Homework 11: Windows Forensic Exam

Vinitra Ramasubramaniam(590F), Gowtham Rangarajan(590F), Samuel Remis(365)

1. Tools Used:

- Autopsy 4.3.0 - "is an end-to-end open source digital forensics platform that makes file system image analysis easier without sacrificing the benefits of open source software". It has been tested by the NIST and hence it is forensically valid.
- Thumbcache viewer 1.0.3.4 - helps open thumbnail database files and view the thumbnail images that were created on Windows Vista, Windows 7, Windows 8, Windows 8.1, and Windows 10. This is forensically valid as it only retrieves views files and does not alter them or create new images in the .db file. Because of this, it may miss some files but any images found using this tool are forensically valid.
- 8zip Lite 1.2.121.0 - helps to unzip the compressed image of the disk in question. This is forensically valid as it is only used to unzip files and does not alter them in any way.
- http://htmledit.squarefree.com/ - an online html viewer to view html code as it would appear on a website. Since we only used an online compiler, anything that shows up can be considered forensically valid.

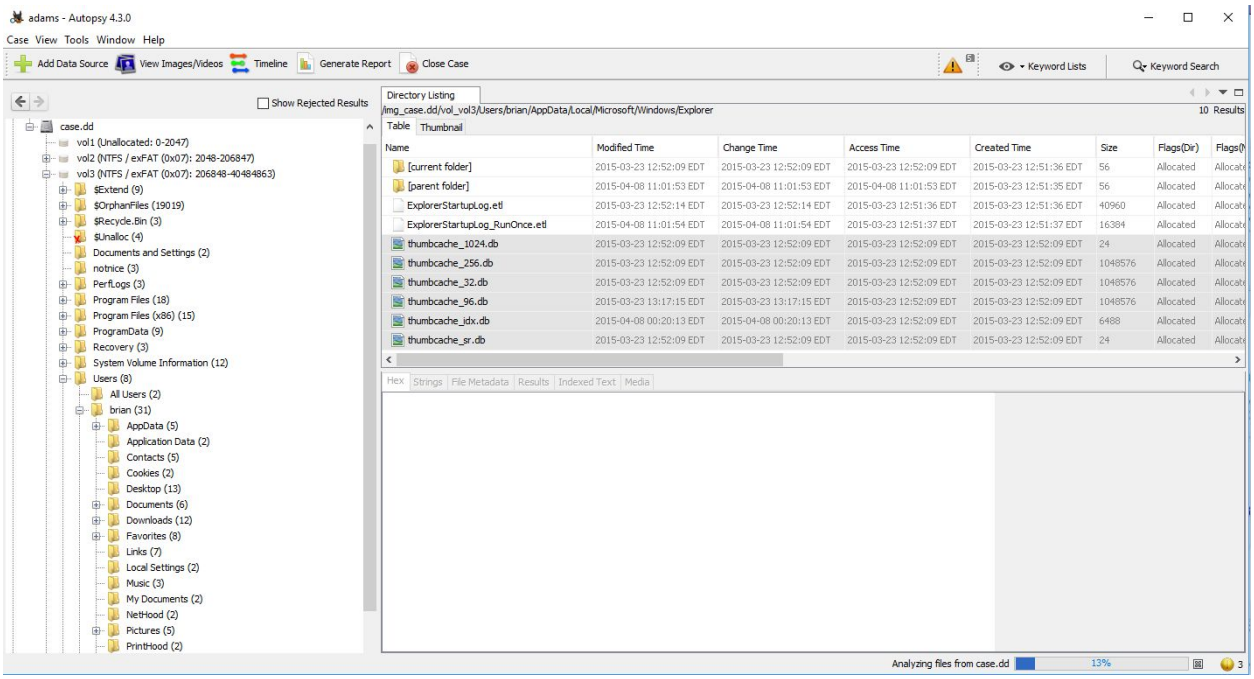
Extraction:

To examine the image, we used 8zip to unzip the image and autopsy to examine it. Through looking at the volumes on the computer, it quickly becomes apparent that most of the relevant data will reside on volume 3; volumes 1 and 4 are empty, and 2 is full of system files that haven't been touched by the user. All user data seems to be residing in volume 3, so we will be referring to only that image from here forward.

2. Processes:

Investigation for Zebra Images

1. **Thumbnails:**
    a. The first thing that we did was attempt to access the thumbnails folder of Brian's copy of windows, because users often overlook that thumbnails are automatically created and saved in a hidden cache every time an image is opened. This is a forensically valid method as it was used by the FBI in 2008.
    b. In order to access the thumbnails, we used autopsy and navigated to the thumbcache folder at /Users/brian/AppData/Local/Microsoft/Windows/Explorer. We selected all of the db files and then extracted them to the local drive. The folder in autopsy with the highlighted db files is shown below.



c. We then opened the db files in thumbcache viewer to see what each thumbnail image looked like. The viewer took the .db files and turned them into a list of files that contained the cached images.
Considering the volume of images, the first thing that we did was trim down the folder of irrelevant images. The trimmed images include png photos since they were images of folders, images that were known to come with windows, and any files that had a size of 0kb in the cache since they contained no useful information. The remaining files as seen in Thumbcache viewer as well as each of 7 unique thumbnail in its largest original resolution are pictured below:

Thumbcache Viewer

File Edit View Tools Help

#	Filename	Cache Entry Offset	Cache Entry S...	Data Offset	Data Size	Data Checksum	Header Checksum
1	38e0def11725e46b.jpg	152960 B	6 KB	153040 B	5 KB	6930cbfab5a0c0ec	db78a436d5aa981d
2	1ef5d97562e4321.jpg	168188 B	6 KB	168266 B	6 KB	f2a4b874f62b0aa8	c4d209249849b0c3
3	1a9568ac930c580a.jpg	193749 B	7 KB	193829 B	7 KB	8b98cd0d25d572a1	45c38ac3dfc9473d
4	f8b718a1b33f6de1.jpg	185889 B	7 KB	185969 B	7 KB	9dab4ea064fff19f	844d645ed46e25c6
5	fe242e1121aa88a8.jpg	278259 B	8 KB	278339 B	8 KB	74b72cf220b75871	27a0e23bb52da893
6	69bf29ef4fd086c0.jpg	159176 B	8 KB	159256 B	8 KB	1869c6828b9986b6	d2ff954ca7697e18
7	35a00b7513064b6b.jpg	15943 B	9 KB	16023 B	9 KB	b00297fceaed790e	46b70916a598554a
8	583938e1aae79cd0.jpg	174552 B	11 KB	174632 B	10 KB	eff372f296409800	070831b674f6540c
9	4e8432f976b82494.jpg	587661 B	11 KB	587741 B	11 KB	a412dab56bee0ad1	5542c0f05f542f06
10	9456216eb58f366c.jpg	599651 B	11 KB	599731 B	11 KB	a412dab56bee0ad1	b292a8aee39b3a95
11	eefd5e7af85b5f9b.jpg	3910 B	11 KB	3990 B	11 KB	24563cd287fbc2d2	d6994aca58d5a6db
12	d60cc76eb37d9d7a.jpg	417218 B	12 KB	417298 B	12 KB	1fdc1661ef9537bd	07159387f6f58562
13	a31e887baa72c012.jpg	231852 B	13 KB	231932 B	12 KB	811a1a66bb0a30b6	92245d2ce14e7196
14	?d050411b?170000000...	447111 B	13 KB	447207 B	12 KB	811a1a66bb0a30b6	87b4647d14f744e5
15	65d3cc65bb130ae.jpg	571657 B	15 KB	571735 B	15 KB	9d718bd2ff52241c	d02bdf15fe1c39c1
16	a7cc6df7252239f3.jpg	245166 B	15 KB	245246 B	15 KB	bfe10376353b5132	6ee7c24042176ff7
17	?d050411b?160000000...	460441 B	15 KB	460537 B	15 KB	bfe10376353b5132	7a2354802446718f
18	a11df6cbdc77a810.jpg	261177 B	16 KB	261257 B	16 KB	8d2b6258597a40bf	f43b597f5736c53e
19	?d050411b?170000000...	430013 B	16 KB	430109 B	16 KB	8d2b6258597a40bf	22f855b14d0c1794

d. Since thumbnails are created only if an image is stored in a directory and opened by a user, this is incriminating evidence. The evidence indicates that these images were stored and opened by someone with access to this computer.

2. **<u>Web data</u>**

The next thing we did was extract some data on his web history using autopsy which is listed on the results tab under extracted content. A user's emails, web history, web cache and web search history could contain valuable evidence that either support or refute the defendant's claim that he was "not into zebras". The reviewed sections are listed below.

a. Cookies:

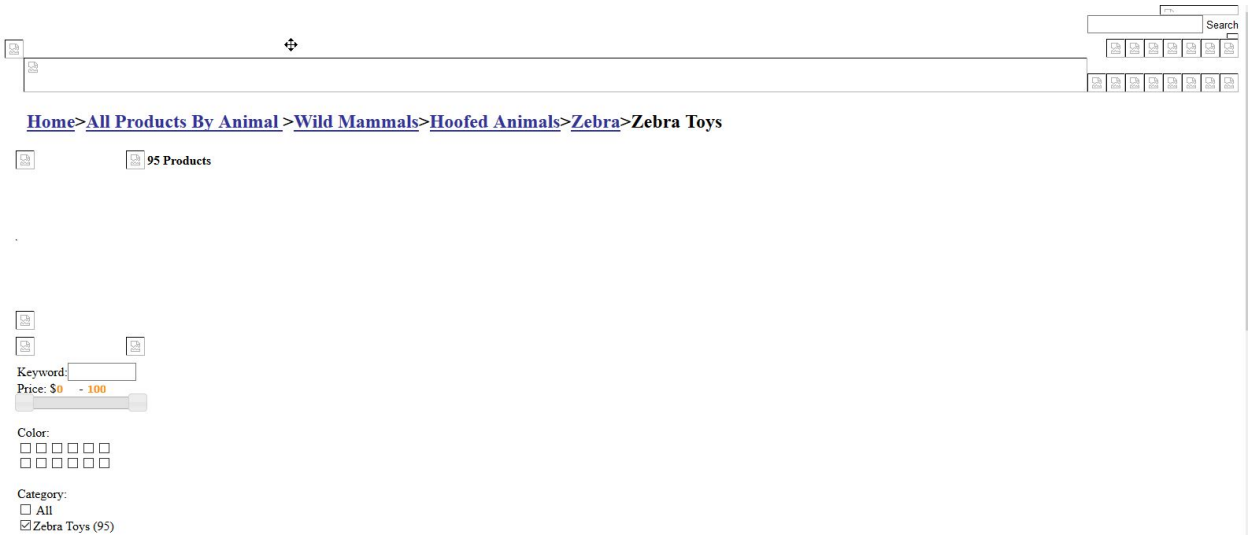
The cookies that were suspicious and we looked into are listed below, as well as the implications of what we found.

i. Eqads.com: this link looked suspicious at first, since it sounds a bit like equine. Upon further examination, this link was not suspicious and was in actuality a site related to ads.
ii. Thebigzoo.com: this link proved to be much more significant: it is a site that sells animal toys aimed at children. There is a section of this site dedicated only to zebras. This is incriminating because a site that sells zebra paraphernalia was tracking his internet history, meaning someone who had access to his computer likely accessed that site.
iii. Secure.thebigzoo.com/shopping: this link is a subsection of the above link. This is further incriminating through suggesting that he logged in and was shopping. The name "secure" in the site suggests that he was logged in and actively using the site.
iv. Bittorrent.com: A site known for downloading images for peers. While not directly incriminating by itself, it is a site that opens the door for illegal downloads to take place.

b. Web History/Search:
An analysis of his web searches through his computer revealed multiple searches for zebras taking place on April 8th 2015 between 04:00 and 04:20. These details and timeline are accounted under "V0100006.log" under the "WebCache" folder. Relevant browsing history is listed below in order of time visited:
i. On April 8th at 04:05, he performed a yahoo image search for "Zebras" and viewed multiple image results.
ii. At 04:06, he performed a yahoo web search for "zebras private download".
iii. At 04:17, he performed a yahoo web search for "zebra jpg 1024".
iv. He viewed a zebra image on flickr at 04:18.
v. Fifteen minutes later at 04:19 he performed a google search for zebras. The exact link of the search can is hyperlinked in this text and viewed 15 images of the animal.
vi. He followed the google search to the wikipedia article for zebras where his computer accessed links to at least 12 images of the animal.
vii. He clicked the back button and then clicked on another google search result. This link was to a broken wikipedia page for Grant's Zebra. His history suggests that he did not perform another search after this.
viii. The computer has cached numerous zebra images between 00:04 and 00:19 on 8th April 2015 under the "Temporary Internet Files" folder. The cached images also include images from www.thebigzoo.com, most of them being zebra paraphernalia.

c. Emails:
i. There was an email from zookeeper@thebigzoo.com that was only html text. When pasted into an html editor, it returned a page with the search

for zebra toys shown below:



3. **Recent Documents:**
   The recent documents folder contains automatically generated link files to recently used documents. Since the link files are automatically generated, this is a potential avenue to find evidence if the defendant hasn't cleared the "Recent Documents" history.
   a. There are link files generated for accessing a removable drive D:\ and an image file "website-Zebra.jpg" on this drive.
   b. He accessed multiple files and folders whose contents appear to be gone from the filesystem.

4. **Deleted files:**
   When a user deletes a contraband file, it is evidence that he/she wants to hide evidence of possession. If we can find evidence of multiple contraband files that have been deleted, it would be valuable evidence against the defendant.
   a. He deleted the images cached under the "Temporary Internet Files" folder.
   b. He deleted an 'unusual-facts-about-zebras.jpg' in his "pictures/pic" folder on at 12:58, 8th April 2015.

Investigation for Contraband Meeting

To investigate the claims of plans to travel to Monterey California for a meeting to exchange contraband, the following techniques were used. All dates and times listed are relative to each other and not absolute.

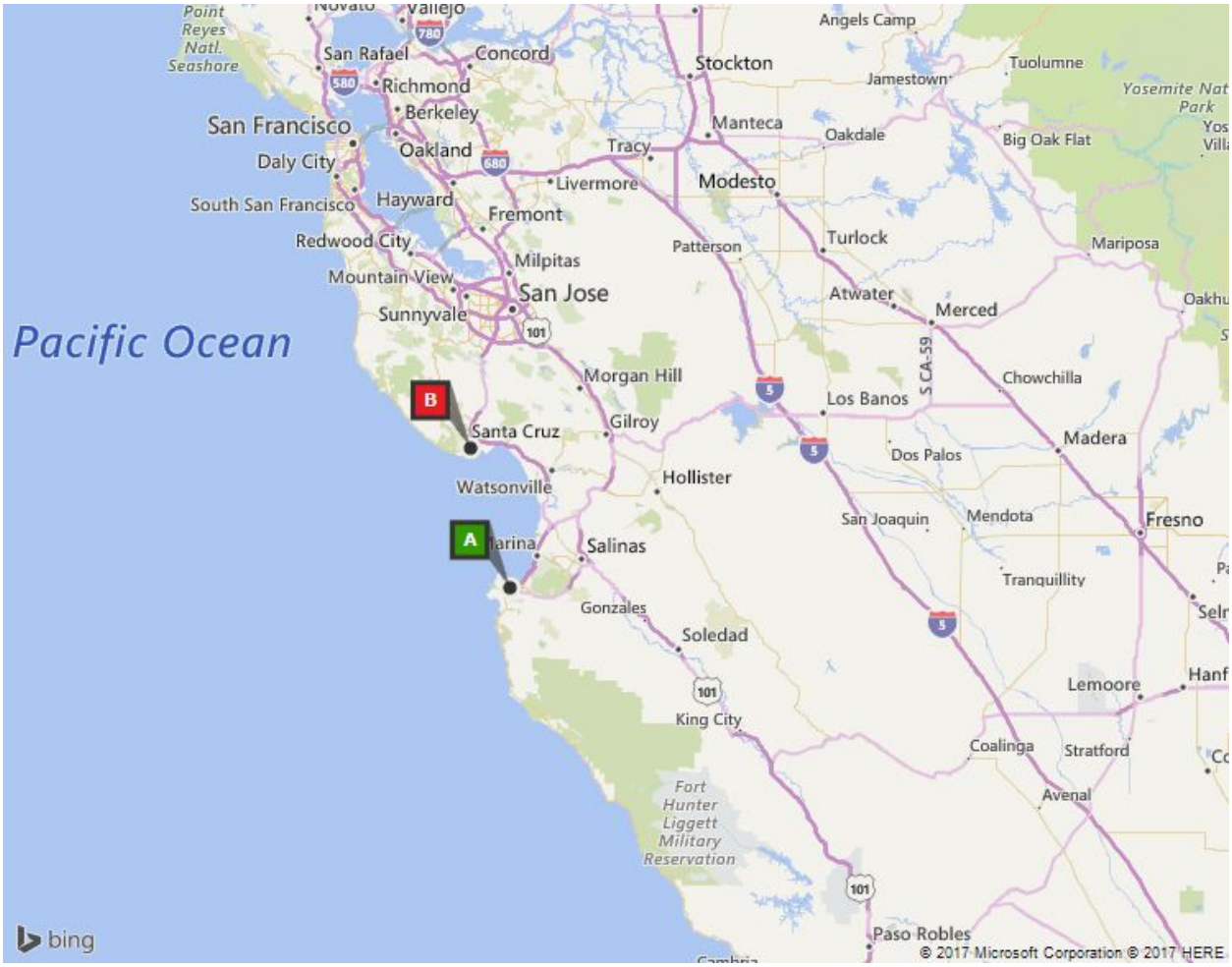
1. **Web History:**
   A user's web history, web cache and web search history could contain valuable evidence that either support or refute the defendant's claim that he had made "no such plans to travel"
   a. Searches:

i. A search for maps was performed on April 8th just after 03:00, suggesting that he was looking for directions somewhere.

b. Web history:

i. On April 7th around 23:54, he conducted a search on bing for directions from Monterey to Santa Cruz. The image of the map was cached in the “Temporary Internet Files”.

ii. On April 8th around 03:54, the same image of the map was cached again. The image is shown below:



Investigation for Meetings with Shima Uma

To confirm/refute Shima Uma’s claims that he met with the defendant and transferred contraband Zebra images to the defendant’s computer, the following techniques were used:

1. **<u>Recent Documents:</u>**

   The recent documents folder contains automatically generated link files to recently used documents. Since the link files are automatically generated, this is a potential avenue to find evidence if the defendant hasn’t cleared the “Recent Documents” history.

a. The link files in the “Recent Documents” folder suggest that he most recently inserted a removable drive mounted on “D:\” into his computer on April 8th at 12:41 and accessed this drive.
b. The details of the removable disk are:
Device Make - Alcor Micro Corp,
Device Model - Flash Drive
Device ID - DCEAF313
c. The link files in the “Recent Documents” folder suggests that an image file named ‘website-Zebra.jpg’ in the removable drive (D:\) was accessed on 8th April at 12:41.

3. Conclusions:

Possession of Zebra Images and intention to possess

- The defendant’s claim that he is “not into zebras” seems highly unlikely based on the amount of contradictory evidence found on his computer including but not limited to, thumbnail images of zebras, internet searches for them, and shopping on a site known to sell contraband (Refer Section 2: Investigation for Zebra Images). The defendant did possess contraband on his computer.
- It is virtually impossible that he had no knowledge of the files, as he actively performed web searches for zebras and related terms, then cleared his cache, and then searched for them again. Clearing the cache shows knowledge of possession and intention to get rid of the contraband under possessession. (Refer Section 2: Investigation for Zebra Images).
- Based on the above points, we can conclude that the defendant knowingly possessed contraband Zebra images on his computer and viewed images on the internet with the intention to possess (although the images found on the defendant’s computer were cached images, the cached images did exist at some point on the defendant’s computer). The fact that the defendant installed bittorrent also supports our argument that the defendant had an intention to possess/distribute.

Intention to trade of contraband

- From the fact that defendant had performed a search for directions from Monterey to Santa Cruz (a cached image of the map), and then deleted his cache, we can conclude that he had intentions to both make the trip and hide evidence of this trip (Refer Section 2: Investigations for Contraband Meeting)

Meetings with Shima Uma

- The claims made by Shima Uma that can neither be confirmed or refuted. During the time frame mentioned by Shima Uma, a removable device was inserted into the defendant’s computer which potentially contained a contraband image of a zebra (Refer Section 2: Investigation for Meetings with Shima Uma). However, we didn’t find any evidence that suggests that the image was copied onto the defendant’s computer.