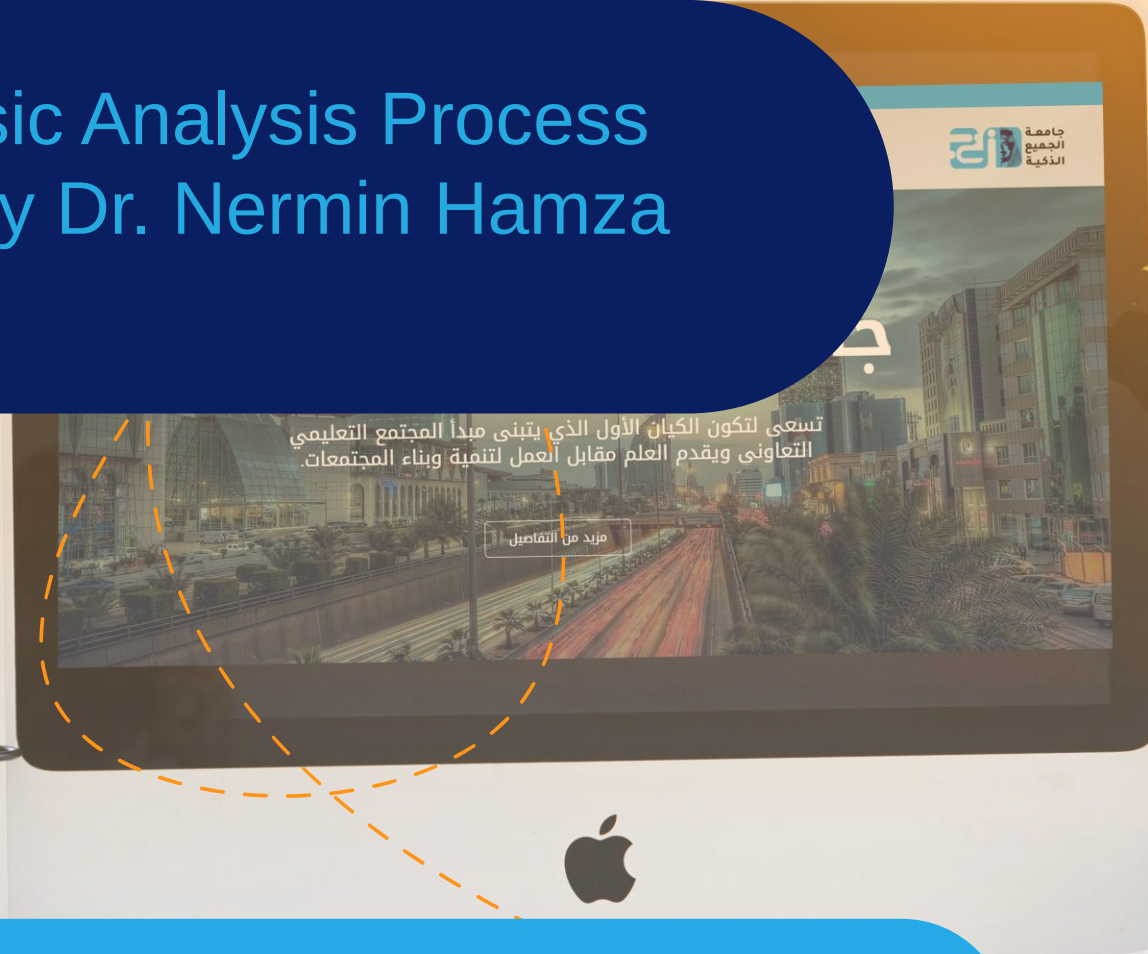


The Forensic Analysis Process

Prepared by Dr. Nermin Hamza

Lecture 2



جامعة القادسية
EVERYONE'S SMART UNIVERSITY

CYB 770
IT Forensics



- **IT Forensics Process Phases**
- **The Investigator**
- **Systematic Approach**
- **Evidence Custody Form**
- **Practices**





Pre-investigation phase: This phase involves all the tasks performed before the commencement of the actual investigation. It involves setting up a computer forensics laboratory, building a forensics workstation, investigation toolkit, the investigation team, obtaining approval from the relevant authority, and so on.



Investigation phase: Considered as the main phase of the computer forensics investigation, it involves acquisition, preservation, and analysis of the evidentiary data to identify the supply of crime and also the offender. This section involves implementing the technical knowledge to find the evidence, examine, document, and preserve the findings also as evidence.



Post-investigation phase: This phase involves reporting and documentation of all the actions undertaken and also the findings throughout the course of an investigation. Make sure that the audience will simply perceive the report also because it provides adequate and acceptable proof.



Lecture 2

The forensic analysis process is made up of five subsets

Pre-Investigation Phase



Pre-investigation considerations

Pre-Investigation Phase



Understanding case information and legal issues

Investigation Phase



Understanding data acquisition

Investigation Phase



Understanding the analysis process

Post-Investigation Phase

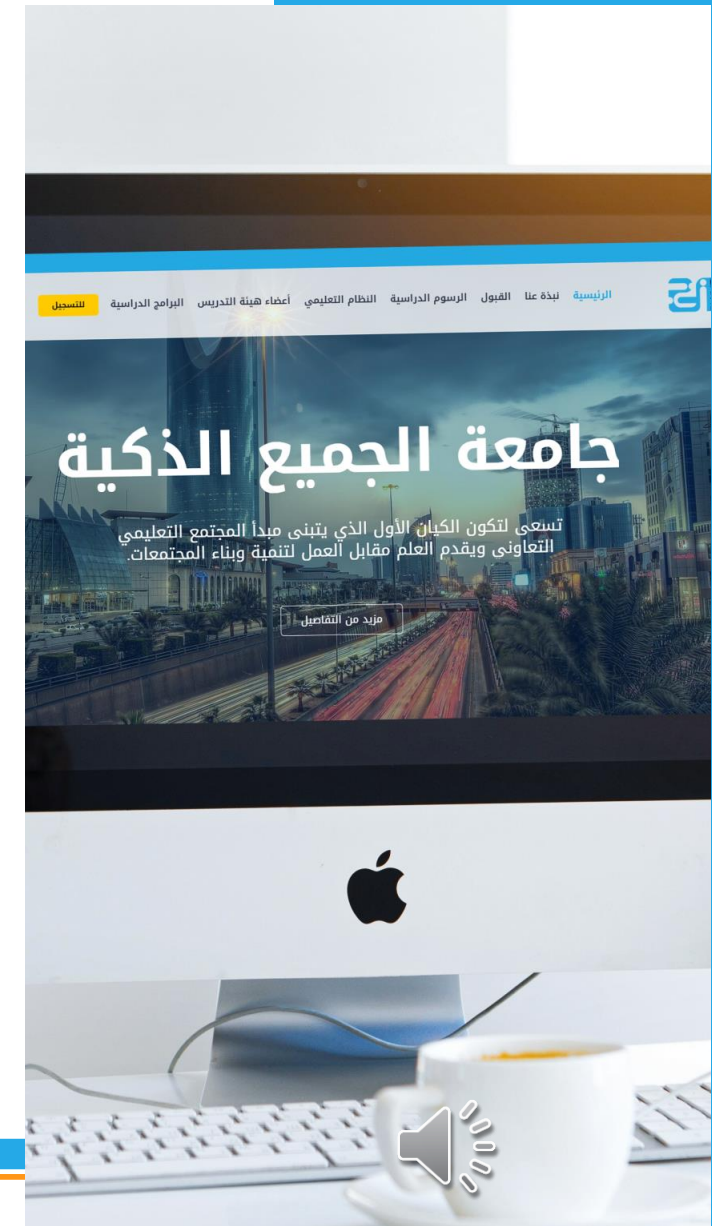


Reporting your findings



Lecture 2

Pre-investigation phase



1. Pre-investigation considerations

Pre-
Investigation
Phase

Determine your budget for hardware, personnel, and training

Before you are ready to begin the investigation, you have to prepare yourself

Some equipment will be reusable, and some will not

The forensic workstation

The response kit

Forensic software

Forensic investigator training



1. Pre-investigation considerations

Pre- Investigation Phase

- Before you are ready to begin the investigation, you have to prepare yourself.
- This includes preparing your equipment, becoming familiar with the current laws and legal decisions and the organization's policies and procedures.
 - The pre-investigation is where you determine **your capabilities and equipment specifications to conduct a forensic exam**, regardless of whether it is in the field or a **lab environment**.
 - Now is the time to determine your **budget for hardware, personnel, and training**



Lecture 2

The forensic workstation : Example

Pre- Investigation Phase

The base model costs approximately \$5,000 and comes with the following:

- An Intel 8700 K processor
- 32 GB of DDR for RAM
- 512 GB SSD

That is a basic forensic workstation and you still have to add storage for the forensic images. The high-end version costs over \$18,000 and comes with the following:

- A dual Intel Xeon E5-2690 v4 Broadwell 2.6 GHz 35MB 14-core server processor
- A 1 TB SSD for the operating system
- A 1 TB SSD or temporary files and processing
- 2 TB SSD for databases
- Several 8 to 6 TB hard drives in a RAID configuration
- 640 GB DDR4 RAM
- An 8 GB GDDR5 graphics processing unit (GPU)



Create a **response kit** that includes documentary paperwork, pens, and storage containers to store digital evidence.

Pre-
Investigation
Phase

It may include :

- **Digital camera:** Capable of still and video recording
- **Latex gloves:** These protect several aspects of the evidence collection
- **Write blocking devices:** a hardware device, such as the *Tableau TK8u USB 3.0 forensic bridge* which allows you to access a storage device without changing its contents.
- **Storage media:** Hard drives can be a traditional spinning disk or SSD and USB devices
- Etc...



- Software that you will use to analyze data.
- Commercial software designed for the forensic process or open-source tools

Autopsy: Autopsy is a fully functioning suite of forensic tools

SIFT Workstation: SIFT is a virtual machine that uses the Ubuntu operating system with multiple forensic tools pre-installed.

Paladin Forensic Suite: Paladin is a live Linux distribution based on Ubuntu and has implemented several open source forensic tools in a user interface called the Paladin toolbox.

CAINE: Computer Aided Investigative Environment (CAINE) is a digital forensics project that provides a GUI



- **International Association of Computer Investigative Specialists (IACIS):**
<https://www.iacis.com/>
- **EnCase Certified Examiner (EnCE):** <https://www.Opentext.com/products-and-solutions/services/training-and-learning/services/encase-training/certifications>
- **Accessdata Certified Examiner (ACE):**
<https://accessdata.com/training/computer-forensics-certification>
- **Computer Hacking Forensic Investigator (CHFI):**
<https://www.eccouncil.org/programs/computer-hacking-forensic-investigatorchfi/>
- **Global Information Assurance Certification (GIAC):**
<https://www.giac.org/certifications>



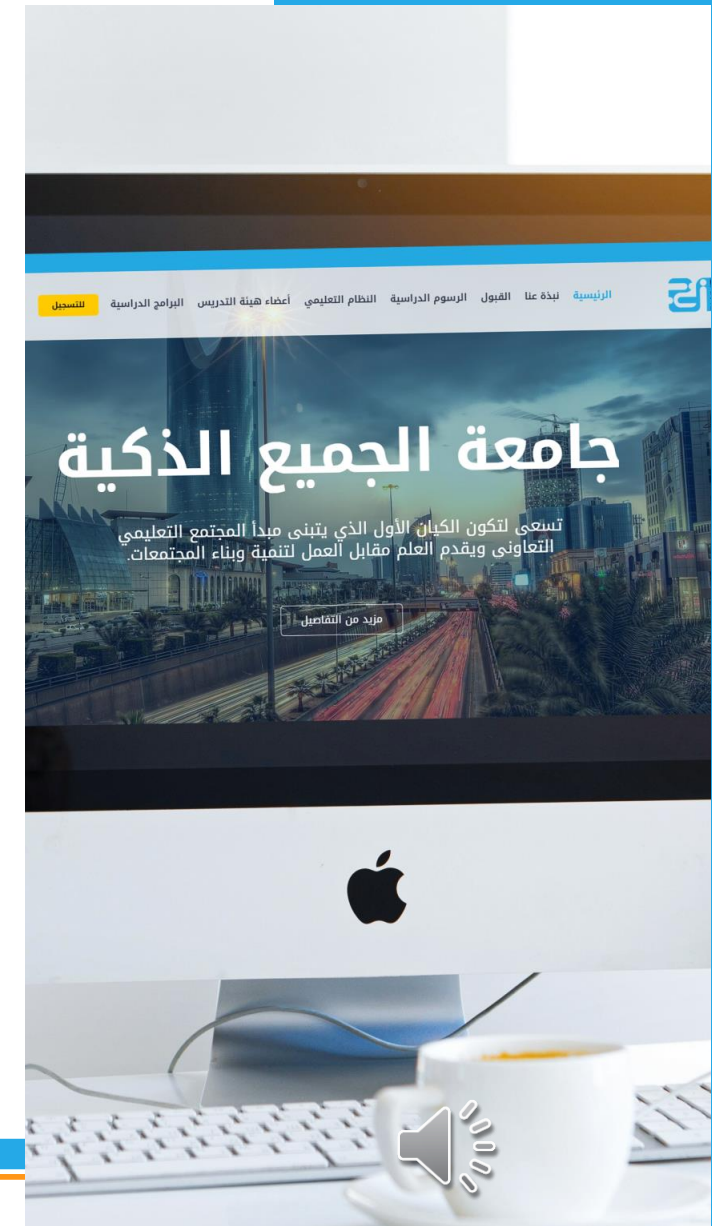
Pre- Investigation Phase

- What is the nature of the investigation?
- What digital evidence do you expect to find at the scene?
- As a government and corporate digital forensic investigator, I have had limits on what I can search for or view on digital devices many times
- **Civil and Criminal**



Lecture 2

Investigation phase



3. Understanding data acquisition



- To collect volatile evidence, we should start from the most to the least volatile
- Collecting the volatile data may not always be possible, depending on the specific set of circumstances you encounter on the scene.
- the goal of digital forensics is to create a **forensic image** for analysis and under normal circumstances.

Investigation
Phase



3. Understanding data acquisition

Investigation
Phase

A forensic image: We are creating a bit-for-bit copy of the source device but we store that data in a forensic image format.
This could be a DD image, an E01 image, or an AFF image.



Portable Devices and Data Storage

- **Power**

- The first rule of securing portables for forensic examination is that if the device is off, leave it off (but keep the battery charged);
- if the device is on, do everything feasible to keep the device powered on until a full examination can be performed



Securing Your Evidence

Investigation
Phase



Write your initials on tape to prove that evidence has not been tampered with



Consider computer specific temperature and humidity ranges

Make sure you have a safe environment for transporting and storing it until a secure evidence container is available



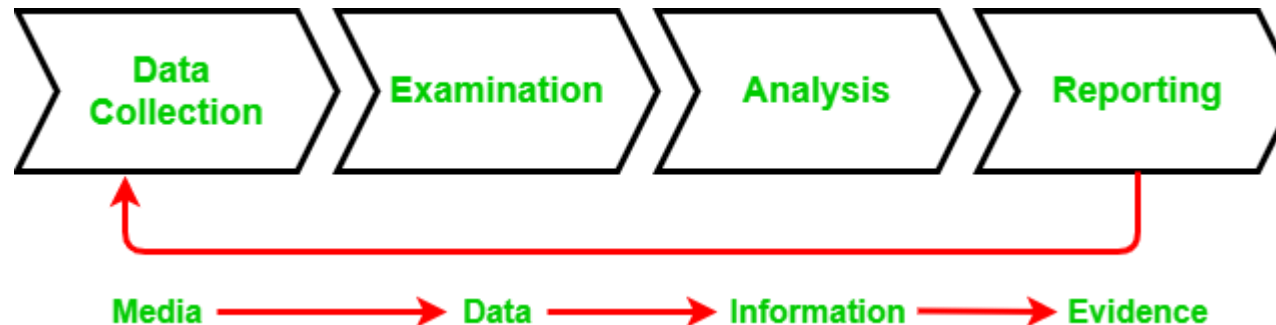


- The chain of custody documents all access to the evidence, who accessed it, when it was accessed, and for what purpose it was accessed.
- Maintaining the **chain of custody** is an integral part of preserving and authenticating evidence, both physical and digital, for an administrative or judicial proceeding.



Investigation Phase

The chain of custody should span from the first step of data collection to examination, analysis, reporting, and the time of presentation to the Courts. This is very important to avoid the possibility of any suggestion that the evidence has been compromised in any way.



4. Understanding the analysis process

Investigation
Phase

Once you have collected data from the scene, you return to your lab and it is now time to start your forensic analysis.

- **Dates and time zones ...**
- **Hash analysis**
- **File signature analysis**
- **Antivirus**



4. Understanding the analysis process

Investigation Phase

- **Dates and time zones ...**

Setting the forensic machine and tools to use **universal time (UTC)**

- **Hash analysis**

- Hash is a digital fingerprint for a file or piece of digital media. It is generated through the use of a one-way cryptographic algorithm.

- MD5 creates a 128-bit digital fingerprint while SHA-1 creates a 160-bit digital fingerprint

```
702edca0b2181c15d457eacac39de39b F:\Hash Test change.txt
```



4. Understanding the analysis process

Investigation
Phase

- **File signature analysis**

- file signature analysis, which is to ensure the file extension matches the file type.
- A user can change the file extension to hide incriminating evidence. The intention behind carrying out a file signature analysis is to determine whether the file signature and file extension are a match.

-X-Ways

- **Antivirus**

Several forensic tools allow you to "mount" the forensic image as a read-only drive and you can then scan the filesystem to help determine whether there is malware installed.

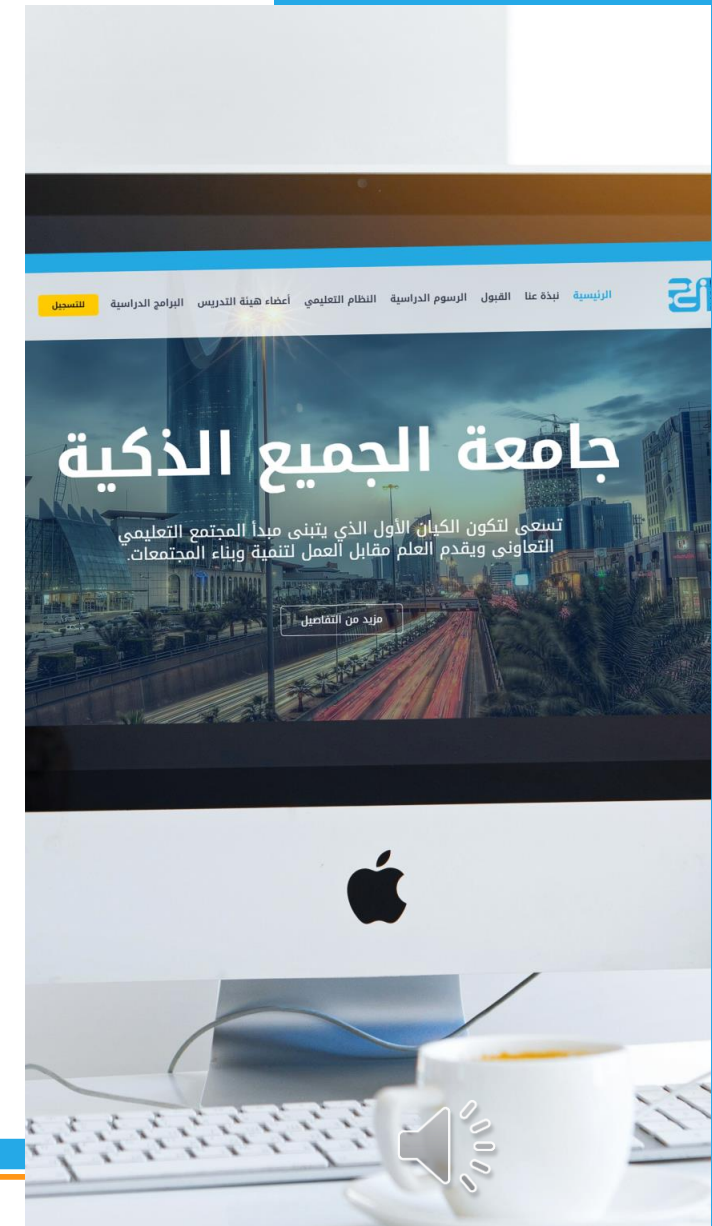
FTK image

Name	10534.gif
Type	jpg
Description	existing
Existent	✓
Size	3.0 KB (3,081)
Modified	07/12/2008 21:51:38 +0
Ext.	gif
Type status	mismatch detected, OK
Type descr.	JPEG



Lecture 2

Post-investigation phase



5. Reporting your findings

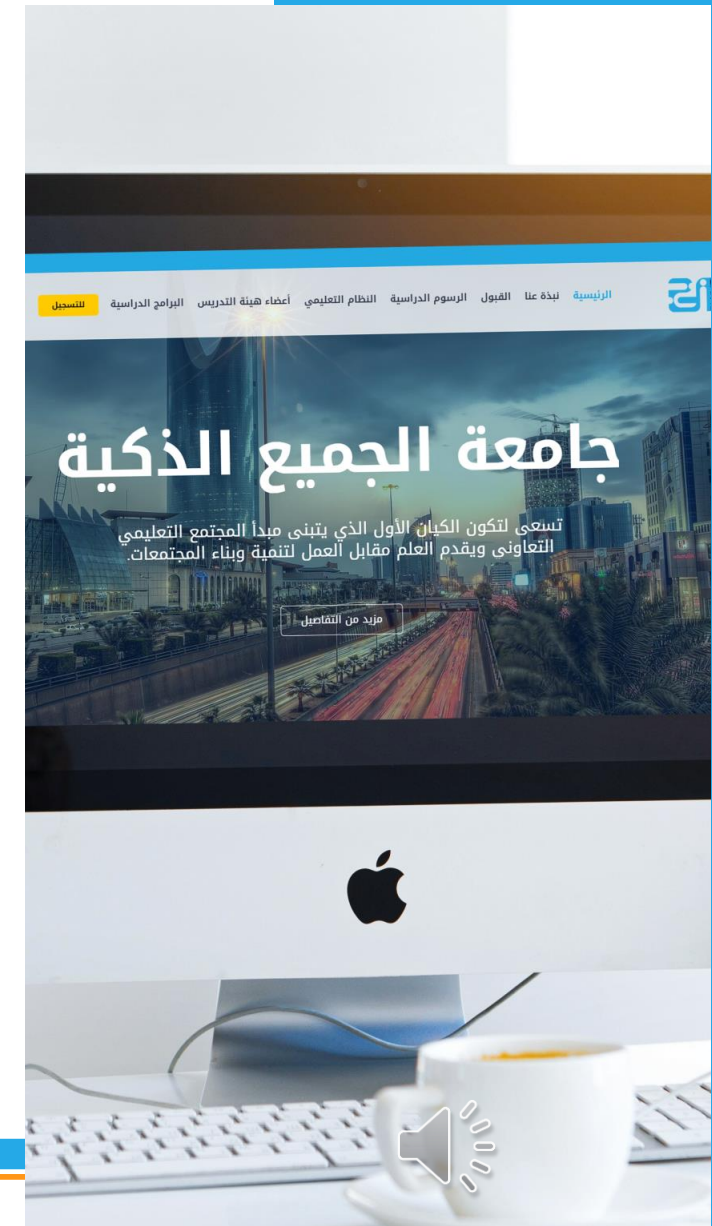
Post-
Investigation
Phase

- Communication between the primary **investigator** and **prosecutor**
- Personal identifiers of the suspect, victim, and witness
- The forensic hardware used
- The forensic software used
- What you examined (even if the examination turned up nothing of evidentiary value)
- Your findings



Lecture 2

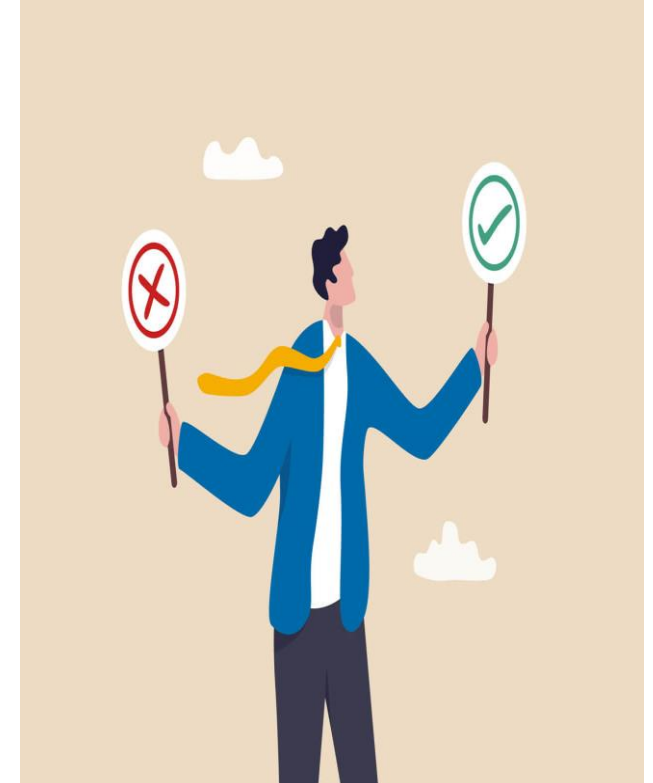
The Investigator



- Digital forensics investigators mainly work to retrieve, catalog, and safeguard digital data related to cybercrime investigations.
- They also preserve evidence to ensure its admissibility in court.
- They may also advise other investigators about the value of digital evidence

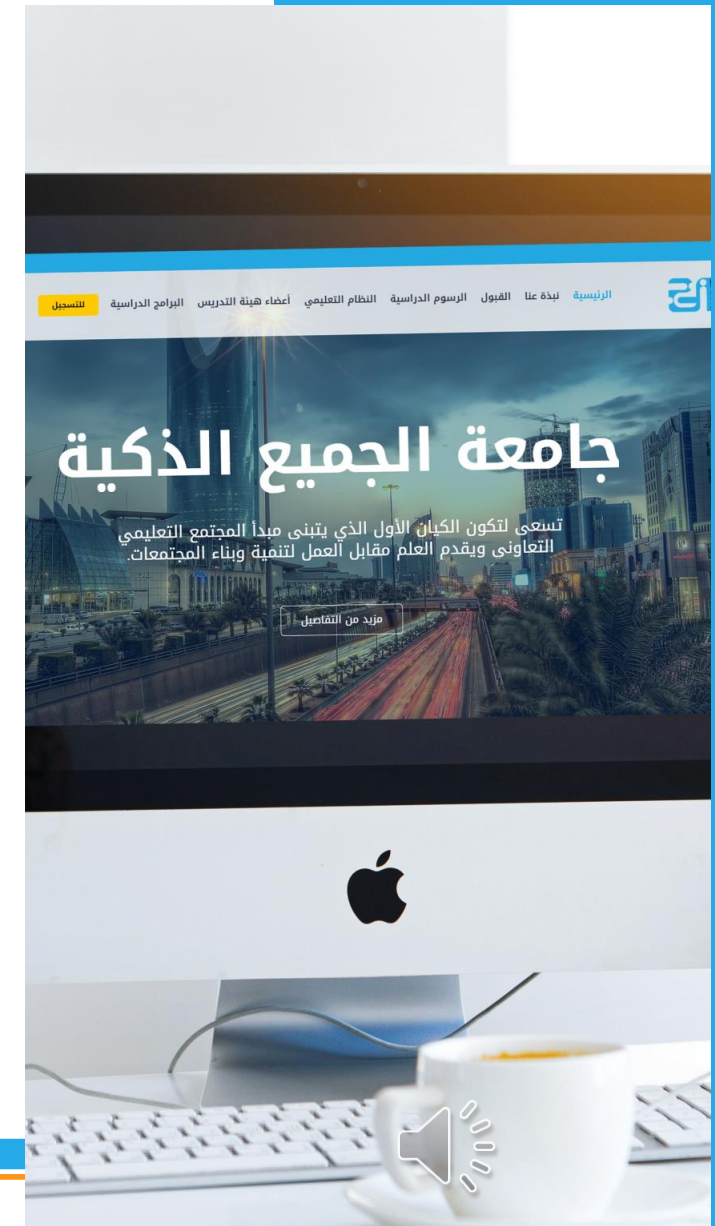


- International Association of Computer Investigative Specialists (IACIS) The IACIS provides a clear guide for ethical behavior of computer forensics investigators.
- The guidelines for IACIS's members that apply to testifying include:
 - ☐ Members should maintain the utmost objectivity in all forensics investigations and present the facts accurately.
 - ☐ The evidence should be examined and analyzed thoroughly.
 - ☐ Only unbiased opinions should be given.
 - ☐ Members must not conceal any findings that would cause the facts of a case to be distorted or misrepresented.

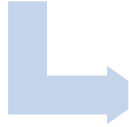


Lecture 2

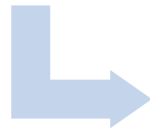
Systematic Approach



Make an initial assessment about the type of case you're investigating : type of case , talk to others involved in the case and ask questions about the incident. law enforcement.



Determine a preliminary design or approach to the case : Outline the general steps you need to follow to investigate the case.

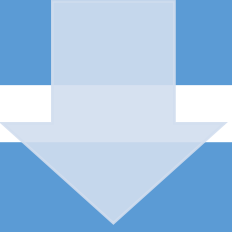


Create a detailed checklist—Refine the general outline by creating a detailed checklist of steps and an estimated amount of time for each step.



Taking a Systematic Approach

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 : you might be seizing multiple computers along with CDs, DVDs, USB drives, mobile devices, and other removable media.



Identify the risks—List the problems you normally expect in the type of case you're handling.



Mitigate or minimize the risks—Identify how you can minimize the risks.



Test the design—Review the decisions you've made and the steps you've completed.



Analyze and recover the digital evidence—Using the software tools and other resources



Taking a Systematic Approach

Investigate the data you recover—View the information recovered from the disk, including existing files, deleted files, e-mail, and Web history.

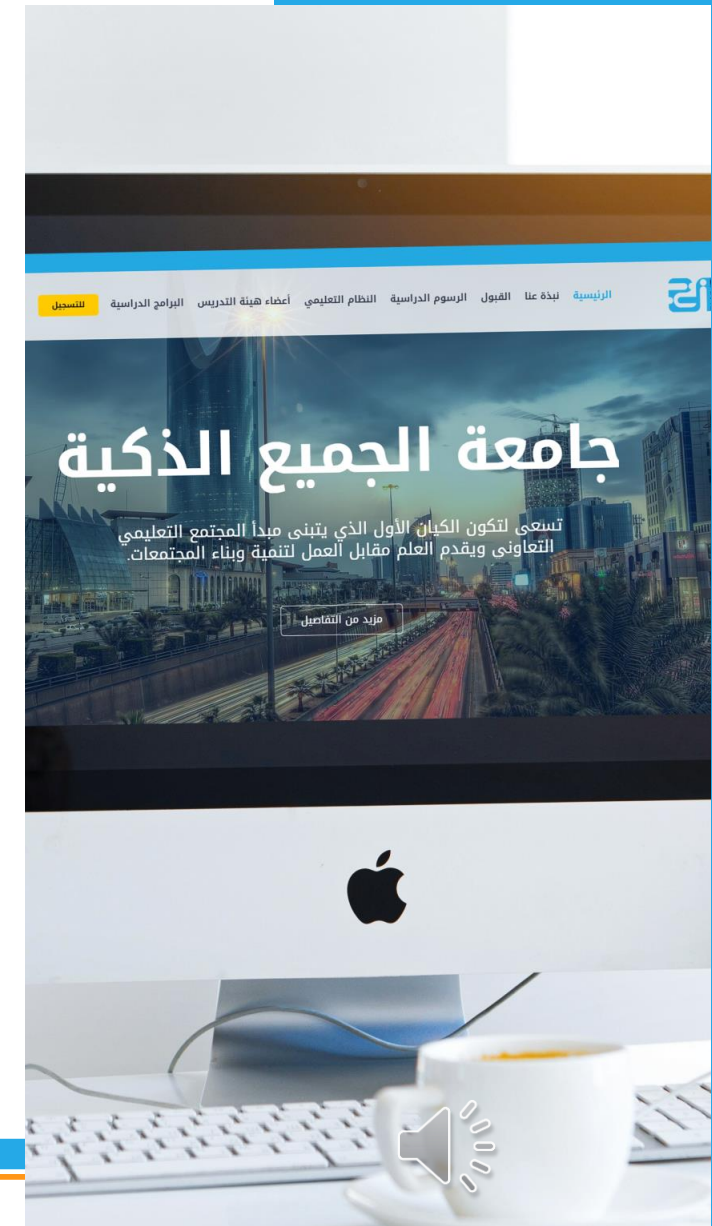
Complete the case report—Write a complete report detailing

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



Lecture 2

Evidence Custody form



Evidence Custody Form

- An **evidence custody form** helps you document what has been done with the original evidence and its forensics copies
- Two types
 - **Single-evidence form**
 - Lists each piece of evidence on a separate page
 - **Multi-evidence form**



Evidence Custody Form

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)
CD-001	1	Ultimate DVD contains servers log from AD001
HD-001	1	Samsung SSD 1TB Ser#ABC9876
HD-002	1	Samsung SSD 512 MB Ser# DEF4567
CP-001	1	Pixel XL 128 MB Ser# A5 12 D3 AC FD
TD-001	1	Generic Thumb drive 32MB (green) unknown SN
MD-001	1	Apple iPad 512mb Ser# 09 E3 4D AB Rose Gold

- A description of the evidence



I use the following numbering system as a part of my process:

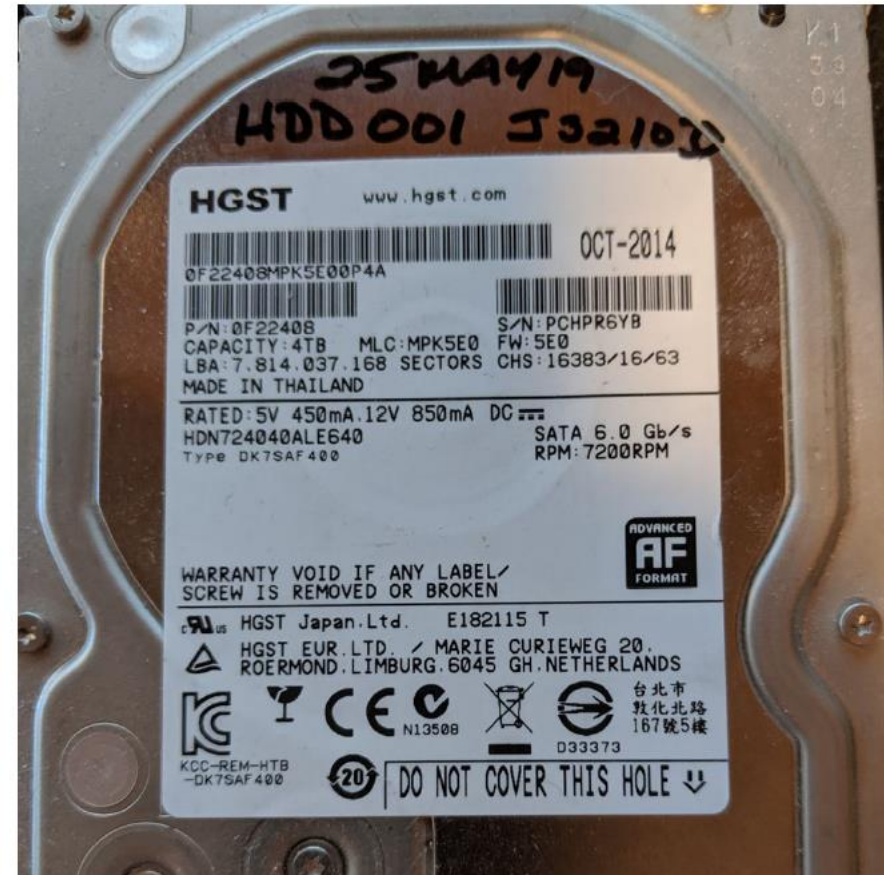
CD/DVD: **CD-XXX**

Hard drive: **HD-XXX**

Thumb drive: **TD-XXX**

Cellphone: **CP-XXX**

Mobile device (not a cellphone): **MD-XXX**



Evidence Custody Form

EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Offense: _____
 Submitting Officer: (Name/ID#) _____
 Victim: _____
 Suspect: _____
 Date/Time Seized: _____ Location of Seizure: _____

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)
CD-001	1	Ultimate DVD contains servers log from AD001
HD-001	1	Samsung SSD 1TB Ser#ABC9876
HD-002	1	Samsung SSD 512 MB Ser# DEF4567
CP-001	1	Pixel XL 128 MB Ser# A5 12 D3 AC FD
TD-001	1	Generic Thumb drive 32MB (green) unknown SN
MD-001	1	Apple iPad 512mb Ser# 09 E3 4D AB Rose Gold

– A description of the evidence



Evidence Custody Form

- **Case number**—The number your organization assigns when an investigation is initiated.
- **Investigating organization**—The name of your organization
- **Investigator**—The name of the investigator assigned to the case.
- **Nature of case**—A short description of the case.
- **Location evidence was obtained**—The exact location where the evidence was collected

EVIDENCE CUSTODY FORM			
Case ID		Evidence Item #	1
Case Lead Investigator			
Nature of Case:			
Source location of Evidence:			
Evidence Initially Recovered at <u>source location</u> by:			
☐ EDI Chief Lead Investigator (see above) ☐ Other EDI Staff: _____ ☒ Other (name/title/company/contact information including full address and phone #): _____			
Date		Time	
If evidence not directly secured by Case Lead Investigator or EDI staff <u>at the source location listed above</u> , complete the shaded section at the time the evidence is turned over to EDI:			
Evidence Provided to EDI By:			
(print name)		(signature)	
(title)		(company)	
(full address)			
(phone #)			
Was receipt given? yes ☐ no (explain):			
Evidence Provided to EDI Staff Listed Below:			
Name:			
Date	Time	Place	
Description of Evidence			



Evidence Custody Form

- **Description of evidence**—A list of the evidence items, such as “hard drive, 250 GB- On a multi-evidence form, write a description for each item of evidence
- **Vendor name**—The name of the manufacturer of the computer component.
- **Model number or serial number**—List the model number or serial number (if available)
- **Evidence recovered by**—The name of the investigator who recovered the evidence
- **Date and time**—The date and time the evidence was taken into custody.



Evidence Custody Form

- **Evidence placed in locker**—Specifies which approved secure 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**



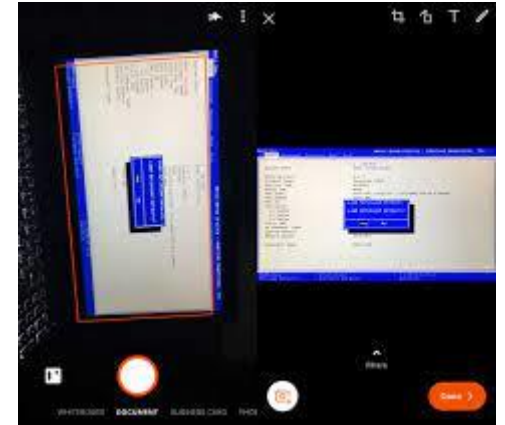
Securing Your Evidence

- Use **evidence bags** to secure and catalog the evidence
- Use computer safe products when collecting computer evidence
 - Antistatic bags
 - Antistatic pads
- Use well padded containers
- Use evidence tape to seal all openings
 - CD drive bays
 - Insertion slots for power supply electrical cords and USB cables



For proper evidence preservation, follow these procedures in order:

- Do not use the computer or attempt to search for evidence.
- Photograph the surrounding area prior to moving any evidence.
- Photograph the front and back of the computer and diagram/label cords and connected devices.
- If the computer is OFF, leave it OFF.
- If the computer is on and something is displayed on the monitor, photograph the screen.



- If the computer is on and the screen is blank, move the mouse or press the space bar (this will display the active image on the screen). After the image appears, photograph the screen.
- If the computer is on and a Computer Forensic Examiner/Analyst is available, consider conducting a volatile memory (RAM) acquisition to capture the data that may be lost when powered off.



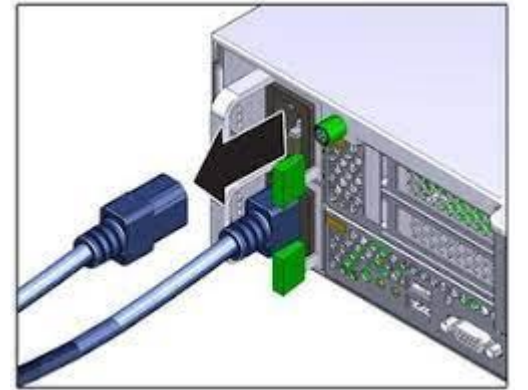
- If the computer is on and networked (attached to a network device such as a router and/or modem) and a Computer Forensic Examiner/Analyst is available consider capturing the volatile network information (IP addresses, open ports, active network connections) and network logs if applicable.
- If networked, unplug the power to the network device(s), and record the MAC address(es) from the device(s).



- If the laptop computer does not shutdown when the power cord is removed, locate and remove the battery.
- The laptop computer battery is commonly located on the bottom and there is usually a button or switch that allows for the removal of the battery.
- If the laptop computer battery cannot be removed (Apple MacBooks, etc.), shut down the computer as normal.
- If the laptop computer battery is removed, do not return it to the battery compartment.



- Disconnect all cords and devices from the computer.
- Package components and transport/store as fragile cargo.
- Keep all computers and electronic storage media away from magnets, radio transmitters (such as police radios - portable or vehicle based) and other potentially damaging elements.



- Collect instruction manuals, documentation, and notes (notes may contain passwords).
- Document all steps involved in the seizure of the computer and components.



- <https://resources.infosecinstitute.com/topic/computer-forensics-legal-ethical-principles/>
- <https://info-savvy.com/forensics-investigation-method-of-computer/>
- “ Best Practices For Seizing Electronic Evidence” , v. 4.2 , U.S. Department of Homeland Security , United States , Secret Service