ITIS 4250 / 5250

Shivani Sathe

Lab # 2

4thth October 2021

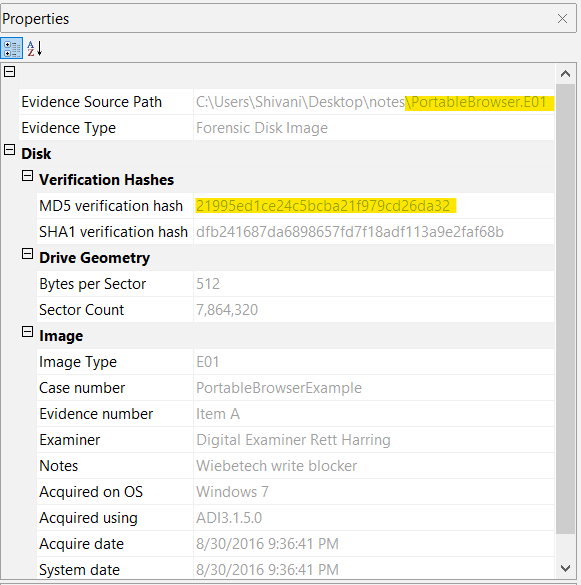
**Overview:**

Dr. Robert Quincy, Chief Forensics Examiner at the UNCC Forensics Laboratory, had asked me to perform technical work on a forensics image. The forensic image PortableBrowser.e01was of a thumb drive provided to me for examination. Dr. Robert Quincy had determined that to further the investigation, forensic analysis to be conducted to determine if the user of the thumb drive had been looking at the prices of Apple computers on eBay or other sites.

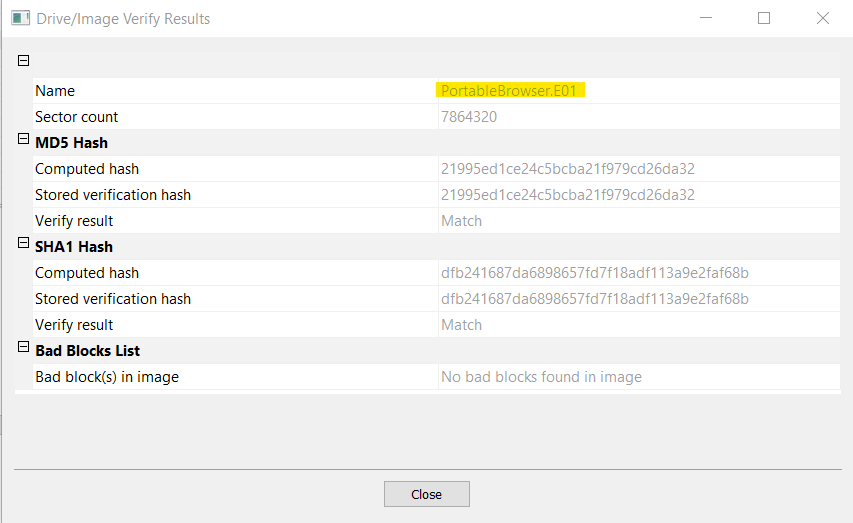
**Forensic Acquisition & Exam Preparation**

To begin the analysis, Windows 10, 64-bit system was used and the forensic image file PortableBrowser.e01 was placed in a newly created folder named ‘**notes**’ on desktop. Later, AccessData FTK Imager 4.5.0.3 was used to load the image to view the file system, sub directories and file contents. MD5 hash was noted after loading the image and the hash value was verified before starting the analysis and also at the end of the analysis. Also, DB Browser for SQLite software was used to view the browser activities done by user of thumb drive.

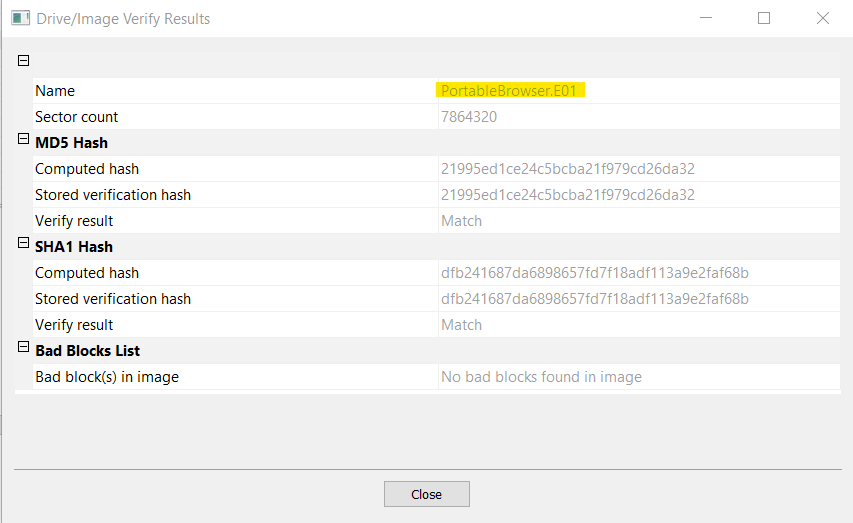
Hash of PortableBrowser.e01 after loading image:



Hash of PortableBrowser.e01 after verification before starting analysis:



Hash of PortableBrowser.e01 after verification after completing the analysis:



**Findings and Report (Forensic Analysis)**

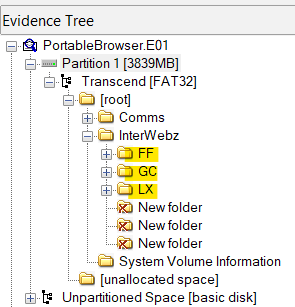
1. **What browsers was the subject using on this thumb drive?**

* **The browsers that were used are Firefox, Google Chrome and Lynx Browser.**
* **To find this, load the image PortableBrowser.e01 in FTK Imager, under Partion 1,**

**expand the ‘Transcend [FAT32]’ file system. Under the root directory, locate a**

**folder named ‘InterWebz’. Once this folder is expanded, the name of the web**

**browsers used can be seen as FF, GC and LX respectively**

****

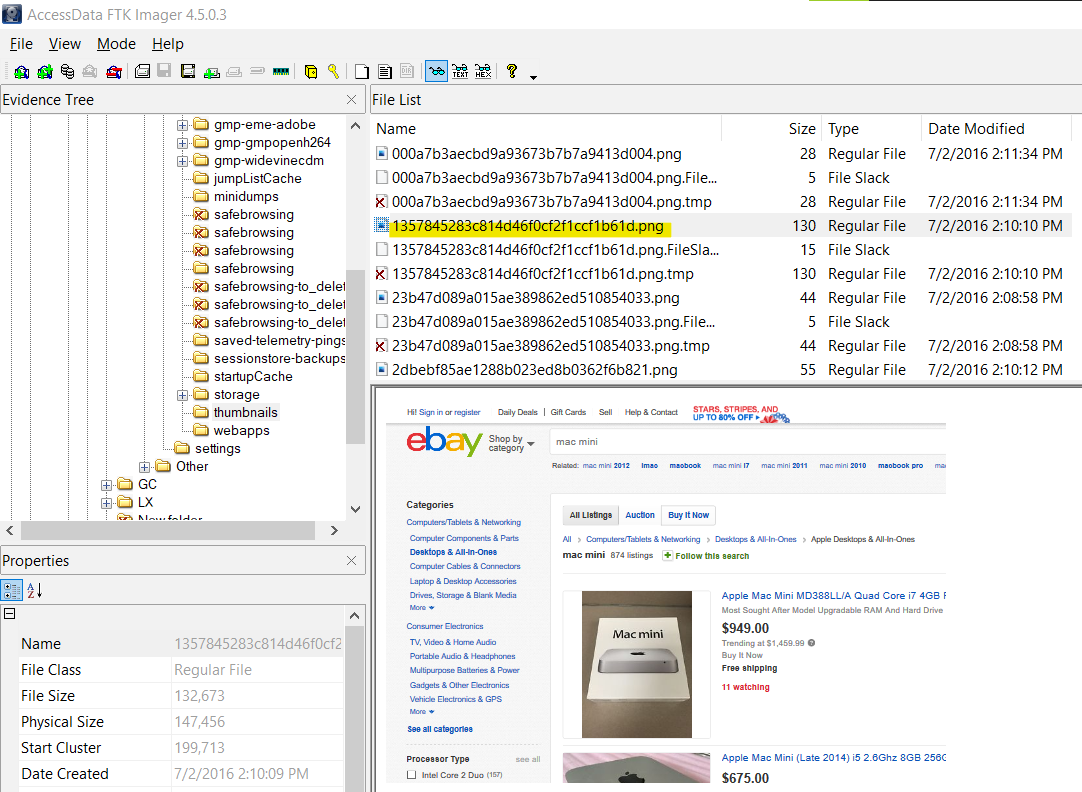
1. **Can you locate a picture of an Apple computer? Where did you find it? (Hint: You may want to look at the pictures in the cache directories for the browsers, or use Autopsy and look at the media files)**

* **Yes, picture of Apple Computer is found.**
* **To find the picture, directory listing is created using FTK Imager to a CSV and .png files are searched. The files are listed in folder named ‘thumbnails’ and is found at below location-**

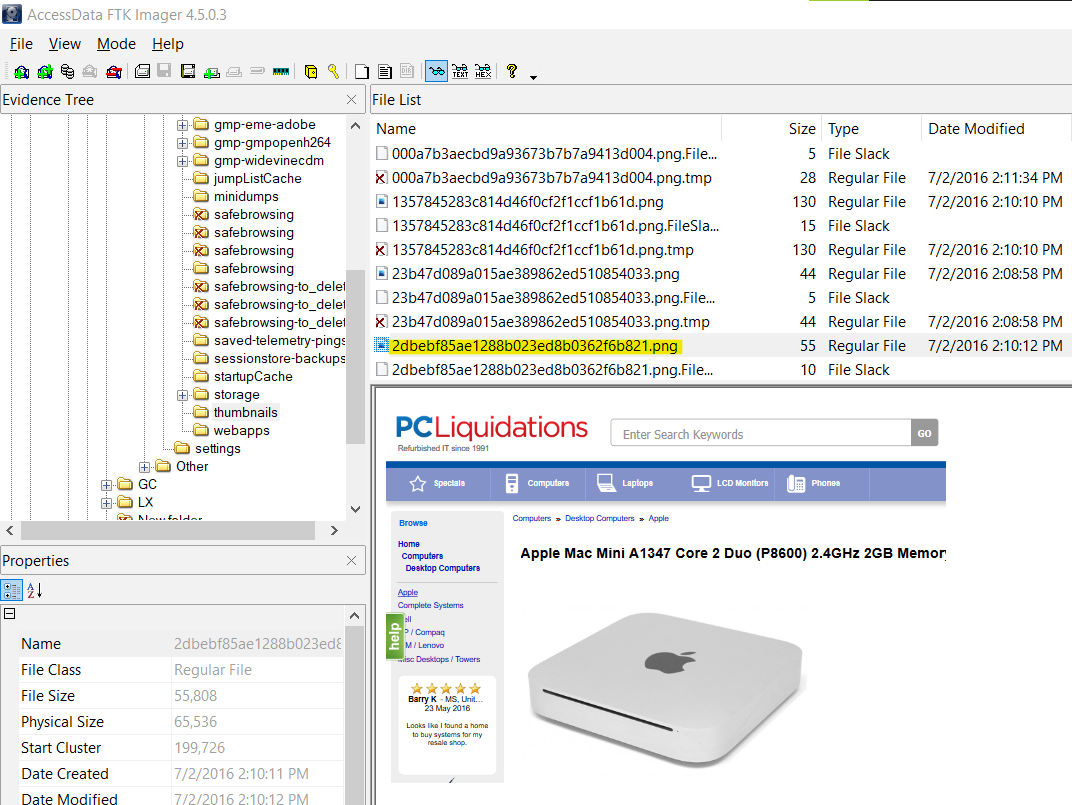
**PortableBrowser.E01 Partition 1\Transcend [FAT32]\[root] \InterWebz\FF\FirefoxPortable\Data\profile\thumbnails folder**

* **There are 3 picture files of an Apple Computer found as listed below-**

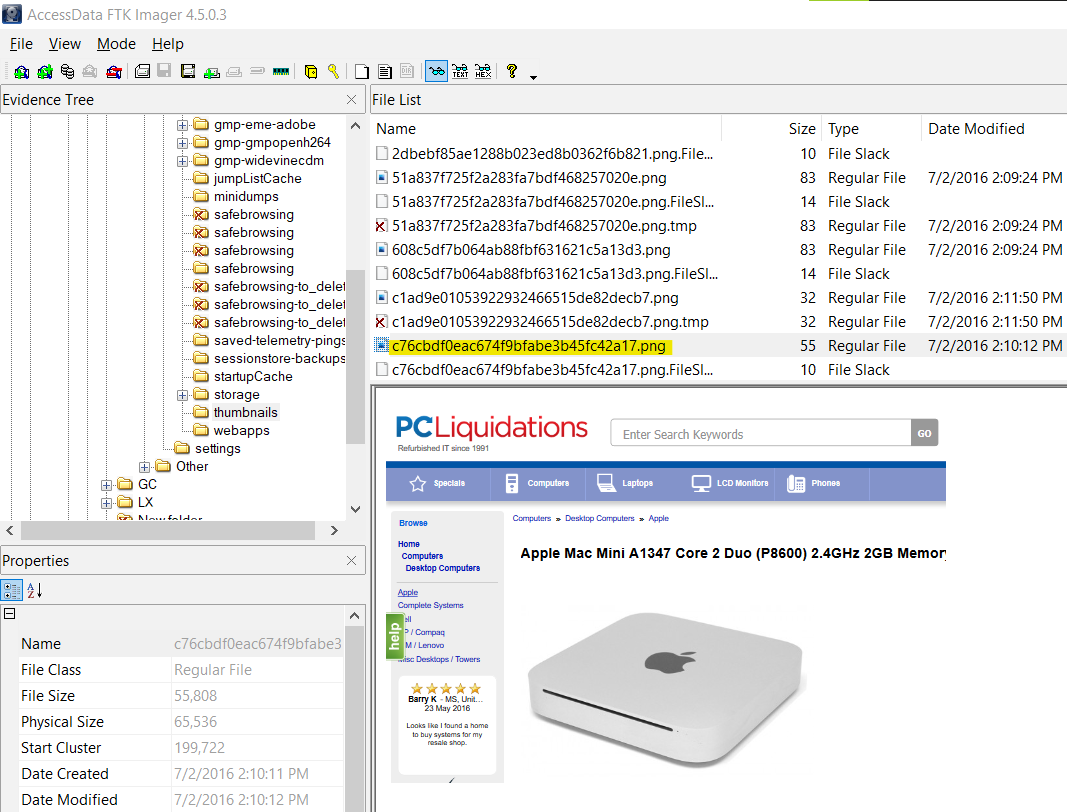
1. **1357845283c814d46f0cf2f1ccf1b61d.png**

****

1. **2dbebf85ae1288b023ed8b0362f6b821.png**

****

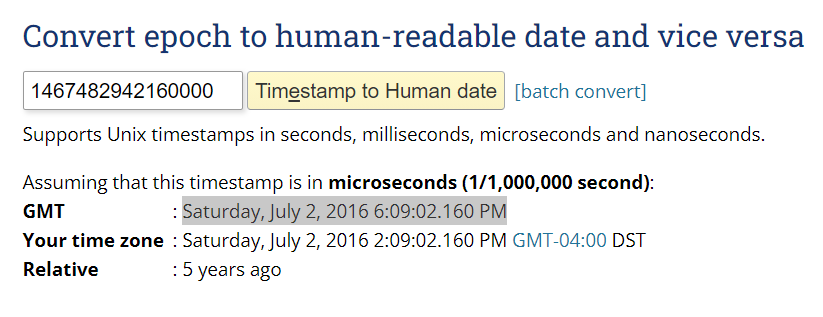
1. **c76cbdf0eac674f9bfabe3b45fc42a17.png**

****

1. **Ensure you have SQL Lite Browser installed (www.sqlitebrowser.org) and find the places.sqlite file (hint: you can create a file and directory listing with FTK Imager to a csv and search that). Open the file with SQLite Browser 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”.**

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

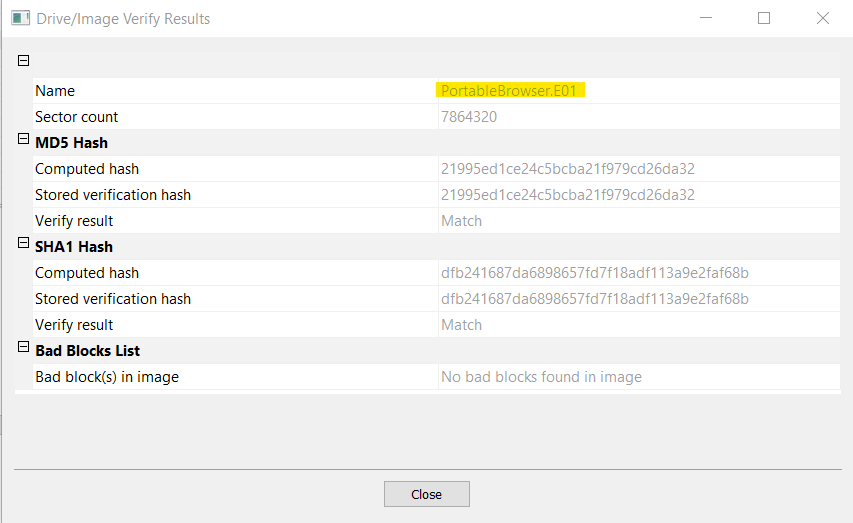
* **This page was accessed on Saturday, July 2, 2016 6:09:02.160 PM GMT. The time (1467482942160000) found from the SQLite Browser tool was in Epoch format. To convert it into human readable format,** [**www.epochconverter.com**](http://www.epochconverter.com) **site was used.**

****

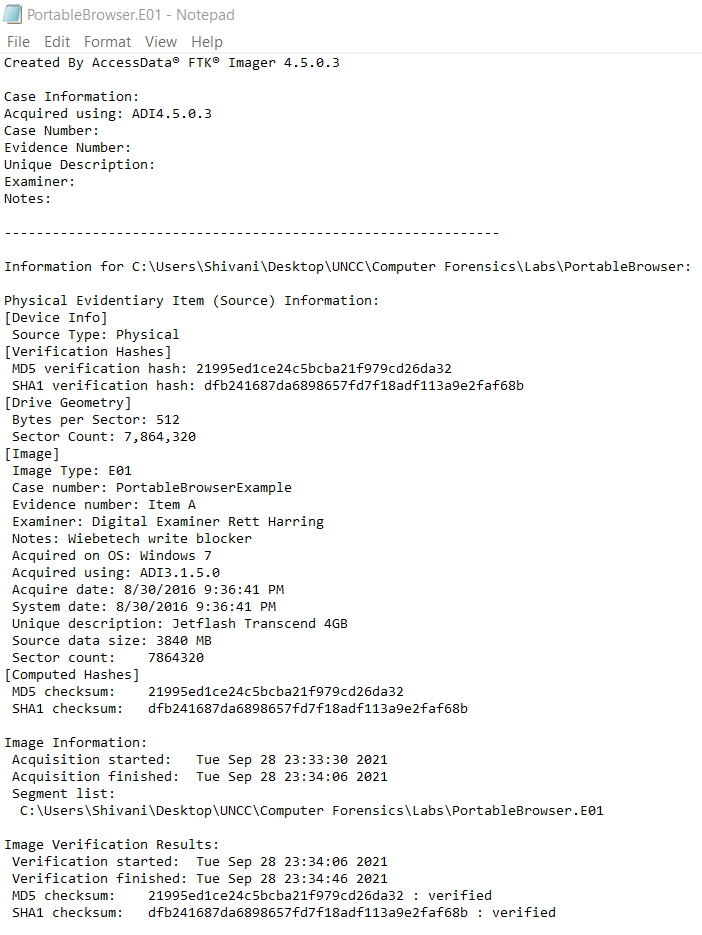
1. **Verify the images once more to ensure you have not altered them.**

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

* **Image was verified after analysis and the hash value matched the original hash values which suggests no alterations were made during the analysis.**



* **Yes, the record is added to the log file.**

****

**Conclusion:**

Overall, in this lab I was asked to determine if the user of the thumb drive had been looking at the prices of Apple computers on eBay or other sites. To begin the analysis, the image was loaded using AccessData FTK Imager 4.5.0.3 on a Windows 10 Machine and the hash value of image was verified to conclude that it was not tampered before the analysis process. All the questions regarding this case were successfully answered with the help of FTK Imager tool and DB Browser for SQLite. At the end of analysis, it was found that the user of the thumb drive was looking at prices of Apple computers on multiple sites as observed in the user’s browser activities and cache directories where pictures of Apple computer with pricing had been found. The image was again verified using AccessData FTK Imager to ensure it is not altered. No evidence has been retained. The forensic image, and answered questions regarding it, were returned to Dr. Robert Quincy.