Lab 4: Disk Image and Partitions

What You Need for this lab

- Install Virtualbox : https://www.virtualbox.org/wiki/Downloads
- Install Kali 2021.4. : https://old.kali.org/kali-images/kali-2021.4/
  - Notes: Suggest You configure the disk size of Kali VM 80G because the size of each leakage cases image is 30G+
- Disk image :

1. **Verify the integrity of the disk image**
   - Create Lab Folder

```
File  Actions  Edit  View  Help
┌──(duanhn㉿duanhn)-[~]
└─$ mkdir Illegal_Download_Case

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

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

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

   - Download Case Materials

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

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

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

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

```
┌──(duanhn㉿duanhn)-[~/Illegal_Download_Case/Case_Materials]
└─$ wget -q https://www.dropbox.com/s/1fop1ooadb2yshu/Disk_Image_ID-2
0210327.001
```

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

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

```
duanhn@duanhn: ~/Illegal_Download_Case/Case_Materials
File  Actions  Edit  View  Help
  GNU nano 5.9                hash_reference.txt *

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

# MD5 and SHA1 for Disk Image
0adf1f182aab391d7042133bb55cf832  Disk_Image_ID-20210327.001
36186d7abc2ab6dfb783f0283e96566db8c0b31c  Disk_Image_ID-20210327.001

# MD5 and SHA1 for Memory Dump
eb741d12f5d4f57d4c1d5962bebb5771  Memory_Dump_ID-20210327.raw
59bfe8d81ce13cdc5a4ffe920adea39ec3257e87  Memory_Dump_ID-20210327.raw

# MD5 and SHA1 for Files Allegedly Download/Uploaded
f9d82438ed446e43cbd06adf74bc875b  Contraband.mp3
cce250d81a2397a4b347b78337219f078dc4e08  Contraband.mp3

b387e833b43b0d34cdcfda14511f6913d  Sample-1.mp3
23181f3d97a836106aae5db68b62b2bc3c44b1c8  Sample-1.mp3

^G Help      ^O Write Out  ^W Where Is  ^K Cut       ^T Execute
^X Exit      ^R Read File  ^\ Replace   ^U Paste     ^J Justify
```

– Install Necessary Software

  - ❑ Hashdeep
  - ❑ Md5deep

sudo apt install hashdeep

```
┌──(duanhn㉿duanhn)-[~]
└─$ sudo apt install hashdeep                                          1 ✗

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for duanhn:
Sorry, try again.
[sudo] password for duanhn:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
hashdeep is already the newest version (4.4-7).
hashdeep set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Step 2.

Make sure you are in the lab folder

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

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

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>*
- *sha1deep <disk image> -bewM <file that contains file names and hash codes>*
- 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.

```
┌──(duanhn㉿duanhn)-[~/Illegal_Download_Case]
└─$ md5deep Case_Materials/Disk_Image_ID-20210327.001 -bewM Case_Materials/ha
sh_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 4
md5deep: Case_Materials/hash_reference.txt: No hash found in line 6
md5deep: Case_Materials/hash_reference.txt: No hash found in line 7
md5deep: Case_Materials/hash_reference.txt: No hash found in line 8
md5deep: Case_Materials/hash_reference.txt: No hash found in line 9
md5deep: Case_Materials/hash_reference.txt: No hash found in line 10
md5deep: Case_Materials/hash_reference.txt: No hash found in line 11
md5deep: Case_Materials/hash_reference.txt: No hash found in line 12
md5deep: Case_Materials/hash_reference.txt: No hash found in line 14
md5deep: Case_Materials/hash_reference.txt: No hash found in line 15
md5deep: Case_Materials/hash_reference.txt: No hash found in line 16
md5deep: Case_Materials/hash_reference.txt: No hash found in line 17
0adf1f182aab391d7042133bb55cf832  Disk_Image_ID-20210327.001 matched Disk_Ima
ge_ID-20210327.001

┌──(duanhn㉿duanhn)-[~/Illegal_Download_Case]
```

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

```
┌──(duanhn㉿duanhn)-[~/Illegal_Download_Case]
└─$ sha1deep Case_Materials/Disk_Image_ID-20210327.001 -bewM Case_Materials/h
ash_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
sha1deep: Case_Materials/hash_reference.txt: No hash found in line 5
sha1deep: Case_Materials/hash_reference.txt: No hash found in line 7
sha1deep: Case_Materials/hash_reference.txt: No hash found in line 8
sha1deep: Case_Materials/hash_reference.txt: No hash found in line 9
sha1deep: Case_Materials/hash_reference.txt: No hash found in line 10
sha1deep: Case_Materials/hash_reference.txt: No hash found in line 11
sha1deep: Case_Materials/hash_reference.txt: No hash found in line 12
sha1deep: Case_Materials/hash_reference.txt: No hash found in line 13
sha1deep: Case_Materials/hash_reference.txt: No hash found in line 15
sha1deep: Case_Materials/hash_reference.txt: No hash found in line 16
36186d7abc2ab6dfb783f0283e96566db8c0b31c  Disk_Image_ID-20210327.001 matched
Disk_Image_ID-20210327.001

┌──(duanhn㉿duanhn)-[~/Illegal_Download_Case]
└─$                                                                    1 ✗
```

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

- How to get help for *fdisk*.

```
┌──(duanhn㉿duanhn)-[~/Illegal_Download_Case]
└─$ fdisk -h                                                          1 ✗

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
```

- Use *fdisk* to get the disk image's partition table.

```
┌──(ubalt㉿ kali-forensics)-[~/Illegal_Download_Case]
└─$ cd Case_Materials
                                        Change into the Case_Materials folder
┌──(ubalt㉿ kali-forensics)-[~/Illegal_Download_Case/Case_Materials]
└─$
                    Note: If you do not know where you are, this will tell you.
```

```
┌──(duanhn㉿duanhn)-[~/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/NT
Disk_Image_ID-20210327.001p2       104448 61890501 61786054 29.5G  7 HPFS/NT
Disk_Image_ID-20210327.001p3     61890560 62910463  1019904  498M 27 Hidden

┌──(duanhn㉿duanhn)-[~/Illegal_Download_Case/Case_Materials]
```

Volume offset #s (in sectors):

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

- How to get help for *fsstat*

```
┌──(duanhn㉿duanhn)-[~/Illegal_Download_Case/Case_Materials]
└─$ fsstat
Missing image name
usage: fsstat [-tvV] [-f fstype] [-i imgtype] [-b dev_sector_size] [-o imgoff
set] 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
```

- Use *fsstat* to get file system details.

```
┌──(duanhn㉿duanhn)-[~/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
```

```
┌──(duanhn㉿duanhn)-[~/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
--------------------------------------------
```

```
┌──(duanhn㉿duanhn)-[~/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
```

<u>Partition 1</u>

File System: -NTFS

Serial Number: - 18EC42BBEC4292C4

Partition 2

File System: -NTFS

Serial Number: E8DE4350DE4315EA

Partition 3

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 ?

- **Partition**: The number/order of the partition on the disk.
- **Flag**: Indicates if the partition is bootable (Boot) or not.
- **Start / End**: The starting and ending sectors of the partition.
- **Sectors**: Total number of sectors in the partition (End - Start + 1).
- **Size**: The actual size of the partition (Sectors × 512 bytes).
- **File System**: The file system type used (e.g., NTFS, FAT, hidden).
- **Serial #**: A unique identifier of the volume, useful in forensic verification.

YOU MUST SUBMIT A FULL-SCREEN IMAGE FOR FULL CREDIT!

Save the document with the filename "**YOUR NAME Lab 4.pdf**", replacing "YOUR NAME" with your real name.

Email the image to the instructor as an attachment to an e-mail message. Send it to: **xxx@fe.edu.vn** with a subject line of "**Lab 4 From YOUR NAME**", replacing "YOUR NAME" with your real name.