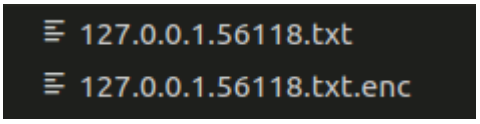
Academic Session 2024-2025
Spring Semester

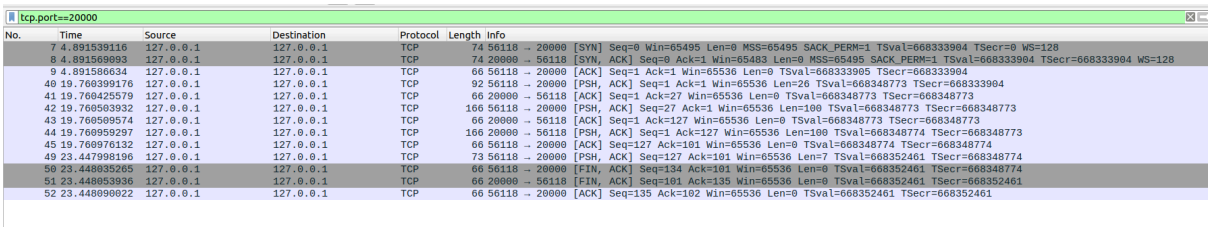
Computer Networks Lab
Assignment 3: TCP Sockets

More Aayush Babasaheb **(22CS30063)**

1.

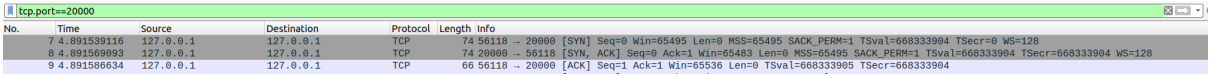
Server IP address: 127.0.0.1
Server port: 20000
Client IP address: 127.0.0.1
Client port: 56118




tcp.port==20000

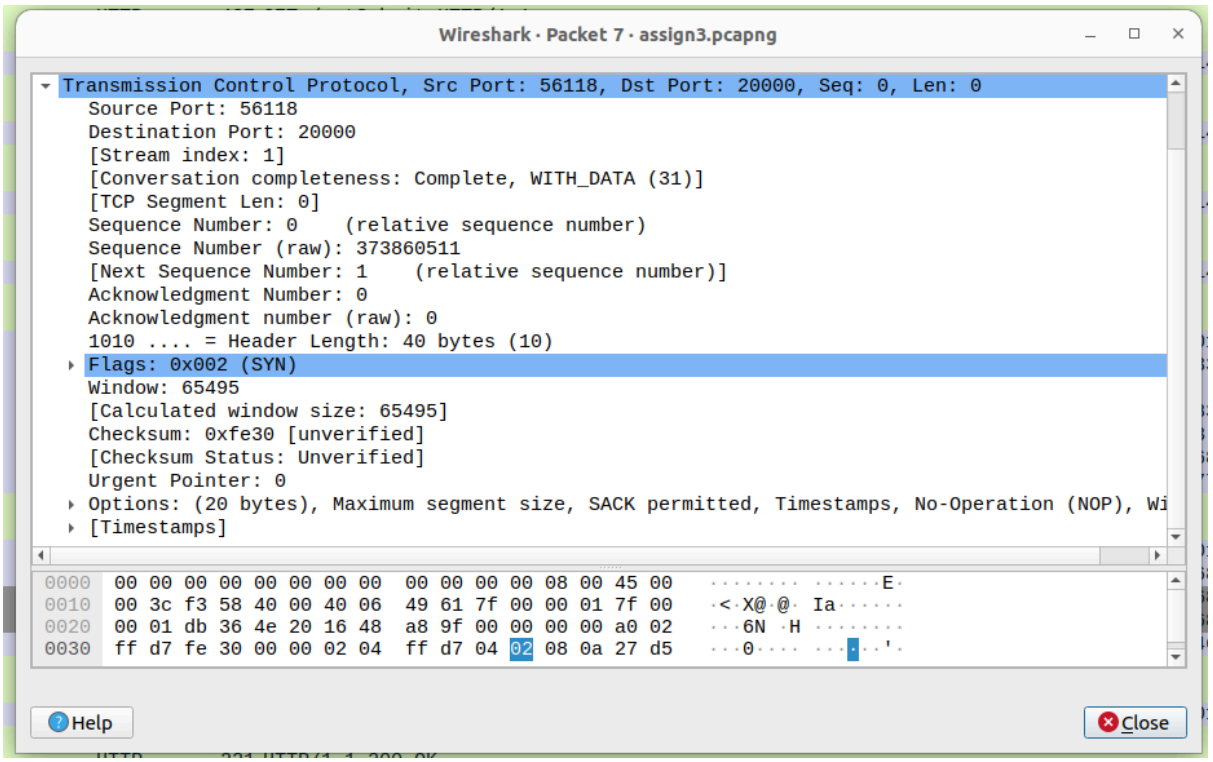
No.	Time	Source	Destination	Protocol	Length	Info
7	4.891539116	127.0.0.1	127.0.0.1	TCP	74	56118 → 20000 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=668333904 TSecr=0 WS=128
8	4.891569093	127.0.0.1	127.0.0.1	TCP	74	20000 → 56118 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=668333904 TSecr=668333904 WS=128
9	4.891586634	127.0.0.1	127.0.0.1	TCP	66	56118 → 20000 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=668333905 TSecr=668333904
40	19.760399176	127.0.0.1	127.0.0.1	TCP	92	56118 → 20000 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=26 TSval=668348773 TSecr=668333904
41	19.760425579	127.0.0.1	127.0.0.1	TCP	66	20000 → 56118 [ACK] Seq=1 Ack=27 Win=65536 Len=0 TSval=668348773 TSecr=668348773
42	19.760503932	127.0.0.1	127.0.0.1	TCP	166	56118 → 20000 [PSH, ACK] Seq=27 Ack=1 Win=65536 Len=100 TSval=668348773 TSecr=668348773
43	19.760509574	127.0.0.1	127.0.0.1	TCP	66	20000 → 56118 [ACK] Seq=1 Ack=127 Win=65536 Len=0 TSval=668348773 TSecr=668348773
44	19.760959297	127.0.0.1	127.0.0.1	TCP	166	20000 → 56118 [PSH, ACK] Seq=1 Ack=127 Win=65536 Len=100 TSval=668348774 TSecr=668348773
45	19.760976132	127.0.0.1	127.0.0.1	TCP	66	56118 → 20000 [ACK] Seq=127 Ack=101 Win=65536 Len=0 TSval=668348774 TSecr=668348774
49	23.447998196	127.0.0.1	127.0.0.1	TCP	73	56118 → 20000 [PSH, ACK] Seq=127 Ack=101 Win=65536 Len=7 TSval=668352461 TSecr=668348774
50	23.448035265	127.0.0.1	127.0.0.1	TCP	66	56118 → 20000 [FIN, ACK] Seq=134 Ack=101 Win=65536 Len=0 TSval=668352461 TSecr=668348774
51	23.448053936	127.0.0.1	127.0.0.1	TCP	66	20000 → 56118 [FIN, ACK] Seq=101 Ack=135 Win=65536 Len=0 TSval=668352461 TSecr=668352461
52	23.448090022	127.0.0.1	127.0.0.1	TCP	66	56118 → 20000 [ACK] Seq=135 Ack=102 Win=65536 Len=0 TSval=668352461 TSecr=668352461

2.

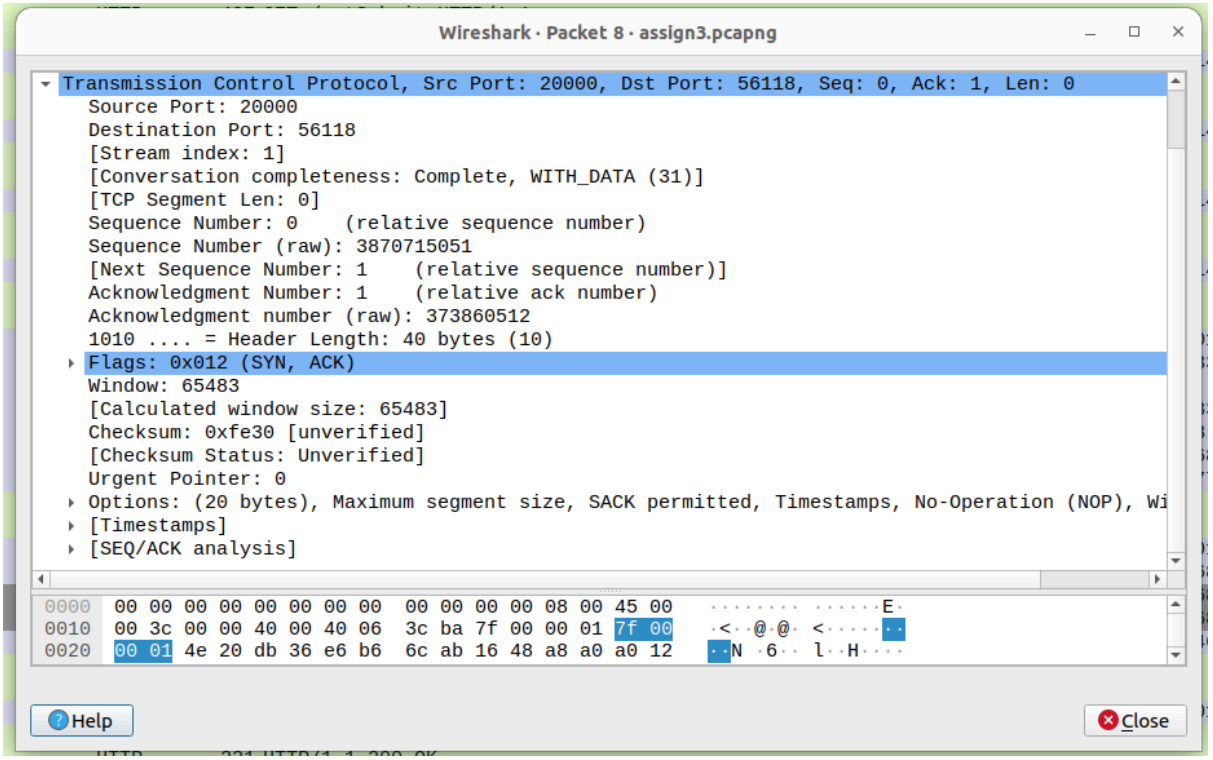

tcp.port==20000

No.	Time	Source	Destination	Protocol	Length	Info
7	4.891539116	127.0.0.1	127.0.0.1	TCP	74	56118 → 20000 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=668333904 TSecr=0 WS=128
8	4.891569093	127.0.0.1	127.0.0.1	TCP	74	20000 → 56118 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=668333904 TSecr=668333904 WS=128
9	4.891586634	127.0.0.1	127.0.0.1	TCP	66	56118 → 20000 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=668333905 TSecr=668333904

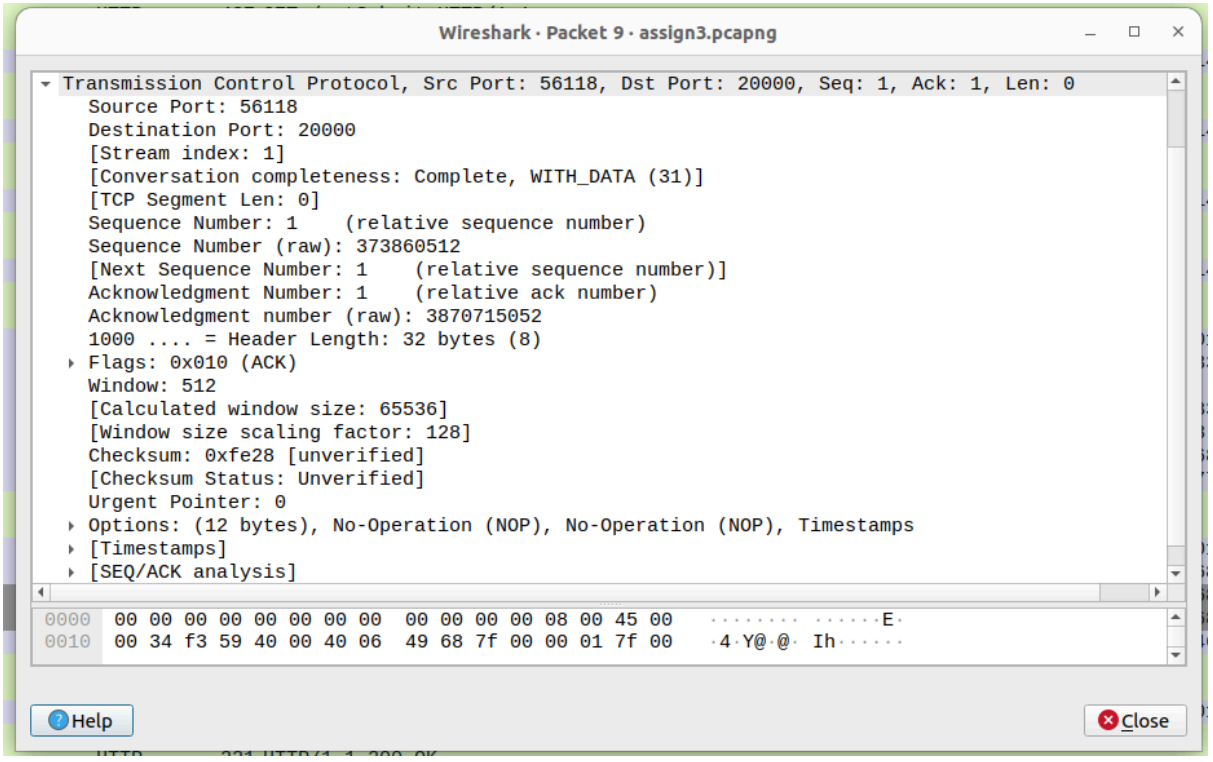
Handshaking occurs in packet 7(SYN), 8(SYN, ACK) and 9 (ACK).
Packet 7 : SYN



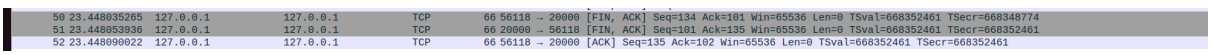
Packet 8: [SYN, ACK]



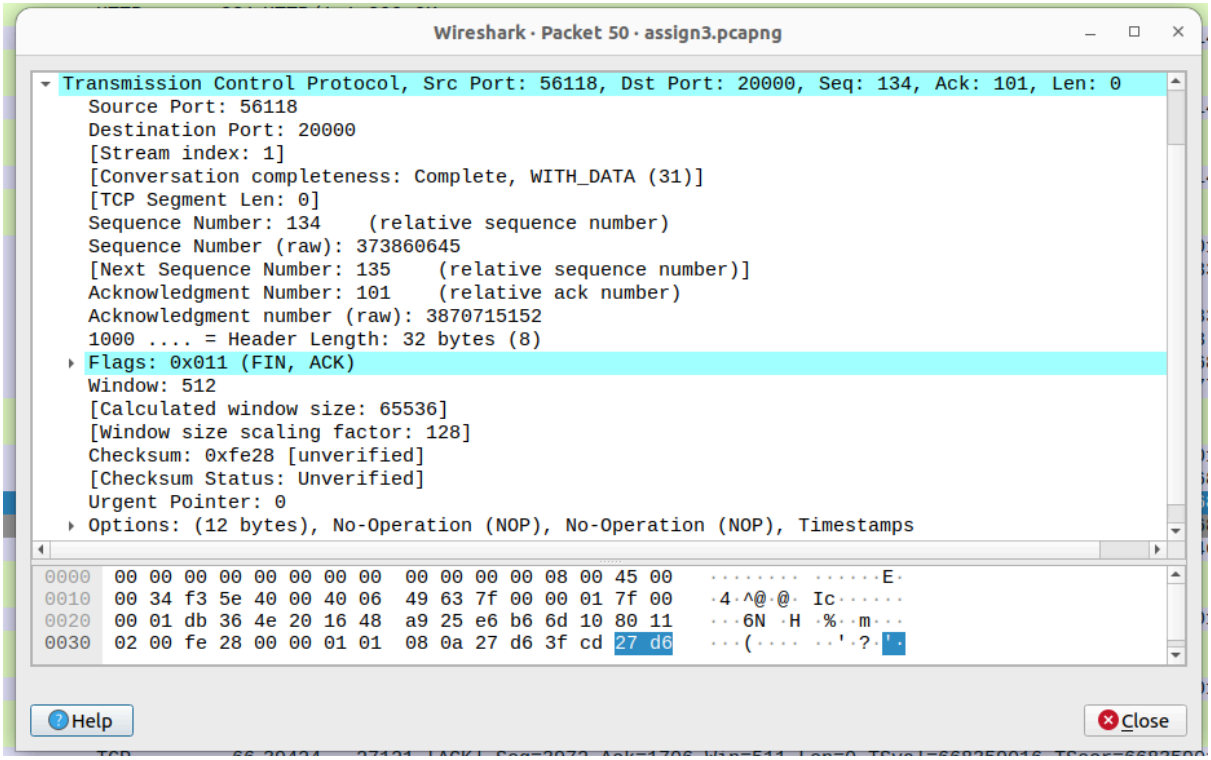
Packet 9: ACK

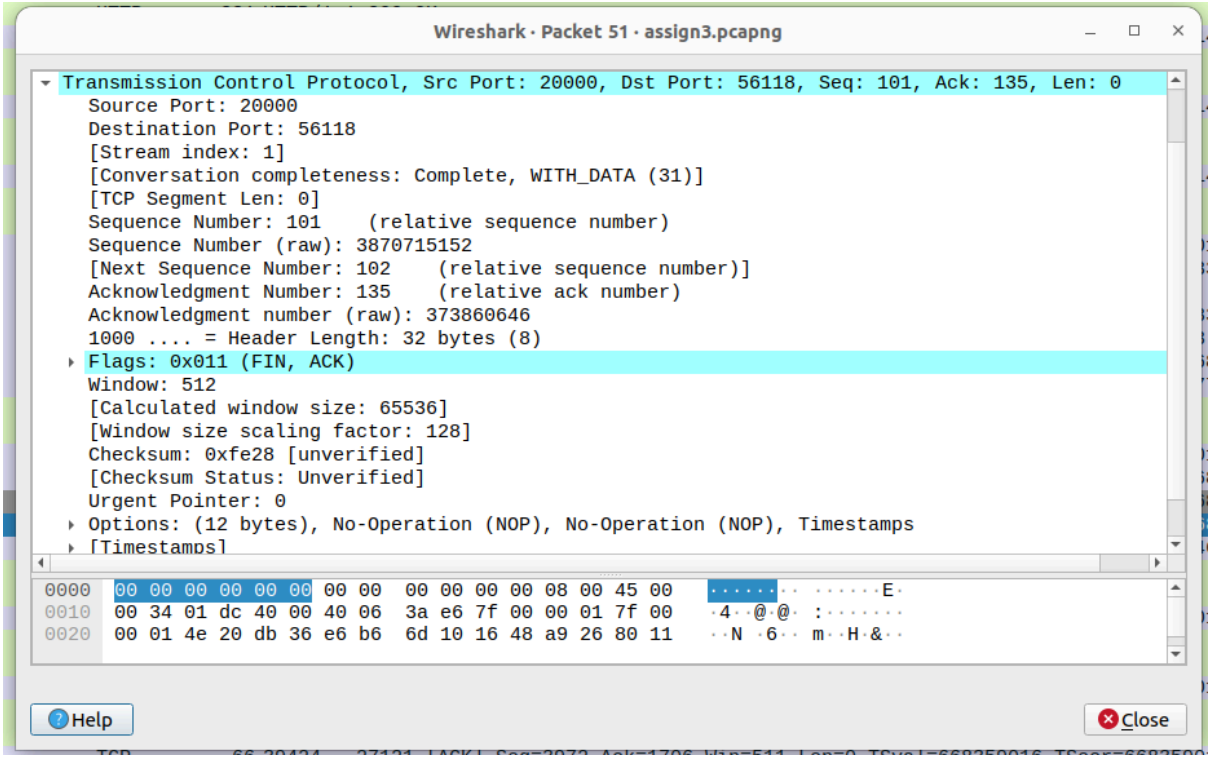


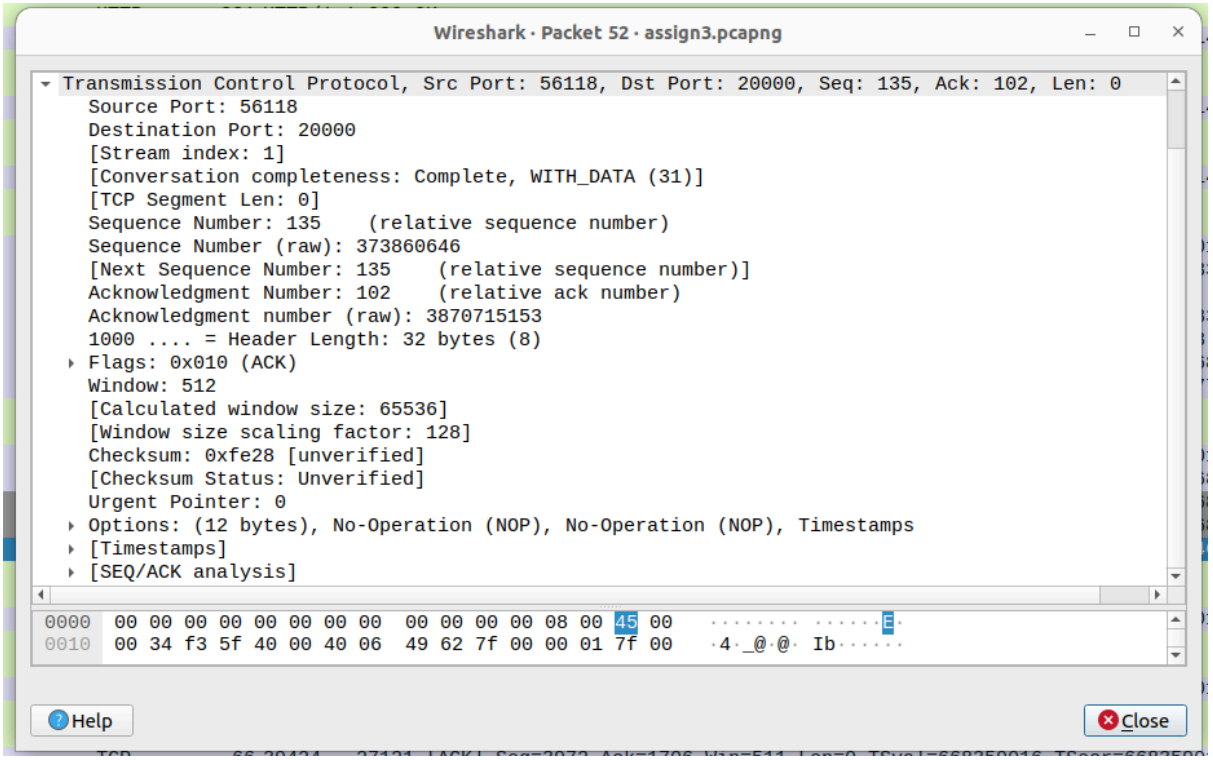
3.



Client initiates the connection closure procedure by sending a (FIN, ACK) packet (packet 50), after which server sends a combined (FIN, ACK) packet (packet 51) to client, and finally client sends ACK (packet 52) to server.

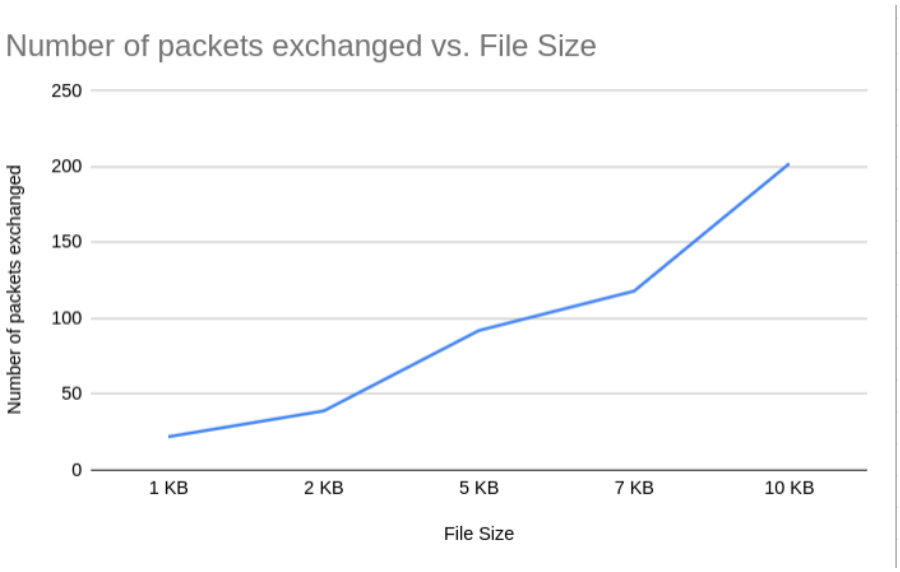

Wireshark · Packet 50 · assign3.pcapng
Transmission Control Protocol, Src Port: 56118, Dst Port: 20000, Seq: 134, Ack: 101, Len: 0
Source Port: 56118
Destination Port: 20000
[Stream index: 1]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 134 (relative sequence number)
Sequence Number (raw): 373860645
[Next Sequence Number: 135 (relative sequence number)]
Acknowledgment Number: 101 (relative ack number)
Acknowledgment number (raw): 3870715152
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
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010 00 34 f3 5e 40 00 40 06 49 63 7f 00 00 01 7f 00
0020 00 01 db 36 4e 20 16 48 a9 25 e6 b6 6d 10 80 11
0030 02 00 fe 28 00 00 01 01 08 0a 27 d6 3f cd 27 d6
Help
Close


Wireshark · Packet 51 · assign3.pcapng
Transmission Control Protocol, Src Port: 20000, Dst Port: 56118, Seq: 101, Ack: 135, Len: 0
Source Port: 20000
Destination Port: 56118
[Stream index: 1]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 0]
Sequence Number: 101 (relative sequence number)
Sequence Number (raw): 3870715152
[Next Sequence Number: 102 (relative sequence number)]
Acknowledgment Number: 135 (relative ack number)
Acknowledgment number (raw): 373860646
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]
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010 00 34 01 dc 40 00 40 06 3a e6 7f 00 00 01 7f 00
0020 00 01 4e 20 db 36 e6 b6 6d 10 16 48 a9 26 80 11
Help
Close



4.

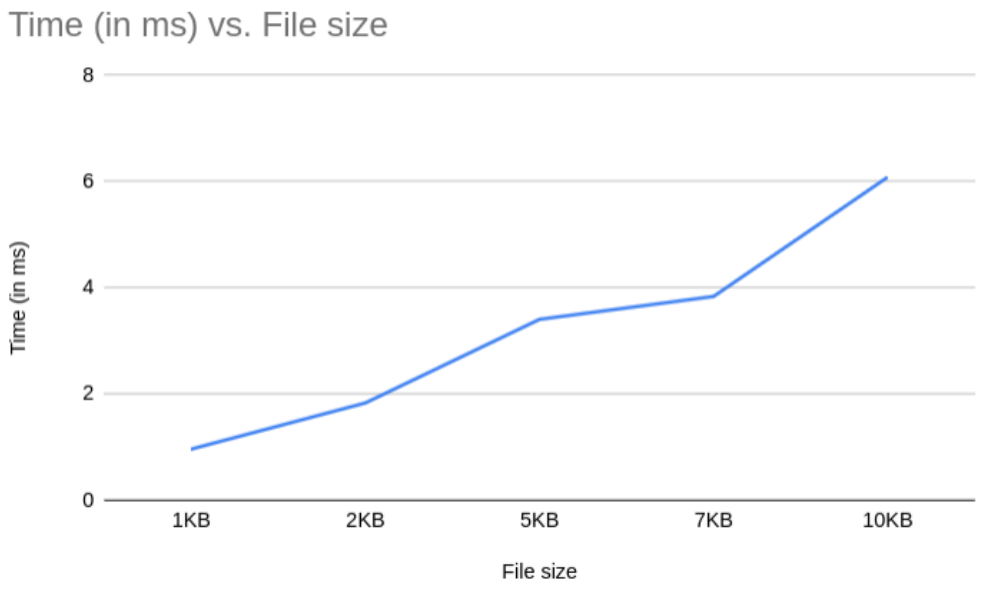
File Size	Number of packets exchanged
1 KB	22
2 KB	39
5 KB	92
7 KB	118
10 KB	202



I consider the packet transfers which occurred while transferring the unencrypted file from client to server and transferring encrypted file from server to client.

5.

File size	Time (in ms)
1KB	0.965
2KB	1.832
5KB	3.406
7KB	3.838
10KB	6.083



6.

Total bytes transferred = 51200 bytes
Total packets transferred = 473
Average packet size = 108.94 bytes