ITIS 4250 / 5250

Lab # 2

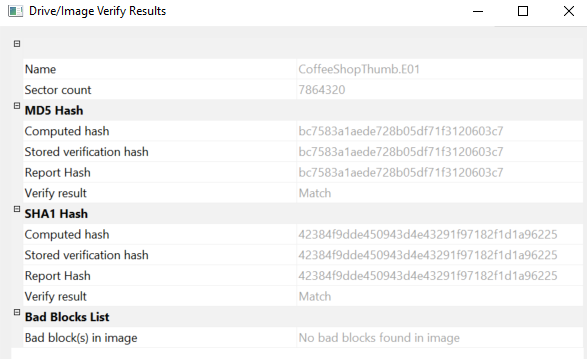
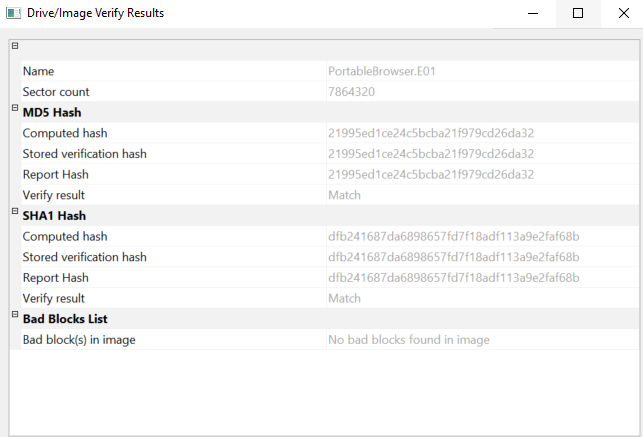
9/25/2019

**Overview:**

This task involves the investigation, validation and analyzation 2 E01 files ‘CoffeeShopThumb.e01’ and ‘PortableBrowser.e01’ for this task. There was proper legal approval for this investigation.

**Forensic Acquisition & Exam Preparation**

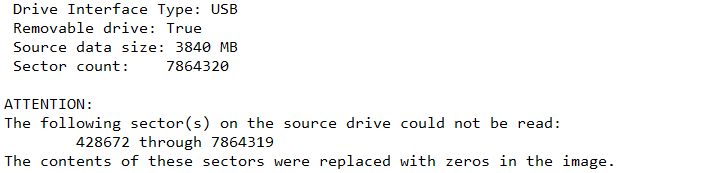
The first step was transferring the files (‘CoffeeShopThumb.e01’ and ‘PortableBrowser.e01’) from Canvas into a fresh folder on my work machine. My machine is a Lenovo Yoga 13 with 8gb of ddr4 ram along with an i5-8500. After transferring ‘CoffeeShopThumb.e01’ and ‘PortableBrowser.e01’ on my machine I verified both files hashes using *Access Data FTK 4.1.1*



**Findings and Report (Forensic Analysis)**

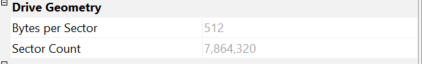
1. Judging by geometry, hash value, folder structure and the log files do these images appear to be of the same thumb drive? How are they similar and how are they dissimilar?

**The geometry and folder structure of these images appears to be the same. They both have the same geometry sector count of 7,864,320, and the folder structure is pretty much identical. When jumping into the log file you can see their key differences because they both have different (md5) hash values bc7583a1aede728b05df71f3120603c7 and 21995ed1ce24c5bcba21f979cd26da32. It appears on the CoffeeShopThumn.E01 there is a loss of data from sector 428672 through 7864319 compared to the other image when inspecting their log files.**



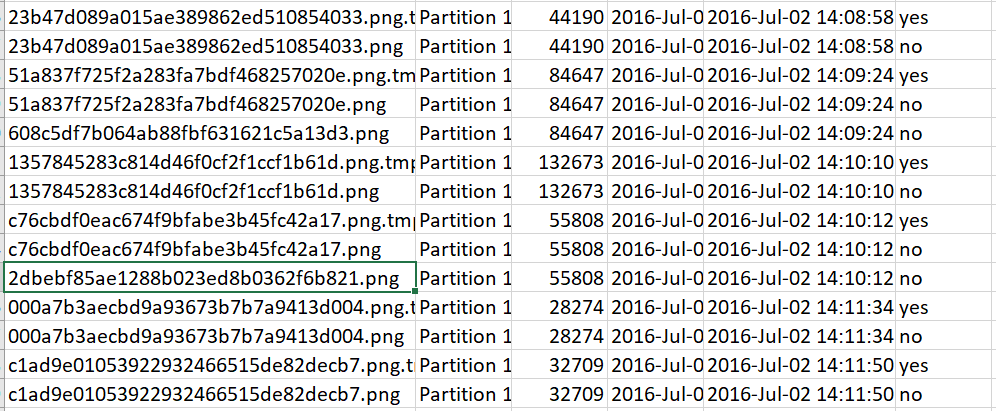
1. How many sectors do each of the images represent in total? Are there any errors showing one image did not record some of the sectors?

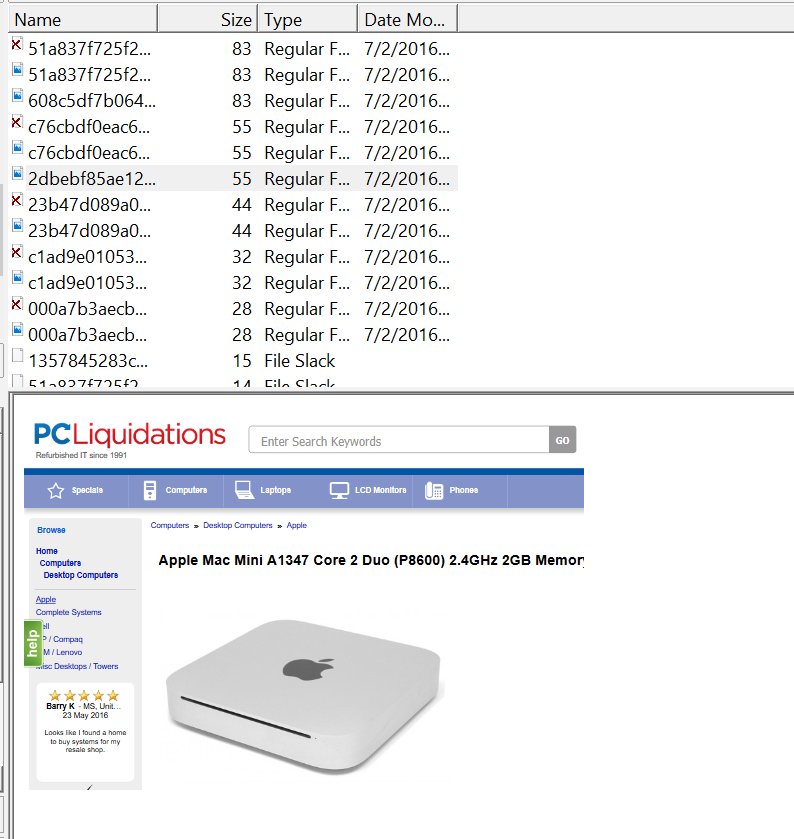
**Each image represents 7,864,320. There are 15,728,640 sectors in total when adding both together. On the Coffee ShopThumb.E01 there is unreadable sectors from 428672 through 7864319.**



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)

**The picture is located at Partition 1\Transcend [FAT32]\[root]\InterWebz\FF\FirefoxPortable\Data\profile\thumbnails\2dbebf85ae1288b023ed8b0362f6b821.png**

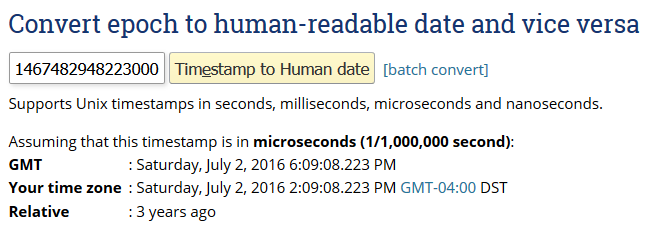
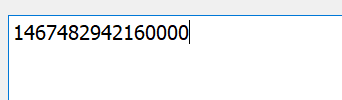




1. When was this page accessed? The date is in epoch format and will need to be converted (try [www.epochconverter.com](http://www.epochconverter.com)).

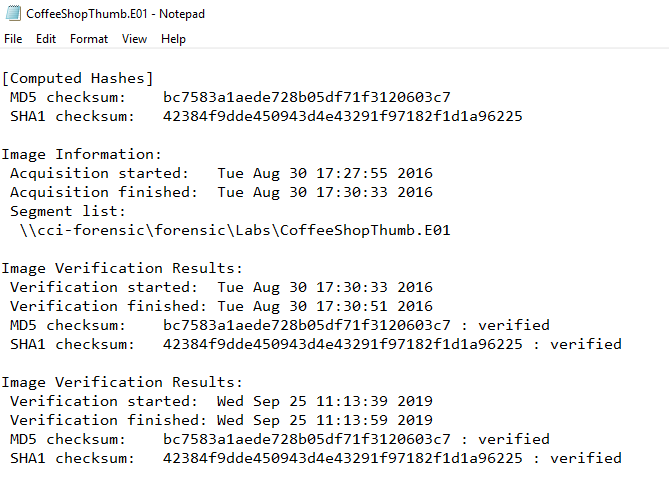
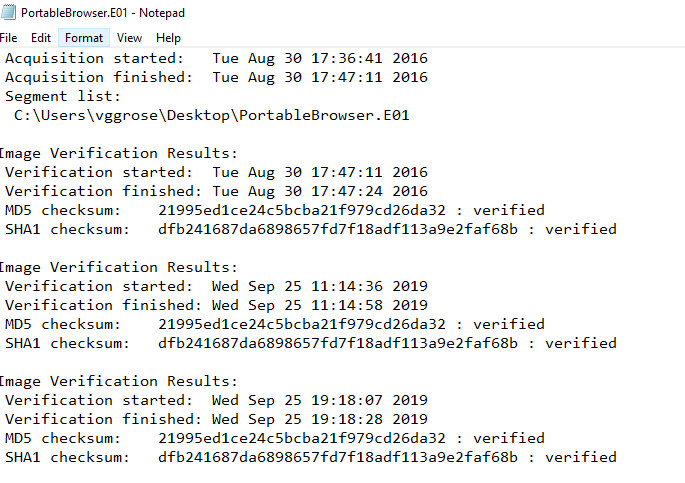
**The page was last accessed on July 2, 2016 at 6:09 PM GMT. This was found by investigation of the places.sqlite file at \Interwebz\FF\Data\Profile\. Using SQLlite I was able to find the page with the title “Apple Mac Mini A1347 Core 2 Duo (P8600) 2.4GHz 2GB Memory 320GB HDD” and from there get its epoch value and convert it to get the time of last access**





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

**When inspecting the log files after verifying both images ‘CoffeeShopThumb.e01’ and ‘PortableBrowser.e01’ there was a new entry that displayed that both images have been verified again.**



**Conclusion:**

After investigating both files CoffeeShopThumb.e01’ and ‘PortableBrowser.e01’ it appears that they are from the same drive. However, CoffeeShopThumb.e01 is unreadable at the sectors from 428672 through 7864319.Then after investigating the files on the drive I was able to find the lost image on the drive and find the epoch time of the last time the page that that image originated from.