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

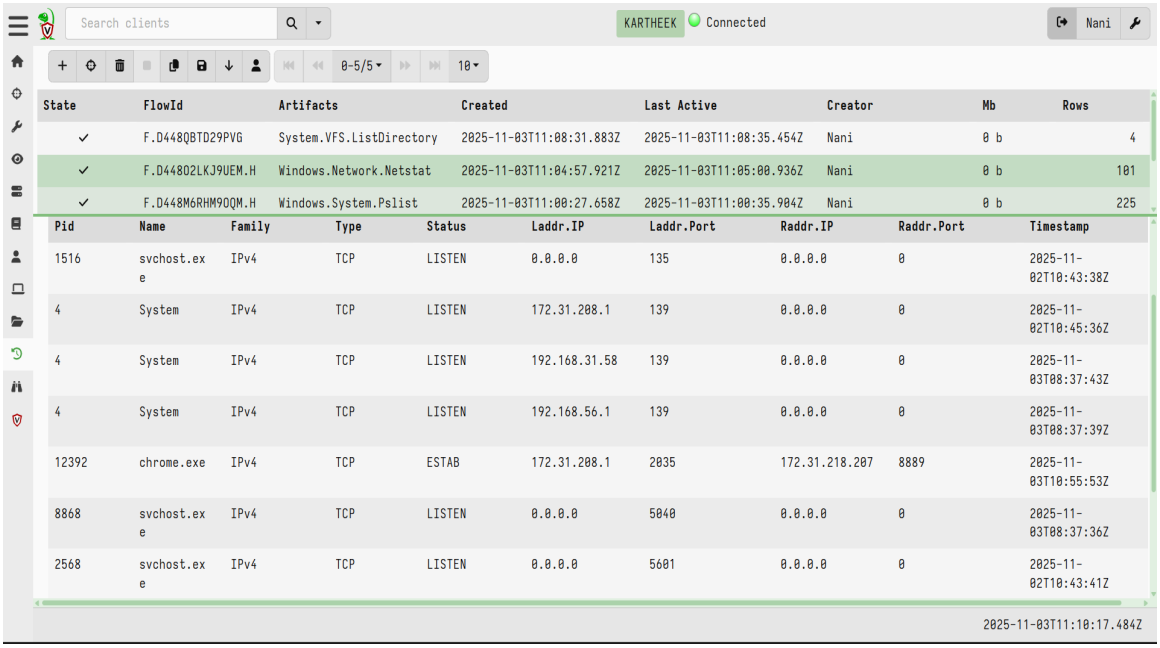
Evidence Analysis is a process of validating the collected evidence using tools such as Velociraptor. This tool is a forensic tool uses query language to analyze the evidence collected. This task focuses on utilizing Velociraptor to analyze network connections from a compromised Windows system and detect 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

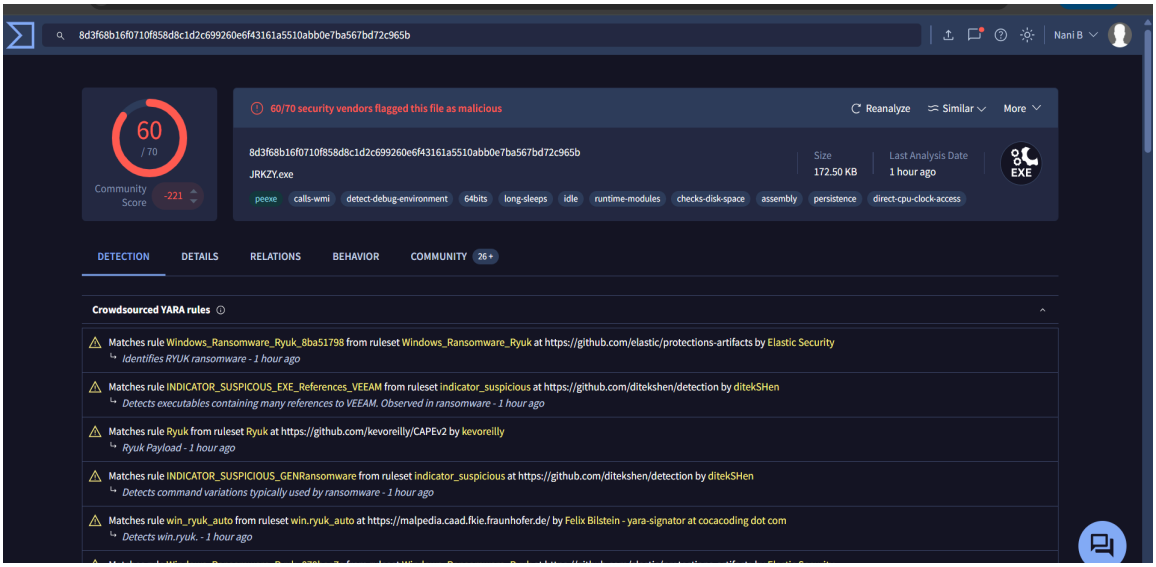
4. Evidence Analysis

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



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.



Item	Description	Collected By	Date	Hash value
Network Log	Server-Z Log	SOC Analyst	02/11/2025	8d3f68b16f0710f858d8c1d2c699260e6f43161a5510abb0e7ba567bd72c965b