

Assignment 13

Part-2

1. The packet number in trace that contains the initial TCP SYN message is: **2368**

2368	21.149406608	10.250.61.113	128.119.240.84	TCP	74 48956 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2338749688 TSecr=0 ...
2369	21.149523592	10.250.61.113	128.119.240.84	TCP	74 48968 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2338749688 TSecr=0 ...
2375	21.395652593	128.119.240.84	10.250.61.113	TCP	66 443 → 48956 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
2376	21.395734732	10.250.61.113	128.119.240.84	TCP	54 48956 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
2377	21.397788484	10.250.61.113	128.119.240.84	TLSv1.2	720 Client Hello (SNI=www.cics.umass.edu)

2. After a TCP connection has been established through a TCP handshake, The TLS handshake takes place.

Part-3

1. The packet number in trace that contains the TLS Client Hello Message is: **2377**
2. The version of TLS as declared in the Client Hello Message: **TLSv1.2**
3. **17** cipher suites are supported by our client as declared in the client Hello message.

Cipher Suites Length: 34

> Cipher Suites (17 suites)

4. The first two hexadecimal digits in the random bytes field of the Client Hello message are: **d7**

Version: TLS 1.2 (0x0303)

> Random: d714ec03ed1741521f42ca4af95aaafea4bf5d577fd764630f5b392a2a3ee15d

Session ID Length: 32

5. The premaster secret is created using the random bytes. That is, a shared secret key known as the pre master key is created by combining the random bytes with additional information sent during the TLS handshake.

Part-4

2389	21.648945323	128.119.240.84	10.250.61.113	TLSv1.2	1514 Server Hello
2390	21.648975388	10.250.61.113	128.119.240.84	TCP	54 48956 → 443 [ACK] Seq=667 Ack=1461 Win=64128 Len=0
2391	21.649580224	128.119.240.84	10.250.61.113	TCP	2690 443 → 48956 [PSH, ACK] Seq=1461 Ack=667 Win=30592 Len=2636 [TCP segment of a reassem..
2392	21.649602873	10.250.61.113	128.119.240.84	TCP	54 48956 → 443 [ACK] Seq=667 Ack=4097 Win=63616 Len=0
2393	21.656660051	128.119.240.84	10.250.61.113	TLSv1.2	1277 Certificate, Server Key Exchange, Server Hello Done

1. The packet number in the trace that contains the TLD Server Hello message is: **2389**

2. The cipher suite chosen by the server is:

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

Compression Method: null (0)

3. **Yes**, the server Hello message contains random bytes, similar to how the Client Hello message contained random bytes. The purpose of the random bytes is to provide assurance that the person you want to connect with is genuinely present and participating in the conversation, rather than just playing back a recorded session to you and possibly passing for someone else.

This is made possible by the randomization, which stops attackers from simulating a number of sessions beforehand and then choosing the most pertinent one for you.

4. The packet number in the trace for the TLS message part that contains the public key certificate is: **2393**

5. The server return **3 certificates**, These are not all for www.cs.umass.edu

The certificates are for:

- InCommon RSA Server CA
- USERTrust RSA Certification Authority

2393	21.656660051	128.119.240.84	10.250.61.113	TLSv1.2	1277	Certificate, Server Key Exchange, Server Hello Done
						Length: 4893
						Certificates Length: 4890
						✓ Certificates (4890 bytes)
						Certificate Length: 1842
						> Certificate [truncated]: 3082072e30820616a00302010202103090854915311cde05eb63eb0
						Certificate Length: 1533
						> Certificate [truncated]: 308205f9308203e1a00302010202104720d0fa85461a7e17a164029
						Certificate Length: 1506
						> Certificate [truncated]: 308205de308203c6a003020102021001fd6d30fca3ca51a81bbc640
						0000 d8 5e d3 54 2f a7 02 04 96 9a 82
						0010 04 ef 1c 01 40 00 26 06 7a b1 80
						0020 3d 71 01 bb bf 3c 6f 4b 07 7b 78
						0030 00 ef 08 80 00 00 69 c7 6b 8c 60
						0040 df e1 32 ae cc 93 3b 51 78 95 67
						0050 0c d0 69 0f 1b 0f f3 25 26 6b 33
						0060 73 43 e5 7e 0e a5 66 b1 29 7c 32
						0070 0d c1 93 54 30 19 13 ac d3 7d 37
						0080 35 5c db 41 d7 12 da a9 49 0b df
						0090 62 8a b5 66 cf 25 88 cd 84 b8 b1
						00a0 02 9e eb 12 4c 95 7c f3 6b 05 a9

6. The name of the certification authority that issued the certificate for

id-at-commonName=www.cs.umass.edu is **University of Massachusetts Amherst**

```
✓ rdnSequence: 4 items (id-at-commonName=www.cs.umass.edu,id-at-organizationName=University of Massachusetts Amherst,
  > RDNSSequence item: 1 item (id-at-countryName=US)
  > RDNSSequence item: 1 item (id-at-stateOrProvinceName=Massachusetts)
  > RDNSSequence item: 1 item (id-at-organizationName=University of Massachusetts Amherst)
  > RDNSSequence item: 1 item (id-at-commonName=www.cs.umass.edu)
```

7. The digital signature algorithm used by the CA to sign this certificate is **1.2.840.113549.1.1.12 (sha256WithRSAEncryption)(sha384WithRSAEncryption)**

8. The first 4 hexadecimal digits of the modulus of the public key being used by www.cics.umass.edu are: **00b3**

```
✓ subjectPublicKey [truncated]: 3082010a0282010100b39e7296158da80176a2f1035c7c61f06120f98!
  modulus: 0x00b39e7296158da80176a2f1035c7c61f06120f9852aad0d20d4931a30842fec1b8724...
  publicExponent: 65537
```

9. The packet number in the trace for the TLS message part that contains the Server Hello Done TLS record is: **2393**

Part-5

1. The packet number in the trace for the TLS message that contains the public key information, Change Cipher Spec and Encrypted Handshake message is: **2395**

2392	21.649602873	10.250.61.113	128.119.240.84	TCP	54	48956 → 443 [ACK] Seq=667 Ack=4097 Win=63616 Len=0
2393	21.656660051	128.119.240.84	10.250.61.113	TLSv1.2	1277	Certificate, Server Key Exchange, Server Hello Done
2394	21.656674341	10.250.61.113	128.119.240.84	TCP	54	48956 → 443 [ACK] Seq=667 Ack=5320 Win=64128 Len=0
2395	21.657927688	10.250.61.113	128.119.240.84	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2396	21.660972956	128.119.240.84	10.250.61.113	TCP	60	443 → 48968 [ACK] Seq=1 Ack=667 Win=30592 Len=0

2. **No.** the client doesn't provide its own CA-signed public key certificate back to the server.

Part-6

1. The given below symmetric key cryptography algorithm is being used by the client and server to encrypt application data: **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)**

2. The symmetric key cryptography algorithm to be used for securing the communication is finally decided and declared during the **"Cipher Suite Negotiation"** step in the **"ClientHello"** and **"ServerHello"** messages in the TLS handshake protocol.

3. Packet no **2449** contains the first encrypted message carrying application data from client to server.

ip.addr == 128.119.240.84						
No.	Time	Source	Destination	Protocol	Length	Info
2449	21.912791761	10.250.61.113	128.119.240.84	TLSv1.2	539	Application Data

4. We will see the content based on the home page and then it will get encrypted.
5. The client-to-server TLS message that terminates the TLS connection is contained in packet number **12306**