M57 Jean Case – Technical Report

Date: 2025-07-27

Investigator: Mohamed Basil (MindSec)

Tool: Autopsy (Linux version)

Forensic Workflow

1. Setup and import of jean.E01 into Autopsy on Kali Linux

2. Enabled modules: File Analysis, Web Artifacts, Data Carving

3. Manual keyword search for 'confidential' and 'delete evidence'

4. Used timeline view for event correlation

5. Extracted web history and registry info on USB devices

Artifacts Recovered

- confidential_client_list.xls (Deleted)

- USB metadata (SanDisk Cruzer Blade)

- suspicious_installer.exe

Timestamps of Interest

USB Connected: 13:23:45

File Accessed: 13:24:10

File Deleted: 13:25:00

USB Disconnected: 13:25:10

Conclusion

The user performed suspicious actions involving USB usage and deletion of sensitive data. Evidence supports an intentional data exfiltration attempt.