

Homework

Level up your forensics discipline: collect evidence from a personal system, build a timeline template, and write a report.

Task 1 — Mini Evidence Collection

Objective: Collect (safely) forensic artifacts from your own system.

Instructions:

- Linux: `last`, `lastb`, `journalctl`, `ss -tnp`, `ps auxf`
- Windows: Event Viewer export of Security log
- Store with timestamps and a hash of each file

Deliverable: A folder structure + a `chain-of-custody.md` note.

Task 2 — Timeline Template

Objective: Build a reusable timeline template and fill it with the lab data.

Instructions:

- Columns: timestamp, source, host, user, event, mitre
- Sort by time, not by source
- Highlight the critical minute

Deliverable: A `timeline.md` with the lab incident as the example.

Task 3 — Forensic Report

Objective: Write a one-page forensic report in the style of a court exhibit.

Instructions:

- Neutral language, no speculation
- Every claim references an evidence line
- Include a limitations section (what you could not determine)

Deliverable: A 600-800 word markdown report.