Digital Forensics Procedure

Forensic Investigation Triggers

Forensic investigation initiated for: Suspected data breach, insider threat, policy violation, legal hold, malware incident.

Security team determines if forensics needed. Legal counsel consulted for investigations with legal implications.

Evidence Preservation

Preserve evidence immediately upon incident detection. Don't alter or access affected systems unnecessarily.

Document chain of custody for all evidence. Use write-blockers for disk imaging. Maintain evidence integrity.

Forensic Imaging

Create bit-for-bit copies of affected systems. Use forensically sound tools (FTK Imager, dd).

Verify image integrity with cryptographic hashes (SHA-256). Store original evidence securely. Work only on copies.

Evidence Collection

Collect: Disk images, memory dumps, log files, network captures, email, documents.

Document: System configuration, running processes, network connections, user accounts, timestamps.

Maintain detailed notes of all collection activities.

Chain of Custody

Document who collected evidence, when, where, and how. Track all evidence transfers.

Store evidence in secure location with restricted access. Log all access to evidence.

Maintain chain of custody documentation for legal proceedings.

Analysis Methodology

Systematic analysis of collected evidence. Timeline reconstruction of events.

Identify: What happened, when, how, who was involved, what data was affected.

Use forensic tools: EnCase, Autopsy, Volatility, Wireshark. Document all analysis steps and findings.

Memory Analysis

Analyze RAM dumps for: Running processes, network connections, loaded drivers, encryption keys.

Memory analysis reveals information not available from disk. Volatile data lost if system powered off.

Network Forensics

Analyze network traffic captures. Identify: Communication with malicious IPs, data exfiltration, lateral movement.

Reconstruct network sessions. Extract files transferred. Identify command and control traffic.

Log Analysis

Correlate logs from multiple sources: System logs, application logs, security logs, network logs.

Identify: Authentication events, file access, process execution, network connections.

Timeline analysis reveals sequence of events.

Malware Analysis

Analyze suspicious files in isolated sandbox environment. Identify: Malware capabilities, indicators of compromise, command and control infrastructure.

Static analysis: File properties, strings, imports. Dynamic analysis: Behavior observation, network activity.

Reporting Findings

Comprehensive forensic report documenting: Investigation scope, methodology, findings, evidence, conclusions.

Include: Timeline of events, technical details, business impact, recommendations.

Report suitable for technical and non-technical audiences. May be used in legal proceedings.

Legal Considerations

Consult legal counsel before investigation. Understand legal requirements and constraints.

Maintain evidence integrity for admissibility. Follow proper procedures for chain of custody.

Privacy considerations for employee data. Comply with data protection regulations.

Expert Testimony

Forensic investigators may be called as expert witnesses. Maintain detailed documentation to support testimony.

Be prepared to explain methodology and findings. Maintain professional certifications and training.

Forensic Tools and Training

Use industry-standard forensic tools. Maintain tool licenses and updates.

Forensic team maintains certifications: GCFE, EnCE, CHFI. Regular training on new techniques and tools.

Evidence Retention

Retain evidence per legal and regulatory requirements. Typically 7 years for legal matters.

Secure storage with restricted access. Document evidence disposal when retention period expires.