

Forensic Investigations



Dr. Lyron H. Andrews

Cybersecurity Advisor - CISSP/CCSP/SSCP/CRISC/CISM/CCSK

<https://www.linkedin.com/in/drlyronhandrews/>



Overview



Define digital forensics and major frameworks

Understand the process flow for collecting evidence

Review variables that may arise during and investigation



Forensic Frameworks and General Principles



Digital forensics investigations
involves the identification,
collection, preservation, and
preservation of digital evidence.



Locard's Principle of Exchange



Examples of Incident Response Frameworks

SWGDE

NIST SP 800-86

IACIS and ACPO



Situations Precipitating Forensic Investigation

Policy violation

Criminal action

Accidental damage

Regulatory
requirements

Legal hold



General Principles of Digital Forensic Investigations

Identifying evidence

Collecting or acquiring evidence

Examining or analyzing evidence

Presentation of finding



Securing the Scene and Gathering Forensic Evidence



Identify Crime Scene



Virtual



Endpoints



Cloud

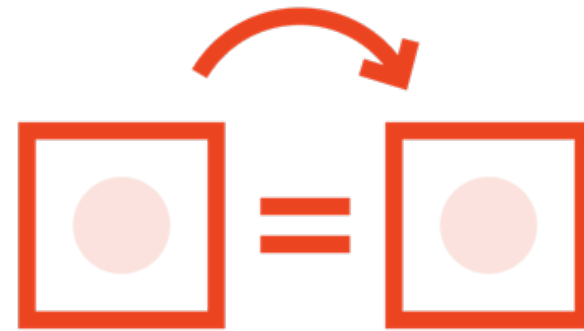
How might the objectives of the
IRT and forensic investigator
expose competing commitments?



Securing the Scene



Documentation



Original proof



Communication

Evidence Gathering Essentials

Do not compromise data

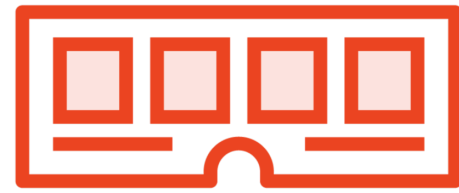
Use industry-accepted tools

Copy with write-block

Prevent subsequent alteration



Working from Most to Least Volatile



Memory



Disk

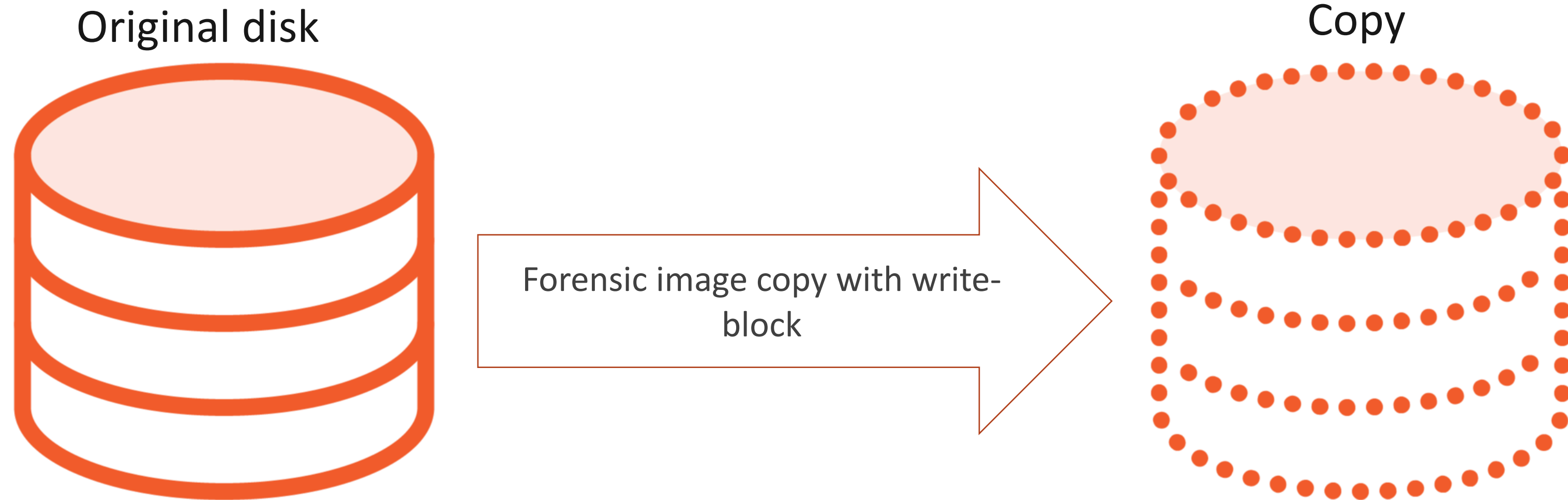


Evidence Capture Process

Original disk



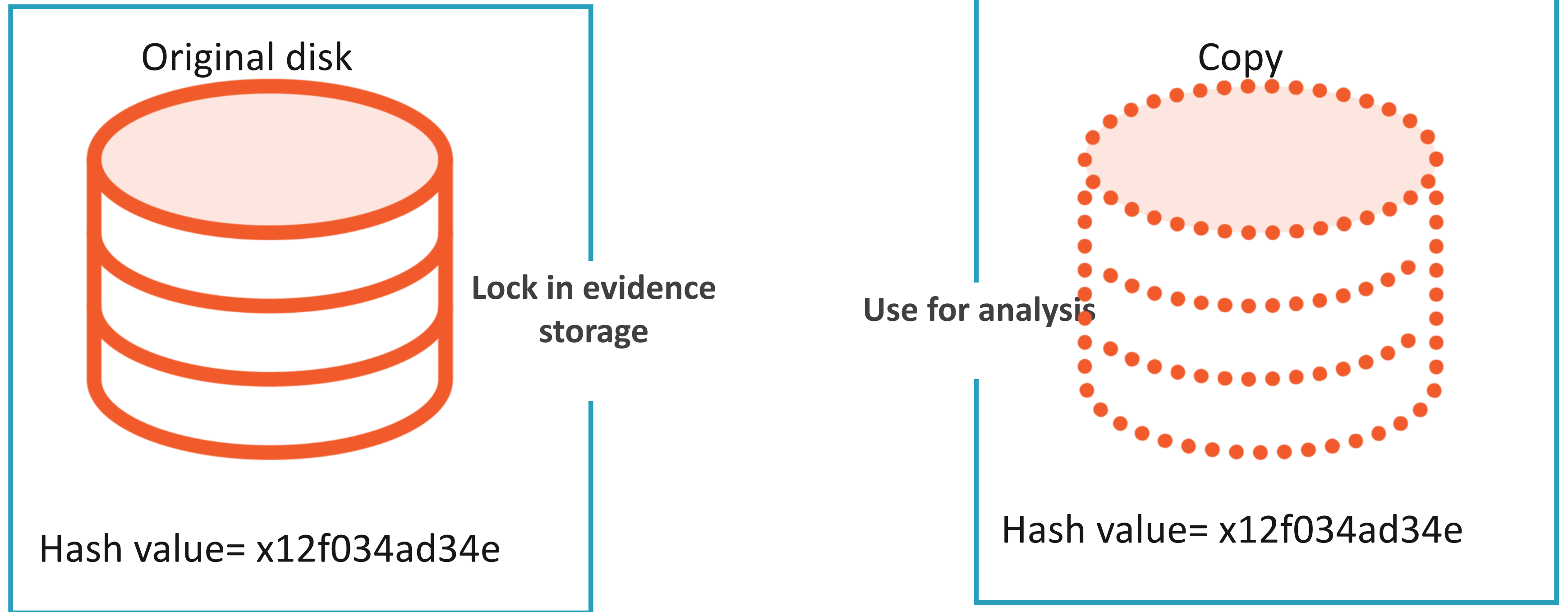
Evidence Capture Process



Evidence Capture Process

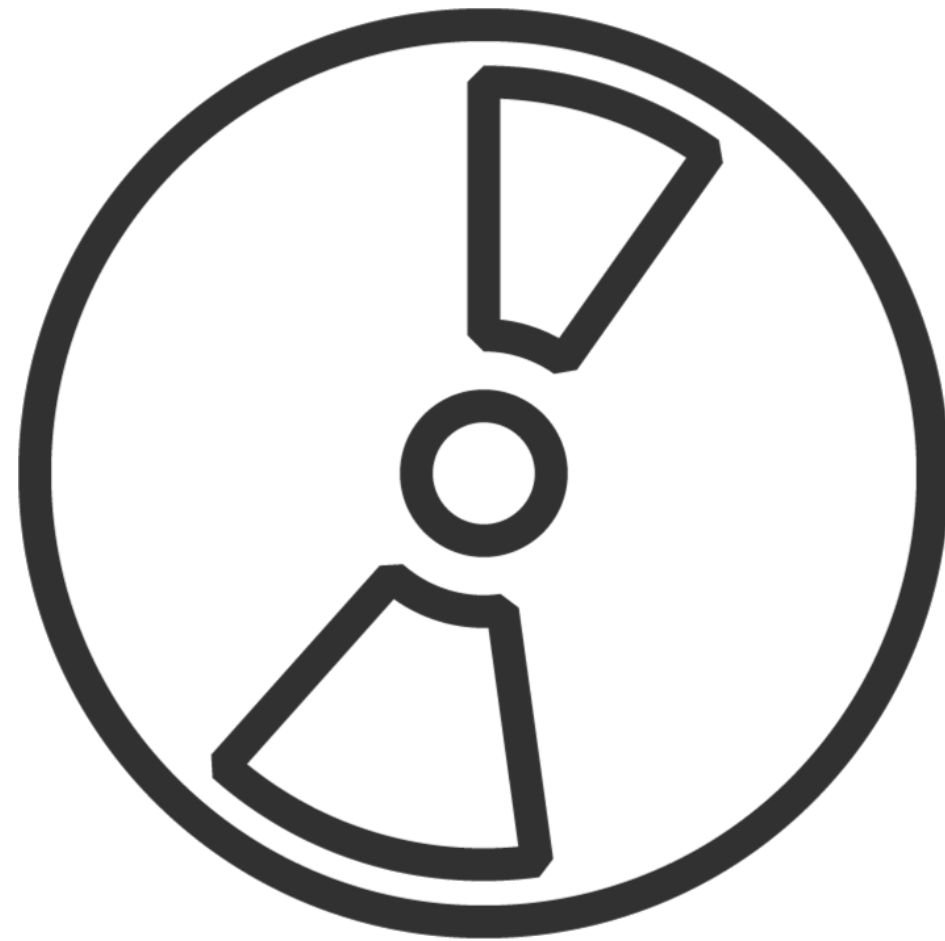


Evidence Capture Process



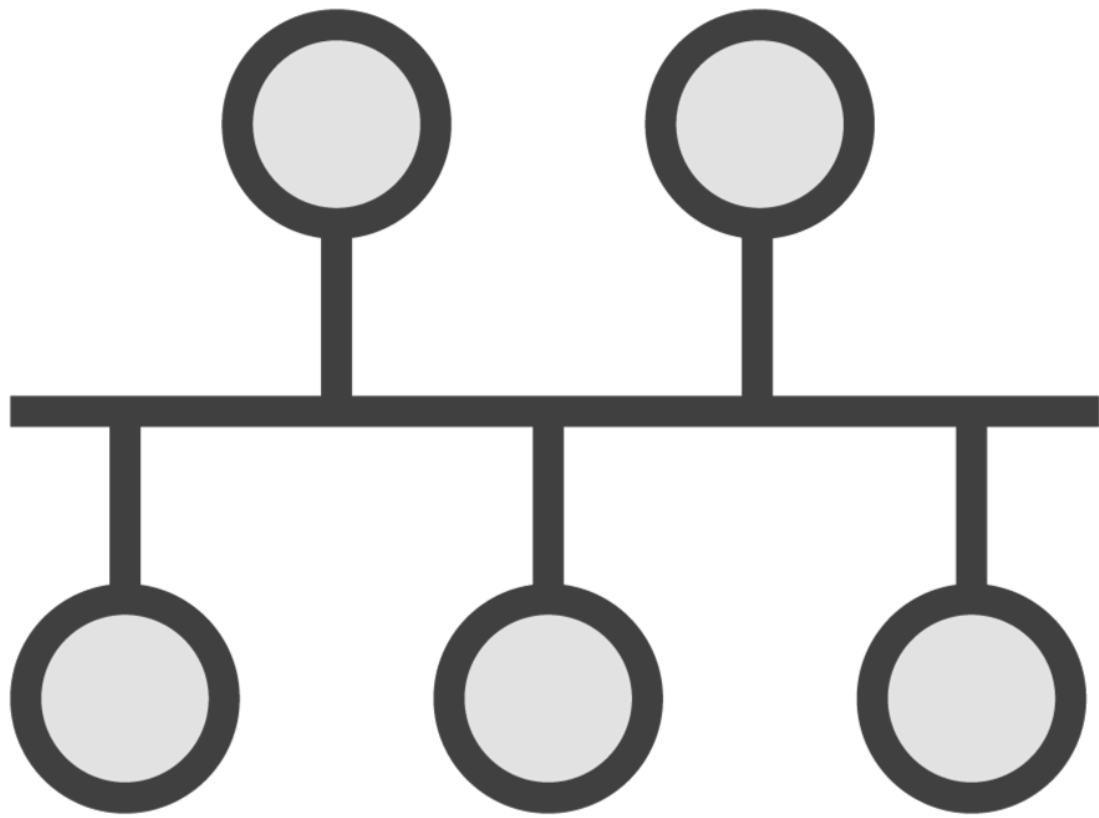
Types of Forensic Analysis





Media Analysis

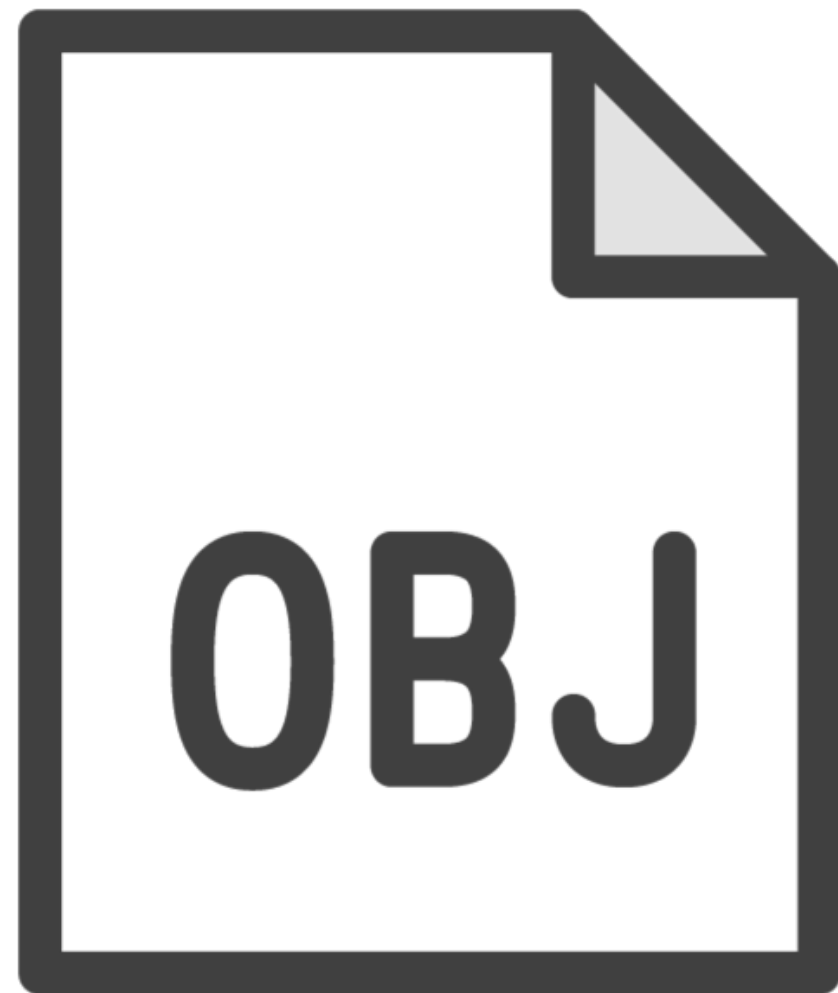
- Multiple media types
- Challenges of damaged and overwritten
- Media recovery specialist requirements



Network Analysis

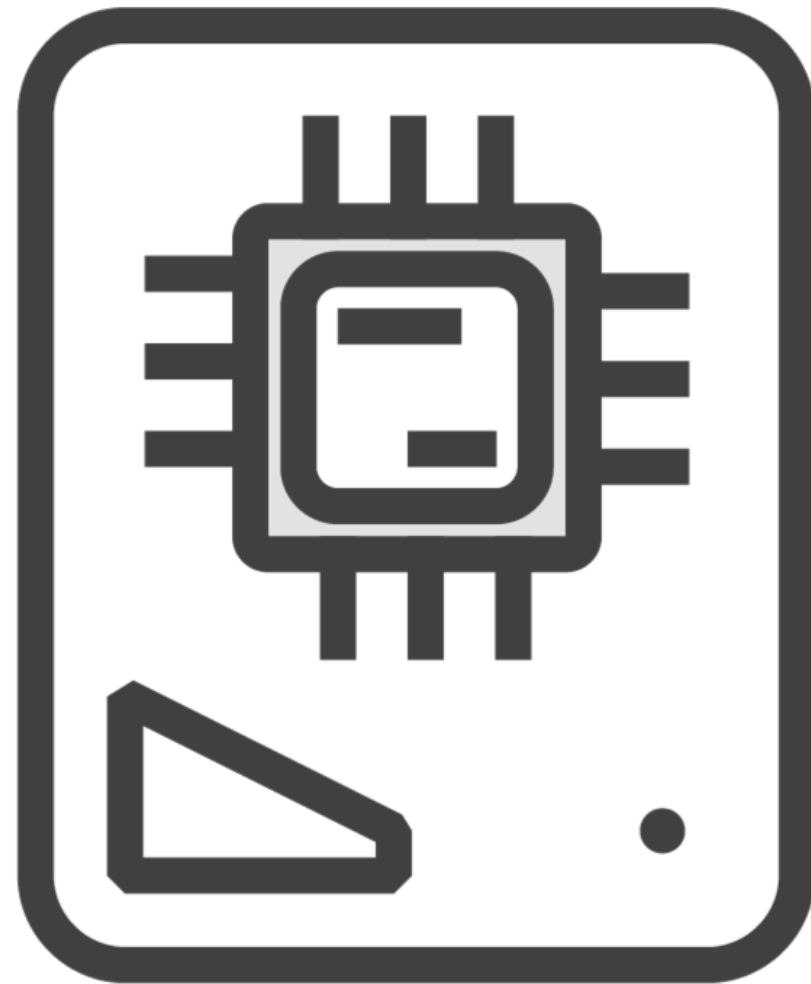
- Examination of network logs and activity
- Mirrors activity associated with IR
- Virtualized networks increase challenge





Software Analysis

- Various forms of program code examined
- Decompiling and reverse engineering
- Author identification
- Content analysis
- Context analysis



Hardware Analysis

- Mobile devices and smartphones
- CMOS chips
- Special challenges

Legal and Ethical Principles Related to Forensic Investigations



Follow the law that is the closest
proximity to your investigation.

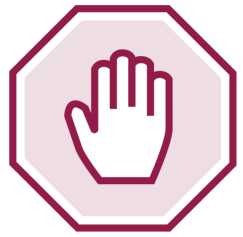




Legal Concerns

- Administrative
- Civil
- Criminal
- Data privacy

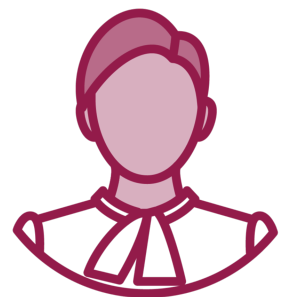
Administrative Investigations



Most investigations begin and end internal to an organization



Interviewing done in accordance with law



Information and evidence collection done by trained professionals



Chain of custody must not be broken



Possible Jeopardy of Criminal Case

Possessions

Relinquish valuables

Freedom

Imprisonment

Life

Capital punishment

Proof of guilt rest with state



Purpose of Tort Case

Damage

Person or property

Negligence

Lack care/diligence

Recovery

Injunction of acts

Defendant must prove not liable



Five Rules of Evidence

Be authentic

Be accurate

Be complete

Be convincing

Be admissible



Summary



What digital forensic skills are needed in your environment

What are the possible media analysis that may be required

What does the law say regarding digital forensics in your locality



Up Next:
BCDR Plan and Activities

