COMPSFI 202
Lab 2
Due Date: 09/04/2025 @ 11:59pm

Writing and Presenting a Digital Forensics Report

Scenario

You are a junior digital forensic examiner asked to investigate a suspicious USB drive connected to a company workstation. Your task is to document the evidence and prepare to testify about your findings.

For the purposes of this lab, assume the following evidence has been discovered:

- A file named `Autorun.inf` was found on the USB drive.
- System logs show the USB drive was mounted at 9:15 AM on August 20, 2025.
- A confidential file named `Sales_Leads.xlsx` was copied to the USB drive.
- A hash value (SHA-256) was calculated for `Sales_Leads.xlsx`:

  f8b2c2b7c4d59e3b67d0f6a2b78e12b4ffb9146e8a8c59aa9a8f3a91a3e6c432

Part 1 – Install and Set Up Autopsy

1. Create a forensic report draft (1–2 pages) with the following sections:

- Abstract/Summary: Briefly explain the purpose of the investigation and what was found.
- Body of Report: Include subsections such as “Evidence Collected,” “Methods Used,” and “Findings.”
- Conclusion: State your conclusion in 3–4 sentences.
- Appendices: Add the hash value and evidence details.

2. Guidelines to follow:

- Use clear, objective language.
- Avoid personal opinions.
- Format headings and subheadings consistently.

COMPSFI 202
Lab 2
Due Date: 09/04/2025 @ 11:59pm

Part 2 – Testimony Practice

Witness Role (Fact vs. Expert)

- Identify whether your role is more suited as a fact witness or an expert witness in this case. Write 3–4 sentences explaining why.

2. Attorney Q&A Simulation

- Write down five potential questions you might be asked in court.
- Provide sample answers in your own words.
- Example:
    - *Question:* How do you know the file copied to the USB was not altered?
    - *Answer:* I verified the integrity of the file by calculating its SHA-256 hash value and confirming it matched throughout the analysis process.

Deliverables

- A 1–2 page forensic report (Word or PDF).
- A separate section with your testimony preparation answers.