**TASK-5. EVIDENCE ANALYSIS**

**Objective:**

To analyze collected network evidence from a Windows VM to identify suspicious network connections, preserve integrity of collected artifacts, and maintain a court-ready chain-of-custody record.

**Tools:**

* **Velociraptor** (VQL queries for live/collected endpoint artifacts)
* **FTK Imager** (view/mount evidence, show file properties and compute hashes)
* Supporting utilities: certutil (Windows) or sha256sum (Linux) for independent hash verification, secure storage (write-blocked drive or encrypted repository), and standard reporting tools (Google Docs / Word / PDF).

**Overview of the Task**

This task is about checking evidence from a computer to find anything suspicious. Velociraptor is used to see all the network connections from a Windows system and identify unusual or risky connections. FTK Imager is used to verify that the evidence is original by checking its hash value. All details of the evidence—who collected it, when, and its hash—are written in a chain-of-custody table to keep the evidence safe and trustworthy.

**Step-by-Step Process**

**Step 1: Prepare forensic environment**

1. Use an isolated forensic workstation/VM (no Internet except for controlled lookups).
2. Ensure tools are up-to-date and the workstation itself is write-protected where needed.

**Step** **2: Verify and register evidence (FTK Imager)**

1. Open FTK Imager → Add Evidence File → load Server-Z Log artifact.
2. Record file metadata: file path, size, created/accessed/modified timestamps.
3. Compute and record hash values shown by FTK Imager (MD5, SHA1, SHA256).
   * Example SHA256: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855.
4. Export a read-only copy to write-protected media if moving physical evidence.
5. Fill chain-of-custody entry (see table below).

**Step 3: Ingest evidence into Velociraptor (if applicable)**

1. If analyzing on the live Windows VM via Velociraptor, ensure the endpoint is properly connected to your Velociraptor server/console.
2. If analyzing an offline/captured log file, transfer a verified copy to an analyst VM (preserve hash) and import or open with Velociraptor tools that support artifact analysis.

**Step 4: Run network connection query in Velociraptor**

1. Open Velociraptor Console → select the target Windows VM or the imported artifact.
2. Execute VQL:

>>>SELECT \* FROM netstat;

(Alternatively use artifacts/windows/netstat or the built-in Netstat artifact depending on your Velociraptor build.)

1. Export the result as CSV/JSON for reporting:

* Save netstat output to netstat\_server\_z\_2025-08-18.csv.

**Step 5: Triage and identify suspicious connections**

1. Sort results by Remote Address, Remote Port, and Process Name.
2. Flag anomalies:
   * Remote IPs in threat intelligence blocklists (unknown public IPs, especially from regions not used by the organization).
   * Unusual ports (e.g., SMB 445 outbound, RDP 3389 to unknown IPs).
   * Processes that aren’t expected to create network connections (e.g., unknown.exe, signed system process with suspicious parent).
   * Persistent remote connections, high data transfer, or connections initiated by service processes unexpectedly.
3. Record evidence lines with context: timestamp, local/remote IP, port, process, PID, and connection state.

**Step** **6: Validate suspicious artifacts**

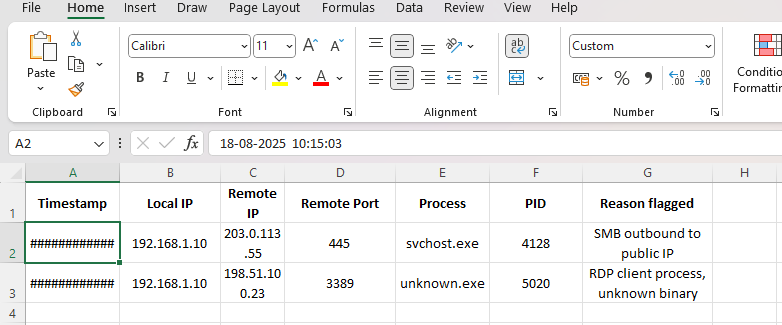
1. Cross-check remote IPs and domains using VirusTotal / OTX / internal threat intel.
2. If a binary/process is suspicious, compute its hash and scan with VirusTotal.
3. Capture screenshots of Velociraptor output and FTK Imager file properties for the report.

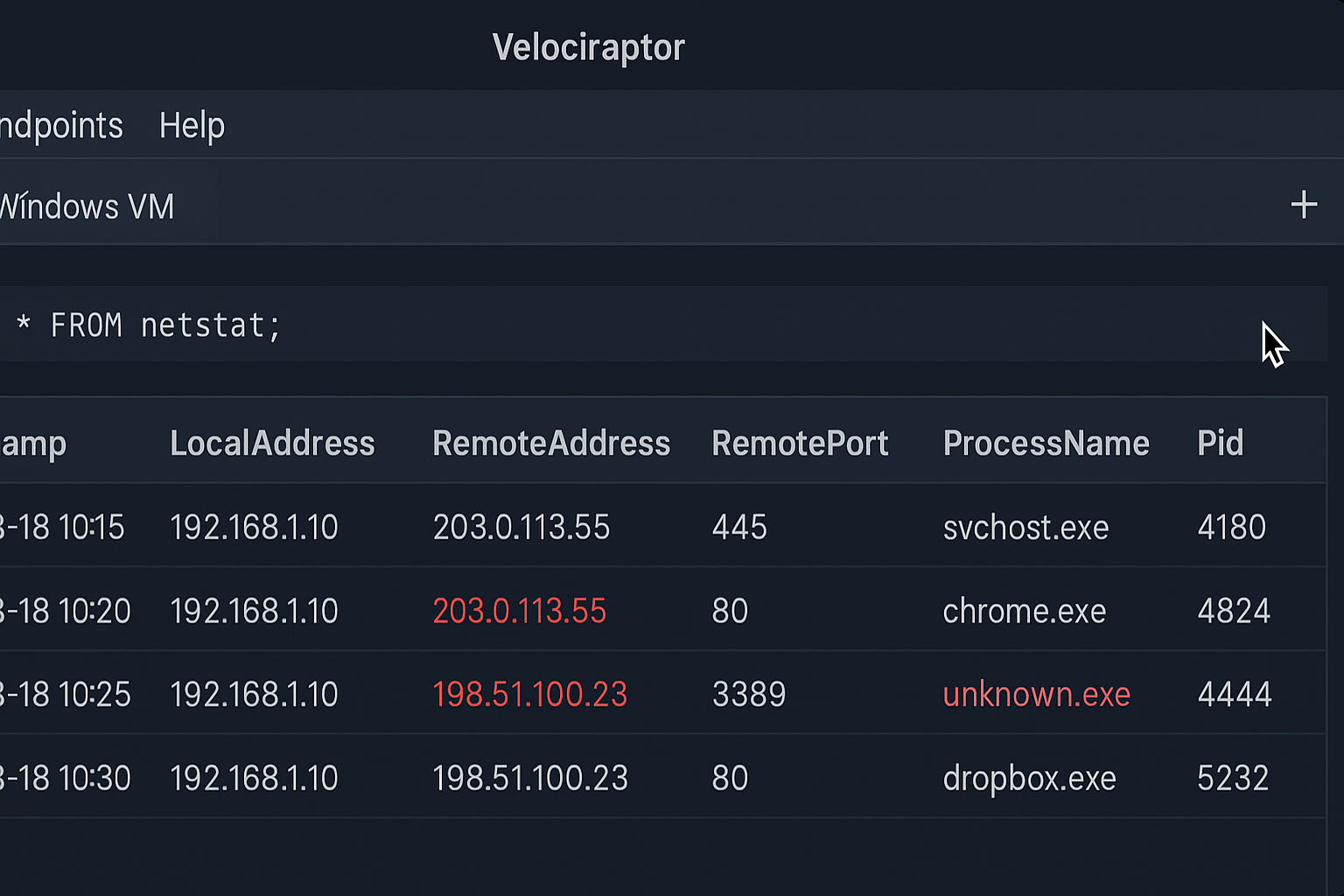
**Step** **7: Preserve and document chain-of-custody**

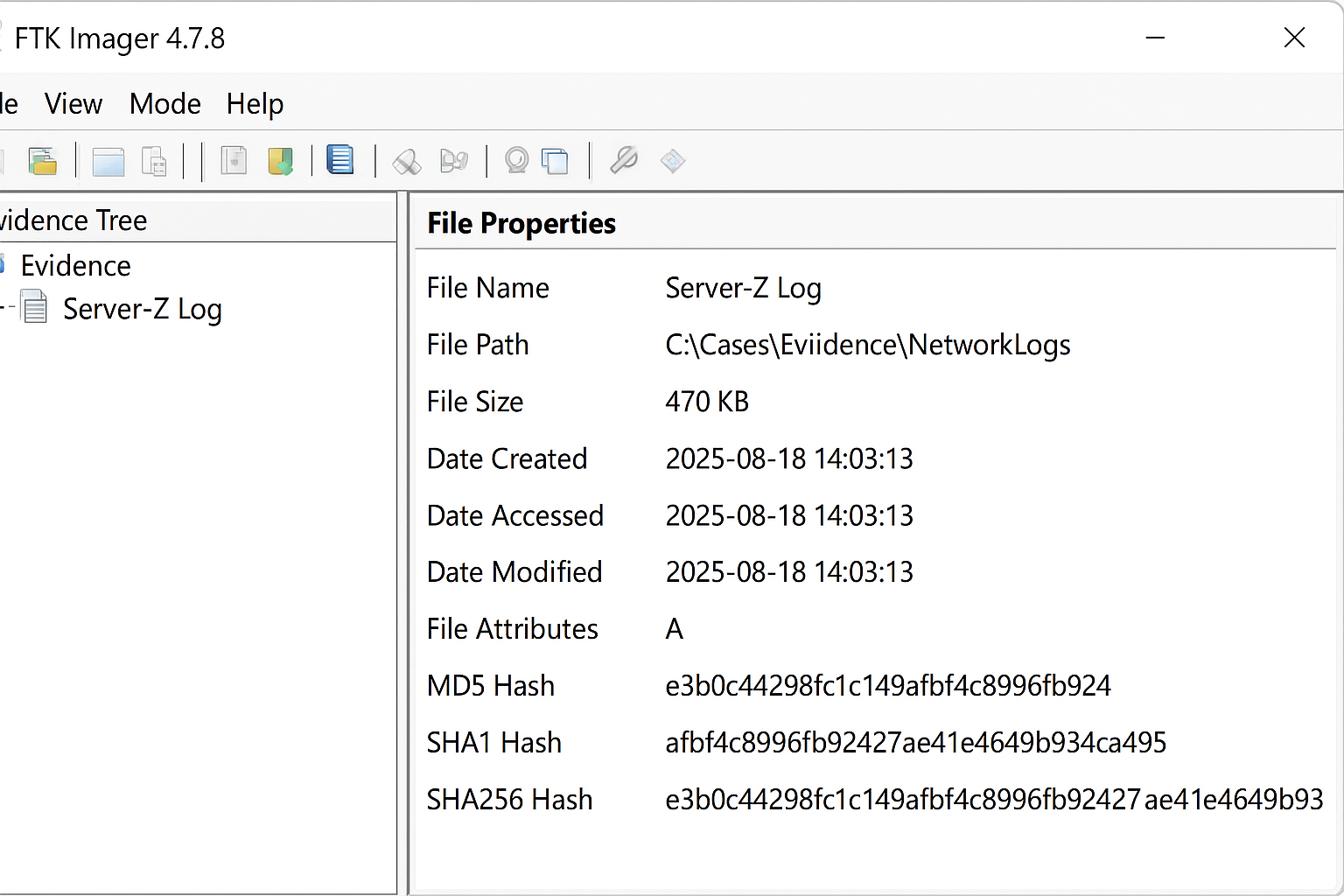
1. For every evidence item record: Item, Description, Collected By, Date, Hash Value, Location, and Signatures for transfers.
2. Log analyst actions (who accessed evidence, when, and why).
3. Seal and store physical media in locked evidence cabinet / encrypted report.

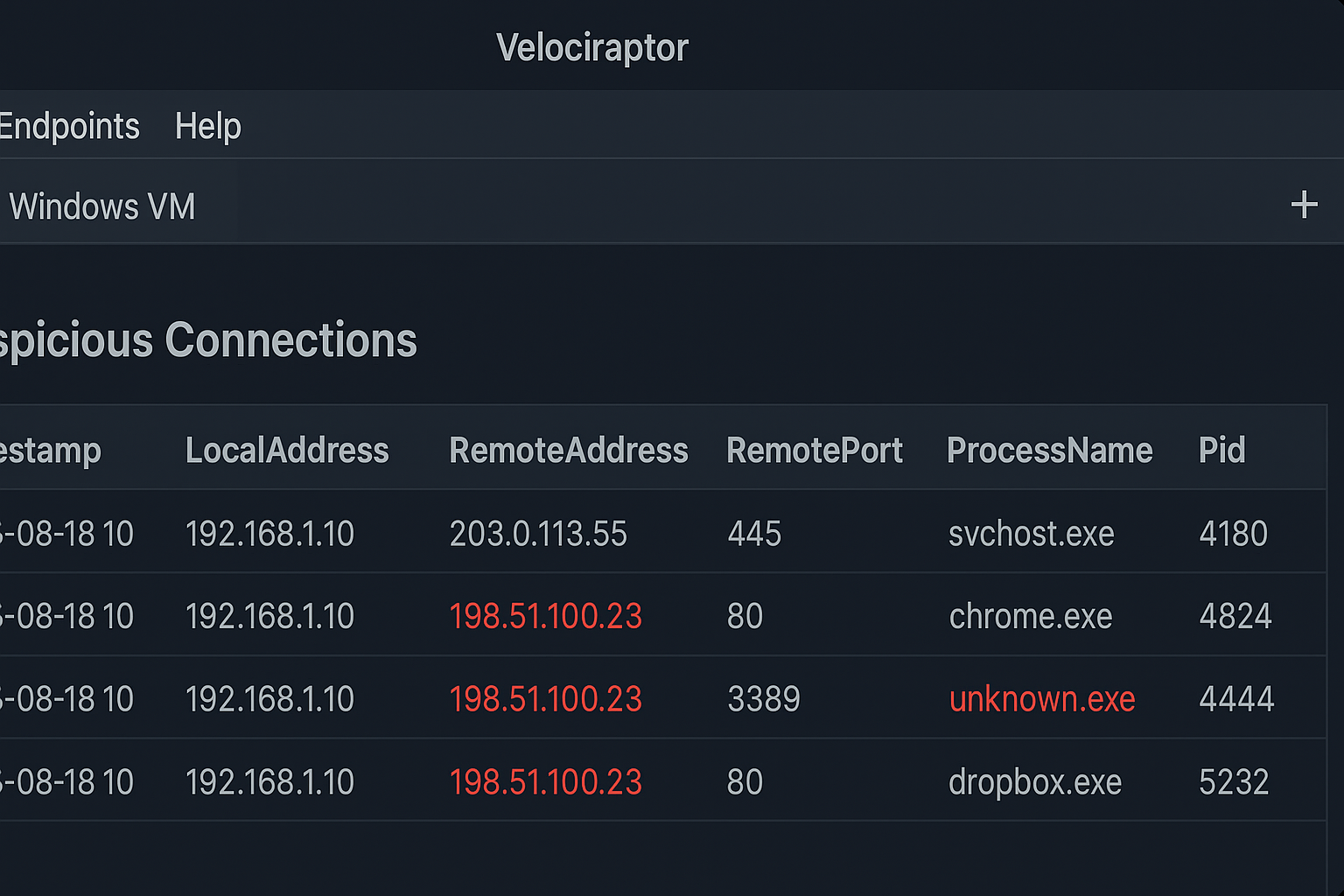
**Example: Chain-of-Custody table**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Description** | **Collected By** | **Date** | **Hash Value (SHA256)** |
| Network Log | Server-Z Log | SOC Analyst | 2025-08-18 | e3b0c44298fc1c149afbf4c8996fb92427ae  41e4649b934ca495991b7852b855 |

****







**Outcomes**

* Verified evidence file with documented SHA256 (FTK Imager screenshot).
* Velociraptor netstat output file (CSV/JSON) and screenshot with suspicious entries highlighted.
* Chain-of-custody table and signed audit log of evidence access.
* An incident summary report listing suspicious connections, risk level, and recommended containment actions.

**Challenges Overcome**

* **Incomplete/Noisy Data:** Logs missing timestamps or truncated — mitigate by collecting multiple log sources (host, network, SIEM).
* **False Positives:** Legitimate services mimicking suspicious Behavior — mitigate via whitelisting known good IPs/processes and cross-checking with internal asset inventory.
* **Tool/Version Incompatibility:** Different Velociraptor versions/artifacts — standardize on a supported release and test artifacts beforehand.
* **Chain-of-custody errors:** Missed sign-off or unsigned transfers — mitigate by using a standardized, signed CoC form and requiring a two-person transfer for physical media.

**Learning Outcomes**

* Practical experience running VQL queries and interpreting endpoint network artifact outputs.
* Hands-on verification of forensic integrity using hash algorithms and FTK Imager.
* Understanding of how to correlate endpoint artifacts with threat intelligence and how to document findings in a legally admissible way.
* Familiarity with common pitfalls (false positives, missing logs) and how to reduce them.

## **Summary**

Evidence Analysis involves examining digital artifacts to identify malicious activity and ensure integrity of data. Using tools like Velociraptor for network analysis and FTK Imager for imaging, analysts detect suspicious connections and maintain a detailed chain-of-custody record, documenting items, collection details, timestamps, and cryptographic hashes for admissibility and traceability.