Evidence Chain of Custody (Failure Documentation)

File Name: 4.1_Evidence_Chain_of_Custody.pdf
Incident: SMB Brute-Force Attack – Velociraptor Data Acquisition Failure
Prepared by: Abhishek Tiwary – SOC Analyst (Tier 1)
Date: 11 Oct 2025

A. Chain of Custody Table

Item	Description	Collected By	Date	Hash Value
CrowdSec Decision Log	Verified BAN rule against Attacker IP (10.178.124.51).	SOC Analyst	11 Oct 2025	2992E8D94BC1ECD3532D5911AAAFF9C9AB16FF8C14E782321EBDB79DE96EA231
Volatile Data (Netstat)	Acquisition **Failed**: VM Kernel Incompatibility (Cannot Execute 64-bit Binary).	SOC Analyst	11 Oct 2025	N/A *(Acquisition Failed)*
Memory	Acquisition **Failed**: VM Kernel **Dump** Incompatibility.	SOC Analyst	11 Oct 2025	N/A *(Acquisition Failed)*
System Host Log	SMB Failed Login Attempts (Windows Security Event Log).	SOC Analyst	11 Oct 2025	419DCEA9D0EB2CBC6AA70FEAA4B43E73912016E05B34A543E3F4FF01150F7CC1

B. Summary

This record documents a **partial evidence collection failure** during the incident response phase.

While **CrowdSec logs and system event logs** were successfully retained and hashed, **Velociraptor volatile data and memory acquisition** failed due to **VM kernel incompatibility**. All evidence and failures were properly documented to maintain **transparency and professional integrity** in the investigation process.