

Maria Valencia

CSC 153

Lab 3

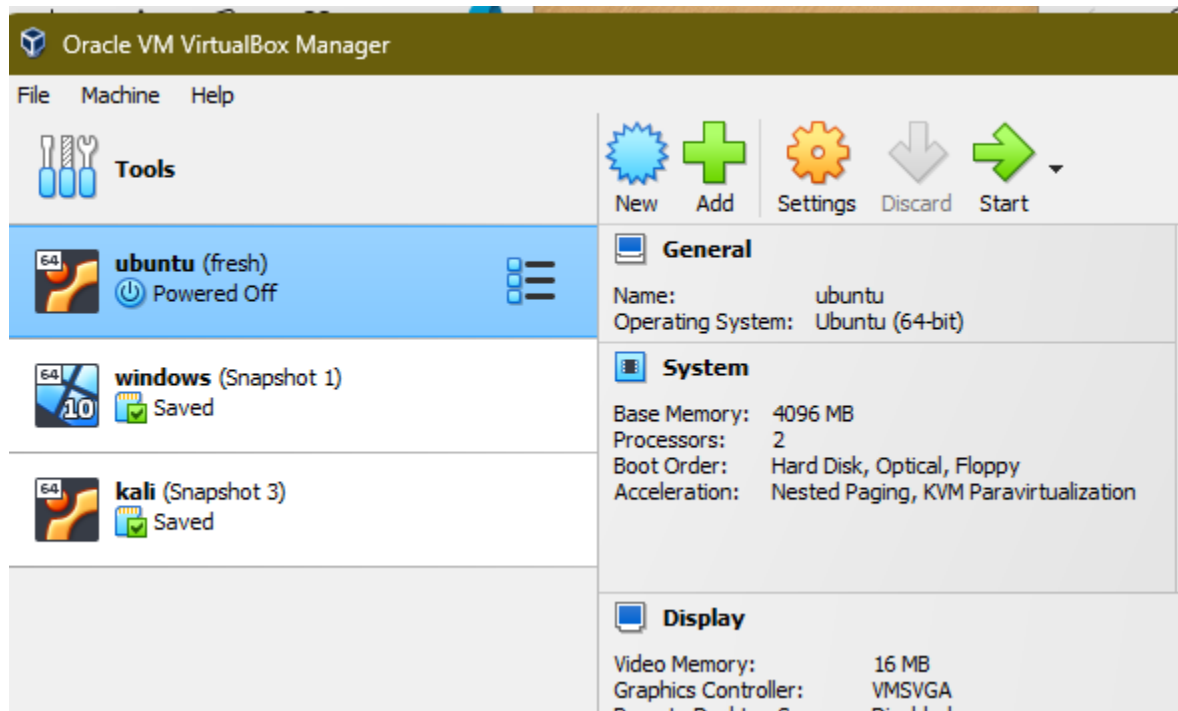
Data Acquisition

In this lab, I performed various data acquisition activities inspired by the demonstrations from the textbook. I prepared a target drive, acquired data using dd and created an image using FTK.

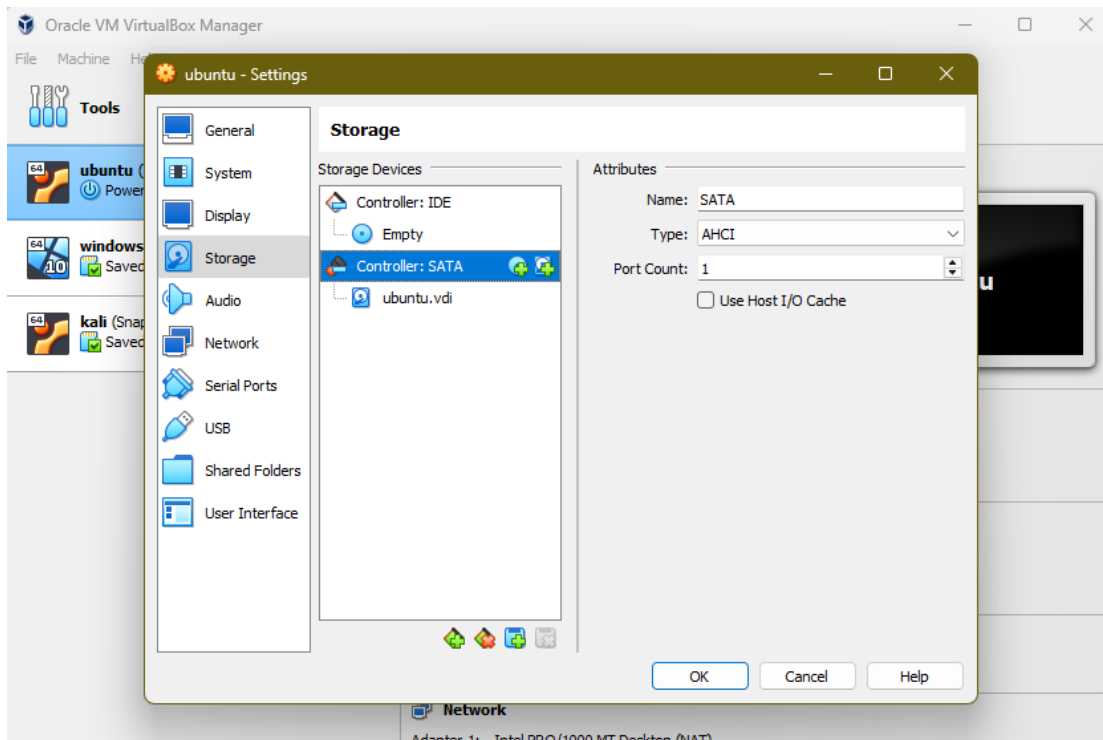
Task 1

In task 1, I created a VHD drive and prepared it for data acquisition using my Ubuntu/Linux VM.

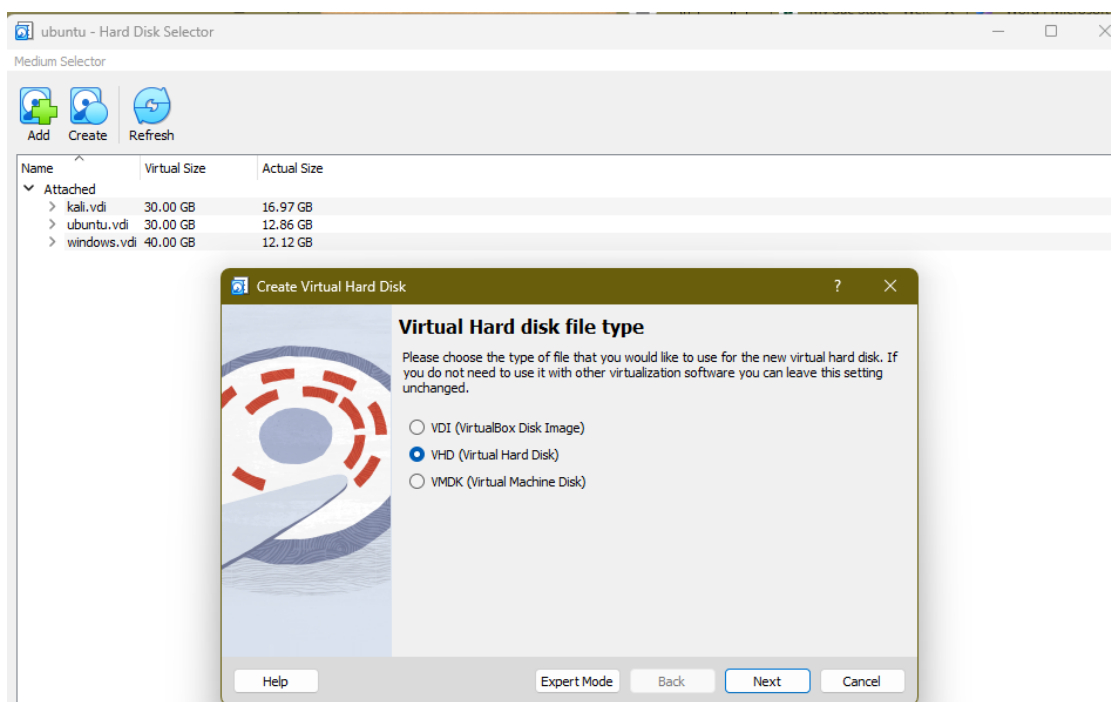
Step 1: I opened VirtualBox and selected the Ubuntu VM settings.



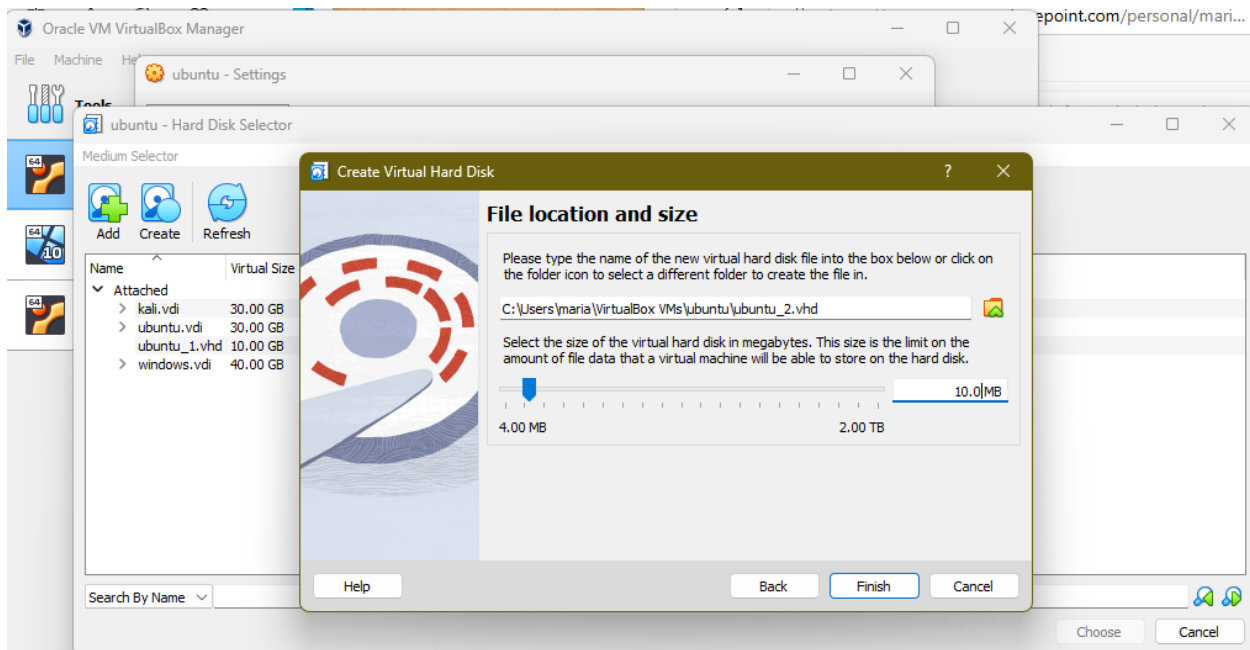
In the settings menu, I selected “Storage” and then “Controller: SATA” and then the “Add hard disk” button in the “Storage devices” section.



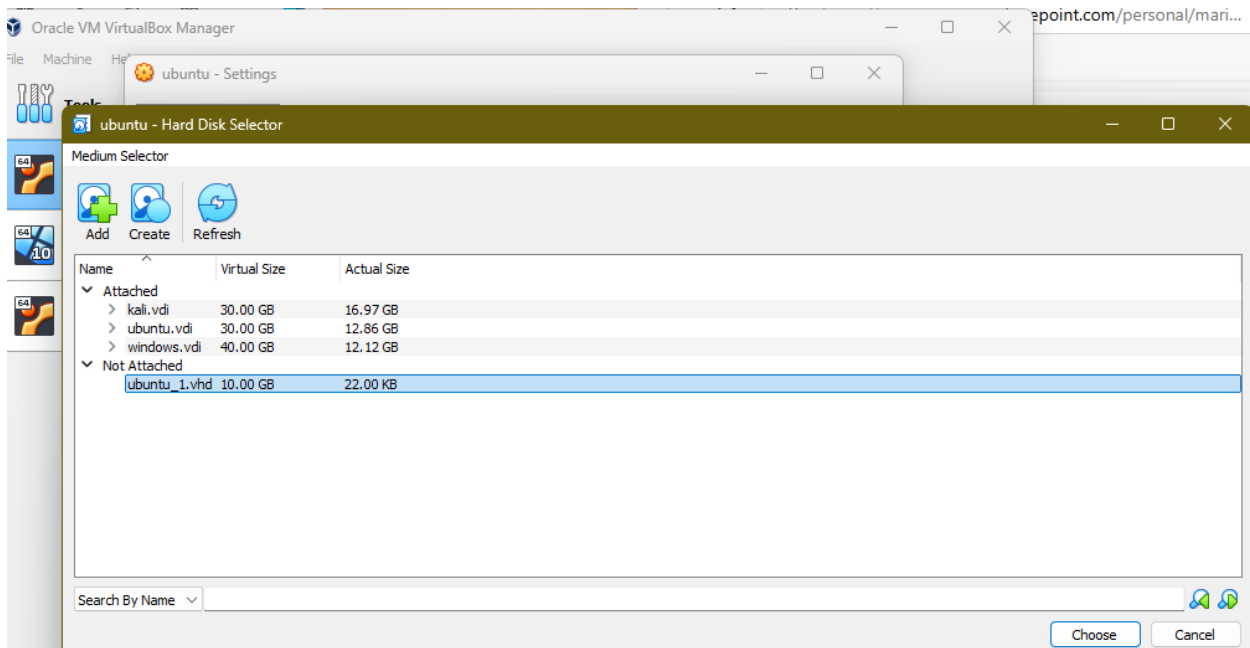
Then I selected create and VHD then next.



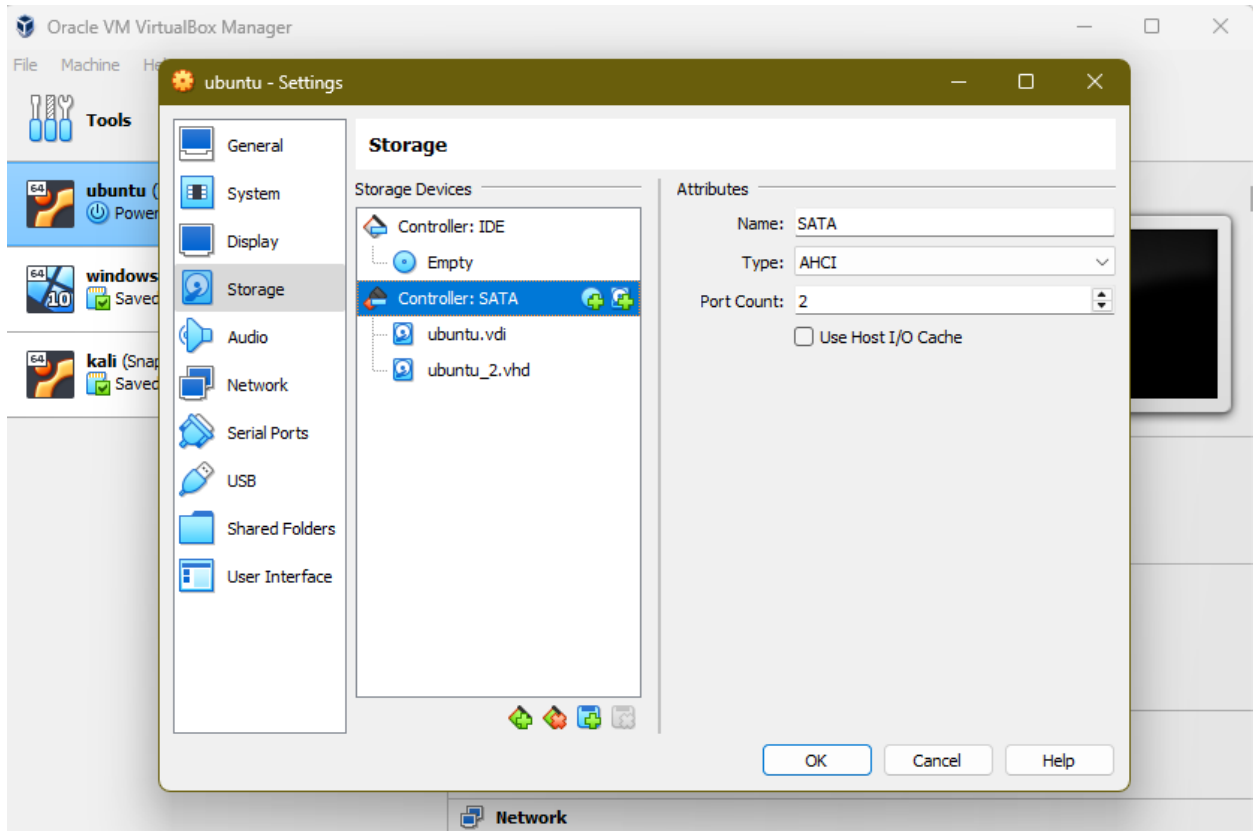
Here I made the disk size 10MB and clicked finish,,



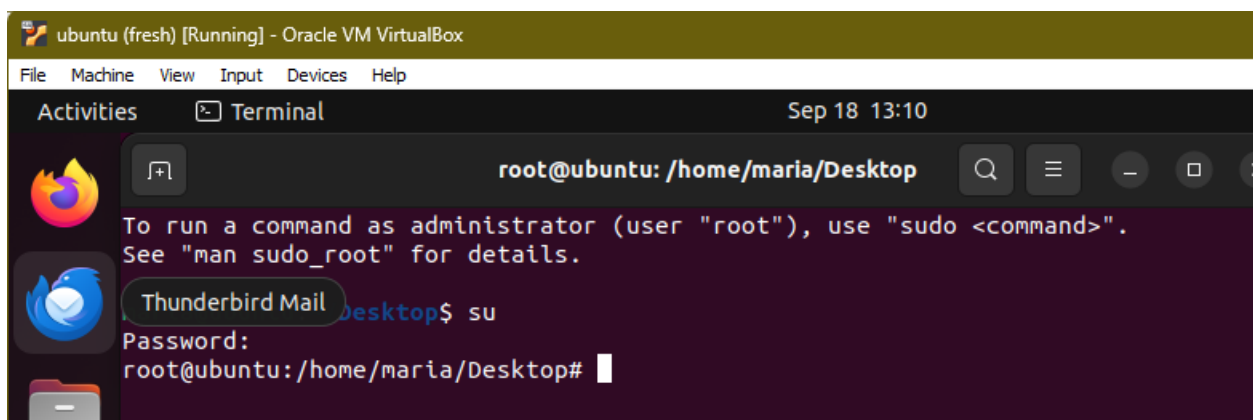
After I created it, I clicked on it and selected choose at the bottom.



Then, I pressed okay and started the VM.



Step 2: After I logged into the VM, I opened a terminal and switched the user to root using the “su” command and entered the user password.



I listed the disk devices using the “fdisk -l” command

```
root@ubuntu: /home/maria/Desktop# fdisk -l
Disk /dev/loop0: 4 KiB, 4096 bytes, 8 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/loop1: 74.21 MiB, 77819904 bytes, 151992 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/loop2: 266.63 MiB, 279584768 bytes, 546064 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/loop3: 496.98 MiB, 521121792 bytes, 1017816 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/loop4: 74.27 MiB, 77881344 bytes, 152112 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/loop5: 91.69 MiB, 96141312 bytes, 187776 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

I then observed the 10 MiB VBOX HARDDISK in the output

```
Disk /dev/sdb: 10 MiB, 10485760 bytes, 20480 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

Then, I pointed fdisk to the target drive by running “fdisk/dev/sdb”

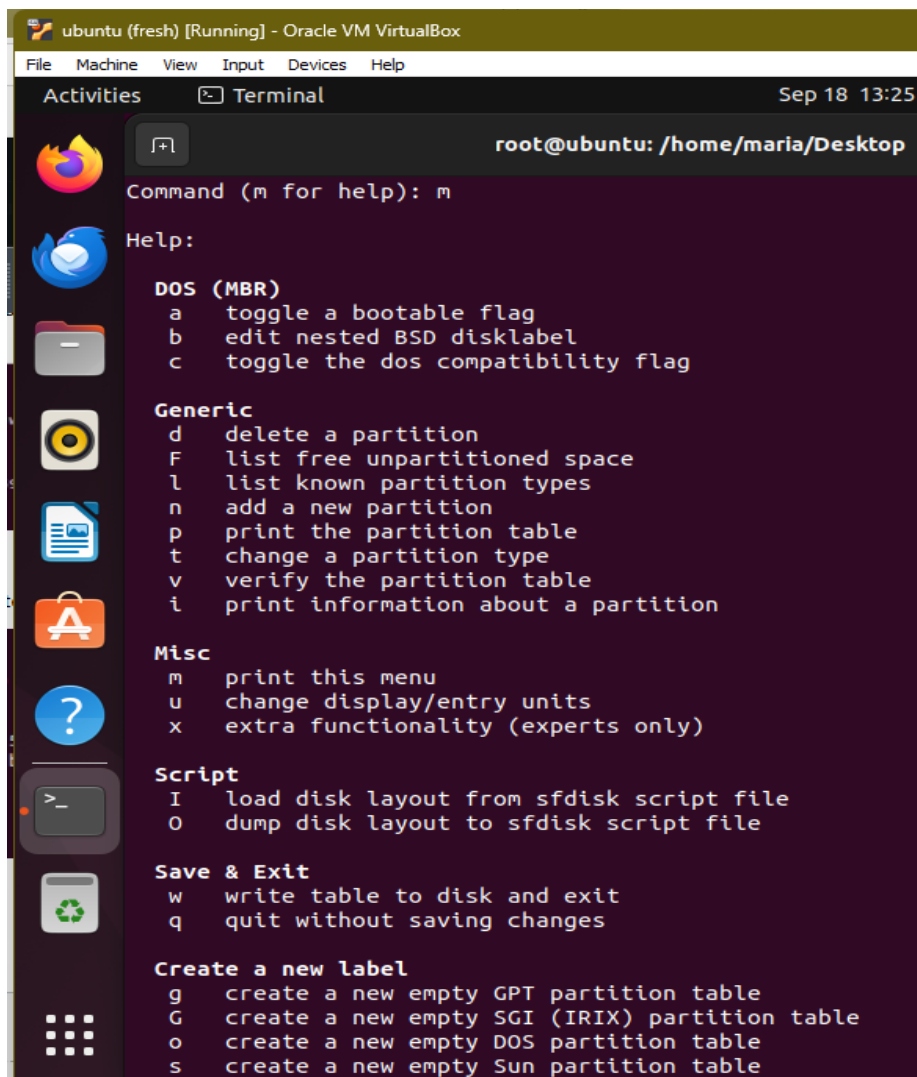
```
root@ubuntu:/home/maria/Desktop# fdisk /dev/sdb

Welcome to fdisk (util-linux 2.37.2).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0xae6b413b.

Command (m for help):
```

I then pressed “m” for the help menu and reviewed the partitions of the target drive using the “p” command.

The screenshot shows a terminal window titled "ubuntu (fresh) [Running] - Oracle VM VirtualBox". The terminal prompt is "root@ubuntu: /home/maria/Desktop". The user has entered the command "m" to view the help menu. The help menu is displayed with the following sections: "DOS (MBR)" with options a, b, and c; "Generic" with options d, F, l, n, p, t, v, and i; "Misc" with options m, u, and x; "Script" with options I and O; "Save & Exit" with options w and q; and "Create a new label" with options g, G, o, and s. The terminal window has a sidebar with various application icons and a top menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". The date and time "Sep 18 13:25" are shown in the top right corner.

```
ubuntu (fresh) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Sep 18 13:25
root@ubuntu: /home/maria/Desktop
Command (m for help): m
Help:
DOS (MBR)
a toggle a bootable flag
b edit nested BSD disklabel
c toggle the dos compatibility flag

Generic
d delete a partition
F list free unpartitioned space
l list known partition types
n add a new partition
p print the partition table
t change a partition type
v verify the partition table
i print information about a partition

Misc
m print this menu
u change display/entry units
x extra functionality (experts only)

Script
I load disk layout from sfdisk script file
O dump disk layout to sfdisk script file

Save & Exit
w write table to disk and exit
q quit without saving changes

Create a new label
g create a new empty GPT partition table
G create a new empty SGI (IRIX) partition table
o create a new empty DOS partition table
s create a new empty Sun partition table
```

```
Command (m for help): p
Disk /dev/sdb: 10 MiB, 10485760 bytes, 20480 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xae6b413b

Command (m for help):
```

Here, I created a primary partition using the “n” command and enter a few times to accept the default options.

```
Command (m for help): n
Partition type
  p   primary (0 primary, 0 extended, 4 free)
  e   extended (container for logical partitions)
Select (default p):

Using default response p.
Partition number (1-4, default 1):
First sector (2048-20479, default 2048):
Last sector, +/-sectors or +/-size[K,M,G,T,P] (2048-20479, default 20479):

Created a new partition 1 of type 'Linux' and of size 9 MiB.

Command (m for help):
```

I observed the new linux partition by pressing the “p” command.

```
Command (m for help): p
Disk /dev/sdb: 10 MiB, 10485760 bytes, 20480 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xae6b413b

Device      Boot Start    End Sectors  Size Id Type
/dev/sdb1           2048 20479   18432    9M 83 Linux

Command (m for help):
```

I changed the target drive's partition to Windows 95 FAT32 file system using the "t" command and "0c" as the hex code.

```
Command (m for help): t
Selected partition 1
Hex code or alias (type L to list all): 0c
Changed type of partition 'Linux' to 'W95 FAT32 (LBA)'.

Command (m for help):
```

I checked the partition file type using the "p" command and observed that it now lists W95 FAT32 (LBA) as the file system.

```
Command (m for help): p
Disk /dev/sdb: 10 MiB, 10485760 bytes, 20480 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xae6b413b

Device            Boot Start    End  Sectors  Size Id Type
/dev/sdb1          2048 20479   18432    9M  c W95 FAT32 (LBA)

Command (m for help):
```

I saved the partition settings using the "w" command.

```
Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.

root@ubuntu:/home/maria/Desktop#
```

I used the "fdisk -l" command to list the drives again and observed the target drive now shows the W95 FAT32 (LBA) partition.

```
Disk /dev/sdb: 10 MiB, 10485760 bytes, 20480 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xae6b413b

Device            Boot Start    End  Sectors  Size Id Type
/dev/sdb1          2048 20479   18432    9M  c W95 FAT32 (LBA)
```


I formatted the partition as a FAT filesystem using “mkfs.msdos -vF32 /dev/sdb1”

```
root@ubuntu:/home/maria/Desktop# mkfs.msdos -vF32 /dev/sdb1
mkfs.fat 4.2 (2021-01-31)
WARNING: Number of clusters for 32 bit FAT is less then suggested minimum.
/dev/sdb1 has 255 heads and 63 sectors per track,
hidden sectors 0x0800;
logical sector size is 512,
using 0xf8 media descriptor, with 18396 sectors;
drive number 0x80;
filesystem has 2 32-bit FATs and 1 sector per cluster.
FAT size is 142 sectors, and provides 18080 clusters.
There are 32 reserved sectors.
Volume ID is a50a211b, no volume label.
root@ubuntu:/home/maria/Desktop#
```

Task 2

In task 2, I conducted my own Ubuntu VM while utilizing the prepared drive from task 1. I copied the first 10 MBs of the VM host onto the prepared drive.

Step 1: I switched the user to root using the “su” command and ran “fdisk -l” to list the devices. I observed that sda1-3 is the host system (system) and sdb1 is the external drive (target).

```
Disk /dev/sda: 30 GiB, 32212254720 bytes, 62914560 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 5B52DB1E-A907-4861-AD93-013FAFBA6849

Device            Start      End  Sectors  Size Type
/dev/sda1          2048      4095     2048    1M BIOS boot
/dev/sda2          4096 1054719 1050624   513M EFI System
/dev/sda3        1054720 62912511 61857792 29.5G Linux filesystem

Disk /dev/sdb: 10 MiB, 10485760 bytes, 20480 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xae6b413b

Device  Boot Start    End  Sectors  Size Id Type
/dev/sdb1      2048 20479    18432    9M  c W95 FAT32 (LBA)
```

I created a mount point for my external drive using the “mkdir /mnt/sdb1” command. I mounted the external drive to the mount point using the “mount -t vfat /dev/sdb1/mnt/sdb1” command. Then, I changed the directory to the mount point using the “cd/mnt/sdb1” command and listed the file contents using “ls -la” command.

```
Disk /dev/loop8: 40.43 MiB, 42393600 bytes, 82800 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
root@ubuntu:/home/maria/Desktop# mkdir /mnt/sdb1
root@ubuntu:/home/maria/Desktop# mount -t vfat /dev/sdb1 /mnt/sdb1
root@ubuntu:/home/maria/Desktop# cd /mnt/sdb1
root@ubuntu:/mnt/sdb1# ls -la
total 5
drwxr-xr-x 2 root root 512 Dec 31 1969 .
drwxr-xr-x 3 root root 4096 Sep 18 13:48 ..
root@ubuntu:/mnt/sdb1#
```

Using dd, I made a forensic copy of the sda3 partition’s first 8 MBs while split into two files using the “dd if=/dev/sda3 bs=512 count=16384 | split -b 4m -image_sda3” command.

```
root@ubuntu:/mnt/sdb1# dd if=/dev/sda3 bs=512 count=16384 | split --b 4m - image_sda3
16384+0 records in
16384+0 records out
8388608 bytes (8.4 MB, 8.0 MiB) copied, 0.296194 s, 28.3 MB/s
root@ubuntu:/mnt/sdb1#
```

I verified 8 MBs were copied into two files using the “ls -lah” command.

```
root@ubuntu:/mnt/sdb1# ls -lah
total 8.1M
drwxr-xr-x 2 root root 512 Dec 31 1969 .
drwxr-xr-x 3 root root 4.0K Sep 18 13:48 ..
-rwxr-xr-x 1 root root 4.0M Sep 18 13:56 image_sda3aa
-rwxr-xr-x 1 root root 4.0M Sep 18 13:56 image_sda3ab
root@ubuntu:/mnt/sdb1#
```

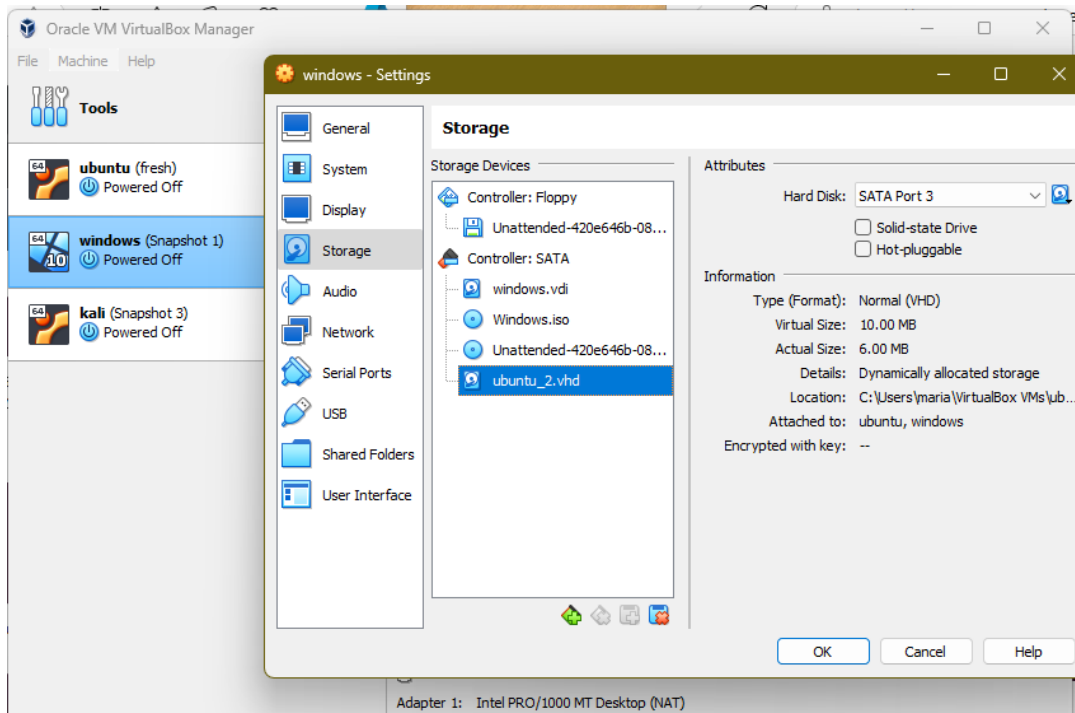
I unmounted the external disk by changing the directory “cd ..” and used the “unmount /dev/sdb1” command.

```
root@ubuntu:/mnt/sdb1# cd ..
root@ubuntu:/mnt# unmount /dev/sdb1
Command 'unmount' not found, did you mean:
  command 'umount' from deb mount (2.37.2-4ubuntu3.4)
Try: apt install <deb name>
root@ubuntu:/mnt# umount /dev/sdb1
root@ubuntu:/mnt#
```

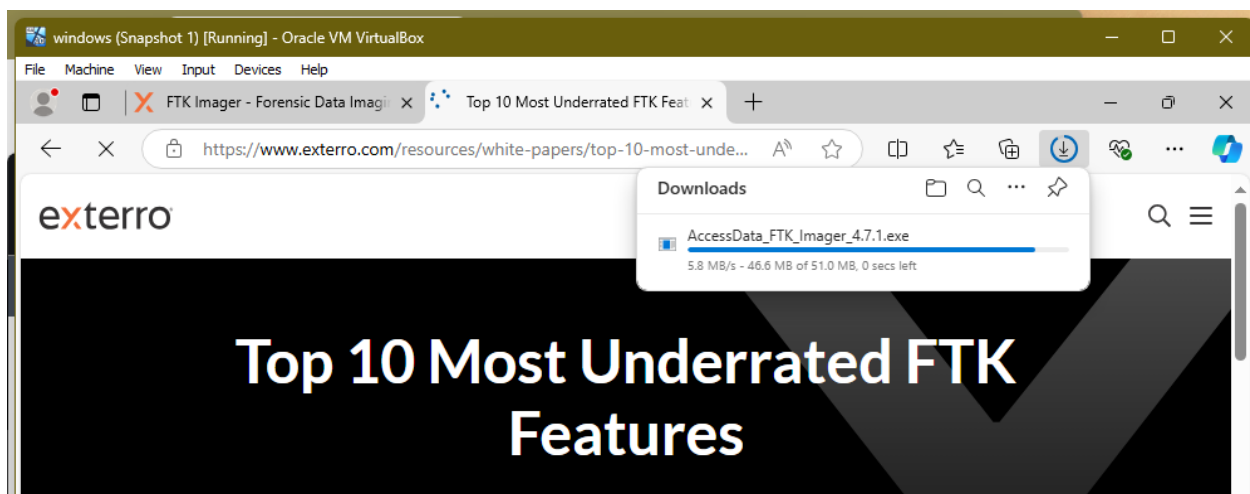
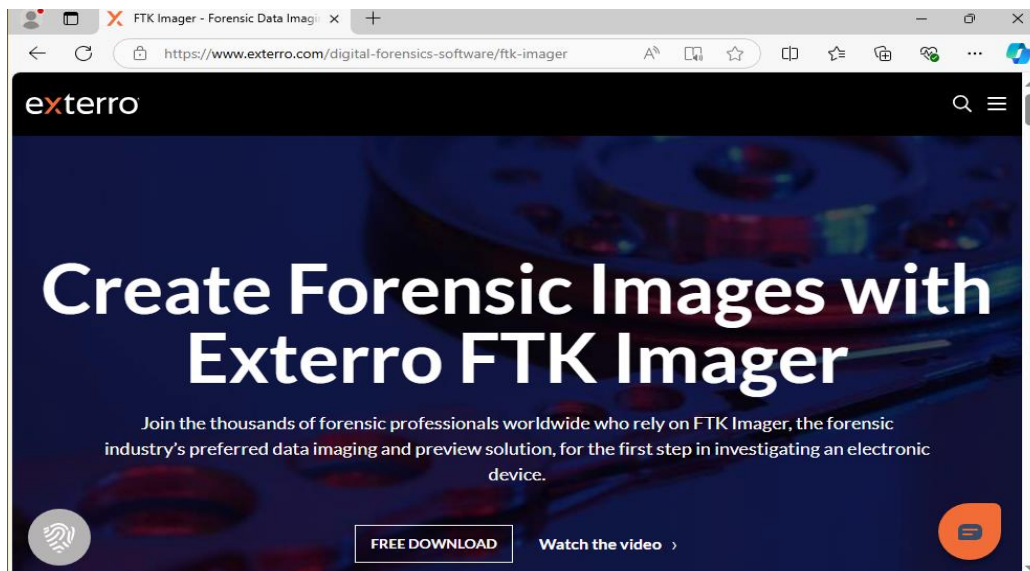
Task 3

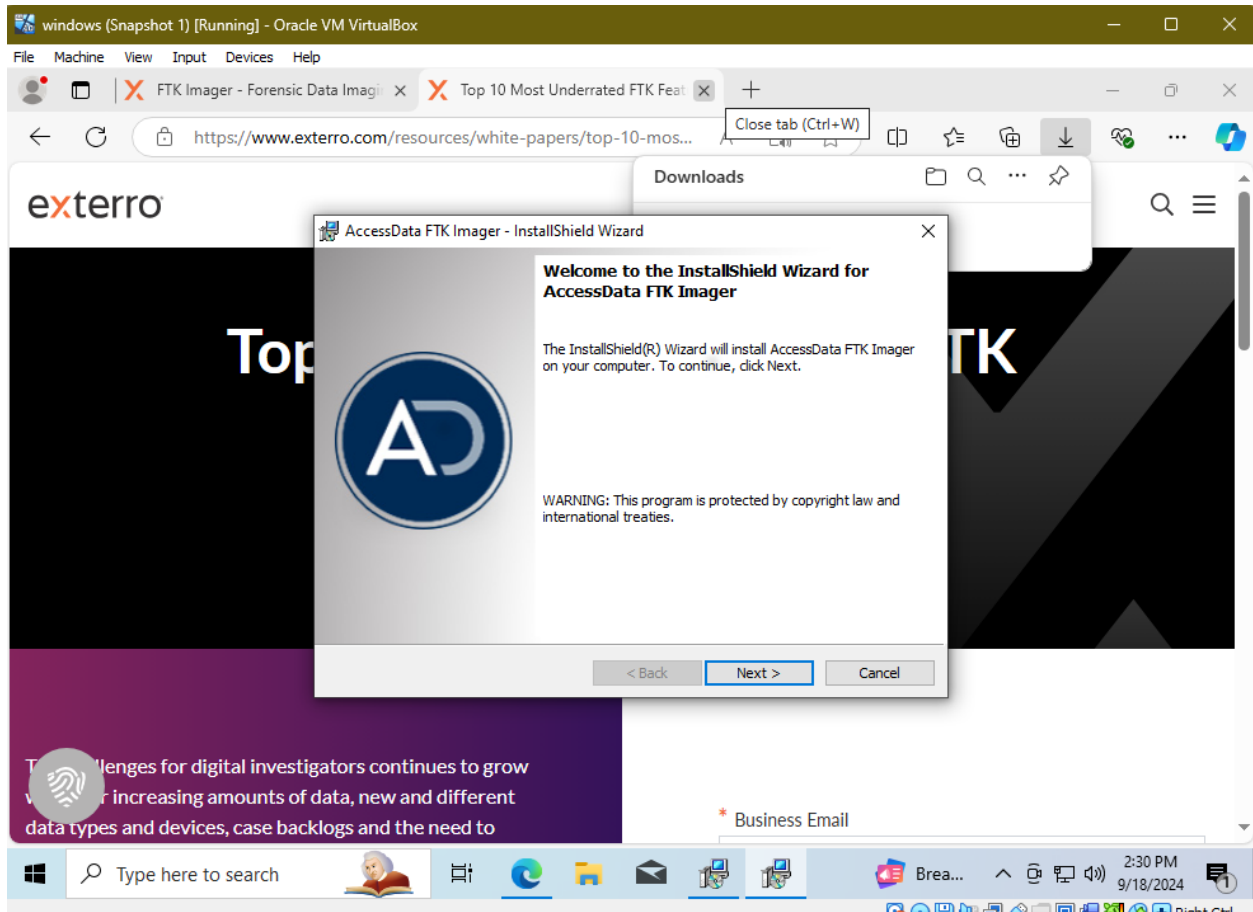
In this task, I utilized the Windows VM and which required me to install FTK Imager and created a forensic image from the VHD used in the last task.

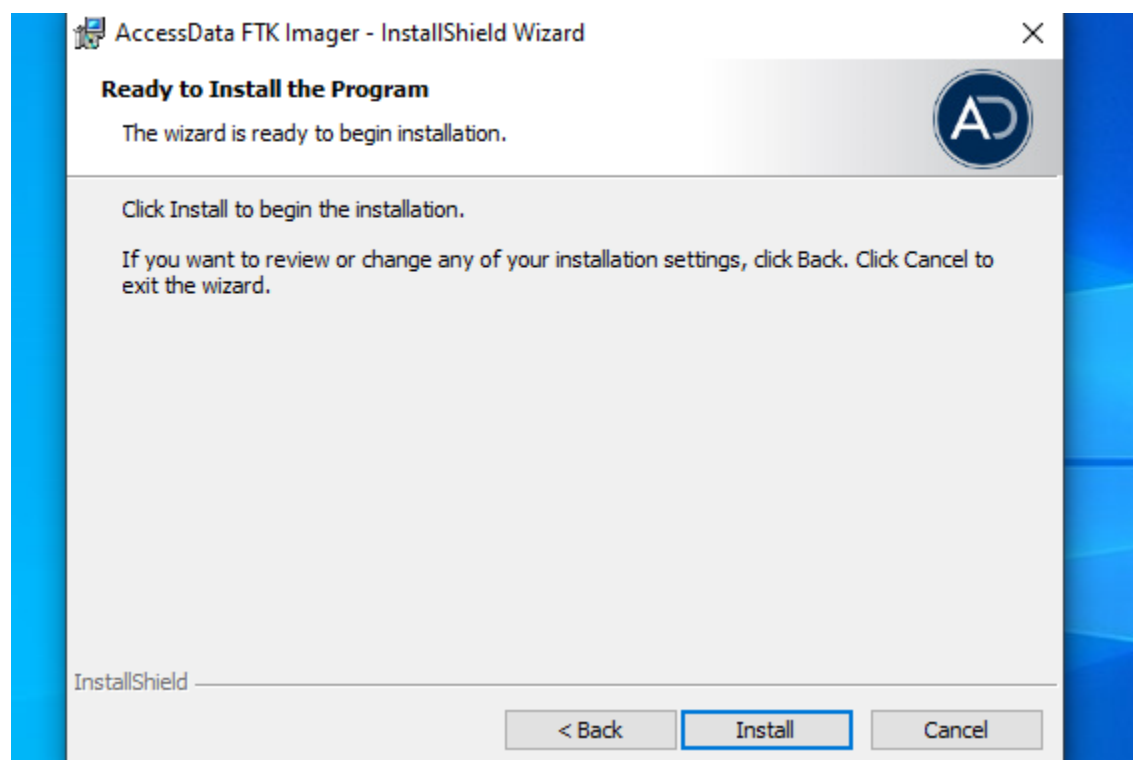
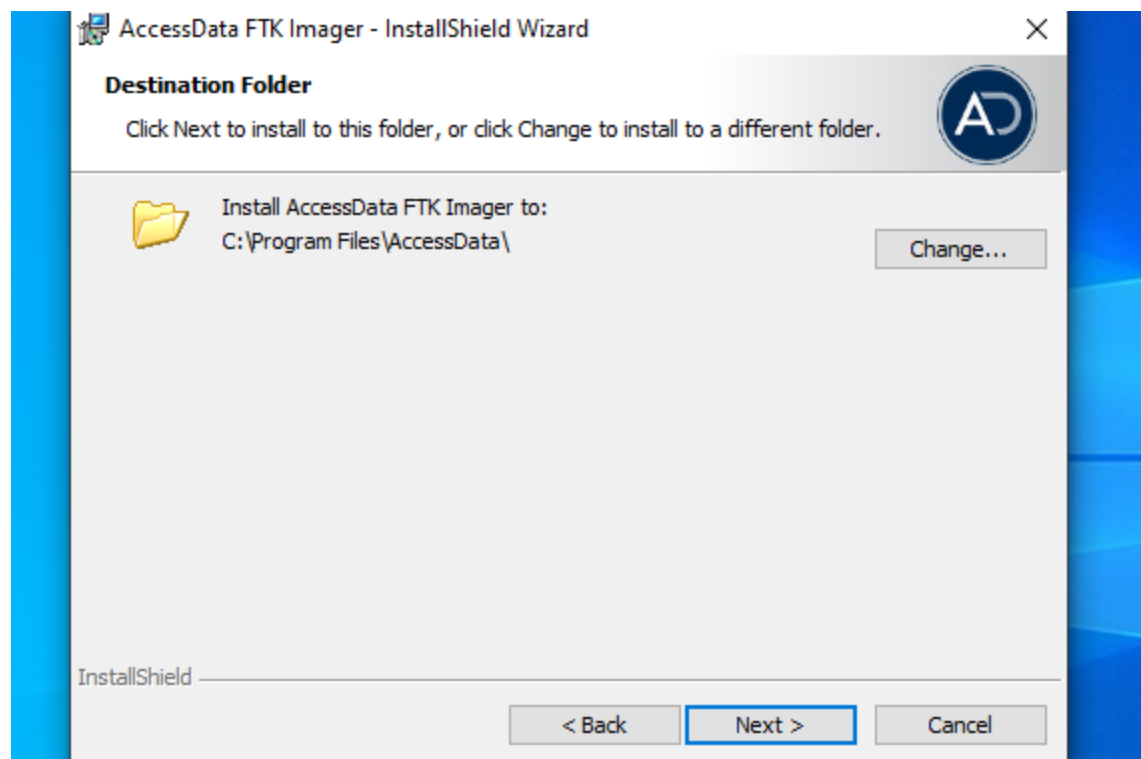
Step 1: I added the VHD drive created in the last task to the windows VM.

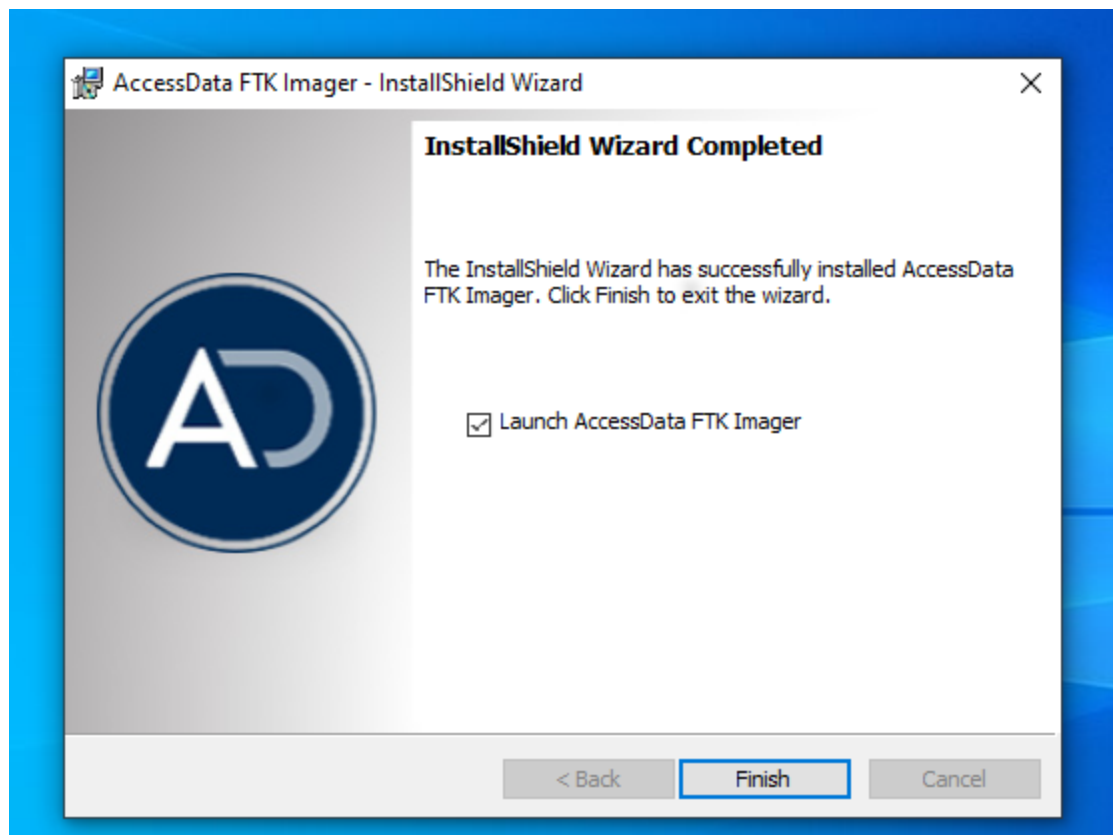


Then, I started the Windows VM and navigated to the exterro site and downloaded the installer. And clicked next and finish when prompted.

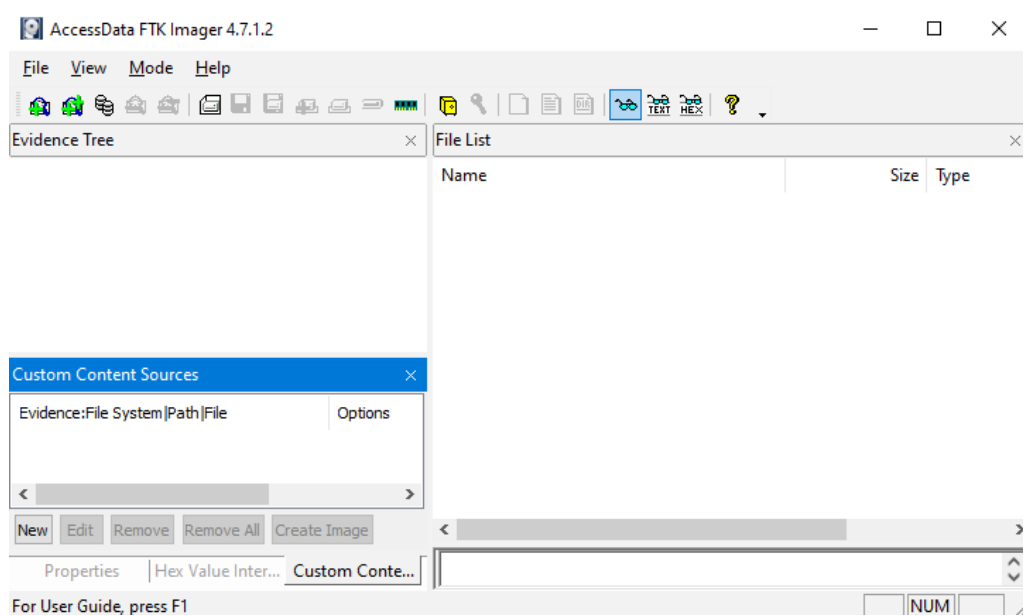




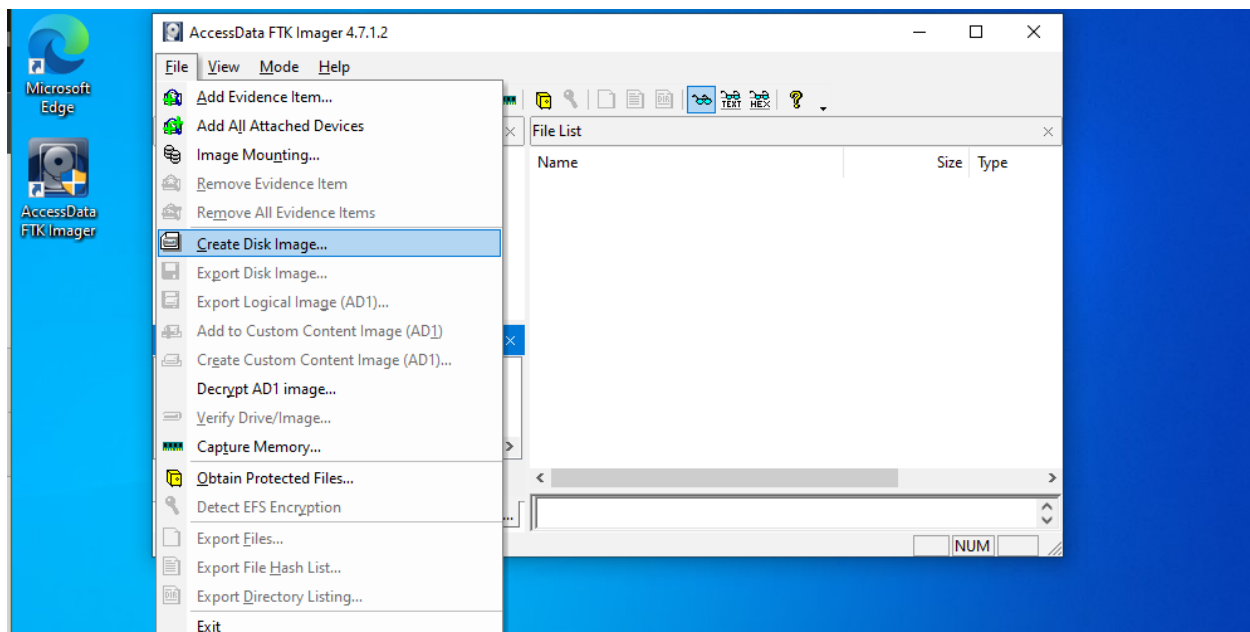




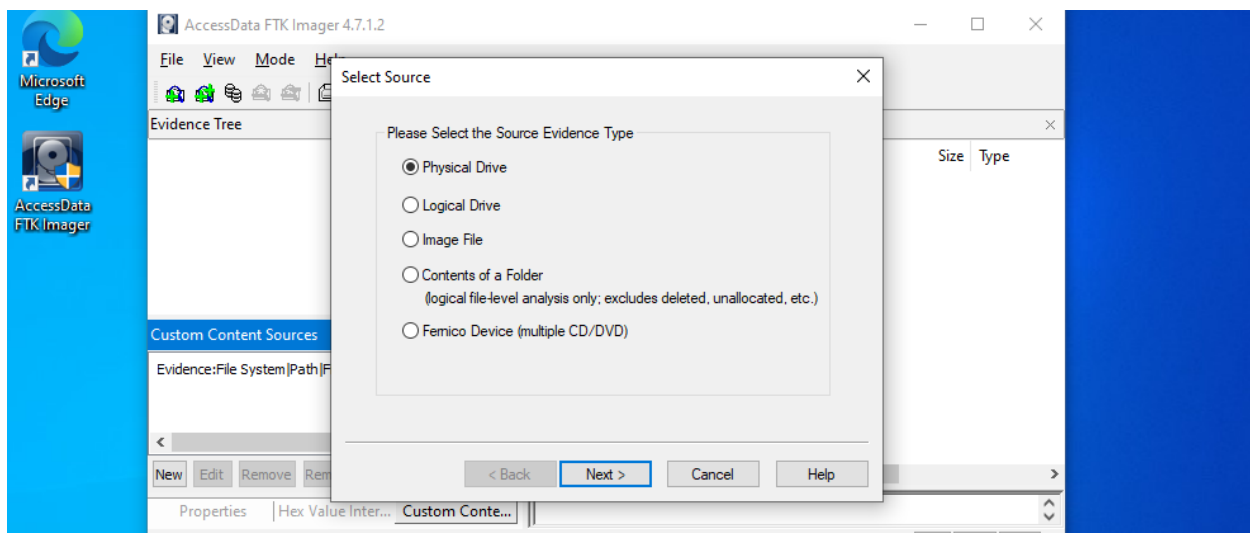
FTK was fully installed and a shortcut on the desktop was created.



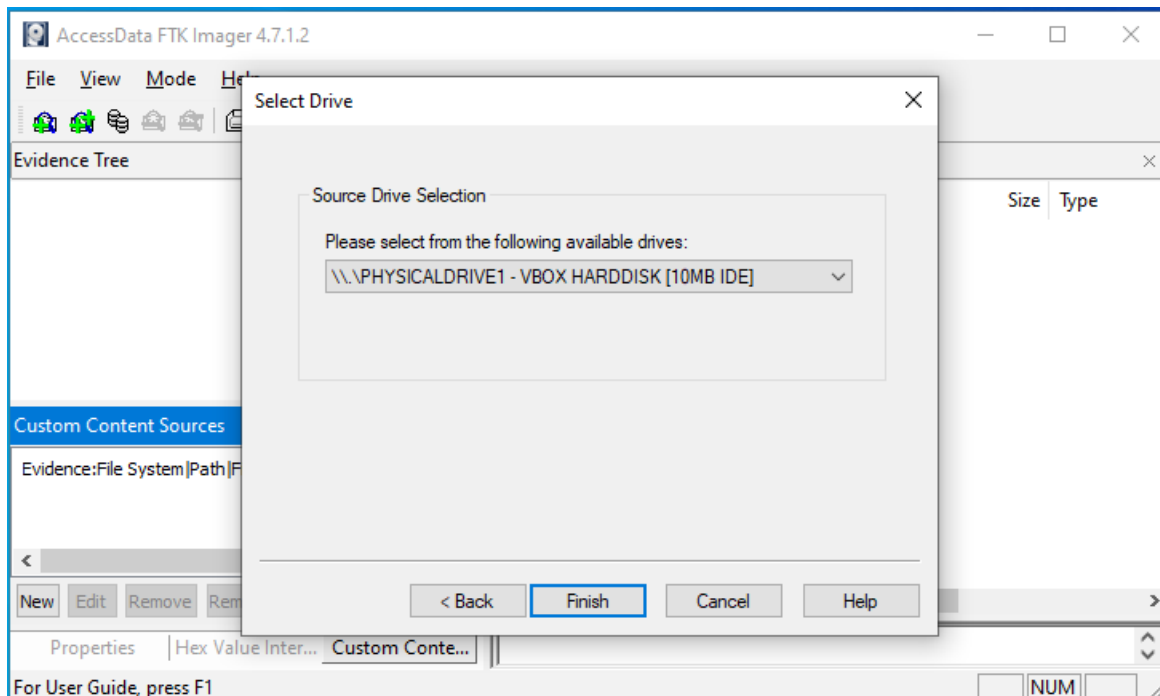
Step 2: I initiated creating a disk image by clicking “file” and “create Disk Image”.



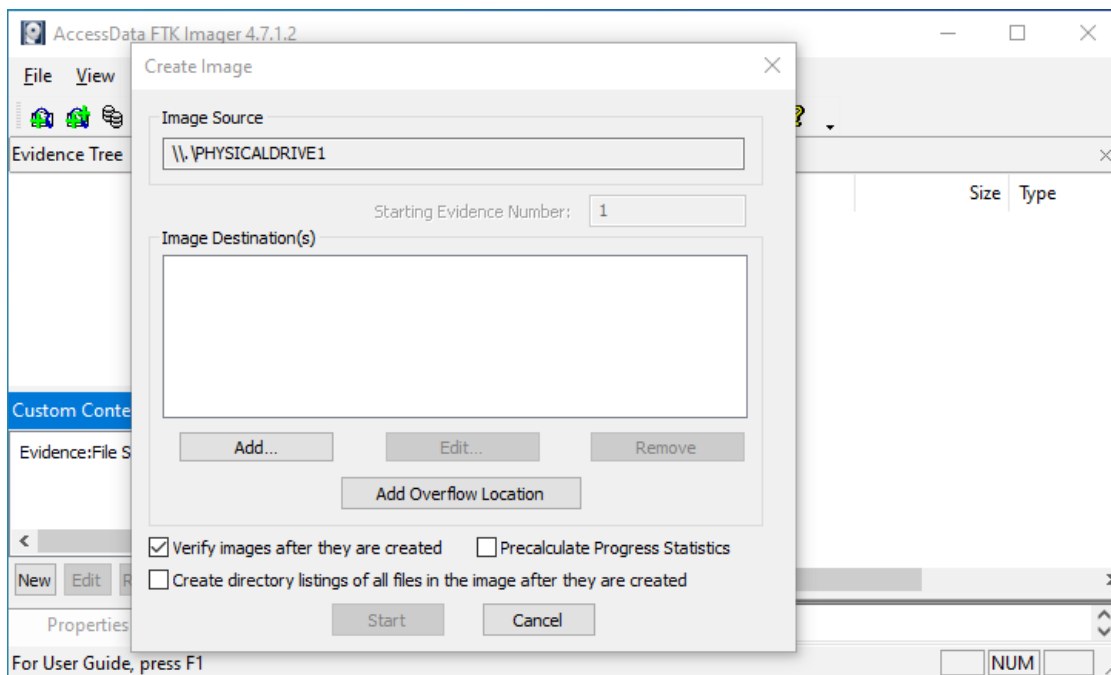
I selected “physical device” and pressed the next button.



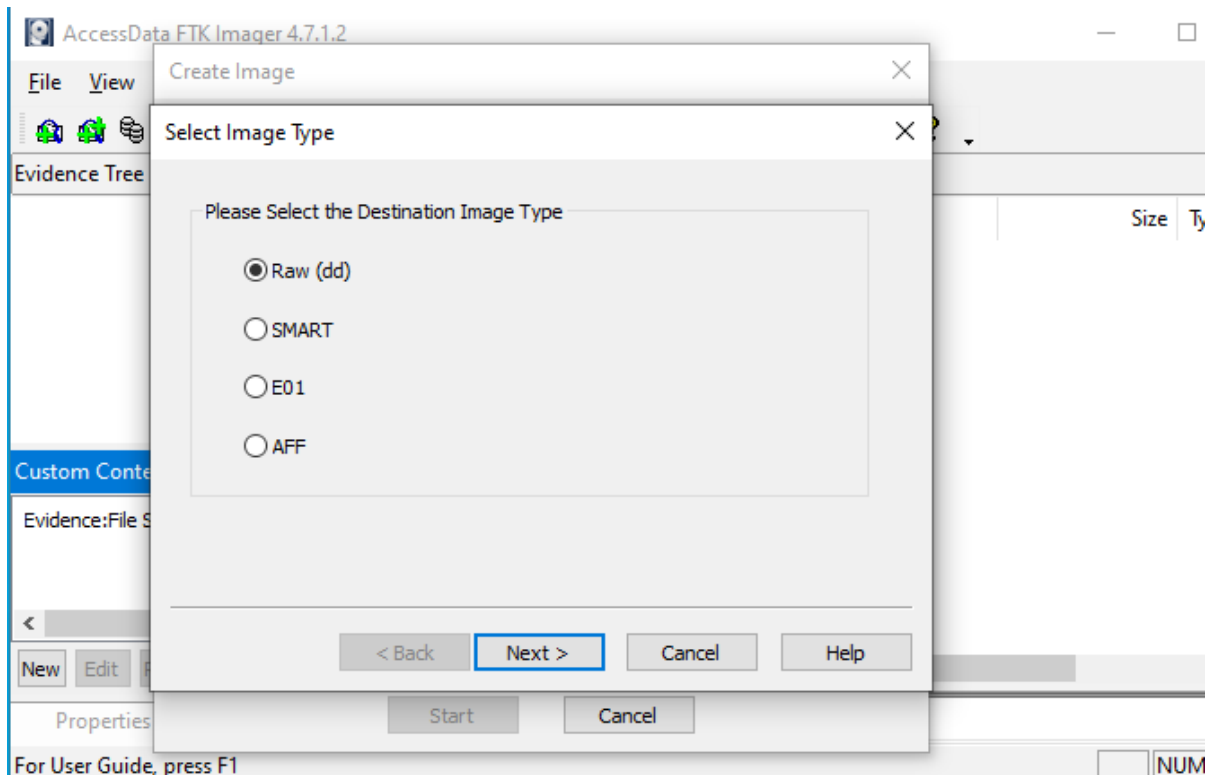
Here, I clicked the drop-down menu and selected the subject drive with 10MB and pressed finish.



Here I ensured that the “Verify images after they are created” checkbox was marked and pressed the “add” button.

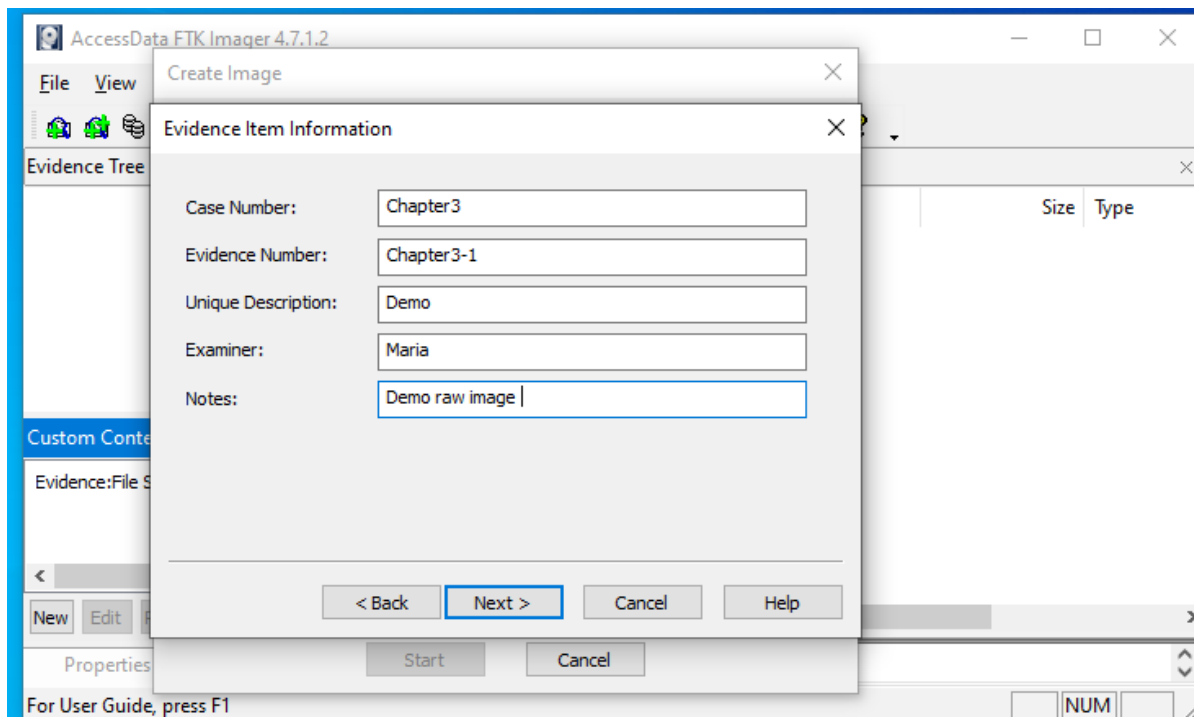


I selected the “Raw (dd)” format and pressed next.

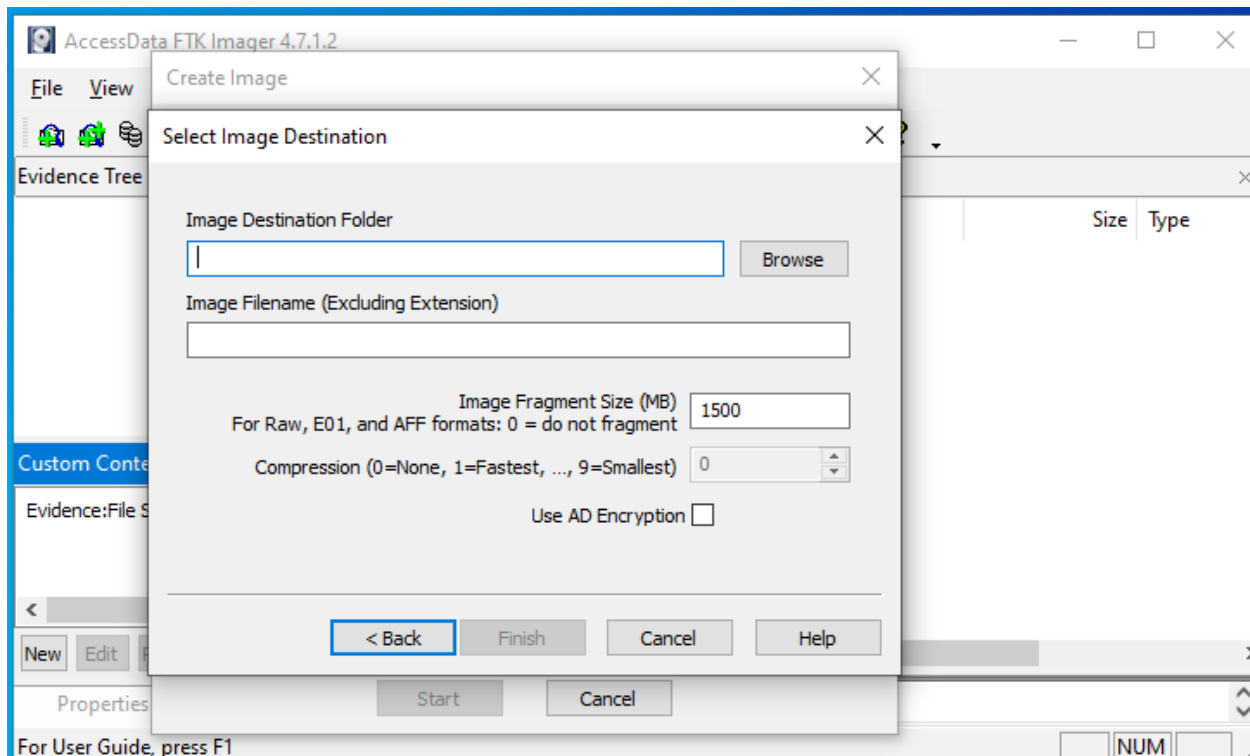


I entered the following information in the Evidence item information window and pressed next.

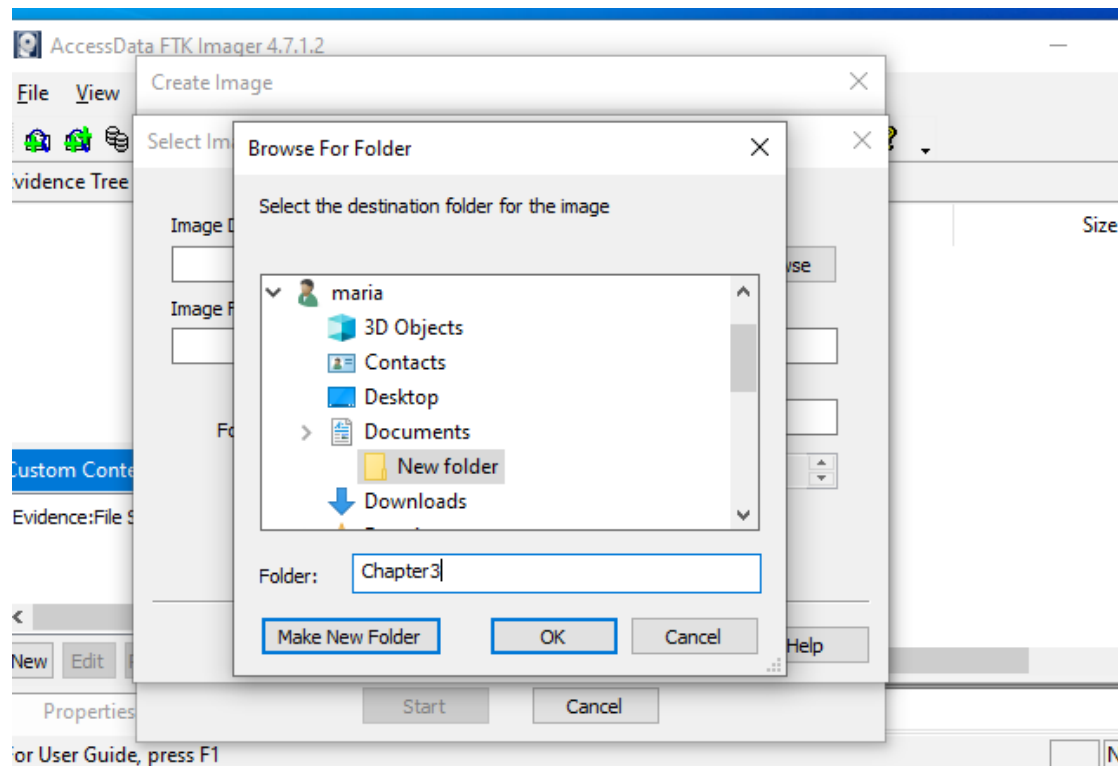
1. Case Number = Chapter 3
2. Evidence Number = Chapter3-1
3. Unique Description = Demo
4. Examiner = Maria
5. Notes = Demo raw image



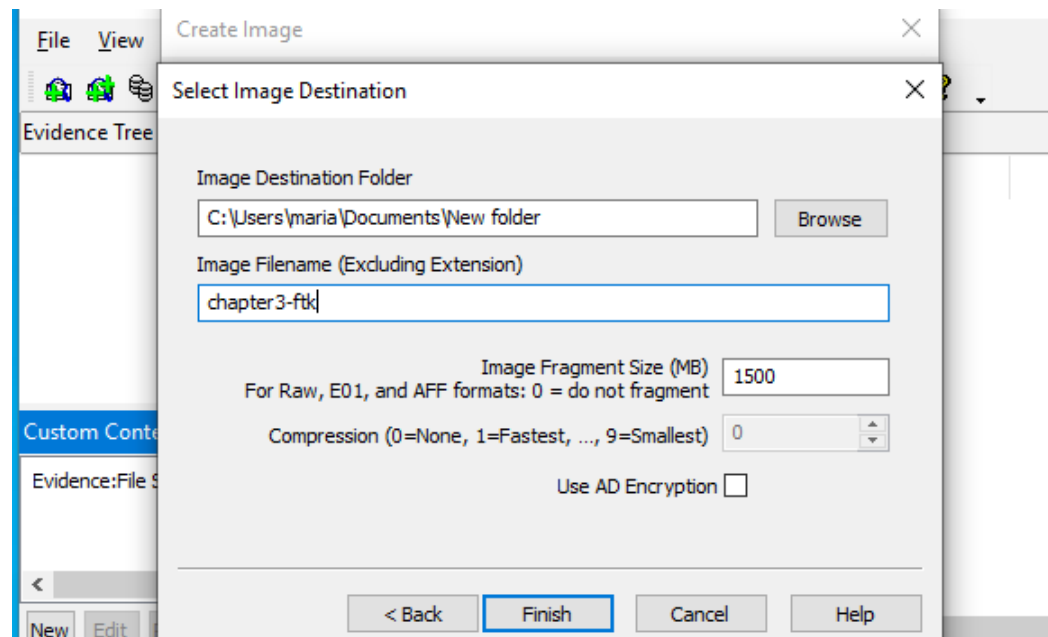
I clicked "Browse" to select an image destination folder



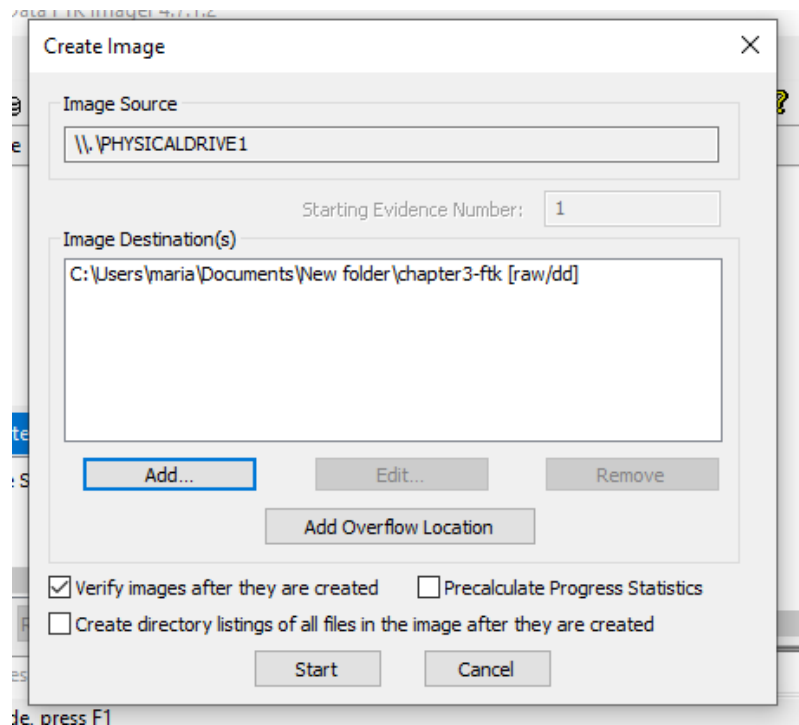
I created a new folder named “Chapter3” under my documents folder and pressed “ok”.



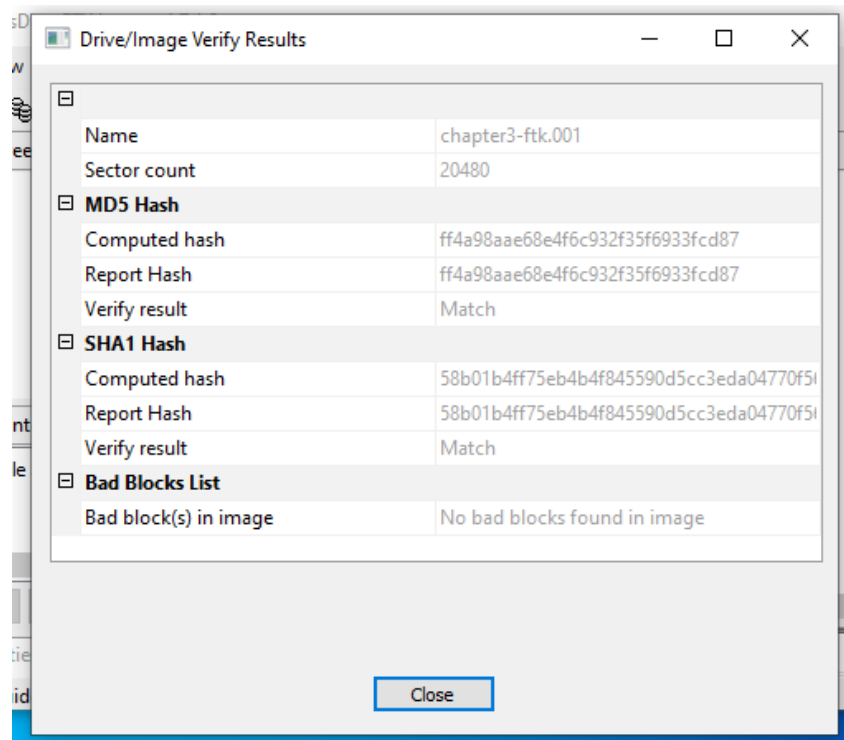
I typed in “chapter3-ftk” in the image file name and selected “finish”



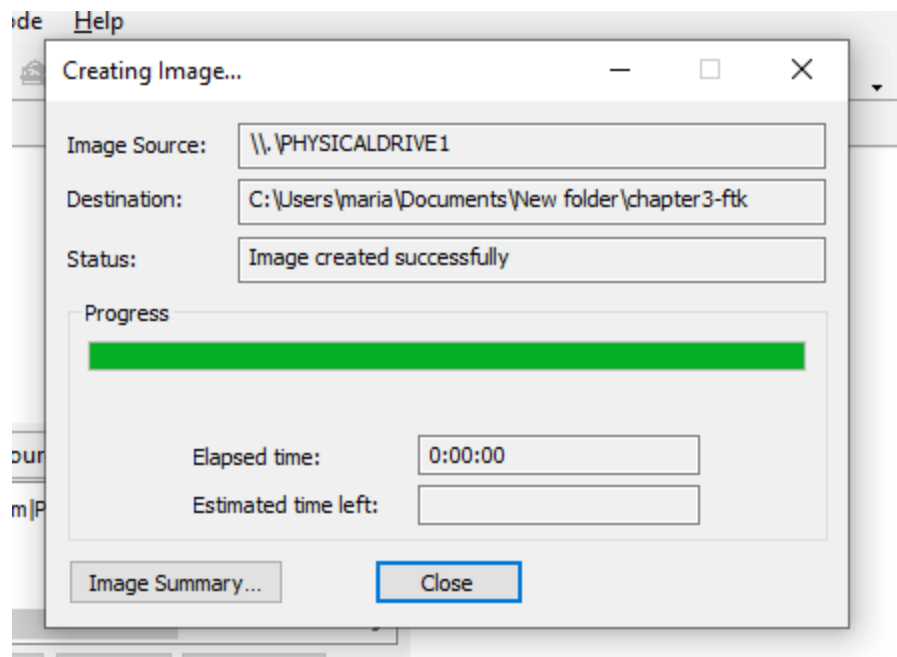
I clicked “start” to initiate the acquisition.



I observed the Drive/Image verify results for no errors and matching hashes then pressed “close”.



I observed that the image was created successfully and pressed “close”.



I navigated to my user's documents/Chapter3 directory and observed the image and log file were created.

