

Digital Forensics Case Study

Methodical Analysis of network traffic to discover evidence of criminal activity.

Adam Board

CMP416: Advanced Digital Forensics

BSc Ethical Hacking Year 4

2023/2024

Note that Information contained in this document is for educational purposes.

Contents

1	Introduction	1
1.1	Aim of Investigation	1
1.2	Methodology.....	1
1.3	Tools Used.....	3
2	Network Data and Evidence Analysis.....	4
2.1	Capture 1.....	4
2.1.1	PCAP Traffic Analysis.....	4
2.1.2	Evidence analysis	5
2.2	Capture 2.....	8
2.2.1	PCAP Traffic Analysis.....	8
2.2.2	Evidence analysis	9
2.3	Capture 3.....	12
2.3.1	PCAP Traffic Analysis.....	12
2.3.2	Evidence analysis	12
3	Discussion.....	15
3.1	Critical Evaluation	15
3.1.1	Capture 1.....	15
3.1.2	Capture 2.....	15
3.1.3	Capture 3.....	15
3.2	Reflection	15
	References	17
	Appendices.....	19
	Appendix A – Decoded Base64 Files	19
3.2.1	BillOfRights.txt	19
3.2.2	GoT Spoilers.docx.....	31
3.2.3	PiD.docx	32
3.2.4	North Korea.docx	32
3.2.5	North Korea.docx – English.....	33
3.2.6	Track 10.docx	33
3.2.7	Chess Rules 1.docx	38
3.2.8	Chess Rules 2.docx	39

3.2.9	Chess Rules 3.docx	39
3.2.10	Chess Rules 4.docx	40
3.2.11	Chess Rules 5.docx	40
3.2.12	Chess Rules 6.docx	43
3.2.13	Chess Rules 7.docx	44
Appendix B – Images Found.....		45
	NK.jpg.....	45
	NorthKorea.jpeg.....	45
Appendix C – scripts found		45
	broken.py	45

1 INTRODUCTION

1.1 AIM OF INVESTIGATION

The analyst, working alongside a health regulatory agency, was aiming to investigate the captured network traffic related to an international drug trafficking case. The analyst was provided three distinct Packet Capture (PCAP) files which contained network traffic from parties of interest. This investigation was conducted following a methodology to ensure that all three PCAP files were analysed thoroughly. This ensures that the investigation can be repeated by another individual with the required knowledge and materials if necessary.

1.2 METHODOLOGY

The methodology for this investigation was to examine the contents of the PCAP files to locate packets containing potential evidence. If potential evidence was found, it was extracted to conduct a further analysis using relevant and appropriate tools. This was based on the final two stages of the OSCAR methodology. The health regulatory agency collected the files and came up with a strategy for what evidence should be found, leaving the only required stages of the methodology to be analysis and reporting.

To prevent evidence tampering and data loss, the three PCAP files were copied and hashed using the SHA1 algorithm. The SHA1 generation can be seen in figure 1.

```

(kali㉿kali)-[~/DFAssessment/pcaps0rg]
$ ls
'Capture 1.pcap'  Capture1.pcap.sha1  'Capture 2.pcap'  'Capture 3.pcap'

(kali㉿kali)-[~/DFAssessment/pcaps0rg]
$ rm Capture1.pcap.sha1

(kali㉿kali)-[~/DFAssessment/pcaps0rg]
$ sha1sum Capture\ 1.pcap > Capture1.pcap.sha1

(kali㉿kali)-[~/DFAssessment/pcaps0rg]
$ sha1sum Capture\ 2.pcap > Capture2.pcap.sha1

(kali㉿kali)-[~/DFAssessment/pcaps0rg]
$ sha1sum Capture\ 3.pcap > Capture3.pcap.sha1

(kali㉿kali)-[~/DFAssessment/pcaps0rg]
$ ls
'Capture 1.pcap'  Capture1.pcap.sha1  'Capture 2.pcap'  Capture2.pcap.sha1  'Capture 3.pcap'  Capture3.pcap.sha1

(kali㉿kali)-[~/DFAssessment/pcaps0rg]
$ cat Capture1.pcap.sha1
5af73c8a3cf1076ffb7b07dcaa6f020f46890a17  Capture 1.pcap

(kali㉿kali)-[~/DFAssessment/pcaps0rg]
$ cat Capture2.pcap.sha1
c6c20ddb6e59c0c9c622f251c470aad145f7c60d  Capture 2.pcap

(kali㉿kali)-[~/DFAssessment/pcaps0rg]
$ cat Capture3.pcap.sha1
1e4c82c0c037c63139ab33e1658f66b1c379cb56  Capture 3.pcap

(kali㉿kali)-[~/DFAssessment/pcaps0rg]
$ ls ..
pcapsCopy  pcaps0rg

(kali㉿kali)-[~/DFAssessment/pcaps0rg]
$

```

Figure 1 PCAPs being copied and hashed using sha1sum.

The copied files were used instead of the original files to preserve the integrity of the original files. This also allows for a hash to be generated throughout the investigation to confirm the copies have not been tampered with. Should the copied version become corrupted or accidentally tampered with, the original files can be copied again to continue the investigation.

This same process of creating copies and generating hashes is continued to be used for any evidence that has been extracted from the captures to ensure their integrity before and after analysis.

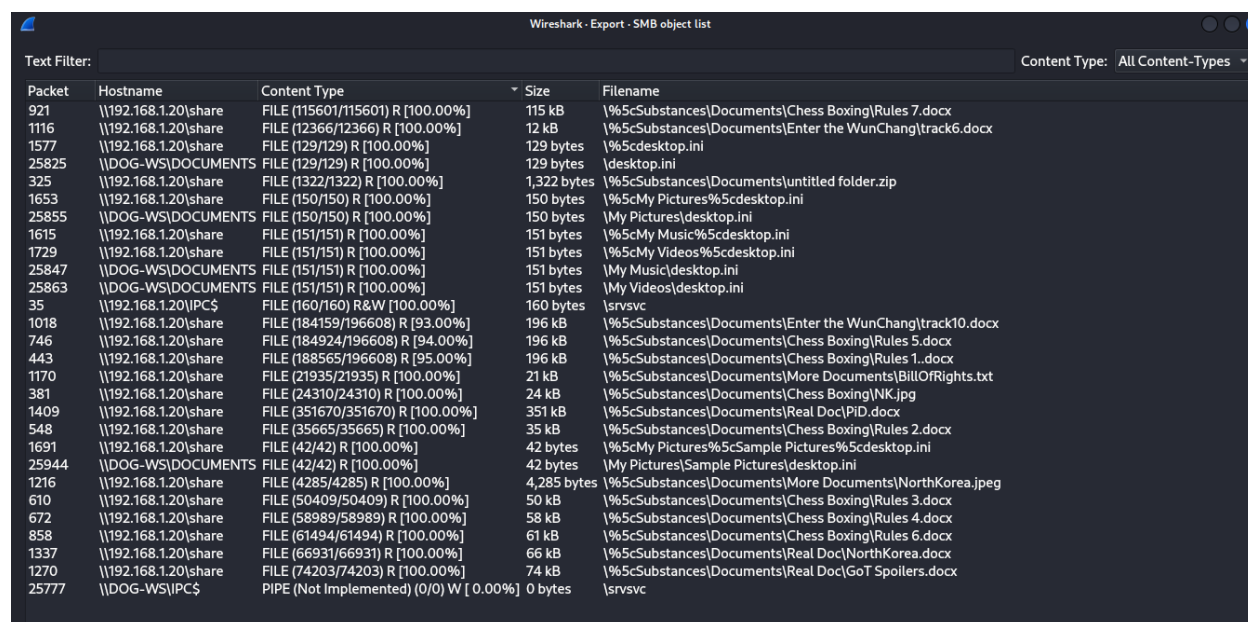
1.3 TOOLS USED

The Following table contains a list of tools used throughout the investigation with a brief description for each tool.

Table 1 List of tools for investigation with brief description

Tool Name	Description
Kali Linux (Kali Linux, 2018)	Kali Linux is an Operating System with various red-teaming and digital forensics tools built-in which can aid in the investigation
Sha1sum (Man7, 2014)	Used to create a hash of each file to determine the integrity of the files throughout the investigation
Wireshark (Wireshark, 2021)	Used to investigate the packets inside of the PCAP files. Includes features such as filtering and object extraction. This improves the efficiency of the investigation.
Cyberchef (GCHQ, 2023)	Web-based data analysis and decoding tool
SilentEye (achorein, 2010)	Software used for steganography
Binwalk (Ubuntu, 2014)	Command line tool used for analysing binary files for files that are embedded as other types of files, including executable code.
Identify (ImageMagick, 2023)	A software program that can analyse image files found and output information such as specifications of images, formatting, and if a file is complete or incomplete.
Exiftools (Harvey, 2023)	Open-source software program for reading, writing, and manipulating metadata of image, audio, video and PDF.
Google Earth (Google, 2023)	Google Earth allows for a 3D viewpoint of the earth. A feature which aided in the investigation was the ability to insert Latitude and Longitude points to pinpoint a location on the Earth.

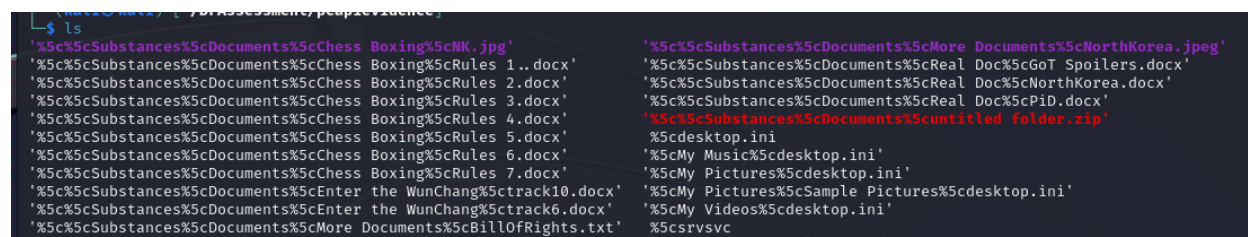
Using Wireshark's "export SMB objects" feature allowed the investigator to export any SMB objects from the PCAP file for further investigation. To maintain the integrity of the extracted objects, they were placed in a "read-only" folder to ensure the files cannot be tampered with. The list of extractable objects can be seen in Figure 5.



Packet	Hostname	Content Type	Size	Filename
921	\\192.168.1.20\share	FILE (115601/115601) R [100.00%]	115 kB	%5cSubstances\Documents\Chess Boxing\Rules 7.docx
1116	\\192.168.1.20\share	FILE (12366/12366) R [100.00%]	12 kB	%5cSubstances\Documents\Enter the WunChang\track6.docx
1577	\\192.168.1.20\share	FILE (129/129) R [100.00%]	129 bytes	%5cdesktop.ini
25825	\\DOG-WS\DOCUMENTS	FILE (129/129) R [100.00%]	129 bytes	\desktop.ini
325	\\192.168.1.20\share	FILE (1322/1322) R [100.00%]	1,322 bytes	%5cSubstances\Documents\untitled folder.zip
1653	\\192.168.1.20\share	FILE (150/150) R [100.00%]	150 bytes	%5cMy Pictures%5cdesktop.ini
25855	\\DOG-WS\DOCUMENTS	FILE (150/150) R [100.00%]	150 bytes	\My Pictures\desktop.ini
1615	\\192.168.1.20\share	FILE (151/151) R [100.00%]	151 bytes	%5cMy Music%5cdesktop.ini
1729	\\192.168.1.20\share	FILE (151/151) R [100.00%]	151 bytes	%5cMy Videos%5cdesktop.ini
25847	\\DOG-WS\DOCUMENTS	FILE (151/151) R [100.00%]	151 bytes	\My Music\desktop.ini
25863	\\DOG-WS\DOCUMENTS	FILE (151/151) R [100.00%]	151 bytes	\My Videos\desktop.ini
35	\\192.168.1.20\IPC\$	FILE (160/160) R&W [100.00%]	160 bytes	\srvsvc
1018	\\192.168.1.20\share	FILE (184159/196608) R [93.00%]	196 kB	%5cSubstances\Documents\Enter the WunChang\track10.docx
748	\\192.168.1.20\share	FILE (184924/196608) R [94.00%]	196 kB	%5cSubstances\Documents\Chess Boxing\Rules 5.docx
443	\\192.168.1.20\share	FILE (188565/196608) R [95.00%]	196 kB	%5cSubstances\Documents\Chess Boxing\Rules 1.docx
1170	\\192.168.1.20\share	FILE (21935/21935) R [100.00%]	21 kB	%5cSubstances\Documents\More Documents\BillOfRights.txt
381	\\192.168.1.20\share	FILE (24310/24310) R [100.00%]	24 kB	%5cSubstances\Documents\Chess Boxing\NK.jpg
1409	\\192.168.1.20\share	FILE (351670/351670) R [100.00%]	351 kB	%5cSubstances\Documents\Real Doc\PiD.docx
548	\\192.168.1.20\share	FILE (35665/35665) R [100.00%]	35 kB	%5cSubstances\Documents\Chess Boxing\Rules 2.docx
1691	\\192.168.1.20\share	FILE (42/42) R [100.00%]	42 bytes	%5cMy Pictures%5cSample Pictures%5cdesktop.ini
25944	\\DOG-WS\DOCUMENTS	FILE (42/42) R [100.00%]	42 bytes	\My Pictures\Sample Pictures\desktop.ini
1216	\\192.168.1.20\share	FILE (4285/4285) R [100.00%]	4,285 bytes	%5cSubstances\Documents\More Documents\NorthKorea.jpeg
610	\\192.168.1.20\share	FILE (50409/50409) R [100.00%]	50 kB	%5cSubstances\Documents\Chess Boxing\Rules 3.docx
672	\\192.168.1.20\share	FILE (58989/58989) R [100.00%]	58 kB	%5cSubstances\Documents\Chess Boxing\Rules 4.docx
858	\\192.168.1.20\share	FILE (61494/61494) R [100.00%]	61 kB	%5cSubstances\Documents\Chess Boxing\Rules 6.docx
1337	\\192.168.1.20\share	FILE (66931/66931) R [100.00%]	66 kB	%5cSubstances\Documents\Real Doc\NorthKorea.docx
1270	\\192.168.1.20\share	FILE (74203/74203) R [100.00%]	74 kB	%5cSubstances\Documents\Real Doc\GoT Spoilers.docx
25777	\\DOG-WS\IPC\$	PIPE (Not Implemented) (0/0) W [0.00%]	0 bytes	\srvsvc

Figure 4 List of extractable SMB objects.

All but one file had successfully downloaded, and duplicate files had been removed from the directory. The results of this can be seen in Figure 6.



```

ls
'%5c%5cSubstances%5cDocuments%5cChess Boxing%5cNK.jpg'
'%5c%5cSubstances%5cDocuments%5cChess Boxing%5cRules 1..docx'
'%5c%5cSubstances%5cDocuments%5cChess Boxing%5cRules 2.docx'
'%5c%5cSubstances%5cDocuments%5cChess Boxing%5cRules 3.docx'
'%5c%5cSubstances%5cDocuments%5cChess Boxing%5cRules 4.docx'
'%5c%5cSubstances%5cDocuments%5cChess Boxing%5cRules 5.docx'
'%5c%5cSubstances%5cDocuments%5cChess Boxing%5cRules 6.docx'
'%5c%5cSubstances%5cDocuments%5cChess Boxing%5cRules 7.docx'
'%5c%5cSubstances%5cDocuments%5cEnter the WunChang%5ctrack10.docx'
'%5c%5cSubstances%5cDocuments%5cEnter the WunChang%5ctrack6.docx'
'%5c%5cSubstances%5cDocuments%5cMore Documents%5cBillOfRights.txt'
'%5c%5cSubstances%5cDocuments%5cMore Documents%5cNorthKorea.jpeg'
'%5c%5cSubstances%5cDocuments%5cReal Doc%5cGoT Spoilers.docx'
'%5c%5cSubstances%5cDocuments%5cReal Doc%5cNorthKorea.docx'
'%5c%5cSubstances%5cDocuments%5cReal Doc%5cPiD.docx'
'%5c%5cSubstances%5cDocuments%5cuntitled folder.zip'
%5cdesktop.ini
'%5cMy Music%5cdesktop.ini'
'%5cMy Pictures%5cdesktop.ini'
'%5cMy Pictures%5cSample Pictures%5cdesktop.ini'
'%5cMy Videos%5cdesktop.ini'
%5csrvsvc

```

Figure 5 Cleanup of Evidence to remove duplicates.

2.1.2 Evidence analysis

The ".ini" and "srvsvc" files had no relevant information for the investigation or had a file size of zero which meant these files were not investigated further.

Before investigating the contents of the files, exiftools was used to check the metadata of the docx and images. All the docx files were found to be originally created in 2014 and have been modified in 2023, which is a gap of nine years. This gap could leave the potential that these files may have been tampered at some point in these 9 years. The metadata can be seen in Figure 6.


```

ExifTool Version Number      : 12.67
File Name                    : %5c%5cSubstances%5cDocuments%5cEnter the WunChang%5ctrack6.docx
Directory                   : .
File Size                    : 12 kB
File Modification Date/Time   : 2023:12:09 17:59:55-05:00
File Access Date/Time        : 2023:12:09 18:19:03-05:00
File Inode Change Date/Time   : 2023:12:09 17:59:55-05:00
File Permissions              : -rw-r--r--
File Type                    : DOCX
File Type Extension           : docx
MIME Type                    : application/vnd.openxmlformats-officedocument.wordprocessingml.document
Zip Required Version          : 20
Zip Bit Flag                  : 0x0006
Zip Compression               : Deflated
Zip Modify Date                : 1980:01:01 00:00:00
Zip CRC                       : 0x6cd2a4df
Zip Compressed Size           : 346
Zip Uncompressed Size         : 1312
Zip File Name                  : [Content_Types].xml
Title                        :
Subject                       :
Creator                       : Bryan Schmidt
Keywords                      :
Description                   :
Last Modified By               : Varun Kumar
Revision Number                : 3
Create Date                   : 2014:06:19 17:24:00Z
Modify Date                    : 2023:10:20 18:48:00Z
Template                      : Normal
Total Edit Time                : 1 minute
Pages                         : 1
Words                         : 81
Characters                    : 464
Application                   : Microsoft Office Word
Doc Security                   : None
Lines                         : 3
Paragraphs                    : 1
Scale Crop                    : No
Company                       : lmg security
Links Up To Date              : No
Characters With Spaces         : 544
Shared Doc                     : No
Hyperlinks Changed            : No
App Version                   : 16.0000

```

Figure 6 Metadata of "track6.docx" extracted using exiftools.

Moving on to the contents of the files, multiple docx files contained text which was assumed to be encoded. The text was copied into CyberChef's "magic" operation to determine the encoding method. Immediately, the encoding was identified as Base64 which is easily decoded using CyberChef's "From Base64" operation. The results from "track6.docx" was of note because it contained the suspected record of drugs and the total quantity of each drug on the list. The decoded results from the file, "track6.docx" can be seen in Figure 7.

Sensitive information CR		
Drugs Records CR		
Number	Drug Name	Amount CR
1	Atorvastatin	114509814 CR
2	Levothyroxine	98970640 CR
3	Metformin	92591486 CR
4	Lisinopril	88597017 CR
5	Amlodipine	69786684 CR
6	Metoprolol	66413692 CR
7	Albuterol	61948347 CR
8	Omeprazole	56300064 CR
9	Losartan	54815411 CR
10	Gabapentin	49961066 CR
11	Hydrochlorothiazide	41476098

Figure 7 Track6 docx results record of drugs and the quantity.

Majority of the decoded files provided information that was not relevant to the case, but can be found in Appendix A.

There were two image files of the North Korean flag, “NK.jpg” and “NorthKorea.jpeg”, both files can be seen in Appendix B.

The tool “Binwalk” was used to check for hidden files within the images. Within “NorthKorea.jpeg” a Python script called “broken.py” was found and extracted. This can be seen in Figure 8.

```
(kali@kali)-[~/DFAssessment/pcap1evidence]
$ binwalk -e %5c%5cSubstances%5cDocuments%5cMore\ Documents%5cNorthKorea.jpeg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
3453	0xD7D	Zip archive data, at least v2.0 to extract, name: untitled/
3492	0xDA4	Zip archive data, at least v2.0 to extract, compressed size: 604, uncompressed size: 1397, name: untitled/broken.py
4263	0x10A7	End of Zip archive, footer length: 22

Figure 8 Binwalk results from "NorthKorea.jpeg".

Upon looking at the script, it appeared to contain functions for encoding and decoding. However, in its current state, there are multiple syntax and import errors that would stop this script from functioning properly. The script “broken.py” can be found in Appendix C.

The last file that was of interest was a zip file named “untitled” which contained a reference to “SilentEye”. Researching this revealed “SilentEye” to be a program related to steganography (achorein, 2010). The reference inside of the zip file suggests that the suspect, or an individual related to the suspect used this software. The zip file containing the reference can be seen in Figure 9.

Location: untitled folder/untitled folder/untitled folder 2/untitled folder/untitled folder/			
Name	Size	Type	Date Modified
SilentEye	0 bytes	Folder	19 June 2014, 13:39

Figure 9 Contents of zip file named "untitled folder".

2.2 CAPTURE 2

2.2.1 PCAP Traffic Analysis

The investigator was informed that Capture 2 contains FTP traffic of potential evidence. The traffic was between a suspected gang member and their foreign contact. Based on the last capture packet having a reference to "SilentEye", potential anti-forensic tactics may have been employed to hide evidence.

The capture's network traffic began 14th October 2023 at 01:33 and ended 21st October at 16:08. Since the health regulatory agency suggested there was suspicious FTP traffic, a filter was applied to examine only FTP and FTP-DATA packets. Doing so revealed the user "ftpuser" successfully logged in to an FTP server using the password "starwars" on 21st October 2023 at 16:03 (according to the login successful packet timestamp). The IP address of the suspect was assumed to be 192.168.1.6 because this was the IP address of the "ftpuser" login attempt. The IP address of the server was 192.168.1.20, which along with the previous IP address mentioned, appear to be the same IP addresses as the ones found in Capture 1, therefore making the user likely to be the same individual. There appears to be two additional IP addresses on a completely different IP address range of 172.29.1.x, which are attempting to list a zip file named "sandwich.zip". However, it runs into 500 errors, which are server-side related errors, and times out.

On the 192 IP addresses range, the suspect appeared to be downloading 5 different zip files using the RETR command, this included 3v0ke.zip, c0ll3ct.zip, d3arth.zip, dr0id.zip, and untitled folder.zip. The RETR command is sent out when a user requests to download a copy of a file from a server (Solarwinds, 2019). The FTP and FTP-DATA filter with evidence of the files being downloaded can be seen in Figure 10.

No.	Time	Source	Destination	Protocol	Length	Info
19261	057021.3259	192.168.1.20	192.168.1.6	FTP	105	Response: 200 PORT command successful. Consider using PASV.
19262	057021.3268	192.168.1.6	192.168.1.20	FTP	70	Request: RETR 3v0ke.zip
19266	057021.3275	192.168.1.20	192.168.1.6	FTP	124	Response: 150 Opening BINARY mode data connection for 3v0ke.zip (12847 bytes).
19267	057021.3276	192.168.1.20	192.168.1.6	FTP-D.	7306	FTP Data: 7240 bytes (PORT) (RETR 3v0ke.zip)
19268	057021.3276	192.168.1.20	192.168.1.6	FTP-D.	5473	FTP Data: 5607 bytes (PORT) (RETR 3v0ke.zip)
19275	057021.3288	192.168.1.20	192.168.1.6	FTP	70	Response: 226 Transfer complete.
19285	057027.4469	192.168.1.6	192.168.1.20	FTP	70	Request: PORT 192,168,1,6,126,1
19286	057027.4471	192.168.1.20	192.168.1.6	FTP	105	Response: 200 PORT command successful. Consider using PASV.
19287	057027.4487	192.168.1.6	192.168.1.20	FTP	72	Request: RETR c0ll3ct.zip
19291	057027.4502	192.168.1.20	192.168.1.6	FTP	126	Response: 150 Opening BINARY mode data connection for c0ll3ct.zip (11226 bytes).
19292	057027.4502	192.168.1.20	192.168.1.6	FTP-D.	7306	FTP Data: 7240 bytes (PORT) (RETR c0ll3ct.zip)
19293	057027.4502	192.168.1.20	192.168.1.6	FTP-D.	4052	FTP Data: 3986 bytes (PORT) (RETR c0ll3ct.zip)
19298	057027.4505	192.168.1.20	192.168.1.6	FTP	70	Response: 226 Transfer complete.
19297	057033.8041	192.168.1.6	192.168.1.20	FTP	70	Request: PORT 192,168,1,6,126,2
19300	057033.8043	192.168.1.20	192.168.1.6	FTP	105	Response: 200 PORT command successful. Consider using PASV.
19309	057033.8071	192.168.1.6	192.168.1.20	FTP	71	Request: RETR d3arth.zip
19313	057033.8074	192.168.1.20	192.168.1.6	FTP	124	Response: 150 Opening BINARY mode data connection for d3arth.zip (9160 bytes).
19314	057033.8074	192.168.1.20	192.168.1.6	FTP-D.	7306	FTP Data: 7240 bytes (PORT) (RETR d3arth.zip)
19315	057033.8074	192.168.1.20	192.168.1.6	FTP-D.	1986	FTP Data: 1920 bytes (PORT) (RETR d3arth.zip)
19321	057033.8076	192.168.1.20	192.168.1.6	FTP	70	Response: 226 Transfer complete.
19332	057040.1690	192.168.1.6	192.168.1.20	FTP	70	Request: PORT 192,168,1,6,126,4
19333	057040.1691	192.168.1.20	192.168.1.6	FTP	105	Response: 200 PORT command successful. Consider using PASV.
19334	057040.1720	192.168.1.6	192.168.1.20	FTP	70	Request: RETR dr0id.zip
19338	057040.1723	192.168.1.20	192.168.1.6	FTP	123	Response: 150 Opening BINARY mode data connection for dr0id.zip (8864 bytes).
19339	057040.1724	192.168.1.20	192.168.1.6	FTP-D.	7306	FTP Data: 7240 bytes (PORT) (RETR dr0id.zip)
19340	057040.1724	192.168.1.20	192.168.1.6	FTP-D.	1000	FTP Data: 1624 bytes (PORT) (RETR dr0id.zip)
19346	057040.1726	192.168.1.20	192.168.1.6	FTP	70	Response: 226 Transfer complete.
19351	057042.7967	192.168.1.6	192.168.1.20	FTP	70	Request: PORT 192,168,1,6,126,5
19352	057042.7969	192.168.1.20	192.168.1.6	FTP	105	Response: 200 PORT command successful. Consider using PASV.
19353	057042.7993	192.168.1.6	192.168.1.20	FTP	60	Request: NLST
19357	057042.7997	192.168.1.20	192.168.1.6	FTP	93	Response: 150 Here comes the directory listing.
19358	057042.7997	192.168.1.20	192.168.1.6	FTP-D.	113	FTP Data: 47 bytes (PORT) (NLST)
19361	057042.7999	192.168.1.20	192.168.1.6	FTP	70	Response: 226 Directory send OK.
19368	057046.4722	192.168.1.6	192.168.1.20	FTP	60	Request: QUIT
19369	057046.6073	192.168.1.20	192.168.1.6	FTP	60	Response: 221 Goodbye.
19424	057218.3631	192.168.1.20	192.168.1.6	FTP	74	Response: 220 (vsFTPd 3.0.3)
19425	057218.3640	192.168.1.6	192.168.1.20	FTP	60	Request: OPTS UTF8 OK
19427	057218.3641	192.168.1.20	192.168.1.6	FTP	80	Response: 200 Always in UTF8 mode.
19434	057231.4089	192.168.1.6	192.168.1.20	FTP	68	Request: USER ftpuser
19436	057231.4091	192.168.1.20	192.168.1.6	FTP	88	Response: 331 Please specify the password.
19438	057234.1019	192.168.1.6	192.168.1.20	FTP	69	Request: PASS starwars
19440	057234.1256	192.168.1.20	192.168.1.6	FTP	77	Response: 230 Login successful.
19443	057237.4703	192.168.1.6	192.168.1.20	FTP	65	Request: CWD files
19445	057237.4704	192.168.1.20	192.168.1.6	FTP	91	Response: 250 Directory successfully changed.
19448	057240.7087	192.168.1.6	192.168.1.20	FTP	79	Request: PORT 192,168,1,6,126,21
19449	057240.7089	192.168.1.20	192.168.1.6	FTP	105	Response: 200 PORT command successful. Consider using PASV.
19450	057240.7844	192.168.1.6	192.168.1.20	FTP	60	Request: NLST
19454	057240.7850	192.168.1.20	192.168.1.6	FTP	93	Response: 150 Here comes the directory listing.
19455	057240.7851	192.168.1.20	192.168.1.6	FTP-D.	134	FTP Data: 68 bytes (PORT) (NLST)

Figure 10 FTP and FTP-DATA filter with evidence of files being downloaded.

Using Wireshark's "export FTP-DATA objects" feature allowed the investigator to export any FTP-DATA objects from the PCAP for further investigation. To maintain the integrity of the extracted objects, they were placed in a "read-only" folder to ensure the files cannot be tampered with. The list of extractable objects can be seen in Figure 11.

Packet	Hostname	Content Type	Size	Filename
19267	192.168.1.20	FTP file	12 kB	3v0ke.zip
19292	192.168.1.20	FTP file	11 kB	c0ll3ct.zip
19314	192.168.1.20	FTP file	9,160 bytes	d3arth.zip
19339	192.168.1.20	FTP file	8,864 bytes	dr0id.zip
19475	192.168.1.20	FTP file	1,322 bytes	untitled folder.zip

Figure 11 List of extractable FTP-DATA objects.

2.2.2 Evidence analysis

After extracting the zip files from the PCAP, a copy of each zip file was made before unzipping them. Once each file had been unzipped, the tree command was run to discover that each folder contained several .jpg images with one-word file names. This can be seen in Figure 12 and 13.

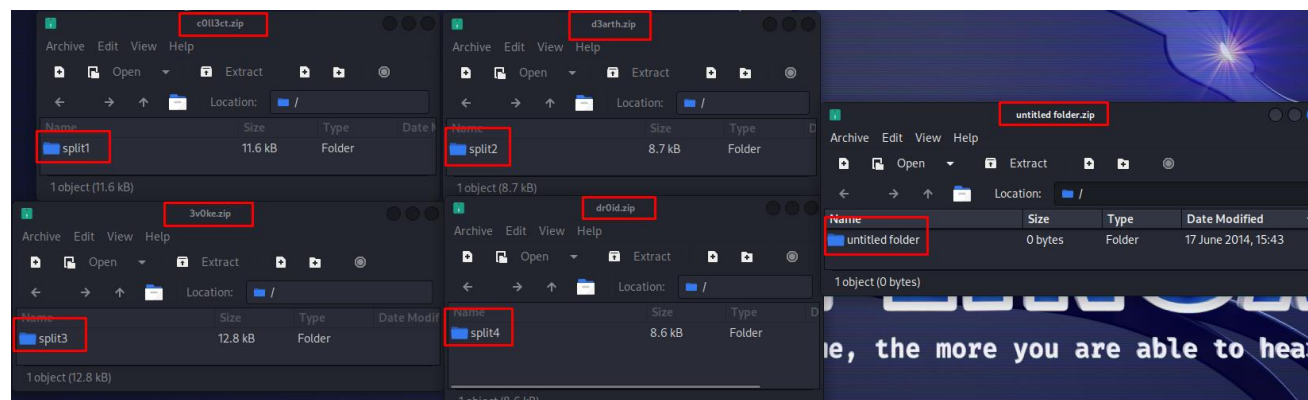


Figure 12 Zip files and their contents.

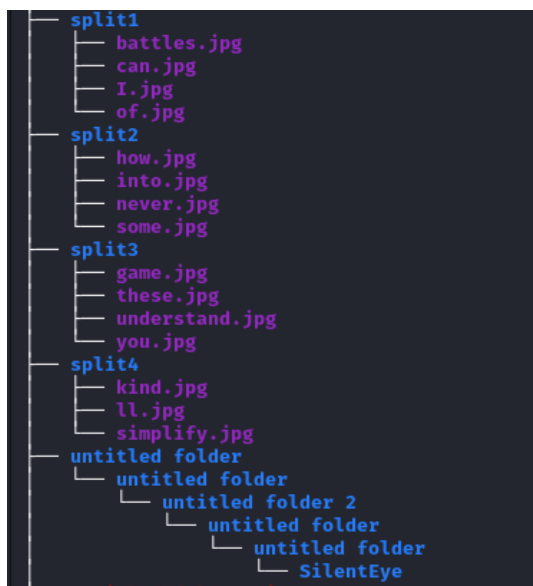


Figure 13 tree command showcasing each of the zip files contents.

The “SilentEye” reference returned in Capture 2 could indicate the suspect had used “SilentEye” in one of the found images. Attempting to open the images revealed that only one image named “l.jpg” on “split1” was capable of opening and the data for the image seemed to be incomplete. The image l.jpg can be seen in Figure 14. Because most of the images were not viewable, they will not be included in an Appendix.

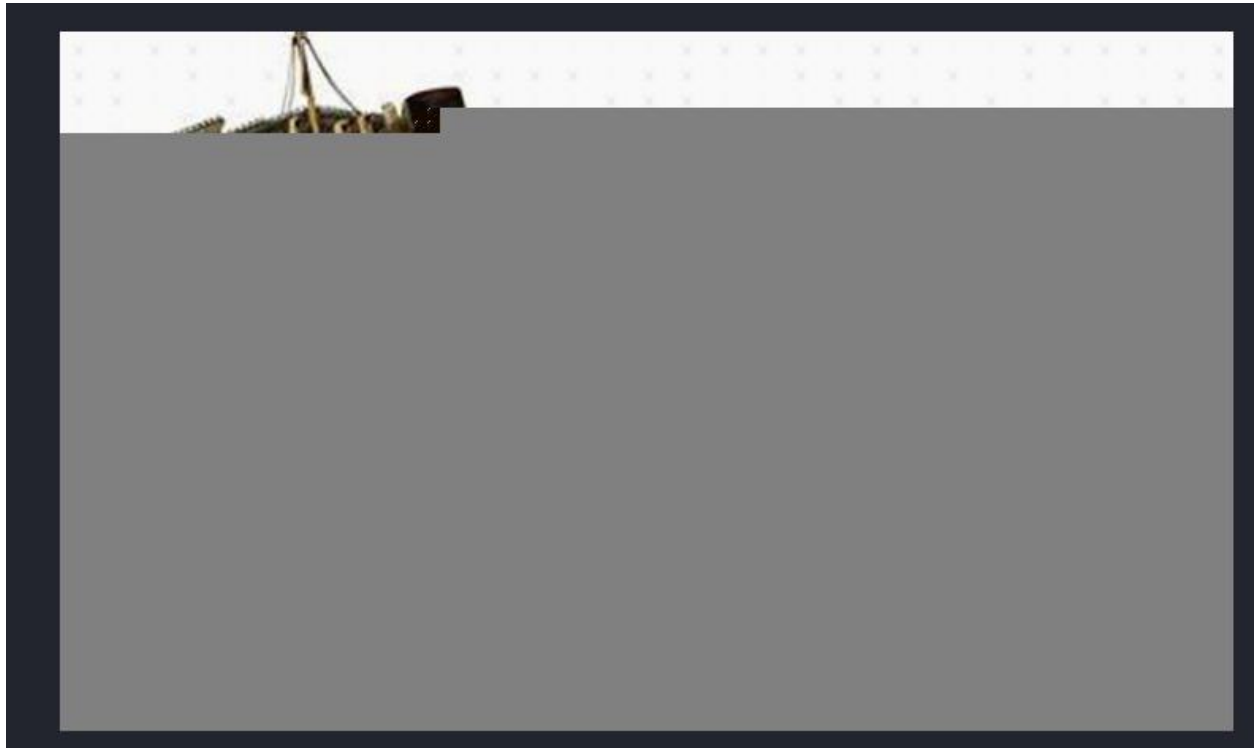


Figure 14 "l.jpg" Incomplete image.

Using the “Identify” software on the image confirms that there is missing data inside each of the images. Running this command on “l.jpg” confirms that it begins as a JPG but ends early as data appears to be missing. The outputs of the “Identify” command can be seen in Figure 15 and 16.

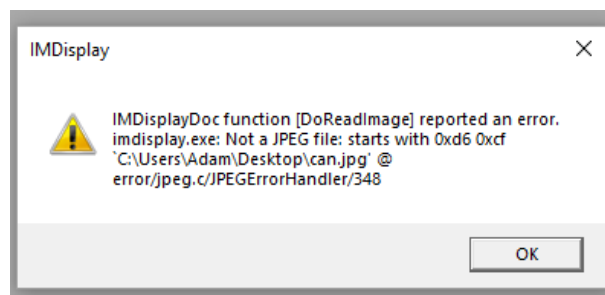


Figure 15 "can.jpg" ran through "identify" software program.

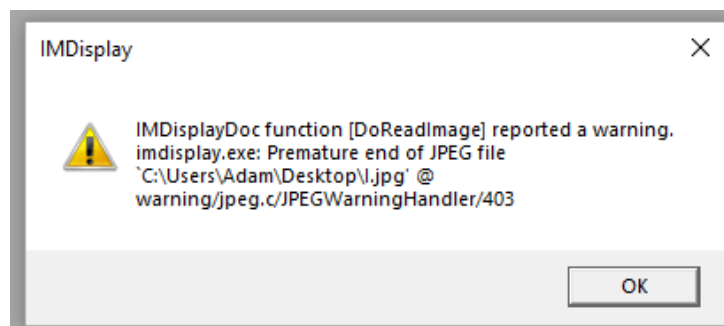


Figure 16 "I.jpg" ran through "identify" software program.

The investigator was given information from the health regulatory agency that an Obi-Wan quote may be of use in this stage of the investigation. Based on the file names of the images, the Obi-Wan quote which matched was: "I'll never understand how you can simplify these battles into some kind of game" (Anon., 2015).

Attempting to concatenate these files together using the "cat" command was the next step. It was assumed the files were split up but could be put back together in the order of the quote to assemble a complete image. The "cat" command and its output can be seen in Figures 17 and 18.

```
(kali@kali) [~/DFAssessment/pcap2evidence]
$ cat I.jpg ll.jpg never.jpg understand.jpg how.jpg you.jpg can.jpg simplify.jpg these.jpg battles.jpg into.jpg some.jpg kind.jpg of.jpg game.jpg > finished.jpg
```

Figure 17 Using "cat" command to assemble complete image.



Figure 18 Completed image fully assembled.

Once the image was viewable, it was put through the software "SilentEye" because it had been referenced twice in the investigation, and this image did not seem to have any relevance to the drug trafficking case. "SilentEye" revealed that an encoded message was hidden inside of the image using steganography. The encoded message was similar to the text found in the docx files from the previous PCAP, which suggests it may be Base64 again. Putting the encoded message into CyberChef revealed the message "May the force be with you". While this message is not relevant to the case, it does confirm that anti-forensic tactics were deployed to hide data.

2.3 CAPTURE 3

2.3.1 PCAP Traffic Analysis

The investigator was informed of communication traffic between El Chapo and a known person of interest involved in the drug trafficking named Narco Polo. It is suspected that they are attempting to arrange a delivery secretly and it would be best to discover the date and time they are planning to meet.

To begin with, searching for “Narco Polo” within Capture 3 using the filter, confirms there was communication between El Chapo and Narco Polo. The conversation appears to start at packet 10597 on 22nd October 2023 at 16:51. Following the communication using Wireshark’s “follow HTTP stream” feature allowed the investigator to view the entire conversation between these two individuals. The filter can be seen in Figure 19 and the messages can be seen in Figure 20.

The image shows a Wireshark packet capture. The top pane displays a list of packets with a filter 'narco.polo' applied. Packet 10597 is selected, showing an HTTP 200 OK response. The bottom pane shows the details of this response, including headers like 'Etag', 'Accept-Ranges', 'Vary', 'Content-Encoding', 'Content-Length', 'Keep-Alive', 'Connection', and 'Content-Type'. The body of the response is a text/html document with HTML tags and a line-based text data section.

No.	Time	Source	Destination	Protocol	Length	Info
11170	2023/10/26.4	192.168.1.6	192.168.1.20	HTTP	491	GET /newchat/@chtr/log.html?_1697994354728 HTTP/1.1
11189	2023/10/26.4	192.168.1.6	192.168.1.20	HTTP	491	GET /newchat/@chtr/log.html?_1697994356728 HTTP/1.1
11189	2023/10/26.4	192.168.1.6	192.168.1.20	HTTP	491	GET /newchat/@chtr/log.html?_1697994359728 HTTP/1.1
11196	2023/10/26.4	192.168.1.6	192.168.1.20	HTTP	491	GET /newchat/@chtr/log.html?_1697994361727 HTTP/1.1
10598	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	286	HTTP/1.1 200 OK (text/html)
10597	2023/10/26.5	192.168.1.6	192.168.1.20	HTTP	865	HTTP/1.1 200 OK (text/html)
10606	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10613	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10619	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10623	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10626	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10630	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10633	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10637	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10647	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10651	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10656	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10660	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10663	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10667	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10676	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10674	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10677	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10683	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10686	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10690	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10693	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10697	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10700	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10764	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10713	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10723	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)
10737	2023/10/26.5	192.168.1.20	192.168.1.6	HTTP	865	HTTP/1.1 200 OK (text/html)

Etag: "541-685dddf6e0b5-gzip"V\n\n\nAccept-Ranges: bytesV\n\nVary: Accept-EncodingV\n\nContent-Encoding: gzipV\n\nContent-Length: 475V\n\n[Content length: 475]\n\nKeep-Alive: timeout=5, max=100V\n\nConnection: Keep-AliveV\n\nContent-Type: text/htmlV\n\nV\n\n[HTTP response 1/92]\n\n[Time since request: 0.000372000 seconds]\n\n[Next request in frame: 10605]\n\n[Next response in frame: 10605]\n\n[Request URI: http://192.168.1.20/newchat/@chtr/log.html?_169799436405]\n\nContent-encoding entity body (gzip): 475 bytes -> 1345 bytes\n\nFile data: 1345 bytes\n\nLine-based text data: text/html (1 lines)\n\n[truncated]<div class='msgln'><i>User El Chapo has joined the chat.</i></div></div><div class='msgln'><i>User Narco Polo has joined the chat.</i></div></div><div class='msgln'>(12:46 PM) El Chapo: Good evening, Narco Polo.
</div><div class='msgln'>(12:46 PM) Narco Polo: Who's on the line?
</div><div class='msgln'>(12:46 PM) El Chapo: Phoenix.
</div><div class='msgln'>(12:46 PM) Narco Polo: Where are you?
</div><div class='msgln'>(12:46 PM) El Chapo: I can't disclose that information, even to you.
</div><div class='msgln'>(12:46 PM) Narco Polo: Are you aware of the current scrutiny on El Chapo?
</div><div class='msgln'>(12:47 PM) El Chapo: Yes, I'm fully aware, However, they will never know it is me behind the shipment.
</div><div class='msgln'>(12:47 PM) Narco Polo: Regardless, we must exercise the highest level of secrecy. Be vigilant. I'd like to meet in 2nd November at 10 PM to plan the secret delivery and avoid any complications.
</div><div class='msgln'>(12:47 PM) El Chapo: At our usual rendezvous point?
</div><div class='msgln'>(12:47 PM) Narco Polo: Yes
</div><div class='msgln'>(12:47 PM) El Chapo: What day?
</div><div class='msgln'>(12:47 PM) Narco Polo: I already mentioned, stay sharp.
</div><div class='msgln'>(12:53 PM) Narco Polo: 36.62575185817829 -117.08896804489794
</div>

Figure 19 Filter to find conversation between El Chapo and Narco Polo.

```
<div class='msgln'><i>User El Chapo has joined the chat.</i></div><div class='msgln'><i>User Narco Polo has joined the chat.</i></div><div class='msgln'>(12:46 PM) <b>El Chapo</b>: Good evening, Narco Polo.<br></div><div class='msgln'>(12:46 PM) <b>Narco Polo</b>: Who&#039;s on the line?<br></div><div class='msgln'>(12:46 PM) <b>El Chapo</b>: Phoenix.<br></div><div class='msgln'>(12:46 PM) <b>Narco Polo</b>: Where are you?<br></div><div class='msgln'>(12:46 PM) <b>El Chapo</b>: I can&#039;t disclose that information, even to you.<br></div><div class='msgln'>(12:46 PM) <b>Narco Polo</b>: Are you aware of the current scrutiny on El Chapo?<br></div><div class='msgln'>(12:47 PM) <b>El Chapo</b>: Yes, I&#039;m fully aware, However, they will never know it is me behind the shipment.<br></div><div class='msgln'>(12:47 PM) <b>Narco Polo</b>: Regardless, we must exercise the highest level of secrecy. Be vigilant. I&#039;d like to meet in 2nd November at 10 PM to plan the secret delivery and avoid any complications.<br></div><div class='msgln'>(12:47 PM) <b>El Chapo</b>: At our usual rendezvous point?<br></div><div class='msgln'>(12:47 PM) <b>Narco Polo</b>: Yes<br></div><div class='msgln'>(12:47 PM) <b>El Chapo</b>: What day?<br></div><div class='msgln'>(12:47 PM) <b>Narco Polo</b>: I already mentioned, stay sharp.<br></div><div class='msgln'>(12:53 PM) <b>Narco Polo</b>: 36.62575185817829 -117.08896804489794<br></div>
```

Figure 20 Conversation between El Chapo and Narco Polo

2.3.2 Evidence analysis

The conversation has been moved to a more readable format to understand the conversation. This can be seen in Table 2.

Table 2 Messages detailing the meeting on 2nd November at 10pm, Geographical co-ordinates given.

Sender	Message	Time
El Chapo	Good evening, Narco Polo	12:46 PM
Narco Polo	Who's on the line?	12:46 PM
El Chapo	Phoenix.	12:46 PM
Narco Polo	Where are you?	12:46 PM
El Chapo	I can't disclose that information, even to you	12:46 PM
Narco Polo	Are you aware of the current scrutiny on El Chapo?	12:46 PM
El Chapo	Yes, I'm fully aware, However, they will never know it is me behind the shipment	12:47 PM
Narco Polo	Regardless, we must exercise the highest level of secrecy. Be vigilant. I'd like to meet in 2 nd November at 10pm to plan the secret delivery and avoid any complications	12:47 PM
El Chapo	At our usual rendezvous point?	12:47 PM
Narco Polo	Yes	12:47 PM
El Chapo	What day?	12:47 PM
Narco Polo	I already mentioned, stay sharp.	12:47 PM
Narco Polo	36.62575185817829 -117.08896804489794	12:53 PM

From the conversation, it seemed that El Chapo was the individual handling the shipment. The two individuals are having a meeting on 2nd November at 10pm to plan a secret delivery. At the end of the message chain, two long numbers are given. The investigator suspected that these are co-ordinates which can be put into Google Earth to give a location. Doing this reveals a location in California, USA, nearby Stovepipe Wells. The screenshot of Google Earth can be viewed in Figure 21.

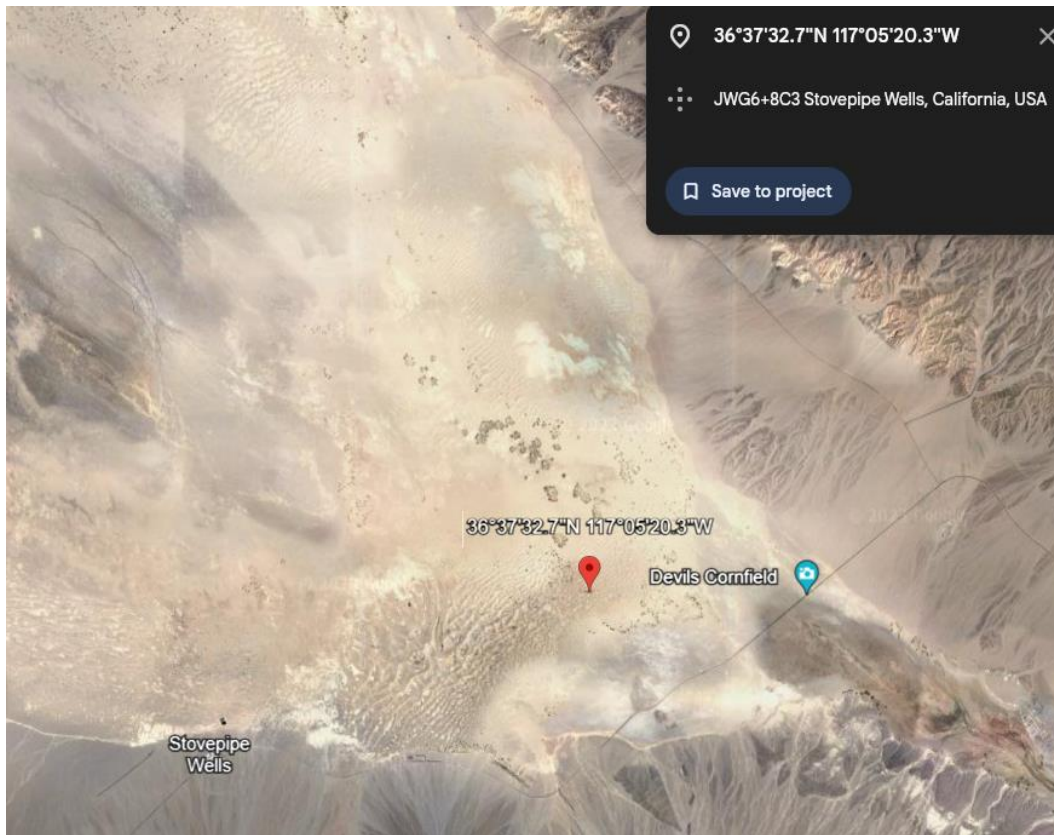


Figure 21 Google Earth of given co-ordinates revealing meetup location.

3 DISCUSSION

3.1 CRITICAL EVALUATION

There were several sections which the investigator had some difficulty with within each Capture.

3.1.1 Capture 1

For the first capture, it was challenging to locate the files relevant to the investigation. To get around this challenge, the investigator used Wireshark's built in "filter" feature to search for specific protocols to quickly find the potential evidence. Further research was required to find the correct files because the standard for SMB had changed to SMBv2. Extracting decoding information was not challenging because the correct tools were used to aid in the investigation. However, reading through the information was time consuming due to the vast quantity of information extracted. This was alleviated by using the instructions provided by the health regulatory agency to narrow down the search criteria to information related to the drugs and the quantity of drugs.

3.1.2 Capture 2

Finding and extracting the files was not challenging because the investigator had used the same method as in Capture 1 to quickly locate the FTP-Data objects that could be extracted. The challenge was discovering the quote based on the file name of each image and reassembling the different images to create one single image. Additionally, identifying that the image had a steganographic technique applied to it to hide a message within the image required critical thinking skills to solve.

3.1.3 Capture 3

The final PCAP file was particularly challenging when attempting to find the communication between the two suspects. To alleviate the challenge, Wireshark's "search" feature allowed the investigator to search for "narco polo" and discover messages between the two individuals. Beyond that, this PCAP file was easier in comparison to the two other PCAP files because the information was all in plaintext and easily extracted from the PCAP file, including the location and time of the secret meetup between the two suspects.

3.2 REFLECTION

Malicious individuals have an immeasurable number of anti-forensic methods to slow down an investigation and make it difficult to discover potential evidence. These methods include encryption, steganography, and file splitting. The methods mentioned had all been included by the suspects in the three PCAP files; In Capture 1, the data inside of the Docx files had been encoded using Base64 to make the evidence appear as "rubbish" data that can slow down an investigator because they have to decode the information before being able to read the data; Capture 2 used steganography, file splitting, and encoding to hide information inside of the PCAP file. Layering these different methods together drastically slows down an investigation and can even cause the investigator to miss vital evidence. Had the suspects used end-to-end encryption to hide the information from the investigator, this

investigation would not have been possible because the data inside of the PCAP files would have been encrypted.

REFERENCES

- achorein, 2010. *SilentEye*. [Online]
Available at: <https://achorein.github.io/silenteye/>
[Accessed 5 December 2023].
- Anon., 2015. *Star Wars: The Clone Wars, Season 2 Quotes*. [Online]
Available at: <https://www.quotes.net/show-quote/76067>
[Accessed 10 December 2023].
- GCHQ, 2023. *CyberChef*. [Online]
Available at: <https://gchq.github.io/CyberChef/>
[Accessed 5 December 2023].
- Google, 2023. *Google Earth*. [Online]
Available at: <https://earth.google.com/web/@36.62396739,-117.12566632,-14.28173895a,33343.27812193d,35y,0h,0t,0r/data=OgMKATA>
[Accessed 11 December 2023].
- Harvey, P., 2023. *ExifTool by Phil Harvey*. [Online]
Available at: <https://exiftool.org>
[Accessed 5 December 2023].
- ImageMagick, 2023. *imagemagick*. [Online]
Available at: <https://imagemagick.org/script/identify.php>
[Accessed 5 December 2023].
- Kali Linux, 2018. *Kali Linux*. [Online]
Available at: <https://www.kali.org>
[Accessed 5 December 2023].
- Man7, 2014. *Sha1sum Linux Manual Page*. [Online]
Available at: <https://man7.org/linux/man-pages/man1/sha1sum.1.html>
[Accessed 5 December 2023].
- Microsoft, 2023. *Overview of file sharing using the SMB 3 protocol in Windows Server*. [Online]
Available at: <https://learn.microsoft.com/en-us/windows-server/storage/file-server/file-server-smb-overview>
[Accessed 6 December 2023].
- Solarwinds, 2019. *RETR FTP Command*. [Online]
Available at: https://solarwindscore.my.site.com/SuccessCenter/s/article/RETR-FTP-command?language=en_US
[Accessed 10 December 2023].
- Ubuntu, 2014. *Manpages binwalk*. [Online]
Available at:

<https://manpages.ubuntu.com/manpages/trusty/man1/binwalk.1.html#:~:text=Binwalk%20is%20a%20tool%20for,embedded%20inside%20of%20firmware%20images>.
[Accessed 5 December 2023].

Wireshark, 2021. *Wireshark Training*. [Online]
Available at: <https://www.wireshark.org/docs/>
[Accessed 5 December 2023].

APPENDICES

APPENDIX A – DECODED BASE64 FILES

3.2.1 BillOfRights.txt

The Bill of Rights: A Transcription

The Preamble to The Bill of Rights

Congress of the United States

begun and held at the City of New-York, on

Wednesday the fourth of March, one thousand seven hundred and eighty nine.

THE Conventions of a number of the States, having at the time of their adopting the Constitution, expressed a desire, in order to prevent misconstruction or abuse of its powers, that further declaratory and restrictive clauses should be added: And as extending the ground of public confidence in the Government, will best ensure the beneficent ends of its institution.

RESOLVED by the Senate and House of Representatives of the United States of America, in Congress assembled, two thirds of both Houses concurring, that the following Articles be proposed to the Legislatures of the several States, as amendments to the Constitution of the United States, all, or any of which Articles, when ratified by three fourths of the said Legislatures, to be valid to all intents and purposes, as part of the said Constitution; viz.

ARTICLES in addition to, and Amendment of the Constitution of the United States of America, proposed by Congress, and ratified by the Legislatures of the several States, pursuant to the fifth Article of the original Constitution.

Note: The following text is a transcription of the first ten amendments to the Constitution in their original form. These amendments were ratified December 15, 1791, and form what is known as the "Bill of Rights."

Amendment I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

Amendment II

A well regulated Militia, being necessary to the security of a free State, the right of the people to keep and bear Arms, shall not be infringed.

Amendment III

No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.

Amendment IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Amendment V

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Amendment VI

In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defence.

Amendment VII

In Suits at common law, where the value in controversy shall exceed twenty dollars, the right of trial by jury shall be preserved, and no fact tried by a jury, shall be otherwise re-examined in any Court of the United States, than according to the rules of the common law.

Amendment VIII

Excessive bail shall not be required, nor excessive fines imposed, nor cruel and unusual punishments inflicted.

Amendment IX

The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.

Amendment X

The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.

AMENDMENT XI

Passed by Congress March 4, 1794. Ratified February 7, 1795.

Note: Article III, section 2, of the Constitution was modified by amendment 11.

The Judicial power of the United States shall not be construed to extend to any suit in law or equity, commenced or prosecuted against one of the United States by Citizens of another State, or by Citizens or Subjects of any Foreign State.

AMENDMENT XII

Passed by Congress December 9, 1803. Ratified June 15, 1804.

Note: A portion of Article II, section 1 of the Constitution was superseded by the 12th amendment.

The Electors shall meet in their respective states and vote by ballot for President and Vice-President, one of whom, at least, shall not be an inhabitant of the same state with themselves; they shall name in their ballots the person voted for as President, and in distinct ballots the person voted for as Vice-President, and they shall make distinct lists of all persons voted for as President, and of all persons voted for as Vice-President, and of the number of votes for each, which lists they shall sign and certify, and transmit sealed to the seat of the government of the United States, directed to the President of the Senate; -- the President of the Senate shall, in the presence of the Senate and House of Representatives, open all the certificates and the votes shall then be counted; -- The person having the greatest number of votes for President, shall be the President, if such number be a majority of the whole number of Electors appointed; and if no person have such majority, then from the persons having the highest numbers not exceeding three on the list of those voted for as President, the House of Representatives shall choose immediately, by ballot, the President. But in choosing the President, the votes shall be taken by states, the representation from each state having one vote; a quorum for this purpose shall consist of a member or members from two-thirds of the states, and a majority of all the states shall be necessary to a choice. [And if the House of Representatives shall not choose a President whenever the right of choice shall devolve upon them, before the fourth day of March next following, then the Vice-President shall act as President, as in case of the death or other constitutional disability of the President. --]* The person having the greatest number of votes as Vice-President, shall be the Vice-President, if such number be a majority of the whole number of Electors appointed, and if no person have a majority, then from the two highest numbers on the list, the Senate shall choose the Vice-President; a quorum for the purpose shall consist of two-thirds of the whole number of Senators, and a majority of the whole number shall be necessary to a choice. But no person constitutionally ineligible to the office of President shall be eligible to that of Vice-President of the United States.

*Superseded by section 3 of the 20th amendment.

AMENDMENT XIII

Passed by Congress January 31, 1865. Ratified December 6, 1865.

Note: A portion of Article IV, section 2, of the Constitution was superseded by the 13th amendment.

Section 1.

Neither slavery nor involuntary servitude, except as a punishment for crime whereof the party shall have been duly convicted, shall exist within the United States, or any place subject to their jurisdiction.

Section 2.

Congress shall have power to enforce this article by appropriate legislation.

AMENDMENT XIV

Passed by Congress June 13, 1866. Ratified July 9, 1868.

Note: Article I, section 2, of the Constitution was modified by section 2 of the 14th amendment.

Section 1.

All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

Section 2.

Representatives shall be apportioned among the several States according to their respective numbers, counting the whole number of persons in each State, excluding Indians not taxed. But when the right to vote at any election for the choice of electors for President and Vice-President of the United States, Representatives in Congress, the Executive and Judicial officers of a State, or the members of the Legislature thereof, is denied to any of the male inhabitants of such State, being twenty-one years of

age,* and citizens of the United States, or in any way abridged, except for participation in rebellion, or other crime, the basis of representation therein shall be reduced in the proportion which the number of such male citizens shall bear to the whole number of male citizens twenty-one years of age in such State.

Section 3.

No person shall be a Senator or Representative in Congress, or elector of President and Vice-President, or hold any office, civil or military, under the United States, or under any State, who, having previously taken an oath, as a member of Congress, or as an officer of the United States, or as a member of any State legislature, or as an executive or judicial officer of any State, to support the Constitution of the United States, shall have engaged in insurrection or rebellion against the same, or given aid or comfort to the enemies thereof. But Congress may by a vote of two-thirds of each House, remove such disability.

Section 4.

The validity of the public debt of the United States, authorized by law, including debts incurred for payment of pensions and bounties for services in suppressing insurrection or rebellion, shall not be questioned. But neither the United States nor any State shall assume or pay any debt or obligation incurred in aid of insurrection or rebellion against the United States, or any claim for the loss or emancipation of any slave; but all such debts, obligations and claims shall be held illegal and void.

Section 5.

The Congress shall have the power to enforce, by appropriate legislation, the provisions of this article.

*Changed by section 1 of the 26th amendment.

AMENDMENT XV

Passed by Congress February 26, 1869. Ratified February 3, 1870.

Section 1.

The right of citizens of the United States to vote shall not be denied or abridged by the United States or by any State on account of race, color, or previous condition of servitude--

Section 2.

The Congress shall have the power to enforce this article by appropriate legislation.

AMENDMENT XVI

Passed by Congress July 2, 1909. Ratified February 3, 1913.

Note: Article I, section 9, of the Constitution was modified by amendment 16.

The Congress shall have power to lay and collect taxes on incomes, from whatever source derived, without apportionment among the several States, and without regard to any census or enumeration.

AMENDMENT XVII

Passed by Congress May 13, 1912. Ratified April 8, 1913.

Note: Article I, section 3, of the Constitution was modified by the 17th amendment.

The Senate of the United States shall be composed of two Senators from each State, elected by the people thereof, for six years; and each Senator shall have one vote. The electors in each State shall have the qualifications requisite for electors of the most numerous branch of the State legislatures.

When vacancies happen in the representation of any State in the Senate, the executive authority of such State shall issue writs of election to fill such vacancies: Provided, That the legislature of any State may empower the executive thereof to make temporary appointments until the people fill the vacancies by election as the legislature may direct.

This amendment shall not be so construed as to affect the election or term of any Senator chosen before it becomes valid as part of the Constitution.

AMENDMENT XVIII

Passed by Congress December 18, 1917. Ratified January 16, 1919. Repealed by amendment 21.

Section 1.

After one year from the ratification of this article the manufacture, sale, or transportation of intoxicating liquors within, the importation thereof into, or the exportation thereof from the United States and all territory subject to the jurisdiction thereof for beverage purposes is hereby prohibited.

Section 2.

The Congress and the several States shall have concurrent power to enforce this article by appropriate legislation.

Section 3.

This article shall be inoperative unless it shall have been ratified as an amendment to the Constitution by the legislatures of the several States, as provided in the Constitution, within seven years from the date of the submission hereof to the States by the Congress.

AMENDMENT XIX

Passed by Congress June 4, 1919. Ratified August 18, 1920.

The right of citizens of the United States to vote shall not be denied or abridged by the United States or by any State on account of sex.

Congress shall have power to enforce this article by appropriate legislation.

AMENDMENT XX

Passed by Congress March 2, 1932. Ratified January 23, 1933.

Note: Article I, section 4, of the Constitution was modified by section 2 of this amendment. In addition, a portion of the 12th amendment was superseded by section 3.

Section 1.

The terms of the President and the Vice President shall end at noon on the 20th day of January, and the terms of Senators and Representatives at noon on the 3rd day of January, of the years in which such terms would have ended if this article had not been ratified; and the terms of their successors shall then begin.

Section 2.

The Congress shall assemble at least once in every year, and such meeting shall begin at noon on the 3d day of January, unless they shall by law appoint a different day.

Section 3.

If, at the time fixed for the beginning of the term of the President, the President elect shall have died, the Vice President elect shall become President. If a President shall not have been chosen before the time fixed for the beginning of his term, or if the President elect shall have failed to qualify, then the Vice President elect shall act as President until a President shall have qualified; and the Congress may by law provide for the case wherein neither a President elect nor a Vice President shall have qualified, declaring who shall then act as President, or the manner in which one who is to act shall be selected, and such person shall act accordingly until a President or Vice President shall have qualified.

Section 4.

The Congress may by law provide for the case of the death of any of the persons from whom the House of Representatives may choose a President whenever the right of choice shall have devolved upon them, and for the case of the death of any of the persons from whom the Senate may choose a Vice President whenever the right of choice shall have devolved upon them.

Section 5.

Sections 1 and 2 shall take effect on the 15th day of October following the ratification of this article.

Section 6.

This article shall be inoperative unless it shall have been ratified as an amendment to the Constitution by the legislatures of three-fourths of the several States within seven years from the date of its submission.

AMENDMENT XXI

Passed by Congress February 20, 1933. Ratified December 5, 1933.

Section 1.

The eighteenth article of amendment to the Constitution of the United States is hereby repealed.

Section 2.

The transportation or importation into any State, Territory, or Possession of the United States for delivery or use therein of intoxicating liquors, in violation of the laws thereof, is hereby prohibited.

Section 3.

This article shall be inoperative unless it shall have been ratified as an amendment to the Constitution by conventions in the several States, as provided in the Constitution, within seven years from the date of the submission hereof to the States by the Congress.

AMENDMENT XXII

Passed by Congress March 21, 1947. Ratified February 27, 1951.

Section 1.

No person shall be elected to the office of the President more than twice, and no person who has held the office of President, or acted as President, for more than two years of a term to which some other person was elected President shall be elected to the office of President more than once. But this Article shall not apply to any person holding the office of President when this Article was proposed by Congress, and shall not prevent any person who may be holding the office of President, or acting as President, during the term within which this Article becomes operative from holding the office of President or acting as President during the remainder of such term.

Section 2.

This article shall be inoperative unless it shall have been ratified as an amendment to the Constitution by the legislatures of three-fourths of the several States within seven years from the date of its submission to the States by the Congress.

AMENDMENT XXIII

Passed by Congress June 16, 1960. Ratified March 29, 1961.

Section 1.

The District constituting the seat of Government of the United States shall appoint in such manner as Congress may direct:

A number of electors of President and Vice President equal to the whole number of Senators and Representatives in Congress to which the District would be entitled if it were a State, but in no event more than the least populous State; they shall be in addition to those appointed by the States, but they shall be considered, for the purposes of the election of President and Vice President, to be electors appointed by a State; and they shall meet in the District and perform such duties as provided by the twelfth article of amendment.

Section 2.

The Congress shall have power to enforce this article by appropriate legislation.

AMENDMENT XXIV

Passed by Congress August 27, 1962. Ratified January 23, 1964.

Section 1.

The right of citizens of the United States to vote in any primary or other election for President or Vice President, for electors for President or Vice President, or for Senator or Representative in Congress, shall not be denied or abridged by the United States or any State by reason of failure to pay any poll tax or other tax.

Section 2.

The Congress shall have power to enforce this article by appropriate legislation.

AMENDMENT XXV

Passed by Congress July 6, 1965. Ratified February 10, 1967.

Note: Article II, section 1, of the Constitution was affected by the 25th amendment.

Section 1.

In case of the removal of the President from office or of his death or resignation, the Vice President shall become President.

Section 2.

Whenever there is a vacancy in the office of the Vice President, the President shall nominate a Vice President who shall take office upon confirmation by a majority vote of both Houses of Congress.

Section 3.

Whenever the President transmits to the President pro tempore of the Senate and the Speaker of the House of Representatives his written declaration that he is unable to discharge the powers and duties of his office, and until he transmits to them a written declaration to the contrary, such powers and duties shall be discharged by the Vice President as Acting President.

Section 4.

Whenever the Vice President and a majority of either the principal officers of the executive departments or of such other body as Congress may by law provide, transmit to the President pro tempore of the Senate and the Speaker of the House of Representatives their written declaration that the President is unable to discharge the powers and duties of his office, the Vice President shall immediately assume the powers and duties of the office as Acting President.

Thereafter, when the President transmits to the President pro tempore of the Senate and the Speaker of the House of Representatives his written declaration that no inability exists, he shall resume the powers and duties of his office unless the Vice President and a majority of either the principal officers of the executive department or of such other body as Congress may by law provide, transmit within four days

to the President pro tempore of the Senate and the Speaker of the House of Representatives their written declaration that the President is unable to discharge the powers and duties of his office. Thereupon Congress shall decide the issue, assembling within forty-eight hours for that purpose if not in session. If the Congress, within twenty-one days after receipt of the latter written declaration, or, if Congress is not in session, within twenty-one days after Congress is required to assemble, determines by two-thirds vote of both Houses that the President is unable to discharge the powers and duties of his office, the Vice President shall continue to discharge the same as Acting President; otherwise, the President shall resume the powers and duties of his office.

AMENDMENT XXVI

Passed by Congress March 23, 1971. Ratified July 1, 1971.

Note: Amendment 14, section 2, of the Constitution was modified by section 1 of the 26th amendment.

Section 1.

The right of citizens of the United States, who are eighteen years of age or older, to vote shall not be denied or abridged by the United States or by any State on account of age.

Section 2.

The Congress shall have power to enforce this article by appropriate legislation.

AMENDMENT XXVII

Originally proposed Sept. 25, 1789. Ratified May 7, 1992.

No law, varying the compensation for the services of the Senators and Representatives, shall take effect, until an election of representatives shall have intervened.

3.2.2 GoT Spoilers.docx

Jon Snow burns down Winterfell (again) and the Wall.

Hodor kills Theon.

Daenerys gets eaten by a dragon.

Stannis falls in love with Tyrion.

3.2.3 PiD.docx

Dear Ed,

Yeah I totally took over for Paul after he died in 1966. You got me. As you can see, we don't even look that much alike:



Before(Paul)



After(Me)

We aren't even the same height! What can I say, people are stupid.

Thanks for the inquiry,

William Campbell

(Paul McCartney)

3.2.4 North Korea.docx

Для кого это может касаться:

Я был свидетелем, что Ким Чен Ун и правительство Северной Кореи разработали программу, которая позволяет им путешествовать во времени. С использованием этой технологии, я считаю, что они намерены двигаться вперед и изменить результаты войны в Корее.

Пожалуйста, Оби-Ван, ты моя единственная надежда.

3.2.5 North Korea.docx – English

To whom it may concern:

I witnessed that Kim Jong Un and the North Korean government have developed a program that allows them to travel through time. By using this technology, I believe they intend to move forward and change the outcome of the Korean War.

Please Obi-Wan, you are my only hope.

3.2.6 Track 10.docx

"Protect Ya Neck"

"So what's up man?"

Cooling man"

"Chilling chilling?"

"Yo you know I had to call, you know why right?"

"Why?"

"Because, yo, I never ever call and ask, you to play something right?"

"Yeah"

"You know what I wanna hear right?"

"What you wanna hear?"

I wanna hear that Wu-Tang joint"

"Wu-Tang again?"

"Ah yeah, again and again!"

[sounds of fighting]

[RZA] Wu-Tang Clan coming at you, protect your neck kid, so set it off the Inspector Deck

[Meth] watch your step kid [8X]

[Inspector Deck]

I smoke on the mic like smoking Joe Frazier

The hell raiser, raising hell with the flavor

Terrorize the jam like troops in Pakistan

Swinging through your town like your neighborhood Spiderman

So uhh, tic toc and keep ticking

While I get you flipping off the shit I'm kicking

The Lone Ranger, code red, danger!

Deep in the dark with the art to rip charts apart

The vandal, too hot to handle

you battle, you're saying Goodbye like Tevin Campbell

Roughneck, Inspector Deck's on the set

The rebel, I make more noise than heavy metal

[Raekwon]

The way I make the crowd go wild, sit back relax won't smile

Rae got it going on pal, call me the rap assassinator

Rhymes rugged and built like Schwarzenegger

And I'm gonna get mad deep like a threat, blow up your project

Then take all your assets

Cause I came to shake the frame in half

With the thoughts that bomb, shit like math!

So if you wanna try to flip go flip on the next man

Cause I grab the clip and

Hit you with sixteen shots and more I got

Going to war with the melting pot hot

[Method]

It's the Method Man for short Mr. Meth

Moving on your left, ah!

And set it off, get it off, let it off like a gat

I wanna break full, cock me back

Small change, they putting shame in the game

I take aim and blow that nigga out the frame

And like Fame, my style'll live forever

Niggaz crossing over, but they don't know no better

But I do, true, can I get a "sue"

Nuff respect due to the one-six-oh

I mean oh, you check out the flow

like the Hudson or PCP when I'm dusting

Niggaz off because I'm hot like sauce

The smoke from the lyrical blunt makes me [cough]

[U-God]

Oh, what, grab my nut get screwed

Ow, here comes my Shaolin style

Sloop, B. A. Buh-B. Y. U

to my crew with the "sue"

[Interlude]

watch your step kid [8X]

[Ol Dirty Bastard] c'mon baby baby c'mon [4X]

[RZA] Yo, you best protect your neck

[Ol Dirty Bastard]

First things first man you're fucking with the worst
I'll be sticking pins in your head like a fucking nurse
I'll attack any nigga who's slack in his mack
Come fully packed with a fat rugged stack
Shame on you when you stepped through to
The Ol Dirty Bastard straight from the Brooklyn Zoo
And I'll be damned if I let any man
Come to my center, you enter the winter
Straight up and down that shit packed jam
You can't slam, don't let me get fool on him man
The Ol Dirty Bastard is dirty and stinking
Ason, unique rolling with the night of the creeps
Niggaz be rolling with a stash
ain't saying cash, bite my style I'll bite your motherfucking ass!

[Ghostface Killah]

For crying out loud my style is wild so book me
Not long is how long that this rhyme took me
Ejecting, styles from my lethal weapon
My pen that rocks from here to Oregon
Here's Mordigan, catch it like a psycho flashback
I love gats, if rap was a gun, you wouldn't bust back
I come with shit that's all types of shapes and sounds
And where I lounge is my stomping grounds
I give a order to my peeps across the water
To go and snatch up props all around the border
And get far like a shooting star
'cause who I am is dim in the light of Pablo Escobar
Point blank as I kick the square biz

There it is you're fucking with pros and there it goes

[RZA]

You chill with the feedback black we don't need that
It's ten o'clock hoe, where the fuck's your seed at?
Feeling mad hostile, ran the apostle
Flowing like Christ when I speaks the gospel
Stroll with the holy roll then attack the globe with the buckus style
the ruckus, ten times ten men committing mad sin
Turn the other cheek and I'll break your fucking chin
Slaying boom-bangs like African drums (we'll be)
Coming around the mountain when I come
Crazy flamboyant for the rap enjoyment
My clan increase like black unemployment
Yeah, another one dare,
Tuh-took a genius (to) take us the fuck outta here

[Genius]

The Wu is too slamming for these Cold Killing labels
Some ain't had hits since I seen Aunt Mabel
Be doing artists in like Cain did Abel
Now they money's gettin stuck to the gum under the table
That's what you get when you misuse what I invent
Your empire falls and you lose every cent
For trying to blow up a scrub
Now that thought was just as bright as a 20-watt light bulb
Should've pumped it when I rocked it
Niggaz so stingy they got short arms and deep pockets
This goes on in some companies

With majors they're scared to death to pump these
 First of all, who's your A&R
 A mountain climber who plays an electric guitar
 But he don't know the meaning of dope
 When he's looking for a suit and tie rap
 that's cleaner than a bar of soap
 And I'm the dirtiest thing in sight
 Matter of fact bring out the girls and let's have a mud fight

[sounds of fighting]

[RZA] You best protect your neck [4X]

3.2.7 Chess Rules 1.docx

1. SUMMARY OF RULES. MAIN POINTS.

TOUCH MOVE rule strictly applies.

â If a piece is touched, then it must be moved (if a legal move is available)

â If an opponentâs piece is touched, it must be taken (if legal).

COUNTDOWN IF STALLING FOR TIME. In general a player manages how much or little time to take for each move, and this is fine! However, if a player clearly plays far too slowly for the specific position, for example when he is facing unavoidable checkmate, the arbiter will do a countdown. He will point at the board, and warn the player by counting to 10 with his hands (just like a boxing referee). If the player has not moved by the count of 10, he loses the game and the match. Note there is no minimum time to make a move! Also, even if there is only 1 legal move, the player should be allowed some time to psychologically compose themselves. It should be considered that a weak player may not realise he only has 1 legal move.

CHESS CLOCK PROTOCOL. The chess clock must be pressed with the SAME HAND that moves the piece.

PRESSING CHECK CLOCK. It is the playerâs responsibility to press his or her clock between chess moves. The competitors may agree in advance to allow the arbiter to issue reminders â especially if both fighters are new to chessboxing.

PIECES KNOCKED DOWN OR NOT PROPERLY ON A SQUARE. If a player knocks down a piece whilst making a move or does not put it properly on a square, he should properly re-position or re-centre the piece in HIS OWN clock time. An offence that puts off the opponent could be punished by adding time to the opponentâs clock.

OTHER RULES to NOTE

• Resignation protocol. For the benefit of the audience, players are strongly encouraged to play until checkmate. If you want to resign (submit) prior to checkmate, do this by knocking over your king and offering a handshake.

• Illegal move. An illegal move must be retracted. The arbiter has the discretion to punish with a time penalty, or disqualify after 3 illegal moves. Extra allowances can be made for novice players.

• Speaking to the arbiter. If a player needs to speak to the arbiter during the chess game, he should remove his headphones. The arbiter will then stop the clock to listen.

• Playing to win on time. If a position is a completely drawn position, and the arbiter believes a player is quickly moving pieces only to win on time, then the arbiter can declare the game a draw.

• Chess Draw. A chess draw will be followed by one boxing round (unless the maximum number of boxing rounds has already happened). The chessboxing bout will therefore be won by whoever has amassed the most boxing points “ judged by punches thrown and overall aggression.

• Drinks Fighters are allowed to bring water to the chess table.

• Cuts In most cases, except for the most superficial examples, a cut will lead to the fight being stopped and a TKO declared.

• General Advice Competitors are reminded that they do not need to move quickly, even if their opponent moves quickly. Adrenaline drastically changes your sense of time. Experience shows that a player is OK until he has 2 minutes of time remaining on the clock, when moves should be speeded up.

3.2.8 Chess Rules 2.docx

2. ENFORCEMENT OF CHESS RULES

In the event of a breach of the rules a penalty can be imposed at the arbiter’s discretion.

3.2.9 Chess Rules 3.docx

3. PENALTIES FOR RULE BREACHES

A chess penalty could take the form of:

• The offence will act as a tie-break if both the boxing and chess are drawn. This is the minimum (default) penalty and applies if there is no other penalty.

• 30 seconds is subtracted from the offender’s clock.

• Forfeit of the bout. This could occur for a serious disciplinary offence, deliberate foul play or a repeated breach (e.g. a total of 3 illegal moves).

3.2.10 Chess Rules 4.docx

4. CHESS CLOCK MALFUNCTION

In the unlikely event the electronic chess clock ceases to operate during a chess round, the arbiter will do one of following, depending on the estimated disruption to the players and spectators:

• Stop the clock and resolve the problem.

• Stop the clock and replace it with a new clock. This action is most likely if there is a repeated malfunction, or itâ€™s one of the later chess rounds where a player is short of time.

3.2.11 Chess Rules 5.docx

5. WCBA CHESS RULES FOR CHESSBOXING

Chess tournament rules have legal points that casual players may be unfamiliar with. The official laws of chess are on the website of FIDE, the chess governing body <http://www.fide.com/component/handbook/?id=32&view=category>.

Highlighted below are legal points that cause most disputes in tournament chess situations.

In addition, some chessboxing laws differ from FIDE rules in order to (i.) ensure the paying public is entertained, (ii.) keep the game flowing with minimal disruption, and (iii.) minimise verbal communication with the competitors. These differences are highlighted where they occur.

Touch move

- Once a piece is touched it MUST be moved, unless “J’adoube” is indicated before touching the piece. If no legal move is admissible, then any other piece can be moved without punishment.
- Once an opponent’s piece is touched it must be captured if there is such a legal move. If it cannot be captured the offender receives no penalty and is free to move without restriction.

Castling touch move

When castling you MUST touch the king first. If you touch the rook first, then you cannot castle, but you must move the rook because of the touch-move rule.

Hand is taken off a piece

When a piece is moved and the hand taken off the piece, the move cannot be retracted – the piece cannot be moved to a different square.

Illegal move

The arbiter will point out the illegal move if it goes unnoticed. Since the punishment for an illegal move is not as severe in chessboxing as in FIDE blitz chess laws, the arbiter will not allow the possibility of an illegal move going uncorrected.

“J’Adoube” rule.

Normal Chess Rules

- If a piece is off centre and is annoying you, state “j’adoube” or “I adjust” BEFORE adjusting its position on the square. One of these phrases should be used regardless of the player’s home language.
- If you state “j’adoube” after or during the piece adjustment, then it counts as a touch move.
- You should only adjust pieces whilst your clock is running. Adjusting during your opponent’s time is forbidden as it is a distraction.

Chessboxing Rules (adapted because both players have headphones)

- With headphones on it is simplest if players don’t try to J’adoube. Pieces will be nicely centred by the arbiter between each chess round. However, if the urge to J’adoube becomes irresistible, follow the below procedure...
- Clearly turn to the arbiter and mouth “J’adoube” AND give the J’adoube hand signal specially developed for chessboxing. Then adjust the piece as in a normal chess game.
- The j’adoube hand signal is the ‘OK’ hand gesture, creating a circle with the thumb and first finger.

Pawn promotion

A key difference between casual chess and tournament rules. When promoting a pawn to a second queen, do NOT use an upside-down rook (as the electronic chessboard will not recognise it). Even if you shout “queen” as you do so, it is still a rook! The chessboxing arbiter will ensure a spare queen is on the table for you to use.

Clock

- The clock MUST be pressed with the same hand that makes the move
- Running out of time. If a player has no time remaining, then he is lost if his opponent can checkmate him assuming the most unskilled play, otherwise the game is a draw. For example, if Player A has three queens and a king, and Player B has one pawn and a king, then Player B wins if Player A runs out of time.
- A player should not start to make his move until the opponent has physically pressed his clock.

- Time scramble – disputes can arise when 1 or both players are short of time and moving extremely quickly:
 - o A player should not start to make his move until the opponent has physically pressed his clock. i.e. you should not rush to move a piece in the brief time between your opponent moving his piece and pressing his clock.
 - o If a player knocks down pieces during a move, he should reset them in his own time before pressing his clock. If he presses his clock without resetting the pieces on their squares, then the opponent can immediately bounce the clock back without making a move, whilst pointing to the offending piece(s) that have been knocked down. The first player should then properly reset the pieces in his own time. [This completely differs from FIDE laws, where the innocent party should stop the clocks and inform the arbiter]. The same action can be performed if a piece is not clearly on a square but significantly overlaps another square such that its position is ambiguous. The arbiter can stop the clocks if there is a flurry of poorly placed pieces, and intervene to reset the board. The arbiter can penalise the offender.
 - o Drawn position – playing to win on time
 - If the arbiter judges the position is a dead draw (e.g. opposite colour bishop ending, or R+K vs R+K), then the arbiter can intervene and declare a draw if a player is simply trying to win on time and not making a concerted effort to win the game. The defender does not need to request the arbiter to make such a judgement; the arbiter will assume the request exists as soon as a player has less than 2 minutes remaining. [This differs from the FIDE laws, which requires the defender to stop the clocks BEFORE he gets into critical time trouble, and ask the arbiter to observe whether the attacker is making a concerted effort to win the game or is just aiming to win on time in a dead drawn position.]
 - Losing position – playing to win on time
 - Note that if a player is in a winning position but is close to losing on time, the arbiter will not intervene in his favour. If he loses on time before he checkmates the opponent, this is more a consequence of time mismanagement than having to make countless moves shuffling pieces in a dead drawn position.
 - Slow playing a lost position – a rule developed for chessboxing to prevent stalling for time.
 - If a player takes too much time in a lost position where he would be expected to play much quicker in a normal chess game, the arbiter can give him a count of 10. The arbiter will visually count with his hands. If no move is made on the count of 10, the player forfeits the game.

Draw by threefold repetition

- If the same position occurs 3 times (and with the same player to move), the player can claim a draw ONLY WHEN IT IS HIS MOVE. He should stop the clock after the opponent's last move, remove his headphones and TELL the arbiter what move he WOULD play to get into the 3rd repetition. DO NOT PLAY THE MOVE, DO NOT PRESS THE CLOCK. If the player is unsure how to pause the clock, then he can take off his headphones and claim the draw. The arbiter will stop the clock as the headphones come off.

If the draw claim is correct and the claimant runs out of time after removing his headphones, the draw will hold.

- A draw by repetition normally occurs by perpetual check so is easy to identify.

50 move rule

A draw can be claimed if neither a piece is taken nor a pawn moved in 50 moves (i.e. 50 White and 50 Black moves). As players are not writing a game score, the arbiter will monitor on their behalf – this is most likely to occur in an ending B+N+K vs. K.

Draw Offer

- Contrary to FIDE rules, players will not be able to offer a draw unless the position is a 'dead draw', as judged by the arbiter.
- The offer of a draw must be made through the arbiter. Make your move, do not press your clock, and then remove the headphones to speak to the arbiter. The arbiter will stop the clock and judge whether a draw offer is acceptable. If so, he will convey to the opponent for consideration and restart the clock (as the opponent can consider the draw offer until he makes his next move).

Verbal Communication with the arbiter

- If a player wants to speak to the arbiter during the game he should remove his headphones. The arbiter will stop the clock to talk. The other player can remove his headphones to listen to the conversation.

Arbiter's decision

- The arbiter's decision is final. The finer rules of chessboxing will no doubt evolve with the sport. Any unanticipated circumstances will be judged considering the official FIDE chess laws, the need for sporting fair play in relation to the tournament chess experience of the chessboxers, and the need to entertain a paying audience.

3.2.12 Chess Rules 6.docx

6. CHESS DRAW IN RELATION TO THE CHESSBOXING BOUT

If a chess draw is declared in any round, there will be at most only one boxing round thereafter. If the chess draw occurs in the final round, then there will be no further boxing round, in line with the original schedule.

In the unlikely event that the chess game is drawn AND the boxing is a tie on points, then the player with the fewest chess penalties is the winner. If these are equal the bout will be declared a draw.

3.2.13 Chess Rules 7.docx

7. HOW CHESS PIECES MOVE “ FINER POINTS THAT CONFUSE BEGINNERS

The complete official laws of chess are on the website of FIDE, the chess governing body.

The Appendix on the above link explains chess notation, and instances where “blitz” or “rapid” chess rules differ from normal “long play” time controls.

Castling

☞ Castling is one move

☞ The king always moves 2 squares, and the rook then goes next to the king on the other side.

☞ All squares between king and rook must be clear. Castling cannot capture a piece.

☞ White Kingside castling moves the King from e1 to g1, and the Rook from h1 to f1.

☞ White Queenside castling moves the King from e1 to c1, and the Rook from a1 to d1.

Castling is not a legal move when

☞ the king is in check

☞ the king moves into check

☞ the king crosses over a square that is attacked (many players are unaware of this subtle point)

☞ a piece is on a square between king and rook

☞ the king has previously moved, even if it has since returned to its original square

☞ the rook to be castled has previously moved, even if it has since returned to its original square

Pawn Promotion

A pawn reaching the eighth rank is 99% of times promoted to a queen, but it can also be “under-promoted” to a knight, bishop or rook.

En Passant

A special type of pawn capture. A pawn attacking a square crossed by an opponent’s pawn which has advanced two squares in one move from its original square may capture this opponent’s pawn as though the latter had been moved only one square. This capture is only legal on the move following this advance and is called an ‘en passant’ capture. “En passant” is French for “as it passes”. See http://en.wikipedia.org/wiki/En_passant for visual examples.

APPENDIX B – IMAGES FOUND

NK.jpg



NorthKorea.jpeg



APPENDIX C – SCRIPTS FOUND

broken.py

```
def fileToString(pathToFile):  
    f = open(pathToFile, "r")  
    strs = ""  
    #adds each line of the file to the strs string  
    for line in f.readlines():  
        strs+=line  
    return strs  
def ASCII():  
    #number of ASCII characters  
    NumOfASCII == 0
```



```

    #returns list of all ASCII characters
    return "".join([chr(i) for i in range(NumOfASCII)])
def sumName(name):
    sums=0
    #sums the indices in ASCII of all the characters in name
    for x in name:
        sums+=ord(x)
    return sums
def indexInFile(password):
    indices = []
    ASCIIArray = ASCII()
    #populates an array of indices to be used by the encoder
    for chrs in password:
        indices.append(ASCIIArray.index(chrs)+sumName(name)*2)
    return indices
def indexInASCII(name):
    indices = []
    ASCIIArray = ASCII()
    #split on all non-numeric characters
    #remove first index because it is blank
    indexList = re.split("[^\d]",encoded)[1:]
    #converts encoded characters to ASCII
    for index in indexList:
        indices.append(ASCIIArray[int(index) - (sumName(name)*2)])
    #returns decoded message
    return "".join(indices)
def encode(name):
    #returns a list of indices to be used for encoding
    indices = indexInFile(password,name)
    #convert file associated with name to a string
    bill = fileToString("./%s.txt"%name)
    encoded = ""
    #add letter in file plus index of the letter in the file to the encoded
string
    for index in indices:
        encoded+=bill[index]+str(index)

    return encoded

```