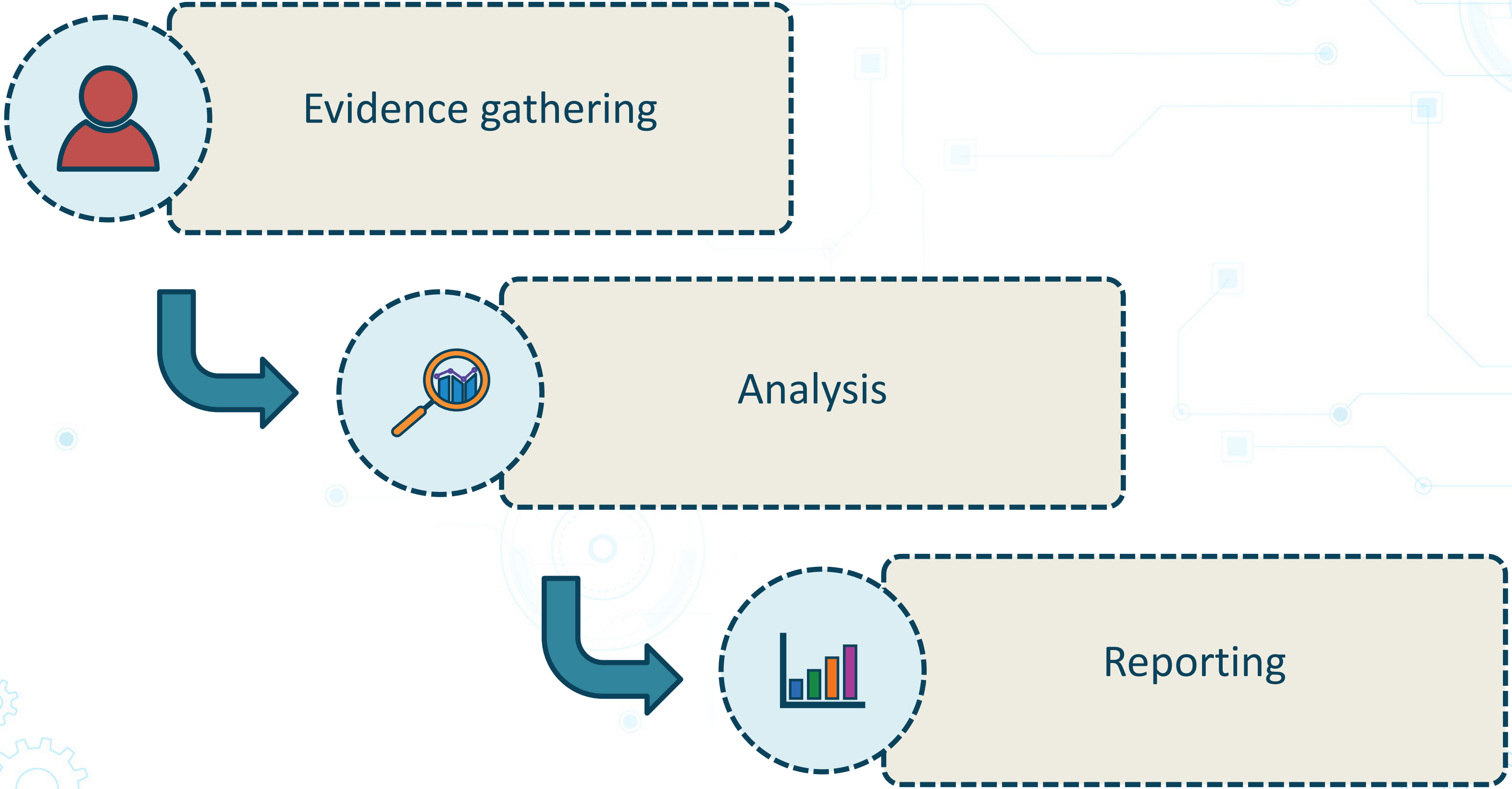
Digital Forensics

- The application of computer science and data recovery to the law
- Specific investigative techniques
  - Potential legal evidence

The Digital Forensics Process



Evidence gathering

Analysis

Reporting

Digital Forensics Results

What happened?

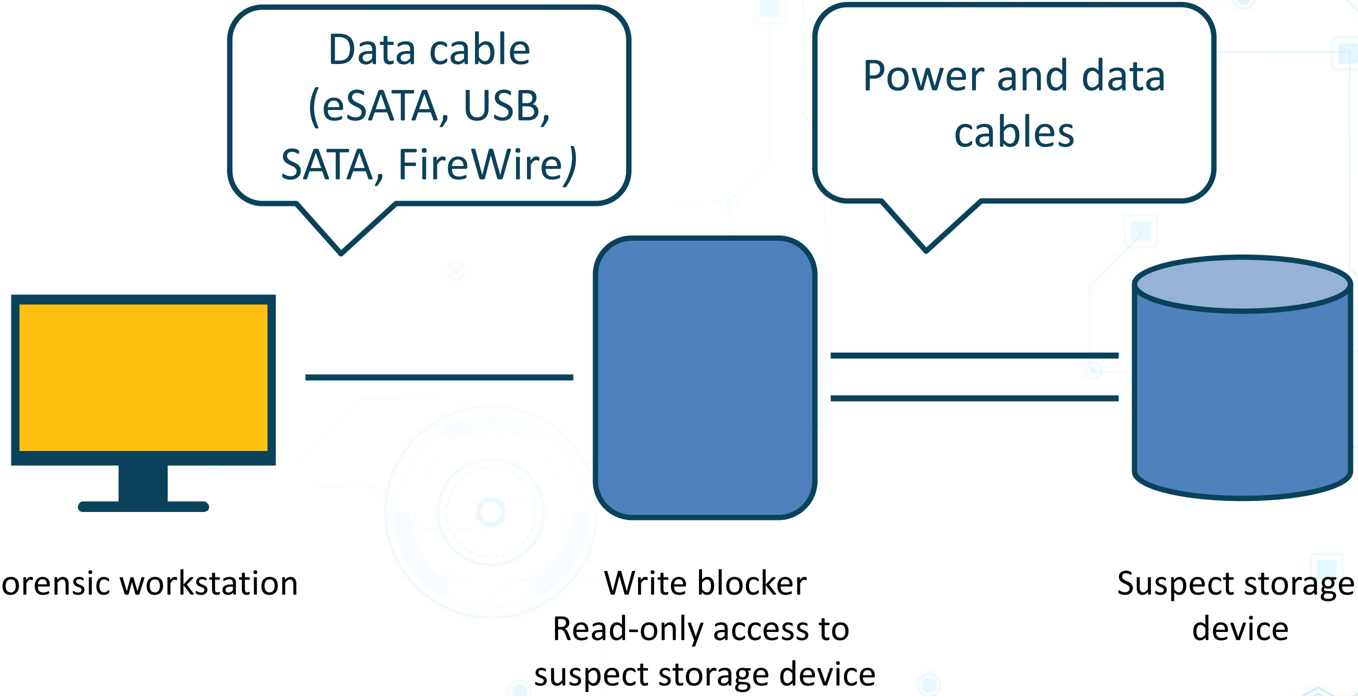
When did it happen?

Who was involved?

Digital Forensics Hardware

- Digital forensics workstation
- Hard drive imaging hardware
  - Faster than software drive imaging tools
  - Compatibility issues with some drives
- Mobile device acquisition tools

External Hardware Write Blocker

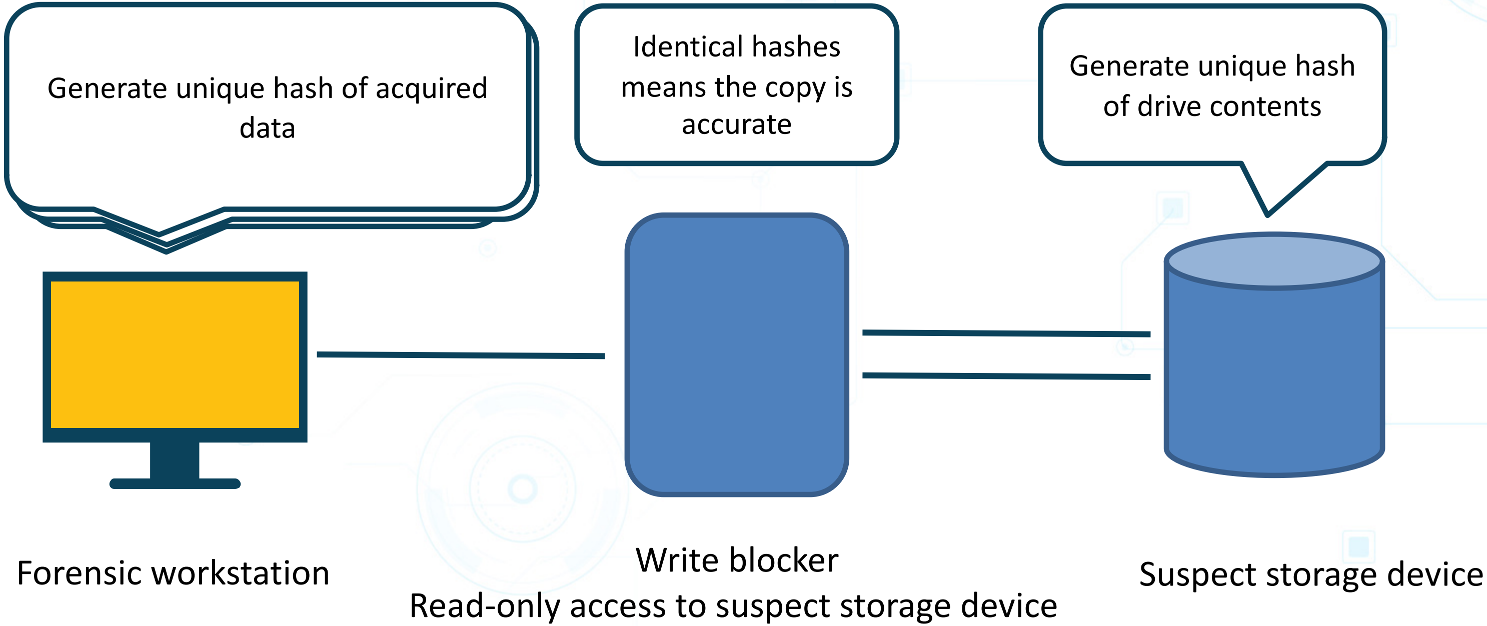


Data cable (eSATA, USB, SATA, FireWire)
Power and data cables
Forensic workstation
Write blocker
Read-only access to suspect storage device
Suspect storage device

Digital Forensics Software

- Installed on forensic workstation
- Hard drive imaging
- Data recovery
- Memory dump/image file analysis

Software Disk Image Acquisition



Generate unique hash of acquired data

Identical hashes means the copy is accurate

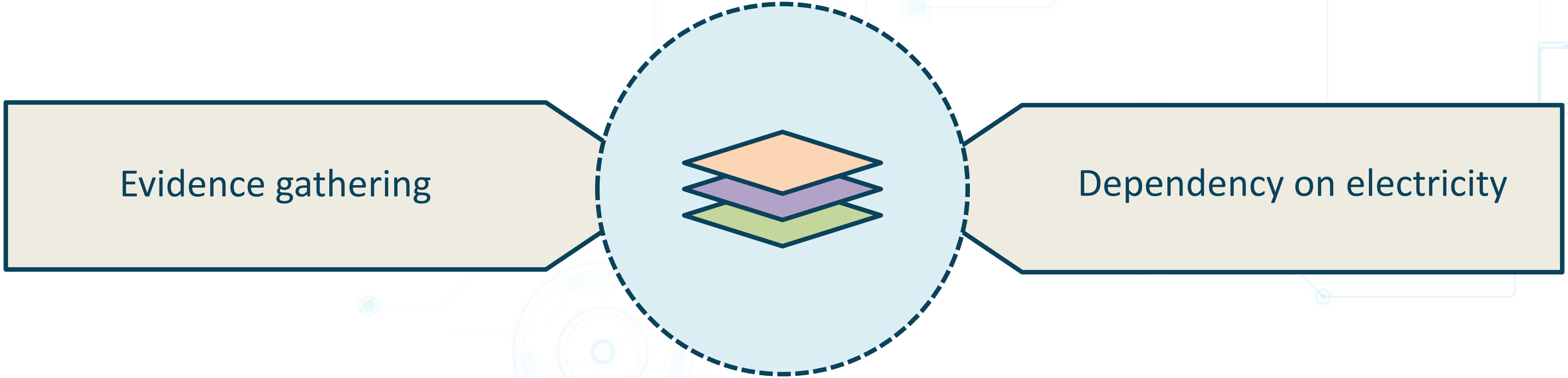
Generate unique hash of drive contents

Forensic workstation

Write blocker
Read-only access to suspect storage device

Suspect storage device

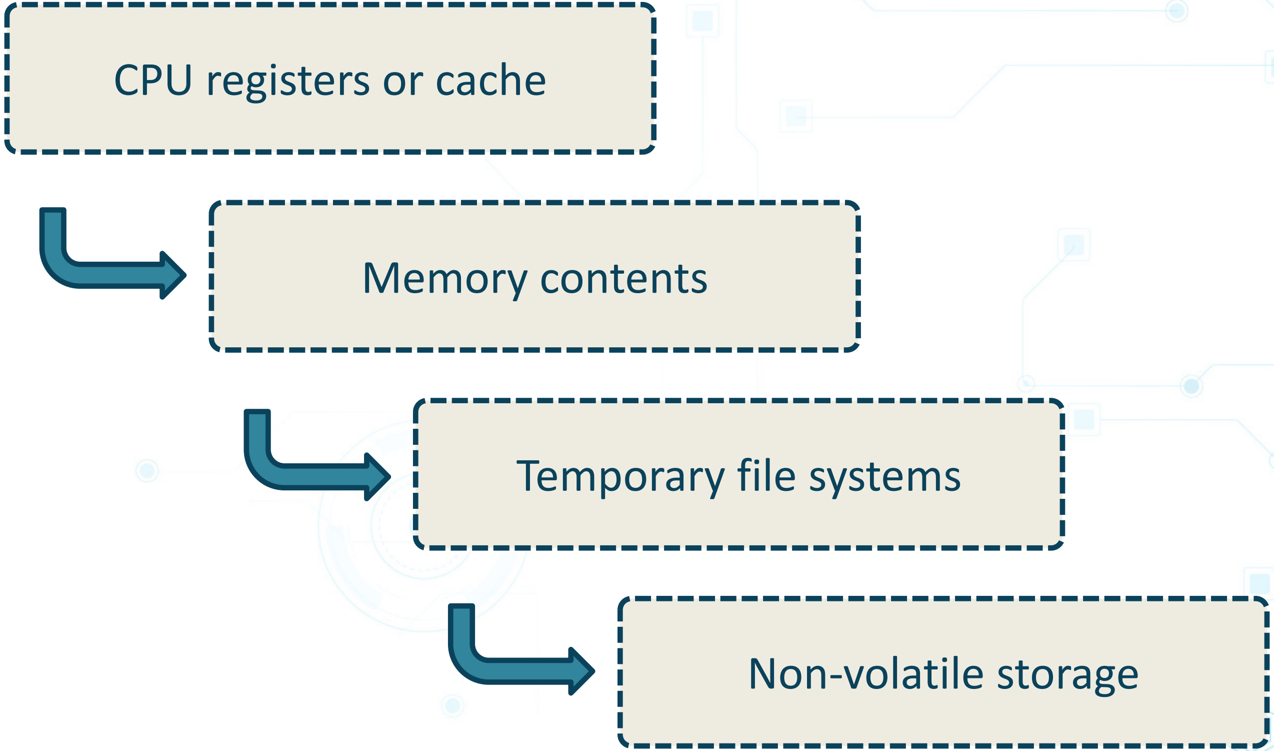
Order of Volatility



Evidence gathering

Dependency on electricity

Order of Volatility



CPU registers or cache

Memory contents

Temporary file systems

Non-volatile storage

Chain of Custody

- Evidence gathering - how?
- Evidence storage - where?
- Evidence access - who?

Evidence Gathering

- First responders
- Always work from a copy of digital data
- Imaging/cloning
- Write-blocking
- Prevent changes to data

Evidence Gathering Examples

- Turn off suspect mobile phone and remove batteries
- Faraday bag
- Take photographs of equipment/computer screens
- Scanner/printer document history
- Security camera footage

Evidence Storage

- Antistatic bags
- Detailed labeling
- Evidence access log
- Climate-controlled storage rooms
- Internal batteries (date/time) and long-term storage

Sample Chain of Custody Form

Case #: **Offense Type:** **First responder ID:** **Suspect ID:** **Date/time:** **Location:**	

Label #:	Date/Time:	Release ID:	Receive ID:	Location/Comments:

In this exercise, you will

- Describe how forensic disk write blockers work
- Describe the evidence order of volatility
- Describe how evidence integrity can be proven
- Use the Linux `dd` command to acquire a disk image

Write Blocker

- Prevents writing to suspect storage device
- Sits between forensic workstation and suspect storage device

Order of Volatility

1. CPU registers or cache
2. Memory
3. Temporary file systems
4. Non-volatile storage

Evidence Integrity

- Chain of custody
  - Document evidence gathering, storage, transfer and use
- Hashing
  - Detect changes