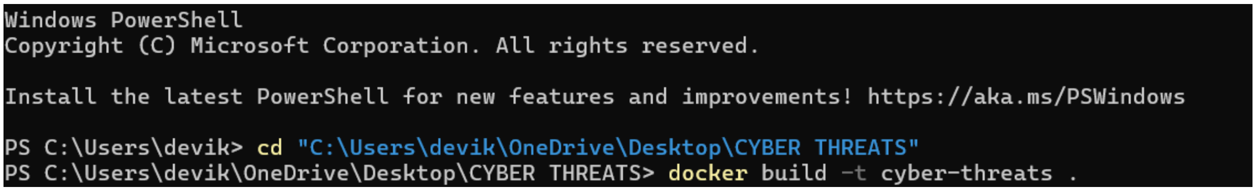
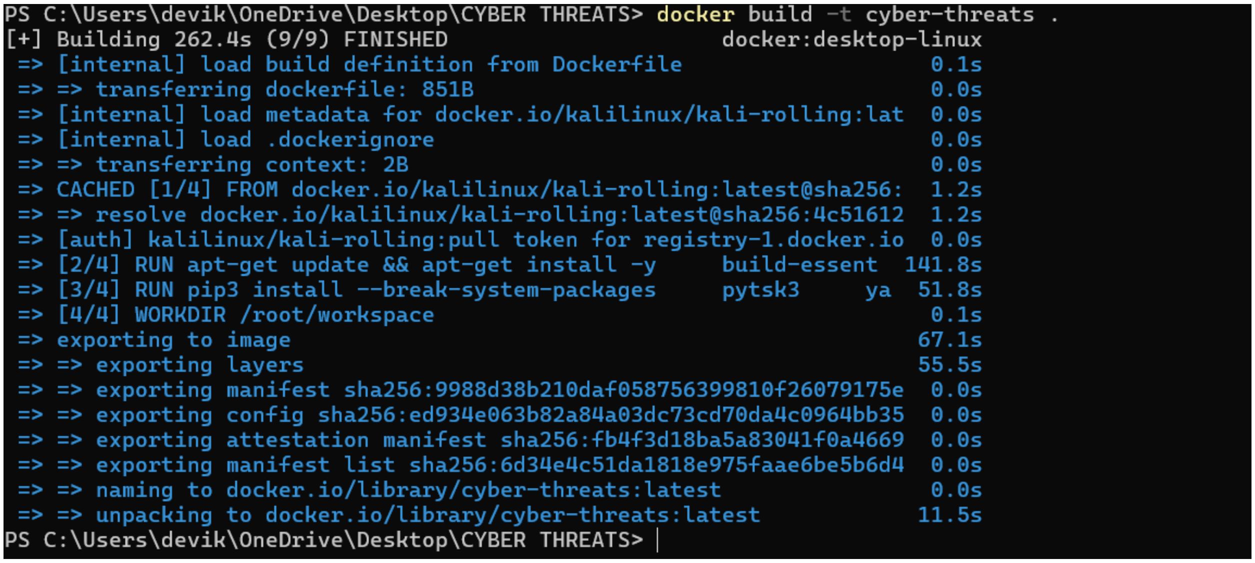
Assignment-1

1. Start Docker Desktop

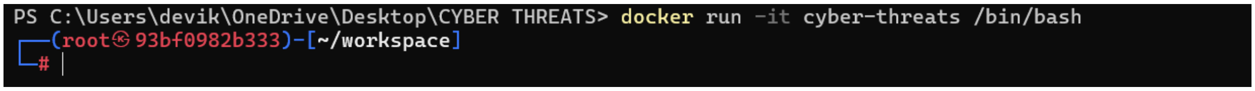


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\devik> cd "C:\Users\devik\OneDrive\Desktop\CYBER THREATS"
PS C:\Users\devik\OneDrive\Desktop\CYBER THREATS> docker build -t cyber-threats .
```

2. Create and Run a Docker Container

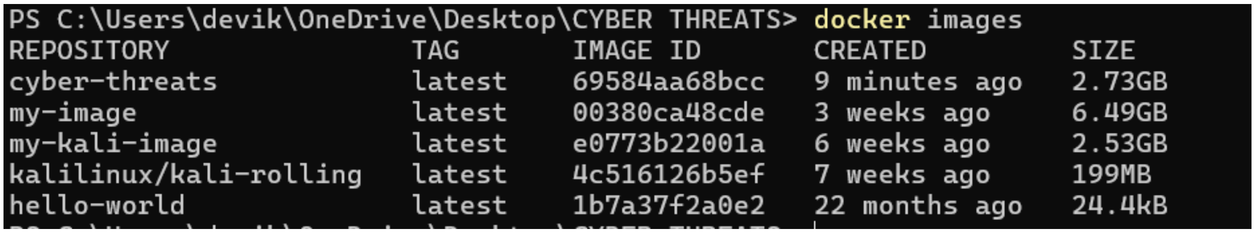


```
PS C:\Users\devik\OneDrive\Desktop\CYBER THREATS> docker build -t cyber-threats .
[+] Building 262.4s (9/9) FINISHED                     docker:desktop-linux
 => [internal] load build definition from Dockerfile                  0.1s
 => => transferring dockerfile: 851B                                  0.0s
 => [internal] load metadata for docker.io/kalilinux/kali-rolling:lat  0.0s
 => [internal] load .dockerignore                                     0.0s
 => => transferring context: 2B                                       0.0s
 => CACHED [1/4] FROM docker.io/kalilinux/kali-rolling:latest@sha256:  1.2s
 => => resolve docker.io/kalilinux/kali-rolling:latest@sha256:4c51612  1.2s
 => [auth] kalilinux/kali-rolling:pull token for registry-1.docker.io  0.0s
 => [2/4] RUN apt-get update && apt-get install -y     build-essent  141.8s
 => [3/4] RUN pip3 install --break-system-packages     pytsk3     ya  51.8s
 => [4/4] WORKDIR /root/workspace                                     0.1s
 => exporting to image                                               67.1s
 => => exporting layers                                              55.5s
 => => exporting manifest sha256:9988d38b210daf058756399810f26079175e  0.0s
 => => exporting config sha256:ed934e063b82a84a03dc73cd70da4c0964bb35  0.0s
 => => exporting attestation manifest sha256:fb4f3d18ba5a83041f0a4669  0.0s
 => => exporting manifest list sha256:6d34e4c51da1818e975faae6be5b6d4  0.0s
 => => naming to docker.io/library/cyber-threats:latest               0.0s
 => => unpacking to docker.io/library/cyber-threats:latest           11.5s
PS C:\Users\devik\OneDrive\Desktop\CYBER THREATS>
```



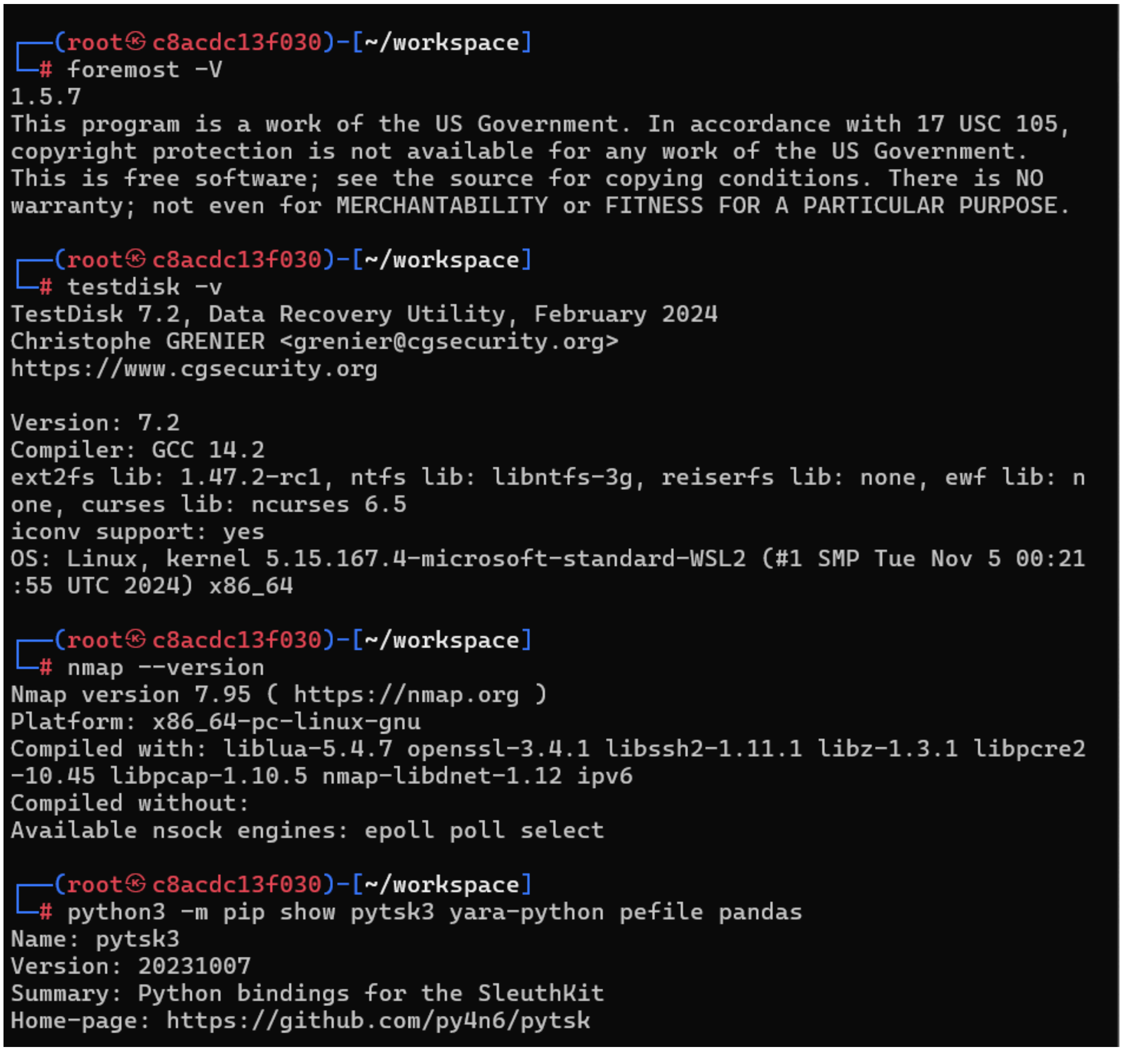
```
PS C:\Users\devik\OneDrive\Desktop\CYBER THREATS> docker run -it cyber-threats /bin/bash
┌──(root㉿93bf0982b333)-[~/workspace]
└─#
```

3.Verify the Built Image

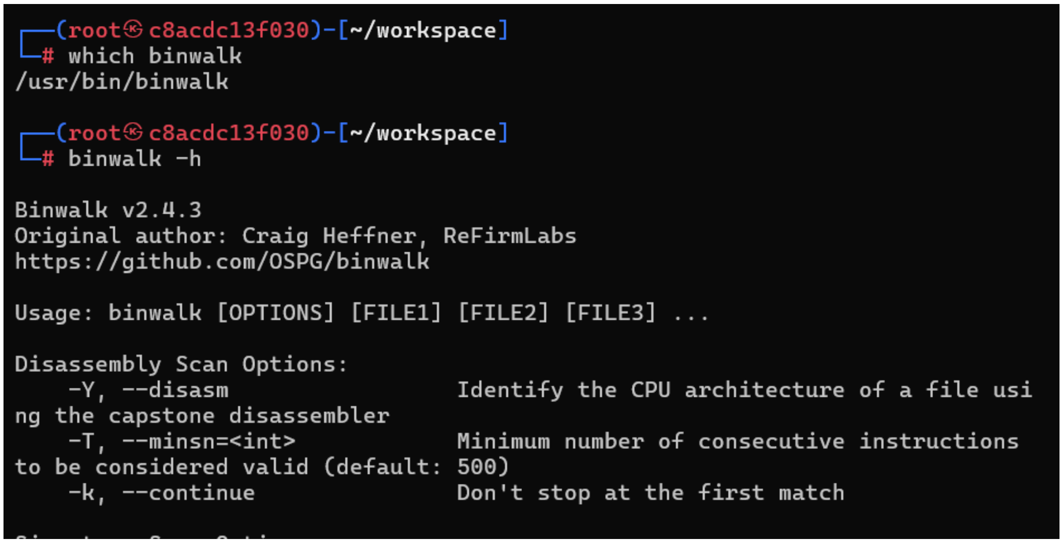


```
PS C:\Users\devik\OneDrive\Desktop\CYBER THREATS> docker images
REPOSITORY                 TAG       IMAGE ID       CREATED          SIZE
cyber-threats              latest    69584aa68bcc   9 minutes ago    2.73GB
my-image                   latest    00380ca48cde   3 weeks ago      6.49GB
my-kali-image              latest    e0773b22001a   6 weeks ago      2.53GB
kalilinux/kali-rolling     latest    4c516126b5ef   7 weeks ago      199MB
hello-world                latest    1b7a37f2a0e2   22 months ago    24.4kB
PS C:\Users\devik\OneDrive\Desktop\CYBER THREATS>
```

4.Verify the Tools in the Container



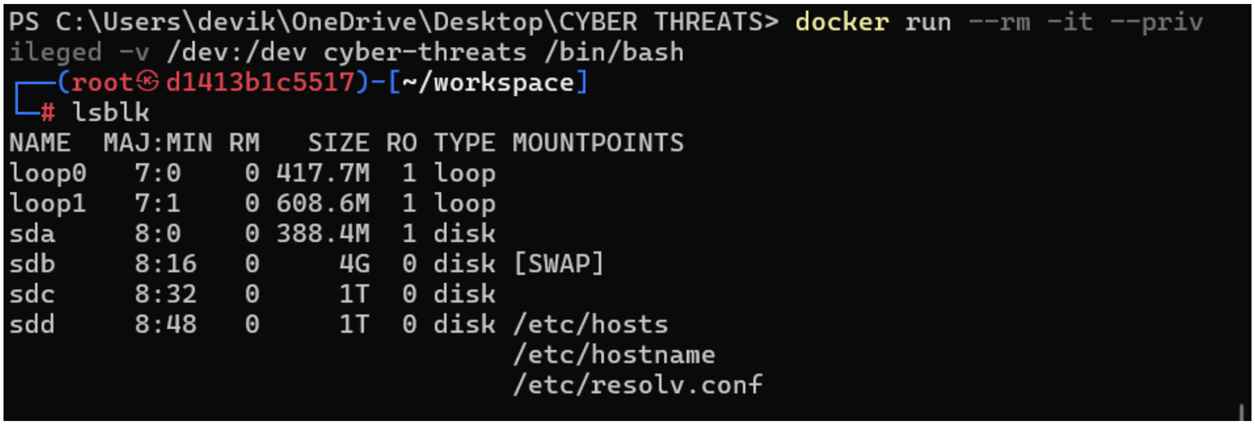
```
┌──(root㉿c8acdc13f030)-[~/workspace]
└─# foremost -V
1.5.7
This program is a work of the US Government. In accordance with 17 USC 105,
copyright protection is not available for any work of the US Government.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

┌──(root㉿c8acdc13f030)-[~/workspace]
└─# testdisk -v
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Version: 7.2
Compiler: GCC 14.2
ext2fs lib: 1.47.2-rc1, ntfs lib: libntfs-3g, reiserfs lib: none, ewf lib: n
one, curses lib: ncurses 6.5
iconv support: yes
OS: Linux, kernel 5.15.167.4-microsoft-standard-WSL2 (#1 SMP Tue Nov 5 00:21
:55 UTC 2024) x86_64

┌──(root㉿c8acdc13f030)-[~/workspace]
└─# nmap --version
Nmap version 7.95 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.7 openssl-3.4.1 libssh2-1.11.1 libz-1.3.1 libpcre2
-10.45 libpcap-1.10.5 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select

┌──(root㉿c8acdc13f030)-[~/workspace]
└─# python3 -m pip show pytsk3 yara-python pefile pandas
Name: pytsk3
Version: 20231007
Summary: Python bindings for the SleuthKit
Home-page: https://github.com/py4n6/pytsk
```



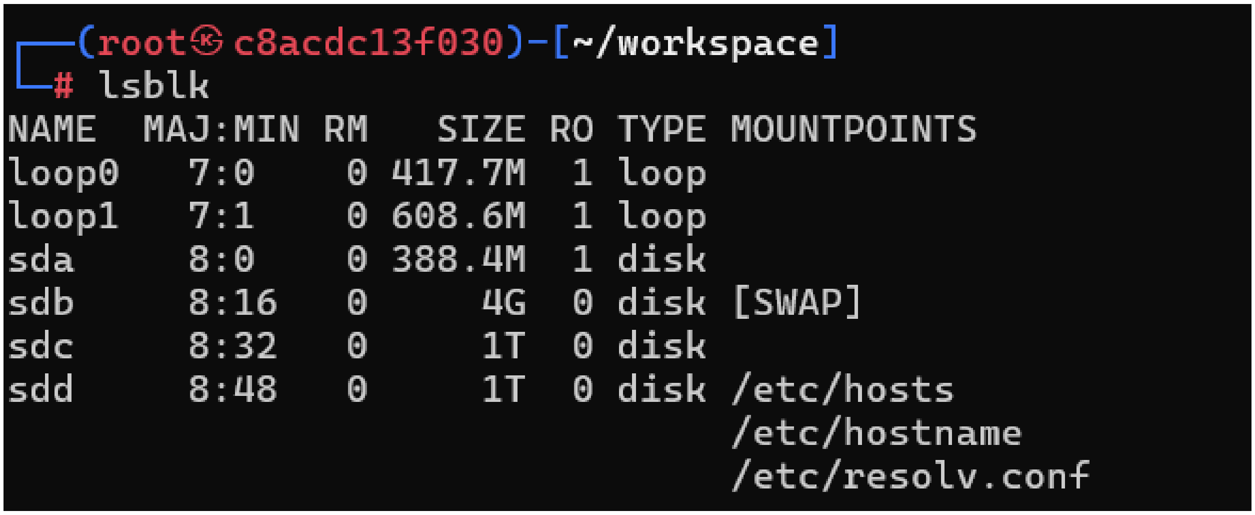
```
┌──(root㉿c8acdc13f030)-[~/workspace]
└─# which binwalk
/usr/bin/binwalk

┌──(root㉿c8acdc13f030)-[~/workspace]
└─# binwalk -h

Binwalk v2.4.3
Original author: Craig Heffner, ReFirmLabs
https://github.com/OSPG/binwalk

Usage: binwalk [OPTIONS] [FILE1] [FILE2] [FILE3] ...

Disassembly Scan Options:
    -Y, --disasm                 Identify the CPU architecture of a file usi
ng the capstone disassembler
    -T, --minsn=<int>            Minimum number of consecutive instructions
to be considered valid (default: 500)
    -k, --continue               Don't stop at the first match
```

5.Copy the Disk Image from Host to the Docker Container

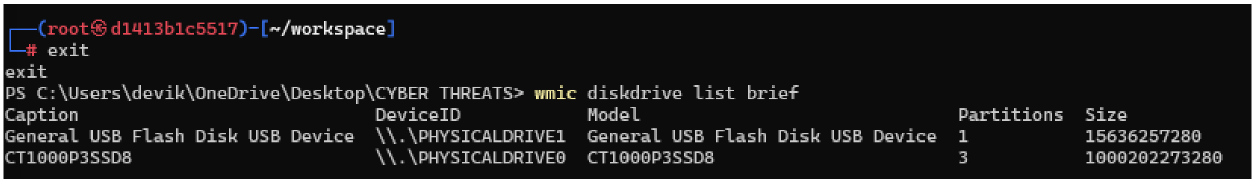
Phase 1: Acquisition (Creating Disk Images)



```
PS C:\Users\devik\OneDrive\Desktop\CYBER THREATS> docker run --rm -it --priv
ileged -v /dev:/dev cyber-threats /bin/bash
┌──(root㉿d1413b1c5517)-[~/workspace]
└─# lsblk
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
loop0    7:0    0 417.7M  1 loop
loop1    7:1    0 608.6M  1 loop
sda      8:0    0 388.4M  1 disk
sdb      8:16   0     4G  0 disk [SWAP]
sdc      8:32   0     1T  0 disk
sdd      8:48   0     1T  0 disk /etc/hosts
                                 /etc/hostname
                                 /etc/resolv.conf
```



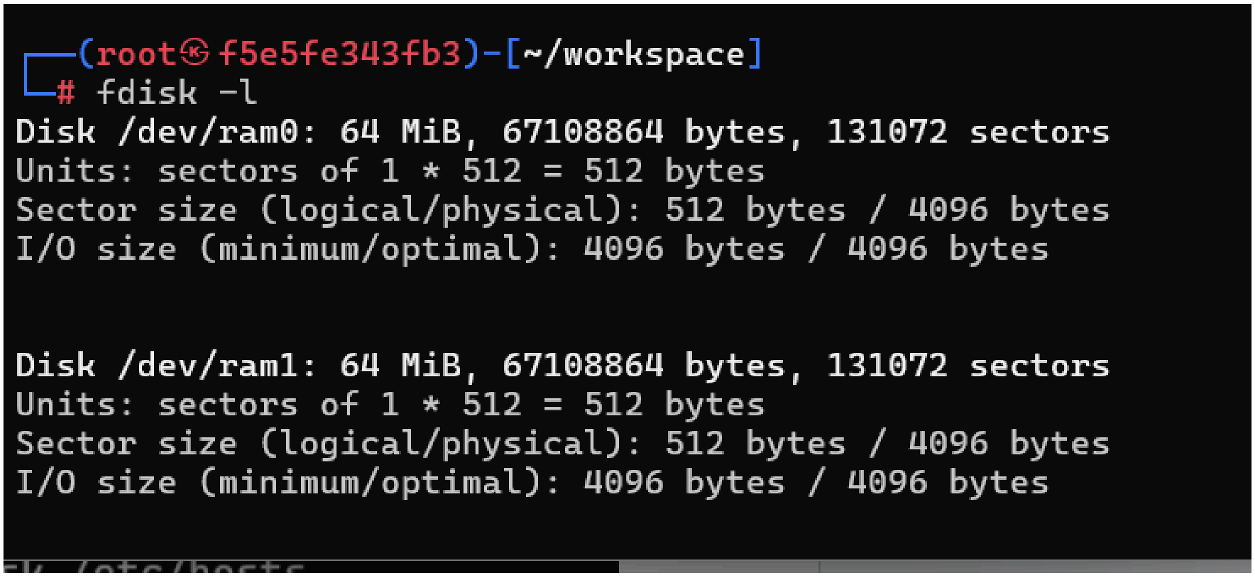
```
┌──(root㉿c8acdc13f030)-[~/workspace]
└─# lsblk
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
loop0    7:0    0 417.7M  1 loop
loop1    7:1    0 608.6M  1 loop
sda      8:0    0 388.4M  1 disk
sdb      8:16   0     4G  0 disk [SWAP]
sdc      8:32   0     1T  0 disk
sdd      8:48   0     1T  0 disk /etc/hosts
                                 /etc/hostname
                                 /etc/resolv.conf
```



```
┌──(root㉿d1413b1c5517)-[~/workspace]
└─# exit
exit
PS C:\Users\devik\OneDrive\Desktop\CYBER THREATS> wmic diskdrive list brief
Caption                            DeviceID            Model                              Partitions  Size
General USB Flash Disk USB Device  \\.\PHYSICALDRIVE1  General USB Flash Disk USB Device  1           15636257280
CT1000P3SSD8                       \\.\PHYSICALDRIVE0  CT1000P3SSD8                       3           1000202273280
```

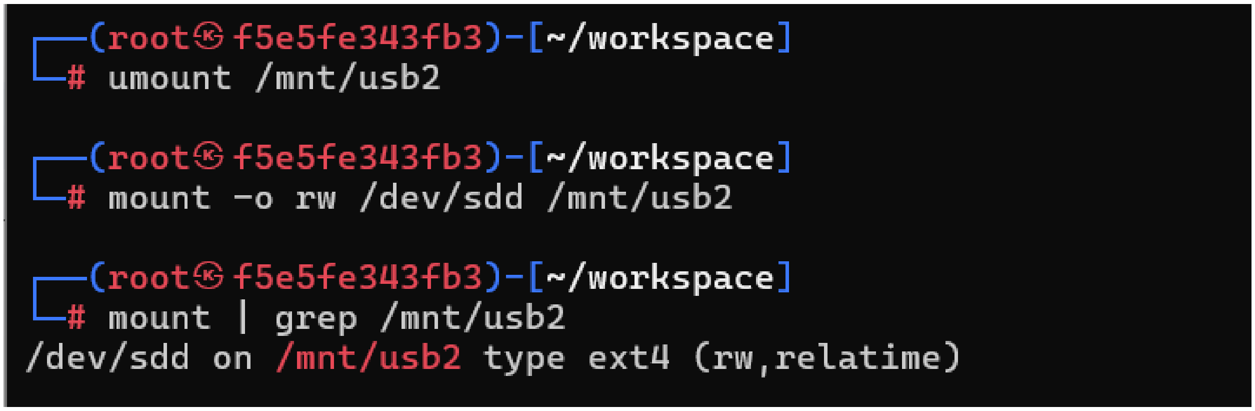
Use `wmic diskdrive list brief` in **Windows PowerShell** to check the device ID of the USB

Identify Partitions



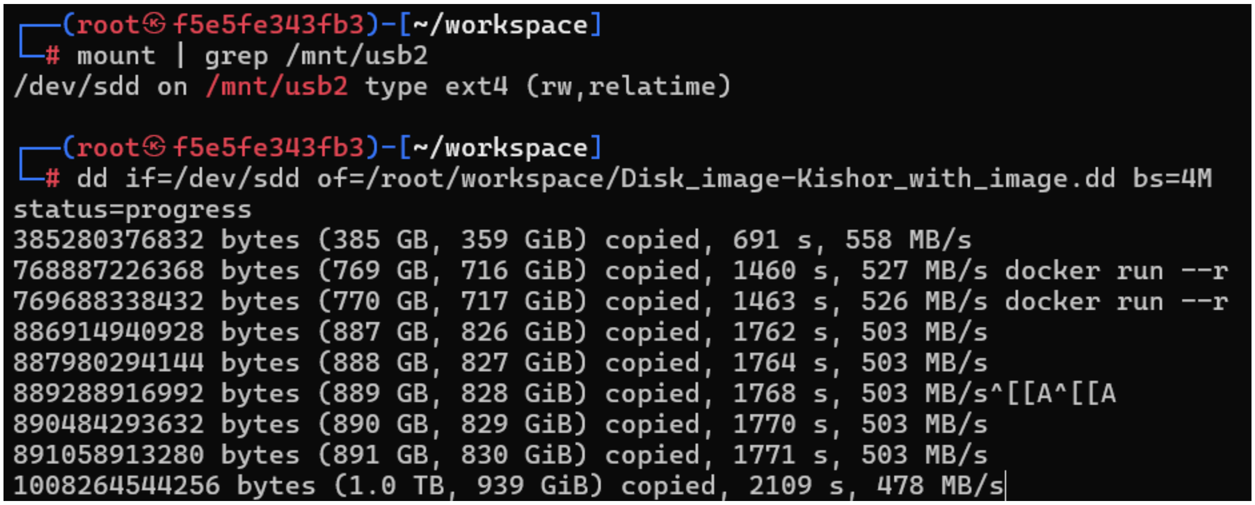
```
┌──(root㉿f5e5fe343fb3)-[~/workspace]
└─# fdisk -l
Disk /dev/ram0: 64 MiB, 67108864 bytes, 131072 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes


Disk /dev/ram1: 64 MiB, 67108864 bytes, 131072 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
```

Mount the USB Drive -Remount it with read/write permissions



```
┌──(root㉿f5e5fe343fb3)-[~/workspace]
└─# umount /mnt/usb2

┌──(root㉿f5e5fe343fb3)-[~/workspace]
└─# mount -o rw /dev/sdd /mnt/usb2

┌──(root㉿f5e5fe343fb3)-[~/workspace]
└─# mount | grep /mnt/usb2
/dev/sdd on /mnt/usb2 type ext4 (rw,relatime)
```

Create Disk Images



```
┌──(root㉿f5e5fe343fb3)-[~/workspace]
└─# mount | grep /mnt/usb2
/dev/sdd on /mnt/usb2 type ext4 (rw,relatime)

┌──(root㉿f5e5fe343fb3)-[~/workspace]
└─# dd if=/dev/sdd of=/root/workspace/Disk_image-Kishor_with_image.dd bs=4M
status=progress
385280376832 bytes (385 GB, 359 GiB) copied, 691 s, 558 MB/s
768887226368 bytes (769 GB, 716 GiB) copied, 1460 s, 527 MB/s docker run --r
769688338432 bytes (770 GB, 717 GiB) copied, 1463 s, 526 MB/s docker run --r
886914940928 bytes (887 GB, 826 GiB) copied, 1762 s, 503 MB/s
887980294144 bytes (888 GB, 827 GiB) copied, 1764 s, 503 MB/s
889288916992 bytes (889 GB, 828 GiB) copied, 1768 s, 503 MB/s^[[A^[[A
890484293632 bytes (890 GB, 829 GiB) copied, 1770 s, 503 MB/s
891058913280 bytes (891 GB, 830 GiB) copied, 1771 s, 503 MB/s
1008264544256 bytes (1.0 TB, 939 GiB) copied, 2109 s, 478 MB/s
```