Forensic Investigation Report

Case ID: DF-001

Investigator: Abigail Jung

Date: April 21, 2025

---

1. Case Summary

On April 21, 2025, a computer lab technician reported a suspected case of unauthorized access involving a shared high school lab computer (Lab-PC01). A student was found logged into the machine, and an open file explorer window revealed a folder labeled “Staff – Confidential,” raising concerns that sensitive files may have been accessed or copied without permission.

The objective of this forensic investigation was to collect and analyze digital evidence from the suspect machine while preserving data integrity and following proper forensic methodology.

---

2. Initial Response

The initial response was performed at approximately 10:00 AM on April 21, 2025. Upon arrival, the investigator observed that the suspect system was powered on, logged into a student account, and displaying a staff-only folder in the file explorer.

Actions Taken:

- Disconnected the machine from the network by unplugging the Ethernet cable to prevent remote access or potential tampering.
- Did not shut down the machine in order to preserve any volatile data (though volatile data collection was ultimately not performed for simplicity).
- Documented the system state with a photograph and written notes.

These actions were taken to stabilize the environment, prevent further tampering, and prepare the system for evidence acquisition.

---

3. Evidence Handling and Data Integrity

To preserve the original data on the suspect system, a forensic disk image was created using **FTK Imager**:

- **Source:** Internal drive of Lab-PC01
- **Output Format:** E01 (EnCase image format)
- **Filename:** Lab-PC01_Evidence.E01
- **Destination:** USB 3.0 external drive (labeled “Evidence Copy – Case 001”)
- **Hash Algorithm Used:** SHA-256
- **Generated Hash:** 7a81c2141c03b245aa15b7b8d948d3e67ecb3f... (truncated for space)

This process ensured that the collected data was a bit-for-bit copy of the original, with cryptographic hash verification used to maintain integrity.

Date/Time	Handler	Action Taken	Notes
04/21/2025 10:00	Abi Esquivel	Isolated suspect system	Student account was active
04/21/2025 10:20	Abigail Jung	Created disk image	Image stored on external USB
04/21/2025 10:30	Abigail Jung	Secured evidence	Stored in locked cabinet

This log tracks all handlers, timestamps, and actions taken to preserve the integrity and authenticity of the evidence.

---

5. Forensic Analysis

Tool Used: Autopsy (The Sleuth Kit)

Image Analyzed: Lab-PC01_Evidence.E01

Findings:

- Navigated to C:\Users\Student\Documents and located a file titled Grades_2024.xlsx, which appeared to be copied from the staff folder.
- File access timestamps showed the file was last opened at **09:45 AM**, shortly before the technician reported the incident.
- Web browser history showed searches for “how to access locked staff files” and “Excel password remover” conducted around **09:30 AM** on the same day.
- No additional malware or suspicious executables were found on the system.

These findings confirmed the file was accessed during the session and indicate intent to bypass access controls.

---

6. Methodology Justification

- **FTK Imager** was selected for evidence acquisition due to its reliability, ability to create forensically sound images, and built-in hash verification.
- **Autopsy** was used for analysis as it provides a user-friendly interface for investigating file systems, deleted files, web history, and file metadata.
- Volatile memory was not collected in this case because the system was idle and not expected to contain time-sensitive data in RAM.

---

7. Conclusion

Based on the file access timestamps, browser activity, and the presence of a copied confidential spreadsheet in the student’s directory, there is clear evidence that the student accessed restricted staff files without authorization.

All evidence was collected and handled in accordance with digital forensics best practices. Data integrity was maintained through cryptographic hashing, and a detailed chain of custody was recorded.