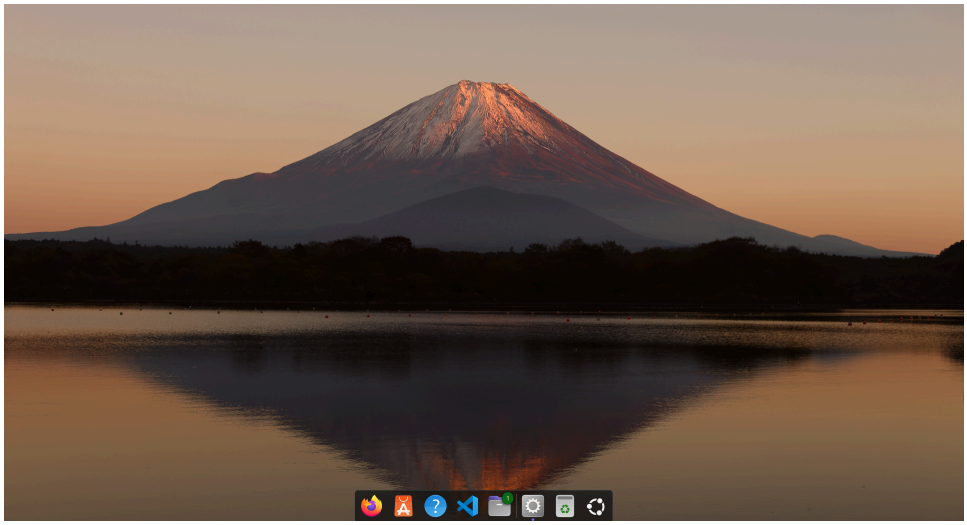
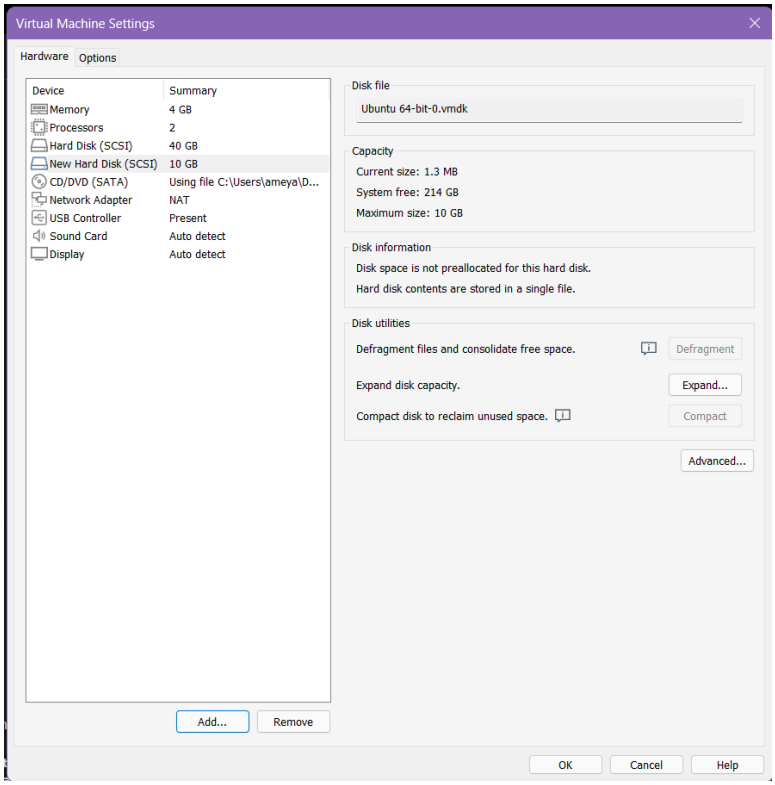
## Step 1: Create a Ubuntu VM / Kali VM



## Step 2: Add a Second Virtual Disk

- Power off the VM.
- Go to VM → Settings → Add → Hard Disk.
- Choose SCSI, 10 GB, and click Finish.
- Power on the VM.



## Step 3: Identify the New Disk

lsblk

Expected Output:

sda (Ubuntu/Kali disk)
sdb (Attached disk for forensic image)

```
student@student-VMware-Virtual-Platform:~$ lsblk
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
loop0    7:0    0     4K  1 loop /snap/bare/5
loop1    7:1    0  73.9M  1 loop /snap/core22/1802
loop2    7:2    0  74.3M  1 loop /snap/core22/1564
loop3    7:3    0 269.8M  1 loop /snap/firefox/4793
loop4    7:4    0  10.7M  1 loop /snap/firmware-updater/127
loop5    7:5    0  11.1M  1 loop /snap/firmware-updater/167
loop6    7:6    0  91.7M  1 loop /snap/gtk-common-themes/1535
loop7    7:7    0   516M  1 loop /snap/gnome-42-2204/202
loop8    7:8    0 505.1M  1 loop /snap/gnome-42-2204/176
loop9    7:9    0  10.5M  1 loop /snap/snap-store/1173
loop10   7:10   0  38.8M  1 loop /snap/snapd/21759
loop11   7:11   0   568K  1 loop /snap/snapd-desktop-integration/253
loop12   7:12   0   500K  1 loop /snap/snapd-desktop-integration/178
sda      8:0    0    40G  0 disk
├─sda1   8:1    0     1M  0 part
└─sda2   8:2    0    40G  0 part /
sdb      8:16   0    10G  0 disk
sr0     11:0    1  1024M  0 rom
student@student-VMware-Virtual-Platform:~$
```

## Step 4: Format and Populate the Secondary Disk

sudo mkfs.ext4 /dev/sdb
sudo mkdir /mnt/evidence
sudo mount /dev/sdb /mnt/evidence
echo "This is confidential evidence." | sudo tee /mnt/evidence/evidence.txt
sudo umount /mnt/evidence

```
student@student-VMware-Virtual-Platform:~$ sudo mkfs.ext4 /dev/sdb
[sudo] password for student:
mke2fs 1.47.0 (5-Feb-2023)
Creating filesystem with 2621440 4k blocks and 655360 inodes
Filesystem UUID: e57f9b5d-c35d-48f7-9aa9-2f4567b04924
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done

student@student-VMware-Virtual-Platform:~$ sudo mkdir /mnt/evidence
sudo mount /dev/sdb /mnt/evidence
student@student-VMware-Virtual-Platform:~$ echo "This is confidential evidence." | sudo tee /mnt/evidence/evidence.txt
This is confidential evidence.
student@student-VMware-Virtual-Platform:~$ sudo umount /mnt/evidence
student@student-VMware-Virtual-Platform:~$
```

**Step 5: Create Forensic Image Using dd**

sudo dd if=/dev/sdb of=forensic_image.img bs=4M status=progress

```
student@student-VMware-Virtual-Platform:~$ sudo dd if=/dev/sdb of=forensic_image.img bs=4M status=progress
10657726464 bytes (11 GB, 9.9 GiB) copied, 16 s, 666 MB/s
2560+0 records in
2560+0 records out
10737418240 bytes (11 GB, 10 GiB) copied, 16.3534 s, 657 MB/s
student@student-VMware-Virtual-Platform:~$
```

**Step 6: Check Image Format**

file forensic_image.img

```
student@student-VMware-Virtual-Platform:~$ file forensic_image.img
forensic_image.img: Linux rev 1.0 ext4 filesystem data, UUID=e57f9b5d-c35d-48f7-9aa9-2f4567b04924 (extents) (64bit) (large files) (huge files)
student@student-VMware-Virtual-Platform:~$
```

**Step 7: Verify Integrity with Hashing**

md5sum forensic_image.img
sha256sum forensic_image.img

```
student@student-VMware-Virtual-Platform:~$ md5sum forensic_image.img
sha256sum forensic_image.img
3f6d5c0c7606374df380e0d800a2b77a  forensic_image.img
630f9cd200308c64f02b6fa3dd6bacb0972eae145a7e968edffe8180713b8943  forensic_image.img
student@student-VMware-Virtual-Platform:~$
```

**Step 8: Mount the Forensic Image (Read-Only)**

sudo mkdir /mnt/forensic
sudo mount -o loop,ro forensic_image.img /mnt/forensic
ls /mnt/forensic

```
student@student-VMware-Virtual-Platform:~$ sudo mkdir /mnt/forensic
student@student-VMware-Virtual-Platform:~$ sudo mount -o loop,ro forensic_image.img /mnt/forensic
student@student-VMware-Virtual-Platform:~$ ls /mnt/forensic
evidence.txt  lost+found
student@student-VMware-Virtual-Platform:~$
```

**Step 9: Use fls for Deleted File Recovery**

fls -f ext4 -r forensic_image.img

```
student@student-VMware-Virtual-Platform:~$ fls -f ext4 -r forensic_image.img
d/d 11: lost+found
r/r 12: evidence.txt
V/V 655361:     $OrphanFiles
student@student-VMware-Virtual-Platform:~$
```

**Step 10: Unmount After Analysis**

sudo umount /mnt/forensic

```
student@student-VMware-Virtual-Platform:~$ sudo umount /mnt/forensic
student@student-VMware-Virtual-Platform:~$
```