



TILAK
MAHARASHTRA
VIDYAPEETH

October - 2025

Assignment No - 01

FORENSIC ACQUISITION AND INTEGRITY VERIFICATION OF SUSPECT'S COMPUTER

Prepared by

Mr Arhant Suhas Gaikwad

Approved by

Dr. Anup Girdhar

(prof. Comp Science
Department)

Practical Work

command

1. sudo fdisk -l

Purpose : It lists all storage devices (disks and partitions) connected to your system.

Output :

```
(arhant@kali)-[~]
$ sudo fdisk -l
Disk /dev/sda: 1.01 GiB, 1085349888 bytes, 2119824 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/sdb: 37.97 GiB, 40770109440 bytes, 79629120 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x426fb435

Device      Boot    Start        End    Sectors    Size Id Type
/dev/sdb1   *          2048    75468799    75466752    36G 83 Linux
/dev/sdb2             75470846    79628287    4157442     2G  f W95 Ext'd (LBA)
/dev/sdb5             75470848    79628287    4157440     2G 82 Linux swap / Solaris
```

2. sudo umount /dev/sdb

Purpose: To safely unmount the suspect's drive before creating a forensic image.

Output :

```
(arhant@kali)-[~]  
$ sudo umount /dev/sdb  
umount: /dev/sdb: not mounted.
```

3.sudo mkdir -p /home/arhant/forensics

Purpose :To create a dedicated directory where the forensic image and related evidence files (like hash logs, reports, etc.) will be securely stored.

Output :

```
(arhant@kali)-[~]  
$ sudo mkdir -p /home/arhant/forensics  
[sudo] password for arhant:
```

4.sudo dd if=/dev/sdb of=/home/arhant/forensics/suspect_forensics.dd

Purpose : To create a bit-by-bit forensic image of the suspect's storage device while ensuring data integrity and preserving digital evidence.

Output :

```
(arhant@kali)-[~]  
$ sudo dd if=/dev/sdb of=/home/arhant/forensics/suspect_forensics.dd  
2119824+0 records in  
2119824+0 records out  
1085349888 bytes (1.1 GB, 1.0 GiB) copied, 16.4996 s, 65.8 MB/s
```

5. md5sum /dev/sdb

Purpose : To generate a unique MD5 hash value (digital fingerprint) of the suspect's disk before or after imaging — ensuring data integrity throughout the forensic process.

Output:

```
(arhant@kali)-[~]  
$ sudo md5sum /dev/sdb  
2f44c453868b026f47445a4659308c46 /dev/sdb
```

6. md5sum /home/arhant/forensics/suspect_forensics.dd

Purpose : To generate a unique MD5 hash value (digital fingerprint) of the suspect's disk before or after imaging — ensuring data integrity throughout the forensic process.

Output:

```
(arhant@kali)-[~]  
$ sudo md5sum /home/arhant/forensics/suspect_forensics.dd  
2f44c453868b026f47445a4659308c46 /home/arhant/forensics/suspect_forensics.dd
```

6.sudo sha256sum /dev/sdb

Purpose : To generate a SHA-256 hash (a cryptographic fingerprint) of the suspect's disk (/dev/sdb) to verify data integrity before and/or after imaging.

Output :

```
(arhant@kali)-[~]  
$ sudo sha256sum /dev/sdb  
020c7e7264c632995d7195eb5fa9ef60a5e4d4cd385aa4808fedc45bba95cfcf /dev/sdb
```

7. sudo sha256 /home/arhant/forensics/suspect_forensics.dd

Purpose: To generate a SHA-256 hash of the forensic image file to ensure it matches the original suspect disk (/dev/sdb) and that no data has been altered during acquisition.

Output:

```
(arhant@kali)-[~]  
$ sudo sha256sum /home/arhant/forensics/suspect_forensics.dd  
020c7e7264c632995d7195eb5fa9ef60a5e4d4cd385aa4808fedc45bba95cfcf
```