LEARNING OBJECTIVES(LO)

The learning objectives of this module are to:

- ✓ LO#01: Understand the Fundamentals of Computer Forensics
- ✓ LO#02: Understand Cybercrimes and their Investigation Procedures
- ✓ LO#03: Understand Digital Evidence and eDiscovery
- ✓ LO#04: Understand Forensic Readiness
- ✓ LO#05: Understand the Role of Various Processes and Technologies in Computer Forensics
- ✓ LO#06: Identify the Roles and Responsibilities of a Forensic Investigator
- ✓ LO#07: Understand the Challenges Faced in Investigating Cyber Crimes
- ✓ LO#08: Understand Various Standards and Best Practices Related to Computer Forensics
- ✓ LO#09: Understand Laws and Legal Compliance in Computer Forensics

Understanding Computer Forensics

- Computer forensics refer to a set of **methodological procedures** and **techniques** that help identify, gather, preserve, extract, interpret, document, and present evidence from computing equipment, such that any discovered evidence is acceptable during a legal and/or administrative proceeding

Objectives:

- To track and **prosecute** the **perpetrators** of a cyber crime
- To gather evidence of cyber crimes in a forensically sound manner
- To estimate the potential impact caused by the incident on the victim and **determine** the **intent** of the **perpetrator**
- To minimize the tangible and intangible losses to the organization
- To **protect** the organization from similar incidents in the future

Scope of Computer Forensics

- Computer forensics has a wide scope in investigating, analyzing, and extracting data from the digital evidence acquired from the crime scenes

Some of the important areas the computer forensics has huge scope

Digital Crime Investigations

Computer forensic techniques used to identify the **culprit** by analyzing the digital evidence

Malware Analysis

Used to analyze the **malware-infected systems** and to examine the malware samples to determine their **behavior**

Incident Response

Used to analyze cyberattacks to determine the **root cause** of the incident

Corporate Investigations

Helps organizations to **investigate cyberattacks** and helps in resolving them

eDiscovery

Used to identify, collect, preserve, and analyze digital evidence in support to **regulatory compliance** and **litigations**

Collaboration with Law Enforcement Agencies

Supports organizations in collaborating with the **law enforcement agencies** during the prosecution and building cases

LO#02: Understand Cybercrimes and their Investigation Procedures

- Types of Cybercrimes
  - Examples of Cybercrimes
- Cyber Attribution
- Cybercrime Investigation
  - Civil vs. Criminal Investigation
  - Administrative Investigation

Types of Cybercrimes

- Cybercrime is defined as **any illegal act** involving a computing device, network, its systems, or its applications

Cybercrime can be categorized into two types based on the line of attack:

Internal/Insider Attack

- Performed on a corporate network or on a single computer by an **entrusted person (insider)** who has authorized access to the network
- Such **insiders** can be former or current employees, business partners, or contractors

External Attack

- Occurs when an **attacker from outside the organization** tries to gain unauthorized access to their computing systems or informational assets
- The attackers **exploit security loopholes** or use **social engineering techniques** to infiltrate the network

Examples of Cybercrimes

1. Espionage
2. Theft of Intellectual Property
3. Manipulation of Data
4. Trojans Horse Attack
5. SQL Injection Attack
6. Brute-force Attack
7. Phishing/Spoofing
8. Privilege Escalation Attack
9. Denial-of-Service Attack
10. Cyber Defamation
11. Cyberterrorism
12. Cyberwarfare

Cyber Attribution

- Cyber attribution is a process of technical methods and organizational measures for **discovering**, **tracing**, and **inculpate** the responsible individual or groups for cyberattacks or malicious campaigns
- Organizations conducts investigations to attribute the cyberattack to an attacker and get a **complete procedural frame of attack** for bringing them in front of **justice**

Cyber Attribution Techniques

1. Use various **forensic analysis tools**, recovery tools, scripts, or applications to obtain relevant and important information about a cyberattack
2. Analyze **technical indications** such as malicious code, command and control infrastructure, digital signatures, and network traffic patterns
3. Understand the **past attacks** and **their motivations** to analyze the behavior of threat actors and to build threat actor profiles for attribution

Cybercrime Investigation

- The investigation of any crime involves the **meticulous collection of clues** and **forensic evidence** with attention to detail
- Inevitably, at least one **electronic device** will be **found** during the investigation, such as a computer, a mobile device, a printer, or an IoT/OT device
- The electronic device acquired from the crime scene might **contain valuable evidence** and play a major role in solving the case
- Therefore, the information contained in the device must be **investigated** in a forensically sound manner in order to be accepted by the court of law
- The different types of approaches to manage cybercrime investigation include **civil**, **criminal**, and **administrative**
- **Processes** such as collection of data, analysis, and presentation **differ based on the type of case**

Civil vs. Criminal Investigation

- Civil cases are brought for **violation of contracts and lawsuits**, where a guilty outcome generally results in **monetary damages** to the plaintiff, whereas criminal cases are generally brought by law enforcement agencies in response to a **suspected violation of law**, where a guilty outcome may result in **monetary damages**, **imprisonment**, or **both**

Criminal Cases

- Investigators must follow a set of standard forensic processes accepted by law in the respective jurisdiction
- Investigators, under a court's warrant, have the authority to **forcibly seize** computing devices
- A **formal** investigation report is required
- **Law enforcement agencies** are responsible for collecting and analyzing evidence
- Punishments are harsh and include a **fine**, **jail sentence**, or **both**

Civil Cases

- Investigators try to show the opposite party some proof to support the claims and induce settlement
- Searching of the devices is generally based on **mutual understanding**
- The initial reporting of the evidence is generally **informal**
- The **claimant** is responsible for the collection and analysis of the evidence
- Punishments include **monetary compensation**

Administrative Investigation

- Administrative investigation refers to an **internal investigation** by an **organization or government** agency to discover if their employees, clients, and partners are complying with the rules or policies

- Administrative investigations are **non-criminal in nature** and are related to misconduct or activities of an employee that include, but are not limited to:
  - Violation of organization's policies, rules, or protocols
  - Violation of regulatory or legal requirements
  - Resource misuse or damage or theft
  - Threatening or violent behavior
  - Improper promotion or pay raises

- Any **violation** may **result** in **disciplinary action** such as demotion, suspension, revocation, penalties, and dismissal

- The investigations are carried out by internal teams such as compliance department, human resources, and internal affairs unit dedicated for this purpose

LO#03: Understand Digital Evidence and eDiscovery

- Introduction to Digital Evidence
- Types of Digital Evidence
- Roles of Digital Evidence
- Sources of Potential Evidence
- Rules of Evidence
- Best Evidence Rule
- Federal Rules of Evidence (United States)
- The ACPO Principles of Digital Evidence
- Computer Forensics vs. eDiscovery
- Legal and IT Team Considerations for eDiscovery
- Best Practices for Handling Digital Evidence

Introduction to Digital Evidence

1. Digital evidence refers to any **electronic data** or **information** that can be collected and used in legal proceedings to support or prove a case

2. Digital evidence includes information that is either stored or transmitted in digital form and has probative value

3. Digital information may be found while examining digital **storage** media, **monitoring** the network traffic, or making duplicate copies of digital data found during a forensics investigation

4. Digital evidence is **circumstantial** and **fragile** in nature, which makes it difficult for a forensic investigator to trace criminal activities

5. According to **Locard's Exchange Principle**, "anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave"

Types of Digital Evidence

Volatile Data

- Data that are **lost as soon as the device is powered off**; examples include system time, logged-on user(s), open files, network information, process information, process-to-port mapping, process memory, clipboard contents, service/driver information, command history, etc.

Non-volatile Data

- Permanent data **stored on secondary storage** devices such as hard disks solid-state drives, and flash drives; examples include hidden files, slack space, swap file, index.dat files, unallocated clusters, unused partitions, hidden partitions, registry settings, event logs, etc.

Roles of Digital Evidence

C|HFI Computer Hacking Forensic INVESTIGATOR

Proof of an Act

- Proof that a **specific action** took place, such as unauthorized access, malware injection, or data exfiltration

Corroborative and Contradictory Evidence

- Support other **pieces of evidence** or testimony
- Challenge statements or **other evidence presented** in a case

Linking Evidence

- Link suspects to **crime scenes**, **victims**, or other suspects
- For example, **shared digital artifacts** could link two devices that were part of the same cyberattack

Exculpatory Evidence

- Exonerate someone from blame
- For example, digital records might show that an accused person was not active on their device at the time of crime

Contextual Evidence

- Provides **context to actions** or **events**, helping to obtain a clearer picture of what transpired

Timeline Construction

- Construct a sequence of events or timeline using system/application logs, metadata, and other timestamps

Identity Verification

- Identify unknown victims or suspects based on personal information found on devices or online

Policy and Compliance Verification

- Determine if employees are adhering to company policies or legal regulations

Sources of Potential Evidence

CHFI Computer Hacking Forensic INVESTIGATOR

User-Created Files

- Address books
- Database files
- Media (images, graphics, audio, video, etc.) files
- Documents (text, spreadsheet, presentation, etc.) files
- Internet bookmarks, favorites, etc.
- Emails and cloud storage files
- Hidden partitions

User-Protected Files

- Compressed files
- Misnamed files
- Encrypted files
- Password-protected files
- Hidden files
- Steganography
- Blockchain ledgers

Computer-Created Files

- Backup files
- Log files
- Configuration files
- Printer spool files
- Cookies
- Swap files
- System files
- History files
- Temporary files

Sources of Potential Evidence (Cont'd)

Device	Location of Potential Evidence
Hard Drive	Text, picture, video, multimedia, database, and computer program files
Thumb Drive, Removable Storage Device and Media	Text, graphics, image, and picture files
Memory Card	Event logs, chat logs, text files, image files, picture files, social media logs, and Internet browsing history
Smart Card	Evidence is found by recognizing or authenticating the information of the card and the user, through the level of access, configurations, permissions, and in the device itself
Dongle	Connection records, IMEI and SIM information, cached data, and file artifacts
Biometric Scanner	Biometric traits, access logs, authentication records
Answering Machine	Voice recordings such as deleted messages, last called number, memo, phone numbers, and tapes
Digital Camera/Surveillance Cameras	Images, video, sound, time, date stamp, etc.
Random Access Memory (RAM) and Volatile Storage	Evidence is located and can be acquired from the main memory of the computer

Sources of Potential Evidence (Cont'd)

Device	Location of Potential Evidence
Handheld Devices	Address book, appointment calendars or information, documents, email, handwriting, password, phone book, text messages, and voice messages
Local Area Network (LAN) Card/ Network Interface Card (NIC)	MAC address, assigned IP address, network configurations, connection logs, and DHCP records
Routers, Modem, Hubs, and Switches	For routers, evidence is found in the configuration files For hubs, switches, and modems evidence is found on the devices themselves
Server	Log files, access records, backup and recovery files, cronjobs, email, and database records
Printer	Evidence is found through usage logs, time and date information, and network identity information
Internet of Things and Wearables	Evidence can be acquired in the form of GPS, audio and video recordings, cloud storage sensors, notification logs, etc.
Global Positioning Systems (GPS)	Evidence is found through previous destinations, way points, routes, travel logs, etc.
Telephones	Evidence is found through names, phone numbers, caller identification information, and last called number

Sources of Potential Evidence (Cont'd)

Device	Location of Potential Evidence
Credit Card Skimmers	Evidence is found through card expiration date, user's address, credit card numbers, user's name, etc.
Digital Watches	Evidence is found through address books, notes, appointment calendars, phone numbers, emails, notification logs, GPS locations, etc.
Messaging Apps (WhatsApp, Telegram, Signal, etc.)	Contact ID, contacts, chat history, status, display name, timestamps, message body, attached files, images, video and audio messages, profile pictures, logs, calls list, geodata, etc.
VoIP systems (like Skype)	User accounts, call list, messages, group chat, contacts, file transfers, voicemails, SMS messages, etc.
Databases	Primary data files, secondary data files, transaction log files, performance statistics, etc.
Web-Based Platforms (Social Media, Forums, and E-commerce)	Profile information, recent logins, status updates, notes, mini-feed, shares, posts, friends list, connections, groups, events, videos, pictures, applications, message inbox (received messages), message outbox (sent messages), users' comments, transactions, wishlist, etc.
ATMs and Point of Sale (POS) Systems	Transaction records, device owner address and phone number, terminal ID, debit or credit card details, authorization number, batch number, etc.
Virtual Environments	Routers, Firewalls and proxy logs, captured network traffic, wireless networks artifacts connected to a system such as profile GUID, profile name, description, first network, MAC address, DNS suffix, etc.
Blockchain and Cryptocurrencies	Browser history searches, addresses or crypto transactions, origin, number of tokens, ownership, transaction details, etc.

Rules of Evidence

Digital evidence collection must be governed by **five basic rules** that make it **admissible in a court of law:**

1 Understandable

Evidence must be **clear and understandable** to the judges

2 Admissible

Evidence must be **related to the fact** being proved

3 Authentic

Evidence must be **real and** appropriately **related** to the incident

4 Reliable

There must be no doubt about the **authenticity or veracity** of the evidence

5 Complete

The evidence must prove the attacker's **actions or** his/her **innocence**

6 Materiality

The evidence should pertain directly to a particular **matter at issue** in the case

Best Evidence Rule

- It states that the court only allows the **original evidence of a document, photograph, or recording** at the trial rather than a copy. However, the duplicate can be accepted as evidence, provided the court finds the party's reasons for submitting the duplicate to be genuine

- The principle underlying the best evidence rule is that the original evidence is considered as the best evidence

Federal Rules of Evidence (United States)

Federal Rules of Evidence	Rule Description
Rule 102: Purpose	These rules should be construed so as to administer every **proceeding fairly**, eliminate **unjustifiable expense** and **delay**, and promote the **development of evidence law**, to the end of ascertaining the truth and securing a just determination
Rule 103: Rulings on Evidence	(a) Preserving a Claim of Error (b) No Need to Renew an Objection or Offer of Proof (c) Court's Statement About the Ruling; Directing an Offer of Proof (d) Preventing the Jury from Hearing Inadmissible Evidence (e) Taking Notice of Plain Error
Rule 104: Preliminary Questions	• Questions of admissibility in general • Relevancy conditioned on a fact • Conducting a hearing so that the jury cannot hear it • Cross-examining a defendant in a criminal case • Evidence relevant to weight and credibility
Rule 105: Limited Admissibility	When evidence that is admissible as to one party or for one purpose but not admissible as to another party or for another purpose is admitted, the court, upon request, **shall restrict the evidence** to its proper scope and instruct the jury accordingly
Rule 801: Hearsay Rule	• Hearsay is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to **prove the truth** of the matter asserted • It is not admissible except as provided by these rules or by other rules prescribed by the Supreme Court pursuant to statutory authority or by Act of Congress
Rule 801: Statements That Are Not Hearsay	• Prior statement **by witness** • Admission by party-opponent

https://www.rulesofevidence.org

Federal Rules of Evidence (US) (Cont'd)

Federal Rules of Evidence	Rule Description
Rule 803: Hearsay Exceptions - Availability of Declarant Immaterial	Even if the declarant is available as a witness, some of them are not excluded by the Hearsay Rule: • Present sense impression • Excited utterance • Statements for purposes of medical diagnosis or treatment • Recorded recollection • Records of regularly conducted activity • Absence of entry in records kept in accordance with the provisions • Public records and reports • Records of vital statistics
Rule 804: Hearsay Exceptions; Declarant Unavailable	If the declarant is unavailable as a witness, the following are not excluded by the Hearsay Rule: • Former testimony • Statement under belief of impending death • Statement against interest • Statement of personal or family history
Rule 1001: Definitions that apply to this article	This rule is related to the contents of writings, recordings, and photographs: *https://www.rulesofevidence.org* A. A 'writing' consists of letters, words, numbers, or their equivalent set down in any form. B. A 'recording' consists of letters, words, numbers, or their equivalent recorded in any manner. C. A 'photograph' means a photographic image or its equivalent stored in any form. D. An 'original' of a writing or recording means the writing or recording itself or any counterpart intended to have the same effect by the person who executed or issued it. A 'duplicate' means a counterpart produced by a mechanical, photographic, chemical, electronic, or other equivalent process or technique that accurately reproduces the original."

Federal Rules of Evidence (US) (Cont'd)

Federal Rules of Evidence	Rule Description
Rule 1002: Requirement of Original	"An original writing, recording, or photograph is required in order to prove its content unless these rules or a federal statute provides otherwise."
Rule 1003: Admissibility of Duplicates	A duplicate is admissible to the same extent as an original unless • A genuine question is raised as to the authenticity of the original, or • In the circumstances it would be unfair to admit the duplicate in lieu of the original
Rule 1004: Admissibility of Other Evidence of Contents	The original is not required, and other evidence of the contents of a writing, recording, or photograph is admissible if: a. Originals are lost or destroyed. All originals are lost or have been destroyed, unless the proponent lost or destroyed them in bad faith b. Original is not obtainable. No original can be obtained by any available judicial process or procedure c. Original is in possession of the opponent. At the time when an original was under the control of the party against whom offered, that party was put on notice, by the pleadings or otherwise, that the contents would be a subject of proof at the hearing, and that party does not produce the original at the hearing d. Collateral matters. The writing, recording, or photograph is not closely related to a controlling issue

https://www.rulesofevidence.org

The Association of Chief Police Officers (ACPO) (inherited into NPCC) Principles of Digital Evidence

- **Principle 1**: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be **relied upon in court**

- **Principle 2**: In exceptional circumstances, where a person finds it necessary **to access original data** held on a computer or on storage media, that person must be competent to do so and be able to explain his/her actions and the impact of those actions on the evidence, in the court

- **Principle 3**: An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An **independent third party** should be able to examine those processes and achieve the same result

- **Principle 4**: The person in charge of the investigation (the case officer) has overall responsibility for **ensuring that the law and these principles** are adhered to

https://www.npcc.police.uk

Computer Forensics vs. eDiscovery

- eDiscovery focuses on obtaining artifacts relevant to the **investigational needs** whereas computer forensics concentrates on finding potentially relevant electronic information to **discover security incidents**
- eDiscovery uses the **Federal Rules of Civil Procedure**, whereas digital forensics follows the **Federal Rules of Criminal Procedure**
- In eDiscovery, investigators deal with only **existing data** to arrive at conclusions. But digital forensics involves carving and recovery techniques to **retrieve deleted files** from the evidence
- eDiscovery process is mainly carried out in **civil cases** while Computer forensic investigations take place mostly in **criminal cases** such as security breaches
- Investigators should follow a **strict-documented procedure** in digital forensic investigation while following **high standards are not required** in eDiscovery

Legal and IT Team Considerations for eDiscovery

- Organizations should build an **in-house eDiscovery team** or avail services from **external eDiscovery service** providers to effectively carry out eDiscovery process

Considerations for Forming an eDiscovery Team

Legal Expert or eDiscovery Attorney

- Define the scenarios for evidence gathering

Project Manager

- Manage eDiscovery process and interact with stakeholders

Team Leads

- Manage workflow of the team to achieve the goals within deadlines

IT Support Personnel

- Deal with all technical issues and necessities during eDiscovery

Processing/Review Personnel

- Find relevant artifacts from the collected data

eDiscovery Software Expert

- Perform deployment and maintenance of eDiscovery tools

IT Professionals

- Collect electronically stored information from potential sources of evidence and preserve them

eDiscovery Service Provider

- Provides assistance to the in-house eDiscovery teams in all stages of eDiscovery

Best Practices for Handling Digital Evidence

C|HFI

01 Maintain a **detailed record** of every individual who has had possession of the evidence

02 Document the **date**, **time**, **purpose**, and any **actions** taken when the evidence is accessed

03 Establish a **digital log** to record and track all events related to the evidence data

04 Avoid unnecessary handling or alteration of the original evidence

05 Use **forensically sound tools** and techniques to acquire digital evidence

06 Generate **cryptographic hash** values for each electronic evidence

07 Store original evidence in a **secure location** with restricted access to prevent tampering

08 Use **write blockers** when accessing storage media to prevent accidental data writes

09 Document every step of the evidence handling process

10 Store digital evidence in **anti-static bags**

11 Limit access to digital evidence to **authorized individuals** only

12 Use **secure methods**, such as encryption, to protect sensitive data

LO#04: Understand Forensic Readiness

- Forensic Readiness
- Forensic Readiness and Business Continuity
- Forensic Readiness Planning
- Forensic Readiness Procedures

Forensic Readiness

- Forensic readiness refers to an organization's ability to **optimally use digital evidence** in a limited time and with minimal investigation costs
- It includes **technical** and **non-technical actions** that maximize an organization's competence in using digital evidence

Goals of Forensic Readiness

1. Act as a deterrent against the risks from internal and external threats
2. Collect acceptable evidence in a forensically sound manner without interfering with the business processes
3. Collect evidence focusing on potential crimes and disputes that may have an adverse impact on an organization
4. Conduct an investigative process at a cost proportional to the incident
5. Ensure that the evidence has a positive impact on the outcome of any legal action
6. Extend the target of information security to the wider threats from cybercrime

Forensic Readiness (Cont'd)

C|HFI

Key Principles of Forensic Readiness

Clear Business Objectives	Ensure compliance with regulations, protect intellectual property, support disciplinary actions, or to prosecute offenders
Comprehensive Policy	Define and maintain a clear policy on the collection and use of digital evidence
Evidence Collection	Ensure that data is collected in a forensically sound manner
Secure Storage	Maintain secure storage for potential evidence
Chain of Custody	Establish and follow a process that tracks how evidence is handled and by whom
Regular Audit and Review	Review and audit the forensic readiness processes to ensure they meet the current needs and challenges of the organization
Legal/Regulatory Awareness	Know how long certain types of data need to be stored, the right to privacy, and any other legal obligations related to evidence
Incident response integration	Ensures that when an incident does occur, the organization is prepared not only to handle the incident but also to collect and manage any associated evidence

Forensic Readiness and Business Continuity

1. Incident response plan of an organization must include both forensic readiness and business continuity as they ensure **proper collection** and **storage of evidence** and restore the business operations respectively
2. An organization can include data backup strategies in their business continuity plan, which can help to **restore the business operations** and become an important source of evidence during an investigation
3. Ensure that both the business continuity and forensic readiness plans use proper channels for **establishing secure communication** as the team will have to share sensitive information
4. Organizations should also introduce **mock drills for practicing forensic readiness** that may include collection of evidence, analysis, etc. like the mock drills carried out for demonstrating business continuity
5. Organizations having preparations to handle any security incident quickly and efficiently can **maintain their market reputation** as compared to organizations that do not have any preparations or forensic readiness
6. Organizations having forensic readiness planning tend to **obtain more vital information** after recovering from an incident to prevent further incidents

Forensics Readiness Planning

Forensic readiness planning refers to a **set of processes** to be followed to achieve and maintain forensics readiness

1. Define **objectives** of forensic readiness
2. Identify the **potential evidence** required for an incident
3. Determine the **sources of evidence**
4. Define a **policy that determines the pathway** to legally extract electronic evidence with minimal disruption
5. Establish a **policy** to **handle and store** the acquired evidence in a secure manner
6. Identify if the incident requires **full or formal investigation**
7. Create a **process** for documenting the procedure
8. Establish a **legal advisory board** to guide the investigation process
9. Keep an **incident response** team ready to review the incident and preserve the evidence
10. Designate **roles and responsibilities** for evidence collection, preservation, and analysis

Forensic Readiness Procedures

Forensic Policy	A set of procedures describing the actions an organization must take to **preserve** and **extract forensic evidence** during an incident; organizations must create and implement a forensics policy for investigators to follow
Forensics in the Information System Life Cycle	To efficiently handle the numerous incidents that an organization might encounter, it is essential that **forensic considerations** be incorporated into the existing information system life cycle
Creating an Investigation Team	Create a forensic investigation team consisting of **forensic investigators**, **IT professionals**, and **incident handlers** Equip the team with **forensic tools** necessary for performing the investigation and providing basic training on the forensics methods and techniques

Forensic Readiness Procedures (Cont'd)

CHFI Computer Hacking Forensic INVESTIGATOR

Maintaining an Inventory

- Maintain an inventory, including devices, systems, and media, to **replace the compromised devices** while performing the investigation; this helps the investigator **re-create the incident scene** and quickly identify affected systems
- Maintain an up-to-date inventory of all **network devices** and **hosts**

Host Monitoring

- Create a database of **cryptographic checksums** of critical files that will help in checking file integrity after an incident
- Event logging helps in capturing security events
- Use operating system's inbuilt backup and recovery utilities or any commercial tool to perform **regular backups**

Network Monitoring

- Install and **securely configure firewalls** and intrusion detection systems to block intrusion attempts and log all allowed and blocked traffic
- Use **access control lists** on routers, firewalls, and IDS
- Deploy a **logical network topology** and create an inventory of all network devices with accurate network maps

LO#05: Understand the Role of Various Processes and Technologies in Computer Forensics

- Computer Forensics as a Part of Incident Response Plan
- Overview of Incident Response Process Flow
- Role of Computer Forensics in SOC Operations
- Role of Threat Intelligence in Computer Forensics
- Role of Artificial Intelligence in Computer Forensics
- Forensics Automation and Orchestration

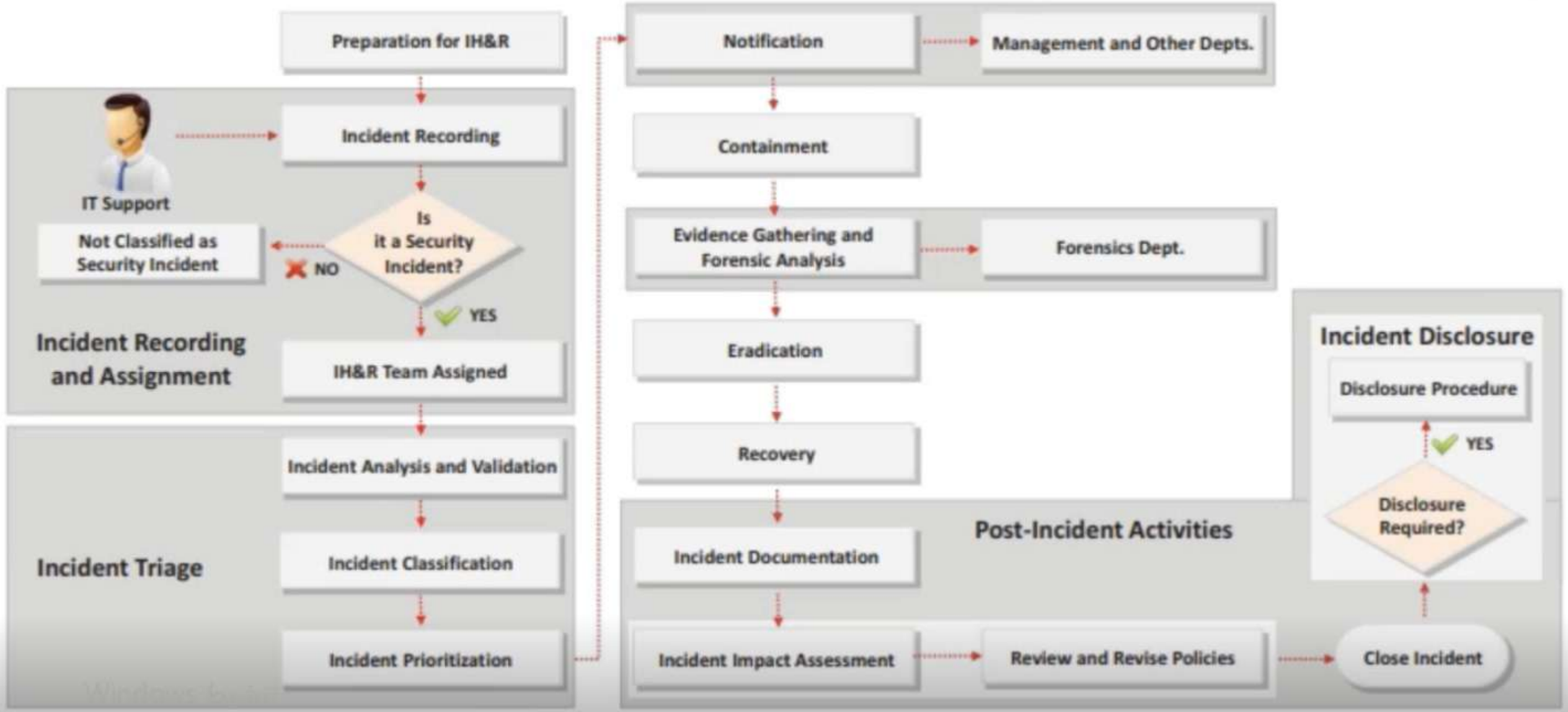
Computer Forensics as a Part of Incident Response Plan

- Integrating computer forensics within an IR plan ensures that valuable **evidence is preserved** and can be used for **post-incident analysis**, **root cause determination**, and, if necessary, **legal actions**

Role of Computer Forensics in Incident Response

1. Prepare for incidents in advance to ensure the integrity and continuity of network infrastructure
2. Provide training to the incident response team on forensic principles
3. Use forensic tools to determine if a security incident has occurred, examining logs, disk records, and other artifacts
4. Conduct a forensic analysis of the affected system to determine the nature of the incident and its impact
5. Generate a timeline for the incident that helps correlate different incidents
6. Identify and track the perpetrators of the crime or incident
7. Extract, process, and interpret the factual evidence so that it proves the attacker's actions in the court
8. Offer ample protection to data resources and ensure regulatory compliance
9. Protect organizations from similar incidents in the future
10. Minimize the tangible and intangible losses to an organization or an individual

Overview of Incident Response Process Flow



Role of Computer Forensics in SOC Operations

Incident Investigation and Analysis

- **Deep dive into incidents**: Computer forensics provides the tools and techniques necessary for a thorough investigation of security incidents
- **Determining the cause**: Forensic analysis helps in identifying the root cause of security breaches, such as vulnerabilities exploited, methods used by attackers, etc.

Evidence Preservation

- **Chain of custody**: Computer forensics ensures the integrity and admissibility of digital evidence
- **Tamper-proof documentation**: Forensic tools and techniques are used to create a tamper-proof record of security incidents, which is crucial for legal and compliance reasons

Enhanced Threat Detection and Response

- **Advanced analysis techniques**: Forensics can uncover sophisticated threat activities that might be missed by standard security tools
- **Improving response strategies**: Insights gained from forensic analysis can inform and improve an organization's response to incidents

Role of Computer Forensics in SOC Operations (Cont'd)

C|HFI Computer Hacking Forensic INVESTIGATOR

Post-incident Recovery	- **Recovery planning:** Forensic analysis provides detailed information on the extent of the damage, which aids in effective recovery and restoration of systems and data - **Lessons learned:** Post-incident reviews using forensic data can yield lessons to prevent future incidents and strengthen the organization's security posture
Compliance and Legal Requirements	- **Regulatory compliance:** Many industries have regulations that require forensic capabilities as part of their cybersecurity measures - **Legal support:** Forensics provides crucial support in legal cases involving cybercrimes, intellectual property theft, or other legal issues involving digital evidence
Training and Awareness	- **Educating the SOC team:** Forensic findings are used to educate and train SOC personnel on emerging threat patterns and attacker techniques - **Proactive threat hunting:** Forensic insights can drive proactive threat hunting initiatives within the SOC, helping to identify and mitigate hidden threats

Role of Threat Intelligence in Computer Forensics

- Integrating threat intelligence during the forensic investigation process can help investigators achieve their goals effectively and efficiently by **collecting** and **providing evidence-based information**
- Threat intelligence allow investigators to understand the attackers' **behaviors**, **attack patterns**, **targets**, and **intentions**, quickly and efficiently during an investigation

1. **Provides appropriate guidance throughout the forensic investigation process**
2. **Prevents the loss of knowledge through cause analysis**
3. **Discovers the indicators of compromise for further investigation**
4. **Identifies the threats at the early stage**
5. **Identifies the TTPs for further analysis**
6. **Allows contextual analysis of the forensic data**
7. **Recognizes and correlates the known attack patterns**
8. **Provides threat hunting abilities to forensic investigators**

Role of Artificial Intelligence in Computer Forensics

- Using AI in computer forensics can help **automate different processes** and **flag the insights quickly** and efficiently which may take a longer time using the traditional way
- It will allow the investigators to perform **live analysis**, **data recovery**, **password recovery**, **known file filtering**, **timeline analysis**, etc. effectively and instantly during an investigation

AI Techniques that can Assist in Computer Forensics

1. Automated Data Analysis
2. Knowledge Representation
3. Reasoning Process
4. Knowledge Discovery
5. Expert Systems
6. Recognizing Patterns
7. Image and Video Analysis
8. Natural Language Processing (NLP)
9. Predictive Analysis

Role of Artificial Intelligence in Computer Forensics (Cont'd)

Role of AI Tools in Computer Forensic Processes

- AI tools can **ease complex tasks** such as processing, analysis, and production of digital evidence in forensic investigations
- AI tools help forensic investigators to **effectively investigate security threats** by minimizing the investigational cost and time

Evidence Processing

- Intakes **large volumes** of data and processes only those having **relevance** to the case
- Processes text messages, videos, images, emails, and so on

Evidence Analysis

- Detects **suspicious emotional tones** in evidence
- Can **decrypt** cipher texts and analyze crime scene
- Maintains a **dataset** about post infamous cyberattacks

Evidence Production

- Utilize the **natural language generation feature** of the AI tools to create productive conclusions about relevant evidence to defend the case

Forensics Automation and Orchestration

- Forensics automation and orchestration can **assist** the investigation process with more **streamlined**, **efficient**, and **sophisticated methodologies** as compared to the traditional manual processes
- Forensics automation is the **process of automating** a single process or a smaller number of tasks, while orchestration involves managing multiple automated tasks to **create a smooth workflow**

Forensics Automation

01 Supports **automated imaging** during an investigation

02 Performs **hash analysis** to identify suspicious or malicious files automatically

03 Allows **keyword searches** while analyzing huge data sets

Forensics Orchestration

01 Optimizes and **organizes the repeated tasks** from multiple devices into a workflow

02 Assists the investigators in managing and **controlling complex workflows**

03 Integrates various forensic tools to perform the **transition of data swiftly**

LO#06: Identify the Roles and Responsibilities of a Forensic Investigator

- Need for a Forensic Investigator
- Roles and Responsibilities of a Forensics Investigator
- What Makes a Good Computer Forensics Investigator?
- Code of Ethics
- Managing Clients or Employers during Investigations
- Accessing Computer Forensics Resources

Need for a Forensic Investigator

Cybercrime Proliferation	With the rise in cybercrimes, there is a growing demand to track, understand, and prosecute these offenses
Cybercrime Investigation	Forensic investigators help organizations and law enforcement agencies investigate and prosecute the perpetrators of cybercrimes
Evidence in Digital Form	Much of today's evidence is stored electronically. This digital evidence often holds the key to many investigations
Complex Digital Environment	Navigating through modern IT environments require specialized expertise
Preservation of Evidence	Forensic investigators know how to properly collect and preserve this evidence in its original form
Legal Standards	Forensic investigators ensure evidence integrity and handle in ways that meet specific legal standards
Litigation Support	Investigators can assist in e-discovery, helping legal teams find the evidence they need
Incident Handling and Response	Forensic investigators help organizations maintain forensics readiness and implement effective incident handling and response
Expert Testimony	Forensic investigators often act as expert witnesses, explaining the evidence and its significance to a judge or jury

Roles and Responsibilities of a Forensics Investigator

1. Determines the **extent of any damage** done during the crime
2. Identifies and **recovers data** of investigative value from computing devices involved in crimes
3. **Extracts the evidence** in a forensically sound manner and ensures appropriate handling of the evidence
4. **Creates forensic images** of evidence for analysis and safeguards them to ensure the integrity of the original data
5. Reconstructs the damaged storage devices and **uncovers the information hidden** on the computer
6. Creates clear, comprehensive, and **structured investigation reports** for presentation in a court of law
7. Acts as an **expert witness** in the course, explaining the specifics of digital evidence and how it is related to the case
8. **Engages with law enforcement**, IT and legal staff; and stakeholders

What Makes a Good Computer Forensics Investigator?

- Interviewing skills to **gather** extensive **information** about the case from the client or victim, witnesses, and suspects
- Researching skills to know the background and **activities pertaining to the client** or victim, witnesses, and suspects
- Strong **analytical skills** to find the evidence and link it to the suspect
- Knowledge of various **digital technologies**, networking, hardware, and **software tools**
- Excellent **critical thinking** and **logical reasoning** skills to identify inconsistencies or anomalies in the collected evidence
- Ability to **control emotions** when dealing with issues that induce anger
- Multi-discipline expertise related to both **criminal** and **civil cases**
- Ability to explain the specifics of forensic investigation findings to non-technical personnel

Code of Ethics

- Code of ethics for computer forensics investigators ensures that they operate with the highest standards of **integrity**, **impartiality**, and **professionalism**

Computer forensic investigator should

- Act in accordance with federal statutes, state statutes, and local laws and policies
- **Testify honestly** before any board, court or trial proceedings
- Always provide **truthful** and **accurate** information
- Avoid biases, conflicts of interest, or any **external influences**
- Respect and protect the **privacy rights** of clients and involved parties
- Maintain a clear **chain of custody** for all evidence to ensure its authenticity and integrity

Computer forensic investigator should not

- Refuse any evidence because that may **cause failure** in the case
- Disclose any information without proper **authorization**
- Take on assignments beyond his/her **skills**
- Perform actions that significantly leads to a **conflict of interest**
- Provide personal or **prejudiced** opinions
- **Retain** any evidence relevant to the case
- Make early or premature assumptions without performing a thorough analysis

Managing Clients or Employers during Investigations

- Managing clients or employers during a forensic investigation requires a blend of **technical acumen**, **communication skills**, and **professional ethics**

Best Practices for Managing Clients or Employers During Investigations

Clear Communication

- Clarify the scope, objectives, potential outcomes, and limitations of the investigation

Set Boundaries

- Do not succumb to pressure to alter findings to suit the narrative of the client or employer

Maintain Confidentiality

- Be cautious about discussing the case outside the designated channels

Maintain Documentation

- Maintain meticulous records of all investigative activities, communications, and findings

Maintain Neutrality

- It is essential to remain objective and let the evidence guide conclusions

Engage Legal Counsel

- In cases where legal implications are evident or anticipated, involve legal counsel early on

Accessing Computer Forensics Resources

Join various discussion **groups and associations** to access resources regarding computer forensics

- **Associations offering computer forensic information**
  - High Technology Crime Investigation Association (HTCIA)
  - International Association of Chiefs of Police (IACP)
  - Association of Cyber Forensics and Threat Investigators (ACFTI)
  - Computer Technology Investigators Network (CITN)
  - Forensic Focus
  - The Association of Digital Forensics, Security and Law (ADFSL)

- Network of **computer forensic experts** and other professionals
- **News services** that are devoted to computer forensics can also be a powerful resource
- **Other resources:**
  - Journals of forensic investigators
  - Actual case studies

LO#07: Understand the Challenges Faced in Investigating Cybercrimes

- Challenges Cybercrimes Pose to Investigators
  - Other Factors that Influence Forensic Investigations
- Computer Forensics: Legal Issues
- Computer Forensics: Privacy Issues

Challenges Cybercrimes Pose to Investigators

General Challenges for the Investigators

- Increased data accessibility speed
- Anonymous identity
- Evolving tools and technologies
- Poor attribution
- Volatile nature of evidence
- Evidence size and complexity
- Increased usage of anti-digital forensics
- Maintaining chain of custody
- Gap in skills
- Limited resources
- Diverse platforms and devices

Other Factors Influencing Forensic Investigations

- Available resources
- Knowledge of automated tools
- Anonymous communications
- Failure of traditional tools
- Increased use of information and communications technology (ICT)
- Modern threats
- Expertise in reasoning
- Voluminous data
- Data storage in multiple jurisdictions
- Lack of forensic readiness in cloud environments

Computer Forensics: Legal Issues

1. **Different jurisdictions:** Legal systems differ across jurisdictions and have different rules for acquiring, preserving, investigating, and presenting digital evidence in a court

2. **Incorrect search and seizure:** Incorrect search and seizure of digital evidence will not be acceptable in the court of law

3. **Lack of globally standard legal framework:** It bring difficulties to investigators while collaborating with other nations for investigating globally expanded cybercrimes

4. **Absence of regulations for cooperation:** It results in poor coordination with the law enforcement agencies that may lead to loss of evidence

5. **Improper data retention and destruction:** Unnecessary holding of critical data for a longer period and destroying the evidence early can raise legal issues

6. **Expert testimony:** Based on the country's jurisdiction, the investigators might need to testify their qualifications, activities, procedures, etc. during the legal inspection

Computer Forensics: Privacy Issues

1. **Overstretching data acquisition:** Due to huge amounts of data, investigators **can acquire more information than is relevant** to the investigation leading to privacy violations

2. **Accessing third-party data:** Accessing third party data **without proper permission** can raise an issue during an investigation

3. **Accessing biometric data:** As many digital devices can **store biometric data** such as **fingerprints**, accessing them without permission may lead to privacy breaches

4. **Bypassing encryption techniques:** Bypassing encryption to **access confidential data** or **disclosing passwords and findings** to the public can be intrusive and violate one's privacy

5. **Consent issues:** For some corporate-related security incidents, **employees might not be aware** of their devices can be investigated without their consent

LO#08: Understand Various Standards and Best Practices Related to Computer Forensics

- ISO Standards
  - ISO/IEC 27037
  - ISO/IEC 27041
  - ISO/IEC 27042
  - ISO/IEC 27043
  - ISO/IEC 27050
- ENFSI Best Practices for Forensic Examination of Digital Technology

ISO Standards

ISO/IEC 27037

- ISO/IEC 27037 is a standard for digital forensics that provides recommendations for specific activities in the process of handling digital evidence, such as **identification**, **collection**, **acquisition**, and **preservation** of digital evidence

It gives guidance for the following devices and circumstances:

- Digital storage media used in standard computers like hard drives, floppy disks, optical and magneto optical disks, data devices with similar functions.
- Mobile phones, personal digital assistants (PDAs), personal electronic devices (PEDs), and memory cards
- Mobile navigation systems
- Digital still and video cameras (including CCTV)
- Standard computer with network connections
- Networks based on TCP/IP and other digital protocols

https://www.iso.org

ISO Standards (Cont'd)

ISO/IEC 27041

- ISO/IEC 27041 is a standard that deals with the investigation of information security incidents by ensuring that the methods and processes used in the investigation are "**fit for purpose**"

The ISO/IEC 27041 standard aims to

- Provide guidelines for **capturing** and **analyzing** functional and non-functional requirements
- Provide guidelines for assessing the levels of **validation** required for the evidence
- Provide guidelines on how **external testing** and **documentation** can be incorporated into the validation process

https://www.iso.org

ISO Standards (Cont'd)

C|HFI Computer Hacking Forensic INVESTIGATOR

ISO/IEC 27042

ISO/IEC 27042 provides guidelines for the **interpretation** and **analysis of digital evidence** in a manner that addresses issues of continuity, validity, reproducibility, and repeatability

ISO/IEC 27043

ISO/IEC 27043 is a standard designed to provide guidelines based on **idealized models for common incident investigation** processes across various incident investigation scenarios involving digital evidence

ISO/IEC 27050

ISO/IEC 27050 deals with **electronic discovery activities** such as identifying, preserving, collecting, processing, reviewing, analyzing, and producing electronically processed information (ESI)

https://www.iso.org

ENFSI Best Practices for Forensic Examination of Digital Technology

C|HFI

1. **Pre-scene preparation:** Develop and arrange the pre-scene preparations proactively so that the forensic laboratory staff can perform their responsibilities timely

2. **Scene assessment:** Discover, seize, and process the exhibits based on the laboratory policy

3. **Laboratory assessment:** Conduct a preliminary risk assessment of the seized exhibits and record the issues, if any

4. **Live analysis of the remote systems:** Be aware of your activities related to remote logging during the live analysis of the remote systems as those activities may be recorded and viewed by the organization

5. **Initial case evaluation:** Conduct an initial evaluation of the case before commencing the formal assessment to check and discuss the organizational requirements, anticipated approach, and potential risks that may arise

6. **Acquisition of data:** Consider the designing procedures of the laboratories during the acquisition of media or evidence that may require physical repairing or taken apart before acquiring data

https://enfsi.eu

ENFSI Best Practices for Forensic Examination of Digital Technology

1. **Pre-scene preparation:** Develop and arrange the pre-scene preparations proactively so that the forensic laboratory staff can perform their responsibilities timely

2. **Scene assessment:** Discover, seize, and process the exhibits based on the laboratory policy

3. **Laboratory assessment:** Conduct a preliminary risk assessment of the seized exhibits and record the issues, if any

4. **Live analysis of the remote systems:** Be aware of your activities related to remote logging during the live analysis of the remote systems as those activities may be recorded and viewed by the organization

5. **Initial case evaluation:** Conduct an initial evaluation of the case before commencing the formal assessment to check and discuss the organizational requirements, anticipated approach, and potential risks that may arise

6. **Acquisition of data:** Consider the designing procedures of the laboratories during the acquisition of media or evidence that may require physical repairing or taken apart before acquiring data

https://enfsi.eu

LO#09: Understand Laws and Legal Compliance in Computer Forensics

- Role of Local/International Agencies during Cybercrime Investigation
- Computer Forensics and Legal Compliance
- Other Laws Relevant to Computer Forensics

Role of Local/International Agencies during Cybercrime Investigation

- Local/international agencies play a crucial role in the investigation, prevention, and prosecution of cybercrimes and act as the **front-line defense against cybercrimes** to provide a comprehensive response to cyber threats

Investigation	Detect the occurrence of **cybercrimes** within their jurisdiction and **collect and preserve** the appropriate digital evidence for prosecution
Jurisdictional Response	**Respond** to cybercrimes that occur within their borders and address cybercrime cases in court if the **criminal activity** affects their jurisdiction's infrastructure
Collaboration	Collaborate with other **states** or **international agencies** such as the FBI, DHS, and secret service if needed
Policy and Regulation	Recommend and implement state-specific **cybercrime laws** and **regulations**, formulate policies that protect state infrastructure
Digital Forensic Labs	**Establish** and **maintain** digital forensic labs in their jurisdiction to assist with cybercrime investigations
Training and Capacity Building	Provide training to **law enforcement officers**, **judicial officers**, and other relevant **stakeholders** on cybercrime

Computer Forensics and Legal Compliance

- Legal compliance in computer forensics ensures that any evidence that is collected and analyzed is **admissible in a court of law**
- Compliance with certain regulations and standards plays an important part in computer forensic investigation and analysis, some of which are as follows:

01 Gramm-Leach-Bliley Act (GLBA)

02 Federal Information Security Modernization Act of 2014 (FISMA)

03 Health Insurance Portability and Accountability Act of 1996 (HIPAA)

04 Electronic Communications Privacy Act

05 General Data Protection Regulation (GDPR)

06 Data Protection Act 2018

07 Payment Card Industry Data Security Standard (PCI DSS)

08 Sarbanes-Oxley Act (SOX) of 2002

Other Laws Relevant to Computer Forensics

United States	Foreign Intelligence Surveillance Act of 1978 (FISA)	https://bja.ojp.gov
	Protect America Act of 2007	https://www.congress.gov
	Privacy Act of 1974	https://www.justice.gov
	National Information Infrastructure Protection Act of 1996	https://www.congress.gov
	Computer Security Act of 1987	https://www.congress.gov
	Freedom of Information Act (FOIA)	https://foia.state.gov
United Kingdom	Regulation of Investigatory Powers Act 2000	http://www.legislation.gov.uk
Australia	Cybercrime Act 2001	https://www.legislation.gov.au
	Information Privacy Act 2014	https://www.legislation.gov.au
India	Information Technology Act	http://www.dot.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	http://www.cybercrimelaw.net
Italy	Penal Code Article 615 ter	http://www.cybercrimelaw.net
Canada	Canadian Criminal Code Section 342.1	https://laws-lois.justice.gc.ca
Singapore	Computer Misuse Act	https://sso.agc.gov.sg
Belgium	Computer Hacking	http://www.cybercrimelaw.net
Philippines	Data Privacy Act of 2012	https://www.privacy.gov.ph
Hong Kong	Cap. 486 Personal Data (Privacy) Ordinance	https://www.pcpd.org.hk

Module Summary

- In this module, we discussed the fundamentals of computer forensics
- This module provided an overview of cybercrimes and their investigation procedures
- It included brief descriptions of digital evidence and eDiscovery
- The module also discussed forensic readiness and forensic readiness procedures
- It also elaborated on the roles of various processes and technologies in computer forensics
- It provided an overview of the forensic investigators' roles and responsibilities
- It also discussed the challenges faced when investigating cybercrimes
- This module discussed various standards and best practices related to computer forensics
- This module concluded with a discussion of laws and legal compliance in computer forensics
- In the next module, we discuss the computer forensic investigation process in detail along with the various phases involved in the process