Tools Used:

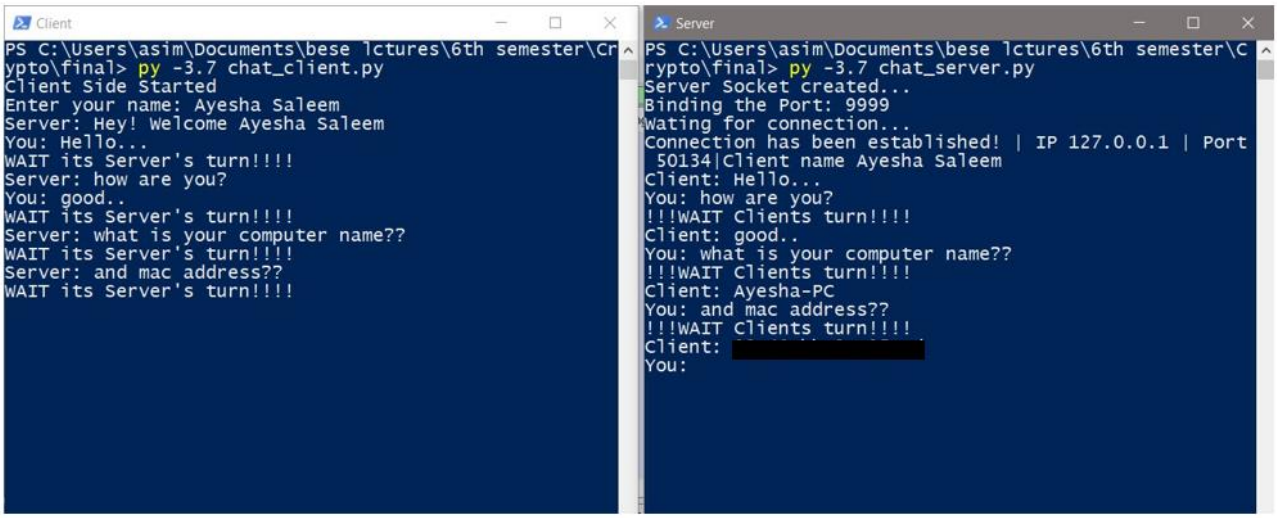
- Visual Studio for coding
- Windows power shell for viewing output
- Wireshark for analyzing packets
- Python language used for coding

Details:

- Server is User A and client is user B.
- At a time 1 message is sent by a user, if B quits A still runs but if A quits B ends automatically.
- Whenever server (user A) send a message with “mac address” in it automatically mac address is sent by the client (user B).
- Similarly if “computer name” is in server’s message host name is sent.
- Once hostname is shared, key is generated on both sides
- Encrypted conversation starts when both hostname and mac address is received at the server and the counter to keep track of encrypted messages starts too.
- After exchange of 5 encrypted messaged key is updated.
- Encrypted messages are sent and decrypted on both ends using same technique on both ends.
- Plain text is displayed on both ends.

Communication:

Plain text is exchanged until MAC address and Computer name is given including these two things.



Wireshark · Packet 6 · Adapter for loopback traffic capture

```
> Frame 6: 57 bytes on wire (456 bits), 57 bytes captured (456 bits) on interface \Device\NPF_Loopback, id 0
v Null/Loopback
    Family: IP (2)
v Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 53
    Identification: 0x3c82 (15490)
  > Flags: 0x40, Don't fragment

0000  02 00 00 00 45 00 00 35  3c 82 40 00 80 06 00 00   ····E··5 <·@·····
0010  7f 00 00 01 7f 00 00 01  c3 d6 27 0f 26 a0 b6 96   ........ ··'·&···
0020  da 11 62 75 50 18 27 f9  21 ad 00 00 41 79 65 73   ··buP·'· !···Ayes
0030  68 61 20 53 61 6c 65 65  6d                        ha Salee m
```

Wireshark · Packet 8 · Adapter for loopback traffic capture

```
> Frame 8: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_Loopback, id 0
v Null/Loopback
    Family: IP (2)
v Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 66
    Identification: 0x3c84 (15492)
  > Flags: 0x40, Don't fragment

0000  02 00 00 00 45 00 00 42  3c 84 40 00 80 06 00 00   ····E··B <·@·····
0010  7f 00 00 01 7f 00 00 01  27 0f c3 d6 da 11 62 75   ........ '·····bu
0020  26 a0 b6 a3 50 18 27 f9  d9 83 00 00 48 65 79 21   &···P·'· ····Hey!
0030  20 57 65 6c 63 6f 6d 65  20 41 79 65 73 68 61 20    Welcome  Ayesha 
0040  53 61 6c 65 65 6d                                  Saleem
```

```
> Flags: 0x40, Don't fragment

0000  02 00 00 00 45 00 00 2e  3c 8a 40 00 80 06 00 00   ····E··· <·@·····
0010  7f 00 00 01 7f 00 00 01  c3 d6 27 0f 26 a0 b6 ab   ........ ··'·&···
0020  da 11 62 9b 50 18 27 f9  7f ea 00 00 67 6f 6f 64   ··b·P·'· ····good
0030  2e 2e                                              ··
```

```
02 00 00 00 45 00 00 44  3c 8c 40 00 80 06 00 00   ····E··D <·@·····
7f 00 00 01 7f 00 00 01  27 0f c3 d6 da 11 62 9b   ........ '·····b·
26 a0 b6 b1 50 18 27 f9  27 b6 00 00 77 68 61 74   &···P·'· '···what
20 69 73 20 79 6f 75 72  20 63 6f 6d 70 75 74 65    is your  compute
72 20 6e 61 6d 65 3f 3f                            r name??
```

```
02 00 00 00 45 00 00 31  3c 8e 40 00 80 06 00 00   ····E··1 <·@·····
7f 00 00 01 7f 00 00 01  c3 d6 27 0f 26 a0 b6 b1   ........ ··'·&···
da 11 62 b7 50 18 27 f9  05 29 00 00 41 79 65 73   ··b·P·'· ·)··Ayes
68 61 2d 50 43                                     ha-PC
```

```
0000  02 00 00 00 45 00 00 39  3c 90 40 00 80 06 00 00   ····E··9 <·@·····
0010  7f 00 00 01 7f 00 00 01  27 0f c3 d6 da 11 62 b7   ........ '·····b·
0020  26 a0 b6 ba 50 18 27 f9  11 1c 00 00 61 6e 64 20   &···P·'· ····and 
0030  6d 61 63 20 61 64 64 72  65 73 73 3f 3f            mac addr ess??
```

```
02 00 00 00 45 00 00 39  3c 92 40 00 80 06 00 00   ····E··9 <·@·····
7f 00 00 01 7f 00 00 01  c3 d6 27 0f 26 a0 b6 ba   ........ ··'·&···
da 11 62 c8 50 18 27 f9  2e b1 00 00 39 38 2d 34   ··b·P·'· ····[redacted]
30 2d 62 62 2d 32 65 2d  39 35 2d 63 64            [redacted]
```

After that, the encrypted text is shared and decrypted text is displayed

```
WAIT its Server's turn!!!!
Server: what is your computer name??
WAIT its Server's turn!!!!
Server: and mac address??
WAIT its Server's turn!!!!
Server: got it
You: okay
WAIT its Server's turn!!!!
Server: now what
You: nothing...
WAIT its Server's turn!!!!
Server: hmm
```

```
Client: Ayesha-PC
You: and mac address??
!!!WAIT Clients turn!!!!
Client: [redacted]
You: got it
!!!WAIT Clients turn!!!!
Client: okay
You: now what
!!!WAIT Clients turn!!!!
Client: nothing...
You: hmm
!!!WAIT Clients turn!!!!
```

```
Length: 61
02 00 00 00 45 00 00 2e  3c 94 40 00 80 06 00 00   ····E··· <·@·····
7f 00 00 01 7f 00 00 01  27 0f c3 d6 da 11 62 c8   ........ '·····b·
26 a0 b6 cb 50 18 27 f9  3b a1 00 00 71 79 64 20   &···P·'· ;···qyd 
73 64                                              sd
```

```
02 00 00 00 45 00 00 37  3c 9e 40 00 80 06 00 00   ····E··7 <·@·····
7f 00 00 01 7f 00 00 01  c3 d6 27 0f 26 a0 b6 d9   ........ ··'·&···
da 11 62 d9 50 18 27 f9  28 46 00 00 42 20 74 66   ··b·P·'· (F··B tf
20 4a 6e 62 6d 62 67 7a  21 21 21                   Jnbmbgz !!!
```