Intro to Cyber Forensics Lab Grading Sheet

Project: Lab 3 – Computer Forensic Tools
Member Name: Alejandro Marin Arellano
Member Name: Christopher Bowen
Member Name: Terrence Scott
Member Name: Saehwan Park
Member Name: George Hendrick
Executive Summary / 4 points
+ v -
□□□ Executive summary is brief and focused to the point of the project □□□□ The
summary clearly illustrates the objectives of the laboratory exercise
Apparatus / 4 points
☐☐☐☐☐ The apparatus are clearly illustrated and documented
Procedures/ 12 points
□□□ Adequate information provided to allow re-creation of work
□□□ Consistent level of coverage throughout the project – nothing overly detailed or omitted
Problem Solving/ 5 points
□□□ All problems identified
□ □ □ Alternative solutions identified
□ □ □ Solutions attempted listed
□ □ □ Final solution detailed (what fixed the problem and why?)
Conclusions & Recommendations / 5 points
□ □ □ Tie back to the learning objectives identified in the executive summary - <u>critical</u>
Conclusions stated in a logical fashion
□ □ □ Conclusions are viable based on the procedures and results
□ □ □ Recommendations practical & relevant
Format & Grammar / 5 points
□ □ □ Table of Contents present
□ □ □ Report written in past tense
□ □ □ Proper voice (no I's, We's, Our's or The group)
□□□ Paper easy to read (fonts, spacing, etc.)
□□□ Proper credit given to sources in bibliography (APA style)
Paper is cohesive and consistent in tone
Spelling & grammar errors: minus one half point for each, up to a max deduction of 5 points – at that time
paper is returned for correction and re-submission with a one letter grade penalty.
Final Score: /35

Contents

1	Exe	cutive Summary	:
2	App	paratus	4
3	Lab	oratory Procedures	Ę
	3.1	Time-line / Log	Ę
	3.2	Procedure	ϵ
	3.3	Files of Interest	6
	3.4	Password Cracking	6
		3.4.1 Windows Passwords Cracking	6
		3.4.2 Zip Brute Force	7
	3.5	Programs of Interest	7
		3.5.1 Suspect Outlook Activity	7
		3.5.2 7zip Activity	7
		3.5.3 Discord	8
		3.5.4 Dropbox	8
	3.6	Figures	10
4	Pro	blem Solving and Troubleshooting	15
5	Cor	aclusion and Recommendations	16
6	Ref	erences	17
\mathbf{A}	ppen	${f dices}$	17

1 Executive Summary

The objective of this lab was to sift through the digital evidence acquired from AI Lagniappe's hard drive recovered at the scene of a suspected digital intellectual property theft. Investigators acquired an image file of the VM used by AI Lagniappe in the acquisition process of the investigation.

The goal of this exercise was for investigators to become familiar using different digital forensic tools such as Autopsy and finding new evidence in the files.

Investigators began by opening the image file into Autopsy and indexing the file system. After indexing, the file system was searched to find any digital evidence regarding the intellectual property theft. Discord logs, several emails and cache data, and zip files were found containing potential evidence. Moreover, other forensic tools were used to analyze the evidence found.

In this lab, investigators gained knowledge by using several computer forensic tools to analyze a forensic image. To ensure proper standards investigators documented every action taken when accomplishing these tasks by taking screenshots of files found and processes ran by using forensic tools.

2 Apparatus

Table 1 lists the hardware and software used in this lab.

Table 1: apparatus of tools used in the image capture process

ITEM/PART	MODEL NUMBER	VERSION	USAGE
Windows 10 Pro VM	N/A	N/A	Forensic image
Kali Linux VM	N/A	4.16.5	Forensic image
Autopsy	N/A	4.20.0	Forensic image analysis
John the Ripper Tool Kit	N/A	1.9.0	Password Cracker
Chrome Cache Viewer	N/A	2.41	Cache Viewer
Disfor	N/A	1.0.11	Discord artifact parser
DB Browser	N/A	3.12.2	SQL Browser

3 Laboratory Procedures

3.1 Time-line / Log

Table 2: The log of all actions taken in the investigation

#	DATE	TIME (24hr)	ACTION TAKEN / INVESTIGATIVE LEAD
1.	02/27/2023	15:30	Loaded ailagniappe.E01 image file into Autopsy, waited for
			entire image file to be indexed
2.	02/27/2023	19:15	Searched for downloads in Discord files, found Discord
			cache files
3.	02/27/2023	19:20	Searched for downloads in Outlook files
4.	02/27/2023	19:23	Found the email addresses lagniappeai@gmail.com and
			sleazysteve@gmail.com, found Windows.edb file
5.	02/27/2023	19:28	Searched for downloads in Dropbox files, found add
			event for not_illegal.zip and delete event for incredi-
			bly_important_drug_nn.h5
6.	02/27/2023	19:31	Searched for downloads in 7zip files, found not_illegal.zip
			file, exported not_illegal.zip file
7.	02/27/2023	19:33	Opened not_illegal.zip using 7zip, found incredi-
			bly_important_drug_nn.h5 file to be password protected
8.	02/27/2023	19:35	Searched through rest of data artifacts, nothing found
9.	02/27/2023	19:56	Attempted to brute force the password to open incredi-
			bly_important_drug_nn.h5 using John the Ripper tool
			kit, was not successful
10.	02/27/2023	20:10	Disfor used to look at Discord cache files
11.	02/27/2023	20:15	chromecacheviewer used to look at Dropbox cache files

3.2 Procedure

Investigators began by acquiring the ailagniappe.E01 image file with the MD5 hash 358709d4dee3b8979a1f352900f7951e and decided to use Autopsy to analyze the image file. The image file was loaded into Autopsy and the modules Android Analyzer, Android Analyzer (aLEAPP), Central Repository, DJI, Drone Analyzer, Data Source Integrity, Email Parser, Embedded File Extractor, Encryption Detection, Extension Mismatch Detector, File Type Identification, GPX Parser, Hash Lookup, Interesting Files Identifier, Keyword Search, PhotoRec Carver, Picture Analyzer, Recent Activity, Virtual Machine Extractor, YARA Analyzer, and iOS Analyzer (iLEAPP) were run on the file to find artifacts. A list of software used in the investigation can be found in Figure 1, and a list of found data artifacts can be found in Figure 2.

3.3 Files of Interest

Investigators found several files of interest, the files are as follows: not illegal.zip -

- A zip file containing a file named "incredibly_important_drug_nn.h5", which investigators suspect to be the drug discovery technology stolen from Super Rick by the suspect.
- The file was found to be encrypted and password protected.
- The file was zip and encrypted using the 7zip application downloaded.
- The file was found on the Desktop and in the suspect user's Dropbox file.
- The file is suspected to be sent out via email to sleazysteve@gmail.com and extracted using Dropbox.
- The file is in the h5 file format which is commonly used as data files in the medical field.

old password.txt -

- The file was deleted, but the suspect did have this file and it was accessed via Notepad.
- Investigators were unable to recover this file.

dropbox illegal data password.txt -

- The file was deleted, but the suspect had this file on their Desktop and it was accessed via Notepad
- Investigators suspect, as the name suggests, this password was used to encrypt the not illegal.zip file.
- Investigators were unable to recover this file

3.4 Password Cracking

3.4.1 Windows Passwords Cracking

After Investigators found the encrypted zip file not_illegal.zip, investigators believed that the windows account ailagniappe may have the used same password. To obtain the password of ailagniappe, investigators extracted both the SAM file and SYSTEM file in /img_ailagniappe.E01/vol_vol6/Windows/System32/config/.

With these files, Investigators used the samdump2 tool kit on kali linux to retrieve the following hash information: \$LM\$aad3b435b51404ee:(Figure 7). Investigators then ran the hash through john the ripper, and the result for the hash was "". Investigators then determined that this password was not the same as the one used to encrypt the zip file.

3.4.2 Zip Brute Force

After investigators detected that the not_illegal.zip was encrypted (using the 7zip application), investigators decided that starting to brute force the password may be a viable way to gain access to the contents of the folder. Investigators researched ways to properly run cracking tools on the zip file and decided that the John the Ripper tool kit was the best available way to conduct password cracking. Investigators ran the not_illegal.zip through zip2john to produce the hash format that was needed for John the Ripper. Next, Investigators ran the hash against the rockyou password last. After 4 minutes and 25 seconds, every password was tested from the list and found unsuccessful. Investigators decided to try a brute force attack using alphanumeric and special characters. The results were unsuccessful after 20 hours (Figure 6). add maybe hashcat

3.5 Programs of Interest

Investigators started by finding all programs of interest downloaded on the virtual machine, as well as programs accessed by the suspect. It became clear to the investigators that the suspect searched for the downloads to Discord, Outlook, Dropbox, and 7Zip in that order, and the suspect downloaded Discord, Dropbox, and 7Zip in that order. A list of web searches can be found in Figure 3, and a list of the suspect's downloads can be found in Figure 4. The suspect also ran multiple other programs. Certain programs of interest, found in the Run Programs section of the generated Data Artifacts, include those such as Microsoft Edge, OneDrive, 7zip, and Notepad.

3.5.1 Suspect Outlook Activity

The suspect was found to have used the email address "lagniappeai@gmail.com" on Outlook and investigators found it very likely that he was in contact with another email address that goes by "sleazysteve@gmail.com". Investigators also found the suspect most likely sent this individual a copy of not_illegal.zip, which investigators are led to believe contains protected intellectual property. Investigators uncovered this by finding a Windows.edb file. Investigators were unable to mount a Microsoft Access Server to accurately view the contents of the edb file, but the text view, shown in Figure 5, indicated not_illegal.zip was likely sent. Investigators plan on renting a Microsoft access server to access the mailbox of lagniappeai.

3.5.2 7zip Activity

Investigators found that 7zip ran by AILagniappe at 11:54 CST 2023-02-22 seen in figure 8. Investigators could not confirm if the file that was zipped with 7zip was not_illegal.zip, however, it is very likely that the suspect used 7zip to encrypt the not_illegal.zip with a password.

3.5.3 Discord

1. Discord Cache Parser

Investigators focused on recovering discord log files from the discord application to give more context of the crime that occurred, After researching the artifacts that discord left behind, investigators learned that discord cache files are stored in chrome cache format(1,2). Investigators first used chromecacheviewer(3) to pull the parse the contents from /img_ailagniappe.E01/vol_vol6/Users/AILAGNIAPPE/AppData/Roaming/discord/Cache/. Partial results are shown in figure 10. After the results were parsed, Investigators manually looked through these files for chat logs and other valuable information. Investigators were not able to find anything pertaining to the investigation, so investigators decided to use another forensic tool to verify if there was not any missing information. Investigators used Disfor, a tool for parsing discord-specific cache files, to parse the contents of the cache folder. After using DisFor the same results occurred with not valuable information found. (Figure 10).

Discord cache folder location:

/img_ailagniappe.E01/vol_vol6/Users/AILAGNIAPPE/AppData/Roaming/discord/Cache/

Resources:

- 1. https://content.govdelivery.com/accounts/USDODDC3/bulletins/2e036a8
- $2. \ https://researchonline.ljmu.ac.uk/id/eprint/14832/3/Discord\%20Server\%20Forensics\%20Analysis\%20and\%20Extraction\%20of\%20Digital\%20Evidence.pdf$
- $2.1\ https://github.com/MichalMotylinski/DiscFor-Discord-Artefact-Extraction-Tool\\ 3.https://www.nirsoft.net/utils/chrome_cache_view.html$

3.5.4 Dropbox

1.DropBox Cache Parser

Next Investigators focused on recovering local cache files stored from DropBox. Dropbox stores it local cache files in /img_ailagniappe.E01/vol_vol6/Users/AILAGNIAPPE/AppData/Roaming/DropboxElectron/Partitions/.(Figure 11) Examiners then precede to extract both /Partitions/1dc15115-1ba7-40b5 -a2b6-e830a49e9bcb/Cache/ and /Partitions/d1fad9a0-edf3-4265-af71 -f565edd18291/Cache/ to look for evidence. The steps taken followed the same steps in the Discord Cache Parser subsection with chromecacheviewer. No valuable evidence was found in these files. Resources:

1. https://www.researchgate.net/publication/342991973_Forensic Analysis of Dropbox Data Remnants on Windows 10

2. DropBox Databases

Next Investigators focused on artifacts found in the local files for dropbox. The folder path follows: /img_ailagniappe.E01/vol_vol6/Users/AILAGNIAPPE/AppData/Local/Dropbox/ format. In ../ instance1 /sync_history.db investigators found important actions taken by AI Lagniappe. The file incredibly_important _drug_h5 was deleted and the file not_illegal.zip was uploaded as seen in figure 11. The next set of artifacts found by Investigators was in /QuitReports/da0f8efe-2419-4148-97a2-60bdccba1362.dbt. The file was encrypted in base64 and after decryption valuable information such as host_id: 14435301457 and machine id: b1d05304-75db-4c31-8f95-2c9ca3f175cf was found (Figure 11). Other database files were found

in the folder, however, Investigators determined that they were encrypted due to the .dbx extension. These files can be decrypted; however, Investigators did not have time to do so.

3.6 Figures

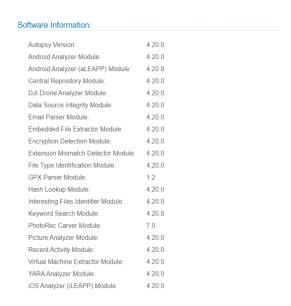


Figure 1: List of software used during the analysis

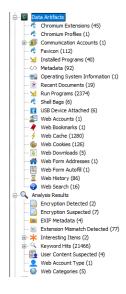


Figure 2: List of found data artifacts on suspect's VM

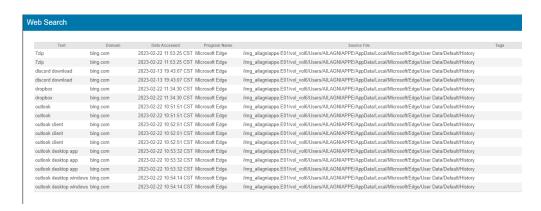


Figure 3: List of web searches done by the suspect



Figure 4: List of suspect's downloads

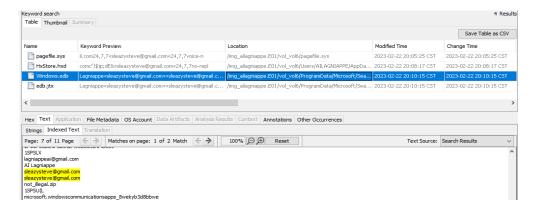


Figure 5: Found Windows.edb file and potential transfer of not illegal.zip

```
s john --wordlist=/usr/share/wordlists/rockyou.txt brute.hash
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 AVX 4x])
Cost 1 (HMAC size) is 9060738 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Og 0:00:00:05 1.63% (ETA: 23:50:14) Og/s 53426p/s 53426c/s 53426C/s jedidah..dukefan
Og 0:00:04:25 DONE (2023-02-28 23:49) Og/s 54088p/s 54088c/s 54088C/s !SkicA!..*7¡Vamos!
Session completed.
```

Figure 6: Attempt to access not_illegal.zip by running the hash against the rockyou word list using John-TheRipper

Figure 7: Attempt to bruteforce not illegal.zip using JohnTheRipper

TZZOLHVA EJE	2023-42-22 (1:53:38 CST (Prefetch File	JUSERSIALAGNIAPPEID
TONIESE	2023-02-22 11:54:12 CST 1	Prefetch File	PROGRAM FILES/7-ZIP
TOEPE	2023-02-22 (1:55-45 CST 1	Prefetch File	PROGRAM FILES/7-ZIP

Figure 8: 7zip Running

```
AT Leonteppe
sheary steve @gmail.com
sleary steve
microsoft.windowscommunicationsapps_8wekyb3d8bbwe
15PS
15PS
15PS
15PS
15PS
15PSI
1
```

Figure 9: windows.edb file

Filenana	UNL	Content Type	Tibe Stee	Last Accessed	Server Time	Server Last Medidad	System	Second	Keepens	Name France	Contest Enredias	Cache Name	Cache Control	ETeg	Address
broatine, materials jum.	https://dianordapp.com/api/18/auth/invation.materiate	application jum.	0.2	3 33 3033 Robits Phil	2-22-2023 6-04-21 804		$\overline{}$	eleui@are	HITTE LA 200			Intera_3 (42792)			142 149 134 23
0900071c785141458787415450c27857 pag	https://discordage.com/assats/000h073c78d3c4af4f78741f4f0c278f7.pog	image yest		3-93-9003 6-06-14 764	2-22-2023 10-11-19-434	8-31-2021 9-13-29 904		ciondifiara	DETTRACTION		_	data_2 [14913]	pohio, manager 2702000	-09060710185143416767431410007617-	160-169-130-23
Sanosaucon sour Sourceassauch The woods	https://docordage.com/accets/047608a100180a100a100a180a181a57775.com80	See worth	24,440	3-32-3031 B-06-11 PM	3-33-3431-10-11-19-434	1-37-3633 E-RO-40 PA4		elemithers.	HTTP-1-1-200				public, man agent (00000)	Charles and the Colonial Assessment Colonial Col	142-149-130-23
4131999413454035546993690019964.wod92	https://docordiage.com/souts/w114986w1745w1175469036900198ba.nod0	foothedt)	26,336	3/23/2023 6:06:15 954		3/27/2023 5:50:40 954							public, near-age+2592000	*#11998##13#5#c155####D689#c198###*	162,159,130,23
20Td4eas120w7das2b0b02bude291as6wod02	https://discordage.com/accets/269d4mas120e7das260603bcde991aeEccet92	feet well?	20,030	2/22/2023 9/06/15 954		1/27/2023 3:30:40 954		shoulthere	MTTP-1.1 200				public, man-age-2392000	"39964eaa130e7daa2505025ude991aeE"	102.139.130.23
5590393.avm	Miles indicated approximate in written stable access,2290292	application/pon		2/22/2023 9/06/14 95/2	2/22/2023 9:09:14 95:0	2/22/2023 4:20:34 954		cloudflare	METTER 1.1 200			data_1 1424941	no-cashe	100797083399V029W003xTW94V88339V687	102.139.134.23
ar467500079x772xd6433.js.	https://discordage.com/assets/ant/Ch/9099v772vdb432.js	application (account)	20,028	3/33/2023 B/06/14 PSE	2/22/2023 B-06/34 POJ	2/22/2023 1:10:33 PM	$\overline{}$		HTTP 1.1 200				public, man-age=2392000	300-8001309AB4669A76634699A0544893BEET	102.139.134.23
404ma7mfa74ma08a1a72.ju	herps delinered approximates with traditional fields 272 (a	application/prosenter		3/33/3003 K-06-14 Ph.E	3/33/3033 #-04/34 POJ						No.	data_2 [2416640]	public, man.ager3192000	757168a438636ra619043a3a4a7rra0506601	142.149.134.23
PAGENDALISMATHORI (A	https://doctor/app.com/assets/1642099611399679G41.js	application prosented	7,406	3-33-3033 R-06-14 PM	3:33 3033 8:04 34 804	2-31-3033 8-33-13 934			HTTP-1-1-200			data_3 (2400234)	public, manager 2192000	No. of Principles Laboratory and Control of	142 110 114 21
SACSOT RESOURCE STRANGE	https://discordage.com/seasts/16/10/1606/fide6/had-ja		4,400	3-33-3033 6-06-14 764		3/12/2003 7:11/10 904		ciondifiera	PETTER & \$ 240				public, man-age-3103000	Withdress Talant Land Dorder and Saleston	140-140-130-23
800494798880945941293s	Mayor indiscondings, constraints 1000 tast 7945400947 art 25 July	application promotes and		2/22/2023 6:06:15 954		2/16/2023 19:22:31 994		Cloudflare					public, near-age+2592000	W118626682416984842228972485406851	162,159,130,23
39753w77wc3546645453.ju	https://discordings.com/assets/20753s/77ac2546083453.js		22,559	3/23/2023 6:06:15 754	2:22:2025 6:06:15 894	3/23/2025 2:15:16 954		Cloudflare	PETTER 1 2 200				public, near-age=2592000	W11 566424846666436364546466616621	162 159 134 23
\$154es4esash7707g777.js	Many Chicago dago, conclusado 915 feedenado 7070 77 de	application because of		2/22/2022 9/09/12 954	2/22/2022 8:09:12 92:0	2/21/2022 0:22:49 934			METTER 1.1 200			data_2 (92224)	politic, man-saw-2292000		102,129,124,22
##292207#4122#1389193s	heters of discountings, complements land \$2200 and \$222 \$1860 Print	medication in account	2,239	2/22/2023 8:00:13 954	2/22/2022 8-06-12 PO.E	2/21/2023 6/23/47 934	-	Talend Care				Mate. 2 1914400	softlin, many age-2392000	2073-0-2220-1-04-0-18a94-90-45-20177471	142,129,124,22
ee1167a428271da89717.is	https://discordings.com/exets/es1167e428371/def8717.in	medication in account		2/22/2023 8:00:13 95.0	2/22/2022 8:08:12 PO.5	2/21/2023 #:23:47 93.6			MTTP-1-1-200			Mate. 2 (2329299)	and tin, many sare-2292000	TOT #7000029254819841240508890192491	102,129,124,22
	hetps://discordapp.com/assats/02001ar801347hash898.js	application presented	434,219	3 32 3023 K-OH 13 PM	2-22-2323 8-04-24 80.6	2 22 2023 4 20 33 904	i –		HTTP-1-1-200	1			public, man agent 190000	W. Total College Colle	142 149 134 23
	https://discordage.com/edu-egi/eluilungs-platform fr/g-scripts-pics-ja	application jacranoige		3-93-9003 6-06-15 764				ciondifiara			1	data_3 [233a120]	man agent \$400, public		160-169-114-21
\$73 Indianonal Carbon \$75 about affects would	https://docordage.com/accets/8711bbfa90bdas0faa0cc873bbf490bda.com80	See worth	21,424	3-32-3031 #-OK-11 PM				elemithers.			_		public, man-age-3103000	* BT 1 Th Earl Challed County and County To A B 4 of Table Co.	142-149-130-23
5659/3 ac Ted ex5 4a24969, worker ja	https://discontings.com/seets/16561ac7a5es54a18669.modes/ja	application (arrange		3/23/2023 6:06:15 954		10/0/2002 2:52:42 954		Cloudflare				data_2 (24574)	public, near-age+2592000	W1784182424ce4f1fee22278c7542a76df	162,159,130,23
690+06223+02x27+x1x8.xx	https://documentago.com/access/090428222400x27ms1x0.as	medication because	200,327	2/22/2022 9:00:12 954	2/22/2022 8:00:00 90:0	2/22/2022 4/20/22 954		Shouttlere	MTTP-1-1-200				and the man-man-2292000	7017-80161445014456241512451549122647	102,129,124,22
estemperocapotario de	Mayor Chicago diago, conscionado efit del debida CECL as PC Jo		476,377	2/22/2022 9/09/12 954	2/22/2022 9:09:09 92:0	2/22/2022 4 20:22 934	-	StoutBare	METTER 1.1 200				graftin, man-age-2292000	9075caD048246994244224990c4a640897	102,129,124,22
	https://discordapp.com/assets/027046/26494aa09a204.js	application/presented		2/22/2023 9/06/12 954	2/22/2023 8:00:00 99.0	2/22/2023 2:13:18 934							public, man-age-2392000	90746841456825124421164874767885061	102.139.134.23
StantiffStorTraTfalija	https://dianordappi.com/assats/03aad169230a77ca7da3.ju	application/prosenter	281,784			2/1/2023 3:48:71 75.6		ricuitiere			No.		public, man.ager3192000	75014201502845465682313576418430010v1	142.149.130.23
	hetys - discordage com assets 9111249770147cs42743.js			3-33-3033 R-06-13 PM	3:33 3033 8:06 64 904	3.31.3033 4.43.38 PM			HTTP-1-1-200				public, manager 2192000	Will SHAD BY BERT STAFFED SELECTION OF THE	142 110 114 21
	https://discordage.com/assats/1/11/cc??f428016a2816.ju	application jacranoige						ciondifiera			-	£50001a	public, man-age-3103000	NO ASSOCIATION STREET,	142 146 114 21
	https://docordiago.com/souts/9x22/2041#044024525480.jp	application promotes and										data_1 (22529)	public, near-age+2592000	W17284764792515498986440231111446617	162,159,130,23
1222990645aac65443aja	https://docordiago.com/assets/12279s/fe6sec668447a.js		160	3/23/2023 6:06/12 854		1/27/2025 6:01:26 954		Cloudflare	PETTER \$ 2 200			data_1 (22764)	public, near-age=2592000	W110he068425ebebles486889111eb801	160 159 130 23
x739504x00x4404x2399.xx	Mayor Chinacon dayan complements in 7299-0 da00m04-0-bit 2398 un	application because of	100	2/22/2022 9/09/12 954		1/27/2022 6:01:26 954			METTER 1.1 200				politica, many name 229/2000	900-8092422228699-042494164220224869-0	102,129,120,22
1229542e28eba26boe21.is	https://discordiage.com/assets/1/29947e2Befsa28fsa491.is	medication in accorde	8,447	2/22/2023 8:06:12 95.6	2/22/2022 8-06-06 PO.5	2/21/2023 2/23:12 934	-	steed@are				Mate. 2 (1892)222	softlin, many sare-2392000	2012 P.00 2 (Page Decay Ov. 2 a 7.7 v (Page 2 8 1 hold 8 1	142,129,124,22
90a6890490906a443371.is	Marin Officer of Sept. complements 90 a 600 ft a 600 ft a 77 ft in	medication in account	7,500	2/22/2023 8:06:12 95.6	2/22/2022 8-08-08 99-0	2/21/2023 #:23:47 93.6						Mate. 2 (1997779)	and tin, many sare-2292000	2011207+4-666/15-696772468(106+668)	102,129,124,22
Bloth Control State Co.	https://discordant.com/assatu/filed/M2cc/M89887787b is	and instructor accorded	6,339					Friend Oars			l be	Totals 2 (3811292)	softlin, manuages2192000	Y07486289442336794890375994384445097	142,159,134,23
	https://discordapp.com/assets/affadiQ1e47afab273afi.js	application because of		3/33/3023 R-06/13 PM	3/23/2023 B-04/04 POJ	3/23/2023 2:13:18 994	$\overline{}$		HTTP 1 1 200			data_2 (1837008)	public, manuager/2192000	WOTTHER Destroy State (see Sept. 1847) 1104	142 139 134 23
3114991819946791309434	hetps://discordapp.com/assats/217a0018100db701200a.ju	application proserves	1,140	3-32-3033 #-OH-13-PH-E				- indiffere				data_2 (1818424)	public, man agent 1000000	Windshallood as house and assessment than the	142 149 134 23
	https://discordage.com/assets/c819977a54f9c5404997.ja	application promotings		2-22-2023 6:06:12 854	2-22-2023 6:06:06 594	2/21/2023 6/25/47 954		Condition			W	data_3 [1602240]	public, man-age=2592000	W-166642021241644614852784493497	160,159,134,23

Figure 10: Parsed Discord cache data

event_type	ne file_even direction file_id		fle_id	local_path	server_path	other_user	timestamp
file	delete	upload	TxJc5aHn7foAAAAAAAAABg	C:\Users\AILAGNIAPPE\Dropbox\incredibly_important_drug_nn.h5		0	1677088448
file	add	upload	Tx3c5aHn7foAAAAAAAAAACA	C:\Users\AILAGNIAPPE\Dropbox\not_illegal.zip	3522666033:/not_illegal.zip	0	1677089082

Figure 11: Sync_history.db of dropbox

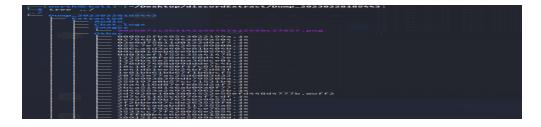


Figure 12: List of suspect's downloads



Figure 13: Base64 decryption of QuitReports

4 Problem Solving and Troubleshooting

Problem: The not_illegal.zip file containing the "incredibly_important_drug_nn.h5" was password protected.

Solution 1: Attempt using previously found passwords during the investigation process.

Solution 2: Attempt using suspicious strings found in the analysis process.

Final Solution: Brute forced the password.

Problem: The file "old" password.txt" was deleted by the suspect.

Solution 1: Investigators were incapable of recovering the file; no solution was found.

Final Solution: No solution was found.

Problem: The file "dropbox illegal data password.txt" was deleted by the suspect.

Solution 1: Investigators were incapable of recovering the file; no solution was found.

Final Solution: No solution was found.

Problem: Unable to find the discord logs and get messages sent and received by suspect.

Solution 1: Investigators were incapable of recovering messages; no solution was found.

Final Solution: No solution was found.

Problem: Unable to find the email logs and get messages sent and received by suspect.

Solution 1: Investigators were incapable of recovering messages; no solution was found.

Final Solution: No solution was found.

5 Conclusion and Recommendations

Investigators found it very likely that the suspect AI Lagniappe stole protected intellectual property from Super Rick. The suspect used 7Zip to encrypt the stolen data, and locked it behind a password, which investigators were not able to recover. It is possible that the file was distributed via discord and is very likely the file was distributed via Outlook and Dropbox.

In this exercise, investigators have learned a method of using forensic analysis tools to analyze evidence taken from a crime scene. After the acquisition and authentication of the evidence, the analysis process is the most important for finding usable evidence. Proper documentation of all tools and how they are used is still imperative to make sure any new evidence found can be used in court. The forensic procedure must be followed regardless of the amount of tools used in an investigation.

Investigators must make sure they are thorough when analyzing evidence as important information could be easy to miss. The large variety of forensic tools that are available facilitate that process and becoming familiar with them early on can benefit investigators to perform evidence analysis faster and more efficiently in the future. 6 References

References

Appendices