SAT1: 010: **Creating a Forensic Hard Drive Capture**

Overview

There are many utilities for acquiring drive images. There are plenty of good tools that provide a high level of automation and assurance. This training will walk the student through the process of taking a drive image using AccessData's FTK Imager tool.

Time: 30 Minutes

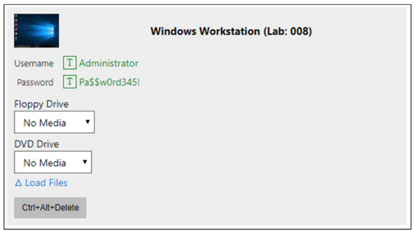
Learning Objectives

Upon completion of this lab, you should be able to:

1. Use FTK Imager to perform a forensic capture of a Windows 10 hard drive and save it for export.

Log in to the Lab Machine

Select the **Windows 10** machine on the Machines Tab.



Windows Workstation (Lab: 008)

Username T Administrator

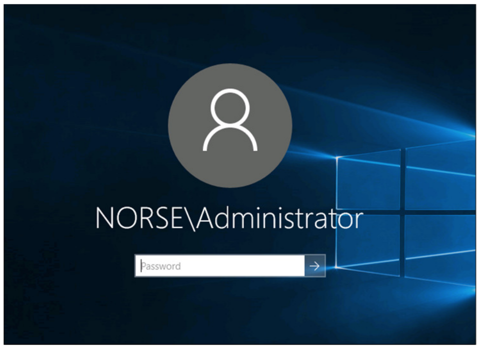
Password T Pa$$w0rd345!

Floppy Drive: No Media

DVD Drive: No Media

Select the Password → on the **Windows 10** machine and

click on the T Pa$$w0rd345! on the **Machines Tab**, and press **Enter** to log in to the machine.



Introduction to FTK Imager

FTK Imager is a Windows acquisition tool included in various forensics toolkits, such as Helix and the SANS SIFT Workstation, and Kali Linux.

The version used for this lab was downloaded directly from the AccessData web site (FTK Imager version 2.6.0).

First, let's talk a little about forensic imaging and security of the image.

________ is is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest - typically rendered as a hexadecimal number, 40 digits long. It was designed by the United States National Security Agency, and is a U.S. Federal Information Processing Standard.

Because we don't want to alter the hard drive we are creating an image of, we don't want to install a tool on the machine we are imaging. In this lab, we will use FTK Imager from an optical drive in order to avoid altering the machine we are working with.

1.0 Prepare the Evidence Disk

In this step, we will prepare your evidence disk for use. We will be using a forensic hard drive that has been attached to the host machine.

Note: Prior to using a hard drive that will contain forensic image(s), you should always verify the drive has no data on it.

1.1 Open **Windows Explorer** and navigate to the Forensic Drive, right click the drive and select **Quick Format**, and wait for the drive to format. Then close the window.

2.0 Create a Forensic Capture

In this step, we will use your prepared evidence disk to acquire an image of a live system using FTK Imager.

Note: Imaging a live system in this training will require physical access to the system that you want to image.

This means you will need to mobilize the toolset you are going to use. You will need your external USB evidence drive and a CD/DVD or **Decide if you are going to image a physical or logical disk**.

This distinction is important and depends on what your goals are. When you acquire a physical disk, you are creating an image of the entire physical hard drive from sector 0 to the last sector on the drive. Doing this means you will also acquire all of the logical volumes on the disk.

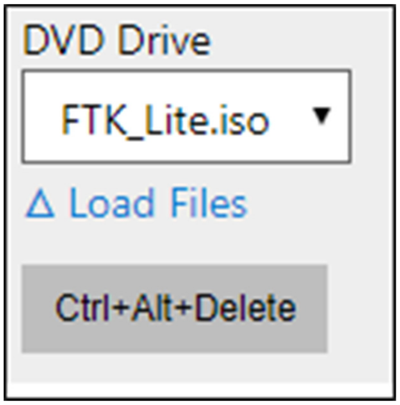
The advantages of acquiring a physical disk is that you capture everything including the all-important master boot record (MBR). The disadvantage to this approach is that it takes longer and requires more space on your evidence drive. Acquiring a logical drive means you are going to image a single logical volume (e.g. C:).

The only thing you will have on your evidence drive is the data space allocated to that particular volume. This means the space starting with the volume boot record (VBR) to the last sector allocated to the volume. Which to choose?

It all depends on the investigative goal.

Note: When in doubt – always take a physical disk image

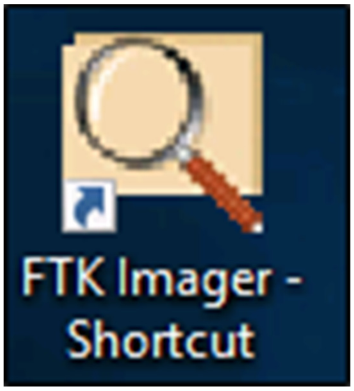
2.1 Ensure that your optical drive has the FTK Imager Lite loaded, you will see this on the Machines tab for the lab machine.



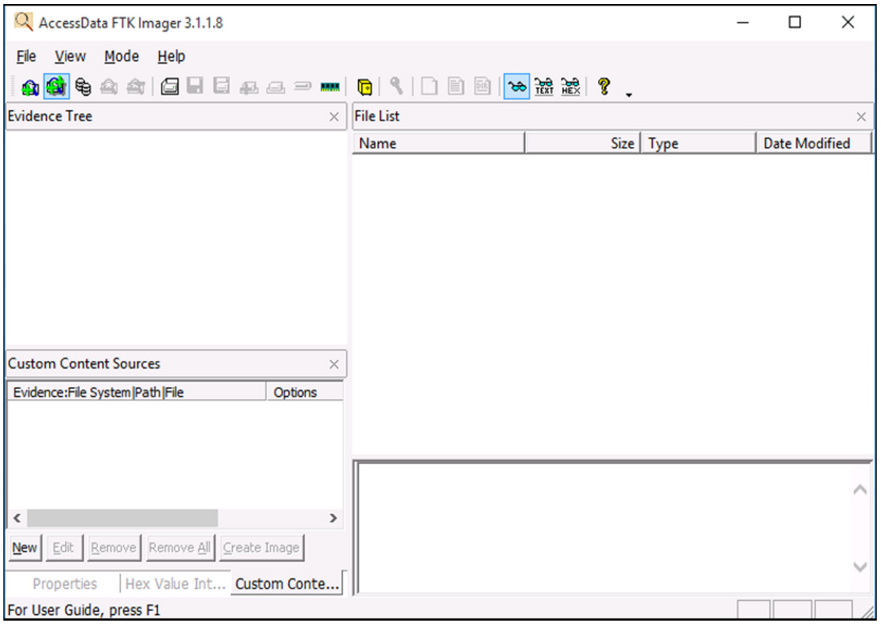
DVD Drive

FTK_Lite.iso

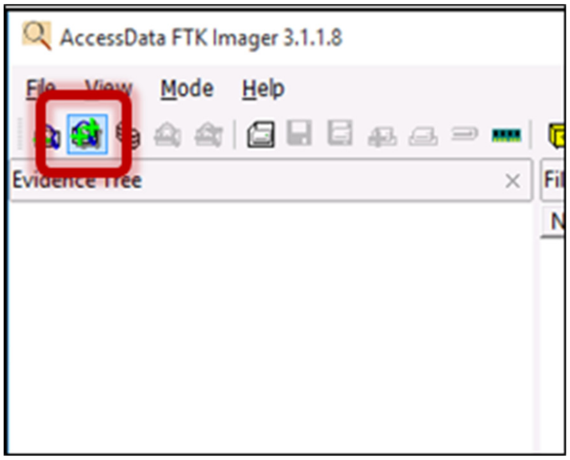
2.2 Click on FTK Imager on the Desktop.



The FTK Imager interface will open on your desktop.



2.3 Click the **Add Evidence Item** button.

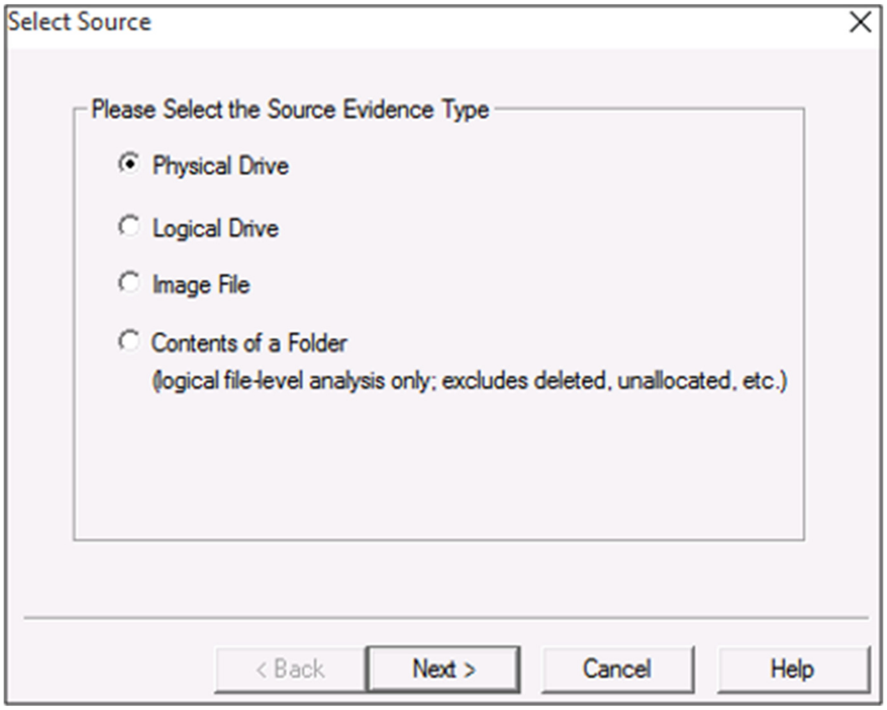


2.4 You now have to tell FTK Imager what you want to image.

Note: there is also a **Image File** option. You would use this option if you want to obtain an image of a VMWare vmdk file. FTK Imager can mount and acquire a virtual machine image.

For this class we will be imaging a **Physical Drive**

2.5 Click Next.



Select Source

Please Select the Source Evidence Type

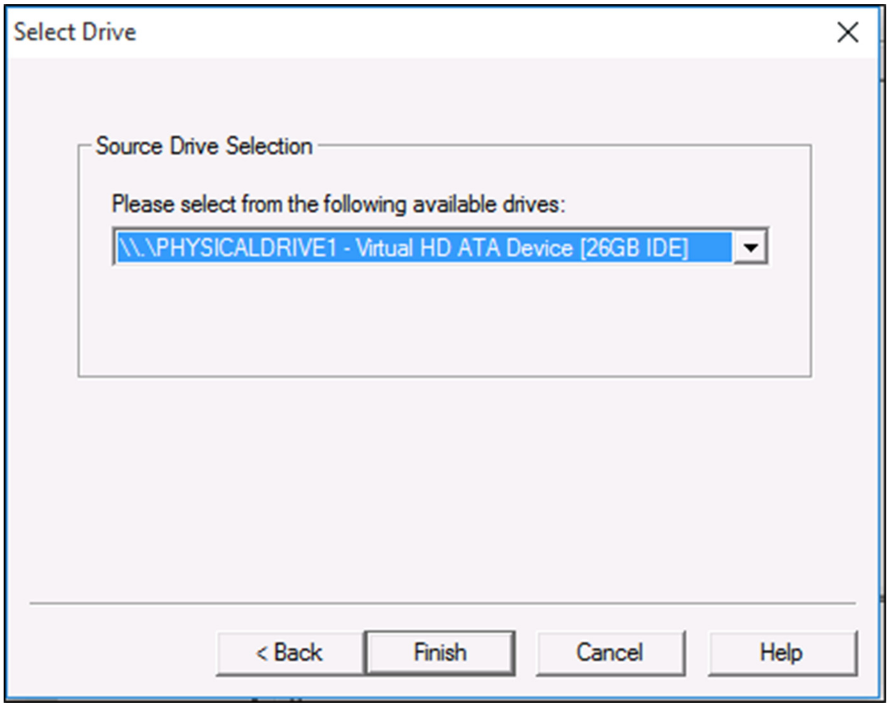
● Physical Drive

○ Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

2.6 From the **Select Drive** dropdown, and choose the physical drive you want to acquire, we will be making an image of Physical Disk 1, and click finish.



Select Drive

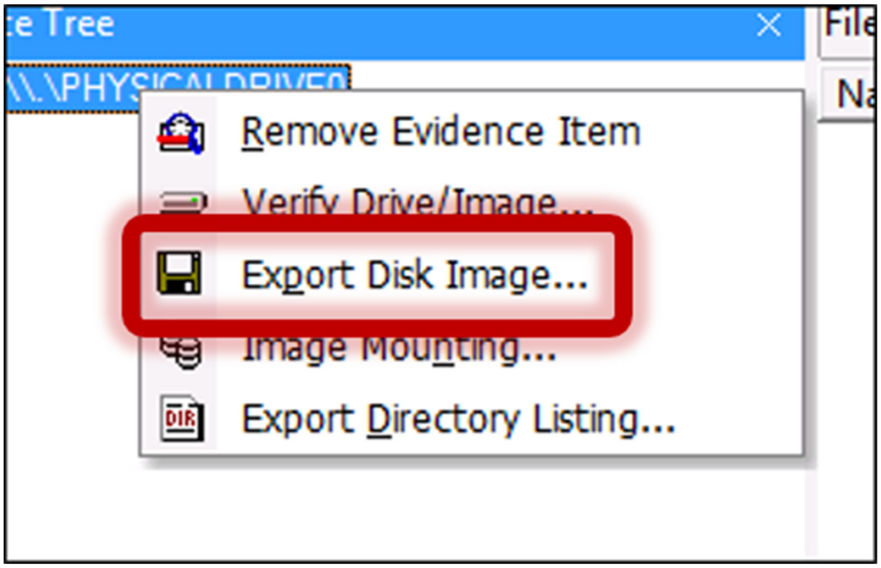
Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE1 - Virtual HD ATA Device [26GB IDE]

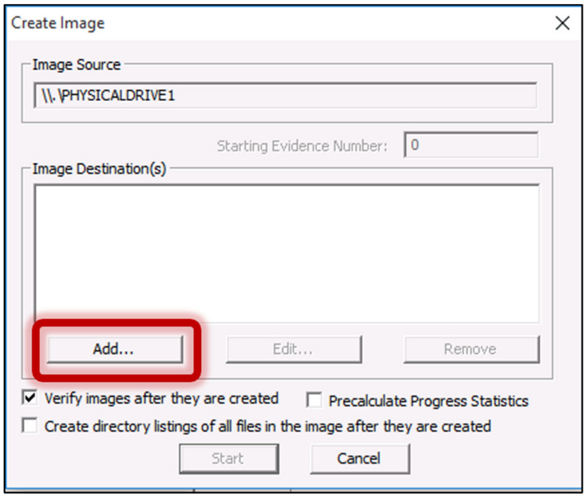
FTK Imager will take a moment, while it is mounting your suspect drive or volume. When it is mounted you will see your suspect drive in the Evidence Tree.

2.7 Right-click on your suspect disk or volume you want to image and select Export Disk Image.



In the next step, you must tell FTK Imager where to put the acquired disk image.

2.8 Click the **Add** button and select on the dialog box.



Create Image

Image Source

\\.\PHYSICALDRIVE1

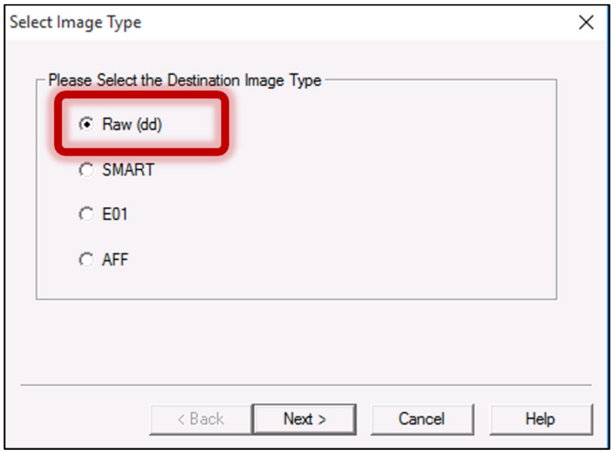
Starting Evidence Number: 0

Image Destination(s)

☑ Verify images after they are created □ Precalculate Progress Statistics

□ Create directory listings of all files in the image after they are created

2.9 Choose the image type you prefer. The most common are **Raw (dd)** and **E01**.


Select Image Type

Please Select the Destination Image Type

● Raw (dd)

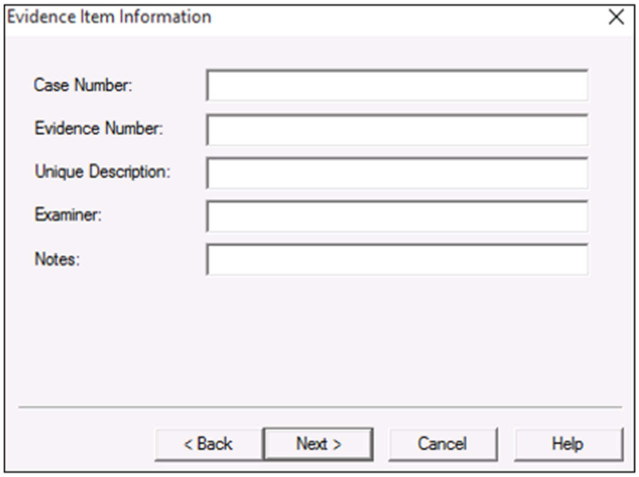
○ SMART

○ E01

○ AFF

Note: The E01 format is used by the EnCase forensic tools and is recognized by most other tools.

We will use Raw for this image, because it is the most flexible. Select the **Raw (dd)** option and click **Next**.


Evidence Item Information

Case Number:

Evidence Number:

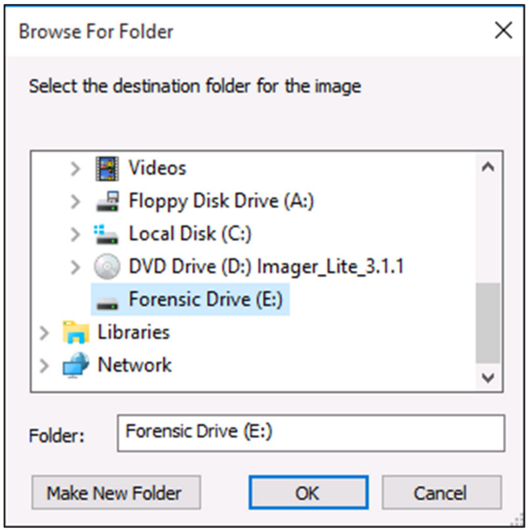
Unique Description:

Examiner:

Notes:

2.10 Fill out the **Evidence Item Information** fields and click **Next**. This information will help you identify the image later.

Next, you will select the destination folder where you want the evidence files placed. This will be your mounted TrueCrypt volume. Select Browse.



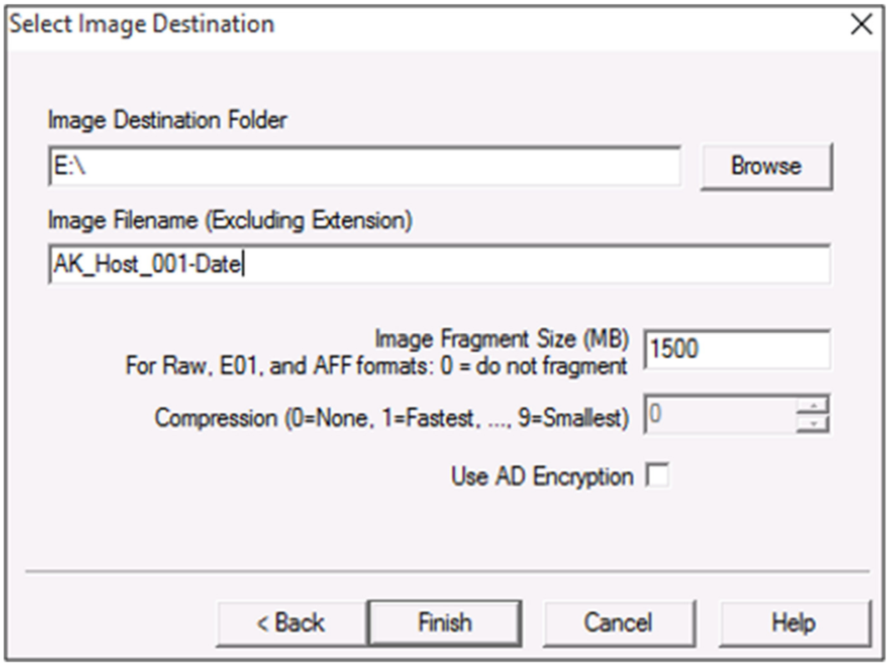
Browse For Folder

Select the destination folder for the image

Folder: Forensic Drive (E:)

2.11 Select the **Forensic Drive**, you can just place it on the drive root. Click **OK**.

Notice the **Image Fragment Size (MB)** field, this tells FTK Imager whether you want your image file in one large file or broken up into file fragments.



Select Image Destination

Image Destination Folder: E:\

Image Filename (Excluding Extension): AK_Host_001-Date

Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment: 1500

Compression (0=None, 1=Fastest, ..., 9=Smallest): 0

Use AD Encryption □

2.12 Name the image *AK_Host_001-(Date)*

The default fragment size is 1500 MB (1.5 GB). This setting will divide your image into a series of sequentially numbered files all 1.5 GB in size except the last file which will be smaller.

Note: If you set this setting to 0, FTK Imager will place the image in a very large single file.

Once you have set the destination folder, FTK Imager has all it needs to begin the acquisition of your suspect system physical disk or logical volume.

2.13 Click Finish.

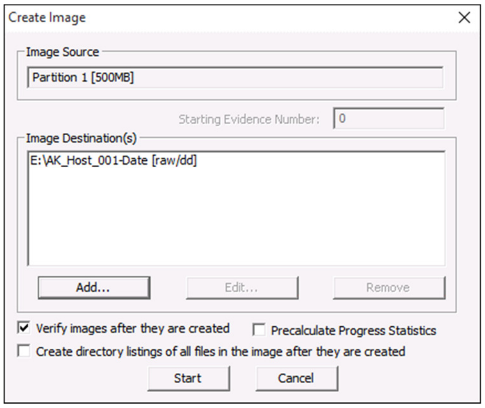

Create Image

Image Source: Partition 1 [500MB]

Starting Evidence Number: 0

Image Destination(s): E:\AK_Host_001-Date [raw/dd]

☑ Verify images after they are created
□ Precalculate Progress Statistics
□ Create directory listings of all files in the image after they are created

2.14 To start the image capture, click Start.

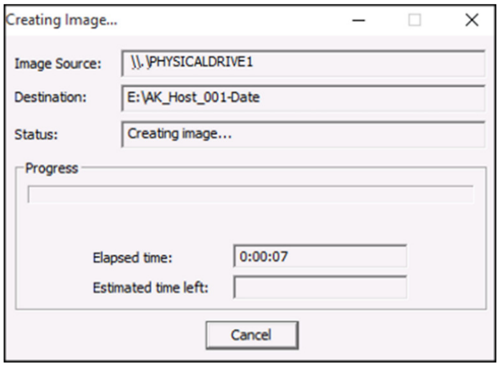

Creating Image...

Image Source: \\.\PHYSICALDRIVE1

Destination: E:\AK_Host_001-Date

Status: Creating image...

Progress

Elapsed time: 0:00:07

Estimated time left:

The imaging process will begin.

Note: Now that we have successfully acquired a forensically sound hard drive image of the evidence hard drive, we can now proceed to analyze it for artifacts and evidence, because of time restraints, the next lab will have an image loaded for your analysis.

Great job, you have completed LAB010!

Thank You, you may now close this module.