IIT BHUBANESWAR

SYSTEM FORENSIC LAB

ASSIGNMENT-2

NAME - CHANDAN KESHARI
ROLL NUMBER - 24CS06022
BRANCH - CSE(MTECH)

Questions

Use the following commands and get the results:

1. df
2. dd
3. fsstat
4. fls
5. ffind
6. istat
7. ils
8. blkstat
9. md5sum

Goal of Assignment:

The objective of this assignment is to enable the investigation of deleted files even after they have been permanently removed previously.

Solution:

In order to utilize the commands mentioned above, the initial step is to install ***sleuthkit***. This tool is a set of open-source command-line digital forensic tools created to assist in examining and analyzing disk images and file systems. ***Brian Carrier*** developed ***TSK***, which is extensively utilized by forensic investigators, law enforcement agencies, and security experts for thorough evaluations of storage media.

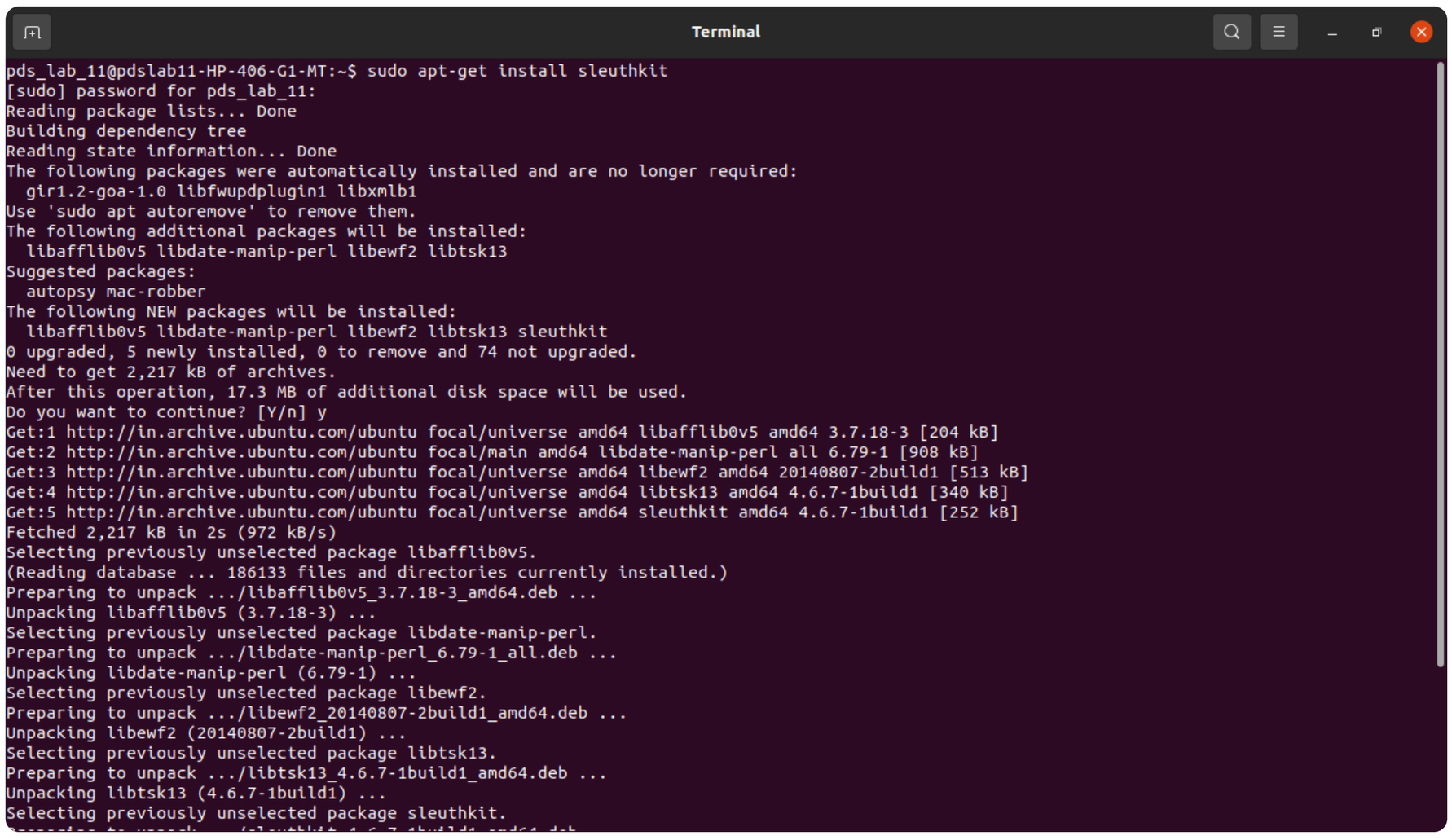
Command:

```
sudo apt-get install sleuthkit
```

Usage:

This command is typically used by forensic analysts or cybersecurity professionals who need to investigate file systems and recover data from various storage devices.

Use:



Command:

```
sudo apt-get install gparted
```

Usage:

GParted is commonly used for tasks related to disk management, including:

- Resizing partitions to allocate space for new operating systems or data.
- Creating new partitions for organizing data or for backup purposes.
- Deleting partitions that are no longer needed.
- Checking and repairing file systems.

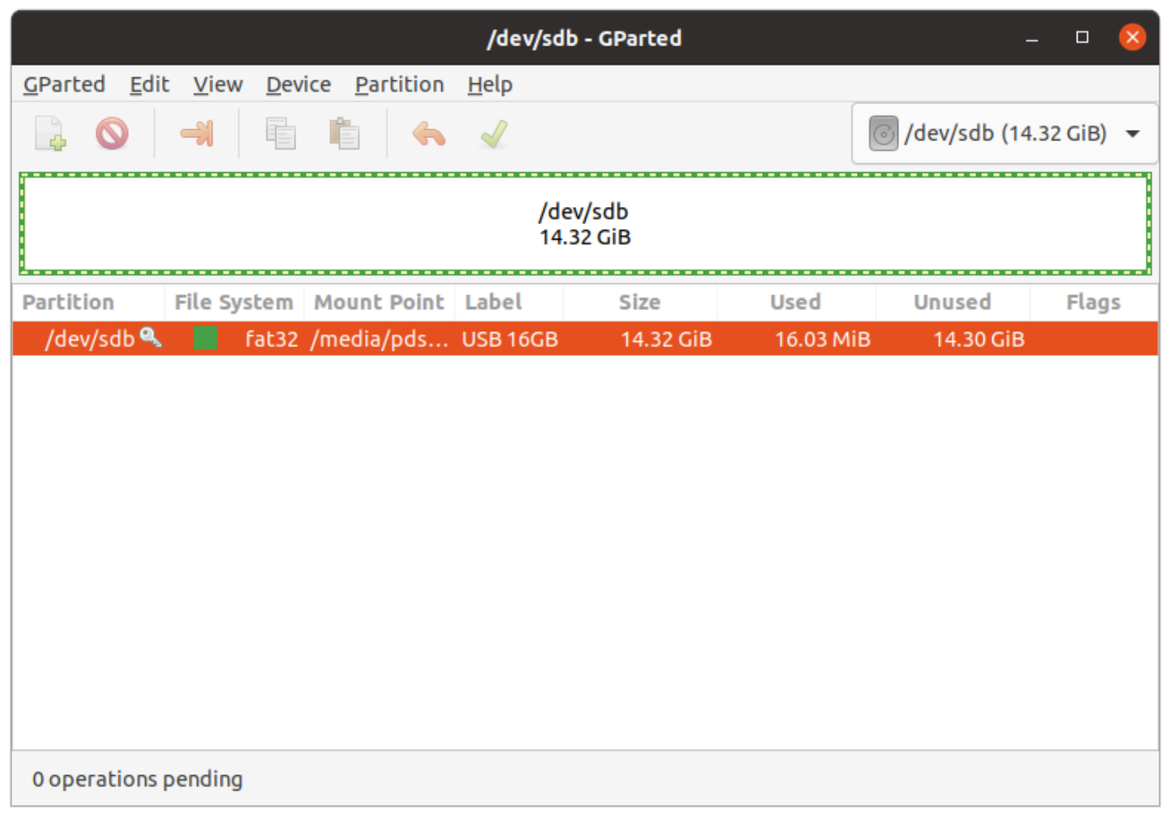
This command is essential for users who need to manage their disk partitions effectively, whether for system maintenance, installation of new operating systems, or optimizing storage usage.

Command:

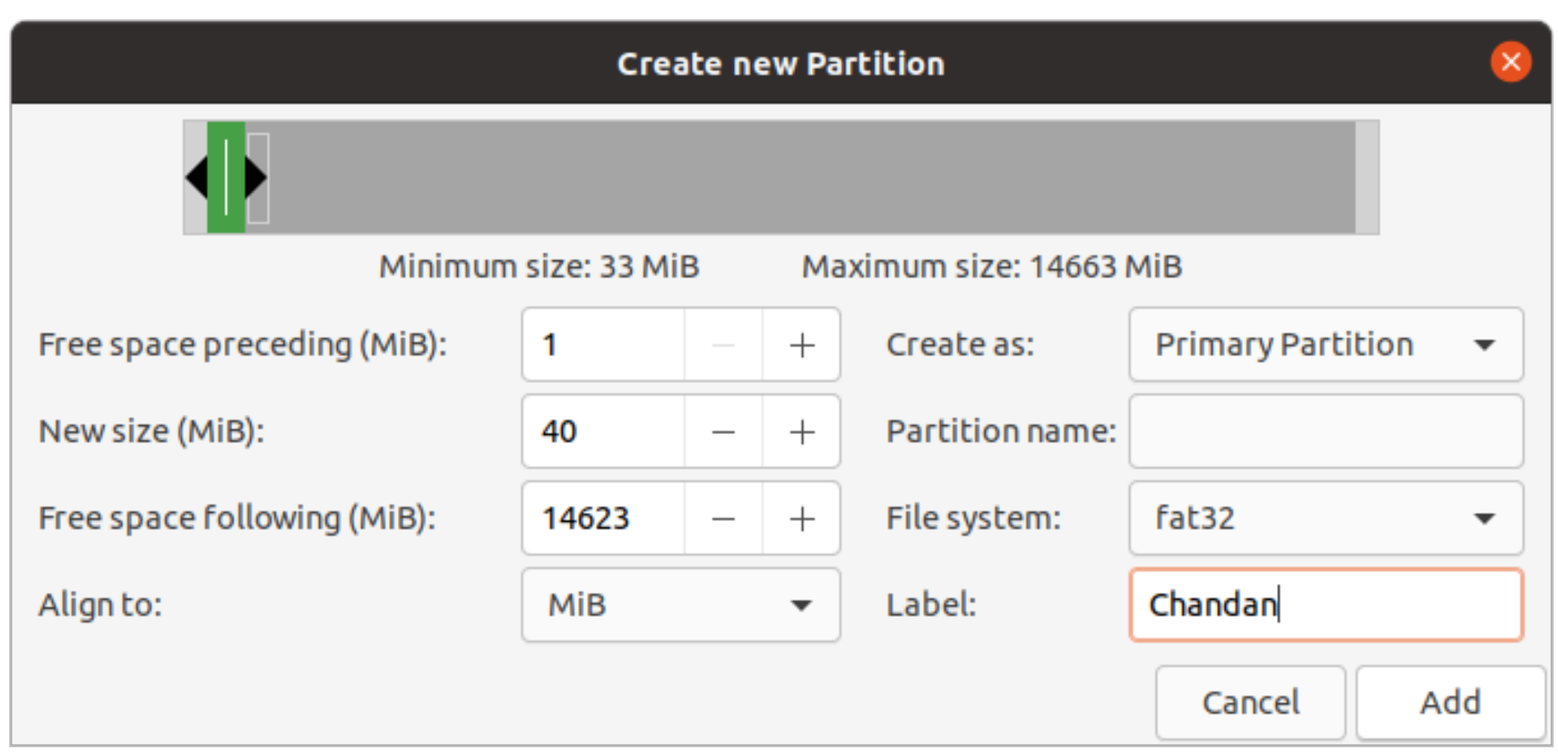
```
sudo gparted
```

This command prompt enables us to open a window for disk partitioning. In this task, we are required to split the disk into two sections: one with 40MB and the other utilizing the remaining space.

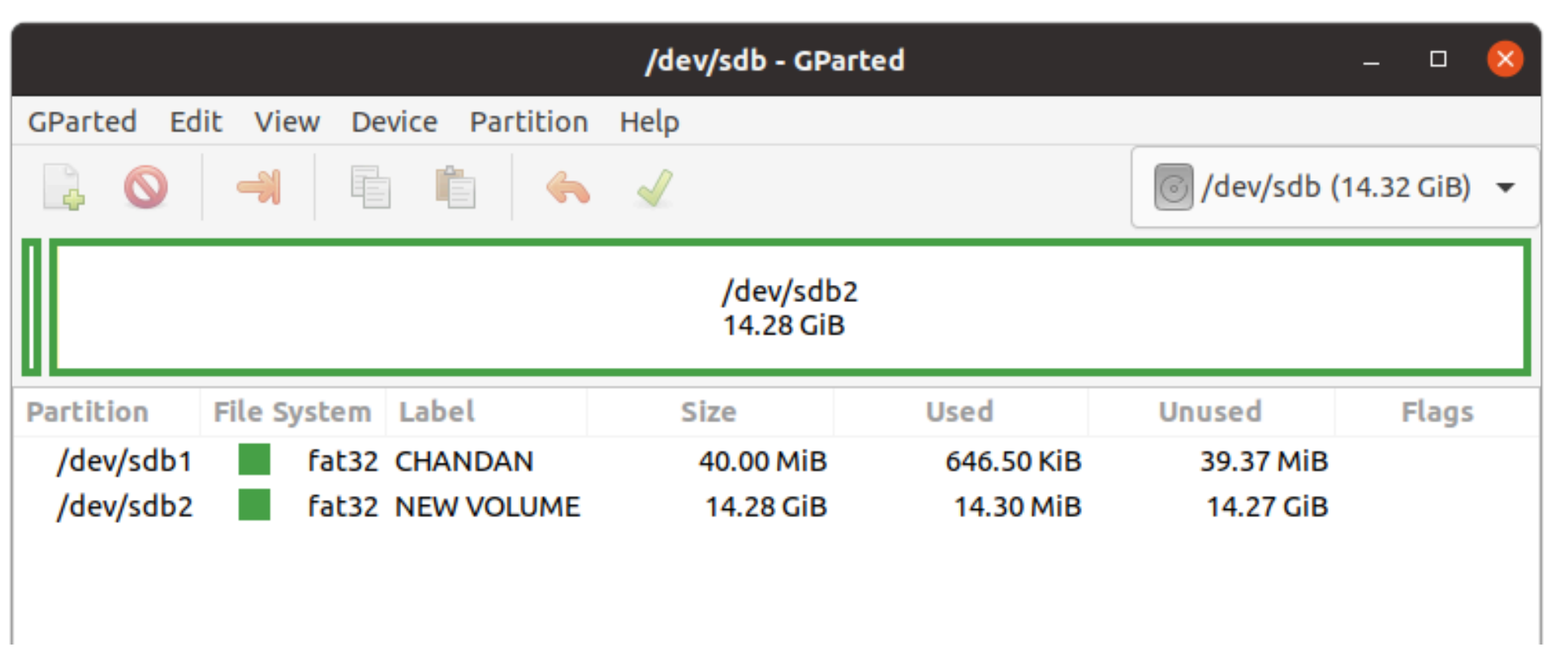
A window will pop up, allowing us to choose our preferred disk from the "GParted" menu in the top left corner. This menu displays the following details.



To create a new partition, click on the "New" button. A window will appear where you can enter details such as ***size***, ***label***, and ***file system*** for the partition.



At last, we can observe that our disk has been divided into two sections.



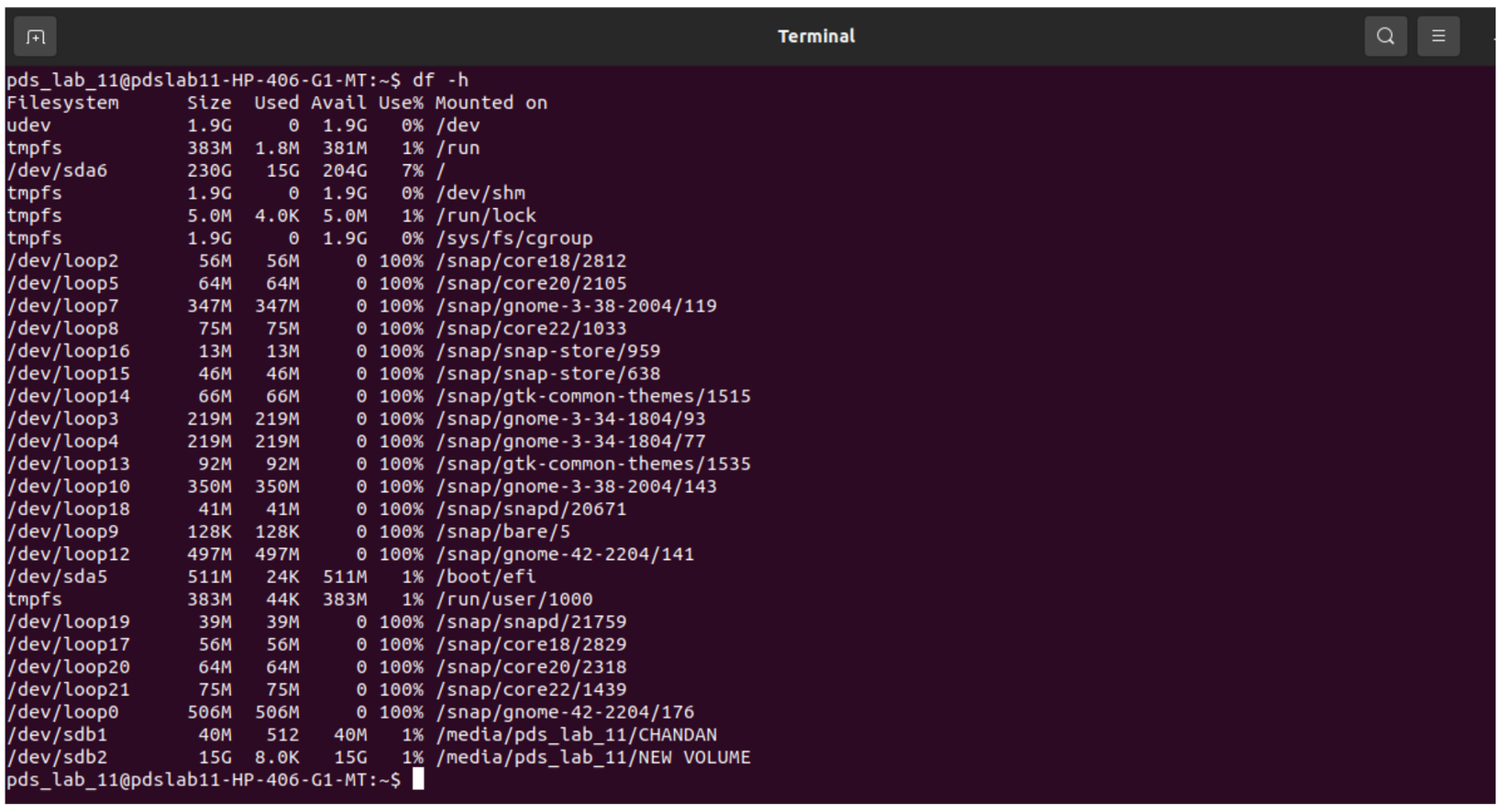
Now, with the setup completed, we can proceed to use the commands mentioned above.

Command:

```
df -h
```

Usage:

This “***df***” command in Unix-like OS, is used to display information about the file system, including the amount of available and used space on mounted file systems.
The "***-h***" option stands for "human-readable" format, which displays the sizes in a more easily understandable format (e.g., kilobytes, megabytes, gigabytes) rather than raw bytes.



Command:

```
sudo dd if=/dev/sdb1 of=/home/pds_lab_11/Desktop/SFLAB/pd.img
```

Usage:

The command using "***dd***", which is a powerful utility for low-level copying and conversion of data.

This command will create a bit-by-bit copy of the partition /dev/sdb1 and save it as an image file named ***pd.img*** on the user's desktop. This is often used for backup purposes or to create disk images for virtualization or recovery.

```
/dev/sdb1        40M   512   40M   1% /media/pds_lab_11/CHANDAN
/dev/sdb2        15G  8.0K   15G   1% /media/pds_lab_11/NEW VOLUME
pds_lab_11@pdslab11-HP-406-G1-MT:~$ sudo dd if=/dev/sdb1 of=/home/pds_lab_11/Desktop/SFLAB/pd.img
81920+0 records in
81920+0 records out
41943040 bytes (42 MB, 40 MiB) copied, 1.29152 s, 32.5 MB/s
pds_lab_11@pdslab11-HP-406-G1-MT:~$
```

Command:

```
fsstat pd.img
```

Usage:

The command "***fsstat pd.img***" is part of sleuthkit collection, which is specifically designed to display file system statistics.
This would provide a detailed report on the file system contained within the pd.img file, allowing for further analysis or recovery efforts.

```
pds_lab_11@pdslab11-HP-406-G1-MT:~/Desktop/SFLAB$ fsstat pd.img
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT32

OEM Name: mkfs.fat
Volume ID: 0xd212251
Volume Label (Boot Sector): CHANDAN
Volume Label (Root Directory): CHANDAN
File System Type Label: FAT32
Next Free Sector (FS Info): 1293
Free Sector Count (FS Info): 80627

Sectors before file system: 2048

File System Layout (in sectors)
Total Range: 0 - 81919
* Reserved: 0 - 31
** Boot Sector: 0
** FS Info Sector: 1
** Backup Boot Sector: 6
* FAT 0: 32 - 661
* FAT 1: 662 - 1291
* Data Area: 1292 - 81919
** Cluster Area: 1292 - 81919
*** Root Directory: 1292 - 1292

METADATA INFORMATION
--------------------------------------------
Range: 2 - 1290054
Root Directory: 2

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 512
Total Cluster Range: 2 - 80629
```

Command:

```
fls pd.img
```

Usage:

The "***fls pd.img***" command is used to list the files and directories present in a disk image file.
"fls" stands for "Forensic LS" and is a tool from the SleuthKit suite of digital forensics utilities. It is used to list the files and directories present in a disk image or a file system. The "fls" command can be used to analyze various file system types, including FAT, NTFS, ext2/ext3, and more.

```
pds_lab_11@pdslab11-HP-406-G1-MT:~/Desktop/SFLAB$ fls pd.img
r/r 3:  CHANDAN     (Volume Label Entry)
r/r * 5:        24CS06022.txt
v/v 1290051:    $MBR
v/v 1290052:    $FAT1
v/v 1290053:    $FAT2
V/V 1290054:    $OrphanFiles
pds_lab_11@pdslab11-HP-406-G1-MT:~/Desktop/SFLAB$
```

Previously, I created a file named "24CS06022.txt" and then permanently removed it. Surprisingly, when using the "fls pd.img" command, I discovered that deleted files are still accessible. The image above displays the file with a number 5 associated with it, signifying the directory entry.

Command:

```
istat pd.img 5
```

Usage:

The "istat" command belongs to the Sleuthkit collection, utilized in digital forensics and incident response to provide details about an image file or partition within a forensic image file. Specifically, in this instance, the command reveals information about the file linked to inode number 5, identified as "24CS06022.txt".

```
pds_lab_11@pdslab11-HP-406-G1-MT:~/Desktop/SFLAB$ istat pd.img 5
Directory Entry: 5
Not Allocated
File Attributes: File, Archive
Size: 15
Name: _4CS06~1.TXT

Directory Entry Times:
Written:        2024-08-09 04:57:14 (IST)
Accessed:       2024-08-09 00:00:00 (IST)
Created:        2024-08-09 04:57:14 (IST)

Sectors:
1293
pds_lab_11@pdslab11-HP-406-G1-MT:~/Desktop/SFLAB$
```

Command:

```
ils pd.img 5
```

Usage:

The command's output will display the files and subdirectories within the designated directory of the image file. This functionality proves beneficial for examining the layout and components of disk images or similar file types that retain directory details.

```
1293
pds_lab_11@pdslab11-HP-406-G1-MT:~/Desktop/SFLAB$ ils pd.img 5
class|host|device|start_time
ils|pdslab11-HP-406-G1-MT||1723179899
st_ino|st_alloc|st_uid|st_gid|st_mtime|st_atime|st_ctime|st_crtime|st_mode|st_nlink|st_size
5|f|0|0|1723159634|1723141800|0|1723159634|777|0|15
pds_lab_11@pdslab11-HP-406-G1-MT:~/Desktop/SFLAB$
```

Command:

```
blkstat pd.img 5
```

Usage:

the command blkstat pd.img 5 is used to query the status or details of block number 5 in the disk image file named pd.img.

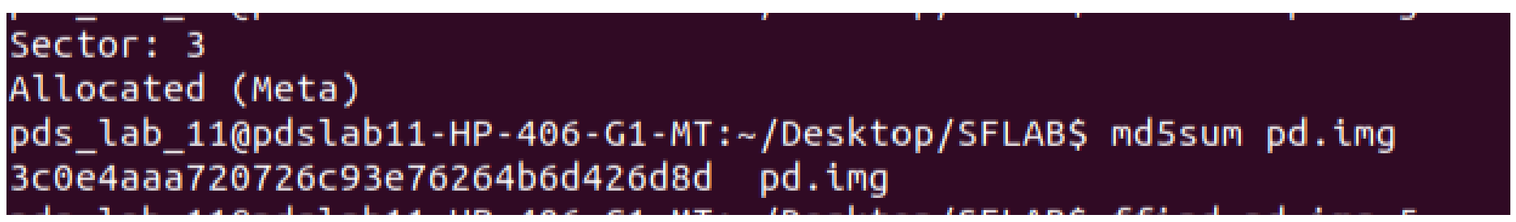
```
5|f|0|0|1723159634|1723141800|0|1723159634|777|0|15
pds_lab_11@pdslab11-HP-406-G1-MT:~/Desktop/SFLAB$ blkstat pd.img 3
Sector: 3
Allocated (Meta)
pds_lab_11@pdslab11-HP-406-G1-MT:~/Desktop/SFLAB$
```

Command:

```
md5sum pd.img
```

Usage:

When we run the command md5sum pd.img, the system will read the contents of pd.img, compute its MD5 hash, and then output the hash value to the terminal. This can be useful for verifying that the file has not been altered or corrupted during transfer or storage.



Command:

```
ffind pd.img 5
```

Usage:

When we run the command ffind pd.img 5, the utility will search through the pd.img disk image for the directory entry numbered 5. The output will typically provide information about the file or directory associated with that entry, such as its name, size, and attributes.