

# 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

+ ✓ -

☐ ☐ ☐ 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 - critical

☐ ☐ ☐ \_\_\_\_\_ 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

<b>1</b>	<b>Executive Summary . . . . .</b>	<b>3</b>
<b>2</b>	<b>Apparatus . . . . .</b>	<b>4</b>
<b>3</b>	<b>Laboratory Procedures . . . . .</b>	<b>5</b>
3.1	Time-line / Log . . . . .	5
3.2	Procedure . . . . .	6
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
<b>4</b>	<b>Problem Solving and Troubleshooting . . . . .</b>	<b>15</b>
<b>5</b>	<b>Conclusion and Recommendations . . . . .</b>	<b>16</b>
<b>6</b>	<b>References . . . . .</b>	<b>17</b>
	<b>Appendices . . . . .</b>	<b>17</b>

# 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 lagniappei@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 incredibly_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 incredibly_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 incredibly_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\_nm.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 list. 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-Artifact-Extraction-Tool>
3. [https://www.nirsoft.net/utils/chrome\\_cache\\_view.html](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](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

Software Information:	
Autopsy Version:	4.20.0
Android Analyzer Module:	4.20.0
Android Analyzer (aLEAPP) Module:	4.20.0
Central Repository Module:	4.20.0
DJI Drone Analyzer Module:	4.20.0
Data Source Integrity Module:	4.20.0
Email Parser Module:	4.20.0
Embedded File Extractor Module:	4.20.0
Encryption Detection Module:	4.20.0
Extension Mismatch Detector Module:	4.20.0
File Type Identification Module:	4.20.0
GPX Parser Module:	1.2
Hash Lookup Module:	4.20.0
Interesting Files Identifier Module:	4.20.0
Keyword Search Module:	4.20.0
PhotoRec Carver Module:	7.0
Picture Analyzer Module:	4.20.0
Recent Activity Module:	4.20.0
Virtual Machine Extractor Module:	4.20.0
YARA Analyzer Module:	4.20.0
iOS Analyzer (iLEAPP) Module:	4.20.0

Figure 1: List of software used during the analysis

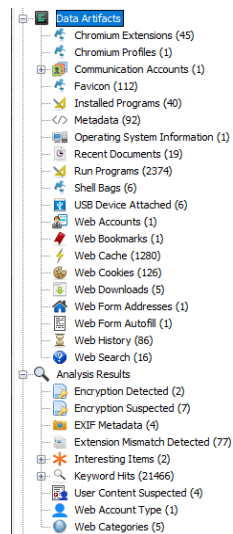


Figure 2: List of found data artifacts on suspect's VM

Web Search						
Text	Domain	Date Accessed	Program Name	Source File	Tags	
Zip	bing.com	2023-02-22 11:53:25 CST	Microsoft Edge	/img_allagniappe.E01vol_vo6/Users/AILAGNIAPPE/AppData/Local/Microsoft/Edge/User Data/Default/History		
Zip	bing.com	2023-02-22 11:53:25 CST	Microsoft Edge	/img_allagniappe.E01vol_vo6/Users/AILAGNIAPPE/AppData/Local/Microsoft/Edge/User Data/Default/History		
discord download	bing.com	2023-02-13 19:43:07 CST	Microsoft Edge	/img_allagniappe.E01vol_vo6/Users/AILAGNIAPPE/AppData/Local/Microsoft/Edge/User Data/Default/History		
discord download	bing.com	2023-02-13 19:43:07 CST	Microsoft Edge	/img_allagniappe.E01vol_vo6/Users/AILAGNIAPPE/AppData/Local/Microsoft/Edge/User Data/Default/History		
dropbox	bing.com	2023-02-22 11:34:30 CST	Microsoft Edge	/img_allagniappe.E01vol_vo6/Users/AILAGNIAPPE/AppData/Local/Microsoft/Edge/User Data/Default/History		
dropbox	bing.com	2023-02-22 11:34:30 CST	Microsoft Edge	/img_allagniappe.E01vol_vo6/Users/AILAGNIAPPE/AppData/Local/Microsoft/Edge/User Data/Default/History		
outlook	bing.com	2023-02-22 10:51:51 CST	Microsoft Edge	/img_allagniappe.E01vol_vo6/Users/AILAGNIAPPE/AppData/Local/Microsoft/Edge/User Data/Default/History		
outlook client	bing.com	2023-02-22 10:52:51 CST	Microsoft Edge	/img_allagniappe.E01vol_vo6/Users/AILAGNIAPPE/AppData/Local/Microsoft/Edge/User Data/Default/History		
outlook client	bing.com	2023-02-22 10:52:51 CST	Microsoft Edge	/img_allagniappe.E01vol_vo6/Users/AILAGNIAPPE/AppData/Local/Microsoft/Edge/User Data/Default/History		
outlook client	bing.com	2023-02-22 10:52:51 CST	Microsoft Edge	/img_allagniappe.E01vol_vo6/Users/AILAGNIAPPE/AppData/Local/Microsoft/Edge/User Data/Default/History		
outlook desktop app	bing.com	2023-02-22 10:53:32 CST	Microsoft Edge	/img_allagniappe.E01vol_vo6/Users/AILAGNIAPPE/AppData/Local/Microsoft/Edge/User Data/Default/History		
outlook desktop app	bing.com	2023-02-22 10:53:32 CST	Microsoft Edge	/img_allagniappe.E01vol_vo6/Users/AILAGNIAPPE/AppData/Local/Microsoft/Edge/User Data/Default/History		
outlook desktop app	bing.com	2023-02-22 10:53:32 CST	Microsoft Edge	/img_allagniappe.E01vol_vo6/Users/AILAGNIAPPE/AppData/Local/Microsoft/Edge/User Data/Default/History		
outlook desktop windows	bing.com	2023-02-22 10:54:14 CST	Microsoft Edge	/img_allagniappe.E01vol_vo6/Users/AILAGNIAPPE/AppData/Local/Microsoft/Edge/User Data/Default/History		
outlook desktop windows	bing.com	2023-02-22 10:54:14 CST	Microsoft Edge	/img_allagniappe.E01vol_vo6/Users/AILAGNIAPPE/AppData/Local/Microsoft/Edge/User Data/Default/History		

Figure 3: List of web searches done by the suspect






Listing							
Web Downloads							
Table	Thumbnail	Summary					
Source Name	S	C	O	Path	URL	▲ Date Accessed	Domain
 History			1	C:\Users\AILAGNIAPPE\Downloads\DiscordSetup.exe	https://discord.com/a...	2023-02-13 19:43:15 CST	discord.com
 History			0	C:\Users\AILAGNIAPPE\Downloads\DiscordSetup.exe	https://dl.discordapp...	2023-02-13 19:43:15 CST	discordapp.net
 History			1	C:\Users\AILAGNIAPPE\Downloads\Dropbox\Installer.exe	https://www.dropbo...	2023-02-22 11:34:53 CST	dropbox.com
 History			1	C:\Users\AILAGNIAPPE\Downloads\Dropbox\Installer.exe	https://dl-web.dropb...	2023-02-22 11:34:53 CST	dropbox.com
 History			1	C:\Users\AILAGNIAPPE\Downloads\7z2201-x64.exe	https://www.7-zip.or...	2023-02-22 11:53:31 CST	7-zip.org

Figure 4: List of suspect's downloads

Keyword search					4 Results
Table Thumbnail Summary					
					Save Table as CSV
Name	Keyword Preview	Location	Modified Time	Change Time	
pagefile.sys	il.com24,7,7*sleazysteve@gmail.com<24,7,7voice-n	/img_allagnippe.E01/vol_volo/pagefile.sys	2023-02-22 20:05:25 CST	2023-02-22 20:05:25 CST	
HxStore.hxd	comc"/\$p;de8sleazysteve@gmail.com<24,7,7no-repl	/img_allagnippe.E01/vol_volo/Users/AIAGNIAPPE/AppDa...	2023-02-22 20:08:17 CST	2023-02-22 20:08:17 CST	
Windows.edb	Lagniappe@sleazysteve@gmail.com<sleazysteve@gmail.c...	/img_allagnippe.E01/vol_volo/ProgramData/Microsoft/Sea...	2023-02-22 20:10:15 CST	2023-02-22 20:10:15 CST	
edb.jtx	Lagniappe@sleazysteve@gmail.com<sleazysteve@gmail.c...	/img_allagnippe.E01/vol_volo/ProgramData/Microsoft/Sea...	2023-02-22 20:10:15 CST	2023-02-22 20:10:15 CST	

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

```

$ 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
0g 0:00:00:05 1.63% (ETA: 23:50:14) 0g/s 53426p/s 53426c/s 53426C/s jedidah..dukefan
0g 0:00:04:25 DONE (2023-02-28 23:49) 0g/s 54088p/s 54088c/s 54088C/s !SkicA!..*7iVamos!
Session completed.

```

Figure 6: Attempt to access not\_illegal.zip by running the hash against the rockyou word list using JohnTheRipper

```

$ john --incremental 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
0g 0:00:00:02 0g/s 36680p/s 36680c/s 36680C/s 153216..090983
0g 0:00:00:04 0g/s 42794p/s 42794c/s 42794C/s sumpia..mc1594
0g 0:00:18:09 0g/s 54734p/s 54734c/s 54734C/s daskrt81..dellbfff
0g 0:20:54:17 0g/s 56585p/s 56585c/s 56585C/s jhdsur1..jhdsp21
0g 0:20:54:23 0g/s 56584p/s 56584c/s 56584C/s jlues8x..jlueyjm

```

Figure 7: Attempt to bruteforce not\_illegal.zip using JohnTheRipper

72221104.E0E	2023-02-22 11:53:30 CST 1	Patched File	USERS\ALAGNIAPPE\
72711.E0E	2023-02-22 11:54:10 CST 1	Patched File	PROGRAM FILES\7-ZIP
728.E0E	2023-02-22 11:55:40 CST 1	Patched File	PROGRAM FILES\7-ZIP

Figure 8: 7zip Running



[illegible]

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