ITIS 5250

Sahil Bhirud - 801138029

Lab - 2

**Overview:**

In this lab, I have been asked to examine two disk images, viz. **“CoffeeShopThumb.E01”** and **“PortableBrowser.E01”** using the FTK Imager Tool and SQL Lite Browser. I had to share my views on the similarities and dissimilarities in the two files based on the factors like drive geometry, folder structure, etc. I also had to find the location of a given image and the date and time when it was accessed.

**Forensic Acquisition and Exam Preparation:**

I downloaded the images on my personal laptop and used **FTK Imager Tool** to extract information from the disk images. The first task I performed was that I verified the hash values of the images. The result is shown below:

A screenshot of a cell phone

Description automatically generated

A screenshot of a social media post

Description automatically generated

**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?**

From the properties of both the images, I concluded that even though the images have the same size and are also of the same brand (Transcend), the MD5 hash values of both the images are different which means that the images are not identical.

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

Secondly, log file of **CoffeeShopThumb.E01** shows that image could not read some of the sectors on the source drive and hence the contents were replaced with zeroes.

A screenshot of a cell phone

Description automatically generated

The folder structure of both the images are same except that we could see some of the folders either empty or missing in **CoffeeShopThumb.E01**. Therefore, I infer that the sectors which couldn’t be read contained the missing contents of the drive.

A screenshot of a social media post

Description automatically generated

A screenshot of a social media post

Description automatically generated

1. **How are they similar and how are they dissimilar?**

Both the images have the same size, drive geometry and file system but they have different MD5 hash values since the contents are not the same in both the images.

A screenshot of a cell phone

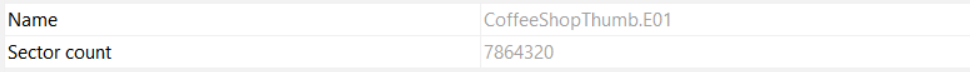
Description automatically generated

A screenshot of a cell phone

Description automatically generated

1. **How many sectors do each of the images represent in total?**

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

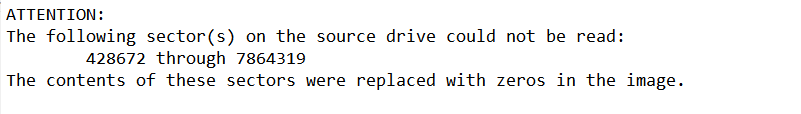


A screenshot of a cell phone

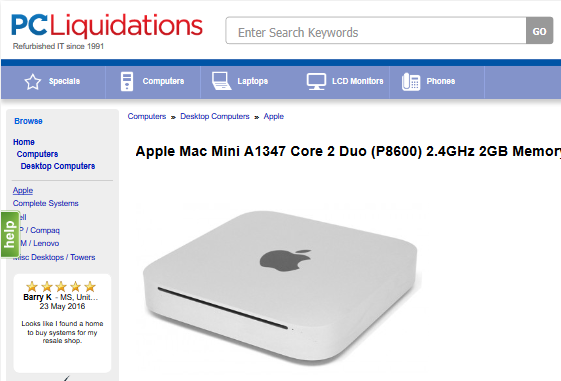
Description automatically generated

1. **Are there any errors showing one image did not record some of the sectors?**

Yes, the log file of **CoffeeShopThumb.E01** shows that the image did not record sectors 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)**

****

After checking the spreadsheet for PNG files, I found two files with this picture. They were located in the same directory in PortableBrowser.E01: **Partition1\Transcend[FAT32]\[root]\InterWebz\FF\FirefoxPortable\Data\profile\thumbnails\**

A screenshot of a cell phone

Description automatically generated

1. **Ensure you have SQL Lite Browser installed (**[**www.sqlitebrowser.org**](http://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”.**

**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 image was accessed on the website [www.pcliquidations.com](http://www.pcliquidations.com)

The epoch time of the last accessed time of the page is **1467482942160000.**

A screenshot of a computer

Description automatically generated

A screenshot of a cell phone

Description automatically generated

As seen, the website was accessed on **Saturday, July 2, 2016 2:09:02.160 PM (GMT).**

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?**

Final MD5 hash verification of CoffeeThumb.E01:

A screenshot of a cell phone

Description automatically generated

Final MD5 hash verification of PortableBrowser.E01:

A screenshot of a cell phone

Description automatically generated

Also, an entry was added in the log files of both the images, representing that hash verification was done.

A screenshot of a social media post

Description automatically generated

**Conclusion:**

After the acquisition and examination of the two image files I have concluded that:

1. Both the images are of the same thumb drive, having the same size and brand name.
2. The MD5 has values are different because the contents in the images are different.
3. The contents are different because CoffeeShopThumb.E01 image did not record all the sectors.
4. The given image is located at “Partition1\Transcend[FAT32]\[root]\InterWebz\FF\FirefoxPortable\Data\profile\thumbnails\” in PortableBrowser.E01 and was accessed on Saturday, July 2, 2016 2:09:02.160 PM (GMT).
5. Every hash value verification record is added in the log file.