CS 798: Digital Forensics and Incident Response

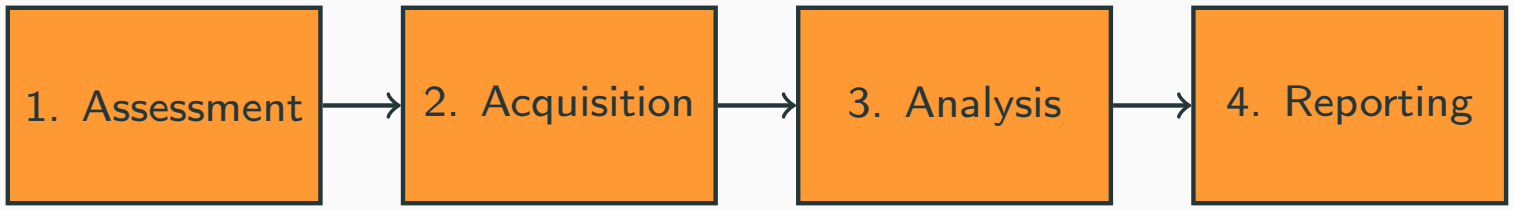
Lecture 4 - Evidence Acquisition

Diogo Barradas

Winter 2025

University of Waterloo

Recall the Kruse & Heiser model...



- **1. Assessment:** Prepare plan of action, and find potential sources of digital evidence
- **2. Acquisition:** Prevent changes of in situ digital evidence and collects them
- **3. Analysis:** Search for and interpret evidence trace in order to reconstruct the crime scene
- **4. Reporting:** Reporting of findings in a manner which satisfies the context of the investigation

Outline

1. Tools for evidence acquisition
2. Obstacles to evidence acquisition
3. Evidence acquisition from computers

What are we looking for? Digital artifacts

- **Digital artifacts**: Part or entirely of the digital state of a computer system at a given time
- Examples:
  - Videos, documents, audio recordings, emails, photos
  - Location data, social circles, cached content, communications data
  - Backup archives, web activity logs, configuration files, access control logs
  - ...
- Need to extract them from one or more computer systems

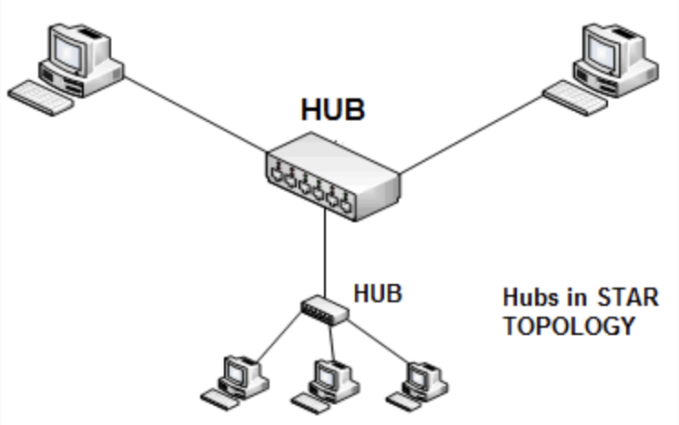
Our main concern when acquiring evidence

- To preserve digital way in a way that:
  1. Maintains an accurate representation of the original data, and
  2. Maximizes its usefulness for decision makers, i.e., it is as complete as possible
- Simply put:
  - We want to get the most evidence we can with the least amount of alteration

Today: collect evidence from the crime scene

Computer networks

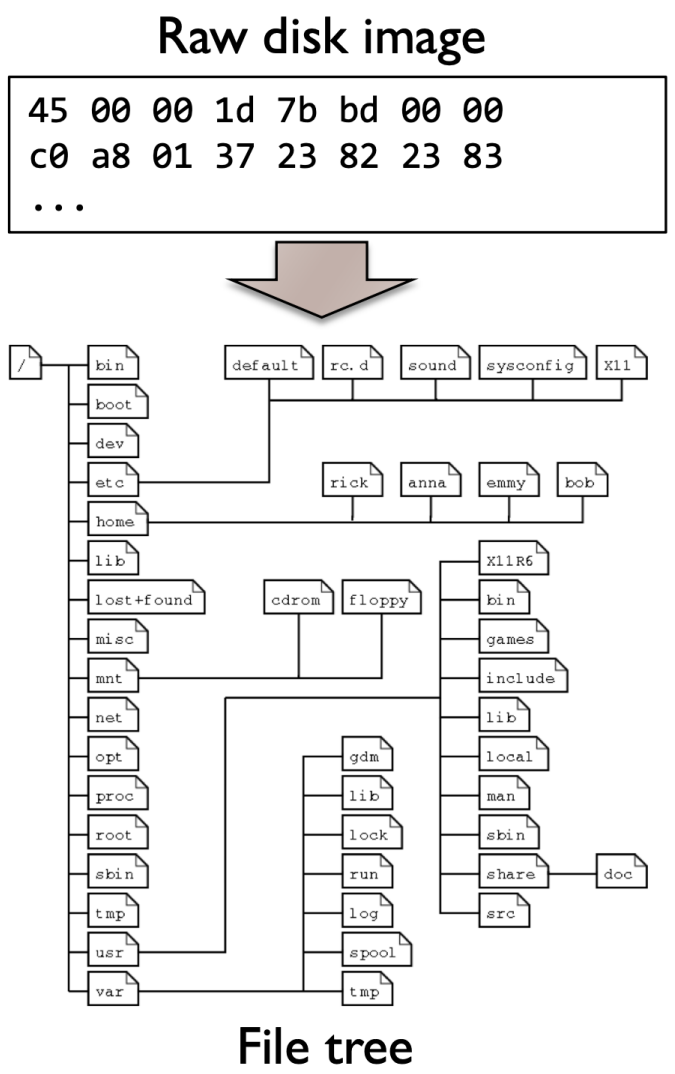
- A computer system = graph of interconnected devices
- **Outer boxes**: computers holding potential evidence
  - E.g., servers, smartphones
- **Inner boxes**: network components connecting outer boxes
  - You need a signed letter of agreement outlining the scope of the investigation along with contractual details
- Boxes provide sources of evidence



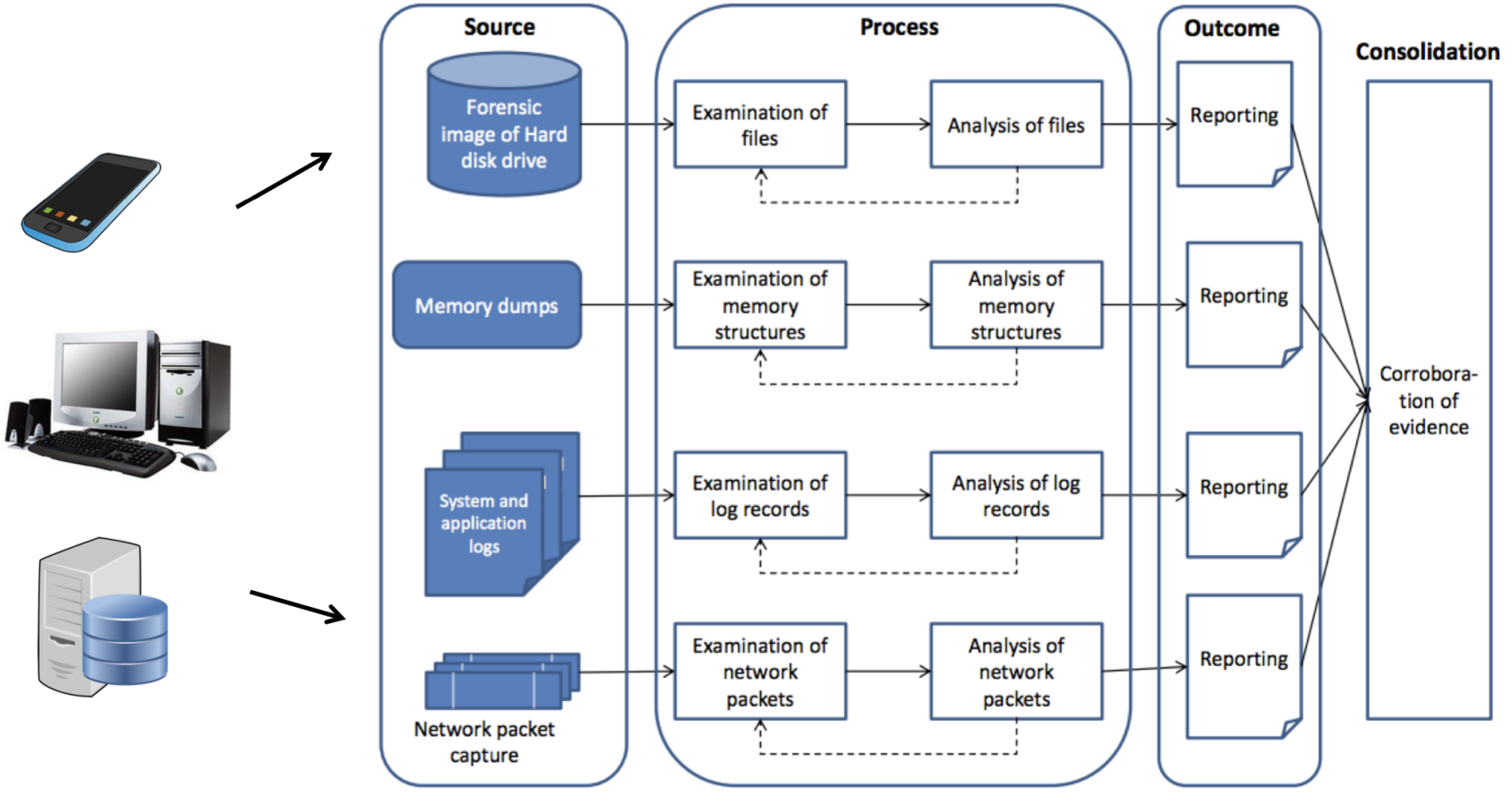
Tools for evidence acquisition

Forensic tools

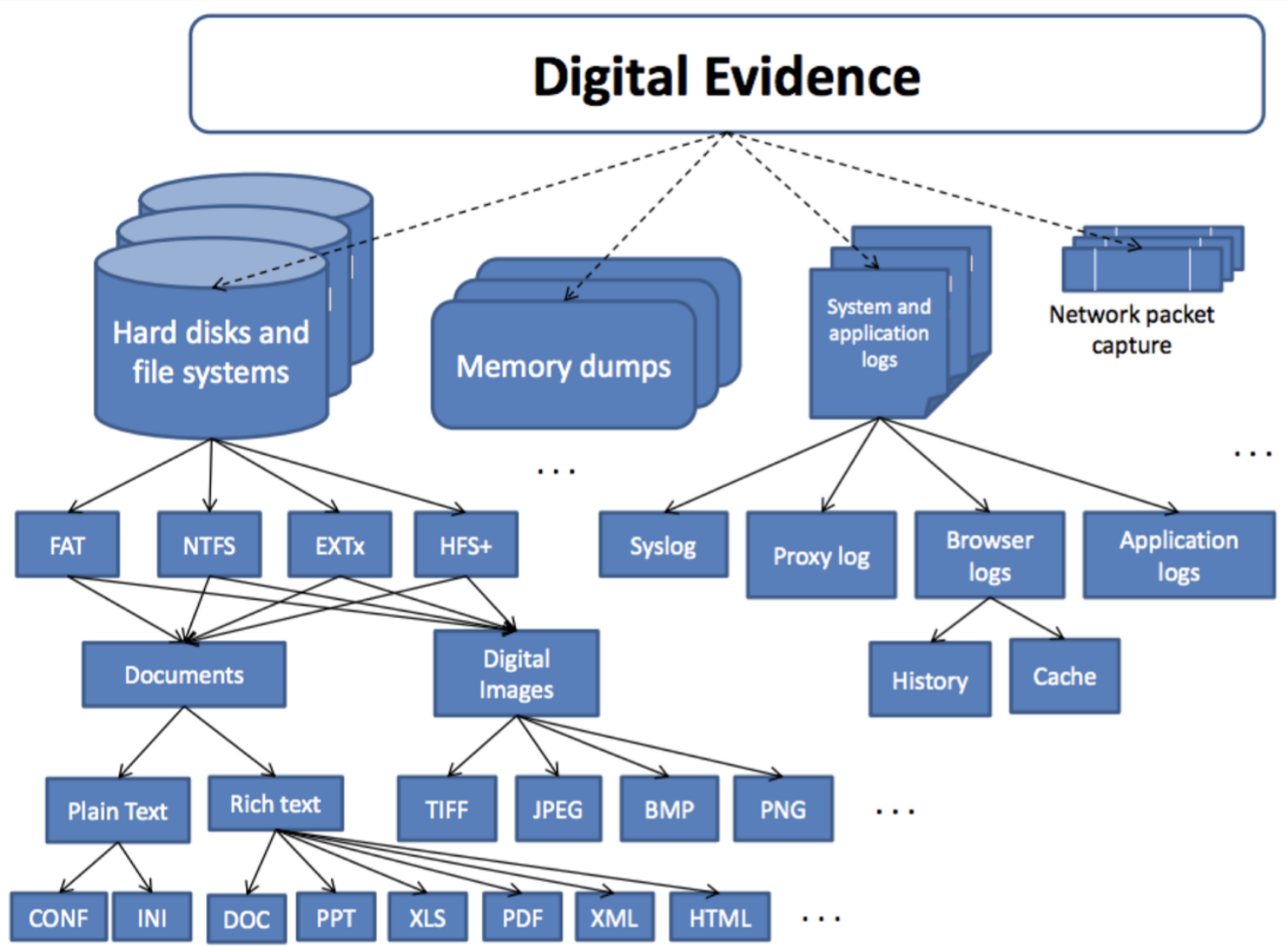
- Translate data through one or more layers of abstraction



Typical workflow of forensic tool utilization



Tools generate multiple data items



Ideal properties of forensic tools

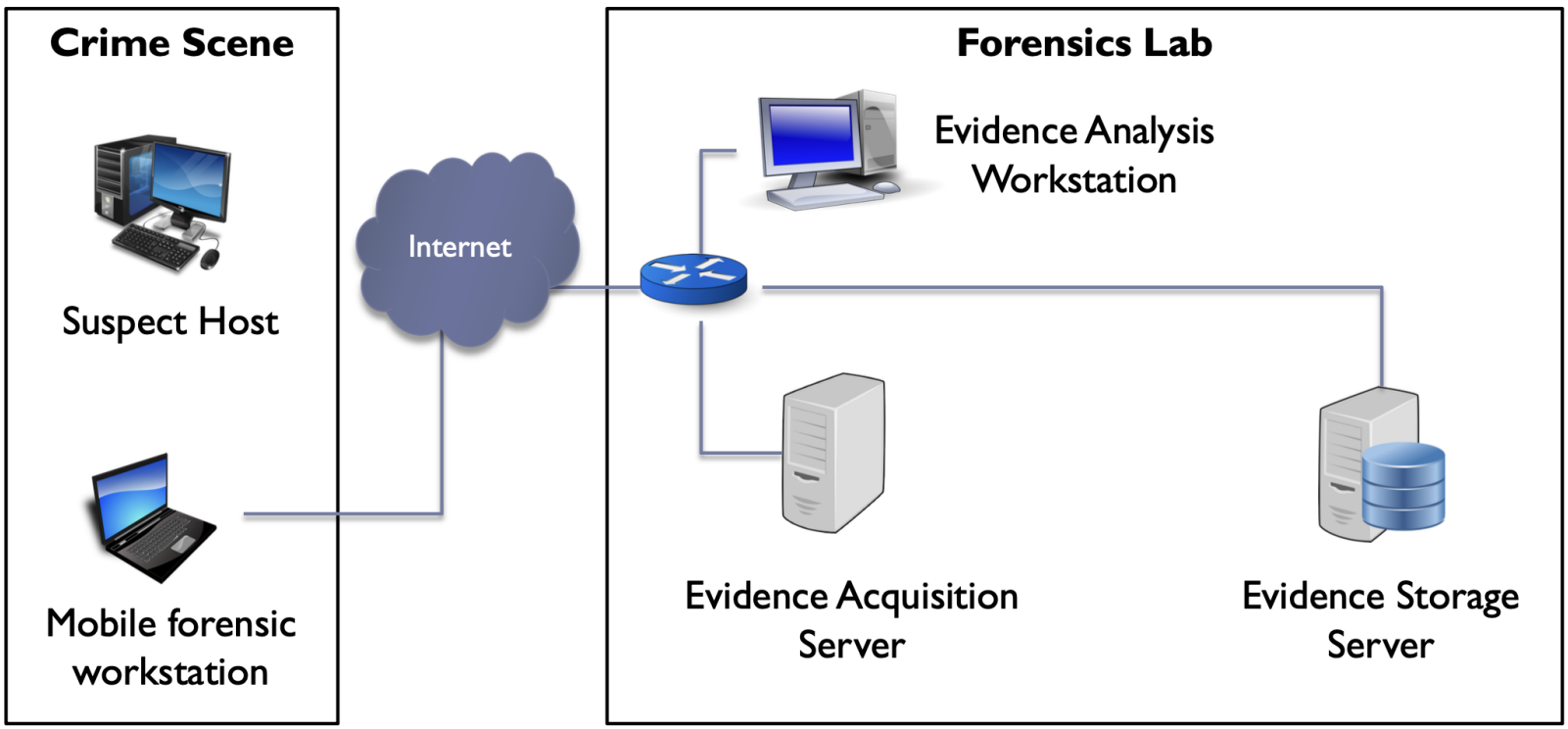
- **Usability**
  - Present data at a useful layer of abstraction for investigators
- **Comprehensiveness**
  - Reveal all relevant data
- **Accuracy**
  - The tool output error must be as low as possible
- **Determinism**
  - Produce the same output when given the same rule set and input data
- **Verifiability**
  - Be able to verify the results, either manually or using independent tool set
- **Performance**

The first responder forensic toolkit

- Backpack or case containing:
  - Mobile forensic workstation (laptop)
  - Bootable forensically-sound OS
  - Forensically clean storage devices for evidence collection: USB pen, external drive
  - Write blocker
  - Faraday bag
  - Other accessories: power cord, power adapters, network cables, power battery

The forensics lab

- Contains equipment for backing up evidence acquisition and supporting preservation and analysis of evidence



Obstacles to evidence acquisition

Obstacle 1: Heterogeneity of technology

Computer platforms

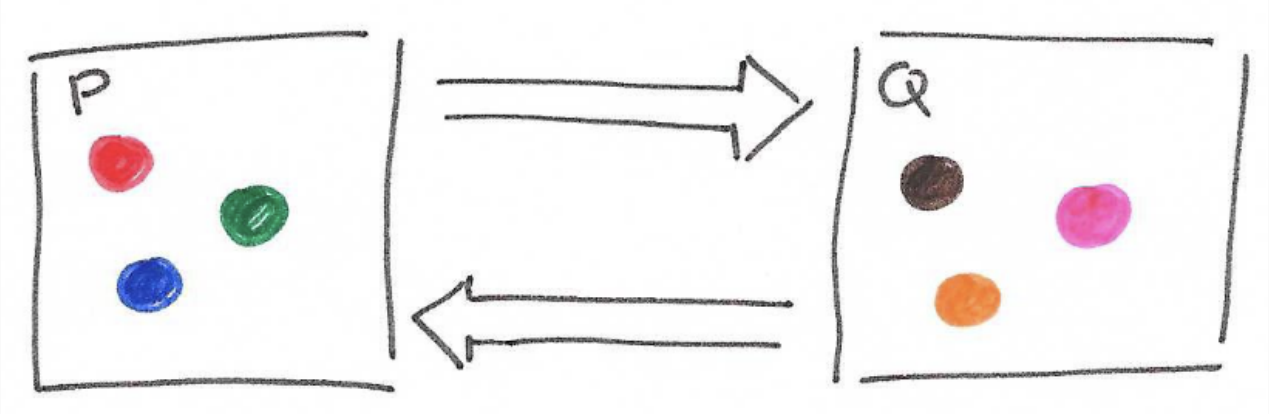
Hardware components

Technologies for similar platforms

Hardware generations

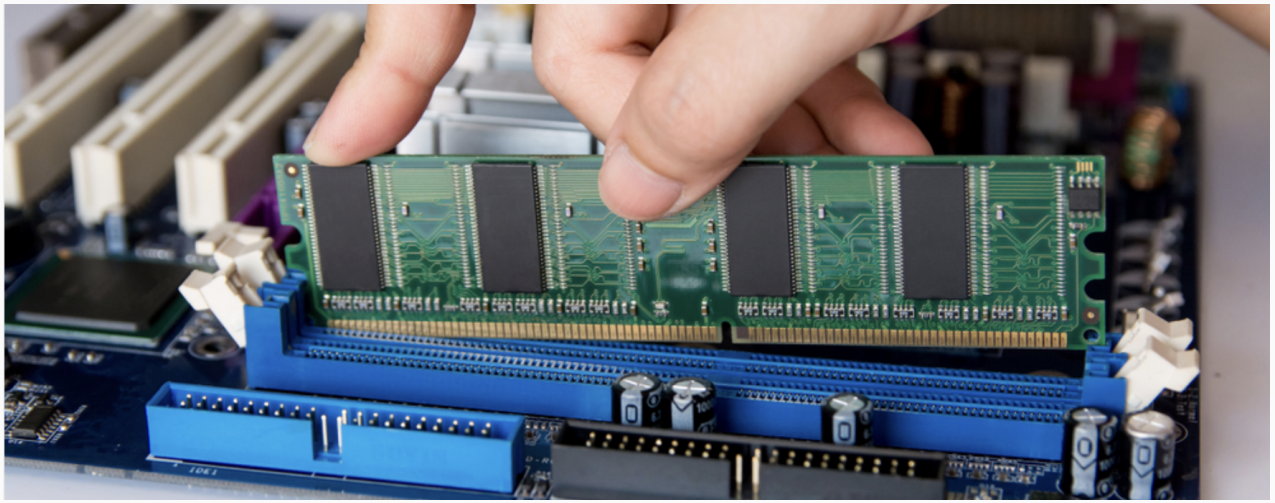
Obstacle 2: Dynamism of system state

- The system state changes which may complicate the task of acquiring a consistent snapshot of evidence
- Some parts of the system may change, but may not be relevant for the forensic analysis
- The lower is the dynamism the higher can the accuracy be because we can obtain consistent data

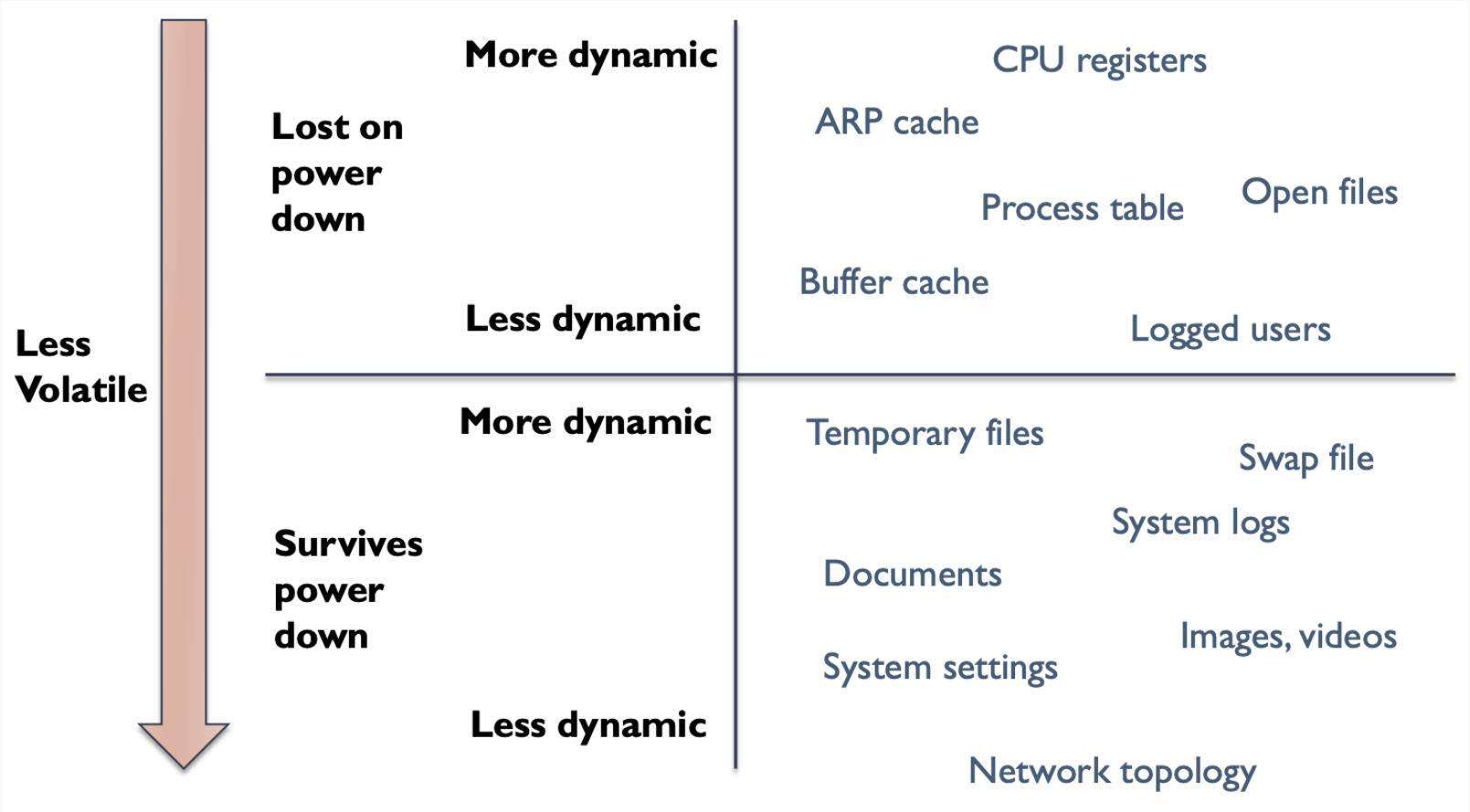


Obstacle 3: Volatility of digital evidence

- Tells how long data can survive in a system
- The volatility level depends on whether:
  - A consistent power supply is required for storage
  - How fast data changes



Volatility level examples



Obstacle 4: Accessibility of digital artifacts

- **Locally accessible**
  - The investigator has access to the HW holding the data
  - E.g., file system of an apprehended computer or mobile device
- **Remotely accessible**
  - Only remote access to the computer system where data lives
  - E.g., gmail account of known password by the investigator
- **Inaccessible**
  - Cannot be retrieved no matter whether or not the forensic investigator is in possession of the host hardware device
  - E.g., encrypted file system w/ unknown key, private cloud store

Obstacle 5: Potentially large amount of data

- Triage may be necessary

FORBES > BUSINESS

BREAKING

‘Massive Amount’ Of Evidence Against Serial Killer Suspect Rex Heuermann Includes Terabytes Of Documents, Photos And Videos, Prosecutors Say

Antonio Pequeño IV Forbes Staff

I cover breaking news.

Follow

Aug 1, 2023, 05:41pm EDT

29 March 2019 - 17:40

French prosecutors copied 26 terabytes of Rui Pinto's files before extradition

They obtained authorization to copy the documents seized from the hacker

Evidence acquisition from computers

Storage devices were found in crime scene

- How to handle such devices?

Hard drives

Thumb drives

Smart hubs

Fitness trackers

Memory cards

General procedure for handling storage devices

- If you can take the device:
  - Tag, bag, create chain of custody, bring to lab for data extraction
- Otherwise, perform data extraction on spot
  - Extract the data into the mobile station or upload it to remote lab server
- Procedure for data extraction from the device:
  - Copy the data from the device without causing alterations
  - Calculate the hash
  - Create at least another copy (double check the hash)

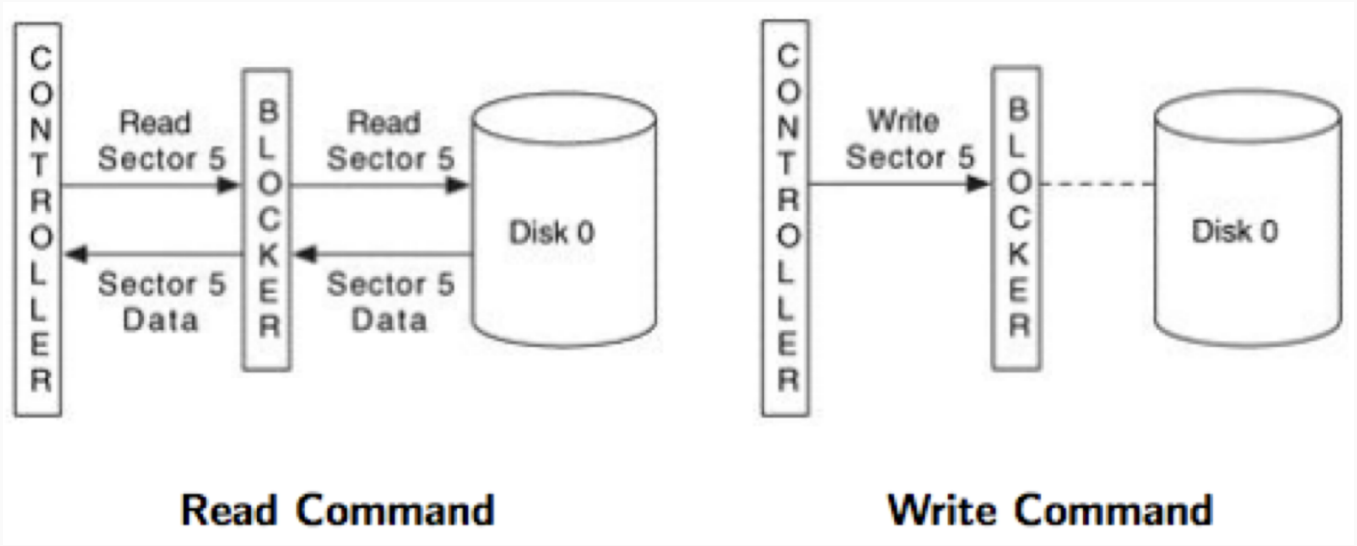
Write blockers

- Be very careful at mounting the storage device!
  - E.g., Windows creates thumbnails and recycle bin folders on plugged devices!
- Write blockers allow acquisition of data from a storage device without changing the drive's contents
  - Write commands are blocked
  - Only read commands are allowed to pass the write blocker
  - Types of blockers: hardware write blocker and software write blocker

Hardware write blocker

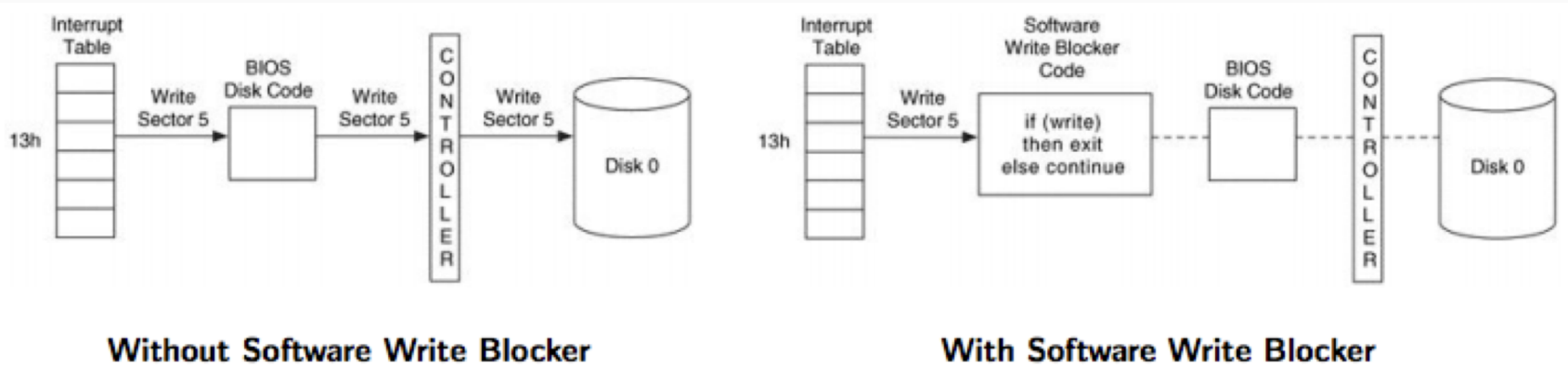
- HWB sits in between forensic station and storage device
  - Supported storage interfaces are ATA, SCSI, Firewire, USB or SATA
- The forensic station's controller cannot write values to the command register, which writes or erases data on the storage device

HW Write blocker



Software write blocker

- SWB is a software layer that sits in between the OS and the device driver for the storage device
- Prevents all disc requests that use sysem calls to write data to the storage device



Methods for copying the data

- **Logical acquisition**
  - Select relevant files to be copied from the device
  - Faster and takes up less space, but incomplete capture
- **Bit-stream copy**
  - Exact bit-by-bit copy of the original storage medium
  - Capture includes meta-data and both active (known files) as well as inactive data (deleted file fragments)
  - To disk:
    - The destination disc must be wiped before acquisition
    - The destination disc must not be mounted
  - To file, aka bit-stream image (e.g., image.dd)
    - The file can be saved on a hard disc or other storage media

Linux tools for image creation and inspection

- Extract a disk image using the dd tool family
  - `dc3ddif=/dev/sda3of=/home/forensics/disk.imghash=md5log=/home/forensics/disk.log`
- Mount disk image/partition read only:
  - `mount-r/home/forensics/disk.img/mnt/mount_point`
- Obtain partition information:
  - `sfdisk -l disk.img`
  - `fdisk -lu disk.img`
- Can split (and mount) the image to individual partitions
  - `dd if=disk.img bs= 512 skip=xxx count=xxx of=partition.dd`

Data acquisition over the network

- We can create an image file over the network
  - Transmitting data from source media over network and write data to file
- How to:
  - First, prepare the lab computer (IP address 192.168.0.11) for the reception of data
    - `netcat -l -p 9000 | dd of=file.dd`
  - Then, start the transmission on the source computer
    - `dd if=/dev/hda | netcat 192.168.0.11 9000`

A computer has been found in the crime scene and it is powered off.

What would you do?

What happens when the computer is turned on

- Evidence can be tampered with or even destroyed!
  - Files in the boot process are modified
  - Autorun features / boot up scripts
  - Malware executed upon boot

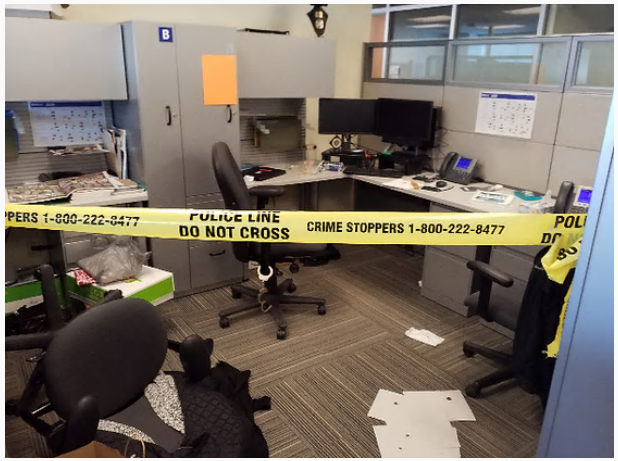
What happens when the computer is turned on

- Evidence can be tampered with or even destroyed!
  - Files in the boot process are modified
  - Autorun features / boot up scripts
  - Malware executed upon boot

If the computer is off, leave it off!

Seizing a computer

- Tape over the power receptacle on the back of the computer
- Bag the power cable in an evidence bag along with an evidence tag



  - If the computer is a laptop, open it and remove the battery; bag the battery with an evidence tag

What if you can't bring the entire computer?

- Bring the hard disks
  - Need to open the computer's case and extract the hard disk
  - Then seize the hard disk

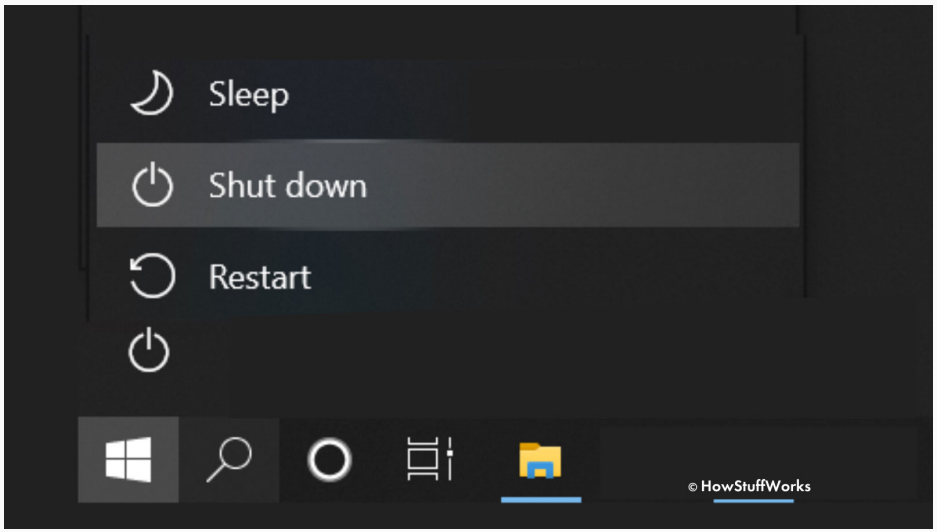
- If you can't bring the disk
  - Boot a trusted forensic OS (e.g., Kali) from DVD / USB drive
  - Identify the device that corresponds to the source disk
  - Perform a logical or bit-stream copy of the disk

A computer has been found in the crime scene and it is powered on.

What would you do?

Graceful shutdowns may change the data!

- Some files are usually updated on power off
- Shutdown services or scripts may have been changed!
  - e.g., delete folders containing incriminating evidence



Pull the power plug?

- In the past, most computer forensics experts recommended pulling the power cable on a computer right away
- Most experts agreed that you should not go to any extraordinary efforts to gather volatile data stored in RAM

Advantages of pulling the power plug

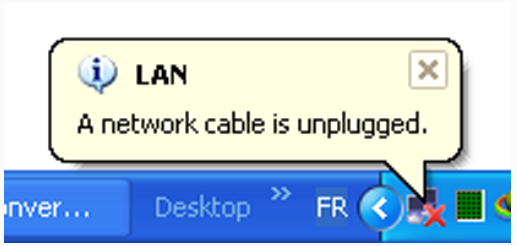
- May help preserve evidence, for example:
  - Any script the suspect has written that should execute upon shutdown doesn't get a chance to run
  - Temporary word-processing and other interim files remain on the hard drive, whereas they might get deleted if the software applications shut down more gracefully

Disadvantages of pulling the power plug

- Information may be lost by virtue of the volatility of data
  - RAM maintains process context information, network state information, and much more
  - Once a system is powered down, the contents of that memory are lost and cannot be recovered (usually)
- **Examples:**
  - On a suspect's computer there is an important message stored in RAM that will be lost if the computer is unplugged
  - In network intrusions, it is desirable to gather data related to active processes such as malware resident in memory

A similar dillema: Unplugging the network cable

- To prevent anyone from accessing systems from outside the crime scene, it is advisable to disable network connectivity
- However, this action can destroy evidence and eliminate investigative opportunities

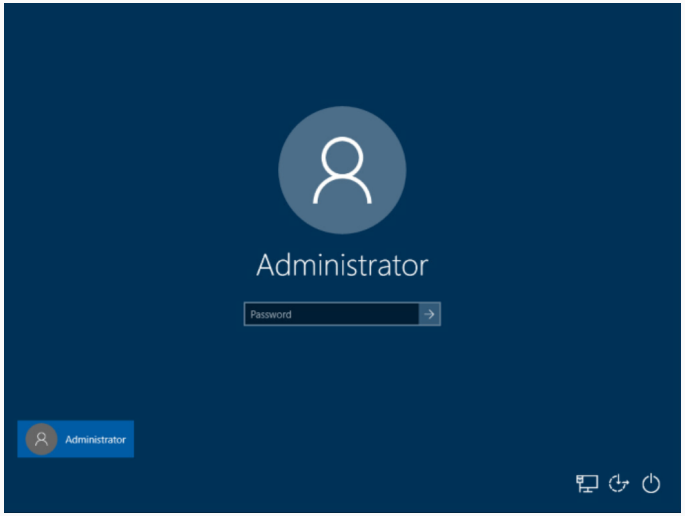


Disadvantages of disconnecting the network cable

- The opportunity to list the active connections to the system is lost: investigators may never know which other computers on the network might contain evidence
- In certain cases such as network intrusions, disconnecting network connections may eliminate an opportunity to gather network traffic of the perpetrator in action
- Furthermore, it can seriously impact a business: disconnecting an e-mail server or an e-commerce site's main transaction server can cause significant losses

First observation to make

- Is the system password protected?
  - If if is but there are logged-in accounts, switching off the computer may result in loss of credentials and prevent you from logging back in
    - It may be necessary to perform live forensics
  - If it is and there are no logged-in accounts, pull the power plug: there's not much one can do



Live forensics

- It may be necessary to perform operations on a system that contains evidence, especially in networked systems
- Live forensics vs. dead/postmortem forensics
  - Live: analysis is done on a live system
  - Dead/postmortem: analysis done on powered off system
- General procedure for live forensics:
  - The evidence system must be running and logged in
  - Ideally, run forensically sound tools from DVD or USB stick
  - Collect evidence to external storage or network share
  - Create log entry for every single command you execute

Live forensics

- **Files and network connections**
  - List open files
    - `lsof -nDr`
  - List network connections
    - `netstat -nap`
  - List network routes
    - `netstat -nr`
  - List deleted and open files
    - `ils -O /dev/hdaN`
  - List network addressess
    - `ifconfig`
- **Processes**
  - List processes
    - `ps -auxl`
  - Process memory
    - `pcat <PID>`
- **Users**
  - List active users
    - `who -iHl`
  - System info
    - `tar cf - /proc`

Useful data to collect in live analysis

- **Memory**
  - Memory dump
    - `LiME, AVML`
  - Swap space
    - `dd if=/dev/SWAPdev bs=2k`
- **Volumes and file systems**
  - Encrypted volumes
    - `dd if=/dev/hdaN bs=2k`
  - Temporary partitions
    - `dd if=/dev/TMPdev bs=2k`
  - File access times
    - `ls -alRu`
- **System-specific structures**
  - Windows registry
  - Windows event log
- **Applications**
  - Browsers
    - Password caches
    - Web cache
  - Cloud applications
    - Dropbox, etc.
  - Messaging & media
    - Email clients
    - Facebook accounts

Risk assessment before live forensics

- Different kinds of information: running processes, network connections, and data stored in memory
  - Memory may contain: decrypted applications, cryptographic keys, passwords, code that has not been saved to disk, etc.
- It may be worthwhile considering manual closure of various applications, but requires expert knowledge
  - Closing Microsoft Internet Explorer will flush data to the hard drive, thus benefitting the investigation and avoiding data loss
  - However, closing KaZaA (P2P app) could result in the loss of data

Collect evidence by which order?

- To ensure all relevant data is collected, you should prepare an order of volatility while gathering evidence
  - From the most volatile to the least
- Example of an OoV in a network intrusion investigation:
  1. ARP cache
  2. Process table
  3. Kernel statistics and modules
  4. Logs
  5. User files

Summary of approaches to data preservation

What to Preserve	Implications
Original hard drive	Any operations that are needed can be performed. Failure of the hard drive may render its contents inaccessible.
Forensic duplicate of original	The entire contents of the hard drive are preserved, including deleted hard drive data. This is generally done performing a bit-stream copy. However, it may be infeasible or not permitted under certain circumstances (e.g., large hard drives, legal protections).
Select files from original hard drive	Other files on the hard drive that may be relevant will not be preserved, and deleted data will not be preserved. For the selected files, important information or metadata may be lost or misinterpreted during acquisition.
Converted versions of files	For the selected files, important information or metadata may be lost or misinterpreted during conversion.
Relevant portions of files	Digital investigators only know what is relevant at a certain moment and may miss some relevant information, particularly if new facts come to light later.
Written notes detailing portions of files	The approach does not preserve the original digital evidence and is not feasible with large amounts of data.

Takeaways

- Data acquisition is a task that poses a number of obstacles for forensic analysis
- To forensically acquire data from computers, many factors must be considered, e.g., whether to power off the computer, unplug the network cord, etc.
- There is no silver bullet: often, one needs to decide based on the specific case, always in the interest of acquiring most evidence with least amount of change

Pointers

- **Textbook:**
  - Casey – Chapters 7 & 15.3 & 16.4 & 22.3
- **Other resources:**
  - A Guide for First Responders (USDJ)
- **Acknowledgements:**
  - Slides adapted from Nuno Santos's Forensics Cyber-Security course at Técnico Lisbon