ITIS 4250 / 5250

Pooja Haridasyam

Lab # 1

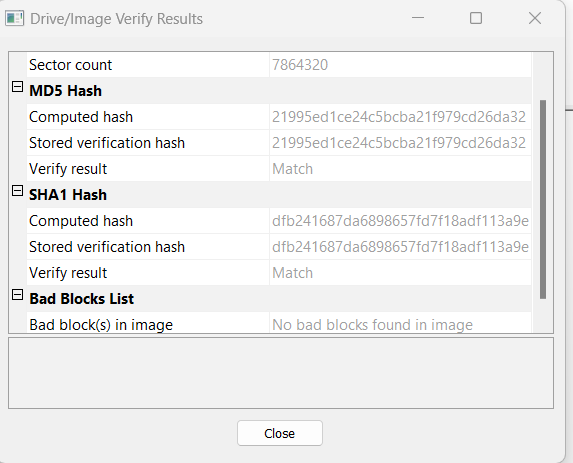
Feb 13th, 2023

**Overview:**

For this lab, I've used "CoffeeShopper" file to verify a forensics image provided by the Cybersecurity Center. I must utilize the "FTK Imager" tool to extract information from the file, including the MD5 hash value, the file systems included in the picture, and the size of the original drive, in order to prepare a forensic report.

**Forensic Acquisition & Exam Preparation:**

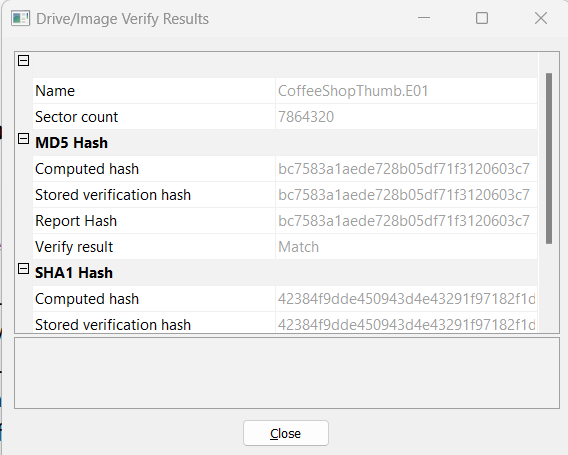
Through canvas, I was able to access the Forensic image in the network's Shared Folder. FTK Imager 4.7.1.2 is the program used to retrieve and extract data from the image. After gaining access to the picture file, the Hash verification process was started. The image's MD5 hash is seen in the image below:



**Findings and Report (Forensic Analysis):**

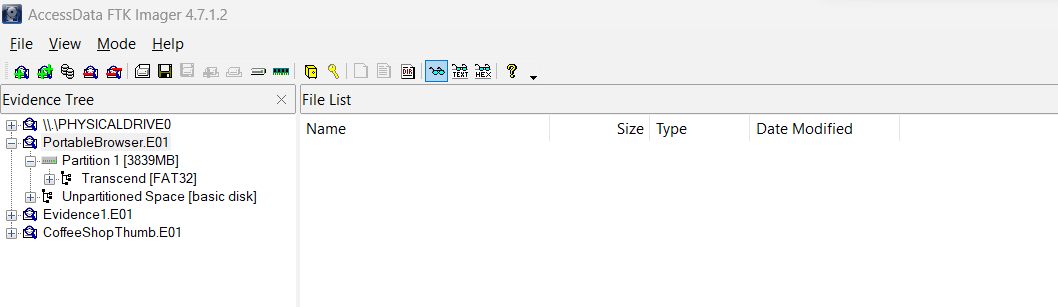
**a. What was the MD5 hash value for PortableBrowser.e01? How about CoffeeShopper?**

I have added E01 file to the FTK Imager using the "Add Evidence Item" option from the File Menu. After the Image was loaded, I selected "Verify Drive/Image" option by right clicking on the "PortableBrowser. E01" under the Evidence Tree in the left pane of the software. The MD5 Hash value that was calculated by the FTK Imager as shown in the image on the next page is: 21995ed1ce24c5bcba21f979cd26da32 and MD5 Hash value for “CoffeeShopper” is bc7583a1aede728b05df71f3120603c7.



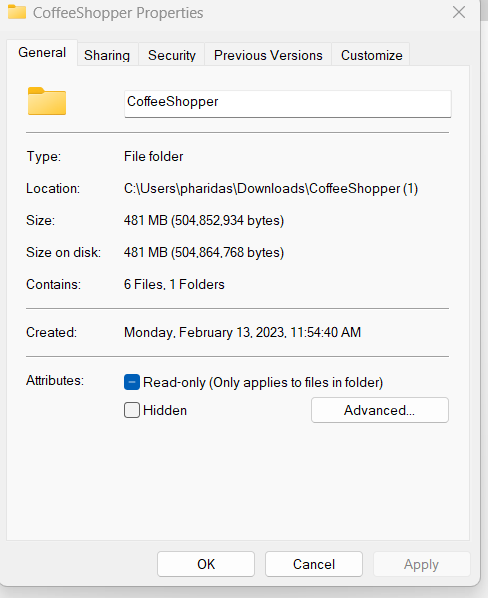
**b. What file systems are present within PortableBrowser.e01? (FAT32, NTFS, EXT3, Reiser, ZFS, UDF etc)**

The File systems present in PortableBrowser.E01 is FAT32. It is the only partition in Portable Browser.



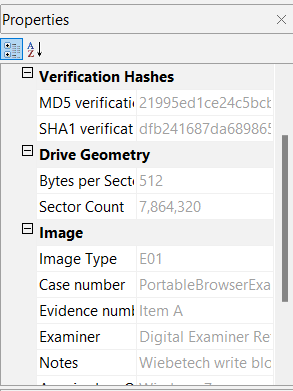
**c. What are the file size for PortableBrowser.e01 and CoffeeShopper.e01, and what was the size of the original device (hard drive) that PortableBrowser.e01 is imaged from? How about CoffeeShopper?**

The file size for the CoffeeShopper file is **504,852,934** bytes. I found the size by viewing properties of the file.



The file size for the “PortableBrowser” is **4,026,531,840** bytes. I found this by counting the total number of sectors and dividing it by the number of bytes in each sector. When I chose "Properties" from the "View" Menu, I found this information in the "Drive Geometry" section.

7,864,320 \* 512 bytes = **4,026,531,840 bytes**



**d. How are an image and a physical drive different as they appear in FTK Imager? (specifically about the details of their appearance/labeling in FTK Imager)?**

In FTK Imager, both an image and a physical drive will appear as a device or logical unit under the "Evidence" section in the main interface. However, there are some differences in the way they appear and are labeled:

* Image: An image file in FTK Imager will appear with the label "Image File" and the path to the image file. The image file will contain all the data from a previously acquired and saved disk or drive, and FTK Imager will treat it as a virtual representation of the original evidence.
* Physical Drive: A physical drive connected to the computer running FTK Imager will appear with the label "Local Physical Device" and the assigned drive letter or identifier. The physical drive represents the actual physical disk and FTK Imager will access it directly to gather information and make an acquisition.

The main difference between an image and a physical drive in FTK Imager is the way they are represented and labeled in the interface, with an image appearing as a file and a physical drive appearing as a device.

**e. Did FTK imager generate a log for the image you created out of PortableBrowser? Does this hash value match the original?**

Yes, FTK Imager generates a log file when you create an image of a disk or drive, including a PortableBrowser. The log file contains details about the imaging process, such as the start and end time, the source and destination of the image, and any error messages that may have occurred.

The hash value for the image created from the PortableBrowser is **21995ed1ce24c5bcba21f979cd26da32.** And the hash value for the original is **21995ed1ce24c5bcba21f979cd26da32.** From this we can say that the hash values match.

**f. Do PortableBrowser and CoffeeShopper appear to be the same thumb drive? How are they similar and how are they different?**

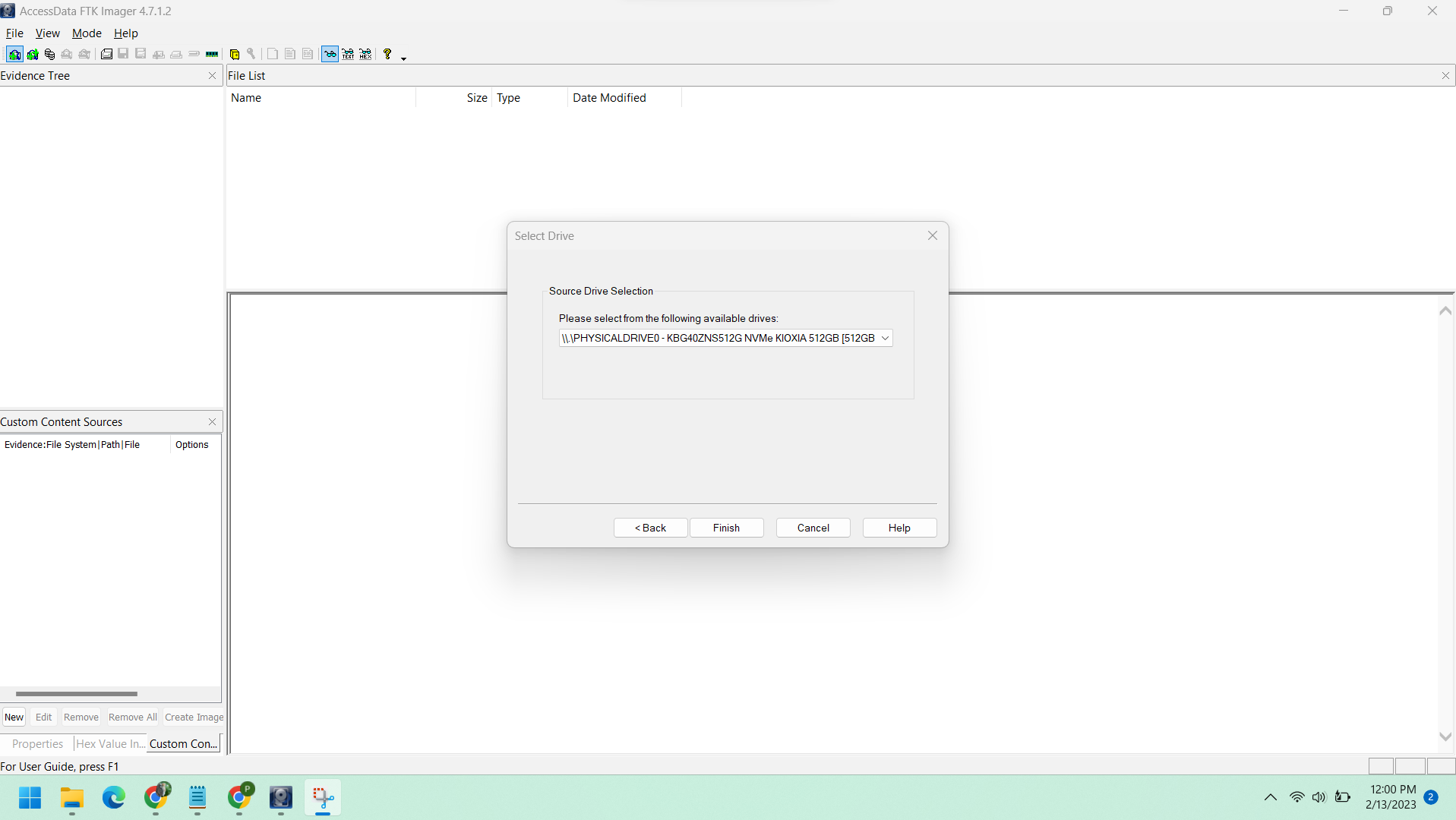
In FTK Imager, Portable Browser and Coffee Shopper would show up as two distinct physical units, and the resulting images would be two different files that represented the data and file system structures found on each thumb drive.

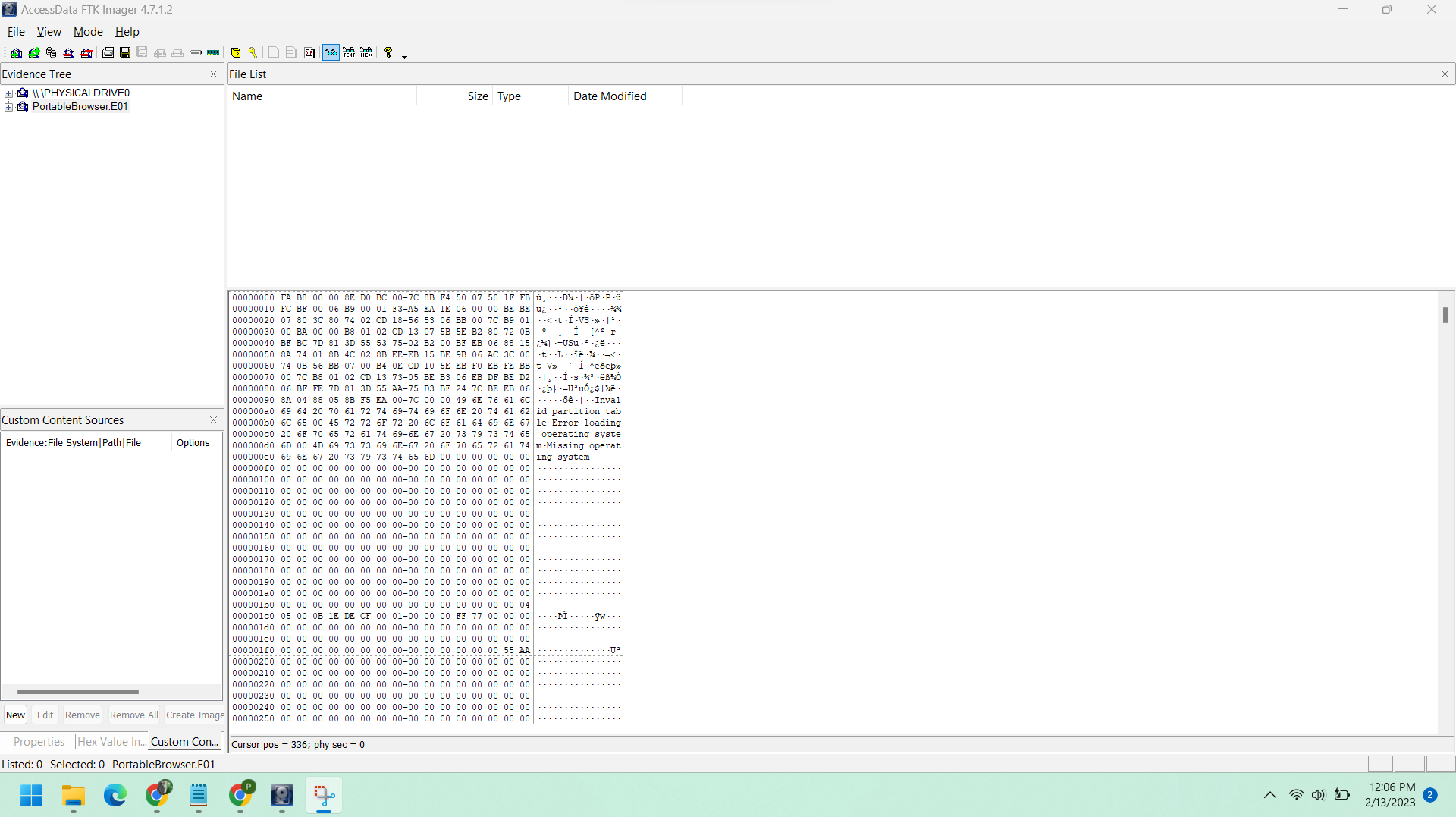
**Conclusion:**

After verifying the forensic image, I carried out various procedures to identify information such as the hash value, the types of file systems on the drive, the size of the image file, and the capacity of the original drive that the image was derived from. And manually adding the image from the local disk.

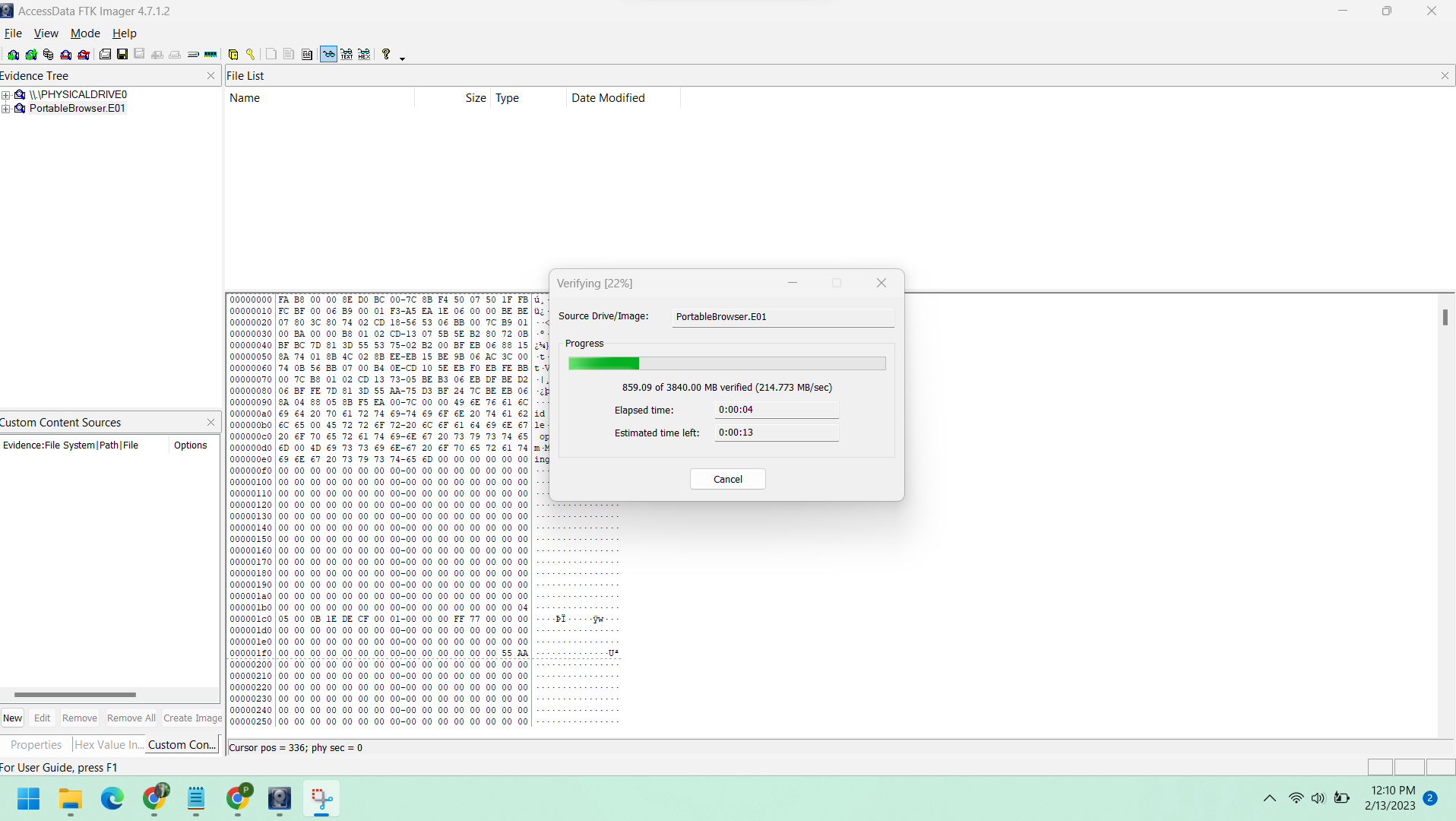
**Screenshots of the TASK**

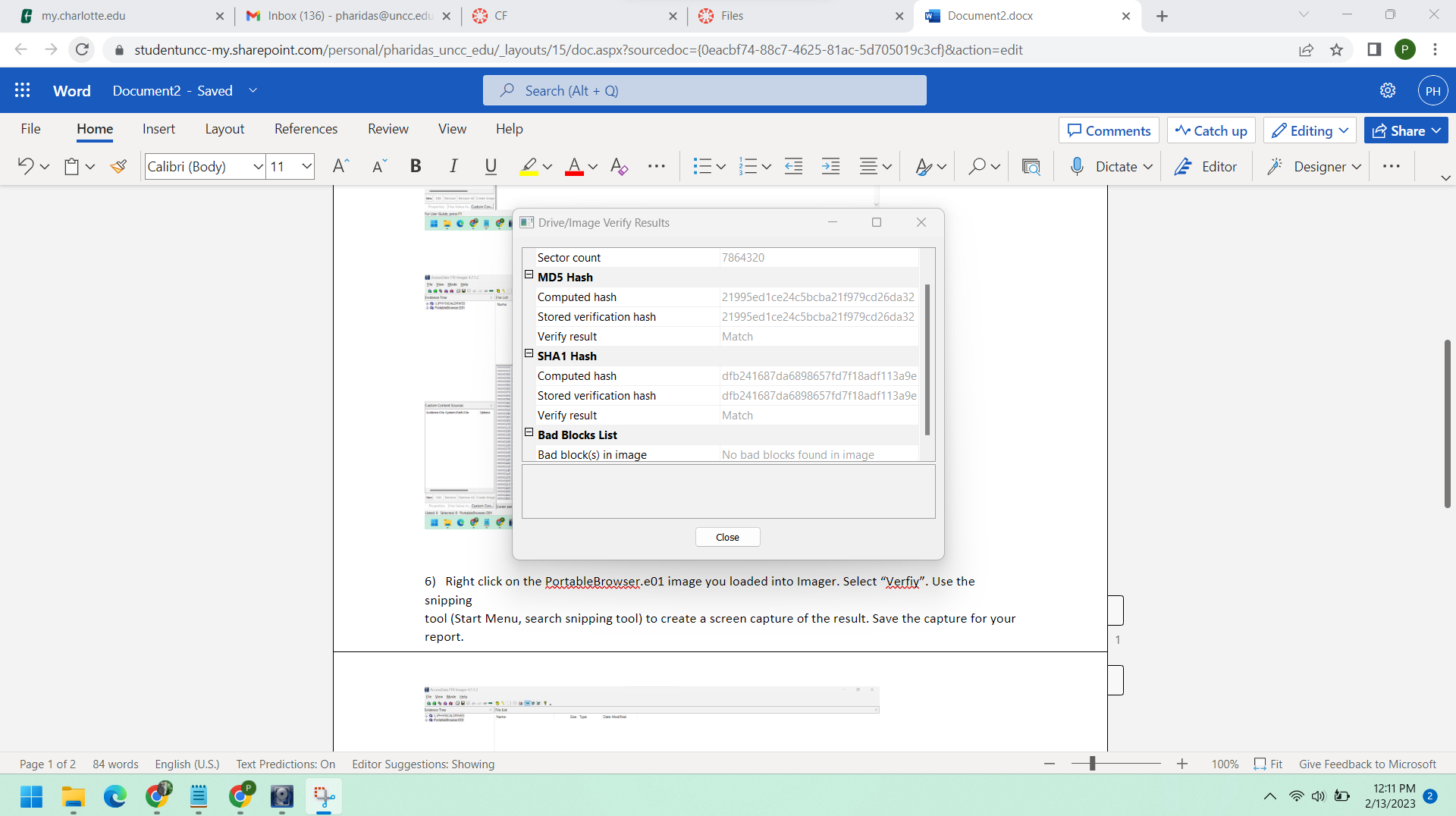
**5) Add a physical drive (your workstation hard drive should be \\PHYSICALDRIVE0, or a thumb drive may be another physical you can add. ), an image file (use PortableBrowser.e01) and the notes folder.**   
**Be sure to note differences in the representation of an image file and the physical drive.**



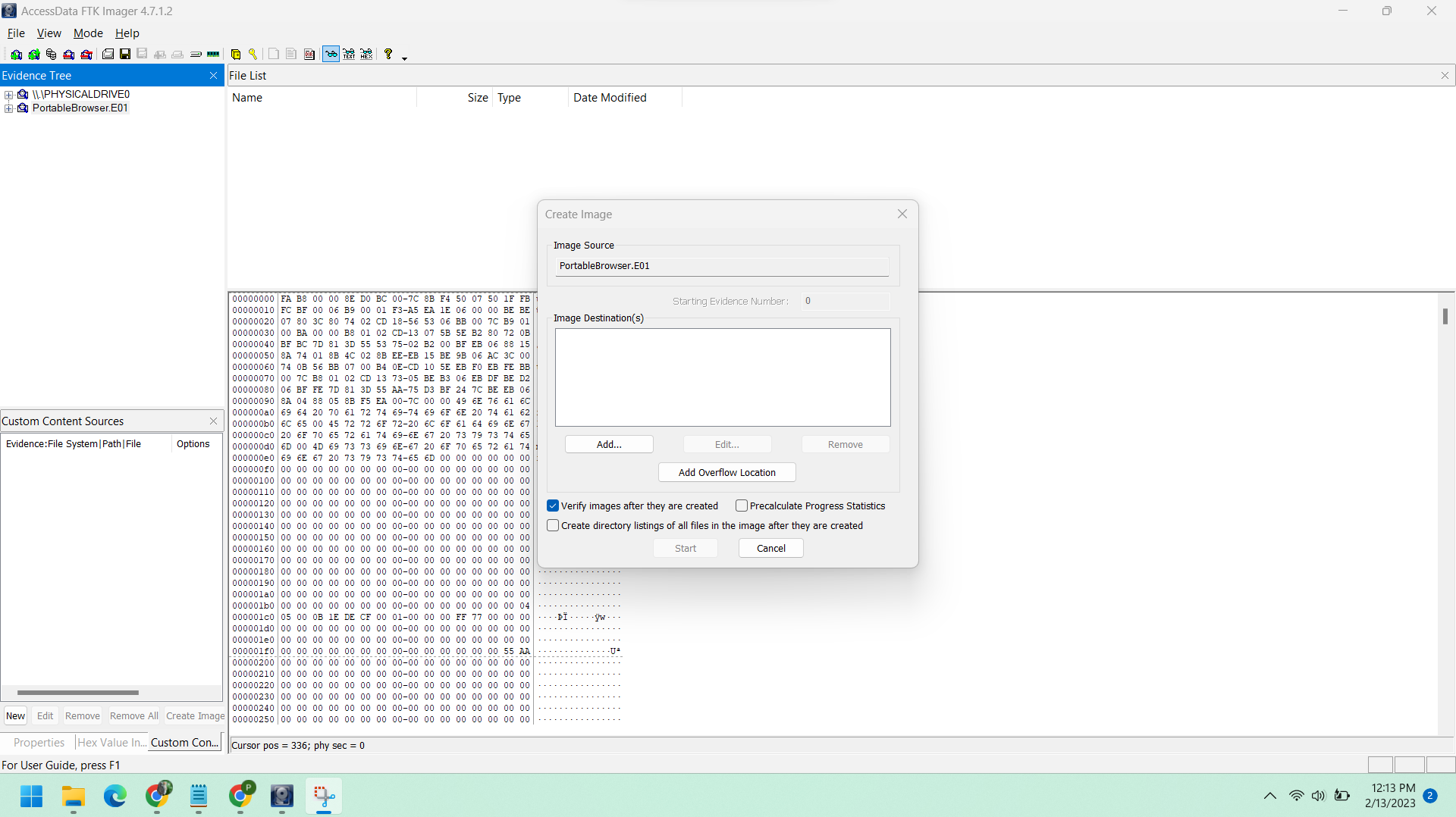


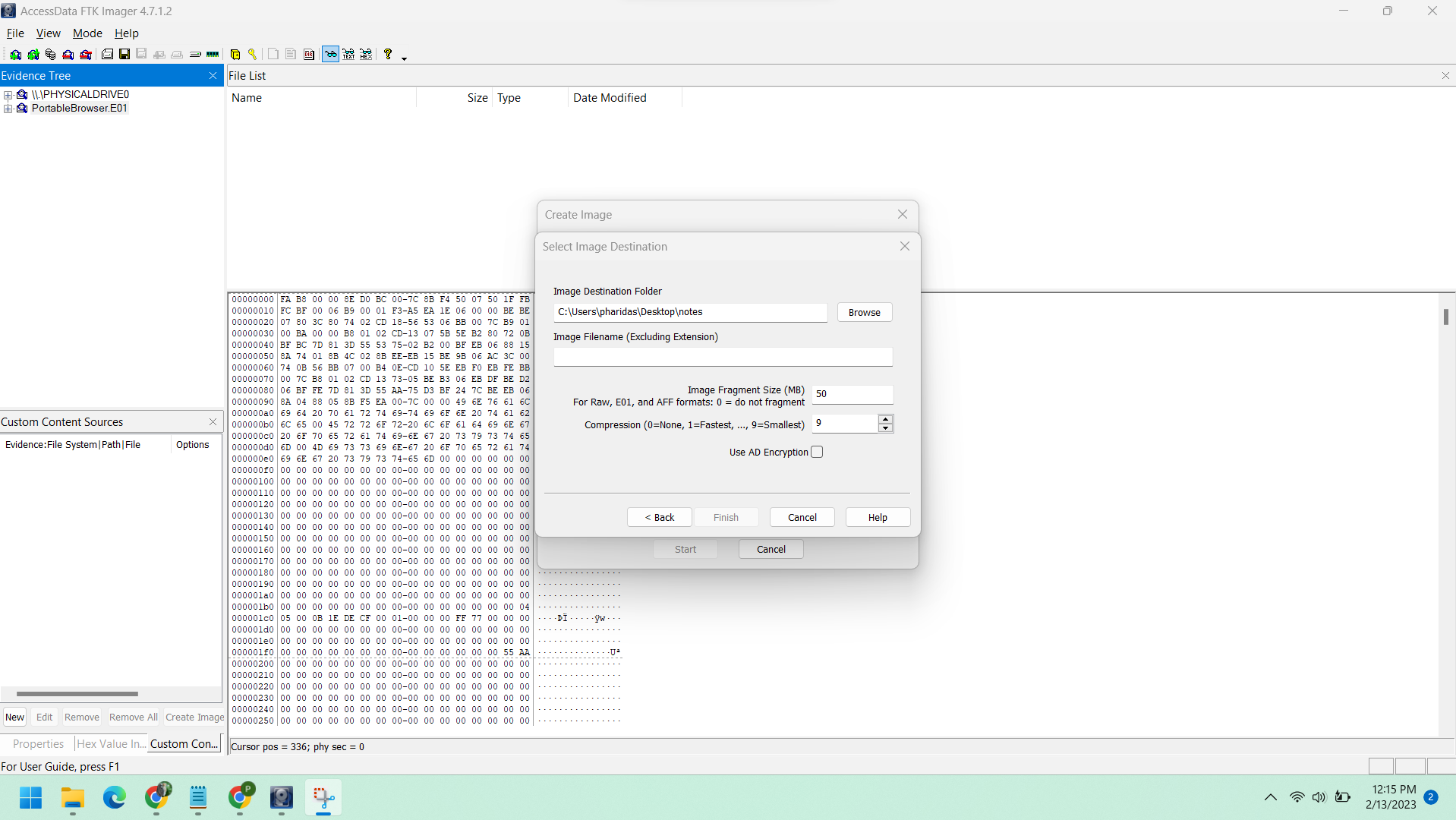
**6) Right click on the PortableBrowser.e01 image you loaded into Imager. Select “Verify”. Use the snipping tool (Start Menu, search snipping tool) to create a screen capture of the result. Save the capture for your report.**





**7) Right click on the PortableBrowser.e01 and select “Export to disk image”. Follow the menus and make a new forensic image from the existing one. You should make several files by selecting E01, size 50, compression 9. If you want to do the non-graded mmls option also, go to Optional Step A.**





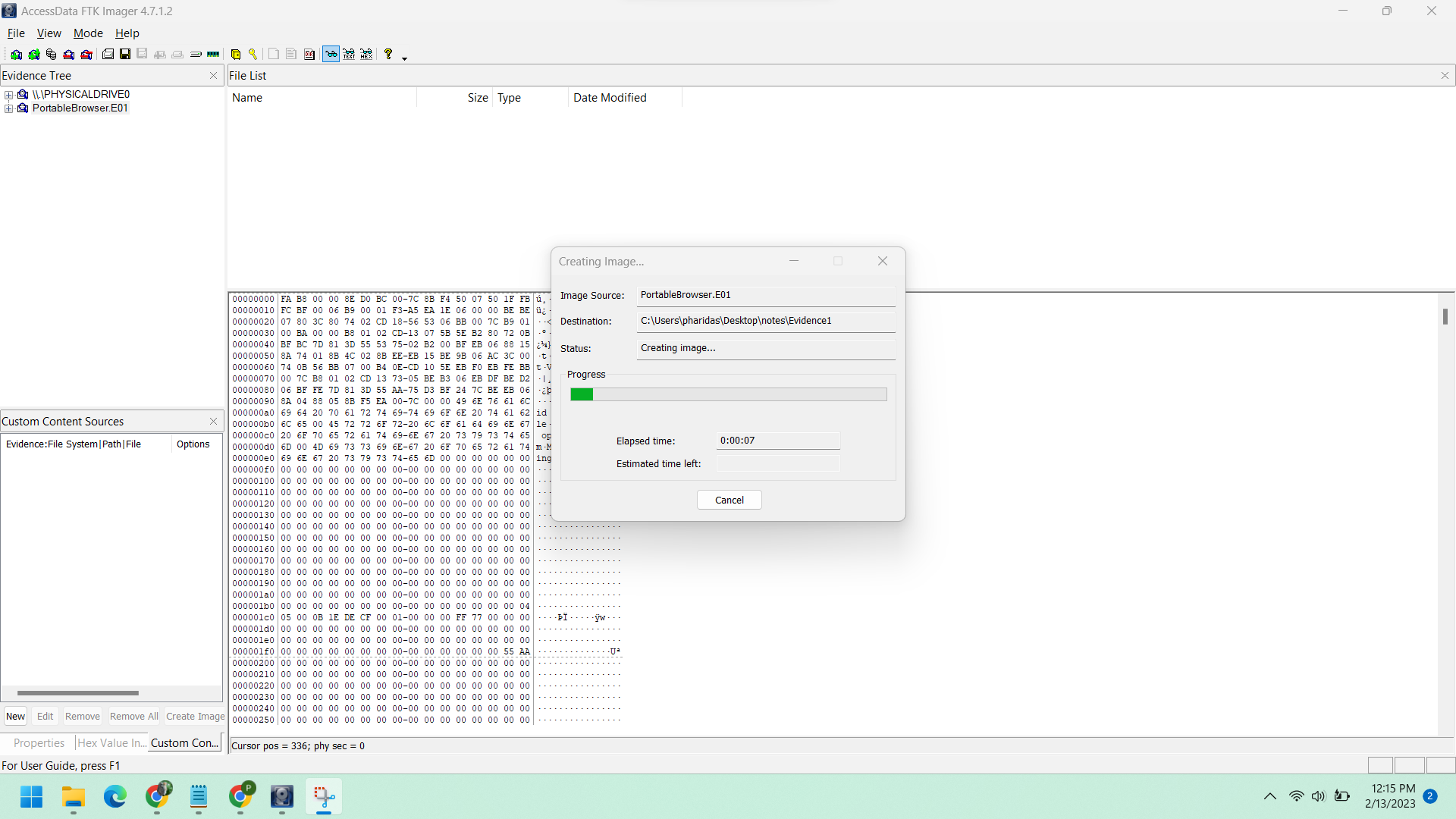
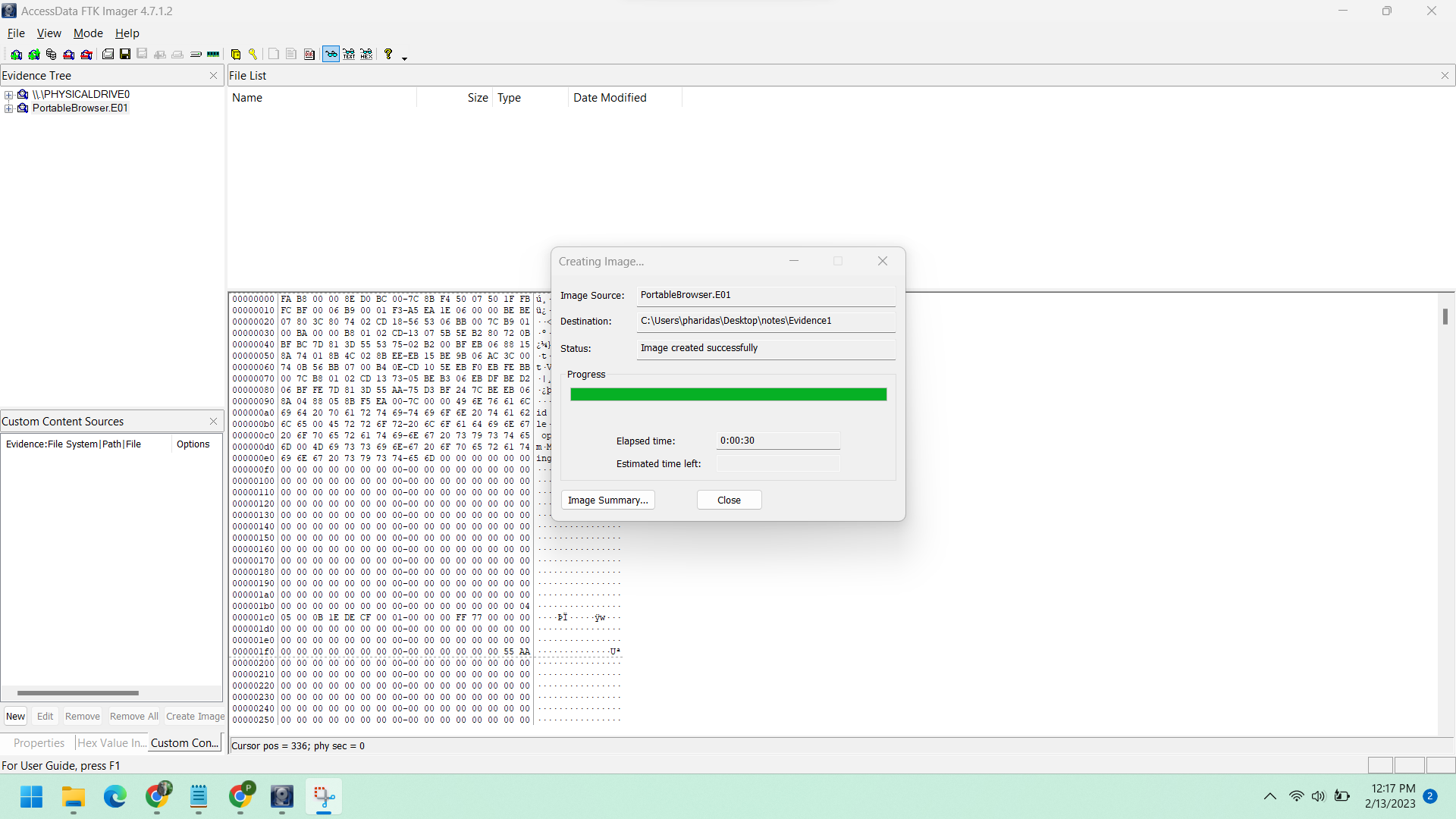
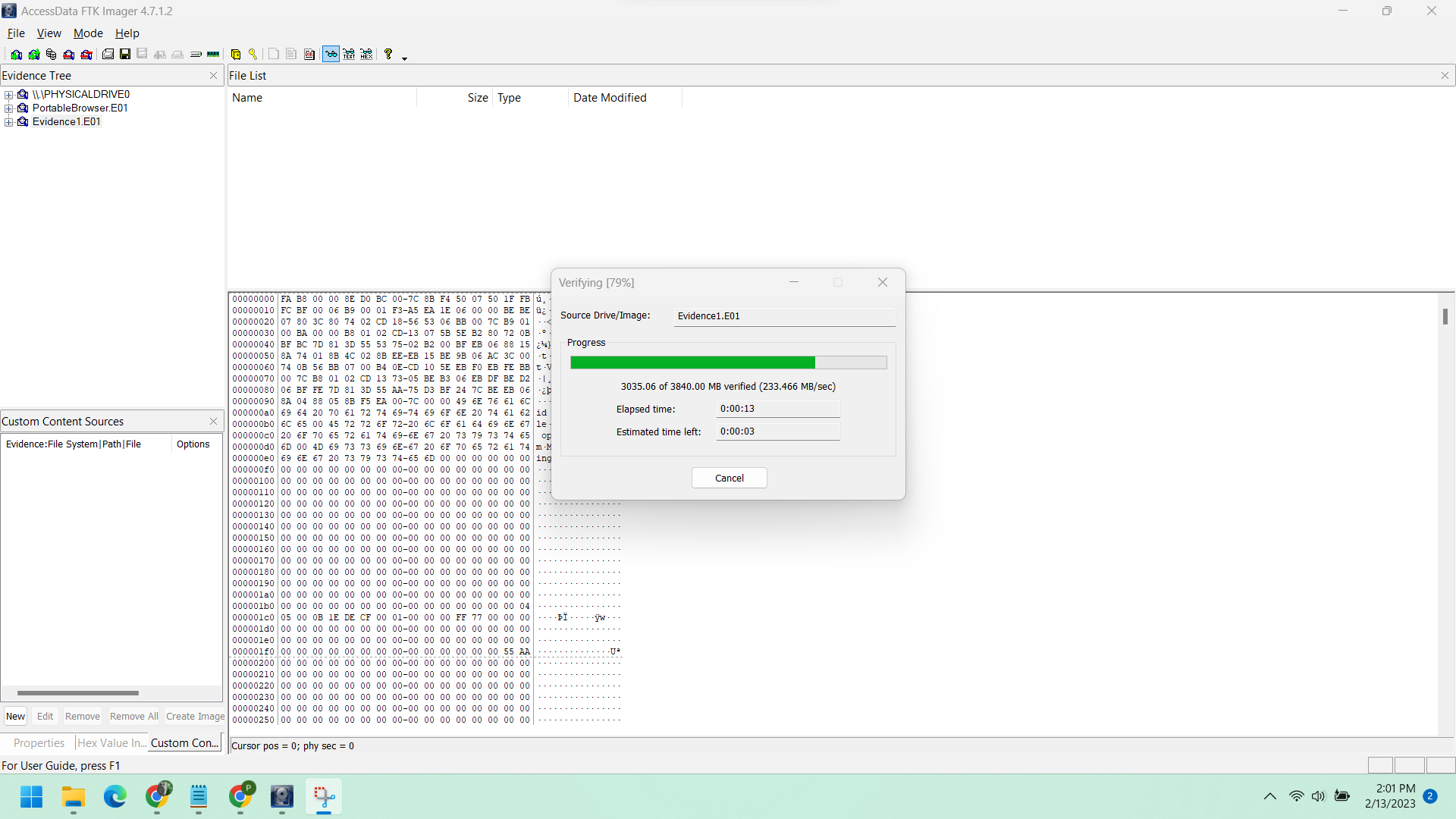
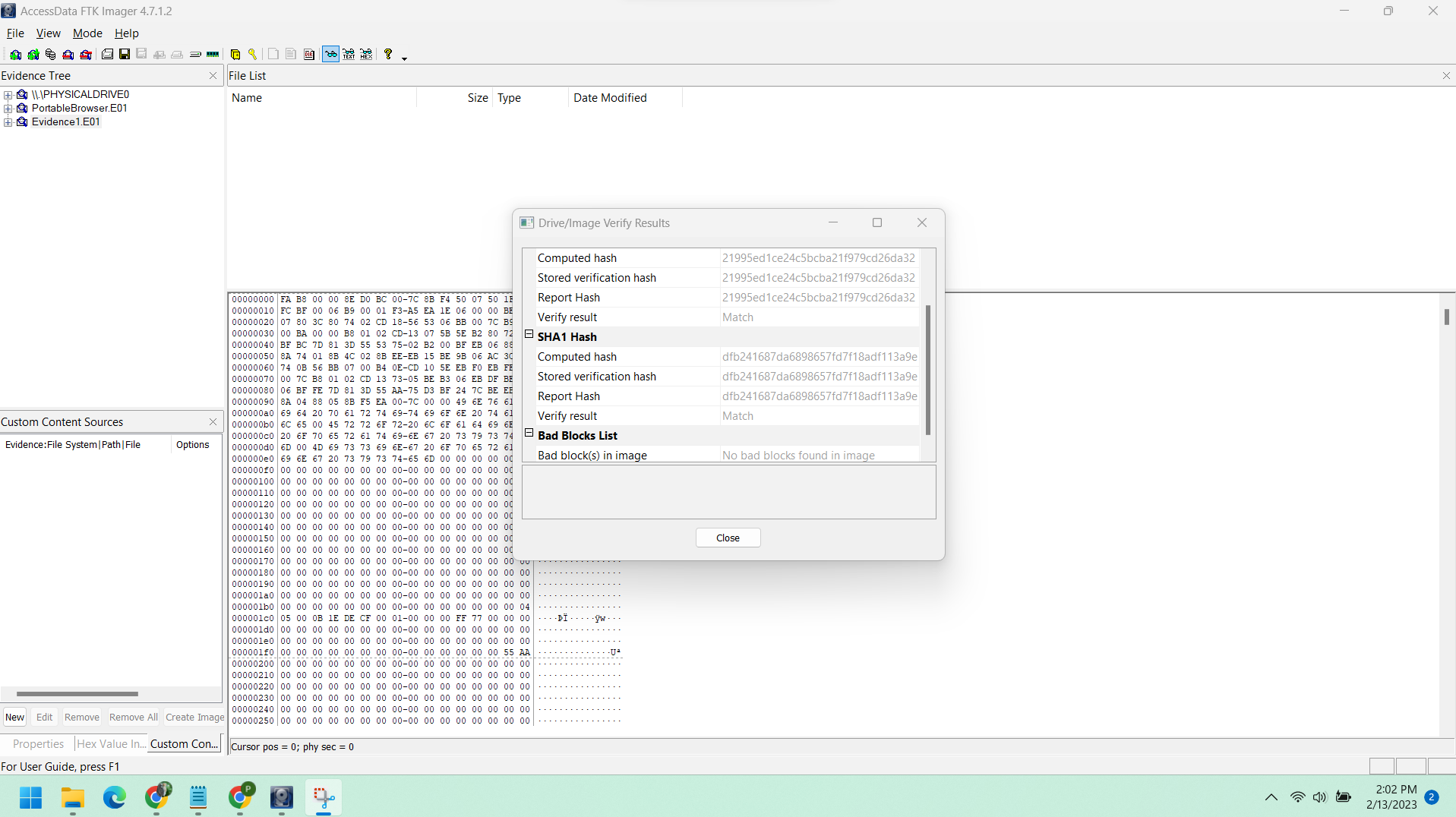


Image created successfully



**8) Right click on the disk image you created and select the option to verify the image. Compare to the original hash value for the original. Load the CoffeeShopper image as well and verify it. Browse both images briefly to observe their filesystems, volume names and top level directories.**





Coffee shopper

