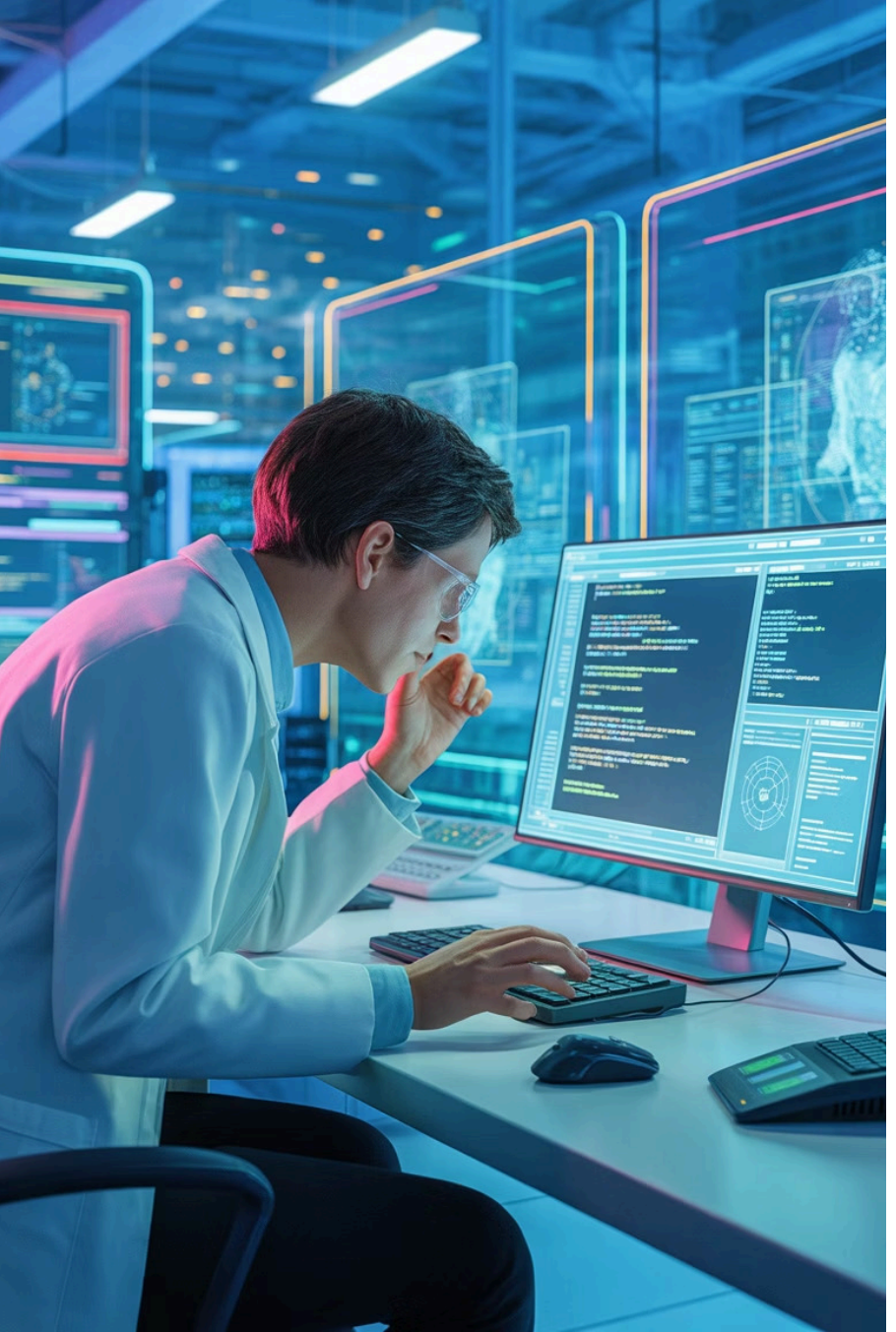


# Methodology of Cyber Forensics

Cyber forensics follows a systematic process for investigating digital crimes. It relies on established protocols to ensure evidence integrity throughout investigations.

# Case Preparation in Cyber Forensics

### Define Objectives

Establish clear goals based on the initial incident report. Determine what evidence needs to be collected.

### Assign Resources

Allocate specialized team members with appropriate skills. Ensure proper tools and equipment are available.

### Legal Requirements

Identify applicable laws and regulations. Obtain necessary warrants and permissions before proceeding.

### Documentation

Create initial case files with scope details. Record background information and suspected timeline of events.

# Phases of the Investigation Process

### Identification

Recognize and locate relevant digital evidence sources. Determine which devices may contain critical data.

### Preservation

Secure evidence to prevent modification. Create forensic images of original data sources.

### Collection

Gather data systematically from systems, networks, and storage devices. Follow strict protocols.

### Examination & Analysis

Extract and interpret evidence. Discover hidden or deleted information through specialized techniques.

### Documentation & Reporting

Record findings comprehensively. Prepare reports suitable for legal proceedings and internal review.

# Types of Cyber Forensics Investigation

### Computer Forensics

Examines personal computers and local storage. Recovers deleted files and analyzes user activity.

### Network Forensics

Analyzes traffic patterns and suspicious connections. Examines firewall logs and packet captures.

### Mobile Forensics

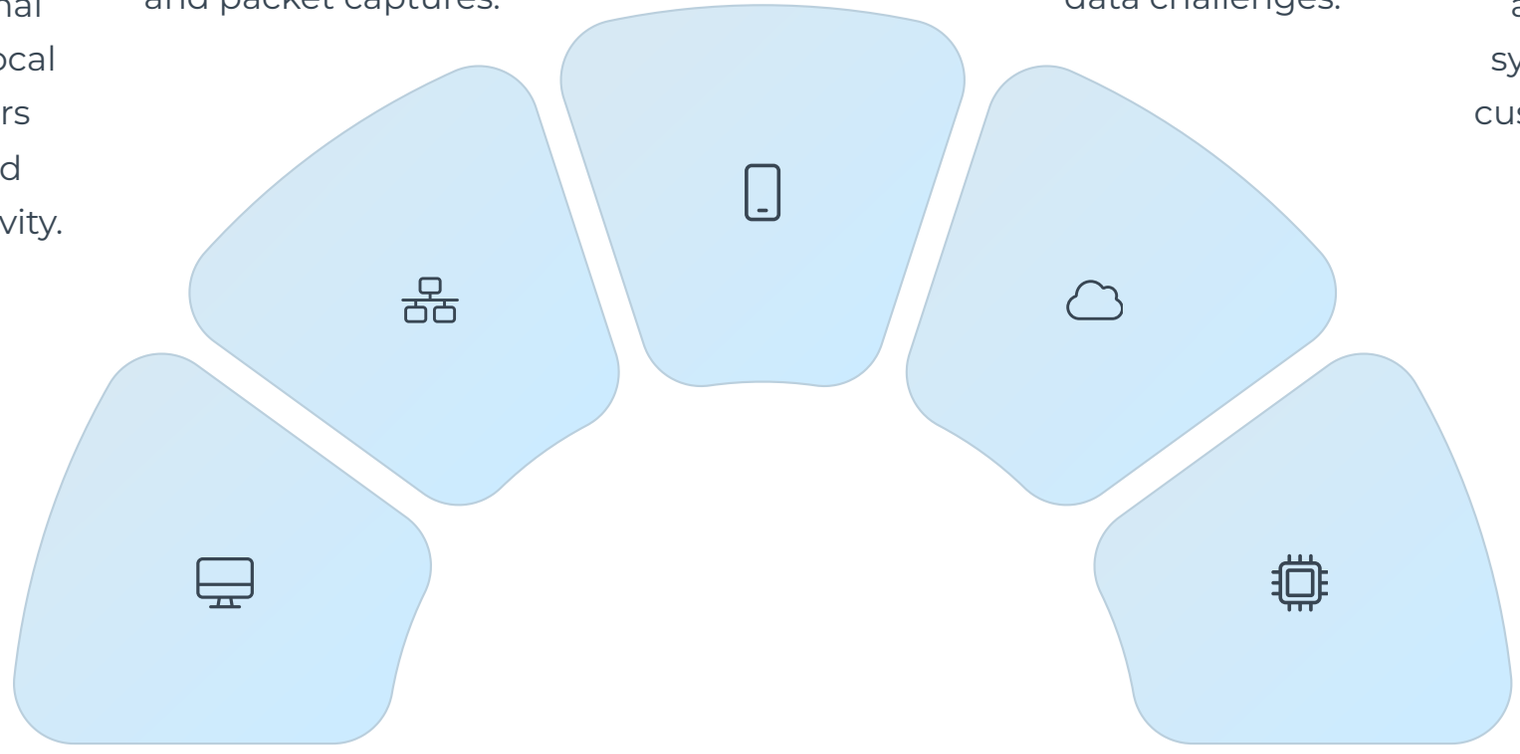
Extracts data from smartphones and tablets. Recovers messages, location data, and app usage.

### Cloud Forensics

Investigates virtualized environments and distributed storage. Handles multi-tenant data challenges.

### Specialized Device Forensics

Examines IoT devices and embedded systems. Requires custom approaches for proprietary hardware.



# Digital Evidence Collection Process

### System Isolation

Secure affected systems to prevent contamination. Disconnect network access when appropriate. Document the state before changes.

### Forensic Imaging

Use write blockers to prevent modifications. Create bit-by-bit copies of storage media. Verify images with hash values.

### Comprehensive Collection

Gather logs, memory dumps, and network captures. Collect both volatile and non-volatile data. Prioritize time-sensitive information.

### Chain of Custody

Document who handled evidence and when. Record all transfers between team members. Maintain secure storage for all items.


# Forensics Analysis Preparation

## Evidence Verification

Calculate and compare hash values. Ensure data integrity before analysis begins. Document validation procedures thoroughly.

## Lab Environment Setup

Prepare isolated analysis workstations. Install forensic software suites. Configure virtual machines for malware analysis.

## Target Determination

Identify key evidence sources to examine. Create analysis strategy based on case objectives. Focus on high-value data first.

## Workflow Prioritization

Establish examination sequence. Allocate resources to critical areas. Create timeline for deliverables and interim reports.

# Special Cases in Cyber Forensics

### Encrypted Data Recovery

Employ specialized techniques for protected information. Use legal means to obtain keys when possible. Document all decryption attempts.

### Live System Analysis

Capture volatile memory before shutdown. Document running processes and network connections. Preserve ephemeral evidence quickly.

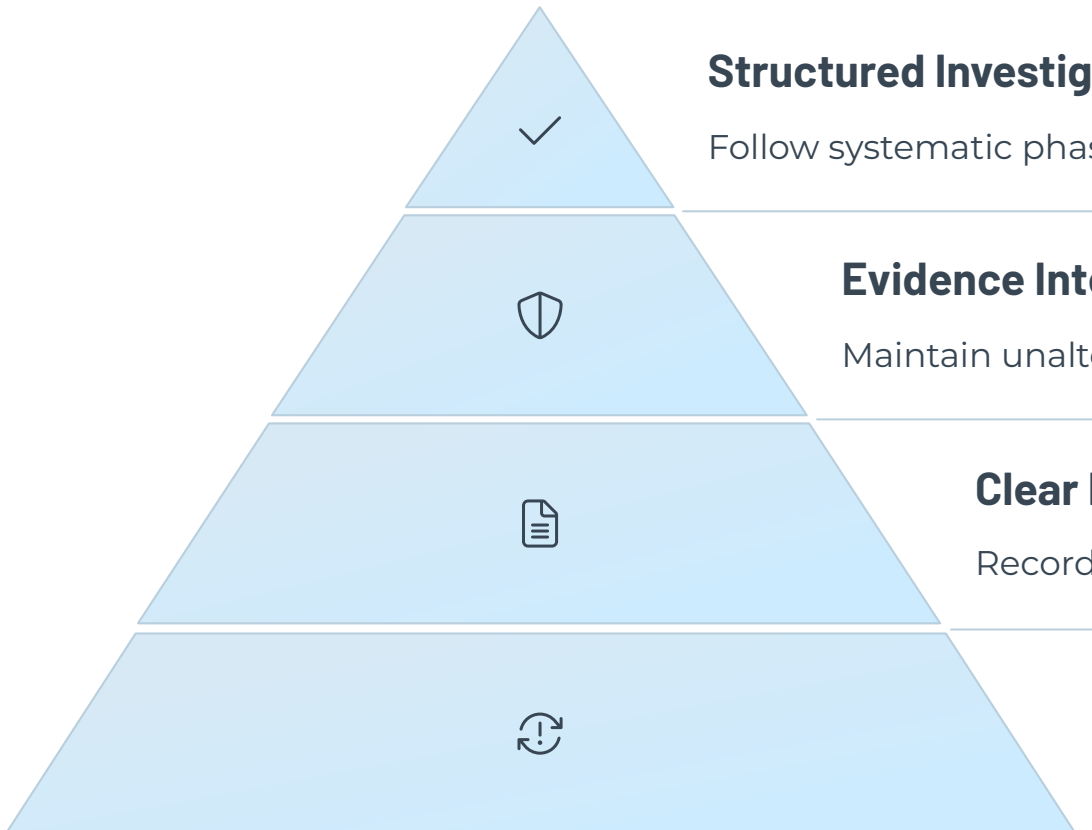
### Multi-Jurisdiction Investigations

Navigate different legal frameworks across borders. Coordinate with international authorities. Ensure evidence admissibility in relevant courts.

### Novel Malware Analysis

Identify zero-day threats safely. Use sandboxed environments for dynamic analysis. Develop custom extraction tools when needed.

# Summary: Key Principles of Cyber Forensics Methodology



### Structured Investigation

Follow systematic phases for reliable results

### Evidence Integrity

Maintain unaltered data throughout the process

### Clear Documentation

Record all actions for legal and internal review

### Methodology Adaptation

Evolve techniques for new technologies and threats