**DOUGLAS AKWASI KWARTENG**

**Evidence Verification and Comparison on behalf of**

**Dr. Robert Quincy for the Cybersecurity Center at UNCC**

**University of North Carolina at Charlotte**

**Digital Forensics Laboratory**

## Overview

On February 09, 2026, Dr. Robert Quincy, Chief Forensics Examiner at the UNCC Forensics Laboratory, directed an examination of two forensic images: RettsThumbDrive.E01 and rettcopy.E01. The objective of this technical work was to verify the integrity of the provided forensic images, export the evidence, and determine whether the two images originated from the same physical thumb drive or not.

The University Attorney has determined that the original device was abandoned property; therefore, no additional legal authority was required for this examination.

## Exam Preparation

The examination was conducted on a Dell laptop equipped with 16GB of RAM and a 2TB Hard Drive, running a Windows 10 Virtual Machine with 8GB of allocated RAM and a 500GB virtual disk.

The primary tools used for this examination were:

- Forensic Tool Kit (FTK) Imager version 4.7.1.2: Used for image verification, property analysis, and evidence export.
- Autopsy version 4.21.0: Used for file system analysis and cross-image content comparison.

Both the rettsThumbDrive.E01 and the rettcopy.E01 images were uploaded into the autopsy and the FTK imager for this analysis. Their MD5 hash values were verified before the analysis.

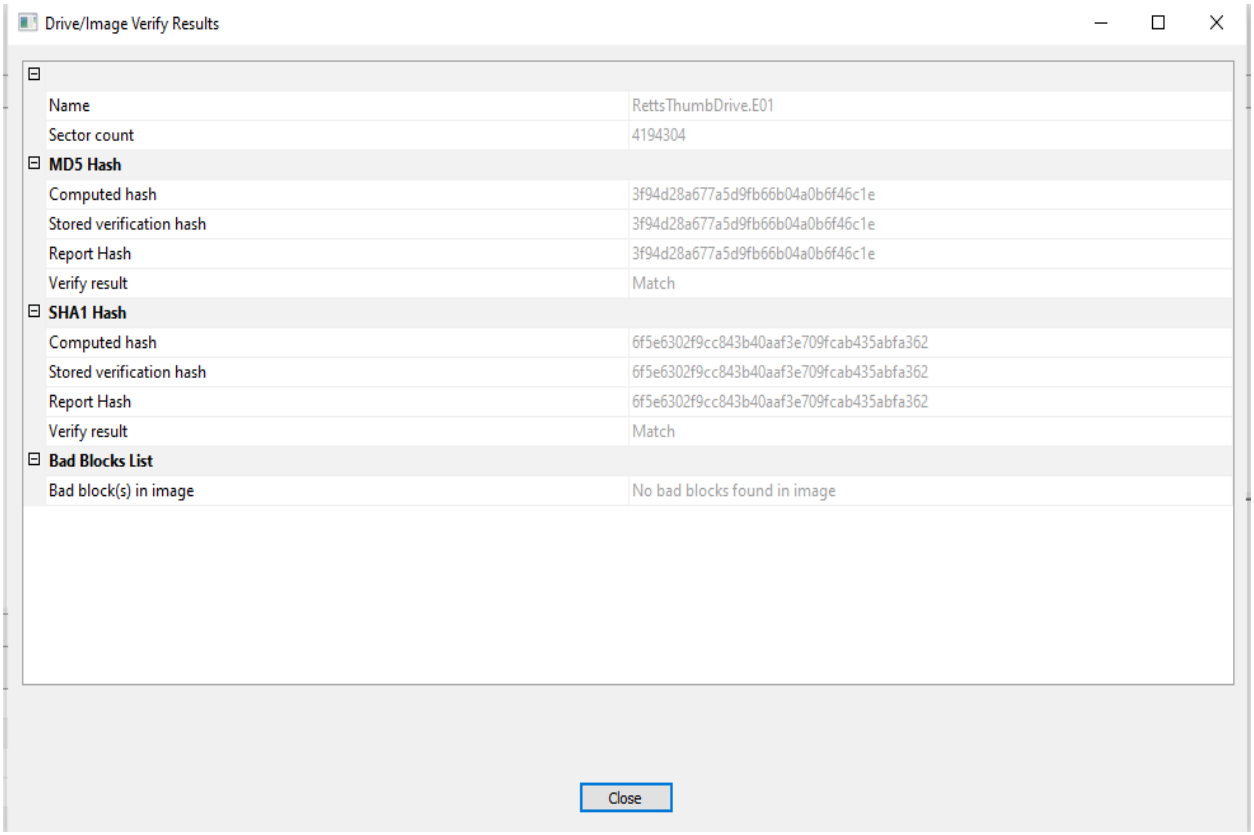



Figure 1.0 rettsThumbDrive.E01 Verified

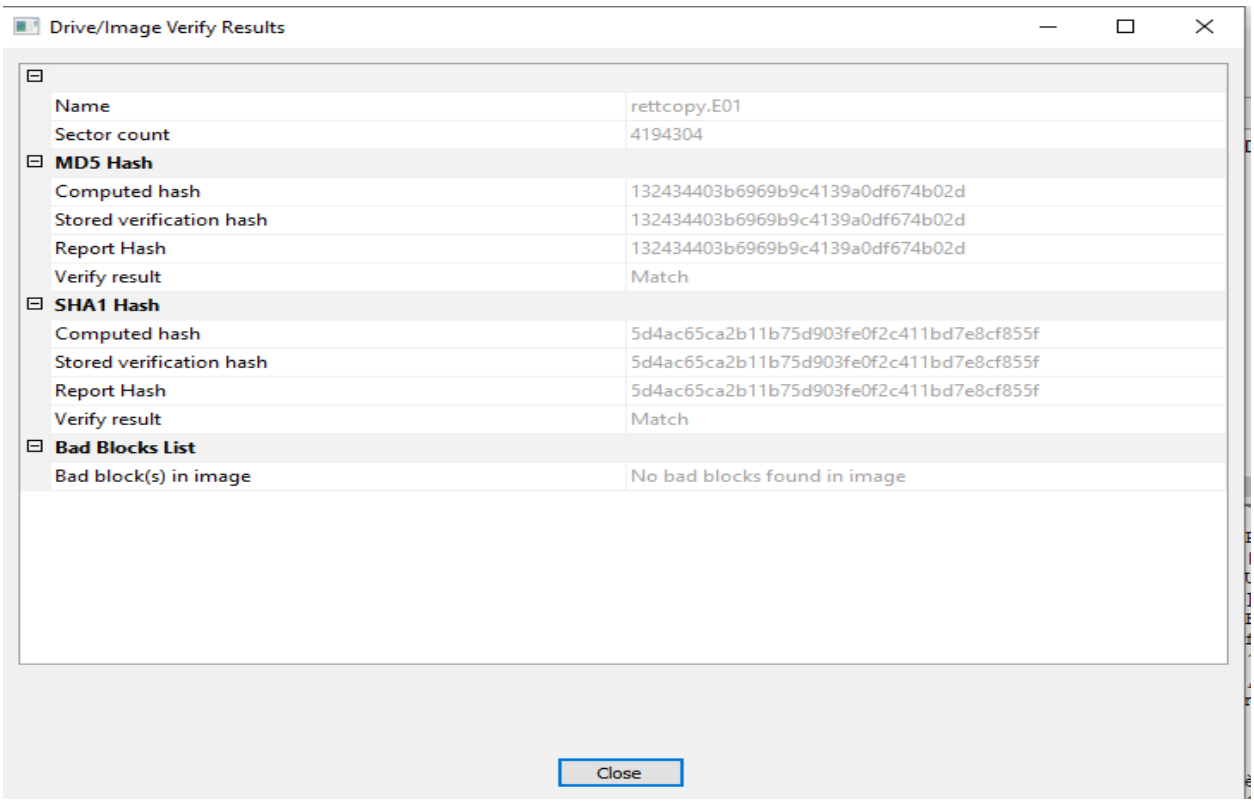



Figure 2.0 rettsThumbDrive.E01 Verified

Also, a disk image was exported to a rettsThumbDriveCopy.E01, and its MD5 hash value was also verified.

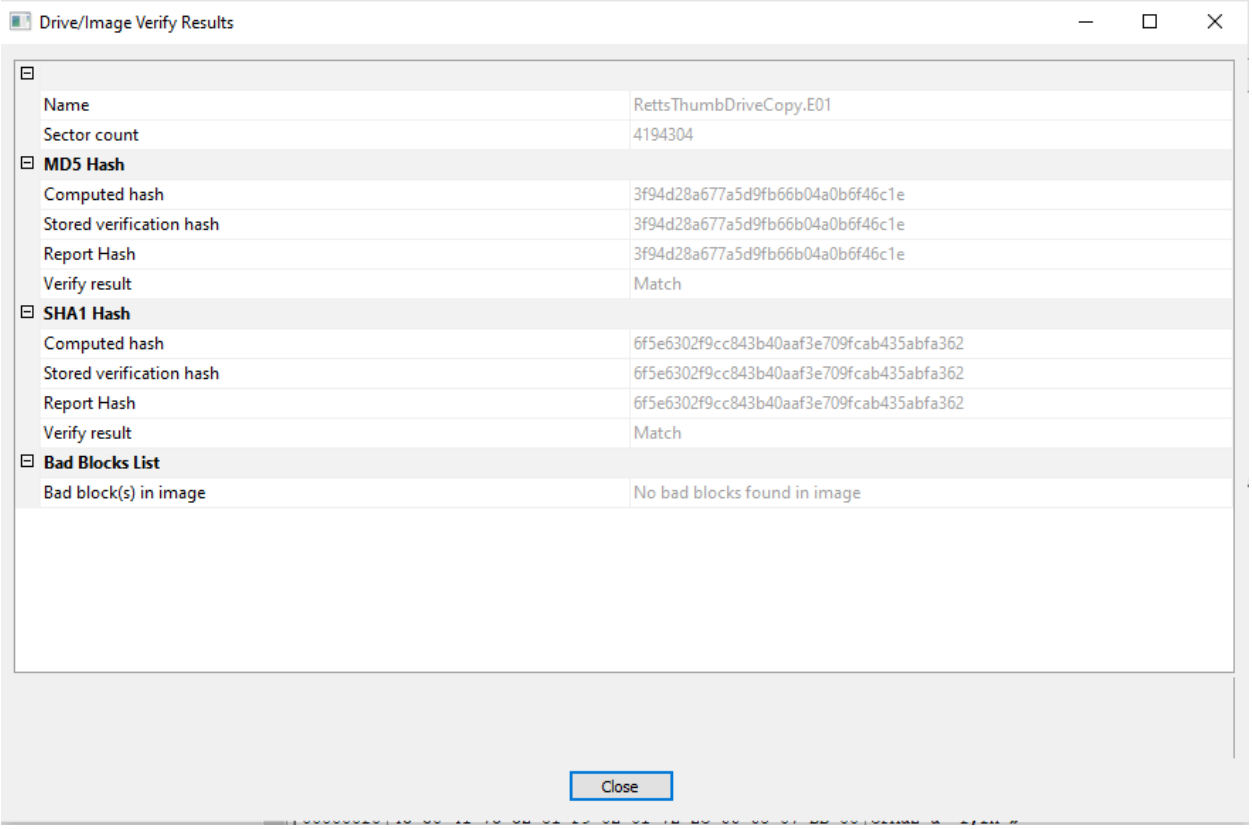



Figure 3.0 rettsThumbDriveCopy.E01 Verified

## Analysis

1. **What was the MD5 hash value for RettsThumb.e01? Rettcopy.e01?**

RettsThumbDrive.e01's MD5 hash, 3f94d28a677a5d9fb66b04a0b6f46c1e, was confirmed. As for rettcopy.e01, the MD5 hash was confirmed to be 132434403b6969b9c4139a0df674b02d. Also, It was verified that neither image included any problematic blocks. Using FTK imager, this was accomplished by selecting the Verify Drive/Image button with a right-click on each image. Locate the result image shown in figure 1.0 and 2.0 respectively.

.

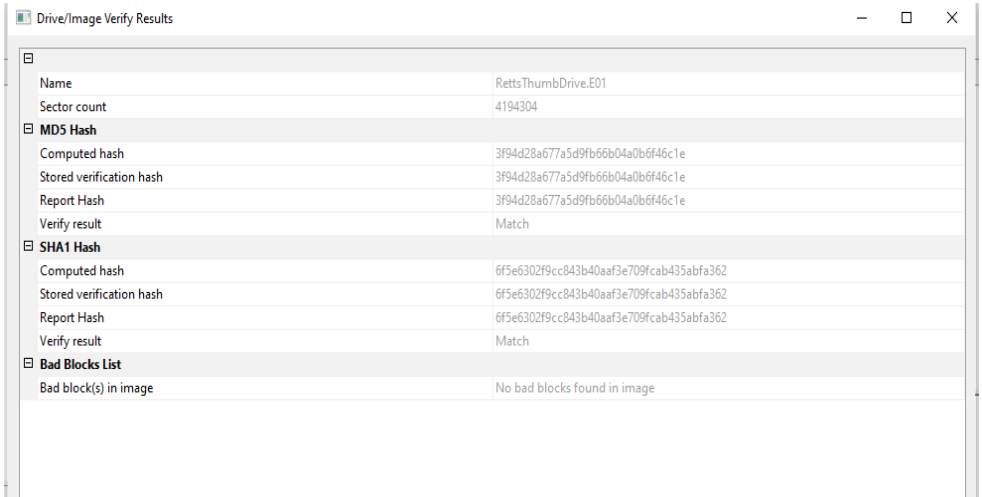


Figure 4.0 rettsThumbDrive.E01 Verified

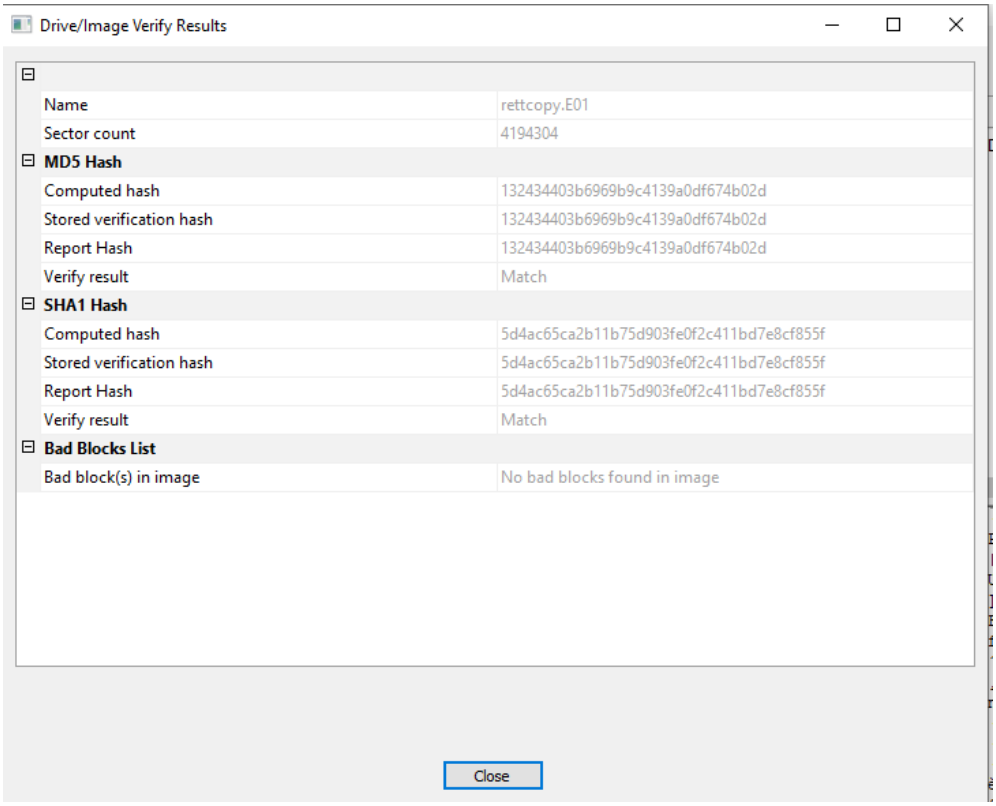



**Figure 5.0 rettcopy.E01 verified.**

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

**Answer:**
Analysis in both FTK Imager and Autopsy confirmed that RettsThumbDrive.e01 contains a single partition of approximately 2045 MB formatted with the FAT16 file system. The volume label is identified as RETTSTHUMB as shown in the image below.

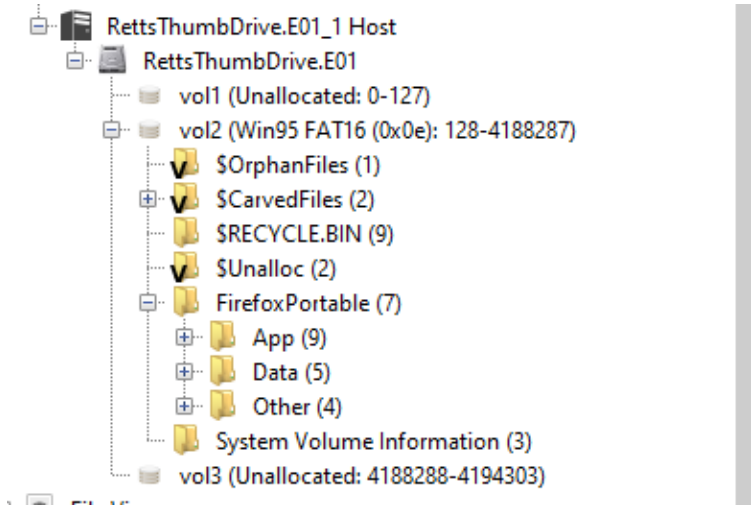


**Figure 6.0 rettsThumbDrive.E01 file systems image.**

3. **What is the file size for RettsThumb.e01, and what was the size of the original device (hard drive) that RettsThumb.e01 is imaged from? How about rettcopy.e01?**

   **Answer:**

   The physical size of the forensic image file RettsThumbDrive.e01 is 534 MB. The original device size, however, was determined by multiplying the sector count of 4,194,304 by the bytes per sector of 512, resulting in 2,147,483,648 bytes, or 2 GB. rettcopy.E01 has the same 534 MB file size and the same 2 GB original device geometry. The two files were opened in their original folder, and the file size was displayed by right-clicking on each one and choosing Properties. I also chose each image in Autopsy, and the property section displays the number of sectors as well as the number of bytes per sector, which were multiplied to determine the device sizes.

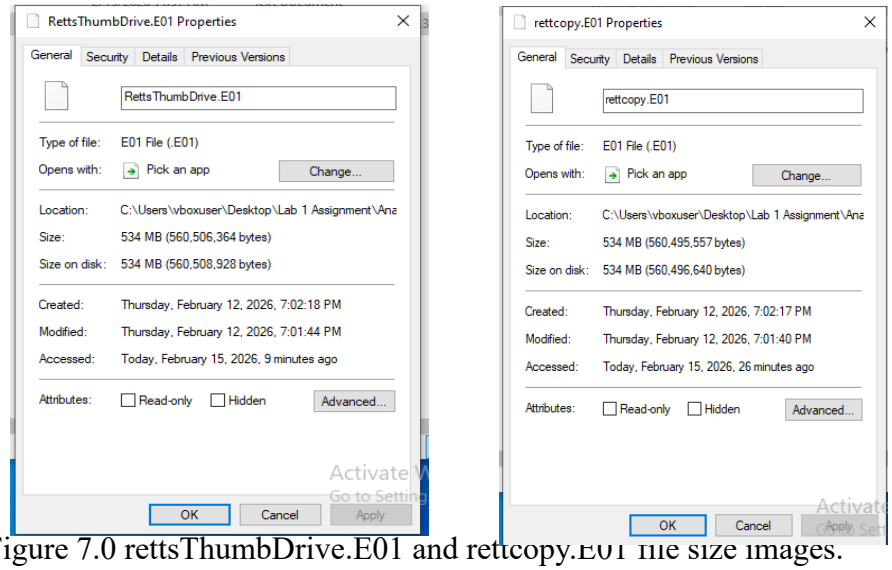



Figure 7.0 rettsThumbDrive.E01 and rettcopy.E01 file size images.

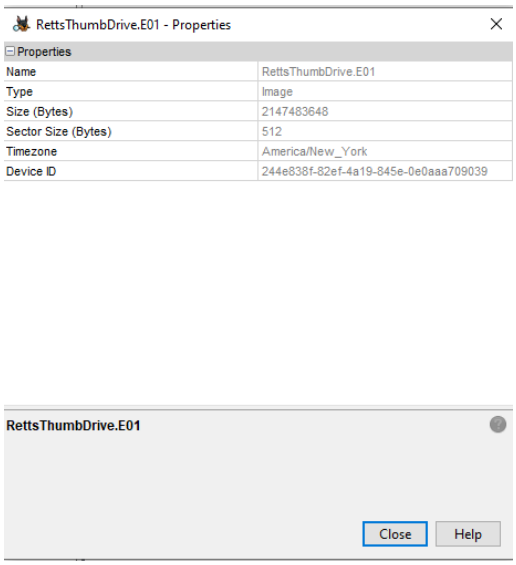
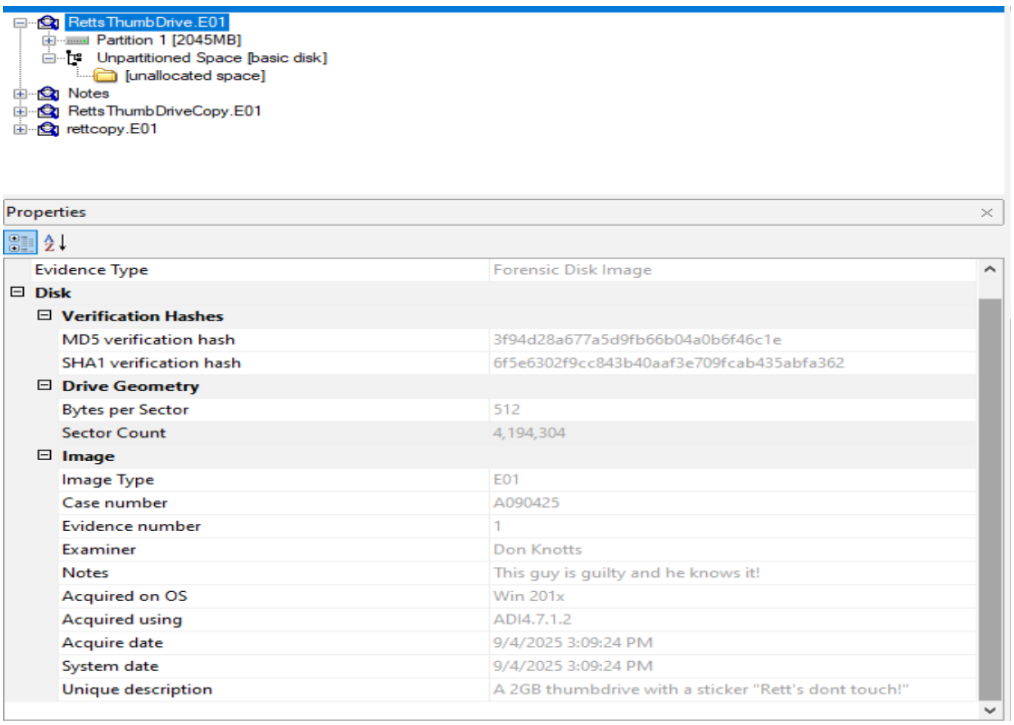



**Figure 8.0 Autopsy property showing the device size of rettsThumbDrive.E01.**

4. **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)?**

**Answer:**

The rettcopy and the rettsThumbDrive.E01 is different since the rettsThumb picture has a clear description: "A 2GB thumbdrive with a sticker that reads, 'Rett's do not touch!'" In contrast, rettcopy is simply referred to as "untitle." Additionally, the device ID for the rettsThumbDrive was 244e838f-82ef-4a19-845e-0e0aaa709039, which is not the same as the device ID for the rettcopy, which is 057d49f6-258a-41cb-9832-4711b98042b8. Once more, the two drives' MD5 hashes differ. rettsThumbDrive.E01's MD5 hash, 3f94d28a677a5d9fb66b04a0b6f46c1e, was confirmed. As for rettcopy.E01, the MD5 hash was confirmed to be 132434403b6969b9c4139a0df674b02d.



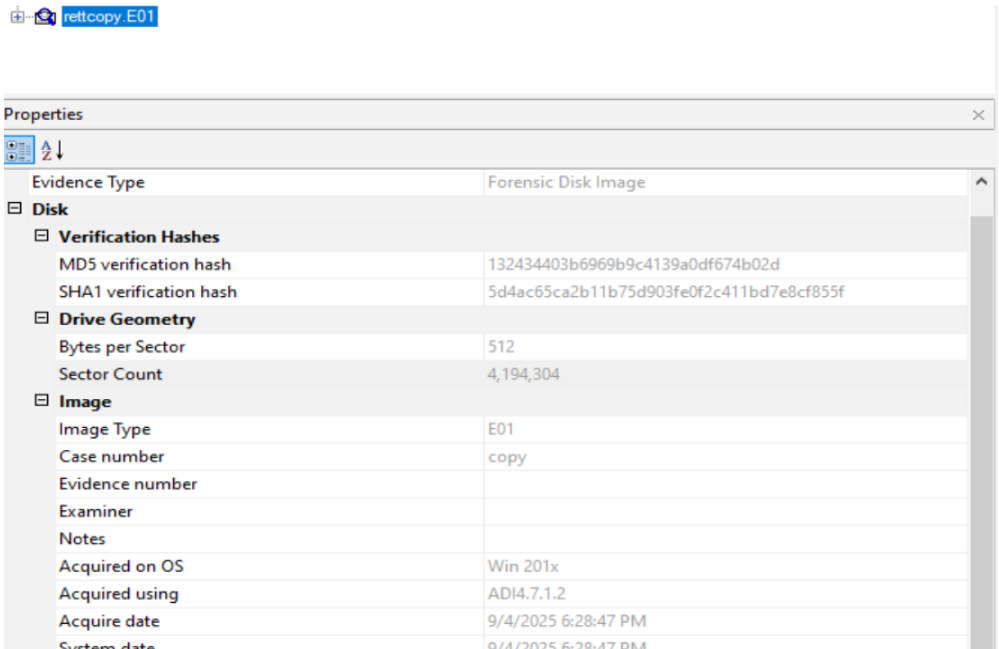



**Figure 9.0 rettsThumbDrive.E01 and rettcopy image showing their MD5 differences in FTK imaging.**

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

   **Answer:**

   Yes, the FTK imager generated a log for the image we created out of the RettsThumbDrive. Also, the exported image or the RettsThumDriveCopy was verified, and the hash matches that of rettsThumb drive.

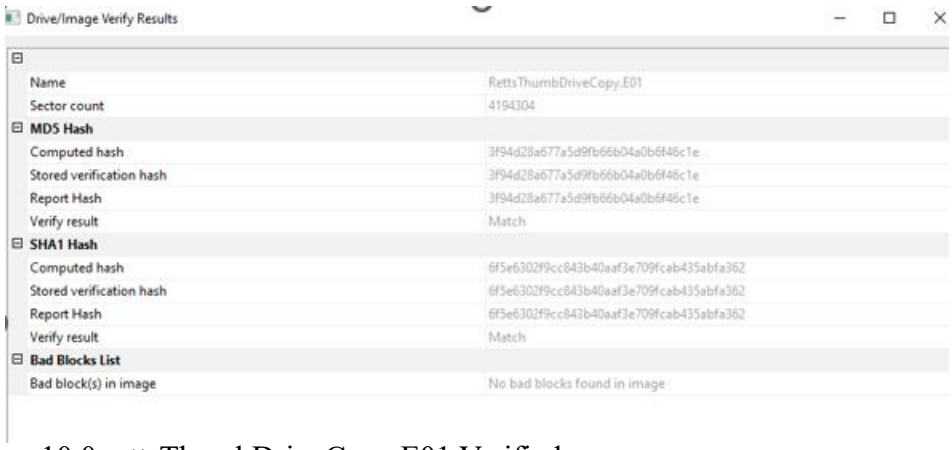



Figure 10.0 rettsThumbDriveCopy.E01 Verified

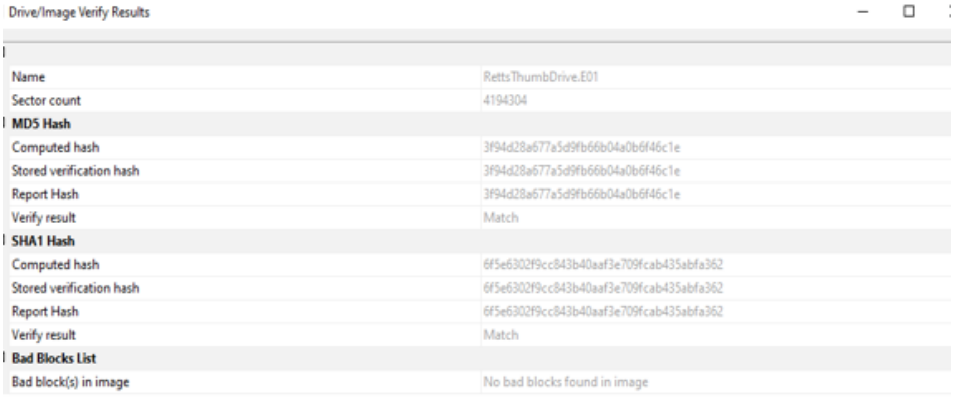



Figure 11.0 rettsThumbDrive.E01 Verified

```
Created By AccessData® FTK® Imager 4.7.1.2

Case Information:
Acquired using: ADI4.7.1.2
Case Number: C00102122026
Evidence Number: E00102122026
Unique description: Copy of RettsThumbDrive from Cybersecurity Center at UNCC
Examiner: Douglas
Notes: A copy image made on RettsThumbDrive from Cybersecurity Center at UNCC

--------------------------------------------------------------

Information for C:\Users\vboxuser\Desktop\Lab 1 Assignment\Analysis_ftk\Output\RettsThumbDriveCopy:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Verification Hashes]
 MD5 verification hash: 3f94d28a677a5d9fb66b04a0b6f46c1e
 SHA1 verification hash: 6f5e6302f9cc843b40aaf3e709fcab435abfa362
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 4,194,304
[Image]
 Image Type: E01
 Case number: A090425
 Evidence number: 1
 Examiner: Don Knotts
 Notes: This guy is guilty and he knows it!
 Acquired on OS: Win 201x
 Acquired using: ADI4.7.1.2
 Acquire date: 9/4/2025 3:09:24 PM
 System date: 9/4/2025 3:09:24 PM
 Unique description: A 2GB thumbdrive with a sticker "Rett's dont touch!"
 Source data size: 2048 MB
 Sector count:    4194304
[Computed Hashes]
 MD5 checksum:    3f94d28a677a5d9fb66b04a0b6f46c1e
 SHA1 checksum:   6f5e6302f9cc843b40aaf3e709fcab435abfa362

Image Information:
```

**Figure 12.0 shows the log of the exported rettsThumb image.**

6. **Do RettsThumb and rettcopy appear to be the same thumb drive? How are they similar and how are they different?**

**Answer:**

Even though both images appear to be from the same kind of 2 GB flash drive and have the same FAT16 file system, they are not exact replicas. Even while they have similar fundamentals, such as the size of the device and the format of the data, the real evidence is different. To begin with, their MD5 hashes are completely different. Beyond that, the labels are different. The rettsThumbDrive has a special note that reads, "A 2GB thumbdrive with a sticker that reads, 'Rett's do not touch!'" but the rettcopy simply has the label "untitled." However, the Autopsy shows that there are only 231 files in the rettcopy compared to around 27,970 in the rettsThumbDrive picture. Due to the number of files and artifacts, I can't say these are the same thumb drive in the same state.

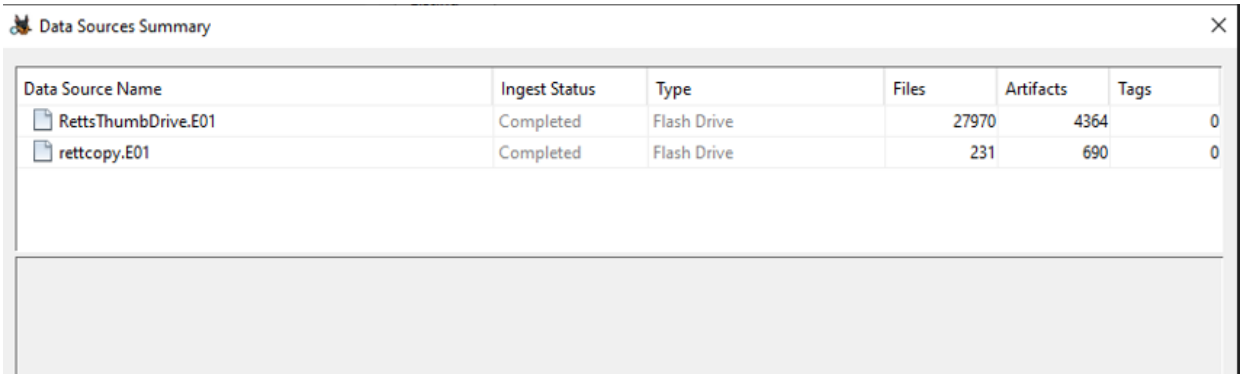



Figure 13.0 Autopsy summary showing 231 files for rettcopy and 27,970 for RettsThumbDrive

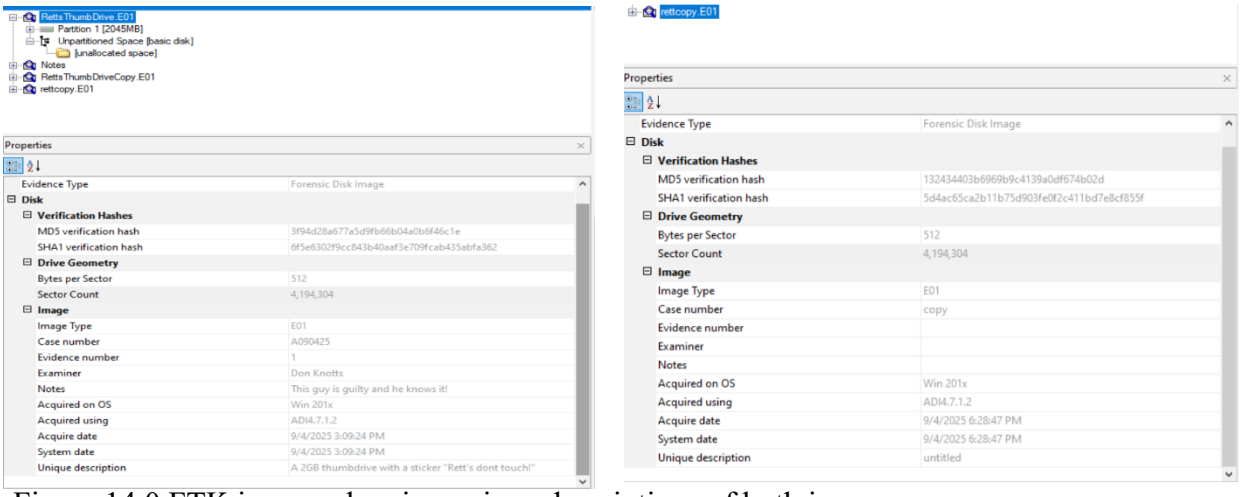



Figure 14.0 FTK imager showing unique descriptions of both images.

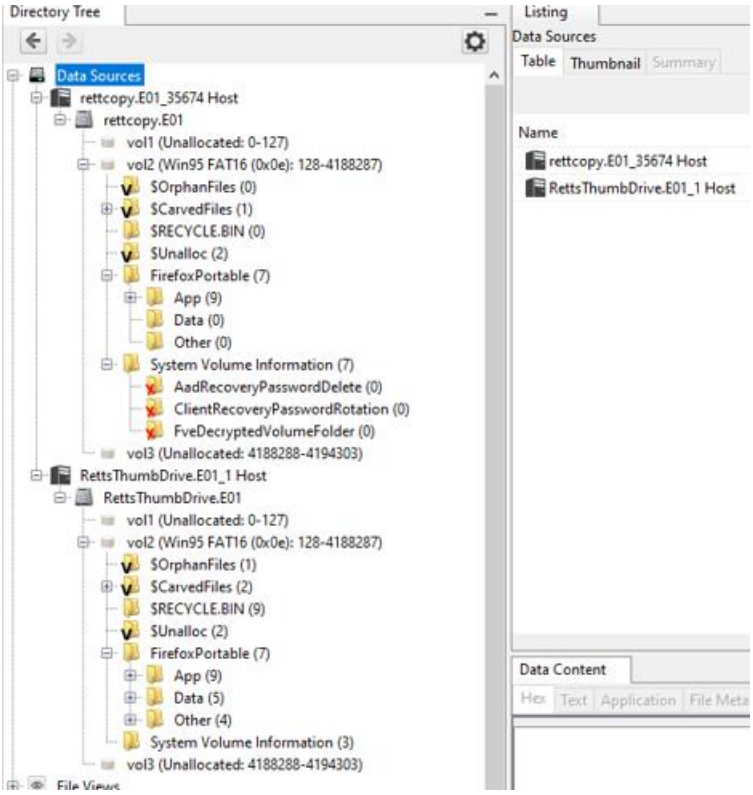



Figure 15.0 Autopsy directory tree showing that both rettcopy.E01and rettsThumbDrive.E01 have the same FAT16 file system.

**Conclusion**

The examination successfully verified the integrity of both forensic images. While RettsThumbDrive.e01 and rettcopy.e01 share similar physical geometry and file system types, the mathematical hash values, unique device identifiers, and vastly different file counts confirm they are distinct pieces of evidence. The re-acquisition of RettsThumbDrive was successful, maintaining perfect data integrity as proven by the matching MD5 hashes.

| Name | RettsThumbDrive.E01 |
|---|---|
| Sector count | 4194304 |
| **MD5 Hash** | |
| Computed hash | 3f94d28a677a5d9fb66b04a0b6f46c1e |
| Stored verification hash | 3f94d28a677a5d9fb66b04a0b6f46c1e |
| Report Hash | 3f94d28a677a5d9fb66b04a0b6f46c1e |
| Verify result | Match |
| **SHA1 Hash** | |
| Computed hash | 6f5e6302f9cc843b40aaf3e709fcab435abfa362 |
| Stored verification hash | 6f5e6302f9cc843b40aaf3e709fcab435abfa362 |
| Report Hash | 6f5e6302f9cc843b40aaf3e709fcab435abfa362 |
| Verify result | Match |
| **Bad Blocks List** | |
| Bad block(s) in image | No bad blocks found in image |

| Name | rettcopy.E01 |
|---|---|
| Sector count | 4194304 |
| **MD5 Hash** | |
| Computed hash | 132434403b6969b9c4139a0df674b02d |
| Stored verification hash | 132434403b6969b9c4139a0df674b02d |
| Report Hash | 132434403b6969b9c4139a0df674b02d |
| Verify result | Match |
| **SHA1 Hash** | |
| Computed hash | 5d4ac65ca2b11b75d903fe0f2c411bd7e8cf855f |
| Stored verification hash | 5d4ac65ca2b11b75d903fe0f2c411bd7e8cf855f |
| Report Hash | 5d4ac65ca2b11b75d903fe0f2c411bd7e8cf855f |
| Verify result | Match |
| **Bad Blocks List** | |
| Bad block(s) in image | No bad blocks found in image |

Figure 16.0 MD5 hashes of both RettsThumbDrive.E01 and rettcopy.E01verified after the analysis

**Douglas Akwasi Kwarteng**

Forensic Student