

Prepared by Dr. Nermin Ewais

CYB 670
IT Forensics

Lecture 01



Introduction to IT Forensic

Lecture 01

CYB 670
IT Forensics

Prepared by
Dr. Nermin Ewais

- Introduction to IT Forensic
- Forensic Process
- Data Acquisition
- Computer System
- Operating system forensic
- Network forensic
- E-mail and Social Media Investigation
- Mobile Device and Cloud Forensic
- Report writing

- Learn Computer Forensics
William Oettinger
2020 Packt Publishing
- Guide to Computer Forensics and Investigations: Processing
Digital Evidence 6th Edition
Bill Nelson , Amelia Phillips and Christopher Steuart Cengage
Learning, Inc 2019

- VMware Workstation Pro
- Virtualbox

Introduction of IT Forensic

- IT Forensic Meaning.
- A Brief History of Digital Forensics
- What is cybercrime? An Overview
- Crime investigation
- Crime scene مسرح الجريمة
- Criminal investigations
- Criminal conspiracy
- Some forms of digital evidence

IT : Information
Technology

What is the meaning for
forensics?
The adjective forensic
comes from the Latin
word forensis, meaning
“in open court” or
“public

When you describe
something as forensic
you usually mean that it
has to do with finding
evidence to solve a
crime.

- **Forensic science** is a critical element of the criminal justice system.
- **Forensic scientists** examine and analyze evidence from crime scenes and elsewhere to develop objective findings that can assist in the investigation and prosecution of perpetrators of crime or absolve an innocent person from suspicion.s

- It is a division of forensics involving the recovery and analysis of data that has been recovered from digital devices.
- At one time, the term **IT Forensics or Digital Forensic** was as a synonym for computer forensics, but now involves all devices capable of storing digital data. No matter what term is used, the goal is to identify, collect, and examine/analyze digital data while preserving its integrity.

- Digital forensics is not only about finding the **artifact**, it is a formal examination/analysis of the **digital evidence** to prove or to disapprove whether the accused committed the violation.
- A key point is : **find evidence , find all the artifacts**
- **To be a digital forensic examiner:** you need to have a desire to ask questions, have specialized equipment, and have the required training.

IT Forensic meaning

- If you are in the **IT field**, you will understand networking and computer operating systems,
- but you will *lack knowledge of how to preserve evidence, maintain a chain of custody, and present it in a criminal/administrative proceeding.*



If you are an **investigator**, you will understand the chain of custody, evidence preservation, and testifying in a criminal/administrative proceeding. However, you may lack experience in the digital field.



- To be an effective **digital forensic examiner**, you have to be part of both those worlds



To understand how digital forensics works, the process of digital forensics can be broken down into 5 steps:

- *Identification*
- *Preservation*
- *Analysis*
- *Documentation*
- *Presentation*

A digital forensics investigation is used for (why to use?):

- *Identifying the cause and possible intent of a cyber attack*
- *Safeguarding digital evidence used in the attack before it becomes obsolete*
- *Minimizing the losses of the attacked organization*
- *Protecting the organization from similar incident in the future*

As Investigation

- FBI (1932): Set up a lab to offer forensics services to all field agents and other law authorities across the USA.

AS Crimes

- 1970s electronic crime were increased especially in financial systems
- In 1978 the first computer crime was recognized in the Florida Computer Crime Act.

As Technical Part

- 1985 : Xtree Gold file manager program under DOS
- 1990 : Norton Diskeditor is a hexa-editor for logical and physical Disk. It analyze the file system structure



- 1989, the International Association of Computer Investigative Specialists (IACIS) was created (it is a non-profit of digital forensic professionals).
- At 1991 IACIS introduced training on software for digital forensics.
 - Preparing search warrants
 - Undeleted files
 - File compression
 - Ethical use of software



- 1991 ,IRS created search-warrant programs
- 1998, **CFCE the Certified Forensic Computer Examiner** was first certification in computer forensic is conducted by IACIS
- 1998, EnCase released is the first commercial GUI software for computer Forensics
- **ILook** is currently maintained by the IRS Criminal Investigation Division
- **AccessData Forensic Toolkit (FTK)** is a popular commercial product



- In 2000, the First FBI Regional Computer Forensic Laboratory established.
- In 2002, Scientific Working Group on Digital Evidence (SWGDE) published the first book about digital forensic called “Best practices for Computer Forensics”.

What does the word Cyber Crimes mean?

- The term cyber means : culture of computers or networks or any information technology
- The term crime means : is an unlawful act committed .

Cybercrime is any criminal activity that involves a computer, networked device or a network.

Computers can contain information that helps law enforcement determine:

- Chain of events leading to a crime
- Evidence that can lead to a conviction

Cybercrime can be categorized into 2 types:

1. Single event from perspective of the victim
2. Pronounced human element.

Single event from perspective of the victim

It mostly technology in nature

1. Trojan, keystroke logger to steal private information
2. Phishing ex: calming to be a bank with link that leads to a hostile website.

Pronounced human element

Child predation , planning or carrying out terrorist activities, cyberstalking and harassment ...etc.

Cybercrime categories

- 1- Cybercrime against Persons**
- 2- Cybercrime against Property**
- 3- Cybercrime against Governments and**
- 4- Cybercrime against Society**

A) Cyber Crime, A Threat To Person:-

Cyber crimes committed against persons. This kind of offences affected directly personality of individual.

Ex:

- **Harassment via E-Mails:** This is very common type of harassment through sending letters, attachments of files & folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Facebook, Twitter, Orkut etc. increasing day by day.
- **Child Pornography:** In this cyber crime defaulters create, distribute, or access materials that sexually exploit underage children.

Cybercrime categories

2- Cybercrime against Property

- **Hacking Computer System:** Hackers attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer. Those attacks were not mainly intended for financial gai.
- **Internet Time Thefts:** Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person.

3- Cybercrime against Governments

The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to the international governments as also to threaten the citizens of a country.

Ex:

- **Cyber Terrorism:** Cyber terrorism is a issue in the domestic as well as global concern. Terrorist attacks on the Internet are by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer network etc.
- **Cyber Warfare :-** It refers to politically motivated hacking to conduct sabotage and espionage.

4- Cybercrime against Society

An unlawful act done with the intention of causing harm to the cyberspace will affect large number of people, association, society.

- **Financial Crimes:** The Network sites & phone Networking where culprit will try to attack by sending bogus mails or messages through internet, e.g Using credit cards by obtaining password illegally.
- **Child Pornography:** It involves the use of computer network to create, distribute or access materials that sexually exploit underage children.
- **Online Gambling:** Online fraud & Cheating is one of the most lucrative business that are growing today in cyber space eg. Credit card crime, contractual crime, offering job

1. Speed (speed in technology so investigator should be warrant before start procedure)
2. Anonymity cyber criminals can easily hide their identity
3. Volatile nature evidence : can be easily lost
4. Evidence size and complexity : according to type of digital devices => increasing in evidence data and complexity
5. Anti digital forensics : attacker are using encryption and data hiding
6. Global origin and difference in law : different laws in different counter

- **Civil** : Civil law deals with the regulation of private conduct between individuals, organizations and government agencies. Civil laws are applied when an individual has had his or her rights violated or when individuals have disputes with other individuals or organizations.
- **Criminal** : criminal case is a decision that the person or organization that is accused of breaking the law. Criminal crimes laws establish legal punishments for those convicted of crimes like arson, assault and theft.
- **Administration** : Administrative law imposes obligations on the executive branch of government in its dealings with members of the society and in its exercise of executive power

- The main purpose of digital forensics is to **collect, preserve, and analyze electronic evidence** in a way that maintains its integrity and can be used in court.
- It ensures that digital evidence is handled carefully so it remains reliable and admissible during legal proceedings.

- The knowledge gained from digital forensic investigations helps in:
 - Designing **better security measures** (like intrusion detection systems, logging policies, or encryption strategies).
 - Raising **awareness** among employees and the public about digital threats.
 - Acting as a **deterrent**—when criminals know that their digital footprints can be traced, they may think twice before committing crimes.
- Courts rely heavily on **digital evidence**, so the existence of digital forensics strengthens the rule of law in the digital era.

Figure 1-8.



The crime scene

- The first responder
- The investigator
- Crime scene technician



First responders

The first responders are the first ones on the scene.

They will do this until the investigator arrives.

The first responder's primary mission is to **make the scene safe and secure** and ensure that no one can contaminate the evidence.

The first responder must have basic knowledge of what items could contain digital evidence when they secure the scene.

- Potential victims ضحية
- Witnesses شاهد
- Subjects
- Maintain control

- Upon arriving at the scene, the first responder and the investigator **will coordinate**, and information sharing will now start
- The first responder will provide the basic information
- The investigator will want to know whether the first responder(s) touched anything, moved anything, or changed anything within the crime scene.



The investigator takes charge of the scene and directs all activity

A chain of custody must be completed and maintained showing who found the item and who maintained control until the completion of the judicial or administrative proceeding.

Finally, we come to the crime scene technician.

This person be a sworn محلف or unsworn position within the law enforcement agency.

They have specialized training in the collection of evidence



- Existing Files
- Deleted files
- Log files
- Special file system (registry file)
- Email archive – printer pool
- Administrative setting
- Internet history

Examples

- Michelle Theer was convicted of a crime against a person. She conspired with John Diamond to commit the crime against her husband, Marty.
- Investigators had no direct evidence, no physical evidence, and no eyewitness evidence, but they had digital evidence showing the conspiracy to commit the crime.
- Investigators recovered over 80,000 emails and instant messages between Diamond and Michelle that showed a personal relationship between the two and the messages showing the conspiracy between them to commit the crime.

Social media (another story)

The case of Larry Jo Thomas:

As investigators processed the crime scene, a bracelet that was "distinctive" was found and collected as evidence.

The investigators examined Thomas's Facebook page and found a photo of Thomas posing with an item similar to what was used at the crime scene.

Vehicles (example)

Newer vehicles are connected to the network and have their own Wi-Fi connection and sync data between mobile devices, GPS data, and the vehicle's black box.

Potentially, the investigator can show the subjects performing reconnaissance on their targets, meetings between the conspirators at a shared location, or where they have traveled to and returned using toll passes.

Physical and Digital security

- The organization has to be proactive and identify the critical infrastructure that needs protection.
- If an attacker is successful, the digital forensic investigator will have to determine how the attacker got past the established protocols.
- The organization's physical and digital defenses should be multifaceted and not rely on a single aspect.

Access control is essential;

- a locked door could be access control, such as, controlling access to the server room.
- Now, the door could be locked and unlocked with a biometric or a physical token and the organization maintains the access control logs off-site.



Hacker

It's a malicious user gaining access to information systems

White Hat	Black Hat	Activist
They hack into the systems to discover the liabilities before the bad actors.	They hack into systems for their own personal gain. (Bad Actor)	They hack into the system to expose the activities, harass the owner, or to promote a political agenda. (Bad Actor)

- Learn Computer Forensics
William Oettinger
2020 Packt Publishing
- Kharat, Shital, Cyber Crime – A Threat to Persons, Property, Government and Societies (March 1, 2017). <http://dx.doi.org/10.2139/ssrn.2913438>



Thank You