Evidence Preservation

1. Objective

- This report contains the details of the task includes Volatile Data Collection, and Evidence Collection. The goal of this task is to:
- Learn collection of volatile data and also collect network connections from Windows VM.
- Collect the memory dump data as evidence and also learn hashing of a file.

2. Introduction

This task includes collection of evidence from the different sources and also learn how to create a hash file using SHA256 sum and also practice chain-of-custody.

3. Tools & Setup

- Velociraptor
- FTK Imager

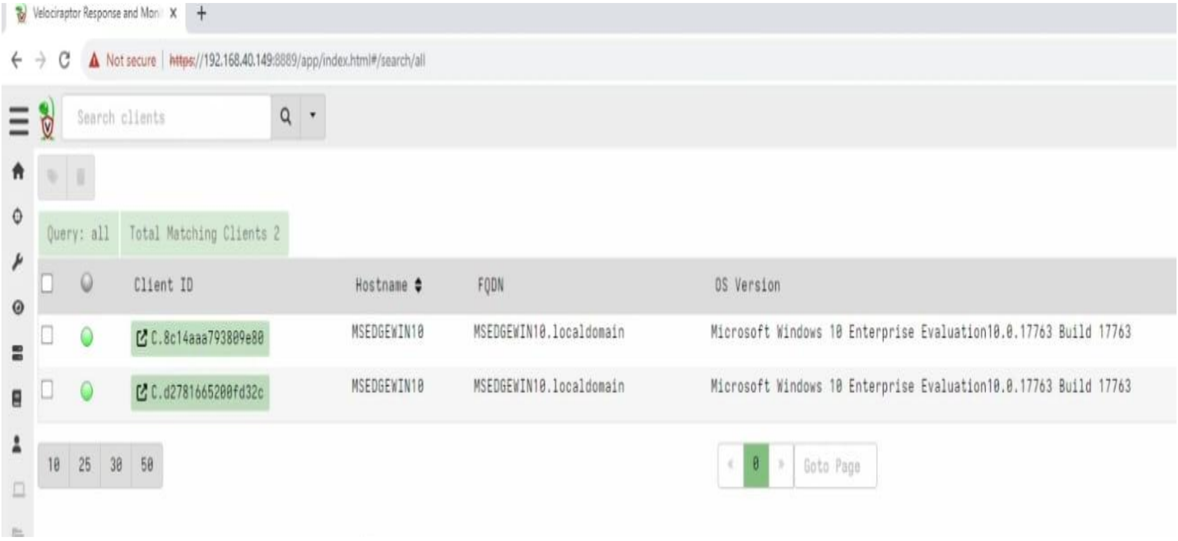
4. Evidence Preservation

Evidence preservation involves a series of procedures like creating forensic images, collecting relevant data to create a record that is not changed by anyone. This part is crucial part of incident response and digital forensics, ensuring alteration of data for later analysis.

4.1 Volatile Data Collection

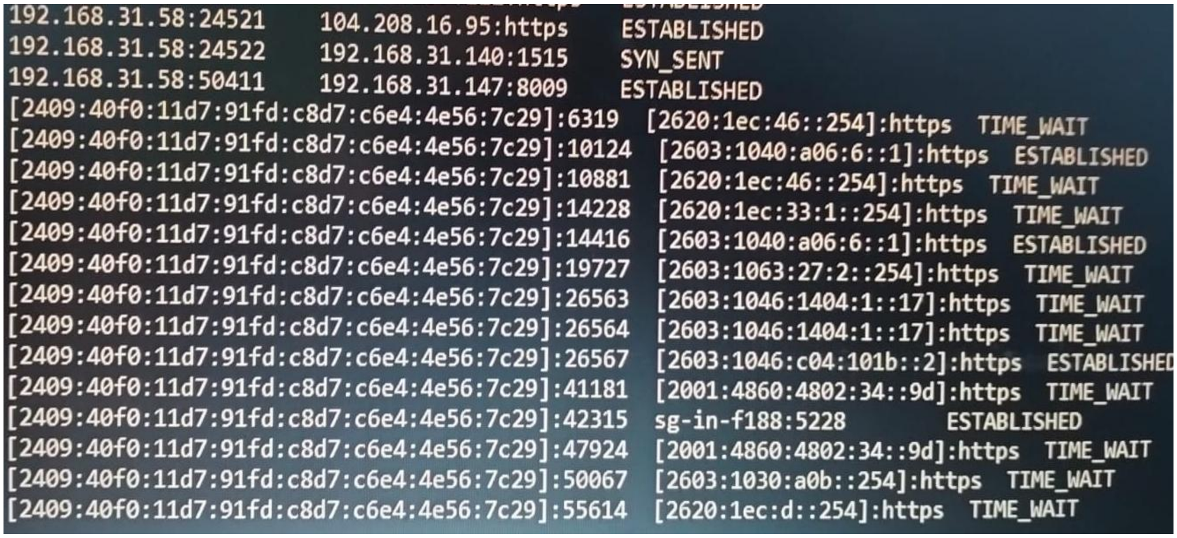
Volatile Data Collection using Velociraptor to collect network connections (SELECT * FROM nestat) from a Windows VM.

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 includes the protocols used and connections established.



```
192.168.31.58:24521    104.208.16.95:https    ESTABLISHED
192.168.31.58:24522    192.168.31.140:1515    SYN_SENT
192.168.31.58:50411    192.168.31.147:8009    ESTABLISHED
[2409:40f0:11d7:91fd:c8d7:c6e4:4e56:7c29]:6319  [2620:1ec:46::254]:https  TIME_WAIT
[2409:40f0:11d7:91fd:c8d7:c6e4:4e56:7c29]:10124  [2603:1040:a06:6::1]:https  ESTABLISHED
[2409:40f0:11d7:91fd:c8d7:c6e4:4e56:7c29]:10881  [2620:1ec:46::254]:https  TIME_WAIT
[2409:40f0:11d7:91fd:c8d7:c6e4:4e56:7c29]:14228  [2620:1ec:33:1::254]:https  TIME_WAIT
[2409:40f0:11d7:91fd:c8d7:c6e4:4e56:7c29]:14416  [2603:1040:a06:6::1]:https  ESTABLISHED
[2409:40f0:11d7:91fd:c8d7:c6e4:4e56:7c29]:19727  [2603:1063:27:2::254]:https  TIME_WAIT
[2409:40f0:11d7:91fd:c8d7:c6e4:4e56:7c29]:26563  [2603:1046:1404:1::17]:https  TIME_WAIT
[2409:40f0:11d7:91fd:c8d7:c6e4:4e56:7c29]:26564  [2603:1046:1404:1::17]:https  TIME_WAIT
[2409:40f0:11d7:91fd:c8d7:c6e4:4e56:7c29]:26567  [2603:1046:c04:101b::2]:https  ESTABLISHED
[2409:40f0:11d7:91fd:c8d7:c6e4:4e56:7c29]:41181  [2001:4860:4802:34::9d]:https  TIME_WAIT
[2409:40f0:11d7:91fd:c8d7:c6e4:4e56:7c29]:42315  sg-in-f188:5228        ESTABLISHED
[2409:40f0:11d7:91fd:c8d7:c6e4:4e56:7c29]:47924  [2001:4860:4802:34::9d]:https  TIME_WAIT
[2409:40f0:11d7:91fd:c8d7:c6e4:4e56:7c29]:50067  [2603:1030:a0b::254]:https  TIME_WAIT
[2409:40f0:11d7:91fd:c8d7:c6e4:4e56:7c29]:55614  [2620:1ec:d::254]:https  TIME_WAIT
```

4.2 Evidence Collection

Using Velociraptor collect a memory dump (SELECT* FROM Artifacts.Wnidows. Memory.Acquisition) and hash it using sha256sum.

generated a hash file using sha256sum. The hash file that generated is b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2def23d

Item	Description	Collected By	Date	Hash Value
Memory Dump	Server-X Dump	SOC Analyst	2025-10-10	b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2def23d