



FORENSICS V2 LAB SERIES

Lab 01: Creating a Forensic Image

Document Version: 2021-01-11

Copyright © 2021 Network Development Group, Inc.
www.netdevgroup.com

NETLAB+ is a registered trademark of Network Development Group, Inc.

Microsoft® and Windows® are registered trademarks of Microsoft Corporation in the United States and other countries. Google is a registered trademark of Google, LLC. Amazon is a registered trademark of Amazon in the United States and other countries.

Contents

Introduction	3
Objectives.....	3
Lab Topology	4
Lab Settings	5
1 Getting Familiar with FTK Imager	6
2 Create a Physical Forensic Image.....	10
3 Create a Logical Forensic Image.....	20
4 Verify the Image Contents by Reviewing the Image Report.....	27
5 Verify the Image Contents by Opening the Image in FTK Imager	30

Introduction

One of the goals of a digital forensic examination is to maintain the integrity of the evidence. This can be done through a series of methods such as documentation, imaging, and hashing. The exercises outlined in this lab will cover the imaging portion of the digital forensic process. It will teach a user how to use free digital forensic tools to create a court-admissible forensic image and how to review this imaged data. Let us get started!!

Objectives

- Getting familiar with FTK Imager
- Creating a forensic image in a windows environment
- Verifying the content of the image to ensure that the capture was successful

Lab Topology



Lab Settings

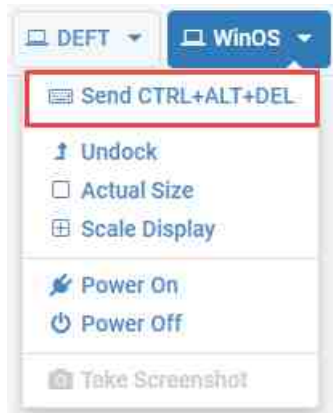
The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address / Subnet Mask	Account (if needed)	Password (if needed)
Caine	172.16.16.30	caine	Train1ng\$
CSI-Linux	172.16.16.40	csi	csi
DEFT	172.16.16.20	deft	Train1ng\$
WinOS	172.16.16.10	Administrator	Train1ng\$

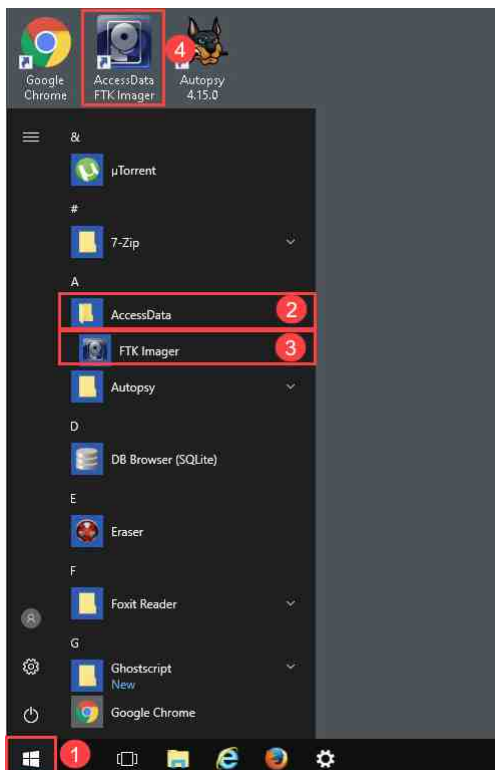
1 Getting Familiar with FTK Imager

The first thing we will do is get you familiar with the graphical user interface of FTK Imager.

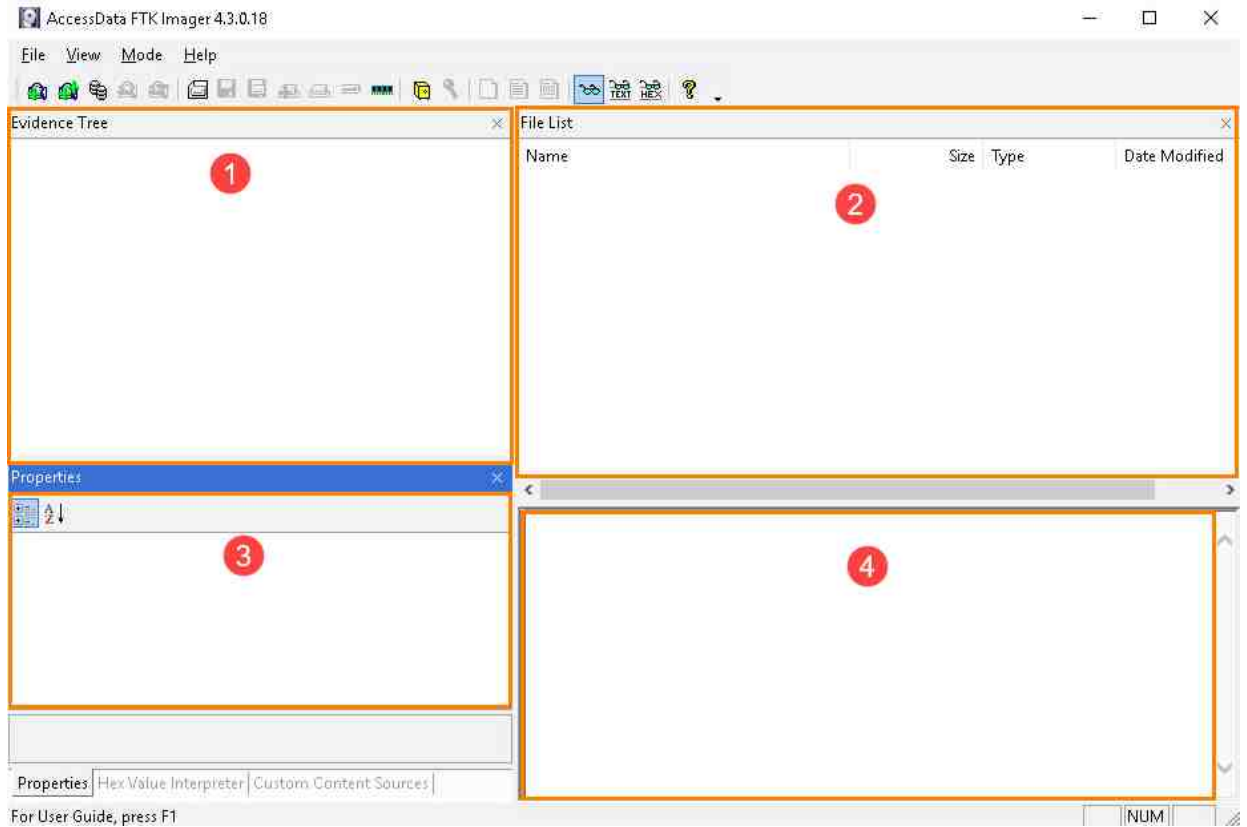
1. To begin, launch the WinOS virtual machine to access the graphical login screen.
 - a. Select Send CTRL+ALT+DEL from the dropdown menu to be prompted with the login screen.



- b. Log in as Administrator using the password: Train1ng\$
2. Once you are logged into the VM, launch the FTK Imager program from the Windows menu by navigating to Start Menu > AccessData > FTK Imager as seen in items 1, 2, and 3 below. Alternatively, you can open it by clicking the icon from the desktop, as seen in item 4.

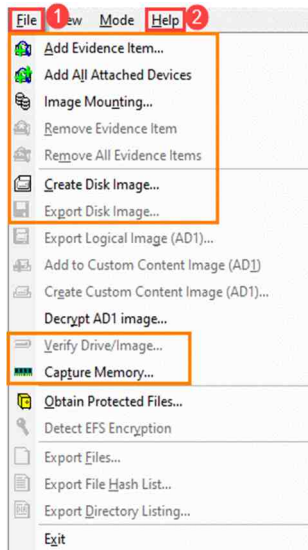











3. The following window will appear. Look at the sections highlighted in red. These are the different areas of the interface.



1	Evidence Tree	Displays evidence item(s) in a tree format
2	File list	Displays the list of files that are selected in the evidence tree pane
3	Properties	Contains various details about items selected in either the evidence tree or the file list panes
4	View pane	This is the box located in the bottom right corner of the FTK Imager window and displays the contents of files selected in the File list pane

4. Now let us look at the menus to see some important options. We will start with the File menu. To access this, select the File button at the top-left corner of the GUI, seen in item 1 below, which will reveal the menu as seen below.

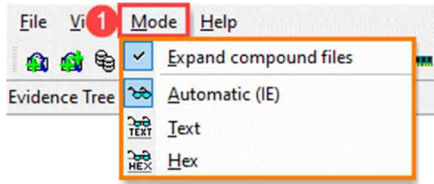


 Add Evidence Item...	Allows the user to add a single evidence item
 Add All Attached Devices	Allows the user to add all storage devices attached to the computer (<i>Beware as this option only adds live volumes</i>)
 Image Mounting...	Allows the user to mount an evidence item so that it can be viewed as an attached storage device
 Remove Evidence Item	Allows a user to remove a single evidence item
 Remove All Evidence Items	Allows a user to remove all evidence items that are currently loaded
 Create Disk Image...	Allows a user to create a forensic image of a storage device
 Export Disk Image...	Allows a user to create a disk image from a storage device that is already loaded in FTK Imager
 Verify Drive/Image...	Allows a user to perform a hash comparison of a forensic image
 Capture Memory...	Allows a user to capture an image of the RAM for the host that FTK Imager is running on



The table on the right outlines the most common options highlighted in red on the menu. Please refer to the user manual located in the help tab highlighted in item 2 for definitions on the remainder.

- Let us look at another important menu. This is the option called Mode. To get to it, select the Mode button at the top-left corner of the GUI, seen in item 1 below, to reveal the menu, as seen below.



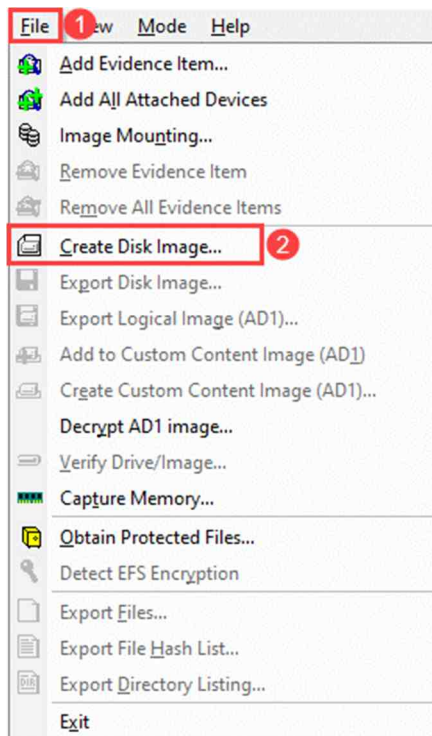
Expand Compound Files	Toggles the option to expand compound files such as Zip, tar, etc.
Automatic	Allows the software to choose how to display a file in the view pane (using IE, Text view, or Hex view)
Text	Switches the view pane to only show selected files in raw text
Hex	The Hex option switches the view pane to only show selected files in Hexadecimal

- The remaining menus are equally as important, but we will not cover them in this lab. Now let us move on to the good stuff, creating a forensic image!

2 Create a Physical Forensic Image

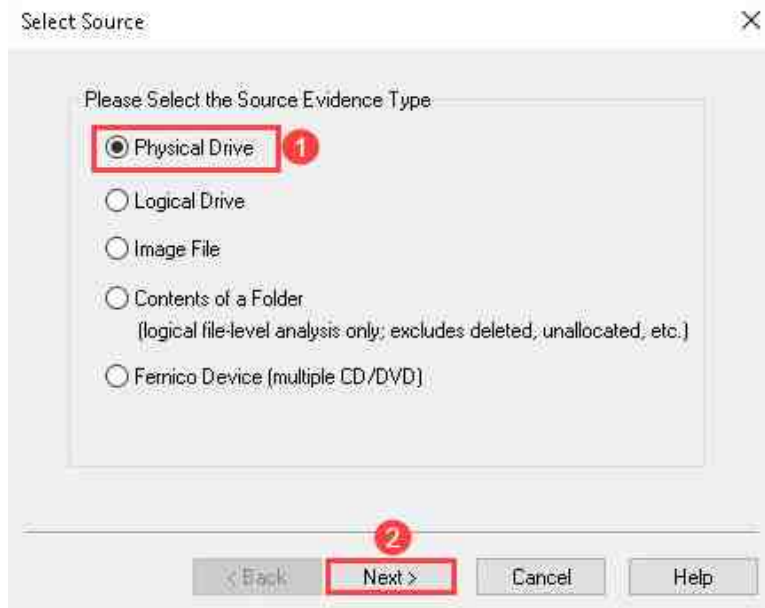
A forensic image of original evidence is required to avoid changing valuable data and risk making the evidence found inadmissible in court. In this task, we will walk through the steps for creating a forensic image of a physical drive on the lab machine. The best image for forensic analysis is always a physical image as it contains the most data. There are cases when a logical image is necessary as well, and we will cover this later in the lab. Let us get started!

1. FTK Imager should already be open. If not, reopen it and navigate to File > Create Disk Image as seen in items 1 and 2 below. This will open the Select Source window that will allow you to choose what type of volume you intend to replicate.



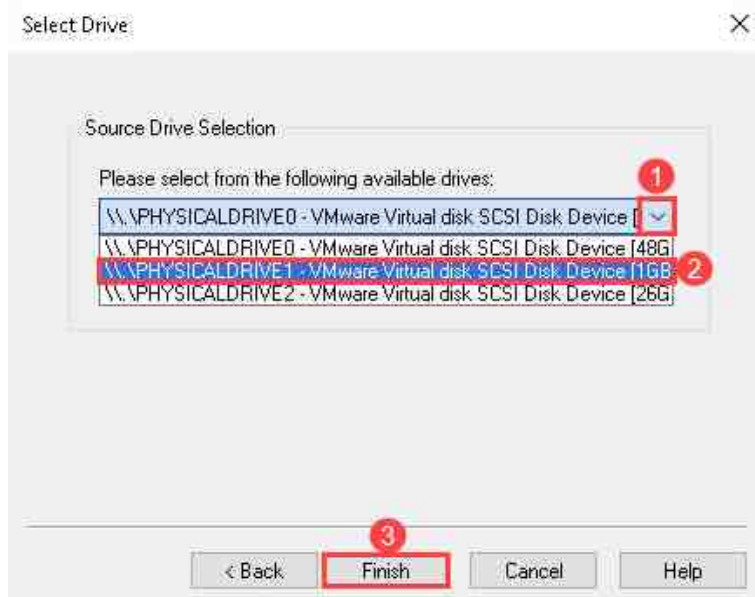
A hardware or software write-blocker must be used when imaging the original evidence.

2. Once you see the Select Source window, select the Physical Drive radio button, and then click Next seen in items 1 and 2 below. This will take you to the Select Drive window.

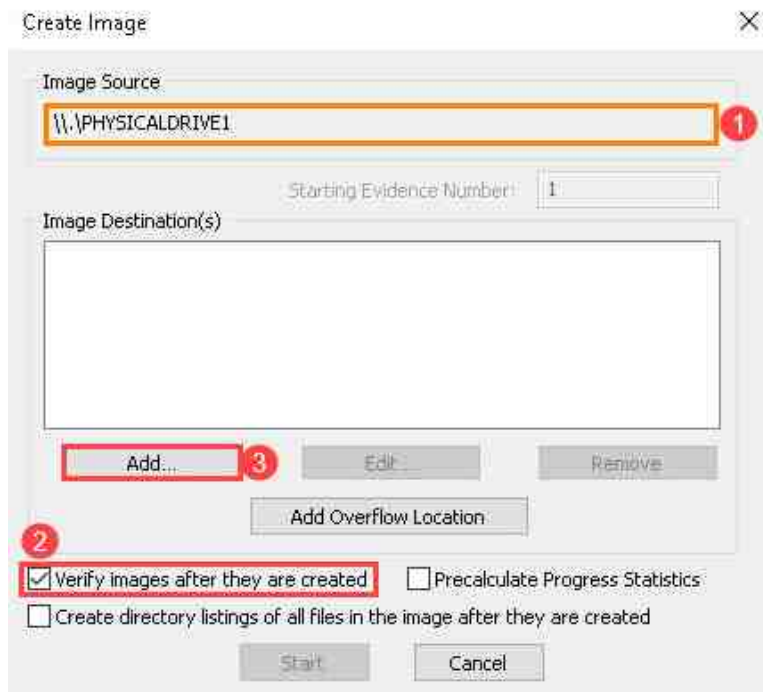


FTK Imager may hang right here, please be patient and do NOT click Next again.

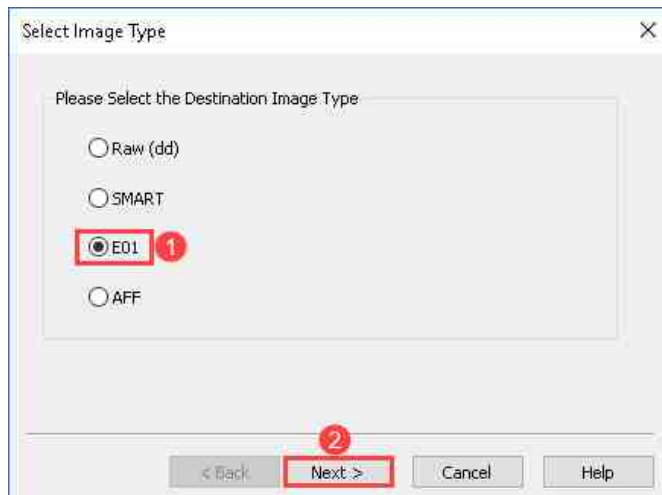
3. The select drive window will allow you to choose which volume you intend to replicate. Once you are in the Select Drive window, select the drive labeled PHYSICALDRIVE1 from the dropdown menu and then select Finish as seen in items 1, 2, and 3 below. This will take you to the Create Image window.



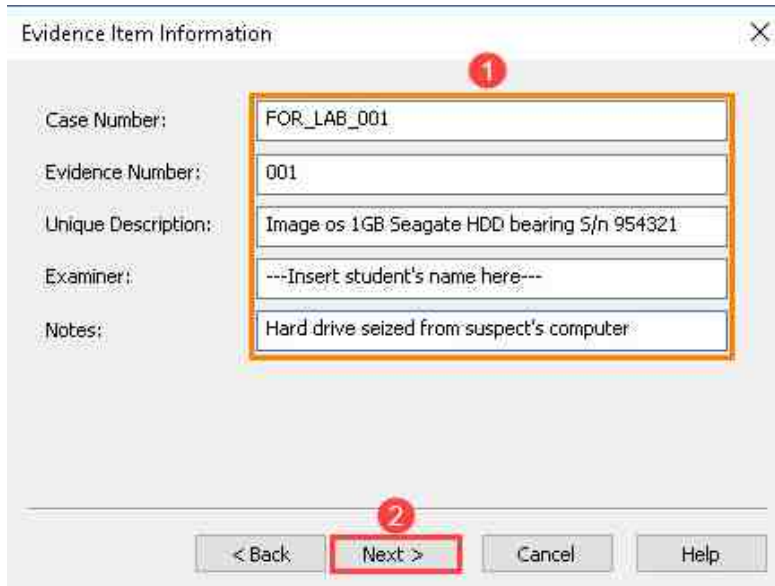
4. The Create Image window will give you the option to choose an image destination. It will also show the image source you selected, as seen in item 1. It also has several other useful options, such as:
 - Ñ Verifying your images after they are created, performs a comparison of the hashes before and after imaging to ensure nothing changed.
 - Ñ Precalculate Progress Statistics allows you to do a check to see a time estimate and determine if you have enough storage space for the image.
 - Ñ Create a directory listing of all files after the image is created, allows you to output a file containing a tree-style list of directories contained in the image.
 - Ñ Add Overflow Location, gives you an option to store the image if the destination is full.
5. For this exercise, only check the Verify images after they are created checkbox, as seen in item 2 below.
6. In the Create Image window, add the image destination. This can be achieved by clicking the Add button, seen in item 3, which will open the Select Image Type window.



7. This Select Image Type window allows you to choose from four (4) types of forensic image formats:
- Ñ Raw (dd) - This is a full image dump that uses no compression and does not store information about the image within it.
 - Ñ SMART - This format is used mainly for the SMART tool for Linux. It supports compression and segmentation but is not widely used anymore.
 - Ñ Advanced Forensic Format (AFF) - This format creates a raw image and stores the image metadata in a separate file. It supports compression and segmentation.
 - Ñ Expert Witness Format (E01) - This format is the most common forensic image type and supports compression and segmentation. It also stores data within the image container that can be used to help verify the image.
8. Let us use the E01 format for this exercise. To choose it, select the radio button beside E01 and then click Next, as seen in items 1 and 2, to go to the Evidence Item Information window.



9. The Evidence Item Information window is where you will fill in the information that will be permanently associated with the image. Ensure you fill it out accurately. Let us put some information in these fields. Use the information highlighted in item 1 below to fill in the fields. Click Next seen in item 2 when you are done. Note, the Examiner field should contain your name.



The screenshot shows the 'Evidence Item Information' dialog box. It contains several text input fields. A red circle with the number '1' is placed above a group of fields: 'Case Number', 'Evidence Number', 'Unique Description', 'Examiner', and 'Notes'. These fields are filled with the following text: 'FOR_LAB_001', '001', 'Image os 1GB Seagate HDD bearing S/n 954321', '---Insert student's name here---', and 'Hard drive seized from suspect's computer' respectively. At the bottom of the dialog, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. A red circle with the number '2' is placed above the 'Next >' button, which is also highlighted with a red rectangle.

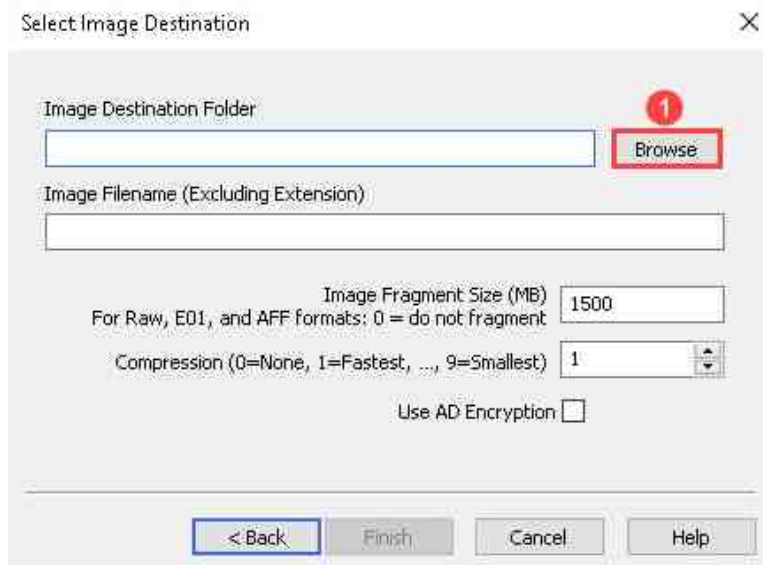
Case Number:	FOR_LAB_001
Evidence Number:	001
Unique Description:	Image os 1GB Seagate HDD bearing S/n 954321
Examiner:	---Insert student's name here---
Notes:	Hard drive seized from suspect's computer

< Back **Next >** Cancel Help

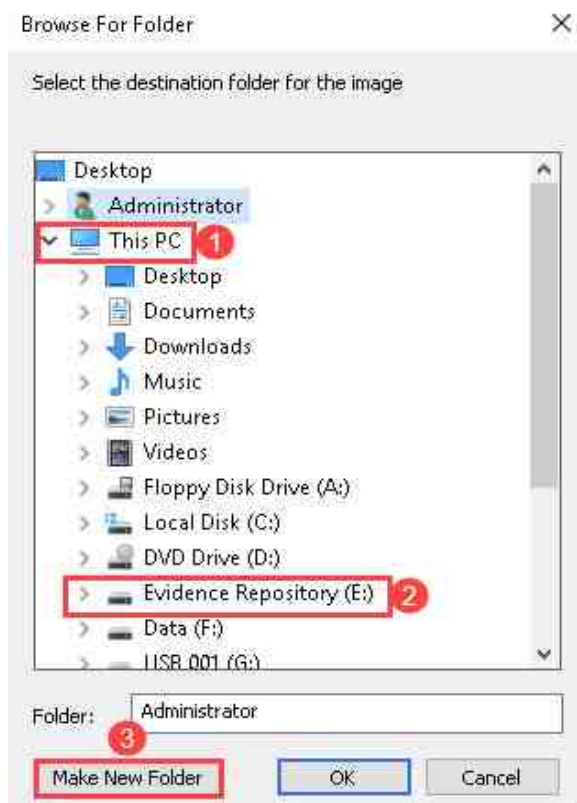
10. Now you should be at the Select Image Destination window. This window allows you to:

- Ñ set the storage location for the image.
- Ñ create a filename for the image.
- Ñ set the size of each image segment in megabytes (MB).
- Ñ adjust the level of compression. In this field, zero (0) means no compression while nine (9) means the highest compression possible; and
- Ñ choose whether to use AD Encryption to protect your image.

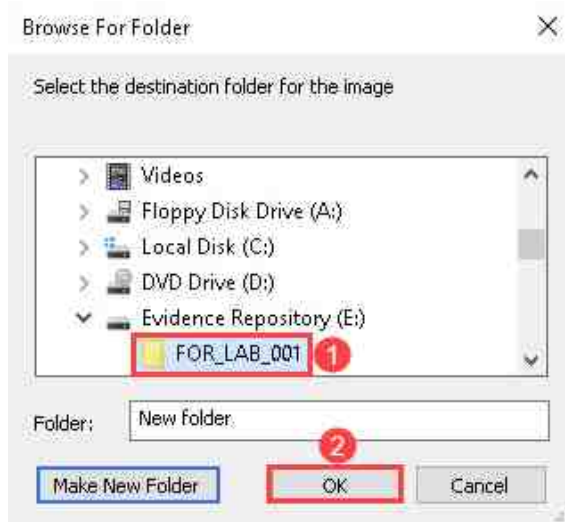
11. First, let us focus on setting the storage location for the image. To do this, select the Browse button seen in item 1 below. This will open the Browse for Folder window, which allows you to choose a location to store the image.



12. Once you are in the Browse for Folder window, navigate to ThisPC and select the disk drive labeled Evidence Repository (E:) and then click the Make New Folder option seen in items 1, 2, and 3 below. This will create a new folder in the Evidence Repository drive.

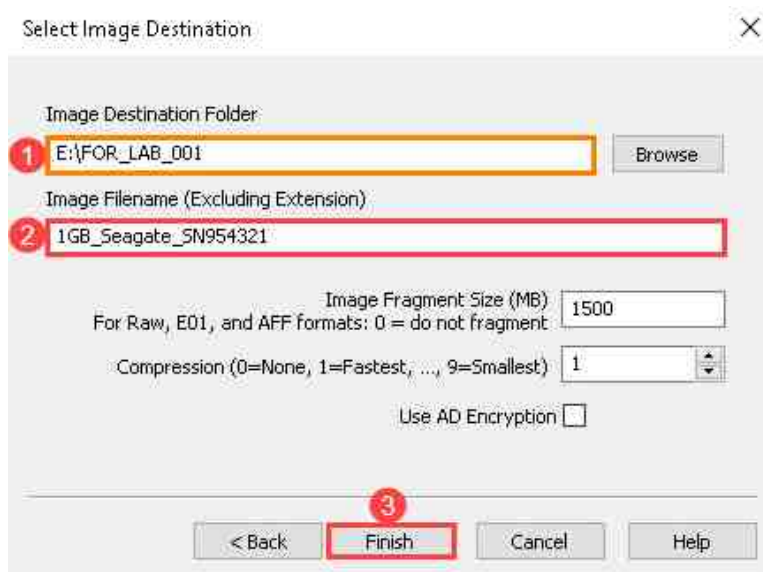


13. Let us give the folder a name to help us keep track of its content. Name the folder FOR_LAB_001 and then select OK, as seen in items 1 and 2 below, to go back to the Select Image Destination window.



Check that the image destination path, highlighted in item 1 below, is correct. It is common for the path to remain as New Folder, even after you rename it.

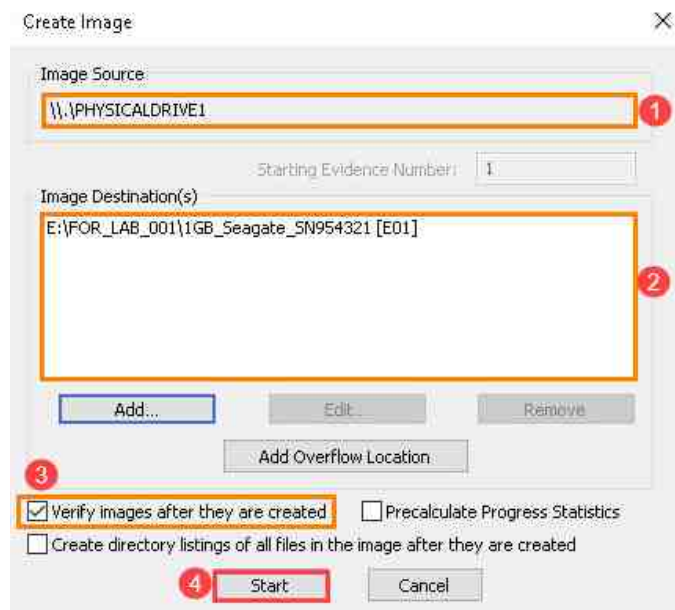
14. Once you are back in the Select Image Destination window, create a name for the image. An example is highlighted in item 2 below. Remember to check that the image destination path in item 1 is correct.



15. Leave the other settings at their default state and select Finish, seen in item 3 above, to go back to the Create Image window.

16. Now that you are back at the Create Image window, you need to verify that all the correct paths were selected. This is extremely important. Errors made at this phase can destroy the very data you aim to replicate. Before moving to the next step:

- Ñ Verify that the source is the one you intended to image as highlighted in item 1.
- Ñ Ensure that the destination path is the same as the one outlined in item 2.
- Ñ Ensure that the Verify images after they are created checkbox is ☒ checked as seen in item 3.



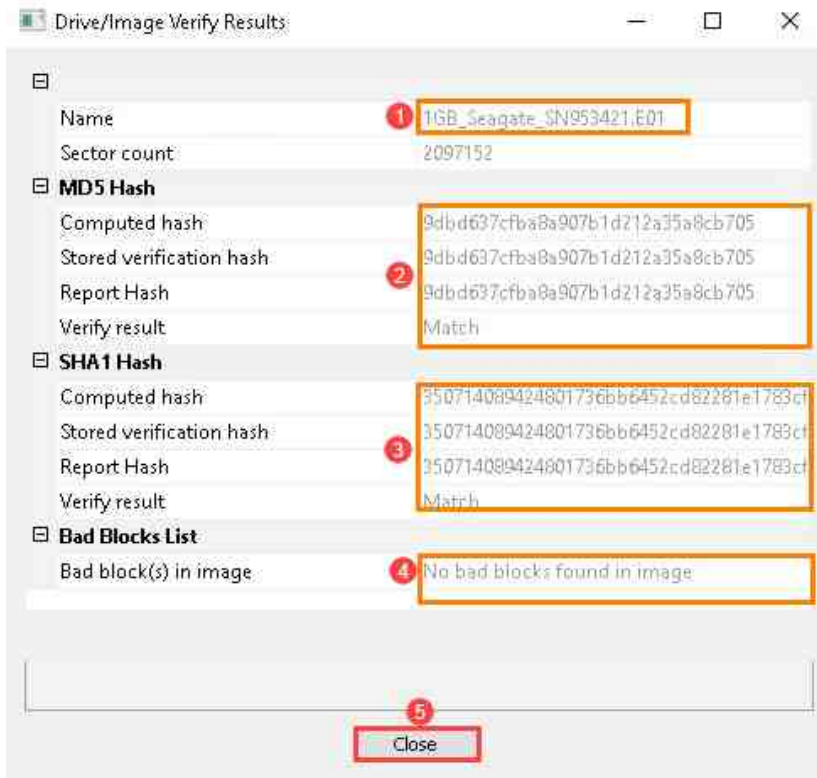
**Please
Note**

The Add Overflow Location is used ONLY if the image source is suspected to be greater than the destination. However, forensics best practices dictate that you ensure the destination has enough capacity for the source.

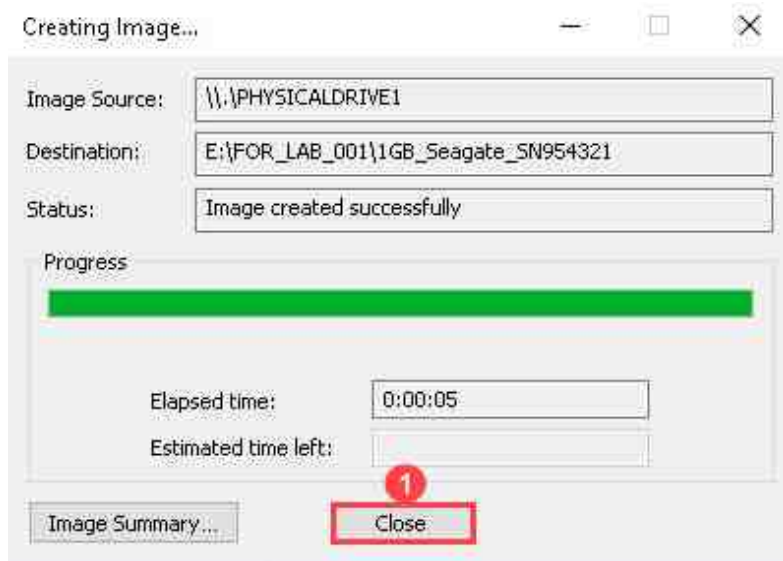
If Overflow location is selected, the verify images after they are created option should be unchecked as FTK imager cannot verify image segments stored in multiple locations. However, the image created can be verified later using the Verify Drive/Image option.

17. If you are here, it means that you have done all the verification checks and now you are good to go. To start the image, click the Start button highlighted in item 4 above. This will commence the imaging process.

18. Once the imaging is done, you will see the Drive/Image Verify Results window appear. This window only appears if you selected Verify Images after they are created before creating the image. It lists the image name seen in item 1, the MD5 and SHA1 verification hashes seen in items 2 and 3, and any detected bad blocks seen in item 4. Once you are done reviewing this data, click the Close button seen in item 5.



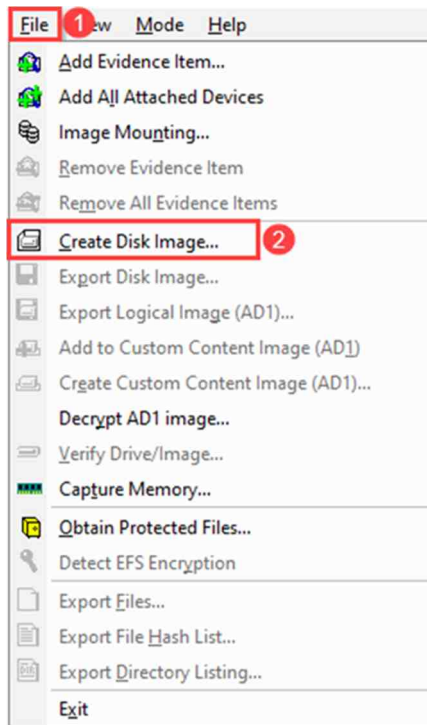
19. The window behind the Drive/Image Verify Results window should appear as below and will display a message that says Image created successfully. This means that you have completed the first and most important step of the forensic examination process. Click Close seen in item 1 below to close the dialogue box.



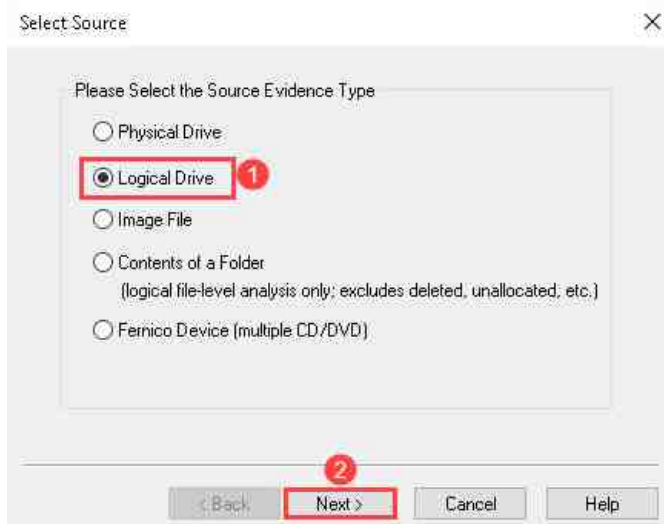
3 Create a Logical Forensic Image

In the previous task, we mentioned that there were times when a logical image is all that is necessary or all that you can get. In this task, you will learn to create a logical image.

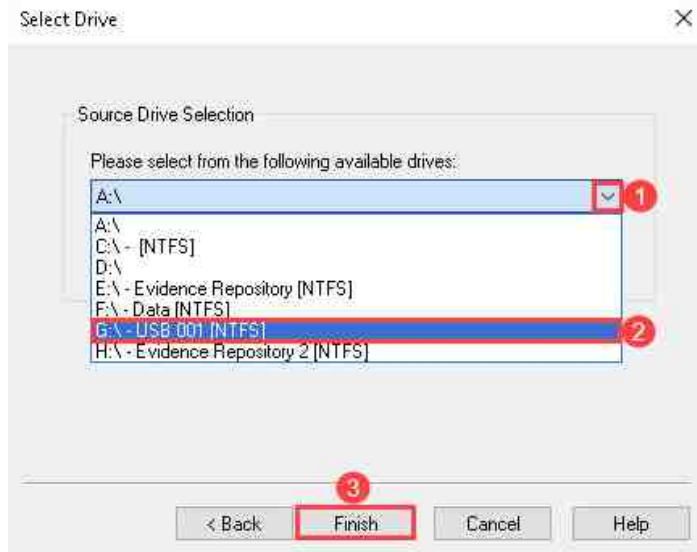
1. Let us go back to the FTK Imager interface and select the options File > Create Disk Image, as seen in items 1 and 2 below, to open the Select Source window.



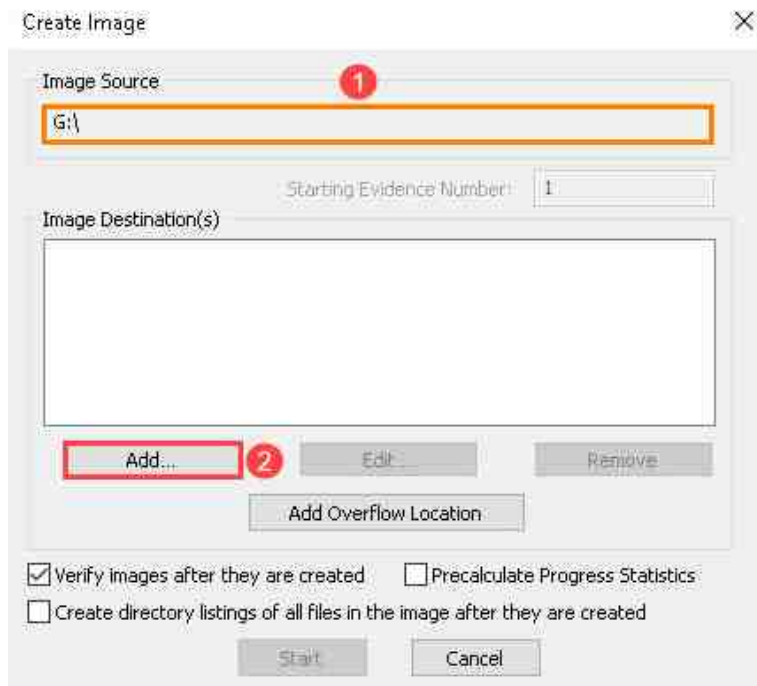
2. Once you get to the Select Source window, click the Logical Drive radio button seen in item 1. The logical drive option will allow you to choose a partition instead of the entire disk drive. Now click Next, as seen in item 2, to proceed to the Select Drive window.



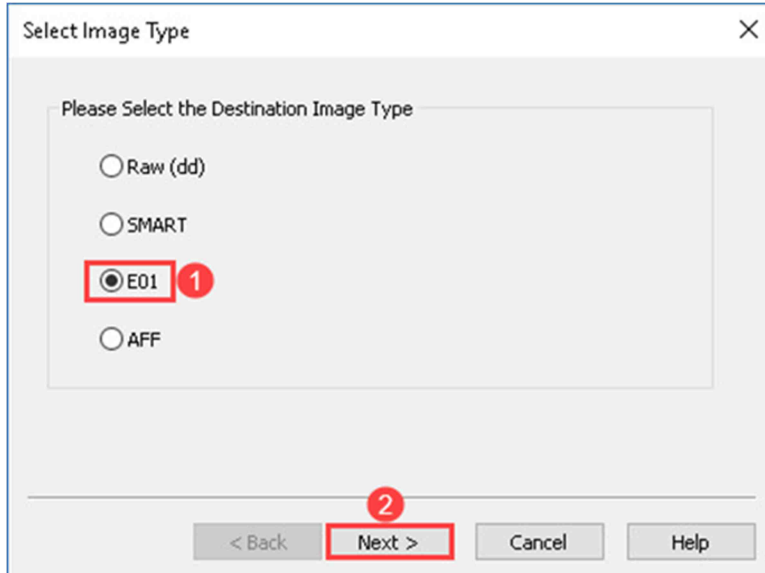
- When you get to the Select Drive window, select G:\ USB 001 [NTFS] from the dropdown menu and then click Finish, as seen in items 1, 2, and 3 below, to the Create Image window like you did before.



- When you get to the Create Image window, verify that the correct drive letter was selected. The drive letter should match the one seen in item 1 below. Next, select the Add button, seen in item 2, to open the Select Image Type window.

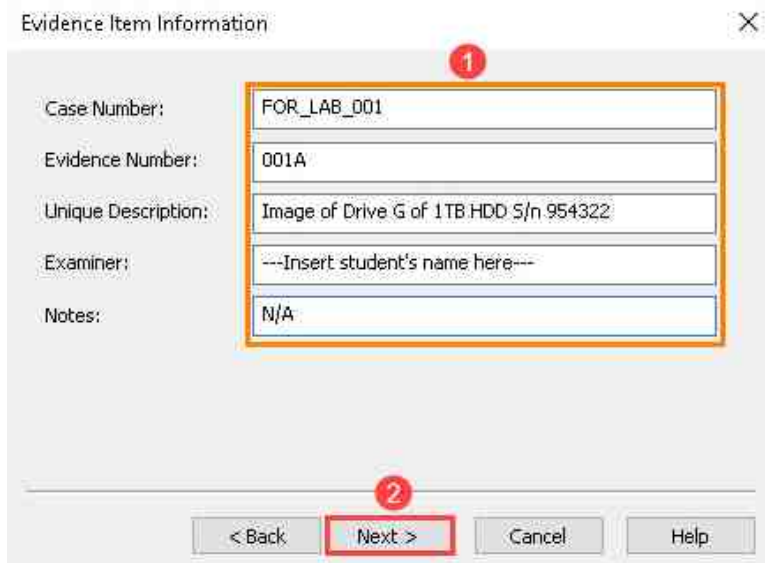


- Let us use the E01 format for this exercise as well. To choose it, select the radio button beside E01 and then click Next, as seen in items 1 and 2, to go to the Evidence Item Information window.



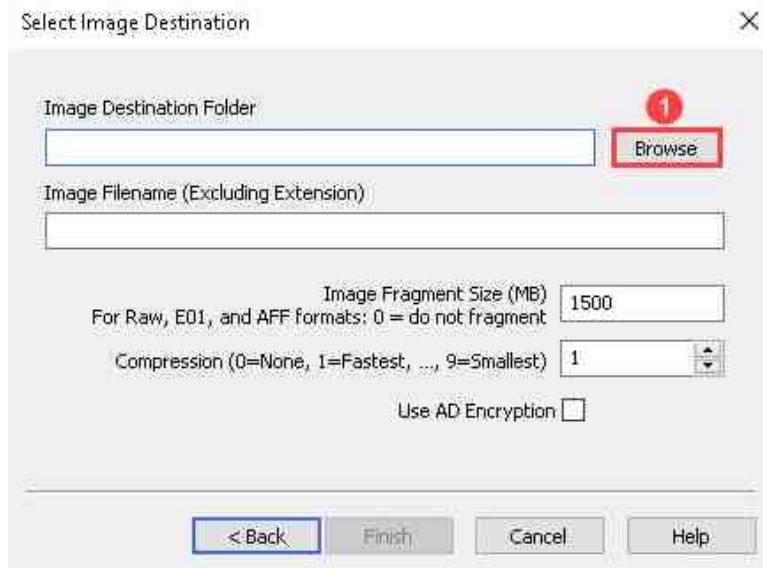
The 'Select Image Type' dialog box contains a section titled 'Please Select the Destination Image Type'. It has four radio button options: 'Raw (dd)', 'SMART', 'E01', and 'AFF'. The 'E01' option is selected and highlighted with a red box and a red circle with the number '1'. At the bottom of the dialog, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a red box and a red circle with the number '2'.

- You are back to the Evidence Item Information window, fill in the information as seen in the fields below, and then click Next as seen in items 1 and 2. Remember, the Examiner field should contain your name.

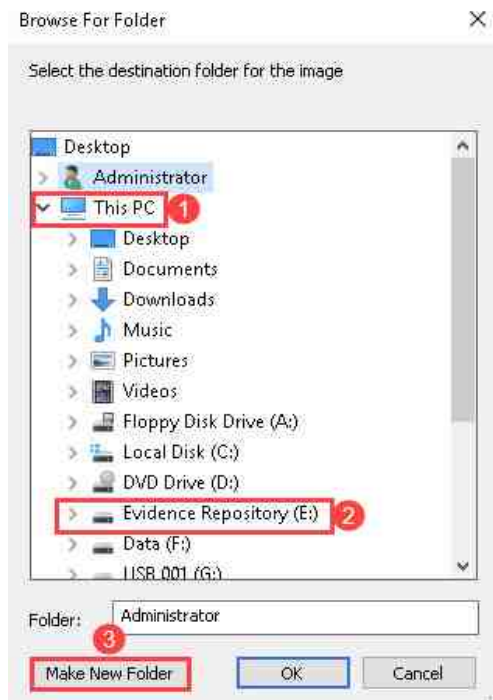


The 'Evidence Item Information' dialog box contains several text input fields. A red box with a red circle and the number '1' highlights the 'Case Number', 'Evidence Number', 'Unique Description', 'Examiner', and 'Notes' fields. The values entered are: 'FOR_LAB_001' for Case Number, '001A' for Evidence Number, 'Image of Drive G of 1TB HDD S/n 954322' for Unique Description, '---Insert student's name here---' for Examiner, and 'N/A' for Notes. At the bottom of the dialog, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a red box and a red circle with the number '2'.

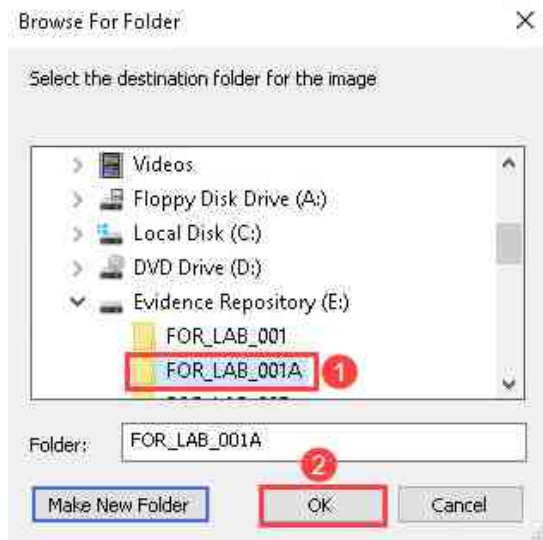
- Wow! You entered all that information already; that was quick. Then, you should now be seeing the Select Image Destination window. Here, select Browse, seen in item 1 below, to open the Browse for Folder window, which allows you to choose a location to store the image.



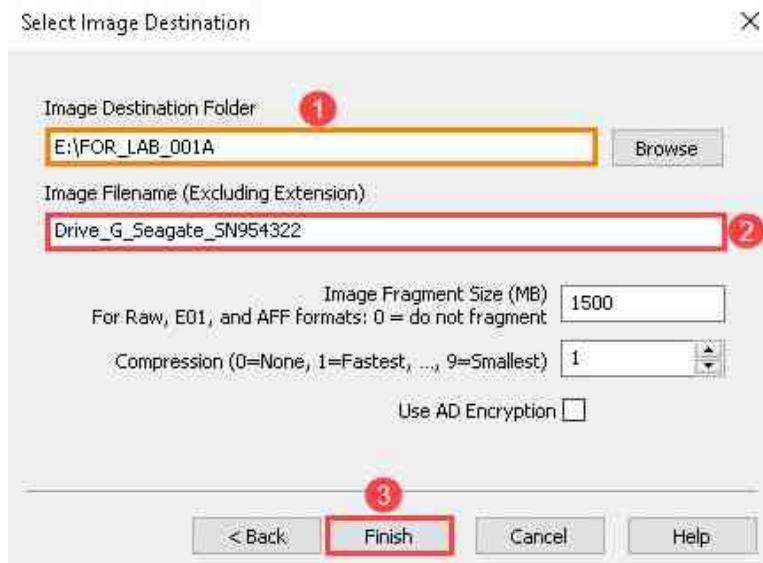
- Like you did before, browse to ThisPC > (E:) Evidence Repository and then select the Make New Folder option as seen in items 1, 2, and 3.



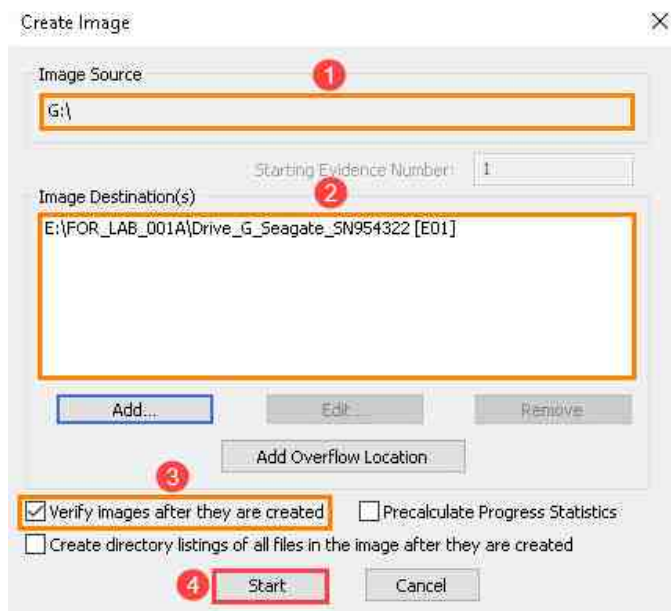
9. Name the new folder FOR-LAB-001A and then select OK, as seen in items 1 and 2, to go back to the Select Image Destination window.



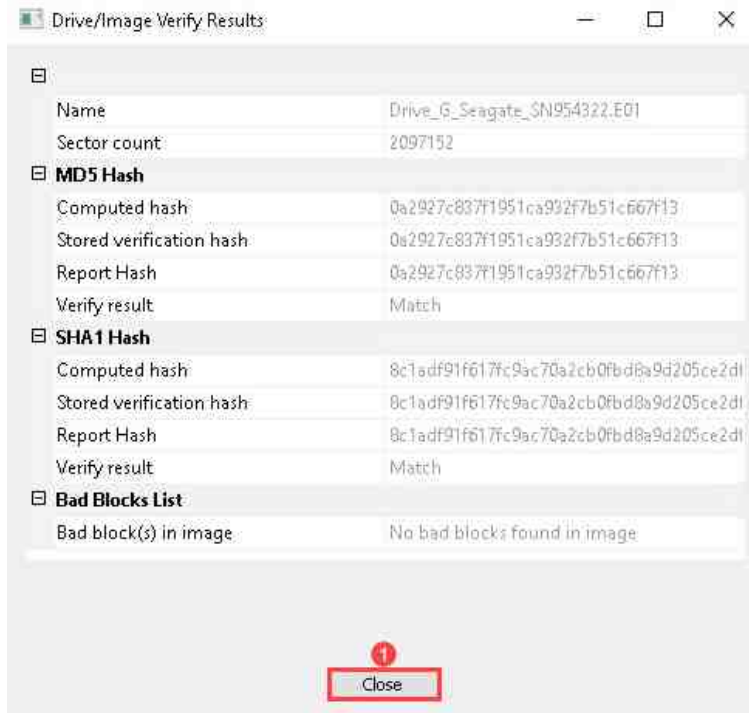
10. Once you are back in the Select Image Destination window, create a name for the image. An example is highlighted in item 2 below. Remember to check that the image destination path in item 1 is correct. Next, click Finish, as seen in item 3.



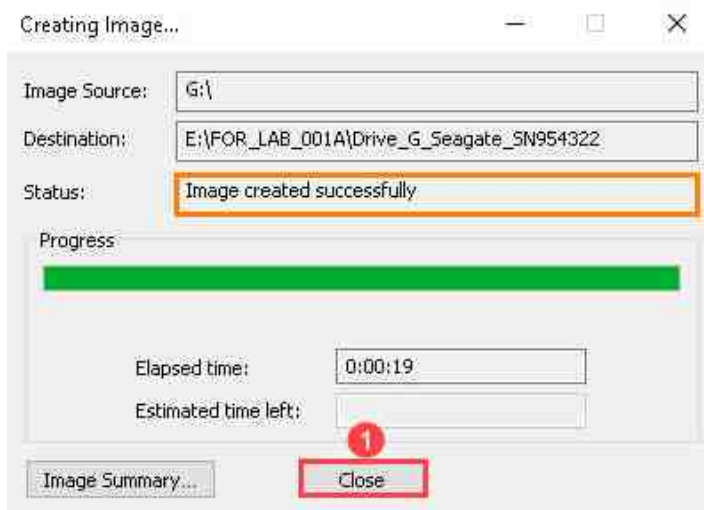
11. The Create Image window is your last chance to verify that you have all the correct paths selected. Remember, errors made at this phase can destroy the very data you aim to replicate.
12. Before proceeding:
 -) Verify that the source is the one you intended to image, as highlighted in item 1 below.
 -) Ensure that the destination path is the same as the one outlined in item 2 below.
 -) Ensure that the Verify images after they are created checkbox is checked as seen in item 3.
13. If you are sure that all the correct options were selected, you can click the Start button highlighted in item 4 below. This will commence the imaging process.



14. Now the logical image is complete, and you should see the Drive/Image Verify Results window appear as seen below. After reviewing the results of the verification, click Close to close the window.



15. Next, verify that the message Image created successfully is displayed in the Creating Image window and then click Close as seen in item 1 below.



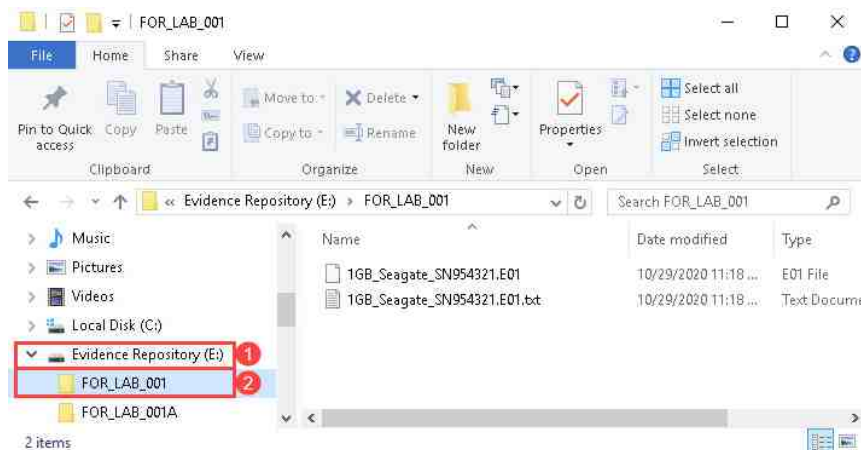
4 Verify the Image Contents by Reviewing the Image Report

Once you have created an image, there are two main things you need to check before packaging for storage. You need to:

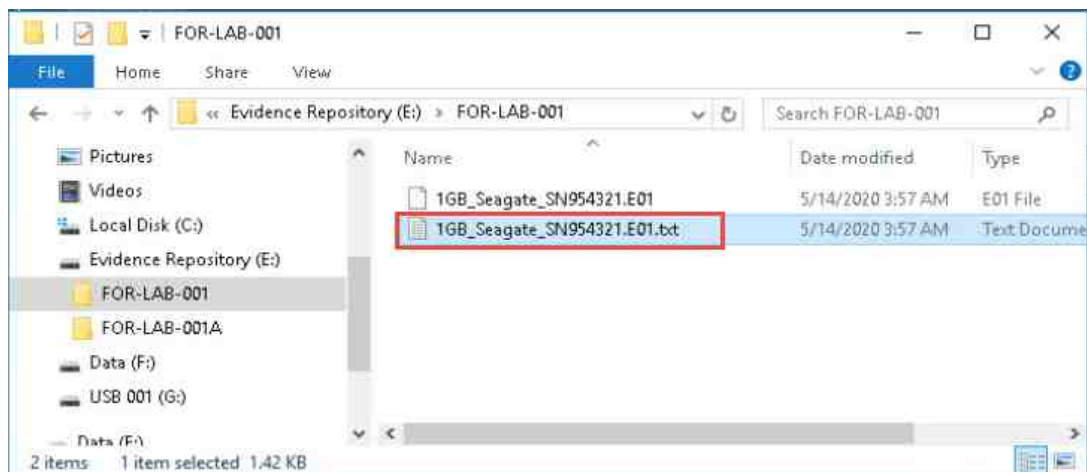
-) Verify the image process had no errors by reviewing the image report; and
-) Ensure that the content you captured is accessible.

Let us begin by reviewing the image report and checking for errors.

1. Open windows explorer and browse to Evidence Repository (E:) > FOR-LAB-001 as seen in items 1 and 2 below.



2. The folder will contain file(s) with the extension E01. Double-click the file named 1GB_Seagate_SN954321.E01.txt to open it in notepad. This is FTK Imager's image report file.



Ordinarily you would see several fragments of the imaged hard drive. This is determined by the defined Image fragment size, currently the default is 1500MB which is greater than the total capacity of the hard drive. So, one fragment was created.

3. The image report will look like the text box in the snapshots below.



The case information highlighted below is where you can see the information you typed about the image and verify whether the information was accurate.



```
1GB_Seagate_SN954321.E01.txt - Notepad
File Edit Format View Help
Created By: AccessData® FTK® Imager 4.3.0.18

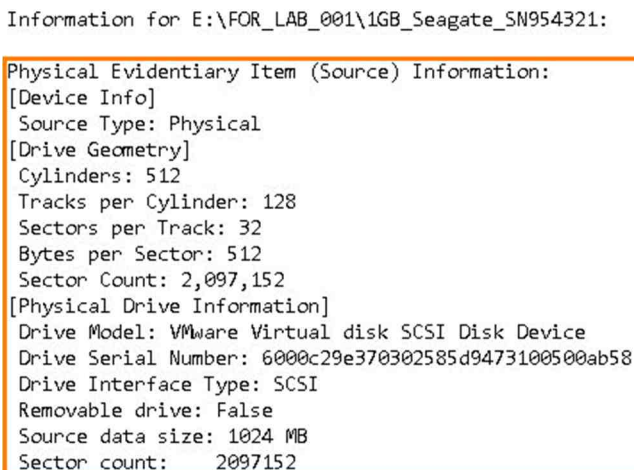
Case Information:
Acquired using: ADI4.3.0.18
Case Number: FOR_LAB_001
Evidence Number: 001
Unique description: Image os: 1GB Seagate HDD bearing S/n 954321
Examiner: Andrew A.
Notes: Hard drive seized from suspect's computer

-----

Information for E:\FOR_LAB_001\1GB_Seagate_SN954321:
```



The Image information category highlighted below is where you can determine how much data was imaged and review the Drive Model and Serial Number as well as the disk geometry information.



```
Information for E:\FOR_LAB_001\1GB_Seagate_SN954321:

Physical Evidentiary Item (Source) Information:
[Device Info]
Source Type: Physical
[Drive Geometry]
Cylinders: 512
Tracks per Cylinder: 128
Sectors per Track: 32
Bytes per Sector: 512
Sector Count: 2,097,152
[Physical Drive Information]
Drive Model: VMware Virtual disk SCSI Disk Device
Drive Serial Number: 6000c29e370302585d9473100500ab58
Drive Interface Type: SCSI
Removable drive: False
Source data size: 1024 MB
Sector count: 2097152
```



The Acquisition start and end times highlighted contain the times and the segment list to know the names and paths of all the segments created during the imaging process.

```
[Computed Hashes]
MD5 checksum: 41cf98f622791425f6aa8beddb714bd4
SHA1 checksum: a4e5e4f68176b103c025d6a91dd9ebe4e30fefe2
```

```
Image Information:
Acquisition started: Thu Oct 29 23:18:18 2020
Acquisition finished: Thu Oct 29 23:18:23 2020
Segment list:
E:\FOR_LAB_001\1GB_Seagate_SN954321.E01
```

```
Image Verification Results:
Verification started: Thu Oct 29 23:18:23 2020
Verification finished: Thu Oct 29 23:18:28 2020
MD5 checksum: 41cf98f622791425f6aa8beddb714bd4 : verified
SHA1 checksum: a4e5e4f68176b103c025d6a91dd9ebe4e30fefe2 : verified
```



The Computed Hashes information and the image verification results highlighted allow you to Compare the hashes from the computed hashes data with the verification results to determine if they match.

```
[Computed Hashes]
MD5 checksum: 41cf98f622791425f6aa8beddb714bd4
SHA1 checksum: a4e5e4f68176b103c025d6a91dd9ebe4e30fefe2
```

```
Image Information:
Acquisition started: Thu Oct 29 23:18:18 2020
Acquisition finished: Thu Oct 29 23:18:23 2020
Segment list:
E:\FOR_LAB_001\1GB_Seagate_SN954321.E01
```

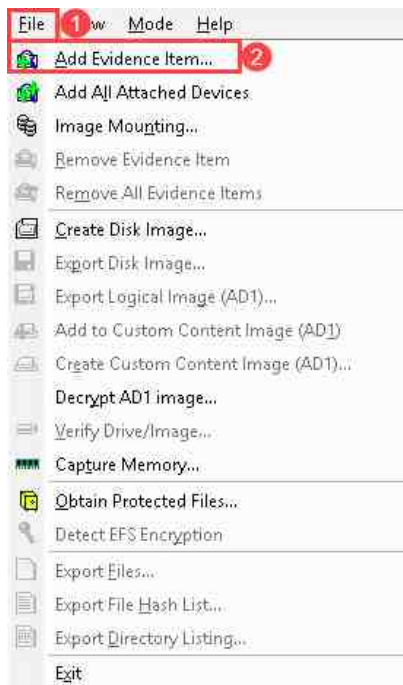
```
Image Verification Results:
Verification started: Thu Oct 29 23:18:23 2020
Verification finished: Thu Oct 29 23:18:28 2020
MD5 checksum: 41cf98f622791425f6aa8beddb714bd4 : verified
SHA1 checksum: a4e5e4f68176b103c025d6a91dd9ebe4e30fefe2 : verified
```

4. Once you have verified that the report seems accurate, proceed to the image report for the logical image labeled FOR-LAB-001A located at E:\FOR-LAB-001A and perform the same review.

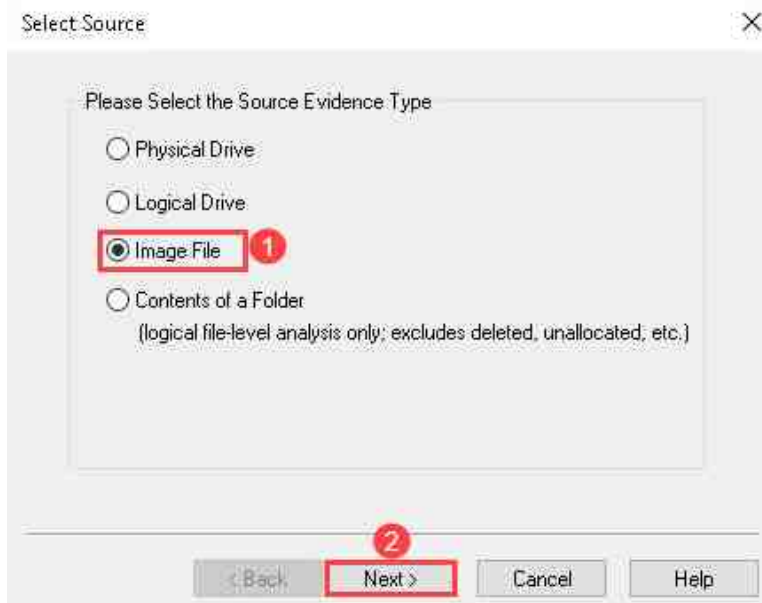
5 Verify the Image Contents by Opening the Image in FTK Imager

Great, you are here! Since you can verify that the reports look good, let us try to open each image and see if the file systems are recognized. Let us start with the physical image.

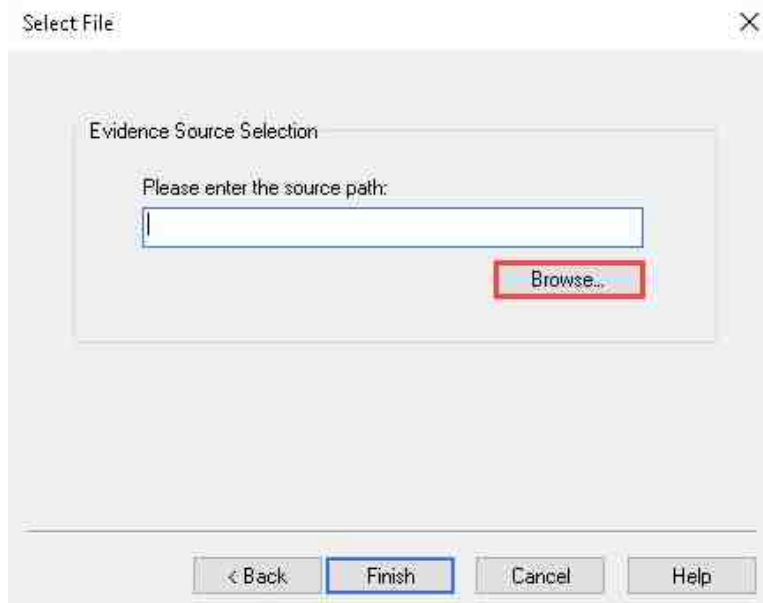
1. Let us go back to FTK Imager and select the options File > Add Evidence Item, as seen in items 1 and 2, to open the Select Source window.



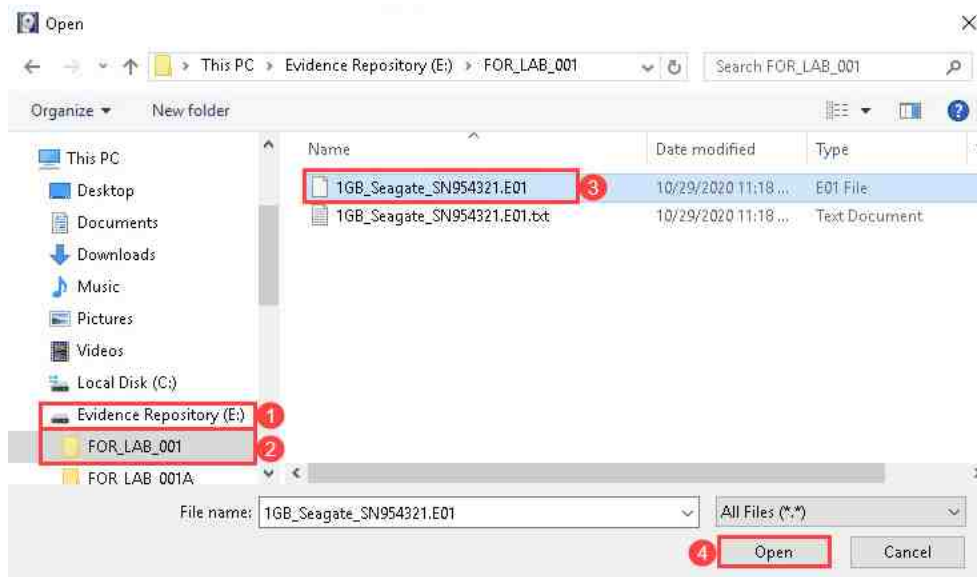
2. This time, select the Image File radio button and then select Next, as seen in items 1 and 2, to proceed to the Select File window.



- The Select File window will allow you to choose the image you want to open. Click the Browse button highlighted below. This will open the File Selection window, which will allow you to browse to the appropriate image file.

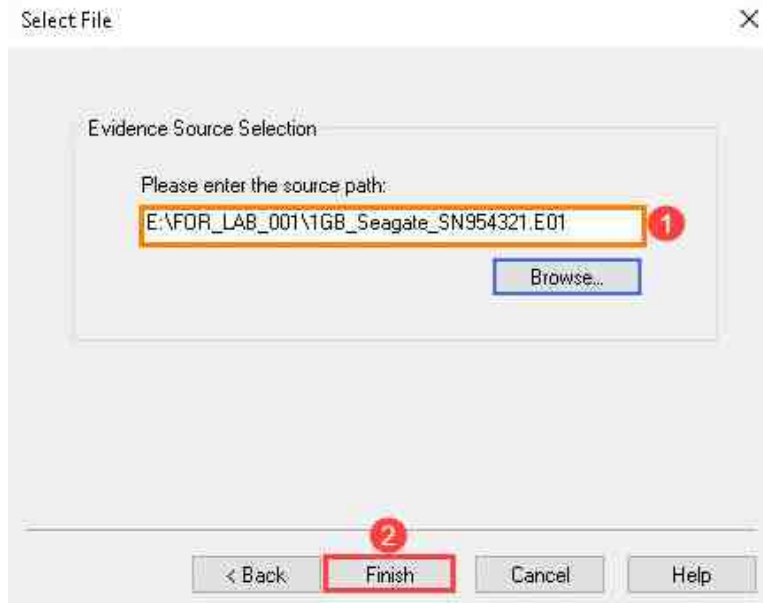


- In the Select File window, browse to Evidence Repository (E:) > FOR-LAB-001 and select the image file called 1GB_Seagate_SN954321.E01 as seen in items 1, 2, and 3 below. Once the image is selected, click Open as seen in item 4 below.

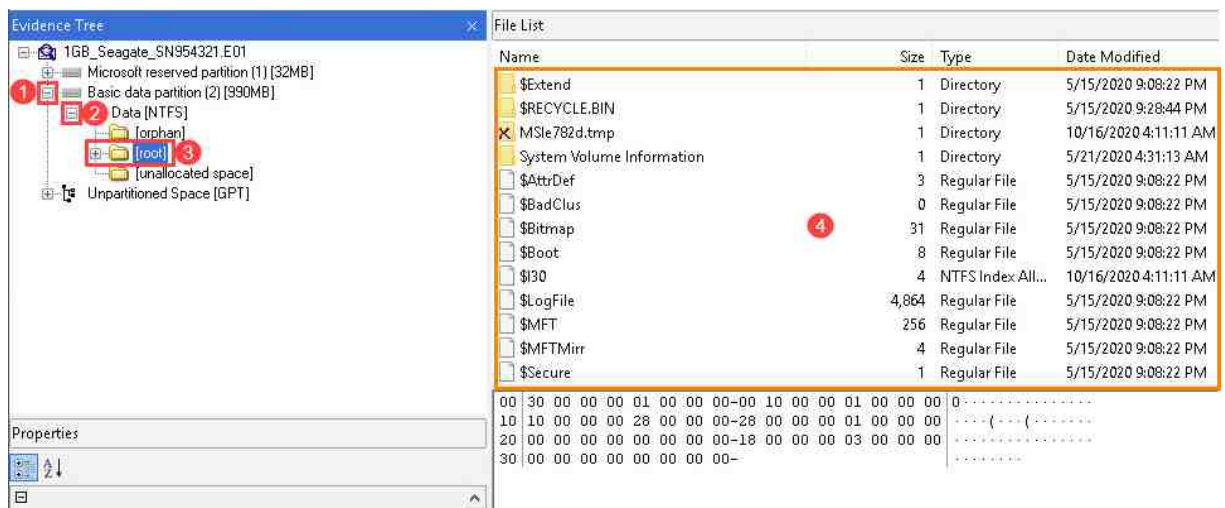


If multiple image fragments were created during the imaging process, FTK Imager will automatically add the remaining files when loading.

5. Once you are back to the Select File window, verify that the path of the selected file matches the one highlighted in item 1 below. Once you have verified, click the Finish button highlighted in item 2. This will take you to the main GUI, where the image will be loaded in the Evidence Tree Pane.



6. In the Evidence Tree pane, click the + signs beside 1GB_Seagate_SN954321.E01, as seen in item 1 below. This will expand and reveal the partitions of the drive. Next, click the + sign beside Basic data partition (2) as highlighted in item 2 below. This will expand and reveal the file system and the volume name, Data. Now click the + sign beside Data, as seen in item 3, to reveal the root, orphan, and unallocated directories. The root directory is the main directory on the partition, and all other directories and files on the volume will appear under root. The orphan folder contains deleted orphaned files, and the unallocated space folder contains unallocated space represented as files. The folder we are currently interested in is root. Click the folder called root, as seen in item 4, to expand it and see the files that are on the volume in the File List pane seen in item 5.



The hard drive imaged in this lab will not contain any user created files but feel free to browse the file structure.

7. If you can open the root directory and view its contents, then it means the image was successfully created and can be opened without issues. Repeat these steps to view the contents of the logical image stored in the folder named FOR-LAB-001A.

8. You have now successfully created and verified two digital forensic images and are ready to move on to the next phase on the chain-of-custody.
9. The lab is now complete. Please close all open programs by clicking the X at the top-right corner of the windows, as highlighted below.