ITIS 5250
Parag Mhatre
Lab 2
Oct 2nd, 2018

Overview:

In this Lab, I have been given two files, viz. **"CoffeeShopThumb.E01"** and **"PortableBrowser.E01"**. I been asked to make use of the **"FTK Imager Tool"** and **"SQL Lite Browser"** to examine both the images and answer questions like the date and time when a particular image was accessed, location of that image, my thoughts 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 through the Forensics Lab in **Cone 169** and transferred it to my device. 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. The MD5 Hash of both the images are as given below:

CoffeeShopThumb.E01:

Name	CoffeeShopThumb.E01
Sector count	7864320
MD5 Hash	
Computed hash	bc7583a1aede728b05df71f3120603c7
Stored verification hash	bc7583a1aede728b05df71f3120603c7
Report Hash	bc7583a1aede728b05df71f3120603c7
Verify result	Match
SHA1 Hash	

PortableBrowser.E01:

Name	PortableBrowser.E01
Sector count	7864320
MD5 Hash	
Computed hash	21995ed1ce24c5bcba21f979cd26da32
Stored verification hash	21995ed1ce24c5bcba21f979cd26da32
Report Hash	21995ed1ce24c5bcba21f979cd26da32
Verify result	Match
SHA1 Hash	

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?**

CoffeeShopThumb.E01

Disk	
Verification Hashes	
MD5 verification hash	bc7583a1aede728b05df71f3120603c7
SHA1 verification hash	42384f9dde450943d4e43291f97182f1d1a96225
Drive Geometry	
Bytes per Sector	512
Sector Count	7,864,320
Image	
Image Type	E01
Case number	CoffeeShopThumb
Evidence number	Item A
Examiner	Det. Peter Weller
Notes	Imaged in the UNCC Forensics Lab using a Wiebetech USB write bloc
Acquired on OS	Windows 7
Acquired using	ADI3.1.5.0
Acquire 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)

PortableBrowser.E01:

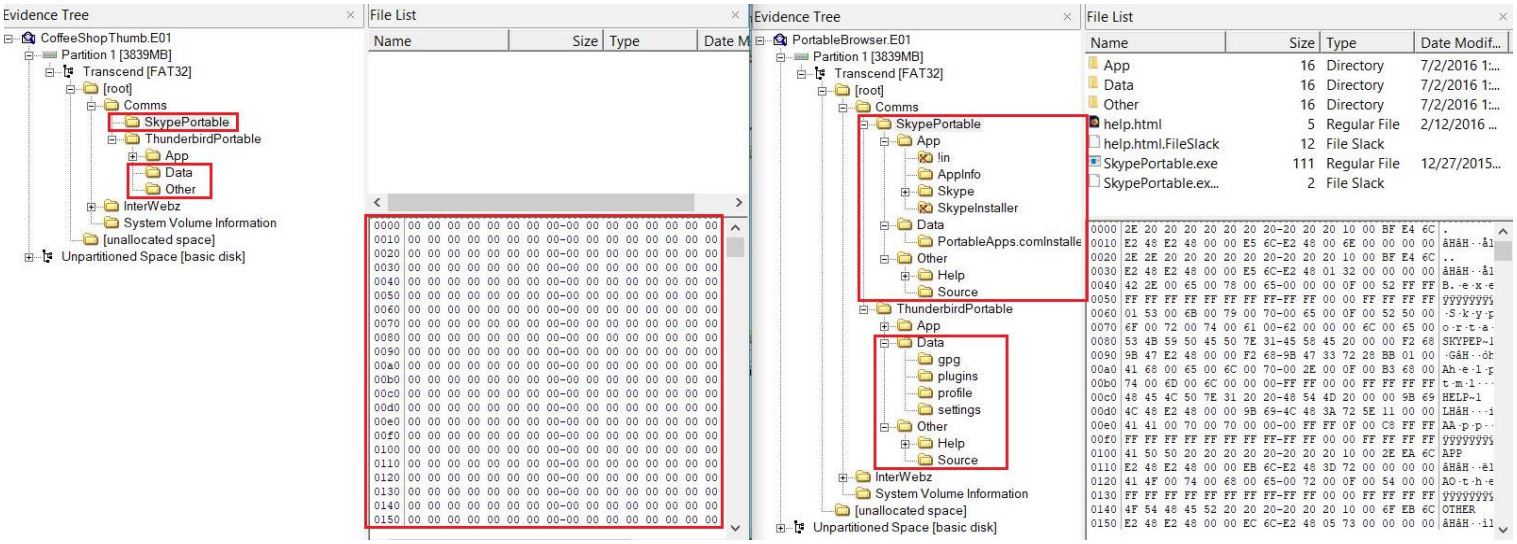
Disk	
Verification Hashes	
MD5 verification hash	21995ed1ce24c5bcba21f979cd26da32
SHA1 verification hash	dfb241687da6898657fd7f18adf113a9e2faf68b
Drive Geometry	
Bytes per Sector	512
Sector Count	7,864,320
Image	
Image Type	E01
Case number	PortableBrowserExample
Evidence number	Item A
Examiner	Digital 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

From the properties of both the images, I inferred that the drives of both the images have the **same size** are of the **same brand – "Transcend".**
On the other hand, the **MD5 hash values of both the images are different**, meaning that the images are not identical.

Log File Screenshotw of CoffeeShopThumb.E01:

```
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.
```

The log files of both the images show the drive geometry to be same, but the CoffeeShopThumb.E01 has a **bad sector entry** which tells that the sectors from **428672 to 7864319** couldn't be read and the **contents of those sectors were replaced by zeros.**



The **folder structure of both the files is the same** except some differences where some content is missing (some folders are empty) 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 that the system was unable to read.**

In my opinion, the **images appear to be of the same thumb drive.**

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?

Name	CoffeeShopThumb.E01
Sector count	7864320

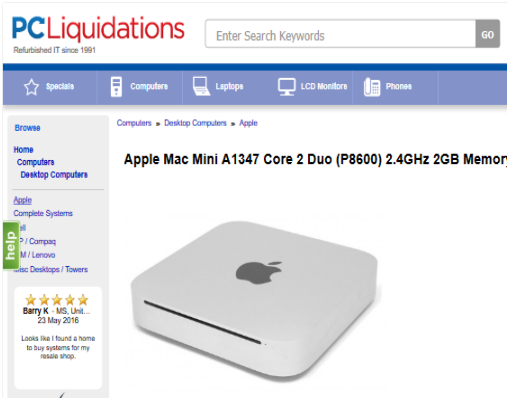
Name	PortableBrowser.E01
Sector count	7864320

Both the images represent **7864320 sectors** in total.

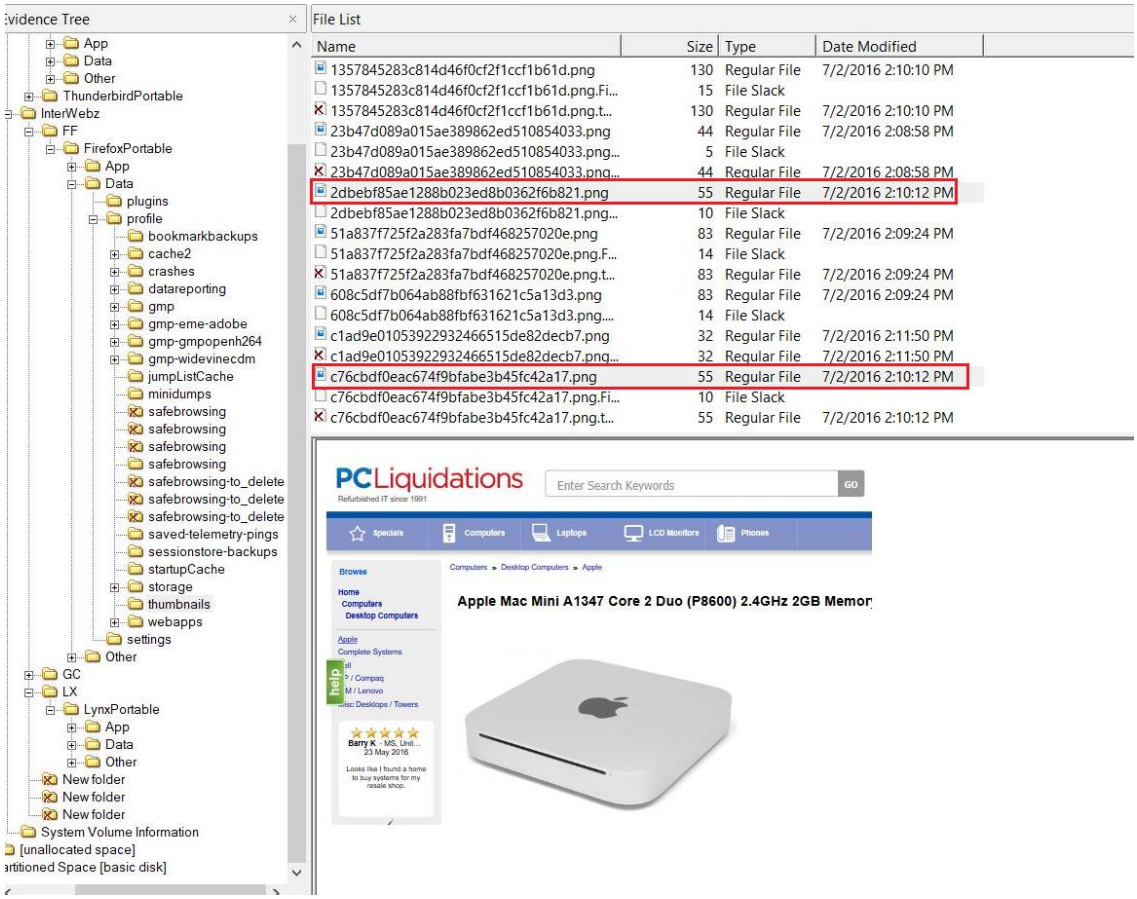
```
ATTENTION:
The following sector(s) on the source drive could not be read:
        428672 through 7864319
The contents of these sectors were replaced with zeros in the image.
```

The **log file of "CoffeeShopThumb.E01"** has an entry that 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?

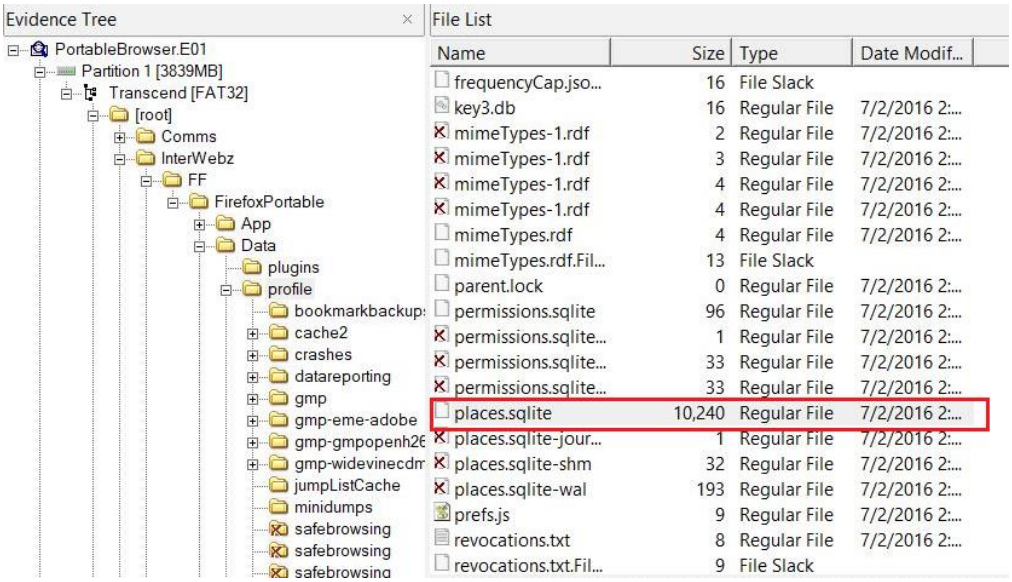


After checking the spreadsheet for PNG files, I **found two files** (highlighted in the image below) with this picture. Both the files were in the same folder.
The path is:
Partition 1\Transcend [FAT32]\[root]\InterWebz\FF\FirefoxPortable\Data\profile\thumbnails



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".

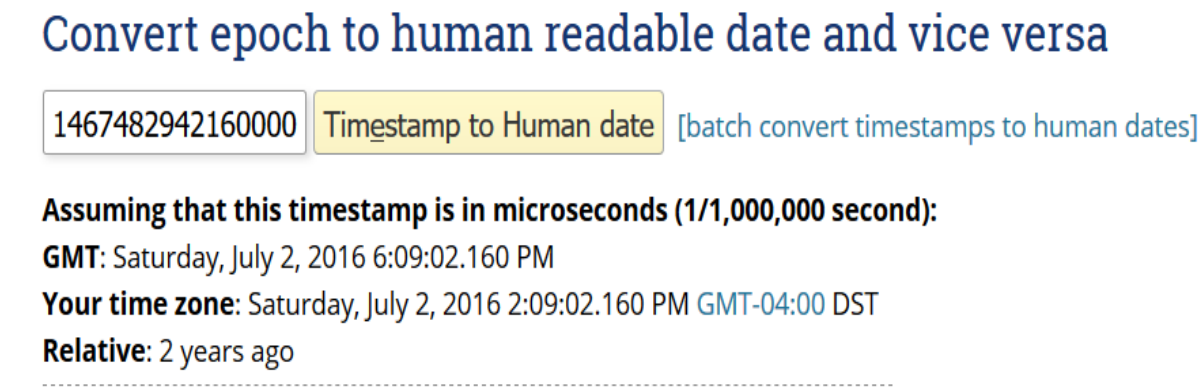
a. When was this page accessed? The date is in epoch format and will need to be converted (try www.epochconverter.com).



I accessed the file – **"places.sqlite"** from the given location and extracted it on my machine.
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**

4	6	http://www.mozilla.com/en-US...	NULL	moc.allizom.www.	0	0	0	3	140	NULL	kuLcB9woAOGO
5	7	http://www.mozilla.com/en-US...	NULL	moc.allizom.www.	0	0	0	4	140	NULL	TxS-u56mfo0i
6	8	http://portableapps.com/	NULL	moc.sppaelbatrop.	0	0	0	5	140	NULL	H8aJZGpusH8b
7	9	place:sort=8&maxResults=10	NULL	.	0	0	0	NULL	0	NULL	_SWHyHQG7O...
8	10	place:folder=BOOKMARKS_ME...	NULL	.	0	0	0	NULL	0	NULL	eHM_CqEGoSDO
9	11	place:type=6&sort=14&maxRe...	NULL	.	0	0	0	NULL	0	NULL	gnWiwpxIKqqn
10	15	http://www.pcliquidations.com...	Apple Mac Mini A1347 Core 2 ...	moc.snoitadiuqilcp.www.	1	0	0	NULL	175	1467482942160000	gxjKmvIbWzkU
11	18	http://www.macofalltrades.co...	Used Apple Mac mini 1.83GHz...	moc.sedartllafocam.www.	1	0	0	NULL	175	1467482944526000	Z8MzwyN2_Rm1
12	20	http://www.ebay.com/sch/i.ht...	mac mini | eBay	moc.yabe.www.	1	0	0	9	175	1467482950485000	P5txq3IAioFS
13	21	place:type=3&sort=4	NULL	NULL	0	1	0	NULL	0	NULL	0VJuElLwCQ9o
14	22	place:transition=7&sort=4	NULL	NULL	0	1	0	NULL	0	NULL	M7MxhTj9966O
15	23	place:type=6&sort=1	NULL	NULL	0	1	0	NULL	0	NULL	0WCQgVNa9YUo



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?

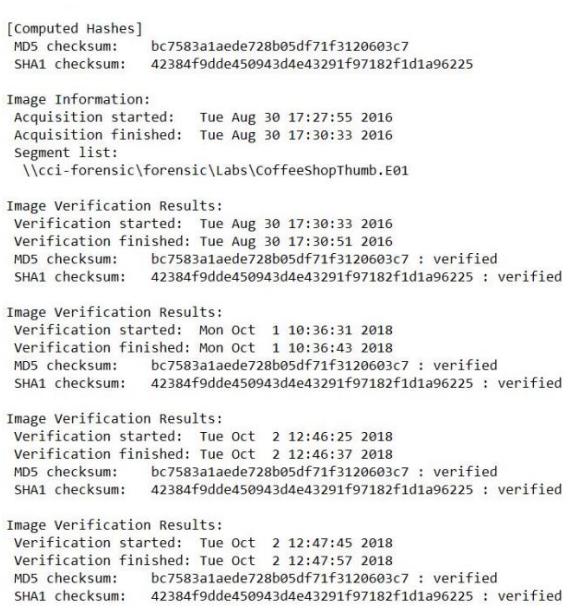
Final MD5 Hash verification of CoffeeThumb.E01:

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

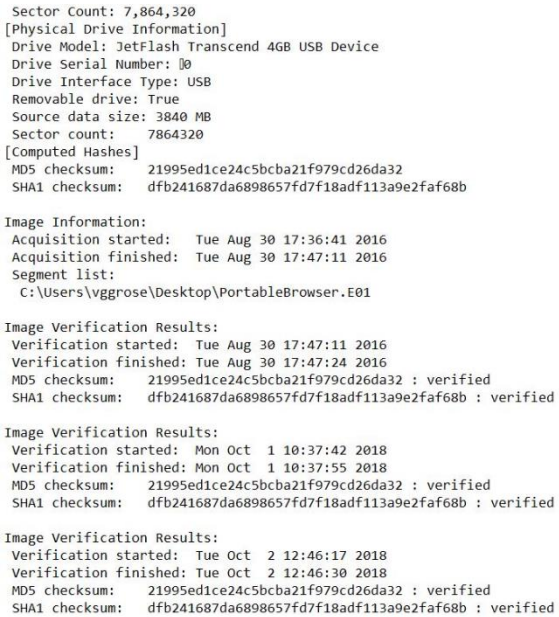
Final MD5 Hash verification of PortableBrowser.E01:

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

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.**



```
[Computed Hashes]
 MD5 checksum:    bc7583a1aede728b05df71f3120603c7
 SHA1 checksum:   42384f9dde450943d4e43291f97182f1d1a96225

Image Information:
 Acquisition started:   Tue Aug 30 17:27:55 2016
 Acquisition finished:  Tue Aug 30 17:30:33 2016
 Segment list:
  \\cci-forensic\forensic\Labs\CoffeeShopThumb.E01

Image Verification Results:
 Verification started:  Tue Aug 30 17:30:33 2016
 Verification finished: Tue Aug 30 17:30:51 2016
 MD5 checksum:    bc7583a1aede728b05df71f3120603c7 : verified
 SHA1 checksum:   42384f9dde450943d4e43291f97182f1d1a96225 : verified

Image Verification Results:
 Verification started:  Mon Oct  1 10:36:31 2018
 Verification finished: Mon Oct  1 10:36:43 2018
 MD5 checksum:    bc7583a1aede728b05df71f3120603c7 : verified
 SHA1 checksum:   42384f9dde450943d4e43291f97182f1d1a96225 : verified

Image Verification Results:
 Verification started:  Tue Oct  2 12:46:25 2018
 Verification finished: Tue Oct  2 12:46:37 2018
 MD5 checksum:    bc7583a1aede728b05df71f3120603c7 : verified
 SHA1 checksum:   42384f9dde450943d4e43291f97182f1d1a96225 : verified

Image Verification Results:
 Verification started:  Tue Oct  2 12:47:45 2018
 Verification finished: Tue Oct  2 12:47:57 2018
 MD5 checksum:    bc7583a1aede728b05df71f3120603c7 : verified
 SHA1 checksum:   42384f9dde450943d4e43291f97182f1d1a96225 : verified
```



```
 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

Image Verification Results:
 Verification started:  Mon Oct  1 10:37:42 2018
 Verification finished: Mon Oct  1 10:37:55 2018
 MD5 checksum:    21995ed1ce24c5bcba21f979cd26da32 : verified
 SHA1 checksum:   dfb241687da6898657fd7f18adf113a9e2faf68b : verified

Image Verification Results:
 Verification started:  Tue Oct  2 12:46:17 2018
 Verification finished: Tue Oct  2 12:46:30 2018
 MD5 checksum:    21995ed1ce24c5bcba21f979cd26da32 : verified
 SHA1 checksum:   dfb241687da6898657fd7f18adf113a9e2faf68b : verified
```

After examining the log files, I can see that **an entry is added to the files every time a Hash verification is done**.

Conclusion:

After acquiring 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 information I found was as follows:

1. Both the images are of a drive having same size and Brand name.
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 folders are empty(contents replaced with zeros).
5. The file was located in the drive with the path as - Partition 1\Transcend [FAT32]\[root]\InterWebz\FF\FirefoxPortable\Data\profile\thumbnails\2dbebf85ae1288b023ed8b0362f6b821.png
6. Opening "places.sqlite" in SQL Lite Browser, the time when the page was accessed was 1467482942160000 which in Human readable time format translates to GMT: Saturday, July 2, 2016 6:09:02.160 PM.
7. Reverification of the hashes was done to check if the images were altered in the process and it was found that every hash check enters a entry into the log files.
8. Also, from points 1, 2,3 and 4, I think that the both the images are of the same thumb drive.