ITIS 4250 / 5250

Shivani Sathe

Lab # 1

24th September 2021

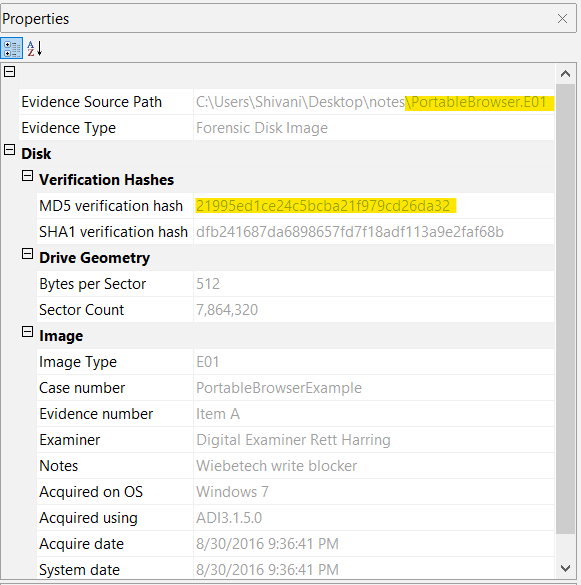
**Overview:**

On September 18th, 2021, Dr. Robert Quincy, Chief Forensics Examiner at the UNCC Forensics Laboratory, had asked me to perform technical work on a forensics image. 2 forensic images of a thumb drive namely, PortableBrowser.e01 and CoffeeShopThumb.E01 were provided by Cybersecurity Center at UNCC for examination. Dr. Robert Quincy has determined that to further the investigation, a forensic analysis to include verification of a forensics image to determine whether the 2 images are of the same thumb drive or not be performed on the submitted evidence. Also, as per The University Attorney, the original device was abandoned property and no legal authority is required.

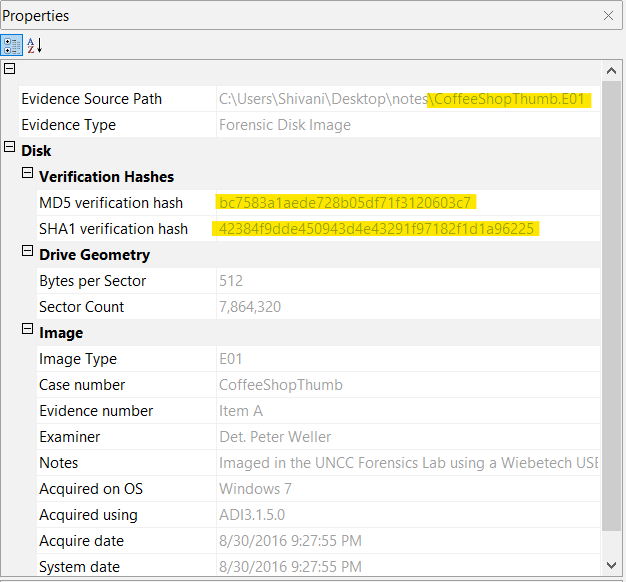
**Forensic Acquisition & Exam Preparation**

To begin the analysis, Windows 10, 64-bit system with 8GB RAM was used with. The two forensic image files PortableBrowser.e01 and CoffeeShopThumb.E01 were placed in a newly created folder named ‘**notes**’ on desktop. Later, FTK Imager 4.5.0.3 was used to load both the images to view the file systems each disk was formatted with, their original size, volume names and top-level directories. MD5 hash was noted after loading the image and the has value was verified before starting and after the analysis.

Hash of PortableBrowser.e01 after loading image:

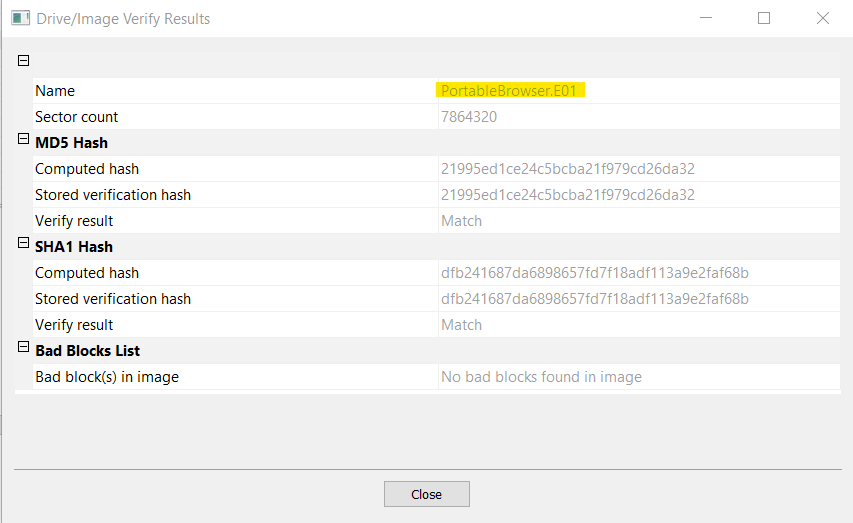


Hash of CoffeeShopThumb.E01 after loading image:

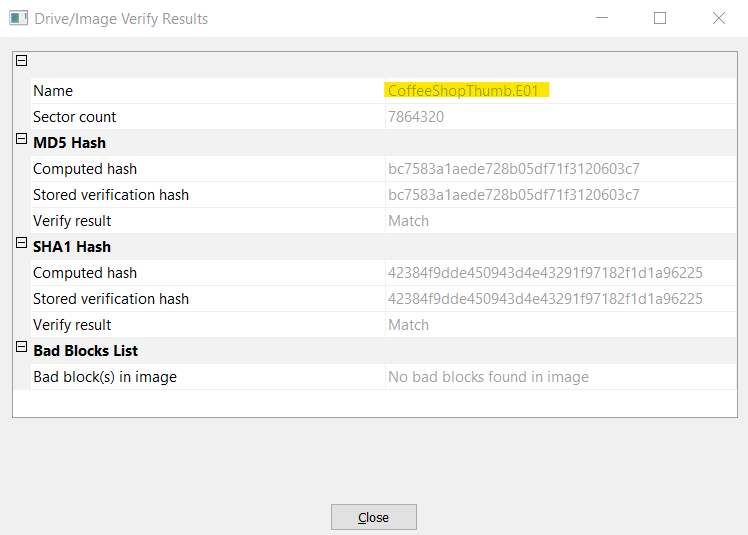


**Before beginning the analysis, it was ensured that both the image files were verified.**

Hash of PortableBrowser.e01 after verification:

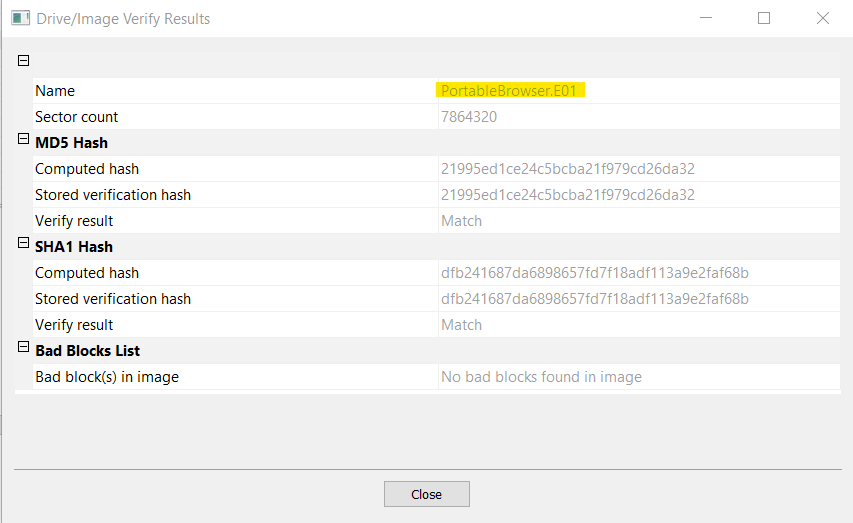


Hash of CoffeeShopThumb.E01 after verification:

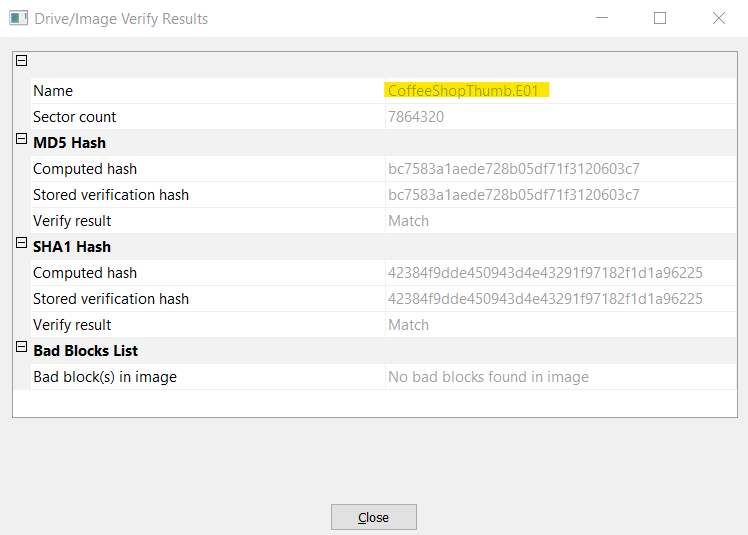


**After completing the analysis:**

Hash of PortableBrowser.e01 after verification:



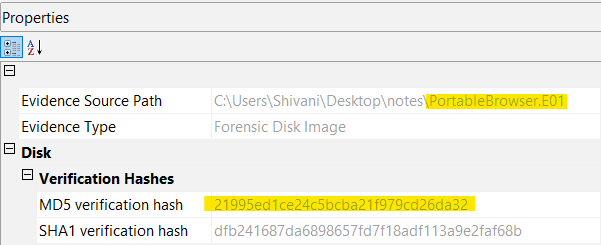
Hash of CoffeeShopThumb.E01 after verification:



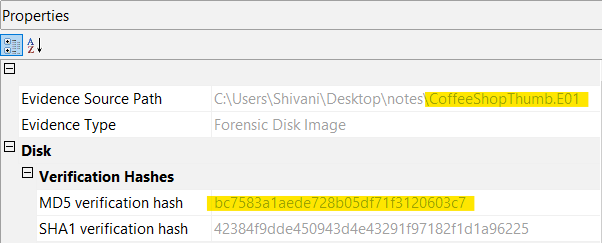
**Findings and Report (Forensic Analysis)**

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

* **Hash of PortableBrowser.e01 is 21995ed1ce24c5bcba21f979cd26da32**
* **This MD5 hash value is found in the ‘Properties’ tab of FTK Imager after loading the forensic image file ‘PortableBrowser.e01’ and selecting it.**

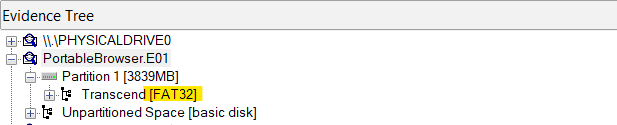


* **Hash of CoffeeShopper is bc7583a1aede728b05df71f3120603c7**
* **This MD5 hash value is found in the ‘Properties’ tab of FTK Imager after loading the forensic image file ‘CoffeeShopper’ and selecting it.**



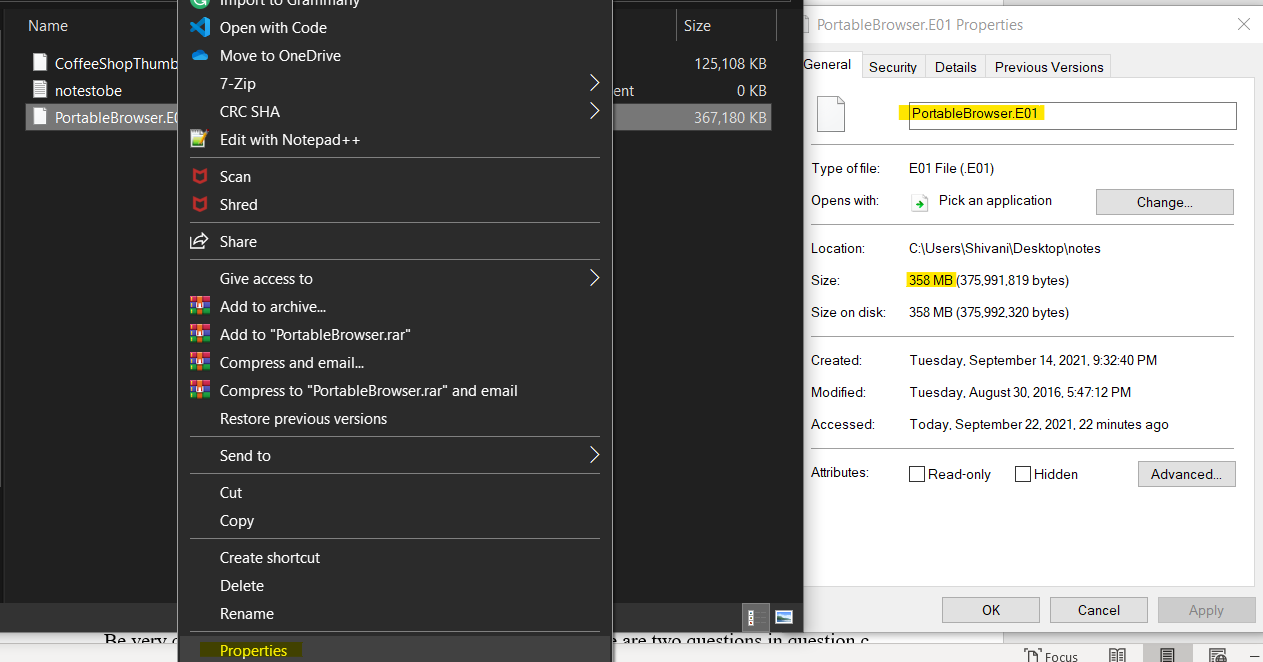
1. **What file systems are present within PortableBrowser.e01? (FAT32, NTFS, EXT3, Reiser, ZFS, UDF, etc)**

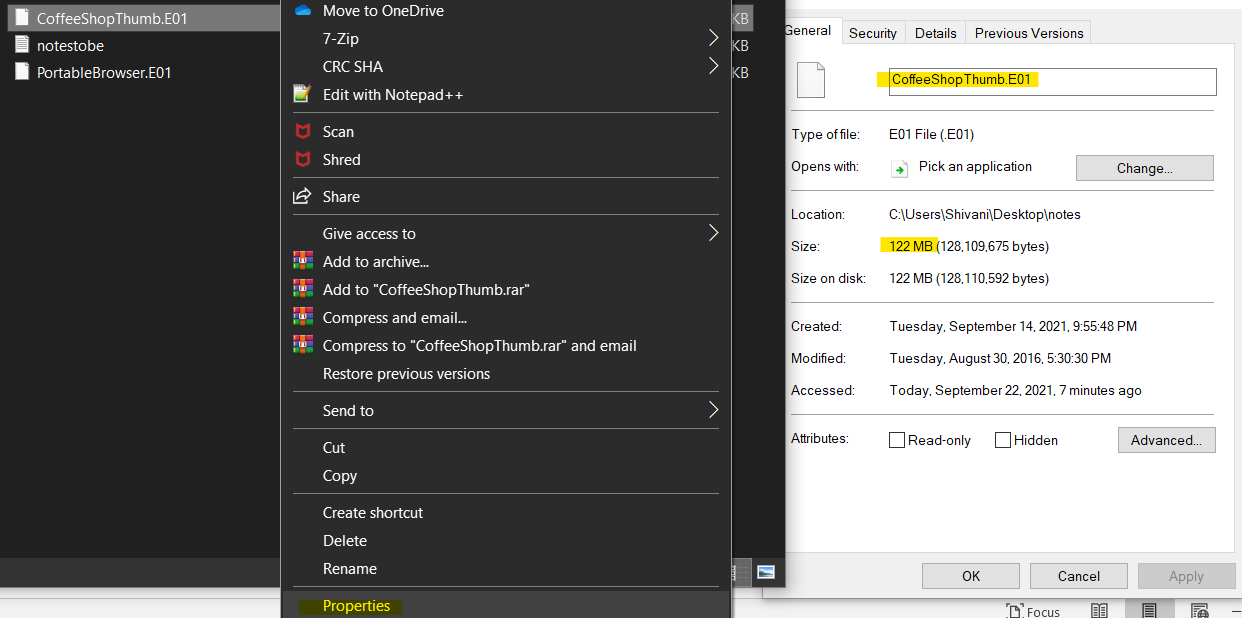
* **The file system present in ‘PortableBrowser.e01’ is FAT32.**
* **To find the file system, the forensic image ‘PortableBrowser.e01’ was loaded in FTK imager. The image file was expanded using ‘+’ icon to browse through the volume levels and it was found that the file had 1 Partition. Upon expanding the partition, it was observed the image files has only 1 files system present which is FAT32.**

****

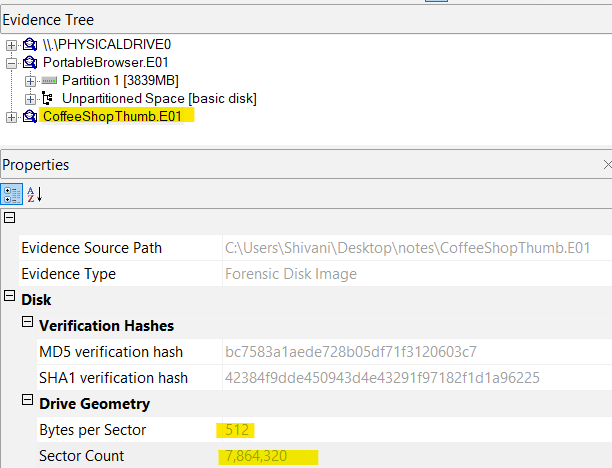
1. **What are the file size for PortableBrowser.e01 and CoffeeShopper.e01, and what was the size of the original device (hard drive) that PortableBrowser.e01 is imaged from? How about CoffeeShopper?**

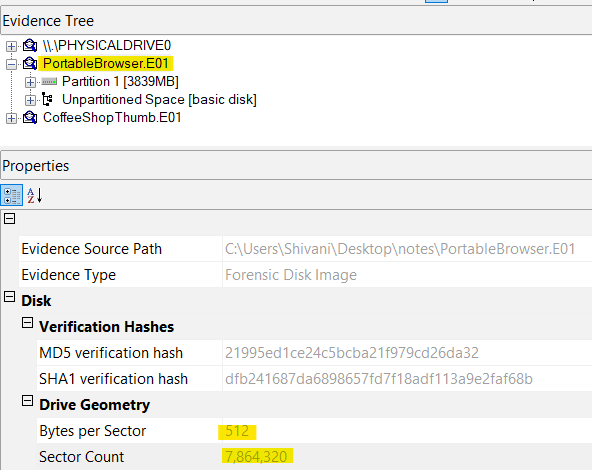
* **The file size of PortableBrowser.e01 is 358 MB**
* **The file size of CoffeeShopper is 122 MB**
* **A folder named ‘notes’ was created comprising of the above two files. To find the file size, the properties were checked of both the files by right clicking on them.**

****



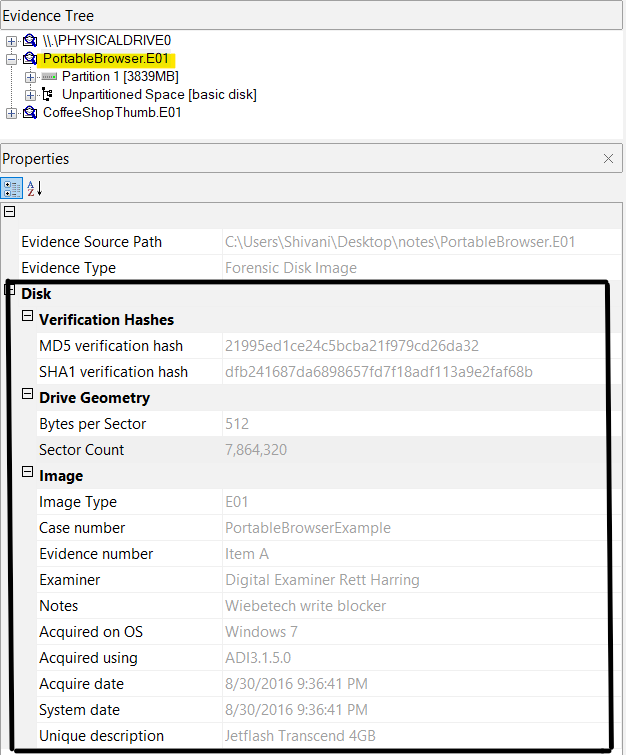
* **The hard drive is logically divided into sectors of data. Original size is found by multiplying “Bytes per sector” with “Sector Count”. These can be found in properties tab of both the image file once the files are loaded and selected.**
* **512 \* 7,864,320 = 4,026,531,840 Bytes ~ 3.75 GB.**
* **The hard drive size is same for both image files.**

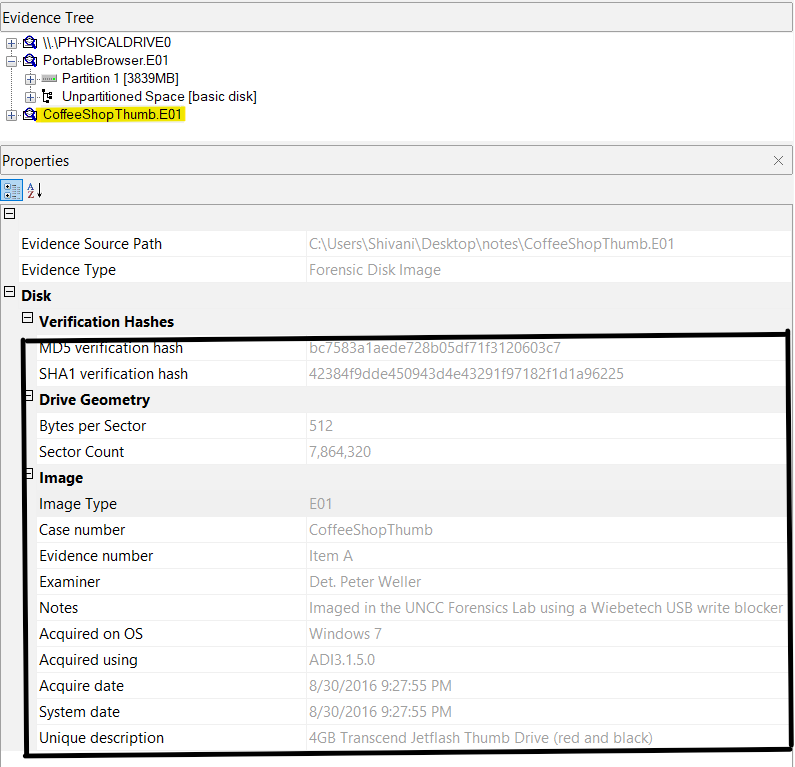


****

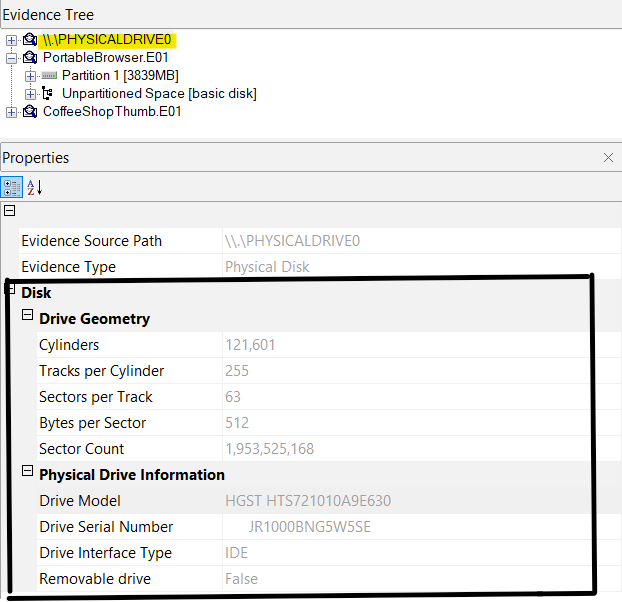
1. **How are an image and a physical drive different as they appear in FTK Imager? (specifically about the details of their appearance/labeling in FTK Imager)?**

* **For an Image file, in properties tab, there is a MD5 and SHA1 hash value and in drive geometry tab there are only two fields- Bytes per Sector and Sector Count.**
* **It has Image information Tab which gives details of like Image type, Case number, Evidence number, Examiner name, OS on which it was acquired from, Tool with which is was acquired, Acquire and System date and Unique description that gives information about the thumb drive name and size.**

****

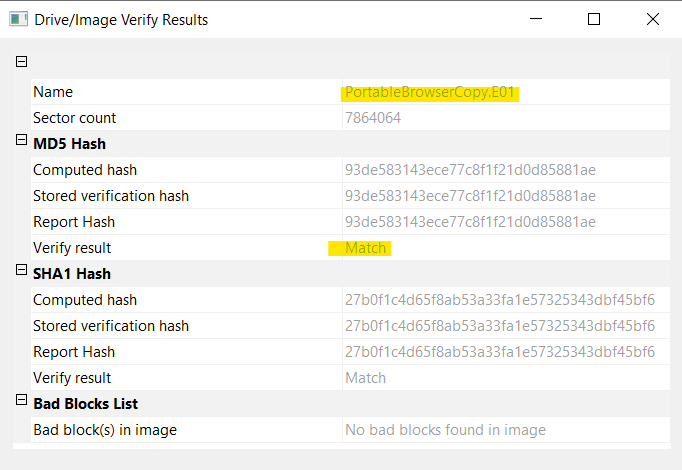
****

* **For a Physical drive, there is no hash value. The Drive Geometry contains more fields of detailed information compared to image file which comprises of Cylinders, Tracks per Cylinders, Sectors per Track, Bytes per Sector and Sector Count.**
* **It contains Physical Drive information such as Drive model, Serial number, its interface type and weather or not its removable.**

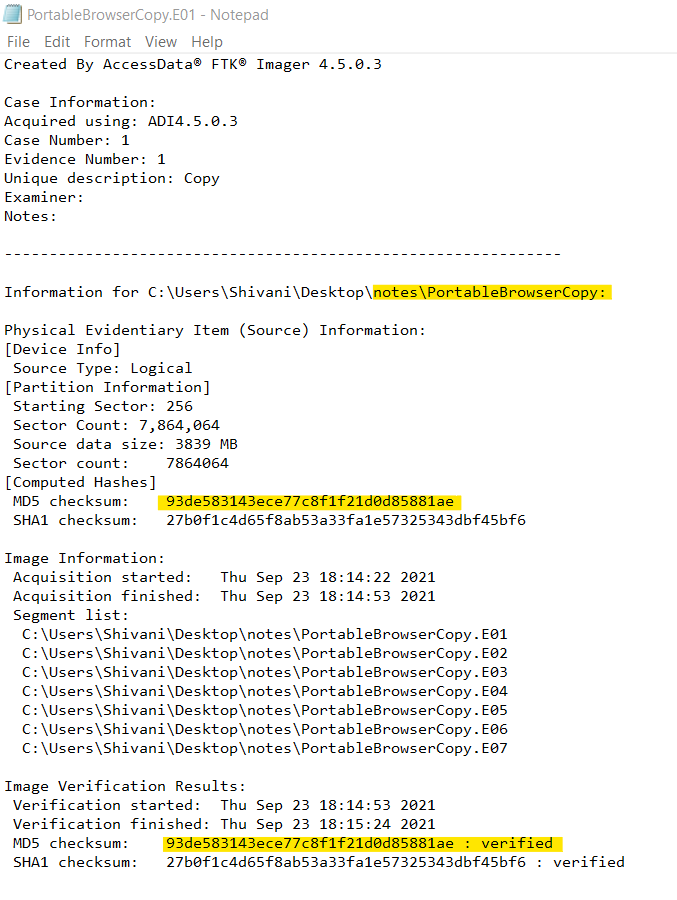


1. **Did FTK imager generate a log for the image you created out of PortableBrowser? Does this hash value match the original?**

* **Yes, FTK Imager generated log for the image and the hash value also matched the original hash value.**

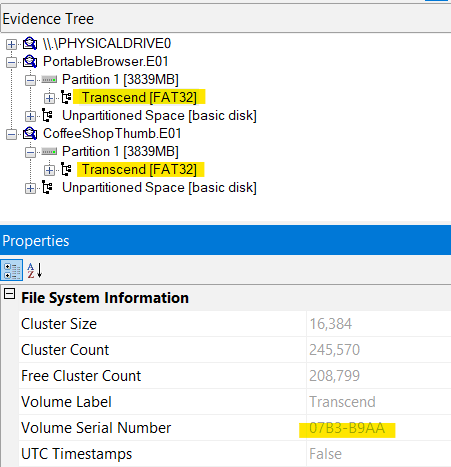
****

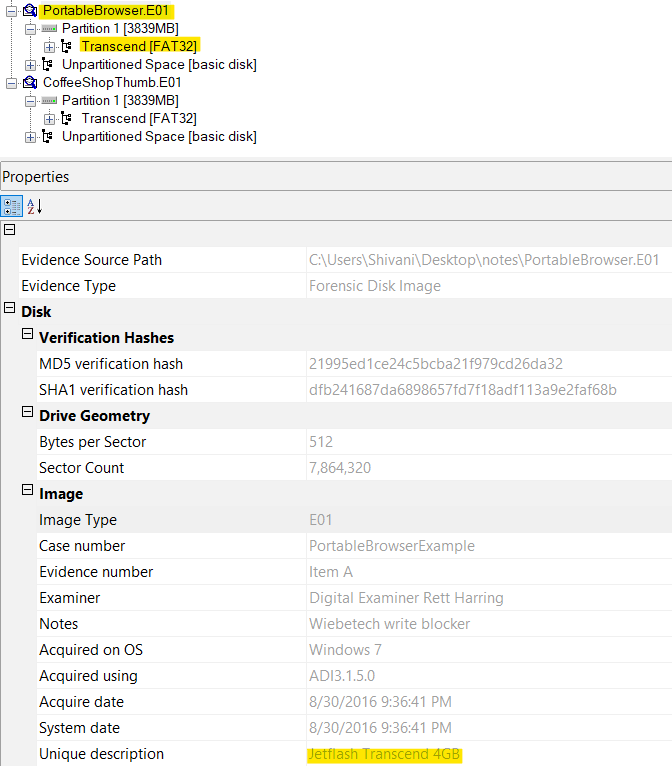
* **The destination of log file was selected as the ‘notes’ folder where the PortableBrowser image file was kept initially.**

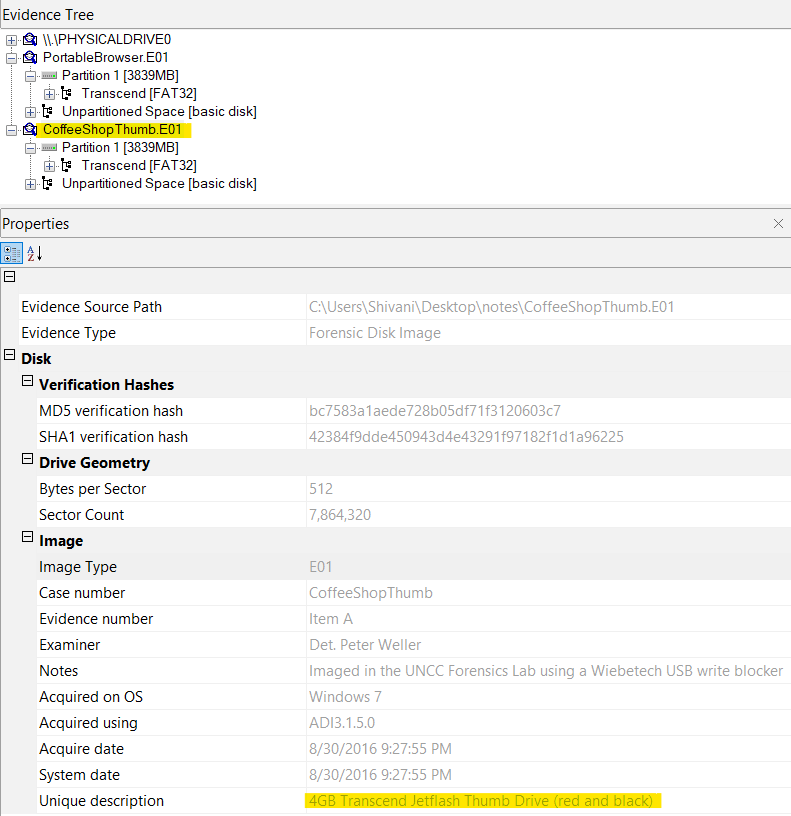
****

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

* **PortableBrowser and CoffeeShopper both appear to be the same thumb drive.**
* **This is because when clicked on the filesystem ‘Transcend [FAT32]’ of both the images, there is a Volume Serial Number in in the ‘Properties’ tab which is same for both image files.**
* **Volume Serial number is a unique value that is assigned whenever a new file system is created.**
* **Also, when selected the image files, under properties, the field of ‘Unique Description’ of both the image files states the thumb drive description to be Jetflash Transcend 4GB.**

****

****

****

**Conclusion:**

To sum up, in this lab it was asked to verify if the two forensic images ‘PortableBrowser.e01’ and ‘CoffeeShopThumb.E01’ which were provided by Cybersecurity Center at UNCC were of the same thumb drive or not. To begin the analysis, the images were loaded using FTK Imager 4.5.0.3 on a Windows 10 Machine. All the questions regarding this case were successfully answered with the help of FTK Imager tool. At the end of analysis, it was found that the 2 images were of same thumb drive as both images have same Volume Serial Numbers and Unique Description. No evidence has been retained. The forensic image, and answered questions regarding it, were returned to Dr. Robert Quincy.