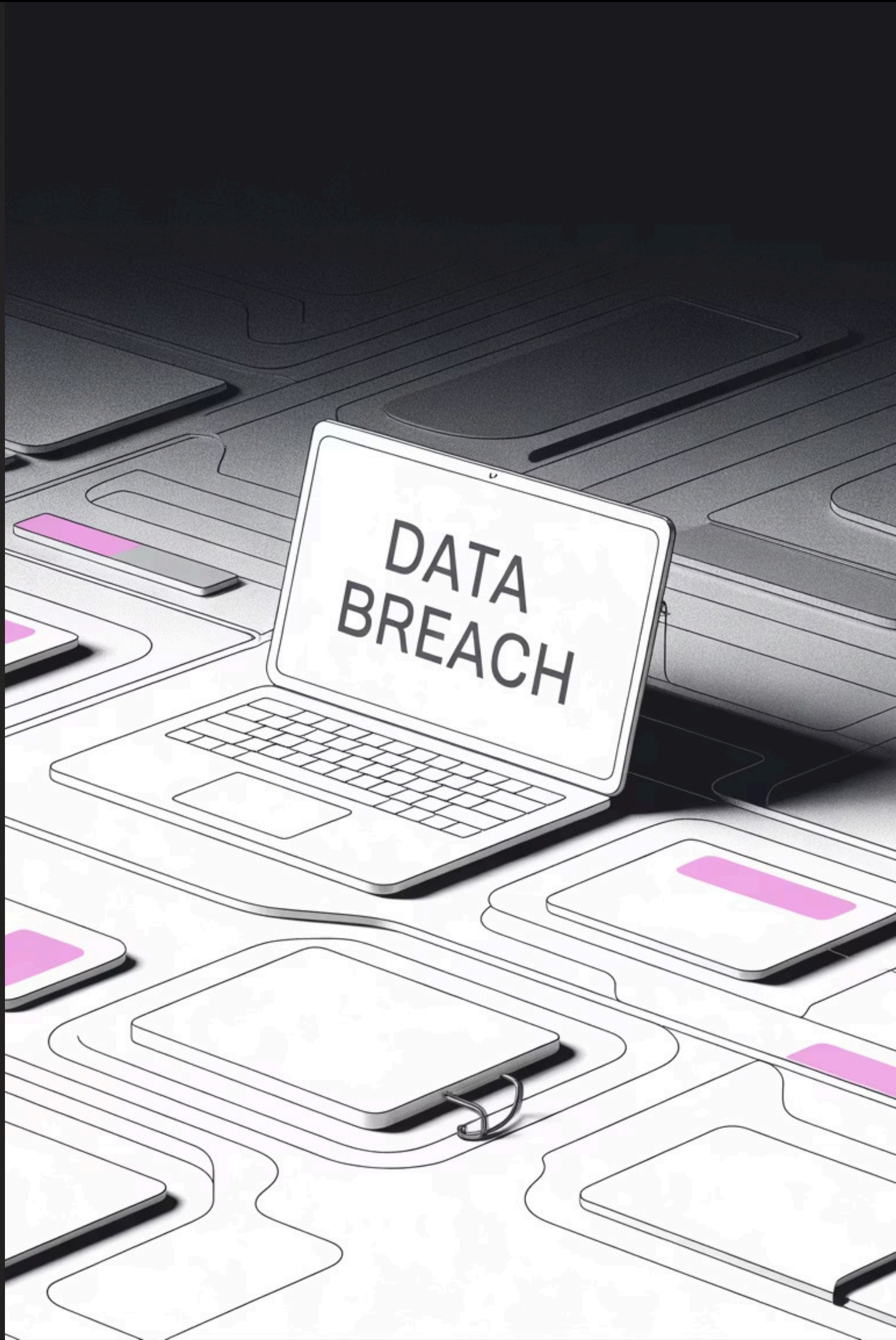
Digital Forensic Investigation Fundamentals

Chapter 3: Methodologies, Lab Setup & Professional Standards



Learning Objectives

01

Master Forensic Methodologies

Understand formal investigation frameworks and best practices

02

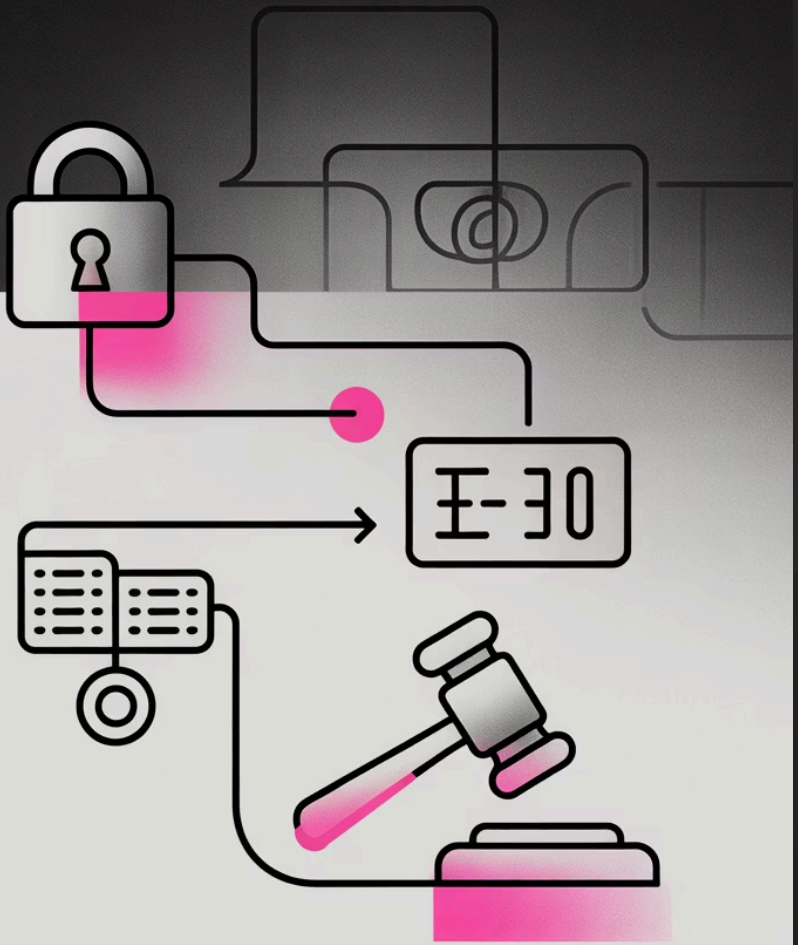
Configure Professional Labs

Set up secure, accredited forensic workspaces

03

Apply Industry Software

Demonstrate proficiency with major forensic tools



Three Core Principles

Preserve Original Evidence

Work from bit-level copies only

Create analysis and backup copies

Follow Locard's Principle of Transference

Adhere to Legal Rules

Comply with jurisdiction requirements

Authenticate evidence properly

Maintain admissibility standards

Maintain Objectivity

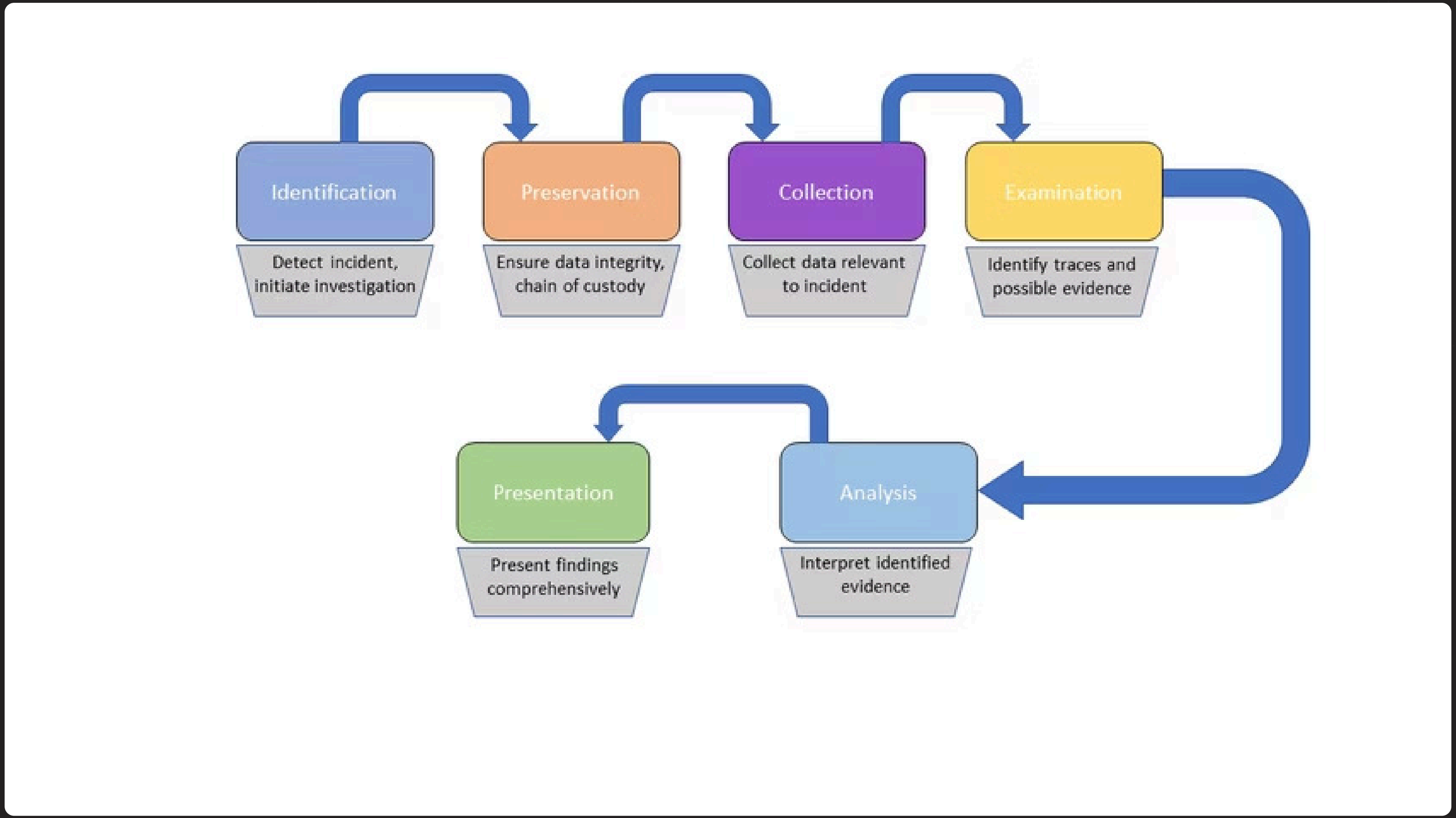
Create formal analysis plans

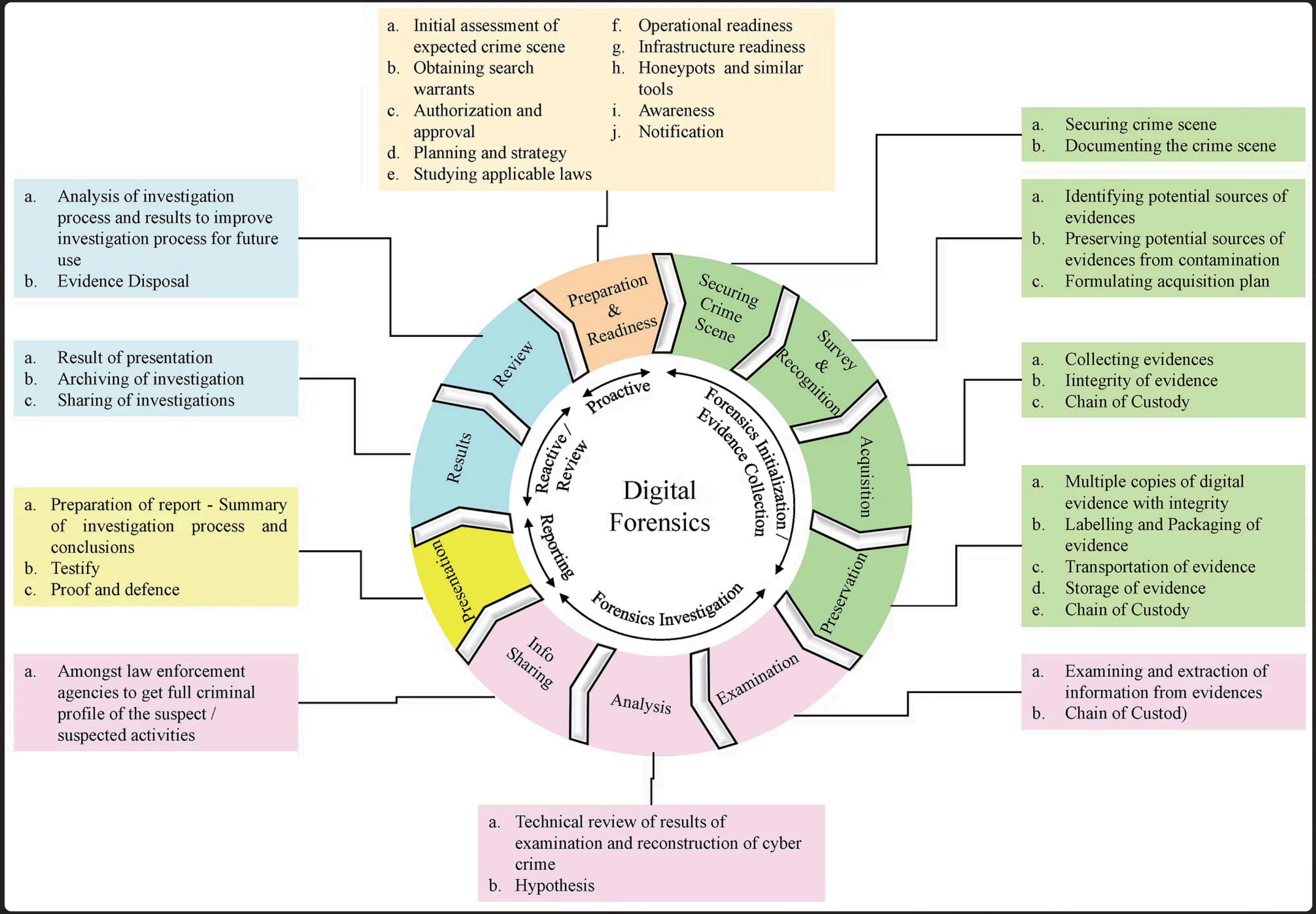
Operate within expertise boundaries

Preserve professional credibility

Formal Forensic Frameworks

DFRWS Framework


Identification
Detect incident, initiate investigation
Preservation
Ensure data integrity, chain of custody
Collection
Collect data relevant to incident
Examination
Identify traces and possible evidence
Presentation
Present findings comprehensively
Analysis
Interpret identified evidence



a. Initial assessment of expected crime scene
b. Obtaining search warrants
c. Authorization and approval
d. Planning and strategy
e. Studying applicable laws
f. Operational readiness
g. Infrastructure readiness
h. Honeypots and similar tools
i. Awareness
j. Notification

a. Securing crime scene
b. Documenting the crime scene

a. Identifying potential sources of evidences
b. Preserving potential sources of evidences from contamination
c. Formulating acquisition plan

a. Collecting evidences
b. Iintegrity of evidence
c. Chain of Custody

a. Multiple copies of digital evidence with integrity
b. Labelling and Packaging of evidence
c. Transportation of evidence
d. Storage of evidence
e. Chain of Custody

a. Examining and extraction of information from evidences
b. Chain of Custod)

a. Technical review of results of examination and reconstruction of cyber crime
b. Hypothesis

a. Amongst law enforcement agencies to get full criminal profile of the suspect / suspected activities

a. Preparation of report - Summary of investigation process and conclusions
b. Testify
c. Proof and defence

a. Result of presentation
b. Archiving of investigation
c. Sharing of investigations

a. Analysis of investigation process and results to improve investigation process for future use
b. Evidence Disposal

computers

MDPI

Unveiling the Dynamic Landscape of Digital Forensics: The Endless Pursuit

The invention of transistors in the 1940s marked the beginning of a technological revolution that has impacted every aspect of our lives. However, along with the positive advancements, the...

Essential Lab Equipment

Storage Systems

Redundant storage with RAID 5 configuration for data integrity and backup capabilities

Analysis Workstations

Variety of computers with different specifications to handle diverse evidence types

Connection Hardware

Complete set of connectors for all drive types and legacy device compatibility

Lab Security Requirements

Network Isolation

Air-gapped systems prevent evidence contamination

Physical Security

Logged, restricted access with surveillance monitoring

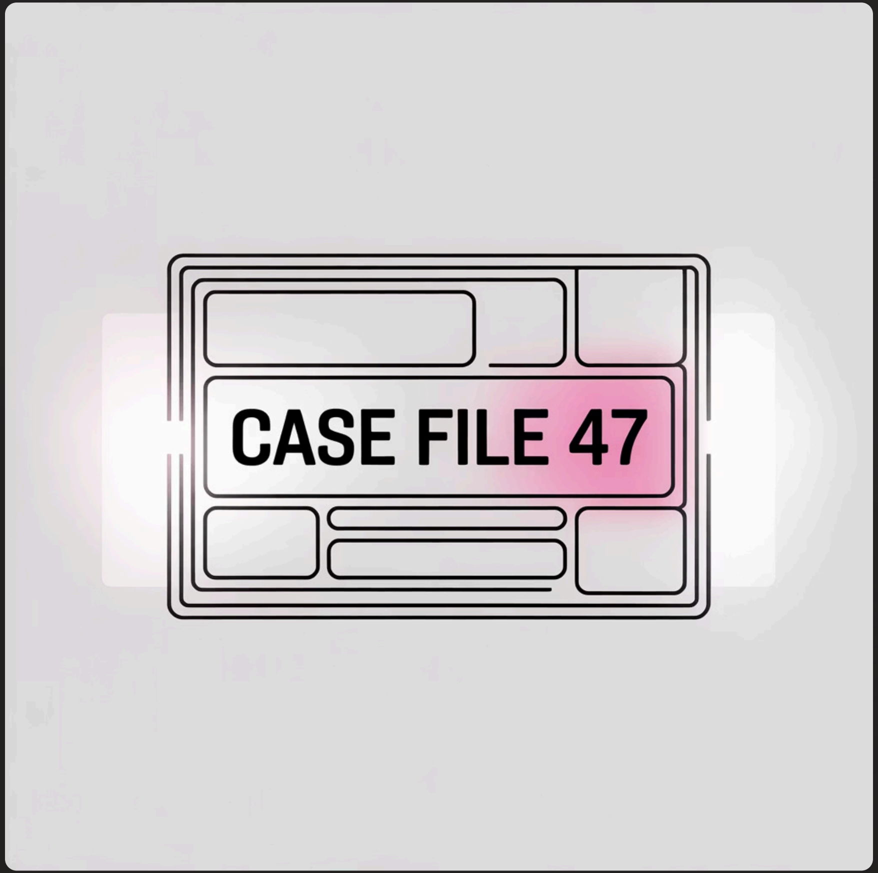
Evidence Protection

Fire-resistant safes for critical evidence storage

Electromagnetic Shielding

TEMPEST guidelines for sensitive investigations

Commercial Forensic Software

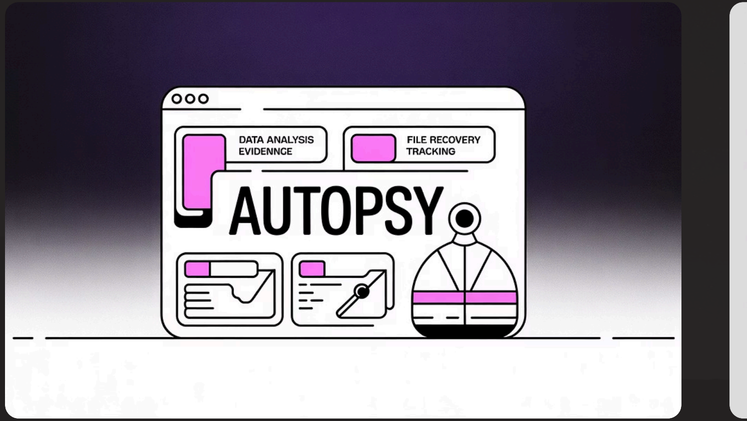


Industry Standard Suites

- **EnCase:** Comprehensive analysis platform
- **Forensic Toolkit (FTK):** Full-featured investigation suite
- **OSForensics:** All-in-one digital investigation tool

Multiple tool validation is best practice for reliable results

Open-Source Forensic Tools

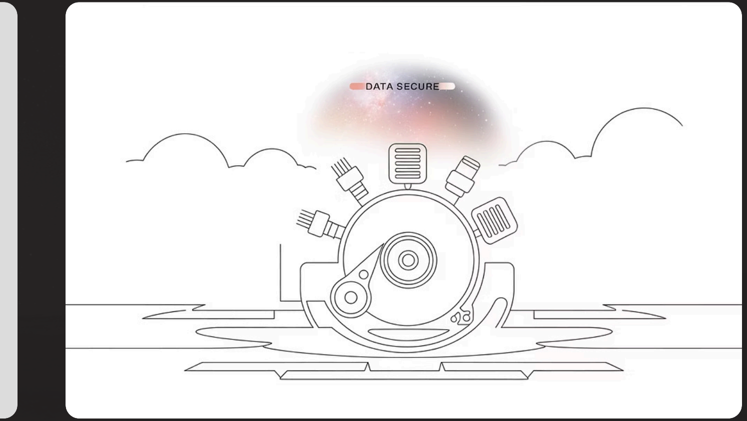


The Sleuth Kit & Autopsy

Powerful open-source platform for file system analysis and timeline creation

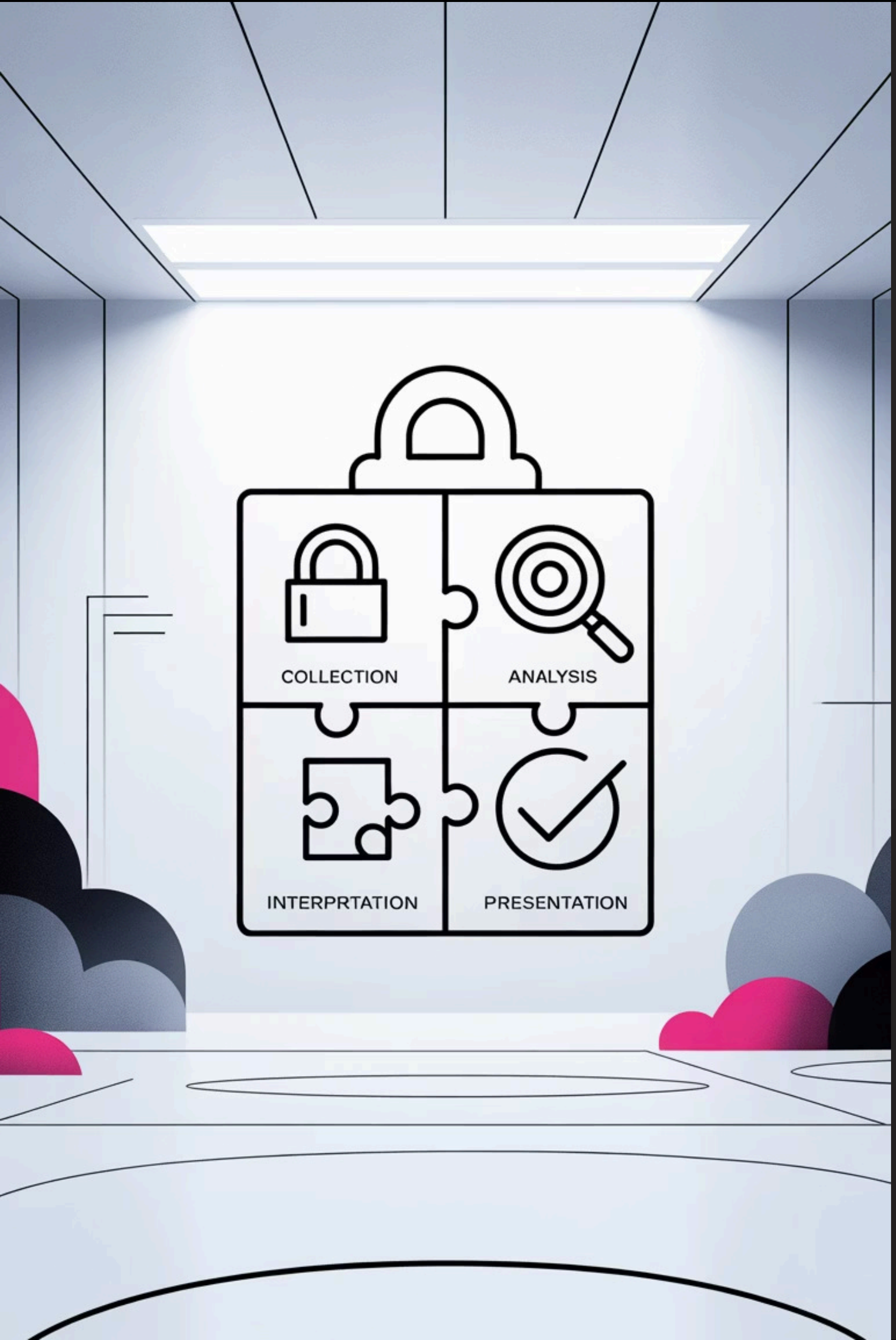
Kali Linux

Penetration testing distribution with extensive forensic tool collection



Specialized Utilities

Helix Live CD, CopyQM Plus disk duplicator, AnaDisk anomaly scanner



Evidence Handling Protocol

1 **Find & Preserve**

Locate digital evidence using proper search protocols

2 **Collect by Volatility**

Prioritize data collection based on Order of Volatility

3 **Bit-Level Analysis**

Capture all potential evidence including file slack space

4 **Document Everything**

Maintain meticulous chain of custody records

Expert Report Requirements

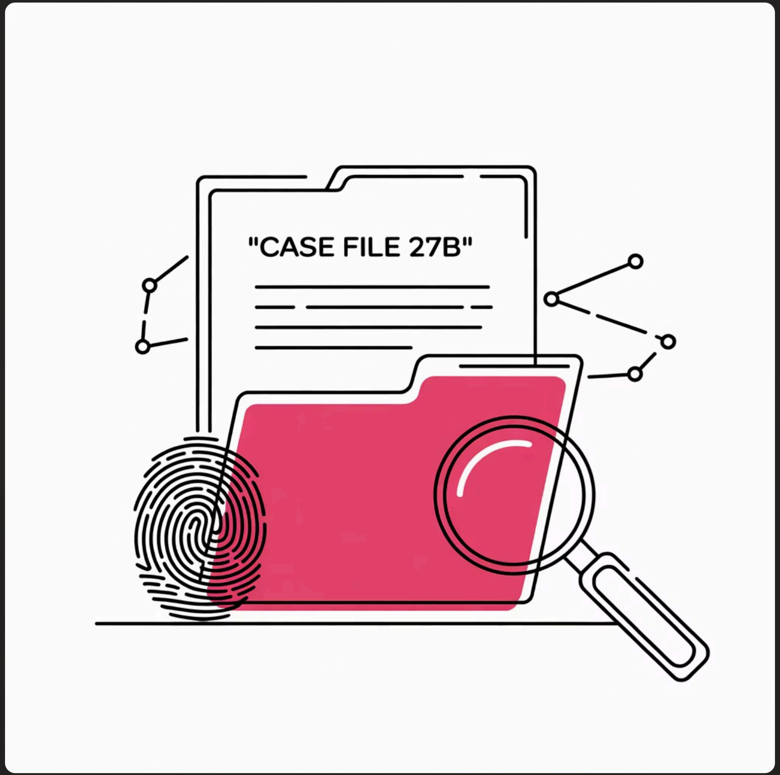
Report Components

- Detailed methodology description
- Complete test procedures
- Comprehensive findings
- Supported conclusions
- Expert's full curriculum vitae

ResearchGate

(PDF) Digital Forensic Exper...

PDF | Digital Forensics Report Template | Find, read and cite al...

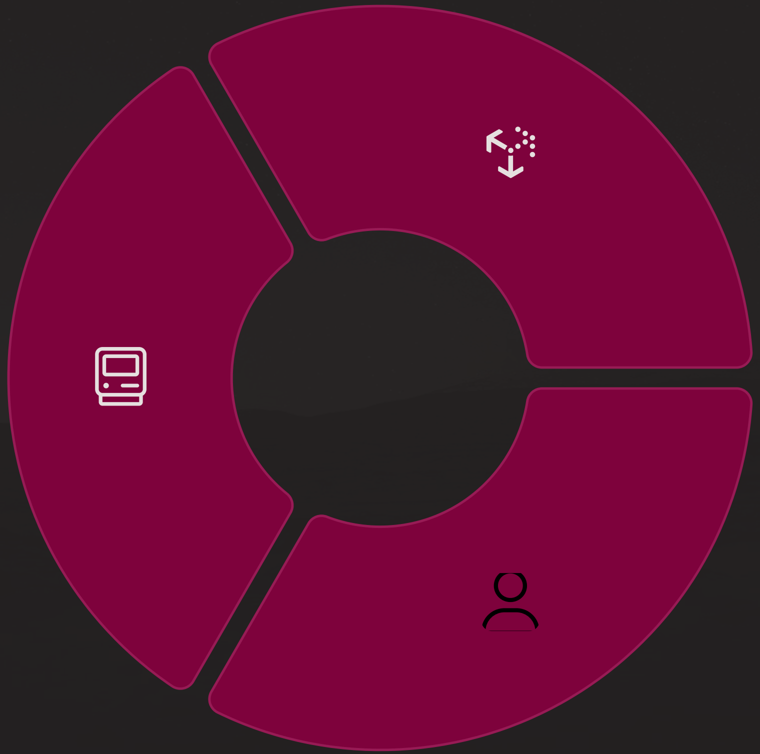


Reports must withstand judicial scrutiny and support expert testimony in court proceedings

Professional Certifications

Foundational Knowledge

- CompTIA A+ (PC Hardware)
- Network+ (Basic Networking)
- Security+ (Security Fundamentals)

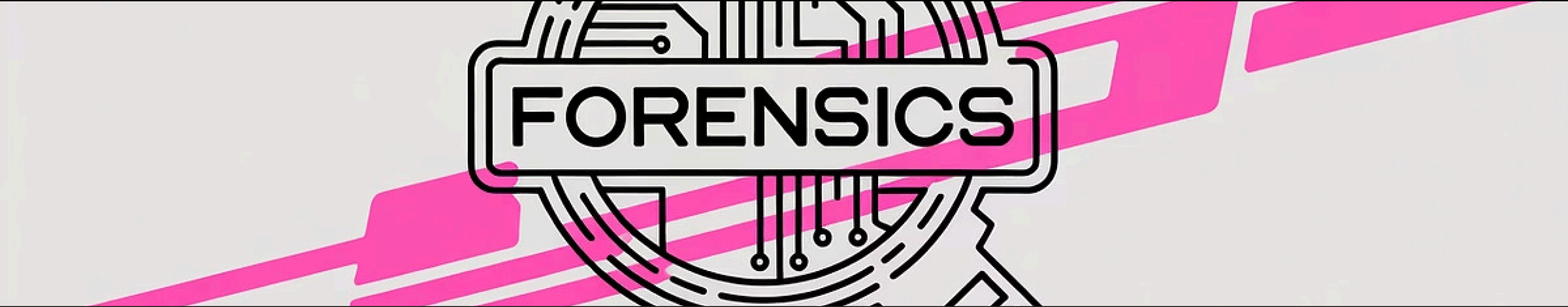


Vendor-Specific

- EnCase Certified Examiner (EnCE)
- AccessData Certified Examiner (ACE)
- OSForensics Certification

General Forensic

- CHFI (EC-Council)
- GCFA (GIAC Analyst)
- GCFE (GIAC Examiner)



Key Takeaways

Evidence Integrity is Paramount

Always preserve originals, work from copies, maintain chain of custody

Follow Established Frameworks

Use DFRWS, SWGDE, or Event-Based models for consistent investigations

Invest in Proper Lab Setup

Security, redundancy, and accreditation ensure reliable results

Continuous Professional Development

Combine formal education, certifications, and hands-on experience