Step 5 - Evidence Analysis Final Report

Executive Summary

Successfully completed comprehensive digital forensics evidence analysis of Windows system (WIN-VM-01) using proper chain of custody procedures.

Analysis revealed normal business network activity with active security monitoring, no indicators of compromise detected.

Activities Completed

- Evidence collected from WIN-VM-01 (192.168.1.84)

- Chain of custody maintained with SHA256 verification

- Network & process analysis performed

Key Findings

- Normal Microsoft and Facebook traffic

- Active SIEM monitoring

- No suspicious processes or IOC found

Risk Level: LOW-MEDIUM

Recommendations:

1. Continue monitoring with Wazuh SIEM

2. Enhance process execution logging

3. Document baseline traffic

4. Retain evidence for future correlation

Investigation Team

- Lead Analyst: analyst.jane

- Analysis Date: September 27, 2025

- Analysis Platform: Kali Linux forensic workstation