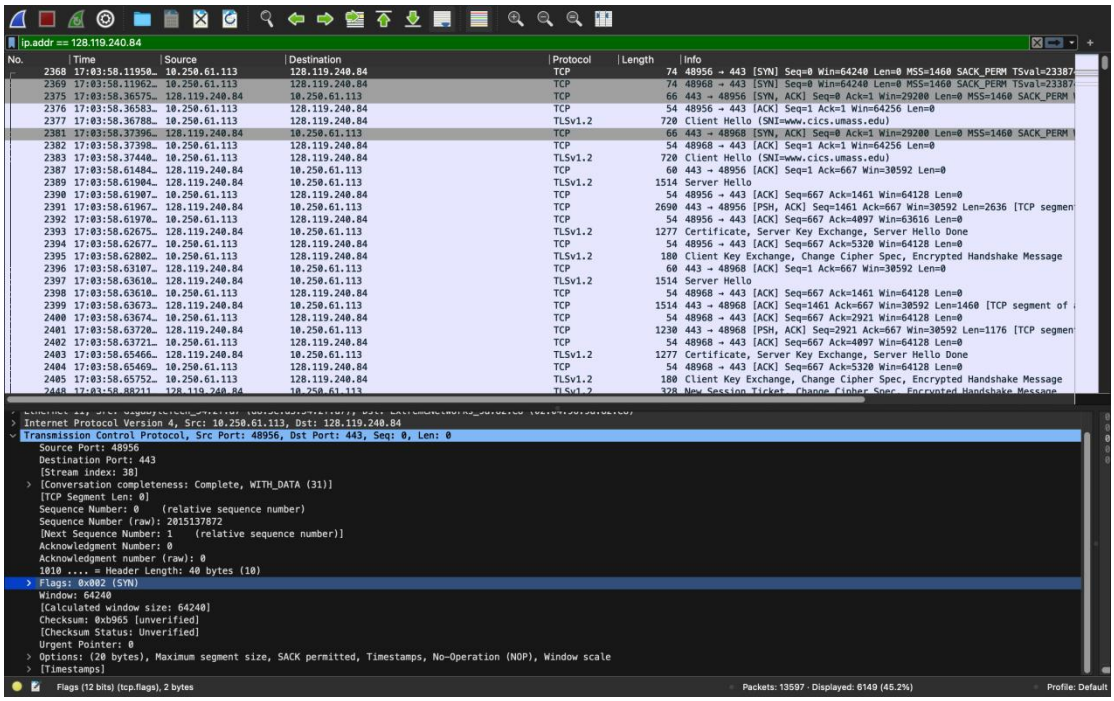
Assignment 13
210010033

Part 2:

1.

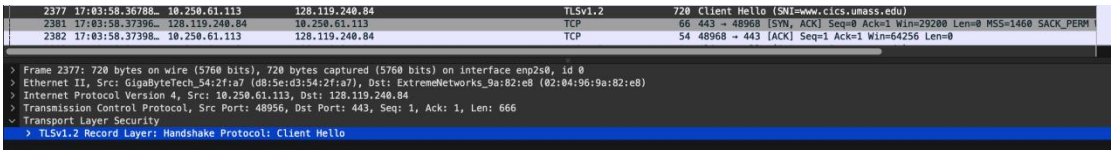


Frame No. 2368 contains the SYN message for the TCP connection.

2. Yes, the first TLS message is sent from the client, since TLS is built on top of TCP/IP, the client must first complete the 3-way TCP handshake with the server.

Part 3:

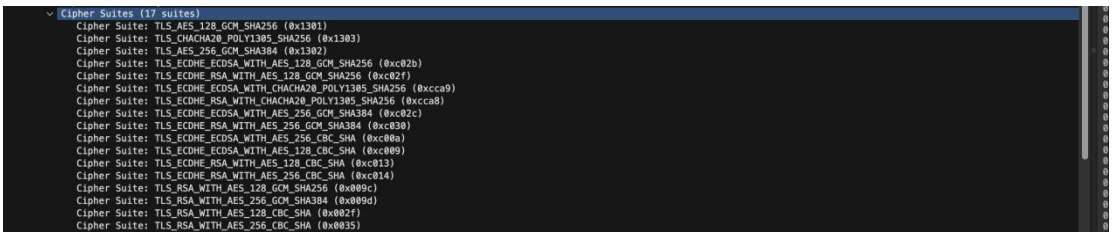
1.



TLS client HELLO message is contained in packet number 2377 in the trace.

2. TLSv1.2 is running as declared in the client HELLO message.

3.



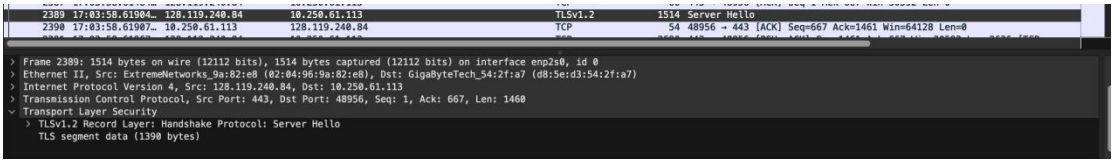
17 cipher suites are supported by the client.

4. The first two hex digits in random bytes are as follows: ed

5. The inclusion of random bytes in the Client HELLO message enhances the security of the TLS handshake by adding randomness, generating key material, and preventing predictable patterns that could be exploited by attackers. Required to compute master_secret key.

Part 4:

1.

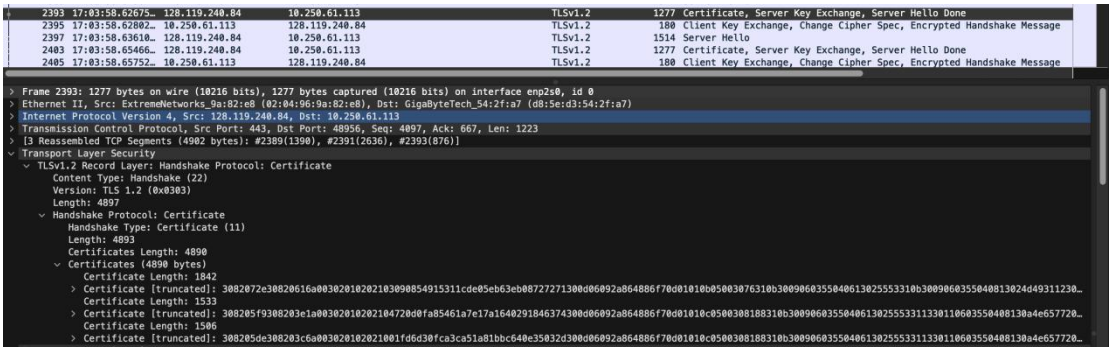


Packet No. 2389 contains the Server Hello message.

2. Cipher Suite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) has been chosen by the server from among those offered by the client.

3. Yes, the server Hello message also contain the random bytes as sent by the client.

4.



Packet No. 2393 contains the public key certificate for www.cics.umass.edu server.

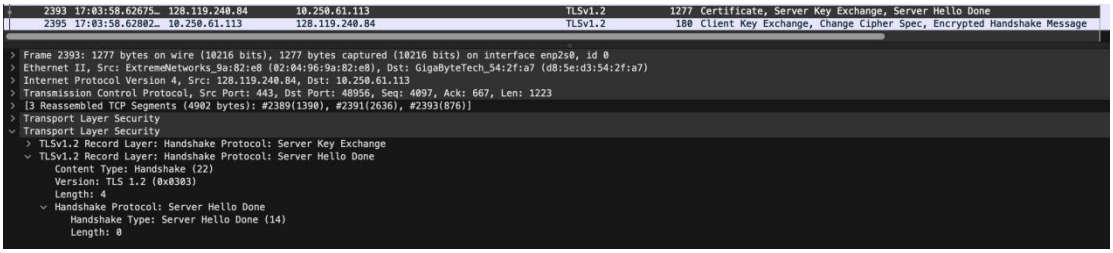
5. 3 certificates are returned, only one of these certificates is for www.cs.umass.edu , the remaining two are for USERTrust RSA Certification Authority and InCommon RSA Server CA

6. InCommon RSA Server CA is the name of the organisation that issued the certificate for www.cs.umass.edu

7. sha256WithRSAEncryption is the algorithm used.

8. 00b3 are the first four hex digits of the mod of the public key used by www.cs.umass.edu

9.



Packet No. 2393 contains the server Hello Done message.

Part 5:

1.

```
2395  21.65792…  10.250.61.113   128.119.240.84  TLSv1.2   180  Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

> Frame 2395: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface enp2s0, id 0
> Ethernet II, Src: GigaByteTech_54:2f:a7 (d8:5e:d3:54:2f:a7), Dst: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8)
> Internet Protocol Version 4, Src: 10.250.61.113, Dst: 128.119.240.84
> Transmission Control Protocol, Src Port: 48956, Dst Port: 443, Seq: 667, Ack: 5320, Len: 126
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 70
    v Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 66
      > EC Diffie-Hellman Client Params
  v TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
      Change Cipher Spec Message
  v TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 40
      Handshake Protocol: Encrypted Handshake Message
```

Frame No. 2395 contains the public key information, Change Cipher Spec, and Encrypted Handshake message, being sent from client to server.

2. No, the client does not provide its CA-signed public key certificate back to the server.

Part 6:

1.

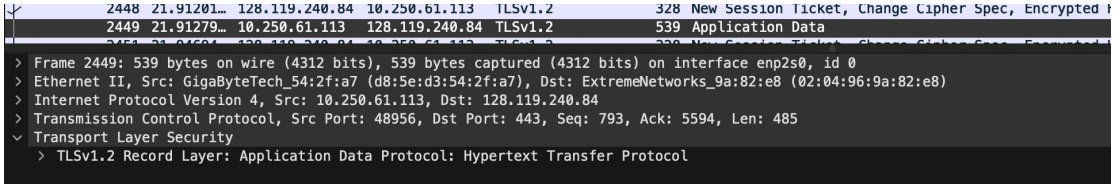
```
2403  21.68457…  128.119.240.84  10.250.61.113   TLSv1.2   1277  Certificate, Server Key Exchange, Server Hello Done
2405  21.68742…  10.250.61.113   128.119.240.84  TLSv1.2   180   Client Key Exchange, Change Cipher Spec, Encrypted Ha

> Frame 2403: 1277 bytes on wire (10216 bits), 1277 bytes captured (10216 bits) on interface enp2s0, id 0
> Ethernet II, Src: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8), Dst: GigaByteTech_54:2f:a7 (d8:5e:d3:54:2f:a7)
> Internet Protocol Version 4, Src: 128.119.240.84, Dst: 10.250.61.113
> Transmission Control Protocol, Src Port: 443, Dst Port: 48968, Seq: 4097, Ack: 667, Len: 1223
> [4 Reassembled TCP Segments (4902 bytes): #2397(1390), #2399(1460), #2401(1176), #2403(876)]
v Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: Certificate
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 333
    v Handshake Protocol: Server Key Exchange
        Handshake Type: Server Key Exchange (12)
        Length: 329
      > EC Diffie-Hellman Server Params
  > TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
```

EC Diffie-Hellman is the symmetric algorithm used by the client and server to encrypt application data(in case of HTTP)

2. It was decided in frame no. 2403 in the Server key exchange message.

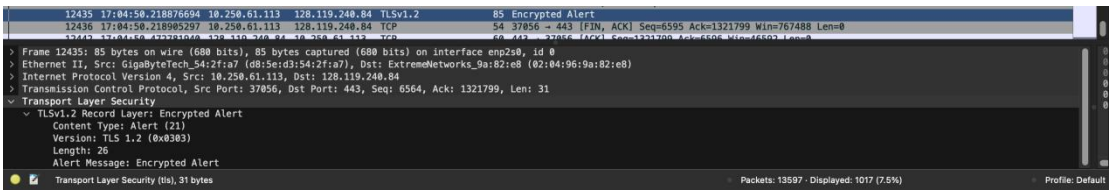
3.



Packet No. 2449 contains first encrypted message carrying application data from client to server.

4. The encrypted application data would include the HTTP requests from the client to the server.

5.



Packet No. 12435 might be the packet which that finally shuts down the TLS connection between the server and the client because its the last Encrypted Alert sent and after this is the last TCP [FIN,ACK] message between the client and www.cs.umass.edu server after which we do not find any communication between these two.