Evidence Preservation & Chain-of-Custody Report

1. Overview

This document describes the procedures followed for practicing evidence preservation and chain-of-custody documentation in a digital forensics and incident response (DFIR) scenario.

The objective is to demonstrate an understanding of how volatile data and memory evidence would be collected, preserved, and documented using appropriate tools.

2. Purpose of the Activity

- To understand proper evidence handling during an investigation
- To simulate volatile data collection using Velociraptor
- To simulate memory acquisition using Velociraptor or FTK Imager
- To practice evidence integrity verification using SHA-256
- To complete a formal chain-of-custody record

3. Tools Referenced

Tool	Purpose
Velociraptor	Remote acquisition of volatile data and memory
FTK Imager	Memory capture and imaging (alternative method)
sha256sum / Get-FileHash	Hash generation to ensure evidence integrity

4. Chain-of-Custody Documentation

Chain-of-Custody Record

Item	Description	Collected By	Date	Hash Value (SHA-256)
Memory Dump	Server-X Dump	SOC Analyst	2025-08-18	`<SHA256 hash>`

5. Simulated Evidence Collected

5.1 Volatile Data (Network Connections)

This would be collected using Velociraptor query:

```
SELECT * FROM netstat
```

This captures active network connections, providing insight into processes, open ports, and potential malicious activity.

5.2 Memory Dump (System RAM)

Memory acquisition would be performed using Velociraptor artifact:

```
Artifact.Windows.Memory.Acquisition
```

or using FTK Imager's *Capture Memory* function.

This provides investigators with in-memory evidence such as running processes, malware injections, credentials, etc.