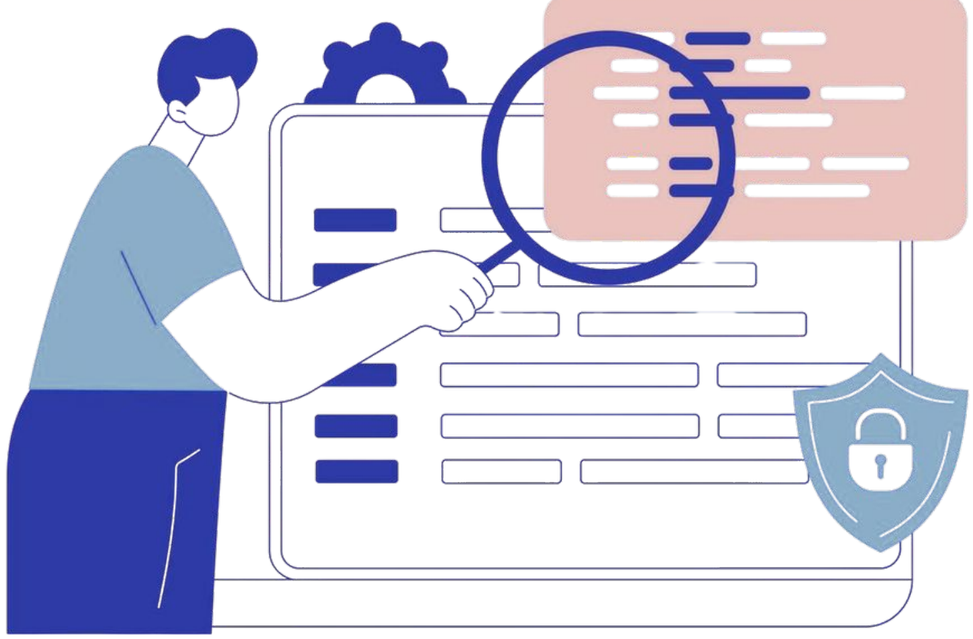


Digital Forensics I

Presented By:

Rakib Hossen
Assistant Professor
Dept. of Cyber Security Engineering (CySE), UFTB

What is forensic?

- **Collection** and **analysis** of evidence
- Using scientific test or techniques
  - ✓To **establish facts** against crime
  - ✓For **presenting** in a **legal proceeding**

- Therefore forensic science is a scientific method of **gathering** and **examining information** about the **past** which is then used in **court of law**

Introduction

01 What is Digital Forensics?

Digital Forensics is the scientific process of:

- Identifying
- Preserving
- Analyzing
- Presenting

Why Digital Forensics is Important?

1. Investigate cyber crimes
2. Incident response
3. Insider threat detection
4. Data breach investigation
5. Legal dispute resolution

DIGITAL FORENSICS

Digital forensics involves the identification, preservation, collection, analysis, and presentation of digital evidence in a legally admissible manner.

❑ Core Components:

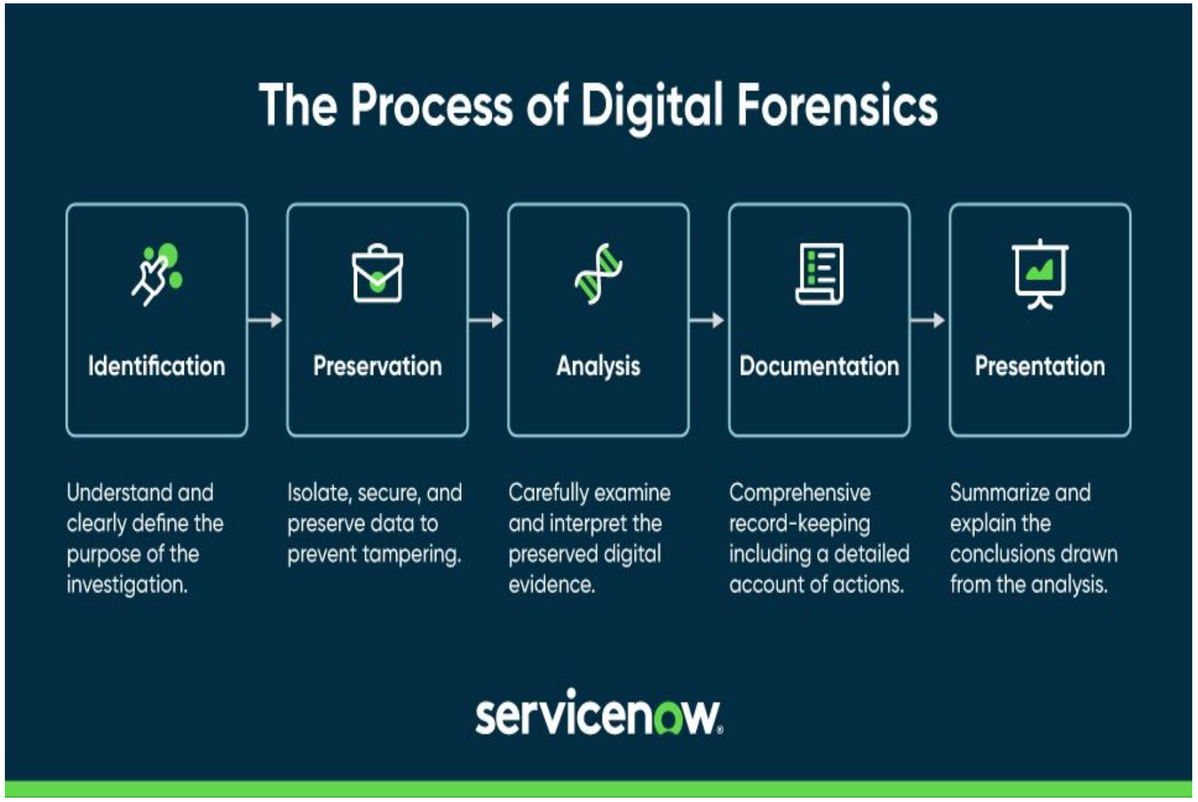
- **Scientific Process:** Methodical approach to evidence handling
- **Legal Framework:** Adherence to rules of evidence
- **Technical Expertise:** Understanding digital systems and data
- **Documentation:** Comprehensive recording of all actions
- **Purpose:** To investigate digital incidents while maintaining evidence integrity for legal proceedings.

Objectives of Digital Forensics

Below are a few objectives of using digital forensics:

- **Evidence to Court:** It recovers, analyzes, and preserves digital and forensic evidence to help the department's investigation to present the evidence in court.
- **Identifying the Culprit:** It aims to cause the attacks and identify the main culprit behind the crimes.
- **Legal Procedures:** To ensure the evidence found at a suspicious crime scene is uncorrupted, we design the methods for collecting and preserving the evidence.
- **Data Redundancy:** Recover the deleted files and subdivide them from digital media to validate them.
- It also encourages you to find the evidence instantly and makes you identify the impact of the culprit on the crime or the attacks.
- Storing the evidence or the proofs by the procedures in the way of legal custody in the court of law.

Process of Digital Forensics



Primary Domains

- **Computer Forensics:** Desktops, laptops, servers
- **Network Forensics:** Traffic analysis, intrusion detection
- **Mobile Forensics:** Smartphones, tablets, GPS devices
- **Database Forensics:** Data manipulation investigation
- **Cloud Forensics:** Virtualized environments and services

Common Applications:

- Criminal investigations
- Corporate security incidents
- Civil litigation support
- Cybersecurity breach response
- Internal policy violation investigations

Types of Digital Forensics

There are a few types of digital forensics that include below:

- **Disk Forensics:** It will deal with deriving the evidence from digital storage media like USB Devices, DVDs, CDs, etc., by gathering the active files or modifying or deleting them.
- **Network Forensics:** It is generally a sub-part of digital forensics relating to the monitoring and detecting system network traffic to extract crucial data for all legal evidence to present at the court.
- **Wireless Forensics:** It is a part of the networking forensics type that aims for wireless forensics to allow the tools needed to gather and extract evidence from networking wireless traffic.
- **Database Forensics:** This type of digital forensics relates to the forensic study and collection of databases and their relevant metadata. It follows investigating techniques to query the database to collect the evidence.
- **Malware Forensics:** This branch of forensics handles identifying malicious code and studying malware issues related to their workload, trojans, viruses, etc.
- **Email Forensics:** This forensic branch handles the recovery of the trashed data and analyses the contents of the emails, including the emails that are deleted or the calendar or the contacts in the email.
- **Memory Forensics:** A forensic analysis collects the data from the computer's cache memory or RAM dump and then gathers the evidence.

Digital Crimes Requiring Forensics:

- **Cybercrime:** Hacking, DDoS attacks, malware distribution
- **Financial Crimes:** Online fraud, identity theft, cryptocurrency scams
- **Intellectual Property Theft:** Trade secret theft, copyright infringement
- **Cyberstalking/Harassment:** Online threats, bullying, extortion
- **Child Exploitation:** Distribution of illegal materials
- **Corporate Espionage:** Data theft from competitors
- **Insider Threats:** Employee data theft or sabotage

FORENSIC MODELING

Common Forensic Process Models:

❖ Digital Forensic Research Workshop (DFRWS) Model:

- Identification → Preservation → Collection → Examination → Analysis → Presentation → Decision

❖ NIST SP 800-86 Model:

- Collection → Examination → Analysis → Reporting

❖ Abstract Digital Forensics Model (ADFM):

- Preparation → Collection → Preservation → Examination → Analysis → Presentation → Dissemination

❖ Integrated Digital Investigation Process (IDIP):

- Readiness → Deployment → Physical Crime Scene → Digital Crime Scene → Review

Introduction

02 Types of Digital Forensics

Computer Forensics

Involves extracting and analyzing data from non-volatile storage, such as desktops, laptops, and hard drives, to recover deleted files, system logs, and user activity, often used to trace data theft or unauthorized access.

01

Network Forensics

Focuses on monitoring and analyzing network traffic to identify, track, or intercept unauthorized access, intrusions (e.g., DDoS attacks), or data exfiltration.

02

Mobile Forensics

Specializes in retrieving data from mobile devices like smartphones, tablets, and wearable devices, including SMS messages, call logs, location data (GPS), and app usage.

03

Cloud Forensics

Involves the investigation of data within cloud environments (SaaS, IaaS, PaaS), including virtual machines, AWS, Azure, and GCP, focusing on API activities and access logs.

04

Memory Forensics

Analyzes volatile data in a system's RAM, such as encryption keys, running processes, and network connections, often crucial for finding evidence that disappears when the machine shuts down.

05

Branches of Digital Forensics

- The technical aspect of an investigation is divided in several sub-branches, relating to the type of digital devices involved:
  - ✓ ***Computer forensics***, ***Firewall Forensics***, ***Database Forensics***, ***Network forensics***, ***Forensic data analysis*** and ***Mobile device forensics***.

- The typical forensic process encompasses **the seizure**, **forensic imaging** and **analysis of digital media** and the **production of a report** into collected evidence.

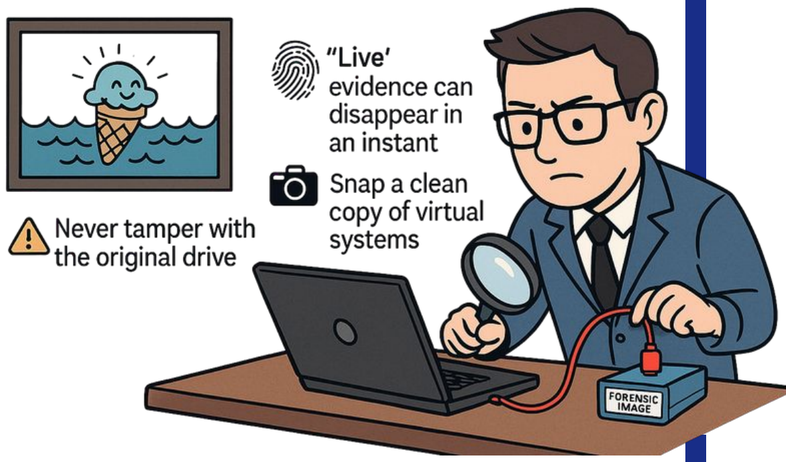
Digital Forensic Devices

Digital Forensic Core

- ***Digital evidence***

✓ Any data that is **recorded** or **preserved** on any medium in or by a **computer system** or other **similar digital device**, that can be **read or understood** by a person or a computer system or other similar device.

✓ It includes a **display**, **printout** or **other output** of that data.



- An evidence must be:
  - ➢ **Admissible**
    - ✓ Conformity with the common law and legislative rules
  - ➢ **Authentic**
    - ✓ In linking data to specific individuals and events
  - ➢ **Fragile**
    - ✓ Easily altered, damaged, or destroyed
  - ➢ **Accurate**
    - ✓ Believed and is consistent
  - ➢ **Complete**
    - ✓ With a full story of particular circumstances.

Forensics Basics & Cyber Criminalities

01 Forensic Basics

1 DIGITAL EVIDENCE

- Emails
- Log files
- Browser history
- Deleted files
- Metadata

Any data stored or transmitted in digital form

2 CHARACTERITICS OF DIGITAL EVIDENCE

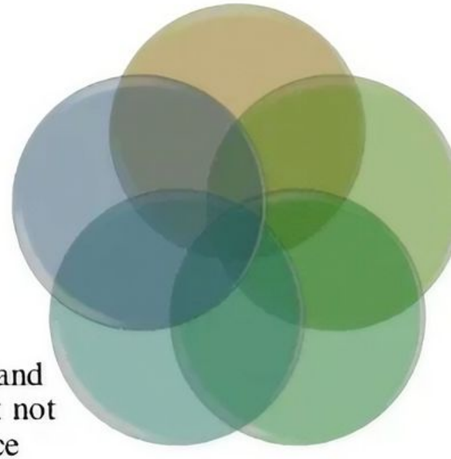
- Easily altred
- Volatile (RAM)
- Requires integrity verification (Hashing – MD5/SHA)

MD5/SHA

- Must maintain Chain of Chain of Custody

Admissible :- It is the most basic rule. The evidence must be able to be used in court.

Believable:-It should be clearly understandable and believable to a jury.



Reliable :- Collection and analysis procedure must not cast doubt on evidence authenticity.

Authentic :- Evidence must relates to the incident in a relevant way.

Complete :- Its not enough to collect evidence that just shoes one perspective of the incident.

Example of Digital Evidence

Many court have allowed theuse of:-

- ✓ e-mails,
- ✓ digital photographs,
- ✓ ATM transaction logs,
- ✓ word processing documents,
- ✓ Instant message histories,
- ✓ files saved from accounting program,
- ✓ spreadsheets,
- ✓ internet browser histories,
- ✓ databases,
- ✓ the contents of computer memory,
- ✓ computer backups, computer printouts,
- ✓ Global Positioning System tracks,
- ✓ logs from a hotel's electronic door locks, and
- ✓ digital video or audio files

Types Of Digital Evidence

- ***Persistant data***

✓ Meaning data that **remains intact** when the digital device is turned off. E.g. hard drives, disk drives and removable storage devices (such as USB drives or flash drives).

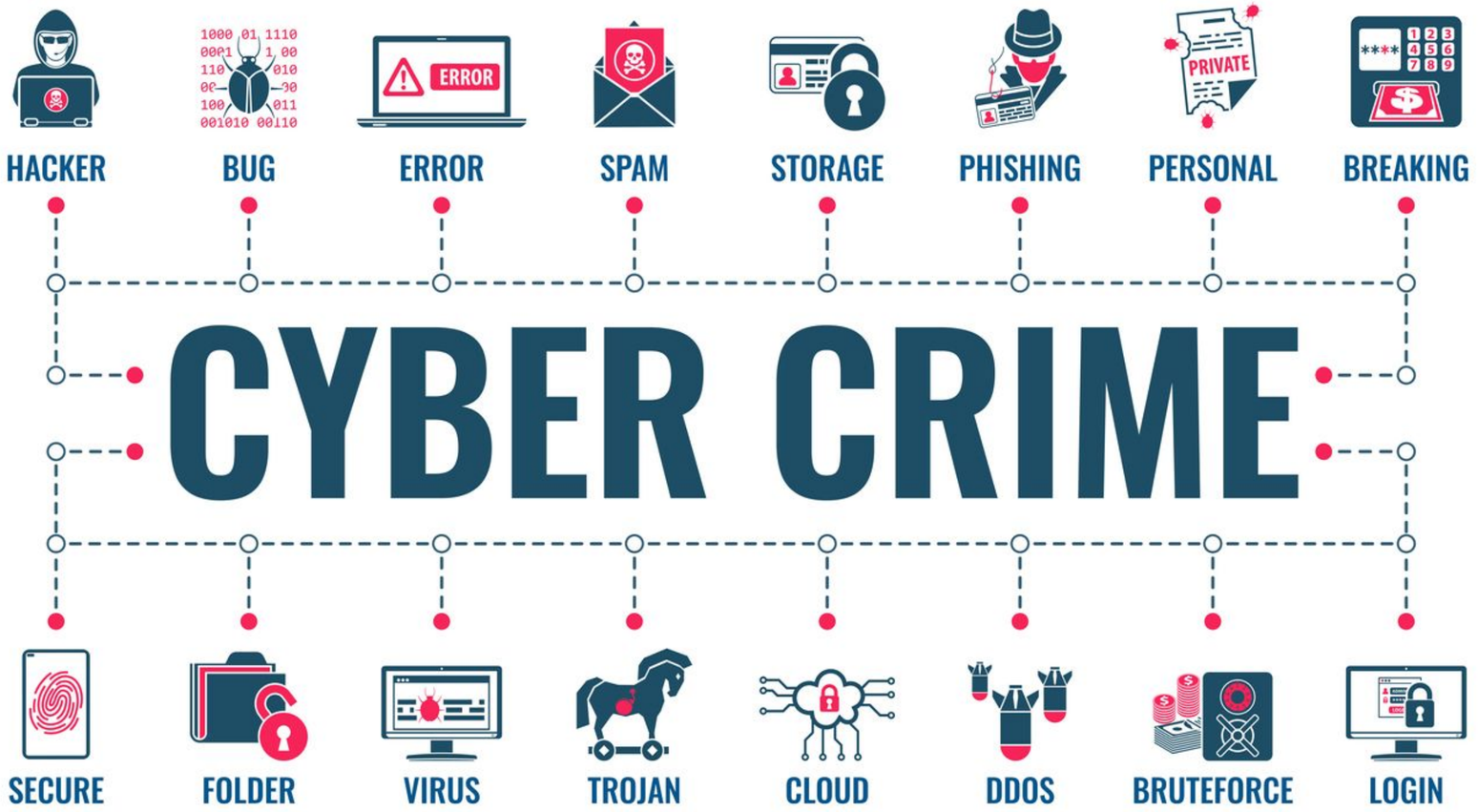
- ***Volatile data***

✓ Which is data that **would be lost** if the digital device is turned off. E.g. deleted files, computer history, the computers registry, temporary files and web browsing history.

Forensics Basics & Cyber Criminalities

02 Common Cyber Criminalities

1. HACKING
2. PHISHING ATTACKS
3. IDENTITY THEFT
4. FINANCIAL FRAUD
5. MALWARE & RANSOMWARE
6. DATA EXFILTRATION
7. INSIDER ATTACKS



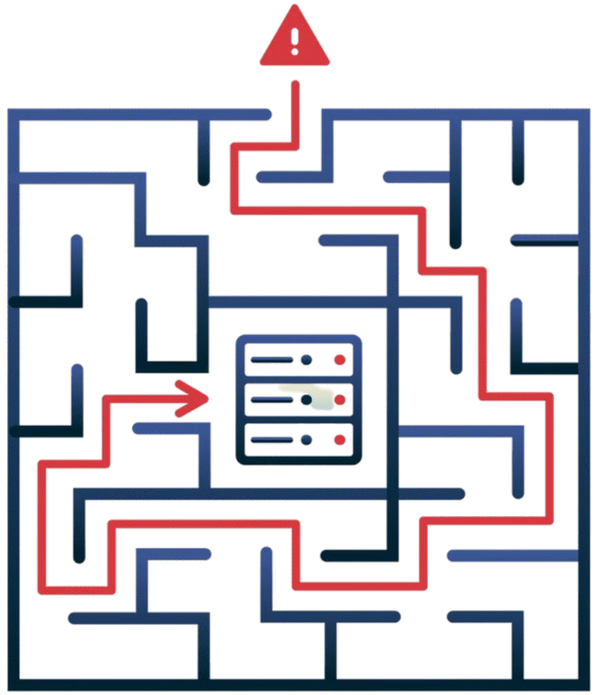
03 Investigation Objective

Identify Attacker: Trace source IPs and analyze TTPs (Tactics, Techniques, and Procedures) to profile the actor.

Determine Vector: Pinpoint the entry point likely phishing, unpatched software/compromised credentials.

Measure Impact: Assess data loss (exfiltration), system downtime, and the cost of remediation.

Legal Proof: Maintain a strict Chain of Custody and use forensic imaging (bit-for-bit copies) to ensure evidence is admissible.



Digital Forensic Process

- Broad process steps:

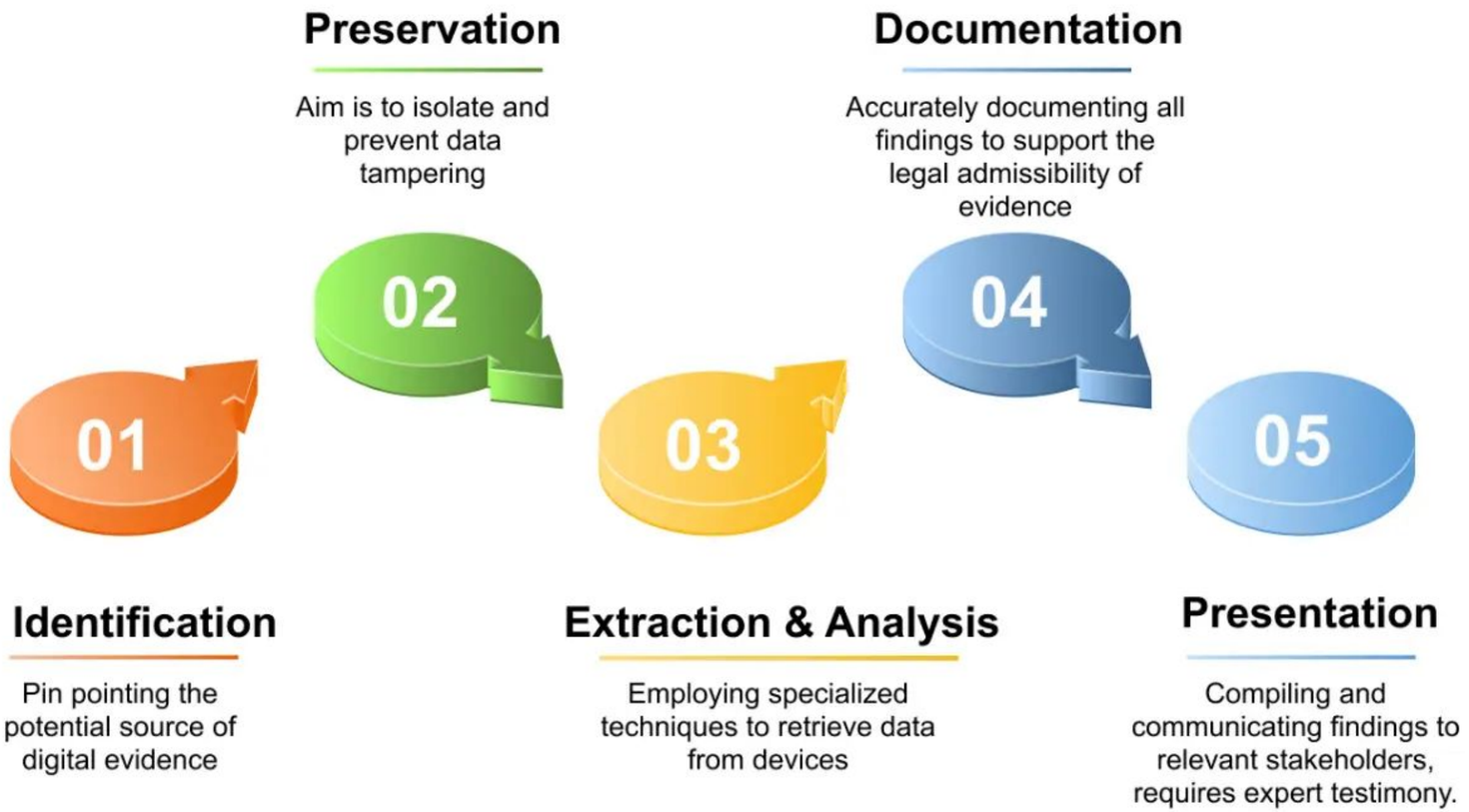
✓Identification

✓Preservation

✓Analysis

✓Documentation

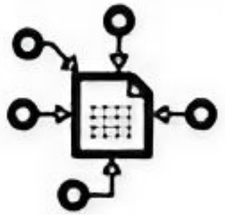
✓Presentation



Digital Forensic Process

Identification

- The first step in the forensic process:
  - What evidence is present
  - Where it is stored and
  - How it is stored
- Electronic stores can be:
  - Person computers
  - Mobile phones
  - PDAs
  - Smart cards



Presentation

- **Summarize** and **provide explanation** of conclusions.
  - ✓ This should be written in a **layperson's terms** using **abstracted terminologies**.
  - ✓ All abstracted terminologies **should reference** the specific details.

Preservation

- ✓ Isolate, secure and preserve the **state of physical** and **digital** evidence.
- ✓ This includes **preventing** people from using the digital device or **allowing other electromagnetic** devices to be used within an affected radius.

Analysis

- ✓ Determine **significance**, **reconstruct fragments of data** and **draw conclusions** based on evidence found.
- ✓ It may take **several iterations of examination** and **analysis** to support a crime theory.

Documentation

- ✓ A record of **all visible data must be created**, which helps in **recreating** the scene and **reviewing** it any time
- ✓ Involves **proper documentation of the crime** scene along with **photographing**, **sketching** and **crime-scene mapping**.

Forensic Modeling & Principles

01 Digital Forensic Investigation Model

Identification

Locate potential digital evidence.

Preservation

- Create forensic image
- Use write blockers
- Hash verification

Collection

Secure acquisition of digital data.

Examination

Recover hidden/deleted data.

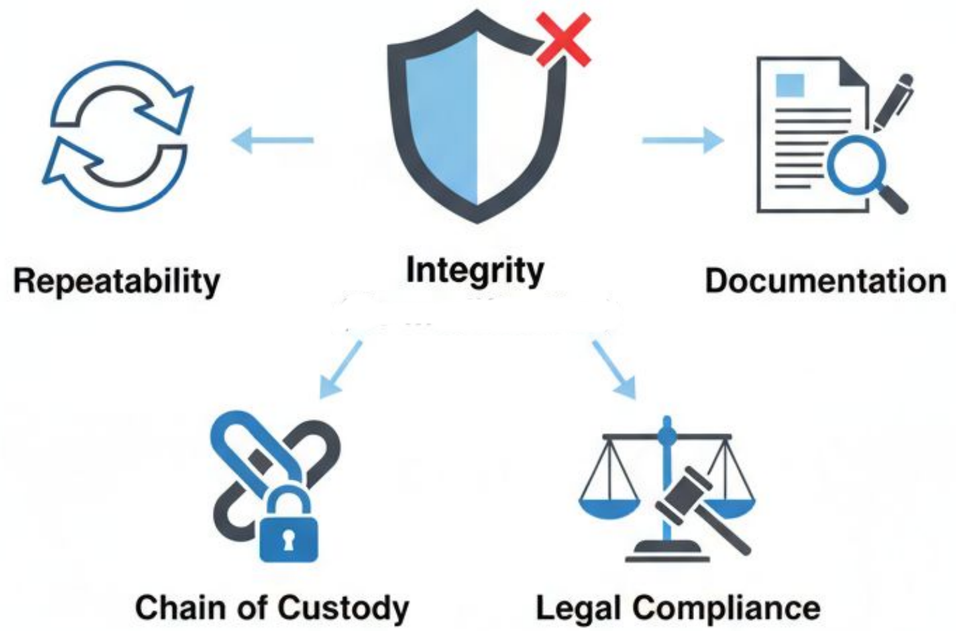
Correlate events & timeline reconstruction.

Presentation

Prepare technical & legal report.

Forensic Modeling & Principles

02 Core Forensic Principles



Integrity

Evidence must remain unaltered. Investigators use hash values (digital fingerprints) and write-blockers to prove the data hasn't changed.

Repeatability

Different examiners using the same tools on the same data must reach the same results.

Documentation

A meticulous "paper trail" of every action, tool, and command used during the investigation.

Chain of Custody

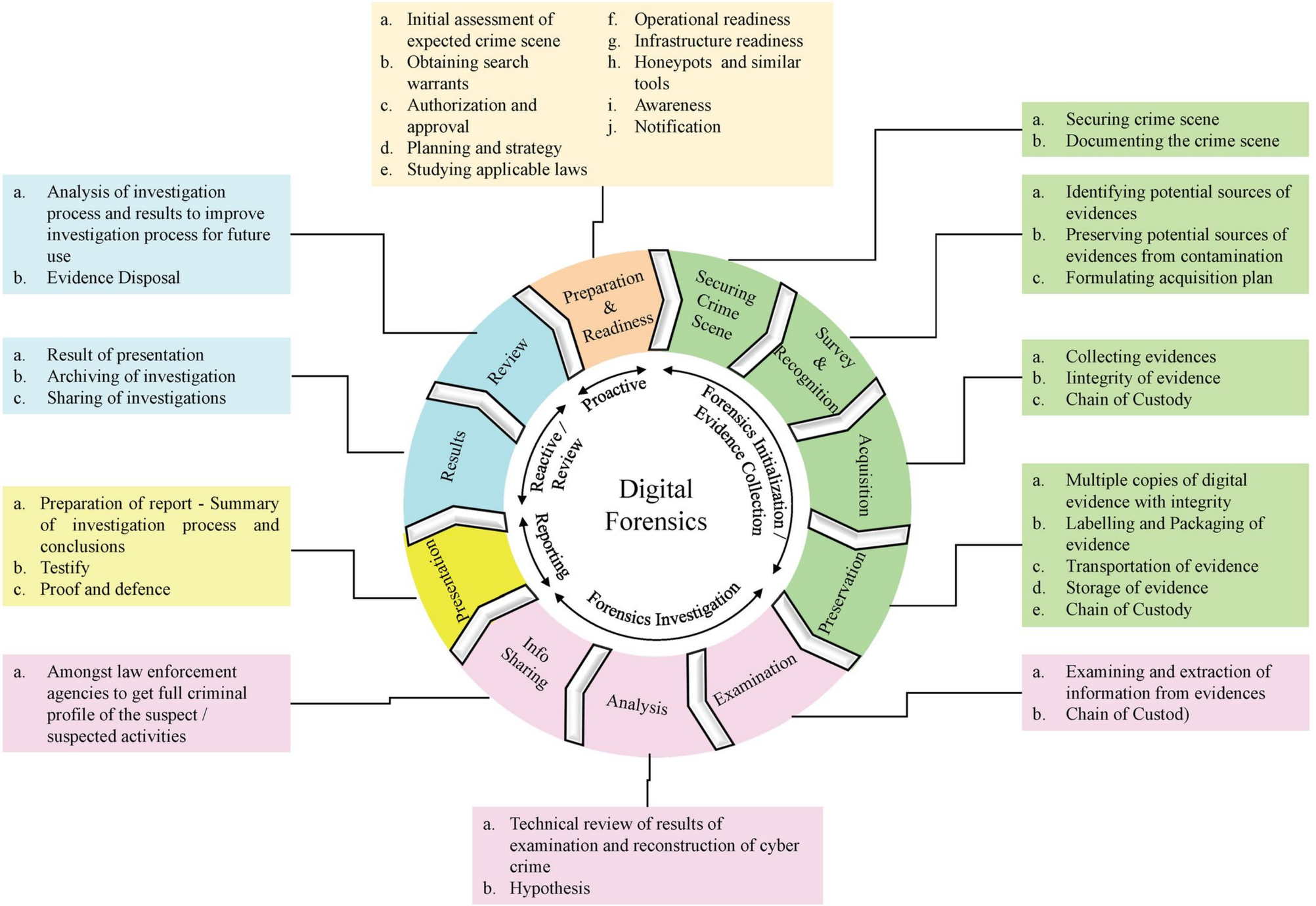
A chronological log of who handled the evidence, when, and why. Any gap can disqualify the evidence.

Legal Compliance

All actions must follow the law (warrants, privacy rights) to ensure findings are admissible in court.

Need for Digital Forensics

- ✓To ensure the integrity of digital system.
- ✓To focus on the response to hi-tech offenses, started to intervene the system.
- ✓Digital forensics has been efficiently used to track down the terrorists from the various parts of the world.
- ✓To produce evidence in the court that can lead to the punishment of the criminal.


a. Initial assessment of expected crime scene
b. Obtaining search warrants
c. Authorization and approval
d. Planning and strategy
e. Studying applicable laws
f. Operational readiness
g. Infrastructure readiness
h. Honeypots and similar tools
i. Awareness
j. Notification
a. Securing crime scene
b. Documenting the crime scene
a. Identifying potential sources of evidences
b. Preserving potential sources of evidences from contamination
c. Formulating acquisition plan
a. Collecting evidences
b. Iintegrity of evidence
c. Chain of Custody
a. Multiple copies of digital evidence with integrity
b. Labelling and Packaging of evidence
c. Transportation of evidence
d. Storage of evidence
e. Chain of Custody
a. Examining and extraction of information from evidences
b. Chain of Custod)
a. Technical review of results of examination and reconstruction of cyber crime
b. Hypothesis
a. Amongst law enforcement agencies to get full criminal profile of the suspect / suspected activities
a. Preparation of report - Summary of investigation process and conclusions
b. Testify
c. Proof and defence
a. Result of presentation
b. Archiving of investigation
c. Sharing of investigations
a. Analysis of investigation process and results to improve investigation process for future use
b. Evidence Disposal
Preparation & Readiness
Securing Crime Scene
Survey & Recognition
Acquisition
Preservation
Examination
Analysis
Info Sharing
Presentation
Results
Review
Proactive
Forensics Initialization / Evidence Collection
Forensics Investigation
Reporting
Reactive / Review
Digital Forensics

COMPUTER FORENSICS

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from computing devices in a way suitable for presentation in a court of law.

- **Computer forensics**
  - Involves obtaining and analyzing digital information
    - As evidence in civil, criminal, or administrative cases
- FBI Computer Analysis and Response Team (CART)
  - Formed in 1984 to handle the increasing number of cases involving digital evidence
- Network forensics
  - Yields information about how a perpetrator or an attacker gained access to a network
- **Data recovery**
  - Recovering information that was deleted by mistake
    - Or lost during a power surge or server crash
  - Typically you know what you're looking for
- **Disaster recovery**
  - Uses computer forensics techniques to retrieve information their clients have lost
- Investigators often work as a team to make computers and networks secure in an organization

Computer Forensics Versus Other Related Disciplines

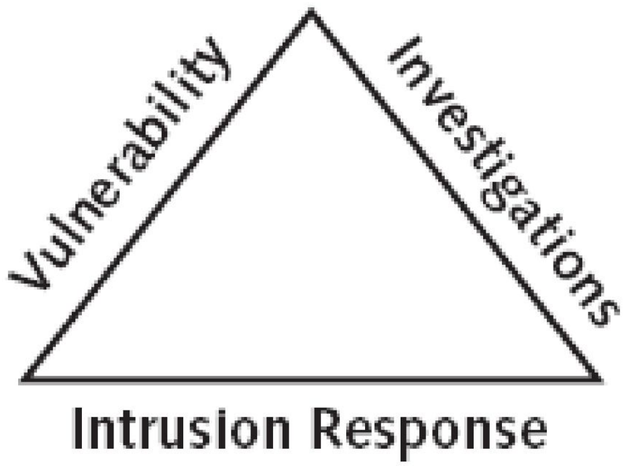


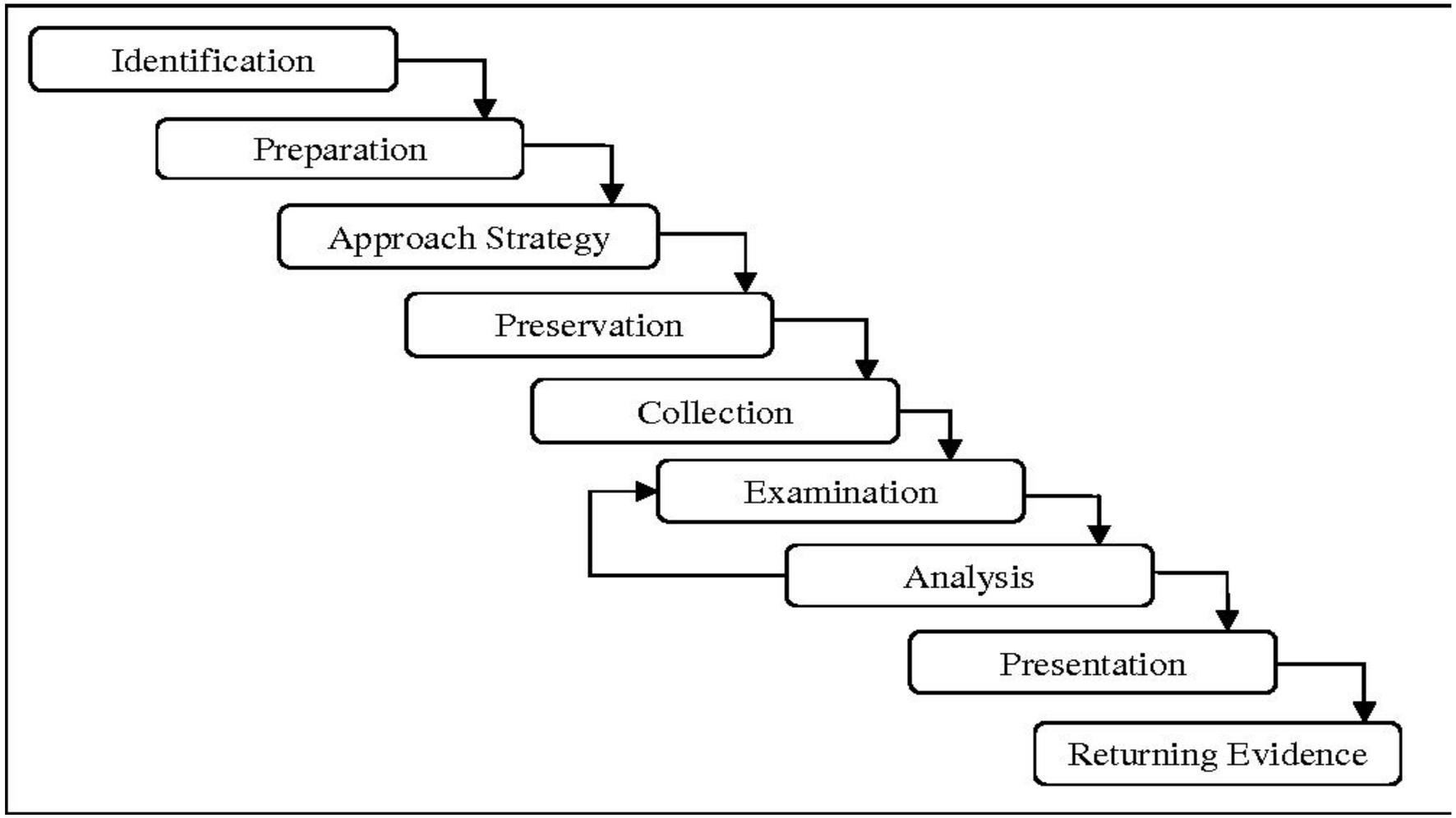
Figure 1-2 The investigations triad

COMPUTER FORENSICS

Key Focus Areas:

- Operating system artifacts
- File system analysis
- Data recovery and reconstruction
- Timeline analysis
- Application-specific evidence

COMPUTER FORENSICS INVESTIGATION PROCESS



Computer Forensics & Investigations

What is Computer Forensics?

01

Branch of digital forensics focusing on:

- Hard drives
- SSDs
- File systems
- OS artifacts
- Logs
- Registry entries

02

Common Investigation Areas

- Deleted file recovery
- Browser artifact analysis
- Email tracing
- USB device tracking
- Log file analysis
- Timeline reconstruction

03

Popular Forensic Tools

- Autopsy
- FTK (Forensic Toolkit)
- EnCase
- Volatility (Memory Forensics)
- Wireshark (Network)

3/4 Phase of Digital Forensics

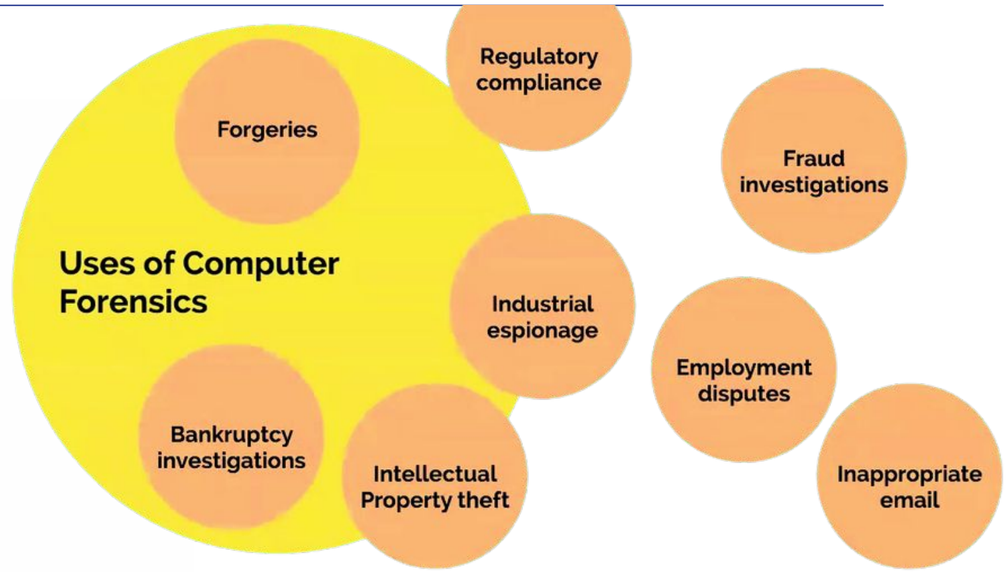
4/4 Applications of Digital Forensics

- Financial Fraud Detection

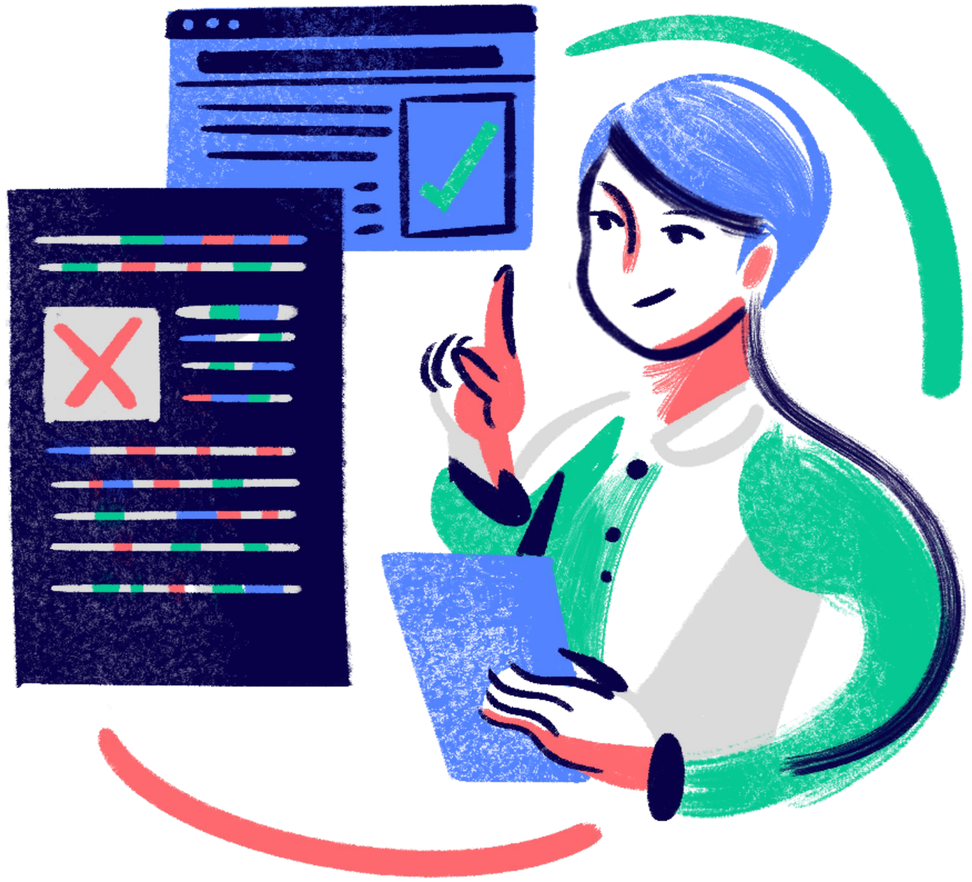
- Criminal Prosecution
✓ Child pornography (Michael Jackson case)

- Civil Litigation (evidence in court cases and proceedings)
✓ Perjury (false swearing) (Clinton - Lewinsky case)

- Corporate Security Policy and Acceptable Use Violations
✓ Embezzlement (Misuse, fraud, cheating etc.)
✓ Email threats data theft-industrial espionage (spying, intelligence units)



Skills Required to Become a Digital Forensic Investigator



Employers look for certified forenstic investigators with key digital forenstic skills, including: are as follows:

- Defeating anti-foressic techniques
- Understanding hard disks and file systems
- Operating system forensics
- Cloud forestic in a cloud environment
- Investtating email crimes
- Mobile device forensics

3/3 Conclusion

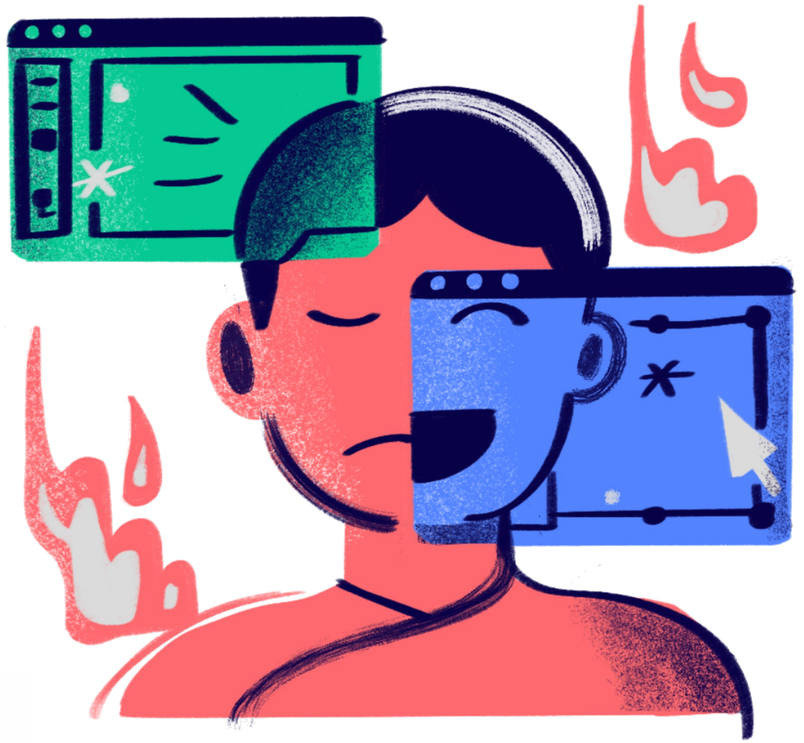
- Digital forensics is important for solving crimes
  - ✓ **with** digital devices
  - ✓ **against** digitial devices
  - ✓ **against people** where **evidence may reside** in a device
- Several **sound tools** and **techniques** exist to **search** and **analyse** digital data
- Regardless of existing tools, evolving digital age and development of technology ***requires heavier research*** in digital forensics

1/2 Challenges

- The **increase of PC's** and **internet access** has made **exchange of information quick** and **inexpensive**.

✓Easy availability of Hacking Tools.

✓Lack of physical evidence makes crimes harder to prosecute.



- The **large amount of storage** space available **to suspects**

✓The rapid technological changes requires constant upgrade or changes to solutions

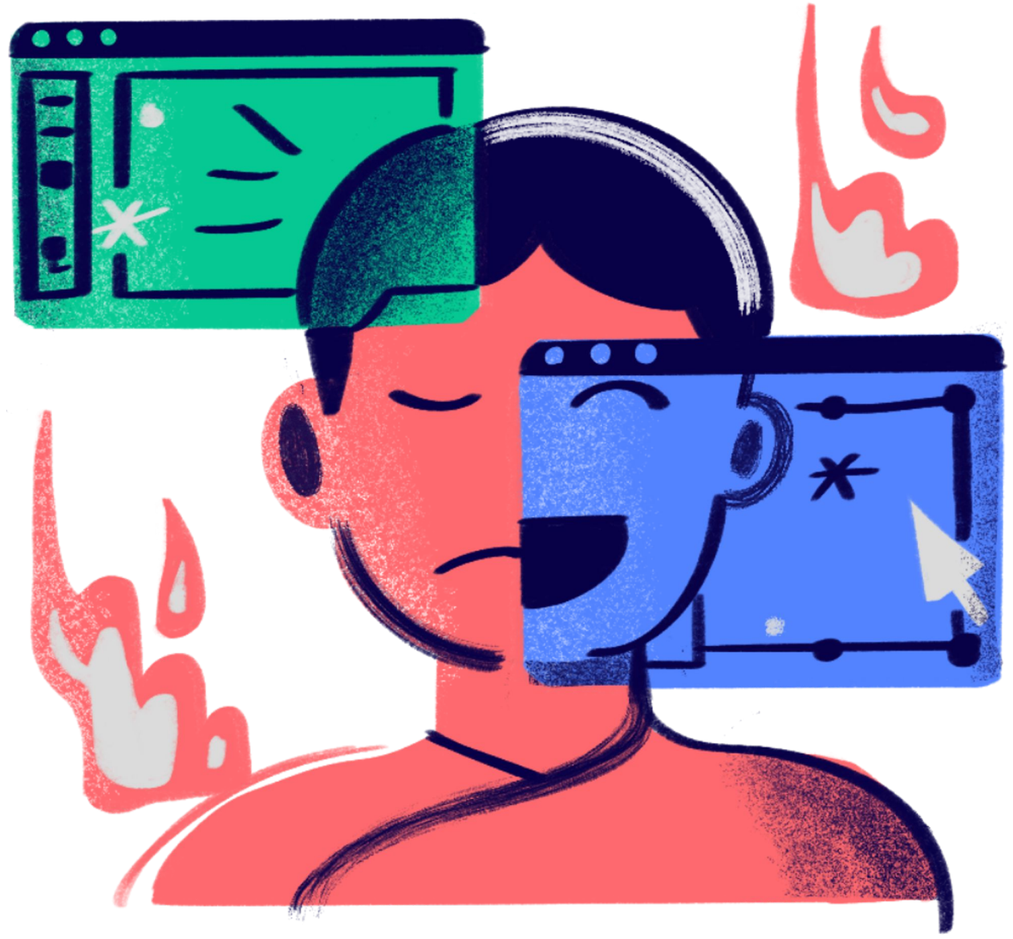
2/2 Challenges

Encryption

- **Challenge:** Ubiquitous hardware-backed encryption and End-to-End Encryption (E2EE) in apps like Signal make data unreadable without a passcode.
- **Result:** Investigators often cannot access devices even with a warrant, forcing a shift to "live" memory forensics to capture keys while a system is running

Anti-forensic techniques

- **Challenge**: Criminals use tools to actively erase traces, such as artifact wiping (permanently deleting logs) and steganography (hiding data inside harmless images).
- **Result:** Many modern attacks are "fileless," living only in RAM, meaning evidence vanishes the moment a device is powered off.



Cloud data jurisdiction, Large-scale data analysis, AI-generated cyber attacks etc.

Thank You!