

# Assignment 3

## TCP Sockets

---

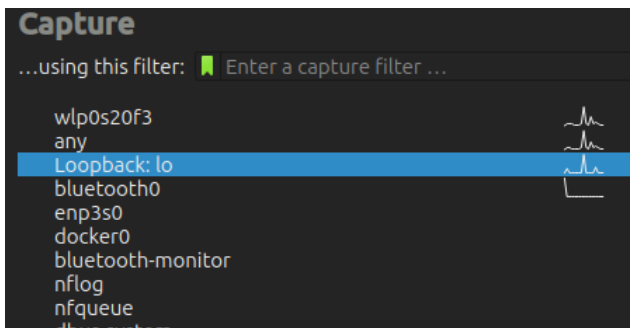
```
harshit@acer-aspire-lite-52: ~/Documents/net/A3
harshit@acer-aspire-lite-52:~/Documents/net/A3$ ./server
server: connection established with client at port 58696
server: connection closed by client at port 58696
server: connection established with client at port 46496
server: connection closed by client at port 46496
[]

harshit@acer-aspire-lite-52:~/Documents/net/A3$ ./client
client: connection established with server
Enter filename: lorem_10000.txt
Enter key: qwertyuiopasdfghjklzxcvbnm
File encrypted with substitution cipher using key QWERTYUIOPASDFGHJKLZXCVBNM
Plaintext: lorem_10000.txt
Ciphertext: lorem_10000.txt.enc

Enter "No" (case-sensitive) to exit, anything else to encrypt another file: No
harshit@acer-aspire-lite-52:~/Documents/net/A3$ ./client
client: connection established with server
Enter filename: lorem_100.txt
Enter key: qwertyuiopasdfghjklzxcvbnm
File encrypted with substitution cipher using key QWERTYUIOPASDFGHJKLZXCVBNM
Plaintext: lorem_100.txt
Ciphertext: lorem_100.txt.enc

Enter "No" (case-sensitive) to exit, anything else to encrypt another file: No
```

For packet analysis, only the Loopback (lo) interface was observed:



## 1. Source & Destination

IP Address	
Server	127.0.0.1 (loopback address)
Client	
Port	
Server	8008 (set by user)
Client	58696 (allocated)

tcp.port == 8008						
No.	Time	Source	Destination	Protocol	Length	Info
31	11.441476	127.0.0.1	127.0.0.1	TCP	74	58696 → 8008 [
32	11.441511	127.0.0.1	127.0.0.1	TCP	74	8008 → 58696 [
33	11.441539	127.0.0.1	127.0.0.1	TCP	66	58696 → 8008 [
46	35.509914	127.0.0.1	127.0.0.1	TCP	92	58696 → 8008 [
47	35.509963	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [
48	35.510060	127.0.0.1	127.0.0.1	TCP	106	58696 → 8008 [
49	35.510080	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [
50	35.510105	127.0.0.1	127.0.0.1	TCP	106	58696 → 8008 [
51	35.510116	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [
▶ Frame 46: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)						
▶ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)						
▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1						
▼ Transmission Control Protocol, Src Port: 58696, Dst Port: 8008, Seq: 1, Ack: 1, Len: 26						
Source Port: 58696						
Destination Port: 8008						
[Stream index: 0]						

---

## 2. Three-way handshake

SYN (client → server)

```
▼ Transmission Control Protocol, Src Port: 58696, Dst Port: 8008, Seq: 0, Len: 0
  Source Port: 58696
  Destination Port: 8008
  [Stream index: 0]
  ▶ [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 713985563
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  1010 .... = Header Length: 40 bytes (10)
  ▼ Flags: 0x002 (SYN)
    000. .... = Reserved: Not set
    ...0 .... = Accurate ECN: Not set
    .... 0... = Congestion Window Reduced: Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...0 = Acknowledgment: Not set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    ▶ .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: .....S.]
  Window: 65495
  [Calculated window size: 65495]
  Checksum: 0xfe30 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  ▶ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation
  ▼ [Timestamps]
    [Time since first frame in this TCP stream: 0.000000000 seconds]
    [Time since previous frame in this TCP stream: 0.000000000 seconds]
```

SYN, ACK (server → client)

```
▼ Transmission Control Protocol, Src Port: 8008, Dst Port: 58696, Seq: 0, Ack: 1,
  Source Port: 8008
  Destination Port: 58696
  [Stream index: 0]
  ▶ [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 0      (relative sequence number)
  Sequence Number (raw): 8059506
  [Next Sequence Number: 1      (relative sequence number)]
  Acknowledgment Number: 1      (relative ack number)
  Acknowledgment number (raw): 713985564
  1010 .... = Header Length: 40 bytes (10)
  ▼ Flags: 0x012 (SYN, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Accurate ECN: Not set
    .... 0... = Congestion Window Reduced: Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    ▶ .... .... ..1. = Syn: Set
    .... .... ...0 = Fin: Not set
    [TCP Flags: .....A..S.]
  Window: 65483
  [Calculated window size: 65483]
  Checksum: 0xfe30 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  ▶ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Op
  ▼ [Timestamps]
    [Time since first frame in this TCP stream: 0.000035000 seconds]
    [Time since previous frame in this TCP stream: 0.000035000 seconds]
  ▼ [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 31]
    [The RTT to ACK the segment was: 0.000035000 seconds]
    [iRTT: 0.000063000 seconds]
```

ACK (client → server)

```
Transmission Control Protocol, Src Port: 58696, Dst Port: 8008, Seq: 1, Ack: 1,
  Source Port: 58696
  Destination Port: 8008
  [Stream index: 0]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 713985564
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 8059507
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x010 (ACK)
    000. .... = Reserved: Not set
    ...0 .... = Accurate ECN: Not set
    .... 0... = Congestion Window Reduced: Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: .....A....]
  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]
    [Time since first frame in this TCP stream: 0.000063000 seconds]
    [Time since previous frame in this TCP stream: 0.000028000 seconds]
  [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 32]
    [The RTT to ACK the segment was: 0.000028000 seconds]
    [iRTT: 0.000063000 seconds]
```

### 3. Connection Closure

FIN, ACK (client → server)

```
▼ Transmission Control Protocol, Src Port: 58696, Dst Port: 8008, Seq: 10058, Ack: 10032,
  Source Port: 58696
  Destination Port: 8008
  [Stream index: 0]
  ▶ [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 10058      (relative sequence number)
  Sequence Number (raw): 713995621
  [Next Sequence Number: 10059      (relative sequence number)]
  Acknowledgment Number: 10032      (relative ack number)
  Acknowledgment number (raw): 8069538
  1000 .... = Header Length: 32 bytes (8)
  ▼ Flags: 0x011 (FIN, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Accurate ECN: Not set
    .... 0... = Congestion Window Reduced: Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    ▶ .... .... ...1 = Fin: Set
  ▼ [TCP Flags: .....A...F]
    ▼ [Expert Info (Note/Sequence): This frame initiates the connection closing]
      [This frame initiates the connection closing]
      [Severity level: Note]
      [Group: Sequence]
  Window: 641
  [Calculated window size: 82048]
  [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]
    [Time since first frame in this TCP stream: 38.388418000 seconds]
    [Time since previous frame in this TCP stream: 14.316782000 seconds]
```

FIN,ACK (server → client)

```
▼ Transmission Control Protocol, Src Port: 8008, Dst Port: 58696, Seq: 10032, Ack: 10059
  Source Port: 8008
  Destination Port: 58696
  [Stream index: 0]
  ▶ [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 10032      (relative sequence number)
  Sequence Number (raw): 8069538
  [Next Sequence Number: 10033      (relative sequence number)]
  Acknowledgment Number: 10059      (relative ack number)
  Acknowledgment number (raw): 713995622
  1000 .... = Header Length: 32 bytes (8)
  ▼ Flags: 0x011 (FIN, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Accurate ECN: Not set
    .... 0... = Congestion Window Reduced: Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...1 = Fin: Set
    ▼ [Expert Info (Chat/Sequence): Connection finish (FIN)]
      [Connection finish (FIN)]
      [Severity level: Chat]
      [Group: Sequence]
    ▼ [TCP Flags: .....A...F]
      ▶ [Expert Info (Note/Sequence): This frame undergoes the connection closing]
      Window: 792
      [Calculated window size: 101376]
      [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]
        [Time since first frame in this TCP stream: 38.388627000 seconds]
        [Time since previous frame in this TCP stream: 0.000209000 seconds]
      ▼ [SEQ/ACK analysis]
        [This is an ACK to the segment in frame: 174]
        [The RTT to ACK the segment was: 0.000209000 seconds]
        [iRTT: 0.000063000 seconds]
```



ACK (client → server)

```
▼ Transmission Control Protocol, Src Port: 58696, Dst Port: 8008, Seq: 10059, Ack: 10033,
  Source Port: 58696
  Destination Port: 8008
  [Stream index: 0]
  ▶ [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 10059      (relative sequence number)
  Sequence Number (raw): 713995622
  [Next Sequence Number: 10059      (relative sequence number)]
  Acknowledgment Number: 10033      (relative ack number)
  Acknowledgment number (raw): 8069539
  1000 .... = Header Length: 32 bytes (8)
  ▼ Flags: 0x010 (ACK)
    000. .... = Reserved: Not set
    ...0 .... = Accurate ECN: Not set
    .... 0... = Congestion Window Reduced: Not set
    .... .0.. = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: .....A....]
  Window: 641
  [Calculated window size: 82048]
  [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]
    [Time since first frame in this TCP stream: 38.388686000 seconds]
    [Time since previous frame in this TCP stream: 0.000059000 seconds]
  ▼ [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 175]
    [The RTT to ACK the segment was: 0.000059000 seconds]
    [iRTT: 0.000063000 seconds]
```

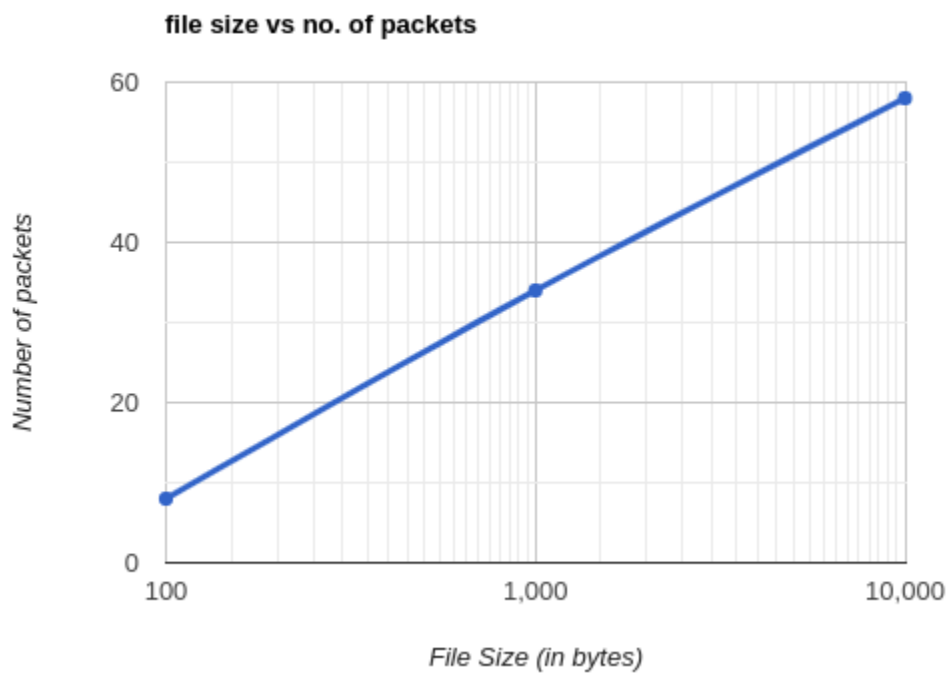
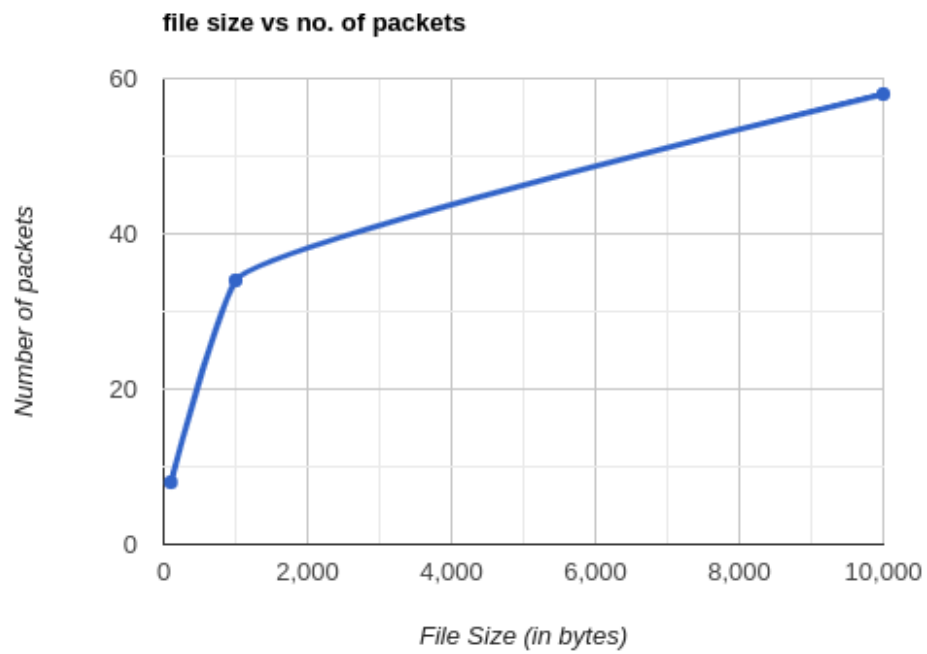


## 4. Number of packets

No. of packets exchanged for the transfer data of 10000-byte file: **56**

tcp.port == 8008									
No.	Time	Source	Destination	Protocol	Length	Info			
31	11.441476	127.0.0.1	127.0.0.1	TCP	74	58696 → 8008 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=1038270516 TSecr=0 WS=128			
32	11.441511	127.0.0.1	127.0.0.1	TCP	74	8008 → 58696 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM TSval=1038270516 TSecr=1038270516 WS=128			
33	11.441539	127.0.0.1	127.0.0.1	TCP	66	58696 → 8008 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1038270516 TSecr=1038270516			
46	35.509914	127.0.0.1	127.0.0.1	TCP	92	58696 → 8008 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=26 TSval=1038294584 TSecr=1038270516			
47	35.509963	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=27 Win=65536 Len=0 TSval=1038294584 TSecr=1038294584			
48	35.510060	127.0.0.1	127.0.0.1	TCP	106	58696 → 8008 [PSH, ACK] Seq=27 Ack=1 Win=65536 Len=40 TSval=1038294584 TSecr=1038294584			
49	35.510080	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=67 Win=65536 Len=0 TSval=1038294584 TSecr=1038294584			
50	35.510105	127.0.0.1	127.0.0.1	TCP	106	58696 → 8008 [PSH, ACK] Seq=67 Ack=1 Win=65536 Len=40 TSval=1038294584 TSecr=1038294584			
51	35.510116	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=197 Win=65536 Len=0 TSval=1038294584 TSecr=1038294584			
52	35.510135	127.0.0.1	127.0.0.1	TCP	106	58696 → 8008 [PSH, ACK] Seq=107 Ack=1 Win=65536 Len=40 TSval=1038294584 TSecr=1038294584			
53	35.510148	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=147 Win=65536 Len=0 TSval=1038294584 TSecr=1038294584			
54	35.510163	127.0.0.1	127.0.0.1	TCP	106	58696 → 8008 [PSH, ACK] Seq=147 Ack=1 Win=65536 Len=40 TSval=1038294584 TSecr=1038294584			
55	35.510177	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=187 Win=65536 Len=0 TSval=1038294584 TSecr=1038294584			
56	35.510192	127.0.0.1	127.0.0.1	TCP	106	58696 → 8008 [PSH, ACK] Seq=187 Ack=1 Win=65536 Len=40 TSval=1038294584 TSecr=1038294584			
57	35.510205	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=227 Win=65536 Len=0 TSval=1038294584 TSecr=1038294584			
58	35.510221	127.0.0.1	127.0.0.1	TCP	106	58696 → 8008 [PSH, ACK] Seq=227 Ack=1 Win=65536 Len=40 TSval=1038294584 TSecr=1038294584			
59	35.510233	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=267 Win=65536 Len=0 TSval=1038294584 TSecr=1038294584			
60	35.510289	127.0.0.1	127.0.0.1	TCP	106	58696 → 8008 [PSH, ACK] Seq=267 Ack=1 Win=65536 Len=40 TSval=1038294585 TSecr=1038294584			
61	35.510391	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=397 Win=65536 Len=0 TSval=1038294585 TSecr=1038294585			
62	35.510317	127.0.0.1	127.0.0.1	TCP	106	58696 → 8008 [PSH, ACK] Seq=397 Ack=1 Win=65536 Len=40 TSval=1038294585 TSecr=1038294585			
63	35.510322	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=347 Win=65536 Len=0 TSval=1038294585 TSecr=1038294585			
64	35.510343	127.0.0.1	127.0.0.1	TCP	106	58696 → 8008 [PSH, ACK] Seq=347 Ack=1 Win=65536 Len=40 TSval=1038294585 TSecr=1038294585			
65	35.510352	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=387 Win=65536 Len=0 TSval=1038294585 TSecr=1038294585			
66	35.510367	127.0.0.1	127.0.0.1	TCP	106	58696 → 8008 [PSH, ACK] Seq=387 Ack=1 Win=65536 Len=40 TSval=1038294585 TSecr=1038294585			
67	35.510375	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=427 Win=65536 Len=0 TSval=1038294585 TSecr=1038294585			
68	35.510390	127.0.0.1	127.0.0.1	TCP	106	58696 → 8008 [PSH, ACK] Seq=427 Ack=1 Win=65536 Len=40 TSval=1038294585 TSecr=1038294585			
69	35.510418	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=467 Win=65536 Len=0 TSval=1038294585 TSecr=1038294585			
70	35.510439	127.0.0.1	127.0.0.1	TCP	706	58696 → 8008 [PSH, ACK] Seq=467 Ack=1 Win=65536 Len=640 TSval=1038294585 TSecr=1038294585			
71	35.510453	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=1107 Win=64896 Len=0 TSval=1038294585 TSecr=1038294585			
72	35.510470	127.0.0.1	127.0.0.1	TCP	106	58696 → 8008 [PSH, ACK] Seq=1107 Ack=1 Win=65536 Len=40 TSval=1038294585 TSecr=1038294585			
73	35.510479	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=1147 Win=64896 Len=0 TSval=1038294585 TSecr=1038294585			
74	35.510494	127.0.0.1	127.0.0.1	TCP	106	58696 → 8008 [PSH, ACK] Seq=1147 Ack=1 Win=65536 Len=40 TSval=1038294585 TSecr=1038294585			
75	35.510507	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=1187 Win=64896 Len=0 TSval=1038294585 TSecr=1038294585			
76	35.510523	127.0.0.1	127.0.0.1	TCP	106	58696 → 8008 [PSH, ACK] Seq=1187 Ack=1 Win=65536 Len=40 TSval=1038294585 TSecr=1038294585			
77	35.510535	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=1227 Win=64896 Len=0 TSval=1038294585 TSecr=1038294585			
78	35.510551	127.0.0.1	127.0.0.1	TCP	106	58696 → 8008 [PSH, ACK] Seq=1227 Ack=1 Win=65536 Len=40 TSval=1038294585 TSecr=1038294585			
79	35.510564	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=1267 Win=64896 Len=0 TSval=1038294585 TSecr=1038294585			
80	35.510600	127.0.0.1	127.0.0.1	TCP	666	58696 → 8008 [PSH, ACK] Seq=1267 Ack=1 Win=65536 Len=600 TSval=1038294585 TSecr=1038294585			
81	35.510643	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=1867 Win=64384 Len=0 TSval=1038294585 TSecr=1038294585			
82	35.510664	127.0.0.1	127.0.0.1	TCP	906	58696 → 8008 [PSH, ACK] Seq=1867 Ack=1 Win=65536 Len=840 TSval=1038294585 TSecr=1038294585			
83	35.510693	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=2707 Win=63616 Len=0 TSval=1038294585 TSecr=1038294585			
84	35.510707	127.0.0.1	127.0.0.1	TCP	826	58696 → 8008 [PSH, ACK] Seq=2707 Ack=1 Win=65536 Len=760 TSval=1038294585 TSecr=1038294585			
85	35.510732	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=3467 Win=62976 Len=0 TSval=1038294585 TSecr=1038294585			
86	35.510745	127.0.0.1	127.0.0.1	TCP	706	58696 → 8008 [PSH, ACK] Seq=3467 Ack=1 Win=65536 Len=640 TSval=1038294585 TSecr=1038294585			
87	35.510768	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=4107 Win=62976 Len=0 TSval=1038294585 TSecr=1038294585			
88	35.510784	127.0.0.1	127.0.0.1	TCP	666	58696 → 8008 [PSH, ACK] Seq=4107 Ack=1 Win=65536 Len=600 TSval=1038294585 TSecr=1038294585			
89	35.510926	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=4707 Win=62976 Len=0 TSval=1038294585 TSecr=1038294585			
90	35.510945	127.0.0.1	127.0.0.1	TCP	3346	58696 → 8008 [PSH, ACK] Seq=4707 Ack=1 Win=65536 Len=3280 TSval=1038294585 TSecr=1038294585			
91	35.510950	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=7987 Win=96384 Len=0 TSval=1038294585 TSecr=1038294585			
92	35.510975	127.0.0.1	127.0.0.1	TCP	346	58696 → 8008 [PSH, ACK] Seq=7987 Ack=1 Win=65536 Len=280 TSval=1038294585 TSecr=1038294585			
93	35.510985	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=8267 Win=99456 Len=0 TSval=1038294585 TSecr=1038294585			
94	35.511002	127.0.0.1	127.0.0.1	TCP	106	58696 → 8008 [PSH, ACK] Seq=8267 Ack=1 Win=65536 Len=40 TSval=1038294585 TSecr=1038294585			
95	35.511041	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=8307 Win=99456 Len=0 TSval=1038294585 TSecr=1038294585			
96	35.511061	127.0.0.1	127.0.0.1	TCP	866	58696 → 8008 [PSH, ACK] Seq=8307 Ack=1 Win=65536 Len=880 TSval=1038294585 TSecr=1038294585			
97	35.511072	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=9107 Win=100352 Len=0 TSval=1038294585 TSecr=1038294585			
98	35.511085	127.0.0.1	127.0.0.1	TCP	386	58696 → 8008 [PSH, ACK] Seq=9107 Ack=1 Win=65536 Len=320 TSval=1038294585 TSecr=1038294585			
99	35.511096	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=9427 Win=101376 Len=0 TSval=1038294585 TSecr=1038294585			
100	35.511110	127.0.0.1	127.0.0.1	TCP	386	58696 → 8008 [PSH, ACK] Seq=9427 Ack=1 Win=65536 Len=320 TSval=1038294585 TSecr=1038294585			
101	35.511162	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=9747 Win=101376 Len=0 TSval=1038294585 TSecr=1038294585			
102	35.511174	127.0.0.1	127.0.0.1	TCP	377	58696 → 8008 [PSH, ACK] Seq=9747 Ack=1 Win=65536 Len=311 TSval=1038294585 TSecr=1038294585			
103	35.511192	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696 [ACK] Seq=1 Ack=10058 Win=101376 Len=0 TSval=1038294585 TSecr=1038294585			
104	35.512096	127.0.0.1	127.0.0.1	TCP	96	8008 → 58696 [PSH, ACK] Seq=1 Ack=10058 Win=101376 Len=30 TSval=1038294586 TSecr=1038294585			
105	35.512115	127.0.0.1	127.0.0.1	TCP	66	58696 → 8008 [ACK] Seq=10058 Ack=31 Win=65536 Len=0 TSval=1038294586 TSecr=1038294586			
106	35.512138	127.0.0.1	127.0.0.1	TCP	96	8008 → 58696 [PSH, ACK] Seq=31 Ack=10058 Win=101376 Len=30 TSval=1038294586 TSecr=1038294586			

File Size (in bytes)	No. of Packets
100	8
1000	34
10000	58



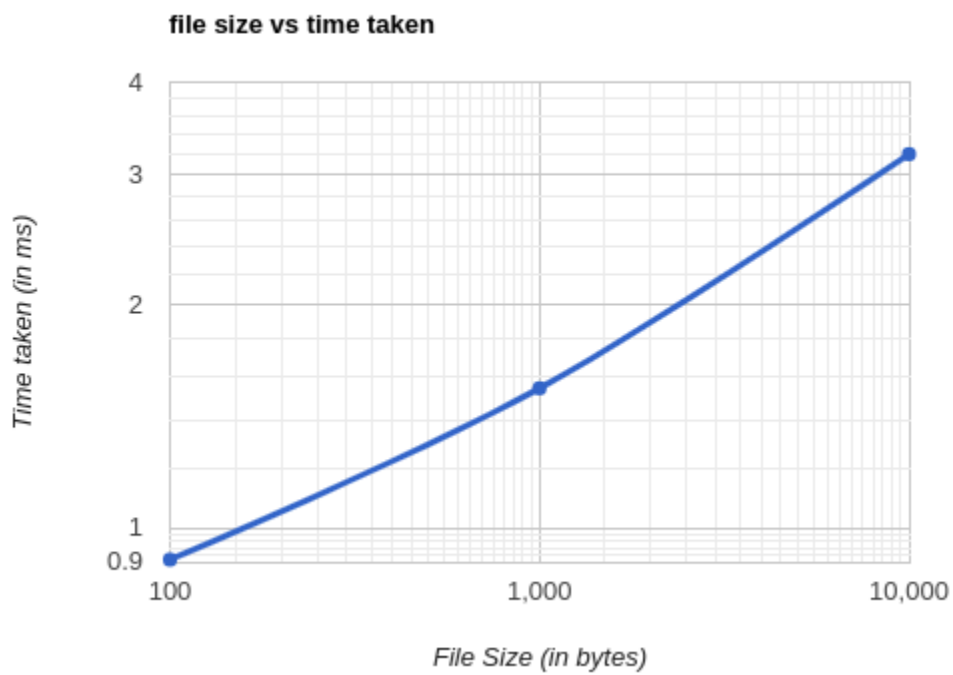
The number of packets appear to be increasing linearly with the logarithm of the file size

## 5. Total time taken

Time taken to encrypt a 10000-byte file: **3.198 ms**

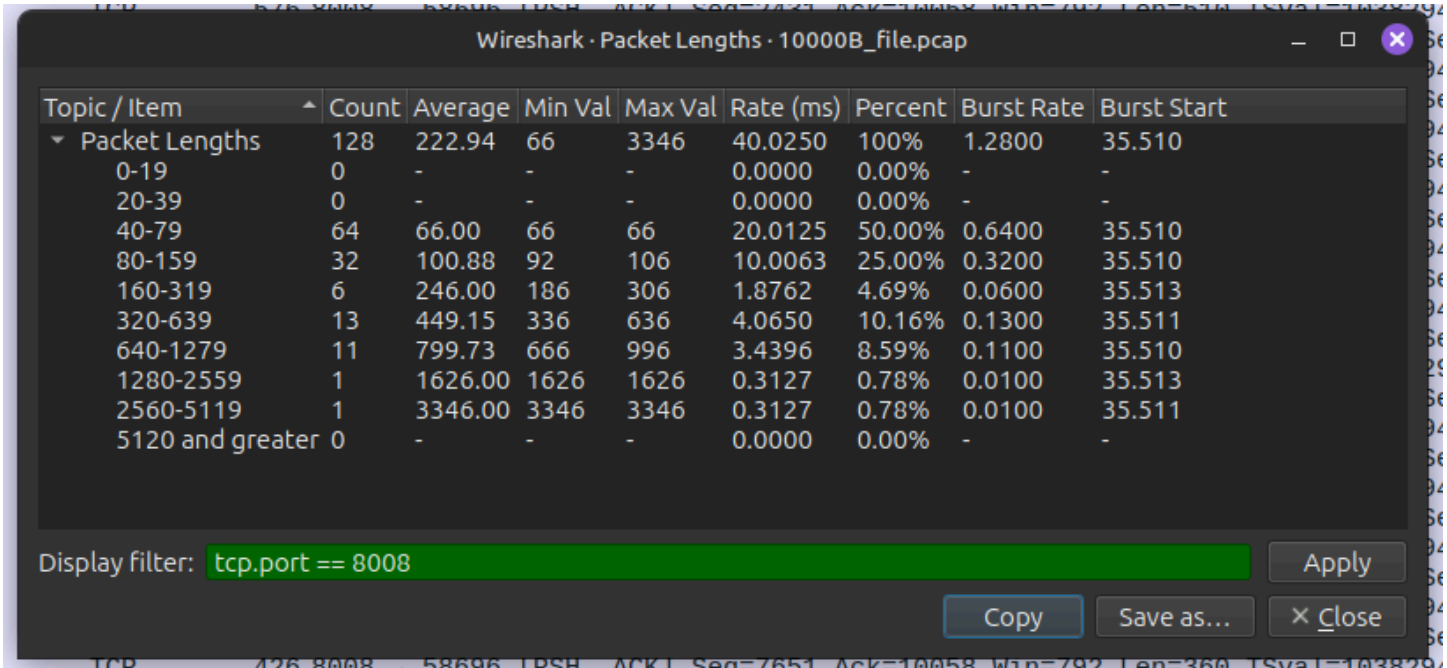
32	11.441511	127.0.0.1	127.0.0.1	TCP	74	8008 → 58696	[SYN, ACK] Seq=1 A
33	11.441539	127.0.0.1	127.0.0.1	TCP	66	58696 → 8008	[ACK] Seq=1 A
46	35.509914	127.0.0.1	127.0.0.1	TCP	92	58696 → 8008	[PSH, ACK] Seq=1 A
47	35.509963	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696	[ACK] Seq=1 A
48	35.510060	127.0.0.1	127.0.0.1	TCP	106	58696 → 8008	[PSH, ACK] Seq=1 A
171	35.513064	127.0.0.1	127.0.0.1	TCP	66	58696 → 8008	[ACK] Seq=1 A
172	35.513077	127.0.0.1	127.0.0.1	TCP	827	8008 → 58696	[PSH, ACK] Seq=1 A
173	35.513112	127.0.0.1	127.0.0.1	TCP	66	58696 → 8008	[ACK] Seq=1 A
174	49.829894	127.0.0.1	127.0.0.1	TCP	66	58696 → 8008	[FIN, ACK] Seq=1 A
175	49.830103	127.0.0.1	127.0.0.1	TCP	66	8008 → 58696	[FIN, ACK] Seq=1 A

File Size (in bytes)	Time Taken (in ms)
100	0.906
1000	1.544
10000	3.198



## 6. Average Packet Size

Packet size statistics for data communication, i.e., considering packets other than those for handshake and connection closure for 10000-byte file ( $2 \times 10000 + 26 = 20,026$  bytes of data transfer):

The image shows the 'Wireshark - Packet Lengths - 10000B\_file.pcap' window. It displays a table of packet length statistics. The 'Display filter' is set to 'tcp.port == 8008'. The table has columns: Topic / Item, Count, Average, Min Val, Max Val, Rate (ms), Percent, Burst Rate, and Burst Start. The data is as follows:

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Packet Lengths	128	222.94	66	3346	40.0250	100%	1.2800	35.510
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	64	66.00	66	66	20.0125	50.00%	0.6400	35.510
80-159	32	100.88	92	106	10.0063	25.00%	0.3200	35.510
160-319	6	246.00	186	306	1.8762	4.69%	0.0600	35.513
320-639	13	449.15	336	636	4.0650	10.16%	0.1300	35.511
640-1279	11	799.73	666	996	3.4396	8.59%	0.1100	35.510
1280-2559	1	1626.00	1626	1626	0.3127	0.78%	0.0100	35.513
2560-5119	1	3346.00	3346	3346	0.3127	0.78%	0.0100	35.511
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

(data calculated after *ignoring* (Ctrl+D) handshake & closure packets)

File Size (in B)	Bytes Transferred	No. of packets	Avg Packet Size (in B)
100	226	20	77.50
1,000	2,026	72	94.28
10,000	20,026	128	222.94

Overall Avg = **167.61 bytes**