ITIS 5250

Ruchira Pokhriyal

Lab 2

09/30/2018

**Overview:**

In this forensics lab, I am introduced to SQL Lite and I will be examining the geometry and folder structure of both of the provided image files. I will also be locating a PNG picture and will be verifying the hash values of the given image files twice- once after loading them into FTK imager and then again after my investigation.

**Forensic Acquisition & Exam Preparation:**

I accessed the image files named ‘CoffeeShopThumb.E01’ and ‘PortableBrowser.E01’ and their log files from the server’s shared directory. Then, I loaded these two images using FTK Imager and performed hash verification by right clicking on both the image files. The hash values were a match for both the files. Following are the descriptions of the two image files:

**CoffeeShopThumb.E01**:

Acquired on OS: Windows 7.

Acquired using: ADI3.1.5.0.

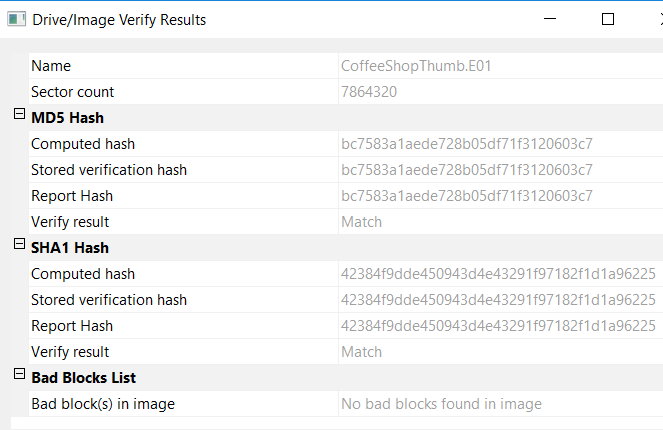
Acquired date: 8/30/2016 9:27:55 PM.

System date: 8/30/2016 9:27:55 PM.

Unique description: 4GB Transcend Jetflash Thumb Drive (red and black).

MD5 Hash Value: bc7583a1aede728b05df71f3120603c7

SHA1 Hash Value: 42384f9dde450943d4e43291f97182f1d1a96225



**PortableBrowser.E01:**

Acquired on OS: Windows 7.

Acquired using: ADI3.1.5.0.

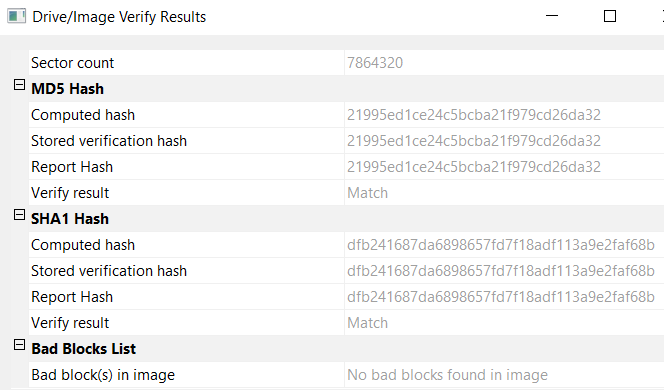
Acquired date: 8/30/2016 9:36:41 PM.

System date: 8/30/2016 9:36:41 PM.

Unique description: Jetflash Transcend 4GB.

MD5 Hash Value: 21995ed1ce24c5bcba21f979cd26da32

SHA1 Hash Value: dfb241687da6898657fd7f18adf113a9e2faf68b

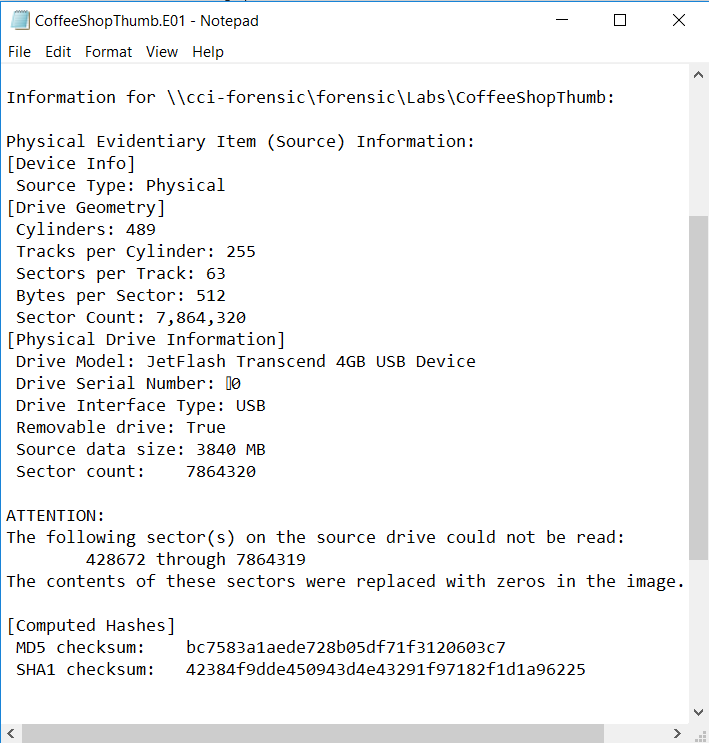
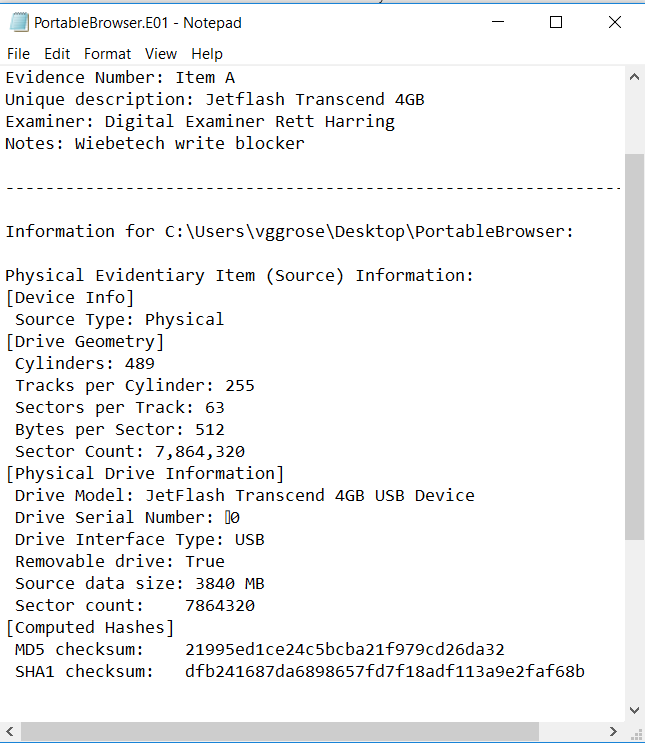


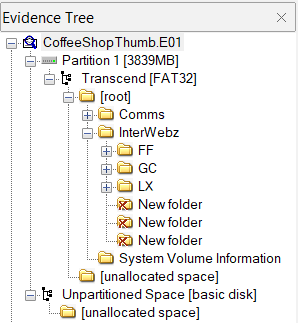
**Findings and Report (Forensic Analysis):**

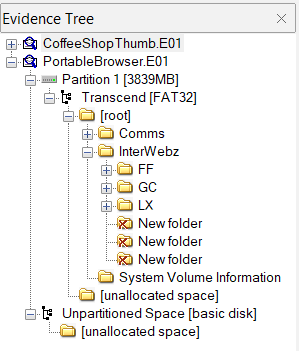
1. **Judging by geometry, hash value, folder structure and the log files do these images appear to be of the same thumb drive? How are they similar and how are they dissimilar?**

As shown below, the geometry of both the image files is identical, which is evident from their log files. The folder structures of the images are identical too and there are two computed hashes of each image: MD5 and SHA1. Furthermore, it can be seen under the evidence tree that both the images have the same partition of 3839MB and their file system is FAT32. Therefore, I can say that both the images appear to be of the same thumb drive. Looking at most of the properties, the two image files appear to be the same but they are not, since the hash values of both the image files differ. Also, some of the sectors in ‘CoffeeShopThumb.E01’ are not being read, according to the image’s log file.

Log file of **‘CoffeeShopThumb.E01’**: Log file of **‘PortableBrowser.E01’:**



File Structure of **‘CoffeeShopThumb.E01’**: File Structure of **‘PortableBrowser.E01’:**



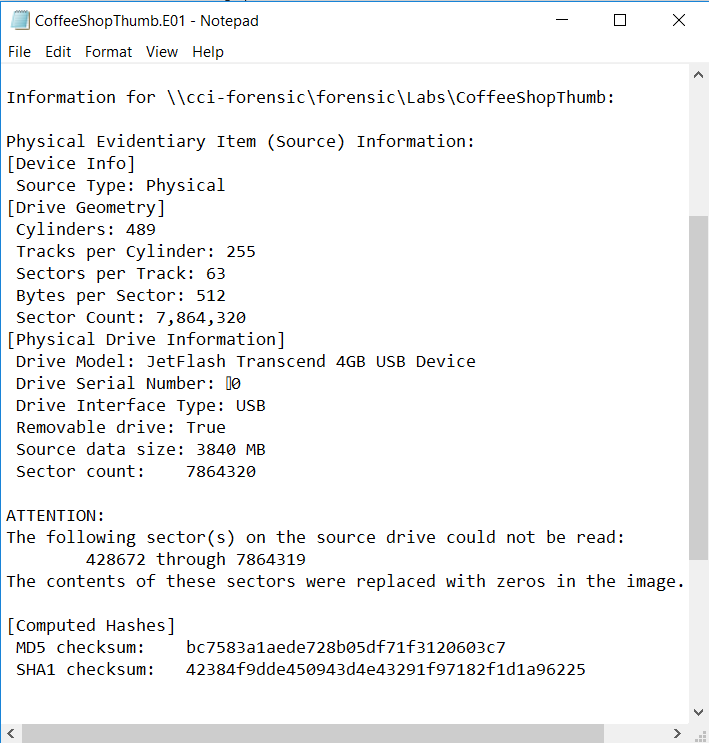
1. **How many sectors do each of the images represent in total? Are there any errors showing one image did not record some of the sectors?**

The sector count of ‘CoffeeShopThumb.E01’ is **7,864,320**.

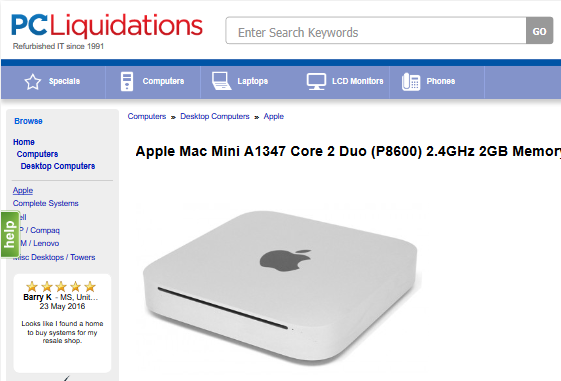
The sector count of ‘PortableBrowser.E01 is **7,864,320** too.

Therefore, the total sector count is **15,728,640**.

Yes, there are errors showing that **‘CoffeeShopThumb.E01’** did not record some of the sectors. As evident from its log file, ‘CoffeeShopThumb.E01’ did not record the sectors from 428672 through 7864319 and the contents of these sectors were replaced with zeros in the image.

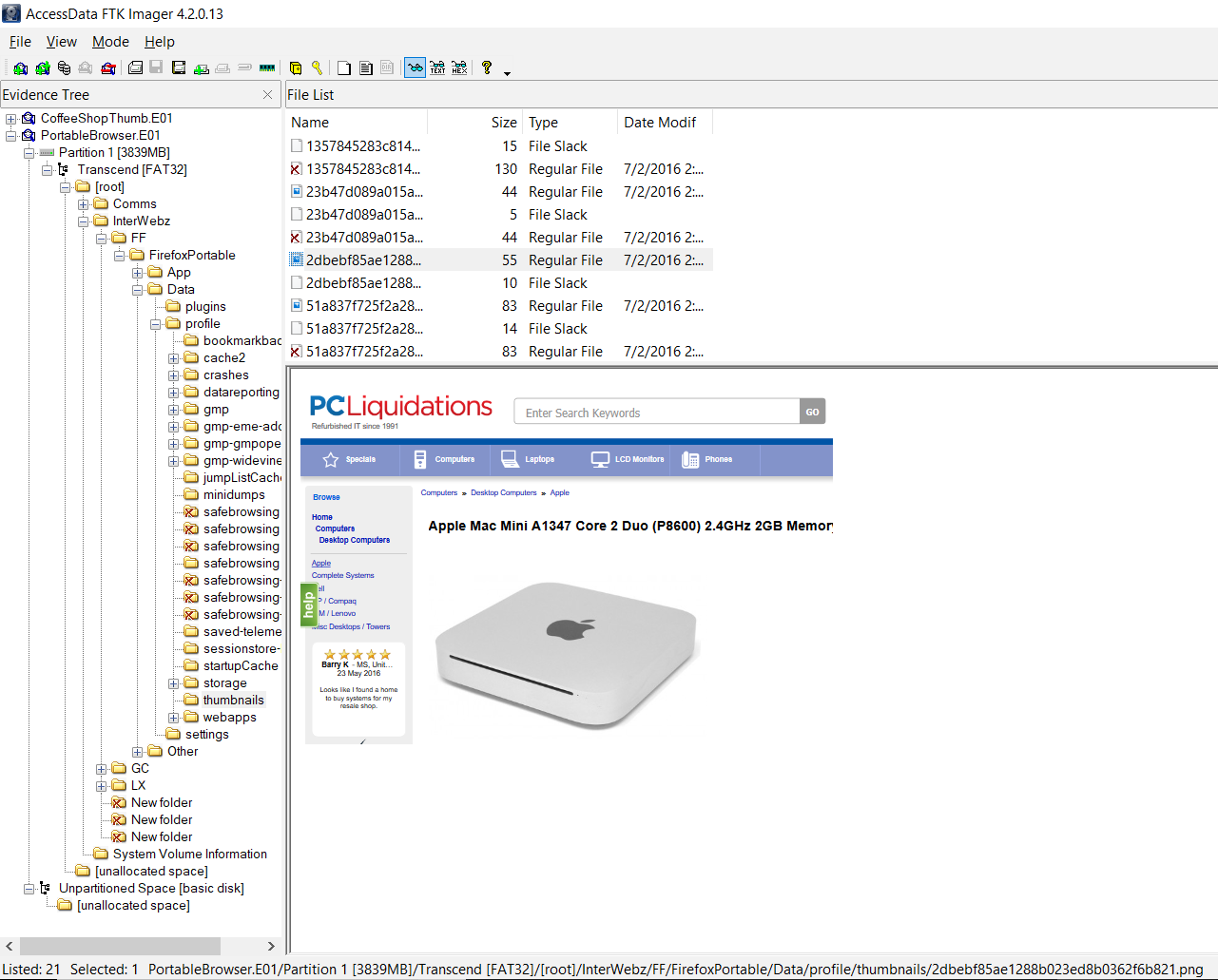


1. **Can you locate the following picture and where did you find it? (Hint: a file listing spreadsheet is provided with the .e01 files, look for png files there and browse to that location with Imager)**



I searched the “.png” extension in the provided spreadsheet and found this picture in ‘PortableBrowser.E01’, after browsing to the following location:

**“Partition 1\Transcend** **[FAT32]\[root]\InterWebz\FF\FirefoxPortable\Data\profile\thumbnails\2dbebf85ae1288b023ed8b0362f6b821.png”**

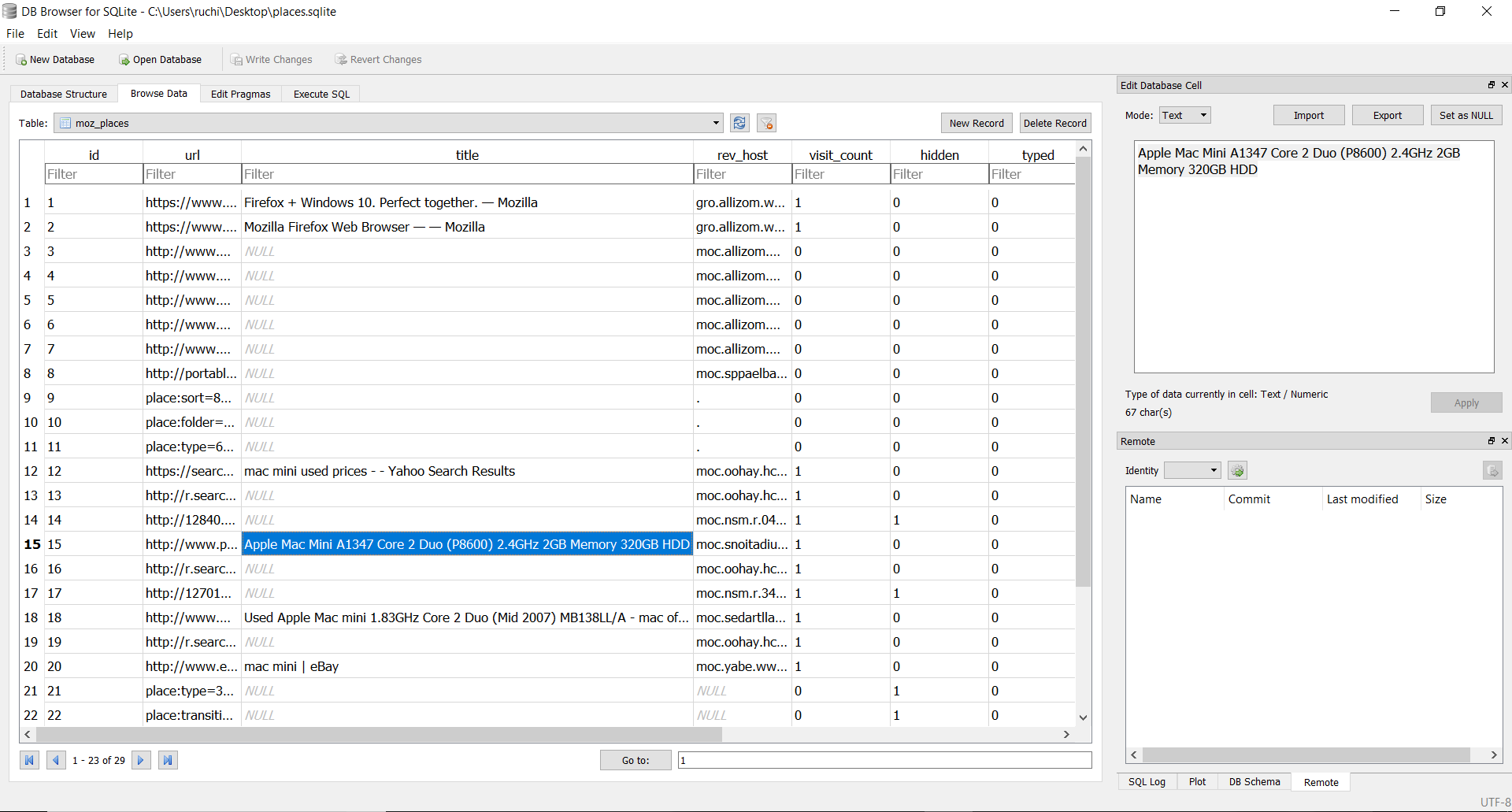


**When was this page accessed?**

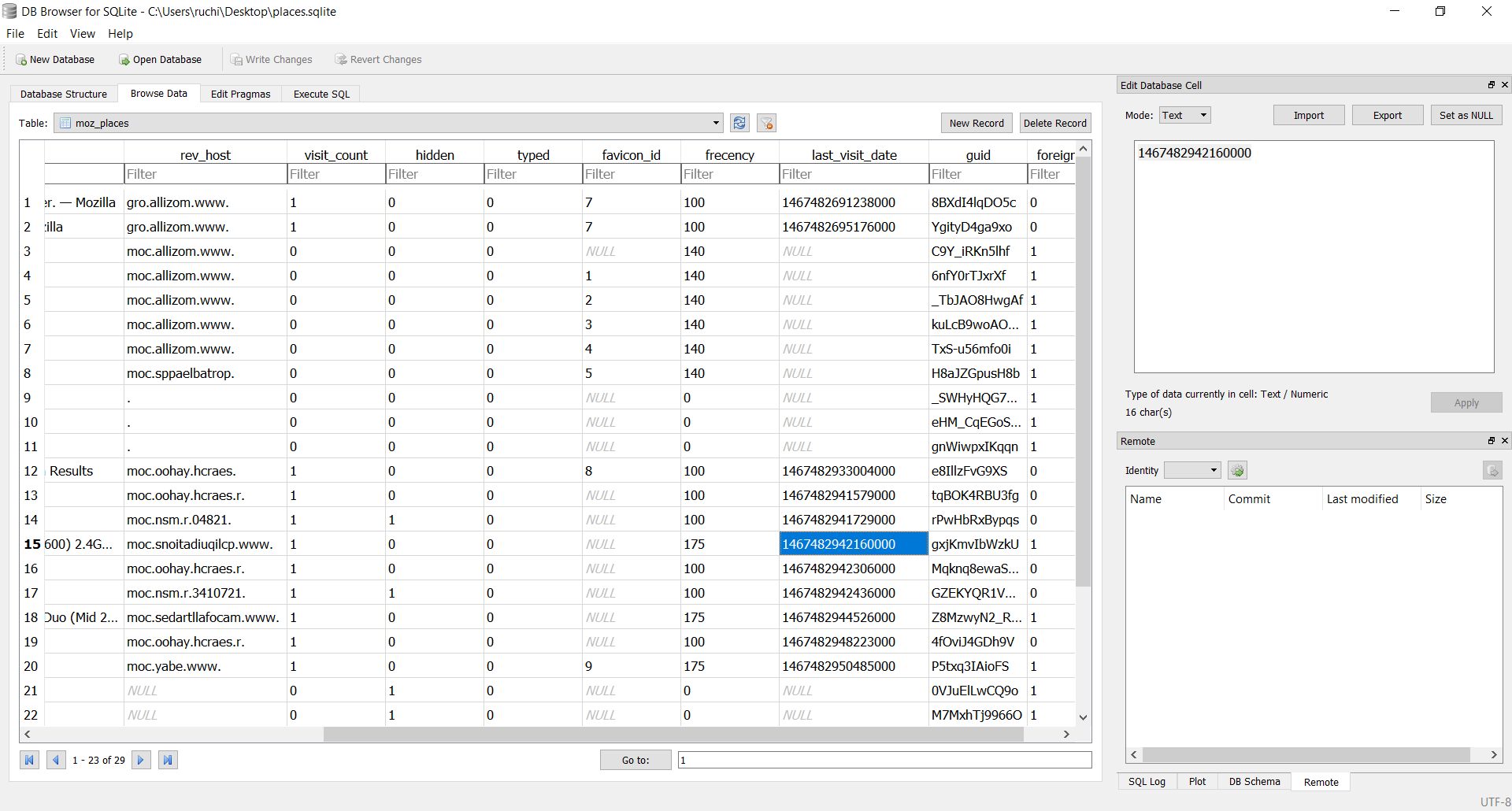
After installing SQL Lite browser, I exported the **‘places.sqlite’** file from the following location of PortableBrowser.E01:

**“InterWebz \ FF \ FirefoxPortable \ Data \ profile”.**

Then, after loading the ‘places.sqlight’ file in SQL Lite, I selected **‘Browse Data’** tab and under the table **‘moz\_places’**, I located **“Apple Mac Mini A1347 Core 2 Duo (P8600) 2.4 GHz 2GB Memory 320GB HDD”.**



As shown below, the page was last accessed on “1467482942160000”.



Since this is in epoch format, I converted it to human readable format by visiting [www.epochconverter.com](http://www.epochconverter.com). After conversion to human readable format, I found the date to be **“Saturday, July 2, 2016 6:09:02.160 PM”.**



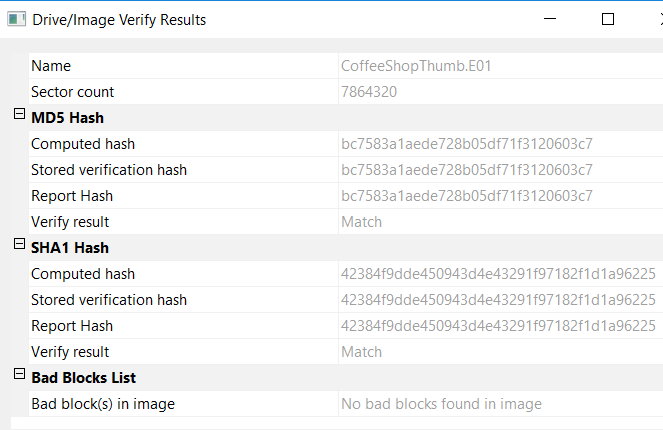
**Was a record added to your log file to show you verified the image?**

I performed the hash verification of both the image files again to ensure that they were not altered in any way during my investigation. Following verification results for both the images show that the image files are unaltered.

**CoffeeShopThumb.E01**:

MD5 Hash Value: bc7583a1aede728b05df71f3120603c7

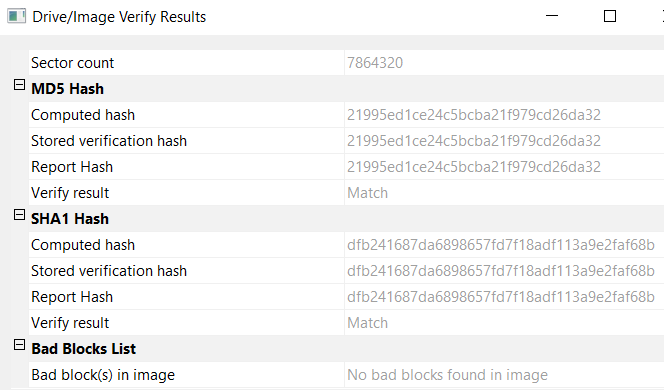
SHA1 Hash Value: 42384f9dde450943d4e43291f97182f1d1a96225



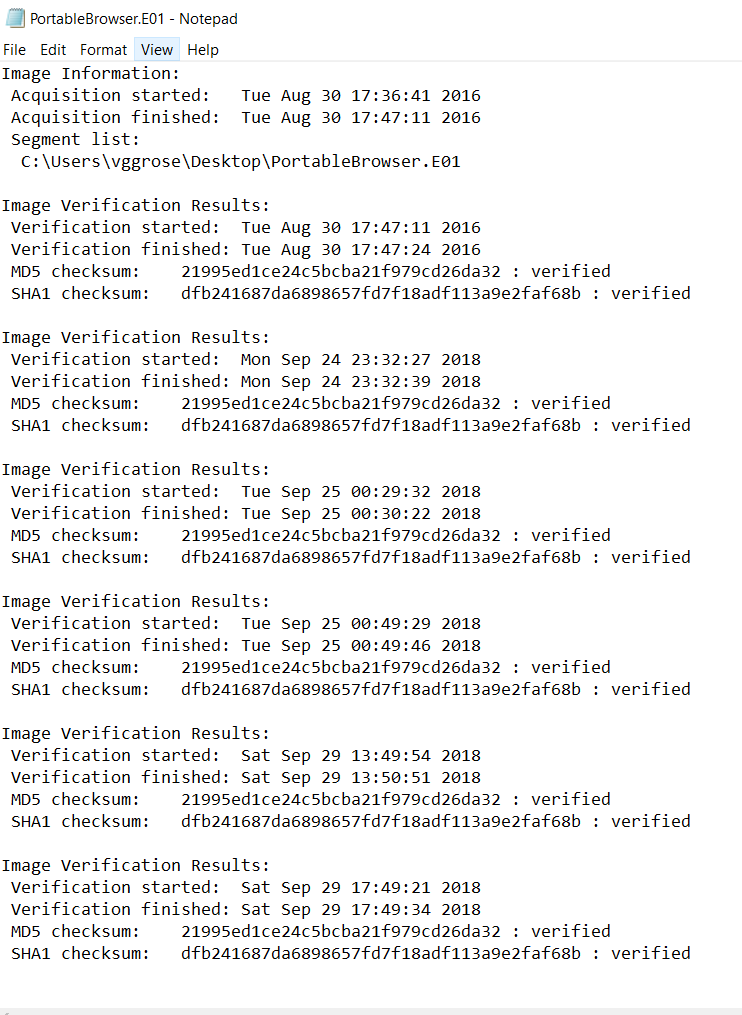
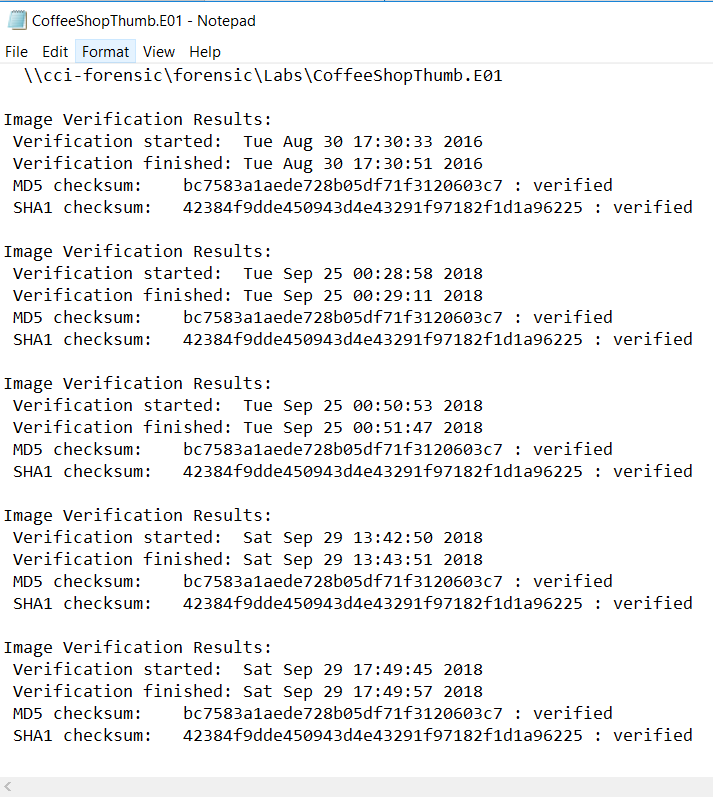
**PortableBrowser.E01:**

MD5 Hash Value: 21995ed1ce24c5bcba21f979cd26da32

SHA1 Hash Value: dfb241687da6898657fd7f18adf113a9e2faf68b



As shown below, records of the hash verification of both the image files were added to their respective log files.

Log file of **‘CoffeeShopThumb.E01’:** Log file of **‘PortableBrowser.E01’:**

**Conclusion:**

I analyzed the folder structure and log files of both the image files, found a ‘.png’ picture using the file listing spreadsheet, and also checked a page and its last access date using SQL Lite. Finally, I performed hash verification of the given image files again, to verify their integrity. This hash verification action was recorded in the log files of both the images files.