MAILAM ENGINEERING COLLEGE

(Approved by AICTE, New Delhi, Affiliated to Anna University, Chennai

A TATA Consultancy Services Accredited Institution)

DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE

UNIT I INTRODUCTION TO DIGITAL FORENSICS

Forensic Science – Digital Forensics – Digital Evidence – The Digital Forensics Process – Introduction – The Identification Phase – The Collection Phase – The Examination Phase – The Analysis Phase – The Presentation Phase.

PART – A

1. **Define forensics science.**
   - Forensic science is the application of scientific methods to establish factual answers to legal problems.
   - It involves the analysis of evidence collected from crime scenes to provide objective information for use in the legal system.

2. **State Locard' s Exchange Principle.**
   Edmond Locard's exchange principle asserts that whenever someone or something comes into contact with another person or object, there is an exchange of materials between them.

3. **Define Crime Reconstruction.**
   - Crime reconstruction involves piecing together the sequence of events surrounding a crime using scientific methods and evidence.
   - By analyzing physical evidence, witness statements, and other relevant information, investigators can reconstruct the actions and events leading up to and following the commission of a crime.

4. **List the Five WH formula sets.**
   - The 5WH formula (who, where, what, when, why, and how) is commonly used to guide investigations and ensure that all relevant aspects of a case are considered.
   - Investigators employ various techniques, such as interviews, surveillance, forensic analysis, and data collection, to uncover facts and establish the truth.

5. **Define Evidence Dynamics.**
   - Evidence dynamics refers to any influence that adds, changes, relocates, obscures, contaminates, or obliterates evidence, regard less of intent.

6. **Define Digital Forensics.**
   - Digital forensics involves the use of scientifically derived methods for the preservation, collection, analysis, and interpretation of digital evidence from various sources.

- Its primary aim is to reconstruct criminal events or anticipate unauthorized actions that disrupt planned operations

7. What is Forensically sound?

- An investigation is forensically sound if it adheres to established digital forensics principles, standards, and process.
- Two fundamental principles, evidence integrity and chain of custody, are paramount in ensuring the reliability and credibility of digital forensic analysis.

8. Define Evidence Integrity.

- Digital evidence encompasses any digital data containing reliable information that can either support or refute hypotheses regarding an incident or crime.

9. What is chain of custody?

- Chain of custody refers to the documentation of acquisition, control, analysis, and disposition of physical and electronic evidence

10. What is Digital Evidence?

- Digital evidence encompasses any digital data containing reliable information that can either support or refute hypotheses regarding an incident or crime.

11. What are the Layers of Abstraction?

- Digital evidence analysis often involves navigating through layers of abstraction, where higher layers conceal implementation details to reduce complexity.
- Forensic analysts must be capable of analyzing data at various layers of abstraction to extract relevant evidence effectively.

12. Define Metadata.

- Metadata, or data about data, is a valuable source of evidence in digital forensics, providing crucial information about data objects.
- It includes details such as the time of creation, geographical location, and device information, which can be instrumental in solving cases.

13. What is Error, Uncertainty, and Loss?

- Understanding and addressing error, uncertainty, and loss are essential for forensic scientists, as they can significantly impact the interpretation of digital evidence.
- Factors like timestamp inaccuracies, geographical location uncertainties, and data ownership complexities must be carefully considered to avoid misinterpretation.

14. What is Digital forensics process?

- The digital forensic process provides a normative framework for conducting digital forensics investigations.
- It draws upon the structure of traditional physical forensics investigations

while encompassing all necessary phases. These phases span from the initial notification of an incident through the reporting stage to the final presentation of findings.

15. Give one Real-World Example of Digital Evidence.

Online Bank Fraud (SpyEye Case):

- The SpyEye case serves as a comprehensive real-world example of online bank fraud, illustrating the complexity and scale of such cybercrimes.
- The case involved the creation and distribution of malware infecting millions of computers worldwide, compromising numerous bank accounts and causing substantial financial losses.
- It highlights the multi-layered nature of cybercrime investigations, involving collaboration between law enforcement agencies and cyber security experts to combat sophisticated criminal operations.

16. Why Do We Need a Process?

- The forensic process provides a structured approach to investigating digital evidence from any device capable of storing or processing digital data.
- Digital forensics processes must adapt traditional investigation practices to effectively gather and manage digital evidence, supporting end-to-end criminal investigations

17. What are the Challenges in Digital Forensics?

- The uncertainties associated with digital evidence, stemming from both accidental and deliberate factors, must be addressed in forensic investigations.
- The complexities involved in determining the origin and authenticity of digital evidence, highlighting the challenges investigators face.

18. List the Principles of Forensics Process.

- A forensically sound process adheres to established principles, standards, and processes in digital forensics.
- Evaluation of forensic tools' trustworthiness is essential, with initiatives like the NIST's project aimed at creating criteria for evaluating forensics tools.

19. Define Identification Phase.

- The task of detecting, recognizing, and determining the incident or crime to investigate. Incidents come to light through various means such as complaints, alerts, or other indicators.
- The identification phase serves as the cornerstone for all subsequent phases or activities during a digital investigation

20. What is collection phase?

The collection phase in digital forensics involves acquiring relevant data from electronic devices using forensically sound methods. This phase is crucial for obtaining evidence for a forensic investigation

21. What is Examination Phase?

- The Examination Phase in digital forensics is a critical step in the process, where collected data is carefully examined and prepared for analysis
- The examination phase aims to retrieve relevant potential digital evidence from collected data sources

22. What is Analysis Phase?

The Analysis Phase in digital forensics is where forensic investigators delve deep into the collected data to determine the digital evidence that supports or refutes a hypothesis regarding a crime, incident, or event

23. Define Presentation Phase.

- The Presentation Phase in digital forensics involves sharing the results of the analysis phase through reports with interested parties, such as a court of law or corporate management.
- The presentation phase is about documenting and presenting the results of the investigation, based on objective findings with a sufficient level of certainty.

24. What is Anti-Forensics?

Anti-forensics techniques are used to make forensic analysis more challenging. Examples include computer media wiping, encryption, obfuscation, and steganography.

25. What is Automation?

Automation plays a significant role in the examination phase, reducing the manual workload and improving efficiency through tasks such as file parsing and string searches.

26. Define Triage.

Triage is crucial when dealing with large volumes of data, helping to identify the most relevant data quickly based on the severity of the case and available resources.

27. What is Remote Acquisition?

Remote forensic acquisition allows for faster investigation but presents challenges such as data transmission over networks and reduced trust.

28. What are the Forensic File Formats?

- Different file formats are used to store collected data, each with its own impact on forensic analysis effectiveness.
- Formats like EnCase, SMART, AFF, and Prodi cover add more information and flexibility to extracted data.

29. Define Data Recovery.

Even deleted files can often be recovered from storage areas, highlighting the importance of documenting actions to maintain evidence integrity.

30. Define Data Reduction and Filtering.

Techniques like hash lookup and known file databases help filter out irrelevant files, reducing the total amount of data for analysis.

PART – B

1. Give a brief introduction about the concepts of Forensic Science.

- History of Forensic Science
- Locard' s Exchange Principle
- Crime Reconstruction
- Investigations
- Evidence Dynamics

Forensics science:

- Forensic science is the application of scientific methods to establish factual answers to legal problems. It involves the analysis of evidence collected from crime scenes to provide objective information for use in the legal system.

History of Forensic Science :

- Forensic science emerged as a distinct discipline during the 19th and early 20th centuries.
- Pioneers like Mathieu Orfila, Alphonse Bertillon, Francis Galton, Hans Gross, Alberts S. Osborn, Leone Lattes, and Edmond Locard made significant contributions to its development.
- Their work in toxicology, anthropometry, fingerprinting, document examination, blood analysis, and crime scene investigation laid the foundation for modern forensic techniques.

Locard' s Exchange Principle:

- Edmond Locard's exchange principle asserts that whenever someone or something comes into contact with another person or object, there is an exchange of materials between them.
- This principle underpins much of forensic science, as it suggests that evidence can be transferred between individuals, objects, or locations during a criminal act, providing valuable clues for investigators.

Crime Reconstruction

- Crime reconstruction involves piecing together the sequence of events surrounding a crime using scientific methods and evidence.
- By analyzing physical evidence, witness statements, and other relevant information, investigators can reconstruct the actions and events leading up to and following the commission of a crime.
- Crime scene reconstruction helps investigators understand how and why a crime occurred, aiding in the identification of suspects and the presentation of evidence in court.

Investigations

- Investigations are systematic inquiries conducted to gather information and evidence about a crime or incident.
- The 5WH formula (who, where, what, when, why, and how) is commonly used to guide investigations and ensure that all relevant aspects of a case are considered.
- Investigators employ various techniques, such as interviews, surveillance, forensic analysis, and data collection, to uncover facts and establish the truth.

Evidence Dynamics

- Evidence dynamics refer to the changes and interactions that occur with physical or digital evidence over time.
- These dynamics can include additions, alterations, relocations, contamination, or destruction of evidence, whether intentional or unintentional.
- Understanding evidence dynamics is essential for preserving the integrity of evidence and accurately interpreting its significance in an investigation or legal proceeding.

2. Discuss about the concept of Digital Forensics.

- Crimes and Incidents
- Digital Devices, Media, and Objects
- Forensic Soundness and Fundamental Principles
- Crime Reconstruction in Digital Forensics

Definition of Digital Forensics:

- Digital forensics involves the use of scientifically derived methods for the preservation, collection, analysis, and interpretation of digital evidence from various sources. Its primary aim is to reconstruct criminal events or anticipate unauthorized actions that disrupt planned operations.

Specialized Fields within Digital Forensics:

- Terms like network forensics, device forensics, and Internet forensics are used to denote specialized areas within digital forensics, reflecting the diverse range of digital sources and technologies involved.
- The ubiquity of digital technology in society has elevated the importance of digital forensics, as evidenced by its increasing relevance in legal cases involving mobile devices, financial transactions, emails, Internet activities, and GPS systems.

Digital Archaeology and Digital Geology:

- Digital archaeology refers to traces of human behavior in computer systems, while digital geology pertains to traces generated by the inherent processes of computer systems themselves.
- Understanding both digital archaeology and digital geology is crucial for interpreting digital evidence accurately and comprehensively.

Responsibilities of Forensic Scientists in Digital Forensics:

- Forensic scientists play a vital role in establishing factual answers to legal problems through the rigorous processing and analysis of digital evidence.
- This responsibility necessitates adherence to strict standards and procedures to ensure the integrity of the investigation and the reliability of its conclusions.

Crimes and Incidents:

- Digital forensics is applicable in both criminal law and private law contexts, serving as a crucial tool for law enforcement agencies investigating crimes and organizations addressing incidents such as policy violations.
- Incidents in digital forensics encompass digital events or sequences of events, with the scene of the incident analogous to a traditional crime scene.

Digital Devices, Media, and Objects:

- Digital forensics distinguishes between digital devices (e.g., laptops, smartphones), digital media (e.g., hard drives, memory), and digital objects (discrete collections of digital data).
- Forensic analysts primarily work with digital objects, which are collections of digital data derived from digital media.

Forensic Soundness and Fundamental Principles:

- Forensic soundness in digital forensics entails adherence to established principles, standards, and processes throughout the investigation.
- Two fundamental principles, evidence integrity and chain of custody, are paramount in ensuring the reliability and credibility of digital forensic analysis.

Crime Reconstruction in Digital Forensics:

- Crime reconstruction in digital forensics involves a five-step process for event-based reconstruction, including evidence examination, role classification, event construction and testing, event sequencing, and hypothesis testing.
- This method can be applied using physical or virtual test beds to simulate experiments and validate hypotheses in digital forensic investigations.

3. Explain in detail about Digital Evidence.

- Definition of Digital Evidence
- Layers of Abstraction
- Metadata
- Error, Uncertainty, and Loss
- Real-World Example: Online Bank Fraud (SpyEye Case)

Definition of Digital Evidence:

- Digital evidence encompasses any digital data containing reliable information that can either support or refute hypotheses regarding an incident or crime.

Layers of Abstraction:

- Digital evidence analysis often involves navigating through layers of abstraction, where higher layers conceal implementation details to reduce complexity.
- Forensic analysts must be capable of analyzing data at various layers of abstraction to extract relevant evidence effectively.

Metadata:

- Metadata, or data about data, is a valuable source of evidence in digital forensics, providing crucial information about data objects.
- It includes details such as the time of creation, geographical location, and device information, which can be instrumental in solving cases.

Error, Uncertainty, and Loss:

- Understanding and addressing error, uncertainty, and loss are essential for forensic scientists, as they can significantly impact the interpretation of digital evidence.
- Factors like timestamp inaccuracies, geographical location uncertainties, and data ownership complexities must be carefully considered to avoid misinterpretation.

Real-World Example: Online Bank Fraud (SpyEye Case):

- The SpyEye case serves as a comprehensive real-world example of online bank fraud, illustrating the complexity and scale of such cybercrimes.
- The case involved the creation and distribution of malware infecting millions of computers worldwide, compromising numerous bank accounts and causing substantial financial losses.
- It highlights the multi-layered nature of cybercrime investigations, involving collaboration between law enforcement agencies and cyber security experts to combat sophisticated criminal operations.

4. Explain about The Digital Forensics Process.

- The digital forensic process provides a normative framework for conducting digital forensics investigations.
- It draws upon the structure of traditional physical forensics investigations while encompassing all necessary phases. These phases span from the initial notification of an incident through the reporting stage to the final presentation of findings.
- Adherence to a defined process is crucial for identifying digital objects that reflect relevant facts, whether in criminal or civil courts of law, or in corporate and private investigations.
- This process functions as a component of a quality assurance system for digital forensics.
- The process is delineated into five consecutive but iterative phases, each serving a distinct purpose: Figure 1.1 shows the chain of Custody and Evidence Integrity.

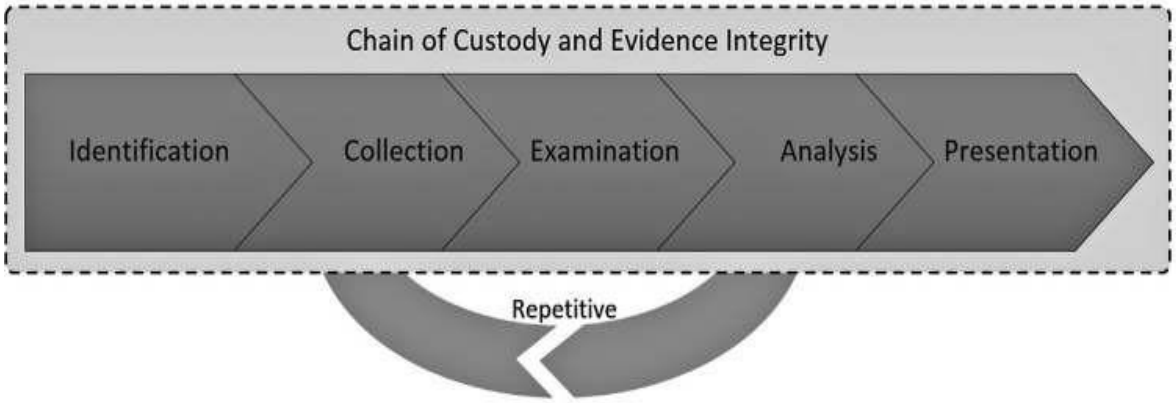

Figure 1.1. The chain of Custody and Evidence Integrity.

1. **Identification of Potential Evidence Sources:** In this phase, potential evidence sources are identified from digital devices involved in the investigation.
2. **Collection of Digital Raw Data:** Once potential evidence sources are identified, digital raw data is collected by copying the source in a forensically sound manner.
3. **Examination of Raw Data:** The raw data is examined in this phase, where it is organized and structured to facilitate processing and comprehension.
4. **Analysis:** The analysis phase aims to gain a deeper understanding of the data and identify digital objects that serve as evidence to be presented in court or to relevant entities.
5. **Reporting and Presentation:** Finally, the findings of the analysis are reported and presented to the appropriate stakeholders, whether in court or within the investigative entity.

While the process is described as a step-by-step progression, it is acknowledged that multiple iterations of several phases may be necessary. This iterative approach allows for thorough examination and analysis of the digital evidence, ensuring comprehensive investigative outcomes.

5. Give an introduction about Evolution of Cybercrime.

Evolution of Cybercrime:

- Over the past decade, cybercrime has undergone significant evolution driven by factors such as technologically adept attackers, advanced technology, and strong incentives.
- Cybercriminals now execute sophisticated attacks exploiting extensive digital networks and numerous endpoints simultaneously, leading to data breaches and disclosures.
- The prevalence of cybercrime underscores the necessity for well-defined forensic investigation processes and appropriate tools to investigate incidents effectively.

Challenges in Digital Forensics:

- The uncertainties associated with digital evidence, stemming from both accidental and deliberate factors, must be addressed in forensic investigations.

Adapting to Technological Advancements:

- The dynamic nature of the digital landscape necessitates continual adaptation of digital forensics practices.
- While cybercrimes may evolve in complexity, the tools available to investigators also advance, aiding in the investigation process.

Why Do We Need a Process?

- The forensic process provides a structured approach to investigating digital evidence from any device capable of storing or processing digital data.

- Digital forensics processes must adapt traditional investigation practices to effectively gather and manage digital evidence, supporting end-to-end criminal investigations

Universal Application of the Process:

- The digital forensics process is universally applicable to investigations involving various digital devices and technologies, including computer forensics, mobile forensics, and Internet forensics.
- It facilitates the identification of evidence crucial for answering key investigative questions.

Principles of a Forensics Process:

- A forensically sound process adheres to established principles, standards, and processes in digital forensics.
- Evaluation of forensic tools' trustworthiness is essential, with initiatives like the NIST's project aimed at creating criteria for evaluating forensics tools.

Finding the Digital Evidence:

- Digital evidence, defined in alignment with Carrier and Spafford (2004a, 2004c), encompasses any digital data supporting or refuting hypotheses about incidents or crimes.
- The digital forensics process involves identifying potential evidence sources, collecting digital raw data, examining and analyzing the data, and presenting findings to courts or relevant entities.

Iterative Nature of the Process:

- The digital forensics process is iterative, often requiring multiple iterations for different potential evidence sources.
- Each source undergoes collection, examination, and analysis phases, with simultaneous analysis of data from multiple sources to establish correlations and form conclusive evidence.

6. Explain about the concept of Identification Phase in digital forensics.

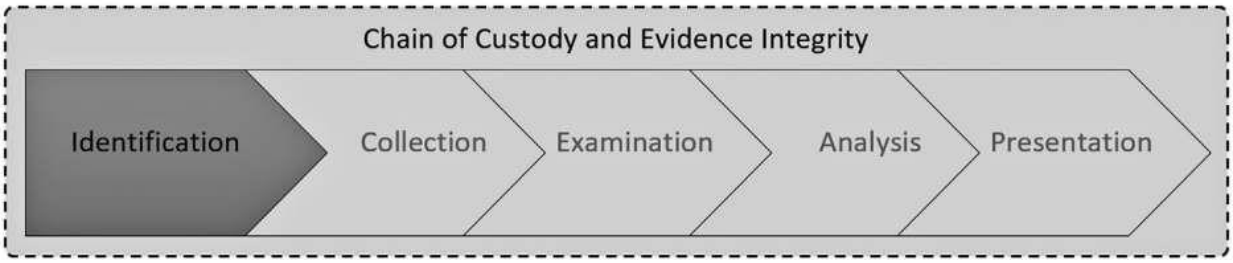

Figure 1.2 Digital forensics process: Identification Phase

- Incidents come to light through various means such as complaints, alerts, or other indicators.
- The identification phase serves as the cornerstone for all subsequent phases or

activities during a digital investigation.

- It helps determine which evidence or objects to focus on, leading to the formation of a hypothesis about the event or crime. Figure 1.2 shows the digital forensics process: Identification Phase.

Preparations and Deployment of Tools and Resources

- Effective planning is essential to ensure the efficiency and success of an investigation, regardless of its nature. This section emphasizes the importance of proper preparation before an incident occurs.

- It highlights the need for a well-trained investigative team and access to necessary resources and tools. Additionally, guidelines for establishing a forensics laboratory and evaluating forensic tools' integrity and compliance with evidence standards are discussed.

The First Responder

- The first responder, typically a police officer in criminal cases, plays a crucial role in handling potential evidence, including digital devices, at the scene of an incident.

- Standard operating procedures (SOPs) are essential to guide evidence identification activities and maintain evidence integrity. Figure 6.1 underscores the importance of adhering to proper procedures to avoid compromising evidence, as demonstrated by a real-life case.

At the Scene of the Incident

- Understanding the characteristics of a digital crime scene and ensuring proper preservation of evidence are key aspects discussed in this section.

- Whether in a private home or a corporate setting, identifying and securing potential evidence sources is crucial. The section also emphasizes the need for meticulous documentation throughout the investigation process.

Dealing with Live and Dead Systems

- Differentiating between live and dead systems is vital in digital forensics investigations. Special precautions must be taken to prevent data loss or alteration, whether a system is powered on or off.

- Considerations for preserving evidence integrity and minimizing the risk of unintended changes are discussed.

Chain of Custody

- Maintaining the chain of custody is paramount for ensuring the admissibility of evidence in legal proceedings. Proper documentation of handling procedures, including who handled the evidence, when and how it was acquired, and any changes made, is essential.

- The section stresses the importance of integrity checks and timestamps to support the chain of custody and mitigate the risk of evidence exclusion from a case.

7. Explain about The Collection Phase in digital forensics.

. Introduction

The collection phase in digital forensics involves acquiring relevant data from electronic devices using forensically sound methods. This phase is crucial for obtaining evidence for a forensic investigation. Figure 1.3 shows the Digital Forensics process: Collection Phase

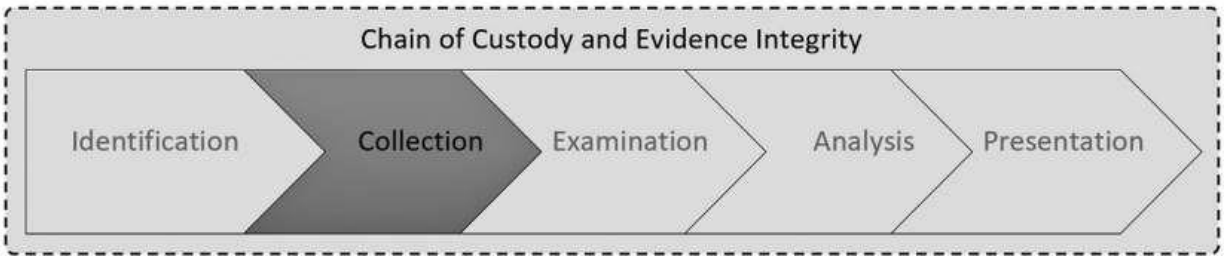

Figure 1.3 digital forensics process: Collection Phase

Key Points

1. **Purpose of Collection Phase**: The collection phase involves making a digital copy of data using approved methods to ensure forensic soundness.
2. **Metadata**: Metadata about the case should be tied to potential evidence, including case details, timestamps, and location information.
3. **Example Case**: The SpyEye online banking fraud case illustrates the variety of potential evidence sources, including victim computers, bank records, malware evidence, server logs, and network monitoring data.
4. **Sources of Digital Evidence**: Digital evidence can be found in various sources such as hard drives, flash drives, memory, smartphones, computer networks, and the Internet.
5. **Physical Location of Systems**: In cases where systems cannot be moved, data must be collected at their physical location.
6. **Multiple Evidence Sources**: Digital evidence is often distributed across multiple devices and locations.
7. **Evidence Reconstruction**: Media storing data may be damaged intentionally or unintentionally, requiring data recovery techniques.
8. **Evidence Integrity**: Maintaining evidence integrity is critical, achieved through measures like write blockers and cryptographic hashes.
9. **Order of Volatility**: Prioritizing data collection based on the volatility of data sources helps preserve critical evidence.
10. **Dual-Tool Verification**: Using multiple forensic tools to verify results enhances confidence in the integrity of collected evidence.
11. **Remote Acquisition**: Remote forensic acquisition allows for faster

investigation but presents challenges such as data transmission over networks and reduced trust.

12. **Global Cooperation**: In multinational cases, collaboration between forensic units from different countries is essential for successful investigations.

Conclusion

The collection phase is a fundamental step in digital forensics, involving the acquisition of data from various sources using approved methods. Ensuring evidence integrity, prioritizing data collection, and leveraging global cooperation are essential for successful investigations.

8. Explain in detail about The Examination Phase of digital forensics.

in detail.

The Examination Phase in digital forensics is a critical step in the process, where collected data is carefully examined and prepared for analysis. Let's break down some key points from the text. Figure 1.4 shows digital forensics process: Examination Phase

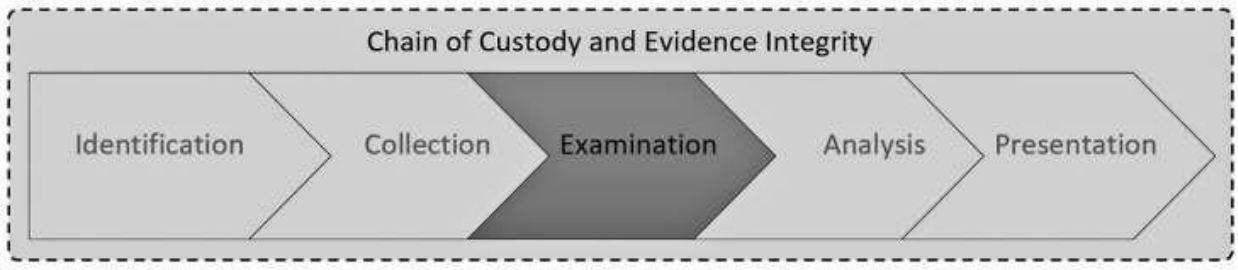

Figure 1.4 digital forensics process: Examination Phase

1. **Purpose**: The examination phase aims to retrieve relevant potential digital evidence from collected data sources.
2. **Preparation and Extraction**: This phase involves preparing and extracting potential digital evidence from the collected data sources. Digital forensics tools are often used to automate these tasks, but manual examination is also important for experienced forensic investigators.
3. **Triage**: Triage is crucial when dealing with large volumes of data, helping to identify the most relevant data quickly based on the severity of the case and available resources.
4. **Data Examination Techniques**: Various techniques such as file hashing, keyword searches, and metadata extraction are employed to structure and organize data for analysis.
5. **Forensic File Formats**: Different file formats are used to store collected data, each with its own impact on forensic analysis effectiveness. Formats like EnCase, SMART, AFF, and Prodi cover add more information and flexibility to extracted data.

6. **Data Recovery**: Even deleted files can often be recovered from storage areas, highlighting the importance of documenting actions to maintain evidence integrity.
7. **Data Reduction and Filtering**: Techniques like hash lookup and known file databases help filter out irrelevant files, reducing the total amount of data for analysis. Figure 1.5 shows Examination Phase: Data Reduction and Filtering

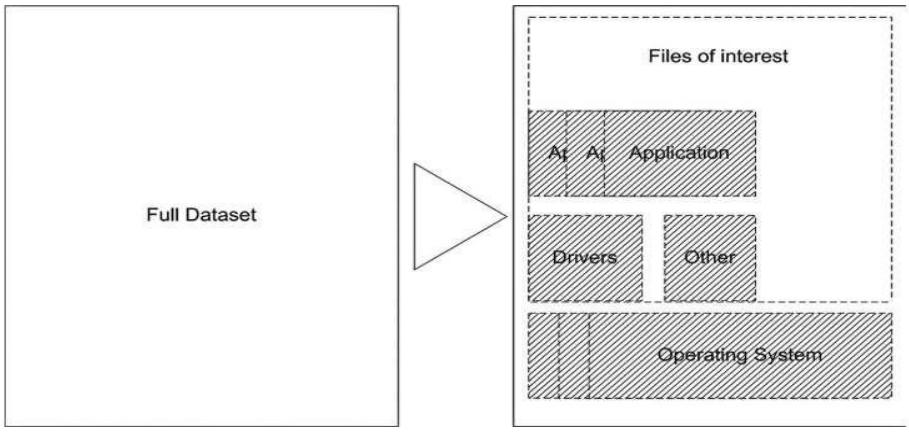

Figure 1.5 Examination Phase: Data Reduction and Filtering

8. **Timestamps**: Recording correct timestamps aids in correlating data across multiple sources, though adjustments may be needed for time zone differences.
9. **Compression, Encryption, and Obfuscation**: Compressed and encrypted files must be handled appropriately during examination, which may involve decompression or decryption. Obfuscation techniques like steganography add complexity to forensic analysis.
10. **Data and File Carving**:

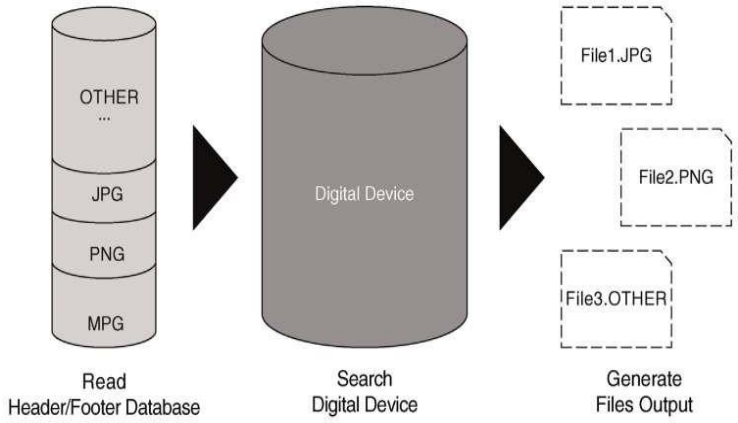

Figure 1.6 Examination Phase: Data and File Carving

Tools and techniques are used to parse and carve unstructured and raw binary data, helping to recover potentially valuable evidence from collected data sources. Figure1.6 Shows Examination Phase: Data and File Carving

11. **Automation**: Automation plays a significant role in the examination phase, reducing the manual workload and improving efficiency through tasks such as file parsing and string searches.

By following these steps and employing various techniques and tools, forensic investigators can effectively examine and prepare digital evidence for further analysis and investigation.

9. Explain about The Analysis Phase of digital forensics in detail.

The Analysis Phase in digital forensics is where forensic investigators delve deep into the collected data to determine the digital evidence that supports or refutes a hypothesis regarding a crime, incident, or event. Here's a breakdown of key points from the text: Figure 1.7 The digital forensics process: Analysis Phase

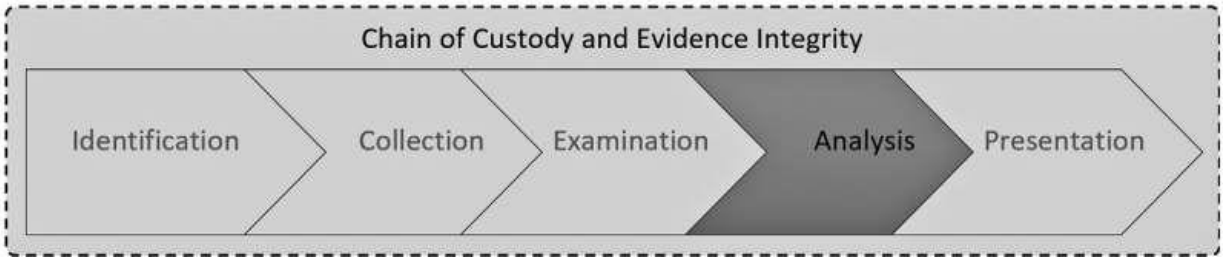

Figure 1.7 digital forensics process: Analysis Phase

1. **Purpose**: The analysis phase involves processing information to determine the facts about an event, the significance of the evidence, and the person(s) responsible.
2. **Techniques Used**: Techniques such as statistical methods, manual analysis, data format understanding, data mining, and time lining are employed during analysis. Computational methods and machine learning are also applied for automating analysis tasks and recognizing patterns.
3. **Iterative Process**: The analysis phase is iterative, with investigators forming and testing hypotheses about the case, often requiring the collection of additional data objects until the results are sufficient for the investigation's purpose.
4. **Layers of Abstraction**: Different layers of data interpretation exist, such as what end-user applications see, what the operating system sees, and what is stored in bits and bytes on the storage device. Understanding these layers is crucial for accurate analysis.
5. **Evidence Types**: The type of evidence depends on the nature of the crime. Examples include email communications, malicious applications, and data related to cybercrimes or physical crimes.
6. **String and Keyword Searches**: String and keyword searches simplify analysis, allowing investigators to search for specific information relevant to the case, such as names, addresses, or sensitive data like Social Security or credit card numbers.
7. **Anti-Forensics**: Anti-forensics techniques are used to make forensic analysis more challenging. Examples include computer media wiping, encryption, obfuscation, and steganography.

8. **Automated Analysis**: Automation plays a significant role in analyzing large data volumes and obfuscated malware. Computational forensics methods, data mining, and forensic analytics are employed to identify and analyze relevant evidence.
9. **Time lining of Events**: Time lining helps in understanding the sequence of events, especially useful in criminal investigations. File and system logs, along with physical and digital events, contribute to creating timelines.
10. **Graphs and Visual Representations**: Graphs and visual representations help in understanding relationships between data objects, individuals, and network interactions, aiding in investigative analysis.
11. **Link Analysis**:

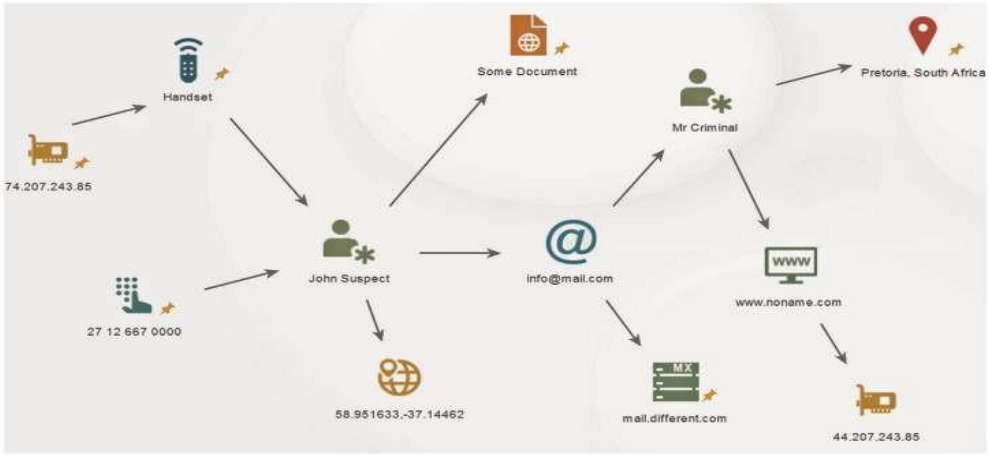

Figure 2.19 Graphical representation of connected entities in digital evidence with Maltego.

Figure 1.8 Graphical representation of connected entities in digital evidence with Meltego

12. Link analysis is used to identify and visualize relationships among interconnected objects, providing insights into complex networks of data. It's valuable in various domains, including digital forensics, law enforcement, and intelligence.

By employing these techniques and tools, forensic investigators can effectively analyze digital evidence to uncover crucial insights and facts about a case, helping to support or refute hypotheses and identify responsible parties.

10. Explain Presentation Phase of digital forensics in detail.

The Presentation Phase in digital forensics involves sharing the results of the analysis phase through reports with interested parties, such as a court of law or corporate management. Here's a breakdown of key points from the text Figure 1.9 shows digital forensics process: Presentation Phase

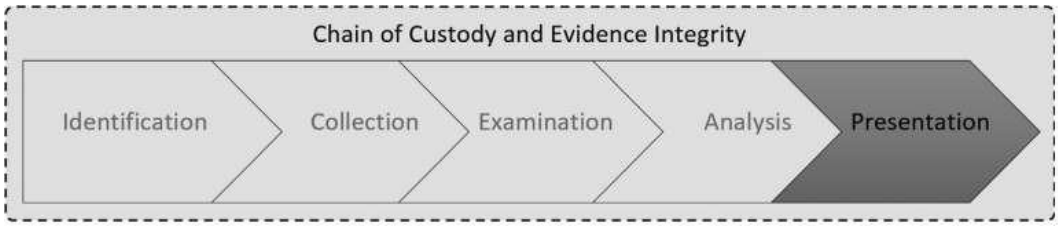

Figure 1.9 digital forensics process: Presentation Phase

1. **Purpose**: The presentation phase is about documenting and presenting the results of the investigation, based on objective findings with a sufficient level of certainty. It involves summarizing findings and describing all actions taken during the investigation in a clear and understandable manner.
2. **Final Reports**: The final report should include relevant case management information, such as roles and tasks assigned, executive summaries of information sources and evidence, forensic acquisition and analysis details reflecting chain of custody and evidence integrity, visualizations, tools used, and findings. While digital forensics tools have reporting functionality, the investigator must ensure that the report is understandable to a third party and sufficiently documents reproducibility.
3. **Presentation of Evidence**: Visual aids such as diagrams, graphics, and timelines are valuable for presenting complex information in an accessible way. Visualizations help identify patterns and information that may not be immediately obvious from text alone.
4. **Chain of Custody**: Documenting the chain of custody is crucial for maintaining the integrity of the evidence presented in court. It ensures that all activities conducted during the investigation are documented and can be verified. Failure to document the chain of custody could compromise the trust in the authenticity and integrity of the evidence in court.
5. **Final Presentation**: The documented evidence, methods used, and expert testimony form the basis of the final presentation to a court of law or corporate audience, depending on the context of the investigation.

UNIT - 2

UNIT 2 DIGITAL CRIME AND INVESTIGATION

Digital Crime – Substantive Criminal Law – General Conditions – Offenses – Investigation Methods for Collecting Digital Evidence – International Cooperation to Collect Digital Evidence

PART - A

1. **What is cybercrime law?**

The expression cybercrime law is applied to signify the "legal regulation of digital crime and digital evidence." Crime and evidence are different phenomena governed by different sets of legal rules

2. **Define criminal offences.**

A criminal offense is defined by the conditions set out by a provision laid down in formal legislation of the national legal system. The provision must be in force when the crime was committed

3. **What is Coercive Investigation Method?**

An investigation method is coercive when it lawfully can be applied against an individual without her consent or cooperation, despite that her right to personal liberty, property, or private life is interfered with.

4. **Define Organized Criminal Group.**

Organized criminal group is a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes. In order to obtain, directly or indirectly, a financial or other material benefit.

5. **Define Computer Data.**

Computer data means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

6. **What is illegal access?**

"The access to the whole or any part of a computer system without right." National legislation may apply the condition that the offence be committed by in fringing security measures.

7. **What is illegal interception?**

The interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electro magnetic emissions from a computer system carrying such computer data.

8. **Compare Data and system Interference.**

Data interference	System interference
• The damaging, deletion, deterioration, alteration or suppression of computer data without right. • National criminal law may apply the condition that the conduct results in serious harm	• The serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

9. What do you mean by Racist and Xenophobic Speech?

Racist or xenophobic material means any written material, any image or any other Representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, color, descent or national or ethnic origin, as well as religion if used as pretext for any of these factors.

10. Write about the search of a smartphone.

- A person arrived at the airport with fake ID documents. Icelandic police officers seized his smartphone, reckoning that it contained information that could reveal his identity.
- The seizure was lawful, but search of the smartphone could not lawfully be conducted without a new permission by the court. It was relevant that a smartphone contains content stemming from communication, which is at the core of the protection of the ECHr article 8.
- The judgment was followed up with a second judgment the same season (spring 2016). The need for explicit permissions both for seizure and search is thus settled Icelandic law.

11. What are the Real Time Investigation methods?

- Traffic data, in real-time, associated with specified communications in its Territory transmitted by means of a computer system.

- Content data, in real-time, of specified communications in its territory Transmitted by means of a computer system.

12. Compare search and Seizure.

Search	Seizure
(a). Computer system or part of it and computer data stored there in. (b) a computer-data storage medium in which computer data may be stored	(a) Seize or similarly secure a computer system or part of it or a computer-data storage medium. (b)make and retain a copy of those computer data; (c) maintain the integrity of the relevant stored computer data; (d) render inaccessible or remove those computer data in the accessed computer system."

13. What is production order?

- Production order is a means for getting access to digital evidence in possession of a third party that is cooperative with the law enforcement agency.
- Article 18 imposes an obligation on the parties to authorize this method in national legislation. The method is traditional, so article 18 only clarifies its application to computer data. The order can concern historical data and future data

14. Infer the Megaupload.com.

In January 2012, the site Megaupload.com was seized and shut down by the US Department of Justice, charged with criminal copyright infringement and racketeering. The site had 66.6 million users, whose accounts thus became inaccessible. US officials claimed that the investigation was not directed at individual users, but at individuals who had offered and made profits from the services. Still, millions of users were affected by the measure.

15. What are the Conditions and Safeguards Concerning Coercive Methods?

Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

16. What is the Scope of the Investigation Methods?

Each Party shall apply the powers and procedures to

a) The criminal offences established in accordance with Articles2 through 11 of this Convention.

b) Other criminal offences committed by means of a computer system.

c) The collection of evidence in electronic form of a criminal offence.

17. How to Identity Theft in Relation to Fraud?

Identity theft in relation to fraud may entail the misappropriation of the identity (such as the name, date of birth, current address, or previous addresses) of another person, without their knowledge or consent. These identity details are then used to obtain goods and services in that person's name.

18. Explain any example for the Offenses Related to Infringements of Copyright and Related Rights.

The article confers an obligation to criminalize acts that impinge on the rights laid down in a number of treaties concerning the protection of copyrights and related rights, where such acts are committed willfully, on a commercial scale, and by means of a computer system.

- The Agreement on Trade-Related Aspects of Intellectual Property Rights
- The WIPO Copyright Treaty
- The International Convention for the Protection of Performers, Producers of Phono-grams and Broadcasting Organization's (Rome Convention)

PART - B

1. **Explain about the Digital Crime – Substantive Criminal Law.**

The Cybercrime Convention categorizes criminal offenses into four main groups:

1. **Offenses against Confidentiality, Integrity, and Availability of Computer Data and Systems (Articles 2-6):** These include unauthorized access, interception of data, data interference, system interference, and misuse of devices.
2. **Computer-related Offenses (Articles 7 and 8):** This category covers computer-related forgery and fraud, involving the creation, alteration, or suppression of computer data with fraudulent intent.
3. **Content-related Offenses (Article 9):** Offenses related to child sexual abuse material, encompassing the creation, distribution, or possession of pornographic material involving minors.
4. **Infringements of Copyright and Related Rights (Article 10):** Violations involving unauthorized use or distribution of copyrighted works and related rights.

Additionally, the Convention addresses aiding, abetting, and attempt to commit offenses (Article 11) and corporate liability (Article 12), holding legal entities accountable for committing offenses.

Article 13 mandates that crimes must be punishable by effective, proportionate, and dissuasive sanctions, including deprivation of liberty. The national legal provisions prescribe maximum penalties for each offense, ensuring consistency in sentencing practices. However, actual punishment may vary between jurisdictions due to differences in legal principles, social and cultural traditions. To address disparities, some jurisdictions develop sentencing guidelines or appoint advisory bodies to suggest standard rates for certain offenses.

2. **Elaborate the general Conditions for Criminal Liability.**

To secure a conviction for a criminal offense, certain conditions must be met, encompassing both objective and subjective elements:

- Objective Conditions of the Offense
- Subjective Conditions of Intent
- Criminal Capability
- Absence of Legal Justifications
- Criminal Capability
- Absence of Legal Justifications
- Moment of Committing the Act
- Subjective Condition and Interpretations
- Attempt, Aiding, and Abetting
- Individual Judgment and Punishment
- Legal Application and Jurisdictional Variations

- **Objective Conditions of the Offense**
  - The act must be defined as criminal by law, specifying its scope and parameters.
  - This includes the "When, Where, and How" aspects of the offense.

- **Subjective Conditions of Intent:**
  - The individual must have acted with intent (dolus), signifying awareness and volition.
  - Intent is inferred from words like knowingly, intentionally, or forsett.
  - It must cover all objective conditions and pertains to the "Why" aspect of the offense.

- **Criminal Capability:**
  - The individual must meet age and mental capacity requirements determined by law.
  - Primarily addresses the "Who" aspect of the offense.

- **Absence of Legal Justifications:**
  - No circumstances should render an otherwise criminal act lawful, such as emergency situations.
  - Concerns the "When, Where, How, and Why" of the offense.

- **Moment of Committing the Act:**
  - All conditions must be fulfilled by the perpetrator at the time of committing the crime.
  - Time frame ranges from split-second actions to prolonged behaviors.

- **Subjective Condition and Interpretations:**
  - Unintentional actions do not lead to criminal liability.
  - Good intentions do not negate criminal intent.
  - Error regarding relevant facts negates intent.
  - Proof of intent is crucial for establishing liability.

- **Attempt, Aiding, and Abetting:**
  - Attempt requires action with intent to complete the crime.
  - Aiding and abetting involve intentionally assisting or encouraging the main perpetrator.
  - Organized crime liability can extend beyond direct involvement.

- **Individual Judgment and Punishment:**
  - Each suspect is judged based on their actions and intent.
  - Punishment is individually determined but tends to be uniform for similar offenses.
- **Legal Application and Jurisdictional Variations:**
  - Legal provisions vary across jurisdictions, impacting the elements required for conviction.

- Evidence must align with the specific legal requirements of the jurisdiction trying the case.

Understanding and applying these conditions systematically is essential for building a case and ensuring the proper adjudication of criminal offenses.

3. **Explain in detail about the concept of Offenses.**

The Cybercrime Convention aims to address offenses against the confidentiality, integrity, and availability of computer data and systems. Here's a summary of key points regarding these offenses:

- Focus on Data Protection
- Definition of Computer Data and System
- Illegal Access and Interception
- Security Measures
- Protection of Communication
- Protection Levels
- Completion of Offenses
- Information Fencing
- Password Intrusion vs. Identity Theft
- Interference with Security Measures
- Definition of Access
- Data and System Interference

- **Focus on Data Protection:** The convention prioritizes the protection of computer data rather than physical equipment. Computer data is broadly defined to include any representation of facts, information, or concepts processed by a computer system.

- **Definition of Computer Data and System:** Computer data encompasses user-generated content and program files, while a computer system includes any device or group of interconnected devices that automatically process data.

- **Illegal Access and Interception:** Offenses such as illegal access and interception are addressed by the convention. Illegal access refers to gaining unauthorized access to a computer system, often by circumventing security measures. Illegal interception involves capturing non-public transmissions of computer data without authorization.

- **Security Measures:** National legislation may require offenses to involve the infringement of security measures for them to be considered illegal access. Circumvention of security measures can occur through password intrusion or exploiting system vulnerabilities.

- **Protection of Communication:** Illegal interception protects private communications, whether they occur between different systems or within a computer system itself. This includes safeguarding against keystroke loggers and other methods used to intercept sensitive information.

- **Protection Levels:** Articles 2 and 3 of the convention provide different levels of protection. Article 2 protects against illegal access to computer systems, while Article 3 protects against the interception of non-public data during transmission.

- **Completion of Offenses:** An offense under Article 2 is completed once access has been gained, whereas an offense under Article 3 is completed when interception succeeds. Both articles may apply to successive steps of criminal activity, along with Article 5, which covers system interference.

- **Information Fencing:** While Articles 2 and 3 do not directly protect property rights to data, the concept of information fencing has developed in national legal systems. Information fencing involves dealing unlawfully with stolen or copied data, especially if it has economic value.

- **Password Intrusion vs. Identity Theft:** Password intrusion differs from identity theft, as it involves breaching computer security rather than interfering with the right to private life. The immediate victim of password intrusion is the owner of the password, not a third party defrauded by identity theft.

- **Interference with Security Measures:** There is debate over whether automatic circumvention of security measures, such as CAPTCHA, constitutes illegal access. The interpretation may depend on technical hindrances, contractual conditions, and social norms within national legal rules.

- **Definition of Access:** "Access" is interpreted to imply control over a computer system or user account. Sending emails or files to a system is not considered access unless it is done without right, such as through a Trojan attachment.

- **Data and System Interference:** Articles 4 and 5 of the convention address damaging, deletion, alteration, or suppression of computer data (Article 4) and serious hindrance to the functioning of a computer system (Article 5). These offenses supplement traditional vandalism provisions and cover actions such as DDOS attacks and insertion of malware.

- **Article 4 - Data Interference:**
  - Article 4 covers any interference with computer data, but if the interference affects the computer system itself, it might be considered vandalism under traditional provisions or serious hindrance under Article 5.
  - Examples of actions covered by Article 4 include deleting a user registry on a cloud service, changing passwords, replacing files with defacing web pages, or encrypting files for extortion.

- **Article 5 - System Interference:**
  - Article 5 addresses serious hindrance to the functioning of a computer system, such as DDOS attacks or insertion of malware that slows down or stops the system.
  - Malware, including logical bombs, spyware, and backdoors, can interfere with system functioning, and the critical point for completion of the offense is when the malware is inserted.

- **Article 6 - Misuse of Devices:**
  - Article 6 addresses the production, sale, procurement, import, distribution, or making available of devices or data primarily designed for committing offenses mentioned in Articles 2-5.
  - There's no obligation to criminalize if the motive is other than committing these offenses.
  - The provision covers physical devices (e.g., keystroke loggers) and computer programs (e.g., malware) designed for illegal purposes.

3. Explain the Investigation Methods for Collecting Digital Evidence.

In the context of criminal procedure and digital forensic investigations, several key points are worth noting:

- Collection of Digital Evidence
- Digital Forensic Process
- Search and Seizure of Digital Evidence:
- Terminology and Misunderstandings
  - Trans border Access to Stored Computer Data Where Publicly Available
  - Online Undercover Operations
  - Scope and Safeguards of Investigation Methods
  - Search and Seizure (Article 19)
  - Production Order

- **Collection of Digital Evidence:**

  - The main aim of a criminal investigation is to collect evidence to identify suspects and prove or disprove alleged crimes.
  - Each investigative step must be justified based on the nature of the crime and specific circumstances, preventing arbitrary interference and waste of resources.
  - The principle of relevancy applies to every investigative method, including digital evidence collection.

- **Digital Forensic Process:**
  - Digital investigations should adhere to the digital forensic process to ensure forensic soundness, evidence integrity, and chain of custody.
  - The digital forensic process must fit into the framework of procedural criminal law, considering relevancy, legality, and the right to a fair trial.
- **Search and Seizure of Digital Evidence:**
  - Search involves looking for evidence, while seizure means taking control over it.
  - In the digital forensic process, the distinction between search and seizure might not be apparent; legal definitions are determined by conditions in procedural law.
  - In a scenario where police seize a suspect's laptop, the crucial point in time determines whether the data is seized or not.
  - Seizure triggers the suspect's legal right to challenge it, potentially leading to the return of the seized material if a court deems it irrelevant.
- **Terminology and Misunderstandings:**
  - Terms like "securing data" may have different meanings in multidisciplinary teams, leading to misunderstandings, especially regarding breaches of procedure.
  - Whether a deviation from the digital forensic process affects the admissibility of evidence depends on national legal rules and principles of fair trial.
- **Trans border Access to Stored Computer Data Where Publicly Available:**
  - According to the Cybercrime Convention's Article 32(a), a party can access publicly available stored computer data without authorization from another party, regardless of its geographical location.
  - "Publicly available (open source) stored computer data" refers to data accessible to the public, such as information on websites or services that anyone can access without restrictions.
  - Law enforcement officials can subscribe to or register for services available to the public to access data for investigative purposes.
  - The term "stored" excludes real-time methods like interception, and the data must be publicly available.
- **Online Undercover Operations:**
  - The Cybercrime Convention doesn't explicitly address undercover operations, but its international cooperation procedures can facilitate such activities.
  - Online undercover operations involve activities like identifying, viewing, and downloading copyright-infringing materials, opening premium accounts on websites for analysis, and performing network analysis.
- **Scope and Safeguards of Investigation Methods:**
  - The Cybercrime Convention outlines investigation methods such as preservation and production order, search and seizure, and real-time collection of traffic data and interception of content data.
  - These methods must be implemented in national procedural legislation for specific criminal investigations or proceedings and are suspicion-based.
  - The scope of the methods includes criminal offenses established by the convention, other offenses committed using a computer system, and the collection of electronic evidence of any criminal offense.

- Safeguards include adherence to procedural principles of legality and proportionality, judicial or independent supervision, grounds justifying application, and limitation of scope and duration.
- Examples illustrate the impact of investigation methods on third parties, such as the seizure of Megaupload.com affecting millions of users and the balancing of rights in the analysis of seized computer files.

➢ **Search and Seizure (Article 19)**

The competent authority shall be empowered to

1) Search

a). Computer system or part of it and computer data stored there in.

b). a computer-data storage medium in which computer data may be stored

2) Seizure

Seize or similarly secure computer data accessed [by a search pursuant to These measures shall include the power to

(a) seize or similarly secure a computer system or part of it or a computer-data storage medium;

(b) make and retain a copy of those computer data;

(c) maintain the integrity of the relevant stored computer data;

(d) render inaccessible or remove those computer data in the accessed computer system.

Production Order:

- Article 18 of the Cybercrime Convention allows for the use of production orders to access digital evidence held by third parties cooperating with law enforcement agencies.
- These orders apply to both historical and future data.
- Production orders may be necessary even if the third party is cooperative due to legal duties of confidentiality, data protection rules, or commercial preferences.
- The suitability of a production order depends on the accessibility of the data; if data is readily accessible, seizure may be more practical.
- Subscriber data, such as identity data about subscribers to e-commerce services, can be subject to production orders.
- National legislation determines the procedures for production orders and the grounds for issuing them.
- Expedited preservation orders (Articles 16 and 17) are used to preserve stored data or traffic data when immediate seizure is not possible.
- Real-time investigation methods (Articles 20 and 21) allow for the collection or recording of traffic data or content data of specified communications in real-time, subject to suspicion-based limitations and specific communication addresses.
- These methods may involve technical means such as IMSI catching, silent SMS, or bulk data collection from mobile base stations.

4. Describe the International Cooperation to Collect Digital Evidence in detail .

International Cooperation in Collecting Digital Evidence

Principle of Sovereignty

- Law enforcement agencies' power is limited to their nation's territory.
- Accessing evidence in another state without permission violates that state's sovereignty.

Securing Evidence Abroad:

- Requesting assistance from the state where evidence is located is necessary to avoid sovereignty violations.

Narrowing Focus:

- Various procedures exist for international cooperation against crime.
- Focus here is on procedures for collecting evidence through coercive measures.
- Not required for collecting information from publicly available Internet sites.

Mutual Legal Assistance vs. Police Cooperation:

- Mutual legal assistance procedures used when obtaining evidence through coercive measures.
- Police cooperation useful in preparing for such requests.
- Involves requesting state (seeking assistance) and requested state (receiving request).

Definition of Digital Evidence:

- Audio or video-recorded testimony not considered digital evidence.
- Digital evidence includes objects collected through computer surveillance or interception of electronic communications.
- Information in police registries not considered digital evidence; governed by data protection rules for international exchanges.

Trans border Access to Digital Evidence

Accessibility vs. Geographical Localization:

- Global communication networks and cloud services make digital evidence technically accessible globally.
- Criteria for international cooperation may shift from territorial localization to controllability of computer data.

Article 32(b) of the Cybercrime Convention:

- Allows a party to access stored computer data in another party with lawful and voluntary consent.
- Challenges exist in determining the exact location of stored data and obtaining lawful and voluntary consent.

Mutual Legal Assistance

Basic Principles and Formal Steps:

- No obligation for a nation state to provide assistance in securing digital evidence without a cooperation treaty.
- Requesting state must demonstrate reciprocity and legal basis for the requested assistance.
- Formal request must describe the crime, cite relevant legal provisions, and demonstrate legal permission.

International Conventions Concerning Mutual Legal Assistance:

- Cybercrime Convention obligates parties to assist each other in collecting digital evidence.
- Dual criminality principle applies, but some flexibility exists regarding offenses' classification.
- EU and other international conventions supplement mutual legal assistance efforts, facilitating cooperation in criminal matters.

EU's Role:

- EU conventions and agreements with non-member states enhance mutual legal assistance and cooperation in criminal matters.
- Euro just system facilitates practical cooperation procedures among prosecutors and courts within the EU.

Nordic Cooperation:

- Nordic countries have a history of close cooperation, reducing bureaucracy and increasing efficiency.
- Different procedures apply once a non-Nordic state is involved in cooperation efforts.

International Police Cooperation and Joint Investigation Teams Informal Cooperation:

- Traditionally, police officers cooperated informally through channels like Interpol or direct phone calls.
- Liaison officers stationed abroad may also assist in cooperation efforts.
- Europol and its European Cybercrime Center (EC3) play a significant role in combating organized crime, including cybercrimes.

Formal Procedures for Cooperation:

- Formal procedures of mutual legal assistance are necessary to support requests for coercive methods.
- Informal assistance from foreign police officers may help explore options before formal requests.

Subscriber Data Disclosure:

- In some jurisdictions, subscriber data may be directly disclosed to criminal investigators in the police, facilitating cooperation.
- Routine procedures for police cooperation observe data protection rules applicable to international police cooperation.

Schengen Information System (SIS):

- Within the EU, the SIS enables rapid assistance and information transfer, managed by National Central Bureaus of Schengen member states.

Consultations and Joint Investigation Teams (JITs):

- Meetings (consultations) are held to identify practical steps for lawfully obtaining evidence abroad.
- Europol and Euro just support the setup of JITs in Europe, consisting of law enforcement representatives from at least two states.
- JITs receive support from Europol and Euro just in terms of tactical, technical, and legal advice, as well as practical assistance.

5. Explain in detail on Search and Seizure (Article 19).

Search and Seizure

The competent authority shall be empowered to

2) Search

a). Computer system or part of it and computer data stored there in.

b). A computer-data storage medium in which computer data may be stored

2) Seizure

Seize or similarly secure computer data accessed [by a search pursuant to These measures shall include the power to

(a) seize or similarly secure a computer system or part of it or a computer-data storage medium;

(b) make and retain a copy of those computer data;

(c) maintain the integrity of the relevant stored computer data;

(d) render inaccessible or remove those computer data in the accessed computer system.

- Article 19 of the Cybercrime Convention regulates search and seizure, emphasizing the need to confine these methods within the territory
- Theprovision outlines the authority to search computer systems, storage media, and seize computer data, including the power to make copies, maintain data integrity, and render data inaccessible or remove it from accessed systems.
- Distinctions are made between physical equipment and computer data, with both subject to search and seizure.
- Digital devices and storage media may be seized during a house search and must be documented to maintain the chain of custody.
- Once data relevant to the investigation is secured, seizure of equipment must be lifted, unless other reasons justify its retention.
- Legal provisions must permit the securing of computer data as evidence independent of the digital equipment. Questions arise regarding when data is seized, the obligation to seize data through copying, routine application of hash analysis, and the need for separate permissions for searching digital devices seized for evidentiary purposes.
- TheConvention obligates parties to empower criminal investigators to order individuals

with knowledge of computer systems to provide login information, but the extent of this obligation regarding decryption is unclear.

- Physical coercion to obtain access data requires a separate legal basis and is not currently provided for in Norwegian procedural law

Main Rules

- To make sense of article 19, one must distinguish between the physical equipment, including storage media, and the computer data (bits and bytes).
- It is clear that a computer system or part of it (e.g., a user account) can be searched. In addition, a computer-storage medium can be searched.
- This is, for instance, a USB stick, a CD or DVD disk, a hard drive, as well as every little chip or memory card that can contain data. The kind of device is legally irrelevant. Consequently, when one looks into the contents of a computer system, one conducts a search.
- Similarly, a criminal investigator who looks into a laptop or a smartphone performs a search of the device (a smartphone is a computer system that resembles a phone).
- To maintain the chain of custody, two reports are needed: one that describes the house search, and one specifying the seized objects.
- The seizure of the digital equipment must be lifted, and the equipment returned to the owner.
- The potential evidence has been secured, seizure of the equipment cannot be upheld for evidentiary purposes.

Special Issues

- The first question is whether at all computer data can be seized. This must be performed by making a copy to the criminal investigator's storage media.

- The computer data to be secured as evidence independent of the digital equipment.
- The Norwegian Supreme Court seems to go down a different avenue: data that is copied without the police looking into it beforehand is deemed to be seized first when relevant files are picked out as evidence.
- **Example : Search of a Smartphone**
  - A person arrived at the airport with fake ID documents. Icelandic police officers seized his smartphone, reckoning that it contained information that could reveal his identity.

- The seizure was lawful, but search of the smartphone could not lawfully be conducted without a new permission by the court. It was relevant that a smartphone contains content stemming from communication, which is at the core of the protection of the ECHr article 8.
- The judgment was followed up with a second judgment the same season (spring 2016). The need for explicit permissions both for seizure and search is thus settled Icelandic law.

UNIT - 3

UNIT III DIGITAL FORENSIC READINESS

Introduction – Law Enforcement versus Enterprise Digital Forensic Readiness –Rationale for Digital Forensic Readiness – Frameworks, Standards and Methodologies –Enterprise Digital Forensic Readiness – Challenges in Digital Forensics

1. **Define Digital forensics readiness.**

   Digital forensic readiness involves being prepared to conduct digital investigations and present evidence effectively, whether to auditors, legal advisors, or in court. It aims to reconstruct incidents and find evidence that supports or refutes claims.

2. **Define Enterprise Digital Forensic Readiness.**

   The ability to conduct digital investigations in an enterprise with minimal cost and disruption to business operations while maximizing the usefulness of evidence.

3. **What is Rowlingson's Ten-Step Process?**
   - Builds on forensic readiness objectives.
   - Proposes a ten-step framework focusing on business context, risk alignment, business continuity, and incident response.
   - Offers a comprehensive description of steps without delving into specific policies or tools.

4. **What is Grobler et al.'s Forensic Readiness Framework?**
   - Introduces comprehensive digital evidence that carries evidentiary weight.
   - Proposes a framework grouping forensic readiness activities into dimensions.
   - Emphasizes the need for organizations to be aware of risks and legal requirements when collecting evidence.

5. **List the advantages of Usefulness of Digital Evidence.**
   - evidentiary weight in a court of law,
   - relevant and sufficient for
   - determining root cause,
   - linking the attacker to the incident.

6. What are the Technology Digital Forensic in Laboratory ?

- The ISO 17025 (ISO/IEC, 2005) standard,
- The ISO 27001 (ISO/IEC, 2013) standard,
- The ISO 9001 (ISO, 2008) standard,
- The ILAC-G19:2002 (ILAC-G19, 2002) guidelines, and
- Other general good practices.

7. What is Objective Test?

- A test which having been documented and validated is under control so that it can be demonstrated that all appropriately trained staff will obtain the same results within defined limits.
- These defined limits relate to expressions of degrees of probability as well as numerical values.

8. Define Validation.

- Validation is the confirmation by examination and the provision of objective evidence that a tool, technique or procedure functions correctly and as intended

9. Define Verification.

- Verification is the confirmation of a validation with laboratories tools, techniques and procedures.

10. List the awareness training the employee must know.

- incident response and forensic team(s),
- IT and information security,
- legal department,
- human resources,
- media contacts and public relations, and
- other employees(e.g., those reporting incidents, and people under investigation).

11. What is digital forensics life cycle?

- The digital forensics lifecycle is a methodical approach designed to ensure that digital evidence is handled with the utmost care and precision. Each phase, from identification to documentation, plays a critical role in maintaining the integrity and reliability of the forensic process.

12. What is data enterprise analysis ?

- Enterprise analytics is the practice of harnessing available internal and relevant external data to inform business decisions and transform data into insight. It is a critical component of any enterprise's digital transformation efforts.

13. What is law enforcement in digital forensics?

- Digital forensics ensures integrity of computer systems by preserving the data and information at original state during investigations. · In-depth Analysis. To reconstruct events and create timelines of illegal behavior, forensic specialists can examine digital artifacts including emails, log files, and file metadata

14. How much evidentiary weight does digital evidence carry?

- This can be expressed through degrees of trustworthiness, relevance, sufficiency, and validity.

15. Define RACI

- R stands for responsibility (role performs the activity).
- A stand for accountability (role is accountable for the success of the activity and has approval authority).
- C stands for consulted (role provides input for the activity).
- I stand for informed (role receives information related to activities, decisions, or deliverables).

16. List some important questions when preparing for a digital investigation the enterprise should ask and evaluate in a legal context.

- Which scenarios require the enterprise to exercise due diligence and collect digital evidence?
- What is considered to be the digital evidence, and when it is admissible in a court of law?
- Which information and data can be collected as digital evidence, and under
- What circumstances?
- What are the requirements or procedures required for collecting, preserving, and presenting digital evidence in court

17. Define NISTSP 800-86.

- SP 800-86 (NIST SP800-86; NIST, 2006) discusses the phases of the digital forensic process: collection, examination, analysis, and reporting.
- This standard includes general recommendations as well as more detailed technical guidelines for evidence collection and examination from data files, operating systems, networks, applications, and other sources

18. Define SWGDE.

- The Scientific Working Group on Digital Evidence (SWGDE, 2013) lists the primary types of errors found in the implementation of digital forensic tools: incompleteness, inaccuracy, and misinterpretation.
- The focus of the guidelines is to understand the limitations of tools and techniques, as well as to discuss error mitigation techniques, including tool testing, verification, procedures, and peer reviews.

19. Define Armando Angulo Case.

- The usual route to beating the DEA in a case is arguing that the evidence is insufficient. But for Armando Angulo, the win comes from the opposite A federal judge in Iowa dismissed the charge last week at the request of prosecutors, who want to throw out the many records collected over their nine-year investigation to free up space.
- Continued storage of these materials is difficult and expensive.

20. Define Endicott-Popovsky et al.'s Forensic Readiness Framework.

- Presents a multi-layer framework for network forensics.
- First layer: theoretical base covering information security governance and embedding forensics in information assurance.
- Second layer: "3R" strategy model (resistance, recognition, recovery) and a fourth R - redress (accountability in court).
- Third layer: information systems development life cycle with forensic capabilities like chain of custody procedures

PART - B

1. Give a brief Introduction about Digital forensics readiness.

Introduction:

- Television series often glamorize digital forensics, portraying it as exciting and straightforward. However, real-life digital investigations are much more complex and require substantial preparation.
- This chapter explores the concept of digital forensic readiness, which involves preparing for efficient and effective digital investigations.

Definition:

- Digital forensic readiness involves being prepared to conduct digital investigations and present evidence effectively, whether to auditors, legal advisors, or in court.
- It aims to reconstruct incidents and find evidence that supports or refutes claims.

Key Points:

- **Efficient Investigations**: Ideally, all digital devices would be seized, and all data analyzed to quickly draw conclusions. However, limited resources and time necessitate focusing on the most valuable artifacts for the specific incident.
- **Objectives:** J. Tan outlines two primary objectives:
  - Maximizing the usefulness of incident evidence data.
  - Minimizing the cost of forensics during an incident response.

Definition Summary:

- Digital forensic readiness is defined as the ability to perform digital investigations with minimal cost while maximizing the usefulness of evidence.
- By focusing on these principles, organizations can be better prepared to handle digital investigations efficiently and effectively

2. Explain in detail on Law Enforcement versus Enterprise Digital Forensic Readiness.

Overview:

- Digital investigations are commonly associated with law enforcement, but enterprises are increasingly applying digital forensics for various internal

purposes. This has given rise to a subarea known as enterprise digital forensics.

Law Enforcement:

- Conducts digital investigations primarily for criminal cases.
- Collects and analyzes digital evidence to be presented in court.
- Forensic principles and methodologies must be strictly followed to ensure evidence is admissible.

Enterprise:

- Uses digital forensics to investigate incidents, ensure compliance, support disciplinary actions, and more.
- May perform initial investigations before involving law enforcement.
- Evidence gathered may be used internally or in court if criminal activity is discovered.
- Must ensure business continuity and minimize disruptions during investigations.
- Follows forensic principles to maintain the integrity and usefulness of evidence.

Enterprise Digital Forensic Readiness Definition:

- The ability to conduct digital investigations in an enterprise with minimal cost and disruption to business operations while maximizing the usefulness of evidence.

Key Points:

- Enterprises need to balance investigation with ongoing business operations.
- Different laws and regulations may apply to private investigators and forensic professionals in enterprises compared to law enforcement.
- Terms like enterprise forensic readiness, computer forensic readiness, and corporate forensics are synonymous with digital forensic readiness in an enterprise context.

This distinction highlights the need for both law enforcement and enterprises to be prepared for digital investigations, though their approaches and priorities may differ.

3. Describe in detail why a Rational for Digital Forensics Readiness in required.

Digital forensic readiness ensures efficient and effective digital investigations by minimizing costs and maximizing the usefulness of collected digital evidence.

Cost

- **Minimizing Costs:** Digital forensic readiness aims to reduce the costs associated with investigations, including time, effort, equipment, and other direct expenses.
- **Resource Management:** Unlike TV portrayals, real-life investigations often involve multiple concurrent cases, requiring efficient resource management.

- **Cost Components:** Costs include the hours spent on investigation, fees, equipment, and other related expenses. For example, a two-hour intrusion can lead to 40 hours of forensic analysis.
- **Case Examples:**
  - New Zealand hacker: 417 hours of investigation costing $27,800.
  - Russian hacker: 9 months of investigation costing $100,000.
- **Indirect Costs:** Disruption to business operations and the need for legal counseling also add to the costs.
- **Cost-Benefit Analysis:** Enterprises often use cost-benefit analysis to decide whether to pursue legal action or involve law enforcement based on the cost versus the potential benefits or compensation.

Usefulness of Digital Evidence

- **Maximizing Usefulness:** Useful digital evidence must be relevant, sufficient, and have evidentiary weight in a court of law.
- **Existence of Evidence:** Digital evidence can be transient and easily destroyed, requiring timely and appropriate collection methods.
- **Example:** Improper handling by IT support can destroy potential evidence, complicating forensic investigations.

- **Evidentiary Weight:** Evidence must be trustworthy, relevant, sufficient, and valid.
  - Relevance: Evidence must help prove or disprove elements of the incident.
  - Sufficiency: There must be enough evidence to thoroughly examine the incident.
  - Trustworthiness: Evidence must be accurate, authentic, and reliably collected.
  - Validity: Evidence must be collected in a forensically sound manner to be
  - admissible in court.

- **Examples of Evidence Handling Issues:**
  - Legal Assistant Incident: Improper handling led to changes in 192 files.
  - Surveillance Footage: Missing critical footage impacted the investigation.
  - Armando Angulo Case: Evidence storage costs led to case dismissal.
  - Evidence Eliminator Case: Attempted deletion of evidence led to case dismissal.
  - Julie Amero Case: Misunderstanding of digital evidence led to wrongful conviction, later overturned due to proper forensic analysis.

- **Forensically Sound Collection:** Proper procedures, tools, and processes are essential for collecting and preserving digital evidence.

Digital forensic readiness involves preparation and planning to ensure that digital evidence can be efficiently collected, preserved, and used effectively in investigations, whether for internal enterprise purposes or legal proceedings.

4. Explain the different Frameworks, Standards and Methodologies in detail.

Digital forensic readiness lacks a universally accepted approach. Various standards, frameworks, and methodologies have been proposed by standardization bodies, organizations, and researchers, reflecting the evolving nature of this discipline.

Standards

ISO/IEC 27037

- Defines digital evidence and its governance principles: relevance, reliability, and sufficiency.
- Outlines general requirements for handling digital evidence, emphasizing audit ability, justifiability, and either repeatability or reproducibility.
- Details initial processes for handling digital evidence: identification, collection, acquisition, and preservation.

ISO/IEC 17025

- Sets requirements for forensic laboratories, focusing on both management and technical aspects.
- Emphasizes technical requirements related to methodology, equipment handling,
- sampling, and quality assurance.

NIST SP 800-86

- Discusses phases of the digital forensic process: collection, examination, analysis, and reporting.
- Provides general recommendations and detailed technical guidelines for evidence collection and examination from various sources.

Guidelines

IOCE Guidelines

- Developed by the International Organization on Computer Evidence.
- Provide high-level descriptions and specific principles for digital forensic examination procedures.
- Focus on preserving evidence integrity and maintaining the chain of custody.

SWGDE Guidelines

- Developed by the Scientific Working Group on Digital Evidence.
- Address common errors in digital forensic tools: incompleteness, inaccuracy, and misinterpretation
- Discuss error mitigation techniques, including tool testing, verification, procedures, and peer reviews.

ENFSI Guidelines

- Published by the European Network of Forensic Science Institutes.
- Offer a Best Practice Manual for the Forensic Examination of Digital Technology.
- Include guidance on procedures, quality principles, training processes, and approaches for forensic laboratories

Research

Rowlingson's Ten-Step Process (2004)

- Builds on forensic readiness objectives.
- Proposes a ten-step framework focusing on business context, risk alignment, business continuity, and incident response.
- Offers a comprehensive description of steps without delving into specific policies or tools .

Grobler et al.'s Forensic Readiness Framework (2010)

- Introduces comprehensive digital evidence that carries evidentiary weight.
- Proposes a framework grouping forensic readiness activities into dimensions.
- Emphasizes the need for organizations to be aware of risks and legal requirements when collecting evidence.

Endicott-Popovsky et al.'s Forensic Readiness Framework (2007)

- Presents a multi-layer framework for network forensics.
- First layer: theoretical base covering information security governance and embedding
- forensics in information assurance.
- Second layer: "3R" strategy model (resistance, recognition, recovery) and a fourth R - redress (accountability in court).
- Third layer: information systems development life cycle with forensic capabilities like chain of custody procedures.

5. Compare and contrast policy, processes and procedures of Digital Forensic Readiness.

Enterprises are complex entities that need to maintain smooth operations. When an incident occurs, swift action is crucial, making prior planning and preparation essential for digital forensic readiness

Legal Aspects

- **Jurisdictional Compliance**: Enterprises must adhere to local laws and regulations for collecting, analyzing, and presenting digital evidence. This is particularly challenging for international organizations.
- **Cybercrime Types:** Identifying relevant cybercrime types helps determine when digital evidence is required.
- **Key Legal Questions:** Enterprises should address scenarios for due diligence, admissibility of digital evidence, permissible data collection, and requirements for evidence handling.

Example: SpyEye Online Banking Fraud

- **Incident Scenario:** Involves crimes such as computer intrusion and unlawful dealings.
- **Data Retention vs. Privacy:** Conflicting requirements (e.g., 90-day data retention vs. 30-day privacy regulation) highlight the need for careful compliance management.

Policy, Processes, and Procedures

- **Evidence Management Practices:** Enterprises should follow generally accepted practices and align digital forensic policies with existing frameworks.
- **Risk-Based Approach:** Integrating digital forensics within the information security framework involves assessing risks and choosing appropriate risk-handling measures, focusing on confidentiality, integrity, and availability

Example: SpyEye Online Banking Fraud Risk Scenario

- **Risk Scenario:** Unauthorized transactions lead to financial losses and reputational damage.
- **Risk Assessment:** Helps prioritize incidents based on potential impact, guiding the decision between restoring operations and conducting full-scale investigations.

● **Incident Response vs. Digital Forensics**: Incident response aims to restore operations quickly, while digital forensics focuses on evidence preservation, potentially delaying restoration. Balancing these goals is crucial for minimal business disruption

Policy

- **Policy Framework:** Should include purpose, scope, legal requirements, alignment with other enterprise frameworks, and relationships with other policies.
- High-Level Policy: Supported by sub policies, guidelines, and procedures, or integrated into other enterprise policies like incident response or information security.

Processes and Procedures

- Digital Forensic Readiness Process:
  1. Identify relevant laws and regulations.
  2. Perform or obtain risk assessments.
  3. Identify incident scenarios requiring digital evidence.
  4. Integrate digital forensics with existing frameworks.
  5. Define or update digital forensic policies.
  6. Set policies for outsourcing and third-party use.
  7. Define sub policies and procedures.
  8. Establish organizational structure.
  9. Specify roles, responsibilities, and required skills.
  10. Conduct operational and awareness training.
  11. Prepare tools and infrastructure.
  12. Evaluate process effectiveness and quality.

Key Considerations: Evidence handling, monitoring, privacy protection, incident escalation, specific investigation types, external reporting, third-party involvement, laboratory preparation, training, and competency requirements.

6. Explain in detail on Challenges in Digital Forensics.

Key Challenge:

- Handling vast amounts of unstructured data with inherent uncertainties and errors.
- Each phase of the digital forensics process is time and resource-intensive, often exceeding available resources.

Solutions:

- Leveraging big data, automation, and computational methods to enhance efficiency.

Phases Supported by Computational Methods:

a. **Identification Phase:** Intelligent detection and identification methods.
b. **Collection Phase:** Automated remote evidence acquisition tools with evidence integrity assurance.
c. **Examination Phase:** Automated data recovery and reduction.
d. **Analysis Phase:** Computational methods and machine learning to identify patterns.
e. **Presentation Phase:** Visualization tools and automated report generation.

Computational Forensics

Definition:

- Application of computational methods to forensics, involving modeling, simulation, and computer-based analysis and recognition.

Objectives:

1. In-depth understanding of forensic disciplines.
2. Evaluation of scientific methods.
3. Systematic forensic approach using computer science, applied mathematics, and statistics.

Applications

1. Large-Scale Investigations:

- Managing large data volumes from diverse sources using computational methods.
- Example: Automatic identification of malware traces and network traffic analysis using link-mining techniques and Neuro-Fuzzy (NF) algorithms.

2. Automation:

- Reducing manual efforts and enhancing quality through comprehensive automation.
- Examples: Forensic reconstruction of computer intrusions, geolocation of IP addresses using triangulation.

3. Analysis:

Strengthening evidence analysis through computational methods.

Example: Identification and extraction of cryptographic keys from volatile memory, approximate hash-based matching for data similarity, intrusion detection through correlation feature selection.

4. Forensic Soundness:

●Ensuring evidence integrity and chain of custody in computational methods.

● Implementing comprehensive testing for forensic tools to prevent unintentional mistakes and intentional tampering.

Evolving Field: Digital forensics is constantly evolving due to the increasing complexity of technologies. The Testimony Forensics Group outlines several key research areas to address current challenges.

Key Research Areas:

1. Large-Scale Investigations:

- Focus: Automatic searching through vast amounts of electronic storage both within closed systems and on the Internet (including the dark net).
- Challenge: Efficiently managing and analyzing terabytes of data.

2. Internet and Cloud Forensics:

- Focus: Rapid acquisition, correlation, and analysis of evidence from the Internet and cloud services.
- **Challenge:** Developing new tools and methods, and educating law enforcement and practitioners.

3. Embedded Systems and IoT:

- Focus: Forensic analysis of mobile devices and other embedded systems, including both hardware and software.
- Challenge: Proprietary technology, device-specific hardware, customized data acquisition, and decoding binary data.

4. Cross-Media Search and Data Integration:

- Focus: Accessing and integrating data from diverse sources, with an emphasis on data enrichment from Internet sources.
- Challenge: Effective cross-media search technologies.

5. Encrypted Evidence:

- Focus: Developing algorithms to analyze encrypted evidence and cryptographic credentials.
- Challenge: Overcoming encryption barriers to access and interpret evidence.

6. Computational Intelligence:

- Focus: Advanced computing technologies for more objective evidence analysis and decision-making.
- Challenge: Implementing computational intelligence to enhance accuracy and efficiency.

Attribution and Profiling:

- Focus: Methods and tools for digital perpetrator attribution and profiling, visualizing criminal relationships, and geographical mapping of evidence.
- Challenge: Accurate identification and profiling of digital criminals.