Network Forensics

Investigation Report

Nick Nesterenko

CMP416: Advanced Digital Forensics: Coursework 2

BSc (Hons) Ethical Hacking, Year 4

2022/23

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

+Contents

1 Introduction

1.1 The Aim of the Investigation

It was instructed by the National Security Agency (NSA) to perform a forensic network investigation of the three provided network capture files the agency exfiltrated from parties of interest. The aim of the investigation was to recover requested evidence which would support the international sporting competition corruption case. It also needed to demonstrate the network forensic process and critical evaluation of the tools used in accordance with the chosen methodology for each capture file.

1.2 Overview of the Methodology

For the purposes of this investigation, it was decided to use *OSCAR* methodology. This methodology was as it is an industry standard and tested methodology developed to use during *Network Forensics* which was relevant to the current investigation (Jaswal, 2019). This methodology is also often used by the European Union Agency of Cybersecurity (ENISA) which proves its credibility and effectiveness which would be beneficial for the current corruption case investigation (ENISA, 2022). The five steps of OSCAR methodology are as follows:

1. **O** – Obtain information. Learn about the incident and targeted environments.
2. **S** – Strategize. Plan the investigation based on information gathered.
3. **C** – Collect. Acquire the evidence as per plan.
4. **A** – Analyse. Analyse acquired evidence using different techniques eliminating false positives.
5. **R** – Report. Produce the investigation, must be in layman's terms.

This methodology was used during the investigation and each step mentioned can be found in detail in Section 2 of this report.

2 METHODOLOGY AND FINDINGS

2.1 OBTAIN INFORMATION

The first step of the investigation was to outline currently obtained information. In this investigation, only the case brief and some information about the three provided network capture files were provided.

2.1.1 What happened?

The National Security Agency has enlisted the services of a network forensics investigator to analyse three provided network captures obtained from parties of interest in an international sporting competition corruption case. The timeframe of the event was not communicated, neither the dates of the investigation. The threat actors were also unknown at this stage as it was one of the primary goals of this investigation.

2.1.2 Provided information and potential evidence sources

Three different network capture files were provided. The first capture contains files related to suspected bribery, and it was required recover details about the usernames and how they were hidden. Details of other discovered files are of no interest to this investigation.

The second capture contains FTP and other traffic between the suspected corrupt official and a foreign national, the investigator must decode the traffic and provide evidence of the exchanged item. It was provided that there were suspicions about anti-forensic practices being in used in this capture file.

The third capture contains communication traffic between two individuals, it was needed to uncover the details of their conversation and the planned discrete meeting time and date. Two names were suggested, Ill-Song as well as the Ann Dercover, a known person who was taking part in the international competition.

2.1.3 Additional interesting information

The National Security Agency was “tipped” some interesting information regarding the one capture file which was flagged as critical for this investigation. The second capture file contained obscured data and “an Edward Snowden quote” could help the process of deciphering.

2.2 STRATEGIZE

The second stage of the investigation was planning which included outline of the goals and objectives, data preservation measures and the overview of potential challenges which would help progress during the “Collect” stage.

2.2.1 Identifying the goals of the forensic investigation

As there were three capture files provided, it was essential to provide goals and objectives for each one of them as well as additional objectives in accordance with the previously obtained information from the NSA.

Goals:

- Identify details of the usernames and how they were hidden in Capture 1.pcap.
- Decode the traffic and provide evidence of the item exchanged in Capture 2.pcap.
- Uncover the details of the conversation and planned meeting time and date in Capture 3.pcap.

Additional Objectives:

- Make sure the methodology is forensically sound and suits the investigation.
- Describe the tools and techniques used to recover evidence.
- Provide analysis of the network data (Who? When? How?) to establish context and validate evidence.
- Provide critical evaluation of the challenges faced during the investigation and how they were overcome.
- Suggest how malicious hacking behavior can impede an investigation.

2.2.2 Data preservation and chain of custody summary

The provided network captures were copied locally, and the original files were moved to an external drive for the investigation to ensure data preservation. Any recovered evidence will be stored in two different places and verified with MD5 hashes to ensure its integrity. The chain of custody for the files will be established and documented by the NSA to maintain the integrity of the evidence but will not be detailed in this report.

2.2.3 Overview of potential challenges

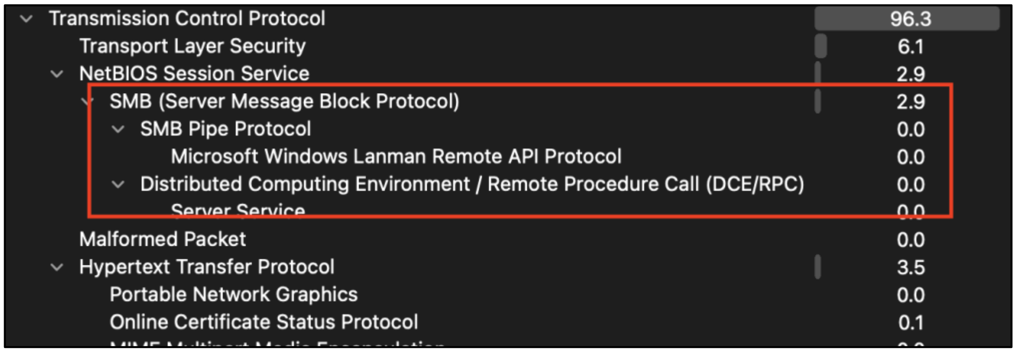
Based on the information provided, there could be some potential challenges encountered during the investigation, some of them include:

- Lack of details about the case.
- Limited knowledge about the network capture files.
- Suspected use of anti-forensic practices.
- The need to recover hidden details.
- Limited time and resources.
- Potential for contamination or alteration of the evidence.

2.3 Collect and Analyse

Considering the information gathered in previous steps it was decided to figure the initial steps for each capture which would assist progressing through the investigation. During this stage, the tools and techniques would be described. Note: any other evidence except for the goals of the investig

Firstly, it was needed to determine the protocol used for downloading files in the first capture file which posed a challenge as the related intel was not provided. A packet analysis tool called Wireshark was used to overcome that. Wireshark provided a graphical user interface for examining network traffic and advanced filtering capabilities. It was decided to use statistic flow analysis techniques using Wireshark's Protocol Hierarchy, which revealed the presence of the Server Message Block (SMB) protocol. This indicated that the files could have been transferred using SMB during the download, as it is commonly used for file sharing and other network services in Windows-based environments (Figure 1):



```
⌄ Transmission Control Protocol                                          96.3
      Transport Layer Security                                            6.1
  ⌄ NetBIOS Session Service                                               2.9
    ⌄ SMB (Server Message Block Protocol)                                 2.9
      ⌄ SMB Pipe Protocol                                                 0.0
            Microsoft Windows Lanman Remote API Protocol                  0.0
      ⌄ Distributed Computing Environment / Remote Procedure Call (DCE/RPC) 0.0
            Server Service                                                0.0
      Malformed Packet                                                    0.0
  ⌄ Hypertext Transfer Protocol                                           3.5
        Portable Network Graphics                                         0.0
        Online Certificate Status Protocol                                0.1
        MIME Multipart Media Encapsulation
```

Figure 1: Using Wireshak's Protocol Hierarchy with Capture 1.pcap

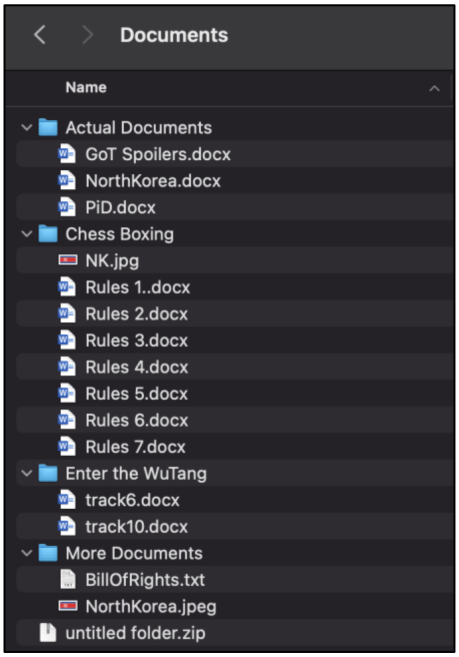
The use of SMB protocol suggested the first entry vector for evidence retrieval, so it was decided to focus on recovering data from the first capture file. The .pcap was filtered for SMB packets using Wireshark to see if there were any files transmitted via SMB that could contain usernames which could be used throughout the investigation.

The filtered network data revealed that some of the files were transferred using the SMB protocol on July 11th, 2014, between 21:22:08 to 21:22:55, the timing also matched the expected for SMB. Hosts 172.29.1.23 and 172.29.1.20 were identified as FOX-WS and DOG-WS, respectively. FOX-WS established a connection to DOG-WS's IPC share and browsed the available shares. Then, \DOG-WS\DOCUMENTS share and \DOG-WS\BLAH share were accessed, eventually leading to the download of the file Documents.zip.

Using this information, Wireshark was used to extract the files transferred using the Export SMB functionality in Wireshark which confirmed the presence of Documents.zip, the file was exported and stored securely in two different places and the hash of the file was:

7acb8f883a9a943131f8e60d5646725f

After unarchiving the recovered file, several directories and files were discovered, mostly Microsoft Word files. After inspecting the filenames and contents of the files, two patterns were observed. The first being that the contents of the Word files were scrambled in some way, which was considered an attempt to obscure valuable data. Second, the recovered files included a directory named "Chess Boxing" (Figure 2), suggesting a possible connection to Chess or Boxing. In order to decipher the text in the .docx files, CyberChef was used with its Magic function to successfully decode the encrypted data.



Documents

Name

- Actual Documents
  - GoT Spoilers.docx
  - NorthKorea.docx
  - PiD.docx
- Chess Boxing
  - NK.jpg
  - Rules 1..docx
  - Rules 2.docx
  - Rules 3.docx
  - Rules 4.docx
  - Rules 5.docx
  - Rules 6.docx
  - Rules 7.docx
- Enter the WuTang
  - track6.docx
  - track10.docx
- More Documents
  - BillOfRights.txt
  - NorthKorea.jpeg
- untitled folder.zip

Figure 2: Contents of the Documents.zip

After examining the encoded text, the information containing usernames was located in the "Enter the WuTang" directory, in the track6.docx file. The list of usernames contained a list of names, some of which were names of the WuTang Clan, which is a hip hop group from *Staten Island, New York*, as well as some other names which stood out, not only by the name, but by the format too. The title of the document also referred to the Chess Boxing, which elevated its significance.

- Mr. Method
- Kim Ill-Song
- Mr. Razor
- Mr. Genius
- Mr. G. Killah
- Matt Cassel
- Mr. I. Deck
- Mr. M Killa
- Mr. O.D.B.
- Mr. Raekwon
- Mr. U-God
- Mr. Cappadonna (possibly)
- John Woo?
- Mr. Nas

Green names suggest difference in format and Red names suggest people who weren't part of the WuTang Clan.

The next step was to find entry vectors for evidence gathering in the second capture. As mentioned by the brief, the suspects were using File Transfer Protocol (FTP). To validate this, Protocol Hierarchy was used in Wireshark for statistic flow analysis which proved that the FTP was used and outlined presence of the FTP-DATA. The timeline of this incident was on July 2nd, 2014 from 17:38:50 to 17:52:32.

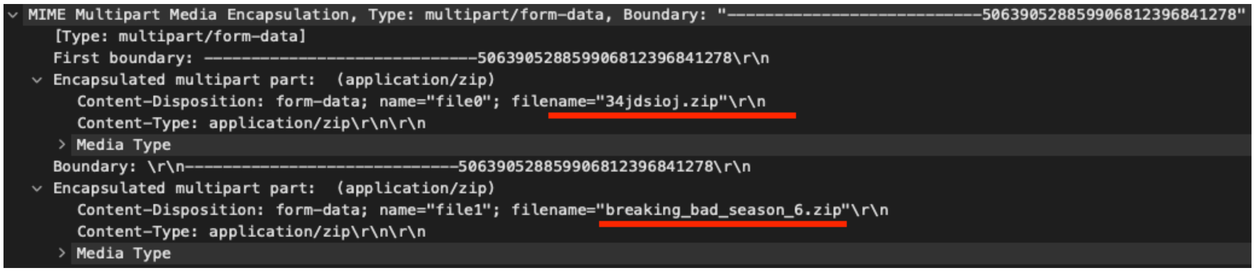
The FTP-DATA protocol was examined because it is often used for transferring the actual data of files over a network. By examining the FTP-DATA protocol, it was possible to locate the first details of the exchanged files. The packet data suggested an exchange of two archives named **sandofwhich.zip** and **ojd34.zip**. Using Wireshark's "Follow TCP Stream", the two archives were retrieved by saving the TCP steams 158 and 159 as raw data and adding the .zip extension to the created file.

Unarchiving the data revealed a set of corrupted images with interesting single-worded names. At the beginning, it was decided to check for any hidden steganography using binwalk tool data as the brief suggested anti-forensic practices. *binwalk* is a tool commonly used to find hidden data in files, however in this case it did not give any results.

Some of the file names included freedom.jpg and web-based.jpg, which suggested some correlation to the earlier mention Snowden's quote. By analysing those patterns, it was decided to attempt to rearrange the files into a quote. To find clues on the exact quote, google was used by searching for all the words detailed in the file names. The google search revealed a few quotes but one of them appeared to be the most common:

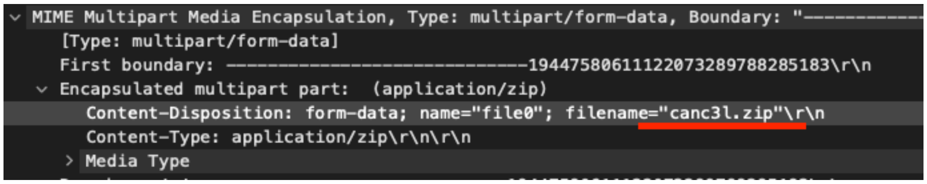
> "*I'm willing to sacrifice all of that because I can't in good conscience allow the US government to destroy privacy, internet freedom and basic liberties for people around the world with this massive surveillance machine they're secretly building.*" (The Guardian, 2013)

Although the quote seemed to match, it was clear that the data of the retrieved archives were not enough to complete the quote, therefore it was required to find additional information. At this stage it was clear that there was a pattern in using .zip archives while exchanging files, therefore the packets were filtered with keyword "zip" in the packet list which revealed two additional post requests at packets 2666 and 8190 revealed 3 additional zip archives using the packet details in the MIME protocol which is an extension to the SMTP and used for mailing (Figure 3 and 4):



```
⌄ MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "---------------------------50639052885990681239684127 8"
    [Type: multipart/form-data]
    First boundary: -----------------------------506390528859906812396841278\r\n
  ⌄ Encapsulated multipart part:  (application/zip)
      Content-Disposition: form-data; name="file0"; filename="34jdsioj.zip"\r\n
      Content-Type: application/zip\r\n\r\n
    › Media Type
    Boundary: \r\n-----------------------------506390528859906812396841278\r\n
  ⌄ Encapsulated multipart part:  (application/zip)
      Content-Disposition: form-data; name="file1"; filename="breaking_bad_season_6.zip"\r\n
      Content-Type: application/zip\r\n\r\n
    › Media Type
```

Figure 3: Packet 2666 details revealing two .zip files

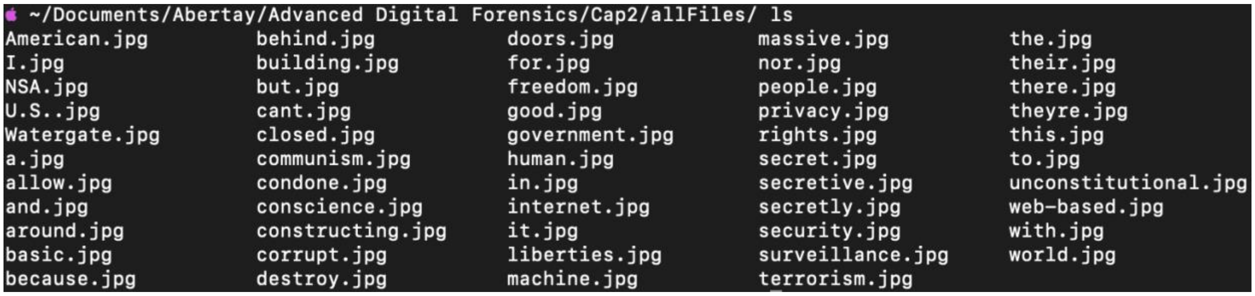


```
⌄ MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "-----------
    [Type: multipart/form-data]
    First boundary: ---------------------------194475806111220732897882851 83\r\n
  ⌄ Encapsulated multipart part:  (application/zip)
      Content-Disposition: form-data; name="file0"; filename="canc3l.zip"\r\n
      Content-Type: application/zip\r\n\r\n
    › Media Type
```

Figure 4: Packet 8190 details revealing one .zip file

Following the TCP steams revealed that packets 2666 and 8190 are part of the same TCP stream 42. This suggested that in order to recover the files, it would require to use file carving technique. The TCP steam was then exported as HEX and opened to using the HxD hex editor.

Using the magic number of .zip files (50 4B 03 04), the beginning of the three archives were located and using the header "Content-Disposition", beginning of which represented the End Of File. The three archives were saved with the .zip file extension which allowed to retrieve the missing files. All the files from the five archives were then put into one folder for rearranging using *cat* command (Figure 5):



```
 ~/Documents/Abertay/Advanced Digital Forensics/Cap2/allFiles/ ls
American.jpg         behind.jpg           doors.jpg            massive.jpg          the.jpg
I.jpg                building.jpg         for.jpg              nor.jpg              their.jpg
NSA.jpg              but.jpg              freedom.jpg          people.jpg           there.jpg
U.S..jpg             cant.jpg             good.jpg             privacy.jpg          theyre.jpg
Watergate.jpg        closed.jpg           government.jpg       rights.jpg           this.jpg
a.jpg                communism.jpg        human.jpg            secret.jpg           to.jpg
allow.jpg            condone.jpg          in.jpg               secretive.jpg        unconstitutional.jpg
and.jpg              conscience.jpg       internet.jpg         secretly.jpg         web-based.jpg
around.jpg           constructing.jpg     it.jpg               security.jpg         with.jpg
basic.jpg            corrupt.jpg          liberties.jpg        surveillance.jpg     world.jpg
because.jpg          destroy.jpg          machine.jpg          terrorism.jpg
```

Figure 5: List of all corrupted .jpeg files

Finally, the images were rearranged using the previously mentioned quote and put into one image file which revealed an image of luxurious chess board, previously mentioned "Chess Boxing" started to shape its relevance to the case (Figure 6):

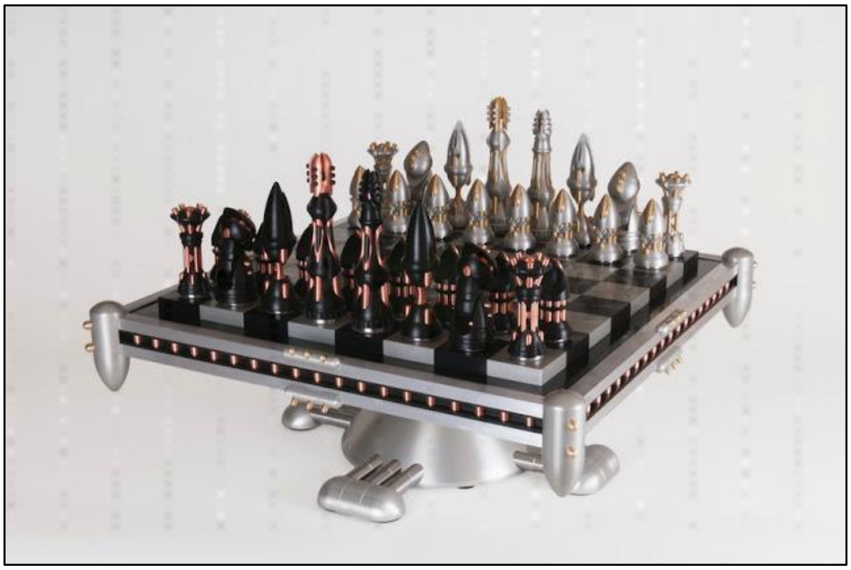


Figure 6: Combined image

Finally, the last capture file was analysed. It was provided in the brief that there is a conversation that involved two names, Ill-Song and Ann Dercover. Using statistic flow analysis and Wireshark's Protocol Hierarchy feature, it was discovered that there were .json files transferred using HTTP protocol. Based on this intel, the packets were filtered to HTTP and it was looked for the keywords "application/json" and "Ill-Song" in the packet list. This revelled the conversation. Packet details also suggested some interesting information such as email addresses of the two and ZIP code of Ann which was US **59801**.

The details of the packets were analysed and put into a table using Microsoft Excel manually:

ID	Time and Date	Sender	Message text
1	02/07/2014 17:39:43	Kim Ill-song	Good afternoon Ann
2	02/07/2014 17:39:53	Ann	Who is this?
3	02/07/2014 17:40:19	Kim Ill-song	Castling
4	02/07/2014 17:40:24	Ann	Where are you?
5	02/07/2014 17:40:52	Kim Ill-song	I know I can't tell you that
6	02/07/2014 17:42:03	Ann	Do you know that there are people investigating Kim Ill-Song?
7	02/07/2014 17:42:31	Kim Ill-song	Of course. However they will never know that it is me behind the bribes.
8	02/07/2014 17:43:33	Ann	Still we should be careful. Pay attention. I want to meet in September at 5pm.
9	02/07/2014 17:43:49	Kim Ill-song	At our old meetup spot?
10	02/07/2014 17:44:06	Ann	Yes
11	02/07/2014 17:44:29	Kim Ill-song	What day?
12	02/07/2014 17:51:10	Ann	I told you to pay attention

The date of the meeting was missing therefore the additional information was required to be located, it was noticed that after the end of the conversation, geolocation pins were exchanged using *mob.mapquestapi.com*, all those files were extracted using Wireshark and the coordinated were filtered using Excel and put into a .csv file which was then converted online into .klm file which was then used against google earth which showed a number made up of the geolocation pins (Figure 7):

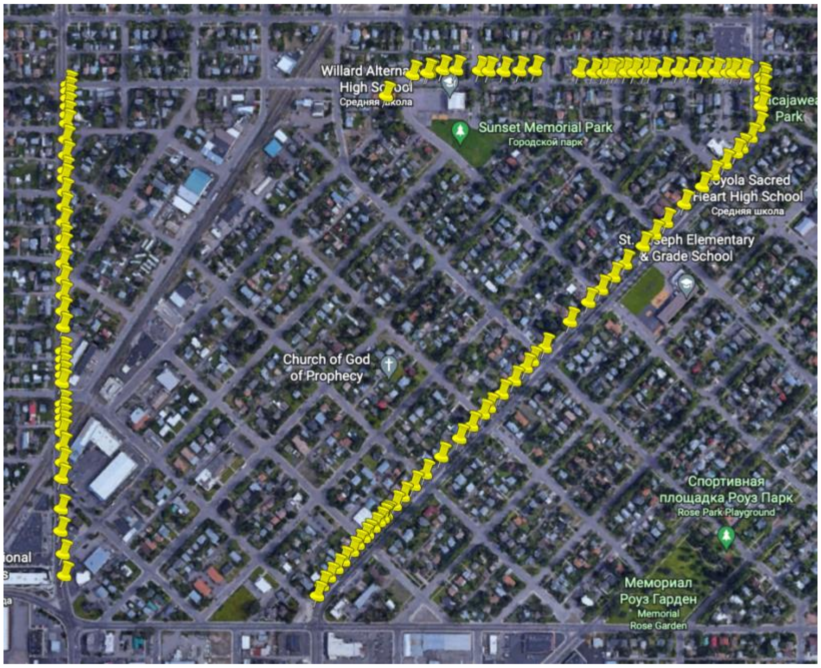


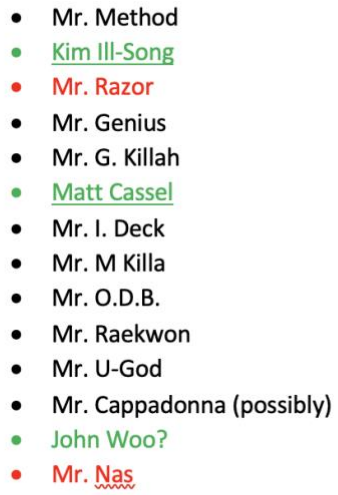
Figure 7: geolocation pins

The final date of the meeting was 17th of September, 5pm, location unknown.

2.4 REPORT

The report stage of this investigation was out of the scope as NSA would pass the evidence to the authorities combined with other information gathered outside of this network forensics investigation, however it was decided to summarise the findings.

Capture 1.pcap revealed the usernames of “The Mystery of Chess Boxing”:



- Mr. Method
- Kim Ill-Song
- Mr. Razor
- Mr. Genius
- Mr. G. Killah
- Matt Cassel
- Mr. I. Deck
- Mr. M Killa
- Mr. O.D.B.
- Mr. Raekwon
- Mr. U-God
- Mr. Cappadonna (possibly)
- John Woo?
- Mr. Nas

Figure 8: Key evidence 1, list of usernames

Capture 2.pcap revealed exchanged item during the bribery, which was the fancy chess set:

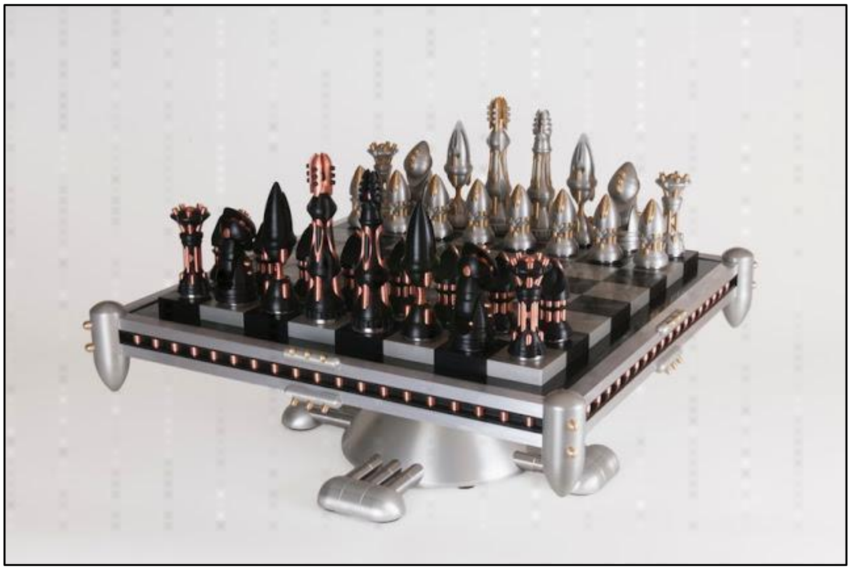


Figure 9: Key evidence, exchanged item

Finally, Capture 3.pcap revealed the details of the conversation of Ill-Son, which based on the conversation may have been Matt Cassel and Ann Dercover, the final time and date of the meeting was 17th of September, 5pm:

Table 1: Key evidence 3, the conversation

ID	Time and Date	Sender	Message text
1	02/07/2014 17:39:43	Kim Ill-song	Good afternoon Ann
2	02/07/2014 17:39:53	Ann	Who is this?
3	02/07/2014 17:40:19	Kim Ill-song	Castling
4	02/07/2014 17:40:24	Ann	Where are you?
5	02/07/2014 17:40:52	Kim Ill-song	I know I can’t tell you that
6	02/07/2014 17:42:03	Ann	Do you know that there are people investigating Kim Ill-Song?
7	02/07/2014 17:42:31	Kim Ill-song	Of course. However they will never know that it is me behind the bribes.
8	02/07/2014 17:43:33	Ann	Still we should be careful. Pay attention. I want to meet in September at 5pm.
9	02/07/2014 17:43:49	Kim Ill-song	At our old meetup spot?
10	02/07/2014 17:44:06	Ann	Yes
11	02/07/2014 17:44:29	Kim Ill-song	What day?
12	02/07/2014 17:51:10	Ann	I told you to pay attention

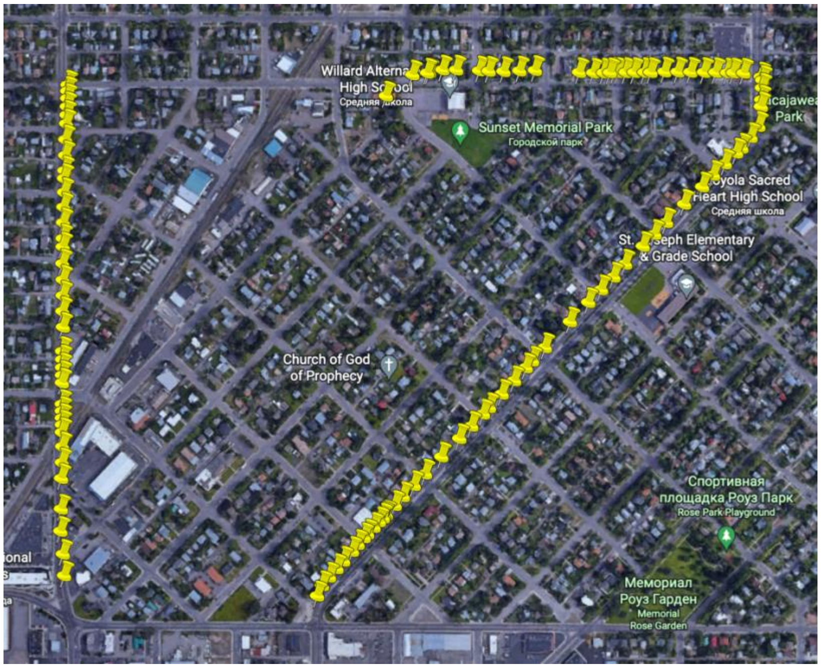


Figure 10: Key evidence 4, the date

3 CRITICAL EVALUATION AND DISCUSSION

3.1 CRITICAL EVALUATION

There were several parts of the investigation which involved anti-forensic measures which lead the investigation to a wrong direction. The challenges were overcome using standardise techniques alongside the OSCAR methodology. The data stored in the packets also helped the investigation progress which made it possible to locate all key evidence requested by the NSA. Overall, there could be several bribers in this investigation and to have a better understanding, it is required to obtain additional information.

In conclusion, the forensic network investigation of the three provided network capture files was successful in achieving its goals. The chosen methodology, OSCAR, proved to be effective in uncovering the evidence needed to support the international sporting competition corruption case. The recovered evidence, along with the detailed investigation report, can be used to further the case and bring the perpetrators to justice.

3.2 FURTHER DISCUSSION

The behavior of a malicious hacker can impede an investigation in a number of ways. For example, the misuse of protocols can make it difficult for investigators to identify and track the hacker's activities. Data obscuring techniques, such as encryption and steganography, can make it difficult or impossible to extract useful evidence from captured network traffic. Additionally, the use of anti-forensic tools and practices can destroy or alter evidence, making it difficult or impossible to accurately reconstruct the events of an attack.

REFERENCES

Jaswal, N. (2019) Hands-on network forensics: investigate network attacks and find evidence using common network forensic tools. 1st edition.

Forensic Analysis Network: Incident Response Toolset, Document for students (2022) *ENISA*. Available at: https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material (Accessed: December 8, 2022).

Mattwojo (2022) *Windows dev kit 2023 (project volterra)*, *(Project Volterra) | Microsoft Learn*. Available at: https://learn.microsoft.com/en-us/windows/arm/dev-kit/ (Accessed: December 7, 2022).

Yoachimik, O. (2022) *Mantis - the most powerful botnet to date*, *The Cloudflare Blog*. The Cloudflare Blog. Available at: https://blog.cloudflare.com/mantis-botnet/ (Accessed: December 7, 2022).

Eliot (2009) *Tagged - stormfucker*, *Hackaday*. Available at: https://hackaday.com/tag/stormfucker/

Davidoff, S. and Ham, J. (2012) Network forensics: tracking hackers through cyberspace. Upper Saddle River, NJ: Prentice Hall.

Qureshi, S., Tunio, S., Akhtar, F., Wajahat, A., Nazir, A. and Ullah, F. (2021). Network Forensics: A Comprehensive Review of Tools and Techniques. *International Journal of Advanced Computer Science and Applications*, *12*(5).

Gary Kessler Associates (2019) *GCK'S FILE SIGNATURES TABLE*. Available at: https://www.garykessler.net/library/file_sigs.html (Accessed: December 8, 2022).

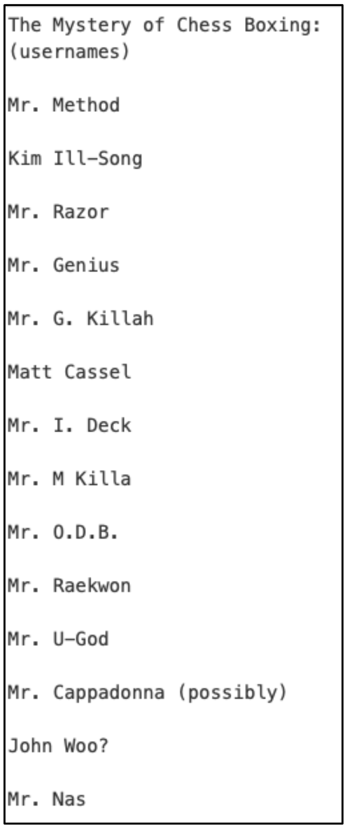
The Guardian (2013) *Edward Snowden: the whistleblower behind the NSA surveillance revelations*. Available at: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (Accessed: December 8, 2022).

APPENDICES

3.3 CAPTURE 1.PCAP

3.3.1 Important files

Track6.docx



The Mystery of Chess Boxing:
(usernames)

Mr. Method

Kim Ill-Song

Mr. Razor

Mr. Genius

Mr. G. Killah

Matt Cassel

Mr. I. Deck

Mr. M Killa

Mr. O.D.B.

Mr. Raekwon

Mr. U-God

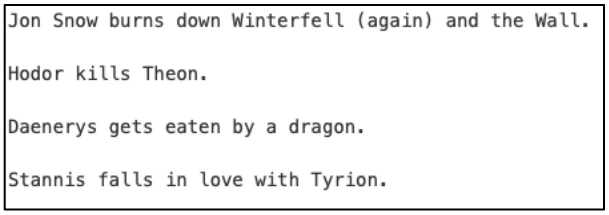
Mr. Cappadonna (possibly)

John Woo?

Mr. Nas

3.3.2 Out of scope

GoT Spoilers.docx



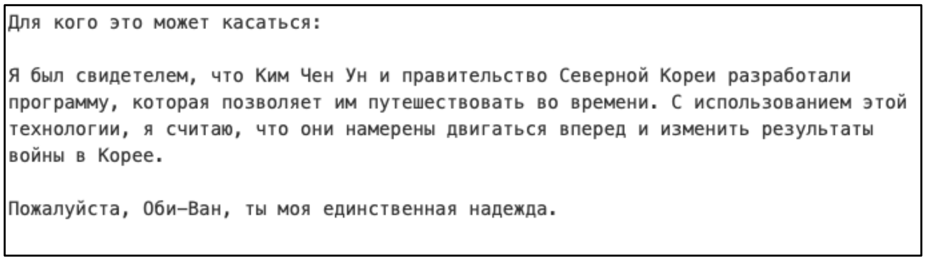
Jon Snow burns down Winterfell (again) and the Wall.

Hodor kills Theon.

Daenerys gets eaten by a dragon.

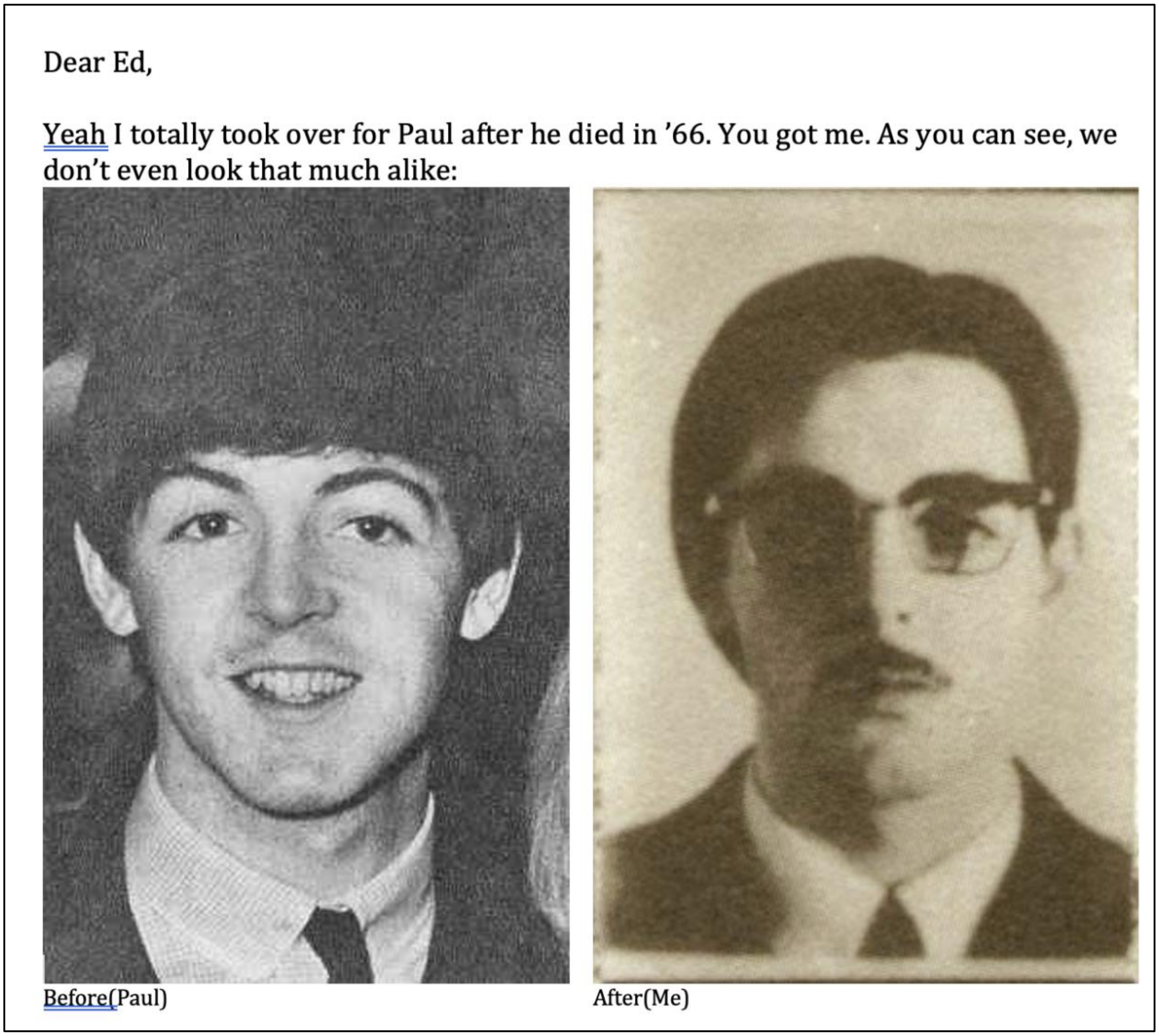
Stannis falls in love with Tyrion.

NorthKorea.docx



```
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.
```

PiD.docx



Dear Ed,

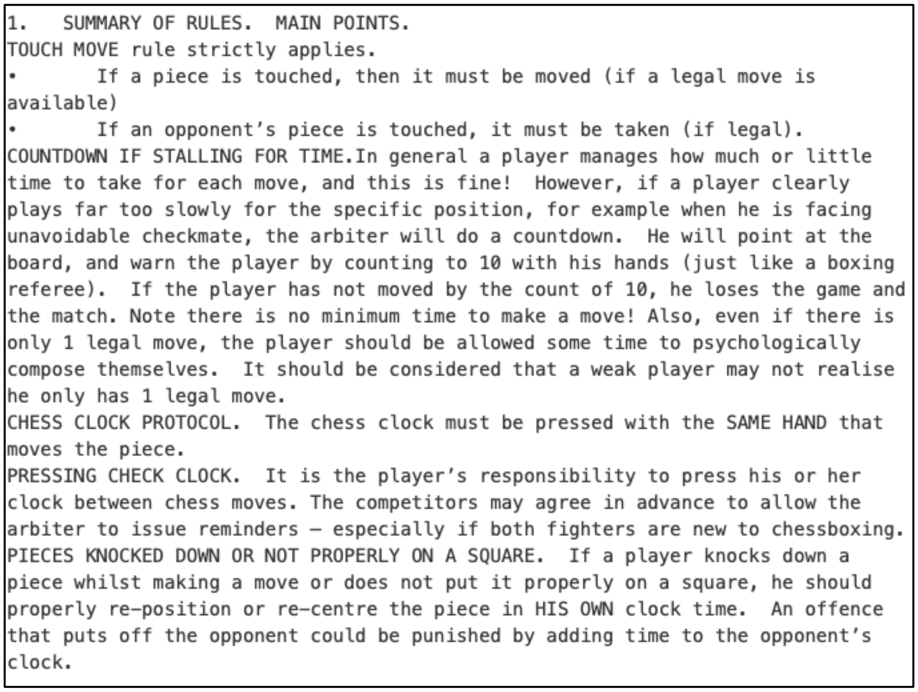
Yeah I totally took over for Paul after he died in ’66. You got me. As you can see, we don’t even look that much alike:

Before(Paul)

After(Me)

NK.jpg

Rules 1..docx



1. SUMMARY OF RULES. MAIN POINTS.

TOUCH MOVE rule strictly applies.

- If a piece is touched, then it must be moved (if a legal move is available)
- If an opponent's piece is touched, it must be taken (if legal).

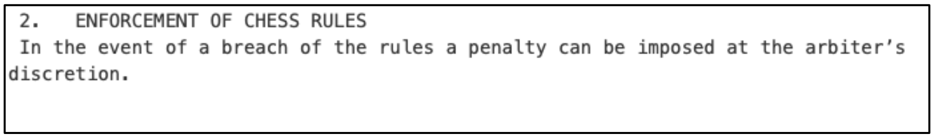
COUNTDOWN IF STALLING FOR TIME.In general a player manages how much or little time to take for each move, and this is fine! However, if a player clearly plays far too slowly for the specific position, for example when he is facing unavoidable checkmate, the arbiter will do a countdown. He will point at the board, and warn the player by counting to 10 with his hands (just like a boxing referee). If the player has not moved by the count of 10, he loses the game and the match. Note there is no minimum time to make a move! Also, even if there is only 1 legal move, the player should be allowed some time to psychologically compose themselves. It should be considered that a weak player may not realise he only has 1 legal move.

CHESS CLOCK PROTOCOL. The chess clock must be pressed with the SAME HAND that moves the piece.

PRESSING CHECK CLOCK. It is the player's responsibility to press his or her clock between chess moves. The competitors may agree in advance to allow the arbiter to issue reminders – especially if both fighters are new to chessboxing.

PIECES KNOCKED DOWN OR NOT PROPERLY ON A SQUARE. If a player knocks down a piece whilst making a move or does not put it properly on a square, he should properly re-position or re-centre the piece in HIS OWN clock time. An offence that puts off the opponent could be punished by adding time to the opponent's clock.

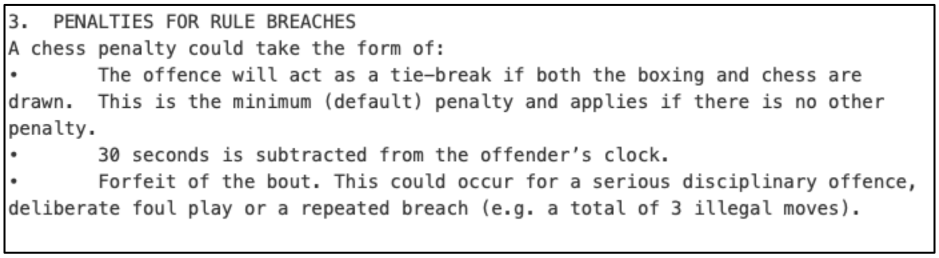
Rules 2.docx



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

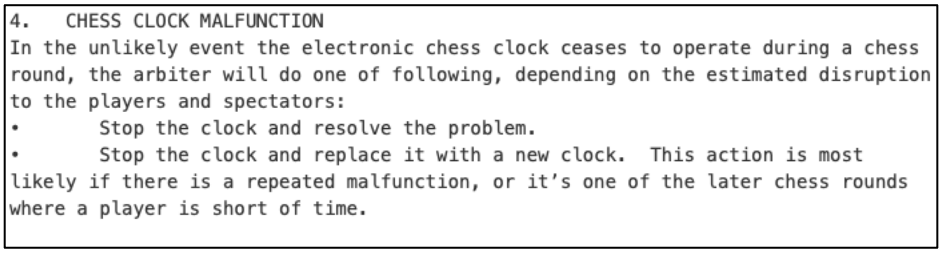


3. PENALTIES FOR RULE BREACHES

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

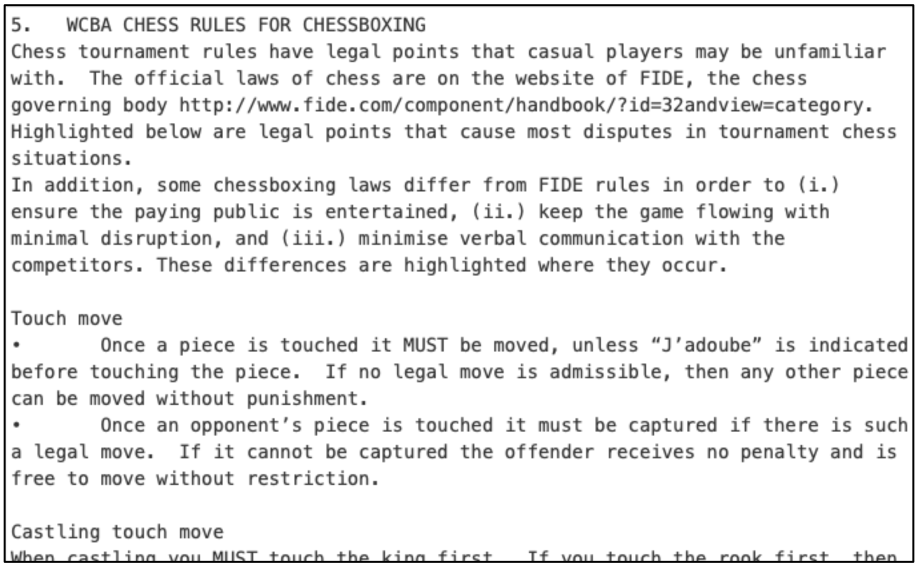


4. CHESS CLOCK MALFUNCTION

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.

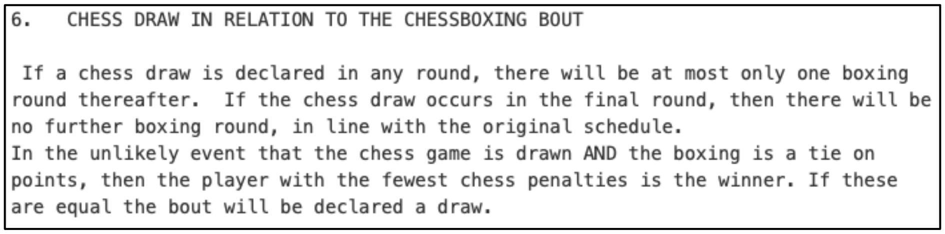
Touch move

- 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

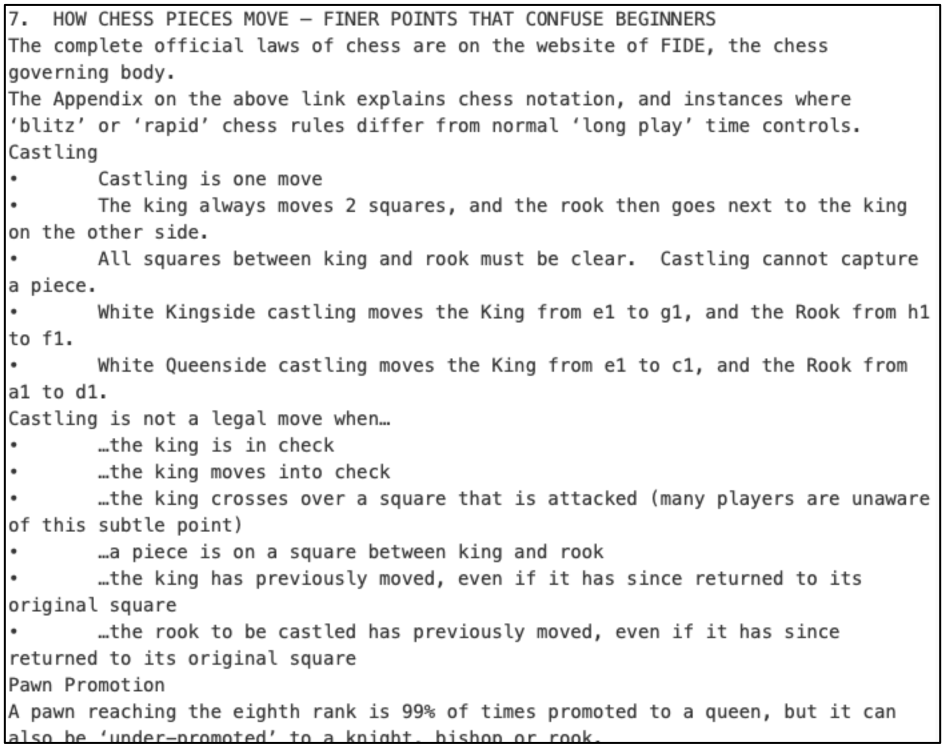
Rules 6.docx



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

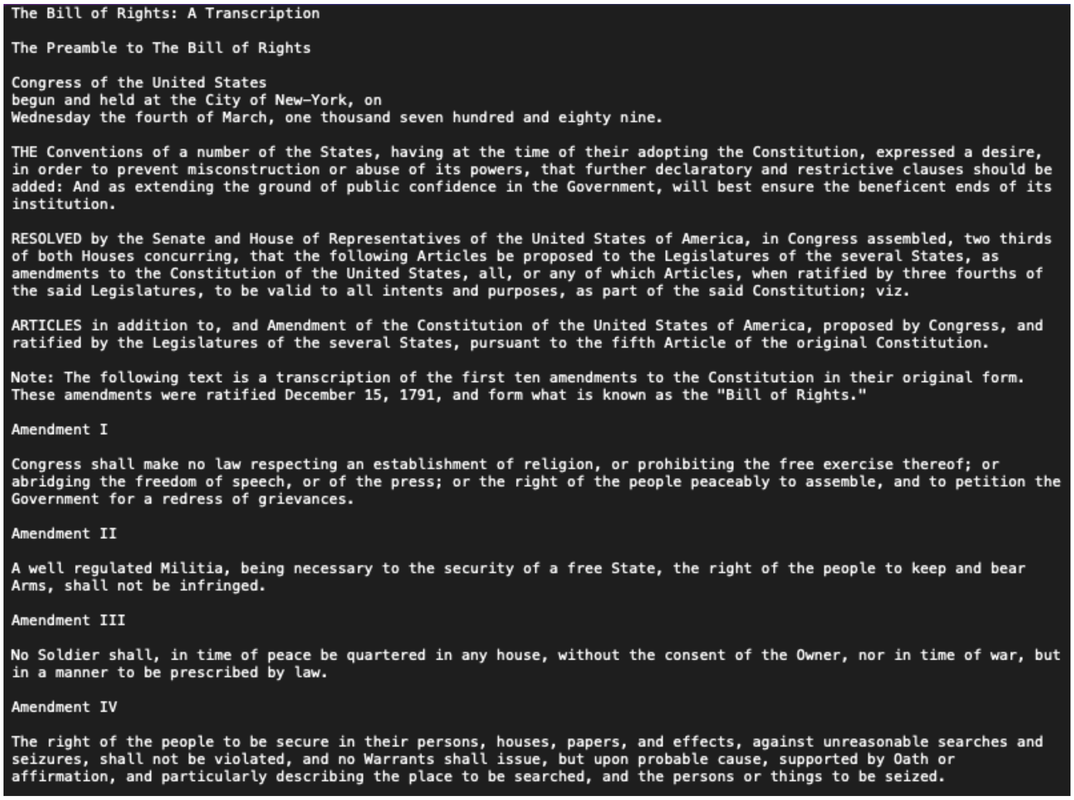
• Castling is one move
• The king always moves 2 squares, and the rook then goes next to the king on the other side.
• All squares between king and rook must be clear. Castling cannot capture a piece.
• White Kingside castling moves the King from e1 to g1, and the Rook from h1 to f1.
• White Queenside 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.

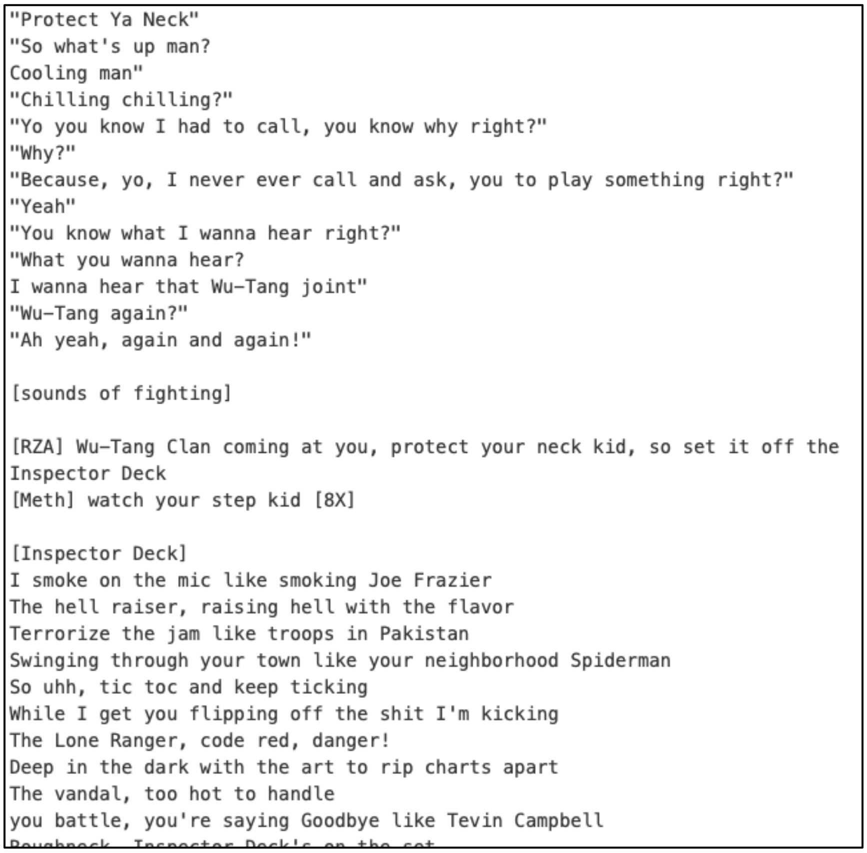
BillOfRights.txt



```
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.
```

NorthKorea.jpeg

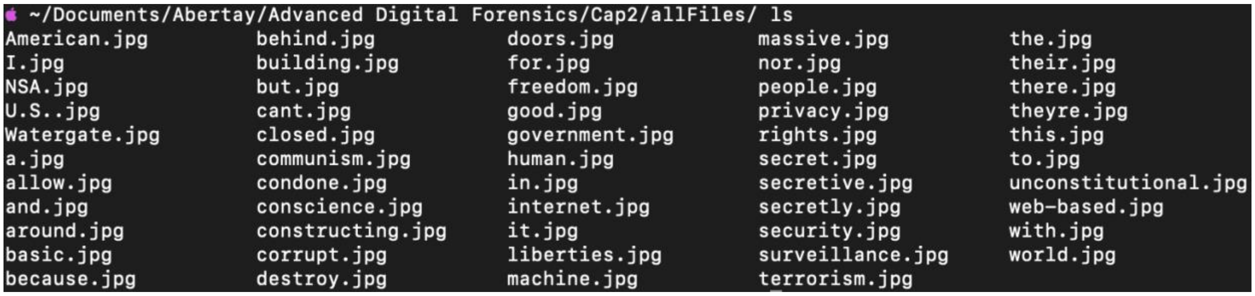
Track10.docx



```
"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
```

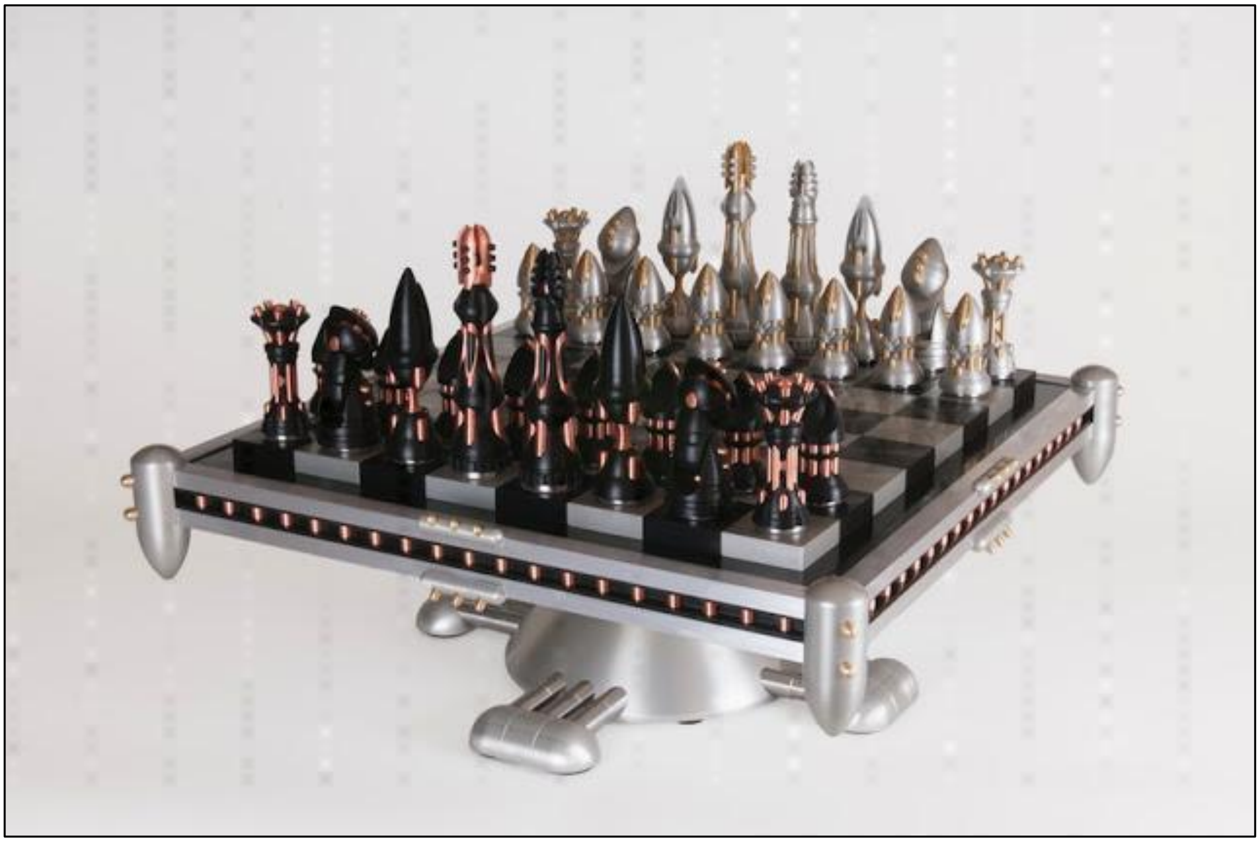
3.4 CAPTURE 2.PCAP

List of all files recovered from 5 archives



```
 ~/Documents/Abertay/Advanced Digital Forensics/Cap2/allFiles/ ls
American.jpg         behind.jpg           doors.jpg            massive.jpg          the.jpg
I.jpg                building.jpg         for.jpg              nor.jpg              their.jpg
NSA.jpg              but.jpg              freedom.jpg          people.jpg           there.jpg
U.S..jpg             cant.jpg             good.jpg             privacy.jpg          theyre.jpg
Watergate.jpg        closed.jpg           government.jpg       rights.jpg           this.jpg
a.jpg                communism.jpg        human.jpg            secret.jpg           to.jpg
allow.jpg            condone.jpg          in.jpg               secretive.jpg        unconstitutional.jpg
and.jpg              conscience.jpg       internet.jpg         secretly.jpg         web-based.jpg
around.jpg           constructing.jpg     it.jpg               security.jpg         with.jpg
basic.jpg            corrupt.jpg          liberties.jpg        surveillance.jpg     world.jpg
because.jpg          destroy.jpg          machine.jpg          terrorism.jpg
```

Combined-image.jpg



3.5 Capture 3.pcap

Conversation transcript

ID	Time and Date	Sender	Message text
1	02/07/2014 17:39:43	Kim Ill-song	Good afternoon Ann
2	02/07/2014 17:39:53	Ann	Who is this?
3	02/07/2014 17:40:19	Kim Ill-song	Castling
4	02/07/2014 17:40:24	Ann	Where are you?
5	02/07/2014 17:40:52	Kim Ill-song	I know I can't tell you that
6	02/07/2014 17:42:03	Ann	Do you know that there are people investigating Kim Ill-Song?
7	02/07/2014 17:42:31	Kim Ill-song	Of course. However they will never know that it is me behind the bribes.
8	02/07/2014 17:43:33	Ann	Still we should be careful. Pay attention. I want to meet in September at 5pm.
9	02/07/2014 17:43:49	Kim Ill-song	At our old meetup spot?
10	02/07/2014 17:44:06	Ann	Yes
11	02/07/2014 17:44:29	Kim Ill-song	What day?
12	02/07/2014 17:51:10	Ann	I told you to pay attention

List of all coordinates

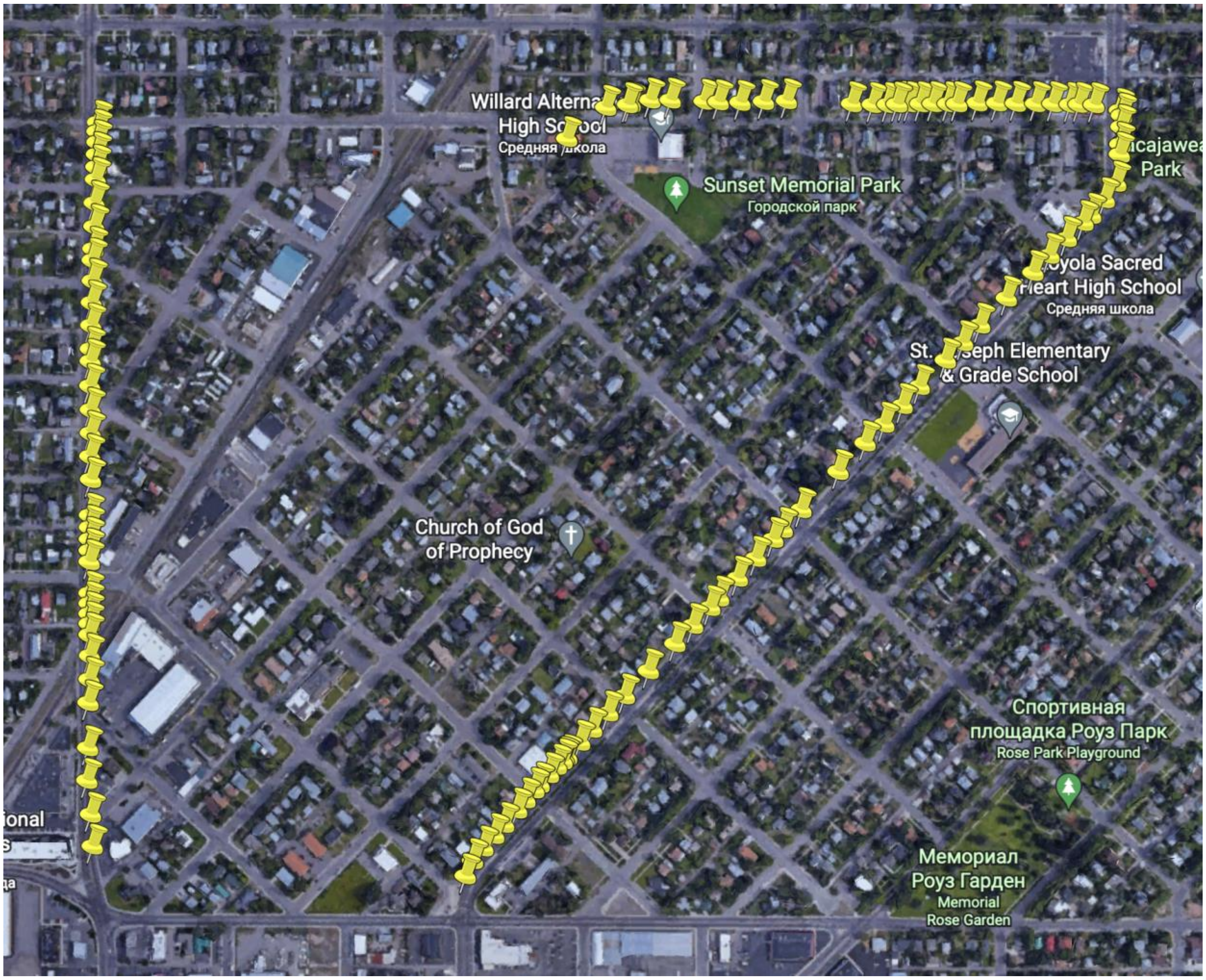
x	y
46.8566132	-114.01861
46.8569336	-114.01863
46.8572731	-114.01868
46.8576012	-114.01867
46.8580551	-114.01866
46.8582878	-114.01865
46.8585243	-114.01864
46.8587341	-114.01865
46.8588448	-114.01865
46.8589439	-114.01865
46.8590469	-114.01865
46.8591499	-114.01865
46.8594666	-114.01865

46.8595772	-114.01865
46.8596916	-114.01865
46.8598099	-114.01865
46.859932	-114.01865
46.8602905	-114.01863
46.8605232	-114.01864
46.8607559	-114.01863
46.8609886	-114.01863
46.8612289	-114.01864
46.8614769	-114.01863
46.861599	-114.01863
46.8618355	-114.01862
46.8620644	-114.01862
46.8622818	-114.0186
46.8624878	-114.0186
46.8626022	-114.01859
46.8628273	-114.01858
46.8630638	-114.01858
46.8633003	-114.01856
46.8634262	-114.01855
46.8635521	-114.01855
46.8636742	-114.01854
46.863781	-114.01854
46.8638725	-114.01853
46.8637047	-114.01164
46.8637085	-114.01163
46.8640175	-114.01107
46.8640442	-114.01075
46.864048	-114.01071
46.86409	-114.01042
46.86409	-114.01012
46.8640785	-114.00963
46.8640709	-114.00942
46.8640671	-114.0091
46.8640747	-114.00876
46.8640823	-114.00842
46.8640518	-114.00747
46.8640442	-114.00716
46.8640442	-114.00694

46.864048	-114.00681
46.8640556	-114.00671
46.8640518	-114.00662
46.8640518	-114.00646
46.8640518	-114.00628
46.8640518	-114.00606
46.8640518	-114.00593
46.8640595	-114.00563
46.8640595	-114.00534
46.8640556	-114.00507
46.8640518	-114.00478
46.8640518	-114.00452
46.8640442	-114.00427
46.8640442	-114.00414
46.8640404	-114.00392
46.8639832	-114.00355
46.8639336	-114.00352
46.8638191	-114.00352
46.8636437	-114.00354
46.8635445	-114.00355
46.8632546	-114.0036
46.8630905	-114.00377
46.8629341	-114.00397
46.8628616	-114.00408
46.8627014	-114.00433
46.8625336	-114.00458
46.8623619	-114.00481
46.8621063	-114.0052
46.8618355	-114.00559
46.86166	-114.00584
46.8614845	-114.0061
46.8612213	-114.00648
46.8610306	-114.00673
46.8608437	-114.007
46.8606567	-114.00727
46.8603706	-114.00767
46.8599892	-114.00821
46.8597908	-114.00848
46.8596916	-114.00862

46.8595009	-114.00887
46.8593025	-114.00914
46.8591042	-114.00941
46.8590088	-114.00954
46.8588295	-114.0098
46.8586464	-114.01006
46.8583756	-114.01044
46.8581238	-114.0108
46.8579521	-114.01104
46.8577881	-114.01128
46.8576584	-114.01145
46.8575134	-114.01164
46.8574905	-114.01169
46.8574715	-114.01171
46.8574181	-114.0118
46.8573341	-114.01191
46.857235	-114.01205
46.8571816	-114.01212
46.8570824	-114.01225
46.8569794	-114.01237
46.8568344	-114.01257
46.8567238	-114.01271
46.8565979	-114.01287
46.856472	-114.01302
46.8563194	-114.01313

Resulting number


Willard Alterna
High Sc ool
Средняя школа
Sunset Memorial Park
Городской парк
cajawea
Park
yola Sacred
Heart High School
Средняя школа
St. seph Elementary
& Grade School
Church of God
of Prophecy
Спортивная
площадка Роуз Парк
Rose Park Playground
Мемориал
Роуз Гарден
Memorial
Rose Garden
ional