University of Sheffield

Forensics Case Study

Jagpreet

Digital Forensics

December 14, 2022

Contents

List of Figures

List of Tables

Chapter 1

Part 1

1.1 A

From the point of arrest Following will be my approach:

- Identifying Potential Sources of evidences such as Cameras around Prison Area, Mobile Tower dumps to locate Leo R activity in the area,
- Handling and Transporting the collected Digital evidences properly and carefully, avoid exposure to magnetic fields by using tools such as Faraday Bags, or unauthorized access.
- Establish a proper Chain of custody so that only authorised and competent people handle the evidence.
- Using tools such as DRone open-source Parser(DROP) to analyze the drone.
- mapping out the network of people in contact with Leo R, his contact inside the prison and other people who may have come in contact with Leo R.
- Evidences from non Digital Forensics areas can provide context when analysing Digital evidence, setting up a good cooperation with the Police will be key for a smooth forensics examination.
- The forensics evidence collected and analysed should be able to stand and survive challenges in the court of law, Therefore the tools used and files analyzed should be done properly, for example by providing hashes of files as evidence of their integrity and non tampering.

1.2 B

The following approach was taken to investigate this case :

- As the usb image was not very large in size, and the kind of items straight forward, It was not very difficult to find out the necessary evidence to reach a conclusion.
- As the type of Drone used DJI Phantom 2 vision drone can carry upto 200 grams of drugs, My initial goal was to find evidence regarding any drugs.
  - Although there were some text files with GPS co-ordinates and satellite positions which may be used to synchronize drug drops inside a prison facility, any further evidence towards drug delivery as a motive was lacking.
  - Other images contaning beakers and drugs were either drugs for Tuberculosis or being used in conducting blood tests.
- After writing off drug delivery as the primary motive for Leo R to fly his drone I investigated other files and found the following evidence which demonstrates that Leo R was trying to execute a prison break using Drones, other willing co-conspirators by digging a tunnel into the prison to get his Friend Adam out.

– His possession of text files containing GPS coordinates with Satellite data implies he was trying to accurately predict the path of the tunnel as by calibrating with the satellites properly, he can pinpoint the location of the place from where tunnel ends and starts.

– He has kept the layout of the prison in a zip file called Keep safe.zip , and in other places , some of which are shown in figure 1.1

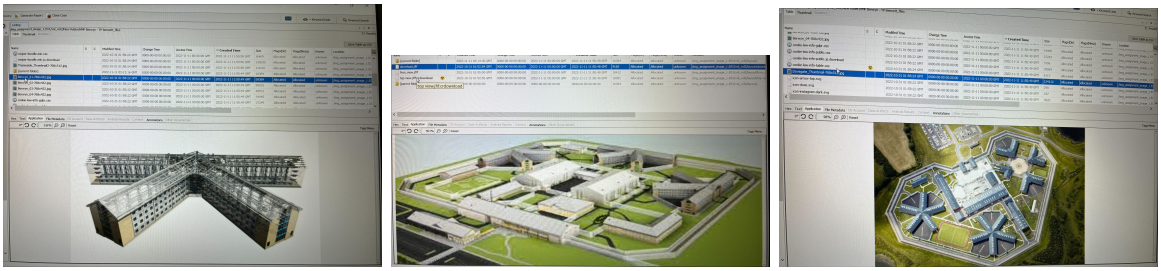


Figure 1.1: *Layout*

– The E-mail to be sent saved as e-mail to send.txt in personals.zip asking Robin for help on his plan after being recommended by Roxy, is further evidence of his intent.

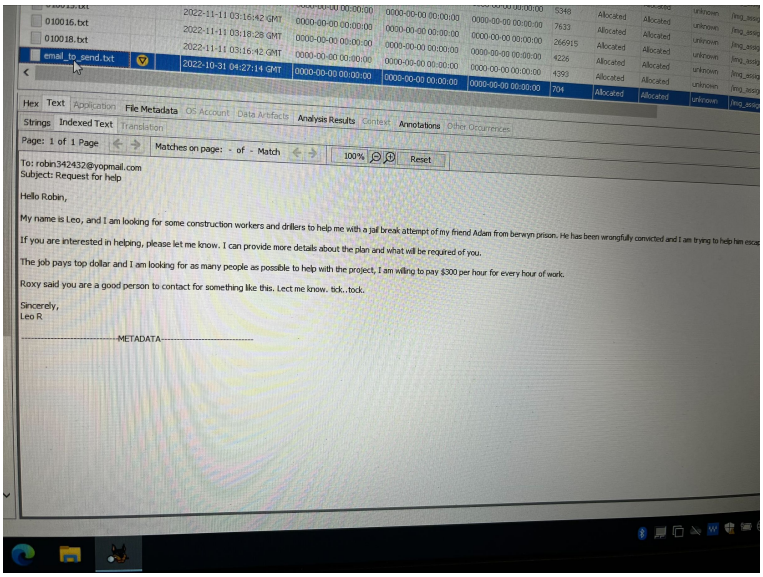


Figure 1.2: *E-mail*

– He also has a list named materials needed.txt which lists out materials such as excavator and things which are meant to build a tunnel.

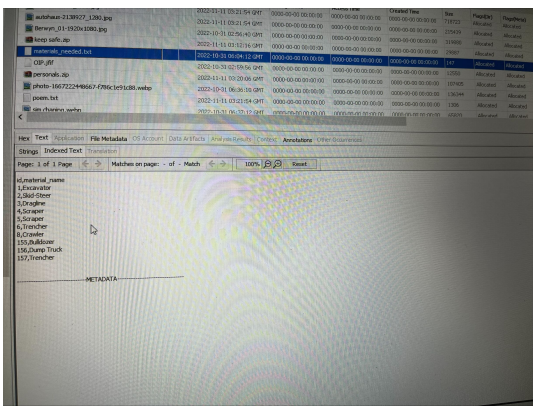


Figure 1.3: *Caption*

To conclude, however it may be just an ruse as the e-mail was not sent, for a cover to deliver drugs into the prison, and As Leo is a seasoned criminal, he may be trying to gamer the system by attempting to throw off the police off his drug delivery creimes. Auxillary evidence would be needed to reacha conclusion.

Chapter 2

Part 2

Following steps were followed in conducting the Forensics investigation:

- Establishing Chain of custody after taking in the disk image and network capture of Ciara's laptop. As the information regarding Ciara was scarce, such as her job role in the company, company's name was not known at the outset, A Brute Force approach was adopted to find first few clues.
- Ciara seems to be using Cy in her newly created e-mail id.
- Autopsy tool was used to analyze the Laptop's Digital image and following information was extracted :

Persons of Interest			
Person	E-mails	Company	Account Creation
Ciara	ciarabartcy@gmail.com, CiaraTx@Tutanota.com, ciarabart@philotess.com,	Philotess, Cy == CyCo??	03-Jan-2020, , 03-Jan-2020
Petra Lee	petrealee95@protonmail.com	-	-
alex michael	alexmichael@protonmail.com, alexxysteercy@gmail.com	Ciara contact	03-Jan-2020
Jude Nyugen	jude.nyugen@philotess.com	Philotess, Possible Co-conspirator?	-
Chris Laurent	chris.laurent@philotess.com	Philotess, Possible Co-conspirator?	-

Table 2.1: *Persons of Interest*

- Upon inspection it was found that much suspicious activity happened on 3 January 2020:
- Accounts were made using Ciara's Credentials adn email'id on platforms such as tutanota.com which provide encrypted e-mail services as shown below :

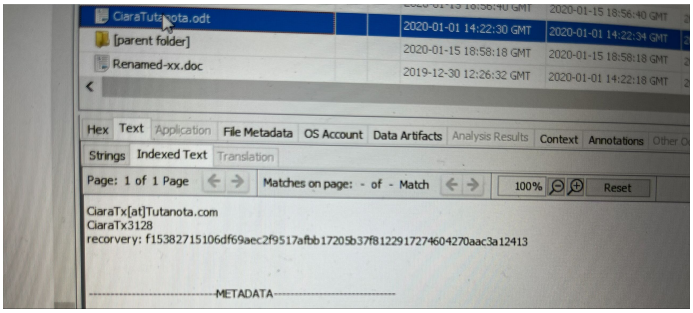


Figure 2.1: *Tutanota*

Network Traffic		
Ip= Addresses	Websites	Filenames or passwords?
192.168.0.42	google.fr visited, mail.ovh visited, Using Ftp service, Potential document transfer in three documents,	Ciara, TCiara,CiaraBird, mozilla@example.com
192.168.0.46	192.168.0.42	-
192.168.0.12	192.168.0.42	-
192.168.0.254	192.168.0.42	-

Table 2.2: *Network*

- Softwares were downloaded such as FileZilla, and websites visited such as signal , which also provide encrypted communication services.

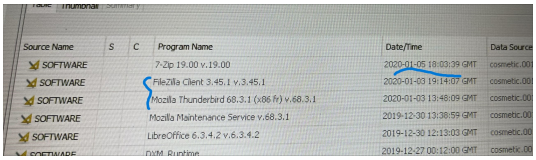


Figure 2.2: *Filezilla*

- Suspicious E-mail Conversations:

  E-mail sent from Jude Nyugen talking about a confidential meeting as shown below: E-mail on the right from Chris

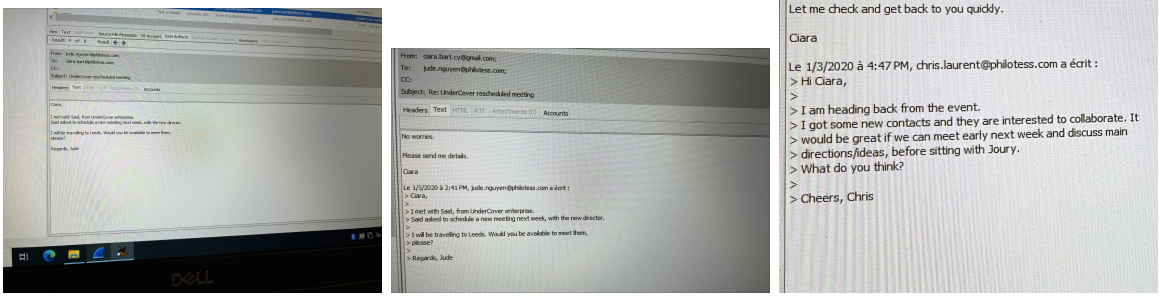


Figure 2.3: *undercover E-mail*

  laurent which may or may not be malicious.

- Network Traffic Analysis of Ciara's Laptop gave following information:

- One of the documents can be recovered using Wireshark → Export Objects FTP-DATA called newcollection.docx which talks about new collection release dates and talks about a Prototype Location which is Pr, which may be code for Paris, where Cyco is Located.

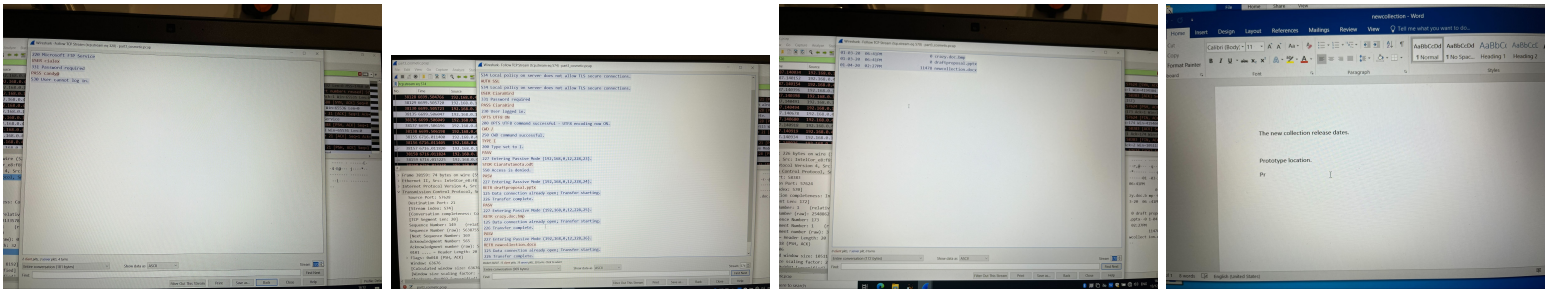


Figure 2.4: *FTP capture*

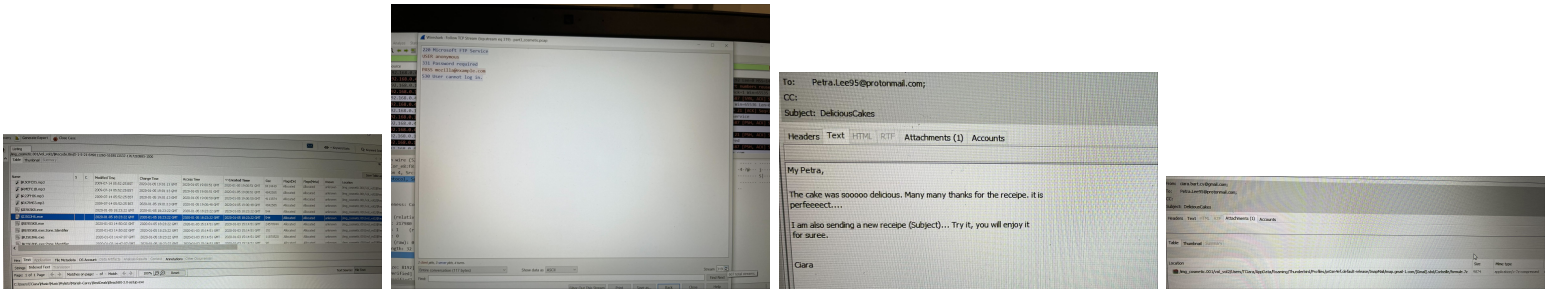


Figure 2.5: *5 jan 2020*

- Suspicious Activity on 5 Jan 2020 as shown in Fig 2.5 is :
  - Downloading Bleach Bit which is used to delete data permanently and make any recovery harder.
  - A email is sent to Nyugen containing a purported cake recipe, but the zip file is protected by a password, which seems strange as why would anyone password lock a cake recipe.

- Company Data Found in possession of Ciara: She has a list of ingredients of how to manufacture a product, and sales data for company in three years 2017,2018,2019 as shown in figure 2.6.

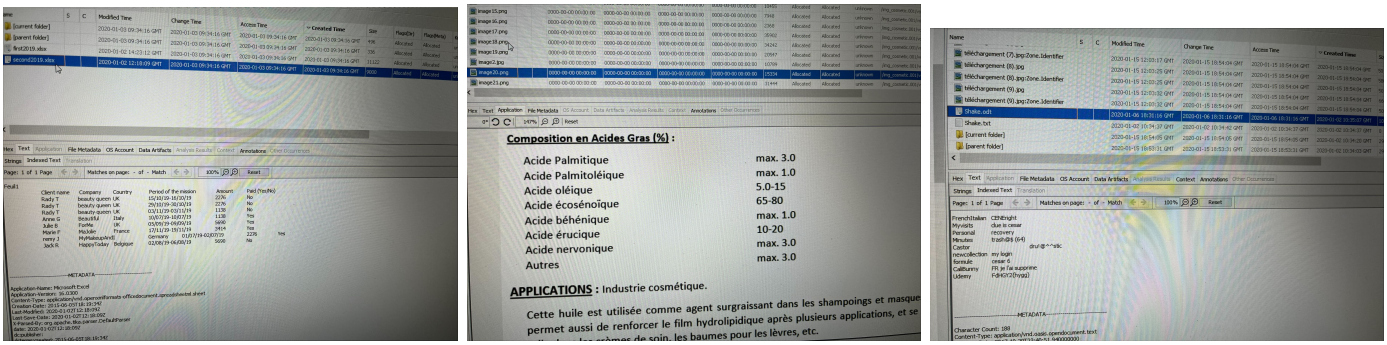


Figure 2.6: *Sensitive Data*

- Encrypted Files Found such as formule.zip,CaliBunny.zip etc which cannot be opened. Although several passwords are found, none of them work on these files. One such file containing passwords recovered from Autopsy is shown on the right in figure 2.6:

To Conclude the actions of Ciara point towards intent, purpose and capability of having commmited the offence of sharing confidential Data with a potential competitor, However due to constraints of the data available and capacity and competence of the investigator, it can not be said conclusively that Ciara has committed the crime she is accused of.

Chapter 3

Part 3

As an Forensic Analyst handling the incident, I will adopt the SANS Incident Handling Framework, and follow any company policies or standard operating procedures. My response will be following:

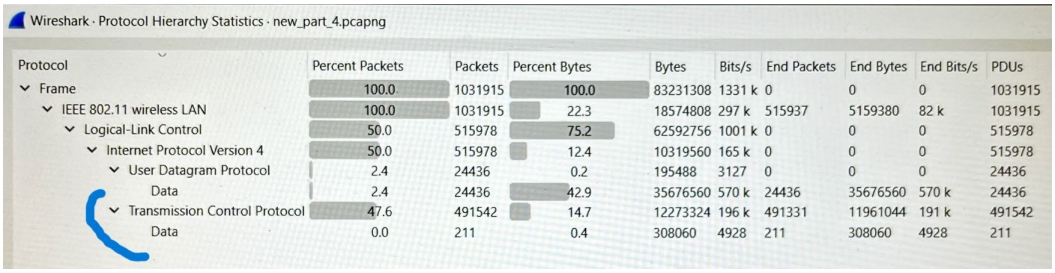
1. Identification:
    - Identifying the extent of the ransomware and other servers if affected and classifying level as High or Moderate ,Reporting to the relevant authorities such as CERT.
    - Protection of evidence such as the two hard drives and RAM and other logs such as Operating System logs and network logs, Conducting Interviews, and documenting evidence establishing Chain of Custody.
2. Containment:
    - Preparing backups and changing passwords, Securing other servers through Isolation or updating Security Levels
    - Collection of further evidence depending on the order of volatility, where evidence collection proceeds from most volatile such as Registers and Cache to Disks etc.
3. Eradication:
    - Using the two Hard drives from the infected server and the memory capture, we can perform Root Cause Analysis to know how the system was compromised and what type of steps are available to get rid of the ransomware.
    - Other additional information from the Containment step can help in dealing with the ransomware.
    - Using Tools such as Anti-Virus or external help we can eradicate the ransomware from the system if possible.
    - Care should be taken to account for presence of any backdoors installed into the system by the ransomware.
4. Recovery:
    - Making sure that the infected system is working, and the threat has been contained or eliminated.
    - Monitoring the system, and observing system logs
    - Making Sure all hardware and software are updated to latest security standards
5. Follow Up:
    - Performing Cost Analysis and extent of damage caused to the organisation
    - Lessons learned that will cover the effectiveness of response, as the Security team was unable to identify and assess the threat properly despite being alerted by system administrator.
6. Preparation:
    - Revising and Updating any policies to make further responses more effective, for example, Having a security team available 24x7 is better to protect the core business interest for the organisation.
    - Better training and awareness necessary for both staff and clients tom improve security.

Chapter 4

Part 4

For Analysing the PCAP file, Wire-shark was used and following steps were taken:

- Understanding Overall nature of network traffic in the system, For that we Use Wire-shark → Statistics → Protocol Hierarchy, which is shown below:

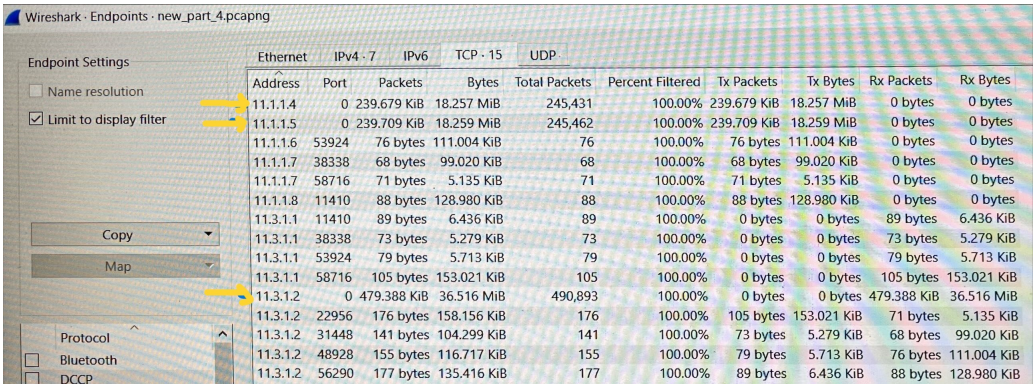


Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	1031915	100.0	83231308	1331 k	0	0	0	1031915
IEEE 802.11 wireless LAN	100.0	1031915	22.3	18574808	297 k	515937	5159380	82 k	1031915
Logical-Link Control	50.0	515978	75.2	62592756	1001 k	0	0	0	515978
Internet Protocol Version 4	50.0	515978	12.4	10319560	165 k	0	0	0	515978
User Datagram Protocol	2.4	24436	0.2	195488	3127	0	0	0	24436
Data	2.4	24436	42.9	35676560	570 k	24436	35676560	570 k	24436
Transmission Control Protocol	47.6	491542	14.7	12273324	196 k	491331	11961044	191 k	491542
Data	0.0	211	0.4	308060	4928	211	308060	4928	211

Figure 4.1: *Protocol Hierarchy*

We can see that major traffic in the network is TCP traffic.

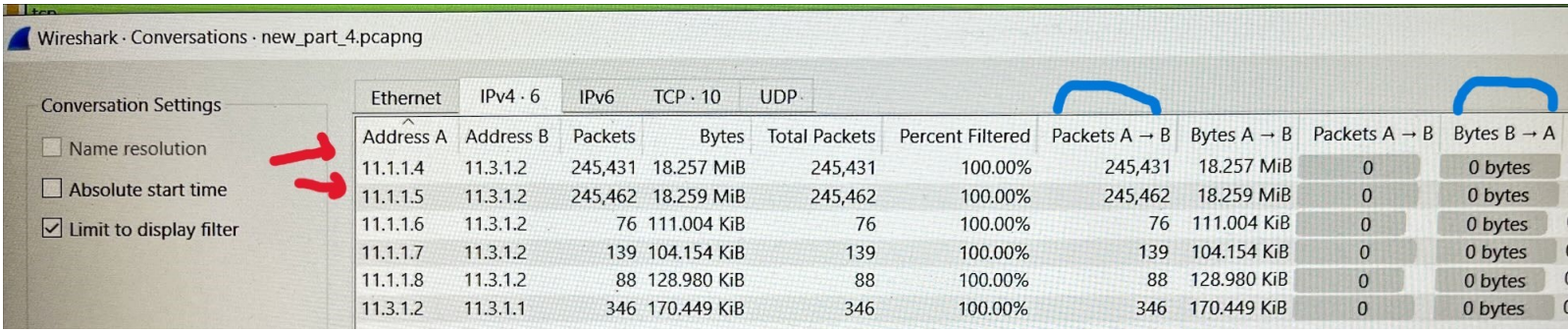
- Now we investigate What type of interactions and with what IP addresses is happening in the network, For that we use Wire-shark → Statistics → Endpoints, and observe that the major network traffic is between IP address 11.1.1.4, 11.1.1.5 and 11.3.1.2.



Address	Port	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
11.1.1.4	0	239.679 KiB	18.257 MiB	245,431	100.00%	239.679 KiB	18.257 MiB	0 bytes	0 bytes
11.1.1.5	0	239.709 KiB	18.259 MiB	245,462	100.00%	239.709 KiB	18.259 MiB	0 bytes	0 bytes
11.1.1.6	53924	76 bytes	111.004 KiB	76	100.00%	76 bytes	111.004 KiB	0 bytes	0 bytes
11.1.1.7	38338	68 bytes	99.020 KiB	68	100.00%	68 bytes	99.020 KiB	0 bytes	0 bytes
11.1.1.7	58716	71 bytes	5.135 KiB	71	100.00%	71 bytes	5.135 KiB	0 bytes	0 bytes
11.1.1.8	11410	88 bytes	128.980 KiB	88	100.00%	88 bytes	128.980 KiB	0 bytes	0 bytes
11.3.1.1	11410	89 bytes	6.436 KiB	89	100.00%	0 bytes	0 bytes	89 bytes	6.436 KiB
11.3.1.1	38338	73 bytes	5.279 KiB	73	100.00%	0 bytes	0 bytes	73 bytes	5.279 KiB
11.3.1.1	53924	79 bytes	5.713 KiB	79	100.00%	0 bytes	0 bytes	79 bytes	5.713 KiB
11.3.1.1	58716	105 bytes	153.021 KiB	105	100.00%	0 bytes	0 bytes	105 bytes	153.021 KiB
11.3.1.2	0	479.388 KiB	36.516 MiB	490,893	100.00%	0 bytes	0 bytes	479.388 KiB	36.516 MiB
11.3.1.2	22956	176 bytes	158.156 KiB	176	100.00%	105 bytes	153.021 KiB	71 bytes	5.135 KiB
11.3.1.2	31448	141 bytes	104.299 KiB	141	100.00%	73 bytes	5.279 KiB	68 bytes	99.020 KiB
11.3.1.2	48928	155 bytes	116.717 KiB	155	100.00%	79 bytes	5.713 KiB	76 bytes	111.004 KiB
11.3.1.2	56290	177 bytes	135.416 KiB	177	100.00%	89 bytes	6.436 KiB	88 bytes	128.980 KiB

Figure 4.2: *Endpoints*

- Next we want to see What type of interactions is happening between these IP addresses, for that we use Wire-shark → Statistics → Conversations: We observe the major traffic is one way from IP addresses 11.1.1.4, 11.1.1.5 towards 11.3.1.2.



Address A	Address B	Packets	Bytes	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets A → B	Bytes B → A
11.1.1.4	11.3.1.2	245,431	18.257 MiB	245,431	100.00%	245,431	18.257 MiB	0	0 bytes
11.1.1.5	11.3.1.2	245,462	18.259 MiB	245,462	100.00%	245,462	18.259 MiB	0	0 bytes
11.1.1.6	11.3.1.2	76	111.004 KiB	76	100.00%	76	111.004 KiB	0	0 bytes
11.1.1.7	11.3.1.2	139	104.154 KiB	139	100.00%	139	104.154 KiB	0	0 bytes
11.1.1.8	11.3.1.2	88	128.980 KiB	88	100.00%	88	128.980 KiB	0	0 bytes
11.3.1.2	11.3.1.1	346	170.449 KiB	346	100.00%	346	170.449 KiB	0	0 bytes

Figure 4.3: *Conversations*

- Upon inspection of the packets its observed that :
  - The packets being sent are SYN packets or requests for synchronization with the server to establish a TCP connection.
  - The packets are all of same length i.e 78 bytes.
  - The ACK packets that are to acknowledge the request are not being accepted back by the sender IP.

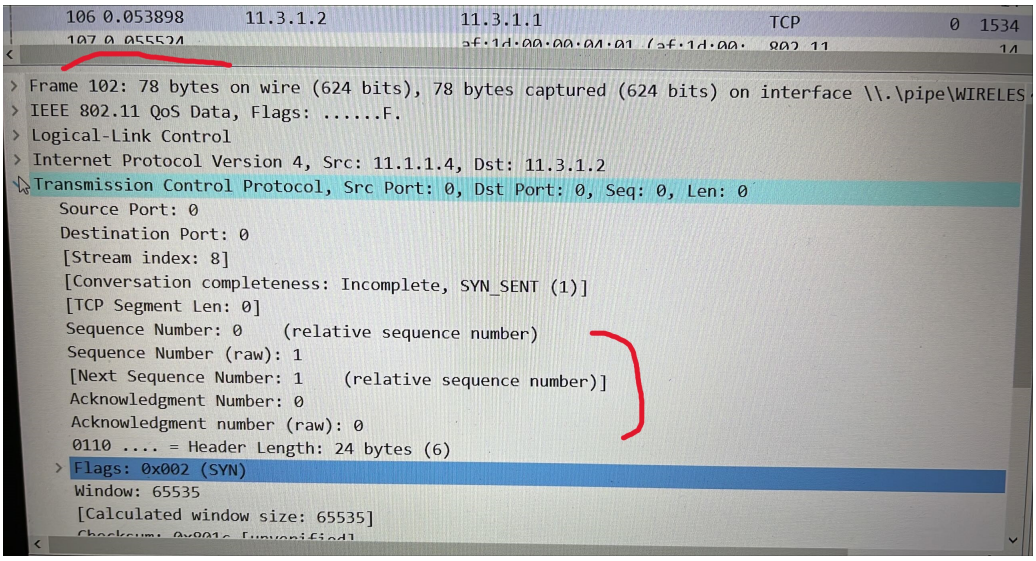


Figure 4.4: *Packet Nature*

- By setting up filter for tcp.flags.syn == 1 and tcp.flags.ack == 0 , we can see that the server is under a type of attack known as SYN flood,a form of denial-of-service attack in which an attacker rapidly initiates a connection to a server without finalizing the connection. The server has to spend resources waiting for half-opened connections, which can consume enough resources to make the system unresponsive to legitimate traffic[CERT [1996]]

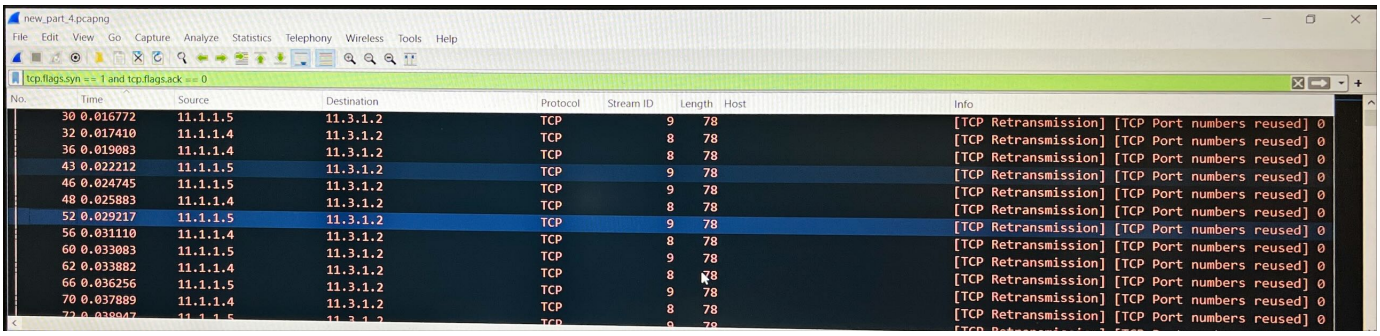


Figure 4.5: *Flag Filter*

To mitigate against such attacks, Recycling oldest half-open TCP connections, Creating SYN cache and cookies or increasing backlog queue are possible solutions.

Bibliography

CERT. Cert. 1996. URL https://web.archive.org/web/20001214111600/http://www.cert.org/advisories/CA-1996-21.html.