ulm university universität ulm

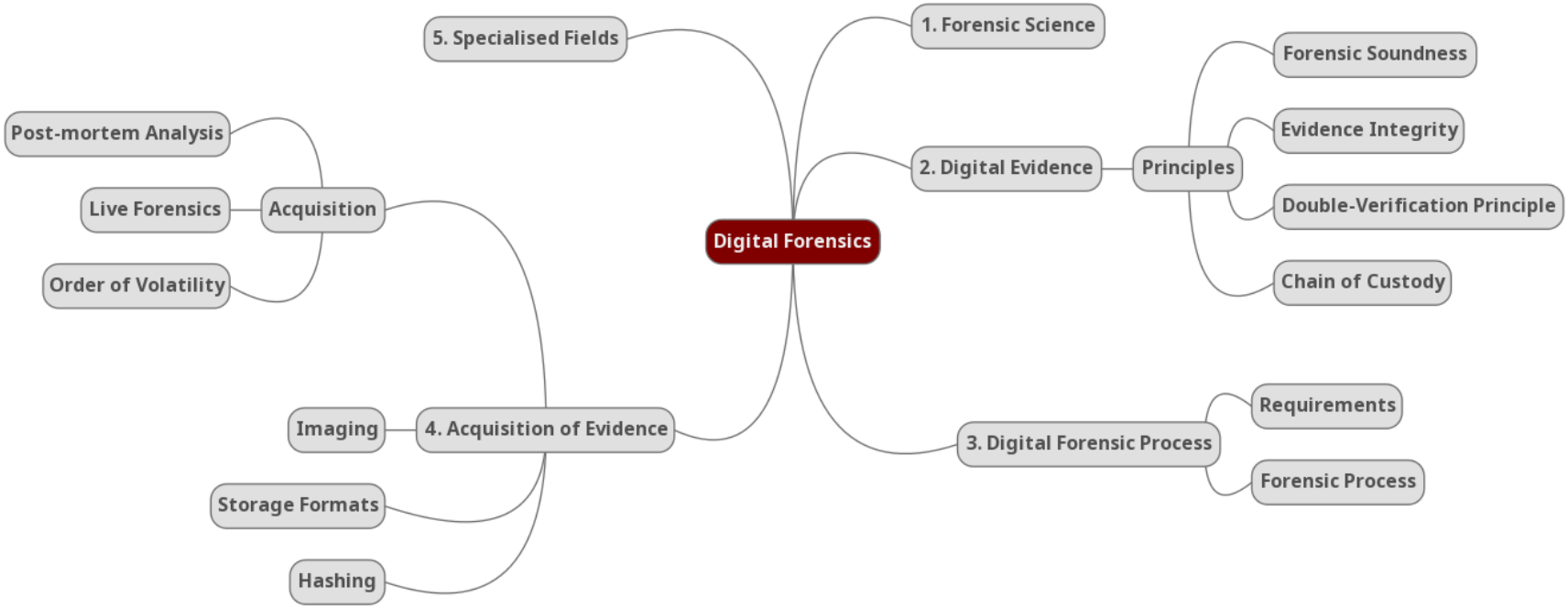
Chapter 2: Digital Forensics

Introduction to Digital Forensics

Fröhlich, Hosh

https://www.schlechtlaw.com/wp-content/uploads/2018/06/digital-forensics.jpg

Slide 2

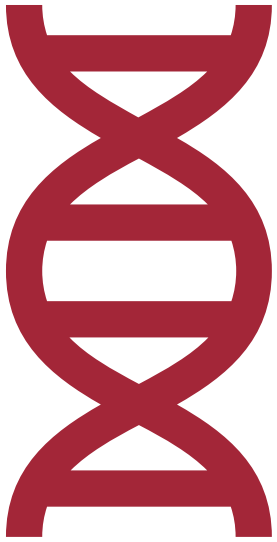

Digital Forensics
1. Forensic Science
2. Digital Evidence
Principles
Forensic Soundness
Evidence Integrity
Double-Verification Principle
Chain of Custody
3. Digital Forensic Process
Requirements
Forensic Process
4. Acquisition of Evidence
Acquisition
Post-mortem Analysis
Live Forensics
Order of Volatility
Imaging
Storage Formats
Hashing
5. Specialised Fields

Literature

- Computer Forensik: Computerstraftaten erkennen, ermitteln, aufklären
  - Alexander Geschonneck
- Digital Forensics
  - André Arnes et al.
- Leitfaden "IT-Forensik" des BSI
  - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=2
- Applying traditional forensic Taxonomy to digital Forensics
  - https://link.springer.com/content/pdf/10.1007%2F978-0-387-84927-0_2.pdf

Forensic Science

Forensic Science



Locard's Exchange Principle

Digital Forensics

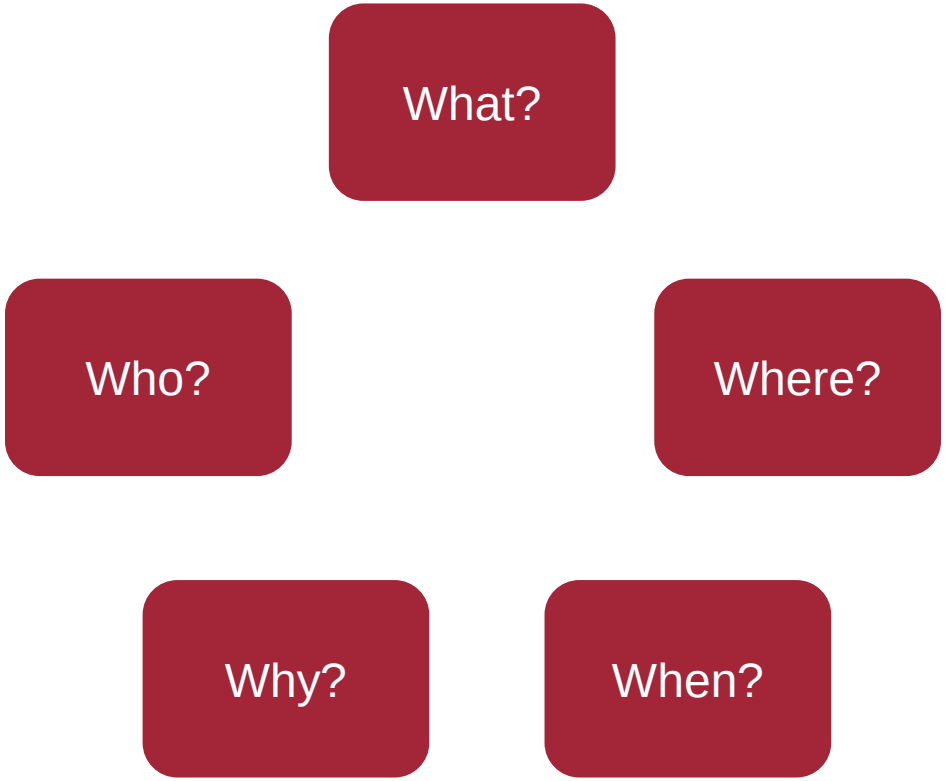
Digital Forensics

“Digital Forensics is the scientific use of methods on digital evidence to reconstruct unauthorised actions.”

https://i0.wp.com/wausaupilotandreview.com/wp-content/uploads/2017/10/Crime-Scene.jpg?fit=1280%2C960&ssl=1

Issues of an Investigation

The 5-W’s



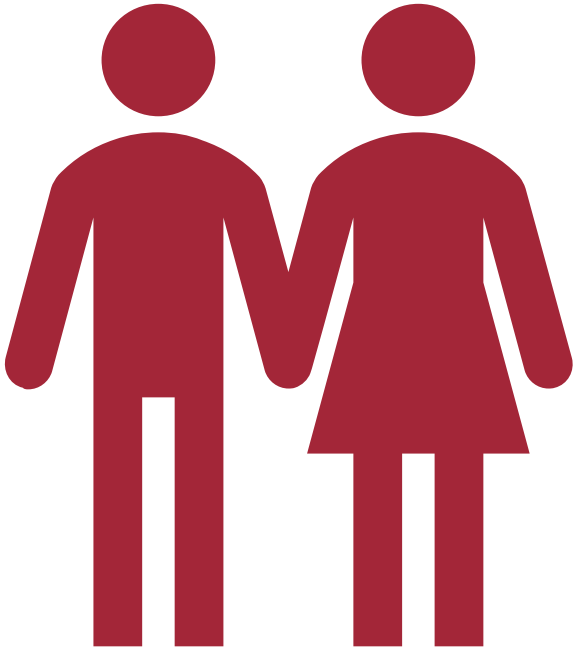
How & Lessons Learned

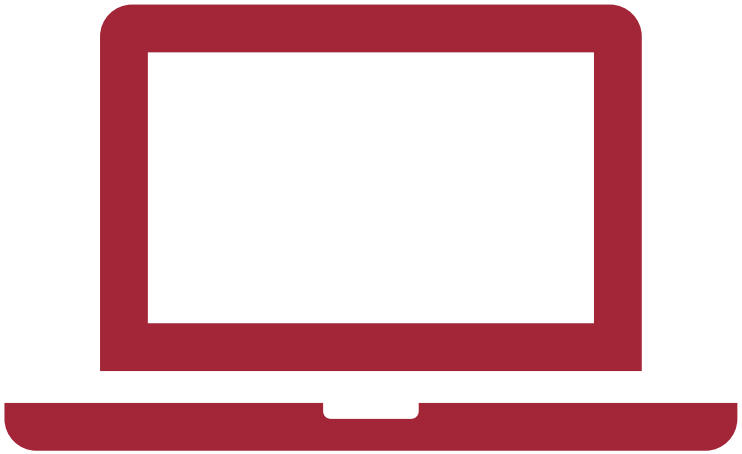
- How?
- Lessons learned

Digital Evidence

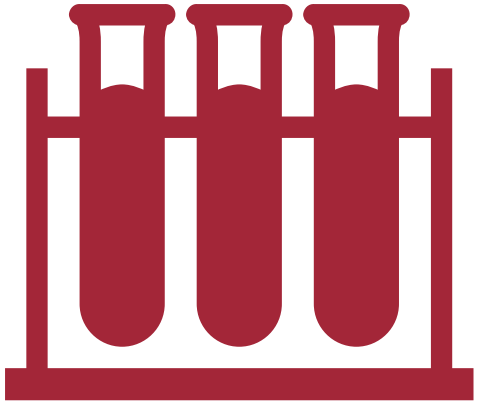
Digital Geology vs. Digital Archaeology

Digital Archaeology vs. Digital Geology



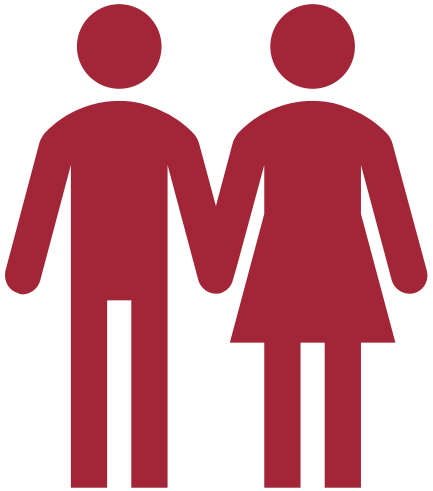


Principles



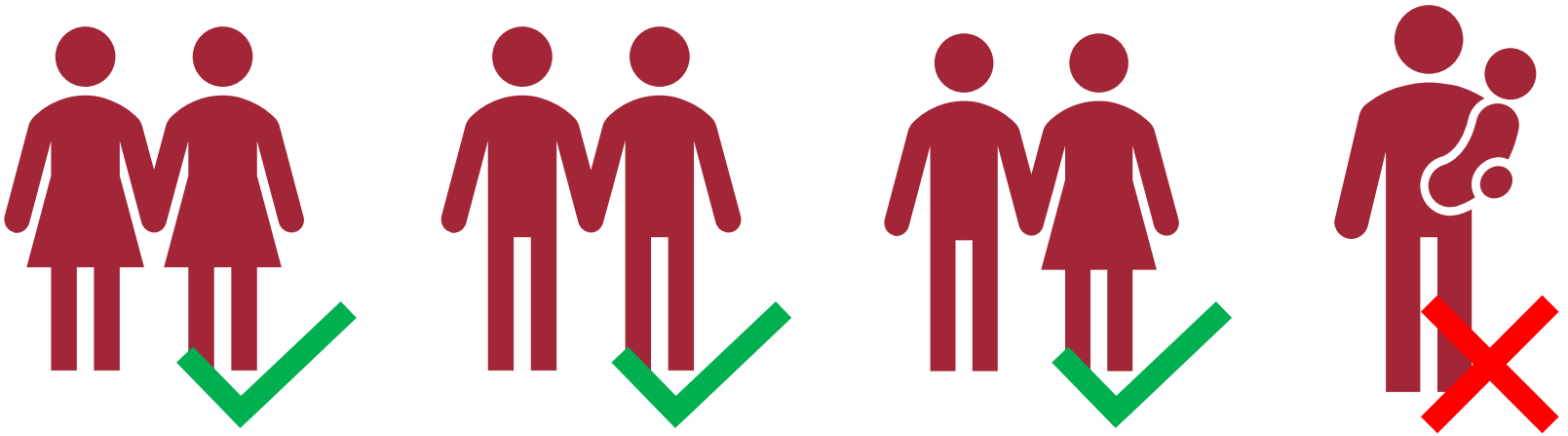
Forensic Soundness

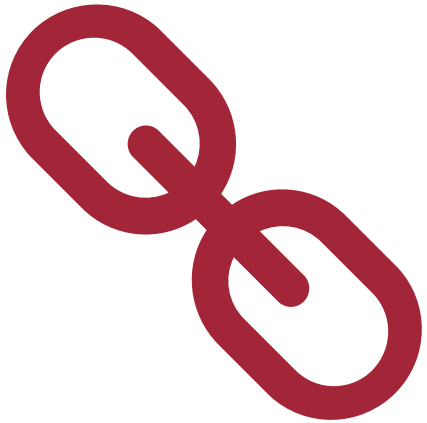
Evidence Integrity



Double Verification Principle

Double Verification Principle





Chain of Custody

Digital Forensic Process

Requirements

Requirements

- *Acceptance*
- *Reliability*
- *Repeatability and Reproducibility*
- *Evidence Integrity*
- *Cause and Effect*
- *Documentation*

Requirements

- ***Acceptance***
- *Reliability*
- *Repeatability and Reproducibility*
- *Evidence Integrity*
- *Cause and Effect*
- *Documentation*

Requirements

- *Acceptance*
- ***Reliability***
- *Repeatability and Reproducibility*
- *Evidence Integrity*
- *Cause and Effect*
- *Documentation*

Requirements

- *Acceptance*
- *Reliability*
- ***Repeatability and Reproducibility***
- *Evidence Integrity*
- *Cause and Effect*
- *Documentation*

Requirements

- *Acceptance*
- *Reliability*
- *Repeatability and Reproducibility*
- ***Evidence Integrity***
- *Cause and Effect*
- *Documentation*

Requirements

- *Acceptance*
- *Reliability*
- *Repeatability and Reproducibility*
- *Evidence Integrity*
- ***Cause and Effect***
- *Documentation*

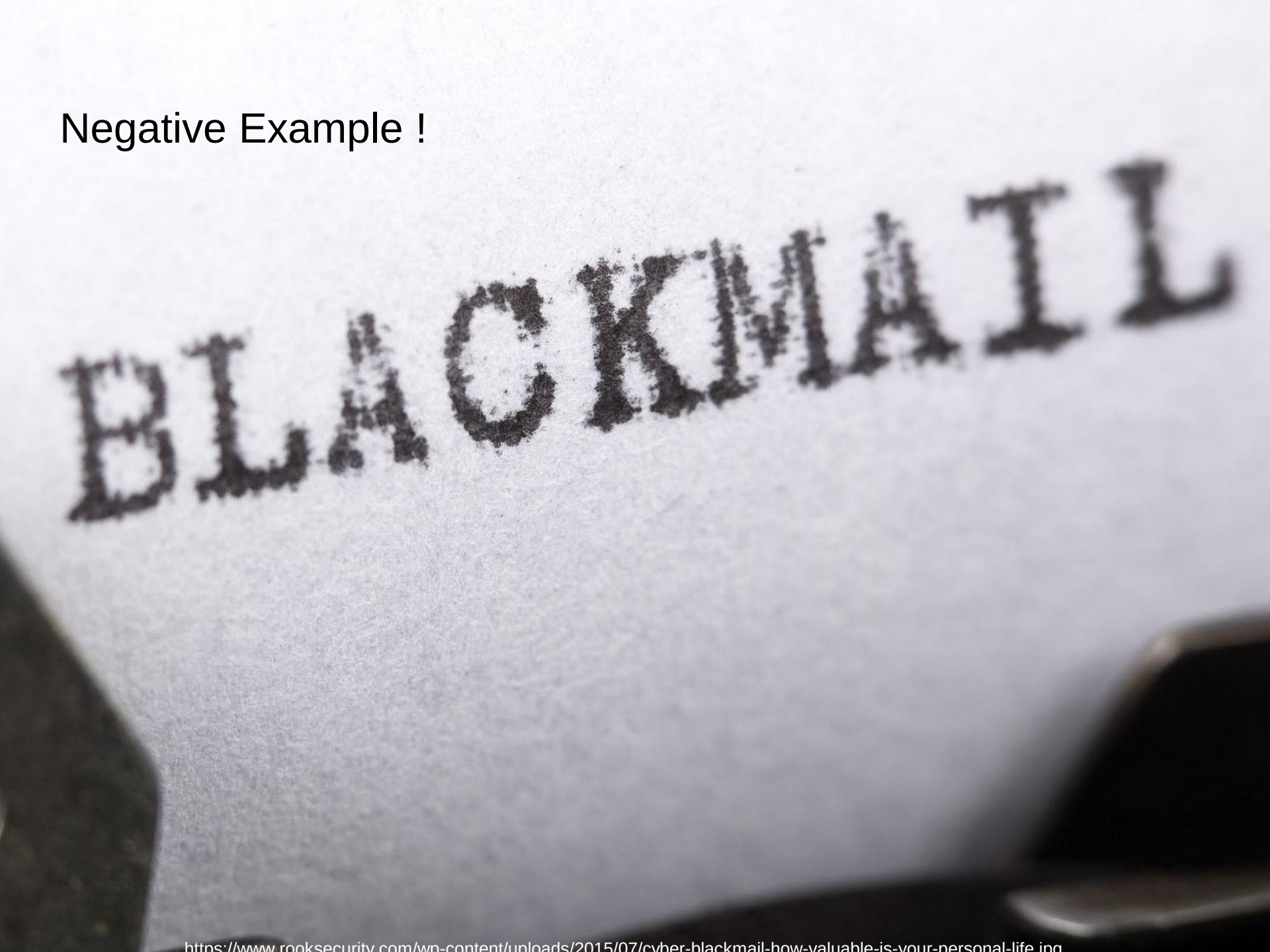
Requirements

- *Acceptance*
- *Reliability*
- *Repeatability and Reproducibility*
- *Evidence Integrity*
- *Cause and Effect*
- ***Documentation***

Requirements

- *Acceptance*
- *Reliability*
- *Repeatability and Reproducibility*
- *Evidence Integrity*
- *Cause and Effect*
- *Documentation*

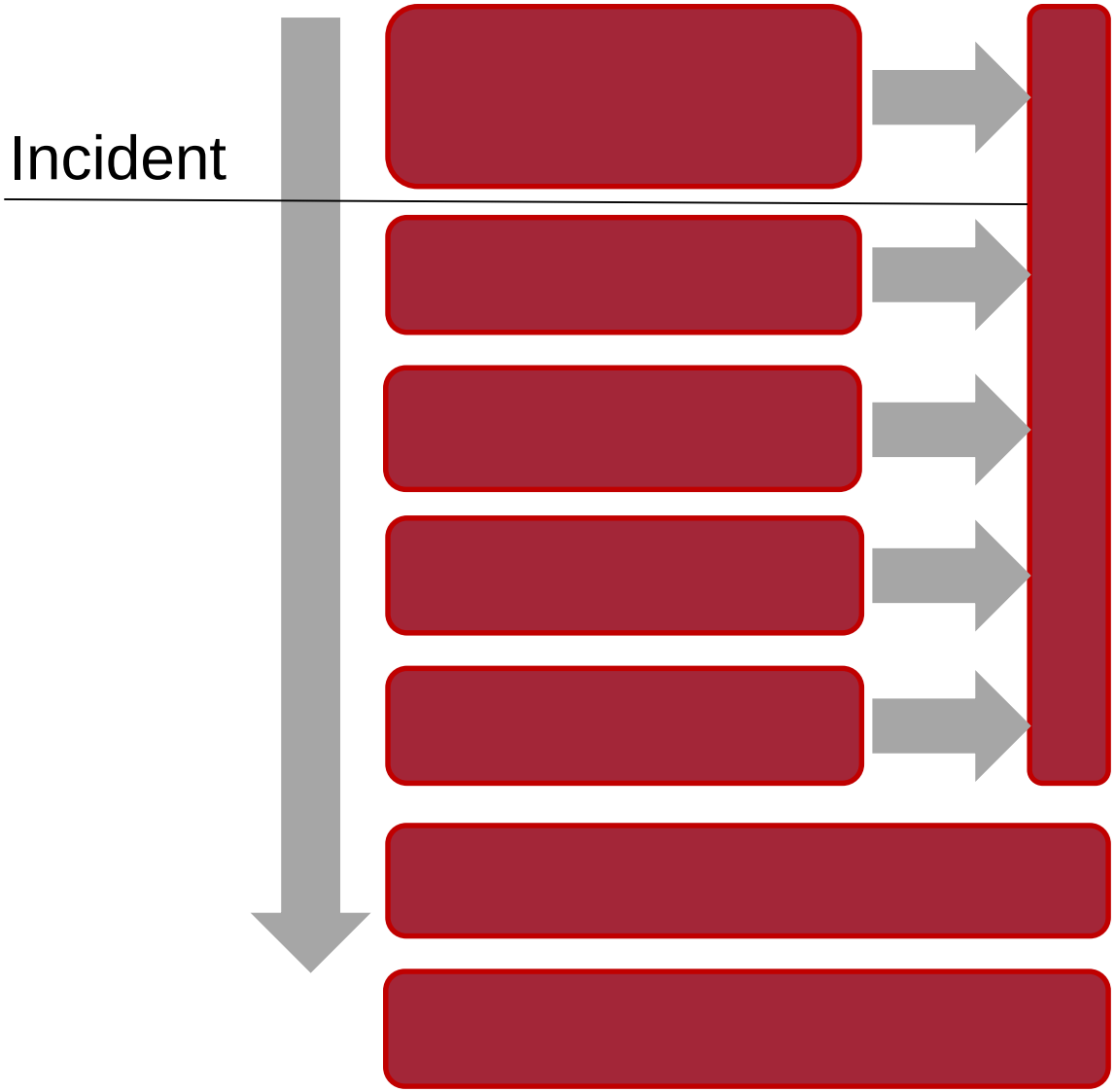
Negative Example !



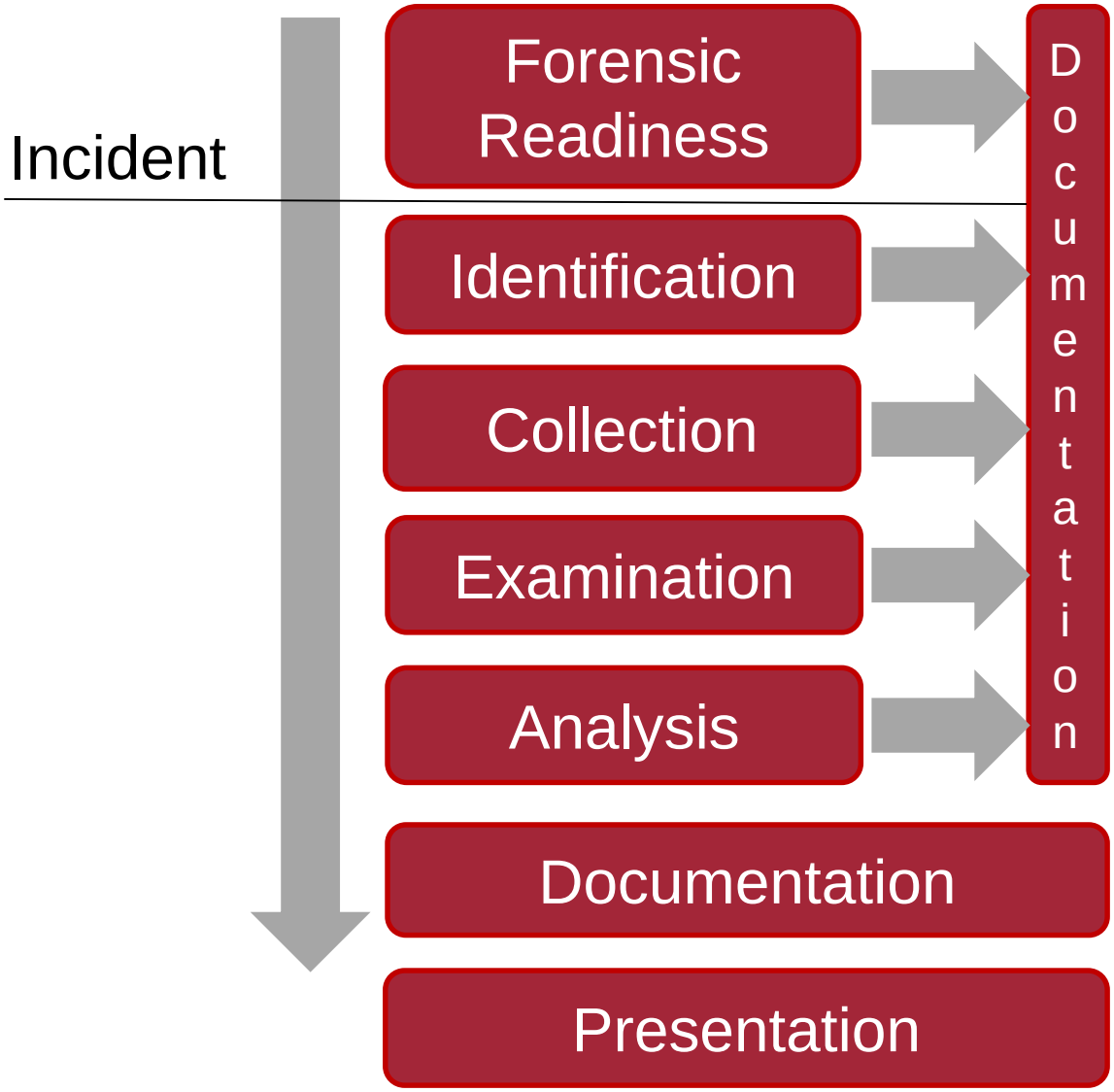
https://www.rooksecurity.com/wp-content/uploads/2015/07/cyber-blackmail-how-valuable-is-your-personal-life.jpg

Digital Forensic Process

Digital Forensic Process

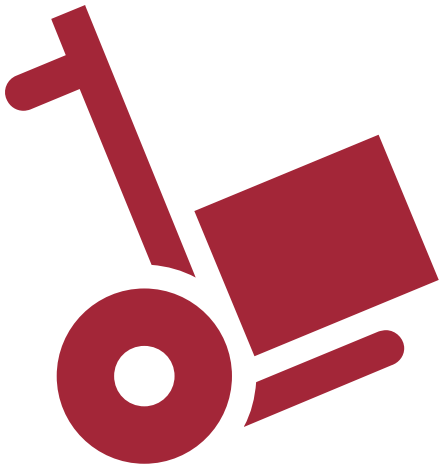


Digital Forensic Process

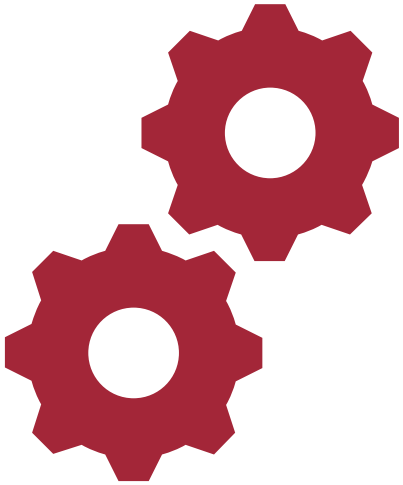


Forensic Readiness

Identification



Collection



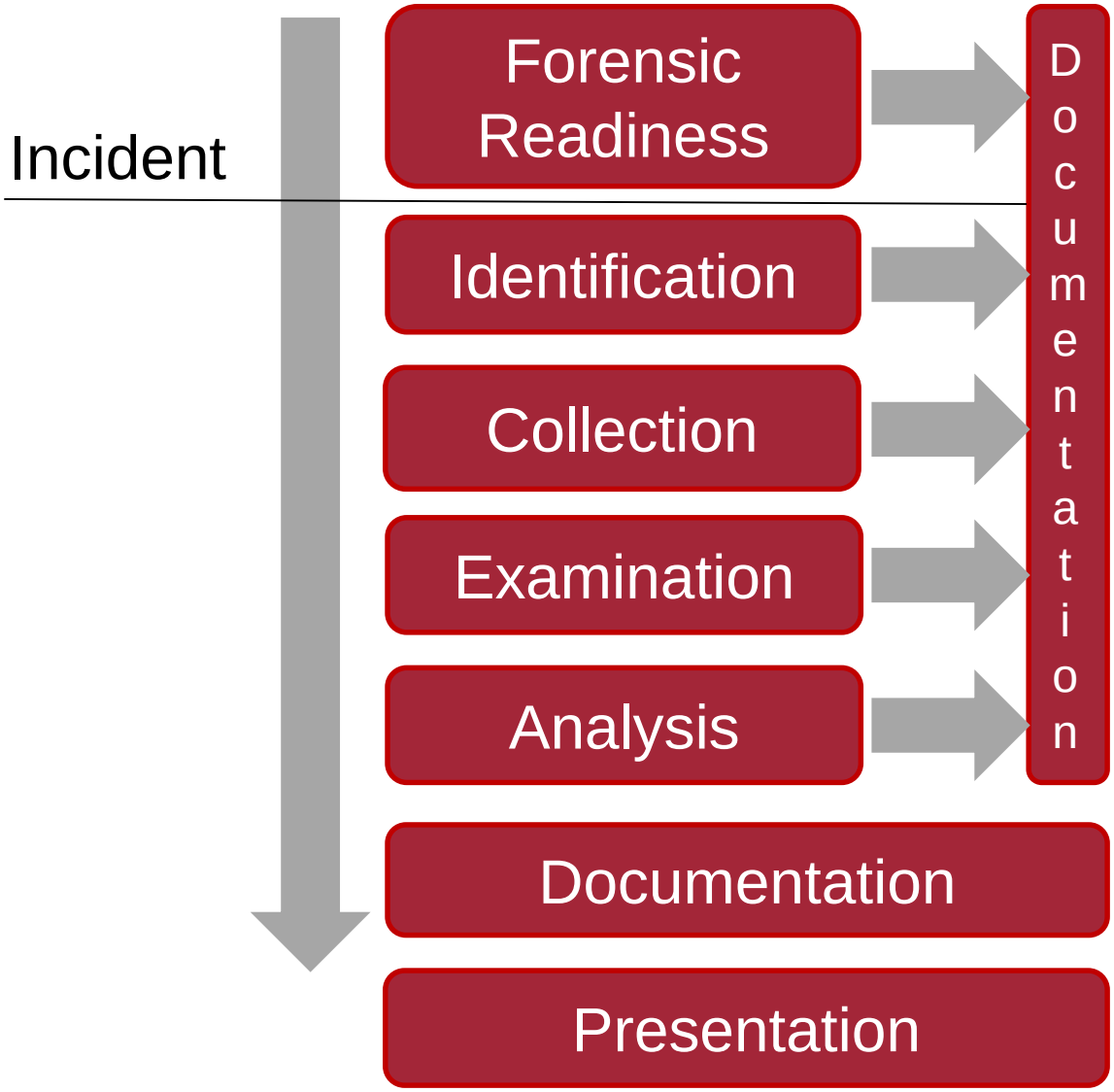
Examination

Analysis

Documentation

Presentation

Digital Forensic Process

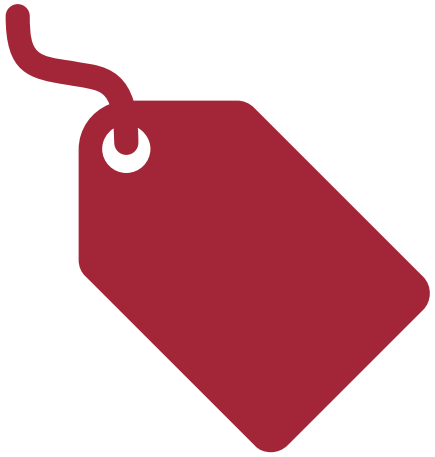


SAP

Secure
Analyse
Present

IPM

Investigative
Process
Model



Acquisition

Wiping

Post-mortem Analysis

vs.

Live Forensics

Post-mortem Analysis

Turned Off

Persistent Data

Post Incident

Live Forensics

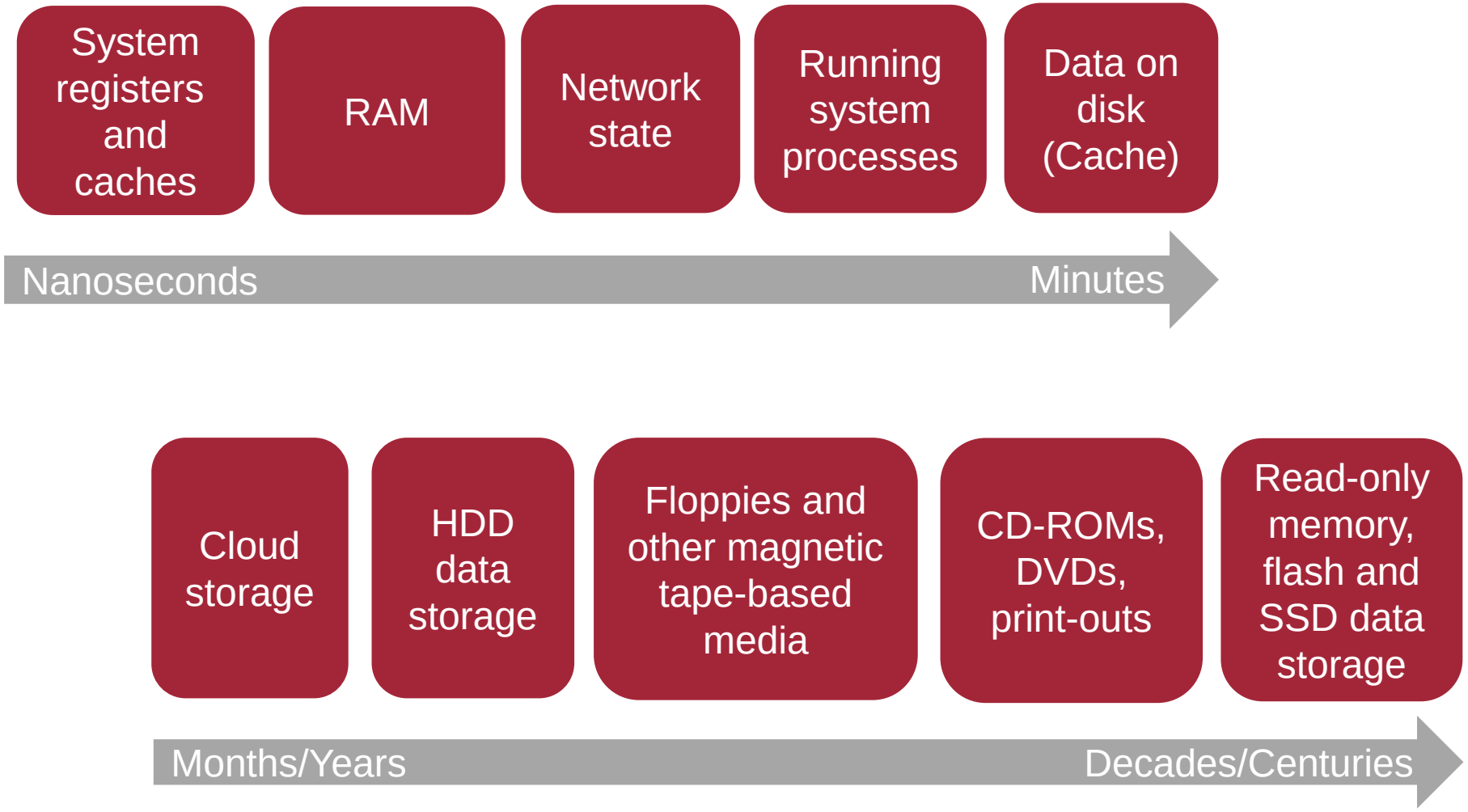
Turned On

Volatile Data

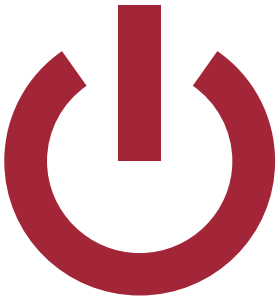
During Incident

Order of Volatility

Order of Volatility



Steps of an Acquisition



Power Status

Network Status

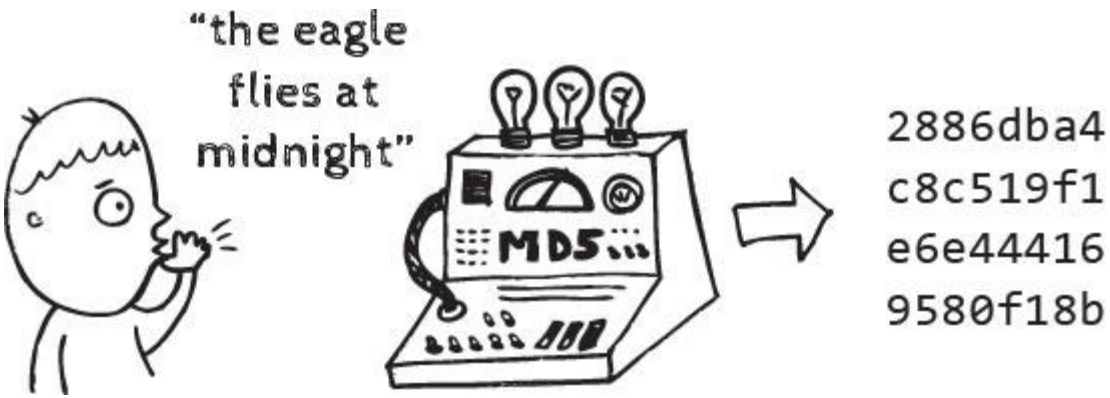
Imaging

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

Storage Formats

- Raw Image Format (.dd)
- EnCase Evidence File (.E01)
- Logical Evidence File (.L01)
- Custom Content Image (.AD1)
- Advanced Forensic Format (.AFF)

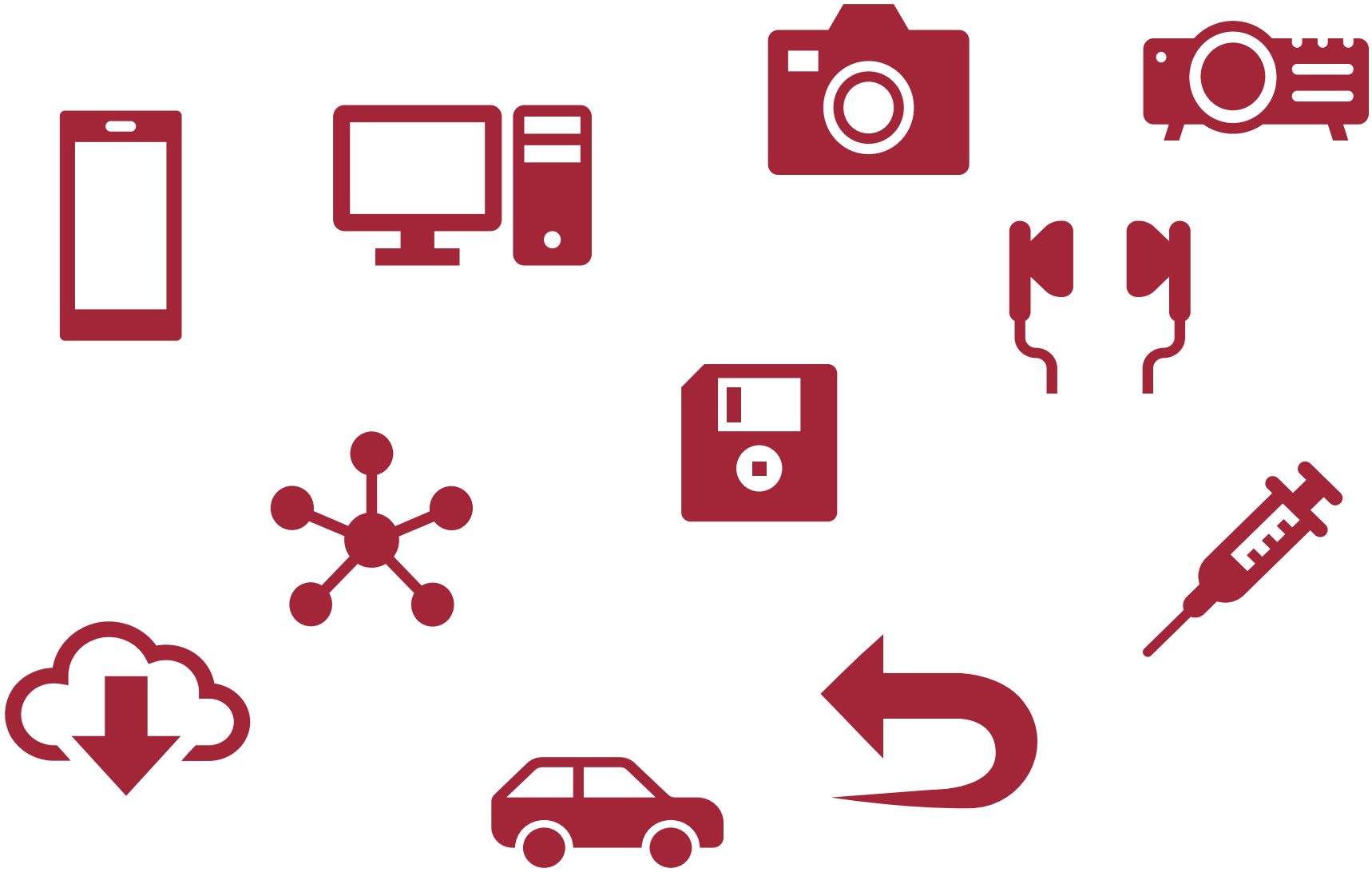
File Hashing



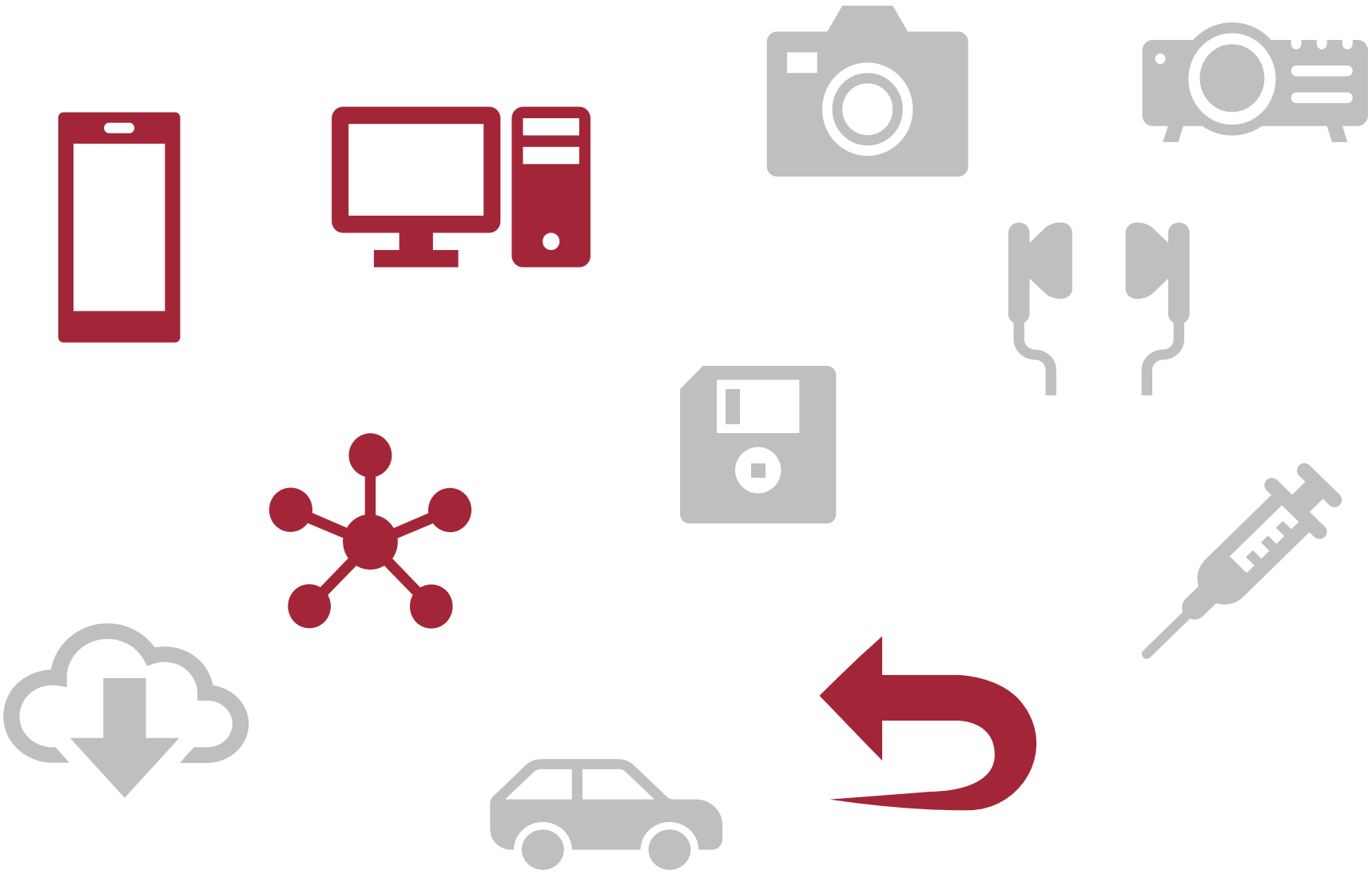
https://www.crypto-news.net/wp-content/uploads/2017/02/eagle.jpg

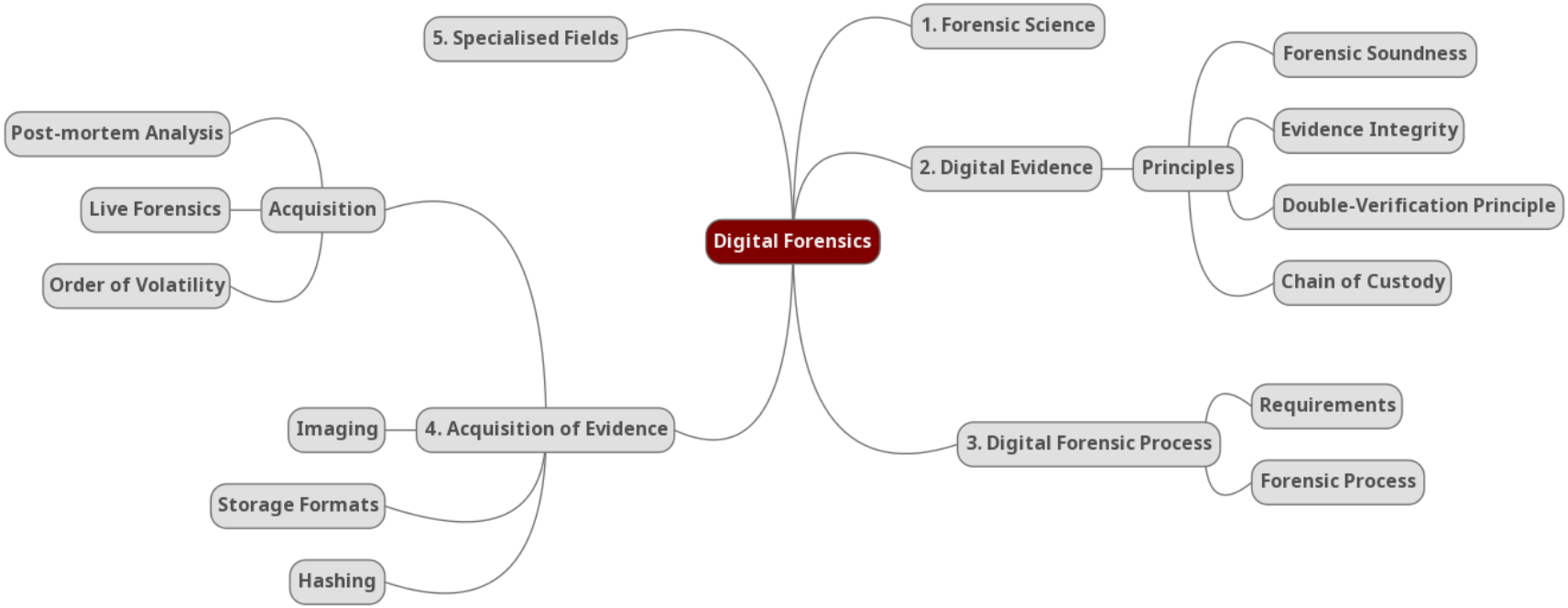
https://en.unesco.org/creativity/sites/creativity/files/thematic_monitoring.jpg

Specialised Fields



Specialised Fields




Digital Forensics
1. Forensic Science
2. Digital Evidence
Principles
Forensic Soundness
Evidence Integrity
Double-Verification Principle
Chain of Custody
3. Digital Forensic Process
Requirements
Forensic Process
4. Acquisition of Evidence
Acquisition
Post-mortem Analysis
Live Forensics
Order of Volatility
Imaging
Storage Formats
Hashing
5. Specialised Fields

ulm university universität ulm

Chapter 2: Digital Forensics

Introduction to Digital Forensics

Fröhlich, Hosh

https://www.schlechtlaw.com/wp-content/uploads/2018/06/digital-forensics.jpg