Introduction to Digital Forensics

Contents

- In this chapter, we will cover the following topics:
  - Defining digital forensics and goals
  - Defining cybercrime and cybercrime sources
  - Computers in cybercrimes
  - Digital forensics categories
  - Forensic data analysis
  - Digital forensic users
  - Investigation types
  - Forensics readiness
  - Digital evidence types
  - Electronic evidence location
  - Chain of custody
  - Examination process

Defining digital forensics

- Digital forensics is a branch of forensic science that uses scientific understanding to acquire, evaluate, record, and present digital evidence related to computer crime in court.
- The main goal is to figure out what happened, when it happened, and who did it.
- The term “digital forensics” is a catch-all word for computer forensics or, more recently, “cyber forensics.”
- These investigations include user laptops, computers, mobile phones, network devices, Webcams, tablets, camcorders, IoT and smart home devices, and storage media such as USB drives, CD/DVD, SD cards, and tapes, among other digital systems and devices that can send, receive, and store digital data.

Defining digital forensics

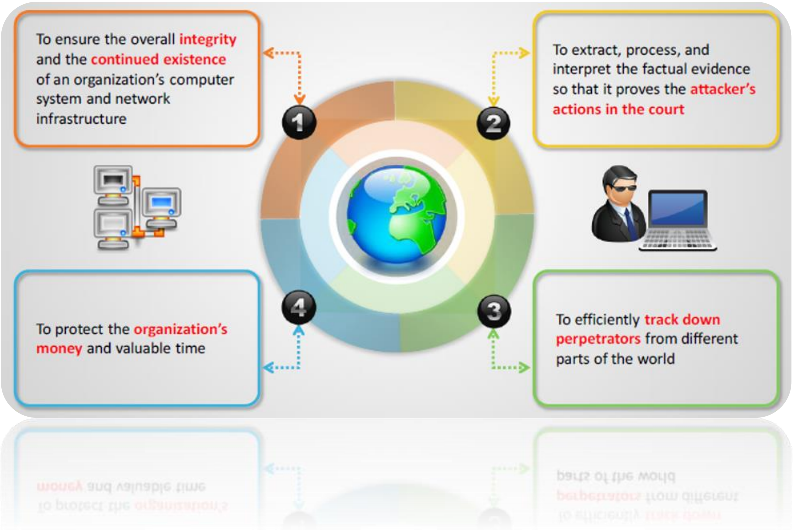
- Objectives

To recover, analyze, and preserve computer and related materials in such a way that they can be presented as evidence in a court of law

To identify the evidence quickly, estimate the potential impact of the malicious activity on the victim, and assess the intent and identity of the perpetrator

Defining digital forensics

- Need for computer forensics



1 To ensure the overall integrity and the continued existence of an organization's computer system and network infrastructure

2 To extract, process, and interpret the factual evidence so that it proves the attacker's actions in the court

3 To efficiently track down perpetrators from different parts of the world

4 To protect the organization's money and valuable time

Defining digital forensics

- Digital forensics is a relatively new profession in the cybersecurity domain that is becoming increasingly important as the number of crimes and unlawful actions in cyberspace increases.
- In comparison to conventional forensic science (blood tests, DNA profiling, or fingerprinting)
  - digital forensics is a young science;
  - the fact that it interacts with rapid changes in the computing ecosystem around us and reaches other domains (such as the judicial process, law enforcement, management consulting, information technology, and the borderless scope of the internet),
    - makes it a difficult field that requires constant development of its foes.

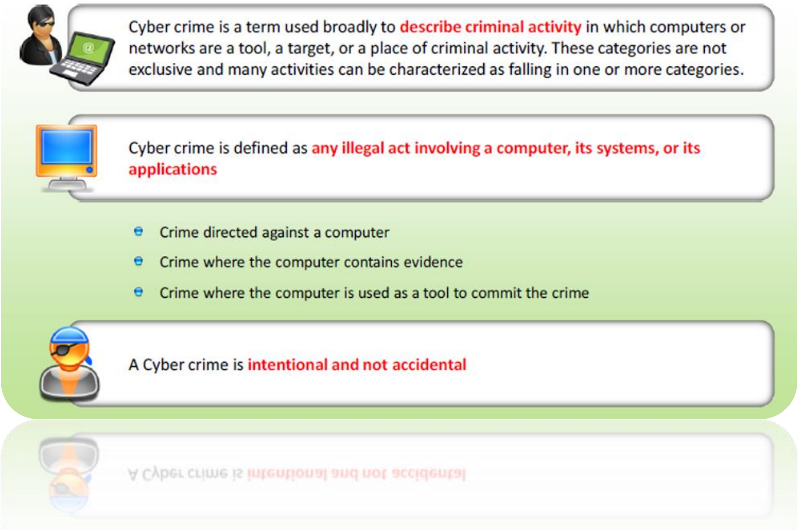
Digital forensics goals

- The basic goal of digital forensics is to investigate crimes committed with computer systems that store and processes digital data and to extract forensic' digital evidence to present in court.
- This is achieved in the following ways using digital forensics.
- Locating and preserving legal evidence on computer devices in a way that is acceptable in a court of law.
  - Follow court-approved technological methods to preserve and recover evidence.
  - Assigning responsibility for an activity to the person who initiated it.
  - Determining data breaches inside a company.
  - Identifying the extent of any damage that may occur as a result of a data breach.
  - Compiling the findings into a formal report that may be submitted in court.
  - Providing expert evidence in court as a guide.

Defining cybercrime

- Any illegal activity carried out on a computer or via a computer network, such as the internet, is referred to as cybercrime.
- Cybercrime is defined as any unlawful behavior done against or with the use of a computer or computer network.
- The fundamental motivation for cybercrime is financial gain (for example: spreading malware to steal access codes to bank accounts).
- However, different motives drive a significant portion of cybercrime, including disrupting service (for example, DDoS attacks to shut down a target organization's services), stealing confidential data (for example, consumer data and medical information), cyber espionage (corporate trade and military secrets), or illegally exchanging copyrighted materials.

Defining cybercrime



Cyber crime is a term used broadly to **describe criminal activity** in which computers or networks are a tool, a target, or a place of criminal activity. These categories are not exclusive and many activities can be characterized as falling in one or more categories.

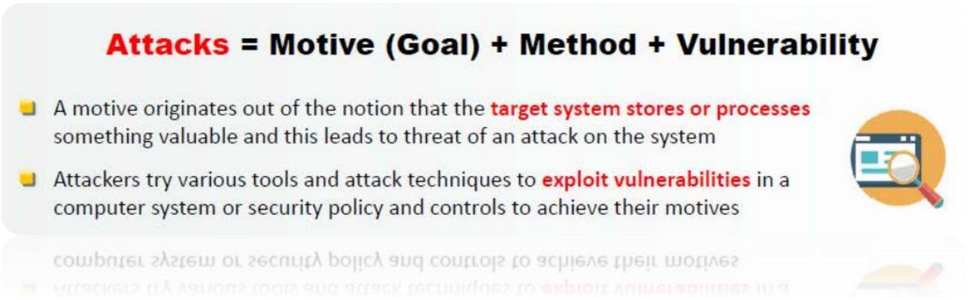
Cyber crime is defined as **any illegal act involving a computer, its systems, or its applications**

- Crime directed against a computer
- Crime where the computer contains evidence
- Crime where the computer is used as a tool to commit the crime

A Cyber crime is **intentional and not accidental**

Defining cybercrime

- Security Attack
  - any action that compromises the security of information owned by an organization

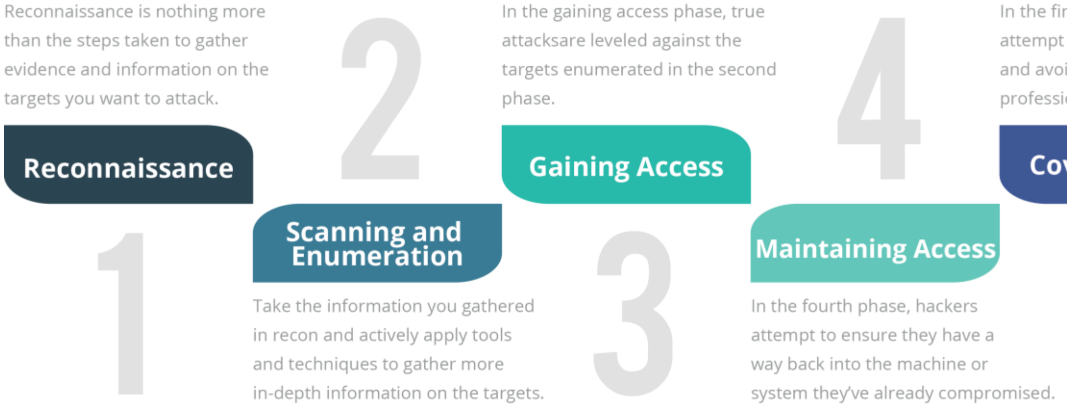


Attacks = Motive (Goal) + Method + Vulnerability

- A motive originates out of the notion that the **target system stores or processes** something valuable and this leads to threat of an attack on the system
- Attackers try various tools and attack techniques to **exploit vulnerabilities** in a computer system or security policy and controls to achieve their motives

Defining cybercrime

- Hacking phases



Reconnaissance is nothing more than the steps taken to gather evidence and information on the targets you want to attack.

Take the information you gathered in recon and actively apply tools and techniques to gather more in-depth information on the targets.

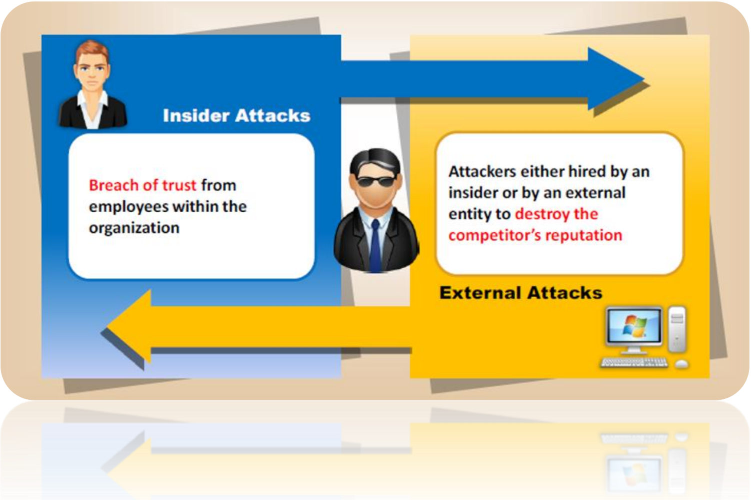
In the gaining access phase, true attacksare leveled against the targets enumerated in the second phase.

In the fourth phase, hackers attempt to ensure they have a way back into the machine or system they've already compromised.

In the final phase, attackers attempt to conceal their success and avoid detection by security professionals.

Sources of cybercrime

- Insider threats and external attacks are the two primary sources of cybercrime.



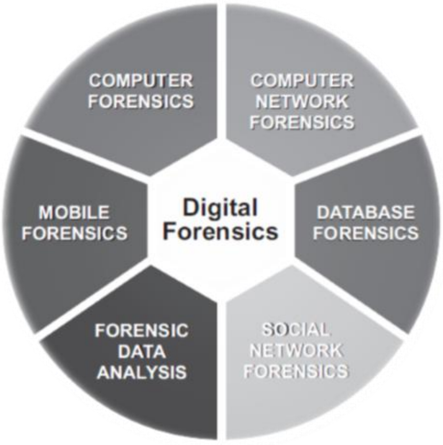
Breach of trust from employees within the organization

Attackers either hired by an insider or by an external entity to destroy the competitor's reputation

Computers in cybercrimes

- Cybercrime may be classified into three types based on how a computer was used to commit a crime.
  - The computer is used as a weapon in the commission of a crime. Launching denial-of-service (DoS) attacks or delivering ransomware are two examples.
  - Crime has been committed against a computing device. Obtaining illegal access to a target computer, for example.
  - The computer is used to aid in the commission of a crime. Using a computer to keep incriminating data or communicate with other criminals online, for example.

Digital forensics categories



Digital forensics investigation types

- According to who is in charge of commencing the inquiry, digital forensic investigations may be divided into two categories:
  - Public investigation
  - Private sector investigations
- Criminal cases leveraging investigations are handled according to the legal guidelines set out by the appropriate authorities.
- Law enforcement agencies participate in public investigations, which are conducted under national or state legislation.
- The three main phases of these investigations are complaint, investigation, and prosecution.
- Private investigations are commonly conducted by businesses to investigate policy violations, legal problems, unfair dismissal, or the leak of secret information as industrial espionage

Type of digital evidence

- User-created data
  - Previous backups (including both cloud storage backups and offline backups such as CDs/DVDs and tapes)
  - Account details (username, picture, and password)
  - E-mail messages and attachments (both online and client e-mails as Outlook)
  - Audio and video files
  - Address book and calendar
  - Webcam recordings (digital photos and videos)
  - Content files (for example, MS Office documents, IM conversations, bookmarks), spreadsheets, databases, and any other digitally stored text
  - Hidden and encrypted files (including zipped folders) created by the computer user
- Machine and network-created data

Type of digital evidence

- User-created data
- Machine and network-created data
  - Configuration files and audit trails, including third-party service providers (for example, Internet service providers(ISPs) often retain customers’ accounts and browser history logs)
  - Logs on the computer under Windows OS contain the following logs:
  - Logs for application, security, setup, system, forward events, apps, and services
  - GPS tracking information history
  - Temporary files
  - Information from the browser (browser history, cookies, and download history)
  - In addition to the IP addresses associated with a LAN network and the broadcast settings, devices have Internet protocol (IP) and MAC addresses
  - Instant messenger history and buddy list (Skype and WhatsApp) (from devices with GPS capability)
  - Application and Windows history (for example, a recently opened file in MS Office)
  - Under Windows computers, restore points
  - E-mail header information
  - Registry files in Windows OS
  - Hidden and conventional system files
  - Printer spooler files
  - Virtual machines
  - Surveillance video recordings
  - Paging and hibernation files and memory dump files

Locations of electronic evidence

- Systems: Desktops, Laptops, Tablets, Servers, and RAIDs
- Network devices: Hubs, switches, modems, routers, and wireless access points
- Internet-enabled home automation and IoT devices: Air conditioners and Smart refrigerators
- DVRs and surveillance systems
- MP3 players
- GPS devices
- Smartphones
- PDA
- Game stations—Xbox, PlayStation
- Digital cameras
- Smart cards
- Pagers
- Digital voice recorders

Chain of custody

- A chain of custody is required for any digital forensic investigation approach.
- A proper chain of custody should detail how digital evidence was discovered, gathered, transported, researched (analyzed), stored, and maintained by the various parties involved in the investigation.
- The ultimate goal is to protect the integrity of digital evidence by tracking down everyone who had contact with it from the moment it was collected until it was presented in court.
- If we fail to understand who made contact with the evidence at any time throughout the investigation, the chain of custody will be jeopardized, and the obtained evidence will be rendered useless in a court of law.
- To maintain a proper chain of custody that is acceptable in court, an audit record for all acquired digital evidence that tracks the movements and possessors of digital evidence at all times must be preserved

Chain of custody

- If the chain of custody is valid, investigators will be capable of answering questions in a court of law:
  - What is the definition of digital evidence? (For example, describe the digital proof that was obtained.)
  - Where did you find the digital evidence? (For example, a computer, tablet, or mobile phone; furthermore, the status of the computing device
  - when the digital evidence is acquired—ON or OFF?)
  - How did the digital evidence come to be? (For example, tools employed; you should also indicate the procedures done to protect evidence integrity throughout the acquisition phase.)
  - What methods were used to transfer, preserve, and handle digital evidence?
  - What methods were used to assess the digital evidence? (For example, any tools and procedures used.)
  - When, by whom, and for what purpose was digital evidence accessed?
  - What was the role of digital evidence in the investigation?

Examination process

- Although there is no globally agreed method or procedure for performing digital forensic investigations, various approaches are in place, with varying stages or phases. However, all strategies divide the job into four primary phases.
  - Search and seizure
  - Acquiring
  - Analyze
  - Information gathering and reporting

- 1. Computer Forensics is also known as.
  - a. Digital Forensic Science
  - b. Computer Crime Stream
  - c. Computer Forensic Science
  - d. Computer Forensics Investigations

- 2. Computer Forensics can also be used in civil proceedings.
  - a. True
  - b. False
  - c. Can be Yes or No
  - d. Cannot say

- 3. You are supposed to maintain three types of records in Forensics, which of these is not a record?
  - a. Chain of Custody
  - b. Documenting crime scene
  - c. Searching crime scene
  - d. Documenting actions

- 4. Volatile data resides in.
  - a. Registries
  - b. Cache
  - c. RAM
  - d. All the above

- 5. Forensic investigators should satisfy ….
  - a. Contribute to society and human being
  - b. Avoid harm to others
  - c. Honest and trustworthy
  - d. All Of the Above

- 6. Digital evidence is used to establish a credible link between……….
  - a. Attacker and victim and the crime scene
  - b. Attacker And information
  - c. Either A or B
  - d. Both A and B

- 7. The evidence and proof that can be obtained from the electronic source is called the…….
  - a. Digital Evidence
  - b. Explainable evidence
  - c. Either A or B
  - d. Both A and B

- 8. Digital Evidence must follow the requirement of the …
  - a. Ideal Evidence Rule
  - b. Best Evidence Rule
  - c. Exchange Rule
  - d. All of the mentioned

- 9. A false positive can be defined as …
  - a. An alert that indicates nefarious activity on a system that, upon further inspection, turns out to represent legitimate network traffic or behavior
  - b. An alert that indicates nefarious activity on a system that, upon further inspection, turns out to truly be nefarious activity
  - c. The lack of an alert for nefarious activity
  - d. All of the above

- 10. A valid definition of digital evidence is:
  - a. None of the below
  - b. Data stored or transmitted using a computer
  - c. Digital data of probative value
  - d. Any digital evidence on a computer