

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

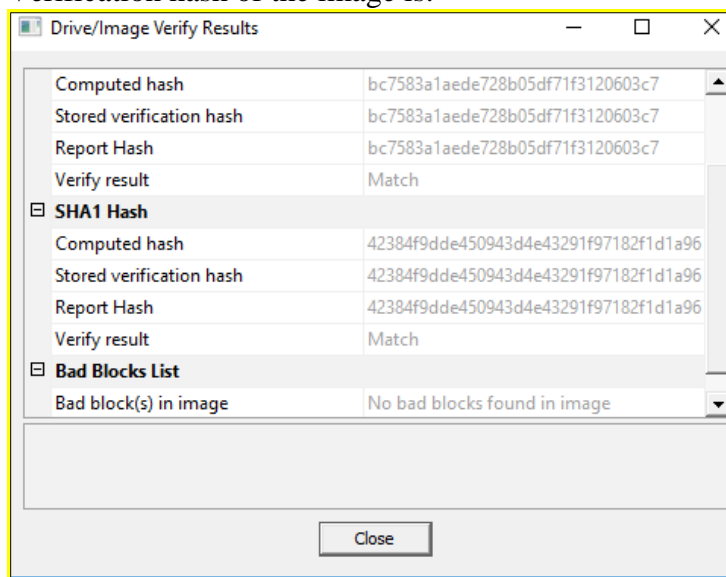
Acquired using: ADI3.1.5.0

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

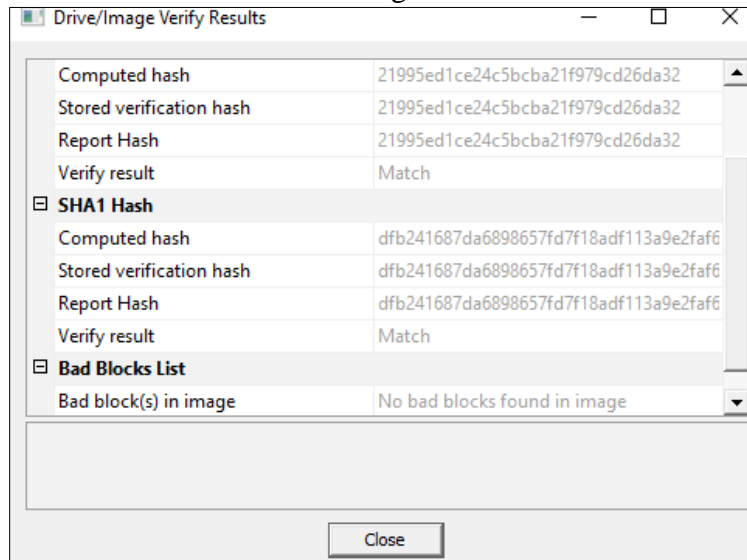
Acquired using: ADI3.1.5.0

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: 00
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

-----

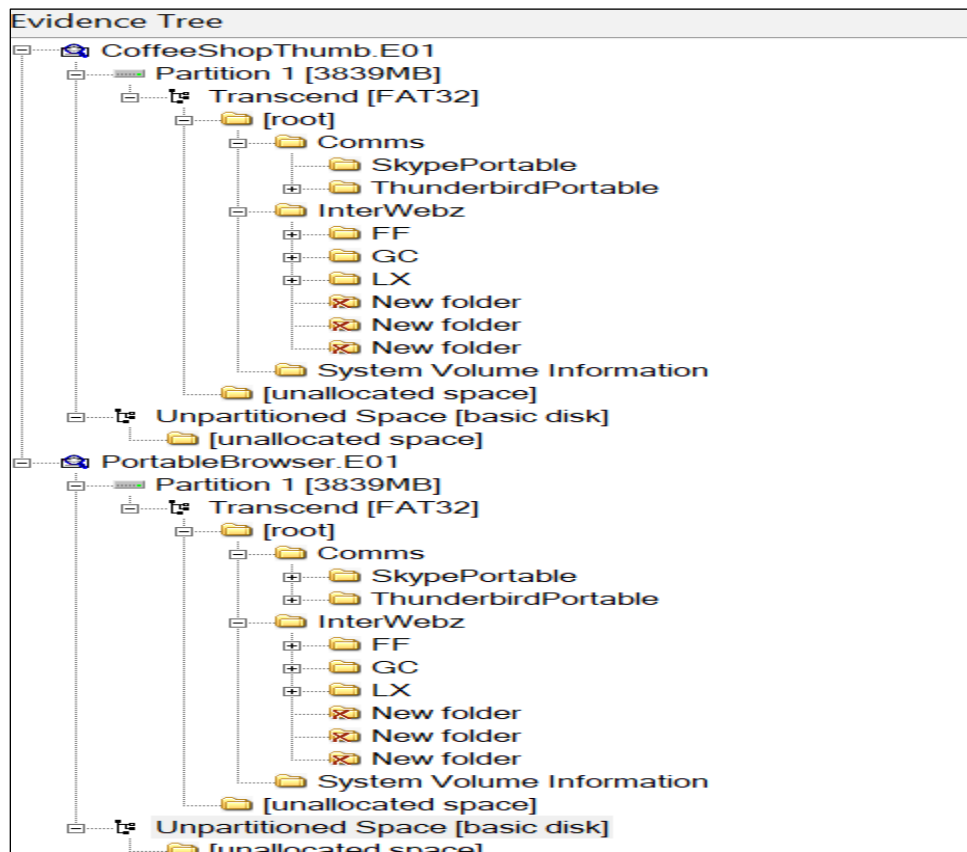
Information for C:\Users\vggrore\Desktop\PortableBrowser:

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: 00
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\vggrore\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
```

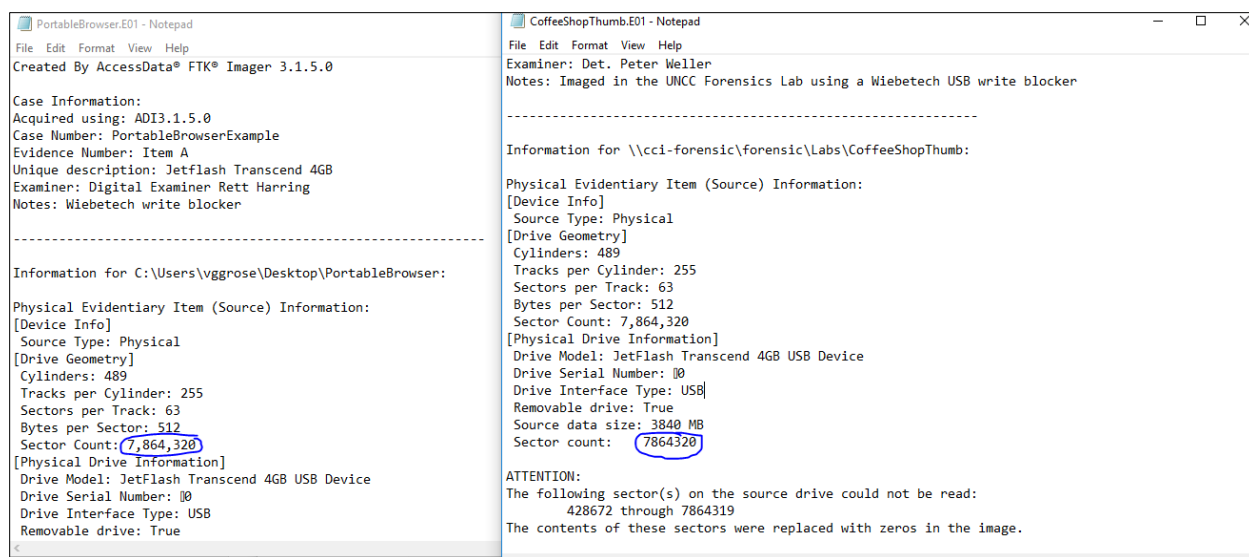
Folder Structure:



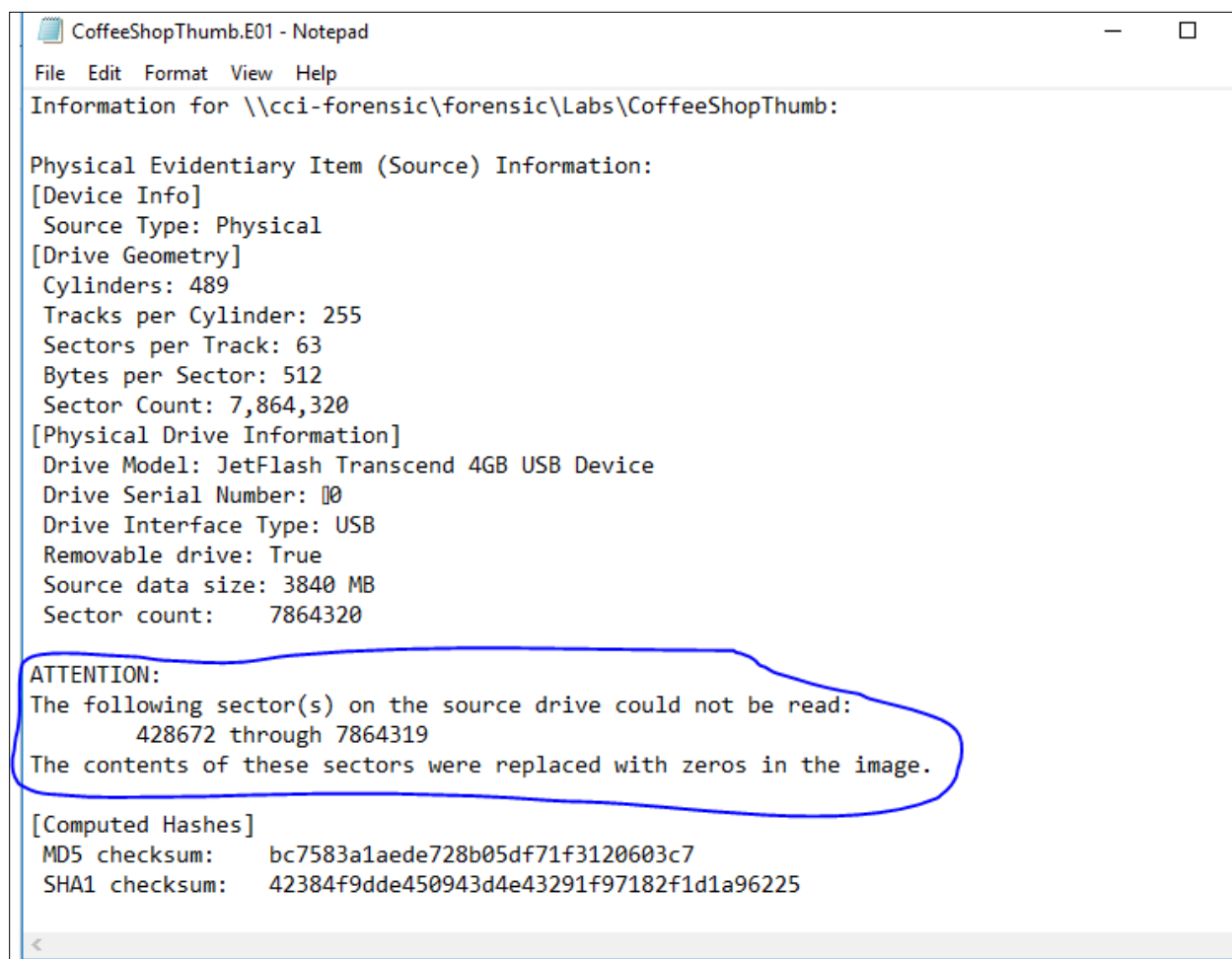
Moreover, both these images have same partition of 3839MB and their file system is FAT32.

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?

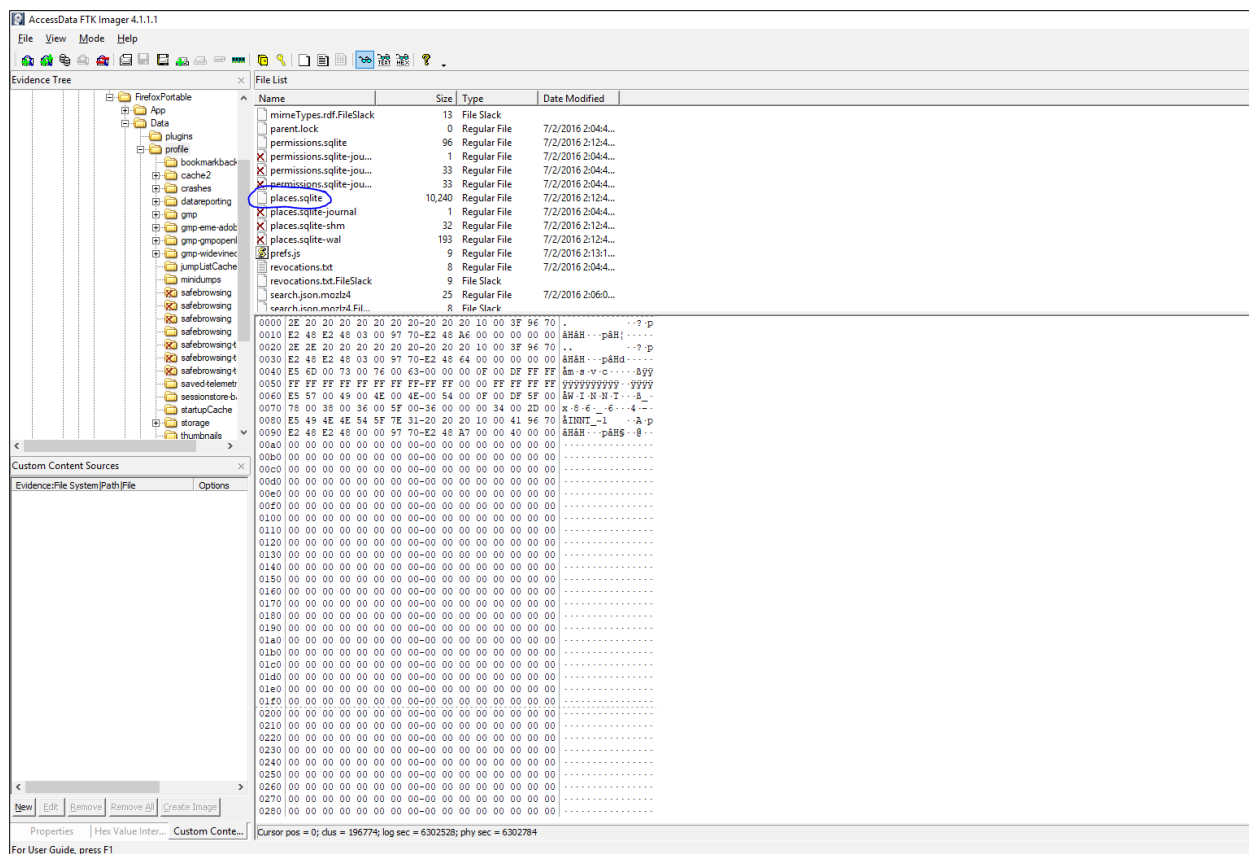


After checking the spreadsheet for PNG files, I found file (highlighted in the image below) with this picture.

The path is:

Partition 1\Transcend

[FAT32]\[root]\InterWebz\FF\FirefoxPortable\Data\profile\thumbnails\2dbebf85ae1288b023e.png



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

DB Browser for SQLite - C:\Users\angell\Desktop\Lab2\places.sqlite

File Edit View Help

New Database Open Database Write Changes Revert Changes

Database Structure Browse Data Edit Pragma Execute SQL

Table: mos_places

id	url	title	rev_host	visit_count	hidden	typed	favicon_id	frequency	last_visit_date	guid	foreign_count
1	https://www.mozilla.org/en-U...	Firefox + Win...	gro.allizom.w...	1	0	0	7	100	14674826912...	8BXdHlqD0Sc	0
2	https://www.mozilla.org/en-U...	Mozilla Firefo...	gro.allizom.w...	1	0	0	7	100	14674826951...	YgthY4ge9ao	0
3	http://www.mozilla.com/en-U...		moc.allizom...	0	0	0		140		C9Y_RKnSbf	1
4	http://www.mozilla.com/en-U...		moc.allizom...	0	0	0	1	140		6nFYvT3xXf	1
5	http://www.mozilla.com/en-U...		moc.allizom...	0	0	0	2	140		_TbJA0BHwgAf	1
6	http://www.mozilla.com/en-U...		moc.allizom...	0	0	0	3	140		kulc89wvAOGO	1
7	http://www.mozilla.com/en-U...		moc.allizom...	0	0	0	4	140		TxS-u56mf0i	1
8	http://portableapps.com/		moc.sppelba...	0	0	0	5	140		H8aZGpusH8b	1
9	place:sort=8&maxResults=10		.	0	0	0				_SWHyHQG7...	1
10	place:folder=BOOKMARKS_ME...		.	0	0	0		0		eHM_CqEGG...	1
11	place:type=6&sort=14&maxR...		.	0	0	0		0		gnWwpxdKqgn	1
12	https://search.yahoo.com/yhs/...	mac mini use...	moc.oohay.hc...	1	0	0	8	100	14674829330...	e8BlzVG9X5	0
13	http://i.search.yahoo.com/cbc...		moc.oohay.hc...	1	0	0		100	14674829413...	tbOKARBUJfg	0
14	http://12840.r.msn.com/7ld=...		moc.nsm.r.04...	1	1	0		100	14674829417...	rPvH8Rbypgs	0
15	http://www.pciquidations.com...	Apple Mac M...	moc.snoitadu...	1	0	0		175	14674829421...	gqKmvBvWdKU	1
16	http://i.search.yahoo.com/cbc...		moc.oohay.hc...	1	0	0		100	14674829423...	MqknqBewa5GR	0
17	http://1270143.r.msn.com/7ld...		moc.nsm.r.34...	1	1	0		100	14674829424...	GZEKvYR1VU...	0
18	http://www.macosfalltrades.co...	Used Apple M...	moc.sedartllef...	1	0	0		175	14674829445...	Z8Mzvyf02_R...	1
19	http://i.search.yahoo.com/_yht...		moc.oohay.hc...	1	0	0		100	14674829482...	4fOvO4GDh8V	0
20	http://www.ebay.com/sch/lht...	mac mini eBay	moc.yabe.www...	1	0	0	9	175	14674829504...	P5tq33AioFS	1
21	place:type=3&sort=4			0	1	0		0		0V3uELwCQ9o	1
22	place:transition=7&sort=4			0	1	0		0		M7MhTj99660	1
23	place:type=6&sort=1			0	1	0		0		0WCQgVNe9Y...	1
24	place:folder=TOOLBAR			0	1	0		0		qkazyTnsHGWj	1
25	place:folder=BOOKMARKS_ME...			0	1	0		0		qJefl,1fFOa5r	1
26	place:folder=UNFILED_BOOKM...			0	1	0		0		RCEGR9qID5m	1
27	https://search.yahoo.com/yhs/...	nc stealing un...	moc.oohay.hc...	1	0	0	8	100	14674830892...	0Lzr9fHG8e	0
28	http://i.search.yahoo.com/_yht...		moc.oohay.hc...	1	0	0		100	14674830948...	bwL0d4FfgMW	0
29	http://www.criminaldefense.la...	North Carolin...	moc.reyvalles...	1	0	0	10	175	14674830951...	wvp5Ty61vs1	1

Go to: 1

Apple Mac Mini A1347 Core 2 Duo (P8600) 2.4GHz 2GB Memory 320GB HDD

Type of data currently in cell: Text / Numeric

67 char(s)

Remote

Identity

Name Commit Last modified Size

SQL Log Plot DB Schema Remote

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

DB Browser for SQLite - C:\Users\angell\Desktop\Lab2\places.sqlite

File Edit View Help

New Database Open Database Write Changes Revert Changes

Database Structure Browse Data Edit Pragma Execute SQL

Table: mos_places

id	url	title	rev_host	visit_count	hidden	typed	favicon_id	frequency	last_visit_date	guid	foreign_count
1	https://www.mozilla.org/en-U...	Firefox + Win...	gro.allizom.w...	1	0	0	7	100	1467482691238000	8BXdHlqD0Sc	0
2	https://www.mozilla.org/en-U...	Mozilla Firefo...	gro.allizom.w...	1	0	0	7	100	1467482695176000	YgthY4ge9ao	0
3	http://www.mozilla.com/en-U...		moc.allizom...	0	0	0		140		C9Y_RKnSbf	1
4	http://www.mozilla.com/en-U...		moc.allizom...	0	0	0	1	140		6nFYvT3xXf	1
5	http://www.mozilla.com/en-U...		moc.allizom...	0	0	0	2	140		_TbJA0BHwgAf	1
6	http://www.mozilla.com/en-U...		moc.allizom...	0	0	0	3	140		kulc89wvAOGO	1
7	http://www.mozilla.com/en-U...		moc.allizom...	0	0	0	4	140		TxS-u56mf0i	1
8	http://portableapps.com/		moc.sppelba...	0	0	0	5	140		H8aZGpusH8b	1
9	place:sort=8&maxResults=10		.	0	0	0				_SWHyHQG7...	1
10	place:folder=BOOKMARKS_ME...		.	0	0	0		0		eHM_CqEGG...	1
11	place:type=6&sort=14&maxR...		.	0	0	0		0		gnWwpxdKqgn	1
12	https://search.yahoo.com/yhs/...	mac mini use...	moc.oohay.hc...	1	0	0	8	100	1467482933004000	e8BlzVG9X5	0
13	http://i.search.yahoo.com/cbc...		moc.oohay.hc...	1	0	0		100	1467482941379000	tbOKARBUJfg	0
14	http://12840.r.msn.com/7ld=...		moc.nsm.r.04...	1	1	0		100	1467482941729000	rPvH8Rbypgs	0
15	http://www.pciquidations.com...	Apple Mac M...	moc.snoitadu...	1	0	0		175	1467482942160000	gqKmvBvWdKU	1
16	http://i.search.yahoo.com/cbc...		moc.oohay.hc...	1	0	0		100	1467482942306000	MqknqBewa5GR	0
17	http://1270143.r.msn.com/7ld...		moc.nsm.r.34...	1	1	0		100	1467482942436000	GZEKvYR1VU...	0
18	http://www.macosfalltrades.co...	Used Apple M...	moc.sedartllef...	1	0	0		175	1467482944526000	Z8Mzvyf02_R...	1
19	http://i.search.yahoo.com/_yht...		moc.oohay.hc...	1	0	0		100	1467482948223000	4fOvO4GDh8V	0
20	http://www.ebay.com/sch/lht...	mac mini eBay	moc.yabe.www...	1	0	0	9	175	1467482950485000	P5tq33AioFS	1
21	place:type=3&sort=4			0	1	0		0		0V3uELwCQ9o	1
22	place:transition=7&sort=4			0	1	0		0		M7MhTj99660	1
23	place:type=6&sort=1			0	1	0		0		0WCQgVNe9Y...	1
24	place:folder=TOOLBAR			0	1	0		0		qkazyTnsHGWj	1
25	place:folder=BOOKMARKS_ME...			0	1	0		0		qJefl,1fFOa5r	1
26	place:folder=UNFILED_BOOKM...			0	1	0		0		RCEGR9qID5m	1
27	https://search.yahoo.com/yhs/...	nc stealing un...	moc.oohay.hc...	1	0	0	8	100	1467483089297000	0Lzr9fHG8e	0
28	http://i.search.yahoo.com/_yht...		moc.oohay.hc...	1	0	0		100	1467483094830000	bwL0d4FfgMW	0
29	http://www.criminaldefense.la...	North Carolin...	moc.reyvalles...	1	0	0	10	175	1467483095119000	wvp5Ty61vs1	1

Go to: 1

1467482942160000

Type of data currently in cell: Text / Numeric

16 char(s)

Remote

Identity

Name Commit Last modified Size

SQL Log Plot DB Schema Remote

EpochConverter

Epoch & Unix Timestamp Conversion Tools

The current Unix epoch time is **1538523725**

Convert epoch to human readable date and vice versa

[batch convert timestamps to human dates]

Assuming that this timestamp is in microseconds (1/1,000,000 second):
GMT: Saturday, July 2, 2016 6:09:02.160 PM
Your time zone: Saturday, July 2, 2016 2:09:02.160 PM GMT-04:00 DST
Relative: 2 years ago

Yr Mon Day Hr Min Sec GMT

2018 10 2 23 41 8 GMT

Pages
Home

Tools
Epoch converter
Batch converter
Epoch clock
Time zone converter
Epoch timestamp list
LDAP converter
WebKit/Chrome timestamp
Unix hex timestamp
Cocoa Core Data timestamp
Mac HFS+ timestamp
SAS timestamp
Seconds/days since year 0
Countdown in seconds
Bin/Oct/Hex converter

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.

Drive/Image Verify Results

Sector count: 7864320

MD5 Hash

Computed hash	bc7583a1aede728b05df71f3120603c7
Stored verification hash	bc7583a1aede728b05df71f3120603c7
Report Hash	bc7583a1aede728b05df71f3120603c7
Verify result	Match

SHA1 Hash

Computed hash	42384f9dde450943d4e43291f97182f1d1a96
Stored verification hash	42384f9dde450943d4e43291f97182f1d1a96
Report Hash	42384f9dde450943d4e43291f97182f1d1a96
Verify result	Match

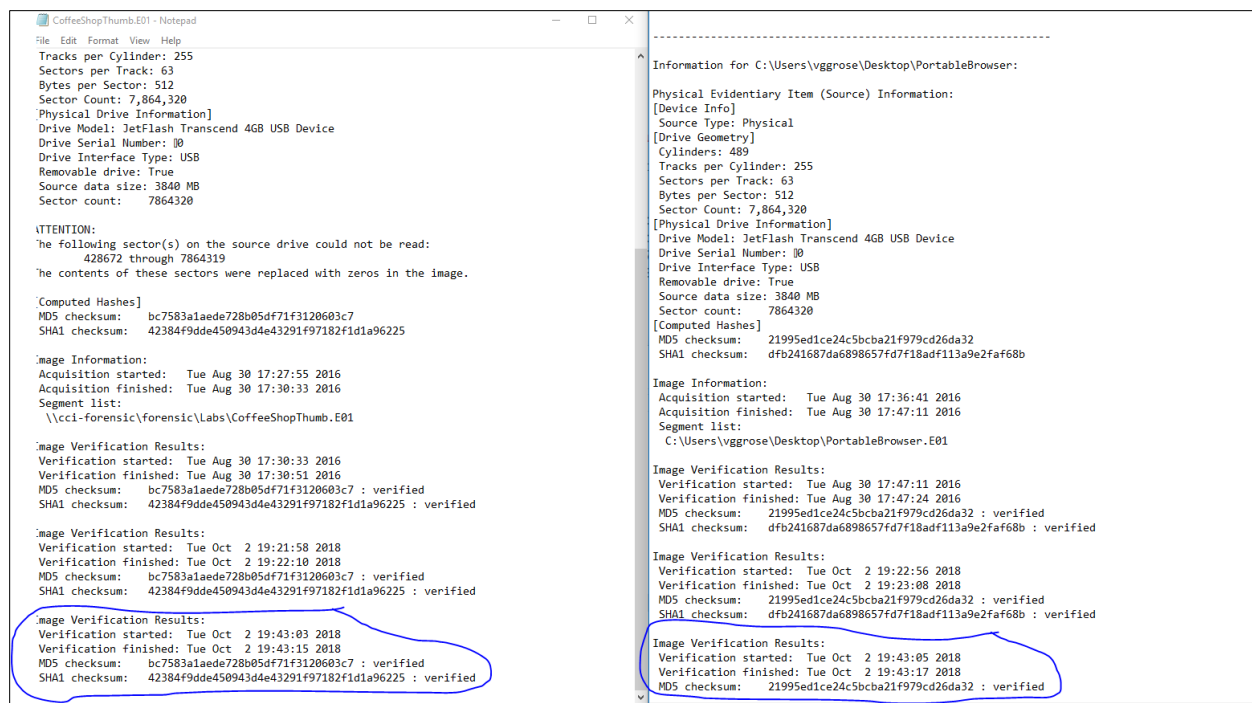
Bad Blocks List

Bad block(s) in image	No bad blocks found in image
-----------------------	------------------------------

Close

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\2dbefb85ae1288b023e.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.