

INFORMATION SECURITY

ASSIGNMENT - 2

BY:

Saeed Ud Din Ahmad

22i-0938

CS-H

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

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

Frame 3: 482 bytes on wire (3856 bits), 482 bytes captured (3856 bits) on interface \Device\NPF_{...} Loopback

Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

Transmission Control Protocol, Src Port: 63004, Dst Port: 5000, Seq: 1, Ack: 1, Len: 438

Data (438 bytes)

0000 02 00 00 00 45 00 01 de 5f 03 40 00 80 06 00 00 ...E...@....
0010 7f 00 00 01 7f 00 00 01 f6 1c 13 88 c2 4e 1a 5d ...j...N...
0020 8c 6a c0 0e 50 18 00 f8 e0 0a 00 00 7b 22 74 79 ...j P...["ty
0030 70 65 22 3a 20 22 6d 73 67 22 2c 20 22 73 65 71 ...pE" "ms g", "seq
0040 6e 6f 22 3a 20 32 2c 20 22 74 73 22 3a 20 31 37 ...no": 2, "tct": 17
0050 36 33 33 35 35 34 35 30 38 30 33 2c 20 22 63 74 ...63355450 803, "ct
0060 22 3a 20 22 2b 44 41 71 34 62 46 6f 76 73 72 64 ...": "+Daq 4bFovsrd
0070 4c 62 64 35 38 70 2b 41 41 51 3d 3d 22 2c 20 22 ...lbd58p-A AQ=","
0080 72 69 67 22 3a 20 22 4a 45 4b 56 6e 3a 43 76 42 ...s1g" "3 RWMCuB
0090 64 30 33 74 68 6f 79 6c 33 6f 54 39 4f 6a 78 6a ...a03thoyl 3oT90Jxj
00a0 46 61 4b 6a 75 4f 2f 53 69 6d 4a 77 4a 4d 6c 63 ...FakJu0/S 3mJwM1c
00b0 56 32 2b 37 7a 46 34 32 71 2f 73 73 6c 35 6f 34 ...V2+7zf42 q/s150a
00c0 4d 67 53 49 4a 57 30 5a 66 65 36 76 4c 78 42 7a ...Ag51DhWt f6d4L0z
00d0 67 6c 77 30 50 5a 4a 6a 74 4a 6f 35 74 68 33 41 ...glw0P2nj tHo5th3A
00e0 6e 42 36 54 79 4c 54 62 74 56 44 4a 66 31 36 55 ...nB6TyLTb tV0Jf1G0
00f0 65 79 73 6b 49 34 64 49 56 73 2b 52 6d 37 43 39 ...eyakI4dt Vs+Rm7C9
0100 39 59 36 75 30 57 70 72 72 72 46 41 75 52 76 38 ...9f6u0bnp- nFfAu0v8
0110 55 48 4f 58 41 33 32 47 42 47 72 31 64 44 6b 62 ...tH0XA32G B6r10Nkb
0120 33 72 44 4e 75 2f 4a 31 59 32 39 72 30 51 36 41 ...3r0Nu/31 Y29r0Q6A
0130 4b 2f 4c 2f 52 76 57 5a 37 61 61 2b 7a 30 39 47 ...K/L/RvWZ 7aa+209G
0140 6c 30 4a 56 6c 69 31 6a 37 65 2b 79 67 73 6f 42 ...l0V1l1l3 7e+ysg8
0150 68 37 37 6f 62 70 75 4e 76 4e 42 4d 6d 2f 73 6e ...h770bpuu vNB6w/sr

2. Encrypted Chat Message

No.	Time	Source	Destination	Protocol	Length	Info
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

Data (438 bytes)

[Length: 438]

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 00E... _@... ..
7f 00 00 01 7f 00 00 01 c6 15 13 88 e8 9b 74 12t.
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	ØL2BUwQR 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	MBØZBU1Q tTlUxGDA
57 42 67 4e 56 42 41 4d 4d 44 30 5a 42 5c 6e 55	WBgNVBAM MDØZB\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	TAeFwØyN TExMTcwN
44 41 35 4d 6a 5a 61 46 77 30 79 4e 6a 45 78 4d	DA5MjZaF wØyNjExM
54 63 77 4e 44 45 30 4d 6a 5a 61 4d 44 6b 78 5c	TcwNDEØM jZaMDkx\
6e 43 7a 41 4a 42 67 4e 56 42 41 59 54 41 6c 42	nCzAJBgN VBAYTA1B
4c 4d 52 4d 77 45 51 59 44 56 51 51 4b 44 41 70	LMRMwEQY DVQØKDap
54 5a 57 4e 31 63 6d 56 44 61 47 46 30 4d 52 55	TZWN1cmV DaGFØMRU
77 45 77 59 44 56 51 51 44 44 41 78 6a 62 47 6c	wEwYDVQØ DDAxjbG1

This is Client Certificate Exchange

00	02 00 00 00	45 00 04 ef	5f 9c 40 00 80 06 00 00E..._@.....
10	7f 00 00 01	7f 00 00 01	13 88 c6 15 d8 65 d9 50e 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 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 fIAiafuZ
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	VQKKDApT 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.