EVIDENCE PRESERVATION REPORT

1. Introduction

Evidence preservation is a critical process in digital forensics and incident response that ensures security evidence is collected, stored, and maintained without modification. Proper evidence handling helps maintain data integrity and supports further investigation, legal proceedings, and incident analysis.

This practical demonstrates evidence preservation procedures using simulated forensic data based on industry practices and frameworks such as National Institute of Standards and Technology incident handling guidelines, MITRE ATT&CK attack analysis methods, and SOC monitoring practices followed by Wazuh. The process follows standard forensic principles including evidence acquisition, hashing, storage, and chain-of-custody documentation.

The objective is to collect, verify, and preserve digital evidence securely while maintaining authenticity and integrity.

2. Objective

- To understand digital evidence preservation procedures.
- To perform secure evidence collection.
- To maintain chain of custody documentation.
- To verify data integrity using hashing techniques.
- To ensure forensic readiness for incident investigation.

3. Digital Evidence Preservation Process

Evidence preservation follows structured forensic procedures.

3.1 Identification

- Identify affected systems.
- Detect compromised assets.
- Determine evidence sources.

3.2 Collection

- Acquire volatile and non-volatile data.
- Capture memory and system logs.
- Record system activity.

3.3 Preservation

- Store evidence securely.
- Prevent unauthorized access.
- Maintain original data integrity.

3.4 Documentation

- Record evidence details.
- Maintain chain-of-custody records.
- Track handling procedures.

3.5 Verification

- Generate hash values.
- Validate evidence authenticity.

---

4. Tools

Tool	Purpose
Velociraptor	Volatile data collection
FTK Imager	Disk and memory acquisition
SHA-256 Hashing	Evidence integrity verification
Log Monitoring Tools	Activity analysis

These tools help ensure reliable forensic data collection and analysis.

---

5. Evidence Collection Procedure

Evidence was collected from compromised systems to identify malicious activity.

5.1 Volatile Data Collection

Volatile data includes temporary system information such as running processes and network connections.

Collected Volatile Data

Data Type	Description
Network Connections	Active system connections
Running Processes	Executing applications
Memory Dump	RAM data snapshot

Volatile data was collected before system shutdown to prevent data loss.

5.2 Memory Acquisition

Memory acquisition captures system RAM to analyze active processes and malware behavior.

Evidence Item	Description	Tool Used
Memory Dump	System memory capture	Velociraptor

The memory dump was stored in secure storage for forensic analysis.

5.3 Disk Evidence Collection

Disk imaging was performed to capture file system activity and system artifacts.

Evidence Item	Description	Tool Used
Disk Image	Full system disk capture	FTK Imager
Log Files	System activity records	Log Monitoring Tool

Disk images were preserved in read-only format.

---

6. Evidence Integrity Verification

To maintain authenticity, hash values were generated.

Hashing Method

- SHA-256 cryptographic hashing used.
- Ensures evidence is not modified.
- Detects unauthorized changes.

Evidence Hash Record

Evidence Item	Collected By	Date	Hash Algorithm	Hash Value
Memory Dump	SOC Analyst	18-08-2025	SHA-256	Generated
Disk Image	SOC Analyst	18-08-2025	SHA-256	Generated

Matching hash values confirm evidence integrity.

---

7. Chain of Custody Documentation

Chain of custody tracks evidence handling from collection to storage.

Chain of Custody Record

Evidence ID	Description	Collected By	Date	Storage Location
EV-001	Memory Dump	SOC Analyst	18-08-2025	Secure Storage
EV-002	Disk Image	SOC Analyst	18-08-2025	Forensic Repository

This ensures accountability and traceability.

---

8. Evidence Storage and Security

Collected evidence was stored securely using the following methods:

- Restricted access storage.
- Encrypted storage systems.
- Backup of forensic data.
- Read-only evidence format.

Secure storage prevents evidence tampering.

9. Investigation Support

Preserved evidence supports:

- Malware analysis.
- Attack reconstruction.
- Incident timeline creation.
- Root cause analysis.

Proper evidence handling improves incident response effectiveness.

---

10. Challenges in Evidence Preservation

- Risk of data alteration.
- Handling large data volumes.
- Maintaining secure storage.
- Ensuring complete documentation.

Following standard forensic procedures minimizes these risks.

---

11. Conclusion

The practical demonstrated structured evidence preservation procedures including identification, collection, verification, and storage of digital evidence. The process maintained data integrity through hashing and chain-of-custody documentation. Evidence preservation ensures reliable forensic investigation and supports effective incident response in SOC environments.