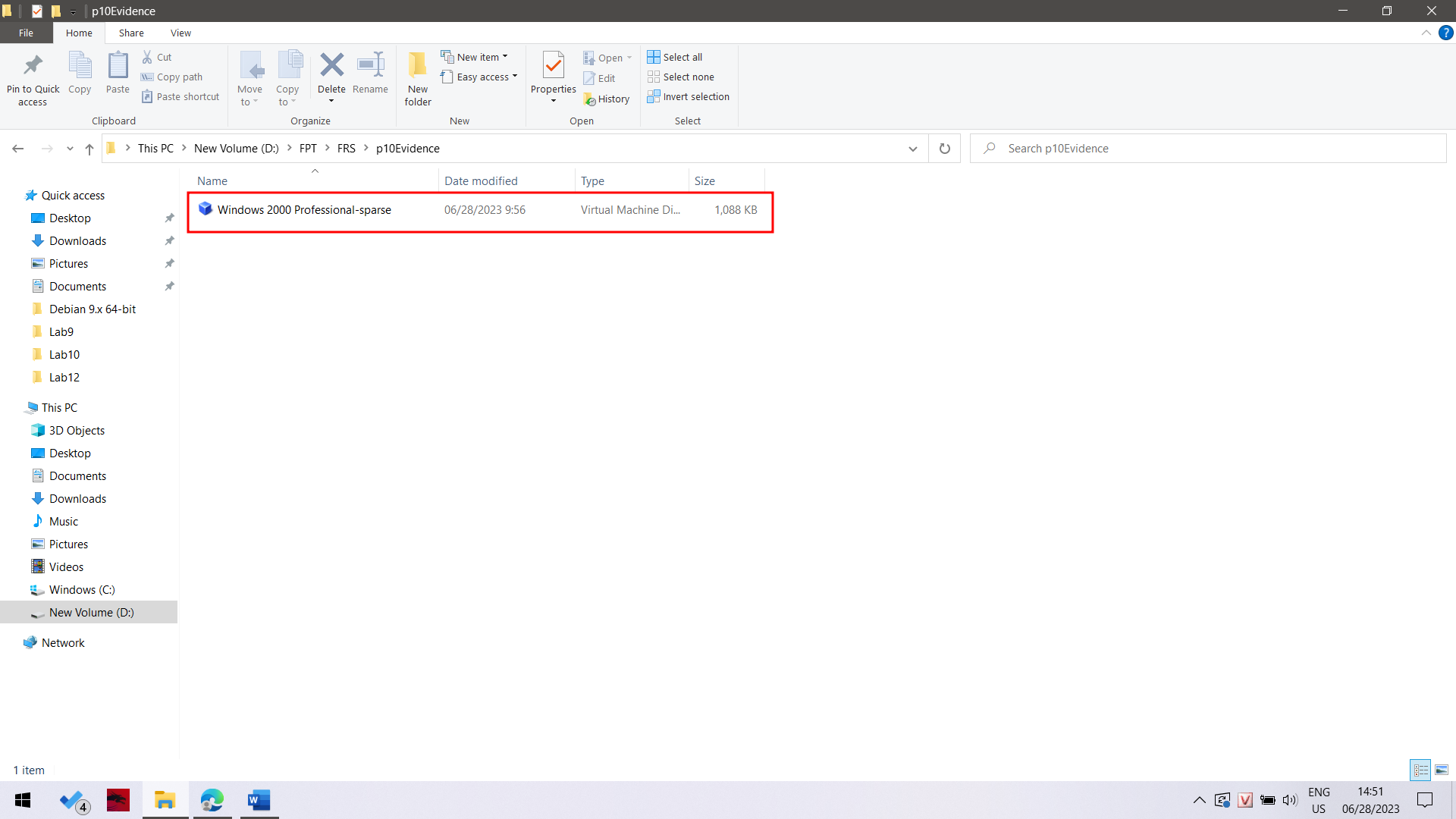
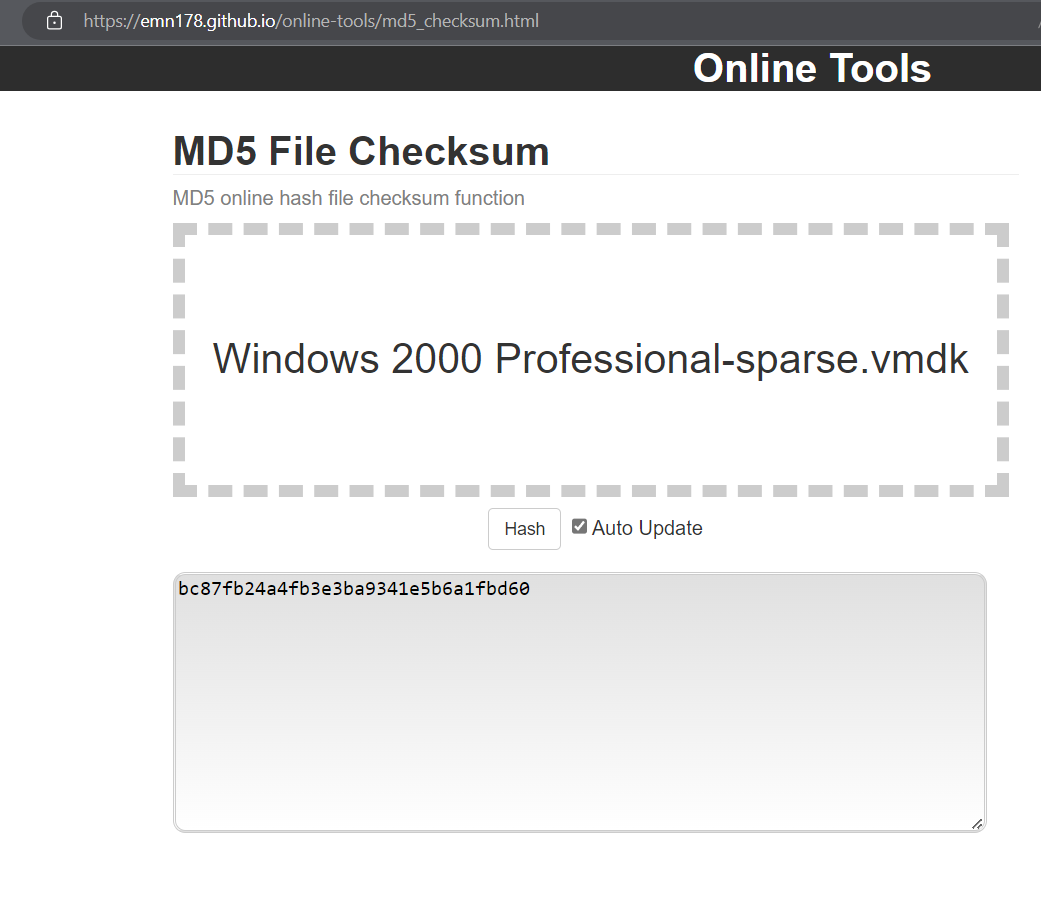
**Lab 10: Static Acquisition with BackTrack**

Bây giờ ta sẽ download ổ đĩa evidence về máy.



Ở bài lab này em không sử dụng back track mà sử dụng máy ảo kali linux cho quá trình điều tra.



Ta thực hiện checksum cho file evidence.

**Connecting the Evidence Drive**

In VMware Player, on the lower right, click "Edit virtual machine settings".

In the "Virtual Machine Settings" box, click the Add... button.

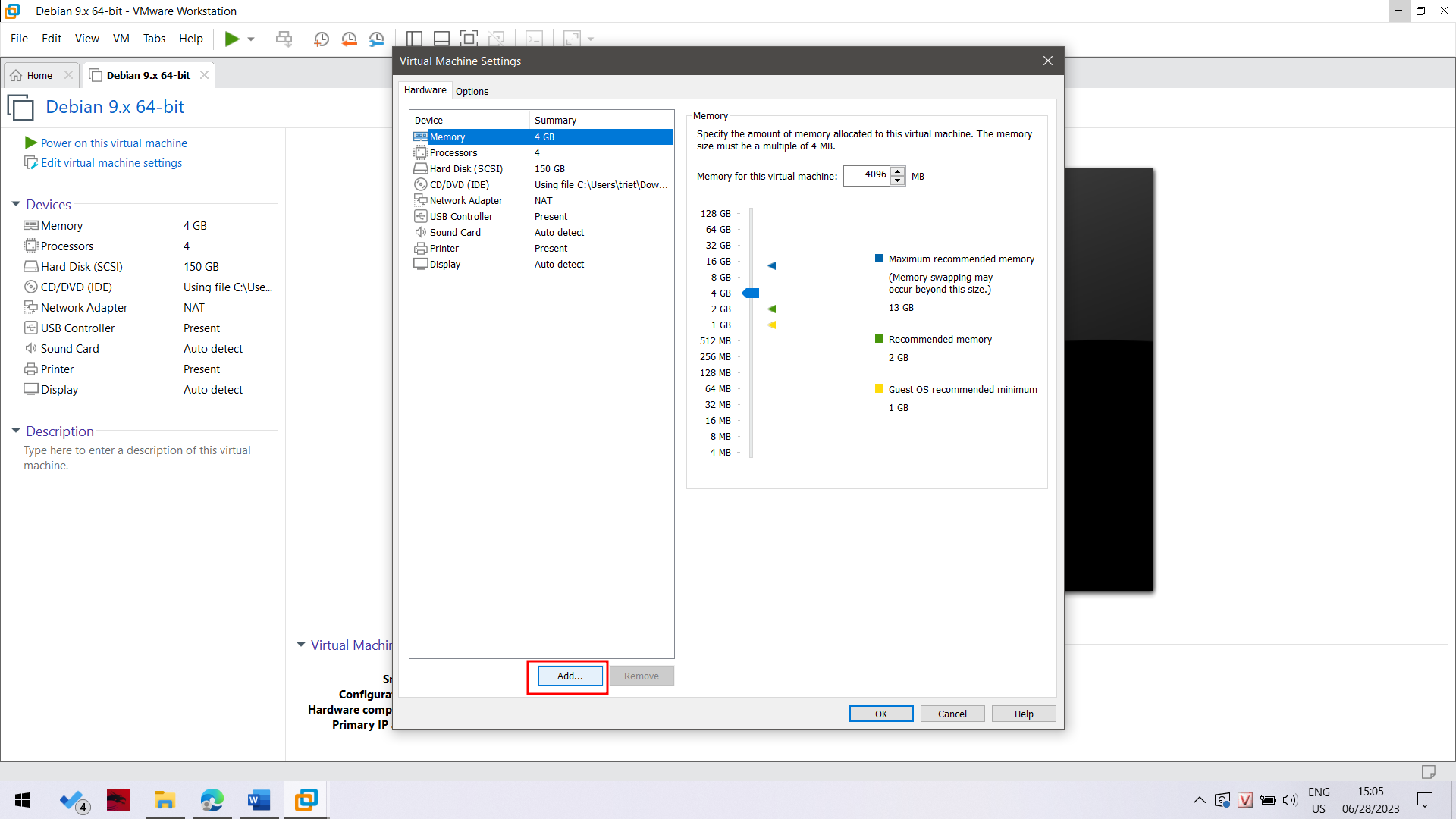
In the "Hardware Type" box, click "Hard Disk". Click Next.

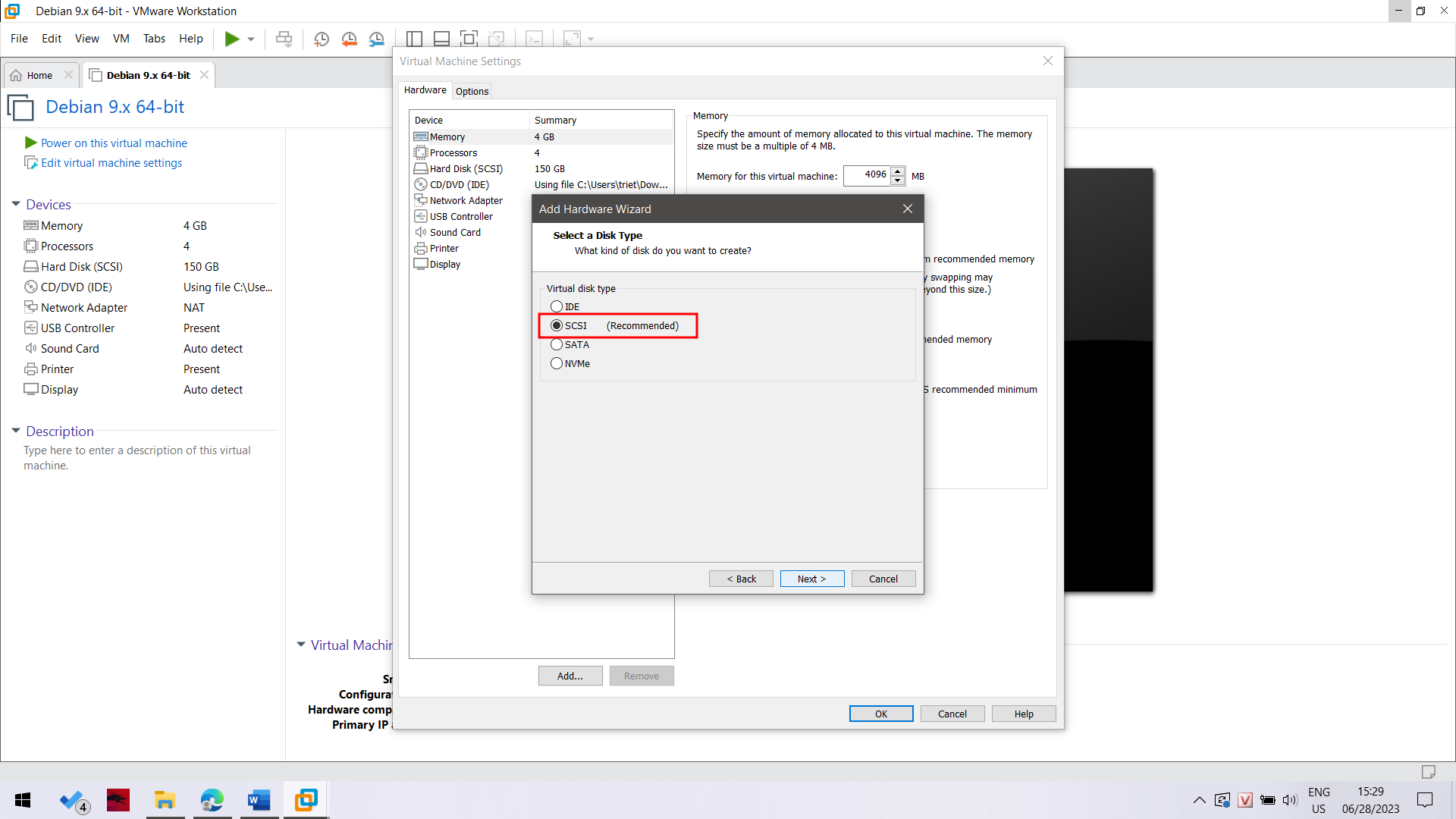
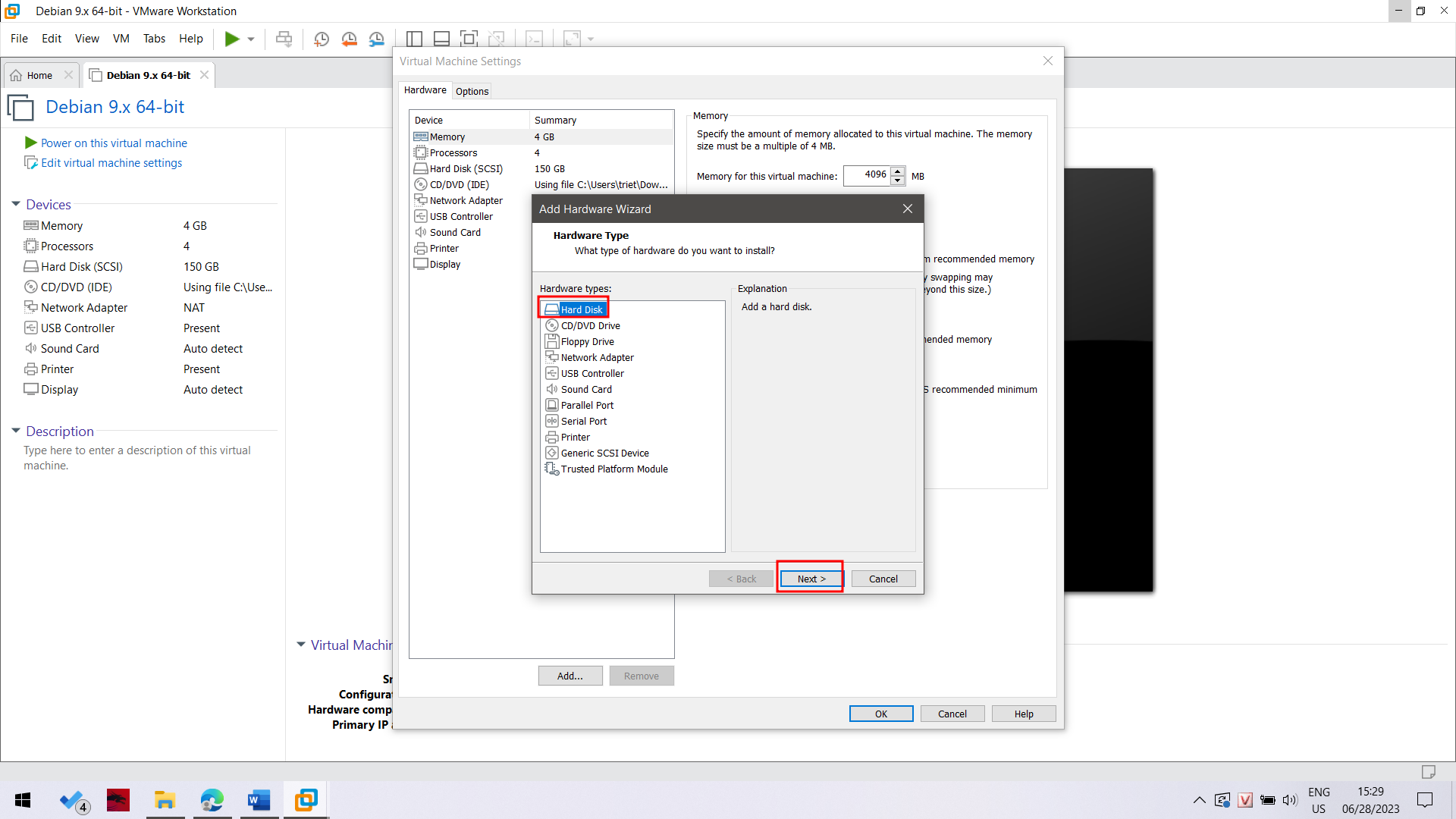
In the "Select a Disk" box, click "Use an existing virtual disk". Click Next.

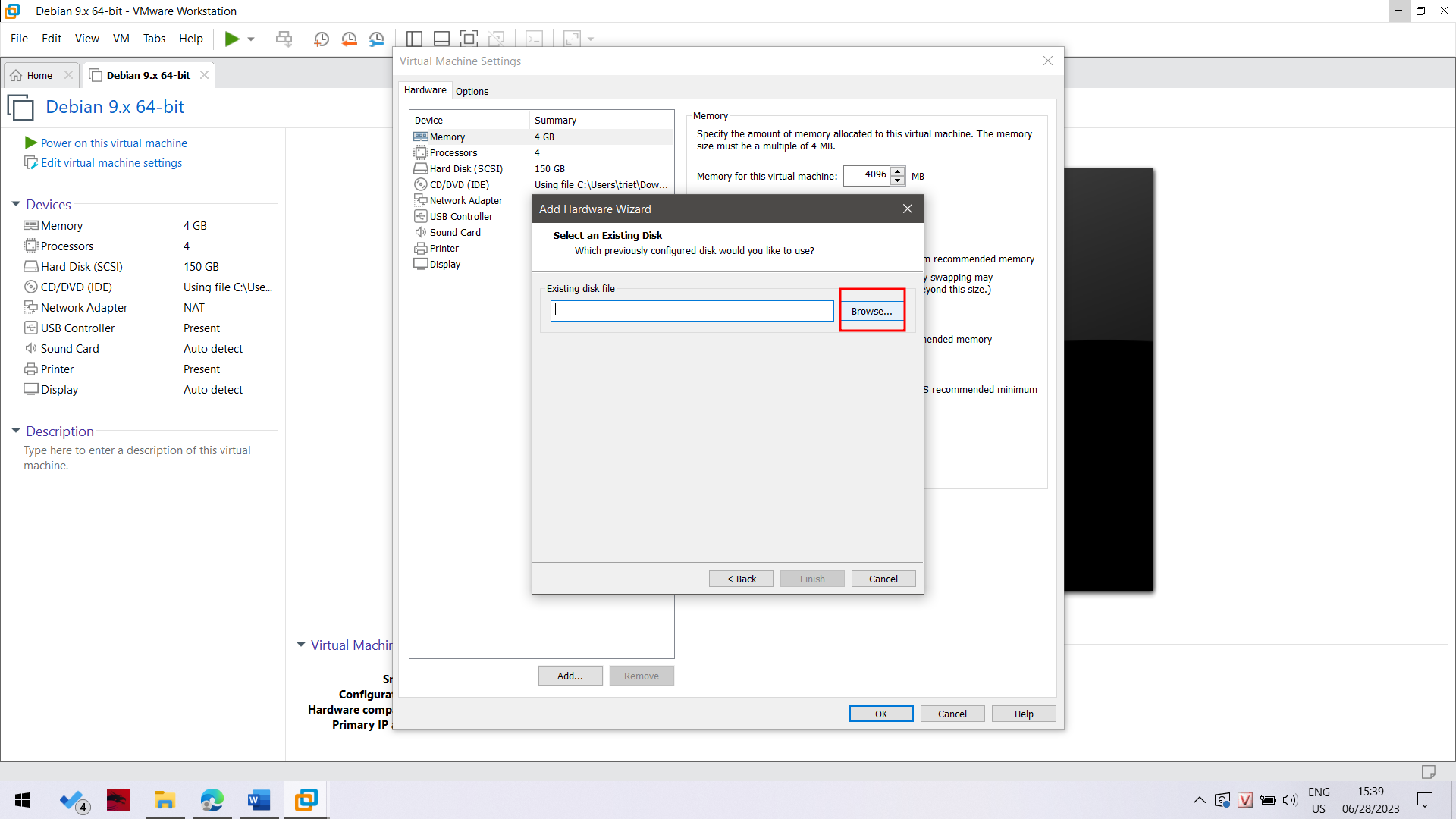
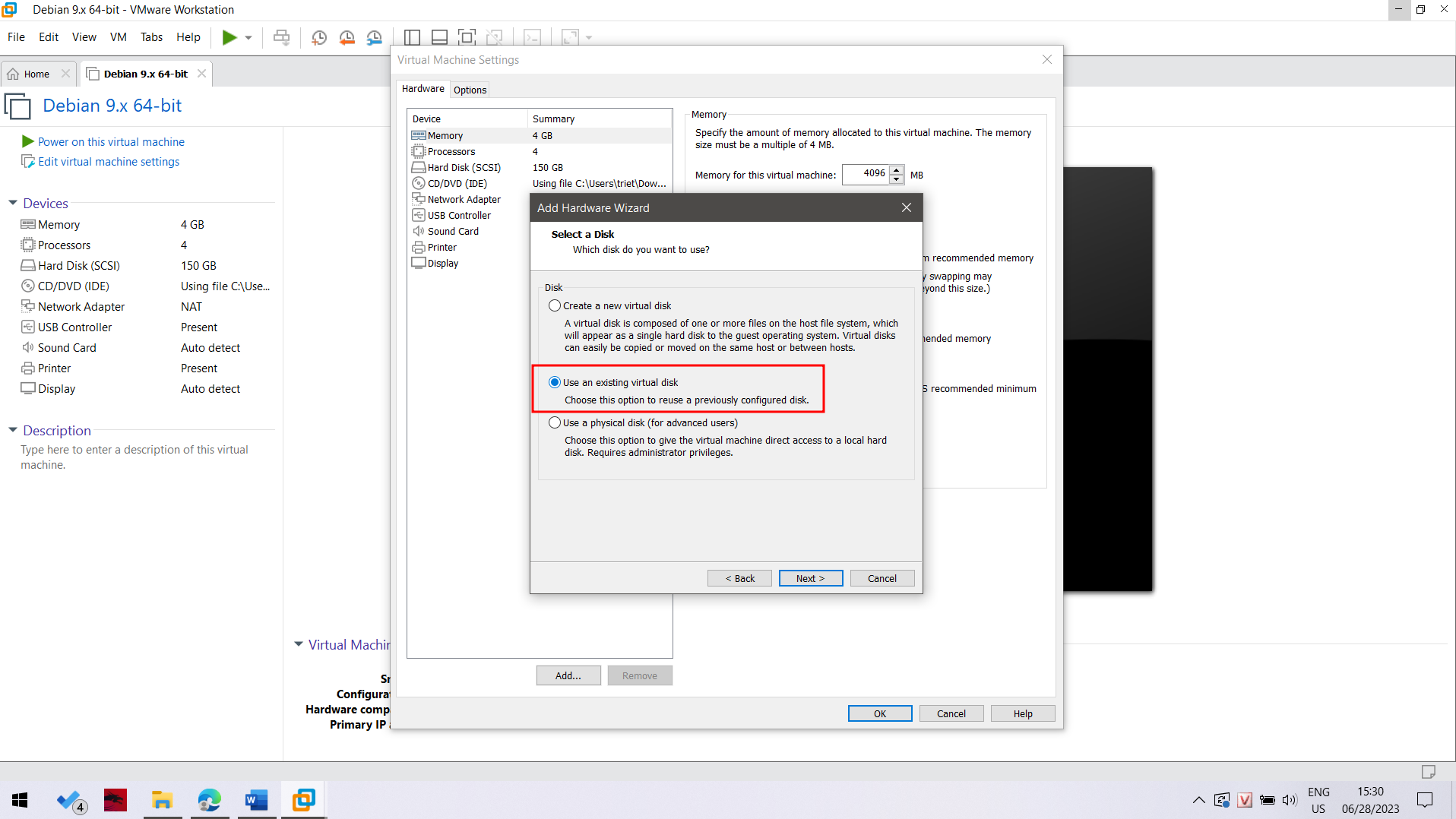
In the "Select an Existing Disk" box, click the Browse... button. Navigate to your "Windows 2000 Professional-sparse.vmdk" file and double-click it.

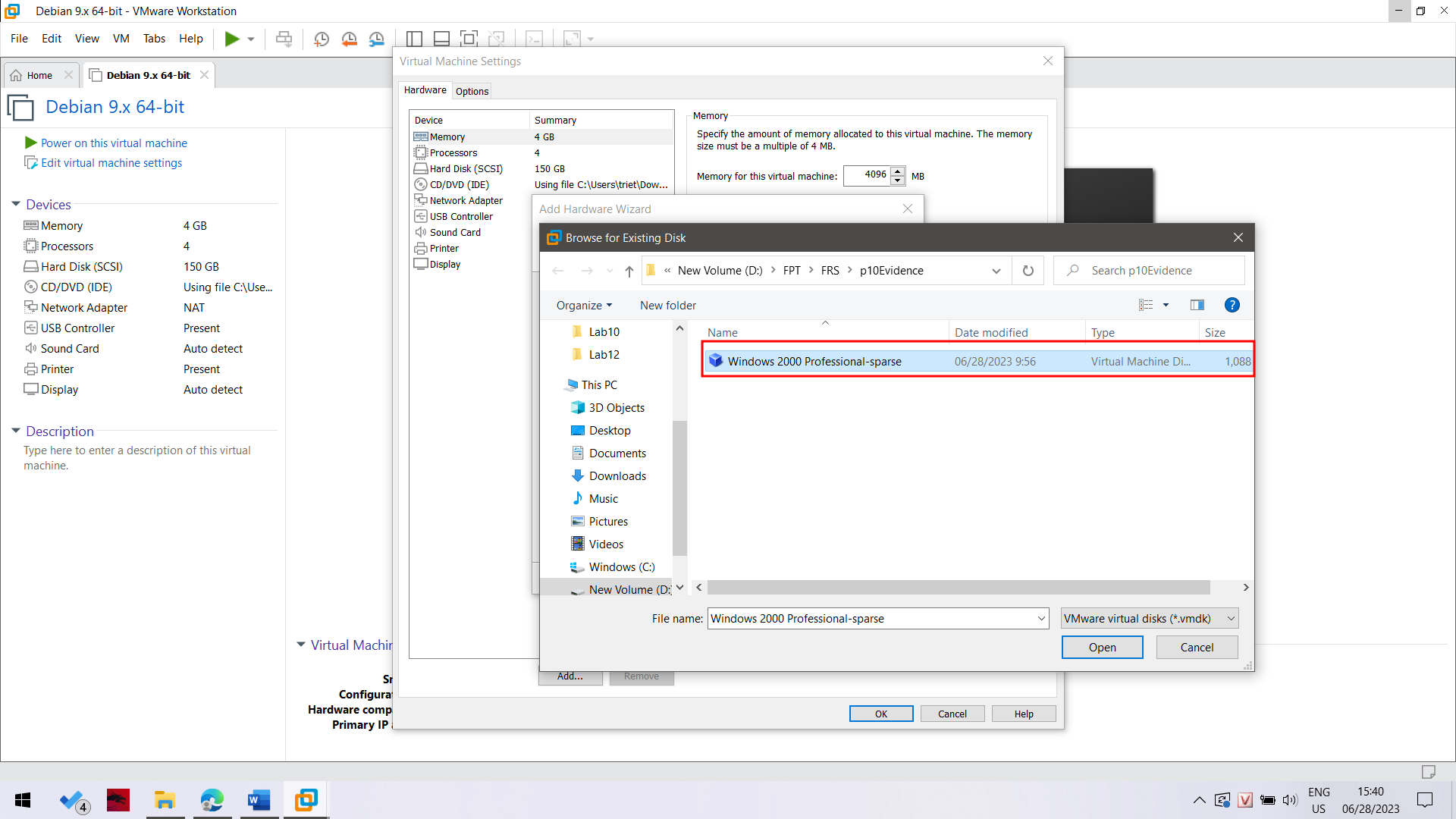
A box pops up asking if you want to 'Convert existing virtual disk to newer format?", as shown below.

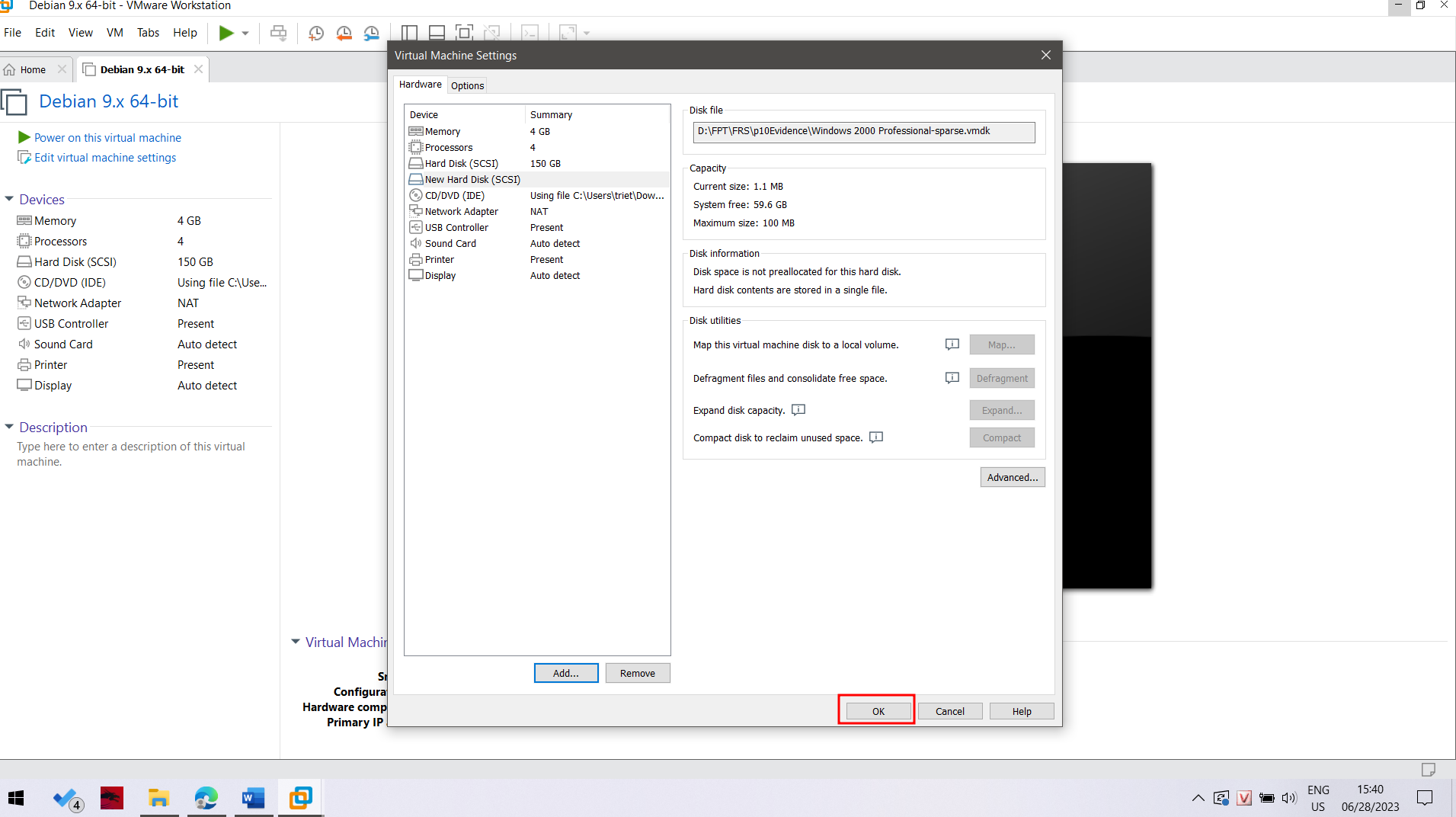
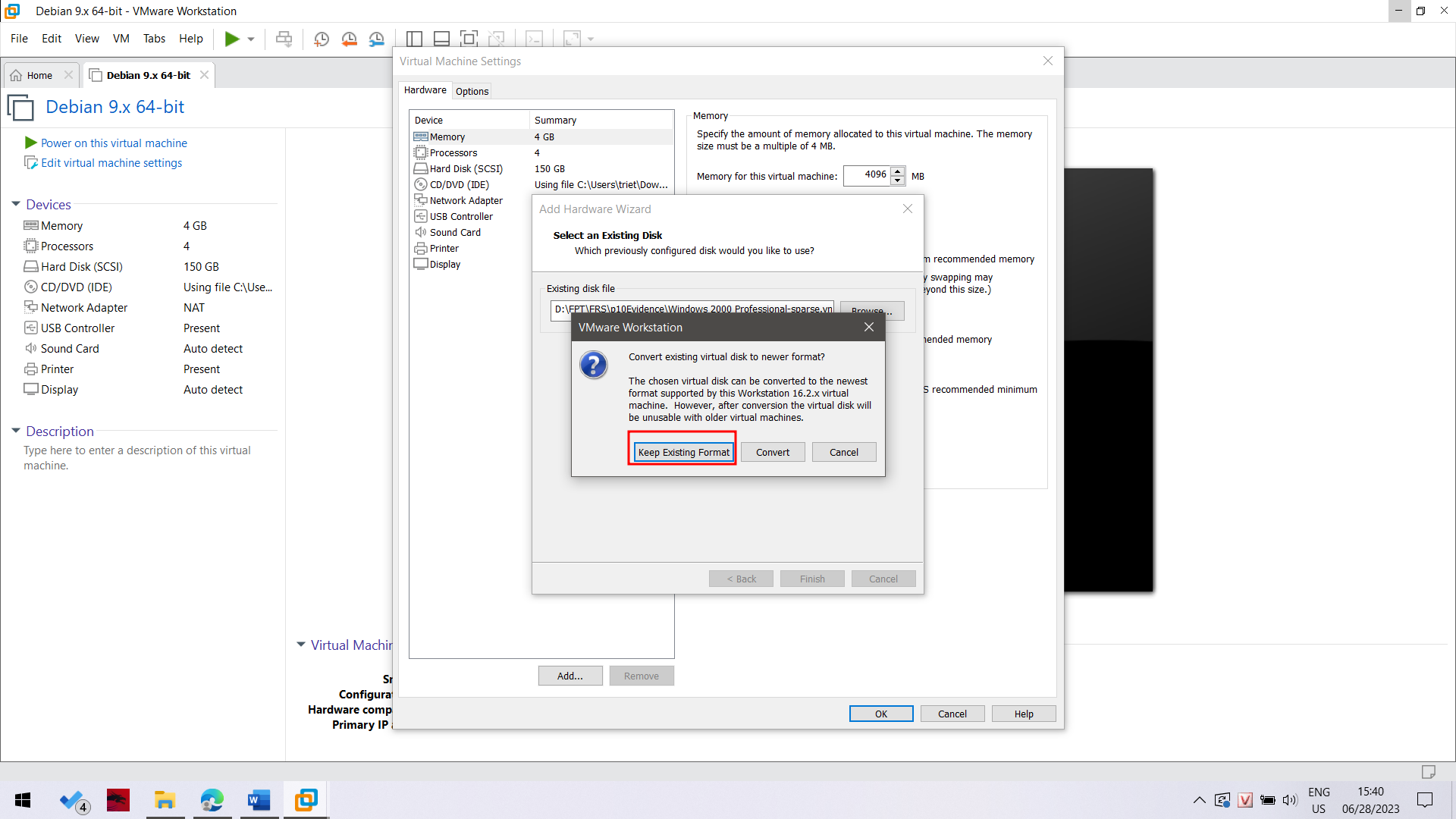
This is the evidence drive, we certainly don't want to change anything, so click "Keep Existing Format".



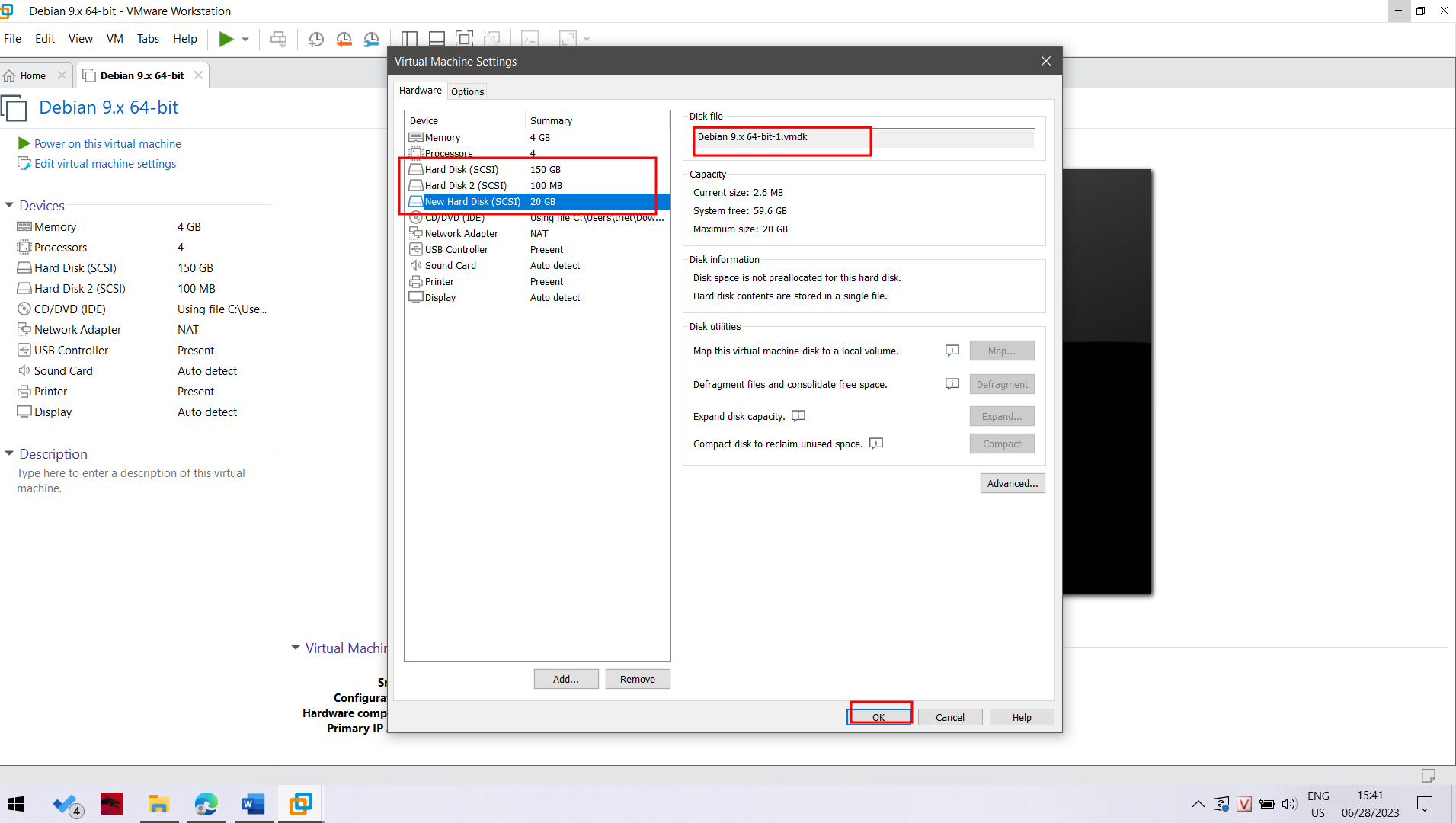




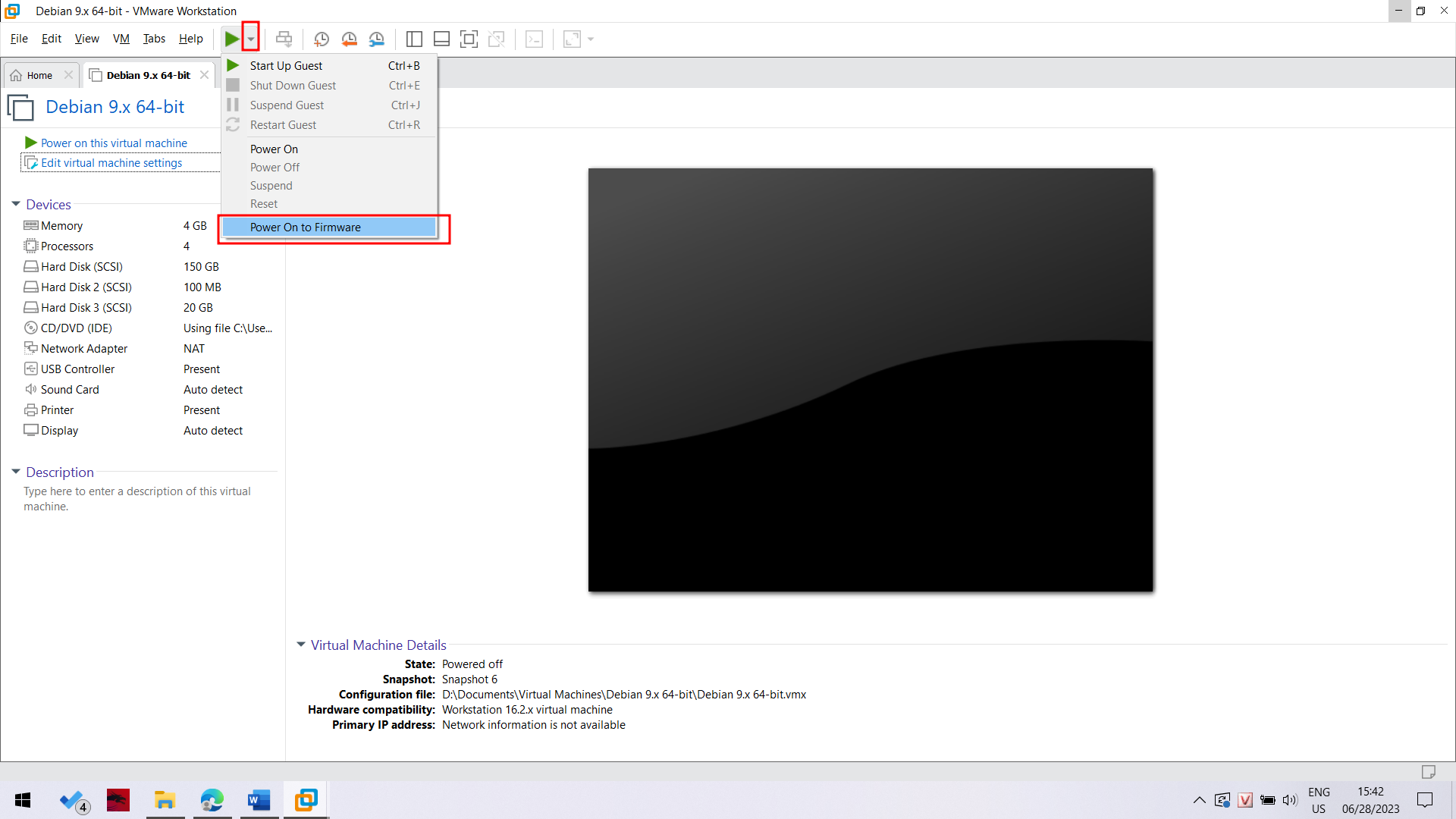


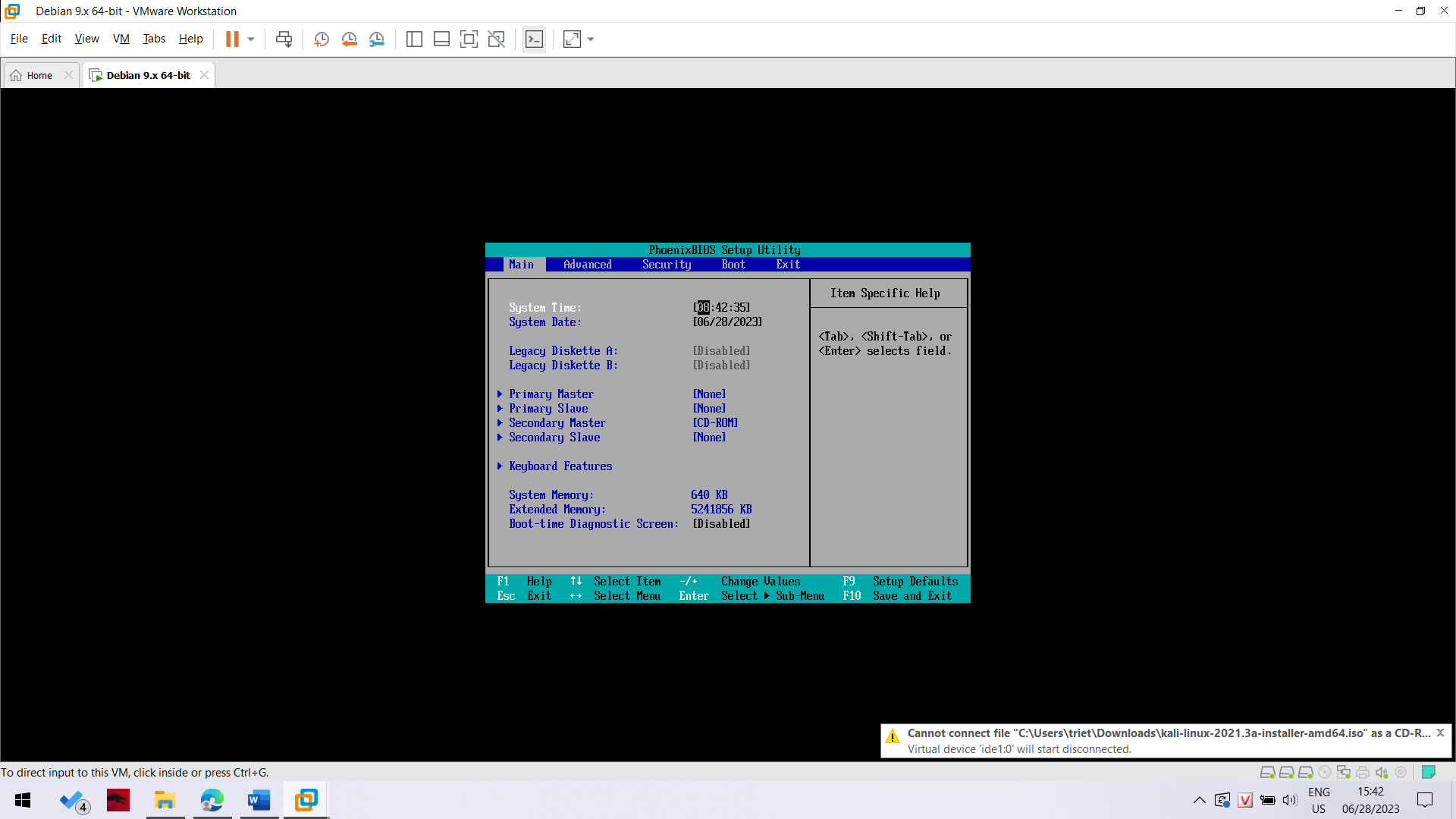


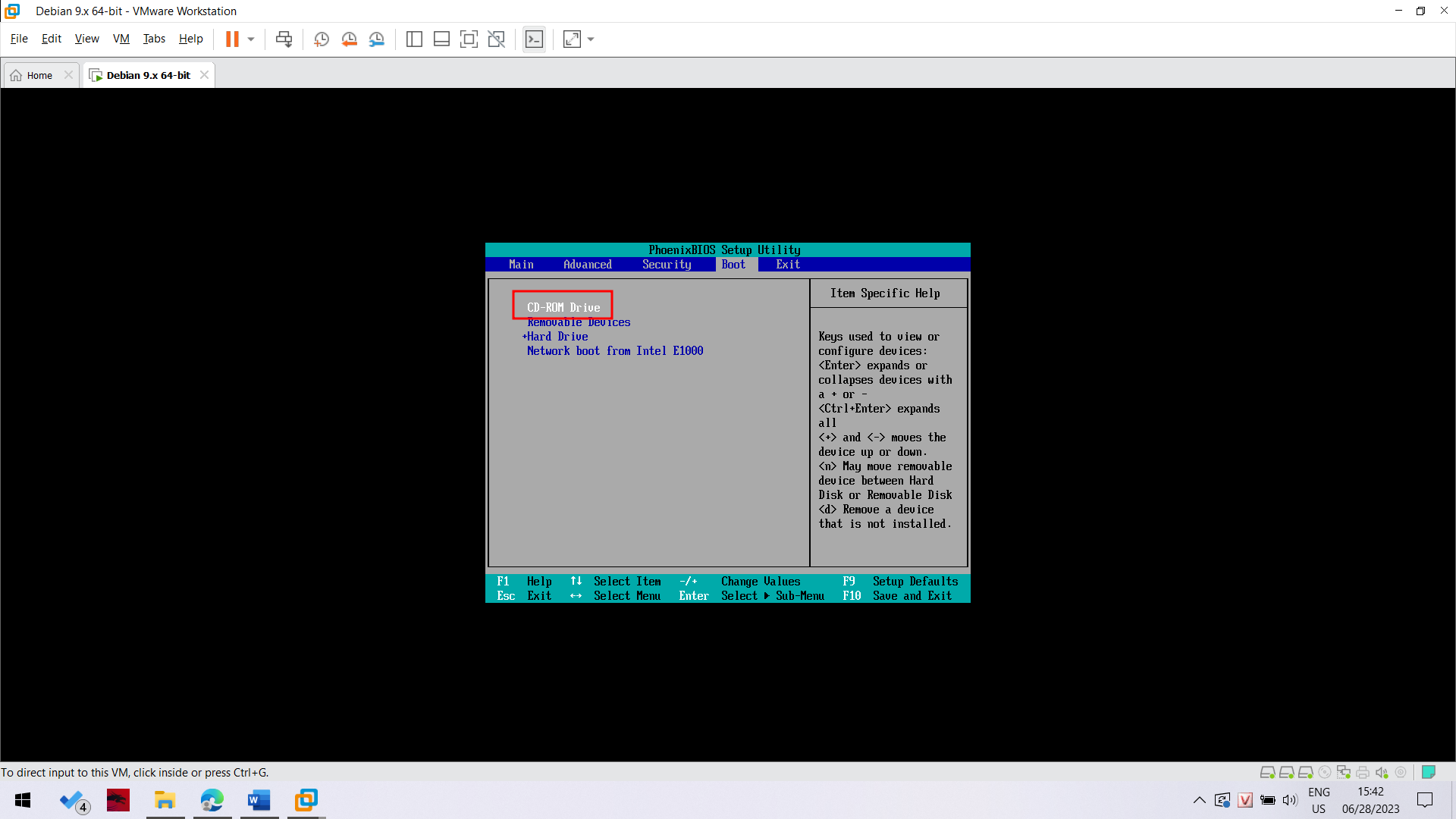
Tuy nhiên em sẽ add thêm một ổ cứng 20gb trống nữa để thực hiện mount ổ đĩa evidence ra đó.

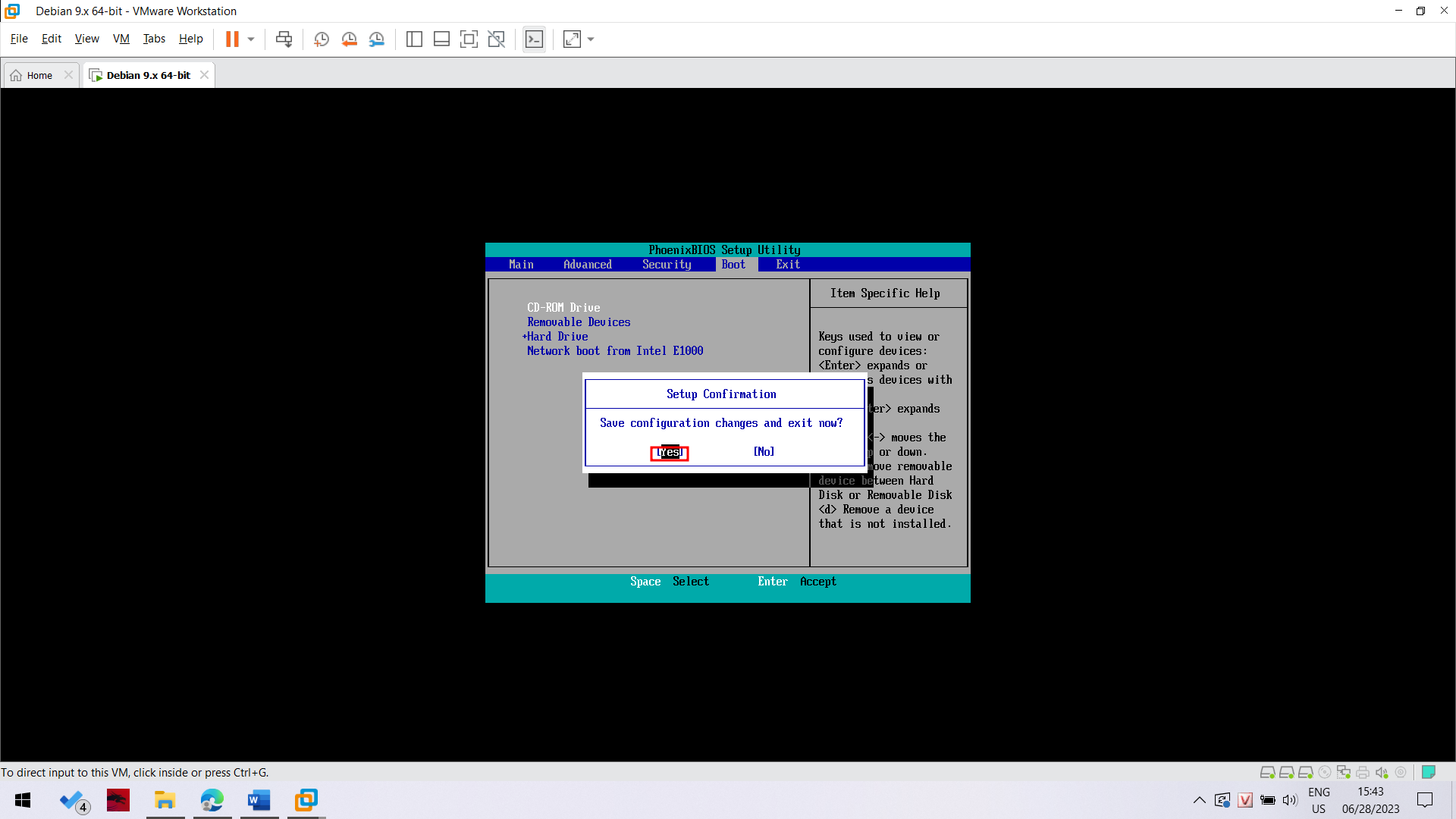


Boot vào firmware bằng cách nhấn F2 hoặc bấm như sau.







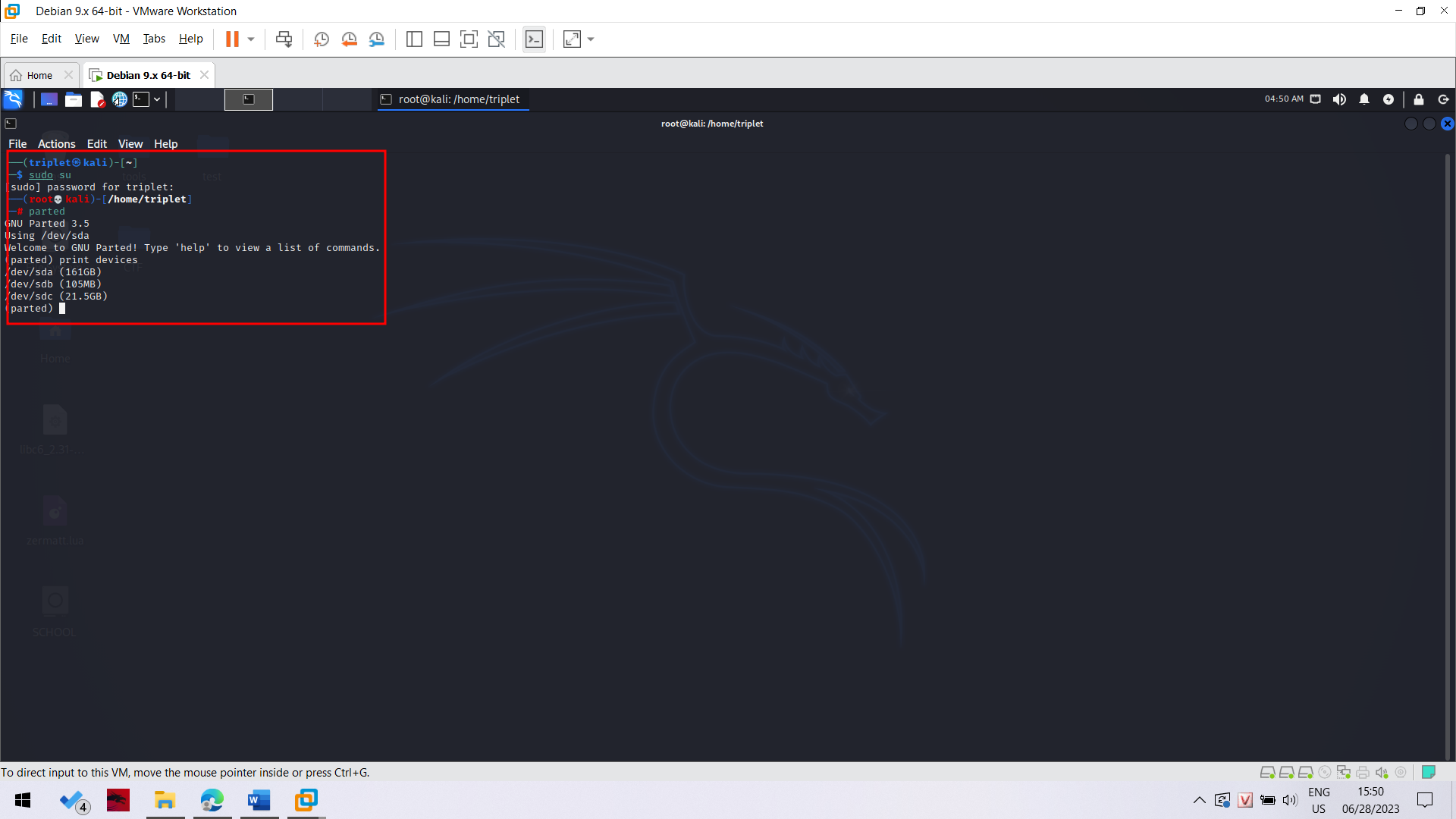


In the BIOS, use the arrow keys to adjust the boot order, moving the CD-ROM to the top, as shown above.

Press F10 and Enter to save the BIOS settings.

A prompt says boot:. Press Enter.

Bây giờ chúng ta sẽ tiến hành format ổ cứng.



This lists the attached devices, as shown above on this page.

Find the evidence drive--it is 105 MB in size. When I did it, the evidence drive was /dev/sdb.

The 21.5 GB empty hard drive available to perform collection was /dev/sdc.

**Formatting the Empty Drive**

We will use the empty drive to acquire an image of the evidence drive. It must be formatted first.

In the Terminal window, at the (parted) prompt, enter these commands, pressing the Enter key after each one.

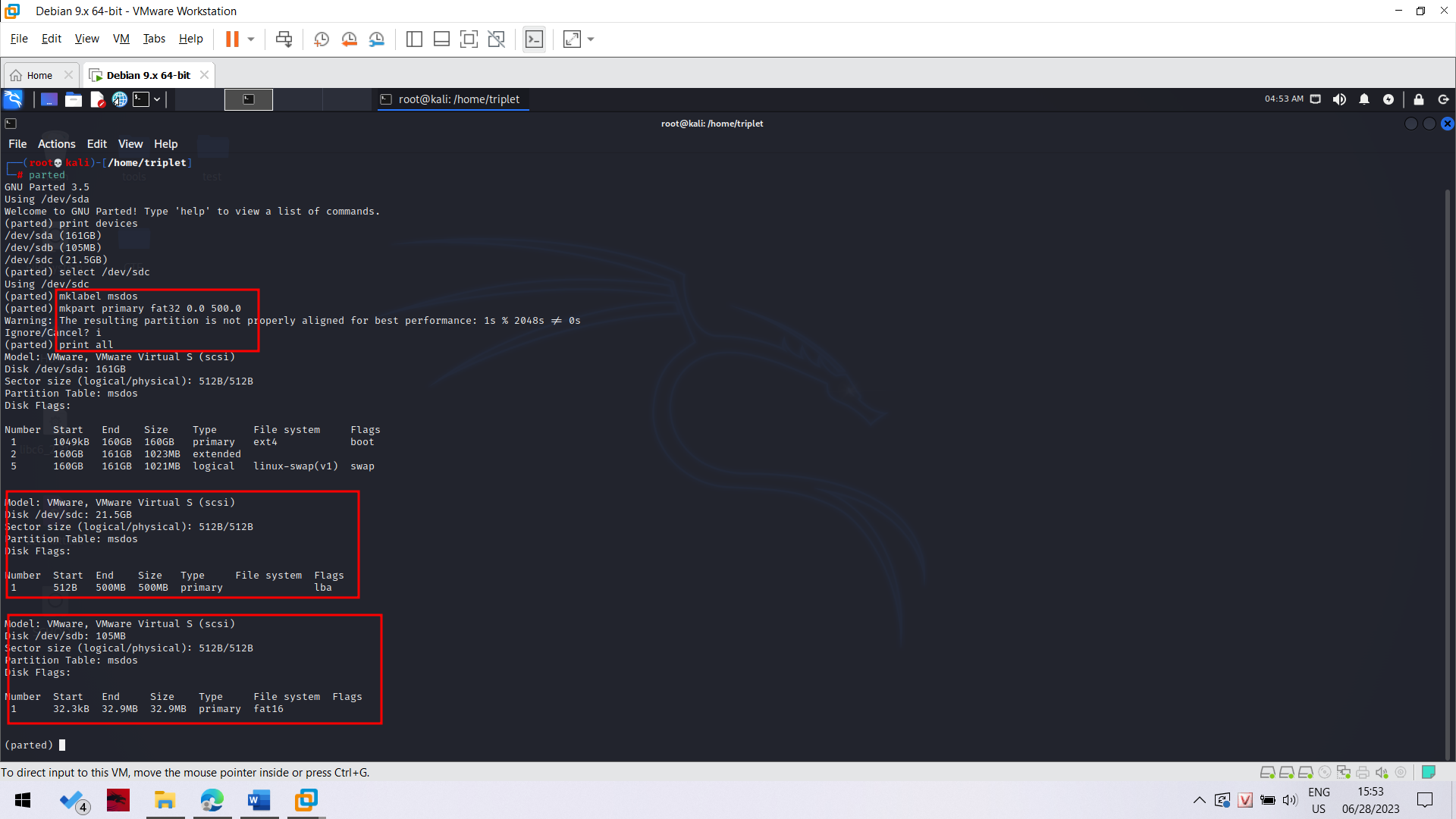
These commands make a 500 MB partition on the empty drive.

In the first command, make sure you are selecting the empty drive, not the evidence drive!

**select /dev/sdc**

**mklabel msdos**

**mkpart primary fat32 0.0 500.0**



In the Terminal window, at the (parted) prompt, enter this command, and then press Enter:

quit

This closes parted and returns you to the normal Linux bash prompt.

**Mounting the Partition**

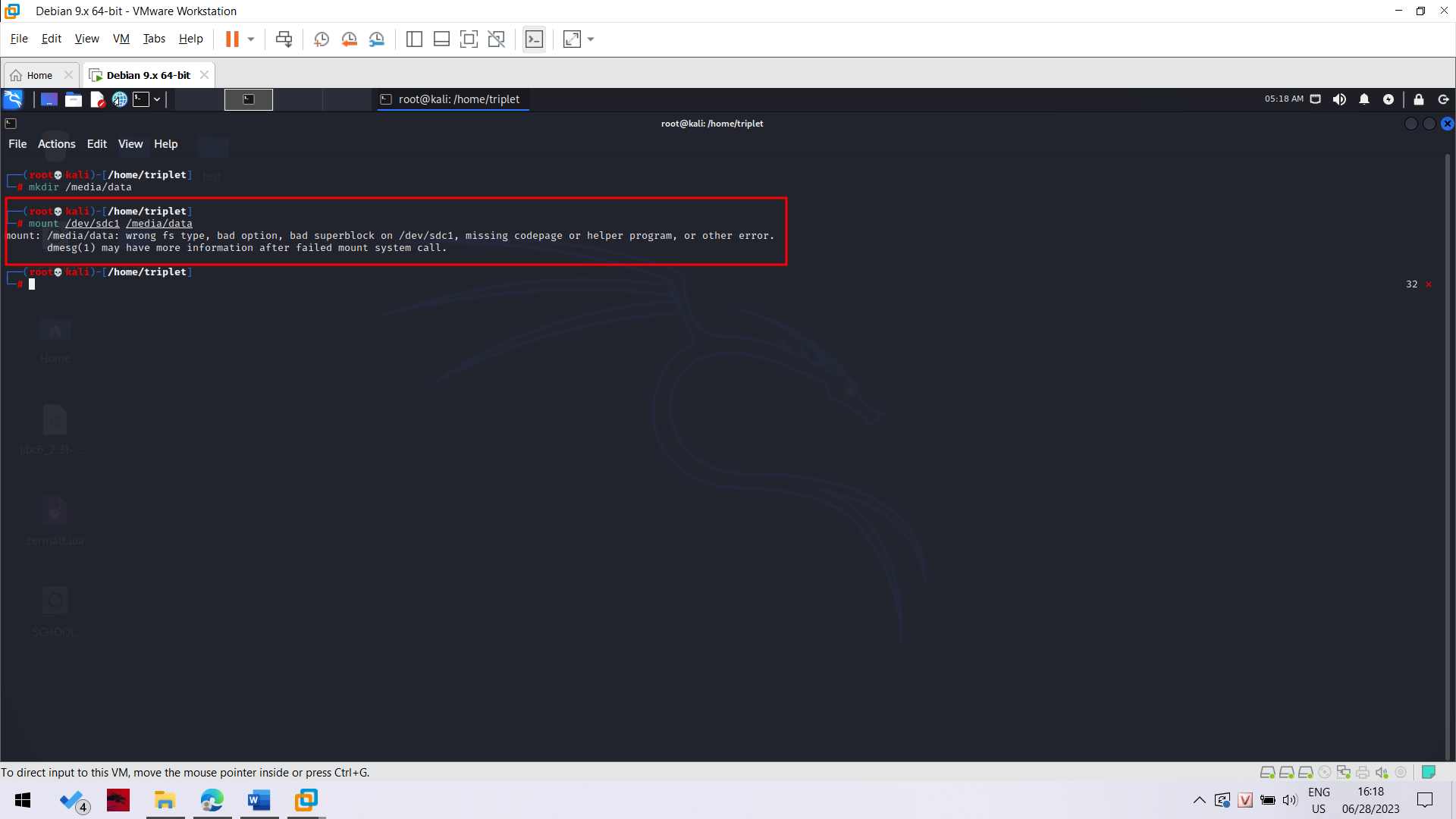
Now you must mount the new partition.

These are the missing steps in the classroom demo on 2-14-13. The earlier version of Backtrack I used previously automatically mounted the filesystem.

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

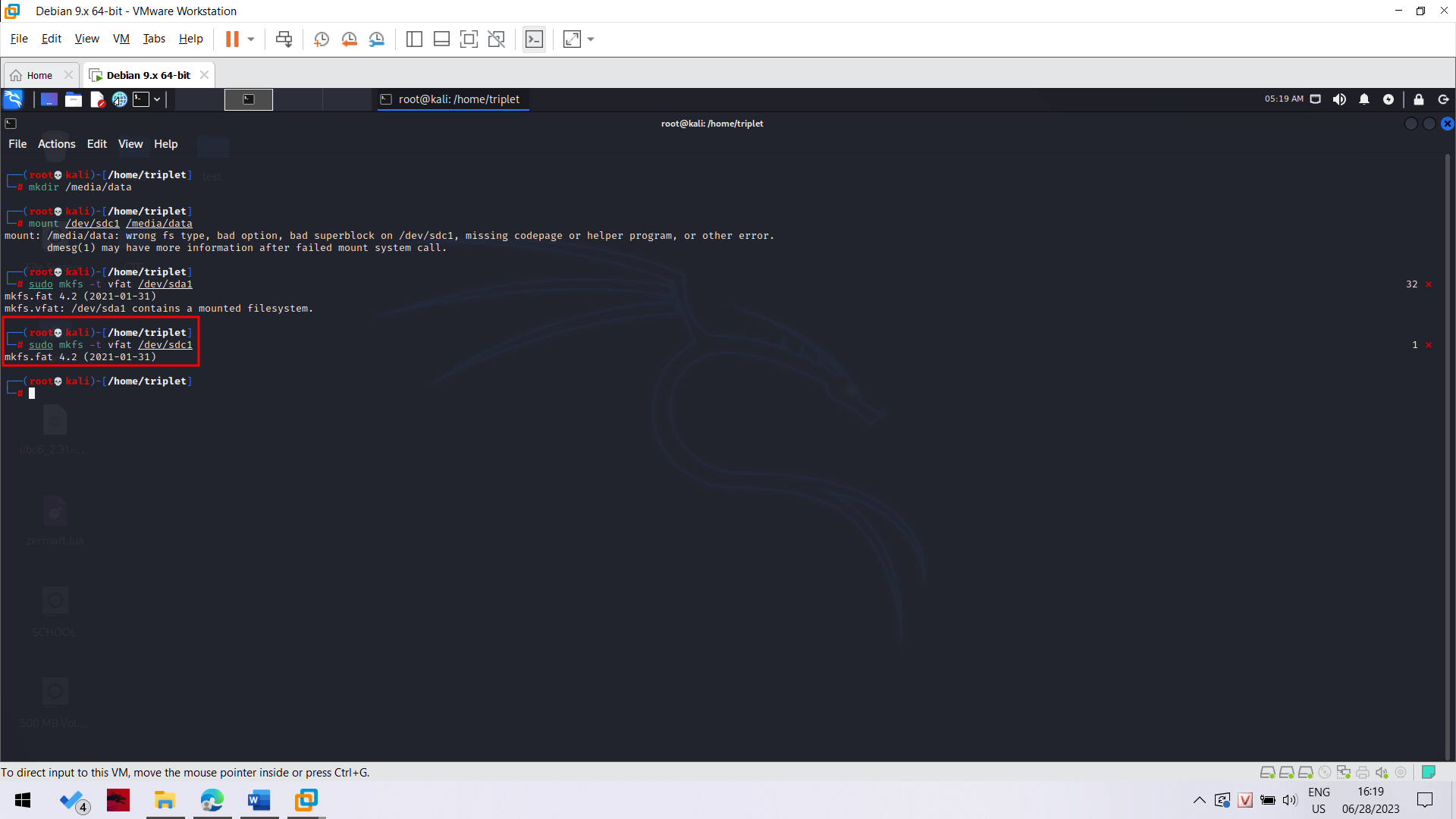
**mkdir /media/data**

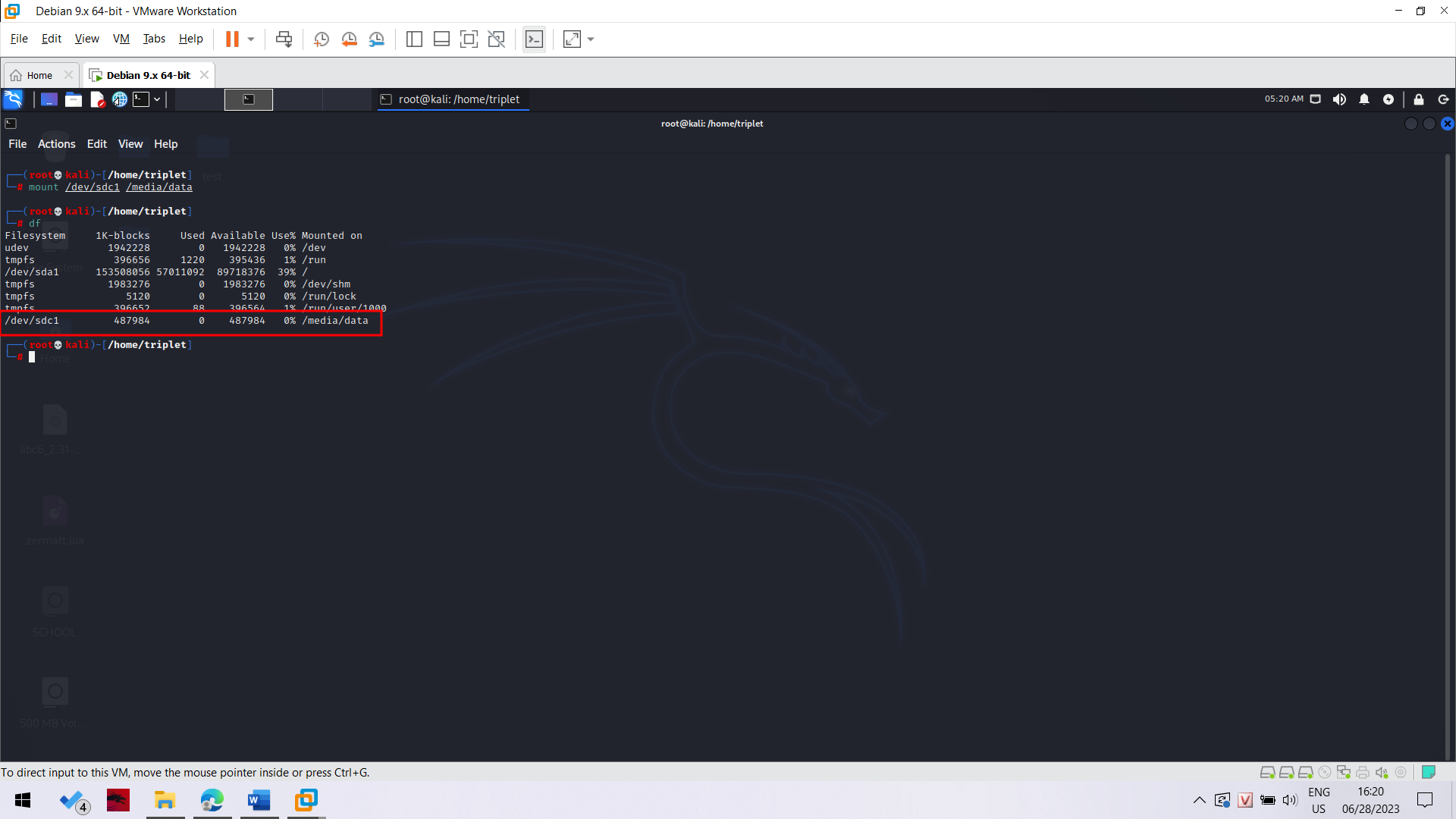
**mount /dev/sdc1 /media/data**



**Error -> Fix by using this**

sudo mkfs -t vfat /dev/sdc1





**Df**

**Testing the Working Partition**

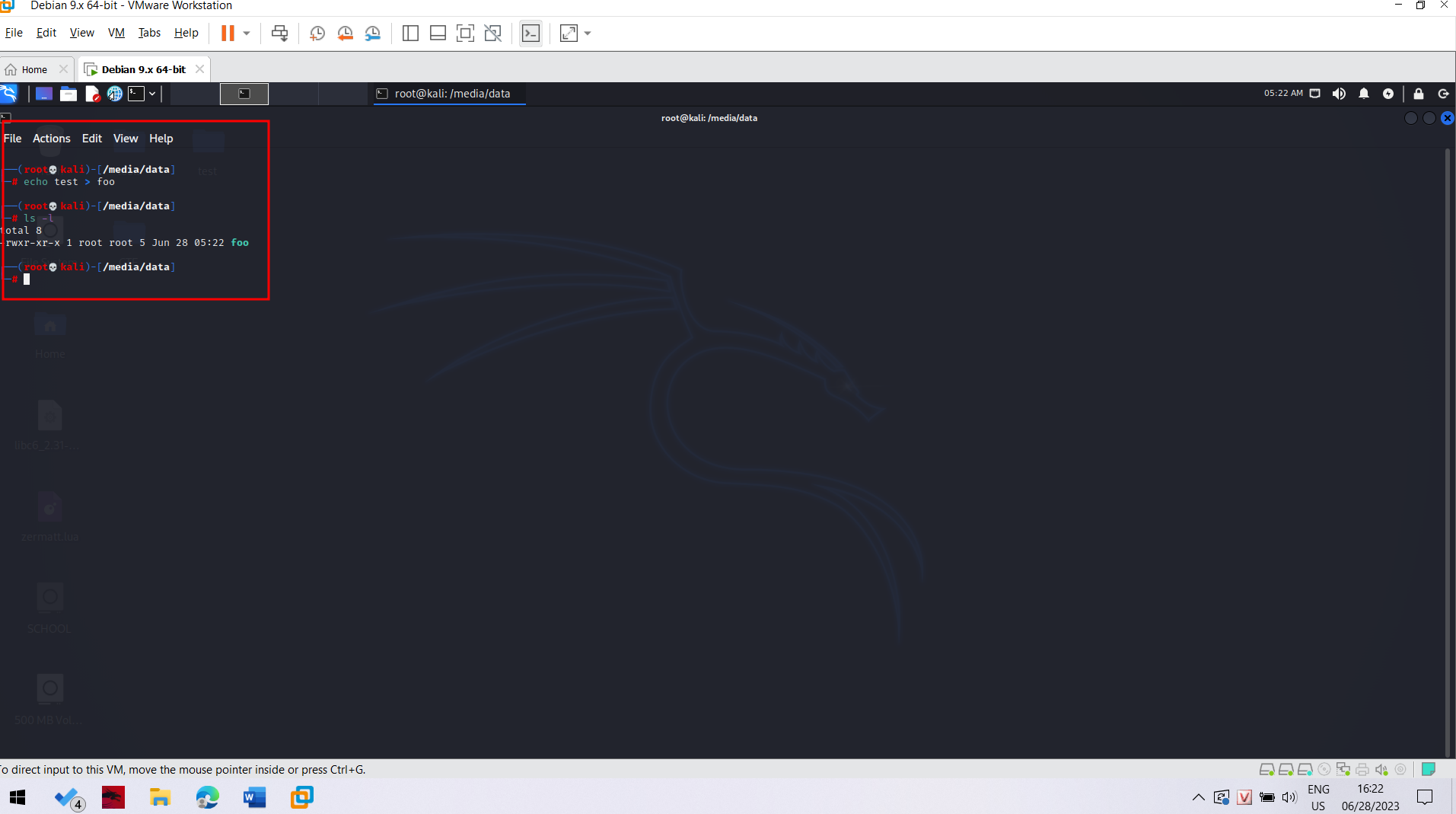
In the Terminal window, type these commands, pressing Enter after each one.

These commands change the working directory to the empty drive, create a small file on it, and display a directory of files.

Notice that the last command contains two lowercase "L" characters--they are not numeral "1" characters.

cd /media/data

echo test > foo

ls -l 

**Acquiring an Image of the Whole Evidence Disk with dd**

In the Terminal window, type these commands, pressing Enter after each one.

The dd command copies data from the evidence drive to a file named YOURNAME-dd. (Replace YOURNAME with your own name).

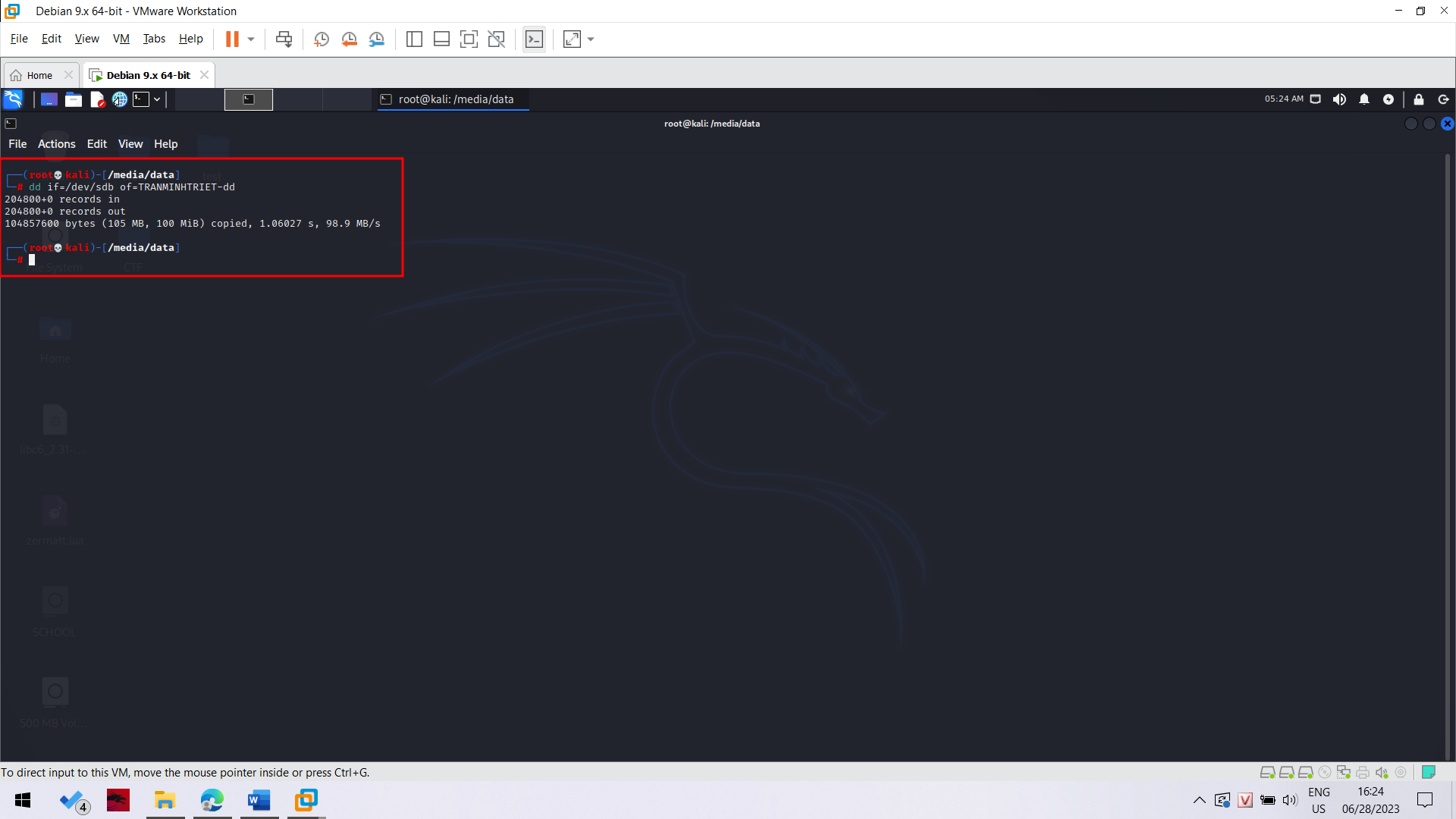
The md5sum command calculates the md5 hash and puts it in a file named YOURNAME-dd-hash.

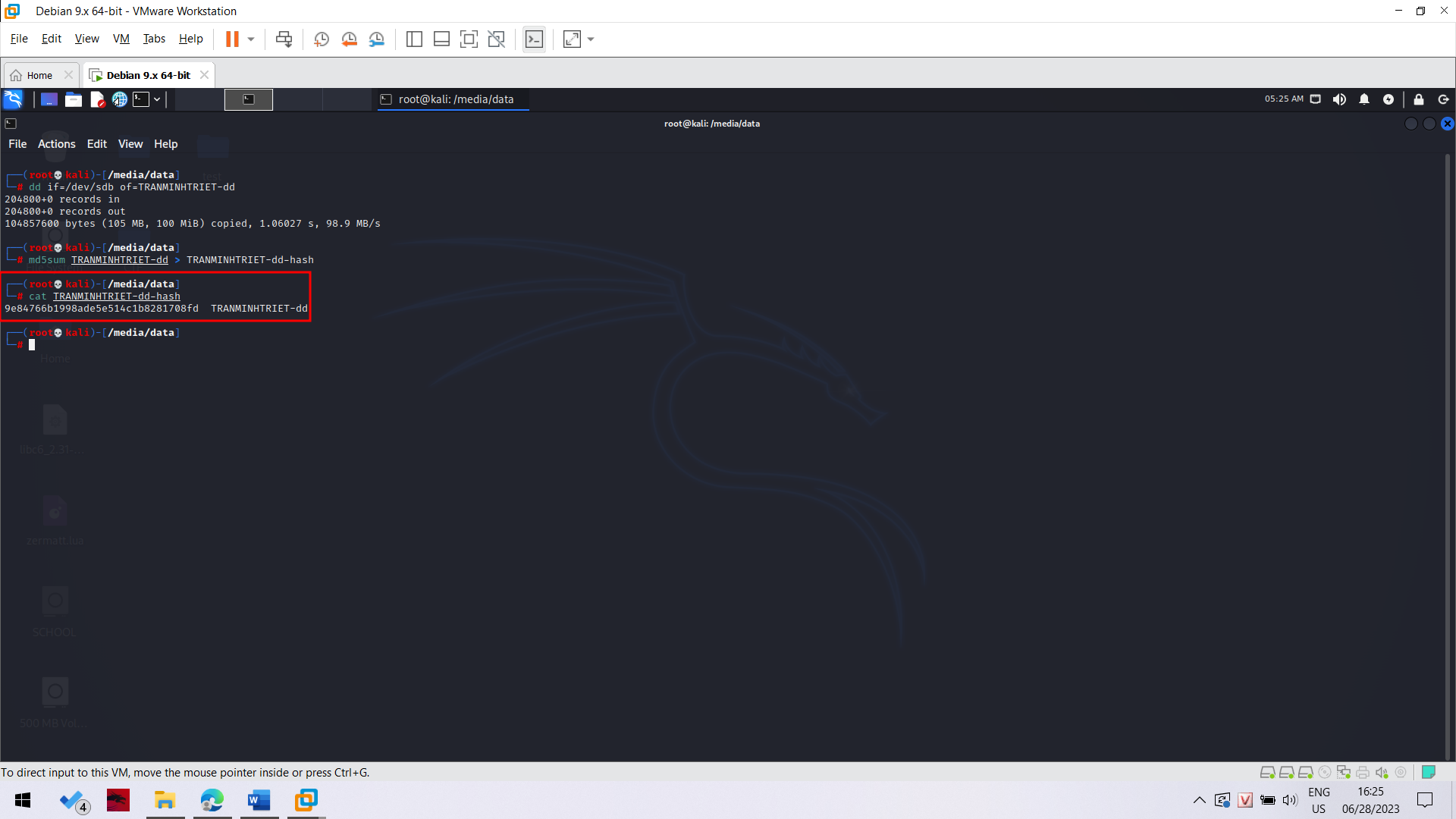
The cat command prints the contents of the YOURNAME-dd-hash file.

dd if=/dev/sda of=YOURNAME-dd

md5sum YOURNAME-dd > YOURNAME-dd-hash

cat YOURNAME-dd-hash





Đoạn hash giống y chang trong bài lab

**Comparing the Hash to the Hashcalc Value**

This hash doesn't match the MD5 hash you calculated previously from the VMware hard disk file. That's OK, because the VMware hard disk format is not a simple dd of a hard drive.

**Acquiring an Image of One Partition with dd**

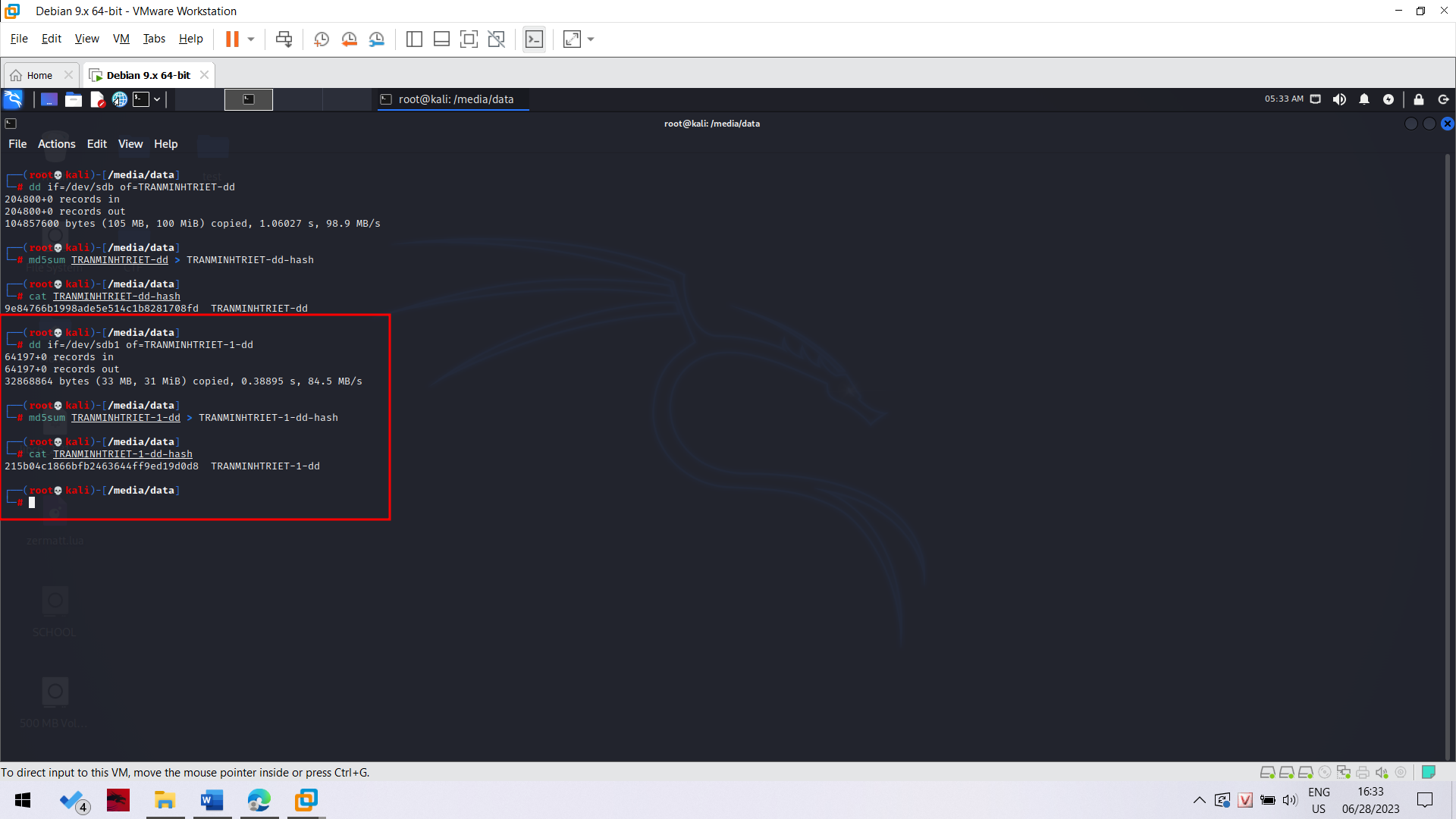
We could also capture only the partition from the drive, which might contain all the data we are interested in, or perhaps all the data we are authorized to collect.

In the Terminal window, type these commands, pressing Enter after each one.

**dd if=/dev/sdb1 of=YOURNAME-1-dd**

**md5sum YOURNAME-1-dd > YOURNAME-1-dd-hash**

**cat YOURNAME-1-dd-hash**



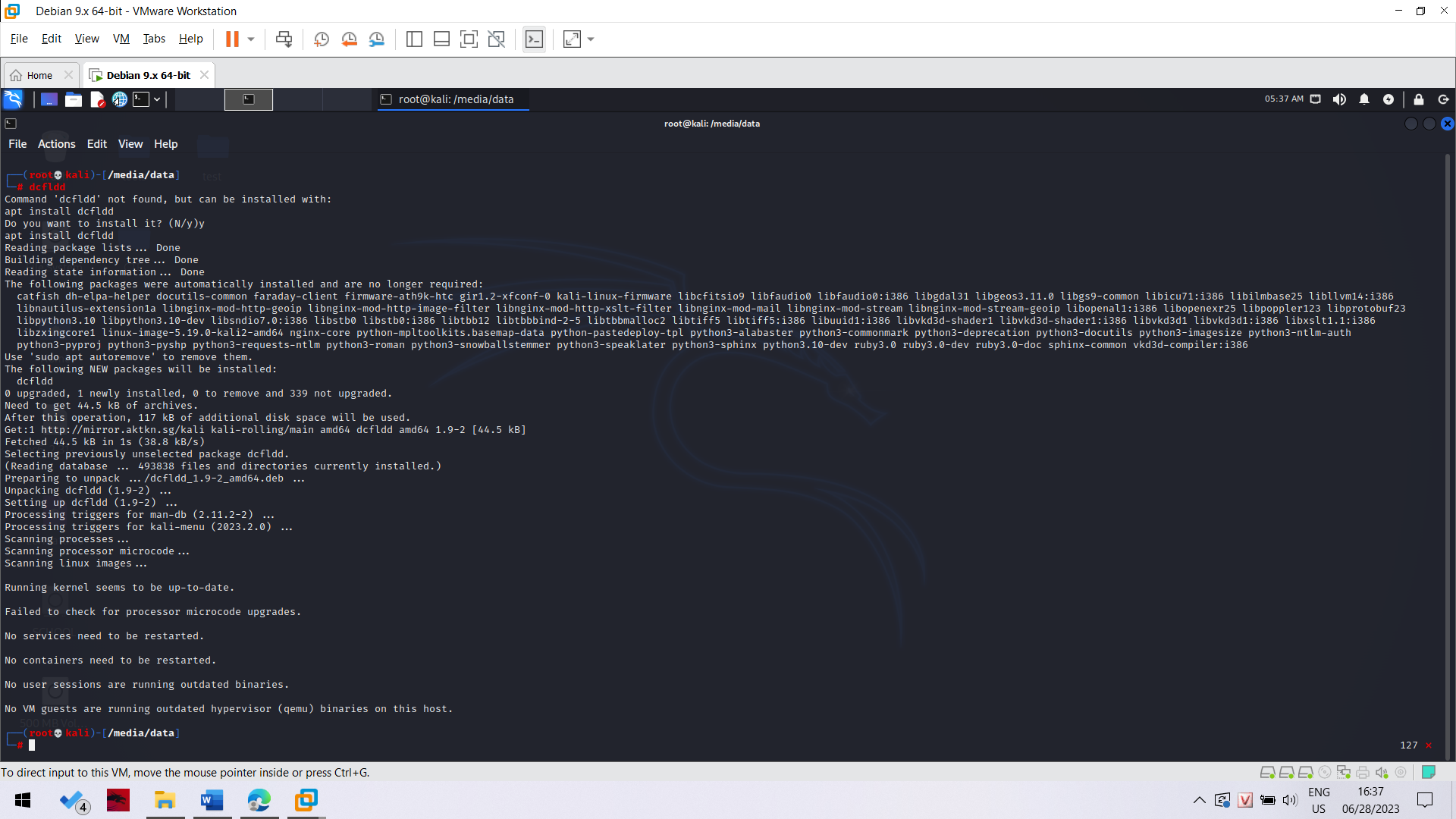
**Acquiring an Image of the Whole Evidence Disk with dcfldd**

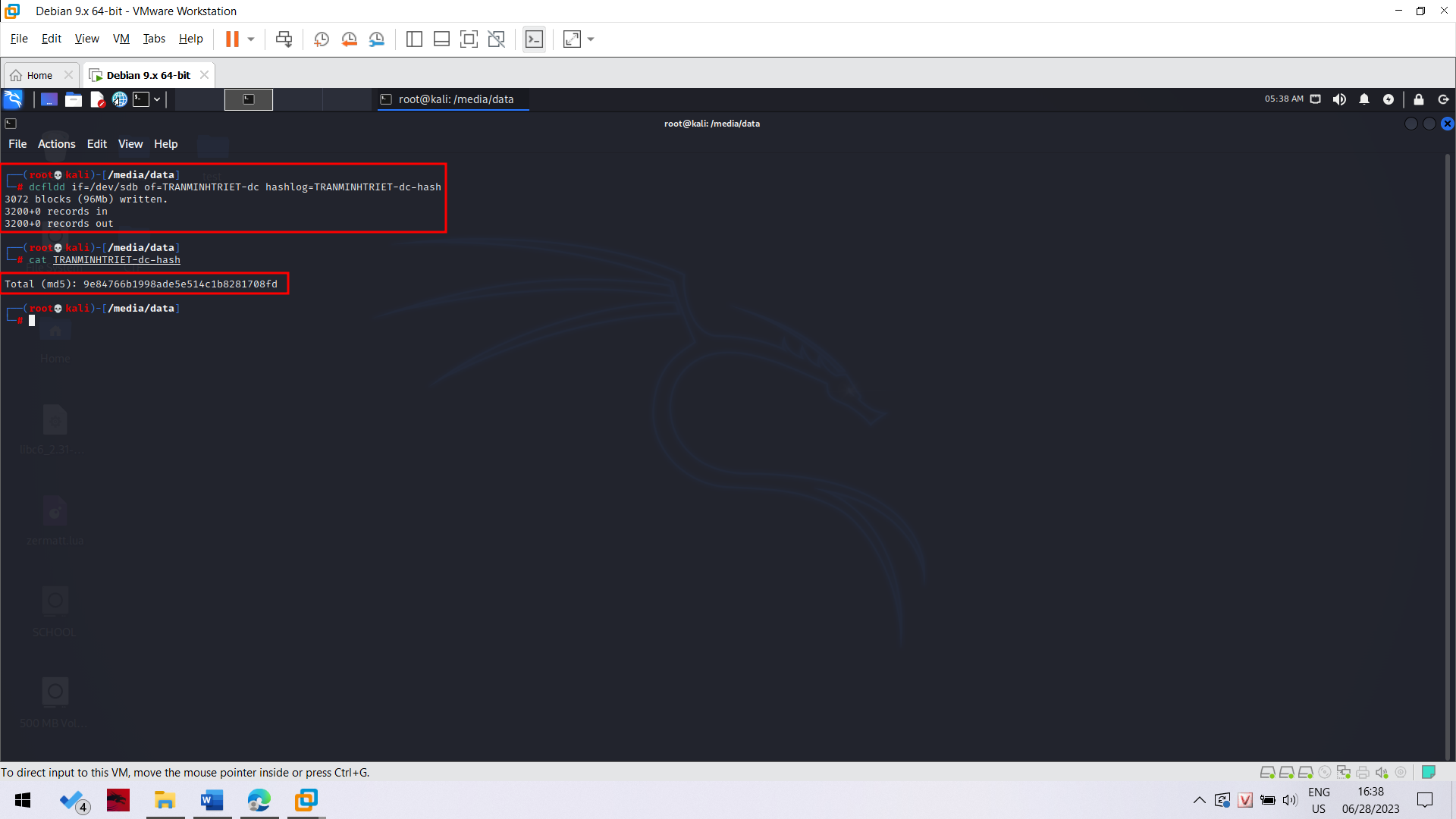
dcfldd is an enhanced version of dd developed by the U.S. Department of Defense Computer Forensics Lab. It's included in BackTrack.

In the Terminal window, type these commands, pressing Enter after each one.

**dcfldd if=/dev/sda of=YOURNAME-dc hashlog=YOURNAME-dc-hash**

**cat YOURNAME-dc-hash**





Notice that this is nicer--it shows a running count of blocks written to reassure you that it hasn't crashed.

The hash value should match the hash value you calculated earlier after the dd command.

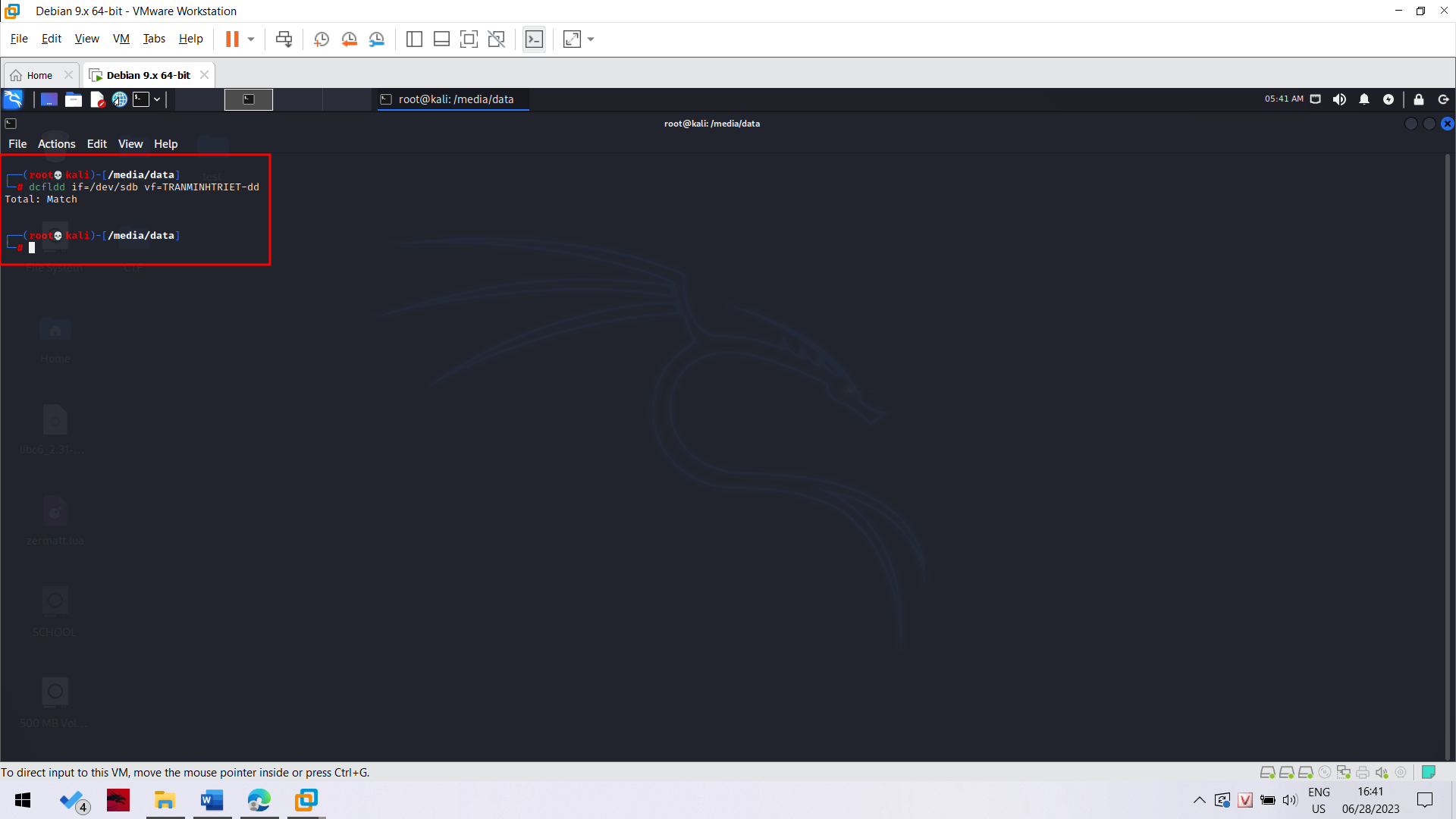
In the Terminal window, type this command, followed by the Enter key. (The command contains two lowercase L characters, and no numerals.)

ls -l

**Using dcfldd to Verify the Image**

In the Terminal window, type this command, followed by the Enter key:

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



The vf value points to an image which is compared to the if file.

The result is "Total: Match", as shown below on this page.