# **EVIDENCE PRESERVATION**

## **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**

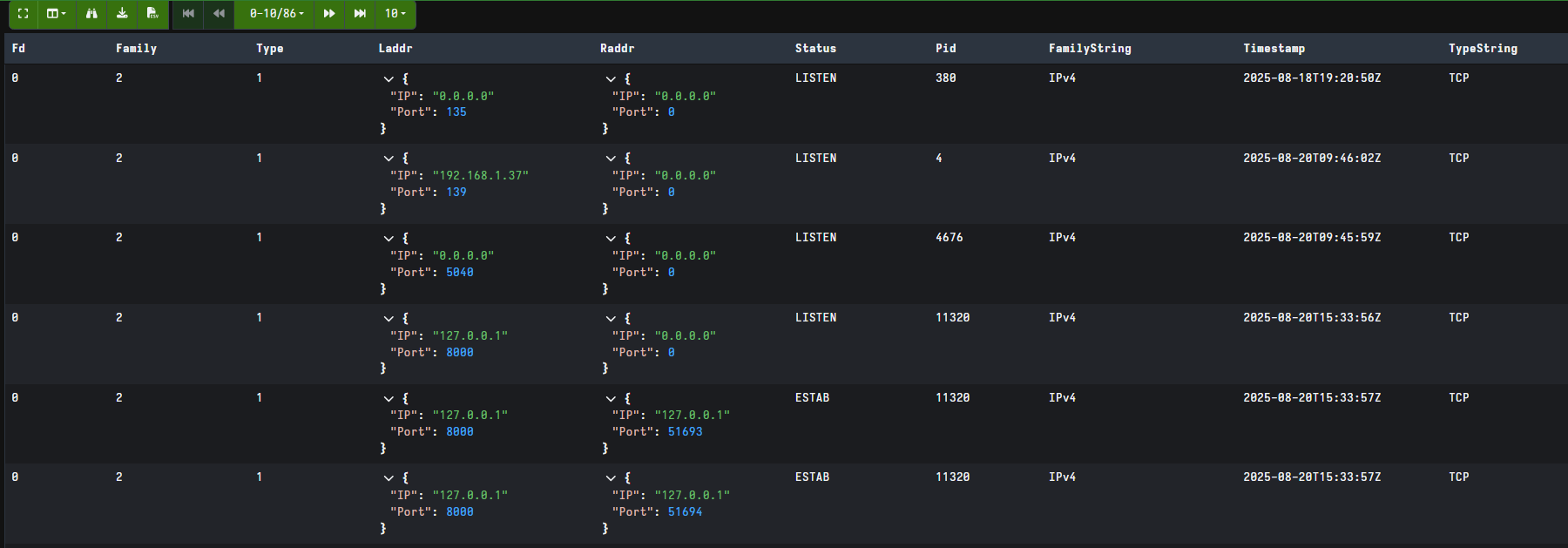
* Open the Velociraptor client or GUI.
* Navigate to the **Notebook** or artifact execution interface.

#### **Analyze Live Network Connections (Netstat)**

1. Open **PowerShell** or **Command Prompt** with admin privileges.
2. Run Netstat to list all current network connections and listening ports:

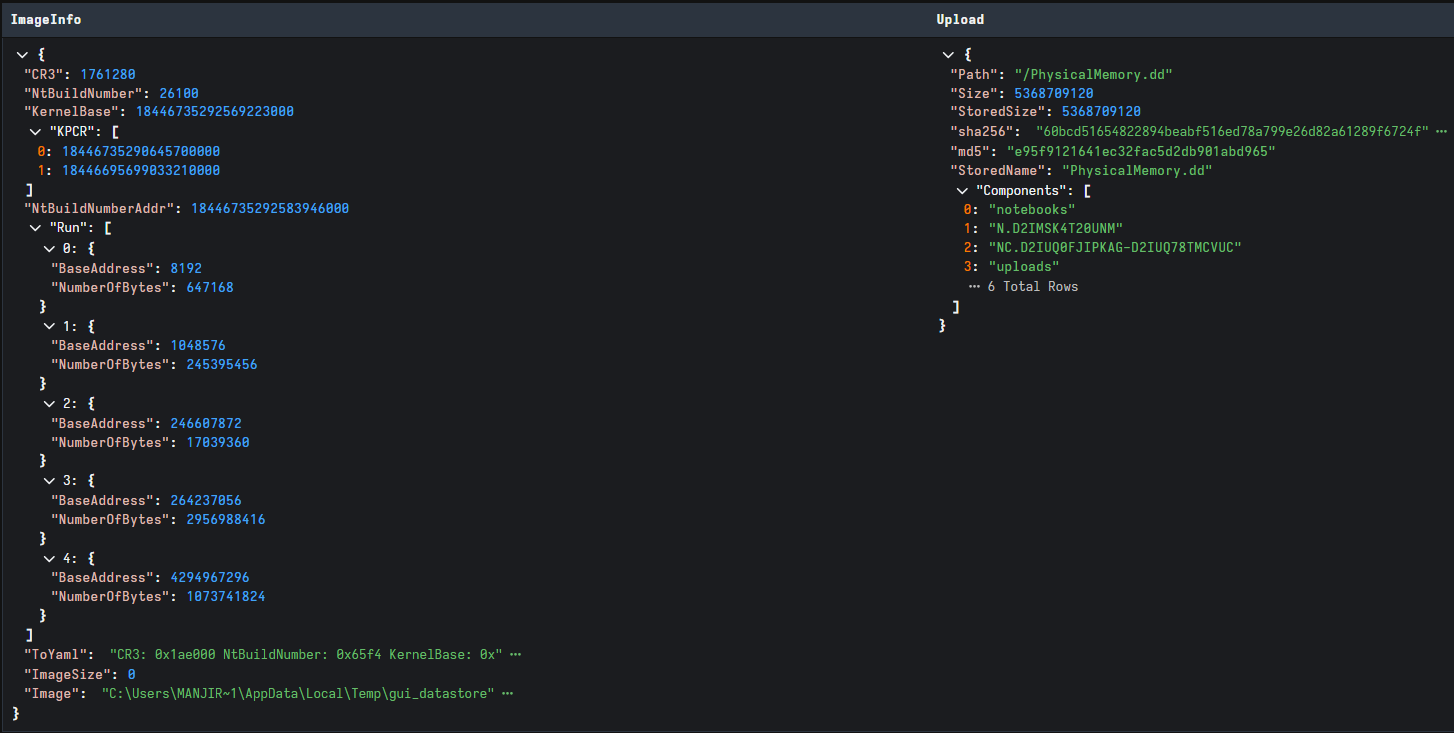
#### **Example output format:**

* **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.



#### **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\artifacts\PhysicalMemory.dd

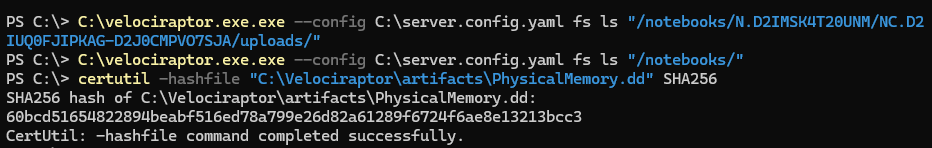


#### **Verify Hash with CertUtil**

* Open **PowerShell** as Administrator.
* Run the following command:
* certutil -hashfile "C:\Velociraptor\artifacts\PhysicalMemory.dd" SHA256
* **Output Example:** SHA256 hash of C:\Velociraptor\artifacts\PhysicalMemory.dd: 60bcd51654822894beabf516ed78a799e26d82a61289f6724f6ae8e13213bcc3
* CertUtil: -hashfile command completed successfully.

#### **Document Findings**

* **Record the following information:**
  + **File Name**: PhysicalMemory.dd
  + **Location**: C:\Velociraptor\artifacts\
  + **SHA256 Hash**: 60bcd51654822894beabf516ed78a799e26d82a61289f6724f6ae8e13213bcc3
  + **Date/Time of Acquisition**
  + **Operator’s Name / ID**



This documentation ensures **chain-of-custody** integrity.

**Troubleshooting**

* **Issue: CertUtil not recognized**
  + Ensure you are running PowerShell or Command Prompt on Windows.
* **Issue: Large file slows hashing**
  + Use SHA256 instead of SHA512 for performance balance.
* **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