

# Digital Forensics (IFS4102) Lab 2:

## Static Acquisition

### Lab Objectives

In this lab, you will perform **static/non-volatile forensically-sound data acquisitions** using both your Windows and Linux forensic workstations.<sup>1</sup> Additionally, you will also **access and inspect** the acquired image files.

More specifically, we want to achieve the following **objectives**:

1. To perform a **static data acquisition** of an external (USB thumb) drive using your **Windows** forensic workstation with the following steps:
  - a. (Optional) Simulate a hardware write blocker using a Windows-based software write blocker;
  - b. Create a forensic disk image of the target drive;
  - c. Compare the hashes of the original drive and the disk image file.
2. To **access and inspect** the created disk image file using a forensic tool, and also export some files of interest.
3. (Optional) To **mount** the created disk image file as an accessible drive, and analyse the contained files using **external tools**, e.g. an anti-virus scanner.
4. To perform a static data acquisition of an external drive using your **Linux** forensic workstation using:
  - a. `dd`;
  - b. (Optional) `dcfldd`.

---

<sup>1</sup> In our lab notes, tasks that need to be done with your *Windows* forensic workstation are indicated as **Win-FWS**, whereas tasks for your *Linux* forensic workstation (e.g. Kali Linux or SIFT) are indicated as **Lin-FWS**.

## **[Optional] Task 1-A (Win-FWS):**

### **Setting Up Software Write Blocker in Windows**

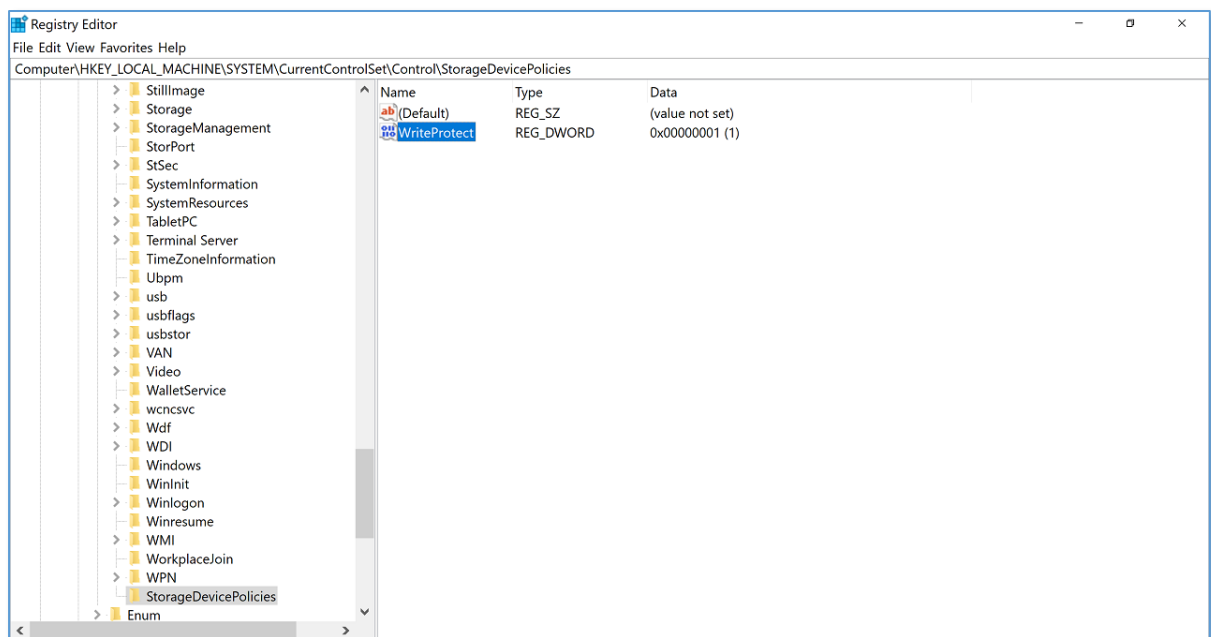
#### **Important Notes:**

- You will use your **Windows** forensic workstation for Tasks 1-A to 1-C.
- For this Task 1-A, you will need Windows XP SP2 or newer, so that you can add a registry entry that will block write access to devices connected to USB ports.
- Before your acquisition, first prepare a USB thumb drive as your static acquisition target by creating some folders and copying some files into the folders. Don't forget to eject the thumb drive afterwards.
- Configure a software write blocker using RegEdit with the steps below.  
**Be *very careful* when editing your registry entries!** A Windows VM is thus recommended. Note that a registry entry is *case sensitive*.
- To disable your software write blocker later on, do change the data of a registry key's value that is set in Step 9 below to 0.

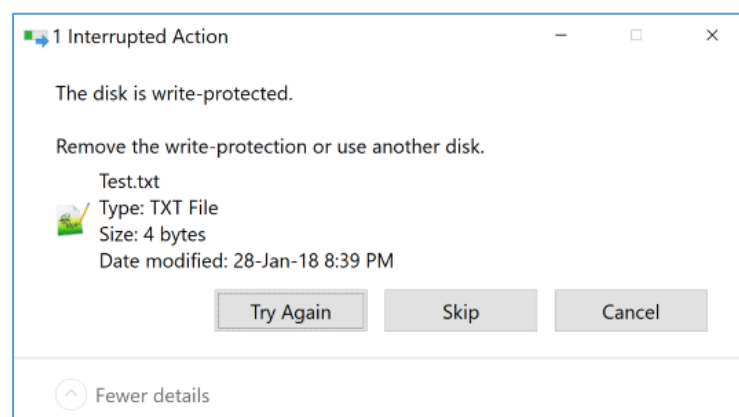
#### **Steps:**

1. Open a command prompt on your Windows machine.
2. Launch the Registry Editor (RegEdit) by invoking: `regedit`.
3. Navigate to the following registry key:  
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\.`
4. Right-click on "Control", select "New", then select "Key".
5. Type the name `StorageDevicePolicies` and press Enter.
6. Right-click on the right window pane.

7. Select “New” and then “DWORD (32-bit) Value”.
8. Change the (value) name to WriteProtect.
9. Double-click on its data, and change it from 0 to 1.
10. Click the “OK” button.
11. You should have a new registry entry with its created value entry as below:



12. Close the Registry Editor window.
13. Now insert your target thumb drive into a USB port of your machine.
14. Try copying a file into the device. You should receive a prompt like this:



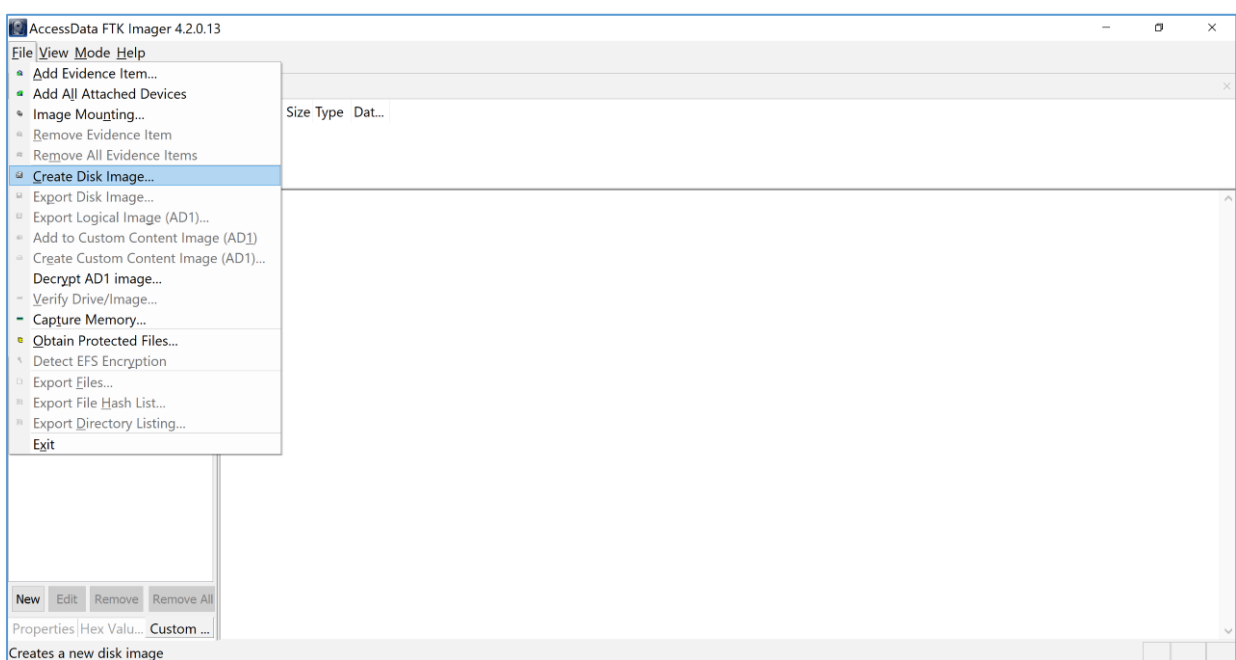
## Task 1-B&C (Win-FWS): Creating an Image of Your Drive

### Important Notes:

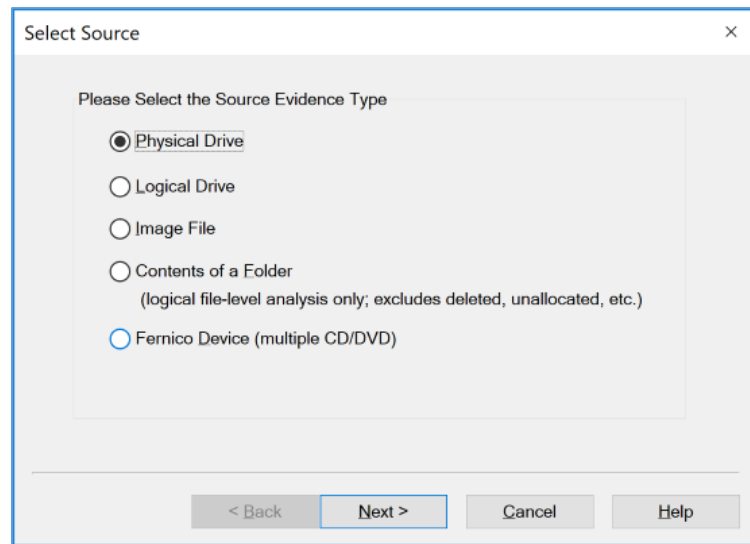
- Using your Windows forensic workstation, you are going to create a forensic **disk image** of your target thumb drive by employing **FTK Imager** from AccessData (recently acquired by Exterro).
- Please ensure that your workstation's hard drive *has enough storage space* to store the created disk image file.

### Steps:

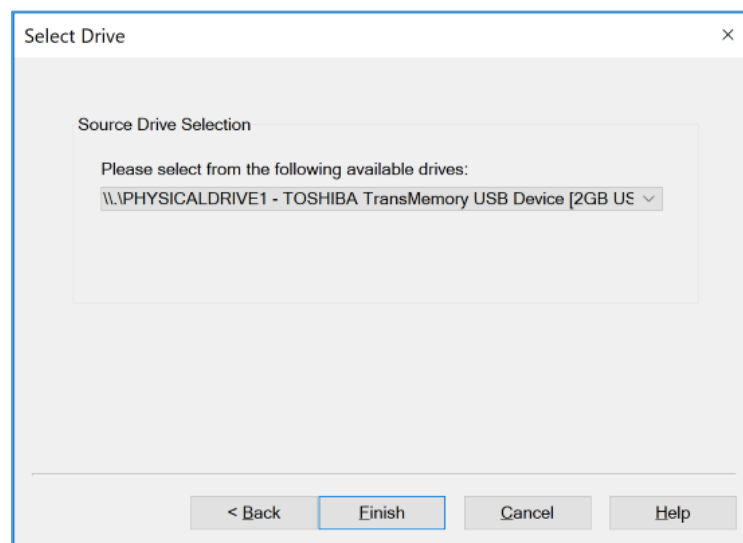
1. Download **FTK Imager 4.7** from <https://www.exterro.com/ftk-imager> and install it. (Note that the UI of this latest version of FTK Imager may be slightly different from the screenshots given below.)
2. Connect your target thumb drive to your machine's USB port (if still needed).
3. Launch FTK Imager.
4. From the main menu, select "File" and choose "Create Disk Image...":



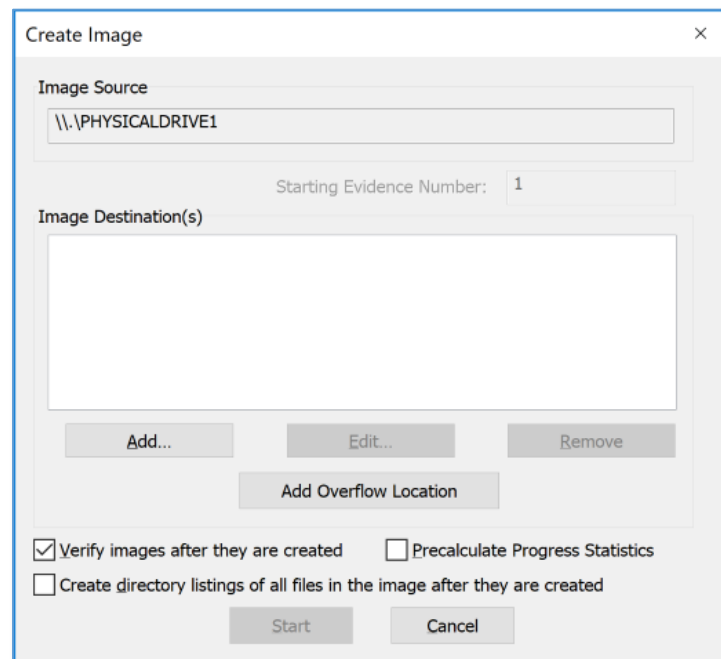
5. In the “Select Source” window below, select “Physical Drive”, then click the “Next” button:



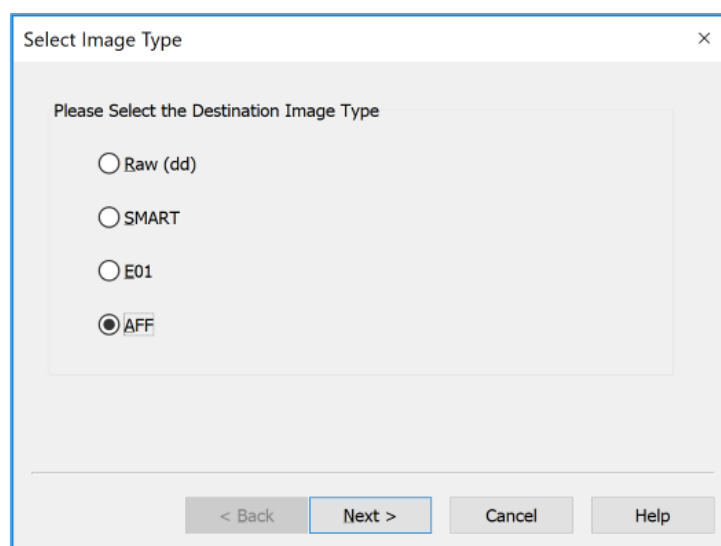
6. Identify your drive location, and click the “Finish” button:



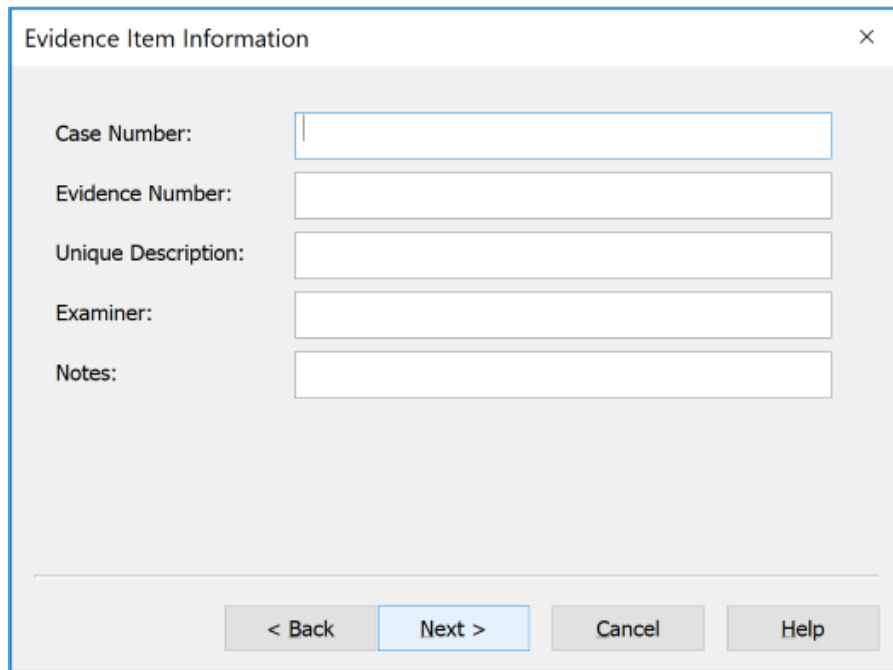
7. Identify your image destination location by clicking the “Add...” button:



8. Select your preferred image type, such as the Advanced Forensics Format (AFF) or the Encase's Expert Witness Format (EWF) with its .E01 extension, and then click the “Next” button:



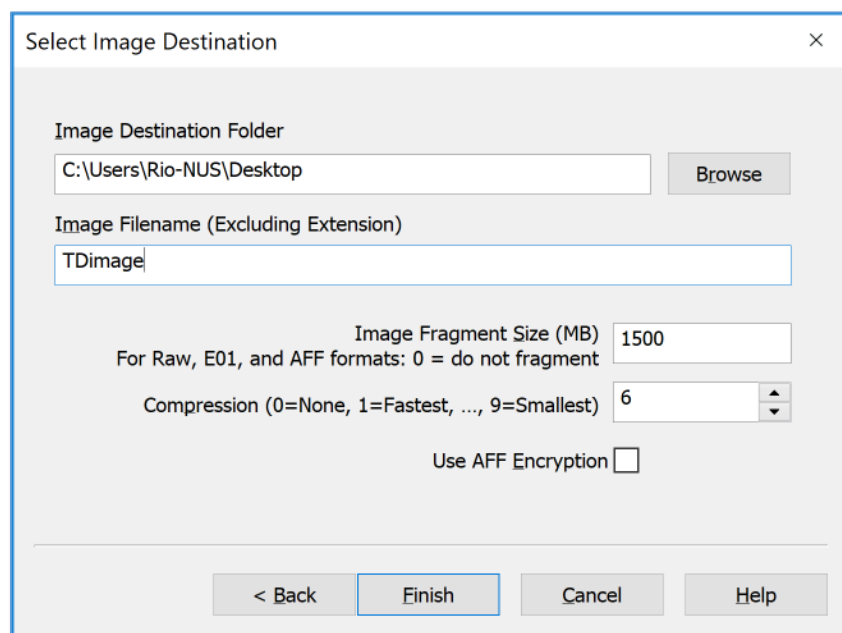
9. Enter the description of your evidence item, and then click the “Next” button:



The "Evidence Item Information" dialog box contains the following fields and controls:

- Case Number:
- Evidence Number:
- Unique Description:
- Examiner:
- Notes:
- Navigation buttons at the bottom: < Back, Next > (highlighted), Cancel, and Help.

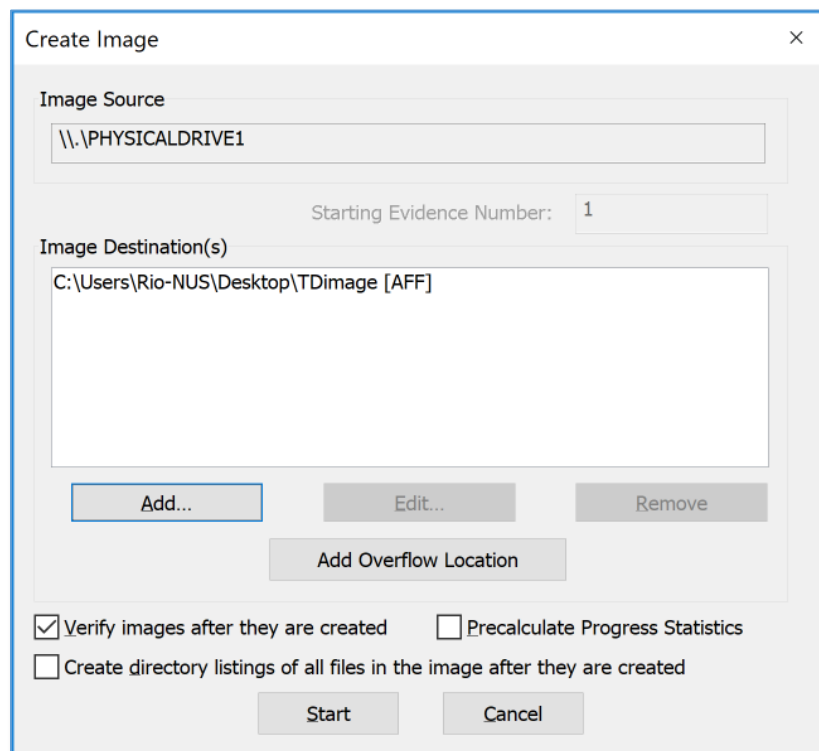
10. Identify the folder and filename of your image destination. By default, FTK Imager will split the image across multiple files once the file size reaches 1,500MB. You can modify the image fragment size if desired. The size of 0 means “do not fragment”. Once ready, click the “Finish” button.



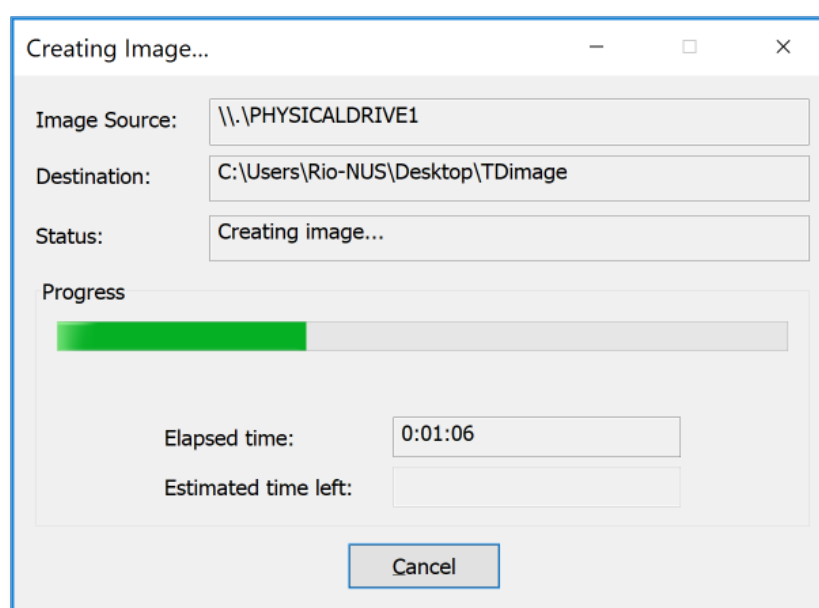
The "Select Image Destination" dialog box contains the following fields and controls:

- Image Destination Folder:  Browse
- Image Filename (Excluding Extension):
- Image Fragment Size (MB):   
For Raw, E01, and AFF formats: 0 = do not fragment
- Compression (0=None, 1=Fastest, ..., 9=Smallest):
- Use AFF Encryption: ☐
- Navigation buttons at the bottom: < Back, Finish (highlighted), Cancel, and Help.

11. Specify the overflow location if necessary. Ensure that the “Verify images after they are created” option is checked. Once ready, click the “Start” button to start the disk imaging.

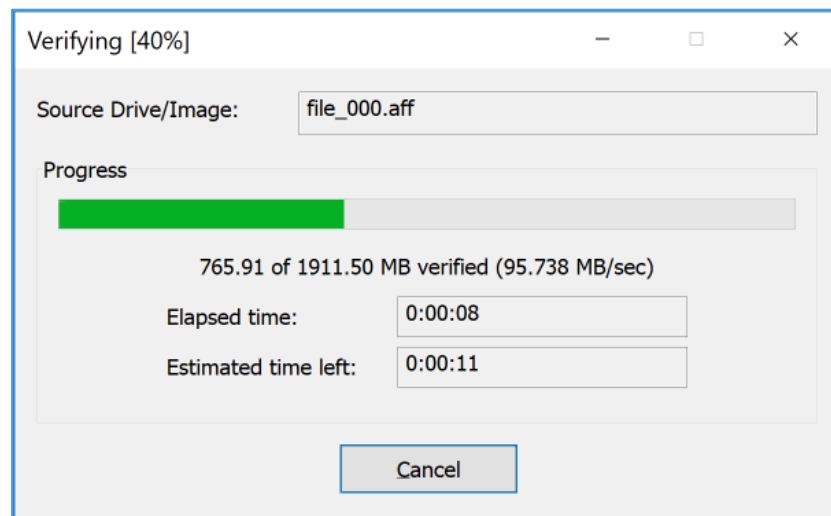


12. FTK Imager will show a progress bar while it is imaging the target drive:

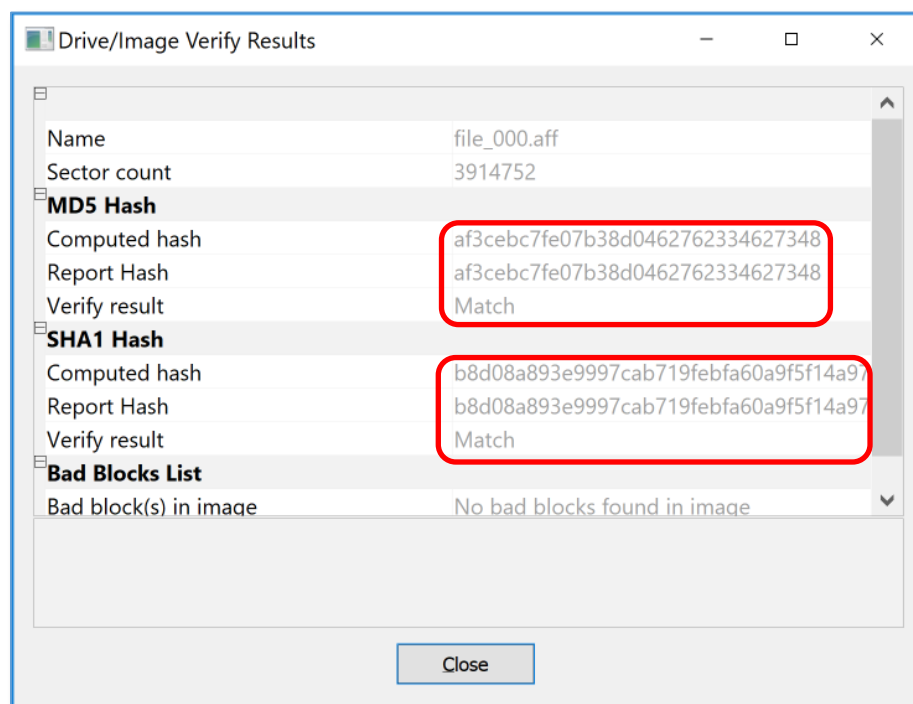




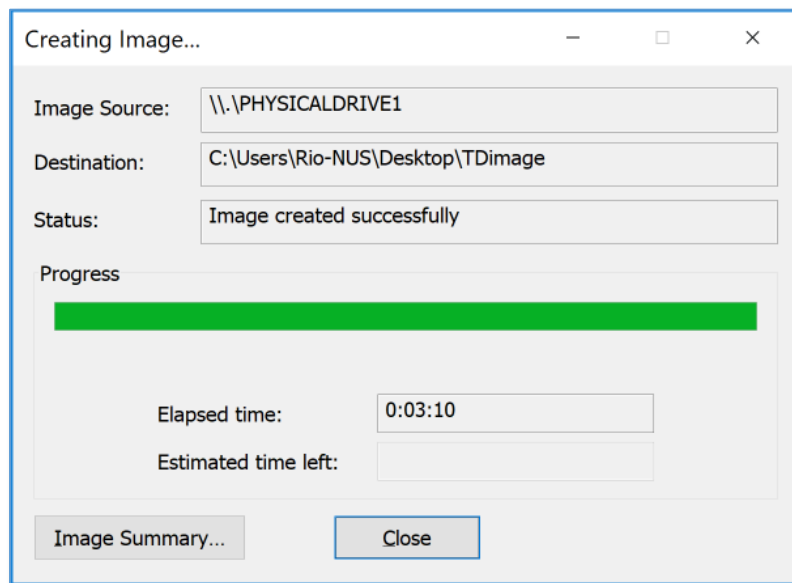
13. After FTK Imager completes the imaging, it will then verify the image:



14. FTK Imager will show the verification results. Ensure that the MD5 and SHA1 hash value comparisons do match:



15. Once the imaging is completed, the elapsed time is also shown:



16. A text file detailing the created forensic disk image is put within the same directory as the forensic image file. Open and check the file, then try answering the following questions regarding your created image file:

- a. What is your target drive's serial number (if indicated)?
- b. What is the size of the drive?
- c. How many sectors are there?
- d. What are the MD5 and SHA1 hash values of the drive?
- e. Was an exact forensic image replica created by FTK Imager?  
How do you know that?

---

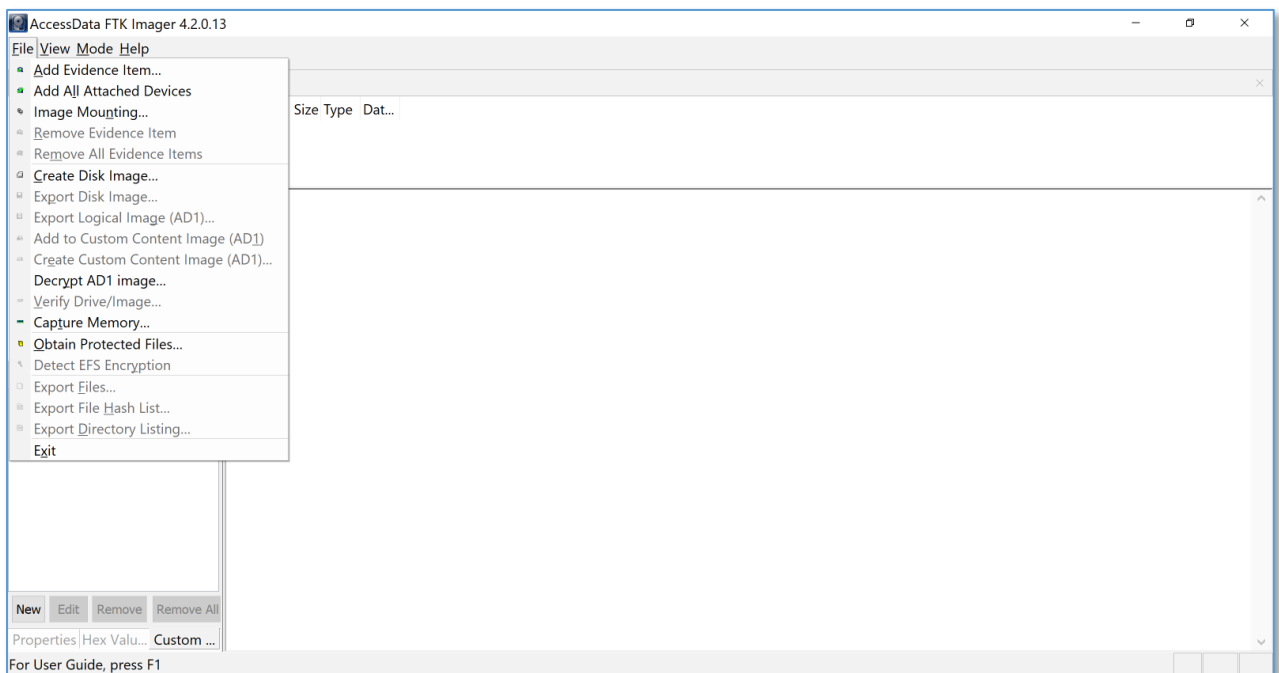
## Task 2 (Win-FWS): Accessing the Created Disk Image File and Exporting Some Files

### Important Notes:

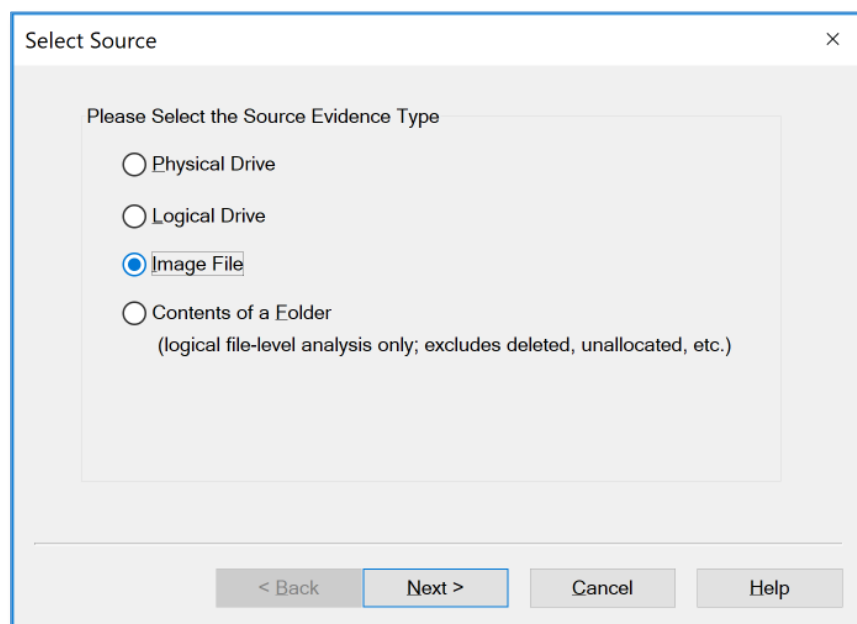
- Now you are going to **access** your created **disk image file** using FTK Imager, and **export** some files into your Windows forensic workstation.
- Alternatively, you can use a **given sample disk image** “SuspectDrive1.E01” downloadable from [https://drive.google.com/file/d/1SiJOaWEmKYyXXKI-PEJP3-I2j1iOC\\_p3/view?usp=sharing](https://drive.google.com/file/d/1SiJOaWEmKYyXXKI-PEJP3-I2j1iOC_p3/view?usp=sharing). Its MD5 value (see below for generating the value in Windows) is b66270513117670d11ebe2191e947a6d.
- In Windows, you can calculate the MD5 hash value of a file using the built-in `certutil` command: `certutil -hashfile <file> md5`  
Alternatively, you can use other available GUI-based hashing tools in Windows, such as:
  - HashCalc (<https://www.slavasoft.com/hashcalc/>), which can produce the hash value of a file, text string, or hex string;
  - HashMyFiles ([https://www.nirsoft.net/utils/hash\\_my\\_files.html](https://www.nirsoft.net/utils/hash_my_files.html)), which can hash **multiple files or a folder** in your system.

### Steps:

1. Launch FTK Imager.
2. From its main menu, select “File”, and then select “Add evidence item...” as shown below:

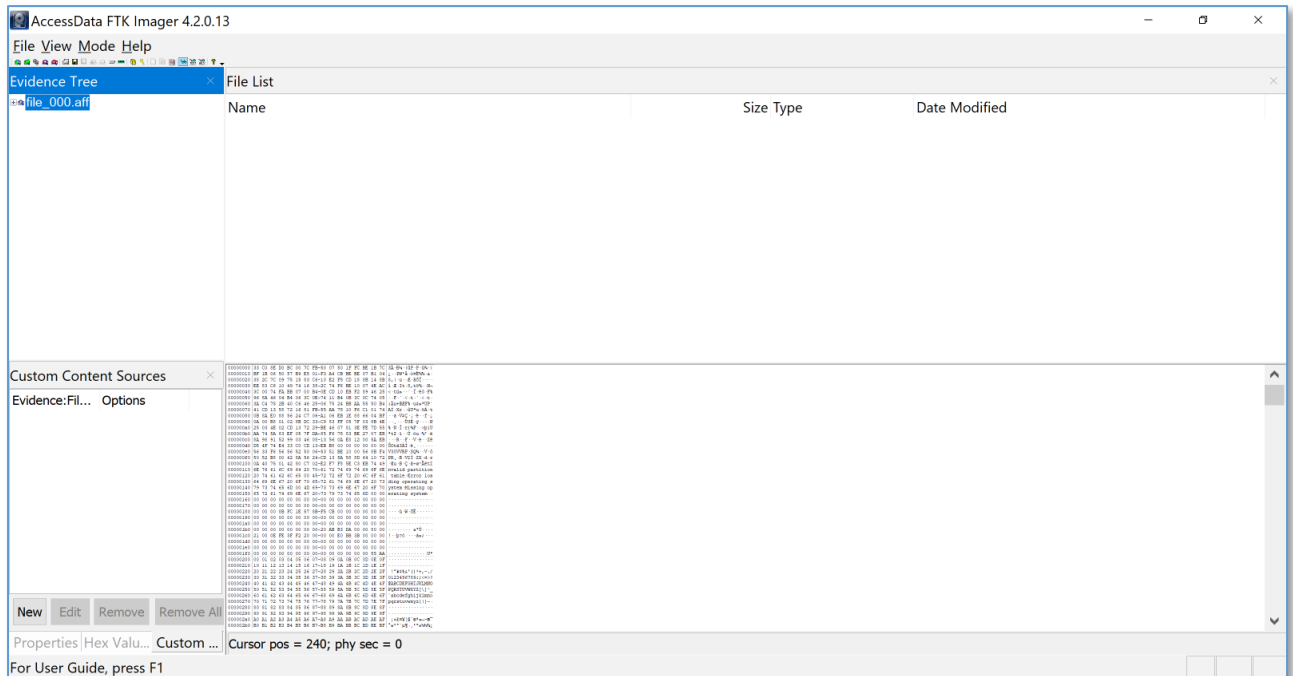


3. Select “Image File” as your source evidence type, then click the “Next” button:

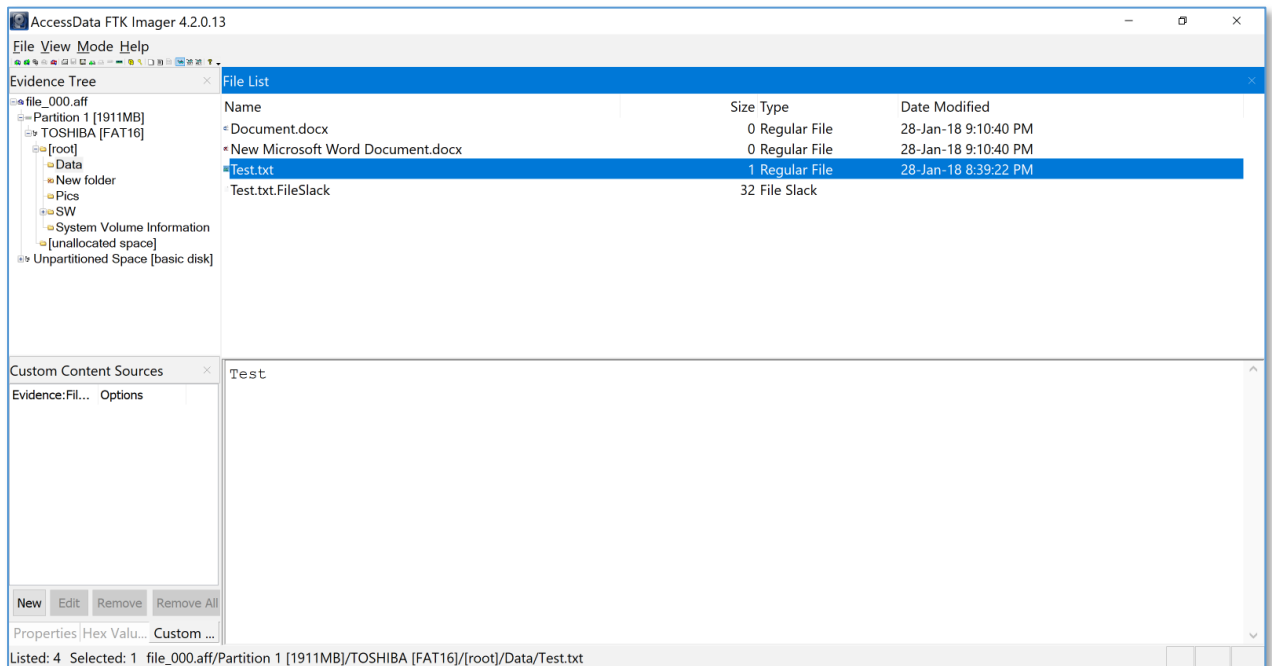


4. Browse to your image file location, and click the “Finish” button.

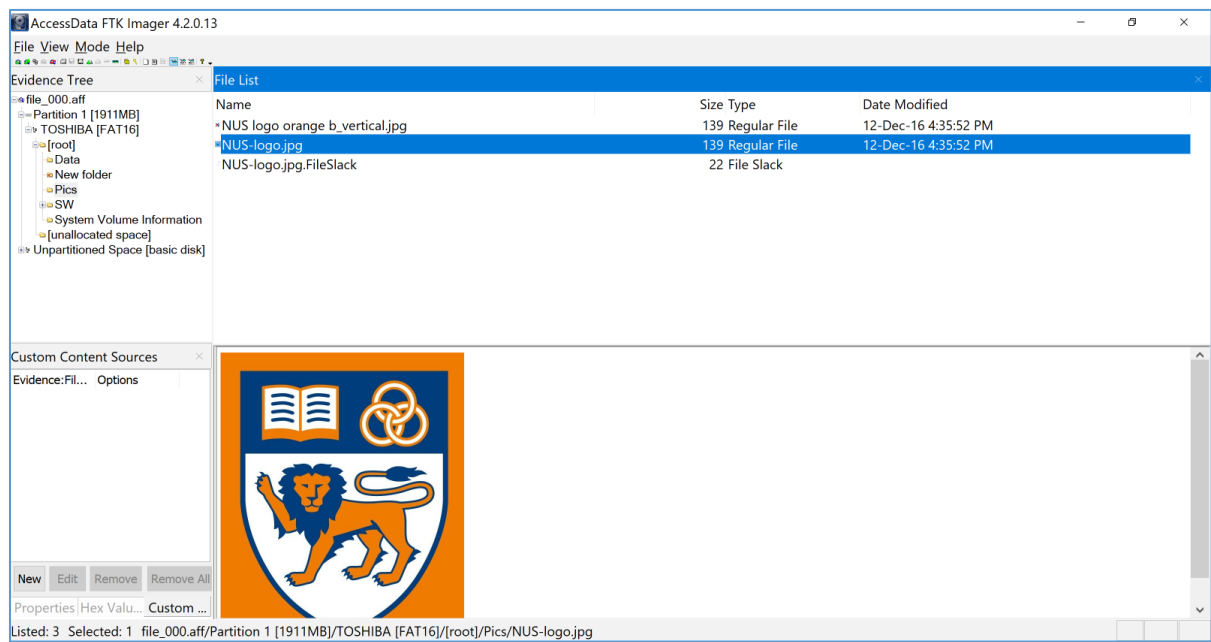
5. FTK Imager will open the image file, and show the evidence in its window similar to the screenshot shown below:



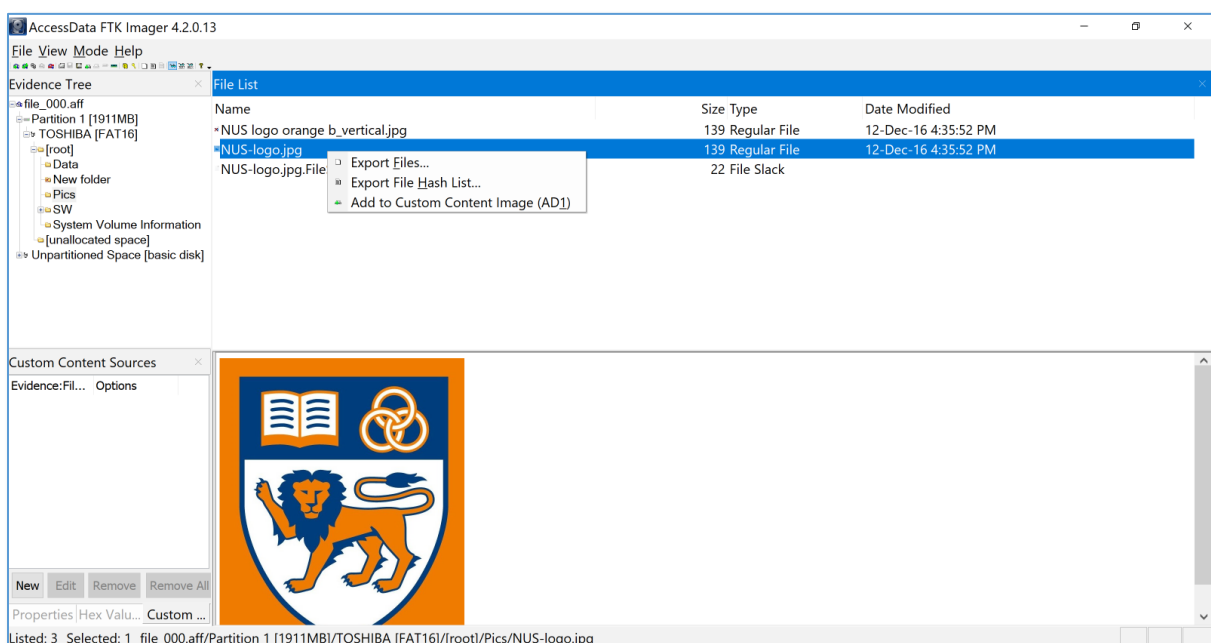
6. Navigate the “Evidence Tree” by clicking the + symbol to expand an entry.



7. Select your **target folder** in the “Evidence Tree” pane, and then select a **target file** (e.g. NUS-logo.jpg below) in the “File List” pane. You can see the file’s preview in the “Viewer” pane. (Note: you can also select *multiple* files, e.g. for a common subsequent export step, by shift-clicking the files.)



8. Extract/export a file by right-clicking on the file and then select “Export files...”.



9. Choose a destination folder and then click the “OK” button.
10. After the file has been exported, the export results will be displayed.
11. Verify that you can access the exported file(s) on your Windows forensic workstation.

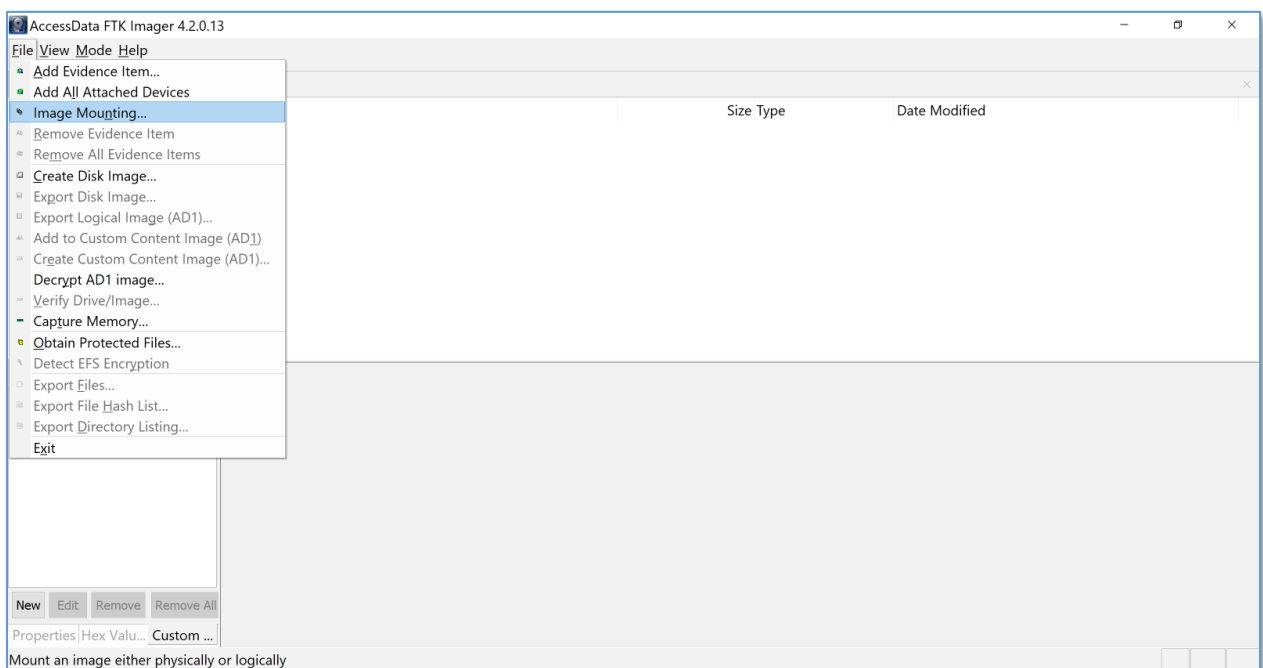
## ***[Optional]* Task 3 (Win-FWS): Mounting the Created Disk Image File using FTK Imager and Scanning for Malware**

### **Important Notes:**

- Besides browsing and extracting files, you can also use FTK Imager to **mount** the created forensic image file as **an accessible *drive***. Subsequently, you can utilize other **external tools** on your workstation to inspect the files.
- In this exercise, we will access the mounted drive by **scanning** it for possible malware using Windows Defender tool (or any other anti-virus software installed on your machine).
- For the **disk image**, you can use one that you previously used in Task 2.

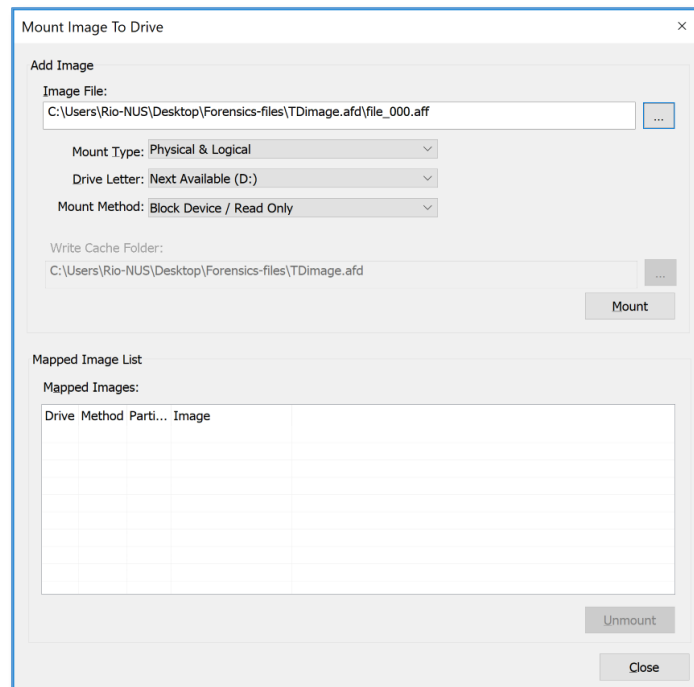
### **Steps:**

1. Launch FTK Imager.
2. From its main menu, select “File”, and then select “Image Mounting...” as shown below:

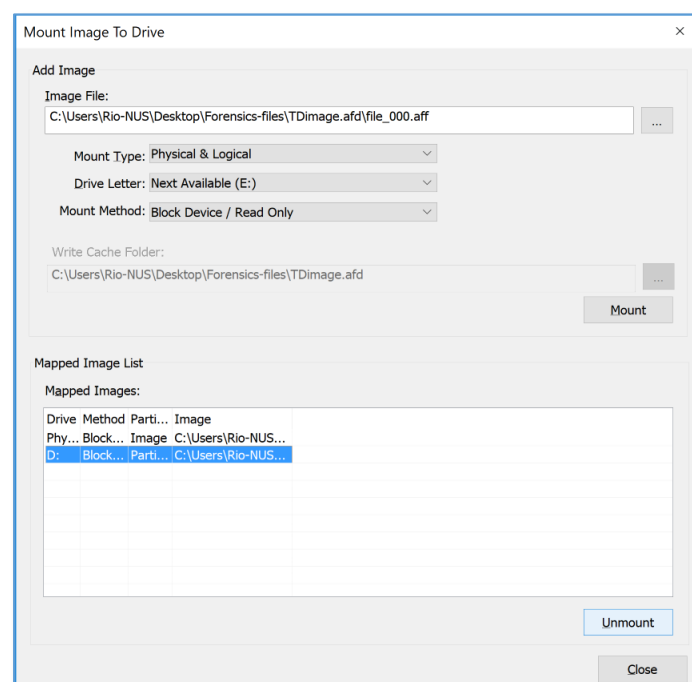




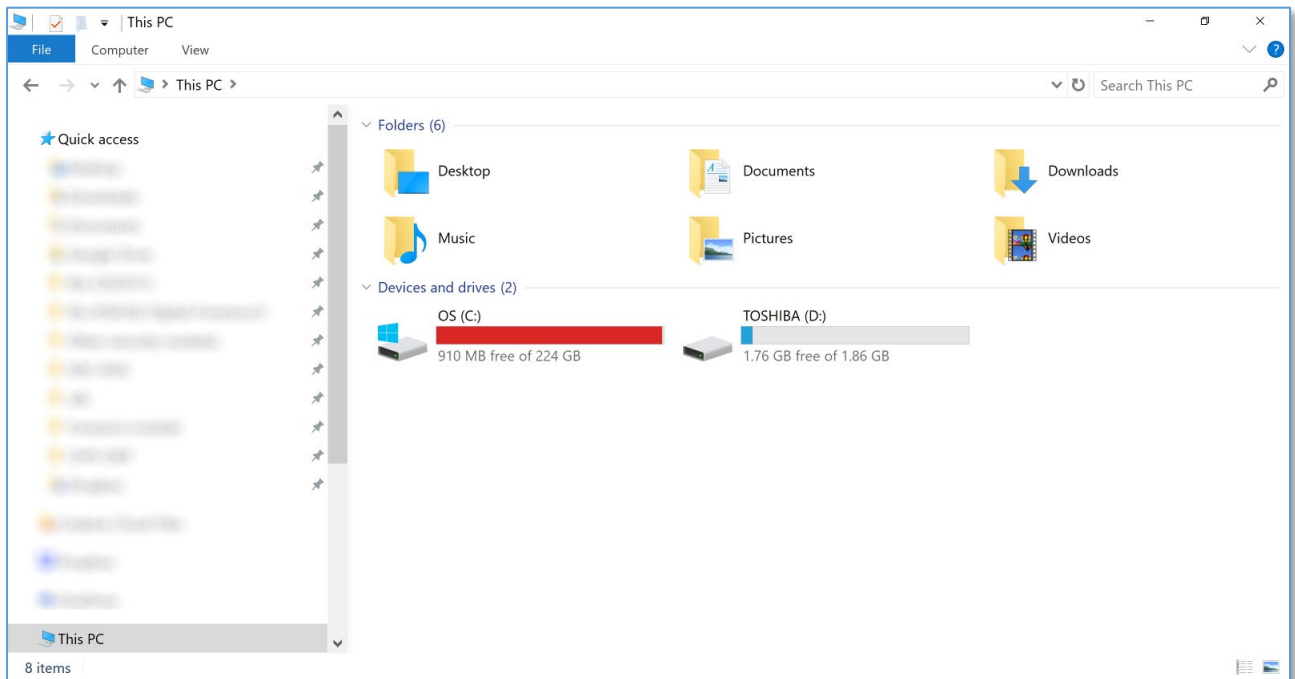
3. In the “Mount Image to Drive” window, select the “...” button and then specify your image file location:



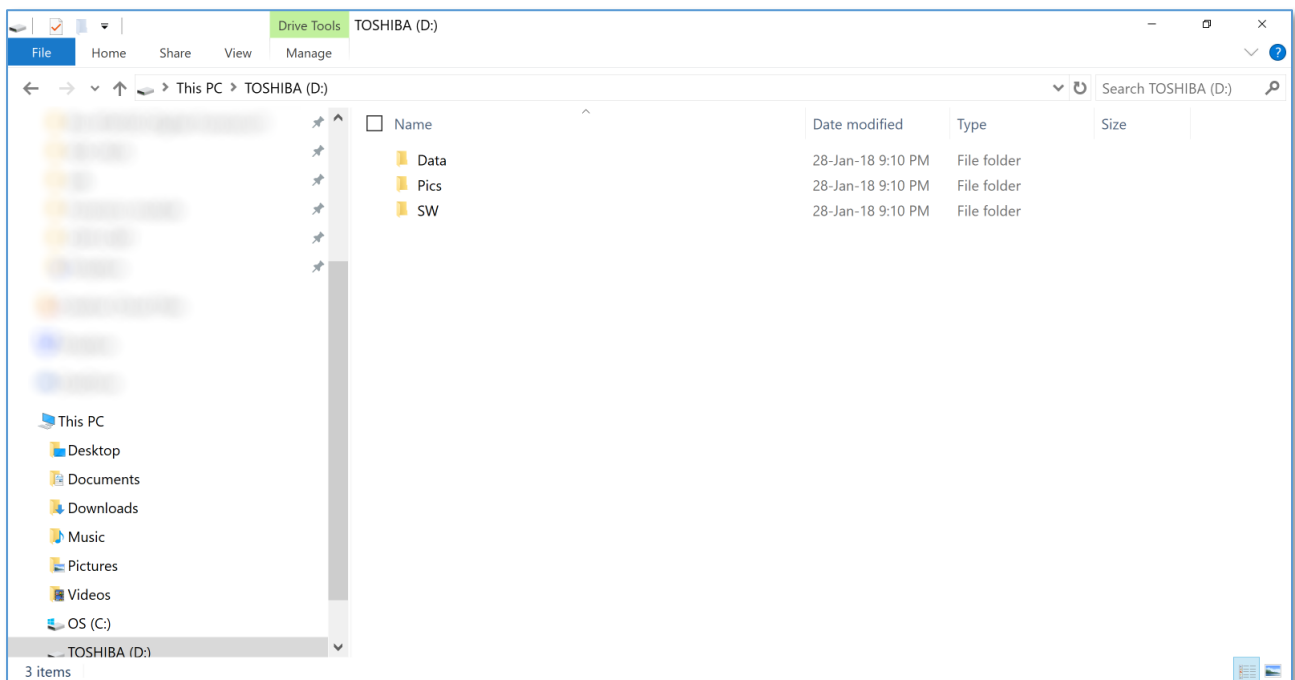
4. Configure the mount type, drive letter, and mount method as desired.
5. Click the “Mount” button. The mapped images will be shown on the list:



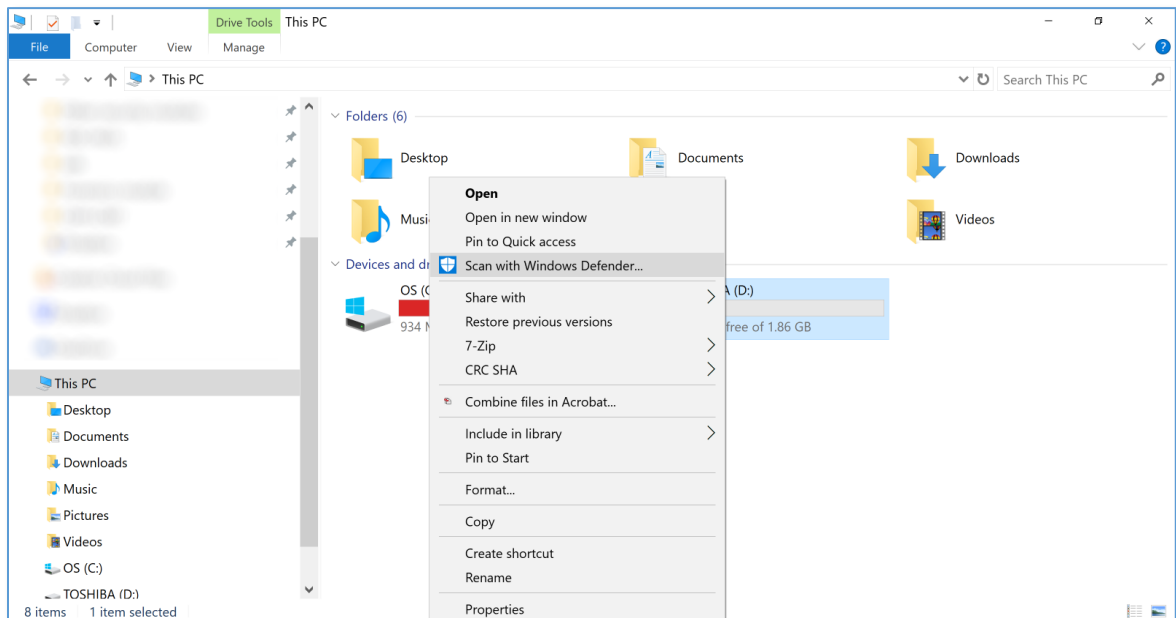
6. Now, launch File Explorer, and check that the mapped drive is visible:



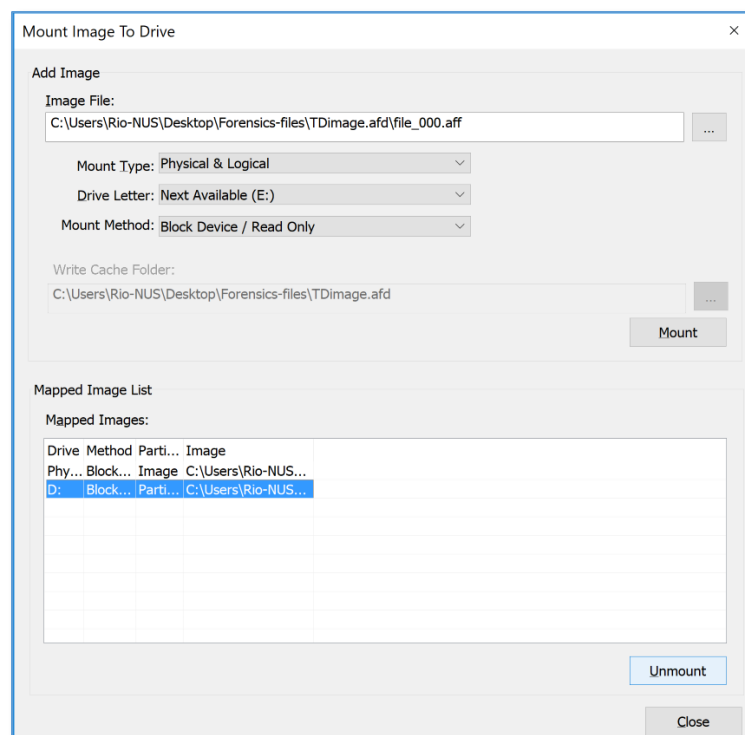
7. Navigate and access the mapped drive:



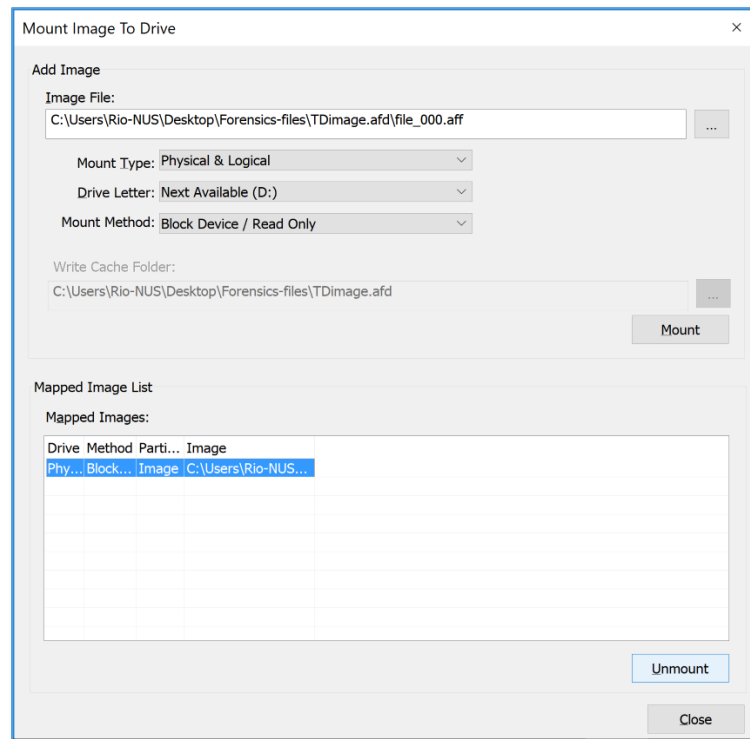
8. Right-click the drive as shown below, and then scan it with Windows Defender (or any other installed anti-virus software on your machine):



9. Once the scanning is completed, unmount the image file by selecting the mapped images in the “Mapped Image List” pane, and clicking “Unmount”:



10. Verify that the image file has been correctly unmounted, and the previously mapped drive is no longer accessible by File Explorer.



---

## Task 4-A (Lin-FWS): Creating a Forensic Image of Your Target Drive using Linux Forensic Workstation (With dd)

### Important Notes:

- You will now use your **Linux** forensic workstation to create a disk image of an external drive by using **dd tool**.
- Since dd does not come with a built-in hashing tool, you will need to manually compare the **hash values** of the target drive and the created disk image file after your acquisition.

### Steps:

1. Start your Linux forensic workstation.
2. Connect your target thumb drive to your machine's USB port (if necessary).  
Make sure that the attached drive is recognised by the OS.

3. Launch a terminal.

4. First, check the attached drive pathname by running:

```
# fdisk -l
```

5. Suppose your drive is referred to as /dev/sdb.

Run dd using the following command (*note*: this step may take a while):

```
# dd if=/dev/sdb of=/root/disk1.img conv=noerror,sync
```

[Note that, by default, if dd encounters an error while reading an input block,

it will stop running. You can **force dd to continue** by using the option

conv=noerror. Additionally, to **place zeros** in place of the errors

encountered, also include the sync option as in the sample command above.]

6. Calculate the hash value of the drive by running:

```
# md5sum /dev/sdb
```

7. Calculate the hash value of the created disk image file by running:

```
# md5sum /root/disk1.img
```

8. Compare the two outputted hash values. Make sure that they do match.

## Additional Notes on dd:

- dd is a popular Linux tool for copying copy a file. You can check its man page, e.g. <http://man7.org/linux/man-pages/man1/dd.1.html>, for its **various flags** such as `bs` (block size), `count`, `conv`, and `status`. You can also utilize its `skip` and `seek` options to skip  $n$  blocks at the start of the input and output, respectively.
- dd can also be employed for other purposes, such as:
  - Data conversion/modification: see [https://en.wikipedia.org/wiki/Dd\\_\(Unix\)#In-place\\_modification](https://en.wikipedia.org/wiki/Dd_(Unix)#In-place_modification);
  - Disk wipe: see [https://en.wikipedia.org/wiki/Dd\\_\(Unix\)#Disk\\_wipe](https://en.wikipedia.org/wiki/Dd_(Unix)#Disk_wipe).
- It is possible to transfer the acquired data **over a network**. That is, the target output file is on a host different from the one storing the input (device) file. For this purpose, you can also employ **netcat (nc)** as follows:
  - On the host storing the input file:

```
# dd if=/dev/sdb conv=noerror,sync |  
nc -w 5 <destination-host-IP> <destination-host-port>
```
  - On the destination host to store the output file (e.g. `disk1.img`):

```
# nc -lp <destination-host-port> > /root/disk1.img
```
- Note that data transfer using `nc` is **not** secured (e.g. encrypted). As such, you may want to perform a network-based acquisition using `dd` *only* over

a trusted network. Alternatively, you can consider employing **CryptCat** (<http://cryptcat.sourceforge.net/>), which enhances netcat with encryption.

- If needed, you can use the Windows version of dd (<http://www.chrysocome.net/dd>) on your Windows forensics workstation.

To identify devices connected to your machine, run: `dd --list`.

For your subsequent copy operation using dd in Windows, note that you will need to specify the suitable **DOS device path(s)** as described in

<https://docs.microsoft.com/en-us/dotnet/standard/io/file-path-formats>.

Also note that, to image a USB drive, you should utilize the `--size` option as explained in <http://www.chrysocome.net/dd>.

As such, you can run dd in Windows as in the following sample command:

```
dd if=\\.\E: of=C:\disk1.img --size --progress
```

---

## ***[Optional]* Task 4-B (Lin-FWS): Creating a Disk Image of Your Target Drive using Linux Forensic Workstation (With dcfldd)**

### **Important Notes:**

- In this exercise, you will image an external drive using a more forensically-oriented dd version called **dcfldd** on your Linux forensic workstation.
- Among its **extra features**, dcfldd allows more than one output file, supports simultaneous multiple checksum calculations, provides a verification mode for file matching, and can display the percentage progress of an operation.

### **Steps:**

1. Connect your target thumb drive to your machine's USB port (if necessary).  
Make sure that the attached drive is recognised by the OS.

2. Launch a terminal.

3. First, check the drive pathname by running:

```
# fdisk -l
```

4. Suppose your drive is referred to as /dev/sdb.

Run dcfldd as follows (*note*: this step may take a while):

```
# dcfldd if=/dev/sdb of=/root/disk1.img hash=md5  
hashlog=hashlog.log
```

5. Calculate the hash value of the drive using the command below:

```
# md5sum /dev/sdb
```

6. Compare the two reported hash values. Make sure that they do match.