Evidence Preservation Report

1. Objective

To preserve volatile and non-volatile forensic evidence from Windows VM using Velociraptor. This includes collection of live network connections and full memory acquisition, followed by cryptographic hashing for integrity verification.

2. Volatile Evidence Collection

Procedure Summary

- Launched Velociraptor client/agent on Windows VM.
- Executed query:
- *SELECT * FROM netstat*
- Exported results as netstat.csv for forensic review.
- File secured in evidence directory with timestamp & analyst signature.

3. Memory Acquisition (Non-Volatile Evidence)

Item	Description	Collected By	Date	Hash Value
Memory Dump	Server-X Memory Acquisition (raw dump)	SOC L1 Analyst	2025-12-11	F4B95AC370BCF11761E98089733EF1D004A679D9139A3D35770AE92B17370111

Table 1: Memory acquisition

Procedure Summary

- Run Velociraptor memory acquisition artifact:
- Artifact.Windows.Memory.Acquisition
- Memory dump exported as .raw/.img format.
- Hash value generated for integrity validation using sha256sum:
- sha256sum memory.raw > hash.txt
- Hash file stored alongside netstat file.

4. Chain-of-Custody Log

Evidence	Handler	Action	Date/Time
netstat.csv	SOC L1 Analyst	Collected & Stored	2025-12-11
memory.raw	SOC L1 Analyst	Acquired & Hashed	2025-12-11
hash.txt	SOC L1 Analyst	Integrity Verified	2025-12-11

Table 2: Chain-of-Custody log

5. Summary

Evidence is preserved by collecting volatile data (netstat output) and memory dumps using Velociraptor. All evidence is hashed with SHA256, securely stored, and documented in a Chain-of-Custody form, recording who collected it, when, how, and ensuring integrity throughout the process.