

Hands On Lab – Digital Forensics Fundamentals

Tools Required:

- Download and install Autopsy (free, open-source forensic analysis tool)
<https://www.autopsy.com/download/>
- Disk image from Digital Corpora (choose a manageable size, like M57-Patents or some NPS test image) <https://cfreds.nist.gov>

By the end of this lab, you will be able to:

1. Acquire and load a forensic image into Autopsy.
2. Explore and recover deleted files.
3. Verify evidence integrity with hash values.
4. Document findings in a short report.

Part 1 – Install and Set Up Autopsy

- Download and install Autopsy from [autopsy.com/download](https://www.autopsy.com/download)
- Launch Autopsy and create a New Case.
 - Case Name: `Module1Lab_[YourLastName]`
 - Base Directory: choose a local folder.
- 2. Record the case number and directory path in your notes.

Deliverable: Screenshot of your Autopsy case creation screen.

Part 2 – Add Evidence

1. Download a small sample forensic image (suggested: NIST CFReDS “M57-Patents” image).
 - Direct link: <https://cfreds.nist.gov/>
 - Choose the smallest image file to save time
2. In Autopsy, add the image as a Data Source.
3. Generate MD5 and SHA1 hash values in Autopsy (or with a free tool like `md5sum/sha1sum` on Linux/Mac).

Deliverable: Screenshot of Autopsy showing evidence loaded + the hash values you recorded.

Part 3 – Evidence Analysis

- Use Autopsy’s “File Analysis” features to:
 - Recover a deleted file, inspect web history, documents, or system artifacts.

COMPSFI 202

Lab 1

Due Date: 09/02/2025 @ 11:59pm

- Identify and note details, such as file names, relevance, and context.

Deliverable: Screenshots of discovered evidence + brief (3–5 line) explanation.

Part 4 – Reporting & Reflection

- Use Autopsy’s report generator to produce an HTML or PDF case summary.
- Write (5–7 sentences) addressing:
 - Challenges encountered during the analysis.
 - How this approach might differ in public-sector (law enforcement) vs. private-sector (corporate) settings.

Deliverable: Autopsy-generated report and the reflection text.

Submission Checklist

- Case setup screenshot
- Image loaded + hash values screenshot
- Evidence discovery screenshots + explanations
- Autopsy report (HTML/PDF)
- Reflection write-up