ITIS 4250
Efren Antonio
Lab #1
September 19, 2024

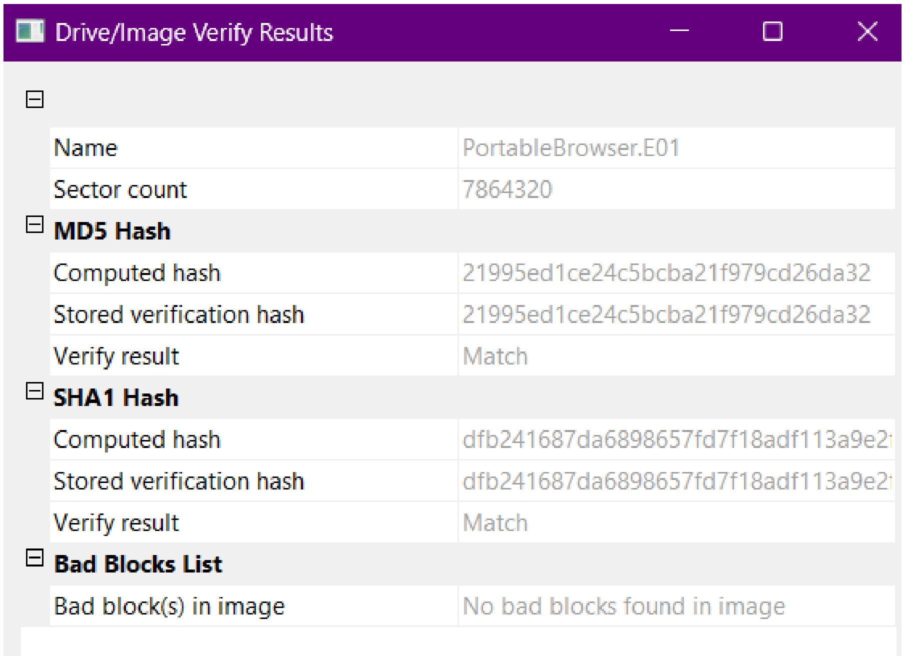
Overview

On September 19, 2024, Dr. Robert Quincy, Chief Forensics Examiner at the UNCC Forensics Laboratory, provided me with a forensics image of a thumb drive for analysis. The image was submitted by the Cybersecurity Center at UNCC, with the university's legal department confirming that the original device was abandoned property, therefore no legal authority is required for examination.

Dr. Quincy has requested a forensic analysis to verify whether the image corresponds to a specific thumb drive and to compare it against a second forensics image to determine if both images originate from the same device

Exam Preparation

The examination environment used is a HP Laptop running Microsoft Windows 11 Home version 10.0.22631. The tool used for verification of the image is Forensic Tool Kit (FTK) Imager version 4.7.1.2. The verified hash of the image is **21995ed1ce24c5bcba21f979cd26da32** and is provided below:



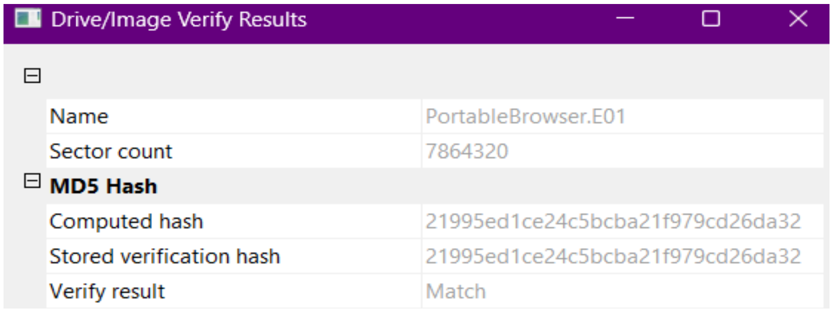
Name	PortableBrowser.E01
Sector count	7864320
MD5 Hash	
Computed hash	21995ed1ce24c5bcba21f979cd26da32
Stored verification hash	21995ed1ce24c5bcba21f979cd26da32
Verify result	Match
SHA1 Hash	
Computed hash	dfb241687da6898657fd7f18adf113a9e2
Stored verification hash	dfb241687da6898657fd7f18adf113a9e2
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Figure 1: FTK Imager MD5 Hash Verification

Analysis

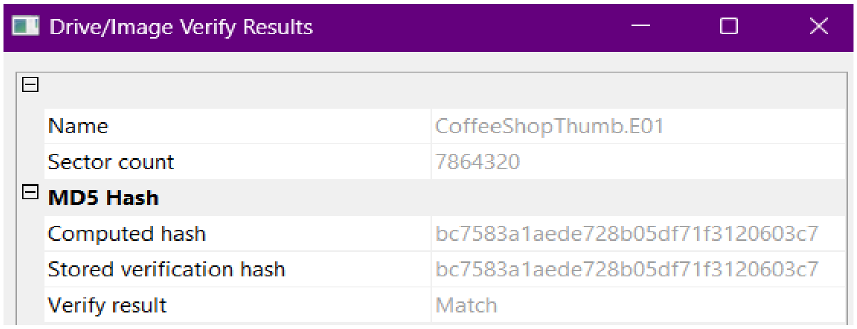
a. What was the MD5 hash value for PortableBrowser.e01? How about CoffeeShopper?

The MD5 hash value for PortableBrowser.e01 is 21995ed1ce24c5bcba21f979cd26da32. The MD5 hash value for CoffeeShopper is bc7583a1aede728b05df71f3120603c7. I found these by verifying the images with FTK Imager seen in the screenshots below:



Name	PortableBrowser.E01
Sector count	7864320
MD5 Hash	
Computed hash	21995ed1ce24c5bcba21f979cd26da32
Stored verification hash	21995ed1ce24c5bcba21f979cd26da32
Verify result	Match

Figure 2: MD5 Hash Value For PortableBrowser.e01

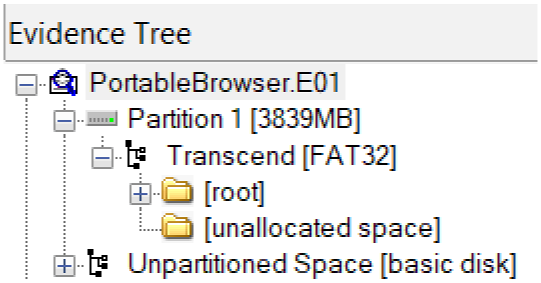


Name	CoffeeShopThumb.E01
Sector count	7864320
MD5 Hash	
Computed hash	bc7583a1aede728b05df71f3120603c7
Stored verification hash	bc7583a1aede728b05df71f3120603c7
Verify result	Match

Figure 3: MD5 Hash Value For CoffeeShopThumb.e01

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

The file system present within PortableBrowser.e01 is FAT32. This can be seen in the screenshot below:

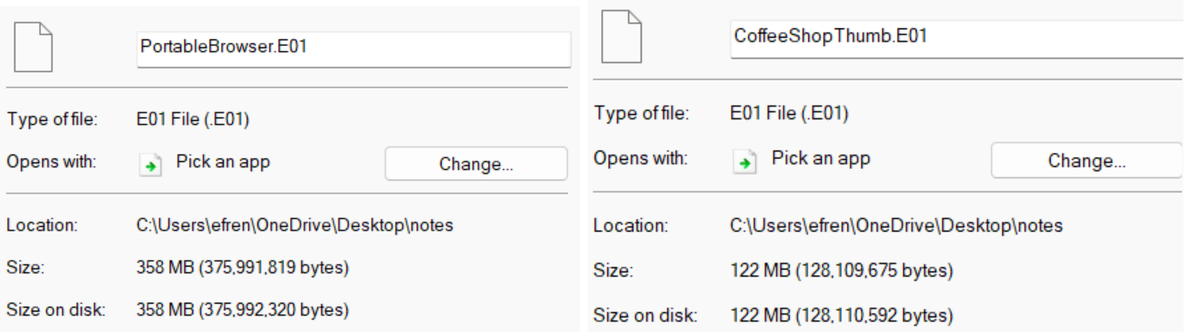

Evidence Tree

- PortableBrowser.E01
  - Partition 1 [3839MB]
    - Transcend [FAT32]
      - [root]
      - [unallocated space]
  - Unpartitioned Space [basic disk]

Figure 4: File System Present

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 PortableBrowser.e01 is 358 MB. The file size for CoffeeShopper is 122 MB. The size of the original device PortableBrowser.e01 is imaged from is 4 GB. The size of the original device CoffeeShopper is imaged from is 4 GB. I found these sizes by multiplying the sector size of 512 bytes times 7.8 million sectors for a total of approximately 4.02 GBs.



PortableBrowser.E01

Type of file: E01 File (.E01)

Opens with: Pick an app

Location: C:\Users\efren\OneDrive\Desktop\notes

Size: 358 MB (375,991,819 bytes)

Size on disk: 358 MB (375,992,320 bytes)

CoffeeShopThumb.E01

Type of file: E01 File (.E01)

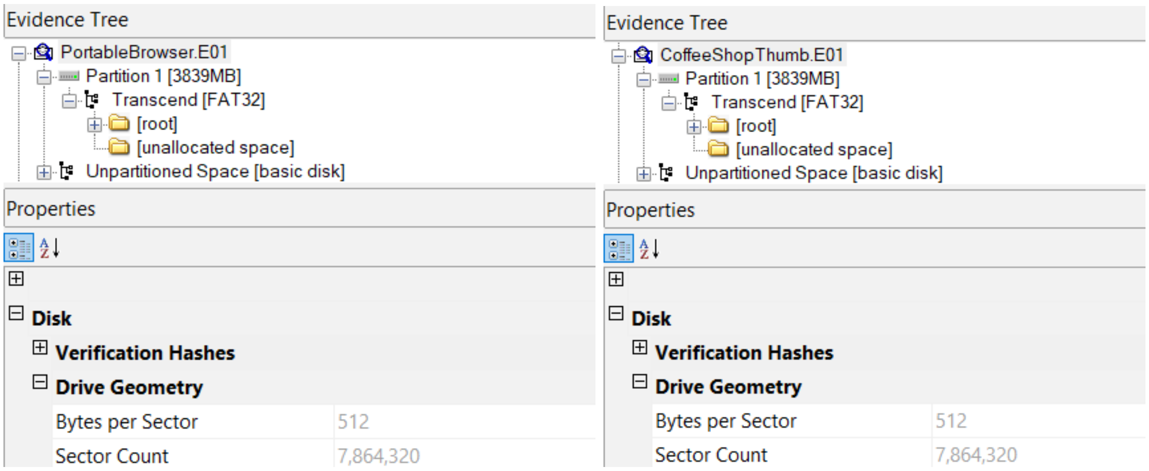
Opens with: Pick an app

Location: C:\Users\efren\OneDrive\Desktop\notes

Size: 122 MB (128,109,675 bytes)

Size on disk: 122 MB (128,110,592 bytes)

Figure 5: File Sizes For PortableBrowser.e01 And CoffeeShopThumb.e01



Evidence Tree

PortableBrowser.E01
- Partition 1 [3839MB]
  - Transcend [FAT32]
    - [root]
    - [unallocated space]
- Unpartitioned Space [basic disk]

Properties

Disk
- Verification Hashes
- Drive Geometry
  - Bytes per Sector: 512
  - Sector Count: 7,864,320

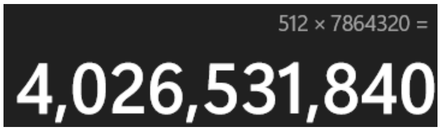
Evidence Tree

CoffeeShopThumb.E01
- Partition 1 [3839MB]
  - Transcend [FAT32]
    - [root]
    - [unallocated space]
- Unpartitioned Space [basic disk]

Properties

Disk
- Verification Hashes
- Drive Geometry
  - Bytes per Sector: 512
  - Sector Count: 7,864,320

Figure 6: FTK Imager Drive Geometry



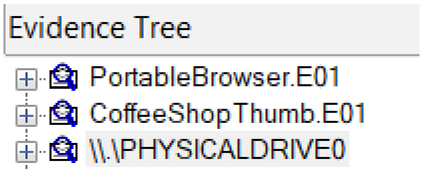
512 × 7864320 =

4,026,531,840

Figure 7: Windows Calculator For Calculating Disk Size

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)?

An image appears in FTK imager as the name of the file followed by its file path (.e01, .aff, .dd, etc.), “PortableBrowser.e01” for example. A physical drive appears as the physical device name, “\\.\PHYSICALDRIVE0” for example. An image has some added embedded metadata relating to the case which doesn’t appear for the physical drive. This metadata can be seen in Figure 8 below:



Evidence Tree

- PortableBrowser.E01
- CoffeeShopThumb.E01
- \\.\PHYSICALDRIVE0

Figure 8: Differences Between Image & Physical Drives In FTK Imager

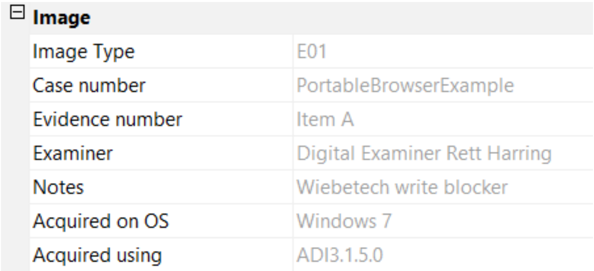
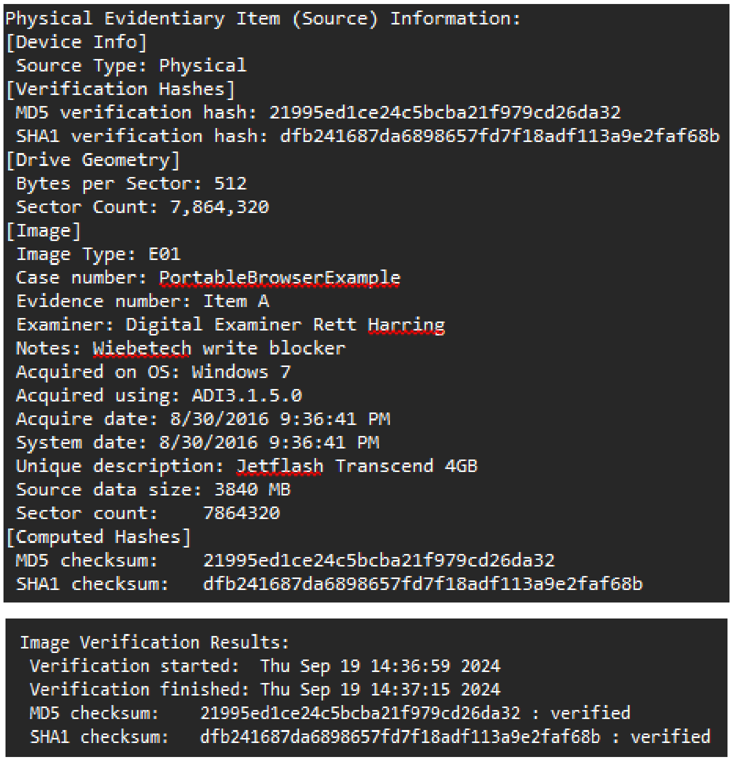


Image	
Image Type	E01
Case number	PortableBrowserExample
Evidence number	Item A
Examiner	Digital Examiner Rett Harring
Notes	Wiebetech write blocker
Acquired on OS	Windows 7
Acquired using	ADI3.1.5.0

Figure 9: Embedded Metadata Showing Case Information

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

FTK imager generated a log for the image I created out of PortableBrowser.e01. The hash value in the log matches the original image hash value. The log is provided below:



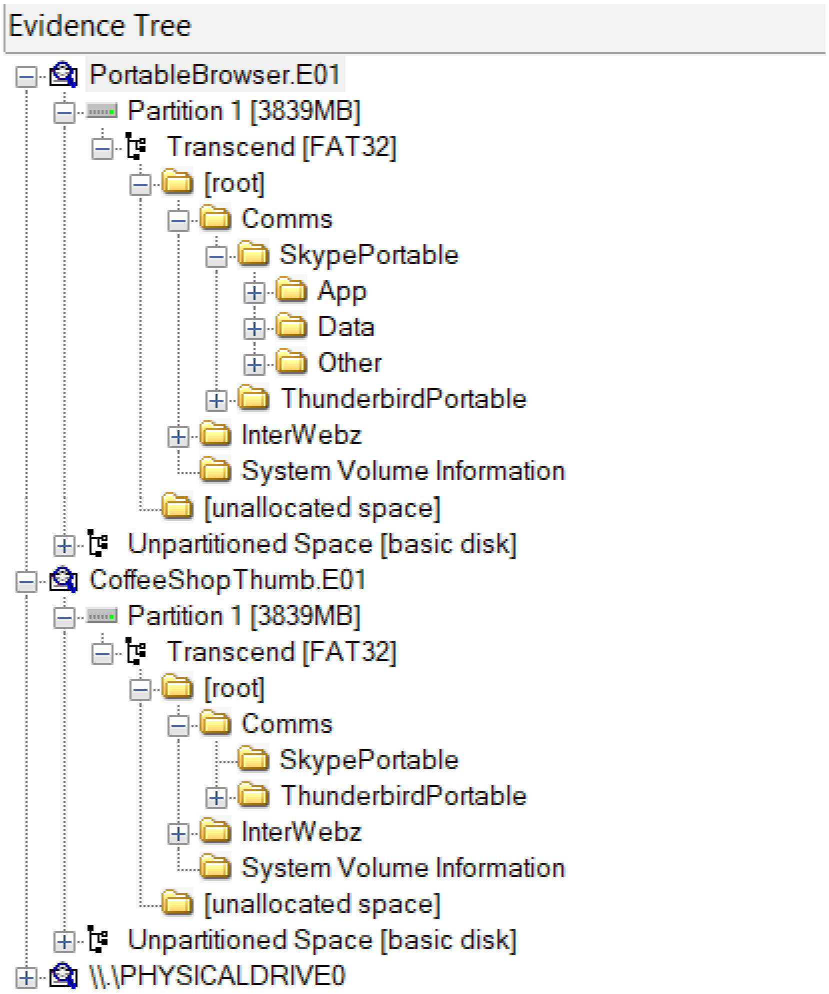
```
Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Verification Hashes]
 MD5 verification hash: 21995ed1ce24c5bcba21f979cd26da32
 SHA1 verification hash: dfb241687da6898657fd7f18adf113a9e2faf68b
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 7,864,320
[Image]
 Image Type: E01
 Case number: PortableBrowserExample
 Evidence number: Item A
 Examiner: Digital Examiner Rett Harring
 Notes: Wiebetech write blocker
 Acquired on OS: Windows 7
 Acquired using: ADI3.1.5.0
 Acquire date: 8/30/2016 9:36:41 PM
 System date: 8/30/2016 9:36:41 PM
 Unique description: Jetflash Transcend 4GB
 Source data size: 3840 MB
 Sector count:    7864320
[Computed Hashes]
 MD5 checksum:    21995ed1ce24c5bcba21f979cd26da32
 SHA1 checksum:   dfb241687da6898657fd7f18adf113a9e2faf68b
```

```
Image Verification Results:
 Verification started:  Thu Sep 19 14:36:59 2024
 Verification finished: Thu Sep 19 14:37:15 2024
 MD5 checksum:    21995ed1ce24c5bcba21f979cd26da32 : verified
 SHA1 checksum:   dfb241687da6898657fd7f18adf113a9e2faf68b : verified
```

Figure 10: Log Generated From PortableBrowser Image

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

PortableBrowser and CoffeeShopper appear to be the same thumb drive, they have the same file sizes and hard drive sizes, refer to Figure 5. They have the same files inside of their thumb drives, the only difference is the SkypePortable folder inside the PortableBrowser contains items inside of it while the same folder in the CoffeeShopper is empty.

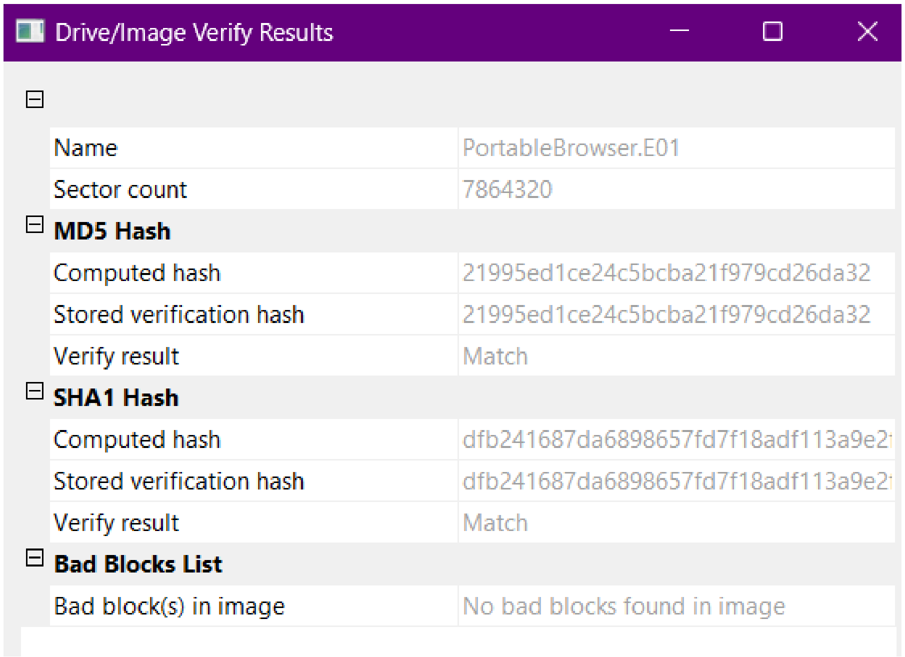


```
Evidence Tree
⊟ PortableBrowser.E01
    ⊟ Partition 1 [3839MB]
        ⊟ Transcend [FAT32]
            ⊟ [root]
                ⊟ Comms
                    ⊟ SkypePortable
                        ⊞ App
                        ⊞ Data
                        ⊞ Other
                    ⊞ ThunderbirdPortable
                ⊞ InterWebz
                  System Volume Information
              [unallocated space]
    ⊞ Unpartitioned Space [basic disk]
⊟ CoffeeShopThumb.E01
    ⊟ Partition 1 [3839MB]
        ⊟ Transcend [FAT32]
            ⊟ [root]
                ⊟ Comms
                      SkypePortable
                    ⊞ ThunderbirdPortable
                ⊞ InterWebz
                  System Volume Information
              [unallocated space]
    ⊞ Unpartitioned Space [basic disk]
⊞ \\.\PHYSICALDRIVE0
```

Figure 11: Files Inside Both Thumb Drives

Conclusion

The forensic analysis of both thumb drive images, PortableBrowser.e01 and CoffeeShopper, shows that both images most likely originated from the same thumb drive. Both images share identical file sizes, hard drive sizes, and use the same FAT32 file system structure. The only notable difference is that the SkypePortable folder within the PortableBrowser image contains files, while the same folder in CoffeeShopper is empty. The hash values of both images were verified and matched the original hashes, confirming the integrity of the forensic images.



Name	PortableBrowser.E01
Sector count	7864320
MD5 Hash	
Computed hash	21995ed1ce24c5bcba21f979cd26da32
Stored verification hash	21995ed1ce24c5bcba21f979cd26da32
Verify result	Match
SHA1 Hash	
Computed hash	dfb241687da6898657fd7f18adf113a9e2
Stored verification hash	dfb241687da6898657fd7f18adf113a9e2
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Figure 12: Reverified MD5 Hash Value After The Examination

Signed:

Efren Antonio