

LAB 10

Thầy Mai Hoàng Đình
Trường đại học FPT

Người thực hiện
Đặng Hoàng Nguyên

Lab-Project 10: Static Acquisition with BackTrack

Những thứ chúng ta cần trong bài lab này

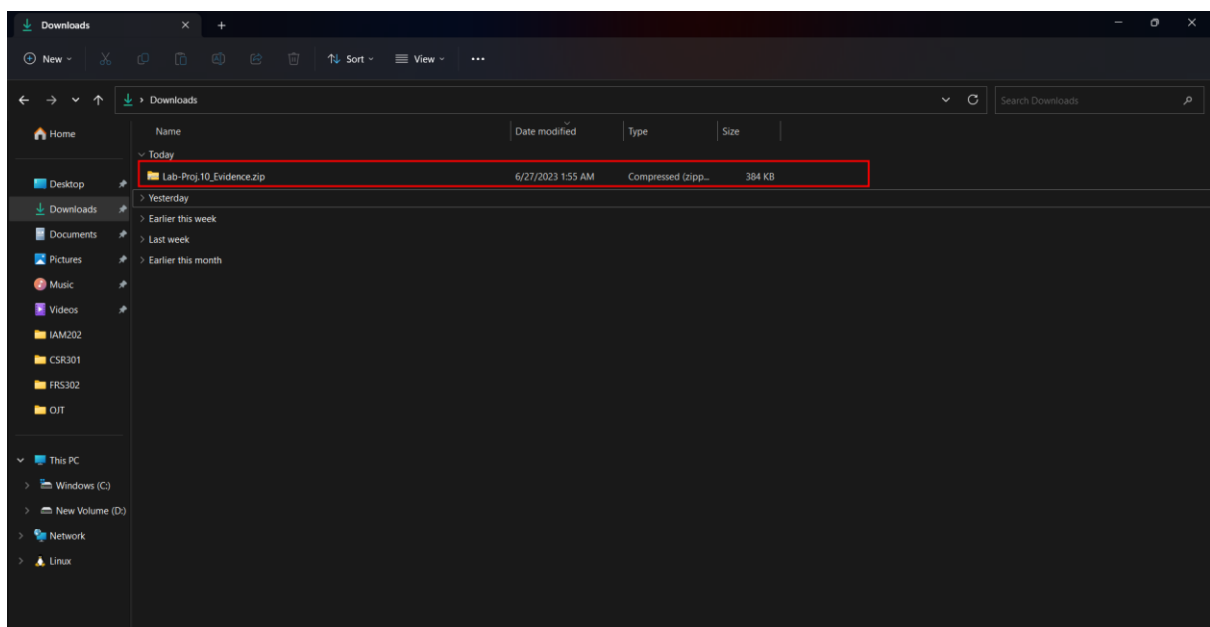
- VMware Player
- Máy ảo có thể là Kali hoặc Backtrack – Backtrack là phiên bản cũ hơn của Kali.

Những file chúng ta cần

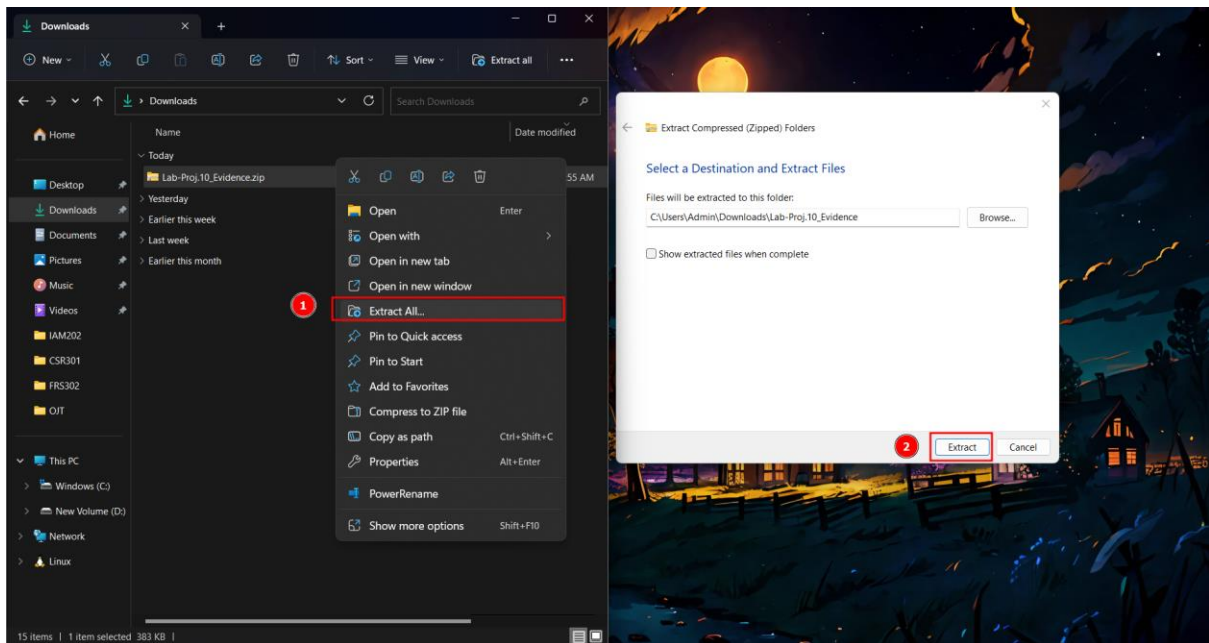
Chúng ta có thể Download backtrack theo đường dẫn dưới đây:

- <http://www.backtrack-linux.org/downloads>

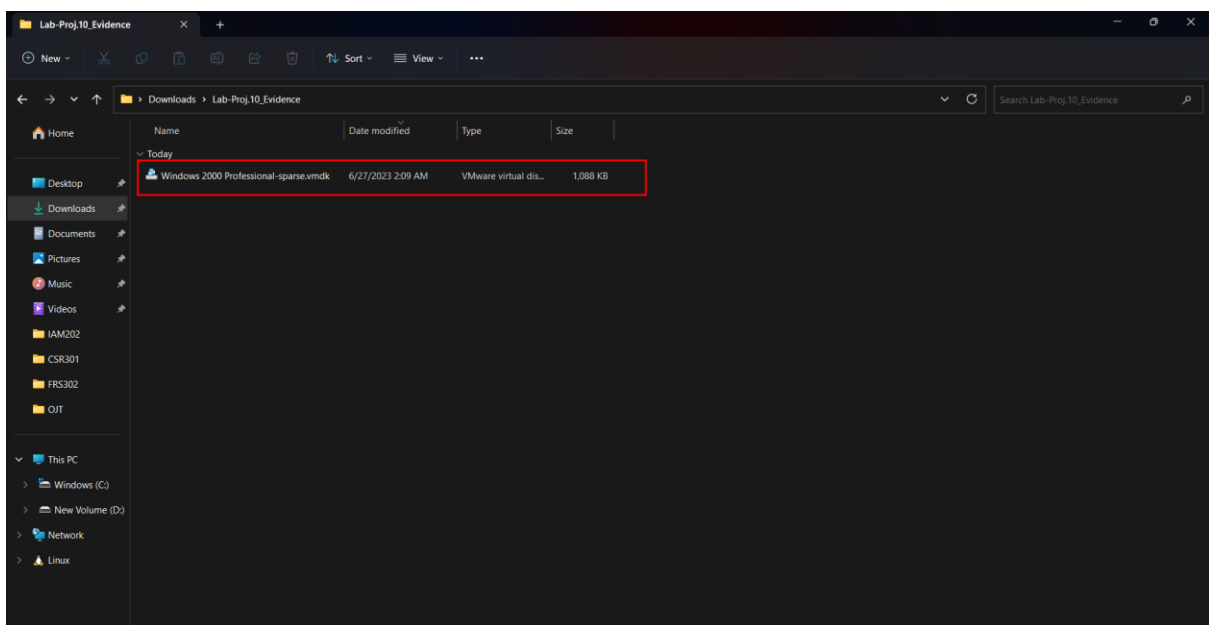
Tải xuống **p10Evidence.zip** từ bên trong OneDrive. Sau khi download xong nó sẽ nằm ở bên trong folder đã được Download, trong trường hợp này là folder Download



Nhấn chuột phải vào file **p10Evidence.zip** và nhấn "**Extract All**", **Extract**.



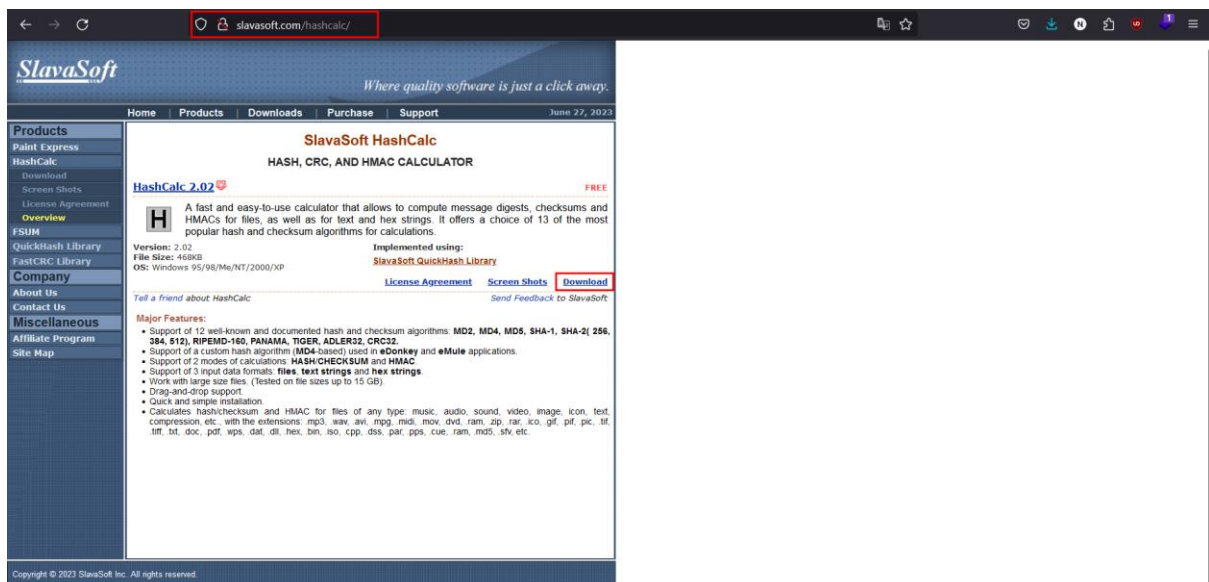
Sau khi giải nén xong sẽ có một màn hình mới xuất hiện và có một file mang tên là: "Windows 2000 Professional-sparse.vmdk". Đó chính là file bằng chứng mà chúng ta sẽ cần để điều tra



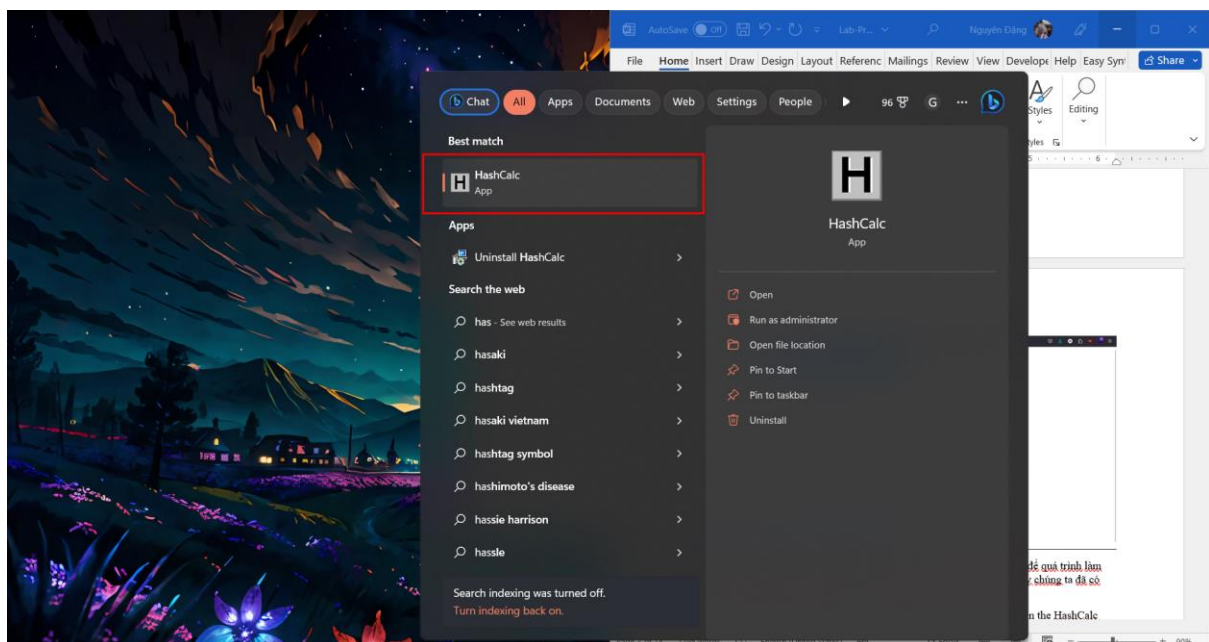
Checking the Hash Value of the Evidence File

Để check rằng đây là một file bằng chứng đúng thì chúng ta sẽ sử dụng phần mềm HashCalc để có thể check mã hash của file. Có thể tải tại đường link sau:

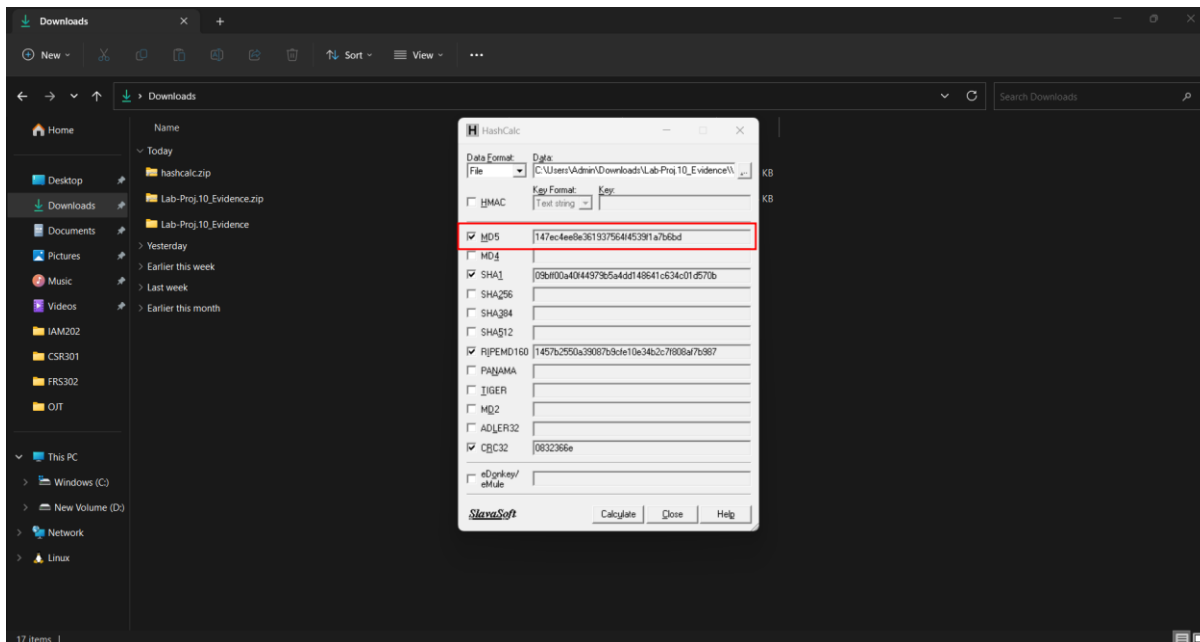
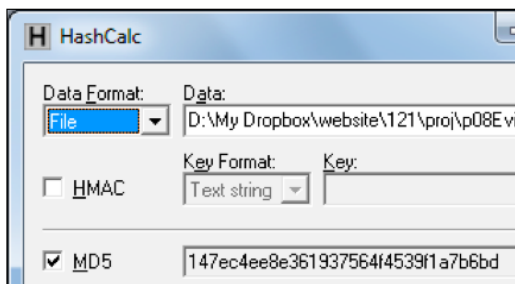
- <http://slavasoft.com/hashcalc>



Sau khi download xong chúng ta sẽ cài đặt theo những thông số mặc định để quá trình làm lab được diễn ra một cách dễ dàng. Sau khi cài xong ta có thể thấy rằng máy chúng ta đã có HashCalc



Chúng ta sẽ kéo file "**Windows 2000 Professional-sparse.vmdk**" vào bên trong HashCalc. Chúng ta sẽ check xem rằng mã MD5 của chúng có trùng với MD5 mà bài lab đã đưa ra không.



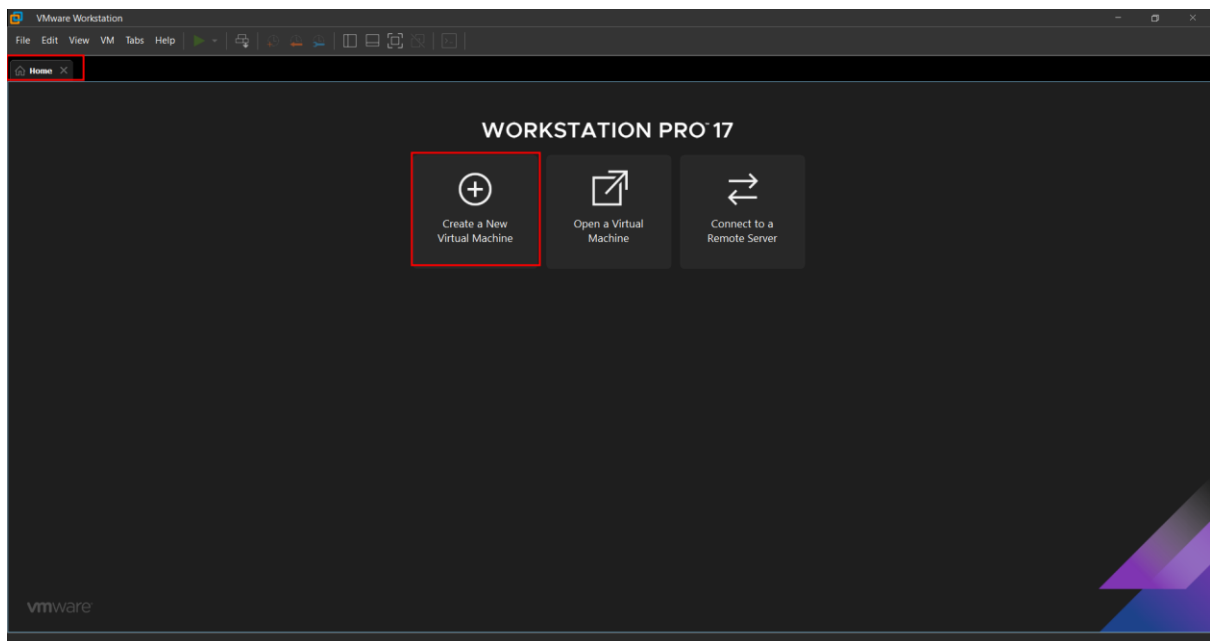
Mã của chúng ta đã trùng với mã của đề đã đưa ra. Vậy là chúng ta đã chuẩn bị xong những thứ để dung cho bài lab ngày hôm nay.

Nếu chúng ta có máy ảo Kali sẵn rồi thì có thể bỏ qua bước dưới đây:

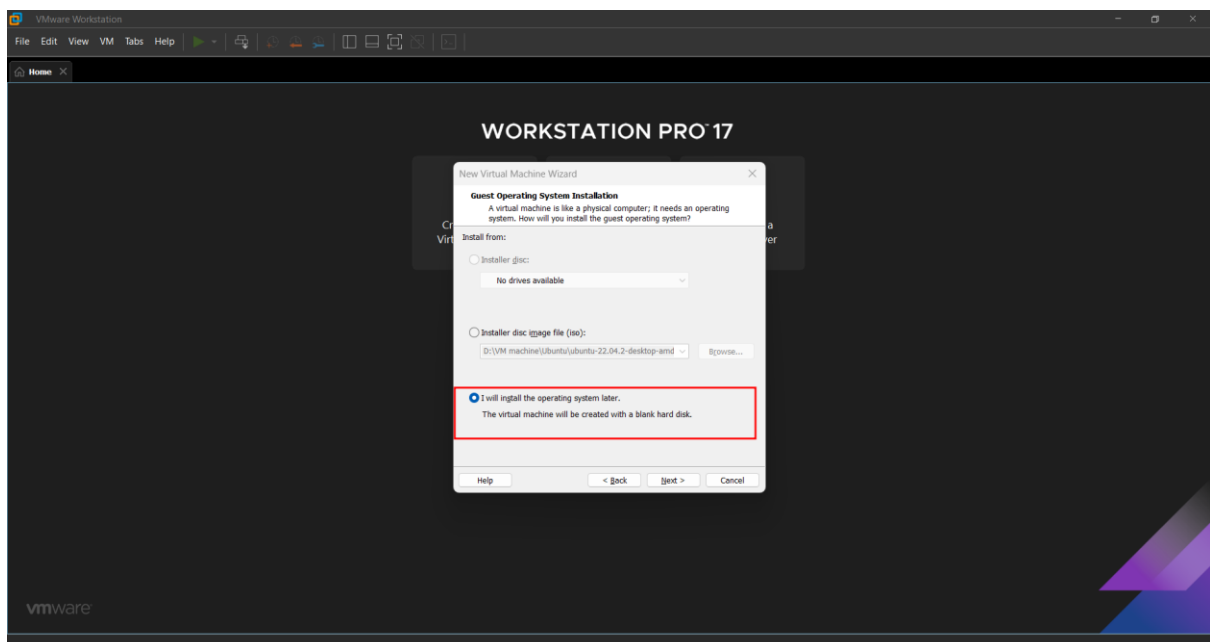
Creating a New Virtual Machine

Chúng ta sẽ khởi động máy ảo lên

Để tạo máy ảo mới, trong giao diện Home, chúng ta sẽ click vào "**Create a new Virtual Machine**" hoặc chúng ta có thể nhấn tổ hợp **Ctrl + N** để có thể tạo máy ảo mới

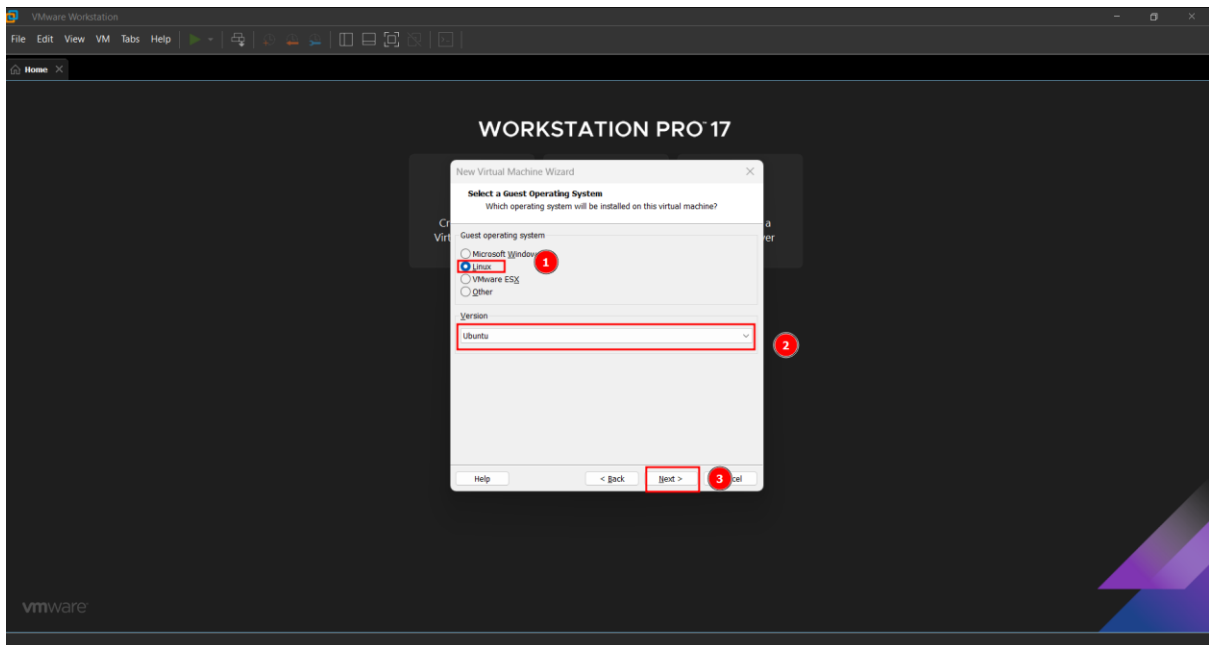


Trong phần "New Virtual Machine Wizard", nhấn vào chỗ **"I will install the operating system later"** để setup những thông số cơ bản trước như hình bên dưới và sau đó click **Next**.



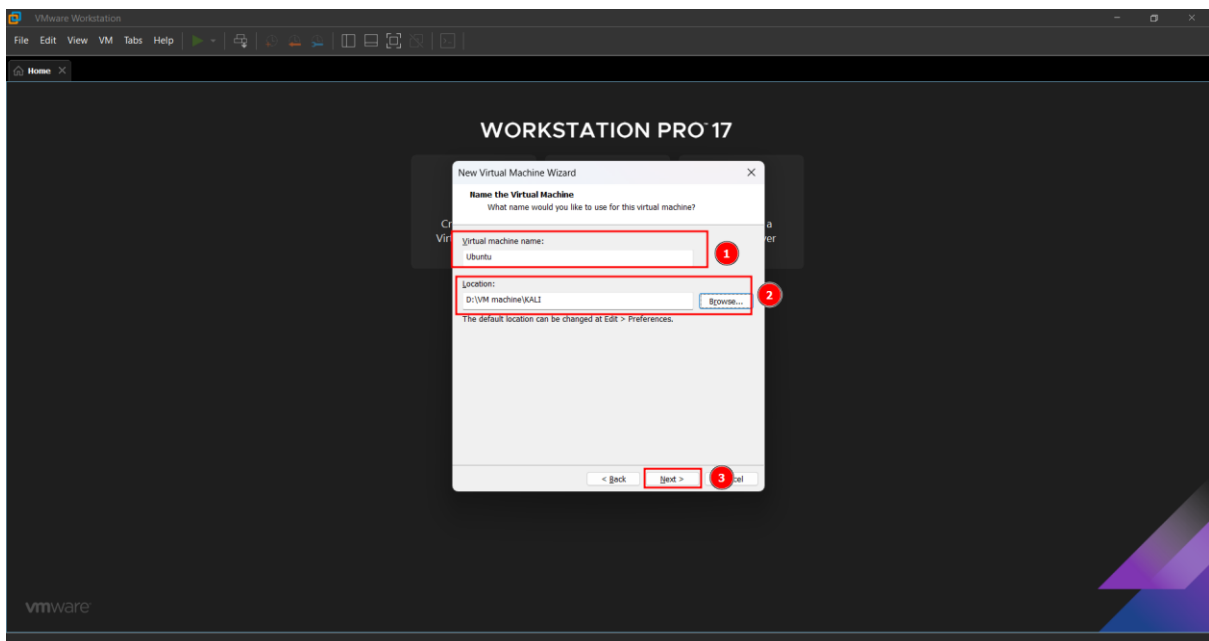
Trong phần "Select a Guest Operating System", Chọn "Guest Operating System" là **Linux** và "version" là **Ubuntu** như hình bên dưới và sau đó nhấn **Next**.

Lưu ý: Điều này rất quan trọng vì vậy VMware sẽ sử dụng trình điều khiển chuột phù hợp, đặc biệt là trên netbook và hệ thống có chuột USB.



Trong phần "Name the Virtual Machine" chúng ta sẽ đặt tên cho máy chúng ta và ở đây chúng ta sẽ để là Nguyendh

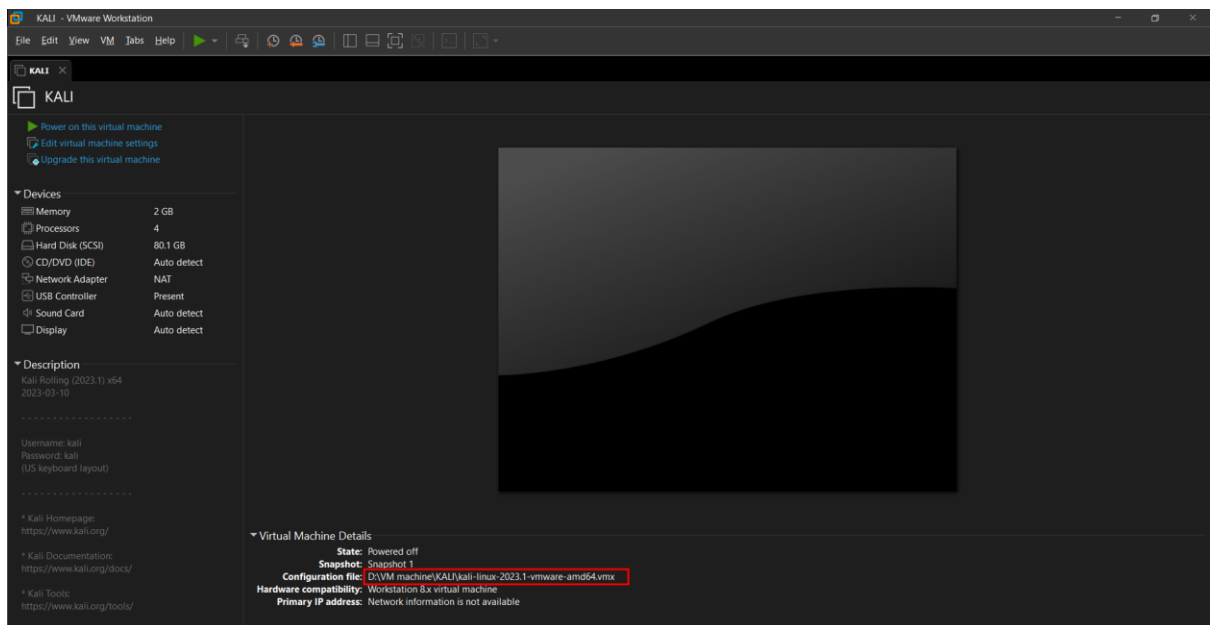
Và sau đó chọn nơi để có thể lưu máy ảo của chúng ta. Trong trường hợp này sẽ là đường dẫn D:\\VM machine\\Kali và sau đó nhấn **Next**



Trong phần "Specify Disk Capacity" chọn hết tất cả cài đặt mặc định của máy và cứ nhấn tiếp tục cho tới khi hoàn thành.

Trong phần "Ready to Create Virtual Machine", nhấn **Finish**.

Sau khi làm xong chúng ta sẽ hiện ra một máy ảo giống như thế này là thành công

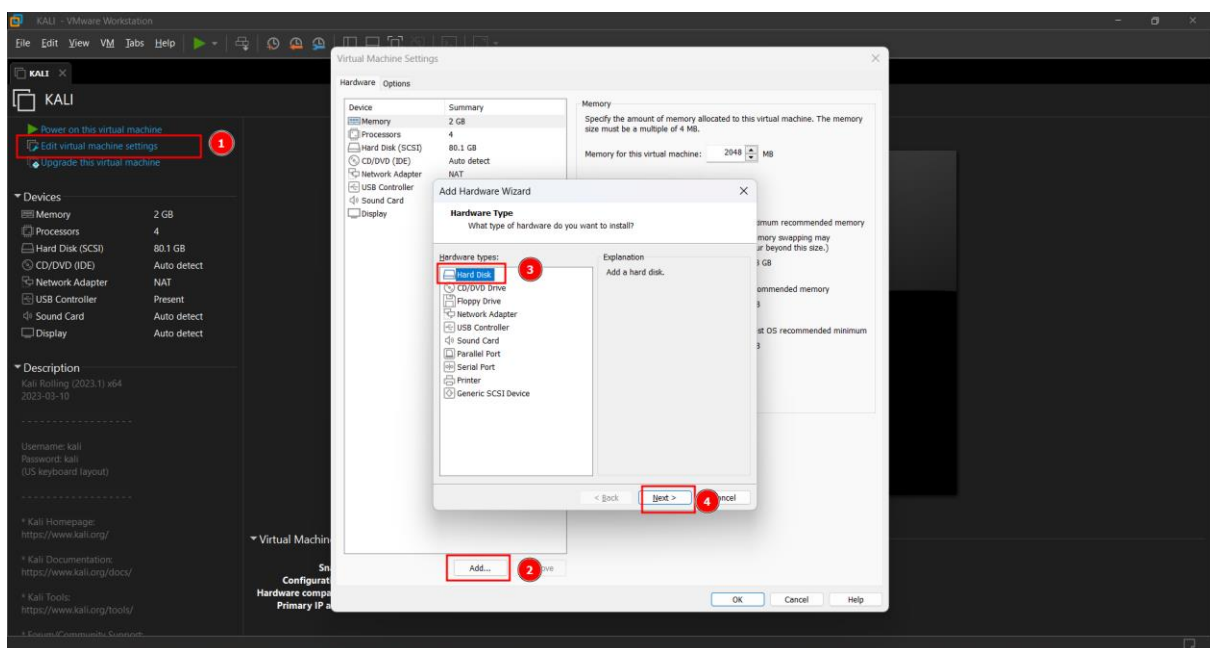


Connecting the Evidence Drive

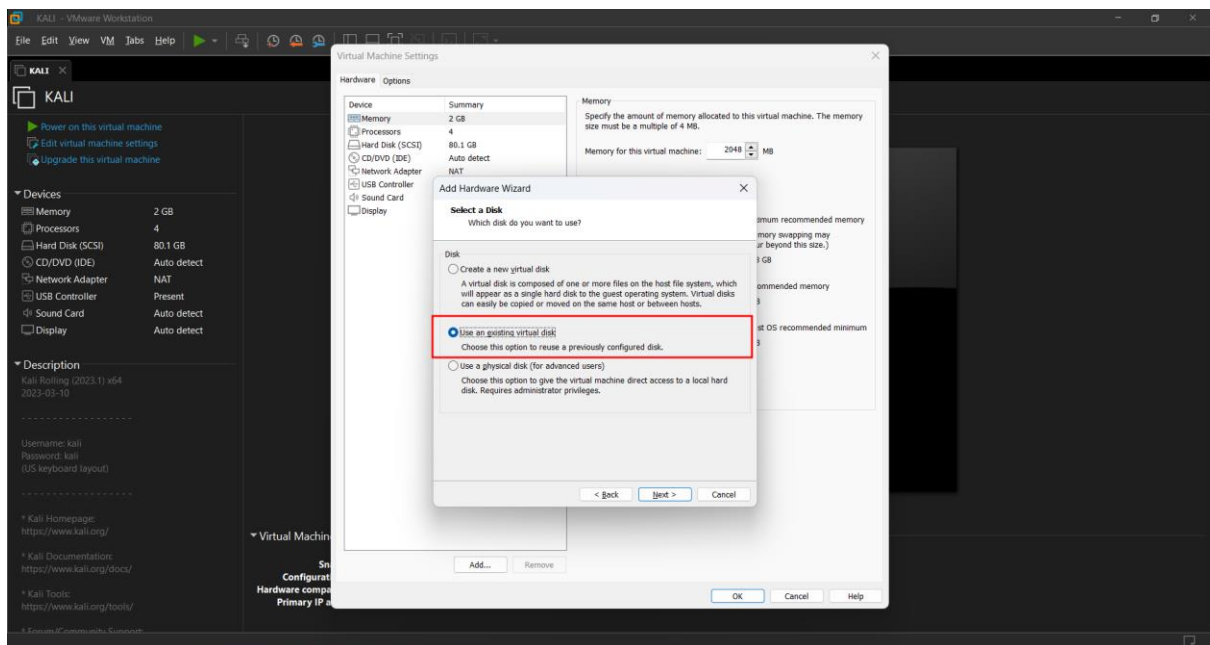
Trong VMware Player, nhấn vào **"Edit virtual machine settings"**.

Tron phần "Virtual Machine Settings", chọn vào nút **Add...**

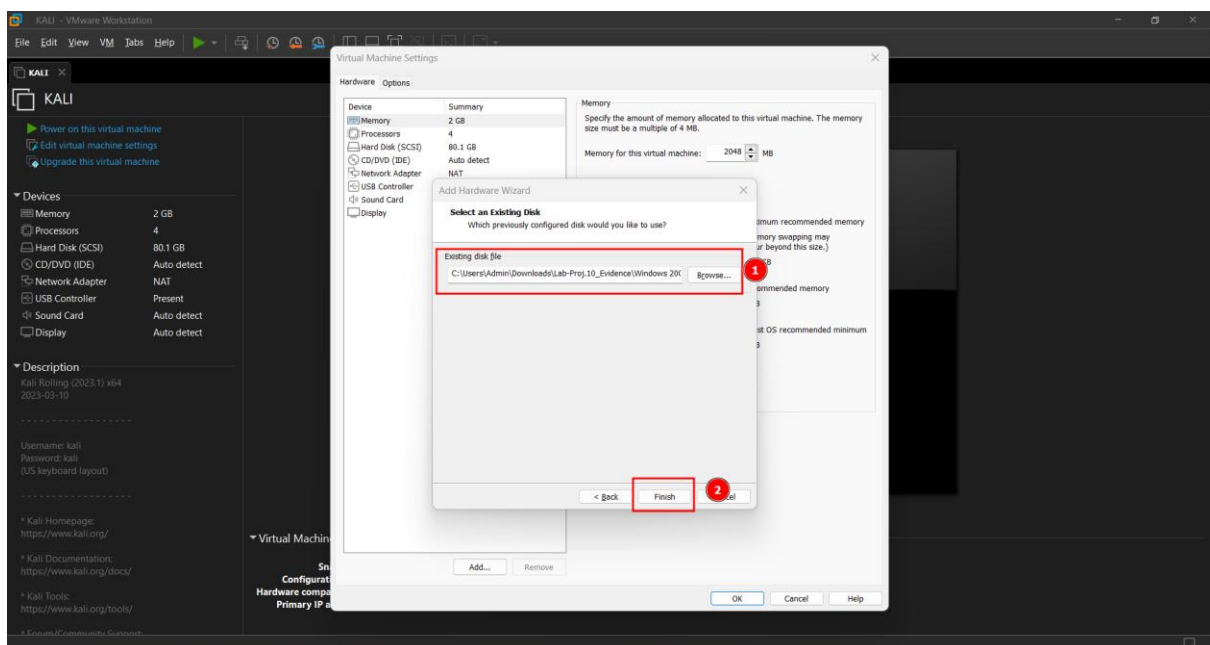
Trong phần "Hardware Type", chọn vào phần **"Hard Disk"**. Nhấn **Next**.



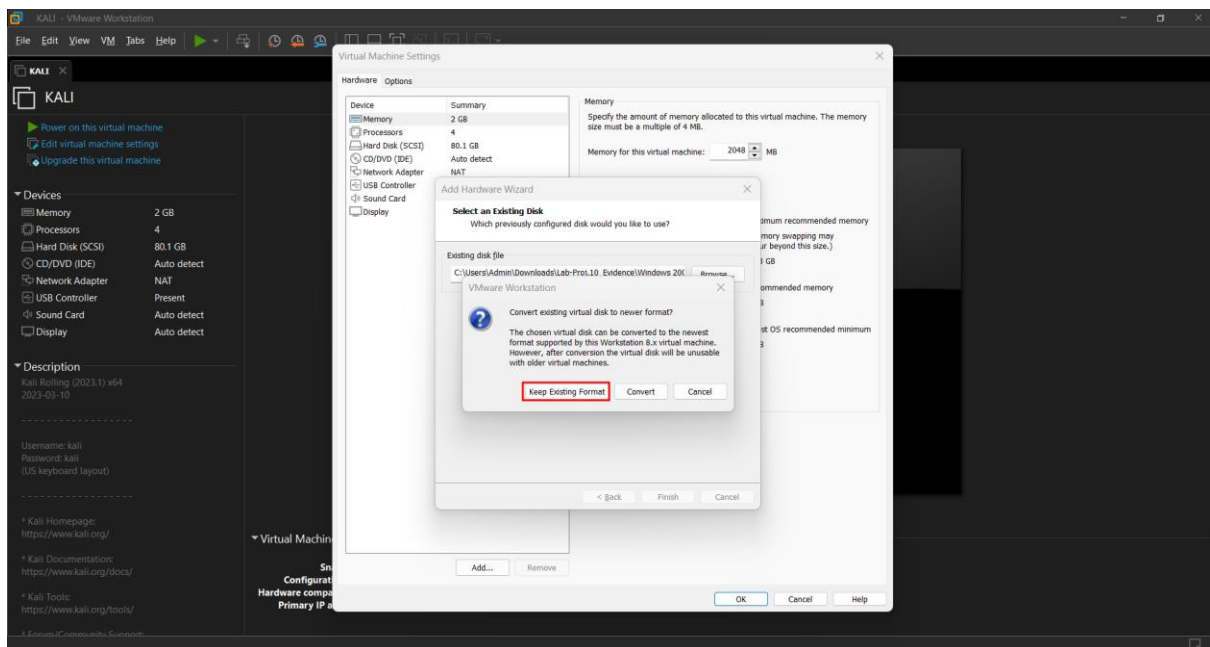
Trong phần "Select a Disk", nhấn chọn vào **"Use an existing virtual disk"**. Sau đó nhấn **Next**.



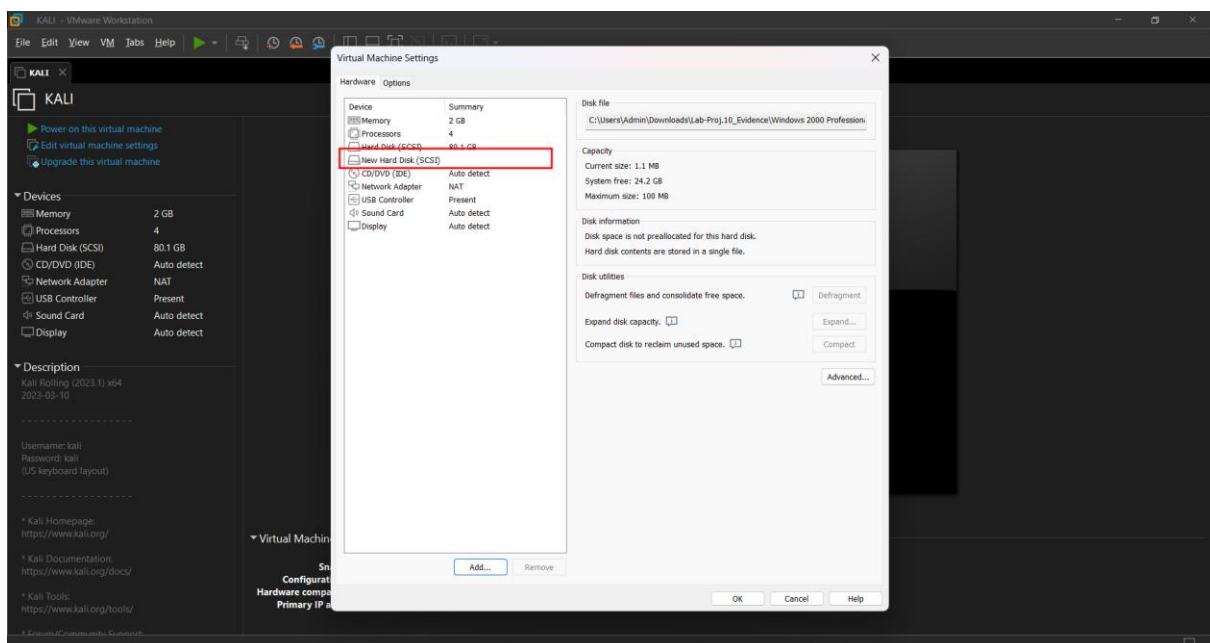
Trong phần "Select an Existing Disk", nhấn chọn vào nút **Browse...** . Chúng ta sẽ đi đến nơi có chứa "**Windows 2000 Professional-sparse.vmdk**" và click chọn vào nó. Trong trường hợp máy em sau khi giải nén ra vẫn ở trong thư mục Downloads



Có một hộp thoại hiện lên và hỏi chúng ta có muốn 'Convert existing virtual disk to newer format?'. Vì đây là một file bản chún nên chúng ta không nên chỉnh sửa bất cứ mọtjt thứ gì bên trong nó nên chúng ta sẽ chọn vào "**Keep Existing Format**".



Trong phần "Virtual Machine Settings" hiện giờ sẽ xuất hiện "New Hard Disk", hiển thị như hình bên dưới



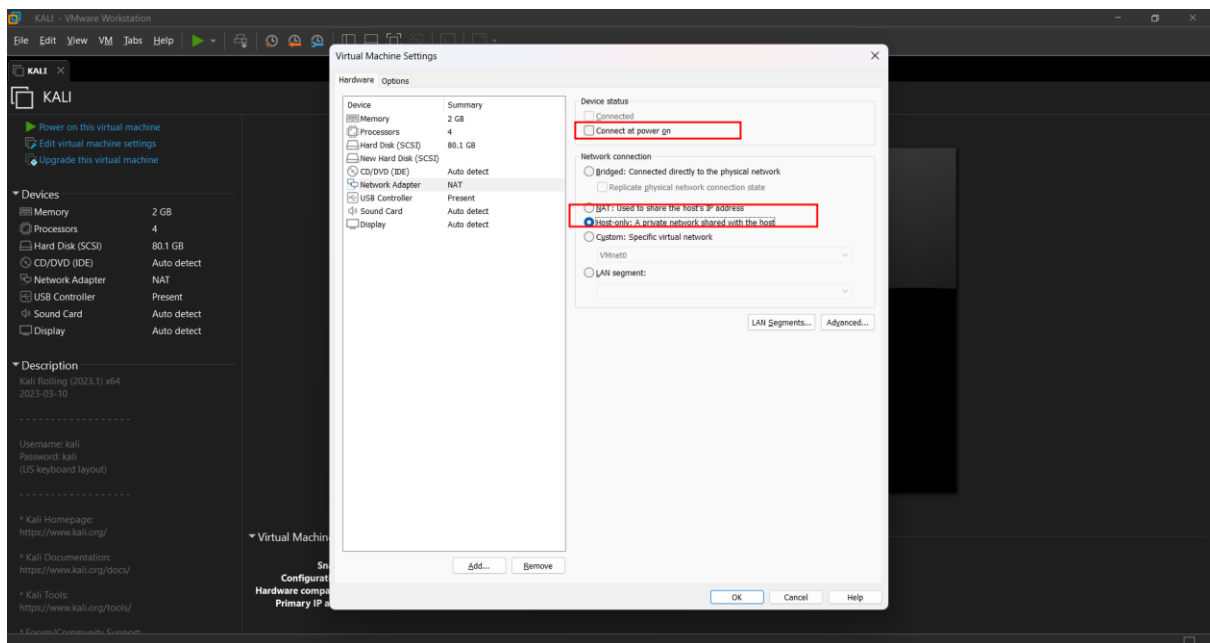
Disabling Networking

Một quy tắc cơ bản của pháp y là LÀM VIỆC TRONG PHÒNG KÍN - nói cách khác, không kết nối với Internet trong khi ồ đĩa.

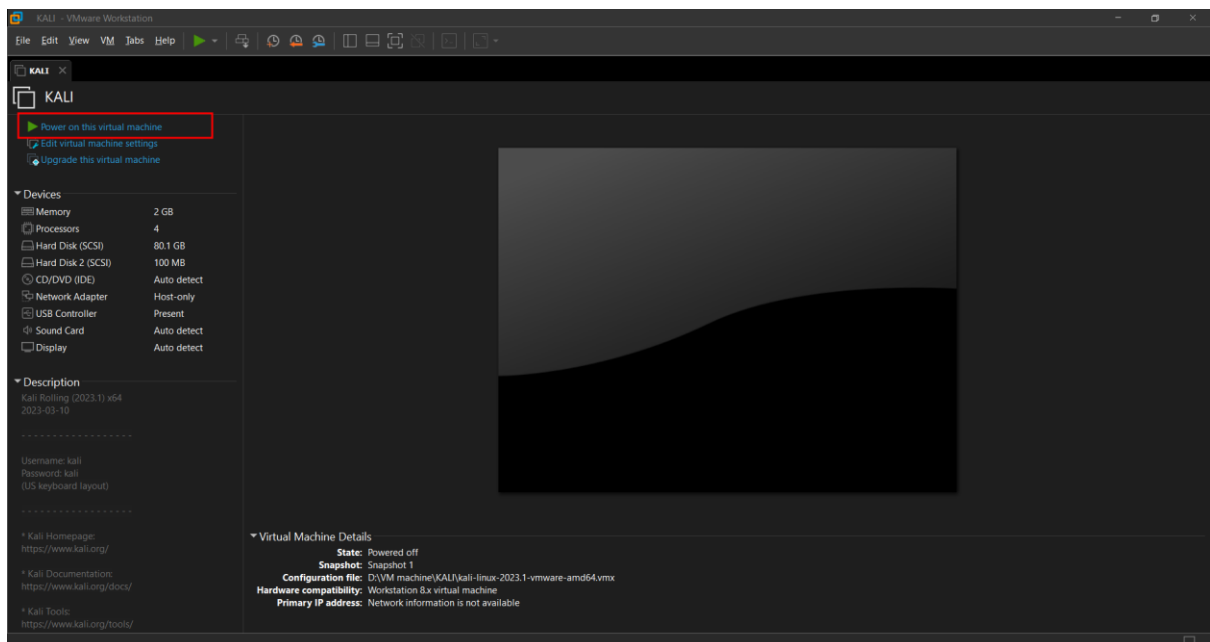
Để ngắt kết nối, trong phần "Virtual Machine Settings" nhấn chọn vào phần Network Adapter

Bên phía bên trái, chúng ta sẽ bỏ click vào "**Connect at power on**" box.

Bên phía bên trái, chúng ta sẽ cài đặt mạng với chế độ là Host only như hình bên dưới.

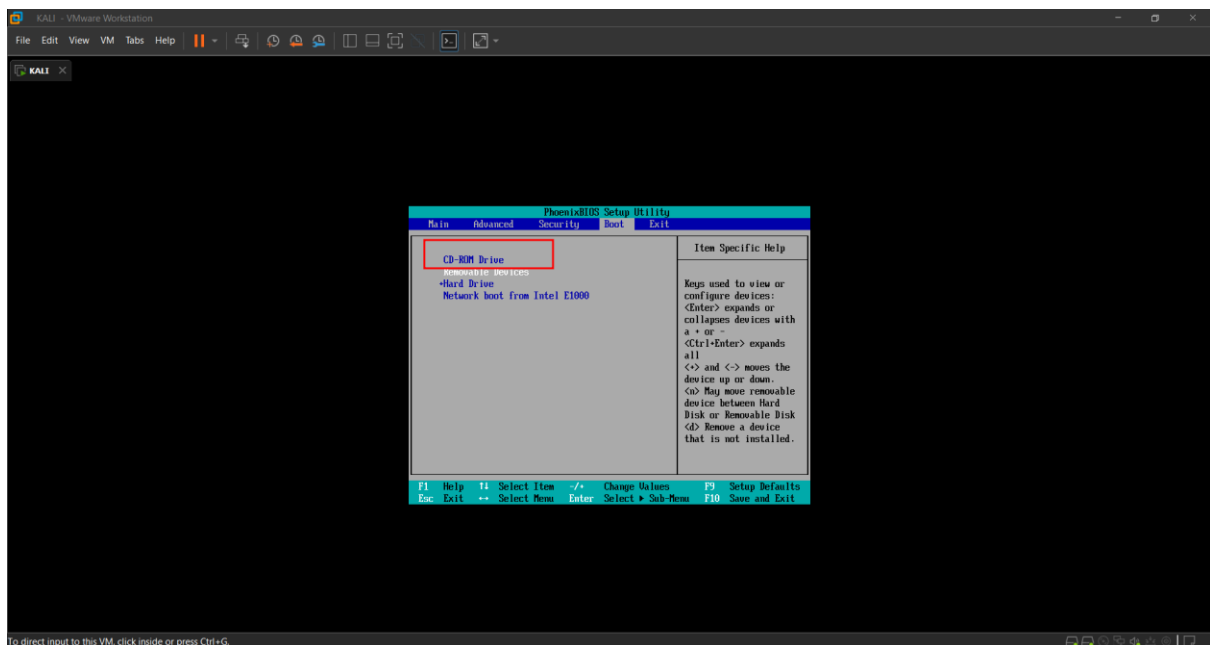


Trong VMware Player, chọn vào "**Power on virtual machine**".



Sau đó khi máy ảo đang chuẩn bị vào thì chúng ta sẽ nhấn F2 để có thể vào bios

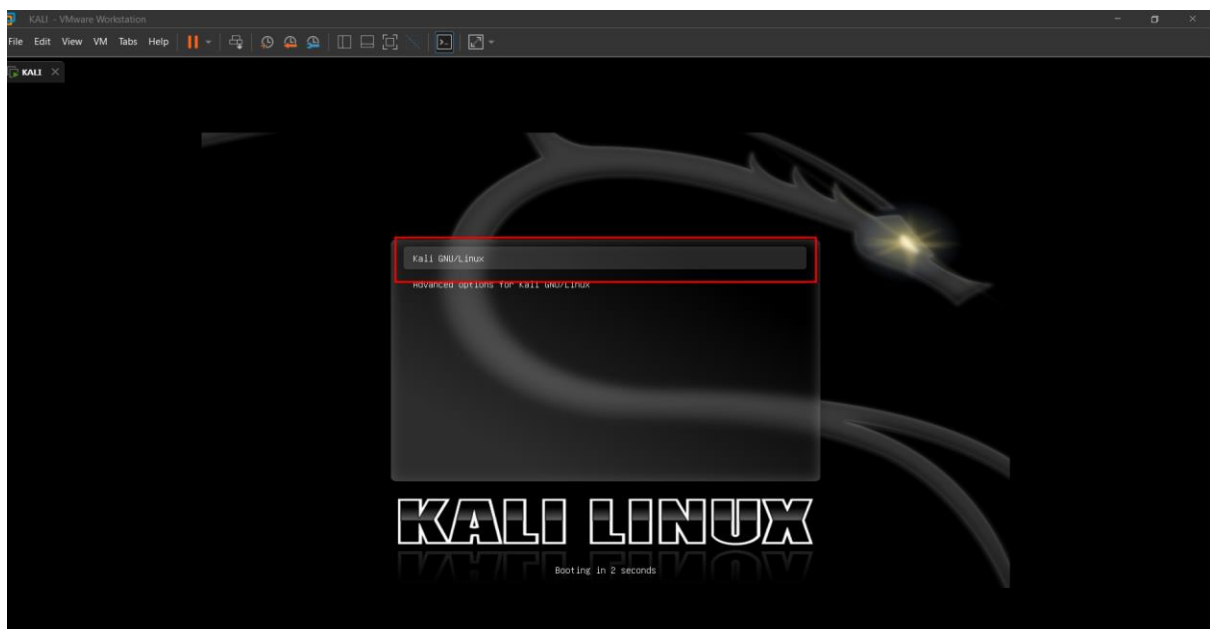
Bios sẽ xuất hiện như hình bên dưới. Nếu nó không xuất hiện thì chúng ta sẽ nhấn tổ hợp **Ctrl + R** để có thể restart lại máy và thử lại cho tới khi nào vào thì thôi



Trong BIOS, sử dụng các phím di chuyển lên xuống để có thể chuyển CD-ROM lên trên đầu tiên như hình bên trên. Sau đó nhấn **F10** và enter để có thể save setting

Vào bên trong màn hình boot, ta sẽ thấy Kali được hoạt động như hình bên dưới

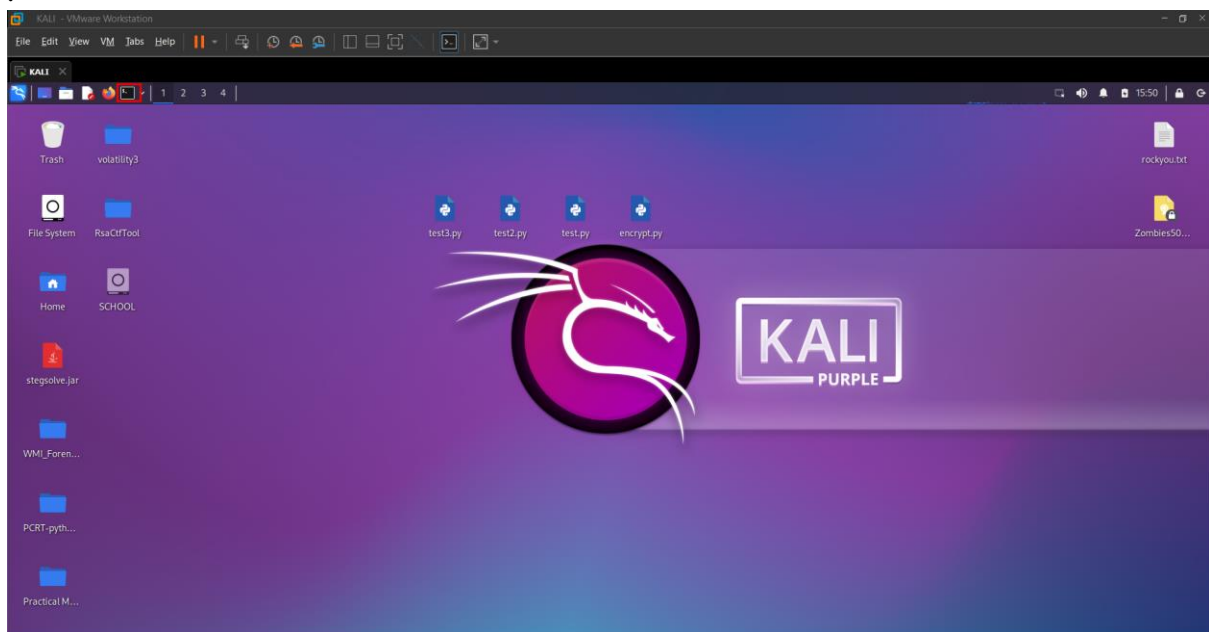
BackTrack starts, as shown below.



The Kali Desktop

Khi màn hình tải, ta sẽ thấy một màn hình trang trí, như được hiển thị bên dưới trên trang này.

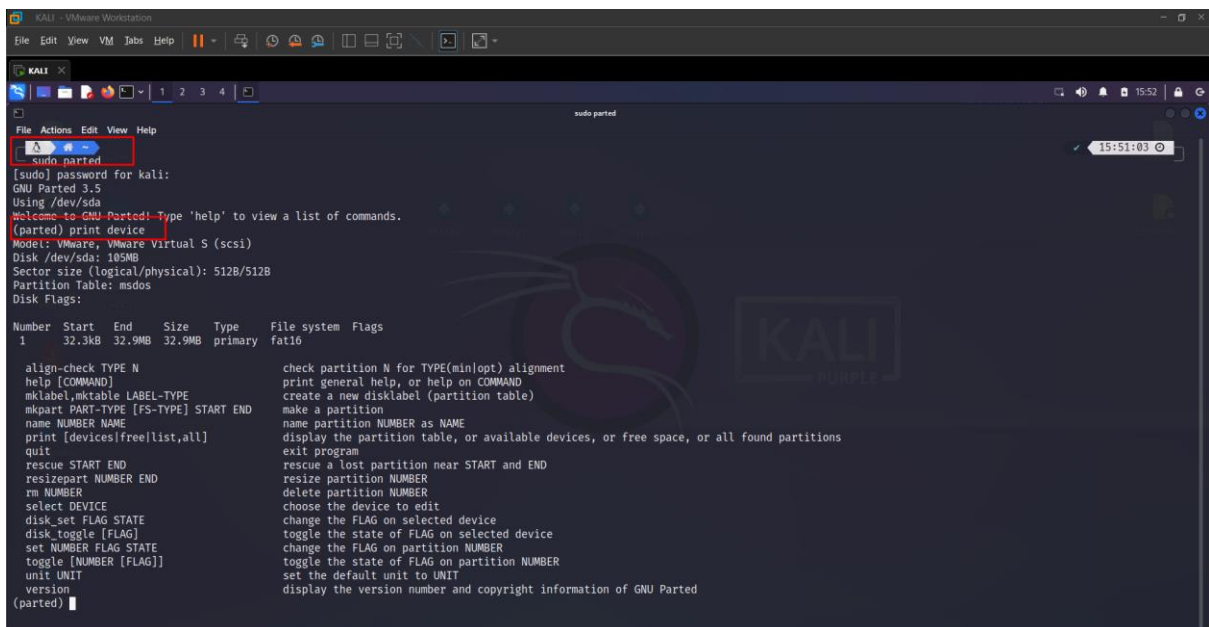
Ở phía trên bên trái, bên phải của biểu tượng Firefox, nhấp vào biểu tượng hình vuông màu đen để mở cửa sổ Terminal



Identifying the Drives with parted

Trong cửa sổ Terminal, chúng ta sẽ nhập lần lượt các câu lệnh sau:

- **parted**
- **print devices**



Đây là những danh sách các ổ đĩa được gắn vào bên trong. Chúng ta sẽ thấy được có một file bằng chứng là /dev/sda với dung lượng là 105MB.

Formatting the Empty Drive

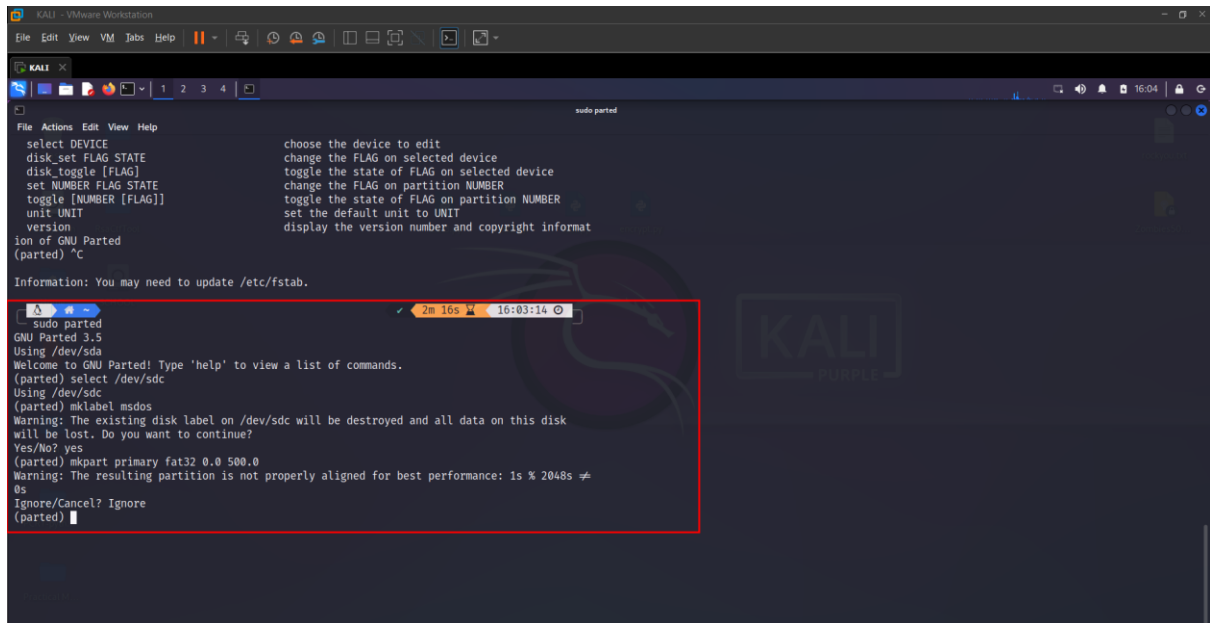
Trong màn hình Terminal, tại command (parted), sử dụng các command sau và sau đó nhấn Enter sau mỗi lần nhập.

Các câu lệnh này sẽ giúp tạo ra một ổ đĩa trống 500MB

Câu lệnh đầu tiên sẽ đảm bảo rằng ổ đĩa chúng ta lấy không phải là ổ đĩa đã dùng bằng chứng

- **select /dev/sdc**
- **mklabel msdos**
- **mkpart primary fat32 0.0 500.0**

Một dòng tin nhắn nói rằng: "The resulting partition is not properly aligned for best performance". Nhấn **ignore** và nhấn Enter để bỏ qua cảnh báo.



```
KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
sudo parted
File Actions Edit View Help
select DEVICE
disk.set FLAG STATE
disk.toggle [FLAG]
set NUMBER FLAG STATE
toggle [NUMBER [FLAG]]
unit UNIT
version
ion of GNU Parted
(parted) ^C
choose the device to edit
change the FLAG on selected device
toggle the state of FLAG on selected device
change the FLAG on partition NUMBER
toggle the state of FLAG on partition NUMBER
set the default unit to UNIT
display the version number and copyright informat
Information: You may need to update /etc/fstab.
sudo parted
GNU Parted 3.5
Using /dev/sdb
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted) select /dev/sdc
Using /dev/sdc
(parted) mklabel msdos
Warning: The existing disk label on /dev/sdc will be destroyed and all data on this disk
will be lost. Do you want to continue?
Yes/No? yes
(parted) mkpart primary fat32 0.0 500.0
Warning: The resulting partition is not properly aligned for best performance: 1s % 2048s !=
0s
Ignore/Cancel? Ignore
(parted)
```

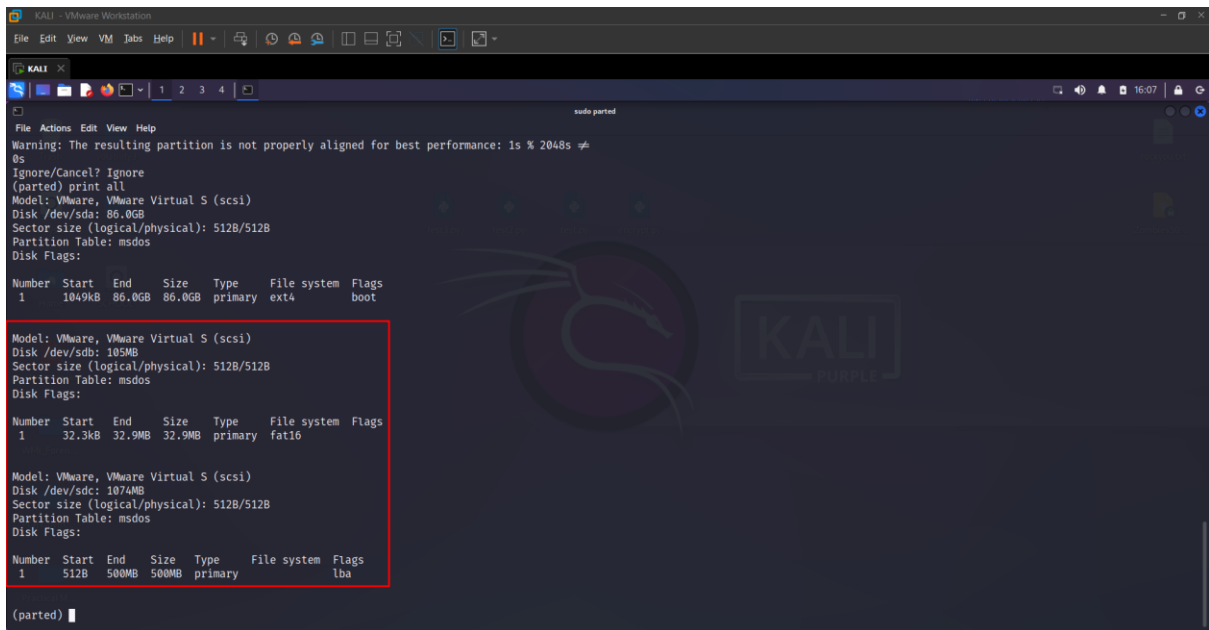
Trong màn hình Terminal, tại command (parted), sử dụng các command sau

- **print all**

Một danh sách của các phân vùng được xuất hiện

Ta có thể thấy rằng có một phân vùng 32.9MB trên /dev/sdb và có một phân vùng 500MB trên ổ đĩa trống /dev/sdc

A list of partitions appears, as shown below on this page.



```
Warning: The resulting partition is not properly aligned for best performance: 1s % 2048s ≠
0s
Ignore/Cancel? Ignore
(parted) print all
Model: VMware, VMware Virtual S (scsi)
Disk /dev/sda: 86.0GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start  End    Size  Type  File system  Flags
1       1049kB  86.0GB  86.0GB  primary  ext4         boot

Model: VMware, VMware Virtual S (scsi)
Disk /dev/sdb: 105MB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start  End    Size  Type  File system  Flags
1       32.3kB  32.9MB  32.9MB  primary  fat16

Model: VMware, VMware Virtual S (scsi)
Disk /dev/sdc: 1074MB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start  End    Size  Type  File system  Flags
1       512B   500MB  500MB  primary  lba
```

Sau đó nhập câu lệnh sau để thoát khỏi chương trình

- **quit**

Mounting the Partition

Now you must mount the new partition.

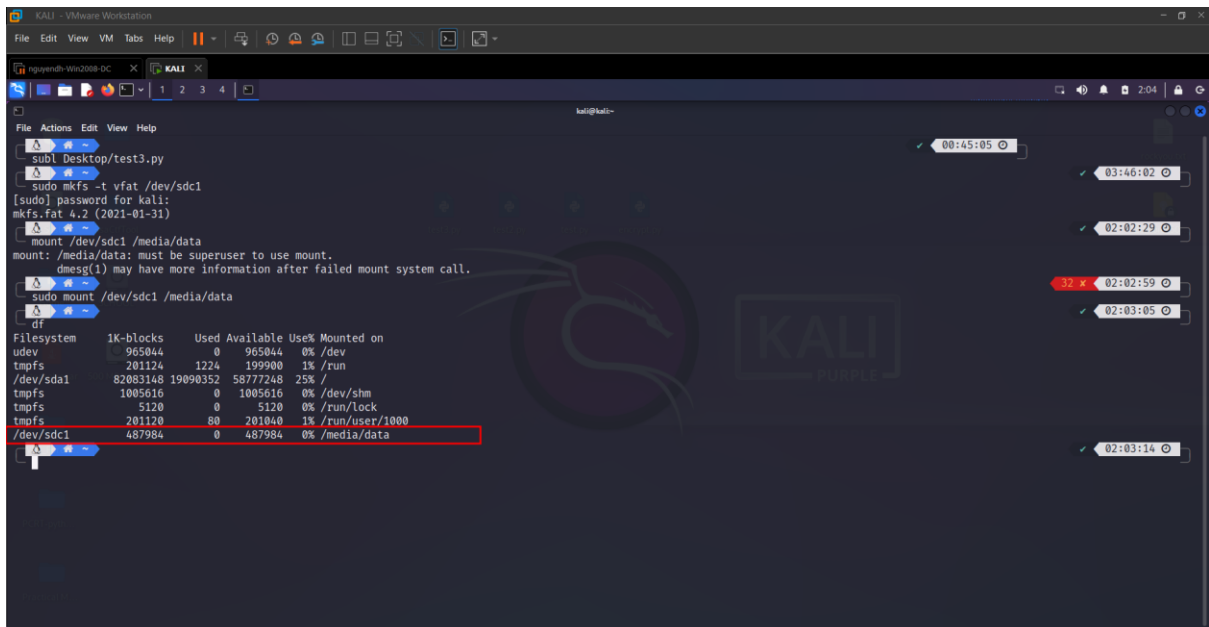
In the Terminal window, at the # prompt, enter these commands, and pressing Enter after each one:

mkdir /media/data

mount /dev/sdb1 /media/data

df

Như ta thấy được hình bên dưới ở dòng cuối cùng /dev/sdc1 được mount tại /media/data, như hình bên dưới.



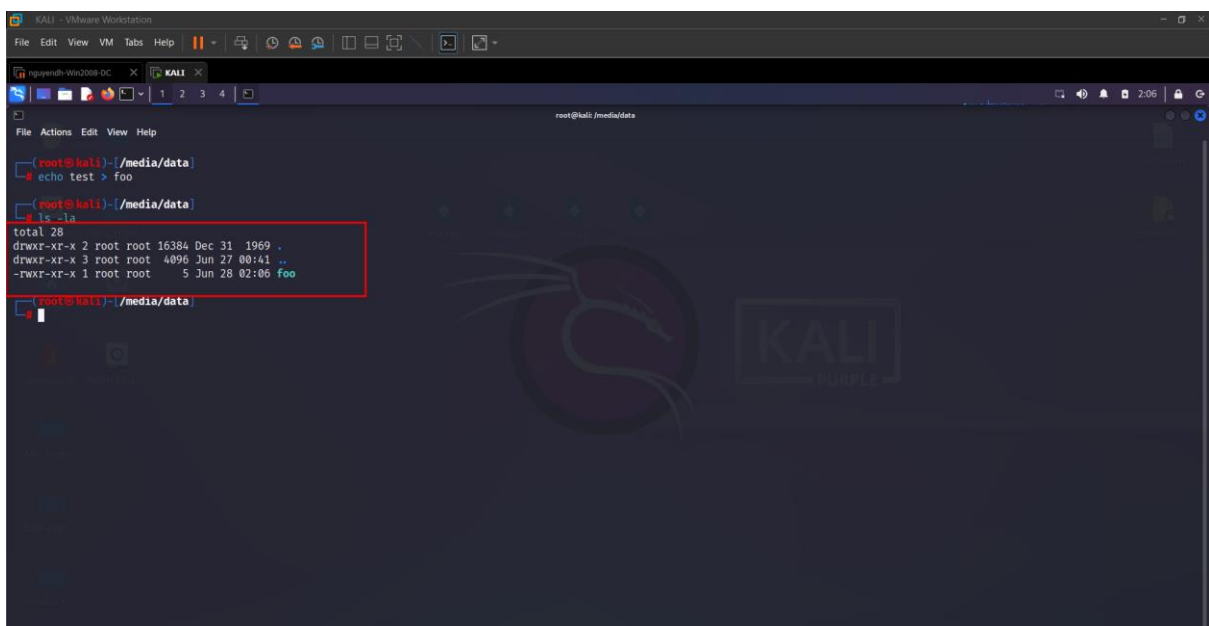
Testing the Working Partition

Trong cửa sổ Terminal, nhập các lệnh sau đây và nhấn Enter sau mỗi lệnh.

Những lệnh này thay đổi thư mục làm việc sang ổ đĩa trống, tạo một tập tin nhỏ trên nó và hiển thị danh sách các tập tin.

Lưu ý rằng lệnh cuối cùng bao gồm hai ký tự "L" viết thường - chúng không phải là ký tự "1" số.

- **cd /media/data**
- **echo test > foo**
- **ls -l**



Có một tệp tên foo đã được tạo và bây giờ partition đã sẵn sàng để có thể sử dụng

Acquiring an Image of the Whole Evidence Disk with dd

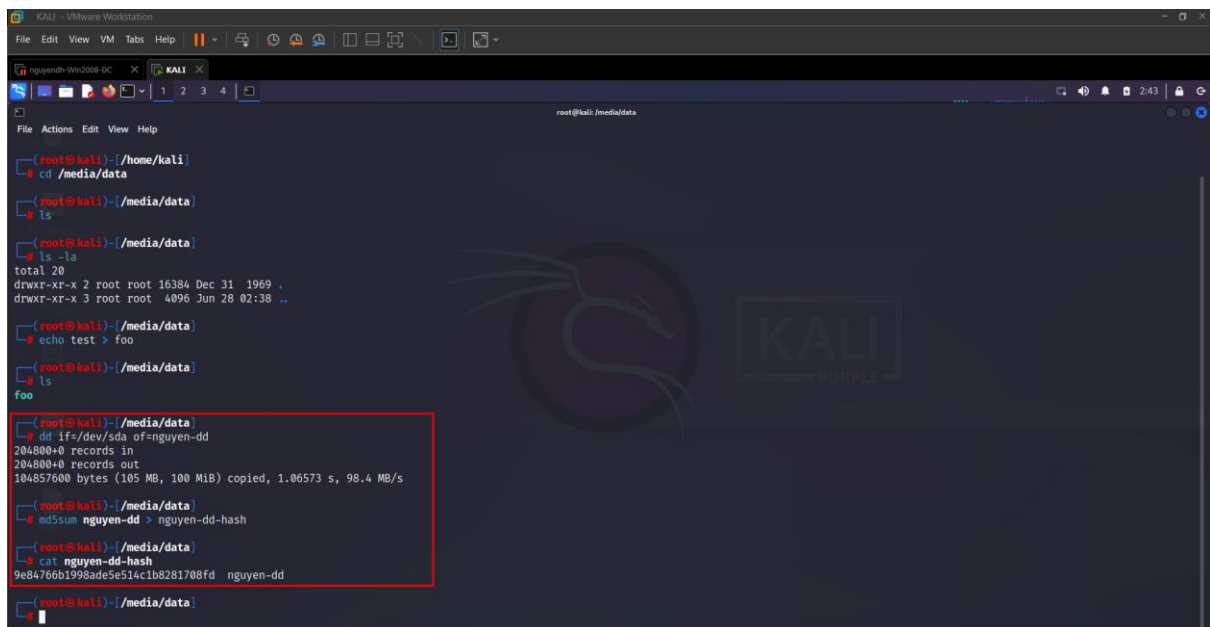
Trên cửa sổ Terminal, hãy nhập các lệnh sau đây và nhấn Enter sau mỗi lệnh.

Lưu ý: Hãy thay thế YOURNAME bằng tên của bạn trong các lệnh dưới đây.

1. Sao chép dữ liệu từ ổ đĩa chứa bằng lệnh dd và lưu vào một tập tin có tên YOURNAME-dd.
2. Tính toán mã băm MD5 bằng lệnh md5sum và lưu vào một tập tin có tên YOURNAME-dd-hash.
3. Hiển thị nội dung của tập tin YOURNAME-dd-hash bằng lệnh cat.

Hãy nhớ thay thế "/đường_dẫn/ổ_đĩa_chứa" bằng đường dẫn thực tế đến ổ đĩa chứa dữ liệu mà bạn muốn sao chép.

- **dd if=/dev/sda of=YOURNAME-dd**
- **md5sum nguyen-dd > nguyen-dd-hash**
- **cat YOURNAME-dd-hash**

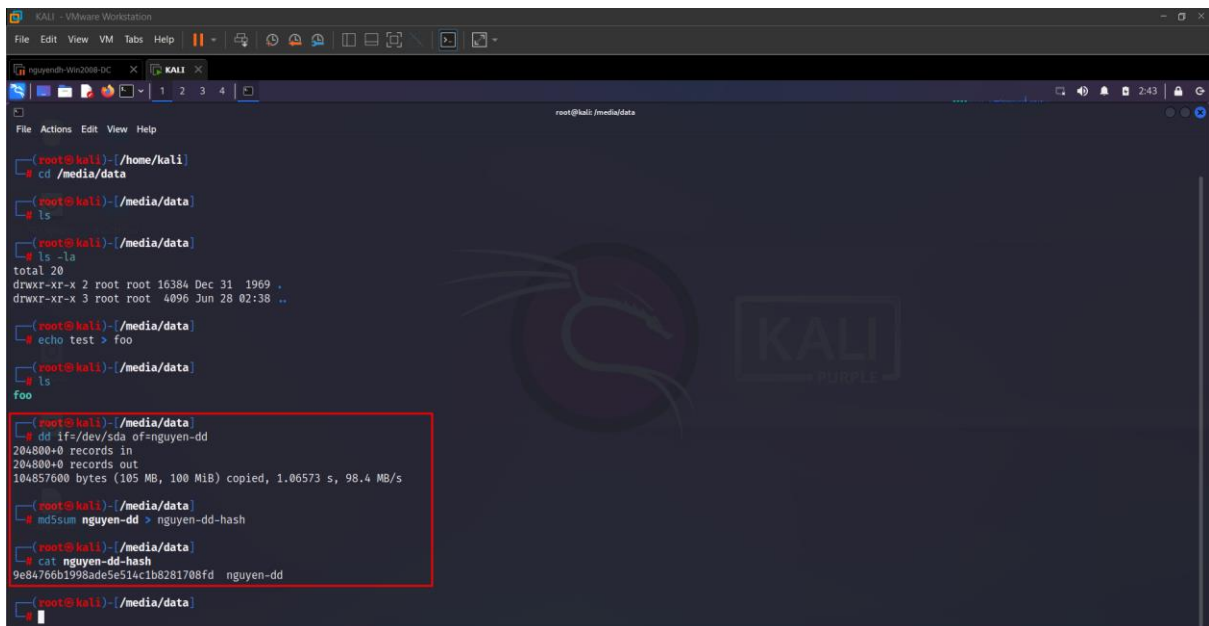
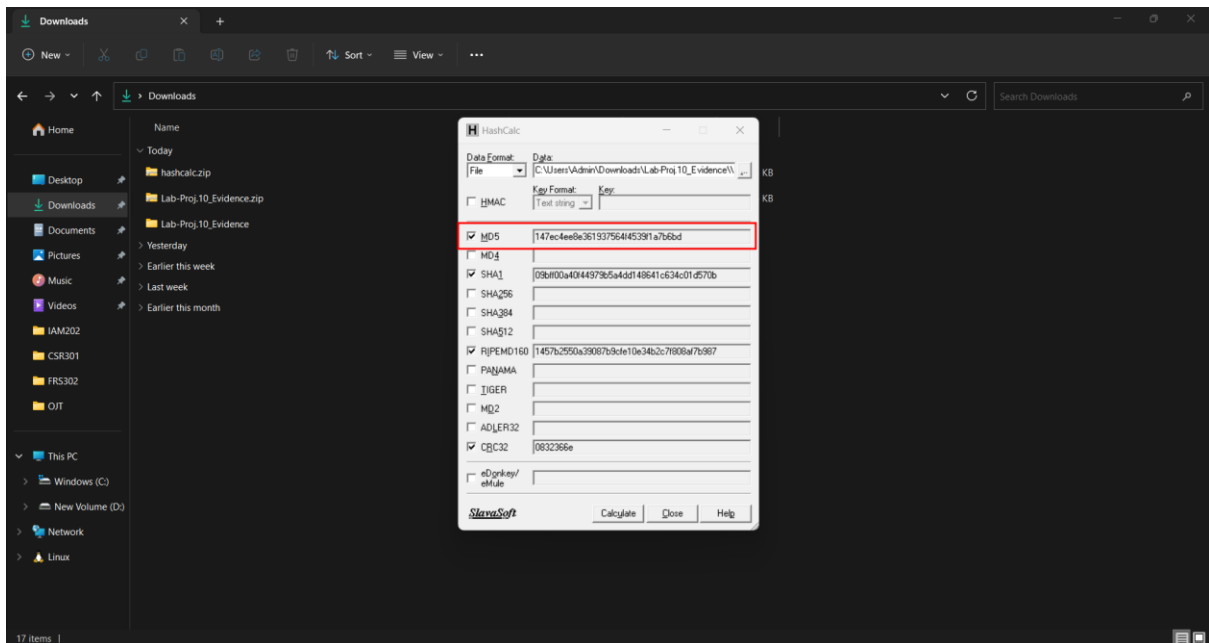


```
(root@kali)~/home/kali
# cd /media/data
(root@kali)~/media/data
# ls
(root@kali)~/media/data
# ls -la
total 20
drwxr-xr-x 2 root root 16384 Dec 31 1969 .
drwxr-xr-x 3 root root 4096 Jun 28 02:38 ..
(root@kali)~/media/data
# echo test > foo
(root@kali)~/media/data
# ls
foo
(root@kali)~/media/data
# dd if=/dev/sda of=nguyen-dd
204800+0 records in
204800+0 records out
104857600 bytes (105 MB, 100 MiB) copied, 1.06573 s, 98.4 MB/s
(root@kali)~/media/data
# md5sum nguyen-dd > nguyen-dd-hash
(root@kali)~/media/data
# cat nguyen-dd-hash
9e84766b1998ade5e514c1b8281708fd  nguyen-dd
(root@kali)~/media/data
```

Mã hash của chúng ta sẽ được hiển thị như hình bên trên

Comparing the Hash to the Hashcalc Value

Nếu so sánh hai mã hash MD5 với cái chúng ta đã tính toán từ trước thì hai mã không giống nhau. Bởi vì file đã được thêm header, rollback data và một số thứ khác đã làm đến md5sum bị thay đổi

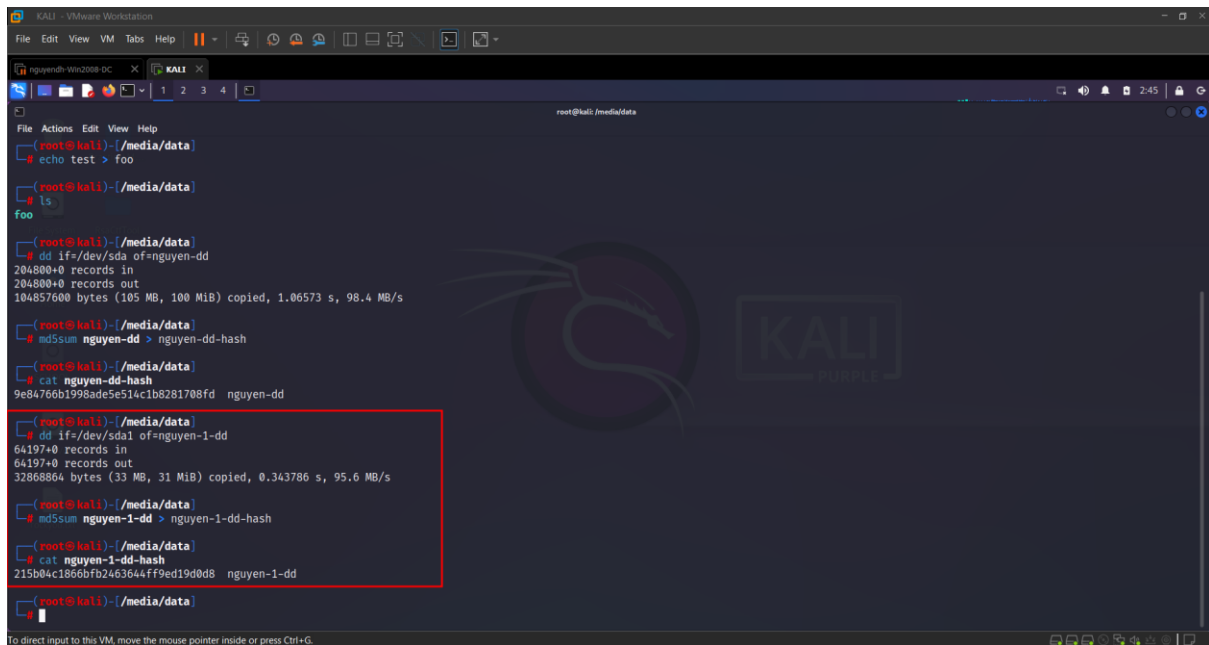


Acquiring an Image of One Partition with dd

Chúng ta cũng có thể sao lưu chỉ phân vùng từ ổ đĩa, có thể chứa tất cả dữ liệu mà chúng ta quan tâm, hoặc có thể chứa tất cả dữ liệu mà chúng ta được ủy quyền thu thập.

Trong cửa sổ Terminal, gõ các lệnh sau đây, nhấn Enter sau mỗi lệnh.

- **dd if=/dev/sda1 of=nguyen-1-dd**
- **md5sum nguyen-1-dd > nguyen-1-dd-hash**
- **cat YOURNAME-1-dd-hash**



```
(root@kali)~/media/data
# echo test > foo

(root@kali)~/media/data
# ls
foo

(root@kali)~/media/data
# dd if=/dev/sda of=nguyen-dd
204800+0 records in
204800+0 records out
104857600 bytes (105 MB, 100 MiB) copied, 1.06573 s, 98.4 MB/s

(root@kali)~/media/data
# md5sum nguyen-dd > nguyen-dd-hash

(root@kali)~/media/data
# cat nguyen-dd-hash
9e84766b1998ade5e514c1b8281708fd  nguyen-dd

(root@kali)~/media/data
# dd if=/dev/sda1 of=nguyen-1-dd
64197+0 records in
64197+0 records out
32868864 bytes (33 MB, 31 MiB) copied, 0.343786 s, 95.6 MB/s

(root@kali)~/media/data
# md5sum nguyen-1-dd > nguyen-1-dd-hash

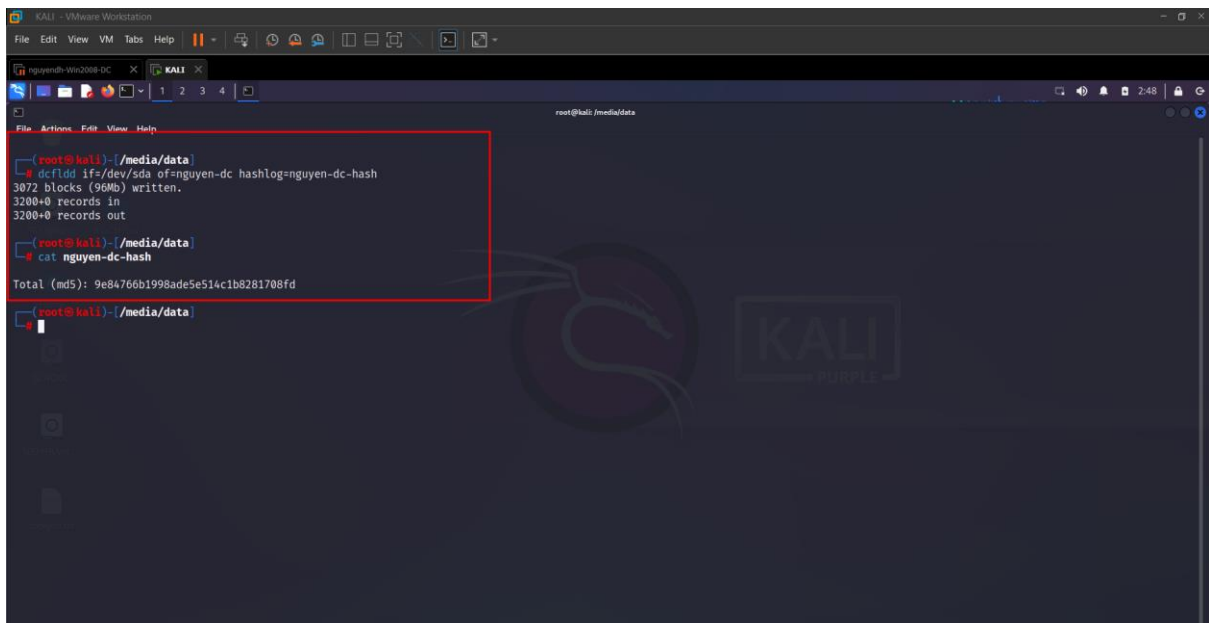
(root@kali)~/media/data
# cat nguyen-1-dd-hash
215b04c1866bfb2463644ff9ed19d0d8  nguyen-1-dd

(root@kali)~/media/data
#
```

Acquiring an Image of the Whole Evidence Disk with dcfldd

Trong terminal gõ các lệnh sau:

- **dcfldd if=/dev/sdc of=nguyen-dc hashlog=nguyen-dc-hash**
- **cat nguyen-dc-hash**



```
(root@kali)~/media/data
# dcfldd if=/dev/sda of=nguyen-dc hashlog=nguyen-dc-hash
3072 blocks (96MB) written.
3200+0 records in
3200+0 records out

Total (md5): 9e84766b1998ade5e514c1b8281708fd

(root@kali)~/media/data
# cat nguyen-dc-hash
```

Using dcfldd to Verify the Image

Trong terminal gõ các lệnh sau:

- **dcfldd if=/dev/sda vf=nguyen-dd**

Giá trị vf value dùng để so sánh với giá trị được truyền vào bên trong if.

Kết quả "Total: Match", được hiển thị như hình bên dưới.

```
(root@kali)-[/media/data]
# dd if=/dev/sda of=nguyen-dc hashlog=nguyen-dc-hash
3072 blocks (96MB) written.
3200+0 records in
3200+0 records out

(root@kali)-[/media/data]
# cat nguyen-dc-hash
Total (md5): 9e84766b1998ade5e514c1b8281708fd

(root@kali)-[/media/data]
# dd if=/dev/sda vf=nguyen-dd
Total: Match

(root@kali)-[/media/data]
```

Testing the Effects of an Error

Nếu bạn mắc lỗi khi thực hiện một lệnh và ghi vào ổ đĩa chứa bằng chứng, điều gì sẽ xảy ra?

Trong cửa sổ Terminal, hãy nhập lệnh sau đây, sau đó nhấn Enter:

- `echo test > /dev/sda`

Việc này có làm hỏng dữ liệu chứng cứ không? Để kiểm tra, hãy chạy lại lệnh xác minh sau đây:

- `dd if=/dev/sda vf=proj10-dd`

```
(root@kali)-[/media/data]
# dd if=/dev/sda of=nguyen-dc hashlog=nguyen-dc-hash
3072 blocks (96MB) written.
3200+0 records in
3200+0 records out

(root@kali)-[/media/data]
# cat nguyen-dc-hash
Total (md5): 9e84766b1998ade5e514c1b8281708fd

(root@kali)-[/media/data]
# dd if=/dev/sda vf=nguyen-dd
Total: Match

(root@kali)-[/media/data]
# echo test > /dev/sda

(root@kali)-[/media/data]
# dd if=/dev/sda vf=nguyen-dd
0 - 0: Mismatch
Total: Mismatch

(root@kali)-[/media/data]
```

Như chúng ta đã thấy, tệp không còn khớp với ổ đĩa. Chứng cứ đã bị thay đổi! Vì vậy, mặc dù kỹ thuật này hoạt động, nhưng nó không tốt bằng việc sử dụng một thiết bị chặn ghi phân cứng.