1. Evidence Analysis

Objective

The objective of this activity was to collect, preserve, and analyze digital forensic evidence from a Windows virtual machine while maintaining forensic integrity and adhering to proper chain-of-custody procedures. The task focused on capturing volatile data using Velociraptor, verifying evidence integrity through cryptographic hashing, and thoroughly documenting all collected artifacts to support investigative and legal requirements..

1) Step 1: Volatile Data Collection

- Connected to the Windows VM through the Velociraptor web interface.
- Executed the following Velociraptor query to collect active network connections:
  - SELECT * FROM netstat.

Results

- Volatile data containing active network connections was successfully collected and preserved in CSV format.
- SHA-256 hashing confirmed the integrity.
- All evidence was properly documented with clear chain-of-custody records, ensuring forensic soundness and admissibility.

Item	Description	Collected By	Date	Hash value
Network Log	Server-Z log	SOC Analyst	2026-02-12	03948864fa8464a32798191b9d55d3c 6b785e3ae21175a35ab9f9c01c8e414fb

Conclusion

This task demonstrated effective evidence preservation and forensic data acquisition using Velociraptor. Volatile network data was collected while minimizing impact on the system state. Evidence integrity was validated through SHA-256 hashing to ensure authenticity. Detailed chain-of-custody documentation was maintained to preserve reliability and legal admissibility. The overall workflow aligns with established best practices in incident response and digital forensic investigations..