CMP416: Forensic Network Investigation Report

Alex McNaughton [2000207]

Contents

1. Introduction 2
2. Capture 1 3
   2.1. Identification 3
   2.2. Collection and Preservation 3
   2.3. Strategize 3
   2.4. Methodology 3
   2.5. Analysis 5
   2.6. Documentation and Presentation 5
3. Capture 2 5
   3.1. Identification 5
   3.2. Collection 6
   3.3. Strategize 6
   3.4. Methodology 6
   3.5. Analysis 7
   3.6. Documentation and Presentation 7
4. Capture 3 8
   4.1. Identification 8
   4.2. Collection 8
   4.3. Strategize 8
   4.4. Methodology 8
   4.5. Analysis 9
      4.5.1. Inconsistencies in capture timing 10
   4.6. Documentation and Presentation 10
5. Timeline 11
   5.1. Capture 1 (Oct 20, 2023 19:18:01 - Oct 22, 2023 05:23:52) 11
   5.2. Capture 2 (Oct 14, 2023 05:33:35 - Oct 21, 2023 20:08:03) 11
   5.3. Capture 3 (Jul 2, 2014 16:38:50 - Oct 22, 2023 16:56:49) 11
6. Evaluation 12
7. Conclusion 14
8. Additional Data 14

Appendix A: MD5 hashes of evidence 14
Appendix B: Chat logs using provided timestamp 14
Appendix C: Drug list obtained in Capture 1 15
Appendix D: Combined result of output 15

1. Introduction

The investigative team has been tasked by the health regulatory agency to investigate 3 capture files obtained by recording traffic within a drug trafficking network. Throughout the course of this report, the investigative team will identify sources of evidence within each capture file, strategize methods to obtain evidence from each log, apply these strategies to the evidence, and procure the required information from each capture. Once completed, the investigative team will critically evaluate the investigative methods applied, the tools used to extract evidence, and the nature of the methods used to obfuscate the data from investigators.

Through forensic methodology, the investigative team were able to extract all of the evidence required by the health regulatory agency, and have presented the information collected within the Additional data section. Evaluation of the tools used proved that they were forensically sound and did not tamper with evidence. Evaluation of the methods employed by the drug trafficking ring showed that the employees of the ring were using out of date and insecure methods to conduct their business.

2. Capture 1

2.1. Identification

Capture 1 is a PCAP file given to the forensic investigators as part of the ongoing investigation into the international drug trafficking case. Capture 1 is described by the health regulatory agency to contain a record of the inventory of drugs available to the trafficking network. As part of the investigation, it was made apparent that the exact quantities and method of obfuscation were required.

2.2. Collection and Preservation

Capture 1 was downloaded from the source into a Kali Linux virtual machine. Once extracted, an MD5 hash was generated of the file before any forensic analysis to maintain validity of the evidence.

2.3. Strategize

In order to deliver the required evidence from the given file, a network log analysis tool is required to further the investigation into the given network traffic, and extract the inventory of drugs from this traffic. Using a network analysis tool like Wireshark would be a perfect tool for this use case, as it contains all the functionality required to successfully begin identifying possible suspicious data found in the network log.

2.4. Methodology

Analysing capture 1 using Wireshark immediately reveals some information about the network log and the nature of the network activity captured. The start of the network capture can be identified by reading the metadata associated with the first packet, which sets the start date and time of the capture at exactly Oct 20, 2023 19:18:01.909165. The start of this log also shows that some file sharing is being attempted through the SMB port.

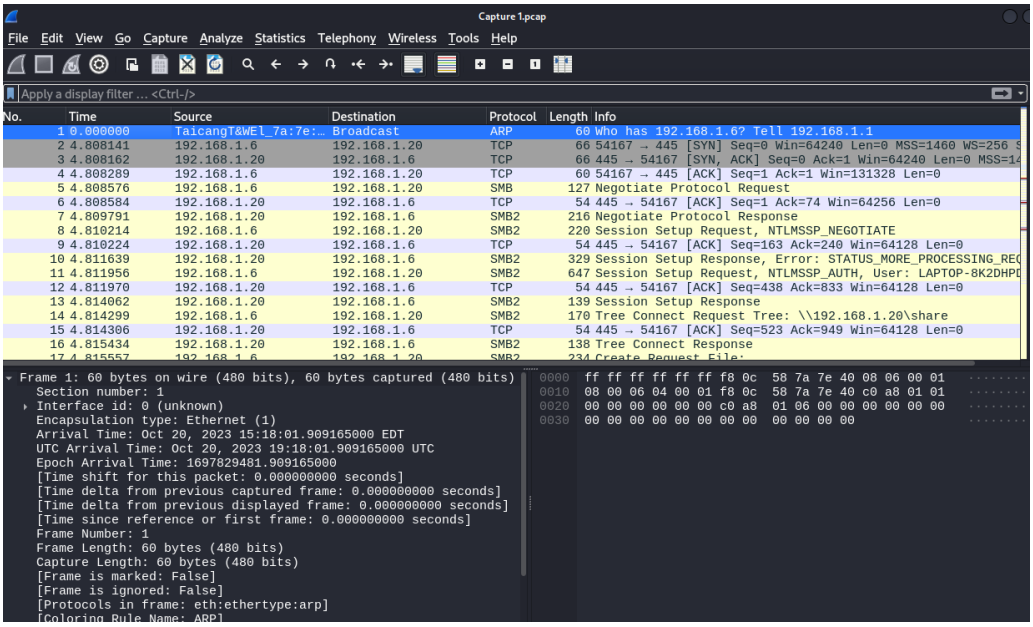

Fig 1: Screenshot of the first packet date and file sharing ports open

If any files were sent using the SMB protocol, they would be available for extraction using Wireshark's "Export Objects" tool. Using this tool, its possible to identify several files that were sent over the network using this protocol.

325	\\192.168.1.20\share	FILE (13…	1,322 bytes	\%5cSubstances\Documents\untitled folder.zip
381	\\192.168.1.20\share	FILE (24…	24 kB	\%5cSubstances\Documents\Chess Boxing\NK.jpg
443	\\192.168.1.20\share	FILE (18…	196 kB	\%5cSubstances\Documents\Chess Boxing\Rules 1..docx
548	\\192.168.1.20\share	FILE (35…	35 kB	\%5cSubstances\Documents\Chess Boxing\Rules 2.docx
610	\\192.168.1.20\share	FILE (50…	50 kB	\%5cSubstances\Documents\Chess Boxing\Rules 3.docx
672	\\192.168.1.20\share	FILE (58…	58 kB	\%5cSubstances\Documents\Chess Boxing\Rules 4.docx
746	\\192.168.1.20\share	FILE (18…	196 kB	\%5cSubstances\Documents\Chess Boxing\Rules 5.docx
858	\\192.168.1.20\share	FILE (61…	61 kB	\%5cSubstances\Documents\Chess Boxing\Rules 6.docx
921	\\192.168.1.20\share	FILE (11…	115 kB	\%5cSubstances\Documents\Chess Boxing\Rules 7.docx
1018	\\192.168.1.20\share	FILE (18…	196 kB	\%5cSubstances\Documents\Enter the WunChang\track10.docx
1116	\\192.168.1.20\share	FILE (12…	12 kB	\%5cSubstances\Documents\Enter the WunChang\track6.docx
1170	\\192.168.1.20\share	FILE (21…	21 kB	\%5cSubstances\Documents\More Documents\BillOfRights.txt
1216	\\192.168.1.20\share	FILE (42…	4,285 bytes	\%5cSubstances\Documents\More Documents\NorthKorea.jpeg
1270	\\192.168.1.20\share	FILE (74…	74 kB	\%5cSubstances\Documents\Real Doc\GoT Spoilers.docx
1337	\\192.168.1.20\share	FILE (66…	66 kB	\%5cSubstances\Documents\Real Doc\NorthKorea.docx
1409	\\192.168.1.20\share	FILE (35…	351 kB	\%5cSubstances\Documents\Real Doc\PiD.docx

Fig 2: a segment of the files identified within Capture 1

Multiple files identified in this capture were stored under a subdirectory named 'Substances' . These files were then extracted from the log as they were assumed to be significant to the primary goal of investigating this network log. Once extracted from the log file, these files could be more closely examined.

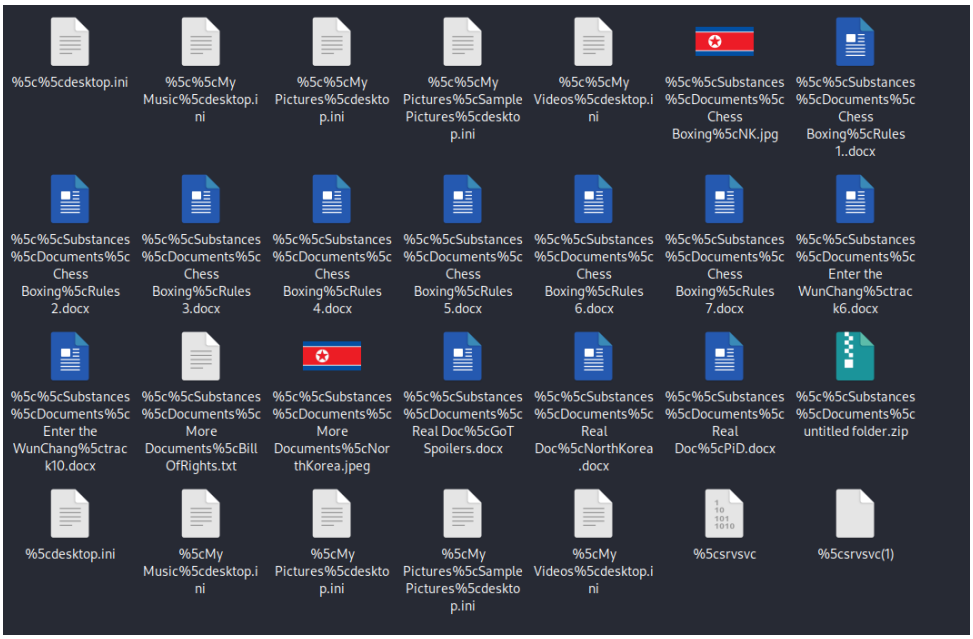

Fig 3: Extracted SMB files from capture 1

Since most of the files found were Microsoft Word documents, analysis of these files was done first. The data held within these files can be found by changing the file extension of the document to .zip, and opening the file in any archive program. Doing this and navigating to a documents 'document.xml' reveals the text and images available on the document. Multiple documents found in this extraction were found to be obfuscated using a Base64 encoding.

Fig 4: track6.docx's document.xml

Decoding the files in this extraction revealed that track6.docx contained an obfuscated list of drugs and quantities.

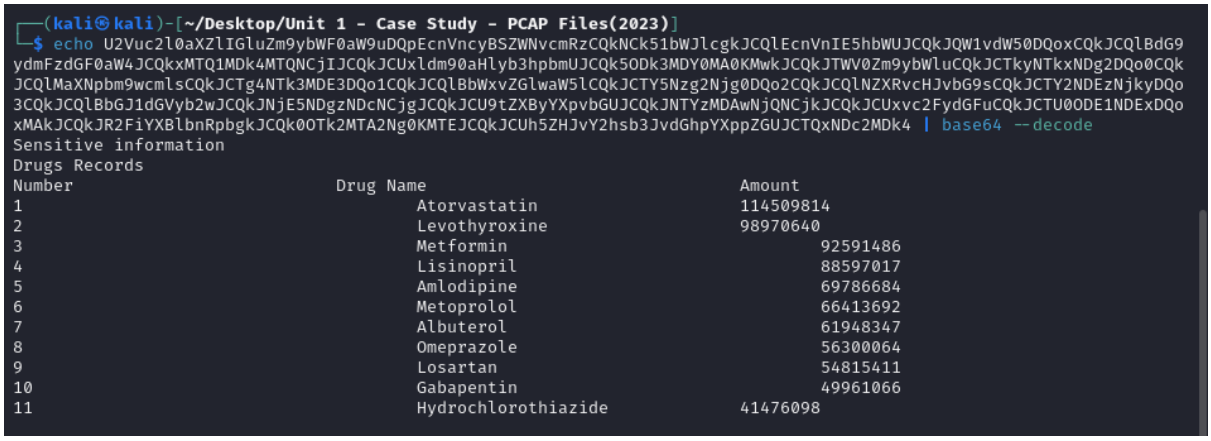

Fig 5: Decoding the string in track6.docx using base64's decode option.

2.5. Analysis

From the investigation, we can confirm that capture 1 contains an inventory of drugs with each drugs name and quantity. Further analysis of the captured file can also provide some additional information about the information found. Firstly, navigating to the files 'core.xml' can provide an author and creation time of the file. Reading this XML file reveals that the author of the file is named 'Bryan Schmidt' and the file was created on the 19th June 2014.

2.6. Documentation and Presentation

The list found within track6.docx was extracted from the files and presented as part of this document in Appendix C, and has been converted from its text format into a table to make it more readable.

3. Capture 2

3.1. Identification

Like capture 1, capture 2 is a PCAP network log provided to the investigators by the health regulatory agency. Provided with the log are instructions describing the type of evidence that needs to be extracted from this log: evidence of an item delivered to a

foreign contact through FTP that has been forensically obfuscated, using a quote from Star Wars in some way to decipher the message.

3.2. Collection

Capture 2 was collected in the same archive as capture 1 inside the Kali Linux virtual machine, and a hash was made to detect any accidental tampering from investigative tools. Opening the file in Wireshark and using the 'ftp-data' filter reveals that some archives were definitely sent over the network during the network logs capture window.

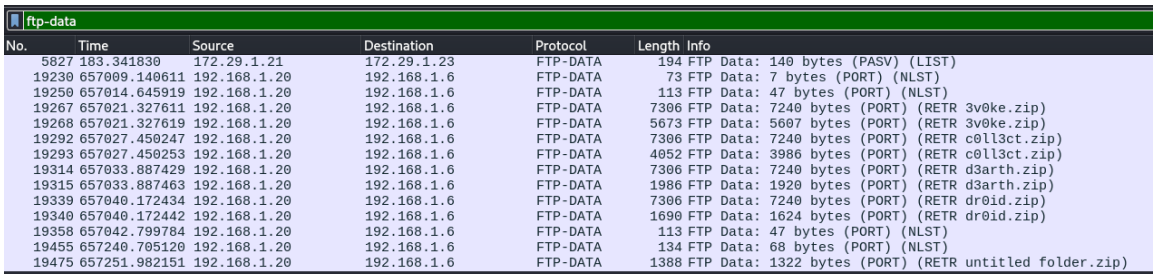

Fig 6: .zip archives sent over FTP.

3.3. Strategize

Knowing that the log contains zip files sent over FTP, it is assumed that the evidence needed from this log is contained inside these archives. To extract them, Wireshark's Extract Object tool will need to be used. Once extracted, its likely that the files will be obfuscated in some way to make it harder to decipher the message contained within. Using a hex editor like HxD will make it easier to analyse the obfuscated data and figure out a way to decode the data. Using HxD on Kali linux will require using Wine to make the tool compatible with Kali, as there is no distribution of the hex editor available natively for Linux.

3.4. Methodology

Using Wireshark's extract object tool filtered for FTP-DATA allows for each archive to be found and extracted out of the log file.

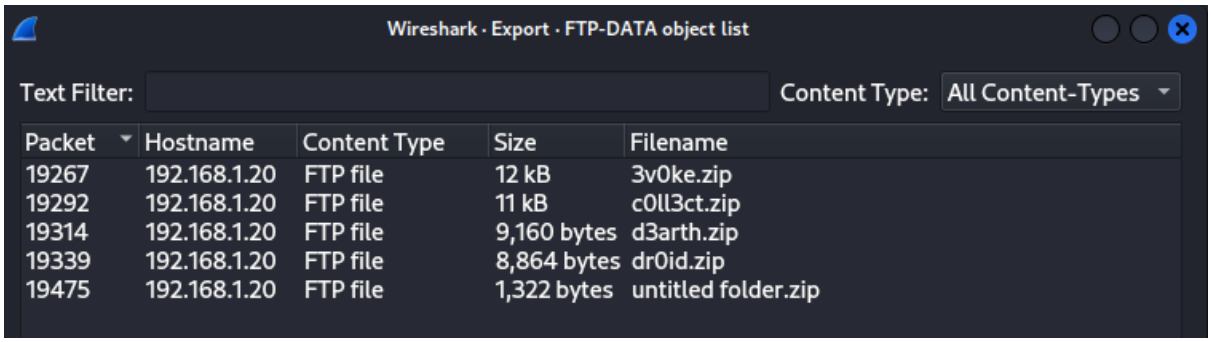

Fig 7: the archives present within the log file.

Once the archives are extracted, the inside of each archive can be viewed. Each archive contained a file named 'split' followed by a number from 1-4. Within these split files were multiple broken images, with a word or part of a word as their file name. these files were then extracted and put in the same directory.

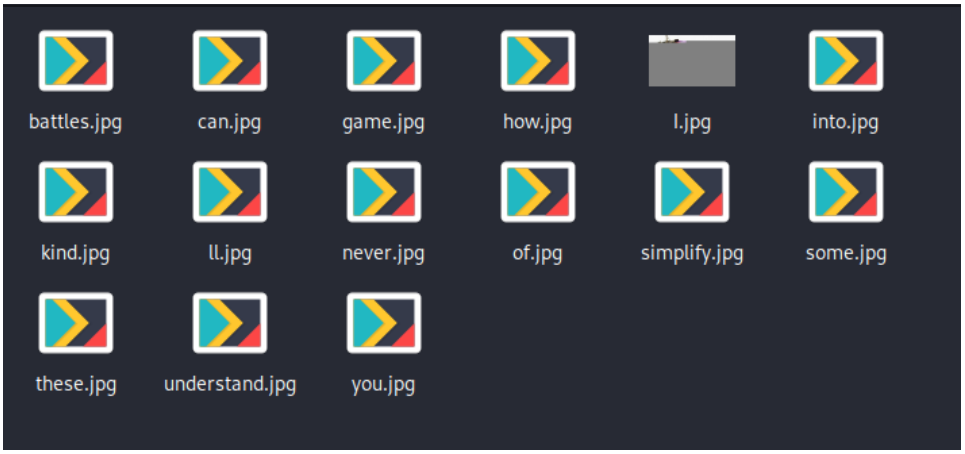

Fig 8: the segments after extraction.

Using HxD, its was possible to identify the start of the sequence for the file. Since ‘I.jpg’ is the only image in the group to contain a properly formatted header, and since the file contained the first part of an image, it can be assumed that the order of these segments begin with ‘I.jpg’. Using this information along with the additional information given with the log file, it was theorized that the order of the data correlates with a quote from season 2 of Star Wars: The Clone Wars (“I'll never understand how you can simplify these battles into some kind of game”). Assuming this, HxD can be used to concatenate each segment into a single file. Doing so in the order of the quote revealed the following image:

Fig 9: Result of combining each segment together

3.5. Analysis

Given that the output of the combined segments was sent over FTP, and used the additional information, it is likely that the toy boat is the item that has been delivered to the foreign contact. While there is some steganographic information hidden within the combined output, this information does not pertain to any items sent. What the use of steganography and the use of anti-forensic methods tell the investigation is that the members of this trafficking ring are, at the very least, aware of these forensic methods, and have the resources and expertise available to perform them.

3.6. Documentation and Presentation

While Fig 9 provides a look at the sent item. Appendix D provides the full image again for preservation purposes.

4. Capture 3

4.1. Identification

Capture 3 is another PCAP file provided with captures 1 and 2, and comes with a different set of objectives and evidence to capture. Within this log file is communication between two parties associated with the drug trafficking network, with a time and meeting place established during this communication. Finding this time and location is vital to the investigation.

4.2. Collection

Like the other log files, capture 3 was loaded into a Kali Linux virtual machine and a hash was generated to detect tampering. Opening the file with Wireshark confirmed that there was traffic data available in the log.

4.3. Strategize

Since it is unknown how the communication between parties was performed, some statistical analysis of the packets captured will be required to determine the method of communication. This is possible using Wireshark's statistics tab. Once the method of communication is established, further strategy can be established.

4.4. Methodology

Using Wireshark's protocol hierarchy tool, its possible to observe how much of the captured traffic is made up of specific protocols. Using this tool on capture 3 revealed that a significant amount of data was sent using HTTP.

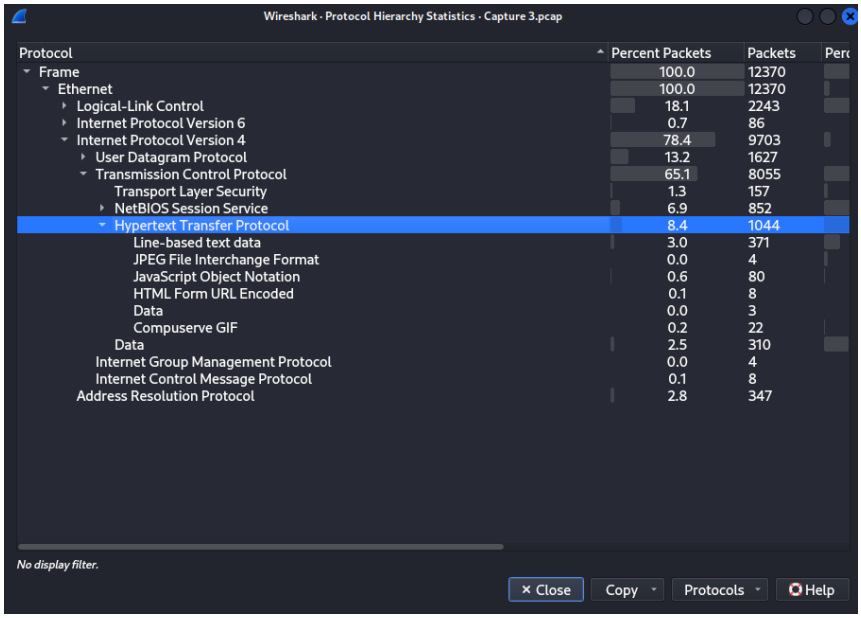

Fig 10: Statistical analysis of Capture 3

Knowing this, it was likely that the communication that contained the time and date of the meeting was made using this protocol. Filtering the log by HTTP requests revealed a string of packets being sent and received from a subdomain named /newchat/@@cht/log.html

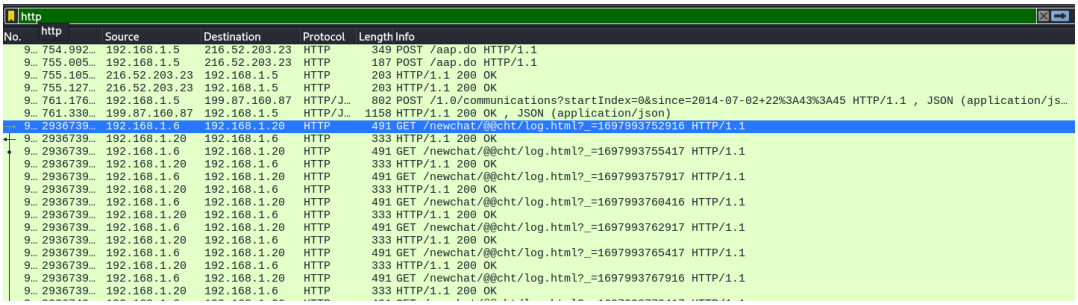

Fig 11: suspicious packets found by filtering

Using Wireshark's export object tool, its possible to extract the log.html file form the network log and view it in a web browser. Doing so reveals the following chat log:

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

Fig 12: latest version of the chat log

4.5. Analysis

The chat logs recovered from the log file indicate that the meeting place and time of the two parties is the 2nd of November 2023 at 10pm at the co-ordinates posted to the chat. These co-ordinates point to a location approximately one mile off of the CA-190 highway in Death Valley National Park, California.

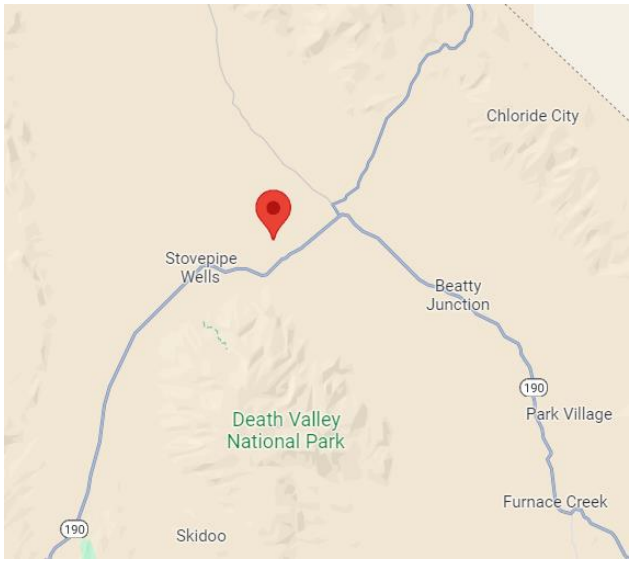

Fig 13: Location mentioned within the capture 3 log file

Looking at the other log files that are present in the capture, each return of the chat log subpage contains a string of numbers at the end of the URL. When this number is treated as a UNIX time stamp, and converted into a date and time. If these timings are reliable, this timestamp should provide the exact time that these messages were sent, spanning from exactly 16:56:42 UTC, when El Chapo joins the chat, to 16:55:59 UTC,

when the co-ordinates are sent. The arrival time of these messages in the chat logs, however, are four hours behind the arrival time stated in the Wireshark logs and the chat logs. This implies that the recipient of these logs is within a time zone that is behind UTC, and given the location sent in the chat it is likely that the recipient of this chat is in California.

Using this chat log, it is also possible to ascertain the IP address of 'Narco Polo'. Within the chat log, post requests to the server can be seen being made that contain text that corresponds to chat messages made by Narco Polo within the chat logs. This implies that the local IP address of Narco Polo is 192.168.1.6, as his messages are being send from this local network IP address. Whether this means that Narco Polo is identifiable in other captures is not verifiable however, as Narco Polo has not been identified in any of the other network logs.

4.5.1. Inconsistencies in capture timing

Analysing the times in capture 3 return some inconsistencies in timing from the chat logs versus the servers. The servers time that it returns along with the log.html file is further ahead in time versus the time that is saved with the packets in the metadata of the log file by about 10 minutes

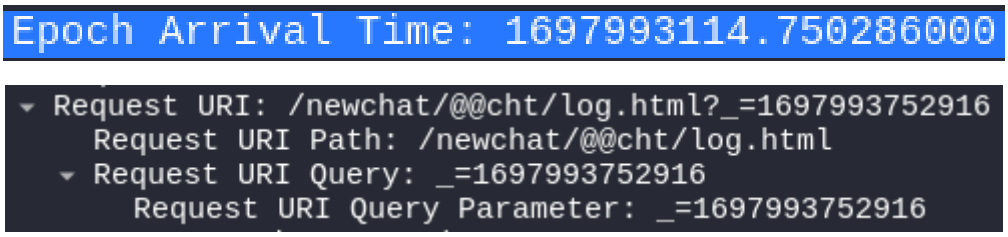

Fig 13: Epoch Arrival time of the packet (Above) versus the value returned from the chat server (Below)

Since the numbers are very similar, it is still likely that the value returned from the chat server is still a UNIX timestamp. However, the fact that the timings are so far apart raises some suspicion that either one may be incorrect.

Another suspicious inconsistency is found earlier in the capture file, where the timestamp of the packets changes dramatically between two packets. Frame 9919 in capture 3 is dated to have been captured on July 2nd 2014, whereas the next frame (coincidentally the first time the chat log is accessed) is captured a whole 9 years later on October 22nd 2023. While it is not completely impossible that no packets were sent within this time frame, it is extremely unlikely that this was the case. This time difference further raises suspicion in relation the validity of capture 3 as forensically sound evidence.

All of these inconsistencies found within capture 3 raises the suspicion that capture 3 has been modified prior to reaching the hands of investigators. While the evidence gathered during the investigation of capture 3 will be presented and documented alongside other evidence, it should be duly noted that these timing differences question the validity of the digital evidence.

4.6. Documentation and Presentation

The chat logs found within capture 3 have been converted into a more readable format and attached as part of this document to Appendix B. This table uses the time stamps available as part of the servers logs, and may be different from the time stamps available to the network log.

5. Timeline

Developing a timeline of events for the combined incidents is imperative to developing an idea of when each incident occurred, who the parties of each incident were, and how these incidents were carried out. Using the timestamps in each log file an exact timeline of events can be carried out. For consistency with other sections of the report, all timestamps used in this section are converted to UTC.

5.1. Capture 1 (Oct 20, 2023 19:18:01 - Oct 22, 2023 05:23:52)

Oct 20, 2023 19:18:06 – 192.168.1.6 begins to establish a SMB connection to 192.168.1.20

19:18:06 – 192.168.1.20 returns a STATUS_SUCCESS indicating the two machines have established communication

19:18:06 – 192.168.1.6 views the files located in 192.168.1.20/share

19:18:20 – 192.168.1.6 starts requesting files from 192.168.1.20

19:18:22 – 192.168.1.6 requests to read the file track6.docx, which contains the inventory of drugs. This file's data is transferred from 192.168.1.20 to 192.168.1.6.

19:18:36 – 192.168.1.6 disconnects from the SMB connection, which is acknowledged by 191.168.1.20

19:18:36 to Oct 22, 2023 05:23:52 – no data of relevance to the investigation is sent

5.2. Capture 2 (Oct 14, 2023 05:33:35 - Oct 21, 2023 20:08:03)

Oct 14, 2023 05:33:35 to Oct 21, 2023 20:02:42 – Nothing related to the investigation is sent.

Oct 21, 2023 20:03:20 – 192.168.1.6 establishes an FTP connection with 192.168.1.20, using the username 'ftpuser' and the password 'starwars'.

20:03:56 – 192.168.1.6 requests and receives the first segments of the image, contained in '3v0ke.zip'

20:03:56 to 20:04:15 – 192.168.1.6 requests and receives the other segments of the image, contained in 'c0ll3ct.zip', 'd3arth.zip', and 'dr0id.zip'.

20:04:21 – 192.168.1.6 requests to disconnect from the FTP connection, which is acknowledged by 192.168.1.20. No further information related to the investigation is contained in the capture.

5.3. Capture 3 (Jul 2, 2014 16:38:50 - Oct 22, 2023 16:56:49)

(Due to inconsistencies in the timings of the capture file, the exact times for this capture are unverifiable. For this timeline, the packet metadata has been used instead of the timestamp found during investigation)

Jul 2, 2014 16:38:50 to Oct 22, 2023 16:45:14 – no evidence relating to the investigation is found.

Oct 22, 2023 16:45:14 – 192.168.1.6 requests the chat page for the first time

16:46:27 – 192.168.1.6 sends their first message to the chat. In the chat logs they are identified as ‘El Chapo’

16:47:45 – 192.168.1.6 receives the message from ‘Narco Polo’ to meet on the 2nd of November at 10pm

16:54:16 – 192.168.1.6 receives the co-ordinates pointing to Death Valley National Park.

12:56:04 – 192.168.1.6 stops communicating with the chat server.

12:56:04 to 16:56:49 – no packets of relation to the investigation are sent.

6. Evaluation

Maintaining the forensic validity of the evidence procured is vital to the success of the overall investigation. Over the course of the investigation, heavy consideration was made to ensure that the evidence provided to investigators was kept exactly the way it was given, in order to prevent the tampering of evidence. As stated in the methodology of each capture, hashes were made of each capture file before investigation began. Doing this allowed investigators to routinely check the captures hash and, if any modification of the file had taken place, be able to identify the exact moment that a forensic method has accidentally tampered with evidence. Doing this allows investigators to maintain the validity of the evidence, as a lack of change in the hash of each file confirms that there has been no modification to the initial evidence. The hashes of each capture file before and after investigation are available in Appendix A, and their lack of change verifies the validity of the evidence.

Providing a replicable method of evidence extraction also provides forensic validity to the evidence obtained during the course of the investigation. Each step of the process required to obtain the evidence from the capture files has been thoroughly documented, providing an easy way to recreate the exact method used to capture the required evidence for this investigation.

Maintaining forensic validity throughout the investigation adds credibility to the evidence found while investigating, and allows investigators to safely confirm that their methods have been performed in a forensically sound manner.

For the majority of the investigation methodology, Wireshark has been a key tool in identifying the critical evidence needed to complete this investigation. Wireshark’s ability to collate and extract data that can be used as evidence from the log files makes it significantly easier to analyse and verify evidence that might be harder to extract manually. Although, due to its significant use in this investigation, it is important to evaluate whether Wireshark’s functionality is forensically minded enough for investigation, otherwise the majority of evidence may be put into question.

Wireshark’s capabilities as a forensic tool can be verified by any capable developer, as the network analysers code is completely open source and viewable by anyone. This open source ethos allows the tool to maintain a strong level of information security, as a community of developers can verify exactly how each aspect of the tool works. Where

Wireshark also maintains strong functionality in forensic investigation is in its ability to capture a vast amount of data about each packet recorded, specifically its ability to provide timestamps for each and every packet within its logs. This timestamping makes it easy for forensic investigators to develop a timeline of events, as they are able to easily identify exactly when each event in the network took place. Due to both its forensic functionality, and its ability to be easily evaluated by independent parties, it is safe to consider the evidence gathered using Wireshark as forensically verifiable.

Using HxD within a Kali Linux virtual machine provided some challenges to investigation that were unforeseen at the start of investigating. While HxD is a powerful hex editor with a variety of functions, it is unavailable for GNU/Linux distributions such as Kali. Finding a way to use this tool on such a platform became a reasonable problem to solve, as the functionality of HxD would greatly improve the analysis of evidence found within the capture logs. Using a compatibility layer such as Wine would allow for the use of HxD in Linux, and so the investigative team used Wine as part of the investigation to facilitate the use of HxD as a hex editor and file concatenator. However, use of this compatibility layer may raise concerns regarding the forensic validity of HxD as a forensic tool. To test this, copies of the evidence had a hash generated and were then accessed by HxD. once access had finished, another hash was generated to compare against the original, which would show a change in hash if the evidence had been affected by HxD. Doing this returned no change in the hash, and thus confirms that the use of HxD in Kali using Wine does not tamper the evidence.

The behaviour and methods employed by the drug trafficking ring were intentionally performed to impede investigation and prevent detection by other parties. This can be seen most clearly in capture 2, where the methods performed on the message found converted a viewable file into a segmented list of unreadable binary files. Combined with a reasonably esoteric method to recombine the file, this obfuscation of data is clearly designed to prevent outside parties from viewing the messages. The trafficking ring also makes ample use of Base64 encoding as seen in capture 1. This encoding this easy to decode using basic tools, and can even be done online. While being a fairly insecure way to obfuscate data, it is still able to completely convert plain text into an unreadable mess, making it unreadable to a layman with no knowledge of computing or security.

The obfuscation methods used by the drug trafficking ring, however, are unlikely to be difficult to decipher for even entry level forensic investigators. Firstly, a considerable lack of secure obfuscation has been used in every capture. In capture 1, the most basic form of obfuscation is used to encode the files on the SMB share. In capture 2, the zip files each segment is contained in requires no password to open, which is a function that is readily available in most archive creation tools. Capture 2 also contains evidence of a insecure FTP server, for which login credentials were easily obtained due to the protocols lack of security. Capture 3 showed that the users of the chat room were accessing the chat using unsecured HTML, allowing for investigators to easily view what they were saying through the log.

The severe lack of security within every aspect of the technology used by the drug trafficking ring imply that the organization is either unaware or unable to perform the most basic forms of cyber security, and continue to indict themselves with every criminal act recorded.

7. Conclusion

Despite suspicions of capture 3's validity, all captures provided contain clear digital evidence of suspected drug trafficking. The analysis of each capture file indicate that the ring is highly organized but lacking in computer security. The capture files provided seem to also contain a wide variety of other data captured about the drug ring, which could provide further information about the ring if a wider scope and increased time was given to their investigation.

8. Additional Data

Appendix A: MD5 hashes of evidence

Log File	Hash Before	Hash After	Change
Capture 1.pcap	9e13d6c7c5920007240eeb80f9c1f47e	9e13d6c7c5920007240eeb80f9c1f47e	No Change
Capture 2.pcap	cc211ce173f3b928b11e5f256f448788	cc211ce173f3b928b11e5f256f448788	No Change
Capture 3.pcap	cec76ac8f5e6bae30a27b1671fffbc11	cec76ac8f5e6bae30a27b1671fffbc11	No Change

Appendix B: Chat logs using provided timestamp

Time	User	Message
N/A	El Chapo	*User El Chapo has joined the chat.*
N/A	Narco Polo	*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

Appendix C: Drug list obtained in Capture 1

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

Appendix D: Combined result of output