

Title: Evidence Chain of Custody (Failure Documentation)

Prepared by: Mayuri Sawle

Date: 25 Nov 2025

Item	Description	Collecte d By	Date	Hash Value
Memor y Dump	Windows 10(post- SMB brute- force containment)	SOC Analyst	2025 -11- 25	e4c57e0f94cc7a4a2a8dfb301ac5541f9a9c82baedbb341d8d6c8f7d8f002ab

Evidence was preserved after SMB brute-force containment using Velociraptor to collect volatile network data and a full memory dump. Netstat connections were exported to CSV, and the memory image was hashed with SHA-256 for integrity. Chain-of-custody documentation was completed to ensure proper handling and forensic reliability.