**Digital Forensics Essentials**   
Module Notes

Table of Contents

[1 Computer Forensics Fundamentals 3](#_Toc141115390)

[1.1 Fundamentals of Computer Forensics 3](#_Toc141115391)

[1.2 Digital Evidence 4](#_Toc141115392)

[1.3 Forensic Readiness 4](#_Toc141115393)

[1.4 Roles and Responsibilities of a Forensic Investigator 4](#_Toc141115394)

[1.5 Legal Compliance in Computer Forensics 4](#_Toc141115395)

[2 Computer Forensics Investigation Process 5](#_Toc141115396)

[2.1 Forensic Investigation Process and its Importance 5](#_Toc141115397)

[2.2 Forensic Investigation Process - Pre-investigation Phase 5](#_Toc141115398)

[2.3 Forensic Investigation Process - Investigation Phase 5](#_Toc141115399)

[2.4 Forensic Investigation Process - Post-investigation Phase 5](#_Toc141115400)

[3 Understanding Hard Disks and File Systems 6](#_Toc141115401)

[3.1 Different Types of Disk Drives and their Characteristics 6](#_Toc141115402)

[3.2 Logical Structure of a Disk 6](#_Toc141115403)

[3.3 Booting Process of Windows, Linux, and Mac Operating Systems 6](#_Toc141115404)

[3.4 File Systems of Windows, Linux, and Mac Operating Systems 6](#_Toc141115405)

[3.5 File System Examination 6](#_Toc141115406)

[4 Data Acquisition and Duplication 7](#_Toc141115407)

[4.1 Data Acquisition Fundamentals 7](#_Toc141115408)

[4.2 Types of Data Acquisition 7](#_Toc141115409)

[4.3 Data Acquisition Format 7](#_Toc141115410)

[4.4 Data Acquisition Methodology 7](#_Toc141115411)

[5 Defeating Anti-forensics Techniques 8](#_Toc141115412)

[5.1 Anti-forensics and its Techniques 8](#_Toc141115413)

[5.2 Anti-forensics Countermeasures 8](#_Toc141115414)

[6 Windows Forensics 9](#_Toc141115415)

[6.1 Volatile and Non-Volatile Information 9](#_Toc141115416)

[6.2 Windows Memory and Registry Analysis 9](#_Toc141115417)

[6.3 Cache, Cookie, and History Recorded in Web Browsers 9](#_Toc141115418)

[6.4 Windows Files and Metadata 9](#_Toc141115419)

[7 Linux and Mac Forensics 10](#_Toc141115420)

[7.1 Volatile and Non-Volatile Data in Linux 10](#_Toc141115421)

[7.2 Analyse Filesystem Images Using the Sleuth Kit 10](#_Toc141115422)

[7.3 Memory Forensics 402 Mac Forensics 10](#_Toc141115423)

[8 Network Forensics 11](#_Toc141115424)

[8.1 Network Forensics Fundamentals 11](#_Toc141115425)

[8.2 Event Correlation Concepts and Types 11](#_Toc141115426)

[8.3 Identify Indicators of Compromise (IoCs) from Network Logs 11](#_Toc141115427)

[8.4 Investigate Network Traffic 11](#_Toc141115428)

[9 Investigating Web Attacks 12](#_Toc141115429)

[9.1 Web Application Forensics 12](#_Toc141115430)

[9.2 IIS and Apache Web Server Logs 12](#_Toc141115431)

[9.3 Investigating Web Attacks on Windows-based Servers 12](#_Toc141115432)

[9.4 Detect and Investigate Attacks on Web Applications 12](#_Toc141115433)

[10 Dark Web Forensics 13](#_Toc141115434)

[10.1 Dark Web 13](#_Toc141115435)

[10.2 Dark Web Forensics 13](#_Toc141115436)

[10.3 Tor Browser Forensics 13](#_Toc141115437)

[11 Investigating Email Crimes 14](#_Toc141115438)

[11.1 Email Basics 14](#_Toc141115439)

[11.2 Email Crime Investigation and its Steps 14](#_Toc141115440)

[12 Malware Forensics 15](#_Toc141115441)

[12.1 Malware, its Components and Distribution Methods 15](#_Toc141115442)

[12.2 Malware Forensics Fundamentals and Recognize Types of Malware 15](#_Toc141115443)

[12.3 Analysis Static Malware Analysis 15](#_Toc141115444)

[12.4 Analyse Suspicious Word Documents Dynamic Malware Analysis 15](#_Toc141115445)

[12.5 System Behaviour Analysis 15](#_Toc141115446)

[12.6 Network Behaviour Analysis 15](#_Toc141115447)

# Computer Forensics Fundamentals

## 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.

## 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.

## 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.

## 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.

## 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.

# Computer Forensics Investigation Process

## Forensic Investigation Process and its Importance

As digital evidence is fragile in nature, following strict guidelines and thorough forensic investigation process that ensure the integrity of evidence is critical to prove a case in the court of law.

The forensics investigation process to be followed should comply with local laws and established precedents (similar or previous cases).

The investigators must follow a repeatable and well-documented set of steps such that every iteration of analysis provides the same findings otherwise the findings of the investigation can be invalidated during the cross examination in a court of law.

Phases Involved in the Forensics Investigation Process

*Pre-Investigation Phase*

* Deals with tasks to be performed prior to the commencement of the actual investigation.
* Involves setting up a computer forensics lab, building a computer forensics workstation, developing an investigation toolkit, setting up an investigation team, getting approval from the relevant authority, etc.

*Investigation Phase*

* The main phase of the computer forensics investigation process.
* Involves acquisition, preservation and analysis of evidentiary data to identify the source of the crime and the culprit behind it.

*Post-Investigation Phase*

* Includes documentation of all actions undertaken and all findings uncovered during the investigation.
* Ensures that the report is easily explicable to the target audience and that it provides adequate and acceptable evidence.

## Forensic Investigation Process - Pre-investigation Phase

Setting Up a Computer Forensics Lab

A *Computer Forensics Lab (CFL)* is a location that houses instruments, software and hardware tools and forensic workstations required for conducting a computer-based investigation regarding the collected evidence.

1. *Planning and budgeting considerations*
   * Number of expected cases
   * Type of investigation
   * Manpower
   * Equipment and software requirement
2. *Physical and structural design considerations*
   * Lab size
   * Access to essential services
   * Space estimation for work area and evidence storage
   * Heating, ventilation and air-conditioning
3. *Work area considerations*
   * Workstation requirement
   * Ambience (climate/atmosphere)
   * Internet, network and communication line
   * Lighting systems and emergency power
4. *Physical security considerations*
   * Electronic sign-in
   * Intrusion alarm systems
   * Fire suppression systems
5. *Human resource consideration*
   * Number of required personnel
   * Training and certification
6. *Forensic lab licensing* 
   * ASCLD/Lab accreditation
   * ISO/IEC 17025 accreditation

Building the Investigation Team

* Keep the team small to protect the confidentiality of the investigation and to guard against information leaks.
* Identify team members and assign them responsibilities.
* Ensure that every team member has the necessary clearance and authorisation to conduct assigned tasks.
* Assign one team member as the technical lead of the investigation.

People Involved in an Investigation Team

* *Photographer:* Photographs the crime scene and the evidence gathered.
* *Incident Responder:* Responsible for the measures to be taken when an incident occurs.
* *Incident Analyser:* Analyses the incidents based on their occurrence.
* *Evidence Examiner/Investigator:* Examines the evidence acquired and sorts the useful evidence.
* *Evidence Documenter:* Documents all the evidence and the phases present in the investigation process.
* *Evidence Manager:* Manages the evidence in such a way that it is admissible in the court of law.
* *Evidence Witness:* Offers a formal opinion in the form of a testimony in the court of law.
* *Attorney:* Provides legal advice.

Understanding the Hardware and Software Requirements of a Forensic Lab

A digital forensic lab should have all the necessary hardware and software tools to support the investigation process, starting from searching and seizing the evidence to reporting the outcome of the analysis.

*Hardware*

* Two or more forensic workstations with good processing power and RAM.
* Specialised cables.
* Write-blockers and drive duplicators.
* Archive and Restore devices.
* Media sterilisation systems.
* Other requirement that allows forensic software tools to work.
* Computer Forensic hardware toolkit, such as *Paraben’s First Responder Bundle*, *DeepSpar Disk Imager*, *FRED forensic workstation* etc.

*Software*

* OSes
* Data discovery tools
* Password-cracking tools
* Acquisition tools
* Data analysers
* Data recovery tools
* File viewers (image and graphics)
* File types conversion tools
* Security and Utilities software
* Computer forensic software tools such as *Wireshark*, Access Data’s *FTK* etc.

## Forensic Investigation Process - Investigation Phase

Computer Forensics Investigation Methodology

1. Documenting the Electronic Crime Scene
2. Search and Seizure
3. Evidence Preservation
4. Case Analysis
5. Data Analysis
6. Data Acquisition
7. Reporting
8. Testifying as an Expert Witness

1. Documenting the Electronic Crime Scene

Documentation of the electronic crime scene is necessary to maintain a record of all the forensic investigation processes performed to identify, extract, analyse and preserve the evidence.

Points to remember when documenting the crime scene:

* Document the physical crime scene, nothing the position of the system and other equipment if any.
* Document details of any related or difficult-to-find electronic components.
* Record the state of computer systems, digital storage media and electronic devices, including their power status.

2. Search and Seizure

1. Planning the search and seizure

* Seeking consent
* Obtaining witness signature
* Obtaining warrant for search and seizure
* Collecting incident information

1. Initial search of the scene
2. Securing and evaluating the crime scene
3. Seizing evidence at crime scene
   * Dealing with powered-on computers
   * Dealing with powered-off computers
   * Dealing with networked computers
   * Operating System shutdown procedure
   * Dealing with mobiles and other handheld devices

*Planning the Search and Seizure*

A search and seizure plan should contain the following details:

* Description of the incident.
* Case name or title of the incident.
* Location of the incident.
* Applicable jurisdiction and relevant legislation.
* Determining the extent of authority to search.
* Creating a chain of custody document.
* Details of equipment to be seized.
* Search and seizure type (overt/covert).
* Approval from local management.
* Health and safety precautions.

3. Evidence Preservation

1. Evidence preservation refers to the proper handling and documentation of evidence to ensure that it is free from any contamination.
2. Any physical and/or digital evidence seized should be isolated, secured, transported and preserved to protect its true state.
3. At the time of evidence transfer, both the sender and the receiver need to provide information about the date and time of transfer in the chain of custody record.
4. The procedures used to protect the evidence and document it while collecting and shipping are as follows:

* The logbook of the project.
* A tag to uniquely identify any evidence.
* A chain of custody record.

4. Case Analysis

Investigators can relate the evidential data to the case details for understanding how the complete incident took place and determining the future actions such as the following:

* Determine the possibility of exploring other investigative procedures to gather additional evidence (e.g., checking host data and examining network service logs for any information of evidentiary value, collecting case-specific evidence from social media, identifying remote storage locations, etc.)
* Gather additional information related to the case (e.g., aliases, email accounts, ISP used, names, network configuration, system logs and passwords) by interviewing the respective individuals.
* Consider the relevance of components that are out of the scope of investigation, e.g., equipment such as laminators, check papers, scanners and printers in cases of any fraud.

5. Data Analysis

* Data analysis refers to the process or examining, identifying, separating, converting and modelling data to isolate useful information.
* Data analysis techniques depend on the scope of the case or the client’s requirements.
* This phase includes the following:
* Analysis of the file’s content, date and time of file creation and modification, users associated with file creation, access and file modification and physical storage location of the file.
* Timeline generation.
* Identification of the root cause of the incident.

6. Data Acquisition

* Forensic data acquisition is a process of imaging or collecting information from various media in accordance with certain standards for analysing its forensic value.
* Investigators can then forensically process and examine the collected data to extract information relevant to any particular case or incident while protecting the integrity of the data.
* It is one of the most critical steps of digital forensics as improper acquisition may alter data in evidence media and render it inadmissible in the court of law.
* Investigators should be able to verify the accuracy of acquired data and the complete process should be auditable and acceptable to the court.

## Forensic Investigation Process - Post-investigation Phase

Gathering and Organising Information

Documentation in each phase should be identified to decide whether it is appropriate to the investigation and should be organised in specific categories.

Following are the procedures for the gathering and organising of the required documentation:

* Gather all notes from different phases of the investigation process.
* Identify the facts to be included in the report for supporting the conclusions.
* List all the evidence to submit within the report.
* List the conclusions that need to be in the report.
* Organise and classify the information gathered to create a concise and accurate report.

Writing the Investigation Report

Report writing is a crucial step in the outcome of the investigation. A good report should:

* Accurately define the details of an incident.
* Convey all necessary information in a concise manner.
* Be technically sound and understandable to the target audience.
* Be structured in a logical manner so that information can be easily located.
* Be able to withstand legal inspection.
* Adhere to local laws to be admissible in court.

Forensics Investigation Report Template

* Executive summary
  + Case number.
  + Names and Socials Security Numbers of authors, investigators and examiners.
  + Purpose of investigation.
  + Significant findings.
  + Signature analysis.
* Investigation objectives
* Details of the incident
  + Date and time the incident allegedly occurred.
  + Date and time the incident was reported to the agency’s personnel.
  + Details of the person or persons reporting the incident.
* Investigation process
  + Date and time the investigation was assigned.
  + Allocated investigators.
* Evidence information
  + Location of the evidence.
  + List of the collected evidence.
  + Tools involved in collecting the evidence.
  + Preservation of the evidence.
* Evaluation and analysis process
  + Initial evaluation of the evidence.
  + Investigative techniques.
  + Analysis of the computer evidence (tools involved)
* Relevant findings
* Supporting files
  + Attachments and appendices.
  + Full path of the important files.
  + Expert reviews and opinion.
* Other supporting details
  + Attacker’s methodology.
  + User’s applications and internet activity.
  + Recommendations.

Testifying as an Expert Witness

Presenting digital evidence in the court requires knowledge of new, specialised, evolving and sometimes complex technology.

Things that take place in a court room:

* Familiarise the expert witness with the usual procedures that are followed during a trial.
* The attorney introduces the expert witness.
* The opposing counsel may try to discredit the expert witness.
* The attorney leads the expert witness through the evidence.
* Later it is followed by the opposing counsel’s cross examination.

# Understanding Hard Disks and File Systems

## Different Types of Disk Drives and their Characteristics

Understand Hard Disk Drive

HDD is a non-volatile digital data storage device that records date magnetically on a metallic platter.

The read/write performance of an HDD is directly proportional to the RPM (revolutions per minute) of the drive platter.

A diagram of a computer system

Description automatically generated

Understanding Hard Disk Drive: Tracks

* Tracks are the concentric circles on platters where all the information is stored.
* The drive head can access these circular rings in one position at a time.
* Tracks are numbered for identification purposes.
* Read/write is performed by rolling headers from the inner to outmost part of the disk.

Understanding Hard Disk Drive: Track Numbering

* Track numbering on a hard disk begins at 0 from the outer edge and moves towards the centre. The number of tracks on a hard disk depends on the size of the disk.
* The read/write heads on both surfaces of a platter are tightly packed and locked together on an assembly of head arms.
* The arms move in and out together to physically locate all heads at the same track number.
* Therefore, a track location is often referred to as a cylinder number rather than a track number.
* A cylinder is a group of all tracks that start at the same head position on the disk.

Understanding Hard Disk Drive: Sector

1. A sector is the smallest physical storage unit on the disk platter.
2. Each sector holds data of fixed size: 512 bytes for HDDs, 2048 bytes for CD-ROMs and DVD-ROMs. Latest HDDs use 4096-byte (4KB) sectors.
3. Each disk sector is labelled using the factory track-positioning data.
4. The optimal method of storing a file on a disk is in a contiguous series.
5. E.g., if the file size is 600-bytes, two 512-bytes sectors are allocated for the file.

Understanding Hard Disk Drive: Sector Addressing

* Cylinders, heads and sectors (CHS) determine the address of the individual sectors on the disk.
* When a disk is formatted, it is divided into tracks and sector.
* E.g., the formatted disk must contain 50 tracks, each of which is divided into 10 sectors.
* Track and sector numbers are used by the OS and disk drive to identify the stored information.

Understanding Hard Disk Drive: 4K Sectors

New hard drives use 4096-bytes (4KB or 4K) advanced format sectors.

Generation-one Advanced Format, also called as 4K sector technology, efficiently uses the storage surface media of a disk by merging eight512-byte sectors into a single sector of 4096-bytes.

A diagram of a number of data

Description automatically generated with medium confidence

Data Density on a Hard Disk

* Data is recorded on a hard disk using a method called zoned bit recording (aka multiple zone recording).
* In this technique, tracks are combined in zones depending on their distance from the centre of the disk.
* Each zone is assigned a number of sectors per track.

Types of data densities on a hard disk

* *Track Density:* The space between tracks on a disk.
* *Areal Density:* The number of bits per square inch on a platter.
* *Bit Density:* The bits per unit length of track.

CHS Data Addressing and Disk Capacity Calculation

The CHS addressing method addresses each physical block of data on a hard disk by specifying the cylinder (radius), head (platter side) and sector (angular position).

*Example of Disk Capacity Calculation*

A disk drive has 16,384 cylinders, 80 heads and 63 sectors per track. Assume – a sector has 512 bytes. What is the capacity of such a disk?

Answer:

Measuring the Hard Disk Performance

Data is stored on the board in the form of files.

When a running program requests a file, the hard disk recovers the byte content of the file and sends the bytes to the CPU, one at a time, for further processing.

Hard disks performance is measured by these factors:

* *Data rate:* It is a ratio from the number of bytes per second that the hard disk sends to the CPU.
* *Seek time:* It is the amount of time required to send the first byte of the file to the CPU, when it requests the file.

Understanding Solid-State Drive (SSD)

* SSD is a non-volatile storage device that uses NAND flash memory chips to store the digital data.
* SSDs are faster than HDDs as they have no moving parts and the read/write performance depends on data connection of the drive.

1. *NAND Flash Memory:* The main data storage unit made up of floating gate transistors which retain the charge state even without power.
2. *Controller:* A processor that acts as a bridge between the flash memory components and the computer (host) by executing firmware-level software.
3. *DRAM:* A volatile memory that provides fast read/writer performance.
4. *Host Interface:* An SSD connects to the host machine using an interface. The commonly used SSD interfaces are SATA, PCIe, SCSI, etc.

A close-up of a computer chip

Description automatically generated

Disk Interfaces

* *ATA/PATA (IDE/EIDE):* ATA (Advanced Technology Attachment) is the official ANSI (American National Standards Institute) name of Integrated Drive Electronics (IDE) a standard interface between a motherboard’s data bus and storage disk.
* *Serial ATA/SATA (AHCI):* It is an advancement of ATA and uses serial signalling, unlike IDE’s parallel signalling.
* *Serial Attached SCSI:* SAS (Serial Attachment SCSI) is the successor and an advancement alternative to parallel SCSI in enterprise environment.
* PCIe SSD: A PCIe (Peripheral Component Interconnect Express) SSD is a high-speed serial expansion card that integrates flash directly into the motherboard.
* *SCSI:* SCSI (Small Computer System Interface) refers to a set of ANSI standard interfaces based on the parallel bust structure and designed to connect multiple peripherals to a computer.

## Logical Structure of a Disk

Logical Structure of Disks

* The logical structure of a hard disk is the file system & software utilised to control access to the storage on the disk.
* A hard disk’s logical structure has a significant influence on the performance, consistency, expandability and compatibility of the storage subsystem of the hard disk.
* Different OSes have different file systems and use various methods of arranging and controlling access to data on the hard disk.

Clusters

* A cluster is the smallest logical storage unit.
* A set of sectors within a disk ranging from cluster number 2-32 or more depending on the formatting scheme in use.
* The file system divides the storage on a disk volume into discreet chunks of data for efficient disk usage and performance. These chunks are called clusters.
* The process by which files are allocated to clusters in called allocation, therefore, clusters are also known as allocation units.
* In the File Allocation Table (FAT) file systems, the clusters linked with a file keep track of file data in the hard disk’s file allocation table.

Cluster Size

* Cluster sizing has a significant impact on the performance of an OS and disk utilisation.
* Cluster size can be altered for optimum disk storage.
* The size of a cluster depends on the size of the disk partition and type of file system installed on the partition.
* A large cluster size (greater than one sector) has the following effects:
  + Minimises the fragmentation problem.
  + Increases the probability of unused space in the cluster.
  + Reduces the disk storage area in which information can be saved.
  + Reduces the unused area on the disk.

Lost Clusters

1. When the OS marks clusters as used but does not allocate them to any file, such clusters are known as lost clusters.
2. A lost cluster is a FAT file system error that results from the way the FAT file system allocates space and chains files together.
3. It is mainly the result of a logical structure error and not a physical disk error.
4. They usually occur because of interrupted file activities caused when, e.g., a file is not properly closed, thus, the clusters involved in such activity are never linked correctly to a file.
5. CHKDSK is a system tool in Windows that authenticates the file system reliability of a volume and repairs logical file system errors.

Slack Space

* Slack space is the storage area of a disk between the end of a file and the end of a cluster.
* If the file size is less than the cluster size, a full cluster is still assigned to that file. The remaining unused space is called slack space.
* E.g., if the partition size is 4 GB, each cluster will be 32 KB in size. Even if a file requires only 10 KB, the entire 32 KB will be allocated to that file, resulting in 22 KB of slack space.

A diagram of a cluster

Description automatically generated

Master Boot Record (MBR)

1. The MBR is the first sector (“sector zero”) of a data storage device such as a hard disk.
2. The information regarding the files on the disk, their locations and sizes and other important data is stored in the MBR file.
3. In practice, MBR almost always refers to the 512-byte boot sector (or partition sector) of a disk.
4. MBR is used for the following:
   * + - Holding a partition table which refers to the partitions of a hard disk.
       - Bootstrapping an OS.
       - Distinctively recognising individual hard disk media with a 32-bit disk signature.

Structure of a Master Boot Record (MBR)

The structure of a MBR consists of three parts:

1. *Master Boot Code or Boot Strap:* It is an executable code and responsible for loading OS into computer memory. It consists of a data structure of 446 bytes.
2. Partition Table: It maintains the data of all the hard disk partitions and consists of a data structure 64 bytes.
3. Disk Signature: It is located at the end of the MBR and contains only 2 bytes of data. It is required by BIOS during booting.

A close-up of a document

Description automatically generated

Disk Partitions

Disk partitioning is the creation of logical divisions on a storage device (HDD/SSD) to allow the user to apply OS-specific logical formatting.

The disk-partitioning process is the same for both HDDs and SSDs.

1. *Primary Partition:* It is a hard drive that holds the information regarding the OS, system area and other information required for booting. In MS-DOS and earlier versions of Microsoft Windows systems, the first partition (C:) must be a primary partition.
2. *Extended Partition:* It is a logical drive that holds the information regarding stored data and filed in the disk.

BIOS Parameter Block (BPB)

* The BPB is a data structure in the partition boot sector.
* It describes the physical layout of a data storage volume, such as the number of heads & the size of the tracks on the drive.
* BPB in the file systems such as FAT12 (except in DOS 1.x), FAT16, FAT32, HPFS (High Performance File System) and NTFS (New Technology File System) defines the file system structure.
* The BPB length varies for FAT16, FAT31 and NTFS boot sectors due to different types of fields and the amount of data stored in them.
* BPB assists investigators to locate the file table on the hard drive.

A table with text and numbers

Description automatically generatedA table with text and numbers

Description automatically generated

Globally Unique Identifier (GUID)

The GUID is a 128-bit unique reference number used as an identifier in computer. In general, GUIDs are displayed as 32 hexadecimal digits with groups separated by hyphens.

Common uses:

* In Windows Registry, GUIDs are used to identify COM (Component Object Model) DLLs (dynamic-link libraries).
* In database tables, GUIDs are used as primary key values.
* In some instances, a website may assign a GUID to a user’s browser to record and track the session.
* Windows assigns a GUID to a username to identify user accounts.

GUID Partition Table (GPT)

* Unified Extensible Firmware Interface (UEFI) replaces legacy BIOS firmware interfaces.
* UEFI is a specification that defines a software interface between an OS and platform firmware.
* It uses a partition system known as GPT, which replaces the traditional MBR.

Advantages of GPT disk layout:

* Supports up to 138 partitions and uses 64-bit Logical Block Addresses (LBA).
* Supports a maximum partition size ranging from 2 Tebibytes (TiB) to 8 Zebibytes (ZiB).
* Provides primary and backup partition table for redundancy.

A screenshot of a computer screen

Description automatically generated

## Booting Process of Windows, Linux, and Mac Operating Systems

## File Systems of Windows, Linux, and Mac Operating Systems

## File System Examination

# Data Acquisition and Duplication

## Data Acquisition Fundamentals

## Types of Data Acquisition

## Data Acquisition Format

## Data Acquisition Methodology

# Defeating Anti-forensics Techniques

## Anti-forensics and its Techniques

## Anti-forensics Countermeasures

# Windows Forensics

## Volatile and Non-Volatile Information

## Windows Memory and Registry Analysis

## Cache, Cookie, and History Recorded in Web Browsers

## Windows Files and Metadata

# Linux and Mac Forensics

## Volatile and Non-Volatile Data in Linux

## Analyse Filesystem Images Using the Sleuth Kit

## Memory Forensics 402 Mac Forensics

# Network Forensics

## Network Forensics Fundamentals

## Event Correlation Concepts and Types

## Identify Indicators of Compromise (IoCs) from Network Logs

## Investigate Network Traffic

# Investigating Web Attacks

## Web Application Forensics

## IIS and Apache Web Server Logs

## Investigating Web Attacks on Windows-based Servers

## Detect and Investigate Attacks on Web Applications

# Dark Web Forensics

## Dark Web

## Dark Web Forensics

## Tor Browser Forensics

# Investigating Email Crimes

## Email Basics

## Email Crime Investigation and its Steps

# Malware Forensics

## Malware, its Components and Distribution Methods

## Malware Forensics Fundamentals and Recognize Types of Malware

## Analysis Static Malware Analysis

## Analyse Suspicious Word Documents Dynamic Malware Analysis

## System Behaviour Analysis

## Network Behaviour Analysis