Digital Forensics Essentials

Module Notes

Table of Contents

1 Computer Forensics Fundamentals

1.1 Fundamentals of Computer Forensics

Objectives of Computer Forensics

- ⇒ Identify, gather, and preserve the evidence of a cybercrime.
- ⇒ Identify and gather evidence of cybercrimes in a forensically sound manner.
- ⇒ Track and prosecute the perpetrators in a court of law.
- ⇒ Interpret, document, and present the evidence such that it is admissible during prosecution.
- ⇒ Estimate the potential impact of malicious activity on the victim and assess the intent of the perpetrator.
- ⇒ Find vulnerabilities and security loopholes that help attackers.
- ⇒ Understand the techniques and methods used by attackers to avert prosecution and overcome them.
- ⇒ Recover deleted files, hidden files, and temporary data that can be used as evidence.
- ⇒ Perform incident response to prevent further loss of intellectual property, finances, and reputation during an attack.
- ⇒ Know the laws of various regions and areas, as digital crimes are widespread and remote.
- ⇒ Know the process of handling multiple platforms, data types, and operating systems.
- ⇒ Learn to identify and use the appropriate tools for forensic investigations.
- ⇒ Prepare for incidents in advance to ensure the integrity and continuity of network infrastructure.
- ⇒ Offer ample protection to data resources and ensure regulatory compliance.
- ⇒ Protect the organisation from similar incidents in the future.
- ⇒ Help counteract online crimes such as abuse, bullying, and reputation damage.
- ⇒ Minimise the tangible and intangible losses to an organisation or an individual.
- ⇒ Support the prosecution of the perpetrator of a cybercrime.

Need for Computer Forensics

- ⇒ Ensure the overall integrity and the continued existence of an organization's computer system and network infrastructure.
- ⇒ Help the organization capture important information if their computer systems or networks are compromised. Forensic evidence also helps prosecute the perpetrator of a cybercrime, if caught.
- ⇒ Extract, process, and interpret the actual evidence so that it proves the attacker's actions and their guilt or innocence in court.
- ⇒ Efficiently track down perpetrators/terrorists from different parts of the world. Terrorists who use the Internet as a communication medium can be tracked down, and their plans can be discovered. IP addresses are vital to finding the geographical location of the terrorists.
- ⇒ Save the organisation's money and valuable time. Many managers allocate a large portion of their IT budget for computer and network security.
- ⇒ Cases of complex tracking such as ransomware attacks, email spamming, etc.

When to use Computer Forensics

- ⇒ Prepare for incidents by securing/strengthening the defence mechanism as well as closing the loopholes in security.
- ⇒ Gaining knowledge of the regulations related to cyber laws and comply with them.
- ⇒ Report incidents involving a breach of cybersecurity.
- ⇒ Identify the actions needed for incident response.
- ⇒ Act against copyright and intellectual property theft/misuse.
- ⇒ Settle disputes among employees or between the employer and employees.
- ⇒ Estimate and minimize the damage to resources in a corporate setup.
- ⇒ Set a security parameter and formulate security norms for ensuring forensic readiness.

Types of Cybercrimes

Cybercrime: any illegal act involving a computing device, network, its systems, or its applications.

1. *Internal/Insider attacks:* an attack performed on a corporate network or on a single computer by an entrusted person (insider) who has authorised access to the network. Such insiders can be former or current employees, business partners, or contractors.

2. *External attacks:* occurs when an attacker from outside the organisation tries to gain unauthorised access to its computing systems or informational assets. These attackers exploit security loopholes or use social engineering techniques to infiltrate the network.

Examples of Cybercrimes

- ⇒ *Espionage:* corporate espionage is a central threat to organizations because competitors often attempt to secure sensitive data through open-source intelligence gathering. Through this approach, competitors can launch similar products in the market, alter prices, and generally undermine the market position of a target organization.
- ⇒ *Intellectual Property Theft:* the process of stealing trade secrets, copyrights, or patent rights of an asset or a material belonging to individuals or entities. The stolen property is generally handed over to rivals or other competitors, resulting in huge losses to the organization that developed or owned it.
- ⇒ *Data Manipulation:* a malicious activity in which attackers modify, change, or alter valuable digital content or sensitive data during transmission, instead of directly stealing the data from the company. Data-manipulation attacks can lead to the loss of trust and integrity.
- ⇒ *Trojan Horse Attack:* A computer Trojan is a seemingly harmless program with hidden malicious code. It gains control when users perform certain actions, like unwittingly installing malicious software or clicking on malicious links. Once activated, Trojans give attackers complete access to the compromised system, leading to potential severe damage, including harm to the file allocation table on the hard disk.
- ⇒ *Structured Query Language Attack:* In this technique, the attacker injects malicious SQL queries into a user input form either to gain unauthorised access to a database or to retrieve information directly from the database.
- ⇒ *Brute-force Attack:* the process of using a software tool or script to guess the login credentials or keys or discover hidden applications or webpages through a trial-and-error method. A brute-force attack is performed by attempting all possible combinations of usernames and passwords to determine valid credentials.
- ⇒ *Phishing/Spoofing:* a technique in which an attacker sends an email or provides a link falsely claiming to be from a legitimate site to acquire a user's personal or account information.
- ⇒ *Privilege Escalation Attacks:* If a user is assigned higher privileges, they can modify or interact with more restricted parts of the system or application than less privileged users. Attackers initially gain system access with low privilege and then attempt to gain higher privileges to perform activities restricted from less privileged users.
- ⇒ *Denial of Service (DoS) Attack:* an attack on a computer or network that reduces, restricts, or prevents access to system resources for legitimate users. In a DoS attack, attackers flood a victim's system with nonlegitimate service requests or traffic to overload its resources and shut down the system, leading to the unavailability of the victim's website or at least significantly reducing the victim's system or network performance.
- ⇒ *Cyber Defamation:* an offensive activity wherein a computer or device connected to the web is employed as a tool or source point to damage the reputation of an organisation or individual. Sending defamatory emails or posting defamatory statements on social media can damage the reputation of the target organisation/entity to a great extent.
- ⇒ *Cyberterrorism:* an offensive activity wherein a computer or device connected to the web is employed as a tool or source point to damage the reputation of an organization or individual. Sending defamatory emails or posting defamatory statements on social media can damage the reputation of the target organization or entity to a great extent.
- ⇒ *Cyberwarfare:* the use of information systems against the virtual personas of individuals or groups. It includes information terrorism, semantic attacks (like hacker warfare, but instead of harming a system, it takes over the system while maintaining the perception that it is operating correctly), and simula-warfare (war simulated by, for example, acquiring weapons for mere demonstration rather than actual use).

Impact of Cybercrimes at the Organisational Level

- ⇒ Loss of confidentiality, integrity and availability of information stored in organisational systems.
- ⇒ Theft of sensitive data.
- ⇒ Sudden disruption of business activities.
- ⇒ Loss of customer and stakeholder trust.
- ⇒ Substantial reputational damage.
- ⇒ Huge financial losses.
- ⇒ Penalties arising from the failure to comply with regulations.

1.2 Digital Evidence

Digital evidence: "any information of probative value that is either stored or transmitted in a digital form".

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

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:* this refers to the temporary information on a digital device that requires a constant power supply and is deleted if the power supply is interrupted. For example, the Random-Access Memory stores the most volatile data and discards it when the device is switched off. Important volatile data 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:* this refers to the permanent data stored on secondary storage devices, such as hard disks and memory cards. Non-volatile data do not depend on the power supply and remain intact even when the device is switched off. Examples include hidden files, slack space, swap file, index.dat files, unallocated clusters, unused partitions, hidden partitions, registry settings, and event logs.

Roles of Digital Evidence

Examples of cases where digital evidence may assist the forensic investigator in the prosecution or defence of a suspect:

- ⇒ Identity theft
- ⇒ Malicious attacks on the computer systems themselves
- ⇒ Information leakage
- ⇒ Unauthorised transmission of information
- ⇒ Theft of commercial secrets
- ⇒ Use/abuse of the Internet
- ⇒ Production of false documents and accounts
- ⇒ Unauthorised encryption/password protection of documents
- ⇒ Abuse of systems
- ⇒ Email communication between suspects/conspirators

Sources of Potential Evidence

- ⇒ *User-created Files*
  - ⇒ Address books
  - ⇒ Database files
  - ⇒ Media (images, graphics, audio, video, etc.) files
  - ⇒ Documents (text, spreadsheet, presentation, etc.) files
  - ⇒ Internet bookmarks, favourites, etc.
- ⇒ *User-Protected Files*
  - ⇒ Compressed files
  - ⇒ Misnamed files
  - ⇒ Encrypted files
  - ⇒ Password-protected files
  - ⇒ Hidden files
  - ⇒ Steganography
- ⇒ *Computer-Created Files*
  - ⇒ Backup files
  - ⇒ Log files
  - ⇒ Configuration files
  - ⇒ Printer spool files
  - ⇒ Cookies
  - ⇒ Swap files
  - ⇒ System files
  - ⇒ History files
  - ⇒ Temporary files

Device: Location of Potential Evidence
Hard Drive: text, picture, video, multimedia, database, and computer program files.
Thumb Drive: text, graphics, image, and picture files.
Memory Card: event logs, chat logs, text files, image files, picture files, and internet browsing history.
Smart Card/Dongle/Biometric Scanner: evidence is found by recognising or authenticating the information of the card and the user, through the level of access, configurations, permissions, and in the device itself.
Answering Machine: voice recordings such as deleted messages, last called number, memo, phone numbers, and tapes.
Digital Camera/Surveillance Cameras: images, removable cartridges, video, sound, time, and date stamp, etc.
RAM and Volatile Storage: evidence is located and can be acquired from the main memory of the computer.
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 (Media Access Control) address.
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.
Network Cables and Connectors: on the devices themselves.
Server: computer system.
Printer: evidence is found through usage logs, time and date information, and network identity information, ink cartridges, and time and date stamp.
Internet of Things and wearables: evidence can be acquired in the form of GPS, audio and video recordings, cloud storage sensors, etc.
Removable Storage Device and Media: storage device and media such as tape, CD, DVD, and Blu-ray contain the evidence in the devices themselves.
Scanner: evidence is found by looking at the marks on the glass of the scanner
Telephones: evidence is found through names, phone numbers, caller identification information, appointment information, electronic mail, and pages, etc.
Copiers: documents, user usage logs, time, and date stamps, etc.
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 book, notes, appointment calendars, phone numbers, email, etc.
Fax Machines: evidence is found through documents, phone numbers, film cartridge, send or receive logs.
GPS: evidence is found through previous destinations, way points, routes, travel logs, etc.

Rules of Evidence

1. *Understandable:* investigators and prosecutors must present the evidence in a clear and comprehensible manner to the members of the jury. They must explain the facts clearly and obtain expert opinion to confirm the investigation process.
2. *Admissible:* investigators need to present evidence in an admissible manner, which means that it should be relevant to the case, act in support of the client presenting it, and be well-communicated and non-prejudiced
3. *Authentic:* given that digital evidence can be easily manipulated, its ownership needs to be clarified. Therefore, investigators must provide supporting documents regarding the authenticity of the evidence with details such as the source of the evidence and its relevance to the case. If necessary, they must also furnish details such as the author of the evidence or path of transmission.
4. *Reliable:* forensic investigators should extract and handle the evidence while maintaining a record of the tasks performed during the process to prove that the evidence is dependable. Forensic investigations must be conducted only on copies of the evidence because working on the original evidence may manipulate it and make it inadmissible in the court.
5. *Complete:* the evidence must be complete, which means that it must either prove or disprove the consensual fact in the litigation. If the evidence fails to do so, the court is liable to dismiss the case, citing a lack of integral evidence.

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 best evidence rule states that the court only allows the original evidence of a document, photograph, or recording at the trial and not a copy. However, the duplicate may be accepted as evidence, provided the court finds the party's reasons for submitting the duplicate to be genuine.

Federal Rules of Evidence (United States)

A set of rules that governs the introduction of evidence at civil and criminal trials in United States federal trial courts.

Scientific Working Group on Digital Evidence (SWGDE)

Principle 1: "In order to ensure that digital evidence is collected, preserved, examined, or transferred in a manner that safeguards the accuracy and reliability of the evidence, law enforcement and forensic organizations must establish and maintain an effective quality system."

Standard Operating Procedures (SOPs): "SOPs are documented quality-control guidelines that must be supported by proper case records and broadly accepted procedures, equipment, and materials."
Implementation of SOPs allows you to operate company-compliant policies and plans. It is important that no modifications are made to SOPs before implementation to achieve the desired outputs. However, if any modifications are required, they must be communicated before starting an investigation.

Standards and Criteria 1.1
All agencies that seize and/or examine digital evidence must maintain an appropriate SOP document. All elements of an agency's policies and procedures concerning digital evidence must be clearly set forth in this SOP document, which must be issued under the agency's management authority.

Standards and Criteria 1.2
Agency management must review the SOPs on an annual basis to ensure their continued suitability and effectiveness.

Standards and Criteria 1.3
Procedures used must be generally accepted in the field or supported by data gathered and recorded in a scientific manner.

Standards and Criteria 1.4
The agency must maintain written copies of appropriate technical procedures.

Standards and Criteria 1.5
The agency must use hardware and software that are appropriate and effective for the seizure or examination procedure.

Standards and Criteria 1.6
All activity relating to the seizure, storage, examination, or transfer of the digital evidence must be recorded in writing and be available for review and testimony.

Standards and Criteria 1.7
Any action that has the potential to alter, damage, or destroy any aspect of the original evidence must be performed by qualified persons in a forensically sound manner.

The Association of Chief Police Officers (ACPO) 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 in necessary to access original data held on a computer or on storage media, that person must be able to do so and be able to explain their actions and the impact of their 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.

1.3 Forensic Readiness

Forensic Readiness

Refers to an organisation's ability to optimally use digital evidence in a limited period and with minimal investigation costs.
Benefits of forensics readiness include:

- ⇒ Fast and efficient investigation with minimal disruption to the business.
- ⇒ Provides security from cybercrimes such as intellectual property theft, fraud or extortion.
- ⇒ Offers structured storage of evidence that reduces the cost and time of an investigation.
- ⇒ Enhanced communication and collaboration between an organisation and law enforcement agencies.
- ⇒ Helps the organisation use the digital evidence in its own defence.

Forensic Readiness and Business Continuity

Forensic readiness helps maintain business continuity by allowing quick and easy identification of the impacted components and replacing them to continue the services and business.

Forensic readiness allows business to

- ⇒ Quickly determine the incidents.
- ⇒ Collect legally sound evidence and analyse it to identify attackers.
- ⇒ Minimise the required resources.
- ⇒ Quickly recover from damage with less downtime.
- ⇒ Gather evidence to claim insurance.
- ⇒ Legally prosecute the perpetrators and claim damages.

Lack of forensic readiness may result in

- ⇒ Loss of clients because of damage to the organisation's reputation.
- ⇒ System downtime.
- ⇒ Data manipulation, deletion and theft.
- ⇒ Inability to collect legally sound evidence.

Forensic Readiness Planning

Refers to a set of processes to be followed to achieve and maintain forensic readiness.

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

1.4 Roles and Responsibilities of a Forensic Investigator

Need for a Forensic Investigator

- ⇒ *Cybercrime Investigation:* Forensic investigators help organisations and law enforcement agencies investigate and prosecute the perpetrators of cybercrimes.
- ⇒ *Sound Evidence Handling:* If a technically inexperienced person examines the evidence, it might become inadmissible in a court of law.
- ⇒ *Incident Handling and Response:* Forensic investigators help organisations maintain forensics readiness and implement effective incident handling and response.

Roles and Responsibilities of a Forensic Investigator

A forensic investigator performs the following tasks:

- ⇒ Determines the extent of any damage done during the crime.
- ⇒ Recovers data of investigate value from computing devices involved in crimes.
- ⇒ Creates an image of the original evidence without tampering with it to maintain its integrity.
- ⇒ Guides the officials carrying out the investigation.
- ⇒ Analyses the evidence data found.
- ⇒ Prepares the analysis report.
- ⇒ Updates the organisation about various attack methods & data recovery techniques and maintains a record of them.
- ⇒ Addresses the issue in a court of law and attempts to win the case by testifying in court.

What Makes a Good Forensic Investigator?

- ⇒ Interviewing skills to gather extensive information about the case from the client or victim, witnesses and suspects.
- ⇒ Excellent writing skills to detail findings in the report and has knowledge of the laws relevant to the case.
- ⇒ Strong analytical skills to find the evidence and link it to the suspect.
- ⇒ Excellent communication skills to explain their findings to the audience.
- ⇒ Remains updated about new methodologies and forensic technology.
- ⇒ Knowledgeable in more than one computer platform (including, Windows, Macintosh and Linux).
- ⇒ Knowledge of various technologies, hardware and software.
- ⇒ Develops and maintains contact with computing, networking and investigating professionals.

1.5 Legal Compliance in Computer Forensics

Computer Forensics and Legal Compliance

Compliance with certain regulations and standards plays an important part in computer forensic investigation and analysis, come of which are as follows:

- ⇒ *Gramm-Leach-Bliley Act of 1999 (GLBA):* Ensures that financial institutions and their affiliates safeguard the confidentiality of PII gathered from customer records in paper, electronic or other forms.
- ⇒ *Federal Information Security Modernisation Act of 2014 (FISMA):* Defines a comprehensive framework to protect government information, operations, and assets against threats.
- ⇒ *Health Insurance Portability and Accountability Act of 1996 (HIPAA):* Requires health care professionals to protect privacy and create standards for electronic transfers of health data.
- ⇒ *Payment Card Industry Data Security Standard (PCI DSS):* Safeguards and optimises the security of sensitive cardholder data, such as credit card numbers, expiration dates and security codes.
- ⇒ *Electronic Communications Privacy Act (1986):* Protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically.
- ⇒ *General Data Protection Regulation Act (GDPR):* Lists the rights of the data subject, meaning the rights of the individuals whose personal data is being processed.
- ⇒ *Data Protection Act 2018:* Applies to 'personal data', which is information which relates to individuals. It gives individuals the right to access their own personal data through subject access requests and contains rules which must be followed when personal data is processed.
- ⇒ *Sarbanes-Oxley Act of 2002 (SOX):* Protects investors by improving the accuracy & reliability of corporate disclosures.

2 Computer Forensics Investigation Process

2.1 Forensic Investigation Process and its Importance
2.2 Forensic Investigation Process - Pre-investigation Phase
2.3 Forensic Investigation Process - Investigation Phase
2.4 Forensic Investigation Process - Post-investigation Phase

3 Understanding Hard Disks and File Systems

3.1 Different Types of Disk Drives and their Characteristics
3.2 Logical Structure of a Disk
3.3 Booting Process of Windows, Linux, and Mac Operating Systems
3.4 File Systems of Windows, Linux, and Mac Operating Systems
3.5 File System Examination

4 Data Acquisition and Duplication

4.1 Data Acquisition Fundamentals
4.2 Types of Data Acquisition
4.3 Data Acquisition Format
4.4 Data Acquisition Methodology

5 Defeating Anti-forensics Techniques

5.1 Anti-forensics and its Techniques
5.2 Anti-forensics Countermeasures

6 Windows Forensics

6.1 Volatile and Non-Volatile Information
6.2 Windows Memory and Registry Analysis
6.3 Cache, Cookie, and History Recorded in Web Browsers
6.4 Windows Files and Metadata

7 Linux and Mac Forensics

7.1 Volatile and Non-Volatile Data in Linux
7.2 Analyse Filesystem Images Using the Sleuth Kit
7.3 Memory Forensics 402 Mac Forensics

8 Network Forensics

8.1 Network Forensics Fundamentals
8.2 Event Correlation Concepts and Types
8.3 Identify Indicators of Compromise (IoCs) from Network Logs
8.4 Investigate Network Traffic

9 Investigating Web Attacks

10 Dark Web Forensics

10.1 Dark Web
10.2 Dark Web Forensics
10.3 Tor Browser Forensics

11 Investigating Email Crimes

11.1 Email Basics
11.2 Email Crime Investigation and its Steps

12 Malware Forensics

12.1 Malware, its Components and Distribution Methods
12.2 Malware Forensics Fundamentals and Recognize Types of Malware
12.3 Analysis Static Malware Analysis
12.4 Analyse Suspicious Word Documents Dynamic Malware Analysis
12.5 System Behaviour Analysis
12.6 Network Behaviour Analysis