CS39006: Networks Laboratory - Assignment 3 Report

Name: Ansh Sahu
Roll Number: 22CS30010
Date: February 3, 2025
Google Drive Link for pcap File: drive link

1. Introduction

This report documents the implementation and analysis of a TCP socket-based client-server application that performs Substitution Cipher encryption. The report also includes Wireshark analysis to examine network traffic during communication.

---

2. Implementation of TCP Client and Server

2.1 Client (retrieveencfileclient.c)

- Establishes a TCP connection with the server.
- Takes input from the user: filename and encryption key.
- Reads and sends the file content and key to the server in small chunks.
- Receives and stores the encrypted file.
- Continues operation until the user decides to stop.

2.2 Server (doencfileserver.c)

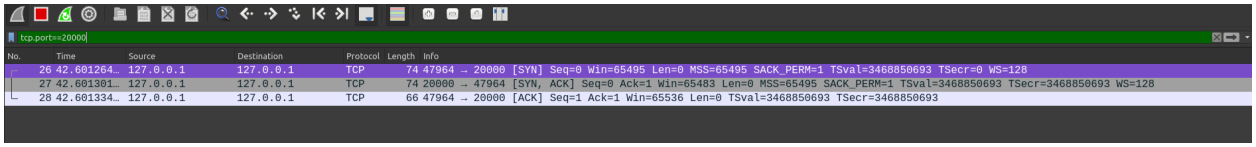
- Listens for incoming client connections.
- Receives and stores the file and key.
- Encrypts the file using Substitution Cipher.
- Sends the encrypted file back to the client.
- Handles multiple file encryption requests before closing the connection.

---

3. Wireshark Analysis

3.1 Source and Destination IP Addresses and Ports

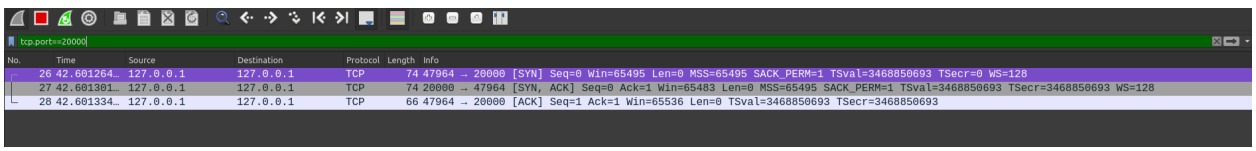
- The communication between the client and server was captured.
- Source IP: 127.0.0.1
- Destination IP: 127.0.0.1
- Source Port: 20000
- Destination Port: 20000
- **Screenshot:**



No.	Time	Source	Destination	Protocol	Length	Info
26	42.601264…	127.0.0.1	127.0.0.1	TCP	74	47964 → 20000 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=3468850693 TSecr=0 WS=128
27	42.601301…	127.0.0.1	127.0.0.1	TCP	74	20000 → 47964 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=3468850693 TSecr=3468850693 WS=128
28	42.601334…	127.0.0.1	127.0.0.1	TCP	66	47964 → 20000 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3468850693 TSecr=3468850693

3.2 Three-Way Handshake

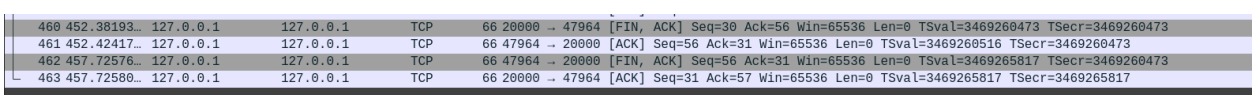
- The TCP connection follows the three-step handshake:
  1. SYN (Client → Server)
  2. SYN-ACK (Server → Client)
  3. ACK (Client → Server)
- **Screenshot:**



No.	Time	Source	Destination	Protocol	Length	Info
26	42.601264…	127.0.0.1	127.0.0.1	TCP	74	47964 → 20000 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=3468850693 TSecr=0 WS=128
27	42.601301…	127.0.0.1	127.0.0.1	TCP	74	20000 → 47964 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=3468850693 TSecr=3468850693 WS=128
28	42.601334…	127.0.0.1	127.0.0.1	TCP	66	47964 → 20000 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3468850693 TSecr=3468850693

3.3 Connection Closure

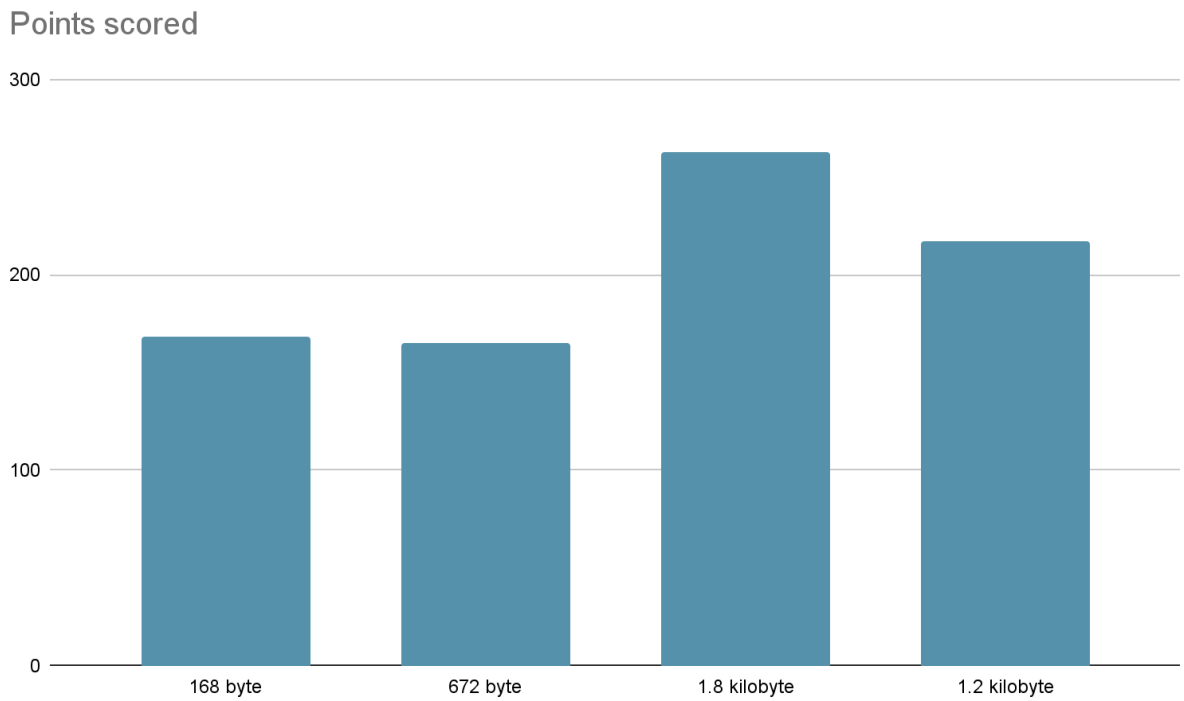
- The connection terminates using the four-step FIN sequence:
  1. FIN (Client → Server)
  2. ACK (Server → Client)
  3. FIN (Server → Client)
  4. ACK (Client → Server)
- **Screenshot:**



460	452.38193…	127.0.0.1	127.0.0.1	TCP	66	20000 → 47964 [FIN, ACK] Seq=30 Ack=56 Win=65536 Len=0 TSval=3469260473 TSecr=3469260473
461	452.42417…	127.0.0.1	127.0.0.1	TCP	66	47964 → 20000 [ACK] Seq=56 Ack=31 Win=65536 Len=0 TSval=3469260516 TSecr=3469260473
462	457.72576…	127.0.0.1	127.0.0.1	TCP	66	47964 → 20000 [FIN, ACK] Seq=56 Ack=31 Win=65536 Len=0 TSval=3469265817 TSecr=3469260473
463	457.72580…	127.0.0.1	127.0.0.1	TCP	66	20000 → 47964 [ACK] Seq=31 Ack=57 Win=65536 Len=0 TSval=3469265817 TSecr=3469265817

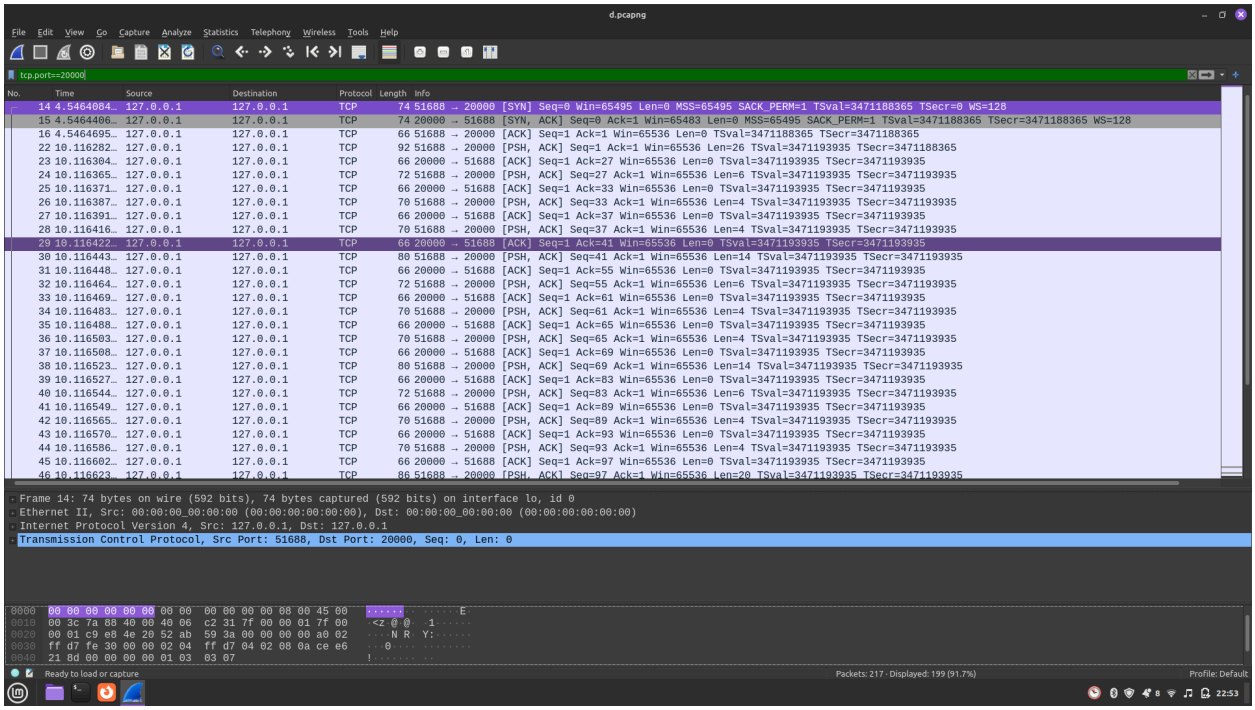
3.4 Number of Packets Exchanged During File Transfer

- Number of packets exchanged: { 29 for 28 bytes,105 for 168 bytes,168 for 672 bytes,289 for 1.8 bytes}
- **Graph:** *(Plot file size vs. number of packets.)*



- **Screenshot:**

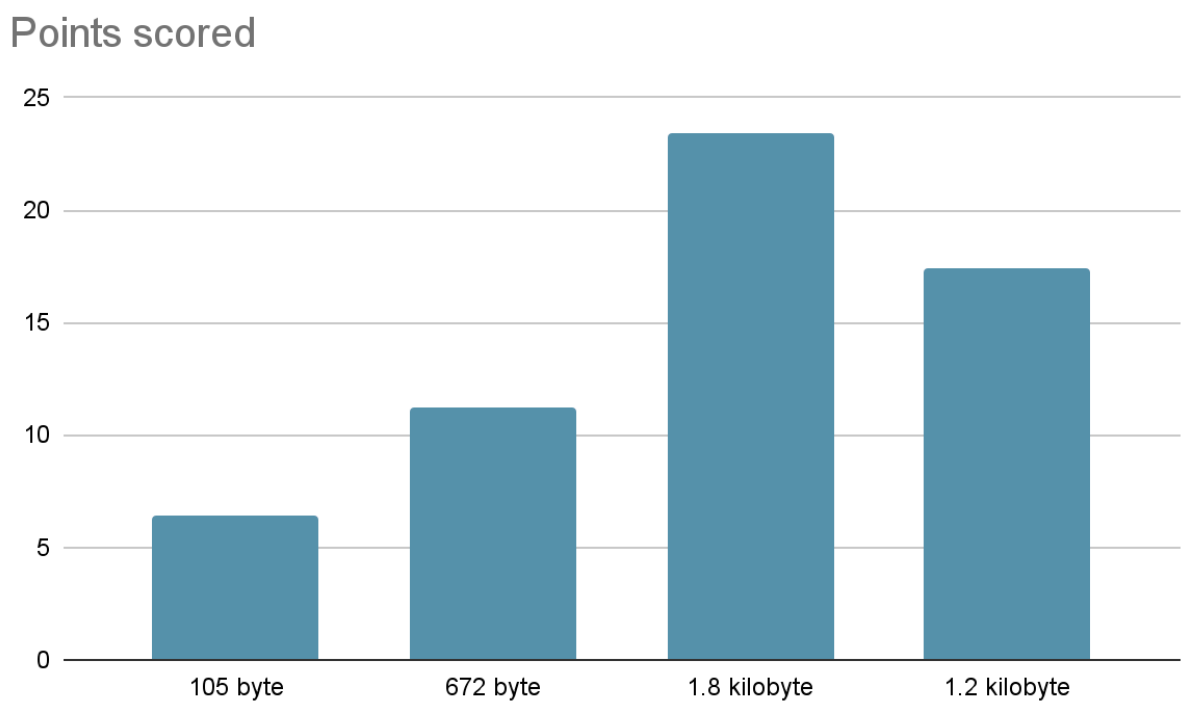
No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000…	127.0.0.1	127.0.0.1	TCP	92	47088 → 20000 [PSH, ACK] Seq=1 Ack=1 Win=512 Len=26 TSval=3470451174 TSecr=3470424466
2	0.0000261…	127.0.0.1	127.0.0.1	TCP	66	20000 → 47088 [ACK] Seq=1 Ack=27 Win=512 Len=0 TSval=3470451174 TSecr=3470451174
3	0.0001346…	127.0.0.1	127.0.0.1	TCP	72	47088 → 20000 [PSH, ACK] Seq=27 Ack=1 Win=512 Len=6 TSval=3470451174 TSecr=3470451174
4	0.0001484…	127.0.0.1	127.0.0.1	TCP	66	20000 → 47088 [ACK] Seq=1 Ack=33 Win=512 Len=0 TSval=3470451174 TSecr=3470451174
5	0.0001933…	127.0.0.1	127.0.0.1	TCP	70	47088 → 20000 [PSH, ACK] Seq=33 Ack=1 Win=512 Len=4 TSval=3470451174 TSecr=3470451174
6	0.0002053…	127.0.0.1	127.0.0.1	TCP	66	20000 → 47088 [ACK] Seq=1 Ack=37 Win=512 Len=0 TSval=3470451174 TSecr=3470451174
7	0.0002439…	127.0.0.1	127.0.0.1	TCP	70	47088 → 20000 [PSH, ACK] Seq=37 Ack=1 Win=512 Len=4 TSval=3470451174 TSecr=3470451174
8	0.0002558…	127.0.0.1	127.0.0.1	TCP	66	20000 → 47088 [ACK] Seq=1 Ack=41 Win=512 Len=0 TSval=3470451174 TSecr=3470451174
9	0.0002946…	127.0.0.1	127.0.0.1	TCP	80	47088 → 20000 [PSH, ACK] Seq=41 Ack=1 Win=512 Len=14 TSval=3470451175 TSecr=3470451174
10	0.0003049…	127.0.0.1	127.0.0.1	TCP	66	20000 → 47088 [ACK] Seq=1 Ack=55 Win=512 Len=0 TSval=3470451175 TSecr=3470451175
11	0.0003442…	127.0.0.1	127.0.0.1	TCP	67	47088 → 20000 [PSH, ACK] Seq=55 Ack=1 Win=512 Len=1 TSval=3470451175 TSecr=3470451175
12	0.0003537…	127.0.0.1	127.0.0.1	TCP	66	20000 → 47088 [ACK] Seq=1 Ack=56 Win=512 Len=0 TSval=3470451175 TSecr=3470451175
13	0.0012298…	127.0.0.1	127.0.0.1	TCP	72	20000 → 47088 [PSH, ACK] Seq=1 Ack=56 Win=512 Len=6 TSval=3470451175 TSecr=3470451175
14	0.0012564…	127.0.0.1	127.0.0.1	TCP	66	47088 → 20000 [ACK] Seq=56 Ack=7 Win=512 Len=0 TSval=3470451175 TSecr=3470451175
15	0.0013222…	127.0.0.1	127.0.0.1	TCP	70	20000 → 47088 [PSH, ACK] Seq=7 Ack=56 Win=512 Len=4 TSval=3470451176 TSecr=3470451175
16	0.0013327…	127.0.0.1	127.0.0.1	TCP	66	47088 → 20000 [ACK] Seq=56 Ack=11 Win=512 Len=0 TSval=3470451176 TSecr=3470451176
17	0.0013530…	127.0.0.1	127.0.0.1	TCP	70	20000 → 47088 [PSH, ACK] Seq=11 Ack=56 Win=512 Len=4 TSval=3470451176 TSecr=3470451176
18	0.0013617…	127.0.0.1	127.0.0.1	TCP	66	47088 → 20000 [ACK] Seq=56 Ack=15 Win=512 Len=0 TSval=3470451176 TSecr=3470451176
19	0.0013816…	127.0.0.1	127.0.0.1	TCP	80	20000 → 47088 [PSH, ACK] Seq=15 Ack=56 Win=512 Len=14 TSval=3470451176 TSecr=3470451176
20	0.0013900…	127.0.0.1	127.0.0.1	TCP	66	47088 → 20000 [ACK] Seq=56 Ack=29 Win=512 Len=0 TSval=3470451176 TSecr=3470451176
21	0.0014305…	127.0.0.1	127.0.0.1	TCP	67	20000 → 47088 [PSH, ACK] Seq=29 Ack=56 Win=512 Len=1 TSval=3470451176 TSecr=3470451176
22	0.0014396…	127.0.0.1	127.0.0.1	TCP	66	47088 → 20000 [ACK] Seq=56 Ack=30 Win=512 Len=0 TSval=3470451176 TSecr=3470451176
23	0.0015791…	127.0.0.1	127.0.0.1	TCP	66	20000 → 47088 [FIN, ACK] Seq=30 Ack=56 Win=512 Len=0 TSval=3470451176 TSecr=3470451176
24	0.0453214…	127.0.0.1	127.0.0.1	TCP	66	47088 → 20000 [ACK] Seq=56 Ack=31 Win=512 Len=0 TSval=3470451220 TSecr=3470451176



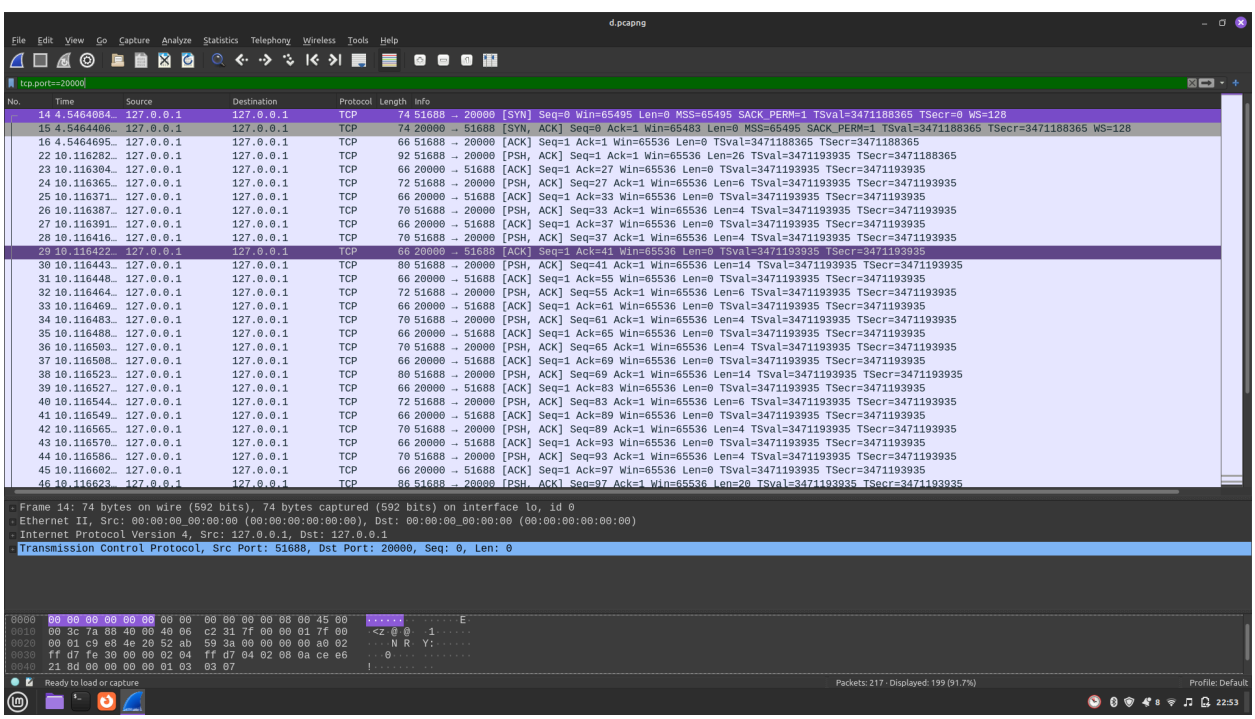
3.5 File Transfer Time Analysis

- Time taken for:
  - File transfer from client to server:{6.46 ms}
  - Encryption at the server: {11.ms}
  - Sending encrypted file back to client: {22ms}

- **Graph:**



- **Screenshot:**



3.6 Average Packet Size

- The average packet size during data communication: 82 bytes

---

4. Conclusion

- Successfully implemented TCP-based client-server file encryption.
- Observed network traffic using Wireshark.
- Analyzed packet exchange, handshake, and connection closure.