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

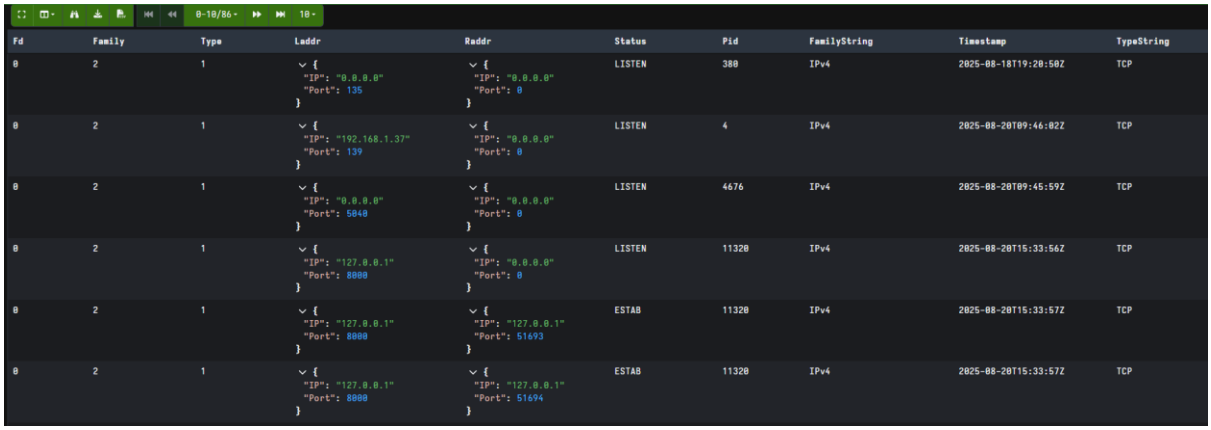
- Open the Velociraptor client or GUI.
- Navigate to the **Notebook** or artifact execution interface.

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:

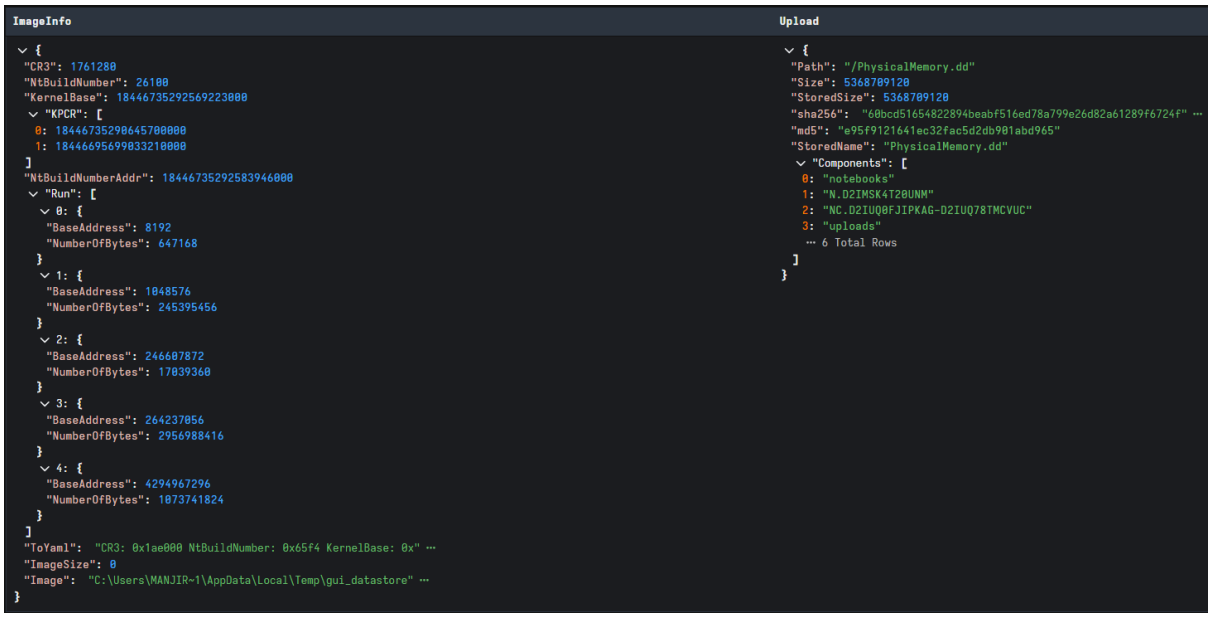
- **Proto**: Protocol used (TCP/UDP).
- **Local Address**: IP and port of the local system.
- **Foreign Address**: Remote IP and port connected to.
- **State**: Status of the connection (e.g., LISTENING, ESTABLISHED).
- **PID**: Process ID linked to the connection.



Fd	Family	Type	Laddr	Raddr	Status	Pid	FamilyString	Timestamp	TypeString
0	2	1	{ "IP": "0.0.0.0" "Port": 135 }	{ "IP": "0.0.0.0" "Port": 0 }	LISTEN	380	IPv4	2025-08-18T19:20:50Z	TCP
0	2	1	{ "IP": "192.168.1.37" "Port": 139 }	{ "IP": "0.0.0.0" "Port": 0 }	LISTEN	4	IPv4	2025-08-20T09:46:02Z	TCP
0	2	1	{ "IP": "0.0.0.0" "Port": 5040 }	{ "IP": "0.0.0.0" "Port": 0 }	LISTEN	4676	IPv4	2025-08-20T09:45:59Z	TCP
0	2	1	{ "IP": "127.0.0.1" "Port": 8000 }	{ "IP": "0.0.0.0" "Port": 0 }	LISTEN	11320	IPv4	2025-08-20T15:33:56Z	TCP
0	2	1	{ "IP": "127.0.0.1" "Port": 8000 }	{ "IP": "127.0.0.1" "Port": 51693 }	ESTAB	11320	IPv4	2025-08-20T15:33:57Z	TCP
0	2	1	{ "IP": "127.0.0.1" "Port": 8000 }	{ "IP": "127.0.0.1" "Port": 51694 }	ESTAB	11320	IPv4	2025-08-20T15:33:57Z	TCP

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



ImageInfo

```
{
 "CR3": 1761280
 "NtBuildNumber": 26100
 "KernelBase": 18446735292569223000
 "KPCR": [
  0: 18446735298645700000
  1: 18446695699833210000
 ]
 "NtBuildNumberAddr": 18446735292583946000
 "Run": [
  0: {
   "BaseAddress": 8192
   "NumberOfBytes": 647168
  }
  1: {
   "BaseAddress": 1048576
   "NumberOfBytes": 245395456
  }
  2: {
   "BaseAddress": 246607872
   "NumberOfBytes": 17039360
  }
  3: {
   "BaseAddress": 264237056
   "NumberOfBytes": 2956988416
  }
  4: {
   "BaseAddress": 4294967296
   "NumberOfBytes": 1073741824
  }
 ]
 "ToYaml": "CR3: 0x1ae000 NtBuildNumber: 0x65f4 KernelBase: 0x" …
 "ImageSize": 0
 "Image": "C:\Users\MANJIR~1\AppData\Local\Temp\gui_datastore" …
}
```

Upload

```
{
 "Path": "/PhysicalMemory.dd"
 "Size": 5368709120
 "StoredSize": 5368709120
 "sha256": "60bcd51654822894beabf516ed78a799e26d82a61289f6724f" …
 "md5": "e95f9121641ec32fac5d2db901abd965"
 "StoredName": "PhysicalMemory.dd"
 "Components": [
  0: "notebooks"
  1: "N.D2IMSK4T20UNM"
  2: "NC.D2IUQ0FJIPKAG-D2IUQ78TMCVUC"
  3: "uploads"
  … 6 Total Rows
 ]
}
```

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**

```
PS C:\> C:\velociraptor.exe.exe --config C:\server.config.yaml fs ls "/notebooks/N.D2IMSK4T20UNM/NC.D2
IUQ0FJIPKAG-D2J0CMPVO7SJA/uploads/"
PS C:\> C:\velociraptor.exe.exe --config C:\server.config.yaml fs ls "/notebooks/"
PS C:\> certutil -hashfile "C:\Velociraptor\artifacts\PhysicalMemory.dd" SHA256
SHA256 hash of C:\Velociraptor\artifacts\PhysicalMemory.dd:
60bcd51654822894beabf516ed78a799e26d82a61289f6724f6ae8e13213bcc3
CertUtil: -hashfile command completed successfully.
```

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