ITIS 5250
Sneha Rangari
Lab 2
10/02/2018

Overview:

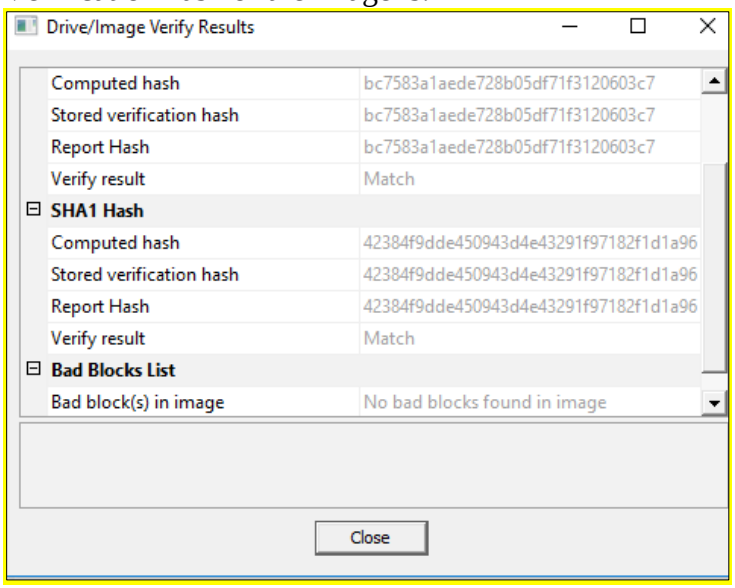
In this Lab, I have been given two files, namely "CoffeeShopThumb.E01" and "PortableBrowser.E01". I have been asked to make use of the "FTK Imager Tool" and "SQL Lite Browser" to examine geometry and folder structure of both the images and answer questions like the date and time when a particular image was accessed, location of that image, my views on whether both the images are of the same thumb drive, etc.

Forensic Acquisition & Exam Preparation:

I accessed the Forensic images in the Shared Folder on the network from the Forensics Lab in Cone 169. , I accessed images named 'CoffeeShopThumb.E01' and 'PortableBrowser.E01' and their log files. The software used for accessing & extracting information from the image is FTK Imager 4.1.1.1 The first step undertaken after accessing the image files was the Hash verification along with description of two images from txt files.

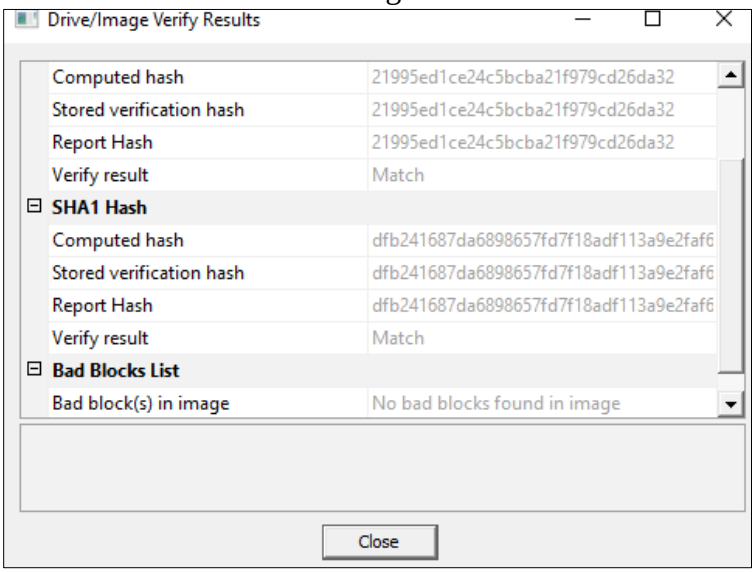
CoffeeShopThumb.E01:

Acquired on OS: Windows 7
Acquired using: ADI3.1.5.0
Acquired date: 8/30/2016 9:27:55 PM
System date: 8/30/2016 9:27:55 PM
Unique description: 4GB Transcend Jetflash Thumb Drive (red and black)
Verification hash of the image is:



PortableBrowser.E01:

Acquired on OS: Windows 7
Acquired using: ADI3.1.5.0
Acquired date: 8/30/2016 9:36:41 PM
System date: 8/30/2016 9:36:41 PM
Unique description: Jetflash Transcend 4GB
Verification hashes of the image is:

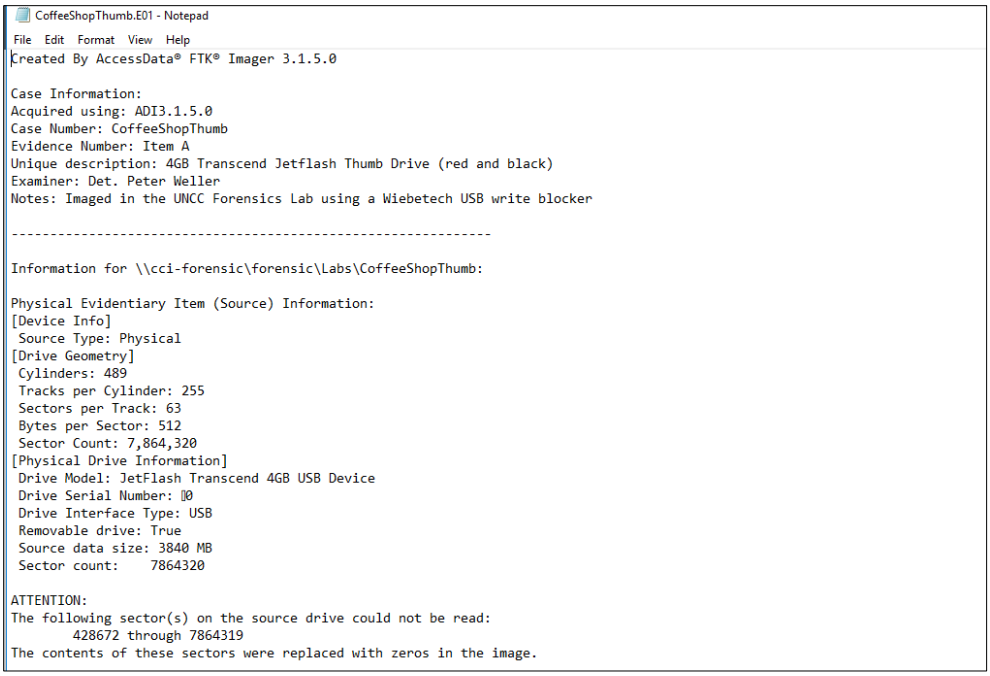


Findings and Report (Forensic Analysis):

1. a. Judging by geometry, hash value, folder structure and the log files do these images appear to be of the same thumb drive? How are they similar and how are they dissimilar?

The geometry of both these images verified by tracks per cylinder, Sectors per track, Bytes per sector, Sector count and physical drive information and thus they are identical which is evident from their log files given as CoffeeShopThumb.E01.txt and PortableBrowser.E01.txt. There are two computed hashes of each image. i.e. MD5 and SHA1 as shown in Forensic Acquisition & Exam Preparation section.

CoffeeShopThumb.E01:

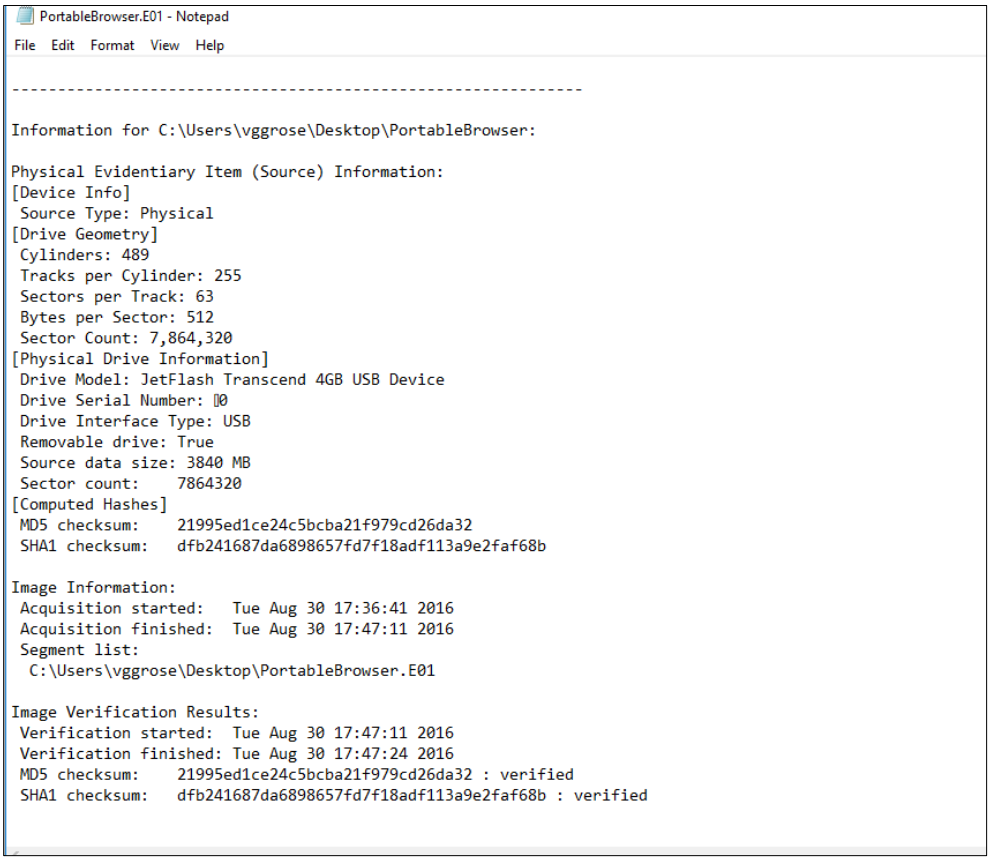


CoffeeShopThumb.E01 - Notepad

File Edit Format View Help

```
Created By AccessData® FTK® Imager 3.1.5.0

Case Information:
Acquired using: ADI3.1.5.0
Case Number: CoffeeShopThumb
Evidence Number: Item A
Unique description: 4GB Transcend Jetflash Thumb Drive (red and black)
Examiner: Det. Peter Weller
Notes: Imaged in the UNCC Forensics Lab using a Wiebetech USB write blocker

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

Information for \\cci-forensic\forensic\Labs\CoffeeShopThumb:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 489
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 7,864,320
[Physical Drive Information]
 Drive Model: JetFlash Transcend 4GB USB Device
 Drive Serial Number: 0
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 3840 MB
 Sector count:    7864320

ATTENTION:
The following sector(s) on the source drive could not be read:
       428672 through 7864319
The contents of these sectors were replaced with zeros in the image.
```

PortableBrowser.E01:

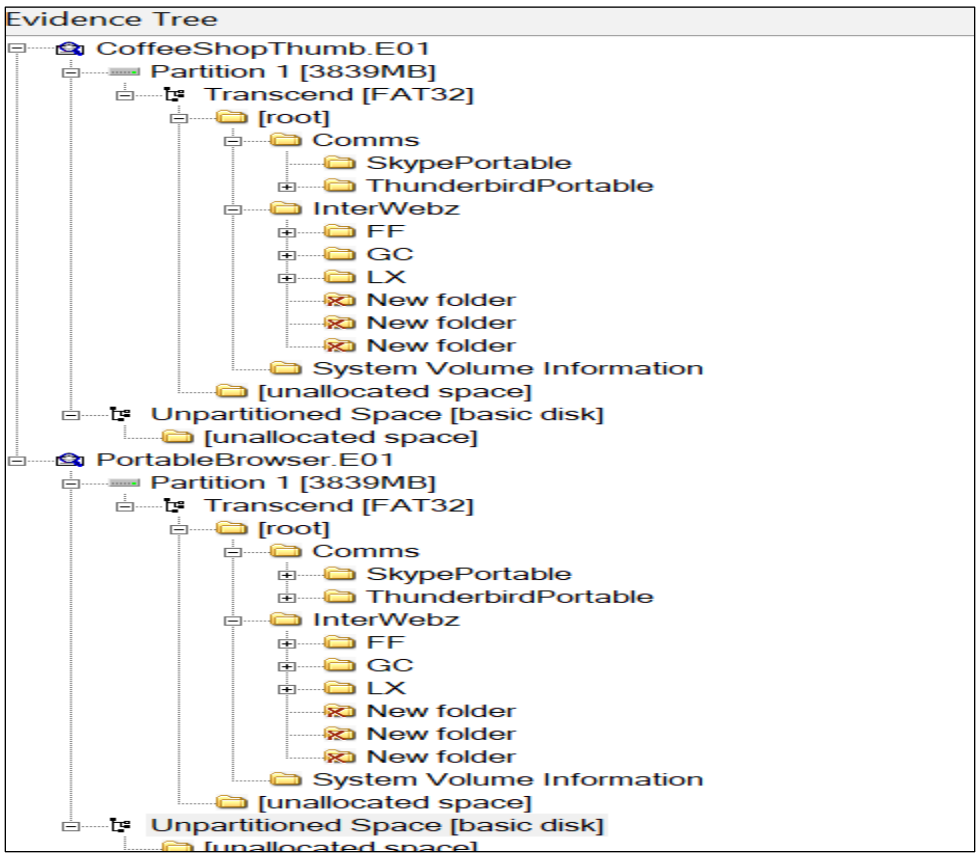


PortableBrowser.E01 - Notepad

File Edit Format View Help

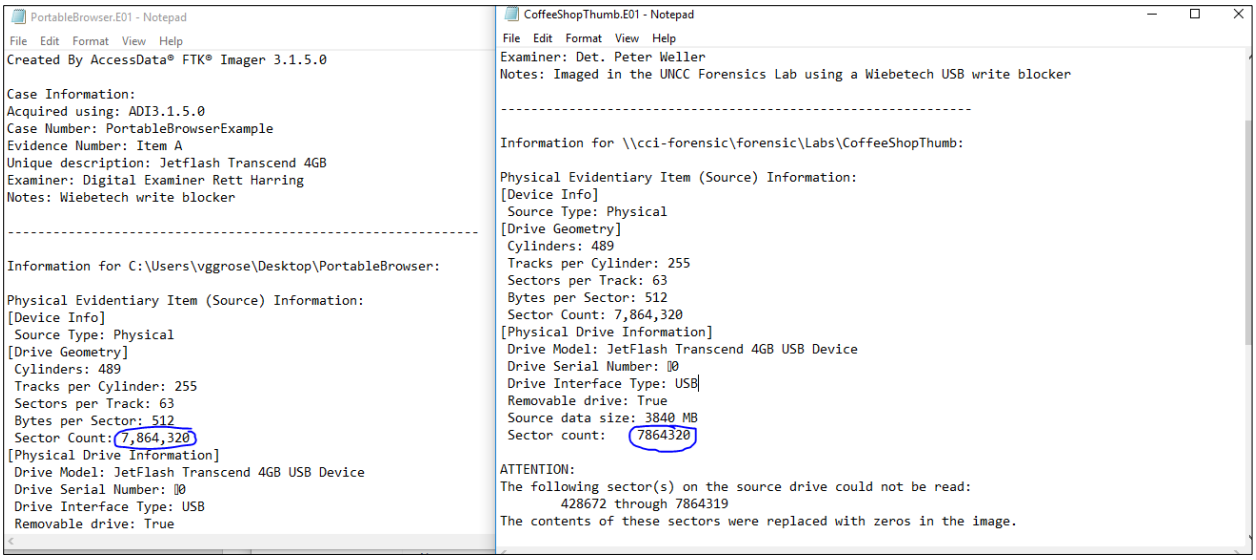
```
------------------------------------------------------------

Information for C:\Users\vggrose\Desktop\PortableBrowser:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 489
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 7,864,320
[Physical Drive Information]
 Drive Model: JetFlash Transcend 4GB USB Device
 Drive Serial Number: 0
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 3840 MB
 Sector count:    7864320
[Computed Hashes]
 MD5 checksum:    21995ed1ce24c5bcba21f979cd26da32
 SHA1 checksum:   dfb241687da6898657fd7f18adf113a9e2faf68b

Image Information:
 Acquisition started:   Tue Aug 30 17:36:41 2016
 Acquisition finished:  Tue Aug 30 17:47:11 2016
 Segment list:
  C:\Users\vggrose\Desktop\PortableBrowser.E01

Image Verification Results:
 Verification started:  Tue Aug 30 17:47:11 2016
 Verification finished: Tue Aug 30 17:47:24 2016
 MD5 checksum:    21995ed1ce24c5bcba21f979cd26da32 : verified
 SHA1 checksum:   dfb241687da6898657fd7f18adf113a9e2faf68b : verified
```

Folder Structure:

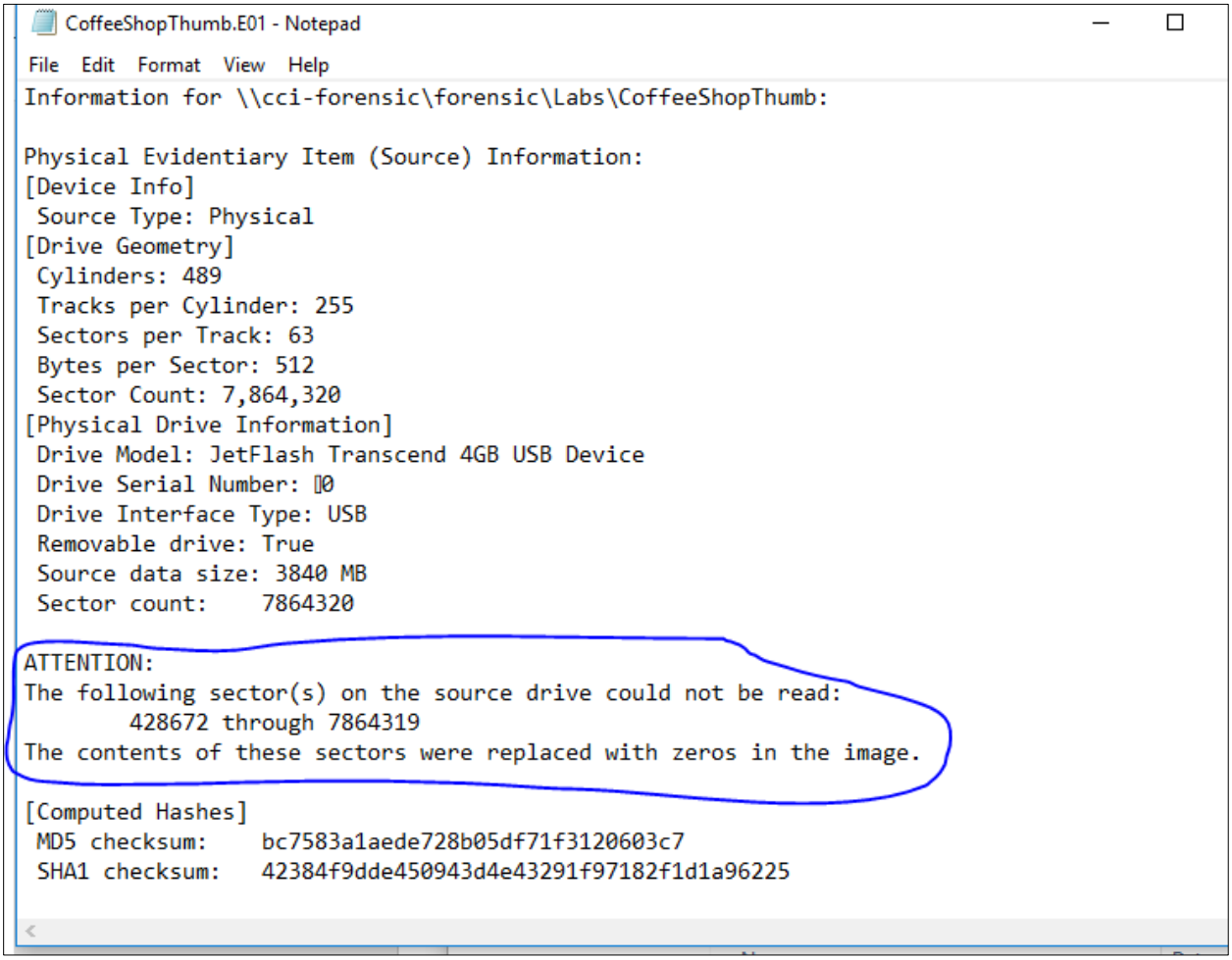


Moreover, both these images have same partition of 3839MB and their file system is FAT32.
The folder structure of both the images is very similar except some differences where some content is missing in the "CoffeeShopThumb.E01". The content which is missing/empty in the image, is all zeros and its log file tells us that the content from the unreadable sectors was replaced by zeros. Thus, I infer that the content that is missing/empty is from the bad sectors. So, I can say that both images appear to be of the same thumb drive as unique description is also having same for both images as Jetflash Transcend 4GB.

b. How many sectors do each of the images represent in total? Are there any errors showing one image did not record some of the sectors?

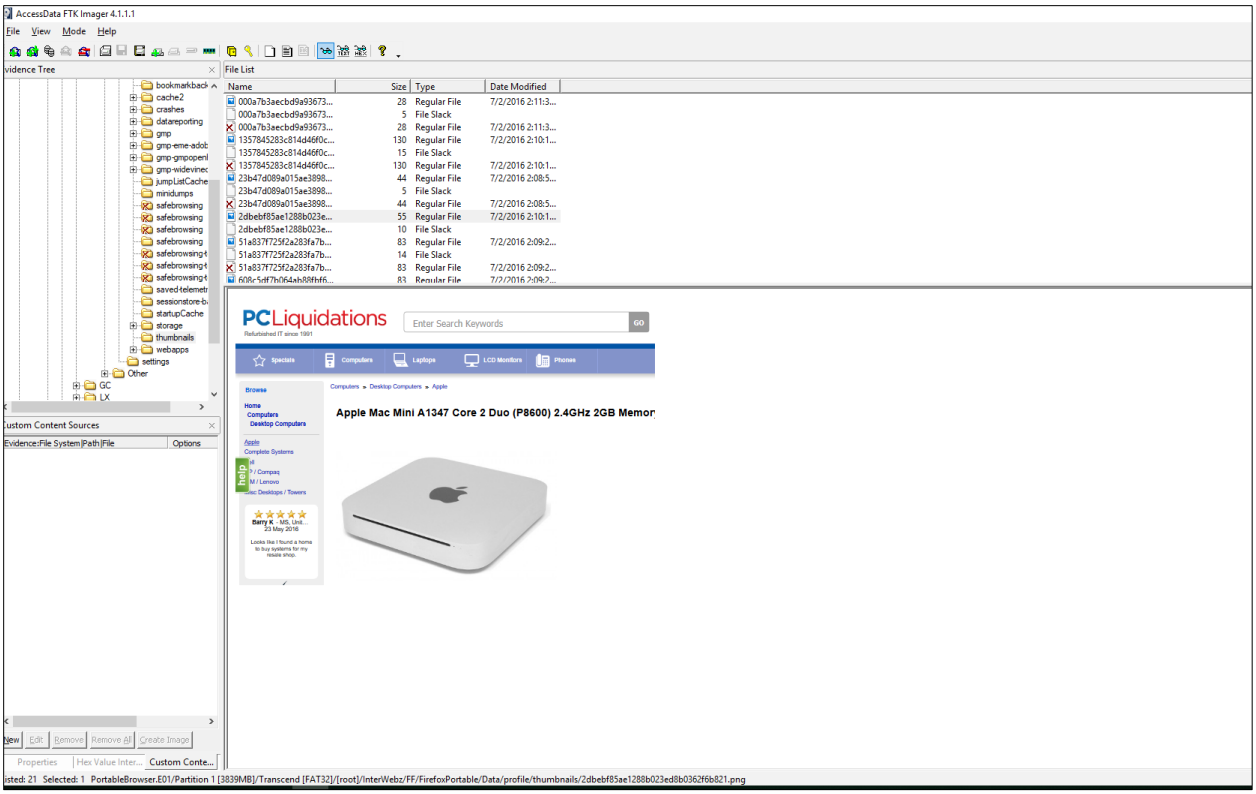


The sector count of each image is **7,864,320**. So, in total their sector count is **15,728,640**. But 'CoffeeShopThumb.E01' did not record some of the sectors from 428672 to 7864319 could not be read and were replaced by zeros in the image.



c. Can you locate the following picture and where did you find it?

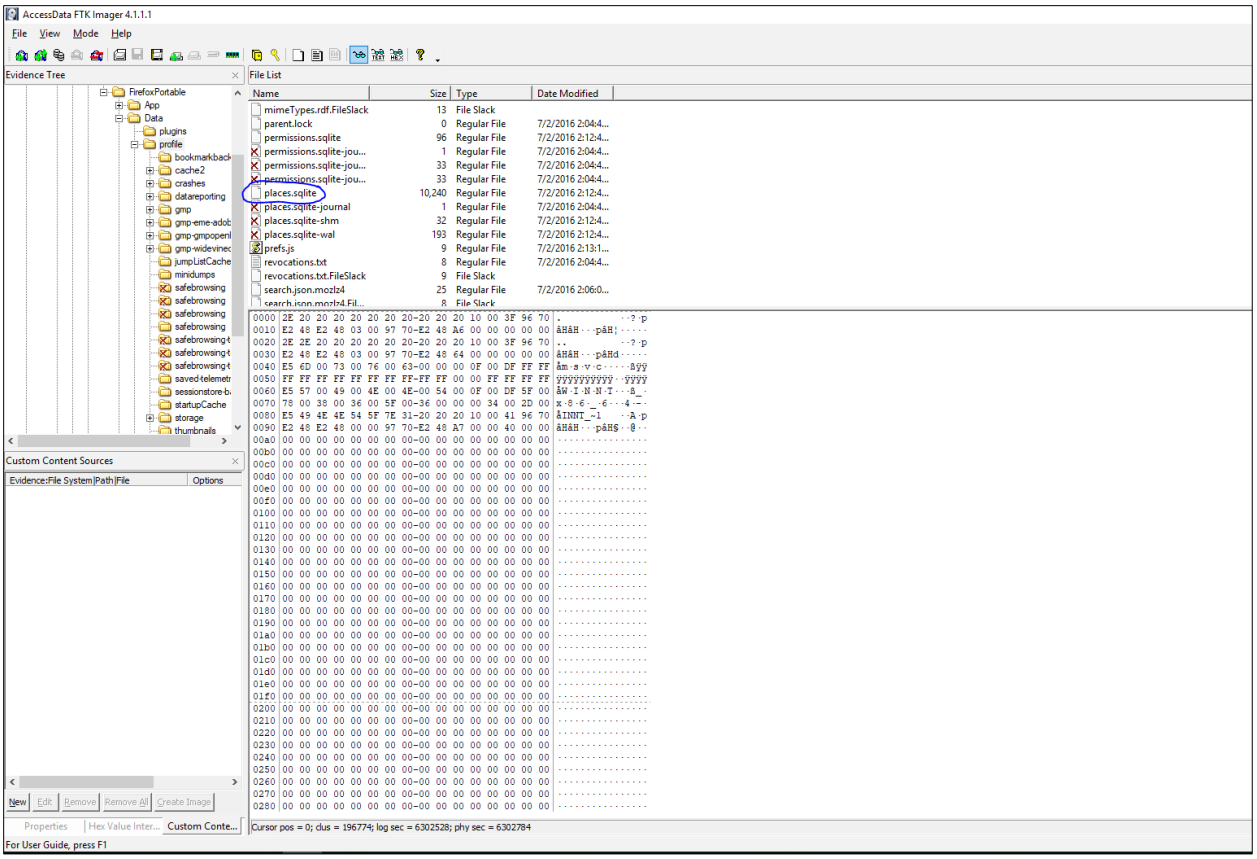
After checking the spreadsheet for PNG files, I found file (highlighted in the image below) with this picture.
The path is:
Partition 1\Transcend [FAT32]\[root]\InterWebz\FF\FirefoxPortable\Data\profile\thumbnails\2dbebf85ae1288b023e.png



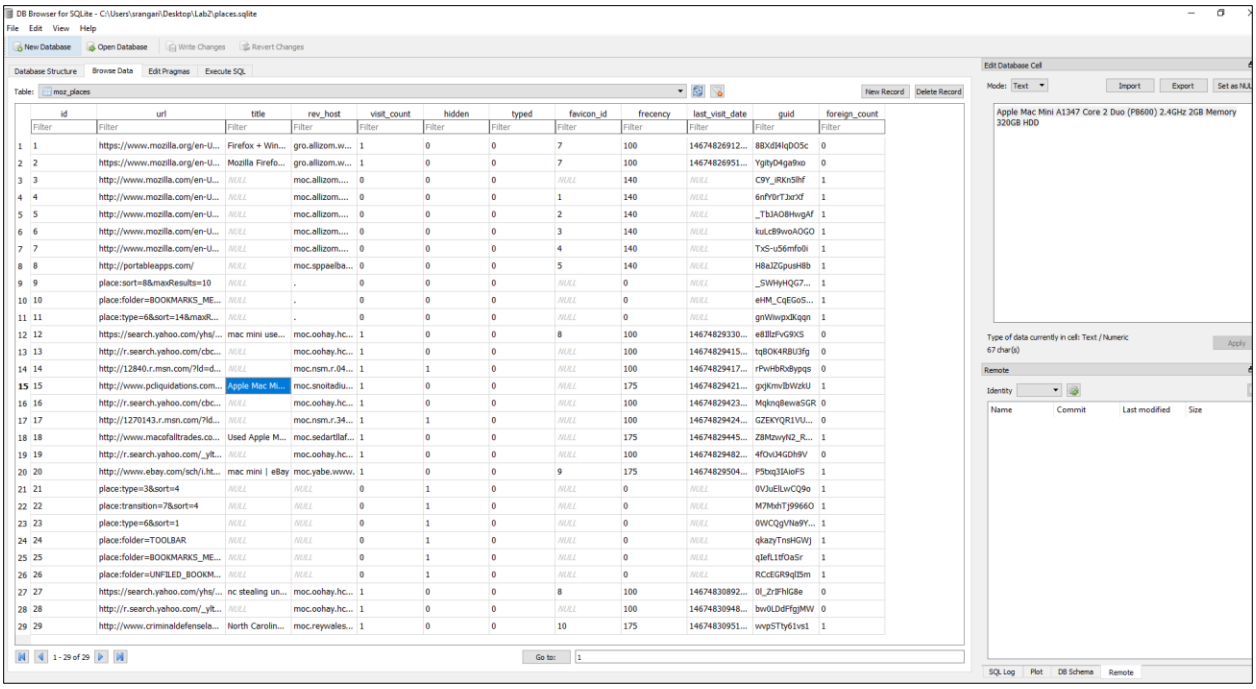
2. Ensure you have SQL Lite Browser installed (www.sqlitebrowser.org) and find the places.sqlite file from the Firefox portable \Interwebz\FF\Data\Profile\. Open the file with SQLite and select the Browse tab. Find the moz_places table and then locate the visited page with this title "Apple Mac Mini A1347 Core 2 Duo (P8600) 2.4GHz 2GB Memory 320GB HDD".

a. When was this page accessed? The date is in epoch format and will need to be converted (try www.epochconverter.com).

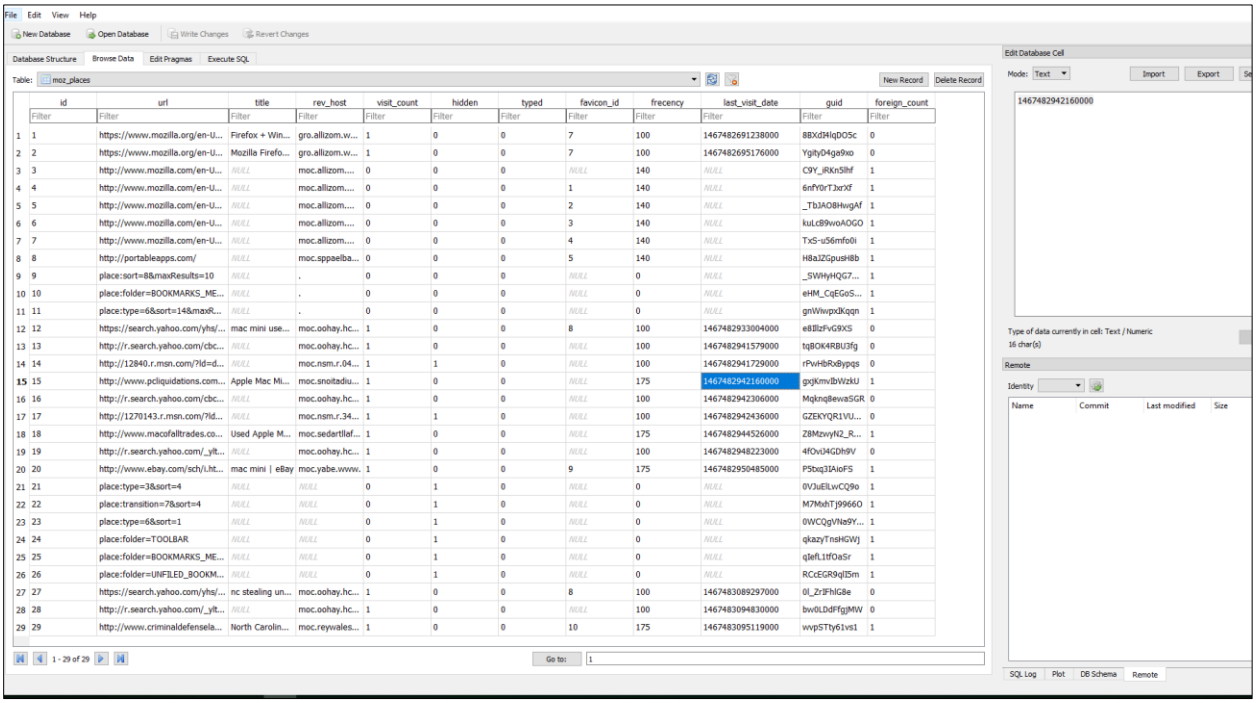
Now, after installing SQL Lite browser, I opened 'places.sqlite' file from the following location of PortableBrowser.E01: InterWebz \ FF \ FirefoxPortable \ Data \ profile

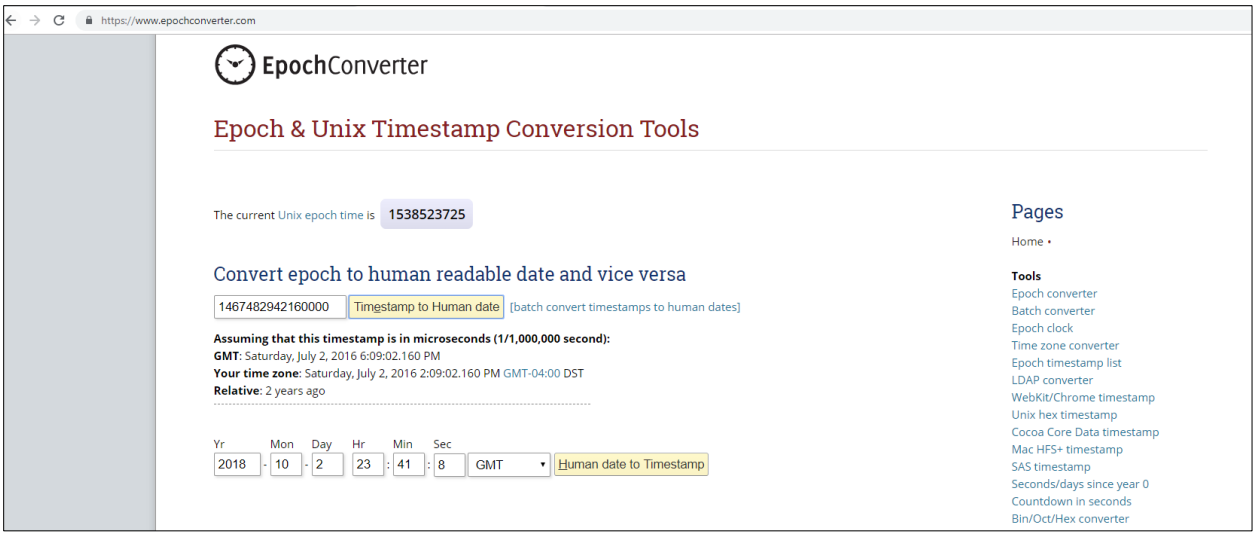


After opening it up in SQLite browser, selecting moz_places from the Browse tab, I located the page with the title – “Apple Mac Mini A1347 Core 2 Duo (P8600) 2.4GHz 2GB Memory 320GB HDD”.
The page was accessed on the website www.pcliquidations.com



The Epoch time of the last accessed time of the page is – “1467482942160000”





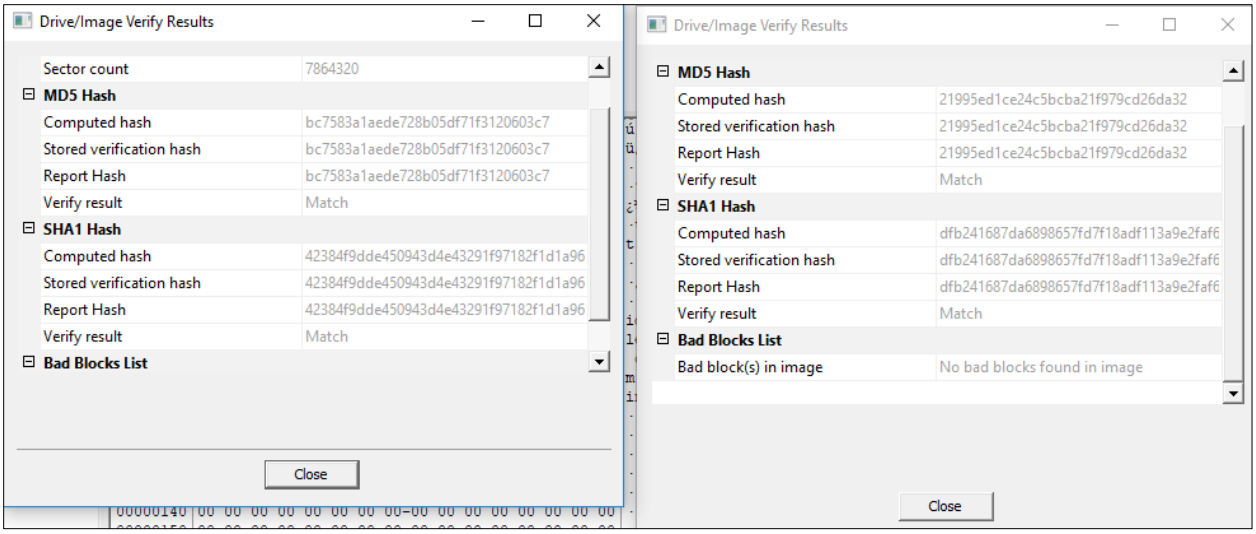
This date is in epoch format, so I converted it to Human readable format by visiting www.epochconverter.com .

The conversion of Epoch time to GMT as shown in the image above, 1467482942160000 comes to GMT: Saturday, July 2, 2016 6:09:02.160 PM.

3. Verify the images once more to ensure you have not altered them.

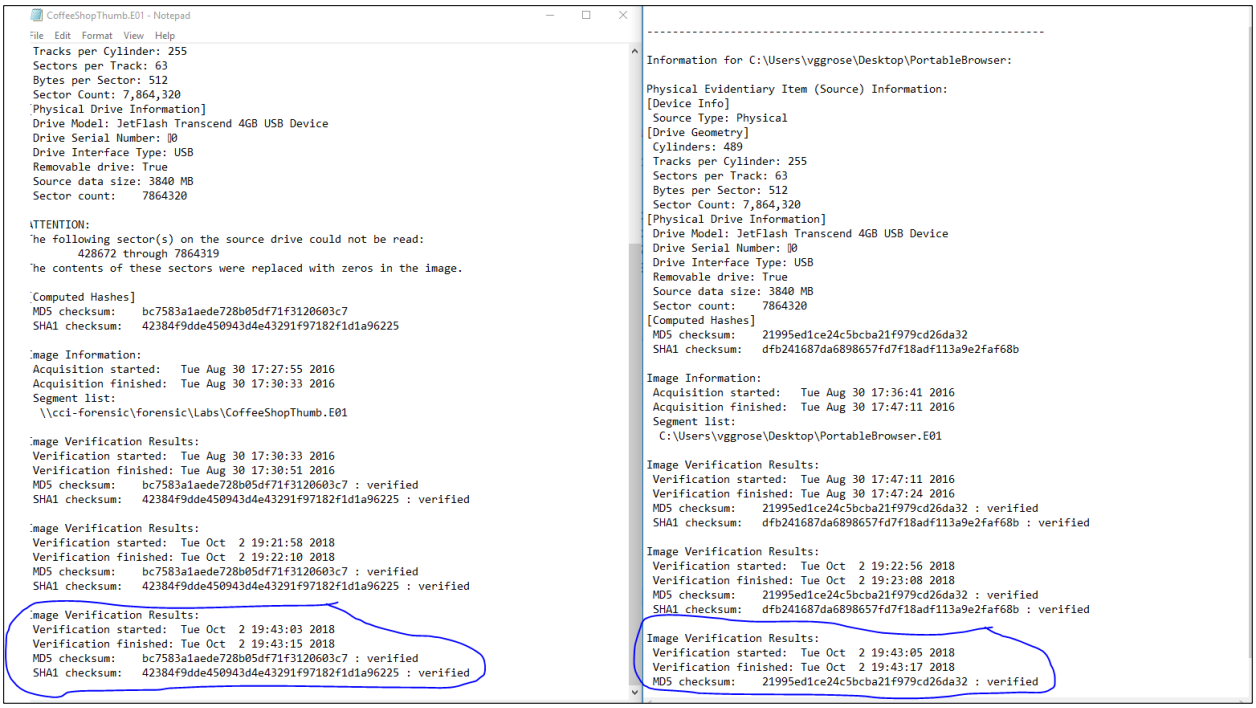
a. Was a record added to your log file to show you verified the image?

Verification results for both the images shows that they are not altered.



Thus I verified the images again after performing all the operations to make sure that the images were not modified. As seen from both the MD5 Hash verifications, none of the images were altered.

Also records are added to log files of both the images as shown.



Conclusion:

After obtaining and verifying the forensic images, I performed various operations using FTK Imager Tool to find information like the Hash verification of the Forensic Images, examining folder structure and log files, check the sector count, locating a picture file, extracting "places.sqlite" and examining it using SQL Lite Browser, and rechecking the log files for entries. The integrity of images provided was successfully verified by comparing the hash values.
The information I found was as follows:
1. Both the images are of a drive having same size and make (Transcend).
2. MD5 Hash values of both images are different.
3. Some sectors from CoffeeShopThumb.E01 were not read by the tool and the content was replaced by zeros.
4. The folder structure of the drives is the same except where some content is missing in the "CoffeeShopThumb.E01"
5. Location of the given image is
Partition 1\Transcend[FAT32]\[root]\InterWebz\FF\FirefoxPortable\Data\profile\thumbnails\2dbebf85ae1288b023e.png
6. Using SQLite browser, selecting moz_places from the Browse tab, "Apple Mac Mini A1347 Core 2 Duo (P8600) 2.4GHz 2GB Memory 320GB HDD" was found. The page was accessed from the website www.pcliquidations.com on July 2nd 2016.
7. Conversion of epoch format to human readable format.
8. Verified that both images were not altered.
9. Image verification records got added to log files.