

## Evidence Analysis

### 1. Objective

This report contains the details of the task including Evidence Analysis, and Chain-of-Custody..

The goal of this task is to:

- Learn analysis of evidence along with Chain-of-Custody using forensic tools.

### 2. Introduction

Evidence Analysis is a process of validating the collected evidence using tools such as Velociraptor. This tool is a forensic tool uses query language to analyze the evidence collected. This task focuses on utilizing Velociraptor to analyze network connections from a compromised Windows system and detect potentially malicious communication channels. Additionally, proper documentation of evidence is maintained through a chain-of-custody **record**, ensuring collected data remains authentic, untampered, and admissible during investigations. By combining technical analysis with forensic handling procedures, this exercise reinforces both analytical accuracy and legal accountability in cybersecurity operations.

### 3. Tools

- Velociraptor setup using its official documentation.  
<https://docs.velociraptor.app/downloads/>
- FTK Imager (Forensic Tool Kit) setup using documentation.  
<https://www.exterro.com/ftk-product-downloads/ftk-imager-4-7-3-81>

### 4. Evidence Analysis

Analyzing evidence, using Velociraptor tool to analyze network connections (SELECT \* FROM netstat) from a Windows VM. Identifying suspicious connections.

Search clients		Q	KARTHEEK Connected					Nani	
			0-5/5	10					
State	FlowId	Artifacts		Created	Last Active		Creator	Mb	Rows
✓	F.D448QBT029PVG	System.VFS.ListDirectory		2025-11-03T11:08:31.883Z	2025-11-03T11:08:35.454Z		Nani	0 b	4
✓	F.D44802LKJ9UEM.H	Windows.Network.Netstat		2025-11-03T11:04:57.921Z	2025-11-03T11:05:00.936Z		Nani	0 b	101
✓	F.D448M6RHM90QM.H	Windows.System.Pslist		2025-11-03T11:00:27.658Z	2025-11-03T11:00:35.984Z		Nani	0 b	225
Pid	Name	Family	Type	Status	Laddr.IP	Laddr.Port	Raddr.IP	Raddr.Port	Timestamp
1516	svchost.exe	IPv4	TCP	LISTEN	0.0.0.0	135	0.0.0.0	0	2025-11-02T10:43:38Z
4	System	IPv4	TCP	LISTEN	172.31.208.1	139	0.0.0.0	0	2025-11-02T10:45:36Z
4	System	IPv4	TCP	LISTEN	192.168.31.58	139	0.0.0.0	0	2025-11-03T08:37:43Z
4	System	IPv4	TCP	LISTEN	192.168.56.1	139	0.0.0.0	0	2025-11-03T08:37:39Z
12392	chrome.exe	IPv4	TCP	ESTAB	172.31.208.1	2035	172.31.218.207	8889	2025-11-03T10:55:53Z
8868	svchost.exe	IPv4	TCP	LISTEN	0.0.0.0	5048	0.0.0.0	0	2025-11-03T08:37:36Z
2568	svchost.exe	IPv4	TCP	LISTEN	0.0.0.0	5601	0.0.0.0	0	2025-11-02T10:43:41Z

## 5 Chain-of-Custody

Chain-of-Custody means securing the collected evidence in-order to submit to the court for the legal proceedings. In this process each and everything is completely documented. The metadata includes Item, Description, Collected By, Date, and Hash value.

The screenshot shows the VirusShare analysis interface for the file `8d3f68b16f0710f858d8c1d2c699260e6f43161a5510abb0e7ba567bd72c965b`. The main summary indicates 60/70 security vendors flagged it as malicious. Below this, the file's metadata is listed: `JRKZY.exe`, `peexe`, `calls-wmi`, `detect-debug-environment`, `64bits`, `long-sleeps`, `idle`, `runtime-modules`, `checks-disk-space`, `assembly`, `persistence`, `direct-cpu-clock-access`, Size `172.50 KB`, and Last Analysis Date `1 hour ago`. The file is identified as an `EXE` file. The interface includes tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (with 26+ items). A section titled "Crowdsourced YARA rules" lists several matches:

- Matches rule `Windows_Ransomware_Ryuk_b8a51798` from ruleset `Windows_Ransomware` at <https://github.com/elastic/protections-artifacts> by `Elastic Security`
  - ↳ `Identifies RYUK ransomware` - 1 hour ago
- Matches rule `INDICATOR_SUSPICIOUS_EXE_References_VEEAM` from ruleset `Indicator_suspicious` at <https://github.com/ditekshen/detection> by `ditekSHen`
  - ↳ `Detects executables containing many references to VEEAM. Observed in ransomware` - 1 hour ago
- Matches rule `Ryuk` from ruleset `Ryuk` at <https://github.com/kevoreilly/CAPEv2> by `kevoreilly`
  - ↳ `Ryuk Payload` - 1 hour ago
- Matches rule `INDICATOR_SUSPICIOUS_GENransomware` from ruleset `indicator_suspicious` at <https://github.com/ditekshen/detection> by `ditekSHen`
  - ↳ `Detects command variations typically used by ransomware` - 1 hour ago
- Matches rule `win_ryuk_auto` from ruleset `win.ryuk_auto` at <https://malpedia.caad.fkie.fraunhofer.de/> by `Felix Bilstein - yara-signator` at `cocacoding dot com`
  - ↳ `Detests win.ryuk` - 1 hour ago

Item	Description	Collected By	Date	Hash value
Network Log	Server-Z Log	SOC Analyst	02/11/2025	8d3f68b16f0710f858d 8c1d2c699260e6f4316 1a5510abb0e7ba567b d72c965b