

USB Forensic Investigation: Lab 1.2

General Topic: Deleted File Recovery (DFR)

High-Level Goals: This lab aims to make the student gain the following experiences/knowledge.

- (a) Experience that reformatted files *can sometimes* be recovered
- (b) How to use a DFR tool (Autopsy)
- (c) Experience the difference in outcomes of recovery process for different file types (ex: text file vs. Jpg file)

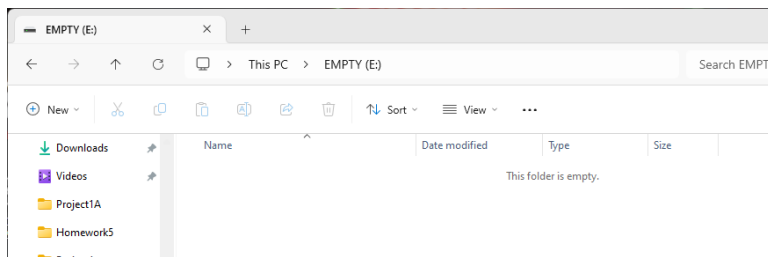
A cybercriminal named Smarter Malory has been placed under arrest for the following crimes: forgery, selling stolen gift cards, illegal drugs, elicited photos, as well as many other computer crimes. Fortunately, we found a few USB thumb drives riddled throughout her home. She claims she only used them for her photography job. In fact, she *formatted* every thumb drive recently, using the “*quick format*” option, and she is convinced that all her activity is undetectable on the flash drives. 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 had “malicious” content on it, but it is “quick formatted”.

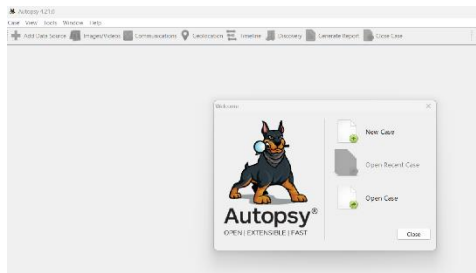
Lab Setup: Have the Autopsy software pre-installed on the Windows machine.

Task A: Startup Tasks

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



Task A1- Launch Autopsy on the Windows PC and feed in 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

Formatting drives (using the “quick format” option) 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 a drive has been reformatted?

Task B1- Just like Lab 1, investigate the recovered files in the '*Deleted Files*' Section on the left-hand pane. Be sure to check out each clickable tab on every recovered 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.