M57 Jean Case – Executive Report

Date: 2025-07-27

Investigator: Mohamed Basil (MindSec)

Tool: Autopsy (Linux version)

# Summary

The investigation focused on suspected insider threat activity involving unauthorized USB usage and data exfiltration. Key evidence shows confidential files were accessed and deleted shortly after a SanDisk USB was connected to the system. The browsing activity suggested intentional cover-up attempts.

# Key Findings

- Deleted confidential files recovered

- USB connection with suspicious timing

- Web access to file transfer platforms

- Timeline correlation confirmed unauthorized activity

# Recommendations

- Enforce DLP policies for USB control

- Conduct employee awareness training

- Implement alerting for suspicious USB behavior