ESOF 422:

Advanced Software Engineering: Cyber Practices

Introduction to Digital Forensics

Reese Pearsall

Spring 2025

Announcements

Digital Forensics

Digital Forensics is the collection, analysis, and interpretation of digital evidence

- Can help support or refute a theory of how an offense occurred or that critical address critical elements of the offense such as intent or an alibi
- Digital Evidence plays a crucial part in many modern-day investigations

In our scope of digital forensics, we are focusing on **incident response**.

→ System has been compromised, now must analyze, recover, and report on the threat

→ Crucial for understanding threats and hardening security

→ Import legal implications

Goals

When responding to an incident, we want to answer important questions such as

- When did the incident happen? What is the timeline?
- What is the root cause of the incident?
- Who attacked us?
- Why did they attack us?
- What is the scope of the damage?

Reflection

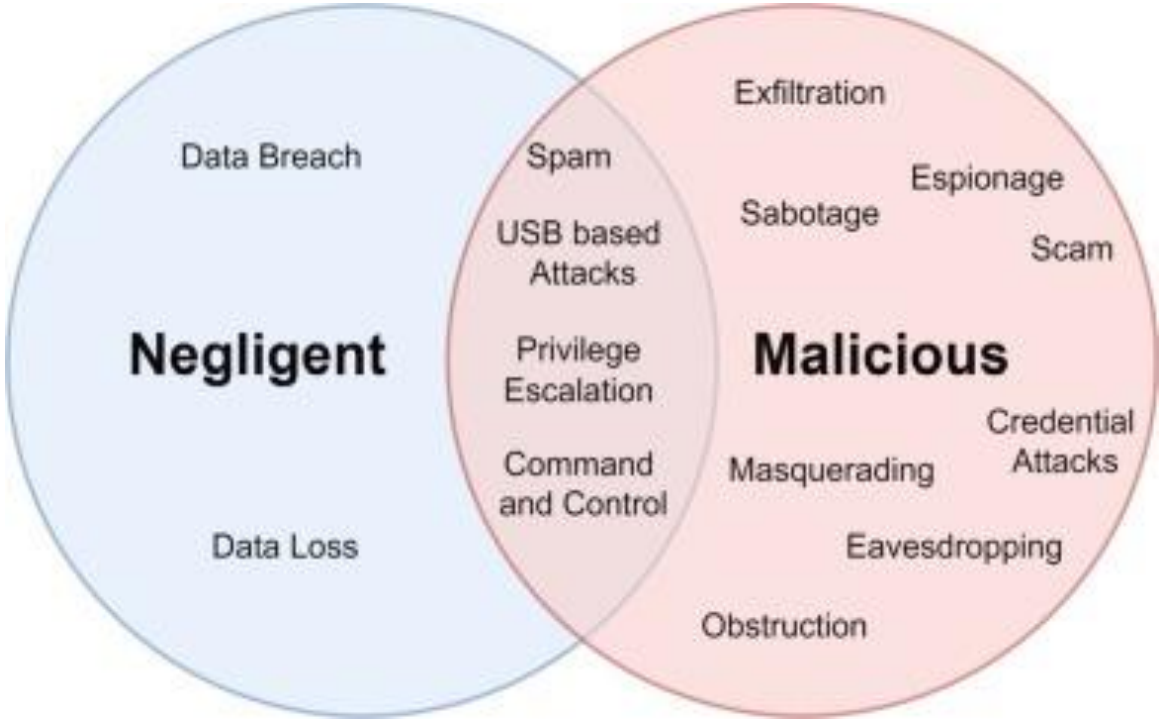
- Did staff and organizations perform as expected?
- What will our organization do next time?
- What corrective actions need to happen?

Important Difference

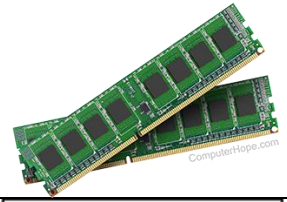
Cybersecurity	Digital Forensics
Prevents attacks, Securing devices, CIA	Investigates after an attack
Real-time response	Post-incident analysis
Proactive	Reactive
Building	Investigating and Analyzing

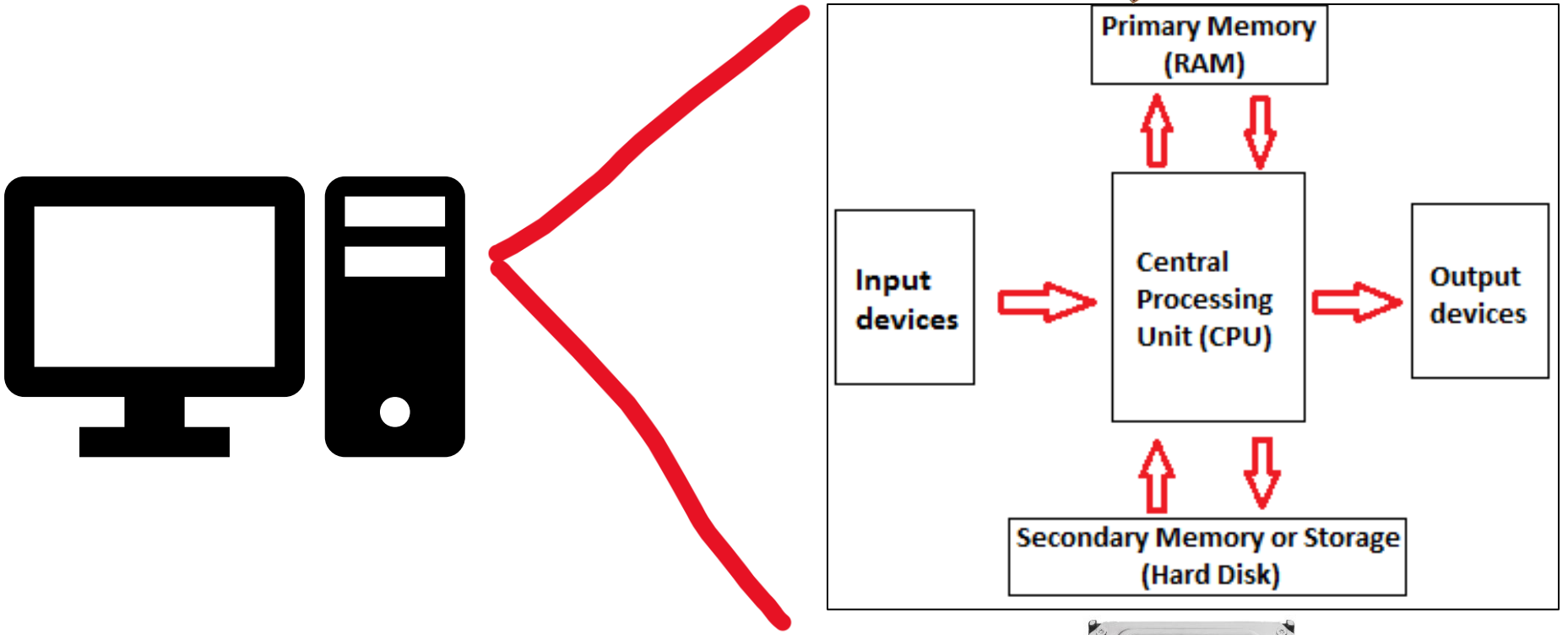
Common Use Cases

- Data Breaches
- Insider threats
- Malware infections
- Intellectual property theft
- Employee Misconduct

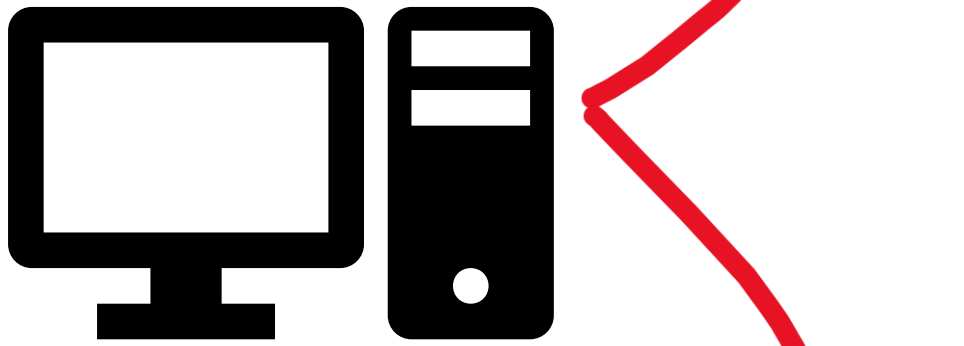


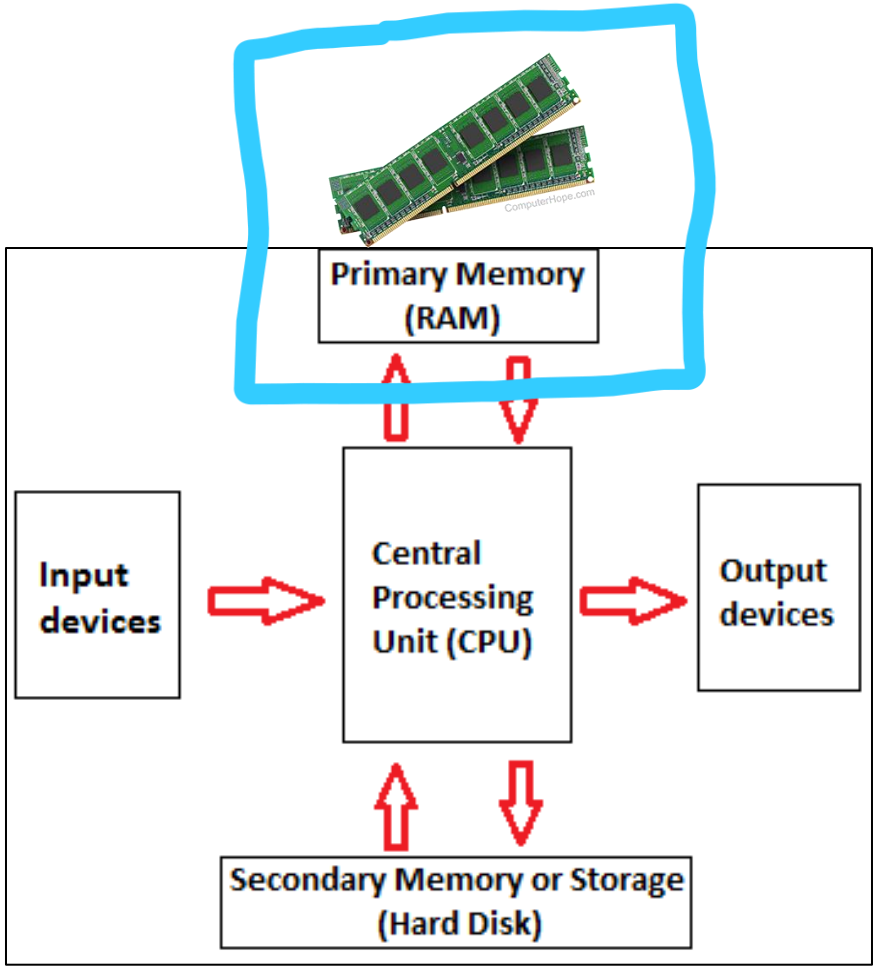
Types of Forensics





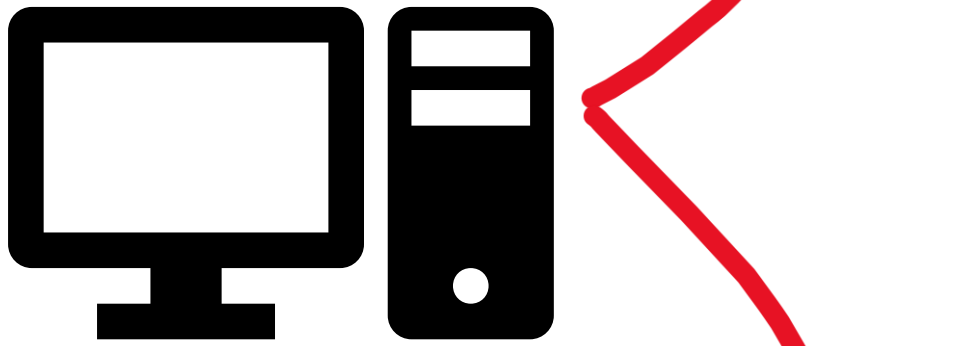
Types of Forensics

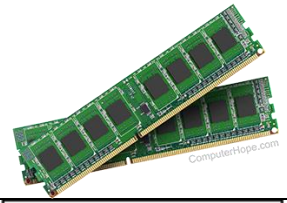


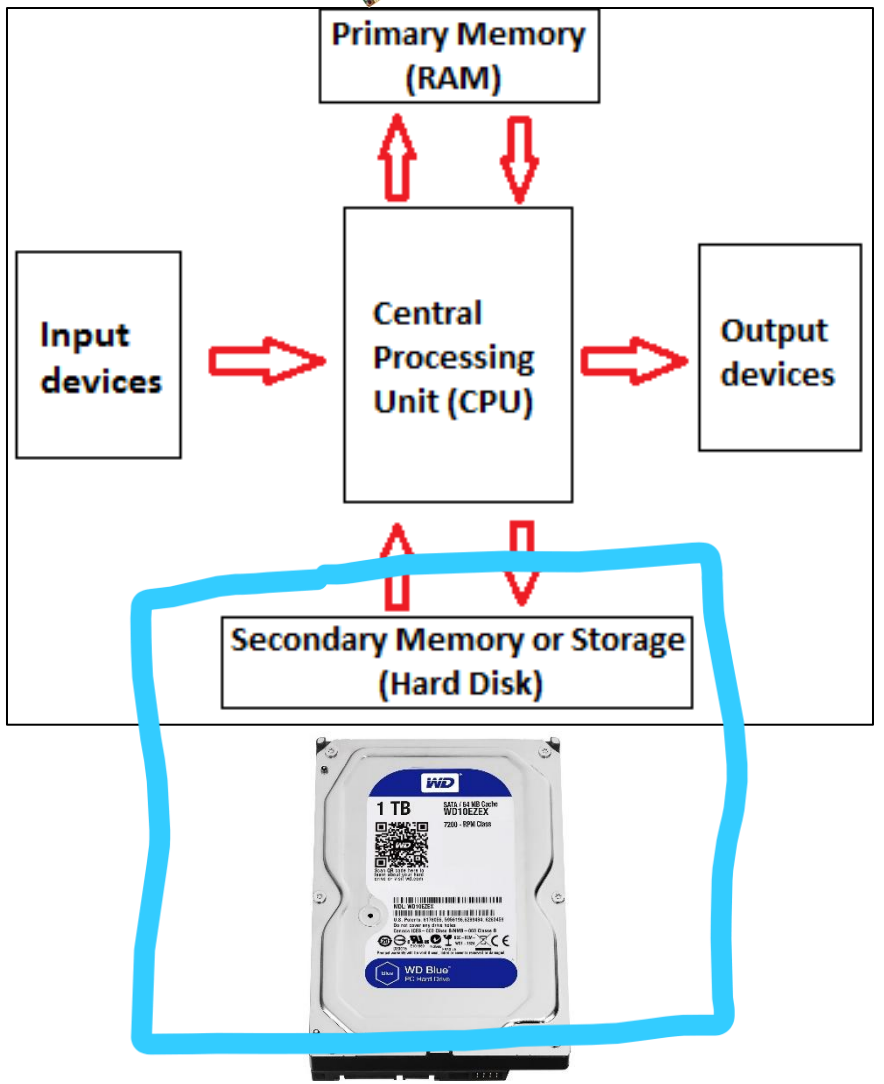


Memory forensics focuses on analyzing volatile data in RAM

Types of Forensics

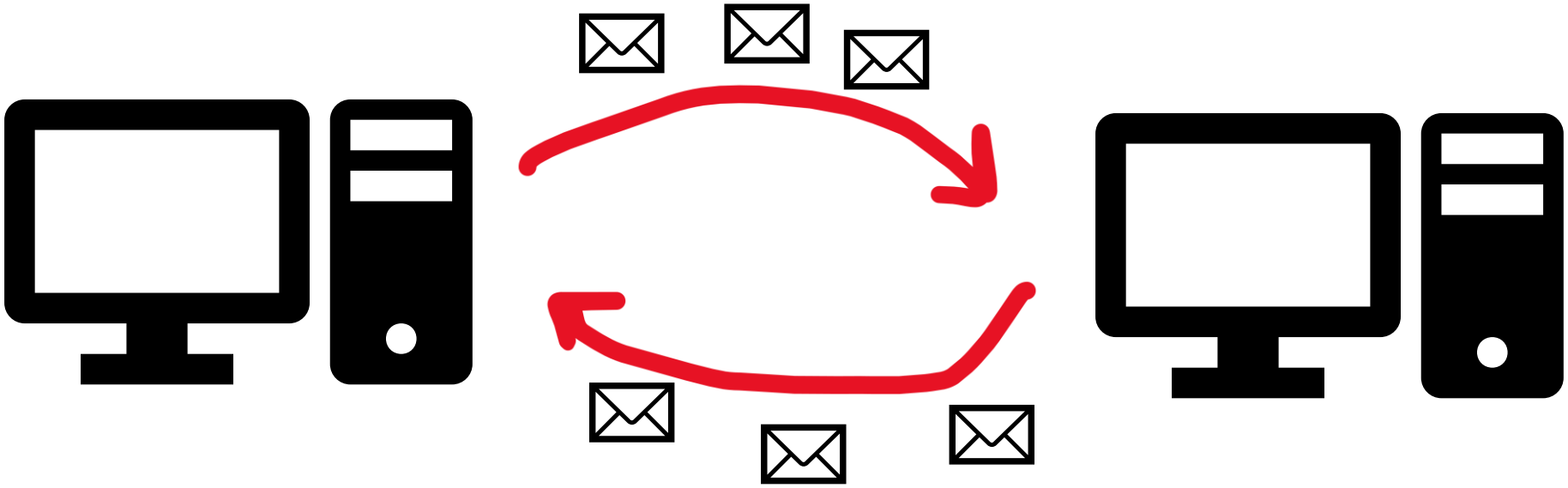






Disk forensics focuses on analyzing non-volatile data in persistent memory

Types of Forensics



Network forensics focuses on analyzing digital evidence from network traffic

Digital Evidence Processing

It is critical to follow appropriate processes and procedures when collecting and processing digital evidence

- Not following processes could put an investigator at legal risk
- Improperly collected or tracked evidence could be inadmissible in court

NIST 800-61r2 and **NIST IR 8387** provides guidelines and best practices for incident response and digital evidence preservation

Context

Context is critical

- Always important to understand the “why” of the case that you’re working on
- Timelines can be critical
- Will directly influence what data you collect, how you process it
- Technical vs. Corporate vs Legal vs Law Enforcement

Digital Evidence Collection

- Digital evidence is typically collected through software or hardware tools
- Hardware tools are used when the device is physically in the possession of the investigator and provide power and an interface to access on the target device
- Implicants of these choices on the principles of computer-based evidence exchange
- We collect **artifacts** on the system

Volatile Artifacts

- Does not persistent across power cycles
- RAM contents, fileless malware
- Faster

Non-volatile Artifacts

- Does persistent across power cycles
- Hard drive contents, malware
- Slower

Disk Capture (Non-volatile artifacts)

Creating a copy of the contents of a hard drive to a file for analysis

Must have a way to:

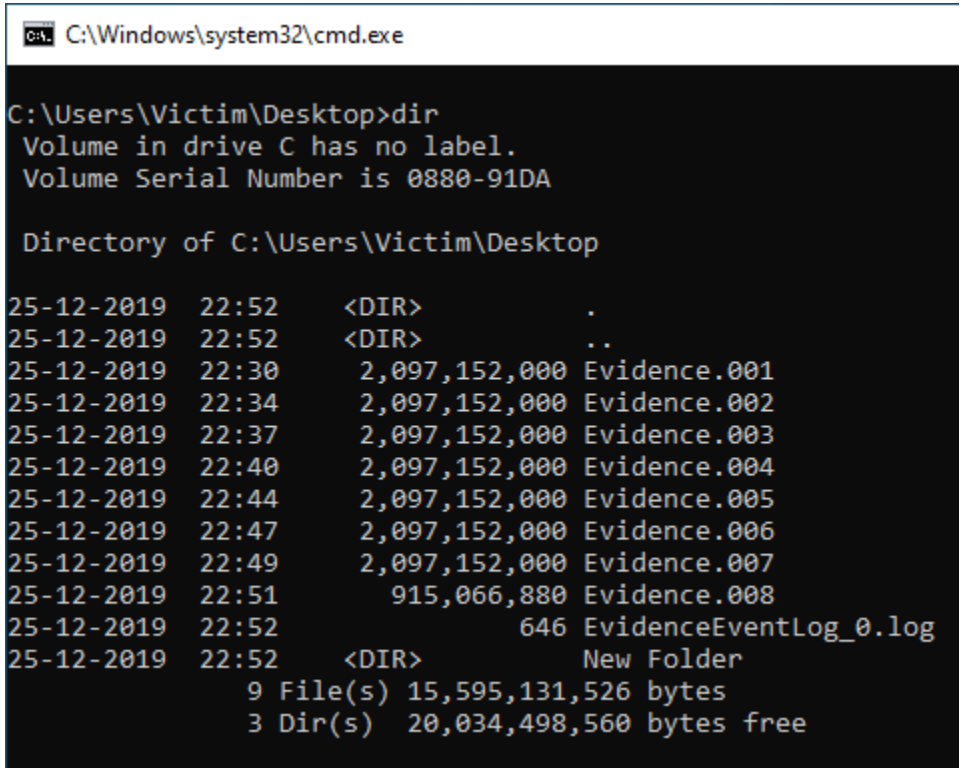
- Access data (physically and virtually)
- Power on the device

Pros:

- May get deleted files
- Will be able to parse the entire “raw” disk and data structures

Cons:

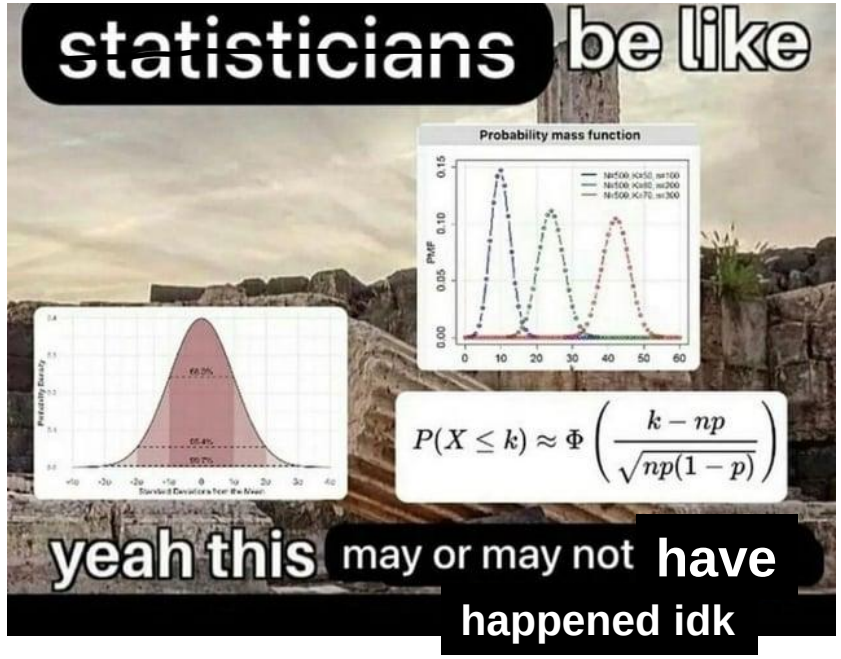
- Capture used and “unused” disk space
- Time consuming
- Very large output file



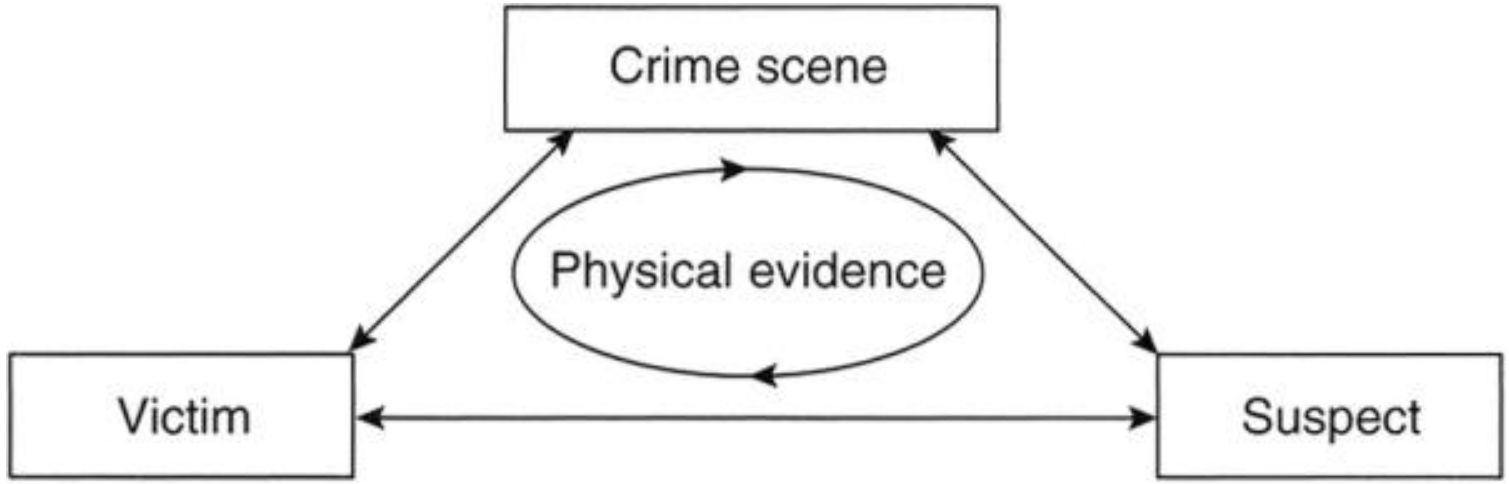
Certainty

- We're almost never "certain". This is a protected term that must be used with extreme care
- We cannot be certain of what occurred at a crime scene or other situation when we have only a limited amount of information
- We present possibilities and hypotheses and the evidence and information that support or refute these hypotheses

forensics



Locard's Exchange Principle: every contact leaves a trace



Anyone, or anything, entering a crime scene

- takes something of the scene with them
- leaves something of themselves behind when they leave.

1.Data Exchange: Every interaction with digital devices involves data exchange. Actions leave behind traces in the form of data packets, logs, or artefacts.

2.Digital Evidence: When a hacker gains unauthorized access to a system, they may leave behind login records, IP addresses, or malware signatures.

Authentication

- Integrity of data/records being analyzed
- Must be able to show:
  - → Contents of record are unchanged
  - → Information in record originates from purported source
  - → Extraneous information such as data of collection/record is accurate

Integrity

- Showing that evidence has not been modified since time of collection
- Use message digest (hash) functions to perform this work for us
- Hash functions always produce the same output for a given input
- SHA256/SHA512 is ideal

Soundness

- How the evidence was handled (preserved and examined)
- Consists of two key concepts
  - → Non-modification of evidence
  - → Documentation (tools, time, methods, hashes)

Chain of Custody

- Documentation that proves continuity of possession of evidence

Repeatability

- For a given piece of evidence, the process by which it is analyzed and information that analysis is repeatable
- Enables independent verification

Evidence Characteristics

-Class characteristics: similar between groups of items (ex. file formats, headers)
-Unique traits: can be tied to an individual (ex. MAC address, static IPs)

Disk Capture (Non-volatile artifacts)

Creating a copy of the contents of a hard drive to a file for analysis

Must have a way to:

- Access data (physically and virtually)
- Power on the device

A **write blocker** is a tool that permits *read-only* access to storage devices and copies hard disk contents

Read-only → evidence won't change. Maintains integrity of machine

USB 3.1 - PCIe SSD Write Blocker Kit

SKU: W2455

Description | Contents | Specs

The **Digital Intelligence USB 3.1 - PCIe write blocker kit** is used to create forensically sound images of PCIe connected NVMe M.2 and U.2 SSD storage drives. This imaging device is sold as a kit only and includes all components necessary to quickly and efficiently image M.2 and U.2 SSD's. Requires third party forensic imaging software for operation.

This device is user switchable from write blocked (read-only) to general purpose (read-write) for non-forensic applications. LEDs provide quick status during device operation.

Connects to host system computers using USB 3.1 technology for fast, convenient operation.

Kit includes quickstart guide for operational reference.

MSRP

$350.00

Capturing Volatile Evidence

- Volatile evidence is non-persistent when power is lost to the device
- Main component that affects us is any system with RAM
- RAM loses all contents when system is powered off

- Volatile evidence capture requires interacting with a running system
- Typically done remotely over SSH using RAM capture tools (software)
- Need to be careful to understand how you're capturing RAM
    - -You need administrative access
    - -You could be creating new files on disk
    - -You can trigger an antivirus

Communication