Evidence Analysis Report

1. Executive Summary

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.

Item	Description	Collected By	Date	Hash Value
Netstat Log	Server-Z Log	SOC L1 Analyst	2025-12-25	dbbda55f88d35f777a29ddd7ad8a59b86 f4c277b04a4cbb109f5ba28f6214ca0

Table 1: Memory acquisition

- Hash value generated for integrity validation using sha256sum:
- certutil -hashfile netstat.csv SHA256
- Hash file stored alongside netstat file.

3. Chain-of-Custody Log

Evidence	Handler	Action	Date/Time
netstat.csv	SOC L1 Analyst	Collected & Stored	2025-12-25 14:00:00
hash.txt	SOC L1 Analyst	Integrity Verified	2025-12-25 14:05:00

Table 2: Chain-of-Custody log

4. Summary

Evidence is preserved by collecting volatile data (netstat output) 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.