Division of Information Technology & Sciences
Department of Computer & Digital Forensics
FOR 120– Introduction to Digital Forensic Analysis

Physical vs Logical Image

Overview:

The lab consists of four tasks. The tasks will teach you the difference between physical and logical forensic images. The tasks will also teach you the correct steps for acquiring a physical or logical image using FTK Imager.

Notes:

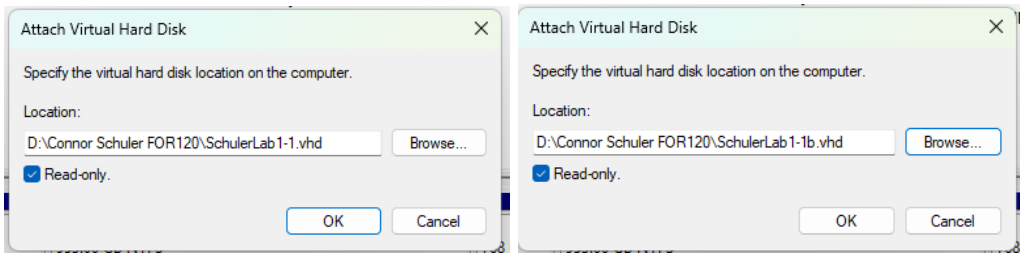
1. You are required to provide screenshots of any step performed during the Lab. Screenshots should clearly show any step used and its results. This could be done using a tool such as the “Snip and Sketch” tool, to highlight your work.
2. A thorough explanation and analysis are required to demonstrate your understanding of all steps that you performed.
3. Submission rules: please submit all answers to canvas.
4. Make sure to always report the image verification results.

Required Tools: FTK Imager
** The images created in this lab will be used in later assignments, so please remember where they are stored so you do not repeat the steps again.

TASK #1 – CREATING A PHYSICAL FORENSIC IMAGES

1. Attach the VHD files that were created in the first lab

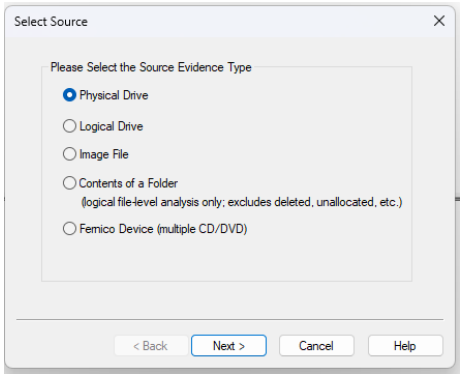
Images show two VHDs being attached, it specifies the paths of the VHDs as on the D: drive is a folder called "Connor Schuler FOR-120."

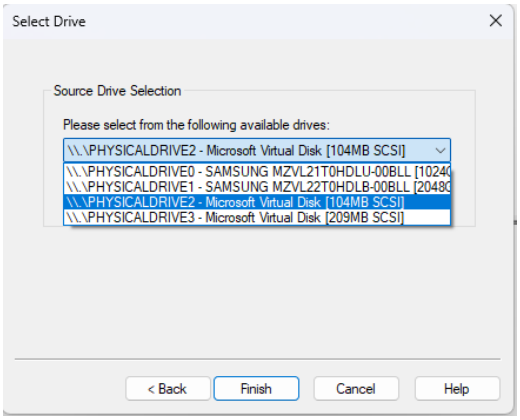


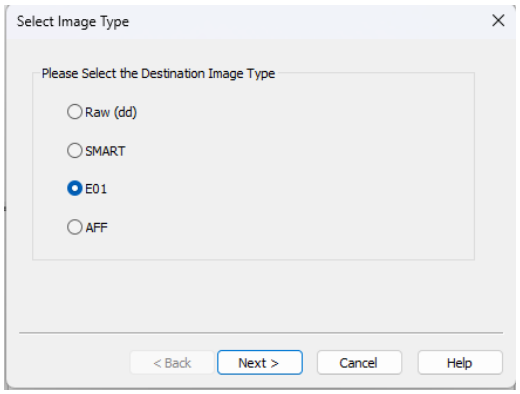
2. Create an E01 physical image of evidence #1 VHD

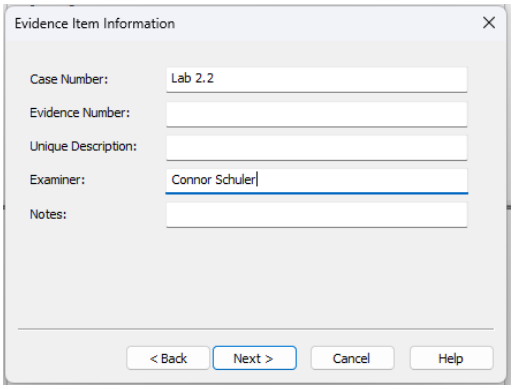
Images (in order) show:

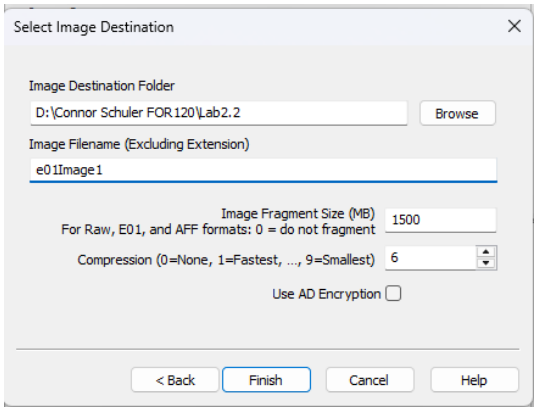
- **Physical drive image**
- **Selected physical drive of 104MB Drive 2**
- **Image type E01**
- **Case number and examiner**
- **Image destination of e01Image1 in folder Lab2.2**
- **Successful image creation**
- **Image hash validation**

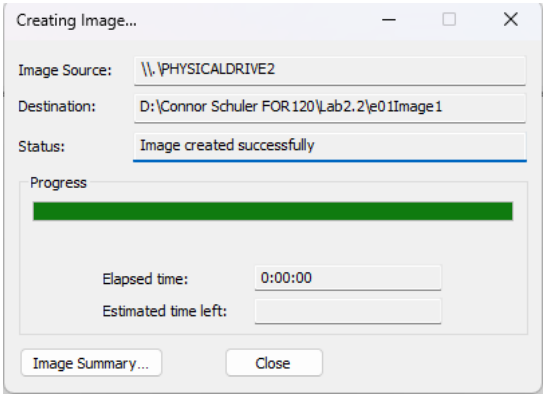

Select Source
Please Select the Source Evidence Type
Physical Drive
Logical Drive
Image File
Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
Femico Device (multiple CD/DVD)
< Back
Next >
Cancel
Help

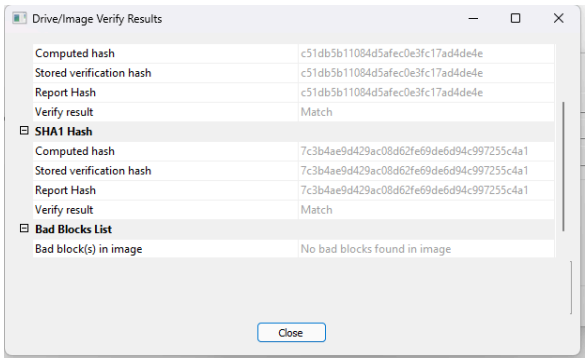

Select Drive
Source Drive Selection
Please select from the following available drives:
\\.\PHYSICALDRIVE2 - Microsoft Virtual Disk [104MB SCSI]
\\.\PHYSICALDRIVE0 - SAMSUNG MZVL21T0HDLU-00BLL [1024
\\.\PHYSICALDRIVE1 - SAMSUNG MZVL22T0HDLB-00BLL [2048
\\.\PHYSICALDRIVE2 - Microsoft Virtual Disk [104MB SCSI]
\\.\PHYSICALDRIVE3 - Microsoft Virtual Disk [209MB SCSI]
< Back
Finish
Cancel
Help


Select Image Type
Please Select the Destination Image Type
Raw (dd)
SMART
E01
AFF
< Back
Next >
Cancel
Help


Evidence Item Information
Case Number:
Lab 2.2
Evidence Number:
Unique Description:
Examiner:
Connor Schuler
Notes:
< Back
Next >
Cancel
Help

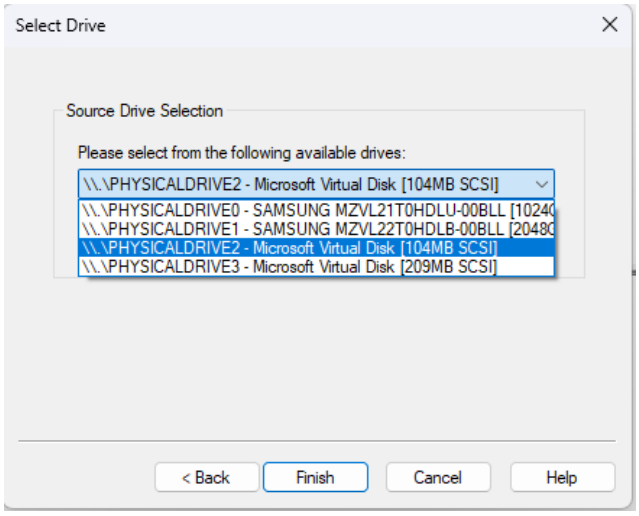

Select Image Destination
Image Destination Folder
D:\Connor Schuler FOR120\Lab2.2
Browse
Image Filename (Excluding Extension)
e01Image1
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment
1500
Compression (0=None, 1=Fastest, ..., 9=Smallest)
6
Use AD Encryption
< Back
Finish
Cancel
Help


Creating Image...
Image Source:
\\.\PHYSICALDRIVE2
Destination:
D:\Connor Schuler FOR120\Lab2.2\e01Image1
Status:
Image created successfully
Progress
Elapsed time:
0:00:00
Estimated time left:
Image Summary...
Close


Drive/Image Verify Results
Computed hash
c51db5b11084d5afec0e3fc17ad4de4e
Stored verification hash
c51db5b11084d5afec0e3fc17ad4de4e
Report Hash
c51db5b11084d5afec0e3fc17ad4de4e
Verify result
Match
SHA1 Hash
Computed hash
7c3b4ae9d429ac08d62fe69de6d94c997255c4a1
Stored verification hash
7c3b4ae9d429ac08d62fe69de6d94c997255c4a1
Report Hash
7c3b4ae9d429ac08d62fe69de6d94c997255c4a1
Verify result
Match
Bad Blocks List
Bad block(s) in image
No bad blocks found in image
Close

3. While you are going through the imaging steps, what types of information does FTK Imager provide about each disk?

- **Drive number**
- **Disk type/brand**
- **Disk size and interface**

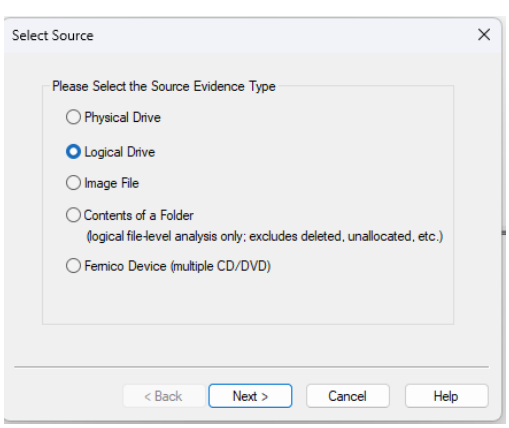


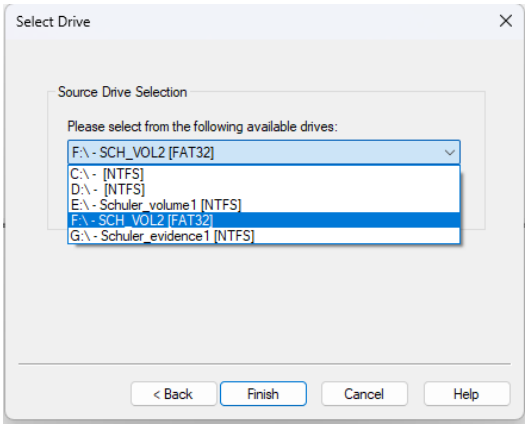
TASK #2 – CREATING LOGICAL FORENSIC IMAGES

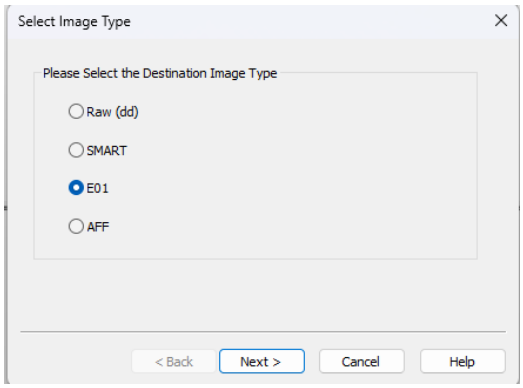
1. Create an E01 logical image of the second volume of evidence #2 VHD

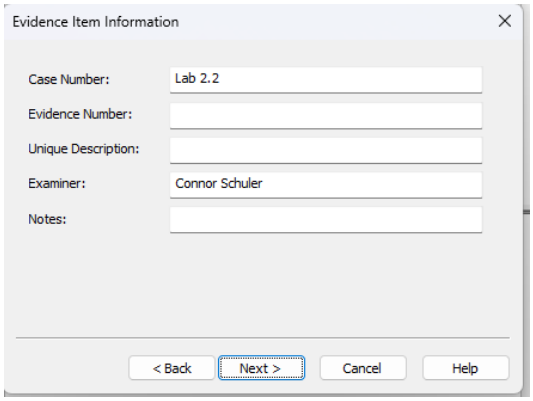
Images (in order) show:

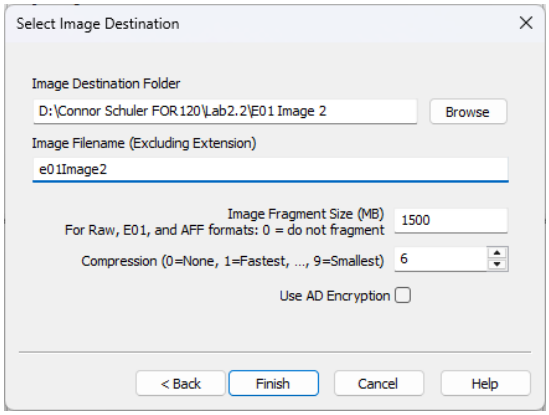
- **Logical drive image**
- **Selected logical drive of SCH_VOL2, FAT32 mounted as F:**
- **Image type E01**
- **Case number and examiner**
- **Image destination of e01Image2 in folder Lab2.2**
- **Successful image creation**
- **Image hash validation**

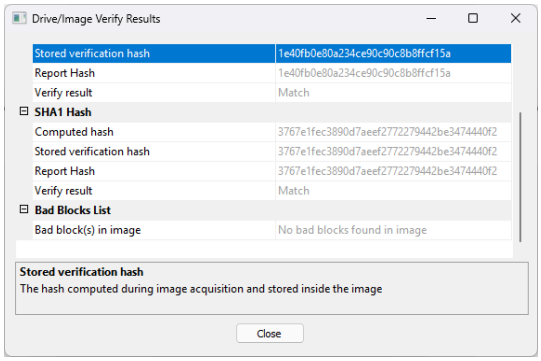






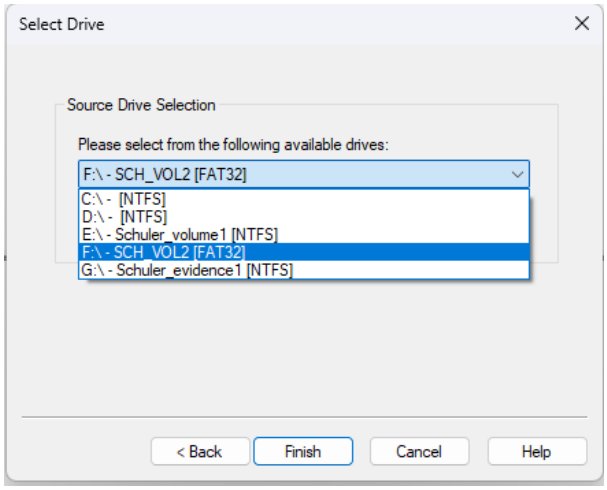






2. What are the available volumes and their info in your system?

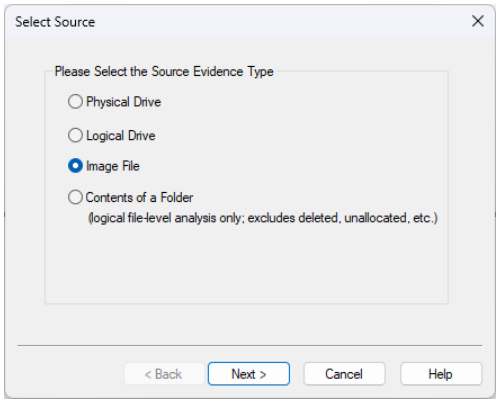
- **C:\ (NTFS)**
- **D:\ (NTFS)**
- **E:\ (NTFS)**
- **F:\ (FAT32)**
- **G:\ (NTFS)**

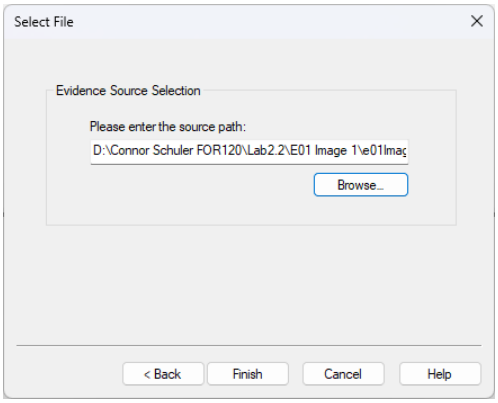


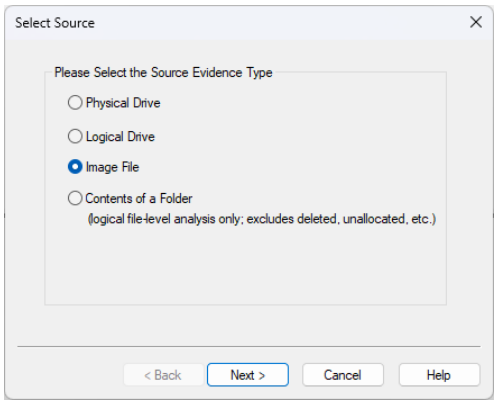
TASK #3 – COMPARING THE IMAGES

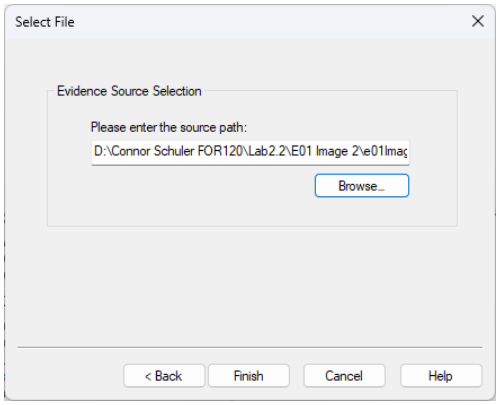
1. Add the two created images (physical and logical) to FTK Imager

Images shows two E01 images being added to FTK Imager. One in the folder "Lab2.2\E01 Image 1" and another in "Lab2.2\E01 Image 2".









2. Expand each of the images, and talk about the differences between them

The physical image shows partitions and volume sizes. It also has a section for orphaned files, but that might be a feature of NTFS. The logical image does not show file sizes, while the physical image does show that information.

3. What does a physical image allow you to see that you can not see in a logical image?

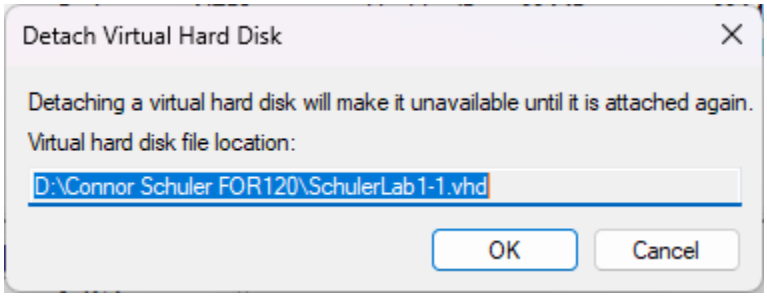
Physical images show partitions and volumes, while logical images only show a specific partition or volume. Physical images will also show unpartitioned space.

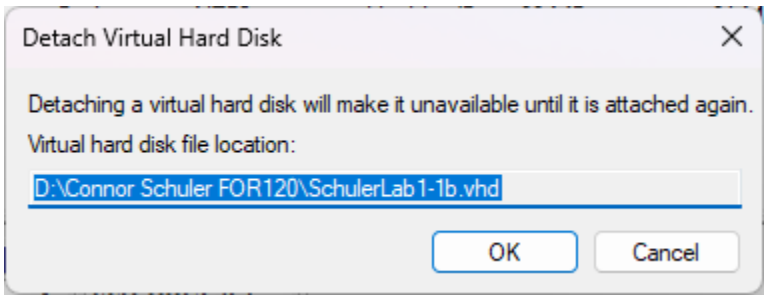
4. What is the difference between unpartitioned space and unallocated (free) space?

Unpartitioned space is raw disk space not assigned to any partition or drive letter, making it unusable for file storage. On the other hand, free space is unused capacity within an existing partition that could be used for file storage.

5. Close FTK Imager and detach the two VHDs that you have attached

Images show both VHDs being detached.





Task #4 – Reflect on what you learned in this lab

This lab showed me the different types of images that can be taken, their similarities and differences, and ways to look at them in FTK imager.