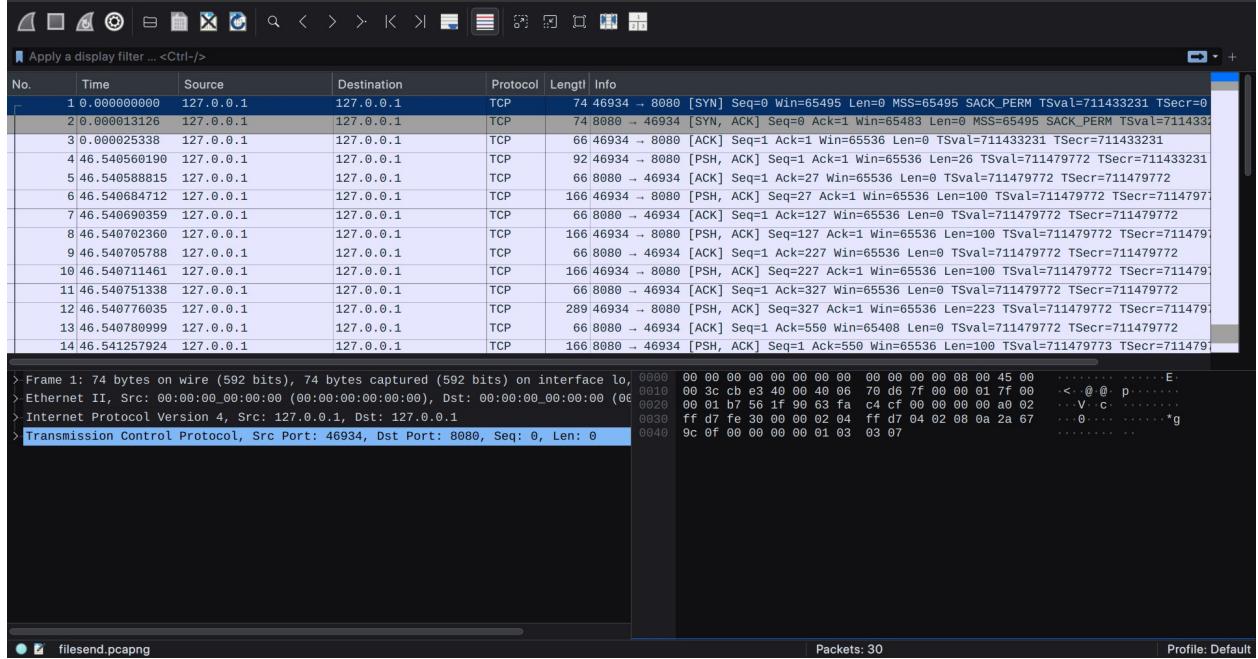


- What are the source and destination IP Addresses and ports ? Share the screenshots to justify your answer.

Both IP addresses are 127.0.0.1. The client port is 46934 and destination port is 8080.



- Inspect the three-way-handshaking procedure and capture all packets exchanged for it. Attach the necessary screenshots to demonstrate it.

In a 3-way handshake in TCP, 3 packets are exchanged between the server and the client -

- SYN : sent from client to server to initiate connection.
- SYN-ACK : server responds with a SYN-ACK packet to client.
- ACK : client sends it to server to confirm the connection.

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	127.0.0.1	127.0.0.1	TCP	74	46934 → 8080 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TStamp=711433231 TSecr=0
2	0.0000013126	127.0.0.1	127.0.0.1	TCP	74	8080 → 46934 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM TStamp=711433231 TSecr=711433231
3	0.0000025338	127.0.0.1	127.0.0.1	TCP	66	46934 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TStamp=711433231 TSecr=711433231
4	46.540560190	127.0.0.1	127.0.0.1	TCP	92	46934 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=26 TStamp=711479772 TSecr=711433231
5	46.540588815	127.0.0.1	127.0.0.1	TCP	66	8080 → 46934 [ACK] Seq=1 Ack=27 Win=65536 Len=0 TStamp=711479772 TSecr=711479772
6	46.540684712	127.0.0.1	127.0.0.1	TCP	166	46934 → 8080 [PSH, ACK] Seq=27 Ack=1 Win=65536 Len=100 TStamp=711479772 TSecr=711479772
7	46.540690359	127.0.0.1	127.0.0.1	TCP	66	8080 → 46934 [ACK] Seq=1 Ack=127 Win=65536 Len=0 TStamp=711479772 TSecr=711479772
8	46.540702360	127.0.0.1	127.0.0.1	TCP	166	46934 → 8080 [PSH, ACK] Seq=127 Ack=1 Win=65536 Len=100 TStamp=711479772 TSecr=711479772
9	46.540750788	127.0.0.1	127.0.0.1	TCP	66	8080 → 46934 [ACK] Seq=1 Ack=227 Win=65536 Len=0 TStamp=711479772 TSecr=711479772
10	46.540711461	127.0.0.1	127.0.0.1	TCP	166	46934 → 8080 [PSH, ACK] Seq=227 Ack=1 Win=65536 Len=100 TStamp=711479772 TSecr=711479772
11	46.540751338	127.0.0.1	127.0.0.1	TCP	66	8080 → 46934 [ACK] Seq=1 Ack=327 Win=65536 Len=0 TStamp=711479772 TSecr=711479772
12	46.540776035	127.0.0.1	127.0.0.1	TCP	289	46934 → 8080 [PSH, ACK] Seq=327 Ack=1 Win=65536 Len=223 TStamp=711479772 TSecr=711479772
13	46.540780999	127.0.0.1	127.0.0.1	TCP	66	8080 → 46934 [ACK] Seq=1 Ack=550 Win=65408 Len=0 TStamp=711479772 TSecr=711479772
14	46.541257924	127.0.0.1	127.0.0.1	TCP	166	8080 → 46934 [PSH, ACK] Seq=1 Ack=550 Win=65536 Len=100 TStamp=711479773 TSecr=711479773

```

Sequence Number (raw): 1677378767
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1010 .... = Header Length: 40 bytes (10)
> Flags: 0x002 (SYN)
Window: 65495
[Calculated window size: 65495]
Checksum: 0xe0e0 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Oper
> [timestamps]

```

Flags (tcp.flags), 12 bits

Packets: 30 | Profile: Default

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	127.0.0.1	127.0.0.1	TCP	74	46934 → 8080 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TStamp=711433231 TSecr=0
2	0.0000013126	127.0.0.1	127.0.0.1	TCP	74	8080 → 46934 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM TStamp=711433231 TSecr=711433231
3	0.0000025338	127.0.0.1	127.0.0.1	TCP	66	46934 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TStamp=711433231 TSecr=711433231
4	46.540560190	127.0.0.1	127.0.0.1	TCP	92	46934 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=26 TStamp=711479772 TSecr=711433231
5	46.540588815	127.0.0.1	127.0.0.1	TCP	66	8080 → 46934 [ACK] Seq=1 Ack=27 Win=65536 Len=0 TStamp=711479772 TSecr=711479772
6	46.540684712	127.0.0.1	127.0.0.1	TCP	166	46934 → 8080 [PSH, ACK] Seq=27 Ack=1 Win=65536 Len=100 TStamp=711479772 TSecr=711479772
7	46.540690359	127.0.0.1	127.0.0.1	TCP	66	8080 → 46934 [ACK] Seq=1 Ack=127 Win=65536 Len=0 TStamp=711479772 TSecr=711479772
8	46.540702360	127.0.0.1	127.0.0.1	TCP	166	46934 → 8080 [PSH, ACK] Seq=127 Ack=1 Win=65536 Len=100 TStamp=711479772 TSecr=711479772
9	46.540750788	127.0.0.1	127.0.0.1	TCP	66	8080 → 46934 [ACK] Seq=1 Ack=227 Win=65536 Len=0 TStamp=711479772 TSecr=711479772
10	46.540711461	127.0.0.1	127.0.0.1	TCP	166	46934 → 8080 [PSH, ACK] Seq=227 Ack=1 Win=65536 Len=100 TStamp=711479772 TSecr=711479772
11	46.540751338	127.0.0.1	127.0.0.1	TCP	66	8080 → 46934 [ACK] Seq=1 Ack=327 Win=65536 Len=0 TStamp=711479772 TSecr=711479772
12	46.540776035	127.0.0.1	127.0.0.1	TCP	289	46934 → 8080 [PSH, ACK] Seq=327 Ack=1 Win=65536 Len=223 TStamp=711479772 TSecr=711479772
13	46.540780999	127.0.0.1	127.0.0.1	TCP	66	8080 → 46934 [ACK] Seq=1 Ack=550 Win=65408 Len=0 TStamp=711479772 TSecr=711479772
14	46.541257924	127.0.0.1	127.0.0.1	TCP	166	8080 → 46934 [PSH, ACK] Seq=1 Ack=550 Win=65536 Len=100 TStamp=711479773 TSecr=711479773

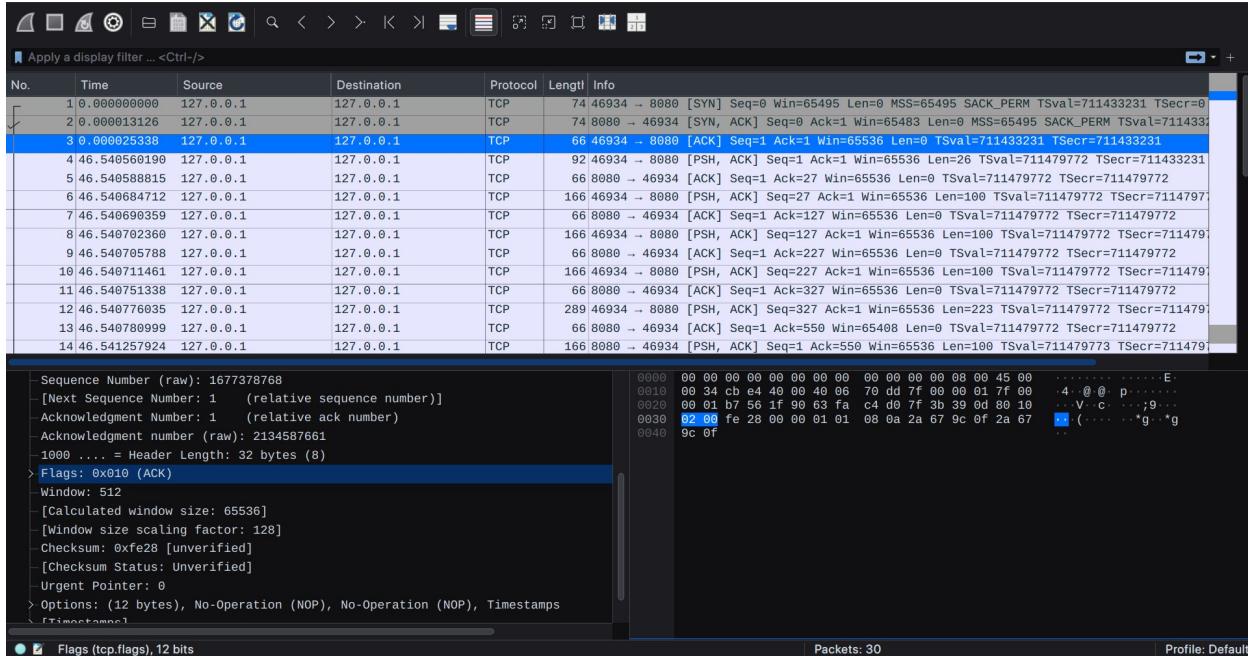
```

Sequence Number (raw): 2134587660
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1677378768
1010 .... = Header Length: 40 bytes (10)
> Flags: 0x012 (SYN, ACK)
Window: 65483
[Calculated window size: 65483]
Checksum: 0xe0e0 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Oper
> [timestamps]
< FIN/ACK analysis

```

Flags (tcp.flags), 12 bits

Packets: 30 | Profile: Default



3. Inspect the connection closure procedure and capture all packets exchanged for it.  
Attach the necessary screenshots to demonstrate it.

The three-packet connection closure sequence observed in Wireshark (FIN,ACK; FIN,ACK; ACK) can be explained through the analysis of the implemented client and server code. Here's a detailed breakdown of the connection termination process:

#### 1. Client-Initiated Connection Closure (First FIN,ACK):

When the client application completes its file transfer operations and the user chooses not to encrypt another file, the following code executes:

```
if (strcasecmp(choice, "No") == 0) {
    break;
}

close(sock);
```

This close() system call triggers the transmission of the initial FIN packet.

#### 2. Server Response and Closure (Second FIN,ACK):

The server detects the connection termination during its next read operation:

```
ssize_t key_bytes = read(client_sock, key, 26);

if (key_bytes <= 0) break; // Connection termination detected
```

Upon detection, the server executes:

```

close(client_sock);

close(server_fd);

```

This generates the second FIN,ACK packet.

### 3. Client's Final Acknowledgment (Third ACK):

The client's TCP stack automatically generates the final ACK packet in response to the server's FIN packet, completing the three-way connection termination.

No.	Time	Source	Destination	Protocol	Length	Info
18	46.541305991	127.0.0.1	127.0.0.1	TCP	166	8080 → 46934 [PSH, ACK] Seq=201 Ack=550 Win=65536 Len=100 TSval=711479773 TSecr=711479773
19	46.541310967	127.0.0.1	127.0.0.1	TCP	66	46934 → 8080 [ACK] Seq=550 Ack=301 Win=65536 Len=0 TSval=711479773 TSecr=711479773
20	46.541319986	127.0.0.1	127.0.0.1	TCP	166	8080 → 46934 [PSH, ACK] Seq=301 Ack=550 Win=65536 Len=100 TSval=711479773 TSecr=711479773
21	46.541324375	127.0.0.1	127.0.0.1	TCP	66	46934 → 8080 [ACK] Seq=550 Ack=401 Win=65536 Len=0 TSval=711479773 TSecr=711479773
22	46.541333572	127.0.0.1	127.0.0.1	TCP	166	8080 → 46934 [PSH, ACK] Seq=401 Ack=550 Win=65536 Len=100 TSval=711479773 TSecr=711479773
23	46.541338160	127.0.0.1	127.0.0.1	TCP	66	46934 → 8080 [ACK] Seq=550 Ack=501 Win=65536 Len=0 TSval=711479773 TSecr=711479773
24	46.541349107	127.0.0.1	127.0.0.1	TCP	85	8080 → 46934 [PSH, ACK] Seq=501 Ack=550 Win=65536 Len=19 TSval=711479773 TSecr=711479773
25	46.541353310	127.0.0.1	127.0.0.1	TCP	66	46934 → 8080 [ACK] Seq=550 Ack=520 Win=65536 Len=0 TSval=711479773 TSecr=711479773
26	46.541361839	127.0.0.1	127.0.0.1	TCP	70	8080 → 46934 [PSH, ACK] Seq=520 Ack=550 Win=65536 Len=4 TSval=711479773 TSecr=711479773
27	46.541378290	127.0.0.1	127.0.0.1	TCP	66	46934 → 8080 [ACK] Seq=550 Ack=524 Win=65536 Len=0 TSval=711479773 TSecr=711479773
28	51.841091376	127.0.0.1	127.0.0.1	TCP	66	46934 → 8080 [FIN, ACK] Seq=550 Ack=524 Win=65536 Len=0 TSval=711485072 TSecr=711479773
29	51.841227794	127.0.0.1	127.0.0.1	TCP	66	8080 → 46934 [FIN, ACK] Seq=524 Ack=551 Win=65536 Len=0 TSval=711485073 TSecr=711485073
30	51.841277898	127.0.0.1	127.0.0.1	TCP	66	46934 → 8080 [ACK] Seq=551 Ack=525 Win=65536 Len=0 TSval=711485073 TSecr=711485073

[Next Sequence Number: 551 (relative sequence number)]  
Acknowledgment Number: 524 (relative ack number)  
Acknowledgment number (raw): 2134588184  
1000 .... = Header Length: 32 bytes (8)  
> Flags: 0x011 (FIN, ACK)  
Window: 512  
[Calculated window size: 65536]  
[Window size scaling factor: 128]  
Checksum: 0xfe28 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps  
> [Timestamps]

Packets: 30 Profile: Default

No.	Time	Source	Destination	Protocol	Length	Info
18	46.541305991	127.0.0.1	127.0.0.1	TCP	166	8080 → 46934 [PSH, ACK] Seq=201 Ack=550 Win=65536 Len=100 TSval=711479773 TSecr=711479773
19	46.541310967	127.0.0.1	127.0.0.1	TCP	66	46934 → 8080 [ACK] Seq=550 Ack=301 Win=65536 Len=0 TSval=711479773 TSecr=711479773
20	46.541319986	127.0.0.1	127.0.0.1	TCP	166	8080 → 46934 [PSH, ACK] Seq=301 Ack=550 Win=65536 Len=100 TSval=711479773 TSecr=711479773
21	46.541324375	127.0.0.1	127.0.0.1	TCP	66	46934 → 8080 [ACK] Seq=550 Ack=401 Win=65536 Len=0 TSval=711479773 TSecr=711479773
22	46.541333572	127.0.0.1	127.0.0.1	TCP	166	8080 → 46934 [PSH, ACK] Seq=401 Ack=550 Win=65536 Len=100 TSval=711479773 TSecr=711479773
23	46.541338160	127.0.0.1	127.0.0.1	TCP	66	46934 → 8080 [ACK] Seq=550 Ack=501 Win=65536 Len=0 TSval=711479773 TSecr=711479773
24	46.541349107	127.0.0.1	127.0.0.1	TCP	85	8080 → 46934 [PSH, ACK] Seq=501 Ack=550 Win=65536 Len=19 TSval=711479773 TSecr=711479773
25	46.541353310	127.0.0.1	127.0.0.1	TCP	66	46934 → 8080 [ACK] Seq=550 Ack=520 Win=65536 Len=0 TSval=711479773 TSecr=711479773
26	46.541361839	127.0.0.1	127.0.0.1	TCP	70	8080 → 46934 [PSH, ACK] Seq=520 Ack=550 Win=65536 Len=4 TSval=711479773 TSecr=711479773
27	46.541378290	127.0.0.1	127.0.0.1	TCP	66	46934 → 8080 [ACK] Seq=550 Ack=524 Win=65536 Len=0 TSval=711479773 TSecr=711479773
28	51.841091376	127.0.0.1	127.0.0.1	TCP	66	46934 → 8080 [FIN, ACK] Seq=550 Ack=524 Win=65536 Len=0 TSval=711485072 TSecr=711479773
29	51.841227794	127.0.0.1	127.0.0.1	TCP	66	8080 → 46934 [FIN, ACK] Seq=524 Ack=551 Win=65536 Len=0 TSval=711485073 TSecr=711485073
30	51.841277898	127.0.0.1	127.0.0.1	TCP	66	46934 → 8080 [ACK] Seq=551 Ack=525 Win=65536 Len=0 TSval=711485073 TSecr=711485073

Acknowledgment Number: 551 (relative ack number)  
Acknowledgment number (raw): 1677379318  
1000 .... = Header Length: 32 bytes (8)  
> Flags: 0x011 (FIN, ACK)  
Window: 512  
[Calculated window size: 65536]  
[Window size scaling factor: 128]  
Checksum: 0xfe28 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps  
> [Timestamps]  
> [SEQ/ACK analysis]

Packets: 30 Profile: Default

Wireshark Network Traffic Analysis

Selected Packet: 30 (Index 30)

Flags: `0x010 (ACK)`

Window: 512

[Calculated window size: 65536]

[Window size scaling factor: 128]

Checksum: `0xfe28 [unverified]`

[Checksum Status: Unverified]

Urgent Pointer: 0

> Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

> [Timestamps]

> [SEQ/ACK analysis]

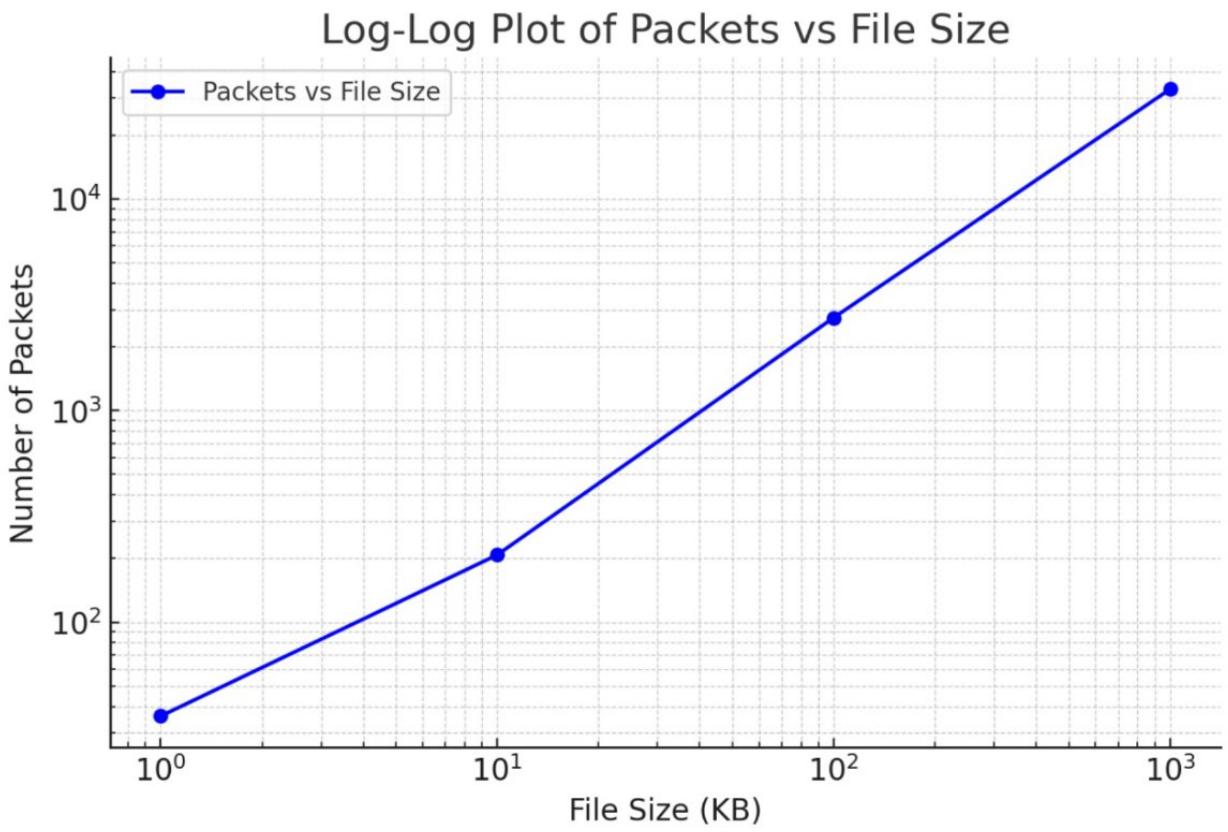
Flags (tcp.flags), 12 bits

Packets: 30

Profile: Default

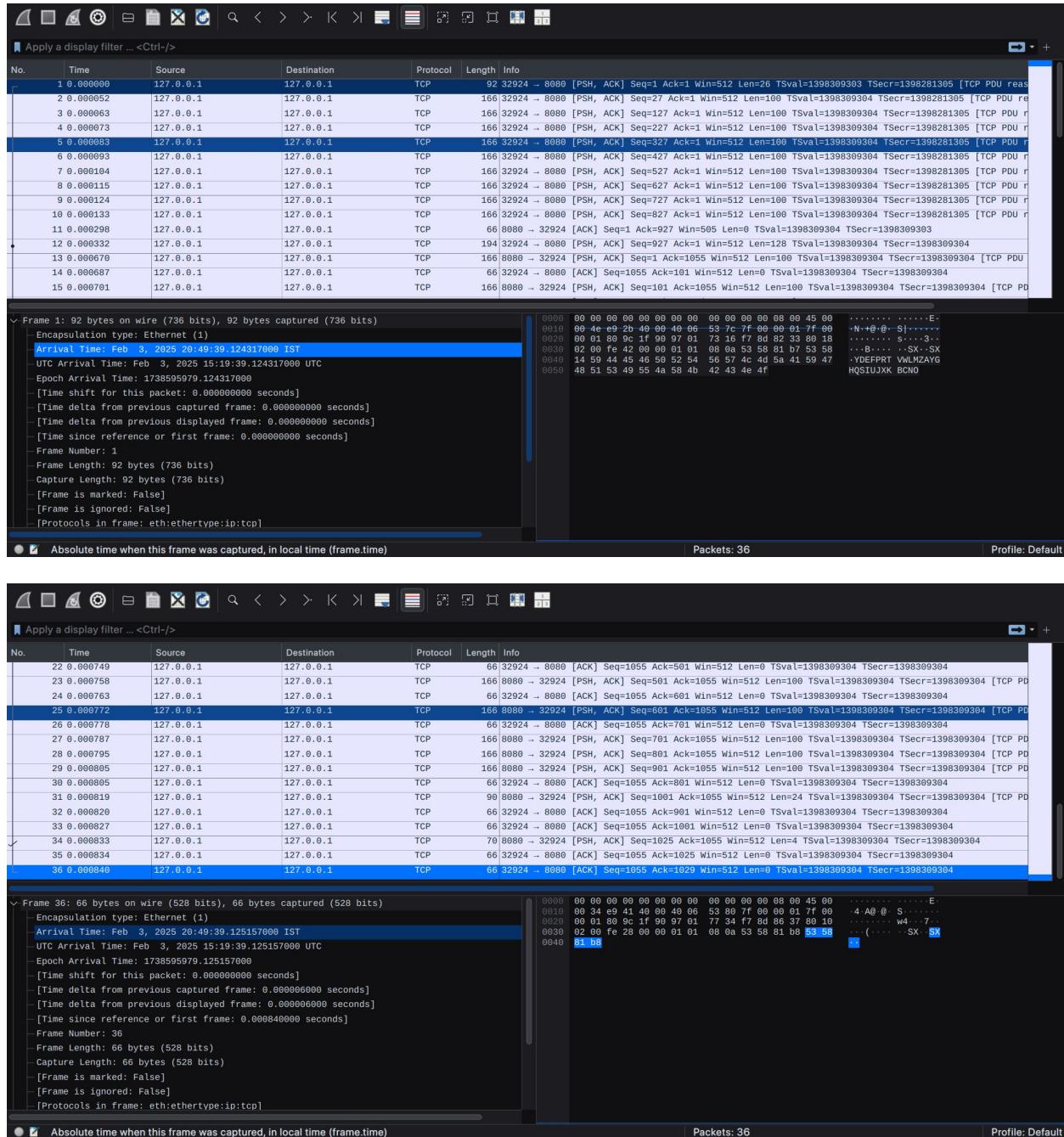
4. Inspect the traffics and count the number of packets exchanged for transfer of a file(related to data only) between client and server. Plot a graph “file size vs the number of packets” clearly based on your observation.

The screenshots are given in the next question



The

5. Measure the total time taken for the file transfer, its encryption and send it back from server to the client. Plot a graph “file size versus time” clearly based on your observation and also attach the necessary screenshots.



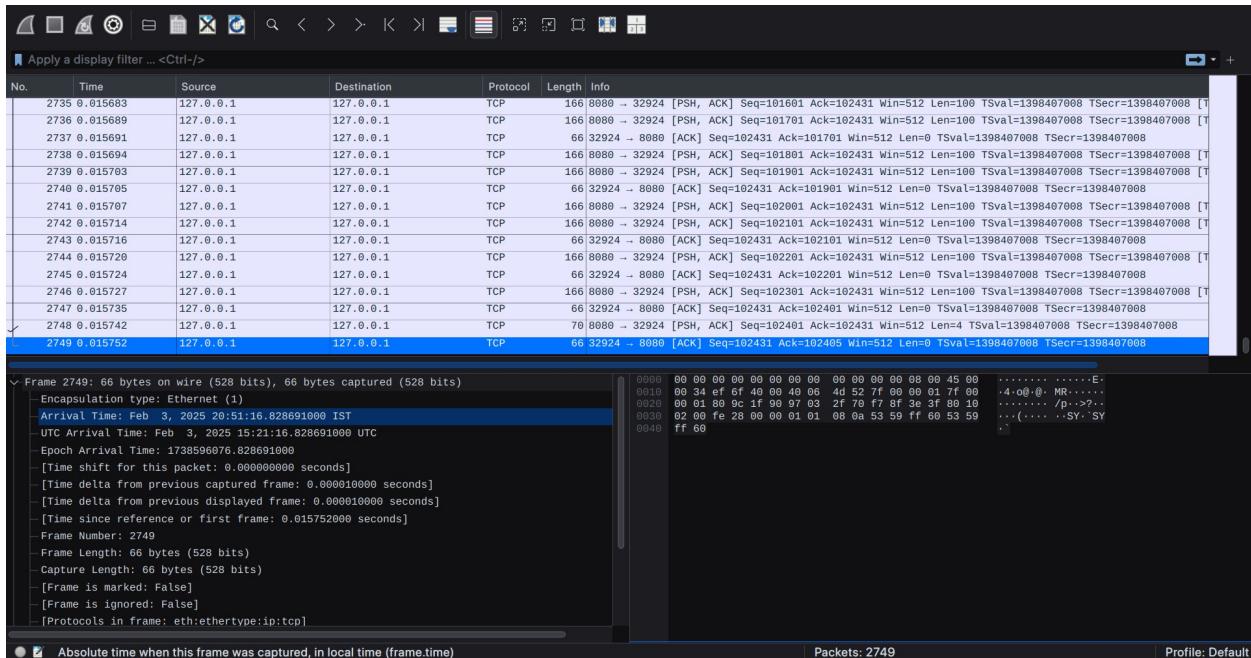
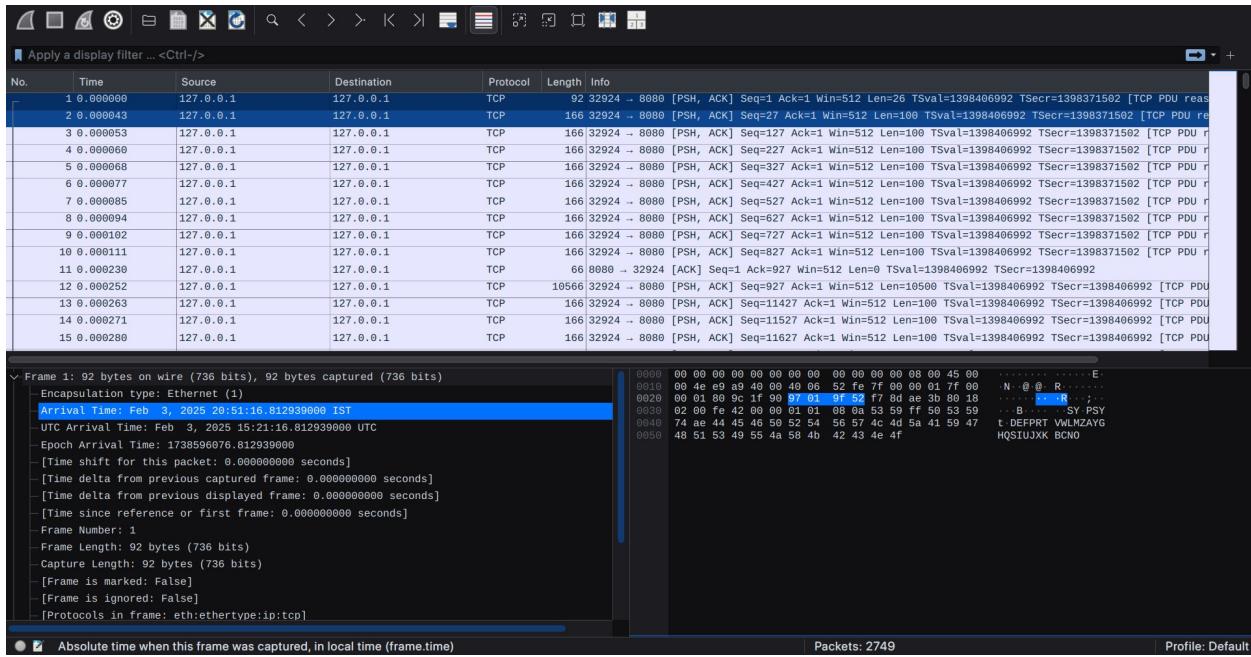
These two show the start and end times for a 1 KB packet.

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
194	0.002646	127.0.0.1	127.0.0.1	TCP	166	8080 → 32924 [PSH, ACK] Seq=9701 Ack=10271 Win=512 Len=100 TStamp=1398371502 TSecr=1398371502 [TCP]
195	0.002649	127.0.0.1	127.0.0.1	TCP	66	32924 → 8080 [ACK] Seq=10271 Ack=9701 Win=512 Len=0 TStamp=1398371502 TSecr=1398371502
196	0.002660	127.0.0.1	127.0.0.1	TCP	166	8080 → 32924 [PSH, ACK] Seq=9801 Ack=10271 Win=512 Len=100 TStamp=1398371502 TSecr=1398371502 [TCP]
197	0.002663	127.0.0.1	127.0.0.1	TCP	66	32924 → 8080 [ACK] Seq=10271 Ack=9801 Win=512 Len=0 TStamp=1398371502 TSecr=1398371502
198	0.002669	127.0.0.1	127.0.0.1	TCP	166	8080 → 32924 [PSH, ACK] Seq=9901 Ack=10271 Win=512 Len=100 TStamp=1398371502 TSecr=1398371502 [TCP]
199	0.002673	127.0.0.1	127.0.0.1	TCP	66	32924 → 8080 [ACK] Seq=10271 Ack=9901 Win=512 Len=0 TStamp=1398371502 TSecr=1398371502
200	0.002682	127.0.0.1	127.0.0.1	TCP	166	8080 → 32924 [PSH, ACK] Seq=10001 Ack=10271 Win=512 Len=100 TStamp=1398371502 TSecr=1398371502 [TCP]
201	0.002685	127.0.0.1	127.0.0.1	TCP	66	32924 → 8080 [ACK] Seq=10271 Ack=10001 Win=512 Len=0 TStamp=1398371502 TSecr=1398371502
202	0.002692	127.0.0.1	127.0.0.1	TCP	166	8080 → 32924 [PSH, ACK] Seq=10101 Ack=10271 Win=512 Len=100 TStamp=1398371502 TSecr=1398371502 [TCP]
203	0.002696	127.0.0.1	127.0.0.1	TCP	66	32924 → 8080 [ACK] Seq=10271 Ack=10101 Win=512 Len=0 TStamp=1398371502 TSecr=1398371502
204	0.002707	127.0.0.1	127.0.0.1	TCP	166	8080 → 32924 [PSH, ACK] Seq=10269 Ack=10271 Win=512 Len=40 TStamp=1398371502 TSecr=1398371502 [TCP]
205	0.002708	127.0.0.1	127.0.0.1	TCP	66	32924 → 8080 [ACK] Seq=10271 Ack=10201 Win=512 Len=0 TStamp=1398371502 TSecr=1398371502
206	0.002718	127.0.0.1	127.0.0.1	TCP	70	8080 → 32924 [PSH, ACK] Seq=10241 Ack=10271 Win=512 Len=4 TStamp=1398371502 TSecr=1398371502
207	0.002721	127.0.0.1	127.0.0.1	TCP	66	32924 → 8080 [ACK] Seq=10271 Ack=10241 Win=512 Len=0 TStamp=1398371502 TSecr=1398371502
208	0.002732	127.0.0.1	127.0.0.1	TCP	66	32924 → 8080 [ACK] Seq=10271 Ack=10245 Win=512 Len=0 TStamp=1398371502 TSecr=1398371502

Frame 208: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)  
Encapsulation type: Ethernet (1)  
Arrival Time: Feb 3, 2025 20:50:41.322560000 IST  
UTC Arrival Time: Feb 3, 2025 15:20:41.322560000 UTC  
Epoch Arrival Time: 1788596041.322560000  
[Time shift for this packet: 0.000000000 seconds]  
[Time delta from previous captured frame: 0.000011000 seconds]  
[Time delta from previous displayed frame: 0.000011000 seconds]  
[Time since reference or first frame: 0.002732000 seconds]  
Frame Number: 208  
Frame Length: 66 bytes (528 bits)  
Capture Length: 66 bytes (528 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ethertype:ip:tcp]  
Absolute time when this frame was captured, in local time (frame.time)

These show for the start and end of the process for a 10 KB packet.



These show for the start and end of a 100 KB packet.

Apply a display filter ... <Ctrl+>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	TCP	92	33810 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=512 Len=26 TSval=3779785218 TSscr=3779764431 [TCP PDU reas...
2	0.000096	127.0.0.1	127.0.0.1	TCP	166	33810 → 8080 [PSH, ACK] Seq=27 Ack=1 Win=512 Len=100 TSval=3779785218 TSscr=3779764431 [TCP PDU r...
3	0.000114	127.0.0.1	127.0.0.1	TCP	166	33810 → 8080 [PSH, ACK] Seq=127 Ack=2 Win=512 Len=100 TSval=3779785218 TSscr=3779764431 [TCP PDU r...
4	0.000131	127.0.0.1	127.0.0.1	TCP	166	33810 → 8080 [PSH, ACK] Seq=227 Ack=1 Win=512 Len=100 TSval=3779785218 TSscr=3779764431 [TCP PDU r...
5	0.000151	127.0.0.1	127.0.0.1	TCP	166	33810 → 8080 [PSH, ACK] Seq=327 Ack=1 Win=512 Len=100 TSval=3779785218 TSscr=3779764431 [TCP PDU r...
6	0.000164	127.0.0.1	127.0.0.1	TCP	166	33810 → 8080 [PSH, ACK] Seq=427 Ack=1 Win=512 Len=100 TSval=3779785218 TSscr=3779764431 [TCP PDU r...
7	0.000177	127.0.0.1	127.0.0.1	TCP	166	33810 → 8080 [PSH, ACK] Seq=527 Ack=1 Win=512 Len=100 TSval=3779785218 TSscr=3779764431 [TCP PDU r...
8	0.000192	127.0.0.1	127.0.0.1	TCP	166	33810 → 8080 [PSH, ACK] Seq=627 Ack=1 Win=512 Len=100 TSval=3779785218 TSscr=3779764431 [TCP PDU r...
9	0.000205	127.0.0.1	127.0.0.1	TCP	166	33810 → 8080 [PSH, ACK] Seq=727 Ack=1 Win=512 Len=100 TSval=3779785218 TSscr=3779764431 [TCP PDU r...
10	0.000218	127.0.0.1	127.0.0.1	TCP	166	33810 → 8080 [PSH, ACK] Seq=827 Ack=1 Win=512 Len=100 TSval=3779785218 TSscr=3779764431 [TCP PDU r...
11	0.000468	127.0.0.1	127.0.0.1	TCP	66	8080 → 33810 [ACK] Seq=1 Ack=927 Win=505 Len=0 TSval=3779785218 TSscr=3779785218 [TCP PDU r...
12	0.000561	127.0.0.1	127.0.0.1	TCP	1166	33810 → 8080 [PSH, ACK] Seq=927 Ack=1 Win=512 Len=11600 TSval=3779785218 TSscr=3779785218 [TCP PDU r...
13	0.000584	127.0.0.1	127.0.0.1	TCP	166	33810 → 8080 [PSH, ACK] Seq=12527 Ack=1 Win=512 Len=100 TSval=3779785218 TSscr=3779785218 [TCP PDU r...
14	0.000613	127.0.0.1	127.0.0.1	TCP	166	33810 → 8080 [PSH, ACK] Seq=12627 Ack=1 Win=512 Len=100 TSval=3779785219 TSscr=3779785218 [TCP PDU r...
15	0.000636	127.0.0.1	127.0.0.1	TCP	66	8080 → 33810 [ACK] Seq=1 Ack=12627 Win=429 Len=9 TSval=3779785219 TSscr=3779785218

Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)

Encapsulation type: Ethernet (1)

Arrival Time: Feb 3, 2025 21:49:55.454722000 IST

UTC Arrival Time: Feb 3, 2025 16:19:55.454722000 UTC

Epoch Arrival Time: 1738599595.454722000

[Time shift for this packet: 0.000000000 seconds]

[Time delta from previous captured frame: 0.000000000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 0.000000000 seconds]

Frame Number: 1

Frame Length: 92 bytes (736 bits)

Capture Length: 92 bytes (736 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp]

Apply a display filter... <Ctrl>->

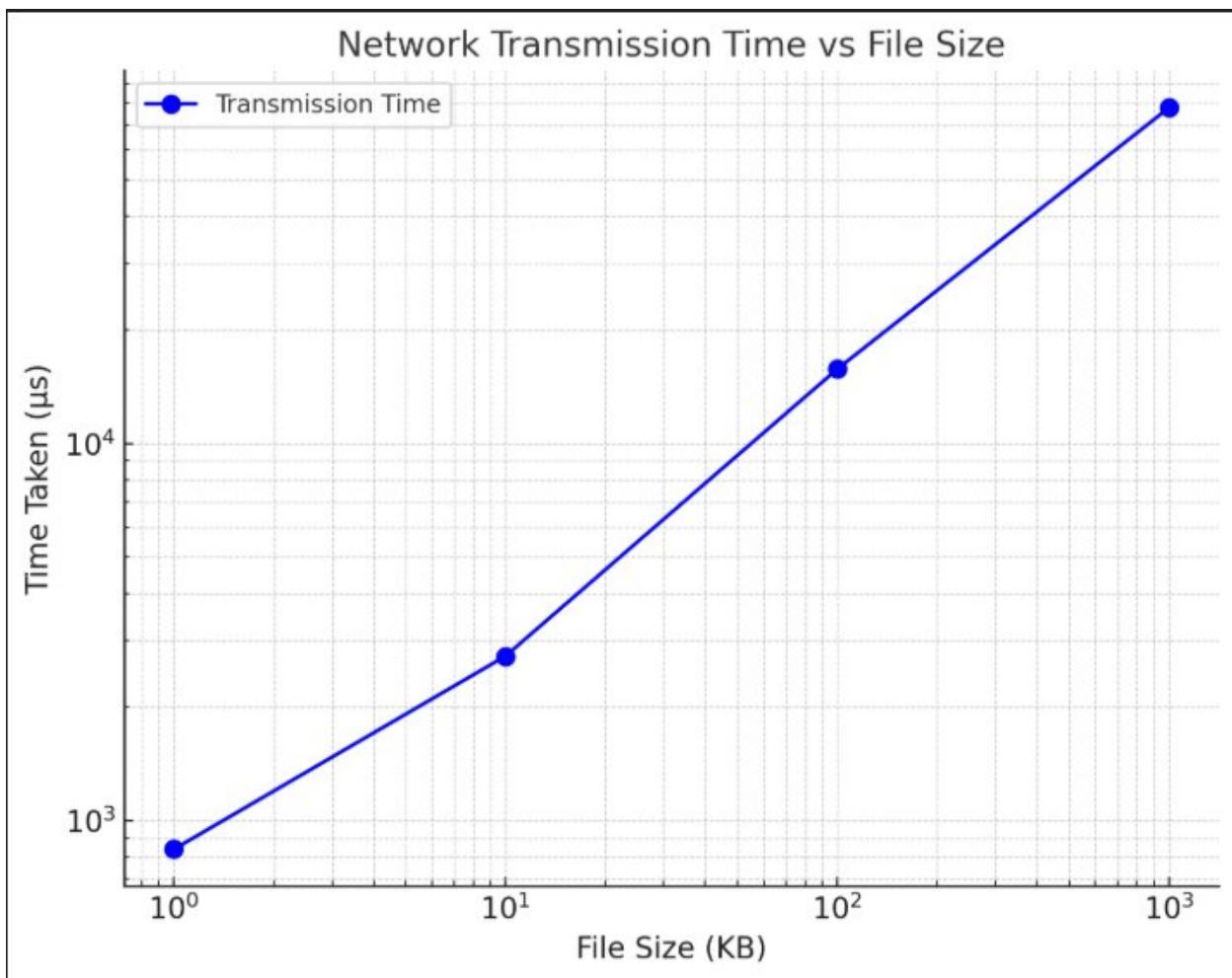
No.	Time	Source	Destination	Protocol	Length	Info
33053	0.077638	127.0.0.1	127.0.0.1	TCP	66	33810 → 8088 [ACK] Seq=1048607 Ack=1047901 Win=512 Len=0 Tsvl=3779785296 Tscr=3779785296
33054	0.077638	127.0.0.1	127.0.0.1	TCP	166	8080 → 33810 [PSH, ACK] Seq=1047901 Ack=1048607 Win=512 Len=100 Tsvl=3779785296 Tscr=3779785296
33055	0.077640	127.0.0.1	127.0.0.1	TCP	66	33810 → 8088 [ACK] Seq=1048607 Ack=1048901 Win=512 Len=0 Tsvl=3779785296 Tscr=3779785296
33056	0.077641	127.0.0.1	127.0.0.1	TCP	166	8080 → 33810 [PSH, ACK] Seq=1048901 Ack=1048607 Win=512 Len=100 Tsvl=3779785296 Tscr=3779785296
33057	0.077643	127.0.0.1	127.0.0.1	TCP	66	33810 → 8088 [ACK] Seq=1048607 Ack=1048101 Win=512 Len=0 Tsvl=3779785296 Tscr=3779785296
33058	0.077643	127.0.0.1	127.0.0.1	TCP	166	8080 → 33810 [PSH, ACK] Seq=1048101 Ack=1048607 Win=512 Len=100 Tsvl=3779785296 Tscr=3779785296
33059	0.077645	127.0.0.1	127.0.0.1	TCP	66	33810 → 8088 [ACK] Seq=1048607 Ack=1048261 Win=512 Len=0 Tsvl=3779785296 Tscr=3779785296
33060	0.077646	127.0.0.1	127.0.0.1	TCP	166	8080 → 33810 [PSH, ACK] Seq=1048261 Ack=1048607 Win=512 Len=100 Tsvl=3779785296 Tscr=3779785296
33061	0.077649	127.0.0.1	127.0.0.1	TCP	166	8080 → 33810 [PSH, ACK] Seq=1048301 Ack=1048607 Win=512 Len=100 Tsvl=3779785296 Tscr=3779785296
33062	0.077649	127.0.0.1	127.0.0.1	TCP	66	33810 → 8088 [ACK] Seq=1048607 Ack=1048301 Win=512 Len=0 Tsvl=3779785296 Tscr=3779785296
33063	0.077652	127.0.0.1	127.0.0.1	TCP	66	33810 → 8088 [ACK] Seq=1048607 Ack=1048401 Win=512 Len=0 Tsvl=3779785296 Tscr=3779785296
33064	0.077652	127.0.0.1	127.0.0.1	TCP	166	8080 → 33810 [PSH, ACK] Seq=1048401 Ack=1048607 Win=512 Len=100 Tsvl=3779785296 Tscr=3779785296
33065	0.077654	127.0.0.1	127.0.0.1	TCP	66	33810 → 8088 [ACK] Seq=1048607 Ack=1048501 Win=512 Len=0 Tsvl=3779785296 Tscr=3779785296
33066	0.077658	127.0.0.1	127.0.0.1	TCP	142	8080 → 33810 [PSH, ACK] Seq=1048501 Ack=1048607 Win=512 Len=76 Tsvl=3779785296 Tscr=3779785296
33067	0.077661	127.0.0.1	127.0.0.1	TCP	78	8080 → 33810 [PSH, ACK] Seq=1048577 Ack=1048607 Win=512 Len=4 Tsvl=3779785296 Tscr=3779785296

Frame 33067: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)  
Encapsulation type: Ethernet (1)  
Arrival Time: Feb 3, 2025 21:49:55.532383000 IST  
UTC Arrival Time: Feb 3, 2025 16:19:55.532383000 UTC  
Epoch Arrival Time: 1738599595.532383000  
[Time shift for this packet: 0.000000000 seconds]  
[Time delta from previous captured frame: 0.000003000 seconds]  
[Time delta from previous displayed frame: 0.000003000 seconds]  
[Time since reference or first frame: 0.077661000 seconds]  
Frame Number: 33067  
Frame Length: 70 bytes (560 bits)  
Capture Length: 70 bytes (560 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ethertype:ip:tcp]

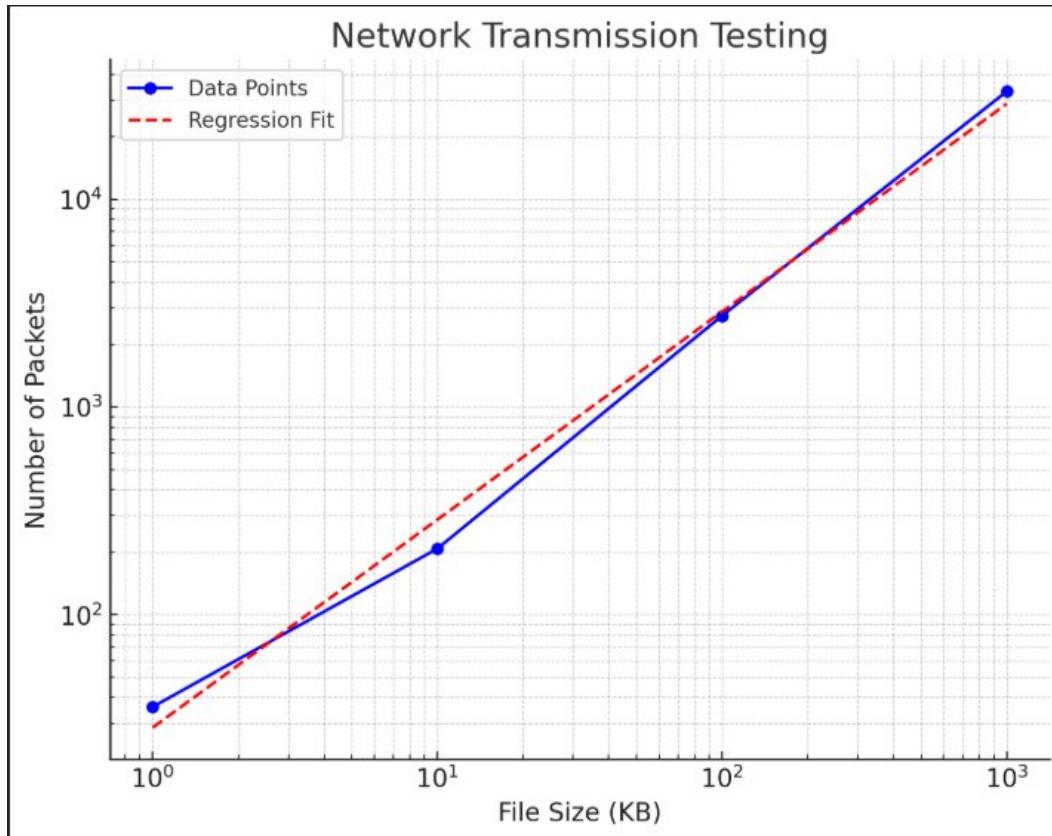
0000	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 45 00	..-.-.-----E-
0010	00 38 bd f9 40 40 4d	7e c4 7f 00 00 01 7f 00	-B-B@..-----
0020	00 01 1f 94 84 12 bd ce	b1 2b 86 2f 5f a8 09 18	..!+..-----
0030	02 00 fe 2c 00 01 01 08	0a e1 4a f2 50 e1 4a	..J-P-J
0040	f2 56 45 f4 46 0a		.PEOF.

Frame (70 bytes) Reassembled TCP (1048580 bytes)

These show for the start and end of the process for a 1 MB packet.



6. Calculate the average size packet exchanged during data communication? Take reference of the plotted graph in the above question.



From the best fit line, the average packet size is 71.04 bytes(ignore stuff other than my data that are sent in the packets, like headers etc).