

USB Forensic Investigation: Lab 1.1

General Topic: Deleted File Recovery (DFR)

High-Level Goals

This lab aims to make the student gain the following experiences/knowledge:

- (a) Experience that deleted files *can sometimes* be recovered
- (b) How to use a DFR tool (Autopsy)
- (c) Experience the difference in outcomes of recovery process in different scenarios (e.g., the deleted file being in the root folder vs. being in a sub-folder)

The Real-Life Scenario

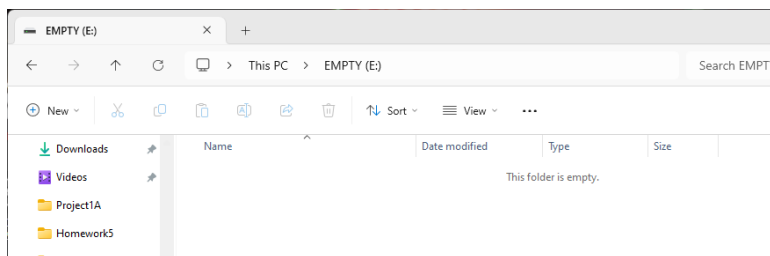
A cybercriminal named Malicious Malory has been placed under arrest for the following crimes: forgery, selling stolen gift cards, illegal drugs, elicited photos, as well as many other computer crimes. Fortunately, we found a few USB thumb drives riddled throughout her home. She claims she only used them for her photography job and deleted all the files in every thumb drive. We need evidence to convict her of her crimes.

Items needed: The instructor prepares a thumb drive (refer to the lab-setup-for-instructors document) and give it a group of students. The thumb drive has deleted “malicious” content on it.

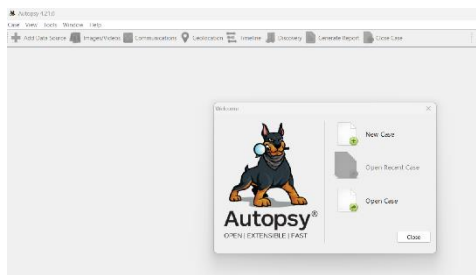
Lab Setup: Have the Autopsy software pre-installed on the Windows machine.

Task A: Startup Tasks

Task A0- Plug in the suspected thumb drive to a Windows PC. Open the contents of the thumb drive through File Explorer and note that the drive is empty.



Task A1- Launch Autopsy on the Windows PC and feed the USB drive to Autopsy.



Be sure to not add any files to the USB flash drive.

Task A2- Create a new case and hit finish when done (be patient as it loads up).

Task A3- Once the new case loads up, add the USB device as the 'local disk' and hit finish again.

Task B: Deleted File Recovery

Deleting files on a drive does not mean the data is fully deleted. In many cases, the raw data is still sitting on the storage device waiting to be overwritten by a newly created file... or recovered by a digital forensics investigator.

Main Challenge: How much data can be recovered after the files have been deleted?

Task B1- After Autopsy *completely* finishes its forensic analysis, view the 'Deleted Files' Section on the left-hand pane. One important note is that for every file that is recovered, the metadata for that specific file may be different than others. Thoroughly examine every clickable tab relating to each file.

Task C: Reporting Results

Task C1- One person out of the group needs to report the group's result in the Word Document template provided. More detail is better. Screenshots are nice as well.

Task C2- At the end, we will collect everyone's results and review them together.