Họ và tên: Trần Trí Dũng

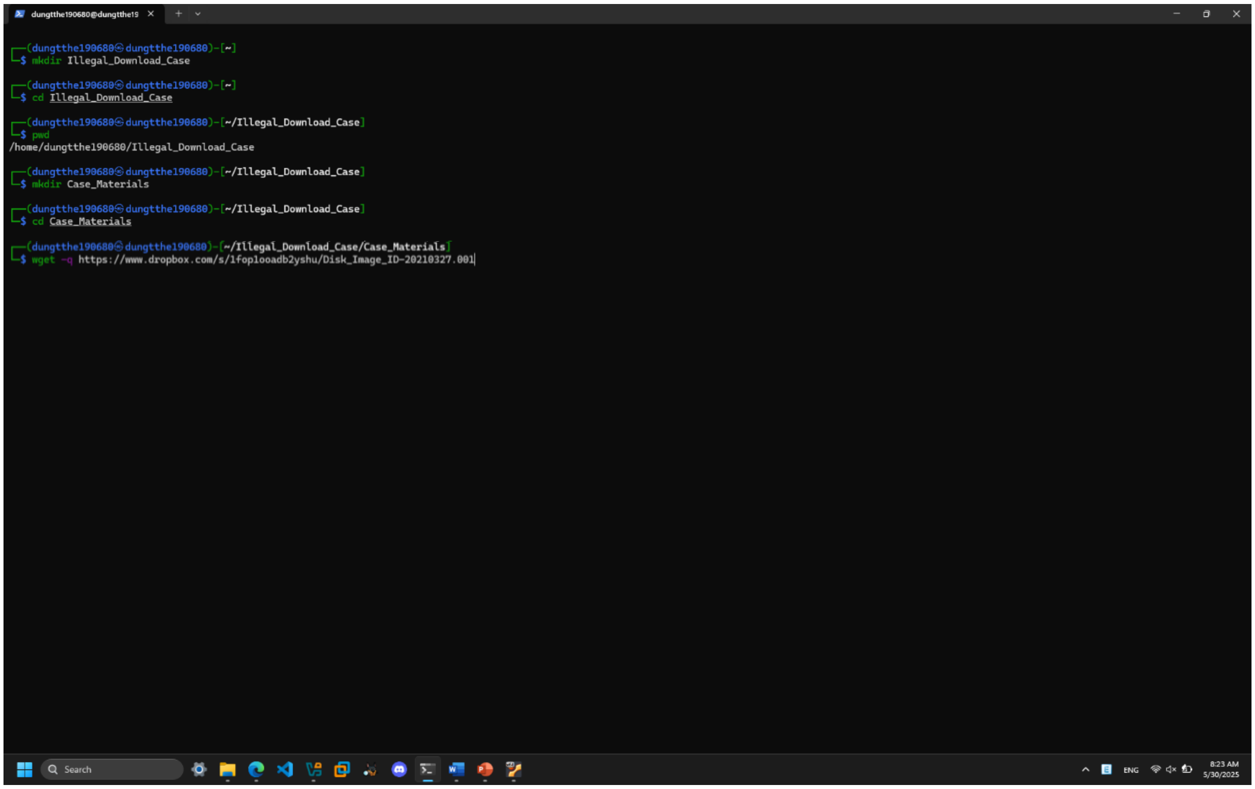
Mã số sinh viên: HE190680

Lớp: IA1901

Lab 4: Disk Image and Partitions

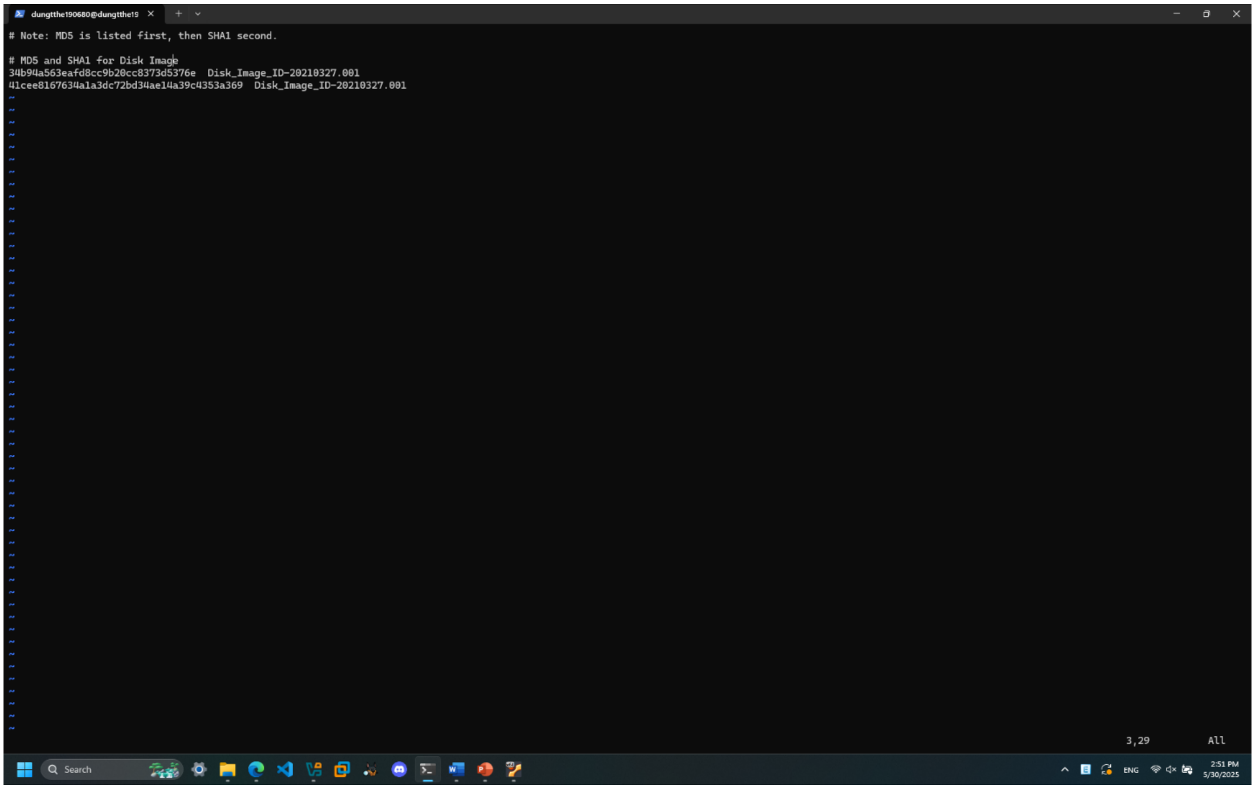
1. Verify the integrity of the disk image

Create Lab Folder -> Download Case Materials -> Use wget to download disk image:



```
┌──(dungtthe190680㉿dungtthe190680)-[~]
└─$ mkdir Illegal_Download_Case

┌──(dungtthe190680㉿dungtthe190680)-[~]
└─$ cd Illegal_Download_Case

┌──(dungtthe190680㉿dungtthe190680)-[~/Illegal_Download_Case]
└─$ pwd
/home/dungtthe190680/Illegal_Download_Case

┌──(dungtthe190680㉿dungtthe190680)-[~/Illegal_Download_Case]
└─$ mkdir Case_Materials

┌──(dungtthe190680㉿dungtthe190680)-[~/Illegal_Download_Case]
└─$ cd Case_Materials

┌──(dungtthe190680㉿dungtthe190680)-[~/Illegal_Download_Case/Case_Materials]
└─$ wget -q https://www.dropbox.com/s/1fop1ooadb2yshu/Disk_Image_ID-20210327.001
```

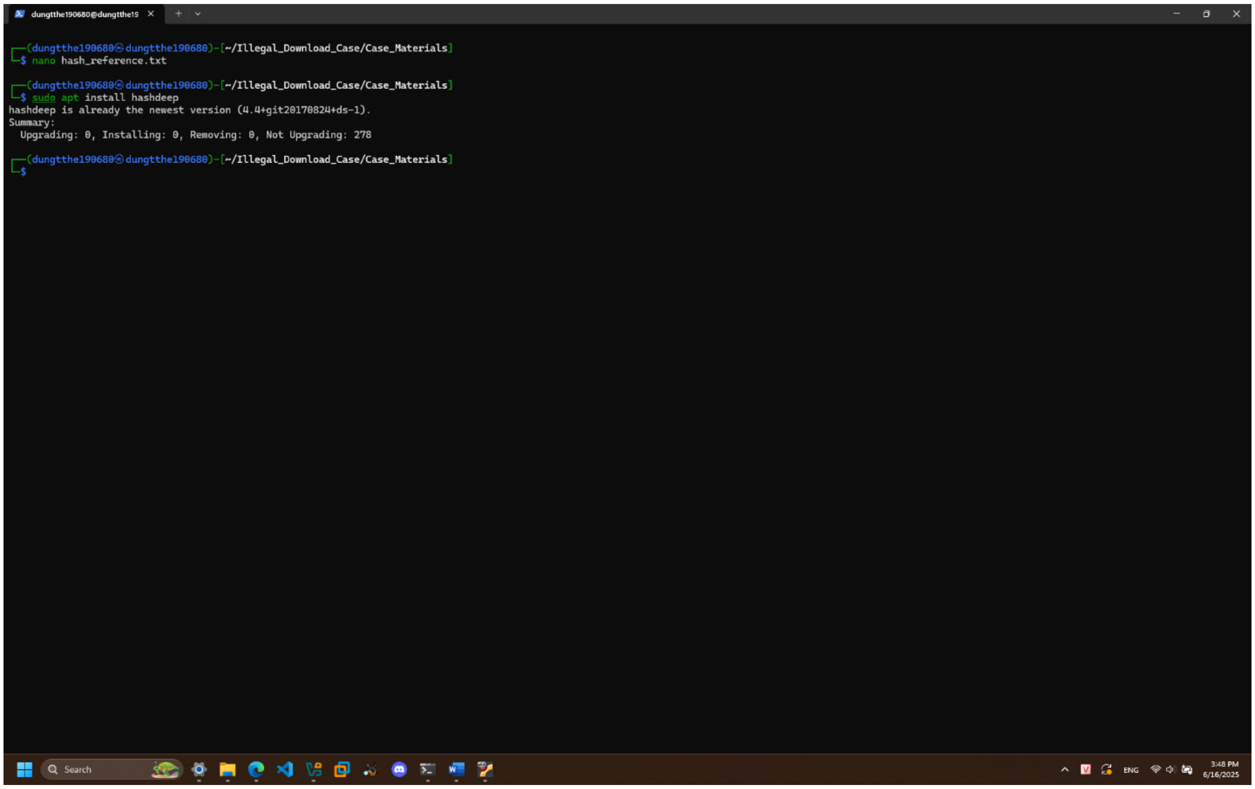
Record Hash Information -> Open a text file using the text editor Nano:



```
# Note: MD5 is listed first, then SHA1 second.

# MD5 and SHA1 for Disk Image
34b94a563eafd8cc9b20cc8373d5376e  Disk_Image_ID-20210327.001
41cee8167634a1a3dc72bd34ae14a39c4353a369  Disk_Image_ID-20210327.001
```

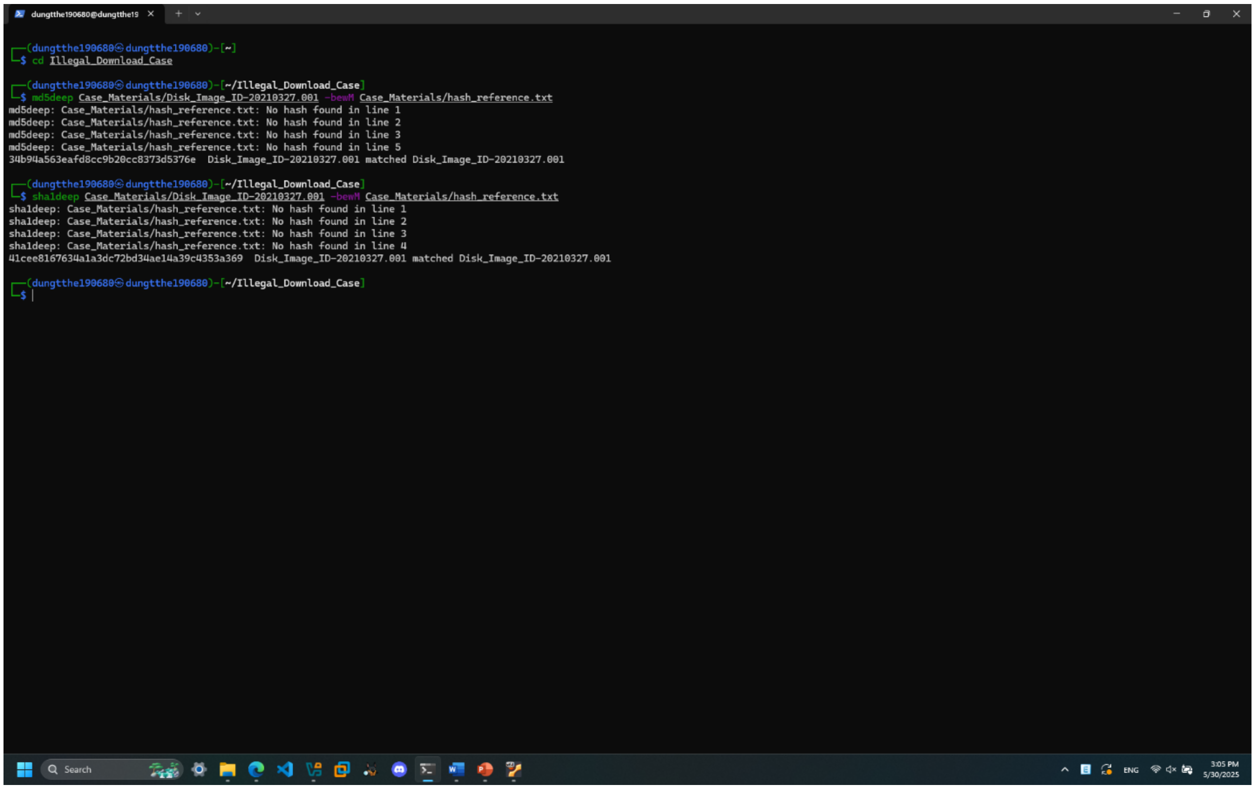
```
3,29          All
```

Install Necessary Software:



```
┌──(dungtthe190680㉿dungtthe190680)-[~/Illegal_Download_Case/Case_Materials]
└─$ nano hash_reference.txt

┌──(dungtthe190680㉿dungtthe190680)-[~/Illegal_Download_Case/Case_Materials]
└─$ sudo apt install hashdeep
hashdeep is already the newest version (4.4+git20170824+ds-1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 278

┌──(dungtthe190680㉿dungtthe190680)-[~/Illegal_Download_Case/Case_Materials]
└─$
```

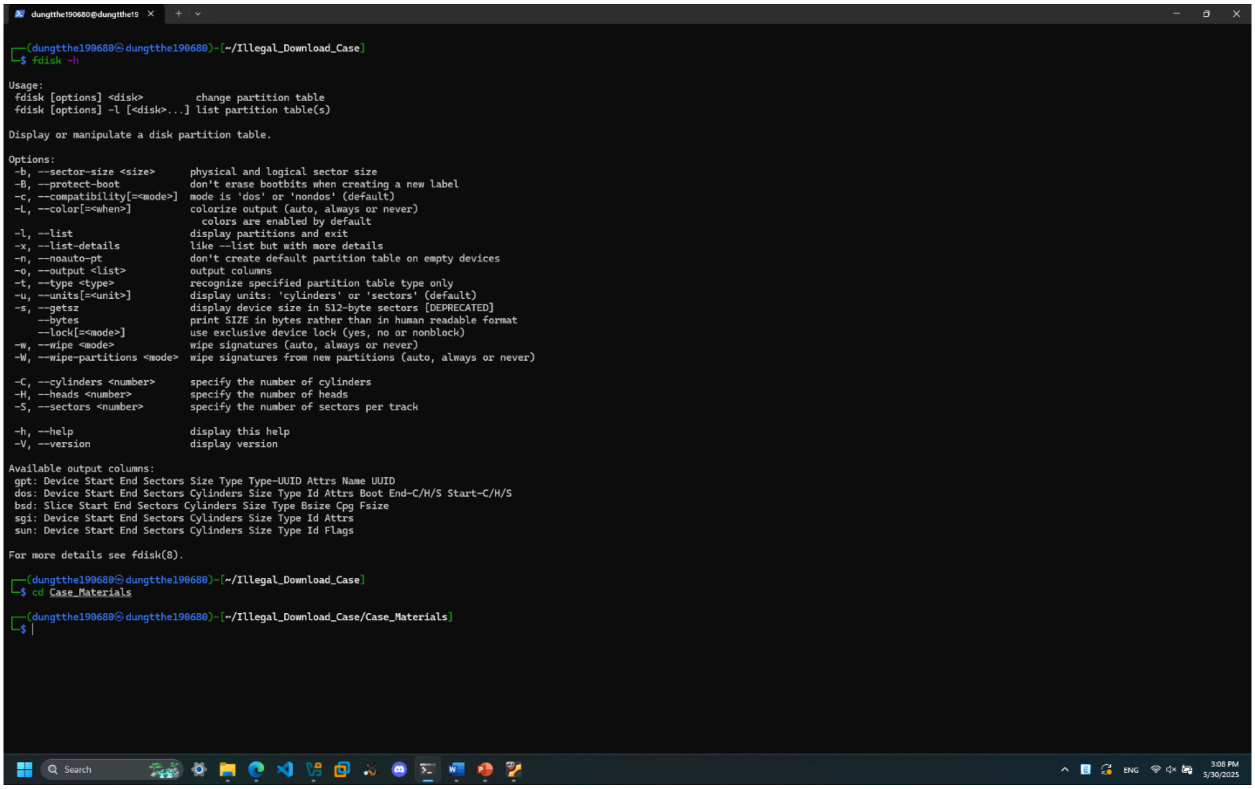
Move to the lab folder -> Use MD5deep and SHA1deep to verify the hashes of the disk image:



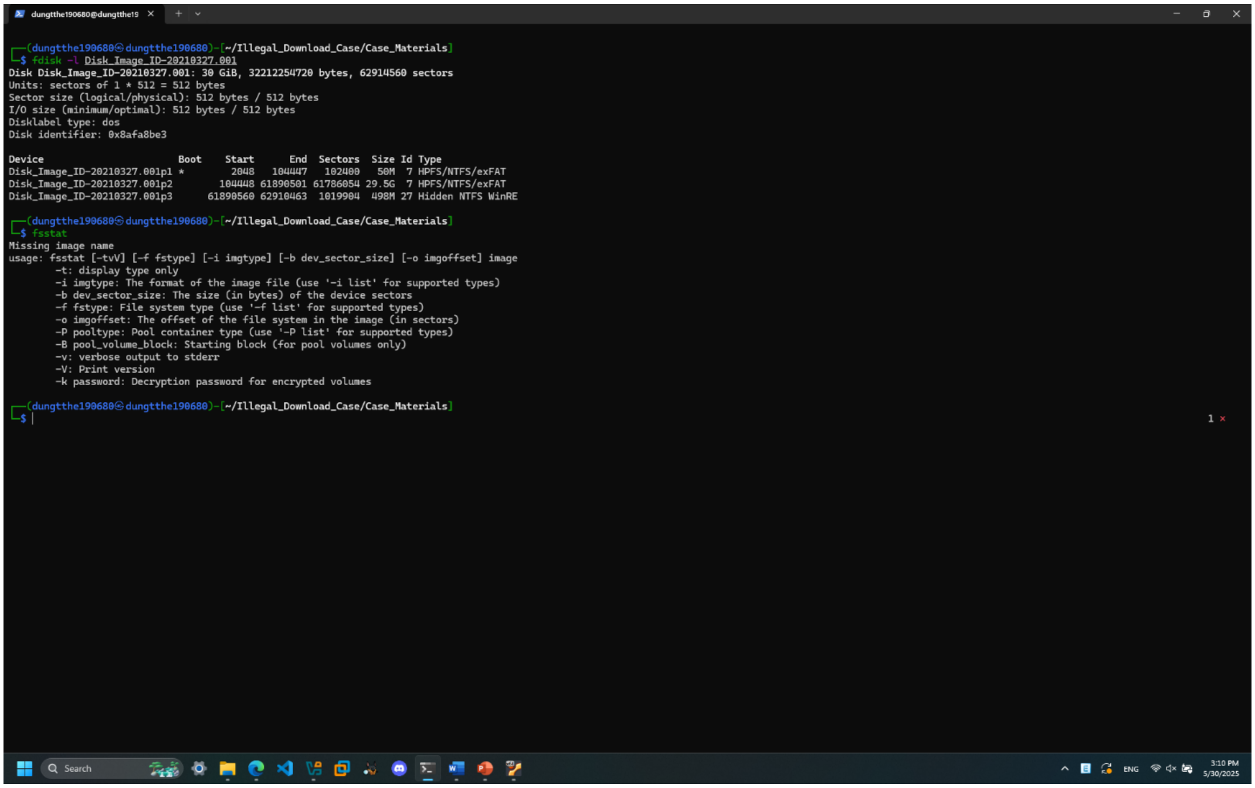
```
┌──(dungtthe190680㉿dungtthe190680)-[~]
└─$ cd Illegal_Download_Case

┌──(dungtthe190680㉿dungtthe190680)-[~/Illegal_Download_Case]
└─$ md5deep Case_Materials/Disk_Image_ID-20210327.001 -bewM Case_Materials/hash_reference.txt
md5deep: Case_Materials/hash_reference.txt: No hash found in line 1
md5deep: Case_Materials/hash_reference.txt: No hash found in line 2
md5deep: Case_Materials/hash_reference.txt: No hash found in line 3
md5deep: Case_Materials/hash_reference.txt: No hash found in line 5
34b94a563eafd8cc9b20cc8373d5376e  Disk_Image_ID-20210327.001 matched Disk_Image_ID-20210327.001

┌──(dungtthe190680㉿dungtthe190680)-[~/Illegal_Download_Case]
└─$ sha1deep Case_Materials/Disk_Image_ID-20210327.001 -bewM Case_Materials/hash_reference.txt
sha1deep: Case_Materials/hash_reference.txt: No hash found in line 1
sha1deep: Case_Materials/hash_reference.txt: No hash found in line 2
sha1deep: Case_Materials/hash_reference.txt: No hash found in line 3
sha1deep: Case_Materials/hash_reference.txt: No hash found in line 4
41cee8167634a1a3dc72bd34ae14a39c4353a369  Disk_Image_ID-20210327.001 matched Disk_Image_ID-20210327.001

┌──(dungtthe190680㉿dungtthe190680)-[~/Illegal_Download_Case]
└─$ |
```

2. Identify the OS of the system as well as its name, accounts, and partitions.

Get help for fdisk -> Use fdisk to get the disk image’s partition table -> Get help for fsstat:

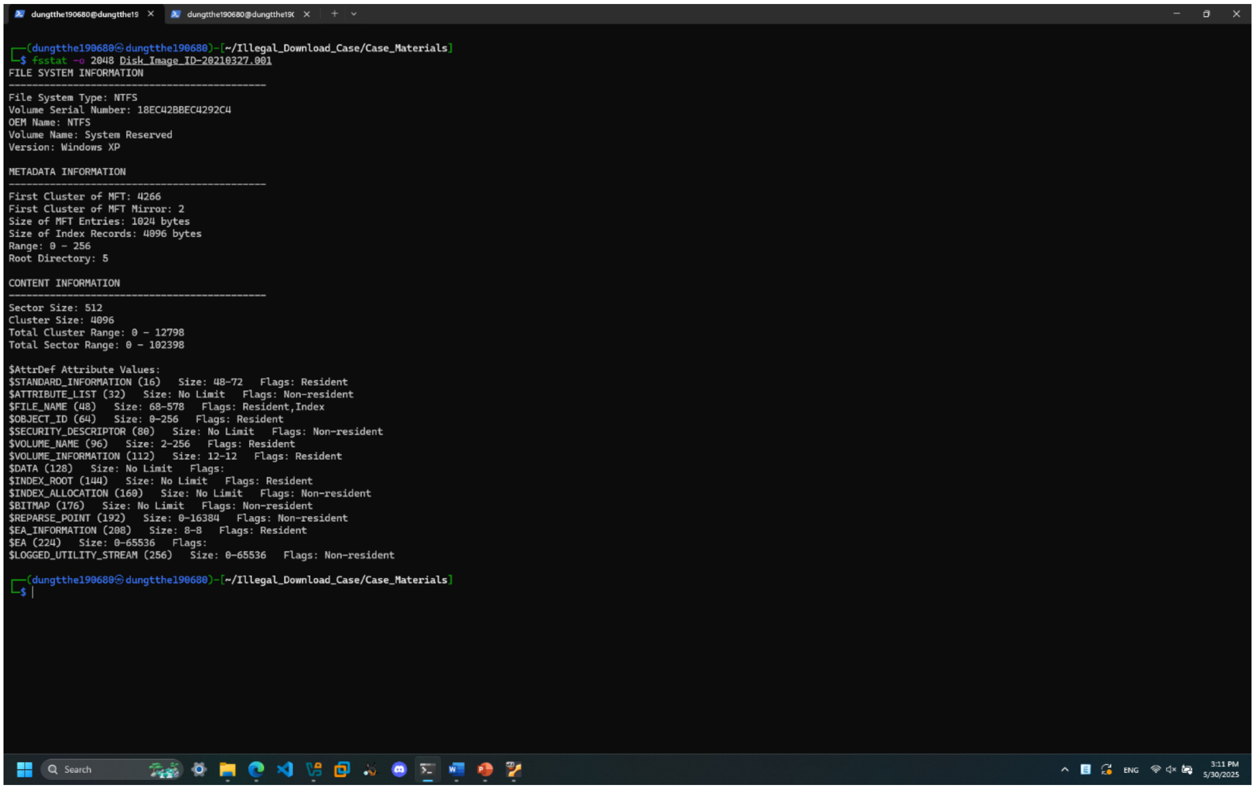


```
┌──(dungtthe190680㉿dungtthe190680)-[~/Illegal_Download_Case]
└─$ fdisk -h

Usage:
 fdisk [options] <disk>         change partition table
 fdisk [options] -l [<disk>...] list partition table(s)

Display or manipulate a disk partition table.

Options:
 -b, --sector-size <size>      physical and logical sector size
 -B, --protect-boot            don't erase bootbits when creating a new label
 -c, --compatibility[=<mode>]  mode is 'dos' or 'nondos' (default)
 -L, --color[=<when>]          colorize output (auto, always or never)
                                 colors are enabled by default
 -l, --list                    display partitions and exit
 -x, --list-details            like --list but with more details
 -n, --noauto-pt               don't create default partition table on empty devices
 -o, --output <list>           output columns
 -t, --type <type>             recognize specified partition table type only
 -u, --units[=<unit>]          display units: 'cylinders' or 'sectors' (default)
 -s, --getsz                   display device size in 512-byte sectors [DEPRECATED]
     --bytes                   print SIZE in bytes rather than in human readable format
     --lock[=<mode>]           use exclusive device lock (yes, no or nonblock)
 -w, --wipe <mode>             wipe signatures (auto, always or never)
 -W, --wipe-partitions <mode>  wipe signatures from new partitions (auto, always or never)

 -C, --cylinders <number>      specify the number of cylinders
 -H, --heads <number>          specify the number of heads
 -S, --sectors <number>        specify the number of sectors per track

 -h, --help                    display this help
 -V, --version                 display version

Available output columns:
 gpt: Device Start End Sectors Size Type Type-UUID Attrs Name UUID
 dos: Device Start End Sectors Cylinders Size Type Id Attrs Boot End-C/H/S Start-C/H/S
 bsd: Slice Start End Sectors Cylinders Size Type Bsize Cpg Fsize
 sgi: Device Start End Sectors Cylinders Size Type Id Attrs
 sun: Device Start End Sectors Cylinders Size Type Id Flags

For more details see fdisk(8).

┌──(dungtthe190680㉿dungtthe190680)-[~/Illegal_Download_Case]
└─$ cd Case_Materials

┌──(dungtthe190680㉿dungtthe190680)-[~/Illegal_Download_Case/Case_Materials]
└─$ |
```

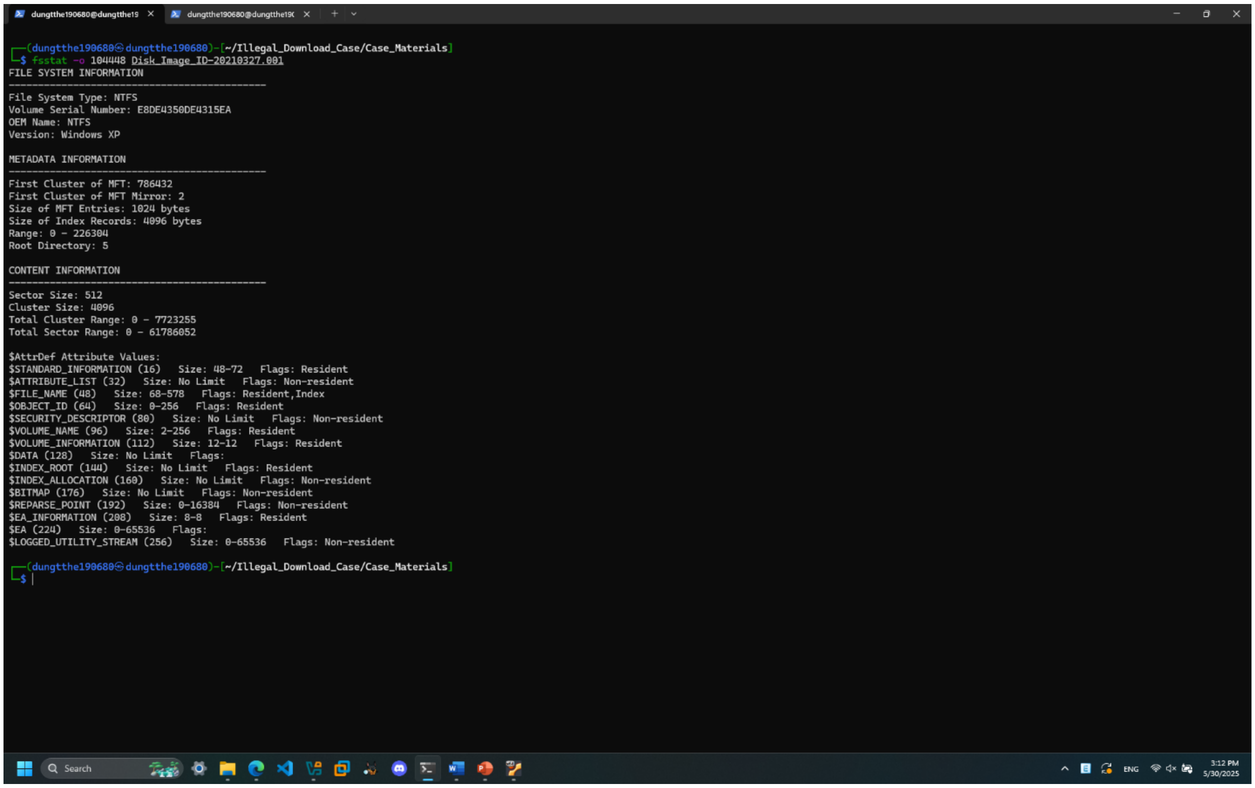


```
┌──(dungtthe190680㉿dungtthe190680)-[~/Illegal_Download_Case/Case_Materials]
└─$ fdisk -l Disk_Image_ID-20210327.001
Disk Disk_Image_ID-20210327.001: 30 GiB, 32212254720 bytes, 62914560 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x8afa8be3

Device                         Boot    Start      End  Sectors  Size Id Type
Disk_Image_ID-20210327.001p1 *          2048   104447   102400   50M  7 HPFS/NTFS/exFAT
Disk_Image_ID-20210327.001p2          104448 61890501 61786054 29.5G  7 HPFS/NTFS/exFAT
Disk_Image_ID-20210327.001p3        61890560 62910463  1019904  498M 27 Hidden NTFS WinRE

┌──(dungtthe190680㉿dungtthe190680)-[~/Illegal_Download_Case/Case_Materials]
└─$ fsstat
Missing image name
usage: fsstat [-tvV] [-f fstype] [-i imgtype] [-b dev_sector_size] [-o imgoffset] image
        -t: display type only
        -i imgtype: The format of the image file (use '-i list' for supported types)
        -b dev_sector_size: The size (in bytes) of the device sectors
        -f fstype: File system type (use '-f list' for supported types)
        -o imgoffset: The offset of the file system in the image (in sectors)
        -P pooltype: Pool container type (use '-P list' for supported types)
        -B pool_volume_block: Starting block (for pool volumes only)
        -v: verbose output to stderr
        -V: Print version
        -k password: Decryption password for encrypted volumes

┌──(dungtthe190680㉿dungtthe190680)-[~/Illegal_Download_Case/Case_Materials]
└─$ |                                                                                       1 ×
```

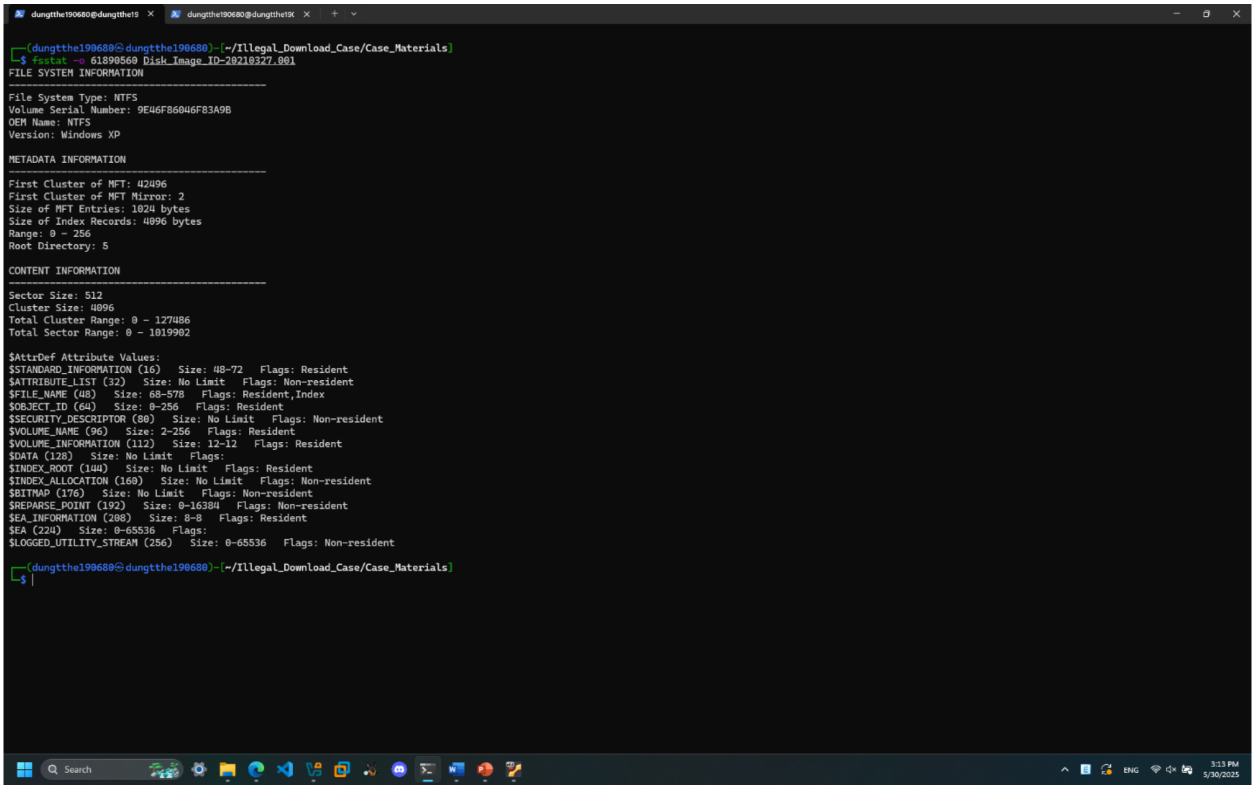
Use fsstat to get file system details:



```
┌──(dungtthe190680㉿dungtthe190680)-[~/Illegal_Download_Case/Case_Materials]
└─$ fsstat -o 2048 Disk_Image_ID-20210327.001
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: NTFS
Volume Serial Number: 18EC42BBEC4292C4
OEM Name: NTFS
Volume Name: System Reserved
Version: Windows XP

METADATA INFORMATION
--------------------------------------------
First Cluster of MFT: 4266
First Cluster of MFT Mirror: 2
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 256
Root Directory: 5

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 12798
Total Sector Range: 0 - 102398

$AttrDef Attribute Values:
$STANDARD_INFORMATION (16)   Size: 48-72   Flags: Resident
$ATTRIBUTE_LIST (32)   Size: No Limit   Flags: Non-resident
$FILE_NAME (48)   Size: 68-578   Flags: Resident,Index
$OBJECT_ID (64)   Size: 0-256   Flags: Resident
$SECURITY_DESCRIPTOR (80)   Size: No Limit   Flags: Non-resident
$VOLUME_NAME (96)   Size: 2-256   Flags: Resident
$VOLUME_INFORMATION (112)   Size: 12-12   Flags: Resident
$DATA (128)   Size: No Limit   Flags:
$INDEX_ROOT (144)   Size: No Limit   Flags: Resident
$INDEX_ALLOCATION (160)   Size: No Limit   Flags: Non-resident
$BITMAP (176)   Size: No Limit   Flags: Non-resident
$REPARSE_POINT (192)   Size: 0-16384   Flags: Non-resident
$EA_INFORMATION (208)   Size: 8-8   Flags: Resident
$EA (224)   Size: 0-65536   Flags:
$LOGGED_UTILITY_STREAM (256)   Size: 0-65536   Flags: Non-resident

┌──(dungtthe190680㉿dungtthe190680)-[~/Illegal_Download_Case/Case_Materials]
└─$ |
```



```
┌──(dungtthe190680㉿dungtthe190680)-[~/Illegal_Download_Case/Case_Materials]
└─$ fsstat -o 104448 Disk_Image_ID-20210327.001
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: NTFS
Volume Serial Number: E8DE4350DE4315EA
OEM Name: NTFS
Version: Windows XP

METADATA INFORMATION
--------------------------------------------
First Cluster of MFT: 786432
First Cluster of MFT Mirror: 2
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 226304
Root Directory: 5

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 7723255
Total Sector Range: 0 - 61786052

$AttrDef Attribute Values:
$STANDARD_INFORMATION (16)   Size: 48-72   Flags: Resident
$ATTRIBUTE_LIST (32)   Size: No Limit   Flags: Non-resident
$FILE_NAME (48)   Size: 68-578   Flags: Resident,Index
$OBJECT_ID (64)   Size: 0-256   Flags: Resident
$SECURITY_DESCRIPTOR (80)   Size: No Limit   Flags: Non-resident
$VOLUME_NAME (96)   Size: 2-256   Flags: Resident
$VOLUME_INFORMATION (112)   Size: 12-12   Flags: Resident
$DATA (128)   Size: No Limit   Flags:
$INDEX_ROOT (144)   Size: No Limit   Flags: Resident
$INDEX_ALLOCATION (160)   Size: No Limit   Flags: Non-resident
$BITMAP (176)   Size: No Limit   Flags: Non-resident
$REPARSE_POINT (192)   Size: 0-16384   Flags: Non-resident
$EA_INFORMATION (208)   Size: 8-8   Flags: Resident
$EA (224)   Size: 0-65536   Flags:
$LOGGED_UTILITY_STREAM (256)   Size: 0-65536   Flags: Non-resident

┌──(dungtthe190680㉿dungtthe190680)-[~/Illegal_Download_Case/Case_Materials]
└─$ |
```



```
┌──(dungtthe190680㉿dungtthe190680)-[~/Illegal_Download_Case/Case_Materials]
└─$ fsstat -o 61890560 Disk_Image_ID-20210327.001
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: NTFS
Volume Serial Number: 9E46F86046F83A9B
OEM Name: NTFS
Version: Windows XP

METADATA INFORMATION
--------------------------------------------
First Cluster of MFT: 42496
First Cluster of MFT Mirror: 2
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 256
Root Directory: 5

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 127486
Total Sector Range: 0 - 1019902

$AttrDef Attribute Values:
$STANDARD_INFORMATION (16)   Size: 48-72   Flags: Resident
$ATTRIBUTE_LIST (32)   Size: No Limit   Flags: Non-resident
$FILE_NAME (48)   Size: 68-578   Flags: Resident,Index
$OBJECT_ID (64)   Size: 0-256   Flags: Resident
$SECURITY_DESCRIPTOR (80)   Size: No Limit   Flags: Non-resident
$VOLUME_NAME (96)   Size: 2-256   Flags: Resident
$VOLUME_INFORMATION (112)   Size: 12-12   Flags: Resident
$DATA (128)   Size: No Limit   Flags:
$INDEX_ROOT (144)   Size: No Limit   Flags: Resident
$INDEX_ALLOCATION (160)   Size: No Limit   Flags: Non-resident
$BITMAP (176)   Size: No Limit   Flags: Non-resident
$REPARSE_POINT (192)   Size: 0-16384   Flags: Non-resident
$EA_INFORMATION (208)   Size: 8-8   Flags: Resident
$EA (224)   Size: 0-65536   Flags:
$LOGGED_UTILITY_STREAM (256)   Size: 0-65536   Flags: Non-resident

┌──(dungtthe190680㉿dungtthe190680)-[~/Illegal_Download_Case/Case_Materials]
└─$ |
```

Partition 1

File System: NTFS

Serial Number: 18EC42BBEC4292C4

Partition 2

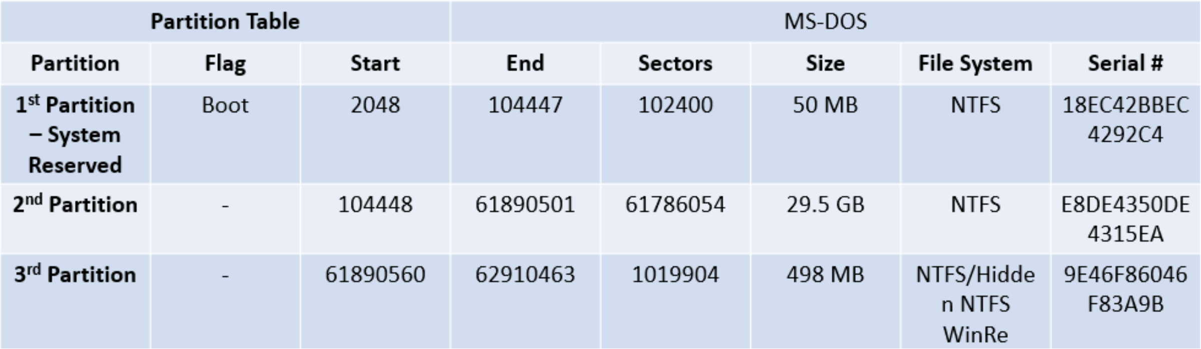
File System: NTFS

Serial Number: E8DE4350DE4315EA

Partition 3

File System: NTFS

Serial Number: 9E46F86046F83A9B



Partition Table			MS-DOS				
Partition	Flag	Start	End	Sectors	Size	File System	Serial #
1st Partition – System Reserved	Boot	2048	104447	102400	50 MB	NTFS	18EC42BBEC4292C4
2nd Partition	-	104448	61890501	61786054	29.5 GB	NTFS	E8DE4350DE4315EA
3rd Partition	-	61890560	62910463	1019904	498 MB	NTFS/Hidden NTFS WinRe	9E46F86046F83A9B

1. Partition: Identifies the partition number and any additional label or purpose.

- **1st Partition – System Reserved**: The first partition, labeled "System Reserved," is typically used in Windows systems to store boot-related files, such as the Boot Configuration Data (BCD) and sometimes the Windows Recovery Environment (WinRE).
- **2nd Partition**: The second partition, with no additional label, is likely the main partition where the Windows operating system and user data are stored (e.g., the C: drive).
- **3rd Partition**: The third partition, also unlabeled here, serves a specific purpose (revealed by the "File System" column as a recovery partition).

2. Flag: Indicates any special attributes or flags associated with the partition.

- **Boot**: Set for the first partition ("Boot" flag), meaning it is bootable and contains the files needed to start the operating system.

- **–**: For the second and third partitions, no flags are set, indicating they are not bootable or marked with other special attributes.

3. Start: The starting sector of the partition on the disk.

- **1st Partition**: Starts at sector 2048, a common starting point for proper disk alignment (2048 × 512 bytes = 1 MiB).
- **2nd Partition**: Starts at sector 104448, right after the first partition ends (104447 + 1).
- **3rd Partition**: Starts at sector 61890560, following the second partition with a small gap (59 sectors), possibly for alignment or reserved space.

4. End: The ending sector of the partition on the disk.

- **1st Partition**: Ends at sector 104447.
- **2nd Partition**: Ends at sector 61890501.
- **3rd Partition**: Ends at sector 62910463.

5. Sectors: The total number of sectors in the partition.

- **1st Partition**: 102400 sectors (calculated as 104447 - 2048 + 1).
- **2nd Partition**: 61786054 sectors (61890501 - 104448 + 1).
- **3rd Partition**: 1019904 sectors (62910463 - 61890560 + 1).

6. Size: The size of the partition in a human-readable format (e.g., MB or GB).

- **1st Partition**: 50 MB (102400 sectors × 512 bytes = 52,428,800 bytes ≈ 50 MB).
- **2nd Partition**: 29.5 GB (61786054 sectors × 512 bytes = 31,634,459,648 bytes ≈ 29.5 GB).
- **3rd Partition**: 498 MB (1019904 sectors × 512 bytes = 522,188,928 bytes ≈ 498 MB).

7. File System: The type of filesystem used in the partition.

- **1st Partition**: NTFS (New Technology File System), standard for Windows partitions.
- **2nd Partition**: NTFS, likely hosting the Windows OS and user data.
- **3rd Partition**: "NTFS/Hidden NTFS WinRE," indicating an NTFS filesystem used for the Windows Recovery Environment (WinRE), hidden from normal view (e.g., not visible in Windows Explorer).

8. Serial: The serial number of the filesystem on the partition.

- **1st Partition**: 18EC42BBEC4292C4.
- **2nd Partition**: E8DE4350DE4315EA.
- **3rd Partition**: 9E46F86046F8349B.