

Forensics Investigation Report

Case 1372: Operation Banjo

Prepared for

Head of Forensic Department

By

Abimbola Omoshola (001184927)
Richa Sarita Bhandari (001185806)
Lois Amarachi Ukaegbu (001180193)

Table of Contents

EXECUTIVE SUMMARY	4
1. INTRODUCTION	4
2. VICTIMS	5
2.1 Victim details	5
3. LOCATION OF EVIDENCE	5
3.1 Evidence description	6
3.2 Seizure details	6
Location of Evidence	6
4. DEFINITIONS	7
4.1 Definitions	7
4.2 Tools	8
5. PRESERVATION OF EVIDENCE	8
5.1 Imaging of Original Evidence	8
5.1.1 Procedures	8
5.1.2 Result	8
5.2 Validation of Investigation Evidence	9
5.2.1 Procedures	9
5.2.2 Result	10
6. ANALYSIS STEPS	11
6.1 Procedures	11
6.1.1 Procedure 1 – Accessing the Zipped folder named “Cut.zip”	11
6.1.2 Procedure 2 – Accessing the zipped folder named “Work.Now.zip”	13
6.1.3 Procedure 3 – Accessing the zipped folder named “M.Q Database.zip”	15
6.1.4 Procedure 4 – Accessing the zipped folder named “Zombies.docx”	17
6.1.5 Procedure 5 – Accessing the zipped file named “Eight.docx”	18
6.1.6 Procedure 6 – Accessing the zipped file named “Donalds.zip”	20
6.1.7 Procedure 7 – Accessing the zipped file named “Stuff.zip”	21
6.1.8 Procedure 8 – Accessing the zipped file named “Weapon Receipt.zip”	23
6.1.9 Procedure 9 – Accessing the “Doc1.docx” File	25
7. RESULTS	26
7.1 Pertinent Document Summaries	26
7.1.1 Document 1 Summary – “Cut.zip”	26
7.1.2 Document 2 Summary – “Work.Now.zip”	26
7.1.3 Document 3 Summary – “M.Q Database.zip”	27
7.1.4 Document 4 Summary – “Zombies.docx”	28
7.1.5 Document 5 Summary - “Eight.docx”	30
7.1.6 Document 6 Summary - “Donalds.zip”	32
7.1.7 Document 7 Summary - “Stuff.zip”	32
7.1.8 Document 8 Summary - “Weapon Receipt.zip”	34
7.1.9 Document 9 Summary – “Doc1.docx”	35
7.2 Pertinent Images Summary	36
7.2.1 Image 1 Summary – Agreement	36
7.2.2 Image 2 Summary – Weapons	36

7.2.3	Image 3 Summary – comrades.txt.....	37
7.2.4	Image 4 Summary – Pretty pay.xlsx	37
7.2.5	Image 5 Summary – Supplied.eml	38
7.2.6	Image 6 Summary – What do you have_.eml	39
7.2.7	Image 7 Summary – are you mental_.eml	39
7.2.8	Image 8 Summary – chill out.eml	39
7.2.9	Image 9 Summary – STOP.eml	40
7.2.10	Image 10 Summary – enough is enough!.eml.....	40
7.2.11	Image 11 Summary – no thanks.eml.....	40
8.	CONCLUSION	41

EXECUTIVE SUMMARY

Recently, a racial assault threatened the community of Greenwich. It was alleged that Keith Kingsman spearheaded this aggravated assault. The victims of this assault were Malcolm M Quacker, the Head of the duck community as well as Mr. & Mrs. Donald, the petrified neighbours of Mr. Quacker. Considering this, it became crucial that we examine and analyse the digital evidence seized from the suspect to enable us to establish an objective finding that would assist in the investigation, either to prosecute the perpetrators of the crime or acquit any innocent person from all forms of allegations.

The compressed evidence file “Operation Banjo” was examined and analysed. Overall, there appears to be ample evidence to prove that the crime was carefully planned over a period. Several email communications between members of the blackout brigade detailing the planned racial attack was discovered. We also found a good number of passworded and plain text documents containing vital information such as locations for the attack, amount to be paid for each duck killed or injured just to mention a few. In addition, emails communications on the purchase and supply of various weapons possibly for the planned attack was also found. There is also evidence of declared hatred nurtured for Mr. Malcolm and other ducks in the city and the plans to get rid of them.

1. INTRODUCTION

At approximately 7.30pm on Friday 11th December 2020, in response to a 999 call, armed police and ambulance crews were dispatched to Blackheath, with instructions specifying to troop within an alleyway, “right next to the KFC”. where two alleged rival gangs had clashed, and gunshots had been heard.

On arrival, police found only one group there, who were, for the majority, seriously injured. They found several people suffering from knife wounds, and others who were badly beaten, with exposed wounds and major bruising.

After determining there were no firearms at the scene, ambulance crews were allowed to attend to the injured. Among the injured was a well-known man, named Malcolm Quacker, a victim who had been severely beaten, and appeared to have been shot. He was immediately taken to A&E. Malcolm Quacker’s records show that several complaints had been made by him, regarding harassment and personal safety policies.

The Police conducted interviews at the scene. Witnesses at the scene stated they were targeted by a gang wearing bandanas bearing the swastika, signifying a local gang, known to the police for past altercations with illegal weapons and racial activism. The witnesses stated that they had noticed a crowd of youths entering the pond area of Blackheath, and they appeared to be up to no good. At the same time another group of older men were seen coming from the area of Greenwich Park and appeared to be carrying

weapons. Soon after arriving at the pond area, the youths chased the group, who were gathered there, straight into the waiting men who began beating, punching and kicking them. Some of the men went in towards the pond area, and that's when shots were heard. Three men came out of the area, and one shouted "job done", and the attackers then ran off back towards the park, where they had come from. One of the casualties had said that they had met by the pond to hear a speech that Malcolm was giving, when suddenly a bunch of youths came out of nowhere, and started to attack them, they ran out of the area, but there was another crowd waiting for them on the other side of the trees. The Police suspected this to be the work of a group known as the Blackout Brigade, led by Keith K. Kingsman, known the police for online racial abuse, before the creation of his gang.

The attackers, who wore swastika crested bandanas, were screaming obscenities such as "Ducks! Go back to your own country", "F*** off now diseased freeloaders", among other things. When examining the area of the crime, a driver's license had been found, under the name "Henry Himler". Henry had been taken for questioning, and after interrogation, he had revealed that he was an unwilling member of a gang, called the "Blackout Brigade", which is known to be led by Keith K. Kingsman, and his sidekicks Rudy Hess and himself, Henry Himler.

Witnesses have also stated that the Quacker family, who are residents at number 18 Pond St had been photographing households on the street. These suspects were identified as the Donald family. Claims have been substantiated by other residents in and around the Pond St. area. When questioned about his involvement in the alleged offence, Mr. Donald said that he had no choice because he had received emails threatening his family and himself. This alone didn't make him decide to do their bidding, it was when he started to receive photos of his daughter, going and coming from school, going to the store, that he felt he had no choice but to comply with their requests.

Keith Kingsman was arrested at 11pm on Saturday 12th December 2020, via a house raid, led by the police for suspicions of aggravated racial assault. A USB stick, as well as an android phone and some physical evidence had been seized. Mr. Kingsman had swallowed, what seemed to be an SD card, which could not be seized.

2. VICTIMS

2.1 Victim details

Malcolm M Quacker - Respected local businessman ("Head" of the duck community)

Mr and Mrs Donald - Frightened neighbours of Mr. Quacker

3. LOCATION OF EVIDENCE

3.1 Evidence description

One 2 GB SanDisk USB was seized (exhibit OB/1)

One Android phone was seized (exhibit OB/2)

Exhibit OB/2 has been sent off for further analysis to the Institution of Forensics Analysis, located in Cambridge.

Exhibit OB/1 has been sent for analysis to the Greenwich Cyber Team for analysis.

OB/3 – photograph of a pamphlet showing dead ducks

OB/4 – photograph of a samurai sword seized during the raid

OB/5 – a photograph of a post it

3.2 Seizure details

Because of the probability of firearms being involved, a warrant was issued, and at 2am on Saturday 12th December 2020, a raid was initiated on Mr. Kingsman's home, where he was arrested for suspicion of inciting a racially motivated riot and causing grievous bodily harm with intent. Once the premises were secured, Digital Forensics officers entered, and seized several items of interest.

3.3 Handling Details (Chain of Custody)

Location of Evidence

12th Dec 20 Exhibits OB/1 and OB/2 were seized

OB/1 was imaged by Greenwich Cyber Team, Detective Inspector Dylan J Walker (DJW)

The original USB has been placed in the secure locker, No 8673

15th Feb 21 The forensics image of OB/1 was passed to the Forensic Department for analysis

20th Feb 22 Exhibit OB/1 (SanDisk USB) was sterilized and checked by the Greenwich Cyber Team

28th Feb 22 The exhibit OB/1 image file (E01) was downloaded by the Greenwich Cyber Team

11th Mar 22 The Greenwich Cyber Team verified the OB/1 image file that was downloaded using two forensic tools namely, FTK Imager and Autopsy

31st Mar 22 Greenwich Cyber Team completed the investigation and sterilized the USB device.

4. DEFINITIONS

4.1 Definitions

Acquisition of Digital Evidence: Begins when information and/or physical items are collected or stored for examination purposes. The term "evidence" implies that the collection of evidence is recognized by the courts. The process of collecting is also assumed to be a legal process and appropriate for rules of evidence in that locality. A data object or physical item only becomes evidence when so deemed by a law enforcement official or designee.

Data Objects: Objects or information of potential probative value that are associated with physical items. Data objects may occur in different formats without altering the original information.

Digital Evidence: Information of probative value stored or transmitted in digital form. **Physical Items:** Items on which data objects or information may be stored and/or through which data objects are transferred.

Original Digital Evidence: Physical items and the data objects associated with such items at the time of acquisition or seizure.

Duplicate Digital Evidence: An accurate digital reproduction of all data objects contained on an original physical item.

Copy: An accurate reproduction of information contained on an original physical item, independent of the original physical item.

Decrypting: Process of converting encrypted data back to its original format.

Data Encryption: This involves the process of scrambling data into an unreadable form, by this only authorized people can use the right key or code and translate the data back to a completely readable form.

Metadata: describes data about data for each file in forensic investigation. This enables forensic investigators to have a clear picture of the history of any electronic file involved in the investigation. It keeps the timeline of the date the file was created and tracks the dates of any changes made to the file.

Data forensics: the process of applying digital analysis or forensic to the recovered digital information to identify evidence of crime and determine the relationship to the suspect(s), by building relevant inferences that can tie the data elements into competent evidence.

Hash Value: The hash value of an electronic file is a set alphanumeric value that is produced to uniquely identify the contents of that file. If in any case, the contents of the file is modified, the value of the hash will change significantly as a flag that the file has been tampered with. Hashing preserves the integrity of any file which is a very useful feature in forensic investigation.

Password Protected: Password protection allows the owner of a document to protect his file or data with a secret code called password. By assigning password to the file, an unauthorized user cannot read

the content of the file, cannot change (edit) the data, and cannot delete any part of the passworded file without the knowledge of the password.

Forensic Artefact: In digital forensic analysis, artefacts are the digital objects or things that may have been inadvertently left behind by the perpetrators of the case crime. These objects, which maybe pictures, are usually left invisible and hidden as it can it give significant clues to the incident being investigated.

Directory: Directory in computing is also known as a folder which represents a collection of various related files created and organized for a particular purpose. A file being contained in a directory is a unit of information stored on a computer and given a name before keeping it in the directory..

Zippered: Zipping involves **packaging a set of individual files into a single file or folder archive that is called a zip file**. Usually, the files in a zip file are compressed so that they take up less space in storage or take less time to send to someone.

4.2 Tools

The following tools were used during the analysis:

Autopsy version 4.19.0 – Autopsy is a tool that allows forensic experts to examine mobile devices or hard drives and recover evidence from it.

FTK Imager version 4.1.1.1 – FTK Imager is a toolkit that allows forensic experts to access digital evidence very quickly to establish if further analysis is required.

Online-Tools – This is an online platform that provides various web tools for free. During this investigation, this tool was used for decrypting data.

Python Shell – An online tool that interprets the Python programming language.

5. PRESERVATION OF EVIDENCE

5.1 Imaging of Original Evidence

5.1.1 Procedures

The original exhibit “Operation Banjo.E01” was not handled by us, however the information provided shows that the imaging of the exhibit was performed by “G.K”.

5.1.2 Result

From figure 1 below, we can see that the imaging was performed using a Win 201x on the 12/Dec/2020.

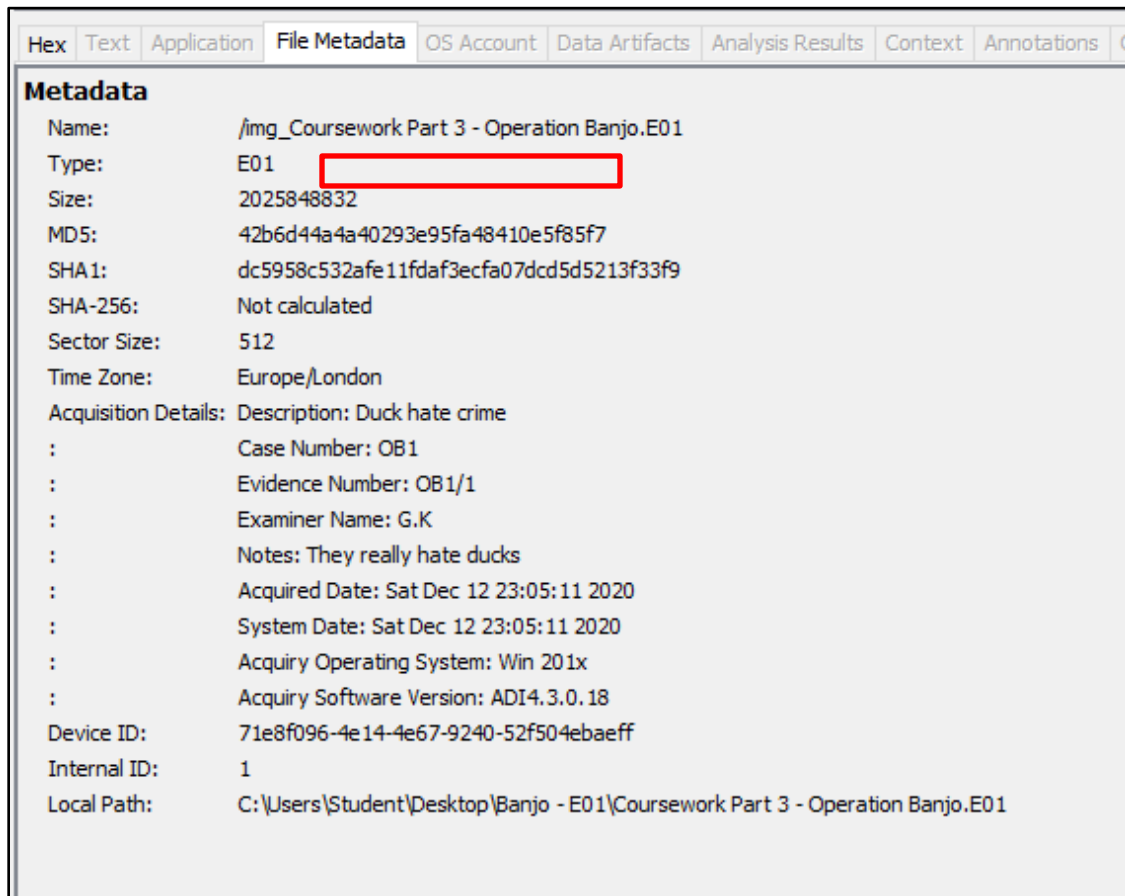


Figure 1: Metadata of the Original Exhibit - OB/1

5.2 Validation of Investigation Evidence

5.2.1 Procedures

Two forensic tools were used to validate the integrity of the original exhibit under investigation and to ascertain that the file is free from any modification. Autopsy version 4.19.0 and FTK imager version 4.1.1.1 were used for validation.

5.2.2 Result

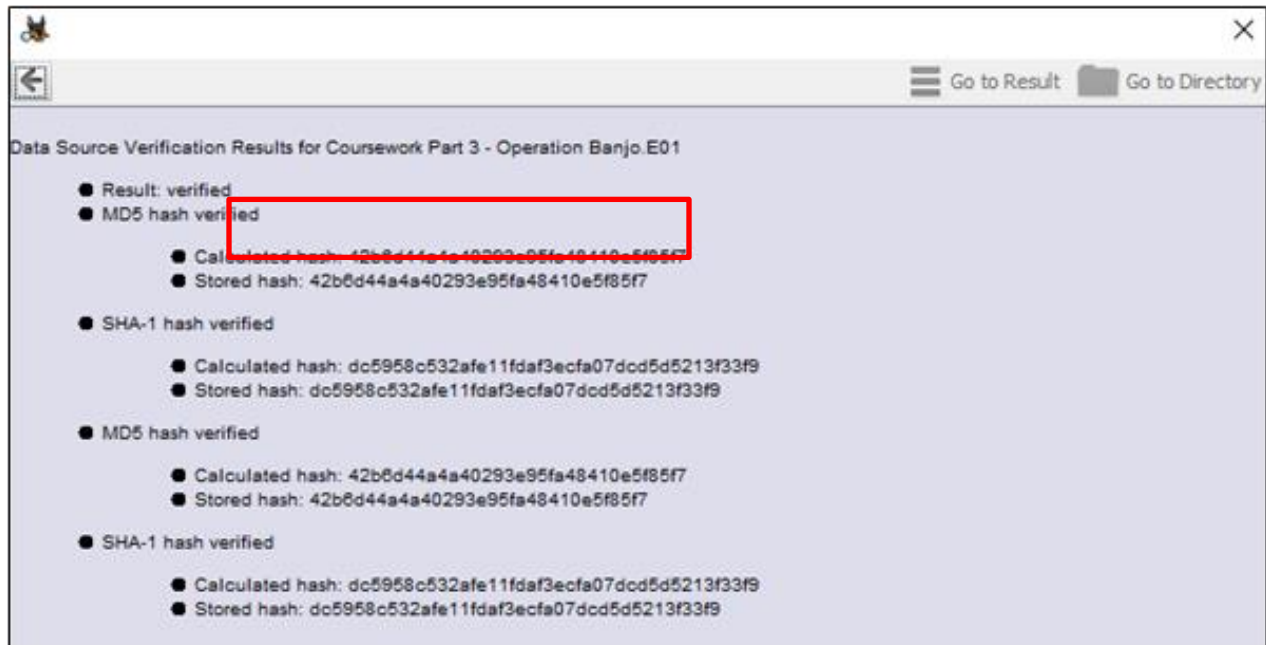


Figure 2: Original Exhibit Validation Using Autopsy v4.19.0

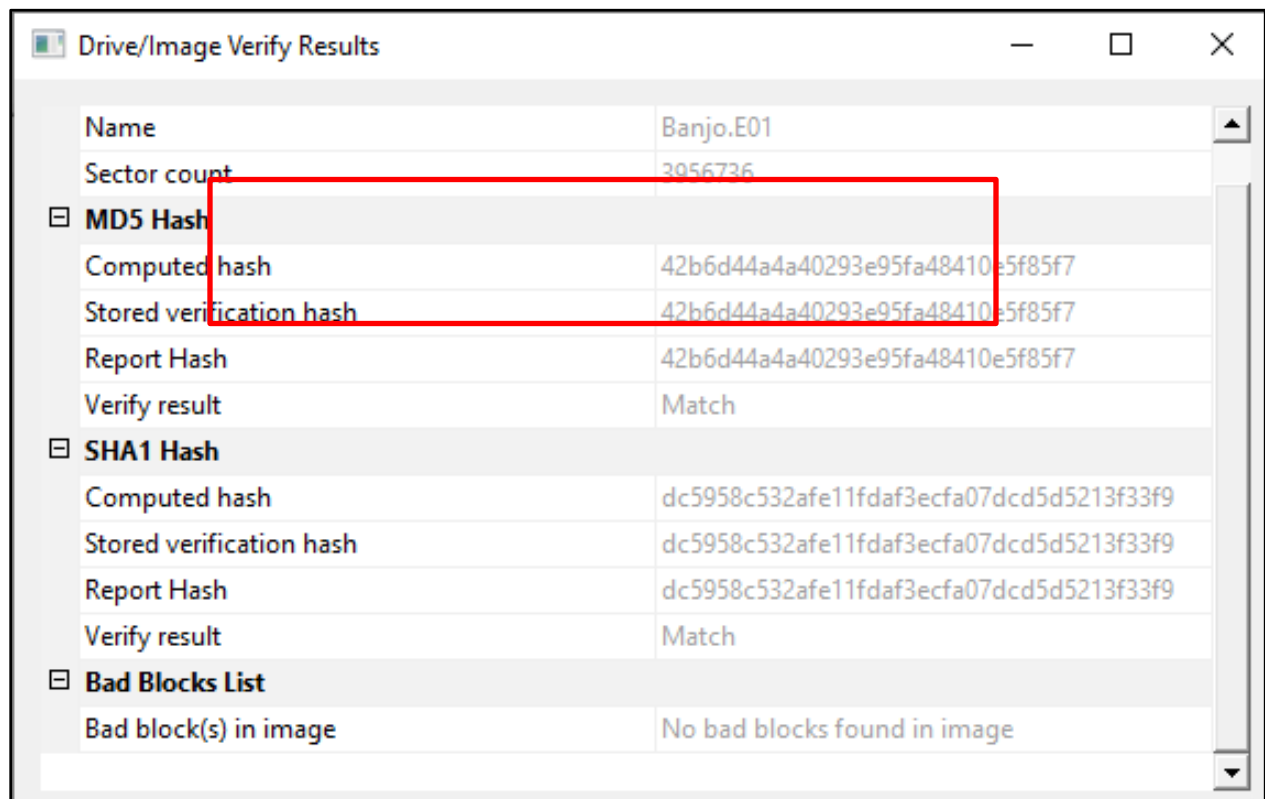


Figure 3: Original Exhibit Validation Using FTK Imager v4.1.1.1

CONFIDENTIAL

6. ANALYSIS STEPS

6.1 Procedures

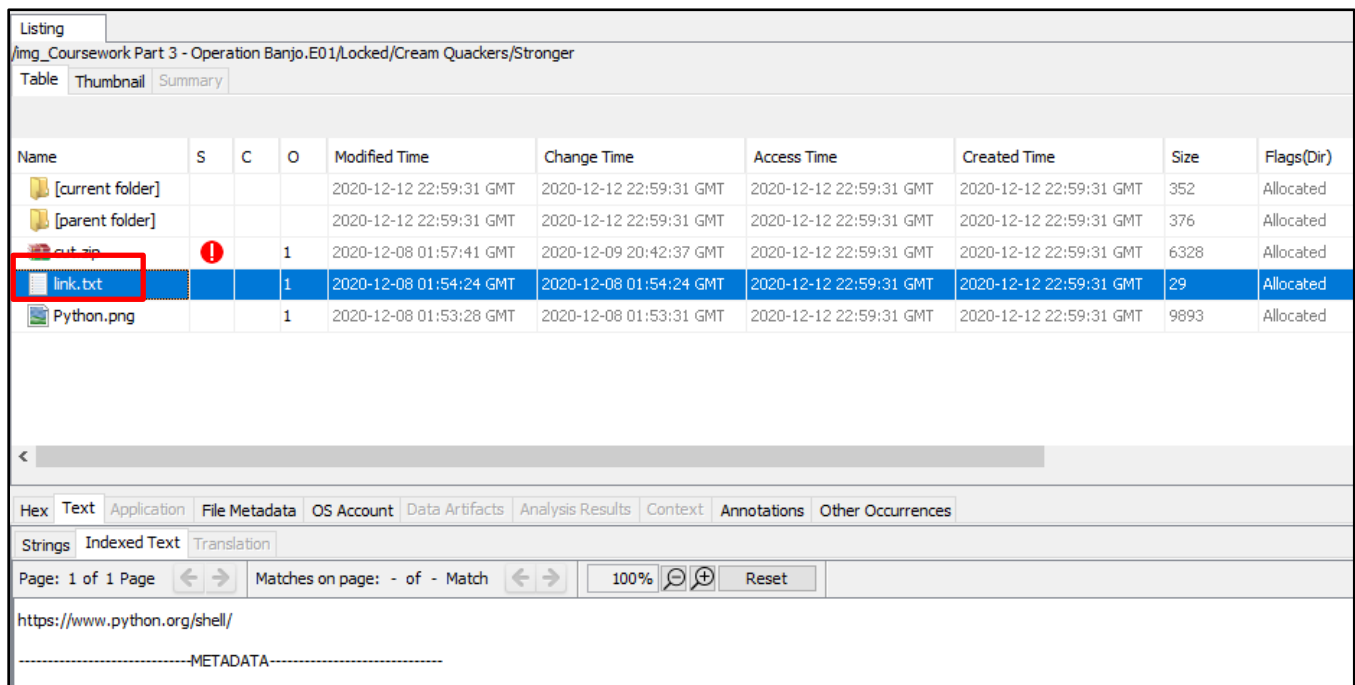
6.1.1 Procedure 1 – Accessing the Zipped folder named “Cut.zip”

Upon loading the image file to Autopsy, we found 8 files that were passworded. We decided to take a closer look. The first file we looked at was the **Cut.zip** file. Unfortunately, we could not access this file by just extracting it, hence, we did further investigation to find clues on how this file could be accessed.

We went to the directory of the zipped file and found a text file named “**link.txt**”. When this file was opened, a link to an online python shell was found as shown in **Figure 4** below.

In addition, we also discovered a picture named “**python.png**” which is shown below. Kindly refer to figure 5 below. The picture found, displayed a python script, which was copied and ran on an online python shell as shown in figure 6 below. The online python shell then produced the value “**job3**”.

We tried to see if this value could be the password to the “Cut.zip” file and we were correct. The content of the “cut.zip” file is shown in **section 7.1.1** below.



The screenshot shows the Autopsy file listing interface. The file list is as follows:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
[current folder]				2020-12-12 22:59:31 GMT	2020-12-12 22:59:31 GMT	2020-12-12 22:59:31 GMT	2020-12-12 22:59:31 GMT	352	Allocated
[parent folder]				2020-12-12 22:59:31 GMT	2020-12-12 22:59:31 GMT	2020-12-12 22:59:31 GMT	2020-12-12 22:59:31 GMT	376	Allocated
cut.zip			1	2020-12-08 01:57:41 GMT	2020-12-09 20:42:37 GMT	2020-12-12 22:59:31 GMT	2020-12-12 22:59:31 GMT	6328	Allocated
link.txt			1	2020-12-08 01:54:24 GMT	2020-12-08 01:54:24 GMT	2020-12-12 22:59:31 GMT	2020-12-12 22:59:31 GMT	29	Allocated
Python.png			1	2020-12-08 01:53:28 GMT	2020-12-08 01:53:31 GMT	2020-12-12 22:59:31 GMT	2020-12-12 22:59:31 GMT	9893	Allocated

Below the file list, the 'Strings' tab is selected, showing the content of the selected file (link.txt):

```
https://www.python.org/shell/
```

Below the strings, the 'METADATA' tab is selected, showing the file's metadata.

Figure 4: Text File Containing Link to an Online Python Shell

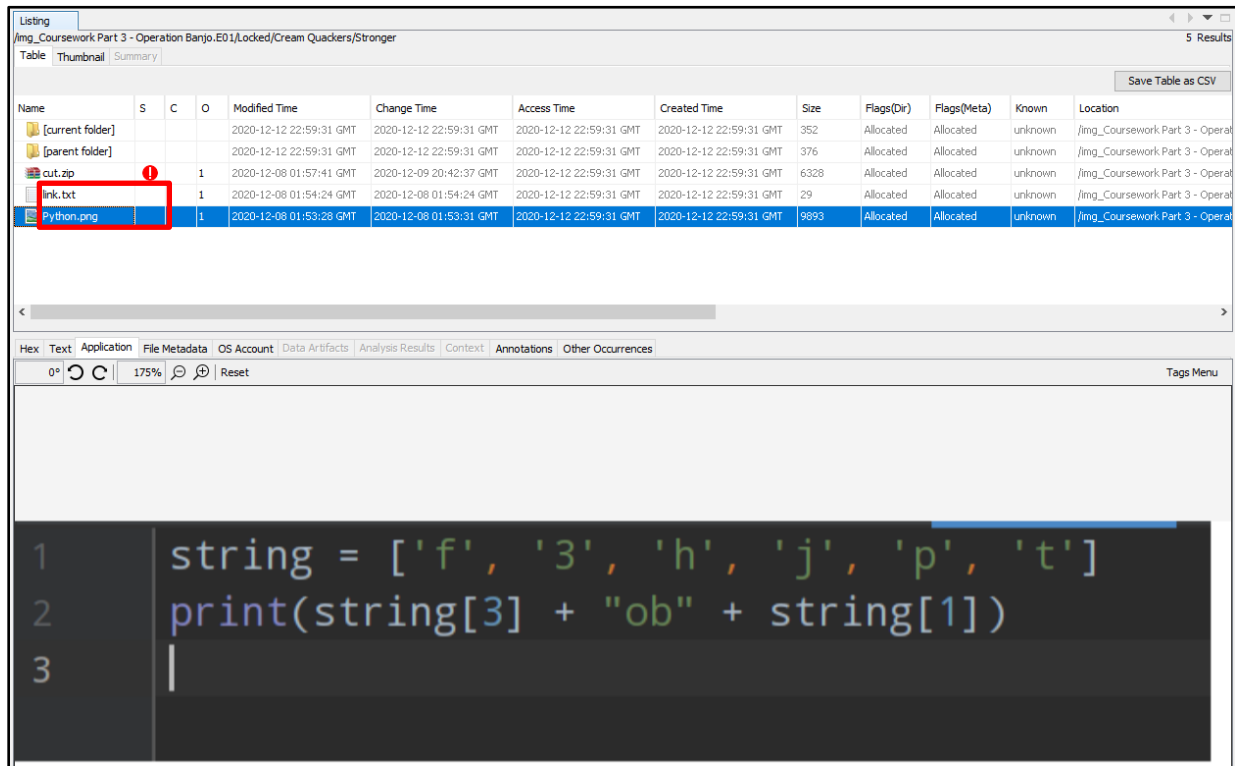


Figure 5: Picture Displaying the Python Script Found

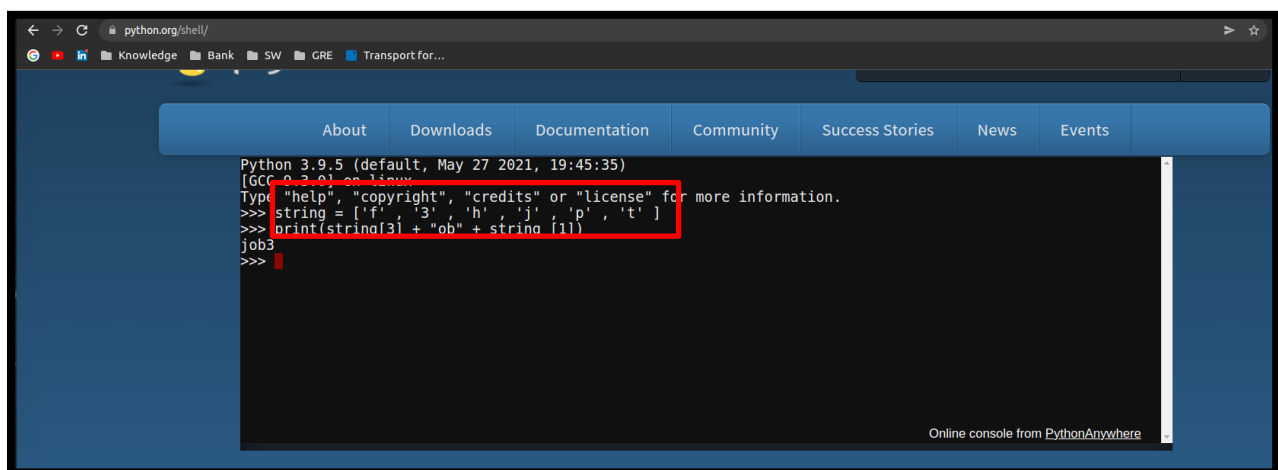


Figure 6: The Online Python Shell

Metadata	
Name:	/img_Coursework Part 3 - Operation Banjo.E01/Locked/Cream Quackers/Stronger/cut.zip
Type:	File System
MIME Type:	application/zip
Size:	6328
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2020-12-08 01:57:41 GMT
Accessed:	2020-12-12 22:59:31 GMT
Created:	2020-12-12 22:59:31 GMT
Changed:	2020-12-09 20:42:37 GMT
MD5:	dffbca3450a90a6e43458551cb51290f
SHA-256:	51cc38dcc91b6c1228215aa0638b0b024df308964128a9e2afd55a6c52b6cc6c
Hash Lookup Results:	UNKNOWN
Internal ID:	377

Figure 7: Metadata of the "Cut.zip" File

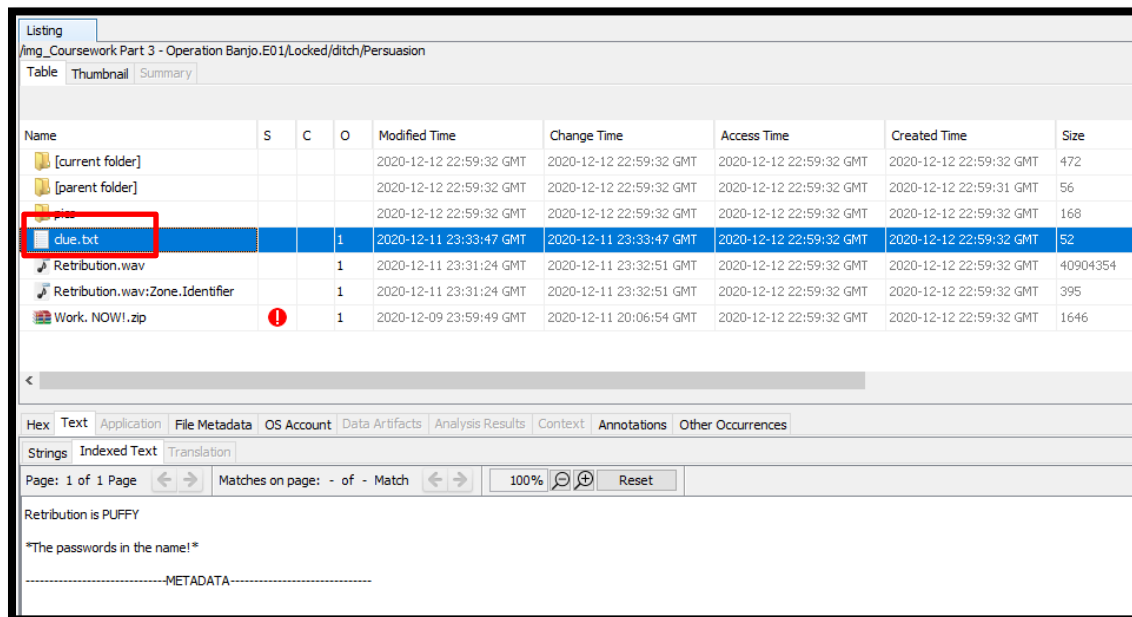
6.1.2 Procedure 2 – Accessing the zipped folder named “Work.Now.zip”

We also found another file named "**Work.Now.zip**" which was zipped and passworded. Again, we were unable to access this file by merely extracting the files. For us to access this file, we decided to search for clues. First, we accessed the directory of the zipped file and found a text file named "**clue.txt**". This file caught our attention and we decided to open the file. In the file was the word "**retribution is PUFFY *passwords in the name***". We also found an image file with a mismatched file extension named "**play at 2.12.txt file**". It had the following written text:

pass = bus_ _ _ _

Retribution!

In addition, we found two audio files named "**retribution.wav**" and "**retribution.wav:zone.identifier**". With this information, we concluded that all files found were linked and had to do with the password for accessing the "**Work.Now**" zipped file. Hence, we listened to the two retribution audio recordings and paid close attention to what was said at 2 minutes 12 seconds. Surprisingly, we got the word "**busstop**" which was used to access the "Work.Now" file. The content of the zipped file is shown in section 7.1.2 below.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]				2020-12-12 22:59:32 GMT	2020-12-12 22:59:32 GMT	2020-12-12 22:59:32 GMT	2020-12-12 22:59:32 GMT	472
[parent folder]				2020-12-12 22:59:32 GMT	2020-12-12 22:59:32 GMT	2020-12-12 22:59:32 GMT	2020-12-12 22:59:31 GMT	56
clue.txt			1	2020-12-11 23:33:47 GMT	2020-12-11 23:33:47 GMT	2020-12-12 22:59:32 GMT	2020-12-12 22:59:32 GMT	52
Retribution.wav			1	2020-12-11 23:31:24 GMT	2020-12-11 23:32:51 GMT	2020-12-12 22:59:32 GMT	2020-12-12 22:59:32 GMT	40904354
Retribution.wav:Zone.Identifier			1	2020-12-11 23:31:24 GMT	2020-12-11 23:32:51 GMT	2020-12-12 22:59:32 GMT	2020-12-12 22:59:32 GMT	395
Work. NOW!.zip			1	2020-12-09 23:59:49 GMT	2020-12-11 20:06:54 GMT	2020-12-12 22:59:32 GMT	2020-12-12 22:59:32 GMT	1646

Retribution is PUFFY

The passwords in the name!

Figure 8: The "Clue.txt" File

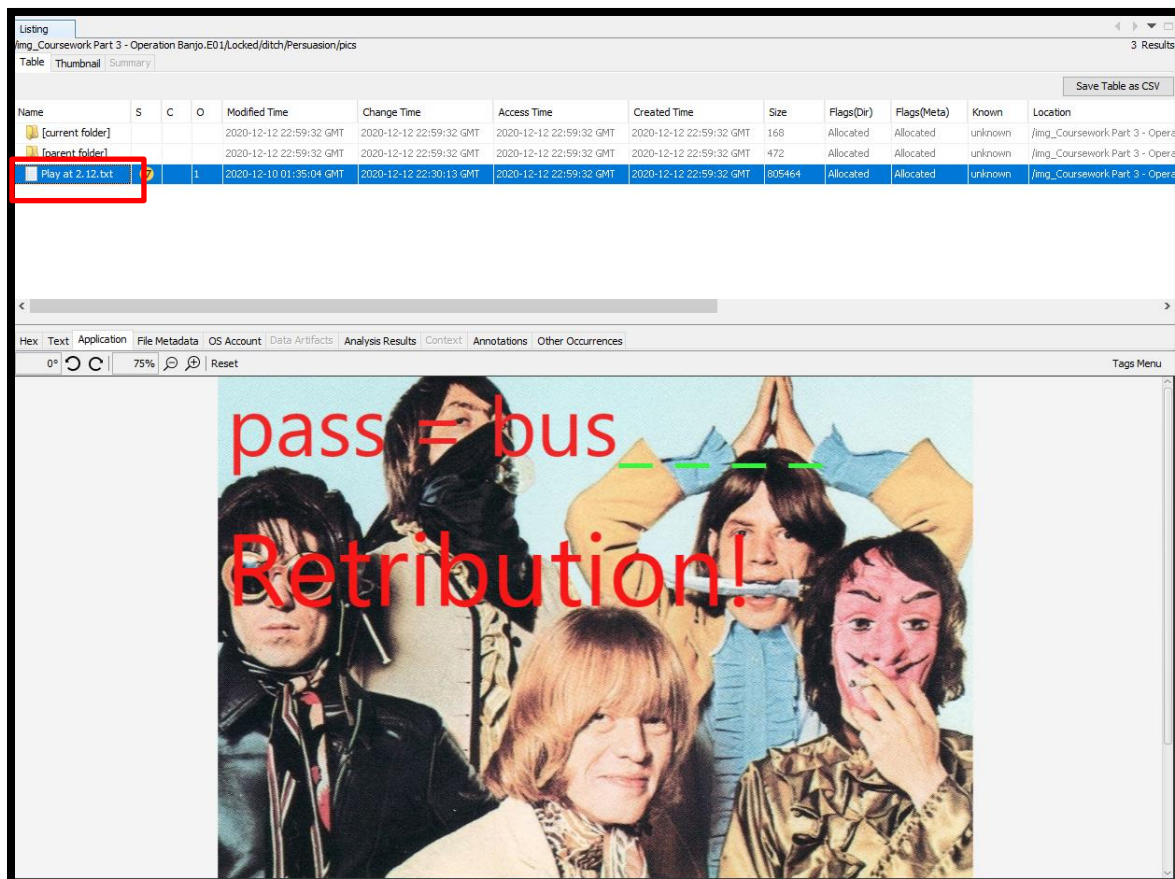


Figure 9: The "play at 2.12.txt file".

due.txt		1	2020-12-11 23:33:47 GMT	2020-12-11 23:33:47 GMT	2020-12-12 22:59:32 GMT
Retribution.wav		1	2020-12-11 23:31:24 GMT	2020-12-11 23:32:51 GMT	2020-12-12 22:59:32 GMT
Retribution.wav:Zone.Identifier		1	2020-12-11 23:31:24 GMT	2020-12-11 23:32:51 GMT	2020-12-12 22:59:32 GMT
Work. NOW!.zip	!	1	2020-12-09 23:59:49 GMT	2020-12-11 20:06:54 GMT	2020-12-12 22:59:32 GMT

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
-----	------	-------------	---------------	------------	----------------	------------------	---------	-------------	-------------------

Page: 1 of 2497 Page: Go to Page: 1 Jump to Offset Launch in HxD

```

0x00000000: 52 49 46 46 9A 26 70 02 57 41 56 45 66 6D 74 20 RIFF.&p.WAVEfmt
0x00000010: 10 00 00 00 01 00 02 00 80 BB 00 00 00 EE 02 00 .....
0x00000020: 04 00 10 00 4C 49 53 54 1A 00 00 00 49 4E 46 4F .....LIST.....INFO
0x00000030: 49 53 46 54 0E 00 00 00 4C 61 76 66 35 38 2E 34 ISFT....Lavf58.4
0x00000040: 35 2E 31 30 30 00 64 61 74 61 54 26 70 02 00 00 S.100.dataTsp...
0x00000050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

Figure 10: The "Retribution.wav" and "Retribution.wav:Zone.Identifier Audio File

Metadata	
Name:	/img_Coursework Part 3 - Operation Banjo.E01/Locked/ditch/Persuasion/Work. NOW!.zip
Type:	File System
MIME Type:	application/zip
Size:	1646
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2020-12-09 23:59:49 GMT
Accessed:	2020-12-12 22:59:32 GMT
Created:	2020-12-12 22:59:32 GMT
Changed:	2020-12-11 20:06:54 GMT
MD5:	b63c7da3692fa60668c8bb2dd926836c
SHA-256:	c37a678f44cd8b503c8082b1343b5f557fa397f139d8a61a4f0db206f6e39a87
Hash Lookup Results:	UNKNOWN
Internal ID:	790

Figure 11: The Metadata for "Work.Now!.zip" file

6.1.3 Procedure 3 – Accessing the zipped folder named “M.Q Database.zip”

We found yet another zipped file. Like the other files discussed above, the “**M.Q Database.zip**” file was not accessible. We needed a password to access this file. Hence, we searched for clues.

First, we accessed the directory of the file and found an image file named "**pattern.ng**" as shown in figure 12 below. Upon opening the file, we discovered that file contained patterns as the name implies. We did elementary mathematics of the pattern and arrived at the value "**597**", which we tried as the password to

access the "M.Q Database.zip" file and it worked. The content of the passworded file "M.Q Database.zip" is shown in section 7.1.3 of this report.

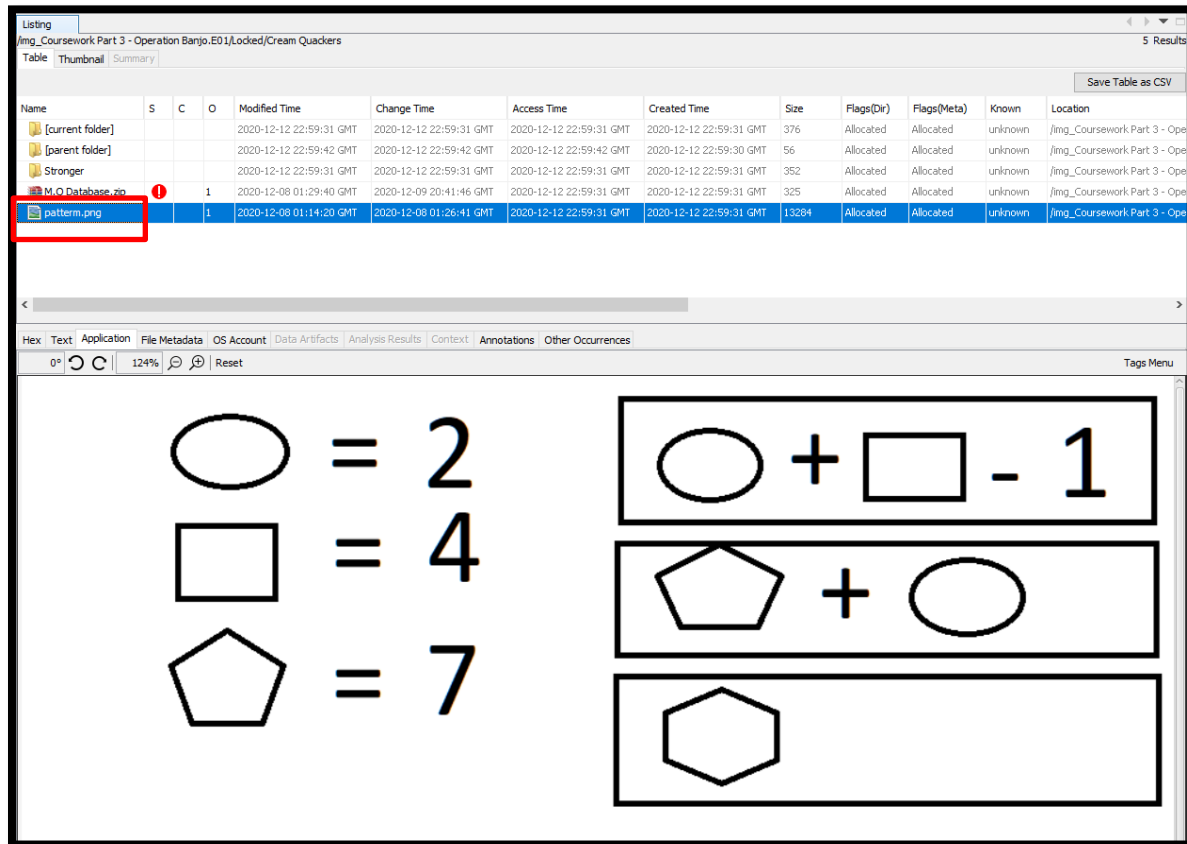


Figure 12: The "Pattern.png" File

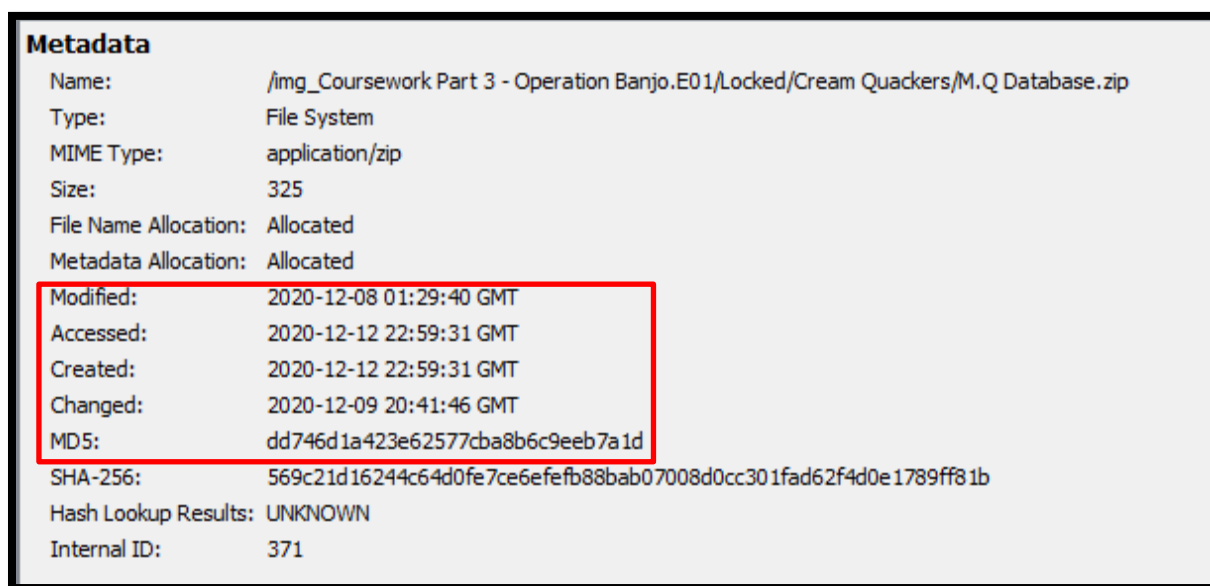


Figure 13: The Metadata for the "M.Q Database.zip" File

6.1.4 Procedure 4 – Accessing the zipped folder named “Zombies.docx”

Yet another zipped file named "**zombies.docx**" was found in the original exhibit. This file was also protected using a password. We were unable to access this file, hence we had to look for clues. As usual, we accessed the directory of the file and found a text file named "**code.docx**". Inside the code.docx file was an image and URL as shown in figure 15 below. We visited the URL and used the information we found to decode what the image translates to "**93116**". This was the password to the "zombies.docx" file. The content of the file is shown in section 7.1.4 of this report.

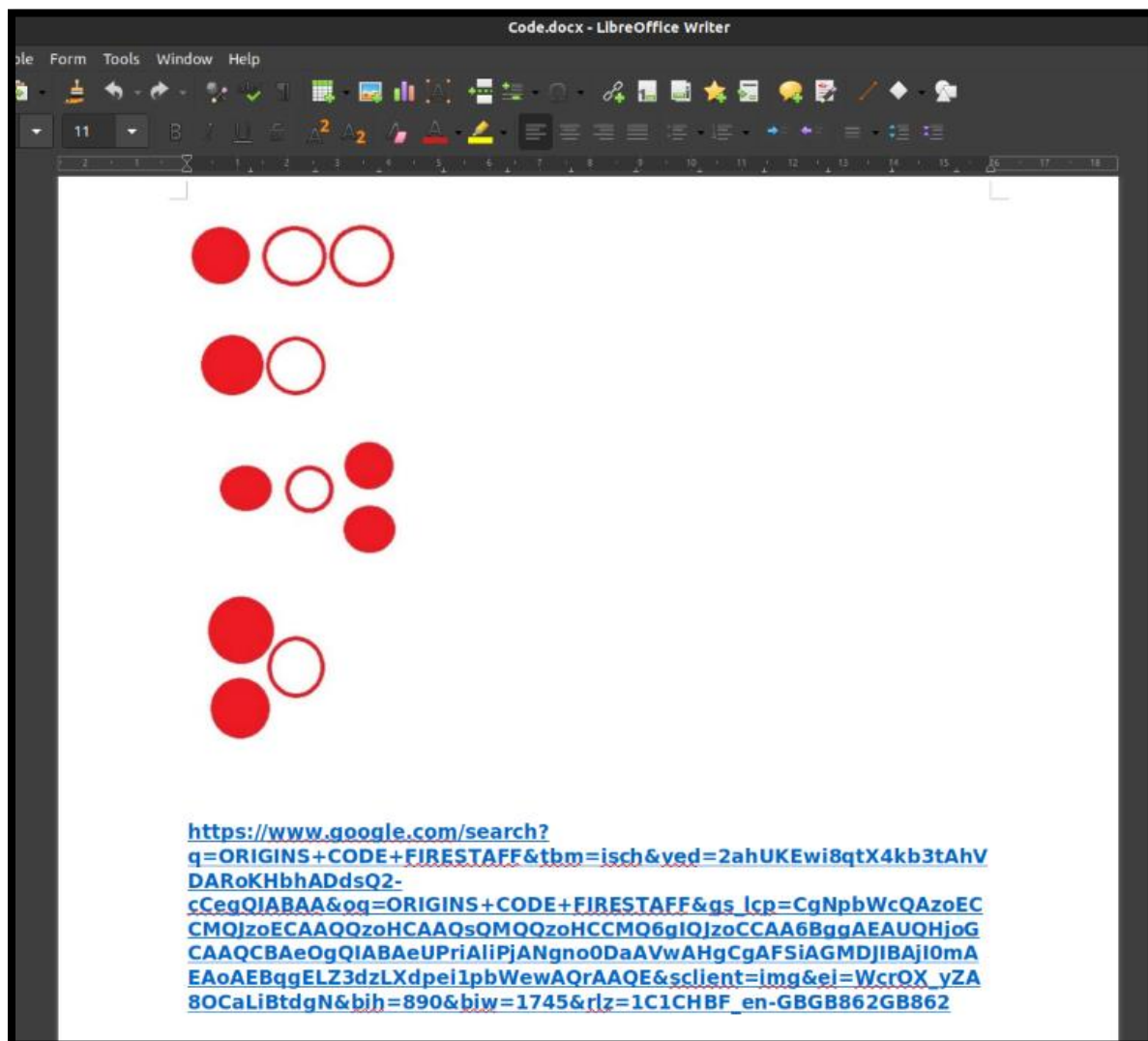


Figure 14: The "Code.docx" File

Metadata	
Name:	/img_Coursework Part 3 - Operation Banjo.E01/Locked/Games/Zombies.docx
Type:	File System
MIME Type:	application/x-ooxml-protected
Size:	19456
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2020-12-08 02:07:35 GMT
Accessed:	2020-12-12 22:59:35 GMT
Created:	2020-12-12 22:59:35 GMT
Changed:	2020-12-08 02:07:35 GMT
MD5:	5c59b88fa1d313af852bd1ae470607d9
SHA-256:	f25d63b46e001be4979342d5b21e5a903fe900a66a0d5df1d0aaf7237040b966
Hash Lookup Results:	UNKNOWN
Internal ID:	1342
Downloaded From:	https://cdn.discordapp.com/attachments/764103696530800691/785648703930368020/Part_2_Medium_Ev_Files.zip

Figure 15: The Metadata for the "Zombies.docx" File

6.1.5 Procedure 5 – Accessing the zipped file named "Eight.docx"

Another file named "**Eight.docx**" was found. To access its content, we needed to search for clues to the password. We checked the file's directory and an image file named "**8 look closely.png**" was found. The file contained an image of a creature known as a "**Charizard**". We came to this conclusion after thorough research over the internet. We tried the word Charizard as the password, but it failed to open the eight.docx file. Hence, we decided to take a closer look at the creature. Seeing that the Charizard had value "**1**" written on it, we decided to try "**Charizard1**" as the password and it worked. The contents of the "Eight.docx" file are shown in section 7.1.5 of this report.

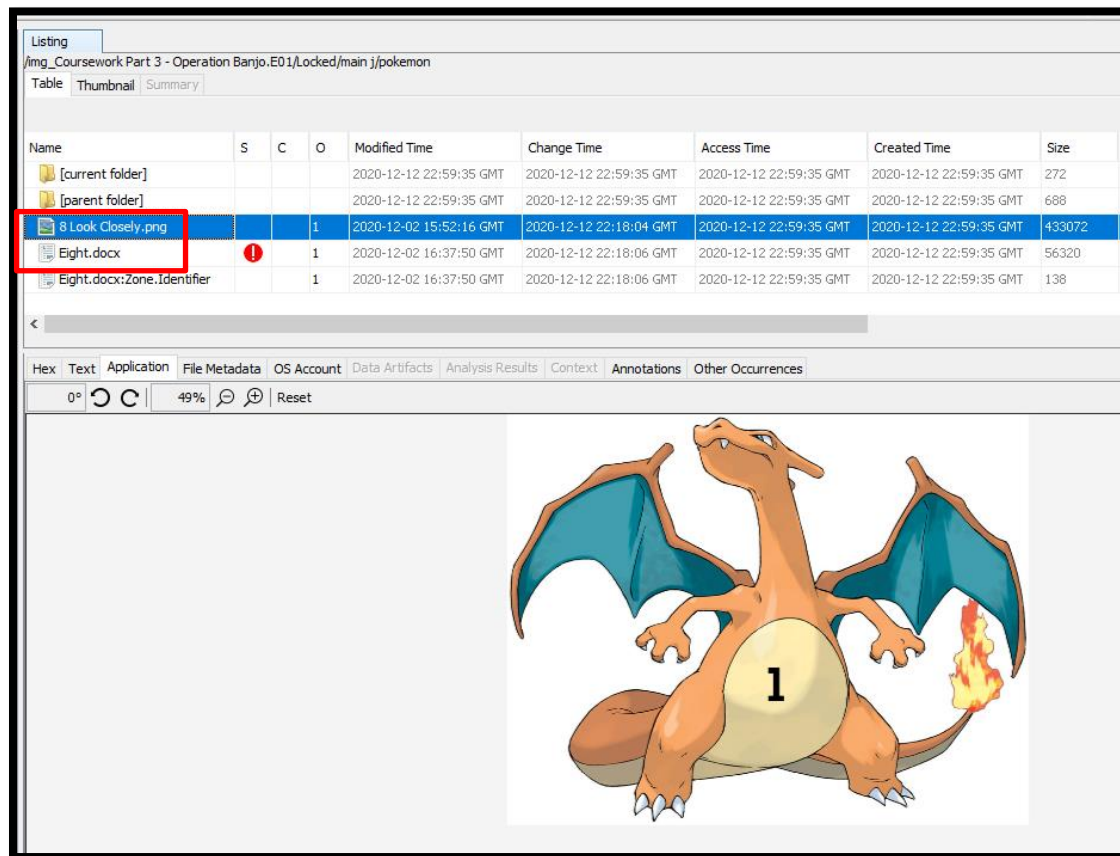


Figure 16: The Image named "8 look closely.png"



Figure 17: The Metadata for the "Eight.docx" File

6.1.6 Procedure 6 – Accessing the zipped file named “Donalds.zip”

We found another file named **"donald.zip"** which was password protected. To access it, we looked for clues. First, we accessed the directory of the zipped file and found a text file named **"password.txt"**. The file was opened and the clue **"- - - - 123"** was found. We looked for other clues to help decipher the missing alphabet and numbers in the word **"- - - - 123"** but could not find any. We also tried several common words and names of individuals under investigation. Unfortunately, none of the combinations worked. And then it hit us that we have seen the word **"banjo"** which is a five-letter word appear in several files and directories. Hence, we decided to try the word **"banjo123"** as the password to the **"donald.zip"** and surprisingly it worked. The content of **"donald.zip"** can be found in section 7.1.6 of this report.

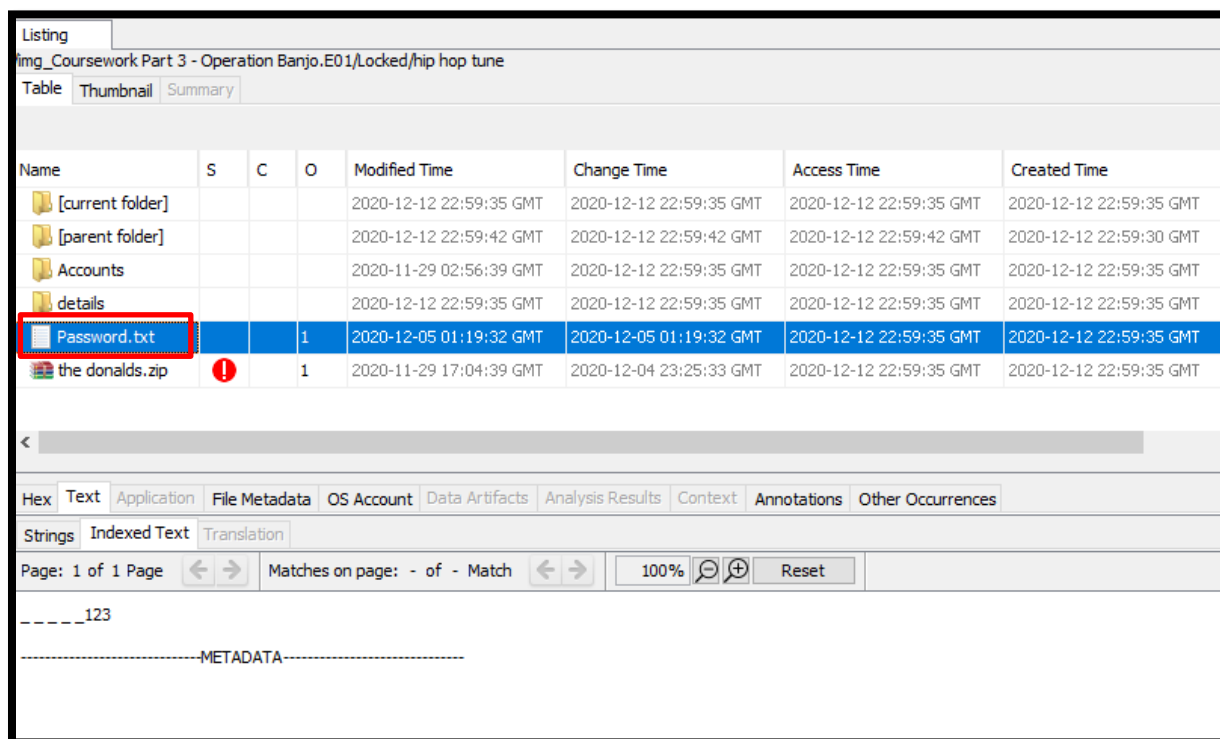


Figure 18: The “Password.txt” File

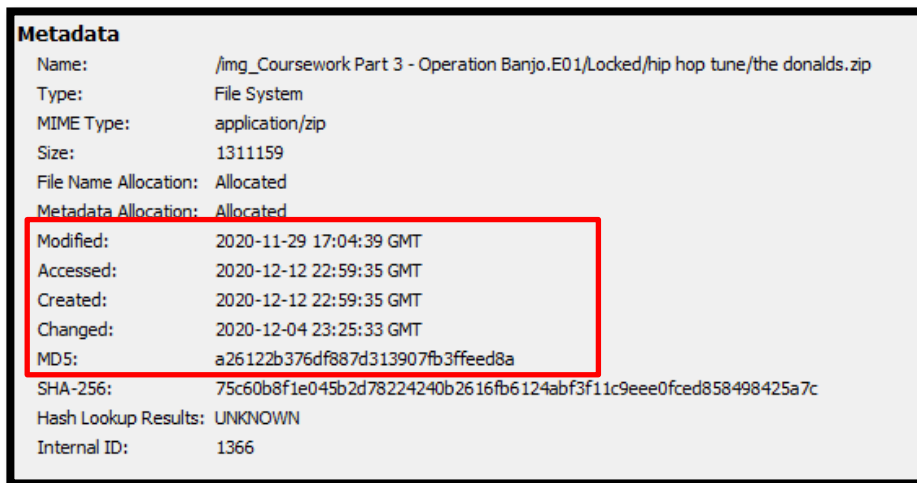


Figure 19: Metadata for the "donalds.zip" file

6.1.7 Procedure 7 – Accessing the zipped file named “Stuff.zip”

Another file that was discovered was the zipped file named **"stuff.zip"**. This file was passworded and could not be accessed. To access this zipped file, we looked for clues. As such, we accessed the directory for the zipped file "stuff.zip" and found a text file named **"tutorial.txt"**. When the "tutorial.txt" file was opened, we found the word **"md5 = Password!!!"**. We also saw two image files named **"dragpassword.jpg"** and **"dragpassword.jpg:zone.identifier"** respectively. We checked to see if the MD5 hash value for the word "password" can be used to access the "stuff.zip" file but unfortunately it did not work. Then we went ahead to try the MD5 hash value for the image file "dragpassword.jpg" and it worked. The content of the "stuff.zip" file is shown in section 7.1.7 of this report.

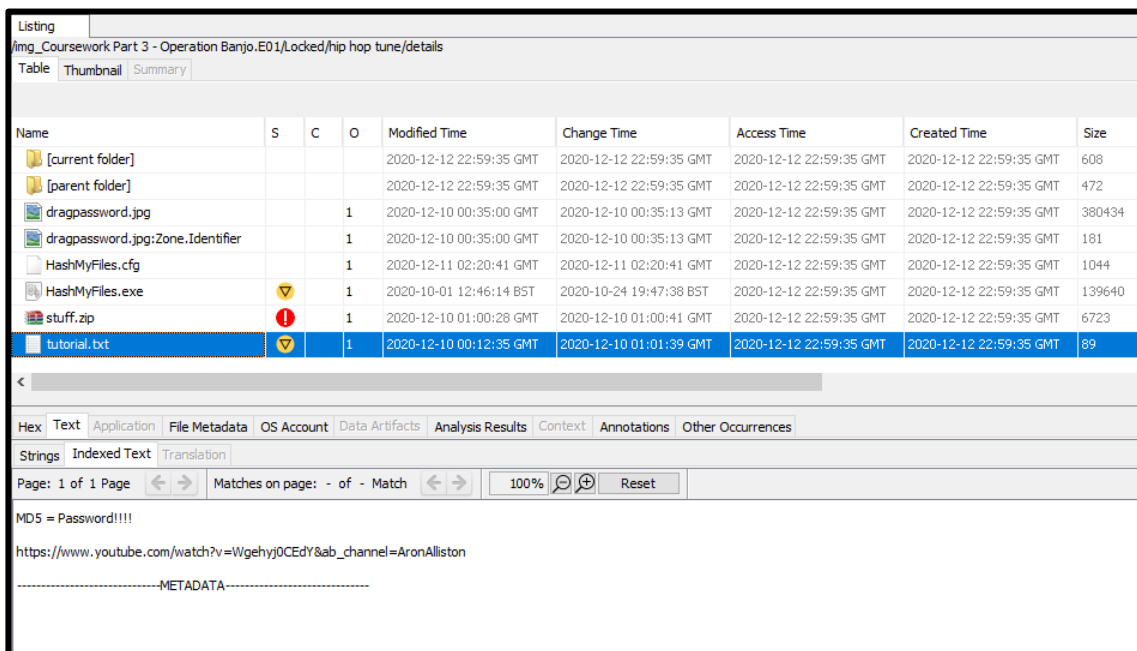


Figure 20: The "Tutorial.txt" File

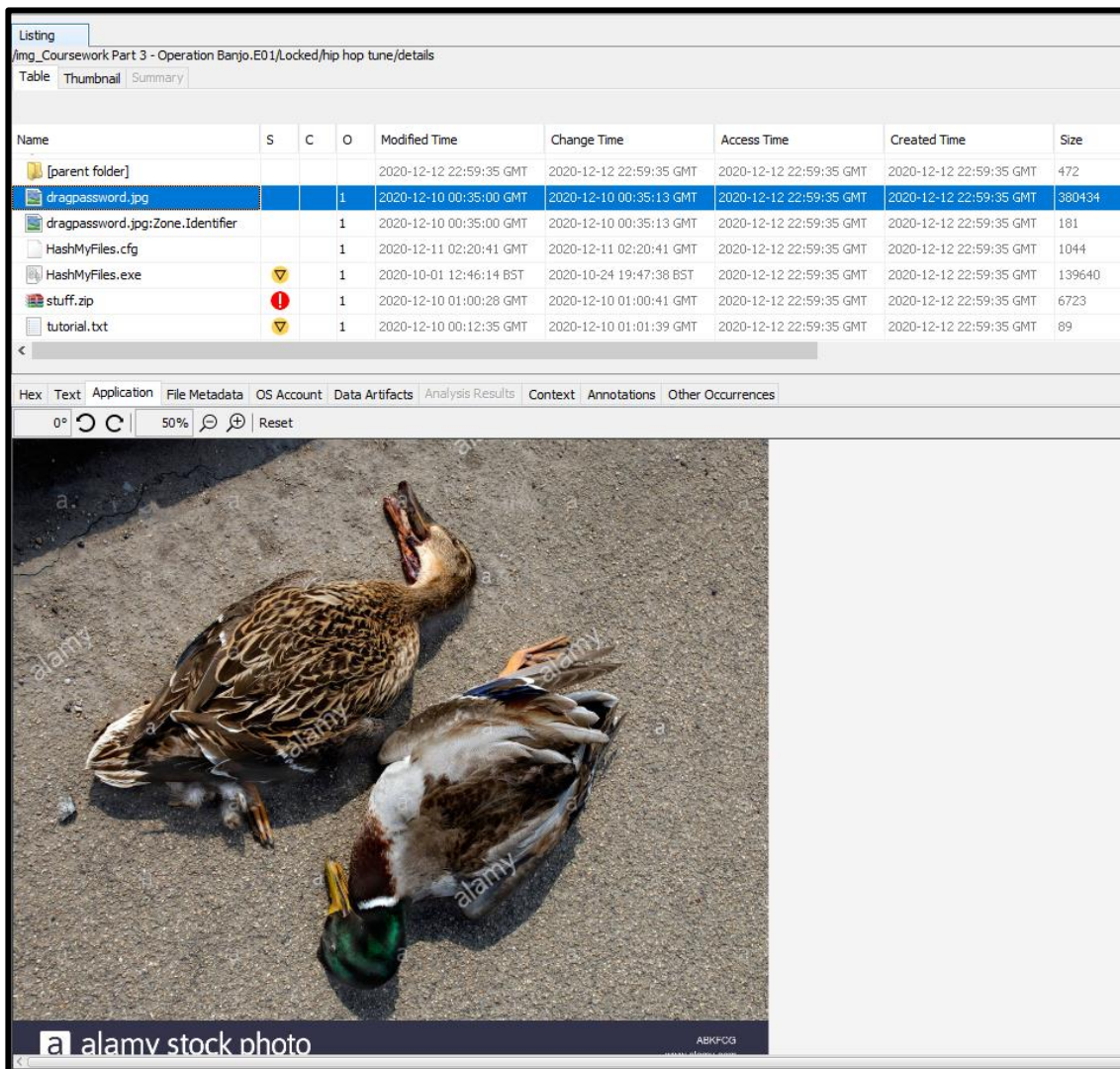


Figure 21: The Image File Named "dragpassword.jpg"

Listing				
/img_Coursework Part 3 - Operation Banjo.E01/Locked/hip hop tune/details				
Table Thumbnail Summary				
Flags(Dir)	Flags(Meta)	Known	Location	MD5 Hash
Allocated	Allocated	unknown	/img_Coursework Part 3 - Operation Banjo.E01/Locked/hip ...	
Allocated	Allocated	unknown	/img_Coursework Part 3 - Operation Banjo.E01/Locked/hip ...	8a63a04e564d43ac967e6a1c05322b3b

Figure 22: The MD5 Hash Value for "dragpassword.jpg"

Metadata	
Name:	/img_Coursework Part 3 - Operation Banjo.E01/Locked/hip hop tune/details/stuff.zip
Type:	File System
MIME Type:	application/zip
Size:	6723
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2020-12-10 01:00:28 GMT
Accessed:	2020-12-12 22:59:35 GMT
Created:	2020-12-12 22:59:35 GMT
Changed:	2020-12-10 01:00:41 GMT
MD5:	e7aa6871f6b3cbb98e390c71babb70fd
SHA-256:	18a4f16a32d613b05c301b86ec5b4dee569812b428a5eaaf790f6102413459a5
Hash Lookup Results:	UNKNOWN
Internal ID:	1362

Figure 23: The Metadata for the "stuff.zip" File

6.1.8 Procedure 8 – Accessing the zipped file named “Weapon Receipt.zip”

We found yet another zipped file named "**Weapon Receipt.zip**", which was passworded. We checked the files directory for clues but could not find any. We randomly searched the entire evidence file for the word "HINTS" and found a picture called "**HINT**" with the word "**ilnvul**" inscribed on it. We accessed the file directory of the picture and found a file containing a link to Caesar-cipher encrypt and decrypt website. We also discovered an image named "**-7**". We thus visited the Caesar-cipher website, inputted the word "ilnvul" and selected the value "-7". We got the word "**begone**" which turned out to be the password for the "Weapon Receipt.zip" file. The content of the "Weapon Receipt.zip" file is shown in section 7.1.8 of this report.

Listing

Images

TableThumbnailSummary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
image9.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	86155	Allocated	Allocated	unknown
image41.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	18049	Allocated	Allocated	unknown
image11.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	61172	Allocated	Allocated	unknown
image54.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	39574	Allocated	Allocated	unknown
image0.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	6726	Allocated	Allocated	unknown
image7.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5876	Allocated	Allocated	unknown
image8.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	21901	Allocated	Allocated	unknown
image1.jpg			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	14989	Allocated	Allocated	unknown
logo-daily-telegraph.png			1	2020-08-06 00:28:21 BST	2020-12-04 00:28:43 GMT	2020-12-12 22:59:30 GMT	2020-12-12 22:59:30 GMT	2208	Allocated	Allocated	unknown
logo-food-network.png			1	2020-08-06 00:28:21 BST	2020-12-04 00:28:43 GMT	2020-12-12 22:59:30 GMT	2020-12-12 22:59:30 GMT	6930	Allocated	Allocated	unknown
logo-good-food.png			1	2020-08-06 00:28:21 BST	2020-12-04 00:28:43 GMT	2020-12-12 22:59:30 GMT	2020-12-12 22:59:30 GMT	911	Allocated	Allocated	unknown
logo-nine.png			1	2020-08-06 00:28:21 BST	2020-12-04 00:28:43 GMT	2020-12-12 22:59:30 GMT	2020-12-12 22:59:30 GMT	4693	Allocated	Allocated	unknown
logo-ten.png			1	2020-08-06 00:28:21 BST	2020-12-04 00:28:43 GMT	2020-12-12 22:59:30 GMT	2020-12-12 22:59:30 GMT	14909	Allocated	Allocated	unknown
HINT.png			1	2020-11-30 00:20:08 GMT	2020-12-12 21:42:51 GMT	2020-12-12 22:59:31 GMT	2020-12-12 22:59:31 GMT	83822	Allocated	Allocated	unknown
247d9890907f4ed8ae16625caf81859c.p			1	2020-12-10 00:45:08 GMT	2020-12-10 00:45:08 GMT	2020-12-12 22:59:31 GMT	2020-12-12 22:59:31 GMT	6039	Allocated	Allocated	unknown
3438e2a59d204bde8f4072bb29dabbf4.p			1	2020-12-10 00:45:08 GMT	2020-12-10 00:45:08 GMT	2020-12-12 22:59:31 GMT	2020-12-12 22:59:31 GMT	2709	Allocated	Allocated	unknown
3b35dc630c02454bb49fc32892e6a6e2.p			1	2020-12-10 00:45:08 GMT	2020-12-10 00:45:08 GMT	2020-12-12 22:59:31 GMT	2020-12-12 22:59:31 GMT	2540	Allocated	Allocated	unknown

HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences

0%188%

Figure 24: The Image File named "HINT"

Metadata	
Name:	/img_Coursework Part 3 - Operation Banjo.E01/Locked/supplies cipher/Weapon Receipt.zip
Type:	File System
MIME Type:	application/zip
Size:	870516
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2020-12-12 16:57:20 GMT
Accessed:	2020-12-12 22:59:35 GMT
Created:	2020-12-12 22:59:35 GMT
Changed:	2020-12-12 16:57:20 GMT
MD5:	208e13be4fc45cf60ebecb1aa479a680
SHA-256:	d340ac5ecb304256df3bb8326874cae5121e44383042408bfe8df4fe13c587cf
Hash Lookup Results:	UNKNOWN
Internal ID:	1567

Figure 25: Metadata for the Weapon Receipt.zip File

6.1.9 Procedure 9 – Accessing the “Doc1.docx” File

A file named “**Doc1.docx**” was found in the folder called “**Flyers**”. When the file was opened, it contained words that looked scrambled. Then we realized that the text was in “**MT Extra font**”. We changed the font style to “**Calibri**” and found a readable text. The readable content of this file is shown in section 7.1.9 of this report.

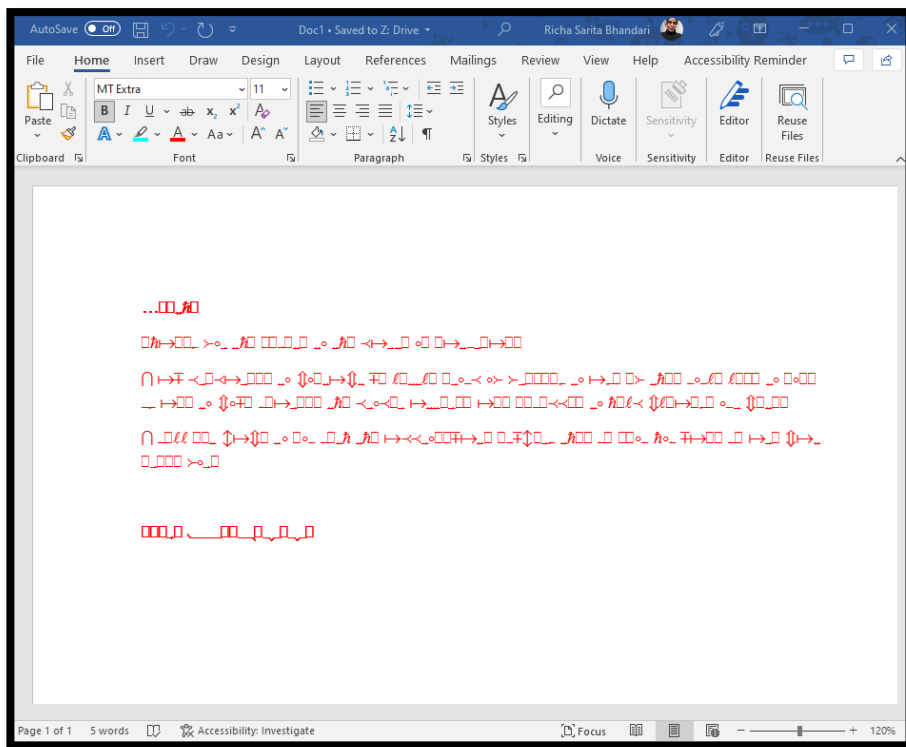


Figure 26: The “Doc1.docx” File

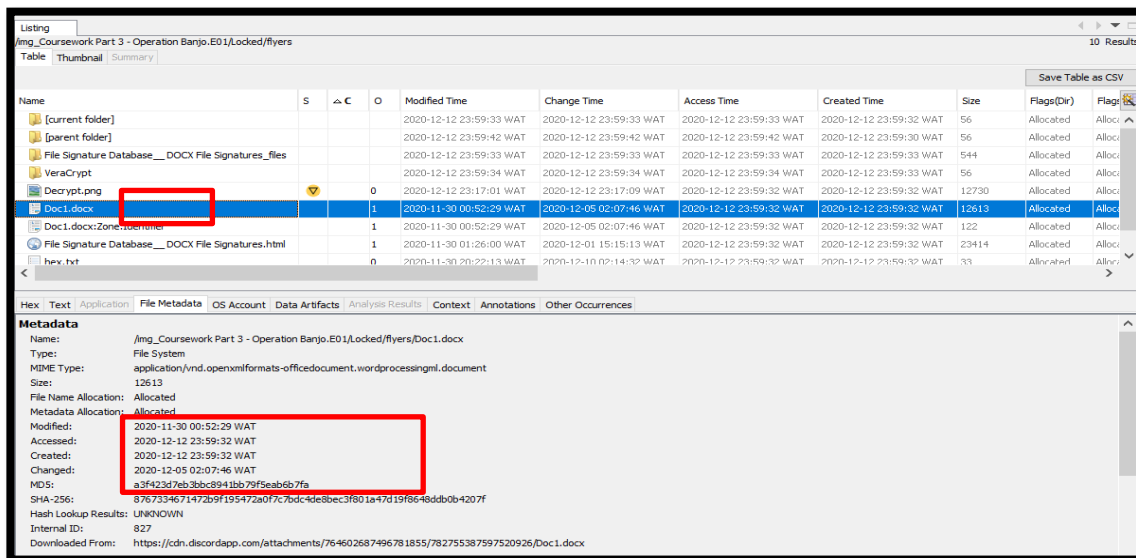


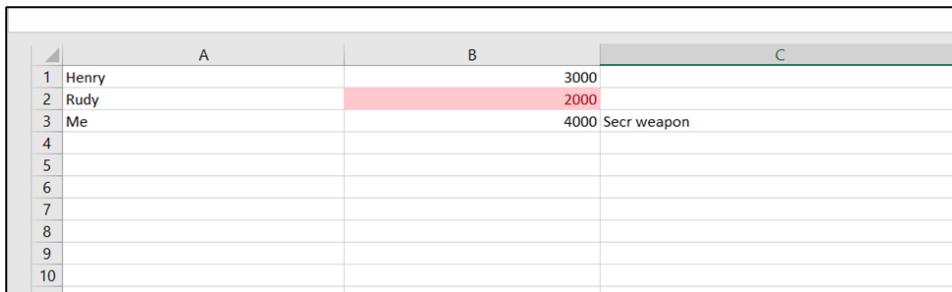
Figure 27: The Doc1.docx file and the associated Metadata

7. RESULTS

7.1 Pertinent Document Summaries

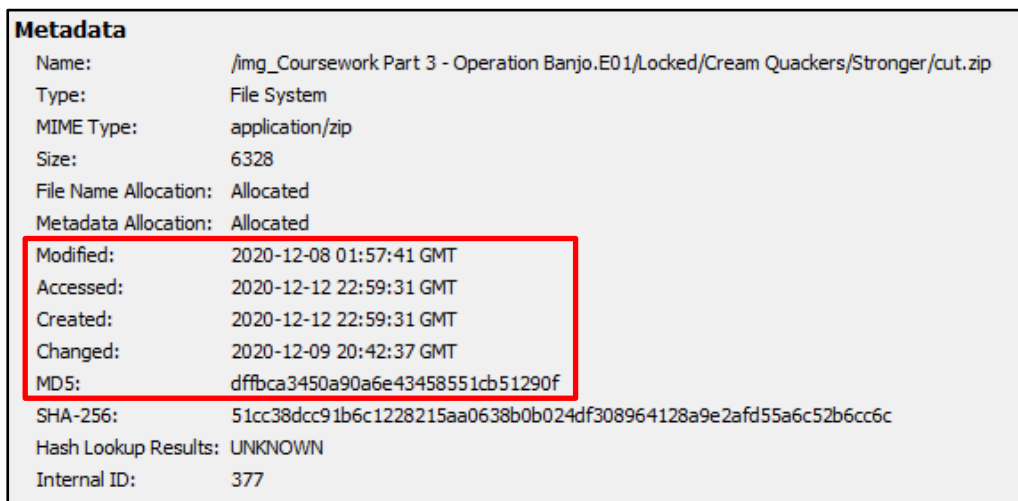
7.1.1 Document 1 Summary – “Cut.zip”

After accessing the “Cut.zip” file with the aid of the password “job3”, an excel sheet named cut.xlsx was found. The excel sheet contained names of some individuals as well as some figures as shown in figure 7 below. This file is not readily available to any individual who uses the computer



	A	B	C
1	Henry	3000	
2	Rudy	2000	
3	Me	4000	Secr weapon
4			
5			
6			
7			
8			
9			
10			

Figure 28: The Excel Sheet Found in the “Cut.zip” File



Metadata	
Name:	/img_Coursework Part 3 - Operation Banjo.E01/Locked/Cream Quackers/Stronger/cut.zip
Type:	File System
MIME Type:	application/zip
Size:	6328
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2020-12-08 01:57:41 GMT
Accessed:	2020-12-12 22:59:31 GMT
Created:	2020-12-12 22:59:31 GMT
Changed:	2020-12-09 20:42:37 GMT
MD5:	dffbca3450a90a6e43458551cb51290f
SHA-256:	51cc38dcc91b6c1228215aa0638b0b024df308964128a9e2afd55a6c52b6cc6c
Hash Lookup Results:	UNKNOWN
Internal ID:	377

Figure 29: Metadata of the “Cut.zip” file

7.1.2 Document 2 Summary – “Work.Now.zip”

Upon accessing the "Work.Now" file using the password "busstop", a "Work.NOW!.eml" file was found. The file contained an email communication between Keith Kingsman and Trio Donald, which was dated September 12, 2020. In the email, Keith Kingsman is requesting for Intel on Malcom Quacker as shown below in figure 30 below. This file is not readily available for any user of the computer

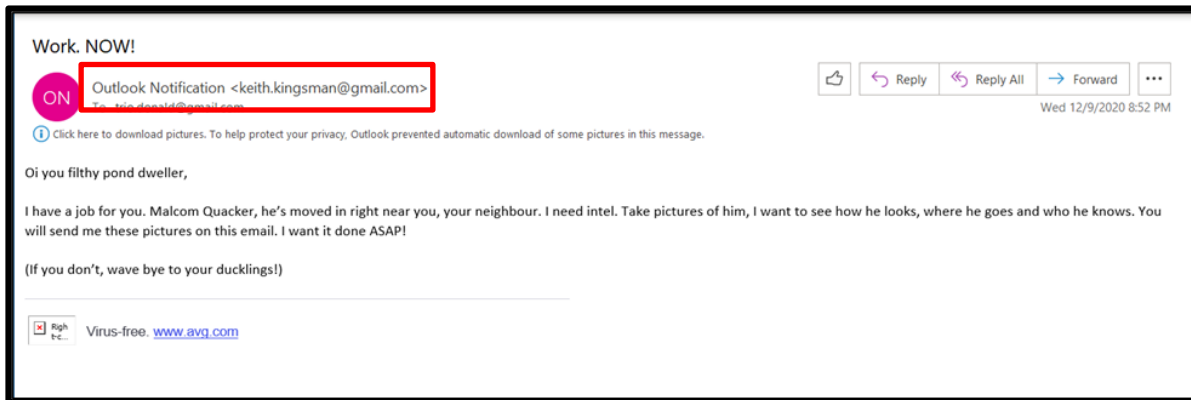


Figure 30: Email Communication where Intel was Requested

Metadata	
Name:	/img_Coursework Part 3 - Operation Banjo.E01/Locked/ditch/Persuasion/Work. NOW!.zip
Type:	File System
MIME Type:	application/zip
Size:	1646
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2020-12-09 23:59:49 GMT
Accessed:	2020-12-12 22:59:32 GMT
Created:	2020-12-12 22:59:32 GMT
Changed:	2020-12-11 20:06:54 GMT
MD5:	b63c7da3692fa60668c8bb2dd926836c
SHA-256:	c37a678f44cd8b503c8082b1343b5f557fa397f139d8a61a4f0db206f6e39a87
Hash Lookup Results:	UNKNOWN
Internal ID:	790

Figure 31: Metadata for "Work.Now!.zip" File

7.1.3 Document 3 Summary – “M.Q Database.zip”

Once we got the password to the M.Q Database.zip file, we were able to access the file. We discovered the file in figure 32 below, which shows a synopsis of the duck leader “Malcom Quaker”. This file is not readily available for any user of the computer

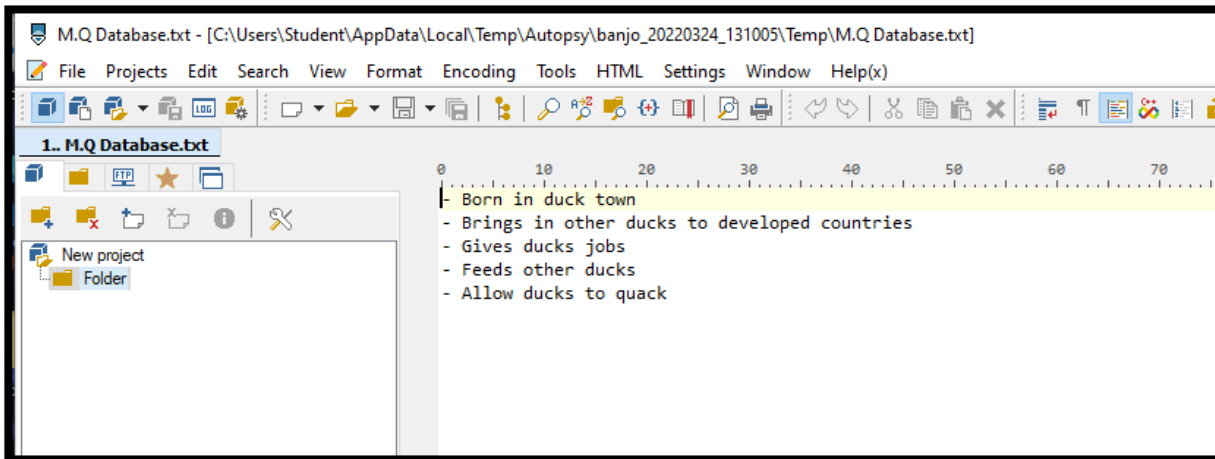


Figure 32: File Found in the "M.Q Database.txt" Zipped File

Metadata	
Name:	/img_Coursework Part 3 - Operation Banjo.E01/Locked/Cream Quackers/M.Q Database.zip
Type:	File System
MIME Type:	application/zip
Size:	325
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2020-12-08 01:29:40 GMT
Accessed:	2020-12-12 22:59:31 GMT
Created:	2020-12-12 22:59:31 GMT
Changed:	2020-12-09 20:41:46 GMT
MD5:	dd746d1a423e62577cba8b6c9eeb7a1d
SHA-256:	569c21d16244c64d0fe7ce6efefb88bab07008d0cc301fad62f4d0e1789ff81b
Hash Lookup Results:	UNKNOWN
Internal ID:	371

Figure 33: The MetaData for M.Q Database.zip

7.1.4 Document 4 Summary – "Zombies.docx"

Having accessed the zombies.docx file using "93116" as the password, we found a text file containing a link. However, we suspected that it may contain additional information which was disguised because when we checked to see what the word count of the file was, we got the value 281 as shown in figure 34 below. Hence, we highlighted the whole document, changed the theme of the text from white to red and discovered the encrypted text in figure 35 below. Using an online tool called "online-toolz.com", we were able to decrypt the text as shown in figure 36 below. The decrypted text shows that the blackout brigade had planned to meet and kill the ducks on Friday the 11th of December. This file is not readily available for any user of the computer.

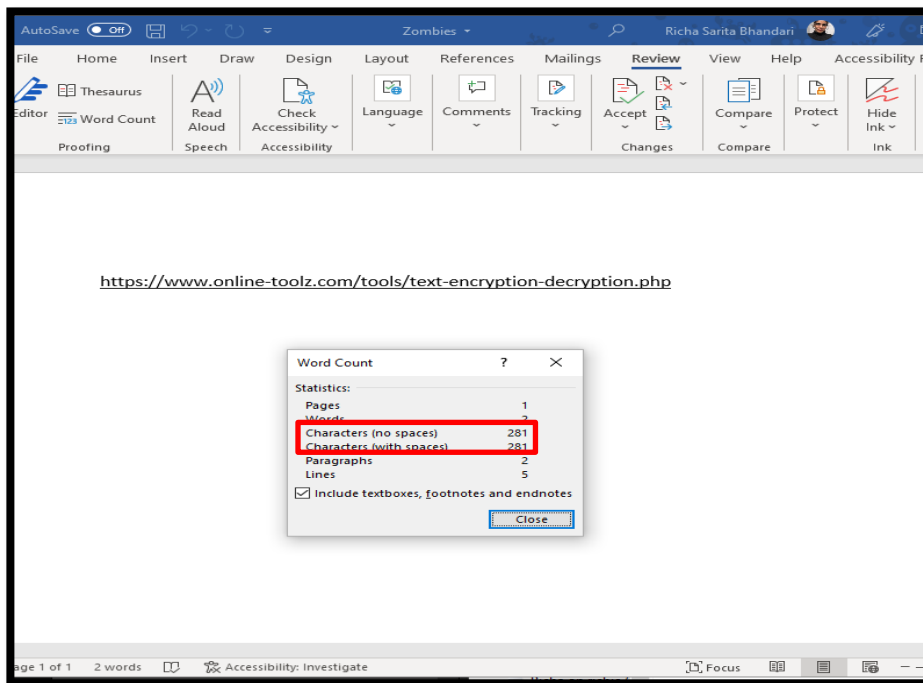


Figure 34: Word Count Showing 281 Characters

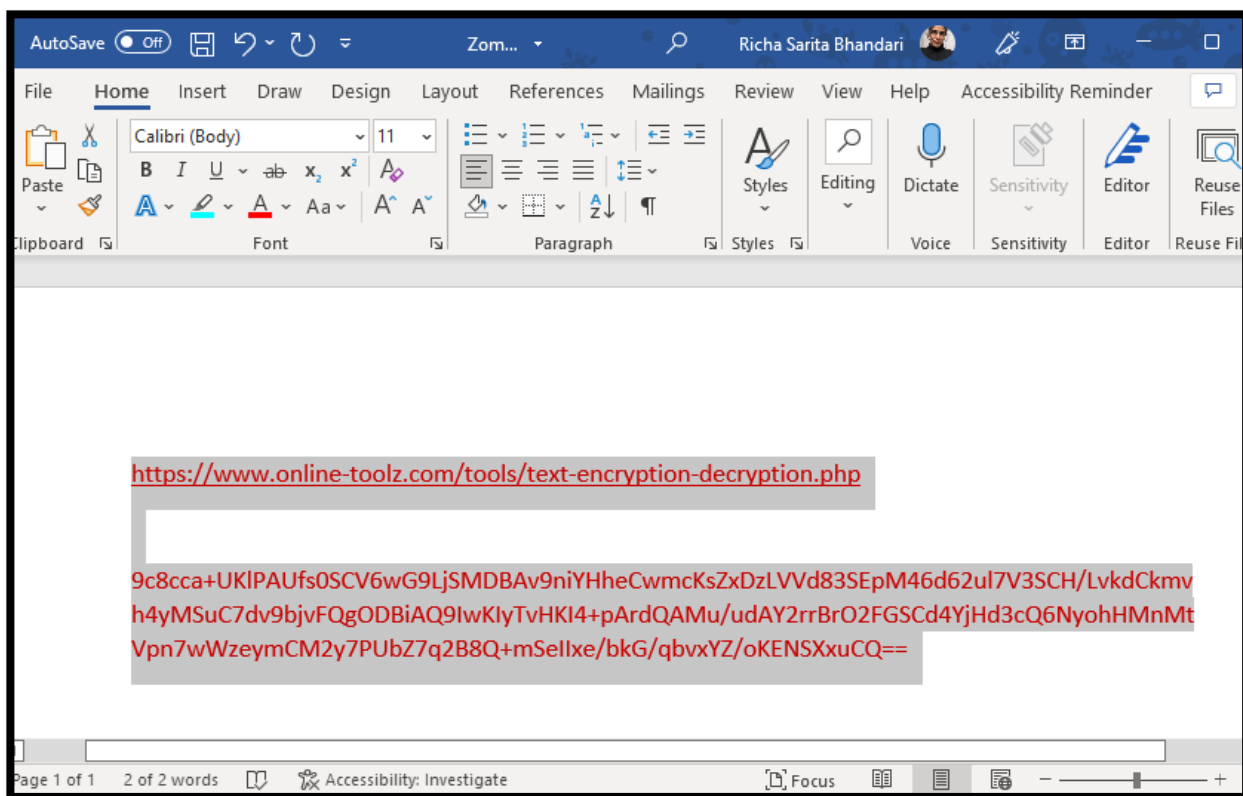


Figure 35: Encrypted Text Discovered

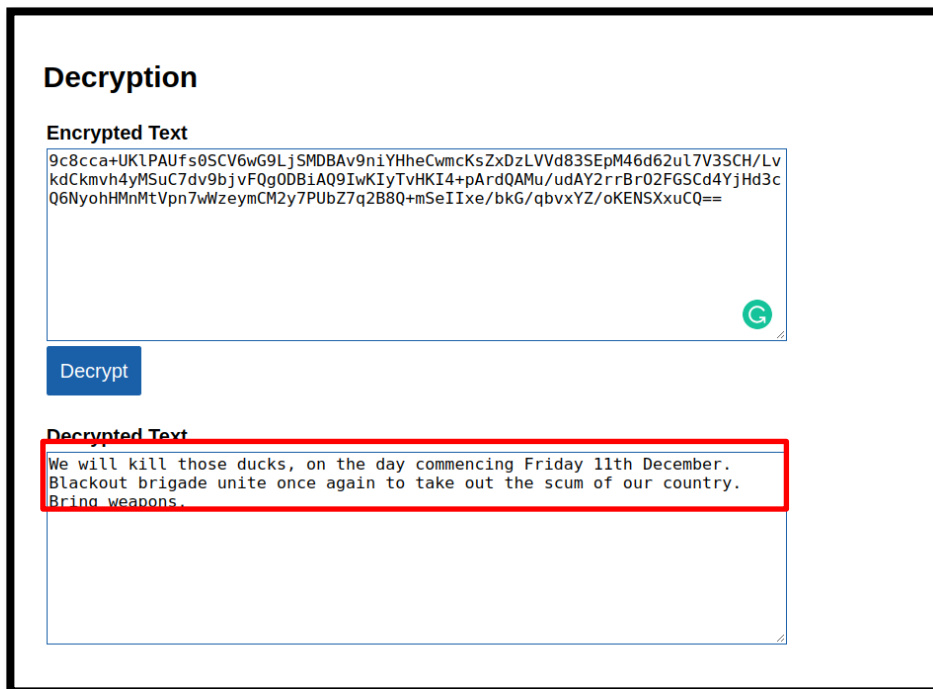


Figure 36: The "online-toolz.com" used to Decrypt Text Found

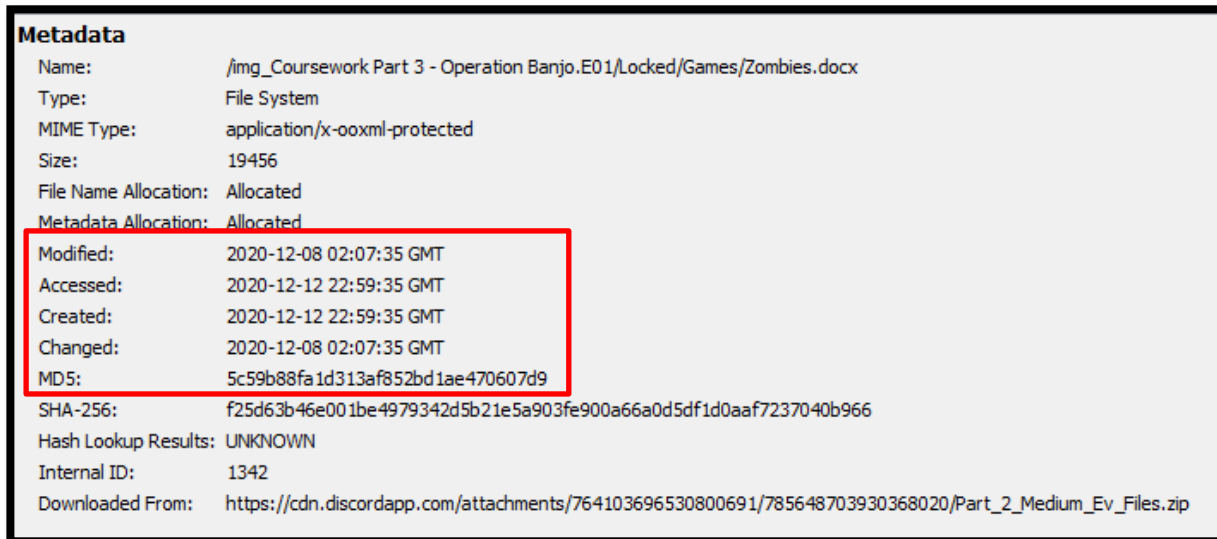


Figure 37: The Metadata for Zombies.docx file

7.1.5 Document 5 Summary - "Eight.docx"

Using the password found, the "Eight.docx" file was accessed and the image in figure 38 below was found. This image clearly outlines the formation of the blackout brigade for the operation banjo. This file is not readily available to any user of the computer.

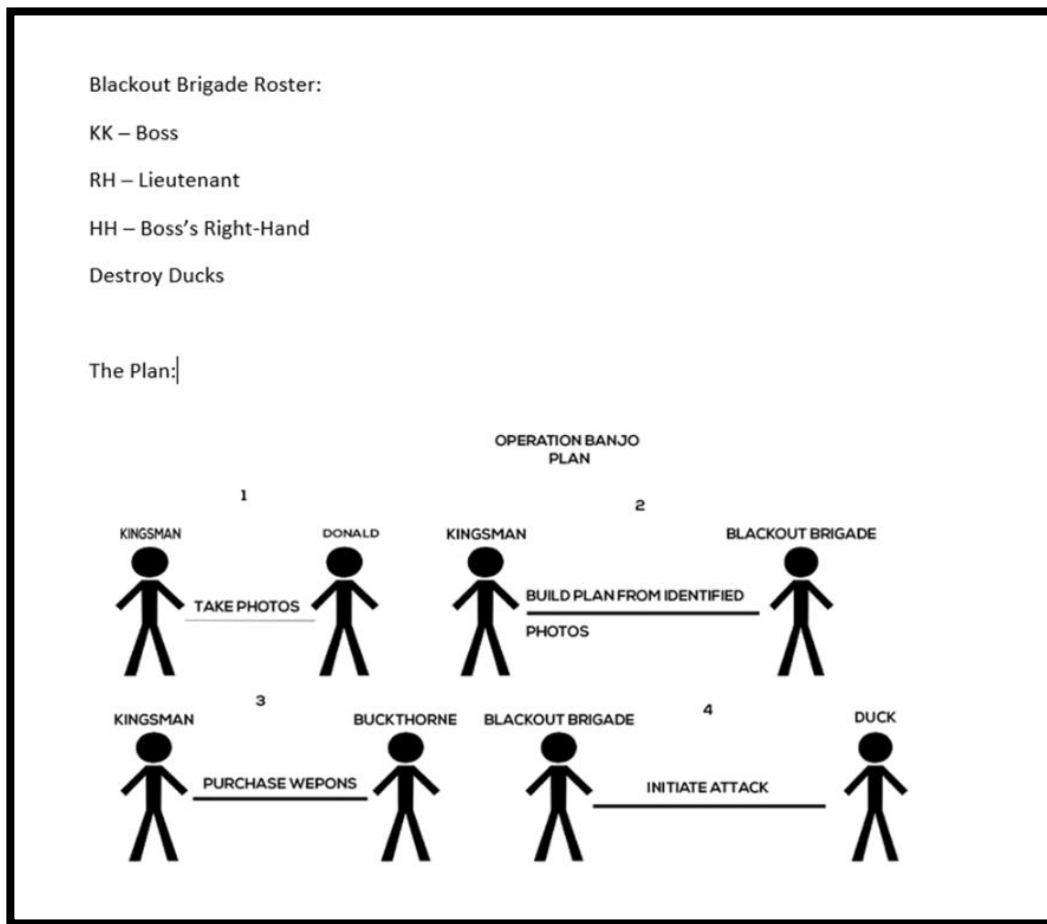


Figure 38: Image Found in the "Eight.docx" File

Metadata	
Name:	/img_Coursework Part 3 - Operation Banjo.E01/Locked/main j/pokemon/Eight.docx
Type:	File System
MIME Type:	application/x-ooxml-protected
Size:	56320
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2020-12-02 16:37:50 GMT
Accessed:	2020-12-12 22:59:35 GMT
Created:	2020-12-12 22:59:35 GMT
Changed:	2020-12-12 22:18:06 GMT
MD5:	4e4cf789aa669749483691f722b94e36
SHA-256:	ca656ad1bb95392b381ec8ea08ab0ec84fb35f3b7af0d62f503ebc09569559ca
Hash Lookup Results:	UNKNOWN
Internal ID:	1478
Downloaded From:	https://cdn.discordapp.com/attachments/764103696530800691/783734211605430272/Part_2_Evidence_Files.zip

Figure 39: The Metadata for the "Eight.docx" File

7.1.6 Document 6 Summary - “Donalds.zip”

Upon accessing the “donalds.zip” file using the password “banjo123”, the text shown in figure 40 below was found. It contains a text requesting intel on the king of all ducks (Mr. Quacker). This file is not readily available for any user of the computer.

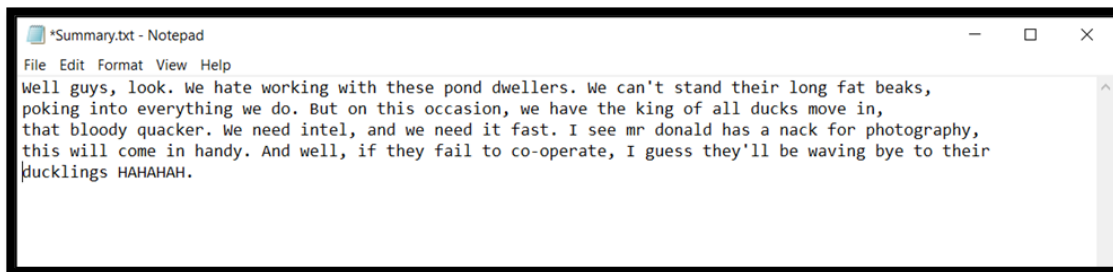


Figure 40: Text Found Upon Opening the "Donalds.zip" File

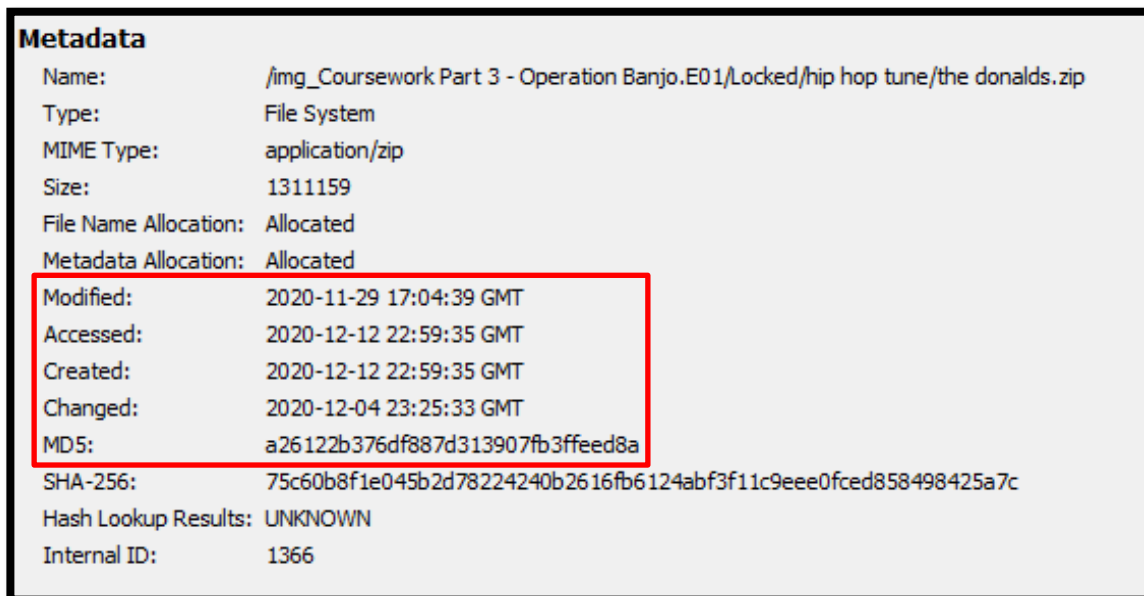
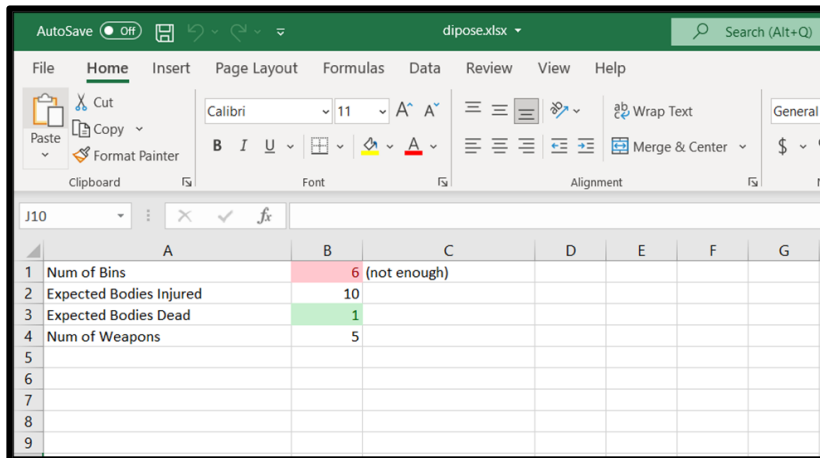


Figure 41: The Metadata for the "Donalds.zip" File

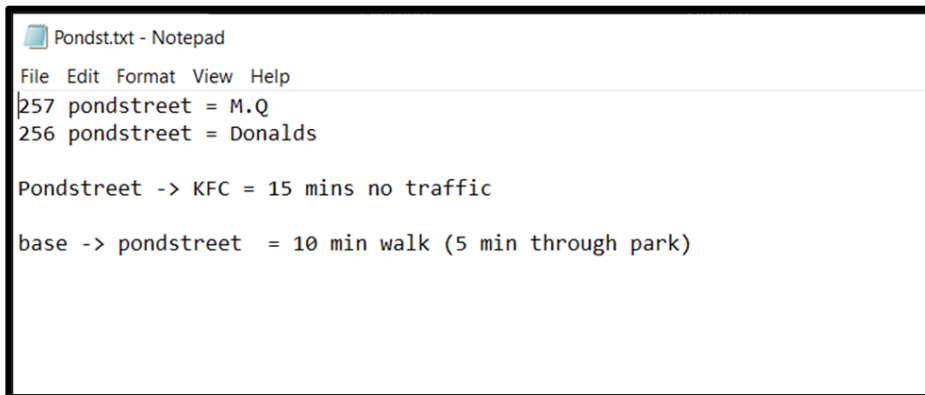
7.1.7 Document 7 Summary - “Stuff.zip”

Once we had the password to the “Stuff.zip” file, we could unzip the file. Upon opening the file, we found an excel sheet named “dispose.xlsx” and a text file named “ponds.txt”. The content of the excel sheet is shown in figure 42 below. It shows the number of bodies expected to be injured and dead. In addition, we also checked the contents of the text file, Its contents provides the coordinates or location where the blackout brigade members are to meet (see figure 43 below). These files are not readily available to the users of the computer.



	A	B	C	D	E	F	G
1	Num of Bins	6 (not enough)					
2	Expected Bodies Injured	10					
3	Expected Bodies Dead	1					
4	Num of Weapons	5					
5							
6							
7							
8							
9							

Figure 42: The "Dipose.xlsx" File

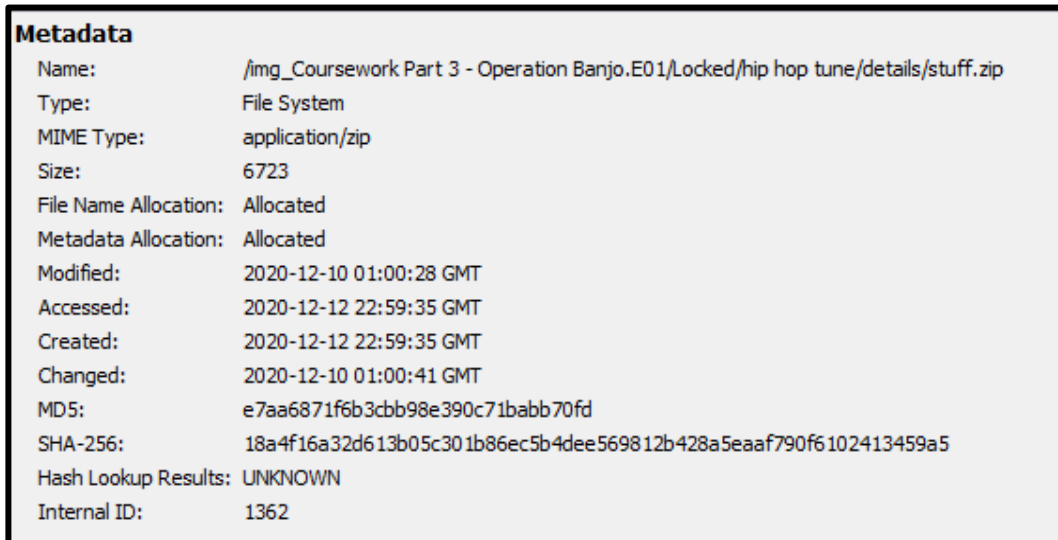


```
Pondst.txt - Notepad
File Edit Format View Help
257 pondstreet = M.Q
256 pondstreet = Donalds

Pondstreet -> KFC = 15 mins no traffic

base -> pondstreet = 10 min walk (5 min through park)
```

Figure 43: The Ponds.txt File



```
Metadata
Name: /img_Coursework Part 3 - Operation Banjo.E01/Locked/hip hop tune/details/stuff.zip
Type: File System
MIME Type: application/zip
Size: 6723
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2020-12-10 01:00:28 GMT
Accessed: 2020-12-12 22:59:35 GMT
Created: 2020-12-12 22:59:35 GMT
Changed: 2020-12-10 01:00:41 GMT
MD5: e7aa6871f6b3cbb98e390c71babb70fd
SHA-256: 18a4f16a32d613b05c301b86ec5b4dee569812b428a5eaaf790f6102413459a5
Hash Lookup Results: UNKNOWN
Internal ID: 1362
```

Figure 44: The Metadata for the "Stuff.zip" File

7.1.8 Document 8 Summary - “Weapon Receipt.zip”

Upon accessing the “weapon receipt.zip” file, using the password “begone”, a screenshot of an email communication between Keith Kingsman and Buckthorn was found. The email communication contained information about the purchase of weapons as shown in figure 45 below. This email communication is not readily available for any user of the computer.

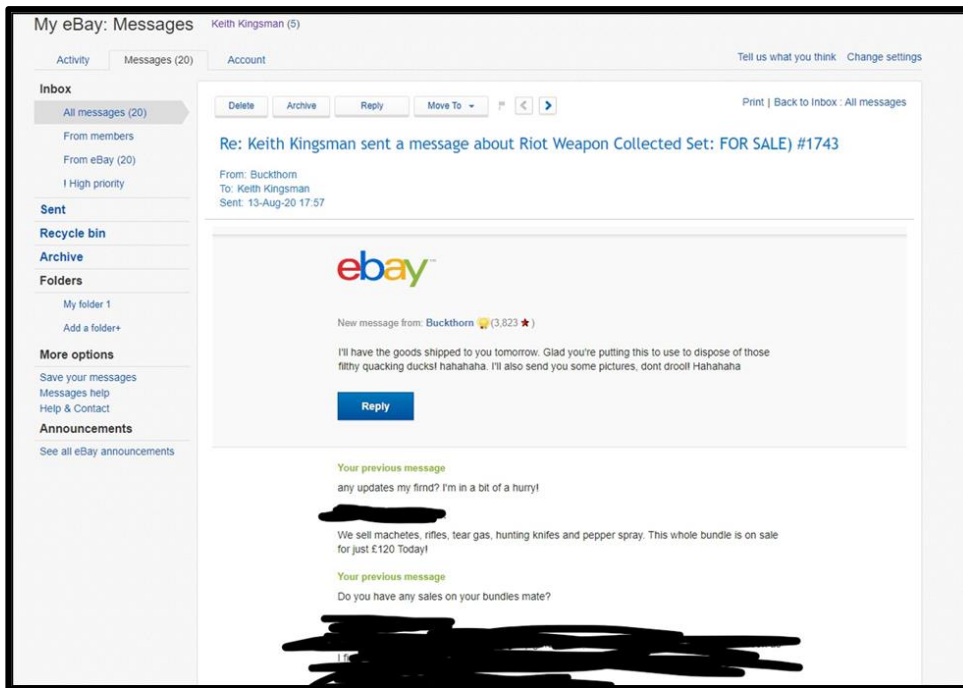


Figure 45: Email Communication Containing Information About the Purchase of Weapons

Metadata	
Name:	/img_Coursework Part 3 - Operation Banjo.E01/Locked/supplies cipher/Weapon Receipt.zip
Type:	File System
MIME Type:	application/zip
Size:	870516
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2020-12-12 16:57:20 GMT
Accessed:	2020-12-12 22:59:35 GMT
Created:	2020-12-12 22:59:35 GMT
Changed:	2020-12-12 16:57:20 GMT
MD5:	208e13be4fc45cf60ebecb1aa479a680
SHA-256:	d340ac5ecb304256df3bb8326874cae5121e44383042408bfe8df4fe13c587cf
Hash Lookup Results:	UNKNOWN
Internal ID:	1567

Figure 46: Metadata of the Weapon Receipt.zip File

7.1.9 Document 9 Summary – “Doc1.docx”

Upon changing the document font style from “MT Extra font” to “Calibri”, we got a readable text, as shown in figure 47 below. The text shows Henry acknowledging receipt of Keith’s invitation to a party scheduled to hold on a Saturday.

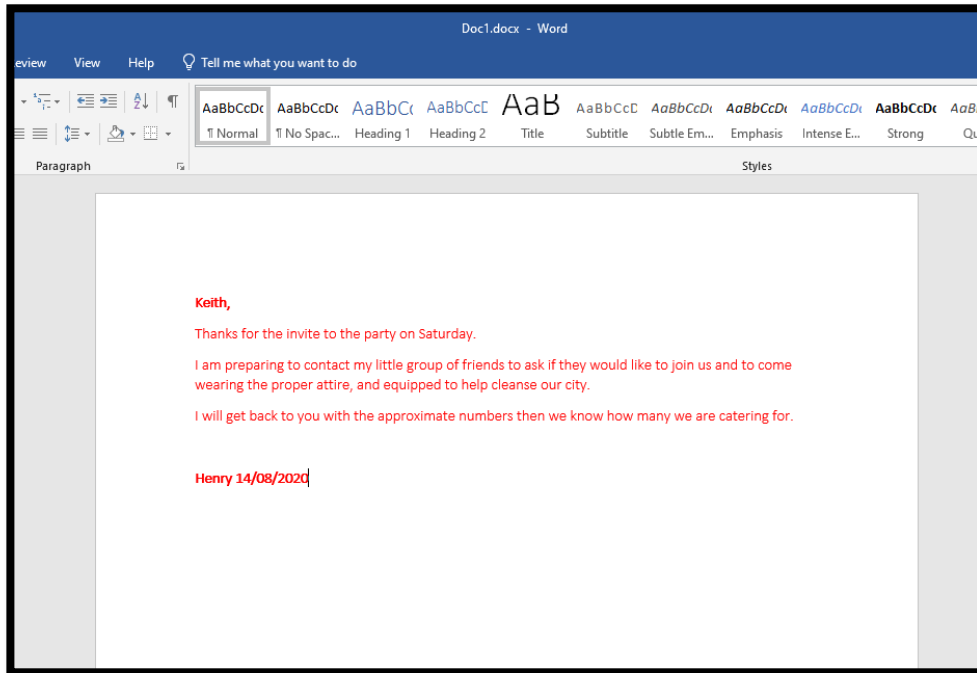


Figure 47: Doc1 After Changing Font Style

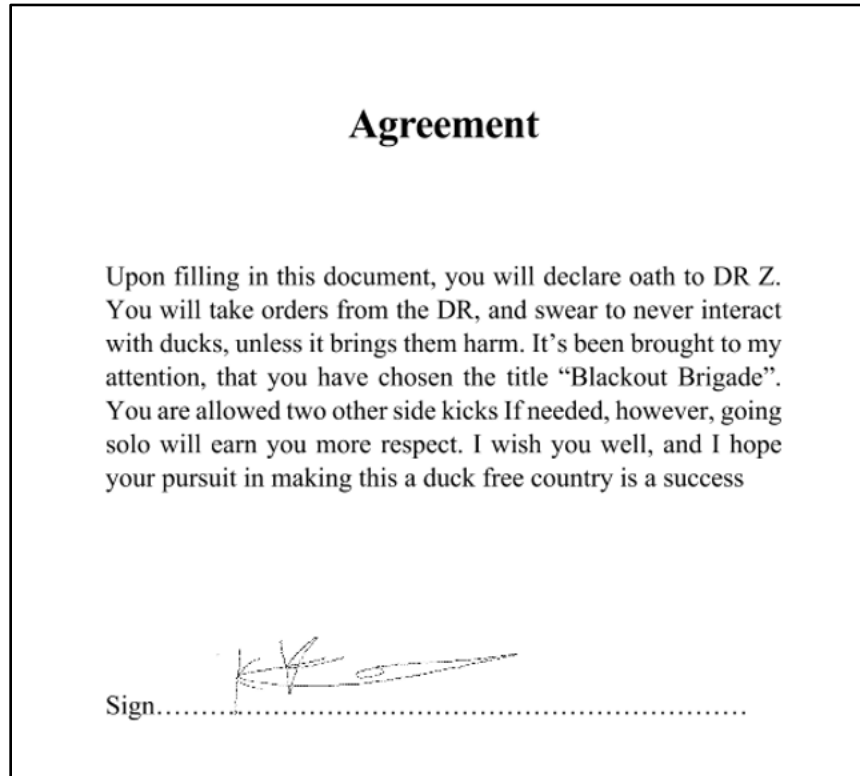
Listing										
/img_Coursework Part 3 - Operation Banjo.E01/Locked/flyers										
10 Results										
Name	S	▲	▼	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
[current folder]					2020-12-12 23:59:33 WAT	2020-12-12 23:59:33 WAT	2020-12-12 23:59:33 WAT	2020-12-12 23:59:32 WAT	56	Allocated
[parent folder]					2020-12-12 23:59:42 WAT	2020-12-12 23:59:42 WAT	2020-12-12 23:59:42 WAT	2020-12-12 23:59:30 WAT	56	Allocated
File Signature Database__DOCX File Signatures_files					2020-12-12 23:59:33 WAT	2020-12-12 23:59:33 WAT	2020-12-12 23:59:33 WAT	2020-12-12 23:59:33 WAT	544	Allocated
VeraCrypt					2020-12-12 23:59:34 WAT	2020-12-12 23:59:34 WAT	2020-12-12 23:59:34 WAT	2020-12-12 23:59:33 WAT	56	Allocated
Decrypt.png				0	2020-11-30 00:52:29 WAT	2020-12-12 23:17:09 WAT	2020-12-12 23:59:32 WAT	2020-12-12 23:59:32 WAT	12730	Allocated
Doc1.docx				1	2020-11-30 00:52:29 WAT	2020-12-05 02:07:46 WAT	2020-12-12 23:59:32 WAT	2020-12-12 23:59:32 WAT	12613	Allocated
Doc1.docx:Zone.Identifier				1	2020-11-30 00:52:29 WAT	2020-12-05 02:07:46 WAT	2020-12-12 23:59:32 WAT	2020-12-12 23:59:32 WAT	122	Allocated
File Signature Database__DOCX File Signatures.html				1	2020-11-30 01:26:00 WAT	2020-12-01 15:15:13 WAT	2020-12-12 23:59:32 WAT	2020-12-12 23:59:32 WAT	23414	Allocated
hex.txt				0	2020-11-30 20:22:13 WAT	2020-12-10 02:14:32 WAT	2020-12-12 23:59:32 WAT	2020-12-12 23:59:32 WAT	33	Allocated
Save Table as CSV										
Metadata										
Name:	/img_Coursework Part 3 - Operation Banjo.E01/Locked/flyers/Doc1.docx									
Type:	File System									
MIME Type:	application/vnd.openxmlformats-officedocument.wordprocessingml.document									
Size:	12613									
File Name Allocation:	Allocated									
Metadata Allocation:	Allocated									
Modified:	2020-11-30 00:52:29 WAT									
Accessed:	2020-12-12 23:59:32 WAT									
Created:	2020-12-12 23:59:32 WAT									
Changed:	2020-12-05 02:07:46 WAT									
MD5:	a3f423d7eb3bbc8941bb79f5eab6b7fa									
SHA-256:	8767334671472b9f195472a0f7c7bdc4de8bec3f801a47d19f8648db0b4207f									
Hash Lookup Results:	UNKNOWN									
Internal ID:	827									
Downloaded From:	https://cdn.discordapp.com/attachments/764602687496781855/782755387597520926/Doc1.docx									

Figure 48: Metadata for the Doc1.docx File

CONFIDENTIAL

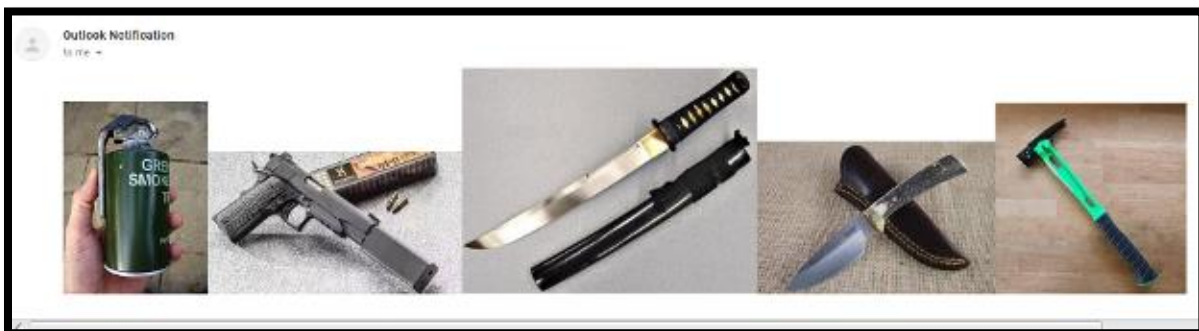
7.2 Pertinent Images Summary

7.2.1 Image 1 Summary – Agreement



The screenshot shows an agreement signed by Keith Kingsman whose aim is to bring harm to the ducks. This screenshot is easily accessible to any user of the computer.

7.2.2 Image 2 Summary – Weapons



This is a screenshot of the various weapons intended to be purchased by Keith Kingsman. This screenshot is easily accessible to any user of the computer.

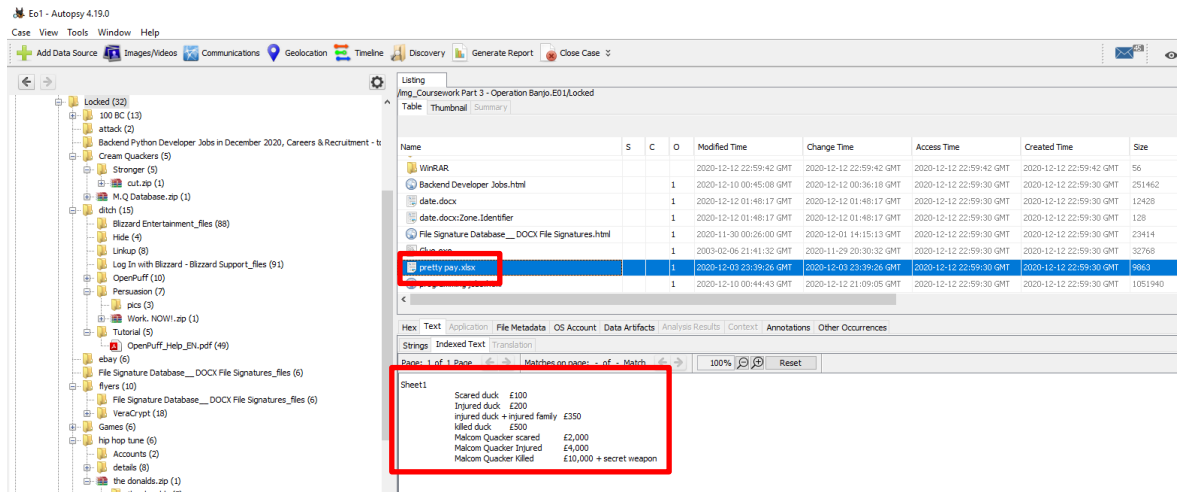
CONFIDENTIAL

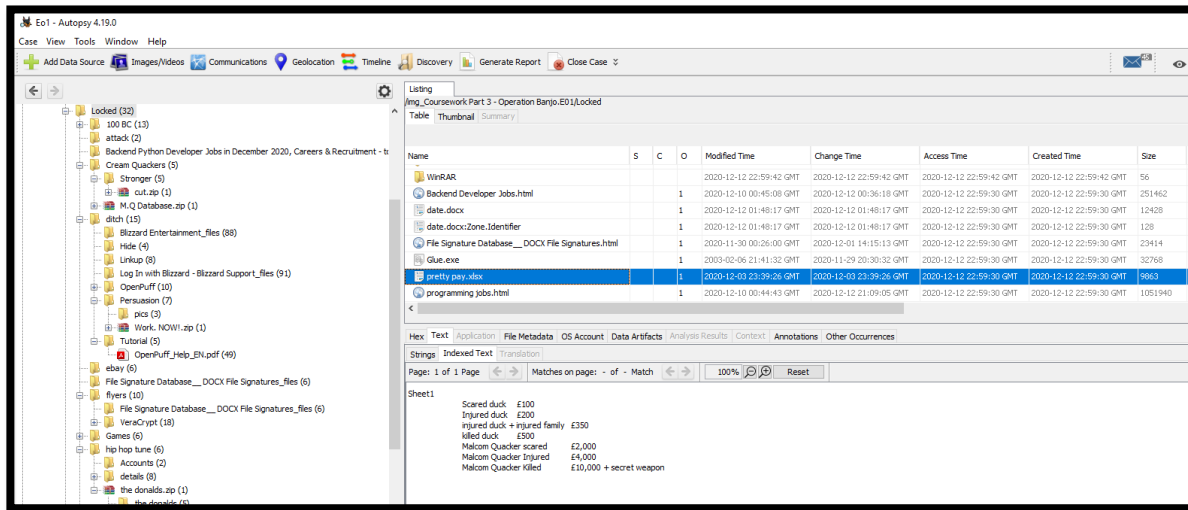
7.2.3 Image 3 Summary – comrades.txt



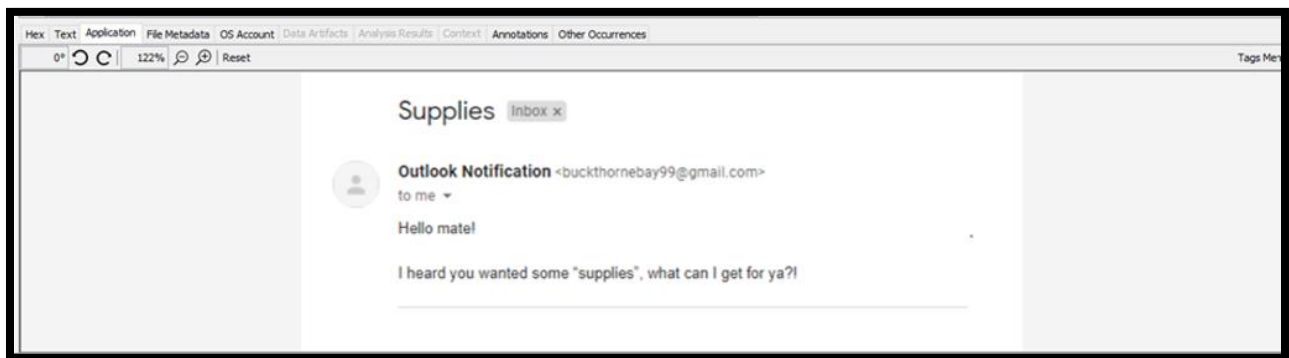
The screenshot above shows a draft message sent to all members of the “blackout brigade” detailing a new task assigned to them. This screenshot is easily accessible to any user of the computer.

7.2.4 Image 4 Summary – Pretty pay.xlsx



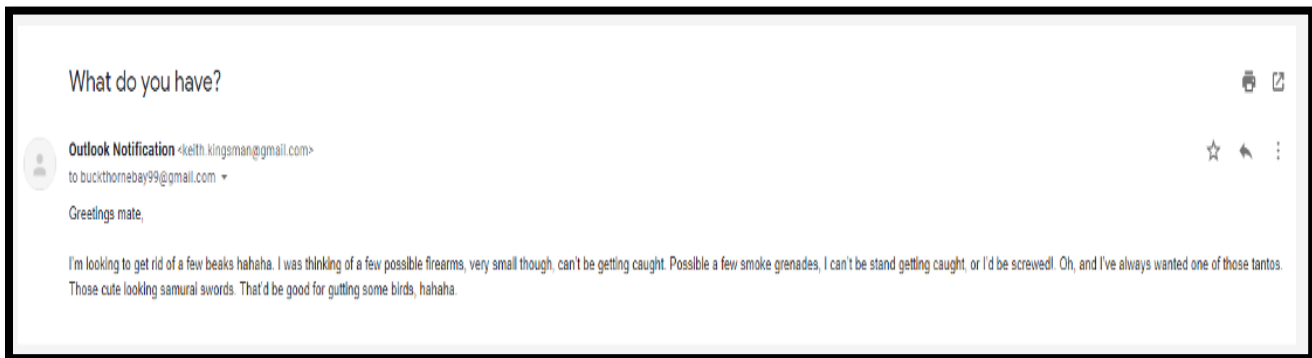


7.2.5 Image 5 Summary – Supplied.eml



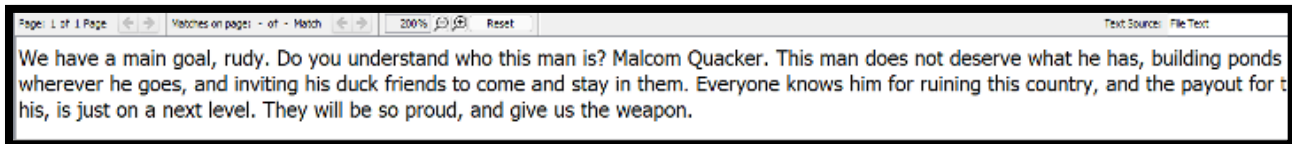
The screenshot above shows an email communication between Buckthorn and Keith Kingsman. Keith Kingsman is actively looking to purchase some supplies, possibly weapons. This email communication is easily accessible to any user using the computer.

7.2.6 Image 6 Summary – What do you have_.eml



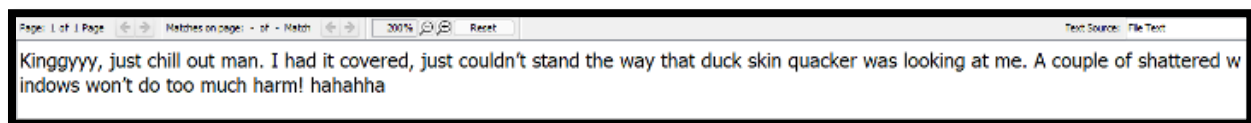
The screenshot above shows another email communication between Buckthorn and Keith Kingsman. In the email communication, Keith Kingsman is seen requesting for a few firearms. This email communication is easily accessible to any user using the computer.

7.2.7 Image 7 Summary – are you mental_.eml



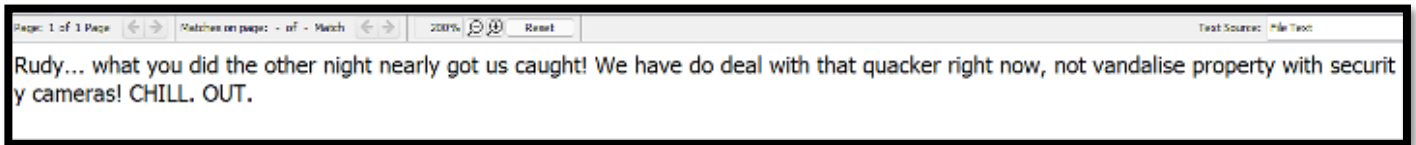
The screenshot above shows an email communication between Keith and Rudy. In this email, Keith explains to Rudy who Mr. Malcom Quacker is. This email communication is easily accessible to any user using the computer.

7.2.8 Image 8 Summary – chill out.eml



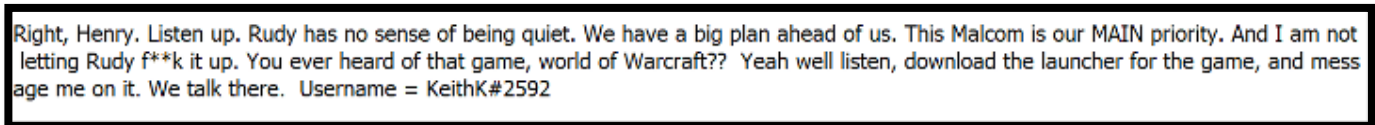
The screenshot above shows yet another email communication between Rudy Hess and Keith Kingsman. Rudy sends an email to Keith assuring him that he had everything under control even though he was violent. This email is not accessible to any user of the computer.

7.2.9 Image 9 Summary – STOP.eml



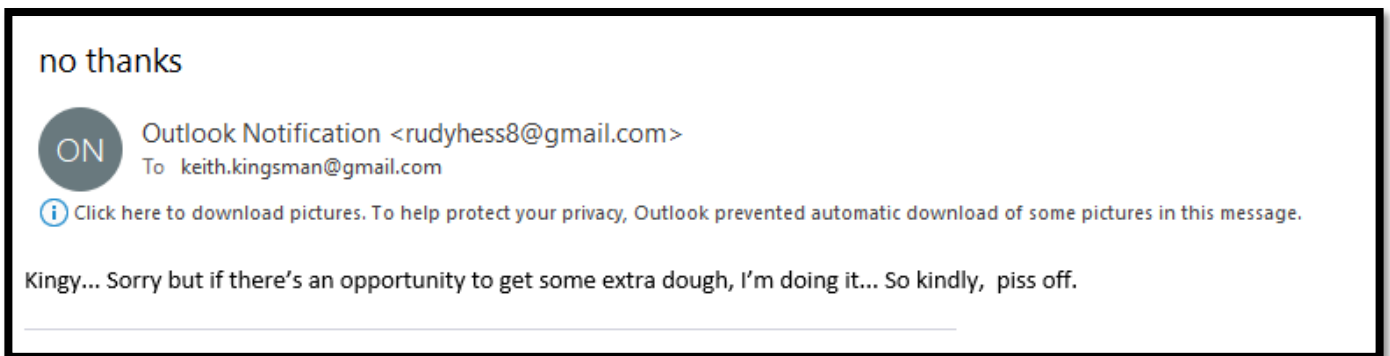
The screenshot above shows an email communication between Keith Kingsman and Rudy Hess. In the email, we see Keith telling Rudy off. It appears Rudy had acted in a way displeasing the blackout brigade. This email communication is easily accessible by any user of the computer.

7.2.10 Image 10 Summary – enough is enough!.eml



The screenshot above shows an email communication between Keith Kingsman and Henry Himler. In the email communication, Keith communicates the need for Rudy to be excluded from operation banjo because they fear he may let the cat out of the bag. They intend to use another platform for their communication and planning. This email communication is easily accessible to any user using the computer.

7.2.11 Image 11 Summary – no thanks.eml



The screenshot above shows an email communication between Rudy Hess and Keith Kingsman. This is communication, it appears that Rudy is disgruntled. This email communication is easily accessible to any user using the computer.

8. CONCLUSION

In the process of forensic data analysis of the Operations Banjo file with the tools specified in section 4.2 of this report, we were able to present evidence of planned attack in the forms of email communications and other kinds of writings, picture of crime-related objects, electronic files and other artefacts. Each file has metadata information which highlights details about the date the file was created, date of any modification and accessed date, and the hash value of the file which maintains the integrity of the file.

Some documents that were decrypted and some other corroborated documentations have timelines of communications and files created in the process of the planned attack. It covers the purchase and delivery of weapons, evidence of payment receipts for the assault weapons purchased, email addresses involved in the communication were identified and some gang-related homicide information. For instance, there is information on some expected number of casualties to get rid of all ducks from the city.

We have been able to present this digital evidence in a manner that preserves the probative value of the evidence and to assure its admissibility in the court. These will provide litigation support that will enable the legal team to establish and prosecute Keith Kingsman and his accomplice if found liable.

Appendix A

Complete the declaration below

This version applies from 3rd April 2019

I (**Abimbola Omoshola, Richa Sarita Bhandari, Lois Amarachi Ukaegbu**) DECLARE THAT:

1. I understand that my duty is to help the court to achieve the overriding objective by giving independent assistance by way of objective, unbiased opinion on matters within my expertise, both in preparing reports and giving oral evidence. I understand that this duty overrides any obligation to the party by whom I am engaged or the person who has paid or is liable to pay me. I confirm that I have complied with and will continue to comply with that duty.
2. I confirm that I have not entered into any arrangement where the amount or payment of my fees is in any way dependent on the outcome of the case.
3. I know of no conflict of interest of any kind, other than any which I have disclosed in my report.
4. I do not consider that any interest which I have disclosed affects my suitability as an expert witness on any issues on which I have given evidence.
5. I will advise the party by whom I am instructed if, between the date of my report and the trial, there is any change in circumstances which affect my answers to points 3 and 4 above.
6. I have shown the sources of all information I have used.
7. I have exercised reasonable care and skill in order to be accurate and complete in preparing this report.
8. I have endeavoured to include in my report those matters, of which I have knowledge or of which I have been made aware, that might adversely affect the validity of my opinion. I have clearly stated any qualifications to my opinion.
9. I have not, without forming an independent view, included or excluded anything which has been suggested to me by others including my instructing lawyers.
10. I will notify those instructing me immediately and confirm in writing if for any reason my existing report requires any correction or qualification.
11. I understand that:
 1. my report will form the evidence to be given under oath or affirmation;
 2. the court may at any stage direct a discussion to take place between experts;
 3. the court may direct that, following a discussion between the experts, a statement should be prepared showing those issues which are agreed and those issues which are not agreed, together with the reasons;
 4. I may be required to attend court to be cross-examined on my report by a cross-examiner assisted by an expert.
 5. I am likely to be the subject of public adverse criticism by the judge if the Court concludes that I have not taken reasonable care in trying to meet the standards set out above.
12. I have read Part 19 of the Criminal Procedure rules and I have complied with its requirements.
13. I confirm that I have acted in accordance with the code of practice or conduct for experts of my discipline, namely [identify the code].
14. [For Experts instructed by the Prosecution only] I confirm that I have read guidance contained in a booklet known as Disclosure: Experts' Evidence and Unused Material which details my role and documents my responsibilities, in relation to disclosure as an expert witness. I have followed the

guidance and recognise the continuing nature of my responsibilities of revelation. In accordance with my duties of disclosure, as documented in the guidance booklet, I confirm that:

1. I have complied with my duties to record, retain and reveal material in accordance with the Criminal Procedure and Investigations Act 1996, as amended;
2. I have compiled an Index of all material. I will ensure that the Index is updated in the event I am provided with or generate additional material;
3. in the event my opinion changes on any material issue, I will inform the investigating officer, as soon as reasonably practicable and give reasons.

STATEMENT OF TRUTH

I confirm that the contents of this report are true to the best of my knowledge and belief and that I make this report knowing that, if it is tendered in evidence, I would be liable to prosecution if I have wilfully stated anything which I know to be false or that I do not believe to be true.

Notes on Codes of Practice & Conduce can be found at the following link

<https://www.academyofexperts.org/guidance/experts-declaration/experts-declaration-criminal-proceedings-england-wales>