UNIT II

Computer Forensics Investigations & Electronic Evidence

DIGITAL FORENSICS

- Digital forensics is the retrieval, analysis, and use of digital evidence in a civil or criminal investigation
- Digital forensic science is a branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrime
- The term digital forensics was first used as a synonym for computer forensics
- However, now it has expanded to cover the investigation of any devices that can store digital data
- Digital forensics is the process of identifying, preserving, analyzing, and documenting digital evidence which can be used by the Court of Law

TYPES OF DIGITAL FORENSICS

- **Disk Forensics:**
- It deals with extracting data from storage media by searching active, modified, or deleted files
- **Network Forensics**:
- It is a sub-branch of digital forensics
- It is related to monitoring and analysis of computer network traffic to collect important information and legal evidence
- **Wireless Forensics**:
- It is a division of network forensics
- The main aim of wireless forensics is to offers the tools need to collect and analyze the data from wireless network traffic
- **Malware Forensics**:
- This branch deals with the identification of malicious code, to study their payload, viruses, worms, etc

TYPES OF DIGITAL FORENSICS

- **Email Forensics:**
- Deals with recovery and analysis of emails, including deleted emails, calendars, and contacts
- **Memory Forensics:**
- It deals with collecting data from system memory (system registers, cache, RAM) in raw form and then carving the data from Raw dump
- **Mobile Phone Forensics:**
- It mainly deals with the examination and analysis of mobile devices
- It helps to retrieve phone and SIM contacts, call logs, incoming, and outgoing SMS/MMS, Audio, videos, etc

TYPES OF DIGITAL FORENSICS

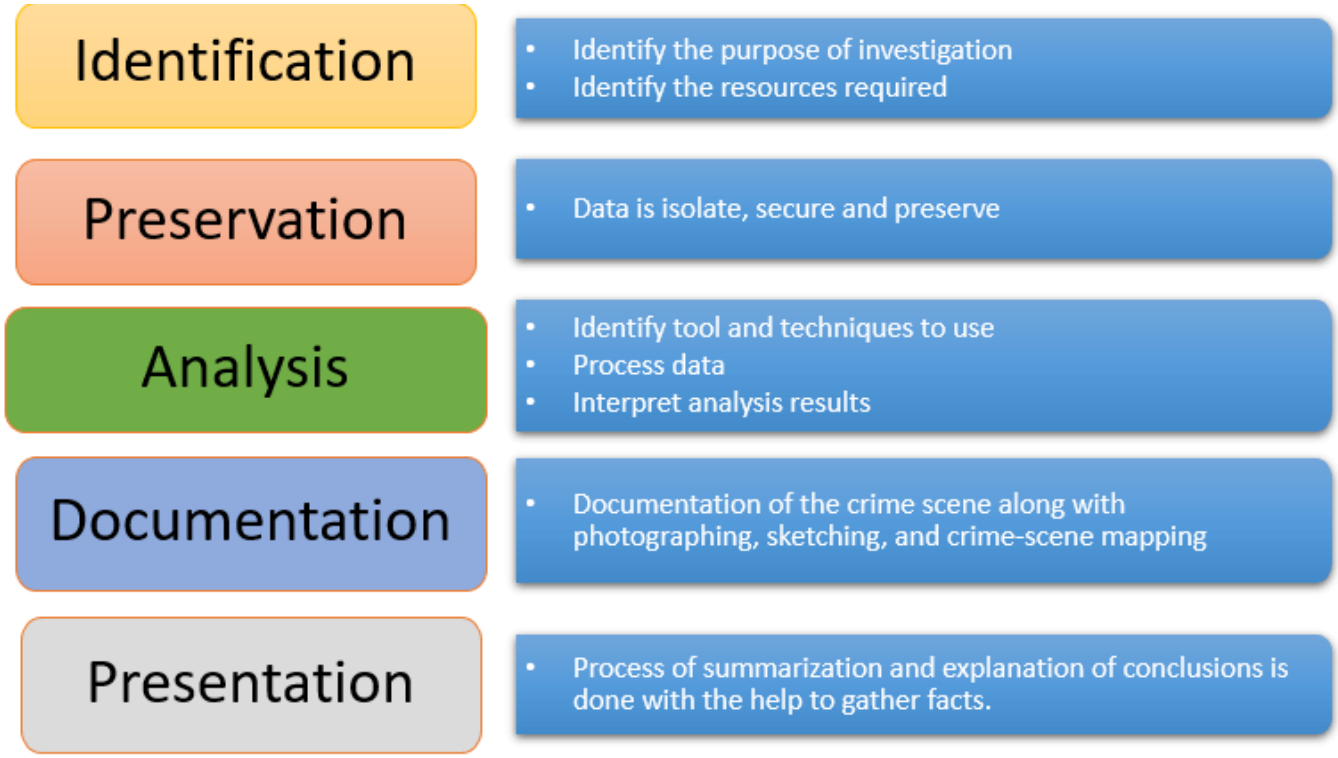
- **Database Forensics**:
- It is a branch of digital forensics relating to the study and examination of databases and their related metadata
- **IoT Forensics**:
- IoT forensics is the practice of analyzing IoT devices to investigate crimes
- Fitness trackers, smart appliances, connected vehicles, would form part of IoT Forensics
- **Cloud Forensics:**
- Cloud forensic is the amalgamation of all the different forensics(i.e. digital forensics, network forensics, hardware forensics etc)

LOCARD'S EXCHANGE PRINCIPLE

- Locard's exchange principle is an important part of forensic science investigation
- It states that any criminal leaves behind a trace when committing a violent crime
- It is the investigator's duty to find this trace evidence and reconstruct the events of the crime
- In other words the perpetrator of a crime will bring something into the crime scene and leave with something from it, and that both can be used as forensic evidence

PROCESS OF DIGITAL FORENSICS

- Digital forensics entails the following steps:



PROCESS OF DIGITAL FORENSICS

- **Identification**
- It is the first step in the forensic process
- The identification process mainly includes things like what evidence is present, where it is stored, and lastly, how it is stored (in which format)
- Electronic storage media can be personal computers, Mobile phones, PDAs, etc
- **Preservation**
- In this phase, data is isolated, secured, and preserved
- It includes preventing people from using the digital device so that digital evidence is not tampered with
- **Analysis**
- In this step, investigation agents reconstruct fragments of data and draw conclusions based on evidence found
- However, it might take numerous iterations of examination to support a specific crime theory

PROCESS OF DIGITAL FORENSICS

- **Documentation**
- In this process, a record of all the visible data must be created
- It helps in recreating the crime scene and reviewing it
- It Involves proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping.
- **Presentation**
- In this last step, the process of summarization and explanation of conclusions is done

DIGITAL INVESTIGATION

- A digital investigation is a process where hypotheses that answer questions about digital events is developed and tested
- A digital forensic investigation is a process that uses science and technology to analyze digital objects and that develops and tests theories
- It should be admissible in a court of law, to answer questions about events that occurred
- In other words, a digital forensic investigation is a more restricted form of digital investigation

DIGITAL CRIME SCENE INVESTIGATION PROCESS

- No single correct methodology for investigation
- One may be more efficient than the other but all may be correct
- Digital crime scene includes digital environment created by hardware and software
- Digital Crime Investigation process has three major phases
  - System Preservation Phase
  - Evidence Searching Phase
  - Event Reconstruction Phase
- Analysis
  - Live – When system resources and OS is investigated to find evidence
  - Dead – When running trusted applications in a trusted OS to find evidence

SYSTEM PRESERVATION PHASE

- Involves preservation of state of digital crime scene
- Action taken is based on legal or operational requirements
- Unplug the system to create a image
- Investigate they system as it is – E.g. honeypot, spyware
- Purpose – To reduce the amount of evidence that could be overwritten
- Write blocker can be used to prevent overwriting of data
- Creating a cryptographic hash of the data like MD5, SHA1, etc

EVIDENCE SEARCHING PHASE

- After data is gathered and preserved, evidence needs to be searched
- Depending the evidence type various locations are searched
- For e.g. For Web browsing habits, there is a need to look at browser history, browser cache, bookmarks, etc
- The hypothesis created based on the case details need to be refuted or supported to ensure appropriateness of evidence collected
- General characteristics of the object being searched needs to be defined and then searched in the data gathered
- Evidence can be searched based on name, pattern, comparing hash, keyword based or searching for IP address, specific port/source address

EVENT RECONSTRUCTION PHASE

- Based on the evidence found reconstruction of the digital event is done in this phase
- During Evidence Searching Phase, if certain files are found which violet IPR laws. This does not tell which event led to the violation. Some file might be downloaded but the app which was used needs to be determined. That means was a malware or a web browser used to download the file
- Once digital event reconstruction is done, it can be compared with physical events
- Event reconstruction requires adequate knowledge of OS and the installed applications

GENERAL GUIDELINES

- PICL should be followed in all investigations to ensure no evidence is left out
  - P – Preservation
  - I – Isolation
  - C - Correlation
  - L - Logging

Preservation

- Original data should be kept in safe custody and investigation should be on the copy of the original data
- Write blocker should be used
- Calculate hash of the original evidence
- Live analysis should be done carefully to prevent overwriting of existing data

GENERAL GUIDELINES

Isolation

- The analysis environment should be isolated from all possible threats
- The data being analysed should not cause any harm to the analysis environment by way of downloads, remote connections, execution of scripts through web browser on opening a HTML file, deleting existing files, etc
- The analysis should be done in a virtual environment to prevent any data loss
- Connection to the outside world should be avoided to prevent any tampering of evidence
- Isolation is implemented using an analysis network that has limited connectivity. For e.g. Using a firewall to prevent outside connection
- Implementing isolation during a live analysis is difficult and hence should be done with caution

GENERAL GUIDELINES

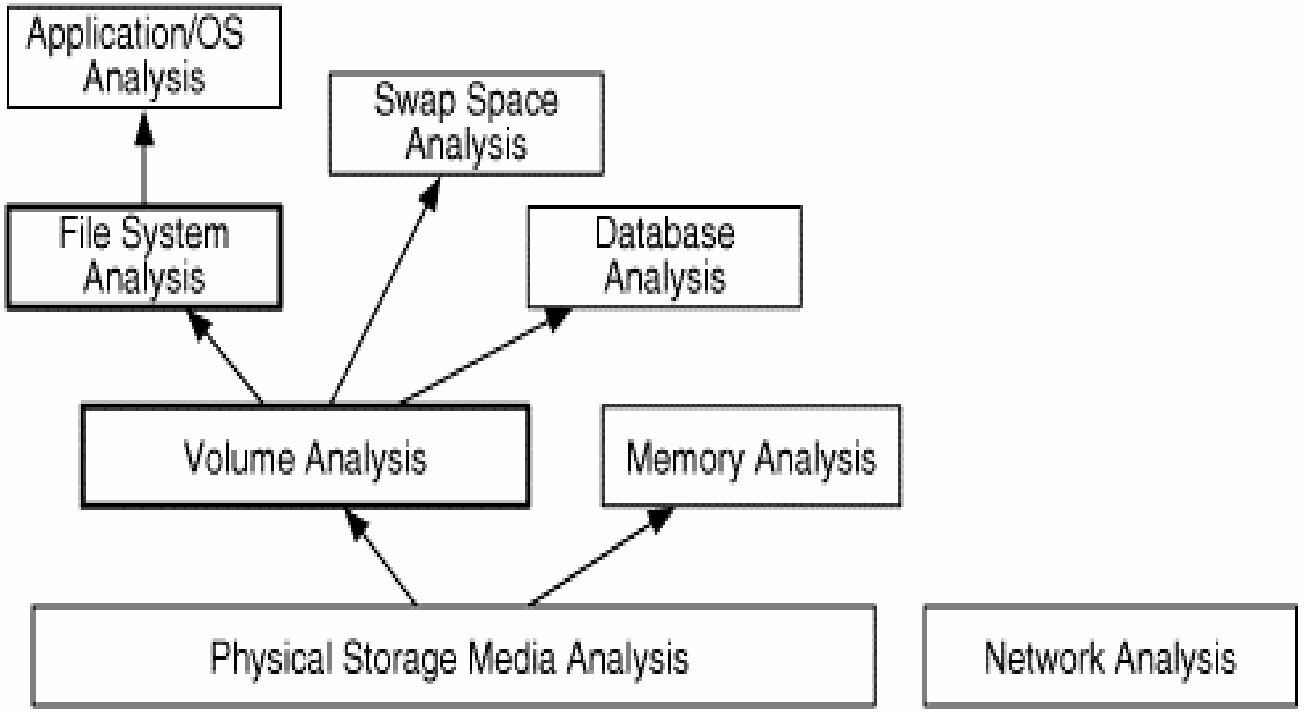
Correlation

- Data should be correlated with other independent sources to prevent any forgery
- Timestamps can be easily manipulated and correlation in preventing such instances
- File activity timeline should be correlated with log entries, network traffic or other events

Logging

- All the actions being taken should be logged and documented
- This will prevent missing important actions and activities
- Data changes during live analysis should be well documented

ANALYSIS



Layers of Analysis

DIGITAL EVIDENCE

- Digital evidence is information and data of value to an investigation that is stored on, received, or transmitted by an electronic device
- This evidence is acquired when data or electronic devices are seized and secured for examination
- Digital evidence
  - Is latent, like fingerprints or DNA evidence
  - Crosses jurisdictional borders quickly and easily
  - Is easily altered, damaged, or destroyed
  - Can be time sensitive

EVIDENCE ACQUISITION

- Evidence handling is one of the most important aspects in the expanding field of computer forensics
- Precautions should be taken in the collection, preservation and transportation of digital evidence
- First responders may follow the steps listed below to guide their handling of digital evidence at an electronic crime scene:
  - Recognize, identify, seize, and secure all digital evidence at the scene
  - Document the entire scene and the specific location of the evidence found
  - Collect, label, and preserve the digital evidence
  - Package and transport digital evidence in a secure manner

EVIDENCE ACQUISITION

- Before collecting evidence at a crime scene, first responders should ensure that
  - Legal authority exists to seize evidence
  - The scene has been secured and documented
  - Appropriate personal protective equipment is used
- First responders without the proper training and skills should not attempt to explore the contents of or to recover information from a computer or other electronic device other than to record what is visible on the display screen
- Do not press any keys or click the mouse

EVIDENCE ACQUISITION

- For proper evidence preservation, follow these procedures in order (Do not use the computer or search for evidence)
  - Photograph the computer and scene
  - If the computer is off do not turn it on
  - If the computer is on photograph the screen
  - Collect live data - start with RAM image and then collect other live data "as required" such as network connection state, logged on users, currently executing processes etc.
  - If hard disk encryption detected such as full disk encryption i.e. PGP Disk — collect "logical image" of hard disk using recommended tools
  - Unplug the power cord from the back of the tower - If the computer is a laptop and does not shut down when the cord is removed then remove the battery

EVIDENCE ACQUISITION

- Document all device model numbers and serial numbers
- Disconnect all cords and devices
- Image hard drives using a write blocker
- Package all components (using anti-static evidence bags)
- Seize all additional storage media (create respective images and place original devices in anti-static evidence bags)
- Keep all media away from magnets, radio transmitters and other potentially damaging elements
- Collect instruction manuals, documentation and note
- Document all steps used in the seizure and maintain proper Chain of Custody

CHAIN OF CUSTODY

- Definition: The movement and location of physical evidence from the time it is obtained until the time it is presented in court
- As is the case with all evidence, it's important to maintain a chain of custody for computer evidence
- The term "chain of custody" refers to documentation that identifies all changes in the control, handling, possession, ownership, or custody of a piece of evidence (physical or electronic)
- It is required to trace the route that evidence takes from the moment it is collected until the time it is presented in Court of Law
- Chain of Custody refers to the logical sequence that records the sequence of custody, control, transfer, analysis and disposition of physical or electronic evidence in legal cases
- Each step in the chain is essential and if there is a break, the evidence may be rendered inadmissible

CHAIN OF CUSTODY

- Maintaining the chain of custody is critical in forensic practice to avert tampering
- A record of the chain of evidence must be maintained and established in the court whenever presenting evidence as an exhibit
- The goal is to establish that the evidence is related to the alleged crime, was collected from the scene, and was in its original/unaltered condition rather than having been tampered with or "planted" deceitfully to make someone seem guilty
- The chain of custody maintains the integrity of the sample
- The traceability of the record of the control, transfer, and analysis of samples indicates the transparency to the procedure

WRITE BLOCKER

- A write blocker is any tool that permits read-only access to data storage devices without compromising the integrity of the data
- It prevents any write access to the hard disk
- Write blockers are devices that allow acquisition of information on a drive without creating the possibility of accidentally damaging the drive contents
- They do this by allowing read commands to pass but by blocking write commands
- As per NIST general guidelines
  - The write-blocker tool shall not allow a protected drive to be changed
  - The write-blocker tool shall not prevent any operations to a drive that is not protected
  - The write-blocker tool shall not prevent obtaining any information from or about any drive

WRITE BLOCKER

- Write Blockers are basically of 2 types: Hardware Write Blocker and Software Write Blocker
- Hardware write blocker—The hardware blocker is a device that is installed that runs software internally to itself and will block the write capability of the computer to the device attached to the write blocker
- Software write blocker—The software blocker is an application that is run on the operating system that implements a software control to turn off the write capability of the operating system

DATA RECOVERY VS CARVING

- The principle of file recovery of deleted files is based on the fact that Windows does not wipe the contents of the file when it's being deleted
- Instead, a file system record storing the exact location of the deleted file on the disk is being marked as "deleted" and the disk space previously occupied by the deleted file is then labeled as available – but not overwritten with zeroes or other data
- Carving means bit-precise and sequential examination of the entire content of the hard drive. The concept of Data Carving is completely different from File Recovery
- File carving works only on raw data on the media and it is not connected with file system structure. File carving doesn't care about any file systems which is used for storing files

DATA RECOVERY VS CARVING

- Data carving or file carving is a forensic method used for reassembling files in unallocated space in the drive
- Data carving allows for detecting and recovering files and other objects based on filesystem contents rather than a filesystem's metadata and file structure
- Data Carving is based on looking for characteristic signatures or patterns
- File recovery techniques make use of the file system information and, by using this information, many files can be recovered
- Scalpel, FTK, Encase, Foremost are some of the data recovery/carving tools

IMPORTANCE OF DATA RECOVERY

- Recover deleted and hidden files
  - File deleted or hidden by criminals can be recovered using data recovery tools which can form important forensic evidence
- Can analyze almost all memory-based devices
  - Deleted files on cellphones, computers, USB, emails, external hard drives, and even cloud-based accounts, GPS devices and smart watches can all be examined for forensic data recovery
- Finding Unknown
  - Patterns, links between various sets of data and connecting the dots to uncover information that might not be initially considered to be irrelevant or inaccessible can be helo in recovering lot of unknowns
- Preserves data integrity
  - The integrity of the collected data is protected by using writer-blocker thereby helping presenting the evidence in its original state