LAB 05

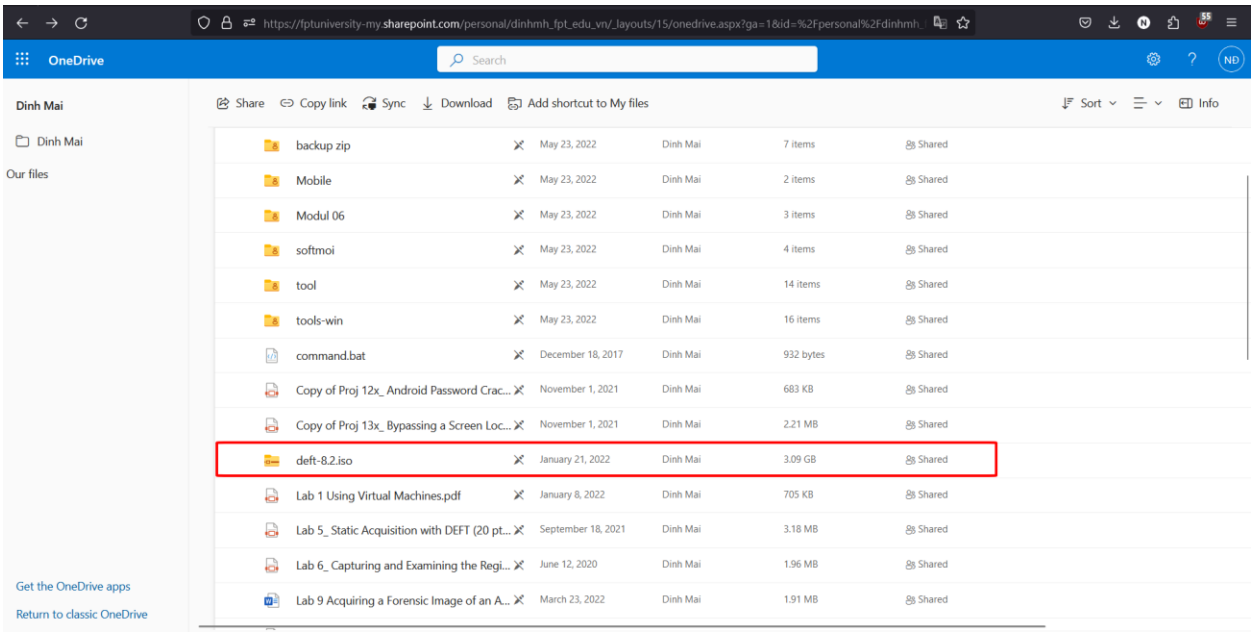
Thầy Mai Hoàng Đỉnh
Trường đại học FPT

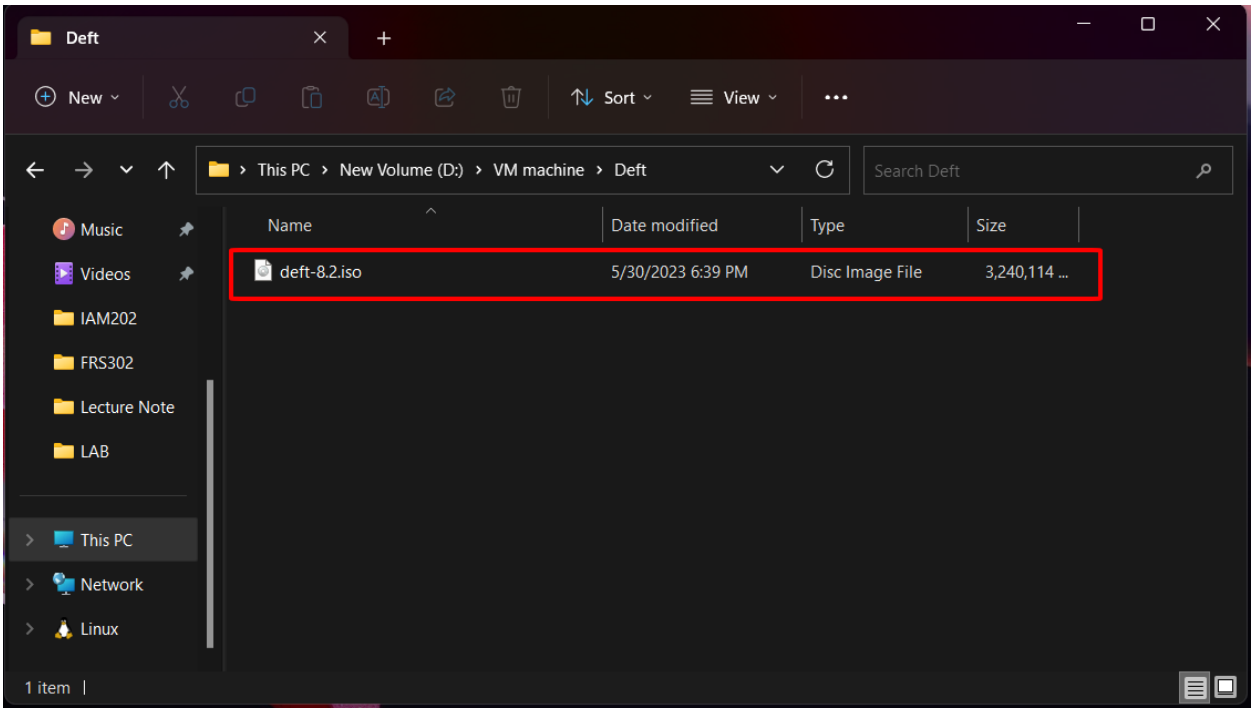
Người thực hiện

Đặng Hoàng Nguyên

Downloading DEFT

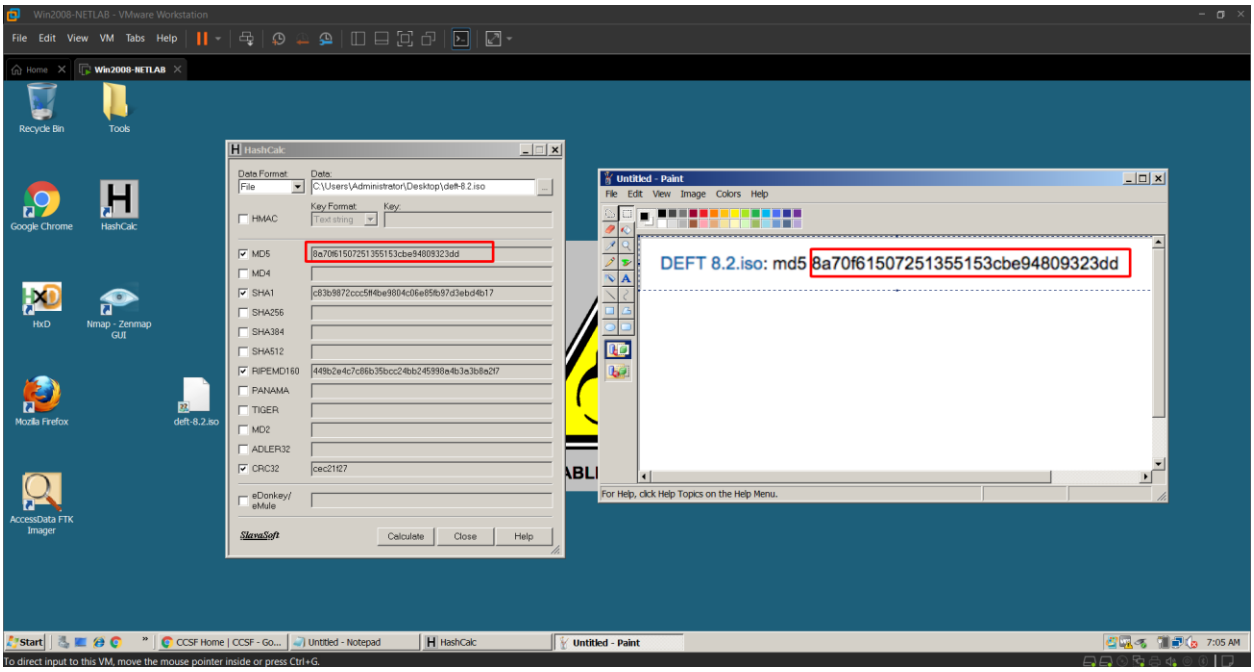
Bên trong onedrive, ta sẽ tải một file có tên là deft-8.2.iso với dung lượng là 3.09GB. Sau khi download xong, chúng ta sẽ có một file iso





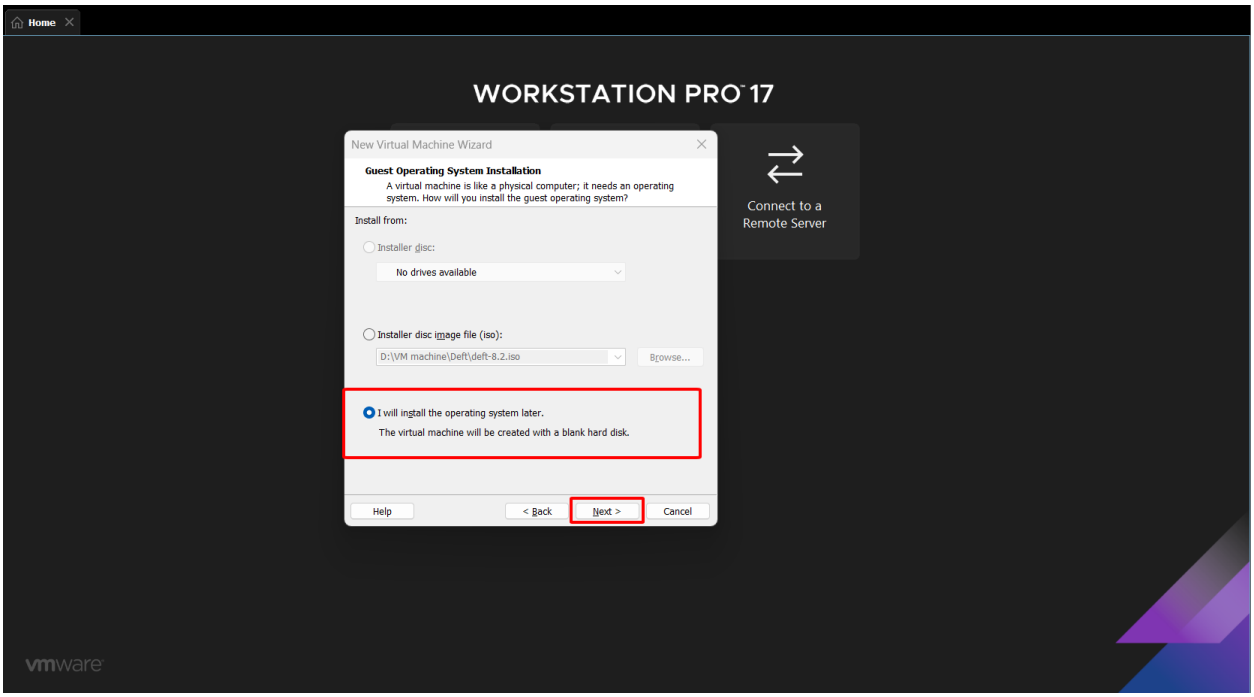
Sau đó sử dụng một công cụ có tên là hashcalc để có thể tính xem mã hash của nó là bao nhiêu, để đảm bảo rằng đây không phải là một file chứa virus. Vì máy Window server 2008 đã có HashCalc nên em sẽ import vào bên trong máy và bắt đầu tính hash của nó.

Như ta có thể thấy hình bên trái (hashcalc) và md5 iso của bài lab đưa là hoàn toàn trùng khớp nên chúng ta sẽ tiếp tục cài đặt máy ảo thông qua file iso

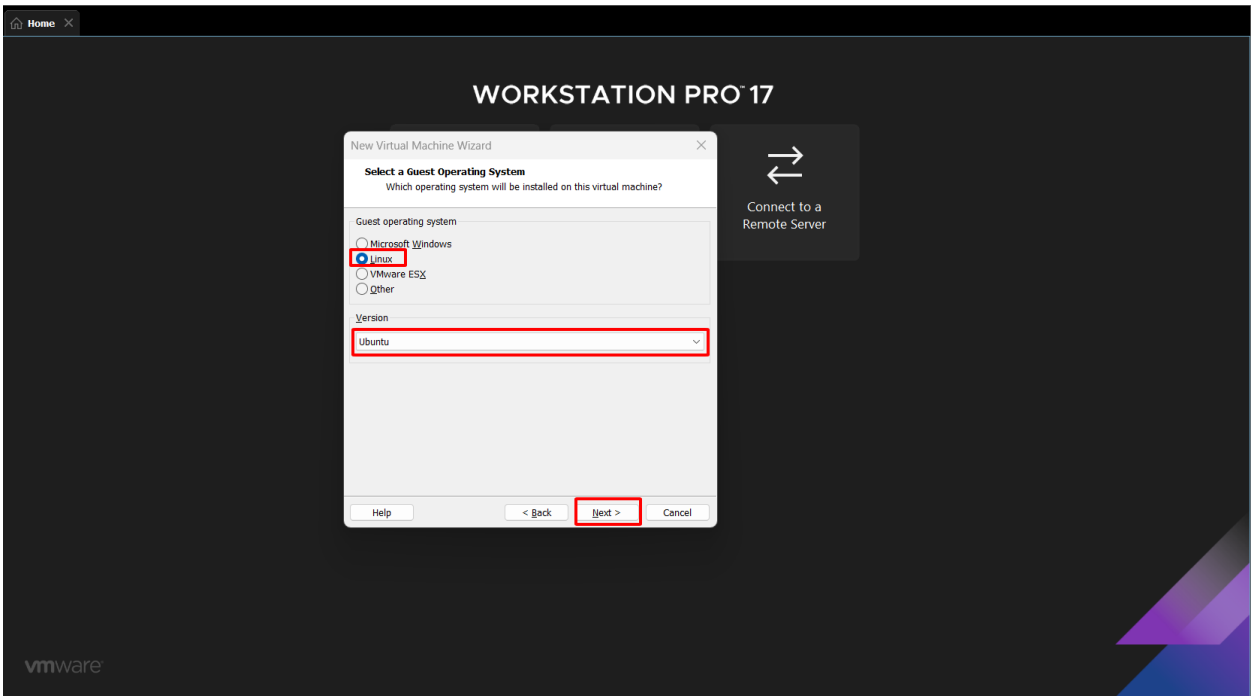


Creating a New Virtual Machine

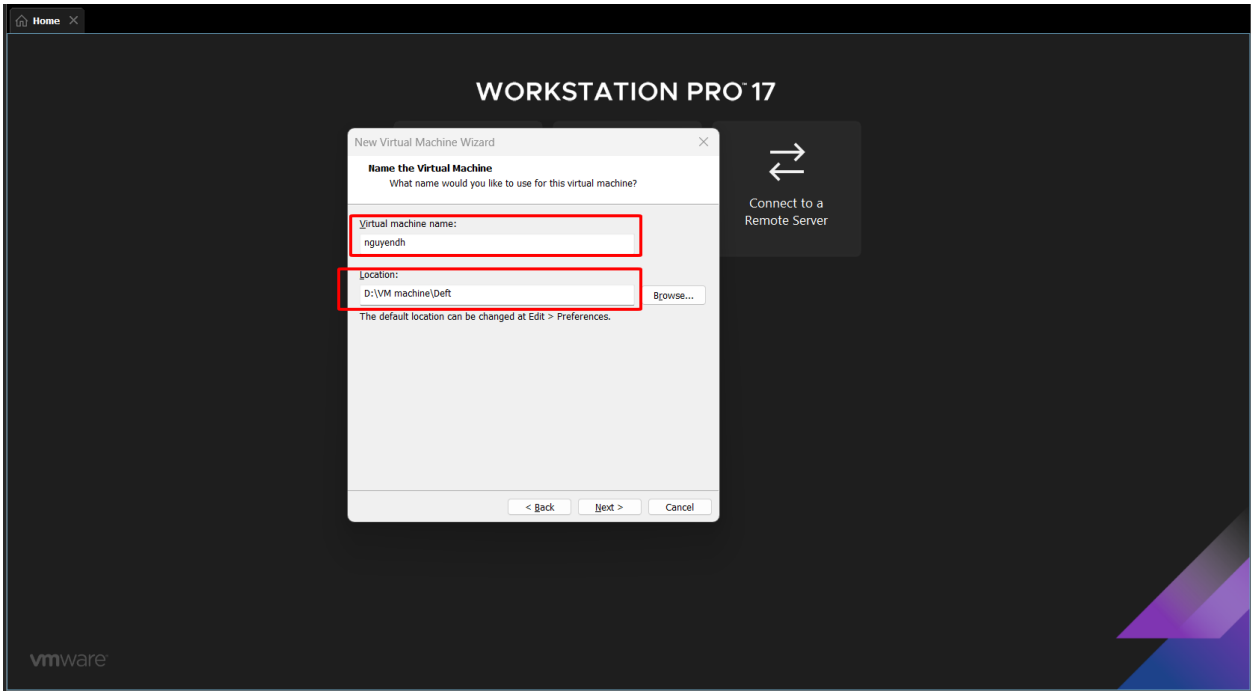
Trong VMware, chúng ta nhấn tổ hợp **ctrl + N**, sau đó nhấn chọn **custome**, sau đó nhấn chọn **"I will install the operating system later"** và sau đó nhấn **next**



Trong phần "Select a Guest Operating System" chọn lần lượt **Linux** và **Ubuntu** như hình bên dưới và chọn **Next**

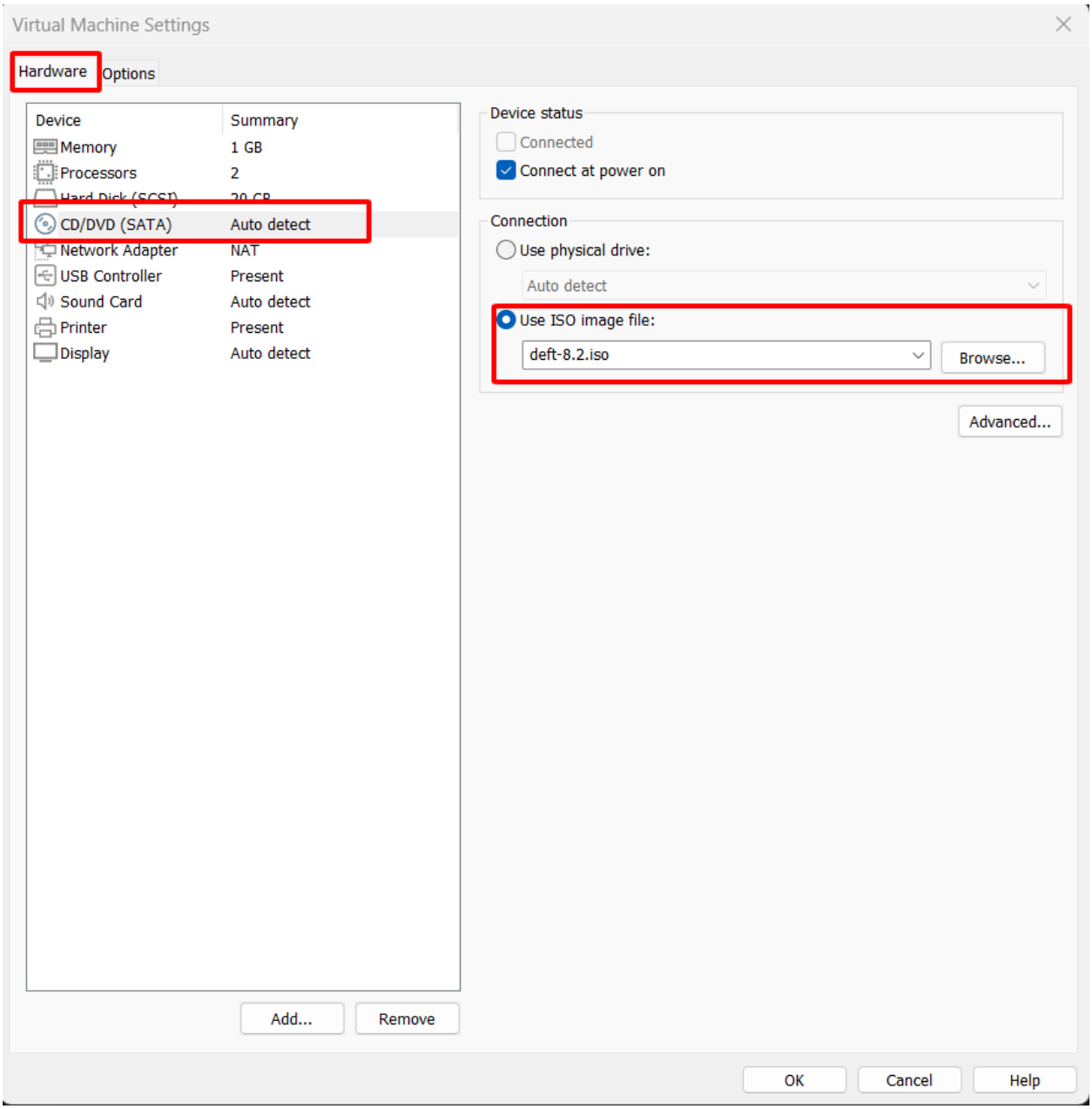


Trong phần "Name the Virtual Machine", nhập tên của máy ảo vào và đường dẫn để lưu máy ảo. Trong trường hợp này sẽ là **nguyendhse171946** và thư mục chứ là D:\\VM machine\Deft

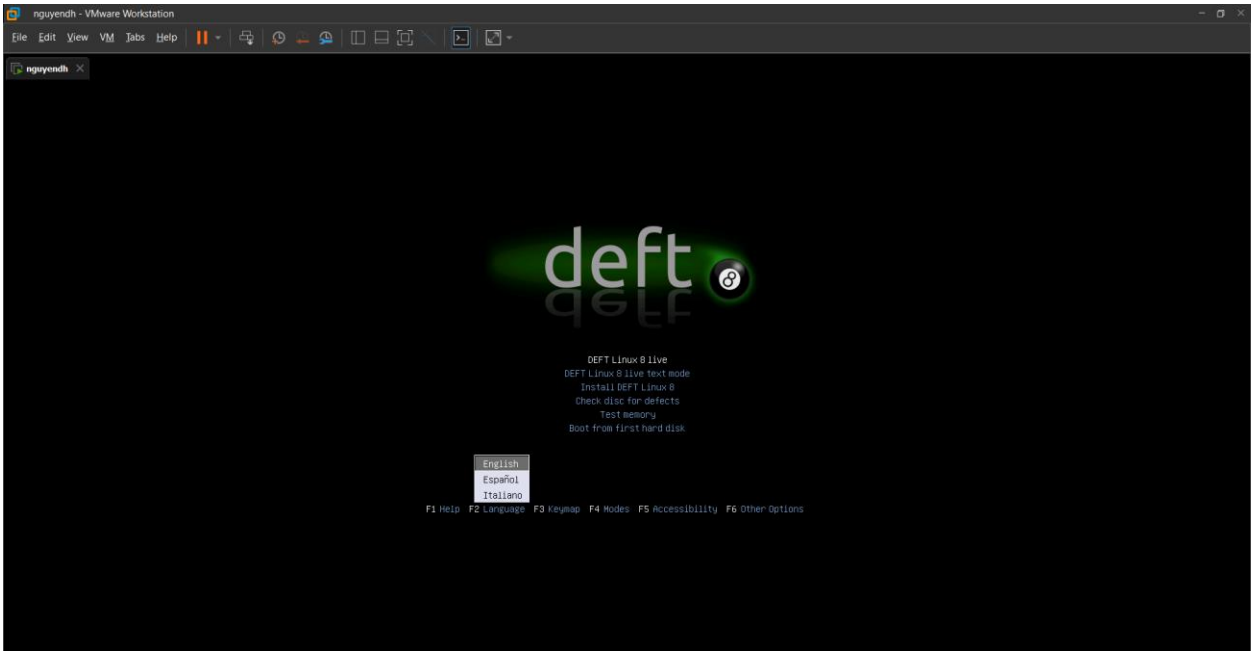


Sau đó chọn số nhân số luồng, số ram, các mục này có thể thay đổi sau, cứ nhấn next cho đến khi kết thúc. Thành công nó sẽ hiện bảng màn hình máy tính, sau đó nhấn Edit virtual machine settings để cho load file iso để hoạt động

Sau đó vào mục CD/DVD thay đổi mục Use physical drive thành use ISO và chỉ tới thư mục chứa file ISO mà ta đã tải. Sau khi thiết lập xong, click **OK** và bắt đầu khởi động máy



Sau khi boot lên ta có được màn hình như sau:

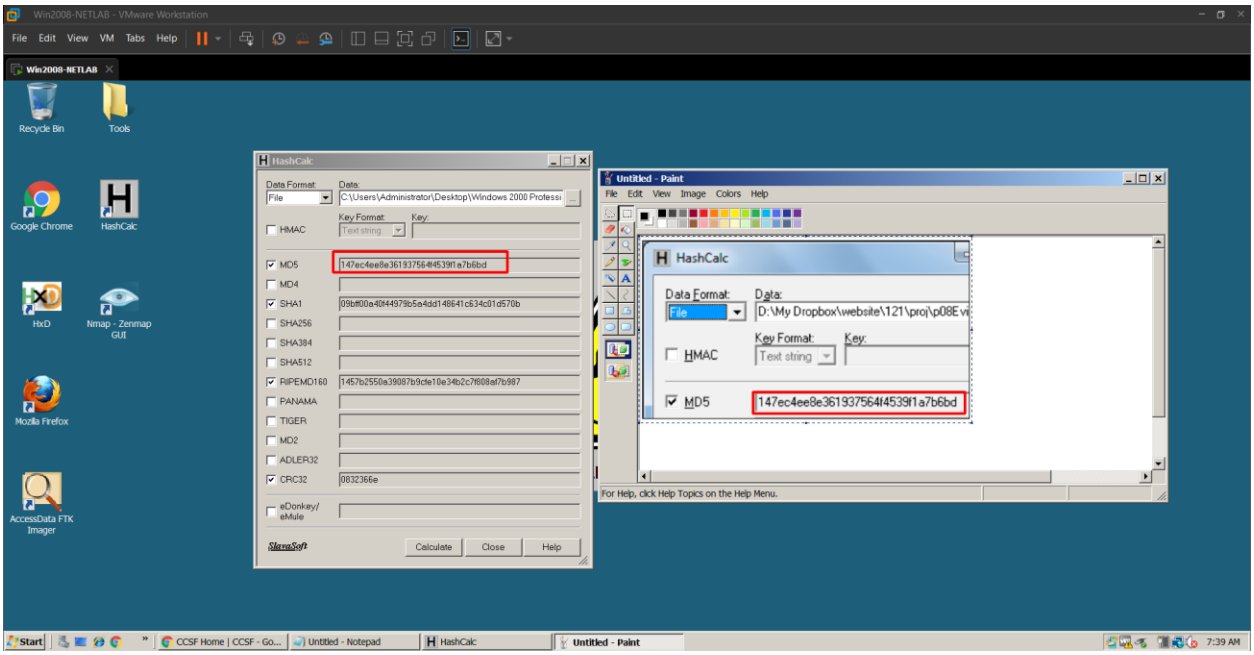


Preparing the Evidence Drive

Link tải: https://samsclass.info/121/proj/p10Evidence.zip

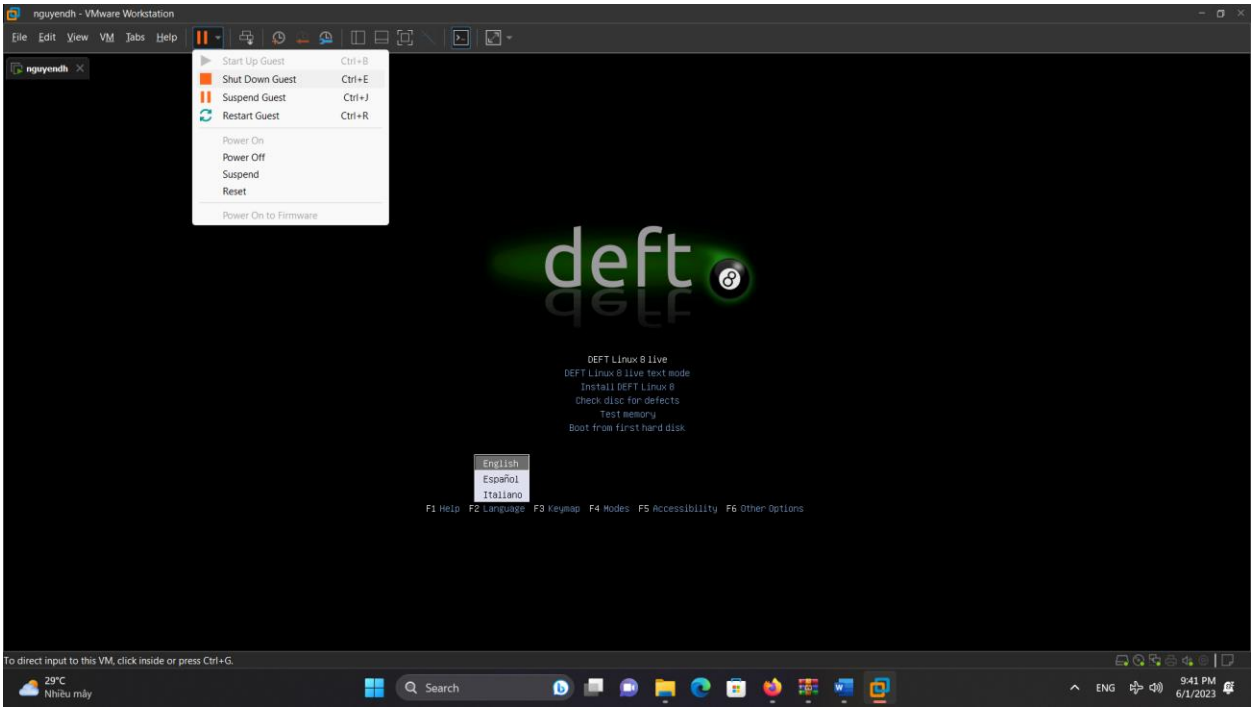
Sau khi tải xong, ta sẽ bắt đầu giải nén bên trong, đó là một file máy ảo của **Windows 2000 Professional**

Sau đó chúng ta sẽ kiểm tra md5 hash của file bằng HashCalc. Nhìn thấy rằng hai mã MD5 này hoàn toàn y chang nhau



Connecting the Evidence Drive

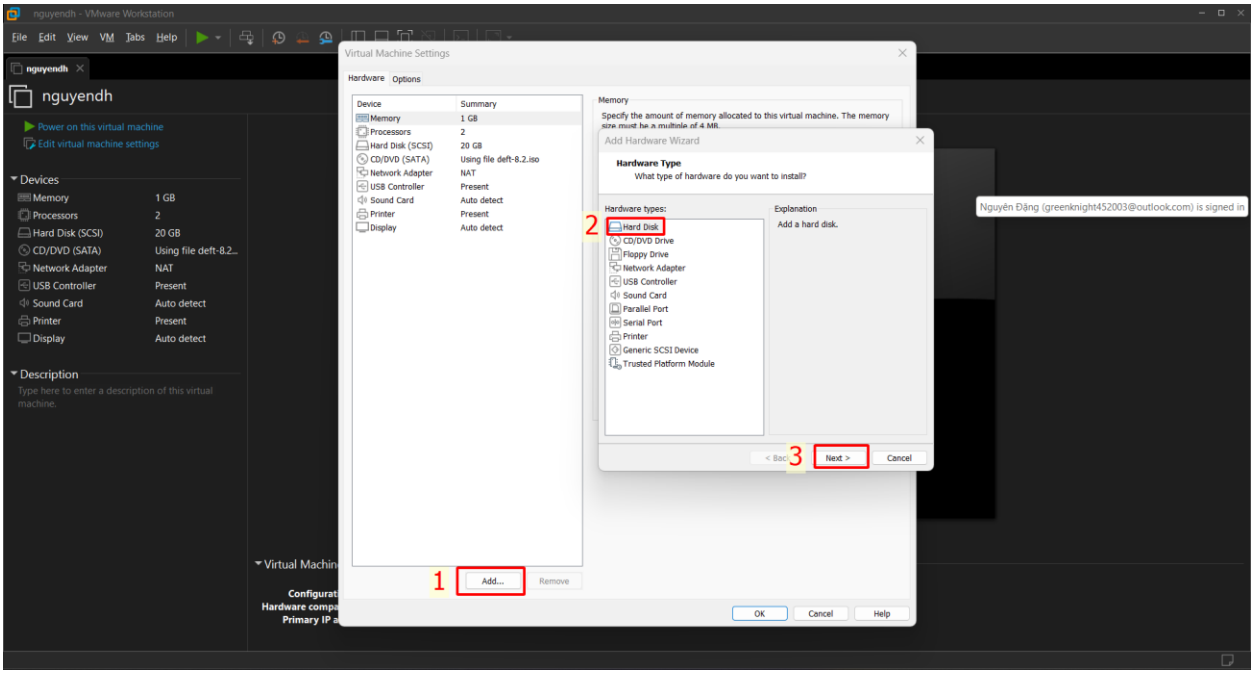
Bên máy ảo Deft, ta sẽ tiến hành tắt máy ảo nóng bằng phím tắt **Ctrl + E**



Sau khi tắt xong, ta sẽ vào lại Edit virtual machine setting, giống như lúc chỉnh iso đĩa cho máy ảo.

Trong **Virtual Machine Settings** nhấn vào nút **add** để thêm ổ đĩa hay là bất cứ thứ gì có thể thêm vào trong máy ảo

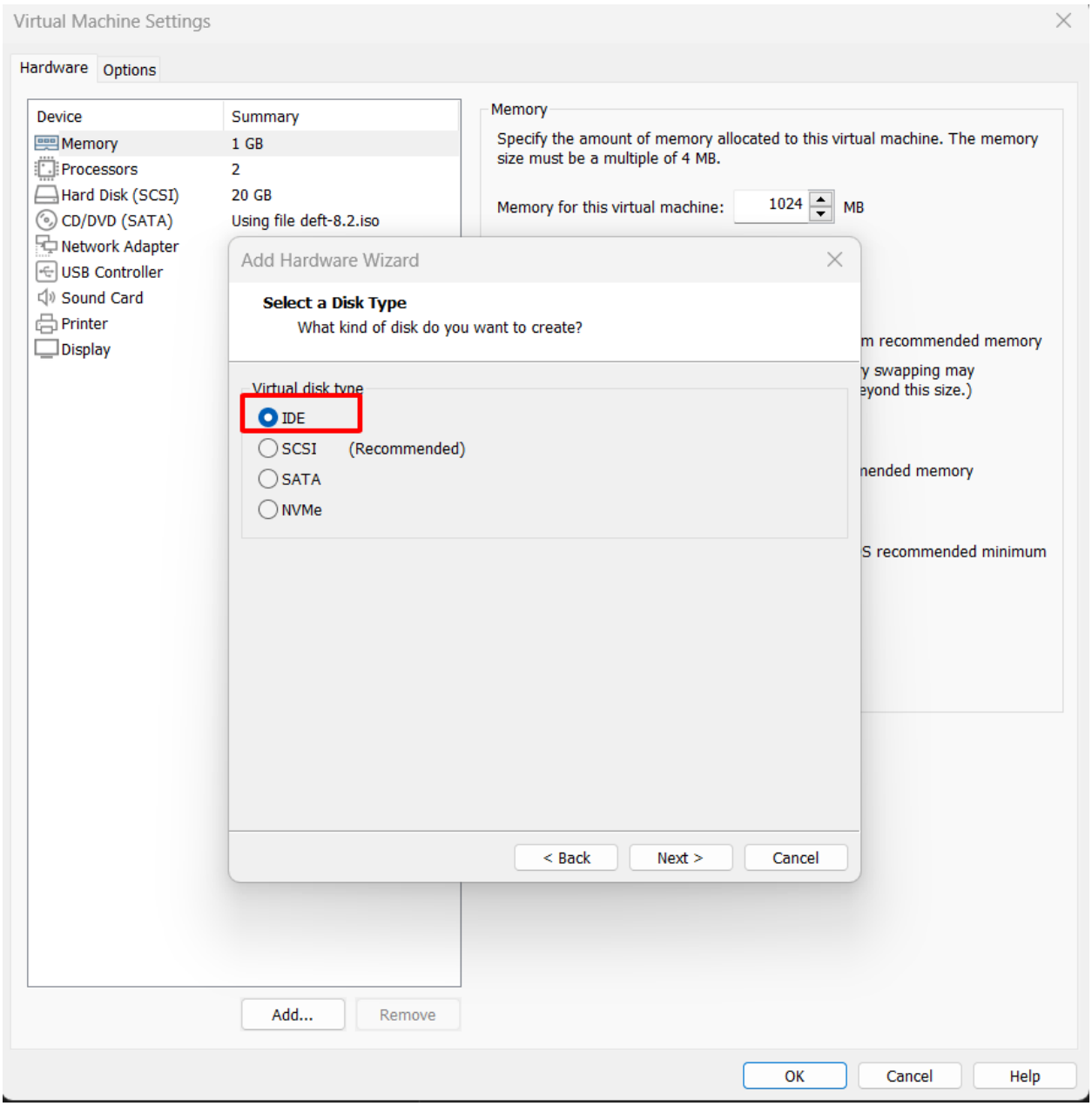
Trong phần "**Hardware type"** Chọn **Hard disk** để tạo thêm một ổ đĩa và nhấn next

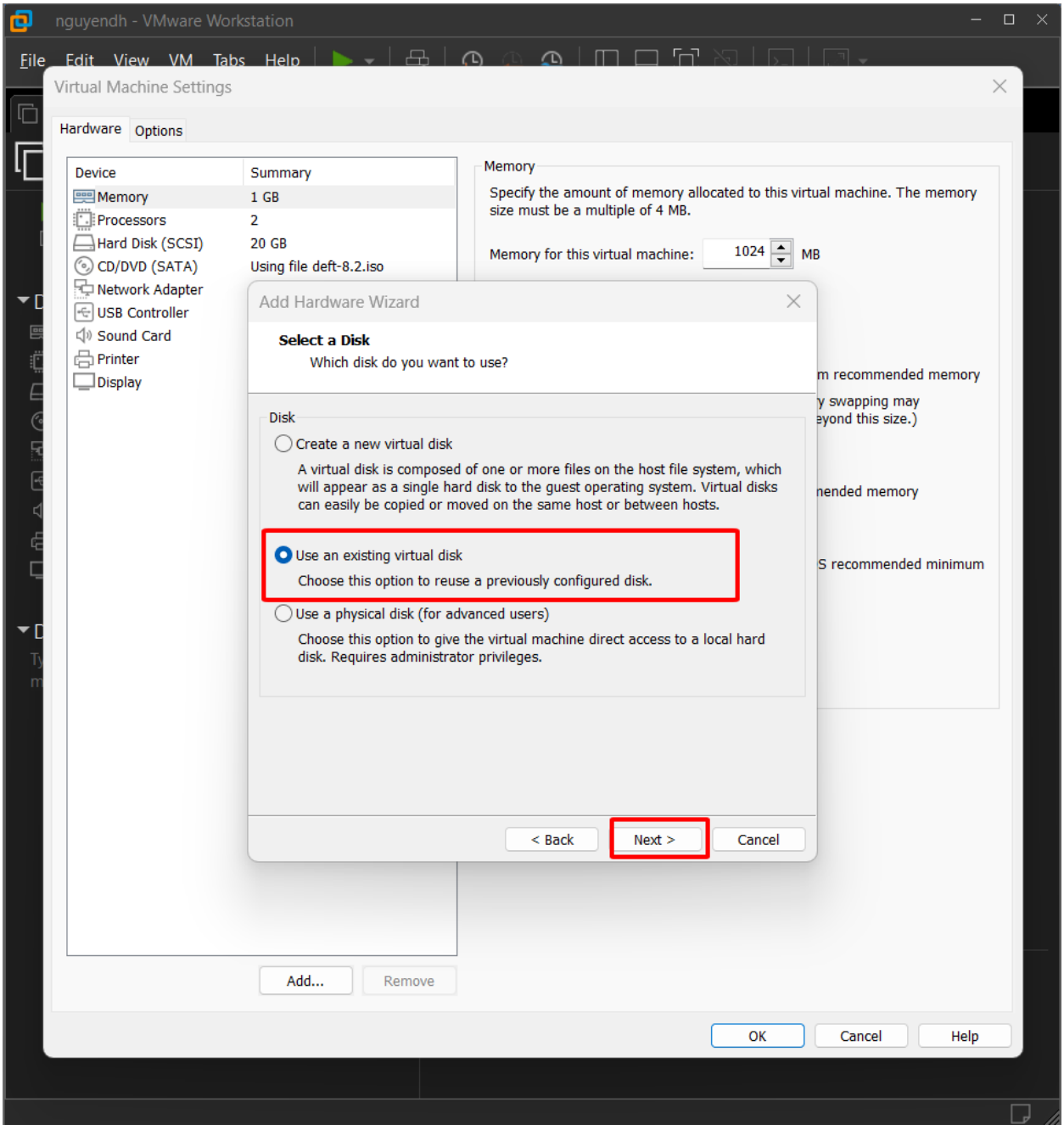


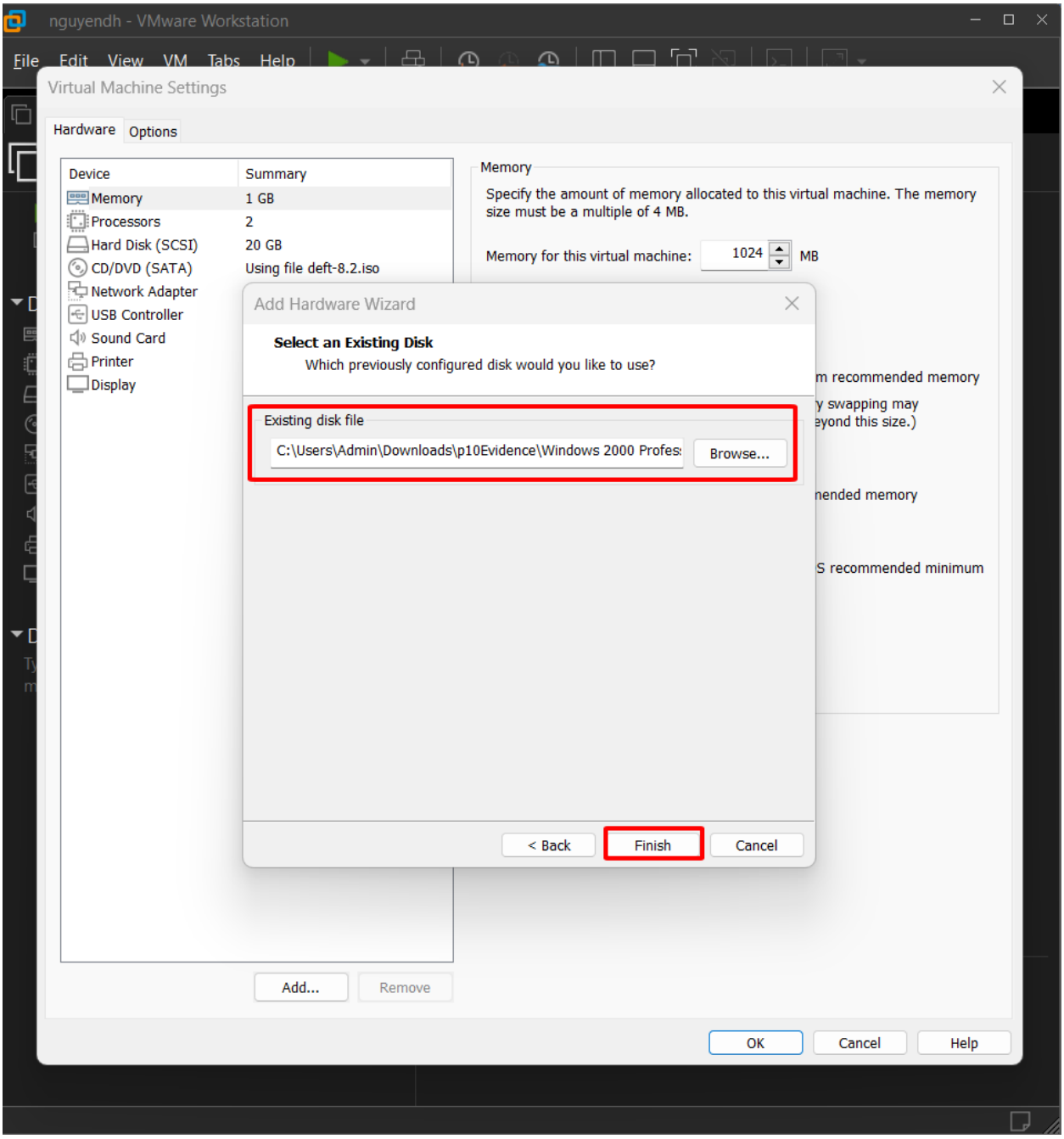
Sau đó nếu có hỏi về loại ổ đĩa mà chunsgt a muốn thêm vào nhấn chọn **IDE**

Trong phần **Select a Disk**, chọn **Use an existing virtual disk** và nhấn **Next**

Trong phần **Select an Existing Disk** chọn vào phần **Browse** và chọn vào phần file Windows 2000 mà ta đã giải nén ra và click **Finish**




nguyendh - VMware Workstation
File Edit View VM Tabs Help
Virtual Machine Settings
Hardware Options
Device Summary
Memory 1 GB
Processors 2
Hard Disk (SCSI) 20 GB
CD/DVD (SATA) Using file deft-8.2.iso
Network Adapter
USB Controller
Sound Card
Printer
Display
Add... Remove
Memory
Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.
Memory for this virtual machine: 1024 MB
Add Hardware Wizard
Select a Disk
Which disk do you want to use?
Disk
Create a new virtual disk
A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts.
Use an existing virtual disk
Choose this option to reuse a previously configured disk.
Use a physical disk (for advanced users)
Choose this option to give the virtual machine direct access to a local hard disk. Requires administrator privileges.
< Back Next > Cancel
OK Cancel Help

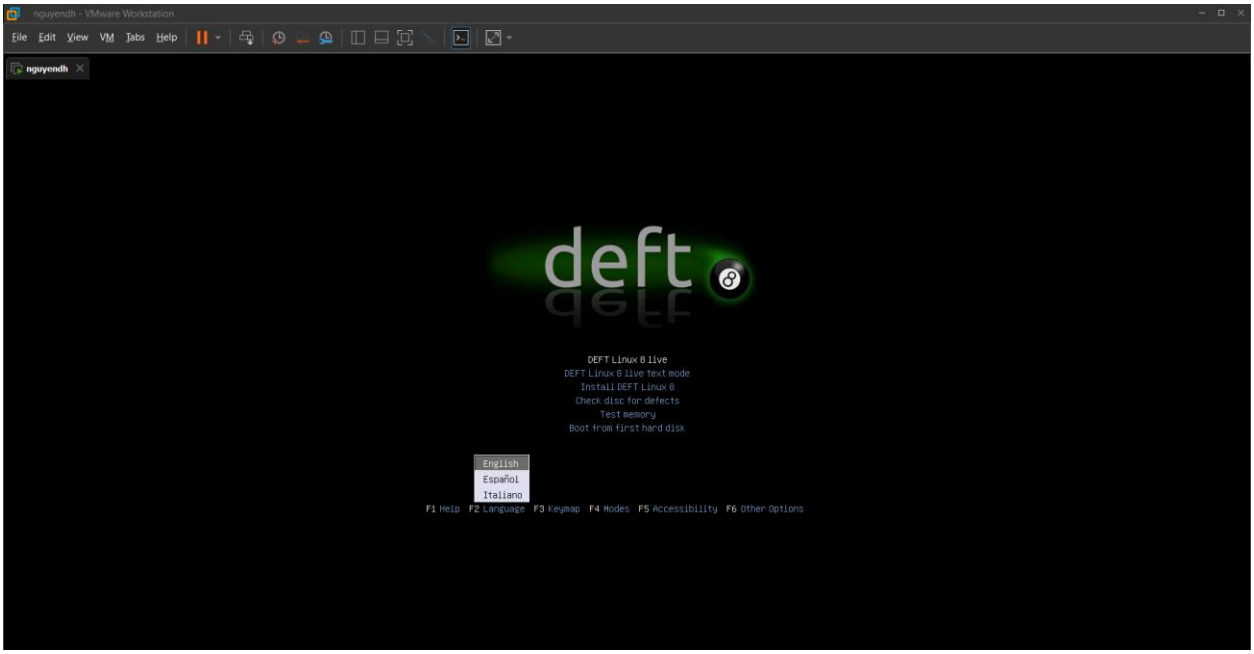


Booting from the DEFT ISO

Bật máy ảo lên

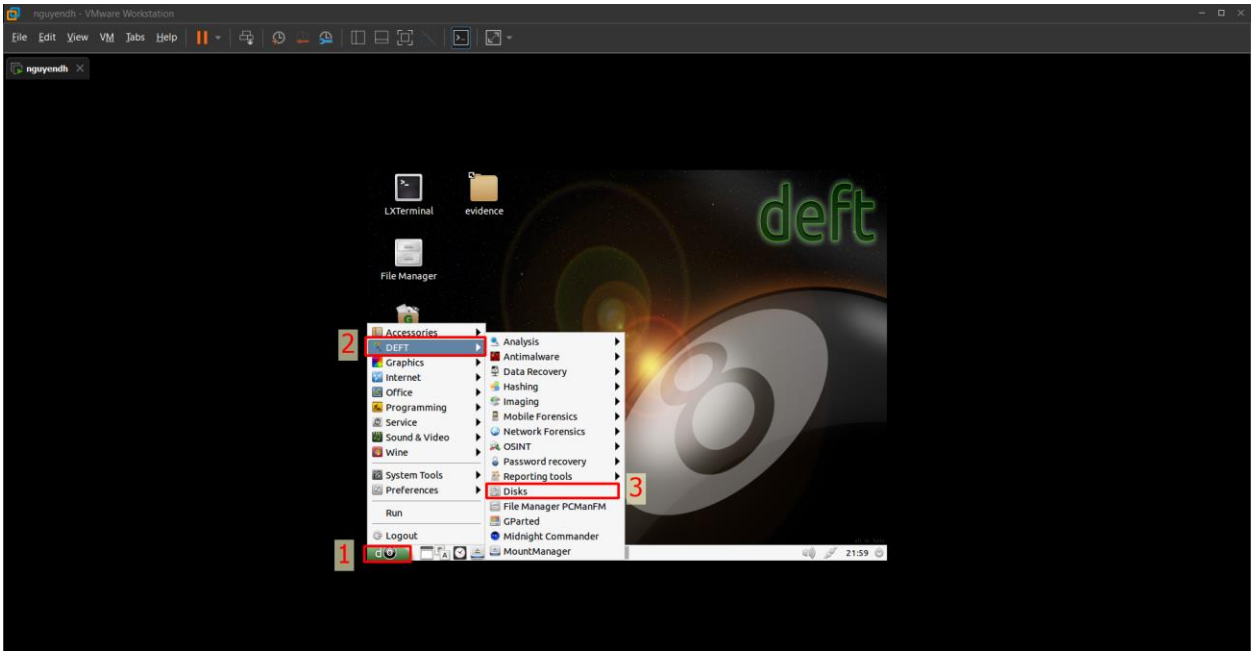
Có một prompt boot:. Bấm phím Enter.

Khi vòa được màn hình boot, như hình bên dưới. Nhấn Enter để chấp nhận ngôn ngữ mặc định là tiếng Anh. Nhấn Enter để chấp nhận lựa chọn khởi động mặc định của "DEFT Linux 8 LIVE".

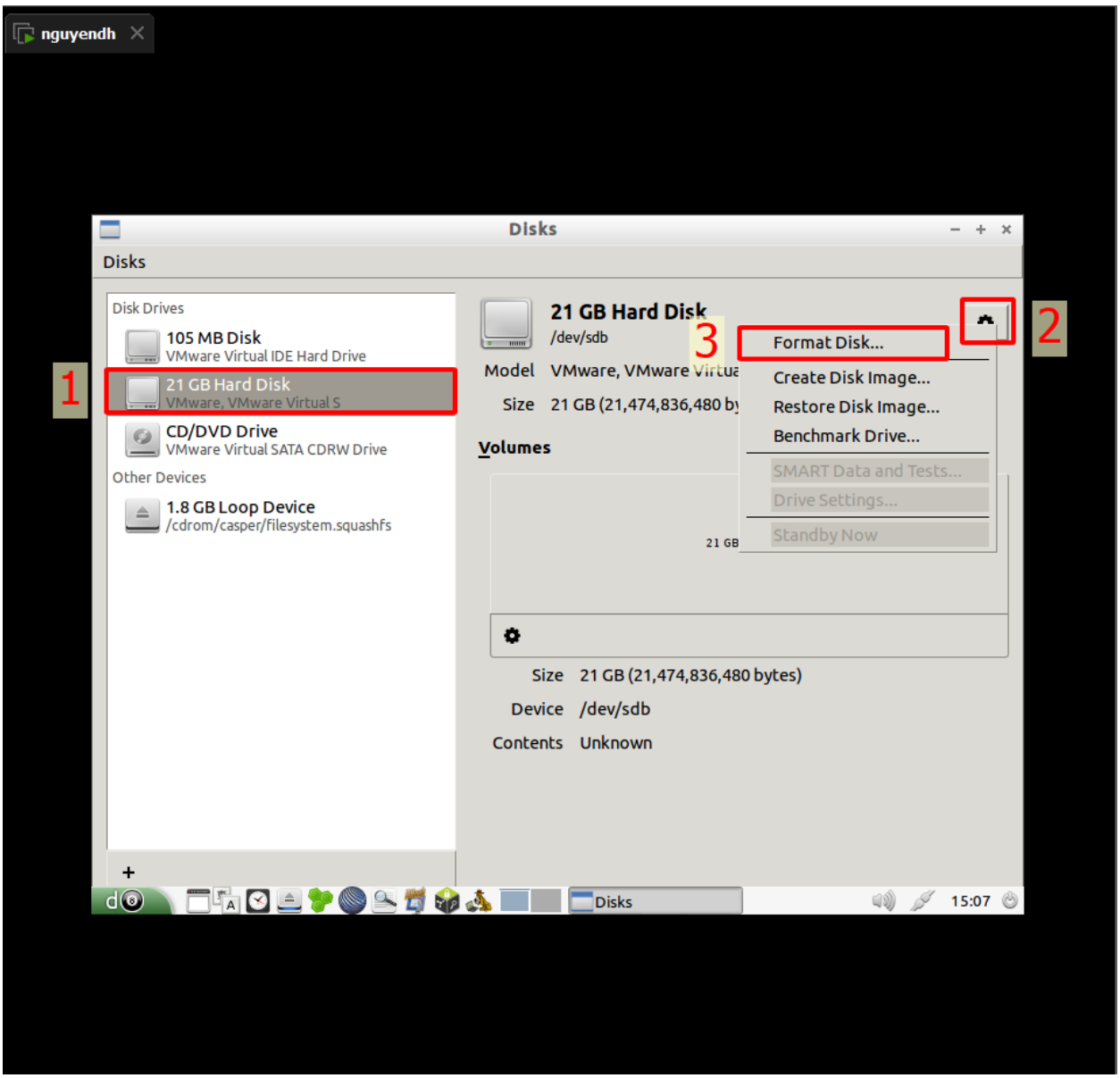


Preparing a Partition to Acquire Data

Sau khi vào được Desktop, ta sẽ chọn vào phần các ổ Đĩa bằng cách vào biểu tượng trái bi → DEFT → Disks. Sau khi nhấn vào, sẽ hiện ra một thông báo, nhấn vào "I know what I am doing" và tiếp tục

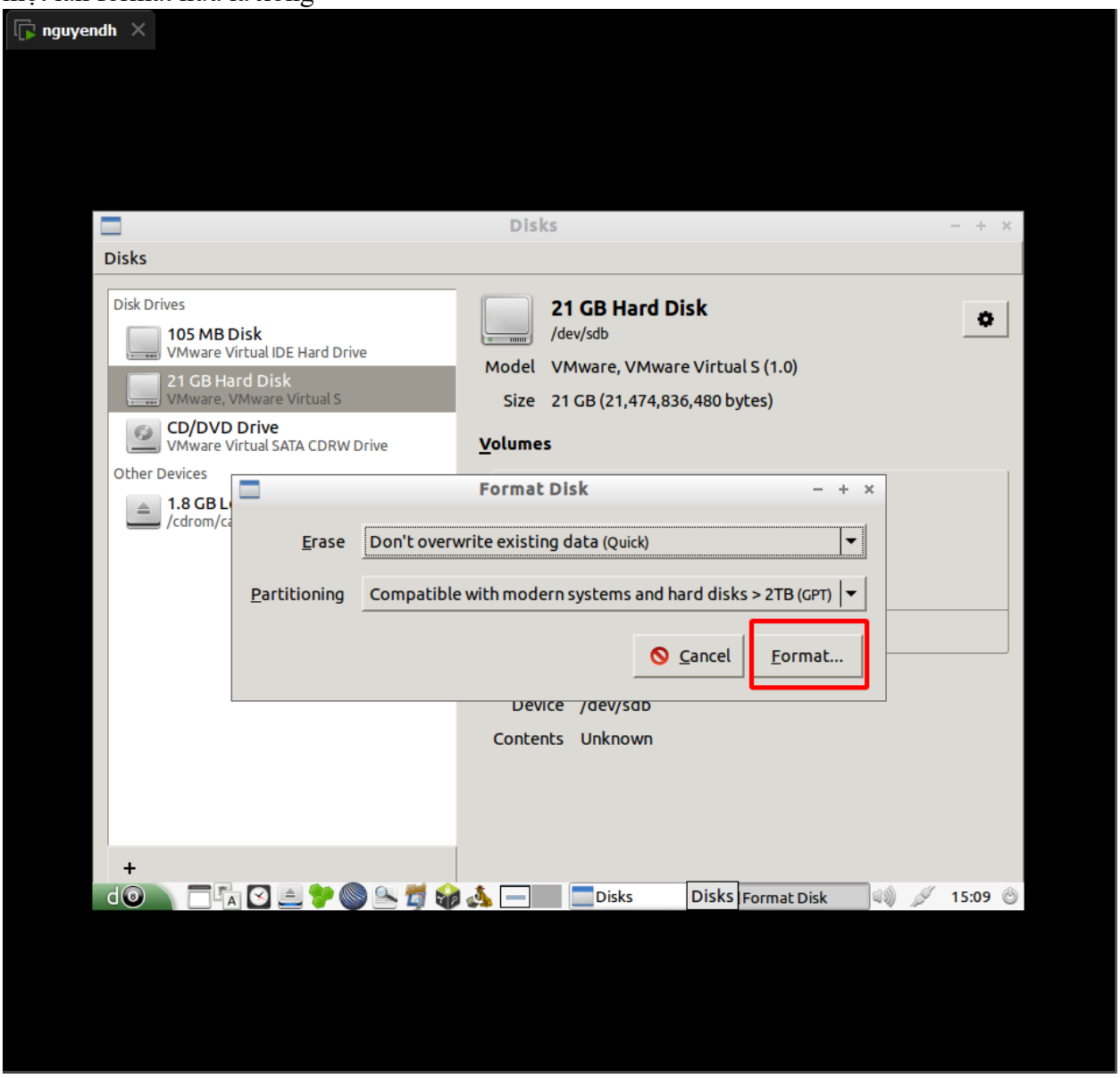


Bên trái có một ổ đĩa **21 GB Hard Disk.** Đây là ổ đĩa trống, nó có tên là unknown, đây là ổ chúng ta sẽ dung để capture image lại. Việc của chúng ta bây giờ sẽ phải format lại ổ đĩa theo hình dưới đây

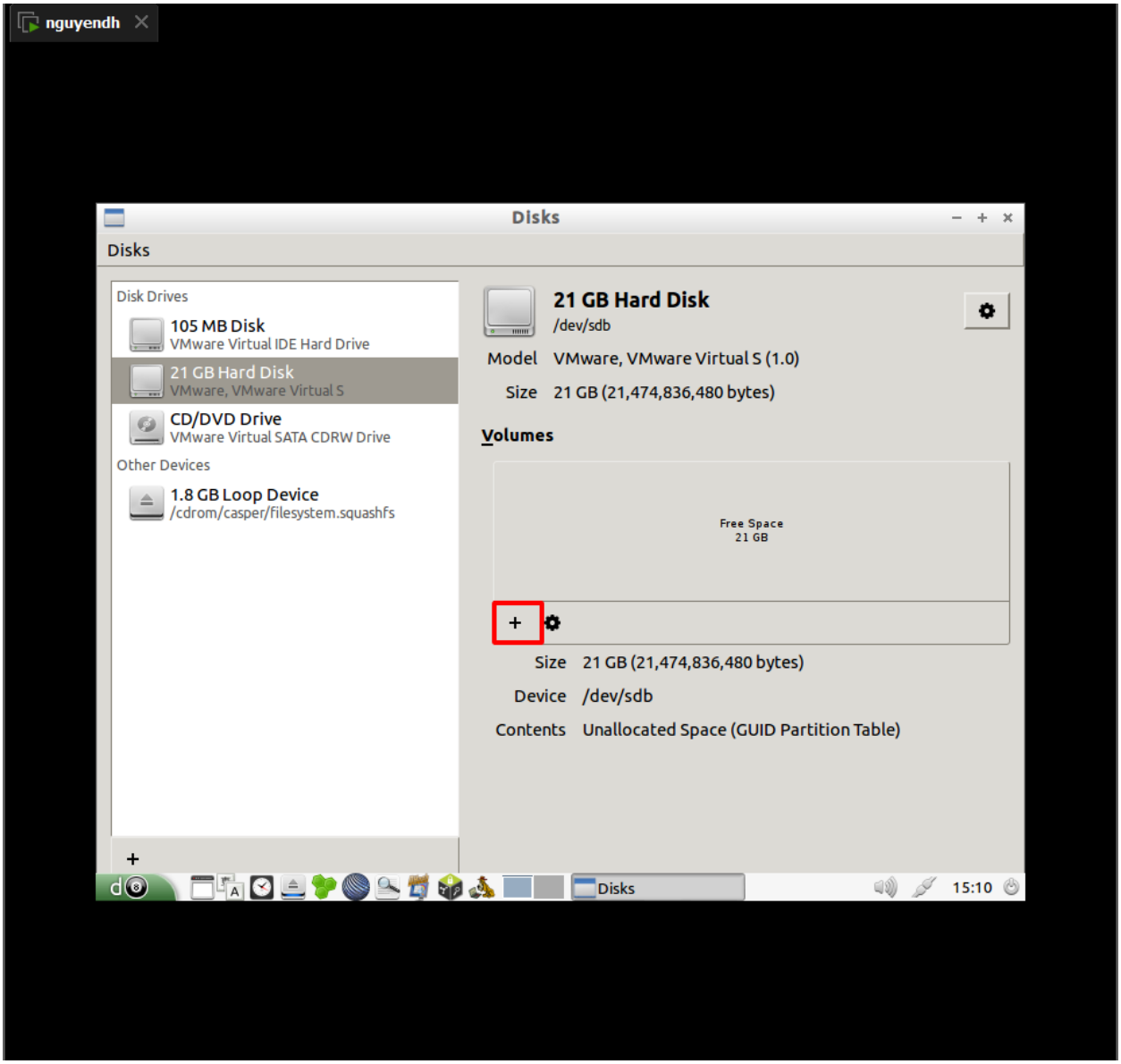


Sau khi nhấn **format disk**, sẽ có một thông báo hiện lên hỏi một số thông tin cơ bản cho ổ sau khi format, chúng ta chỉ cần để mặc định rồi nhấn format. Bên trong "Are you sure...", nhân thêm

một lần format nữa là xong



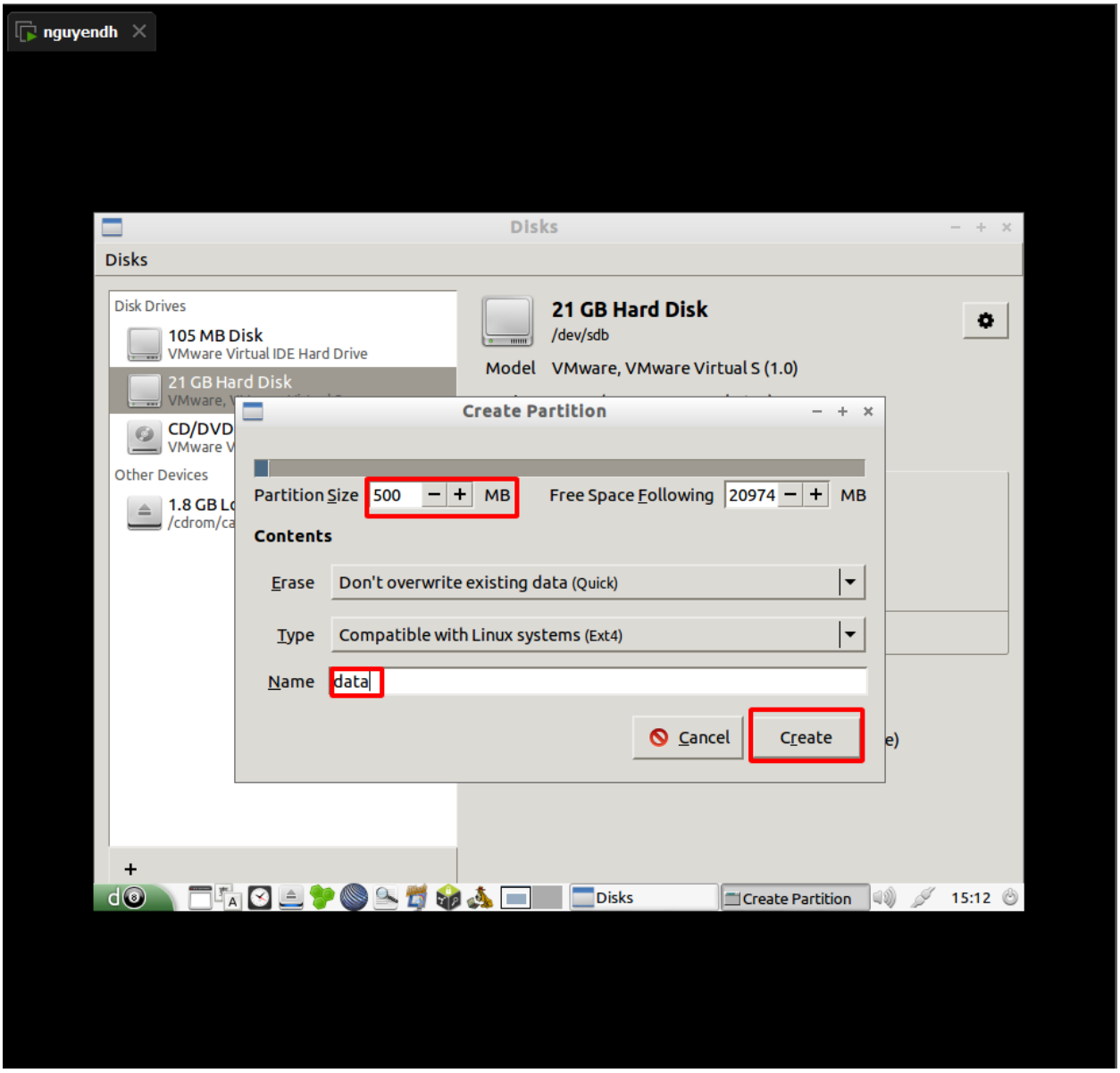
Sau khi format xong, ngay ổ đĩa, sẽ có một dấu cộng như hình dưới đây



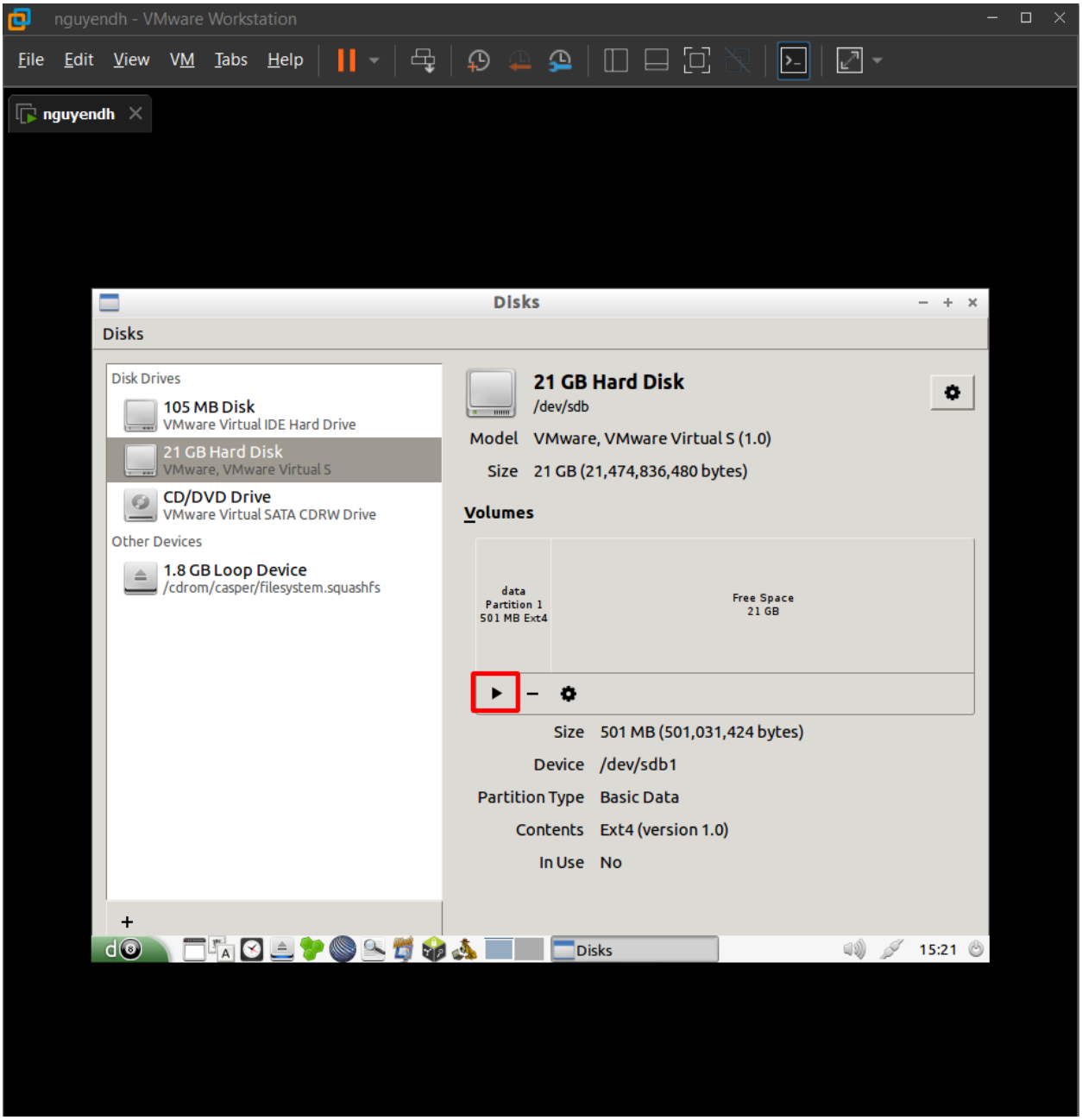
Nhấn vào dấu cộng đó, sẽ hiện ra một phần có tên gọi là “Create Partition”

Nhập partition size là 500 và tên của nó là **data**

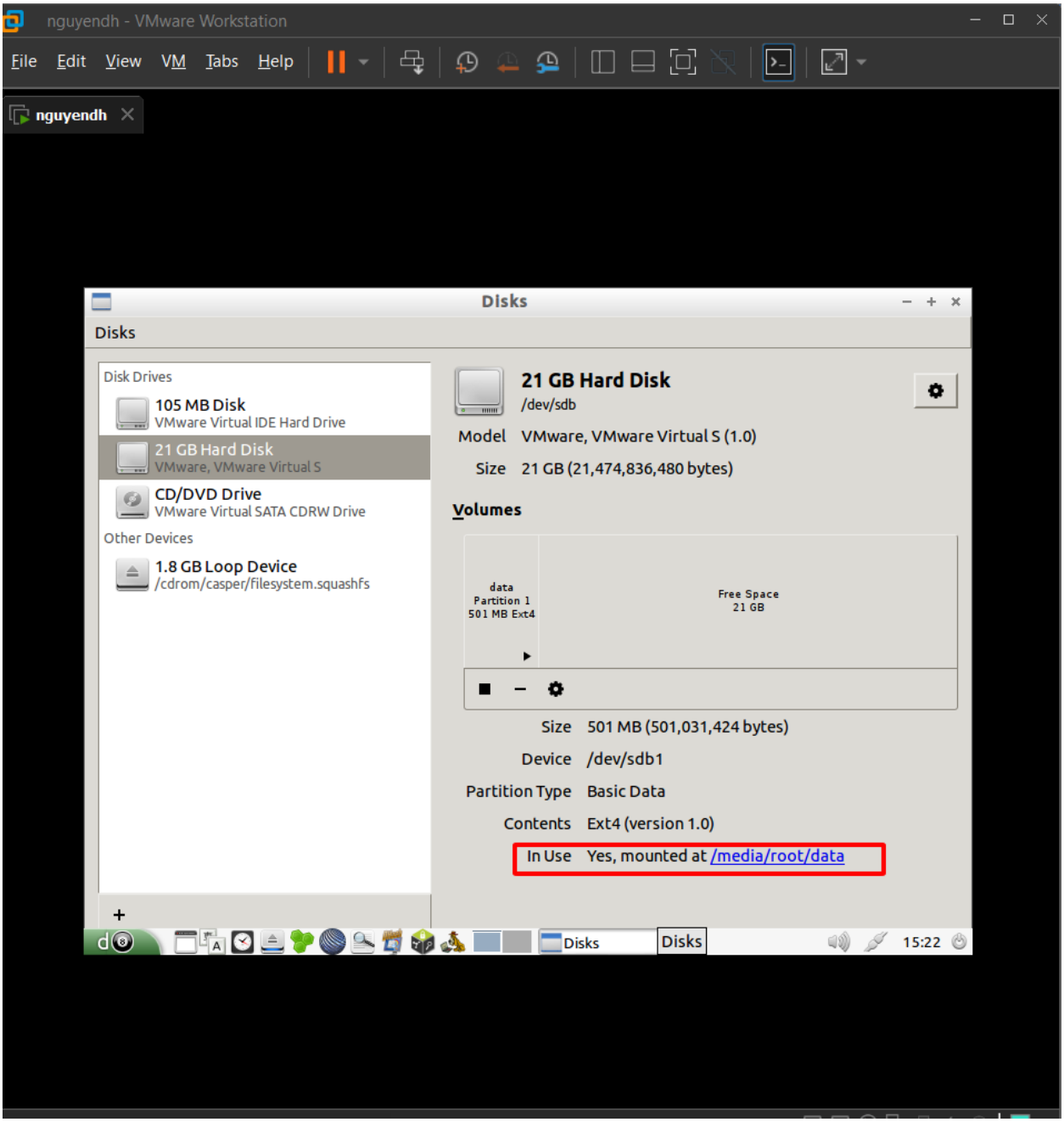
Sau khi hoàn tất nhấn **Create**



Nhấn một nút giống nút play và sau đó mount partition ra

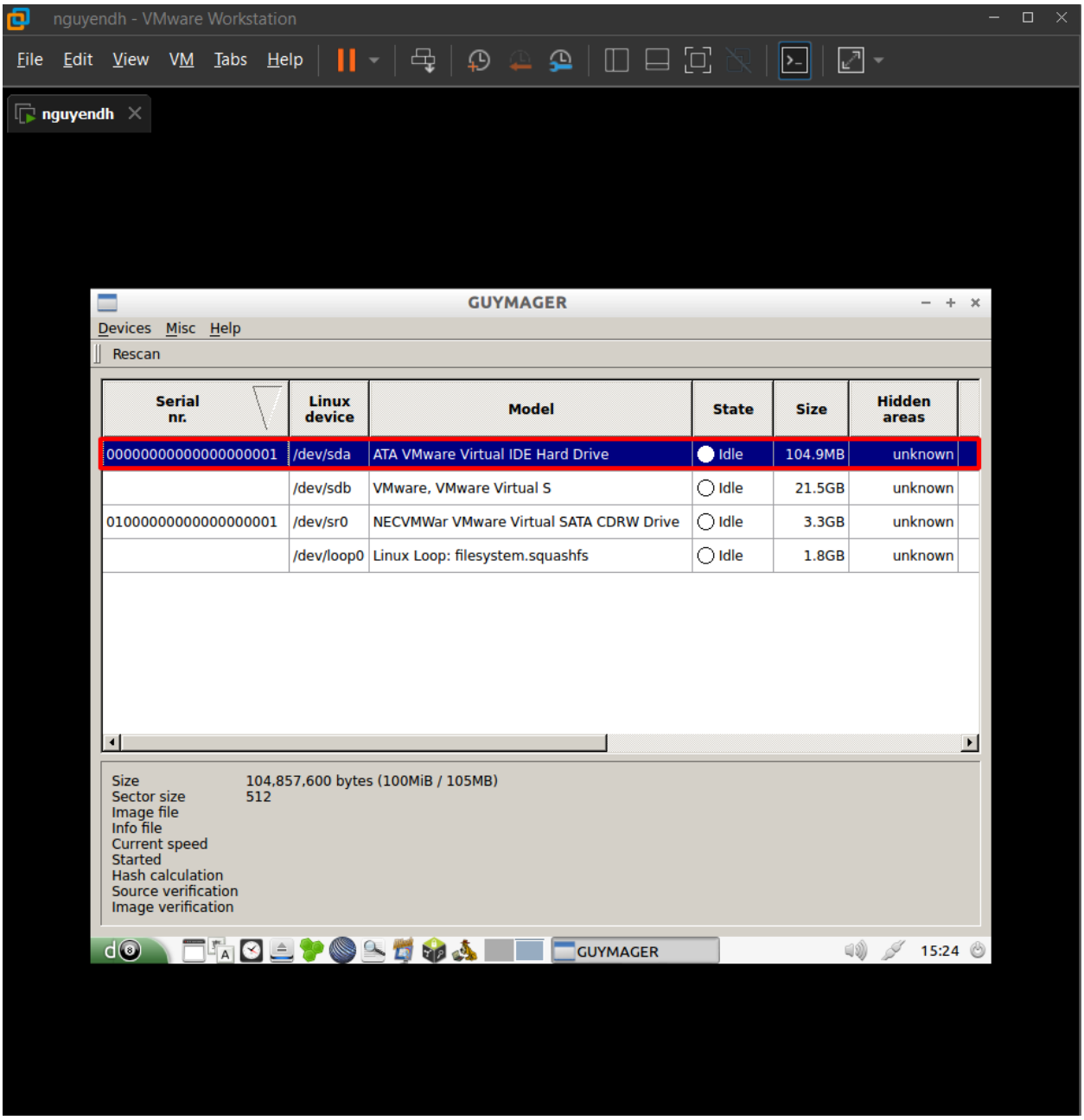


Sau khi xong ở phần bên dưới sẽ hiện ra In use: Yes, mounted at /media/root/data



Acquiring the Evidence Drive with Guymager

Trên Desktop, mở **Guymager,** resize lại ứng dụng cho dễ nhìn và để ý tới ổ có size là 104.9MB



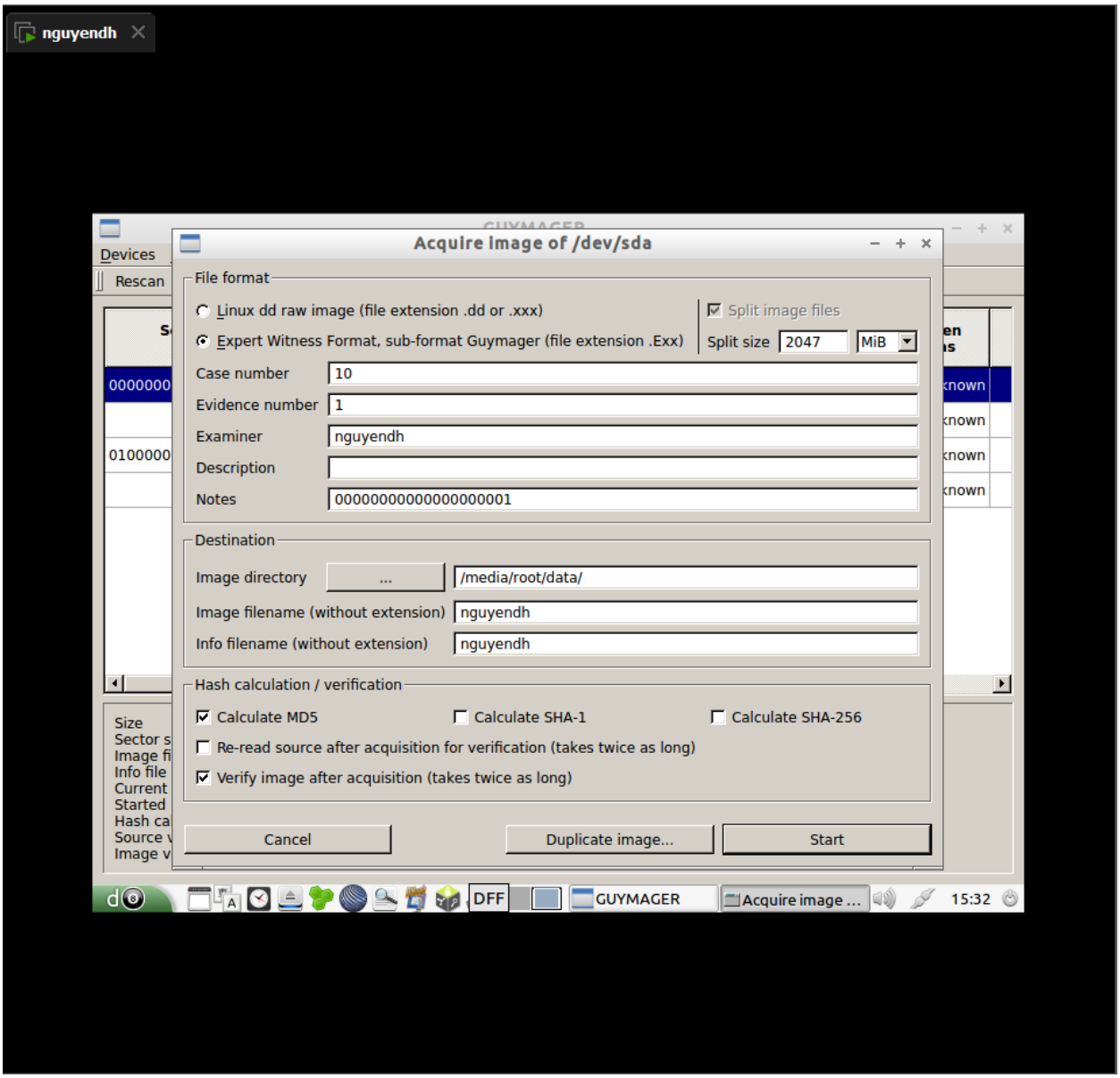
Nhấn chuột phải vào ổ đĩa đó, chọn Acquire Image

Trong phần này ta sẽ setign một số thứ như sau:

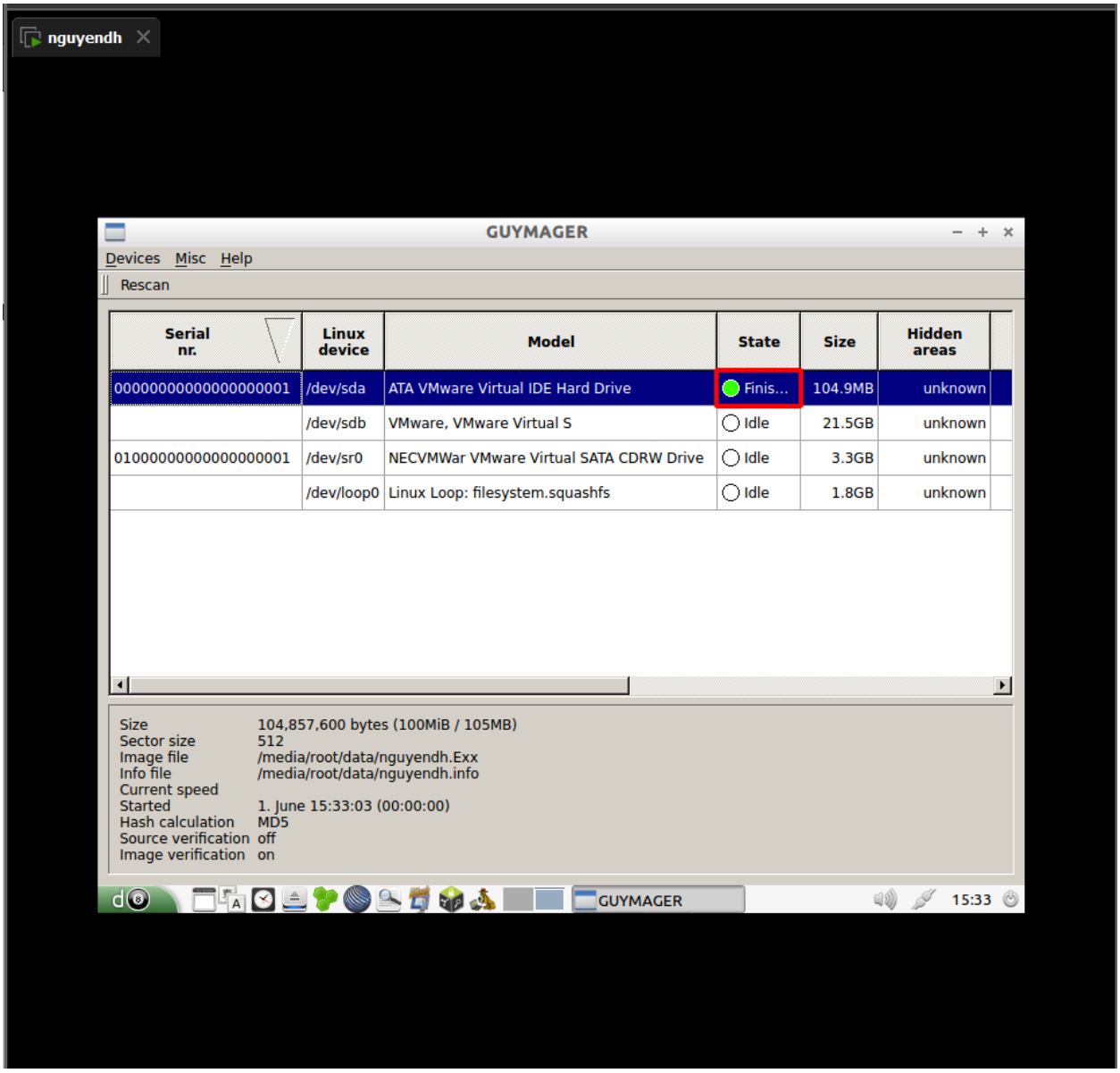
- File format: Expert Witness.
    - Để tên file format là Expert Witness là bởi vì đó một loại hình ảnh đĩa, một loại định dạng thường được sử dụng để chụp và "đóng băng" nội dung và cấu trúc của thiết bị lưu trữ,
- Case number: 10
- Evidence number: 1
- Examiner: tên của chính mình. Ở đây sẽ là nguyendh

- Description: chỉ là chú thích cho image, có cũng được không có cũng không sao
- Destination Image directory: Chúng ta sẽ chọn /media/root/data/
- Destination Image filename: tới phần này là đặt tên cho ổ đĩa, ta có thể đặt sao cũng được. Trong trường hợp này sẽ đặt tên là nguyendh

Dưới đây là hình đã cấu hình cho ổ đĩa. Sau khi hoàn tất, nhấn start để bắt đầu quá trình chạy



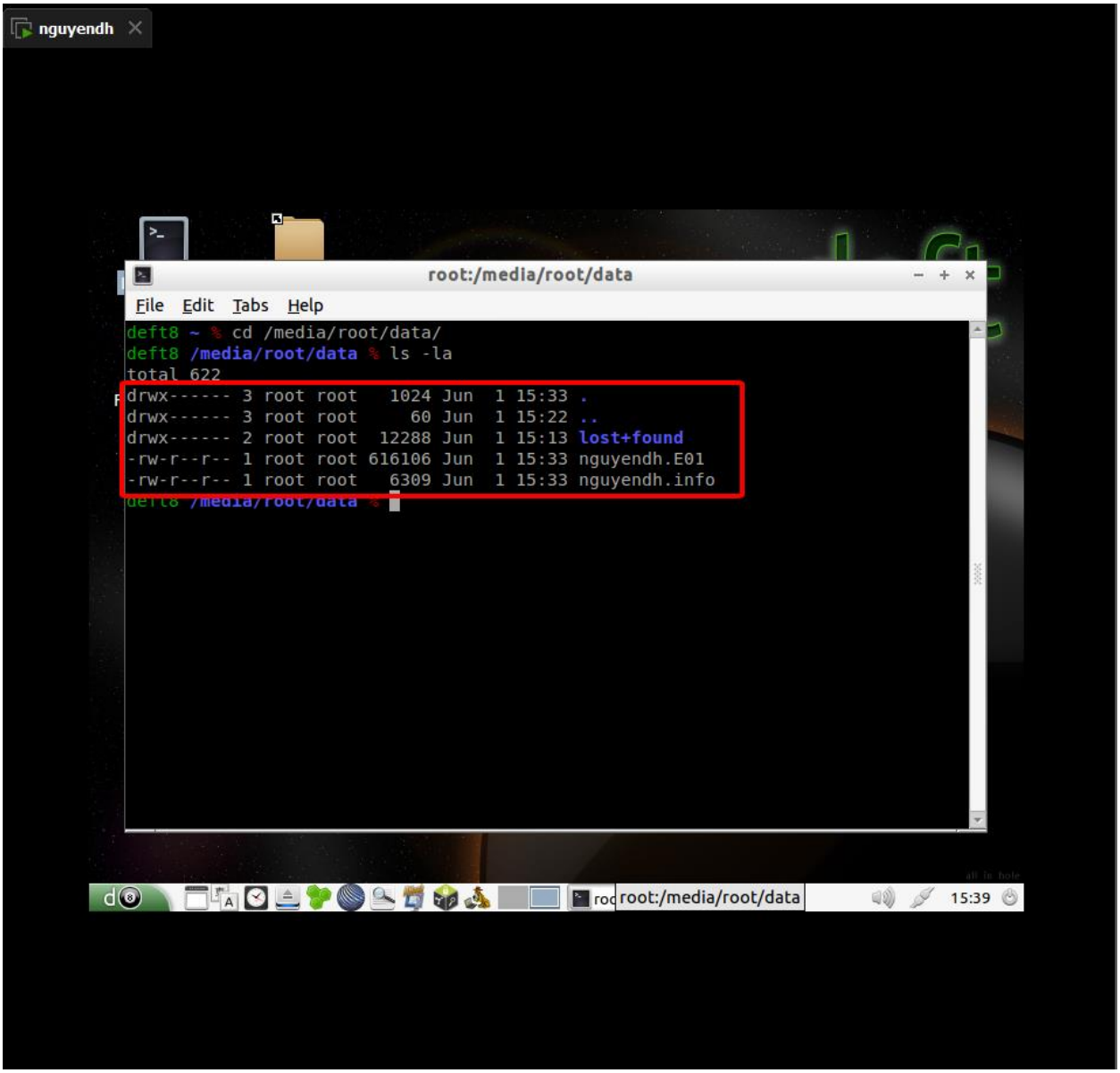
Khi chạy xong, ở các ổ đĩa bên dưới, sẽ có một ổ đĩa xuất hiện màu xanh



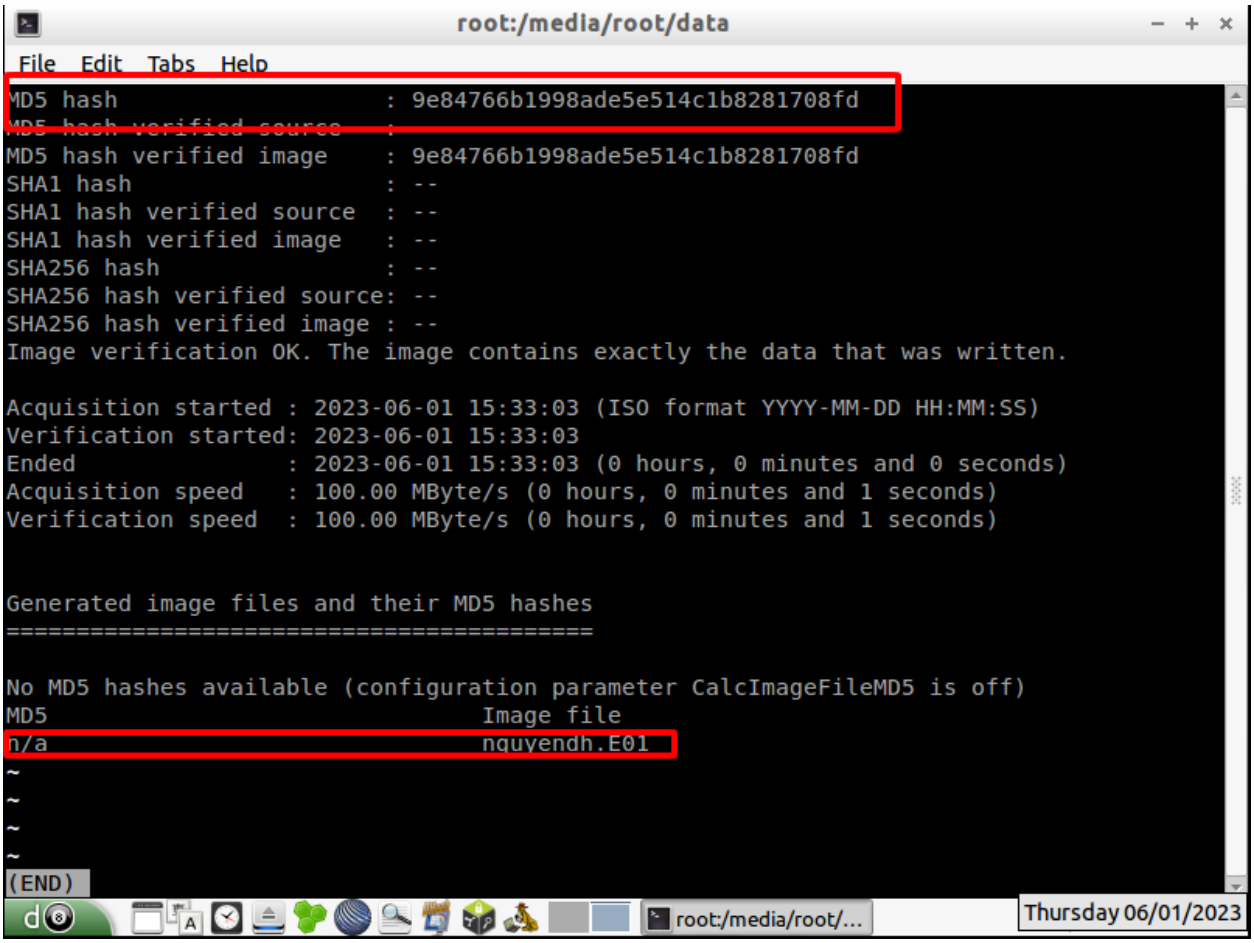
Examining the .E01 Acquired Image

Sau khi thực hiện xogn với ổ đĩa, chúng ta bắt đầu đi phân tích chúng. Image được mount ra đang nằm ở /media/root/data. Việc chúng ta cần làm là **cd /media/root/data** và sau đó **ls -la** để kiểm tra xem là có file chưa.

Ở trong đây đã có hai file là nguyendh.E01 và nguyendh.info trong đó E01 là file expert witness còn file info là file chứa thông tin của image



Sử dụng command less <tên file> để có thể xem được bên trong file đó có chứa cái gì. Ở đây ta sẽ sử dugnj **less nguyendh.info** để check thông tin ổ đĩa như hình dưới là tên ổ đĩa và md5 hash của chúng

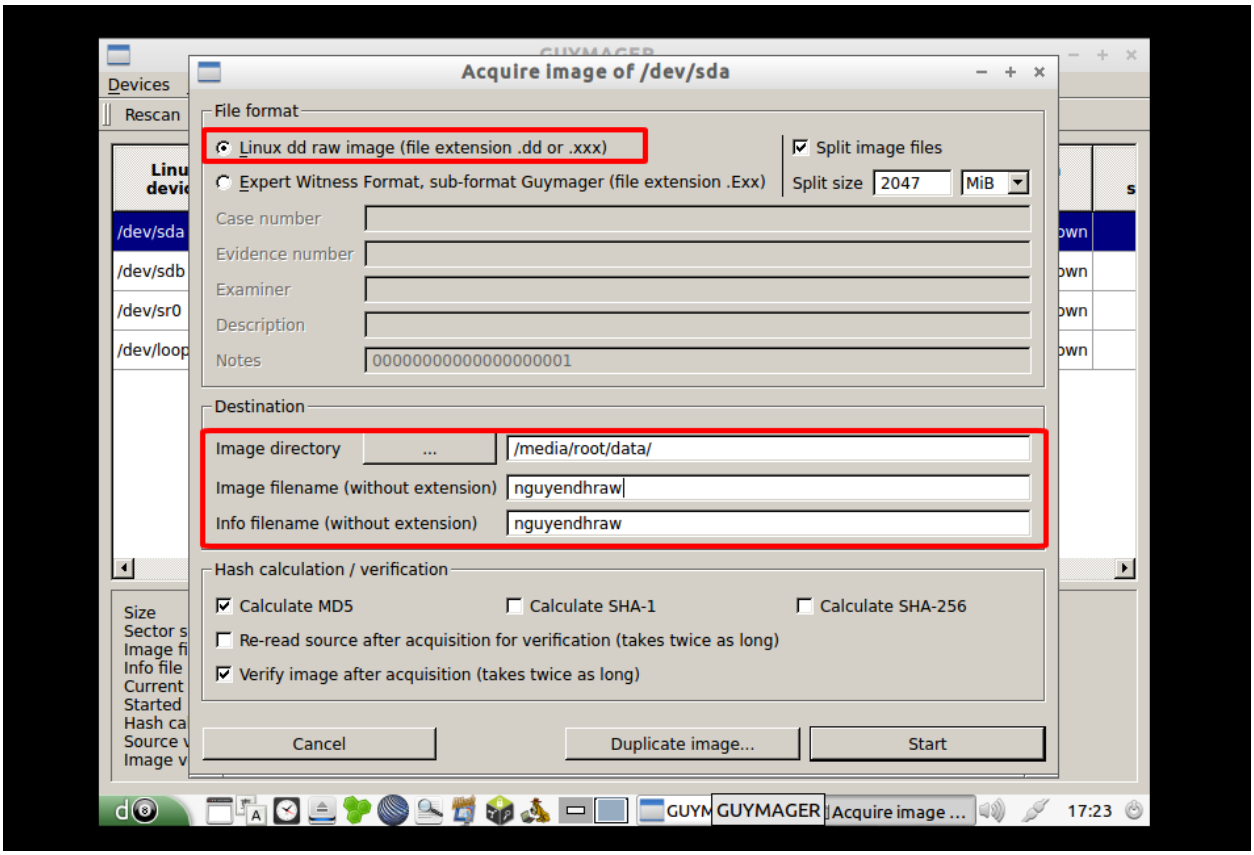


Bây giờ chúng ta sẽ dump một file RAW. Cách làm vẫn như cũ, giống như làm với một file expert witness, ta sẽ vào bên trong **guymagner** để dump ra, click chọn vào ổ có size là **104.9mb** và sau đó chọn vào **Acquire Image.**

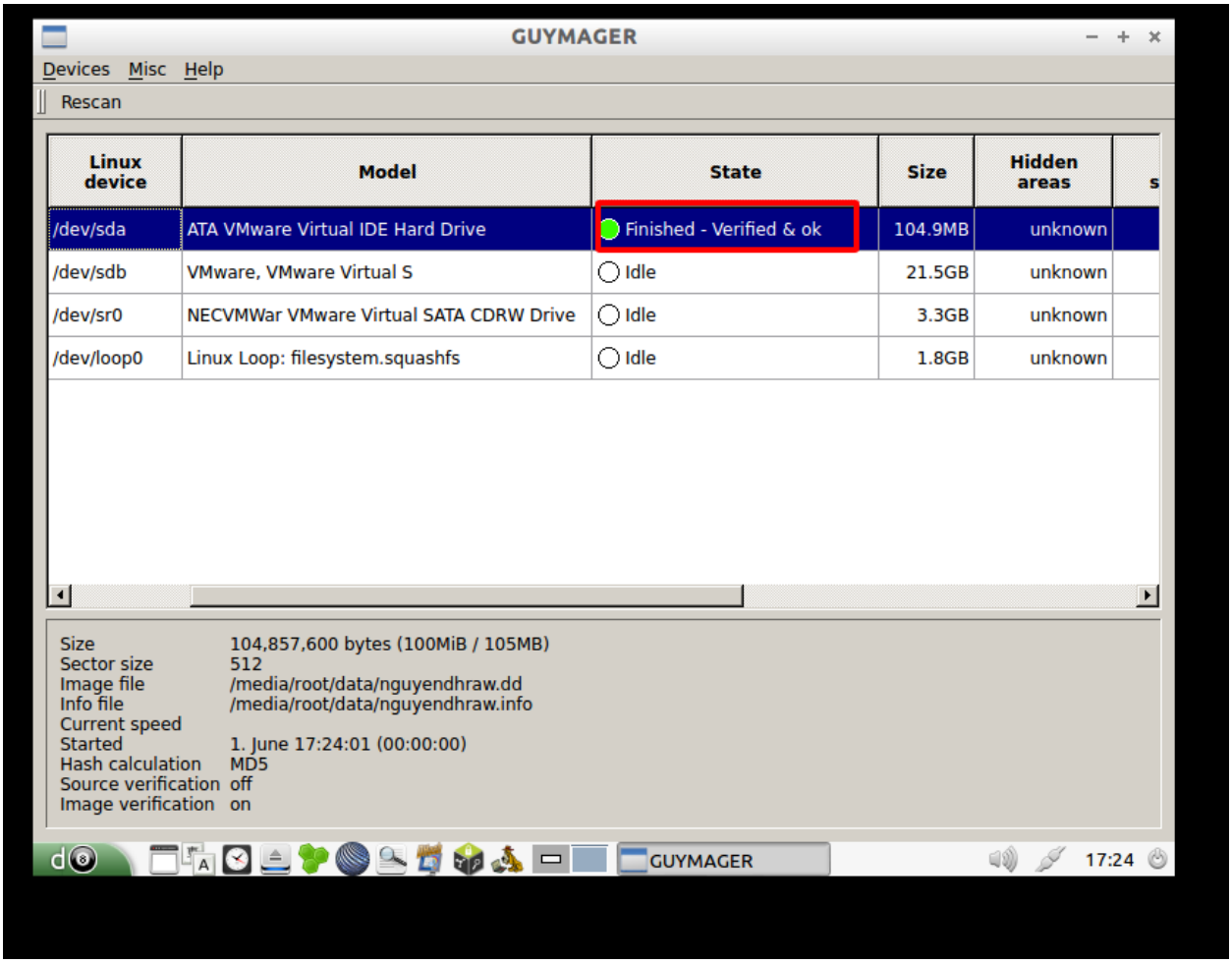
Thay vì bình thường chúng ta sẽ chọn Expert Witness format, bây giờ chúng ta sẽ chọn

- File format: Linux dd raw image
- Destination Image directory: /media/root/data/
- Destination Image filename: nguyendhRAW

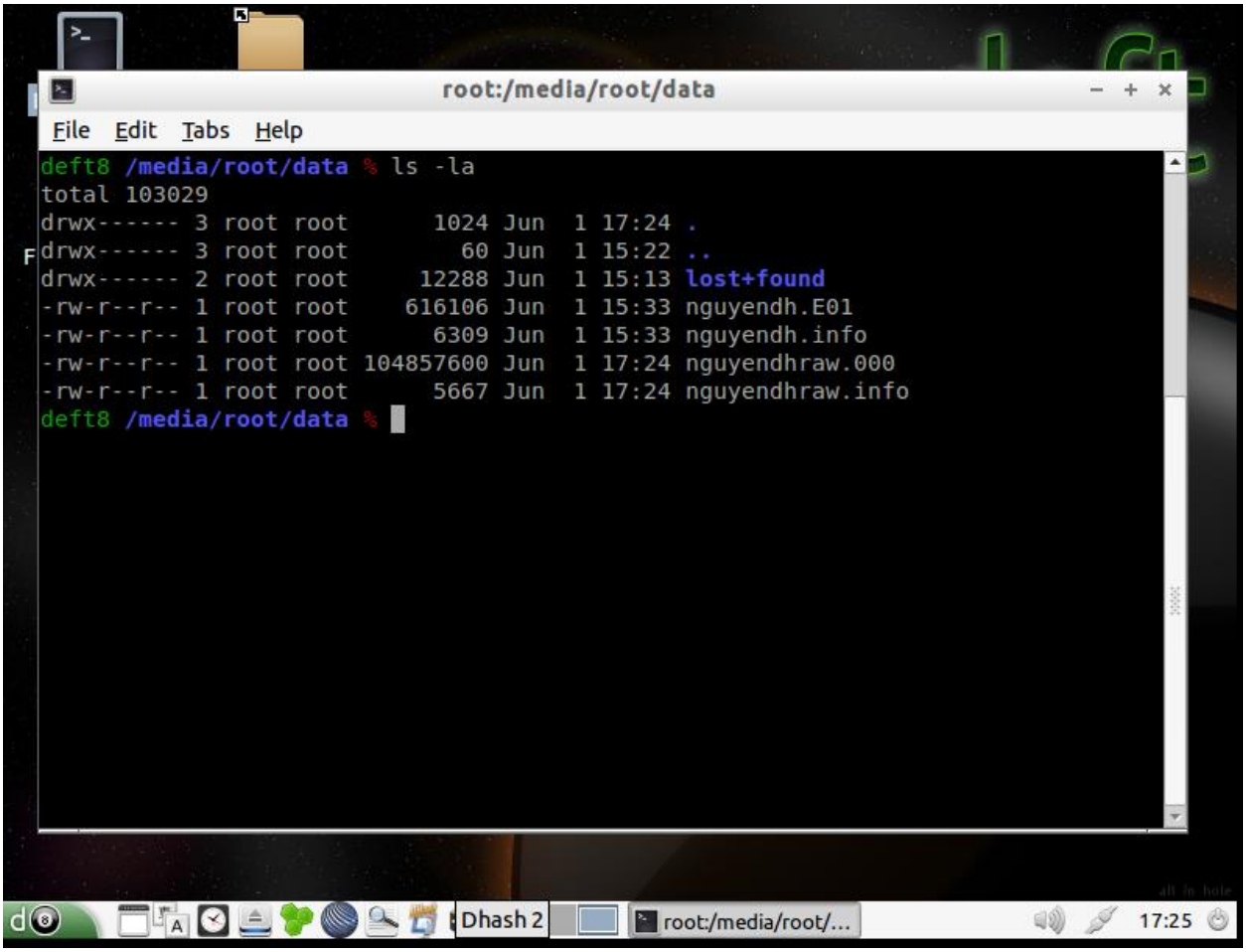
Setting hoàn tất theo hình bên dưới đây

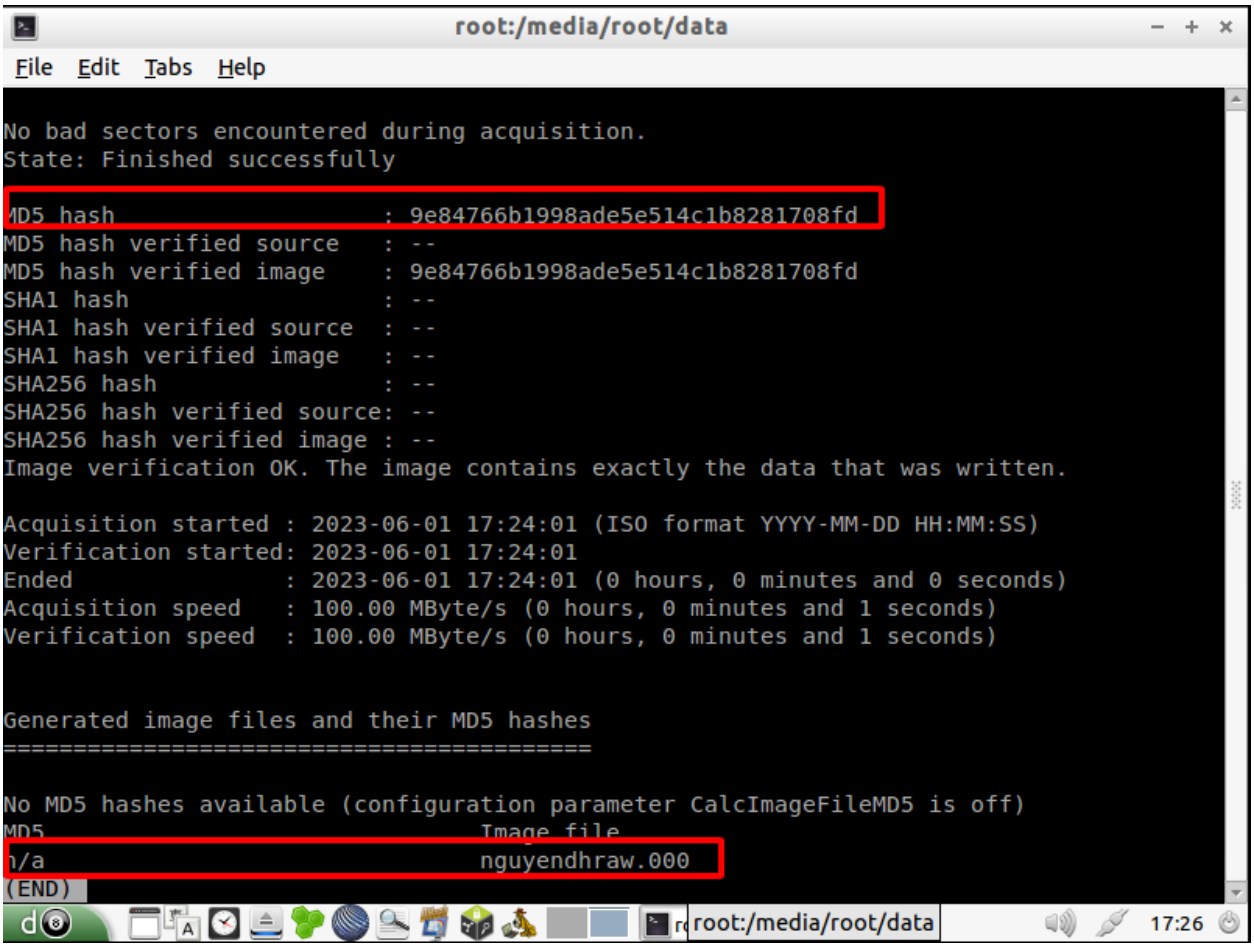


Sau khi hoàn tất việc dump file, nó sẽ hiện thông báo tick màu xanh giống như lúc t làm với file witness



Thử xem file với câu lệnh ls -la trong thư mục /media/root/data. Ở đây ta thấy rằng chúng ta đã tạo thành công một file nguyendhraw.000 với nguyendhraw.info chứ thông tin về ổ


root:/media/root/data
File Edit Tabs Help
deft8 /media/root/data % ls -la
total 103029
drwx------ 3 root root 1024 Jun 1 17:24 .
drwx------ 3 root root 60 Jun 1 15:22 ..
drwx------ 2 root root 12288 Jun 1 15:13 lost+found
-rw-r--r-- 1 root root 616106 Jun 1 15:33 nguyendh.E01
-rw-r--r-- 1 root root 6309 Jun 1 15:33 nguyendh.info
-rw-r--r-- 1 root root 104857600 Jun 1 17:24 nguyendhraw.000
-rw-r--r-- 1 root root 5667 Jun 1 17:24 nguyendhraw.info
deft8 /media/root/data %
Dhash 2
root:/media/root/...
17:25



1. Why do the .dd and .E01 files have different sizes?

Để lý giải cho việc tại sao .dd và .E01 cùng chung một một chỗ là /media/root/data nhưng lại có hai size khác nhau do chúng sử dụng định dạng khác nhau để lưu trữ cùng một dữ liệu. Định dạng file .dd là định dạng hình ảnh ổ đĩa nguyên gốc trực tiếp ánh xạ nội dung của thiết bị lưu trữ, trong khi định dạng file .E01 là định dạng tệp Chứng cứ bao gồm siêu dữ liệu và nén thêm.

2. Which file is the correct evidence image to use in court, or are they both correct?

Về câu hỏi này, theo em thấy tập tin nào là hình ảnh chứng cứ chính xác phải sử dụng trong tòa án, điều đó phụ thuộc vào các tình huống cụ thể của vụ việc và yêu cầu của tòa án hoặc thẩm quyền liên quan. Nói chung, cả hai định dạng được sử dụng phổ biến và được chấp nhận là bằng chứng hợp lệ trong tòa án, nhưng rất quan trọng để tham khảo các chuyên gia pháp lý và tuân theo các quy trình đã thiết lập để xử lý và trình bày bằng chứng số để đảm bảo tính chính xác và sự chấp nhận của tòa án.