CF terminology & relevant concepts

Digital evidence

- **data stored or transmitted in digital form that can be used in court**
- **the cornerstone of any digital forensics investigation**
  - data can be viewed at different levels of abstraction, requires interpretation, are fragile, may be **voluminous**
  - Often is difficult to discover connection data <-> reality
- **requires technical understanding of different possible types (files, emails, logs, metadata) and the legal requirements for collecting and preserving it**
- **knowledge of file systems, network protocols, and encryption methods essential as well**

Chain of custody

- **documented and "unbroken" process of handling evidence from the time it is collected until it is presented in court**
- **ensures that digital evidence has not been tampered with, altered, or accessed by unauthorized parties**
- **critical for the evidence to remain legally admissible in investigations and trials**
- **requires knowledge about how to document evidence collection, storage, and access**
  - involves knowledge of logging procedures, secure storage solutions, and legal protocols.

Data acquisition

- the process of collecting digital evidence from devices without altering or damaging the original data.
- requires knowledge of disk imaging and live data capture
- requires expertise in forensics acquisition and analysis tools, like *FTK Imager, EnCase*
- knowledge of file systems, write-blockers, and hashing is crucial for ensuring integrity

Hashing

- **the process of converting data into a fixed-length string of bits, which represents the data uniquely**
- **to ensure the integrity of digital evidence. A hash value can verify that a file has not been altered during the investigation**
- **requires understanding of hashing algorithms (strengths and weaknesses, e.g. MD5 collision) and formats (*hex, base64*)**
- **requires expertise in hashing tools**
  - *sha256sum, hashdeep*
  - *FTK imager, Autopsy*
- **have to be used any time an evidence is "managed" (copied, moved)**

Write Blocker

- hardware or software tool used to prevent any data from being written to a storage device during analysis, preserving the original data content
- requires understanding of how write-blocking devices work and how they can be implemented in forensic procedures
- essential for legally defensible acquisitions

https://www.flickr.com/photos/joncrel/26922354599

Forensic image

- **A bit-by-bit copy of digital media, including deleted files and data in slack space, which is an exact replica of the original device**
- **Goal: to preserve the original evidence.**
  - **avoiding modification of the original data**
- **requires understanding of mechanisms to copy information in digital devices (file system knowledge and behavior)**
- **requires familiarity with bit-by-bit copy tools (a.k.a. forensic imaging tools)**
  - *Dd (and command line evolution)*
  - *FTK imager, Encase, Guymager*
- ***have to be used any time an evidence is "managed" (copied, moved)***

Scenarios

Typical computer forensics scenario

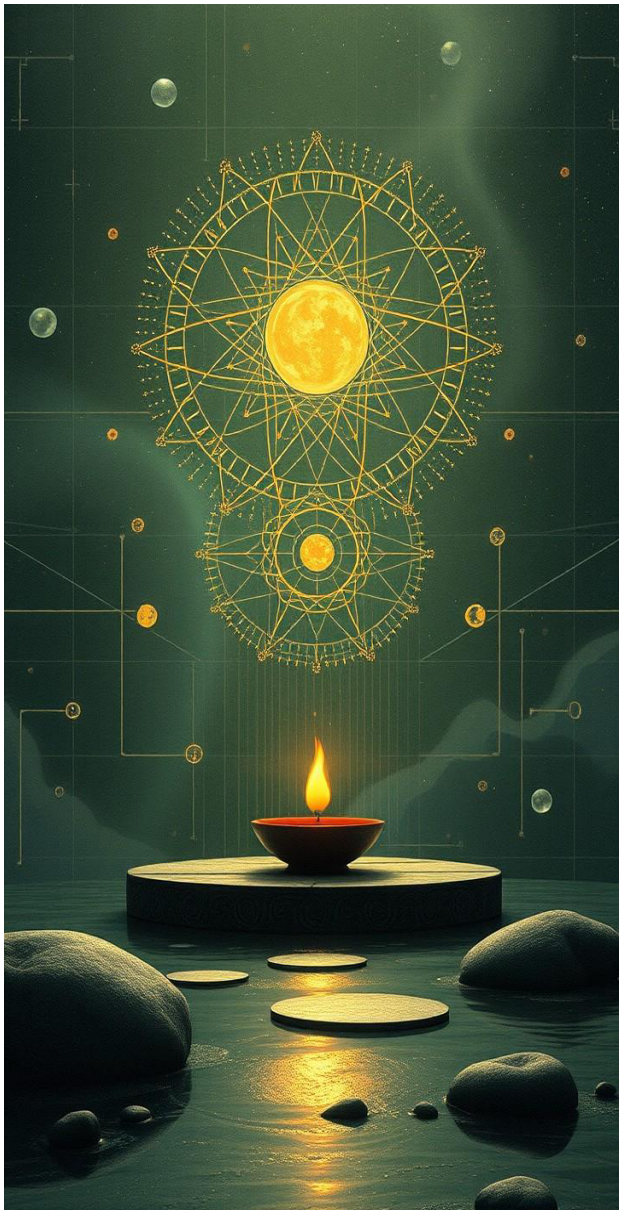
More on Prof. Vaciago' lessons

- **internet abuse from employee**
- **computer-aided frauds**
- **data unauthorized manipulation**
  - data theft
  - data disclosure
- **computer/network damage assessment**
- **…and any time digital evidences may be involved in an incident**

Investigation phases

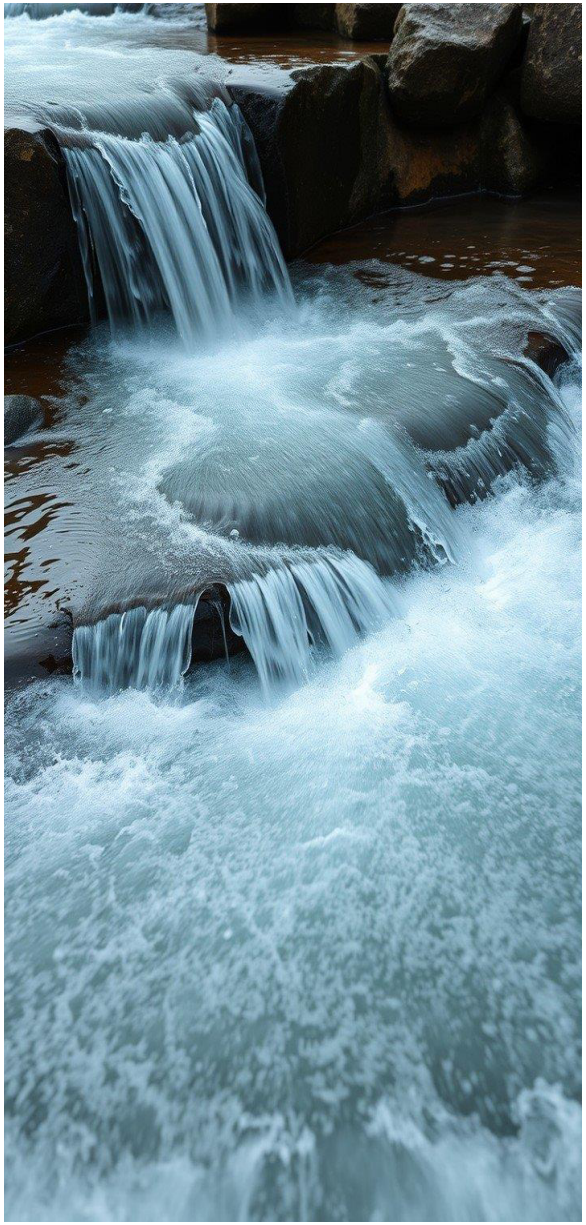
Investigation process

- **many computer forensics standard exists to guide the investigation process**
  - different legal systems, technological evolution, stakeholders (private, public, military,…)
- **like, for example:**
  - NIST family (SP 800-86, **SP 800-101, SP 800-88) to guide digital forensics, mobile forensic,** Integration of Forensic Techniques into Incident Response, media sanitization, ...
  - ACPO Guidelines (UK): Association of Chief Police Officers' best practices for digital evidence handling
  - ISO/IEC 27042: Guidelines for analysis and interpretation of digital evidence
  - **SWGDE (Scientific Working Group on Digital Evidence)**: Best practices for chain of custody documentation
  - ...



Investigation process

- **identification**
  - Identification of potential source of relevant data (digital evidences)
- **collection**
  - physically or remotely taking possession of the evidence (e.g. a computer) and its connection (e.g. network or physical, like USB disk)
- **acquisition**
  - electronically retrieving data by running various CF tools and software suites
- **evaluation**
  - evaluating the data recovered to determine if and how it could be used against the suspect (e.g. for prosecution in court)
- **presentation**
  - presenting the evidence discovered in a manner which is suitable for lawyers, non-technical staff/management and the law (and internal rules)



Identification (I)

- **recognize (**all relevant) **data sources before any acquisition begins, like**
  - hard drives (HDD/SSD)
  - memory (RAM)
  - mobile devices (smartphones, tablets)
  - cloud storage
  - network traffic
  - removable media (USB drives, DVDs)
  - IoT devices and embedded systems
  - ...

Identification (II)

- **actions**
  - perform an initial survey of the scene (physical or network environment)
  - identify key devices and data locations (local storage, remote servers, cloud services)
  - check for connected devices, including peripherals like printers, removable media, or network-attached devices
  - map all potential data sources using network topology diagrams or asset inventories
- **hint: pay attention to "ephemeral" storage of data**
  - e.g. cloud syncing, hidden sector, ...

Collection (I)

- gathering evidence from identified data sources while ensuring the preservation of its integrity
- key point is the implementation of methods that minimize the risk of evidence tampering or data loss

Collection (II)

- **actions**
  - isolate devices to prevent them from being tampered with remotely (e.g., disconnect them from the network)
  - use devices to block external communication for mobile or wireless devices
    - e.g. faraday bags
  - use network isolation tools for virtual and cloud environments to prevent remote access
    - e.g security groups, virtual private cloud, firewall rules, ...

- **hint (for live systems): ensure evidence integrity while maintaining system uptime**
  - shutting down can cause the loss of volatile data (e.g., RAM).

Collection (III)

- create a **detailed record** of the condition **and state of** the evidence
  - take photographs of the devices in situ, including connected peripherals and the physical state
  - record serial numbers, device models, and any other identifiable information
  - document the **scene**, noting which devices were running, whether screens were active or locked, and any other visible indicators
- **hint: complete documentation is crucial to prevent legal challenges regarding the integrity of the evidence**

Collection (IV)

- **prepare for acquisition ensuring no alteration will take place**
  - write blockers for physical storage devices (e.g., hard drives, USB drives).
  - disable connection and syncing and notifications
    - remote wiping or data alterations
- **hint: complex to maintain integrity on live systems (e.g., using remote collection methods that minimize data alteration risks)**

Acquisition (I)

- **the process of creating a forensic copy (bit-by-bit image) of the original data**
- **goal: ensure that the acquired data is a faithful replica of the source**
- **key point: maintaining data integrity**
  - hashing algorithms (for the acquisition process)

Acquisition (II)

- **selection of the acquisition method between**
  - static: the system is powered down.
    - most common method **for acquiring data from hard drives and external media**
  - **live: running system**
    - **Deal with volatile data** like RAM, network connections, or running processes. Critical for live systems, servers, or IoT devices
- action
  - determine the type of data to acquire (e.g., hard drive images, RAM dumps, network traffic)

Acquisition (III) - Static

- **actions:**
  - shut them down carefully to avoid losing data
    - e.g. for encrypted devices, consider methods for capturing data without triggering loss of access (e.g., before the decryption key is wiped from RAM)
  - attach the device to a forensic workstation using a write blocker
  - use forensic imaging tools to create a complete image of the storage device
  - generate a hash value (e.g., SHA-256) of the original media before and after acquisition to verify integrity
  - store the image on a secure forensic storage device
- **hint: pay attention that data is properly hashed and verified post-acquisition**

Acquisition (IV) - Live

- **actions:**
  - choose a method that minimizes system interference while capturing volatile data
  - dump RAM (memory acquisition) and capture data from running processes or network connections.
  - perform **network traffic capture**
  - document all acquisition actions and steps to ensure chain of custody and admissibility
  - hash the volatile data wherever possible to maintain data integrity

Acquisition (V) - Integrity

- **ensure that the acquired data is an exact replica of the original and has not been altered**
- **actions:**
  - choose a method that minimizes system interference while generating a hash (MD5, SHA-256) of the acquired image or data dump
  - compare the hash value to the original data hash (for static data) to verify its integrity
  - document the hashing process, including the algorithms used and the results, in the chain of custody documentation
- **hint: be careful! any discrepancies in hash values would require re-acquisition and could damage the credibility of the evidence**

Acquisition (VI) - Chain of custody

- **ensure a complete, documented chain of custody for the evidence throughout the acquisition process**
- **actions:**
  - record every step in the acquisition process, including personnel involved, tools used, date, and time of acquisition.
  - store the data and evidence securely to avoid unauthorized access or tampering.
- **hint: any "weak ring" in the chain of custody jeopardizes the admissibility in legal or forensic context**

Evaluation (I)

- ensures **the integrity, authenticity, and admissibility of the digital evidence collected during an investigation**
- analyzing, verifying, and validating the evidence to ensure it remains unaltered and trustworthy for legal proceedings or further analysis

Evaluation (II)

- **actions:**
  - (recurring) comparison of fresh and stored hash values
  - (recurring) chain of custody validation
    - handled, documented and transferred securely at each step
  - (recurring) forensics image verification
    - No alteration or gaps in the images
  - (recurring) live data verification

Evaluation (III)

- timestamp and metadata analysis
  - verify file creation, access, and modification dates of data to ensure they match the timeline of the incident
- timeline reconstruction
- cross-reference analysis/consistency verification
  - correlation of digital evidences with external logs or other data to countercheck it is related to the suspected system or device
  - comparison of data from different sources(e.g. logs, email)
- compliancy with current legal/internal standards
  - collection, preservation, evaluation must be coherent to applicable legal procedures...and the documentation must keep track of that
- review of possible anti-forensics techniques

(final) Presentation (I)

- preparing and presenting the findings of the investigation in a clear, accurate, and legally admissible manner
- goal: "translate" the technical details of the forensic analysis into a format that can be understood by non-technical stakeholders, such as lawyers, judges, or company executives
- hint: quality and clarity of the presentation can significantly impact the outcome of legal proceedings or internal investigations

Presentation (II)

- **actions:**
  - review all the data collected, analyzed, and interpreted during the investigation
  - identify key evidences
  - check the correlation of all conclusions to verifiable evidences
  - document the entire forensic process in a formal report (free from technical jargon) that can be submitted as legal evidence
    - ..and securely manage the report as well
- **hints:**
  - no "personal interpretation" unless asked for expert opinion
  - Include appendices with timestamps, metadata, hash values, and technical evidence "reinforcement"