

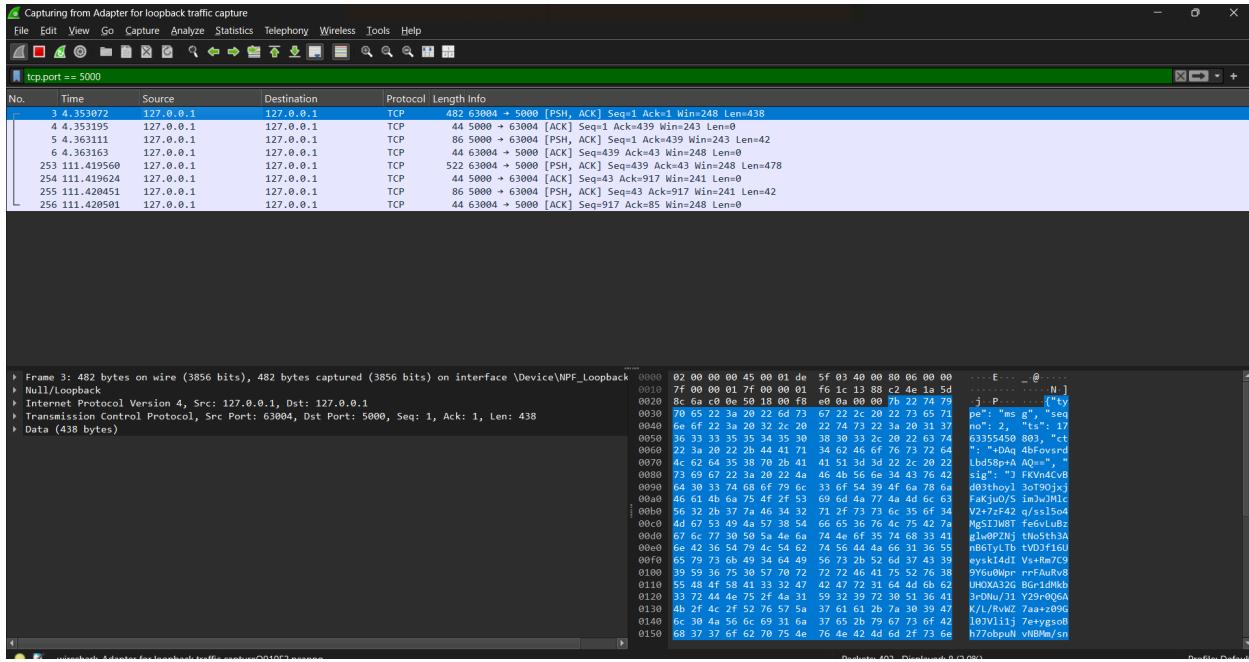
# **INFORMATION SECURITY**

## **ASSIGNMENT - 2**

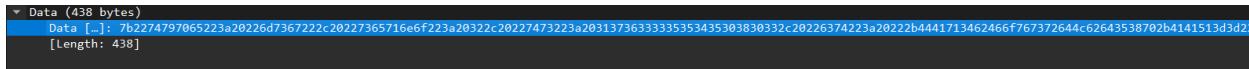
**BY:**

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=439 Win=248 Len=0
253	111.419560	127.0.0.1	127.0.0.1	TCP	522 63004 → 5000 [PSH, ACK] Seq=439 Ack=439 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	111.420591	127.0.0.1	127.0.0.1	TCP	44 63004 → 5000 [ACK] Seq=917 Ack=85 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	.....PP....R...{"ty
d8 65 d9 50 50 18 00 ff	52 bb 00 00 7b 22 74 79	pe": "he llo", "c
70 65 22 3a 20 22 68 65	6c 6c 6f 22 2c 20 22 63	lient_ce rt": "--
6c 69 65 6e 74 5f 63 65	72 74 22 3a 20 22 2d 2d	---BEGIN CERTIFI
2d 2d 2d 42 45 47 49 4e	20 43 45 52 54 49 46 49	CATE-----\nMIIDE
43 41 54 45 2d 2d 2d	2d 5c 6e 4d 49 49 44 45	DCCAfIgA wIBAgIUR
44 43 43 41 66 69 67 41	77 49 42 41 67 49 55 52	0L2BUwQR fB1UqTvA
30 4c 32 42 55 77 51 52	66 42 31 55 71 54 76 41	2txykZh6 FYwDQYJK
32 74 78 79 6b 5a 68 36	46 59 77 44 51 59 4a 4b	oZIhvcNA QEL\nBQA
6f 5a 49 68 76 63 4e 41	51 45 4c 5c 6e 42 51 41	wOTELMAk GA1UEBhM
77 4f 54 45 4c 4d 41 6b	47 41 31 55 45 42 68 4d	CUEsxEDA OBgNVBAo
43 55 45 73 78 45 44 41	4f 42 67 4e 56 42 41 6f	MB0ZBU1Q tTlUxGDA
4d 42 30 5a 42 55 31 51	74 54 6c 55 78 47 44 41	WBgNVBAM MD0ZB\nU
57 42 67 4e 56 42 41 4d	4d 44 30 5a 42 5c 6e 55	1QtTlUgU m9vdCBDQ
31 51 74 54 6c 55 67 55	6d 39 76 64 43 42 44 51	TAeFw0yN TExMTcwN
54 41 65 46 77 30 79 4e	54 45 78 4d 54 63 77 4e	DA5MjZaF w0yNjExM
44 41 35 4d 6a 5a 61 46	77 30 79 4e 6a 45 78 4d	TcwNDE0M jZaMDkx\n
54 63 77 4e 44 45 30 4d	6a 5a 61 4d 44 6b 78 5c	nCzAJBgN VBAYTA1B
6e 43 7a 41 4a 42 67 4e	56 42 41 59 54 41 6c 42	LMRMwEQY DVQQKDAp
4c 4d 52 4d 77 45 51 59	44 56 51 51 4b 44 41 70	TZWN1cmV DaGF0MRU
54 5a 57 4e 31 63 6d 56	44 61 47 46 30 4d 52 55	wEwYDVQQ DDAxjbGl
77 45 77 59 44 56 51 51	44 44 41 78 6a 62 47 6c	

This is Client Certificate Exchange

00	02 00 00 00 45 00 04 ef 5f 9c 40 00 80 06 00 00	....E.... _ @.....
10	7f 00 00 01 7f 00 00 01 13 88 c6 15 d8 65 d9 50	..... . . . . e-P
20	e8 9b 78 d2 50 18 00 fb 2d 09 00 00 7b 22 74 79	..x-P... - - - {"ty
30	70 65 22 3a 20 22 73 65 72 76 65 72 20 68 65 6c	pe": "se rver hel
40	6c 6f 22 2c 20 22 73 65 72 76 65 72 5f 63 65 72	lo", "se rver_cer
50	74 22 3a 20 22 2d 2d 2d 2d 42 45 47 49 4e 20	t": "--- --BEGIN
60	43 45 52 54 49 46 49 43 41 54 45 2d 2d 2d 2d 2d	CERTIFIC ATE-----
70	5c 6e 4d 49 49 44 45 44 43 43 41 66 69 67 41 77	\nMIIDED CCAfigAw
80	49 42 41 67 49 55 43 54 42 77 73 43 62 4a 73 59	IBAgIUCT BwsCbJsy
90	53 6f 35 6b 48 78 35 49 66 6c 41 69 61 66 75 5a	So5kHx5I flAiafuZ
a0	38 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51	8wDQYJKo ZIhvcNAQ
b0	45 4c 5c 6e 42 51 41 77 4f 54 45 4c 4d 41 6b 47	EL\nBQAw OTELMAkG
c0	41 31 55 45 42 68 4d 43 55 45 73 78 45 44 41 4f	A1UEBhMC UEsxEDAO
d0	42 67 4e 56 42 41 6f 4d 42 30 5a 42 55 31 51 74	BgNVBAoM B0ZBU1Qt
e0	54 6c 55 78 47 44 41 57 42 67 4e 56 42 41 4d 4d	TlUxGDAW BgNVBAMM
f0	44 30 5a 42 5c 6e 55 31 51 74 54 6c 55 67 55 6d	D0ZB\nU1 QtTlUgUm
00	39 76 64 43 42 44 51 54 41 65 46 77 30 79 4e 54	9vdCBDQT AeFw0yNT
10	45 78 4d 54 63 77 4e 44 41 35 4d 54 68 61 46 77	ExMTcwND A5MThaFw
20	30 79 4e 6a 45 78 4d 54 63 77 4e 44 45 30 4d 54	0yNjExMT cwNDE0MT
30	68 61 4d 44 6b 78 5c 6e 43 7a 41 4a 42 67 4e 56	haMDkx\n CzAJBgNV
40	42 41 59 54 41 6c 42 4c 4d 52 4d 77 45 51 59 44	BAYTA1BL MRMwEQYD
50	56 51 51 4b 44 41 70 54 5a 57 4e 31 63 6d 56 44	VQQKDApT ZWN1cmVD
60	61 47 46 30 4d 52 55 77 45 77 59 44 56 51 51 44	aGF0MRUw EwYDVQQD

### 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.