Evidence Chain of Custody

A. Document Name

Task 5: Evidence Chain of Custody Table

B. Purpose

This table documents preservation of the volatile memory dump. The SHA256 hash proves the evidence file was not altered after acquisition**.**

C. Chain of Custody Table

Item	Description	Collected By	Date	Hash Value
Memory Dump	Server-Y Dump	SOC Analyst	2025-08-18	<SHA256>

Importance:

- Evidence was collected using Velociraptor to ensure minimal system impact.
- SHA-256 hash was calculated immediately after acquisition.
- Evidence was stored in a write-once, access-controlled directory.
- Chain-of-custody log updated per organizational policy.

Summary (50 Words)

Volatile network connections were captured from Server-Y using Velociraptor and preserved in CSV format. A full memory dump was acquired through the Memory Acquisition artifact, then hashed using SHA-256 to ensure integrity. All evidence was documented following standard forensic chain-of-custody procedures.