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

Image Formats

Overview:

The lab consists of four tasks. The objective of this lab is to learn how to acquire a digital forensic image of a disk drive. The lab tasks focus on creating forensic images of different types, including dd and E01 formats.

Notes:

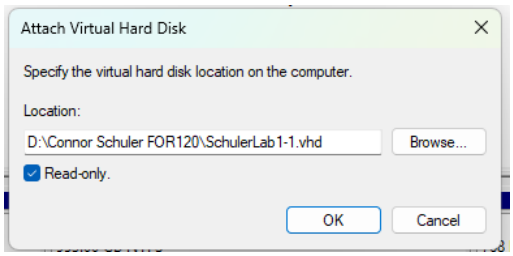
1. You are required to provide screenshots of any step performed during the Lab. Screenshots should clearly show any step used and its results. This could be done using a tool such as the “Snip and Sketch” tool, to highlight your work.
2. A thorough explanation and analysis are required to demonstrate 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.

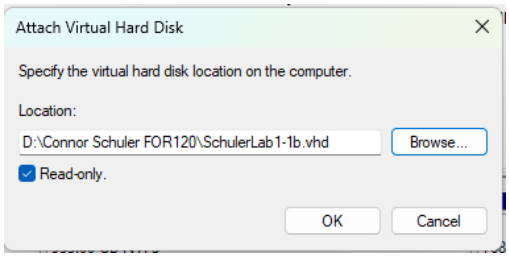
Required Tools: FTK Imager

Task #1 – Attach the VHD files

1. Attach the VHD files that were created in the previous 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."



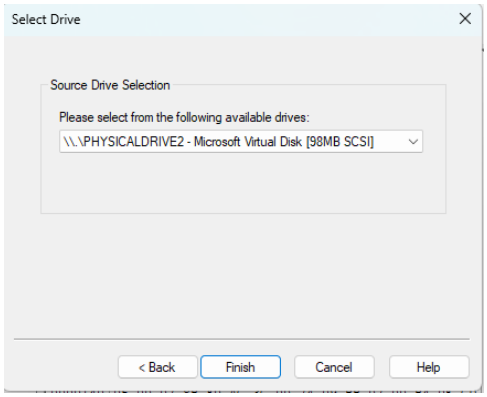


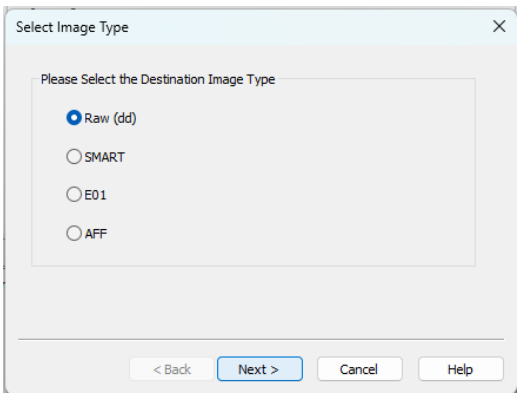
Task #2 – Acquire a dd image

Please read all steps before starting the acquisition

1. Use the FTK imager to create a **dd** physical forensic image from evidence #1 VHD.

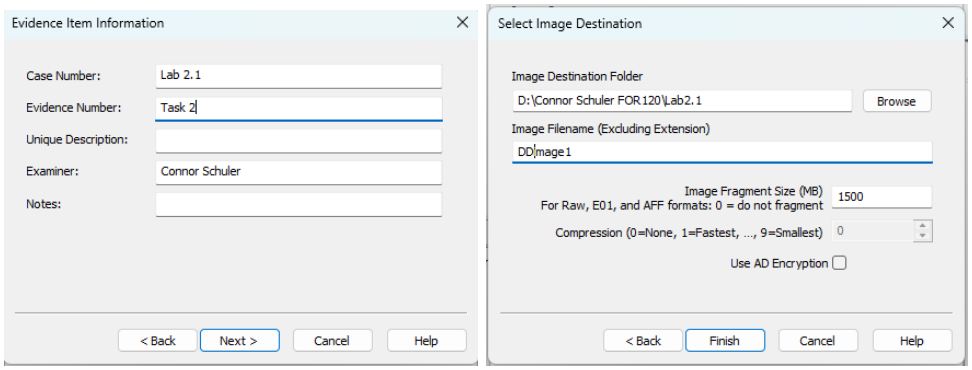
Images show physical drive 2 being selected, and the image as Raw/dd.





2. What are the available options that you can apply to a **dd** image?

Case number, evidence number, unique description, examiner, notes, image name/path, AD encryption, and image fragment size.



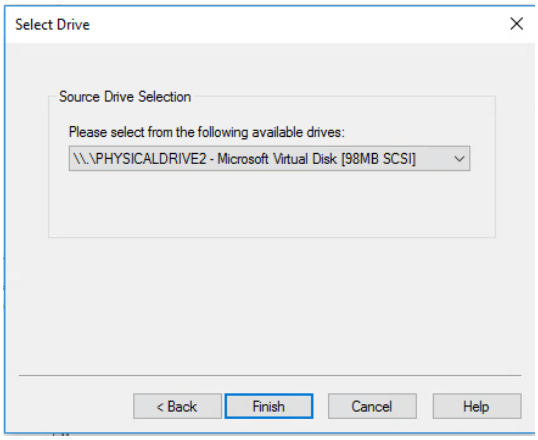
3. Make sure to submit the verification of the imaging, which means that the acquisition was done successfully without errors.

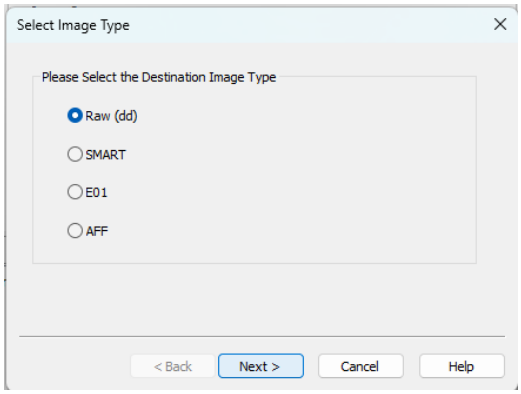
Image shows file hashes for image.

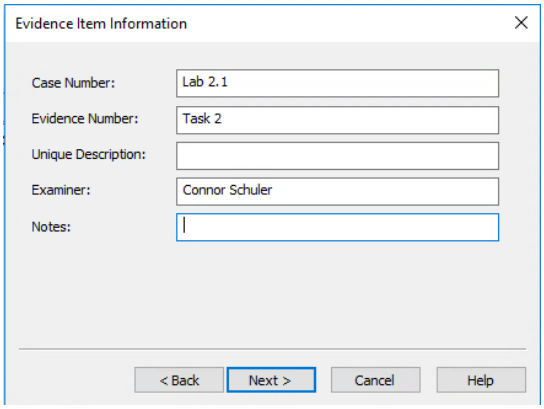
```
[Computed Hashes]
 MD5 checksum:    c51db5b11084d5afec0e3fc17ad4de4e
 SHA1 checksum:   7c3b4ae9d429ac08d62fe69de6d94c997255c4a1

Image Information:
 Acquisition started:   Tue Jan 20 13:57:02 2026
 Acquisition finished:  Tue Jan 20 13:57:02 2026
 Segment list:
  D:\Connor Schuler FOR120\Lab2.1\DDimage1.001
 COMPUTED HASH :  c51db5b11084d5afec0e3fc17ad4de4e
 COMPUTED HASH :  7c3b4ae9d429ac08d62fe69de6d94c997255c4a1

Image Verification Results:
 Verification started:  Tue Jan 20 13:57:02 2026
 Verification finished: Tue Jan 20 13:57:03 2026
 MD5 checksum:    c51db5b11084d5afec0e3fc17ad4de4e : verified
 SHA1 checksum:   7c3b4ae9d429ac08d62fe69de6d94c997255c4a1 : verified
```

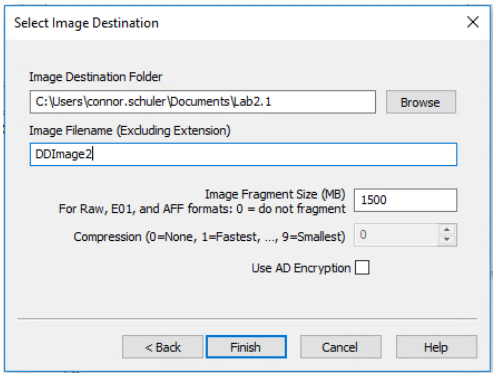
4. Create another dd image from the evidence #1 VHD.

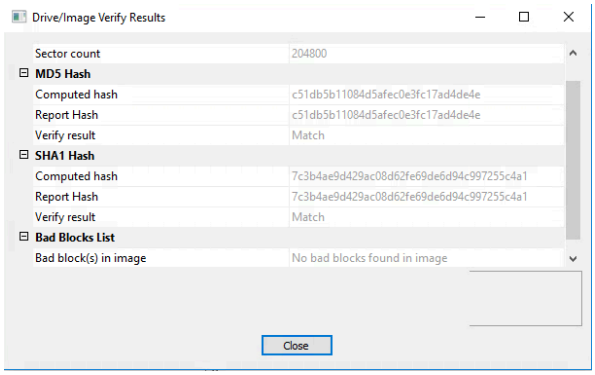
Images show physical drive 2 being selected, and the image as Raw/dd. Then basic case/evidence information and a name/location. Final image shows the hash of the image.









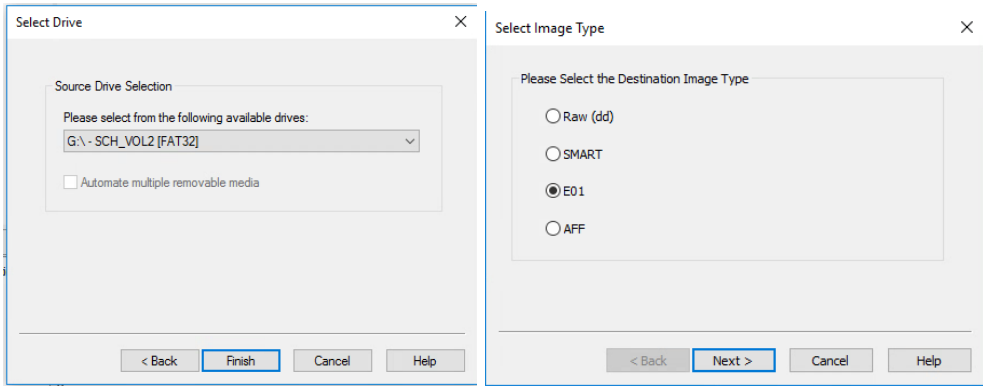


TASK #3 – ACQUIRE AN E01 IMAGE

Please read all five steps before starting the acquisition

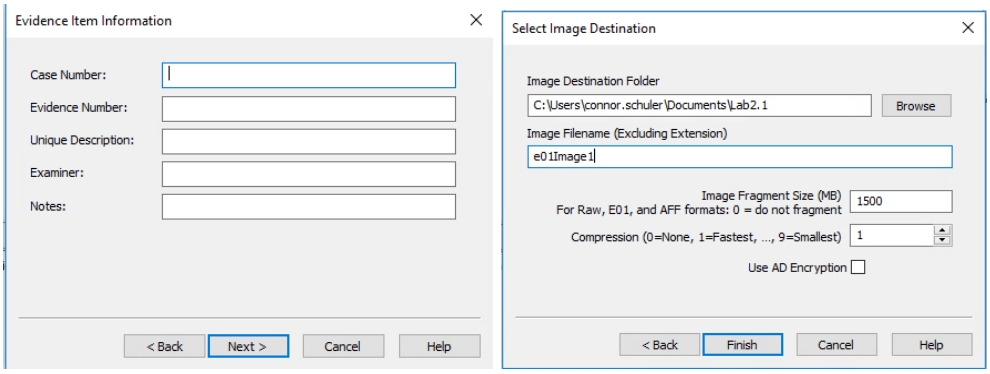
1. Use the FTK imager to create an **E01** logical forensic image from the FAT32 volume on evidence #2 VHD.

Images show the FAT32 volume being selected, and the image as E01.



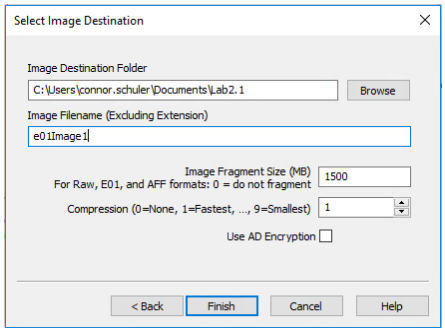
2. What are the available options that you can apply to an **E01** image before the acquisition?

Case number, evidence number, unique description, examiner, notes, image name/path, AD encryption, compression level, and image fragment size.



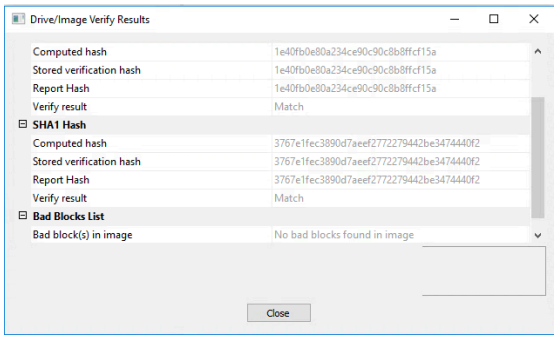
3. Use compression (recommend level 1)

Image shows compression set to 1.,



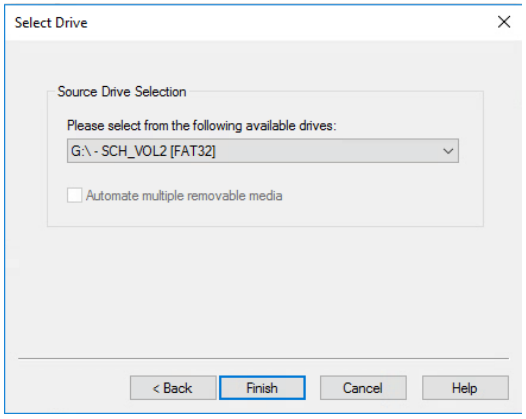
4. Make sure to submit the verification of the imaging, which means that the acquisition was done successfully without errors.

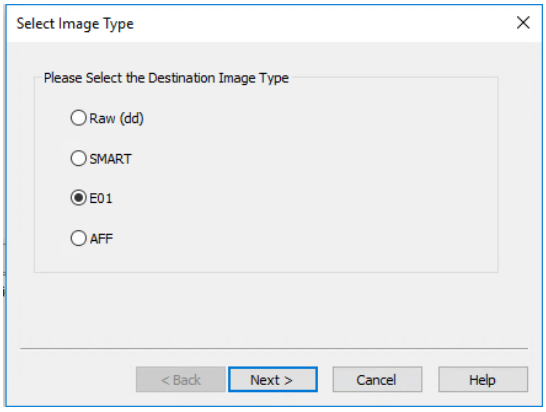
Image shows hashes of E01 image, and no bad blocks in the image.

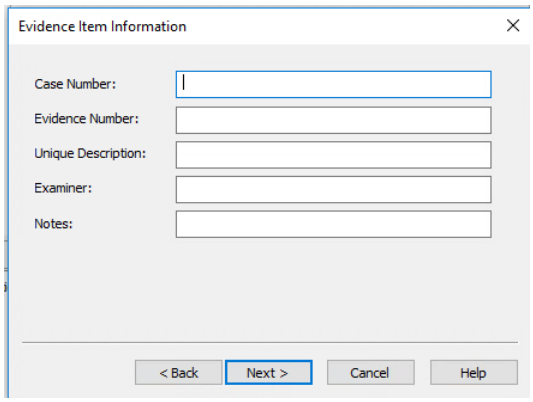


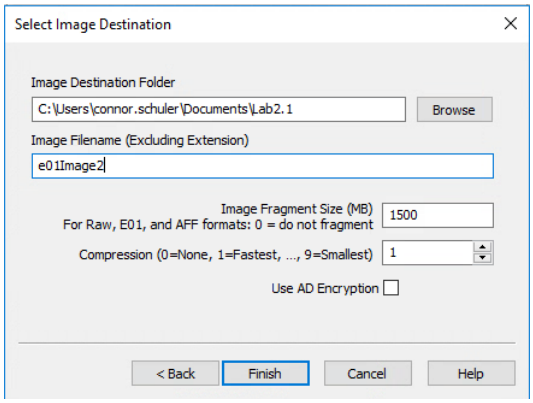
5. Create another E01 image from the FAT32 volume using the same configurations you used for the first E01 image.

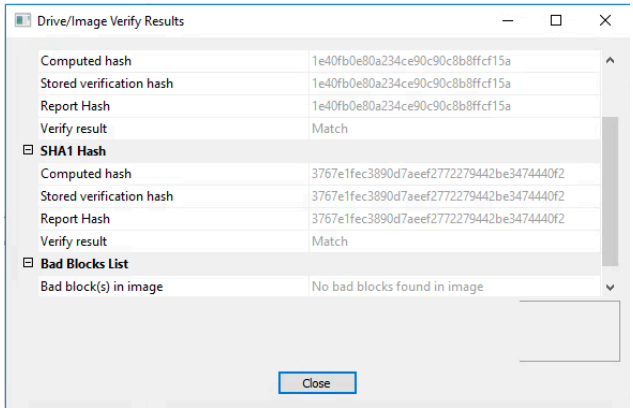
Images show the FAT32 volume being selected, and the image as E01. Then no case information, an image name on e01Image2 in the Lab2.1 folder in documents. The final image shows the validated hash.







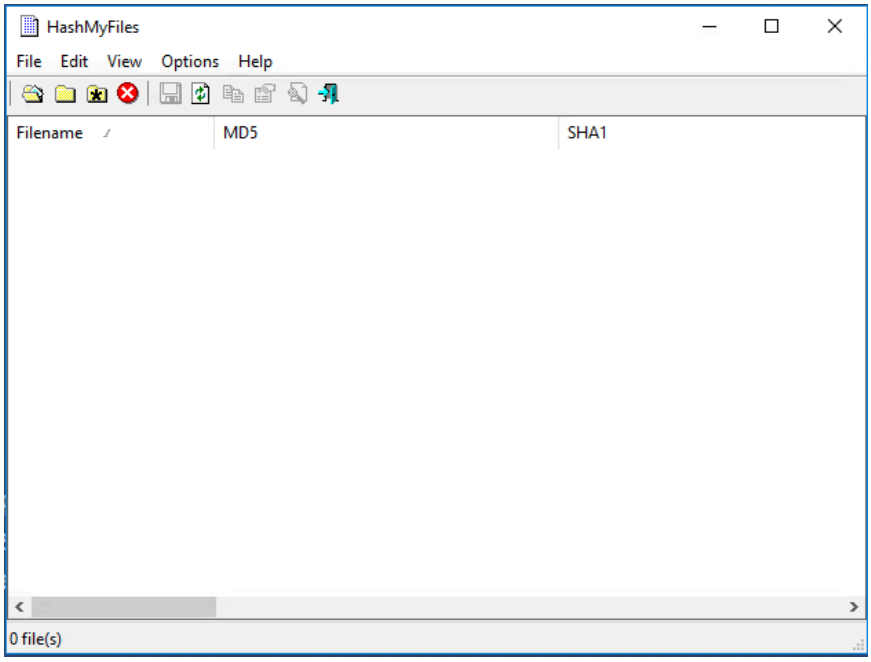




TASK #4 – IMAGE VERIFICATION

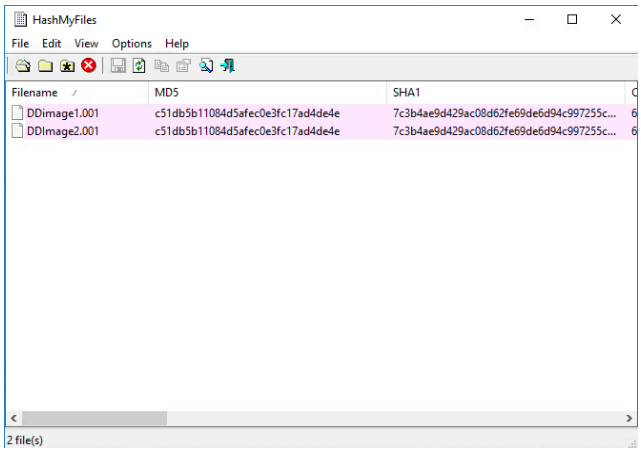
1. Download HashMyFiles tool.

Image shows the HashMyFiles program open and running.



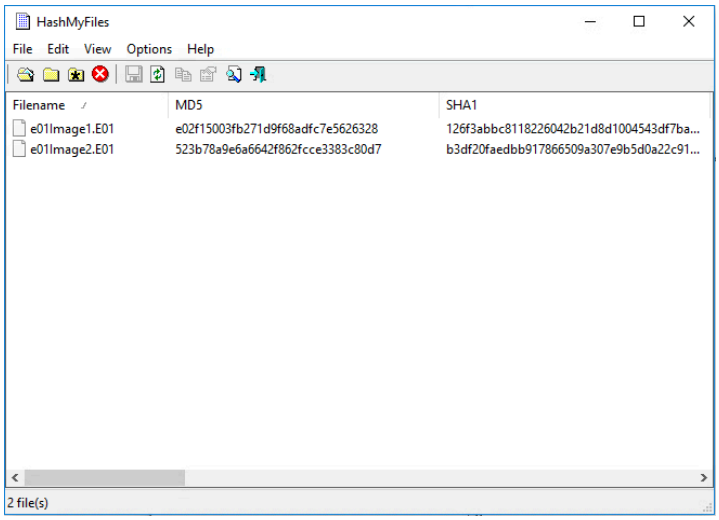
2. Compare the hashes of the two dd images that you created in task #2, are they the same? Why or why not?

They are the same, because they are direct bit for bit copies of the same drive/volume with no attached metadata.



3. Compare the hashes of the two E01 images that you created in task #3, are they the same? Why or why not?

They are not the same, because E01 images store additional metadata within the E01 container. This means that the files have the same image, but have different hashes.

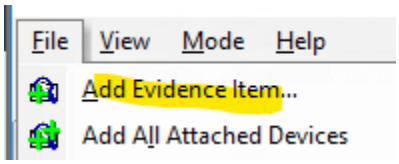


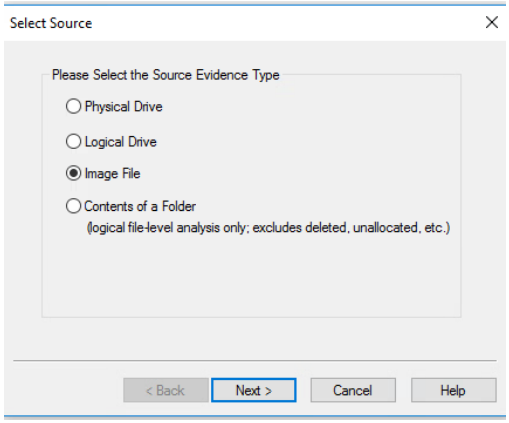
4. How can we verify if two E01 images are the same?

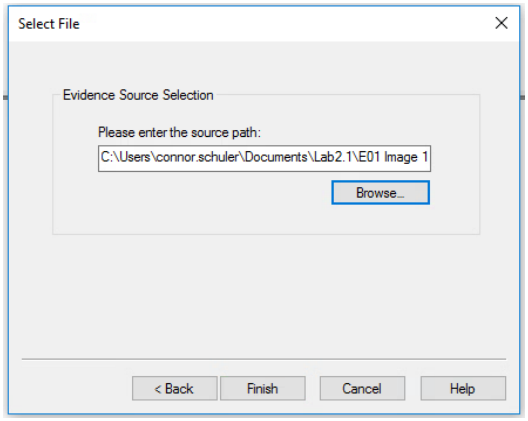
Import image into FTK Imager and verify image.

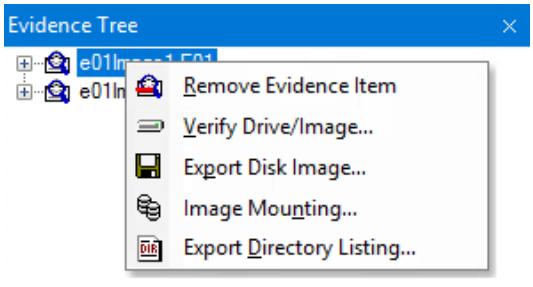
E01 Image 1:

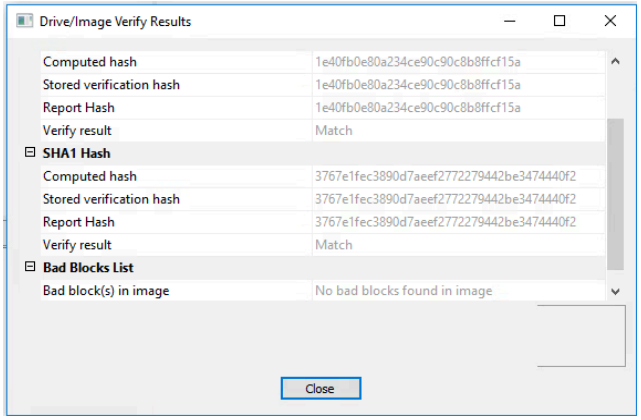
Images show the E01 Image 1 being imported and verified.





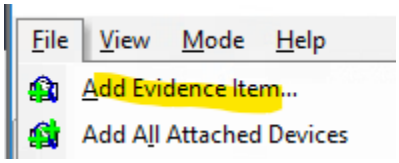


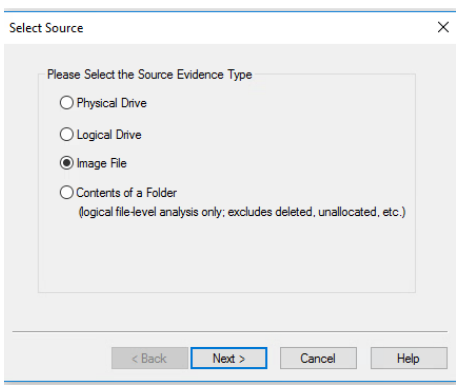


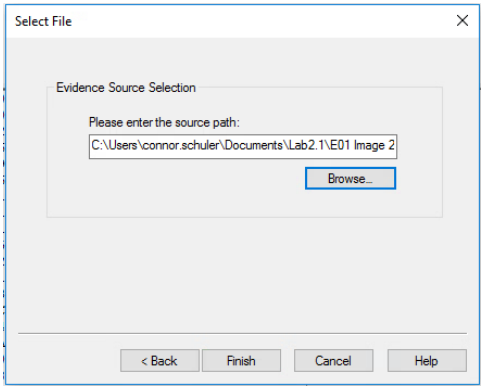


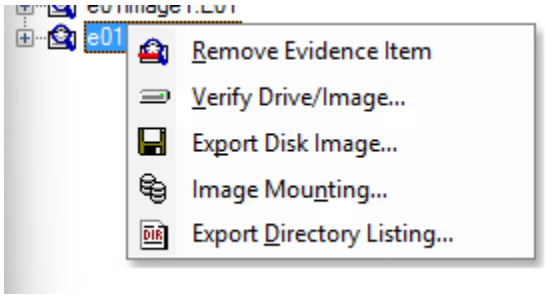
E01 Image 2:

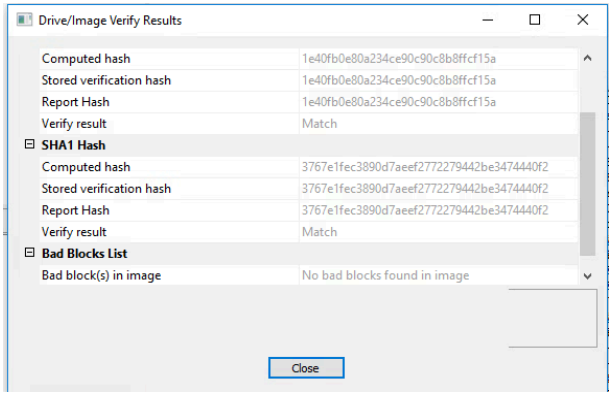
Images show the E01 Image 2 being imported and verified. The reported and computed hashes match E01 Image 1.





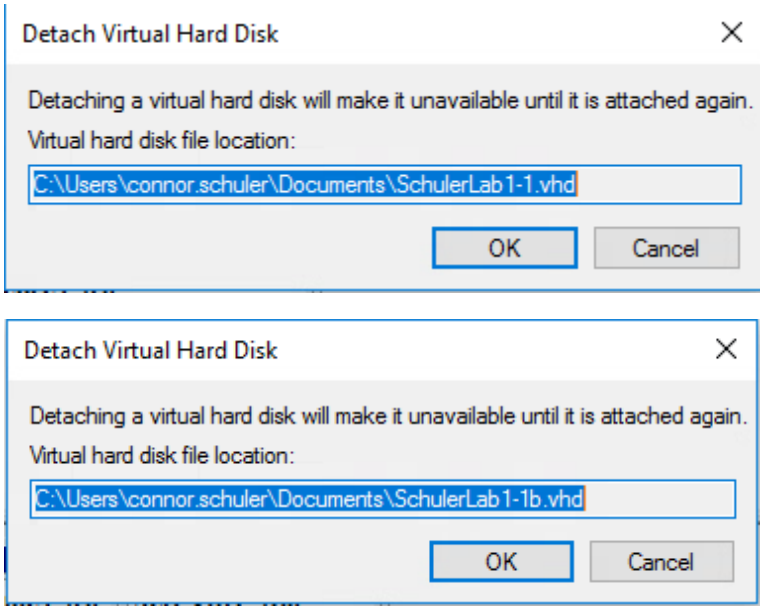






** Remember to detach the VHD files when you finish the lab :)

Images show two VHDs being detached.



TASK #5 – REFLECT ON WHAT YOU LEARNED IN THIS LAB

This lab demonstrated that DD images will have the same hash, but E01 images will not because of additional metadata stored in the file. It also showed me how to validate both E01 and dd images.

IMPORTANT

Remember that VHD files are a virtual representation of Hard Disks, we use them to simulate a real hard disk drive. For testing purposes, it is easier to deal with VHDs than real disks.