Lab 5: Examining the Registry

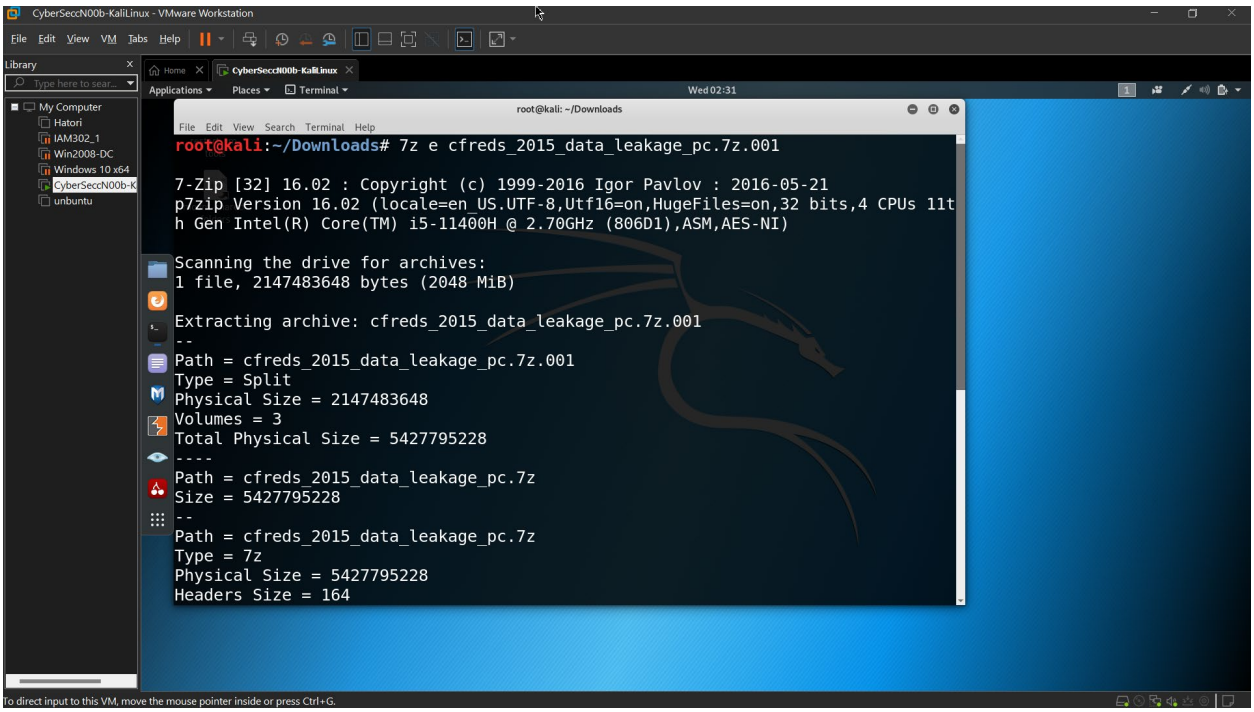
Group: CyberSec_N00b

Member:

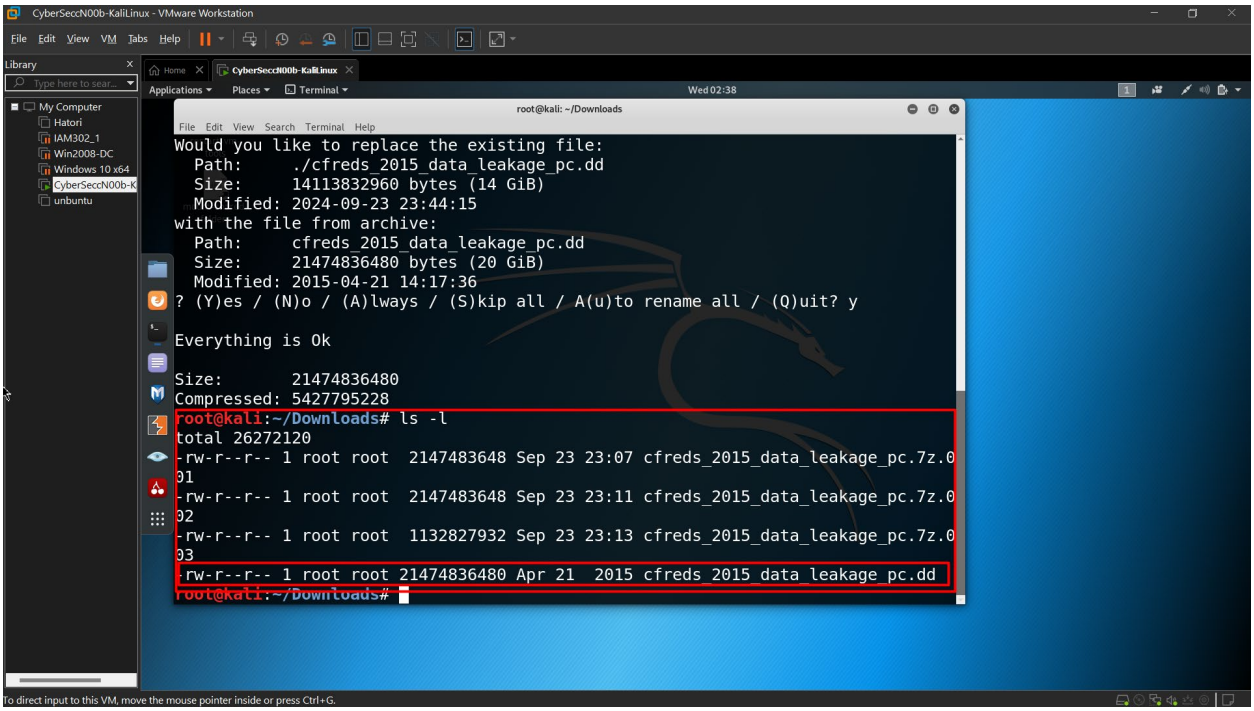
- *Huỳnh Ngọc Quang (SE181838)*
- *Hồ Tài Liên Vy Kha (SE181818)*
- *Hoàng Kim Long (DE180860)*
- *Phạm Thành Long (SE181692)*
- *Nguyễn Lê Hoàng Thông (SE182533)*

Step 1.

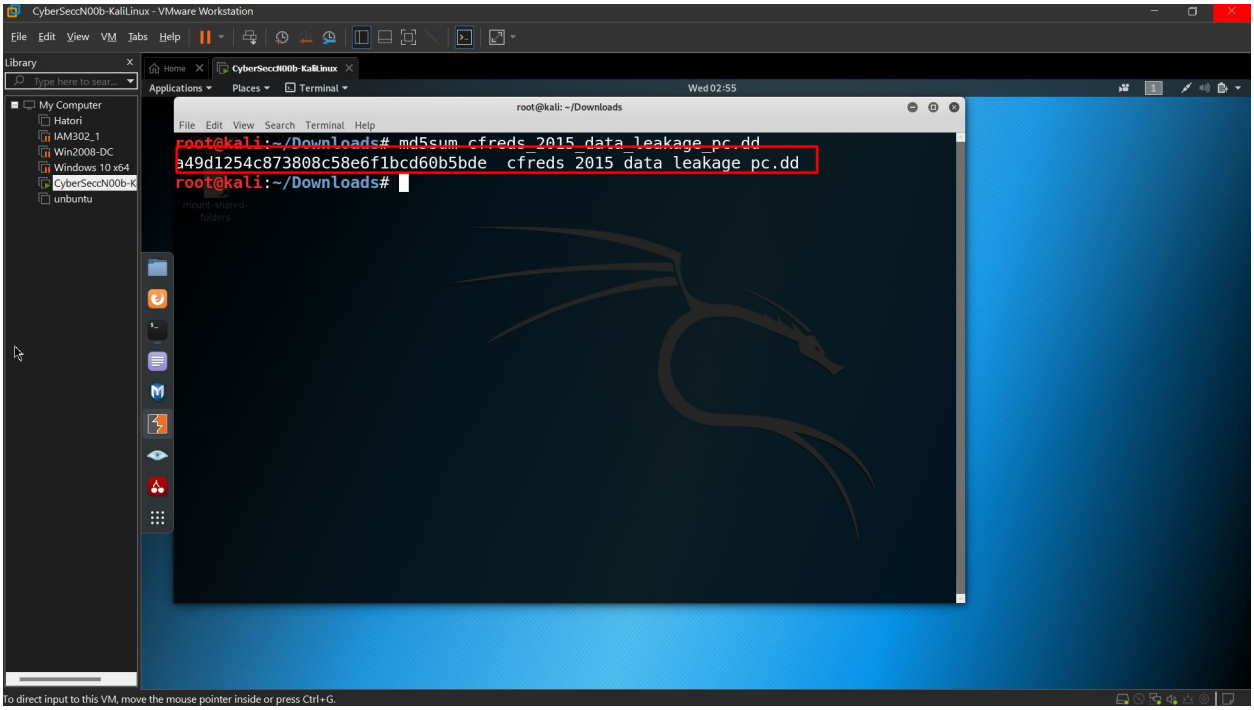
Unzipped the DD image



Verify the unzipped DD image

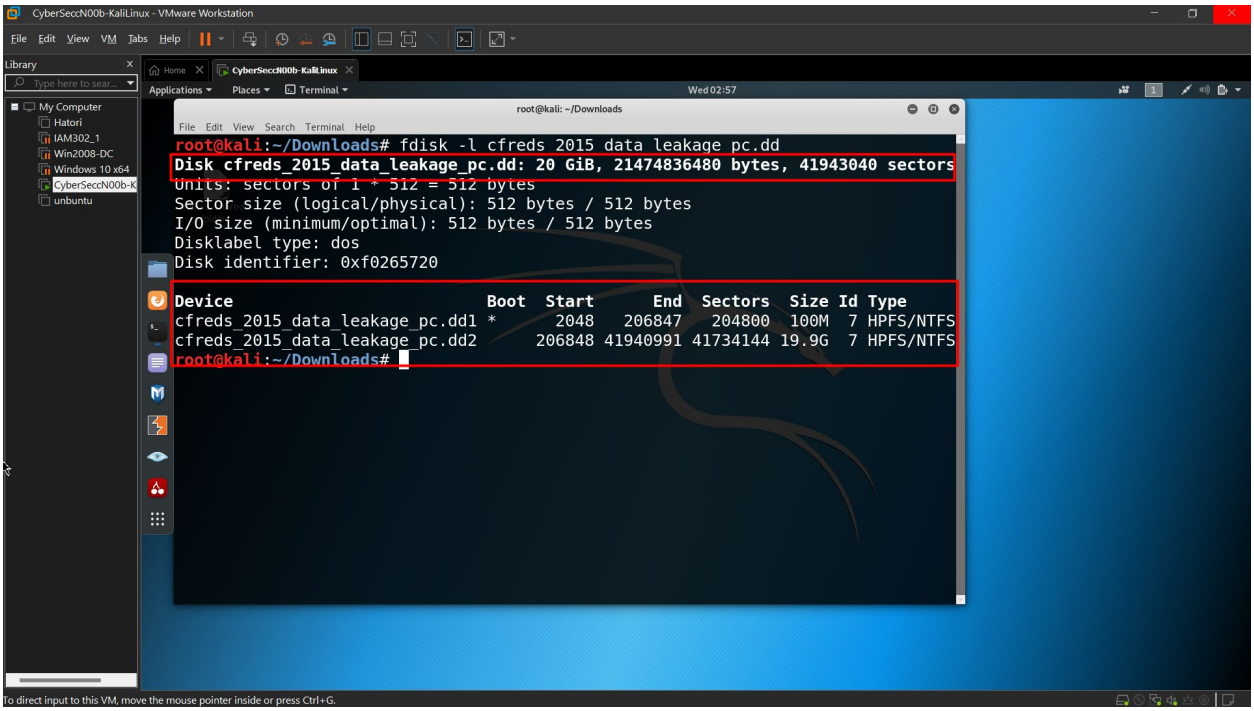


Verify the unzipped DD image with MD5

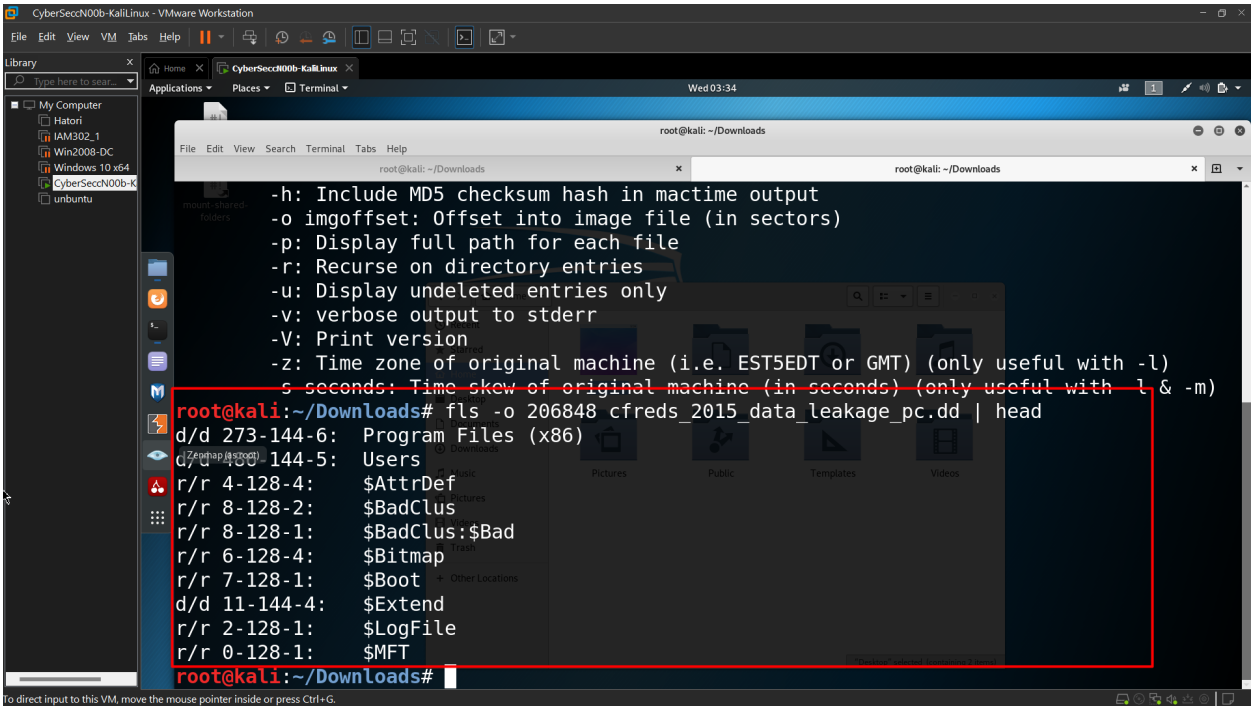


Step 2.

Exam partitions of the DD image using *fdisk*



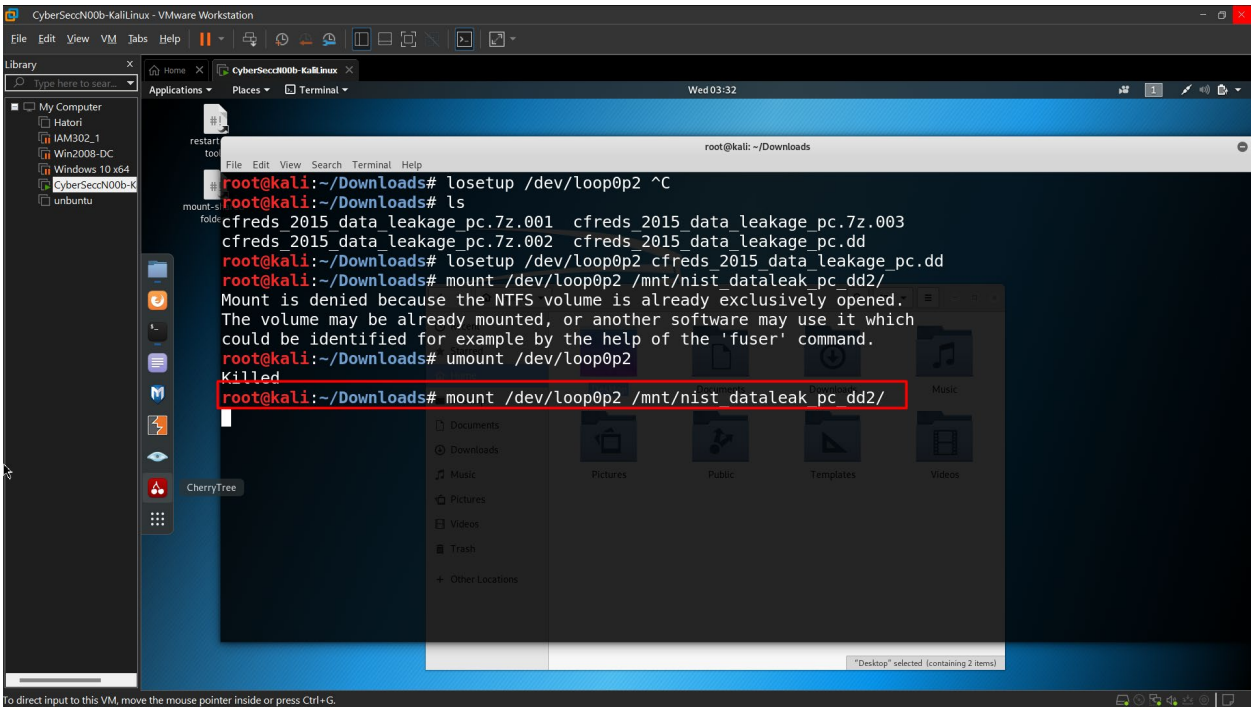
List file/directory names of the system volume



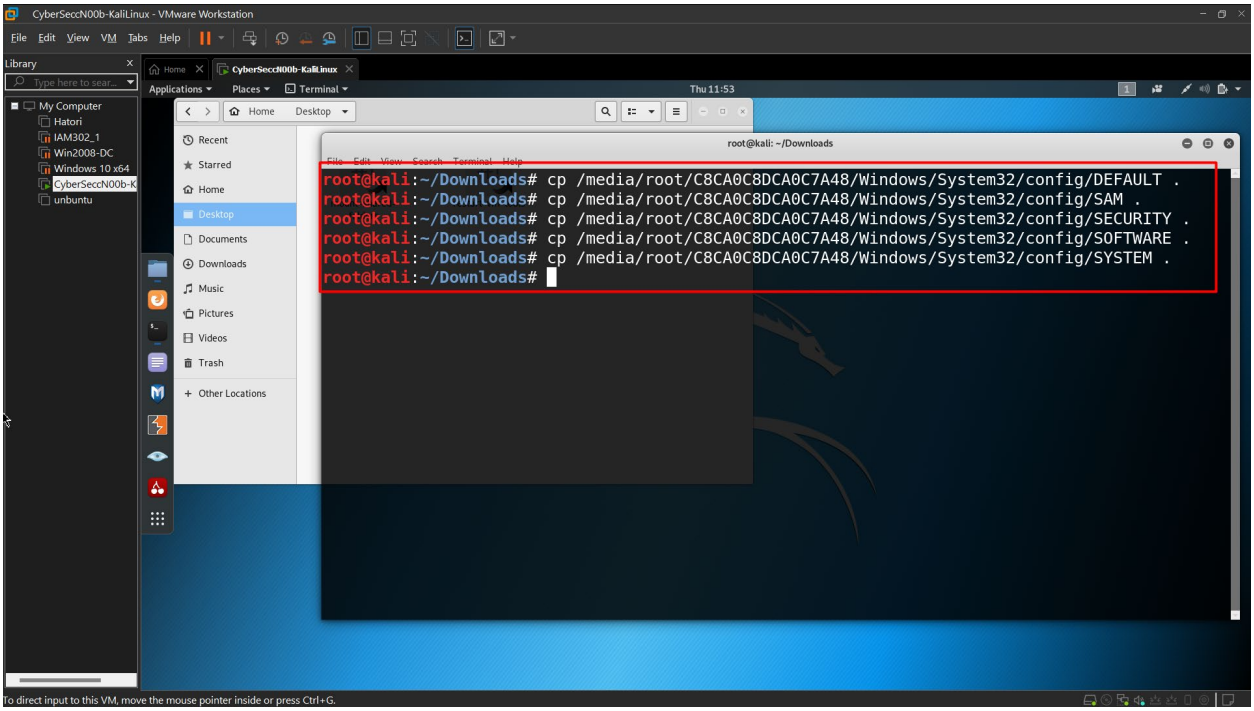
If your VM doesn't support auto-mounting

Create a folder as the mount point

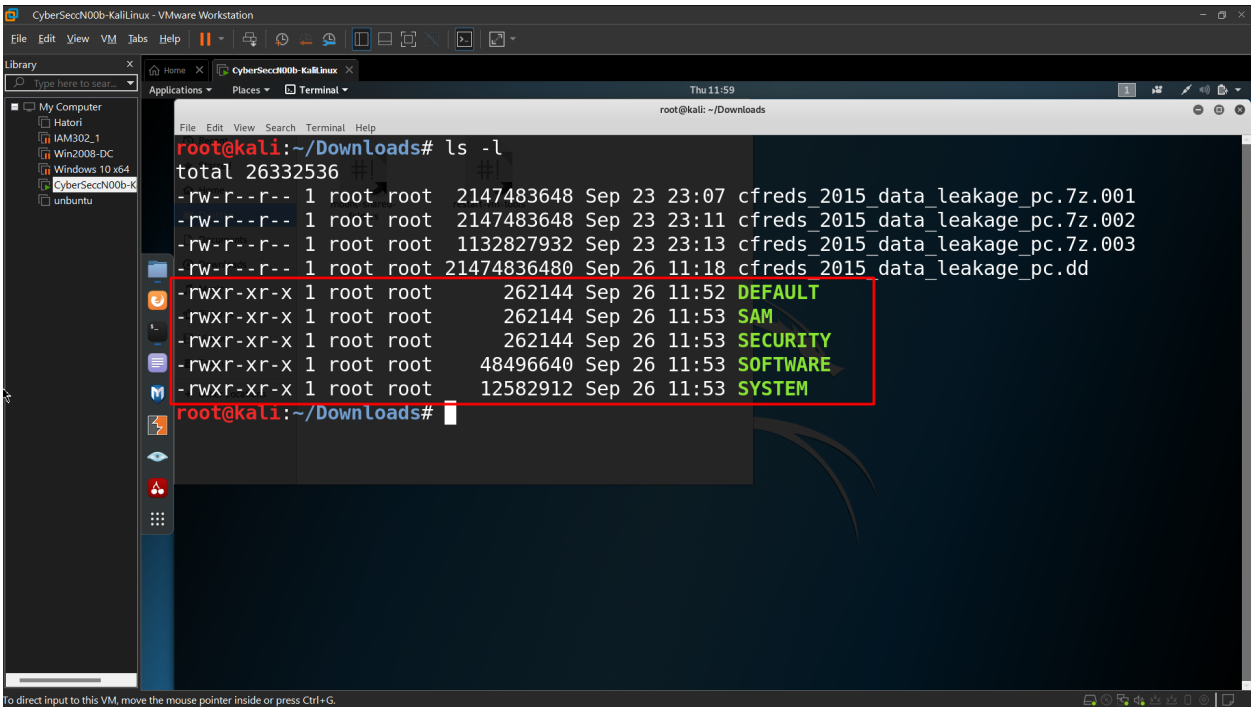
Mount partition 2 to the mounting point



Copy HKEY_LOCAL_MACHINE (Hive) files to \lab

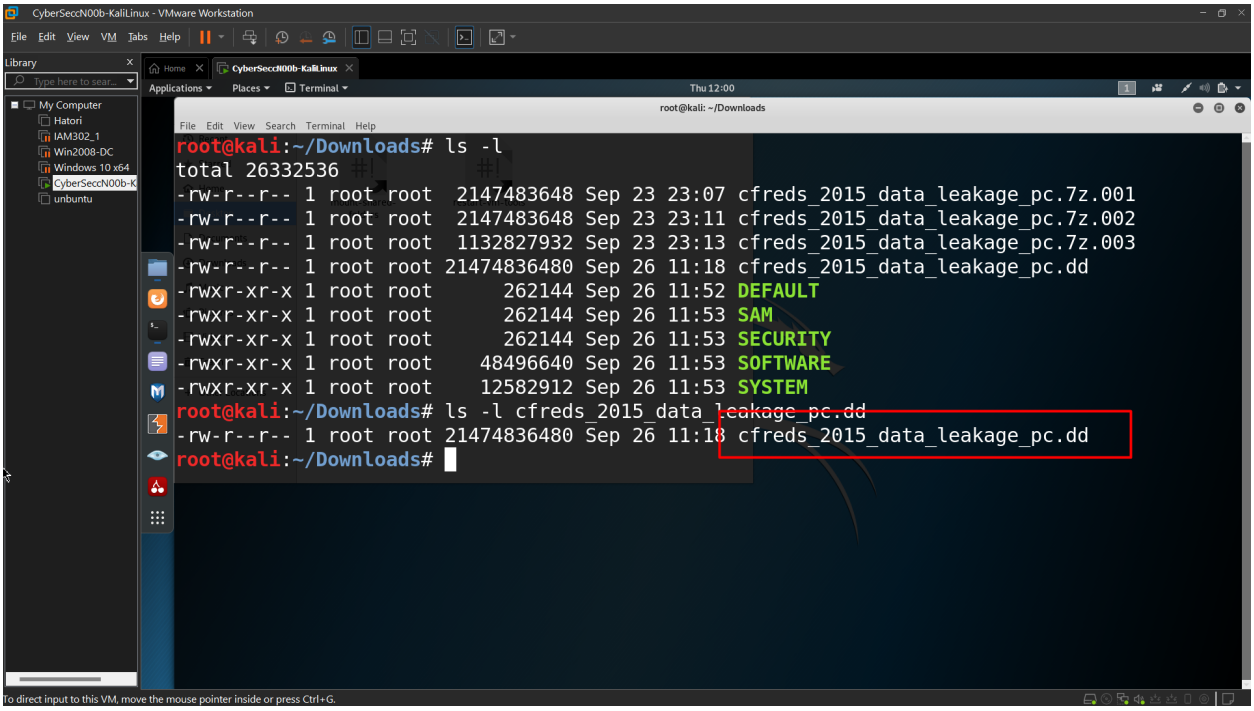


Verify five files

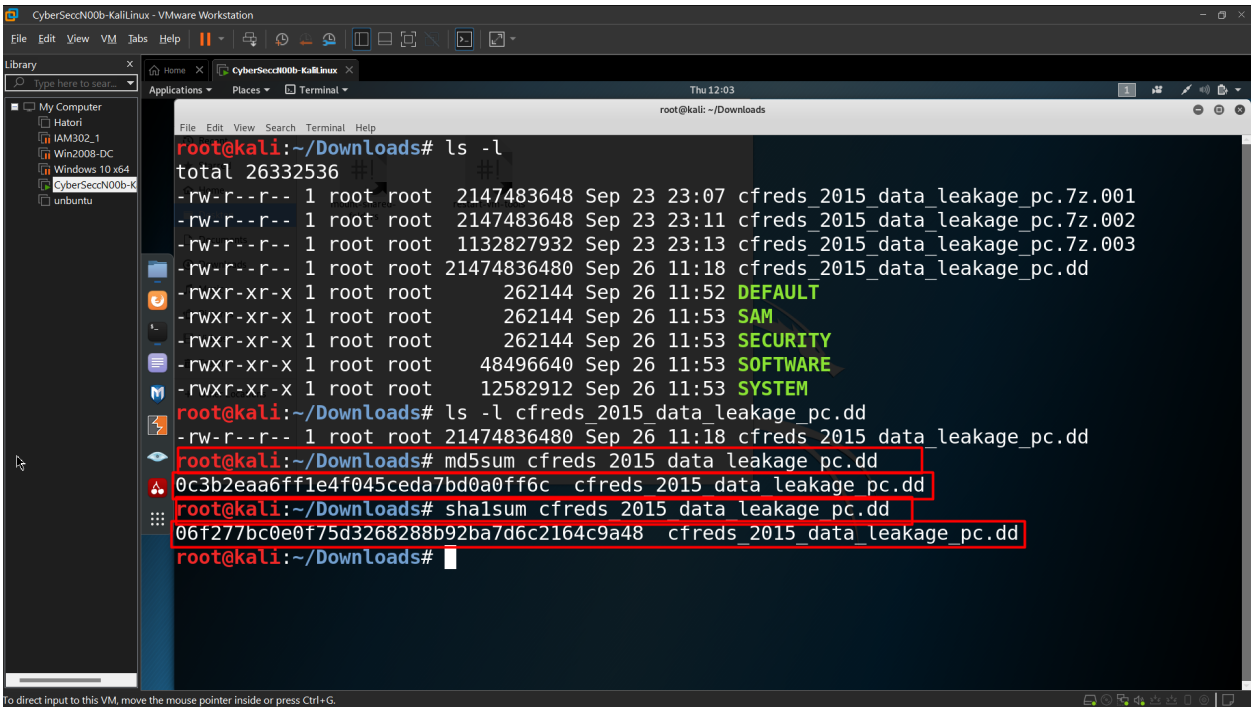


Step 3.

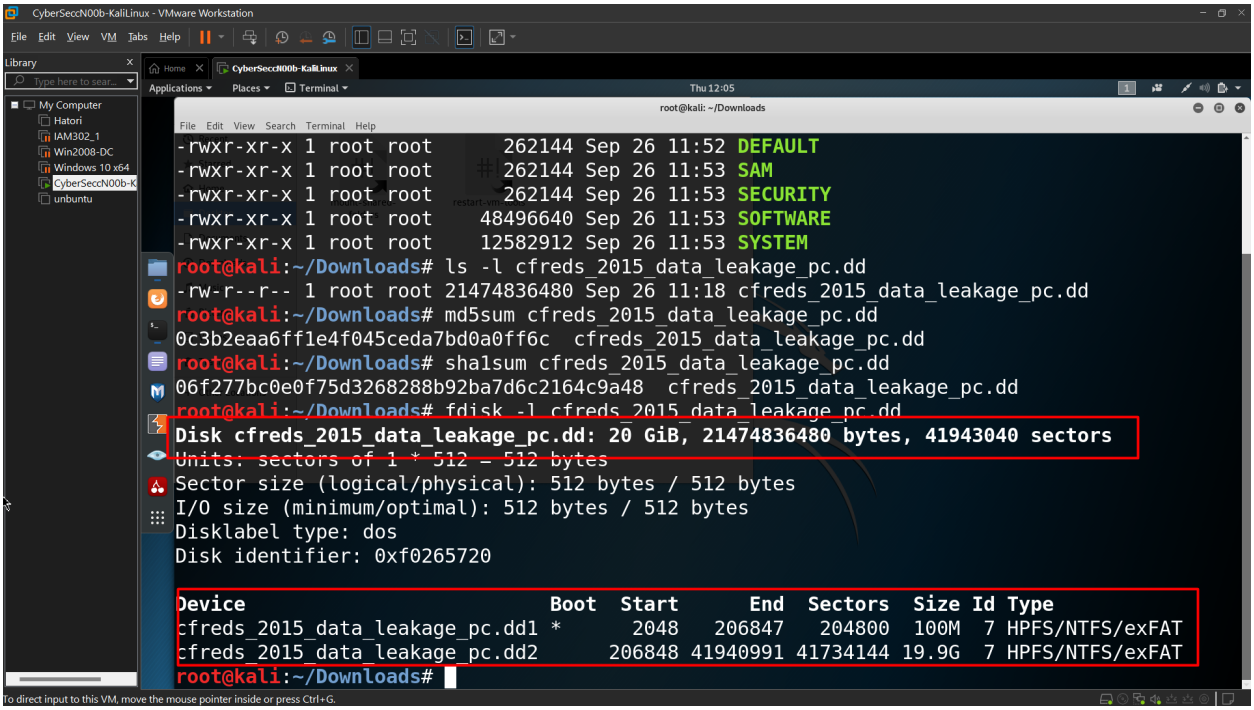
Verify you have the dd image



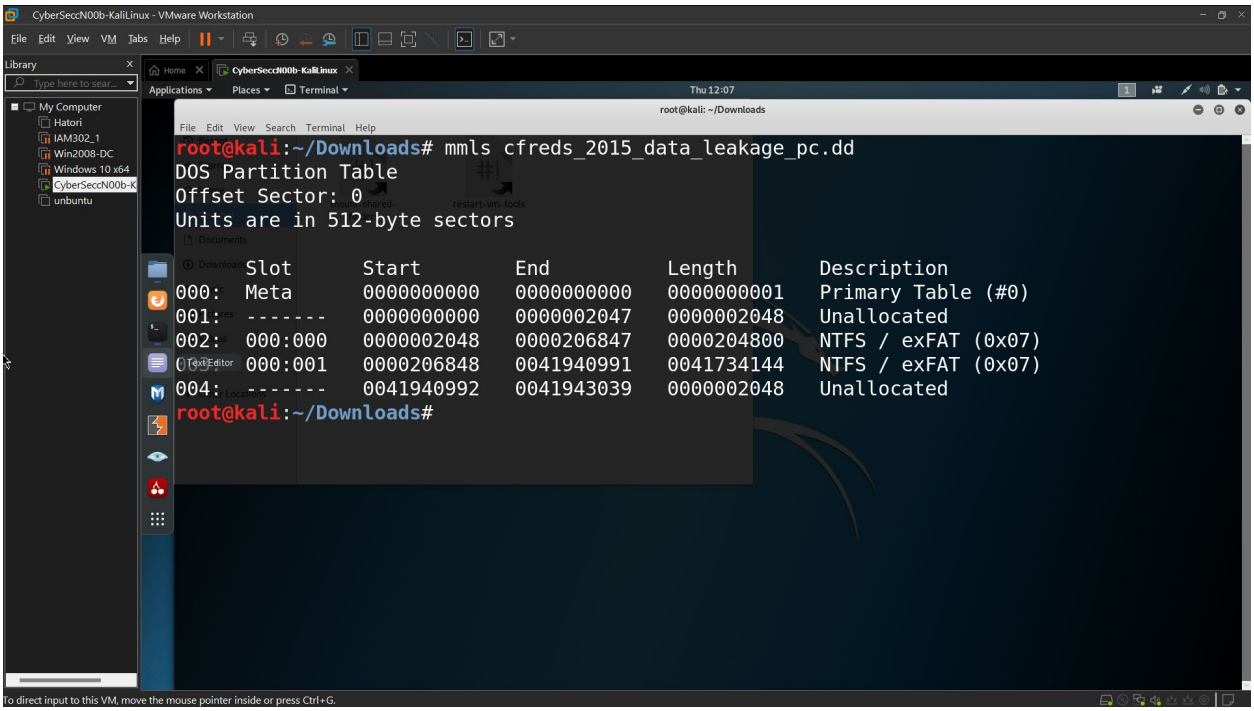
Compute MD5 and SHA1 of the DD image



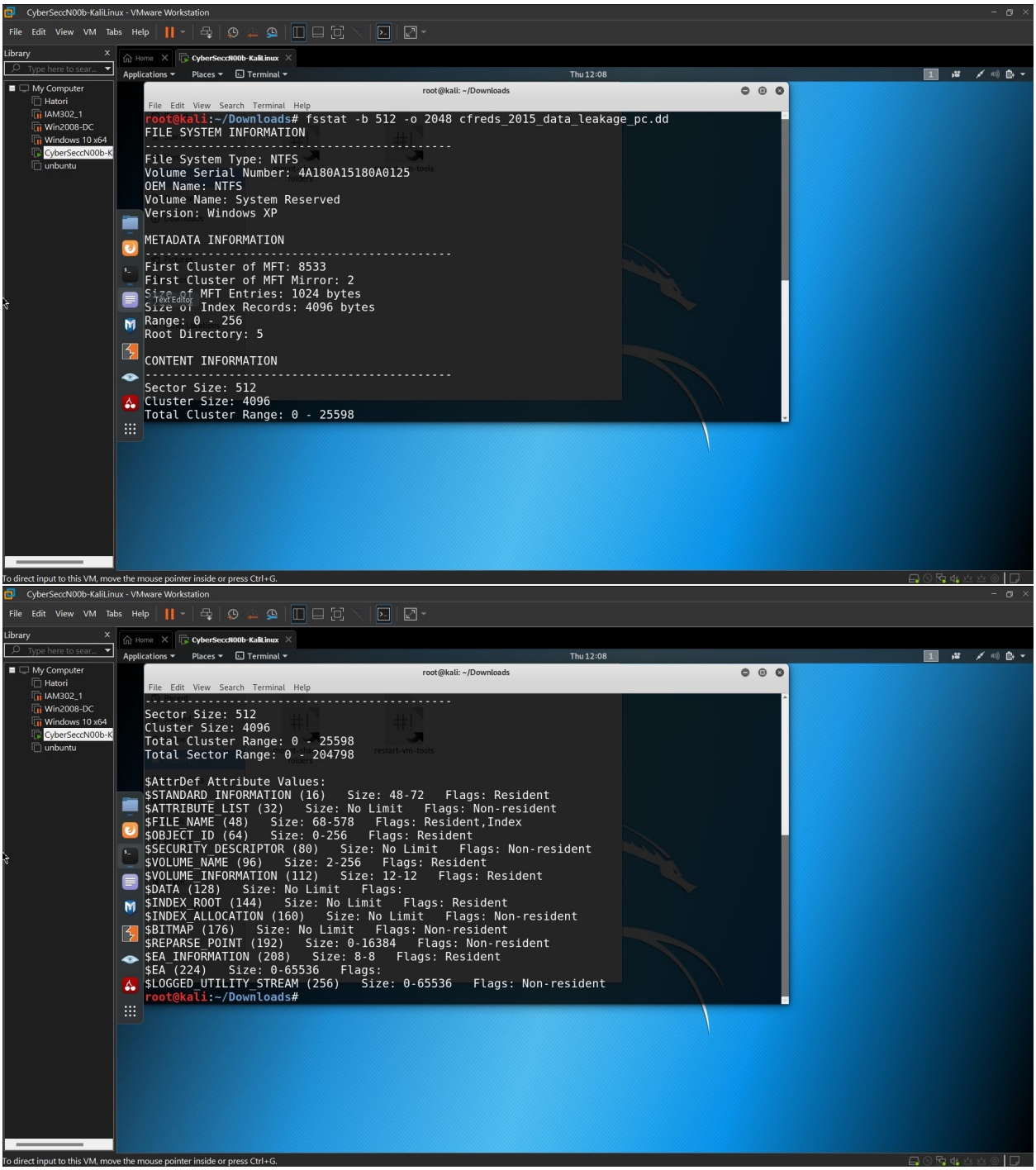
Show partitions of the image



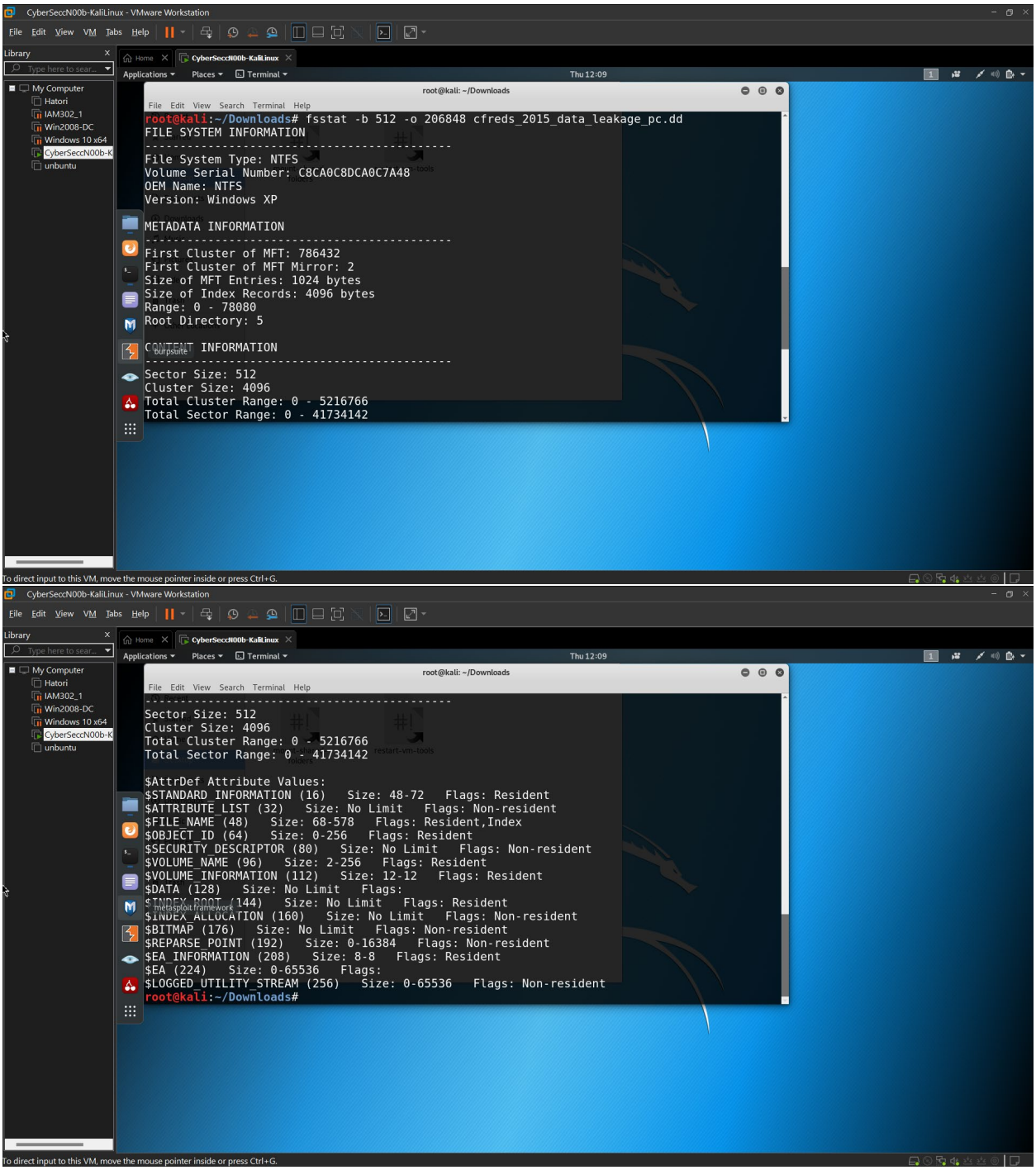
Show partitions and unallocated space using *mmls*



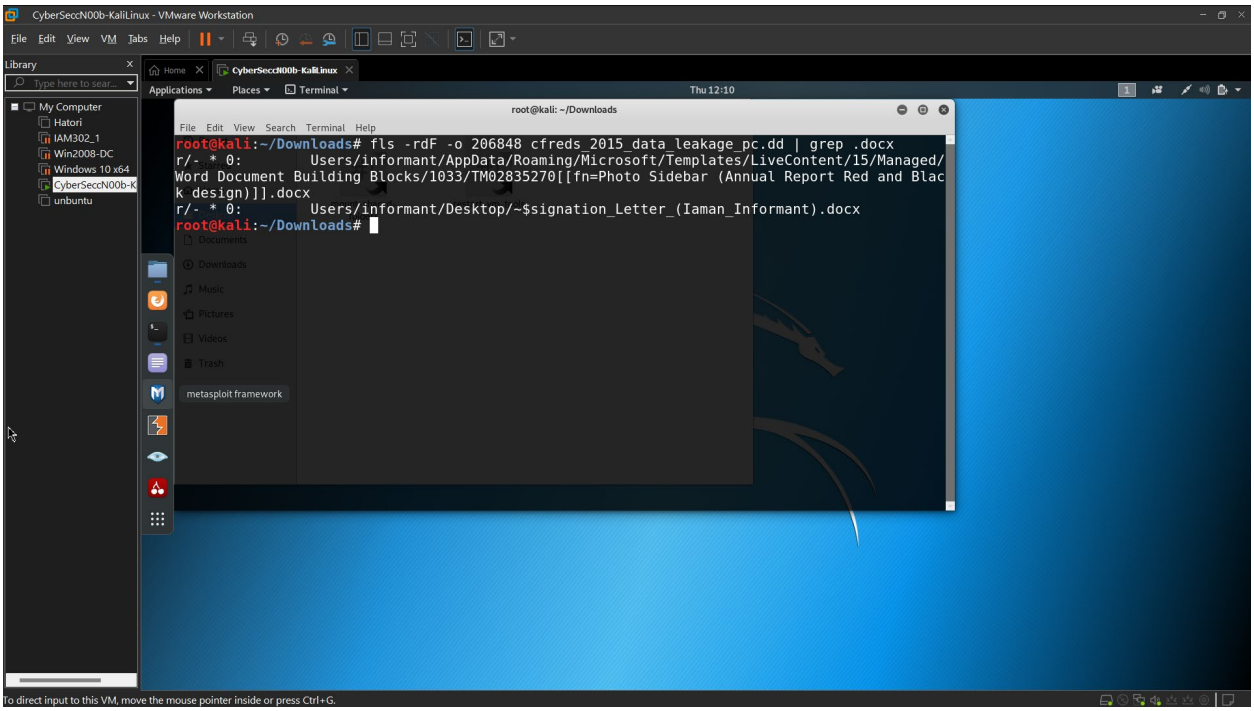
Display file system statistics and metadata information from a disk image (first partition)



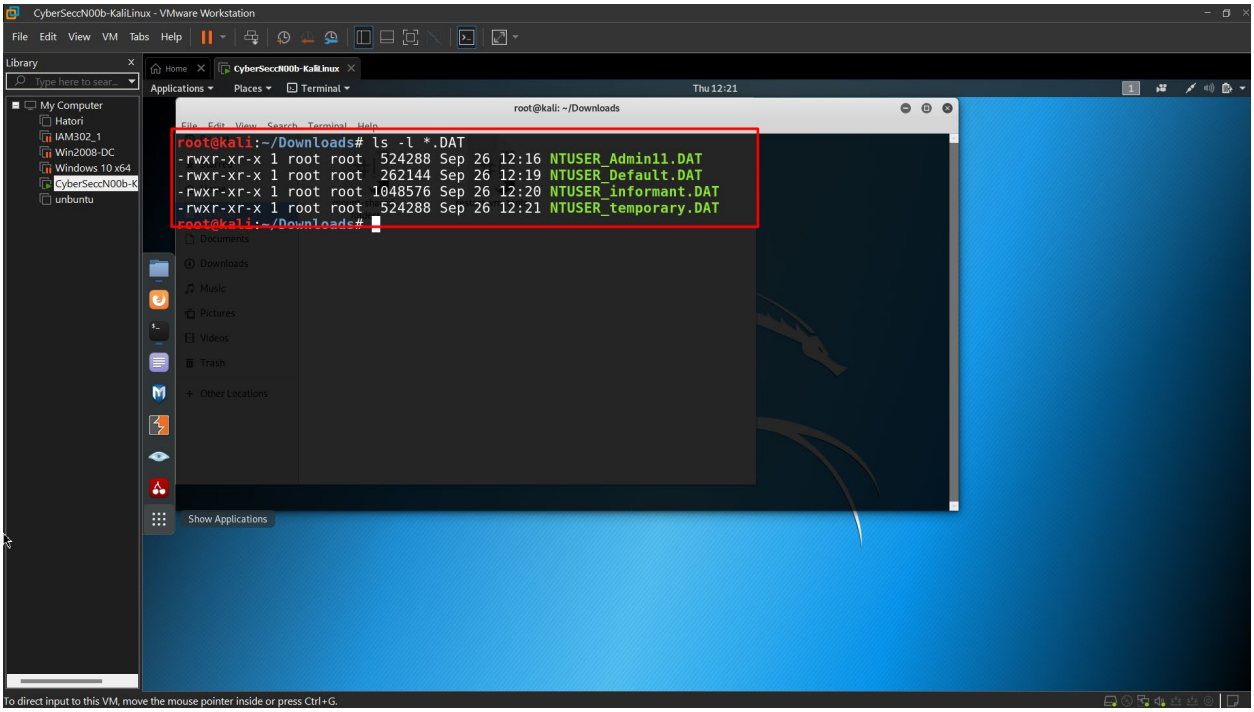
List the second partition details



List all deleted *.docx* files in the whole partition?



Verify Users' information



What is the installed OS information in detail?