# Digital Forensics

CySER Workshop 2025

May 21, 2025

*Slides contribution from MSU ESOF 422*

# Outline

- What is Digital Forensics?
- Digital Evidence and Collection
- Analysis Tools
- Incident Response
- Capture the Flag

# What is Digital Forensics?

# What is forensics?

- “Application of science principles and methods to support legal decision-making in matters of criminal and civil law” – *Wikipedia*
- Collect evidence to support a legal case
- What is our criminal scene investigation method?


https://www.bbc.co.uk/programmes/m000s5xq

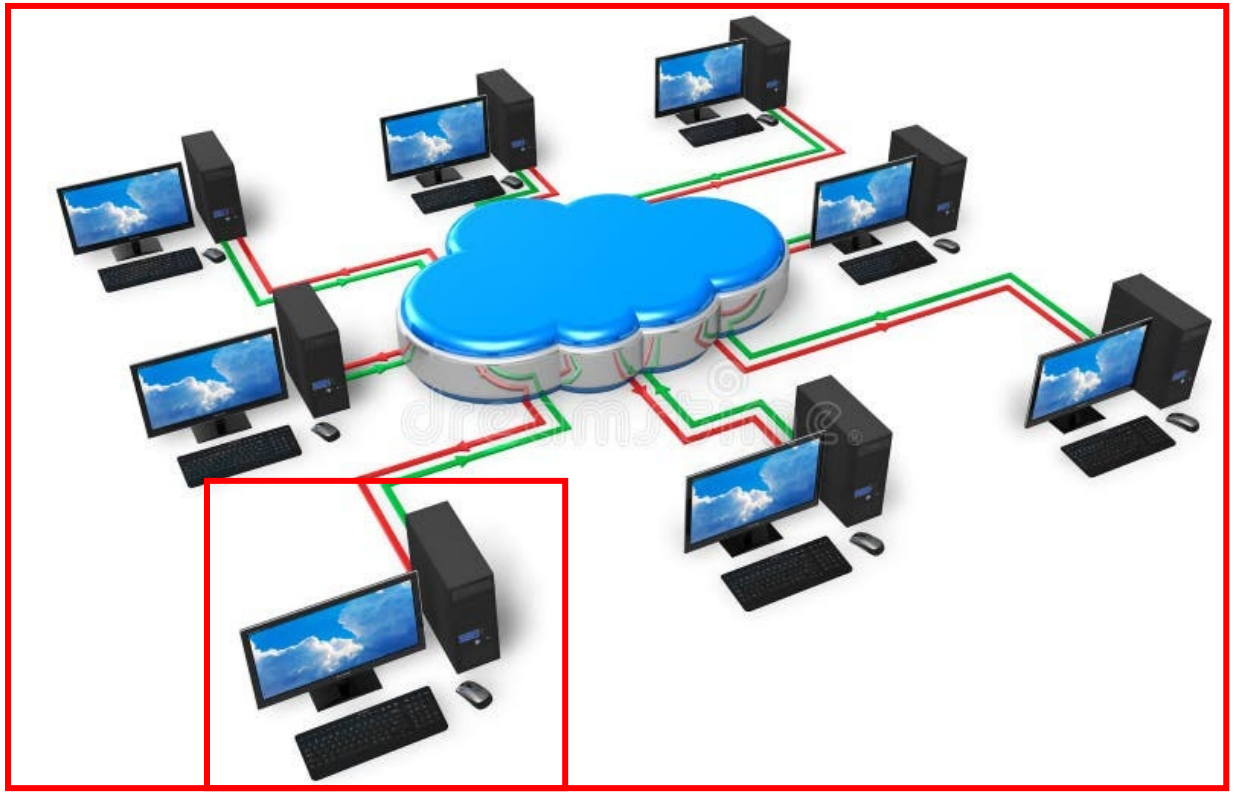
# What is digital forensics?

- Digital Evidence
  - Collect
  - Analyze
  - Interpret
- Real-time or post-attack
- Answer the who, what, when, where, why questions


Image from: https://tehleelmanzoor.medium.com/start-a-digital-forensics-career-with-no-it-experience-virtually-testing-foundation-14230f28576e

# Types of Digital Forensics

- Memory
- Disk
- Network
- Live



https://www.dreamstime.com/illustration/computer-networking-diagram.html

# Memory forensics

- Analysis of data sources from a running system's memory (RAM)
- RAM contains:
  - Programs/files that have been executed
  - Running processes
  - Information on what programs accessed what files
  - Location of open files on disk
  - Keyboard information
  - Opened web pages and network connections
  - Decrypted content
  - Content that is no longer or was never on disk

# Disk forensics

- Investigate magnetic and solid-state disks
- Typically used when you:
  - Cannot access the running state of the system
  - Investigating historical activity
- A file may never be deleted, even if you ‘delete’ it

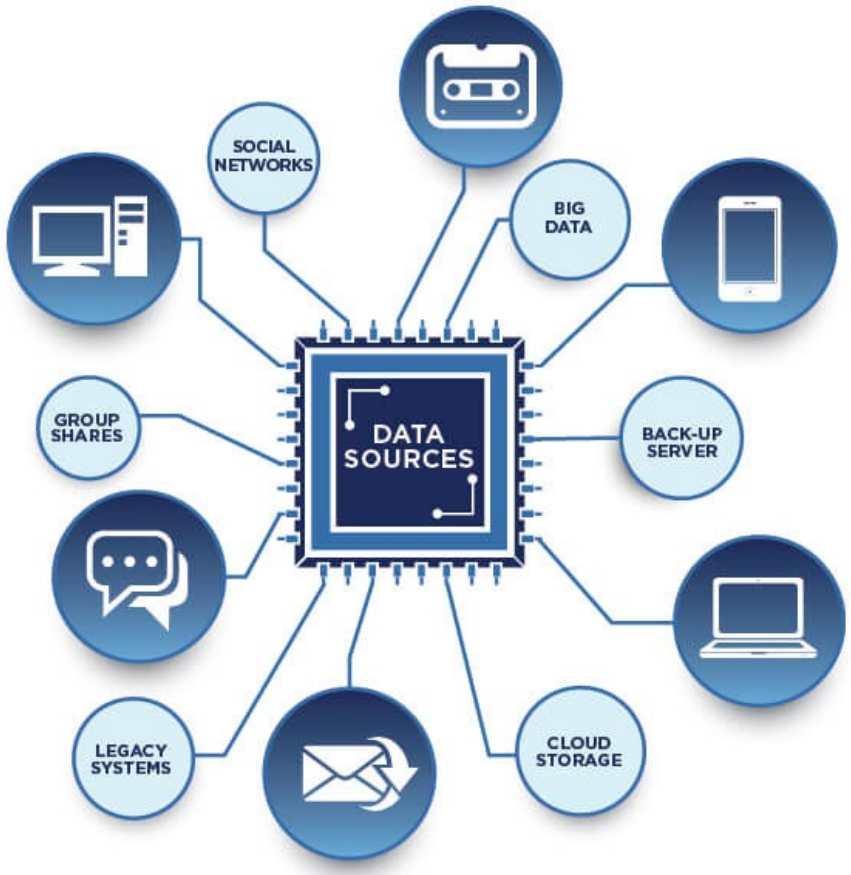
# Network and Live Forensics

- Network forensics
  - Captures and analyzes traffic between systems
  - Packet captures, firewall logs, etc.
- Live forensics
  - Analyze a system that is still running
  - RAM, active processes, volatile configurations, etc.

# Digital Evidence and Collection

# What is digital evidence?

- “Information and data of value to an investigation that is stored on, received, or transmitted by an electronic device” – *National Institute of Justice*
- Used to support or refute criminal offenses




https://hackforlab.com/digital-evidence-india/

# Types of Digital Data

- Open Computer Systems
  - Desktop computer
  - Laptop computer
- Embedded Computer Systems
  - Medical devices
  - Controllers in vehicles
  - Smart cards
  - Mobile device
- Network Systems
  - Internet
  - Wired and wireless telecom systems


Various sources; for illustrative purposes only

# Evidence Collection

- Context is **critical**
- Need to establish the scope of systems and evidence collections plans
  - What evidence do we need to support our investigation?
  - What capture tools do we need?
- **Critical** to follow appropriate processes and procedures

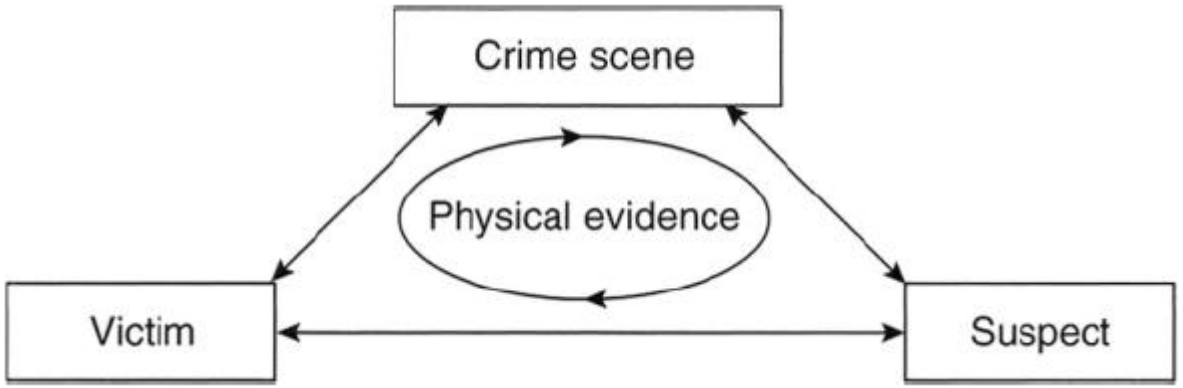

https://arrowheadforensics.com/a-8882-evidence-packaging-kit.html

# Principles of Evidence Collection

1. No action should change the data
2. If accessing original data – must be competent, explain relevance and implications of actions
3. Audit trail or record of all processes applied must be created and preserved
4. Person in charge of the case has the overall responsibility for ensuring laws and principles are followed

# Evidence Exchange

- **Locard's Exchange Principle**:
  - Contact between two items will result in an exchange
  - 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



# Evidence Exchange

- **Data Exchange:**
  - Every interaction with digital devices involves data exchange
  - Actions leave behind traces in the form of data packets, logs, artifacts

Unauthorized access

Possible data left behind?

- Login records
- IP addresses
- Malware signatures

# Integrity & Soundness

- Showing that evidence has not been modified since the time of collection
- We use message digest (hash) functions to perform this work for us
  - SHA256 is common, however, some tools only support MD5 and SHA1
- How was the evidence handled (preserved and examined)
  - Documentation
    - Records the integrity of data and records being analyzed
    - Must show:
      - Timestamps
      - Tools used
      - Methods used
      - Hash values

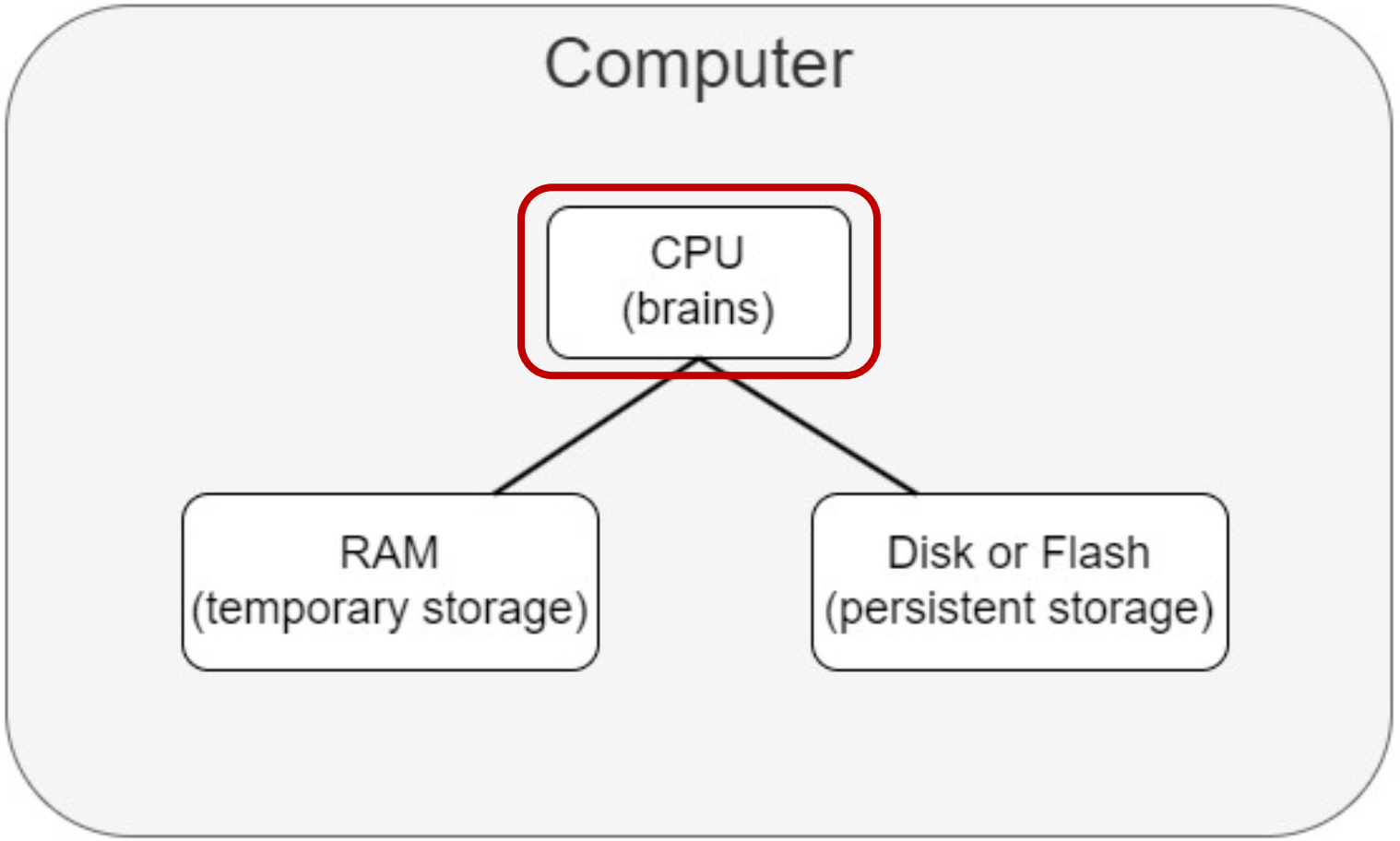
# Legal Considerations

- Evidence **must** be collected and preserved lawfully
  - Failure to follow procedures can make you legally liable
    - Unauthorized access may violate regulations
  - Mishandling data can make it inadmissible in court
    - Search warrants may be required for evidence collection
- Chain of custody is critical for courtroom use

# Digital Evidence Collection

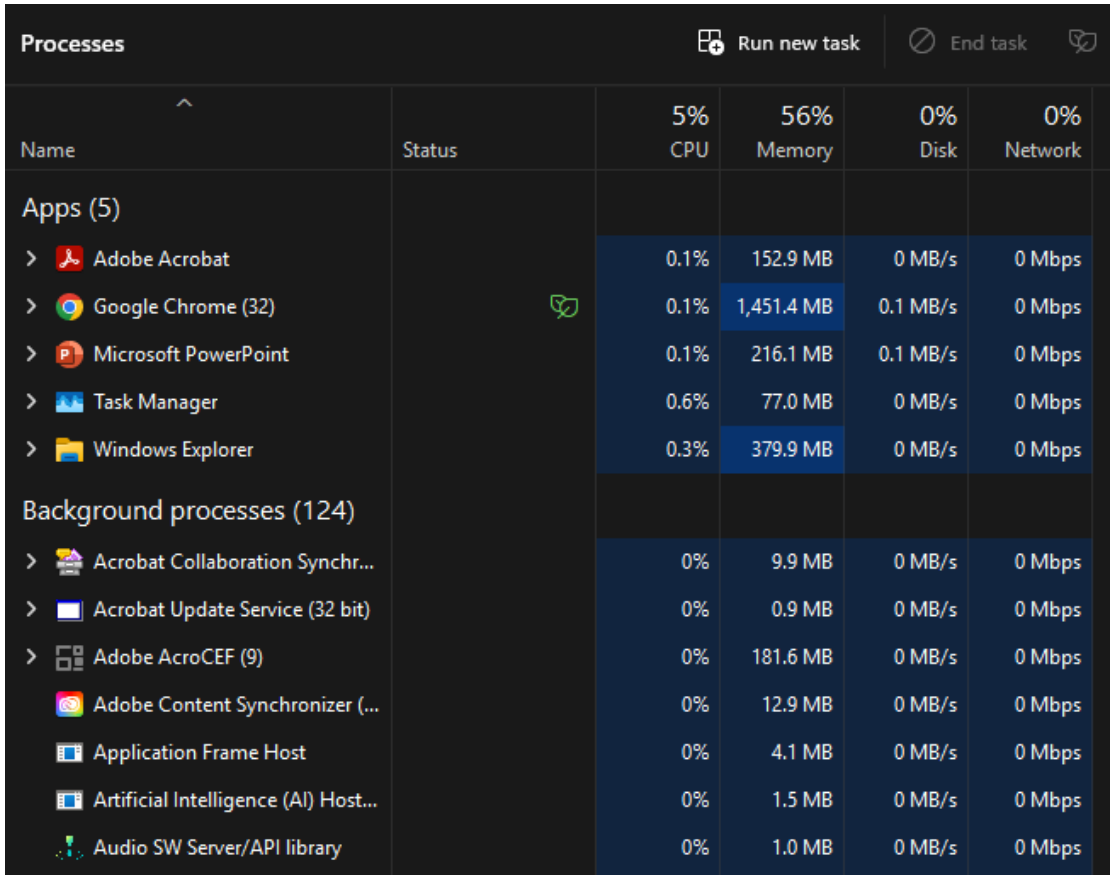
- Digital evidence is typically collected through software or hardware tools
- Software tools vary by need
- Hardware tools are used when:
  - The device is physically in the possession of the investigator
  - The device provides power
  - There is an interface to access the target device
- Collect **artifacts** on the system

# Computer Overview

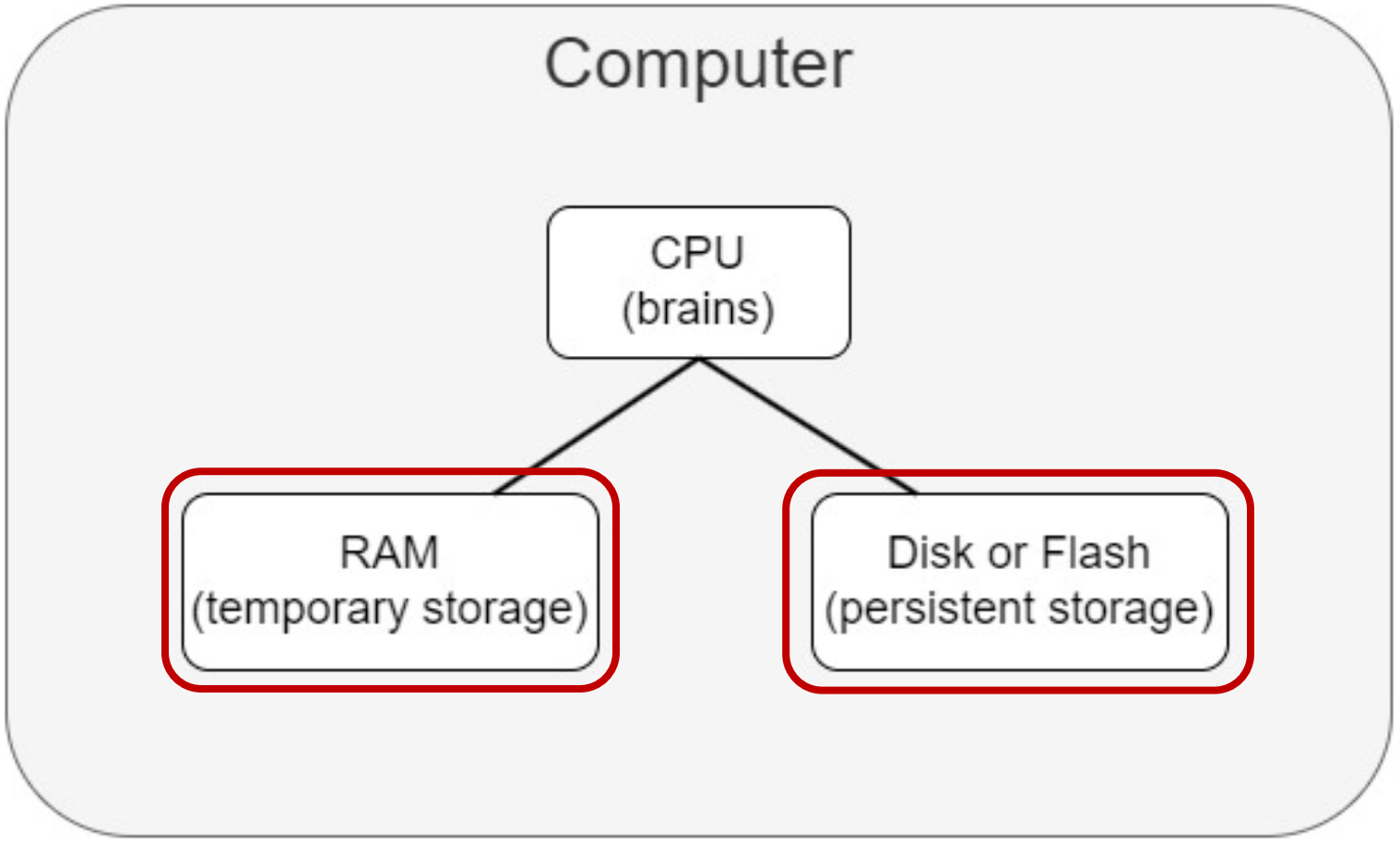


# Processes

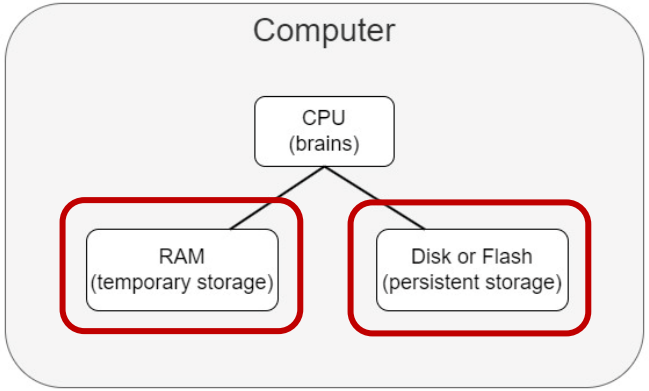
- The operating system (OS) is responsible for creating, managing, and terminating processes
- A process is a running program in memory
  - All code and data for a process exist in memory
  - If malware is running, it should be an active process that the OS is maintaining



# Computer Overview



# Volatile vs Non-Volatile Artifacts



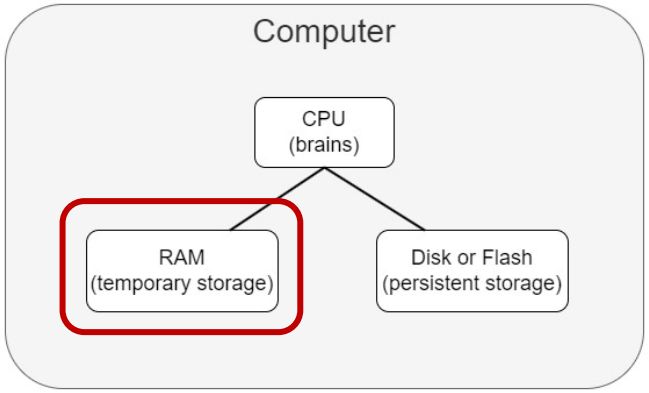

## Volatile

- Does not persist across power cycles
  - RAM
  - Fileless malware
- Must be captured when a system is running
- Faster

## Non-Volatile

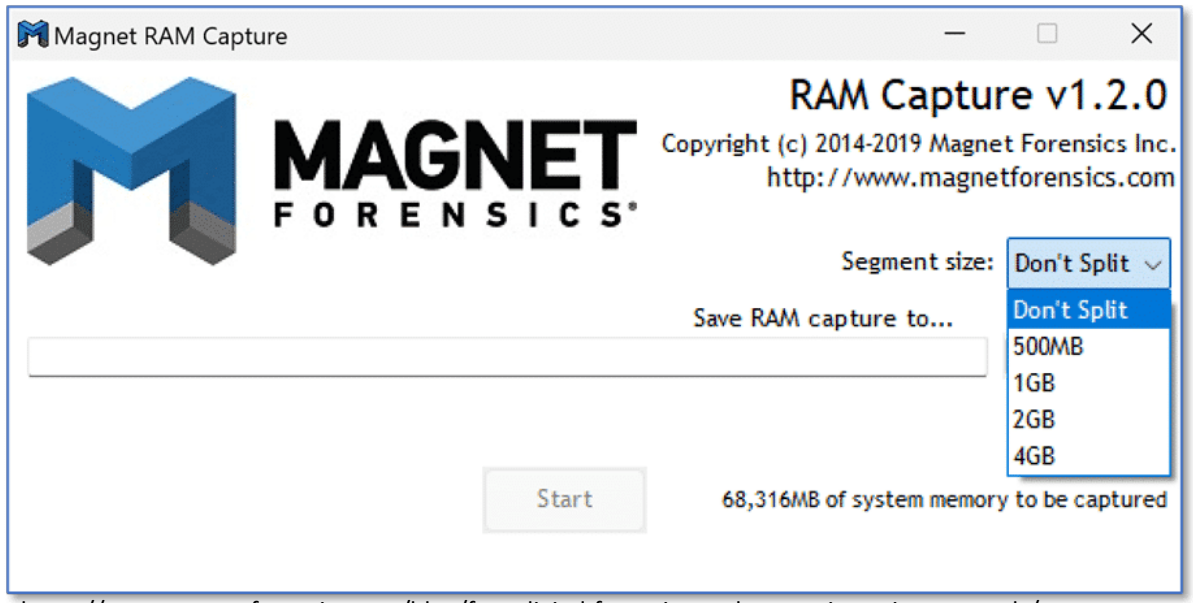
- Does persist across power cycles
  - Hard drive contents
  - Malware
- Can be captured when a system is running or offline
- Purpose of investigation determines best way to capture
- Slower

# Capturing Volatile Artifacts




- Volatile evidence is non-persistent when power is lost to the device
- Want to make a bit-for-bit copy of the contents in RAM
- 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

# Volatile Capture Tools

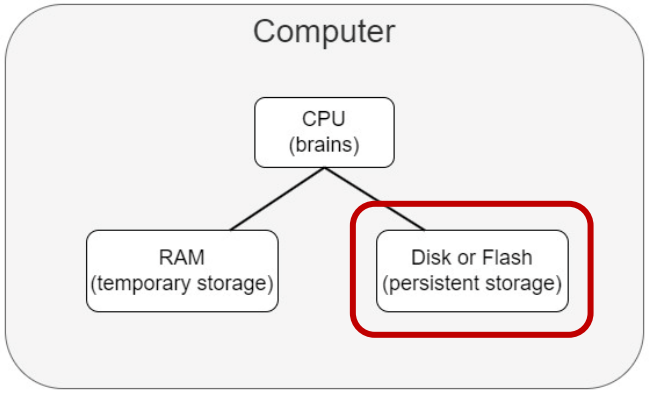



https://www.magnetforensics.com/blog/free-digital-forensics-tools-every-investigator-needs/



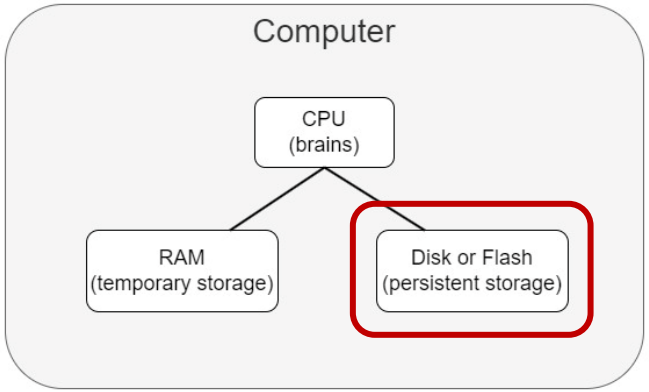
https://hawkeyeforensic.com/2024/01/05/the-top-hardware-and-software-solutions-for-digital-forensic-investigations/

# Capturing Non-Volatile Artifacts




- Interacting with data storage device that does not modify or lose data when powered off
- Must have way to access the data (physically or virtually) and be able to power on the device
- Create a copy of the contents of a hard drive for analysis
  - Two ways to do this: Physical and Logical Disk Captures

# Capturing Non-Volatile Artifacts




| | Physical Disk Capture | Logical Disk Capture |
|---|---|---|
| Description | • Capture bit-by-bit copy of disk<br>• Most defendable and forensically sound collection | • Isolates files on a device<br>• Typically, does not recover deleted items or file fragments<br>• Typically, sufficient for civil litigation |
| Pros | • Access to device artifacts (files, timestamps, event logs, etc.)<br>• Will be able to parse the entire “raw” disk and data structures<br>• May get “deleted” files | • Gives us all the files from the operating system’s point of view<br>• Quick<br>• Smaller output files |
| Cons | • Time consuming<br>• Large output file | • No chance of recovering deleted files |

# Non-Volatile Capture Tools

- 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 the integrity of machine)



https://www.cyint.in/post/write-blocker-blocks-writing-access-upholds-integrity-and-ensures-authenticity

# Capturing Network Artifacts




Various sources; for illustrative purposes only

- Can use software or hardware tools
  - TAPs
  - SPANs
- An additional network interface captures a copy of network traffic
  - Pros:
    - Full capture
    - Can include files, network protocols (standard and non-standard)
  - Cons:
    - Typically have to decrypt in-line man-in-the-middle traffic
    - Newer TLS versions make passive decryption difficult
    - More difficult for cloud environments
    - Metadata becoming less feasible to capture

# Evidence Dynamics

- The real world is imperfect
- Any event, regardless of intent, can occur
  - Change
  - Relocate
  - Obscure
  - Obliterate

# Analysis Tools

# Analysis Tools

- Open source
  - SIFT Workstation – Swiss army knife of incident response and digital forensic tools; disk, memory, and network forensics
  - Autopsy – GUI-based program to analyze smart phones and hard drives
  - The Sleuth Kit – command line tools to analyze disk images and recover files; disk and network
  - Volatility3 – investigative tool to find malicious files and processes; memory forensics
    - https://github.com/volatilityfoundation/volatility3
  - Rekall – forked from Volatility framework; built for more complicated memory forensics

# Volatility3

```
┌──(kali㉿kali)-[~]
└─$ python3 ./volatility3/vol.py -f <FILEPATH> -p <pluginname>
```

- Memory forensics tool
- Independent of the system being investigated
- Offers visibility into the runtime state of the system
  - Any program will typically be in the form of an .exe or .dll file
- Plugins to determine processes in memory, open network ports, find malicious files, and so much more
- Compare volatility commands
  - https://blog.onfvp.com/post/volatility-cheatsheet/

# Volatility3 Plugins

- Plugins
  - windows.pslist
  - windows.pstree
  - windows.netscan
  - windows.malfind
- Outputs can be piped
  - …pstree | grep “LISTENING”
  - …netscan | grep “<IP address>”
- Dump a process
  - python3 ./volatility3/vol.py –f <path to .vmem or .mem> -o <dump dir> windows.memmap –pid <PID>

# Additional Analysis Tools

- CyberChef – Swiss Army knife to decode/encode strings
  - https://gchq.github.io/CyberChef/
- VirusTotal – check for presence of malware
  - https://www.virustotal.com/gui/home/upload
- GoldFynch PST Viewer – review calendar and emails
  - https://goldfynch.com/pst-viewer/index.html

# CyberChef

- CyberChef is a web app that can encrypt, encode, compress, and perform data analysis
  - It is common for a threat actor to obfuscate their payload by encoding it in a certain way
- We can apply CyberChef “recipes” to determine the original payload from an encrypted string

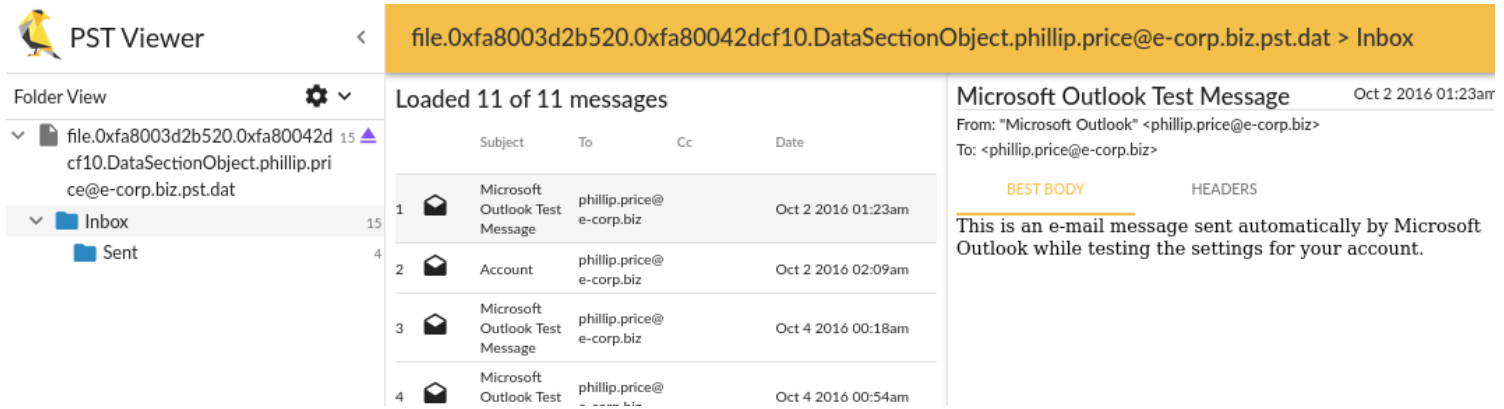
Encrypted String Example:
NDElNjMlNjMlNjUlNzMlNzMlMjAlNjclNzIlNjElNmUlNzQlNjUlNjQlMmUlMjAl
NTQlNjglCjY1JTIwJTY2JTZjJTYxJTY3JTIwJTY5JTczJTIwJTY4JTY5JTY0JTY0JTY1JTZl
JTIwJTY5JQo2ZSUyMCU3NCU2OCU2NSUyMCU2MSU3NCU3NCU2MSU2MyU
2OCU2ZCU2NSU2ZSU3NCU3MyUyZQ==

# VirusTotal

- Massive database of known malware signatures and malicious fingerprints
- Benefits investigations by providing information on whether a file has been flagged as malicious
  - File hashes
  - IP addresses
  - Domain names
- Example: 17ebook.co

# GoldFynch PST Viewer

- View contents of PST or OST email archives
  - Time
  - From
  - Messages
  - Calendars
  - Attachments



# 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 about the evidence and information that support or refute these hypotheses

# Reproducibility

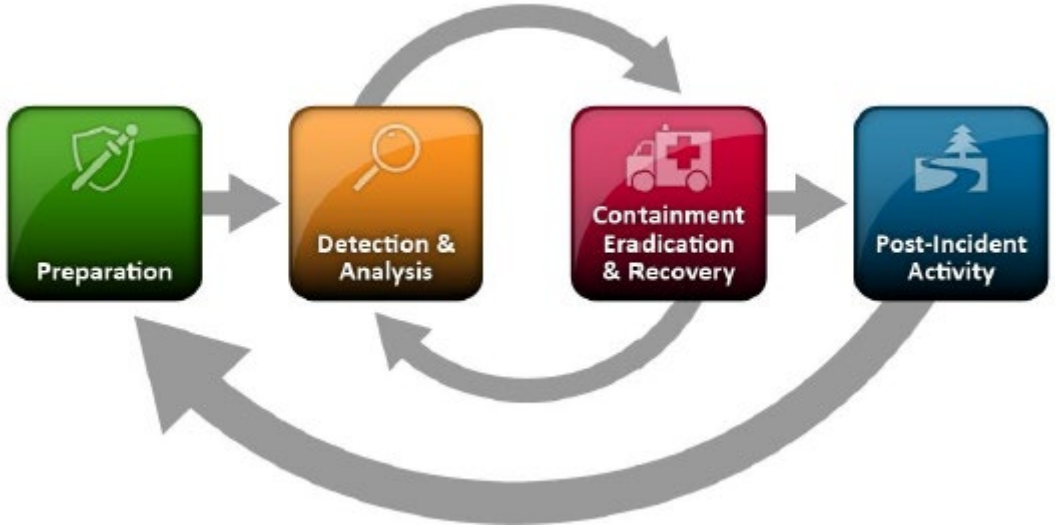
- Want to ensure our analyses are repeatable
- Do we get the same results?

# Incident Response


https://www.forbes.com/sites/daveywinder/2025/05/06/884000-credit-cards-stolen-with-13-million-clicks-by-a-magic-cat/

# Incident Response Standards

- ACPO Good Practice Guide commonly used for criminal investigations
- NIST 800-61r2 & NIST IR 8387 provide guidelines and best practices for incident response and digital evidence preservation
- **Critical** to follow appropriate processes and procedures when collecting evidence




From NIST 800-61r2

# Signs of an Incident

- Precursors
  - Web server logs indicate the presence of unauthorized vulnerability scanning
  - Announcement of a new, relevant vulnerability
  - A threat group stating privately or publicly that they are targeting the organization
- Indicators of Compromise
  - Alerts from reputable sources
  - Suspicious log/audit log entries for key services
  - Configuration changes
  - Multiple failed login or access attempts

# Analysis

- Start collecting at the initial sign of incident
  - Can take an initial system snapshot
- Assess
  - Profile networks and systems
  - Baseline normal behavior
  - Perform event correlation
  - Maintain and use a knowledge base information
  - Use internet search engines for research
  - Collect additional data
  - Filter data
  - Seek assistance from others

# Documentation

- Current status of the incident
- Summary of the incident
- Indicators of the incident
- Actions taken by handlers
- Chain of custody
- Impact assessments
- List of gathered evidence
- Next steps

# Prioritize

- Prioritization of incidents is critical
- Functional impact
  - Impact of the incident on IT system business functionality
- Information impact
  - What's the impact on the confidentiality, integrity, and availability of information
- Recoverability
  - Size of the incident, degree of compromise, and type of resources it affects will impact the amounts of resources needed for recovery

# Notification

- Communication is **critical**
- Key stakeholders must be notified
- Typically documented in an organization's incident response plan
- Notification requirements may vary


From NIST 800-61r2

# Evidence Collection

- Collect digital data that supports the case
  - Disk capture
  - Memory capture
  - Network packets
- Must always be accounted for

# Evidence Analysis

- Identify the attacking host(s)
- Identify the root cause of the incident
- Build a timeline of the incident

# Containment

- Containment strategies vary and must balance the need to prevent additional damage or theft with a need to maintain and collect evidence
- Sometimes occurs before evidence collection
  - Premature containment can lead to situations where an adversary is thought to be “evicted” but is not
- Containment cannot occur without root cause analysis
- Containment typically involves parallel network and identity efforts

# Eradication and Recovery

- Removing adversary access and eliminate vulnerability (eradication)
- Take input form evidence collection and analysis and balance the business capabilities against attacker access
- Phased approaches generally work better
- Ensure systems are functional within expected parameters (recovery)
- Remember to address the root cause

# Reflect

- Reflect on response management
  - What went well?
  - What can we do better next time?
  - What can we learn?
- How can the incident be prevented in the future?

# Career Paths

- Digital Forensics Analyst
- Cybersecurity Incident Responder
- eDiscovery Specialist
- Law enforcement (local, FBI, CIA, etc.)
- Certifications:
  - EnCE – EnCase Certified Examiner
  - GCFA – GIAC Certified Forensic Analyst
  - CHFI – Computer Hacking Forensic Investigator
  - CompTIA Security+

# Capture the Flag

# Instructions

- Get into teams of 3-4
- Log into Linux VM
  - If still needed, install python dependencies from provided code
- Solve the steps in Parts 1 and 2
  - ‘volatility3 setup and capture the flag exercise.pdf’ - https://drive.google.com/file/d/1sjjXbU5sezgMQTvtV3nHFmM7RqdtHhyW/view?usp=drive_link
  - Documentation template - https://docs.google.com/document/d/1kki1qGZaE0gIIVc1O6B4o9iwGEPHCTbl49bIj3IOlCo/edit?usp=drive_link
- 1st, 2nd, and 3rd place prizes!