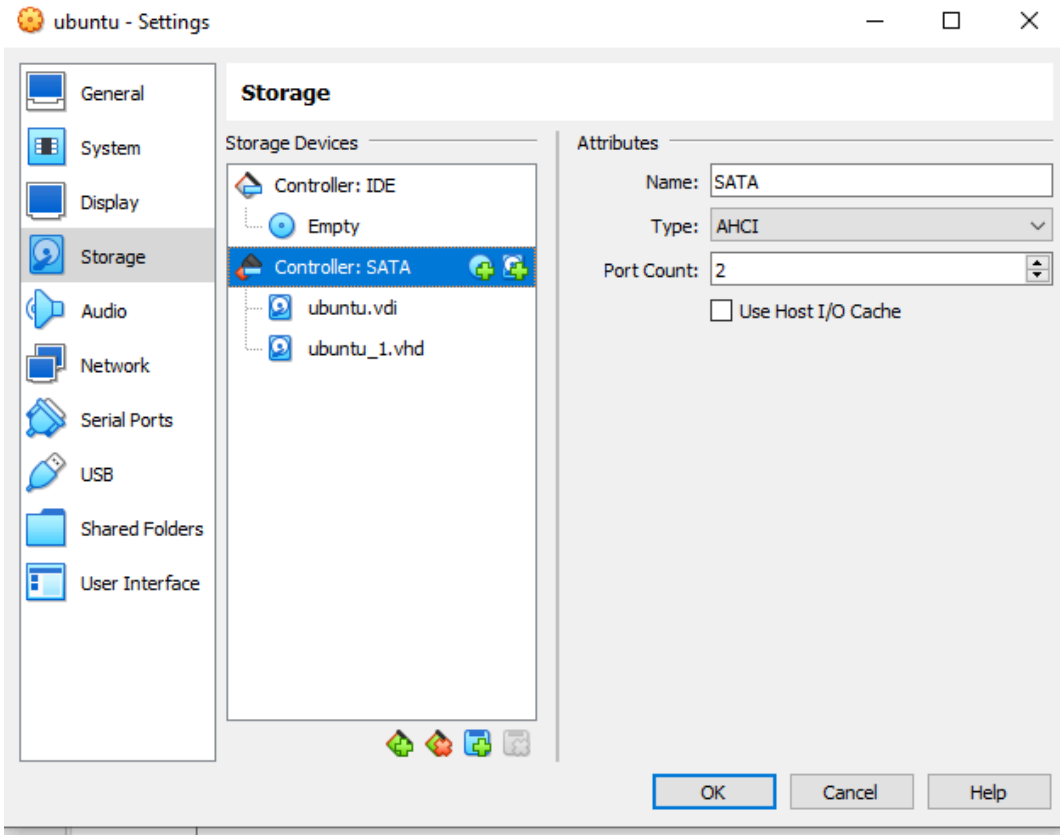
Task 1:



In this step, I have created a Virtual hard Drive for the Ubuntu machine.

```
timothyd@ubuntu:~/Desktop$ su
Password:
root@ubuntu:/home/timothyd/Desktop# fdisk -l
```

In this step, I am switching users and then listing all the disk devices.

```
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
```

Here is the 10 mb disk that I created in step 1.

```
root@ubuntu:/home/timothyd/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 0xea323f4a.
```

In this step, I am pointing the fdisk to the target drive.

```
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: 0xea323f4a
```

In this step, I am printing out the help menu with the “m” command and then I am using the “p” command to print the partition table.

```
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.
```

In this step, I am creating a primary partition using the “n” 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: 0xea323f4a

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

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): 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: 0xea323f4a

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

In this step, I am outputting the new Linux partition with the “p” command. Then I am running the “t” command to change the target drive partition with the hex code “0c”. I then am running the “p” command to show that the change has been implemented.

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

Here, I am saving the partition with the “w” command.

```
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: 0xea323f4a

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

This image shows the new partition on the target drive.

```
root@ubuntu:/home/timothyd/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 982372e2, no volume label.
```

In this step, I am formatting the partition as a FAT filesystem.

Task 2:

```
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: F1F147C5-7285-48C8-A575-CE2A6B0016D2

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: 0xea323f4a

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

In this step, I am listing the devices and showing that sda1, sda2 and sda3 is the host system while sdb1 is the external drive.

```
root@ubuntu:/home/timothyd/Desktop# mkdir /mnt/sdb1
root@ubuntu:/home/timothyd/Desktop# mount -t vfat/defv/sdb1/mnt/sdb1
root@ubuntu:/home/timothyd/Desktop# cd /mnt/sdb1
root@ubuntu:/mnt/sdb1# ls -la
total 8
drwxr-xr-x 2 root root 4096 Feb 16 11:50 .
drwxr-xr-x 3 root root 4096 Feb 16 11:50 ..
```

In this step, I am creating a mount point and mounting the external hard drive. Then I am changing directories to the mount point and listing the file contents.

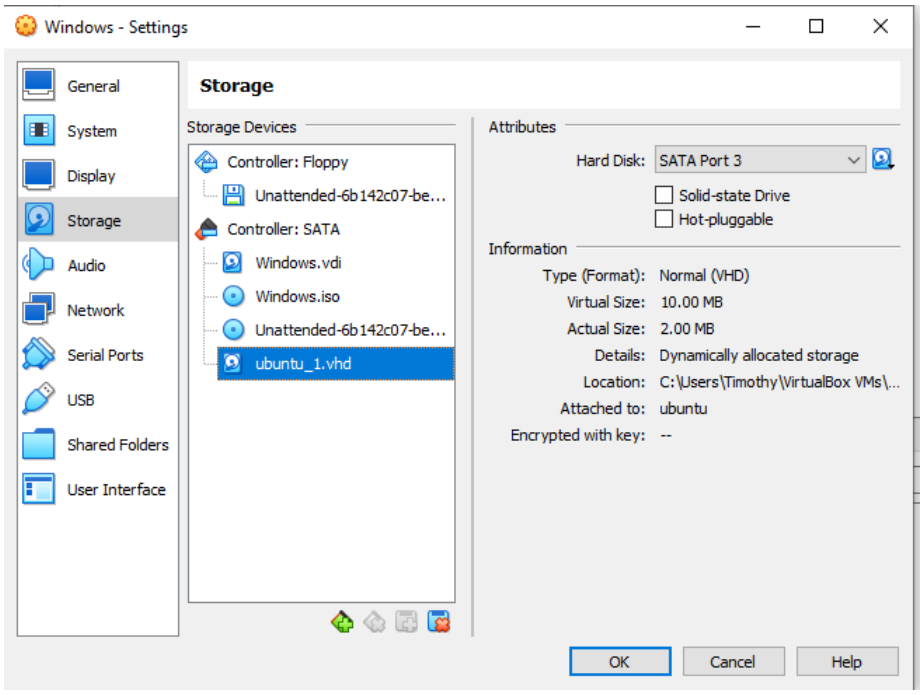
```
root@ubuntu:/mnt/sdb1# dd if=/dev/sda3 bs=512 count=16384 | split -b 4m - image_sda3
16384+0 records in
16384+0 records out
8388608 bytes (8.4 MB, 8.0 MiB) copied, 0.0487865 s, 172 MB/s
root@ubuntu:/mnt/sdb1# ls -lah
total 8.1M
drwxr-xr-x 2 root root 4.0K Feb 16 11:54 .
drwxr-xr-x 3 root root 4.0K Feb 16 11:50 ..
-rw-r--r-- 1 root root 4.0M Feb 16 11:54 image_sda3aa
-rw-r--r-- 1 root root 4.0M Feb 16 11:54 image_sda3ab
```

In this step, I am creating a forensic copy of sda3's partitions first 8 mb. Then I am verifying that 8 mbs were copied.

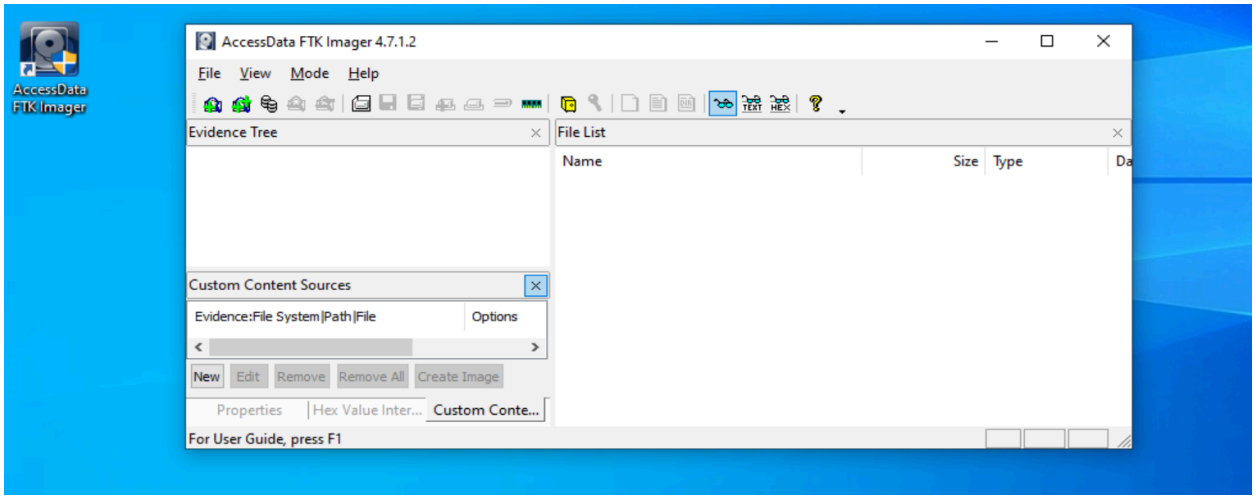
```
root@ubuntu:/mnt# umount /dev/sdb1
```

In this step, I am unmounting the disk.

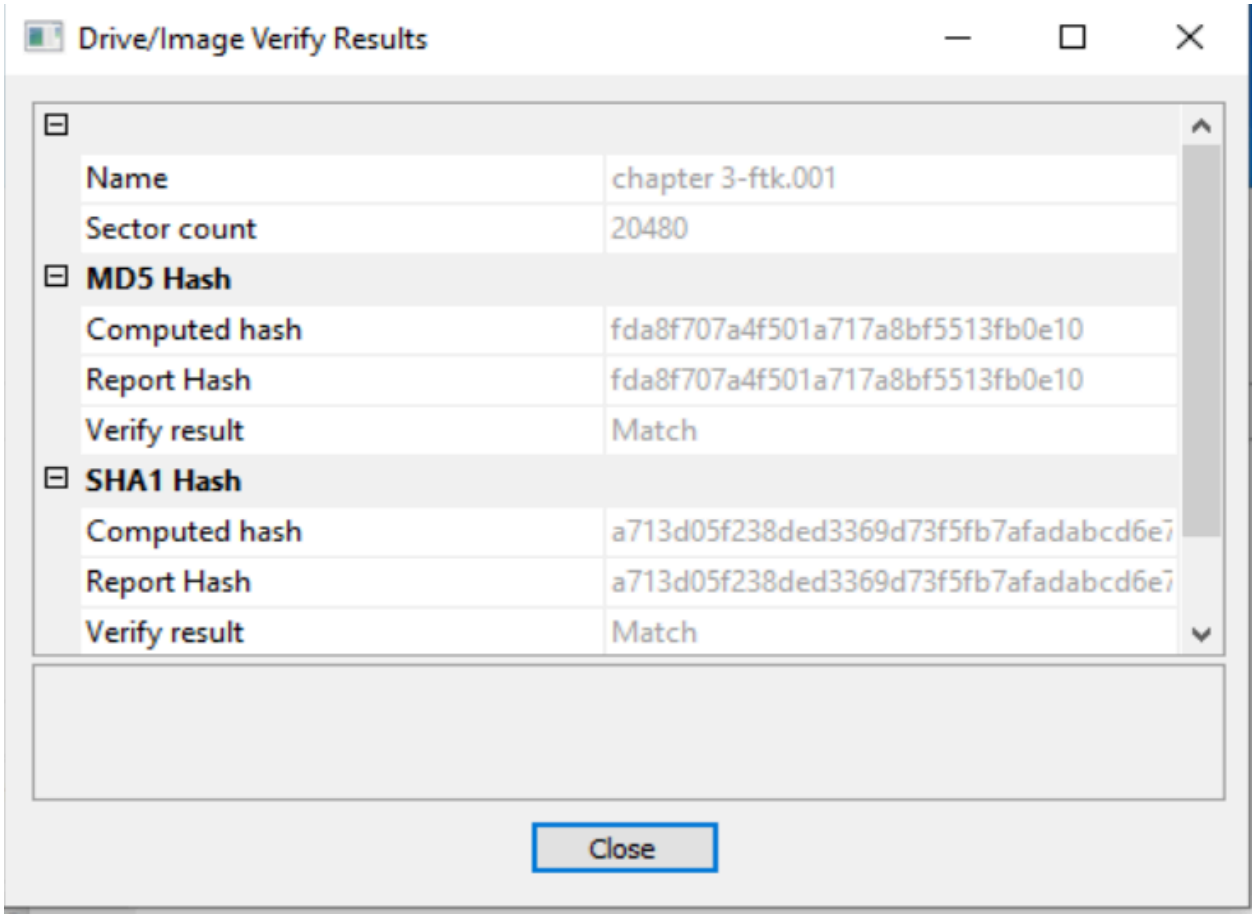
Task 3:



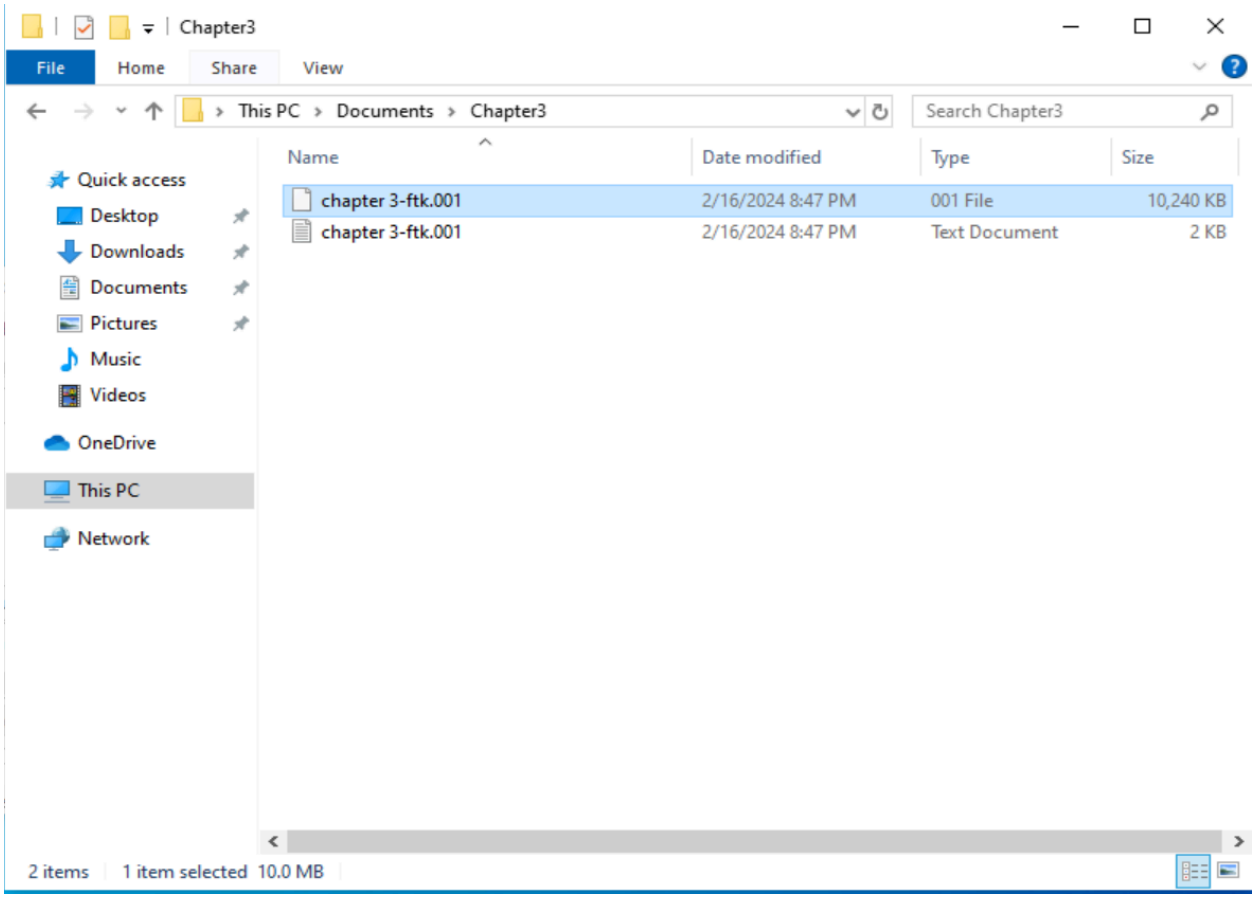
In this step, I am adding the VHD created in the last step to the WIndows VM.



In this step, I have downloaded the FTK.



In thi step, I have downloaded the images to their destination folder and ensured that their was no errors in creating the image.



This image shows that the image and log file are created and have been stored in the right location.