

## Lab 2.1

### General Topic: Identifying real data and metadata of a text file

#### Goals

This lab 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 file (after it was deleted) 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

**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 for the rest of the lab because Linux takes close to the system level, which would allow us to see what happens under the hood.

**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 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-** Use the `fls` command to get the inode number of the new file. **Hint:** refer to the related slides of the module ppt.

**Task B6 -** Use the `fsstat` command to get the file system information of the FORENSICS drive. What is the size of a cluster? What is the location of the reserved area, FAT area, and data area? **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`? **Hint:** refer to the related slides of the module ppt.

**Task B8 –** Carefully inspect the *directory entry* of `foo.txt`. Identify the main items there: (a) filename, (b) starting cluster index of `foo.txt`, and (c) size of `foo.txt`. **Hint:** refer to the related slides of the module ppt.

**Task B9 –** Run the `istat` command to get the stats of `foo.txt`. What is the starting sector index? Is this information consistent with what we learnt in Task B8? **Hint:** refer to the related slides of the module ppt.

**Task B10 –** Now grow the size of `foo.txt` from 1 character to 1024 characters (all 'a's). Reuse the `perl` command to do that. Reuse the `istat` command to get the current stats of `foo.txt`. How many sectors now do host the data of `foo.txt`? **Hint:** refer to the related slides of the module ppt.

### Task C: Delete and Recover

**Motivation:** We want to check if we can recover a deleted file using TSK commands (on Kali Linux), such as `fls` and `icat`.

**Task C1-** Delete `foo.txt` using the `rm` command. Check with `ls` command if the file is deleted. **Hint:** refer to the related slides of the module ppt.

**Task C2-** Use `fls` command on the FORENSICS drive to check if it still identifies (deleted) file `foo.txt`. Then, use `icat` command to recover `foo.txt`. **Hint:** refer to the related slides of the module ppt.

### 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-B10, C1-C2), paste a screenshot (total 13).