TILAK
MAHARASHTRA
VIDYAPEETH

October - 2025

Assigment 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)

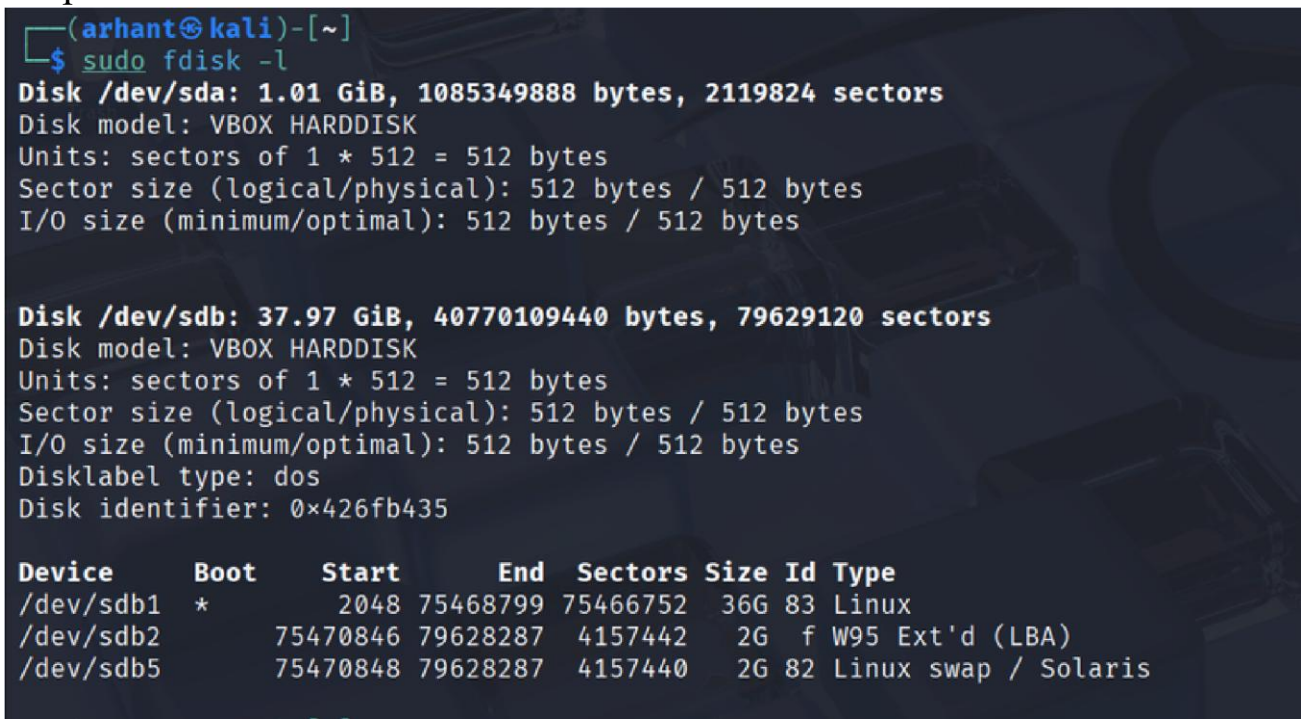
Practical Work

command

1. sudo fdisk -l

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

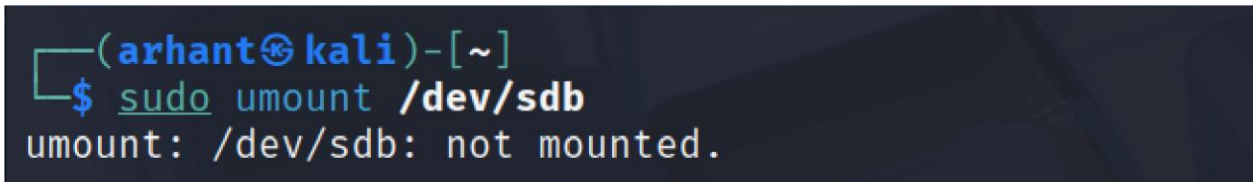
Output :



2. sudo umount /dev/sdb

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

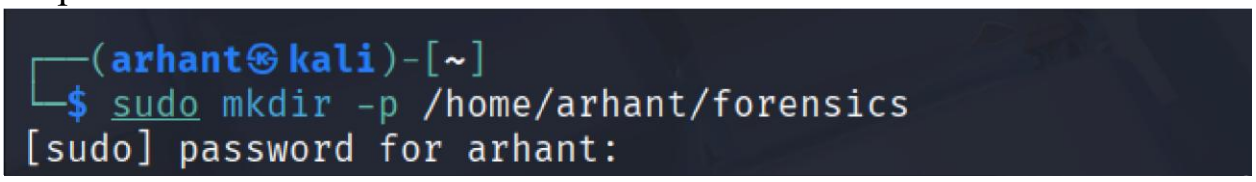
Output :



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 :



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.

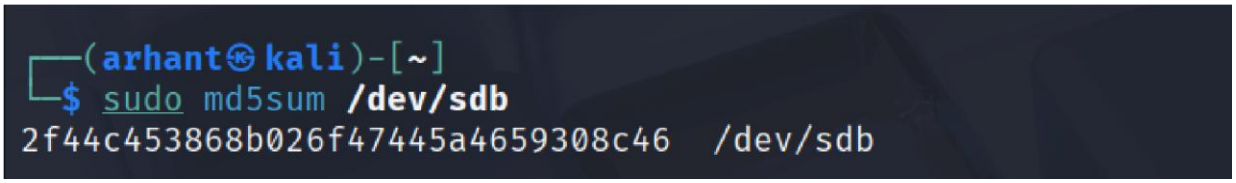
Output :

```
┌──(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.

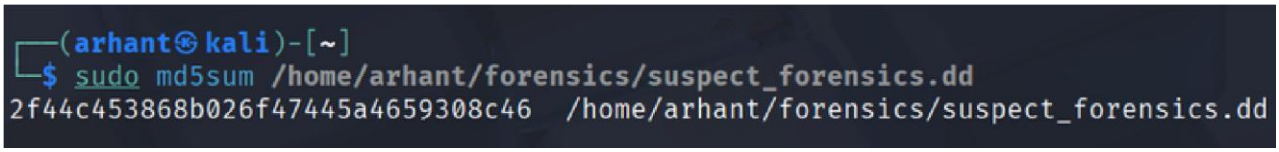
Output:



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:



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 :

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: