Author: P. Rajeev Date: 06-11-2025

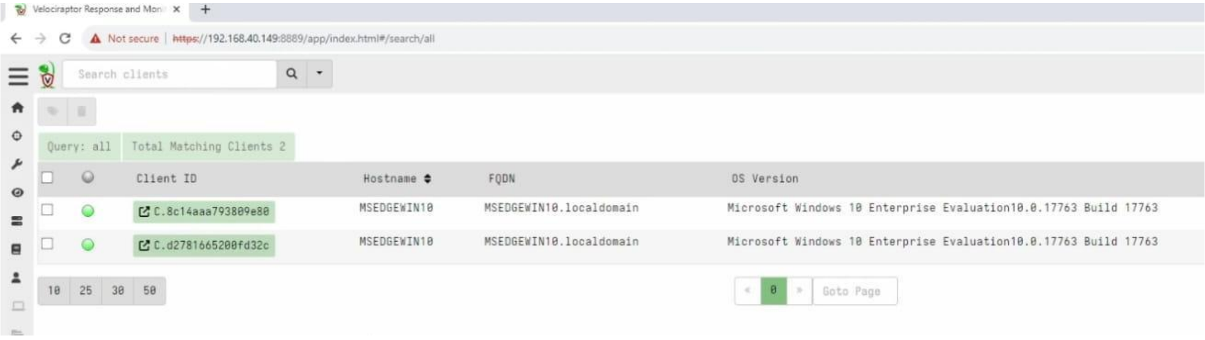
Evidence Preservation

Evidence preservation is the process of securely collecting, handling, and storing digital evidence to maintain its integrity during an investigation. It ensures that data such as logs, memory dumps, and disk images are not altered or tampered with. Proper preservation involves using write blockers, hashing (e.g., MD5, SHA256) to verify integrity, maintaining a clear chain of custody, and documenting every action taken. This guarantees that the evidence remains authentic and admissible for forensic analysis or legal proceedings.

1.Volatile Data Collection

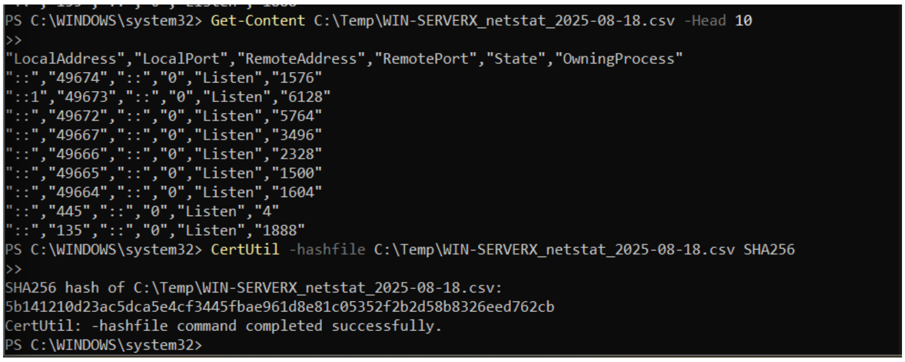
Volatile Data Collection using Velociraptor to collect network connections (SELECT * FROM nestat) from a Windows VM.

Velociraptor client and its interface shown in below image


Velociraptor Response and Mon
Not secure
https://192.168.40.149:8889/app/index.html#/search/all
Search clients
Query: all
Total Matching Clients 2
10
25
30
50
0
Goto Page

		Client ID	Hostname	FQDN	OS Version
□	●	C.8c14aaa793809e80	MSEDGEWIN10	MSEDGEWIN10.localdomain	Microsoft Windows 10 Enterprise Evaluation10.0.17763 Build 17763
□	●	C.d2781665200fd32c	MSEDGEWIN10	MSEDGEWIN10.localdomain	Microsoft Windows 10 Enterprise Evaluation10.0.17763 Build 17763

The below image shows the network statistics that include the protocols used, local and remote addresses, ports, connection states, and the owning processes. Additionally, the SHA256 hash value of the CSV file is generated using the CertUtil command to verify the integrity and authenticity of the collected network data.



```
PS C:\WINDOWS\system32> Get-Content C:\Temp\WIN-SERVERX_netstat_2025-08-18.csv -Head 10
>>
"LocalAddress","LocalPort","RemoteAddress","RemotePort","State","OwningProcess"
"::","49674","::","0","Listen","1576"
"::1","49673","::","0","Listen","6128"
"::","49672","::","0","Listen","5764"
"::","49667","::","0","Listen","3496"
"::","49666","::","0","Listen","2328"
"::","49665","::","0","Listen","1500"
"::","49664","::","0","Listen","1604"
"::","445","::","0","Listen","4"
"::","135","::","0","Listen","1888"
PS C:\WINDOWS\system32> CertUtil -hashfile C:\Temp\WIN-SERVERX_netstat_2025-08-18.csv SHA256
>>
SHA256 hash of C:\Temp\WIN-SERVERX_netstat_2025-08-18.csv:
5b141210d23ac5dca5e4cf3445fbae961d8e81c05352f2b2d58b8326eed762cb
CertUtil: -hashfile command completed successfully.
PS C:\WINDOWS\system32>
```

2. Evidence Collection

Using PowerShell, network statistics were collected from the Windows server (WIN-SERVERX) by exporting active connections and listening ports into a CSV file named **WIN-SERVERX_netstat_2025-11-06.csv**.
The file includes local and remote addresses, ports, connection states, and the corresponding owning processes.

To ensure data integrity, the collected CSV file was hashed using the **CertUtil** command with the **SHA256** algorithm.

The generated hash uniquely identifies the file and can be used later for integrity verification.

The hash file that was generated is:

5b141210d23ac5dca5e4cf34f5fbae961d8e81c05352f2bd58b8326eed762cb

Item	**Description**	**Collected By**	**Date**	**Hash Value**
Network Statistics	WIN-SERVERX Netstat CSV	SOC Analyst	2025-11-06	5b141210d23ac5dca5e4cf34f5fbae961 d8e81c05352f2bd58b8326eed762cb