



**Abertay
University**

Network Forensics Report

Finlay Reid

CMP416: Digital Forensics 2

BSc Ethical Hacking Year 4

2020/21

Abstract

THIS TECHNICAL REPORT DISPLAYS THE FINDINGS OF A FORENSICS INVESTIGATION INTO A MOCK CRIMINAL CASE THAT INVOLVES AN INTERNATIONAL SPORTING COMPETITION CORRUPTION CASE. EACH PCAP FILE WAS INVESTIGATED, AND EVIDENCE FROM THIS WAS RECOVERED, FACILITATING FURTHER ANALYSIS. IN THE FIRST PCAP FILE, A HOST OF FILES WERE RECOVERED THROUGH WIRESHARK'S SMB EXPORT TOOL AND THESE FILES CONTAINED DATA RELATED TO THE CASE. IN THE NEXT PACKET CAPTURE, IRC TRAFFIC WAS RECOVERED, THIS DATA WAS EVIDENCE OF THE USER KIM ILL SONG ATTEMPTING TO BRIBE GOVERNMENT OFFICIALS IN ORDER TO HOST THE WORLD CHESS BOXING CHAMPIONSHIP IN NORTH KOREA SPECIFICALLY THE CAPITAL PYONGYANG. PACKET CAPTURE THREE INVOLVED THE SUSPECT DOWNLOADING FILES OVER THE FTP PROTOCOL, THESE FILES WERE SUCCESSFULLY DISCOVERED AND PRESENTED IN THIS REPORT WHILE CIRCUMVENTING THE ANTI-FORENSIC MEASURES UTILIZED BY THE SUSPECT. PARTICULARLY SPLITTING THE FILES INTO MULTIPLE SMALL PIECES SO AS TO OBFUSCATE THE EVIDENCE. IN THE FINAL PCAP FILE, IT WAS DISCOVERED THE SUSPECT KIM ILL SONG WAS ATTEMPTING TO SET UP A MEETING WITH ANN DECOVER ON THE 17TH OF SEPTEMBER AT 5 PM SOMEWHERE IN MISSOULA MONTANA THROUGH THE ANALYSATION OF HTTP REQUESTS.

Contents

1.1	Background/Tools Used	3
2	Methodology & Procedure	1
2.1	Capture1.PCAP	1
2.2	Capture2.PCAP	5
2.3	Capture3.PCAP	8
2.4	Capture4.pcap.....	11
3	Critical Evaluation	13
	References	14
	Appendices.....	15
3.1	Capture 1 Documents.zip.....	15
3.1.1	Actual Documents.....	15
3.1.2	Chess Boxing	17
3.1.3	Enter the WuTang	23
3.1.4	More Documents	29
3.2	Capture 2 Decoded Communication.....	43
3.3	Capture 3 Recovered Images and Commands	51
3.4	Capture 4 Location Data	53

1.1 BACKGROUND/TOOLS USED

The following technical report presents detailed findings of a mock criminal investigation in which four PCAP files were investigated and analyzed. The scenario involved working with a national security agency on an international sporting competition corruption case from which the PCAP files were recovered. Furthermore, the files were retrieved in a method ensuring the data was not altered in any way ensuring if this was a real-life case the evidence would be admissible in court. All the tools used in the investigation can be seen below in the tools table.

Tools used:

Tool	Tool description	References
Cyberchef	Web tool used for decoding	(CyberChef, 2022)
Cat	Linux command that reads files sequentially, writing them to standard output.	(Granlund and Stallman, 2022)
Binwalk	Analysation, reverse engineering, and firmware extracting utility.	(binwalk manual, 2022)
Google maps	Googles web mapping tool	(About - Google Maps, 2022)
Wireshark	Open source network traffic analyser	(Combs, 2022)
Tshark	Command-line network analyser	(tshark(1), 2022)
Earthpoint Cvs to kml	A tool used to convert CVS files to KML	(Earthpoint, 2022)
Grep	Command searches for lines that contain strings that match a pattern	(grep(1) - Linux manual page, n.d.)

2 METHODOLOGY & PROCEDURE

2.1 CAPTURE1.PCAP

From previous knowledge pertaining to the current case involving suspected bribery in an international competition. It was suggested that files which contained sensitive information were downloaded. Based on the fact that files were downloaded, protocols involving file transfers specifically FTP and SMB were investigated. SMB is a popular protocol used when sharing files over a network and is more commonly used when the file needs to be shared with multiple users. Some of the packets examined contained directories in the info column of Wireshark suggesting these SMB packets required further investigation. As shown below in **Figure 1** there are many SMB packets sent between the 172.29.1.23 and 172.29.1.20 addresses, starting at packet number 5857 where the server declares it is up and running by sending a host announcement frame. Packet number 26195 is the last packet of the SMB session, which is a tree disconnect response, a packet used to confirm the disconnection of the SMB protocol.

25941	21:22:42.749595	172.29.1.23	172.29.1.20	SMB	170 NT Create AndX Request, FID: 0x4003, Path: \DOCUME~
23919	21:22:17.947513	172.29.1.23	172.29.1.20	SMB	186 NT Create AndX Request, FID: 0x4004, Path: \My Musi
23927	21:22:18.030945	172.29.1.23	172.29.1.20	SMB	192 NT Create AndX Request, FID: 0x4005, Path: \My Pict
23935	21:22:18.072913	172.29.1.23	172.29.1.20	SMB	188 NT Create AndX Request, FID: 0x4006, Path: \My Vide

Figure 1 - SMB packets sent

Examining the contents of the SMB packets allowed for more information to be gained about what data was shared and with whom. In packet number 23844 it is clearly shown which user initialized the transfer of files as displayed below in **Figure 2**. Data such as the directories and files present on the host's system were visible also.

23842	641.878089	172.29.1.20	172.29.1.23	SMB	319 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
23844	642.004966	172.29.1.23	172.29.1.20	SMB	504 Session Setup AndX Request, NTLMSSP_AUTH, User: fox-ws\test
23845	642.006724	172.29.1.20	172.29.1.23	SMB	175 Session Setup AndX Response

Figure 2 - Set up request and User

In order to investigate the files downloaded by the suspect the data was first recovered, this was achieved through the use of Wireshark's ability to export smb data to a directory of your choosing. Accessed through the export objects menu this functionality within Wireshark facilitated the full recovery of all the data copied to the suspect's machine. **Figure 3** demonstrates the steps taken to access the Wireshark SMB export tool.

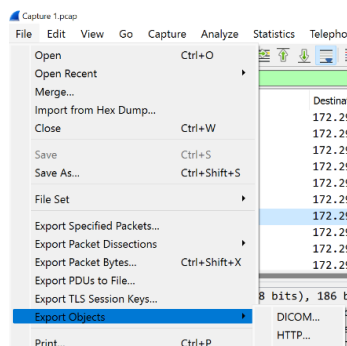
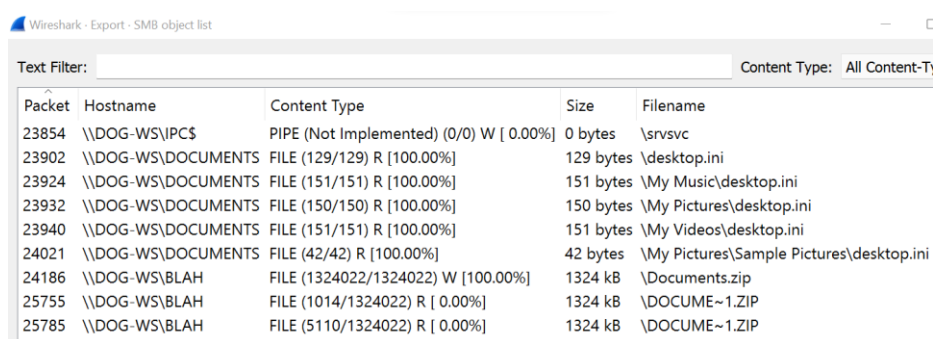


Figure 3 - Path to export tool

Overall nine files were recovered from Wireshark's export tool, while the majority were irrelevant system config files such as .ini and svc. There was a zip folder that contained five interesting folders, inside the directory's there was a host of files including the file types .docx, .jpg and .txt, the full contents of the recovered files can be seen in the *CAPTURE 1 DOCUMENTS.ZIP* appendix section. Within each of the word documents in the zip file, the contents were encoded in base64, using Cyberchef these were decoded and investigated to determine if any of the files contained potential names/aliases of actors in this corruption case. **Figure 4** shows the files in Wireshark's inbuilt SMB export tool, including the packet number of when the file was accessed and **Figure 5** presents the files after the recovery process has happened.



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%]	1324 kB	\Documents.zip
25755	\\DOG-WS\BLAH	FILE (1014/1324022) R [0.00%]	1324 kB	\DOCUME~1.ZIP
25785	\\DOG-WS\BLAH	FILE (5110/1324022) R [0.00%]	1324 kB	\DOCUME~1.ZIP

Figure 4 - SMB Files viewed in Wireshark

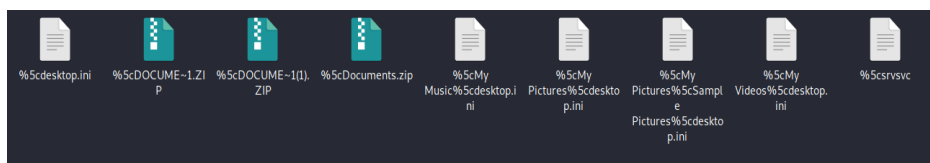


Figure 5 - Exported SMB data viewed in Kali

To ensure no files contained hidden content within them, the tool binwalk was utilized to inspect all the relevant files for embedded files and executable code. Binwalk is a tool commonly used to reverse engineer and used to extract the content of firmware images. Running this utility on the NorthKorea.jpg file located in /Documents/MoreDocuments/ revealed a zip file containing a python script named broken.py, this can be viewed in the *CAPTURE 1 DOCUMENTS.ZIP* appendix section. **Figure 6** demonstrates the binwalk command utilized to achieve this.

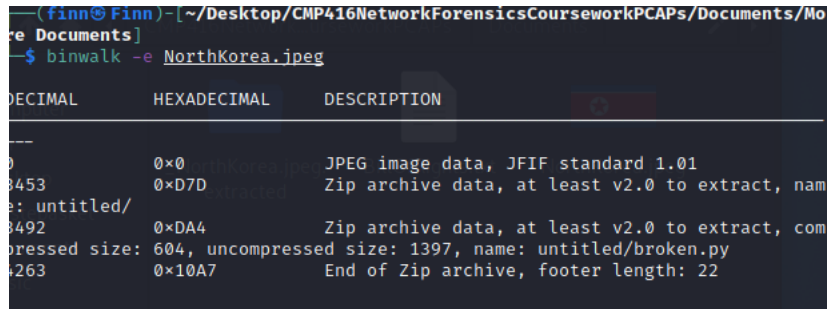


Figure 6 - Binwalk command used on kali

The HTTP data found in the packet capture was also recovered and analysed. Again, using Wireshark's inbuilt HTTP export tool all the pertinent HTTP information was downloaded to the kali machine. The contents of these files included .swf, .png, .bmp, etc. The majority of files were irrelevant however a picture of the suspects browsing habits was painted. **Figure 7** displays the HTTP data being explored through Wireshark and **Figure 8** presents the HTTP files that were downloaded onto the kali machine.

Packet #	Host Name	Content Type	Size	File Name
28	at.atwola.com	text/html	1122 bytes	suite.aspx?kvugc=0;kvui=dd00:
35	mail.aol.com	text/html	91 bytes	BeaconComposeMessageInLine
60	at.atwola.com	application/x-javascript	573 bytes	suite.aspx?kvugc=0;kvui=dd00:
65	o.saaol.com	image/gif	43 bytes	s28361207867109?AQB=1&nd
73	at.atwola.com	application/x-javascript	877 bytes	adlink%2F5113%2F2282005%2
85	imp.bid.ace.advertising.com	application/x-javascript	317 bytes	dref=http%253A%252F%252Fr
285	x.bidswitch.net	image/gif	43 bytes	sync?dsp_id=23&expires=7&s
307	s2.symcb.com	application/ocsp-response	1895 bytes	MFewTzBNMEswSTAJBgUrDgM
311	s2.symcb.com	application/ocsp-response	1895 bytes	MFewTzBNMEswSTAJBgUrDgM
327	ss.symcd.com	application/ocsp-response	1657 bytes	MFewTzBNMEswSTAJBgUrDgM
331	ss.symcd.com	application/ocsp-response	1657 bytes	MFewTzBNMEswSTAJBgUrDgM
755	download.cdn.mozilla.net	application/octet-stream	300 kB	firefox-30.0.complete.mar
802	www.google.com	text/html	231 bytes	\
918	clients1.google.com	application/ocsp-response	463 bytes	MEkwRzBFMEMwQTAJBgUrDg
920	clients1.google.com	application/ocsp-response	463 bytes	MEkwRzBFMEMwQTAJBgUrDg
922	clients1.google.com	application/ocsp-response	463 bytes	MEkwRzBFMEMwQTAJBgUrDg
923	clients1.google.com	application/ocsp-response	463 bytes	MEkwRzBFMEMwQTAJBgUrDg
1092	engine.ap.bittorrent.com	application/json	414 bytes	v2
1093	bench.utorrent.com		398 bytes	e?i=20
1097	engine.ap.bittorrent.com	application/json	413 bytes	v2

Figure 7 - HTTP data viewed in Wireshark

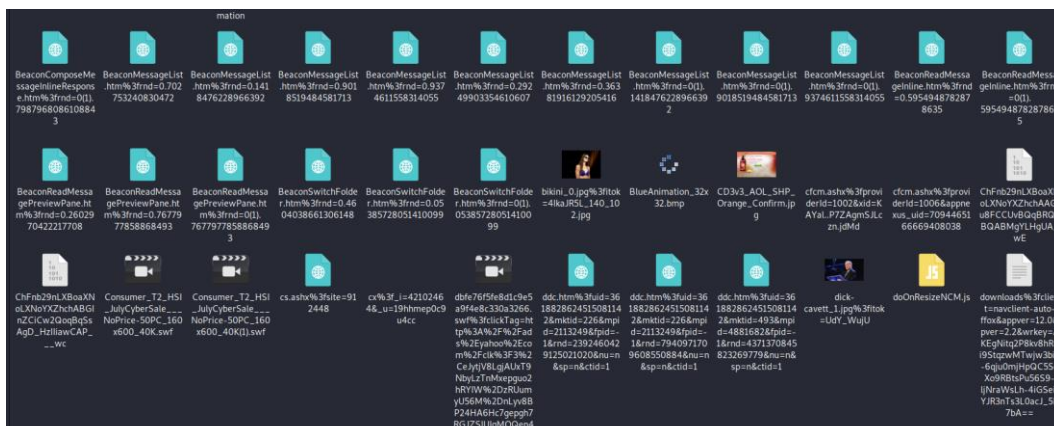


Figure 8 - HTTP data exported and shown in kali

A hidden email conversation was discovered in capture one but it contained no relevant data to the case so the content and procedure were not included in this report. The sent AOL email traffic was between one wikiofleaks@aol.com and snowedinedward@aol.com in which a zip file was recovered containing an additional packet capture. After thoroughly investigating the contents of the PCAP file it was determined to be inconsequential to the case.

2.2 CAPTURE2.PCAP

From previous knowledge relating to the discovery of encrypted traffic between suspected corrupt government officials, it was discovered there was communication over IRC with a foreign national named Ill-Song. IRC being a protocol used for group commination, the packets were analyzed in the packet sniffer application known as Wireshark. A filter was utilized to display the IRC packets only, revealing a large number of packets using the IRC protocol. These contained numerous strings that were consistently repeated, prompting for a closer investigation into the contents of the packets.

Within the host of IRC data, several packets included the 'PRIVMSG' tag in the info column of the packet analyser. Further research indicated this is a command used in IRC to send messages to users and channels. Examining the packets disclosed more information pertaining to the obfuscation methods used, **Figure 9** displays the data that was encoded in either base 64 or base 32 from the NO. 5616 Packet in pcap2. All packets using 'PRIVMSG' included a similar-looking string.

```
..:I1l_S ong!~I1l
_Song@21 6.14.247
.46 PRIV MSG Geni
us1 :SkV RR0MzSkF
NR1RIRV1 MSk1RUUh
JMKRCT1F RSE8zM1Z
OU1NDQV1 URkVCM1c
0NTNKT05 TUzRjQ0p
FQjNXUzN ETUVCWld
LM1RFRUI 0VzY1SkF
NRVFM1p MVE9OUVd
PWkpBTzV VWEkyQkF
PU1VHS01 ERU1GMkd
LSURCT1p TQ0EzRFB
NT1FYSTJ MUE5ZUUh
JMKRTTjU yV08yQkF
NRVFMjM zU01VUUh
HWkxET1Z aR0tJREd
ONVpHMK1 EUE1ZUud
HMzNOT1Y yVzQyTER
NRjJHUzM zT0ZZPT0
9PT09..
```

*Figure 9 - data
obfuscated in packet
no. 5616*

In order to enable further investigation into the packets, first the appropriate data needed to be collocated into a file. Facilitating for all the captured strings to be decoded and analyzed. **Figure 10** presents the command used to achieve this. The CLI network traffic analyser Tshark and the pattern searching command grep were used in conjunction to print the decodable data into a text file.

```
(finn@finn)-[~/Desktop/CMP416NetworkForensicsCourseworkPCAPs]
$ tshark -r 'Capture 2.pcap' -q -z follow,tcp,ascii,0 | grep -i privmsg | > priv.txt
```

Figure 10 - Tshark command used to print all privmsg data into file

- -r – flag used to specify tshark to read from the file.
- -q – the flag that hides packet information
- -z – the flag used to display specific statistics i.e display TCP data in ASCII from index 0
- -i(grep) – the flag used to ignore case distinctions

Having gathered the data neatly into a text file, a clear flow of data was visible, a conversation between government officials and Ill-Song. To Decode the relevant conversations a tool named Cyberchef was utilized to strip any encoding from the packet data, the majority of the messages were first encoded in with Base 64 and Base 32. This obfuscation was commonly backed up with another instance of Base encoding or operations such as Octal or Hex. Overall, 5 conversations took place between ill song and government officials, these include:

The following names are most likely aliases used by the government officials as each is taken from the popular hip hop group Wu-Tang Clan.

RAZOR

Il-songs communication with the user Razor1 lasted over 11 packets discussing the Chess Boxing world title. In one of the messages, a \$700,000 bribe is put to the user Razor and the figure is accepted. Furthermore, the location of the government official Razor is disclosed as the “city of love” when the pair are discussing Pyongyang’s suitability to host the Chess Boxing world title. Researching this phrase it is possible to deduct that the government official resides in Paris, France as its customary to refer to it as the city of love due to its rich romantic history (Why we call Paris the city of love and romance... but is it really?, 2021).

GENIUS

The discussion involving Genuis1 and Ill Song continued for 5 messages, data contained within the decoded conversation reveals the location of the government official as currently Caracas, the capital city of Venezuela. The suspect Ill-song queries the official about the possibility of travelling to Caracas but Genuis1 refuses this request and ill-song states that a time and place will be discussed over a more secure form of communication. No bribe is discussed within the available messages. Location of the government official was found through first the discovery of an md5 hash within the recovered messages and the hash was decrypted by simply researching the string on a web browser, which was discovered to be Caracas.

METHOD

The discussion between the suspect and Method is short with Ill-song opening the conversation expressing his delight in the prospect of hosting the Chess Boxing world title in Pyongyang. However,

Method does not entertain the suspect and completely refuses to continue the conversation stating “I am not interested”. As such the location of the government official remains unknown and from the evidence recovered the official does not accept any bribe.

KILLAH

Initial messages involving Killah and the suspect disclose the official’s location as the country Qatar. Due to Ill-Song opening the conversation by asking how the weather is currently in Qatar, the suspect continues attempting to bribe the official in order to influence the decision to hold the Chess Boxing world title in Pyongyang. However, the Qatari official vehemently refuses the attempted bribe and is disgusted affirming “Nor would I. We do not take kindly to this pathetic notion of bribery”.

RAEKWON

The final set of messages was between Ill-song and an official using the alias Raekwon, initially the official intends to refuse any bribes or to increase the price as it is stated “ I have, but I won’t be bought so easily”. This is in reference to the bribe and Raekwon’s communication with the first official Razor1, presumably, they discussed his receipt of a payoff from ill-song. Further on in the conversation, the official suggests that the price of his bribe is 20 million rubles and ill-song accepts this stating “Consider it done. I will send you the information for the drop-off point soon”. As only two countries use the Rubel currency including Russia and Belarus, and the spelling of currency is the Russian version, it can be deduced that the official is most likely from Russia but this is not for certain (ruble | currency, 2021).

Official Alias	Bribe Accepted	Location	Colour on Map
Razor	Yes	Paris, France	Red
Genius	Unknown	Caracas, Venezuela	Blue
Method	No	Unknown	-
Killah	No	Qatar	Green
Raekwon	Yes	Russia	Black

Table 1 - Location Table

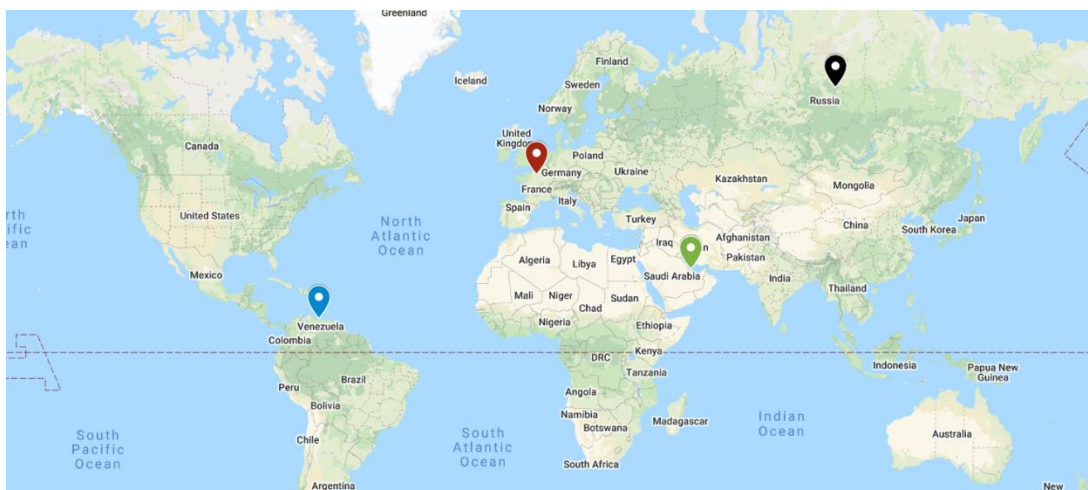


Figure 11 - Map of officials location

2.3 CAPTURE3.PCAP

This criminal investigation had precursory information related to the communication between a suspected corrupt official and a foreign national, this intelligence suggested that files had been exchanged between the individuals and this was achieved through the file transfer protocol. Utilizing Wireshark's ability to filter for specific network protocols packet number 5885 was discovered, by isolating FTP packets, a frame containing one sandofwhich.zip can be seen in **Figure 12**. Suggesting at least one zip file had been transferred from the suspected corrupt official and a foreign national.

5885	181.959170	172.29.1.23	172.29.1.21	FTP	76 Request: RETR sandofwhich.zip
------	------------	-------------	-------------	-----	----------------------------------

Figure 12 - Sandofwhich.zip FTP discovered

As the file transfer protocol is associated with two ports, port 20(FTP-data) in which the actual data is moved over the channel to its specified destination, and port 21 which handles the control data that is sent. Wireshark's in-built filter utility was used at this time isolate the FTP-data packets and from this, another zip file was discovered titled ojd34.zip.

In order to reconstruct the data, the TCP streams of each file were followed through Wireshark. This enabled the full conversation to be saved in the raw format to the local machine which can be seen below in **Figure 13**. Having stored the FTP conversation that transferred the files in the proper method, the next step involved using the proper recovery procedure, and to achieve this the binary analysis utility binwalk was employed.

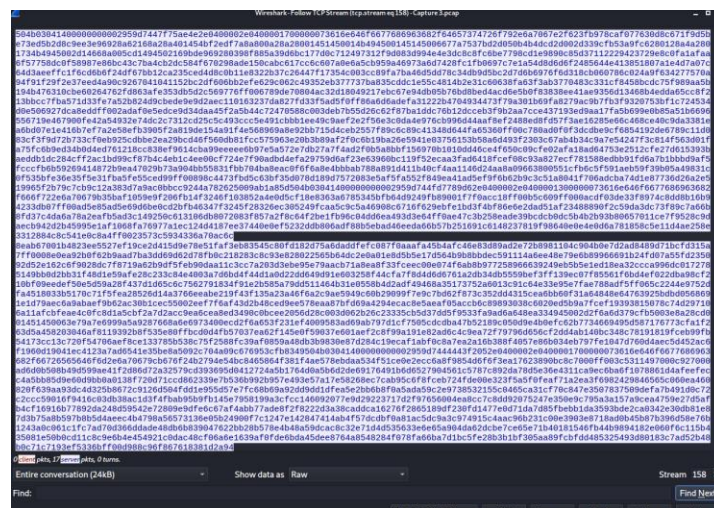


Figure 13 - FTP exchange stored as raw

Figure 14 displays the command used to successfully extract the files from the raw export of the FTP conversation. As seen below from the zip file contained many .jpg files and from the investigation, only one of these files had the .jpg magic number and could be successfully opened. Based on this information it was concluded the suspect had employed anti-forensic measures to conceal the files and hamper forensic investigations. As such the files were separated purposely into smaller sections and these required full reconstruction to view the file as it was meant to be.

```
(finn@finn)~[~/Desktop/New Folder]
$ binwalk -e pcap3zipsand.raw
```

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

Figure 14 - Binwalk command used to extract the file

Again binwalk is used to extract the files and this time for the ojd.zip, like the previous zip this contained further jpg files. **Figure 15** displays the command used and the files extracted.

```
File Actions Edit View Help
(fin@finn)~[~/Desktop/New Folder]
$ binwalk -e pcap3zipojd34.raw
```

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

Figure 15 - Binwalk command on ojd34

The extracted files were then moved to a new folder, due to previous information provided to the investigator it was known that an Edward Snowden quote could help decipher the obsucfacted data. So popular quotes were compared with the words available and from this, it was discovered that the following quote contained many of the keywords.

"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"

However, many of the words were not contained within the extracted zip files and it was concluded that further zip files were transferred between the suspect and ill song. These files would need to be discovered and extracted to complete the jpg file. Upon further analysis of HTTP traffic within the packet capture, it was discovered that there were several POST requests which involved AOL and from this information, it was concluded that further files could have been transferred over email. The TCP stream 42 was saved in the raw format once again and this was followed through one of the POST requests, specifically packet number 6939. Once again using the utility bin walk three more zip files were successfully recovered including 34jdsioj.zip, breaking_bad_season_6.zip and canc3l.zip. These archives contained further jpeg files and were titled as thought, helping in the completion of the quote. Furthermore, two more jpg files could be viewed suggesting these needed reconstruction as well as the first that involved the Edward Snowden quote.

Through the use of the Linux command cat, the first image was successfully reconstructed, by simply following the order of the quote and saving it as image1.jpg an image of a chessboard was deciphered. The next two files required a lot of trial and error to reconstruct the images however a full recovery of the images was completed, following the process of using cat, files were consistently substituted in and out to achieve the valid image. The full commands and images can be seen in *Appendix 2.7 CAPTURE 3 RECOVERED IMAGES AND COMMANDS*.

2.4 CAPTURE4.PCAP

It was known Ill-Song and a person of interest taking part in the international competition was attempting to set up a meeting. Discovered through the recovery of communication between ill song and Ann Dercover. Through analyzing the HTTP traffic in the packet capture the details of the device were discovered, packet no 619 was a post request in which the information related to the device was disclosed. From this, it was discovered the suspects were conversing with one another through the application Textfree, which facilitates users to text and call over the internet for free. Furthermore, the application was being run on a nexus 7 device using android 4.2.2.

```
x-client: textfree-android,2.3.2\r\n
x-os: android,4.2.2\r\n
x-uid: 580781709\r\n
x-gid: 0\r\n
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.2.2; Nexus 7 Build/JDQ39E)\r\n
Host: ads.pinger.com\r\n
```

Figure 16 - Device details

By sorting the info tab, a block of packets became visible which looked suspicious, these were all post requests and contained language data in the info section. Upon further analysis, these select packets contained the correspondence between ill song and Ann Dercover.

3256	17:39:53.385186	192.168.1.5	199.87.160.87	HTTP/J...	869	POST	/1.0/messages/text/send?lang=en-US	HTTP/1.1 ...
4152	17:40:24.848500	192.168.1.5	199.87.160.87	HTTP/J...	871	POST	/1.0/messages/text/send?lang=en-US	HTTP/1.1 ...
4791	17:42:03.678791	192.168.1.5	199.87.160.87	HTTP/J...	922	POST	/1.0/messages/text/send?lang=en-US	HTTP/1.1 ...
5473	17:43:33.123734	192.168.1.5	199.87.160.87	HTTP/J...	937	POST	/1.0/messages/text/send?lang=en-US	HTTP/1.1 ...
5808	17:44:06.959622	192.168.1.5	199.87.160.87	HTTP/J...	860	POST	/1.0/messages/text/send?lang=en-US	HTTP/1.1 ...
22476	17:51:10.504188	192.168.1.5	199.87.160.87	HTTP/J...	889	POST	/1.0/messages/text/send?lang=en-US	HTTP/1.1 ...

Figure 17- HTTP block of POST packets

To have a clearer picture of the conversation the tshark command shown below in **Figure 18** was used. This enabled for the full conversation to be piped to a text file allowing for further analysis of the conversation. Inspecting the details of the conversation Kim ill song first initiates the contact with a good afternoon to Ann Dercover. After exchanging greetings, Ann Dercover then says to Kim "Do you know that there are people investigating Kim Ill-Song?" and from this Kim responds to the question stating "Of course. However, they will never know it is me behind the bribes.". Suggesting that Kim has taken preventive measures to remain anonymous, this could be through the use of an alias or another method. Further on in the conversation details concerning the date and time that they are planning to meet are disclosed. This is stated as September at 5 PM which Kim ill song suggests the usual meeting spot. At the end of the conversation, Kim ill song queries ann to determine what day the meeting will take place to which Ann responds by saying "I told you to pay attention". Overall, the conversation lasts roughly five minutes and it took place on the 2nd of July 2014.

```
(finn@Finn)~[~/Desktop]
$ tshark -r 'Capture 4.pcap' -Y 'http' -T 'json' | grep messageText > message.txt
```

Figure 18 - Tshark command used to gather messages

In order to gather all the coordinates the command shown below was used to pipe all location data located in the URLs into a text file. From inspecting the network packets which contained the

coordinates all seemed to include the host mobquest and this was used in conjunction with t shark to grab the coordinates which were in the longitude and latitude format.

```
(finn@Finn)~[~/Desktop]
$ tshark -r 'Capture 4.pcap' -Y "http.host = mob.mapquestapi.com" > location.txt
```

Figure 19 - Tshark command used to gather location data

Having created the text file with the coordinates the location data was then imported into a CSV file and properly formatted. Using Earthpoints CSV to kml utility the file was successfully converted and doing this ensured a map of the coordinates could be constructed through google maps. As shown below in **Figure 20** the pins on the map are laid out in the number 17 suggesting Kim ill song and Ann Dercover could be meeting on the 17th of September at 5 pm. The exact location of the meeting was not discovered however it was somewhere in Missoula, Montana.

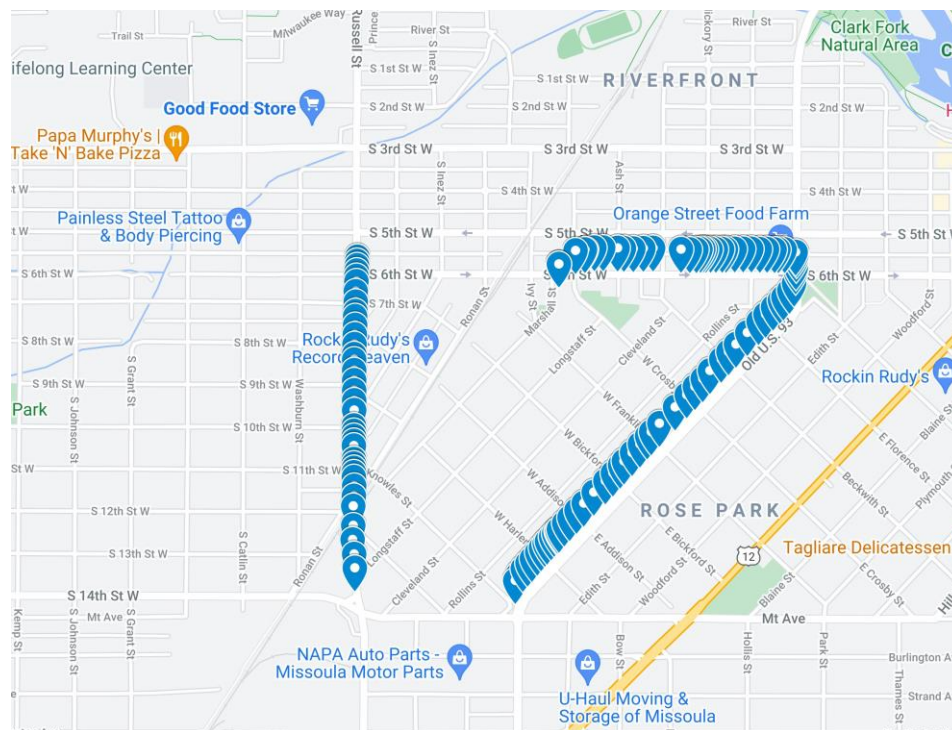


Figure 20 - Map layout of recovered coordinates

3 CRITICAL EVALUATION

Through this mock investigation rules ensuring the sound retrieval of evidence were adhered to mirroring a real-life forensic investigation. The creation and subsequent verification of the files using sha1 hashes confirmed data was not altered during the examination phase of the project. Evidence which was recovered from the PCAP files was securely backed up to the cloud guaranteeing no critical data was lost. During the investigation of the four packet capture files numerous challenges presented themselves which needed to be solved, due to the variety of the scenarios different methods/techniques were utilized to ensure the necessary evidence was obtained. For example tshark commands were regularly employed to pipe large amounts of data into a text file. This was used to save time as manually trawling through the Wireshark interface looking for the specific data could be time consuming. Concerning the tools available throughout the investigation, these were enough for the scenarios given, of course professional tools could have helped speed up the process of evidence recovery. In future network forensic investigations, it could be better to utilize a proper network forensic methodology, to allow for a more systematic examination of the evidence available. Furthermore, if this was a real-world scenario in which a sporting corruption investigation case was taking place. It would be better to carry out the investigation in a more secure environment to ensure data is not leaked or the investigators remain safe when undertaking their job. At the start of the investigation, each PCAP was given a brief look over to determine which would be the easiest and hardest. Based on the current level of knowledge at that time regarding the different network protocols, Wireshark tools etc. This enabled for a plan to be constructed regarding the best method to tackle each individual scenario. Overall, the network forensic investigation lasted over one month from the start of December to January the 11th. During this time evidence related to each scenario was successfully collated and presented in this report, with verbose documentation detailing the different tools and methods that enabled the necessary evidence to be uncovered.

REFERENCES

- Combs, G., 2022. *Wireshark · Go Deep..* [online] Wireshark.org. Available at: <<https://www.wireshark.org/>> [Accessed 10 January 2022].
- Earth Point. 2022. [online] Available at: <<https://www.earthpoint.us/exceltokml.aspx>> [Accessed 5 January 2022].
- Encyclopedia Britannica. 2021. *ruble / currency*. [online] Available at: <<https://www.britannica.com/topic/ruble>> [Accessed 9 December 2021].
- Gchq.github.io. 2022. *CyberChef*. [online] Available at: <<https://gchq.github.io/CyberChef/>> [Accessed 5 January 2022].
- Google.co.uk. 2022. *About - Google Maps*. [online] Available at: <<https://www.google.co.uk/maps/about/mymaps/>> [Accessed 5 January 2022].
- Granlund, T. and Stallman, R., 2022. *cat(1) - Linux manual page*. [online] Man7.org. Available at: <<https://man7.org/linux/man-pages/man1/cat.1.html>> [Accessed 10 January 2022].
- kali.org. 2022. *binwalk manual*. [online] Available at: <<https://www.kali.org/tools/binwalk/>> [Accessed 5 January 2022].
- Man7.org. n.d. *grep(1) - Linux manual page*. [online] Available at: <<https://man7.org/linux/man-pages/man1/grep.1.html>> [Accessed 11 January 2022].
- Md5online.org. 2022. *MD5 Online / Free MD5 Decryption, MD5 Hash Decoder*. [online] Available at: <<https://www.md5online.org/md5-decrypt.html>> [Accessed 5 January 2022].
- Radware.com. n.d. *ShieldSquare Captcha*. [online] Available at: <<https://www.radware.com/security/ddos-knowledge-center/ddospedia/irc-internet-relay-chat/>> [Accessed 5 January 2022].
- SearchNetworking. 2022. *What is the Server Message Block (SMB) protocol? How does it work?*. [online] Available at: <<https://www.techtarget.com/searchnetworking/definition/Server-Message-Block-Protocol>> [Accessed 5 January 2022].
- thelocal. 2021. *Why we call Paris the city of love and romance... but is it really?*. [online] Available at: <<https://www.thelocal.fr/20180214/paris-city-of-love-romance-really/>> [Accessed 9 December 2021].
- Wireshark.org. 2022. *tshark(1)*. [online] Available at: <<https://www.wireshark.org/docs/man-pages/tshark.html>> [Accessed 5 January 2022].

APPENDICES

3.1 CAPTURE 1 DOCUMENTS.ZIP

3.1.1 Actual Documents

GOT Spoilers.docx

Sm9uIFNub3cgYnVybnMgZG93biBXaW50ZXJmZWxslChhZ2FpbikgYW5kiHRoZSBXYWxsLg0KDQpIb2RvciB
raWxscyBUaGVvbi4NCg0KRGFibmVyeXMgZ2V0cyBIYXRlbiBieSBhIGRyYWdvbi4NCg0KU3RhbW5pcyBmY
WxscyBpbiBsb3ZlIHdpdGggVHlyaW9uLiANCg0KDQo=

Decoded = Base64

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

Hodor kills Theon.

Daenerys gets eaten by a dragon.

Stannis falls in love with Tyrion.

Northkorea.docx

0JTQu9GPINC60L7Qs9C+INGN0YLQviDQvNC+0LbQtdGCINC60LDRgdCw0YLRjNGB0Y86IA0KDQrQryDQsd
GL0Lsg0YHQstC40LTQtdGC0LXQu9C10LwslNGH0YLQviDQmtC40Lwg0KfQtdC9INCj0L0g0Lgg0L/RgNCw0L
LQuNGC0LXQu9GM0YHRgtCy0L4g0KHQtdCy0LXRgNC90L7QuSDQmtC+0YDQtdC4INGA0LDQtd9GA0LDQsd
C+0YLQsNC70Lgg0L/RgNC+0LPRgNCw0LzQvNGDLCDQutC+0YLQvtGA0LDRjyDQv9C+0LfQstC+0LvRj9C10Y
lg0LjQvCDQv9GD0YLQtdGI0LXRgdGC0LLQvtCy0LDRgtGMINCy0L4g0LLRgNC10LzQtdC90LguINChINC40YH
Qv9C+0LvRjNC30L7QstCw0L3QuNC10Lwg0Y3RgtC+0Lkg0YLQtdGF0L3QvtC70L7Qs9C40LgslNGPINGB0Yf
QuNGC0LDRjiwg0YfRgtC+INC+0L3QuCDQvdCw0LzQtdGA0LXQvdGLINC00LLQuNCz0LDRgtGM0YHRjyDQs
tC/0LXRgNC10LQg0Lgg0LjQt9C80LXQvdC40YLRjCDRgNC10LfRg9C70YzRgtCw0YLRiyDQstC+0LnQvdGLINC
yINC0L7RgNC10LUuIA0KDQrQn9C+0LbQsNC70YPQudGB0YLQsCwg0J7QsdC4LdCS0LDQvSwg0YLRiyDQv
NC+0Y8g0LXQtNC40L3RgdGC0LLQtdC90L3QsNGPINC90LDQtdNC10LbQtNCwLg0KDQo=

Decoded = Base64 > translation from Russian

For whom it may concern:

I have witnessed Kim Jong Un and the North Korean government develop a program that allows them to travel back in time. With 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.

PiD.docx

RGVhciBFZCwNCg0KWWVhaCBJIHRvdGFsbHkgdG9vayBvdmVylGZvciBQYXVsIGFmdGVyIGhlIGRpZWQgaW4g4oCZNjYulFlvdSBnb3QgbWUulEFzIHlvdSBjYW4gc2VILCB3ZSBkb27igJlOIGV2ZW4gbG9vayB0aGF0IG11Y2ggYWxpa2U6DQo=



Before(Paul)

After(Me)

IAkgCQ0KQmVmb3JlKFBhdWwplAKJCQkJQWZ0ZXIoTWUpdQoNCldlIGFyZW7igJlOIGV2ZW4gdGhlIHhnbWUgaGVpZ2h0ISBXaGF0IGNhbiBJIHNeSwgcGVvcGxIGFyZSBzdHVwaWQuDQoNCg0KVGHhbmztIGZvciB0aGUgaW5xdWlyeSwNCg0KV2IsbGlhbSBDYW1wYmVsbA0KKFBhdWwgTWNDYXJ0bmV5KQ0K

Decoded = Base 64

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:

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

Thanks for the inquiry,

William Campbell

(Paul McCartney)

3.1.2 Chess Boxing

NK.jpg



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.

Rules2.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.

Rules3.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).

Rules4.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.

Rules5.docx

5. WCBA CHESS RULES FOR CHESSBOXING

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

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

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

Touch move

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

Castling touch move

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

Hand is taken off a piece

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

Illegal move

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

“J’Adoube” rule.

Normal Chess Rules

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

Chessboxing Rules (adapted because both players have headphones)

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

Pawn promotion

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

Clock

- The clock MUST be pressed with the same hand that makes the move
- Running out of time. If a player has no time remaining, then he is lost if his opponent can checkmate him assuming the most unskilled play, otherwise the game is a draw. For example, if Player A has three queens and a king, and Player B has one pawn and a king, then Player B wins if Player A runs out of time.

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

Draw by threefold repetition

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

take off his headphones and claim the draw. The arbiter will stop the clock as the headphones come off. If the draw claim is correct and the claimant runs out of time after removing his headphones, the draw will hold.

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

50 move rule

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

Draw Offer

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

Verbal Communication with the arbiter

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

Arbiter's decision

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

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.

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.

3.1.3 Enter the WuTang

Track6.docx

VGHIIE15c3Rlcnkgb2YgQ2hlc3MgQm94aW5nOg0KKHVzZXJuYW1lcykNCg0KTXlulE1dGhvZA0KDQpLaW0gSWxsLVNvbmcNCg0KTXlulFJhem9yDQoNCK1yLiBHZW5pdXMNCG0KTXlulEculEtpbGxhaA0KDQpNYXR0IE Nhc3NIbA0KDQpNci4gSS4gRGVjaw0KDQpNci4gTSBLaWxsYQ0KDQpNci4gTy5ELkluDQoNCK1yLiBSYWVrd 29uDQoNCK1yLiBVLUdvZA0KDQpNci4gQ2FwcGFkb25uYSAocG9zc2libHkpDQoNCKpvaG4gV29vPw0KDQp Nci4gTmFzDQo=

Decoded = Base 64

The Mystery of Chess Boxing:

(usernames)

Mr. Method

Kim III-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

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

[Meth] watch your step kid [8X]

[Inspector Deck]

I smoke on the mic like smoking Joe Frazier

The hell raiser, raising hell with the flavor

Terrorize the jam like troops in Pakistan

Swinging through your town like your neighborhood Spiderman

So uhh, tic toc and keep ticking

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

The Lone Ranger, code red, danger!

Deep in the dark with the art to rip charts apart

The vandal, too hot to handle

you battle, you're saying Goodbye like Tevin Campbell

Roughneck, Inspector Deck's on the set

The rebel, I make more noise than heavy metal

[Raekwon]

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

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

Rhymes rugged and built like Schwarzenegger
And I'm gonna get mad deep like a threat, blow up your project
Then take all your assets
Cause I came to shake the frame in half
With the thoughts that bomb, shit like math!
So if you wanna try to flip go flip on the next man
Cause I grab the clip and
Hit you with sixteen shots and more I got
Going to war with the melting pot hot

[Method]

It's the Method Man for short Mr. Meth
Moving on your left, ah!
And set it off, get it off, let it off like a gat
I wanna break full, cock me back
Small change, they putting shame in the game
I take aim and blow that nigga out the frame
And like Fame, my style'll live forever
Niggaz crossing over, but they don't know no better
But I do, true, can I get a "sue"
Nuff respect due to the one-six-oh
I mean oh, you check out the flow
like the Hudson or PCP when I'm dusting
Niggaz off because I'm hot like sauce
The smoke from the lyrical blunt makes me [cough]

[U-God]

Oh, what, grab my nut get screwed
Ow, here comes my Shaolin style

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

to my crew with the "sue"

[Interlude]

watch your step kid [8X]

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

[RZA] Yo, you best protect your neck

[Ol Dirty Bastard]

First things first man you're fucking with the worst

I'll be sticking pins in your head like a fucking nurse

I'll attack any nigga who's slack in his mack

Come fully packed with a fat rugged stack

Shame on you when you stepped through to

The Ol Dirty Bastard straight from the Brooklyn Zoo

And I'll be damned if I let any man

Come to my center, you enter the winter

Straight up and down that shit packed jam

You can't slam, don't let me get fool on him man

The Ol Dirty Bastard is dirty and stinking

Ason, unique rolling with the night of the creeps

Niggaz be rolling with a stash

ain't saying cash, bite my style I'll bite your motherfucking ass!

[Ghostface Killah]

For crying out loud my style is wild so book me

Not long is how long that this rhyme took me

Ejecting, styles from my lethal weapon

My pen that rocks from here to Oregon

Here's Mordigan, catch it like a psycho flashback
I love gats, if rap was a gun, you wouldn't bust back
I come with shit that's all types of shapes and sounds
And where I lounge is my stomping grounds
I give a order to my peeps across the water
To go and snatch up props all around the border
And get far like a shooting star
'cause who I am is dim in the light of Pablo Escobar
Point blank as I kick the square biz
There it is you're fucking with pros and there it goes

[RZA]

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

[Genius]

The Wu is too slamming for these Cold Killing labels
Some ain't had hits since I seen Aunt Mabel

Be doing artists in like Cain did Abel
Now they money's gettin stuck to the gum under the table
That's what you get when you misuse what I invent
Your empire falls and you lose every cent
For trying to blow up a scrub
Now that thought was just as bright as a 20-watt light bulb
Should've pumped it when I rocked it
Niggaz so stingy they got short arms and deep pockets
This goes on in some companies
With majors they're scared to death to pump these
First of all, who's your A&R
A mountain climber who plays an electric guitar
But he don't know the meaning of dope
When he's looking for a suit and tie rap
that's cleaner than a bar of soap
And I'm the dirtiest thing in sight
Matter of fact bring out the girls and let's have a mud fight

[sounds of fighting]

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

3.1.4 More Documents

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.

NorthKorea.jpg



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

```

3.2 CAPTURE 2 DECODED COMMUNICATION

1) PRIVMSG Razor1

```

:SZaQzRJQ1NNRjVHNjRSTUVCrvNBWUxORUJTWFFZM0pPUINXSUIEQk1KWFhLNUJBT1JVR0tJRFFPSIhYR
zRERk1OMkNBMzNHRUIyR1FaSkFJTIVHSzQzVEVCQkc2NkRKTIpUU0E1M1BPSIdHSUIEVU5GMkdZWkpBT
U5YVzlyTE9NNFFISTNaQUtCNFc2M1RIUEZRVzRaWk8=

```

Decoded = Base 64 > Base32

Mr. Razor, I am excited about the prospect of the Chess Boxing world title coming to Pyongyang.

```
2) Razor1!~malware@216.14.247.46 PRIVMSG Ill_Song : .....
NTc2NTZjNmMyMDc0Njg2NTIwNjQ2NTYzNjk3MzY5NmY2ZTIwNjk3MzlwNmU2Zjc0MjA2NjY5NmU2MTZj
MjA3OTY1NzQyZQ==
```

Decoded = Base64 > Hex

Well the decision is not final yet.

3) PRIVMSG Razor1
:SIOIvZyZVEhQRIFXNFpaQU5GWINBWVRGTUYyWEkyTEdPVldDQTVESU5GWINBNURKTIZTU0EzM0dFQJR
XS1IMU0ZZUUBWkxTTkJRWEEOwKfQRlYhS0IEWE41MldZWkJBtIJVV1daSkFPUIhTQTVUSk9OVVhJSURC
TlpTQ0FaTFIPQINyRTJMRk5aUldLSURYTkJRWEIJQ0NNVlpYSUIDTE41WkdLWUpBTkJRWEdJRFVONFFHNlp
UR01WWkM0PT09

Decoded = Base 64 > Base32

Pyongyang is beautiful this time of year. Perhaps you would like to visit and experience what Best Korea has to offer.

```
4) Razor1!~malware@216.14.247.46 PRIVMSG Ill_Song : .....
NDkyMDYxNmQyMDYxMjA3NjY1NzI3OTIwNjI3NTczNzkyMDZkNjE2ZTJjMjA2Mjc1NzQyMDcwNjU3MjY4
NjE3MDczMjA0OTIwNjM2Zjc1NmM2NDIwNjI2NTIwNzA2NTcyNzM3NTYxNjQ2NTY0MjA3NDZmMjA3NjY
5NzM2OTc0MmUyMDUzNjU2NTIwNjI2NjIwNTA3OTZmNmU2Nzc5NjE2ZTY3MjA2OTczMjA3NDY4NjUyM
DcyNjk2NzY4NzQyMDcwNmM2MTYzNjUyMDY2NmY3MjIwNzQ2ODY1MjA1NzZmNzI2YzY0MjA1NDY5Nz
Q2YzY1MmU=
```

Decoded = Base64 > Hex

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.

5) PRIVMSG Razor1
:S0JTWEUyREJPQlpTQTNUUE9RWENBU0RQTzRRR0NZVFBPVjJDQV NKQU9OU1c0WkJBUEZYWEtJREJFQIR
XU1pUVUg0UUZHMzNOTVYyR1EyTE9NFFISTNaQU01U1hJSURaTjUyU0EzM1ZPUVFHNIpSQU9SVUdLSU
NETKyYSFNJRFBNWVFFWTmZV01VUUDDM1RFRUyR0MyM0ZFQjRXNjVMU0VCWFhPM1JBT1pRV0dZTFV
ORlhXNEIEVE41V1dLNTNJTVZaR0tMUT0=

Decoded = Base 64 > Base32

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.

6) :Razor1!~malware@216.14.247.46 PRIVMSG III_Song : NTM2ZjZkNjU3NzY4NjU3MjY1MjA2NTc4NzA2NTZlNzM2OTc2NjUyYzlwNDkyMDY4NmY3MDY1MmUyMA ==
Decoded = Base 64 > hex
Somewhere expensive, I hope.

7) PRIVMSG Razor1 :R1U9PT09PT0=
Decoded = Base 64 > Base 32
5

8) :Razor1!~malware@216.14.247.46 PRIVMSG III_Song :Mzk=
Decoded = Base 64
9

9) PRIVMSG Razor1 :RzQ9PT09PT0=
Decoded = Base 64 > hex
7

10) :Razor1!~malware@216.14.247.46 PRIVMSG III_Song : MjQzNzMwMzAyYzMwMzAzMDIwNjk3NDIwNjk3MzJlMjA1NzY4NjU3MjY1MjA2MzYxNmUyMDQ5MjA2Z DY1NjU3NDIwNzk2Zjc1M2Y=
Decoded = Base 64 > hex
\$700,000 it is. Where can I meet you?

11)PRIVMSG Razor1 :SkVRSE8yTE1OUVFHRVpKQU5GWENBNURQT1ZSV1FJRfHORjJHUUIEVU5CU1NBWUxFTVJaR0s0M1RGW T09PT09PQ==
Decoded = Base 64 > Base 32

I will be in touch with the address.

12) PRIVMSG Genius1

:SUZaU0E1M0ZFQINHUzQzRE9WWlhHWkxFRUJTV0M0VE1ORINYRUxCQUpFUUdFWkxNTkZTWE1aSkFKR VFHMjJMSE5CMkNBWVRGRUJRv0UzREZfQjJHNkIESU1WV0hBSURaTjUyU0E1M0pPUIVDQTZMUE9WWk NBNDNGTUZaR0cyQk8=

Decoded = Base64 > Base 32

As we discussed earlier, I believe I might be able to help you with your search.
--

13) :Genius1!~malware@216.14.247.46 PRIVMSG III_Song :
--

MTExiDA0MCAxNjMgMTQ1IDE0NSAwNTYgMDQwIDEyNCAxNTAgMTQ1IDE1NiAwNDAgMTY3IDE0NSAw NDAgMTU1IDE2NSAxNjMgMTY0IDA0MCAxNTUgMTQ1IDE0NSAxNjQgMDU0IDA0MCAxNDEgMTU2IDE0 NCAwNDAgMTExIDA0MCAxNjcMTUxIDE1NCAxNTQgMDQwIDE2MyAxNDUgMTQ1IDA0MCAxNjQgMTU wIDE0NSAwNDAgMTY2IDE0MSAxNTQgMTUxIDE0NCAxNTEgMTY0IDE3MSAwNDAgMTU3IDE0NiAwNDA gMTY0IDE1MCAxNTEgMTYzIDA0MCAxNDMgMTU0IDE0MSAxNTEgMTU1IDA1Ng==

Decoded = Base 64 > Octal

I see. Then we must meet, and I will see the validity of this claim.
--

14) PRIVMSG Genius1

:SkVRR0dZTE9FQIJHS0IESk5ZUUDHT0xHTUUYv0VPRERNSVpXRu1KWkc1UVdLTkxETVUyR0VZTEdiQTJEQ0 5MQkdNM1RLWVJBtZVVWEkyREpOWVFISTJERkVCM1dLWkxMRlk9PT09PT0=

Decoded = Base 64 > Base 32

I can be in c9fa5b8cb3b197ae5ce4baf8415a375b within the week.

c9fa5b8cb3b197ae5ce4baf8415a375b

Decoded = md5 hash decrypt

Caracas

15) :Genius1!~malware@216.14.247.46 PRIVMSG III_Song :
--

MTE2IDE1NyAwNTYgMDQwIDExNiAxNTcgMTY0IDA0MCAxNTAgMTQ1IDE2MiAxNDUgMDU2IDA0MCAx MDMgMTQxIDE1NiAwNDAgMTExIDA0MCAxNTYgMTU3IDE2NCAwNDAgMTQ3IDE1NyAwNDAgMTY0IDE 1NyAwNDAgMTcxIDE1NyAxNjUgMDc3
--

Decoded = Base 64 > Octal

No. Not here. Can I not go to you?

16) Genius1

:SkVRR0MzSkFNRIrIRVIMSk1RUUhJMkRCT1FRSE8zM1ZOUINDQVIURkVCMIc0NTNKT05TUzRjQ0pFQjNX
UzNETUVCWldLM1RFRUI0VzY1SkFNrVFHMIpMVE9OUVdPWkpBTzVVWEkyQkFPUIVHS0IERU1GMkdLSU
RCTlpTQ0EzRFBNTIFYSTJMUE5ZUUhJMkRTTjUyV08yQkFNrVFHMIpMzU01VUUhHWkxET1ZaR0tJREdONV
pHMkIEUE1ZUUhHMzNOTIYyVzQyTERNRjJHUzMzT0ZZPT09PT09

Decoded = Base 64 > Base 32

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.

17) PRIVMSG Method

:SIzAqzRjQ05NVjJHUTMzRUZRUUVTSURCTIVRR0s2RERORjJHS1pCQU1GUkc2NUxVRUIyR1FaSkFPQlpHNj
QzUU1WUIhJSURQTVIRSEkyREZFQkXUVpMVE9NUUVFMzNZTKZYR09JRFhONVpHWVpCQU9SVVhJM0RG
RUJSVzYzTEpOWIRTQTVEUEVCSUhTMzNPTTU0V0MzVEhGWT09PT09PQ==

Decoded = Base 64 > Base 32

Mr. Method, I am excited about the prospect of the Chess Boxing world title coming to Pyongyang.

18) :Method!~malware@216.14.247.46 PRIVMSG III_Song :

NDkyMDYxNmQyMDZlNmY3NDIwNzM3NTcyNjUyMDc3Njg2ZjIwNzk2Zjc1MjA2MTcyNjUyYzIwNjI3NTc0
MjA0OTIwNjg2MTc2NjUyMDYxNmUyMDY5NjQ2NTYxMmUyMDQ1Njk3NDY4NjU3MjIwNzc2MTc5MmM
yMDQ5MjA2MTZkMjA2ZTZmNzQyMDY5NmU3NDY1NzI2NTczNzQ2NTY0MmU=

Decoded = Base 64 > Hex

I am not sure who you are, but I have an idea. Either way, I am not interested.

19) PRIVMSG

Method:U1NCaGJTQnFkWE4wSUdodmNHVm1kV3d1SUVsMEIIZHZkV3hrSUcxbFIXNGdjMjhnYlhWamFD
QjBieUJvVWVhabElIUibKRVFHQzNKQU5KMIhHNUJBTKJYWEFaTEdPVldDNEIDSk9RUUhPMzNWTIJTQ0EzTE
ZNRlhdQTQzUEVCV1hLWTNJRUIyRzZJREINRjNHs0IEVU5CU1NBVkrKT1JXR0tJREINVIpHS0xSQUtCV0dLW
UxUTVVRROczM09PTIVXSVpMU0VCVvhJTfE9

Decoded = Base > Hex

I am just hopeful. It would mean so much to have to have the Title here.
Please consider it

20) :Method!~malware@216.14.247.46 PRIVMSG III_Song : NDQ2ZjIwNmU2Zjc0MjA3MzcwNjU2MTZiMjA3NDZmMjA2ZDY1MjA2MTY3NjE2OTZlMmU=
Decoded = Base 64 > Hex
Do not speak to me again.

21) PRIVMSG Killah :SkJYWE9JREpPTVFISTJERkVCM1dLWUxVTkJTWEVJREpOWVFGQ1IMVU1GWkNZSUNOT0IYQ0FTM0pOUI dHQzJCNw==
Decoded = Base 64 > Base 32
How is the weather in Qatar, Mr. Killah?

22) :Killah!~malware@216.14.247.46 PRIVMSG III_Song : MTEwIDE1NyAxNjQgMDU0IDA0MCAxNDEgMTYzIDA0MCAxNDEgMTU0IDE2NyAxNDEgMTcxIDE2MyAwN TYgMDQwIDEyNyAxNTAgMTU3IDA0MCAxNTEgMTYzIDA0MCAxNjQgMTUwIDE1MSAxNjMgMDc3
Decoded = Base 64 > Octal
Hot, as always. Who is this?

23) PRIVMSG Killah :SkVRR0MzSkFNRFVHTVIMTOVCWFdNSUNETkJTWEc0WkFJSIhYUTJMT000WENBU0pBTzVYWEszREVfQld HNjVURkVCMkc2SURUTVZTU0E1REINVVFGSTJMVU5SU1NBMkrGTIJTQ0EyTE9FQkZXNjRURk1FWEE9PT0 9
Decoded = Base 64 > Base 32
I am a fan of Chess Boxing. I would love to see the Title held in Korea.
24) :Killah!~malware@216.14.247.46 PRIVMSG III_Song : MTI3IDE0NSAwNDAGMTY3IDE1MSAxNTQgMTU0IDA0MCAxNTAgMTQxIDE2NiAxNDUgMDQwIDE2NCAx NTcgMDQwIDE2MyAxNDUgMTQ1IDA0MCAxNTAgMTU3IDE2NyAwNDAGMTY0IDE1MCAxNDUgMDQwID E0MiAxNTEgMTQ0IDA0MCAxNjQgMTY1IDE2MiAxNTYgMTYzIDA0MCAxNTcgMTY1IDE2NCAwNTY=
Decoded = Base 64 > Octal
We will have to see how the bid turns out.

25) PRIVMSG Killah

:SkZaU0E1REINVlpHS0IEQk5aNFhJMkRKTlpUU0E1REINRjJDQVnKQU1OWFhLM0RFRUJTRzZJRFVONFFHU
VpMTU9BUUcyWUxMTVVRSFMzM1ZPSVFHSPMRE5GWldTMzNPRUJTV0M0M0pNVlpENj09PQ==

Decoded = Base 64 > Base 32

Is there anything that I could do to help make your decision easier?

26) :Killah!~malware@216.14.247.46 PRIVMSG III_Song :

MTE2IDE1NyAwNDEgMDQwIDEyNCAxNTAgMTQ1IDA0MCAxNDcgMTYyIDE0NSAxNDEgMTY0IDA0MCAx
NTYgMTQxIDE2NCAxNTEgMTU3IDE1NiAwNDAGMTU3IDE0NiAwNDAGMTIxIDE0MSAxNjQgMTQxIDE2Mi
AwNDAGMTY3IDE1NyAxNjUgMTU0IDE0NCAwNDAGMTU2IDE0NSAxNjYgMTQ1IDE2MiAwNDAGMTQyIDE
0NSAwNDAGMTYzIDE2NyAxNDEgMTcxIDE0NSAxNDQgMDQwIDE2MyAxNTcgMDQwIDE0NSAxNDEgMTY
zIDE1MSAxNTQgMTcxIDA1Ng==

Decoded = Base 64 > Octal

No! The great nation of Qatar would never be swayed so easily.

27) :Killah!~malware@216.14.247.46 PRIVMSG III_Song :

MTE2IDE1NyAxNjlgMDQwIDE2NyAxNTcgMTY1IDE1NCAxNDQgMDQwIDExMSAwNTYgMDQwIDEyNyAxN
DUgMDQwIDE0NCAxNTcgMDQwIDE1NiAxNTcgMTY0IDA0MCAxNjQgMTQxIDE1MyAxNDUgMDQwIDE1
MyAxNTEgMTU2IDE0NCAxNTQgMTcxIDA0MCAxNjQgMTU3IDA0MCAxNjQgMTUwIDE1MSAxNjMgMDQ
wIDE2MCAxNDEgMTY0IDE1MCAxNDUgMTY0IDE1MSAxNDMgMDQwIDE1NiAxNTcgMTY0IDE1MSAxNTcg
MTU2IDA0MCAxNTcgMTQ2IDA0MCAxNDlgMTYyIDE1MSAxNDlgMTQ1IDE2MiAxNzEgMDU2

Decoded = Base 64 > Octal

Nor would I. We do not take kindly to this pathetic notion of bribery.

28) PRIVMSG Raekwon

:SlZaQzRJQ1NNRINXVzUzUE5ZV0NBmkrCT1pTU0E2TFBPVVFIRzREUE5OU1c0SURYTkyYr1FJQ05PSVhDQ
VVUQIBKWFhFUFk9

Decoded = Base 64 > Base 32

Mr. Raekwon, have you spoken with Mr. Razor?

29) :Raekwon!~malware@216.14.247.46 PRIVMSG III_Song :

NDkyMDY4NjE3NjY1MmMyMDYyNzU3NDIwNDkyMdc3NmY2ZTkyNzQyMDYyNjUyMDYyNmY3NTY3Njg3
NDIwNzM2ZjIwNjU2MTczNjk2Yzc5MmU=

Decoded = Base 64 > Hex
I have, but I won.t be bought so easily.

30) PRIVMSG Raekwon :SUpYWEtaM0IPUTdTQVQzR0VCUIc2NUxTT05TU0EzVFBPUVhDQVdMUE9VUUdDNFRGRUJRvzRJRFBNWI RHU1kzSk1GV0NBMzNPRUIyR1FaSkFNVjRHS1kzVk9SVVhNWkpBTU5YVzIzTEpPUjJHS1pKQU41VENBNUR JTVVRRVNRmKjNRVhDQVnKQU5KMIhHNUJBTzVRVzQ1QkFQRiHYS0IEVU40UUdXM1RQTzRRSEkyREJPUV FFU0IEQk5VUUdRWkxTTVVRSEkzWkFOQINXWTRCQU5WUUVdXWkpBUEZYWEs0UkFNUINXRzJMVE5GWF c0SURCT01RR0tZTFRQRVFHQzRaQU9CWfhHNDNKTUpXR0tMUkE=
Decoded = Base 64 > Base 32
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.

31 :Raekwon!~malware@216.14.247.46 PRIVMSG Ill_Song : NDkyMDc3NmY3NTZjNjQyMDZINjU2NTY0MjA2MTc0MjA2YzY1NjE3Mzc0MjAzMjMwMjA2ZDY5NmM2Yz Y5NmY2ZTIwNTI3NTYyNmM2NTczMmU=
Decoded = Base 64 > Hex
I would need at least 20 million Rubles.

32) PRIVMSG Raekwon :SU5YVzQ0M0pNUiNYRUIESk9RUUdJMzNPTVVYQ0FTSkFPNVVXWTNCQU9OU1c0WkJBUEZYWEtJRFVOQI NTQTJMT01aWFhFM0xCT1JVVzYzUkFNWihYRUIEVU5CU1NBWkRTTjVZQzIzM0dNWVFIQTmzSk5aMkNB NDNQJTjVYQzQ9PT0=
Decdoed = Base 64 > Base 32
Consider it done. I will send you the information for the drop-off point soon.

3.3 CAPTURE 3 RECOVERED IMAGES AND COMMANDS

```
(finn@Finn)-[~/Desktop/New Folder/cat]
$ cat I.jpg cant.jpg in.jpg good.jpg conscience.jpg allow.jpg the.jpg U.S..jpg government.jpg to.jpg destroy.jpg pr
ivacy.jpg internet.jpg freedom.jpg and.jpg basic.jpg liberties.jpg for.jpg people.jpg around.jpg world.jpg with.jpg t
his.jpg massive.jpg surveillance.jpg machine.jpg theyre.jpg secretly.jpg building.jpg >> image1True.jpg
```

Figure 21 - Cat command used to construct image 1 – The chessboard



Figure 22 - Recovered Image of chessboard

```
(finn@Finn)-[~/Desktop/New Folder/cat]
$ cat condone.jpg American.jpg web-based.jpg rights.jpg constructing.jpg se
curity.jpg terrorism.jpg NSA.jpg Watergate.jpg corrupt.jpg human.jpg behind.j
pg closed.jpg doors.jpg >> image3True1.jpg
```

Figure 23 - Cat command used to create image 3 - Gundam



Figure 24 – Recovered image of gundam

```
(finn@Finn)-[~/Desktop/New Folder/_email.raw.extracted/breaking_bad_season_6]  
$ cat there.jpg their.jpg a.jpg it.jpg but.jpg communism.jpg nor.jpg because.jpg unconstitutional.jpg secretive.jpg secret.jpg >> image2True.jpg
```

Figure 25 - Cat command used for 2nd image – Kim Jong un



Figure 26 - Image 2 - Kim jong un

3.4 CAPTURE 4 LOCATION DATA

Latitude, Longitude

46.85661315917969,-114.01860809326172
46.85693359375,-114.01863098144531
46.85727310180664,-114.01868438720703
46.857601165771484,-114.01866912841797
46.858055114746094,-114.01866149902344
46.8582878112793,-114.01864624023438
46.858524322509766,-114.01863861083984
46.858734130859375,-114.01864624023438
46.85884475708008,-114.01864624023438
46.858943939208984,-114.01864624023438

46.859046936035156,-114.01864624023438
46.85914993286133,-114.01864624023438
46.859466552734375,-114.01864624023438
46.85957717895508,-114.01864624023438
46.85969161987305,-114.01864624023438
46.85980987548828,-114.01864624023438
46.85993194580078,-114.01864624023438
46.86029052734375,-114.01863098144531
46.86052322387695,-114.01863861083984
46.860755920410156,-114.01863098144531
46.86098861694336,-114.01863098144531
46.861228942871094,-114.01863861083984
46.86147689819336,-114.01863098144531
46.86159896850586,-114.01863098144531
46.86183547973633,-114.01862335205078
46.862064361572266,-114.01861572265625
46.862281799316406,-114.01860046386719
46.86248779296875,-114.01860046386719
46.86260223388672,-114.01859283447266
46.86282730102539,-114.0185775756836
46.86306381225586,-114.0185775756836
46.86330032348633,-114.01856231689453
46.863426208496094,-114.0185546875
46.86355209350586,-114.01854705810547
46.86367416381836,-114.01853942871094
46.8637809753418,-114.01853942871094
46.86387252807617,-114.0185317993164
46.863704681396484,-114.01164245605469
46.86370849609375,-114.01163482666016

46.864017486572266,-114.01107025146484
46.864044189453125,-114.01074981689453
46.86404800415039,-114.01071166992188
46.86408996582031,-114.01042175292969
46.86408996582031,-114.01012420654297
46.864078521728516,-114.00962829589844
46.864070892333984,-114.0094223022461
46.86406707763672,-114.00910186767578
46.86407470703125,-114.00875854492188
46.86408233642578,-114.0084228515625
46.864051818847656,-114.0074691772461
46.864044189453125,-114.00716400146484
46.864044189453125,-114.00694274902344
46.86404800415039,-114.00680541992188
46.86405563354492,-114.00670623779297
46.864051818847656,-114.00662231445313
46.864051818847656,-114.00646209716797
46.864051818847656,-114.00627899169922
46.864051818847656,-114.00605773925781
46.864051818847656,-114.00592803955078
46.86405944824219,-114.00563049316406
46.86405944824219,-114.00534057617188
46.86405563354492,-114.00506591796875
46.864051818847656,-114.00477600097656
46.864051818847656,-114.00452423095703
46.864044189453125,-114.0042724609375
46.864044189453125,-114.00414276123047
46.86404037475586,-114.00392150878906
46.863983154296875,-114.00354766845703

46.86393356323242,-114.0035171508789
46.86381912231445,-114.00352478027344
46.863643646240234,-114.0035400390625
46.86354446411133,-114.00354766845703
46.86325454711914,-114.00360107421875
46.86309051513672,-114.00376892089844
46.86293411254883,-114.00396728515625
46.86286163330078,-114.00408172607422
46.862701416015625,-114.00432586669922
46.86253356933594,-114.00457763671875
46.862361907958984,-114.00481414794922
46.86210632324219,-114.00520324707031
46.86183547973633,-114.0055923461914
46.86166000366211,-114.00584411621094
46.86148452758789,-114.00609588623047
46.86122131347656,-114.00647735595703
46.86103057861328,-114.00672912597656
46.860843658447266,-114.00699615478516
46.86065673828125,-114.00727081298828
46.86037063598633,-114.0076675415039
46.859989166259766,-114.00820922851563
46.85979080200195,-114.00848388671875
46.85969161987305,-114.00862121582031
46.859500885009766,-114.00887298583984
46.85930252075195,-114.00914001464844
46.85910415649414,-114.00941467285156
46.8590087890625,-114.0095443725586
46.858829498291016,-114.00979614257813
46.858646392822266,-114.01005554199219

46.858375549316406,-114.01044464111328
46.858123779296875,-114.01079559326172
46.85795211791992,-114.01103973388672
46.8577880859375,-114.01127624511719
46.85765838623047,-114.0114517211914
46.857513427734375,-114.01164245605469
46.85749053955078,-114.01168823242188
46.85747146606445,-114.01171112060547
46.857418060302734,-114.01179504394531
46.85733413696289,-114.01190948486328
46.857234954833984,-114.01204681396484
46.857181549072266,-114.01212310791016
46.85708236694336,-114.01225280761719
46.85697937011719,-114.01237487792969
46.856834411621094,-114.01256561279297
46.85672378540039,-114.01271057128906
46.856597900390625,-114.01287078857422
46.85647201538086,-114.01302337646484
46.856319427490234,-114.013130187988