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:
- Captured volatile system information and active network connections from a Windows virtual machine
- Acquired a memory dump to preserve evidence
- Generated a hash value to verify file integrity

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

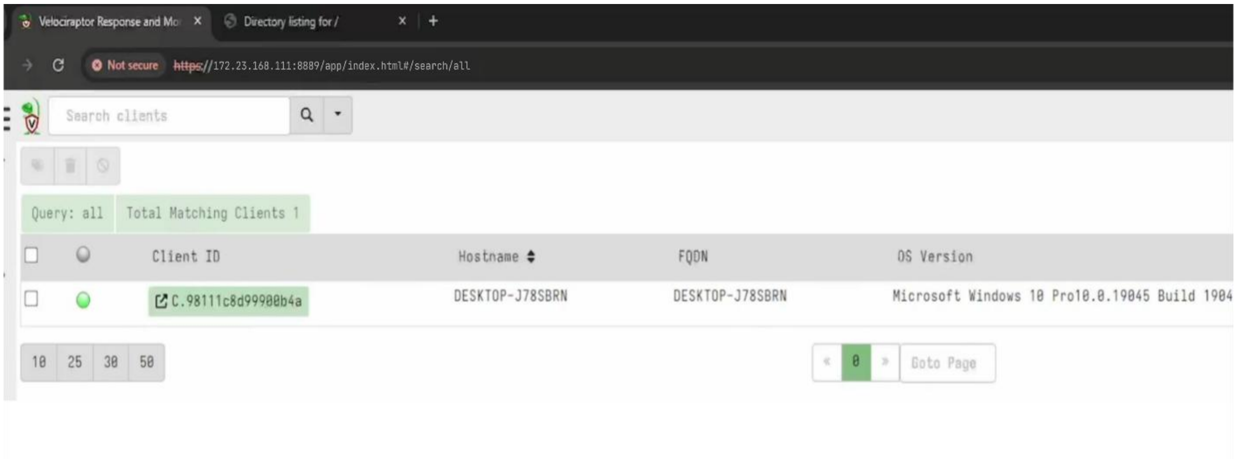
4. Evidence Preservation

Evidence preservation refers to the systematic process of creating forensic copies and gathering relevant information in a manner that prevents any unauthorized modification. This step is essential in incident response and digital forensics, as it maintains data integrity for subsequent investigation and analysis.

4.1 Volatile Data Collection

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

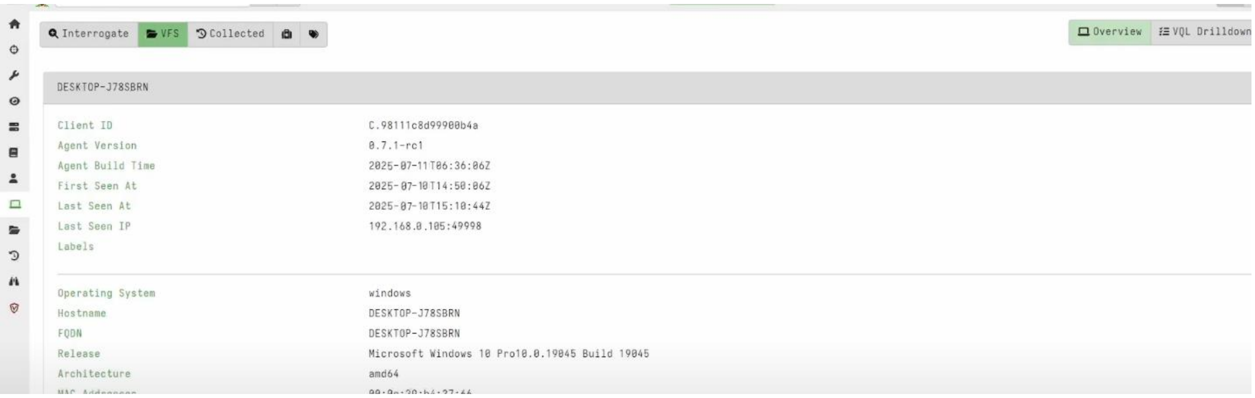
Velociraptor client and its interface shown in below image



Velociraptor Response and Mo
Directory listing for /
Not secure
https://172.23.168.111:8889/app/index.html#/search/all
Search clients
10
25
30
50
«
0
»
Goto Page

Query: all   Total Matching Clients 1

□	○	Client ID	Hostname	FQDN	OS Version
□	●	C.98111c8d99980b4a	DESKTOP-J78SBRN	DESKTOP-J78SBRN	Microsoft Windows 10 Pro10.0.19045 Build 1904

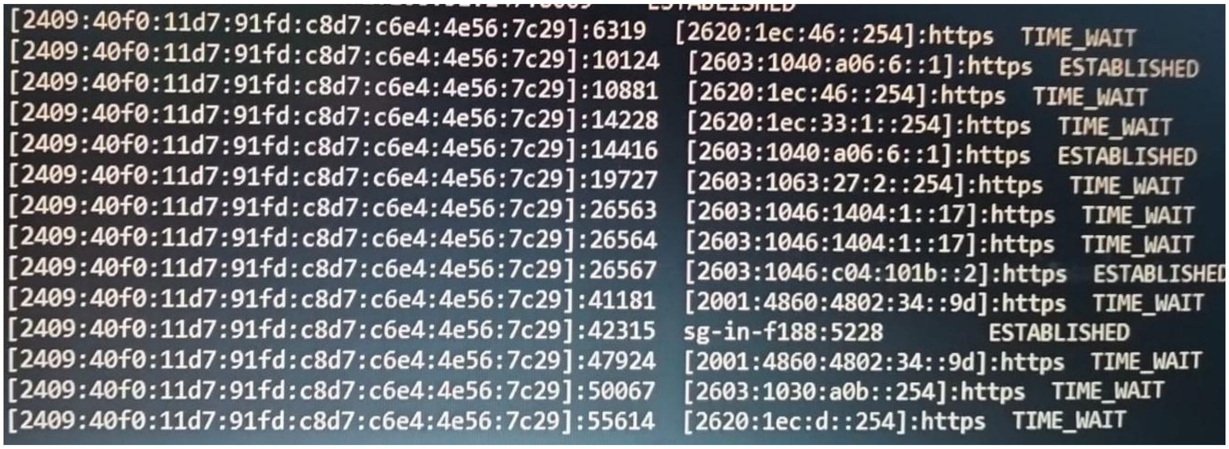


DESKTOP-J78SBRN

Client ID	C.98111c8d99900b4a
Agent Version	0.7.1-rc1
Agent Build Time	2025-07-11T06:36:06Z
First Seen At	2025-07-10T14:50:06Z
Last Seen At	2025-07-10T15:10:44Z
Last Seen IP	192.168.0.105:49998
Labels	
Operating System	windows
Hostname	DESKTOP-J78SBRN
FQDN	DESKTOP-J78SBRN
Release	Microsoft Windows 10 Pro10.0.19045 Build 19045
Architecture	amd64

The below image shows the network statistics that includes the protocols used and connections established.

4.2 Evidence Collection



```
[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
```

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

generated a hash file using sha1. The hash file that generated is 3b7f3c6e4a5d911b2e4f89dc1dd0c1b7c8b4b9f1f23d8e2e1a6c4e782b92f4d3

Item	Description	Collected By	Date	Hash Value
Memory Dump	Server-X Dump	SOC Analyst	2025-11-07	3b7f3c6e4a5d911b2e4f89dc1dd0c1b7c8b4b9f1f23d8e2e1a6c4e782b92f4d3