Evidence Preservation and Analysis

Objective

This task focuses on **digital evidence preservation and analysis**, a critical SOC and DFIR responsibility. The objective is to **collect volatile data, acquire forensic evidence, preserve integrity using hashing, and maintain proper chain-of-custody documentation**.

Tools Used

- **Velociraptor** – Endpoint visibility and forensic data collection
- **FTK Imager** – Forensic evidence acquisition
- **sha256sum** – Cryptographic hashing for integrity verification
- **Google Sheets / Markdown** – Chain-of-custody documentation

Task Overview

1. Volatile Data Collection (Velociraptor)

Purpose:
Capture **live system information** that may be lost after shutdown or reboot.

Activity Performed:

- Connected Velociraptor to a Windows endpoint (Server-Y)
- Executed a query to collect active network connections
- Exported results to CSV format

Query Used:

```
SELECT * FROM netstat
```

Evidence Collected:

- Active TCP/UDP connections
- Remote IP addresses
- Listening services

SOC Value:
Volatile data helps identify **active attacker connections**, lateral movement, or C2 communication during an incident.

2. Evidence Collection (Memory Acquisition)

Purpose:
Preserve **system memory** for deeper forensic analysis.

Activity Performed:

- Used Velociraptor memory acquisition artifact
- Collected full memory dump from Server-Y
- Ensured evidence was stored in a secure location

Artifact Used:

```
SELECT * FROM Artifact.Windows.Memory.Acquisition
```

SOC Value:
Memory dumps can reveal:

- Running malware
- Injected processes
- Encryption keys
- Active attacker tools

3. Evidence Integrity Verification (Hashing)

Purpose:
Ensure evidence has **not been altered** during collection or storage.
Hashing Method:

```
sha256sum Server-Y-MemoryDump.raw
```

Why Hashing Matters:

- Confirms evidence integrity
- Required for legal and compliance purposes
- Protects chain-of-custody

4. Chain-of-Custody Documentation

Purpose:

Maintain accountability and traceability of collected evidence.

Evidence Log Table:

Item	Description	Collected By	Date	Hash Value
Memory Dump	Server-Y Dump	SOC Analyst	2025-08-18	<SHA256>

SOC Best Practice:

Every evidence item must have **collector name, date, and cryptographic hash**.

Summary (50 Words)

Evidence preservation activities included collecting volatile network data and acquiring a full memory dump using Velociraptor. The memory image was hashed with SHA-256 to ensure integrity. Proper chain-of-custody documentation was maintained, demonstrating adherence to forensic best practices and readiness for incident response or legal review.