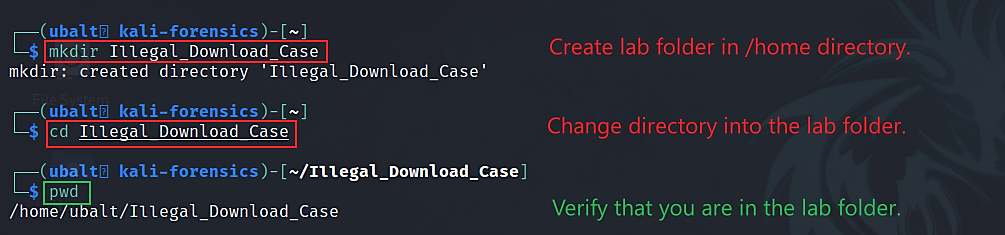
**Lab 4: Disk Image and Partitions**

**What You Need for this lab**

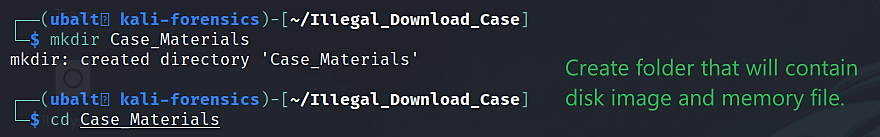
* + Install Virtualbox : <https://www.virtualbox.org/wiki/Downloads>
  + Install Kali 2021.4. : <https://old.kali.org/kali-images/kali-2021.4/>
    - Notes: Suggest You configure the disk size of Kali VM 80G because the size of each leakage cases image is 30G+
* Disk image : <https://www.dropbox.com/s/1fop1ooadb2yshu/Disk_Image_ID-20210327.001>

1. **Verify the integrity of the disk image**

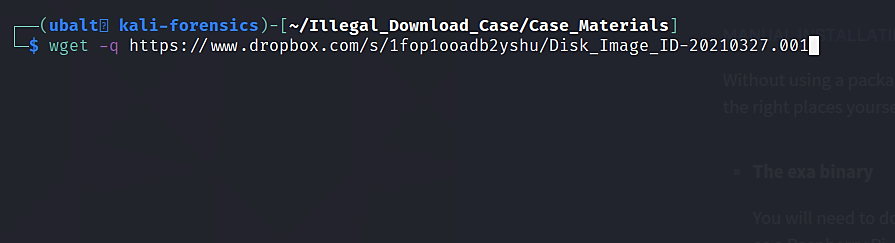
* Create Lab Folder

****

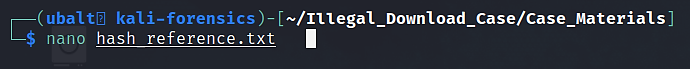
* Download Case Materials

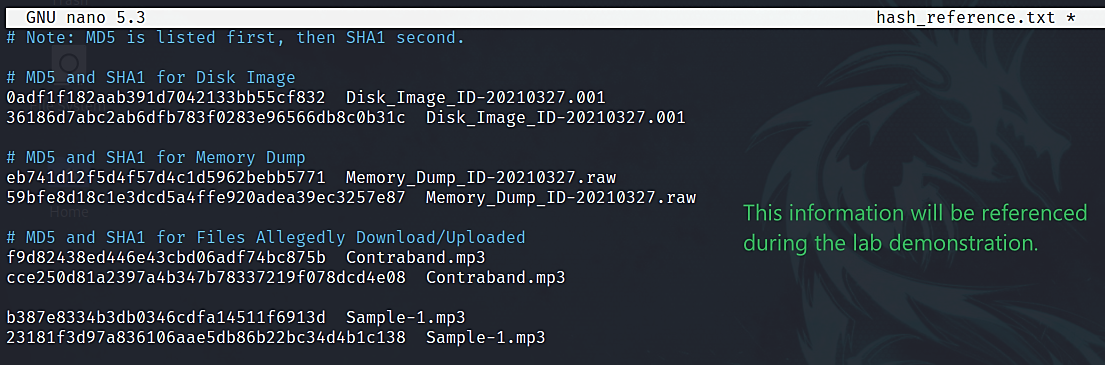
****

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



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



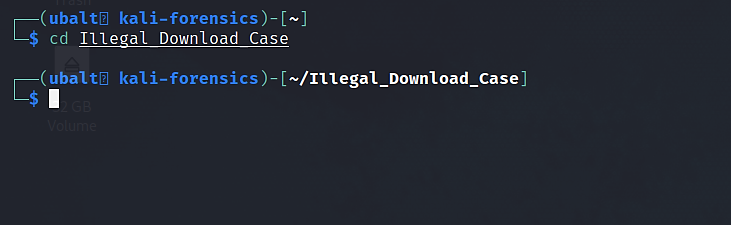


* Install Necessary Software
  + Hashdeep
  + Md5deep

sudo apt install hashdeep

**Step 2.**

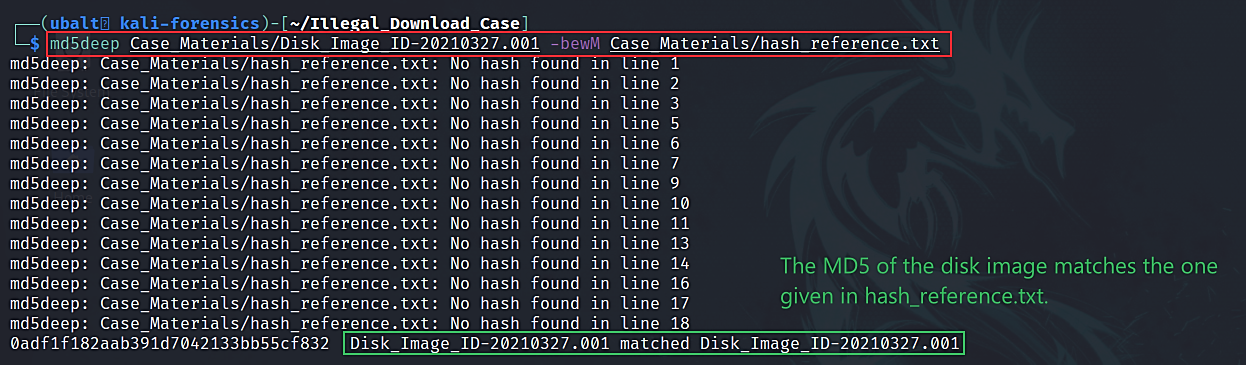
Make sure you are in the lab folder



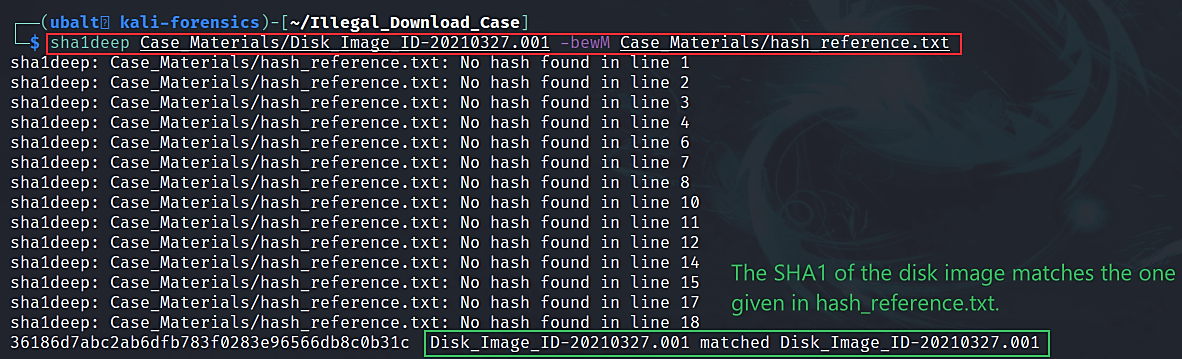
Generate an MD5 and SHA1 hash of the disk image. These tools will compare the MD5 and/or SHA1 hash of the disk image to the MD5 and/or SHA1 hash in the ‘*hash\_reference.txt*’ file.

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.

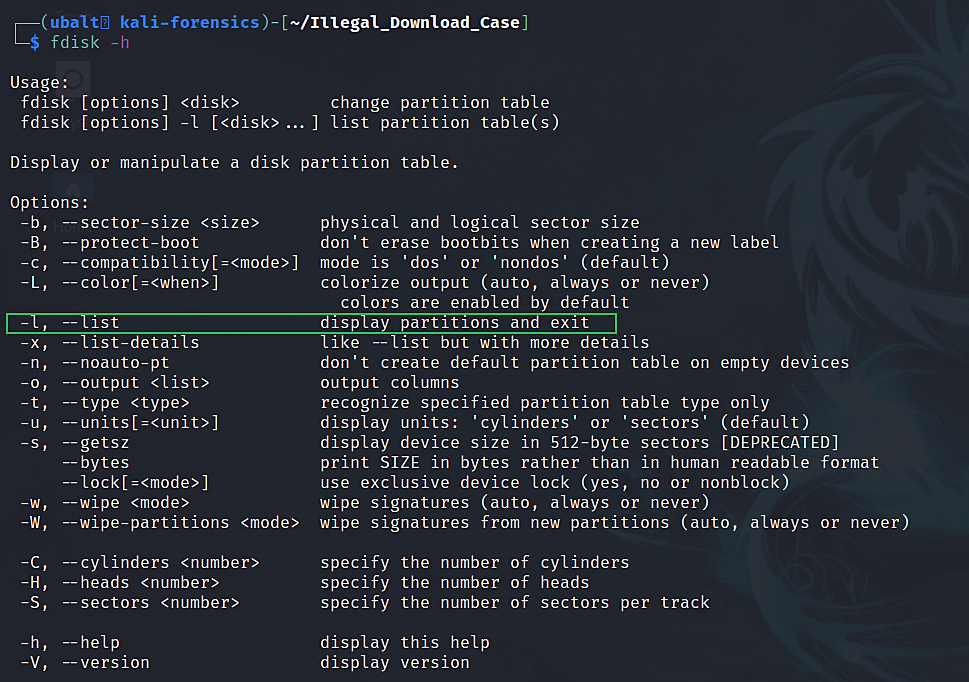


* Use SHA1deep to verify the MD5 hash of the disk image.

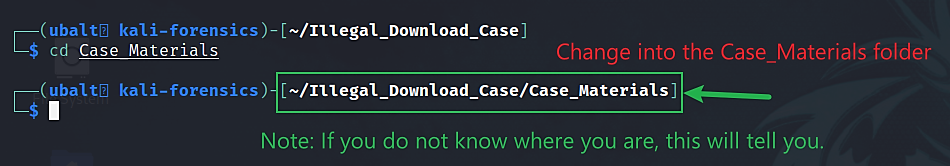


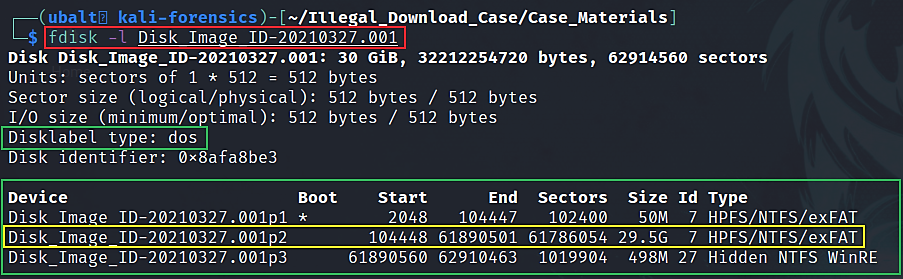
**2. Identify the OS of the system as well as its name, accounts, and partitions.**

* How to get help for *fdisk*.



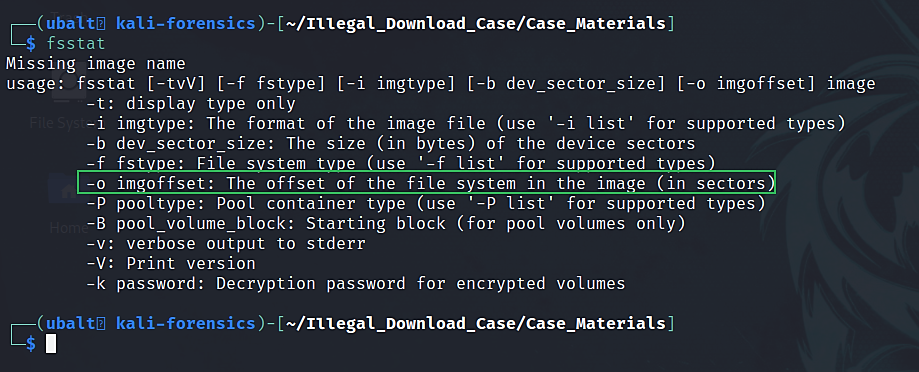
* Use *fdisk* to get the disk image’s partition table.



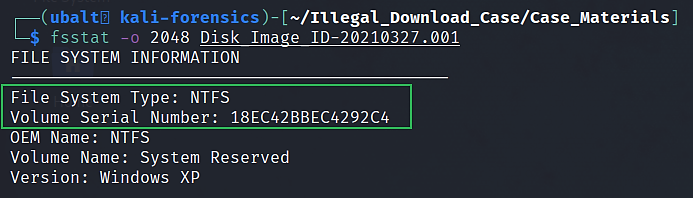


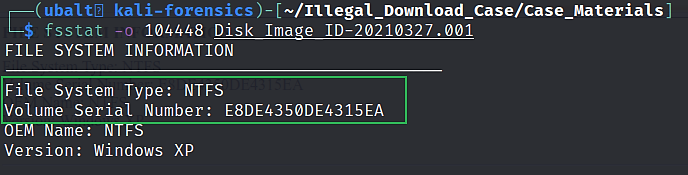
Volume offset #s (in sectors):

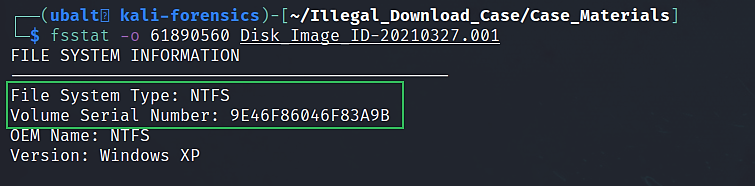
* Partition 1 – 2048
* Partition 2 – 104448
* Partition 3 – 61890560
* How to get help for *fsstat*



* Use *fsstat* to get file system details.







Partition 1

File System: ?

Serial Number: ?

Partition 2

File System: ?

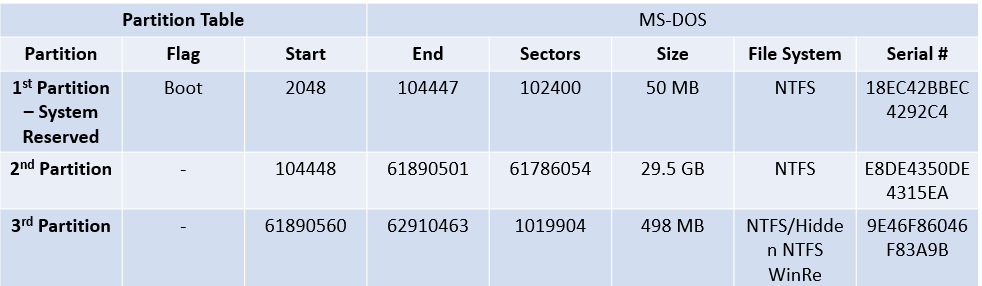
Serial Number: ?

Partition 3

File System: ?

Serial Number: ?

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



Please explain the parameters in the table ?

**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.