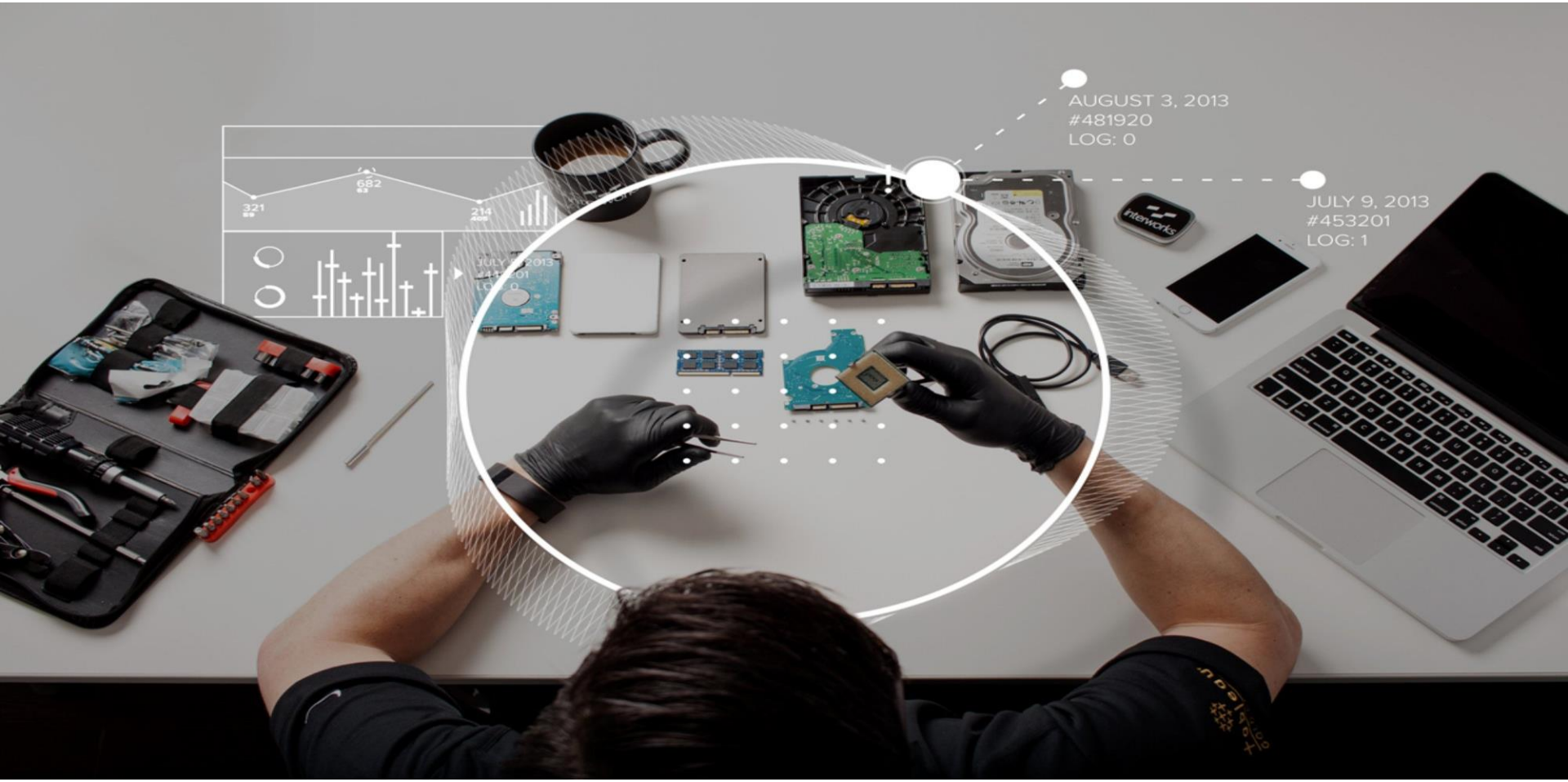


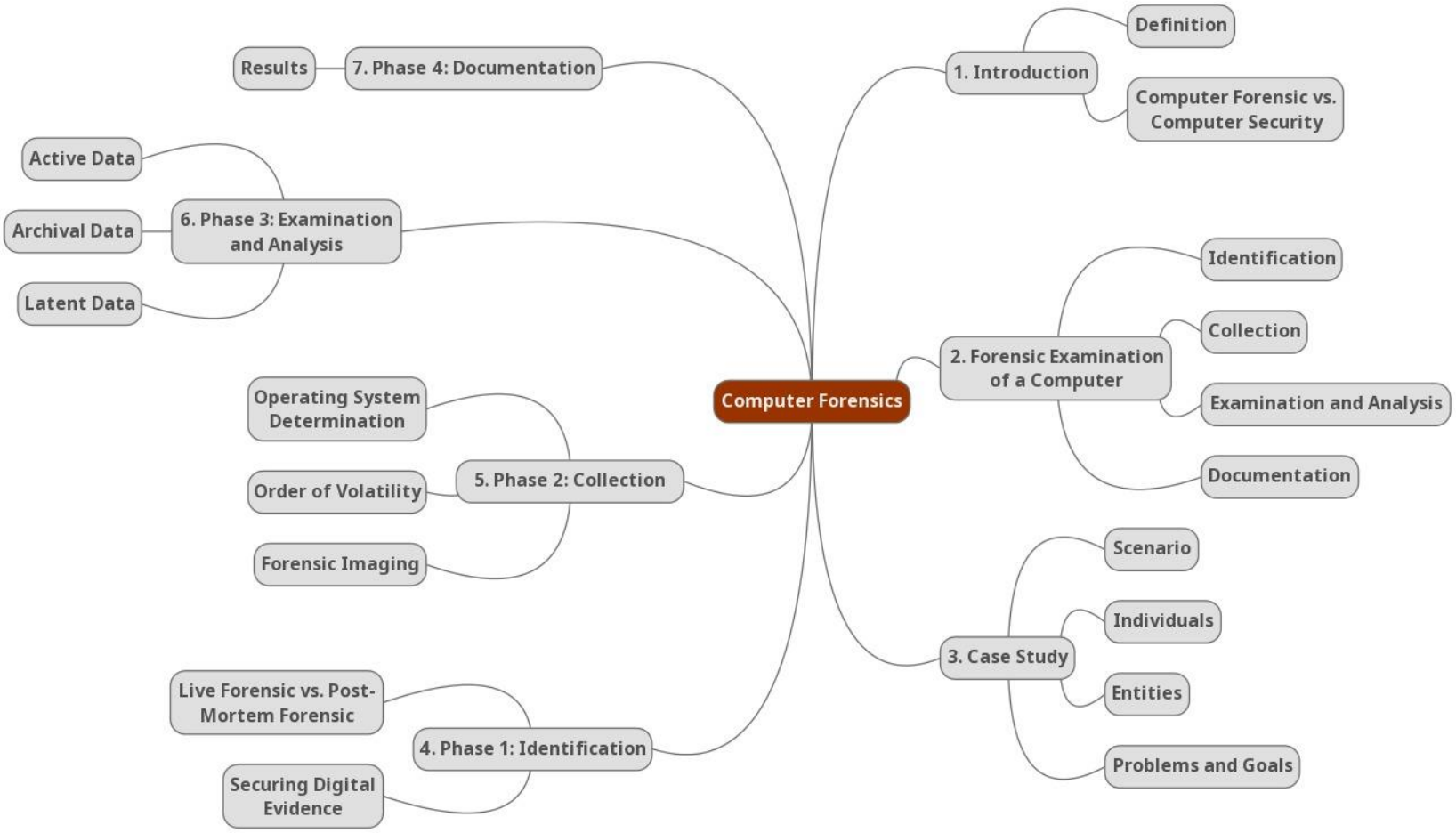
Chapter 4: Computer Forensics

Introduction to Digital Forensics

Fröhlich, Hosh | 06.11.2018

https://thecybersecurityplace.com/wp-content/uploads/2017/11/DF1.jpg

Slide 2


Computer Forensics
1. Introduction
Definition
Computer Forensic vs. Computer Security
2. Forensic Examination of a Computer
Identification
Collection
Examination and Analysis
Documentation
3. Case Study
Scenario
Individuals
Entities
Problems and Goals
4. Phase 1: Identification
Live Forensic vs. Post-Mortem Forensic
Securing Digital Evidence
5. Phase 2: Collection
Operating System Determination
Order of Volatility
Forensic Imaging
6. Phase 3: Examination and Analysis
Active Data
Archival Data
Latent Data
7. Phase 4: Documentation
Results

Literature

- Forensic Analysis of BIOS chips:
  - https://pdfs.semanticscholar.org/8c9c/52eb996937bd216415447c2cc01b8027e1a6.pdf
- Data Carving Techniques:
  - https://www.sans.org/reading-room/whitepapers/forensics/data-carving-concepts-32969
- Windows Registry Forensics:
  - https://pdfs.semanticscholar.org/e802/7056bc7995187457cd61df86c9a13df7d05d.pdf

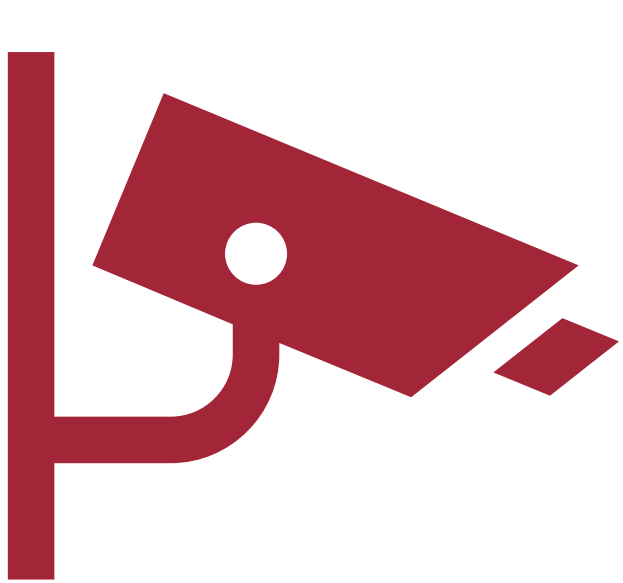
Computer Forensics

Computer Forensics

“Computer forensics is the practice of collecting, analysing and reporting on digital data in a way that is legally admissible .”

http://siginvestigations.com/wp-content/uploads/2014/08/Dollarphotoclub_21941919.jpg

Computer Security vs. Computer Forensics

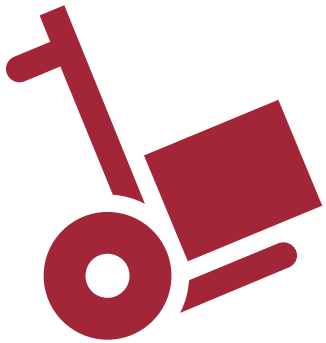


Forensic Examination of a Computer

Four Phases of a Forensic Examination

Identification

Collection



Examination

Documentation

Case Study

Individuals

Alice: CEO

Bob: Shredding Officer

Charlie: Disposal Officer

Dave: Hardware Merchant

Grace: Forensic Investigator

Frank: 3rd Party Investigator

Eve: Black Market Hacker

Scenario

- Bob unhappy with paycheck
- Bob sells hardware to Dave
- Dave sells hardware on black market
- Eve buys hardware, reconstructs data
- Government sues Alice’s company
- Forensic investigation, Bob primary suspect

Entities

- Turned on
- Windows 10
- Unlocked
- HDD & SSD
- WLAN

Problems & Goals

http://www.justshovelmysnow.com/wp-content/uploads/2015/12/Fotolia_86265174_XL-768x662.jpg

Identification Phase

Live Forensics
vs.
Post-Mortem Analysis

Live Forensics vs. Post-Mortem Analysis

- Turned On
- Volatile Data
- During Incident

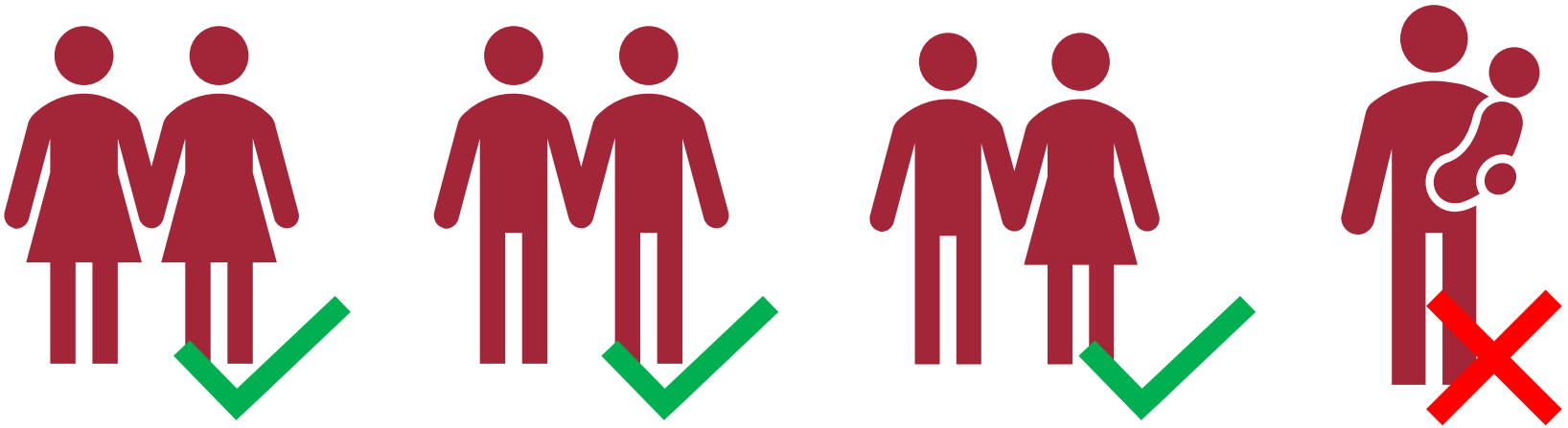
- Turned Off
- Persistent Data
- Post Incident

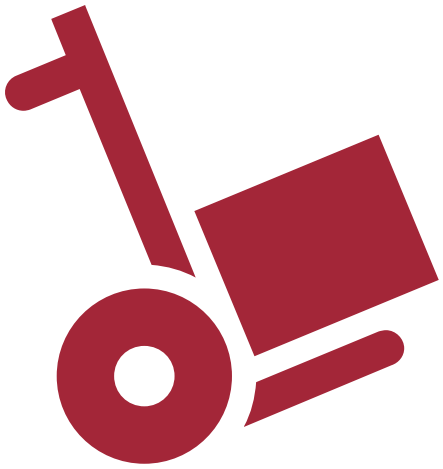
RAM

Random
Access
Memory

https://images.cutimes.com/cutimes/article/2015/07/16/vault.jpg

Double Verification Principle





Collection Phase

CMOS

Complementary
Metal
Oxide
Semiconductor

BIOS

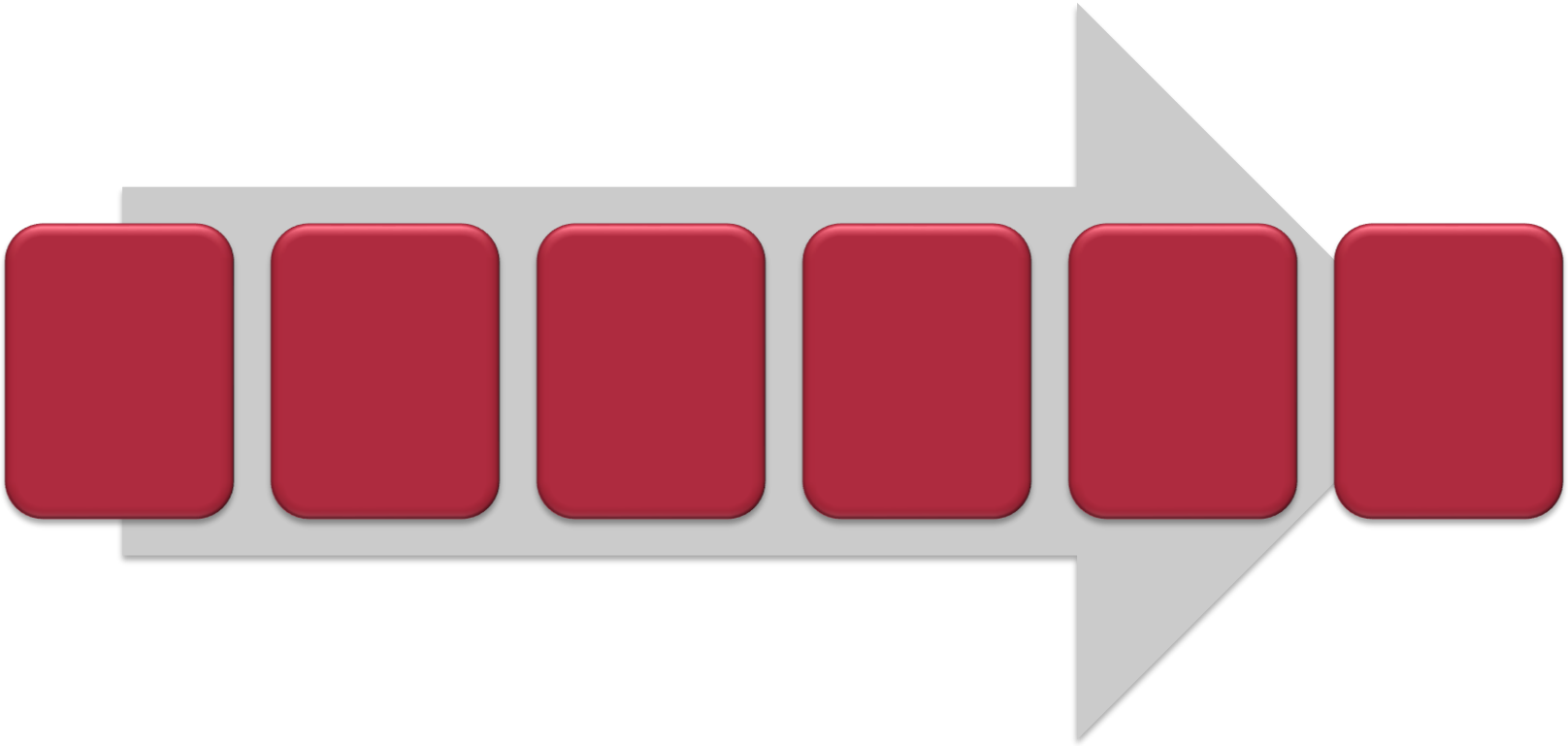
Basic
Input
Output
System

BIOS Demo

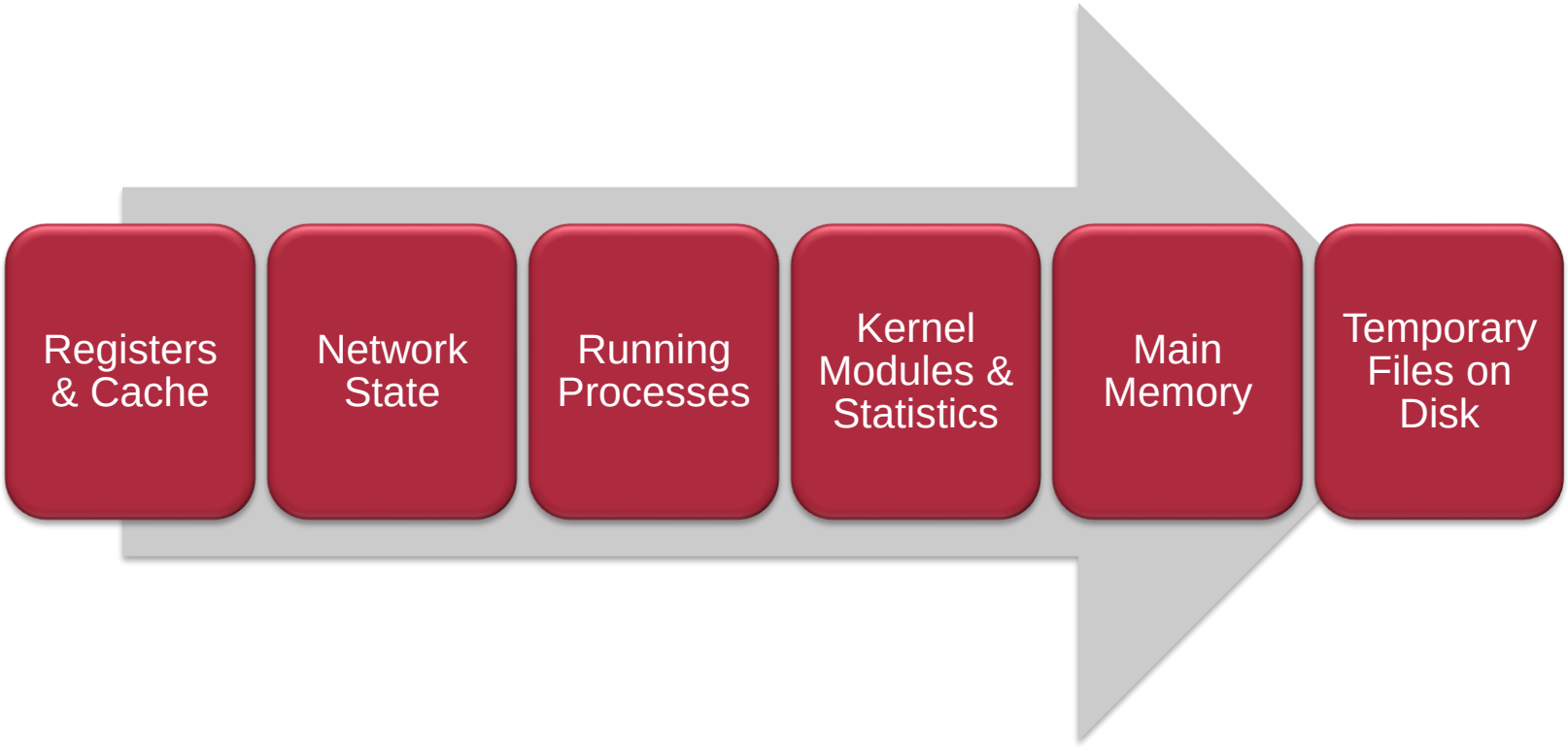
Operating System Determination

- Windows
- Linux
- Mac OS

Order of Volatility



Order of Volatility



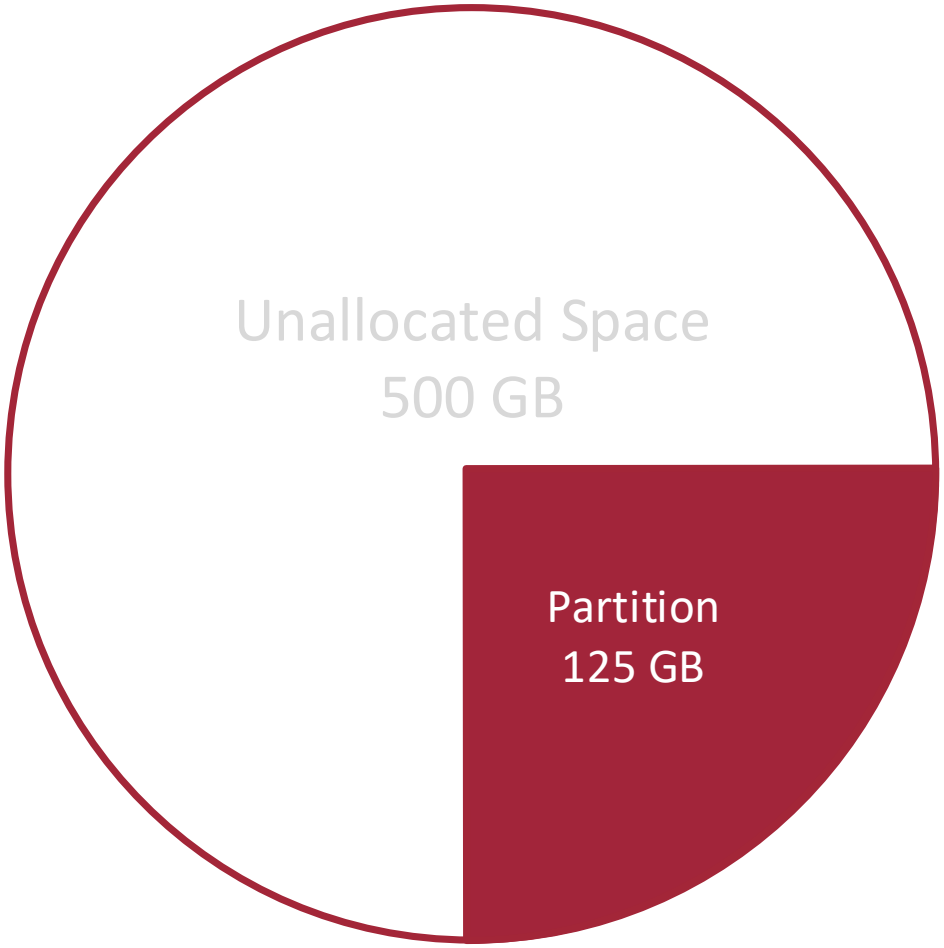
Forensic Imaging

https://saaers.files.wordpress.com/2017/02/20160415_125239.jpg

Disk Structure

- **Partition**
- Volume
- File System

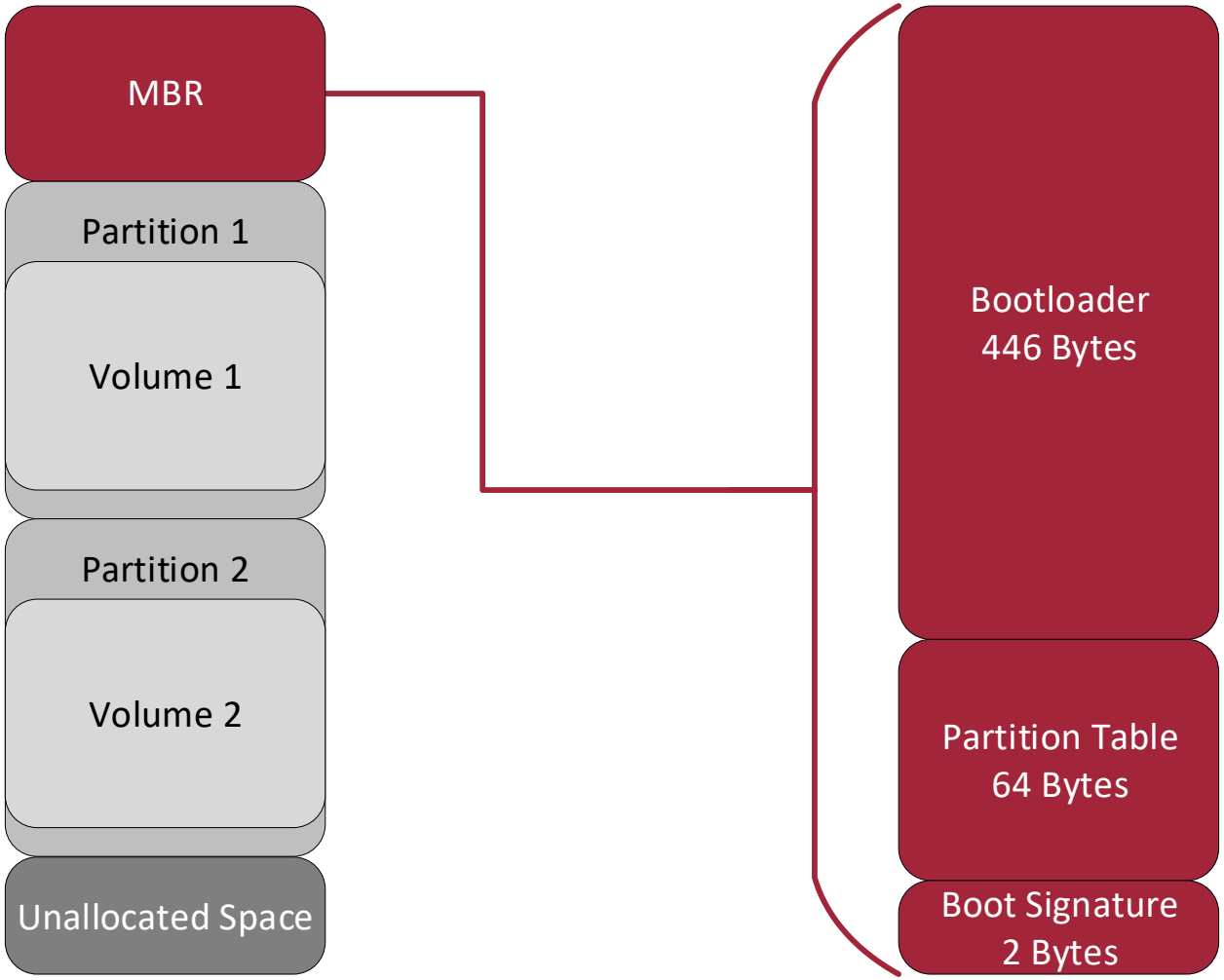
Partition



MBR

Master
Boot
Record

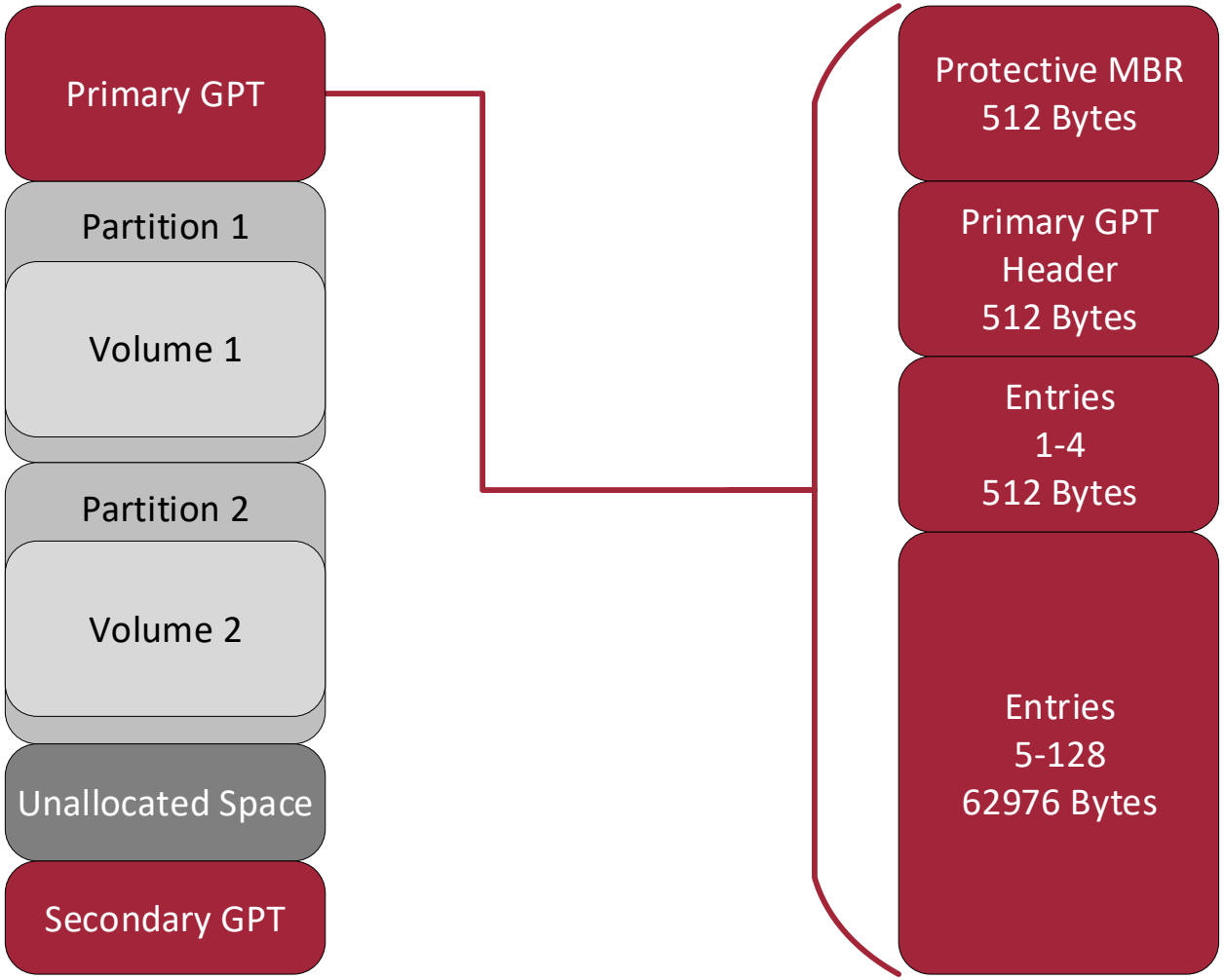
Master Boot Record



GPT

GUID (Global Unique Identifier)
Partition
Table

GUID Partition Table



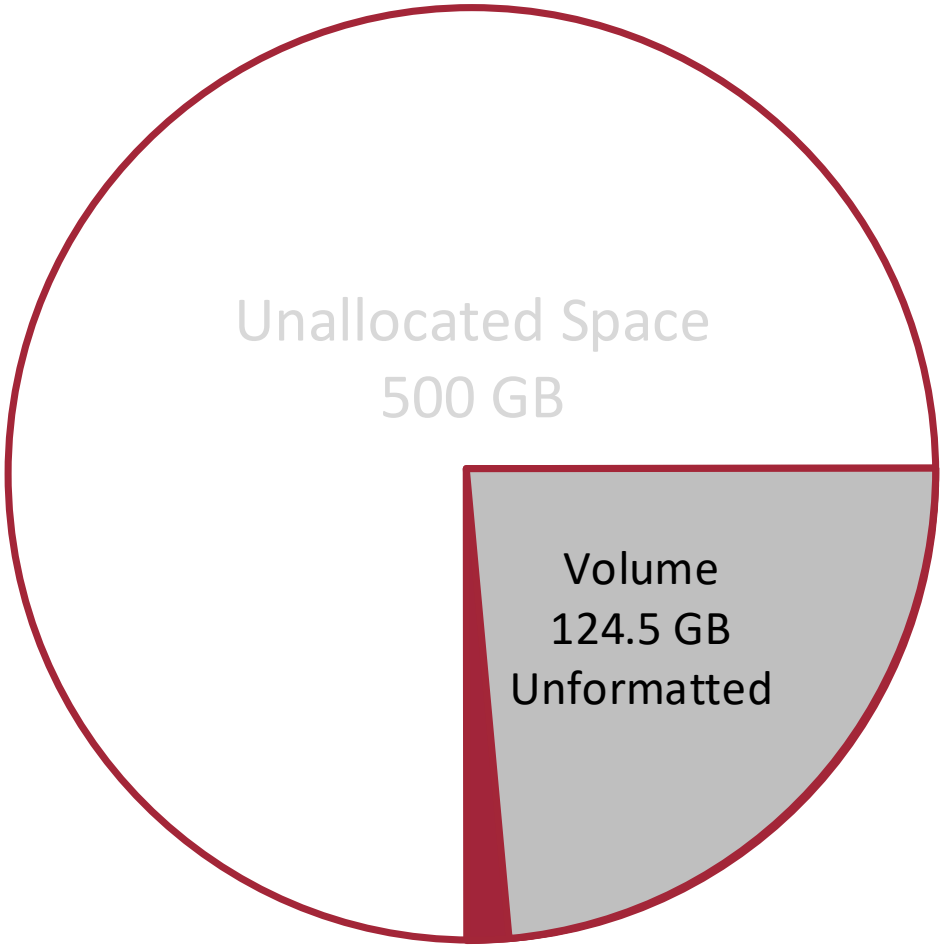
Partition Gap

https://s16353.pcdn.co/wp-content/uploads/2018/02/iStock_41541466_XLARGE-1.jpg

Disk Structure

- Partition
- **Volume**
- File System

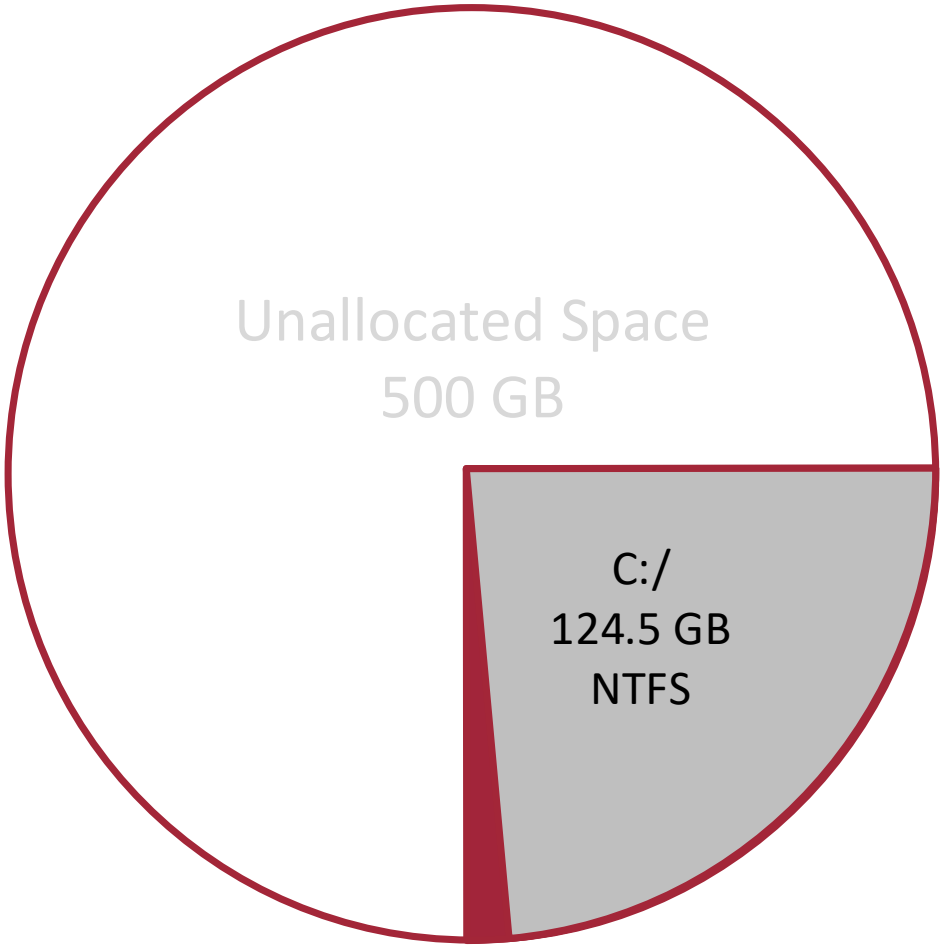
Volume



Disk Structure

- Partition
- Volume
- **File System**

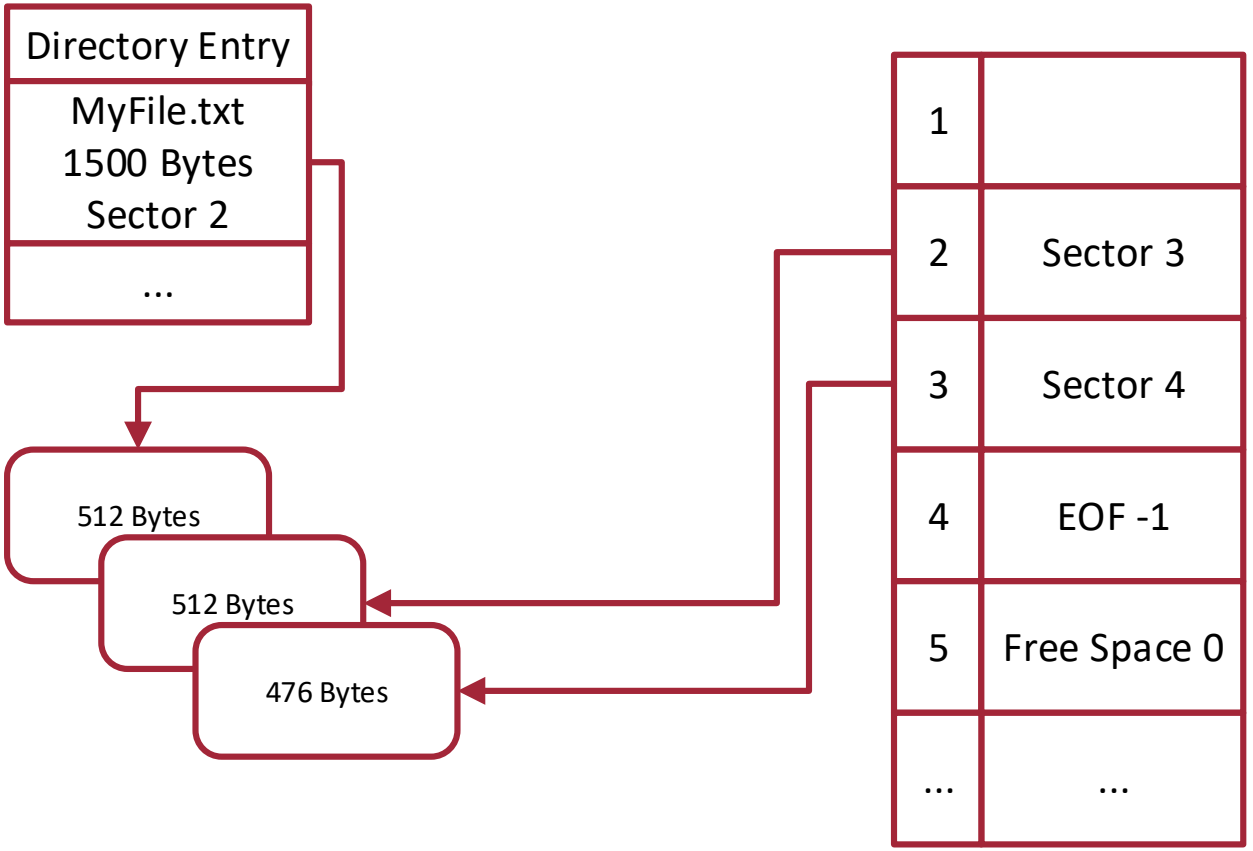
File System



FAT

File
Allocation
Table

File Allocation Table



NTFS

New
Technology
File
System

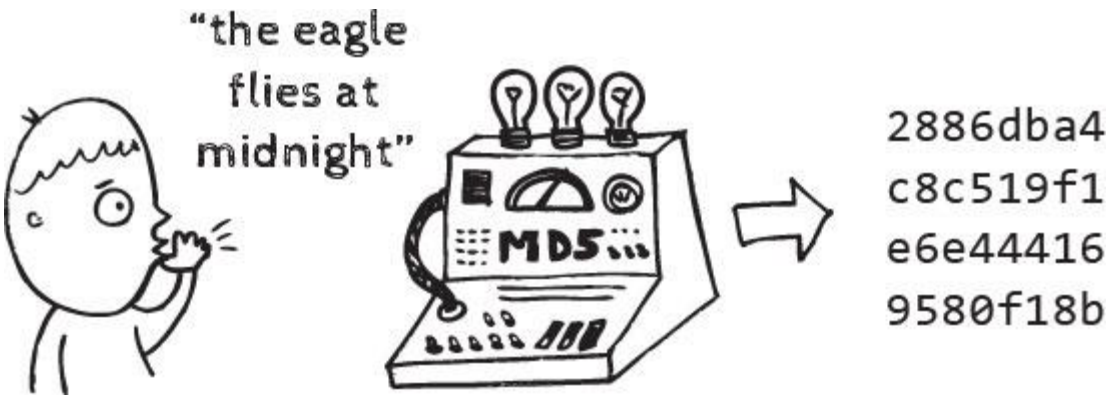
HFS

Hierarchical File System

EXT

Extended
File
System

File Hashing



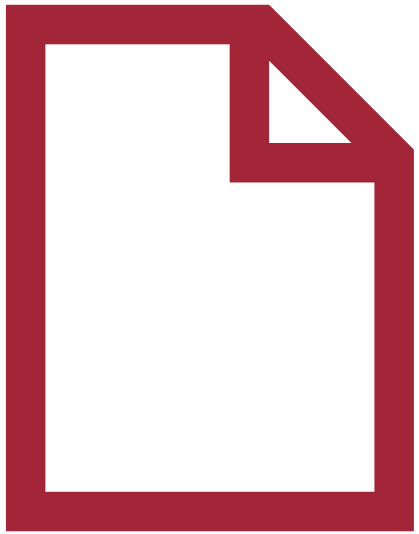
https://www.crypto-news.net/wp-content/uploads/2017/02/eagle.jpg

Examination & Analysis Phase

Exculpatory Evidence
vs.
Inculpatory Evidence

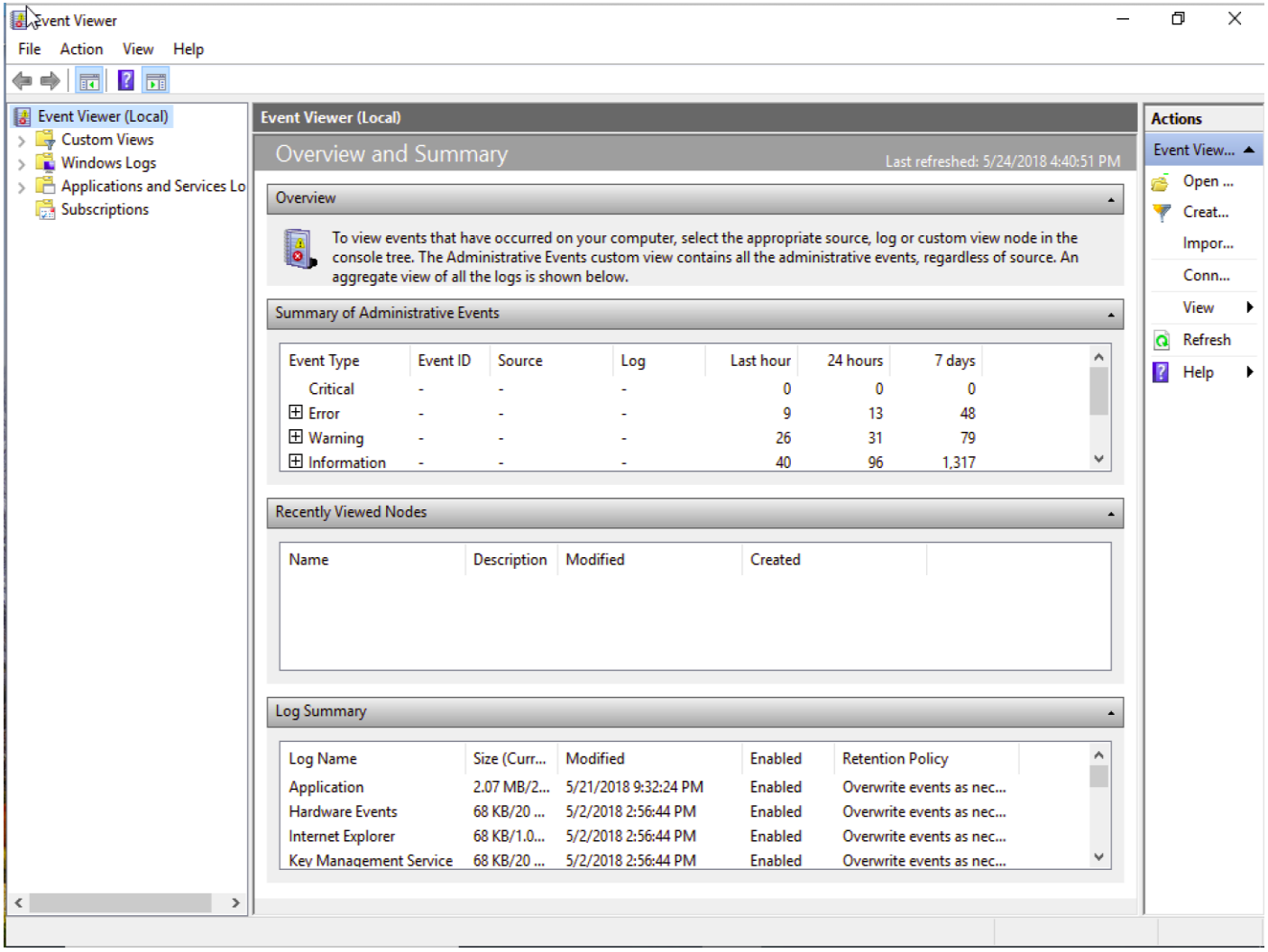
https://evidencesolutions.com/web/images/Article_Graphics/SouthDakotaComputerForensicsLabSDComputerForensicsExpert.JPG

Types of Data



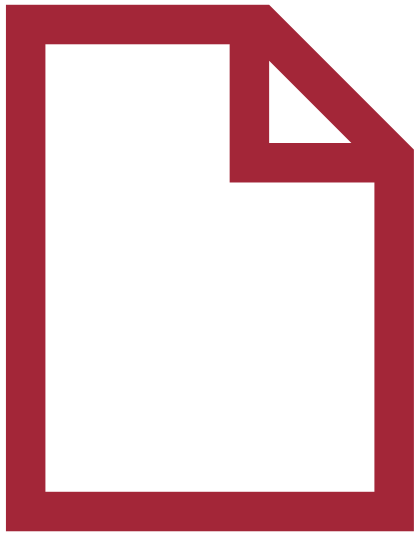
- **Active Data**
- Archival Data
- Latent Data

Log Files



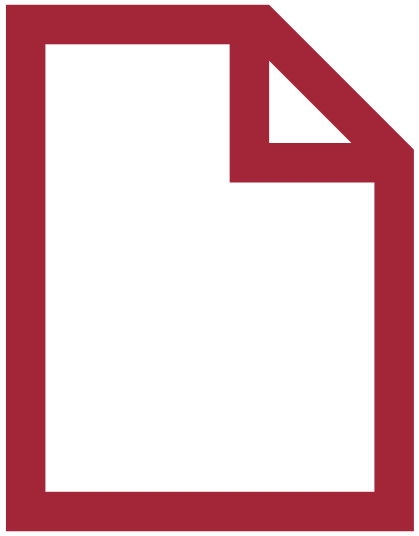
https://support.snapstream.com/hc/article_attachments/360006842554/Step2.png

Types of Data



- Active Data
- **Archival Data**
- Latent Data

Types of Data



- Active Data
- Archival Data
- **Latent Data**

ADS

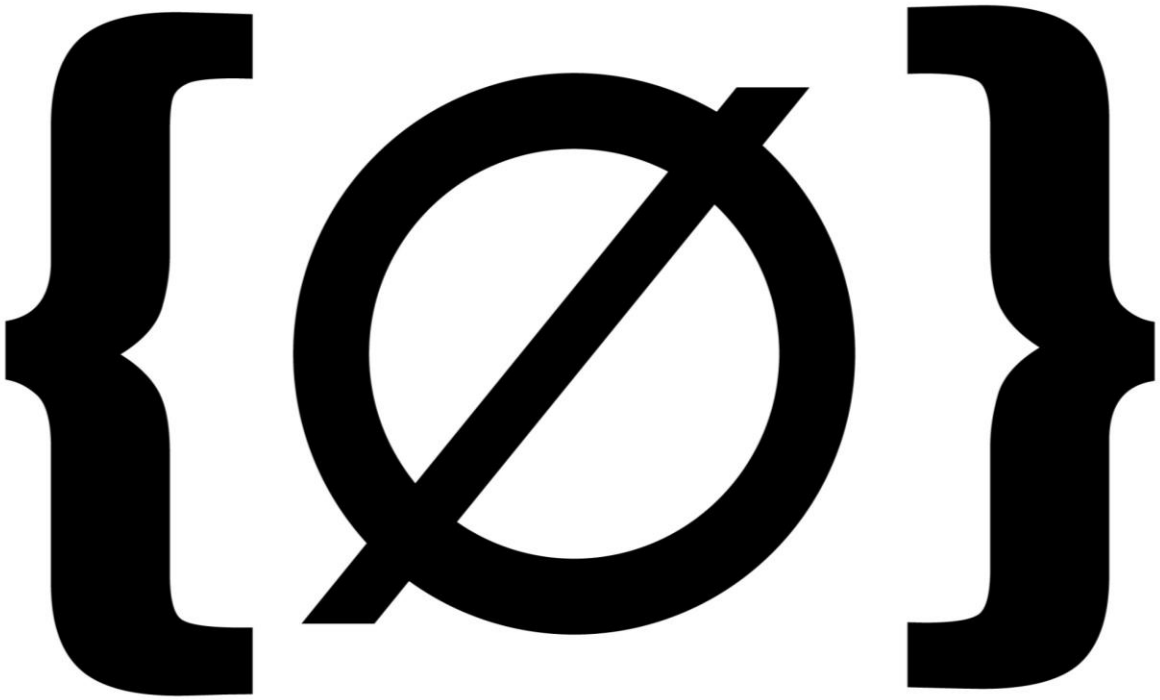
Alternative
Data
Streams

File Carving

File Carving

“File carving in digital forensics is a technique to restore deleted or fragmented files based on their headers.”

File Carving Demo

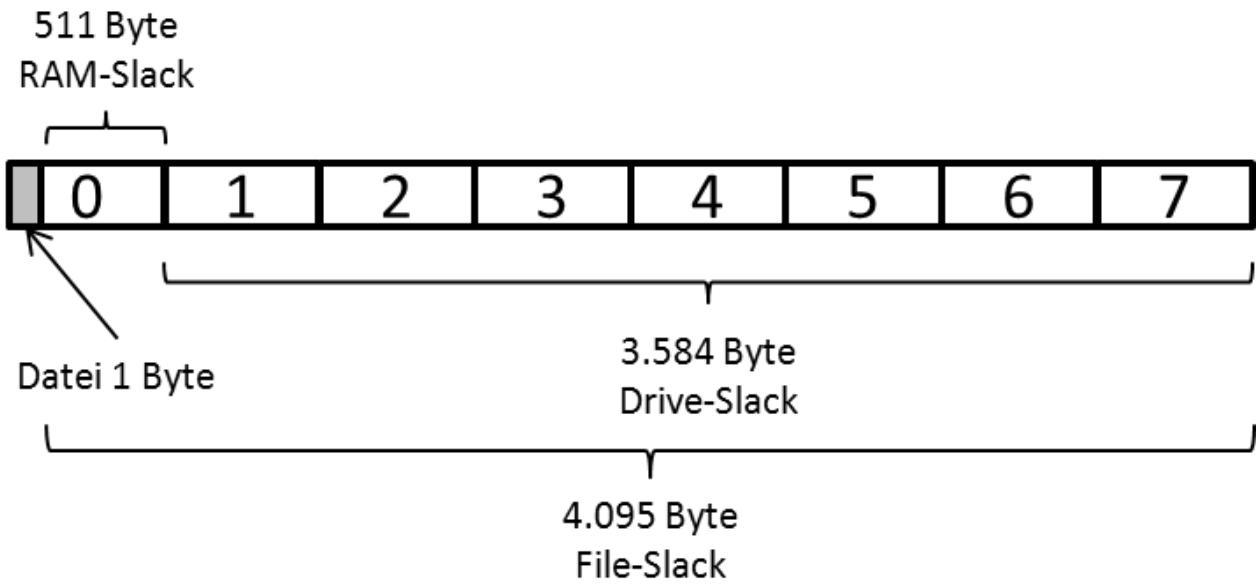


Unall{∅}cated

https://assets.bfg.org/system/logos/2355/original/Unallocated3.jpg

File Slack

File Slack


511 Byte
RAM-Slack
0
1
2
3
4
5
6
7
Datei 1 Byte
3.584 Byte
Drive-Slack
4.095 Byte
File-Slack

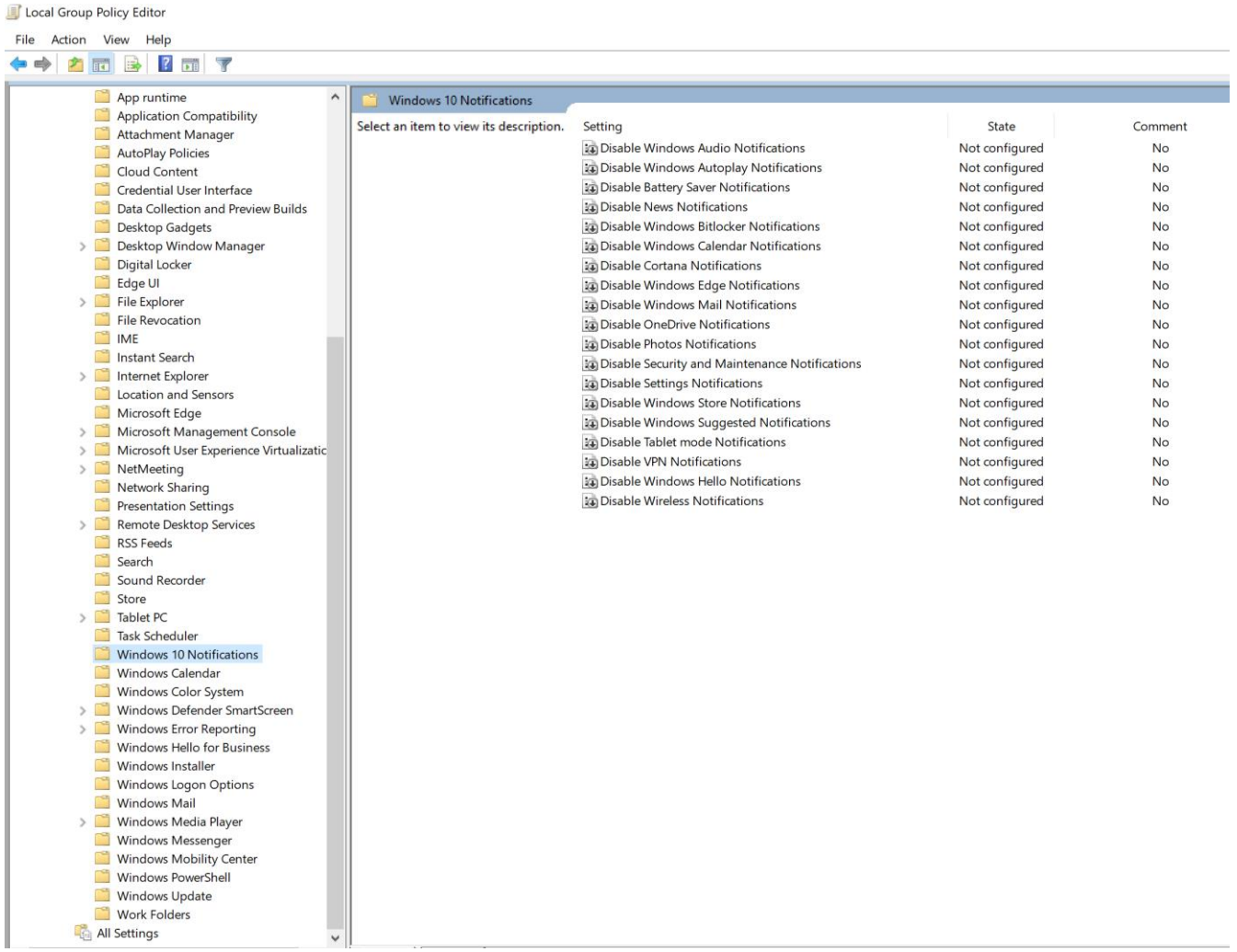
Metadata

“Metadata is descriptive data about actual data.”

MAC

Modified
Accessed
Created

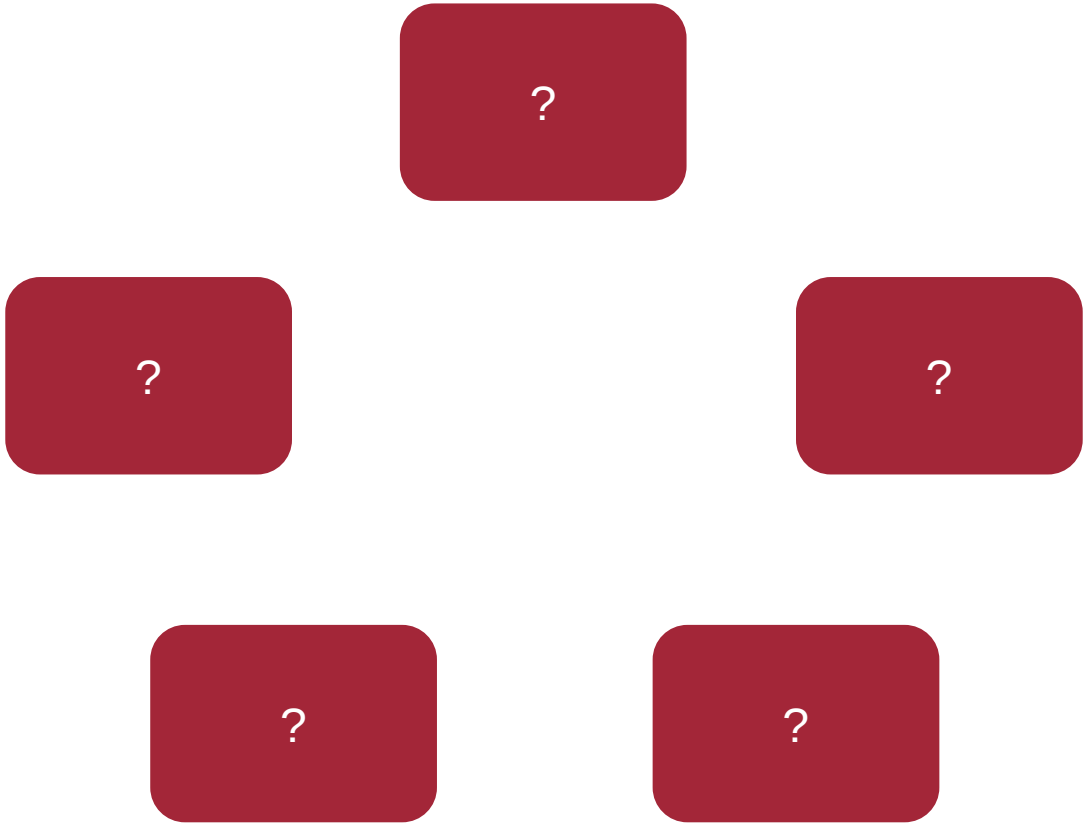
Windows Registry



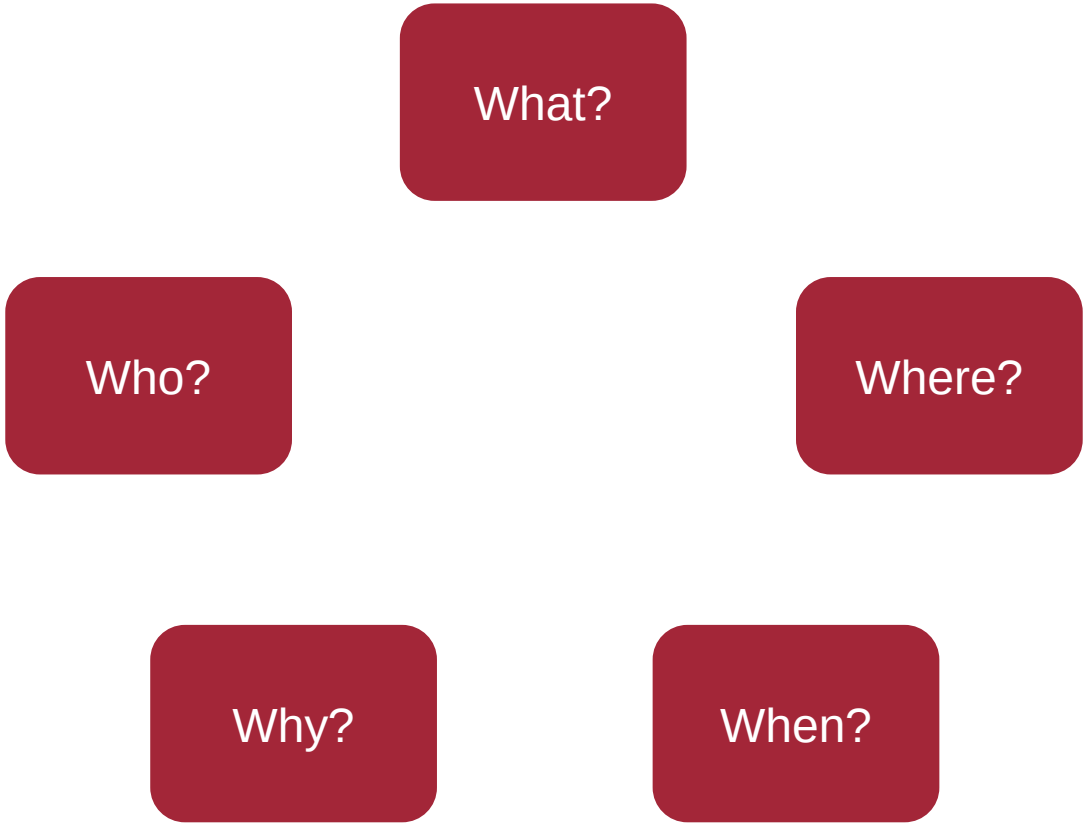
Windows Registry Demo

Documentation Phase

The 5-W’s



The 5-W’s



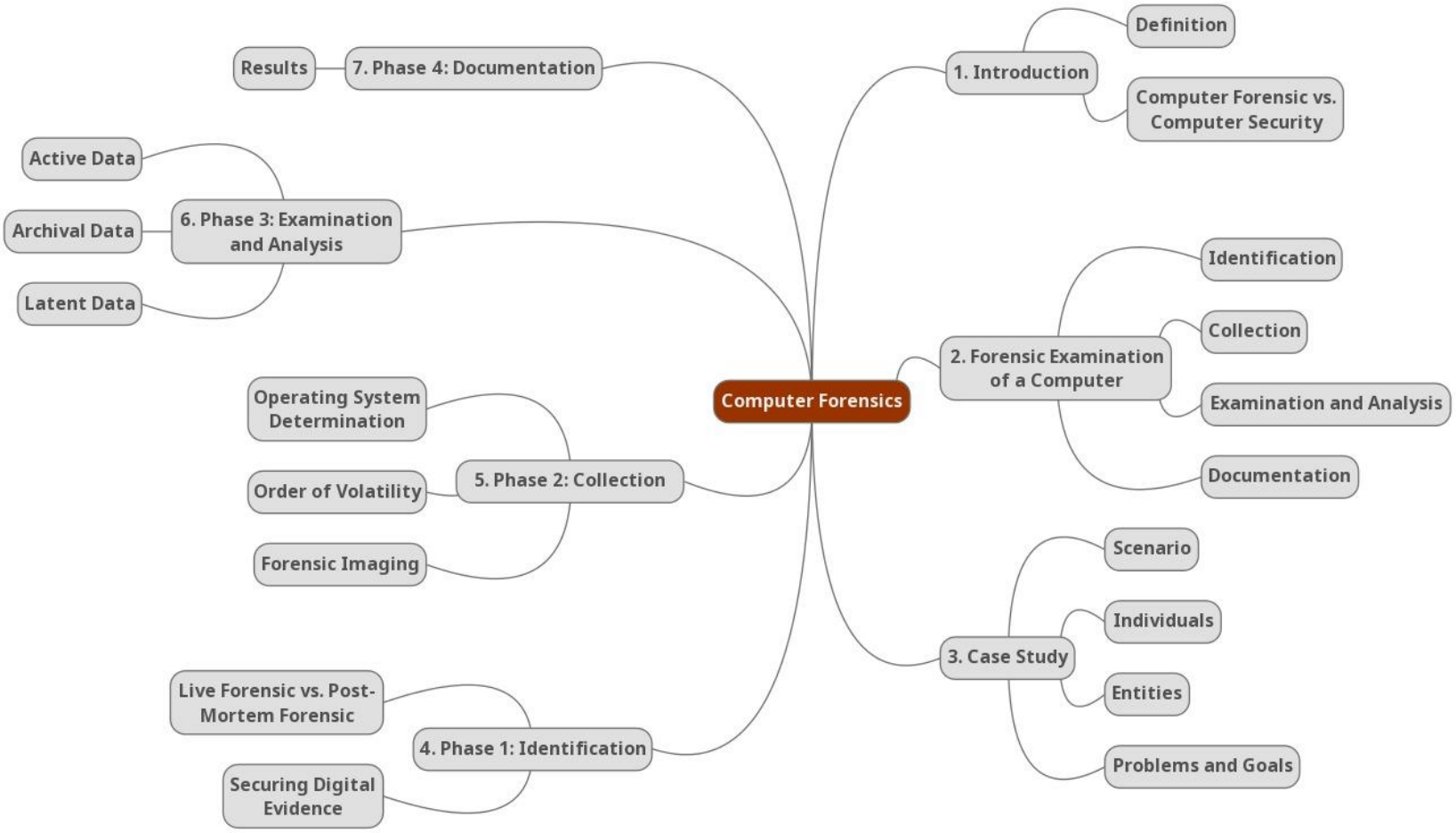
How & Lessons Learned

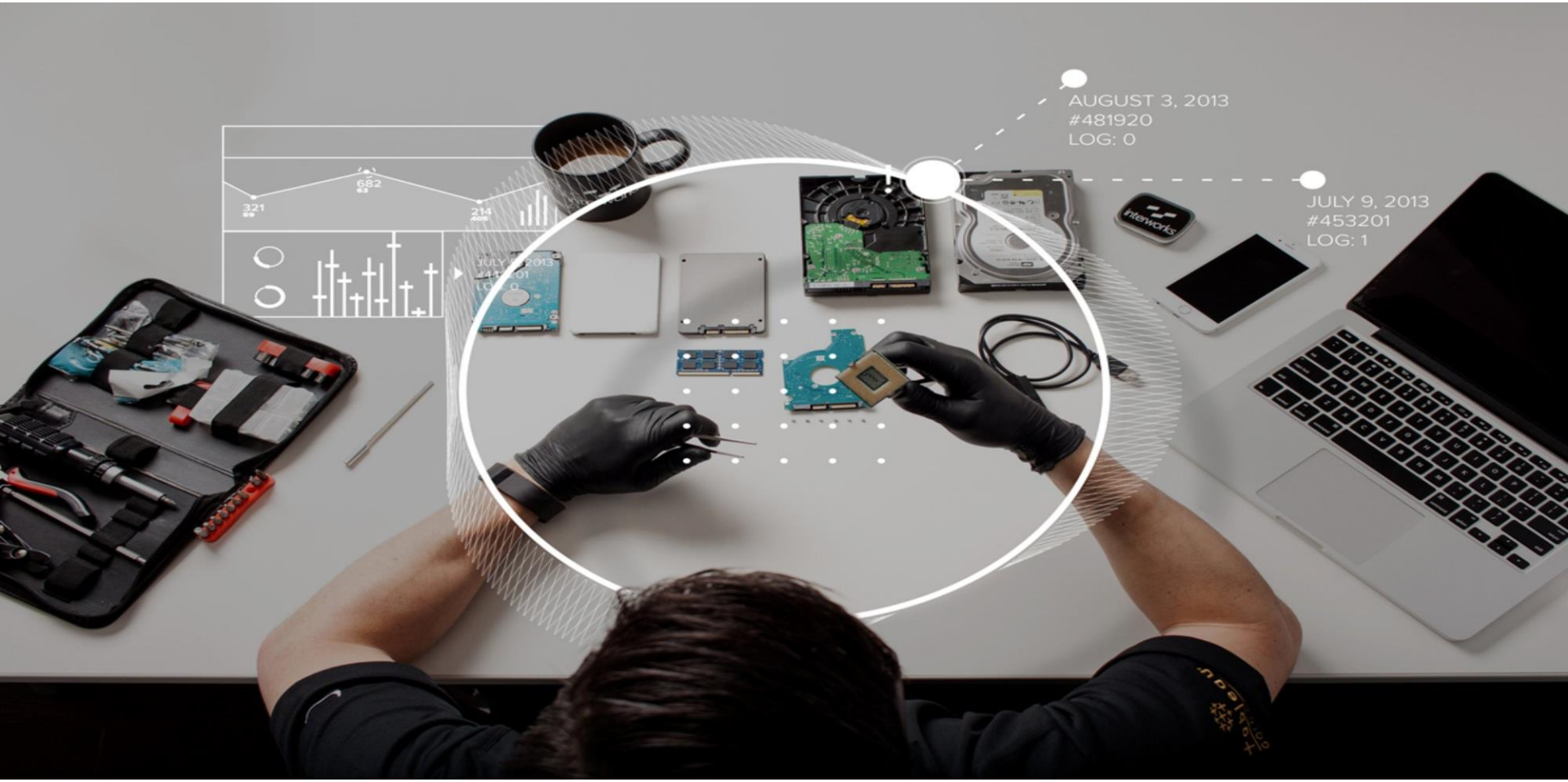
- How
- Lessons learned

Results

- What: Hardware missing
- Where: Alice’s company
- When: 18th of September, 2018
- Why: Disgruntled employee
- Who: Bob

https://d12m9erqbesehq.cloudfront.net/wp-content/uploads/2018/03/05085806/eventbrite-vs-eventsmart-compare_header.jpg


Computer Forensics
1. Introduction
Definition
Computer Forensic vs. Computer Security
2. Forensic Examination of a Computer
Identification
Collection
Examination and Analysis
Documentation
3. Case Study
Scenario
Individuals
Entities
Problems and Goals
4. Phase 1: Identification
Live Forensic vs. Post-Mortem Forensic
Securing Digital Evidence
5. Phase 2: Collection
Operating System Determination
Order of Volatility
Forensic Imaging
6. Phase 3: Examination and Analysis
Active Data
Archival Data
Latent Data
7. Phase 4: Documentation
Results



Chapter 4: Computer Forensics

Introduction to Digital Forensics

Fröhlich, Hosh | 06.11.2018

https://thecybersecurityplace.com/wp-content/uploads/2017/11/DF1.jpg