COMP2310 Digital Forensics

Assignment 1: Digital Forensic report

Due: April 10, 2022.

Contents

Abstract

This digital forensics reports and investigates the findings of the supplied data images primarily with Autopsy, answering five key questions regarding the nature and evidence that was included in the images. Through following a methodological approach, this report satisfies current industry best practices and regulatory standards of investigation. The acquisition of the evidence has been included, and the steps taken in answering the questions were recorded, taking care to show how the final answer was attained. An appendix at the end of the paper has been included, listing key figures and tables acquired from the investigation.

Acquisition

In November 2019 the Australian Intelligence Organisation (ASIO) had tracked the suspect down. In 2020 an examiner completed a network acquisition with a wireless antennae the suspect's computer whilst it was asleep on our behalf. The computer had no password. The acquirer's operating system was Windows XP, software version 4.19.a. There were 8 images acquired: 2 Encase images and 8 disk image parts. The images were examined on a Dell XPS 13 9305 with Windows 10, with Autopsy version 4.19.3 and AccessData FTK Imager 4.5.0.3**.** From the "file metadata" tab in Autopsy, we can determine the hashes of the images to validate the data (see fig. 1). Comparison between the hashes of the images in Table one, and a suspect log confirm that the DD images were the same as when they were acquired (see Fig. 2). Table 1 displays the MD5 hash for Encase.E01/2: aee4fcd9301c03b3b054623ca261959a.

The suspect log (Fig. 2) lists the size of the drive in which the DD images were acquired from as 4.5 GB from a drive with a model number of IBM-DBCA-204860, and a serial number of HQ0RQQF7429. As seen from the file metadata of the Encase file on Autopsy and the suspect log, the acquiring examiner's name is Shane Robinson, and his operating system was Windows XP with an Autopsy software version of 4.19a, with a drive size of 186.3 GB. The current examiner's operating system is Windows 10 Home on a Dell XPS 13 9305 with 16 GB RAM.

The file was loaded into Autopsy [1] by creating a new case, specifying the case name (COP2310-ASS1), and loading in the image files. First, the Encase.E01 was loaded in, with Encase.E02 following automatically, with all ingest modules selected. Next, 8 DD images were added individually, again with all ingest modules selected according. Selecting all the ingest modules enables us to better analyse the suspect's drive by utilising all of Autopsy's provided tools, including the timeline tool.

Evidence analysed

As mentioned, a DD image (in 8 parts, with a suspect log) and an EnCase image (in 2 parts) were acquired from a Dell Latitude Cpi computer. The details of the MD5, and SHA1 and SHA256 hashes can be seen in the Table 1. The file metadata of the images (Fig 2.) reveal that the owner of the drive is Greg Schardt, and the device ID of his computer is "bdb1747d-fae6-4fd3-8438-7b0104e2e52a". The size of the drive was 4.87 GB (the Encase images and DD images combined).

1. What is the image hash? If you are informed that the verification hash is AFF4ECD9301C03C3C054623CA261959A, what would the hash comparison imply? (Disregard this verification hash after this question.

As previously mentioned, the image hash is "aee4fcd9301c03b3b054623ca261959a", which was obtained from the file metadata information from Autopsy (Fig. 1). The hypothetical verification hash of "AFF4ECD9301C03C3C054623CA261959A" does not match the MD5 hash of the Encase files. It also does not match any of the image hashes of the 8 disk image hashes. To confirm the established verification hash, I performed a file validation with FTK Imager [2] by loading the image into the program, and then navigating to the file ribbon, then "Verify File/Image." The verification further confirmed the MD5 hash of being aee4fcd9301c03b3b054623ca261959a (Fig. 3). A comparison between the hashes would imply that the data source has been altered or corrupted in some way, hence the verification hashes do not match.

2. What web browsers were used between 09:00 and 18:00?

On Autopsy, navigating to the "timeline" ribbon at the top of the page, and filtering the results to "Web activity" between the chosen date of August 25, 2004, 09:00-18:00 shows a graphical representation of the 4 web activity listings: Web bookmarks, web cookies, web history, and web search. Comparing this representation (Fig. 4.) to the listings (Fig. 5.), shows it is easier to use the timeline tool to filter for time-based results. Unfortunately, it does not specify the program name, although the web activity listings do.

To get a greater understanding of the web activity, the contents of the web history listing can be exported to a Excel [3] sheet by selecting the "save table as CSV" option in the top right of the listing results. Then, the web results can be ordered and sorted based on the date and time using the "sort" feature. Next, I navigated to the "data" ribbon and filtered the results to exclude any time not on the August 25, 2004. From this, the results between the specified time of 09:00 and 18:00 can be easily found. Upon inspection, the only web browser used was "Internet Explorer." Repeating the same steps with all the other web activity confirms that only Internet Explorer was used. This can also be confirmed by sorting from the "Date accessed" on the listings (Fig. 6.).

3. From the web browsers, list every keyword searched and URLs with their Timestamp.

As seen from Table. 2 And Fig. 7 in the appendix, there are four keywords searched. These can be found in the "The first keyword is "who am I," also searched on Google.com (http://www.google.com/search?hl=en&ie=UTF-8&q=who+am+i), on August 24, 2004, 16:07:32 AEST. The second keyword is "what is my ip," searched on Google.com http://www.google.com/search?q=what+is+my+ip&hl=en&lr=&ie=UTF-8), on August 25, 2004, 16:07:51 AEST. Both keywords appear to have one duplicate search each. Comparison between the web search and web history sections (which has 887 items) reveal that the suspect probably cleared their browser history since there are only 4 searches.

The keyword search results, and other web activity information found on Autopsy are obtained from Internet Explorer index.dat file, a binary log file which stores information about the browsing history, and other activity [4]. Fig 7. Displays some of the "indexed text" tab of the index.dat file which is used to find the keywords searched. The web pages visited are listed — because index.dat stores the visited URLS as well. We can find our keywords searched in the indexed text (because the web search listing for Autopsy does not list the URL, only the domain) and find the exact URLs searched —see Fig. 7 and Table 2. Interestingly, there are no duplicate searches in the Indexed text; perhaps they were searched or loaded twice.

4. What may the files in My Documents/DICTIONARIES be used for?

At first glance, all 6 files in the "DICTIONARIES" folder appear benign, but further investigation suggests that they have a more malicious purpose. The DICTIONARIES file can be found by expanding the Encase.E01 volumes and navigating to "My Documents." The files it contains are interesting:

“Biglist_990218.zip” is 8.7 MB and contains a text file that reveals it contains unique words for password cracking programs (Fig. 8). Indeed, “Biglist_990218.txt” contains a dictionary of strings.

“250MB_WORDLIST.ZIP” is 245 MB file that contains a “Words.lst” file which has a large collection of strings: snippets from websites, plays, books, code, other apparent gibberish.

“Pocket-dic.gz” is 66392 bytes with one file, “pocket-dic,” Listing numerous words alphabetically.

“Test.zip” has a size of 6.4 MB, containing two files: “test.csv” and “test.tab.” They list strings in csv and tab format, respectively.

“Unix_dict.gz” is 77509 bytes and contains one file, “unix.dict “ that also contains a collection of strings.

“words-english.gz” is 85751 bytes, with one file, “words-english.” Like all the files before, it lists numerous strings alphabetically.

After examining the files in DICTIONARIES, it appears evident they were used as cracking dictionaries. Cracking dictionaries are known to be used by hackers to crack passwords. They are often large lists of data containing strings/words —strikingly similar to what we can find in the DICTIONARIES file [5]. It should be noted that the other folders in “My Documents” seems connected to hacking activities as well; the “FOOTPRINTING” folder appears to contains network utility programs and scanners including “SuperScan,” [6] “NetScanTools”, and “nmapNT”; the “EXPLOITATION” folder contains several programs, including “Brutus,” a password cracker, “BUTTsniffer,” a IP and port filter, and other probable exploitation tools; “ENUMERATION” appears to have executables related to web-scanning and information gathering; the other folders appear to be related to hacking, as well.

5. Are there any suspicious-looking encrypted files? If so, please briefly explain how you obtained the contents.

Although Autopsy lists 2 files with suspected encryption in its “Encryption Suspected” listing under “Analysis Results,” it is likely that they are not encrypted. The two files are the same file, “oembios.bin,” however located in different locations. One file path is “/img_Encase.E01/vol_vol2/WINDOWS/system32/oembios.bin, and the other is ““/img_Encase.E01/vol+vol2/WINDOWS/system32/dllcache/oembios.bin.” The file type of “File System” can be acquired from the file metadata information. There are also two other files listed alongside oembios.bin: “oembios.dat” and “oembios.sg.”

The purpose of the oembios.bin files are obscure; however, it appears to be a way for the original equipment manufacturers (OEM) to activate licenced copies of in this case, Windows XP, automatically. The SHA-256 hash of the file is "c5c5cdfeb03f390c3ea4c86d668c74926815a1b3d26c55b2d310212bf511b7b8," and pasting it in virustotal.com reveals it was an authorised file created by Microsoft for Windows XP — the manufacturer, disproving Autopsy's conclusion of the files being suspicious (see Fig. 10).

Autopsy had flagged the oembios.bin files as "Suspected encryption due to high entropy (7.999987)" (see Fig. 9). Entropy is used to identify encrypted or compressed files — something utilised by malware authors. A file with high entropy or randomness generally correlates with the use of compression or encryption [7, p. 40-41]. For some reason they have high entropy, even though they have no reason to be encrypted. Perhaps they are compressed or protected in some way. There is probably no way to obtain their contents, and there probably would not be much to see in the files anyway.

Conclusion

Through the careful analysis of the provided evidence and the use of Autopsy, the five required questions were able to be answered satisfactorily. Additionally, the acquisition of the data sources has been recorded, detailing data hashes and other important peripheral information. The supplied figures and tables better illustrate the steps of the investigation and how the five answers were obtained.

Appendix

Image information				
	MD5	SHA1	SHA-256	size
Encase.E01/E02	aee4fcd9301c03b3b054623ca261959a	n/a	n/a	4871301120
Suspect.001	aee4fcd9301c03b3b054623ca261959a	da2fe30fe21711edf42310873af475859a68f300	65e2002fed0b286f49541c7e97dcec0dda913d51a063ceeed86782bdacda2312	4871301120
Suspect.002	c7227e7eea82d218663257397679a7c4	0dc6676b3aa26634a07aa87813b3125a1cbe1cc9	bef9f7fd39abc1f8e52c7b532b552c7f36c8e5ae8ffb22695cfae3d7a621a292	66623897 6
Suspect.003	ebba35acd7b8aa85a5a7c13f3dd733d2	6c9b58bd55444e50dd83e35c2fb7debf77ec1f1d	37238e7067145ff3c4b2686bd87d6b14d86f0114af4df1366cb726c84d673b4e	66623897 6
Suspect.004	669b6636dcb4783fd5509c4710856c59	9d958582823cc0db882ba148907912336ddceb4f	b665818259fe34789bae514bd182940c745d73e83527ffb04abac32631d949d3	66623897 6
Suspect.005	c46e5760e3821522ee81e675422025bb	aa06b8322c44490a15cae1f1d2014932529df2ba	d7f5109fb7ae257945ae69952f5751e49cbe8f920f08cef24b1f0b1e362227fd	66623897 6
Suspect.006	99511901da2dea772005b5d0d764e750	301f37c1224755f9496d07ec563ff7a0155f3e06	bcd15a7a7c0522600afee9c83c298072ed9ce2b5a03a4620c21c2b016005148f	66623897 6
Suspect.007	99511901da2dea772005b5d0d764e750	301f37c1224755f9496d07ec563ff7a0155f3e06	bcd15a7a7c0522600afee9c83c298072ed9ce2b5a03a4620c21c2b016005148f	66623897 6

Suspect.008	8194a79a5356df79883ae2dc7415929f	b7a51bdfa587fedb5febfd1fe9017aa04d9988fc	7a944d162497d5abbbd01899106ebee724cee23b4e8c59e536437b2656d59774	20762828

Table 1. Validation and verification hashes (MD5 and SHA-256) of data sources and size of data sources.

Web Search Information			
Keyword searched	Domain	Timestamp	URL
“what is my ip”	Google.com	2004-08-25 16:07:51 AEST	http://www.google.com/search?q=what+is+my+ip&hl=en&lr=&ie=UTF-8
“who am I”	Google.com	2004-8-25 16:07:32 AEST	http://www.google.com/search?hl=en&ie=UTF-8&q=who+am+i

Table 2. Keywords searched on the web browser.

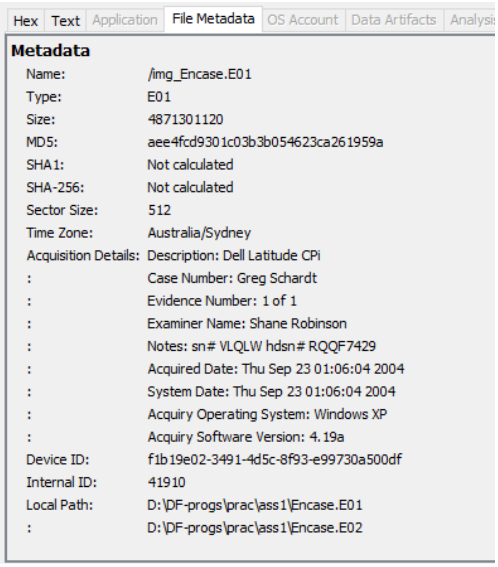
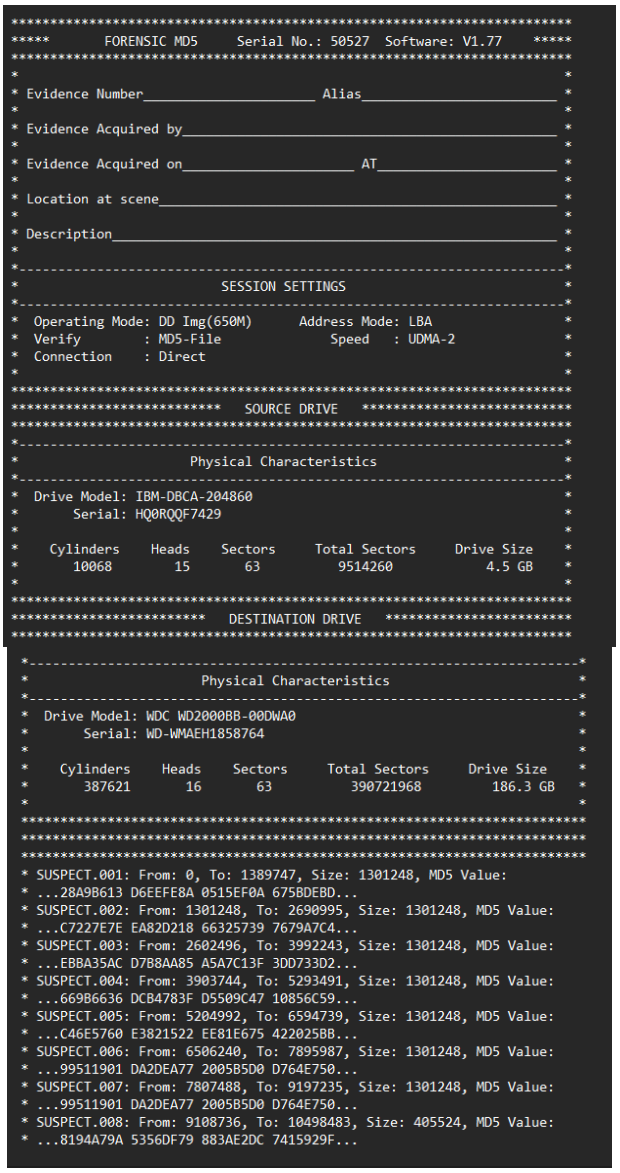


Figure. 1. File Metadata of suspect’s drive on Autopsy.



```
*********************************************************************
*****       FORENSIC MD5     Serial No.: 50527  Software: V1.77    *****
*********************************************************************
*                                                                   *
* Evidence Number_____________________ Alias_____________________   *
*                                                                   *
* Evidence Acquired by_____________________________________________ *
*                                                                   *
* Evidence Acquired on_____________________ AT_____________________ *
*                                                                   *
* Location at scene________________________________________________ *
*                                                                   *
* Description______________________________________________________ *
*                                                                   *
*-------------------------------------------------------------------*
*                         SESSION SETTINGS                          *
*-------------------------------------------------------------------*
*  Operating Mode: DD Img(650M)      Address Mode: LBA              *
*  Verify        : MD5-File             Speed    : UDMA-2          *
*  Connection    : Direct                                          *
*                                                                   *
*********************************************************************
*************************   SOURCE DRIVE   **************************
*********************************************************************
*-------------------------------------------------------------------*
*                     Physical Characteristics                      *
*-------------------------------------------------------------------*
*  Drive Model: IBM-DBCA-204860                                     *
*       Serial: HQ0RQQF7429                                         *
*                                                                   *
*    Cylinders    Heads    Sectors     Total Sectors     Drive Size  *
*       10068        15       63          9514260           4.5 GB  *
*                                                                   *
*********************************************************************
************************   DESTINATION DRIVE   **********************
*********************************************************************
*-------------------------------------------------------------------*
*                     Physical Characteristics                      *
*-------------------------------------------------------------------*
*  Drive Model: WDC WD2000BB-00DWA0                                 *
*       Serial: WD-WMAEH1858764                                     *
*                                                                   *
*    Cylinders    Heads    Sectors     Total Sectors     Drive Size  *
*       387621       16       63          390721968         186.3 GB  *
*                                                                   *
*********************************************************************
*********************************************************************
*********************************************************************
* SUSPECT.001: From: 0, To: 1389747, Size: 1301248, MD5 Value:
* ...28A9B613 D6EEFE8A 0515EF0A 675BDEBD...
* SUSPECT.002: From: 1301248, To: 2690995, Size: 1301248, MD5 Value:
* ...C7227E7E EA82D218 66325739 7679A7C4...
* SUSPECT.003: From: 2602496, To: 3992243, Size: 1301248, MD5 Value:
* ...EBBA35AC D7B8AA85 A5A7C13F 3DD733D2...
* SUSPECT.004: From: 3903744, To: 5293491, Size: 1301248, MD5 Value:
* ...669B6636 DCB4783F D5509C47 10856C59...
* SUSPECT.005: From: 5204992, To: 6594739, Size: 1301248, MD5 Value:
* ...C46E5760 E3821522 EE81E675 422025BB...
* SUSPECT.006: From: 6506240, To: 7895987, Size: 1301248, MD5 Value:
* ...99511901 DA2DEA77 2005B5D0 D764E750...
* SUSPECT.007: From: 7807488, To: 9197235, Size: 1301248, MD5 Value:
* ...99511901 DA2DEA77 2005B5D0 D764E750...
* SUSPECT.008: From: 9108736, To: 10498483, Size: 405524, MD5 Value:
* ...8194A79A 5356DF79 883AE2DC 7415929F...
```

Figure. 2. Suspect log text file that was included with the dd images.

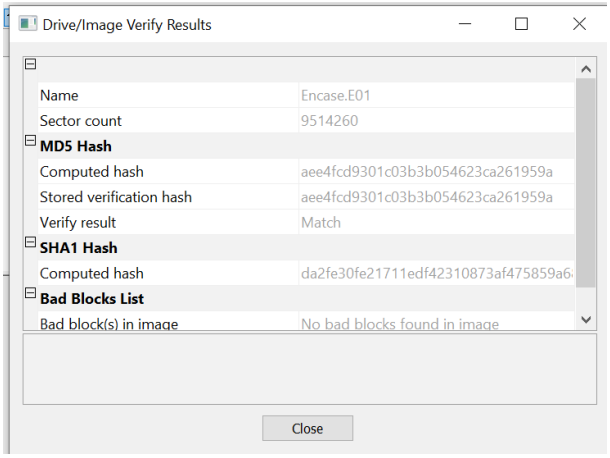


Figure. 3. Image verification results from AccessData FTK Imager.

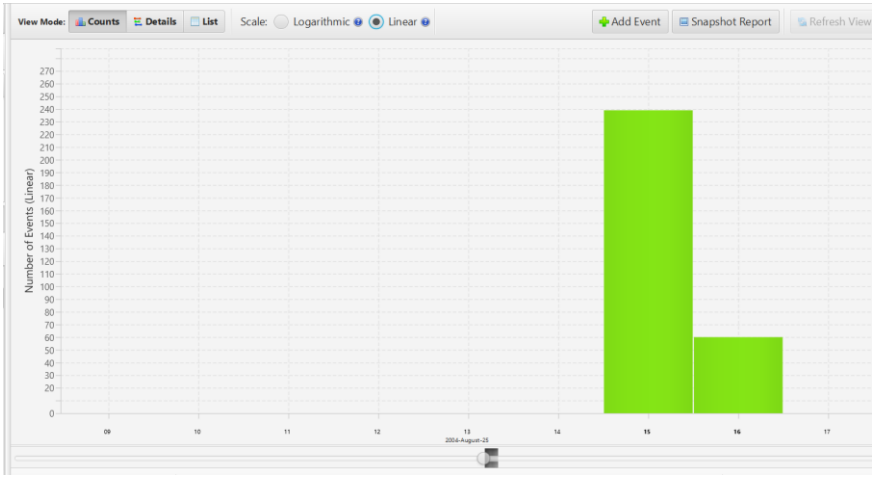


Figure. 4. Graphical results of web activity between the specified time from the timeline tool.

Date/Time	Event Type	Description	Tagged	Hash ...
2004-08 ... :22:49	Web History Accessed	http://shell.windows.com/publishwizard/usa.xml		
2004-08 ... :25:04	Web History Accessed	My Computer		
2004-08 ... :25:04	Web History Accessed	file/Program%20Files/mIRC/channels/channels.txt		
2004-08 ... :25:04	Web History Accessed	file/Program%20Files/Anonymizer/thanks/index.html		
2004-08 ... :25:04	Web History Accessed	http://search.msn.com/results.aspx?FORM=MSNH&q=download%20rencode%20buddy		
2004-08 ... :25:04	Web History Accessed	http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome		
2004-08 ... :25:04	Web History Accessed	http://www.cnn.com/cnn_adspaces/adsPopup2.html?0		
2004-08 ... :25:04	Web History Accessed	www.elitehackers.com		
2004-08 ... :25:04	Web History Accessed	www.cnn.com		
2004-08 ... :25:04	Web History Accessed	www.cleo-and-nacho.com		
2004-08 ... :25:04	Web History Accessed	http://ads1.revenue.net/load/206178/benchmark. ... _RANK=1&O_CREATIVE_ID=206178&O_SITE_ID=10162&		
2004-08 ... :25:04	Web History Accessed	file/Drivers/Anonyymizer/keys.txt		
2004-08 ... :25:04	Web History Accessed	http://search.msn.com/results.aspx?FORM=MSNH&q=hacking		
2004-08 ... :25:04	Web History Accessed	http://www.2600.org/hacked_pages		
2004-08 ... :25:04	Web History Accessed	edit.yahoo.com		
2004-08 ... :25:04	Web History Accessed	http://www.magnescan.com/pricelist.asp		
2004-08 ... :25:04	Web History Accessed	billing.mail.yahoo.com		

Figure. 5. List results of web history from the timeline tool, that does not include the program name.

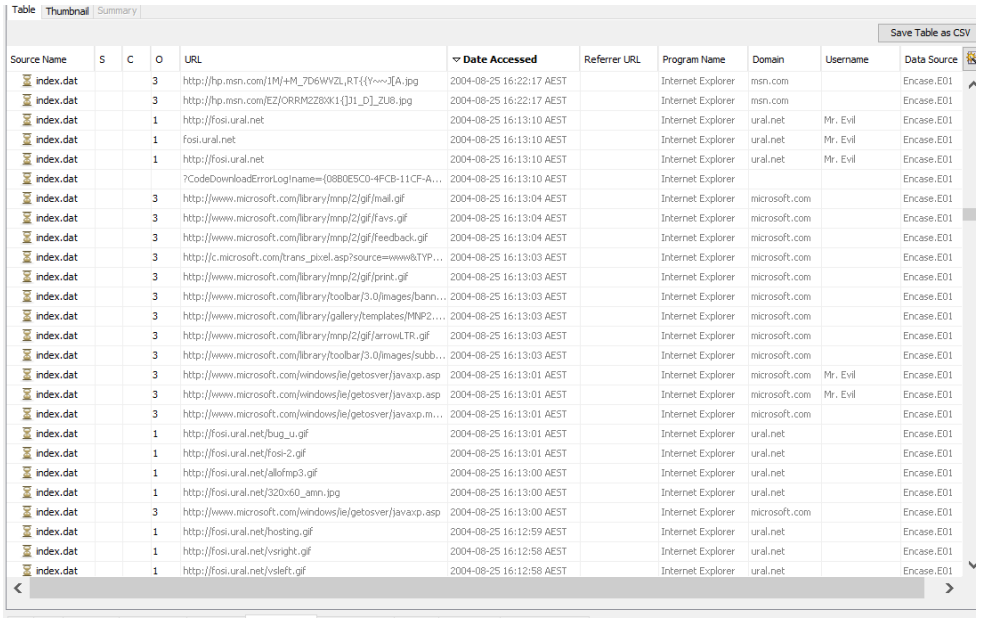


Figure. 6. Listed results from the web history showing the browser used.

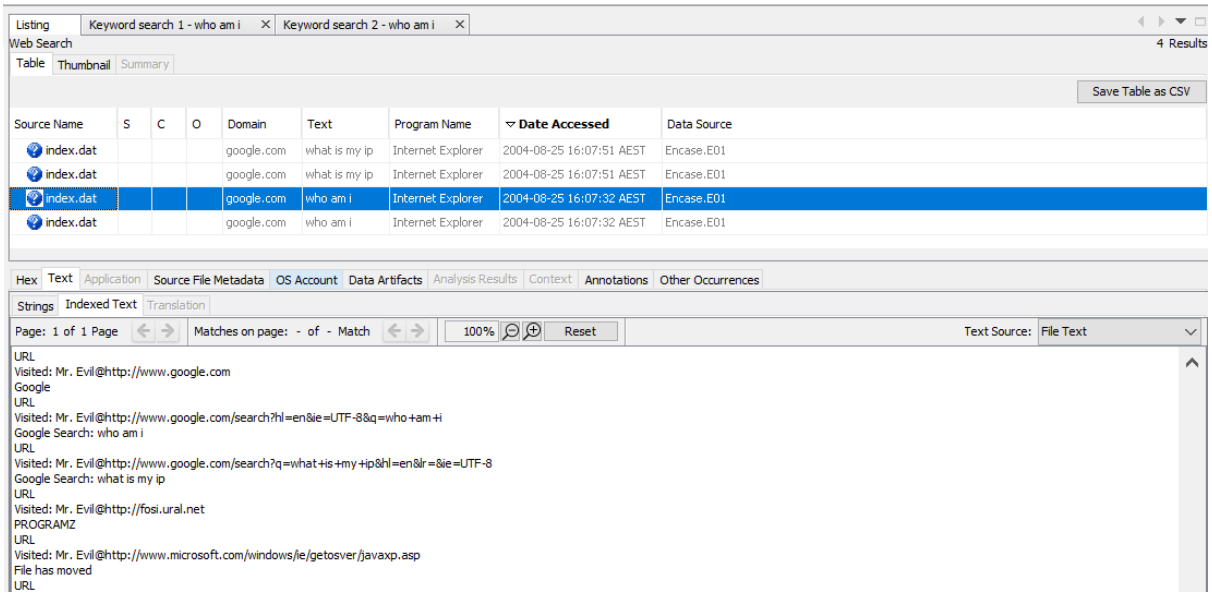


Figure.7. Web searched keyword results and indexed text.

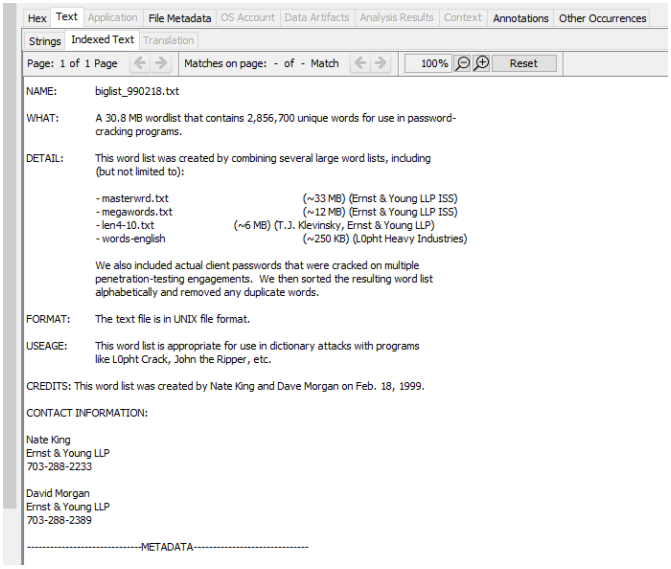


Figure. 8. Contents of readme.txt in biglist_990218.zip.

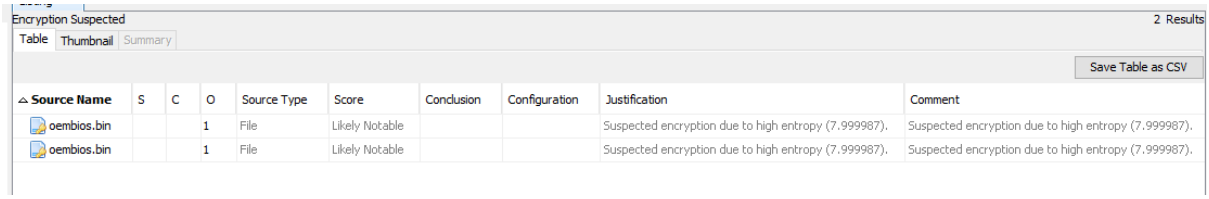


Figure. 9. Files suspected of encryption.

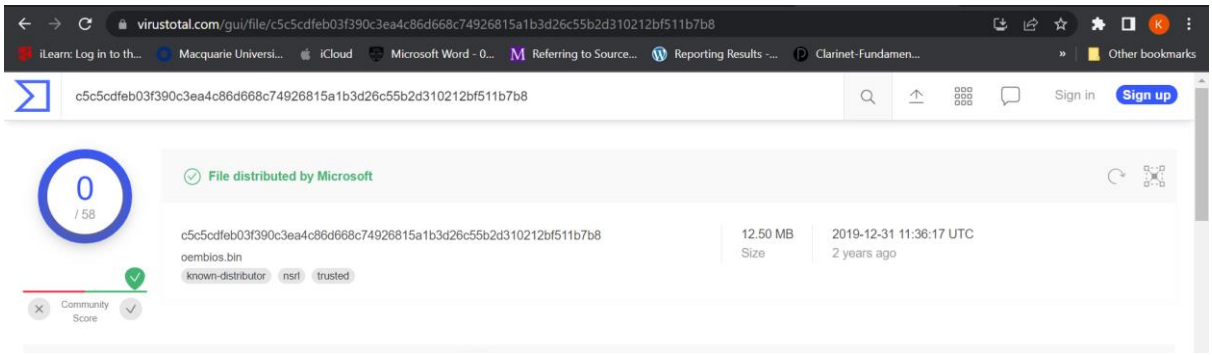


Figure. 10. VirusTotal.com results for SHA-256 hash of oembios.bin.

References

[1] Autopsy 4.19.3 (2022), Basis Technology.

[2] FTK Imager 4.5.0.3 (2022), AccessData.

[3] Excel (2016), Microsoft.

[4] K. Satvat, M. Forshaw, F. Hao, and E. Toreini, “On the privacy of private browsing – A forensic approach,” *Journal of Information Security and Applications*, vol. 19, no. 1, pp. 88–100, Feb. 2014, doi: 10.1016/j.jisa.2014.02.002.

[5] “Cracking Dictionaries,” *Enzoic*, Mar. 30, 2020. https://www.enzoic.com/password-cracking-dictionaries/ (accessed Apr. 08, 2022).

[6] “SuperScan,” *Softonic*. https://superscan.en.softonic.com/ (accessed Apr. 08, 2022).

[7] L. Robert and J. Hamrock, “Using Entropy Analysis to Find Encrypted and Packed Malware,” *IEE Security & Privacy*, pp. 40–45, 2007.