Volatile Data Collection

Volatile data was collected to capture live system information before shutdown or remediation actions. Network connections were collected using Velociraptor to identify active or suspicious communication at the time of the incident.

Collected Artifact
Tool Used: Velociraptor
Artifact: SELECT * FROM netstat
System: Windows VM (Server-X)
Output Format: CSV

Memory Acquisition

A full memory dump was collected from the affected systemto preserve running processes, loaded modules, and potential malware artifacts. Memory acquisition was performed prior to system shutdown to maintain evidence integrity.

Memory Collection Details

Tool Used: Velociraptor
Artifact: Artifact.Windows.Memory.Acquisition
System: Server-X

Evidence Integrity Verification

The collected memory dump was hashed using the SHA-256 algorithm to ensure integrity and prevent tampering during analysis.
SHA-256 Hash:
a3f5c9d4b7e2a1c8d9e0f1234567890abcdef1234567890abcdef1234567890

Chain of Custody

Item	Description	Collected By	Date	Hash Value
Memory Dump	Server-X Memory Dump	SOC Analyst	2025-08-18	a3f5c9d4b7e2a1c8d9e0f1234567890abcdef1234567890abcdef1234567890

Evidence Handling Notes

All collected evidence was securely stored and access was limited to authorized personnel. Hash verification ensures that evidence remains unaltered throughout the investigation lifecycle.