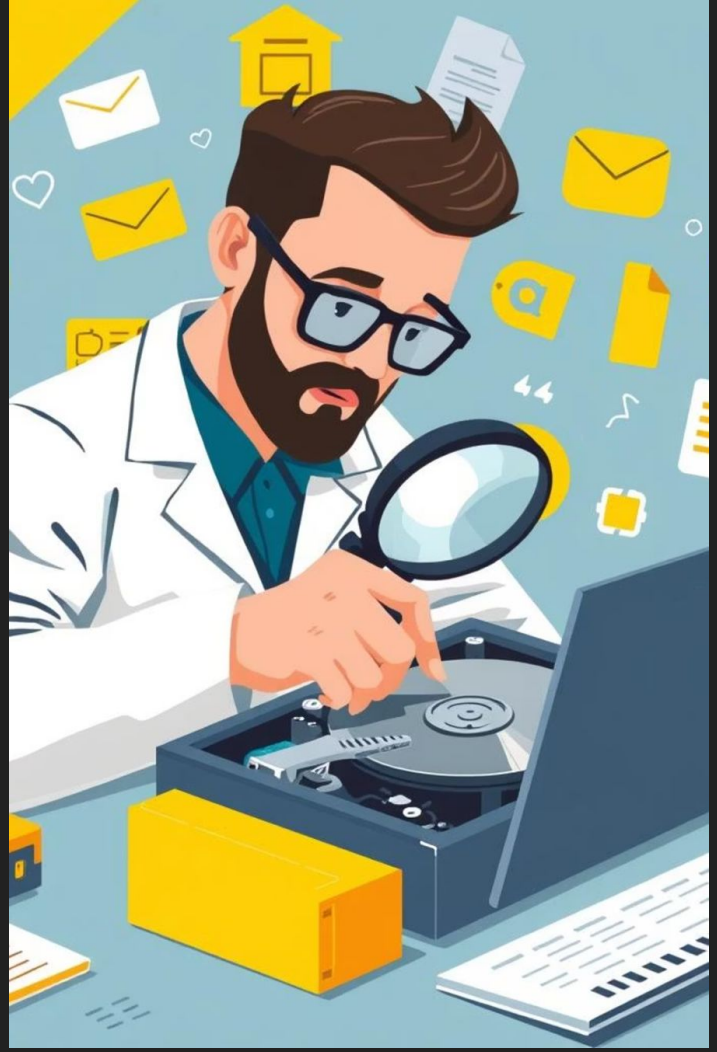
Cyber Forensics

Priya J D, MESCE



Contents

- Overview of cyber crime
- Investigation Steps
- Storage Formats
- Securing Digital Evidence

Cyber Forensics

- Cyber Forensics, also known as digital forensics, is the application of scientific investigation and analysis techniques to identify, collect, examine, and preserve digital evidence in a manner that is legally admissible

- Goal is to aid in the detection and prevention of cybercrime and other legal issues where digital data is relevant

- It encompasses a wide range of activities, from recovering deleted files to analysing network traffic, by adhering to strict legal and ethical guidelines to ensure evidence admissibility in court

Types of Cyber Forensics

- Memory Forensics
  - Deals with collecting information from main memory, cache
- Disk Forensics
  - Deals with recovering information from secondary storage media such as hard disks, pen drives, CD/DVD drives
- Database Forensics
  - Deals with examining and analysing databases

Types of Cyber Forensics

- Email Forensics
  - Deals with extracting information from Emails
- Network Forensics
  - Deals with extracting information from various computer networks
- Mobile Phone Forensics
  - Deals with extracting information from Mobile Phones

Computer Crimes

- Computer crime refers to any criminal activity that involves a computer or network, either as the target of the crime or as a tool used to commit it. Includes a wide array of illicit activities, such as
    - Hacking and unauthorised access to systems
    - Data theft and intellectual property infringement
    - Distribution of malware and ransomware attacks
    - Cyberstalking and Online harassment
    - Financial fraud conducted through digital means

Evolution of Computer Forensics

Year	Event
1835	Scotland Yard's Henry Goddard became the first person to use physical analysis to connect a bullet to the murder weapon
1836	James Marsh developed a chemical test to detect arsenic, which was used during a murder trial
1892	Sir Francis Galton established the first system for classifying fingerprints
1896	Sir Edward Henry, based on the direction, flow, pattern and other characteristics in fingerprints
1920	American physician Calvin Goddard created the comparison microscope to help determine which bullets came from which shell casings
1930	Karl Landsteiner won the Nobel Prize for classifying human blood into its various groups

Evolution of Computer Forensics

Year	Event
1970	Aerospace Corporation in California developed a method for detecting gunshot residue using scanning electron microscopes
1984	FBI Magnetic Media program, which was later renamed to Computer Analysis and Response Team (CART), was created and it is believed to be the beginning of computer forensic
1988	International Association of Computer Investigative Specialists(IACIS) was formed
1995	International Organization on Computer Evidence (IOCE) was formed
1997	G8 nations declared that “Law enforcement personnel must be trained and equipped to address hightech crimes”
1998	• G8 appointed IICE to create international principles, guidelines and procedures relating to digital evidence • 1 st INTERPOL Forensic Science Symposium was held
2000	First FBI Regional Computer Forensic Laboratory established.

Company Policy Violations

Unauthorized Access

Accessing company systems or data without explicit permission, often leading to data breaches or intellectual property theft

Email misuse

Using company email for personal gain, sending inappropriate content, or engaging in phishing attempts against colleagues

Data Exfiltration

Illegally transferring sensitive company data to external storage or personal devices

Network Abuse

Engaging in activities that overload network resources or compromise network security, such as excessive streaming or unauthorised software installations

Preparing a Cyber Forensics Case: The Initial Steps

- The success of any cyber forensics investigation depends on meticulous preparation

This phase involves

- Understanding the scope of the incident
- Identifying potential sources of evidence
- Establishing the necessary legal and technical frameworks to proceed

Preparing a Cyber Forensics Case: The Initial Steps

- Make an initial assessment about the type of case you're investigating
  - To assess the type of case you're handling, talk to others involved in the case and ask questions about the incident
- Determine a preliminary design or approach to the case
  - Outline the general steps you need to follow to investigate the case
- Create a detailed checklist
  - Refine the general outline by creating a detailed checklist of steps and an estimated amount of time for each step
- Determine the resources you need
  - Based on the OS of the computer you're investigating, list the software you plan to use for the investigation
- Obtain and copy an evidence drive

Preparing a Cyber Forensics Case: The Initial Steps

- Identify and minimize the risks
  - List the problems you normally expect in the type of case you're handling. This list is known as a standard risk assessment
- Test the design
  - Review the decisions you've made and the steps you've completed.
- Analyze and recover the digital evidence
  - Using the software tools and other resources you've gathered, and making sure you've addressed any risks and obstacles, examine the disk to find digital evidence

Preparing a Cyber Forensics Case: The Initial Steps

- Investigate the data you recover
  - View the information recovered from the disk, including existing files, deleted files, e-mail, and Web history, and organize the files to help find information relevant to the case
- Complete the case report
  - Write a complete report detailing what you did and what you found
- Critique the case
  - Self-evaluation and peer review to determine how you could have improved your performance

Planning an Investigation

Effective planning is the cornerstone of a successful cyber forensics investigation. It involves a strategic roadmap that outlines the objectives, scope, and resources required to address the digital incident systematically

- Define Objectives
  - Clearly articulate what needs to be achieved, whether it's identifying a perpetrator, recovering data, or understanding an attack's modus operandi
- Identify Scope
  - Determine the systems, networks, and data sources that are relevant to the investigation

Planning an Investigation

- Formulate Hypothesis
  - Develop initial theories about how the incident occurred, which will guide evidence collection and analysis

- Allocate Resources
  - Assign personnel, tools, and timeframes necessary for the investigation, ensuring efficient use of capabilities

Industrial Espionage Investigation

- Identifying the threat
  - Recognizing potential cyber espionage activities like unauthorized access, data breaches and suspicious network activity

- Evidence Gathering
  - Employing forensic tools and techniques to collect and analyse digital evidence

Industrial Espionage Investigation

- Analysis and Reconstruction
  - Examine the collected data to reconstruct the attack timeline, identify the attacker’s methods and understand the extent of data breach

- Reporting and Remediation
  - Preparing detailed reports of the findings and recommending security measures to prevent future attacks

Cyber Forensics Process

Consists of 4 stages

- Assess the situation
  - Analyze the scope of the investigation and the action to be taken
- Acquire the data
  - Gather, protect, and preserve the original evidence
- Analyze the data
  - Examine and correlate digital evidence with events of interest
- Report the investigation
  - Gather and organize collected information and write the final report

Assessment Phase

- Obtain proper authorization
- Understand the laws that might apply to the investigation as well as any internal organization policies
- Identifying team members
- Conduct a thorough assessment
  - Current and potential business impact of the incident
  - Identify affected infrastructure
  - Thorough understanding of the situation

Gathering Evidence

To gather evidence from a digital devices, we have to retrieve the exact copy from the storage medium

- This exact duplicate [includes information such as the boot sector, partition, and unallocated disk space] is called the bit stream copy (forensic copy) of the storage medium

- Example Tools : EnCase, FTK

Gathering Evidence

- The process of extracting this copy is called acquiring an mage or making an image of the storage medium
- This bit stream copy of all data in a disk is stored in a file called bit stream image
- The bit stream copy is different from the backup copy of a disk. Backup software can copy only files that are stored in a folder or are of a known file type. Backup software can’t copy deleted files

Storage Formats for Digital Evidence

The data a forensics acquisition tool collects is stored as an image file in different formats

- **Raw Format**
  - It is bit-by-bit copy of the data on the storage media without any additions and or deletions
  - Widely used for evidence preservation and examination purposes

Storage Formats for Digital Evidence

Advantages

- Fast Data Transfers
- Error Tolerance
  - Capable to ignore minor data read errors on the source drive, which can be beneficial when dealing with damaged or partially corrupted media
- Compatibility
  - Most computer forensics tools support raw format, making it a universal acquisition format for forensic investigations

Storage Formats for Digital Evidence

Disadvantage

- Does not contain any metadata
- Requires as much space as the original disk
- Handling of Bad Sectors
    - Some raw format tools may not effectively collect bad sectors on the source drive, leading to incomplete data acquisition

Storage Formats for Digital Evidence

- **Proprietary Formats**
  - Vendor specific format for storing digital evidence
  - Can only be read by the corresponding vendor software
- Ex.
  - ILookIX image acquisition tool IXImager produces three proprietary formats - IDIF, IRBF and IEIF
  - They can be read by IXImager only

Storage Formats for Digital Evidence

- Advantage
  - Offer the choice to compress or not compress image files
  - Capability to split an image into smaller segmented files for archiving purposes
  - Capability to integrate metadata into the image file, such as date and time of the acquisition, investigator or examiner name, and comments or case details
- Disadvantage : Cannot be read by software from other vendors

Storage Formats for Digital Evidence

- Advanced Forensic Format (AFF)
  - An open source format developed by Dr. Simson L. Garfinkel
  - Capable of producing compressed or uncompressed image files
  - Can store metadata as part of image files

Data Acquisition Methods

- The gathering and recovery of sensitive data during a digital forensic investigation is known as data acquisition
- There are two types of acquisitions
- Static Acquisitions
  - Acquiring data from a seized computer, when it is powered off. Cannot be used to gather volatile data
  - Preferred method for collecting evidence because it preserves the original state of the data

Data Acquisition Methods

- Live Acquisitions
  - Involves extracting data from actively running systems without altering their state
  - This method allows investigators to collect volatile data, such as running processes, open network connections, data loaded into memory and temporary files

Data Acquisition Methods

- For collecting evidence from a large drive Logical acquisition or Sparse acquisition method can be used

- Logical Acquisition captures only specific files of interest to the case or specific types of files

- Sparse Acquisition is similar but also collects fragments of deleted data

Data Acquisition Tools

- Accessing a disk drive directly can easily contaminate the evidence during forensics acquisition. Hence it is accessed indirectly using boot CD/DVD/USB drives
- After booting using CD/DVD/USB Drives, the hard disk is write protected
- Mini-WinFE is one such boot utility for Windows
- Linux boot CD/DVD/USB can also be used for this purpose
- We can also use Linux live CD/DVD/USB drives for digital forensics analysis
- Using a boot CD/DVD/USB drive, we can access the hard disk, without having an OS
- Using a live CD/DVD/USB drive, we can start an OS

Data Acquisition Tools

The following Linux live CD/DVD/USB drives supports digital forensics analysis

- Penguin Sleuth Kit (www.linux-forensics.com)
- CAINE (www.caine-live.net)
- Deft (www.deftlinux.net)
- Kali Linux (www.kali.org)
- Knoppix (www.knopper.net/knoppix/index-en.html)
- SANS Investigate Forensic Toolkit (SIFT)

  http://computer-forensics.sans.org/community/downloads)

Digital Evidence Validation Methods

- Digital Evidence Validation is done to check the integrity of the data collected during investigation
- For this a hashing algorithm utility is applied on a dataset like file or disk drive which create a unique binary or hexadecimal number (hash value) referred as “digital fingerprint”
- This represents the uniqueness of a data set
- Making any alteration in one of the files—even changing one letter from uppercase to lowercase—produces a completely different hash value

Digital Evidence Validation Tools

- Linux Validation Tools
  - The linux shell commands dd and dcfldd, have several options that can be combined with other commands to validate data
  - Current distributions of Linux include two hashing algorithm utilities : md5sum and sha1sum
  - Both utilities can compute hashes of a single file, multiple files, individual or multiple disk partitions, or an entire disk drive

Digital Evidence Validation Tools

- Windows Validation Tools
  - Unlike Linux, Windows has no built-in validation tools. The following third party programs can be used
    - X-Ways WinHex
    - Breakpoint Software Hex Workshop
    - OSForensics
    - Autopsy
    - EnCase
    - FTK

Storing Digital Evidence - Evidence Retention

- The choice of media for storing digital evidence depends on how long you need to keep it. The following storage mediums can be used for digital evidence
  - Magnetic Tapes, Hard Disk Drives, CD/DVD, Pen Drives, Cloud based systems
- If evidence need to be retained for longer periods of time, the following storage mediums are suitable
  - Magnetic Tapes
  - Cloud based systems
- To enhance security it is better to store digital evidence in multiple storage mediums

Storing Digital Evidence - Evidence Retention

Best practices for data storage and archival include the following:

- Physically secure and store the evidence in a tamperproof location
- Ensure that no unauthorized personnel has access to the evidence, over the network or otherwise
- Protect storage equipment from magnetic fields
- Make at least two copies of the evidence collected, and store one copy in a secure offsite location

Storing Digital Evidence - Evidence Retention

- Ensure that the evidence is physically secured (by placing the evidence in a safe) as well as digitally secured (by assigning a password to the storage media)

- Clearly document the chain of custody of the evidence. Create a check-in / check-out list that includes information such as the name of the person examining the evidence, the exact date and time they check out the evidence, and the exact date and time they return it


Thank
You!