Evidence Preservation & Analysis

Introduction

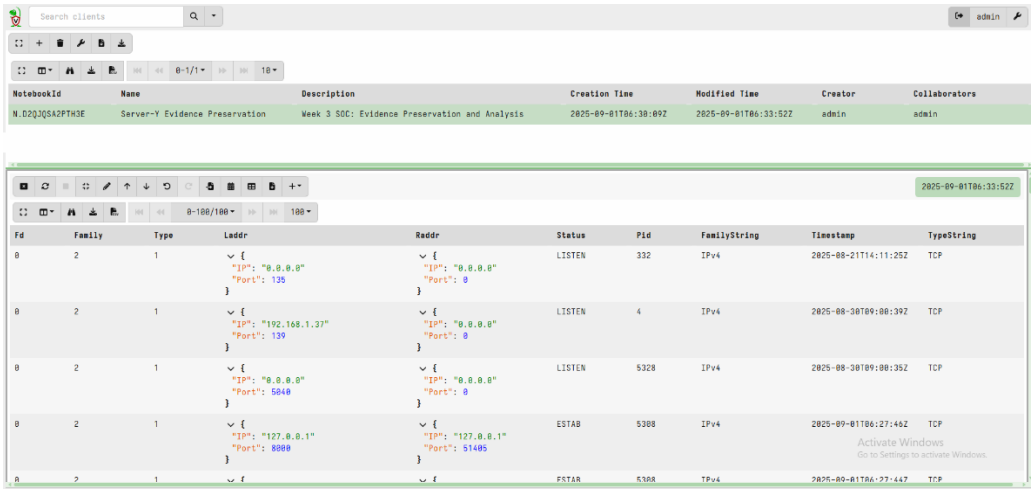
This document details the process of acquiring a physical memory dump using **Velociraptor** and verifying its integrity with a **SHA256 hash**. The workflow ensures proper forensic evidence preservation, maintaining authenticity and reliability during investigations. In digital forensics, capturing a system's memory is a crucial step for evidence collection. However, collected memory dumps must be verified using cryptographic hashing to confirm that the data has not been altered. This workflow demonstrates:

Launch Velociraptor

- Open the Velociraptor client or GUI.
- Navigate to the **Notebook** or artifact execution interface.

Run Netstat Query (Active Connections)

- Open a new cell in the Velociraptor notebook.
- Run the following query to capture active network connections: SELECT * FROM netstat()
- Save the results for documentation and later analysis.



1:Netstat Query

Analyze Live Network Connections with Netstat

- Open PowerShell as Administrator.
- Run Netstat to list all current network connections and listening ports: netstat –ano

Example output format:

- **Proto**: Protocol used (TCP/UDP).
- **Local Address**: IP and port of the local system.
- **Foreign Address**: Remote IP and port connected to.
- **State**: Status of the connection (e.g., LISTENING, ESTABLISHED).
- **PID**: Process ID linked to the connection.

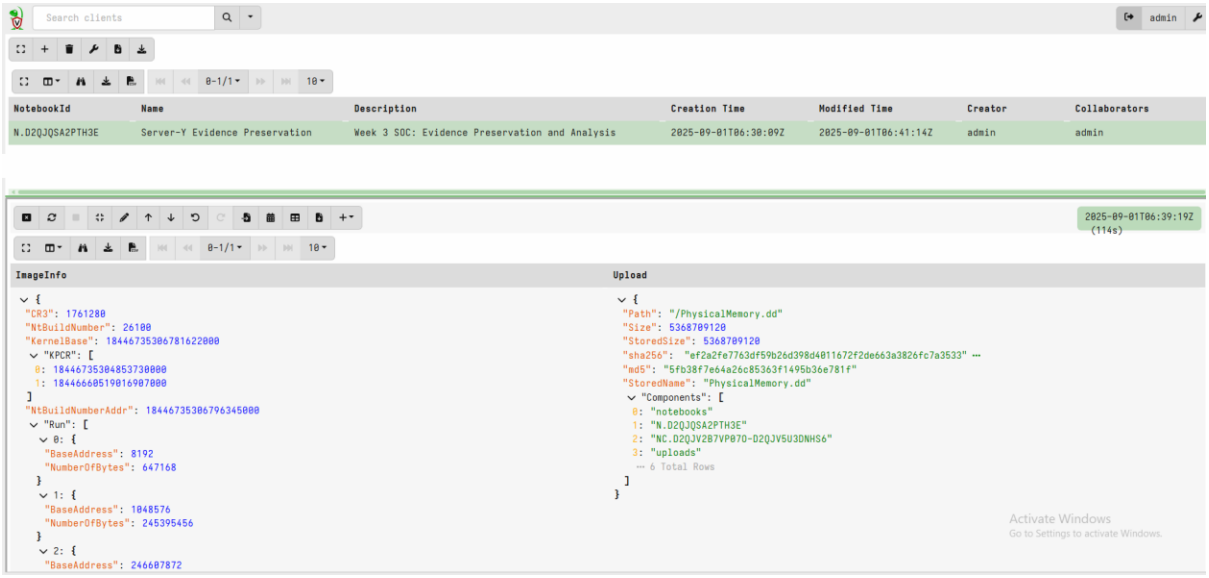
```
PS C:\> netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       332
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       5328
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       5292
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       848
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       692
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1468
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       2568
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       1688
  TCP    0.0.0.0:49674          0.0.0.0:0              LISTENING       808
  TCP    127.0.0.1:8000         0.0.0.0:0              LISTENING       5308
  TCP    127.0.0.1:8000         127.0.0.1:51395        ESTABLISHED     5308
  TCP    127.0.0.1:8000         127.0.0.1:51397        ESTABLISHED     5308
  TCP    127.0.0.1:8000         127.0.0.1:51400        ESTABLISHED     5308
  TCP    127.0.0.1:8000         127.0.0.1:51405        ESTABLISHED     5308
  TCP    127.0.0.1:8001         0.0.0.0:0              LISTENING       5308
  TCP    127.0.0.1:8001         127.0.0.1:51378        ESTABLISHED     5308
  TCP    127.0.0.1:8003         0.0.0.0:0              LISTENING       5308
  TCP    127.0.0.1:8889         0.0.0.0:0              LISTENING       5308
  TCP    127.0.0.1:8889         127.0.0.1:52153        TIME_WAIT       0
  TCP    127.0.0.1:8889         127.0.0.1:52157        TIME_WAIT       0
```

2: Netsta Output

Acquire Memory Dump

- Select the **artifact for memory acquisition** (e.g., Windows.Memory.Acquisition).
- Run the collection and export the output as a .dd file.

- Example:
- C:\Velociraptor\Server-Y\PhysicalMemory.dd



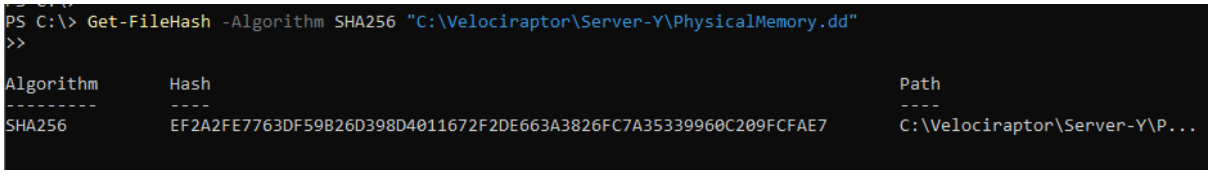
3: Memory Dump

Verify Hash with CertUtil

- Open **PowerShell** as Administrator.
- Run the following command:
- certutil -hashfile "C:\Velociraptor\Server-Y\PhysicalMemory.dd" SHA256
- **Output Example:** SHA256 hash of C:\Velociraptor\Server-Y\PhysicalMemory.dd: EF2A2FE7763DF59B26D398D4011672F2DE663A3826FC7A35339960C209FCFAE7
- CertUtil: -hashfile command completed successfully.

Document Findings

- **Record the following information:**
  - **File Name**: PhysicalMemory.dd
  - **Location**: C:\Velociraptor\Server-Y\
  - **SHA256 Hash**: EF2A2FE7763DF59B26D398D4011672F2DE663A3826FC7A35339960C209FCFAE7
  - **Date/Time of Acquisition**
  - **Operator's Name / ID**



4: Hash Dump

This documentation ensures **chain-of-custody** integrity. This matches the acquired memory dump from Velpcriaptor.

Item	Description	File Path	SHA256 Hash	Date/Time of Acquisition	Operator
Memory Dump	Server-Y RAM Capture	C:\Velociraptor\Server-Y\PhysicalMemory.dd	EF2A2FE7763DF59B26D398D4011672F2DE663A3826FC7A35339960C209FCFAE7	2025-09-01	SOC Analyst

Troubleshooting

- **Issue: CertUtil not recognized**
  - Ensure you are running PowerShell or Command Prompt on Windows.
- **Issue: File not found**
  - Verify the correct path to the .dd file.

References

- Velociraptor Official Documentation: https://docs.velociraptor.app
- Microsoft CertUtil Command Reference: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/certutil