EVIDENCE ANALYSIS

Introduction

In this practical session Velociraptor was used to perform evidence analysis. With FTK Imager a forensic disk image of a Windows VM was acquired and integrity of evidence Objective was ensured through hashing and proper chain of custody.

Tools Used

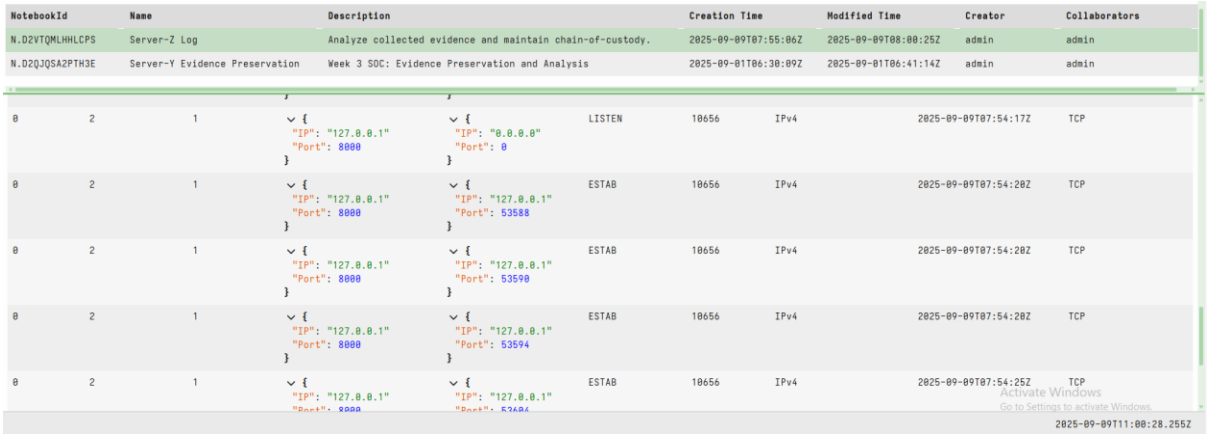
- FTK Imager: Forensic imaging tool to create a bit-by-bit copy of the VM's disk in E001 format.
- Velociraptor: Endpoint monitoring and digital forensics tool used to query system artifacts like network connections, processes, and logs.

Evidence Collection (FTK Imager)

- Selected Physical Drive as source for acquisition.
- Saved image in E01 format with compression and both MD5 + SHA256 hashing enabled.
- Verified image integrity after acquisition (source hash = image hash).
- Recorded details (examiner, case number, evidence number) during acquisition for documentation.

Analysis (Velociraptor)

- Ran a query: SELECT * FROM netstat on the Windows VM to identify active and listening connections.



NotebookId	Name	Description	Creation Time	Modified Time	Creator	Collaborators
N.D2VTQMLHHLCPS	Server-Z Log	Analyze collected evidence and maintain chain-of-custody.	2025-09-09T07:55:06Z	2025-09-09T08:00:25Z	admin	admin
N.D2QJQSA2PTH3E	Server-Y Evidence Preservation	Week 3 SOC: Evidence Preservation and Analysis	2025-09-01T06:30:09Z	2025-09-01T06:41:14Z	admin	admin

0	2	1	{ "IP": "127.0.0.1" "Port": 8000 }	{ "IP": "0.0.0.0" "Port": 0 }	LISTEN	10656	IPv4	2025-09-09T07:54:17Z	TCP
0	2	1	{ "IP": "127.0.0.1" "Port": 8000 }	{ "IP": "127.0.0.1" "Port": 53588 }	ESTAB	10656	IPv4	2025-09-09T07:54:20Z	TCP
0	2	1	{ "IP": "127.0.0.1" "Port": 8000 }	{ "IP": "127.0.0.1" "Port": 53590 }	ESTAB	10656	IPv4	2025-09-09T07:54:20Z	TCP
0	2	1	{ "IP": "127.0.0.1" "Port": 8000 }	{ "IP": "127.0.0.1" "Port": 53594 }	ESTAB	10656	IPv4	2025-09-09T07:54:20Z	TCP
0	2	1	{ "IP": "127.0.0.1" "Port": 8000 }	{ "IP": "127.0.0.1" "Port": 53604 }	ESTAB	10656	IPv4	2025-09-09T07:54:25Z	TCP

2025-09-09T11:00:28.255Z

1: Netstat Query

- Investigated unusual or persistent connections for signs of suspicious activity.

Chain-of-Custody

- Logged the evidence collection details in a table (item, description, collected by, date, hash value).
- Hash ensures that the disk image can be verified as unchanged later.

Item	Description	Collected By	Date/Time	Hash Value (SHA256)	Remarks
Disk Image	Windows VM Disk (E01)	SOC Analyst	2025-09-09 14:30 IST	af23d0c2f98e9a0d14c87d4e5e33c58f27a4b6...	Image verified OK
Netstat Log	Velociraptor export	SOC Analyst	2025-09-09 15:00 IST	47CB0EFAAFC222ADB3A6B047DD976C3D49AB8BCFD95328743A3B24515F9987F4	Collected via query

Outcome

- Forensic image successfully created and verified.
- Suspicious connections identified via Velociraptor for further triage.
- Evidence integrity preserved with proper chain-of-custody records.