



Abertay
University

Case Study

Investigating an international sporting competition corruption case by
recover evidence from network captures

Patrick Collins

CMP416 – Advanced Digital Forensics

BSc Ethical Hacking Year 4

2022/23

Contents

Network Data and Evaluation.....	3
Capture 1.pcap	3
Capture 2.pcap	5
Capture 3.pcap	19
Appendices.....	24
Appendix A	24
Track6 - Enter The Wu Tang Clan.....	24
Track 10 – Enter The Wu Tang Clan	25
PiD	31
Miscellaneous	32
Appendix B – Image Reconstruction.....	42
Appendix C – Meeting communications	44
Ill-Song filter	44
all_messageText.txt	45
Filtered messageText only.....	55
Messages Reconstructed.....	56
Latitude and Longitude Coordinates	56
Coordinates Reconstructed	61
References	66

Capture 1.pcap

The investigator first opened the pcap file in Wireshark to analyse. After going through the packets manually, it was clear a SMB share existed. The packets were filtered with “smb” showing a zip file “Documents.zip” existed (See figure 1).

Figure 1: Packets filtered with “smb” showing “Documents.zip”.

Packet	Hostname	Content Type	Size	Filename
23854	\\DOG-WS\IPC\$	PIPE (Not Implemented) (0/0) W [0.00%]	0 bytes	\srvsvc
23902	\\DOG-WS\DOCUMENTS	FILE (129/129) R [100.00%]	129 bytes	\desktop.ini
23924	\\DOG-WS\DOCUMENTS	FILE (151/151) R [100.00%]	151 bytes	\My Music\desktop.ini
23932	\\DOG-WS\DOCUMENTS	FILE (150/150) R [100.00%]	150 bytes	\My Pictures\desktop.ini
23940	\\DOG-WS\DOCUMENTS	FILE (151/151) R [100.00%]	151 bytes	\My Videos\desktop.ini
24021	\\DOG-WS\DOCUMENTS	FILE (42/42) R [100.00%]	42 bytes	\My Pictures\Sample Pictures\desktop.ini
24186	\\DOG-WS\BLAH	FILE (1324022/1324022) W [100.00%]	1,324kB	\Documents.zip
25755	\\DOG-WS\BLAH	FILE (1014/1324022) R [0.00%]	1,324kB	\DOCUME~1.ZIP
25785	\\DOG-WS\BLAH	FILE (5110/1324022) R [0.00%]	1,324kB	\DOCUME~1.ZIP

PCAP1

File Edit View Go Help

← → ↑ 🏠 ◀ ▶ Desktop Unit 2 - Case Study - PCAP Files PCAP1

Places

- Computer
- kali
- Desktop
- Trash
- Documents
- Music
- Pictures
- Videos
- Downloads

Devices

- File System

Network

- Browse Network

File Explorer View of PCAP1:

- %5cdesktop.ini
- %5cDOCUME~1.ZI
- %5cDOCUME~1(1).ZIP
- %5cDocuments.zip
- %5cMy Music%5cdesktop.i ni
- %5cMy Pictures%5cdesкто p.ini
- %5cMy Pictures%5cSample
- %5cMy Videos%5cdesktop. ini
- %5csrvsvc

9 files: 3.8 MiB (3,972,689 bytes), Free space: 60.8 GiB

Figure 3: Extracted SMB files

Once extracted the files were investigated. Microsoft word documents titled “track6”, “track 10” and “PiD” contained encoded text in base64. The investigator used CyberChef to decode each track (GCHQ, n.d). See Appendix A, images 1, 2&3.

Username

The full list of suspects are taken from “track6.docx”: Mr. Method, Kim Ill-Song, Mr. Razor, Mr. Genius, Mr. G. Killah, Matt Cassel, Mr. I. Deck, Mr. M Killa, Mr. O.D.B., Mr. Raekwon, Mr. U-God, Mr. Cappadonna (possibly), John Woo?, Mr. Nas. See Appendix A for a list of the usernames and its base64 encoding.

Miscellaneous Information

An image of the flag of North Korea and the U.S Bill of Rights was also discovered but deemed not important to the investigation. This can be found in Appendix A.

Capture 2.pcap

FTP and other traffic between a suspected corrupt official and a foreign national.

As anti-forensic practices were suspected the investigator kept this in mind whilst investigating capture 2. Wireshark statistics to find the protocol hierarchy of FTP, as intelligence had provided this as the protocol used for the suspicious traffic. As seen in figure 4, FTP-data is listed as one of the branches.

▼ FTP Data	0.2	35	0.4	
Line-based text data	0.0	1	0.0	
File Transfer Protocol (FTP)	0.2	43	0.0	
Data	0.1	10	0.1	

Figure 4:Wireshark statistics showing FTP Data.

The investigator filtered the packet capture again with “ftp-data” which displayed the traffic of the zip file (Figure 5). Two zip files were present in the packets. “sandofwhich.zip” and “ojd34.zip” (Figure 6).

ftp-data						
No.	Time	Source	Destination	Protocol	Length	Info
5892	182.022621	172.29.1.21	172.29.1.23	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR sandofwhich.zip)
5893	182.022634	172.29.1.21	172.29.1.23	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR sandofwhich.zip)
5894	182.022870	172.29.1.21	172.29.1.23	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR sandofwhich.zip)
5896	182.022886	172.29.1.21	172.29.1.23	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR sandofwhich.zip)
5897	182.023121	172.29.1.21	172.29.1.23	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR sandofwhich.zip)
5898	182.023134	172.29.1.21	172.29.1.23	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR sandofwhich.zip)
5899	182.023369	172.29.1.21	172.29.1.23	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR sandofwhich.zip)
5900	182.023381	172.29.1.21	172.29.1.23	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR sandofwhich.zip)
5901	182.023619	172.29.1.21	172.29.1.23	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR sandofwhich.zip)
5902	182.023630	172.29.1.21	172.29.1.23	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR sandofwhich.zip)
5903	182.023870	172.29.1.21	172.29.1.23	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR sandofwhich.zip)
5904	182.023881	172.29.1.21	172.29.1.23	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR sandofwhich.zip)
5910	182.024370	172.29.1.21	172.29.1.23	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR sandofwhich.zip)
5911	182.024619	172.29.1.21	172.29.1.23	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR sandofwhich.zip)
5912	182.024631	172.29.1.21	172.29.1.23	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR sandofwhich.zip)
5913	182.024869	172.29.1.21	172.29.1.23	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR sandofwhich.zip)
5914	182.024880	172.29.1.21	172.29.1.23	FTP-DATA	1486	FTP Data: 1432 bytes (PASV) (RETR sandofwhich.zip)
5938	183.176206	172.29.1.21	172.29.1.23	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR ojd34.zip)
5939	183.176219	172.29.1.21	172.29.1.23	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR ojd34.zip)
5940	183.176455	172.29.1.21	172.29.1.23	FTP-DATA	1514	FTP Data: 1460 bytes (PASV) (RETR ojd34.zip)

Figure 5: Packets filtered using ftp-data.

1486 FTP Data: 1432 bytes (PASV) (RETR sandofwhich.zip)
1514 FTP Data: 1460 bytes (PASV) (RETR ojd34.zip)

Figure 6: Two zip files “sandofwhich.zip” and “ojd34.zip”.

Using follow -> TCP stream further showed existence of “sandofwhich.zip” which was stored in a server named “Super Secret server” (See Figure7).

```

220 Super Secret Server
USER Ill_Song
331 Please specify the password.
PASS Ill_Song
230 Login successful.
OPTS UTF8 ON
200 Always in UTF8 mode.
CWD /home/Ill_Song
250 Directory successfully changed.
TYPE I
200 Switching to Binary mode.
PASV
227 Entering Passive Mode (172,29,1,21,216,252).
RETR sandofwhich.zip
150 Opening BINARY mode data connection for sandofwhich.zip (24792 bytes).
226 Transfer complete.
500 OOPS: vsf_sysutil_recv_peek: no data

```

Figure 7: sandofwhich.zip in TCP stream.

Extracting sandofwhich.zip

To access this zip file the investigator followed the TCP stream of the first packet of “sandofwhich.zip” in the “ftp-data” filter (Figure 8).

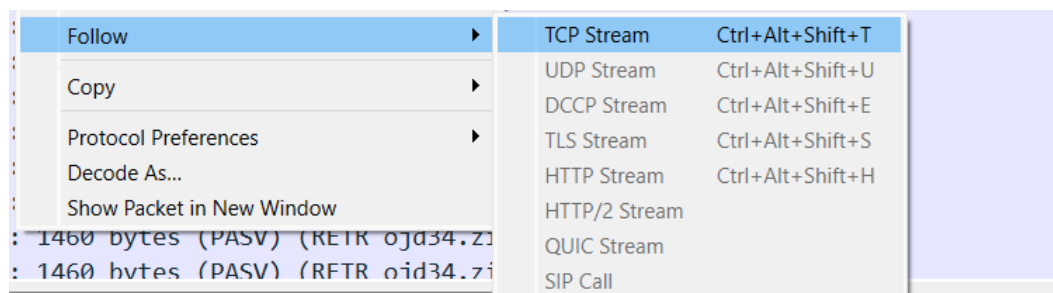


Figure 8: Follow -> TCP Stream in Wireshark on the FTP-DATA packet.

The data stream was converted to “Raw”, and its contents saved as “sandofwhich.raw” (Figure 9 on the next page).

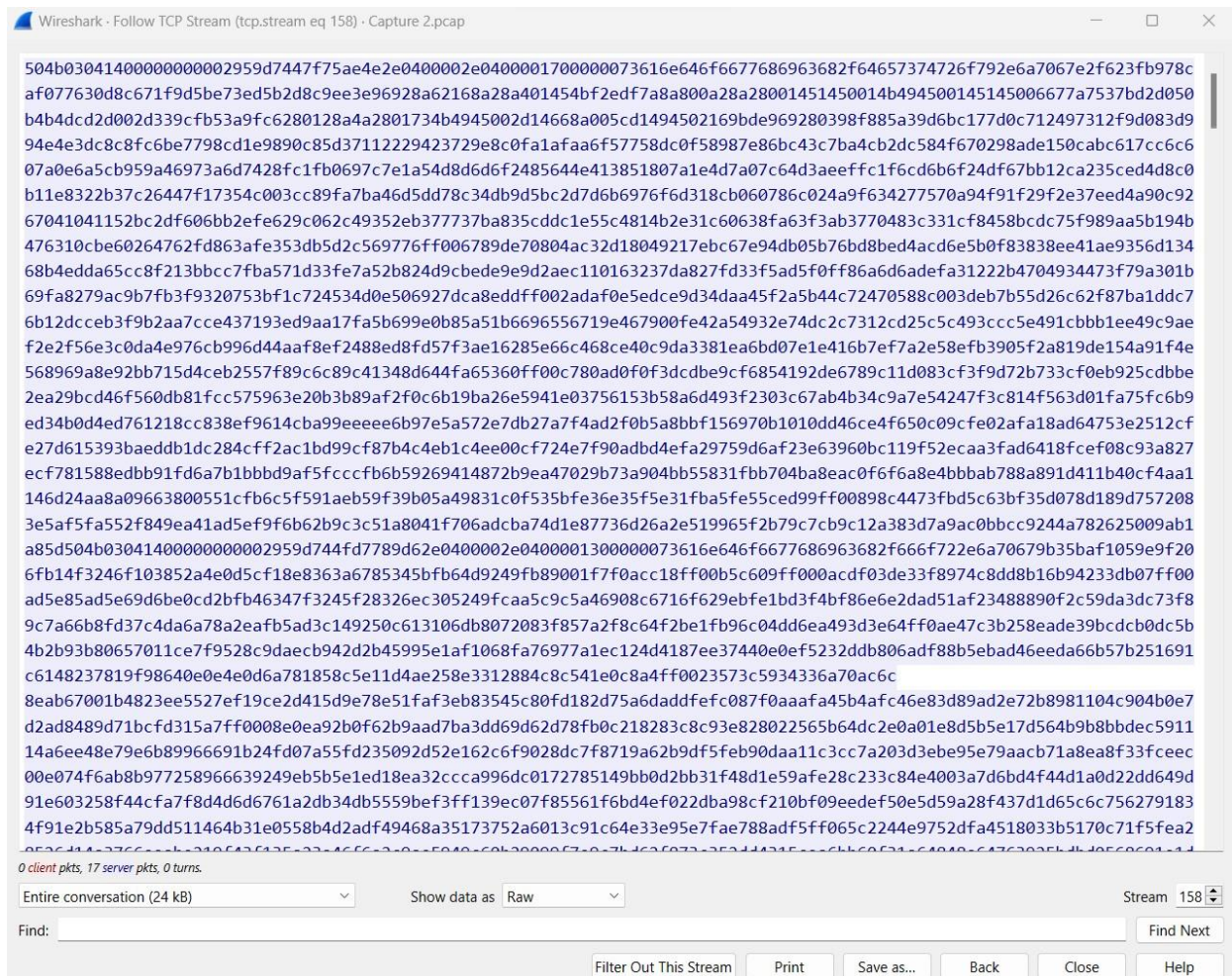


Figure 9: Saving TCP conversation as Raw

To verify the zip file had successfully been extracted, the command “file sandofwhich.raw” was executed. It found the .raw file to be Zip archive data meaning “sandofwhich.zip” had been successfully extracted out of the packet capture.

```
(kali@kali)-[~/Desktop]
$ file sandofwhich.raw
sandofwhich.raw: Zip archive data, at least v2.0 to extract, compression method=store
```

Figure 10: “file” command outputting sandofwhich.raw as a Zip archive.

Unzipping “sandofwhich.zip”

Next, the investigator simply unzipped the archive using “unzip sandofwhich.raw” (Figure 11)

```
(kali@kali)-[~/Desktop]
$ unzip sandofwhich.raw
Archive: sandofwhich.raw
  extracting: sandofwhich/destroy.jpg
  extracting: sandofwhich/for.jpg
  extracting: sandofwhich/freedom.jpg
  extracting: sandofwhich/good.jpg
  extracting: sandofwhich/government.jpg
  inflating: sandofwhich/I.jpg
  extracting: sandofwhich/in.jpg
  extracting: sandofwhich/NSA.jpg
  extracting: sandofwhich/rights.jpg
  extracting: sandofwhich/security.jpg
```

Figure 11: Unzipping the zip file.

```
(kali㉿kali)-[~/Desktop/sandofwhich]
$ ls -la
total 60
drwxr-xr-x  2 kali kali 4096 Dec 12 00:45 .
drwxr-xr-x 18 kali kali 4096 Dec 12 00:45 ..
-rw-r--r--  1 kali kali 1070 Jun 23  2014 destroy.jpg
-rw-r--r--  1 kali kali 1070 Jun 23  2014 for.jpg
-rw-r--r--  1 kali kali 1070 Jun 23  2014 freedom.jpg
-rw-r--r--  1 kali kali 1070 Jun 23  2014 good.jpg
-rw-r--r--  1 kali kali 1070 Jun 23  2014 government.jpg
-rw-r--r--  1 kali kali 1070 Jun 23  2014 I.jpg
-rw-r--r--  1 kali kali 1070 Jun 23  2014 in.jpg
-rw-r--r--  1 kali kali 5436 Jun 23  2014 NSA.jpg
-rw-r--r--  1 kali kali 5436 Jun 23  2014 rights.jpg
-rw-r--r--  1 kali kali 5436 Jun 23  2014 security.jpg
```

Figure 12: Contents of sandofwhich.zip

However, the investigator could not open any of the files except “I.jpg” (Figure 13) and came to the conclusion that the files were fragmented with “I.jpg” being the start of the image.

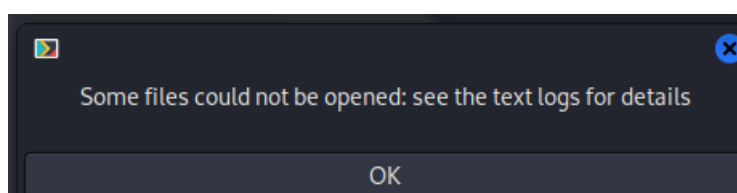


Figure 13: Unable to open unzipped images.

Getting all of the fragmented images

Due to this discovery the investigator went back to the capture to extract the second zip file discovered “ojd34.zip”. The same method of extraction was used, with the first packet of the “ojd34.zip” selected and its TCP Stream followed (Figure 14). The data was changed to raw and saved as “ojd34.raw” (Figure 15 on the next page).

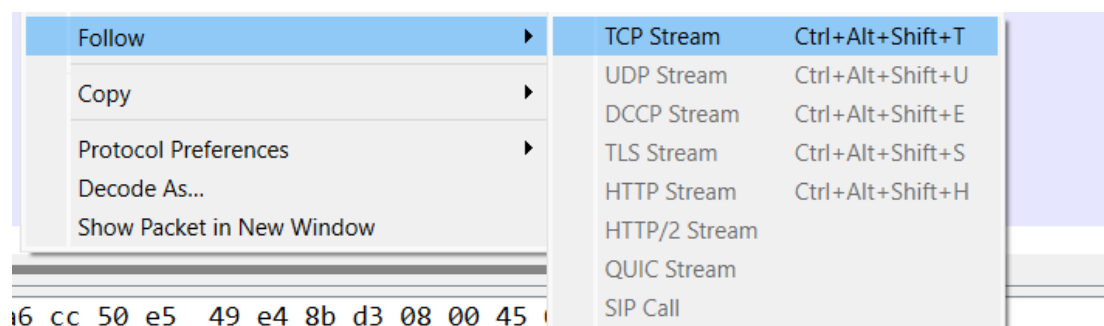


Figure 14: Following TCP stream for “ojd34.zip”

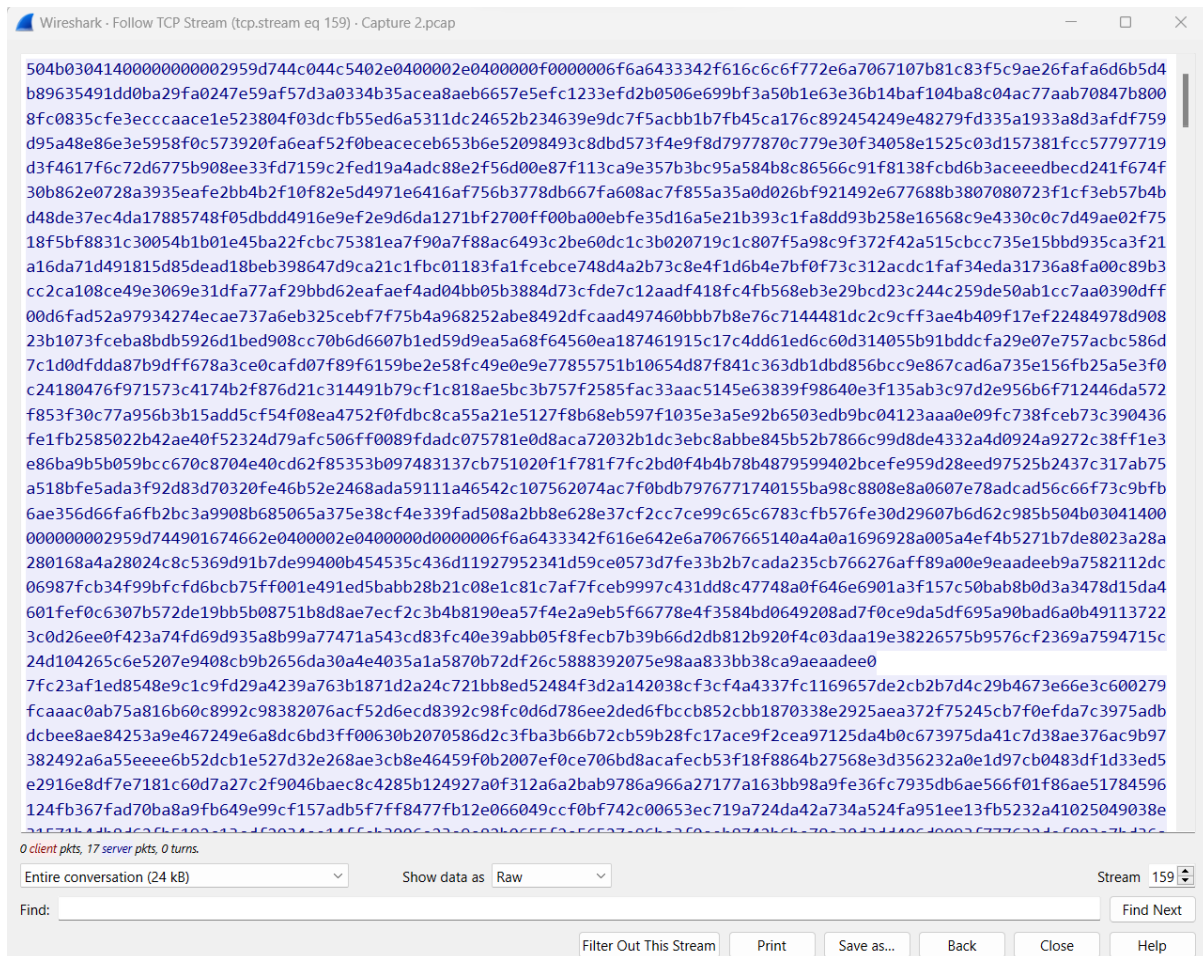


Figure 15: Saving ojd34.zip as Raw data.

After successfully extracting the second zip file, the file command executed confirmed it was a Zip archive just like the first zip file (Figure 16). The investigator simply unzipped the “ojd34.raw” Zip archive which revealed the second half of the fragmented images (Figure 17).

```
(kali@kali)-[~/Desktop]
$ file ojd34.raw
ojd34.raw: Zip archive data, at least v2.0 to extract, compression method=store
```

Figure 16: Executing file command on the ojd34.raw file to confirm it's a Zip archive.

```
(kali@kali)-[~/Desktop]
$ unzip ojd34.raw
Archive:  ojd34.raw
  extracting: ojd34/allow.jpg
  extracting: ojd34/and.jpg
  extracting: ojd34/around.jpg
  extracting: ojd34/basic.jpg
    inflating: ojd34/building.jpg
    inflating: ojd34/cant.jpg
  extracting: ojd34/conscience.jpg
  extracting: ojd34/terrorism.jpg
  extracting: ojd34/Watergate.jpg
  extracting: ojd34/web-based.jpg
```

Figure 17: unzipping the ojd34.zip file

```
(kali㉿kali)~[~/Desktop/ojd34]
$ ls -la
total 60
drwxr-xr-x  2 kali kali 4096 Dec 12 01:04 .
drwxr-xr-x 19 kali kali 4096 Dec 12 01:04 ..
-rw-r--r--  1 kali kali 1070 Jun 23 2014 allow.jpg
-rw-r--r--  1 kali kali 1070 Jun 23 2014 and.jpg
-rw-r--r--  1 kali kali 1070 Jun 23 2014 around.jpg
-rw-r--r--  1 kali kali 1070 Jun 23 2014 basic.jpg
-rw-r--r--  1 kali kali 1051 Jun 23 2014 building.jpg
-rw-r--r--  1 kali kali 1070 Jun 23 2014 cant.jpg
-rw-r--r--  1 kali kali 1070 Jun 23 2014 conscience.jpg
-rw-r--r--  1 kali kali 5436 Jun 23 2014 terrorism.jpg
-rw-r--r--  1 kali kali 5436 Jun 23 2014 Watergate.jpg
-rw-r--r--  1 kali kali 5436 Jun 23 2014 web-based.jpg
```

Figure 18: ojd34.zip's images

Again, the images were unable to be opened by the investigator confirming the images had been fragmented requiring reconstruction (Figure 19).

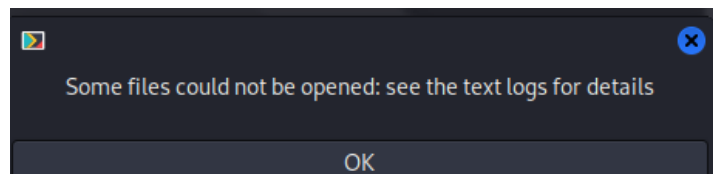


Figure 19: Unable to open any of "ojd34.zip's images.

Reconstructing the images

The investigator was provided with information that some anti-forensic practices have been used to hide information sent. Which explained the suspicious files that had been extracted. A tip told the investigation team that an Edward Snowden quote may help decipher the contents of the images.

As the base image for the fragmented image starts with "I", a popular Edward Snowden quote was researched with this beginning (Figure 20).

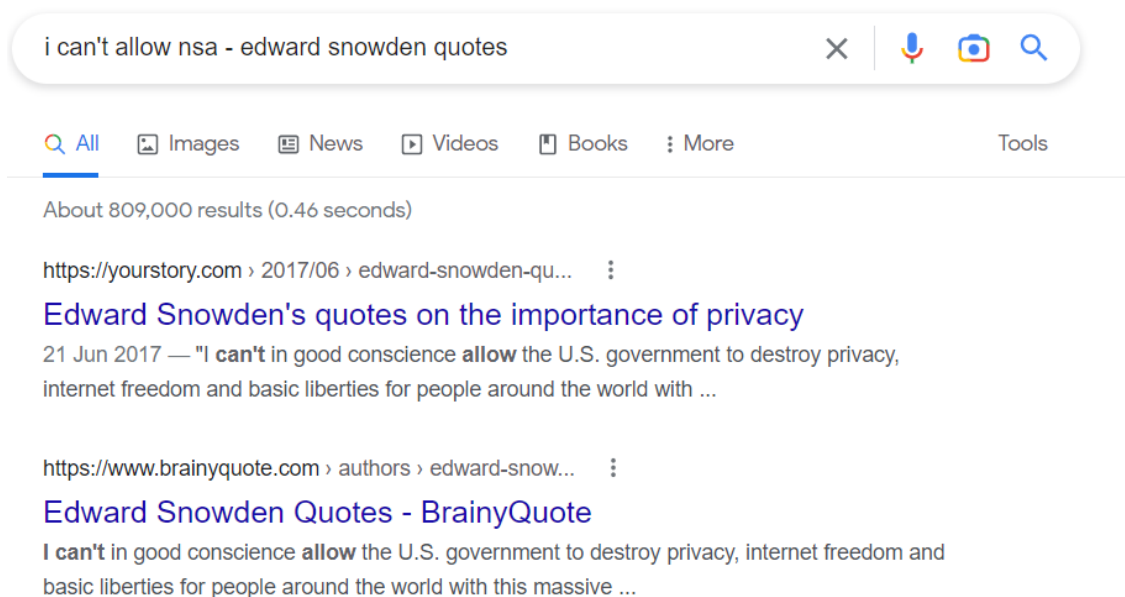


Figure 20: Edward Snowden quote

The full quote matching the image names found is below (See Figure 21 also):

"I can't in good conscience allow the U.S. government to destroy privacy, internet freedom and basic liberties for people around the world with this massive surveillance machine they're secretly building." – Edward Snowden (BrainyQuote, n.d)

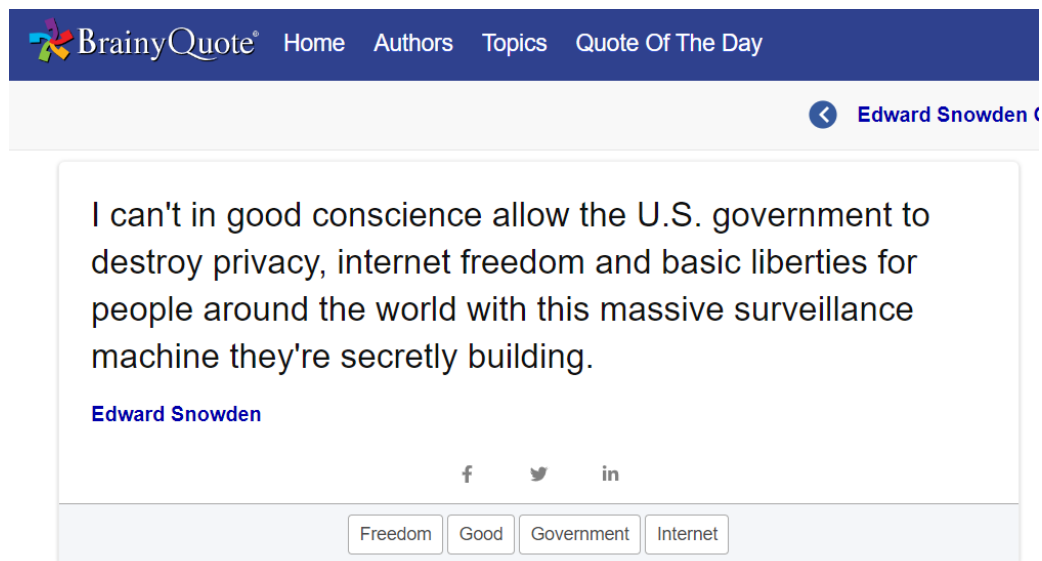


Figure 21: Edward Snowden Quote.

This quote fits the order of the base image and multiple image names obtained. Now it is just reconstructing in the order of the quote starting with "I.jpg". However, the investigator did not have all the images to reconstruct the quote with "the.jpg" missing.(See figure 22).

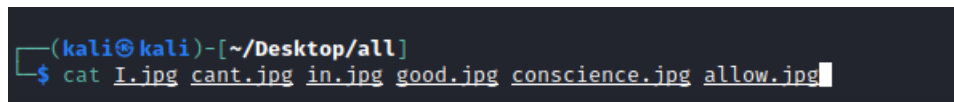


Figure 22: Incomplete images for reconstruction.

To find the missing images the capture was searched for any .zip files using the ngrep tool with the command "`ngrep -I Capture\ 2.pcap ".zip" | grep -E -o ".{0,0}filename=.{0,26}"`". (See figure 23 and Appendix B). From the output three more zip files were discovered (Figure 23). "34jdsioj.zip", "breaking_bad_season_6.zip" and "canc3l.zip".

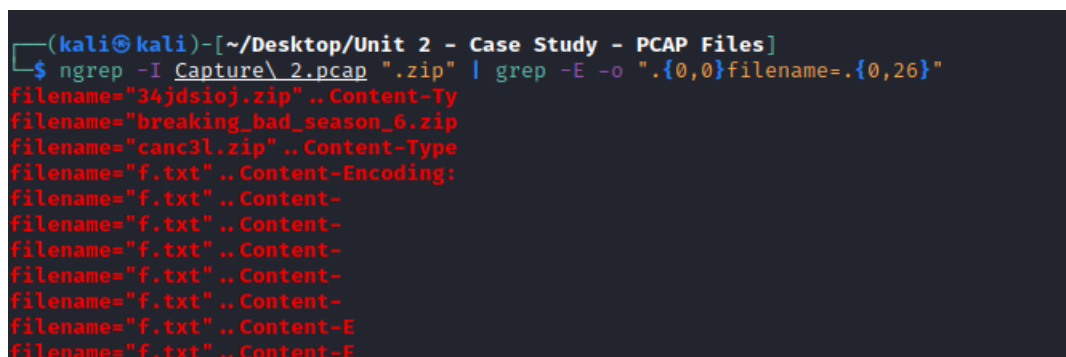


Figure 23: Finding 3 more .zip files within capture 2.

Within Wireshark, a string search was performed by Edit -> Find Packet and entering the format of the filename “ *filename=“34jdsioj.zip”*”(Figure 24).

The screenshot shows the Wireshark interface with a search filter applied: `filename="34jdsioj.zip"`. The packet list displays several HTTP POST requests to `/38602-516/aol-6/en-us/common/rpc/RPC.aspx?user=XYqMriCaSe&tran`. The packet details pane shows the selected packet (No. 8491) with the following structure:

- File Data: 45969 bytes
- MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "-----506390528859906812396841278\r\n"
- First boundary: "-----506390528859906812396841278\r\n"
- Encapsulated multipart part: (application/zip)
- Content-Disposition: form-data; name="file0"; filename="34jdsioj.zip"\r\n

The packet bytes pane shows the raw data of the selected packet, including the Content-Disposition header and the file data.

Figure 24: Searching for string “filename=“34jdsioj.zip”

The packet highlighted was selected and its TCP stream followed (Figure 25).

The screenshot shows the Wireshark packet details pane with the selected packet (No. 8491) highlighted. The packet details pane shows the selected packet (No. 8491) with the following structure:

- File Data: 45969 bytes
- MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "-----506390528859906812396841278\r\n"
- First boundary: "-----506390528859906812396841278\r\n"
- Encapsulated multipart part: (application/zip)
- Content-Disposition: form-data; name="file0"; filename="34jdsioj.zip"\r\n

The packet bytes pane shows the raw data of the selected packet, including the Content-Disposition header and the file data.

Figure 25: Following TCP stream for 34jdsioj.zip

Next the data was filtered on communication between Ip addresses `172.29.1.21:48055` and `54.12.132.39:80` and saved as “Raw” into a filename “34jdsioj.raw” (Figure 26).

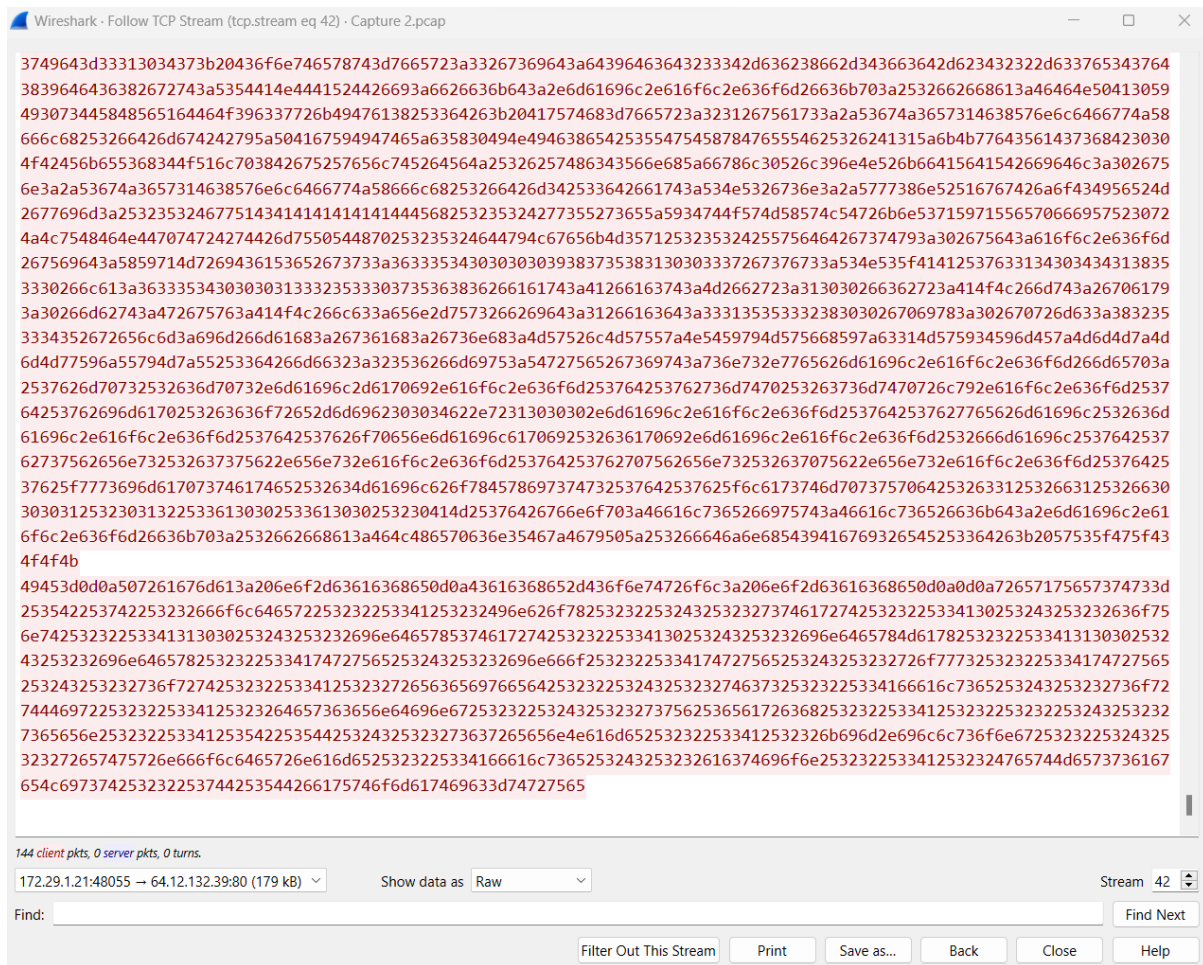


Figure 26: Saving TCP stream of 34jdsioj.zip as Raw.

Once extracted the raw data was unzipped using “*unzip 34jdsioj.raw*” (Figure 27)

```
(kali㉿kali)-[~/Desktop]
$ unzip 34jdsioj.raw
Archive: 34jdsioj.raw
warning [34jdsioj.raw]: 126409 extra bytes at beginning or within zipfile
(attempting to process anyway)
  inflating: canc3l/American.jpg
  extracting: canc3l/behind.jpg
  extracting: canc3l/closed.jpg
  inflating: canc3l/condone.jpg
  extracting: canc3l/constructing.jpg
  extracting: canc3l/internet.jpg
  extracting: canc3l/people.jpg
  extracting: canc3l/privacy.jpg
  extracting: canc3l/secretly.jpg
  extracting: canc3l/surveillance.jpg
  extracting: canc3l/to.jpg
  extracting: canc3l/U.S..jpg
```

Figure 27: Unzipping 34jdsioj.raw

```
(kali@kali)-[~/Desktop]
$ ls -la canc3l
total 76
drwxr-xr-x  2 kali kali 4096 Dec 12 19:16 .
drwxr-xr-x 21 kali kali 4096 Dec 12 19:16 ..
-rw-r--r--  1 kali kali 5436 Jun 23 2014 American.jpg
-rw-r--r--  1 kali kali 5436 Jun 23 2014 behind.jpg
-rw-r--r--  1 kali kali 5436 Jun 23 2014 closed.jpg
-rw-r--r--  1 kali kali 5436 Jun 23 2014 condone.jpg
-rw-r--r--  1 kali kali 5436 Jun 23 2014 constructing.jpg
-rw-r--r--  1 kali kali 1070 Jun 23 2014 internet.jpg
-rw-r--r--  1 kali kali 1070 Jun 23 2014 people.jpg
-rw-r--r--  1 kali kali 1070 Jun 23 2014 privacy.jpg
-rw-r--r--  1 kali kali 1070 Jun 23 2014 secretly.jpg
-rw-r--r--  1 kali kali 1070 Jun 23 2014 surveillance.jpg
-rw-r--r--  1 kali kali 1070 Jun 23 2014 to.jpg
-rw-r--r--  1 kali kali 1070 Jun 23 2014 U.S..jpg
```

Figure 28: 34jdsioj.zip's images

However, the other two zip files discovered were not extracted so the investigator used the tool "binwalk" and command "*binwalk -e 34jdsioj.raw*" to fully extract all zip files contained within the raw data (Figure 29).

```
(kali@kali)-[~/Desktop]
$ binwalk -e 34jdsioj.raw
```

DECIMAL	HEXADECFIMAL	DESCRIPTION
25130	0x622A	Zip archive data, at least v2.0 to extract, compressed size: 5436, uncompressed size: 5436, name: 34jdsioj/corrupt.jpg
30616	0x7798	Zip archive data, at least v2.0 to extract, compressed size: 5435, uncompressed size: 5435, name: 34jdsioj/doors.jpg
36099	0x8D03	Zip archive data, at least v2.0 to extract, compressed size: 5436, uncompressed size: 5436, name: 34jdsioj/human.jpg
41583	0xA26F	Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: 34jdsioj/liberties.jpg
42705	0xA6D1	Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: 34jdsioj/machine.jpg
43825	0xAB31	Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: 34jdsioj/massive.jpg
44945	0xAF91	Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: 34jdsioj/the.jpg
46061	0xB3ED	Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: 34jdsioj/theyre.jpg
47180	0xB84C	Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: 34jdsioj/this.jpg
48297	0xBCA9	Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: 34jdsioj/with.jpg
49414	0xC106	Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: 34jdsioj/world.jpg
51243	0xC82B	End of Zip archive, footer length: 22
51442	0xC8F2	Zip archive data, at least v2.0 to extract, compressed size: 1454, uncompressed size: 1454, name: breaking_bad_season_6/a.jpg
52953	0xCED9	Zip archive data, at least v2.0 to extract, compressed size: 1454, uncompressed size: 1454, name: breaking_bad_season_6/because.jpg
54470	0xD4C6	Zip archive data, at least v2.0 to extract, compressed size: 1454, uncompressed size: 1454, name: breaking_bad_season_6/but.jpg
55983	0xDAAF	Zip archive data, at least v2.0 to extract, compressed size: 1454, uncompressed size: 1454, name: breaking_bad_season_6/communism.jpg
57502	0xE09E	Zip archive data, at least v2.0 to extract, compressed size: 1454, uncompressed size: 1454, name: breaking_bad_season_6/it.jpg
59014	0xE686	Zip archive data, at least v2.0 to extract, compressed size: 1454, uncompressed size: 1454, name: breaking_bad_season_6/nor.jpg
60527	0xEC6F	Zip archive data, at least v2.0 to extract, compressed size: 1444, uncompressed size: 1444, name: breaking_bad_season_6/secret.jpg
62033	0xF251	Zip archive data, at least v2.0 to extract, compressed size: 1454, uncompressed size: 1454, name: breaking_bad_season_6/secretive.jpg
63552	0xF840	Zip archive data, at least v2.0 to extract, compressed size: 1454, uncompressed size: 1454, name: breaking_bad_season_6/their.jpg
65067	0xFE2B	Zip archive data, at least v2.0 to extract, compressed size: 1291, uncompressed size: 1454, name: breaking_bad_season_6/there.jpg
66419	0x10373	Zip archive data, at least v2.0 to extract, compressed size: 1454, uncompressed size: 1454, name: breaking_bad_season_6/unconstitutional.jpg
68803	0x10CC3	End of Zip archive, footer length: 22
126409	0x1EDC9	Zip archive data, at least v2.0 to extract, compressed size: 5426, uncompressed size: 5436, name: canc3l/American.jpg
131884	0x2032C	Zip archive data, at least v2.0 to extract, compressed size: 5436, uncompressed size: 5436, name: canc3l/behind.jpg
137367	0x21897	Zip archive data, at least v2.0 to extract, compressed size: 5436, uncompressed size: 5436, name: canc3l/closed.jpg
142850	0x22E02	Zip archive data, at least v2.0 to extract, compressed size: 5093, uncompressed size: 5436, name: canc3l/condone.jpg
147991	0x24217	Zip archive data, at least v2.0 to extract, compressed size: 5436, uncompressed size: 5436, name: canc3l/constructing.jpg
153480	0x25788	Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: canc3l/internet.jpg
154599	0x258E7	Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: canc3l/people.jpg
155716	0x26044	Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: canc3l/privacy.jpg
156834	0x264A2	Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: canc3l/secretly.jpg
157953	0x26901	Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: canc3l/surveillance.jpg
159076	0x26D64	Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: canc3l/to.jpg
160189	0x271BD	Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: canc3l/U.S..jpg
162074	0x2791A	End of Zip archive, footer length: 22

Figure 29: Using binwalk tool to fully extract all archives

Finally, all images were placed into one single folder ready for image reconstruction (Figure 30).

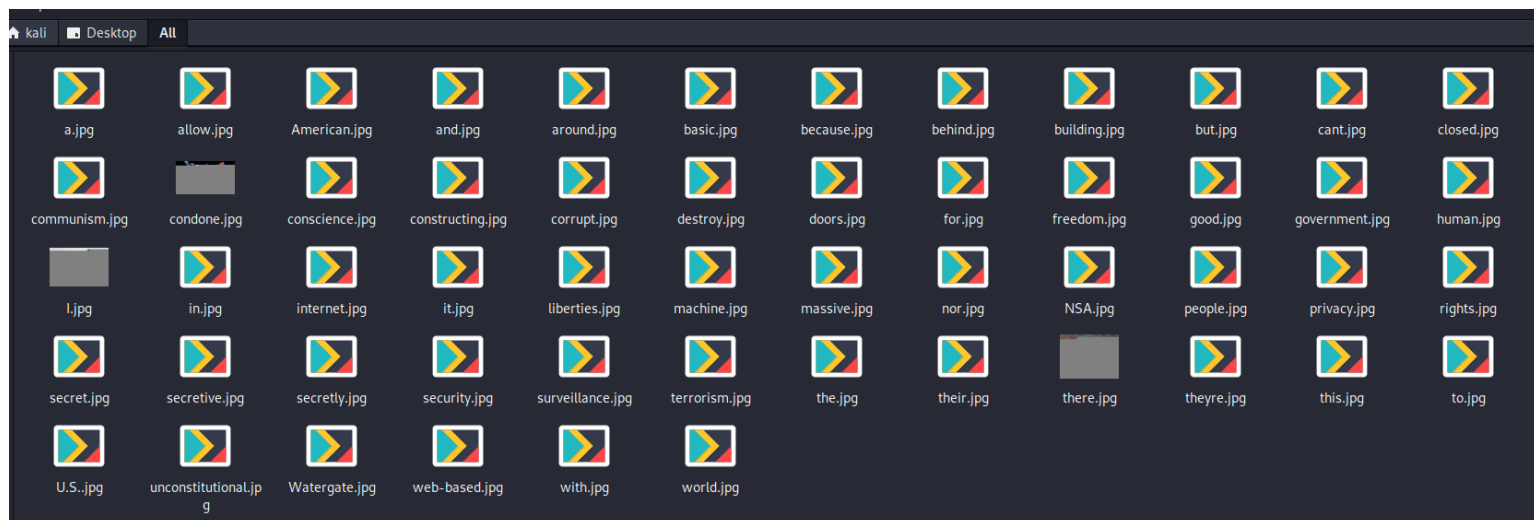


Figure 30: All images placed into one single folder

Reconstructing the images

The investigator simply used the previously discovered quote to reconstruct the image using “cat” and outputting to an image (Figure 31 and Appendix B).

```
(kali@kali)-[~/Desktop/All]
$ cat I.jpg cant.jpg in.jpg good.jpg conscience.jpg allow.jpg the.jpg U.S..jpg government.jpg t
o.jpg destroy.jpg privacy.jpg internet.jpg freedom.jpg and.jpg basic.jpg liberties.jpg for.jpg pe
ople.jpg around.jpg world.jpg with.jpg this.jpg massive.jpg surveillance.jpg machine.jpg theyre.j
pg secretly.jpg building.jpg > snowden.jpg
```

Figure 31: Command to reconstruct the Snowden image.



Figure 32: Snowden image fully reconstructed showing a chess board

The item the corrupt official received must have been this chess board. Although the main image had been reconstructed thanks to the tip it appeared there were two other images that had been fragmented.

Second image – Kim

A base image “there.jpg” could be opened to see the beginning of the image (Figure 33). The investigator tried connecting with one other image to see the second piece of the image (Figure 34). Doing so got the second piece of the image reconstructed (Figure 35)



Figure 33: “there.jpg”

```
(kali㉿kali)-[~/Desktop/_34jdsioj.raw.extracted/breaking_bad_season_6]
$ cat there.jpg their.jpg > test.jpg
```

Figure 34: cat command on two images for test



Figure 35: Partially reconstructed “test.jpg” image

The investigator simply pieced the puzzle of fragmented images together until it was fully reconstructed (Figure 36 and Appendix B).

```
(kali㉿kali)-[~/Desktop/All]
$ cat there.jpg their.jpg a.jpg it.jpg but.jpg communism.jpg nor.jpg because.jpg unconstitution
al.jpg secretive.jpg secret.jpg > image2.jpg
```

Figure 36: Second image reconstructed command.

The reconstructed image is a picture of Kim Jong-un and can be seen in Figure 37 and Appendix B, Figure 3.



Figure 37: Kim Jong-un image

Third image - Robot

A base image “condone.jpg” could be opened to see the beginning of the image (Figure 38).



Figure 38: condone.jpg base image

The investigator used the same method to reconstruct this image (Figures 39 and 40).

```
(kali@kali)-[~/Desktop/_34jdsioj.raw.extracted/canc3l]  
$ cat condone.jpg American.jpg > test3.jpg
```

Figure 39: cat command to test reconstruction



Figure 40: Partially reconstructed third image.

The investigator simply pieced the puzzle of fragmented images together until it was fully reconstructed (Figure 41 and Appendix B).

```
(kali㉿kali)-[~/Desktop/All]  
$ cat condone.jpg American.jpg web-based.jpg rights.jpg constructing.jpg security.jpg terrorism  
.jpg NSA.jpg Watergate.jpg corrupt.jpg human.jpg behind.jpg closed.jpg doors.jpg > image3.jpg
```

Figure 41: Third image reconstructed command.

The reconstructed image is a picture of a robot and can be seen in Figure 42 and Appendix B, Figure .



Figure 42: Robot image reconstructed.

Reconstructing all fragmented images were particularly challenging to the investigator due to the methods used by the suspects. This shows that anti-forensic practices can impede investigator attempts at successfully retrieving information quickly.

Capture 3.pcap

Communication traffic between Ill-Song and a known person of interest taking part in the international competition—Ann Dercover.

The investigator first began investigating the third capture by using the tool ngrep, and the command “*ngrep -I Capture\ 3.pcap “Ill-Song”*” to get packets from the capture.

```
(kali@kali)-[~/Desktop/Unit 2 - Case Study - PCAP Files]
$ ngrep -I Capture\ 3.pcap "Ill-Song"
input: Capture 3.pcap
filter: ((ip || ip6) || (vlan 86 (ip || ip6)))
match (JIT): Ill-Song
```

Figure 43: ngrep command searching for “Ill-Song”

The output returned two IP addresses “192.168.1.5 and 199.87.160.87” (Figure 44 and Appendix C).

```
T 192.168.1.5:39312 → 199.87.160.87:80 [AP] #3777
POST /1.0/messages/text/send?lang=en-US HTTP/1.1..x-rest-method: POST..Content-Type: application/json..X-Install-Id: 6965edb59a7b2
android,4.2.2..x-uid: 580781709..x-gid: 0..Authorization: OAuth realm="http://api.pinger.com", oauth_consumer_key="580781709%3Bt
re_method="HMAC-SHA1", oauth_timestamp="1404340884", oauth_nonce="yllcitpdjfmkqpr", oauth_signature="LT%2FKyayOPT8%2BZxTUKw0wFudNx
: Keep-Alive..User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)...{"senderId":"14068522589","senderName":"Ann","recipientId":"+
investigating Kim Ill-Song?","senderType":"phone","sendAsSms":0,"recipientType":"phone"}
```

Figure 44: ngrep output for “Ill-Song”

A Wireshark filter was then applied, “*ip.addr==192.168.1.5 and ip.addr==199.87.160.87 && http*”, to show communication between the two suspects (Figure 45). HTTP/JSON protocol packets displayed “messageText” between suspects (Figure 46).

ip.addr==192.168.1.5 and ip.addr==199.87.160.87 && http						
No.	Time	Source	Destination	Protocol	Length	Info
2089	42.963288	192.168.1.5	199.87.160.87	HTTP/JSON	823	POST /1.0/log/exit HTTP/1.1 , JavaScript Object Notation (appli
2098	42.971040	192.168.1.5	199.87.160.87	HTTP	719	POST /1.0/my HTTP/1.1
2099	42.971055	192.168.1.5	199.87.160.87	HTTP/JSON	847	POST /1.0/marketingOpeningSequence HTTP/1.1 , JavaScript Object
2134	43.112337	199.87.160.87	192.168.1.5	HTTP/JSON	291	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
2141	43.122797	199.87.160.87	192.168.1.5	HTTP/JSON	1387	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
2148	43.138521	199.87.160.87	192.168.1.5	HTTP/JSON	319	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
2499	48.844239	192.168.1.5	199.87.160.87	HTTP	732	POST /1.0/account/hideAds HTTP/1.1
2500	48.844256	192.168.1.5	199.87.160.87	HTTP	728	POST /1.0/voice/balance HTTP/1.1
2505	48.845580	192.168.1.5	199.87.160.87	HTTP/JSON	802	POST /1.0/communications?startIndex=0&since=2014-07-02+22%3A34%3
2532	48.999278	199.87.160.87	192.168.1.5	HTTP/JSON	322	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
2539	49.019300	199.87.160.87	192.168.1.5	HTTP/JSON	355	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
2541	49.022687	199.87.160.87	192.168.1.5	HTTP/JSON	1158	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
2604	49.283285	192.168.1.5	199.87.160.87	HTTP	761	POST /1.0/account/contacts?since=2014-07-02+22%3A36%3A26 HTTP/1.
2605	49.283302	192.168.1.5	199.87.160.87	HTTP/JSON	876	POST /1.0/communications HTTP/1.1 , JavaScript Object Notation (
2617	49.423275	199.87.160.87	192.168.1.5	HTTP/JSON	366	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
2632	49.441621	199.87.160.87	192.168.1.5	HTTP/JSON	296	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
2731	53.099438	192.168.1.5	199.87.160.87	HTTP/JSON	802	POST /1.0/communications?startIndex=0&since=2014-07-02+22%3A38%3
2776	53.351262	199.87.160.87	192.168.1.5	HTTP/JSON	851	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
2811	53.581443	192.168.1.5	199.87.160.87	HTTP	763	POST /1.0/account/contacts?since=2014-07-02+22%3A37%3A31 HTTP/1.
2836	53.734750	199.87.160.87	192.168.1.5	HTTP/JSON	366	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)

Figure 45: HTTP/JSON protocol

```
[Path with value: /result/recMessages/[]/messageType]
▼ Member: messageText
[Path with value: /result/recMessages/[]/messageText:What day?]
[Member with value: messageText:What day?]
String value: What day?
Key: messageText
```

Figure 46: messageText value in packets

Ngrep was used again to filter the capture to find all values of “messageText” (Figure 47). For the command used, see appendix C “all_messageText.txt” and “Filtered messageText only”.


```
(kali㉿kali)-[~/Desktop/Unit 2 - Case Study - PCAP Files]
$ ngrep -I Capture\ 3.pcap "messageText" | grep -E -o ".{0,0}messageText.{0,65}"
messageText
messageText:"Good afternoon, Ann.,"recipientType":"p
messageText:"this is a test","recipientType":"phone","recipientId":"1406924
messageText:"Good afternoon, Ann.,"recipientType":"p
messageText:"this is a test","recipientType":"phone","recipientId":"1406924
messageText:"Good afternoon, Ann.,"recipientType":"p
messageText:"Good afternoon, Ann.,"recipientType":"p
messageText:"Good afternoon, Ann.,"recipientType":"phone","r
messageText:"Castling.,"recipientType":"phone","recipientId":"14068522589"
messageText:"Good afternoon, Ann.,"recipientType":"phone","r
messageText:"Castling.,"recipientType":"phone","recipientId":"14068522589"
messageText:"Castling.,"recipientType":"phone","recip
messageText:"Castling.,"recipientType":"phone","recipi
messageText:"where are you?","recipientType":"phone","recipientId":"1406924
messageText:"Castling.,"recipientType":"phone","recipi
messageText:"where are you?","recipientType":"phone","recipientId":"1406924
messageText:"I know I can't tell you that.,"recipient
messageText:"I know I can't tell you that.,"recipientT
messageText:"Do you know that there are people investigating Kim Ill-Song?"
messageText:"I know I can't tell you that.,"recipientT
messageText:"Do you know that there are people investigating Kim Ill-Song?"
messageText:"Of course. However, they will never kno
messageText:"Of course. However, they will never kno
messageText:"Of course. However, they will never kn
messageText:"still we should be careful. Pay attention. I
messageText:"Of course. However, they will never kn
messageText:"still we should be careful. Pay attention. I
messageText:"At our old meetup spot?","recipientType":
messageText:"At our old meetup spot?","recipientType":
messageText:"At our old meetup spot?","recipientType":"phone",
messageText:"What day?","recipientType":"phone","recipientId":"14068522589"
messageText:"At our old meetup spot?","recipientType":"phone",
messageText:"What day?","recipientType":"phone","recipientId":"14068522589"
messageText:"What day?","recipientType":"phone","recip
messageText:"What day?","recipientType":"phone","recip
messageText:"What day?","recipientType":"phone","recip
messageText:"I told you to pay attention.,"recipientType":"phone","recipie
messageText:"What day?","recipientType":"phone","recip
messageText:"I told you to pay attention.,"recipientType":"phone","recipie
```

Figure 47: Ngrep Filtered capture containing message conversation

The messages were then reconstructed into a legible conversation by the investigator from this information.

Details of conversation

Messages:

1. Sender Name: Kim Ill-song
Message: **Good afternoon, Ann.**
2. Sender Name: Ann
Message: **who is this?**
3. Sender Name: Kim Ill-Song
Message: **Castling.**
4. Sender Name : Ann
Message: **where are you?**
5. Sender Name: Kim Ill-Song
Message: **I know I can't tell you that.**
6. Sender Name: Ann
Message: **Do you know that there are people investigating Kim Ill-Song?**
7. Sender Name: Kim Ill-Song
Message: **Of course. However, they will never know it is me behind the bribes.**
8. Sender Name: Ann
Message: **still we should be careful. Pay attention. I want to meet in September at 5PM.**
9. Sender: Kim Ill-Song

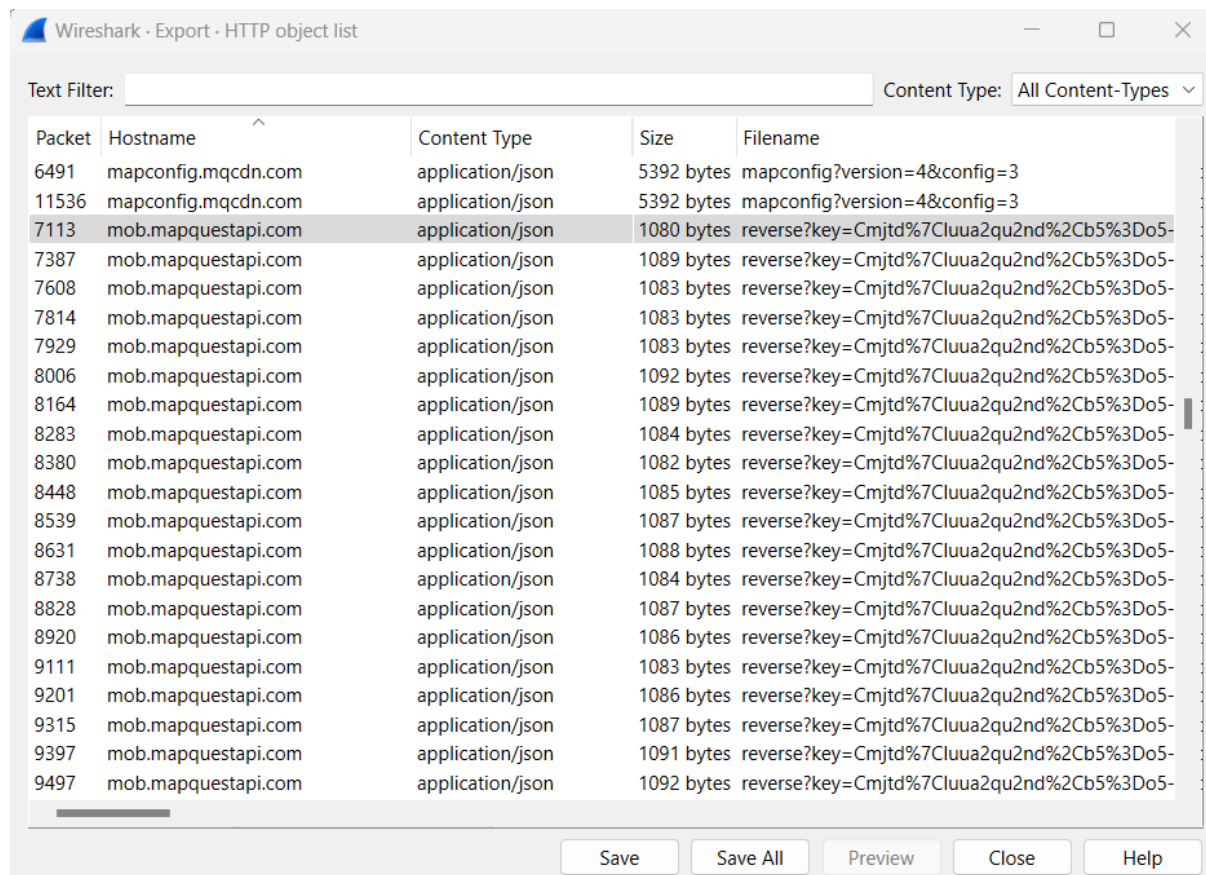
- Message: **At our old meetup spot?**
10. Sender Name: Ann
Message: **yes**
11. Sender Name: Kim Ill-Song
Message: **What day?**
12. Sender Name: Ann
Message: **I told you to pay attention**

When suspects plan to meet

It's clear from the conversation that the suspects plan to meet in September at 5PM. However, Ann held back which day to meet as they were suspicious of an investigation currently taking place. To retrieve the day of the meeting further investigation was needed.

Finding the day of the meeting

The investigator went back to the capture and used “*Export HTTP objects*”. Noticed a map api host called “*mob.mapquestapi.com*” (Figure 48). After inspection it contained Latitude and Longitude coordinates.



Packet	Hostname	Content Type	Size	Filename
6491	mapconfig.mqcdn.com	application/json	5392 bytes	mapconfig?version=4&config=3
11536	mapconfig.mqcdn.com	application/json	5392 bytes	mapconfig?version=4&config=3
7113	mob.mapquestapi.com	application/json	1080 bytes	reverse?key=Cmjtd%7Cluaa2qu2nd%2Cb5%3Do5-
7387	mob.mapquestapi.com	application/json	1089 bytes	reverse?key=Cmjtd%7Cluaa2qu2nd%2Cb5%3Do5-
7608	mob.mapquestapi.com	application/json	1083 bytes	reverse?key=Cmjtd%7Cluaa2qu2nd%2Cb5%3Do5-
7814	mob.mapquestapi.com	application/json	1083 bytes	reverse?key=Cmjtd%7Cluaa2qu2nd%2Cb5%3Do5-
7929	mob.mapquestapi.com	application/json	1083 bytes	reverse?key=Cmjtd%7Cluaa2qu2nd%2Cb5%3Do5-
8006	mob.mapquestapi.com	application/json	1092 bytes	reverse?key=Cmjtd%7Cluaa2qu2nd%2Cb5%3Do5-
8164	mob.mapquestapi.com	application/json	1089 bytes	reverse?key=Cmjtd%7Cluaa2qu2nd%2Cb5%3Do5-
8283	mob.mapquestapi.com	application/json	1084 bytes	reverse?key=Cmjtd%7Cluaa2qu2nd%2Cb5%3Do5-
8380	mob.mapquestapi.com	application/json	1082 bytes	reverse?key=Cmjtd%7Cluaa2qu2nd%2Cb5%3Do5-
8448	mob.mapquestapi.com	application/json	1085 bytes	reverse?key=Cmjtd%7Cluaa2qu2nd%2Cb5%3Do5-
8539	mob.mapquestapi.com	application/json	1087 bytes	reverse?key=Cmjtd%7Cluaa2qu2nd%2Cb5%3Do5-
8631	mob.mapquestapi.com	application/json	1088 bytes	reverse?key=Cmjtd%7Cluaa2qu2nd%2Cb5%3Do5-
8738	mob.mapquestapi.com	application/json	1084 bytes	reverse?key=Cmjtd%7Cluaa2qu2nd%2Cb5%3Do5-
8828	mob.mapquestapi.com	application/json	1087 bytes	reverse?key=Cmjtd%7Cluaa2qu2nd%2Cb5%3Do5-
8920	mob.mapquestapi.com	application/json	1086 bytes	reverse?key=Cmjtd%7Cluaa2qu2nd%2Cb5%3Do5-
9111	mob.mapquestapi.com	application/json	1083 bytes	reverse?key=Cmjtd%7Cluaa2qu2nd%2Cb5%3Do5-
9201	mob.mapquestapi.com	application/json	1086 bytes	reverse?key=Cmjtd%7Cluaa2qu2nd%2Cb5%3Do5-
9315	mob.mapquestapi.com	application/json	1087 bytes	reverse?key=Cmjtd%7Cluaa2qu2nd%2Cb5%3Do5-
9397	mob.mapquestapi.com	application/json	1091 bytes	reverse?key=Cmjtd%7Cluaa2qu2nd%2Cb5%3Do5-
9497	mob.mapquestapi.com	application/json	1092 bytes	reverse?key=Cmjtd%7Cluaa2qu2nd%2Cb5%3Do5-

Figure 48: “*mob.mapquestapi.com*” hostname

The investigator filtered this host name in the pcap3 capture using ngrep again which displayed all coordinates (Figure 49). See Appendix C for the command used and the full list of coordinates.

```

(kali@kali)-[~/Desktop/Unit 2 - Case Study - PCAP Files]
$ ngrep -I Capture\ 3.pcap "mob.mapquestapi.com" | grep -E -o ".{0,0}location.{0,45}"
location=46.85661315917969%2C-114.01860809326172 HTTP
location=46.85661315917969%2C-114.01860809326172 HTTP
location=46.85693359375%2C-114.01863098144531 HTTP/1.
location=46.85693359375%2C-114.01863098144531 HTTP/1.
location=46.85727310180664%2C-114.01868438720703 HTTP
location=46.85727310180664%2C-114.01868438720703 HTTP
location=46.857601165771484%2C-114.01866912841797 HTT
location=46.857601165771484%2C-114.01866912841797 HTT
location=46.858055114746094%2C-114.01866149902344 HTT
location=46.858055114746094%2C-114.01866149902344 HTT
location=46.8582878112793%2C-114.01864624023438 HTTP/
location=46.8582878112793%2C-114.01864624023438 HTTP/
location=46.858524322509766%2C-114.01863861083984 HTT
location=46.858524322509766%2C-114.01863861083984 HTT
location=46.858734130859375%2C-114.01864624023438 HTT

```

Figure 49: Filtering capture based on map api to find coordinates.

Finally, all that was left was to plot the coordinates on a map. The investigator used an online coordinate plotter to achieve this (mobisoftinfotech n.d). The coordinates discovered were entered into the tool (Figure 50). The plotted coordinates revealed the number “17” on the map (Figure 51).

Paste/Enter Geo Points Details

46.85661315917969,-114.01860809326172 ,
46.85661315917969,-114.01860809326172 ,
46.85693359375,-114.01863098144531 ,
46.85693359375,-114.01863098144531 ,
46.85727310180664,-114.01868438720703 ,
46.85727310180664,-114.01868438720703 ,
46.857601165771484,-114.01866912841797 ,
46.857601165771484,-114.01866912841797 ,
46.858055114746094,-114.01866149902344 ,
46.858055114746094,-114.01866149902344

☐ Show Point Numbers
☐ Show Lines

Update Map

Figure 50: Plotting discovered coordinates

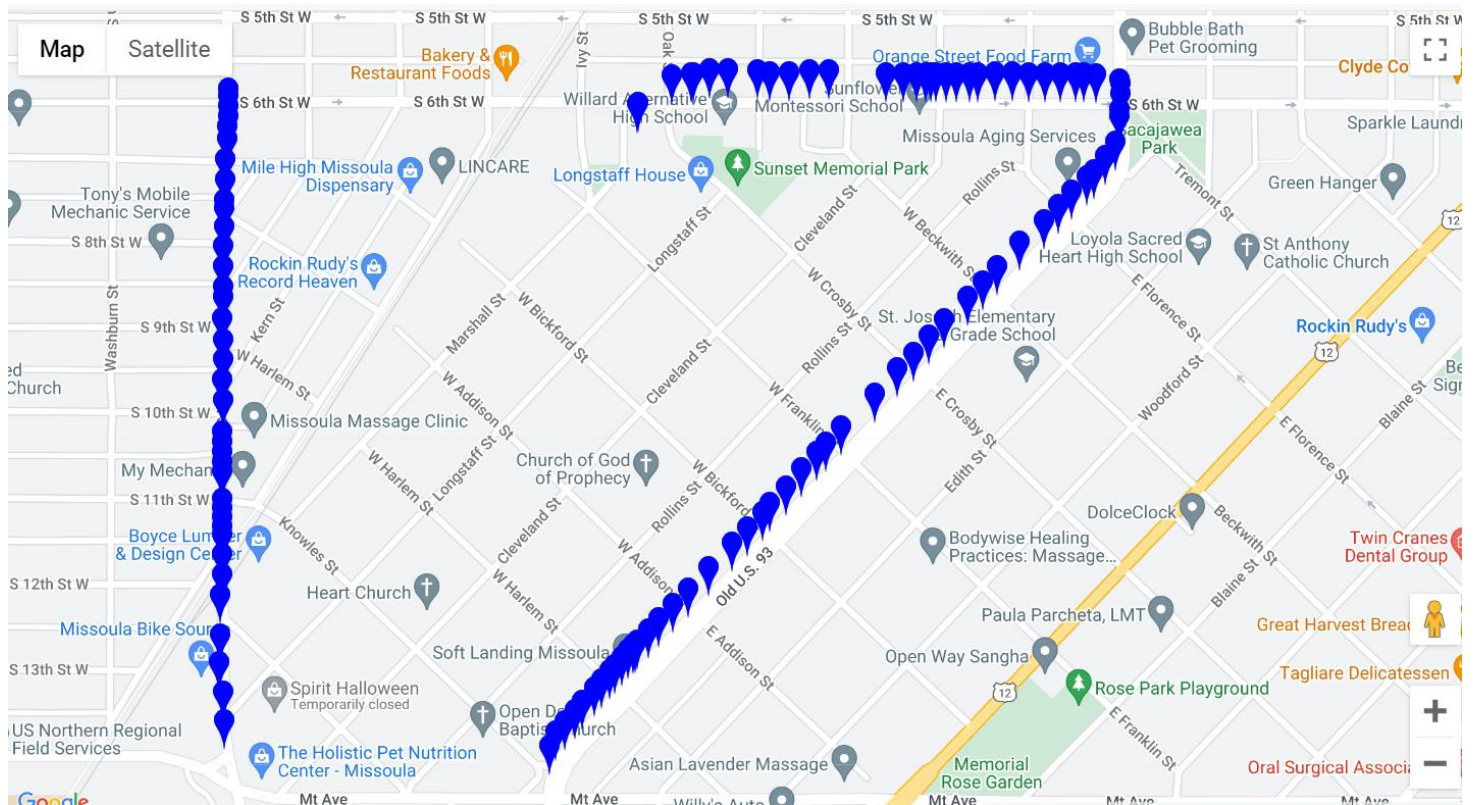


Figure 51: Number 17 displayed from coordinates.

It's reasonable to gather from this information that Ann Dercover and Kim Ill-Song are planning to meet on the 17th of September 2014 at 5PM.

The investigator found that reconstructing communications between Ann and Kim were particularly challenging. There wasn't any anti-forensic methods used by the suspects for the first part, as the conversation was pieced together relatively quickly. However, one of the suspects chose to obscure the day on which to meet by using coordinates. The investigator took a significant time to find these coordinates, carving it from the packets and finally plotting it on a map to reveal the day.

Methods used to hide information significantly increases the time it takes to do a forensic investigation, which is vital information considering this meetup would be happening soon. If the forensic investigator takes too long to reconstruct, then the meeting would have already taken place and suspects not caught.

Appendices

Appendix A

Track6 - Enter The Wu Tang Clan

VGhIIIE15c3Rlcnkgb2YgQ2hlc3MgQm94aW5nOg0KKHVzZXJuYW1lcykNCg0KTXluIE1ldGhvZA0KDQpLaW0gSWxsLVNvbmcNCg0KTXluIFJhem9yDQoNCk1yLiBHZW5pdXMNCg0KTXluIEcuIEtpbGxhaA0KDQpNYXR0IENhc3NlbaA0KDQpNci4gSS4gRGVjaw0KDQpNci4gTSBLaWxsYQ0KDQpNci4gTy5ELkluDQoNCk1yLiBSYWVrd29uDQoNCk1yLiBVLUdvZA0KDQpNci4gQ2FwcGFkb25uYSAocG9zc2libHkpDQoNCkpvaG4gV29vPw0KDQpNci4gTmFzDQo=

The Mystery of Chess Boxing:

(usernames)

Mr. Method

Kim Ill-Song

Mr. Razor

Mr. Genius

Mr. G. Killah

Matt Cassel

Mr. I. Deck

Mr. M Killa

Mr. O.D.B.

Mr. Raekwon

Mr. U-God

Mr. Cappadonna (possibly)

John Woo?

Mr. Nas

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars ☐ Strict mode

STEP

BAKE!

☒ Auto Bake

Input

start: 69 end: 70 length: 1 length: 344 lines: 1

VGhIIIE15c3Rlcnkgb2YgQ2hlc3MgQm94aW5nOg0KKHVzZXJuYW1lcykNCg0KTXluIE1ldGhvZA0KDQpLaW0gSWxsLVNvbmcNCg0KTXluIFJhem9yDQoNCk1yLiBHZW5pdXMNCg0KTXluIEcuIEtpbGxhaA0KDQpNYXR0IENhc3NlbaA0KDQpNci4gSS4gRGVjaw0KDQpNci4gTSBLaWxsYQ0KDQpNci4gTy5ELkluDQoNCk1yLiBSYWVrd29uDQoNCk1yLiBVLUdvZA0KDQpNci4gQ2FwcGFkb25uYSAocG9zc2libHkpDQoNCkpvaG4gV29vPw0KDQpNci4gTmFzDQo=

Output

start: 52 end: 52 length: 0 time: 1ms length: 257 lines: 31

The Mystery of Chess Boxing:
(usernames)

Mr. Method

Kim Ill-Song

Mr. Razor

Mr. Genius

Mr. G. Killah

Matt Cassel

Mr. I. Deck

Mr. M Killa

Mr. O.D.B.

Mr. Raekwon

Mr. U-God

Figure 1: Decoding base64 of track6 Usernames

Track 10 – Enter The Wu Tang Clan

IIByb3RIY3QgWWEgTmVjayINCiJTbyB3aGF0J3MgdXAgbWFuPw0KQ29vbGluZyBtYW4iD
QoiQ2hpbGxpbmcgY2hpbGxpbmc/Ig0KIllvIHlvdSBrbm93IEkgaGFkiHRvIGNhbGwsIHlvdSB
bm93IHdoeSBYaWdodD8iDQoiV2h5PyINCiJCZWNhdXNlLCB5bywgSSBuZXZlciBldmVyiG
NhbGwgYW5kIGFzaywgeW91IHRvIHBSYXkgc29tZXRoZW5nIHJpZ2h0PyINCiJZZWFolG0K
IllvdSBrbm93IHdoYXQgSSB3YW5uYSBoZWYyIHJpZ2h0PyINCiJXaGF0IHlvdSB3YW5uYS
BoZWYyPw0KSSB3YW5uYSBoZWYyIHRoYXQgV3UtVGFuZyBqb2ludCINCiJXdS1UYW5nI
GFuYWluPyINCiJBaCB5ZWFOlCBhZ2FpbiBhbmQgYWdhaW4hlg0KDQpbcb291bmRzIG9mI
GZpZ2h0aW5nXQ0KDQpbUlPbXSBXdS1UYW5nIENsYW4gY29taW5nIGF0IHlvdSwgcHJvd
GVjdCB5b3VyiG5IY2sga2lkLCBzbyBzZXQgaXQgb2ZmIHROZSBjbNwZWN0b3lgRGVjaw
0KW01ldGhdIHdhGdGNolIHlvdXlGc3RlcCBraWQgWzhYXQ0KDQpbSW5zcGVjdG9yIERIY2td
DQpJIHntb2tllG9uIHROZSBtaWmGblRZSBzbW9raW5nIEpvZSBGcmF6aWVvDQpUaGUga
GVsbCBYyWlZlZlIiHJhaXNpbmcgaGVsbCB3aXRolHROZSBmbGF2b3INCiRlcnJvcml6ZSB
0aGUgamFtIGxpa2UgdHJvb3BzIGlulFBha2lzdGFuDQpTd2luZ2luZyB0aHJvdWd0IHlvdXlGd
G93biBsaWtllIHlvdXlgbmVpZ2hib3Job29kIFNwaWRlcm1hbg0KU28gdWhoLCB0aWMgdG9jI
GFuZCBZZWVwIHRpY2tpbmcNCldoaWxIEkgZ2V0IHlvdSBmbGlwcGluZyBvZmYgdGhlIHNo
aXQgSSdtIGtpY2tpbmcNCiRoZSBMb25lIFJhbmdlcwY29kZSBYyZWQsIGRhbmdlcicENCKRI
ZXAgYW4gdGhlIGRhcmSgd2l0aCB0aGUgYXJ0IHROVHJpcCBjaGFydHMgYXBhcnQNCiRoZ
SB2YW5kYWwslIHRvbyBob3QgdG8gaGFuZGxldQp5b3UgYmF0dGxldCB5b3UncmUgc2F5
aW5nIEdvb2RieWUgbGlRZSBUXZpbiBDYW1wYmVsbA0KUm91Z2huZWNRlCBjbNwZWN
N0b3lgRGVjaydzIG9uIHROZSBzZXQNCiRoZSBYyZWJlCBwgSSBtYWtllG1vcmUgdm9pc2Ug
dGhhbiBoZWY2eSBtZXRhA0KDQpbUmFla3dvbl0NCiRoZSB3YXkgSSBtYWtllHROZSBjcm
93ZCBnbyB3aWxkLCBzaXQgYmFjayByZWxheCB3b24ndCBzbWlsZQ0KUmFllGdvdCBpdC
Bnb2luZyBvbiBwYWwslIGNhbGwgbWUgdGhlIHJhcCBhc3Nhc3NpbmF0b3INCiJoeW1lcyBy
dWdnZWQgYW5kIGJ1aWx0IGxpa2UgU2Nod2FyemVuZWdnZXINCKFuZCBJJ20gZ29ubm
EgZ2V0IG1hZCBkZWVwIGxpa2UgYSB0aHJIYXQsIGJsb3cgdXAgeW91ciBwcm9qZWN0D
QpUaGVuIHRha2UgYWxsIHlvdXlGyXNzZXRzDQpDYXVzZSBjIGNhbWUgdG8gc2hha2Ug
dGhlIGZyYW1lIGlulGhhbGYNCldpdGggdGhlIHRob3VnaHRzIHRoYXQgYm9tYiwgc2hpdCB
saWtllG1hdGghDQpTbyBpZiB5b3Ugd2FubmEgdHJ5IHRvIGZsaXAgZ28gZmxpcCBvbiB0a
GUgdmV4dCBtYW4NCkNhdxNlIEkgZ3JhYiB0aGUgY2xpcCBhbmQNCkhpdCB5b3Ugd2l0a
CBzaXh0ZWVulHNob3RzIGFuZCBtb3JlIEkgZ290DQpHb2luZyB0byB3YXlGd2l0aCB0aGUg
bWVsdGluZyBwb3QgaG90DQoNCltNZXRob2RdDQpJdCdzIHRoZSBnZXROb2QgTWFuIG
ZvciBzaG9ydCBNCi4gTWV0aA0KTW92aW5nIG9uIHlvdXlgbGVmdCwgYWghDQpBbmQgc2
V0IGl0IG9mZiwigZ2V0IGl0IG9mZiwigGV0IGl0IG9mZiBsaWtllEGZ2F0DQpJIHdhbm5hIGJ
yZWFrIGZ1bGwslGNvY2sgbWUgYmFjaw0KU21hbGwgY2hhbmdlLCB0aGV5IHb1dHRpbm
cgc2hhbWUgaW4gdGhlIGdhbWUNCkkgdGFrZSBhaW0gYW5kIGJsb3cgdGhhbCBuaWdnY
SBvdXQgdGhlIGZyYW1lDQpBbmQgbGlRZSBGYW1lLCBteSBzdHlsZSdsbCBsaXZlIGZvc
V2ZXINCK5pZ2dheiBjcm9zc2luZyBvdmVylCBidXQgdGhleSBkb24ndCBrbm93IG5vIGJldHR
lG0KQnV0IEkgZG8slHRYdWUslGNhbiBjIGdldCBhICJzdWUiDQpOdWZmlHJlc3BIY3QgZH
VIIHRvIHRoZSBvbmUtc2l4LW9oDQpJIG1YW4gb2gsIHlvdSBjaGVjayBvdXQgdGhlIGZsb3c
NCmxa2UgdGhlIEh1ZHNvbiBvciBQQQ1Agd2hlbiBJJ20gZHVzdGluZW0KTmlnZ2F6IG9mZiBi
ZWNhdXNlIEknSBob3QgbGlRZSBzYXVjZQ0KVGHlHntb2tllGZyb20gdGhlIGx5cmllYyWwgY
mx1bnQgbWFrZXMMgbWUgW2NvdWdoXQ0KDQpbVS1Hb2RdDQpPaCwgZ2hhbCwgZ3JhYi
BteSBudXQgZ2V0IHJcmV3ZWQNCk93LCBoZXJlIGNvbWVzIG15IFNoYW5aW4gc3R5bG
UNCINSb29wLCBCLiBBLiBCdWgtQi4gWS4gVQ0KdG8gbXkgY3JldyB3aXRolHROZSAic3Vl
g0KDQpbSW50ZXJsdWRlXQ0Kd2F0Y2ggeW91ciBzdGVwIGtpZCBbOFhdDQpbT2wgRGly
dHkgQmFzdGFyZGF0Yydtb24gYmFieSBiYWJ5IGMnbW9uIFs0WF0NCItSWkFdlFlvLCB5b3
UgYmVzdCBwcm90ZWN0IHlvdXlgbmVjaw0KDQpbT2wgRGlydHkgQmFzdGFyZGF0NCkZpc
nN0IHROaW5ncyBmaXJzdCBtYW4geW91J3JlIGZ1Y2tpbmcgd2l0aCB0aGUgd29yc3QNCk
nbGwgYmUgc3RpY2tpbmcgcGlucyBpbiB5b3VyiGhYyWQgbGlRZSBhIGZ1Y2tpbmcgbnVyc2
UNCkknbgWgYXR0YWNrIGFueSBuaWdnYSB3aG8ncyBzbGFjayBpbiBoaXMgbWFrjaw0KQ

29tZSBmdWxseSBwYWNrZWQgd2l0aCBhIGZhdCBydWdnZWQgc3RhY2sNCiNoYW1lIG9uIHlvdSB3aGVuIHlvdSBzdGVwcGVkIHROcm91Z2ggdG8NCiRoZSBPbCBEaXJ0eSBCYXN0YXJkIHNoYXN0cmFpZ2h0IGZyb20gdGhllEJyb29rbHlulFpwbW0KQW5klEknBwGwYmUgZGFtbnVklGlmIEkgbGV0IGFueSBtYW4NCKNvbWUgdG8gbXkgY2VudGVyLCB5b3UgZW50ZXlGdGhllHdpbnRlCG0KU3RyYWlnaHQgdXAgYW5klGRvd24gdGhhdCBzaGl0IHByY2t1ZCBqYW0NCllvdSBjYW4ndCBzbGFtLCBkb24ndCBsZXQgbWUgZ2V0IGZvb2wgb24gaGltIG1hbg0KVGHllE9sIERpcnR5IEJhc3RhcmQgaXMgZGlydHkgYW5klHN0aW5raW5nDQpBc29uLCB1bmlxdWUgcm9sbGluZyB3aXR0IHROZSBuaWdodCBvZiB0aGUgY3JlZXBzDQpOaWdnYXogYmUgcm9sbGluZyB3aXR0IGegc3Rhc2gNCmFpbid0IHNeWluZyBjYXNoLCBiaXRlIG15IHNoeWxllEknBwGwYmUgZSB5b3VyIG1vdGhlcmZ1Y2tpbmCGYXNzIQ0KDQpbR2hvc3RmYWNlIEtpbGxhaF0NCkZvciBjcnlpbmcgb3V0IGxvdWQgbXkgc3R5bGUgaXMgd2lsZCBzbyBib29rIG1lDQpOb3QgbG9uZyBpcyBob3cgbG9uZyB0aGF0IHROaXMgc3R5bGUgcm9sbGluZyB3aXR0IGegc3Rhc2gNCmFpbid0IHNeWluZyBjYXNoLCBiaXRlIG15IHNoeWxllEknBwGwYmUgZSB5b3VyIG1vdGhlcmZ1Y2tpbmCGYXNzIQ0KDQpbR2hvc3RmYWNlIEtpbGxhaF0NCkZvciBjcnlpbmcgb3V0IGxvdWQgbXkgc3R5bGUgaXMgd2lsZCBzbyBib29rIG1lDQpOb3QgbG9uZyBpcyBob3cgbG9uZyB0aGF0IHROaXMgc3R5bGUgcm9sbGluZyB3aXR0IGegc3Rhc2gNCmFpbid0IHNeWluZyBjYXNoLCBiaXRlIG15IHNoeWxllEknBwGwYmUgZSB5b3VyIG1vdGhlcmZ1Y2tpbmCGYXNzIQ0KDQpbR2hvc3RmYWNlIEtpbGxhaF0NCkZvciBjcnlpbmcgb3V0IGxvdWQgbXkgc3R5bGUgaXMgd2lsZCBzbyBib29rIG1lDQpOb3QgbG9uZyBpcyBob3cgbG9uZyB0aGF0IHROaXMgc3R5bGUgcm9sbGluZyB3aXR0IGegc3Rhc2gNCmFpbid0IHNeWluZyBjYXNoLCBiaXRlIG15IHNoeWxllEknBwGwYmUgZSB5b3VyIG1vdGhlcmZ1Y2tpbmCGYXNzIQ0KDQpbR2hvc3RmYWNlIEtpbGxhaF0NCkZvciBjcnlpbmcgb3V0IGxvdWQgbXkgc3R5bGUgaXMgd2lsZCBzbyBib29rIG1lDQpOb3QgbG9uZyBpcyBob3cgbG9uZyB0aGF0IHROaXMgc3R5bGUgcm9sbGluZyB3aXR0IGegc3Rhc2gNCmFpbid0IHNeWluZyBjYXNoLCBiaXRlIG15IHNoeWxllEknBwGwYmUgZSB5b3VyIG1vdGhlcmZ1Y2tpbmCGYXNzIQ0KDQpbR2hvc3RmYWNlIEtpbGxhaF0NCkZvciBjcnlpbmcgb3V0IGxvdWQgbXkgc3R5bGUgaXMgd2lsZCBzbyBib29rIG1lDQpOb3QgbG9uZyBpcyBob3cgbG9uZyB0aGF0IHROaXMgc3R5bGUgcm9sbGluZyB3aXR0IGegc3Rhc2gNCmFpbid0IHNeWluZyBjYXNoLCBiaXRlIG15IHNoeWxllEknBwGwYmUgZSB5b3VyIG1vdGhlcmZ1Y2tpbmCGYXNzIQ0KDQpbR2hvc3RmYWNlIEtpbGxhaF0NCkZvciBjcnlpbmcgb3V0IGxvdWQgbXkgc3R5bGUgaXMgd2lsZCBzbyBib29rIG1lDQpOb3QgbG9uZyBpcyBob3cgbG9uZyB0aGF0IHROaXMgc3R5bGUgcm9sbGluZyB3aXR0IGegc3Rhc2gNCmFpbid0IHNeWluZyBjYXNoLCBiaXRlIG15IHNoeWxllEknBwGwYmUgZSB5b3VyIG1vdGhlcmZ1Y2tpbmCGYXNzIQ0KDQpbR2hvc3RmYWNlIEtpbGxhaF0NCkZvciBjcnlpbmcgb3V0IGxvdWQgbXkgc3R5bGUgaXMgd2lsZCBzbyBib29rIG1lDQpOb3QgbG9uZyBpcyBob3cgbG9uZyB0aGF0IHROaXMgc3R5bGUgcm9sbGluZyB3aXR0IGegc3Rhc2gNCmFpbid0IHNeWluZyBjYXNoLCBiaXRlIG15IHNoeWxllEknBwGwYmUgZSB5b3VyIG1vdGhlcmZ1Y2tpbmCGYXNzIQ0KDQpbR2hvc3RmYWNlIEtpbGxhaF0NCkZvciBjcnlpbmcgb3V0IGxvdWQgbXkgc3R5bGUgaXMgd2lsZCBzbyBib29rIG1lDQpOb3QgbG9uZyBpcyBob3cgbG9uZyB0aGF0IHROaXMgc3R5bGUgcm9sbGluZyB3aXR0IGegc3Rhc2gNCmFpbid0IHNeWluZyBjYXNoLCBiaXRlIG15IHNoeWxllEknBwGwYmUgZSB5b3VyIG1vdGhlcmZ1Y2tpbmCGYXNzIQ0KDQpbR2hvc3RmYWNlIEtpbGxhaF0NCkZvciBjcnlpbmcgb3V0IGxvdWQgbXkgc3R5bGUgaXMgd2lsZCBzbyBib29rIG1lDQpOb3QgbG9uZyBpcyBob3cgbG9uZyB0aGF0IHROaXMgc3R5bGUgcm9sbGluZyB3aXR0IGegc3Rhc2gNCmFpbid0IHNeWluZyBjYXNoLCBiaXRlIG15IHNoeWxllEknBwGwYmUgZSB5b3VyIG1vdGhlcmZ1Y2tpbmCGYXNzIQ0KDQpbR2hvc3RmYWNlIEtpbGxhaF0NCkZvciBjcnlpbmcgb3V0IGxvdWQgbXkgc3R5bGUgaXMgd2lsZCBzbyBib29rIG1lDQpOb3QgbG9uZyBpcyBob3cgbG9uZyB0aGF0IHROaXMgc3R5bGUgcm9sbGluZyB3aXR0IGegc3Rhc2gNCmFpbid0IHNeWluZyBjYXNoLCBiaXRlIG15IHNoeWxllEknBwGwYmUgZSB5b3VyIG1vdGhlcmZ1Y2tpbmCGYXNzIQ0KDQpbR2hvc3RmYWNlIEtpbGxhaF0NCkZvciBjcnlpbmcgb3V0IGxvdWQgbXkgc3R5bGUgaXMgd2lsZCBzbyBib29rIG1lDQpOb3QgbG9uZyBpcyBob3cgbG9uZyB0aGF0IHROaXMgc3R5bGUgcm9sbGluZyB3aXR0IGegc3Rhc2gNCmFpbid0IHNeWluZyBjYXNoLCBiaXRlIG15IHNoeWxllEknBwGwYmUgZSB5b3VyIG1vdGhlcmZ1Y2tpbmCGYXNzIQ0KDQpbR2hvc3RmYWNlIEtpbGxhaF0NCkZvciBjcnlpbmcgb3V0IGxvdWQgbXkgc3R5bGUgaXMgd2lsZCBzbyBib29rIG1lDQpOb3QgbG9uZyBpcyBob3cgbG9uZyB0aGF0IHROaXMgc3R5bGUgcm9sbGluZyB3aXR0IGegc3Rhc2gNCmFpbid0IHNeWluZyBjYXNoLCBiaXRlIG15IHNoeWxllEknBwGwYmUgZSB5b3VyIG1vdGhlcmZ1Y2tpbmCGYXNzIQ0KDQpbR2hvc3RmYWNlIEtpbGxhaF0NCkZvciBjcnlpbmcgb3V0IGxvdWQgbXkgc3R5bGUgaXMgd2lsZCBzbyBib29rIG1lDQpOb3QgbG9uZyBpcyBob3cgbG9uZyB0aGF0IHROaXMgc3R5bGUgcm9sbGluZyB3aXR0IGegc3Rhc2gNCmFpbid0IHNeWluZyBjYXNoLCBiaXRlIG15IHNoeWxllEknBwGwYmUgZSB5b3VyIG1vdGhlcmZ1Y2tpbmCGYXNzIQ0KDQpbR2hvc3RmYWNlIEtpbGxhaF0NCkZvciBjcnlpbmcgb3V0IGxvdWQgbXkgc3R5bGUgaXMgd2lsZCBzbyBib29rIG1lDQpOb3QgbG9uZyBpcyBob3cgbG9uZyB0aGF0IHROaXMgc3R5bGUgcm9sbGluZyB3aXR0IGegc3Rhc2gNCmFpbid0IHNeWluZyBjYXNoLCBiaXRlIG15IHNoeWxllEknBwGwYmUgZSB5b3VyIG1vdGhlcmZ1Y2tpbmCGYXNzIQ0KDQpbR2hvc3RmYWNlIEtpbGxhaF0NCkZvciBjcnlpbmcgb3V0IGxvdWQgbXkgc3R5bGUgaXMgd2lsZCBzbyBib29rIG1lDQpOb3QgbG9uZyBpcyBob3cgbG9uZyB0aGF0IHROaXMgc3R5bGUgcm9sbGluZyB3aXR0IGegc3Rhc2gNCmFpbid0IHNeWluZyBjYXNoLCBiaXRlIG15IHNoeWxllEknBwGwYmUgZSB5b3VyIG1vdGhlcmZ1Y2tpbmCGYXNzIQ0KDQpbR2hvc3RmYWNlIEtpbGxhaF0NCkZvciBjcnlpbmcgb3V0IGxvdWQgbXkgc3R5bGUgaXMgd2lsZCBzbyBib29rIG1lDQpOb3QgbG9uZyBpcyBob3cgbG9uZyB0aGF0IHROaXMgc3R5bGUgcm9sbGluZyB3aXR0IGegc3Rhc2gNCmFpbid0IHNeWluZyBjYXNoLCBiaXRlIG15IHNoeWxllEknBwGwYmUgZSB5b3VyIG1vdGhlcmZ1Y2tpbmCGYXNzIQ0KDQpbR2hvc3RmYWNlIEtpbGxhaF0NCkZvciBjcnlpbmcgb3V0IGxvdWQgbXkgc3R5bGUgaXMgd2lsZCBzbyBib29rIG1lDQpOb3QgbG9uZyBpcyBob3cgbG9uZyB0aGF0IHROaXMgc3R5bGUgcm9sbGluZyB3aXR0IGegc3Rhc2gNCmFpbid0IHNeWluZyBjYXNoLCBiaXRlIG15IHNoeWxllEknBwGwYmUgZSB5b3VyIG1vdGhlcmZ1Y2tpbmCGYXNzIQ0KDQpbR2hvc3RmYWNlIEtpbGxhaF0NCkZvciBjcnlpbmcgb3V0IGxvdWQgbXkgc3R5bGUgaXMgd2lsZCBzbyBib29rIG1lDQpOb3QgbG9uZyBpcyBob3cgbG9uZyB0aGF0IHROaXMgc3R5bGUgcm9sbGluZyB3aXR0IGegc3Rhc2gNCmFpbid0IHNeWluZyBjYXNoLCBiaXRlIG15IHNoeWxllEknBwGwYmUgZSB5b3VyIG1vdGhlcmZ1Y2tpbmCGYXNzIQ0KDQpbR2hvc3RmYWNlIEtpbGxhaF0NCkZvciBjcnlpbmcgb3V0IGxvdWQgbXkgc3R5bGUgaXMgd2lsZCBzbyBib29rIG1lDQpOb3QgbG9uZyBpcyBob3cgbG9uZyB0aGF0IHROaXMgc3R5bGUgcm9sbGluZyB3aXR0IGegc3Rhc2gNCmFpbid

3MgaGF2ZSBhIG11ZCBmaWdodA0KDQpbc291bmRzIG9mIGZpZ2h0aW5nXQ0KDQpbUlp
BXSbZb3UgYmVzdCBwcm90ZWN0IHlvdXlgbmVjayBbNFhdDQoNCg==

"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]

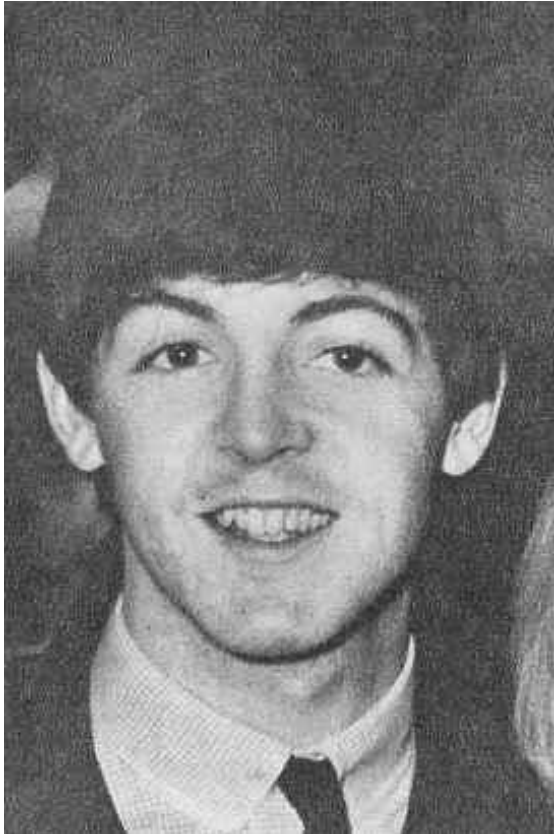
[RZA] You best protect your neck [4X]

PiD

RGVhciBFZCwNCg0KWWVhaCBJIHRvdGFsbHkgdG9vayBvdmVylIGZvciBQYXVslIGFmdG
VyIGHlIGRpZWQgaW4g4oCZNjYulFlvdSBnb3QgbWUulEFzIHlvdSBjYW4gc2VILCB3ZSBkb
27igJI0IGV2ZW4gbG9vayB0aGF0IG11Y2ggYWxpa2U6DQo=

Dear Ed,

Yeah I totally took over for Paul after he died in '66. You got me. As you can see, we don't even look that much alike:



Before(Paul)



After(Me)

IAkgCQ0KQmVmb3JIKFBhdWwplAkJCQkJQWZ0ZXIoTWUpDQoNCldlIGFyZW7igJI0IGV2Z
W4gdGhlIHhnbWUgaGVpZ2h0ISBXaGF0IGNhbiBJIHNeSwgcGVvcGxIGFyZSBzdHVwa
WQuDQoNCg0KVGHbmtzIGZvciB0aGUgaW5xdWlyeSwNCg0KV2lsbGlhbSBDYW1wYmV
sbA0KKFBhdWwgTWNDYXJ0bmV5KQ0K

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

Thanks for the inquiry,

William Campbell
(Paul McCartney)

Recipe

From Base64

Alphabet

A-Za-z0-9+/=

☒ Remove non-alphabet chars
☐ Strict mode

Input

length: 418
lines: 3

RGVhc iBFZCwNCg0KwMvhaCBJIHRvdGFsbHkgdG9vayBvdmVyIGZvciBQYXVsIGFmdGVyIGhlIGRpZWQgaW4g4oCZNjYuIFlvdS
Bnb3QgbWUuIEFzIHlvdSBjYW4gc2VlLCB3ZSBkb27igJl0IGV2ZW4gbG9vayB0aGF0IG11Y2ggYwXpa2U6DQo=

IAkgCQ0KQmVmb3JlKFBhdwpiIAkJCQkJQWZ0ZXI0TWUpDQoNCldlIGFyZW7igJl0IGV2ZW4gdGhlIHhnbWUgaGvpZ2h0ISBXaG
F0IGNhb iBJIHNheSwgcGVvcGx1IGFyZSBzdHVwaWQuDQoNCg0KVghbmtzIGZvciB0aGUgaW5xdWlyeSwNCg0KV2l5bG1hbsBD
Yw1wYmVs bA0KKFBhdWwgTWNDYXJ0bmV5KQ0K

Output

time: 1ms
length: 305
lines: 14

Dear Ed,

Yeah I totally took over for Paul after he died in '66. 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)	

STEP

BAKE!

Auto Bake

Figure 3: Decoding PiD from base64 using CyberChef.

Miscellaneous



Figure 4: "NorthKorea.jpg"

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.

Appendix B – Image Reconstruction

```
ngrep -l Capture\ 2.pcap ".zip" | grep -E -o ".{0,0}filename=.{0,26}"
```

```
filename="34jdsioj.zip"..Content-Ty  
filename="breaking_bad_season_6.zip  
filename="canc3l.zip"..Content-Type  
filename="f.txt"..Content-Encoding:  
filename="f.txt"..Content-  
filename="f.txt"..Content-  
filename="f.txt"..Content-  
filename="f.txt"..Content-  
filename="f.txt"..Content-E  
filename="f.txt"..Content-E
```

```
cat l.jpg cant.jpg in.jpg good.jpg conscience.jpg allow.jpg the.jpg U.S..jpg government.jpg  
to.jpg destroy.jpg privacy.jpg internet.jpg freedom.jpg and.jpg basic.jpg liberties.jpg for.jpg  
people.jpg around.jpg world.jpg with.jpg this.jpg massive.jpg surveillance.jpg machine.jpg  
theyre.jpg secretly.jpg building.jpg > snowden.jpg
```



Figure 1: Snowden Quote image reconstruction.

cat there.jpg their.jpg a.jpg it.jpg but.jpg communism.jpg nor.jpg because.jpg
unconstitutional.jpg secretive.jpg secret.jpg > image2.jpg



Figure 2: Kim Jong-un image reconstruction

cat condone.jpg American.jpg web-based.jpg rights.jpg constructing.jpg security.jpg
terrorism.jpg NSA.jpg Watergate.jpg corrupt.jpg human.jpg behind.jpg closed.jpg doors.jpg >
image3.jpg



Figure 3: Robot image reconstruction

Appendix C – Meeting communications

Ill-Song filter

```
ngrep -I Capture\ 3.pcap "Ill-Song"
```

```
input: Capture 3.pcap
```

```
filter: ((ip || ip6) || (vlan && (ip || ip6)))
```

```
match (JIT): Ill-Song
```

```
T 192.168.1.5:39312 -> 199.87.160.87:80 [AP] #3777
```

```
POST /1.0/messages/text/send?lang=en-US HTTP/1.1..x-rest-method: POST..Content-Type: application/json..X-Install-Id: 6965eedb59a7b282f94dd58e7a451474..x-client: textfree-android,2.3.2..x-os:
```

```
android,4.2.2..x-uid: 580781709..x-gid: 0..Authorization: OAuth realm="http://api.pinger.com", oauth_consumer_key="580781709%3Btextfree-android-332281036089711-1404333778292", oauth_signatu
```

```
re_method="HMAC-SHA1", oauth_timestamp="1404340884", oauth_nonce="yllcitpjdjfmkqpr", oauth_signature="LT%2FKyayOPT8%2BZxTUKw0wFudNxYk%3D"..Content-Length: 210..Host: api.pinger.com..Connection
```

```
: Keep-Alive..User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)....{"senderId":"14068522589","senderName":"Ann","recipientId":"+14069243754","messageTxt":"Do you know that there are people investigating Kim Ill-Song?","senderType":"phone","sendAsSms":0,"recipientType":"phone"} #
```

```
T 192.168.1.5:39312 -> 199.87.160.87:80 [AP] #3778
```

```
POST /1.0/messages/text/send?lang=en-US HTTP/1.1..x-rest-method: POST..Content-Type: application/json..X-Install-Id: 6965eedb59a7b282f94dd58e7a451474..x-client: textfree-android,2.3.2..x-os:
```

```
android,4.2.2..x-uid: 580781709..x-gid: 0..Authorization: OAuth realm="http://api.pinger.com", oauth_consumer_key="580781709%3Btextfree-android-332281036089711-1404333778292", oauth_signatu
```

```
re_method="HMAC-SHA1", oauth_timestamp="1404340884", oauth_nonce="yllcitpjdjfmkqpr", oauth_signature="LT%2FKyayOPT8%2BZxTUKw0wFudNxYk%3D"..Content-Length: 210..Host: api.pinger.com..Connection
```

```
: Keep-Alive..User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)....{"senderId":"14068522589","senderName":"Ann","recipientId":"+14069243754","messageTxt":"Do you know that there are people investigating Kim Ill-Song?","senderType":"phone","sendAsSms":0,"recipientType":"phone"} #####
```

```
#####
```

```
T 199.87.160.87:80 -> 192.168.1.5:47289 [AP] #3865
```

```
HTTP/1.1 200 OK..Date: Wed, 02 Jul 2014 22:41:37 GMT..Server: Apache..X-Host: sj2-web13..Content-Length: 945..Keep-Alive: timeout=10, max=4..Connection: Keep-Alive..Content-Type: application/j
```

```
son....{"success":"messages retrieved","result":{"recMessages":[{"messageId":"dc821c4eeacd713cfef5cea15e803040","messageType":"normal","messageText":"I know I can't tell you that.", "recipientT
```

```
ype":"phone","recipientId":"14068522589","senderType":"phone","senderId":"14069243754","senderName":"Kim Ill-song","time":"2014-07-02 22:40:05","messageStatus":"read","deliveryMethod":"onnet"}]
```

```
,"sentMessages":[{"messageId":"bdc2b81acb8e3bff28a1e87ff44ee5d7","messageType":"normal","messageText":"Do you know that there are people investigating Kim Ill-Song?","recipientType":"phone","
```

```
recipientId":"14069243754","senderType":"phone","senderId":"14068522589","senderName":
:"Ann Dercover","time":"2014-07-02
22:41:25","messageStatus":"read","deliveryMethod":"onnet"},"brandedSyst
emMessages":[],"calls":[],"voicemails":[],"now":"2014-07-02
22:41:31","largestCount":1,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0
,"numTextsRec":0,"inviteCount":0}}.
#
```

```
T 199.87.160.87:80 -> 192.168.1.5:47289 [AP] #3866
HTTP/1.1 200 OK..Date: Wed, 02 Jul 2014 22:41:37 GMT..Server: Apache..X-Host: sj2-
web13..Content-Length: 945..Keep-Alive: timeout=10, max=4..Connection: Keep-
Alive..Content-Type: application/j
son....{"success":"messages
retrieved","result":{"recMessages":[{"messageId":"dc821c4eeacd713cfef5cea15e803040","m
essageType":"normal","messageText":"I know I can't tell you that.", "recipientT
```

```
ype":"phone","recipientId":"14068522589","senderType":"phone","senderId":"14069243754",
"senderName":"Kim Ill-song","time":"2014-07-02
22:40:05","messageStatus":"read","deliveryMethod":"onnet"}
], "sentMessages":[{"messageId":"bdc2b81acb8e3bff28a1e87ff44ee5d7","messageType":"no
rmal","messageText":"Do you know that there are people investigating Kim Ill-
Song?","recipientType":"phone", "
```

```
recipientId":"14069243754","senderType":"phone","senderId":"14068522589","senderName"
:"Ann Dercover","time":"2014-07-02
22:41:25","messageStatus":"read","deliveryMethod":"onnet"},"brandedSyst
emMessages":[],"calls":[],"voicemails":[],"now":"2014-07-02
22:41:31","largestCount":1,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0
,"numTextsRec":0,"inviteCount":0}}.
```

[all_messageText.txt](#)

```
ngrep -I Capture\ 3.pcap "messageText"
```

```
input: Capture 3.pcap
```

```
filter: ((ip || ip6) || (vlan && (ip || ip6)))
```

```
match (JIT): messageText
```

```
T 199.87.160.87:80 -> 192.168.1.5:56183 [AP] #2023
```

```
HTTP/1.1 200 OK..Date: Wed, 02 Jul 2014 22:39:00 GMT..Server: Apache..X-Host: sj2-
web32..Content-Length: 892..Keep-Alive: timeout=10, max=16..Connection: Keep-
Alive..Content-Type: application/
```

```
json....{"success":"messages
retrieved","result":{"recMessages":[{"messageId":"45b537c51e5cf2f90f31779e9ec8fc46","me
ssageType":"normal","messageText":"Good afternoon, Ann.", "recipientType":"p
```

```
hone","recipientId":"14068522589","senderType":"phone","senderId":"14069243754","sender
Name":"Kim Ill-song","time":"2014-07-02
22:38:55","messageStatus":"unread","deliveryMethod":"onnet"},"se
```

```
ntMessages":[{"messageId":"d275712ce4c2b1b420bd1ba0728b79af","messageType":"norm
al","messageText":"this is a
test","recipientType":"phone","recipientId":"14069243754","senderType":"phone","sen
```

derId":"14068522589","senderName":"Ann Dercover","time":"2014-07-02
22:34:13","messageStatus":"read","deliveryMethod":"onnet"},"brandedSystemMessages":[],"
calls":[],"voicemails":[],"now":"201
4-07-02

22:38:57","largestCount":1,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0
,"numTextsRec":0,"inviteCount":0}}.

##

T 199.87.160.87:80 -> 192.168.1.5:56183 [AP] #2025

HTTP/1.1 200 OK..Date: Wed, 02 Jul 2014 22:39:00 GMT..Server: Apache..X-Host: sj2-
web32..Content-Length: 892..Keep-Alive: timeout=10, max=16..Connection: Keep-
Alive..Content-Type: application/

json....{"success":"messages
retrieved","result":{"recMessages":[{"messageId":"45b537c51e5cf2f90f31779e9ec8fc46","me
ssageType":"normal","messageText":"Good afternoon, Ann.", "recipientType":"p

hone","recipientId":"14068522589","senderType":"phone","senderId":"14069243754","sender
Name":"Kim Ill-song","time":"2014-07-02
22:38:55","messageStatus":"unread","deliveryMethod":"onnet"},"se

ntMessages":[{"messageId":"d275712ce4c2b1b420bd1ba0728b79af","messageType":"norm
al","messageText":"this is a

test","recipientType":"phone","recipientId":"14069243754","senderType":"phone","sen

derId":"14068522589","senderName":"Ann Dercover","time":"2014-07-02

22:34:13","messageStatus":"read","deliveryMethod":"onnet"},"brandedSystemMessages":[],"
calls":[],"voicemails":[],"now":"201
4-07-02

22:38:57","largestCount":1,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0
,"numTextsRec":0,"inviteCount":0}}.

T 199.87.160.87:80 -> 192.168.1.5:58487 [AP] #2209

HTTP/1.1 200 OK..Date: Wed, 02 Jul 2014 22:39:05 GMT..Server: Apache..X-Host: sj2-
web12..Content-Length: 585..Keep-Alive: timeout=10, max=36..Connection: Keep-
Alive..Content-Type: application/

json....{"success":"messages
retrieved","result":{"recMessages":[{"messageId":"45b537c51e5cf2f90f31779e9ec8fc46","me
ssageType":"normal","messageText":"Good afternoon, Ann.", "recipientType":"p

hone","recipientId":"14068522589","senderType":"phone","senderId":"14069243754","sender
Name":"Kim Ill-song","time":"2014-07-02

22:38:55","messageStatus":"read","deliveryMethod":"onnet"},"sent

Messages":[],"brandedSystemMessages":[],"calls":[],"voicemails":[],"now":"2014-07-02

22:38:57","largestCount":1,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0
,"numTextsRec":0,"

inviteCount":0}}.

#

T 199.87.160.87:80 -> 192.168.1.5:58487 [AP] #2210

HTTP/1.1 200 OK..Date: Wed, 02 Jul 2014 22:39:05 GMT..Server: Apache..X-Host: sj2-
web12..Content-Length: 585..Keep-Alive: timeout=10, max=36..Connection: Keep-
Alive..Content-Type: application/

json....{"success":"messages
retrieved","result":{"recMessages":[{"messageId":"45b537c51e5cf2f90f31779e9ec8fc46","me
ssageType":"normal","messageText":"Good afternoon, Ann.", "recipientType":"p

hone","recipientId":"14068522589","senderType":"phone","senderId":"14069243754","sender
Name":"Kim Ill-song","time":"2014-07-02

22:38:55","messageStatus":"read","deliveryMethod":"onnet"},"sent

Messages":[],"brandedSystemMessages":[],"calls":[],"voicemails":[],"now":"2014-07-02 22:38:57","largestCount":1,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0,"numTextsRec":0,"inviteCount":0}}.

T 199.87.160.87:80 -> 192.168.1.5:51189 [AP] #3069

{"success":"messages retrieved","result":{"recMessages":[{"messageId":"45b537c51e5cf2f90f31779e9ec8fc46","messageType":"normal","messageText":"Good afternoon, Ann.", "recipientType":"phone", "r

ecipientId":"14068522589","senderType":"phone","senderId":"14069243754","senderName":"Kim Ill-song","time":"2014-07-02 22:38:55","messageStatus":"read","deliveryMethod":"onnet"},"{"messageId":"

c113ed366ab0fba64f6215f41d6fb127","messageType":"normal","messageText":"Castling.", "recipientType":"phone","recipientId":"14068522589","senderType":"phone","senderId":"14069243754","senderName

":"Kim Ill-song","time":"2014-07-02 22:39:31","messageStatus":"unread","deliveryMethod":"onnet"},"sentMessages":[{"messageId":"eb232446d54193d00876830421797030","messageType":"normal","messageText":"who is

this?","recipientType":"phone","recipientId":"14069243754","senderType":"phone","senderId":"14068522589","senderName":"Ann Dercover","time":"2014-07-02 22:39:15","messageStatus"

":"read","deliveryMethod":"onnet"},"brandedSystemMessages":[],"calls":[],"voicemails":[],"now":"2014-07-02

22:39:32","largestCount":2,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0,"numTextsRec":0,"inviteCount":0}}.

##

T 199.87.160.87:80 -> 192.168.1.5:51189 [AP] #3071

{"success":"messages retrieved","result":{"recMessages":[{"messageId":"45b537c51e5cf2f90f31779e9ec8fc46","messageType":"normal","messageText":"Good afternoon, Ann.", "recipientType":"phone", "r

ecipientId":"14068522589","senderType":"phone","senderId":"14069243754","senderName":"Kim Ill-song","time":"2014-07-02 22:38:55","messageStatus":"read","deliveryMethod":"onnet"},"{"messageId":"

c113ed366ab0fba64f6215f41d6fb127","messageType":"normal","messageText":"Castling.", "recipientType":"phone","recipientId":"14068522589","senderType":"phone","senderId":"14069243754","senderName

":"Kim Ill-song","time":"2014-07-02 22:39:31","messageStatus":"unread","deliveryMethod":"onnet"},"sentMessages":[{"messageId":"eb232446d54193d00876830421797030","messageType":"normal","messageText":"who is

this?","recipientType":"phone","recipientId":"14069243754","senderType":"phone","senderId":"14068522589","senderName":"Ann Dercover","time":"2014-07-02 22:39:15","messageStatus"

":"read","deliveryMethod":"onnet"},"brandedSystemMessages":[],"calls":[],"voicemails":[],"now":"2014-07-02

22:39:32","largestCount":2,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0,"numTextsRec":0,"inviteCount":0}}.

#####

T 199.87.160.87:80 -> 192.168.1.5:56880 [AP] #3247

HTTP/1.1 200 OK..Date: Wed, 02 Jul 2014 22:39:41 GMT..Server: Apache..X-Host: sj2-web34..Content-Length: 573..Keep-Alive: timeout=10, max=17..Connection: Keep-Alive..Content-Type: application/

json....{"success":"messages
retrieved","result":{"recMessages":[{"messageId":"c113ed366ab0fba64f6215f41d6fb127","messageType":"normal","messageText":"Castling.", "recipientType":"phone","recip

ientId":"14068522589","senderType":"phone","senderId":"14069243754","senderName":"Kim
Ill-song","time":"2014-07-02

22:39:31","messageStatus":"read","deliveryMethod":"onnet"}],"sentMessages":[]

, "brandedSystemMessages":[],"calls":[],"voicemails":[],"now":"2014-07-02

22:39:32","largestCount":1,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0
,"numTextsRec":0,"inviteCount":0}}.

#

T 199.87.160.87:80 -> 192.168.1.5:56880 [AP] #3248

HTTP/1.1 200 OK..Date: Wed, 02 Jul 2014 22:39:41 GMT..Server: Apache..X-Host: sj2-web34..Content-Length: 573..Keep-Alive: timeout=10, max=17..Connection: Keep-Alive..Content-Type: application/

json....{"success":"messages
retrieved","result":{"recMessages":[{"messageId":"c113ed366ab0fba64f6215f41d6fb127","messageType":"normal","messageText":"Castling.", "recipientType":"phone","recip

ientId":"14068522589","senderType":"phone","senderId":"14069243754","senderName":"Kim
Ill-song","time":"2014-07-02

22:39:31","messageStatus":"read","deliveryMethod":"onnet"}],"sentMessages":[]

, "brandedSystemMessages":[],"calls":[],"voicemails":[],"now":"2014-07-02

22:39:32","largestCount":1,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0
,"numTextsRec":0,"inviteCount":0}}.

T 199.87.160.87:80 -> 192.168.1.5:39427 [AP] #3440

HTTP/1.1 200 OK..Date: Wed, 02 Jul 2014 22:40:00 GMT..Server: Apache..X-Host: sj2-web04..Content-Length: 878..Keep-Alive: timeout=10, max=2..Connection: Keep-Alive..Content-Type: application/j

son....{"success":"messages
retrieved","result":{"recMessages":[{"messageId":"c113ed366ab0fba64f6215f41d6fb127","messageType":"normal","messageText":"Castling.", "recipientType":"phone","recip

entId":"14068522589","senderType":"phone","senderId":"14069243754","senderName":"Kim
Ill-song","time":"2014-07-02

22:39:31","messageStatus":"read","deliveryMethod":"onnet"}],"sentMessages":[{"

messageId":"4125737ad17157e816310b4f2f98752a","messageType":"normal","messageText":"where are

you?","recipientType":"phone","recipientId":"14069243754","senderType":"phone","senderId":"1406852

2589","senderName":"Ann Dercover","time":"2014-07-02

22:39:46","messageStatus":"read","deliveryMethod":"onnet"}],"brandedSystemMessages":[],"calls":[],"voicemails":[],"now":"2014-07-02 22:39:5

4", "largestCount": 1, "smsCreditBalance": 0, "callingCreditBalance": 0, "numTextsSent": 0, "numTextsRec": 0, "inviteCount": 0}}.

#

T 199.87.160.87:80 -> 192.168.1.5:39427 [AP] #3441

HTTP/1.1 200 OK..Date: Wed, 02 Jul 2014 22:40:00 GMT..Server: Apache..X-Host: sj2-web04..Content-Length: 878..Keep-Alive: timeout=10, max=2..Connection: Keep-Alive..Content-Type: application/j

son....{"success": "messages
retrieved", "result": {"recMessages": [{"messageId": "c113ed366ab0fba64f6215f41d6fb127", "messageType": "normal", "messageText": "Castling.", "recipientType": "phone", "recipientId": "14068522589", "senderType": "phone", "senderId": "14069243754", "senderName": "Kim Ill-song", "time": "2014-07-02 22:39:31", "messageStatus": "read", "deliveryMethod": "onnet"}], "sentMessages": [{"messageId": "4125737ad17157e816310b4f2f98752a", "messageType": "normal", "messageText": "where are you?", "recipientType": "phone", "recipientId": "14069243754", "senderType": "phone", "senderId": "14068522589", "senderName": "Ann Dercover", "time": "2014-07-02 22:39:46", "messageStatus": "read", "deliveryMethod": "onnet"}], "brandedSystemMessages": [], "calls": [], "voicemails": [], "now": "2014-07-02 22:39:54"}]}

entId": "14068522589", "senderType": "phone", "senderId": "14069243754", "senderName": "Kim Ill-song", "time": "2014-07-02

22:39:31", "messageStatus": "read", "deliveryMethod": "onnet"}], "sentMessages": [{"

messageId": "4125737ad17157e816310b4f2f98752a", "messageType": "normal", "messageText": "where are

you?", "recipientType": "phone", "recipientId": "14069243754", "senderType": "phone", "senderId": "1406852

2589", "senderName": "Ann Dercover", "time": "2014-07-02

22:39:46", "messageStatus": "read", "deliveryMethod": "onnet"}], "brandedSystemMessages": [], "calls": [], "voicemails": [], "now": "2014-07-02 22:39:54"}]}

4", "largestCount": 1, "smsCreditBalance": 0, "callingCreditBalance": 0, "numTextsSent": 0, "numTextsRec": 0, "inviteCount": 0}}.

T 199.87.160.87:80 -> 192.168.1.5:42044 [AP] #3534

HTTP/1.1 200 OK..Date: Wed, 02 Jul 2014 22:40:14 GMT..Server: Apache..X-Host: sj2-web07..Content-Length: 595..Keep-Alive: timeout=10, max=49..Connection: Keep-Alive..Content-Type: application/

json....{"success": "messages
retrieved", "result": {"recMessages": [{"messageId": "dc821c4eeacd713cfef5cea15e803040", "messageType": "normal", "messageText": "I know I can't tell you that.", "recipientType": "phone", "recipientId": "14068522589", "senderType": "phone", "senderId": "14069243754", "senderName": "Kim Ill-song", "time": "2014-07-02 22:40:05", "messageStatus": "unread", "deliveryMethod": "onnet"}], "sentMessages": [], "brandedSystemMessages": [], "calls": [], "voicemails": [], "now": "2014-07-02 22:40:06", "largestCount": 1, "smsCreditBalance": 0, "callingCreditBalance": 0, "numTextsSent": 0, "numTextsRec": 0, "inviteCount": 0}}.

Type": "phone", "recipientId": "14068522589", "senderType": "phone", "senderId": "14069243754", "senderName": "Kim Ill-song", "time": "2014-07-02

22:40:05", "messageStatus": "unread", "deliveryMethod": "onnet"}], "sentMessages": [], "brandedSystemMessages": [], "calls": [], "voicemails": [], "now": "2014-07-02

07-02 22:40:06", "largestCount": 1, "smsCreditBalance": 0, "callingCreditBalance": 0, "numTextsSent": 0, "numTextsRec": 0, "inviteCount": 0}}.

tsRec": 0, "inviteCount": 0}}.

#

T 199.87.160.87:80 -> 192.168.1.5:42044 [AP] #3535

HTTP/1.1 200 OK..Date: Wed, 02 Jul 2014 22:40:14 GMT..Server: Apache..X-Host: sj2-web07..Content-Length: 595..Keep-Alive: timeout=10, max=49..Connection: Keep-Alive..Content-Type: application/

json....{"success": "messages
retrieved", "result": {"recMessages": [{"messageId": "dc821c4eeacd713cfef5cea15e803040", "messageType": "normal", "messageText": "I know I can't tell you that.", "recipientType": "phone", "recipientId": "14068522589", "senderType": "phone", "senderId": "14069243754", "senderName": "Kim Ill-song", "time": "2014-07-02 22:40:05", "messageStatus": "unread", "deliveryMethod": "onnet"}], "sentMessages": [], "brandedSystemMessages": [], "calls": [], "voicemails": [], "now": "2014-07-02 22:40:06", "largestCount": 1, "smsCreditBalance": 0, "callingCreditBalance": 0, "numTextsSent": 0, "numTextsRec": 0, "inviteCount": 0}}.

Type": "phone", "recipientId": "14068522589", "senderType": "phone", "senderId": "14069243754", "senderName": "Kim Ill-song", "time": "2014-07-02

22:40:05", "messageStatus": "unread", "deliveryMethod": "onnet"}], "sentMessages": [], "brandedSystemMessages": [], "calls": [], "voicemails": [], "now": "2014-07-02 22:40:06", "largestCount": 1, "smsCreditBalance": 0, "callingCreditBalance": 0, "numTextsSent": 0, "numTextsRec": 0, "inviteCount": 0}}.

t"}], "sentMessages": [], "brandedSystemMessages": [], "calls": [], "voicemails": [], "now": "2014-07-02 22:40:06", "largestCount": 1, "smsCreditBalance": 0, "callingCreditBalance": 0, "numTextsSent": 0, "numTextsRec": 0, "inviteCount": 0}}.

T 199.87.160.87:80 -> 192.168.1.5:47289 [AP] #3865

HTTP/1.1 200 OK..Date: Wed, 02 Jul 2014 22:41:37 GMT..Server: Apache..X-Host: sj2-web13..Content-Length: 945..Keep-Alive: timeout=10, max=4..Connection: Keep-Alive..Content-Type: application/j

son....{"success": "messages retrieved", "result": {"recMessages": [{"messageId": "dc821c4eeacd713cfef5cea15e803040", "messageType": "normal", "messageText": "I know I can't tell you that.", "recipientT

ype": "phone", "recipientId": "14068522589", "senderType": "phone", "senderId": "14069243754", "senderName": "Kim Ill-song", "time": "2014-07-02 22:40:05", "messageStatus": "read", "deliveryMethod": "onnet"}

], "sentMessages": [{"messageId": "bdc2b81acb8e3bff28a1e87ff44ee5d7", "messageType": "normal", "messageText": "Do you know that there are people investigating Kim Ill-Song?", "recipientType": "phone", "

recipientId": "14069243754", "senderType": "phone", "senderId": "14068522589", "senderName": "Ann Dercover", "time": "2014-07-02

22:41:25", "messageStatus": "read", "deliveryMethod": "onnet"}], "brandedSyst

emMessages": [], "calls": [], "voicemails": [], "now": "2014-07-02

22:41:31", "largestCount": 1, "smsCreditBalance": 0, "callingCreditBalance": 0, "numTextsSent": 0, "numTextsRec": 0, "inviteCount": 0}}.

#

T 199.87.160.87:80 -> 192.168.1.5:47289 [AP] #3866

HTTP/1.1 200 OK..Date: Wed, 02 Jul 2014 22:41:37 GMT..Server: Apache..X-Host: sj2-web13..Content-Length: 945..Keep-Alive: timeout=10, max=4..Connection: Keep-Alive..Content-Type: application/j

son....{"success": "messages retrieved", "result": {"recMessages": [{"messageId": "dc821c4eeacd713cfef5cea15e803040", "messageType": "normal", "messageText": "I know I can't tell you that.", "recipientT

ype": "phone", "recipientId": "14068522589", "senderType": "phone", "senderId": "14069243754", "senderName": "Kim Ill-song", "time": "2014-07-02 22:40:05", "messageStatus": "read", "deliveryMethod": "onnet"}

], "sentMessages": [{"messageId": "bdc2b81acb8e3bff28a1e87ff44ee5d7", "messageType": "normal", "messageText": "Do you know that there are people investigating Kim Ill-Song?", "recipientType": "phone", "

recipientId": "14069243754", "senderType": "phone", "senderId": "14068522589", "senderName": "Ann Dercover", "time": "2014-07-02

22:41:25", "messageStatus": "read", "deliveryMethod": "onnet"}], "brandedSyst

emMessages": [], "calls": [], "voicemails": [], "now": "2014-07-02

22:41:31", "largestCount": 1, "smsCreditBalance": 0, "callingCreditBalance": 0, "numTextsSent": 0, "numTextsRec": 0, "inviteCount": 0}}.

#####

T 199.87.160.87:80 -> 192.168.1.5:54994 [AP] #3955

T 199.87.160.87:80 -> 192.168.1.5:33205 [AP] #4347

HTTP/1.1 200 OK..Date: Wed, 02 Jul 2014 22:43:01 GMT..Server: Apache..X-Host: sj2-web36..Content-Length: 1003..Keep-Alive: timeout=10, max=16..Connection: Keep-Alive..Content-Type: application

```
/json....{"success":"messages
retrieved","result":{"recMessages":[{"messageId":"8197385d4b4222e32ec474fa497b70d8","
messageType":"normal","messageText":"Of course. However, they will never kn
ow it is me behind the
bribes.","recipientType":"phone","recipientId":"14068522589","senderType":"phone","senderI
d":"14069243754","senderName":"Kim Ill-song","time":"2014-07-02 22:41:47","mess
```

```
ageStatus":"read","deliveryMethod":"onnet"}],"sentMessages":[{"messageId":"700b4051723f
212b979cf068e59067b9","messageType":"normal","messageText":"still we should be
careful. Pay attention. I
```

```
want to meet in September at
5PM.","recipientType":"phone","recipientId":"14069243754","senderType":"phone","senderId
":"14068522589","senderName":"Ann Dercover","time":"2014-07-02 22:42:54","m
```

```
essageStatus":"read","deliveryMethod":"onnet"}],"brandedSystemMessages":[],"calls":[],"voic
emails":[],"now":"2014-07-02
```

```
22:42:58","largestCount":1,"smsCreditBalance":0,"callingCreditBalance":0
,"numTextsSent":0,"numTextsRec":0,"inviteCount":0}}.
```

```
#####
#####
```

T 199.87.160.87:80 -> 192.168.1.5:48325 [AP] #4439

HTTP/1.1 200 OK..Date: Wed, 02 Jul 2014 22:43:11 GMT..Server: Apache..X-Host: sj2-web04..Content-Length: 589..Keep-Alive: timeout=10, max=40..Connection: Keep-Alive..Content-Type: application/

```
json....{"success":"messages
retrieved","result":{"recMessages":[{"messageId":"e5d6be661c5ed90cfb27a0fb50b33bf2","m
essageType":"normal","messageText":"At our old meetup spot?","recipientType":
```

```
"phone","recipientId":"14068522589","senderType":"phone","senderId":"14069243754","send
erName":"Kim Ill-song","time":"2014-07-02
```

```
22:43:06","messageStatus":"unread","deliveryMethod":"onnet"}],"
```

```
sentMessages":[],"brandedSystemMessages":[],"calls":[],"voicemails":[],"now":"2014-07-02
22:43:07","largestCount":1,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0
,"numTextsRec"
:0,"inviteCount":0}}.
```

#

T 199.87.160.87:80 -> 192.168.1.5:48325 [AP] #4440

HTTP/1.1 200 OK..Date: Wed, 02 Jul 2014 22:43:11 GMT..Server: Apache..X-Host: sj2-web04..Content-Length: 589..Keep-Alive: timeout=10, max=40..Connection: Keep-Alive..Content-Type: application/

```
json....{"success":"messages
retrieved","result":{"recMessages":[{"messageId":"e5d6be661c5ed90cfb27a0fb50b33bf2","m
essageType":"normal","messageText":"At our old meetup spot?","recipientType":
```

```
"phone","recipientId":"14068522589","senderType":"phone","senderId":"14069243754","send
erName":"Kim Ill-song","time":"2014-07-02
```

```
22:43:06","messageStatus":"unread","deliveryMethod":"onnet"}],"
```

```
sentMessages":[],"brandedSystemMessages":[],"calls":[],"voicemails":[],"now":"2014-07-02
22:43:07","largestCount":1,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0
,"numTextsRec"
:0,"inviteCount":0}}.
```


#####

T 199.87.160.87:80 -> 192.168.1.5:34995 [AP] #4651

```
{ "success": "messages
retrieved", "result": { "recMessages": [ { "messageId": "e5d6be661c5ed90cfb27a0fb50b33bf2", "m
essageType": "normal", "messageText": "At our old meetup spot?", "recipientType": "phone",
```

```
"recipientId": "14068522589", "senderType": "phone", "senderId": "14069243754", "senderName
": "Kim Ill-song", "time": "2014-07-02
```

```
22:43:06", "messageStatus": "read", "deliveryMethod": "onnet"}, { "messageId"
: "b5860bdea833df4231c31dfbecbedf0d", "messageType": "normal", "messageText": "What
day?", "recipientType": "phone", "recipientId": "14068522589", "senderType": "phone", "senderId"
: "14069243754", "senderNa
```

```
me": "Kim Ill-song", "time": "2014-07-02
```

```
22:43:44", "messageStatus": "unread", "deliveryMethod": "onnet"}], "sentMessages": [ { "message
Id": "9854f7107287ad4d6a6a69b25fc3da57", "messageType": "normal", "mess
```

```
ageText": "yes", "recipientType": "phone", "recipientId": "14069243754", "senderType": "phone", "
senderId": "14068522589", "senderName": "Ann Dercover", "time": "2014-07-02
```

```
22:43:28", "messageStatus": "read"
```

```
, "deliveryMethod": "onnet"}], "brandedSystemMessages": [], "calls": [], "voicemails": [], "now": "201
4-07-02
```

```
22:43:45", "largestCount": 2, "smsCreditBalance": 0, "callingCreditBalance": 0, "numTextsSent": 0
, "n
```

```
umTextsRec": 0, "inviteCount": 0}}.
```

##

T 199.87.160.87:80 -> 192.168.1.5:34995 [AP] #4653

```
{ "success": "messages
retrieved", "result": { "recMessages": [ { "messageId": "e5d6be661c5ed90cfb27a0fb50b33bf2", "m
essageType": "normal", "messageText": "At our old meetup spot?", "recipientType": "phone",
```

```
"recipientId": "14068522589", "senderType": "phone", "senderId": "14069243754", "senderName
": "Kim Ill-song", "time": "2014-07-02
```

```
22:43:06", "messageStatus": "read", "deliveryMethod": "onnet"}, { "messageId"
: "b5860bdea833df4231c31dfbecbedf0d", "messageType": "normal", "messageText": "What
day?", "recipientType": "phone", "recipientId": "14068522589", "senderType": "phone", "senderId"
: "14069243754", "senderNa
```

```
me": "Kim Ill-song", "time": "2014-07-02
```

```
22:43:44", "messageStatus": "unread", "deliveryMethod": "onnet"}], "sentMessages": [ { "message
Id": "9854f7107287ad4d6a6a69b25fc3da57", "messageType": "normal", "mess
```

```
ageText": "yes", "recipientType": "phone", "recipientId": "14069243754", "senderType": "phone", "
senderId": "14068522589", "senderName": "Ann Dercover", "time": "2014-07-02
```

```
22:43:28", "messageStatus": "read"
```

```
, "deliveryMethod": "onnet"}], "brandedSystemMessages": [], "calls": [], "voicemails": [], "now": "201
4-07-02
```

```
22:43:45", "largestCount": 2, "smsCreditBalance": 0, "callingCreditBalance": 0, "numTextsSent": 0
, "n
```

```
umTextsRec": 0, "inviteCount": 0}}.
```


#####

T 199.87.160.87:80 -> 192.168.1.5:48377 [AP] #4804

HTTP/1.1 200 OK..Date: Wed, 02 Jul 2014 22:43:51 GMT..Server: Apache..X-Host: sj2-web09..Content-Length: 573..Keep-Alive: timeout=10, max=41..Connection: Keep-Alive..Content-Type: application/

json....{"success":"messages
retrieved","result":{"recMessages":[{"messageId":"b5860bdea833df4231c31dfbecbedf0d","messageType":"normal","messageText":"What day?","recipientType":"phone","recip

ientId":"14068522589","senderType":"phone","senderId":"14069243754","senderName":"Kim
Ill-song","time":"2014-07-02

22:43:44","messageStatus":"read","deliveryMethod":"onnet"},"sentMessages":[]

,"brandedSystemMessages":[],"calls":[],"voicemails":[],"now":"2014-07-02

22:43:45","largestCount":1,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0
,"numTextsRec":0,"inviteCount"

:0}}.

#

T 199.87.160.87:80 -> 192.168.1.5:48377 [AP] #4805

HTTP/1.1 200 OK..Date: Wed, 02 Jul 2014 22:43:51 GMT..Server: Apache..X-Host: sj2-web09..Content-Length: 573..Keep-Alive: timeout=10, max=41..Connection: Keep-Alive..Content-Type: application/

json....{"success":"messages
retrieved","result":{"recMessages":[{"messageId":"b5860bdea833df4231c31dfbecbedf0d","messageType":"normal","messageText":"What day?","recipientType":"phone","recip

ientId":"14068522589","senderType":"phone","senderId":"14069243754","senderName":"Kim
Ill-song","time":"2014-07-02

22:43:44","messageStatus":"read","deliveryMethod":"onnet"},"sentMessages":[]

,"brandedSystemMessages":[],"calls":[],"voicemails":[],"now":"2014-07-02

22:43:45","largestCount":1,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0
,"numTextsRec":0,"inviteCount"

:0}}.

T 199.87.160.87:80 -> 192.168.1.5:39570 [AP] #19458

HTTP/1.1 200 OK..Date: Wed, 02 Jul 2014 22:50:53 GMT..Server: Apache..X-Host: sj2-web05..Content-Length: 892..Keep-Alive: timeout=10, max=50..Connection: Keep-Alive..Content-Type: application/

json....{"success":"messages
retrieved","result":{"recMessages":[{"messageId":"b5860bdea833df4231c31dfbecbedf0d","messageType":"normal","messageText":"What day?","recipientType":"phone","recip

ientId":"14068522589","senderType":"phone","senderId":"14069243754","senderName":"Kim
Ill-song","time":"2014-07-02

22:43:44","messageStatus":"read","deliveryMethod":"onnet"},"sentMessages":[{"

"messageId":"3ceeadc119a0225656c73b3fbfd3418f","messageType":"normal","messageText":"I told you to pay

attention.","recipientType":"phone","recipientId":"14069243754","senderType":"phone","senderId":"14068522589","senderName":"Ann Dercover","time":"2014-07-02

22:50:32","messageStatus":"read","deliveryMethod":"onnet"},"brandedSystemMessages":[],"calls":[],"voicemails":[],"now":"2014-07-02

22:50:45","largestCount":1,"smsCreditBalance":0,"callingCreditBalance":0,"numTextsSent":0
,"numTextsRec":0,"inviteCount":0}}.

#

T 199.87.160.87:80 -> 192.168.1.5:39570 [AP] #19459

```
json....{"success":"messages
retrieved","result":{"recMessages":[{"messageId":"b5860bdea833df4231c31dfbecbedf0d","m
essageType":"normal","messageText":"What day?","recipientType":"phone","recip
```

```
ientId":"14068522589","senderType":"phone","senderId":"14069243754","senderName":"Kim  
Ill-song","time":"2014-07-02  
22:43:44","messageStatus":"read","deliveryMethod":"onnet"}}, "sentMessages":{
```

```
"messageId":"3ceeadc119a0225656c73b3fbfd3418f","messageType":"normal","messageText":"I told you to pay attention.", "recipientType":"phone", "recipientId":"14069243754", "senderType":"phone", "senderId":"14068522589", "senderName":"Ann Dercover", "time":"2014-07-02 22:50:32", "messageStatus":"read", "deliveryMethod":"onnet"}], "brandedSystemMessages":[, "calls":[, "voicemails":[, "now":"2014-07-02
```

```
22:50:45", "largestCount": 1, "smsCreditBalance": 0, "callingCreditBalance": 0, "numTextsSent": 0, "numTextsRec": 0, "inviteCount": 0}}).
```

```
#####
#####
#####
```

Filtered messageText only

```
└─$ ngrep -l Capture\ 3.pcap "messageText" | grep -E -o ".{0,0}messageText.{0,65}"
```

messageText

messageText": "Good afternoon, Ann.", "recipientType": "p
messageText": "this is a test", "recipientType": "phone", "recipientId": "1406924
messageText": "Good afternoon, Ann.", "recipientType": "p
messageText": "this is a test", "recipientType": "phone", "recipientId": "1406924
messageText": "Good afternoon, Ann.", "recipientType": "p
messageText": "Good afternoon, Ann.", "recipientType": "p
messageText": "Good afternoon, Ann.", "recipientType": "phone", "r
messageText": "Castling.", "recipientType": "phone", "recipientId": "14068522589"
messageText": "Good afternoon, Ann.", "recipientType": "phone", "r
messageText": "Castling.", "recipientType": "phone", "recipientId": "14068522589"
messageText": "Castling.", "recipientType": "phone", "recip
messageText": "Castling.", "recipientType": "phone", "recip
messageText": "Castling.", "recipientType": "phone", "recipi
messageText": "where are you?", "recipientType": "phone", "recipientId": "1406924
messageText": "Castling.", "recipientType": "phone", "recipi
messageText": "where are you?", "recipientType": "phone", "recipientId": "1406924
messageText": "I know I can't tell you that.", "recipient
messageText": "I know I can't tell you that.", "recipient
messageText": "I know I can't tell you that.", "recipientT
messageText": "Do you know that there are people investigating Kim III-Song?"
messageText": "I know I can't tell you that.", "recipientT
messageText": "Do you know that there are people investigating Kim III-Song?"
messageText": "Of course. However, they will never kno
messageText": "Of course. However, they will never kno
messageText": "Of course. However, they will never kn
messageText": "still we should be careful. Pay attention. I
messageText": "Of course. However, they will never kn
messageText": "still we should be careful. Pay attention. I

```

messageText":"At our old meetup spot?","recipientType":
messageText":"At our old meetup spot?","recipientType":
messageText":"At our old meetup spot?","recipientType":"phone",
messageText":"What day?","recipientType":"phone","recipientId":"14068522589"
messageText":"At our old meetup spot?","recipientType":"phone",
messageText":"What day?","recipientType":"phone","recipientId":"14068522589"
messageText":"What day?","recipientType":"phone","recip
messageText":"What day?","recipientType":"phone","recip
messageText":"What day?","recipientType":"phone","recip
messageText":"I told you to pay attention.","recipientType":"phone","recipie
messageText":"What day?","recipientType":"phone","recip
messageText":"I told you to pay attention.","recipientType":"phone","recipie

```

Messages Reconstructed

1. Sender Name: Kim Ill-song
Message: **Good afternoon, Ann.**
2. Sender Name: Ann
Message: **who is this?**
3. Sender Name: Kim Ill-Song
Message: **Castling.**
4. Sender: Ann
Message: **where are you?**
5. Sender: Kim Ill-Song
Message: **I know I can't tell you that.**
6. Sender: Ann
Message: **Do you know that there are people investigating Kim Ill-Song?**
7. Sender Name: Kim Ill-Song
Message: **Of course. However, they will never know it is me behind the bribes.**
8. Sender Name: Ann
Message: **still we should be careful. Pay attention. I want to meet in September at 5PM.**
9. Sender: Kim Ill-Song
Message: **At our old meetup spot?**
10. Sender: Ann
Message: **yes**
11. Sender Name: Kim Ill-Song
Message: **What day?**
12. Sender Name: Ann
Message: **I told you to pay attention**

Latitude and Longitude Coordinates

```
ngrep -l Capture\ 3.pcap "mob.mapquestapi.com" | grep -E -o ".{0,0}location.{0,45}"
```

```

location=46.85661315917969%2C-114.01860809326172 HTTP
location=46.85661315917969%2C-114.01860809326172 HTTP
location=46.85693359375%2C-114.01863098144531 HTTP/1.
location=46.85693359375%2C-114.01863098144531 HTTP/1.
location=46.85727310180664%2C-114.01868438720703 HTTP
location=46.85727310180664%2C-114.01868438720703 HTTP
location=46.857601165771484%2C-114.01866912841797 HTT
location=46.857601165771484%2C-114.01866912841797 HTT
location=46.858055114746094%2C-114.01866149902344 HTT
location=46.858055114746094%2C-114.01866149902344 HTT
location=46.8582878112793%2C-114.01864624023438 HTTP/
location=46.8582878112793%2C-114.01864624023438 HTTP/

```

location=46.858524322509766%2C-114.01863861083984 HTTP
location=46.858524322509766%2C-114.01863861083984 HTTP
location=46.858734130859375%2C-114.01864624023438 HTTP
location=46.858734130859375%2C-114.01864624023438 HTTP
location=46.85884475708008%2C-114.01864624023438 HTTP
location=46.85884475708008%2C-114.01864624023438 HTTP
location=46.858943939208984%2C-114.01864624023438 HTTP
location=46.858943939208984%2C-114.01864624023438 HTTP
location=46.859046936035156%2C-114.01864624023438 HTTP
location=46.859046936035156%2C-114.01864624023438 HTTP
location=46.85914993286133%2C-114.01864624023438 HTTP
location=46.85914993286133%2C-114.01864624023438 HTTP
location=46.859466552734375%2C-114.01864624023438 HTTP
location=46.859466552734375%2C-114.01864624023438 HTTP
location=46.85957717895508%2C-114.01864624023438 HTTP
location=46.85957717895508%2C-114.01864624023438 HTTP
location=46.85969161987305%2C-114.01864624023438 HTTP
location=46.85969161987305%2C-114.01864624023438 HTTP
location=46.85980987548828%2C-114.01864624023438 HTTP
location=46.85980987548828%2C-114.01864624023438 HTTP
location=46.85993194580078%2C-114.01864624023438 HTTP
location=46.85993194580078%2C-114.01864624023438 HTTP
location=46.86029052734375%2C-114.01863098144531 HTTP
location=46.86029052734375%2C-114.01863098144531 HTTP
location=46.86052322387695%2C-114.01863861083984 HTTP
location=46.86052322387695%2C-114.01863861083984 HTTP
location=46.860755920410156%2C-114.01863098144531 HTTP
location=46.860755920410156%2C-114.01863098144531 HTTP
location=46.86098861694336%2C-114.01863098144531 HTTP
location=46.86098861694336%2C-114.01863098144531 HTTP
location=46.861228942871094%2C-114.01863861083984 HTTP
location=46.861228942871094%2C-114.01863861083984 HTTP
location=46.86147689819336%2C-114.01863098144531 HTTP
location=46.86147689819336%2C-114.01863098144531 HTTP
location=46.86159896850586%2C-114.01863098144531 HTTP
location=46.86159896850586%2C-114.01863098144531 HTTP
location=46.86183547973633%2C-114.01862335205078 HTTP
location=46.86183547973633%2C-114.01862335205078 HTTP
location=46.862064361572266%2C-114.01861572265625 HTTP
location=46.862064361572266%2C-114.01861572265625 HTTP
location=46.862281799316406%2C-114.01860046386719 HTTP
location=46.862281799316406%2C-114.01860046386719 HTTP
location=46.86248779296875%2C-114.01860046386719 HTTP
location=46.86248779296875%2C-114.01860046386719 HTTP
location=46.86260223388672%2C-114.01859283447266 HTTP
location=46.86260223388672%2C-114.01859283447266 HTTP
location=46.86282730102539%2C-114.0185775756836 HTTP/
location=46.86282730102539%2C-114.0185775756836 HTTP/
location=46.86306381225586%2C-114.0185775756836 HTTP/
location=46.86306381225586%2C-114.0185775756836 HTTP/
location=46.86330032348633%2C-114.01856231689453 HTTP
location=46.86330032348633%2C-114.01856231689453 HTTP
location=46.863426208496094%2C-114.0185546875 HTTP/1.
location=46.863426208496094%2C-114.0185546875 HTTP/1.
location=46.86355209350586%2C-114.01854705810547 HTTP

location=46.86355209350586%2C-114.01854705810547 HTTP
location=46.86367416381836%2C-114.01853942871094 HTTP
location=46.86367416381836%2C-114.01853942871094 HTTP
location=46.8637809753418%2C-114.01853942871094 HTTP/
location=46.8637809753418%2C-114.01853942871094 HTTP/
location=46.86387252807617%2C-114.0185317993164 HTTP/
location=46.86387252807617%2C-114.0185317993164 HTTP/
location=46.863704681396484%2C-114.01164245605469 HTT
location=46.863704681396484%2C-114.01164245605469 HTT
location=46.86370849609375%2C-114.01163482666016 HTTP
location=46.86370849609375%2C-114.01163482666016 HTTP
location=46.864017486572266%2C-114.01107025146484 HTT
location=46.864017486572266%2C-114.01107025146484 HTT
location=46.864044189453125%2C-114.01074981689453 HTT
location=46.864044189453125%2C-114.01074981689453 HTT
location=46.86404800415039%2C-114.01071166992188 HTTP
location=46.86404800415039%2C-114.01071166992188 HTTP
location=46.86408996582031%2C-114.01042175292969 HTTP
location=46.86408996582031%2C-114.01042175292969 HTTP
location=46.86408996582031%2C-114.01012420654297 HTTP
location=46.86408996582031%2C-114.01012420654297 HTTP
location=46.864078521728516%2C-114.00962829589844 HTT
location=46.864078521728516%2C-114.00962829589844 HTT
location=46.864070892333984%2C-114.0094223022461 HTTP
location=46.864070892333984%2C-114.0094223022461 HTTP
location=46.86406707763672%2C-114.00910186767578 HTTP
location=46.86406707763672%2C-114.00910186767578 HTTP
location=46.86407470703125%2C-114.00875854492188 HTTP
location=46.86407470703125%2C-114.00875854492188 HTTP
location=46.86408233642578%2C-114.0084228515625 HTTP/
location=46.86408233642578%2C-114.0084228515625 HTTP/
location=46.864051818847656%2C-114.0074691772461 HTTP
location=46.864051818847656%2C-114.0074691772461 HTTP
location=46.864044189453125%2C-114.00716400146484 HTT
location=46.864044189453125%2C-114.00716400146484 HTT
location=46.864044189453125%2C-114.00694274902344 HTT
location=46.864044189453125%2C-114.00694274902344 HTT
location=46.86404800415039%2C-114.00680541992188 HTTP
location=46.86404800415039%2C-114.00680541992188 HTTP
location=46.86405563354492%2C-114.00670623779297 HTTP
location=46.86405563354492%2C-114.00670623779297 HTTP
location=46.864051818847656%2C-114.00662231445313 HTT
location=46.864051818847656%2C-114.00662231445313 HTT
location=46.864051818847656%2C-114.00646209716797 HTT
location=46.864051818847656%2C-114.00646209716797 HTT
location=46.864051818847656%2C-114.00627899169922 HTT
location=46.864051818847656%2C-114.00627899169922 HTT
location=46.864051818847656%2C-114.00605773925781 HTT
location=46.864051818847656%2C-114.00605773925781 HTT
location=46.864051818847656%2C-114.00592803955078 HTT
location=46.864051818847656%2C-114.00592803955078 HTT
location=46.86405944824219%2C-114.00563049316406 HTTP
location=46.86405944824219%2C-114.00563049316406 HTTP
location=46.86405944824219%2C-114.00534057617188 HTTP
location=46.86405944824219%2C-114.00534057617188 HTTP

location=46.86405563354492%2C-114.00506591796875 HTTP
location=46.86405563354492%2C-114.00506591796875 HTTP
location=46.864051818847656%2C-114.00477600097656 HTT
location=46.864051818847656%2C-114.00477600097656 HTT
location=46.864051818847656%2C-114.00452423095703 HTT
location=46.864051818847656%2C-114.00452423095703 HTT
location=46.864044189453125%2C-114.0042724609375 HTTP
location=46.864044189453125%2C-114.0042724609375 HTTP
location=46.864044189453125%2C-114.00414276123047 HTT
location=46.864044189453125%2C-114.00414276123047 HTT
location=46.86404037475586%2C-114.00392150878906 HTTP
location=46.86404037475586%2C-114.00392150878906 HTTP
location=46.863983154296875%2C-114.00354766845703 HTT
location=46.863983154296875%2C-114.00354766845703 HTT
location=46.86393356323242%2C-114.0035171508789 HTTP/
location=46.86393356323242%2C-114.0035171508789 HTTP/
location=46.86381912231445%2C-114.00352478027344 HTTP
location=46.86381912231445%2C-114.00352478027344 HTTP
location=46.863643646240234%2C-114.0035400390625 HTTP
location=46.863643646240234%2C-114.0035400390625 HTTP
location=46.86354446411133%2C-114.00354766845703 HTTP
location=46.86354446411133%2C-114.00354766845703 HTTP
location=46.86325454711914%2C-114.00360107421875 HTTP
location=46.86325454711914%2C-114.00360107421875 HTTP
location=46.86309051513672%2C-114.00376892089844 HTTP
location=46.86309051513672%2C-114.00376892089844 HTTP
location=46.86293411254883%2C-114.00396728515625 HTTP
location=46.86293411254883%2C-114.00396728515625 HTTP
location=46.86286163330078%2C-114.00408172607422 HTTP
location=46.86286163330078%2C-114.00408172607422 HTTP
location=46.862701416015625%2C-114.00432586669922 HTT
location=46.862701416015625%2C-114.00432586669922 HTT
location=46.86253356933594%2C-114.00457763671875 HTTP
location=46.86253356933594%2C-114.00457763671875 HTTP
location=46.862361907958984%2C-114.00481414794922 HTT
location=46.862361907958984%2C-114.00481414794922 HTT
location=46.86210632324219%2C-114.00520324707031 HTTP
location=46.86210632324219%2C-114.00520324707031 HTTP
location=46.86183547973633%2C-114.0055923461914 HTTP/
location=46.86183547973633%2C-114.0055923461914 HTTP/
location=46.86166000366211%2C-114.00584411621094 HTTP
location=46.86166000366211%2C-114.00584411621094 HTTP
location=46.86148452758789%2C-114.00609588623047 HTTP
location=46.86148452758789%2C-114.00609588623047 HTTP
location=46.86122131347656%2C-114.00647735595703 HTTP
location=46.86122131347656%2C-114.00647735595703 HTTP
location=46.86103057861328%2C-114.00672912597656 HTTP
location=46.86103057861328%2C-114.00672912597656 HTTP
location=46.860843658447266%2C-114.00699615478516 HTT
location=46.860843658447266%2C-114.00699615478516 HTT
location=46.86065673828125%2C-114.00727081298828 HTTP
location=46.86065673828125%2C-114.00727081298828 HTTP
location=46.86037063598633%2C-114.0076675415039 HTTP/
location=46.86037063598633%2C-114.0076675415039 HTTP/
location=46.859989166259766%2C-114.00820922851563 HTT

location=46.859989166259766%2C-114.00820922851563 HTTP
location=46.85979080200195%2C-114.00848388671875 HTTP
location=46.85979080200195%2C-114.00848388671875 HTTP
location=46.85969161987305%2C-114.00862121582031 HTTP
location=46.85969161987305%2C-114.00862121582031 HTTP
location=46.859500885009766%2C-114.00887298583984 HTTP
location=46.859500885009766%2C-114.00887298583984 HTTP
location=46.85930252075195%2C-114.00914001464844 HTTP
location=46.85930252075195%2C-114.00914001464844 HTTP
location=46.85910415649414%2C-114.00941467285156 HTTP
location=46.85910415649414%2C-114.00941467285156 HTTP
location=46.8590087890625%2C-114.0095443725586 HTTP/1
location=46.8590087890625%2C-114.0095443725586 HTTP/1
location=46.858829498291016%2C-114.00979614257813 HTTP
location=46.858829498291016%2C-114.00979614257813 HTTP
location=46.858646392822266%2C-114.01005554199219 HTTP
location=46.858646392822266%2C-114.01005554199219 HTTP
location=46.858375549316406%2C-114.01044464111328 HTTP
location=46.858375549316406%2C-114.01044464111328 HTTP
location=46.858123779296875%2C-114.01079559326172 HTTP
location=46.858123779296875%2C-114.01079559326172 HTTP
location=46.85795211791992%2C-114.01103973388672 HTTP
location=46.85795211791992%2C-114.01103973388672 HTTP
location=46.8577880859375%2C-114.01127624511719 HTTP/
location=46.8577880859375%2C-114.01127624511719 HTTP/
location=46.85765838623047%2C-114.0114517211914 HTTP/
location=46.85765838623047%2C-114.0114517211914 HTTP/
location=46.857513427734375%2C-114.01164245605469 HTTP
location=46.857513427734375%2C-114.01164245605469 HTTP
location=46.85749053955078%2C-114.01168823242188 HTTP
location=46.85749053955078%2C-114.01168823242188 HTTP
location=46.85747146606445%2C-114.01171112060547 HTTP
location=46.85747146606445%2C-114.01171112060547 HTTP
location=46.857418060302734%2C-114.01179504394531 HTTP
location=46.857418060302734%2C-114.01179504394531 HTTP
location=46.85733413696289%2C-114.01190948486328 HTTP
location=46.85733413696289%2C-114.01190948486328 HTTP
location=46.857234954833984%2C-114.01204681396484 HTTP
location=46.857234954833984%2C-114.01204681396484 HTTP
location=46.857181549072266%2C-114.01212310791016 HTTP
location=46.857181549072266%2C-114.01212310791016 HTTP
location=46.85708236694336%2C-114.01225280761719 HTTP
location=46.85708236694336%2C-114.01225280761719 HTTP
location=46.85697937011719%2C-114.01237487792969 HTTP
location=46.85697937011719%2C-114.01237487792969 HTTP
location=46.856834411621094%2C-114.01256561279297 HTTP
location=46.856834411621094%2C-114.01256561279297 HTTP
location=46.85672378540039%2C-114.01271057128906 HTTP
location=46.85672378540039%2C-114.01271057128906 HTTP
location=46.856597900390625%2C-114.01287078857422 HTTP
location=46.856597900390625%2C-114.01287078857422 HTTP
location=46.85647201538086%2C-114.01302337646484 HTTP
location=46.85647201538086%2C-114.01302337646484 HTTP
location=46.856319427490234%2C-114.01313018798828 HTTP
location=46.856319427490234%2C-114.01313018798828 HTTP

Coordinates Reconstructed

Latitude	Longitude
46.85661315917969	-114.01860809326172
46.85661315917969	-114.01860809326172
46.85693359375	-114.01863098144531
46.85693359375	-114.01863098144531
46.85727310180664	-114.01868438720703
46.85727310180664	-114.01868438720703
46.857601165771484	-114.01866912841797
46.857601165771484	-114.01866912841797
46.858055114746094	-114.01866149902344
46.858055114746094	-114.01866149902344
46.8582878112793	-114.01864624023438
46.8582878112793	-114.01864624023438
46.858524322509766	-114.01863861083984
46.858524322509766	-114.01863861083984
46.858734130859375	-114.01864624023438
46.858734130859375	-114.01864624023438
46.85884475708008	-114.01864624023438
46.85884475708008	-114.01864624023438
46.858943939208984	-114.01864624023438
46.858943939208984	-114.01864624023438
46.859046936035156	-114.01864624023438
46.859046936035156	-114.01864624023438
46.85914993286133	-114.01864624023438
46.85914993286133	-114.01864624023438
46.859466552734375	-114.01864624023438
46.859466552734375	-114.01864624023438
46.85957717895508	-114.01864624023438
46.85957717895508	-114.01864624023438
46.85969161987305	-114.01864624023438
46.85969161987305	-114.01864624023438
46.85980987548828	-114.01864624023438
46.85980987548828	-114.01864624023438
46.85993194580078	-114.01864624023438
46.85993194580078	-114.01864624023438
46.86029052734375	-114.01863098144531
46.86029052734375	-114.01863098144531
46.86052322387695	-114.01863861083984
46.86052322387695	-114.01863861083984
46.860755920410156	-114.01863098144531
46.860755920410156	-114.01863098144531
46.86098861694336	-114.01863098144531
46.86098861694336	-114.01863098144531
46.861228942871094	-114.01863861083984
46.861228942871094	-114.01863861083984
46.86147689819336	-114.01863098144531
46.86147689819336	-114.01863098144531
46.86159896850586	-114.01863098144531
46.86159896850586	-114.01863098144531
46.86183547973633	-114.01862335205078

46.86183547973633	-114.01862335205078
46.862064361572266	-114.01861572265625
46.862064361572266	-114.01861572265625
46.862281799316406	-114.01860046386719
46.862281799316406	-114.01860046386719
46.86248779296875	-114.01860046386719
46.86248779296875	-114.01860046386719
46.86260223388672	-114.01859283447266
46.86260223388672	-114.01859283447266
46.86282730102539	-114.0185775756836
46.86282730102539	-114.0185775756836
46.86306381225586	-114.0185775756836
46.86306381225586	-114.0185775756836
46.86330032348633	-114.01856231689453
46.86330032348633	-114.01856231689453
46.863426208496094	-114.0185546875
46.863426208496094	-114.0185546875
46.86355209350586	-114.01854705810547
46.86355209350586	-114.01854705810547
46.86367416381836	-114.01853942871094
46.86367416381836	-114.01853942871094
46.8637809753418	-114.01853942871094
46.8637809753418	-114.01853942871094
46.86387252807617	-114.0185317993164
46.86387252807617	-114.0185317993164
46.863704681396484	-114.01164245605469
46.863704681396484	-114.01164245605469
46.86370849609375	-114.01163482666016
46.86370849609375	-114.01163482666016
46.864017486572266	-114.01107025146484
46.864017486572266	-114.01107025146484
46.864044189453125	-114.01074981689453
46.864044189453125	-114.01074981689453
46.86404800415039	-114.01071166992188
46.86404800415039	-114.01071166992188
46.86408996582031	-114.01042175292969
46.86408996582031	-114.01042175292969
46.86408996582031	-114.01012420654297
46.86408996582031	-114.01012420654297
46.864078521728516	-114.00962829589844
46.864078521728516	-114.00962829589844
46.864070892333984	-114.0094223022461
46.864070892333984	-114.0094223022461
46.86406707763672	-114.00910186767578
46.86406707763672	-114.00910186767578
46.86407470703125	-114.00875854492188
46.86407470703125	-114.00875854492188
46.86408233642578	-114.0084228515625
46.86408233642578	-114.0084228515625
46.864051818847656	-114.0074691772461
46.864051818847656	-114.0074691772461
46.864044189453125	-114.00716400146484
46.864044189453125	-114.00716400146484

46.864044189453125	-114.00694274902344
46.864044189453125	-114.00694274902344
46.86404800415039	-114.00680541992188
46.86404800415039	-114.00680541992188
46.86405563354492	-114.00670623779297
46.86405563354492	-114.00670623779297
46.864051818847656	-114.00662231445313
46.864051818847656	-114.00662231445313
46.864051818847656	-114.00646209716797
46.864051818847656	-114.00646209716797
46.864051818847656	-114.00627899169922
46.864051818847656	-114.00627899169922
46.864051818847656	-114.00605773925781
46.864051818847656	-114.00605773925781
46.864051818847656	-114.00592803955078
46.864051818847656	-114.00592803955078
46.86405944824219	-114.00563049316406
46.86405944824219	-114.00563049316406
46.86405944824219	-114.00534057617188
46.86405944824219	-114.00534057617188
46.86405563354492	-114.00506591796875
46.86405563354492	-114.00506591796875
46.864051818847656	-114.00477600097656
46.864051818847656	-114.00477600097656
46.864051818847656	-114.00452423095703
46.864051818847656	-114.00452423095703
46.864044189453125	-114.0042724609375
46.864044189453125	-114.0042724609375
46.864044189453125	-114.00414276123047
46.864044189453125	-114.00414276123047
46.86404037475586	-114.00392150878906
46.86404037475586	-114.00392150878906
46.863983154296875	-114.00354766845703
46.863983154296875	-114.00354766845703
46.86393356323242	-114.0035171508789
46.86393356323242	-114.0035171508789
46.86381912231445	-114.00352478027344
46.86381912231445	-114.00352478027344
46.863643646240234	-114.0035400390625
46.863643646240234	-114.0035400390625
46.86354446411133	-114.00354766845703
46.86354446411133	-114.00354766845703
46.86325454711914	-114.00360107421875
46.86325454711914	-114.00360107421875
46.86309051513672	-114.00376892089844
46.86309051513672	-114.00376892089844
46.86293411254883	-114.00396728515625
46.86293411254883	-114.00396728515625
46.86286163330078	-114.00408172607422
46.86286163330078	-114.00408172607422
46.862701416015625	-114.00432586669922
46.862701416015625	-114.00432586669922
46.86253356933594	-114.00457763671875

46.86253356933594	-114.00457763671875
46.862361907958984	-114.00481414794922
46.862361907958984	-114.00481414794922
46.86210632324219	-114.00520324707031
46.86210632324219	-114.00520324707031
46.86183547973633	-114.0055923461914
46.86183547973633	-114.0055923461914
46.86166000366211	-114.00584411621094
46.86166000366211	-114.00584411621094
46.86148452758789	-114.00609588623047
46.86148452758789	-114.00609588623047
46.86122131347656	-114.00647735595703
46.86122131347656	-114.00647735595703
46.86103057861328	-114.00672912597656
46.86103057861328	-114.00672912597656
46.860843658447266	-114.00699615478516
46.860843658447266	-114.00699615478516
46.86065673828125	-114.00727081298828
46.86065673828125	-114.00727081298828
46.86037063598633	-114.0076675415039
46.86037063598633	-114.0076675415039
46.859989166259766	-114.00820922851563
46.859989166259766	-114.00820922851563
46.85979080200195	-114.00848388671875
46.85979080200195	-114.00848388671875
46.85969161987305	-114.00862121582031
46.85969161987305	-114.00862121582031
46.859500885009766	-114.00887298583984
46.859500885009766	-114.00887298583984
46.85930252075195	-114.00914001464844
46.85930252075195	-114.00914001464844
46.85910415649414	-114.00941467285156
46.85910415649414	-114.00941467285156
46.8590087890625	-114.0095443725586 1
46.8590087890625	-114.0095443725586 1
46.858829498291016	-114.00979614257813
46.858829498291016	-114.00979614257813
46.858646392822266	-114.01005554199219
46.858646392822266	-114.01005554199219
46.858375549316406	-114.01044464111328
46.858375549316406	-114.01044464111328
46.858123779296875	-114.01079559326172
46.858123779296875	-114.01079559326172
46.85795211791992	-114.01103973388672
46.85795211791992	-114.01103973388672
46.8577880859375	-114.01127624511719
46.8577880859375	-114.01127624511719
46.85765838623047	-114.0114517211914
46.85765838623047	-114.0114517211914
46.857513427734375	-114.01164245605469
46.857513427734375	-114.01164245605469
46.85749053955078	-114.01168823242188
46.85749053955078	-114.01168823242188

46.85747146606445	-114.01171112060547
46.85747146606445	-114.01171112060547
46.857418060302734	-114.01179504394531
46.857418060302734	-114.01179504394531
46.85733413696289	-114.01190948486328
46.85733413696289	-114.01190948486328
46.857234954833984	-114.01204681396484
46.857234954833984	-114.01204681396484
46.857181549072266	-114.01212310791016
46.857181549072266	-114.01212310791016
46.85708236694336	-114.01225280761719
46.85708236694336	-114.01225280761719
46.85697937011719	-114.01237487792969
46.85697937011719	-114.01237487792969
46.856834411621094	-114.01256561279297
46.856834411621094	-114.01256561279297
46.85672378540039	-114.01271057128906
46.85672378540039	-114.01271057128906
46.856597900390625	-114.01287078857422
46.856597900390625	-114.01287078857422
46.85647201538086	-114.01302337646484
46.85647201538086	-114.01302337646484
46.856319427490234	-114.01313018798828
46.856319427490234	-114.01313018798828

References

Wireshark (no date) 5.7. *exporting data*. Available at: https://www.wireshark.org/docs/wsug_html_chunked/ChIOExportSection.html [Accessed: December 9, 2022].

GCHQ (no date) CyberChef. Available at: <https://gchq.github.io/CyberChef/> [Accessed: December 10, 2022].

BrainyQuote (no date) Edward Snowden quotes, BrainyQuote.com. Available at: https://www.brainyquote.com/quotes/edward_snowden_523849 [Accessed: December 11, 2022].

mobisoftinfotech (no date) Mi Map Tools:GeoPlotter, MI Map Tools: GeoPlotter. Available at: <https://mobisoftinfotech.com/tools/plot-multiple-points-on-map/> [Accessed: December 12, 2022].