Lab 4: Disk Image and Partitions

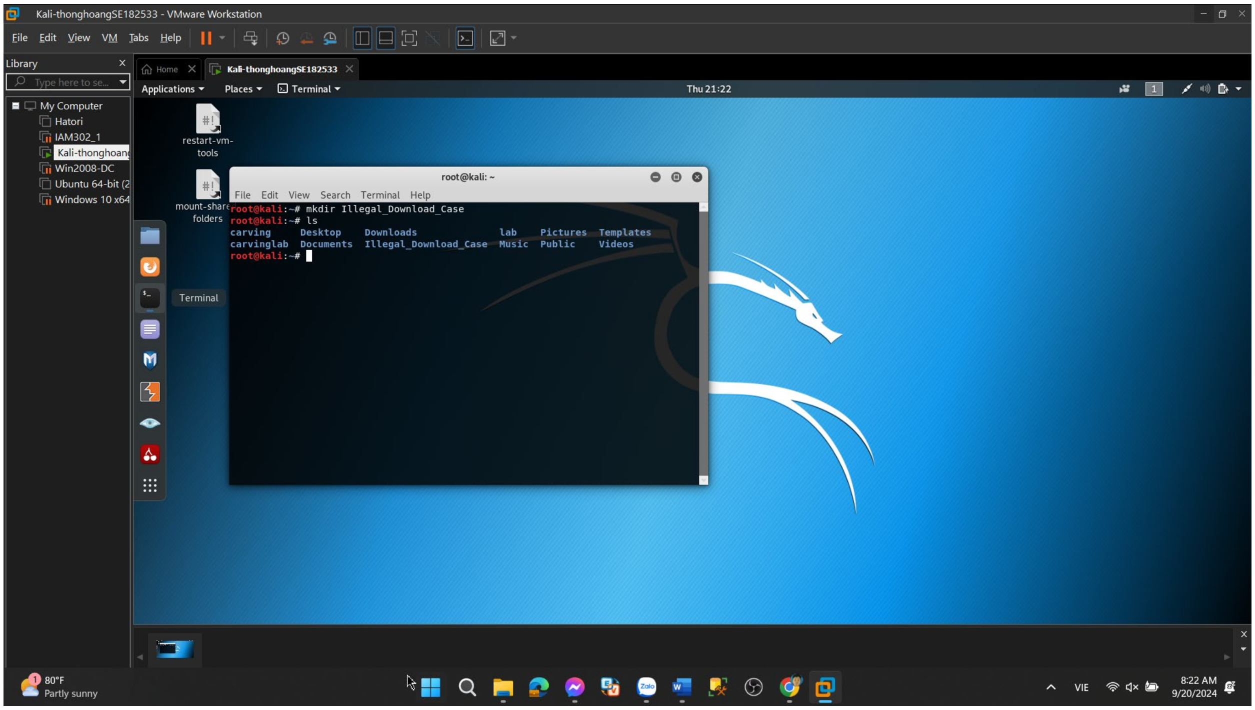
Group: CyberSec_N00b

Member:

- *Huỳnh Ngọc Quang (SE181838)*
- *Hồ Tài Liên Vy Kha (SE181818)*
- *Hoàng Kim Long (DE180860)*
- *Phạm Thành Long (SE181692)*
- *Nguyễn Lê Hoàng Thông (SE182533)*

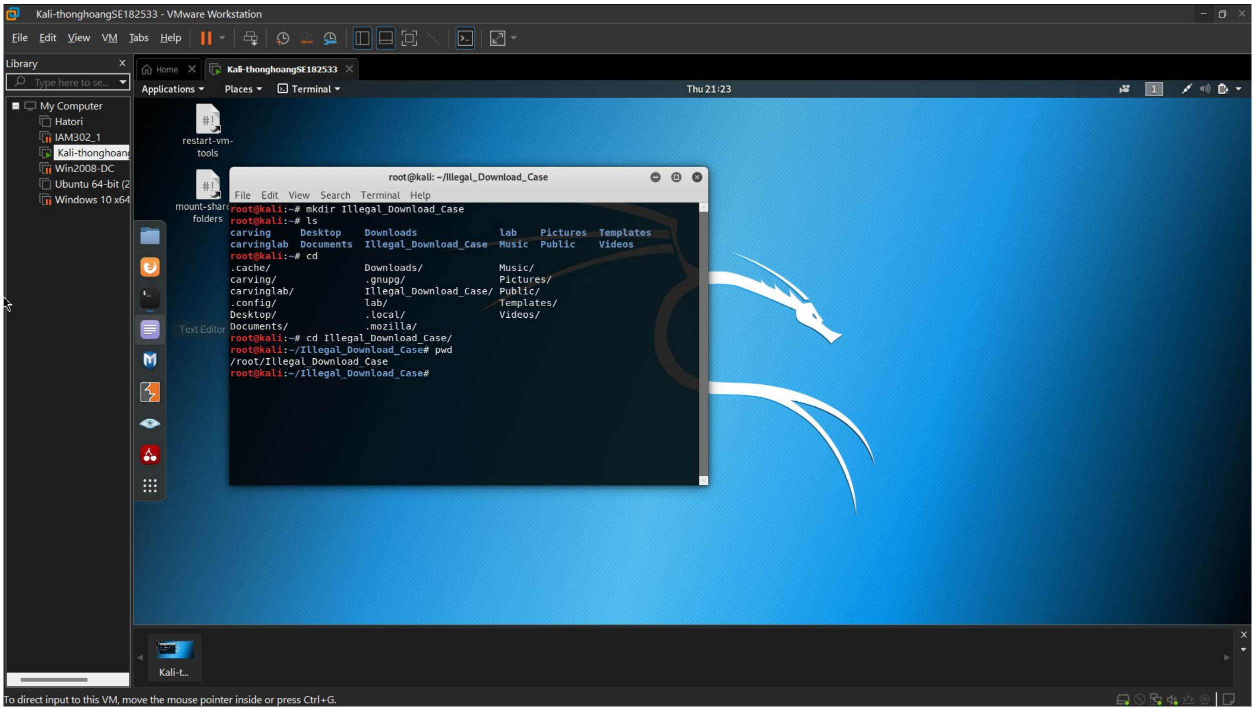
1. Verify the integrity of the disk image

– Create Lab Folder



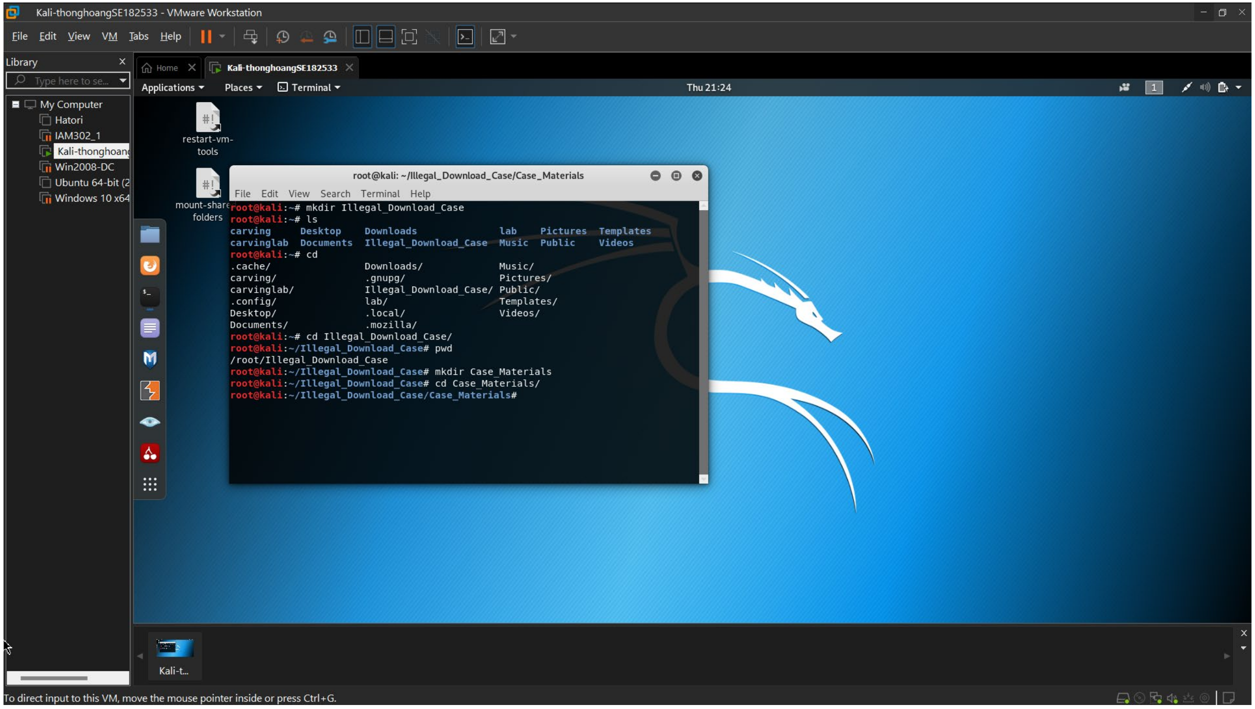
```
root@kali:~# mkdir Illegal_Download_Case
root@kali:~# ls
carving    Desktop    Downloads              lab    Pictures  Templates
carvinglab Documents  Illegal_Download_Case  Music  Public    Videos
root@kali:~# 
```

– Download Case Materials



```
root@kali:~# mkdir Illegal_Download_Case
root@kali:~# ls
carving     Desktop    Downloads            lab    Pictures  Templates
carvinglab  Documents  Illegal_Download_Case  Music  Public    Videos
root@kali:~# cd
.cache/              Downloads/             Music/
carving/             .gnupg/                Pictures/
carvinglab/          Illegal_Download_Case/ Public/
.config/             lab/                   Templates/
Desktop/             .local/                Videos/
Documents/           .mozilla/
root@kali:~# cd Illegal_Download_Case/
root@kali:~/Illegal_Download_Case# pwd
/root/Illegal_Download_Case
root@kali:~/Illegal_Download_Case#
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



```
root@kali:~# mkdir Illegal_Download_Case
root@kali:~# ls
carving     Desktop    Downloads            lab    Pictures  Templates
carvinglab  Documents  Illegal_Download_Case  Music  Public    Videos
root@kali:~# cd
.cache/              Downloads/             Music/
carving/             .gnupg/                Pictures/
carvinglab/          Illegal_Download_Case/ Public/
.config/             lab/                   Templates/
Desktop/             .local/                Videos/
Documents/           .mozilla/
root@kali:~# cd Illegal_Download_Case/
root@kali:~/Illegal_Download_Case# pwd
/root/Illegal_Download_Case
root@kali:~/Illegal_Download_Case# mkdir Case_Materials
root@kali:~/Illegal_Download_Case# cd Case_Materials/
root@kali:~/Illegal_Download_Case/Case_Materials#
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- Use *wget* to download disk image. (about 30GB) Install Necessary Software

  ❑ Hashdeep

  ❑ Md5deep

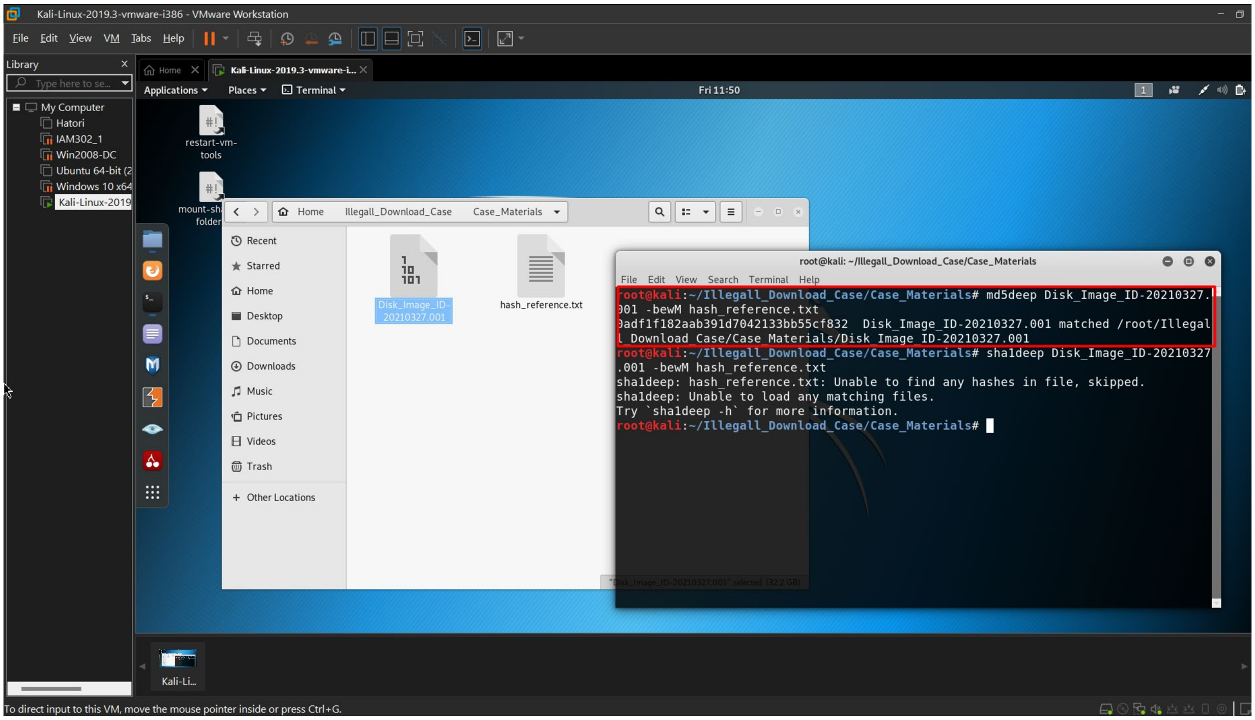
sudo apt install hashdeep

Step 2.

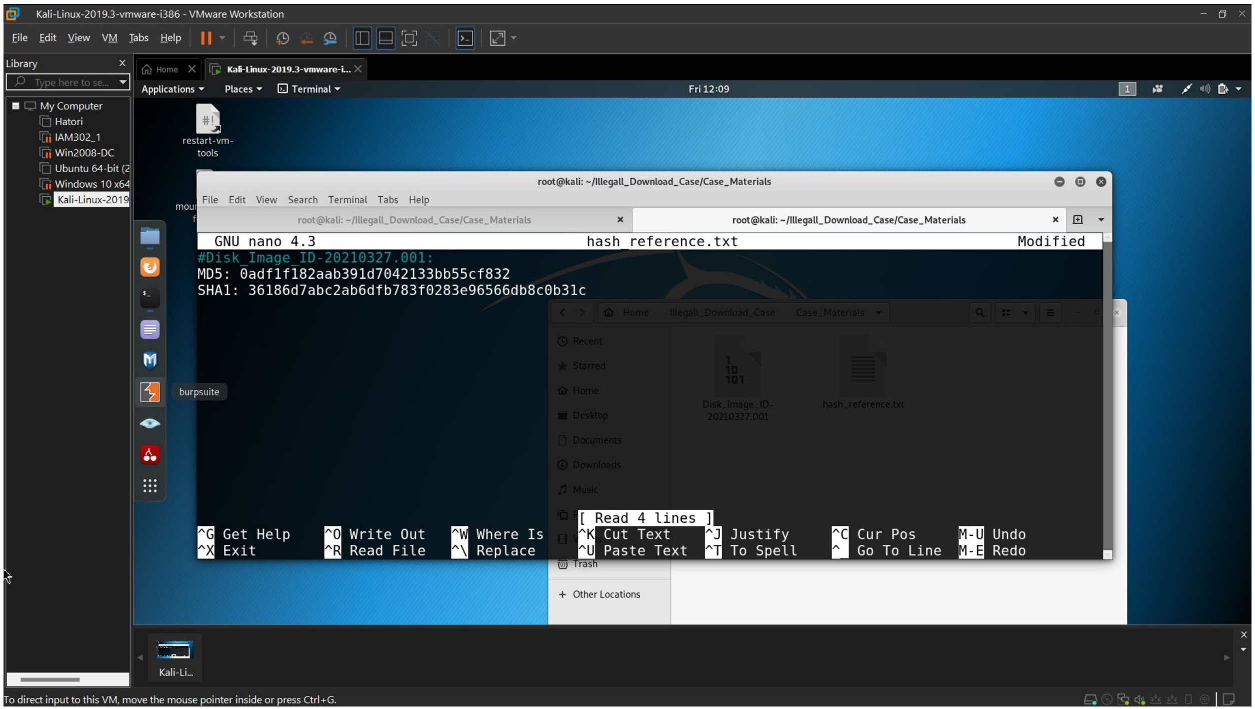
Generate an MD5 and SHA1 hash of the disk image. These tools will compare the MD5 and/or SHA1 hash of the disk image to the MD5 and/or SHA1 hash in the '*hash_reference.txt*' file.

Commands

- *md5deep <disk image> -bewM <file that contains file names and hash codes>*



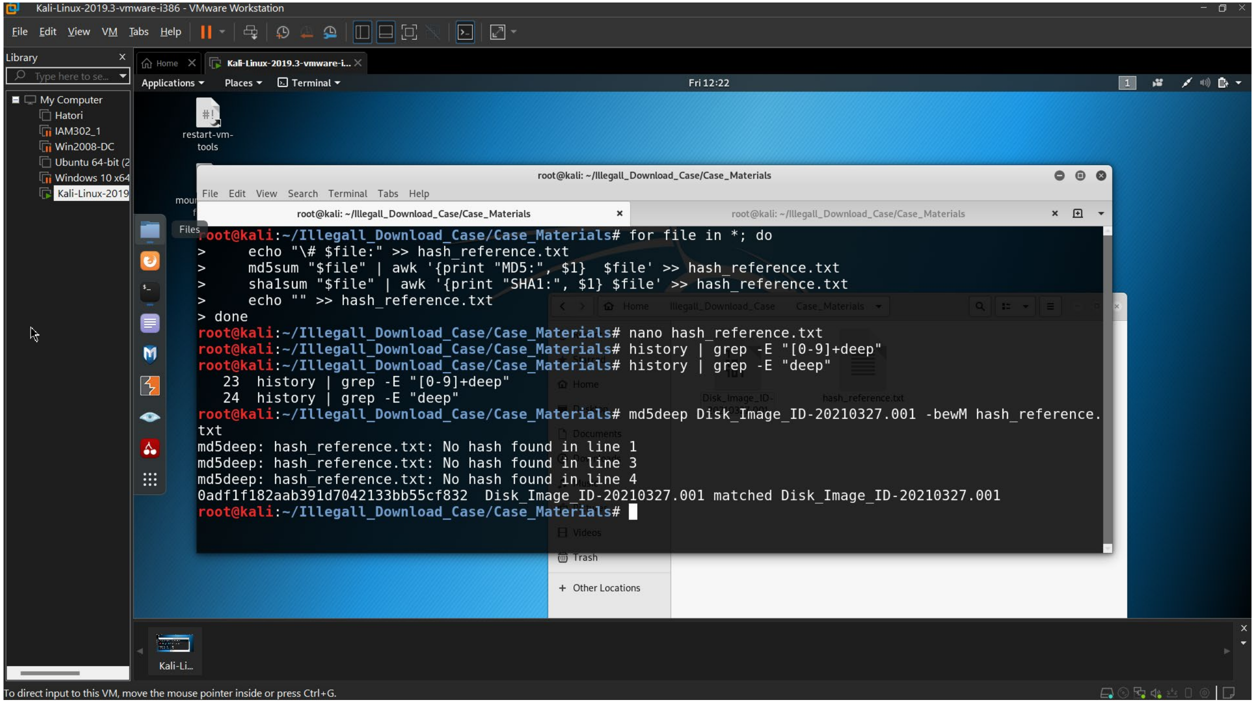
```
root@kali:~/Illegall_Download_Case/Case_Materials# md5deep Disk_Image_ID-20210327.
001 -bewM hash_reference.txt
0adf1f182aab391d7042133bb55cf832  Disk_Image_ID-20210327.001 matched /root/Illegal
l_Download_Case/Case_Materials/Disk_Image_ID-20210327.001
root@kali:~/Illegall_Download_Case/Case_Materials# sha1deep Disk_Image_ID-20210327
.001 -bewM hash_reference.txt
sha1deep: hash_reference.txt: Unable to find any hashes in file, skipped.
sha1deep: Unable to load any matching files.
Try `sha1deep -h` for more information.
root@kali:~/Illegall_Download_Case/Case_Materials# 
```



Kali-Linux-2019.3-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Hatori
IAM302_1
Win2008-DC
Ubuntu 64-bit (2
Windows 10 x64
Kali-Linux-2019
Home
Kali-Linux-2019.3-vmware-i...
Applications
Places
Terminal
Fri 12:09
restart-vm-tools
burpsuite
root@kali: ~/Illegall_Download_Case/Case_Materials
File Edit View Search Terminal Tabs Help
Disk_Image_ID-20210327.001
hash_reference.txt
Other Locations
Kali-Li...

```
  GNU nano 4.3                  hash_reference.txt                  Modified
#Disk_Image_ID-20210327.001:
MD5: 0adf1f182aab391d7042133bb55cf832
SHA1: 36186d7abc2ab6dfb783f0283e96566db8c0b31c

                              [ Read 4 lines ]
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo
```

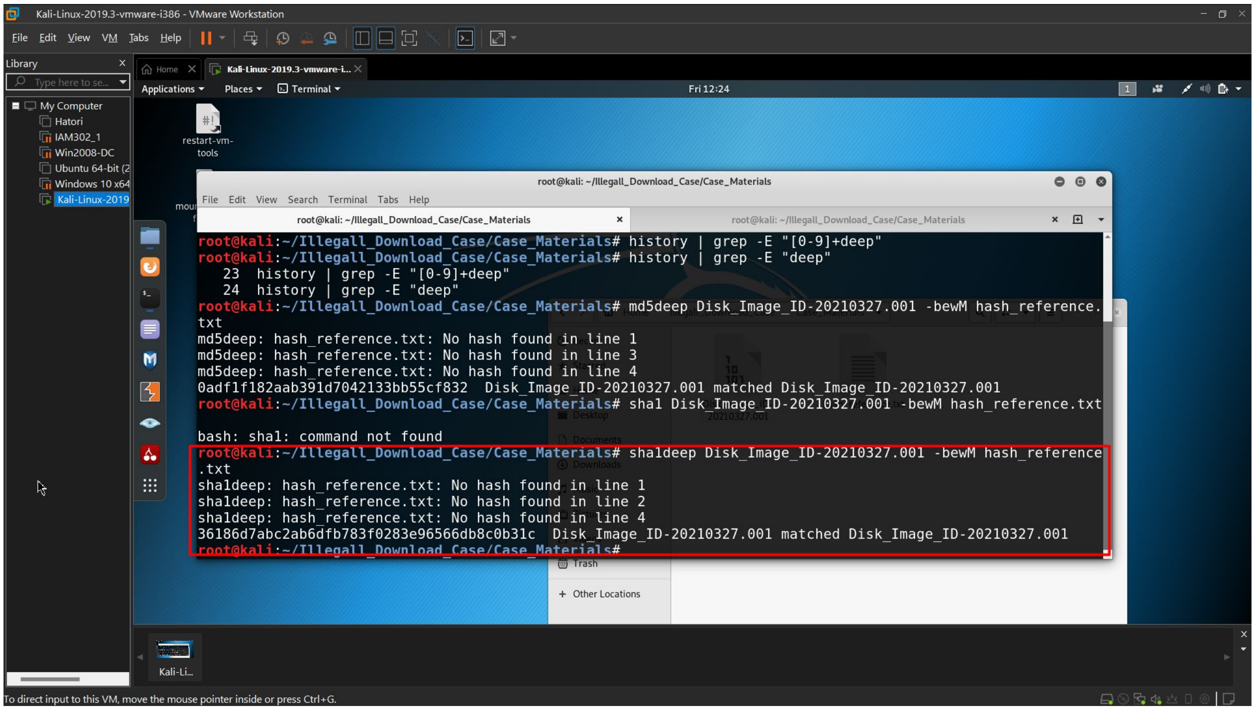
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Kali-Linux-2019.3-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Hatori
IAM302_1
Win2008-DC
Ubuntu 64-bit (2
Windows 10 x64
Kali-Linux-2019
Home
Kali-Linux-2019.3-vmware-i...
Applications
Places
Terminal
Fri 12:22
restart-vm-tools
Files
root@kali: ~/Illegall_Download_Case/Case_Materials
File Edit View Search Terminal Tabs Help
Other Locations
Kali-Li...

```
root@kali:~/Illegall_Download_Case/Case_Materials# for file in *; do
>     echo "\# $file:" >> hash_reference.txt
>     md5sum "$file" | awk '{print "MD5:", $1}  $file' >> hash_reference.txt
>     sha1sum "$file" | awk '{print "SHA1:", $1} $file' >> hash_reference.txt
>     echo "" >> hash_reference.txt
> done
root@kali:~/Illegall_Download_Case/Case_Materials# nano hash_reference.txt
root@kali:~/Illegall_Download_Case/Case_Materials# history | grep -E "[0-9]+deep"
root@kali:~/Illegall_Download_Case/Case_Materials# history | grep -E "deep"
   23  history | grep -E "[0-9]+deep"
   24  history | grep -E "deep"
root@kali:~/Illegall_Download_Case/Case_Materials# md5deep Disk_Image_ID-20210327.001 -bewM hash_reference.
txt
md5deep: hash_reference.txt: No hash found in line 1
md5deep: hash_reference.txt: No hash found in line 3
md5deep: hash_reference.txt: No hash found in line 4
0adf1f182aab391d7042133bb55cf832  Disk_Image_ID-20210327.001 matched Disk_Image_ID-20210327.001
root@kali:~/Illegall_Download_Case/Case_Materials# 
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



```
root@kali:~/Illegall_Download_Case/Case_Materials# history | grep -E "[0-9]+deep"
root@kali:~/Illegall_Download_Case/Case_Materials# history | grep -E "deep"
   23  history | grep -E "[0-9]+deep"
   24  history | grep -E "deep"
root@kali:~/Illegall_Download_Case/Case_Materials# md5deep Disk_Image_ID-20210327.001 -bewM hash_reference.
txt
md5deep: hash_reference.txt: No hash found in line 1
md5deep: hash_reference.txt: No hash found in line 3
md5deep: hash_reference.txt: No hash found in line 4
0adf1f182aab391d7042133bb55cf832  Disk_Image_ID-20210327.001 matched Disk_Image_ID-20210327.001
root@kali:~/Illegall_Download_Case/Case_Materials# sha1 Disk_Image_ID-20210327.001 -bewM hash_reference.txt

bash: sha1: command not found
root@kali:~/Illegall_Download_Case/Case_Materials# sha1deep Disk_Image_ID-20210327.001 -bewM hash_reference
.txt
sha1deep: hash_reference.txt: No hash found in line 1
sha1deep: hash_reference.txt: No hash found in line 2
sha1deep: hash_reference.txt: No hash found in line 4
36186d7abc2ab6dfb783f0283e96566db8c0b31c  Disk_Image_ID-20210327.001 matched Disk_Image_ID-20210327.001
root@kali:~/Illegall_Download_Case/Case_Materials#
```

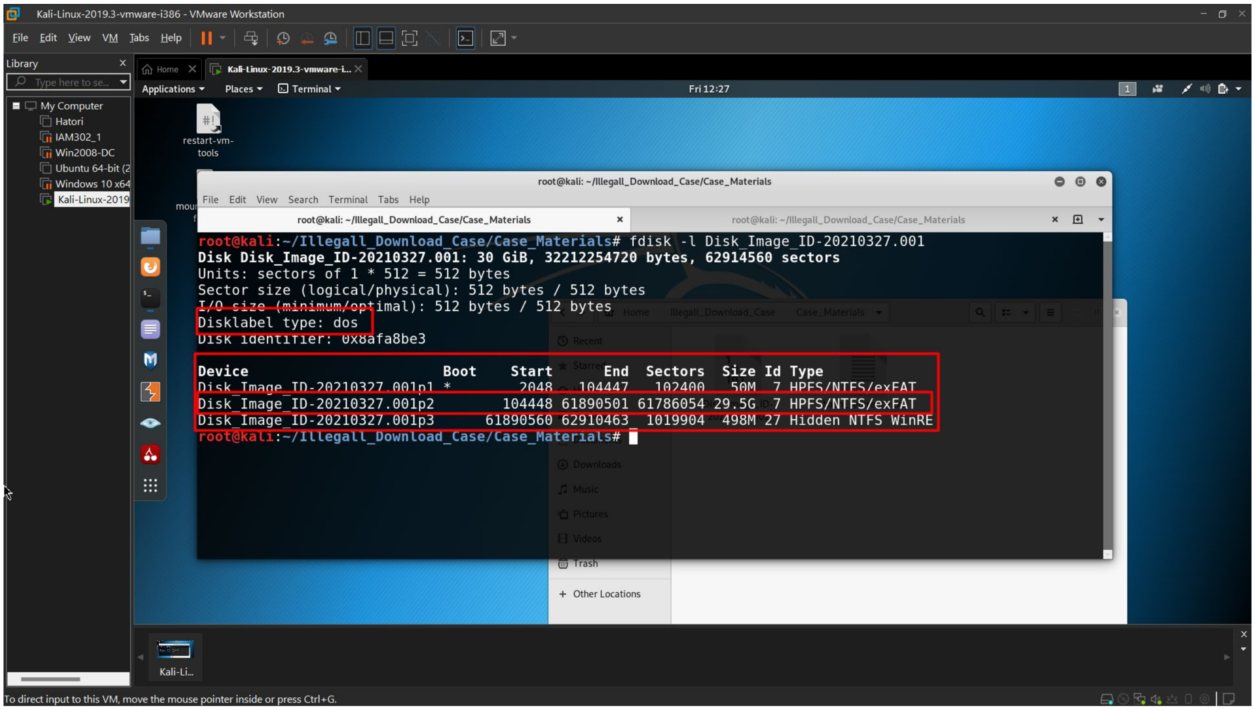
Kali-Linux-2019.3-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Hatori
IAM302_1
Win2008-DC
Ubuntu 64-bit (2
Windows 10 x64
Kali-Linux-2019
Home
Kali-Linux-2019.3-vmware-i...
Applications
Places
Terminal
Fri 12:24
restart-vm-tools
root@kali: ~/Illegall_Download_Case/Case_Materials
File Edit View Search Terminal Tabs Help
Trash
Other Locations
Kali-Li...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- Note: You would replace <disk image> with the file path to the disk image. The same applies to anything else contained in between ‘< >’.

- Use MD5deep to verify the MD5 hash of the disk image.

- Use SHA1deep to verify the MD5 hash of the disk image.

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



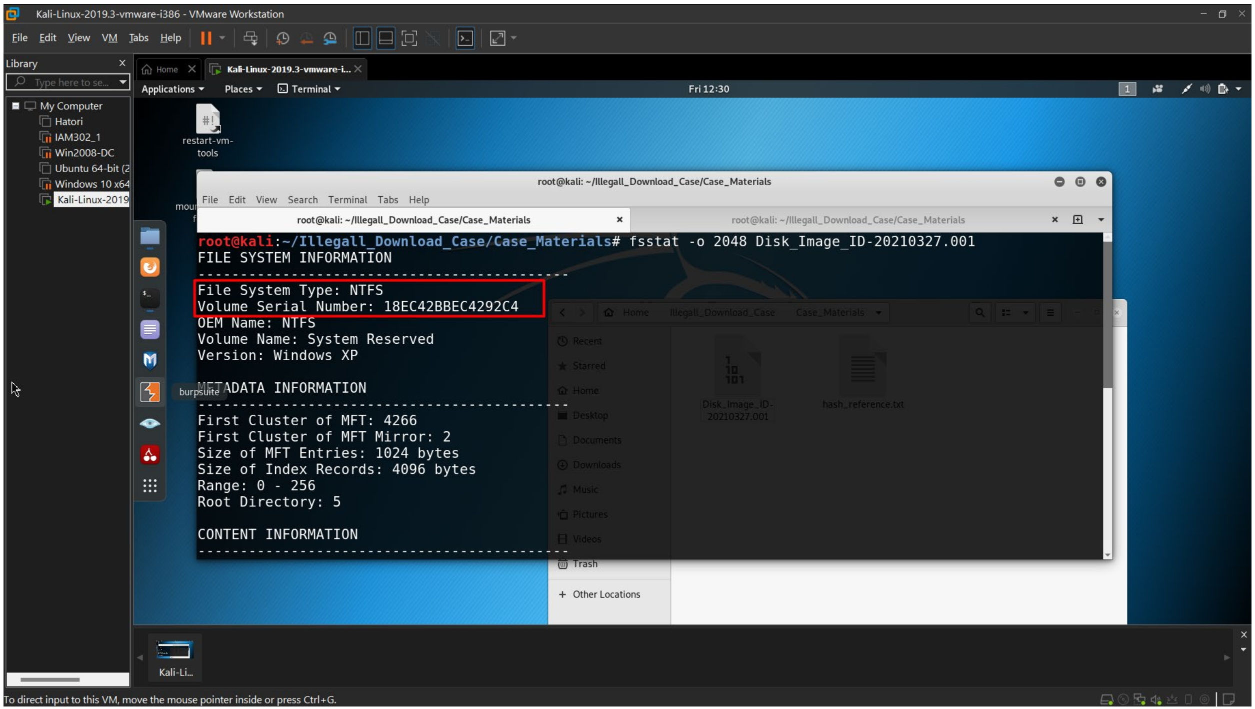
Kali-Linux-2019.3-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Hatori
IAM302_1
Win2008-DC
Ubuntu 64-bit (2
Windows 10 x64
Kali-Linux-2019
Home
Kali-Linux-2019.3-vmware-i...
Applications
Places
Terminal
Fri 12:27
restart-vm-tools
root@kali: ~/Illegall_Download_Case/Case_Materials
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
root@kali:~/Illegall_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
root@kali:~/Illegall_Download_Case/Case_Materials#
```

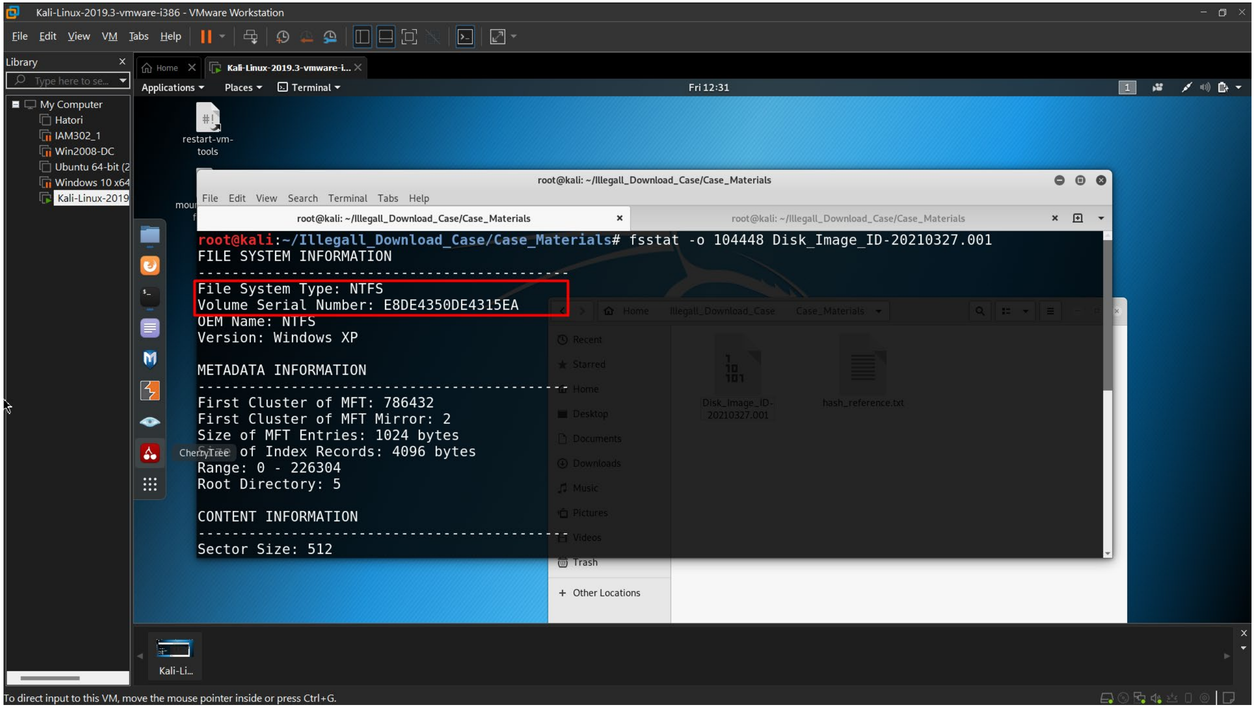
Volume offset #s (in sectors):

- Partition 1 – 2048
- Partition 2 – 104448
- Partition 3 – 61890560

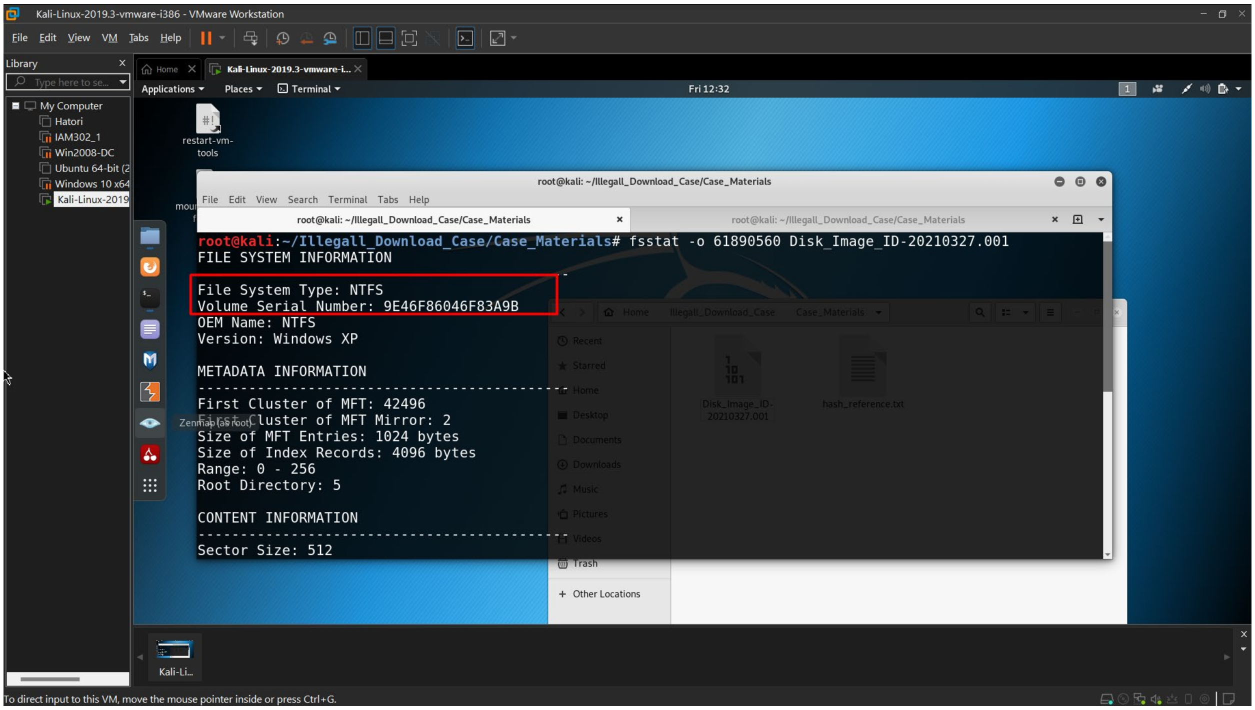
- How to get help for *fsstat*
- Use *fsstat* to get file system details.


Kali-Linux-2019.3-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Hatori
IAM302_1
Win2008-DC
Ubuntu 64-bit (2
Windows 10 x64
Kali-Linux-2019
Applications
Places
Terminal
Fri 12:30
restart-vm-tools
burpsuite
Disk_Image_ID-20210327.001
hash_reference.txt
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
root@kali:~/Illegall_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
--------------------------------------------
```


Kali-Linux-2019.3-vmware-i386 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Hatori
IAM302_1
Win2008-DC
Ubuntu 64-bit (2
Windows 10 x64
Kali-Linux-2019
Applications
Places
Terminal
Fri 12:31
restart-vm-tools
CherryTree
Disk_Image_ID-20210327.001
hash_reference.txt
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
root@kali:~/Illegall_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
```



```
root@kali:~/Illegall_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
```

<u>Partition 1</u>

File System: NTFS

Serial Number: 18EC42BBEC4292C4

<u>Partition 2</u>

File System: NTFS

Serial Number: E8DE4350DE4315EA

<u>Partition 3</u>

File System: NTFS

Serial Number: 9E46F86046F83A9B

- Using *fdisk* and *fsstat*, we obtained this information:

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

Please explain the parameters in the table ?

1. Flag: Indicates special attributes of the partition.

- For the 1st Partition, it is flagged as **Boot**, meaning it contains the boot loader necessary for starting the operating system.

2. Start and End: These columns indicate the starting and ending sector numbers for each partition on the disk.

- Start: The sector where the partition begins.

- End: The sector where the partition ends.

3. Sectors: This is the total number of sectors occupied by the partition. Each sector typically has a size of 512 bytes.

4. Size: The total size of the partition, calculated based on the number of sectors.

5. File System: This indicates the type of file system used on the partition.

- In the image, NTFS (New Technology File System) is used, which is commonly found on Windows systems.

6. Serial#: This is the unique identifier for each partition. The serial number is generated when the file system is created.