for all versions of FAT, NTFS, Ext2 through Ext4, Next3, and CDFS and UDF (used for CDs and DVDs). However, the evaluation version of WinHex can read *only* FAT12, FAT16, FAT32, exFAT, and NTFS. The licensed version also includes a RAM editor; a data interpreter that converts hexadecimal, decimal, and binary values; editing functions for data; file concatenating and splitting; several hashing algorithms for files; data recovery; searching capabilities for text or hex values; and more. In addition, this program and its associated files can fit on a USB drive, which enables you to run it in any Windows OS.

Note

The evaluation version of WinHex can write up to only 200 KB of data at a time. To have the capability of writing more than 200 KB of data, you need to purchase a licensed copy of this tool.

Materials Required

This lab requires the following:

- Windows
- WinHex (the most recent evaluation version, downloaded in **Step 1**)

Estimated completion time: 10 minutes

Activity

In this lab, you download WinHex:

1. Start a Web browser, go to http://x-ways.com/winhex/index-m.html, and click **Download**, as shown in Figure 1-3.

Figure 1-3.

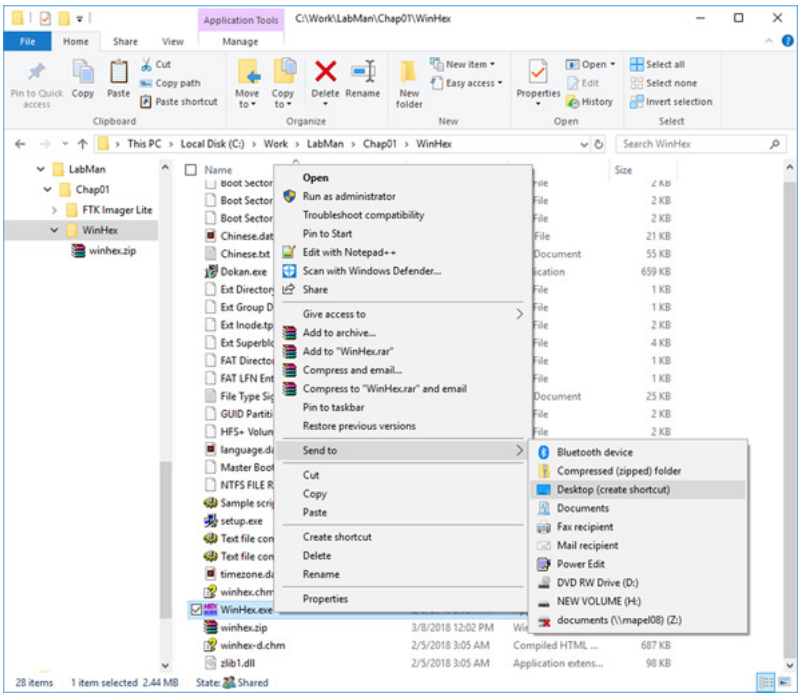
Source: X-Ways AG, www.x-ways.net

Downloading an evaluation copy of WinHex

2. When the download is finished, open File Explorer, and create a subfolder of your work folder named **WinHex**. Copy or move the **winhex.zip** file to this subfolder, and extract its contents to the same subfolder.

3. In File Explorer, navigate to the **WinHex** subfolder. Right-click the **winhex.exe** file, point to **Send to**, and click **Desktop (create shortcut)**, as shown in Figure 1-4.

Figure 1-4.



Creating a desktop icon for WinHex

4. Close File Explorer.

Note

To run WinHex from a USB drive, open File Explorer, and copy the contents of the WinHex subfolder to the USB drive. Then double-click WinHex.exe to start WinHex.

Review Questions

1. The evaluation version of WinHex can be used to search all the following file systems except which one?
   a. FAT16
   b. HFS+
   c. NTFS
   d. exFAT
2. The evaluation version of WinHex can write up to how many bytes of data?
   a. 200 KB
   b. 200 MB
   c. 2 TB
   d. An unlimited number of bytes
3. The licensed version of WinHex includes a RAM editor. True or False?
4. WinHex can't produce file hash values. True or False?
5. Which of the following statements is correct? (Choose all that apply.)
   a. WinHex has advanced data manipulation features.
   b. WinHex can't concatenate or split files.
   c. WinHex can't perform hexadecimal searches on a disk drive.
   d. WinHex includes hashing algorithms.

Lab 1.4. Using Autopsy for Windows

Objectives

After completing this lab, you will be able to:

> - Describe Autopsy's user interface
> - Explain Autopsy's menu options and screen configuration

Digital forensics tools can be intimidating to use. Even with the best instructions, learning how they work can be a challenge. Autopsy for Windows has been designed to make the user interface fairly easy to learn, but you might find some features difficult to understand, especially if you're new to digital forensics. The following lab gives you an overview of the features in Autopsy for Windows.

Materials Required

This lab requires the following:

- Completion of **Lab 1.1**
- Windows

> Estimated completion time: 30 minutes

Activity

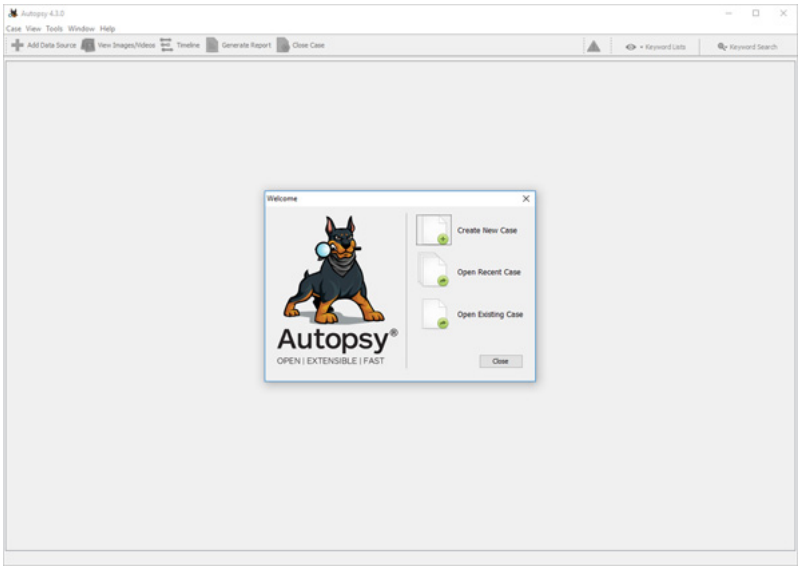
Tip

After completing this lab, if you're interested in learning more about Autopsy's features, see Autopsy User Documentation 4.3 at https://sleuthkit.org/autopsy/docs/user-docs/4.3. For additional instructions on using this tool, go to www.youtube.com and search for "autopsy for windows" to find the latest collection of how-to videos.

In this lab, you learn about menu options and window layouts in Autopsy for Windows. Note that you're not actually performing any steps in Autopsy. You simply read the steps and follow along with the figures:

1. Start Autopsy for Windows, which opens to the Welcome window shown in **Figure 1-5**. This window has three buttons you can choose from: Create New Case, Open Recent Case, and Open Existing Case.

Figure 1-5.

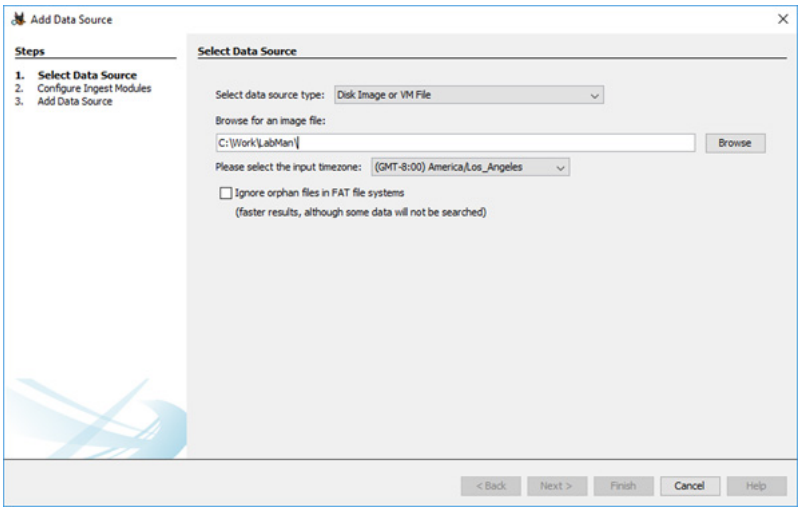


Source: www.sleuthkit.org

Autopsy's Welcome window

2. When you want to begin a new digital evidence analysis, you click the Create New Case button. Doing so starts the New Case Information Wizard, where you enter information about the case. **Figure 1-6** shows the Select Data Source window.

Figure 1-6.

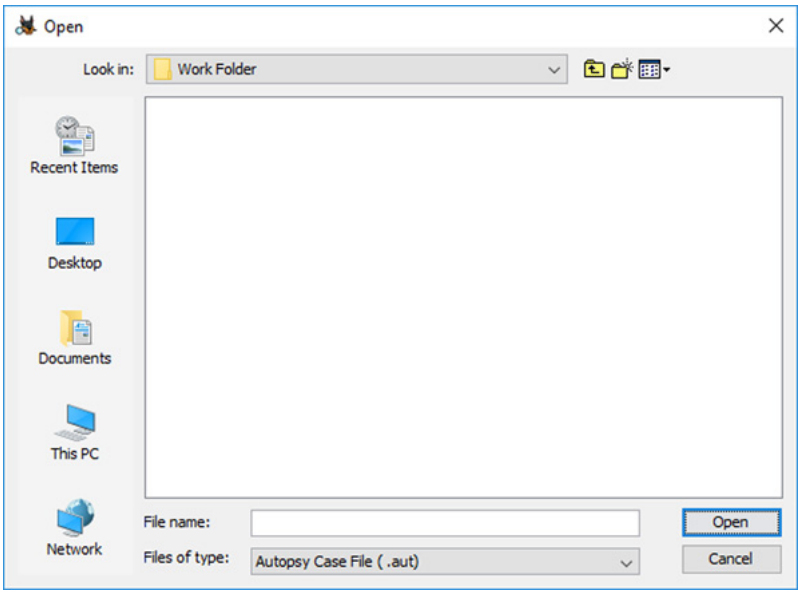


Source: www.sleuthkit.org

The Select Data Source window

3. Clicking the Open Recent Case button displays up to five previous cases. You can select one and click Open to load the case into Autopsy. Clicking the Open Existing Case button enables you to navigate to the folder containing a previous case that isn't listed in the Open Recent Case window. All Autopsy case files have an .aut extension, as shown in Figure 1-7.

Figure 1-7.



Source: www.sleuthkit.org

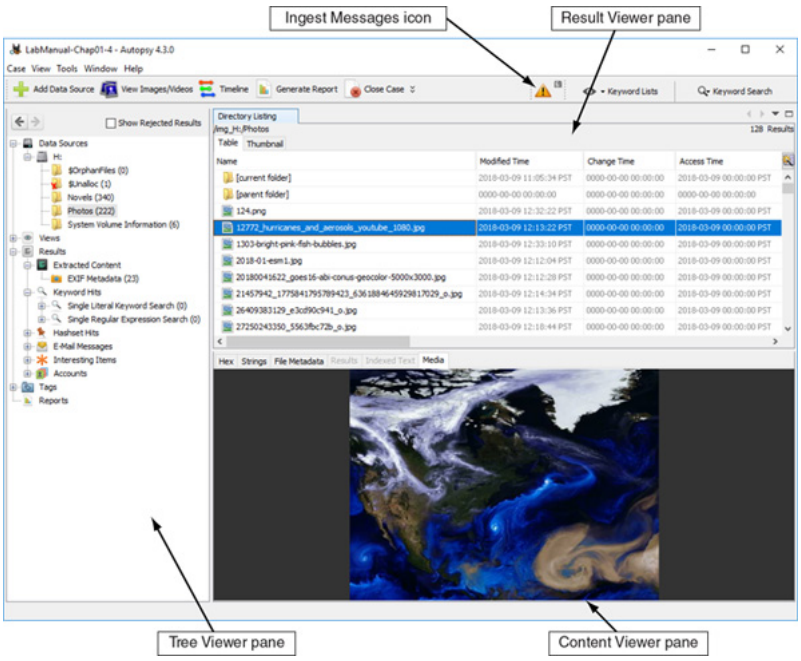
Loading a previous case into Autopsy

4. After you create or load a case into Autopsy, you see the main window, which is divided into three parts. The vertical pane on the left is the Tree Viewer. On the right, the upper pane is the Result Viewer, and the lower pane is the Content Viewer.

5. To expand or collapse items in the Tree Viewer, click the + or - symbol next to an item. Expanding a folder or drive displays its contents in the Result Viewer pane. To view a file's contents, click its filename in the Result Viewer pane, and the Content Viewer pane

displays the contents (see **Figure 1-8**). After you add digital evidence to a case, Autopsy automatically analyzes and catalogs files into different file types, such as photos in the Images folder or Microsoft Word files in the Documents folder. The files listed under the Views, Results, and Tags items are quick reference links to the same data shown under the Data Sources item. The Reports item stores links to all reports you have generated.

Figure 1-8.

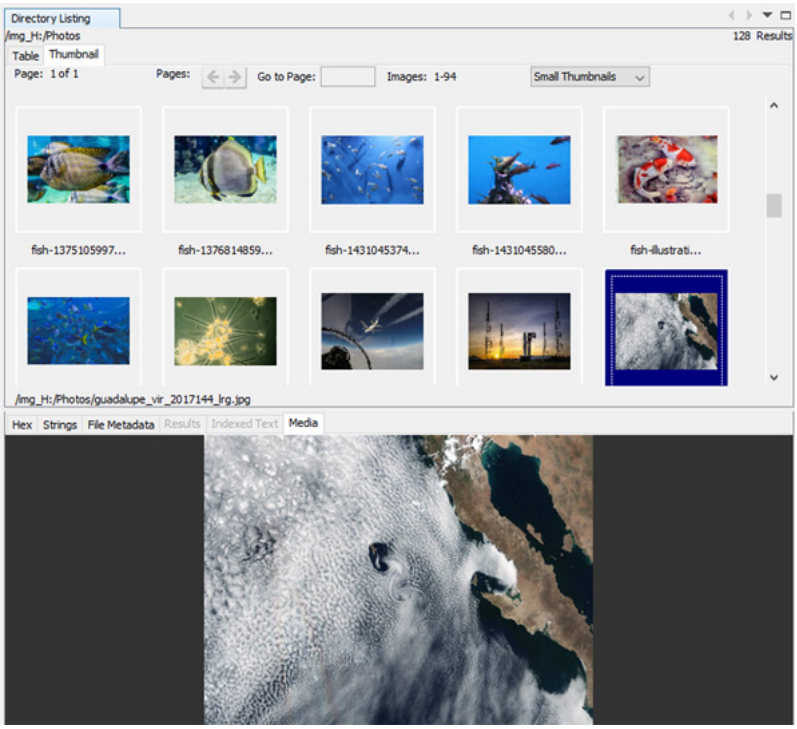


Source: www.sleuthkit.org

Autopsy's main window

6. The Result Viewer pane has a Table tab and a Thumbnail tab. The Table tab lists filenames in the folder you selected in the Tree Viewer. The Thumbnail tab displays thumbnail pictures of files. Clicking a thumbnail displays the full-size image in the Content Viewer (see **Figure 1-9**).

Figure 1-9.

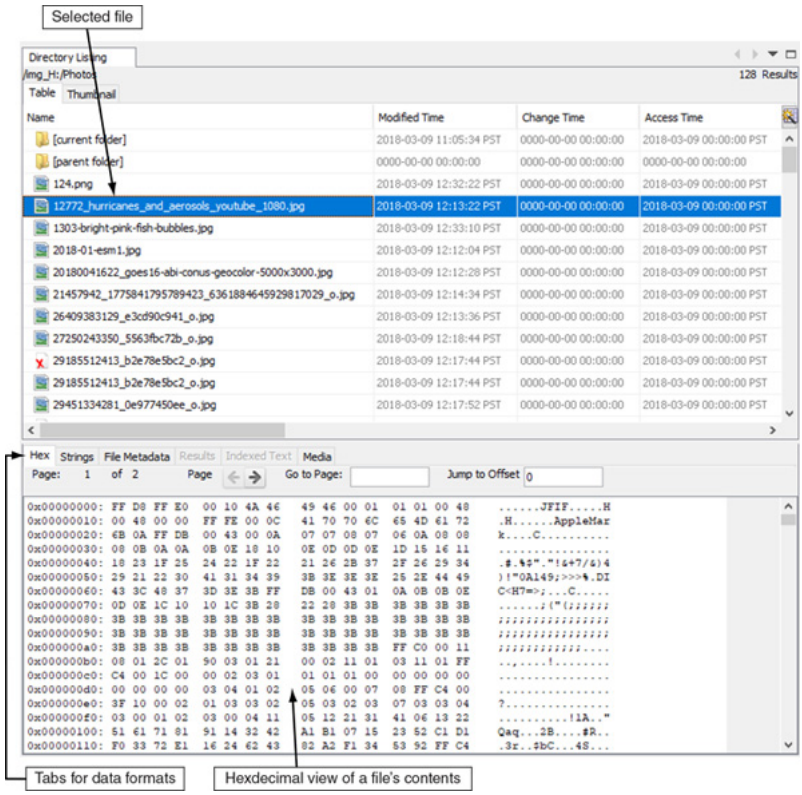


Source: www.sleuthkit.org

Viewing the Thumbnail tab

7. The Content Viewer pane shows the contents of a file selected in the Result Viewer pane. You can view the data in different forms by clicking the Hex, String, File Metadata, Results, Indexed Text, and Media tabs (see **Figure 1-10**). In this example, the Results and Indexed Text tabs are grayed out, which indicates no data result or index data is available for this file.

Figure 1-10.



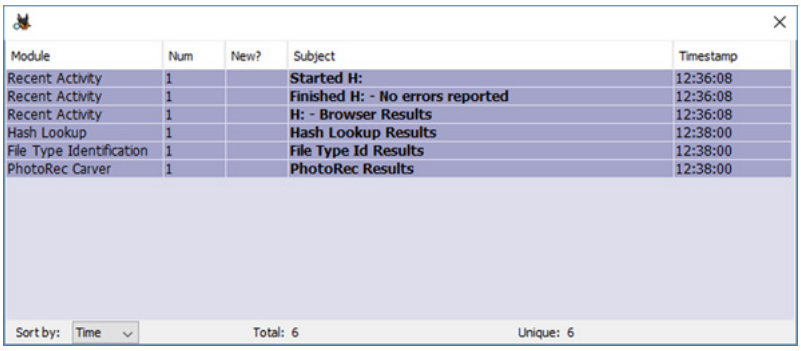
Source: www.sleuthkit.org

Tabs in the Content Viewer pane

8. The menu bar at the top of Autopsy's main window has many additional options. The two most common are Case and Tools. The first three options in the Case menu are identical to the buttons in the Welcome window. Additional options are Add Digital Evidence, View Case Properties, Close, and Exit Autopsy. The Tools menu has analysis options, such as Run Ingest Modules for performing specialized tasks, such as e-mail parsing and photo carving. Output from these tasks is saved under the Tree Viewer's Results item.

9. Immediately below the menu bar is a useful quick link bar for menu options you use more often. For example, the Ingest Messages icon shown in **Figure 1-8** can be used to view a log of Autopsy's activities (see Figure 1-11).

Figure 1-11.



Module	Num	New?	Subject	Timestamp
Recent Activity	1		Started H:	12:36:08
Recent Activity	1		Finished H: - No errors reported	12:36:08
Recent Activity	1		H: - Browser Results	12:36:08
Hash Lookup	1		Hash Lookup Results	12:38:00
File Type Identification	1		File Type Id Results	12:38:00
PhotoRec Carver	1		PhotoRec Results	12:38:00

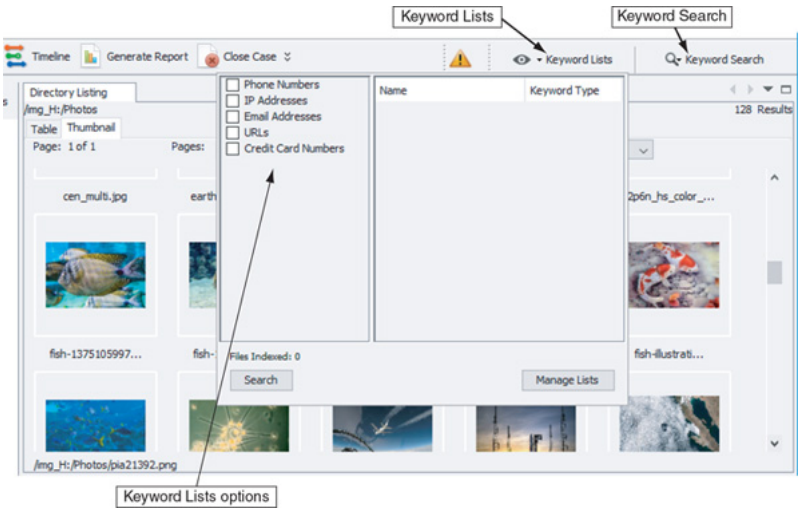
Sort by: Time Total: 6 Unique: 6

Source: www.sleuthkit.org

The Ingest Messages window

10. The quick link bar also has the Keyword Lists and Keyword Search options. As shown in **Figure 1-12**, the Keyword Lists feature has additional parameters, such as phone numbers, e-mail addresses, and credit cards. The Keyword Search feature is used to search for specific words. Results of both search types are stored under the Tree Viewer's Results item.

Figure 1-12.



Source: www.sleuthkit.org

Options for searching keywords

Review Questions

1. The Result Viewer pane in Autopsy displays which of the following?
   a. File contents
   b. Folder names, filenames, and dates
   c. Log data about Autopsy's activities
   d. Timelines of file accesses
2. What type of information is displayed under the Data Sources item in the Tree Viewer?
   a. Folder names and pathnames
   b. Filenames and directory paths
   c. Sorted predefined files
   d. Cataloged file types
3. Which file extension is used for Autopsy case files?
   a. .atp
   b. .aup
   c. .apy
   d. .aut
4. The Ingest Messages window provides what information?
   a. File metadata that's also available in the Content Viewer
   b. A log of activities performed in Autopsy
   c. Timeline information about files listed in the Result Viewer
   d. A listing of predefined search values, such as e-mail addresses

5. The Keyword Lists feature offers which of the following search parameters? (Choose all that apply.)
    a. Phone numbers
    b. IP addresses
    c. Street addresses
    d. Credit card numbers

Chapter 2. The Investigator's Office and Laboratory

Labs included in this chapter

Lab 2.**1**. Wiping a USB Drive Securely

Lab 2.**2**. Using Directory Snoop to Image a USB Drive

Lab 2.**3**. Converting a Raw Image to an .e01 Image

Lab 2.**4**. Imaging Evidence with FTK Imager Lite

Lab 2.**5**. Viewing Images in FTK Imager Lite

Note

Before starting these labs, create a subfolder of your work folder named Ch02.

Lab 2.1. Wiping a USB Drive Securely

Objectives

After completing this lab, you will be able to:

- Wipe a storage device securely
- Explain the purpose of wiping a storage device

Sometimes data must be deleted from a storage device securely to prevent recovering sensitive or secret files. Simply deleting files isn't enough to remove file data because when a file is deleted from a storage device, only the pointer to the file location is removed. The Master File Table (MFT), which stores the physical location of files in the file system, is updated to reflect the free space. The MFT is a separate structure in the NTFS file system; it's not the Recycle Bin. File information might remain on a computer even if it has been deleted from the Recycle Bin. Therefore, deleted data might still exist on a computer until all remnants have been overwritten by new data.

Deleted files often aren't overwritten immediately, and forensics software can be used to recover file remnants and reconstruct an original file by a process known as "data carving." Unless remnants are overwritten with other data, there's no guarantee that the deleted files can't be retrieved and viewed. Therefore, secure destruction of digital data often requires writing a series of 0 or 1 bits to the storage device to overwrite any file remnants.

The National Institute of Standards and Technology (NIST) 800-88 standard requires seven wiping passes over existing data before it can be considered unrecoverable on storage devices. Directory Snoop, a demoware tool, includes a disk wipe feature designed to erase storage media completely; it conforms to NIST standards and prevents any forensic recovery. Before digital evidence can be copied to a storage device for forensic analysis, all previous data stored on the device must be erased completely. In this lab, you wipe data from a USB drive securely to prepare it for forensic imaging.

Materials Required

This lab requires the following:

- Windows
- Data files downloaded to your work folder from this chapter's downloads section in the MindTap
- A USB drive with at least 8 GB of storage containing data that can be erased
- Directory Snoop, downloaded in **Step 1**

Estimated completion time: 20–120 minutes, depending on the size of your USB drive

Activity

In this lab, you wipe the contents of a USB drive with Directory Snoop:

Caution

This lab deletes all data on your USB drive and makes it unrecoverable. Make sure you're using a USB drive with data you don't need to keep.

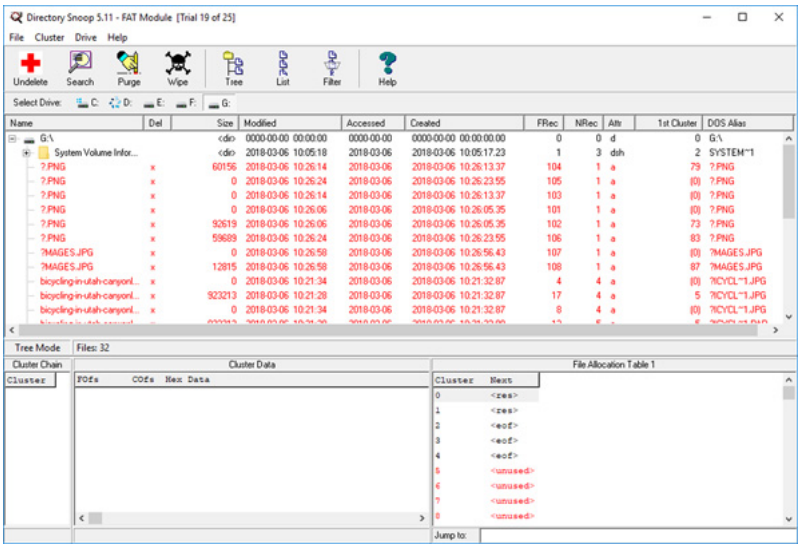
1. Start a Web browser, and go to www.briggsoft.com. Download the current version of Directory Snoop to your work folder.
2. Open File Explorer, and navigate to the folder where you downloaded Directory Snoop. Right-click the **ds95.exe** file and click **Install**. In the UAC message box, if prompted, click **Yes** to continue.
3. In the Welcome to the Directory Snoop Setup Wizard window, click **Next**. In the License Agreement window, click the **I accept the agreement** option button, and then click **Next**.
4. Click **Next** in the Select Destination Location, the Select Components, the Select Start Menu Folder, and the Select Additional Tasks windows.
5. In the Ready to Install window, click **Install** and then **Finish**.

Note

Directory Snoop has two versions: one for NTFS and one for FAT. After you've installed it, your desktop will have two icons, DS-NTFS and DS-FAT. For the following steps, it's assumed you're using a USB drive formatted as FAT. If you're using an NTFS-formatted USB drive, make sure you use the DS-NTFS icon in Step 8 to start Directory Snoop.

6. Log on to your computer, and insert a USB drive containing files you don't need.
7. Start File Explorer, and navigate to the USB drive. Ctrl+click to select all files and folders on the drive, and then click **Delete** on the toolbar.
8. Start Directory Snoop. If necessary, click **Yes** in the UAC message box.
9. On the Select Drive toolbar, click your USB drive (see **Figure 2-1**). (*Note*: Your USB drive letter, which is G in this figure, might be different from what's shown. Remember to verify that you're selecting the correct drive.)

Figure 2-1.



Source: Briggs Softworks, www.briggsoft.com

Selecting a drive in Directory Snoop

Note

The first time you run Directory Snoop, the RawDisk Driver dialog box opens. If you're running Windows 8 or later, click OK. If you're running Windows Vista or 7, click Install Driver, and then click the correct option button for your Windows OS in the Version dialog box. Click OK in the Information dialog box, and click OK in the RawDisk Driver dialog box.

10. To wipe all data, including deleted files, from the selected drive, click the **Wipe** toolbar icon, click **Free drive space** in the drop-down list, and click **OK** in the User Tip message box.

11. In the Wipe Free Space dialog box, click the **Simple 1-pass** option button, and then click **OK**. When the wiping is finished, click **OK** in the message box, and exit Directory Snoop.

12. In File Explorer, right-click the USB drive and click **Format**. In the Format dialog box, click **NTFS** in the File system list box, and type **EVIDENCE** in the Volume label text box. Click **Start** to format the USB drive. Click **OK** in the "Format warning" message box.

13. When the formatting is finished, click **OK** in the Formatting message box, and click **Close** in the Format dialog box. Copy the 11 data files you downloaded to this EVIDENCE USB drive. Label the USB drive, and don't write any more files to it.

14. Close any open windows, and leave your computer running for the next lab.

Review Questions

1. Which statement about deleted files is true?

   a. Deleted files can be rebuilt from remnants that haven't been overwritten.

   b. After a file has been deleted from the Recycle Bin, it can't be recovered.

   c. After a file pointer has been deleted in the MFT, it can't be recovered.

   d. The MFT isn't updated until all file remnants have been overwritten with new data.

2. When a file is deleted from a storage device, only the pointer to the file location is removed. True or False?

3. According to NIST standards, how many wipes should be done to erase data completely?

   Three

   One

   Two

   Seven

4. Which of the following statements about the MFT is true?

   The MFT is overwritten each time a file is deleted.

   The MFT is updated to indicate free space when files are deleted.

   The MFT and the Recycle Bin are the same file structure.

   The MFT isn't used in the NTFS file system.

5. Secure destruction of digital data requires doing which of the following?

   Overwriting the MFT

   Writing 0s and 1s to the storage device to overwrite file remnants

   Writing information in the MFT to file remnant locations

   Deleting files from the Recycle Bin

Lab 2.2. Using Directory Snoop to Image a USB Drive

Objectives

After completing this lab, you will be able to:

- Explain the purpose of disk imaging
- Make a bit-stream image of a USB drive or a similar storage device by copying all its clusters

When computers and devices are seized during a forensics investigation, the process of extracting information includes using disk imaging to make a bit-stream copy of the original storage media. Disk imaging builds forensically sound bit-for-bit copies of the evidence data, including the MFT with all physical file locations containing data or remnants and unallocated free space on the hard disk. After the original medium is duplicated, investigators can safely analyze the file structure and recover potential forensics evidence without the danger of destroying it during the process. Additionally, disk imaging maintains the chain of custody by protecting the evidence from any changes that might render it unusable in court.

Directory Snoop, a data recovery tool designed to work with FAT and NTFS file systems, can copy disk clusters to a raw format file (discussed in more detail in **Chapter 3** of the textbook). In this lab, you simulate seizing digital evidence on the USB drive you prepared in Lab 2.1 and create a raw format file (also known as a bit-stream image) of it. This process is the same procedure you follow during an actual investigation, except you use a write-blocker in actual investigations to prevent any changes to the original evidence during the acquisition. A write-blocker is a hardware or software component inserted between the original storage device and the computer creating the image to prevent what's on the original storage device from being overwritten, which violates the chain of custody.

Materials Required

This lab requires the following:

- Windows
- Directory Snoop
- The USB drive prepared in **Lab 2.1**

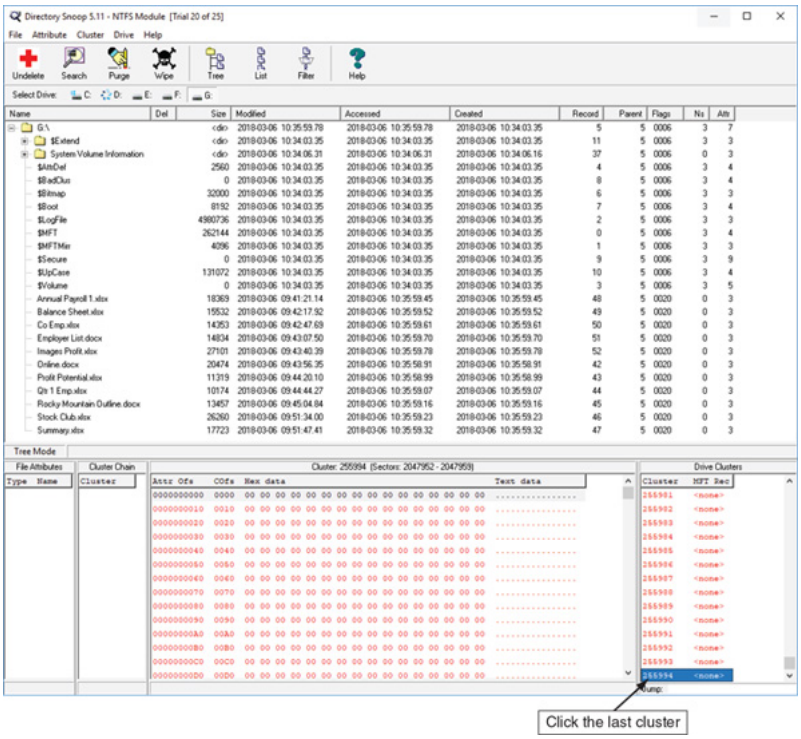
Estimated completion time: 10–20 minutes

Activity

In this lab you make a bit-stream image of the USB drive prepared in **Lab 2.1**. The Cluster, Copy to file menu option can be used to copy any cluster or group of clusters from a drive to a file. Follow these steps to make the bit-stream image:

1. Insert the USB drive containing evidence into your computer.
2. Double-click the **DS-NTFS** desktop icon to start Directory Snoop. On the Select Drive toolbar, click your USB drive.
3. Determine the drive's last cluster address by scrolling to the bottom of the cluster list in the Drive Clusters pane, and then click the last cluster, as shown in **Figure 2-2**.

Figure 2-2.

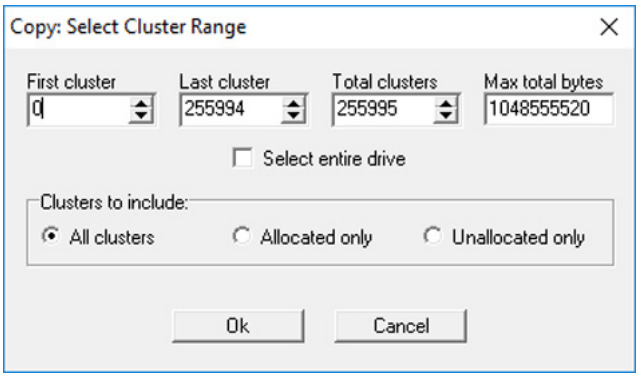


Source: Briggs Softworks, www.briggsoft.com

Selecting the last cluster in the Drive Clusters pane

4. Click **Cluster**, **Copy to file** from the menu. In the Copy: Select Cluster Range dialog box, notice that Directory Snoop automatically fills in the First cluster text box and the Last cluster text box with the last cluster address selected in Step 3. Delete the entry in the First cluster text box, type **0** (see Figure 2-3), click the **All clusters** option button, and then click **OK**.

Figure 2-3.



Source: Briggs Softworks, www.briggsoft.com

Entering the first cluster address

5. In the Select Target File dialog box, click **Browse**, and then navigate to and click your work folder. Type **C2Proj2.001** for the filename, and click **Save** and then **OK**.

6. When the copying is finished, click **OK** in the Information message box, and exit Directory Snoop.

Review Questions

1. Directory Snoop is designed to work with which of the following file systems? (Choose all that apply.)
   a. HFS+
   b. NTFS
   c. Ext4
   d. FAT

2. Disk images don't include the MFT. True or False?

3. Which statement about Directory Snoop's Cluster, Copy to file menu choice is true?

   It doesn't copy the MFT because it isn't needed during analysis.

   It copies all cluster data, including the MFT and unallocated free space, from the original storage device.

   It can copy all or specific clusters of a disk drive.

   It copies only data files; it doesn't include unallocated free space.

4. What's the purpose of a write-blocker?

   Preventing any data on the original storage device from being overwritten, which would violate the chain of custody

   Preventing any data from being written to the forensic image

   Creating file hash values

   Duplicating the MFT

5. What's the purpose of disk imaging? (Choose all that apply.)

   Allowing investigators to calculate hash values

   Giving investigators a way to analyze data without destroying potential evidence on the original medium

   Maintaining the chain of custody

Creating extra copies to share with other investigators

Lab 2.3. Converting a Raw Image to an .E01 Image

Objectives

After completing this lab, you will be able to:

- Describe FTK Imager Lite's conversion features
- Convert a raw format file to an .E01 format file in FTK Imager Lite

In **Lab 2.2**, you learned how to create a bit-stream image with Directory Snoop. Although Directory Snoop isn't a digital forensics tool, it's capable of capturing data in its raw form. It should be used only as an alternative acquisition tool if you're unable to run forensics acquisition tools. An example of when to use it is when your computer is running an older Windows OS version that can't run newer forensics acquisition tools.

One disadvantage of non-forensics acquisition tools is the lack of a feature for validating copied or compressed data. Forensics acquisition tools, such as FTK Imager Lite, typically run an MD5 or SHA-1 hash on acquired data to validate its authenticity. Another advantage of forensics acquisition tools is the capability to compress and split collected data into separate files. Splitting a forensic image into separate files enables you to store data on CDs, DVDs, or smaller USB drives. For more information on acquisitions and validating forensic imaging tools, see **Chapters 3** and 9 of the textbook. In this lab, you convert a raw format file to an .E01 format file that's compressed to reduce its size.

Materials Required

This lab requires the following:

- Windows
- FTK Imager Lite
- The C2Proj2.001 file created in Lab 2.2

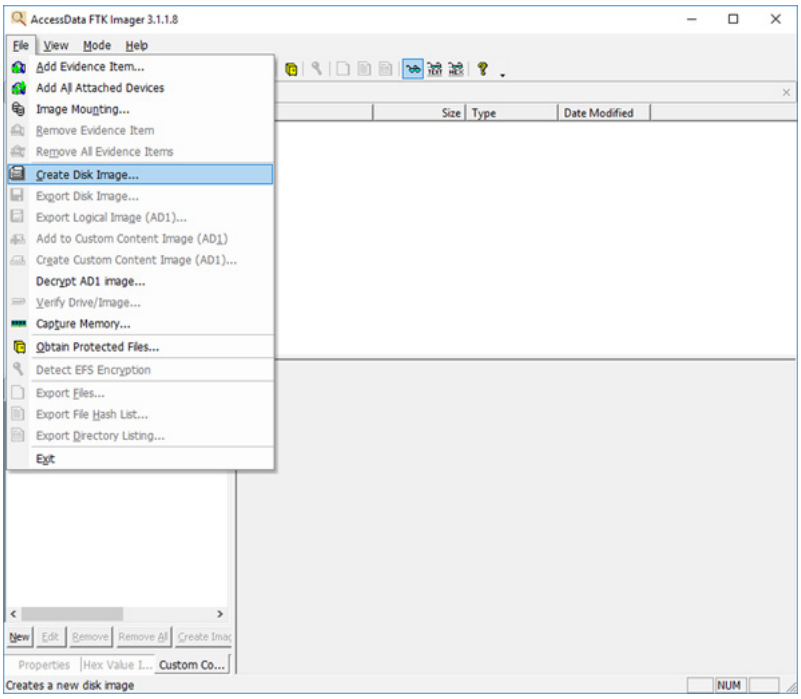
Estimated completion time: 5–15 minutes

Activity

In this lab, you convert the C2Proj2.001 image to the .E01 format:

1. Start FTK Imager Lite, and click **File**, **Create Disk Image** from the menu (see Figure 2-4).

Figure 2-4.

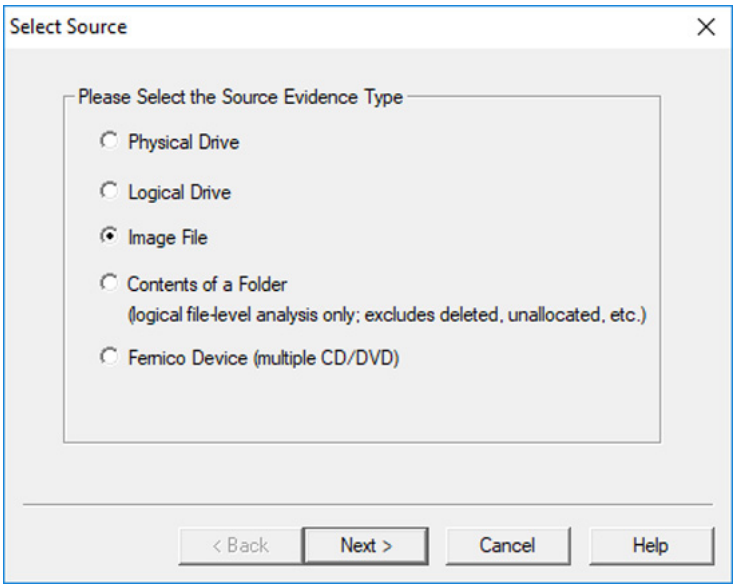


Source: AccessData Group, Inc., www.accessdata.com

The menu choice for creating an image

2. In the Select Source dialog box, click the **Image File** option button (see Figure 2-5), and then click **Next**.

Figure 2-5.



Source: AccessData Group, Inc., www.accessdata.com

Selecting the source to be imaged

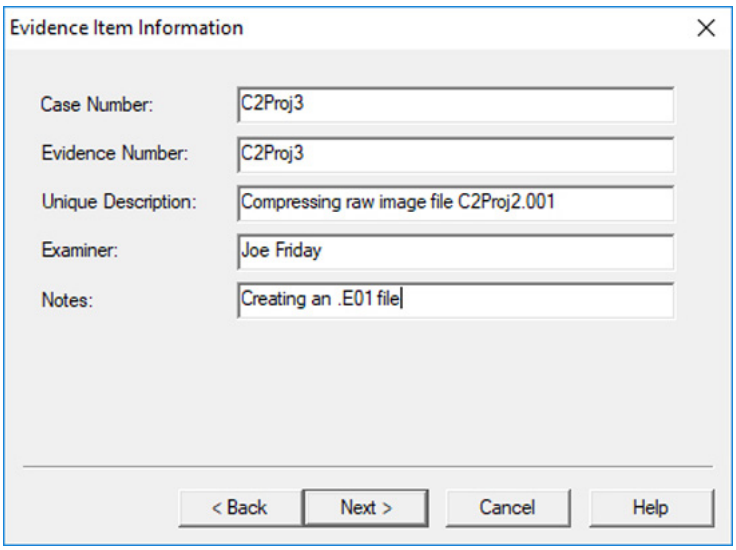
3. In the Select Drive dialog box, click the **Source Drive Selection** list arrow, click **Browse**, navigate to your work folder, click **C2Proj2.001** , click **Open**, and then click **Finish**.

4.

In the Create Image dialog box, click to select the **Verify images after they are created** check box, if necessary, and then click **Add**. In the Select Image Type dialog box, click the **E01** option button, and then click **Next**.

5. In the Evidence Item Information dialog box, type **C2Proj3** in the Case Number text box and the Evidence Number text box, type **Compressing raw image file C2Proj2.001** in the Unique Description text box, type your name in the Examiner text box, type **Creating an .E01 file** in the Notes text box (see Figure 2-6), and then click **Next**.

Figure 2-6.

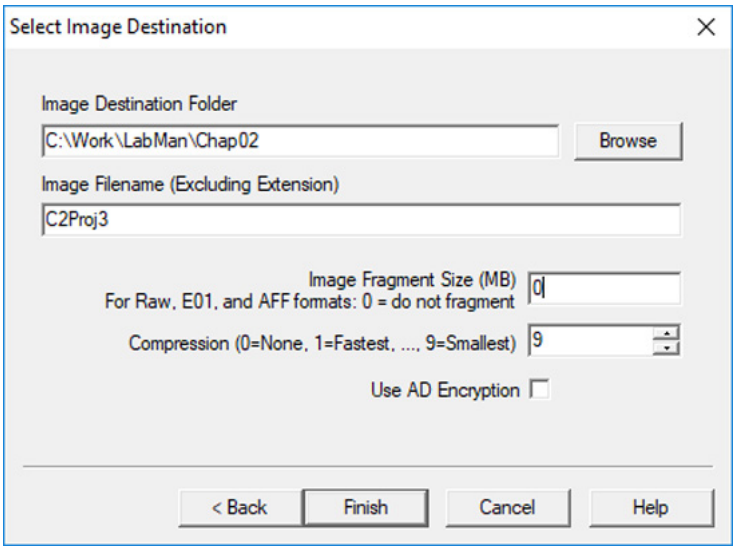


Source: AccessData Group, Inc., www.accessdata.com

Entering case information

6. In the Select Image Destination dialog box, click **Browse** next to the Image Destination Folder text box, navigate to and click your work folder, and then click **OK**. In the Image Filename (Excluding Extension) text box, type **C2Proj3**. In the Image Fragment Size (MB) text box, delete the current entry and type **0** (zero), as shown in Figure 2-7, and then click **Finish**.

Figure 2-7.



Source: AccessData Group, Inc., www.accessdata.com

Entering image destination information

7. In the Create Image dialog box, click to select the **Verify images after they are created** and **Create directory listing of all files in the image after they are created** check boxes, and then click **Start**.

8. When the imaging is finished, click **Close** in the Drive/Image Verify Results dialog box, and then click **Close** again in the Creating Directory Listing window.

9. Leave FTK Imager Lite running for the next lab.

Review Questions

1. What's the intended purpose of Directory Snoop?
   a. Its only purpose is for digital forensics use.
   b. Its primary purpose is for data recovery on disk drives.
   c. Its only purpose is to view files, much like File Explorer.
   d. Its only purpose is for data wiping.

2. Directory Snoop is capable of validating copied or compressed data. True or False?

3. What's the purpose of splitting a forensic image into smaller files?

4. A compressed .E01 image is the same size as the total size of all evidence files on the original source. True or False?

5. Forensics investigators should be familiar with more than one forensics acquisition tool in case a tool fails to run on their computer. True or False?

Lab 2.4. Imaging Evidence with FTK Imager Lite

Objectives

After completing this lab, you will be able to:

- List the image formats FTK Imager Lite supports
- Use FTK Imager Lite to image a USB drive

FTK Imager Lite creates bit-stream images in raw (.dd), SMART (.S01), and .E01 formats and enables investigators to extract Registry files from a Windows computer and import them into Registry-viewing tools, such as AccessData Registry Viewer, for recovering passwords or encrypted files.

FTK Imager Lite isn't optimized to search through large volumes of data to find evidence. Instead, it has verification features, such as MD5 and SHA-1 hashing calculations, to provide redundant verification that files haven't been altered during imaging. It does have some basic search features and can be used to look for deleted files or identify encrypted files. Because of its compact size, this tool can be placed on bootable removable media to make it portable. In **Chapter 3**, you learn how to create a forensic boot CD and USB drive that can be used to write-block a suspect hard drive. The forensic boot CD and USB drive enable you to make a bit-stream image with FTK Imager Lite. In this lab, you identify files that have been deleted on a USB drive.

Materials Required

This lab requires the following:

- Windows
- FTK Imager Lite
- The USB drive prepared in **Lab 2.1**

Estimated completion time: 30–40 minutes

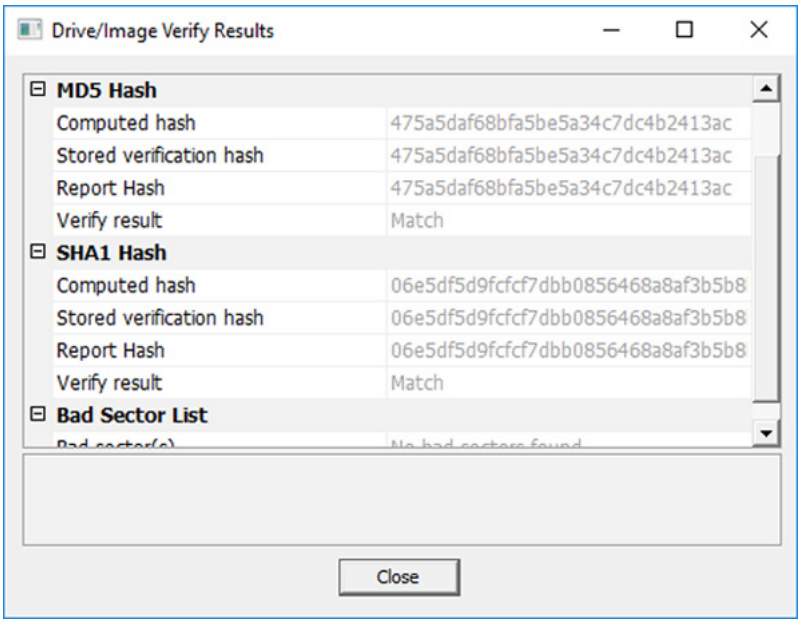
Activity

In this lab, you delete two files on the EVIDENCE drive you created in **Lab 2.1**, and then image the USB drive with FTK Imager Lite to produce an .E01 image:

1. Open File Explorer, and browse to the USB drive. Delete the **Qtr 1 Emp.xlsx** and **Online.docx** files on the USB drive, and then close File Explorer.
2. Start FTK Imager Lite. If the UAC message box opens, click **Yes**. Click **File**, **Create Disk Image** from the menu.
3. In the Select Source dialog box, click the **Logical Drive** option button, and then click **Next**.
4. In the Select Drive dialog box, click the **EVIDENCE [NTFS]** source drive in the drop-down list box, and then click **Finish** to continue.
5. In the Create Image dialog box, click **Add**. In the Select Image Type dialog box, click the **E01** option button, and then click **Next** to continue.
6. In the Evidence Item Information dialog box, type **C2Proj4** in the Case Number and Evidence Number text boxes and **Data recovery** in the Unique Description text box. Enter your name in the Examiner text box, type **USB image with deleted files** in the Notes text box, and click **Next** to continue.
7. In the Select Image Destination dialog box, click the **Browse** button, navigate to and click your work folder, and click **OK**. Type **C2Proj4** in the Image Filename (Excluding Extension) text box, and then click **Finish**.
8. In the Create Image dialog box, click **Start**. When the imaging process is finished, the results are displayed along with the computed MD5 and SHA-1 hashes (see Figure 2-8), which verify the forensic image's integrity. Click **Close** in the Drive/Image Verify Results

and Creating Directory Listing dialog boxes. The C2Proj4.E01 file is used in Lab 2.5. Leave FTK Imager Lite running for the next lab.

Figure 2-8.



Source: AccessData Group, Inc., www.accessdata.com

Verifying the results

Review Questions

1. FTK Imager Lite can produce all the following image formats except which one?
   a. .E01 (Expert Witness)
   b. .dd (raw)
   c. .S01 (SMART)
   d. .Ext4 (Linux)
2. Which of the following features isn't available in FTK Imager Lite?
   a. Creating images in raw and .E01 formats
   b. Being optimized to search large volumes of data
   c. Creating AFF image files
   d. Extracting Windows Registry files
3. FTK Imager Lite is designed to be portable. True or False?
4. FTK Imager Lite calculates which hash values during file imaging? (Choose all that apply.)
   MD5
   SHA-1
   DD5
   CRC-32
5. Why does FTK Imager Lite calculate two hash values?
   So that they can be read by older versions of Microsoft Office
   To provide redundant verification that files haven't been altered during imaging

For use in other forensics tools

None of the above

Lab 2.5. Viewing Images in FTK Imager Lite

Objectives

After completing this lab, you will be able to:

- View images in FTK Imager Lite for preliminary analysis
- Find deleted files and export them for further analysis

FTK Imager Lite has features that are useful for forensic analysis of disk images, such as calculating hash values and viewing file formats based on their file structures. You can also use this tool to search for existing and deleted files on disk images and view data in its readable state as well as hexadecimal bytes written to the disk. In addition, it displays information on physical and logical data blocks, including bad blocks and unallocated blocks; this information can be helpful in recovering deliberately corrupted disk partitions. This feature is also useful in narrowing the search scope for evidence because you can determine quickly whether any data has been deleted from a disk image. In this lab, you examine the C2Proj4.E01 image to find and export the two files that were deleted in Lab 2.4 before the USB drive was imaged.

Materials Required

This lab requires the following:

- Windows
- Microsoft Excel (or open-source spreadsheet software)
- FTK Imager Lite
- The C2Proj4.E01 image from Lab 2.4

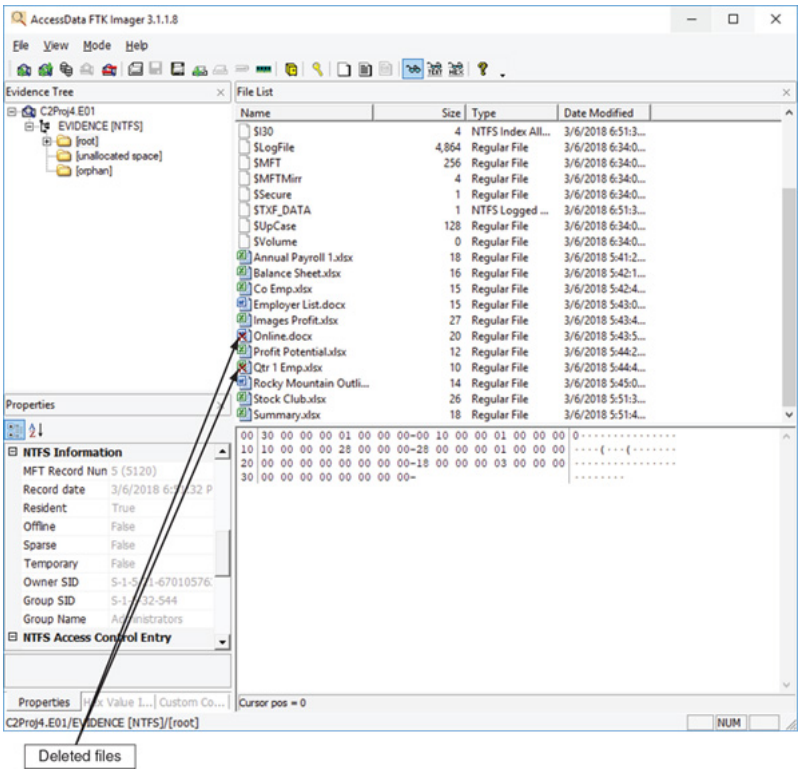
Estimated completion time: 10–15 minutes

Activity

In this lab, you use the USB image created in **Lab 2.4** to recover two deleted files:

1. Start FTK Imager Lite, if necessary, and click **File**, **Add Evidence Item** from the menu.
2. In the Select Source dialog box, click the **Image File** option button, and then click **Next**.
3. In the Select File dialog box, click **Browse**, navigate to your work folder, click the **C2Proj4.E01** file, and then click **Open**. Click **Finish**.
4. In the Evidence Tree pane, expand the **C2Proj4.E01**, **EVIDENCE [NTFS]**, and **[root]** folders, and then click the **[root]** folder to view the files on the imaged drive. Notice that the deleted Qtr 1 Emp.xlsx and Online.docx files display a red X in the File List pane (see Figure 2-9). FTK Imager Lite was able to recover these deleted files from the USB drive, even though they weren't visible in File Explorer.

Figure 2-9.

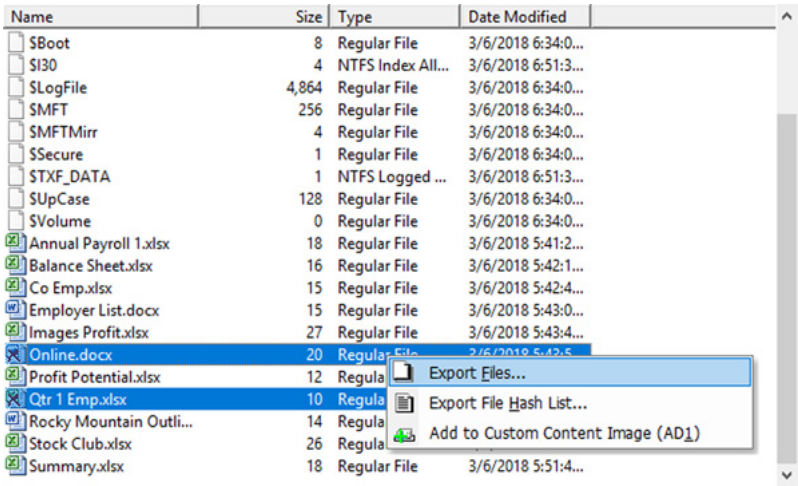


Source: AccessData Group, Inc., www.accessdata.com

Viewing deleted files

5. In the File List pane, Ctrl+click the **Qtr 1 Emp.xlsx** and **Online.docx** deleted files. Right-click this selection and click **Export Files** (see Figure 2-10).

Figure 2-10.



Source: AccessData Group, Inc., www.accessdata.com

Exporting deleted files

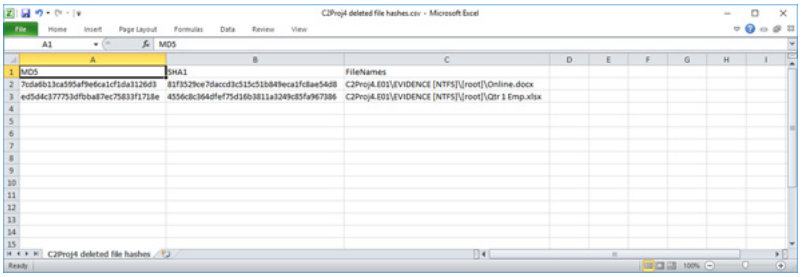
6. In the Browse For Folder dialog box, navigate to and click your work folder, click **OK** to export the files, and then click **OK** in the Export Results dialog box.

7. In the File List pane, Ctrl+click the **Qtr 1 Emp.xlsx** and **Online.docx** deleted files again. Right-click this selection and click **Export File Hash List**.

8. In the Save As dialog box, type **C2Proj4 deleted file hashes** in the File name text box, and then click **Save**.

9. Answer the following review questions, and when you're finished, exit FTK Imager Lite. In File Explorer, navigate to and click your work folder. Double-click the exported **C2Proj4 deleted file hashes.csv** file to open it in Excel. Review the spreadsheet listing the two deleted files and their MD5 and SHA-1 hashes. Expand the columns, if needed, to view the full hash values, as shown in Figure 2-11, and then exit Excel.

Figure 2-11.



Viewing deleted file hashes

10. In File Explorer, find the **C2Proj2.001** and **C2Proj2.E01** images. Notice that the image size of C2Proj4.E01 is much smaller than that of C2Proj2.001. FTK Imager Lite creates a compressed image and preserves all the evidence.

11. Close any open windows.

Review Questions

1. How many Excel files were recovered in the C2Proj4.E01 image?
   a. 3
   b. 7
   c. 11
   d. 4
2. How many deleted files were recovered in the C2Proj4.E01 image?
   a. 2
   b. 7
   c. 11
   d. 4
3. What's the filename of the deleted Excel file in the C2Proj4.E01 image?
   a. Annual Payroll 1.xlsx
   b. Profit Potential.xlsx
   c. Qtr 1 Emp.xlsx
   d. Online.xlsx
4. What's the name of the deleted Word file in the C2Proj4.E01 image?
   a. Employer List.docx
   b. Online.docx
   c. Rocky Mountain Outline.docx
   d. None of the above
5. How many SHA-1 hash files were exported to the C2Proj4 deleted file hashes.csv file?

a. Four

b. Two

c. One

d. None of the above

Chapter 3. Data Acquisition

Labs included in this chapter:

Lab 3.**1**. Creating a DEFT Zero Forensic Boot CD and USB Drive

Lab 3.**2**. Examining a FAT32 Image

Lab 3.**3**. Examining an NTFS Image

Lab 3.**4**. Examining an HFS+ Image

Note

Before starting these labs, create a subfolder of your work folder named Ch03.

Lab 3.1. Creating a DEFT Zero Forensic Boot CD and USB Drive

Objectives

After completing this lab, you will be able to:

- Create a DEFT Zero boot CD and USB drive
- Understand the basic functions of DEFT Zero

Bootable forensics tools can be useful when removing a computer or internal hard drives isn't practical because of a connection with networking components or because removing systems could disrupt an organization's business operations. (For a list of bootable forensics tools that run on CDs or USB drives, see **Chapter 3** of the textbook.) The advantage of using bootable forensics tools is that they contain just basic OS functions and utilities; because of their compact size, they can run in RAM on any computer. Their OS and utilities can be loaded into a RAM disk (a portion of computer memory allocated as a disk drive; see www.techopedia.com/definition/2801/ram-disk) on the host computer. System files, such as page or swap files, are also stored in RAM, which eliminates the need to use the suspect's computer's hard drive to make a forensics acquisition. Having acquisition tools on a boot CD or USB drive enables investigators to create forensic images of storage devices or hardware attached to computers or networks.

One of these bootable forensics tools, DEFT Zero, fits on a CD or small USB drive. It was created by Stefano Fratepietro, Alessandro Rossetti, and Paolo Dal Checco, Ph.D., of the DEFT Association (Digital Evidence and Forensics Toolkit). DEFT Zero is based on Lubuntu Linux and designed to run on both 32-bit and 64-bit platforms. It uses only 400 MB, making it ideal for running on new and older computers. It's packaged with a variety of tools, including forensics acquisition programs, such as Guymager (a Linux forensic imaging tool) and the command-line version of FTK Imager Lite. Using DEFT Zero on a suspect's computer prevents changes to log and OS files when the computer starts. After DEFT Zero has been booted, it enables you to mount the suspect disk drive manually as read-only and the target drive as read-write so that you can copy data to it. In this lab, you use DEFT Zero to build a boot CD and USB drive to perform forensics data acquisitions and access a suspect's drive without altering its contents.

Note

Before using DEFT Zero, review the end user license agreement in the DEFT Manual (available at www.deftlinux.net/deft-manual/). It states that DEFT Association products are noncommercial and free to the public and can't be used for commercial purposes.

Materials Required

This lab requires the following:

- A Windows computer with CD/DVD burning software
- A blank CD and two USB drives that are 1 GB or larger (formatted as exFAT)
- The deftZ-2017-1.iso file downloaded in the first section
- The Etcher-Setup-1.3.1-x64.exe or Etcher-Setup-1.3.1-x86.exe file, downloaded in the second section

Estimated completion time: 60–90 minutes

Activity

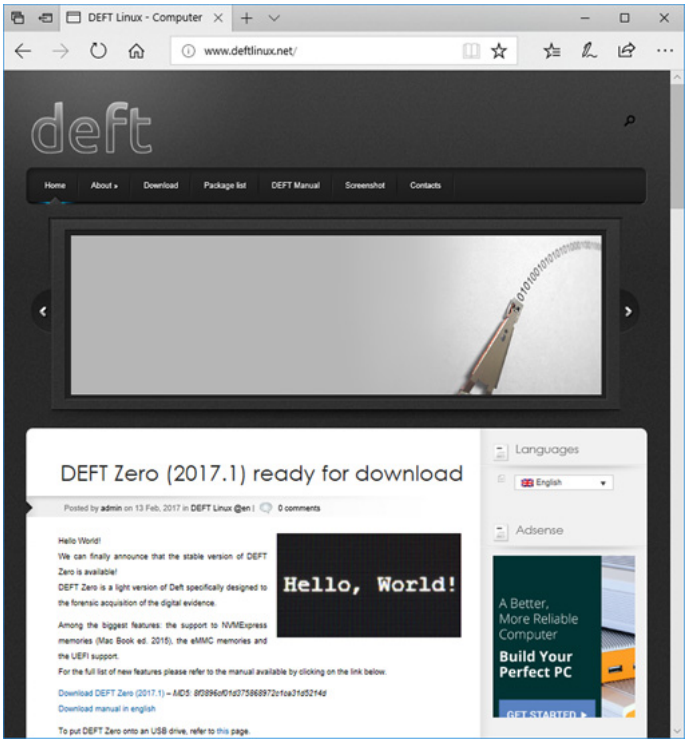
This lab is divided into three sections. The first section shows you how to download and burn a DEFT Zero ISO image to a CD. The second section shows you how to make a bootable DEFT Zero USB drive. In the third section, you boot DEFT Zero and review some of its features.

Creating a DEFT Zero Boot CD

To create a DEFT Zero ISO bootable CD, follow these steps:

1. Start a Web browser, and go to www.deftlinux.net. Click the **Download DEFT Zero (2017.1)** link, shown in Figure 3-1. Save the **deftZ-2017-1.iso** file to your work folder.

Figure 3-1.



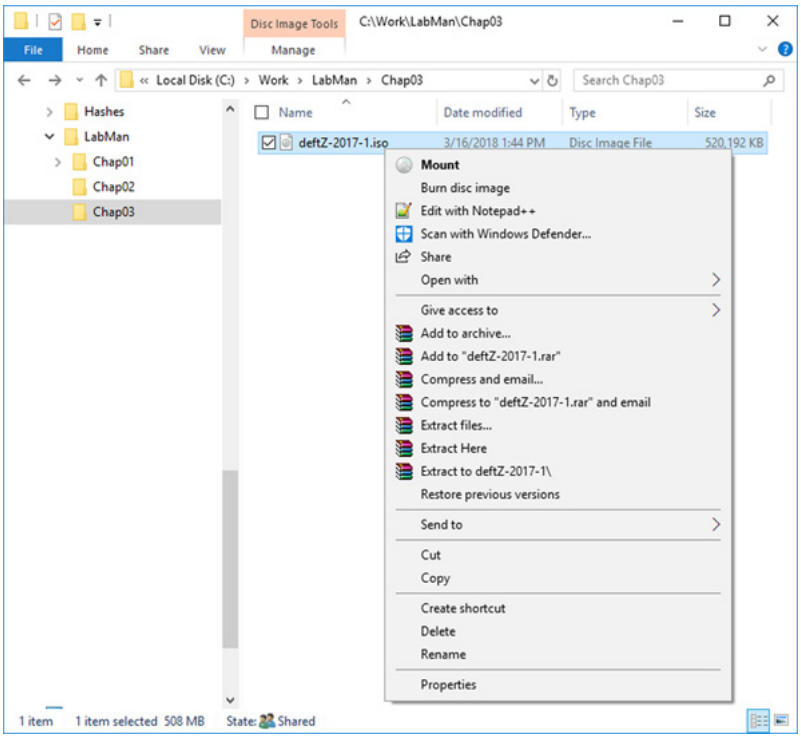
Source: DEFT Association, http://deftlinux.net

Downloading DEFT Zero

2. Insert a blank CD in the CD/DVD drive.
3.

Open File Explorer, and navigate to your work folder. Right-click **deftZ-2017-1.iso** and click **Burn disc image** (see Figure 3-2), or use your preferred CD/DVD burning software.

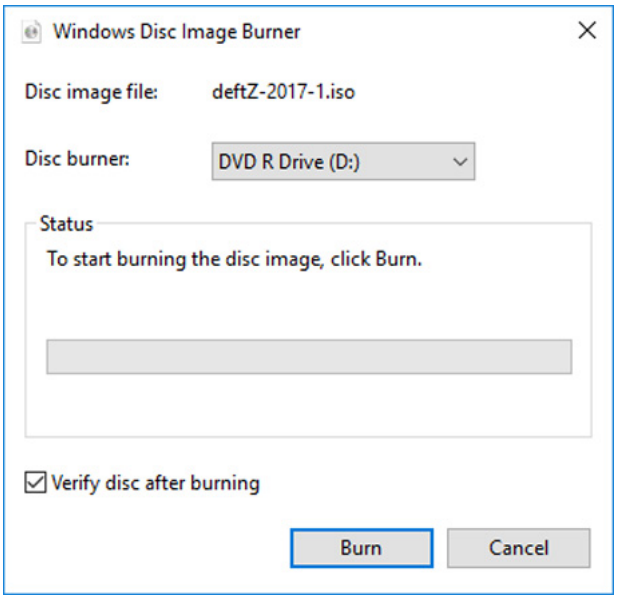
Figure 3-2.



Select the "Burn disc image" option in File Explorer

3. In the Windows Disc Image Burner dialog box, click the **Verify disc after burning** check box (see Figure 3-3), and then click the **Burn** button.

Figure 3-3.



Burning an ISO image to a CD

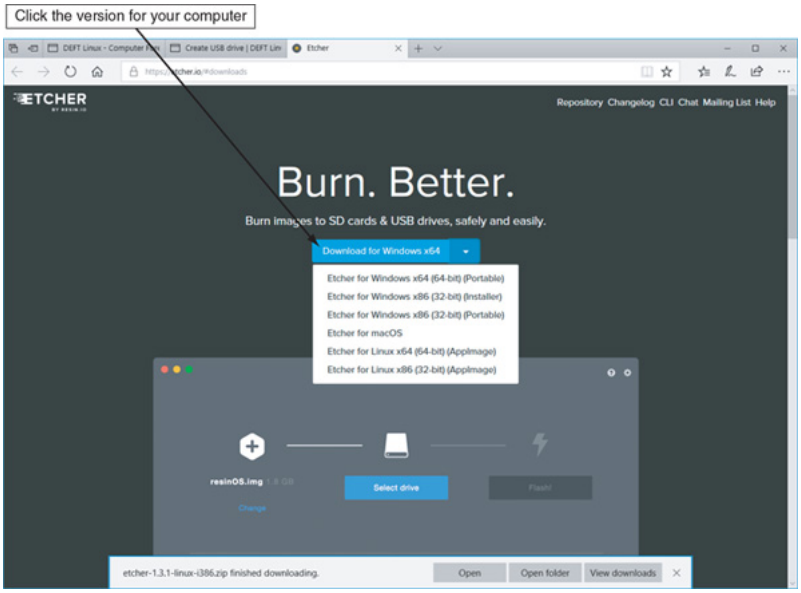
4. When the verification has finished, click **Close**.
5. Eject the CD and label it **DEFT Zero 2017.1**. Close all open windows, and leave your computer running for the next section.

Creating a Bootable USB DEFT Zero Drive

Installing DEFT Zero on a USB drive requires the Etcher tool, which builds bootable ISO images on SD cards and USB drives. To create a DEFT Zero USB bootable drive, follow these steps:

1. Start a Web browser, and go to https://etcher.io/#downloads. Click the **Download for Windows x64** down arrow. Depending on your computer's platform, click **Etcher for Windows x64 (64-bit) (Portable)** for 64-bit computers or **Etcher for Windows x86 (32-bit) (Portable)** for 32-bit computers to start the download (see Figure 3-4). Save **Etcher-Portable-1.3.1-x *nn* .exe** to your work folder.

Figure 3-4.

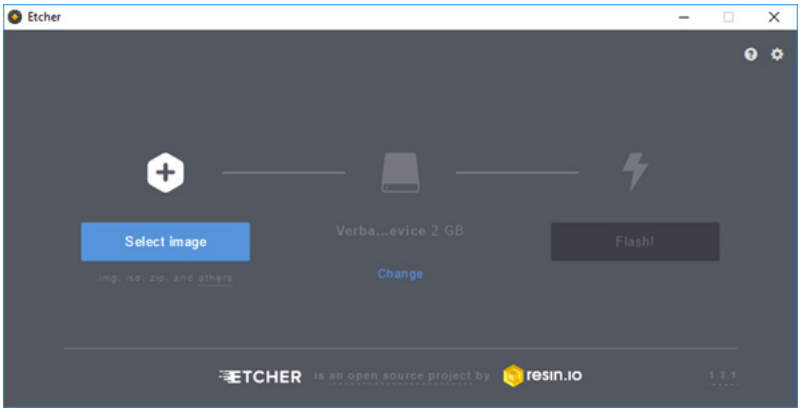


Source: Etcher, http://resin.io

Downloading Etcher

2. Open File Explorer, navigate to your work folder, and double-click **Etcher-Portable-1.3.1-x *nn* .exe** to start Etcher (see Figure 3-5).

Figure 3-5.



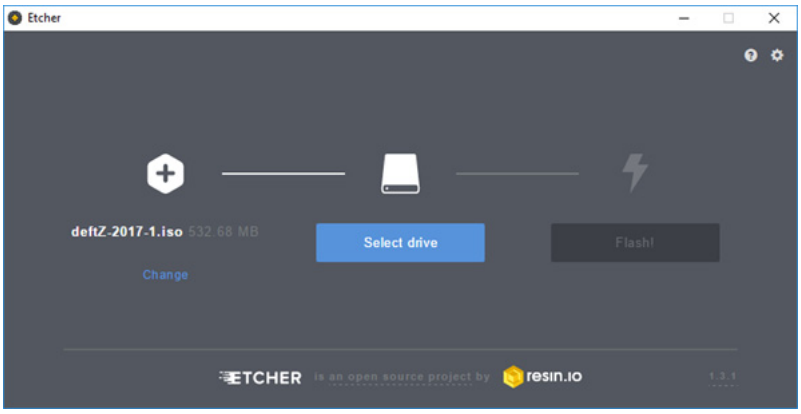
Source: Etcher, http://resin.io

Starting Etcher

3. Click the **Select image** button, and navigate to your work folder. Click the **deftZ-2017-1.iso** file, and click **Open**. Click the **Select drive** button shown in Figure 3-6 (if it's displayed) to open the Select a Drive dialog box (see Figure 3-7). Verify that the current

USB drive is selected, and then click **Continue**. In the main window, click the **Flash!** button to start Etcher.

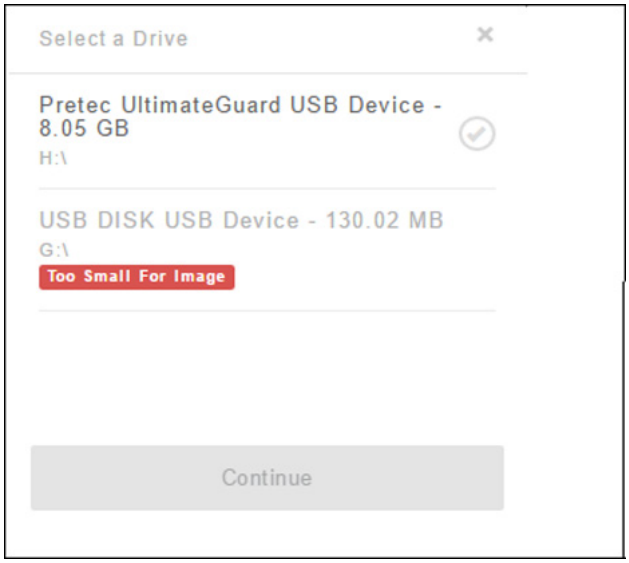
Figure 3-6.



Source: Etcher, http://resin.io

Selecting a USB drive

Figure 3-7.



Source: Etcher, http://resin.io

Confirming the correct USB drive

Note

When Etcher starts, it identifies the USB drive automatically. If more than one USB drive is connected, the Select drive button shown in **Figure 3-6** is displayed so that you can select the correct USB drive. If Etcher displays the wrong ISO image or USB drive, click the Change link to update the selection.

4. When Etcher has finished burning the ISO image, exit it. Remove the USB drive and label it **DEFT Zero**.

6. Connect a second USB drive to your computer. In File Explorer, right-click the new USB drive and click **Rename**. Type **GCFI-Evid** and press **Enter**. Remove the USB drive, and

label it **GCFI-Evid**. Close any open windows, and leave your computer running for the next section.

Learning DEFT Zero Features

Before using DEFT Zero on a suspect's computer, you must know how to access the boot menu. When the computer starts, the system's BIOS or UEFI firmware should be directed to the forensic boot medium. If the boot menu isn't changed, data can be altered on the computer's drive, which isn't what you want for a static acquisition. To access the boot menu, press the correct hot key for the computer's firmware immediately after the system is powered on and the POST has completed all functions just before establishing a connection to the boot medium. On most computers, there's a very short pause at this point (typically 2 to 3 seconds) so that you can access the BIOS, UEFI, or boot menu. If you miss it, power off the computer and power it back on, and attempt to press the hot key again during the pause. For additional information on booting from a CD or USB drive, see www.howtogeek.com/129815/beginner-geek-how-to-change-the-boot-order-in-your-computers-bios/. For a list of major computer manufacturers' hot keys for accessing the boot menu, visit www.disk-image.com/faq-bootmenu.htm.

Another way to change the boot menu is to access the BIOS or UEFI firmware. The DEFT Zero boot medium must be connected to the computer before you access the firmware. In the BIOS/UEFI menu is a boot menu listing the current connected drives and their boot order where you can designate which drive is booted first, second, third, and so on in the motherboard's firmware. After making this update, you save the changes and exit the BIOS/UEFI menu. The firmware then restarts the computer and loads the OS from the drive you selected. For more information on how to access the motherboard's BIOS or UEFI, see www.lifewire.com/bios-setup-utility-access-keys-for-popular-motherboards-2624462.

Note

DEFT Zero includes two forensics acquisition tools: Guymager and the command-line version of FTK Imager Lite. In later chapters, you learn how to use these tools to make static forensic acquisitions.

Caution

When using a DEFT Zero boot USB drive with a second larger USB drive (the drive to receive forensic image files, also known as a "target drive"), the boot menu lists them with their manufacturers' model names, so make sure you note the manufacturer's model name or number for both drives before starting this lab. If you didn't make a note, select the first USB drive to see whether it boots. If it fails, repeat the boot process and select the other USB drive. No harm will occur if you select the wrong USB drive; you just get an error message stating that the assigned boot medium has no OS. In addtion, most computers' boot menus display small USB solid-state drives as "USB" and large USB hard drives as SATA or IDE drives. Knowing the manufacturer's name for the USB boot and target drives helps you determine which one to select.

In this lab, you boot a computer with your DEFT Zero CD or USB drive and review the tool's features:

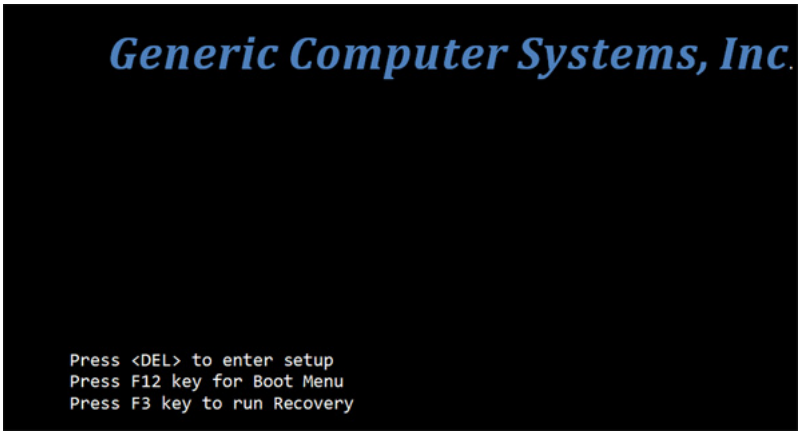
1. For booting to a CD, if your computer is on, open the CD/DVD drive, insert the DEFT Zero CD, and close the drive. If the computer is off and the CD/DVD drive is closed, insert a straightened paper clip into the small hole on the drive's door (the manual eject

hole), and press lightly to open the drive. Pull the tray out all the way, insert the CD, and close the tray. Then skip to **Step 3**.

2. If you're using the DEFT Zero USB drive, insert the drive into a USB port. Next, insert the second USB drive labeled GCFI-Evid into a USB port, and power on the computer.

3. While the computer is starting, read the text that's displayed. Look for any reference to accessing the BIOS, UEFI, or boot menu. **Figure 3-8** shows an example. Press the specified key to access the boot option. In this example, the key for accessing the boot menu is F12.

Figure 3-8.



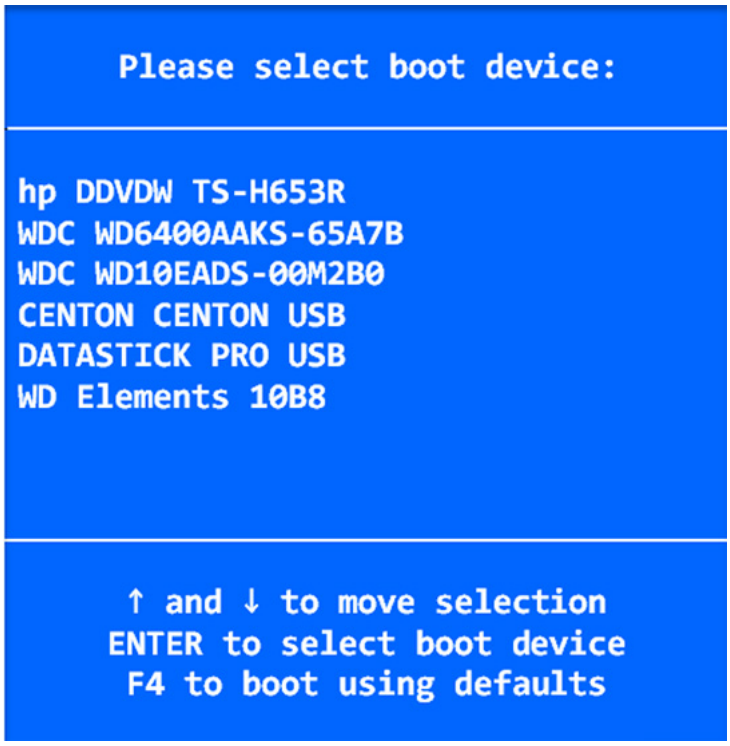
Select the boot option

Note

Figure 3-8 is an example of what's displayed when a computer boots. Your computer might have a different hot key for accessing the boot menu.

4. After pressing the hot key, a menu similar to the one in **Figure 3-9** is displayed. Use the up and down arrow keys to select the DEFT Zero USB drive or CD drive, and press **Enter** to start DEFT Zero.

Figure 3-9.



Selecting the drive to boot from

5. When the DEFT Zero boot loader menu is displayed, make sure the **DEFT-Zero Linux Live-O/S (GUI mode, RAM preload)** option is selected (see Figure 3-10), and press **Enter**.

Figure 3-10.

Source: DEFT Association, http://deftlinux.net

Starting DEFT Zero in GUI mode

Note

DEFT Zero might take a few minutes longer to start than typical Windows computers do because of slower speeds when booting from a USB 1.0 or 2.0 port or a CD/DVD drive.

6. When the DEFT Zero desktop is displayed, click the **d** button shown in the lower-left corner of Figure 3-11. Look at the available options for forensics tools in the DEFT submenu.

Figure 3-11.

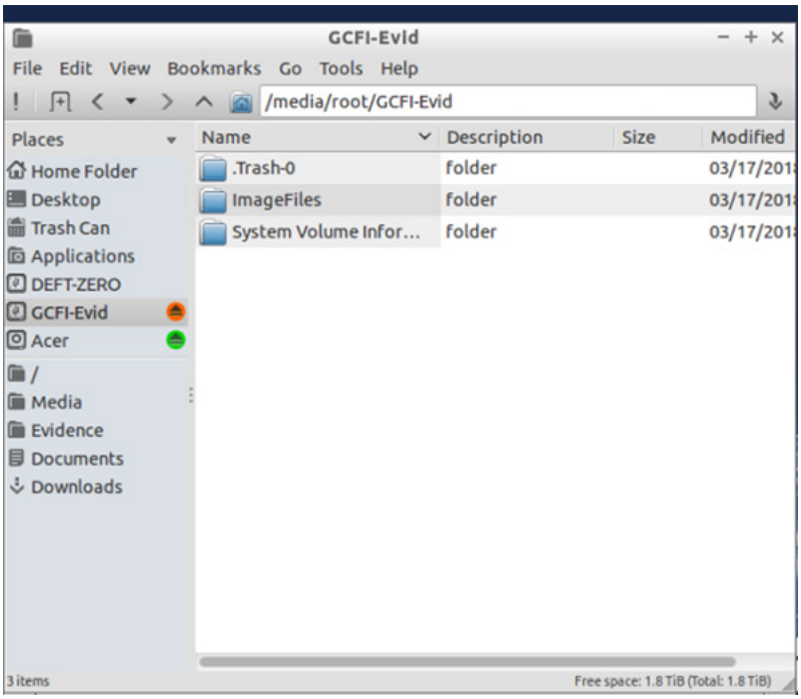
Source: DEFT Association, http://deftlinux.net

The menu in DEFT Zero

7. Double-click the **File Manager PCManFM** desktop icon. In the File List pane on the left, you should see DEFT-ZERO and GCFI-Evid items. DEFT-ZERO is the DEFT Zero RAM disk, and GCFI-Evid is the second USB drive you connected in Step 2. You should also see the C drive of the booted suspect computer (your computer, in this example).

8. To mount GCFI-Evid as a read-write drive, right-click **GCFI-Evid** and click **Mount Volume**. In the Attention dialog box, click **Yes**, and then click **GCFI-Evid** again. Click **File** from the menu, point to **Create New**, and click **Folder**. Type **ImageFiles** in the Creating New Folder text box, and click **OK**. Figure 3-12 shows this new folder listed.

Figure 3-12.



Source: Hon Jen Yee, http://sourceforge.net/projects/pcmanfm

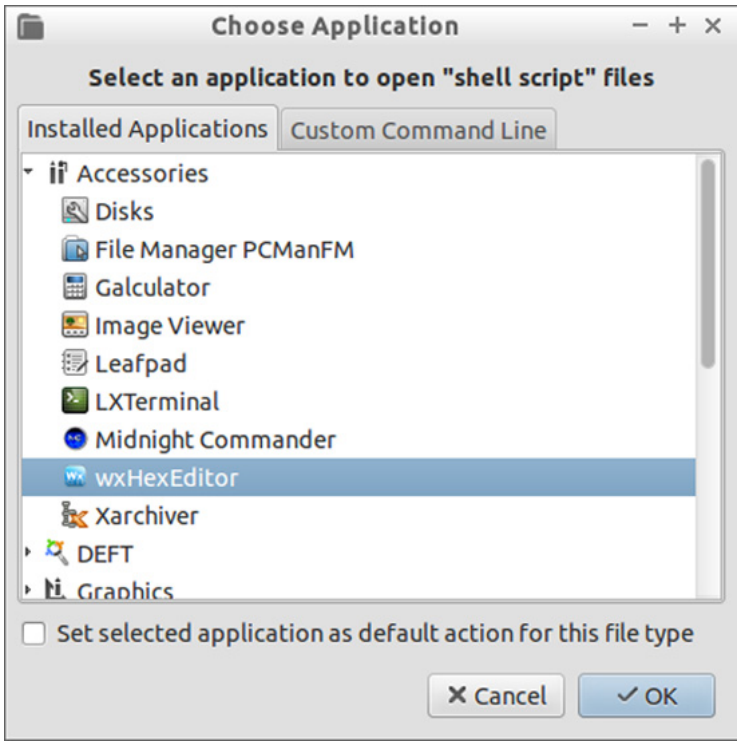
Creating the ImageFiles folder on the GCFI-Evid drive

Note

When a drive is mounted as read-write, an orange eject icon is displayed next to it in the File Listing pane. Drives mounted as read-only have a green eject icon.

9. Right-click your computer's **C** drive (Acer, in Figure 3-12) and click **Mount in protected mode (Read-Only)**. Double-click the **C** drive in the File List pane, and then click to expand the **Windows**, **System32**, and **Config** folders. Scroll down, right-click the **Security registry** file, and click **Open With**. In the Choose Application dialog box, click to expand **Accessories**, click **wxHexEditor** (see Figure 3-13), and click **OK**. In the wxHexEditor License Agreement dialog box, click **OK** to start the hex editor. Figure 3-14 shows the file's contents open in wxHexEditor.

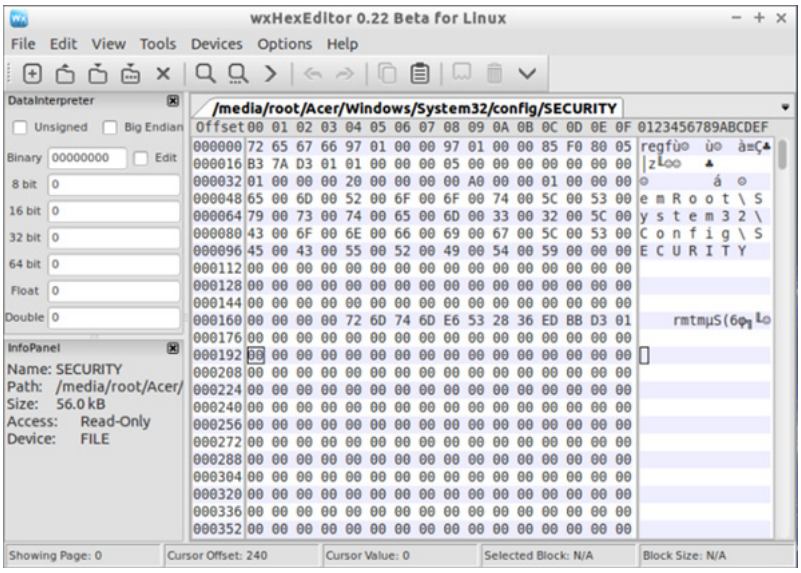
Figure 3-13.



Source: DEFT Association, http://deftlinux.net

Selecting wxHexEditor to open the Security registry file

Figure 3-14.



Source: Erden U. Altinyurt, www.wxhexeditor.org

The Security registry file opened in wxHexEditor

10. Review some other features available in wxHexEditor. When you're finished, exit this tool.

11. Continue exploring tools listed in the DEFT menu. When you're finished, exit DEFT Zero by clicking the shutdown icon at the lower-right corner and clicking **Shutdown**

in the Logout DEFT Zero session dialog box. After the computer shuts down completely, remove all USB drives and the CD, if you used it.

Review Questions

1. What's the OS for DEFT Zero?
    a. Windows 10
    b. WinPE
    c. Lubuntu Linux
    d. OpenBSD
2. Where does DEFT Zero load its OS on the host computer?
    a. On the MFT
    b. In RAM
    c. In the Registry
    d. In unallocated space
3. Examining drives in which mode helps protect evidence from being changed?
    a. Write mode
    b. Safe Boot mode
    c. Read-only mode
    d. Read-write mode
4. With a boot CD, you can create forensic images of which of the following? (Choose all that apply.)
    a. Media in the CD/DVD drive
    b. The computer's BIOS
    c. Attached hardware
    d. Attached storage devices
5. When can you access a computer's boot menu?
    a. Before the OS logon prompt
    b. Before the POST starts
    c. Before the POST has finished
    d. After the POST has finished

Lab 3.2. Examining a FAT Image

Objectives

After completing this lab, you will be able to:

> - Examine images in FTK Imager Lite
> - Identify FAT12, FAT16, and FAT32 file signature

Digital forensics investigators must be familiar with many types of file system structures so that they can search for potential evidence in current and deleted files and folders. Each file system has attributes storing important information that might be useful during an investigation. In many cases, investigators need to establish a timeline surrounding a crime to search for possible suspects.

FAT12 and FAT16 were used in MS-DOS and Windows, but because of their limited support for larger hard drives, they're no longer used for drives larger than 512 MB. FAT32, an improved

version of FAT16, supports disk drives up to 2 terabytes (TB) and filenames up to 255 characters. It's supported by Linux and macOS as well as all versions of Windows except early versions of Windows 95.

Materials Required

This lab requires the following:

- Windows
- FTK Imager Lite
- Microsoft Excel (or open-source spreadsheet software)
- The C3Proj2-1.001, C3Proj2-2.001, and C3Proj2-3.001 files, downloaded to your work folder from this chapter's downloads section

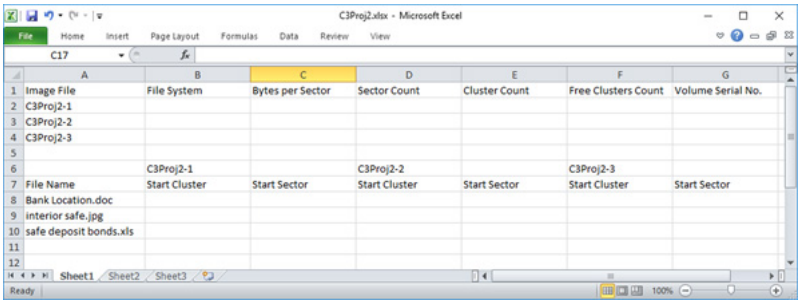
Estimated completion time: 20–30 minutes

Activity

In this lab, you create a spreadsheet for recording FAT 12, FAT 16, and FAT 32 file structure values, and then you examine images in FTK Imager Lite to find these values:

1. Start your spreadsheet software, and create a worksheet with the following labels: In row 1, label columns A through G as **Image File**, **File System**, **Bytes per Sector**, **Sector Count**, **Cluster Count**, **Free Clusters Count**, and **Volume Serial No.** (see Figure 3-15). In column A, rows 2 through 4, type **C3Proj2-1**, **C3Proj2-2**, and **C3Proj2-3**. In cell B6, type **C3Proj2-1**; in cell D6, type **C3Proj2-2**; and in cell F6, type **C3Proj2-3**. In cell A7, type **File Name**; in cells B7, D7, and F7, type **Start Cluster**; and in cells C7, E7, and G7, type **Start Sector**. In cell A8, type **Bank Location.doc**; in cell A9, type **interior safe.jpg**; and in cell A10, type **safe deposit bonds.xls**.

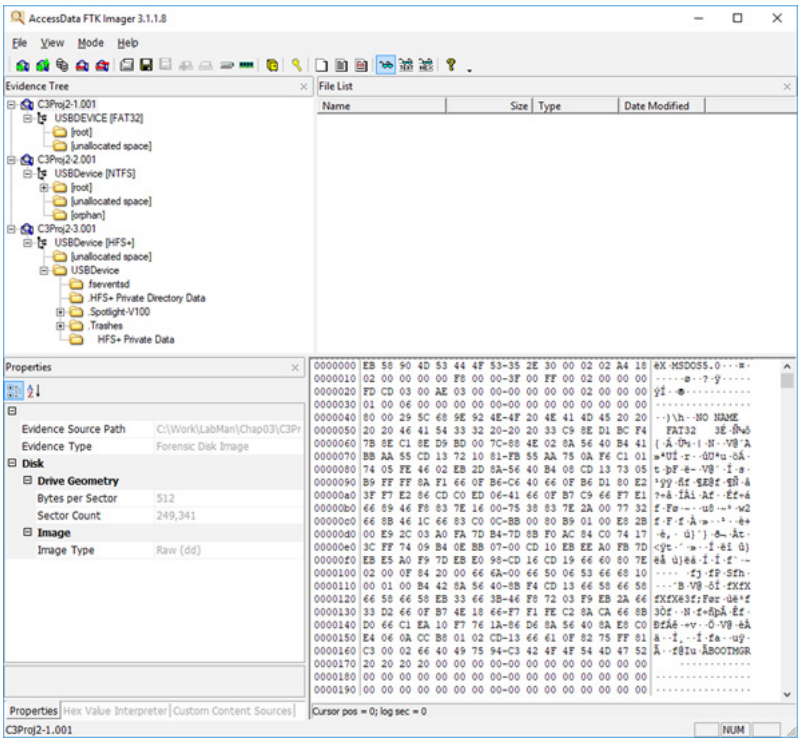
Figure 3-15.



Recording file structure sectors and clusters

2. Start FTK Imager Lite. If necessary, click **Yes** in the UAC message box.
3. Click **File**, **Add Evidence Item** from the menu. In the Select Source dialog box, click the **Image File** option button, and then click **Next**.
4. In the Evidence Source Selection dialog box, click **Browse**, navigate to and click your work folder, click the **C3Proj2-1.001** file, and click **Open**. Click **Finish** to load the file.
5. Repeat **Steps 3** and 4 to load the **C3Proj2-2.001** and **C3Proj2-3.001** files.
6. In the Evidence Tree pane (upper-left pane), expand **C3Proj2-1.001** , **C3Proj2-2.001** , and **C3Proj2-3.001** (see Figure 3-16).

Figure 3-16.



Source: AccessData Group, Inc., www.accessdata.com

Expanding the tree view of image files

7. Click to select **C3Proj2-1.001** . In the Combination pane (lower-right pane), find the information specifying that the OS and file system are MSDOS5.0 and FAT32. Find the Bytes per Sector and Sector Count values in the Properties pane (lower-left pane). Type **FAT32** in cell B2, the Bytes per Sector value in cell C2, and the Sector Count value in cell D2 of your spreadsheet.

8. Click **USBDEVICE [FAT32]** in the Evidence Tree pane. Find the Cluster Count, Free Cluster Count, and Volume Serial No. (if a volume serial number is listed) values in the Properties pane, and record them in your spreadsheet in cells E2, F2, and G2.

9. Repeat **Step 7** for **C3Proj2-2.001** and **C3Proj2-3.001** , and repeat Step 8 to enter the **USBDevice [NTFS]** and **USBDevice [HFS+]** values in the spreadsheet.

10. In the Evidence Tree pane under USBDEVICE [FAT32], click the **[root]** folder. The File List pane shows the files in the C3Proj2-1.001 image and their timestamps. The red X next to some files indicates that the user deleted them. Click each file (including the deleted files) to view it.

11. Click the **HEX** toolbar button to display the hexadecimal values for each file. Then click **Bank Location.doc** in the File List pane, and view its hex information. Find its Start Cluster and Start Sector values in the Properties pane, and record them in your spreadsheet.

12. Click **interior safe.jpg** in the File List pane, and notice the JFIF file signature for a JPEG file. Click the eyeglasses toolbar button (left of the TEXT toolbar button) to see the file in the image viewer. Find the Start Cluster and Start Sector values in the Properties pane, and record them in your spreadsheet.

13. Click **safe deposit bonds.xls** in the File List pane, and view its hex information. Find its Start Cluster and Start Sector values in the Properties pane, and record them in your spreadsheet.

14. Repeat **Steps 10**, 11, 12, and 13 for **USBDevice [NTFS]** and **USBDevice [HFS+]**. Under USBDevice [HFS+], click **UBSDevice** to view files in the File List pane, and notice that HFS+ drives don't have volume serial numbers.

15. Save the spreadsheet as **C3Proj3.xlsx** , and keep it open while you answer the following review questions. When you're finished, close the spreadsheet, and leave FTK Imager Lite running for the next lab.

Review Questions

1. How many clusters are in the FAT32 image?
    a. 120,880
    b. 120,574
    c. 2048
    d. 8192
2. How many files (existing and deleted) are in the FAT32 image?
    a. 9
    b. 11
    c. 16
    d. 10
3. How many Excel files are in the FAT32 image?
    a. 3
    b. 2
    c. 1
    d. 13
4. What's the start sector of the deleted safe deposit bonds.xls file in the C3PROJ2-2.001 image?
    a. 8616
    b. 118,544
    c. 8450
    d. 8262
5. What's the FAT32 drive's volume serial number?
    a. 929E-685C
    b. 2048
    c. C246-C740
    d. 249,341

Lab 3.3. Examining an NTFS Image

Objectives

After completing this lab, you will be able to:

- Examine an NTFS .001 image in FTK Imager Lite
- Identify an NTFS file signature

NTFS is the default file system in NT 3.51 and later as well as Windows Server OSs because it includes file attributes, such as compression and encryption, that aren't available in FAT12, FAT16, or FAT32. NTFS is considered more reliable because of its journaling feature and file

structures that support redundancy, such as a duplicate Master File Table (MFT). It also supports file encryption based on user account information so that multiple users on the same computer can't open each other's encrypted files.

Materials Required

This lab requires the following:

- Windows
- FTK Imager Lite
- WordPad or another text editor
- The C3Proj2-2.001 file from Lab 3.2

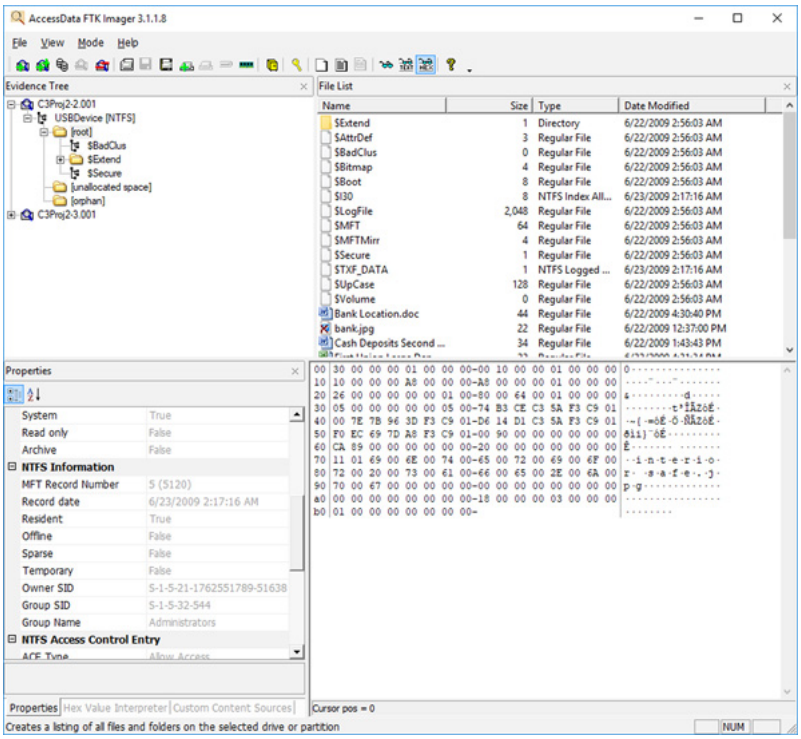
Estimated completion time: 20–30 minutes

Activity

In this lab, you examine the NTFS file structure and compare it with the FAT32 file structure on a USB storage device:

1. In FTK Imager Lite, right-click **C3Proj2-1.001** and click **Remove Evidence Item** to remove this image file.
2. The Combination pane (lower-right) identifies the file system as NTFS. Expand **C3Proj2-2.001** and **USBDevice [NTFS]** in the Evidence Tree pane, and click **C3Proj2-2.001** to select it. The Properties pane shows the image type as "Raw (dd)" and the original disk geometry as 512 bytes per sector with a total of 259,904 sectors.
3. Click the **[root]** folder. The File List pane shows the files in the C3Proj2-2.001 image and their timestamps. Notice that NTFS has additional hidden folders for bad cluster identification ($BadClus) and two copies of the MFT ($MFT and $MFTMirr), as shown in Figure 3-17.

Figure 3-17.



Source: AccessData Group, Inc., www.accessdata.com

Viewing an NTFS image

4. Click each deleted file (with a red X) to view it. Notice that NTFS uses a Date Accessed field in addition to the Date Created and Date Modified fields.

5. Click the **HEX** toolbar button to display the hexadecimal values for each file. Click **Bank Location.doc** in the File List pane, view its hex information, and review its details in the Properties pane. The file signature and file size are the same as in FAT32, but the start locations are different.

6. Click **interior safe.jpg** in the File List pane, and in the Combination pane, notice that the JFIF file signature is the same as the FAT32 file signatures for JPEG files. In addition, in NTFS, JPEG files contain Exif data, which has information about the digital camera's model and manufacturer as well as the shutter speed, lens aperture, and ISO speed used to take the photo. This information can be useful to forensics investigators.

7. Notice the complex file structure of the [root] folder, compared with its structure in other file systems. Expand all subfolders under [root] to see, for example, the $Secure attribute indexes that support NTFS file permissions and the [orphan] folder used to repair files with broken pointers or corrupted indexes.

8. Make a screen capture, and save it in a WordPad document named **Structures.docx** in your work folder. Exit WordPad.

9. Leave FTK Imager Lite running as you answer the following review questions, and then remove this lab's image file by right-clicking **C3Proj2-2.001** and clicking **Remove Evidence Item** to prepare for the next lab. Leave FTK Imager Lite running for the next lab.

Review Questions

1. What's the cluster size in the USBDevice [NTFS] file system?

    a. 2048

   b. 1024
   c. 4096
   d. 31,487
2. What's the volume serial number of the NTFS image?
   a. E16-566
   b. E6FE-1C5F
   c. 2048
   d. 4096
3. What time was the bank.jpg file deleted?
   a. 2:15:31 a.m.
   b. 4:59:14 p.m.
   c. 11:48:03 p.m.
   d. 12:37:21 p.m.
4. What's the physical size of the deleted mark.doc file?
   a. 31,744
   b. 32,768
   c. 16,457
   d. 118,464
5. What folder in the NTFS image is also in the FAT32 image?
   a. [unallocated space]
   b. [root]
   c. [orphan]
   d. [encryption]

Lab 3.4. Examining an HFS+ Image

Objectives

After completing this lab, you will be able to:

> - Process an HFS+ image in FTK Imager Lite
> - Explain the difference between the HFS+, FAT32, and NTFS file systems
> - Find deleted files

HFS+, the file system for Mac OS X 10.4 and later, maintains a journal similar to NTFS to keep track of file changes attempted but not completed because of file errors or hard disk crashes. This journaling feature allows the file system to recover from sudden disk crashes or power losses during a write operation. HFS+ is less susceptible to file corruption caused by broken or missing pointers between blocks of data on a storage device.

Materials Required

This lab requires the following:

- Windows
- FTK Imager Lite
- WordPad or another text editor

- The C3Proj2-3.001 image file from Lab 3.2

Estimated completion time: 10–15 minutes

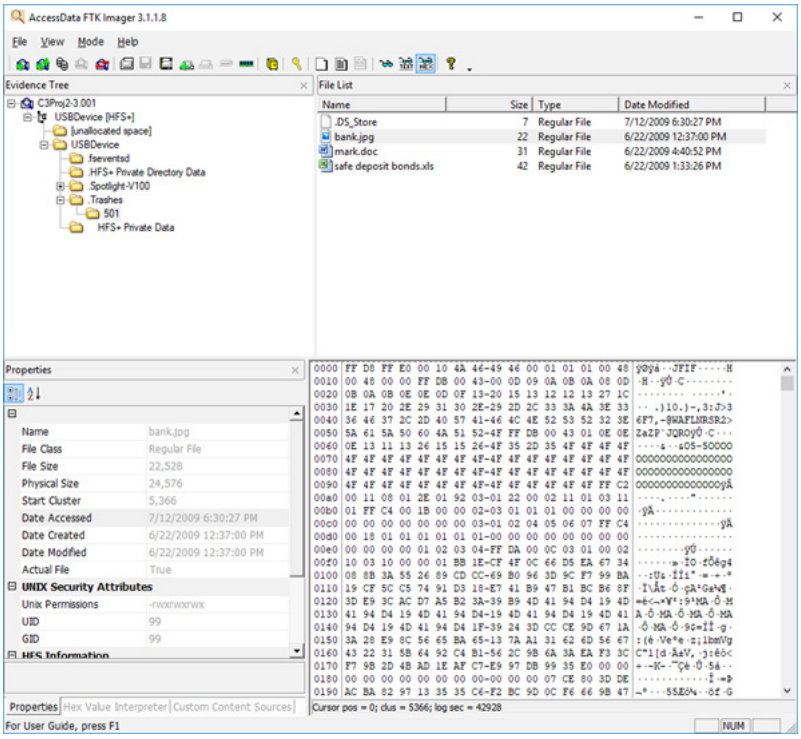
Activity

In this lab, you examine the HFS+ file structure and compare it with the FAT32 and NTFS file structures on a USB storage device:

1. In FTK Imager Lite, expand **C3Proj2-3.001** and **USBDevice [HFS+]** in the Evidence Tree pane, and click to select **C3Proj2-3.001** . The file properties show the image type as “Raw (dd)” and the original disk geometry as 512 bytes per sector with a total of 249,228 sectors.

2. Expand the **.Trashes** folder and click the **501** folder. You should see the same deleted files you’ve seen in previous labs, but HFS+ doesn’t add a red X to indicate they were deleted (see Figure 3-18).

Figure 3-18.



Source: AccessData Group, Inc., www.accessdata.com

Viewing HFS+ deleted files

3. Click each file with an extension to view its properties and security attributes. The Properties pane lists a Date Accessed field in addition to the Date Created and Date Modified fields.

4. Click the **HEX** toolbar button to display the hexadecimal values for each file. Click **Bank Location.doc** in the File List pane, view its hex information, and review its details in the Properties pane. The file signature is the same as in FAT32 and NTFS, but the start locations are different in HFS+.

5. Click **interior safe.jpg** in the File List pane, and notice that the JFIF file signature is the same as in FAT32 and NTFS. HFS+ also displays Exif file data, as NTFS does.

6. Examine the complex file structure of the USBDevice folder. Make a screen capture, and save it in the WordPad **Structures.docx** document created in Lab 3.3. Exit WordPad.

7. Leave FTK Imager Lite running as you answer the following review questions. When you're finished, exit FTK Imager Lite.

Review Questions

1. What's the cluster size in the HFS+ image?
   a. 1024
   b. 2048
   c. 4096
   d. 3077
2. How many clusters are in the HFS+ image?
   a. 31,153
   b. 21,866
   c. 28,099
   d. 249,228
3. What date was the HFS+ partition created?
   a. 6/22/2009
   b. 7/16/2009
   c. 7/12/2009
   d. 7/14/2009
4. What folder doesn't exist in HFS+ but is found in FAT32 and NTFS?
   a. [encryption]
   b. [USB]
   c. [unallocated space]
   d. [root]
5. In what folder are deleted files stored?
   a. .Trashes
   b. 501
   c. [orphan]
   d. [unallocated space]

Chapter 4. Processing Crime and Incident Scenes

Labs included in this chapter:

Lab 4.**1**. Creating a Mini-WinFE Boot CD

Lab 4.**2**. Using Mini-WinFE to Boot and Image a Windows Computer

Lab 4.**3**. Testing the Mini-WinFE Write-Protection Feature

Lab 4.**4**. Creating an Image with Guymager

Note

Before starting these labs, create a subfolder of your work folder named Ch04.

Lab 4.1. Creating a Mini-WinFE Boot CD

Objectives

After completing this lab, you will be able to:

- Prepare a Mini-WinFE boot environment with forensics tools
- Create a Windows boot CD and a USB drive

An important part of processing a crime or an incident scene is collecting digital evidence. As described in **Chapter 3**, physically disconnecting a disk drive from a computer might not be practical in unforeseen circumstances, as when you need special manufacturers' tools to open a laptop computer's case. For these situations, you can use DEFT Zero or other bootable forensics tools, such as Windows Forensic Environment (WinFE), created by Troy Larson at Microsoft, and Mini-WinFE, created by Colin Ramsden, a senior forensic computing analyst with the Royal Military Police. WinFE is based on the Windows Pre-installation Environment (WinPE).

Although limited by the boot medium's disk size, these bare-bones versions of Windows make it possible to install forensics tools on a CD or USB drive. When booted, WinFE and Mini-WinFE load their OSs into a computer's RAM and create a small RAM disk that can be used for saving data. After the computer is shut down, any data saved in RAM is lost. To save data in WinFE or Mini-WinFE to an external drive, you use the disk-mounting tool Disk Mgr, which is included with Mini-WinFE. Mini-WinFE also has the File Manager tool, but it has fewer features than Windows File Explorer does.

In this lab, you create a Mini-WinFE boot CD and USB drive. In the following labs, you learn how to make a forensics acquisition of a suspect's computer. For additional information and guides on Mini-WinFE, see Brett Shavers's Web site, http://brettshavers.cc/index.php/brettsblog/entry/mini-winfe.

As discussed in **Lab 3.1**, bootable forensics tools have several advantages and disadvantages. Some advantages are the following:

- Making an acquisition requires only a boot CD or USB drive and a large USB drive to copy the forensic image to.
- Disassembling a suspect's computer to extract the hard drive for a static acquisition isn't necessary.

The following are some disadvantages:

- Pressing the correct hot key to access a computer's boot menu before the BIOS or UEFI accesses the boot drive can be tricky.

- The time it takes to make an acquisition is influenced by the USB port's throughput speed and the size of the drive.
- Bootable forensics tools have a limited amount of space for additional tools and services.

Note

This lab requires a licensed copy of Microsoft Windows 10 (32-bit) to supply the necessary system files for Mini-WinFE.

Materials Required

This lab requires the following:

- The Windows 10 (32-bit) installation disc
- A blank CD and a USB drive 1 GB or larger
- The Mini-WinFE.2017.04.27.zip file, downloaded in Step 1
- The Imager_Lite_3.1.1.zip and winhex.zip files, downloaded to your work folder in Chapter 1
- Internet access and administrator privileges

Estimated completion time: 45–60 minutes

Activity

This lab is divided into two sections. The first section shows you how to set up the build files for Mini-WinFE, and the second section shows you how to create a Mini-WinFE ISO image, copy it to a small USB drive, and burn it to a CD.

Setting Up Mini-WinFE

Creating a Mini-WinFE bootable CD and USB drive requires placing installation and application files into a work folder. The following steps guide you through preparing a Mini-WinFE ISO image:

1. Start a Web browser, and go to http://reboot.pro/files/download/375-mini-winfe/. Click **Download (Required Software)**. When the file has been downloaded, open File Explorer, and navigate to the download folder. Right-click **Mini-WinFE.2017.04.27.zip** and click **Extract All**. In the Extract Compressed (Zipped) Folders dialog box, click **Browse**, navigate to and click the **C** drive (root folder), and click **Extract**. A subfolder named Mini-WinFE is created automatically.
2. In File Explorer, click the **C:\Mini-WinFE** folder, click the **New folder** toolbar icon, and type **Windows Installation Files**. Insert the Windows installation disc, and copy all files and folders to this subfolder.
3. In File Explorer, copy the **Imager_Lite_3.1.1.zip** and **winhex.zip** files to the C:\Mini-WinFE folder. Right-click each file and click **Extract All**. In the Extract Compressed (Zipped) Folders dialog box, click **Extract** to extract the file's contents into new subfolders created automatically (C:\Mini-WinFE\Imager_Lite_3.1.1 and C:\Mini-WinFE\winhex).

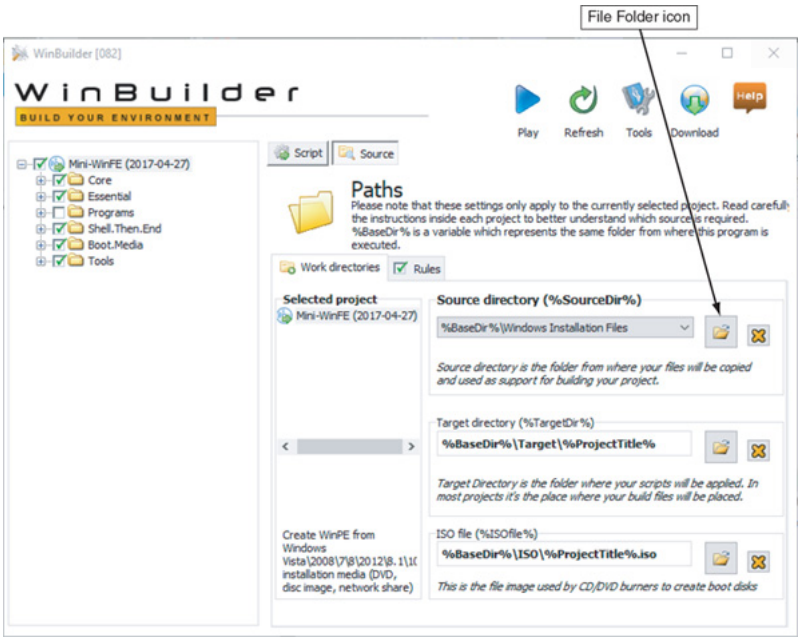
Creating a Mini-WinFE ISO Image

The Mini-WinFE.2017.04.27.zip file contains several tools for creating a bootable Mini-WinFE ISO image. In this lab, you use the WinBuilder tool (extracted from WinBuilder.exe) to create

the ISO image. The following steps explain how to add F.A.U., FTK Imager Lite, and WinHex to a Mini-WinFE ISO image:

1. In File Explorer, navigate to the **C:\Mini-WinFE** folder and double-click the **WinBuilder.exe** file. If necessary, click **Yes** in the UAC message box. After WinBuilder starts, click the **Source** tab in the right pane, and click the **File Folder** icon next to the Source directory (%SourceDir%) text box (see Figure 4-1). Navigate to the **C:\Mini-WinFE** path, click the **Windows Installation Files** folder, and then click **OK**.

Figure 4-1.



Source: Nuno Brito and Peter Schlang, http://winbuilder.net

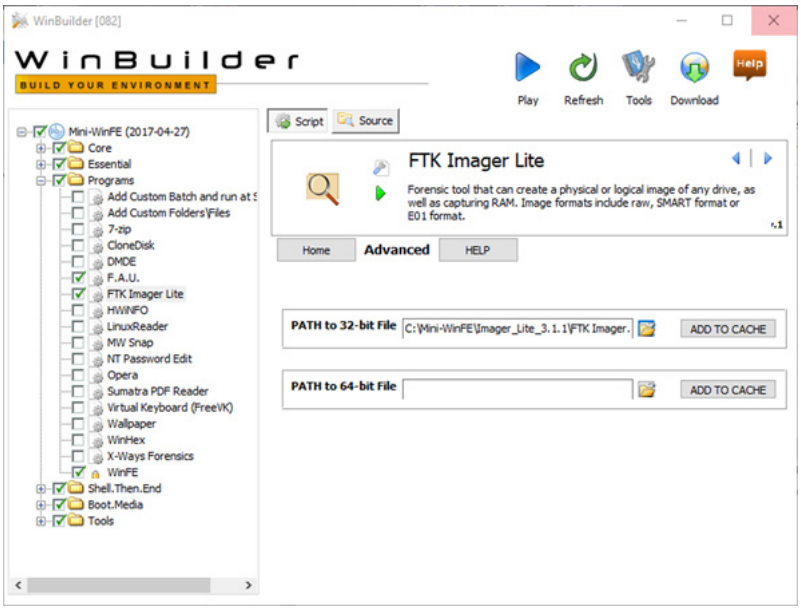
Adding Windows installation files to Mini-WinFE

Note

The variable %BaseDir% in this lab's figures is C:\Mini-WinFE.

2. In the left pane, click to expand **Programs**, and then click **F.A.U.** and **FTK Imager Lite**. (WinFE is selected by default.) Click the **Script** tab in the right pane. Click the **File Folder** icon next to the PATH to 32-bit File text box, navigate to the **C:\Mini-WinFE\Imager_Lite_3.1.1** path, and double-click **FTK Imager.exe** . Figure 4-2 shows the results.

Figure 4-2.



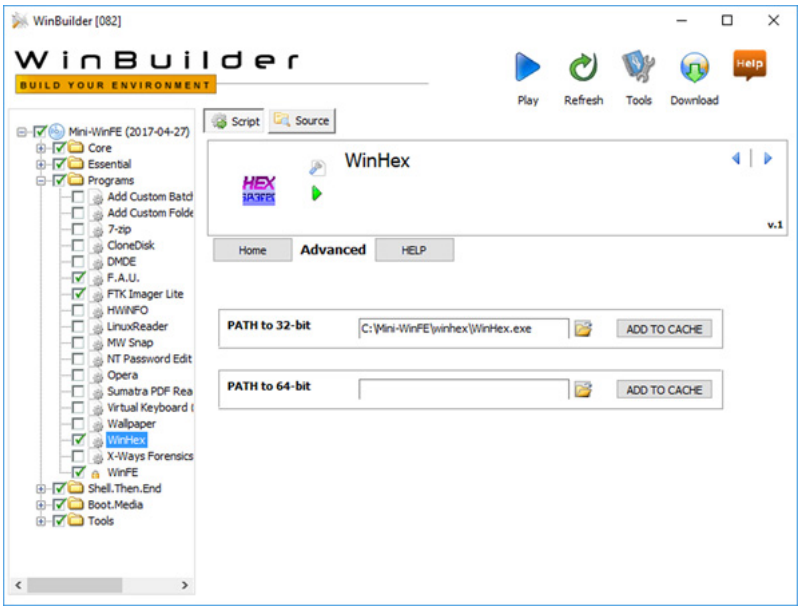
Source: Nuno Brito and Peter Schlang, http://winbuilder.net

Adding FTK Imager Lite to Mini-WinFE

3. Click the **ADD TO CACHE** button next to the PATH to 32-bit File text box, and click **OK**. If necessary, click **OK** again in the Information message box.

4. In the left pane, click to select **WinHex**. In the right pane, click the **File Folder** icon next to the PATH to 32-bit text box. Navigate to the **C:\Mini-WinFE\winhex** path, and double-click **WinHex.exe** . Figure 4-3 shows the results.

Figure 4-3.



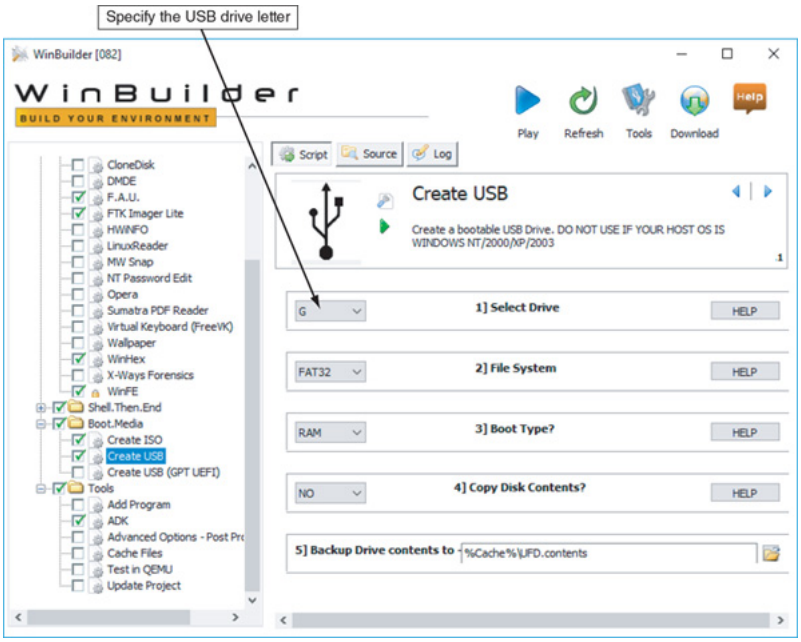
Source: Nuno Brito and Peter Schlang, http://winbuilder.net

Adding WinHex to Mini-WinFE

5. Click the **ADD TO CACHE** button next to the Path to 32-bit text box, and click **OK**. If necessary, click **OK** again in the Information message box.

6. Insert the USB drive into the USB port, and make note of the drive letter assigned when it connects. In the left pane, expand the **Boot Media** folder, and click **Create USB**. In the right pane, click the **1] Select Drive** list arrow, and click the drive letter assigned to the USB drive. Figure 4-4 shows the drive selected.

Figure 4-4.

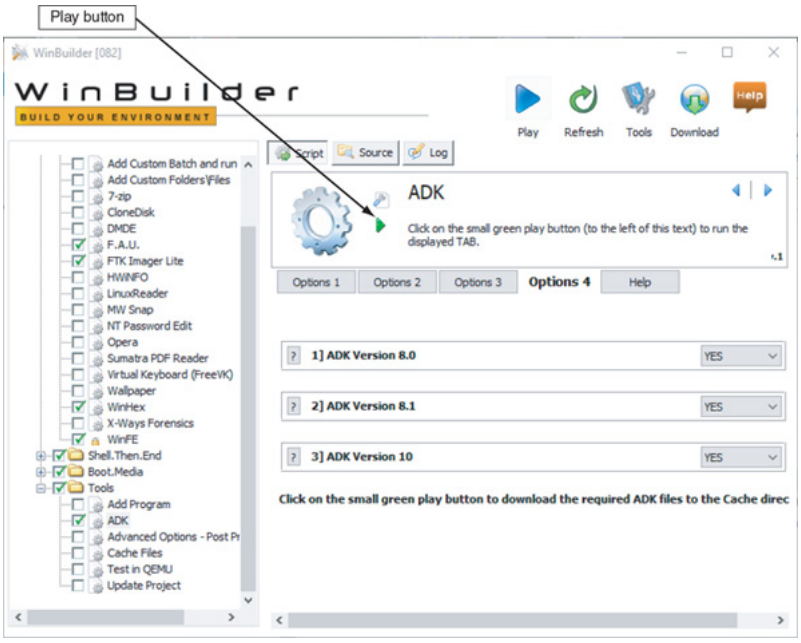


Source: Nuno Brito and Peter Schlang, http://winbuilder.net

Assigning the USB drive letter for the ISO build

7. In the left pane, expand the **Tools** folder, if necessary, and click **ADK**. In the right pane, click the list arrow next to the following text boxes and click **Yes** for each one (see Figure 4-5): 1] ADK Version 8.0, 2] ADK Version 8.1, and 3] ADK Version 10. Click the green **Play** button for each version, and click **OK** in the Information message box. Click the green **Play** button under the ADK heading to make the ADK updates.

Figure 4-5.



Source: Nuno Brito and Peter Schlang, http://winbuilder.net

Selecting ADK versions for Windows

8. At the upper right, click the blue **Play** button. In the Confirmation message box, click **OK**, and then click **OK** and **Yes** in the Information message boxes. When you're finished, exit WinBuilder.

9. Insert a blank CD in the CD/DVD drive. In File Explorer, navigate to the **C:\Mini-WinFE** folder, and click the **WinFE.Project.Output** folder. Right-click the **WinPE.iso** file, point to **Burn disc image**, and click **Burn**.

10. After the disc has been created, click **Close**. Eject the CD, and label it **Mini-WinFE Bootable Forensic Disc**. You use this boot CD in future labs.

Review Questions

1. Which of the following statements about using a bootable forensics tool is incorrect?
   a. Making an acquisition requires only a boot CD or USB drive and a large USB drive to copy the forensic image to.
   b. Disassembling a suspect's computer to extract the hard drive for a static acquisition isn't necessary.
   c. Bootable forensics tools have an unlimited amount of space for additional forensic tools and services.
   d. Pressing the correct hot key to access a computer's boot menu before the BIOS or UEFI accesses the boot drive can be tricky.
2. Where does Mini-WinFE run after it's booted on a computer?
   a. In the MFT
   b. In RAM
   c. In the Registry
   d. In unallocated space
3. The File Manager tool in Mini-WinFE has all the features you find in Windows File Explorer. True or False?

4. The time it takes to make an acquisition with a bootable forensics tool is influenced by which of the following? (Choose all that apply.)
    a. The BIOS version
    b. The USB port's throughput speed
    c. The size of the drive being acquired
    d. The amount of RAM
5. WinFE is based on the Windows Pre-installation Environment (WinPE). True or False?

Lab 4.2. Using Mini-WinFE to Boot and Image a Windows Computer

Objectives

After completing this lab, you will be able to:

> - Boot a Windows computer by using Mini-WinFE
> - Make an image of a Windows hard drive

In **Lab 3.1**, you created a Mini-WinFE boot CD and USB drive that include FTK Imager Lite, WinHex, and other tools on a bootable Windows platform. You can use this medium to mount and examine attached storage devices safely and ensure that the chain of custody is preserved. This medium is useful for other forensics activities, too. For example, a critical task in digital forensics is making a static acquisition of a suspect drive. Using forensics boot tools, such as Mini-WinFE or DEFT Zero, makes it possible to acquire data safely. All you need are a target drive for storing the image and the forensics boot medium. To make the acquisition, boot the suspect's computer with the forensic boot medium, mount the suspect's drive as read-only and the target drive as read-write, and then run the forensics acquisition software. The only other action is to monitor the acquisition periodically to make sure it runs successfully and isn't accessed by an unauthorized person.

In this lab, you also use Disk Mgr, included with Mini-WinFE. It's displayed when you boot Mini-WinFE and lists all connected drives automatically. You can select which drives to mount as read-only to protect them or as read-write to send data to them, such as an image file or a file from the suspect drive. To view the contents of a drive without altering its data, you use Disk Mgr to mount the drive as read-only. To create forensic images, you must connect another drive to the computer before booting WinFE or Mini-WinFE and use Disk Mgr to mount the drive as read-write. After this drive is mounted, you can then write data to it.

Materials Required

This lab requires the following:

- A Windows computer
- The Mini-WinFE Bootable Forensic Disc CD or Mini-WinFE USB drive from **Lab 4.1**
- An additional external hard drive (preferably a USB drive) equal to or larger than the Windows bootable hard drive in your computer
- A SATA cable, if no large USB drive is available

Estimated completion time: 20–30 minutes for setup

Caution ⚠

The time needed to make an acquisition depends on the size of the drive. The larger the drive, the longer the acquisition takes. For small drives, it could take up to 2 hours; for large drives, it could take more than 6 hours. Setting up this acquisition to run overnight is recommended.

Activity

In this lab, you use Mini-WinFE to boot and image a Windows computer. Before starting, make note of the size in bytes of your external USB drives (or internal SATA drive) and the Mini-WinFE USB drive (if you're not using the CD). For demonstration purposes, this lab uses a 1.2 TB Seagate USB drive (for the external drive) and a 50 MB ATTACHE USB drive for the Mini-WinFE drive. Substitute your USB drive sizes for the ones used in this lab.

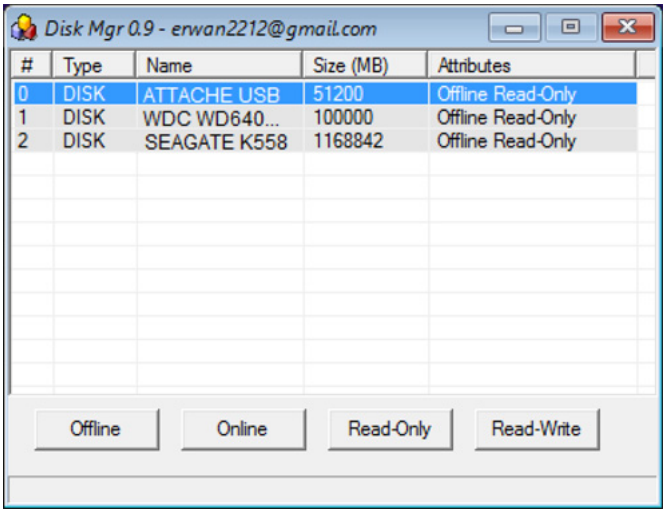
1. Review **Lab 3.1** for instructions on finding the hot key to access your computer's boot menu. (Ask your instructor if you need help with this task.) For a large external USB or SATA drive, do a quick format in File Explorer and give the drive the name **GCFI-Evid**.

2. If you're using the Mini-WinFE USB drive, connect the large USB drive or SATA drive to the computer, and then connect the Mini-WinFE USB drive. If you're using the CD, insert the CD into the CD/DVD drive as described in **Chapter 3**.

3. If the computer is powered off, power it on; if the computer is running, restart it. As soon as the boot options menu is displayed during the POST, press the hot key for accessing the boot menu.

4. In the computer's boot menu, select the Mini-WinFE USB drive or the CD/DVD drive. When Mini-WinFE starts, the Disk Mgr dialog box lists all connected drives (see **Figure 4-6**). Your connected drives will differ.

Figure 4-6.



Source: erwan.l, erwan2212@gmail.com, http://reboot.pro/files/file/573-diskmgr/

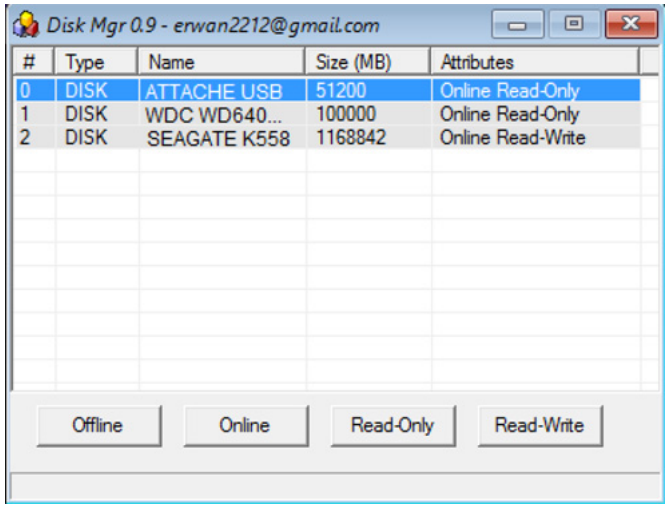
Selecting the external USB drive

5. Determine which drive is your external USB drive. In this example, it's DISK 2, SEAGATE K558, which is 1.16 TB. Click to select the correct drive, and click the **Online** button to mount the drive so that it's visible to Mini-WinFE. In the warning message box, click **Yes**. Click to select this same drive again, and click the **Read-Write** button. In the CloneDisk message box, click **Yes**.

6.

Next, you mount the Mini-WinFE USB drive and the C drive as read-only. For each drive, select the drive, click the **Online** button, and click **Yes** in the warning message box. Figure 4-7 shows the mounted drives. When you're finished, close the Disk Mgr dialog box.

Figure 4-7.



Source: erwan.l, erwan2212@gmail.com, http://reboot.pro/files/file/573-diskmgr/

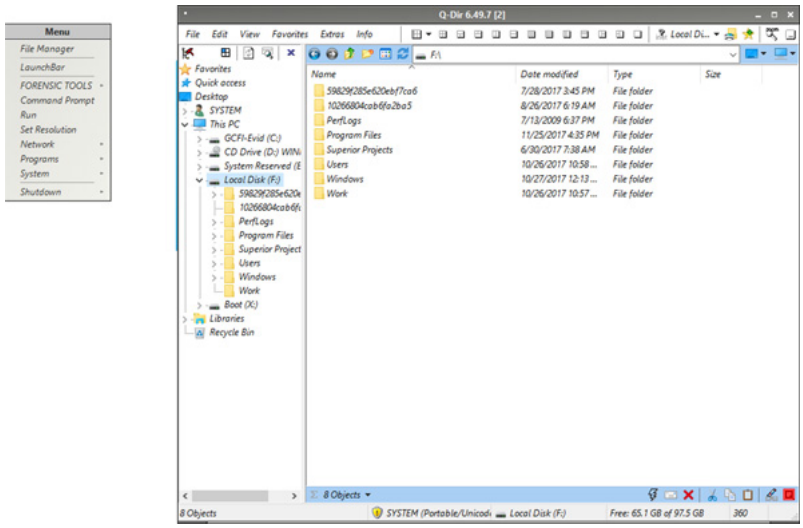
Mounting the external USB drive as read-write and all other drives as read-only

Note

The Attributes column in Disk Mgr shows drives 0 and 1 as Online Read-Only and drive 2 as Online Read-Write.

7. When the Windows Forensic Environment desktop is displayed, note that there's no Start menu. (To display a menu of available tools, you can right-click the desktop.) To make an acquisition, you need to identify the correct drive to image. Right-click the desktop anywhere and click **File Manager**. In File Manager, click to expand **This PC**, and then click each drive and view its contents (see Figure 4-8). When you're finished, close File Manager.

Figure 4-8.



Source: The Quad-Directory Explorer, www.q-dir.com

Using File Manager

Note

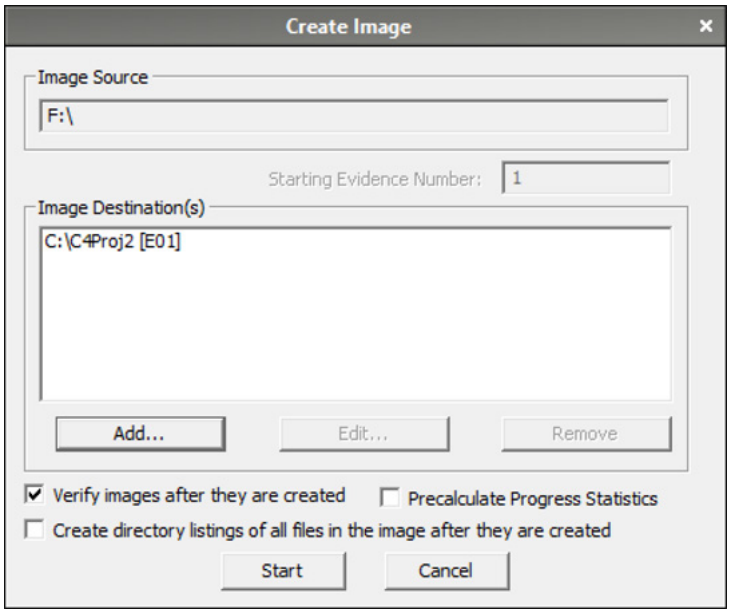
File Manager displays only drives that have been mounted in Disk Mgr. If you don't see any drives, open Disk Mgr (by right-clicking the Windows Forensic Environment desktop, pointing to FORENSIC TOOLS, and clicking Disk Mgr), mount the drives, and set them to read-only for the source (suspect) drive and read-write for the target drive.

8. To make an acquisition, right-click the desktop, point to **FORENSIC TOOLS**, and click **FTK Imager Lite**. Click **File**, **Create Disk Image** from the menu. In the Select Source dialog box, click the **Logical Drive** option button, and then click **Next**. In the Select Drive dialog box, click the **Source Drive Selection** list arrow, click the **C:** drive in the drop-down list, and then click **Finish**.

9. In the Create Image dialog box, click **Add**. In the Select Image Type dialog box, click **E01**, and then click **Next**. Type **C4Proj2** in the Case Number and Evidence Number text boxes, and then click **Next**. Click the **Browse** button next to the Image Destination Folder text box, navigate to and click the **GCFI-Evid** drive, and then click **OK**.

10. In the Select Image Destination dialog box, type **C4Proj2** in the Image Filename (Excluding Extension) text box, and then click **Finish**. In the Create Image dialog box, verify that the image source and image destination settings are correct (see Figure 4-9). Click the **Start** button to begin the imaging process, which could take several hours, depending on the hard drive's size.

Figure 4-9.



Source: AccessData Group, Inc., www.accessdata.com

Checking settings for imaging

11. When the image is finished, exit FTK Imager Lite, but leave the Windows Forensic Environment desktop open as you answer the following review questions. When you're finished, right-click the desktop, point to **Shutdown**, and click **Shutdown**. Leave the USB drives or CD connected for the next lab. If you used a SATA cable, leave it connected, too.

Review Questions

1. The Disk Mgr tool mounts any hard drive connected to the computer automatically. True or False?

2. Which of the following options is available in Disk Mgr? (Choose all that apply.)
   a. Online
   b. Verify Disk
   c. Read-Only
   d. Read-Write

3. Which of the following settings prevents making changes to an attached drive?
   a. Rescan
   b. Mount
   c. Read-Only
   d. Read-Write

4. The reasons for monitoring an acquisition are to make sure unauthorized people don't access the computer and make sure it runs successfully. True or False?

5. In Mini-WinFE, both mounted and unmounted drives are listed in File Manager. True or False?

Lab 4.3. Testing the Mini-WinFE Write-Protection Feature

Objectives

After completing this lab, you will be able to:

- Verify that the WinFE write-protection feature is working correctly

As Windows computers start or are shut down, changes are made to files and folders that can change dates, log files, and most recently used (MRU) devices recorded in the Windows Registry. Therefore, before you search a live storage device, you must use a write-blocker tool to prevent any changes that could affect the chain of custody. Write-blocker tools can be hardware or software, and they're designed to allow examining and imaging computer files or OSs without altering potential evidence. They can be used in two modes: read-only, which allows forensics tools to search without changing file attributes (such as last modified or last accessed times), and read-write, which allows changes to file attribute dates and log files on live storage devices so that forensics tools can be used. Write-blocker tools aren't needed to search CDs and DVDs because they're read-only devices and don't need to be mounted. In this lab, you test the WinFE write-protection feature.

Materials Required

This lab requires the following:

- Windows
- The Mini-WinFE Bootable Forensic Disc CD or Mini-WinFE USB drive from **Lab 4.1**
- The large external USB drive or internal SATA drive from **Lab 4.2**

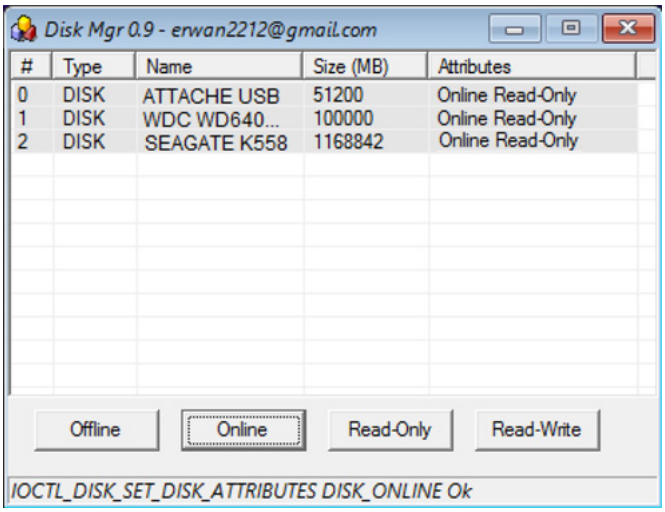
Estimated completion time: 15–20 minutes

Activity

In this lab, you test the WinFE write-protection feature on your external USB drive or internal SATA drive:

1. Power on your computer, and press the hot key for the boot menu during the POST. When the Disk Mgr dialog box opens, click to select the external drive (DISK 2, in this example), click the **Online** button, and click **Yes** in the warning message box. The Attributes column for this drive should list Online Read-Only (see Figure 4-10). Close the Disk Mgr dialog box.

Figure 4-10.

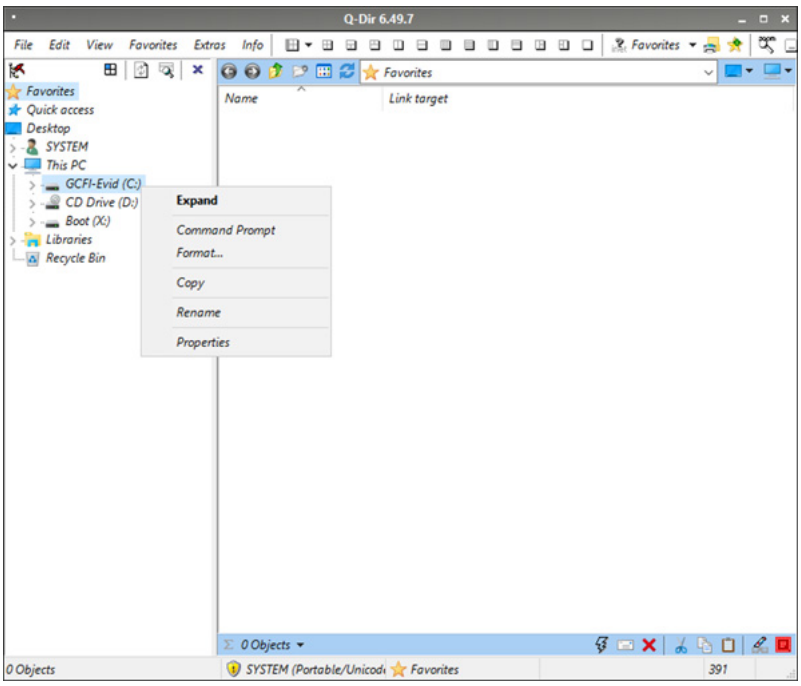


Source: erwan.l, erwan2212@gmail.com, http://reboot.pro/files/file/573-diskmgr/

Mounting an external drive

2. Right-click the Windows Forensic Environment desktop and click **File Manager**. In File Manager, click to expand **This PC**. Right-click **GCFI-Evid (C:)** (see Figure 4-11) and click **Rename**. Type **Test** and press **Enter**. In the error message stating that the disk is write-protected (see Figure 4-12), click **OK**.

Figure 4-11.



Source: erwan.l, erwan2212@gmail.com, http://reboot.pro/files/file/573-diskmgr/

Renaming a disk volume

Figure 4-12.

Source: The Quad-Directory Explorer, www.q-dir.com

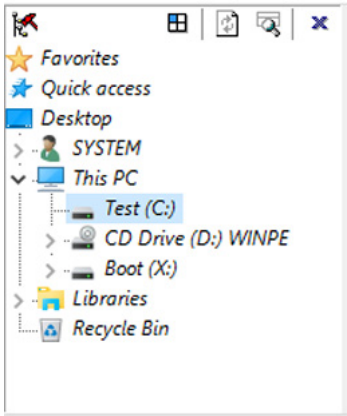
The error message displayed when attempting to write to a write-protected disk

3. Close the File Manager window. Right-click the Windows Forensic Environment desktop, point to **FORENSIC TOOLS**, and click **Disk Mgr**.

4. In Disk Mgr, click the external drive (DISK 2, in this example), and click the **Offline** button. In the CloneDisk message box, click **Yes**, Click the external drive again, and click the **Online** button. In the warning message box, click **Yes**. Click the external drive again, and click the **Read-Write** button. In the CloneDisk message box, click **Yes**, The Attributes column for this drive should list Online Read-Write. Close the Disk Mgr dialog box.

5. Right-click the Windows Forensic Environment desktop and click **File Manager**. In File Manager, click to expand **This PC**. Notice that the external USB drive's volume name has changed to Test (see Figure 4-13).

Figure 4-13.



Source: The Quad-Directory Explorer, www.q-dir.com

Verifying that the USB drive's volume name changed to Test

6. Close File Manager, and then reopen it to confirm that the name change has been saved.

7. Leave File Manager open. Click **Extras**, **System** from the menu, examine the available options, and then answer the following review questions. When you're finished, close File Manager. Right-click the desktop, point to **Shutdown**, and click **Shutdown**. Remove the Mini-WinFE USB drive or CD from the computer, but leave the external USB drive or internal SATA drive connected.

8. Reboot the computer into Windows. In File Explorer, right-click the external USB drive or internal SATA drive and click **Format**. Click the **File System** list arrow and click **NTFS**. Type **GCFI-Evid** in the Volume label text box, click the **Quick Format** check box, and click **Start**. Click **OK** in the Format warning message box, click **OK** in the Format Complete message box, and click **Close** in the Format dialog box.

9.

To prepare for the next lab, connect the DEFT Zero USB drive or insert the DEFT Zero CD in the CD/DVD drive, and then shut down your computer.

Review Questions

1. Why were you unable to change the drive name in **Step 2**?
   a. The drive was mounted.
   b. The drive had been dismounted.
   c. The drive was in read-write mode.
   d. The drive was in read-only mode.
2. In Disk Mgr, you can change a drive to read-write mode only when it's mounted. True or False?
3. How do you show hidden files in File Manager?
   a. Click View, point to Group by, and click Show hidden files & folders.
   b. Click Favorites, Show hidden files & folders.
   c. Click View, Details from the menu.
   d. Click Extras, System from the menu, and click the "Show hidden files & folders" option.
4. Write-blocker tools aren't needed to search CDs and DVDs because they're read-only devices and don't need to be mounted. True or False?
5. You can't search CDs or DVDs in Mini-WinFE File Manager. True or False?

Lab 4.4. Creating an Image with Guymager

Objectives

After completing this lab, you will be able to:

> - Make an image of a Windows computer's physical local C drive with Guymager

DEFT Zero includes several tools for creating images in multiple formats supported by commercial forensics software packages, such as OSForensics, X-Ways Forensics, AccessData, Forensic Explorer, and EnCase, and free forensics tools, such as Autopsy and the command-line version of FTK Imager Lite. Guymager, another tool in DEFT Zero, is capable of making simultaneous acquisitions of multiple storage devices in raw (dd) and .E01 formats. It also performs integrity checks by generating MD5 or SHA-256 hash values while it's imaging data. One shortcoming of Guymager is that it can acquire only physical drives, not logical drives. In this lab, you use Guymager to acquire a computer's physical local C drive.

Materials Required

This lab requires the following:

- A Windows computer
- The DEFT Zero boot USB drive or CD from **Lab 3.1**
- Completion of **Lab 4.3**
- An external or internal NTFS-formatted hard drive equal to or larger than your computer's C drive
- A SATA cable, if necessary

Estimated completion time: 2–10 hours, depending on the hard drive's size

Caution

Because the imaging process in this lab can take so much time, setting it up to run overnight is recommended.

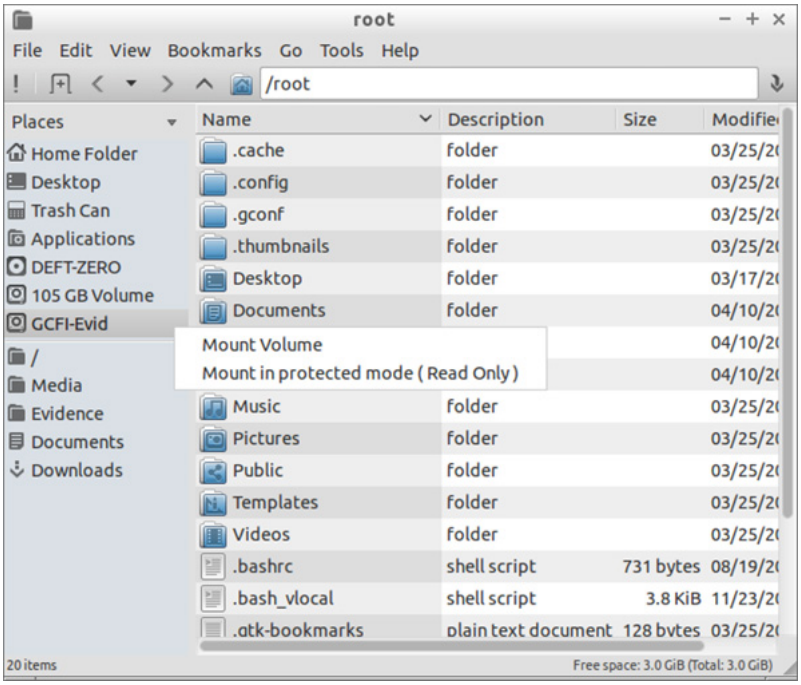
Activity

In this lab, you use Guymager to make an image of your computer:

1. Power on your computer, and press the hot key for the boot menu. When the boot menu is displayed, select the DEFT Zero USB drive or CD/DVD drive, and press **Enter** to start DEFT Zero.

2. When the DEFT Zero desktop is displayed, double-click the **File Manager PCManFM** desktop icon. In the File List pane, right-click **GCFI-Evid** and click **Mount Volume** (see Figure 4-14). In the Attention message box, click **Yes**.

Figure 4-14.



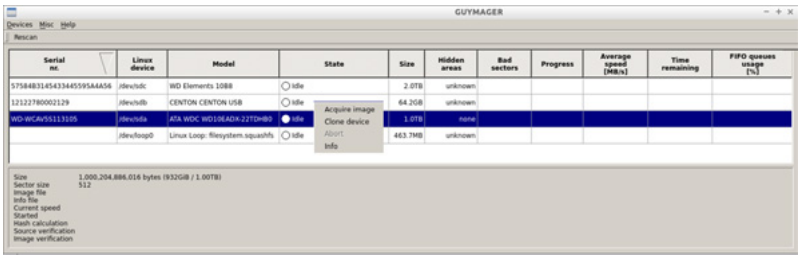
Source: DEFT Association, www.deftlinux.net

Mounting a drive as read-write

3. Click **GCFI-Evid** in the File List pane again. Click **File** from the menu, point to **Create New**, and click **Folder**. In the Create New Folder text box, type **Images**, and then click **OK**.

4. Double-click the **Guymager** desktop icon. In the Guymager main window, look at the Linux device column and find the computer's C drive. (DEFT Zero lists a Windows computer's C drive as /dev/sda.) Right-click the **/dev/sda** drive and click **Acquire image** (see Figure 4-15).

Figure 4-15.

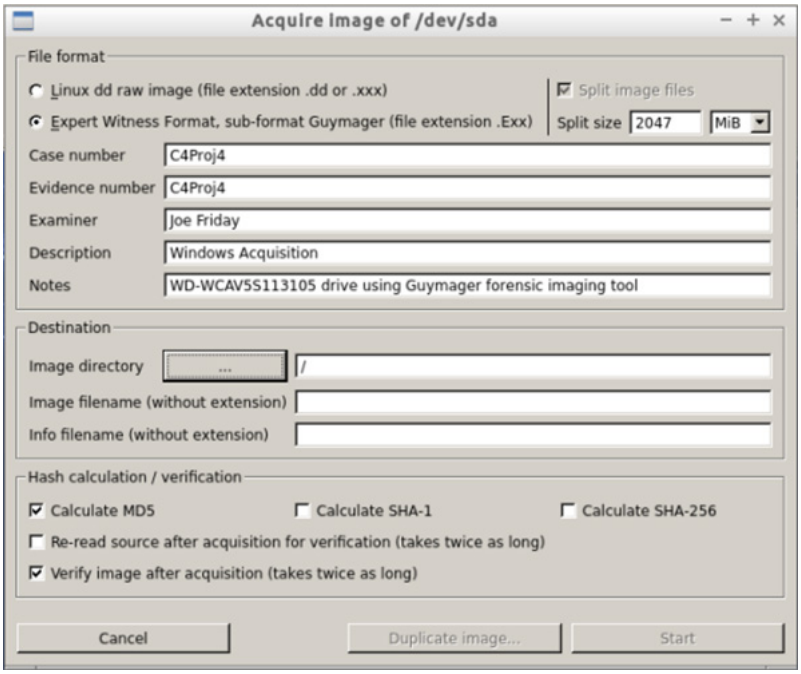


Source: Qt, www.qt.io

Starting an acquisition

5. In the Acquire Image of /dev/sda dialog box, type **C4Proj4** in the Case number and Evidence number text boxes, type your name in the Examiner text box, and type **Windows Acquisition** in the Description text box. In the Notes text box, add details about this acquisition (see Figure 4-16 for an example), and then click the browse button next to the Image directory text box.

Figure 4-16.



Source: Qt, www.qt.io

Filling in case information

6. In the Select destination directory dialog box, double-click **media**, **root**, **GCFI-Evid**, and **Images**, and then click **Choose**. In the Acquire Image of /dev/sda dialog box, click the **Start** button.

7. When the imaging process is finished, exit Guymager and close all open windows. Leave the DEFT desktop open as you answer the following review questions. When you're finished, exit DEFT, and shut down your computer.

Review Questions

1. Guymager creates disk images that are verified by which of the following?

    a. Hard disk capacities

b. MD5 and SHA-256 hash values

c. CRC-32

d. By comparing all bytes to each other

2. DEFT Zero doesn’t support image formats used in free forensics tools. True or False?

3. Guymager can acquire which types of drives?

a. Virtual drives

b. Logical drives

c. RAID drives

d. Physical drives

4. DEFT Zero has no forensics tools for searching hard disks. True or False?

5. Guymager is capable of imaging which of the following?

a. Only one disk at a time

b. Multiple storage devices simultaneously

c. Only dd-formatted images

d. Only USB storage devices

Chapter 5. Working with Windows and CLI Systems

Labs included in this chapter:

Lab 5.**1**. Using DART to Export Windows Registry Files

Lab 5.**2**. Examining the SAM Hive

Lab 5.**3**. Examining the SYSTEM Hive

Lab 5.**4**. Examining the ntuser.dat Registry File

Note

Before starting these labs, create a subfolder of your work folder named Ch05.

Lab 5.1. Using DART to Export Windows Registry Files

Objectives

After completing this lab, you will be able to:

- Describe the Windows forensics tools included with DART
- Export Registry files with FTK Imager in DART

Investigators often encounter running computers that might contain valuable forensics data in RAM or other disk locations that would be lost if the system were shut down. DART is a collection of Windows tools that can be used to examine and image a live (running) Windows computer. It includes imaging, data recovery, forensics, incident response, networking, and password recovery tools as well as tools to view graphics, multimedia, and documents with open-source software. The DART tools can capture the contents of physical RAM on a live computer to yield valuable information, such as open files and cached credentials used to access computer and network resources. DART also includes acquisition tools, such as FTK Imager, HDDRawCopy, and RamCapture, for both 32-bit and 64-bit OSs. Its data recovery tools, such as TestDisk, can recover deleted files on storage devices; recover lost files; and search for FAT, FAT32, NTFS, Ext2, Ext3, and Ext4 partitions. In this lab, you use the forensics tools in DART, such as FTK Imager, and recover Registry files from your live Windows computer.

Materials Required

This lab requires the following:

- Windows
- DART version 2, downloaded in **Step 1**

Estimated completion time: 15–20 minutes

Activity

In this lab, you run FTK Imager from DART to export the Registry files from your Windows computer:

1. Create a subfolder of your work folder named **DART_v2-2014**. Start a Web browser, and go to www.deftlinux.net/2014/04/16/deft-8-1-and-dart-2-2014/. Click the **You can download the DART 2 - 2014 stand alone here** link. Save the **DART_v2-2014.7Z** file in this subfolder, and extract its contents.

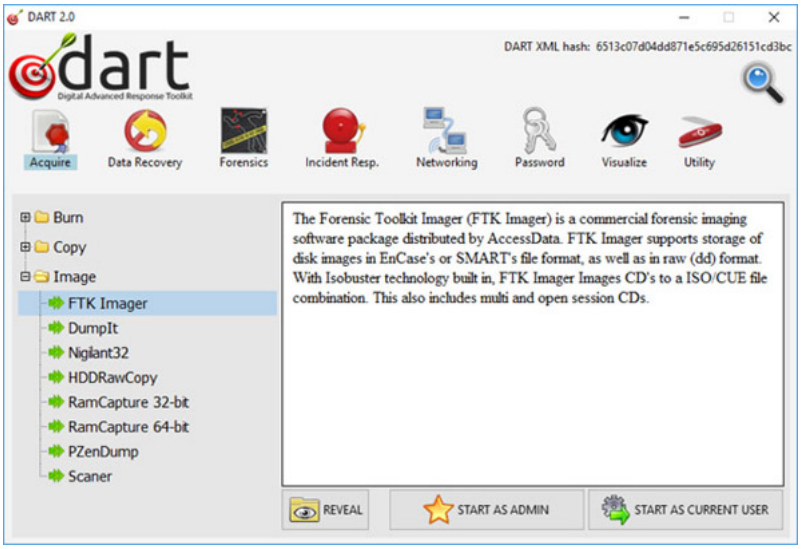
Note

Extracting the contents of the DART version 2 file requires a tool capable of 7-zip extraction, such as WinZip, WinRAR, or 7-Zip. If you don't have one of these tools, go to www.7-zip.org, and download and install the 32-bit or 64-bit freeware 7-Zip tool.

2. Right-click the **dart.exe** file and click **Run as administrator**. If necessary, click **Yes** in the UAC message box. Click **Yes** in the DART DISCLAIMER message box. In the Browse For Folder dialog box, navigate to and click your work folder, and then click **OK**.

3. Click the **Acquire** toolbar icon. In the left pane, click to expand **Image**, and then click **FTK Imager** (see Figure 5-1). Click the **START AS ADMIN** button to start FTK Imager.

Figure 5-1.

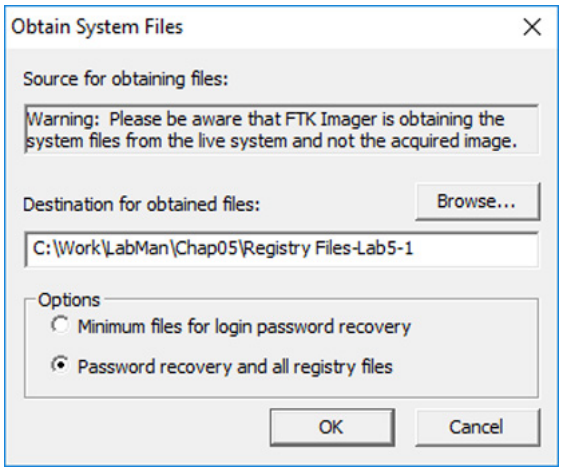


Source: DEFT Association, www.deftlinux.net

Starting FTK Imager from DART

4. Click **File**, **Obtain Protected Files** from the menu. In the Options section of the Obtain System Files dialog box, click the **Password recovery and all registry files** option button. Click the **Browse** button, navigate to and click your work folder, click **Make New Folder**, type **Registry Files-Lab5-1** for the new name, and then click **OK**. Click **OK** to enter this path in the "Destination for obtained files" text box (see Figure 5-2). FTK Imager copies the Windows Registry files to this path.

Figure 5-2.

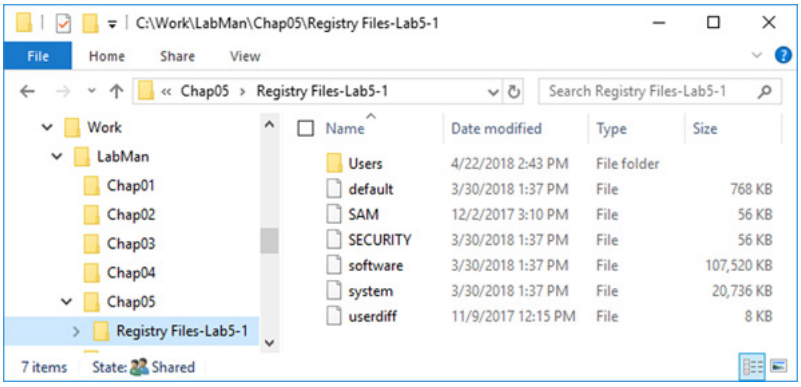


Source: AccessData Group, Inc., www.accessdata.com

Entering a path for copying Registry files

5. In File Explorer, navigate to the **Registry Files-Lab5-1** subfolder of your work folder to view the files on your computer. You should see files representing Registry hives and user accounts on this computer (see Figure 5-3). The exported Registry files can be viewed in any Registry editor, such as AccessData Registry Viewer.

Figure 5-3.



Viewing Registry files

6. Exit FTK Imager, and leave the Registry Files-Lab5-1 subfolder and DART console open as you examine DART's other features and answer the following review questions. When you're finished, exit File Explorer and DART, and leave your computer running for the next lab.

Review Questions

1. DART can be used to boot a Windows computer. True or False?
2. RAM can be captured most safely after a computer is shut down. True or False?
3. DART acquisition tools include which of the following? (Choose all that apply.)
   a. OSForensics
   b. DumpIt
   c. RamCapture
   d. Tcpdump

4. You can use TestDisk to search both Windows and Linux partitions. True or False?
5. DART includes password recovery tools. True or False?

Lab 5.2. Examining the SAM Hive

Objectives

After completing this lab, you will be able to:

> - Examine the SAM hive containing usernames and password hashes
> - View Registry files in Registry Viewer

The Registry is the central repository of settings and data for the Windows environment as a computer boots. It's divided into five hives in the C:\Windows\System32\Config folder. Each hive contains specific data, such as passwords, desktop settings, hardware and software configurations, and other valuable forensic information. The Registry files most useful to forensics investigators are the Security Accounts Manager (SAM) and SYSTEM hives and the ntuser.dat file (which is in the C:\Users*username* folder and is unique for each user). The SAM hive stores information on user accounts and their password hashes as well as group definitions and domain associations by using globally unique IDs (GUIDs). In this lab, you copy Registry files from a Windows image with FTK Imager Lite and view the SAM hive with AccessData Registry Viewer.

Materials Required

This lab requires the following:

- Windows
- Registry Viewer, downloaded in **Step 2**
- FTK Imager Lite
- The InCh05.exe file, downloaded in Step 1

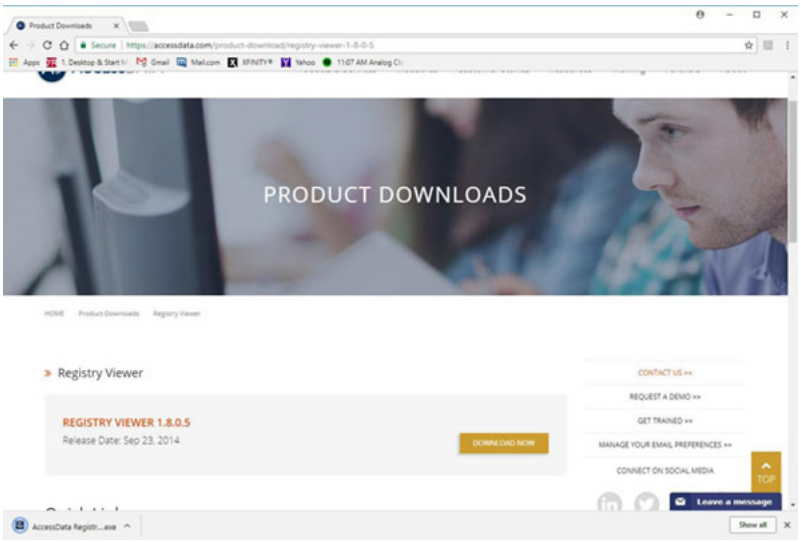
Estimated completion time: 15–20 minutes

Activity

In this lab, you examine the SAM hive to determine the user accounts on a seized computer:

1. Download the **InCh05.exe** to your work folder. In File Explorer, double-click this file and click **Extract** to extract it to your work folder.
2. Create a subfolder of your work folder named **Registry_Viewer**. Start a Web browser, if necessary, and go to https://accessdata.com/product-download/registry-viewer-1-8-0-5. Click **DOWNLOAD NOW** (shown in Figure 5-4) to download Registry Viewer to the Registry_Viewer subfolder.

Figure 5-4.



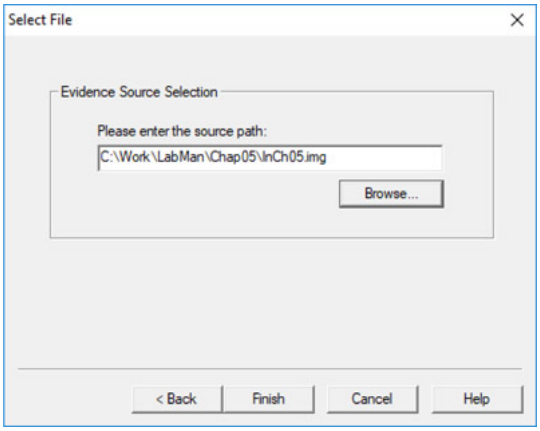
Source: AccessData Group, Inc., www.accessdata.com

Downloading Registry Viewer

3. Open File Explorer, and double-click **AccessData Registry Viewer_1.8.0.5.exe** . In the AccessData Registry Viewer - InstallShield Wizard welcome window, click **Next**, and in the Custom Setup window, click **Next**. In the Ready To Install the Program window, click **Install**, and then click **Finish**.

4. Start FTK Imager Lite. If necessary, click **Yes** in the UAC message box. Click **File**, **Add Evidence** Item from the menu. In the Select Source dialog box, click the **Image File** option button, and then click **Next**. In the Select File dialog box, click **Browse**, navigate to and click your work folder, click the **InCh05.img** file, and then click **OK** to enter this source path (see Figure 5-5). Click **Finish** to open the image in FTK Imager.

Figure 5-5.



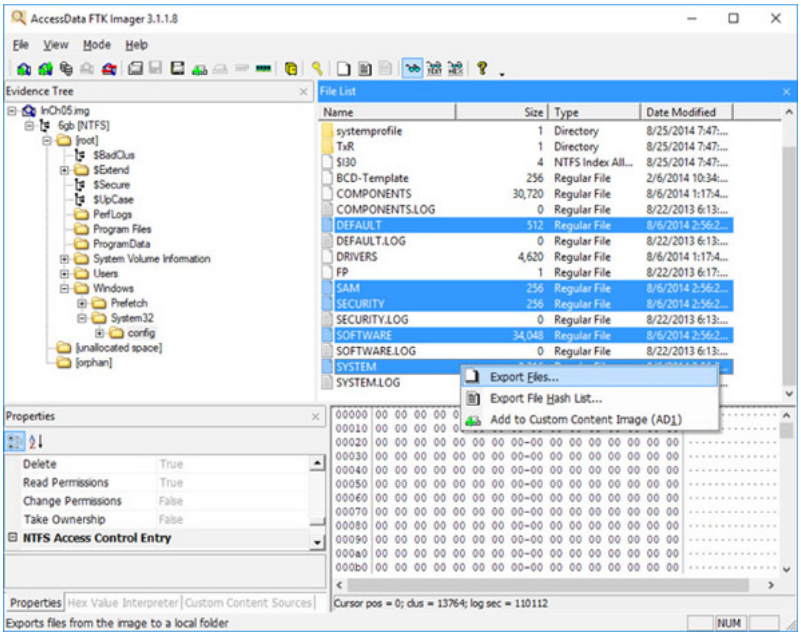
Source: AccessData Group, Inc., www.accessdata.com

Entering a source path for the image

5. In the left pane, click to expand **InCh05.img** , **6gb [NTFS]**, **[root]**, and **Users**. Click the **Denise** folder, and then right-click the **ntuser.dat** file in the File List pane and click **Export Files**. In the Browse For Folder dialog box, navigate to and click your work folder, click **Make New Folder**, and type **Registry Files-Lab5-2** for the new name. Click **OK** to copy the file, and click **OK** in the Export Results message box.

6. In the left pane, click to expand **Windows** and **System32**, and then click **config**. In the File List pane, Ctrl+click **SYSTEM**, **SOFTWARE**, **SECURITY**, **SAM**, and **DEFAULT**. Right-click one of these selected files and click **Export Files** (shown in Figure 5-6). Navigate to and click the **Registry Files-Lab5-2** subfolder of your work folder, and click **OK** to copy the files. Click **OK** in the Export Results message box, and then exit FTK Imager Lite.

Figure 5-6.



Source: AccessData Group, Inc., www.accessdata.com

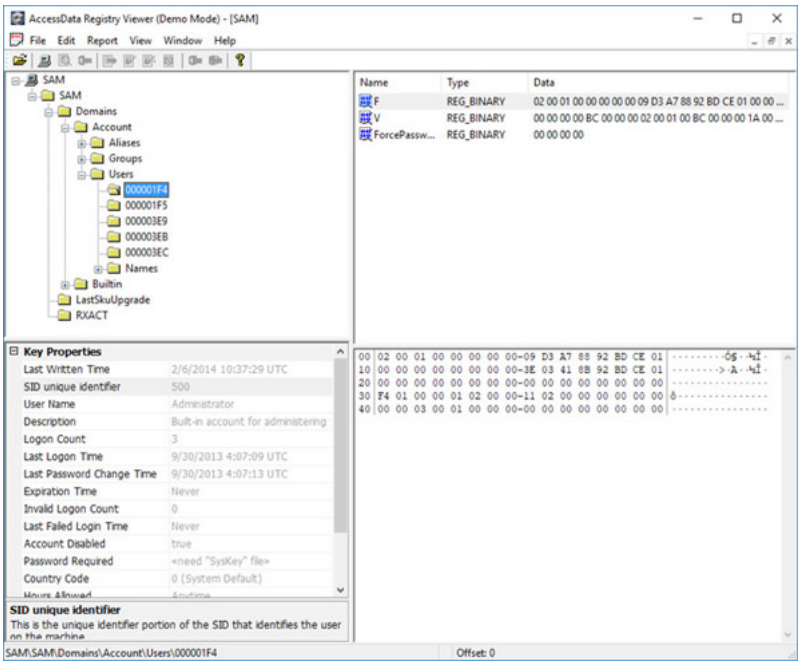
Exporting Registry files

7. Start Registry Viewer, and if necessary, click **Run as administrator**. If necessary, click **Yes** in the UAC message box. Click **Yes** in the ERROR dialog box, click **Cancel** in the Security Device Settings dialog box, and click **OK** in the Registry Viewer dialog box to start Registry Viewer in demo mode.

8. Click **File**, **Open** from the menu. Navigate to the **Registry Files-Lab5-2** subfolder of your work folder, and in the File List pane, click **SAM**, and then click **Open**.

9. In the left pane, click to expand the **SAM**, **Domains**, **Account**, and **Users** folders. Click the **000001F4** folder, and enlarge the Key Properties pane at the lower left. Notice the last logon time and the SID unique identifier field, which indicates the type of account and whether it's created automatically when the OS is installed. Values of 500, 501, and 1000 show default accounts (created automatically). This user account is Administrator, and it has been logged on to three times (see Figure 5-7).

Figure 5-7.



Source: AccessData Group, Inc., www.accessdata.com

Viewing user account information

10. Click the **000003E9** folder. The jfriday account has been logged on to seven times, and the SID value 1001 indicates that this account was created.

11. Click the **000003EC** folder. The Denise Robinson account was created but has never logged on to the computer.

12. Click to expand the **Names** folder, and then click the **jfriday** folder. The Last Written Time entry indicates that this account was accessed on 2/6/2014 when the password was changed.

13. Leave Registry Viewer open as you answer the following review questions. When you're finished, close the SAM hive by clicking **File**, **Close** from the menu. In the Registry Viewer dialog box, click **Yes**, and leave Registry Viewer running for the next lab.

Review Questions

1. The Registry contains how many hives?
   a. Three
   b. Two
   c. Five
   d. Six
2. How many user accounts are disabled?
   a. Two
   b. Seven
   c. One
   d. Three
3. The SAM hive uses PIDs to store information on user accounts. True or False?
4. Name two SID values that indicate whether an account was created automatically.

5. The Key Properties pane in Registry Viewer shows when user accounts have changed their passwords. True or False?

Lab 5.3. Examining the SYSTEM Hive

Objectives

After completing this lab, you will be able to:

> - View the SYSTEM hive in Registry Viewer
> - Look for useful forensic information in the SYSTEM hive

The SYSTEM Registry hive contains drive letter designations for internal and external storage devices, the system name, and configuration data for the system's hardware and software. This hive is important because it can help identify a computer and any storage devices that might have been mounted in the OS. It also contains information on when the Windows partition was created and activated. The product ID (PID) key in the SYSTEM hive is a unique identifier that can act as an electronic fingerprint to identify a legally activated Windows OS.

Materials Required

This lab requires the following:

- Windows
- Registry Viewer
- The SYSTEM hive extracted in **Lab 5.2**

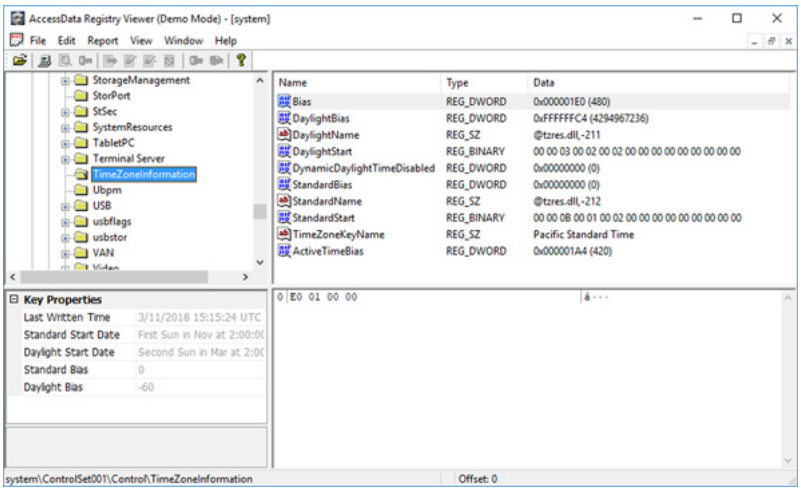
Estimated completion time: 15 minutes

Activity

In this lab, you examine the SYSTEM hive to see how it manages connected devices on a computer:

1. In Registry Viewer, click **File**, **Open** from the menu. Navigate to the **Registry Files-Lab5-2** subfolder of your work folder, click the **SYSTEM** file, and then click **Open**.
2. In the left pane, expand the **ControlSet001**, **Control**, and **ComputerName** folders, and then click the **ComputerName** folder to display the name at the upper right.
3. Scroll down and click the **TimeZoneInformation** folder in the left pane to display the computer's time zone information (see Figure 5-8). This information is critical because timestamps for files, folders, and logs are based on the time zone.

Figure 5-8.



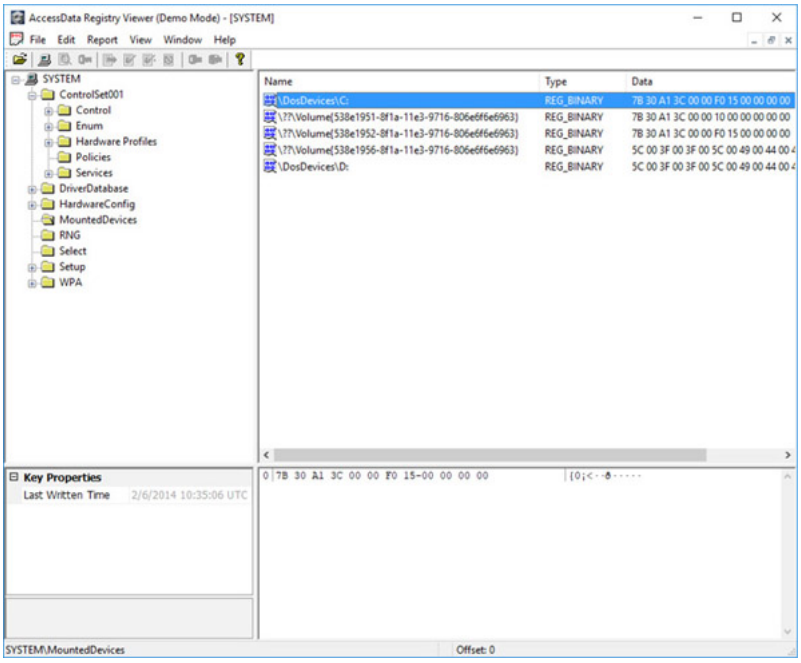
Source: AccessData Group, Inc., www.accessdata.com

Viewing time zone information

4. Scroll down the left pane, and expand the **Enum** folder and the **IDE** folder, which contains IDE storage devices, such as the CD/DVD drive. Expand the **USB** folder to see all USB storage devices plugged into the computer. Each storage device has a unique serial number and a Last Written Time entry in the Key Properties pane.

5. Click the **MountedDevices** folder, which lists every storage device that has been mounted in the Windows OS along with its associated drive letter and GUID value (see Figure 5-9). This information can be used to associate hard drives with a Windows computer.

Figure 5-9.



Source: AccessData Group, Inc., www.accessdata.com

Viewing information on mounted devices

6. Leave Registry Viewer open as you answer the following review questions. When you're finished, close the SYSTEM hive by clicking **File**, **Close** from the menu. In the

Registry Viewer dialog box, click **Yes**, and leave Registry Viewer running for the next lab.

Review Questions

1. What's the computer name of this system?
    a. mnmsrv
    b. GCFI5E
    c. HAL
    d. MSDTC
2. What's the time zone setting for this computer?
    a. EST
    b. MST
    c. CST
    d. PST
3. How many mounted devices on this system have assigned drive letters?
4. What information is stored in the Enum folder?
    a. User account information
    b. Password information
    c. File locations
    d. Hardware and software values
5. The SYSTEM hive contains configuration data for passwords. True or False?

Lab 5.4. Examining the ntuser.dat Registry File

Objectives

After completing this lab, you will be able to:

> - Load a file in Registry Viewer to search for evidence
> - Find Windows user account information in the Registry

The ntuser.dat Registry file contains user-specific information, such as personalized settings for the desktop, software, and e-mail accounts as well as the most recently used (MRU) files and devices. The forensic information in this file can help investigators discover Internet searches and recently used storage devices, for example. The ntuser.dat file is in the C:\Users*username* folder, and each account holder in Windows has a separate ntuser.dat file. Many password decryption tools require both the ntuser.dat file and the SYSTEM Registry hive to retrieve user passwords.

Materials Required

This lab requires the following:

- Windows
- Registry Viewer
- The ntuser.dat file extracted in Lab 5.2

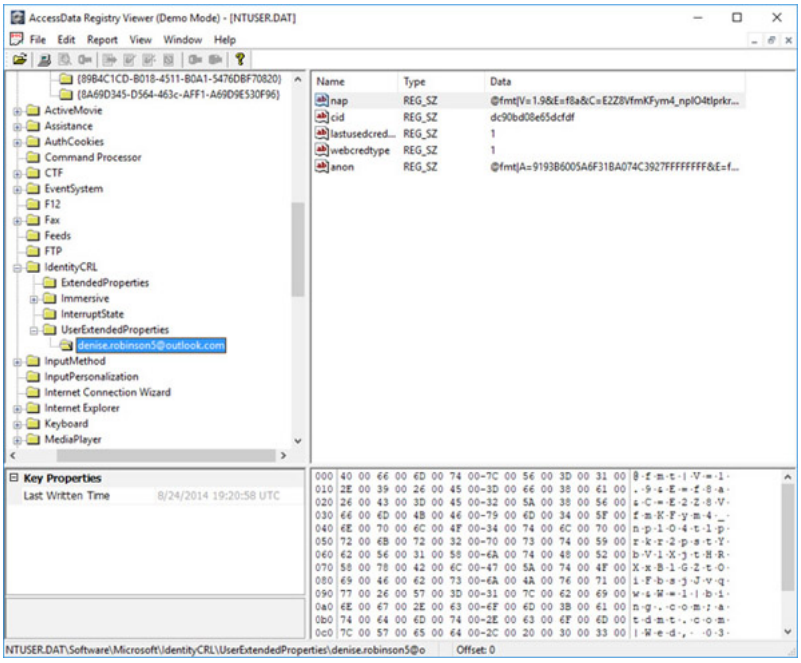
Estimated completion time: 15 minutes

Activity

In this lab, you look for forensic evidence in the ntuser.dat file belonging to a suspect's user account:

1. In Registry Viewer, click **File**, **Open** from the menu. Navigate to the **Registry Files-Lab5-2** subfolder of your work folder, click the **ntuser.dat** file, and then click **Open**.
2. Click **Edit**, **Find** from the menu. In the Find dialog box, type **Denise** and press **Enter**. The first Registry key associated with Denise is displayed at the upper right.
3. Press the **F3** key to search for the next Registry key containing any references to Denise. Notice the GUID associated with the username account information. Press **F3** again to find the next key, and notice the e-mail account for Denise along with her full name (see Figure 5-10).

Figure 5-10.



Source: AccessData Group, Inc., www.accessdata.com

Viewing e-mail account information

4. Click **Edit**, **Find** from the menu. In the Find dialog box, type **jfriday** and press **Enter** to search for any Registry keys associated with this suspect. A message is displayed stating that Registry Viewer couldn't find any keys associated with this user. This happened because each ntuser.dat file is associated with only one user account.
5. Leave Registry Viewer open as you answer the following review questions. When you're finished, exit Registry Viewer, and shut down the computer.

Review Questions

1. The ntuser.dat file contains information on multiple account holders. True or False?
2. What's the e-mail account for the Denise user?
   a. Denise.Robertson@.comcast.net
   b. Denise@AOL.com
   c. denise.robinson5@outlook.com

d. denise.robinson5@comcast.net

3. The ntuser.dat file contains information on which of the following? (Choose all that apply.)
   a. Drive letter designations
   b. Personalized desktop settings
   c. PID key
   d. MRU devices
4. Password decryption tools often need which of the following to retrieve user passwords? (Choose all that apply.)
   a. SYSTEM hive
   b. SAM hive
   c. ntuser.dat file
   d. Enum folder
5. The ntuser.dat file is in which of the following paths?
   a. C:\Windows\System32\Config
   b. C:\Documents and Settings\Users
   c. C:\Users*username*
   d. C:\SYSTEM

Chapter 6. Current Digital Forensics Tools

Labs included in this chapter:

Lab 6.**1**. Using Autopsy 4.7.0 to Search an Image File

Lab 6.**2**. Using OSForensics to Search an Image of a Hard Drive

Lab 6.**3**. Examining a Corrupt Image File with FTK Imager Lite, Autopsy, and WinHex

Note

Before starting these labs, create a subfolder of your work folder named Ch06.

Lab 6.1. Using Autopsy 4.7.0 to Search an Image File

Objectives

After completing this lab, you will be able to:

- Search an image file in Autopsy
- Use the timeline analysis features in Autopsy

Autopsy offers features for producing reports and includes timeline analysis, hash filtering, keyword searches, and searches for Web artifacts, such as bookmarks, history, and cookies, in Firefox, Chrome, and Internet Explorer. In addition, Autopsy can recover deleted files and extract Exif information from multimedia files. It produces fast results by running background tasks in parallel processes that can take advantage of multicore processors.

Digital forensics tools are constantly improving in capabilities and functions. As a digital forensics examiner, you must learn how to use several tools so that if one tool fails, you can switch to another one. Sometimes tools you've relied on don't always work. In these situations, check whether any updated versions are available that might correct the problem you've encountered.

In this lab, you examine an image file that has the first sector area altered, making it unreadable with Autopsy version 4.3.0 that you installed in **Chapter 1**. You need to download and install Autopsy 4.7.0 (or the most current version), and then search for e-mail evidence containing the keyword "Project2400" and explore the timeline features. The image file with the altered first sector is charlie-2009-12-03.E01.

This lab is divided into two sections: The first explains how to download and install Autopsy 4.7.0, and the second shows you how to analyze the evidence.

Materials Required

This lab requires the following:

- Windows
- Internet access
- Autopsy 4.7.0, downloaded in the first section
- The charlie-2009-12-03.E01 file, downloaded in the second section

Estimated completion time: 240–480 minutes

Caution

Processing the data file used in this lab could take more than 4 hours, so you might want to set up this lab to run overnight. The time it takes depends on your computer's CPU speed, the amount of RAM, and the drive access speed.

Activity

Installing Autopsy 4.7.0

In this lab, you download and install Autopsy 4.7.0:

1. Open File Explorer, and create a subfolder of your work folder called **Autopsy**. Start a Web browser, and go to https://www.autopsy.com/download/. Download the 32-bit or 64-bit installation file to your *Work*/Autopsy folder.
2. In File Explorer, navigate to your ***Work*/ Autopsy** folder. Right-click autopsy-4.7.0-*nn*bit.msi (replacing *nn* with 32 or 64, depending on your computer) and click **Install** to begin the installation. If prompted with the UAC message box, click **Yes** to continue.
3. In the Autopsy Setup Wizard welcome window, click **Next**, and in the Select Installation Folder window, click **Next**. In the Ready to Install window, click **Install**.
4. In the Completing the Autopsy Setup Wizard window, click **Finish**, and then exit Autopsy.

Note

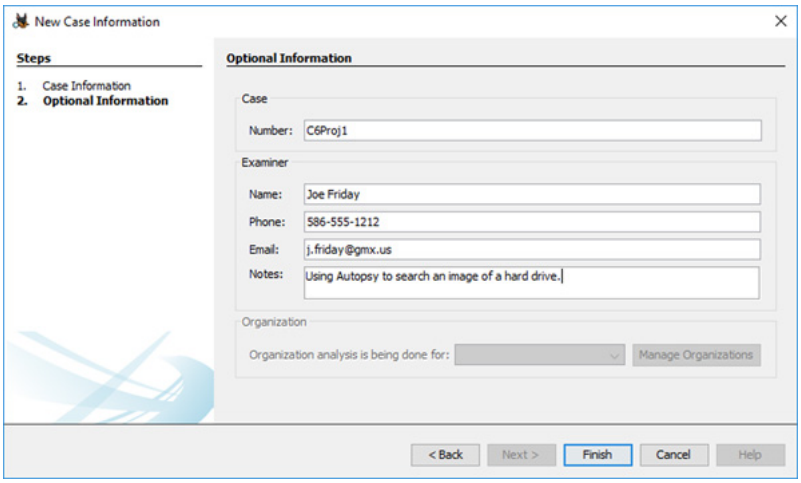
After installing Autopsy 4.7.0, you should have two desktop icons: one for Autopsy 4.3.0 and one for Autopsy 4.7.0. Both programs run separately.

Searching E-mail in Autopsy 4.7.0

In this lab, you use Autopsy to search an image on a Windows computer:

1. Start a Web browser, if necessary, and go to http://downloads.digitalcorpora.org/corpora/scenarios/2009-m57-patents/drives-redacted/. Scroll down, and download **charlie-2009-12-03.E01** file to your work folder.
2. Start Autopsy 4.7.0, and in the Welcome window, click the **Create New Case** button.
3. In the New Case Information window, type **C6Proj1** in the Case Name text box. Click the **Browse** button next to the Base Directory text box, navigate to and click your work folder, click **Select** to enter this path, and then click **Next**. In the Optional Information window, type **C6Proj1** in the Number text box and your name in the Name text box (see Figure 6-1), and then click **Finish**.

Figure 6-1.

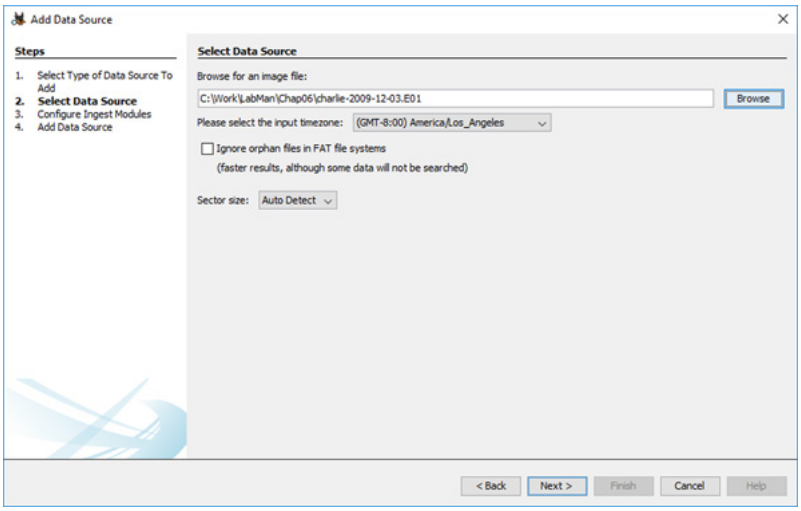


Source: www.sleuthkit.org

Entering case information

4. In the Select Data Source window, click **Disk Image or VM file** in the "Select data source type" list box, if necessary. Click the **Browse** button, navigate to and click your work folder, click **charlie-2009-12-03.E01** , and then click **Open** (see the result in Figure 6-2). Click **Next**.

Figure 6-2.

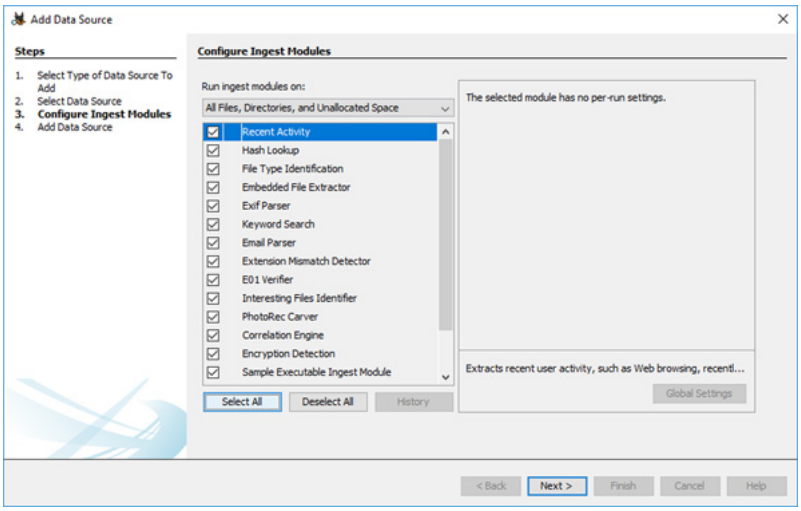


Source: www.sleuthkit.org

Adding an image file

5. In the Configure Ingest Modules window, click **Select All** (see Figure 6-3), and then click **Next** and **Finish** to start analyzing the evidence. (See the Caution at the beginning of this lab about the time this process might take.)

Figure 6-3.



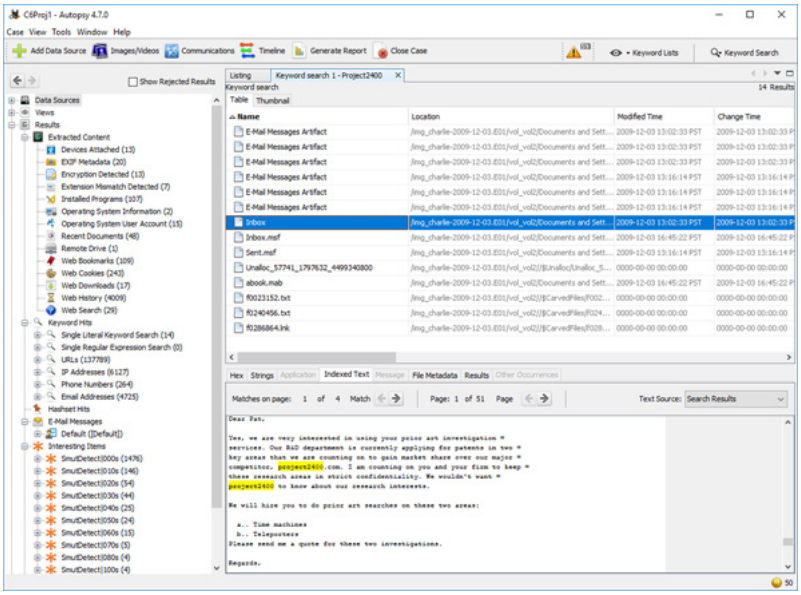
Source: www.sleuthkit.org

Selecting ingest modules

6. Click **Keyword Search** at the upper right, type **Project2400** in the text box, and click the **Search** button. The search should return 14 results.

7. Click the **Keyword search 1 - Project2400** tab in the Result Viewer pane, and then click the **Inbox** entry. Notice that the search results for Project2400 are highlighted in yellow in the Content Viewer pane (see Figure 6-4).

Figure 6-4.



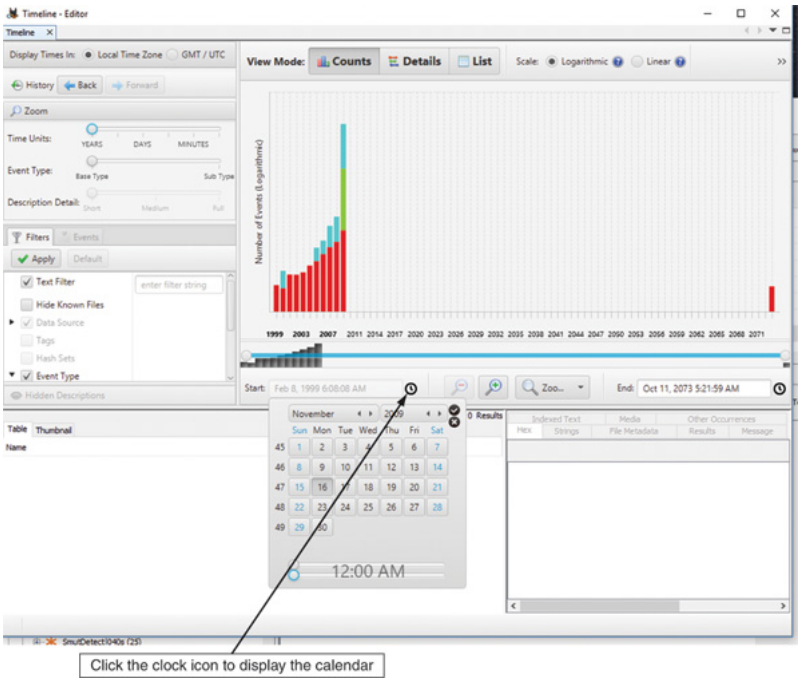
Source: www.sleuthkit.org

Search results displayed in Autopsy

8. Click the **Timeline** toolbar button. By default, the timeline is displayed with a large date range. In this case, you're interested in the period between November 16, 2009, and December 9, 2009. Expand the Timeline - Editor dialog box to make it easier to read, and then click the **clock** icon at the bottom of the upper-right pane. In the calendar, set the starting date to **November 16, 2009**, use the sliders under the calendar to set the time to

12:00 AM, and click the **check mark** icon (see Figure 6-5). Use the same procedure to enter the ending date and time: **December 9, 2009** and **11:59 PM**.

Figure 6-5.

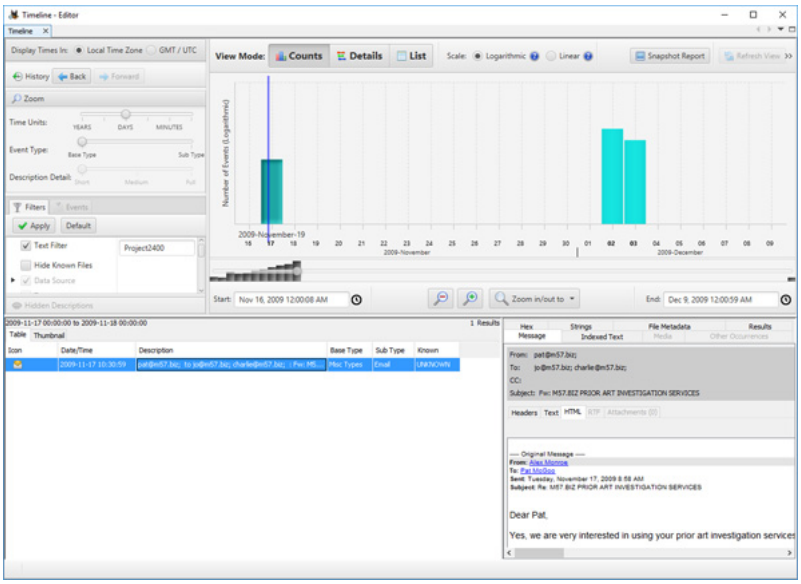


Source: www.sleuthkit.org

Entering timeline settings

9. Click the **Filters** tab, if necessary, on the left. Type **Project2400** in the Text Filter text box, click to select the **Text Filter** check box, and then click the **Apply** button. Click the **Counts** button at the top of the upper-right pane, if necessary, and then click the leftmost bar graph. Click the message displayed in the lower-left pane and view its contents in the lower-right pane (see Figure 6-6). The bar graph heights indicate the number of e-mails per day.

Figure 6-6.



Source: www.sleuthkit.org

Viewing the results of entering a filter value

10. Click the other two bar graphs, and then click the message displayed in the lower-left pane. View each message's contents in the lower-right pane. When you're finished, close this dialog box.

11. In the left pane, expand **Results** and **Extracted Content**, and then click **Web Search**. In the Result Viewer pane, click the **Text** column header to sort its contents alphabetically, and then scroll down and see what searches Charlie performed.

12. Click **Tools, Generate Report** from the menu. In the Generate Report window, click the **Results - HTML** option button, and then click **Next**. In the Configure Artifact Reports window, click **All Results**, and then click **Finish**.

13. When the report is finished, click the **Results - HTML** pathname in the Report Generation Progress window, and leave the report open as you answer the following review questions. When you're finished, exit the Web browser and Autopsy. Save the case, if prompted.

Review Questions

1. How many e-mails did Charlie get?
2. How many e-mails did Charlie send?
3. How many Web searches and Web downloads were done on this computer?
4. In the HTML report, what's the name and IP address of a remote drive connected to this computer?
5. In the results of the filter settings you applied, the bar graph heights indicate the number of e-mails per day. True or False?

Lab 6.2. Using OSForensics to Search an Image of a Hard Drive

Objectives

After completing this lab, you will be able to:

- Search image files in OSForensics
- Use the timeline and file search features in OSForensics

OSForensics can perform searches quickly and is capable of sorting date ranges. Investigators can search for exact phrases, documents, graphics, multimedia files, wildcards, and exclusion files. OSForensics also includes a timeline viewer similar to Autopsy's that can reveal recent activity, such as e-mail correspondence, deleted files, MRU storage devices, attached USB devices, and Web browsing history.

Note

Before beginning this lab, see **Chapter 4** of the textbook for download and installation instructions for OSForensics. In this lab, you use OSForensics to identify additional information in the image from Lab 6.1.

Materials Required

This lab requires the following:

- Windows
- OSForensics
- The charlie-2009-12-03.E01 file from Lab 6.1

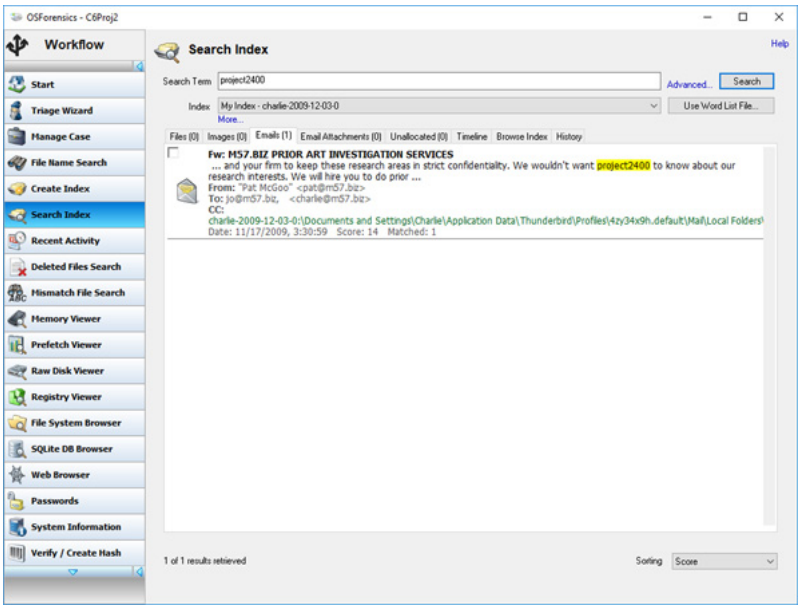
Estimated completion time: 60–120 minutes, depending on your computer's performance

Activity

In this lab, you use OSForensics to search an image on a Windows computer:

1. Start OSForensics. If necessary, click **Continue Using Free Version**. Click **Start** in the left pane, and click **Create Case** in the right pane.
2. In the New Case dialog box, type **C6Proj2** in the Case Name text box and your name in the Investigator text box, and click the **Investigate Disk(s) from Another Machine** option button for the acquisition type. Click **Custom Location** for the case folder. Click the **Browse** button, navigate to and click your work folder, click the **Make New Folder** button, type **C6Proj2**, press **Enter**, and click **OK** twice.
3. Click the **Add Device** button, click the **Image File** option button, and then click the **browse** button. Navigate to and click your work folder, click the **charlie-2009-12-03.E01** file, and click **Open**. Click **Partition 0** in the "Select a partition in the image" dialog box, and then click **OK** twice.
4. Click the **Create Index** button in the left pane. In the Step 1 of 5 window, click the **Use Pre-defined File Types** option button, click the **Uncheck All** button, click the **Emails** and **Images** check boxes, and then click **Next**. In the Step 2 of 5 window, click the **Add** button. In the Add Start Location dialog box, verify that the **Whole Drive** option button is selected, click **OK**, and then click **Next**. In the Step 3 of 5 window, click **Start Indexing**. In the OSForensics - Create Index message box, click **OK** to finish indexing.
5. Click the **Search Index** button in the left pane, type **project2400** in the Search Term text box, and click the **Search** button in the right pane. Figure 6-7 shows the results.

Figure 6-7.

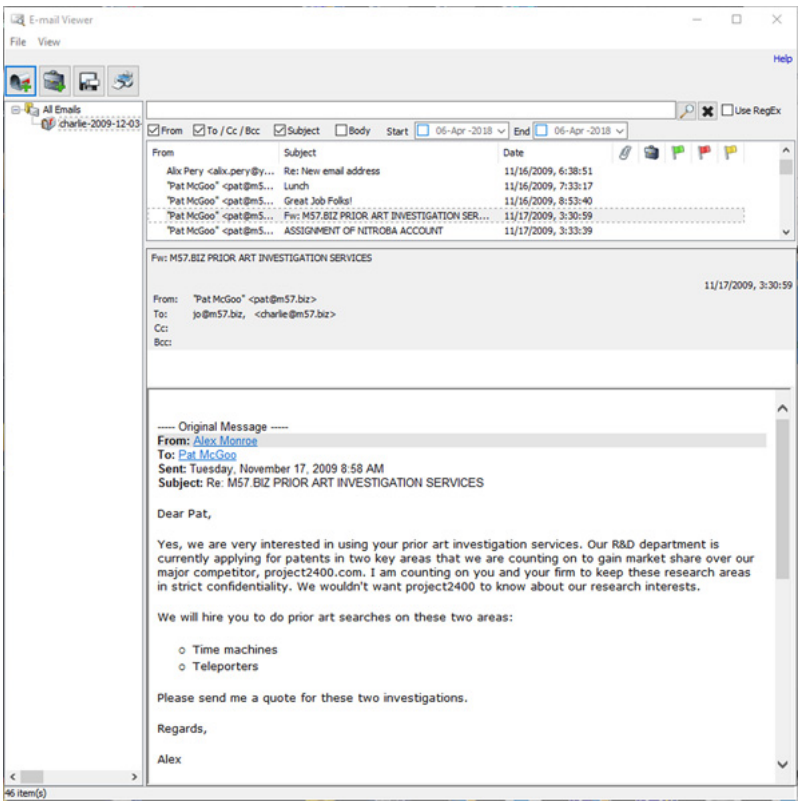


Source: PassMark Software, www.osforensics.com

Viewing the search results

6. Right-click the e-mail in the Search Index pane and click **View with E-mail Viewer** to view its contents in the E-mail Viewer window (see Figure 6-8).

Figure 6-8.



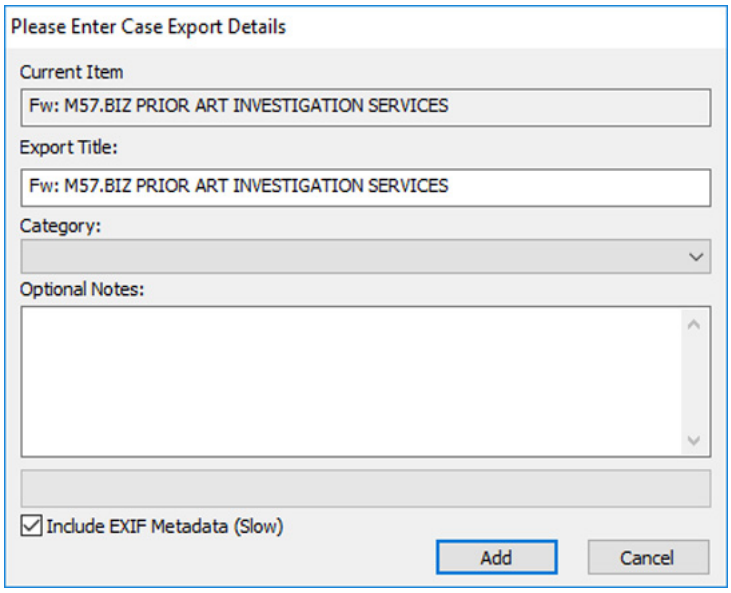
Source: PassMark Software, www.osforensics.com

Examining the e-mail contents

7.

In the E-mail Viewer window's upper pane, click to highlight the message from Pat McGoo dated 11/17/2009, 3:30:59. Click the **Add E-mail to Case** toolbar icon (the briefcase with a plus sign). In the Please Enter Case Export Details dialog box, click the **Include EXIF Metadata (Slow)** check box (see Figure 6-9), and then click **Add**.

Figure 6-9.



Source: PassMark Software, www.osforensics.com

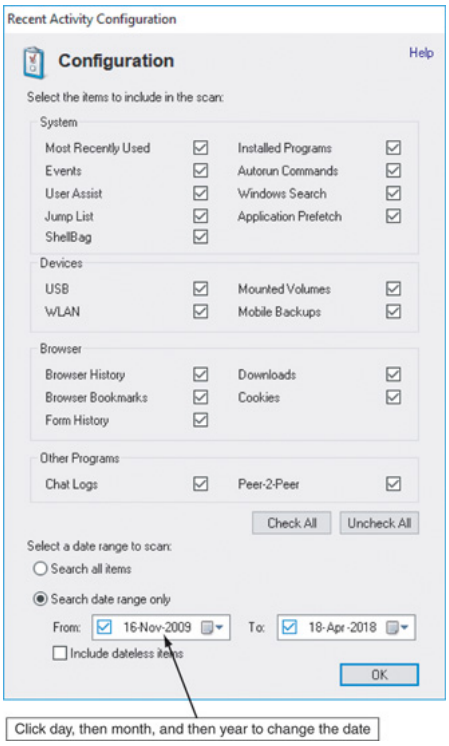
Exporting an e-mail

8. In the E-mail Viewer window's upper pane, right-click the highlighted e-mail, point to **Bookmark**, and click **Red**. Then click **File**, **Close** from the E-mail Viewer menu.

9. Click the **Recent Activity** button in the left pane. In the Recent Activity pane, click the **Scan Drive** option button at the upper left to select the current image, and then click the **Config** button at the upper right to open the Recent Activity Configuration dialog box.

10. Click the **Search date range only** option button. To set the date range, in the From text box, click the current day and type **16**, click the month and type **11** (for November), and then click the year and type **2009** (see Figure 6-10).

Figure 6-10.



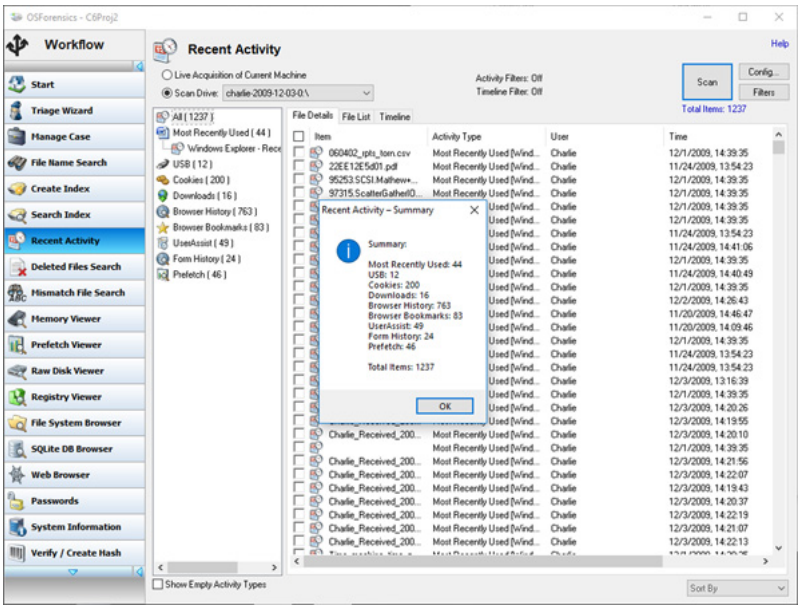
Source: PassMark Software, www.osforensics.com

Setting the From date

11. Repeat **Step 10** for the To text box to set the date to **December 9, 2009**, and then click **OK** to exit the Recent Activity Configuration dialog box.

12. In the Recent Activity pane, click the **Scan** button at the upper right, and then click **OK** in the Recent Activity - Summary dialog box (see Figure 6-11). Then click the **Timeline** tab to display the timeline of events occurring during the date range you configured. Move your cursor over the different colors in the bar graphs to display the number and types of hits found in this scan. To examine the activities in more detail, click the colored section in each bar graph.

Figure 6-11.

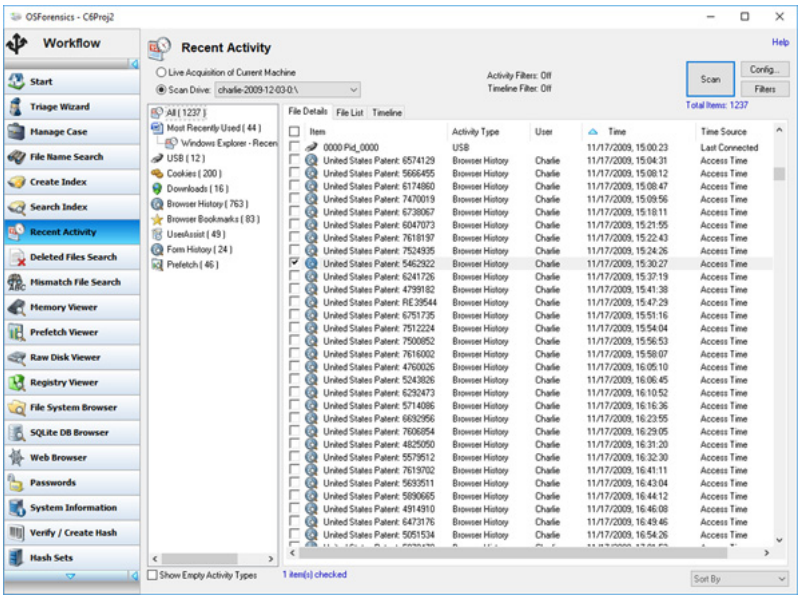


Source: PassMark Software, www.osforensics.com

Viewing the recent activity summary report

13. Click the **File Details** tab, if necessary, and click the **Time** column label to sort activities from oldest at the top to most recent at the bottom. Scroll down until you see the activity dated **11/17/2009, 15:30:27** (see Figure 6-12). Right-click it, point to **Open URL**, and click **Open URL with Internet Browser** to identify the Web page contents.

Figure 6-12.



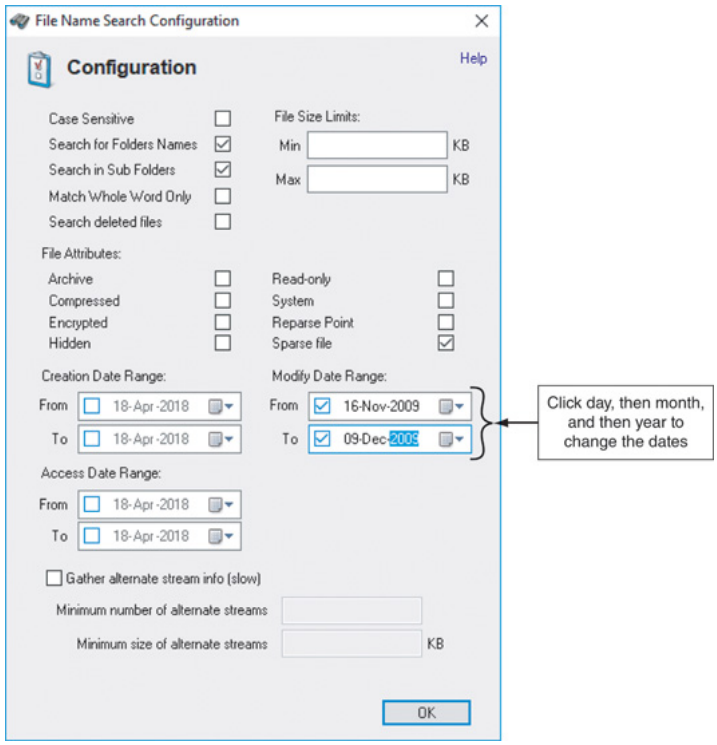
Source: PassMark Software, www.osforensics.com

Finding recent activity for November 17, 2009, 3:30 p.m.

14. Click the **File Name Search** button in the left pane. In the File Name Search pane on the right, click the **ellipse** button next to the Start Folder text box, click **charlie-2009-12-03-0** , and click **OK**. If necessary, click the **Presets** list arrow, and click **Images**. Click the **Config** button to open the File Name Search Configuration dialog box. Under the Modify Date Range heading, click the **From** check box, and then set the From date to

November 16, 2009. Click the **To** check box, and set the To date to **December 9, 2009**, as described in Steps 10 and 11 (see Figure 6-13). Click **OK**.

Figure 6-13.

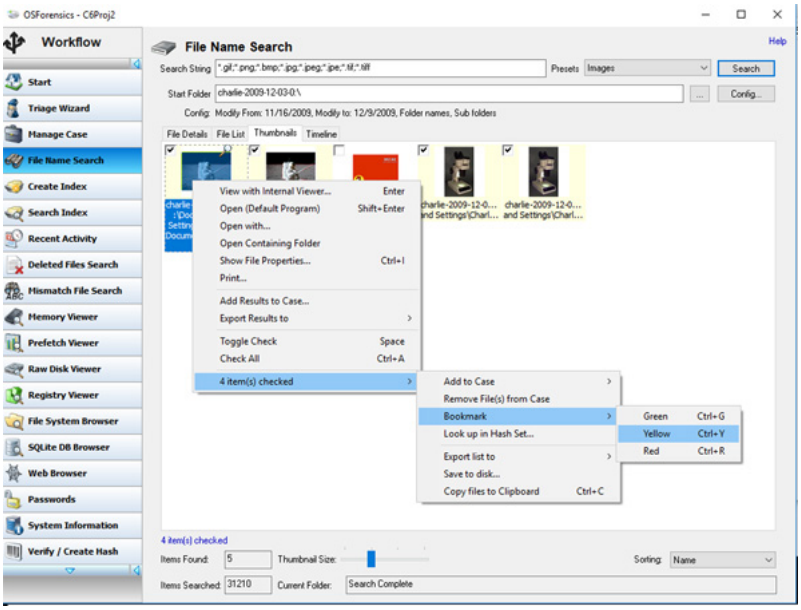


Source: PassMark Software, www.osforensics.com

Setting the date range

15. Click the **Search** button at the upper right of the File Name Search pane. Click the **Thumbnails** tab, and then click the check boxes for all .JPG files. Right-click the first highlighted file, point to **4 item(s) checked** and **Bookmark** (see Figure 6-14), and click **Yellow**.

Figure 6-14.



Source: PassMark Software, www.osforensics.com

Bookmarking .JPG files

16. Click **Start** in the left pane, and click **Generate Report** in the right pane. In the Export Report dialog box, click the **Copy files to report location** option button, and then click **OK**. If necessary, click **OK** in the error message. If the report doesn't open automatically, start a Web browser, and open the **report.html** file in the C6Proj2\Case Report subfolder of your work folder.

17. Leave OSForensics and the Web browser open as you answer the following review questions. When you're finished, exit OSForensics and the Web browser.

Review Questions

1. What was the subject, the sender's name, and the company name in the e-mail sent to Charlie on November 17, 2009, at 3:30 p.m.?
2. How many yellow bookmarks are listed in the HTML report for this case?
3. According to the Recent Activity pane of OSForensics, under the Prefetch heading in the tree view, when was Firefox last run?
4. In the Recent Activity pane of OSForensics, under the Browser History heading in the tree view, what Web page does the item for November 17, 2009, 3:30:27 p.m. open?
5. How many search results did you find for the Project2400 keyword?

Lab 6.3. Examining a Corrupt Image File with FTK Imager Lite, Autopsy, and WinHex

Objectives

After completing this lab, you will be able to:

- Mount an image file as a drive in FTK Imager Lite
- Explain how to identify a corrupt image with WinHex

In **Lab 6.1**, you learned that the charlie-2009-12-03.E01 image couldn't be loaded in Autopsy 4.3.0. In this lab, you examine this image's boot sector to try to find out why Autopsy couldn't read it. This lab is divided into two sections: testing the image in Autopsy 4.3.0 to see the error

message and loading charlie-2009-12-03.E01 in WinHex and comparing it with a known good drive's sector 0.

Materials Required

This lab requires the following:

- Windows
- FTK Imager Lite, Autopsy 4.3.0, and WinHex
- The charlie-2009-12-03.E01 file from Lab 6.1

Estimated completion time: 60 minutes

Activity

Testing an Image File in Autopsy 4.3.0

In this section, you see the error message that occurs when attempting to load charlie-2009-12-03.E01 in Autopsy 4.3.0:

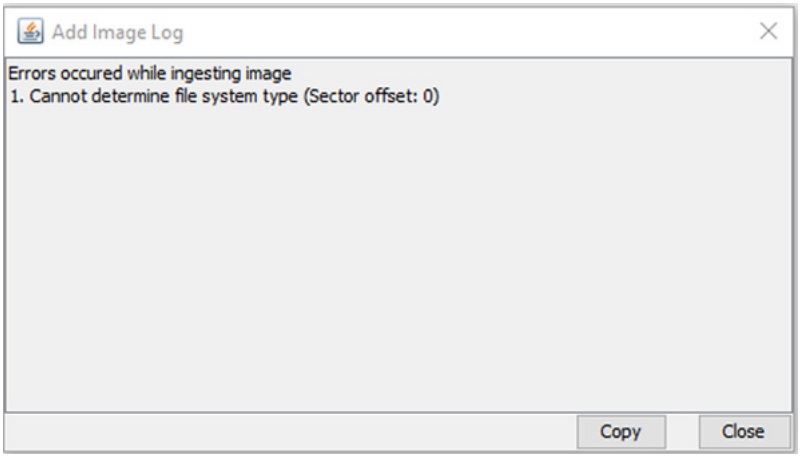
1. Start Autopsy 4.3.0, and click the **Create New Case** button. In the New Case Information window, enter **C6Proj3-1** in the Case Name text box, and click **Browse** next to the Base Directory text box. Navigate to and click your work folder, and click **Select** to enter this path. Make sure the **Single-user** option button is selected for Case Type, and then click **Next**.
2. In the Additional Information window, type **C6Proj3-1** in the Case Number text box and your name in the Examiner text box, and then click **Finish** to start the Add Data Source Wizard.
3. In the Select Data Source window, click **Disk Image or VM file**in the "Select data source type" list box, if necessary. Click the **Browse** button, navigate to and click your work folder, click the **charlie-2009-12-03.E01** file, and then click **Open**. Click **Next**.

Tip

If you get an error message stating that Autopsy 4.3.0 is missing links, exit the program and reinstall it. In the Autopsy Installation Wizard, click the Repair button to correct this error.

4. Keep the default settings in the Configure Ingest Modules window. Click **Next** and then **Finish**.
5. When the error message box is displayed, click the **View Log** button in the Add Data Source window, and then click the **Copy** and **Close** buttons shown in Figure 6-15. Click **Finish**, and then exit Autopsy.

Figure 6-15.



Source: www.sleuthkit.org

Viewing the log error

6. Start a new document in Notepad, and paste the copied error message. Save it as **C6Proj3-1-Autopsy-Error-Msg.txt** in your work folder, and exit Notepad. Proceed to the next section.

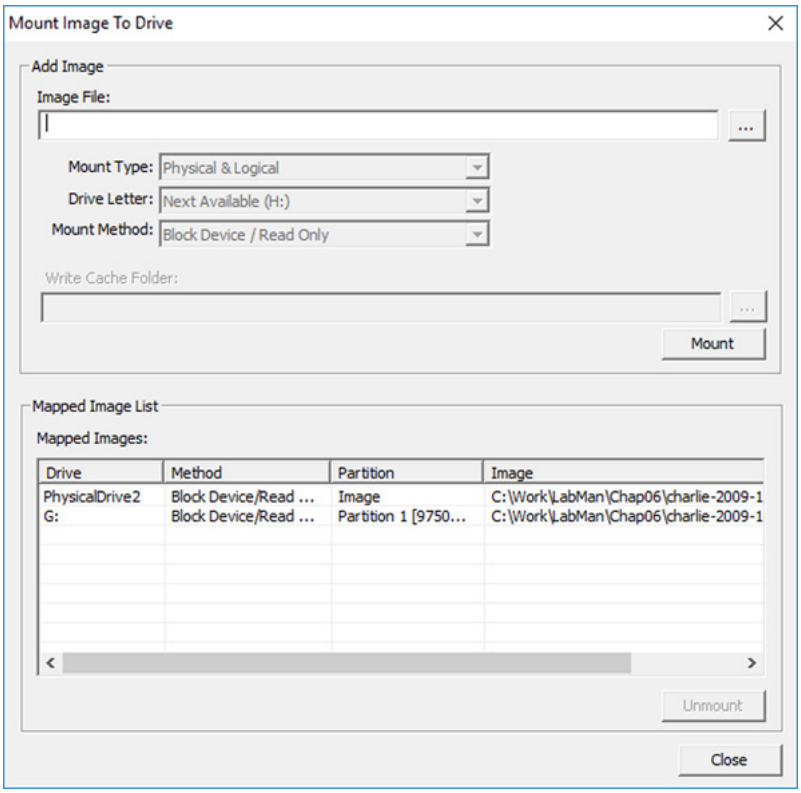
Examining Image Files in WinHex

The error message in **Figure 6-15** states that Autopsy 4.3.0 can't determine the file system when it attempts to read sector 0 of charlie-2009-12-03.E01. In this section, you use WinHex to compare sector 0 of the charlie-2009-12-03.E01 image and your computer's C drive to discover any differences that might have caused this error. For more information on what sector 0 of an NTFS disk drive should contain, refer to the following sources:

- NTFS Partition Boot Sector at www.ntfs.com/ntfs-partition-boot-sector.htm
- Master Boot Sector at https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc976796(v=technet.10)
- COEN 252 Computer Forensics NTFS at www.cse.scu.edu/~tschwarz/COEN252_09/Lectures/NTFS.html
- Disk Concepts and Troubleshooting at https://technet.microsoft.com/en-us/library/cc977221.aspx

1. Start FTK Imager Lite, and click **File**, **Image Mounting** from the menu. In the Mount Image To Drive dialog box, click the **browse** button next to the Image File text box. Navigate to your ***Work*\C6Proj3-2** folder, double-click **charlie-2009-12-03.E01** , and then click the **Mount** button. In the Mapped Image List section at the bottom, note the PhysicalDrive number and the drive letter created for this image file (see Figure 6-16), and then click **Close**. Leave FTK Imager Lite running in the background.

Figure 6-16.



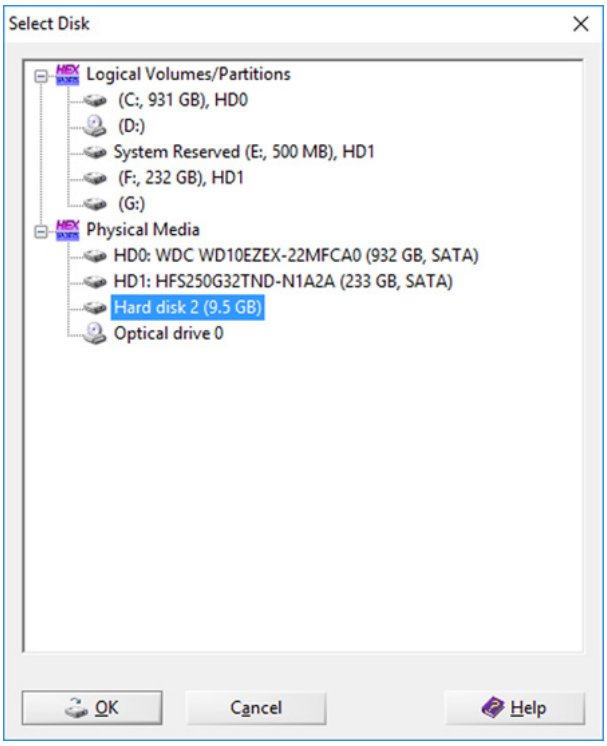
Source: AccessData Group, Inc., www.accessdata.com

Mounting charlie-2009-12-03.E01 in FTK Imager Lite

Note

Figure 6-16 shows that FTK Imager Lite defines the mounted image as PhysicalDrive2 for Drive G. Figure 6-17 shows that WinHex defines it as Hard disk 2 (9.5 GB) for Drive G. Your drive number and letter will most likely be different. In the following steps, substitute the drive number and letter you see in Figures 6-16 and 6-17.

Figure 6-17.



Source: X-Ways AG, www.x-ways.net

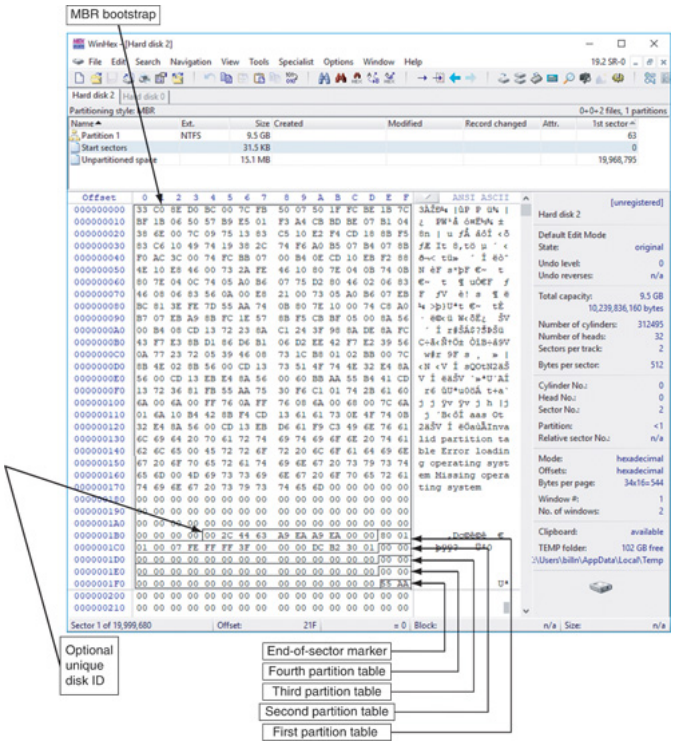
Selecting disk drives in WinHex

2. Start WinHex, and click **OK** in the evaluation warning message. Click **Tools**, **Open Disk** from the menu to open the Select Disk dialog box. Notice that the PhysicalDrive2 entry you saw in FTK Imager Lite is listed as Hard disk 2 in WinHex (refer back to Figure 6-17). Click **Hard disk 2 (9.5 GB)** under the Physical Media heading, and then click **OK**.

3. Click **Tools**, **Open** from the menu again. Under the Physical Media heading, click **HD0: *your-computer-drive's-physical-name*** (which will differ from what's shown in Figure 6-17), and then click **OK**. Click the **Hard disk 2** tab. In the Data Browser pane (upper pane), click **Start sectors**. Then click the **Hard disk 0** tab, and click **Start sectors**.

4. For Windows drives, sector 0 of the MBR is made up of the following fields: the MBR bootstrap starting at offset 000000000; the optional unique disk ID starting at offset 0000001B4; the first partition table starting at offset 0000001BE; the second partition table starting at 0000001CE, the third partition table starting at offset 0000001DE; the fourth partition table starting at offset 0000001EE; and the end-of-sector marker starting at offset 0000001FE. Examine these fields in **Figure 6-18**.

Figure 6-18.

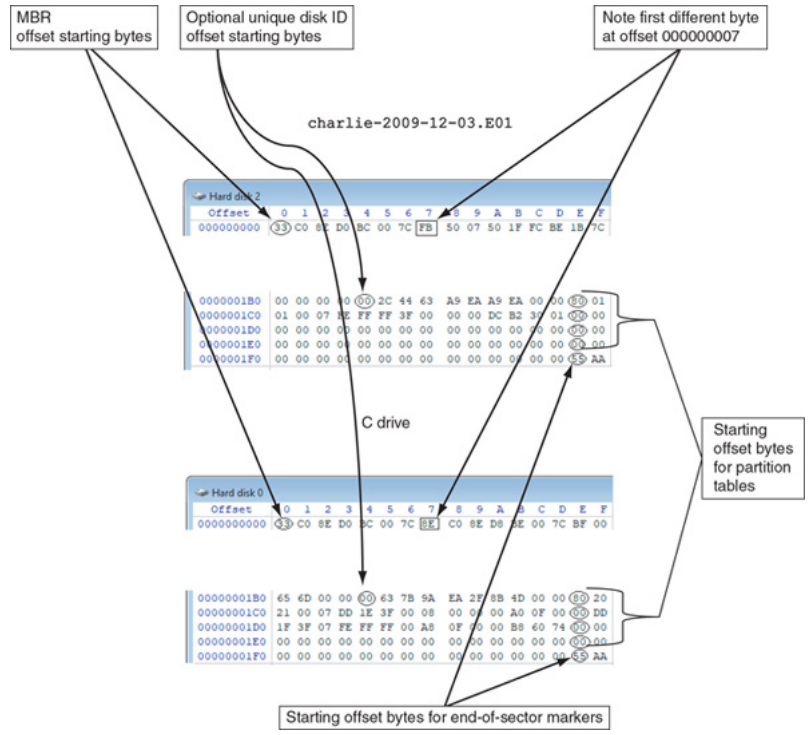


Source: X-Ways AG, www.x-ways.net

Displaying the MBR fields

5. At offsets 0000000000 through 0000000006 the hexadecimal values are identical for both the image and drive C. From offset 000000007 through offset 0000001BD, however, the hexadecimal values are different (see **Figure 6-19**). This difference indicates that the MBR bootstrap code has been altered and might explain why Autopsy 4.3.0 is unable to read sector 0 and identify the file system type. Based on this examination of the MBR, it seems that unlike Autopsy 4.7.0, Autopsy 4.3.0 requires more than the first 7 bytes of the charlie-2009-12-03.E01 file to determine its file system type.

Figure 6-19.



Source: X-Ways AG, www.x-ways.net

Comparing sectors 0 of charlie-2009-12-03.E01 and your C drive

6. Leave FTK Imager Lite and WinHex open as you answer the following review questions. When you're finished, exit FTK Imager Lite and WinHex.

Review Questions

1. When you attempted to load charlie-2009-12-03.E01 in Autopsy 4.3.0, what error message was displayed?
   a. Failed to add data source (critical errors encountered)
   b. Cannot determine file system type (Sector offset: 0)
   c. Cannot determine file system type (Cluster offset: 2)
   d. Failed to load Configure Ingest Module
2. In what dialog box did Autopsy 4.3.0 fail to load charlie-2009-12-03.E01?
   a. Select Data Source
   b. Configure Ingest Modules
   c. Add Data Source
   d. Reporting
3. What are the hexadecimal values for the optional unique disk ID in the MBR for the charlie-2009-12-03.001 image?
   a. 00 2C 44 63 A9 EA A9 EA 00 00
   b. 33 C0 8E D0 BC 00 7C FB
   c. 80 01 01 00 07 FE FF FF 3F 00 00 00 DC B2 30 01
   d. 33 C0 8E D0 BC 00 7C 8E
4. What's the starting offset for a drive's second partition table?

a. 0000001B4

b. 0000001BE

c. 0000001CE

d. 0000001FF

5. FTK Imager Lite can mount both the physical and logical drives of a forensic image. True or False?

Chapter 7. Linux and Macintosh File Systems

Labs included in this chapter:

Lab 7.1 Using Autopsy to Process a Mac OS X Image

Lab 7.2 Using Autopsy to Process a Mac OS 9 Image

Lab 7.3 Using Autopsy to Process a Linux Image

Note

Before starting these labs, create a subfolder of your work folder named Ch07.

Lab 7.1. Using Autopsy to Process a Mac OS X Image

Objectives

After completing this lab, you will be able to:

- Import an OS X image into Autopsy
- Use Autopsy to search for evidence in an OS X image

Autopsy can analyze and extract data from not only Windows and Linux file systems, but also macOS, Mac OS X, and Mac OS 9 file systems. The file system Apple developed for OS X is HFS+. In this lab, you import an OS X image into Autopsy and process it to look for potential evidence.

Materials Required

This lab requires the following:

- Windows
- Autopsy 4.3.0
- The GCFI-OSX.zip file

Estimated completion time: 180–300 minutes

Caution

Processing the data file used in this lab can take 4 hours or more, so you might want to set up this lab to run overnight. The time it takes depends on your computer's CPU speed, the amount of RAM, and the drive access speed.

Activity

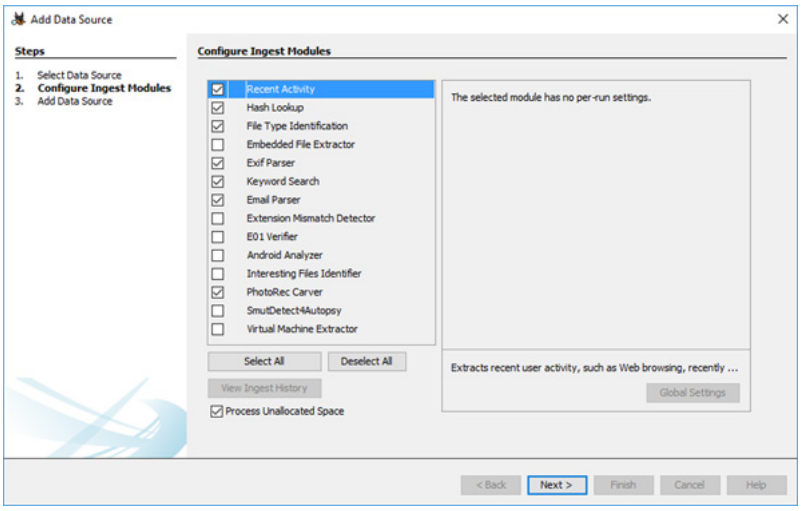
In this lab, you import an OS X image into Autopsy to process evidence:

1. Extract the **GCFI-OSX.zip** file to your work folder. (This process might take a few minutes.) Start Autopsy, and in the Welcome window, click the **Create New Case** button. In the New Case Information window, type **C7Proj1** in the Case Name text box. Click the **Browse** button next to the Base Directory text box, navigate to and click your work folder, click **Select** to enter this path, and then click **Next**.
2. In the Additional Information window, type **C7Proj1** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

3. In the Select Data Source window, click **Disk Image or VM file** in the "Select data source type" list box, if necessary. Click the **Browse** button, navigate to and click your work folder, click the **GCFI-OSX.001** file, and then click **Open**. Click **Next**.

4. In the Configure Ingest Modules window, click **Deselect All**, and then click the **Recent Activity**, **Hash Lookup**, **File Type Identification**, **Exif Parser**, **Keyword Search**, **Email Parser**, and **PhotoRec Carver** check boxes, as shown in Figure 7-1. Click **Next** and then **Finish** to start analyzing the evidence, which could take 4 hours or more. (See the Caution at the beginning of this lab.)

Figure 7-1.



Source: www.sleuthkit.org

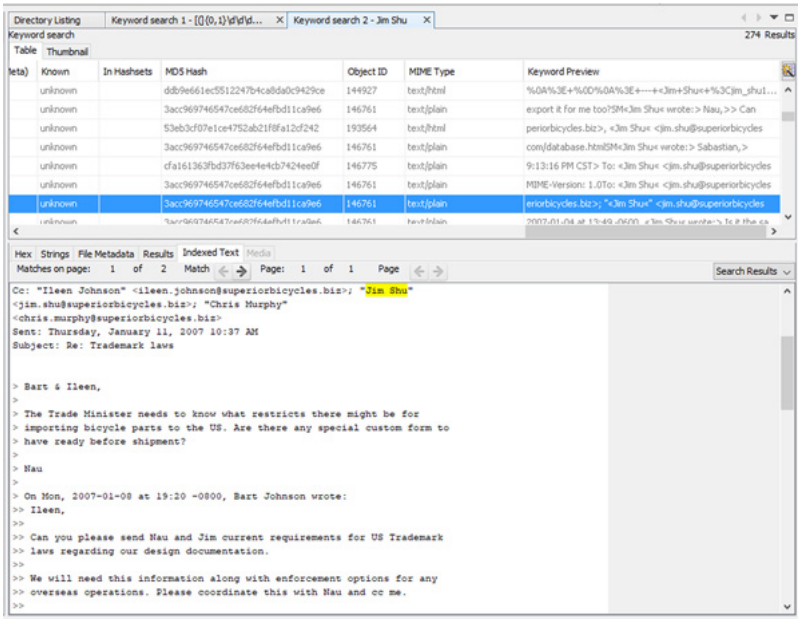
Selecting ingest modules

5. Click the **Keyword Lists** down arrow. Click the **Phone Numbers**, **IP Addresses**, **Email Addresses**, and **URLs** check boxes, and then click the **Search** button. Autopsy begins searching the image, which could take an hour or more.

6. Click **Keyword Search** at the upper right, type **Jim Shu** in the text box, and click **Search**. When the search is finished, click the **Keyword search 2 - Jim Shu** tab, if necessary. Click each item in the Result Viewer pane related to Jim Shu, and examine its contents in the Content Viewer pane.

7. Scroll to the right to display all the file attributes, such as location, timestamps, size, file types, MD5 hash sets, and keyword previews (see **Figure 7-2**).

Figure 7-2.



Source: www.sleuthkit.org

Viewing file attributes

8. In the left pane, expand **Data Sources** and **GCFI-OSX.001** to view the file system folders in the image along with the number of files or folders in each folder. Next, expand **Views**, **File Types**, and **By Extension**, and then click **Images** to see all the graphics files. Click the **Thumbnail** tab in the Result Viewer pane to see the graphics.

9. Under File Types, expand **Documents** to view the file types and the number of hits. To see the plaintext files, click **Plain Text**, and then click the **Table** tab in the Result Viewer pane. Click a file to view it in the Content Viewer pane.

10. In the left pane, expand **Results** and **Keyword Hits**, and then expand **Phone Numbers**, **IP Addresses**, **Email Addresses**, and **URLs** to see the search results.

11. Under Results in the left pane, expand **E-Mail Messages** and its subfolders to view correspondence with Jim Shu, including sent messages, deleted messages, the inbox, and so forth.

12. Leave Autopsy open as you answer the following review questions. When you're finished, click **File**, **Close Case** from the menu, and leave Autopsy running for the next lab.

Review Questions

1. How many Word files are in the GCFI-OSX.001 image?

2. What or who is the subject of the first message from Jim Shu?

   a. Sebastian

   b. Jim Shu

   c. Superior Bicycles

   d. Free tools

3. What phone number had the most search results?

   a. 602-839-2763

   b. 800-810-0595

c. 662-656-5045

d. 859-232-2380

4. The Ext3 file system is used in Mac OS X. True or False?

5. Who sent the last e-mail to Jim Shu?

   a. Martha Dax

   b. Sebastian Mwangonde

   c. Nau Tjeriko

   d. Bart Johnson

Lab 7.2. Using Autopsy to Process a Mac OS 9 Image

Objectives

After completing this lab, you will be able to:

> - Import an OS 9 image into Autopsy
> - Use Autopsy to search for evidence in an OS 9 image

Mac OS 9 is also known as Apple's "classic Mac" OS. This OS, introduced in 1997, lacks many of the features in current file systems, such as protected memory and preemptive multitasking; it uses the older HFS file system. In 2002, Apple officially discontinued OS 9 and later developed Mac OS X and the current macOS operating system. Because forensics investigators might still encounter OS 9 images on older Apple hardware, however, you use Autopsy in this lab to examine an OS 9 image file and search for potential evidence. Because the HFS file system is so different from other file systems, such as those in Linux and Windows, Autopsy 4.3.0 displays files as though they were carved from unallocated space on the drive. Dates and times for recovered files show only zero values.

Materials Required

This lab requires the following:

- Windows
- Autopsy 4.3.0
- The GCFI-OS9.zip file

Estimated completion time: 240–300 minutes

Caution

Processing the data file used in this lab can take 4 hours or more, so you might want to set up this lab to run overnight. The time it takes depends on your computer's CPU speed, the amount of RAM, and the drive access speed.

Activity

In this lab, you import an OS 9 image into Autopsy to process evidence:

1. Extract the **GCFI-OS9.zip** file to your work folder, which might take a few minutes. In Autopsy, click **Case**, **New Case** from the menu. In the New Case Information window,

type **C7Proj2** in the Case Name text box. Verify that your work folder is displayed in the Base Directory text box, and then click **Next**.

2. In the Additional Information window, type **C7Proj2** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

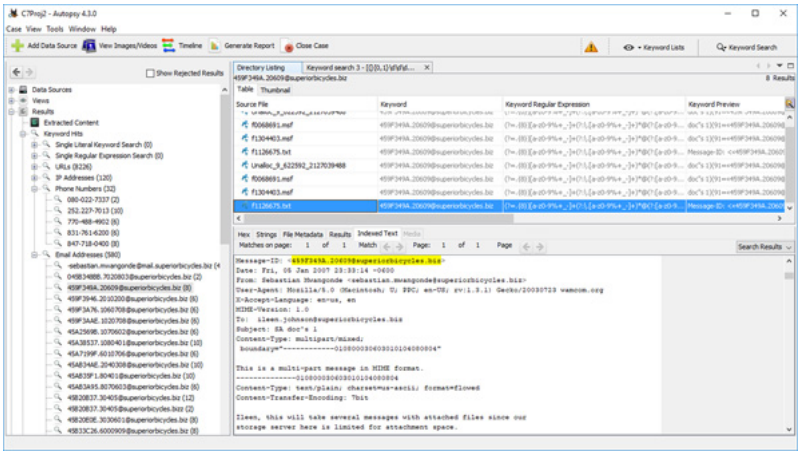
3. In the Select Data Source window, click **Disk Image or VM file** in the "Select data source type" list box, if necessary. Click the **Browse** button, navigate to and click your work folder, click the **GCFI-OS9.001** file, and then click **Open**. Click **Next**.

4. Click **Next** to accept the selected ingest modules (retained from Lab 7.1), and then click **Finish** to start analyzing the evidence, which could take a while.

5. Click the **Keyword Lists** down arrow. Click the **Phone Numbers**, **IP Addresses**, **Email Addresses**, and **URLs** check boxes, and then click the **Search** button. Autopsy begins searching the image, which could take up to 4 hours or more.

6. In the left pane, expand **Keyword Hits**, if necessary, and then expand **Phone Numbers**, **IP Addresses**, **Email Addresses**, and **URLs** to see the search results. Examine the e-mail address results for details such as timestamps and the text of messages (see Figure 7-3).

Figure 7-3.

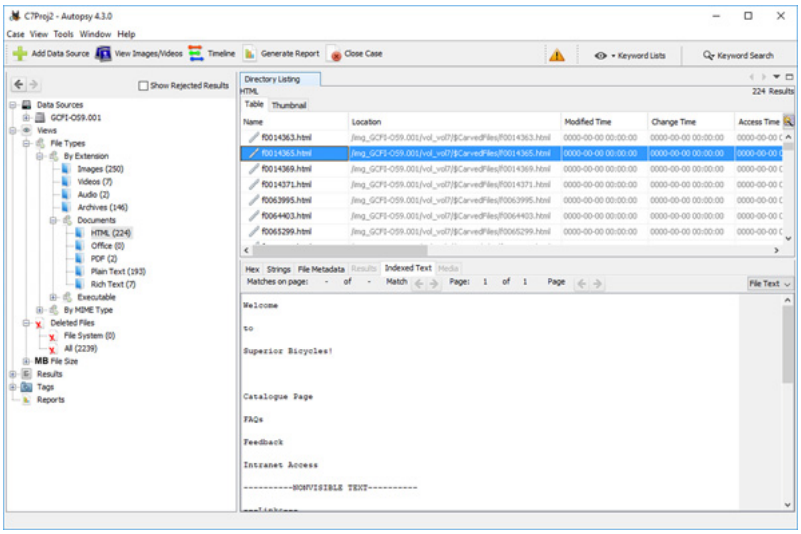


Source: www.sleuthkit.org

Viewing the results of an e-mail search

7. In the left pane, expand **Views**, **File Types**, **By Extension**, and **Documents**, and click **HTML** to view carved HTML files. To view their data, click a file in the Result Viewer pane to see its data in the Content Viewer pane, or click the **Thumbnail** tab to see just the image with its filename. Repeat this process for the **Videos** and **Audio** folders (see Figure 7-4).

Figure 7-4.



Source: www.sleuthkit.org

Viewing files in the HFS drive

Note

Autopsy 4.3.0 can't display filenames and metadata for HFS file systems. It can, however, carve files so that you can search for them and examine their contents. This is why Autopsy displays files starting with the letter "f" followed by a unique number and file extension. For more information on HFS and HFS+, see www.macdisk.com/macforken.php.

8. Leave Autopsy open as you answer the following review questions. When you're finished, click **File**, **Close Case** from the menu, and leave Autopsy running for the next lab.

Review Questions

1. Mac OS 9 uses the HFS file system. True or False?
2. How many videos are in the GCFI-OS9.001 image?
3. The GCFI-OS9.001 image contains executable files. True or False?
4. Which phone number was dialed most often?
   a. 847-718-0400
   b. 770-488-4902
   c. 831-761-6200
   d. 252-227-7013
5. Autopsy displays HFS files as though they were carved from allocated space. True or False?

Lab 7.3. Using Autopsy to Process a Linux Image

Objectives

After completing this lab, you will be able to:

- Import a Linux image into Autopsy
- Use Autopsy to search for evidence on a Linux partition

The Ext3 file system, used in many Linux distributions, added a journaling capability, which has a built-in file recovery mechanism used after a crash. With the increasing popularity of open-source office suites, such as OpenOffice and LibreOffice, forensics investigators are likely to find systems formatted in Ext3. Ext4, the most recent file system, is included in the Linux 4.16 kernel. Autopsy can be used to search images formatted in this file system, too. In this lab, you extract a Linux image and import it into Autopsy for analysis.

Materials Required

This lab requires the following:

- Windows
- Autopsy 4.3.0
- The GCFI-LX.xxx.exe file

Estimated completion time: 180–240 minutes

Caution

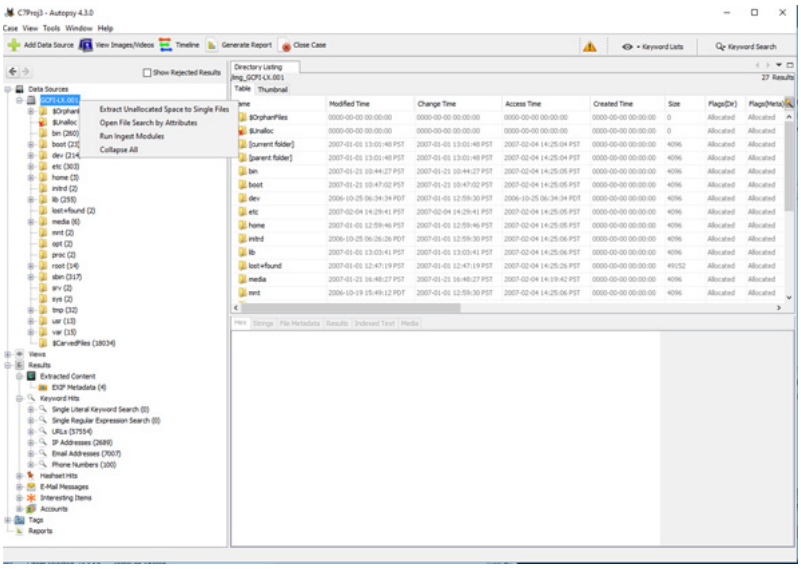
Processing the data file used in this lab can take 4 hours or more, so you might want to set up this lab to run overnight. The time it takes depends on your computer's CPU speed, the amount of RAM, and the drive access speed.

Activity

In this lab, you load a Linux image in Autopsy to process evidence:

1. Extract the **GCFI-LX.xxx.exe** file to your work folder, which might take a few minutes. In Autopsy, click **Case**, **New Case** from the menu. In the New Case Information window, type **C7Proj3** in the Case Name text box, verify that your work folder is displayed in the Base Directory text box, and then click **Next**.
2. In the Additional Information window, type **C7Proj3** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.
3. In the Select Data Source window, click **Disk Image or VM file** in the "Select data source type" list box, if necessary. Click the **Browse** button, navigate to and click your work folder, click the **GCFI-LX.001** file, and then click **Open**. Click **Next**.
4. Click **Next** to accept the selected ingest modules (retained from Lab 7.1), and then click **Finish** to start analyzing the evidence.
5. In the left pane, expand **Data Sources** and **GCFI-LX.001** to view the folder structure (see Figure 7-5). This structure is common in many Linux distributions. Right-click **GCFI-LX.001** to see these options: Extract Unallocated Space to Single Files, Open File Search by Attributes, and Run Ingest Modules (used to process the image again).

Figure 7-5.

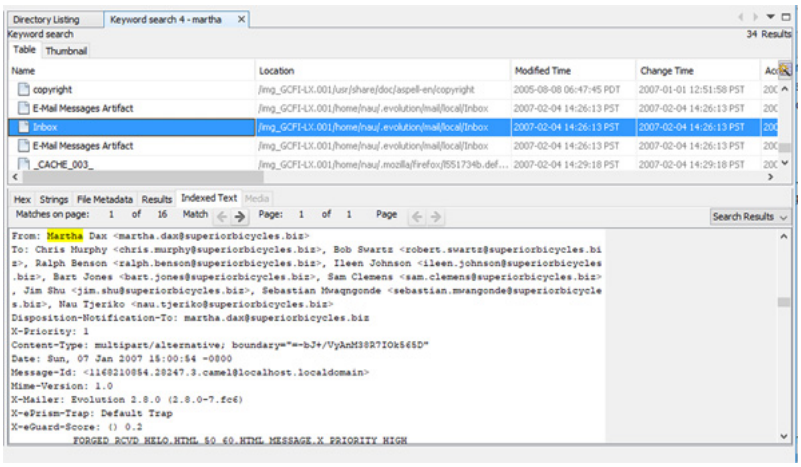


Source: www.sleuthkit.org

Viewing the folder structure

6. Click **Keyword Search** at the upper right, type **martha** in the text box, and click **Search**. In the Result Viewer pane, click the **Keyword search 4 - martha** tab, if necessary, to view all the search results. Scroll down and click the **Inbox** entry to view the e-mail Martha Dax sent to Chris Murphy (see Figure 7-6).

Figure 7-6.



Source: www.sleuthkit.org

Viewing received e-mails

Note

If you exited Autopsy in the previous lab and restarted it for this lab, the Keyword search tab is numbered 1 rather than 4, as in **Figure 7-6**. Likewise, the search tab in the next step will be numbered 2 instead of 5.

7. Click **Keyword Search** at the upper right, type **Chris Murphy** in the text box, and click **Search**. Click the **Keyword search 5 - Chris Murphy** tab, if necessary. In the left pane,

click to expand **Results**, **E-Mail Messages**, and **Default [Default]**, and then click the **Default** folder to see all e-mail correspondence.

8. In the left pane, expand **Extracted Content**, and then click **Extension Mismatch Detected** to view file extensions that don't match their file types. This information might reveal files that have been altered to keep them hidden.

9. Leave Autopsy open as you answer the following review questions. When you're finished, exit Autopsy.

Review Questions

1. How many recovered e-mails are listed under the Default folder?
2. How many Word and Excel files were recovered in this image?
3. Martha communicated via e-mail only with Chris Murphy. True or False?
4. Ext3's journaling feature keeps a log of errors. True or False?
5. In the Results subfolders, how many search matches do you see for the "martha" keyword?

Chapter 8. Recovering Graphics Files

Labs included in this chapter:

Lab 8.1 Using Autopsy to Analyze Multimedia Files

Lab 8.2 Using OSForensics to Analyze Multimedia Files

Lab 8.3 Using WinHex to Analyze Multimedia Files

Note

Before starting these labs, create a subfolder of your work folder named Ch08.

Lab 8.1. Using Autopsy to Analyze Multimedia Files

Objectives

After completing this lab, you will be able to:

- Use Autopsy to analyze multimedia files
- Identify deleted graphics or video files in evidence

Autopsy has tools that can recognize graphics files in images and extract Exif information. Additional features include finding other multimedia files, such as video and audio files, and recovering deleted files from unallocated space. Autopsy also provides graphics information, such as timestamps, MD5 hash values, and file size. In this lab, you analyze multimedia files in an image.

Materials Required

This lab requires the following:

- Windows
- Autopsy 4.3.0
- The jo-favorites-usb-2009-12-11.E01 file, downloaded in Step 1

Estimated completion time: 15–30 minutes, depending on your computer's performance

Activity

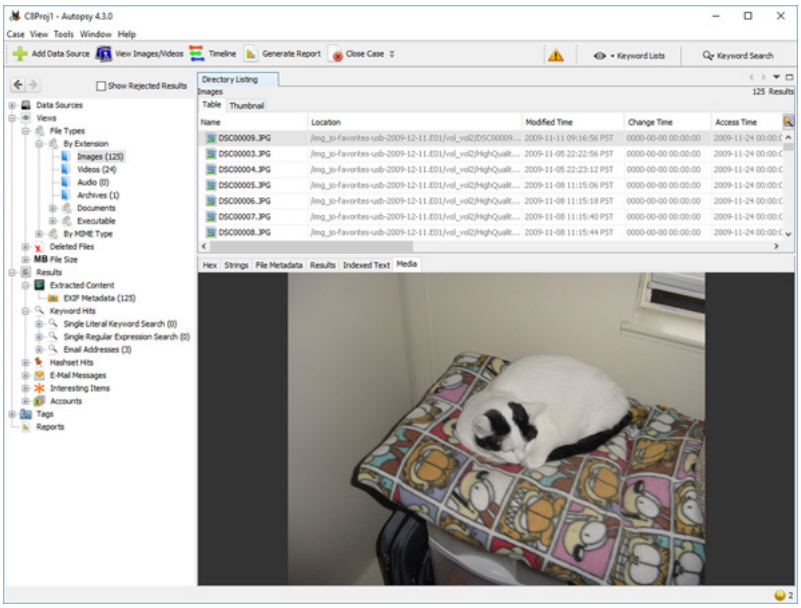
In this lab, you use Autopsy to analyze multimedia files in the jo-favorites-usb-2009-12-11.E01 image of a USB device:

1. Start a Web browser, and go to http://downloads.digitalcorpora.org/corpora/scenarios/2009-m57-patents/drives-redacted/. Download the **jo-favorites-usb-2009-12-11.E01** file to your work folder.
2. Start Autopsy. In the Welcome window, click **Create New Case**.
3. In the New Case Information window, type **C8Proj1** in the Case Name text box. Click the **Browse** button next to the Base Directory text box, navigate to and click your work folder, click **Select** to enter this path, and then click **Next**. In the Additional Information window, type **C8Proj1** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.
4. In the Select Data Source window, click **Disk Image or VM file** in the "Select data source type" list box, if necessary. Click the **Browse** button, navigate to and click your work folder, click the **jo-favorites-usb-2009-12-11.E01** file, and click **Open**. Click **Next**.

5. In the Configure Ingest Modules window, click **Deselect All**, and then click the **Recent Activity**, **Hash Lookup**, **File Type Identification**, **Exif Parser**, **Keyword Search**, **Email Parser**, and **PhotoRec Carver** check boxes. Click **Next** and then **Finish** to start analyzing the evidence.

6. In the left pane, expand **Views**, **File Types**, and **By Extension**, and click the **Images** folders to see the files found on this USB device (see Figure 8-1). In the Result Viewer pane, right-click the first JPG file and click **Properties**. Review the information about the file, and then click **Close**.

Figure 8-1.

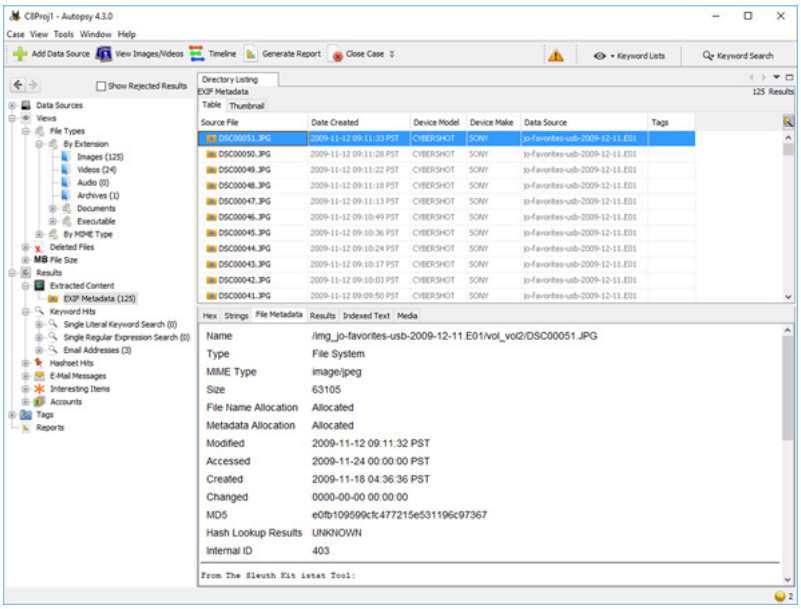


Source: www.sleuthkit.org

Viewing files found in an image

7. Expand **Results** and **Extracted Content**, if necessary, and click **EXIF Metadata** to view the graphics files in the Directory Listing pane. Click the first JPG file, and click the **File Metadata** tab in the Content Viewer pane to view Exif metadata (see Figure 8-2). Click the **Media** tab to view the picture.

Figure 8-2.

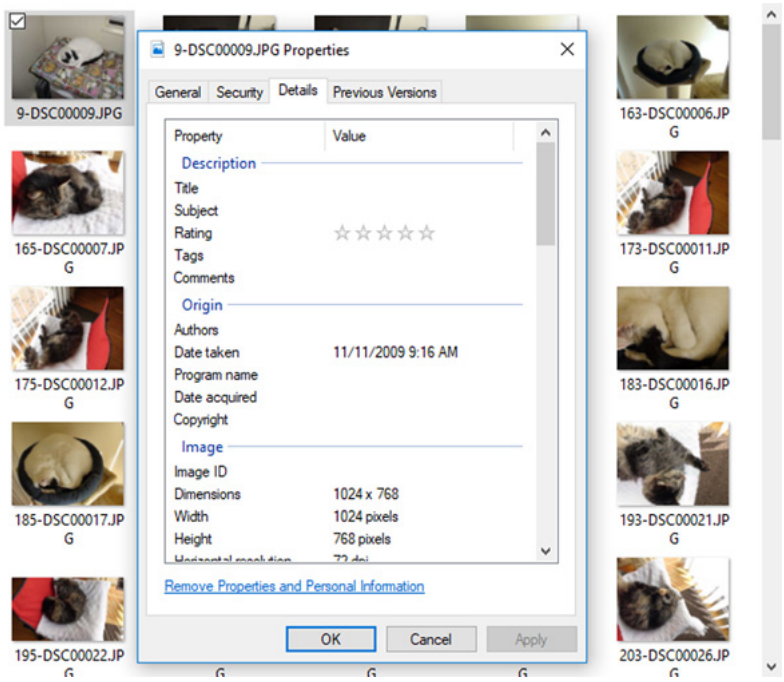


Source: www.sleuthkit.org

Viewing Exif metadata

8. Click the **Hex** tab to view the Exif file header information. Click the first JPG file in the Result Viewer pane, if necessary, and press **Ctrl+A** to select all the files in the Table tab. Right-click the selected files and click **Extract File(s)**. In the Save dialog box, click **Save** to export the files to the default *Work*\C8Proj1\Export folder, and then click **OK**. The NTFS file system in Windows has a built-in Exif viewer. To use this tool, navigate to the ***Work*\C8Proj1\Export** folder in File Explorer. Right-click any graphics file and click **Properties**. Click the **Details** tab to see the Exif information (see Figure 8-3), and then close this dialog box.

Figure 8-3.



Viewing detailed information about a graphics file

9. In the left pane of Autopsy, click the **Videos** folder under By Extension to see the video files in this image. Deleted files are indicated with a red ×. In the Result Viewer pane, scroll to view all the file attributes, such as timestamps and MD5 hash values, and then scroll to the top of the file list in the Table tab. Right-click the **KittyMontage.mov** file and click **Open in External Viewer** to see the video in Windows Media Player or the QuickTime viewer.

10. Leave Autopsy open as you answer the following review questions. When you're finished, exit Autopsy.

Review Questions

1. How many deleted files are in the Videos folder?
   a. 24
   b. 14
   c. 12
   d. 8
2. How many different cameras (denoted as "device models") did you find in the evidence?
   a. 2
   b. 125
   c. 14
   d. 84
3. What file system is used in the jo-favorites-usb-2009-12-11.E01 image?
4. Autopsy doesn't provide camera information, such as exposure time or flash use. True or False?
5. Autopsy displays hash values for video files. True or False?

Lab 8.2. Using OSForensics to Analyze Multimedia Files

Objectives

After completing this lab, you will be able to:

> - Use OSForensics to analyze multimedia files
> - Use OSForensics graphics-viewing tools

OSForensics has a built-in graphics viewer that can open BMP (bitmap), JPG, GIF, PNG, and TIF files and show their Exif information. For video viewing, OSForensics can play a wide variety of video formats. In addition, it can search Windows thumbnail cache folders to look for evidence of graphics files that were deleted. In this lab, you use OSForensics to analyze multimedia files.

Materials Required

This lab requires the following:

- Windows
- OSForensics
- The jo-favorites-usb-2009-12-11.E01 file from Lab 8.1

Estimated completion time: 30–60 minutes

Activity

In this lab, you use OSForensics to analyze multimedia files in the jo-favorites-usb-2009-12-11.E01 image:

1. Start OSForensics, and click **Continue Using Trial Version** in the "Unlicensed trial version" dialog box. Click **Start** in the left pane, if necessary, and click **Create Case** in the right pane.

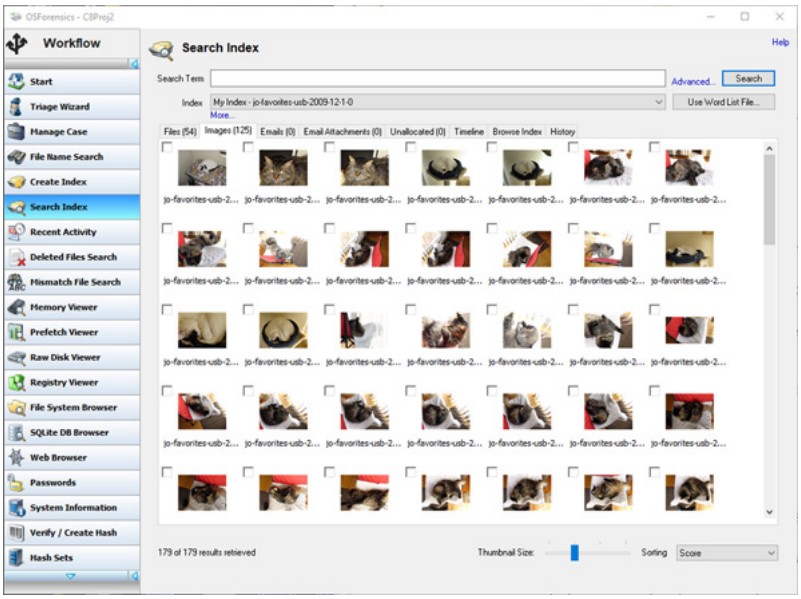
2. In the New Case dialog box, type **C8Proj2** in the Case Name text box, enter your name in the Investigator text box, and click the **Investigate Disk(s) from Another Machine** option button for the acquisition type. Click the **Custom Location** option button for the case folder. Click the **Browse** button, navigate to and click your work folder, click **Make New Folder**, type **C8Proj2**, press **Enter**, and click **OK** twice.

3. In the Manage Case pane on the right, click the **Add Device** button, and click the **Image File** option button. Click the **Browse** button, navigate to and click your work folder, click the **jo-favorites-usb-2009-12-11.E01** file, and click **Open**. In the "Select a partition in the image" dialog box, click **Partition 0**, if necessary, and then click **OK** twice.

4. Click the **Create Index** button in the left pane. In the Step 1 of 5 window, click the **Use Pre-defined File Types** option button, if necessary. Click **Check All**, and then click **Next**. In the Step 2 of 5 window, click the **Add** button. In the Add Start Location dialog box, verify that the **Whole Drive** option button is selected, and then click **OK**. Click **Next**, and in the Step 3 of 5 window, click **Start Indexing**. In the OSForensics - Create Index message box, click **OK**.

5. Click the **Search Index** button in the left pane, click **Search** in the right pane, and click the **Images** tab, if necessary, to view the graphics files (see Figure 8-4).

Figure 8-4.

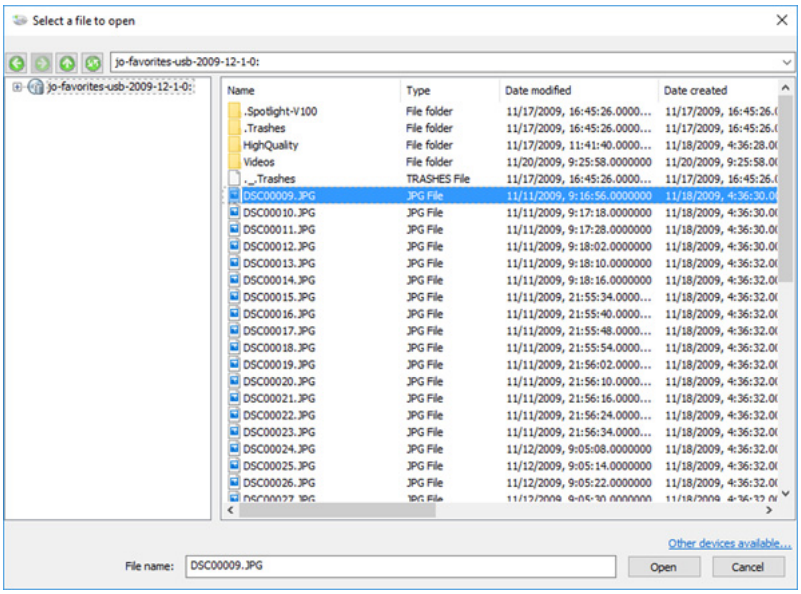


Source: PassMark Software, www.osforensics.com

Viewing graphics files in OSForensics

6. Click **Start** in the left pane, and in the right pane under Viewers, click **File and Hex Viewer**. In the "Select a file to open" dialog box, click **jo-favorites-usb-2009-12-11-0:** in the left pane. In the right pane, click the **DSC00009.JPG** file, and then click **Open** to see the file in the graphics viewer (see Figure 8-5).

Figure 8-5.

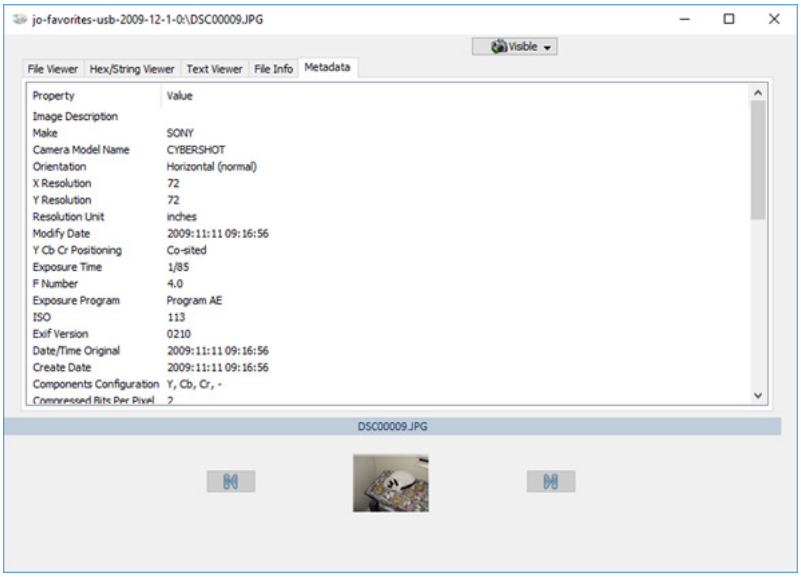


Source: PassMark Software, www.osforensics.com

Selecting a file to open in the graphics viewer

7. In the File and Hex Viewer window, click the **Hex/String Viewer** tab to see the file header hex values, and then click the **Metadata** tab to see the Exif information (see Figure 8-6). Click the **File Info** tab to see the timestamps, file size, and other attributes.

Figure 8-6.

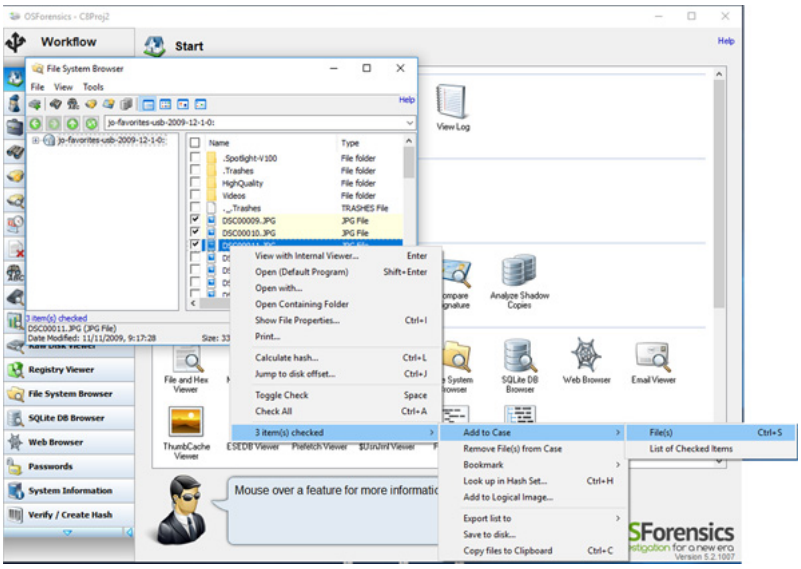


Source: PassMark Software, www.osforensics.com

Viewing Exif information in OSForensics

8. Close the File and Hex Viewer window, and click **File System Browser** in the left pane. Click **jo-favorites-usb-2009-12-11-0:** , and then click the check boxes for **DSC00009.JPG** , **DSC00010.JPG** , and **DSC00011.JPG** . Right-click the selected files, point to **3 item(s) checked** and **Add to Case**, and then click **File(s)**, as shown in Figure 8-7. In the Please Enter Case Export Details window, type **Pictures** in the Export Title text box, click the **Include EXIF Metadata (Slow)** and **Use the same details for all** check boxes, and then click **Add**.

Figure 8-7.



Source: PassMark Software, www.osforensics.com

Adding JPG files to a case

9. Double-click the **Videos** folder in the File System Browser to view the video files. Right-click **MontereyKitty.m4v** and click **View with Internal Viewer**. In the Internal Viewer dialog box, click the blue **Play** button to view the recorded movie file. After viewing the video, close the Internal Viewer dialog box.

10. Click the check boxes for **MontereyKitty.m4v** and **TiggerTheCat.m4v** . Right-click these selected files, point to **2 item(s) checked** and **Add to Case**, and then click **File(s)**. In the Please Enter Case Export Details window, type **Movies** in the Export Title text box, click the **Include EXIF Metadata (Slow)** check box, and then click **Add**. Close the File System Browser dialog box.

11. Click **Start** in the left pane, and then click **Generate Report** in the right pane. In the Export Report dialog box, click the **Copy files to report location** option button, and click the **browse** button next to the Output Location text box. Navigate to and click your work folder, click **Make New Folder**, type **C8Proj2-Report**, press **Enter**, and click **OK** twice.

12. Leave OSForensics open as you answer the following review questions. When you're finished, exit OSForensics.

Review Questions

1. What date was the first video created?
2. How many QuickTime videos (.mov files) are listed in the jo-favorites-usb-2009-12-11.E01 Videos folder?
3. OSForensics has a built-in viewer to play video files. True or False?
4. According to the HTML report you created, what's the create date for the MontereyKitty.m4v file? (*Hint*: Look under Other Artifacts, Files.)
   a. 11/21/2009, 4:36:30
   b. 11/20/2009, 8:57:26
   c. 11/11/2009, 9:16:56
   d. 11/18/2009, 4:36:30

5. In this lab, you viewed information about the DSC000009.JPG file in the File Info tab of the File and Hex Viewer window. What's the starting logical cluster number (LCN) for this file?
    a. 16,692
    b. 335,872
    c. 334,501
    d. 15,592

Lab 8.3. Using WinHex to Analyze Multimedia Files

Objectives

After completing this lab, you will be able to:

> - Use FTK Imager Lite to mount a raw (dd) file as a virtual drive
> - Use WinHex to analyze multimedia files

So far, you've been using the evaluation version of WinHex. It has basic disk-editing functions for reading data, examining data structures, and modifying data. However, it has some limitations, such as not being able to save files larger than 200 KB. The licensed version of WinHex and its forensic version, X-Ways Forensics, can save more than 200 KB and have more features and capabilities, such as case management in X-Ways Forensics. X-Ways Forensics also includes the Case Data utility, which enables you to mount and read raw (dd) or .E01 images and conduct detailed forensic analysis. In addition, it calculates hash values for files so that you can sort and find files by their hash values. The evaluation version of WinHex includes a limited version of the Case Data utility, but it can't mount forensic images or generate reports. It can, however, read and analyze forensic images mounted as virtual drives.

Another feature in the evaluation version of WinHex is the "Explore recursively" function. It displays all files as though they're in one folder. So if you have two or more files with the same name stored in separate folders, they're listed next to each other so that you can easily compare them. You use this function in this lab, along with hashing files, to find and compare identically named files in the jo-favorites-usb-2009-12-11.E01 image.

Materials Required

This lab requires the following:

- Windows
- WinHex and FTK Imager Lite
- The jo-favorites-usb-2009-12-11.E01 file from Lab 8.1

> Estimated completion time: 20–30 minutes

Activity

In this lab, you use FTK Imager Lite to mount jo-favorites-usb-2009-12-11.001 as a virtual drive and analyze its multimedia files in WinHex:

1. Start FTK Imager Lite, and click **File**, **Image Mounting** from the menu. In the Mount Image To Drive dialog box, click the **browse** button next to the Image File text box, navigate to and click your work folder, click the **jo-favorites-usb-2009-12-11.E01** file, and click **Mount**. In the Mapped Image List section, make note of the drive letter created for this image, and then click **Close**.

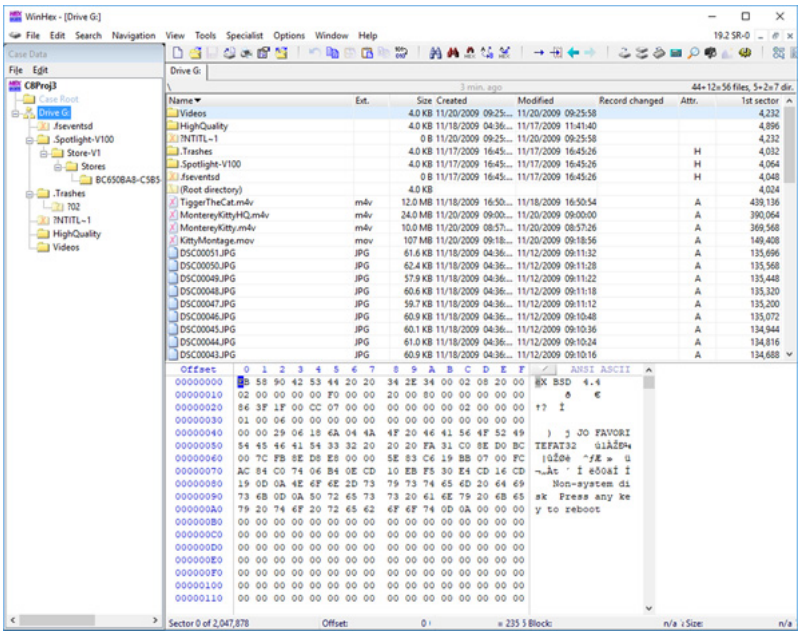
2. Start WinHex. Click **View** from the menu, point to **Show**, and click the **Case Data** check box. In the "WinHex Available only with a superior license type" message box, click **OK**. In the Case Data pane on the left, click **File**, **Create Case** from the menu. In the "WinHex Fully available only with license for X-Ways Forensics" message box, click **OK**.

3. In the Properties dialog box, click the **browse** button next to the Directory text box, navigate to and click your work folder, click the **Create New Folder** icon, type **C8Proj3**, and press **Enter**. Click **OK** to navigate to the new C8Proj3 folder, and then click **OK** twice to close the Select Folder dialog box and the Properties dialog box.

4. In the Case Data pane, click **File**, **Add Medium** from the menu. In the Select Disk dialog box, under the Logical Volumes/Partitions list, click the drive letter for jo-favorites-usb-2009-12-11.001, and then click **OK**.

5. Expand all folders in the Case Data pane, and click **Drive G:**, as shown in Figure 8-8. (*Note*: Your drive letter might be different.)

Figure 8-8.

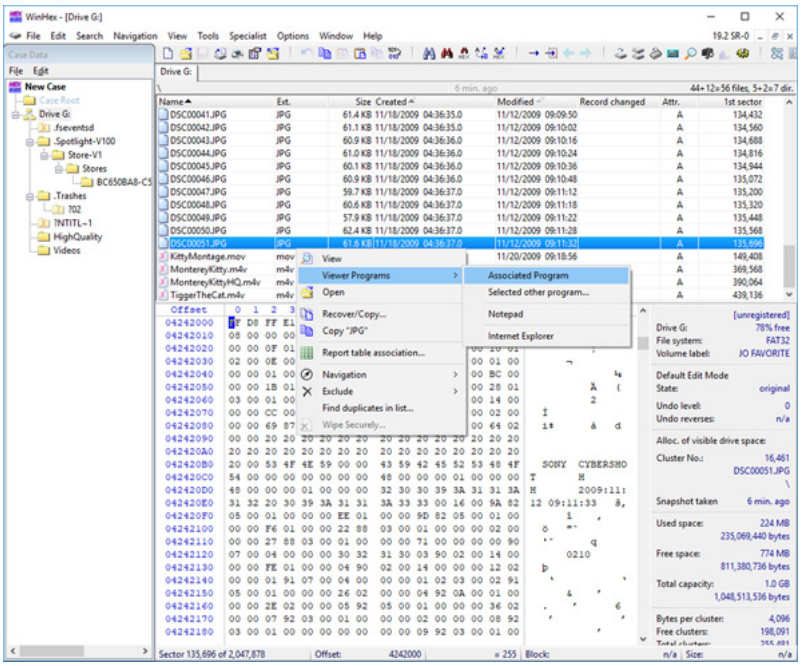


Source: X-Ways AG, www.x-ways.net

Expanding all subfolders

6. In the Directory Listing pane, notice that this drive contains several JPG files and four deleted movie files (.m4v and .mov). Click the **DSC00051.JPG** file. As shown in the hex viewer at the bottom, the hexadecimal value at the beginning of the file (FF D8 FF E1) indicates it's a JPG file with Exif data. Right-click **DSC00051.JPG** , point to **Viewer Programs**, and click **Associated Program** (see Figure 8-9) to view this file's content. Minimize the Windows Photo window (or whatever associated program your computer is configured to use).

Figure 8-9.

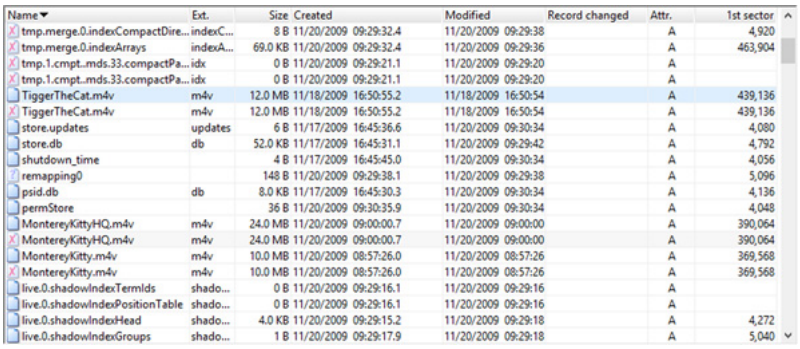


Source: X-Ways AG, www.x-ways.net

Viewing a file with an associated program

7. One method to determine whether two files with the same name are actually the same is to run a hash of each file and look for a match. For this step, right-click **Drive G:** in the Case Data pane and click **Explore recursively**. Scroll down the Directory Listing pane and find the TiggerTheCat.m4v file. Immediately after it is another file with the same name but a red × to the left, which indicates it has been deleted (see Figure 8-10).

Figure 8-10.



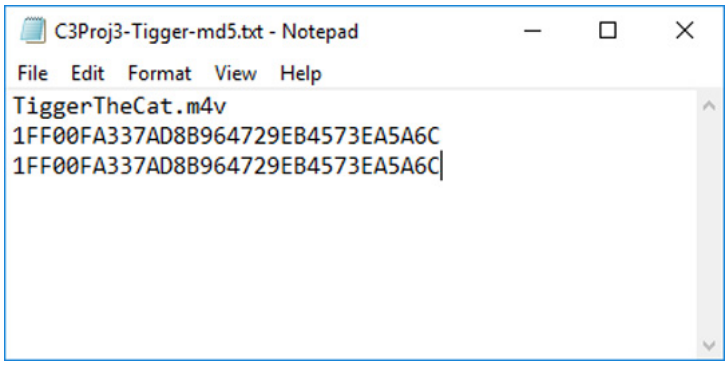
Source: X-Ways AG, www.x-ways.net

Viewing files in WinHex with the "Explore recursively" function

8. Double-click the first **TiggerTheCat.m4v** file to open a new tab labeled TiggerTheCat.m4v. Click the **TiggerTheCat.m4v** tab, and then click **Edit**, **Select All** from the menu. Click **Tools**, **Compute Hash** from the menu. In the Compute hash dialog box, click the down arrow and click **MD5 (128 bit)**, if necessary, and then click **OK**. In the MD5 (128 bit) dialog box, right-click the highlighted MD5 hash value and click **Copy**, and then click **Close**. Start Notepad. In the first line of a new document, type **TiggerTheCat.m4v**, press **Enter**, paste the MD5 hash in the next line, and press **Enter** again so that you can enter the next hash value in Step 9. Save this file in your work folder as **C8Proj3-Tigger-md5.txt** , and leave Notepad running.

9. Click the **Drive G:** tab, and then click **Edit**, **Select All** from the menu. Click **Tools**, **Compute Hash** from the menu. In the Compute hash dialog box, click the down arrow and click **MD5 (128 bit)**, if necessary, and then click **OK**. In the MD5 (128 bit) dialog box, right-click the highlighted MD5 hash value and click **Copy**, and then click **Close**. Paste the MD5 hash in the next line in Notepad, and save this file again. Compare both hashes to verify that they're the same (see Figure 8-11), and then exit Notepad.

Figure 8-11.



Comparing MD5 hash values

10. WinHex has a sort capability similar to what's available in a spreadsheet. To sort any column in the Directory Listing pane, click the column label to sort it with the lowest value at the top. To reverse the sort with the highest value at the top, click the label again. Try sorting the files so that they're in order from largest to smallest.

11. Leave WinHex open as you answer the following review questions. When you're finished, exit WinHex.

Review Questions

1. How many duplicate JPG files are in the jo-favorites-usb-2009-12-11.E01 image?
   a. 55
   b. 98
   c. 84
   d. 49
2. What's the MD5 hash value of the Cat.mov file?
   a. 994FB0038374FDD3655553E904FCC1B7
   b. AF72ABAF3E16CFB9758C8F82524C0C55
   c. 6F8A6A8BB4F5D9454FED503B6C688F5C1363BC62
   d. 3BF06FD991C312BD852C5F7B84D78174
3. How many deleted MOV and M4V files are in jo-favorites-usb-2009-12-11.E01?
   a. 12
   b. 13
   c. 18
   d. 6
4. All the JPG and M4V files in the jo-favorites-usb-2009-12-11.E01 image were last modified on the same date. True or False?

5. The jo-favorites-usb-2009-12-11.E01 image contains a system file named shutdown_time. What folder is it in, and when was it last modified?
    a. .Spotlight-V100\Store-V1\Stores\BC650BA8-C5B5-4A64-8BDB-18A9522BF1D, 11/20/2009 at 09:30:24
    b. .Spotlight-V100\Store-V1\Stores\BC650BA8-C5B5-4A64-8BDB-18A9522BF1D, 11/17/2009 at 16:45:45
    c. .Spotlight-V100\Store-V1\Stores\BC650BA8-C5B5-4A64-8BDB-18A9522BF1D, 11/20/2009 at 09:31:00
    d. .Spotlight-V100\Store-V1\Stores\BC650BA8-C5B5-4A64-8BDB-18A9522BF1D, 11/17/2009 at 16:46:55

Chapter 9. Digital Forensics Analysis and Validation

Labs included in this chapter:

Lab 9.1 Using Autopsy to Search for Keywords in an Image

Lab 9.2 Validating File Hash Values with FTK Imager Lite

Lab 9.3 Validating File Hash Values with WinHex

Note

Before starting these labs, create a subfolder of your work folder named Ch09.

Lab 9.1. Using Autopsy to Search for Keywords in an Image

Objectives

After completing this lab, you will be able to:

- Use the keyword search tools in Autopsy
- Determine hash values for files recovered with search tools

As you've seen, you can use Autopsy to search for keywords in images and find full or partial matches with words or phrases in files, folders, and unallocated disk space. Search results show file attributes, including MD5 hash values, dates and times, and byte sizes. In this lab, you search an image for any references to the keyword "project" and extract the hash values for each file.

Materials Required

This lab requires the following:

- Windows
- Autopsy 4.3.0
- The GCFI-NTFS.E01 file

Estimated completion time: 120–180 minutes, depending on your computer's performance

Activity

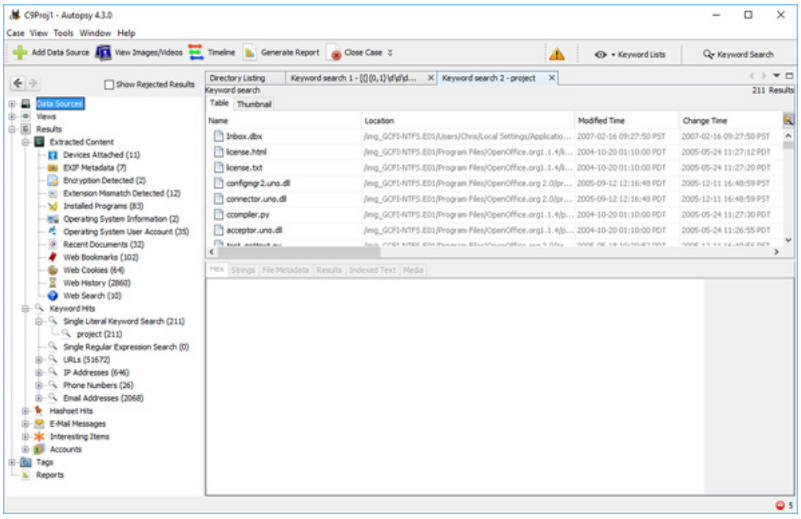
In this lab, you use Autopsy to search for references to the keyword "project":

1. Extract the **GCFI-NTFS.E01** file to your work folder. (This process might take a few minutes.) Start Autopsy, and in the Welcome window, click the **Create New Case** button. In the New Case Information window, type **C9Proj1** in the Case Name text box. Click the **Browse** button next to the Base Directory text box, navigate to and click your work folder, click **Select** to enter this path, and then click **Next**.
2. In the Additional Information window, type **C9Proj1** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.
3. In the Select Data Source window, click **Disk Image or VM File** in the "Select data source type" list box, if necessary. Click the **Browse** button, navigate to and click your work folder, click the **GCFI-NTFS.E01** file, click **Open**, and then click **Next**.
4. In the Configure Ingest Modules window, click **Select All**, click **Next**, and then click **Finish** to start analyzing the evidence.

5. Click the **Keyword Lists** down arrow. Click the **Phone Numbers**, **IP Addresses**, **Email Addresses**, **URLs**, and **Credit Card Numbers** check boxes, and then click the **Search** button. Autopsy begins searching the image.

6. Click **Keyword Search** at the upper right, click the **Exact Match** option button (if necessary), type **project**, and click **Search**. The search returns 211 results (see Figure 9-1).

Figure 9-1.



Source: www.sleuthkit.org

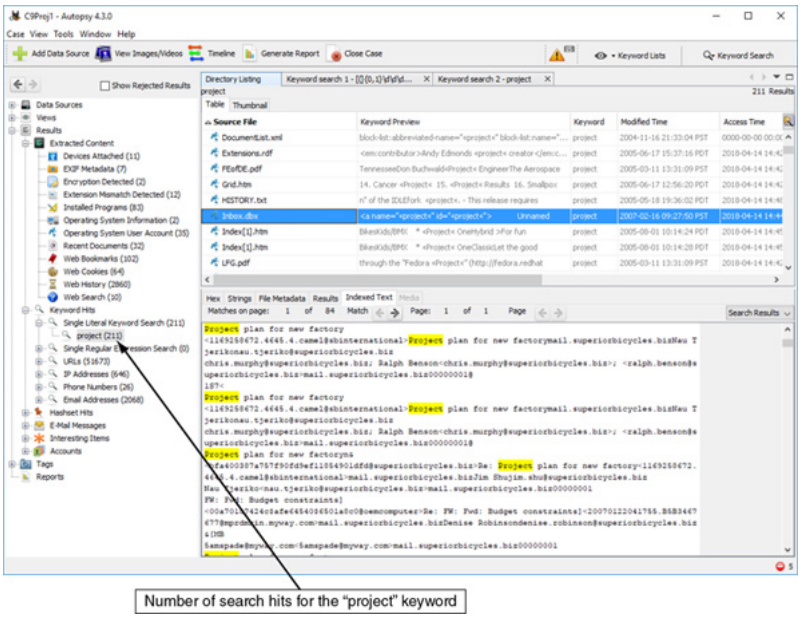
Viewing exact matches in the search results

7. Click the **Keyword search 2 - project** tab, and click the **Name** column header to sort the results alphabetically by name. In the Result Viewer pane, scroll down and click the **CREDITS.txt** file to view its contents in the Content Viewer pane. Notice the yellow highlighted hits for the keyword "project." Scroll to the right to see the attributes, including MD5 hash values.

8. Right-click the **CREDITS.txt** file in the Result Viewer pane and click **Extract File(s)**. Click **Save** to save the files in the Export folder, and click **OK** in the Information message box. This process is used to export evidence that might need further analysis.

9. In the left pane, expand **Keyword Hits** and **Single Literal Keyword Search**, and click **project**. Click the **Source File** column header in the Result Viewer pane to sort the list alphabetically. Scroll down and click the **Inbox.dbx** file, which is the e-mail inbox, to see e-mails with references to "project" highlighted in yellow (see Figure 9-2).

Figure 9-2.



Source: www.sleuthkit.org

Using the built-in file viewer

10. Right-click the **HISTORY.txt** file and click **Extract File(s)**. Click **Save** to save the files in the Export folder, and then click **OK** in the Information message box. Repeat this process for the **LFG.pdf** file, the first **Manual.pdf** file, and the first **README.TXT** file.

11. Leave Autopsy open as you answer the following review questions. When you're finished, leave Autopsy running for **Lab 9.2**.

Review Questions

1. How many exact matches were found for the "project" keyword?
   a. 211
   b. 56,172
   c. 646
   d. 26
2. Autopsy displays SHA-1 hash values with each file result. True or False?
3. Was Jim Shu's e-mail address found in the list of e-mail addresses? (*Hint*: Examine the Keyword Hits subfolders.)
4. How many PDF files are in the GCFI-NTFS.E01 image? (*Hint*: Expand the Views folder to find the answer.)
5. In Autopsy, keyword searches can reveal matches in which of the following? (Choose all that apply.)
   a. Hash values
   b. Unallocated disk space
   c. Files
   d. Folders

Lab 9.2. Validating File Hash Values with FTK Imager Lite

Objectives

After completing this lab, you will be able to:

> - Calculate MD5 hash values in FTK Imager Lite
> - Export file hashes to an Excel file for analysis

FTK Imager Lite can calculate MD5 and SHA-1 hash values in physical and logical hard drive partitions, images of storage devices, and files in folders. The results of calculating file hash values can be exported to an Excel file for use as a validation tool. Although FTK Imager Lite can't be used to edit the hex values of files, it can be used to find files in hidden partitions or slack space on disk drives. In this lab, you use FTK Imager Lite to validate hash values of the files you exported in **Lab 9.1**.

Materials Required

This lab requires the following:

- Windows
- FTK Imager Lite
- Autopsy 4.3.0
- The GCFI-NTFS.E01 file from Lab 9.1
- Microsoft Excel (or open-source spreadsheet software)

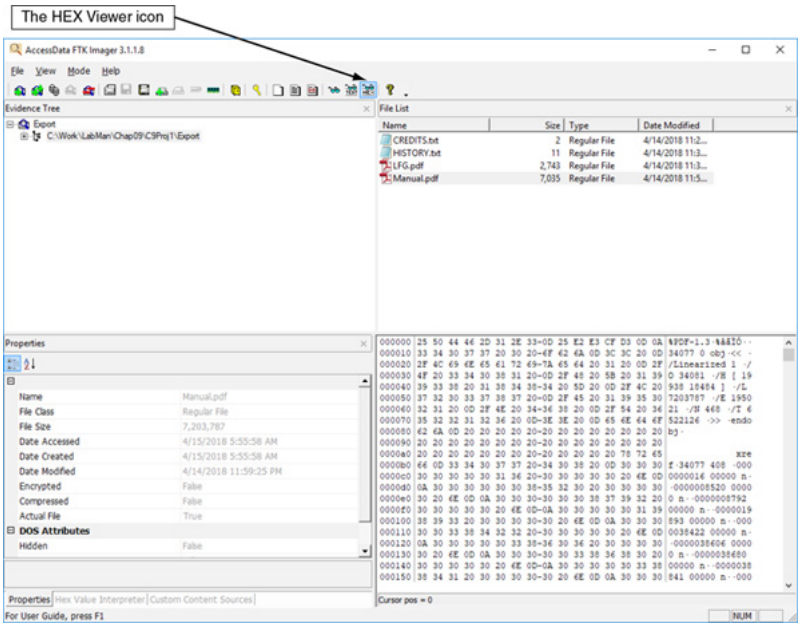
Estimated completion time: 15–30 minutes

Activity

In this lab, you use FTK Imager Lite to calculate the MD5 hash values for the files exported in **Lab 9.1**:

1. Start FTK Imager Lite, clicking **Yes** in the UAC message box, if necessary.
2. Click **File**, **Add Evidence** Item from the menu. In the Select Source dialog box, click the **Contents of a Folder** option button, and then click **Next**. In the Select File dialog box, click **Browse**, type ***Work*\C9Proj1\Export** in the Folder text box, and click **OK**. Click **Finish** to add the files to the Export folder.
3. Expand **Export** in the Evidence Tree pane. Right-click ***Work*\C9Proj1\Export** and click **Export File Hash List**.
4. In the Save As dialog box, click **New folder** at the top, type **C9Proj2**, and click the **Open** button. Type **C9Proj2 Exported Files.csv** in the "File name" text box, verify that the path is your work folder, and click **Save**. FTK Imager Lite saves MD5 and SHA-1 hashes in a .csv file automatically.
5. Click the **eyeglass** toolbar icon, and click the **CREDITS.txt** file to view it. Then click the **HEX Viewer** toolbar icon (eyeglasses above the word "HEX"), and click the **Manual.pdf** file to open it in the built-in file viewer. The file size is displayed in the File List pane, and the image file's size, which includes slack space, is shown in the Properties pane (see Figure 9-3). The hex values are read-only, so they can't be edited.

Figure 9-3.

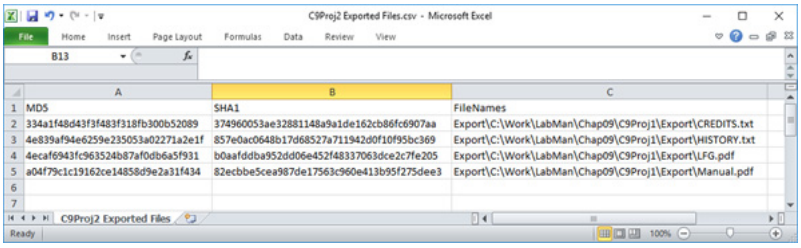


Source: AccessData Group, Inc., www.accessdata.com

Using FTK Imager Lite's built-in file viewer

6. In File Explorer, navigate to your ***Work*\C9Proj2** folder, and double-click **C9Proj2 Exported Files.csv** to open it in your spreadsheet program. Increase the width of columns **A**, **B**, and **C** to view the MD5 and SHA-1 hash values for each file (see Figure 9-4).

Figure 9-4.



Viewing file hashes in Excel

7. In the left pane of Autopsy (left running from **Lab 9.1**), expand **Keyword Hits**, if necessary. Expand **Single Literal Keyword Search**, and then click **project**. Click the **Source File** column header to sort the files, scroll down the list in the Table tab, and double-click CREDITS.txt to display all this file's metadata.

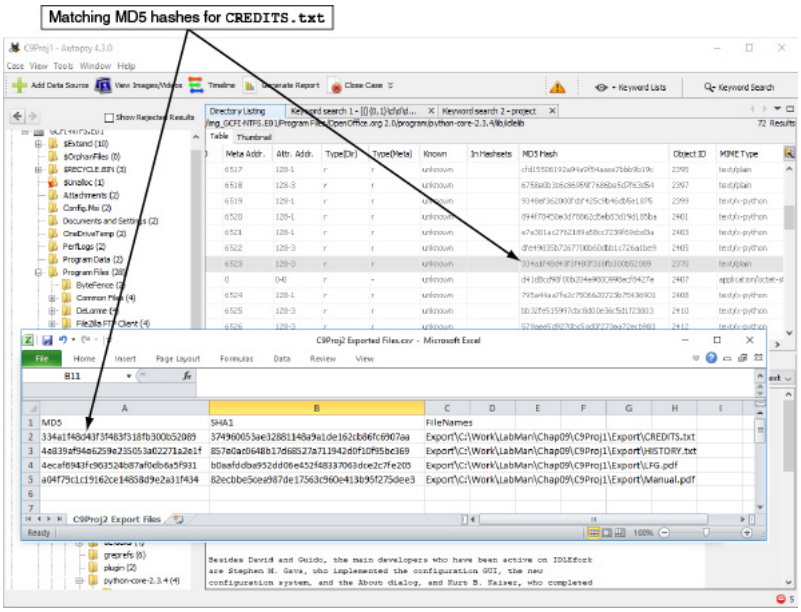
Note

The metadata usually shown in the Result Viewer pane is what's available when the Keyword Hits folder doesn't list MD5 hash values. To view all the file's metadata, including MD5 hash values, double-click the file as directed in **Step 7**. Autopsy automatically switches from the Keyword Hits folder to the Data Sources folder and displays the file's full path. The Result Viewer pane then displays all the file's metadata.

8. In the Result Viewer pane, scroll down and click **CREDITS.txt** . Scroll to the right until the MD5 hash value is displayed, and compare it with the hash value in the C9Proj2

Exported Files.csv file created in Step 4 (see Figure 9-5). If the MD5 hash values in Autopsy match the values in the Excel file, the evidence has been validated.

Figure 9-5.



Source: www.sleuthkit.org

Comparing MD5 hashes

9. Leave FTK Imager Lite and Autopsy open as you answer the following review questions. When you're finished, exit FTK Imager Lite and Autopsy, but leave the spreadsheet open for **Lab 9.3**.

Review Questions

1. FTK Imager Lite can calculate only MD5 hash values. True or False?
2. What's the SHA-1 hash value for the HISTORY.txt file?
3. FTK Imager Lite can find files in hidden partitions and slack space. True or False?
4. What's the file size in bytes of the LFG.pdf file *without* slack space?
   a. 2,808,031
   b. 1718
   c. 2743
   d. 7,203,787
5. FTK Imager Lite can't be used to edit hex values. True or False?

Lab 9.3. Validating File Hash Values with WinHex

Objectives

After completing this lab, you will be able to:

- Use WinHex to calculate MD5 and SHA-1 hash values
- Use WinHex to validate hash values

The evaluation version of WinHex has many of the same features as FTK Imager Lite, such as reading the file structure in storage devices and virtual hard disks and calculating MD5 and SHA-1 hash values, which makes it useful as a forensics validation tool. In addition to MD5 and

SHA-1 hashing, this version of WinHex can calculate several different hashes, such as CRC-16, CRC-32, SHA-256, RipeMD-128, and more. Unlike FTK Imager Lite, the evaluation version of WinHex can be used to edit hexadecimal values in file headers that have been deliberately altered or deleted, and it can view data in partition gaps and hidden disk partitions. In this lab, you examine the exported files from **Lab 9.1** and use WinHex to validate the hash values in the spreadsheet.

Materials Required:

This lab requires the following:

- Windows
- WinHex
- The C9Proj2 Exported Files.csv file from Lab 9.2

Estimated completion time: 20 minutes

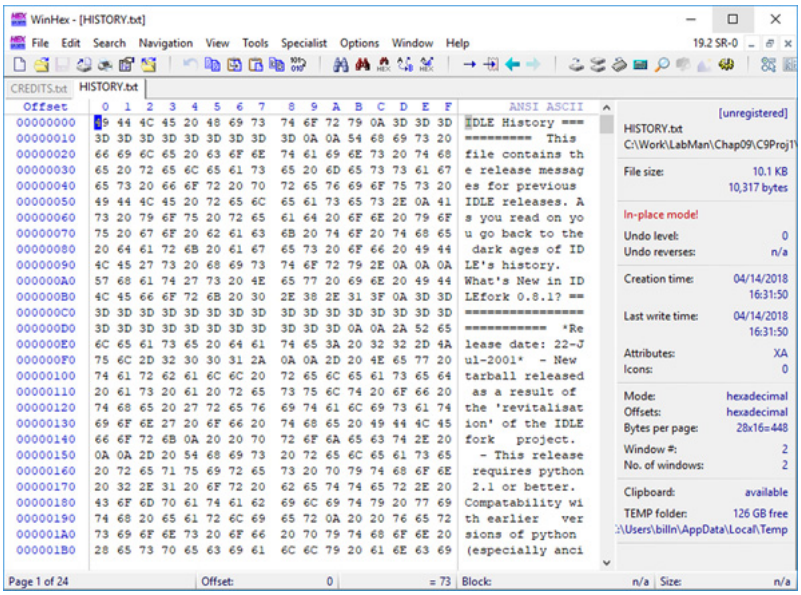
Activity

In this lab, you use WinHex to validate the exported file hashes calculated in **Lab 9.2**:

1. Start WinHex, and click **File**, **Open** from the menu. In the Open Files dialog box, navigate to your ***Work*\C9Proj1\Export** folder, click the **CREDITS.txt** file, and click **Open**.

2. Follow the procedure in **Step 1** to open the **HISTORY.txt** file in WinHex. You should see two tabs, one for each file you have opened (see Figure 9-6). Notice the information in the Info pane on the right, which includes file size. If the Info pane isn't present, click **View**, point to **Show**, and click **Info Pane**.

Figure 9-6.



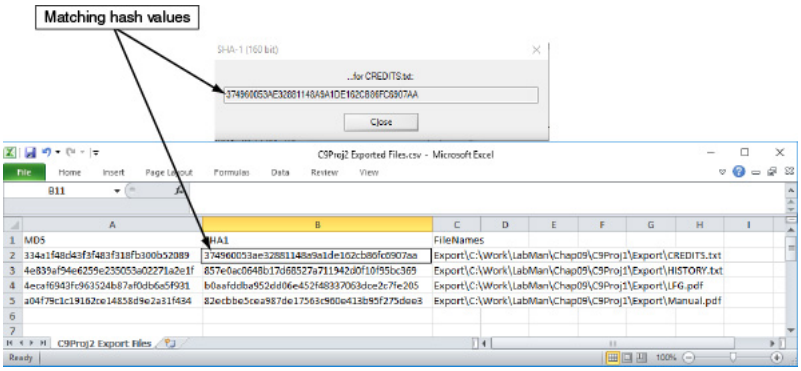
Source: X-Ways AG, www.x-ways.net

Viewing files in WinHex

3. Click the **CREDITS.txt** tab, and click **Tools**, **Compute Hash** from the menu. Click **SHA-1 (160 bit)** in the drop-down list, and click **OK** to see the SHA-1 hash value.

4. To validate your results, compare the SHA-1 hash value in WinHex with the SHA-1 hash value in the C9Proj2 Exported Files.csv file to see whether they match (see Figure 9-7). A match of the hash value between FTK Imager Lite and WinHex validates the exported CREDITS.txt file. Click **Close** in the SHA-1 (160 bit) dialog box.

Figure 9-7.



Source: X-Ways AG, www.x-ways.net

Comparing SHA-1 hash values

5. Repeat **Step 3** with the **HISTORY.txt** file, and compare its SHA-1 hash value with the one in the C9Proj2 Exported Files.csv file to validate its results.

6. Click the **CREDITS.txt** tab, and click **Tools**, **Compute Hash** from the menu. Click **MD5 (128 bit)** in the drop-down list, and click **OK** to see the MD5 hash value. Compare this value with the one in the C9Proj2 Exported Files.csv file, and then click **Close** in the MD5 (128 bit) dialog box.

7. Repeat **Step 6** with the **HISTORY.txt** file, and compare the MD5 hash value with the one in the C9Proj2 Exported Files.csv file. Click **Close** in the MD5 (128 bit) dialog box.

8. Leave WinHex open as you answer the following review questions. When you're finished, close the spreadsheet and exit WinHex.

Review Questions

1. WinHex can calculate only SHA-1 and MD5 hash values. True or False?
2. WinHex can edit hex values in file headers. True or False?
3. What's the size in bytes of the HISTORY.txt file?
4. Both FTK Imager Lite and WinHex can be used to edit hex values in file headers. True or False?
5. The evaluation version of WinHex has which of the following features? (Choose all that apply.)
   a. Viewing data in partition gaps
   b. File-decrypting tools
   c. Editing hexadecimal values
   d. Creating images of storage devices

Chapter 10. Virtual Machine Forensics, Live Acquisitions, and Network Forensics

Labs included in this chapter:

Lab 10.1 Analyzing a Forensic Image Hosting a Virtual Machine

Lab 10.2 Conducting a Live Acquisition

Lab 10.3 Using Kali Linux for Network Forensics

Note

Before starting these labs, create a subfolder of your work folder named Ch10.

Lab 10.1. Analyzing a Forensic Image Hosting a Virtual Machine

Objectives

After completing this lab, you will be able to:

- Identify a virtual machine on a host computer
- Use file hashes to find known files of interest
- Determine files that have mismatched extensions
- Analyze and extract evidence from a virtual machine

Because of the increased use of virtual machines, this lab shows you how to analyze and extract digital evidence from a host computer containing a virtual machine. For this examination, you look for any evidence related to a trade secrets project named Special Project-B, which is a proposal for creating products to restore classic American cars.

Autopsy has ingest modules for accessing virtual machines stored in a forensic image and for identifying files that have mismatched extensions, meaning the extension doesn't match the file type and has possibly been altered. This lab is divided into two sections. In the first, you load known hashes of files from the Special Project-B project into the Autopsy hash database and select the ingest module for detecting mismatched extensions. These hashes help you find files related to Special Project-B in the forensic image, and the extension mismatch module finds files with altered file extensions. In the second section, you continue your examination with the Special Project-B hashes and Autopsy's virtual machine ingest module.

Materials Required

This lab requires the following:

- Windows
- Autopsy 4.3.0
- The GCFI-Special Project-B-md5-hashes.txt and GCFI-Chris_Murphy.E01 files

Estimated completion time: 360–540 minutes, depending on your computer's performance

Caution

Processing the data file used in this lab can take more than 6 hours after the setup, so you might want to set up this lab to run overnight. The time it takes depends on your

computer's CPU speed, the amount of RAM, and the drive access speed.

Activity

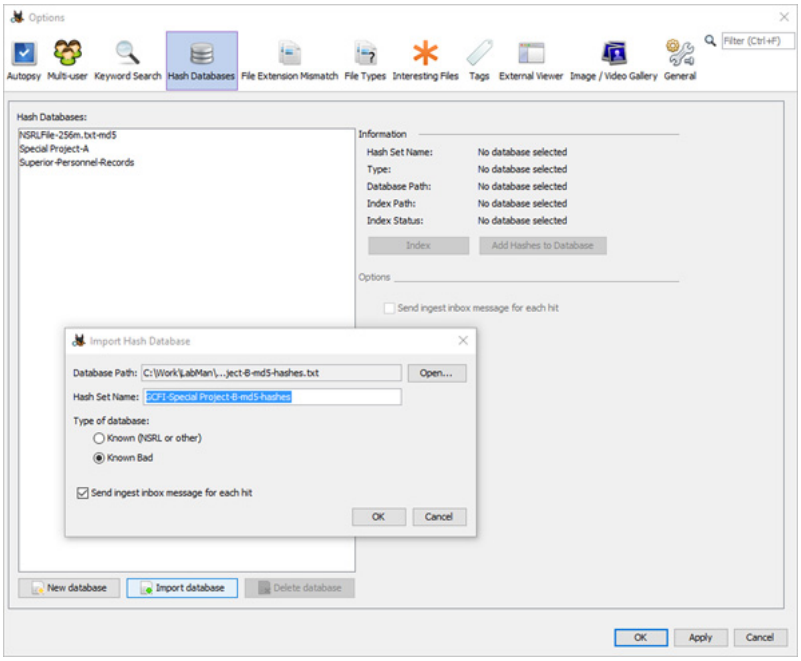
Installing MD5 Hashes in Autopsy

In this section, you install the Special Project-B MD5 hashes from the GCFI-Special Project-B-md5-hashes.txt file into the Autopsy hash database:

1. In File Explorer, extract all data files you downloaded to your work folder. Start Autopsy. In the Welcome window, click **Close**, and then click **Tools**, **Options** from the menu.

2. In the Options window, click the **Hash Databases** toolbar icon. In the Hash Databases window, click the **Import database** button. In the Import Hash Database dialog box, click **Open** next to the Database Path text box, and navigate to and click your work folder. In the Open dialog box, double-click **GCFI-Special Project-B-md5-hashes.txt** . Click the **Known Bad** option button, click the **Send ingest inbox message for each hit** check box (see Figure 10-1), if necessary, and then click **OK**.

Figure 10-1.



Source: www.sleuthkit.org

Creating and saving a new hash database

3. In the Hash Databases window, click the **Index** button in the right pane, and then click **OK** to close this window. Leave Autopsy running for the next lab section.

Analyzing a Windows Image Containing a Virtual Machine

In this section, you analyze and extract data from a Windows image containing a virtual machine:

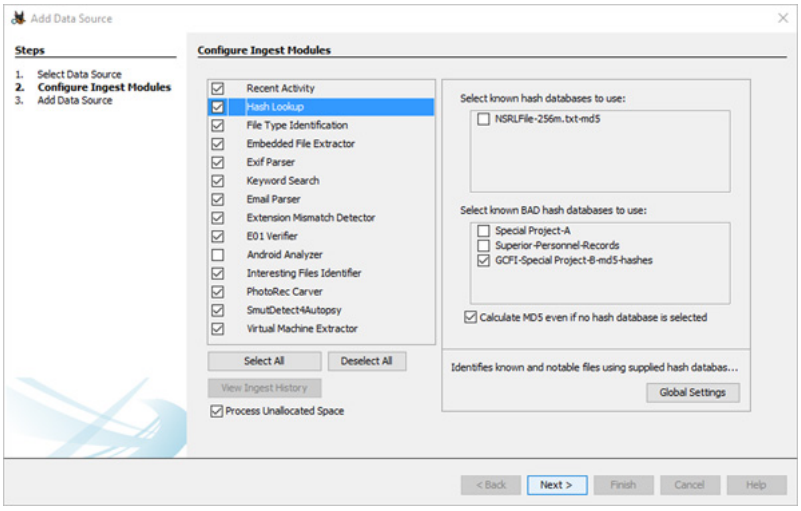
1. In Autopsy, click **Case**, **New Case** from the menu. In the New Case Information window, type **C10Proj1** in the Case Name text box. Click the **Browse** button next to the Base Directory text box, navigate to and click your work folder, click **Select** to enter this path, and then click **Next**.

2. In the Additional Information window, type **C10Proj1** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

3. In the Select Data Source window, click **Disk Image or VM file** in the "Select data source type" list box, if necessary. Click the **Browse** button, navigate to and click your work folder, click the **GCFI-Chris_Murphy.E01** file, and then click **Open**. Click **Next**.

4. In the Configure Ingest Modules window, click the **Select All** button, and then click to clear the **Android Analyzer** check box. Click the **Hash Lookup** check box, and then click the **GCFI-Special Project-B-md5-hashes** check box on the right, if necessary, as shown in Figure 10-2. Click **Next** and **Finish** to start analyzing the evidence.

Figure 10-2.

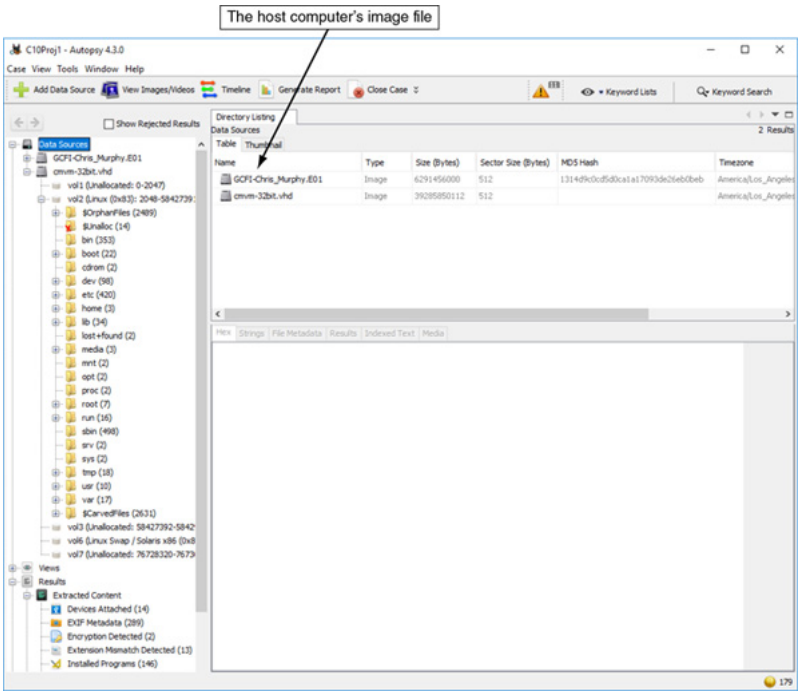


Source: www.sleuthkit.org

Selecting ingest modules

5. When the image file has been processed, notice the cmvm-32bit.vhd file listed in the Result Viewer pane. Autopsy has detected this virtual machine file with its .vhd extension in the GCFI-Chris_Murphy.E01 image. In the left pane, expand **Data Sources**, **cmvm-32bit.vhd** , and **vol2 (Linux (0x83): 2048-58427391)**, as shown in Figure 10-3. The vol2 (Linux (0x83): 2048-58427391) entry indicates that this virtual machine uses a Linux OS.

Figure 10-3.



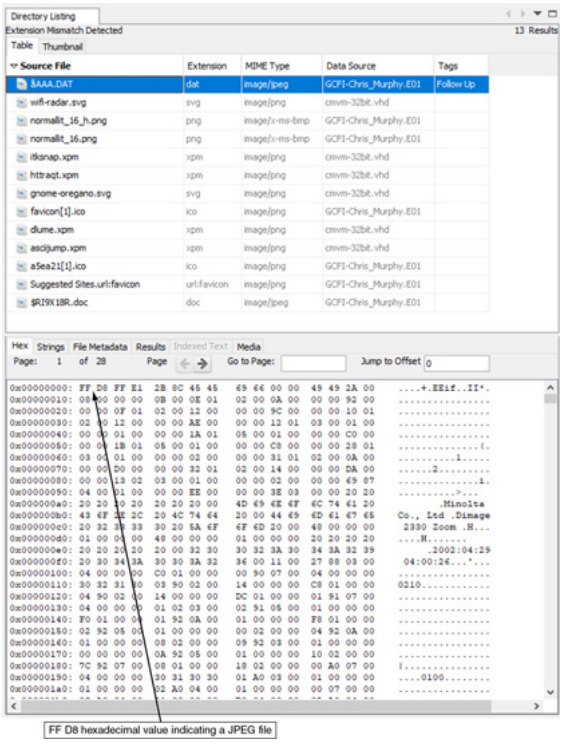
Source: www.sleuthkit.org

Viewing the contents of a virtual machine in Autopsy

6. Scroll down the left pane, expand **Hashset Hits**, and click the **GCFI-Special Project-B-md5-hashes (20)** folder. Click the first file in the Result Viewer pane, and press **Ctrl+A**. Right-click this selection, point to **Tag Files**, and click **Tag and Comment**. In the Create Tag dialog box, click the **New Tag Name** button. In the New Tag section, type **Special Project-B** in the Tag Name Text box, click **OK**, and then click **OK** again.

7. Scroll up the left pane, expand **Results** and **Extracted Content**, and click **Extension Mismatch Detected**. Click the **åAAA.DAT** file in the Result Viewer pane. In the Content Viewer pane, click the **Hex** tab and examine the file's first two bytes in the Content Viewer pane (see Figure 10-4). These bytes, consisting of FF D8, are the binary values for all JPEG files. Therefore, this file is a JPEG file with its extension changed to .DAT. Right-click the **åAAA.DAT** file, point to **Tag Files** and **Quick Tag**, and click **Follow Up**.

Figure 10-4.



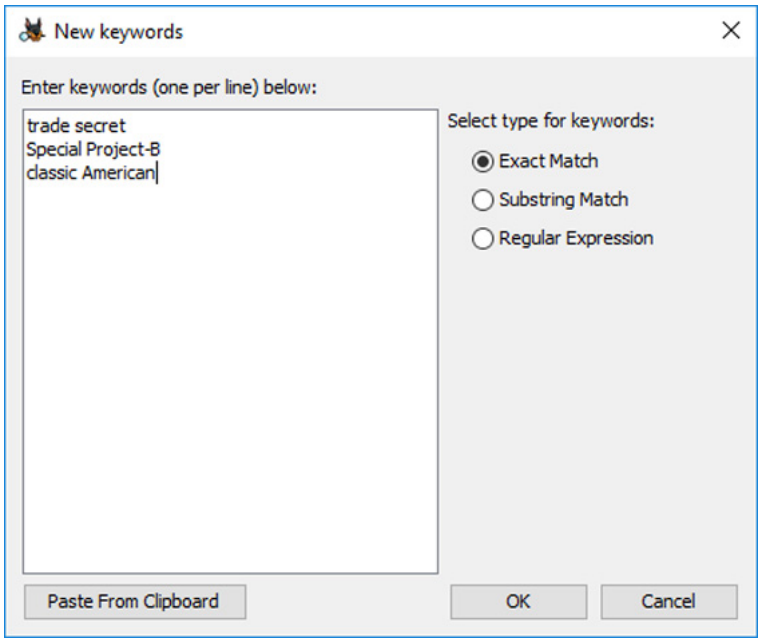
Source: www.sleuthkit.org

Examining a file with a mismatched extension

8. Click the **Keyword Lists** down arrow. In the Keyword Lists dialog box, click the **Manage Lists** button, and then click the **New List** button in the Global Keyword Search Settings dialog box. In the New Keyword List dialog box, type **Special Project-B** in the "New keyword list name" text box to name the list of keywords you're going to create, and then click **OK**.

9. Next, you create the keywords to make up this list. Click the **New List** button in the Global Keyword Search Settings dialog box to open the New keywords dialog box. In the "Enter keywords (one per line) below" list box, type **trade secret**, **Special Project-B**, and **classic American**, pressing **Enter** after each one (see Figure 10-5). Click the **Exact Match** option button, if necessary, and then click **OK** twice.

Figure 10-5.

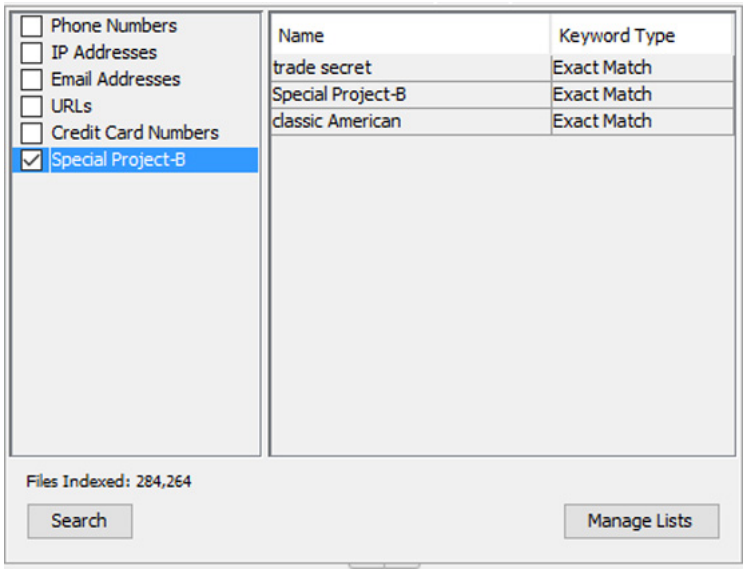


Source: www.sleuthkit.org

Creating a keyword search list

10. Click the **Keyword Lists** down arrow again. Click the **Special Project-B** check box, shown in Figure 10-6, and then click the **Search** button.

Figure 10-6.

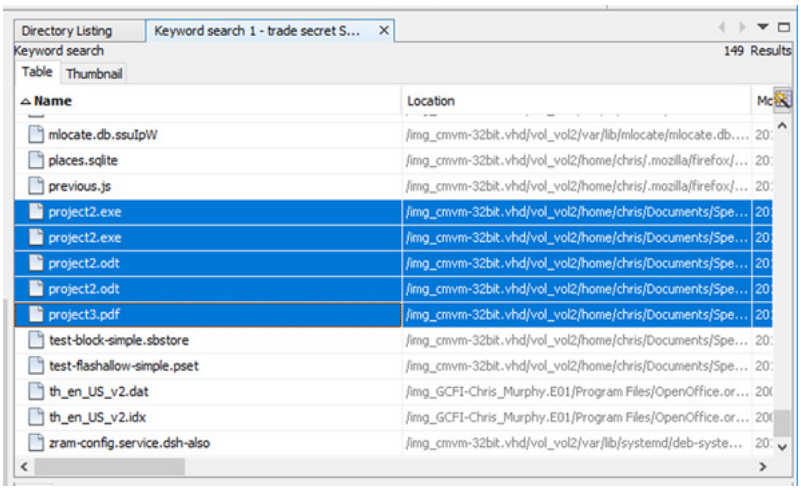


Source: www.sleuthkit.org

Selecting the Special Project-B keyword list

11. When the search is finished, click the **Keyword search 1 - trade secret Special Project-B** tab in the Result Viewer pane. Click the **Name** column header once to sort files alphabetically, and then scroll down. Click the **project2.exe** file, and Shift+click the **project3.pdf** file to select all five project files (see Figure 10-7). Right-click this selection, point to **Tag Files** and **Quick Tag**, and click **Special Project-B**.

Figure 10-7.



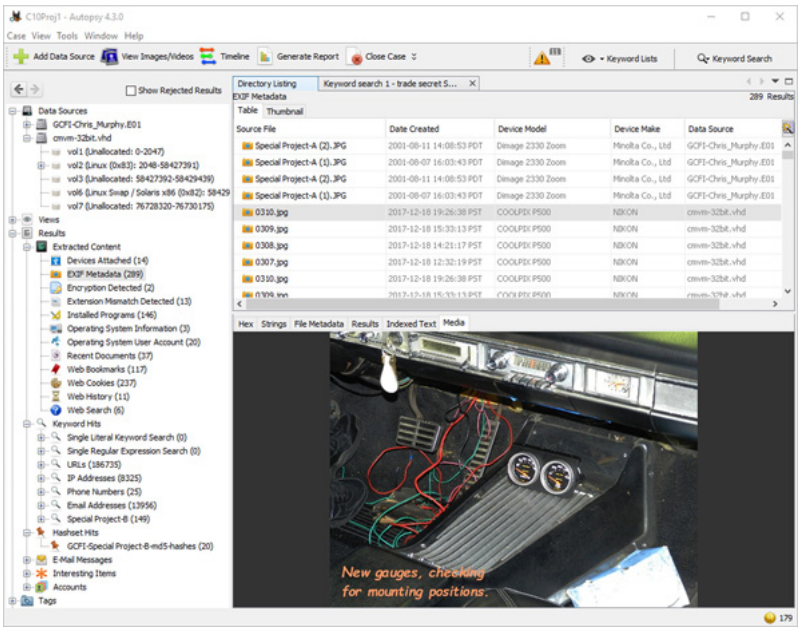
Source: www.sleuthkit.org

Selecting multiple files to tag as Special Project-B

12. In the left pane, expand **Data Sources**, **GCFI-Chris_Murphy.E01** , **Users**, and **Documents**. Click the **Trade Secret1**, **Trade Secret2**, and **Trade Secret3** folders, and examine their contents in the Result Viewer and Content Viewer panes. Expand **cmvm-32bit.vhd** , **vol2 (Linux (0x83): 2048-58427391)**, **home**, and **Documents**, and click **Special Project-B**. Examine its contents in the Result Viewer and Content Viewer panes to see whether it has any data files related to this project.

13. In the left pane, expand **Results** and **Extracted Content**, and click **EXIF Metadata**. Click the **Special Project-A(2).JPG** file in the Result Viewer pane. Notice in the Data Source column that this file is in the GCFI-Chris_Murphy.E01 image on the host computer. Click the **0310.jpg** file, and notice that its data source is cmvm-32bit.vhd, the virtual machine (see Figure 10-8). Double-click the **0310.jpg** file, and Autopsy switches to the folder where this file is found.

Figure 10-8.



Source: www.sleuthkit.org

Determining a file's data source

14. Click **Generate Report**, and in the Generate Report window, click the **Results - HTML** option button in the Report Modules section, and then click **Next**. In the Configure Artifact Reports window, click the **Tagged Results** option button, click **Select All**, and then click **Finish**.

15. When the report is finished, in the Report Generation Progress window, click the **Results - HTML** pathname, and leave the report open as you answer the following review questions. When you're finished, exit the Web browser and Autopsy. Save the case, if prompted.

Review Questions

1. The HTML report's Extension Mismatch Detected link lists the $RI9X1R.doc file. What does Autopsy show as its actual file type?
   a. image/png
   b. image/x-ms-bmp
   c. image/jpeg
   d. image/gif
2. Based on the contents of the virtual machine's Special Project-B folder, what's the target market listed in the business plan?
   a. Outdoor kayak enthusiasts
   b. High-tech bicyclists
   c. NASA contract bidders
   d. Classic American car owners
3. How many Special Project-B.pdf files are listed in the PDF folder?
   a. 9
   b. 7

c. 3

d. 2

4. In what folder did you find the 0310.jpg file?

   a. \img_cmvm-32bit.vhd\vol_vol2\home\chris\Documents\Special Project-B\testfile.dat\Specs

   b. \img_cmvm-32bit.vhd\vol_vol1\home\chris\Documents\Special Project-B\testfile.dat\Specs

   c. img_GCFI-Chris_Murphy.E01\Windows\System32\users\home\chris\Documents\Special Project-B\testfile.dat\Specs

   d. img_GCFI-Chris_Murphy.E01\Windows\System32\users\home\chris\Documents\Special Project-C\testfile.dat\Specs

5. Autopsy identified åAAA.DAT as a JPEG file. What other file in the Extension Mismatch Detected folder is identified as a JPEG file?

   a. $RI9X18R.doc

   b. a5ea21[1].ico

   c. dlume.xpm

   d. httraqt.xpm

Lab 10.2. Conducting a Live Acquisition

Objectives

After completing this lab, you will be able to:

> - Produce a comprehensive audit of a computer's OS and installed applications
> - Make screen captures while examining a live OS
> - Calculate hashes of files and directories in a live OS
> - Collect data from a live OS

The reason for making a live acquisition is to collect digital evidence in real time so that you can see how malware behaves while a computer is running and connected to the Internet. This process requires a target drive, such as a USB drive, with enough disk space to store a forensic image as well as analysis and acquisition software. For example, if you have a computer with a 1 TB drive, the target drive should be at least 2 TB. If the target drive is equal to or smaller than the computer's drive, you can use a second USB drive to run the analysis and acquisition software. This method, however, requires two USB ports, which might be a problem if the computer's ports are already used by a keyboard, mouse, printer, or other peripheral devices.

When you're making a live acquisition, you should also use the compression option available in many acquisition tools so that the forensic image can be stored more easily on the target drive. It's also helpful, but not required, to have administrator privileges for the user account logged on to the computer. Having these privileges can prevent access errors that might occur when copying system files or other user data on the computer.

This lab is divided into three sections: installing tools on a USB drive for collecting data from a computer in real time, exploring the use of these tools, and acquiring data during a live acquisition.

Materials Required

This lab requires the following:

- Windows
- The large external USB drive or internal SATA drive, labeled GCFI-Evid, from **Lab 4.2**
- FTK Imager Lite
- The freeware tools QuickHash GUI for Windows, WinAudit, and MWSnap, downloaded in the first section

Estimated completion time: 360–540 minutes

Caution

Processing the data file used in the third section of this lab can take more than 6 hours after setup, so you might want to finish the first two sections and then set up the third section of this lab to run overnight. The time it takes depends on your computer's CPU speed, amount of RAM, and drive access speed.

Activity

Installing Tools for Live Acquisitions

In this section, you download and install three tools, and then copy them and FTK Imager Lite to a USB drive:

1. Start a Web browser, and go to quickhash-gui.org/downloads/. Scroll to the bottom of the Web page, and click the **Download** link for QuickHash v3.0.2 Windows (or whatever the latest version is). Save the **Quickhash-Windows-v3.0.2.zip** file in your work folder.
2. Go to www.parmavex.co.uk/winaudit.html, and click the **Zip Download** link. Save the **WinAudit.zip** file in your work folder.
3. Go to www.tucows.com/preview/222629, and click the **Download Now** link for MWSnap 3.0.0.74. Save the **MWSnap300.exe** file in your work folder.
4. Open File Explorer, and navigate to your work folder. Right-click **Quickhash-Windows-v3.0.2.zip** and click **Extract All**. In the Extract Compressed (Zipped) Folders dialog box, click **Extract** to copy the zipped data to the Quickhash-Windows-v3.0.2 subfolder that's created automatically.
5. Right-click **WinAudit.zip** in your work folder and click **Extract All**. In the Extract Compressed (Zipped) Folders dialog box, click **Extract** to copy the zipped data to the WinAudit subfolder.
6. Double-click **MWSnap300.exe** to install this tool. In the Installing MWSnap Language window, click **English**, if necessary, and then click **Next**. In the Welcome to MWSnap Installation window, click **Next**. Click **Browse** next to the Destination Directory text box. In the Browse For Folder dialog box, navigate to and click your work folder, click **OK**, and then click **Next**. Click **Finish**, and an MWSnap subfolder is created automatically in your work folder.
7. Insert the GCFI-Evid USB drive in the USB port. In File Explorer, navigate to the GCFI-Evid drive's root folder. Click the **Home** tab, if necessary, click the **New folder** icon, type **Tools**, and press **Enter**. Navigate to your work folder, and copy QuickHash, WinAudit, MWSnap, and FTK Imager Lite to the Tools folder on the GCFI-Evid drive. Leave the USB drive inserted in the computer, and keep File Explorer open for the next section.

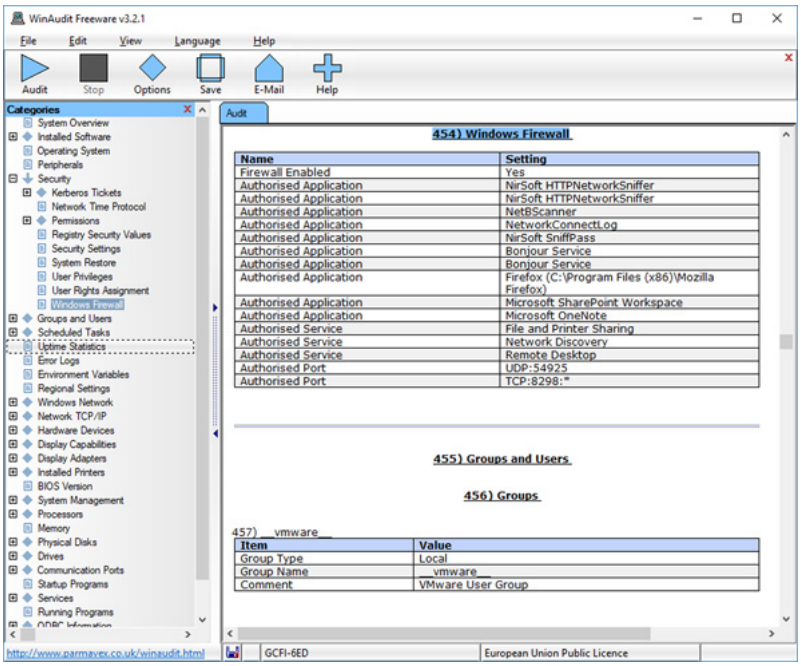
Exploring Tools for Live Acquisitions

In this section, you learn some basic functions in WinAudit, QuickHash, and MWSnap:

1. In File Explorer, double-click the **Tools** folder on the USB drive, and then click the **WinAudit** folder. Double-click the **WinAudit.exe** file to start WinAudit, which immediately begins collecting and displaying information about the computer. This process takes about 4 to 8 minutes. Leave File Explorer open.

2. When WinAudit has finished displaying information, expand **Security** in the left pane, and click **Windows Firewall** to see settings for the computer's firewall (see Figure 10-9). Click **File**, **Save** from the menu. In the Save As dialog box, navigate to the **GCFI-Evid** drive, click the **Create New Folder** icon, type **C10Proj2**, press **Enter** twice, and click the **Save** button. Keep WinAudit running for the review questions at the end of this lab.

Figure 10-9.



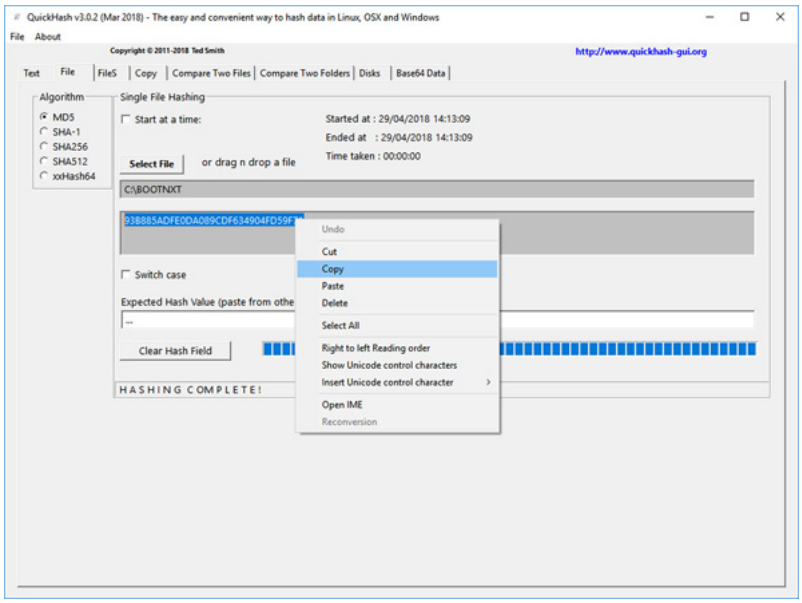
Source: Parmavex Services, www.parmavex.co.uk

Viewing firewall settings in WinAudit

3. In File Explorer, double-click the **Tools** folder on the USB drive, and then click the **QuickHash-Windows-v3.0.2** folder. Double-click the **Windows-x*nn*** (replacing *nn* with 32 or 64, depending on your computer's CPU) folder, and then double-click the **QuickHash-Windows-x*nn*.exe** file to start QuickHash.

4. Click the **MD5** option button in the Algorithm section, and then click the **File** tab. In the Single File Hashing section, click the **Select File** button. In the "Open existing file" dialog box, navigate to the root folder (C drive) of your computer, and double-click **BOOTNXT**. When the hashing is finished, select the hash value in the text box, and then right-click this value and click **Copy**, as shown in Figure 10-10.

Figure 10-10.



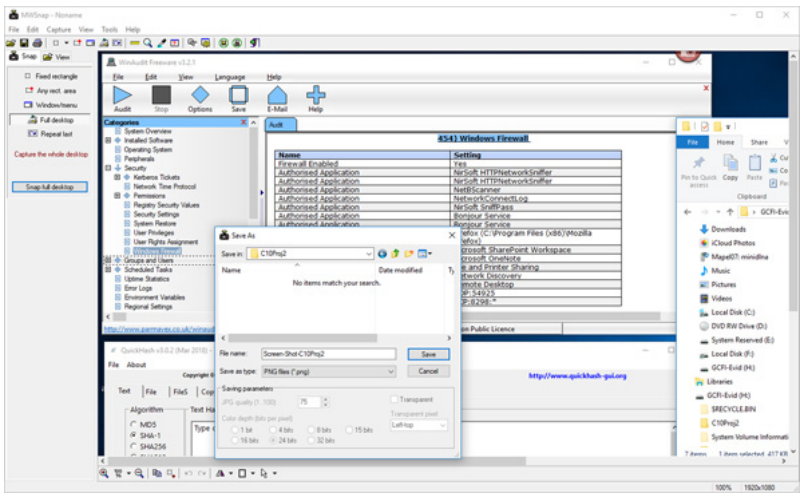
Source: Ted Smith, www.quickhash-gui.org

Copying a hash value in QuickHash

5. Open Notepad, and press **Ctrl+V** to paste this hash value in a new text document. Click **File**, **Save As** from the menu, navigate to and click the **C10Proj2** folder of the GCFI-Evid drive, type **File-BOOTNXT-MD5-hash** in the "File name" text box, and click **Save**. Exit Notepad, but keep QuickHash running for the review questions at the end of this lab.

6. In File Explorer, double-click the **Tools** folder on the USB drive, and then click the **MWSnap** folder. Double-click **MWSnap.exe** to start MWSnap. Click your preferred language, and then click **OK**. Click **Full desktop** in the left pane, and then click the **Snap full desktop** button. Click **File**, **Save As** from the menu. In the Save As dialog box, navigate to and double-click the **GCFI-Evid\C10Proj2** path. In the "File name" text box, type **Screenshot-C10Proj2**. Click the **Save as type** list arrow, click **PNG files (*.png)**, as shown in Figure 10-11, and click **Save**. Keep MWSnap running for the review questions at the end of this lab.

Figure 10-11.



Source: Mirek Wojtowicz, www.mirekw.com

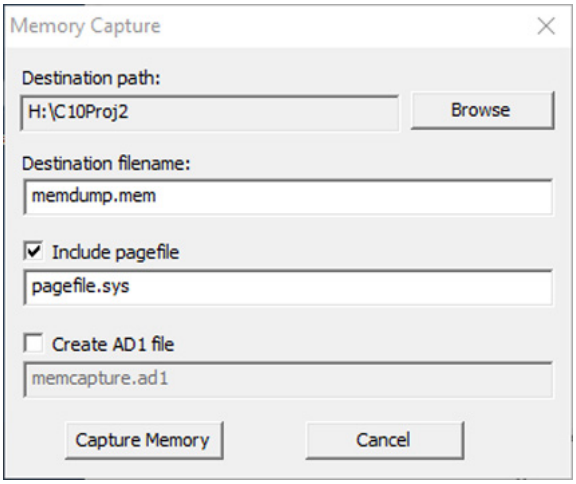
Capturing the full desktop with MWSnap

Capturing Data in a Live Acquisition

In this section, you use FTK Imager Lite to acquire your computer's RAM, the pagefile.sys file, and the C drive:

1. Start FTK Imager Lite, clicking **Yes** in the UAC message box, if necessary.
2. To capture RAM and the pagefile.sys file, click **File**, **Capture Memory** from the menu. In the Memory Capture dialog box, click **Browse**, and navigate to and double-click the **C10Proj2** folder on the GCFI-Evid drive. Click the **Include pagefile** check box (see Figure 10-12), and then click the **Capture Memory** button.

Figure 10-12.

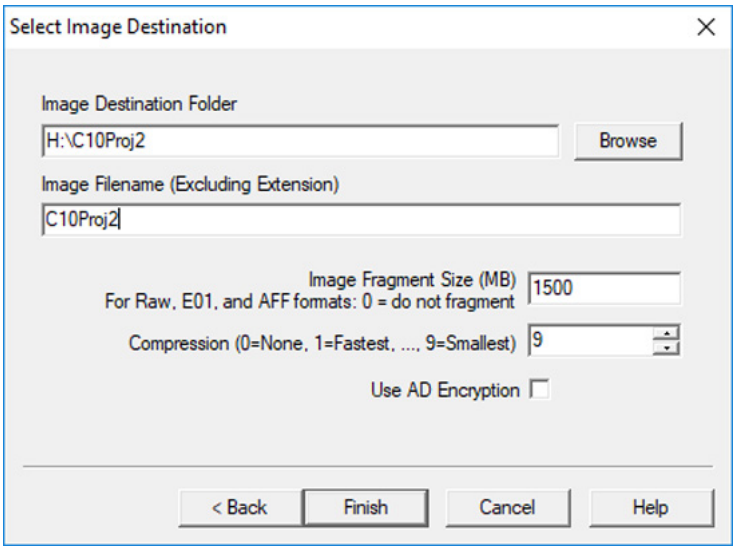


Source: AccessData Group, Inc., www.accessdata.com

Configuring settings for capturing memory in a live acquisition

3. To capture a whole drive, click **File**, **Create Disk Image** from the menu. In the Select Source dialog box, click the **Logical Drive** option button, and then click **Next**. In the Select Drive dialog box, click the **Please select from the following available drives** list arrow, click **C:\ - [NTFS]**, if necessary, and then click **Finish**.
4. In the Create Image dialog box, click **Add**, click the **E01** option button, and click **Next**. Type **C10Proj2** in the Case Number and Evidence Number text boxes, type **Live acquisition** in the Unique Description text box, type your name in the Examiner text box, and then click **Next**.
5. In the Select Image Destination dialog box, click **Browse**, navigate to the **GCFI-Evid** drive, click the **C10Proj2** folder, and then click **OK**. In the Image Filename (Excluding Extension) text box, type **C10Proj2** (see Figure 10-13), and then click **Finish**. In the Create Image dialog box, click **Start**.

Figure 10-13.



Source: AccessData Group, Inc., www.accessdata.com

Configuring a live acquisition of the C drive

6. When the imaging is finished, leave FTK Imager Lite open as you answer the following review questions. When you're finished, exit FTK Imager Lite, WinAudit, QuickHash, and MWSnap.

Review Questions

1. When you're creating a WinAudit report, what formats other than HTML can you choose? (Choose all that apply.)
   a. Rich Text (*.rtf)
   b. Comma Delimited (*.csv)
   c. Extended Markup Language (*.xml)
   d. Portable Document Format (*.pdf)
2. In QuickHash, you can calculate a file hash value in the File tab. Which tab can you use for hashing several files and subdirectories?
   a. Text
   b. FileS
   c. Copy
   d. Disks
3. When conducting a live acquisition, you must have administrator privileges for the user account logged on to the computer. True or False?
4. MWSnap can save captured screenshots in which graphics file formats? (Choose all that apply.)

   TIFF files (*.tif)

   PDF files (*.pdf)

   JPEG files (*.jpg)

   GIF files (*.gif)

5. When you're making a live acquisition, use the compression option in your acquisition software so that the image can be stored more easily on the target drive. True or False?

Lab 10.3. Using Kali Linux for Network Forensics

Objectives

After completing this lab, you will be able to:

- Boot Kali Linux in forensic mode
- Mount drives in read-only and read-write mode
- Identify open ports on your workstation

Kali Linux, funded and managed by Offensive Security (see www.docs.kali.org/introduction/what-is-kali-linux), is a versatile Linux distribution that comes in several ISO configurations. These distributions (or "distros") range from a light version, which is only 856 MB, to a full-featured version, which is 2.8 GB. In addition, it comes in 32-bit, 64-bit, and virtual machine versions. Kali Linux is designed for penetration testing and contains many network security assessment tools, a forensics acquisition tool, and the Linux version of Autopsy.

When a Kali Linux ISO is installed on a CD/DVD or USB drive, the device can be used as a live CD/DVD or live USB drive. When Kali Linux is started, all versions, except the virtual machine version, display a boot menu that includes a forensic mode option. The forensic mode skips mounting drives connected to the computer to prevent writing to these drives.

This lab is divided into three sections: installing Kali Linux as a live USB drive or CD/DVD in forensic mode, mounting drives as read-only and read-write, and determining what network ports are open on your computer.

Materials Required

This lab requires the following:

- A Windows computer with CD/DVD burning software
- A USB drive (4 GB or larger) and a blank CD/DVD
- The large external USB drive or internal SATA drive, labeled GCFI-Evid, from **Lab 10.2**
- The kali-linux-2018.2-amd64.iso or kali-linux-2018.2-i386.iso file, downloaded in the first section
- The Etcher-Setup-1.3.1-x64.exe or Etcher-Setup-1.3.1-x86.exe file from Lab 3.1

Estimated completion time: 60–120 minutes

Caution ⚠

Kali Linux contains specialized network assessment tools that can interfere with the operations of the network your computer is connected to. In addition, Kali Linux tools for password cracking and wireless attacks can trigger antivirus programs on a network. Check with your instructor for any restrictions or permissions needed before doing this lab.

Activity

Installing Kali Linux

In this section, you download and install Kali Linux, create a bootable USB drive or CD/DVD, and then start your computer with Kali Linux:

1. Start a Web browser, and go to www.kali.org/downloads. Click the **Download Kali Linux 64 Bit** or **Kali Linux 32 Bit** link, depending on your computer's CPU. Save the **kali-linux-2018.2-amd64.iso** or **kali-linux-2018.2-i386.iso** file in your work folder.

2. (*Note*: If you're using a USB drive, skip to Step 4.) Insert a blank CD/DVD in the CD/DVD drive. Open File Explorer, and navigate to your work folder. Right-click **kali-linux-2018.2-amd64.iso** or **kali-linux-2018.2-i386.iso** and click **Burn disc image**, or use your preferred CD/DVD burning software.

3. In the Windows Disc Image Burner dialog box, click the **Verify disc after burning** check box, and then click the **Burn** button. When the verification has finished, click **Close**. Eject the CD/DVD and label it **Kali Linux *nn* Bit** (replacing *nn* with 64 or 32, depending on your computer's CPU).

4. To create a bootable USB drive, insert a USB drive (the smaller of the two listed in the "Materials Required" section) in a USB port. In File Explorer, navigate to your work folder, and double-click **Etcher-Portable-1.3.1-xnn.exe** to start Etcher.

5. Click the **Select image** button, and navigate to your work folder. Click the **kali-linux-2018.2-amd64.iso** or **kali-linux-2018.2-i386.iso** file, and click **Open**. Click the **Select drive** button (if it's displayed) to open the Select a Drive dialog box. Verify that the current USB drive is selected, and then click **Continue**. In the main window, click the **Flash!** button to start Etcher.

6. When Etcher has finished copying the ISO image, exit it. Remove the USB drive and label it **Kali Linux *nn* Bit** (replacing *nn* with 64 or 32, depending on your computer's CPU).

7. If you're using the CD/DVD, insert the **Kali Linux *nn* Bit** disc into the CD/DVD drive, and restart the computer. If you're using the USB drive, insert the **Kali Linux *nn* Bit** drive into a USB port, and restart the computer.

8. While the computer is starting, read the text that's displayed. Look for any reference to accessing the BIOS, UEFI, or boot menu. Press the specified key to access the boot option.

9. After you press the hot key, a boot menu is displayed. Use the up and down arrow keys to select the **Kali Linux *nn* Bit** USB drive or CD/DVD, and press **Enter** to start Kali Linux.

10. When the Kali Linux boot loader menu is displayed, make sure the **Live (forensic mode)** option is selected (see Figure 10-14), and press **Enter**. After Kali Linux boots, enter **root** for the username and **toor** for the password in the login dialog box, if necessary.

Figure 10-14.

Source: Kali Linux, www.kali.org

Starting Kali Linux in the forensic mode

Note

If the Kali Linux screensaver is password protected, use the root account name and the toor password to log back into the session.

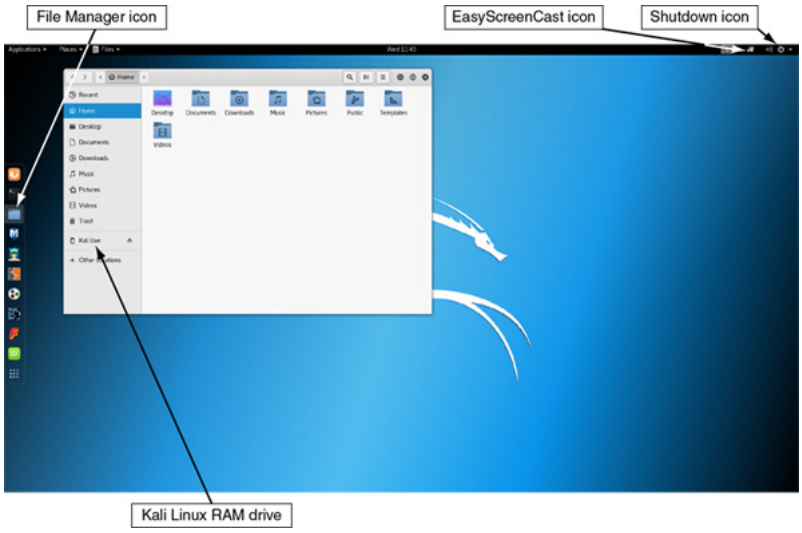
11. When the Kali Linux desktop is displayed, click the **Applications** down arrow in the upper-left corner. Look at the options for network assessment and forensics tools in the Kali Linux submenus, and then leave Kali Linux running for the next section.

Mounting Drives in Kali Linux

In this section, you connect the GCFI-Evid USB drive and mount it in Kali Linux as read-write. Then you mount the C drive as read-only.

1. In Kali Linux, click the **File Manager** icon on the toolbar on the left. The only drive listed in File Manager's left pane is the Kali Live drive (which is the Kali Linux RAM drive), as shown in Figure 10-15.

Figure 10-15.



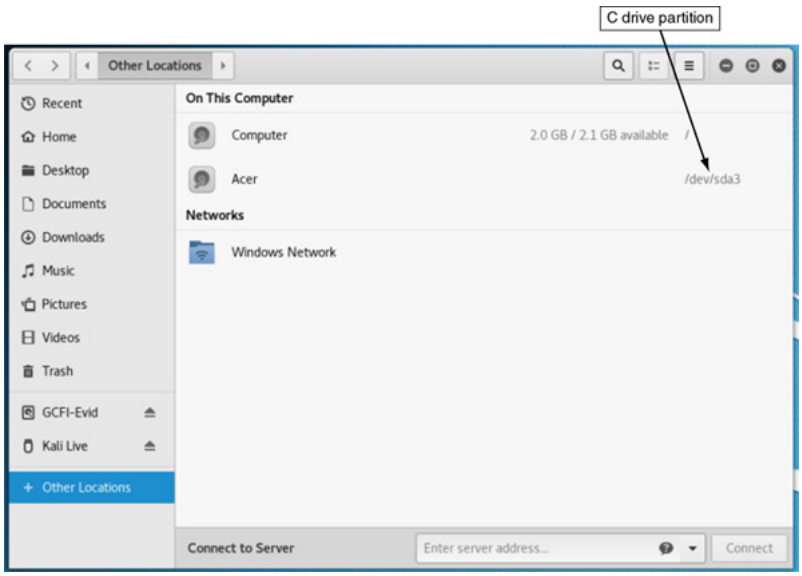
Source: Kali Linux, www.kali.org

Displaying File Manager in Kali Linux

2. Insert the GCFI-Evid USB drive into a USB port, and notice that Kali Linux lists the drive in the left pane of File Manager as soon as it's connected. To mount GCFI-Evid as a read-write drive, right-click **GCFI-Evid** in the left pane and click **Mount**.

3. Click **Other Locations** in the left pane of File Manager. In the right pane, notice that the drive named Acer with the path /dev/sda3 is the C drive partition for this computer (see Figure 10-16). (*Note*: Your computer's C drive name and path will be different from what's shown.) Leave File Manager open.

Figure 10-16.



Source: Kali Linux, www.kali.org

Identifying the C drive

4. To mount the C drive as read-only, click the **Terminal** icon on the toolbar of the Kali desktop. In the terminal window, type **mkdir /media/sda3** and press **Enter**. To create a mount point for the drive, type **ntfs-3g -o ro /dev/sda3 /media/C-drive** and press **Enter**. Leave the terminal window open. Click **Other Locations** in the left pane of File

Manager, and in the right pane, click **Acer** (substituting your computer's drive name) to view the C drive.

5. In the terminal window, type **guymager** and press **Enter** to see how Guymager displays the C drive. When you're finished, exit Guymager. Leave Kali Linux running and the terminal window open for the next section.

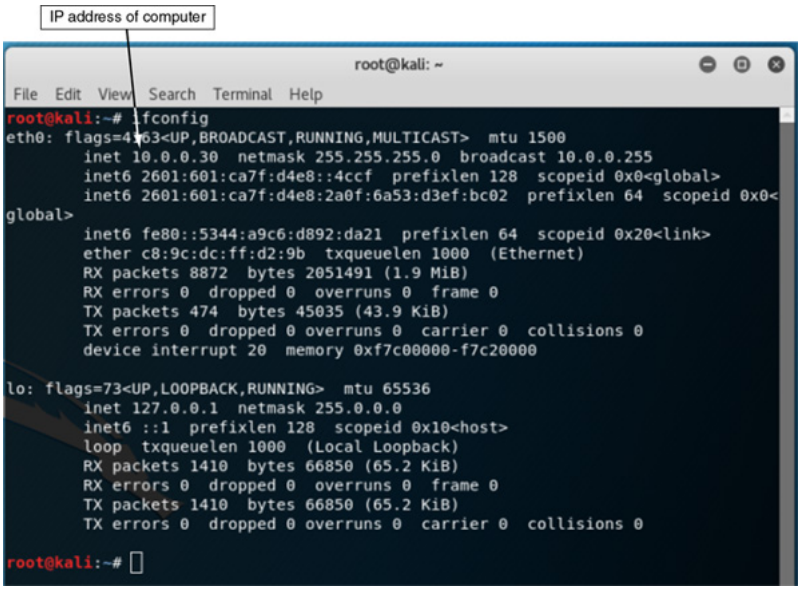
Identifying Open Ports and Making a Screen Capture

In this section, you use nmap to list open ports on your computer, and then use the EasyScreenCast tool to make a screen capture and record your actions:

1. Click the **EasyScreenCast** icon (the movie camera) in the upper-right corner of the Kali desktop, and click **Start Recording**.

2. In the terminal window, type **ifconfig** and press **Enter**. Find your computer's IP address, as shown in Figure 10-17, and then press the **Print Screen** key (substituting the key name on your computer). In this example, the IP address is in the first line of the eth0: section, starting with inet 10.0.0.30. Your ifconfig output will be different.

Figure 10-17.



Source: Kali Linux, www.kali.org

Getting your computer's IP address

Note

The following steps explain how to use nmap for a computer connected to a router. If your computer uses a wireless NIC, its IP address is listed in the wlan0 section of the ifconfig output.

3. Type **nmap -F -oN ~/Desktop/C10Proj3-open-ports-scans.txt 10.0.0.30** and press **Enter**.

4. Click the **EasyScreenCast** icon, and click **Stop Recording**. Click the **File Manager** toolbar icon, if necessary, and then click the **Picture** folder in the left pane. Drag the **Screenshot from *yyyy-mm-dd-hh-mm-ss*.png** file in the right pane to the GCFI-Evid drive.

5. Click the **Video** folder in the left pane, and then drag **Screencast_*mm-dd-yyyy_hh:mm:ss CC*.webm** in the right pane to the GCFI-Evid drive.

6. Drag the **C10Proj3-open-ports-scan.txt** file from the desktop to the GCFI-Evid drive.
7. Leave Kali Linux open as you answer the following review questions. When you're done, close any open windows, and shut down Kali Linux.

Review Questions

1. What is Kali Linux designed to do? (Choose all that apply.)
    a. Data acquisitions
    b. Live forensics analysis of a computer's disk drive
    c. Network penetration testing
    d. Network security assessment
2. Which versions of Kali Linux have a forensic boot mode? (Choose all that apply.)
    a. Kali Linux 64-bit
    b. Kali Linux Light 32-bit
    c. Kali Linux 64-bit VMware VM
    d. Kali Linux 64-bit Vbox
3. In Kali Linux, which of the following methods do you use to access Guymager?
    a. Click Applications, Information Gathering from the menu.
    b. Click Applications, Forensics from the menu.
    c. Click Applications, System Services from the menu.
    d. In a terminal window, type guymager and press Enter.
4. How do you capture a screenshot in Kali Linux?
    a. Click Applications, Information Gathering from the menu.
    b. Click Applications, Reporting Tools from the menu.
    c. Press the Print Screen key.
    d. Click Applications, point to Accessories, and click Midnight Commander.
5. On a computer running a wireless NIC, where do you find its IP address in the ifconfig output?
    a. The wlan0 section
    b. The etho0 section
    c. The lo Link encap:Local Loopback section
    d. The eno1 section

Chapter 11. E-mail and Social Media Investigations

Labs included in this chapter:

Lab 11.1 Using OSForensics to Search for E-mails and Mailboxes

Lab 11.2 Using Autopsy to Search for E-mails and Mailboxes

Lab 11.3 Finding Google Searches and Multiple E-mail Accounts

Note

Before starting these labs, create a subfolder of your work folder named Ch11.

Lab 11.1. Using OSForensics to Search for E-mails and Mailboxes

Objectives

After completing this lab, you will be able to:

- Load an image containing e-mails in OSForensics
- Search e-mails in OSForensics

OSForensics can't process Outlook .pst files, but it can extract messages from .pst files found on a drive or in an image of a drive. For this lab, Ron Torvald is a possible suspect in a case involving cybercrime and theft of computer files. You examine an image from Ron Torvald's computer to look for e-mail evidence of his criminal activity.

Materials Required

This lab requires the following:

- Windows
- OSForensics
- The MS E-mail Files.E01 file

Estimated completion time: 30–60 minutes

Activity

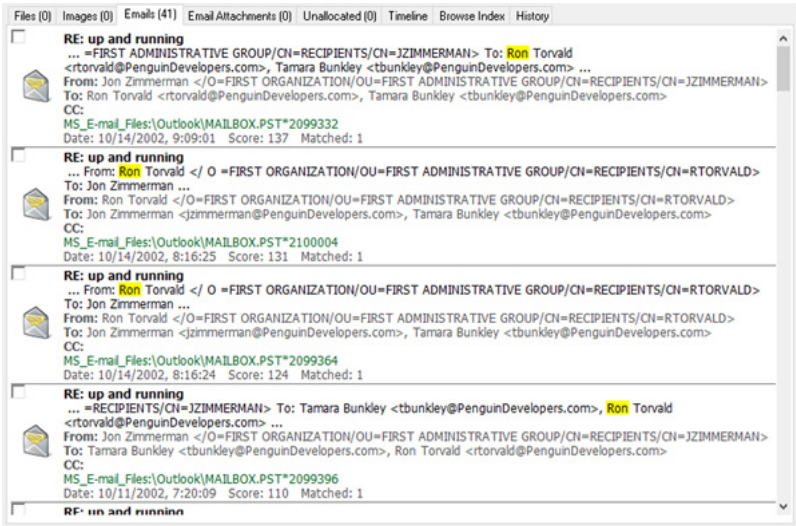
In this lab, you use OSForensics to search for e-mail evidence involving Ron Torvald:

1. Start OSForensics, and click **Yes** in the UAC message box. If necessary, click **Continue Using Free Version**. Click **Start** in the left pane, and click **Create Case** in the right pane.
2. In the New Case dialog box, type **C11Proj1** in the Case Name text box, type your name in the Investigator text box, and click the **Investigate Disk(s) from Another Machine** option button.
3. Click the **Custom Location** option button. Click **Browse**, navigate to and click your work folder, click the **Make New Folder** button, type **C11Proj1**, and click **OK** twice.
4. Click the **Add Device** button, click the **Image File** option button, click the **ellipse** button, navigate to and click your work folder, double-click **MS E-mail Files.E01** , and click **OK**.
5.

In the left pane, click **Create Index**. In the Step 1 of 5 window, click the **Use Pre-defined File Types** option button, click **Check All**, and click **Next**. In the Step 2 of 5 window, click the **Add** button. In the Add Start Location dialog box, verify that the **Whole Drive** option button is selected, and then click **OK**. Click **Next**, and in the Step 3 of 5 window, click **Start Indexing**. When OSForensics finishes indexing, click **OK** in the warning message box.

6. Click the **Search Index** button in the left pane, type **Ron** in the Enter Search Words text box, and click **Search** in the right pane. The e-mails on Ron Torvald's computer are listed in the Emails tab with their file headers containing timestamp confirmation data (see Figure 11-1).

Figure 11-1.

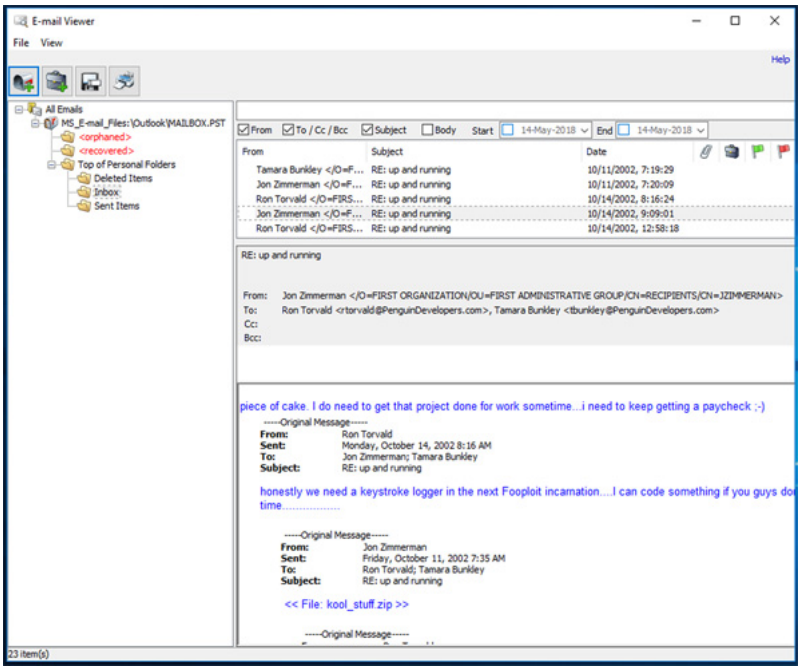


Source: PassMark Software, www.osforensics.com

E-mails displayed with file headers

7. Right-click the first e-mail and click **View with E-mail Viewer** to open the OSForensics E-mail Viewer (see Figure 11-2).

Figure 11-2.

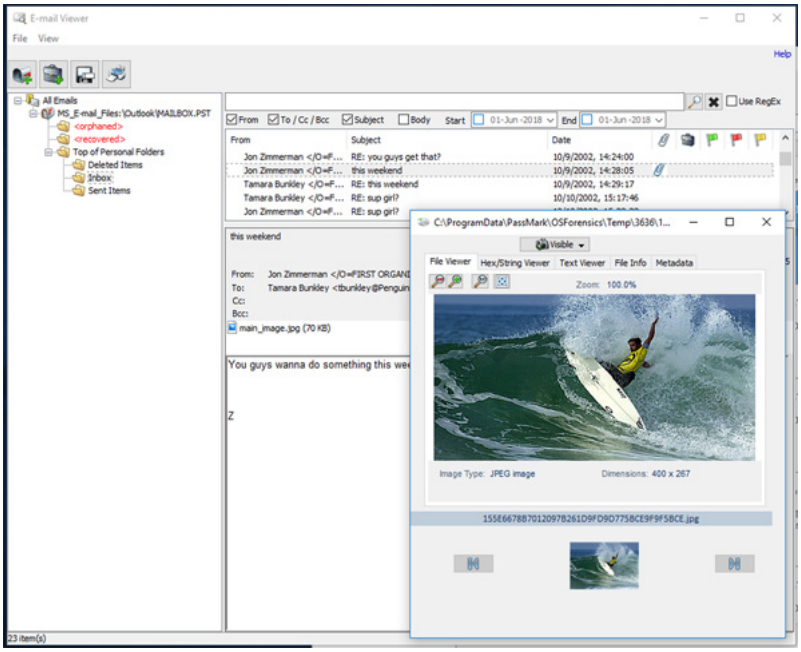


Source: PassMark Software, www.osforensics.com

Opening an e-mail in the built-in viewer

8. In the upper pane, scroll up and click the e-mail from Jon Zimmerman dated 10/9/2002, 14:28:05. In the lower pane, double-click the attached file **main_image.jpg (70 KB)** to view it (see Figure 11-3). In the left pane, expand **MS_E-mail_Files:\Outlook\MAILBOX.PST** and **Top of Personal Folders,** if necessary, to see the Deleted Items, Inbox, and Sent Items folders. Click the **Deleted Items** folder to see deleted e-mails.

Figure 11-3.



Source: PassMark Software, www.osforensics.com

Viewing a file attached to an e-mail

Tip

Files attached to e-mails have a paper clip symbol next to the timestamp in the upper pane.

9. In the left pane, click the **MS_E-mail:\Outlook\MAILBOX.PST** folder, and in the upper pane, click the **From** column header to sort the messages alphabetically. Scroll down the upper pane to find e-mails from Tamara Bunkley. Click the e-mail with the subject "RE: this weekend," and examine its contents in the lower pane. Notice that it's a reply to an e-mail sent by Jon Zimmerman.

10. Leave OSForensics open as you answer the following review questions. When you're finished, close all open windows, and exit OSForensics.

Review Questions

1. How many e-mails were deleted from Ron Torvald's Outlook mailbox?
2. How many e-mails with attached files did Ron Torvald get from Tamara Bunkley?
3. Deleted e-mails with attachments can't be viewed. True or False?
4. How many e-mails did you find by using "Ron" as a search keyword?
5. How many zipped files are attached to e-mails?

Lab 11.2. Using Autopsy to Search for E-mails and Mailboxes

Objectives

After completing this lab, you will be able to:

- Load an image containing e-mails in Autopsy
- Use Autopsy to look for evidence in e-mails

Like OSForensics, Autopsy can't process Outlook .pst files individually, so you must search an entire image to find e-mail evidence. In previous labs, you validated the results of forensic searches by using multiple software tools to find additional evidence. In this lab, you use Autopsy to search for e-mail evidence in an image and try to find additional e-mails that might not have been discovered in OSForensics.

Materials Required

This lab requires the following:

- Windows
- Autopsy 4.3.0
- The MS E-mail Files.E01 file from Lab 11.1

Estimated completion time: 30–60 minutes

Activity

In this lab, you search the MS E-mail Files.E01 file in Autopsy to find e-mail evidence:

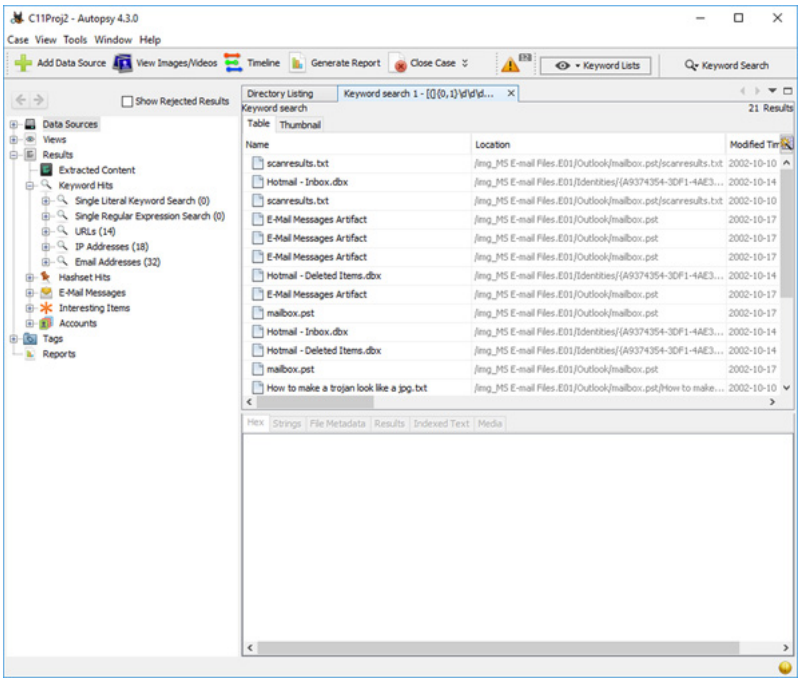
1. Start Autopsy, and click the **Create New Case** button. In the New Case Information window, type **C11Proj2** in the Case Name text box. Click **Browse** next to the Base

Directory text box, navigate to and click your work folder, click **Select** to enter this path, and then click **Next**. In the Additional Information window, type **C11Proj2** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

2. In the Select Data Source window, click **Disk Image or VM file** in the "Select data source type" list box, if necessary. Click **Browse**, navigate to your work folder, double-click the **MS E-mail Files.E01** file, and click **Next**. In the Configure Ingest Modules window, click **Select All**, and then click **Next** and **Finish** to start analyzing the evidence.

3. Click the **Keyword Lists** down arrow, click the **Phone Numbers**, **IP Addresses**, **Email Addresses**, and **URLs** check boxes, and then click the **Search** button to begin searching for mailboxes and files that match the phone number, IP address, e-mail address, or URL patterns. Figure 11-4 shows the results.

Figure 11-4.



Source: www.sleuthkit.org

Viewing mailboxes found in an image

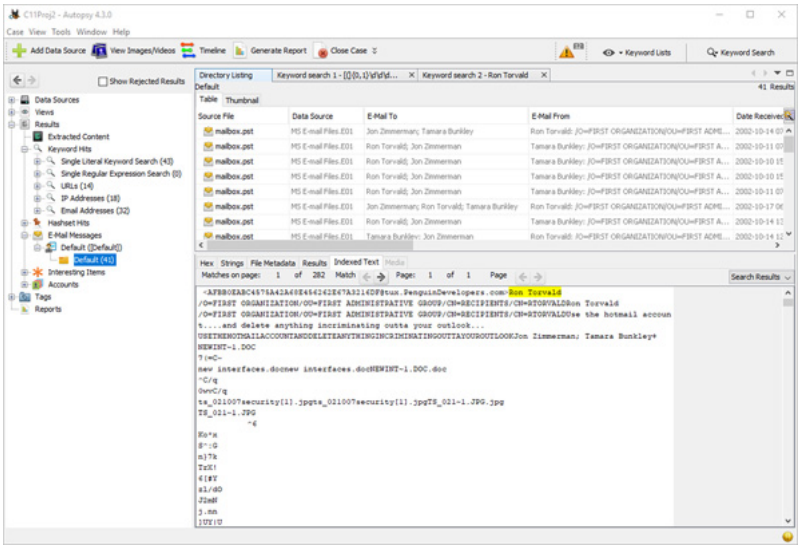
4. Click **Keyword Search** at the upper right, type **Ron Torvald**, and click **Search**.

5. In the Result Viewer pane, scroll down and click the **Sent Items.dbx** folder to see the e-mails Ron Torvald sent; his name is highlighted in yellow in these e-mails. Use the Content Viewer pane to view the contents of these e-mails.

6. In the Result Viewer pane, scroll up and click the **mailbox.pst** folder to see the e-mails Ron Torvald received; again, his name is highlighted in yellow. View the e-mails' contents in the Content Viewer pane.

7. In the left pane, expand **E-Mail Messages** and **Default ([Default])**, and click the **Default** folder to see e-mails listed in the E-Mail To and E-Mail From columns, as shown in Figure 11-5.

Figure 11-5.



Source: www.sleuthkit.org

Viewing all e-mails

8. In the left pane, expand **Views**, **File Types**, and **By Extensions**, and then click the **Images** folder. Click the **Thumbnail** tab in the Result Viewer pane to see the pictures attached to e-mails. Click the **Table** tab, and scroll to the right to see the MD5 hash value for each graphics file.

9. In the left pane, expand **Results** and **Keyword Hits**, and click the **Email Addresses** folder. In the Result Viewer pane, examine the Files with Hits column to find each of these e-mail addresses.

10. Leave Autopsy open as you answer the following review questions. When you're finished, close all open windows, and exit Autopsy.

Review Questions

1. How many graphics files did Autopsy recover?
2. How many Hotmail e-mail addresses did you find?
3. How many video files are attached to e-mails in the MS E-mail Files.E01 image?
   a. 16
   b. 0
   c. 2
   d. 3
4. In the Archive folder (under the File Type, By Extension path), how many archive files did Autopsy recover?
   a. 0
   b. 1
   c. 2
   d. 5
5. Autopsy recovered the same number of e-mails as OSForensics did. True or False?

Lab 11.3. Finding Google Searches and Multiple E-mail Accounts

Objectives

After completing this lab, you will be able to:

- Find Google searches and associated text
- Find mailboxes associated with multiple e-mail accounts

Frodo Baggins, a suspect in a digital crime, used his forensics skills to discover account passwords by using information he found in the Windows Registry. In this lab, you use Autopsy to find e-mail and Google search evidence showing that Frodo Baggins hacked a Windows computer's Registry to discover user account passwords.

Materials Required

This lab requires the following:

- Windows
- Autopsy 4.3.0
- The precious.001 file

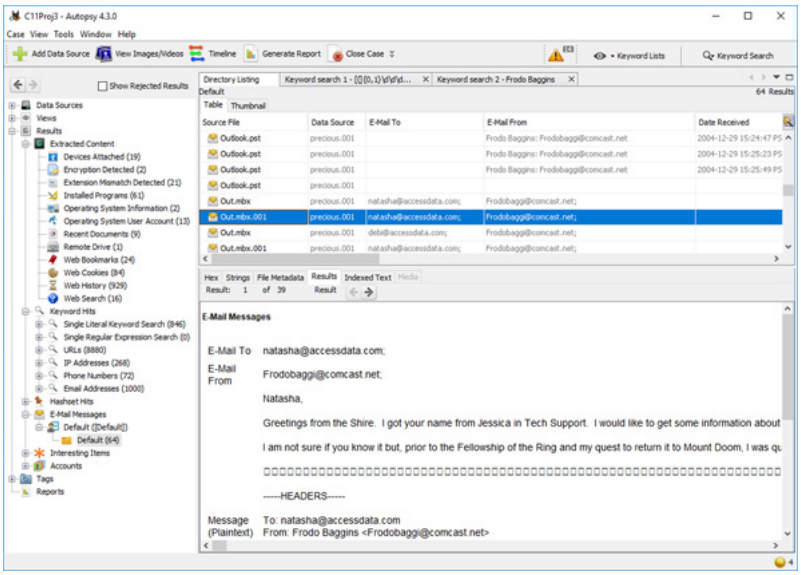
Estimated completion time: 60 minutes

Activity

In this lab, you use Autopsy to find evidence of Google searches and multiple e-mail accounts on a Windows computer:

1. Start Autopsy, and click the **Create New Case** button. In the New Case Information window, type **C11Proj3** in the Case Name text box. Click **Browse** next to the Base Directory text box, navigate to and click your work folder, click **Select** to enter this path, and then click **Next**. In the Additional Information window, type **C11Proj3** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.
2. In the Select Data Source window, click **Disk Image or VM file** in the "Select data source type" list box, if necessary. Click **Browse**, navigate to and click your work folder, double-click the **precious.001** file, and click **Next**. In the Configure Ingest Modules window, click **Next** and then **Finish** to start analyzing the evidence.
3. Click the **Keyword Lists** down arrow, click the **Phone Numbers**, **IP Addresses**, **Email Addresses**, and **URLs** check boxes, and then click **Search** to view all the mailboxes on this computer.
4. Click **Keyword Search** at the upper right, type **Frodo Baggins**, and click **Search**.
5. In the left pane, expand **E-Mail Messages** and **Default ([Default])** and click the **Default** folder. Scroll down the Result Viewer pane, and click the first **Out.mbx.001** mailbox to see its contents in the Content Viewer pane (see Figure 11-6).

Figure 11-6.



Source: www.sleuthkit.org

Viewing the text of an e-mail

Note

Some results in **Figure 11-6** are duplicated because of the combined keyword searches 1 and 2.

6. Click the **Indexed Text** tab in the Content Viewer pane to see the e-mail header information, including the Message-Id, which uniquely identifies the message in the e-mail server database.

7. In the left pane, expand **Results** and **Extracted Content**, if necessary, and click the **Web Search** folder. In the Result Viewer pane, examine the Text column to see Internet Relay Chat (IRC) searches.

8. In the left pane, expand **Keyword Hits**, if necessary, and click the **Email Addresses** folder. Examine the Result Viewer pane to find any e-mail addresses that might belong to Frodo Baggins.

9. Leave Autopsy open as you answer the following review questions. When you're finished, exit Autopsy.

Review Questions

1. How many e-mails, including duplicates, did you find?
2. How many different Frodo Baggins e-mail addresses did Autopsy recover?
3. Frodo Baggins didn't have an AOL e-mail account. True or False?
4. How many Google searches for the term "computer forensics" were made?
5. MD5 hash values are displayed automatically in the default mailbox view. True or False?

Chapter 12. Mobile Device Forensics

Labs included in this chapter:

Lab 12.1 Examining Cell Phone Storage Devices

Lab 12.2 Using FTK Imager Lite to View Text Messages, Phone Numbers, and Photos

Lab 12.3 Using Autopsy to Search Cloud Backups of Mobile Devices

Note

Before starting these labs, create a subfolder of your work folder named Ch12.

Lab 12.1. Examining Cell Phone Storage Devices

Objectives

After completing this lab, you will be able to:

- Process an image of a cell phone and its storage device in Autopsy
- Examine forensic data on cell phones and their storage devices

Most cell phones support removable memory storage devices, such as MicroSD flash devices, that can store up to 400 GB of data. These devices can contain personal information, photos, and other data that's useful in a forensics investigation. Creating an image of these devices separately from imaging cell phones is recommended. Recovering cell phone data can be challenging because no single standard exists for how and where phones store messages, and file systems vary from manufacturer to manufacturer. In this lab, you use Autopsy to process a forensic image of a Motorola cell phone and its MicroSD storage device.

Materials Required

This lab requires the following:

- Windows
- Autopsy 4.3.0?
- The Motorola.E01 file

Estimated completion time: 90–120 minutes, depending on your computer's performance

Activity

In this lab, you examine a Motorola cell phone image to look for forensic evidence:

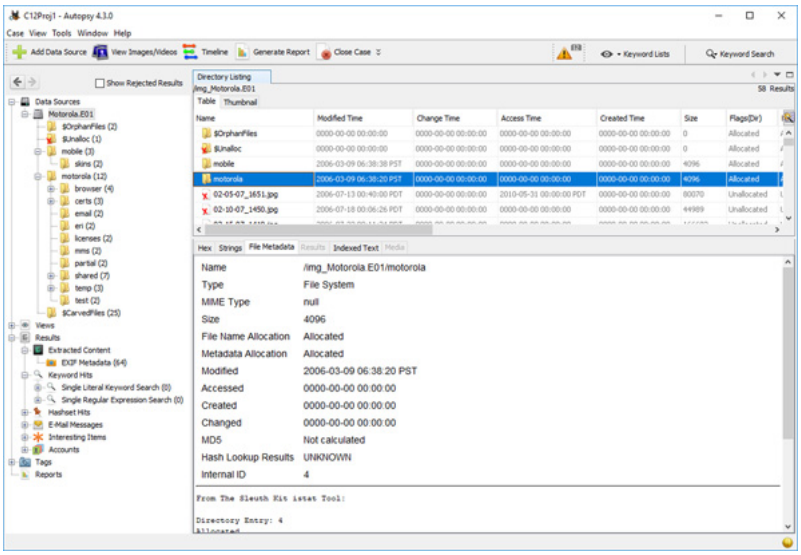
1. Start Autopsy, and in the Welcome window, click the **Create New Case** button. In the New Case Information window, type **C12Proj1** in the Case Name text box. Click the **Browse** button next to the Base Directory text box, navigate to and click your work folder, click **Select** to enter this path, and then click **Next**.

2. In the Additional Information window, type **C12Proj1** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

3. In the Select Data Source window, click **Disk Image or VM file** in the "Select data source type" list box, if necessary. Click the **Browse** button, navigate to your work folder, click the **Motorola.E01** file, and click **Open**. Click **Next**. In the Configure Ingest Modules window, click **Select All**, and then click **Next**, and **Finish** to start analyzing the evidence.

4. In the left pane, expand **Data Sources**, and double-click the **Motorola.E01** folder to view the phone's OS folders and its MicroSD storage device. Click the **motorola** folder in the Result Viewer pane, and click the **File Metadata** tab in the Content Viewer pane to see the MicroSD storage device (see Figure 12-1). In the Result Viewer pane, a red × next to files means they were deleted. The Unallocated entry in the Flags(Dir) column means these files are in unallocated space on the storage device. Click the first two deleted files to see the recovered JPG files on this storage device. Click the third deleted file, and notice a blank photo in the Content Viewer pane, which indicates the file header was recovered, but the image content can't be recovered.

Figure 12-1.

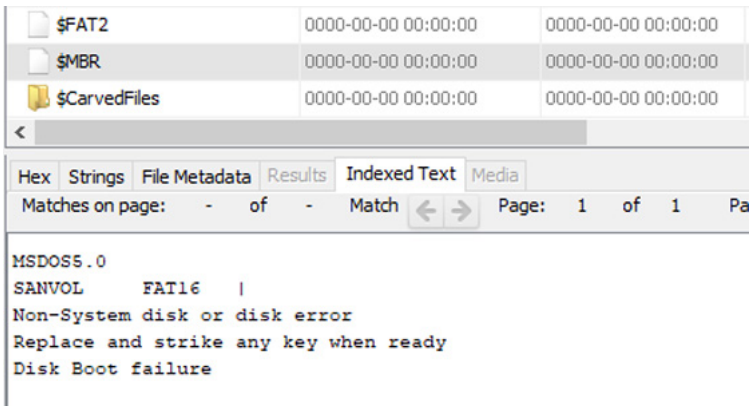


Source: www.sleuthkit.org

Viewing cell phone data in Autopsy

5. Scroll down the Result Viewer pane, and click the **$MBR** file. Its icon and metadata are grayed out, indicating it's a hidden system file. This file is the Master Boot Record and contains the file system information needed to mount the storage device. Click the **Indexed Text** tab in the Content Viewer pane, if necessary, to see that the file system is FAT16 and the storage device is named SANVOL (see Figure 12-2). SANVOL, manufactured by SanDisk, is a MicroSD storage device, which can help forensics investigators identify it.

Figure 12-2.



Source: www.sleuthkit.org

Viewing file system information

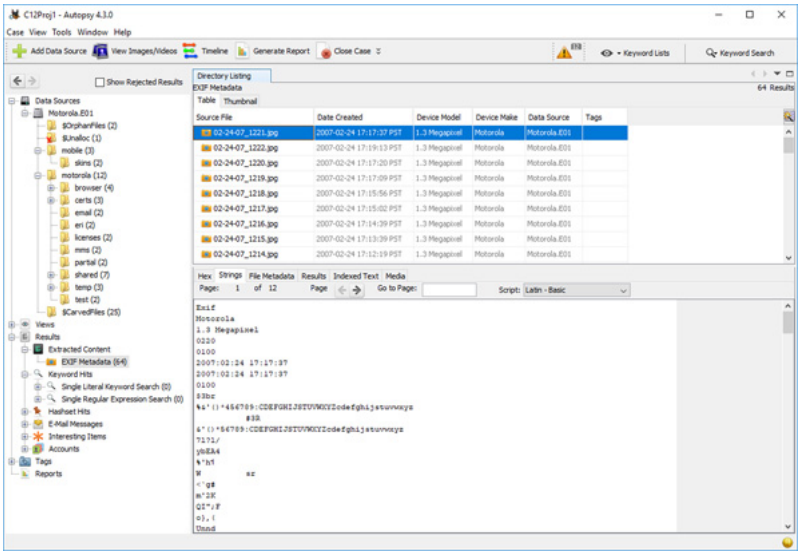
6. Click the **$CarvedFiles** folder in the left pane to see data on graphics files carved from unallocated space. Click the **Thumbnail** tab in the Result Viewer pane, and scroll down to see all the recovered files, including blank (unrecovered) photos in the cell phone's memory storage.

Note

Most cell phones and tablets have built-in memory storage in addition to what's available on storage devices.

7. In the left pane, expand **Extracted Content**, if necessary, and click the **EXIF Metadata** folder. In the Result Viewer pane, click the first graphics file, and then click the **Indexed Text** tab in the Content Viewer pane to see detailed metadata about this file. Click the **Strings** tab, and notice that the second and third lines list Motorola and 1.3 Megapixel. Autopsy interprets and displays this information in the Result Viewer pane as the phone's device model and make (see Figure 12-3).

Figure 12-3.



Source: www.sleuthkit.org

Viewing Exif information

8. Leave Autopsy open as you answer the following review questions. When you're finished, exit Autopsy.

Review Questions

1. Under the EXIF Metadata folder in the left pane of Autopsy, how many pictures have been recovered from the cell phone image?

2. How many subfolders are under the motorola folder (the MicroSD storage device)?

   a. 10

   b. 16

   c. 31

   d. 64

3. Which file system is in use on the MicroSD storage device?

   a. NTFS

b. FAT32

c. FAT16

d. HPF+

4. What's the resolution of the cell phone's camera?

a. Can't be determined from the evidence

b. 3.0 MP

c. 4.0 MP

d. 1.3 MP

5. Which column do you check to determine whether a file is in unallocated space?

Lab 12.2. Using FTK Imager Lite to View Text Messages, Phone Numbers, and Photos

Objectives

After completing this lab, you will be able to:

> - Process a cell phone image in FTK Imager Lite
> - Use FTK Imager Lite to look for cell phone evidence

Recovering forensic data from cell phones and other mobile devices can be challenging because of the wide variety of platforms, such as Apple iOS, Google OS, Android, Windows Mobile, and others. Some forensics tools capture data by using USB adapters or tablet devices that create an .E01 or a raw image that can be processed by most forensics tools. AccessData Mobile Phone Examiner (MPE+) creates .ad1 images that can be processed by Forensic Toolkit or FTK Imager Lite to recover evidence. FTK Imager Lite is useful for screening devices before having to use expensive and often time-consuming forensics tools. In this lab, you process the .ad1 image of an LG 6000 cell phone to look for evidence.

Materials Required

This lab requires the following:

- Windows
- FTK Imager Lite
- The LG_6000_4d76e052.ad1 file

Estimated completion time: 30–60 minutes

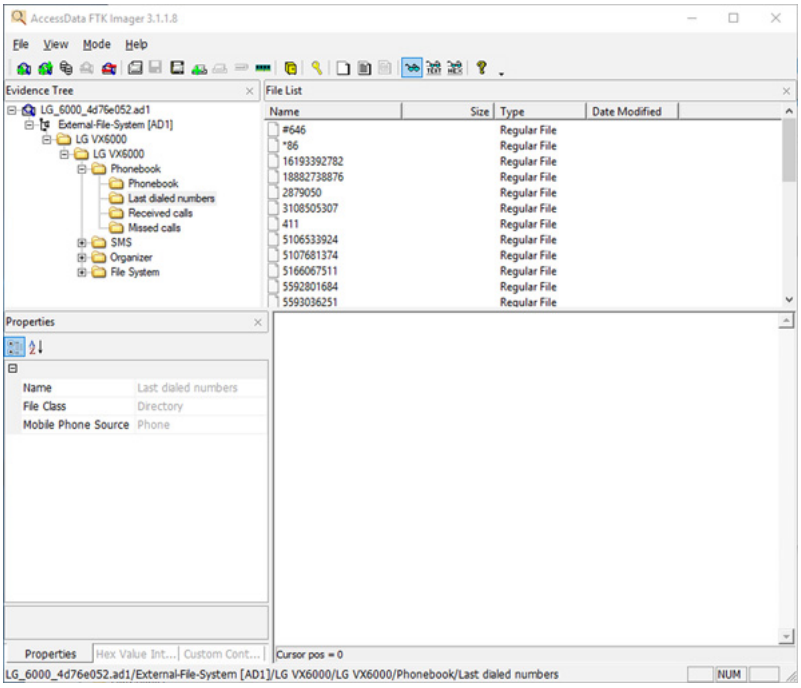
Activity

In this lab, you examine a cell phone image in FTK Imager Lite:

1. Start FTK Imager Lite, clicking **Yes** in the UAC message box, if necessary.
2. Click **File**, **Add Evidence Item** from the menu. In the Select Source dialog box, click the **Image File** option button, and then click **Next**.
3. In the Select File dialog box, click **Browse**, navigate to your work folder, double-click the **LG_6000_4d76e052.ad1** file, and then click **Finish**.
4. In the Evidence Tree pane, expand **LG_6000_4d76e052.ad1** , **External-File-System [AD1]**, and **LG VX6000**. Expand the **LG VX6000** and **Phonebook** subfolders.

5. Click the **Last dialed numbers** folder. The most recent numbers stored in the phone's memory are shown in the File List pane on the right (see Figure 12-4). Use the scrollbar, if needed, to view all the numbers.

Figure 12-4.



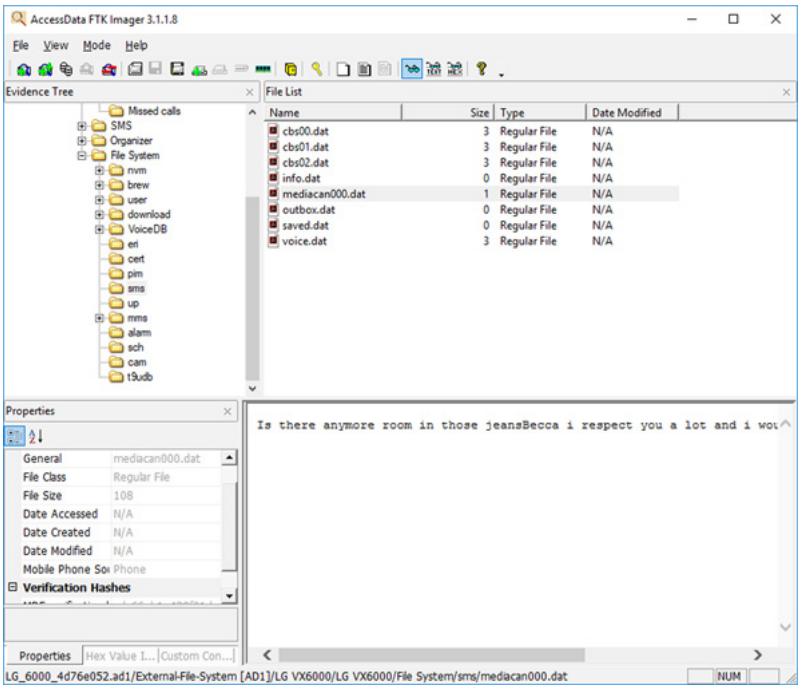
Source: AccessData Group, Inc., www.accessdata.com

Viewing the most recent phone numbers dialed

6. Click the **Received calls** folder to see inbound calls. This image file doesn't show the times and dates of these calls, but you can get this information from the service provider or through AccessData MPE+. Next, click the **Missed calls** folder to see inbound calls that weren't answered.

7. In the Evidence Tree pane, expand **File System**, and then click the **sms** folder to view text messages sent to the phone. In the File List pane, click the **mediacan000.dat** file, and read its contents in the lower-right pane (see Figure 12-5).

Figure 12-5.



Source: AccessData Group, Inc., www.accessdata.com

Viewing the contents of a text message

8. Click the **eyeglass** toolbar icon, and then click the **cam** folder in the Evidence Tree pane to look for photos taken by the phone's camera. Click each **.jpg** file in the File List pane to see it in the viewer.

9. Leave FTK Imager Lite open as you answer the following review questions. When you're finished, exit FTK Imager Lite.

Review Questions

1. How many phone numbers with a valid number of digits were dialed on this phone?
   a. 25
   b. 28
   c. This information can't be determined based on the data recovered.
   d. No numbers were dialed.
2. How many received calls couldn't be identified?
3. FTK Imager Lite can be used to determine outgoing call dates and times on cell phones. True or False?
4. How many photos were taken by this phone's camera?
5. How many dialed calls were local numbers, not long distance?

Lab 12.3. Using Autopsy to Search Cloud Backups of Mobile Devices

Objectives

After completing this lab, you will be able to:

- Search cloud backups in Autopsy

- Use Autopsy to search for evidence linked between multiple images

In Chapter 12 of the textbook, you processed a case involving the seizure of cloud backup images of Randall's and Sarah's mobile devices. You need to look for additional bank information or funding indicating that a money-laundering scheme was used to avoid taxes. In this lab, you examine the same two images to look for this information.

Materials Required

This lab requires the following:

- Windows
- Autopsy 4.3.0
- The InCh12Randall.exe and InCh12Sarah.exe files

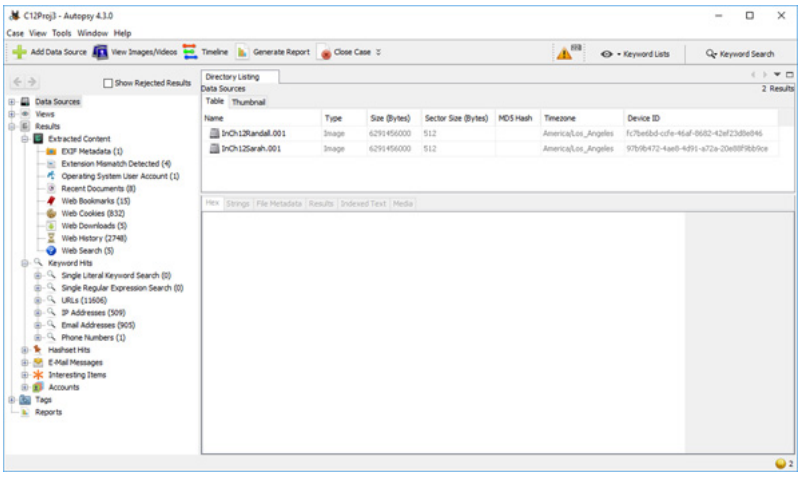
Estimated completion time: 60–90 minutes

Activity

In this lab, you use Autopsy to search mobile device images for evidence involving money transfers between bank accounts:

1. Extract the **InCh12Randall.exe** and **InCh12Sarah.exe** files to your work folder. (This process might take a few minutes.) Start Autopsy, and in the Welcome window, click the **Create New Case** button. In the New Case Information window, type **C12Proj3** in the Case Name text box, verify that your work folder is displayed in the Base Directory text box, and then click **Next**.
2. In the Additional Information window, type **C12Proj3** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.
3. In the Select Data Source window, click **Disk Image or VM file** in the "Select data source type" list box, if necessary. Click the **Browse** button, navigate to and click your work folder, double-click the **InCh12Randall.001** file, and then click **Next**.
4. In the Configure Ingest Modules window, click **Select All**, and then click **Next** and **Finish** to start analyzing the evidence.
5. Click the **Add Data Source** button. In the Select Data Source window, click **Disk Image or VM file** in the "Select data source type" list box, if necessary. Click the **Browse** button, navigate to and click your work folder, double-click the **InCh12Sarah.001** file, and then click **Next**.
6. Click **Next** to accept the ingest modules configured in Step 4, and then click **Finish** to start analyzing the evidence, which takes a few minutes. When it's finished, you should see the two image files in the Directory Listing pane on the right (see Figure 12-6).

Figure 12-6.



Source: www.sleuthkit.org

Image files loaded in Autopsy

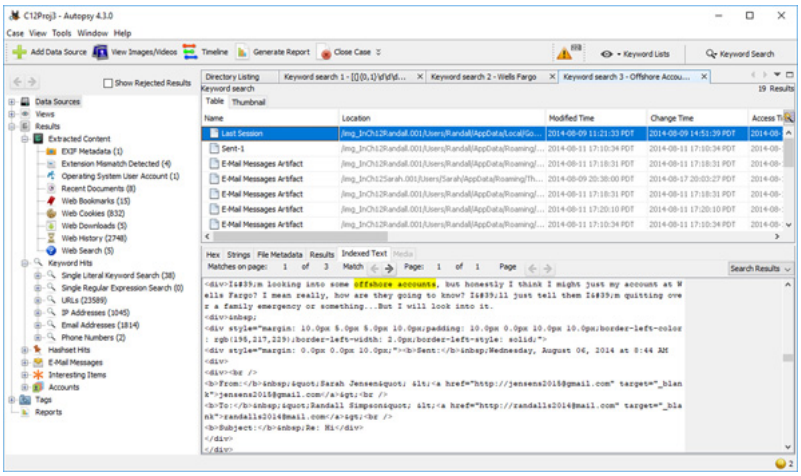
7. Click the **Keyword Lists** down arrow. Click the **Phone Numbers**, **IP Addresses**, **Email Addresses**, and **URLs** check boxes, and then click the **Search** button. Wait until the search is finished before going on to the next step.

8. Click **Keyword Search** at the upper right, type **Wells Fargo**, and click **Search**. Click **Keyword Search** again, type **Offshore Accounts**, and click **Search**.

9. Click the **Keyword search 2 - Wells Fargo** tab, and click the first e-mail listed. The Content Viewer pane shows the keyword highlighted in yellow. Click the **Inbox**, **Sent Mail**, and **Trash** e-mails in the Result Viewer pane, and read each one in the Content Viewer pane.

10. Click the **Keyword search 3 - Offshore Accounts** tab, and click the first e-mail listed. The Content Viewer pane shows the keyword highlighted in yellow (see Figure 12-7). Click the **Inbox**, **Sent Mail**, and **Trash** e-mails in the Result Viewer pane, and read each one in the Content Viewer pane.

Figure 12-7.



Source: www.sleuthkit.org

Viewing the keyword search results

11. Leave Autopsy open as you answer the following review questions. Use additional functions in Autopsy, such as other keyword searches, to find the answers to these

questions. When you're finished, exit Autopsy.

Review Questions

1. How much money did Randall Simpson tell Sarah to ask her boss to fund?
2. What phone number was recovered in the evidence?
3. How many recovered e-mails were in the Default folder?
    a. 866
    b. 341
    c. 225
    d. 6782
4. No photos were recovered on either mobile device. True or False?
5. Evidence shows that both Randall and Sarah were involved in transferring money. True or False?

Chapter 13. Cloud Forensics

Labs included in this chapter:

Lab 13.1 Examining Dropbox Cloud Storage

Lab 13.2 Examining Google Drive Cloud Storage

Lab 13.3 Examining OneDrive Cloud Storage

Note

Before starting these labs, create a subfolder of your work folder named Ch13.

Lab 13.1. Examining Dropbox Cloud Storage

Objectives

After completing this lab, you will be able to:

- Look for Dropbox account information
- Search for files transferred with Dropbox

Dropbox cloud storage uses several files on a client computer to store information. An important one is filecache.dbx, which stores information on shared directories associated with a Dropbox user account and file transfers between Dropbox and the client's system. Dropbox files on a system indicate a source of forensic evidence.

Materials Required

This lab requires the following:

- Windows
- Autopsy 4.3.0
- The Dropbox account folder from Data Files

Estimated completion time: 20–40 minutes, depending on your computer's performance

Activity

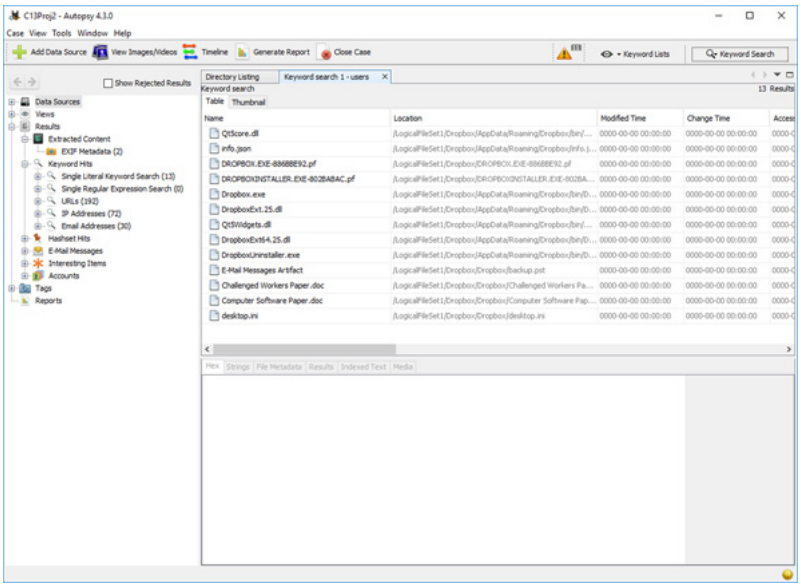
In this lab, you examine a Dropbox account to look for evidence:

1. Start Autopsy. In the Welcome window, click **Create New Case**. In the New Case Information window, type **C13Proj1** in the Case Name text box, and then click **Next**. In the Additional Information window, type **C13Proj1** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

2. In the Select Data Source window, click the **Select data source type** down arrow, click **Logical Files**, and then click **Add**. Click the **Browse** button, navigate to and click your work folder, click the **Dropbox** folder, click **Open**, and then click **Next**. In the Configure Ingest Modules window, click **Next** to accept the default modules, and then click **Finish**.

3. Click **Keyword Search** at the upper right, type **users** in the text box, and click **Search** to look for the username associated with this Dropbox account. Figure 13-1 shows the results.

Figure 13-1.



Source: www.sleuthkit.org

Viewing the Dropbox search results

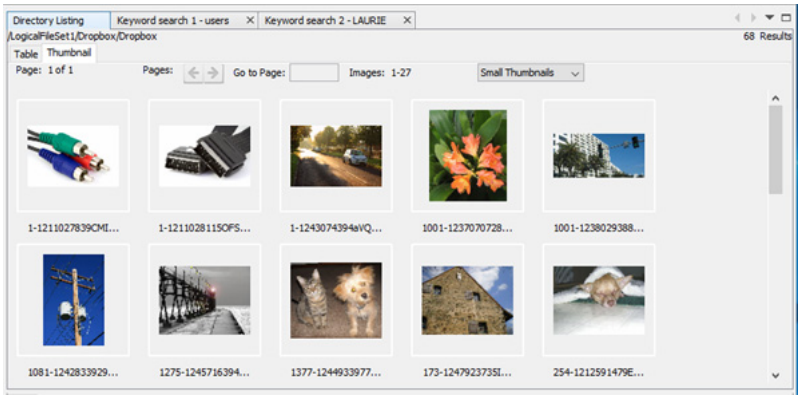
4. In the Result Viewer pane, click the **DROPBOXINSTALLER.EXE-802BABAC.pf** file, which is the Dropbox prefetch file. You can then see the username LAURIE in the Content Viewer pane to the right of the word USERS.

5. Click **Keyword Search** at the upper right, type **LAURIE** in the text box, and click **Search** to look for other information associated with this user account.

6. In the left pane, expand **Data Sources**, **LogicalFileSet1**, **Dropbox**, and **AppData**, and click the **Dropbox** folder to see the files that were synced with cloud storage.

7. Click the **Thumbnail** tab in the Result Viewer pane to see the images transferred with Dropbox (see Figure 13-2). If necessary, scroll to see all the files.

Figure 13-2.



Source: www.sleuthkit.org

Images transferred with Dropbox

8. In the left pane, expand **Views**, **File Types**, and **By Extension**, and click **Documents**. Click the **Table** tab in the Result Viewer pane to see the documents stored in the cloud.

9. Click **Keyword Search** at the upper right, type **filecache.dbx** in the text box, and click **Search** to look for this file containing information on shared directories and file

transfers.

10. In the left pane, expand all folders under **Data Sources**, and examine their contents to see what file types are stored in each folder.

Note

The filecache.dbx file is in base-64 format, so you need specialized software to read it. One tool for this purpose is Magnet Forensics Dropbox Decryptor. For more information on this free tool, go to www.magnetforensics.com/free-tool-dropbox-decryptor/. To run this tool, you need the password for the Dropbox account you're investigating. See the Magnet Forensic Web site for more information about decrypting filecache.dbx.

11. Leave Autopsy open as you answer the following review questions. When you're finished, exit Autopsy.

Review Questions

1. Under the Documents folder, how many Office files were recovered from this Dropbox account?
   a. 1
   b. 9
   c. 68
   d. 38
2. In the left pane of Autopsy, where are the prefetch (.pf) files for this Dropbox account shown?
   a. LogicalFileSet1(1), Dropbox(4)
   b. LogicalFileSet1(1), Dropbox(4), AppData(1)
   c. Views, File Type, By Extension, Executable
   d. Views, File Type, By MIME Type, pdf
3. Autopsy can read the contents of the filecache.dbx file. True or False?
4. What usernames are associated with this Dropbox account?
5. What tool can be used to decode Dropbox-encoded files?
   a. Autopsy 4.3.0 or later
   b. WinHex
   c. QuickHash-Windows
   d. Magnet Forensics Dropbox Decryptor

Lab 13.2. Examining Google Drive Cloud Storage

Objectives

After completing this lab, you will be able to:

- Describe the Google Drive cloud storage structure
- Use an SQL viewer and convert UNIX timestamps

Searching for information on Google Drive cloud storage is much easier than finding Dropbox information because Google Drive doesn't use a base-64 file format. It stores information on local cloud entries (such as filenames, MD5 hash values, modified and created dates in UNIX

timestamp format, and the status of the file, if it was deleted) in the snapshot.db database. To view this database, you use an SQL viewer, such as DB Browser for SQLite. To convert UNIX timestamps, you can use online tools, such as EpochConverter (www.epochconverter.com).

In addition, Google Drive has two subfolders of interest to digital forensics examiners: the AppData folder, where all user information is stored, and the Google Drive folder, where all data files are stored. In this lab, you look for information on Google Drive transactions.

Materials Required

This lab requires the following:

- Windows
- Autopsy 4.3.0
- DB Browser for SQLite, downloaded in **Step 9**
- EpochConverter, downloaded in **Step 11**
- The Google Drive account folder from Data Files

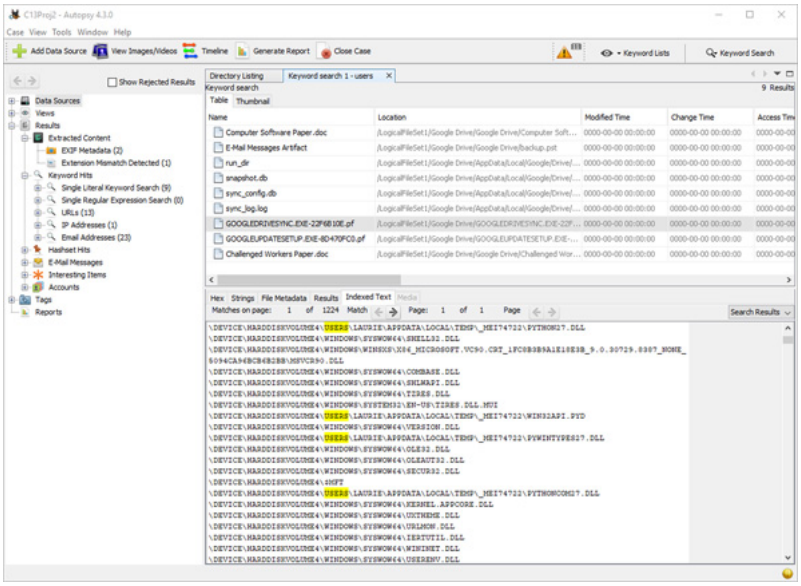
Estimated completion time: 30–45 minutes

Activity

In this lab, you examine a Google Drive account on a computer to look for evidence:

1. Start Autopsy. In the Welcome window, click **Create New Case**.
2. In the New Case Information window, type **C13Proj2** in the Case Name text box, and then click **Next**. In the Additional Information window, type **C13Proj2** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.
3. In the Select Data Source window, click the **Select data source type** down arrow, click **Logical Files**, and then click **Add**. Click the **Browse** button, navigate to and click your work folder, click the **Google Drive** folder, click **Open**, and then click **Next**. In the Configure Ingest Modules window, click **Next** to accept the default modules, and then click **Finish**.
4. Click **Keyword Search** at the upper right, type **users** in the text box, and click **Search** to look for the username associated with this Google Drive account.
5. In the Result Viewer pane, click the **GOOGLEDRIVESYNC.EXE-22F6B10E.pf** file, a Google Drive prefetch file, to see the username for this account in the Content Viewer pane, as shown in Figure 13-3.

Figure 13-3.



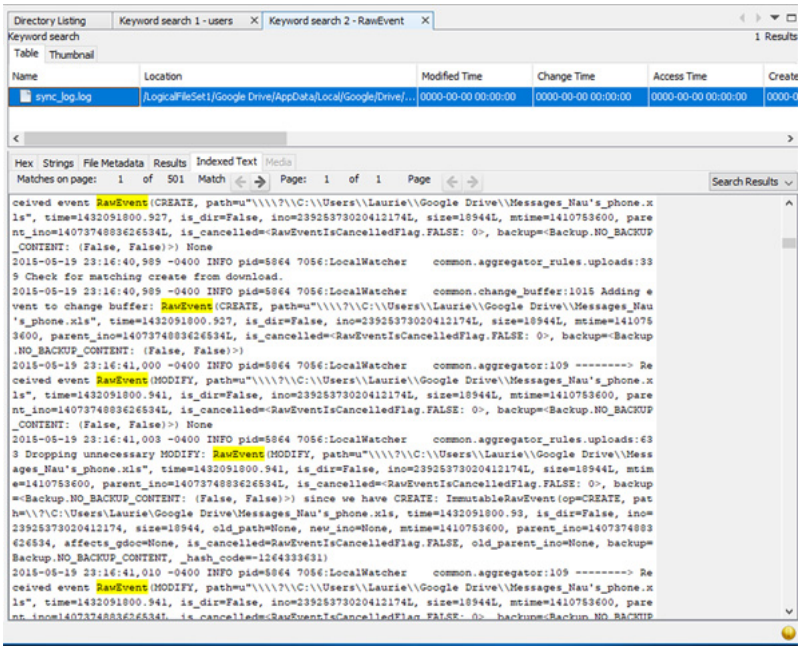
Source: www.sleuthkit.org

Viewing Google Drive search results

6. In the Result Viewer pane, click the **sync_log.log** file to see a detailed list of a user's cloud transactions. This log file isn't in a base-64 format, so you can view it with a text editor or the Autopsy built-in viewer.

7. Click **Keyword Search** at the upper right, type **RawEvent** in the text box, and click **Search**. Then click **sync_log.log** in the Result Viewer pane to look for the create, modify, and deleted dates for this account's cloud transactions. Figure 13-4 shows the results.

Figure 13-4.



Source: www.sleuthkit.org

Viewing search results for the RawEvent keyword

Tip

The string values that indicate UNIX timestamps are RawEvent (CREATE, RawEvent (MODIFY, and RawEvent (DELETE.

8. In the left pane, expand **Results** and **Keyword Hits**, if necessary. Click the **Single Literal Keyword Search** folder, and then double-click **users (9)** in the Result Viewer pane. Right-click the **snapshot.db** file, point to **Extract File(s)**, and click **Save** to extract this file to the C:*Work*\C13Proj2\Export folder. Click **OK**.

9. Start a Web browser, and go to http://sqlitebrowser.org. Download and install the correct DB Browser for SQLite (32-bit or 64-bit) for your version of Windows.

10. Start DB Browser for SQLite, and click **File**, **Open Database** from the menu. Navigate to **C:*Work*\C13Proj2\Export**, and double-click the **snapshot.db** file.

11. Click the **Browse Data** tab to view Google Drive filenames with their modified and created UNIX timestamps, which show the last date and time data was synced with the cloud. To convert the UNIX timestamps, start a Web browser, if necessary, and go to www.epochconverter.com. Copy each timestamp from DB Browser for SQLite, and paste it in the text box at the top of the EpochConverter page. Click the **Timestamp to Human date** button.

Tip

To see how to do a batch conversion of UNIX timestamps in Excel, see the "Convert Timestamp To Date" section of the article at www.extendoffice.com/documents/excel/2473-excel-timestamp-to-date.html. For more information about Google Drive artifacts, see http://bitforensics.blogspot.com/2012/12/google-drive-artifacts-explained.html.

12. Leave all windows open as you answer the following review questions. When you're finished, exit Autopsy, DB Browser for SQLite, and EpochConverter, and close any open windows.

Review Questions

1. Which Google Drive file contains the list of deleted files?
   a. snapshot.db
   b. sync_log.log
   c. RawEvent
   d. Prefetch
2. What folder contains user files for Google Drive?
   a. Google Drive
   b. AppData
   c. Program Files (x86)
   d. LogicalfileSet1
3. There are no PDF files in this Google Drive account. True or False?
4. How many Office files were recovered from this account?

a. 1

b. 18

c. 39

d. 60

5. When was the ademco.jpg file modified?

a. 22 Jun 2009 12:33:31 GMT

b. 21 May 2015 14:18:55 GMT

c. 20 May 2015 03:18:34 GMT

d. 03 Mar 2003 19:28:22 GMT

Lab 13.3. Examining OneDrive Cloud Storage

Objectives

After completing this lab, you will be able to:

- Describe the OneDrive files of interest to forensics investigators
- Search OneDrive for information on user accounts and file transactions

The OneDrive cloud service is included in Windows installations. The OneDrive user account used in this lab was recovered from the same computer as the one in **Labs 13.1** and 13.2. However, because criminals might not use the same cloud service for all transactions, examining files to look for evidence of other cloud services can be useful. OneDrive stores information about file transactions in the SyncDiagnostics.log file. The SyncEngine files (with an .etl extension) manage synchronization between OneDrive and a user's computer. In addition, the ONEDRIVESETUP.EXE-*nnnnnnn*.pf prefetch file can be useful for finding client-linked folders storing documents and paths that tie the computer to a OneDrive cloud account. In this lab, you process a OneDrive account folder to look for evidence on usernames and file transactions.

Tip

You might find OneDrive folders and files listed as SkyDrive in older Windows versions. Searching for both names is best to make sure no information is overlooked.

Materials Required

This lab requires the following:

- Windows
- Autopsy 4.3.0
- The OneDrive account folder from Data Files

Estimated completion time: 30–60 minutes

Activity

In this lab, you examine a OneDrive account to look for evidence on usernames and file transactions:

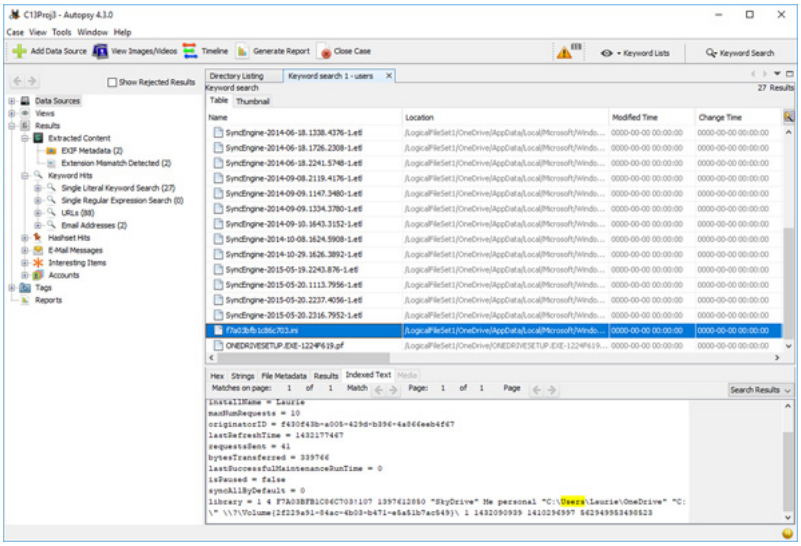
1. Start Autopsy. In the Welcome window, click **Create New Case**.

2. In the New Case Information window, type **C13Proj3** in the Case Name text box, and then click **Next**. In the Additional Information window, type **C13Proj3** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

3. In the Select Data Source window, click the **Select data source type** down arrow, click **Logical Files**, and then click **Add**. Click the **Browse** button, navigate to and click your work folder, click the **OneDrive** folder, click **Open**, and then click **Next**. In the Configure Ingest Modules window, click **Next** to accept the default modules, and then click **Finish**.

4. Click **Keyword Search** at the upper right, type **users** in the text box, and then click **Search** to look for the username information associated with this OneDrive account. Click the **f7a03bfb1c86c703.ini** file in the Result Viewer pane to view the username for this OneDrive account (see Figure 13-5). Click the **ONEDRIVESETUP.EXE-1224F619.pf** prefetch file to see the folders, system files, and paths linked with this OneDrive account.

Figure 13-5.

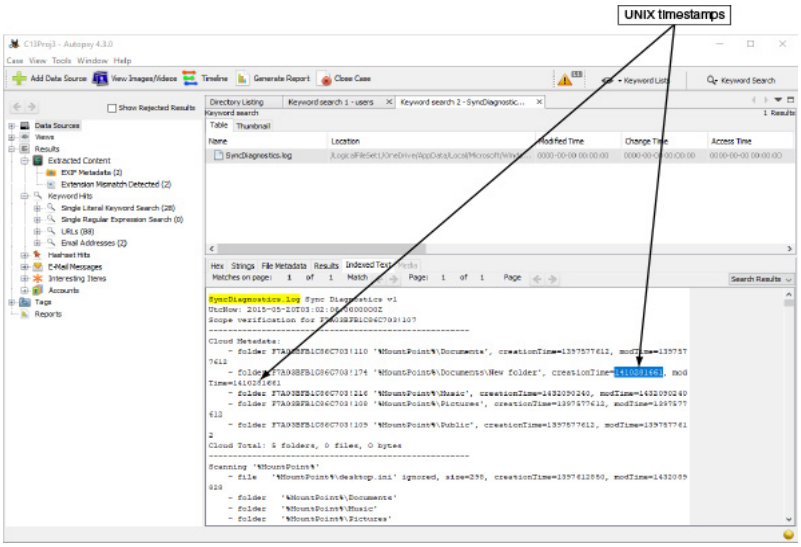


Source: www.sleuthkit.org

Viewing OneDrive search results

5. Click **Keyword Search** at the upper right, type **SyncDiagnostics.log** in the text box, and then click **Search**. Click the **Table** tab, if necessary, in the Result Viewer pane. Click the **SyncDiagnostics.log** file, and then click the **Indexed Text** tab, if necessary, in the Content Viewer pane to see additional metadata about folder transactions associated with this OneDrive account (see Figure 13-6).

Figure 13-6.



Source: www.sleuthkit.org

Information in the SyncDiagnostics.log file

Tip

In **Figure 13-6**, the Cloud Metadata section of the Content Viewer pane contains a list of folders, such as '%MountPoint%\Documents', followed with timestamps for creationTime=*nnnnnnnnnn* and modTime=*nnnnnnnnnn* . They're UNIX timestamps; see the Tip after Step 11 in Lab 13-2 for information on converting these values to a human-readable format.

6. In the left pane, expand **Views**, **File Types**, and **By Extension**, and click **Documents**. Click the **Table** tab in the Result Viewer pane, if necessary, to see the documents stored in the cloud.

7. Leave Autopsy open as you answer the following review questions. When you're finished, exit Autopsy.

Review Questions

1. How many Office documents were recovered from this OneDrive account?

   2

   5

   10

   0

2. How many JPEG files were recovered from this OneDrive account?

   28

   10

   27

   9

3. How many SyncEngine files are in this OneDrive account? (*Hint*: Use the Keyword Search function.)

1

25

27

28

4. According to the f7a03bfb1c86c703.ini file, how many users are listed for this OneDrive account?

1

2

5

6

5. Which file stores information about OneDrive file transactions?

SkyDriveApp-2015-05-19.2252.1288-1.etl

ONEDRIVESETUP.EXE-1224F610.pf

f7a03bfb1c86c703.ini

SyncDiagnostics.log

Chapter 14. Report Writing for High-Tech Investigations

Labs included in this chapter:

Lab 14.1 Investigating Corporate Espionage

Lab 14.2 Adding Evidence to a Case

Lab 14.3 Preparing a Report

Note

Before starting these labs, create a subfolder of your work folder named Ch14.

Lab 14.1. Investigating Corporate Espionage

Objectives

After completing this lab, you will be able to:

- Search for evidence in preparation for a criminal case
- Use Autopsy search tools to find e-mail evidence

Billions of dollars are lost each year to foreign competitors through economic espionage, usually involving employees attempting to make fast cash by selling trade secrets (www.fbi.gov/investigate/counterintelligence#Economic-Espionage). A patent search company called m57.biz specializes in researching patents before the U.S. Patent Office grants them. Charlie Brown, an employee of this company, is suspected of selling patent information to an outside competitor, and private investigators have been asked to conduct a search of his desktop computer. The responding investigator made a forensic image of Charlie's desktop computer and photographed his desk and work area. The investigator has given you this forensic image, and your supervisor asked you to search for any correspondence with potential evidence of economic espionage. In the investigator's photos of Charlie's work area, you noticed a sticky note with the word "Project2400" written on it.

Like other commercial forensics tools, Autopsy has a report generator that displays evidence found in a forensic image or on a drive. Report generators can produce files in HTML, Excel, and other formats, such as Rich Text Format (.rtf) and Comma Separated Values (.csv). As handy as report generators are, they typically include more information than needed to identify evidence, which can make displaying your findings in an easy-to-read format difficult. However, in Autopsy, you can display evidence in a text form that's easy to copy and paste into other applications, such as Notepad, Word, or Excel.

Materials Required

This lab requires the following:

- Windows
- Autopsy 4.7.0
- Microsoft Word (or open-source office software)
- The charlie-2009-12-11.E01 and charlie-work-usb-2009-12-11.E01 files, downloaded to your work folder in Step 1

Estimated completion time: 180–240 minutes, depending on your computer's performance

Caution

These files could take up to 4 hours to process, depending on your computer's performance, so you might want to set this lab up to run overnight.

Activity

In this lab, you search the forensic image of Charlie Brown's computer for evidence of corporate espionage, and then copy this evidence to a Word document to create a final report:

1. Start a Web browser, and go to http://downloads.digitalcorpora.org/corpora/scenarios/2009-m57-patents/drives-redacted/. Download the **charlie-2009-12-11.E01** and **charlie-work-usb-2009-12-11.E01** files to your work folder.

Note

The charlie-work-usb-2009-12-11.E01 file is used in Lab 14.2.

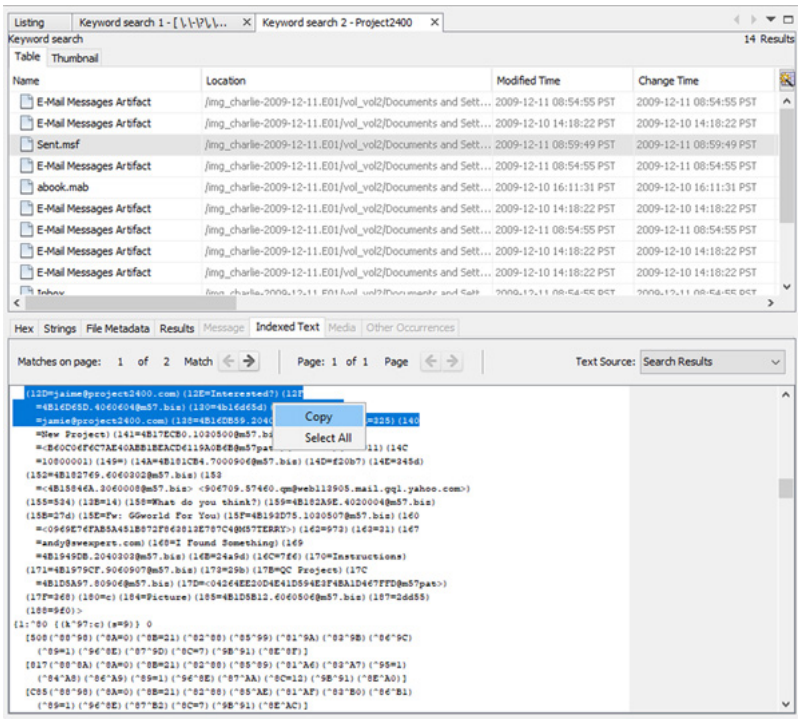
2. Start Autopsy. In the Welcome window, click the **Create New Case** button. In the New Case Information window, type **C14Proj1** in the Case Name text box. Click the **Browse** button next to the Base Directory text box, navigate to and click your work folder, click **Select** to enter this path, and then click **Next**. In the Additional Information window, type **C14Proj1** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

3. In the Select Data Source window, click **Disk Image or VM File** in the "Select data source type" list box, if necessary. Click **Browse**, navigate to and click your work folder, double-click the **charlie-2009-12-11.E01** file, and then click **Next**. Click **Next** to accept the default ingest modules, and then click **Finish** to begin processing the image.

4. When the processing is finished, click the **Keyword Lists** down arrow. Click the **Phone Numbers**, **IP Addresses**, **Email Addresses**, and **URLs** check boxes, and then click **Search**. The information that's returned could be useful in finding persons of interest who have been in contact with the suspect or Web sites that were visited to conduct research related to a crime.

5. Click **Keyword Search** at the upper right, click the **Exact Match** option button (if necessary) in the Keyword Search dialog box, type **Project2400** in the Keyword Search text box, and click the **Search** button. Examine each hit's data in the Content Viewer pane. After reviewing all the hits, click **Sent.msf** in the Result Viewer pane, and then select the first three lines displayed in the Content Viewer pane. Right-click this selection and click **Copy** (see Figure 14-1).

Figure 14-1.



Source: www.sleuthkit.org

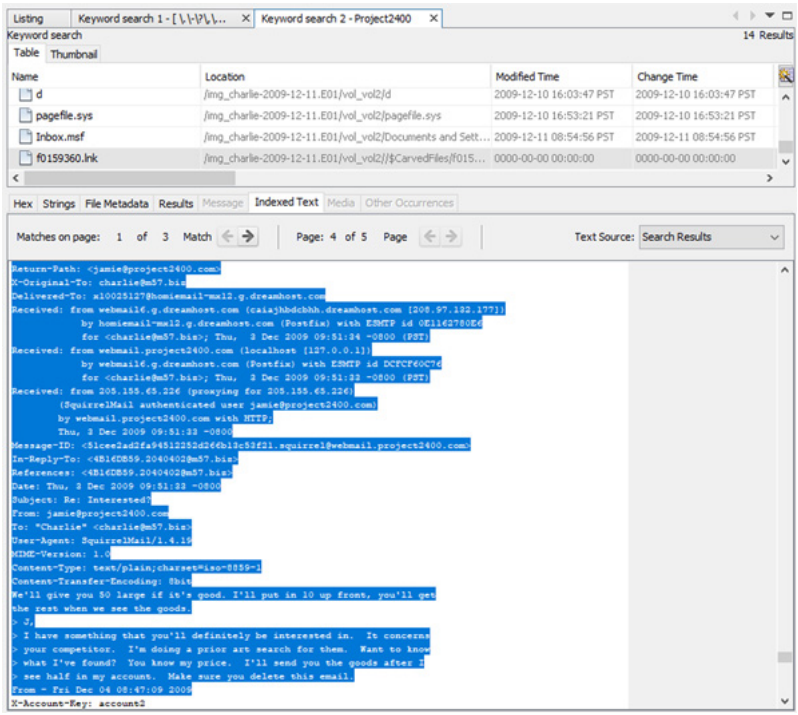
Collecting instances of the Project2400 keyword from the Sent.msf file

6. Start Microsoft Word, type **C14Proj1-Evidence** on the first line of a new document, press **Enter**, type **File: Sent.msf**, press **Enter** again, press **Ctrl+V** to paste the copied data from Autopsy, and press **Enter**. Click **File**, **Save As** from the menu. In the Save As dialog box, navigate to and click your ***Work*\C14Proj1\Export** folder, type **C14Proj1-Evidence-Collections** in the "File name" text box, and click **Save**. Leave this document open for subsequent steps.

7. In Autopsy, click **abook.mab** in the Result Viewer pane, and then select the first line displayed in the Content Viewer pane. Right-click this line and click **Copy**. In the Word document you created in Step 6, type **File: abook.mab** on the last line, press **Enter**, press **Ctrl+V**, and press **Enter**. Click **File**, **Save** from the menu, and leave this document open.

8. Scroll down the files in the Result Viewer pane, and click **f0159360.lnk** . Select the first 32 lines displayed in the Content Viewer pane (see Figure 14-2). Right-click this selection and click **Copy**. In the Word document, type **File: f0159360.lnk** on the last line, press **Enter**, press **Ctrl+V**, and press **Enter**. Click **File**, **Save** from the menu, and leave this document open.

Figure 14-2.



Source: www.sleuthkit.org

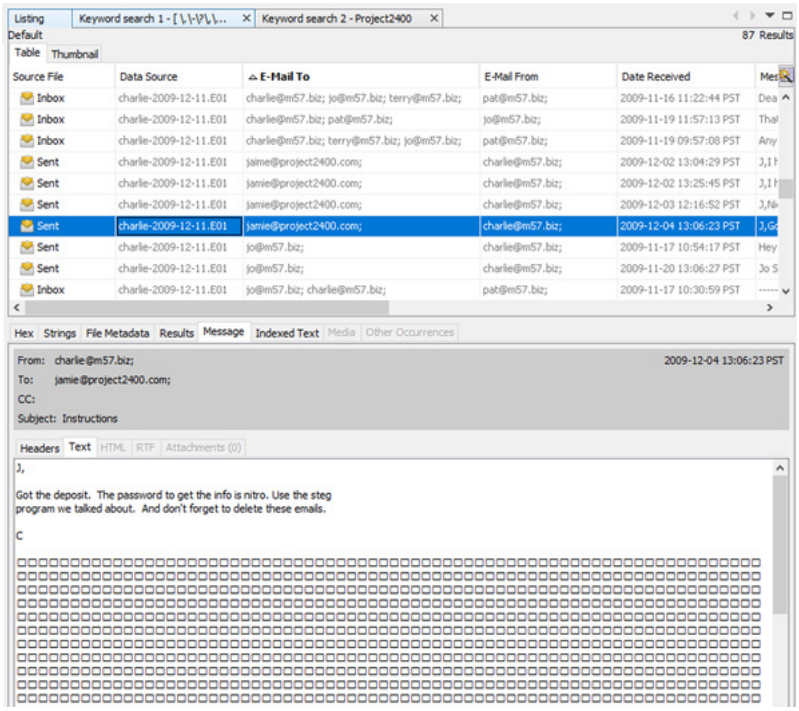
Selecting e-mail data

Note

There are two Project2400 e-mail accounts for Jamie. It's possible Jamie is using an alias e-mail address—jaime@project2400.com—in addition to the jamie@project2400.com address. (Notice that his first name is spelled two different ways in these addresses.) Criminals often use aliases to confuse forensics investigators or law enforcement agents.

9. Now that you've established Charlie and Jamie are communicating with each other, expand **E-Mail Messages** and **Default [Default]** in the left pane, and then click the **Default** folder to view all e-mails. Click the **E-Mail To** column header in the Result Viewer pane to sort e-mails by username, and find the e-mails sent to jamie@project2400.com and jaime@project2400.com. In the Default folder, notice there are two e-mails for each e-mail account. Based on the information in the last e-mail to jamie@project2400.com, Charlie has received a deposit and sent a password to Jamie for retrieving information stored in a password-protected steganography file (see Figure 14-3).

Figure 14-3.



Source: www.sleuthkit.org

Confirmation of a money transfer to Charlie

10. Click the **Results** tab in the Content Viewer pane. Right-click anywhere in this pane and click **Select All**. Right-click this selection again and click **Copy**. In the Word document, type **E-mail: Jamie@project2400.com** on the last line, press **Enter**, press **Ctrl+V**, and press **Enter**. Click **File**, **Save** from the menu, and leave this document open.

11. Click **Keyword Search** at the upper right, type **steganography**, click the **Exact Match** option button (if necessary), and click **Search** to find information on the steganography program Charlie mentioned in his e-mail to Jamie. Click the **_CACHE_003** file in the Result Viewer pane; this file stores the results of a Google search for "steganography freeware tools." Right-click **_CACHE_003** , point to **Tag Files**, and click **Tag and Comment**. In the Create Tag dialog box, click **New Tag**, type **Steg Program Information** in the Tag Name text box, click the **Tag indicates item is notable** check box, and click **OK** twice to bookmark this file.

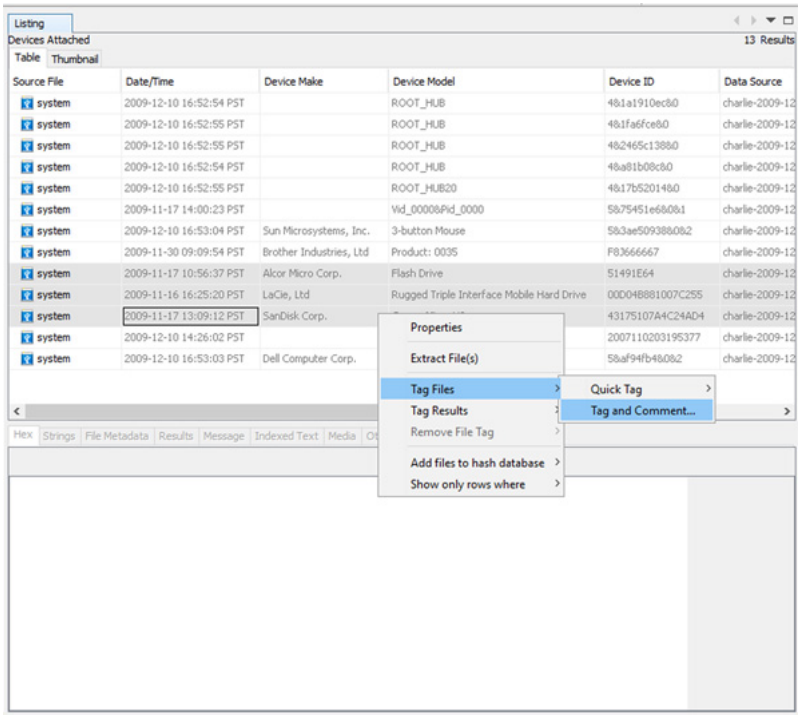
12. In the left pane, click to expand **Results** and **Extracted Content**, if necessary, and click the **Web Search** folder to see whether any other search terms were used to find free steganography tools. Scroll down the Result Viewer pane to find a search for "steganography tool free" in the Text column. Right-click **steganography tool free**, point to **Tag Files**, and click **Tag and Comment**. In the Create Tag dialog box, click **New Tag**, type **Google Searches for Steg Programs**, click the **Tag indicates item is notable** check box, and click **OK** twice.

13. Right-click anywhere in the Content Viewer pane and click **Select All**. Right-click this selection again and click **Copy**. In the Word document, type **Web Searches: Steg** on the last line, press **Enter**, press **Ctrl+V**, and press **Enter** again. Click **File**, **Save** from the menu, and leave this document open.

14. In the left pane, expand **E-Mail Messages**, and then click **Devices Attached** to look for any attached storage devices. You see that Charlie attached an Alcor Micro Corp. flash drive, a SanDisk Corp. Cruzer Micro U3 device, and a Lacie, Ltd mobile hard drive to

his computer. Shift+click all three devices in the Result Viewer pane, and then right-click this selection, point to **Tag Files**, and click **Tag and Comment** (see Figure 14-4). In the Create Tag dialog box, click **New Tag**, type **External Storage Devices** in the Tag Name text box, click the **Tag indicates item is notable** check box, and click **OK** twice.

Figure 14-4.



Source: www.sleuthkit.org

Tagging external storage devices

15. Leave Autopsy and Word open as you answer the following review questions. When you're finished, leave Autopsy running for the following labs, save the Word file, and exit Word.

Review Questions

1. When did Charlie send a password to Jamie?
   a. 2009-11-19
   b. 2009-12-02
   c. 2009-12-03
   d. 2009-12-04
2. When did Charlie do a search for steganography programs?
   a. 2009-11-19
   b. 2009-12-02
   c. 2009-12-03
   d. 2009-12-04
3. Report generators can produce files only in HTML or Excel format. True or False?
4. How many e-mails did Charlie send to Jamie's jamie@project2400.com e-mail account?
   2

4

13

6

5. Which of the following .exe files in the Web Downloads folder is a steganography tool? (*Hint*: Do an online search to find information on these files.)

FoxitReader31_url_Setup_1030.exe

QuickTimeInstaller.exe

invsect2.exe

7z465.exe

Lab 14.2. Adding Evidence to a Case

Objectives

After completing this lab, you will be able to:

- Add new evidence to an existing case
- Search for evidence common to more than one device

During a subsequent search of Charlie Brown's desk, an investigator found a USB drive and submitted it for forensic analysis to see whether it contains any evidence indicating Charlie was involved in selling information to competitors. Normally, you process all digital evidence that's recovered at the same time. However, you had already processed the image of Charlie's hard drive, so now you need to add this recently discovered device to the existing case.

Materials Required

This lab requires the following:

- Windows
- Autopsy 4.7.0
- The charlie-work-usb-2009-12-11.E01 file, downloaded in Lab 14.1

Estimated completion time: 30–60 minutes

Activity

In this lab, you add an image of a USB drive to the evidence recovered earlier from Charlie's desk:

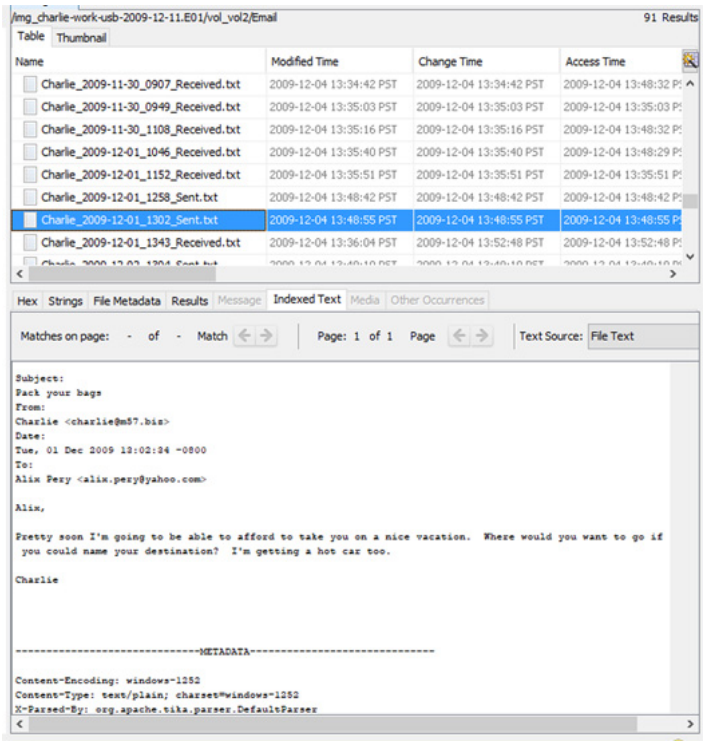
1. If necessary, start Autopsy, and click **Open Recent Case**. Click the **C14Proj1** case name, and then click **OK** to load the case.

2. Click the **Add Data Source** button, click **Browse**, click the **charlie-work-usb-2009-12-11.E01** file, click **Open**, and then click **Next**. Click **Next** to accept the default ingest modules, and then click **Finish** to add the image of the USB device.

3. When the image has finished processing, expand **charlie-work-usb-2009-12-11.E01** and **vol2 (NTFS/exFAT (0x07): 1-1059061248)** in the left pane, and then click the **E-mail Messages** folder. This folder contains the backup of Charlie's e-mails from November 16, 2009, to December 4, 2009, and all the e-mails were copied to the USB drive from December 3 to December 4, 2009. Scroll down the Result Viewer pane, and click the **Charlie_2009-12-01_1302_Sent.txt** file. The message shown in the Content Viewer pane

was sent from Charlie to Alix and says that he'll be able to afford a nice vacation soon (see Figure 14-5).

Figure 14-5.



Source: www.sleuthkit.org

Viewing the e-mail to Alix

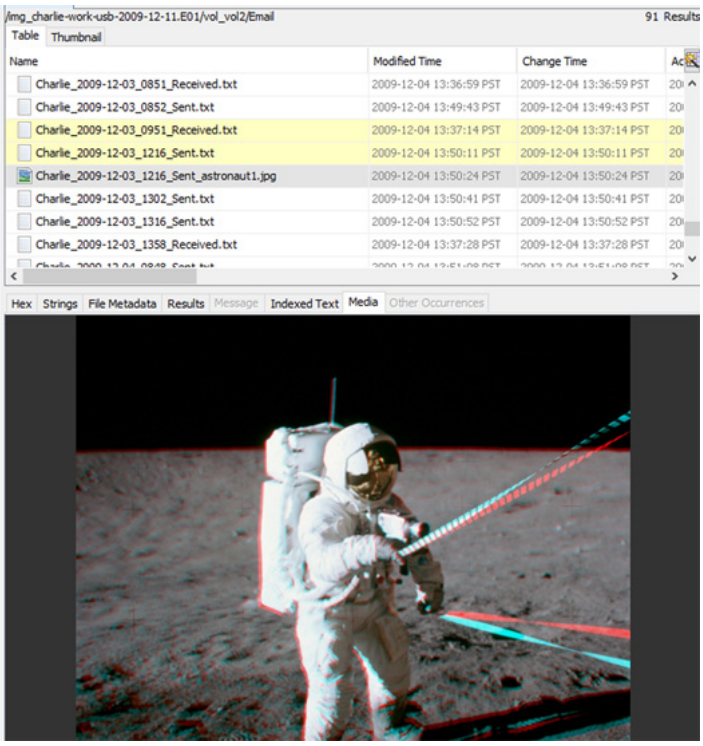
4. Click the **Charlie_2009-12-02_1304_Sent.txt** file in the Result Viewer pane to see the first e-mail to Jamie offering information for money. Obviously, Charlie wants this e-mail deleted after Jamie reads it. Right-click the file, point to **Tag Files**, and click **Tag and Comment**. In the Create Tag dialog box, click **New Tag**, type **USB Backup of Charlie's E-mail** in the Tag Name text box, click the **Tag indicates item is notable** check box, and click **OK** twice to bookmark this file.

5. Scroll down the Result Viewer pane, and click the **Charlie_2009-12-03_0951_Received.txt** file, which is the e-mail from Jamie offering Charlie "50 large" if the file is good. Right-click the file, point to **Tag Files**, and click **Quick Tag**. In the Quick Tag list, click **USB Backup of Charlie's E-mail** to add it to the bookmarked files.

6. Click the **Charlie_2009-12-03_1216_Sent.txt** file to see the e-mail Charlie sent to Jamie with the file he sold attached. Right-click the file, point to **Tag Files**, and click **Quick Tag**. In the Quick Tag list, click **USB Backup of Charlie's E-mail** to add it to the bookmarked files.

7. Click the next file in the Result Viewer pane, **Charlie_2009-12-03_1216_Sent_astronaut1.jpg** , which contains the astronaut1.jpg file attached to the previous e-mail, as denoted by the same timestamp (see Figure 14-6). Shift+click both e-mails and the attached JPG file, and then right-click this selection, point to **Tag Files**, and click **Tag and Comment**. In the Create Tag dialog box, click **New Tag**, type **File Transferred to Jamie** in the Tag Name text box, click the **Tag indicates item is notable** check box, and click **OK** twice.

Figure 14-6.

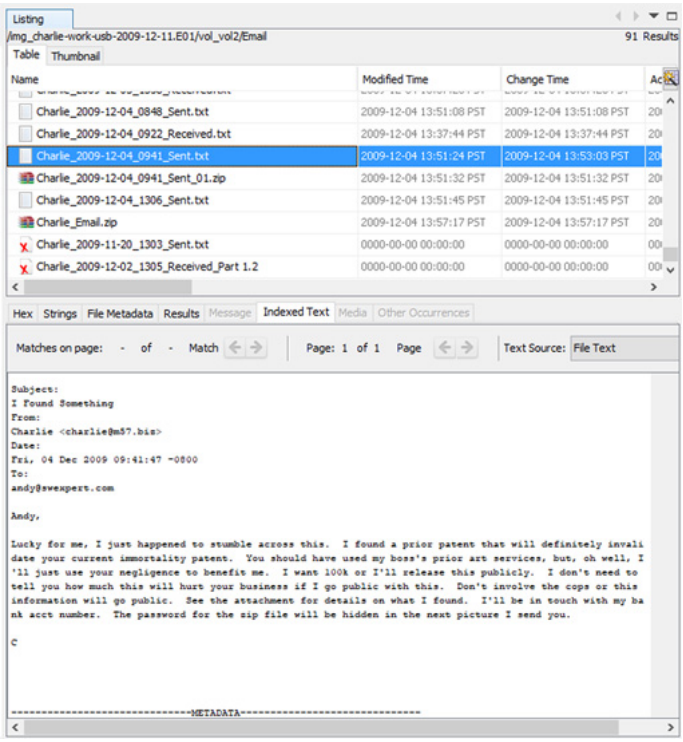


Source: www.sleuthkit.org

Viewing the file transferred to Jamie

8. Click the remaining e-mails to find any other incriminating messages. Click the **Charlie_2009-12-04_0941_Sent.txt** file to see an e-mail to Andy that's blackmailing him for $100,000 on a pending patent. Figure 14-7 shows the results. It seems to be another unrelated act of economic espionage involving Charlie. The next file contains the zipped file Charlie sent Andy.

Figure 14-7.



Source: www.sleuthkit.org

Viewing the blackmail e-mail

9. Click the **Charlie_2009-12-04_1306_Sent.txt** file to see Charlie's response to Jamie; it acknowledges that he received the money and gives Jamie the password to unlock the file. Again, Charlie asks Jamie to delete the e-mail. Shift+click the **Charlie_2009-12-04_0941_Sent.txt** , **Charlie_2009-12-04_1306_Sent.txt** , and **Charlie_2009-12-04_0941_Sent_01.zip** files. Right-click this selection, point to **Tag Files**, and click **Tag and Comment**. In the Create Tag dialog box, click **New Tag**, type **New Blackmail Evidence** in the Tag Name text box, click the **Tag indicates item is notable** check box, and click **OK** twice.

10. Leave Autopsy open as you answer the following review questions. When you're finished, leave Autopsy running for the next lab.

Review Questions

1. When did Charlie first approach Jamie to offer competitor information?
    a. 2009-11-19
    b. 2009-12-02
    c. 2009-12-03
    d. 2009-12-04
2. What's the password for the steganography file Charlie sent to Jamie?
    a. project2400
    b. m57
    c. nitro
    d. None
3. What's the domain name in Andy's e-mail address?

a. project.com

b. m57.biz

c. project2400.com

d. swexpert.com

4. What's the name of the file Charlie sent Jamie?

a. astronaut1.jpg

b. astronaut.jpg

c. astronaut1.png

d. astronaut.bmp

5. Charlie sent Andy a password via e-mail. True or False?

Lab 14.3. Preparing a Report

Objectives

After completing this lab, you will be able to:

> - Generate a report on the results of a forensic analysis
> - Find information in an HTML report

Now that you have processed images of Charlie's hard drive and USB drive, you need to generate a report for the owner of m57.biz. This report helps you prepare for meeting with the owner and supports your investigation's findings.

Materials Required

This lab requires the following:

- Windows
- Microsoft Word and Excel (or open-source office software)
- Autopsy 4.7.0

> Estimated completion time: 15–30 minutes

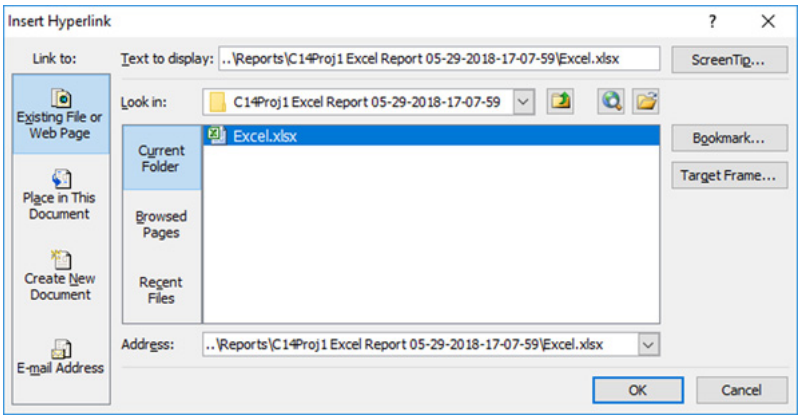
Activity

In this lab, you generate a report with the bookmarked files you added in **Labs 14.1** and 14.2 and review the results:

1. If necessary, start Autopsy, and click **Open Recent Case**. Click the **C14Proj1** case name, and then click **Open** to load the case.
2. Click **Tools, Generate Report** from the menu. In the Generate Report window, click the **Excel Report** option button, and then click **Next**.
3. In the Configure Artifact Reports window, click the **All Results** option button, and then click **Finish**. When the report is finished, click the **Excel Report** pathname in the Report Generation Progress window.
4. In File Explorer, navigate to your ***Work*\C14Proj1\Export** folder, and double-click **C14Proj1-Evidence-Collections.docx** to open it in Word. Scroll down and click the last line in the document, and then click **Insert**, **Hyperlink** from the menu. In the Insert Hyperlink dialog box, click the **Up On Folder** icon, double-click the **Reports** folder, double-

click **C14Proj1 Excel Report 05-29-2018-17-07-59\Excel.xlsx** (although your filename will show the current date), and then double-click **Excel.xlsx** (see Figure 14-8).

Figure 14-8.



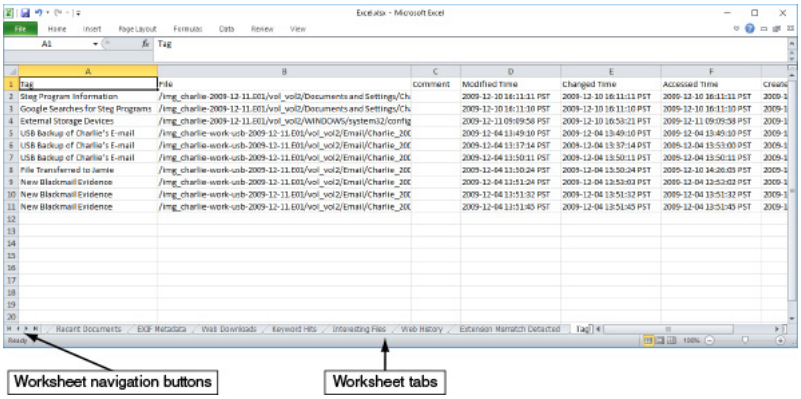
Source: www.sleuthkit.org

Inserting a hyperlink into Word

5. In Word, Ctrl+click the ..**Reports\C14Proj1 Excel Report 05-29-2018-17-07-59\Excel.xlsx** link to open the Excel report file.

6. In Excel, click the **right arrow** icon at the lower left. (Figure 14-9 points out these worksheet navigation icons.) Scroll to the right, click the **Tagged Files** worksheet tab, and review the timestamps, file sizes, and MD5 hashes in the Excel report.

Figure 14-9.

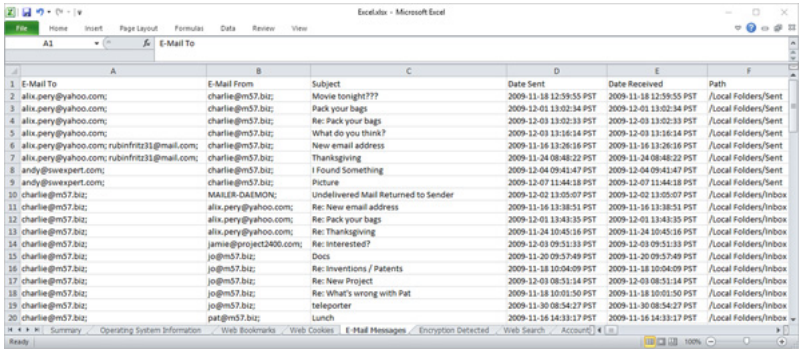


Source: www.sleuthkit.org

Finding the Tagged Files worksheet

7. In Excel, click the **left arrow** icon at the lower left. Scroll to the left, click the **E-Mail Messages** worksheet tab, and review the to and from addresses, subjects, timestamps, and locations on the storage device.

Figure 14-10.



	A	B	C	D	E	F
1	E-Mail To	E-Mail From	Subject	Date Sent	Date Received	Path
2	alix.pery@yahoo.com;	charlie@m57.biz;	Movie tonight???	2009-11-18 12:59:55 PST	2009-11-18 12:59:55 PST	/Local Folders/Sent
3	alix.pery@yahoo.com;	charlie@m57.biz;	Pack your bags	2009-12-01 13:02:34 PST	2009-12-01 13:02:34 PST	/Local Folders/Sent
4	alix.pery@yahoo.com;	charlie@m57.biz;	Re: Pack your bags	2009-12-03 13:02:33 PST	2009-12-03 13:02:33 PST	/Local Folders/Sent
5	alix.pery@yahoo.com;	charlie@m57.biz;	What do you think?	2009-12-03 13:16:14 PST	2009-12-03 13:16:14 PST	/Local Folders/Sent
6	alix.pery@yahoo.com; rubinfritz31@mail.com;	charlie@m57.biz;	New email address	2009-11-16 13:26:16 PST	2009-11-16 13:26:16 PST	/Local Folders/Sent
7	alix.pery@yahoo.com; rubinfritz31@mail.com;	charlie@m57.biz;	Thanksgiving	2009-11-24 08:48:22 PST	2009-11-24 08:48:22 PST	/Local Folders/Sent
8	andy@swexpert.com;	charlie@m57.biz;	I Found Something	2009-12-04 09:41:47 PST	2009-12-04 09:41:47 PST	/Local Folders/Sent
9	andy@swexpert.com;	charlie@m57.biz;	Picture	2009-12-07 11:44:18 PST	2009-12-07 11:44:18 PST	/Local Folders/Sent
10	charlie@m57.biz;	MAILER-DAEMON;	Undelivered Mail Returned to Sender	2009-12-02 13:05:07 PST	2009-12-02 13:05:07 PST	/Local Folders/Inbox
11	charlie@m57.biz;	alix.pery@yahoo.com;	Re: New email address	2009-11-16 13:38:51 PST	2009-11-16 13:38:51 PST	/Local Folders/Inbox
12	charlie@m57.biz;	alix.pery@yahoo.com;	Re: Pack your bags	2009-12-01 13:43:35 PST	2009-12-01 13:43:35 PST	/Local Folders/Inbox
13	charlie@m57.biz;	alix.pery@yahoo.com;	Re: Thanksgiving	2009-11-24 10:45:16 PST	2009-11-24 10:45:16 PST	/Local Folders/Inbox
14	charlie@m57.biz;	jamie@project2400.com;	Re: Interested?	2009-12-03 09:51:33 PST	2009-12-03 09:51:33 PST	/Local Folders/Inbox
15	charlie@m57.biz;	jo@m57.biz;	Docs	2009-11-20 09:57:49 PST	2009-11-20 09:57:49 PST	/Local Folders/Inbox
16	charlie@m57.biz;	jo@m57.biz;	Re: Inventions / Patents	2009-11-18 10:04:09 PST	2009-11-18 10:04:09 PST	/Local Folders/Inbox
17	charlie@m57.biz;	jo@m57.biz;	Re: New Project	2009-12-03 08:51:14 PST	2009-12-03 08:51:14 PST	/Local Folders/Inbox
18	charlie@m57.biz;	jo@m57.biz;	Re: What's wrong with Pat	2009-11-18 10:01:50 PST	2009-11-18 10:01:50 PST	/Local Folders/Inbox
19	charlie@m57.biz;	jo@m57.biz;	teleporter	2009-11-30 08:54:27 PST	2009-11-30 08:54:27 PST	/Local Folders/Inbox
20	charlie@m57.biz;	pat@m57.biz;	Lunch	2009-11-16 14:33:17 PST	2009-11-16 14:33:17 PST	/Local Folders/Inbox

Source: www.sleuthkit.org

Displaying the E-Mail Messages worksheet

8. Leave the Autopsy report open as you answer the following review questions. When you're finished, exit Autopsy, Excel, and Word, and close all open windows.

Review Questions

1. Based on the Excel report's Web Search worksheet, how many times did Charlie search for information on steganography?
   a. 1
   b. 3
   c. 5
   d. 14
2. What OS was installed on Charlie's computer?
   a. Windows 10 Home, Service Pack 1
   b. Windows 8.1 Professional, Service Pack 3
   c. Windows 7 Server, Service Pack 2
   d. Windows XP, Service Pack 3
3. Based on the Excel report's Devices Attached worksheet, how many USB drives were attached to Charlie's computer?
   a. 3
   b. 6
   c. 7
   d. 13
4. Based on the Excel report's Encryption Detected worksheet, how many zipped file attachments did Autopsy detect?
   a. 1
   b. 2
   c. 9
   d. 12
5. What hex editor did Charlie install on his computer?
   a. Hex Workshop
   b. HxD

c. Cygnus Hex Editor FREE EDITION 1.00 v.1.00

d. WinHex

Chapter 15. Expert Testimony in Digital Investigations

Labs included in this chapter:

Lab 15.1 Conducting a Preliminary Investigation

Lab 15.2 Investigating an Arsonist

Lab 15.3 Recovering a Password from Password-Protected Files

Note

Before starting these labs, create a subfolder of your work folder named Ch15.

Lab 15.1. Conducting a Preliminary Investigation

Objectives

After completing this lab, you will be able to:

- Use FTK Imager Lite to conduct a preliminary investigation
- Export file hashes to validate recovered evidence

Arsonists often return to the scenes of fires they started and take photos to remember the event or gloat about their handiwork. Several years ago, the fire marshal determined that multiple fires near Roslyn and Winthrop were the work of an arsonist. This arsonist left notes signed "Trogdor the Burninator" that challenged the police to capture him before his next fire. The police believed the suspect was using a computer at a local company, Superior Bicycles, and had permission from the company's owner to examine the computer on site to determine whether there was any evidence on the hard drive. In this lab, you conduct a preliminary investigation of the hard drive image before getting a warrant to seize the computer.

Materials Required

This lab requires the following:

- Windows
- Microsoft Excel (or open-source spreadsheet software)
- FTK Imager Lite
- The GCFI-Bart_Jones.E01 file

Estimated completion time: 30–60 minutes

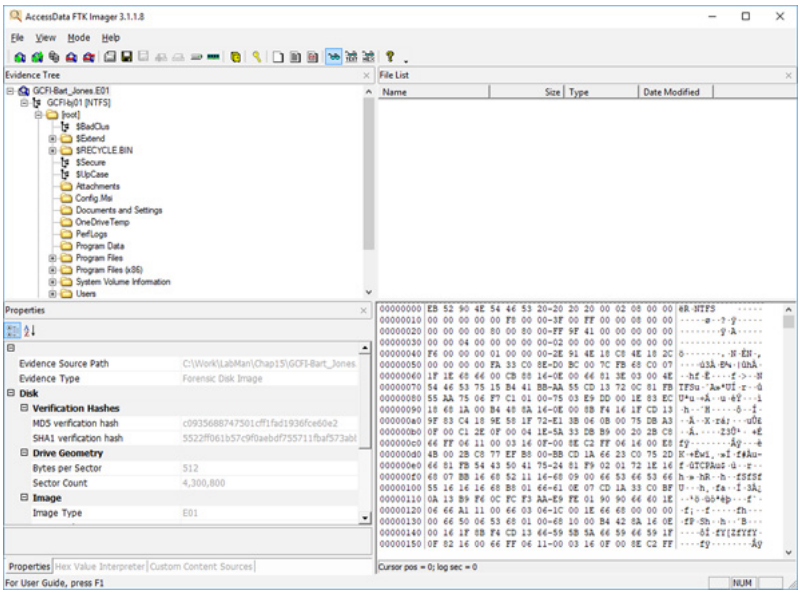
Activity

In this lab, you conduct a preliminary investigation of the GCFI-Bart_Jones.E01 image to look for potential evidence:

1. Start FTK Imager Lite, clicking **Yes** in the UAC message box, if necessary. Click **File**, **Add Evidence Item** from the menu.
2. In the Select Source dialog box, click the **Image File** option button, and then click **Next**.
3. In the Select File dialog box, click **Browse**, navigate to your work folder, click the **GCFI-Bart_Jones.E01** file, click **Open**, and then click **Finish** to add the image to FTK Imager Lite.
4.

In the Evidence Tree pane, expand **GCFI-Bart_Jones.E01** , **GCFI-bj01 [NTFS]**, and **[root]** to view the image (see Figure 15-1).

Figure 15-1.



Source: AccessData Group, Inc., www.accessdata.com

Viewing the image of the suspect hard drive

5. Right-click **GCFI-Bart_Jones.E01** in the Evidence Tree pane and click **Export Directory Listing**. Navigate to your work folder, type **Preliminary Search** in the "File name" text box, click **Save**, and click **Close** in the Creating Directory Listing [100%] dialog box to export the list of files.

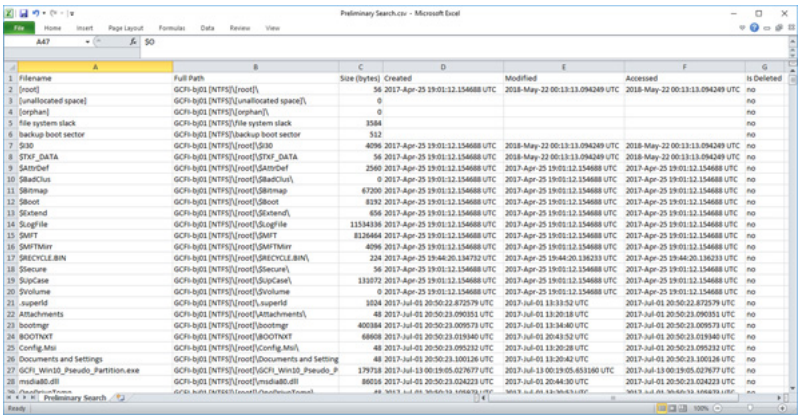
Note

FTK Imager Lite exports directory listings in the comma-separated values (CSV) format and automatically adds the .csv extension when you save the file.

6. Right-click **GCFI-bj01 [NTFS]** in the Evidence Tree pane and click **Export File Hash List**. In the Save As dialog box, type **Firestarter File Hashes** in the "File name" text box, and click **Save**.

7. In File Explorer, navigate to your work folder. Double-click the **Preliminary Search.csv** file to open it in Excel. This directory listing contains a list of filenames, their paths on the disk, and file attributes. Increase the width of columns **A** through **G**, as shown in Figure 15-2.

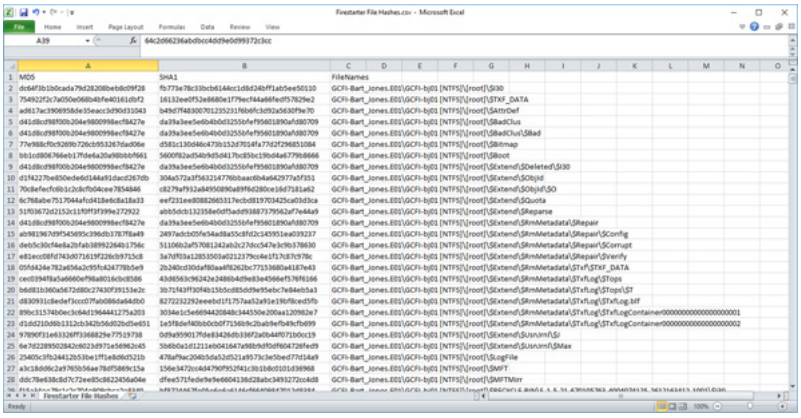
Figure 15-2.



Viewing the directory listing in a spreadsheet

8. Minimize this window. In File Explorer, double-click the **Firestarter File Hashes.csv** file in your work folder to open it in Excel. Increase the width of the **A** and **B** columns to view the entire hash signatures of files in the image (see Figure 15-3).

Figure 15-3.



Viewing file hashes in a spreadsheet

9. Leave the Excel files and FTK Imager Lite open as you answer the following review questions. When you're finished, exit FTK Imager Lite, but leave the two spreadsheet files open.

Review Questions

1. What's the volume serial number of the GCFI-Bart_Jones.E01 image?
   a. FIRESTARTER
   b. 2,056,257
   c. 184E-912E
   d. Can't be determined from the evidence
2. What date was the root folder in the GCFI-Bart_Jones.E01 image last accessed?
   a. 3/22/2009
   b. 4/25/2017
   c. 1/31/2004
   d. 5/22/2018

3. What deleted Office files were found in the GCFI-Bart_Jones.E01 image's RECYCLED BIN folder?
    a. !ATE1.XLS
    b. CV.DOC
    c. Burninator1.docx, Burninator2.doc, Burninator3.doc, and Burninator4.doc
    d. Special Project A-Victor-rev01.docx, Special Project A-Whiskey-rev01.docx, Special Project A-Xray-rev01.docx, Special Project A-Yankee-rev01.docx, and Special Project A-Zebra1-rev01.docx
4. What types of nonsystem files are in the RECYCLED BIN\Pleasure folder? (Choose all that apply.)
    a. .doc and .docx files
    b. .xls and .xlsx files
    c. .gif files
    d. .jpg files
5. Which two types of file hashes are included in the Firestarter File Hashes.csv file?

Lab 15.2. Investigating an Arsonist

Objectives

After completing this lab, you will be able to:

> - Search for evidence in preparation for a criminal case
> - Use Autopsy search tools to find evidence and create a report
> - Research artifacts to see whether they might of evidentiary value

After conducting a preliminary investigation, you have found the arsonist and the computer used to document his crimes. During your analysis of the GCFI-Bart_Jones.E01 file, you recovered images of fires in the RECYCLED BIN folder that seem to be plans to commit arson. You also found a folder named Lumbermill, which could indicate scenes of previous fires. In this lab, you use Autopsy to analyze the GCFI-Bart_Jones.E01 image and gather evidence to build a case. Your findings will be presented in a report to the criminal prosecuting attorney to use in the arson charges against Bart Jones. If the case goes to trial, you'll use the report in your testimony as an expert witness for the prosecution.

Materials Required

This lab requires the following:

- Windows
- Microsoft Notepad (or an open-source text editor)
- Autopsy 4.3.0
- The GCFI-Bart_Jones.E01 file from Lab 15.1

Estimated completion time: 90–120 minutes, depending on your computer's performance

Caution ⚠

This file could take a few hours to process, depending on your computer's performance, so you might want to set it up to process overnight.

Tip

When a newer version of Autopsy is installed, as you did in **Chapter 6**, Autopsy 4.3.0 might display an error message when you're configuring ingest modules. If this happens, and you want to continue using version 4.3.0 for this lab, try uninstalling all versions of Autopsy and then reinstalling version 4.3.0. If you want to use the latest version of Autopsy for this lab, it might have some differences that aren't shown in this lab.

Activity

In this lab, you process the GCFI-Bart_Jones.E01 image to find and tag evidence of arson and use it to generate a report to be submitted to the criminal prosecuting attorney office for review:

1. Start Autopsy. In the Welcome window, click **Create New Case**. In the New Case Information window, type **C15Proj2** in the Case Name text box. Click the **Browse** button next to the Base Directory text box, navigate to and click your work folder, click **Select** to enter this path, and then click **Next**. In the Additional Information window, type **C15Proj2** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

Tip

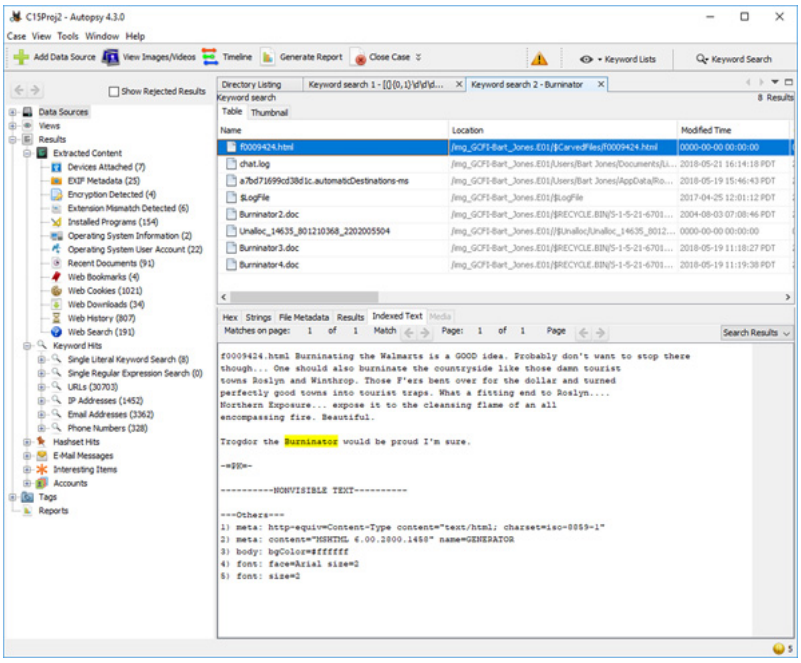
If you get an error message stating that Autopsy 4.3.0 is missing links, exit the program and reinstall it. In the Autopsy Installation Wizard, click the Repair button to correct this error.

2. In the Select Data Source window, click **Disk Image or VM File** in the "Select data source type" list box. Click **Browse**, navigate to and click your work folder, click the **GCFI-Bart_Jones.E01** file, click **Open**, and then click **Next**. In the Configure Ingest Modules window, click **Select All**, and then click to clear the **Virtual Machine Extraction**, **SmutDetect4Autopsy**, and **Android Analyzer** check boxes. Click **Next**, and then click **Finish**.

3. When the processing is finished, click the **Keyword Lists** down arrow. Click the **Phone Numbers**, **IP Addresses**, **Email Addresses**, and **URLs** check boxes, and then click **Search**. (The search takes about 20 minutes.)

4. Click **Keyword Search** at the upper right, click the **Exact Match** option button (if necessary), type **Burninator**, and click **Search**. Click the first file in the Result Viewer pane, **f0000944.html** , and notice that it's a recovered file that Autopsy has placed in the $CarvedFiles folder (see the Location column in Figure 15-4). In addition, because it's a carved file, no additional dates and timestamps are available for this file, and it can't be tagged as evidence.

Figure 15-4.



Source: www.sleuthkit.org

Finding incriminating text in a carved file

Tip

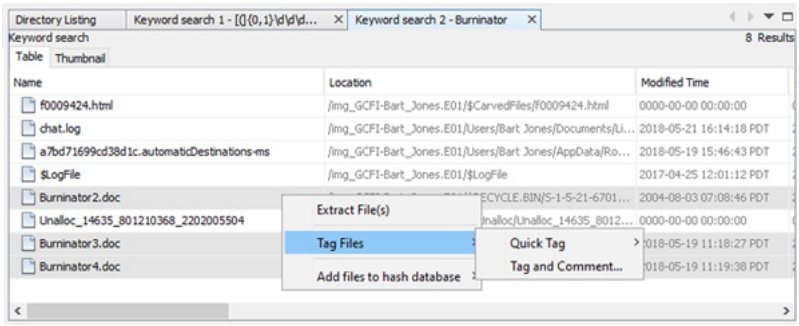
To collect carved data as evidence, select and copy the data in the Content Viewer pane and paste it into Notepad or Word. Then save the copied data as a separate file that can be included in a final report.

5. Click the **Strings** tab in the Content Viewer pane, click anywhere in the Content Viewer pane, and then press **Ctrl+A** to select all the text. Right-click this selection and click **Copy**. Start Notepad, and in a new document, click **Edit**, **Paste** from the menu. Click **File**, **Save As** from the menu, navigate to and click your work folder, type **f00009424.html** in the "File name" text box, and click **Save**. Exit Notepad.

6. Click the next file in the Result Viewer pane, **chat.log** . Notice that it contains a conversation between MasterBlastre and PhyreKing. Right-click **chat.log** , point to **Tag Files**, and click **Tag and Comment**. In the Create Tag dialog box, click the **New Tag Name** button. In the New Tag section, type **Burninator** in the Tag Name text box, and click **OK** twice.

7. Click and examine **Burninator2.doc** , **Burninator3.doc** , and **Burninator4.doc** . When you're finished, Ctrl+click these three files. Right-click this selection, point to **Tag Files** and **Quick Tag** (see Figure 15-5), and in the Quick Tag list, click **Burninator**.

Figure 15-5.

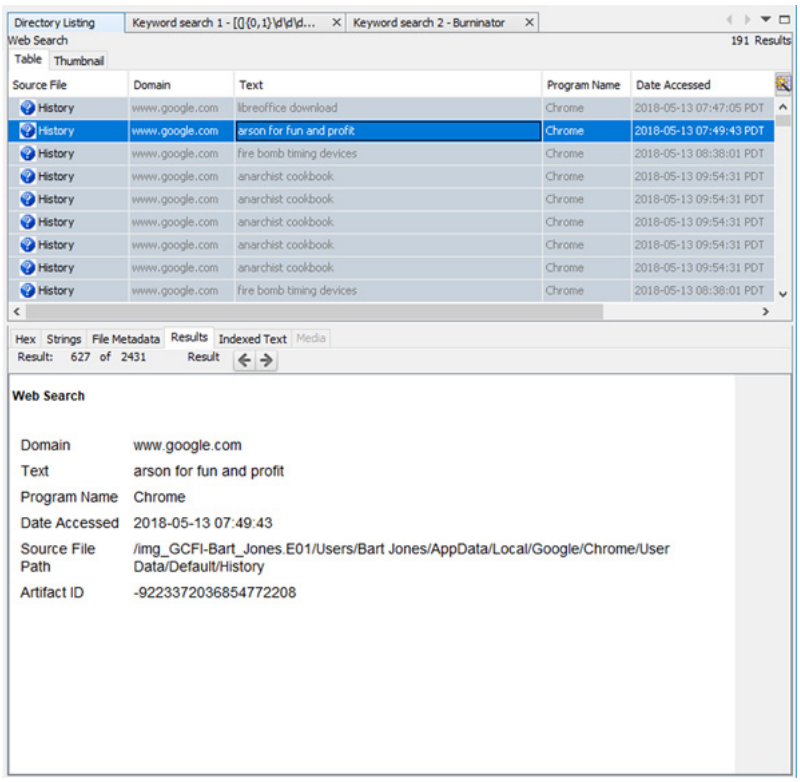


Source: www.sleuthkit.org

Tagging Burninator files

8. In the left pane, expand **Results** and **Extracted Content**, if necessary, and click the **Web Search** folder. In the Result Viewer pane, right-click "arson for fun and profit," the second item in the list (see Figure 15-6). Point to **Tag Files**, and click **Tag and Comment**. In the Create Tag dialog box, click the **New Tag Name** button. In the New Tag section, type **Web Searches** in the Tag Name text box, and click **OK** twice.

Figure 15-6.



Source: www.sleuthkit.org

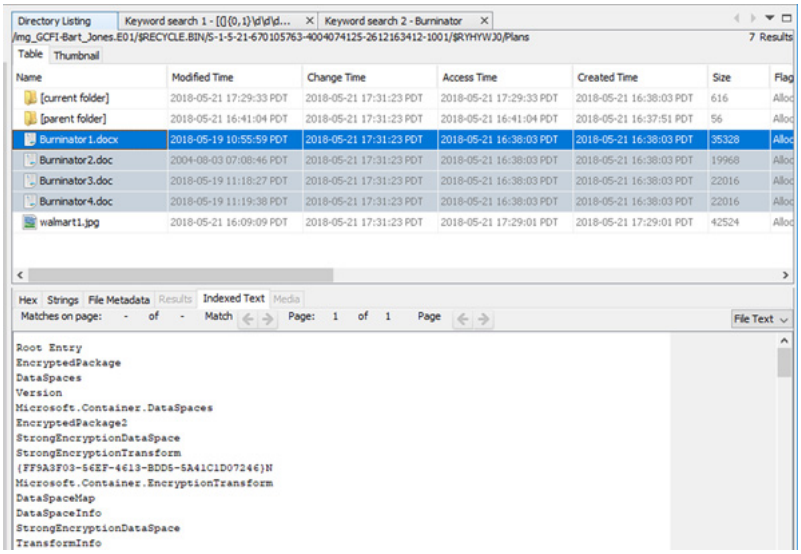
Tagging Web searches

9. In answering **Lab 15.1**'s review questions, you found several deleted files in the RECYCLED BIN folder. In the left pane, expand **Data Sources**, **GCFI-Bart_Jones.E01** , **$RECYCLED BIN**, **S-1-5-21-670105763-4004074125-26122163412-1001(198)**, and **$RYHYWJ0(13)**, and click the **Plans** folder. In the Result Viewer pane, the three Burninator files are grayed out, indicating that they've been tagged previously. Another file,

Burninator1.docx, has not been tagged. Right-click **Burninator1.docx** , point to **Tag Files** and **Quick Tag**, and in the Quick Tag list, click **Burninator**.

10. Click **Burninator1.docx** in the Result Viewer pane. In the Content Viewer pane, notice that the second line says "EncryptedPackage" (see Figure 15-7). Shift+click **Burninator4.doc** in the Result Viewer pane to select all the Burninator files. Right-click this selection and click **Extract File(s)**. In the Save dialog box, click **Save**, and then click **OK** in the information message box.

Figure 15-7.



Source: www.sleuthkit.org

Finding an encrypted Word file

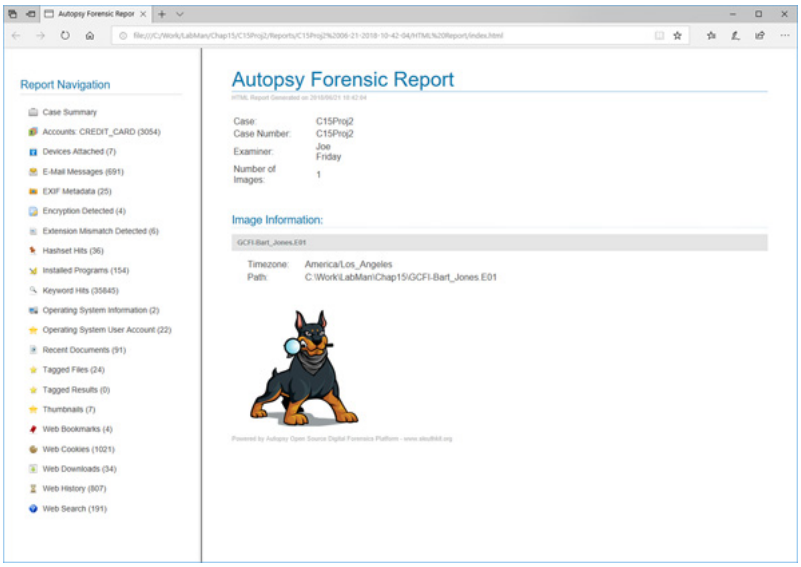
11. To find additional evidence of unsolved arson cases or to see whether Bob Jones had any interest in fires, click the **Favorites** folder in the left pane. In the Result Viewer pane, click **fire1.png** , scroll down, and Shift+click the last file, **fireF.png** . Right-click this selection, point to **Tag Files**, and click **Tag and Comment**. In the Create Tag dialog box, click the **New Tag Name** button. In the New Tag section, type **Possible Past Arson Incident** in the Tag Name text box, and then click **OK** twice.

12. In the left pane, expand the **Pleasure** folder, if necessary, and click the **Lumbermill** folder. In the Result Viewer pane, click **Gulf-Breeze_-Heart-Pine-Lumber-Mill_01.jpg.0.6.jpg** , scroll down, and Shift+click the last file, **Resolution%20Community%20Sawmill.jpg** . Right-click this selection, point to **Tag Files** and click **Quick Tag**, and in the Quick Tag list, click **Possible Past Arson Incident**.

13. In **Step 10**, you saw that the Burninator1.docx file's contents indicate it's an encrypted file. If necessary, expand the **Results** and **Extracted Content** folders in the left pane, and click the **Encryption Detected** folder. Click **Personal.zip** , and Shift+click the last of the three **testzip.zip** files. Right-click this selection and click **Extract File(s)**. In the Save dialog box, click **Save**, and then click **OK** in the information message box.

14. At this point, you've collected enough evidence. Click **Tools**, **Generate Report** from the menu. In the Generate Report window, click the **Results - HTML** option button, and then click **Next**. In the Configure Artifact Reports window, click **All Results**, if necessary, and then click **Finish**. A green checkmark is displayed in the progress bar when the report is finished. Click the **Results - HTML** pathname in the Report Generation Progress window to see the report (see Figure 15-8).

Figure 15-8.



Source: www.sleuthkit.org

Viewing the Autopsy report

15. Leave the Autopsy report open as you answer the following review questions. When you're finished, leave Autopsy running for the next lab.

Review Questions

1. What's the Modified Time value for the Burninator1.docx file contained in burner.zip?
   a. 2018-05-19 10:55:59 PDT
   b. 2018-05-21 17:31:23 PDT
   c. 2018-05-21 16:38:03 PDT
   d. 0000-00-00 00:00:00
2. No additional dates and timestamps are available for the f0000944.html file because it's an extracted file. True or False?
3. Based on the Web Search folder's contents, what topics were searched for on Bart Jones's computer? (Choose all that apply.)
   a. Nuclear bomb timer designs
   b. Insurance payout for fire damage
   c. Picric acid formula
   d. Fire bomb timing devices
4. You noticed the term "picric acid" in Web searches done from Bart Jones's computer. To see whether this information might be of evidentiary value to the case, do an online search. Which of the following explains the use of picric acid?
   a. Military explosives
   b. Burn treatment
   c. A fire suppressant
   d. Specialized plastic lubricant
5. The chat.log file contains messages from two people texting to each other. What is MasterBlastre's first name?
   a. Bart

b. Tom

c. Chris

d. Jim

Lab 15.3. Recovering a Password from Password-Protected Files

Objectives

After completing this lab, you will be able to:

- Collect additional evidence to prepare for testimony in a trial
- Determine whether a warning banner is displayed when logging on
- Recover passwords for password-protected files

After submitting the report from **Lab 15.2**, you get a message from the criminal prosecuting attorney asking for two additional items in the GCFI-Bart_Jones.E01 image. First, the attorney wants to confirm that the computer Bart Jones used at Superior Bicycles, Inc., has a warning banner in the Windows Registry legalnotice field stating that the user has no right of privacy. Second, he wants you to extract the data in the password-protected Personal.zip and Burninator1.docx files and determine what potential evidence they contain. With this information, the criminal prosecuting attorney plans to have you testify in a hearing that the computer used by Bart Jones has a warning banner displayed when a user logs on to it, and the computer had password-protected files containing additional evidence about the arson case.

This lab is divided into two sections: verifying that Bart Jones's computer displayed a warning banner when he logged on, and recovering a password from password-protected files.

Materials Required

This lab requires the following:

- Windows
- Autopsy 4.3.0
- Microsoft Word, Notepad, and Excel (or open-source office software)
- AccessData Registry Viewer
- KRyLack Software Free ZIP Password Recovery, installed in the second section
- The GCFI-Bart_Jones.E01 file from Lab 15.1

Estimated completion time: 45–90 minutes, depending on your computer's performance

Activity

Verifying the Existence of a Warning Banner

In this section, you use Autopsy and Registry Viewer to verify that the GCFI-Bart_Jones.E01 image contains a warning banner:

1. Start Autopsy, if necessary, and in the Welcome window, click **Open Recent Case**. If you left Autopsy running, click **Case**, **Open Recent Case** from the menu. In the Open Recent Case dialog box, click **C15Proj2**, and then click **Open**.

2. In the left pane, expand **Data Sources**, **GCFI-Bart_Jones.E01** , **Windows**, and **System32**, and click the **Config** folder. Scroll down the Result Viewer pane, and then

right-click **SOFTWARE** and click **Extract File(s)**. In the Save dialog box, navigate to and click your work folder, click **Save**, and click **OK**. Leave Autopsy running for the next section.

3. Start Registry Viewer. If you get an error message, click **No** to run the program in demo mode, and click **OK** in the "No dongle found" message box. Click **File**, **Open** from the menu, navigate to and click ***Work*\C15Proj2\Export** folder, click **SOFTWARE**, and then click **Open**.

4. In the tree view on the left, scroll down and expand **Microsoft**, **Windows**, **CurrentVersion**, **Policies**, and **System**. In the list of Registry keys at the upper right, click the **legalnoticetext** key. Right-click the hexadecimal data in the lower-right pane and click **Select All**. Right-click this selection and click **Copy unicode**.

5. Open a new document in Notepad, and click **Edit**, **Paste** from the menu. Click **File**, **Save As** from the menu, navigate to and click your work folder, and type **LegalNoticeText** in the "File name" text box. Click **Save**, and exit Notepad and Registry Viewer.

Recovering a Password from Password-Protected Files

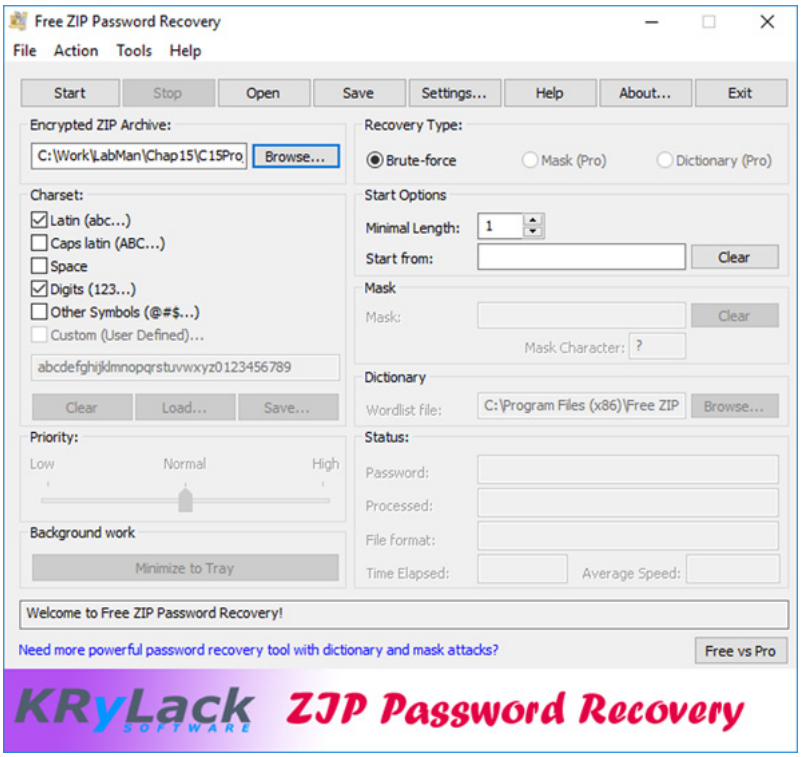
In this section, you use Autopsy and Free ZIP Password Recovery to recover the password for Personal.zip, and then search this file for possible passwords for Burninator1.docx so that you can present its contents to the criminal prosecuting attorney:

1. In File Explorer, create a subfolder of your work folder called **Krylack**. Start a Web browser, and go to www.krylack.com/free-zip-password-recovery/. Download the installation file for Free ZIP Password Recovery to your ***Work*\Krylack** folder.

2. In File Explorer, navigate to the ***Work*\Krylack** folder and double-click **free-zip-password-recovery.exe** . In the Welcome window, click **Next**, and then click **Install** in the Select Installation Folder window. In the Completing the Free ZIP Password Recovery Setup Wizard window, click the **Launch Free ZIP Password Recovery** check box, if necessary, and then click **Finish**.

3. In the Free ZIP Password Recovery window, click **Browse** next to the Encrypted ZIP Archive text box. In the Open Encrypted File dialog box, navigate to ***Work*\C15Proj2\Export**, and double-click **Personal.zip** . In the Charset section, click the **Latin (abc...)** and **Digits (123...)** check boxes (see Figure 15-9). In the Recovery Type section, click the **Brute-force** option button, if necessary, and in the Start Options section, click the **Minimal Length** up arrow to enter **8**, and then click the **Start** button at the top.

Figure 15-9.



Source: Serhiy Horobets, www.krylack.com

Recovering a password from a zipped file

4. When the password recovery is finished, click **Copy** and then **Close** in the Password Recovered dialog box. In File Explorer, navigate to the ***Work*\C15Proj1\Export** folder, and click **Personal.zip** . Click the **Extract** tab, and click the **Extract all** icon. Click the **Extract** button in the Extract Compressed (Zipped) Folders dialog box. Click the **Password** text box and press **Ctrl+V**, and then click **OK** in the "Password needed" dialog box to open the file.

5. When all files in Personal.zip have been extracted, a new File Explorer window opens. In the right pane, double-click the **Personal** folder, and then open and examine the contents of **Profit&Loss.ods** , **Shopping-List.ods** , and **temp.txt** . Leave all these files open so that you can refer to them in the Review Questions section at the end of this lab.

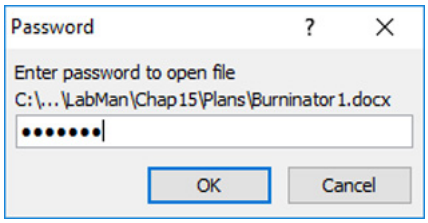
Note

For the purposes of this lab, the password for Personal.zip is very simple, but keep in mind that the longer and more complex a password is, the longer password-recovery tools take to recover it. Complex passwords including lowercase and uppercase letters, numbers, spaces, and symbols can take several days or weeks to recover.

6. In File Explorer, double-click the **temp.txt** file to open it in Notepad. This file contains 10 lines of text, and it's possible one of these lines could be the password for Burninator1.docx in the Plans subfolder.

7. Double-click the **Plans** subfolder and then **Burninator1.docx** . If you're prompted for a password, refer to temp.txt to see whether one of the words listed in it open the file. For example, in the Password dialog box, type **00000000**, the first line in temp.txt (see Figure 15-10), and then click **OK**.

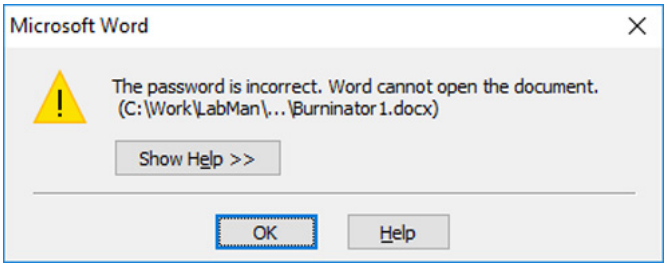
Figure 15-10.



Entering the password to open Burninator1.docx

8. If an error message is displayed (see **Figure 15-11**), click **OK** and repeat the procedure in Step 7 with the next possible password from temp.txt. When you have opened the Burninator1.docx file in Word, review its contents and leave it open for the Review Questions.

Figure 15-11.



Error message that's displayed when using the wrong password

9. After opening Burninator1.docx, review the contents of the **Favorites** and **My Research** folders. Note the type of files in each of these folders.

10. In the left pane of Autopsy, expand the **Results** folder, and click the **Installed Programs** folder. In the Result Viewer pane, click the **Program Name** column header to sort installed programs alphabetically. Scroll down the list of programs to see whether any might be capable of hiding information or password-protecting files. (*Note*: Online research can be useful in this process.) Make a note of each program you suspect is capable of these functions; this information could be used as part of your testimony for a hearing.

11. Leave Autopsy and Word open as you answer the following review questions. When you're finished, exit Autopsy, Word, Notepad, and Free ZIP Password Recovery.

Review Questions

1. The Personal.zip file in the \Users\Bart Jones\Documents path contains which of the following LibreOffice documents? (Choose all that apply.)
   a. Checklist.odt
   b. Profit&Loss.ods
   c. Shopping-List.ods
   d. CV.DOC
2. What's the password for the Burninator1.docx file?
   a. 00000000
   b. aaaaaaaa
   c. trogdor
   d. burn

3. According to the Profit&Loss.ods file, how much insurance money was collected in July 2018?
    a. $274,000.00
    b. $35,000.00
    c. 309,000.00
    d. $35,000.00
4. You discovered a known steganography program named Camouflage in the Installed Programs folder. It's been downloaded from http://camouflage.unfiction.com. What other steganography programs have been installed on Bart Jones's computer? (Choose all that apply.)
    a. Crypture
    b. OpenStego v.0.7.1
    c. Quick Stego 1.2
    d. Steganofile v.1.0
5. The Burninator1.docx file states that the fire will start around what time?
    a. 0100 hrs. to 0200 hrs.
    b. 0305 hrs. to 0310 hrs.
    c. 0345 hrs. to 0355 hrs.
    d. 0430 hrs. to 0530 hrs.

Chapter 16. Ethics for the Expert Witness

Labs included in this chapter:

Lab 16.1 Rebuilding an MFT Record from a Corrupt Image

Note

Before starting these labs, create a subfolder of your work folder named Ch16.

Lab 16.1. Rebuilding an MFT Record from a Corrupt Image

Objectives

After completing this lab, you will be able to:

- Duplicate a forensic image to use for rebuilding a corrupt MFT record
- Correct a corrupt MFT record in a duplicate forensic image
- Create a list of files from the duplicate forensic image's Documents folder

After you finish an investigation, it might be several months or even years before the case goes to trial. Because digital forensics tools get frequent upgrades, you should reexamine cases processed more than six months ago that haven't gone to trial yet. Software upgrades might find additional digital evidence than what you found with older versions of your tools.

Sometimes you need to work around your tools' limitations, too. Throughout the projects in the textbook and lab manual, you've learned how to conduct forensics analysis with freeware and evaluation versions of tools. These tools are well designed but lack the full features of their licensed versions. In addition, in some situations, your tools can't perform certain functions and, therefore, can hinder an examination. You need the skills and knowledge to come up with workaround solutions for these situations. This lab is a continuation of the in-chapter activity in Chapter 16 of the textbook, in which you apply your knowledge to the problem of the 200 KB limitation in the evaluation version of WinHex. In the in-chapter activity, you were able to carve and recover known files from the GCFI-js02.001 image by analyzing the MFT records but weren't able to correct the record for the JShu folder.

The attorney for this case has instructed you to reexamine the GCFI-js02.001 image and see whether you can correct the corrupt MFT record for the JShu folder on a duplicate GCFI-js02.001 image. You use FTK Imager Lite, to duplicate GCFI-js02.001, the evaluation version of WinHex to find the offset byte address of the corrupt MFT record in GCFI-js02.001 and to copy the corrected data from the MFT-test file in the in-chapter activity in Chapter 16 of the textbook, and the HxD hexadecimal editor to save the updated duplicate forensic image. The attorney also wants you to create a list of all subfolders and files in the Documents folder of the GCFI-js02.001 image to see whether there's any additional related evidence; for this task, you use Autopsy.

Note

As a digital forensic examiner, it's your ethical responsibility to explain to the attorney that a follow-up analysis for all previous cases should be done to ensure that all evidence has been identified. This follow-up is recommended to avoid any unexpected surprises discovered by an expert witness for the opposing attorney.

This lab is divided into four sections:

- Copying GCFI-js02.001 and renaming it as C16Proj1.001 to use for correcting the corrupt MFT record
- Determining the starting offset byte address for the corrupt MFT record in GCFI-js02.001
- Copying the corrected MFT record for the JShu folder from the MFT-test file to C16Proj1.001 (the duplicate forensic image)
- Conducting a forensic analysis of C16Proj1.001 and creating a list of files found in the Documents folder

Materials Required

This lab requires the following:

- Windows
- FTK Imager Lite, Autopsy 4.3.0, and WinHex
- The Ch16Inchp.exe file, downloaded to your work folder from the Data Files, or the GCFI-js02.001 file, copied from the in-chapter activity in Chapter 16 of the textbook
- The MFT-test file copied from the in-chapter activity in Chapter 16 of the textbook
- HxD, downloaded in the third section

Note

The HxD hexadecimal editor lacks functions included in the evaluation version of WinHex, such as bit-shifting and viewing directory paths on a drive.

Estimated completion time: 60–120 minutes, depending on your computer's performance

Caution

For all digital forensics analysis that requires changing the original digital evidence as described in this lab, always make a copy of the original evidence and make changes *only* to this copy. Do not alter the original data.

Activity

Creating a Duplicate Forensic Image

In this section, you create a duplicate of the GCFI-js02.001 forensic image:

Note

If you downloaded Ch16Inchp.exe from the Data Files, extract this file to your work folder before starting Step 1.

1. Start FTK Imager Lite, and click **File**, **Create Disk Image** from the menu. In the Select Source dialog box, click the **Image File** option button, and then click **Next**. In the Select File dialog box, click the **Browse** button, navigate to and click your work folder, click **GCFI-js02.001** , and then click **Open**. Click **Finish**.
2. In the Create Image dialog box, click to select the **Verify images after they are created** check box, if necessary, and then click **Add**. In the Select Image Type dialog

box, click the **Raw (dd)** option button, if necessary, and then click **Next**.

3. In the Evidence Item Information dialog box, type **C16Proj1** in the Case Number text box and the Evidence Number text box, type **Recovery file for GCFI-js02.001** in the Unique Description text box, type your name in the Examiner text box, type **Creating a recovery file** in the Notes text box, and then click **Next**.

4. In the Select Image Destination dialog box, click **Browse** next to the Image Destination Folder text box, navigate to and click your work folder, and then click **OK**. In the Image Filename (Excluding Extension) text box, type **C16Proj1**. In the Image Fragment Size (MB) text box, delete the current entry and type **0** (zero), and then click **Finish**. In the Create Image dialog box click **Start**.

5. When the imaging is finished, click **Close** in the Drive/Image Verify Results dialog box, and then click **Close** again in the Creating Directory Listing window. Leave FTK Imager Lite running for the next sections.

Determining the Offset Byte Address of the Corrupt MFT Record

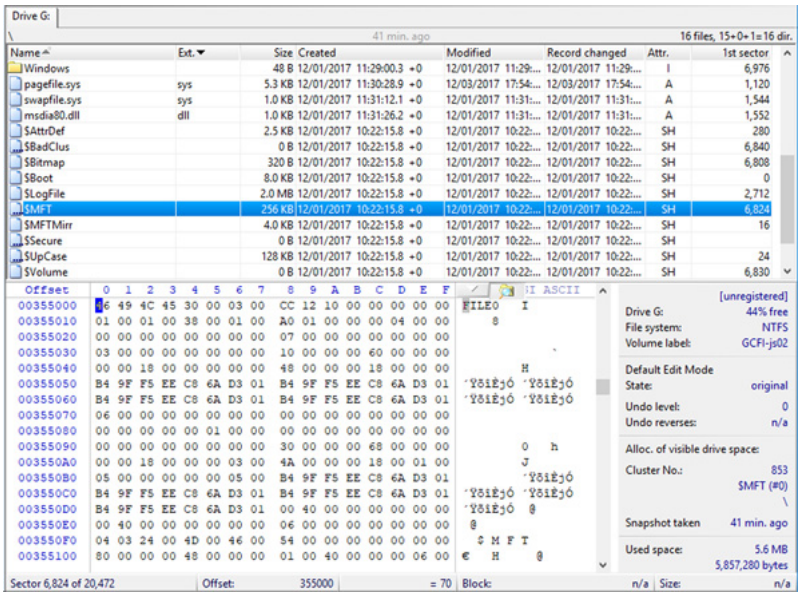
In this section, you determine the corrupt MFT record's offset byte address in the GCFI-js02.001 image. It's the absolute byte offset address where the record is located in the image (not the address in the MFT record).

1. In FTK Imager Lite, click **File**, **Image Mounting** from the menu. In the Mount Image To Drive dialog box, click the **browse** button next to the Image File text box, navigate to and click your work folder, and double-click **GCFI-js02.001** . Click the **Mount** button. Note the drive letter assigned to the mounted image in the Mapped Image List section. Click **Close**, and minimize FTK Imager Lite.

2. Start WinHex, and click **OK** in the evaluation warning message. Click **Tools**, **Open Disk** from the menu to open the Select Disk dialog box. In the Logical Volumes/Partitions section, click **GCFI-js02 (G:)**, and then click **OK**. (*Note*: Your drive letter might be different.)

3. Scroll down the list of folders and files in the upper pane, and then click **$MFT** , as shown in Figure 16-1. In the lower pane, notice the offset position 00355000; it's the starting byte for the $MFT file.

Figure 16-1.

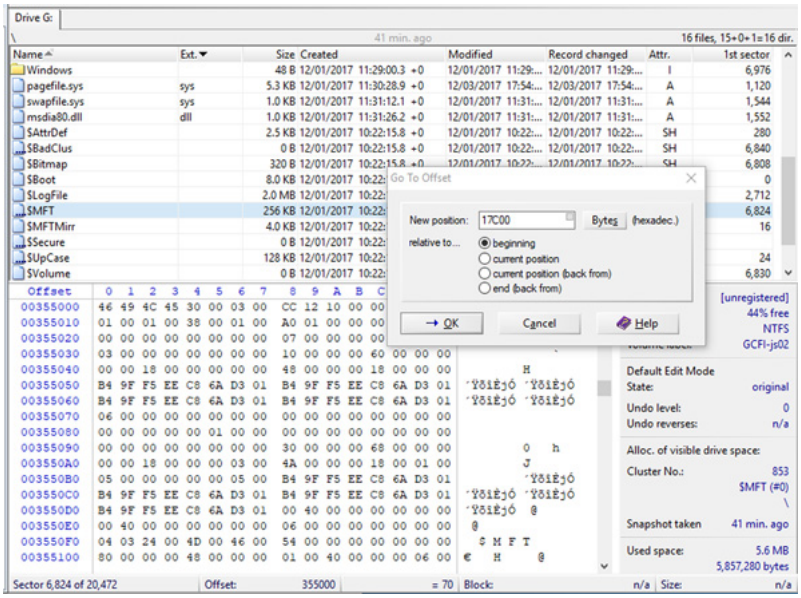


Source: X-Ways AG, www.x-ways.net

Determining the starting sector for the $MFT file

4. Next, you need to determine the starting offset byte position for the corrupt JShu folder's record in the $MFT file. In Chapter 16 of the textbook, you found the corrupt record at offset 000177C0 (see Figure 16-5 in the textbook). To find this record's absolute starting position in GCFI-js02.001, click the first byte in the lower pane at offset **00355000**. Click **Navigation**, **Go To Offset** from the menu. In the Go To Offset dialog box, type **17C00** in the "New position" text box (see Figure 16-2), click the **current position** option button, and click **OK**.

Figure 16-2.

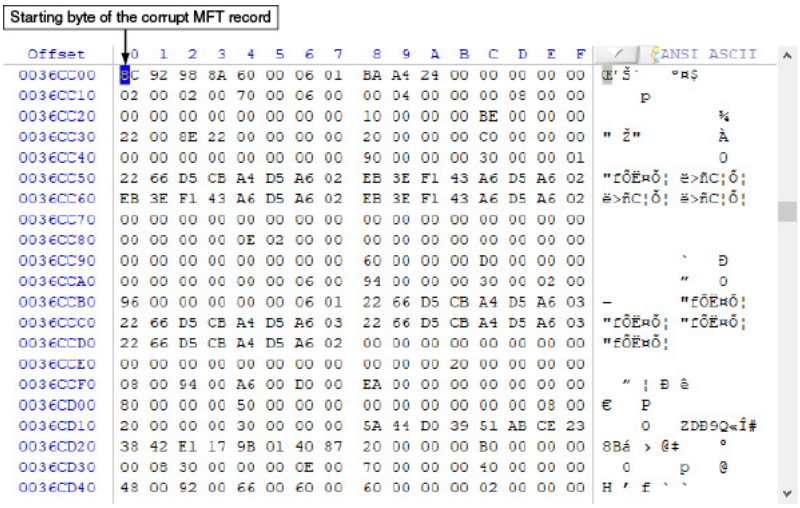


Source: X-Ways AG, www.x-ways.net

Finding the corrupt MFT record's starting offset byte position

5. WinHex displays the corrupt record's starting offset byte position, 0036CC00, in the lower pane (see **Figure 16-3**). Make a note of this hexadecimal number for the next section. Leave WinHex and FTK Imager Lite running for the review questions at the end of this lab.

Figure 16-3.



Source: X-Ways AG, www.x-ways.net

Identifying the starting offset byte position

Copying the Corrected MFT Record

In this section, you install the HxD hexadecimal editor and copy the corrected MFT record from MFT-test to the 0036CC00 offset in G16Proj1.001:

1. Start a Web browser, and go to https://mh-nexus.de/en/downloads.php?product=HxD20. Click the **HxD20** link, and download **HxDSetup.zip** to your work folder.

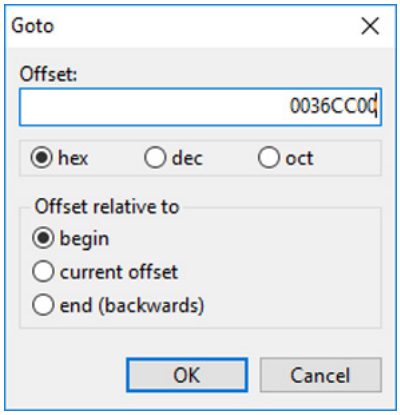
2. In File Explorer, navigate to your work folder. Right-click **HxDSetup.zip** , and click **Extract All**. In the Extract Compressed (Zipped) Folders dialog box, click **Extract**.

3. When the extraction is finished, a new File Explorer window opens to the HxDSetup subfolder. Double-click the **HxDSetup.exe** file to start the installation. In the Select Setup Language window, click **OK**, and in the Setup - HxD Hex Editor welcome window, click **Next**. In the License Agreement window, click the **I accept the agreement** option button, and then click **Next**. In the Pick Installation Mode window, click the **Normal - Integration into Windows** option button, if necessary, and then click **Next**.

4. In the Select Destination Location window, click **Next**, and in the Select Start Menu Folder window, click **Next**. In the Select Additional Tasks window, click the **Create a Quick Launch shortcut** option button, if necessary, and then click **Next**. In the Ready to Install window, click **Install**, and in the Completing the HxD Hex Editor Setup Wizard window, click **Finish**.

5. Start HxD, if necessary, and click **File**, **Open** from the menu. Navigate to and click your work folder, and double-click **C16Proj1.001** . Click **Search**, **Goto** from the menu. In the Goto dialog box, type **0036CC00** in the Offset text box, click the **hex** and **begin** options buttons, if necessary (see Figure 16-4), and then click **OK.**

Figure 16-4.

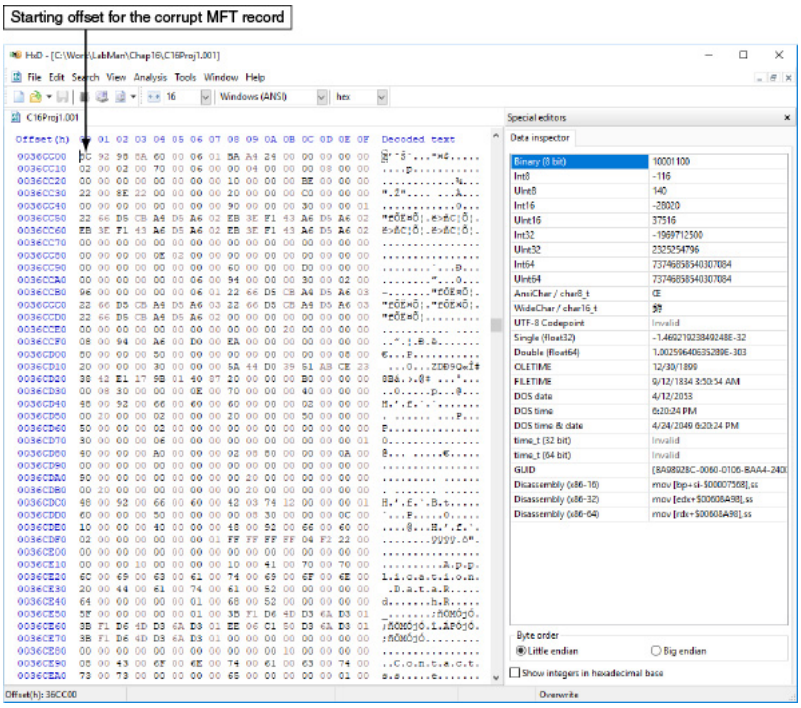


Source: Maël Hörz, www.mh-nexus.de

Navigating to the 0036CC00 offset

6. Scroll down to display the hexadecimal code from offsets 0036CC00 to 0036CE00 (see **Figure 16-5**).

Figure 16-5.

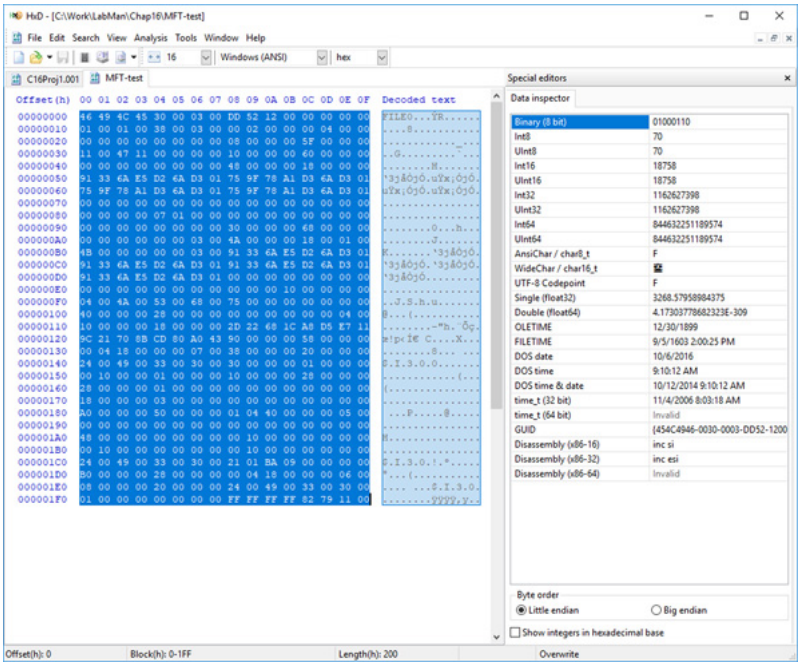


Source: Maël Hörz, www.mh-nexus.de

Examining the corrupt MFT record in C16Proj1.001

7. Click **File**, **Open** from the menu. Navigate to and click your work folder, and double-click **MFT-test** . Click **Edit**, **Select All** from the menu, and press **Ctrl+C** to copy this file (see Figure 16-6).

Figure 16-6.



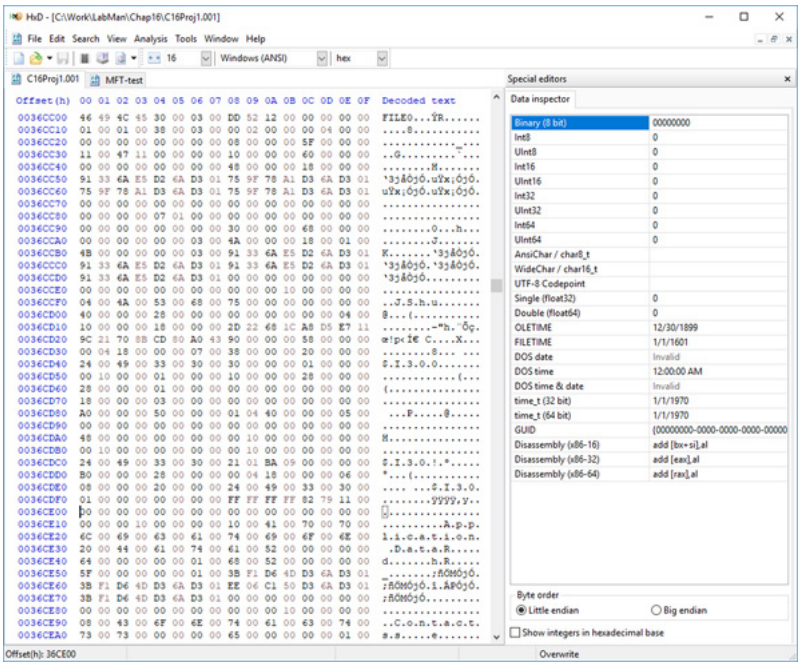
Source: Maël Hörz, www.mh-nexus.de

Copying the corrected MFT record

8.

In HxD, click the **C16Proj1** tab, and make sure the cursor is at offset **0036CC00**. Click **Edit**, **Paste write** from the menu to paste the corrected MFT record into the C16Proj1.001 image, as shown in Figure 16-7. (*Note*: The "Paste write" option overwrites the incorrect data.) Click **File**, **Save** from the menu to save these changes.

Figure 16-7.



Source: Maël Hörz, www.mh-nexus.de

Pasting the corrected MFT record into C16Proj1.001

9. Leave WinHex, FTK Imager Lite, and HxD running to answer review questions at the end of this lab.

Extracting Additional Evidence

In this section, you use Autopsy and FTK Imager Lite to collect a list of files from the Documents folder in C16Proj1.001:

1. Start Autopsy 4.3.0, and in the Welcome window, click the **Create New Case** button. In the New Case Information window, type **C16Proj1** in the Case Name text box. Click the **Browse** button next to the Base Directory text box, navigate to and click your work folder, click **Select** to enter this path, and then click **Next**.

2. In the Additional Information window, type **C16Proj1** in the Case Number text box and your name in the Examiner text box, and then click **Finish**.

3. In the Select Data Source window, click **Disk Image or VM File** in the "Select data source type" list box, if necessary. Click the **Browse** button, navigate to and click your work folder, click the **C16Proj1.001** file, click **Open**, and then click **Next**.

4. In the Configure Ingest Modules window, click **Select All**. Click **Next** and then **Finish** to start analyzing the evidence.

5. Click the **Keyword Lists** down arrow. Click the **Phone Numbers**, **IP Addresses**, **Email Addresses**, **URLs**, and **Credit Card Numbers** check boxes, and then click the **Search** button. Autopsy begins searching the image.

6. In the left pane, expand **Data Sources**, **Users**, and **Jshu**. Right-click the **Documents** folder and click **Extract File(s)**. In the Save dialog box, click **Save**, and click **OK** in the

Information message box.

7. In the left pane, expand the **Documents** folder and click the **Special Project A** folder. Right-click the **f0034789.jpg** file in the Result Viewer pane, point to **Tag File** and **Quick Tag**, and click **Follow Up** in the Quick Tag list.

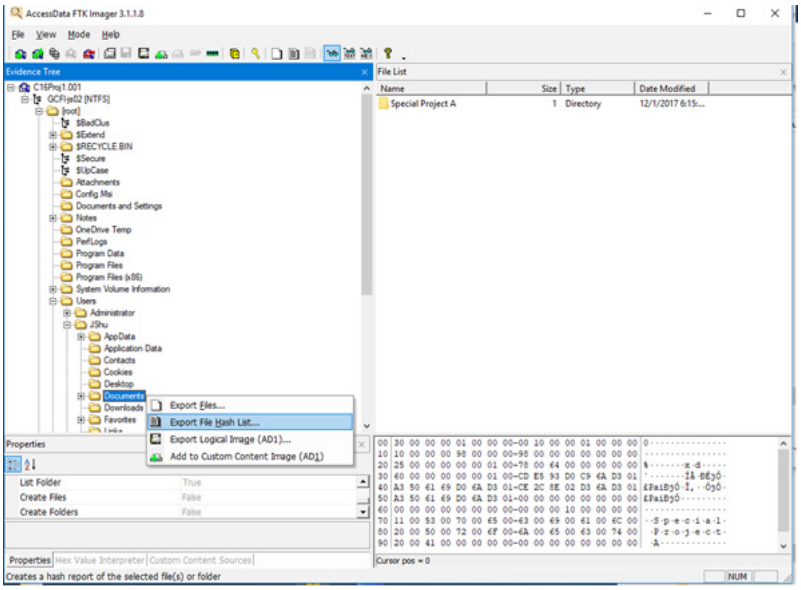
8. In the left pane, expand **Special Project A** and **Tom's Stuff**, and click the **Kayak** folder. Shift+click the **Kayak4(1).JPG** and **Kayak4.JPG** files in the Result Viewer pane. Right-click this selection, point to **Tag File** and **Quick Tag**, and click **Follow Up** in the Quick Tag list.

9. Click **Tools**, **Generate Report** from the menu. In the Generate Report window, click the **Results - HTML** option button, and then click **Next**. In the Configure Artifact Reports window, click **All Results**, if necessary, and then click **Finish**. When the report is finished, click the **Results - HTML** pathname in the Report Generation Progress window to see the report. Leave the report open in Autopsy to answer the following review questions.

10. In FTK Imager Lite, click **File Add Evidence Item** from the menu. In the Select Source dialog box, click the **Image File** option button, and then click **Next**. In the Select File dialog box, click the **Browse** button, navigate to and click your work folder, click **C16Proj1.001** , and then click **Open**. Click **Finish**.

11. In the left pane, expand **C16Proj1.001** , **GCFI-js02 [NTFS]**, **[root]**, **Users**, and **JShu**. Right-click the **Documents** folder and click **Export File Hash List** (see Figure 16-8). In the Save As dialog box that opens automatically, navigate to and click your work folder. In the "File name" text box, type **C16Proj1-File-List.csv**, and click **Save** to create a list of all files in the Documents folder.

Figure 16-8.



Source: AccessData Group, Inc., www.accessdata.com

Exporting the file hash list

12. When you're finished answering the review questions, exit all programs used in this lab.

Review Questions

1. When you created a duplicate image, FTK Imager Lite created C16Proj1.001.txt to store case information about the image. What's the SHA-1 hash value for the duplicate image?

a. 16e6a2f9ae4e77483f1fc49dba56cf7a

b. 16c6a2f9ae4e77483f1fc49dba56cf7a

c. e2cb77486ddb5d479c0bd2667c8185686deeb415

d. e2cb77486ddb5d479c0bd2667c8185686dccb415

2. In WinHex, what's the starting offset byte position for the $MFT file?

   a. 0035000

   b. 17C00

   c. 0036CC00

   d. 00000000

3. How many hexadecimal bytes did you copy from WinHex to HxD?

   a. 512

   b. 200

   c. 400

   d. 2048

4. In Autopsy, what type of files were extracted from the C16Proj1.001 image?

   a. .pdf files

   b. .txt files

   c. .jpg files

   d. .doc files

5. According to the Autopsy report, what are the camera's manufacturer and model listed in the EXIF Metadata section?

   a. Lica M3

   b. Minolta Co., Ltd Dimage 2330 Zoom

   c. Canon Power Shot 600

   d. Nikon Coolpic P7000

Appendix A. Certification Test References

This appendix gives you an overview of National Institute of Standards and Technology (NIST) testing processes for certification of digital forensics tools and digital forensics training programs offering certificates.

NIST Digital Forensics Tool Testing

NIST provides several resources on digital forensics tool testing. Check these resources regularly for the latest updates and test results. The following links on the NIST Web site are of specific interest to forensics examiners:

- The Computer Forensics Tool Testing (CFTT) Project (www.cftt.nist.gov)
- The National Software Reference Library (NSRL) Project (www.nsrl.nist.gov/index.html)

The CFTT Project was developed to give the legal community, law enforcement, and forensics tool vendors a program to validate the reliability of these tools. As part of the validation, this project is intended to help vendors improve their products to ensure that their results stand up in court.

The NSRL is a repository of known software and files from computer vendors. OS and application files are identified by their unique hash values, usually MD5 and SHA-1 hashes. Forensics examiners can filter out known files by their hash values; this process reduces the number of files they need to inspect for possible digital evidence. The NSRL also contains hash values for known bad files, typically computer viruses and contraband material.

Types of Digital Forensics Certifications

Several organizations, both public and private, have developed certification programs for digital forensics examiners. Some organizations specialize in certain areas, and others take a general overview approach, but all provide a baseline for what examiners are supposed to be proficient in when conducting computer investigations. These organizations typically have fees for membership and certification exams.

Some of these organizations have come and gone for a variety of reasons. If you decide to get a certification, examine the sponsoring organization's history and management and check the board of directors' or advisers' credentials. With this information, you can determine an organization's focus. For example, if an organization's members are well known for disk and media forensics, you know the certification is oriented toward stand-alone computing exams. If an organization's members are well known for network and intrusion forensics, you know the certification focuses on network firewalls and other related network intrusion topics. In addition, the older the organization is, the better the chances are that it will be around for future support.

Digital forensics certification organizations can be divided into three categories:

- Professional certifying organizations
- Application vendor certifying companies
- Digital forensics public and private training groups

The following sections describe some well-known certifying organizations, but many other organizations provide certification. When selecting a certification program, research it thoroughly to make sure it fits your needs. All these programs require a sizable investment of your time and money.

Professional Certifying Organizations

These organizations are typically nonprofit or not-for-profit groups that have specific missions to provide guidelines and training for digital forensics.

IACIS Certification

The International Association of Computer Investigative Specialists (IACIS) is a nonprofit organization formed to promote professional standards and certify forensics examiners. Through IACIS, you can become a Certified Forensic Computer Examiner (CFCE). To qualify to take the CFCE exam, you must be an active law enforcement officer or other person qualified to be an IACIS member. For more information on qualification requirements, visit www.iacis.com.

IACIS offers an extensive testing program to verify competence in performing a computing investigation. The examination process is not a training program; it's strictly a testing program. Applicants are screened before acceptance into the certification program, and IACIS is the sole decision maker for all applicants. Applying for the certification requires completing an application form and paying the associated fee. For the latest information on fees, go to http://members.iacis.com/certification. If you're rejected for any reason, your fee is returned. If you're accepted into the program, a monitor (an IACIS CFCE member) directs you through the testing.

ISFCE Certification

Similar to IACIS, the International Society of Forensic Computer Examiners (ISFCE) provides guidelines for training for its Certified Computer Examiner (CCE) certification. You can find current information on ISFCE at www.isfce.com and more information on the CCE certification at www.certified-computer-examiner.com. Currently, several universities and colleges sponsor credited and non-credited digital forensics classes for this certification. In addition, many commercial forensics training companies offer CCE training.

GIAC Certification

The SysAdmin, Audit, Network, Security (SANS) Institute offers extensive training in all aspects of computing security, including forensics. The SANS certification program is called Global Information Assurance Certification (GIAC; www.giac.org/overview) and has several training tracks. One track, Global Certified Forensic Analyst (GCFA), provides unique training in network intrusion response forensics for computer media. Tools used for GCFA training are open source and require extensive knowledge of UNIX and Linux. For more information on this program, visit www.giac.org/certifications/security/gcfa.php.

Application Vendor Certifying Companies

Several digital forensics application vendors have developed their own certification programs. These programs follow standard guidelines for practices used in all digital forensics investigations and examinations. In addition, these vendor-specific exams certify that people earning these certifications are competent in using their forensics tools. Two well-established vendor certification programs are Guidance Software EnCase Certified Engineer (EnCE) and AccessData Certified Examiner (ACE).

EnCE Certification

For acceptance into the EnCE certification program, you must meet one of several prerequisite options defined at www.guidancesoftware.com/training/Pages/ence-certification-program.aspx.

ACE Certification

For acceptance into the ACE certification program, you must meet one of several prerequisite options defined at http://accessdata.com/training/computer-forensics/certification.

Digital Forensics Public and Private Training Groups

Several small businesses, universities, and colleges have developed program certificates for successful completion of their coursework; these organizations can be divided into academic institutions and private training companies. The programs range from one day to several months of classroom work. Most academic institutions offer college credit for their courses, and private training companies typically offer continuing education credits. For more information on these programs, refer to the Web sites listed in the following sections. To find other programs, do a search on "digital forensics certificates."

Academic Institutions

Here are some leading schools offering digital forensics certificates:

- British Columbia Institute of Technology, www.bcit.ca/study/programs/526jadcert
- California State at Fullerton, http://extension.fullerton.edu/ProfessionalDevelopment/Certificates/Computer-Forensics1
- Century College (cloud virtualization forensics), www.century.edu/futurestudents/programs/pnd.aspx?id=9
- Champlain College, http://digitalforensics.champlain.edu
- College of San Mateo, http://collegeofsanmateo.edu/degrees/
- DeVry University, www.devry.edu/degree-programs/college-engineering-information-sciences/computer-forensics-about.html
- University of Central Florida, www.ucf.edu/online/degree/digital-forensics-m-s/
- University of Maryland University College, www.umuc.edu/academic-programs/masters-degrees/digital-forensics-and-cyber-investigations.cfm
- University of Rhode Island, www.dfcsc.uri.edu/academics/
- Wilber Wright College, www.ccc.edu/colleges/wright/programs/Pages/Computer-Security-and-Forensic-Investigation-Basic-Certificate.aspx

To find additional accredited schools, search online for "colleges offering degrees in digital forensics."

Private Training Companies

The following list shows a few private training companies offering digital forensics certificates:

- ed2go, www.ed2go.com/career/training-programs/forensic-computer-training
- Computer Forensic Training Center Online, www.cftco.com
- NW3C, www.nw3c.org/home
- SANS DFIR, https://digital-forensics.sans.org/certification

Web Site References

The following Web sites collect and list resources for digital forensics training:

- Guide to Online Programs for Digital Forensics, www.forensicscolleges.com/blog/resources/computer-forensics-education-guide
- Computer Forensics Education - Course Directory, www.forensicfocus.com/computer-forensics-education-directory

Appendix B. Digital Forensics References

This book is only the beginning of digital forensics and investigations. To master all levels of digital forensics, you should familiarize yourself with the works of other authors who have made significant contributions to this profession. This appendix lists international standards, digital forensics books, operating system books, and legal references that can expand your skills and understanding of conducting digital investigations. In addition, you'll find helpful Web links, e-mail lists, and professional journals.

International Organization of Standards 27000

The International Organization of Standards (ISO) is an organization that publishes guidelines for many manufactured items as well as digital forensics functions. It's in the process of developing additional standards for digital forensics so that collected evidence can be shared more easily. The 27000 series of ISO documents deals with digital security, and the following relate to digital forensics:

- ISO/IEC 27037:2012 – Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence
- ISO/IEC 27038:2014 – Information technology – Security techniques – Specification for digital redaction
- ISO/IEC 27039 – Information technology – Security techniques – Selection, deployment and operation of intrusion detection and prevention systems
- ISO/IEC 27040 – Information technology – Security techniques – Storage security
- ISO/IEC 27041:2015 – Information technology – Security techniques – Guidelines for assuring suitability and adequacy of incident investigative methods
- ISO/IEC 27042:2015 – Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence
- ISO/IEC 27043:2015 – Information technology – Security techniques – Incident investigation principles and processes
- ISO/IEC 27050:2015+ – Information technology – Security techniques – Electronic discovery
- ISO/IEC 27102 – Information technology – Security techniques – Cyberinsurance (draft)
- ISO/IEC SD 27103 – Information technology – Security techniques – Cybersecurity and ISO and IEC standards (draft)–For more information, see www.iso27001security.com/html/27000.html.

Digital Forensics Reference Books

In recent years, several books on digital forensics have been published. The following sections list a variety of books that can expand your technical skills and understanding of digital investigations. Some of these books might be out of print and not available through retail bookstores, such as Amazon and Barnes & Noble. For out-of-print books, check with Abe Books (www.abebooks.com) to see whether books you're looking for are in stock. Abe Books and other used book dealers can search other resources for unique out-of-print books.

Brown, Christopher L. T. *Computer Evidence: Collection & Preservation*. Course Technology, 2009 (ISBN 1584506997).

Bunting, Steve and William Wei. *EnCase Computer Forensics: The Official EnCE: EnCase Certified Examiner Study Guide*. Sybex, 2012 (ISBN 0470901063).

Carrier, Brian. *File System Forensic Analysis*. Addison-Wesley Professional, 2005 (ISBN 0321268172).

Carvey, Harlan. *Windows Forensic Analysis DVD Toolkit*, 2nd ed. Syngress, 2009 (ISBN 1597494224).

Casey, Eoghan. *Handbook of Digital Forensics and Investigation*. Academic Press, 2009 (ISBN 0123742676).

Casey, Eoghan, ed. *Digital Evidence and Computer Crime*. Academic Press, 2011 (ISBN 0123742684).

Casey, Eoghan, ed. *Handbook of Computer Crime Investigation, Forensic Tools and Technology*. Academic Press, 1997 (ISBN 0121631036).

Clark, Franklin and Ken Diliberto. *Investigating Computer Crime*. CRC Press, 1996 (ISBN 0849381584).

Fowler, Kevvie. *SQL Server Forensic Analysis*. Addison-Wesley Professional, 2008 (ISBN 0321544366).

Garrison, Clint P. *Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data*. Syngress, 2010 (ISBN 1597495379).

Hayes, Darren R. *A Practical Guide to Computer Forensics Investigations*. Pearson IT Cybersecurity Curriculum, 2014 (ISBN 0789741156).

Icove, David, Karl Seger, and William VonStorch. *Computer Crime, A Crimefighter's Handbook*. O'Reilly & Associates, Inc., 1995 (ISBN 1565920864).

Jones, Keith J., Richard Bejtlich, and Curtis W. Rose. *Real Digital Forensics: Computer Security and Incident Response*. Addison-Wesley Professional, 2005 (ISBN 0321240693).

Kruse II, Warren G. and Jay G. Heiser. *Computer Forensics: Incident Response Essentials*. Pearson Education, 2001 (ISBN 0201707195).

Kubansiak, Ryan R., Sean Morrissey, and Jesse Varsalone (tech. ed.). *Mac OS X, iPod, and iPhone Forensic Analysis DVD Toolkit*. Syngress, 2008 (ISBN 1597492973).

Ligh, Michael Hale, Andrew Case, Jamie Levy, Arron Walters. *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory*. Wiley, 2014 (ISBN 1118825098).

Malin, Cameron H., James M. Aquilma, and Eoghan Casey. *Malware Forensics: Investigating and Analyzing Malicious Code*. Syngress, 2008 (ISBN 159749268X).

Martin, James P. and Harry Cendrowski. *Cloud Computing and Electronic Discovery*. Wiley, 2014 (ISBN 1118764307).

Mel, H. X. and Dons Baker. *Cryptography Decrypted*. Addison-Wesley, 2001 (ISBN 0201616475).

Pogue, Chris, Cory Altheide, and Todd Haverkos. *UNIX and Linux Forensic Analysis DVD Toolkit*. Syngress, 2008 (ISBN 1597492698).

Prosise, Chris, Kevin Mandia, and Matt Pepe. *Incident Response: Computer Forensics*. McGraw-Hill, 2014 (ISBN 0071798684).

Quick, Darren, Ben Martini, and Raymond Choo. *Cloud Storage Forensics*. Syngress, 2013 (ISBN 9780124199705).

Rosenblatt, Kenneth S. *High-Technology Crime*. KSK Publications, 1995 (ISBN 0964817101).

Ruan, Keyun. *Cybercrime and Cloud Forensics: Applications for Investigation Processes*. IGI Global, 2012 (ISBN 1466626623).

Sammes, A. J. and Brian Jenkinson. *Forensic Computing*, 2nd ed. Springer, 2007 (ISBN 1846283973).

Shavers, Brett. *Placing the Suspect Behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects*. Syngress, 2013 (ISBN 1597499859).

Shavers, Brett, and John Bair. *Hiding Behind the Keyboard: Uncovering Covert Communication Methods with Forensic Analysis*. Syngress, 2016 (ISBN 0128033401).

Shavers, Brett, and Eric Zimmerman. *X-Ways Forensics Practitioner's Guide*. Syngress, 2009 (ISBN 0124116051).

Stephenson, Peter. *Investigating Computer-Related Crime*. CRC Press, 2000 (ISBN 0849322189).

MS-DOS and PowerShell Reference Books

The following books are good references on how to use MS-DOS and PowerShell and how to create your own script files. Some of these books might be out of print. If you can't find them at a local bookstore, try searching for them on eBay or at www.bookfinder.com.

Cooper, Jim. *Special Edition Using MS-DOS 6.22*, 3rd ed. Que, 2002 (ISBN 0789725738).

Gookin, Dan. *DOS for Dummies*, 3rd ed. Wiley Publishing, Inc., 1999 (ISBN 0764503618).

Holmes, Lee. *Windows PowerShell Cookbook: The Complete Guide to Scripting Microsoft's Command Shell*, 3rd ed. O'Reilly Media, 2013 (ISBN 1449320686).

Menefee, Craig and Nick Anis. *Harnessing DOS 6.0, Batch File and Command Macro Power* . Bantam Computer Books, 1993 (ISBN 0553351885).

Wilson, Ed. *Windows PowerShell Step by Step*, 3rd ed. Microsoft Press, 2015 (ISBN 100735675112).

Windows Reference Books

The better you understand the many versions of Windows operating systems, the better you understand what data you're looking for and recovering. For a current list of Windows OS and application books, see Microsoft Press (www.microsoftpressstore.com). In addition, you should search for the latest Windows books at your favorite retail provider's Web site.

Linux Reference Books

Linux is becoming more popular with end users and digital forensics examiners. The more you know and understand about Linux, the easier it is to use. It makes dynamic control of processes possible, which is beneficial to digital forensics examiners.

Helmke, Matthew. *Ubuntu Unleashed*. Sams Publishing, 2014 (ISBN 0672336936).

Rankin, Kyle. *Knoppix Hacks: 100 Industrial-Strength Tips and Tools*. O'Reilly Media, Inc., 2004 (ISBN 0596007876).

Siever, Ellen, et al. *Linux in a Nutshell: A Desktop Quick Reference*. O'Reilly Media, Inc., 2000 (ISBN 0596000251).

Sobell, Mark G. *A Practical Guide to Linux Commands, Editors, and Shell Programming*. Prentice Hall PTR, 2012 (ISBN 013308504X).

Tyler, Chris. *Fedora Linux: A Complete Guide to Red Hat's Community Distribution*. O'Reilly Media, Inc., 2006 (ISBN 0596526822).

Legal Reference Books

The following books are guides on expert testimony:

Babitsky, Steven and James J. Mangraviti, Jr. *How to Become a Dangerous Expert Witness: Advanced Techniques and Strategies*. SEAK, Inc., 2005 (ISBN 1892904276).

Babitsky, Steven, James J. Mangraviti, Jr., and Christopher J. Todd. *The Comprehensive Forensic Services Manual: The Essential Resources for All Experts*. SEAK, Inc., 2000 (ISBN 1892904071).

Babitsky, Steven, James J. Mangraviti, Jr., and Christopher J. Todd. *The Comprehensive Forensic Services Manual: The Essential Resources for All Experts*. SEAK, Inc., 2002 Supplement (ISBN 1892904225).

Smith, Fred Chris and Rebecca Gurley Bace. *A Guide to Forensic Testimony: The Art and Practice of Presenting Testimony as an Expert Technical Witness*. Addison-Wesley Professional, 2002 (ISBN 0201752794).

Web Sites

Association of Certified Fraud Examiners, www.acfe.com

CERIAS, www.cerias.purdue.edu/site/research/forensics/

CERT, www.cert.org

Champlain College, Computer & Digital Forensics, http://digitalforensics.champlain.edu

Computer Crime Research Center, www.crime-research.org

Computer Forensic Analysis, www.porcupine.org/forensics/

Computer Forensics, Cybercrime and Steganography Resources, www.forensics.nl

Computer Technology Investigators Network, www.ctin.org

Forensic Magazine, www.dfinews.com

Digital Forensic Research Workshop, www.dfrws.org

FBI's Forensic Science Communications, www.fbi.gov/about-us/lab/forensic-science-communications

Forensic Focus, www.forensicfocus.com

High Tech Crime Consortium, www.hightechcrimecops.org

International Federation for Information Processing, www.ifip.org

International High Technology Crime Investigation Association, www.htcia.org

Journal of Digital Forensics, Security and Law, http://commons.erau.edu/jdfsl/

SANS, www.sans.org

Sleuth Kit, www.sleuthkit.org

Source Forge, Digital Forensics Tool Testing Images, http://dftt.sourceforge.net

US-CERT, www.us-cert.gov

Steganalysis References

The following are useful references for learning more about steganalysis methods:

"JPEG steganography detection with Benford's Law" (Panagiotis Andriotis, George Oikonomou, and Theo Tryfonas, www.fortoo.eu/m/page-media/4/jpeg-steganography.pdf, 2013)

"Multi-class Blind Steganalysis for JPEG Images" (Tomas Pevny and Jessica Fridrich, http://dde.binghamton.edu/tomas/pdfs/pev06-spie.pdf, 2010)

"Steganalysis of Images Created Using Current Steganography Software" (Neil F. Johnson and Sushil Jajodia, www.jjtc.com/ihws98/jjgmu.html, 1998)

You can find additional references at http://josea1.weebly.com/references.html.

E-mail Lists

Computer Forensics World, www.computerforensicsworld.com/index.php

X-Ways Support Forum, www.winhex.net

Yahoo! Groups

Computer Forensics Tool Testing (CFTT), https://groups.yahoo.com/neo/groups/cftt/info

Mobile Phone Forensics, https://groups.yahoo.com/neo/groups/mobile-cell-phone-forensics/info

Professional Journals

Digital Forensics Magazine (www.digitalforensicsmagazine.com)

Digital Investigations (www.journals.elsevier.com/digital-investigation)

Forensic Science Communications (www.fbi.gov/about-us/lab/forensic-science-communications)

International Journal of Cyber Criminology (www.cybercrimejournal.com)

International Journal of Cyber-Security and Digital Forensics (http://sdiwc.net/security-journal/index.php)

International Journal of Electronic Security and Digital Forensics (www.inderscience.com/jhome.php?jcode=ijesdf)

International Journal of Forensic Computer Science (www.ijofcs.org)

Journal of Digital Forensics, Security and Law (http://commons.erau.edu/jdfsl/)

Appendix C. Digital Forensics Lab Considerations

In Chapter 2 **, you learned what's needed for a digital forensics lab. This appendix** addresses some additional considerations for planning and operating a lab.

International Lab Certification

In addition to the American Society of Crime Laboratory Directors (ASCLD; www.ascld.org), the International Organization of Standards (ISO) has requirements for standard processes that transcend national boundaries. An organization can become ISO certified when it has integrated processes to ensure that established requirements in products and services are met consistently. Of special interest to digital forensics examiners are the following ISO standards that can be applied to lab operation:

- ISO 9000: Quality management system in production environments
- ISO 9001: Quality management
- ISO 9069: Software quality model
- ISO 9241: Ergonomic requirements for office work with visual display
- ISO 17025: General requirements for competence of test and calibration laboratories
- ISO 27001: Information technology – Security techniques – Information security management systems

Note

For more information on ISO standards, visit www.iso.org, www.ansi.org/standards_activities/iso_programs/overview.aspx?menuid=3, and www.fasor.com/iso25.

Considering Office Ergonomics

Because digital investigations often require hours of processing drives for evidence, your workspace should be as comfortable as possible to prevent repetitive-motion injuries and other computer work–related injuries. Ergonomics is the study of designing equipment to meet the human need for comfort and allow improved productivity and involves psychology, anatomy, and physiology. Understanding psychology helps designers create equipment that people can easily understand how to use. Ergonomic design also considers anatomy to make sure the equipment correctly fits the person using it. Physiology helps determine how much effort or energy the person using the equipment must expend.

To ensure an ergonomic workspace, review the following questions when arranging your workspace and selecting lab furniture:

- *Desk or workstation table*—Is the desk placed at the correct height for you? Do you need a chair that's lower or higher than normal to make the desktop easy to reach and comfortable to use? Are your wrists straight when sitting? Is this position comfortable? Are the heels of your hands in a comfortable position? Do they exert too much pressure on the desktop? Do you need a keyboard or mouse pad?
- *Chair*—Can your chair's height be adjusted? Is the back of the chair too long or too short? Is the seat portion too long or too short for your thighs? Are the seat and back padded enough to be comfortable? Can you sit up straight when viewing the monitor? Are your elbows in a comfortable position while working? How do your shoulders and back feel while sitting and working at the workstation? Is your head facing the monitor, or do you have to turn your head because you can't position the chair in front of the monitor?

- *Workbench*—Is the workbench for your lab facility at the correct height when you're standing in front of it? Can you reach the back of the bench easily without having to stand on a stool?

Besides furniture, consider the ergonomics of your keyboard and mouse. These two items probably contribute to more repetitive-motion injuries than any other devices because they were designed for moderate but not extensive use. Using the keyboard for several hours at a time can be painful and cause physical problems. Make sure your wrists are straight when you're working with a keyboard or mouse, even if these items are ergonomically designed.

If you work with computers for hours in one position, you'll injure yourself. No matter how well the furniture, keyboard, or mouse is designed, always take breaks to stretch and rest your body.

Considering Environmental Conditions

Your lab's ventilation and temperature also contribute to your comfort and productivity. Although a typical desktop computer uses standard household electricity, computers get warm as they run. Unless you invest in a liquid-cooled computer case for your forensic workstation, a standard desktop computer generates heat. The more workstations you're running, the hotter your lab, so the room needs adequate air conditioning and ventilation. Consult with your building's facility coordinator to determine whether the room can be upgraded to handle your current and expected computing needs.

Use the following checklist of heating, ventilation, and air-conditioning (HVAC) system questions when planning your digital forensics laboratory:

- How large is the room, and how much air moves through it per minute?
- Can the room handle the increased heat that workstations generate?
- How many workstations will be placed in this room? What's the maximum number of workstations the room can handle?
- Can the room handle the heat output from a small RAID server?

Lighting

Lighting is often an overlooked environmental issue in digital forensics labs. Most offices have too many lights at the wrong illumination, which can cause headaches and eyestrain. Several vendors offer natural or full-spectrum lighting, which is less fatiguing than standard incandescent or fluorescent lights, although it doesn't have any health benefits.

Tip

In 1986, the Food and Drug Administration (FDA) issued a Health Fraud Notice about "false and misleading" claims and "gross deceptions" by light bulb and lamp manufacturers on the benefits of full-spectrum lighting (*FDA Enforcement Report: Health Fraud Notice*, 1986, WL 59812).

If the lighting in your lab is a problem, consult with facility management and find out what products can best meet your needs. For additional information on dealing with eyestrain, see https://support.apple.com/en-us/HT205655.

Considering Structural Design Factors

The physical construction of your digital forensics lab is another factor to consider. Your lab should be a safe, secure, lockable room. Processing a drive or creating an image can take anywhere from a few hours to several days or weeks. When you must leave evidence

unattended overnight, you need a secure location—a room that no unauthorized people can access without your control.

Tip

The National Industrial Security Program Operating Manual (NISPOM), Chapter 5, Section 8, page 1, "Construction Requirements," gives an overview of how to build a secure lab. See www.dss.mil/documents/odaa/nispom2006-5220.pdf for details.

To ensure physical security, examine the facility's hardware, walls, ceiling, floors, and windows. Make sure only heavy-duty building material has been used in the construction. All hardware, such as door hinges on the outside of the lab, should be peened, pinned, brazed, or spot-welded to prevent removal.

Walls can be constructed of plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, glass, wire mesh, expanded metal, or other materials offering resistance to and evidence of unauthorized entry. If you use insert panels, you need to install material that can reveal evidence of an attempt to gain entry.

Ceilings, like walls, can be constructed of plaster, gypsum wallboard, acoustic ceiling panels, hardboard, wood, plywood, ceiling tile, or other material that offers some sort of resistance and makes detection possible if access is attempted. False or drop ceilings in which the walls don't extend to the true ceiling because of hanging ceiling tile must be reinforced with wire mesh or 18-gauge expanded metal that extends from the top of the false wall to the true ceiling. This material must overlap adjoining walls and should provide resistance so that attempted access can be detected.

If you have raised floors, which are common in data centers, look for large openings in the perimeter walls. If you find any, use the same types of material described for ceilings to make sure the floor provides resistance and shows evidence of someone attempting to access the lab.

Avoid windows on the lab exterior. If you're assigned a room with exterior windows, install additional material, such as wire mesh, on the inside to improve security. If your lab must be placed on an exterior wall, request an upper floor, not a ground floor. Also, make sure monitors face away from windows to prevent unauthorized people from being able to see what you're working on.

Doors can be wood (solid core) or metal and shouldn't have windows. If the door does have a window, it should have wire mesh in the glass for resistance so that attempted entries can be detected. The door's locking device should have a heavy-duty, built-in combination device or a high-quality key-locking doorknob. If you're using a key-locking doorknob, only authorized personnel should have a copy of the key.

Note

Depending on your lab's location, you might need to install intrusion detection systems and fire alarms. Consult and contract with a bonded alarm company.

Determining Electrical Needs

You need enough electrical power to run workstations and other equipment; 15-amp and 20-amp service are preferred for electrical outlets. In addition, you should have enough electrical outlets spaced throughout the lab for easy access, eliminating the need for extension cords or electrical plug strips, which are potential fire hazards.

If you have adequate electrical power for your operation, power fluctuations aren't usually a problem unless you're in an area with poor electrical service. Most computers are fairly tolerant of power fluctuations, although they do cause electrical wear and tear on computer components. However, all electrical devices eventually fail, usually because of accumulated electrical voltage spikes. If your lab equipment exhibits unexplained failures, consult with your facilities manager to check for problems with electrical power.

In addition, uninterruptible power supply (UPS) units must be connected to all forensic workstations to reduce electrical problems. If a power failure occurs, a UPS unit enables you to continue working until you can shut down your computer safely. Most UPS units also block or filter electrical fluctuations, which helps minimize computer component problems that might corrupt and destroy evidence stored on sensitive magnetic media.

Planning for Communications

When you're planning voice and data communications, keep in mind that each examiner needs a telephone. Unless you're working in a TEMPEST environment, which has special voice and data access requirements, you can install a multiline Integrated Services Digital Network (ISDN) phone system in the lab. ISDN is the easiest way for lab personnel to handle incoming calls.

You also need dial-up or broadband Internet access. Digital forensics software vendors often provide updates and patches on their Web sites, and you need to be able to download them. Internet access is also needed to conduct research on evidence you find and to consult with other forensics professionals. However, don't keep your workstation connected to the Internet while conducting your analysis unless absolutely necessary. Internet connections can compromise your system's security, even with a firewall installed.

Setting up a LAN for workstations in a lab enables you to transfer data to other examiners easily and makes operations run more smoothly. For example, you can share a RAID file server and printers on a LAN. This setup is especially useful when you have specialty printers connected to a print server. Using a central RAID server also saves time when you're copying large files, such as image files.

If your organization is part of a WAN, consider having a separate computer used only to connect to the WAN to protect the security of your forensic workstations. By keeping your forensic workstations physically separate from the WAN, you eliminate any intentional or unintentional access to your evidence or work product. For example, although workstations on a WAN can receive notices to upgrade software, doing so while your forensic workstation is connected to the WAN can corrupt evidence. Isolating systems prevents this corruption.

Installing Fire-Suppression Systems

Any electrical device can cause a fire, although fires aren't common with computers. However, an electrical short in a computer might destroy a cable. If the power on a low-voltage cable is high enough, it could ignite other combustible items nearby. Computers can also cause fires if a hard disk's servo-voice coil actuators freeze because of damage to the drive. When this happens, the head assembly can't move. The disk's circuit card then applies more electrical power to actuators to try to move the head assembly, which passes too much power through the disk. Disk components can handle only so much power before they fail and overload the cables connecting the drive to the computer. When too much power is applied to these low-voltage cables, especially ribbon cables, sparks can fly, causing a fire.

Most offices are equipped with fire sprinkler systems and dry chemical fire extinguishers (B rated). For most forensics lab operations, these fire-suppression systems work well, and no additional protection is required. However, if your lab facility has raised floors, you might need to install a dry chemical fire-suppression system. If you have any concerns, contact your facility coordinator or the local fire marshal. For additional information on best practices for fire extinguishers, see

www.fia.uk.com/filemanager/root/site_assets/news/fia_best_practice_guide_2014_final_version_46193.pdf. For information on computer room fire-suppression systems, see https://kinetixfire.com/an-overview-of-fm-200-carbon-dioxide-wet-chemical-and-dry-chemical-fire-suppression-systems/ and www.assured-ltd.co.uk/blog/five-main-types-fire-suppression/.

Appendix D. Legacy File System and Forensics Tools

This appendix gives you information about older file systems, such as Microsoft File Allocation Table (FAT) and Mac HFS and HFS+, and MS-DOS tools. It also introduces the MS-DOS forensics tools X-Ways Replica and Digital Intelligence DriveSpy, and there's a short discussion of how hexadecimal numbers relate to binary setting in bytes.

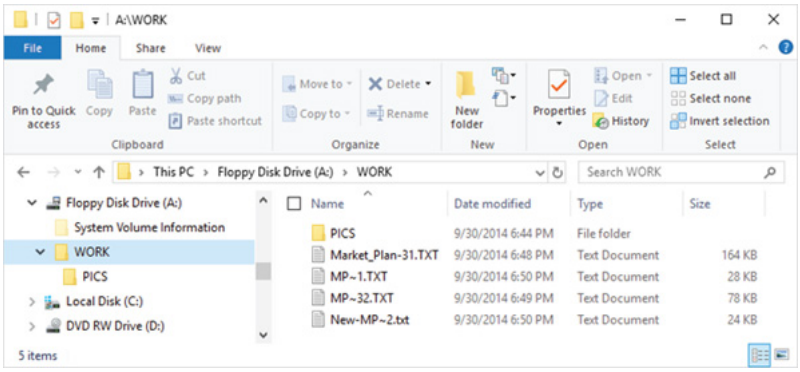
Overview of FAT Directory Structures

When Microsoft created the MS-DOS operating system, data was stored on floppy disks. Floppy disks have a limited maximum size, so the addressable storage space is small compared with modern hard disks. All floppy disks for Microsoft OSs use the FAT12 file system. (FAT file systems are explained in more detail in **Chapter 5**.) Because of the limited disk and memory space on older computers, Microsoft engineered FAT12 so that directory names could be only one to eight characters. Filenames could be up to eight characters, and file extensions could be zero to three characters. This naming scheme is often called the "8.3 naming convention." The characters in file extensions identify the file type, such as .doc for a Word document or .xls for an Excel spreadsheet.

When larger drives were developed, Microsoft reengineered FAT and created FAT16, which allows up to 2 GB of addressable storage space for drive partitions. With further advances in disk technologies, Microsoft created FAT32, which can access up to 2 terabytes (TB) or more of storage space. In MS-DOS 6.22, the same directory and filename conventions from FAT12 were carried over to FAT16. The latest versions of FAT can now have names longer than eight characters and file extensions of more than three characters.

When Microsoft implemented Unicode, it developed the Virtual FAT (VFAT) file system. At that time, VFAT provided two filenames for every file: a long filename in the 16-bit Unicode format, when displayed in a hexadecimal editor with null (00) values between each character, and a short filename that uses eight-character filenames and three-character extensions. The purpose of having both filenames was for backward-compatibility. For example, **Figure D-1** shows four files, one with a long filename (Market_Plan-31.TXT) and three with short filenames. When you view Market_Plan-31.TXT in MS-DOS with the dir command, you see its name converted to the short filename: Market~1.TXT (see Figure D-2).

Figure D-1.



Viewing filenaming in File Explorer

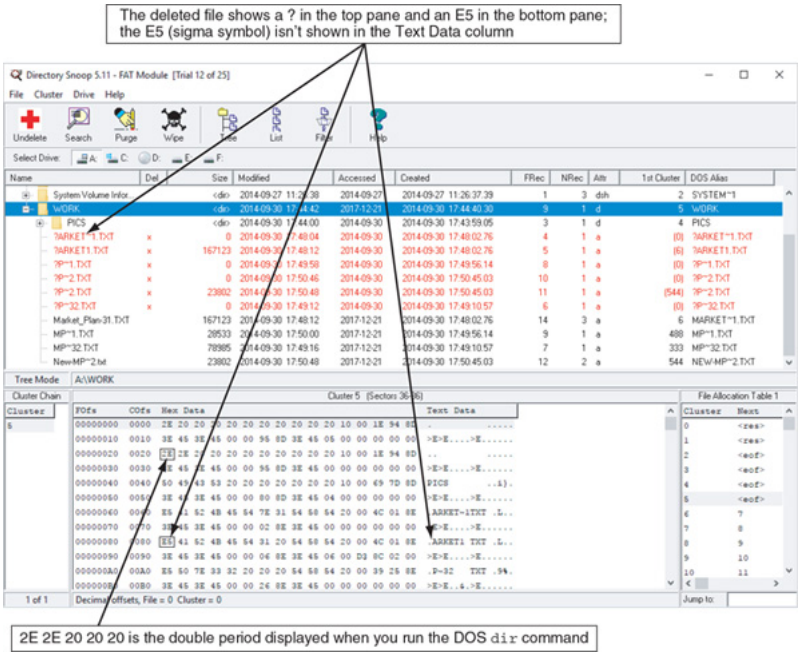
Figure D-2.

```
A:\WORK\ DIR
 Volume in drive A has no label
 Volume Serial Number is E452-FA5F

   Directory: A:\WORK

09/30/2014 5:44 PM    <DIR>              .
09/30/2014 5:44 PM    <DIR>              ..
09/30/2014 5:44 PM    <DIR>              PICS
09/30/2014 5:48 PM               167,123 MARKET~1.TXT
09/30/2014 5:49 PM                78,985 MP~32.TXT
09/30/2014 5:50 PM                28,533 MP~1.TXT
09/30/2014 5:50 PM                23,802 New-MP~2.TXT
               4 File(s)          298,433 bytes
               3 Dir(s)           613,376 bytes free

A:\WORK>_
```

Viewing filenaming in Windows PowerShell with the dir command

A useful tool that can run in Windows is the shareware Directory Snoop from Briggs Softworks (www.briggsoft.com/dsnoop.htm). Directory Snoop is a convenient GUI tool for inspecting and recovering deleted data from disks. Figure D-3 shows an example of using it for FAT partitions. Note that no long filenames are listed in the bottom pane, which indicates that MS-DOS 6.22 or earlier was used to format the floppy disk and write data to it.

Figure D-3.



Source: Briggs Softworks, www.briggsoft.com

Using Directory Snoop

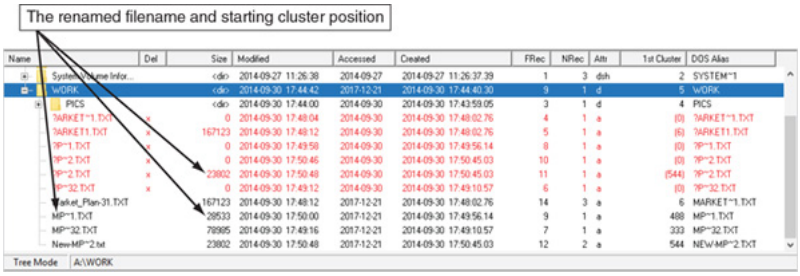
FAT directories contain specific information about the files stored in them. All FAT directories start with a hexadecimal 2E followed by several hexadecimal 20 values. A hexadecimal 2E converts to the ASCII value for a period, and a hexadecimal 20 represents a space. (For an explanation of hexadecimal numbers, see "**An Overview of Hexadecimal Numbering**" later in this appendix.) The following information is listed for all files in a directory:

- Long filename for Windows 95 or later FAT disks
- Short filename (8.3 naming convention)

- Attributes assigned to the file
- Case and creation time in milliseconds
- Creation time of the file
- Creation date of the file
- Last access date of the file
- Starting cluster high-word for FAT32 file systems
- Modified timestamp
- Modified date stamp
- Starting cluster of the file (assigned by FAT when all links to the file are listed)
- File size

When a file is deleted in a FAT directory, a hexadecimal E5 is inserted as the filename's first character (see the callout in **Figure D-3**). If the file is renamed, an entry with the new filename is created, and the old filename is marked as deleted with the E5 value, just as though the file had been deleted. These entries aren't usually deleted from the directory. Figure D-4 shows a renamed file in a directory on a FAT12 drive. Notice the size of this renamed file and the byte size of the deleted file and the renamed file.

Figure D-4.



Source: Briggs Softworks, www.briggsoft.com

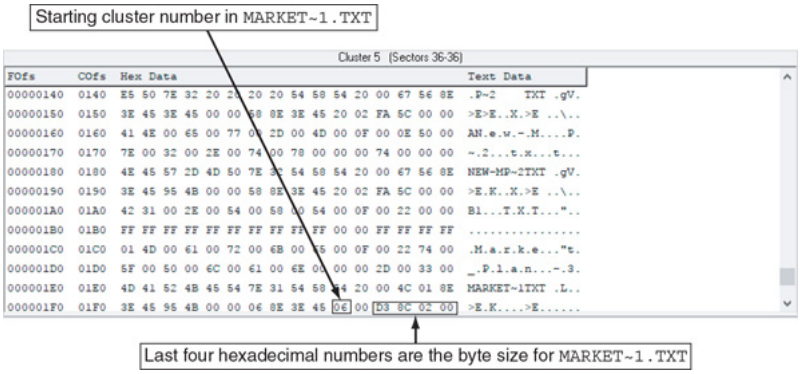
Using Directory Snoop with a FAT12 drive

You can also reverse-engineer the starting cluster position and file size. These values are listed in hexadecimal format in the directory. To convert hexadecimal values to decimal, use the Windows scientific calculator:

1. In Windows, click **Search**, type **Calculator**, and click the **Calculator** icon.
2. Click **View**, **Programmer** from the Calculator menu.
3. In the Programmer Calculator window, click the **HEX** option button.
4. Using the keyboard or number buttons, enter the hexadecimal value you want to convert, and then click the **DEC** option button.

As shown in **Figure D-5**, the last four hexadecimal numbers are the byte size for the MARKET~l.TXT file. When converting these numbers from hexadecimal to decimal, you read them from right to left: 00 02 8C D3, in this example. What's displayed with the dir command or in File Explorer might be slightly smaller than what's converted. Figure D-5 also shows MARKET-l.TXT's starting cluster number in hexadecimal. To convert these numbers to decimal, you enter them from right to left: 00 06.

Figure D-5.



Source: Briggs Softworks, www.briggsoft.com

Converting from hexadecimal to decimal

Notice the decimal value 6 entered in the calculator. In FAT directory entries, the file's starting cluster position is at offset 1A hexadecimal or 26 decimal from the first position where the filename is displayed. Remember, the first position where the filename appears has the starting value of 0. The file's byte size is located starting at offset 1C hexadecimal or 28 decimal. These values are read from right to left.

In digital forensics investigations, often you need to determine the size of a file that has been deleted and overwritten by a newer file. This information can give you clues about copies of the deleted file on other disks.

DOS Forensics Tools

During the 1980s and 1990s, digital forensics tools were designed to run on MS-DOS. These tools can collect digital evidence from FAT drives on PCs and consist of utilities that handle tasks such as data acquisitions of file slack space and unallocated space, text string searches, and other functions. Most of these tools can fit on a forensic boot floppy disk, which is used to access a PC's drive to acquire and examine its contents. Currently, only a few vendors still sell DOS forensics tools, such as these two:

- *X-Ways Replica*—This disk forensic acquisition program can run from a removable storage medium running Microsoft DOS 6.22. For more information, see www.x-ways.net/replica.html.
- *DriveSpy*—This DOS command-line program can acquire forensic images, search for text and hexadecimal data strings, view FAT links showing the cluster where data is located (useful for finding fragments of residual data), and perform other analysis functions. For more information, see www.digitalintelligence.com/software/disoftware/drivespy.

Legacy Mac File Systems

Chapter 7 mentioned legacy Mac file systems. Table D-1 shows the Hierarchical File System (HFS) block positions, and Table D-2 shows the Extended Format File System (HFS+) byte offset positions.

Table D-1. HFS System Files

HFS block position	HFS structure	Purpose of structure
0 and 1	Boot block	Startup volume containing boot instructions; also stores system files and Finder information.

HFS block position	HFS structure	Purpose of structure
2	Master Directory Block (MDB)	Contains volume creation date and time and location of other system files, such as Volume Bitmap. A duplicate of this file called the Alternate MDB is located at the second-to-last block on the volume. Its purpose is to provide information to OS disk utilities.
3	Volume Bitmap	Tracks used and unused blocks on the volume.
-	Catalog	Lists all files and directories on the volume. It's a B*-tree file that uses the extents overflow file to coordinate all file allocations to the volume.
-	Extents overflow file	This B*-tree file lists the extra extents, which are the allocated blocks used to store data files.

Table D-2. HFS+ System Files

HFS+ byte offset (fixed starting position)	HFS+ structure	Purpose of structure
-	Boot blocks	No change from HFS.
1024	Volume Information Block (VIB)	Replaces the MDB used in HFS.
Not fixed	Allocation file	Tracks available free blocks on the volume; replaces the HFS Volume Bitmap.
Not fixed	Extents overflow file	For files with more than eight extents, additional extents are recorded and managed through this B*-tree system file.
Not fixed	Catalog	Similar to an HFS catalog, this improved version allows up to eight extents for each file's forks. It's a B*-tree file.
Not fixed	Attributes file	Stores new file attribute information that isn't available in HFS. The new attributes are inline data attribute records, fork data attribute records, and extension attribute records.
Not fixed	Startup file	New to HFS+, this file can boot non-HFS and non-HFS+ volumes.
Not fixed	Alternate VIB	Same file as the HFS Alternate MDB.
-	Reserved (512 bytes)	Last sector of the volume; used by Apple during manufacturing.

Tip

For more on B*-tree and HFS, see http://tldp.org/HOWTO/Filesystems-HOWTO-7.html.

An Overview of Hexadecimal Numbering

To understand hexadecimal numbering, you need to understand binary data. Information in a computer is stored in binary digits called "bits." Like a light switch, a bit is either off or on. Bits set to off are given the value 0, and bits set to on are given the value 1. Bits can be turned on or off, depending on what values they're assigned by programs. ASCII has established a list of bit patterns associated with letters, numbers, and other symbols. These bits are grouped into bytes, which consist of 8 consecutive bits.

Computers communicate and store data only in binary fashion: 0s and 1s. When you're looking at raw binary data, it's difficult to interpret all these 0s and 1s and determine where bytes start and end. To make binary data easier to view, computer scientists apply the base-16 numbering system to bits. You're familiar with base-10 numbering, in which numbers are represented as 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9, and the next number after 9 is 10. In base-16 numbering (also called "hexadecimal" or just "hex"), the symbols are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F, and the next number after F is defined as 10. Counting bits in base-16

numbering is much easier than in base-10 numbering. Typically, a 0x is added at the front of a number to indicate that it's a hexadecimal value. So, for example, the hexadecimal number 9 is written as 0x09, and the number B is written as 0x0B. The 0 between the x and the hexadecimal number is used to provide a place for numbers greater than 0x09, such as 0x12 (with the equivalent decimal value of 18).

To determine the numeric value for decimal or hexadecimal binary digits, you read the pattern from right to left and add the value of the bit's position. For example, the letter A pattern of 01000001 is 0x41 in hexadecimal, as shown in **Table D-3**, and for the lowercase letter a, the pattern is 01100001, as shown in Table D-4.

Table D-3. Calculating Decimal and Hexadecimal Bit Patterns for the Letter A

Hexadecimal numbers	80	40	20	10	8	4	2	1
Binary numbers	0	1	0	0	0	0	0	1
Decimal numbers	128	64	32	16	8	4	2	1

Table D-4. Calculating Decimal and Hexadecimal Bit Patterns for the Letter A

Hexadecimal numbers	80	40	20	10	8	4	2	1
Binary numbers	0	1	1	0	0	0	0	1
Decimal numbers	128	64	32	16	8	4	2	1

Adding the decimal values in **Table D-3** from right to left results in $1 + 64 = 65$. For the hexadecimal values, it's $0x01 + 0x40 = 0x41$. For the lowercase letter a, add the decimal values in Table D-4 from right to left: $1 + 32 + 64 = 97$. For the hexadecimal values, it's $0x01 + 0x20 + 0x40 = 0x61$.

For more information on bits, bytes, and hexadecimal numbering, refer to the following Web sites:

- www.theproblemsite.com/codes/hex.asp
- http://homepage.smc.edu/morgan_david/cs40/hex-system.htm
- www.mathsisfun.com/hexadecimals.html
- http://whatis.techtarget.com/definition/hexadecimal
- www.tcpipguide.com/free/t_BinaryInformationandRepresentationBitsBytesNibbles-2.htm