

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

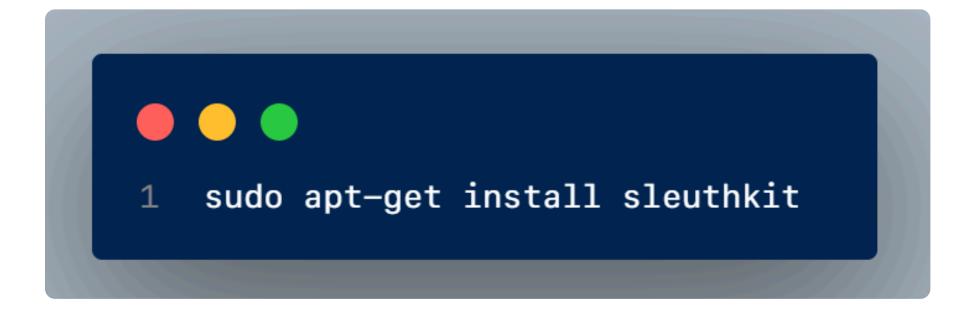
Goal of Assignment:

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:

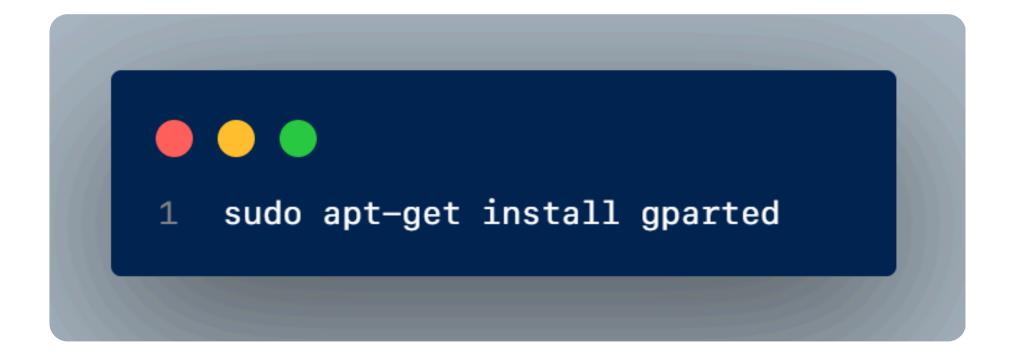


Usage:

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:

```
Terminal
pds_lab_11@pdslab11-HP-406-G1-MT:~$ sudo apt-get install sleuthkit
[sudo] password for pds_lab_11:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
 gir1.2-goa-1.0 libfwupdplugin1 libxmlb1
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
 libafflib0v5 libdate-manip-perl libewf2 libtsk13
Suggested packages:
 autopsy mac-robber
The following NEW packages will be installed:
 libafflib0v5 libdate-manip-perl libewf2 libtsk13 sleuthkit
O upgraded, 5 newly installed, O to remove and 74 not upgraded.
Need to get 2,217 kB of archives.
After this operation, 17.3 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 libafflib0v5 amd64 3.7.18-3 [204 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libdate-manip-perl all 6.79-1 [908 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 libewf2 amd64 20140807-2build1 [513 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 libtsk13 amd64 4.6.7-1build1 [340 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 sleuthkit amd64 4.6.7-1build1 [252 kB]
Fetched 2,217 kB in 2s (972 kB/s)
Selecting previously unselected package libafflib0v5.
(Reading database ... 186133 files and directories currently installed.)
Preparing to unpack .../libafflib0v5_3.7.18-3_amd64.deb ...
Unpacking libafflib0v5 (3.7.18-3) ...
Selecting previously unselected package libdate-manip-perl.
Preparing to unpack .../libdate-manip-perl_6.79-1_all.deb ...
Unpacking libdate-manip-perl (6.79-1) ...
Selecting previously unselected package libewf2.
Preparing to unpack .../libewf2_20140807-2build1_amd64.deb ...
Unpacking libewf2 (20140807-2build1) ...
Selecting previously unselected package libtsk13.
Preparing to unpack .../libtsk13_4.6.7-1build1_amd64.deb ...
Unpacking libtsk13 (4.6.7-1build1) ...
Selecting previously unselected package sleuthkit.
```



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.

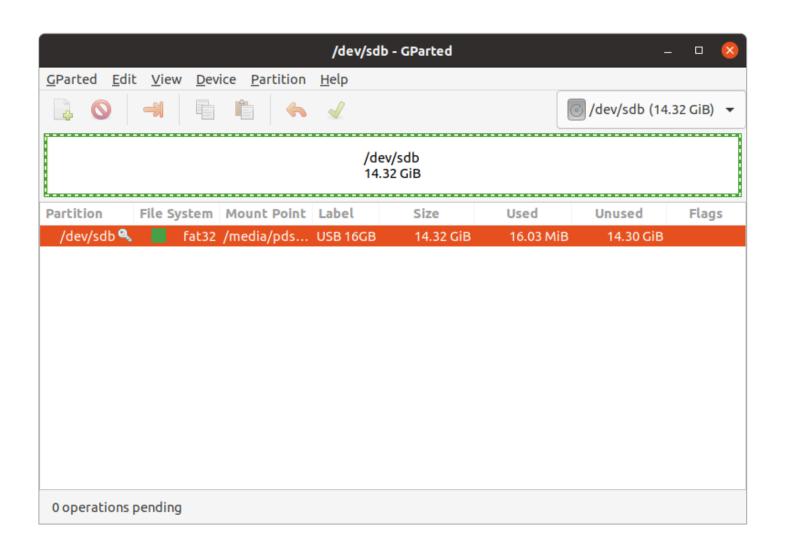
This command is essential for users who need to manage their disk partitions effectively, whether for system maintenance, installation of new operating systems, or optimizing storage usage.

Command:

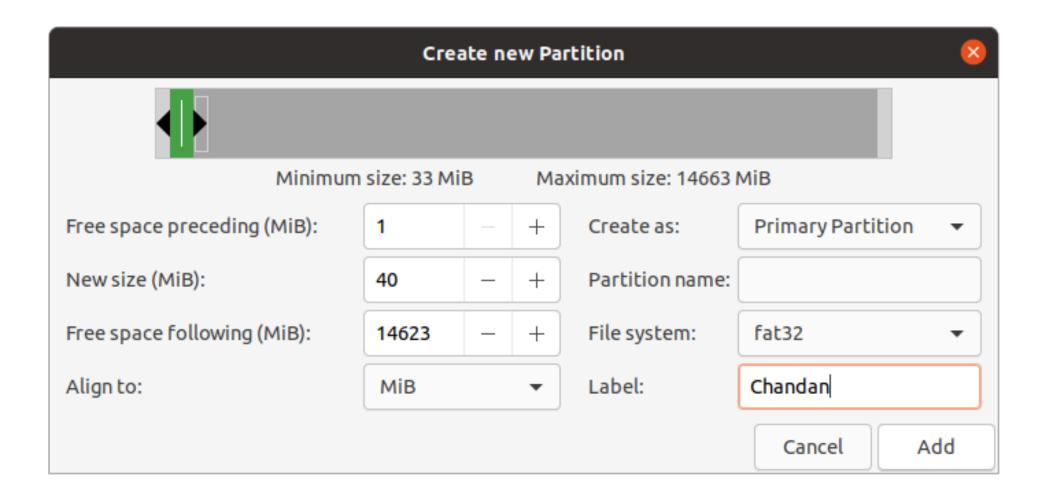


This command prompt enables us to open a window for disk partitioning. In this task, we are required to split the disk into two sections: one with 40MB and the other utilizing the remaining space.

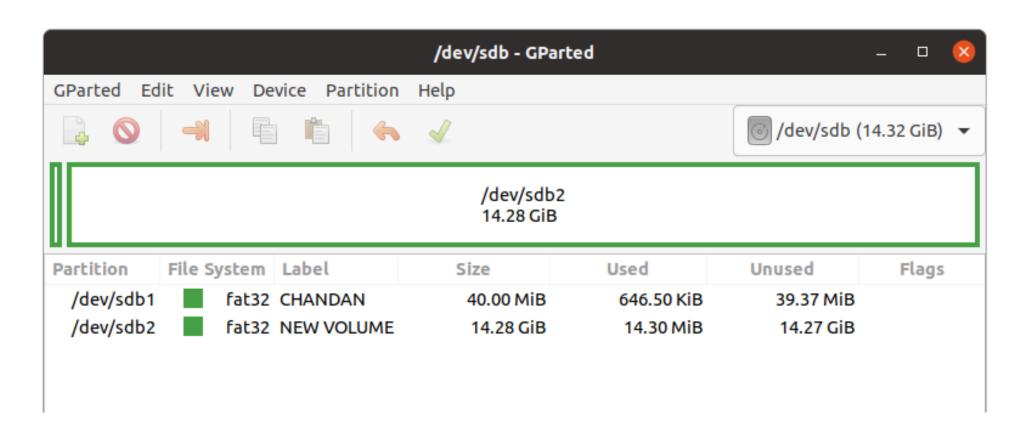
A window will pop up, allowing us to choose our preferred disk from the "GParted" menu in the top left corner. This menu displays the following details.



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.

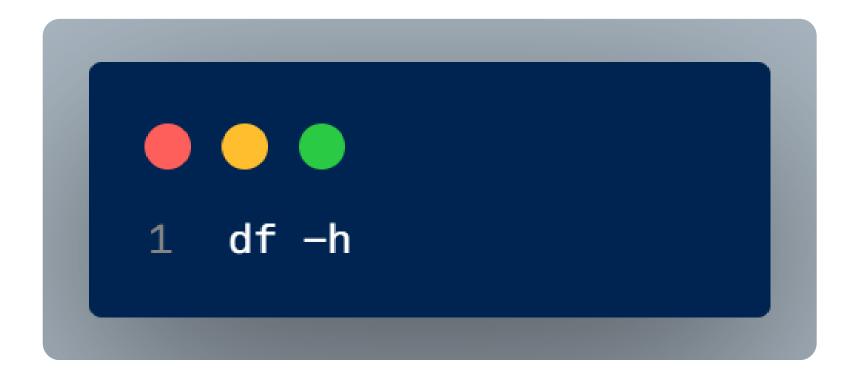


At last, we can observe that our disk has been divided into two sections.



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

Command:



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.

```
Q =
                                                                  Terminal
pds_lab_11@pdslab11-HP-406-G1-MT:~$ df -h
Filesystem
               Size Used Avail Use% Mounted on
                       0 1.9G 0% /dev
               1.9G
udev
               383M 1.8M 381M
tmpfs
                                 1% /run
                     15G 204G
/dev/sda6
               230G
                      0 1.9G 0% /dev/shm
tmpfs
               1.9G
               5.0M 4.0K 5.0M 1% /run/lock
tmpfs
                     0 1.9G 0%/sys/fs/cgroup
               1.9G
tmpfs
/dev/loop2
                56M
                    56M
                             0 100% /snap/core18/2812
                             0 100% /snap/core20/2105
/dev/loop5
                64M
                     64M
/dev/loop7
               347M 347M
                             0 100% /snap/gnome-3-38-2004/119
/dev/loop8
                    75M
                75M
                             0 100% /snap/core22/1033
/dev/loop16
                13M
                     13M
                             0 100% /snap/snap-store/959
/dev/loop15
                46M
                             0 100% /snap/snap-store/638
                     46M
/dev/loop14
                66M
                    66M
                             0 100% /snap/gtk-common-themes/1515
/dev/loop3
               219M 219M
                             0 100% /snap/gnome-3-34-1804/93
/dev/loop4
               219M 219M
                             0 100% /snap/gnome-3-34-1804/77
/dev/loop13
               92M 92M
                             0 100% /snap/gtk-common-themes/1535
                             0 100% /snap/gnome-3-38-2004/143
/dev/loop10
               350M 350M
/dev/loop18
               41M
                     41M
                             0 100% /snap/snapd/20671
/dev/loop9
               128K
                    128K
                             0 100% /snap/bare/5
/dev/loop12
               497M
                    497M
                             0 100% /snap/gnome-42-2204/141
/dev/sda5
                     24K 511M 1% /boot/efi
               511M
tmpfs
                     44K 383M 1% /run/user/1000
               383M
/dev/loop19
                39M
                     39M
                             0 100% /snap/snapd/21759
/dev/loop17
                56M
                    56M
                             0 100% /snap/core18/2829
/dev/loop20
                64M
                    64M
                             0 100% /snap/core20/2318
/dev/loop21
                75M
                     75M
                             0 100% /snap/core22/1439
/dev/loop0
/dev/sdb1
               506M 506M
                             0 100% /snap/gnome-42-2204/176
                     512
                                1% /media/pds_lab_11/CHANDAN
                40M
                            40M
/dev/sdb2
                15G 8.0K
                           15G 1½ /media/pds_lab_11/NEW VOLUME
pds_lab_11@pdslab11-HP-406-G1-MT:~$
```

```
1 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:



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.

```
Terminal
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
```



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.

```
[<del>+</del>]
                                                                         Term
pds_lab_11@pdslab11-HP-406-G1-MT:~/Desktop/SFLAB$ fls pd.img
                     (Volume Label Entry)
r/r 3: CHANDAN
                 24CS06022.txt
г/г * 5:
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:



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$
```

```
1 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.

```
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$
```

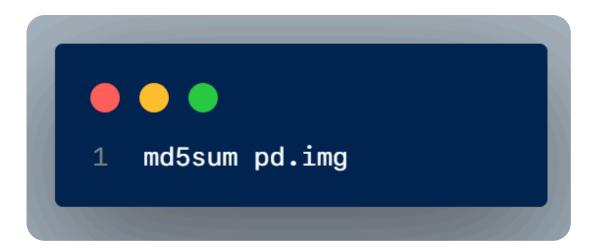
Command:



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$
```

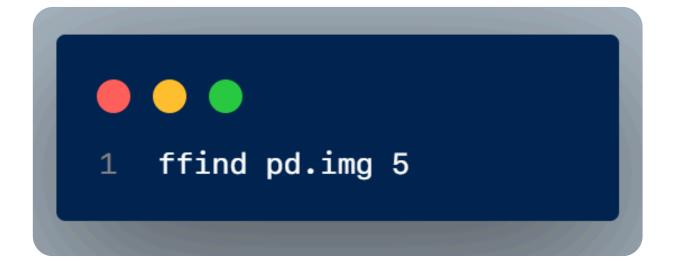


Usage:

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.

```
Sector: 3
Allocated (Meta)
pds_lab_11@pdslab11-HP-406-G1-MT:~/Desktop/SFLAB$ md5sum pd.img
3c0e4aaa720726c93e76264b6d426d8d pd.img
```

Command:



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.

```
library@library-Veriton-M4690G-D22W5:~/Desktop/SFLAB$ ffind pd.img 5

* /Document.txt
library@library-Veriton-M4690G-D22W5:~/Desktop/SFLAB$
```