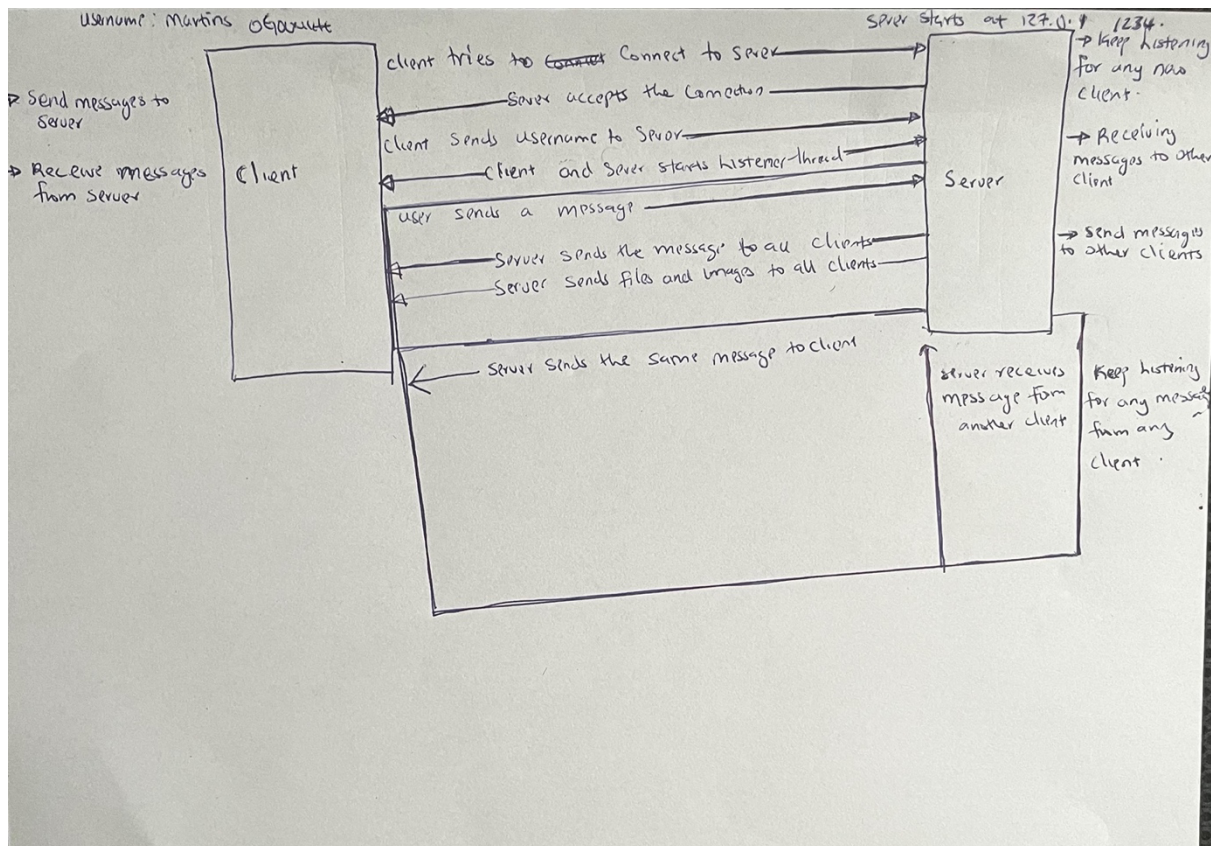


# PROJECT REPORT

## Task 1

### Detailed Project Deliverables



### System architecture design (graphical + text description)

The above diagram shows how client connection is made to the server running on a local 127.0.0.1 and a port number of 1234. Client sends messages, files and images through the server to another client user connected to the same server

### DETAILED PROTOCOL SPECIFICATION

1.The connection feature is running a TCP protocol and socket. connect() method

2. message feature is running on a UTF -8 Encoded Text protocol and `sendall(message. encode())` method
- 3 . File transfer is running on a TCP, chunked binary protocol and a header +`sendal(filedate)` method
4. Handling running with a multithreading protocol and a `threading.thread()` method

## **NETWORK COMMUNICATION FLOW**

Client connects to server through the socket

Client sends username

Server accepts connection and adds client to active list

Client send messages or files

Server connects data to all other connected clients

## **PROTOCOL ANALYSIS**

I choose TCP (Transmission control protocol) because it ensures reliable message delivery and in order packet transmission. Which is important for both messaging and file transfer. Compared to the IPV4 the TCP is considered better.

## **PROS**

1. It offers error detection
2. Reliable data delivery (good for file transfer )
3. Easy to work with

## **CONS**

1. High latency
2. Resource consumption

LINKS TO MY DEMO VIDEO :

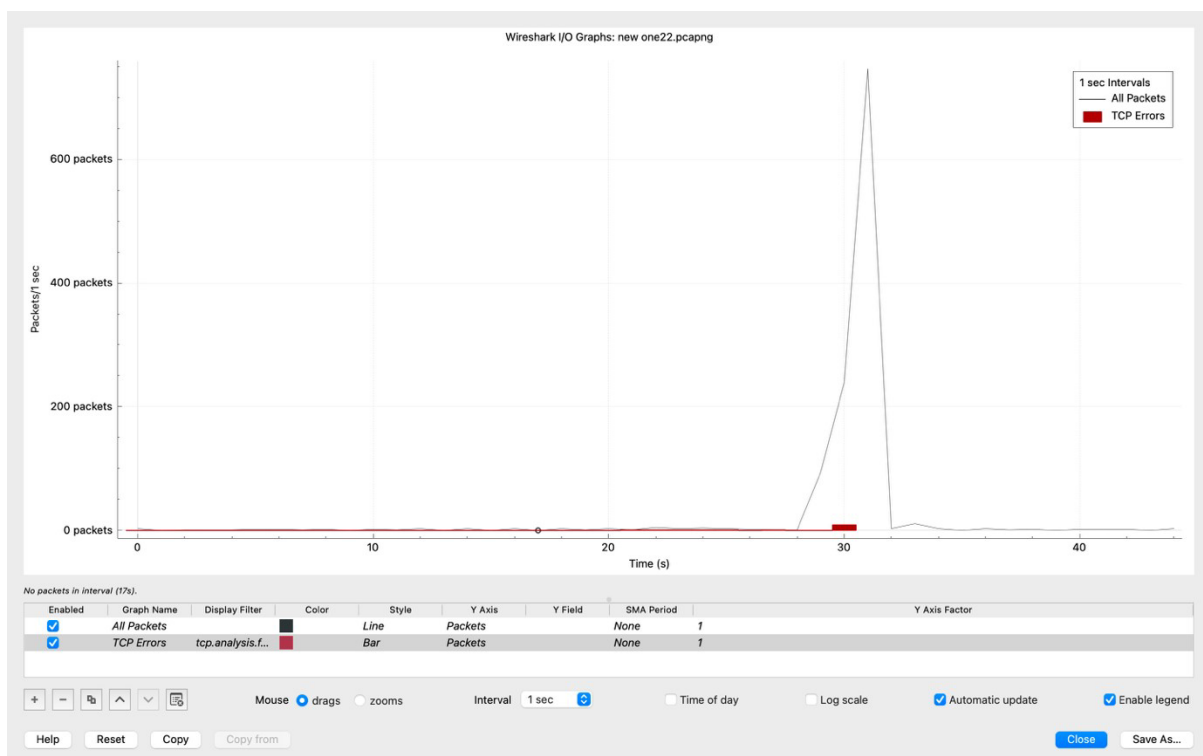
<https://youtu.be/EExDW4bXgF0?si=la0eLkaWsmw4EGKB>

LINK TO MY GITHUB REPOSITORY :

<https://github.com/mart23333/martinschizaramogowuihe.git>

## Task 2

# Wireshark Analysis and Firewall



## I/O GRAPH

The graph shows that around 30 second mark there was a sudden surge to over 600 packets which can suggest a possible malicious activity this sometimes often

consist of malware beaconing, DDos attempts and port scanning. TCP errors red bars shows or suggests failed connections.

SECURITY ISSUES

- 1. infested internal device communicating outbound
- 2. This likely suggests intrusion attempts and compromised host

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	1163	100.0	972199	173 k	0	0	0	1163
Ethernet	100.0	1163	1.7	16534	2949	0	0	0	1163
Internet Protocol Version 6	0.1	1	0.0	40	7	0	0	0	1
User Datagram Protocol	0.1	1	0.0	8	1	0	0	0	1
Multicast Domain Name System	0.1	1	0.1	769	137	1	769	137	1
Internet Protocol Version 4	94.9	1104	2.3	22080	3938	0	0	0	1104
User Datagram Protocol	65.2	758	0.6	6064	1081	0	0	0	758
QUIC IETF	63.5	738	73.2	711314	126 k	738	710826	126 k	742
Multicast Domain Name System	0.1	1	0.1	769	137	1	769	137	1
Domain Name System	0.9	10	0.1	612	109	10	612	109	10
Data	0.8	9	0.0	334	59	9	334	59	9
Transmission Control Protocol	29.7	345	1.2	11220	2001	231	7572	1350	345
Transport Layer Security	9.8	114	20.1	195655	34 k	114	195655	34 k	114
Internet Control Message Protocol	0.1	1	0.0	36	6	1	36	6	1
HomePlug AV protocol	1.8	21	0.1	966	172	21	966	172	21
Data	1.7	20	0.1	920	164	20	920	164	20
Address Resolution Protocol	1.5	17	0.0	476	84	17	476	84	17

No display filter.

HelpCopyProtocolsClose

PROTOCOL HIERARACY STATISTICS

- 1. TLS9.8%packetsshowsenCRYPTedwebtraHicandmonitoringforsuspicious destinations
- 2. Data1.7% packets shows generic data packets without a clear application protocol which will which suggest an investigation for hidden traffics
- 3. TCP29.7%which shows potential or mixed use example scanning attempts
- 4. QUIC63.5%packet prevents threats

CONVERSATION STATISTICS

Conversation Settings											
<input type="checkbox"/> Name resolution <input type="checkbox"/> Absolute start time <input type="checkbox"/> Limit to display filter											
<input type="button" value="Copy"/> <input checked="" type="button" value="Follow Stream..."/> <input type="button" value="Graph..."/>											
Protocol <input type="checkbox"/> Bluetooth <input type="checkbox"/> BPv7 <input type="checkbox"/> DCCP <input checked="" type="checkbox"/> Ethernet <input type="checkbox"/> FC <input type="checkbox"/> FDDI <input type="checkbox"/> IEEE 802.11 <input type="checkbox"/> IEEE 802.15.4 <input checked="" type="checkbox"/> IPv4 <input checked="" type="checkbox"/> IPv6 <input type="checkbox"/> IPX <input type="checkbox"/> JXTA <input type="checkbox"/> LTP <input type="checkbox"/> MPTCP <input type="checkbox"/> NCP <input type="checkbox"/> openSAFETY <input type="checkbox"/> RSVP <input type="checkbox"/> SCTP											
Filter list for specific type											
<input type="button" value="Help"/> <input type="button" value="Close"/>											

Ethernet - 6   IPv4 - 9 <b>IPv6 - 1</b> TCP - 3   UDP - 19											
Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s
104.18.43.204	192.168.178.25	2	134 bytes	3	1	64 bytes	1	70 bytes	25.192006	0.0001	
192.168.178.22	224.0.0.251	1	811 bytes	2	1	811 bytes	0	0 bytes	22.939361	0.0000	
192.168.178.25	104.18.32.47	307	205 kB	4	132	108 kB	175	97 kB	29.489759	1.7325	498 I
192.168.178.25	104.18.41.158	18	9 kB	6	8	4 kB	10	5 kB	29.680304	0.0464	737 I
192.168.178.25	172.64.144.52	720	733 kB	8	128	20 kB	592	713 kB	31.278294	0.3478	450 I
192.168.178.25	172.64.155.209	31	18 kB	7	16	15 kB	15	3 kB	30.377588	3.1426	38 I
192.168.178.25	192.168.0.244	7	546 bytes	1	7	546 bytes	0	0 bytes	20.479881	7.0041	623 b
192.168.178.25	192.168.178.1	10	1 kB	5	5	408 bytes	5	624 bytes	29.659386	1.6156	2020 b
192.168.178.27	192.168.178.255	8	648 bytes	0	8	648 bytes	0	0 bytes	0.000000	41.5749	124 b

## CONVERSATION IPV4

A device (192.168.178.25) shows high throughput communication with multiple Cloudflare Ips this could be signs of malware beaconing or unauthorized software

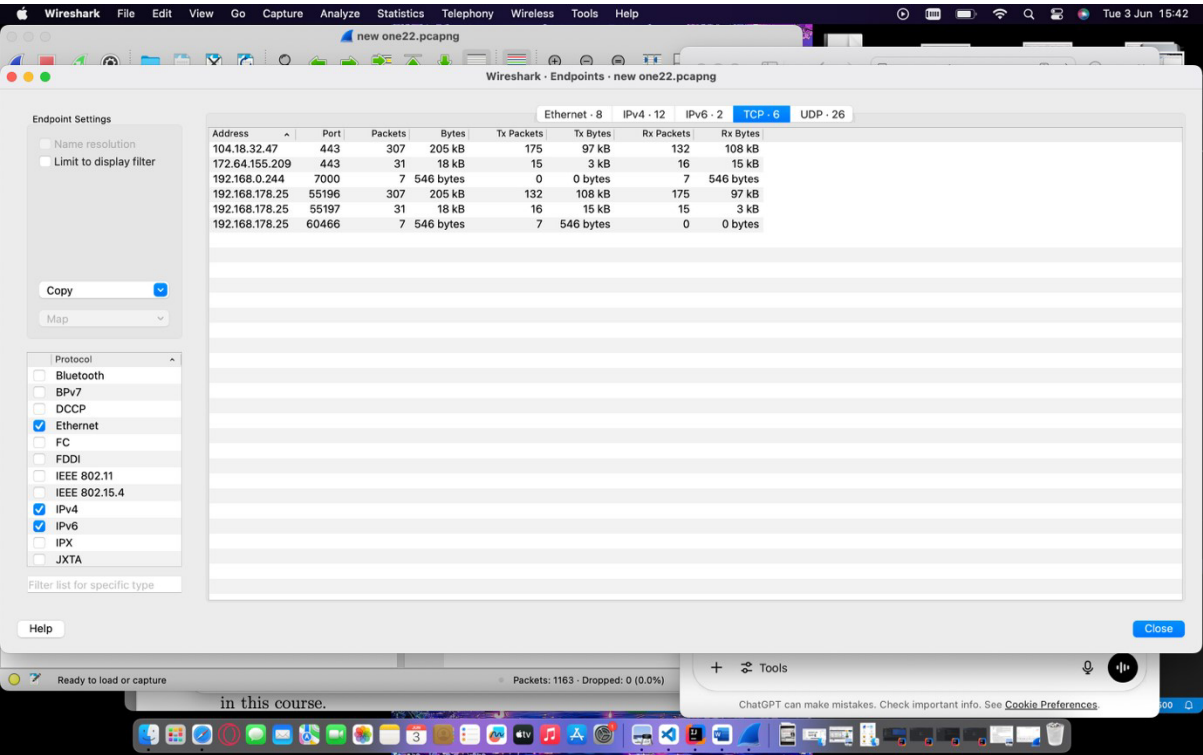
Conversation Settings											
<input type="checkbox"/> Name resolution <input type="checkbox"/> Absolute start time <input type="checkbox"/> Limit to display filter											
<input type="button" value="Copy"/> <input checked="" type="button" value="Follow Stream..."/> <input type="button" value="Graph..."/>											
Protocol <input type="checkbox"/> Bluetooth <input type="checkbox"/> BPv7 <input type="checkbox"/> DCCP <input checked="" type="checkbox"/> Ethernet <input type="checkbox"/> FC <input type="checkbox"/> FDDI <input type="checkbox"/> IEEE 802.11 <input type="checkbox"/> IEEE 802.15.4 <input checked="" type="checkbox"/> IPv4 <input checked="" type="checkbox"/> IPv6 <input type="checkbox"/> IPX <input type="checkbox"/> JXTA <input type="checkbox"/> LTP <input type="checkbox"/> MPTCP <input type="checkbox"/> NCP <input type="checkbox"/> openSAFETY <input type="checkbox"/> RSVP <input type="checkbox"/> SCTP											
Filter list for specific type											
<input type="button" value="Help"/> <input type="button" value="Close"/>											

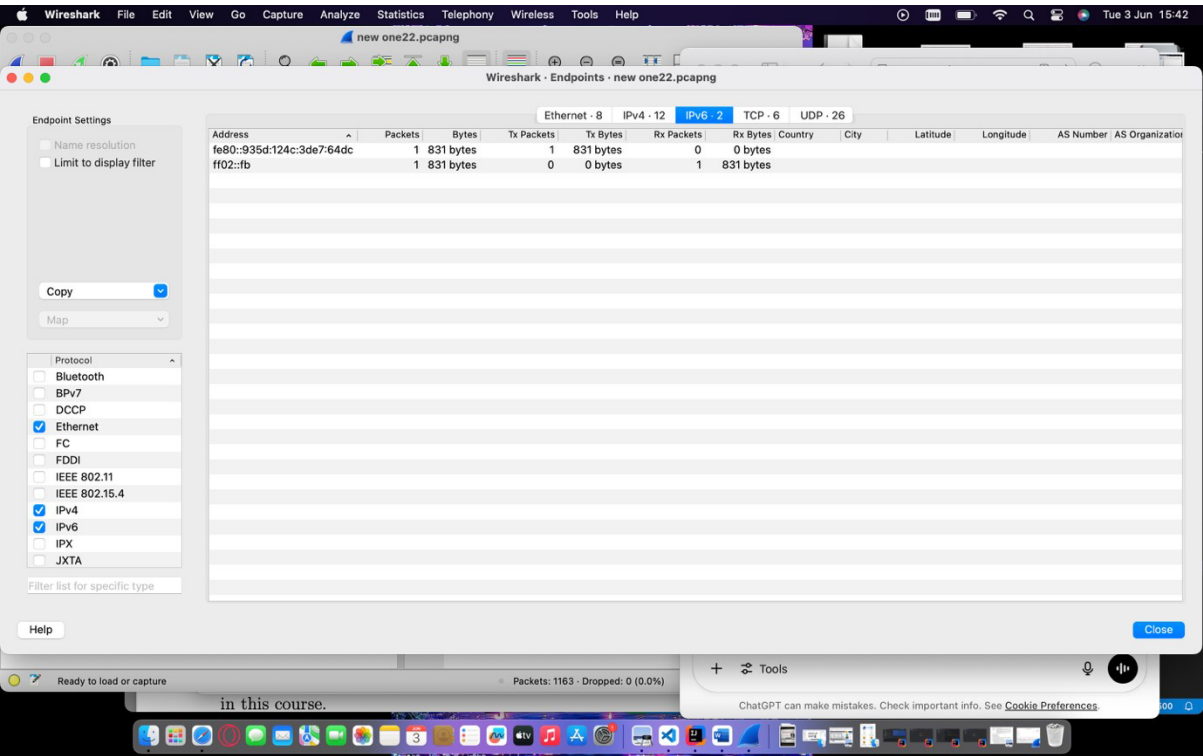
Ethernet - 6   IPv4 - 9 <b>IPv6 - 1</b> TCP - 3   UDP - 19											
Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s
fe80::935d:124c:3de7:64dc	ff02::fb	1	831 bytes	0	1	831 bytes	0	0 bytes	22.940850	0.0000	

CONVERSATION IPV6 shows only one packet but not really harmful

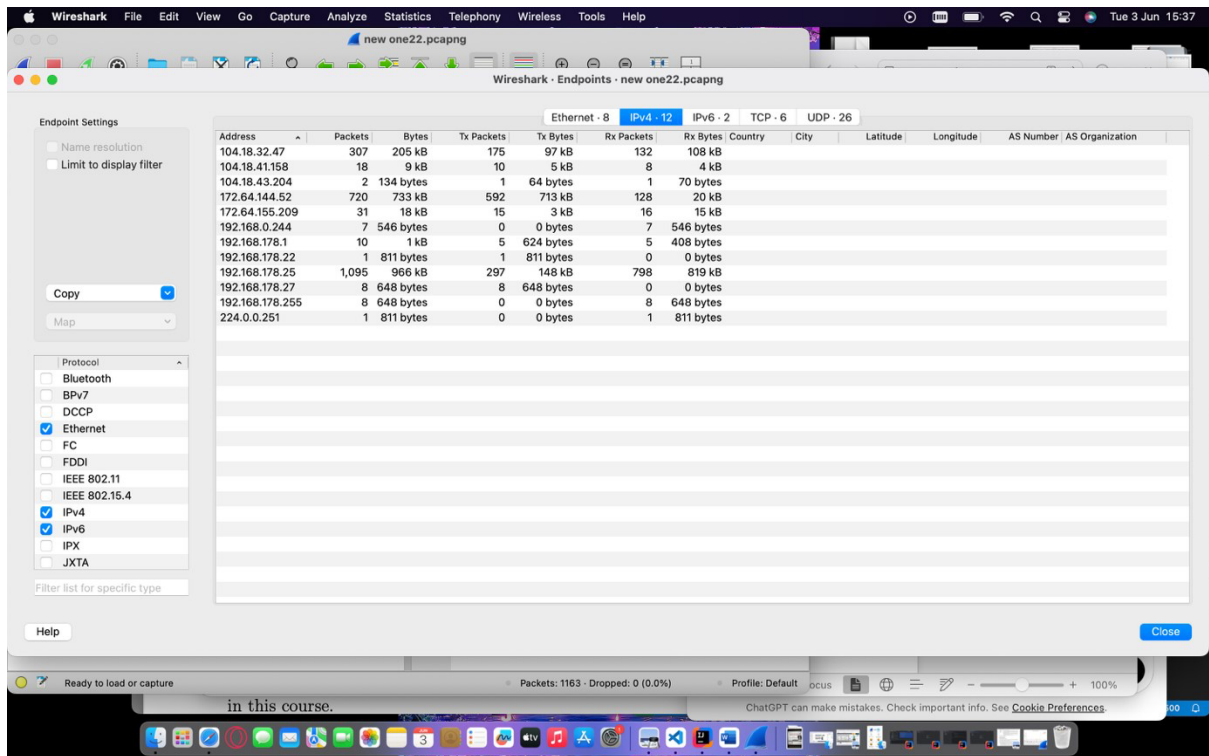
# ENDDPOINT STATISTICS



TCP Endpoints well encrypted doesn't raise any suspicious alarm



IPV6 shows no suspicious traffic



IP 192.168.178.25 is the main host and is responsible for 1095 packets and nearly 1mb of total traffic which shows it is very active

## FIREWALL DROP/PERMIT RULES

Action Source IP Destination IP Protocol Port Description

Drop	Any	192.168.178.25	TCP	443	Block external traffic from unknown host
PERMIT	192.168.178.0/24	Any	TCP	80	Allow free access to internal users

## CONCLUSION

From my analysis I can draw a conclusion that the packet volume, choice of port and external destination warrants an immediate containment and fire wall enforcement. And more monitoring analysis to protect against both known and stealth threats

LINK TO MY GITHUB REPOSITORY :

<https://github.com/mart23333/martinschizaramogowuihe.git>

## **BIOGRAPHY**

All about python(2021) :How to create a real time chat app in python using socket programming[video] Available at :

<https://youtu.be/hBnOdIg0jAM?si=njanWgq6sV40U0oh> (

Accessed : 28 may 2025)