**Evidence Preservation & Analysis Report**

**Date:** 2025-09-05  
**Environment:**

* Compromised Server-Y (Debian 22.x, 192.168.204.137)
* Windows 11 Agent VM (192.168.204.138)
* Attack simulation conducted with Hydra brute force on SSH.

**Tools Used:**

* **Velociraptor** (Windows Agent: evidence collection and volatile data capture)
* **FTK Imager** (disk and memory acquisition for forensic preservation)

**1) Volatile Data Collection (Windows VM 192.168.204.138)**

Volatile data was collected from the **Windows 11 Agent VM** using Velociraptor. The following query enumerated active network connections:

SELECT \* FROM netstat

**Execution (Velociraptor CLI on analyst machine):**

velociraptor query "SELECT \* FROM netstat" --format csv > netstat\_connections\_2025-08-18.csv

**Result:**  
A CSV file (netstat\_connections\_2025-08-18.csv) preserving all network sessions, including any suspicious connections to/from **192.168.204.137**.

**2) Memory Acquisition (Windows VM 192.168.204.138)**

Velociraptor’s memory acquisition artifact was used:

SELECT \* FROM Artifact.Windows.Memory.Acquisition

**Execution:**

velociraptor artifacts collect Artifact.Windows.Memory.Acquisition --output memory\_dump\_2025-08-18.raw

This created a **full memory image** of the Windows 11 Agent.

**3) Evidence Hashing (Chain-of-Custody)**

To ensure forensic integrity, the memory dump was hashed:

sha256sum memory\_dump\_2025-08-18.raw > memory\_dump\_2025-08-18.sha256

hash value:

ab34c7e29efc1c2f98e2cd23d3e8eac1f12e891a76bc87a08fa13c5a9a24d9e3 memory\_dump\_2025-08-18.raw

**4) Evidence Collection Table**

| **Item** | **Description** | **Collected By** | **Date** | **Hash Value** |
| --- | --- | --- | --- | --- |
| Netstat CSV | Network Connections | SOC Analyst | 2025-08-18 | N/A (CSV file preserved, no hash required but optional) |
| Memory Dump | Windows 11 Agent Memory | SOC Analyst | 2025-08-18 | ab34c7e29efc1c2f98e2cd23d3e8eac1f12e891a76bc87a08fa13c5a9a24d9e3 |

**5) FTK Imager Workflow (Preservation of Debian VM Disk)**

Additionally, a forensic image of **Server-Y (192.168.204.137, Debian 22.x)** was created with FTK Imager (run from host system):

1. Launch **FTK Imager** → Create Disk Image.
2. Source: Select the Debian VM virtual disk (e.g., .vdi / .vmdk).
3. Output: Save as ServerY\_Debian22\_2025-08-18.E01.
4. Generate hashes (MD5 + SHA256).

**SHA256:**

6b7a3142b991ad12fd23c14a58b94287046b631b23c5cb97e6d285c928dc765e

**6) Chain-of-Custody Documentation**

All evidence files are stored under /opt/evidence/incidents/2025-08-18-ServerY/ with strict access controls (SOC analyst only).

* **Timestamps:** Evidence collected between 2025-08-18 13:00 and 13:30 UTC.
* **Integrity:** All large artifacts hashed with SHA256.
* **Custodian:** SOC Analyst (primary handler).
* **Transfer:** If required forensics escalation, hashes and logs accompany all transfers.