5. Digital Forensics

EN6106 - Emerging Topics in Information Technology

Level III - Semester 6

Overview

This lecture covers what forensic science is, the basic concepts of digital forensics, and the process of Digital Forensics.

Overall, the course aims to equip students with the knowledge on how investigation and analysis of digital evidence in a wide range of legal and criminal cases are carried out.

Intended Learning Outcomes

At the end of this lesson, you will be able to;

- Define what is forensic science
- Describe the process of identifying, collecting, examining and analyzing digital evidence
- Understand the role of digital forensics in legal and criminal investigations
- Identify and categorize the types of digital evidence and the tools used to acquire and analyze digital data
- Identify the branches of digital forensics
- Identify & develop practical skills required for digital forensics investigation, such as data recovery, data analysis, and report writing.

List of sub topics

- 5.1 Forensic Science
- 5.2 Introduction to Digital Forensics
  - 5.2.1 Types of Digital Evidence
  - 5.2.2 The History and Evolution of Digital Forensics
  - 5.2.3 History of Computer Crimes
  - 5.2.4 Technological Advances Over Time
  - 5.2.5 Applications of Digital Forensics
  - 5.2.6 Role of Digital Forensics in Law Enforcement
- 5.3 Digital Forensic Procedure
  - 5.3.1 Identification Phase
  - 5.3.2 Collection Phase
    - 5.3.2.1 Chain of Custody
  - 5.3.3 Examination Phase
  - 5.3.4 Analysis Phase
- 5.4 Example Use case Scenario
- 5.5 Skills Required for Digital Forensics Investigation

5.1 Forensic Science

A scientific discipline that applies scientific methods and principles to the investigation of crimes and legal issues

- Involves the collection, analysis, and interpretation of physical evidence, such as blood, fingerprints, DNA, and fibers, to help determine the facts of a case

- Uses a variety of specialized techniques, instruments, and technologies to analyze evidence and reconstruct crime scenes.

- Forensic science is made up of many specialized areas, including:
  - Forensic Biology
  - Forensic Chemistry
  - Forensic Toxicology
  - Forensic Psychology
  - Digital Forensic

5.1 Forensic Science Contd.

- Forensic Biology - study of biological evidence such as DNA, blood, and other bodily fluids
- Forensic Chemistry - the analysis of chemicals and materials found at crime scenes
- Forensic Toxicology - the study of the effects of drugs and poisons on the body
- Forensic Psychology - the study of human behavior and how it relates to criminal investigations
- Digital Forensic - analyzes, examines,identifies and recovers the digital evidences residing on electronic devices

5.2 Introduction to Digital Forensics

- Digital forensics involves the recovery, preservation, analysis, and presentation of electronic data that has been stored, transmitted, or processed on digital devices such as computers, mobile phones, and other digital storage media.

Source: https://interworks.com/blog/bstephens/2016/02/05/what-digital-forensics/

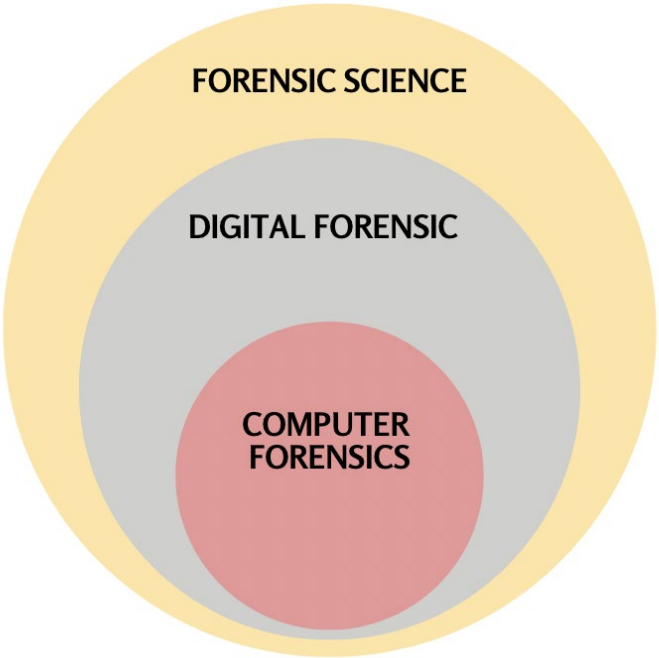
5.2.1 Types of digital evidence

- Digital evidence refers to information stored or transmitted in binary form that can be relied upon in court as evidence

- It can include various types of data, such as
  - Computer and mobile device data
  - Email and messaging data
  - Internet data
  - Social media data
  - Cloud data
  - Network data
  - Audio and video data
  - Metadata - information about a file, such as the date and time it was created or modified, and can be used to piece together a timeline of events

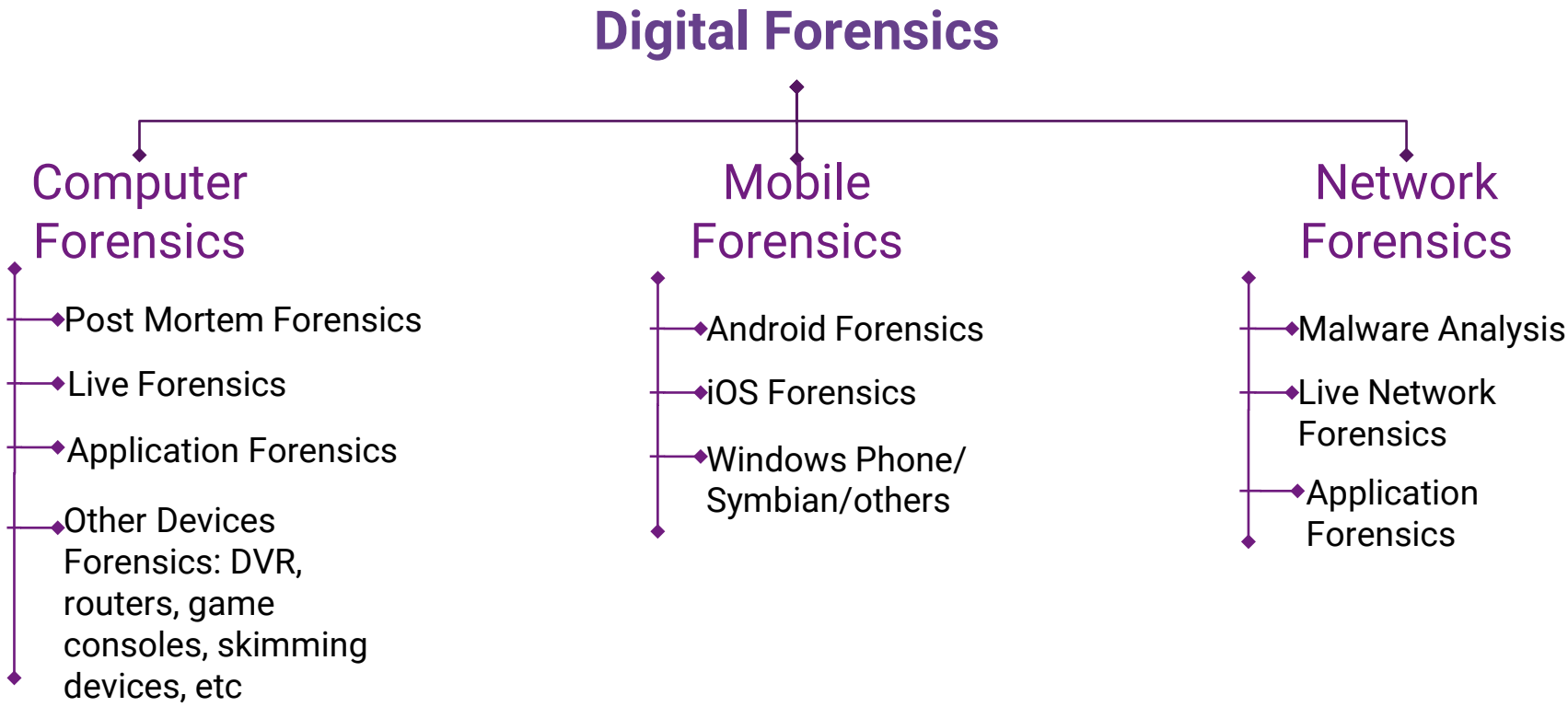
5.2.2 The History and Evolution of Digital Forensics

- Digital forensics - Field that emerged in response to computer-related crime and the need to investigate digital evidence
- Computer forensics has its roots in the field of digital forensics

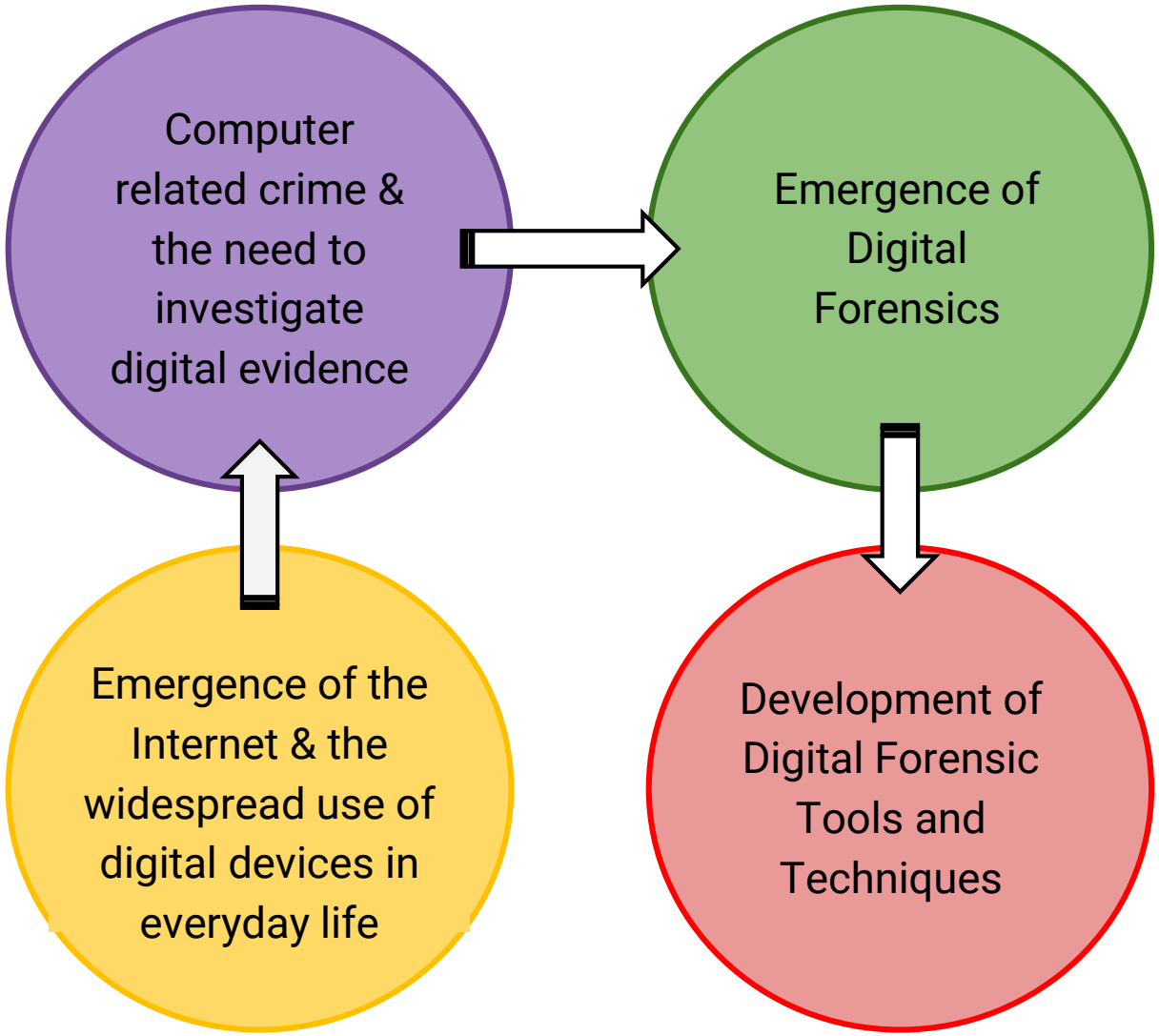


5.2.2 The History and Evolution of Digital Forensics Contd.

- The following chart shows the main subcategories and subject areas of Digital Forensics



5.2.2 The History and Evolution of Digital Forensics Contd.



5.2.3 History of Computer Crimes

Year	History
1978	First computer crime in Florida which involved unauthorized modification and deletion of data on a computer system.
Prior 1980	Computer crimes were solved using existing laws. No federal laws for computer crimes.
1983	Canada – The first country to pass legislation dealing with computer crimes.
1984	United States passed Federal Computer Fraud & Abuse Act
1990	United Kingdom passed British Computer Misuse Act.
1992	Collier & Spaul wrote a paper 'A forensic methodology for countering computer crime.'
2002	Scientific Working Group on Digital Evidence (SWGDE) produced a paper 'Best practices for computer forensic'.
2005	Publication of an ISO standard (ISO 17025, General requirements) for the competence of testing & calibration laboratories.
2005 Onwards till now	Various dimensions related to computer crimes are being discussed.

Ref 2 : History Evolution of digital forensic

5.2.4 Technological Advances Over Time

- Here are some technological advances that have allowed digital forensics to evolve over time
  - **Imaging Technology**: allow digital forensic investigators to create forensic images of storage devices and analyze them using specialized software
  - **Data Recovery Tools**: To recover lost or deleted data from digital devices, even if the data has been intentionally deleted or hidden
  - **Mobile Forensics**: Specialized software and tools for mobiles to allow investigators to recover data from mobile devices and analyze it in a forensically sound manner
  - **Cloud Forensics**: To recover and analyze cloud based data

5.2.4 Technological Advances Over Time Contd.

- **Artificial Intelligence and Machine Learning**: Development of automated tools that can aid in the analysis of digital evidence. They can quickly identify patterns and anomalies in large datasets, making it easier for investigators to focus on areas of interest.
- **Blockchain Forensics**: To trace cryptocurrency transactions and analyze them in a forensically sound manner
- **Live Forensics**: To analyze digital devices in real-time, allowing them to quickly identify and respond to security threats
- **Virtualization Technology**: To create virtual machines and environments for forensic analysis, reducing the need for physical hardware and making it easier to test and validate forensic tools and techniques.

5.2.5 Applications of Digital Forensics

- Used mainly in the following two applications

Criminal Law

- Evidence collected to support or oppose a proposed explanation or argument in the court
- Forensics procedures similar to those used in criminal investigations
  - With different legal requirements and limitations

Private Investigation

- Mainly used by corporate world
- Used when companies are suspicious that employees may be performing an illegal activity on their computers that is against company policy

5.2.6 Role of Digital Forensics in Law Enforcement

- **Cybercrime Investigations** - To identify and track down cyber criminals by analyzing digital evidence, such as IP addresses, log files, and other metadata
- **Digital Evidence Collection** - To prove a suspect's involvement in a crime or to provide alibis for innocent suspects. Includes evidence from computers, mobile devices, and other digital storage media.
- **Child Exploitation Cases** - To uncover evidence of child pornography or other illegal activities involving children. This evidence can be used to prosecute and convict offenders, as well as to rescue and protect victims.
- **Fraud Investigations** - Analyze digital records and financial transactions to identify patterns and anomalies that may indicate fraudulent activity

5.2.6 Role of Digital Forensics in Law Enforcement Contd.

- **Terrorism Investigations** - To track down and identify individuals and groups involved in terrorist activities

- **Courtroom Presentations** - Digital forensic evidence can be presented in court as evidence to support the prosecution's case. Digital forensic experts may be called to testify in court and explain their findings to the judge and jury.

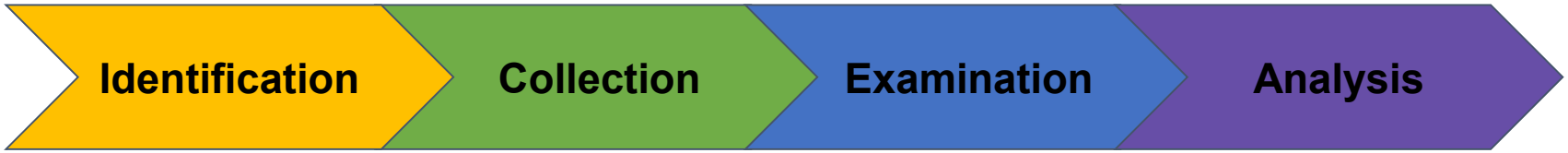
- **Investigative Efficiency** - Help law enforcement agencies to work more efficiently by reducing the time and resources required to investigate crimes.

With digital evidence, investigators can quickly identify suspects, track their movements, and gather evidence to support a prosecution.

5.3 Digital Forensics Procedures

- As discussed in previous slides, Digital forensic investigation is the process of collecting, preserving, analyzing, and presenting digital evidence in a manner that is admissible in court.

- The process of digital forensic investigation typically involves 4 phases:



These phases are critical to the digital forensic investigation process and are typically followed in sequence.

5.3.1 Identification Phase

- First step in a digital forensics investigation
- Begins with gathering of information from stakeholders involved in the investigation
  - Law enforcement
  - Corporate security
  - Legal teams
- Review information to determine scope and objectives
- Identify potential sources of digital evidence relevant to the case
- Identify devices and storage media that may contain relevant information - computers, mobile phones, external hard drives, and cloud storage services

5.3.1 Identification Phase Contd.

- Identify potential locations of digital evidence - email accounts, social media platforms, cloud storage services, and other online repositories

- Identify relevant metadata, which can provide valuable information such as
  - Date and time
  - Location of a file or piece of data
  - User who created it

Identification phase is critical to the success of a digital forensics investigation, as it ensures that all potential sources of digital evidence are identified and preserved for later analysis in the subsequent phases of the investigation.

5.3.2 Collection Phase

- Investigator gathers all potential sources of digital evidence identified during the Identification phase
- Include physical devices, as well as digital data stored on remote servers or in the cloud
- Can be collected using a variety of tools and techniques, such as
  - Imaging a hard drive
  - Creating a forensic copy of a mobile device
  - Using network sniffing tools to capture network traffic

It's important to collect digital evidence in a forensically sound manner to ensure that it is admissible in court and has not been tampered with.

5.3.2 Collection Phase Contd.

- Can be time-consuming
- Requires a high degree of attention to detail to ensure all potential sources of digital evidence are collected and preserved
- Should create a detailed chain of custody for each piece of evidence collected
- Important to obtain a search warrant or other legal authorization before collecting digital evidence
- May also involve interviewing potential witnesses and conducting other investigative work to identify additional sources of digital evidence

5.3.2.1 Chain of Custody

- A way to document the handling and movement of evidence in a digital forensics investigation
- It is a record of who had control of the evidence, when they had the evidence, and what they did with the evidence
- The goal is to ensure that the evidence is reliable and admissible in court
- Helps prevent tampering, contamination, or loss of evidence
- Starts when the evidence is first collected and ends when presented in court
- Each person who handles the evidence must document their actions and sign the chain of custody form.

5.3.2.1 Chain of Custody Contd.

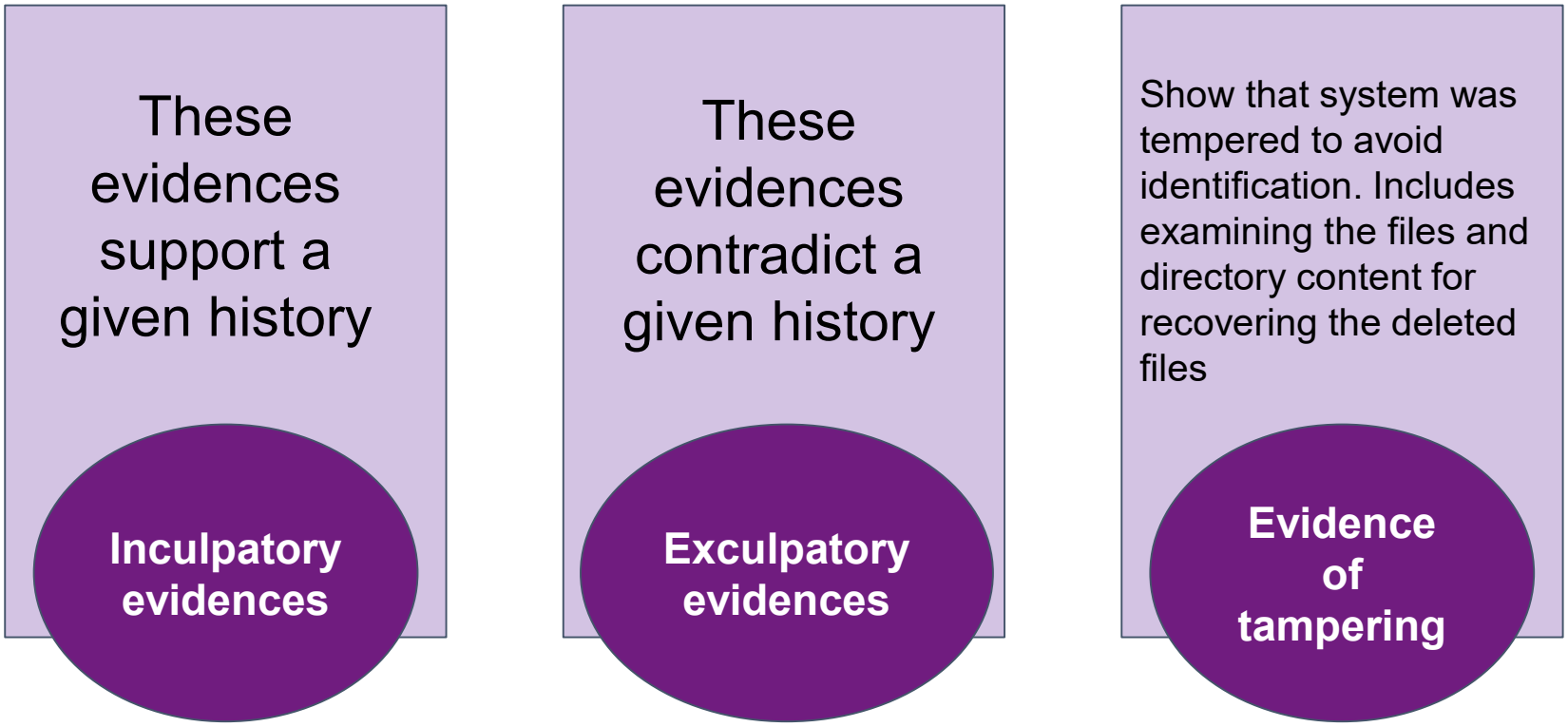
- Chain of custody form should include
  - The date
  - Time
  - Location
  - Description of the evidence
  - The name of the person handling the evidence
- Any breaks in the chain of custody can weaken the credibility
- And may result in it being excluded from the trial
- It is important to maintain a complete and unbroken chain of custody throughout the investigation

5.3.3 Examination Phase

- Digital forensics investigator carefully examines the digital evidence collected in the previous phase
- Use a variety of techniques to examine digital evidence, including specialized software tools and manual analysis
- Purpose is to determine the relevance and significance of digital evidence to the investigation
- May also attempt to identify patterns or connections between different pieces of digital evidence
- Important to ensure that only relevant and significant evidence is analyzed in the subsequent phases of the investigation.

5.3.3 Examination Phase Contd

- This phase gives three kinds of evidences as follows



5.3.4 Analysis phase

- Investigator reviews and interprets the digital evidence to draw conclusions and develop a report of findings
- Looks for patterns, connections, and other meaningful relationships to develop an understanding of the case
- May also use specialized software to help interpret the digital evidence, such as
  - Data recovery tools
  - Network analysis tools
  - Decryption tools
- Goal of the analysis phase is to provide a clear and detailed report of the digital evidence and findings that can be used in legal proceedings or other contexts

5.4 Example Use case Scenario

A Cybercrime Investigation at a Retail Company

- **Identification Phase:**

A large retail company reports to law enforcement that its servers have been hacked and confidential customer data has been stolen. The digital forensics team is brought in to identify the extent of the data breach and the specific data that has been compromised.

- **Collection Phase:**

The digital forensics team first secures the affected servers and makes forensic images to preserve the data in its original state. They also collect other relevant evidence, such as server logs and network traffic, to determine how the hackers gained access to the system. Additionally, they conduct interviews with company employees to gather information about any suspicious activity they may have noticed.

5.4 Example Use case Scenario Contd.

A Cybercrime Investigation at a Retail Company

- **Examination Phase:**

Using specialized software and tools, the digital forensics team examines the preserved images to recover the stolen customer data. They analyze the server logs and network traffic to identify any suspicious activity or connections. They also use forensic tools to recover deleted files and any other data that may have been hidden or encrypted.

- **Analysis Phase:**

The digital forensics team analyzes the recovered data and other evidence to determine the scope and impact of the data breach. They identify the specific customer data that has been compromised, such as names, addresses, and credit card numbers, and assess the potential harm to the affected individuals.

5.4 Example Use case Scenario Contd.

A Cybercrime Investigation at a Retail Company

- **Analysis Phase Contd:**

They also identify any patterns or trends in the network traffic that may indicate the source of the attack, and analyze the recovered data to determine if the hackers attempted to alter or delete any data

Overall, by following the four phases of digital forensics, the digital forensics team is able to identify the extent of the data breach, recover the stolen data, and provide valuable evidence for the company and law enforcement in their investigation of the cybercrime. In this case, the company is able to take steps to notify and protect their affected customers, and law enforcement is able to pursue the hackers and hold them accountable for their actions.

5.5 Skills Required for Digital Forensics Investigation

- **Outstanding Thinking Capabilities** - capable of applying different tools and methodologies on a particular assignment for obtaining the output. Must be able to find different patterns and make correlations among them
- **Technical Skills** - field requires the knowledge of network, how digital system interacts
- **Passionate about Cyber Security** - needs lot of passion for someone to become an ace digital forensic investigator
- **Communication Skills** - to coordinate with various teams and to extract any missing data or information
- **Skillful in Report Making** - Forensic examiner must mention all findings in a final report. Hence must have good skills of report making and an attention to detail

References

- Ref 1 : Spring Microservices, https://spring.io/microservices

- Ref 2 : Shrivastava, Gulshan & Sharma, Kavita & Dwivedi, Akansha. (2012). FORENSIC COMPUTING MODELS: TECHNICAL OVERVIEW. Computer Science & Information Technology. 2. 10.5121/csit.2012.2222.

Summary

Forensic science	• Forensic Biology • Forensic Chemistry • Forensic Toxicology • Forensic Psychology • Digital Forensic
Digital Forensics	• Computer Forensics • Mobile Forensics • Network Forensics • Database Forensics
Digital Forensics Procedures	• Identification • Collection • Examination • Analysis