Abertay University

Network Forensics

Mairi MacLeod: 1700231

CMP416 - Digital Forensics 2

BSc(Hons) Ethical Hacking

5th January 2021

Contents

1 Investigation of Capture1.pcap **4**

1.1 Folder Contents . . . 4

1.2 Searching for Steganography . . . 5

2 Investigation of Capture2.pcap **7**

2.1 Finding and Decoding Messages . . . 7

2.2 Conversations' Content . . . 7

3 Investigation of Capture3.pcap **9**

3.1 Locating the Files . . . 9

3.2 Creating the Image File . . . 10

4 Investigation of Capture4.pcap **11**

4.1 Conversation Content . . . 11

4.2 Finding the Location . . . 11

5 References **13**

6 Appendices **14**

6.1 Capture1.pcap . . . 14

6.1.1 Diagram of Documents.zip's contents . . . 14

6.1.2 Translation of GoT Spoilers.docx . . . 14

6.1.3 Translation of NorthKorea.docx . . . 15

6.1.4 PiD.docx . . . 15

6.1.5 NK.jpg . . . 16

6.1.6 Translation of Rules 1.docx . . . 16

6.1.7 Translation of Rules 2.docx . . . 17

6.1.8 Translation of Rules 3.docx . . . 17

6.1.9 Translation of Rules 4.docx . . . 17

6.1.10 Translation of Rules 5.docx . . . 17

6.1.11 Translation of Rules 6.docx . . . 19

6.1.12 Translation of Rules 7.docx . . . 19

6.1.13 Translation of track6.docx . . . 20

6.1.14 Translation of track10.docx . . . 20

6.1.15 BillOfRights.txt . . . 23

6.1.16 NorthKorea.jpeg . . . 30

6.1.17 broken.py 30
6.2 Capture2.pcap 32
6.2.1 Messages between Ill-Song and 'Razor1' 32
6.2.2 Messages between Ill-Song and 'Genius1' 32
6.2.3 Messages between Ill-Song and Method 32
6.2.4 Messages between Ill-Song and Killah 33
6.2.5 Messages between Ill-Song and Raekwon 33
6.3 Capture3.pcap 34
6.3.1 Contents of Found Zipped Archives 34
6.3.2 Snowden Quote Image 35
6.3.3 Kim Jong-Un Image 35
6.3.4 Unsuccessful Reconstruction of Transformers Image 36
6.4 Capture4.pcap 37
6.4.1 Messages between Ill-Song and Decover 37

1 Investigation of Capture1.pcap

For this case the investigator was looking for downloaded files, the first step was to export files from the capture. This revealed nine items, three zipped archives, five `.ini` files and a file called *srsvc*, assumed to be a Windows *srsvc.dll*. *(Figure 1)*

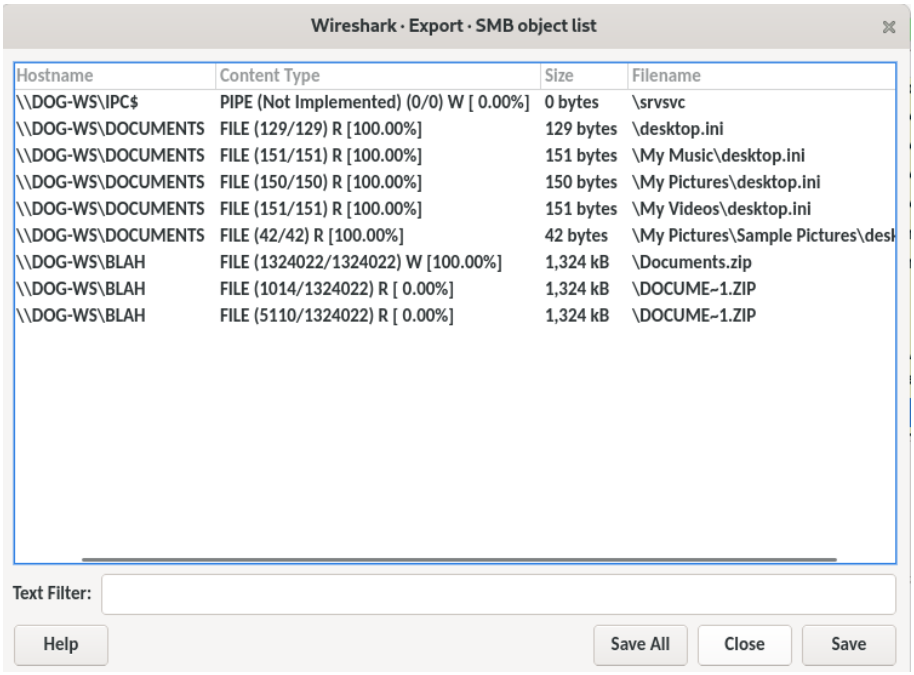


Figure 1: SMB objects found

After exporting these files the traffic streams were tracked back, this revealed more information regarding how they were downloaded and the folders which were browsed through via Server Message Block (SMB). SMB provides shared access to resources and files between computers.

1.1 Folder Contents

Both *DOCUME.ZIP* folders were empty but as the hashes differed these were clearly not the same file. Documents.zip contained multiple files and folders within itself. *(Appendix 5.1.1)*. The first folder *Actual Documents* contained three `.docx` files which contained with Base64 encoded text: *GoT spoilers*, *NorthKorea* and *PiD*.

GoT spoilers.docx decoded to four sentences that list various events that happen in the Game of Thrones series. *NorthKorea.docx* when decoded is written in Russian and details a theory that the North Korean government is planning on travelling back in time to win the Korean war. The final document in this folder, *PiD.docx*, contains two images and the text alleges that Beatles singer Paul McCartney has been dead for years and the author replaced him. *(Appendices 5.1.2 - 5.1.4)*

In the second folder, *Chess Boxing*, there are seven `.docx` files and a `JPEG` image. The seven text documents contain the rule regarding the sport 'chess boxing'; again encoded using base64. The image, *NK.jpg*, is of the North Korean flag. *(Appendices 5.1.6 - 5.1.12)*

The third folder, *Enter the WuTang*, contains two more `.docx` files encoded with base64. The first file is a list of usernames, the investigator assumes these to be the aliases of the persons involved in the potential bribery incident. *(Figure 2)* The second file, *track10.docx*, is the lyrics for a Wu Tang Clan song. *(Appendices 5.1.13 and 5.1.14)*

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

Figure 2: Decoded Contents of track6.docx

More Documents is the next notable folder and contains the text file which contains a transcript of the American Bill of Rights. The only other item in this folder is another image of the North Korean flag. *(Appendices 5.1.15 and 5.1.16)*

The final folder is zipped and contains three untitled folders a 'untitled folder 2' and finally an empty folder called SilentEye.

1.2 Searching for Steganography

The images, NK.jpg and NorthKorea.jpeg are on first appearances just photos of the North Korean flag. However, the investigator noted that NorthKorea.jpeg was significantly larger in file size and decided to check for steganography. The command `binwalk -e [filename]` was used and this revealed a zipped folder called *D7D* in *NorthKorea.jpeg*. *(Figure 3) (ReFirm Labs, 2021)*

```
[mairi@speedy Documents]$ binwalk -e Chess\ Boxing/NK.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 1600 x 800, 8-bit/color RGBA, non-interlaced

[mairi@speedy Documents]$ binwalk -e More\ Documents/NorthKorea.jpeg

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

Figure 3: Binwalk Results for NorthKorea.jpeg

This contained an untitled folder that contains a Python script called broken.py. *(Appendix 5.1.17)* As the name suggests the script does not work and contains many programming errors. It appears that it was created to try and encode files, this coupled with the fact that it was hidden inside of another file implies that the use case for this script was potentially to hide documents related to the bribing of chess boxing officials.

2 Investigation of Capture2.pcap

2.1 Finding and Decoding Messages

The PCAP was for IRC traffic and exported into a separate pcap file which was then filtered further using `irc.response`. This revealed all of the sent and received IRC messages and reduced the number of packets to view from 26320 to 198. The packets the investigator was interested in had the caption PRVMSG in the info section of the packet.

This traffic listed the sender and recipient followed by the message content. *(Figure 4)* All messages were encoded at least twice, all used base64 as the final obfuscating method but the other encoding methods varied on who sent the message. *GitHub, 2019) Ill-Song* favoured using Base32 on the first encoding. *Razor1*, *Method* and *Raekwon* used Hexadecimal encoding. *Genius1* and *Killah* used Octal.

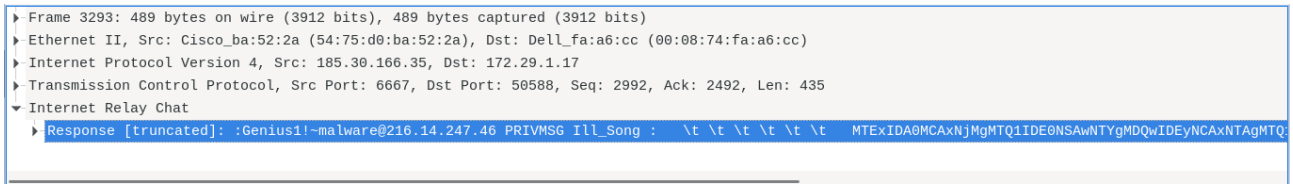


Figure 4: Contents of IRC Packet

2.2 Conversations' Content

The decoded the contents of the messages can be seen in Appendices 5.2.1 - 5.2.5 but a summary of them is as follows:

- Ill-Song contacts Mr.Razor
  - Ill-Song offered to send Razor a gift to 'encourage' his support of the Chess Boxing World Title being held in Pyongyang.
  - Razor agrees to this stating that he hopes Ill-Song pays for an expensive holiday from the "city of love" which they haggle to a price of $700,000.
  - Mr. Razor asks where he can meet Ill-Song who says he will give him an address at a later date.
- Ill-Song then messages the user Genius1; it can be inferred that this is Mr. Genius from the `track6.docx` list from the earlier investigation. *(Appendix 5.1.13)*
  - Ill-Song states that they have had previous conversations about a search that Genius1 is undertaking.
  - Genius1 then asks where they can meet Ill-Song who responds that they can go to Caracas by the end of the week.
  - Genius1 is cautious about this and asks if they can meet elsewhere.
  - Ill-Song says they will message Genius1 later with another location using a more secure messaging service.
- The third conversation is between Ill-Song and Mr. Method.

  - Ill-Song shares their excitement surrounding the idea of this event being held in the Peoples' Republic of Korea (PRK)
  - Method states their disinterest in communicating with Ill-Song due to their understanding of who Ill-Song is.
  - Ill-Song asks Method to reconsider to which Method replies "Do not speak to me again" ending the communication.

- Ill-Song attempts to communicate with Mr. Killah
  - Ill-Song asks about the weather, where Mr Killah is, in Qatar.
  - Killah requests the identity of who is messaging him
  - Ill-Song explains his motives and offers a bribe
  - Mr. Killah is offended and rejects the bribery offer wholeheartedly.

- The last conversation found was between Ill-Song and Mr. Raewkon.
  - After being asked if he had spoken to Mr. Razor, Raewkon stated that he would not be "so easily bought" and demanded a minimum of 20,000,000 Rubles.
  - Ill-Song agreed to this amount and said that he will send the drop off location information at a later date.

In summary; Mr. Razor and Mr. Raekwon explicitly took bribes from Ill-Song, it is heavily implied that Mr. Genius did as well but no amount is mentioned in the messages and both Mr. Killah and Mr. Method outright refuse any form of bribery. As for their expected locations; Razor1 is in Paris, Genius1 is in Caracas, Killah is in Qatar, Raekwon is in Russia and Method is unknown.

3 Investigation of Capture3.pcap

3.1 Locating the Files

First the PCAP was filtered for `ftp-data` traffic in order to investigate what files were transferred. This lead the investigator to find two `.zip` files: *ojd34.zip* and *sandofwhich.zip*. Further investigation of the PCAP traffic revealed three more archives, *34jdsioj.zip*, *breaking_bad_season6.zip* and *canc3l.zip*. In order to extract the contents the packets referring to these archives were exported to a separate PCAP file and `binwalk -e` was used to gather the data. *(Figures 5 and 6) (ReFirm Labs, 2021)*

```
[mairi@speedy Forensics 2]$ binwalk -e sandwitchzip

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: sandofwhich/destroy.jpg
1123          0x463           Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: sandofwhich/for.jpg
2242          0x8C2           Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: sandofwhich/freedom.jpg
3365          0xD25           Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: sandofwhich/good.jpg
4485          0x1185          Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: sandofwhich/government.jpg
5611          0x15EB          Zip archive data, at least v2.0 to extract, compressed size: 860, uncompressed size: 1070, name: sandofwhich/I.jpg
6518          0x1976          Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: sandofwhich/in.jpg
7636          0x1DD4          Zip archive data, at least v2.0 to extract, compressed size: 5436, uncompressed size: 5436, name: sandofwhich/NSA.jpg
13121         0x3341          Zip archive data, at least v2.0 to extract, compressed size: 5436, uncompressed size: 5436, name: sandofwhich/rights.jpg
18609         0x48B1          Zip archive data, at least v2.0 to extract, compressed size: 5436, uncompressed size: 5436, name: sandofwhich/security.jpg
24770         0x60C2          End of Zip archive, footer length: 22
```

Figure 5: Contents of sandofwhich.zip

```
[mairi@speedy Forensics 2]$ binwalk -e ojd34zip

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: ojd34/allow.jpg
1115          0x45B           Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: ojd34/and.jpg
2228          0x8B4           Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: ojd34/around.jpg
3344          0xD10           Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: ojd34/basic.jpg
4459          0x116B          Zip archive data, at least v2.0 to extract, compressed size: 984, uncompressed size: 1051, name: ojd34/building.jpg
5491          0x1573          Zip archive data, at least v2.0 to extract, compressed size: 954, uncompressed size: 1070, name: ojd34/cant.jpg
6489          0x1959          Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: ojd34/conscience.jpg
7609          0x1DB9          Zip archive data, at least v2.0 to extract, compressed size: 5436, uncompressed size: 5436, name: ojd34/terrorism.jpg
13094         0x3326          Zip archive data, at least v2.0 to extract, compressed size: 5436, uncompressed size: 5436, name: ojd34/Watergate.jpg
18579         0x4893          Zip archive data, at least v2.0 to extract, compressed size: 5436, uncompressed size: 5436, name: ojd34/web-based.jpg
24692         0x6074          End of Zip archive, footer length: 22
```

Figure 6: Contents of ojd34.zip

This revealed that all of the zipped archives contained a number of files ending in `.jpg`. *(Appendix 5.3.1)* However when trying to open them it was revealed that they were not JPEGs as only three of them actually contained the required magic number, `0x4A464946`, to start an image file. *(Figure 7) (Kessler, 2019)* This implies that the other files may fit together and create one larger image as opposed to being individual images themselves.

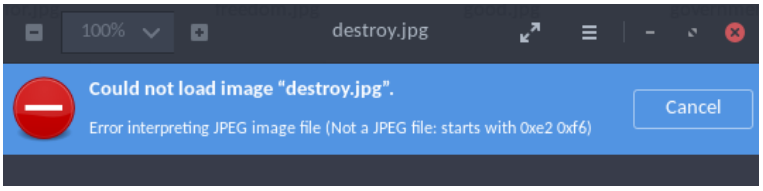


Figure 7: Error Message When Image Was Opened

3.2 Creating the Image File

It was noted that some of the filenames were all words found in a famous quote by Edward Snowden.

““I can’t in good conscience allow the US 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, 2013

The investigator then decided to attempt to piece together the image by using `cat` to combine all of the files together in the order that their name’s appear in the quote, as shown below.

```
[mairi@speedy quote]$ cat I.jpg cant.jpg in.jpg good.jpg conscienc
e.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 mass
ive.jpg surveillance.jpg machine.jpg theyre.jpg secretly.jpg build
ing.jpg > fullImage.jpg
```

Figure 8: Command for Creating Full Image

This revealed an image of a chess board. Out of the other files ending in `.jpg` found two of them contain the required magic number for a JPEG implying that two more image files exist. The leftover `.jpg` files did not appear to belong to any quote so the investigator had to use trial an error in attempting to recover the full images. One of them was successfully reconstructed, it contained an image of the North Korean leader Kim Jong-Un, but the other, an image of a Transformers character, was not. In both reconstructed images steganography was searched for but no hidden files were found. *(Appendices 5.3.2 - 5.3.4)*

4 Investigation of Capture4.pcap

As the investigator was looking for communications they first attempted to filter for AIM traffic. After this revealed nothing filtering for http traffic was instead attempted and the TCP streams investigated, in order to see if another messaging service was used. This revealed that Ill-Song and Ann Decover had been texting each other using the application TextFree.

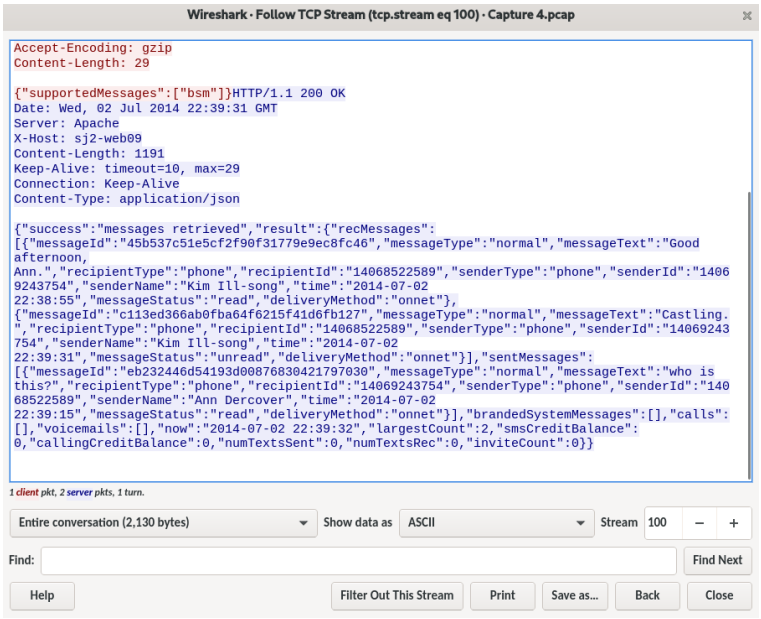


Figure 9: TCP Stream Revealing the Start of Their Communications

4.1 Conversation Content

As the messages contents were stored in JSON the investigator put all of the messages into a `.txt` file and used the command `cat messages.txt | jq` to display them in a more readable format. The messages reveal that Ill-Song is aware that they are being investigated in regards to the bribery case, Ann asks him to be careful and requests that they meet in their 'old meetup spot' at 5pm in September. *(Appendix 5.4.1)*.

The next step was to attempt to find the location of their meeting and the exact date date in September. As there were no more texts between them after the above messages the investigator decided to look elsewhere for this information. After looking through the traffic sent from Decover's IP address, 192.168.1.5, the investigator discovered multiple calls to a webpage `mob.mapquestapi.com`. As they held location data they were then filtered using `http.host==mob.mapquestapi.com` and the 116 packets were exported to a csv file.

4.2 Finding the Location

In order to plot the points onto a map the investigator decided to use Keyhole Markup Language (KML). *(Google Developers, 2020)* This allowed the investigator to insert the co-ordinates from the csv file into a KML file which displays all of them as points on a map. To

separate the location data from the other packet information a command was ran that used a series of cutting unnecessary data and replacing characters to make a csv that held only the latitude and longitude of each location. *(Figure 10)* Once the data was organised correctly, a CSV to KML converter was used to put the data into the correct format for displaying on a map. *(Convertcsv.com, 2013)*

```
[mairi@speedy PCAPs]$ tail -n116 location.csv | cut -d, -f7 | cut -d\& -f4 | awk '{ print $1 }' | sed 's_%2C_,_g;s_location=__g' > loca
tiondata.csv
```

Figure 10: Command for Extracting Location Data

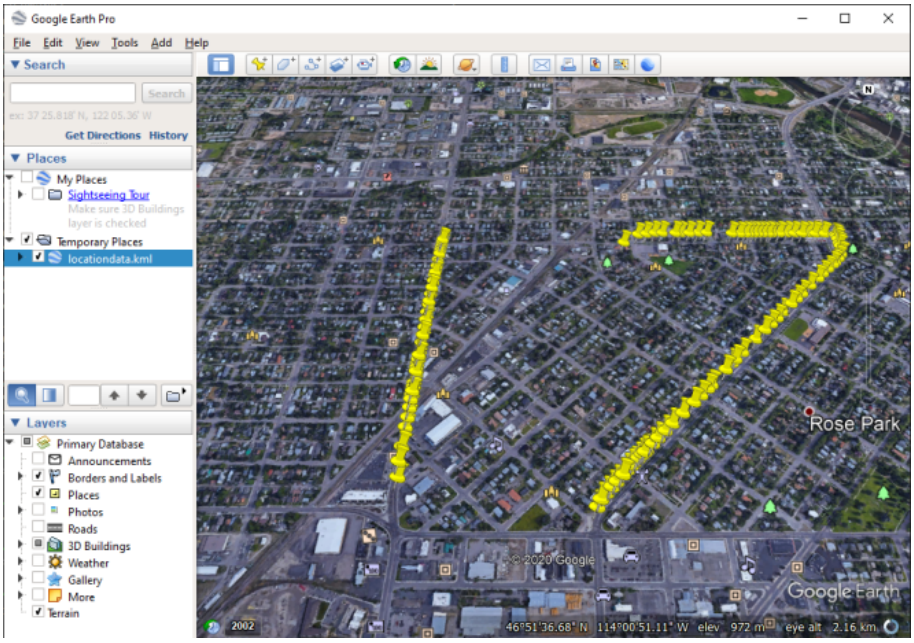


Figure 11: Map with Points Plotted

As shown above this resulted in a map with the points creating a seventeen, which implies that the date Ann and Kim are to planning on meeting is the 17th of September at 5pm.

5 References

Convertcsv.com. (2013). *CSV To KML Converter.* [online] Available at: https://www.convertcsv.com/csv-to-kml.htm [Accessed 3 Jan. 2021].

Github (2019). *CyberChef.* [online] Available at: https://gchq.github.io/CyberChef/. [Accessed 20 Dec. 2020]

Google Developers. (2020). *Keyhole Markup Language.* [online] Available at: https://developers.google.com/kml/ [Accessed 3 Jan. 2021].

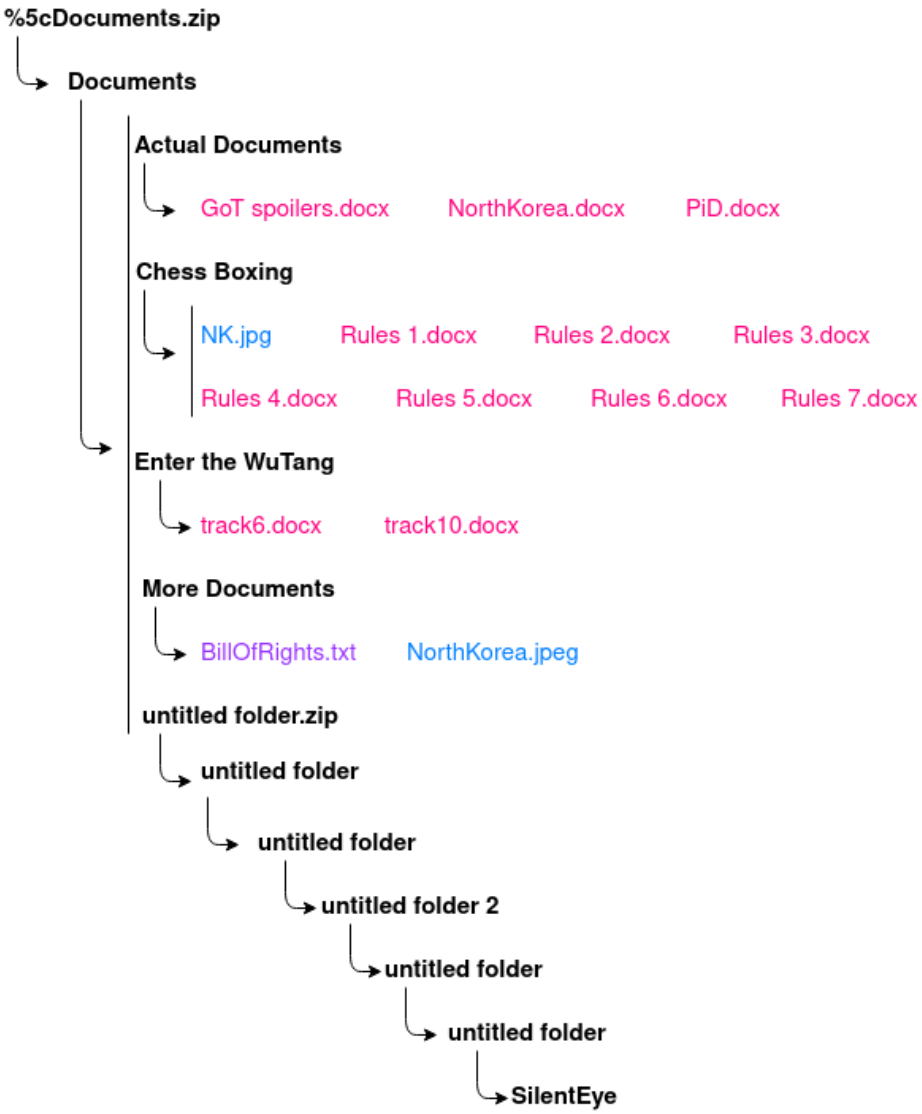
Kessler, G. (2019). *File Signatures.* [online] Garykessler.net. Available at: https://www.garykessler.net/library/file_sigs.html. [Accessed 26 Dec. 2020]

ReFirm Labs. (2020). *Binwalk — Firmware Extraction.* [online] Available at: https://www.refirmlabs.com/binwalk/ [Accessed 26 Dec. 2020].

6 Appendices

6.1 Capture1.pcap

6.1.1 Diagram of Documents.zip's contents



6.1.2 Translation of GoT Spoilers.docx

Translation:
Jon Snow burns down Winterfell (again) and the Wall.
Hodor kills Theon.
Daenerys gets eaten by a dragon.
Stannis falls in love with Tyrion.

6.1.3 Translation of NorthKorea.docx

(Original Russian):
Для кого это может касаться:

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

Пожалуйста, Оби-Ван, ты моя единственная надежда.

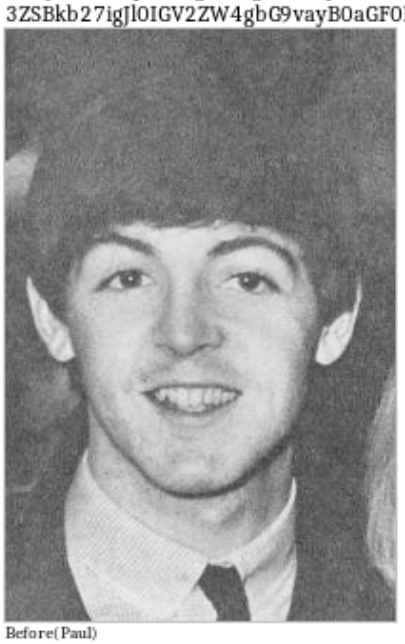
Translation (English):
For whom it may concern:

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

Please Obi-Wan, you are my only hope.

6.1.4 PiD.docx

RGVhciBFZCwNCg0KWWVhaCBJIHRvdGFsbHkgdG9vayBvdmVyIGZvciBQYXVsIGFm
dGVyIGhlIGRpZWQgaW4g4oCZNjYuIFlvdSBnb3QgbWUuIEFzIHlvdSBjYW4gc2VlLCB
3ZSBkb27igJl0IGV2ZW4gbG9vayB0aGF0IG11Y2ggYWxpa2U6DQo=



Before(Paul)

After(Me)

IAkgCQ0KQmVmb3JlKFBhdWwpIAkJCQkJQWZ0ZXIoTWUpDQoNCldlIGFyZW7igJl0I
GV2ZW4gdGhlIHNhbWUgaGVpZ2h0ISBXaGF0IGNhbiBJIHNheSwgcGVvcGxlIGFyZSB
zdHVwaWQuDQoNCg0KVGhhbmtzIGZvciB0aGUgaW5xdWlyeSwNCg0KV2lsbGlhbSB
DYW1wYmVsbA0KKFBhdWwgTWNDYXJ0bmV5KQ0K

Translation:
Dear Ed,
Yeah I totally took over for Paul after he died in 66. You got me. As you can see, we don' even look that much alike: We aren't even the same height! What can I say, people are stupid.
Thanks for the inquiry,
William Campbell(Paul McCartney)

6.1.5 NK.jpg

6.1.6 Translation of Rules 1.docx

1. SUMMARY OF RULES. MAIN POINTS. TOUCH MOVE rule strictly applies. • If a piece is touched, then it must be moved (if a legal move is available) • If an opponent's piece is touched, it must be taken (if legal). COUNTDOWN IF STALLING FOR TIME.In general a player manages how much or little time to take for each move, and this is fine! However, if a player clearly plays far too slowly for the specific position, for example when he is facing unavoidable checkmate, the arbiter will do a countdown. He will point at the board, and warn the player by counting to 10 with his hands (just like a boxing referee). If the player has not moved by the count of 10, he loses the game and the match. Note there is no minimum time to make a move! Also, even if there is only 1 legal move, the player should be allowed some time to psychologically compose themselves. It should be considered that a weak player may not realise he only has 1 legal move. CHESS CLOCK PROTOCOL. The chess clock must be pressed with the SAME HAND that moves the piece. PRESSING CHECK CLOCK. It is the player's responsibility to press his or her clock between chess moves. The competitors may agree in advance to allow the arbiter to issue reminders – especially if both fighters are new to chessboxing. PIECES KNOCKED DOWN OR NOT PROPERLY ON A SQUARE. If a player knocks down a piece whilst making a move or does not put it properly on a square, he should properly re-position or re-centre the piece in HIS OWN clock time. An offence that puts off the opponent could be punished by adding time to the opponent's clock.

OTHER RULES to NOTE • Resignation protocol. For the benefit of the audience, players are strongly encouraged to play until checkmate. If you want to resign (submit) prior to checkmate, do this by knocking over your king and offering a handshake. • Illegal move. An illegal move must be retracted. The arbiter has the discretion to punish with a time penalty, or disqualify after 3 illegal moves. Extra allowances can be made for novice players. • Speaking to the arbiter. If a player needs to speak to the arbiter during the chess game, he should remove his headphones. The arbiter will then stop the clock to listen. • Playing to win on time. If a position is a completely drawn position, and the arbiter believes a player is quickly moving pieces only to win on time, then the arbiter can declare the game a draw. • Chess Draw. A chess draw will be followed by one boxing

round (unless the maximum number of boxing rounds has already happened). The chessboxing bout will therefore be won by whoever has amassed the most boxing points – judged by punches thrown and overall aggression. • Drinks Fighters are allowed to bring water to the chess table. • Cuts In most cases, except for the most superficial examples, a cut will lead to the fight being stopped and a TKO declared. • General Advice Competitors are reminded that they do not need to move quickly, even if their opponent moves quickly. Adrenaline drastically changes your sense of time. Experience shows that a player is OK until he has 2 minutes of time remaining on the clock, when moves should be speeded up.

6.1.7 Translation of Rules 2.docx

2. ENFORCEMENT OF CHESS RULES In the event of a breach of the rules a penalty can be imposed at the arbiter's discretion.

6.1.8 Translation of Rules 3.docx

3. PENALTIES FOR RULE BREACHES A chess penalty could take the form of: • The offence will act as a tie-break if both the boxing and chess are drawn. This is the minimum (default) penalty and applies if there is no other penalty. • 30 seconds is subtracted from the offender's clock. • Forfeit of the bout. This could occur for a serious disciplinary offence, deliberate foul play or a repeated breach (e.g. a total of 3 illegal moves).

6.1.9 Translation of Rules 4.docx

4. CHESS CLOCK MALFUNCTION In the unlikely event the electronic chess clock ceases to operate during a chess round, the arbiter will do one of following, depending on the estimated disruption to the players and spectators: • Stop the clock and resolve the problem. • Stop the clock and replace it with a new clock. This action is most likely if there is a repeated malfunction, or it's one of the later chess rounds where a player is short of time.

6.1.10 Translation of Rules 5.docx

5. WCBA CHESS RULES FOR CHESSBOXING Chess tournament rules have legal points that casual players may be unfamiliar with. The official laws of chess are on the website of FIDE, the chess governing body http://www.fide.com/component/handbook/?id=32andview=category. Highlighted below are legal points that cause most disputes in tournament chess situations. In addition, some chessboxing laws differ from FIDE rules in order to (i.) ensure the paying public is entertained, (ii.) keep the game flowing with minimal disruption, and (iii.) minimise verbal communication with the competitors. These differences are highlighted where they occur.

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

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

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

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

"J'Adoube" rule. Normal Chess Rules • If a piece is off centre and is annoying you, state "j'adoube" or "I adjust" BEFORE adjusting its position on the square. One of these phrases should be used regardless of the player's home language. • If you state "j'adoube" after or during the piece adjustment, then it counts as a touch move. • You should only adjust pieces whilst your clock is running. Adjusting during your opponent's time is forbidden as it is a distraction. Chessboxing Rules (adapted because both players have headphones) • With headphones on it is simplest if players don't try to J'adoube. Pieces will be nicely centred by the arbiter between each chess round. However, if the urge to J'adoube becomes irresistible, follow the below procedure... • Clearly turn to the arbiter and mouth "J'adoube" AND give the J'adoube hand signal specially developed for chessboxing. Then adjust the piece as in a normal chess game. • The j'adoube hand signal is the 'OK' hand gesture, creating a circle with the thumb and first finger.

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

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

Draw by threefold repetition • If the same position occurs 3 times (and with the same player to move), the player can claim a draw ONLY WHEN IT IS HIS MOVE. He should stop the clock after the opponent's last move, remove his headphones and TELL the arbiter what move he WOULD play to get into the 3rd repetition. DO NOT PLAY THE MOVE, DO NOT PRESS THE CLOCK. If the player is unsure how to pause the clock, then he can take off his headphones and claim the draw. The arbiter will stop the clock as the headphones come off. If the draw claim is correct and the claimant runs out of time after removing his headphones, the draw will hold. • A draw by repetition normally occurs by perpetual check so is easy to identify.

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

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

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

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

6.1.11 Translation of Rules 6.docx

6. CHESS DRAW IN RELATION TO THE CHESSBOXING BOUT

If a chess draw is declared in any round, there will be at most only one boxing round thereafter. If the chess draw occurs in the final round, then there will be no further boxing round, in line with the original schedule. In the unlikely event that the chess game is drawn AND the boxing is a tie on points, then the player with the fewest chess penalties is the winner. If these are equal the bout will be declared a draw.

6.1.12 Translation of Rules 7.docx

7. HOW CHESS PIECES MOVE – FINER POINTS THAT CONFUSE BEGINNERS The complete official laws of chess are on the website of FIDE, the chess governing body. The Appendix on the above link explains chess notation, and instances where 'blitz' or 'rapid' chess rules differ from normal 'long play' time controls. Castling • Castling is one move • The king always moves 2 squares, and the rook then goes next to the king on the other side. • All squares between king and rook must be clear. Castling cannot capture a piece. • White Kingside castling moves the King from e1 to g1, and the Rook from h1 to f1. • White Queenside castling moves the King from e1 to c1, and the Rook from a1 to d1. Castling is not a legal move when... • ... the king is in check • ... the king moves into check • ... the king crosses over a square that is attacked (many players are unaware of this subtle point) • ... a piece is on a square between king and rook • ... the king has previously moved, even if it has since returned to its original square • ... the rook to be castled has previously moved, even if it has since returned to its original square Pawn

Promotion A pawn reaching the eighth rank is 99% of times promoted to a queen, but it can also be ‘under-promoted’ to a knight, bishop or rook. En Passant A special type of pawn capture. A pawn attacking a square crossed by an opponent‘s pawn which has advanced two squares in one move from its original square may capture this opponent‘s pawn as though the latter had been moved only one square. This capture is only legal on the move following this advance and is called an ‘en passant‘ capture. ‘En passant’ is French for ‘as it passes’. See http://en.wikipedia.org/wiki/En_passant for visual examples.

6.1.13 Translation of track6.docx

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

6.1.14 Translation of track10.docx

”Protect Ya Neck”
”So what’s up man?
Cooling man”
”Chilling chilling?”
”Yo you know I had to call, you know why right?”
”Why?”
”Because, yo, I never ever call and ask, you to play something right?”
”Yeah”
”You know what I wanna hear right?”
”What you wanna hear?
I wanna hear that Wu-Tang joint”
”Wu-Tang again?”
”Ah yeah, again and again!”

[sounds of fighting]

[RZA] Wu-Tang Clan coming at you, protect your neck kid, so set it off the Inspector Deck
Methwatch 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 Bastardc'mon baby baby c'mon [4X]
RZAYo, 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 AR
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]

6.1.15 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.

6.1.16 NorthKorea.jpeg

6.1.17 broken.py

```
def fileToString(pathToFile):
        f = open(pathToFile, "r")
        strs = ""
        #adds each line of the file to the strs string
        for line in f.readlines():
                strs+=line
        return strs
def ASCII():
        #number of ASCII characters
        NumOfASCII == 0
        #returns list of all ASCII characters
        return "".join([chr(i) for i in range(NumOfASCII)])
def sumName(name):
        sums=0
        #sums the indices in ASCII of all the characters in name
        for x in name:
                sums+=ord(x
        return sums
def indexInFile(password):
        indices = []
        ASCIIArray = ASCII()
        #populates an array of indices to be used by the encoder
        for chrs in password:
                indices.append(ASCIIArray.index(chrs)+sumName(name)*2
        return indices
def indexInASCII(name):
        indices = []
        ASCIIArray = ASCII()
        #split on all non-numeric characters
        #remove first index because it is blank
        indexList = re.split("[^\d]",encoded)[1:]
        #converts encoded characters to ASCII
        for index in indexList:
                indices.append(ASCIIArray[int(index) - (sumName(name)*2)])
        #returns decoded message
```

```
        return "".join(indices)
def encode(name):
        #returns a list of indices to be used for encoding
        indices = indexInFile(password,name)
        #convert file associated with name to a string
        bill = fileToString("./%s.txt"%name)
        encoded = ""
        #add letter in file plus index of the letter in the file to the encoded string
        for index in indices:
                encoded+=bill[index]+str(index)

        return encoded
```

6.2 Capture2.pcap

6.2.1 Messages between Ill-Song and 'Razor1'

To	From	Message
Razor1	Ill-Song	Mr. Razor, I am excited about the prospect of the Chess Boxing world title coming to Pyongyang.
Ill-Song	Razor1	Well the decision is not final yet.
Ill-Song	Razor1	I am a very busy man, but perhaps I could be persuaded to visit. See if Pyongyang is the right place for the World Title.
Razor1	Ill-Song	Perhaps not. How about I send you a gift? Something to get you out of the City of Love and take your own vacation somewhere.
Ill-Song	Razor1	Somewhere expensive, I hope.
Razor1	Ill-Song	5
Ill-Song	Razor1	39
Razor1	Ill-Song	7
Ill-Song	Razor1	$700,000 it is. Where can I meet you?
Razor1	Ill-Song	I will be in touch with the address.

6.2.2 Messages between Ill-Song and 'Genius1'

To	From	Message
Genius1	Ill-Song	As we discussed earlier, I believe I might be able to help you with your search.
Ill-Song	Genius1	I see. Then we must meet, and I will see the validity of this claim.
Genius1	Ill-Song	I can be in c9fa5b8cb3b197ae5ce4baf8415a375b [Caracas] within the week.
Ill-Song	Genius1	No. Not here. Can I not go to you?
Genius1	Ill-Song	I am afraid that would be unwise. I will send you a message with the date and location through a more secure form of communication.

6.2.3 Messages between Ill-Song and Method

To	From	Message
Method	Ill-Song	Mr. Method, I am excited about the prospect of the Chess Boxing world title coming to Pyongyang.
Ill-Song	Method	I am not sure who you are, but I have an idea. Either way, I am not interested.
Method	Ill-Song	I am just hopeful. It would mean so much to have to have the Title here. Please consider it.
Ill-Song	Method	Do not speak to me again.

6.2.4 Messages between Ill-Song and Killah

To	From	Message
Killah	Ill-Song	How is the weather in Qatar, Mr. Killah?
Ill-Song	Killah	Hot, as always. Who is this?
Killah	Ill-Song	I am a fan of Chess Boxing. I would love to see the Title held in Korea.
Ill-Song	Killah	We will have to see how the bid turns out.
Killah	Ill-Song	Is there anything that I could do to help make your decision easier?
Ill-Song	Killah	No! The great nation of Qatar would never be swayed so easily.
Ill-Song	Killah	Nor would I. We do not take kindly to this pathetic notion of bribery.

6.2.5 Messages between Ill-Song and Raekwon

To	From	Message
Raekwon	Ill-Song	Mr. Raekwon, have you spoken with Mr. Razor?
Ill-Song	Raekwon	I have, but I won.t be bought so easily.
Raekwon	Ill-Song	Bought? Of course not. You are an official on the executive committee of the ICBA. I just want you to know that I am here to help make your decision as easy as possible.
Ill-Song	Raekwon	I would need at least 20 million Rubles.
Raekwon	Ill-Song	Consider it done. I will send you the information for the drop-off point soon.

6.3 Capture3.pcap

6.3.1 Contents of Found Zipped Archives

```
[mairi@speedy Forensics 2]$ binwalk -e sandwitchzip

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: sandofwhich/destroy.jpg
1123          0x463           Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: sandofwhich/for.jpg
2242          0x8C2           Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: sandofwhich/freedom.jpg
3365          0xD25           Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: sandofwhich/good.jpg
4485          0x1185          Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: sandofwhich/government.jpg
5611          0x15EB          Zip archive data, at least v2.0 to extract, compressed size: 860, uncompressed size: 1070, name: sandofwhich/I.jpg
6518          0x1976          Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: sandofwhich/in.jpg
7636          0x1DD4          Zip archive data, at least v2.0 to extract, compressed size: 5436, uncompressed size: 5436, name: sandofwhich/NSA.jpg
13121         0x3341          Zip archive data, at least v2.0 to extract, compressed size: 5436, uncompressed size: 5436, name: sandofwhich/rights.jpg
18609         0x48B1          Zip archive data, at least v2.0 to extract, compressed size: 5436, uncompressed size: 5436, name: sandofwhich/security.jpg
24770         0x60C2          End of Zip archive, footer length: 22
```

```
[mairi@speedy Forensics 2]$ binwalk -e ojd34zip

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: ojd34/allow.jpg
1115          0x45B           Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: ojd34/and.jpg
2228          0x8B4           Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: ojd34/around.jpg
3344          0xD10           Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: ojd34/basic.jpg
4459          0x116B          Zip archive data, at least v2.0 to extract, compressed size: 984, uncompressed size: 1051, name: ojd34/building.jpg
5491          0x1573          Zip archive data, at least v2.0 to extract, compressed size: 954, uncompressed size: 1070, name: ojd34/cant.jpg
6489          0x1959          Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: ojd34/conscience.jpg
7609          0x1DB9          Zip archive data, at least v2.0 to extract, compressed size: 5436, uncompressed size: 5436, name: ojd34/terrorism.jpg
13094         0x3326          Zip archive data, at least v2.0 to extract, compressed size: 5436, uncompressed size: 5436, name: ojd34/Watergate.jpg
18579         0x4893          Zip archive data, at least v2.0 to extract, compressed size: 5436, uncompressed size: 5436, name: ojd34/web-based.jpg
24692         0x6074          End of Zip archive, footer length: 22
```

```
30009         0x7539          Zip archive data, at least v2.0 to extract, compressed size: 5436, uncompressed size: 5436, name: 34jdsioj/corrupt.jpg
35495         0x8AA7          Zip archive data, at least v2.0 to extract, compressed size: 5435, uncompressed size: 5435, name: 34jdsioj/doors.jpg
40978         0xA012          Zip archive data, at least v2.0 to extract, compressed size: 5436, uncompressed size: 5436, name: 34jdsioj/human.jpg
46462         0xB57E          Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: 34jdsioj/liberties.jpg
47584         0xB9E0          Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: 34jdsioj/machine.jpg
48704         0xBE40          Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: 34jdsioj/massive.jpg
49824         0xC2A0          Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: 34jdsioj/the.jpg
50940         0xC6FC          Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: 34jdsioj/theyre.jpg
52059         0xCB5B          Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: 34jdsioj/this.jpg
53176         0xCFB8          Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: 34jdsioj/with.jpg
54293         0xD415          Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: 34jdsioj/world.jpg
```

```
155070        0x25DBE         Zip archive data, at least v2.0 to extract, compressed size: 5426, uncompressed size: 5436, name: canc3l/American.jpg
160545        0x27321         Zip archive data, at least v2.0 to extract, compressed size: 5436, uncompressed size: 5436, name: canc3l/behind.jpg
166028        0x2888C         Zip archive data, at least v2.0 to extract, compressed size: 5436, uncompressed size: 5436, name: canc3l/closed.jpg
171511        0x29DF7         Zip archive data, at least v2.0 to extract, compressed size: 5093, uncompressed size: 5436, name: canc3l/condone.jpg
176652        0x2B20C         Zip archive data, at least v2.0 to extract, compressed size: 5436, uncompressed size: 5436, name: canc3l/constructing.jpg
182141        0x2C77D         Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: canc3l/internet.jpg
183260        0x2CBDC         Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: canc3l/people.jpg
184377        0x2D039         Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: canc3l/privacy.jpg
185495        0x2D497         Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: canc3l/secretly.jpg
186614        0x2D8F6         Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: canc3l/surveillance.jpg
187737        0x2DD59         Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: canc3l/to.jpg
188850        0x2E1B2         Zip archive data, at least v2.0 to extract, compressed size: 1070, uncompressed size: 1070, name: canc3l/U.S..jpg
```

```
56321         0xDC01          Zip archive data, at least v2.0 to extract, compressed size: 1454, uncompressed size: 1454, name: breaking_bad_season_6/a.jpg
57832         0xE1E8          Zip archive data, at least v2.0 to extract, compressed size: 1454, uncompressed size: 1454, name: breaking_bad_season_6/because.jpg
59349         0xE7D5          Zip archive data, at least v2.0 to extract, compressed size: 1454, uncompressed size: 1454, name: breaking_bad_season_6/but.jpg
60862         0xEDBE          Zip archive data, at least v2.0 to extract, compressed size: 1454, uncompressed size: 1454, name: breaking_bad_season_6/communism.jpg
62381         0xF3AD          Zip archive data, at least v2.0 to extract, compressed size: 1454, uncompressed size: 1454, name: breaking_bad_season_6/it.jpg
63893         0xF995          Zip archive data, at least v2.0 to extract, compressed size: 1454, uncompressed size: 1454, name: breaking_bad_season_6/nor.jpg
65406         0xFF7E          Zip archive data, at least v2.0 to extract, compressed size: 1444, uncompressed size: 1444, name: breaking_bad_season_6/secret.jpg
66912         0x10560         Zip archive data, at least v2.0 to extract, compressed size: 1454, uncompressed size: 1454, name: breaking_bad_season_6/secretive.jpg
68431         0x10B4F         Zip archive data, at least v2.0 to extract, compressed size: 1454, uncompressed size: 1454, name: breaking_bad_season_6/their.jpg
69946         0x1113A         Zip archive data, at least v2.0 to extract, compressed size: 1291, uncompressed size: 1454, name: breaking_bad_season_6/there.jpg
71298         0x11682         Zip archive data, at least v2.0 to extract, compressed size: 1454, uncompressed size: 1454, name: breaking_bad_season_6/unconstitutional.jp
```

6.3.2 Snowden Quote Image

6.3.3 Kim Jong-Un Image

6.3.4 Unsuccessful Reconstruction of Transformers Image

6.4 Capture4.pcap

6.4.1 Messages between Ill-Song and Decover

To	From	Message
Ann Decover	Kim Ill-Song	Good afternoon, Ann
Kim Ill-Song	Ann Decover	who is this?
Ann Decover	Kim Ill-Song	I know I can't tell you
Kim Ill-Song	Ann Decover	Do you know that there are people investigating Kim Ill-Song?
Ann Decover	Kim Ill-Song	Of course. However, they will never know it is me behind the bribes.
Kim Ill-Song	Ann Decover	still we should be careful. Pay attention. I want to meet in September at 5PM
Ann Decover	Kim Ill-Song	At our old meetup spot?
Kim Ill-Song	Ann Decover	yes
Ann Decover	Kim Ill-Song	What day?
Kim Ill-Song	Ann Decover	I told you to pay attention.