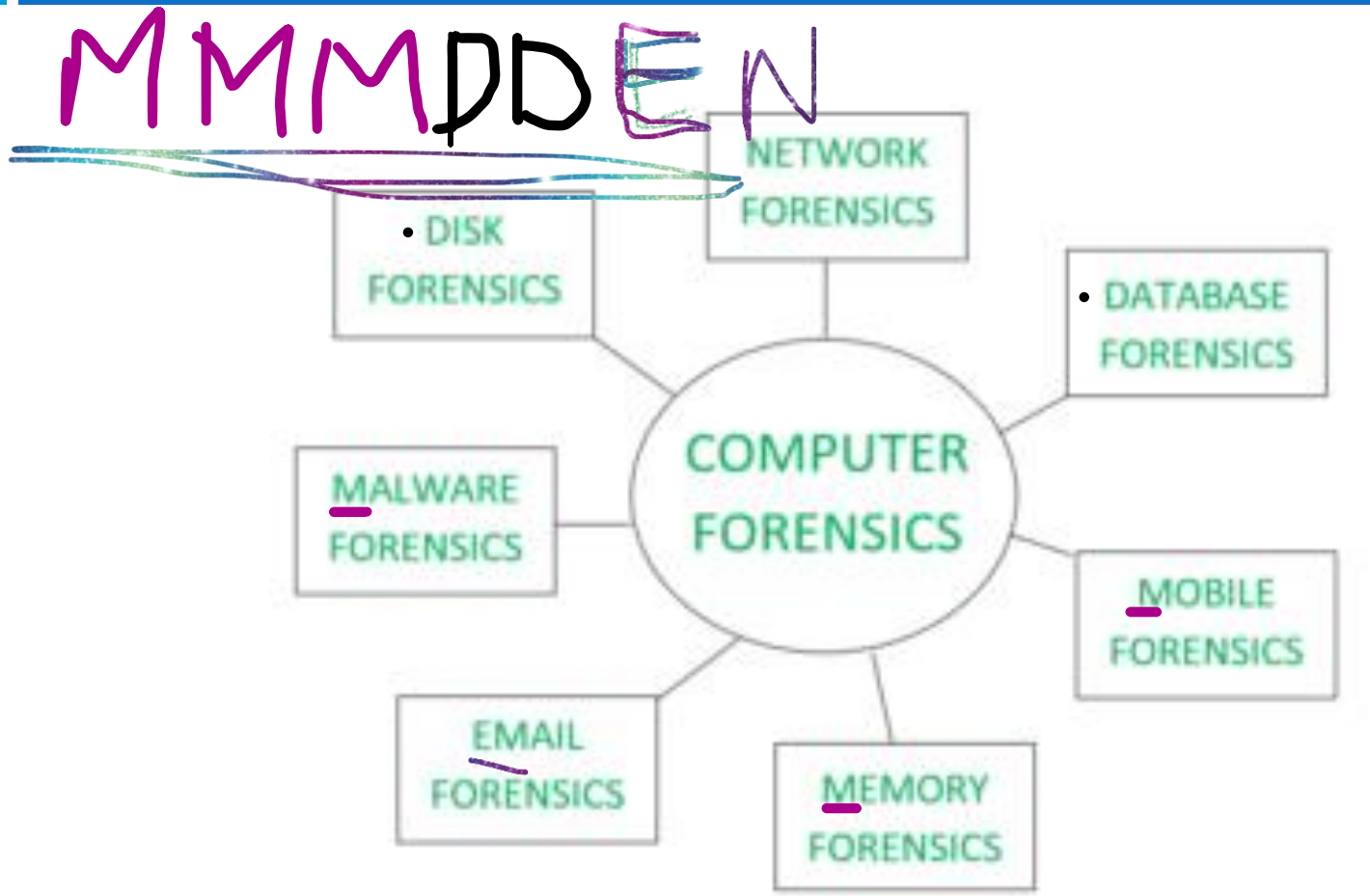
ITDO6014
ETHICAL HACKING AND FORENSICS

Module 3: Computer Forensics

Introduction of Computer Forensics

- Computer Forensics is a scientific method of investigation and analysis in order to gather evidence from digital devices or computer networks and components which is suitable for presentation in a court of law or legal body. It involves performing a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it.

Introduction to Digital Forensics



Introduction to Digital Forensics

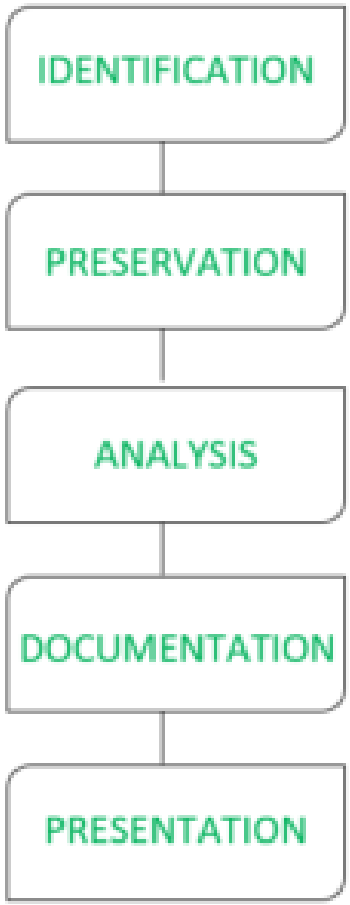
- **TYPES**
- Disk Forensics: It deals with extracting raw data from the primary or secondary storage of the device by searching active, modified, or deleted files.
- Network Forensics: It is a sub-branch of Computer Forensics that involves monitoring and analyzing the computer network traffic.
- Database Forensics: It deals with the study and examination of databases and their related metadata.
- Malware Forensics: It deals with the identification of suspicious code and studying viruses, worms, etc.

Introduction to Digital Forensics

- Email Forensics: It deals with emails and their recovery and analysis, including deleted emails, calendars, and contacts.
- Memory Forensics: Deals with collecting data from system memory (system registers, cache, RAM) in raw form and then analyzing it for further investigation.
- Mobile Phone Forensics: It mainly deals with the examination and analysis of phones and smartphones and helps to retrieve contacts, call logs, incoming, and outgoing SMS, etc., and other data present in it.

Introduction to Digital Forensics

- **How does computer forensics work?**



IPAD-P

Introduction to Digital Forensics

- **How does computer forensics work?**
- Identification: Identifying what evidence is present, where it is stored, and how it is stored (in which format). Electronic devices can be personal computers, Mobile phones, PDAs, etc.
- Preservation: Data is isolated, secured, and preserved. It includes prohibiting unauthorized personnel from using the digital device so that digital evidence, mistakenly or purposely, is not tampered with and making a copy of the original evidence.

Introduction to Digital Forensics

- Analysis: Forensic lab personnel reconstruct fragments of data and draw conclusions based on evidence.
- Documentation: A record of all the visible data is created. It helps in recreating and reviewing the crime scene. All the findings from the investigations are documented.
- Presentation: All the documented findings are produced in a court of law for further investigations.

Objectives of computer forensics

- It helps to recover, analyze, and preserve computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law.
- It helps to postulate the motive behind the crime and identity of the main culprit.
- Designing procedures at a suspected crime scene which helps you to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.

Objectives of computer forensics

- Helps you to identify the evidence quickly, and also allows you to estimate the potential impact of the malicious activity on the victim
- Producing a computer forensic report which offers a complete report on the investigation process.
- Preserving the evidence by following the chain of custody.

Evidence Collection

- **Disk Forensics**:
- **Procedure**:
  - The first step is to create a forensic copy, commonly known as a disk image, of the entire disk or specific partitions. This ensures that the original evidence remains unchanged during analysis.
  - Tools like Forensic Imager, dd ("data duplicator" or "disk dump,"), or EnCase can be used to create the disk image.
  - Once the image is created, analysis tools are used to examine the contents of the disk image without altering it.
- **Example**:
  - Suppose a suspect's computer is suspected of containing evidence related to a cybercrime. A forensic investigator would acquire a forensic image of the suspect's hard drive using a write-blocking device to prevent any modifications to the original data. This image would then be analyzed to extract relevant files, documents, emails, browsing history, etc.

Evidence Collection

- **Memory Forensics**:
- **Procedure**:
  - Memory forensics involves capturing the volatile memory (RAM) of a computer system to analyze running processes, open network connections, and other volatile data.
  - Tools like Volatility, Rekall, or WinPmem are used to acquire memory dumps.
  - Analysis involves examining the memory dump to identify running processes, injected code, open network connections, encryption keys, and other volatile artifacts.
- **Example**:
  - In an investigation involving a suspected malware infection, memory forensics can be used to identify the malware's presence in the system's memory, analyze its behavior, and extract indicators of compromise (IOCs) for further investigation.

Evidence Collection

- **Registry Forensics**:
- **Procedure**:
  - Registry forensics involves extracting and analyzing data stored in the Windows registry, which contains configuration settings and information about installed software, user accounts, and system configurations.
  - Tools like Registry Viewer, RegRipper, or Registry Explorer are used to extract and analyze registry hives.
  - Analysis involves examining registry keys, values, and timestamps to reconstruct user activities, installed software, USB device usage, and other system changes.
- **Example**:
  - In a corporate espionage case, registry forensics may reveal evidence of unauthorized software installations, changes to system configurations, or suspicious user activity, helping investigators identify insider threats or security breaches.

Evidence Collection

- **Log Analysis**:
  - **Procedure**:
    - Log analysis involves collecting and examining logs generated by various components of a computer system, such as operating systems, applications, firewalls, and network devices.
    - Tools like ELK Stack (Elasticsearch, Logstash, Kibana), Splunk, or Wireshark are used for log collection, parsing, and analysis.
    - Analysis involves correlating log entries across different sources to reconstruct events, identify anomalies, detect intrusions, and establish timelines of activities.
  - **Example**:
    - In a data breach investigation, log analysis can reveal unauthorized access attempts, abnormal network traffic patterns, and data exfiltration activities, helping investigators determine the extent of the breach and identify the attacker's tactics, techniques, and procedures (TTPs).

Evidence Acquisition, Analysis and Examination

- In computer forensics, evidence acquisition, analysis, and examination are crucial stages in the investigation process, regardless of the platform or type of digital evidence being examined.
- **Evidence Acquisition**:
- **Definition**: Evidence acquisition involves the collection and preservation of digital evidence in a forensically sound manner to ensure its integrity and admissibility in legal proceedings.
- **Example**:
  - For Windows:
    - Evidence acquisition from a Windows system involves creating a forensic image of the hard drive using tools like FTK Imager, EnCase, or dd.
    - Example: In a case involving alleged data theft from a company's Windows-based computers, forensic investigators would use write-blocking devices to acquire forensic images of the suspect's hard drives to preserve the original evidence.

Evidence Acquisition, Analysis and Examination

- For Linux:
  - Acquisition from a Linux system can be done similarly to Windows, creating a forensic image of the hard drive or relevant partitions.
  - Example: In an investigation of a cyberattack on a Linux-based server, forensic experts would use tools like dd or dc3dd to acquire a forensic image of the server's disk for analysis.
- For Email:
  - Evidence acquisition in email forensics involves obtaining copies of emails and associated metadata from email servers, client applications, or cloud services.
  - Example: In a case involving email harassment, investigators may obtain a subpoena to collect email evidence from the suspect's email provider, capturing both the content and metadata (e.g., sender, recipient, timestamps) for analysis.

Evidence Acquisition, Analysis and Examination

- For Web:
  - Web evidence acquisition includes capturing web server logs, browser history, cache files, and other artifacts related to web activity.
  - Example: In an investigation of an online fraud scheme, forensic analysts would collect web server logs from the targeted website to trace the activities of the perpetrators, such as IP addresses accessing the site, pages visited, and actions taken.
- For Malware:
  - Acquiring evidence related to malware involves capturing samples of malicious files, memory dumps, network traffic, and system logs.
  - Example: In a malware infection investigation, forensic investigators would use specialized tools to acquire memory dumps, capture network traffic, and extract malware samples from infected systems for analysis and identification.

Evidence Acquisition, Analysis and Examination

- **Evidence Analysis**:
- **Definition**: Evidence analysis involves examining and interpreting the collected digital evidence to identify relevant information, patterns, and anomalies.
- **Example**:
  - For Windows:
    - Analysis of Windows evidence may include examining file system artifacts, registry entries, event logs, and user activity to reconstruct events and identify potential evidence of wrongdoing.
    - Example: Analyzing Windows event logs may reveal suspicious login attempts, privilege escalation activities, or unauthorized software installations linked to a security breach.

Evidence Acquisition, Analysis and Examination

- For Linux:
  - Linux evidence analysis involves scrutinizing file system structures, system logs, shell history, and user account activities to uncover evidence of unauthorized access or malicious activities.
  - Example: Analyzing Linux shell history files may reveal commands executed by an intruder, providing insights into their actions and intentions during a system compromise.
- For Email:
  - Email evidence analysis entails examining email content, headers, attachments, and metadata to identify relevant communications, relationships, and timelines.
  - Example: Analyzing email headers may reveal the source IP addresses, routing information, and timestamps, helping investigators trace the origins of phishing emails or identify email spoofing attempts.

Evidence Acquisition, Analysis and Examination

- For Web:
  - Web evidence analysis involves parsing web server logs, browser artifacts, cookies, and session data to reconstruct user interactions, website access patterns, and online activities.
  - Example: Analyzing web server logs may uncover patterns of suspicious HTTP requests, such as SQL injection attempts, directory traversal attacks, or attempts to upload malicious files.
- For Malware:
  - Malware analysis encompasses static and dynamic analysis techniques to understand the behavior, functionality, and impact of malicious software on affected systems.
  - Example: Dynamic analysis of malware involves executing it in a controlled environment (e.g., sandbox) to observe its behavior, network communications, and system modifications, enabling analysts to identify its capabilities and intent.

Evidence Acquisition, Analysis and Examination

- **Evidence Examination**:
- **Definition**: Evidence examination involves reviewing, validating, and documenting findings from the analysis to support investigative conclusions and legal proceedings.
- **Example**:
  - For Windows:
    - Examination of Windows evidence may involve generating forensic reports, timelines, and summaries to document key findings and present them as evidence in court.
    - Example: Producing a forensic report detailing the timeline of events, user activities, and file accesses can help corroborate witness testimonies and support legal arguments in a criminal trial.

Evidence Acquisition, Analysis and Examination

- For Linux:
  - Linux evidence examination includes documenting findings, generating forensic artifacts, and preparing expert witness testimonies to present technical evidence in legal proceedings.
  - Example: Providing expert testimony on Linux system logs, file system structures, and network traffic analysis can help clarify complex technical concepts and assist the court in understanding the significance of digital evidence.
- For Email:
  - Examination of email evidence involves validating the authenticity of emails, preserving metadata integrity, and preparing email chains or excerpts for presentation in court.
  - Example: Presenting authenticated email evidence with preserved metadata, such as email headers and timestamps, can strengthen the credibility of electronic communications and support legal arguments in civil litigation or criminal trials.

Evidence Acquisition, Analysis and Examination

- For Web:
  - Web evidence examination includes preparing visual aids, logs summaries, and data visualizations to illustrate key findings and facilitate understanding by legal stakeholders.
  - Example: Creating graphical representations of web access patterns, user sessions, and IP geolocation data can help elucidate complex technical evidence and enhance jury comprehension in a cybercrime trial.
- For Malware:
  - Examination of malware evidence involves documenting malware characteristics, behavior analysis results, and mitigation recommendations to support incident response efforts and legal actions.
  - Example: Providing expert testimony on malware analysis findings, including indicators of compromise (IOCs), mitigation strategies, and potential attribution information, can assist prosecutors in building a case against cybercriminals and malware authors.

Challenges in Computer Forensics

Computer forensics, like any field, faces various challenges, some of which are unique to its nature as a digital investigation discipline. Here are several key challenges encountered in computer forensics:

- **Technological Complexity**: The rapid evolution of technology presents challenges in keeping forensic tools and techniques up-to-date with the latest devices, operating systems, applications, and encryption methods.
- **Volume and Variety of Data**: The sheer volume and diversity of digital data generated by modern computing devices make it challenging to efficiently collect, process, and analyze evidence.
- **Data Encryption and Protection**: Increasing use of encryption technologies to secure data poses challenges in accessing and decrypting digital evidence, particularly in cases involving encrypted hard drives, communication channels, or cloud storage.

Challenges in Computer Forensics

- **Anti-Forensic Techniques**: Perpetrators may employ anti-forensic techniques to conceal, or destroy digital evidence, such as file wiping, data encryption, steganography, and data manipulation.
- **Data Fragmentation and Deletion**: Deleted files, fragmented data, and file system corruption can complicate evidence recovery and reconstruction efforts, requiring specialized techniques and tools for data carving and reconstruction.
- **Cloud Computing and Virtualization**: The adoption of cloud computing services and virtualized environments introduces challenges in preserving, collecting, and analyzing evidence stored off-site or in shared virtual environments.
- **Jurisdictional and Legal Issues**: Cross-border investigations may face jurisdictional challenges, conflicting legal frameworks, and limitations in obtaining evidence from foreign entities, requiring international cooperation and legal assistance treaties.

Challenges in Computer Forensics

- **Privacy Concerns**: Balancing the need for digital evidence collection with privacy rights and data protection regulations poses ethical and legal challenges, particularly in cases involving personal or sensitive information.
- **Chain of Custody**: Maintaining the integrity and continuity of evidence throughout the forensic process, from acquisition to presentation in court, requires meticulous documentation and adherence to chain of custody procedures.
- **Expertise and Training**: The specialized knowledge and skills required for computer forensics demand continuous training and professional development to keep pace with advancements in technology, forensic techniques, and legal requirements.
- **Resource Constraints**: Limited budgets, staffing shortages, and resource constraints may hinder the capabilities of forensic labs and agencies to effectively investigate and prosecute digital crimes.
- **Data Retention Policies**: Organizations' data retention policies and practices may impact the availability and integrity of digital evidence, necessitating collaboration with IT departments and legal teams to preserve and collect relevant data.

Tools used in Computer Forensics

- Computer forensics involves the investigation and analysis of digital devices and data for legal purposes. Various tools are used throughout the process to gather, preserve, analyze, and present digital evidence. Here are some common tools used in computer forensics:
- **Forensic Imaging Tools**: These tools are used to create exact copies (forensic images) of digital storage media, such as hard drives, USB drives, and memory cards, without altering the original data. Popular tools include:
  - FTK Imager
  - EnCase
  - dd (command-line tool in Unix-like systems)

Tools used in Computer Forensics

- **Data Recovery Tools**: These tools help recover deleted, damaged, or hidden data from storage devices. They can be useful in retrieving evidence that has been intentionally or accidentally deleted. Examples include:
  - Recuva
  - TestDisk
  - PhotoRec
- **File Analysis Tools**: These tools are used to analyze files and metadata to extract relevant information. They can examine file headers, footers, and contents to identify file types and uncover hidden data. Examples include:
  - Hex editors (e.g., HxD, Hex Workshop)
  - FileInsight
  - FileAlyzer

Tools used in Computer Forensics

- **Network Forensics Tools**: These tools are used to monitor, capture, and analyze network traffic to investigate security incidents, such as cyber attacks or unauthorized access. Examples include:
  - Wireshark
  - NetworkMiner
  - tcpdump
- **Mobile Device Forensics Tools**: These tools specialize in extracting and analyzing data from mobile devices such as smartphones and tablets. They can recover call logs, messages, photos, and application data. Examples include:
  - Cellebrite UFED
  - Oxygen Forensic Detective
  - XRY

Tools used in Computer Forensics

- **Memory Forensics Tools**: These tools are used to analyze the volatile memory (RAM) of a computer system to identify running processes, open network connections, and other valuable information that may not be present on disk. Examples include:
  - Volatility Framework
  - Rekall
  - Redline
- **Malware Analysis Tools**: These tools are used to dissect and analyze malicious software to understand its behavior, capabilities, and impact on a system. Examples include:
  - IDA Pro
  - OllyDbg
  - Ghidra

Tools used in Computer Forensics

- **Steganography Detection Tools**: These tools help detect hidden messages or data concealed within digital media files using steganography techniques. Examples include:
- Stegdetect
- OutGuess
- OpenStego