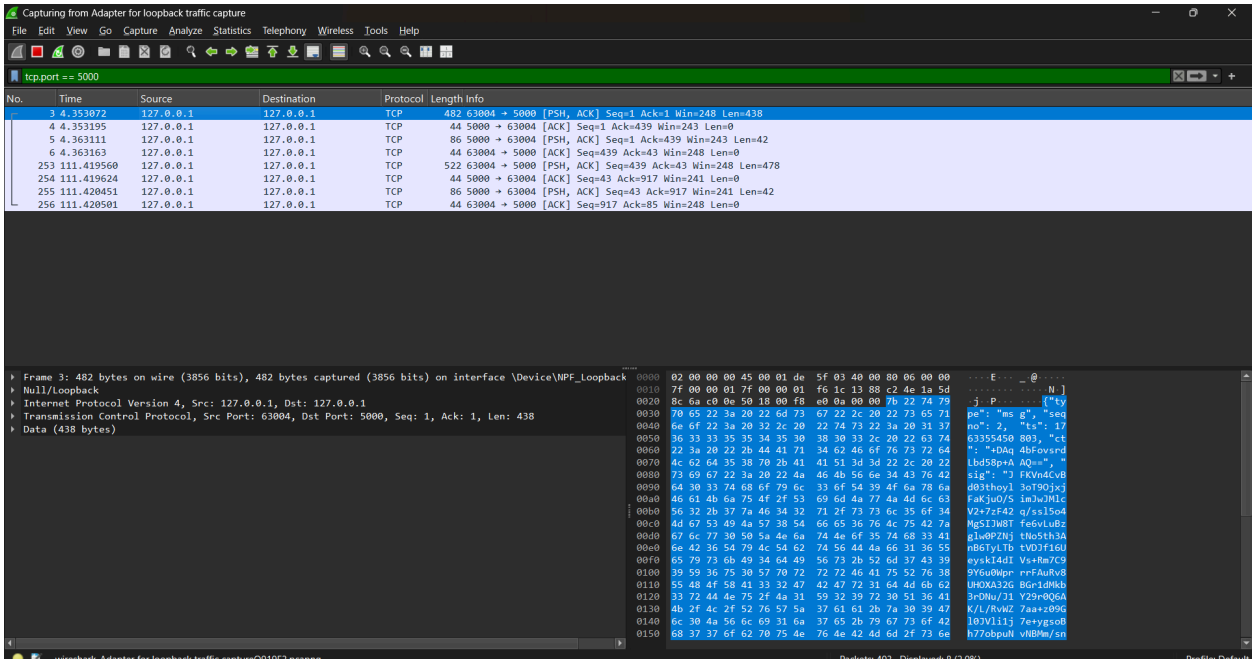
INFORMATION SECURITY

ASSIGNMENT - 2

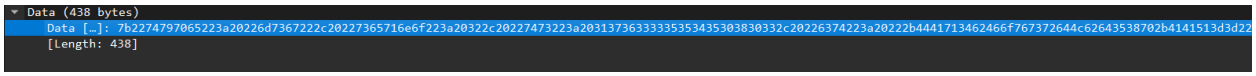
BY:

Saeed Ud Din Ahmad
22i-0938
CS-H

1. Full Handshake Packet (tcp.port == 5000)



2. Encrypted Chat Message

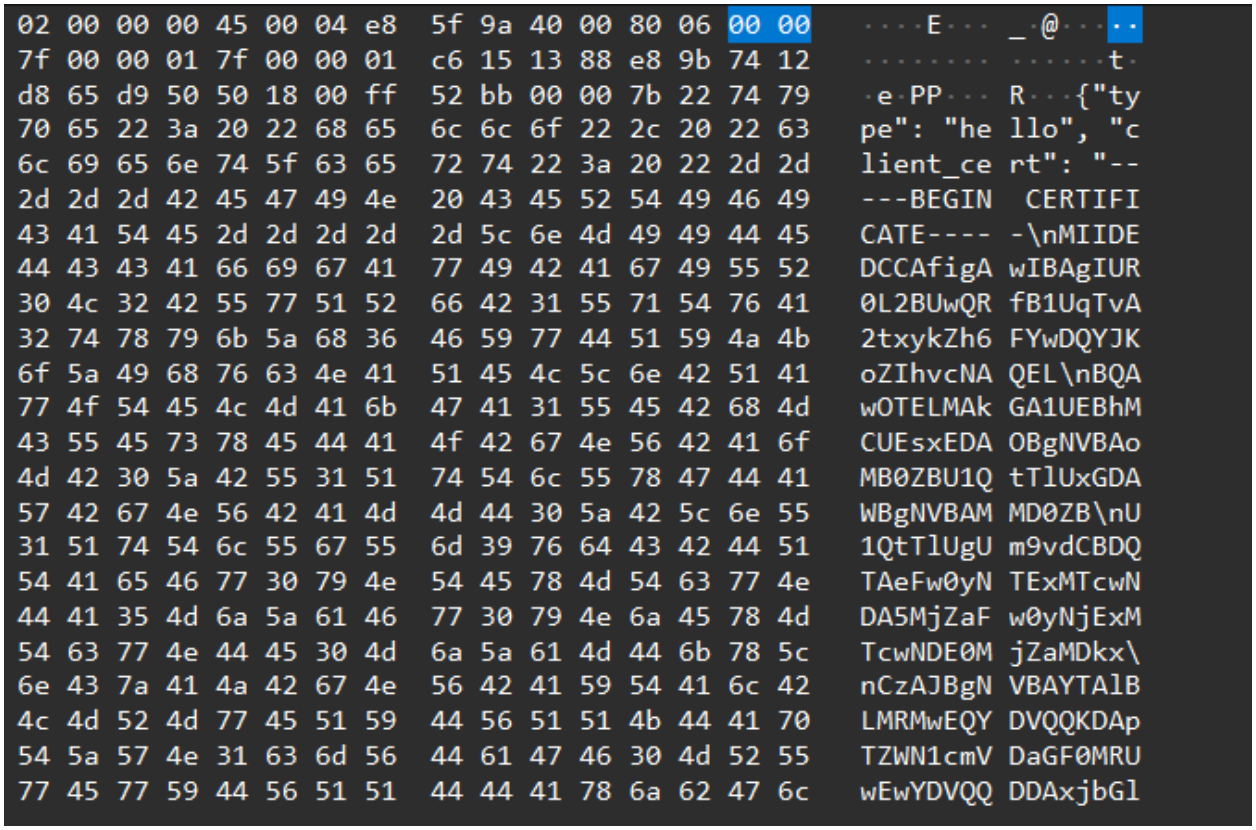


3. ACK from Server (Integrity + Message Sequencing)

No.	Time	Source	Destination	Protocol	Length Info
3	4.353072	127.0.0.1	127.0.0.1	TCP	482 63004 → 5000 [PSH, ACK] Seq=1 Ack=1 Win=248 Len=438
4	4.353195	127.0.0.1	127.0.0.1	TCP	44 5000 → 63004 [ACK] Seq=1 Ack=439 Win=243 Len=0
5	4.363111	127.0.0.1	127.0.0.1	TCP	86 5000 → 63004 [PSH, ACK] Seq=1 Ack=439 Win=243 Len=42
6	4.363163	127.0.0.1	127.0.0.1	TCP	44 63004 → 5000 [ACK] Seq=439 Ack=43 Win=248 Len=0
253	111.419560	127.0.0.1	127.0.0.1	TCP	522 63004 → 5000 [PSH, ACK] Seq=439 Ack=43 Win=248 Len=478
254	111.419624	127.0.0.1	127.0.0.1	TCP	44 5000 → 63004 [ACK] Seq=43 Ack=917 Win=241 Len=0
255	111.420451	127.0.0.1	127.0.0.1	TCP	86 5000 → 63004 [PSH, ACK] Seq=43 Ack=917 Win=241 Len=42
256	111.420501	127.0.0.1	127.0.0.1	TCP	44 63004 → 5000 [ACK] Seq=917 Ack=85 Win=248 Len=0
483	421.283322	127.0.0.1	127.0.0.1	TCP	522 63004 → 5000 [PSH, ACK] Seq=917 Ack=85 Win=248 Len=478
484	421.283389	127.0.0.1	127.0.0.1	TCP	44 5000 → 63004 [ACK] Seq=85 Ack=1395 Win=240 Len=0
485	421.284951	127.0.0.1	127.0.0.1	TCP	86 5000 → 63004 [PSH, ACK] Seq=85 Ack=1395 Win=240 Len=42
486	421.284999	127.0.0.1	127.0.0.1	TCP	44 63004 → 5000 [ACK] Seq=1395 Ack=127 Win=248 Len=0

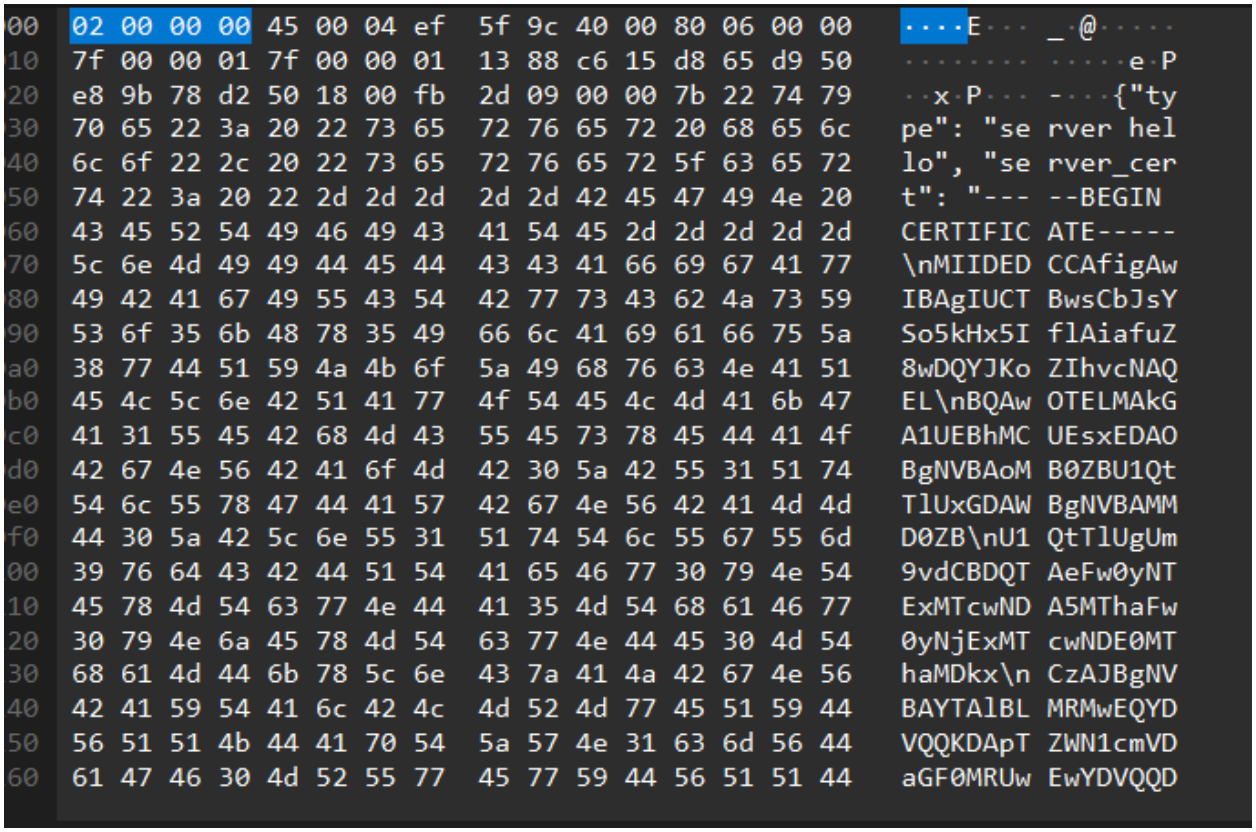
- Server is listening on port 5000
- So packets FROM 5000 → client_port are from the server
- Packets FROM client_port → 5000 are client packets

4. Certificate Exchange



```
02 00 00 00 45 00 04 e8  5f 9a 40 00 80 06 00 00   ····E··· _·@·····
7f 00 00 01 7f 00 00 01  c6 15 13 88 e8 9b 74 12   ········ ·····t·
d8 65 d9 50 50 18 00 ff  52 bb 00 00 7b 22 74 79   ·e·PP··· R···{"ty
70 65 22 3a 20 22 68 65  6c 6c 6f 22 2c 20 22 63   pe": "he llo", "c
6c 69 65 6e 74 5f 63 65  72 74 22 3a 20 22 2d 2d   lient_ce rt": "--
2d 2d 2d 42 45 47 49 4e  20 43 45 52 54 49 46 49   ---BEGIN  CERTIFI
43 41 54 45 2d 2d 2d 2d  2d 5c 6e 4d 49 49 44 45   CATE---- -\nMIIDE
44 43 43 41 66 69 67 41  77 49 42 41 67 49 55 52   DCCAfigA wIBAgIUR
30 4c 32 42 55 77 51 52  66 42 31 55 71 54 76 41   0L2BUwQR fB1UqTvA
32 74 78 79 6b 5a 68 36  46 59 77 44 51 59 4a 4b   2txykZh6 FYwDQYJK
6f 5a 49 68 76 63 4e 41  51 45 4c 5c 6e 42 51 41   oZIhvcNA QEL\nBQA
77 4f 54 45 4c 4d 41 6b  47 41 31 55 45 42 68 4d   wOTELMAk GA1UEBhM
43 55 45 73 78 45 44 41  4f 42 67 4e 56 42 41 6f   CUEsxEDA OBgNVBAo
4d 42 30 5a 42 55 31 51  74 54 6c 55 78 47 44 41   MB0ZBU1Q tTlUxGDA
57 42 67 4e 56 42 41 4d  4d 44 30 5a 42 5c 6e 55   WBgNVBAM MD0ZB\nU
31 51 74 54 6c 55 67 55  6d 39 76 64 43 42 44 51   1QtTlUgU m9vdCBDQ
54 41 65 46 77 30 79 4e  54 45 78 4d 54 63 77 4e   TAeFw0yN TExMTcwN
44 41 35 4d 6a 5a 61 46  77 30 79 4e 6a 45 78 4d   DA5MjZaF w0yNjExM
54 63 77 4e 44 45 30 4d  6a 5a 61 4d 44 6b 78 5c   TcwNDE0M jZaMDkx\
6e 43 7a 41 4a 42 67 4e  56 42 41 59 54 41 6c 42   nCzAJBgN VBAYTAlB
4c 4d 52 4d 77 45 51 59  44 56 51 51 4b 44 41 70   LMRMwEQY DVQQKDAp
54 5a 57 4e 31 63 6d 56  44 61 47 46 30 4d 52 55   TZWN1cmV DaGF0MRU
77 45 77 59 44 56 51 51  44 44 41 78 6a 62 47 6c   wEwYDVQQ DDAxjbGl
```

This is Client Certificate Exchange



Server Hello (Certificate Transmission) – Visible in Wireshark

The Server Hello message is sent in plaintext before Diffie–Hellman is established. Wireshark clearly shows the JSON message containing:

- `type: "server_hello"`
- The full PEM encoded certificate (`"-----BEGIN CERTIFICATE-----"...`)

This demonstrates that certificate exchange happens before encryption, as required by the assignment spec.