

Lab 2.2

General Topic: Investigating metadata and real data of multiple files (text file and photo file) before and after quick format

Goals

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

- (a) Create a partition in a thumb drive using a Windows computer
- (b) Create FAT file system in a partition in a thumb drive
- (c) Create a file using command line interface of Kali Linux
- (d) Identify the real data and metadata of a file using TSK commands
- (e) Recover the files (after “quick format”) using TSK commands

Items needed: Windows 10/11, and a USB thumb drive

Lab Setup: Install virtualbox software on a Windows computer, and then download a Kali VM from the official website of Kali Linux. Then, start the Kali VM.

Task A: Startup Tasks

(Note. Task A0-A1 are same as in Lab 2.1)

Task A0 – Attach the thumb drive to a Windows computer. We assume you have the admin privilege.

Task A1- Start the [disk management](#) tool, which will identify the thumb drive as a disk. Create a partition of size 1 GiB. Then format the new partition to create FAT 32 file system. Label the partition as FORENSICS. We also refer to it as FORENSICS drive.

Task B: Create the Artifacts

Motivation: We use Kali Linux VM whenever possible because Linux takes close to the system level, which would allow us to see what happens under the hood.

(Note. Task B1-B4 are same as in Lab 2.1)

Task B1- Connect the thumb drive to the Kali VM using the “Device” button on the VM. Then, run the lsblk command to identify the thumb drive. As an example, the thumb drive can be identified as /dev/sdb whereas the partition is identified as /dev/sdb1.

Task B2- Mount the partition (that we created before). You may use the following command on a command-line *terminal* to mount: `udisksctl mount -b /dev/sdb1`

As an example, the default mountpoint can be /media/dfroot/FORENSICS.

Task B3- Check the content of the FORENSICS drive on a command-line *terminal*. You need to cd to the mountpoint and then run the ls command. **Hint:** refer to the related slides of the module ppt.

Task B4- Create a file named foo.txt in the root folder of the FORENSICS drive. The file should have only one character ‘a’ as the whole content. You may use the perl command. Use ls and cat command to recheck the size and content of the new file. **Hint:** refer to the related slides of the module ppt.

Task B5- We need to copy a photo file (home.jpg) from the “resource” folder (of this lab) to the FORENSICS drive. To do so, you may detach the thumb drive from Kali VM and then on Windows host machine do the copy operation (i.e., putting home.jpg in the root directory of the FORENSICS drive) and then again attach the thumb drive to Kali VM (i.e. redoing Task B1-B2).

Task B6- Use the fls command to get the inode number of the two files (foo.txt and home.jpg). **Hint:** refer to the related slides of the module ppt.

Task B7 - Use the icat command to check the content of the root directory of the FORENSICS drive. Do you see the metadata (*directory entry*) of foo.txt and that of home.jpg? **Hint:** refer to the related slides of the module ppt.

Task C: Delete and Recover

Motivation: We want to check if we can recover files after “quick format” was done, using TSK commands (on Kali Linux), such as fls and icat.

Task C1- Format the thumb drive using “quick format” option on Windows. To do so, you may detach the thumb drive from Kali VM and then on Windows host machine do the “quick format” and then again attach the thumb drive to Kali VM (i.e. redoing Task B1-B2).

Task C2- Use fls command on the FORENSICS drive to check if it still identifies files foo.txt or home.jpg. It is likely that there is no metadata available, so metadata-based file recovery fails.

Task C3- Use “file carving” mechanism to recover the deleted files. To do so, we will use detach the thumb drive from Kali VM, and on Windows host machine run the Autopsy tool that does have the Photorec file carving module. Is foo.txt recovered? Is home.jpg recovered?

Task D: Reporting Results

Each student needs to report the above results in a Word Document. More detail is better. At the minimum, for each step (A1, B1-B7, C1-C3), paste a screenshot (total 10).