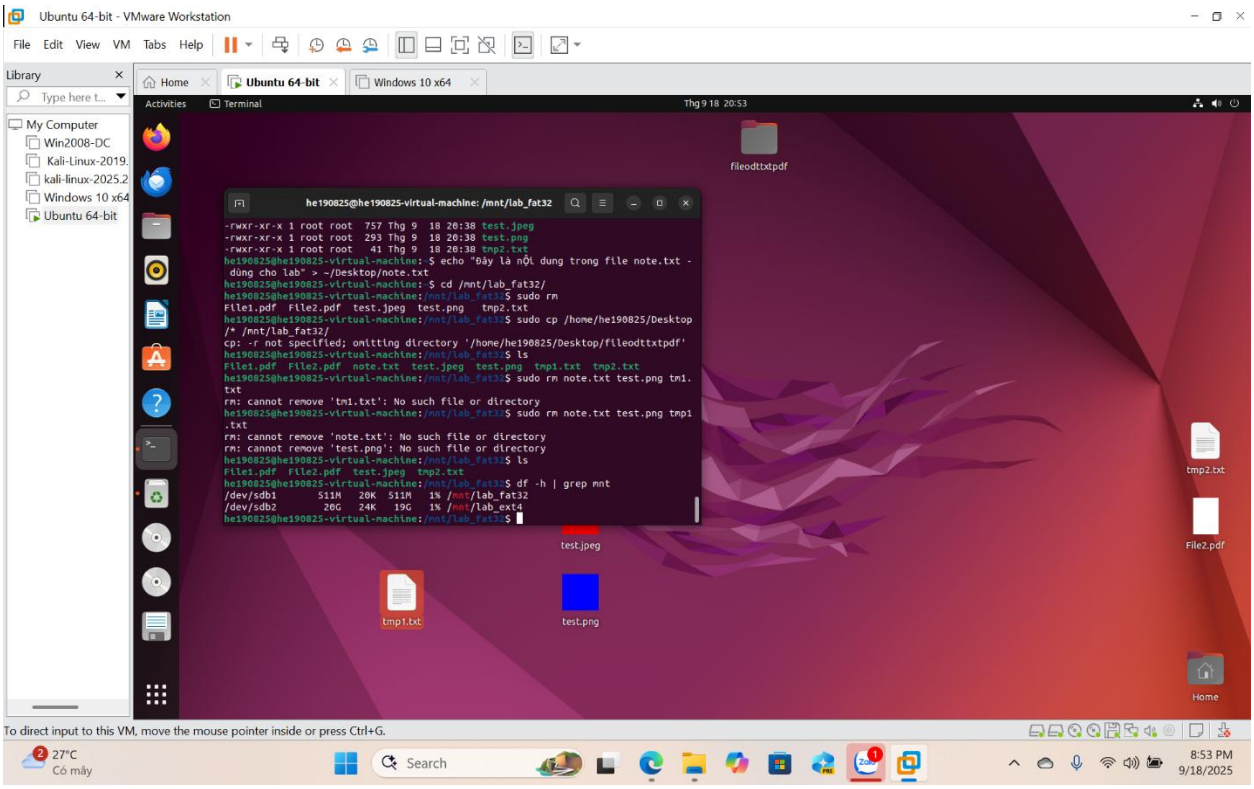
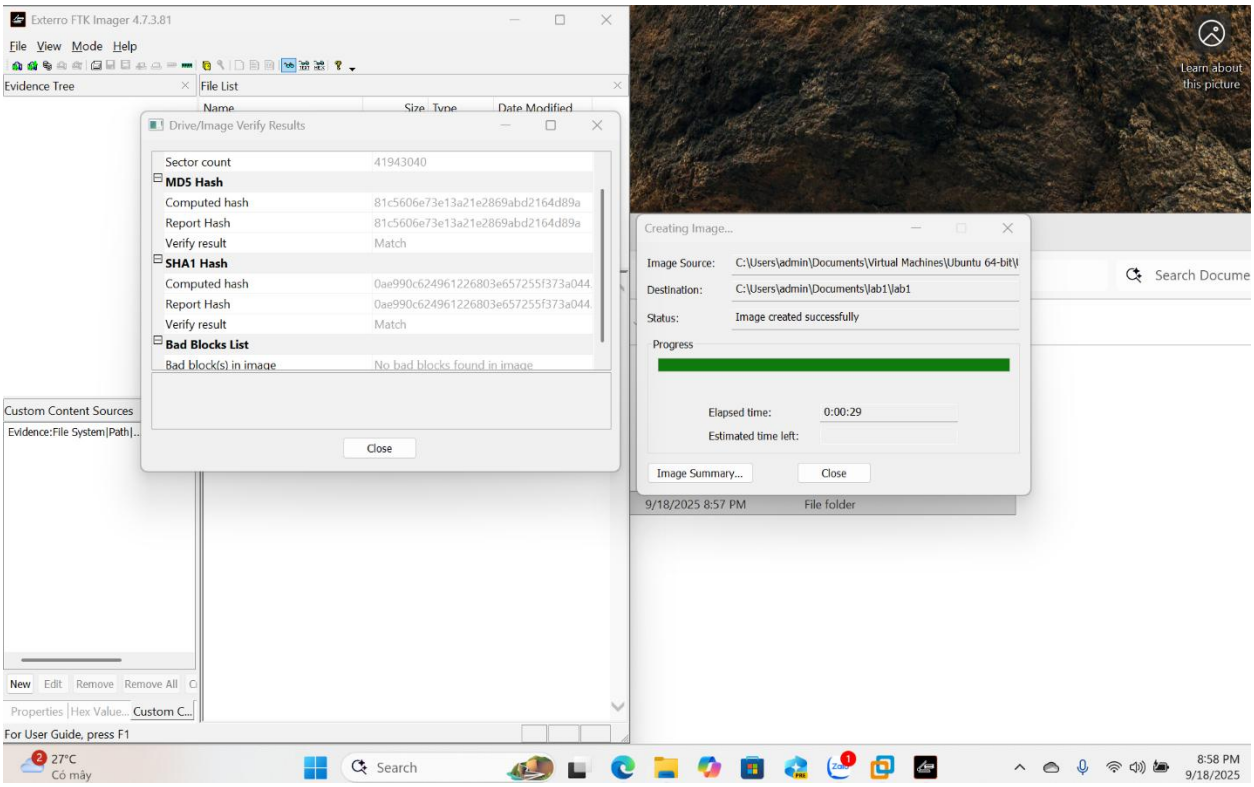
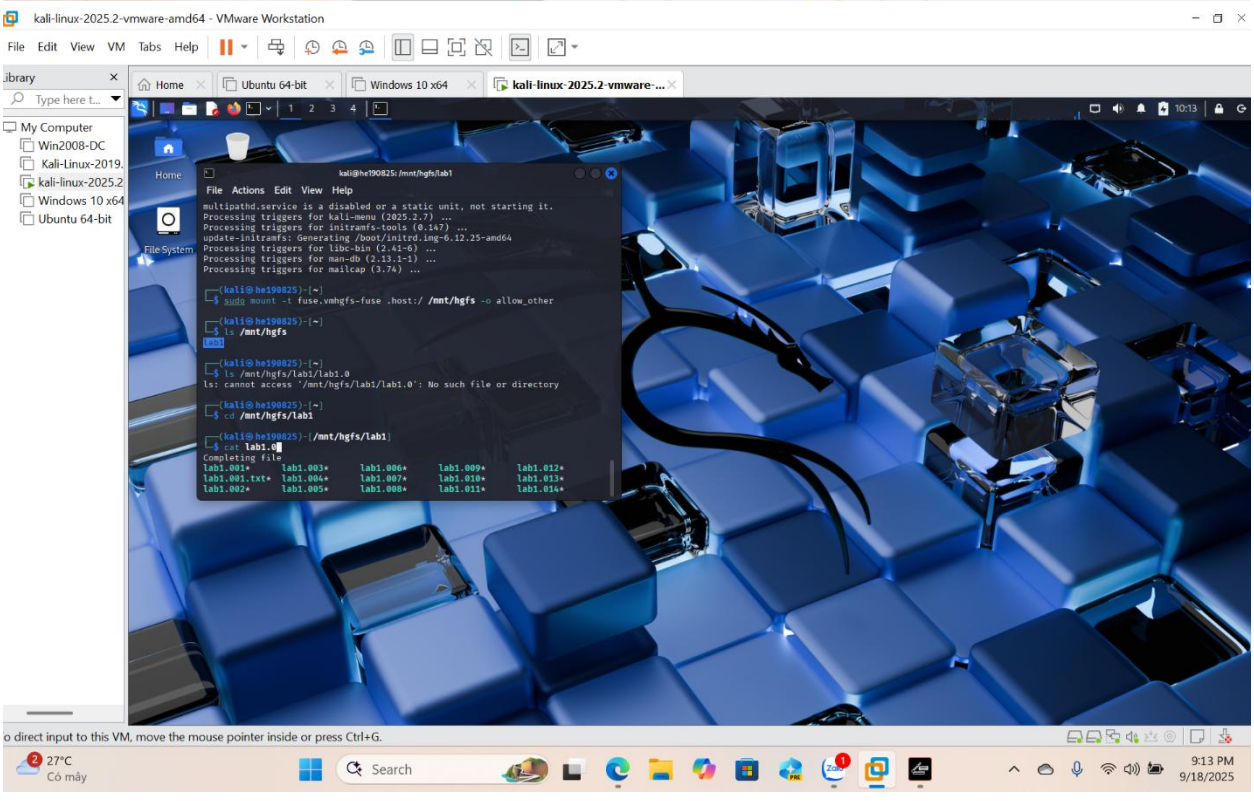
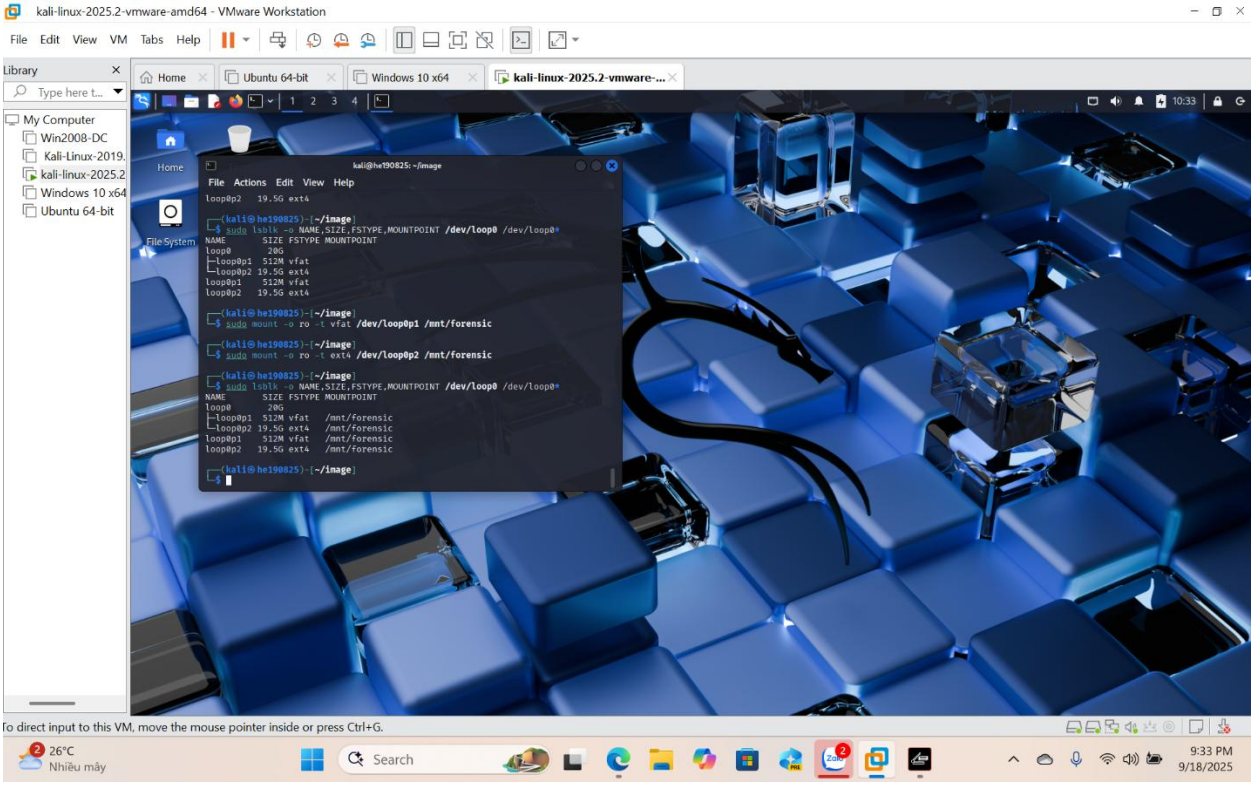
BÁO CÁO LAB 1 FORENSIC

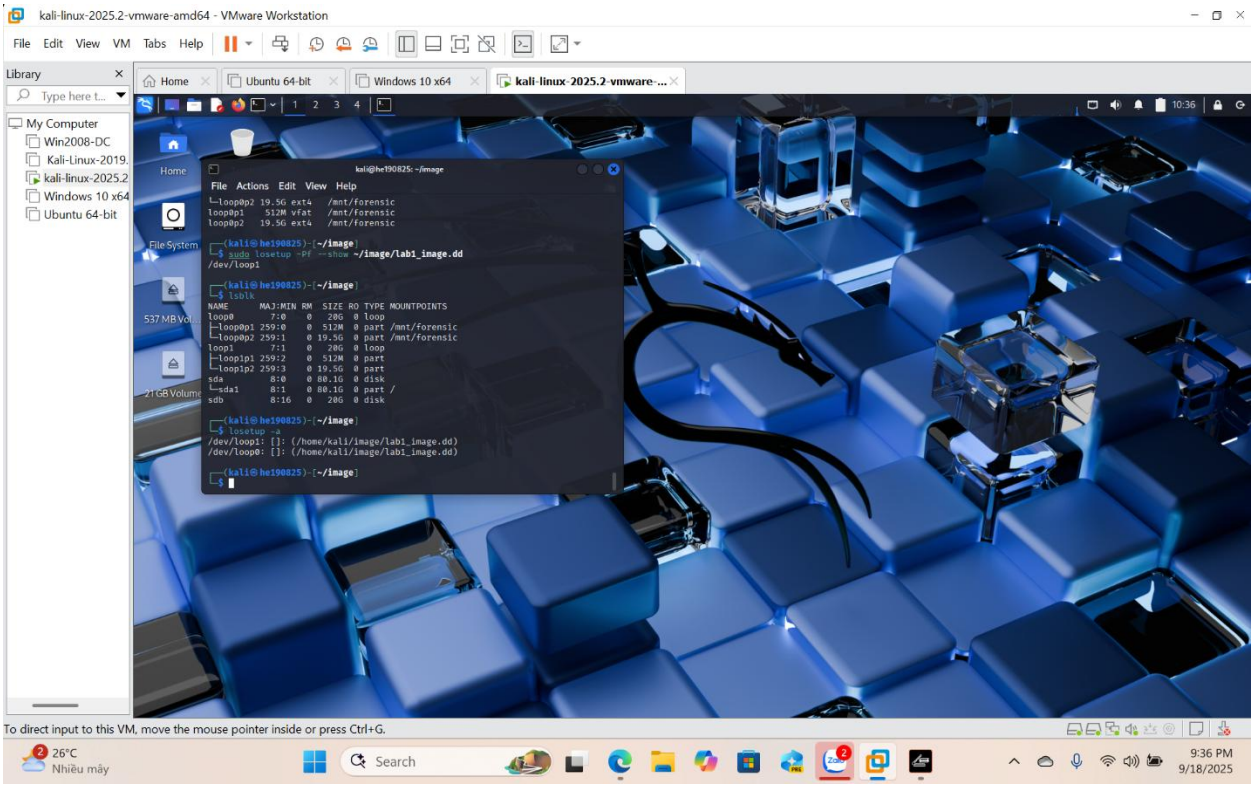
Họ và tên: Hoàng Đình Lâm
MSSV: HE190825
Lớp IA1905

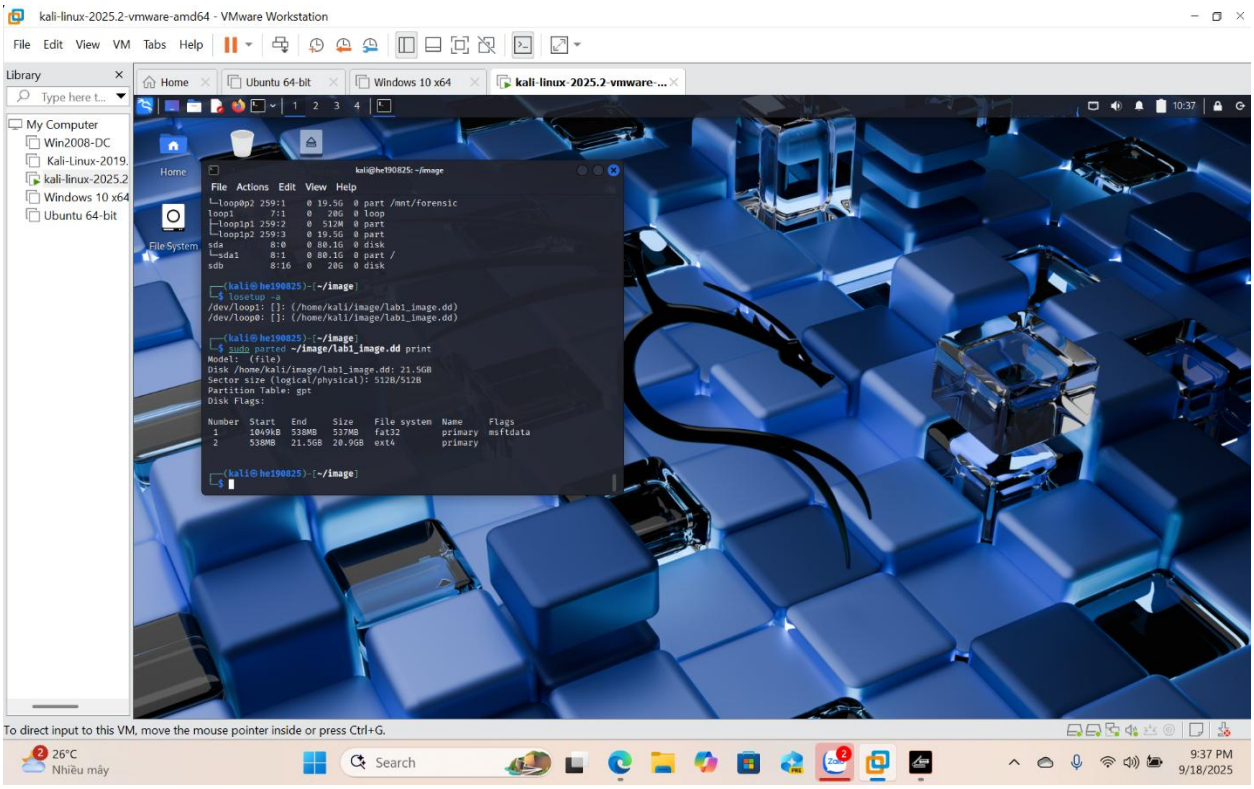


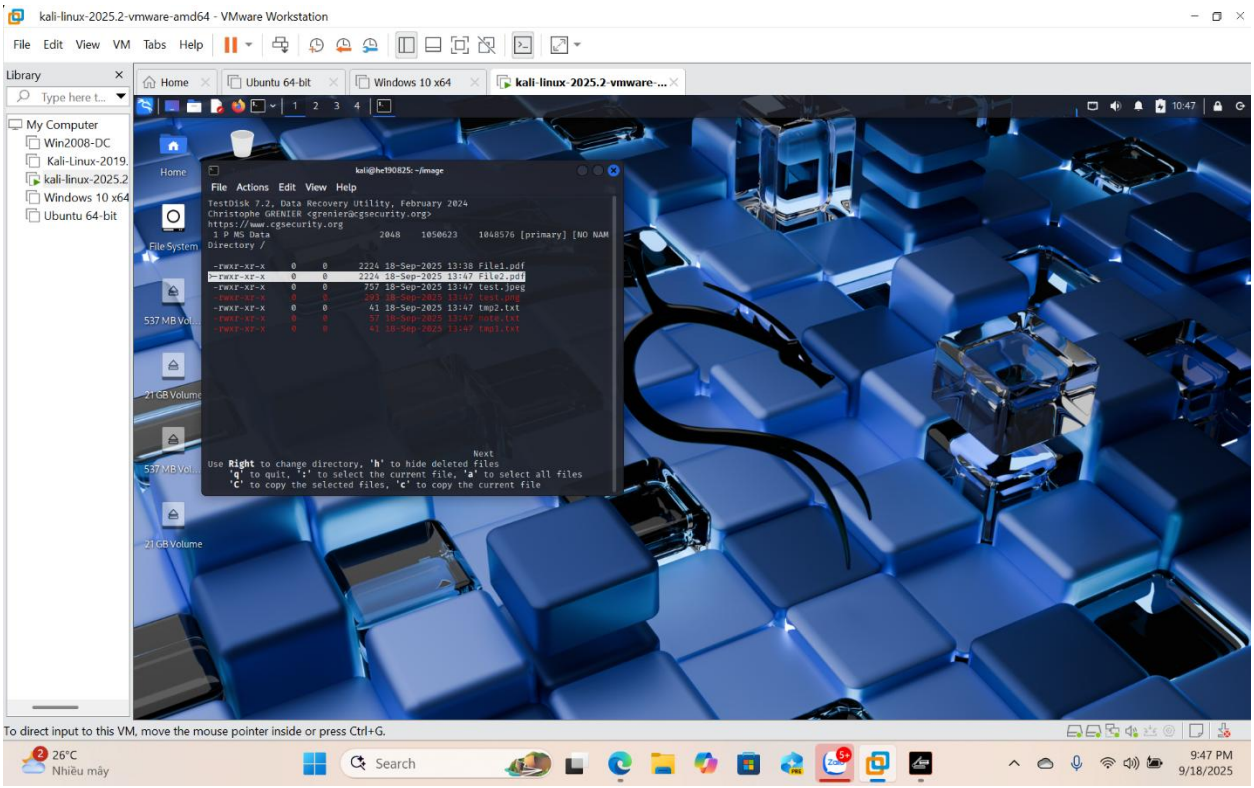

Exterro FTK Imager 4.7.3.81
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Drive/Image Verify Results
Sector count 41943040
MD5 Hash
Computed hash 81c5606e73e13a21e2869abd2164d89a
Report Hash 81c5606e73e13a21e2869abd2164d89a
Verify result Match
SHA1 Hash
Computed hash 0ae990c624961226803e657255f373a044
Report Hash 0ae990c624961226803e657255f373a044
Verify result Match
Bad Blocks List
Bad block(s) in image No bad blocks found in image
Close
Learn about this picture
Creating Image...
Image Source: C:\Users\admin\Documents\Virtual Machines\Ubuntu 64-bit\
Destination: C:\Users\admin\Documents\lab1\lab1
Status: Image created successfully
Progress
Elapsed time: 0:00:29
Estimated time left:
Image Summary...
Close
Search Docume
9/18/2025 8:57 PM File folder
Custom Content Sources
Evidence:File System|Path|...
New Edit Remove Remove All
Properties Hex Value... Custom C...
For User Guide, press F1
27°C Có mây
Search
8:58 PM 9/18/2025

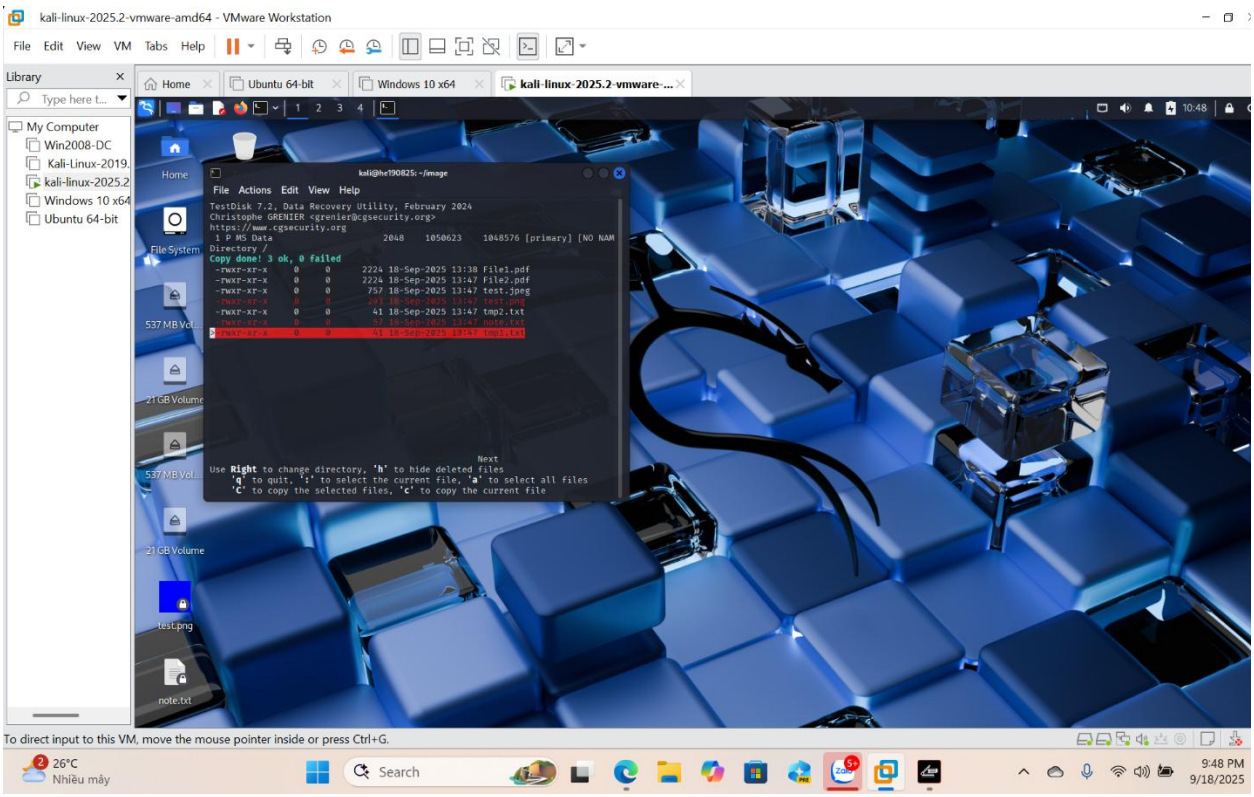

kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Win2008-DC
Kali-Linux-2019.
kali-linux-2025.2
Windows 10 x64
Ubuntu 64-bit
Home
Ubuntu 64-bit
Windows 10 x64
kali-linux-2025.2-vmware-...
kali@he190825: /mnt/hgfs/lab1
File Actions Edit View Help
multipathd.service is a disabled or a static unit, not starting it.
Processing triggers for kali-menu (2025.2.7) ...
Processing triggers for initramfs-tools (0.147) ...
update-initramfs: Generating /boot/initrd.img-6.12.25-amd64
Processing triggers for libc-bin (2.42-6) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for mailcap (3.74) ...
sudo mount -t fuse.vmhgfs-fuse .host:/ /mnt/hgfs -o allow_other
ls /mnt/hgfs
ls /mnt/hgfs/lab1/lab1.0
ls: cannot access '/mnt/hgfs/lab1/lab1.0': No such file or directory
cd /mnt/hgfs/lab1
cat lab1.0
Completing file...
lab1.001* lab1.003* lab1.006* lab1.009* lab1.012*
lab1.001.txt* lab1.004* lab1.007* lab1.010* lab1.013*
lab1.002* lab1.005* lab1.008* lab1.011* lab1.014*
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.
27°C Có mây
Search
9:13 PM 9/18/2025

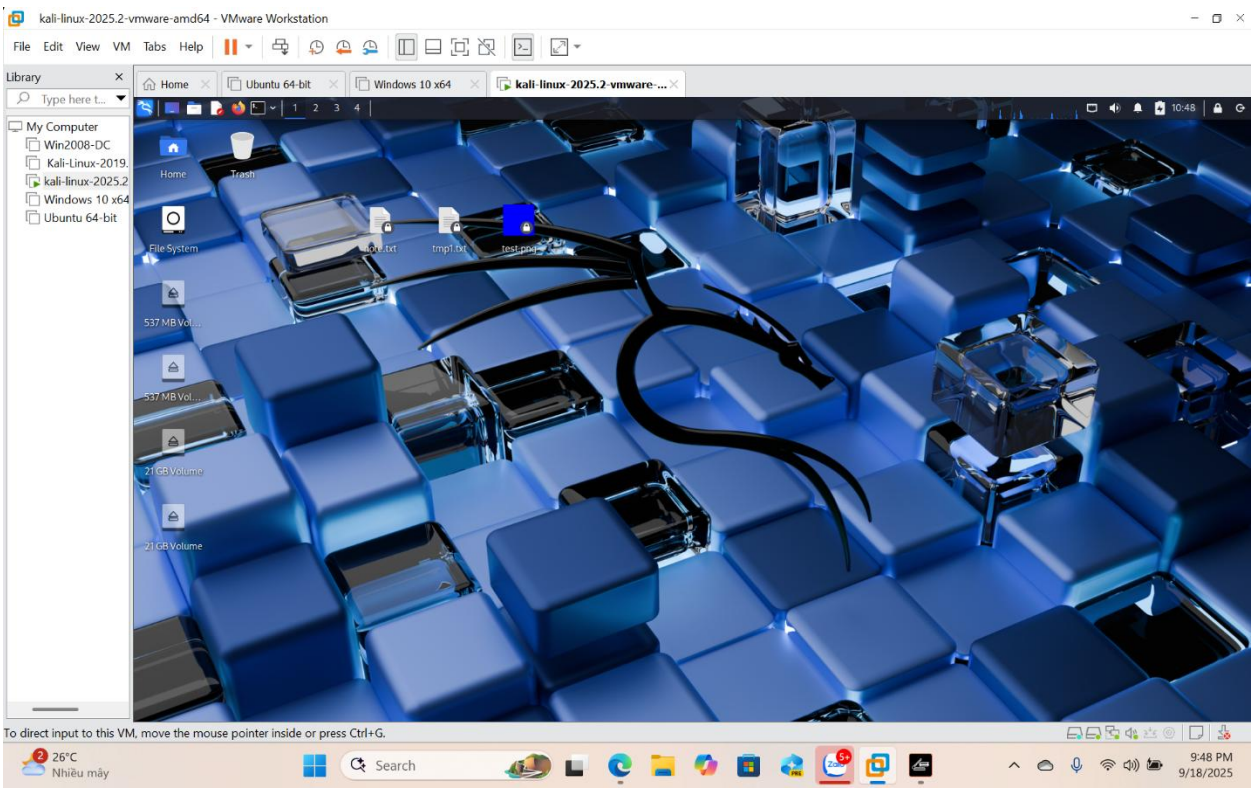

kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Win2008-DC
Kali-Linux-2019.
kali-linux-2025.2
Windows 10 x64
Ubuntu 64-bit
Home
Ubuntu 64-bit
Windows 10 x64
kali-linux-2025.2-vmware-...
kali@he190825: ~/image
File Actions Edit View Help
loop0p2 19.5G ext4
(kali㉿he190825)-[~/image]
$ sudo lsblk -o NAME,SIZE,FSTYPE,MOUNTPOINT /dev/loop0 /dev/loop0p*
NAME SIZE FSTYPE MOUNTPOINT
loop0 20G
├loop0p1 512M vfat
└loop0p2 19.5G ext4
loop0p1 512M vfat
loop0p2 19.5G ext4
(kali㉿he190825)-[~/image]
$ sudo mount -o ro -t vfat /dev/loop0p1 /mnt/forensic
(kali㉿he190825)-[~/image]
$ sudo mount -o ro -t ext4 /dev/loop0p2 /mnt/forensic
(kali㉿he190825)-[~/image]
$ sudo lsblk -o NAME,SIZE,FSTYPE,MOUNTPOINT /dev/loop0 /dev/loop0p*
NAME SIZE FSTYPE MOUNTPOINT
loop0 20G
├loop0p1 512M vfat /mnt/forensic
└loop0p2 19.5G ext4 /mnt/forensic
loop0p1 512M vfat /mnt/forensic
loop0p2 19.5G ext4 /mnt/forensic
(kali㉿he190825)-[~/image]
$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
26°C
Nhiều mây
Search
9:33 PM
9/18/2025


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Win2008-DC
Kali-Linux-2019.
kali-linux-2025.2
Windows 10 x64
Ubuntu 64-bit
Home
Ubuntu 64-bit
Windows 10 x64
kali-linux-2025.2-vmware-...
kali@he190825: ~/image
File Actions Edit View Help
└loop0p2 19.5G ext4 /mnt/forensic
loop0p1 512M vfat /mnt/forensic
loop0p2 19.5G ext4 /mnt/forensic
(kali㉿he190825)-[~/image]
$ sudo losetup -Pf --show ~/image/lab1_image.dd
/dev/loop1
(kali㉿he190825)-[~/image]
$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
loop0 7:0 0 20G 0 loop
├loop0p1 259:0 0 512M 0 part /mnt/forensic
└loop0p2 259:1 0 19.5G 0 part /mnt/forensic
loop1 7:1 0 20G 0 loop
├loop1p1 259:2 0 512M 0 part
└loop1p2 259:3 0 19.5G 0 part
sda 8:0 0 80.1G 0 disk
└sda1 8:1 0 80.1G 0 part /
sdb 8:16 0 20G 0 disk
(kali㉿he190825)-[~/image]
$ losetup -a
/dev/loop1: []: (/home/kali/image/lab1_image.dd)
/dev/loop0: []: (/home/kali/image/lab1_image.dd)
(kali㉿he190825)-[~/image]
$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
26°C
Nhiều mây
Search
9:36 PM
9/18/2025


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Win2008-DC
Kali-Linux-2019.
kali-linux-2025.2
Windows 10 x64
Ubuntu 64-bit
Home
Ubuntu 64-bit
Windows 10 x64
kali-linux-2025.2-vmware-...
10:37
kali@he190825: ~/image
File Actions Edit View Help
└─loop0p2 259:1 0 19.5G 0 part /mnt/forensic
loop1 7:1 0 20G 0 loop
├─loop1p1 259:2 0 512M 0 part
└─loop1p2 259:3 0 19.5G 0 part
sda 8:0 0 80.1G 0 disk
└─sda1 8:1 0 80.1G 0 part /
sdb 8:16 0 20G 0 disk
(kali㉿he190825)-[~/image]
$ losetup -a
/dev/loop1: []: (/home/kali/image/lab1_image.dd)
/dev/loop0: []: (/home/kali/image/lab1_image.dd)
(kali㉿he190825)-[~/image]
$ sudo parted ~/image/lab1_image.dd print
Model: (file)
Disk /home/kali/image/lab1_image.dd: 21.5GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:
Number Start End Size File system Name Flags
1 1049kB 538MB 537MB fat32 primary msftdata
2 538MB 21.5GB 20.9GB ext4 primary
(kali㉿he190825)-[~/image]
$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
26°C
Nhiều mây
Search
9:37 PM
9/18/2025


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Win2008-DC
Kali-Linux-2019.
kali-linux-2025.2
Windows 10 x64
Ubuntu 64-bit
Home
Ubuntu 64-bit
Windows 10 x64
kali-linux-2025.2-vmware-...
10:47
kali@he190825: ~/image
File Actions Edit View Help
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
1 P MS Data 2048 1050623 1048576 [primary] [NO NAM
Directory /
-rwxr-xr-x 0 0 2224 18-Sep-2025 13:38 File1.pdf
-rwxr-xr-x 0 0 2224 18-Sep-2025 13:47 File2.pdf
-rwxr-xr-x 0 0 757 18-Sep-2025 13:47 test.jpeg
-rwxr-xr-x 0 0 41 18-Sep-2025 13:47 tmp2.txt
-rwxr-xr-x 0 0 57 18-Sep-2025 13:47 note.txt
-rwxr-xr-x 0 0 41 18-Sep-2025 13:47 tmp1.txt
Next
Use Right to change directory, 'h' to hide deleted files
'q' to quit, ':' to select the current file, 'a' to select all files
'C' to copy the selected files, 'c' to copy the current file
537 MB Vol...
21 GB Volume
537 MB Vol...
21 GB Volume
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
26°C
Nhiều mây
Search
9:47 PM
9/18/2025


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Win2008-DC
Kali-Linux-2019.
kali-linux-2025.2
Windows 10 x64
Ubuntu 64-bit
Home
Ubuntu 64-bit
Windows 10 x64
kali-linux-2025.2-vmware-...
kali@hc190825: ~/image
File Actions Edit View Help
TestDisk 7.2, Data Recovery Utility, February 2024
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
1 P MS Data 2048 1050623 1048576 [primary] [NO NAM
Directory /
Copy done! 3 ok, 0 failed
-rwxr-xr-x 0 0 2224 18-Sep-2025 13:38 File1.pdf
-rwxr-xr-x 0 0 2224 18-Sep-2025 13:47 File2.pdf
-rwxr-xr-x 0 0 757 18-Sep-2025 13:47 test.jpeg
-rwxr-xr-x 0 0 203 18-Sep-2025 13:47 test.png
-rwxr-xr-x 0 0 41 18-Sep-2025 13:47 tmp2.txt
-rwxr-xr-x 0 0 57 18-Sep-2025 13:47 note.txt
>-rwxr-xr-x 0 0 41 18-Sep-2025 13:47 tmp1.txt
Next
Use Right to change directory, 'h' to hide deleted files
'q' to quit, ':' to select the current file, 'a' to select all files
'C' to copy the selected files, 'c' to copy the current file
Home
File System
537 MB Vol...
21 GB Volume
537 MB Vol...
21 GB Volume
test.png
note.txt
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
26°C
Nhiều mây
Search
9:48 PM
9/18/2025


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
Win2008-DC
Kali-Linux-2019.
kali-linux-2025.2
Windows 10 x64
Ubuntu 64-bit
Home
Ubuntu 64-bit
Windows 10 x64
kali-linux-2025.2-vmware-...
Home
Trash
File System
tmp1.txt
test.png
537 MB Vol...
537 MB Vol...
21 GB Volume
21 GB Volume
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
26°C
Nhiều mây
Search
9:48 PM
9/18/2025