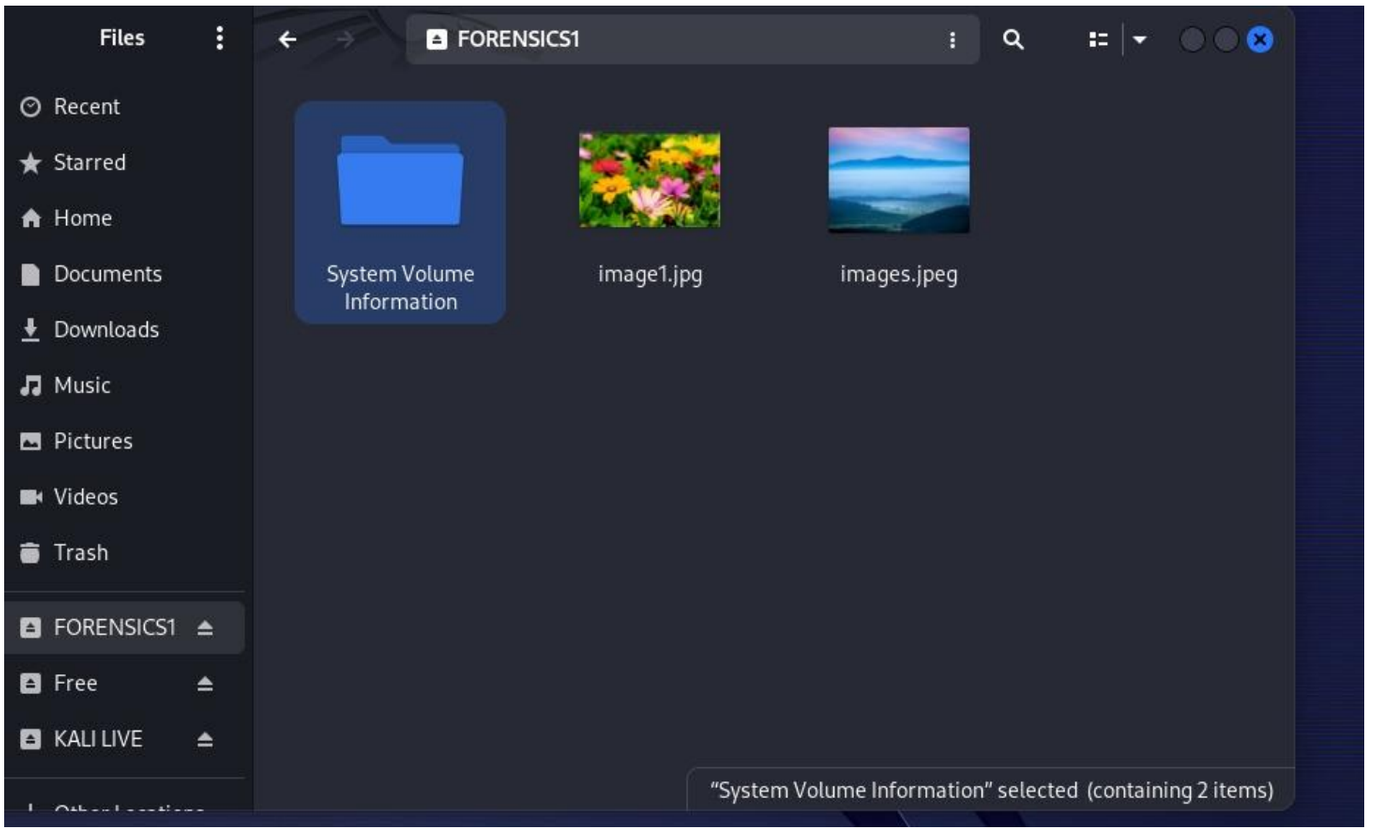
Name: Ghulam Abbas
Roll #: Fa22-BSDFCS/030
Assignment Submitted to: Ms. Fatima

==========

Assignment: Data Recovery (Manual Method Through Header and Footer)

Deleting the image form USB

Save the two jpg images in USB's partition Forensics1 and then delete



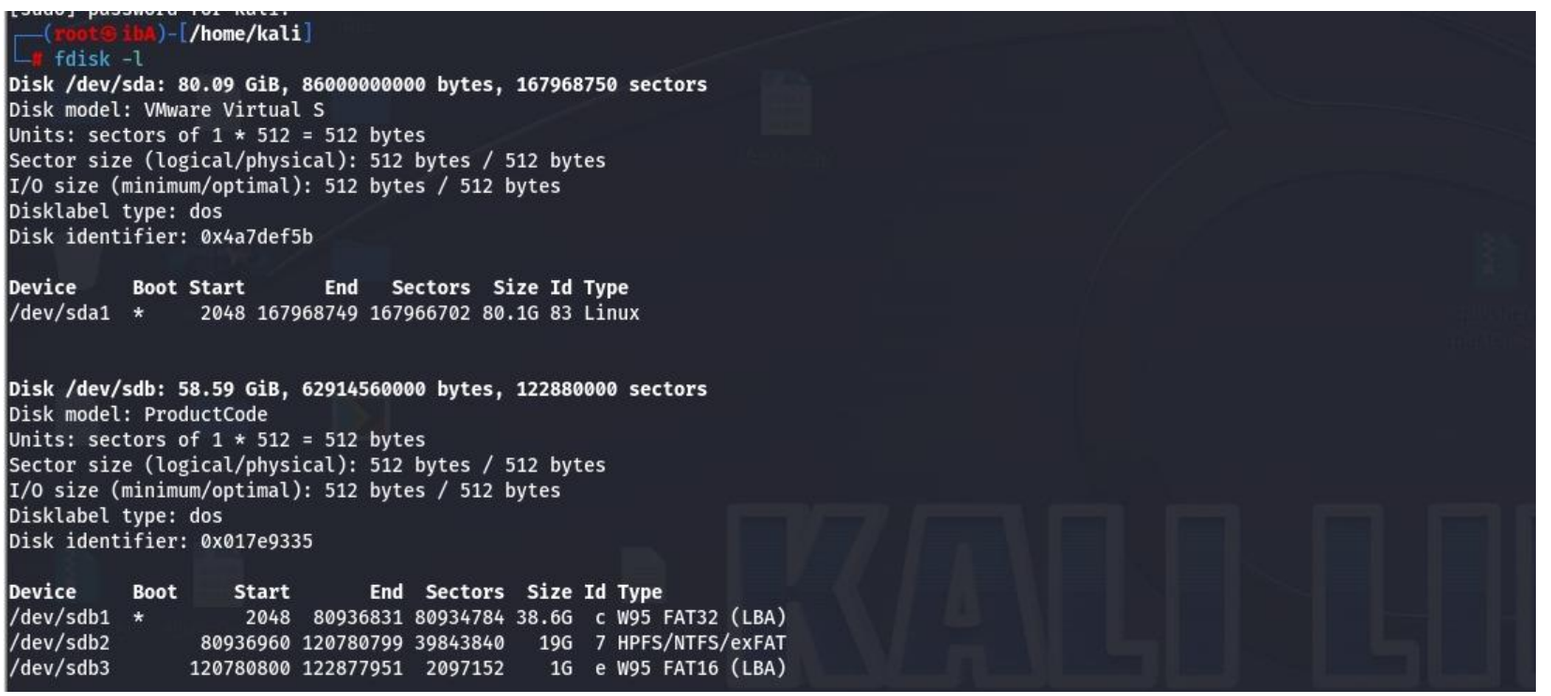
Now start the process of data recovery

1. sudo fdisk -l: -

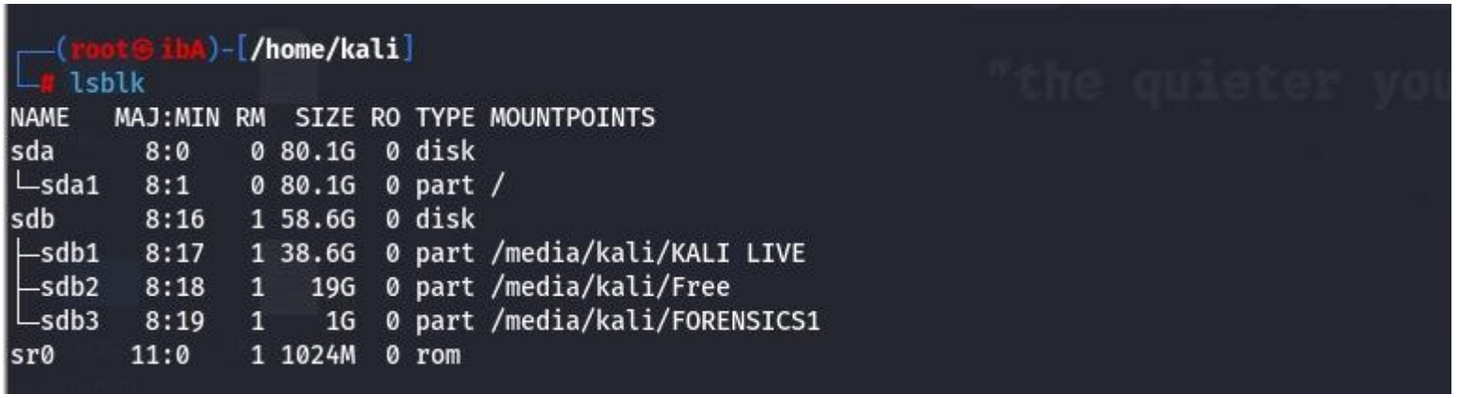
sudo: sudo: This runs the command with superuser (root) privileges, which is necessary for accessing raw disk data.
fdisk -l: The sudo fdisk -l command is used to list information about all disks and partitions currently connected to your system. Here's what it does and what you can expect from its output:

- **List Disks and Partitions:** It displays a summary of all disks (hard drives, USB drives, etc.) and their partitions available on your system.
- **Device Information:** For each device, it shows details such as the device name (/dev/sda, /dev/sdb, etc.), the size of the disk, the type of disk (e.g., GPT or MBR), and information about each partition on the disk.

Cmd: -



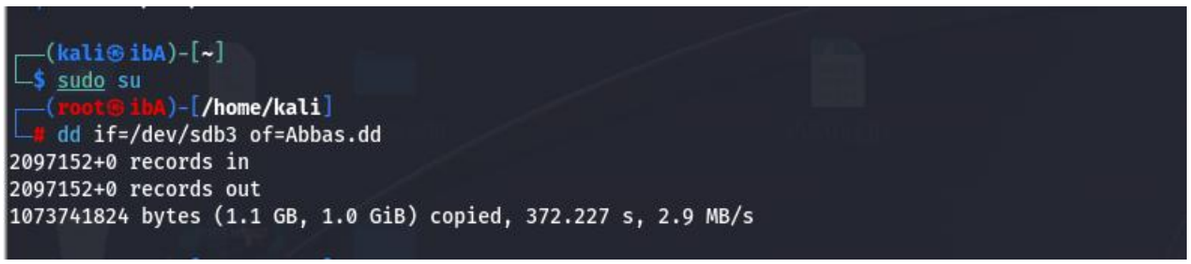
2. lsblk: The lsblk command is used to list information about block devices (such as hard drives, SSDs, USB drives) and their partitions in a tree-like format. It provides a quick overview of the storage devices connected to your system and their relationships.



3. sudo dd if=/dev/sdb3 of=Abbas.dd

The command sudo dd if=/dev/sdb3 of=Abbas.dd in Kali Linux uses the dd utility to create a bit-for-bit copy of a specified partition. Here's a breakdown of what each part of the command does:

- **sudo:** This runs the command with superuser (root) privileges, which is necessary for accessing raw disk data.
- **dd:** This is the command-line utility for low-level copying and conversion of raw data.
- **if=/dev/sdb3:** The if stands for "input file." This specifies the source, which in this case is the third partition on the second hard drive (usually sdb).
- **of=Abbas.dd:** The of stands for "output file." This specifies the destination, which is a file named Abbas.dd.



Hash of image file and device partition

Hashes play a crucial role in digital forensics and the creation of forensic images due to their ability to ensure data integrity, verify authenticity, and aid in evidence preservation.

- **md5sum Abbas.dd > hash.txt:** This command calculates the MD5 checksum (a 128-bit cryptographic hash) of the file Abbas.dd and redirects (>) the output to hash.txt. The MD5 checksum is a way to verify the integrity of a file by producing a unique hash based on its contents.
- **md5sum /dev/sdb3 >> hash.txt:** This command calculates the MD5 checksum of the device /dev/sdb3, which could be a partition or a physical device, and appends (>>) the output to hash.txt.
- **cat hash.txt:** This command displays the contents of hash.txt, showing the MD5 checksums

5. grep JFIF Abbas.dd & grep -oba JFIF Abbas.dd

The message **grep: Abbas.dd: binary file matches** indicates that grep has found matches in the binary file **Abbas.dd**, but it's not displaying the matches by default because it treats the file as binary.

The **grep** command is used to search for patterns within files. When applied to a disk image file like **Abbas.dd**, it can help identify specific data signatures within the raw data.

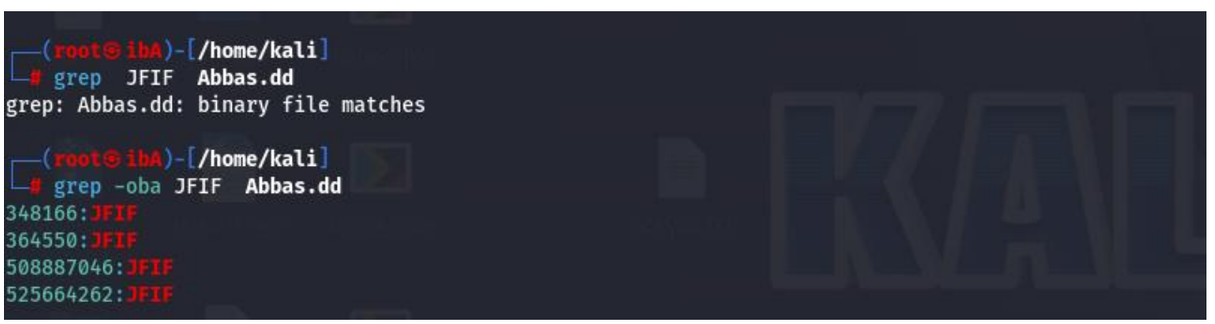
grep JFIF Abbas.dd:

- **grep:** This command searches for occurrences of the string **"JFIF"** within the file **Abbas.dd**.
- **JFIF:** JFIF is a **common marker** in JPEG image files, indicating the beginning of a JPEG file's data.
- This command will output the lines from the file Abbas.dd that contain the string "JFIF".

grep -oba JFIF Abbas.dd:

Indicates that the "JFIF" string, which marks the beginning of JPEG files, was found at the following byte offsets within the Abbas.dd disk image file:

- **-o:** Outputs only the matched parts of the line.
- **-b:** Outputs the byte offset of each matched line.
- **-a:** Treats the file as a binary file (this is crucial for raw disk images or non-text files).
- This command will output the byte offsets and the occurrences of the string **"JFIF"** within the file **Abbas.dd**.



6. xxd Abbas.dd | grep 'd9 ff'

The **xxd** command with **grep 'd9 ff'** searches for occurrences of the **JPEG file** ending marker **(0xFFD9)** within the **Abbas.dd** disk image. The output shows several occurrences, indicating possible end points of JPEG files.

- **xxd**: This command is used to create a hex dump of a file or standard input. It can also convert a hex dump back into its original binary form.
- **Abbas.dd**: This is the disk image file (dd format) you are analyzing. It could be an image of a disk or a partition obtained during forensic investigation.

- **| grep 'd9 ff'**: The pipe (|) sends the output of xxd to grep, which searches for the specified hexadecimal pattern (d9 ff).
- **JPEG Marker**: In JPEG (Joint Photographic Experts Group) files, d9 ff marks the End of Image **(EOI)**. This marker signifies the end of the JPEG data stream and is crucial for parsing and extracting JPEG images correctly.

7. sudo dd if=Abbas.dd of=sec.jpg bs=512 skip=993920 count=1198
sudo dd if=Abbas.dd of=Documents/secc.jpg bs=512 skip=1026688 count=32166

- **of=Documents/secc.jpg:** Specifies the output file (secc.jpg), where the extracted data will be saved. It's placed in the Documents directory relative to your current working directory.
- **bs=512**: Sets the block size to 512 bytes. This is the amount of data that dd will read and write at a time.
- **skip=Starting bytes**: Skips starting bytes e.g 993920 blocks from the beginning of the input file before starting to read data. Each block is 512 bytes.
- **count=ending bytes - starting bytes:** Reads and writes e.g 32166 blocks of data after skipping the specified number of blocks (skip). Each block is 512 bytes in size.

```
┌──(kali㉿ibA)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿ibA)-[/home/kali]
└─# dd if=Abbas.dd of=Documents/secc.jpg bs=512 skip=1026688  count=32166
32166+0 records in
32166+0 records out
16468992 bytes (16 MB, 16 MiB) copied, 0.925829 s, 17.8 MB/s

┌──(root㉿ibA)-[/home/kali]
└─# dd if=Abbas.dd of=Documents/sec.jpg bs=512 skip=993920 count=1198
1198+0 records in
1198+0 records out
613376 bytes (613 kB, 599 KiB) copied, 0.0608928 s, 10.1 MB/s
```

8. Data Recover: -

Deleted images are recovered