Network Forensics Investigation into an International Drug Trafficking Case

Ance Strazdina

CMP416: Advanced Digital Forensics

2023/24

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

Contents

GLOSSARY

FTP – File Transfer Protocol. Enables file sharing across different computer systems by serving resources on servers for client access.

HTML – Hypertext Markup Language. Language used to structure documents designed to be displayed in a web setting.

HTTP – Hypertext Transfer Protocol. Used for transporting information between clients and web servers.

HTTP GET request – requests a representation of a specific resource, for example, web page contents, from a web server via HTTP.

HTTP POST request – requests a web servers to accept data sent via HTTP, for example, messages.

IP – Internet Protocol. Serves as an identifier between hosts on a network.

OSI – Open Systems Interconnection. A theoretical model that defines how devices communicate on a network.

PHP – scripting language used on the server-side for creating web pages.

TCP – Transmission Control Protocol. Communication standard for networked devices that allows for data transmission over a network.

TCP/IP - Transmission Control Protocol/Internet Protocol. A set of standardized rules that define how devices communicate on a network.

1 INTRODUCTION

1.1 INVESTIGATION BRIEF

A health regulatory agency working on an international drug trafficking case has commissioned an investigation of three network captures that have been exfiltrated from parties of interest. The following information has been requested for each capture and must be recovered in a forensically sound manner:

Capture 1

The agency has been alerted of a possible illegal substance smuggling in an international shipment. The target has uploaded files that, according to the informants, may contain a record of the drugs and quantities involved in this case which is vital to this investigation. Information relating to the names of the drugs, the amounts, how the files were encoded, and how they could be decoded has been requested. Details of any other files or data in the log are irrelevant to the investigation.

Capture 2

FTP and other traffic have been detected between a suspected gang member and a foreign contact. The agency has requested for this traffic to be decoded and for evidence of what item the foreign contact received to be provided. Some anti-forensic practices are suspected to have been used to hide the information, however, the agency has been tipped that an Obi-Wan Kenobi quote may help to decipher the message.

Capture 3

Communication traffic between El Chapo and a known person of interest involved in the trafficking, Narco Polo, has been discovered. It is believed that the suspects are trying to arrange a delivery secretly to avoid arrest. Details of the conversation and the date and time when the suspects are planning to meet have been requested.

1.2 AIMS OF THE INVESTIGATION

The aim of this investigation is to perform a thorough network forensic analysis of the provided traffic capture files and obtain the requested material:

1. Names and quantities of the substances involved in this case and information on the encoding schemes used to conceal this information.
2. Evidence of what item was received by the foreign contact.
3. Details, including the date and time of a planned meeting, of an intercepted conversation between suspects El Chapo and Narco Polo.

Achieving this involves the following sub-aims:

- Identifying a network forensics investigation methodology to follow.
- Completing the steps of the methodology and utilising the appropriate tools for each phase to obtain the required information.
- Documenting and analysing the results.

2 METHODOLOGY

2.1 OVERVIEW OF THE NETWORK FORENSICS PRACTICE

This investigation followed the OSCAR network forensics investigation methodology outlined by Jaswal (2019) which includes five main phases:

1. **Obtain.** This phase focuses on obtaining the information about the incident including the environment where it happened. Additional information that can be gathered during this stage includes the date and time of the incident and involved the people and systems involved.
2. **Strategize.** Strategizing involves planning the investigation based on several aspects including evidence acquisition, investigation environment, time allocated for the investigation, and required output.
3. **Collect.** The collection phase involves the acquisition of evidence. Furthermore, this stage defines the steps to ensure its forensic integrity: documenting all actions performed during the investigation, working on copies of the evidence rather than the originals, and generating cryptographic hashes for file verification.
4. **Analyse.** Analysis is performed to obtain the required investigative output. The tools and techniques used during this stage differ on a case-by-case basis, however, an outline of identifying the main events based on the case being investigated and then inspecting these further to obtain the required information is followed.
5. **Report.** The final stage of the methodology relates to producing a report that comprehensively documents the investigation. The report must contain factual details about the background of the investigation, undertaken work, findings, and their analysis in a way that can be reconstructed. Additionally, this must be documented in a way that a non-technical person can understand, so it is easier to utilize in settings such as court hearings.

This methodology is widely used within the industry with organisations such as The European Union Agency for Network and Information Security (ENISA) outlining it in their network forensics training toolset (ENISA, 2016). Its popularity is largely due to its logically structured and comprehensive approach to investigations which offers a systematic method for thoroughly analysing digital evidence. With clearly defined objectives related to the gathering of information related to the incident, planning the investigative work, collecting evidence, and thoroughly analysing it while also ensuring its forensic integrity, this methodology enables investigations to be accurate, forensically sound and well-documented, leading to more meaningful investigational outcomes (Jaswal, 2019).

Sections 2.1.1 - 2.1.5 document how each of the five phases of the OSCAR methodology was applied to this investigation.

2.1.1 Obtain

For this investigation, any information relating to the case was provided in the form of investigation briefs (see Section 1.1). No additional information could be established before the investigation began; however, the following could be recognised:

- The traffic captures were exfiltrated from the parties of interest in an undisclosed network/-s.

- The traffic captures contained various forms of traffic, including FTP, that the suspects used to distribute information.
- Encoding and other anti-forensic practices were present within the data.
- Two people of interest had been identified – El Chapo and Narco Polo.

2.1.2 Strategize

As the evidence for the investigation was provided, evidence acquisition was not factored into the planning process. During this phase, the tasks this investigation should accomplish, identified in Section 1.2, were taken into consideration when outlining the investigation approach. Lastly, as the evidence was provided in a traffic packet capture format, it could be estimated what strategies, including protocol analysis, file carving, and searching for relevant strings, and tools, including *Wireshark* and *tshark,* to use (Davidoff & Ham, 2012) when approaching this investigation.

2.1.3 Collect

The evidence for the investigations did not require collection, so only steps that apply to ensuring its forensic integrity were performed:

1. Extensively documenting all investigative steps (contained in Appendix A – Detailed Investigative Analysis).
2. Securely storing original copies of evidence and investigative output in read-only directories and creating secure external backups in the case of data loss.
3. Creating and working on copies of the original evidence and all investigative output produced.
4. Generating SHA-256 hashes of evidence and investigative output to verify file integrity as the investigation progressed (Appendix C – Cryptographic File Hashes).

2.1.4 Analyse

The evidence of this investigation was in a network traffic packet capture format, so the investigation was approached by applying knowledge of the principles of networking, including protocols, their features, and communication models (TCP/IP and OSI) to the scenario. The captures were first inspected to identify what protocols could have been used to perform actions highlighted in the investigation brief (see Section 1.1). Further analysis was then performed to get a full understanding of the captured events, which included the timestamps, IP addresses, and reconstruction of what transpired over the network. Specific details of this procedure are documented in Appendix A – Detailed Investigative Analysis and the main findings are discussed in Section 3.

2.1.5 Report

This stage was completed by producing the *Network Forensics Investigation into an International Drug Trafficking Case* report. It documents the conducted investigation in detail so it can be reproduced and contains definitions of technical terminology for non-technical audience.

2.2 INVESTIGATIVE TOOLS

CyberChef (v10.5.2) – a web application for encoding and decoding data between various formats that was used to decode files that were obtained from the traffic captures (GCHQ, 2023).

Google Earth (v10.42.0.1) – displays a 3D render of Earth and was used to obtain a geographical location based on provided coordinates (Google LLC, 2023)

Google Search – search engine used to find the right Obi-Wan Kenobi quote (Google LLC, 2023).

Google Translate – a translation tool used to translate text from one of the extracted documents (Google LLC, 2023).

Kali Linux – a Linux distribution tailored for penetration testing and digital forensics maintained by Offensive Security (2023) was used as the main work environment for this investigation. It natively offers numerous network forensics tools as well as many command-line utilities that aid this process, such as *sha256sum* and *chmod* which were used to generate file hashes and change their permissions to read-only to ensure the integrity of the evidence. Additionally, *cat, grep,* and *tree* were used during the investigation to find and/or display information. Lastly, *file* and *binwalk* utilities were used to investigate recovered files.

SilentEye (v0.4.1) – a steganography software that was used to extract hidden data from an image (achorein, 2023).

tshark (v4.0.6) – command line interface for Wireshark that was used to efficiently locate relevant parts of the network traffic and obtain the required information (Wireshark Foundation, 2023).

Wireshark (v4.0.6) – a packet capture and analysis tool that was used to display, filter, and analyse information from the obtained evidence (Wireshark Foundation, 2023).

3 INVESTIGATIVE FINDINGS

This section documents what information from the evidence was vital to establish the context of the incident. For a fully detailed documentation of the performed steps see Appendix A – Detailed Investigative Analysis.

3.1 CAPTURE 1

SHA256 hash: e782a7086cc2b349fb32cf9a2acdf6645c225339752cd981ee0cc063e9c848cb
Capture timeframe: 20.10.2023 19:18:01 UTC - 22.10.2023 05:23:52 UTC.

This capture was analysed by performing protocol analysis which was imperative to identifying communication between the suspects. When inspecting the protocol hierarchy of the capture in *Wireshark*, it could be recognised that Service Message Block version 2 (SMB2) was one of the most used protocols that ran over TCP. Understanding that this protocol is used to access shared resources in networks helped identify it as possibly having been used for accessing the files uploaded by the suspect which were reported to contain the information requested from this capture.

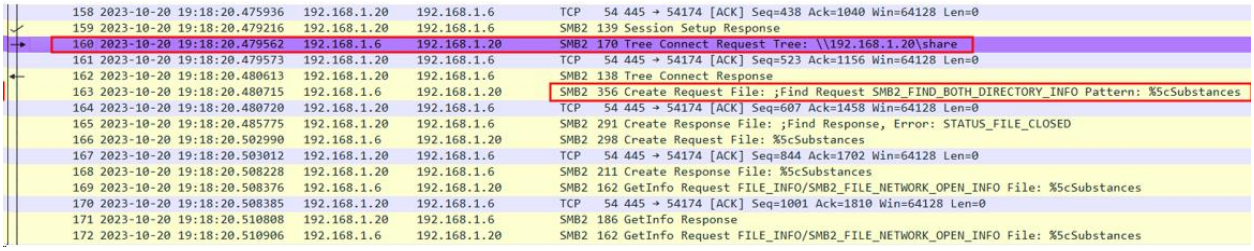


Figure 3-1 Connection to network the share on 192.168.1.20 and request for 'Substances' directory

It was identified that on October 20, 2023, 19:18:20 UTC a network share at 192.168.1.20 was accessed by a host at 192.168.1.6. A directory named *Substances* was requested (Figure 3-1) which merited further inspection. Numerous resources on *192.168.1.20**share* were accessed during this connection (19:18:20 – 19:18:36 UTC) and carving these with *Wireshark's Export Objects* functionality led to the acquisition of 28 files (see Appendix B – Recovered Files). Many of these used steganography and Base64 encoding to conceal their data. While a lot of the file contents were irrelevant to the investigation, a document titled track6.docx (Appendix B – Recovered Files, Word Documents, track6.docx), when decoded from Base64 with CyberChef, revealed the amounts and names of substances that were being trafficked (Figure 3-2):

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

Figure 3-2 Substance names and amounts

11 substances and their amounts were identified; however, no measurement units were specified. It should also be noted that all substances were various types of medication (Drugbank Online, 2023) and are legal in the country where this investigation was conducted (United Kingdom) at the time of writing (December 2023):

- Atorvastatin – lowers lipid levels and reduces the risk of cardiovascular disease.
- Levothyroxine – treats hypothyroidism.
- Metformin – used in type 2 diabetes treatments.
- Lisinopril – used to treat hypertension, heart failure, and acute myocardial infarction.
- Amlodipine – treats hypertension and angina.
- Metoprolol – treatment of hypertension and angina, among others.
- Albuterol – treatment of asthma, bronchitis, and others.
- Omeprazole – used to treat conditions such as heartburn and gastric acid hypersecretion, among others.
- Losartan – used to treat hypertension and diabetic nephropathy, and reduce the risk of stroke.
- Gabapentin – manages peripheral neuropathic pains and other conditions.
- Hydrochlorothiazide – treatment of edema and hypertension.

3.2 CAPTURE 2

SHA256 hash: 034042d655c57403ee44f59587d9b6c832b4cc89a660fe47fb4e69d3ae14e79f
Capture timeframe: 14.10.2023 05:33:35 UTC - 21.10.2023 20:08:03 UTC

A lead about the discovered use of FTP for communication via file transfers was used to investigate this capture file. The protocol was filtered out with *tshark* and knowledge of FTP commands relating to authentication with the server (USER, PASS) and file retrieval (RETR) was used to identify specific events in the captured traffic by displaying packets that used these commands with *grep*.

Over the timeframe of 20:03:24 – 20:07:47 UTC on October 21, 2023, two connections from a host at 192.168.1.6 to an FTP server at 192.168.1.20 with the credentials *ftpuser/starwars* and retrieval of five ZIP archives could be observed (Figure 3-3).

```
┌──(kali㉿kali)-[~/Documents/df/Unit 1 - Case Study - PCAP Files(2023)]
└─$ tshark -r Capture\ 2.pcap -Y "ftp" | grep -i "retr"
19262 657021.326926  192.168.1.6 → 192.168.1.20 FTP 70 Request: RETR 3v0ke.zip
19287 657027.449784  192.168.1.6 → 192.168.1.20 FTP 72 Request: RETR c0ll3ct.zip
19309 657033.887153  192.168.1.6 → 192.168.1.20 FTP 71 Request: RETR d3arth.zip
19334 657040.172024  192.168.1.6 → 192.168.1.20 FTP 70 Request: RETR dr0id.zip
19470 657251.981732  192.168.1.6 → 192.168.1.20 FTP 80 Request: RETR untitled folder.zip
```

Figure 3-3 Retrieval of 5 ZIP archives

Exporting these archives with *tshark* led to the acquisition of a total of 15 JPG files, all being fragments of a larger JPG image as only one of the files had a valid file header but contained an incomplete image. To reassemble the original file, the image files were rearranged and combined with the *cat* utility in the order so their names formed an Obi-Wan Kenobi quote, *I'll never understand how you can simplify these battles into some kind of game*, the use of which was received as a tip in the investigation brief. This revealed that the transferred file was a picture of a boat (Figure 3-4).

Figure 3-4 Reconstructed image

However, the discoloration present in the background of the image, characteristic of steganography, indicated that the image may contain hidden data. *SilentEye*, the use of which was suspected as it was mentioned in the *untitled folder* archives carved from both Capture 1 and 2, was used to uncover a hidden Base64 string within this image. This string was then decoded to *May the force be with you* in CyberChef.

3.3 CAPTURE 3

SHA266 hash: dda90e8e47d0e85ed3e2ca0ce7bbc9712d36286e36b73525df22d464b1dc4ead
Capture timeframe: 02.07.2014 16:38:50 UTC - 22.10.2023 16:56:49 UTC

Investigation of this capture file was approached by using the leads from the investigation brief in conjunction with the use of the frame contains display filter in *tshark* to identify packets that contained anything of interest. Looking for the disclosed suspect names within the capture allowed for the identification of HTTP POST requests containing the names of the suspects in the message body which led to the efficient discovery of the captured conversation between the suspects.

The conversation took place over the timeframe of 16:46:10 – 16:53:55 UTC on October 22, 2023, and originated from a host at 192.168.1.6, who used the name Narco Polo in the chat, addressed to 192.168.1.20.

The traffic between the two identified hosts was filtered out and saved to a new file to allow the extraction of all HTTP objects sent and received during this conversation without obstructing relevant evidence with other network traffic. This resulted in the acquisition of a PHP file containing the code for the chat layout, PHP files containing the messages sent by Narco Polo and HTML chat logs from the responses to HTTP GET requests. Reassembling the chat logs revealed the entire conversation (Figure 3-5) that took place between Narco Polo and El Chapo. It was concluded that the suspects intended to meet in Death Valley, California (36.62575185817829 -117.08896804489794) (Figure 3-6 and Figure 3-7) on Thursday, November 2nd, 2023, 10 PM (likely UTC-4 time zone as the log timestamps are 4 hours behind the capture UTC timestamps).

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

Figure 3-5 Full conversation between the suspects

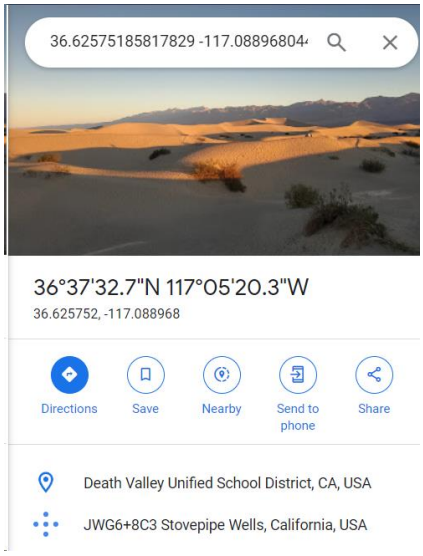


Figure 3-6 Meeting location

Figure 3-7 Satellite view of the meeting location

4 CRITICAL EVALUATION

4.1 INVESTIGATIVE CHALLENGES

The initial challenge was planning the investigative approach. The structuring of the investigative process was addressed by employing a robust methodology that addresses these concerns by defining investigative steps. A knowledge of digital forensics tools that are used in different scenarios helped to plan the process by identifying to right toolset. Additionally, ensuring that the investigation is forensically sound was addressed by a series of organisational measures which guaranteed that the original evidence was stored securely and could not be tampered with. This was continuously validated by checking the SHA-256 hashes of the files.

The primary challenge during the practical work was locating the traffic relevant to the case in the captures. This was addressed by analysing the protocol hierarchy of Capture 1 which helped identify the most used protocols and led to the discovery of possible malicious behaviour. For the other two captures, a knowledge of the protocols used was helpful as the relevant traffic could then be filtered out with the use of display filters in *tshark*. From there, when new leads were identified, the source and destination addresses could be established and used for further progression. The extensive documentation of the entire investigative process as outlined in the OSCAR methodology also helped identify connections between network events and aided in identifying which packets require further investigation and which are unrelated, and how to approach the extraction of further evidence.

Another challenge was identifying and isolating the relevant information from the recovered files. A lot of them contained information not related to the investigation, such as chess boxing rules. This issue was addressed by a thorough analysis of each obtained file to identify the relevant material. The suspects had employed several anti-forensic strategies during their operations such as splitting an image evidence file into smaller fragments and using encoding. Knowledge of file headers and familiarity with encoding algorithms aided in reconstructing the evidence.

Addressing the challenges encountered throughout the investigation outlined the importance of a sound methodology when conducting network forensics investigations to achieve better results. The application of well-defined investigative phases and familiarity with investigative tools and strategies strengthened the quality of the performed investigative work and ensured that the investigation was thorough. Additionally, the methodological approach aided during more challenging parts of the investigation by offering insights into how to address them, strengthening the investigative capability in the process.

4.2 REFLECTIONS

Overall, this investigation was successful at identifying the details of the case that were of interest. The traffic between the identified suspects was thoroughly analysed and all information that was within the scope of the investigation was examined, however, had there not been directions by the health regulatory agency to ignore other traffic, a more thorough investigation could have been performed on the capture files and possibly provide additional information on this case. For example, more advanced criminals could have impeded the investigation by using methods such as password-protected steganography, utilising

more than one host for file sharing, and using encryption. Another concern could be the use of proxy servers, packet header manipulation, session hijacking, etc., to falsify IP addresses and make traffic appear as it originates from other hosts. Packet headers could also have been manipulated to fake protocols and conceal evidence. Additional analysis of the traffic that was deemed irrelevant for this investigation could reveal these practices if any are present.

It should be noted that several pieces of information related to this case were not available during the investigation, such as the country the suspects operated in, and how they acquired and transported their shipments. The identified substances are used for medicinal purposes and the legality of this depends on how they were acquired and transported and their legality in the country the suspects operated in, which remains undisclosed, however, as of the time of writing (December 2023), they are legal in the United Kingdom where this investigation was conducted. As such, it cannot be concluded whether any law has been broken just from this investigation, so the verdict of this falls on the people overseeing this case.

Additionally, the quality of the received evidence may impede the reliability of the investigation, as anomalies can be observed in the original files. One of these anomalies is an instant jump from 2014 to 2023 in packets 9919 – 9920 of Capture 3 (Figure 0-21). The appropriate measures were taken to retain the evidence in the state it was received in, however, it cannot be ruled out that the evidence had been tampered with before turning it in for analysis. As such, the meaningfulness of these results is questionable.

REFERENCES

achorein, 2023. *silenteye.* [Online]
Available at: https://github.com/achorein/silenteye
[Accessed 6 December 2023].

Burgess, B., 2023. *What is Desktop.ini on Windows?.* [Online]
Available at: https://www.groovypost.com/explainer/what-is-desktop-ini-on-windows/
[Accessed 6 December 2023].

Davidoff, S. & Ham, J., 2012. *Network Forensics: Tracking Hackers through Cyberspace.* London: Pearson.

Drugbank Online, 2023. *Building the foundation for better health outcomes.* [Online]
Available at: https://go.drugbank.com
[Accessed 6 December 2023].

ENISA, 2016. *Forensic Analysis Network Incident Response Toolset,* s.l.: ENISA.

file.net, n.d. *What is srvsvc.dll?.* [Online]
Available at: https://www.file.net/process/srvsvc.dll.html
[Accessed 6 December 2023].

GCHQ, 2023. *CyberChef.* [Online]
Available at: https://gchq.github.io/CyberChef/
[Accessed 6 December 2023].

Google LLC, 2023. *Google.* [Online]
Available at: https://www.google.com/
[Accessed 6 December 2023].

Google LLC, 2023. *Google Earth.* [Online]
Available at: https://earth.google.com/
[Accessed 6 December 2023].

Google LLC, 2023. *Google Translate.* [Online]
Available at: https://translate.google.co.uk/
[Accessed 6 December 2023].

Jaswal, N., 2019. *Hands-On Network Forensics : Investigate Network Attacks and Find Evidence Using Common Network Forensic Tools.* Birmingham: Packt Publishing, Limited.

Offensive Security, 2023. *Kali Linux | Penetration Testing and Ethical Hacking Linux Distributio.* [Online]
Available at: https://www.kali.org/
[Accessed 6 December 2023].

Rouse, M., 2011. *NetBIOS Session Service.* [Online]
Available at: https://www.techopedia.com/definition/25190/netbios-session-service-nbss
[Accessed 6 December 2023].

Sheldon, R. & Scarpati, J., 2021. *Server Message Block protocol (SMB protocol).* [Online]
Available at: https://www.techtarget.com/searchnetworking/definition/Server-Message-Block-Protocol
[Accessed 6 December 2023].

Wireshark Foundation, 2023. *Wireshark · Go Deep.* [Online]
Available at: https://www.wireshark.org/
[Accessed 6 December 2023].

APPENDICES (INVESTIGATION OUTPUT)

APPENDIX A – DETAILED INVESTIGATIVE ANALYSIS

Before beginning the investigation on each of the three capture files, several actions were taken to ensure the forensic integrity of the evidence:

1. The directory containing the original evidence was set to read-only (Figure 0-1).

```
┌──(kali㉿kali)-[~/Documents/df]
└─$ sudo chmod a=r -R Unit\ 1\ -\ Case\ Study\ -\ PCAP\ Files\(2023\)

[sudo] password for kali:

┌──(kali㉿kali)-[~/Documents/df]
└─$ sudo chmod a=rx Unit\ 1\ -\ Case\ Study\ -\ PCAP\ Files\(2023\)
```

Figure 0-1 Original evidence set to read-only

2. SHA256 hashes were generated for each file (Figure 0-2, Appendix C – Cryptographic File Hashes Original Evidence FIles). As the investigation progressed these were compared against any new hashes generated for the evidence files whenever they were accessed to observe if they had been changed.

```
┌──(kali㉿kali)-[~/Documents/df/Unit 1 - Case Study - PCAP Files(2023)]
└─$ for i in *; do sha256sum $i; done
e782a7086cc2b349fb32cf9a2acdf6645c225339752cd981ee0cc063e9c848cb  Capture 1.pcap
034042d655c57403ee44f59587d9b6c832b4cc89a660fe47fb4e69d3ae14e79f  Capture 2.pcap
dda90e8e47d0e85ed3e2ca0ce7bbc9712d36286e36b73525df22d464b1dc4ead  Capture 3.pcap
```

Figure 0-2 SHA-256 hashes generated for the capture files

3. Copies of each capture file that would be used during the investigation were created and stored in a different directory from the originals. These copies were used for any investigative actions.

Capture 1
SHA256 hash: e782a7086cc2b349fb32cf9a2acdf6645c225339752cd981ee0cc063e9c848cb
Capture timeframe: 20.10.2023 19:18:01 UTC - 22.10.2023 05:23:52 UTC.

The information contained within the brief for this capture file (Section 1.1 Capture 1) suggests that the suspect has uploaded files that may contain information vital for this investigation. Statistical analysis with Wireshark of the protocols used in the captured network traffic revealed that the most used protocol was TCP with 96.5% of the captured traffic (Figure 0-3).

Protocol	Percent Packets	Packets	Percent Bytes	Bytes
Frame	100.0	32693	100.0	23125434
Ethernet	100.0	32693	2.3	520987
Link Layer Discovery Protocol	0.1	25	0.0	1150
Address Resolution Protocol	0.1	28	0.0	1288
Internet Protocol Version 6	0.1	41	0.0	1640
Logical-Link Control	1.2	386	0.1	16566
Internet Protocol Version 4	98.5	32213	2.8	644260
Data	0.1	18	0.9	214752
Internet Control Message Protocol	0.2	75	0.0	2732
User Datagram Protocol	1.8	590	0.0	4720
Transmission Control Protocol	96.5	31536	94.5	21846164

Figure 0-3 Protocol hierarchy of Capture 1, with TCP being the most used

The most used protocol that ran over TCP was NetBIOS Session Service, which is a method used to connect two hosts for transmitting large amounts of data (Rouse, 2011). Of this, SMB2 is used the most (Figure 0-4).

Transmission Control Protocol	96.5	31536
Hypertext Transfer Protocol	3.3	1074
Transport Layer Security	5.5	1795
NetBIOS Session Service	5.7	1861
SMB (Server Message Block Protocol)	1.8	587
SMB2 (Server Message Block Protocol version 2)	3.7	1196
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	0.0	4
Server Service	0.0	2
Malformed Packet	0.1	24
Data	0.1	35

Figure 0-4 Large usage of SMB2

The use of various versions of the SMB protocol could also be immediately observed when manually examining the capture in *Wireshark* (Figure 0-5).

No.	Time	Source	Destination	Protoc	Leng	Info
1	2023-10-20 19:18:01.909165	TaicangT&WEl_7…	Broadcast	ARP	60	Who has 192.168.1.6? Tell 192.168.1.1
2	2023-10-20 19:18:06.717306	192.168.1.6	192.168.1.…	TCP	66	54167 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
3	2023-10-20 19:18:06.717327	192.168.1.20	192.168.1.6	TCP	66	445 → 54167 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
4	2023-10-20 19:18:06.717454	192.168.1.6	192.168.1.…	TCP	60	54167 → 445 [ACK] Seq=1 Ack=1 Win=131328 Len=0
5	2023-10-20 19:18:06.717741	192.168.1.6	192.168.1.…	SMB	127	Negotiate Protocol Request
6	2023-10-20 19:18:06.717749	192.168.1.20	192.168.1.6	TCP	54	445 → 54167 [ACK] Seq=1 Ack=74 Win=64256 Len=0
7	2023-10-20 19:18:06.718956	192.168.1.20	192.168.1.6	SMB2	216	Negotiate Protocol Response
8	2023-10-20 19:18:06.719379	192.168.1.6	192.168.1.…	SMB2	220	Session Setup Request, NTLMSSP_NEGOTIATE
9	2023-10-20 19:18:06.719389	192.168.1.20	192.168.1.6	TCP	54	445 → 54167 [ACK] Seq=163 Ack=240 Win=64128 Len=0
10	2023-10-20 19:18:06.720804	192.168.1.20	192.168.1.6	SMB2	329	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
11	2023-10-20 19:18:06.721121	192.168.1.6	192.168.1.…	SMB2	647	Session Setup Request, NTLMSSP_AUTH, User: LAPTOP-8K2DHPD7\Varun
12	2023-10-20 19:18:06.721135	192.168.1.20	192.168.1.6	TCP	54	445 → 54167 [ACK] Seq=438 Ack=833 Win=64128 Len=0
13	2023-10-20 19:18:06.723227	192.168.1.20	192.168.1.6	SMB2	139	Session Setup Response
14	2023-10-20 19:18:06.723464	192.168.1.6	192.168.1.…	SMB2	170	Tree Connect Request Tree: \\192.168.1.20\share
15	2023-10-20 19:18:06.723471	192.168.1.20	192.168.1.6	TCP	54	445 → 54167 [ACK] Seq=523 Ack=949 Win=64128 Len=0
16	2023-10-20 19:18:06.724599	192.168.1.20	192.168.1.6	SMB2	138	Tree Connect Response
17	2023-10-20 19:18:06.724722	192.168.1.6	192.168.1.…	SMB2	234	Create Request File:
18	2023-10-20 19:18:06.724733	192.168.1.20	192.168.1.6	TCP	54	445 → 54167 [ACK] Seq=607 Ack=1129 Win=64128 Len=0
19	2023-10-20 19:18:06.729151	192.168.1.20	192.168.1.6	SMB2	211	Create Response File:
20	2023-10-20 19:18:06.729317	192.168.1.6	192.168.1.…	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File:
21	2023-10-20 19:18:06.729324	192.168.1.20	192.168.1.6	TCP	54	445 → 54167 [ACK] Seq=764 Ack=1237 Win=64128 Len=0
22	2023-10-20 19:18:06.766175	192.168.1.20	192.168.1.6	SMB2	186	GetInfo Response
23	2023-10-20 19:18:06.766603	192.168.1.6	192.168.1.…	SMB2	168	Tree Connect Request Tree: \\192.168.1.20\IPC$
24	2023-10-20 19:18:06.766621	192.168.1.20	192.168.1.6	TCP	54	445 → 54167 [ACK] Seq=896 Ack=1351 Win=64128 Len=0
25	2023-10-20 19:18:06.767843	192.168.1.20	192.168.1.6	SMB2	138	Tree Connect Response
26	2023-10-20 19:18:06.768001	192.168.1.6	192.168.1.…	SMB2	190	Create Request File: srvsvc

Figure 0-5 SMB traffic in Wireshark

As this protocol is used to access shared files, printers, serial ports, and other resources over a network (Sheldon & Scarpati, 2021), its usage was further investigated it could have possibly been used to access the reportedly uploaded files. To observe what network shares were accessed via SMB, connection requests were searched for with the display filter _ws.col.info matches "(?i)connect request", which highlighted all packets that contained connection and disconnection requests. Numerous requests from 192.168.1.6 to access network shares on 192.168.1.20 could be observed (Figure 0-6).

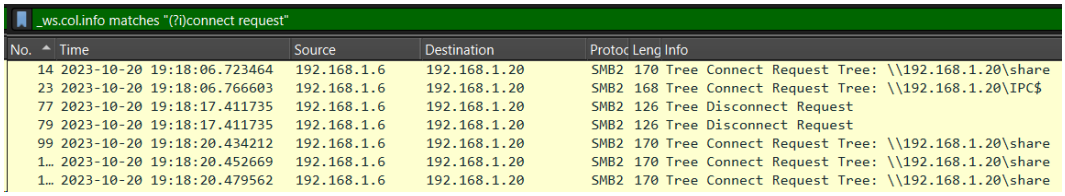


Figure 0-6 Connection requests to network shares on 192.168.1.20

Examining the connection requests to the network shares one by one by following their corresponding TCP streams, revealed access to a possible directory of interest, named *Substances* in TCP stream 3 (display filter – tcp.stream eq 3) when following the connect request from packet 160 (Figure 0-7).

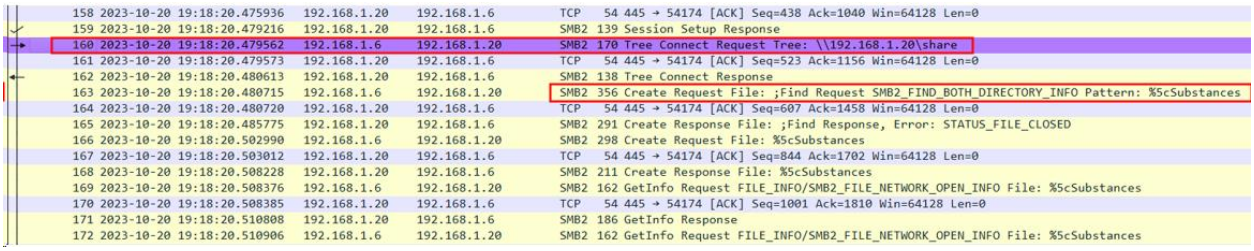


Figure 0-7 Connection to network the share on 192.168.1.20 and request for 'Substances' directory

Several files within this directory appeared to be accessed by the suspect. To obtain the files accessed, SMB objects were exported from the capture in *Wireshark* with *File>Export Objects> SMB…> Save All*. 28 items were extracted from the capture this way (Figure 0-8). As with the original evidence, these files were set to read-only, their SHA-256 hashes were generated (Appendix C – Cryptographic File Hashes Exported SMB Objects), and copies to work on created.

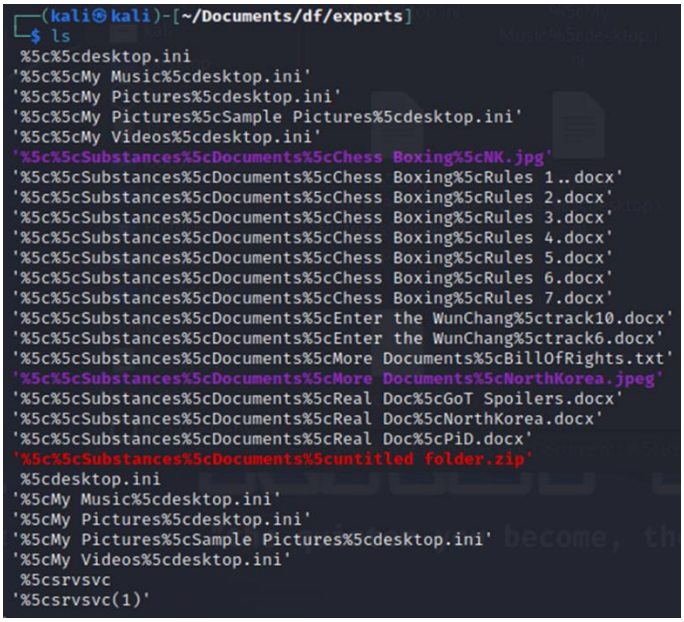


Figure 0-8 Files extracted from Capture 1

10 of the exported files were Dekstop.ini files which are hidden files that store information about the folder configuration in Windows systems (Burgess, 2023). These were not examined further, as they were not relevant to the investigation.

Two images – NK.jpg and NorthKorea.jpeg, both containing the North Korean flag, were also retrieved. Doing the *file* command on them, revealed that NK.jpg had PNG format (Figure 0-9), but the file type of NorthKorea.jpeg matched with its extension.

```
└─$ file %5c%5cSubstances%5cDocuments%5cChess\ Boxing%5cNK.jpg
%5c%5cSubstances%5cDocuments%5cChess Boxing%5cNK.jpg: PNG image data, 1600 x 800, 8-bit/color RGBA
, non-interlaced
```

Figure 0-9 file command used on NK.jpg

Next, *binwalk* was used to discover possible hidden data within the image files. NorthKorea.jpeg contained a hidden ZIP archive (Figure 0-10) which was extracted with binwalk -e.

```
└─$ binwalk %5c%5cSubstances%5cDocuments%5cMore\ Documents%5cNorthKorea.jpeg

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

Figure 0-10 binwalk revealing a hidden ZIP archive in NorthKorea.jpeg

The extracted archive contained a directory titled *untitled* which contained a python script *broken.py* (Appendix B – Recovered Files, Scripts) which appeared to contain functions used to encode messages. The script was unfinished as it contained no calls to the defined functions and several syntax errors.

Among the extracted files were also 12 Word documents that had their contents encoded in Base64. CyberChef and in one case Google Translate were used to decode the file contents. The decoded versions of these files are contained within Appendix B – Recovered Files Word Documents. Of these documents, track6.docx contained a list of drugs and quantities involved in the drug trafficking case (see Figure 0-11) which was what the brief had tasked to find.

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

Figure 0-11 Substance names and amounts

The other documents contained the following:

- **Rules 1 – 7**: Contained an extensive summary of the rules of chess boxing.
- **Track 10**: contained the lyrics to *Protect Ya Neck* by Wu-Tang Clan.
- **GoT spoilers**: contained incorrect information about the plot of Game of Thrones series.
- **NorthKorea**: contained a text in Russian relating to time travel technology possessed by the North Korean government and how they intend to use it, asking for Obi-Wan Kenobi for help.
- **PiD**: contained a letter with images where the author (William Campbell) jokes about supposedly stealing Paul McCartney's identity after the real Paul's alleged death in 1966.

The extracted files also contained BillOfRights.txt – a text file containing the US Bill of Rights and amendments.

Lastly, an empty ZIP archive titled *untitled folder* was also retrieved. It contained a folder by the same name and several other nested folders all named *untitled folder* or *untitled folder 2*. The innermost directory was called *SilentEye* which may have been a reference to a steganography tool by the same name (Figure 0-12).

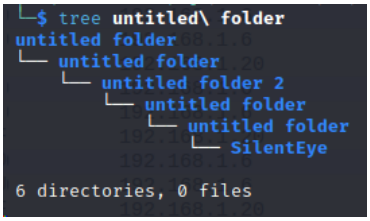


Figure 0-12 Structure of 'untitled folder'

Two more files named *srvsvc,* were also retrieved. One of them was empty, and the other was 1kb in size. This filename refers to the Windows Dynamic Linked Library (srvsvc.dll) which is responsible for managing access to resources shared over a network (file.net, n.d.). These files were deemed not relevant to the investigation.

Capture 2
SHA256 hash: 034042d655c57403ee44f59587d9b6c832b4cc89a660fe47fb4e69d3ae14e79f
Capture timeframe: 14.10.2023 05:33:35 UTC - 21.10.2023 20:08:03 UTC

The brief for this capture mentions the use of FTP so it was filtered and displayed with *tshark*. The use of *grep* to search for FTP-specific commands, such as specifying username (USER) and password (PASS) when connecting to the server (Figure 0-13), helped identify FTP two connections to a server at 192.168.1.20 from 192.168.1.6 with the credentials *ftpuser* and *starwars* in packets 19206, 19211, 19434, and 19438.

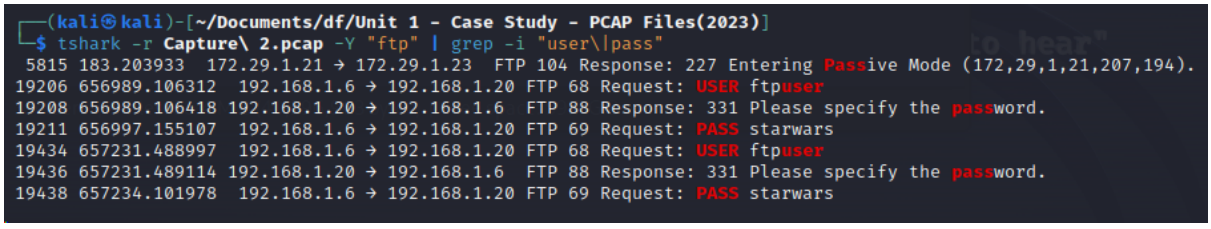


Figure 0-13 Connection to the FTP server at 192.168.1.20

Searching for the retrieved files (RETR command) revealed 5 ZIP archives that were retrieved by *ftpuser* (Figure 0-14). Four of them were obtained after the first connection attempt to the server and the fifth (untitled folder.zip) was retreived during the second connection attempt.

```
┌──(kali㉿kali)-[~/Documents/df/Unit 1 - Case Study - PCAP Files(2023)]
└─$ tshark -r Capture\ 2.pcap -Y "ftp" | grep -i "retr"
19262 657021.326926  192.168.1.6 → 192.168.1.20 FTP 70 Request: RETR 3v0ke.zip
19287 657027.449784  192.168.1.6 → 192.168.1.20 FTP 72 Request: RETR c0ll3ct.zip
19309 657033.887153  192.168.1.6 → 192.168.1.20 FTP 71 Request: RETR d3arth.zip
19334 657040.172024  192.168.1.6 → 192.168.1.20 FTP 70 Request: RETR dr0id.zip
19470 657251.981732  192.168.1.6 → 192.168.1.20 FTP 80 Request: RETR untitled folder.zip
```

Figure 0-14 Retrieval of 5 ZIP archives

These archives were extracted with *tshark* with the command: tshark -r Capture\ 2.pcap --export-objects "ftp-data,../exports/pcap2". As before, to ensure the forensic integrity of the evidence, file hashes were generated (Appendix C – Cryptographic File Hashes, Exported FTP-DATA), and copies to work on were created while the originals were kept as read-only.

The *untitled folder* archive was the same as the one retrieved from Capture 1 (Figure 0-12). The other four ZIP archives contained folders titled *split1*, *split2*, *split3* and *split4* respectively (Figure 0-15, Figure 0-16, Figure 0-17, Figure 0-18). These folders contained 3-4 JPG images each, however, only the image from *split1*, titled I.jpg had a valid file signature. I.jpg also appeared to only contain the top part of an image, so it was concluded that the rest of the JPG files were all fragments of the same image.

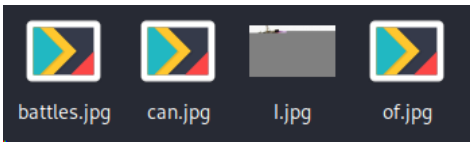


Figure 0-15 split1

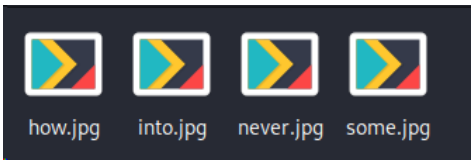


Figure 0-16 split2

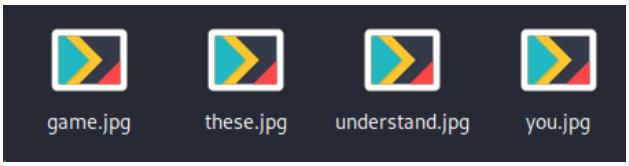


Figure 0-17 split3

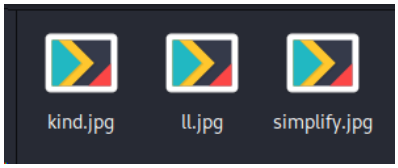


Figure 0-18 split4

To reconstruct the original image the images were arranged in an order so their names would spell an Obi-Wan Kenobi quote based on the received tip (Section 1.1 Capture 2). This quote was found by searching for *obi wan Kenobi quotes "simplify"* in Google to find a quote that contains one of the words ("simplify") that were used as filenames. A quote from season 2, episode 5 of *Star Wars: The Clone Wars* was identified as a match: *I'll never understand how you can simplify these battles into some kind of game*.

To reassemble the image, the *cat* utility was used to output the contents of each file in the right order and write them to a new image file (Figure 0-19).

```
┌──(kali㉿kali)-[~/…/exports/pcap2/copies/output]
└─$ cat I.jpg ll.jpg never.jpg understand.jpg how.jpg you.jpg can.jpg simplify.jpg these.jpg battles.jpg into.jpg some.jpg kind.jpg
of.jpg game.jpg > output.jpg
```

Figure 0-19 Reassembling the image

The reassembled image displayed a boat (Figure 0-20). The image background contained discoloured dots which indicated the possible presence of steganography. As the *SilentEye* steganography tool had been referenced in traffic from Captures 1 and 2, it was used to retrieve the hidden message within this picture.

Figure 0-20 Reconstructed image

Using the default password – *silenteye*, revealed a Base64 encoded string *TWF5IHRoZSBmb3JjZSBiZSB3aXRoIHlvdQ==* hidden within the image (Figure 0-21). CyberChef was used to decode it to: *May the force be with you.*

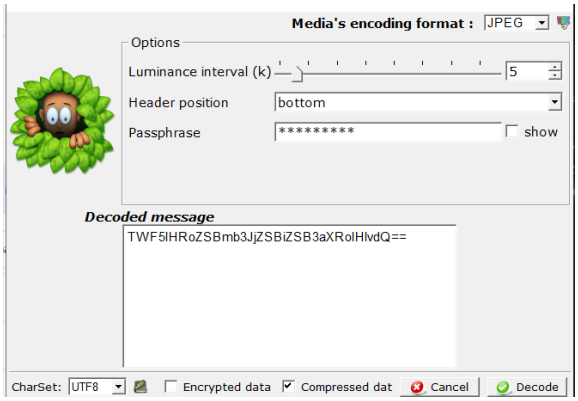


Figure 0-21 Hidden string extracted from the image

No other traffic of interest was identified between the hosts 192.168.1.6 and 192.168.1.20 so it could be concluded that the foreign contact received an image of a boat, split into numerous fragments as an anti-forensic practice, that contained a Base64 encoded message hidden within.

Capture 3
SHA266 hash: dda90e8e47d0e85ed3e2ca0ce7bbc9712d36286e36b73525df22d464b1dc4ead
Capture timeframe: 02.07.2014 16:38:50 UTC - 22.10.2023 16:56:49 UTC

This capture contained an anomalous jump from 2014 to 2023 in the timestamps of packets 9919 and 9920 (Figure 0-22):

```
 9919 2014-07-02 16:52:32.749857   Intel_f9:ae:3e  ASUSTekCOMPU_99:1f… LLC    66 I, N(R)=16, N(S)=0; DSAP 0x2e Individual, SSAP 0x56 Command
 9920 2023-10-22 16:45:14.750286   192.168.1.6     192.168.1.20        HTTP  491 GET /newchat/@@cht/log.html?_=1697993752916 HTTP/1.1
```

Figure 0-22 Anomalous time change within the capture

Based on the brief for this capture, *tshark* was used to perform a string search to establish if any packets contained the mention of the identified suspects: Narco Polo and El Chapo. This proved valuable as communication between 192.168.1.6 and 192.168.1.20 that contained mentions of these names was identified (Figure 0-23). The packet information outlined the use of HTTP POST requests to send chat messages between the two parties.

```
┌──(kali㉿kali)-[~/Documents/df/Unit 1 - Case Study - PCAP Files(2023)]
└─$ tshark -r Capture\ 3.pcap -Y "frame contains \"Polo\""
10024 293674040.354931  192.168.1.6 → 192.168.1.20 HTTP 747 POST /newchat/@@cht/index.php HTTP/1.1  (application/x-www-form-ur
lencoded)

┌──(kali㉿kali)-[~/Documents/df/Unit 1 - Case Study - PCAP Files(2023)]
└─$ tshark -r Capture\ 3.pcap -Y "frame contains \"Chapo\""
10105 293674088.265366  192.168.1.6 → 192.168.1.20 HTTP 631 POST /newchat/@@cht/post.php HTTP/1.1  (application/x-www-form-urlencoded)
```

Figure 0-23 HTTP POST requests containing names of the suspects

Dumping the contents of one of these packets (packet 10105) with *tshark -V* revealed the full message (Figure 0-24):

```
    File Data: 57 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
    Form item: "text" = "Are you aware of the current scrutiny on El Chapo?"
        Key: text
        Value: Are you aware of the current scrutiny on El Chapo?
```

Figure 0-24 A chat message between the suspects

To obtain the entire conversation between the suspects, traffic to and from the IP address 192.168.1.6 was filtered out and written to a new capture file (tshark -r Capture\ 3.pcap -Y "ip.addr==192.168.1.6" -w filtered.pcap). This file was then used to extract all HTTP objects related to the traffic originating from or being addressed to this host, so no irrelevant output would be obtained (tshark -r filtered.pcap --export-objects "http, ../exports/pcap3").

This retrieved 308 items: HTML and PHP files. One of the PHP files contained the HTML code for the chat layout and the rest contained the messages sent by Narco Polo from 192.168.1.6 with HTTP POST requests. The HTML files contained chat logs of the entire conversation. To obtain a clear overview of the

entire conversation every HTML file was combined with *cat* (for i in log*; do cat $i; done > chat.html). This resulted in the transcript of the entire conversation[1].

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

Figure 0-25 Full conversation between the suspects

The resulting chat conversation overview (Figure 0-25) revealed that the suspects arranged a meeting for the 2nd of November at 10 PM. The year of this conversation is not specified in the logs, but upon manually examining the corresponding POST requests with *Wireshark*, it could be seen that the conversation took place in 2023, making November 2 a Thursday. Furthermore, coordinates, 36.62575185817829 -117.08896804489794, could be seen and inputting these in Google Earth revealed that the meeting was supposed to take place in Death Valley, California, USA (Figure 0-26 and Figure 0-27). This concluded the investigation of Capture 3 with the requested information obtained.

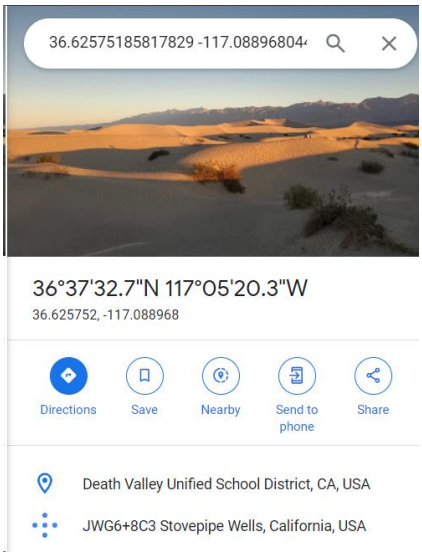


Figure 0-26 Meeting location

Figure 0-27 Satellite view of the meeting location

[1]It should be noted that this step resulted in the conversation transcript repeating numerous times in the output as it was reassembled from duplicate log files originating from HTML GET requests. A new chat log containing the entire message history so far was retrieved every time a request was made hence the repetition.

APPENDIX B – RECOVERED FILES

Images

NK.jpg

NorthKorea.jpeg

Scripts

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
```

Word Documents

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.

Rules 2.docx

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

Rules 3.docx

3. PENALTIES FOR RULE BREACHES
A chess penalty could take the form of:

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

Rules 4.docx

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

- Stop the clock and resolve the problem.
- Stop the clock and replace it with a new clock. This action is most likely if there is a repeated malfunction, or it's one of the later chess rounds where a player is short of time.

Rules 5.docx

5. WCBA CHESS RULES FOR CHESSBOXING
Chess tournament rules have legal points that casual players may be unfamiliar with. The official laws of chess are on the website of FIDE, the chess governing body http://www.fide.com/component/handbook/?id=32andview=category. Highlighted below are legal points that cause most disputes in tournament chess situations.

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

Touch move

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

Castling touch move

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

Hand is taken off a piece

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

Illegal move

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

"J'Adoube" rule.

Normal Chess Rules

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

Chessboxing Rules (adapted because both players have headphones)

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

Pawn promotion

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

Clock

- The clock MUST be pressed with the same hand that makes the move
- Running out of time. If a player has no time remaining, then he is lost if his opponent can checkmate him assuming the most unskilled play, otherwise the game is a draw. For example, if Player A has three queens and a king, and Player B has one pawn and a king, then Player B wins if Player A runs out of time.
- A player should not start to make his move until the opponent has physically pressed his clock.
- Time scramble – disputes can arise when 1 or both players are short of time and moving extremely quickly:
  - 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.
  - 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.
  - 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.

track6.docx

Sensitive information

Drugs Records

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

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]

GoT Spoilers.docx

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

Hodor kills Theon.

Daenerys gets eaten by a dragon.

Stannis falls in love with Tyrion.

NorthKorea.docx

Original Decoded Text:

Для кого это может касаться:

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

Пожалуйста, Оби-Ван, ты моя единственная надежда.

English Translation:

To whom it may concern:

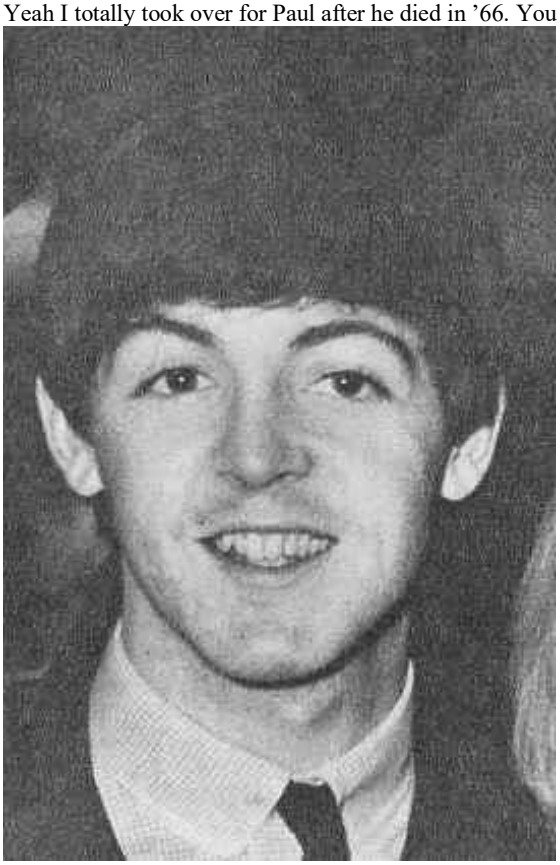
I witnessed that Kim Jong Un and the North Korean government have developed a program that allows them to travel through time. By using this technology, I believe they intend to move forward and change the outcome of the Korean War.

Please, Obi-Wan, you are my only hope.

PiD.docx

Dear Ed,

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



Before(Paul)

After(Me)

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

Thanks for the inquiry,

William Campbell
(Paul McCartney)

Text 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.

APPENDIX C – CRYPTOGRAPHIC FILE HASHES

Original Evidence FIles

e782a7086cc2b349fb32cf9a2acdf6645c225339752cd981ee0cc063e9c848cb Capture 1.pcap
034042d655c57403ee44f59587d9b6c832b4cc89a660fe47fb4e69d3ae14e79f Capture 2.pcap
dda90e8e47d0e85ed3e2ca0ce7bbc9712d36286e36b73525df22d464b1dc4ead Capture 3.pcap

Exported SMB Objects

35522adcad64c91a0b20f15e0c855245f12a1f728c19e23bb17427570269fdb6 %5c%5cdesktop.ini
b5a55fb776eec1ba507d7fce31dfbe0d95387c17bf90fffb4aeb05b65f79d3eb %5c%5cMy Music%5cdesktop.ini
46b0d485985dbf8bab8bbce705f700360b369321964e8c97c686799ae95fffcd %5c%5cMy Pictures%5cdesktop.ini
29e208e2247ddf5d4bef09f41a08c6f5aad712a4fbf485add0840180cbb0abe7 %5c%5cMy Pictures%5cSample Pictures%5cdesktop.ini
6fb593f03442fa41e4c86be61b86d22a5548f210b00d418497a9b0225bda1a91 %5c%5cMy Videos%5cdesktop.ini
2288c6a607e6a7656c47e38bdbfcfa0175843506ffe6f1b897432601728c1f91 %5c%5cSubstances%5cDocuments%5cChess Boxing%5cNK.jpg
a8f280b082b84f25c3627c4575868d4f93ab9ffb2a6b0516a10c5fd2143aff0e %5c%5cSubstances%5cDocuments%5cChess Boxing%5cRules 1..docx
e7f44df6ca4618f2724b97d31cfe4167497374a05109cfd3e6b5997011780781 %5c%5cSubstances%5cDocuments%5cChess Boxing%5cRules 2.docx
63b2ef33ad0ce414cce34262b27b4af48bec0bb0803a1d399cb5a61407f056ad %5c%5cSubstances%5cDocuments%5cChess Boxing%5cRules 3.docx
1c0177ec10c47baef1fec48367108fabe3e9b0947634d61749c6d5e924dfaa05 %5c%5cSubstances%5cDocuments%5cChess Boxing%5cRules 4.docx
f7b475ab71ab296de241156a4f591d2d0047a9649c6bdaa17ca71ffe8a693538 %5c%5cSubstances%5cDocuments%5cChess Boxing%5cRules 5.docx
42571c4311c1c69d499d3b97ec91d629bbb9b2e16eb37caeab0a341f04b5ad7c %5c%5cSubstances%5cDocuments%5cChess Boxing%5cRules 6.docx
15746f43d97ac9588dac17f2f381277aa546005e8bf0732db00ba372e9e65124 %5c%5cSubstances%5cDocuments%5cChess Boxing%5cRules 7.docx
ea249f9224b39e04bd35e0ce49501e024c80812a160e8682a708ba1c9d826130 %5c%5cSubstances%5cDocuments%5cEnter the WunChang%5ctrack6.docx
5e15d11699ba6bf7499a703a17110eb00e3ea9fe83583f3464333c10d67dc5a1 %5c%5cSubstances%5cDocuments%5cEnter the WunChang%5ctrack10.docx
cf0ae48fdef7829bf6f1ecb501488bd5ad58012c1ba17239c5ee1346a7b0d743 %5c%5cSubstances%5cDocuments%5cMore Documents%5cBillOfRights.txt
adb289290cfb1a6441da251c4024eb0795f2b3159ce219dd2934d4699a922af8 %5c%5cSubstances%5cDocuments%5cMore Documents%5cNorthKorea.jpeg
28fb083122aa50bda024398d81eb6d27f7e0ad1c2f46ad3a2038272746564ac6 %5c%5cSubstances%5cDocuments%5cReal Doc%5cGoT Spoilers.docx
856732a7772c5984d7eae44d16a333acefcc278c35b6f5e9f319de3c9e4e3ecb %5c%5cSubstances%5cDocuments%5cReal Doc%5cNorthKorea.docx
07a4540f9203f946f75dcc3b2b873ee412db2569d0beb3c7e71e96f4c415ebfd %5c%5cSubstances%5cDocuments%5cReal Doc%5cPiD.docx

41b423319d29345d72b651b19a9f2f1999638d24ae3e64fb1f9943229ef89bf4 %5c%5cSubstances%5c Documents%5cuntitled folder.zip
35522adcad64c91a0b20f15e0c855245f12a1f728c19e23bb17427570269fdb6 %5cdesktop.ini
b5a55fb776eec1ba507d7fce31dfbe0d95387c17bf90fffb4aeb05b65f79d3eb %5cMy Music%5cdesktop.ini
46b0d485985dbf8bab8bbce705f700360b369321964e8c97c686799ae95fffcd %5cMy Pictures%5cdesktop.ini
29e208e2247ddf5d4bef09f41a08c6f5aad712a4fbf485add0840180cbb0abe7 %5cMy Pictures%5cSample Pictures%5cdesktop.ini
6fb593f03442fa41e4c86be61b86d22a5548f210b00d418497a9b0225bda1a91 %5cMy Videos%5cdesktop.ini
99e227a8cf8089434d5510e2097bf90dab1d0ac6ad5484eeb3734188306e8fad %5csrvsvc
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 %5csrvsvc(1)

Exported FTP-DATA

95899a51fbda8d72c634d6a101e919cf115b3e6b429c96f69a2768378bfd68e7 3v0ke.zip
f00d3f9b3edfec34c2abeb8c833962f79fcf520abe2b6a54f88aa21963bdbdd2 c0ll3ct.zip
2261c9ae9143a2e4c4a26c506903958a9379b47bc403dc5e133268e0f7387066 d3arth.zip
23b0028fe108bdf34c6eca1fd9b67f91e3eb7717ce0038cfc2e9bdb4a67a8768 dr0id.zip
41b423319d29345d72b651b19a9f2f1999638d24ae3e64fb1f9943229ef89bf4 untitled folder.zip