

# Assignment 13

## 210010033

### Part 2:

1.

The image shows a Wireshark packet capture of a network connection. The top pane displays a list of packets. Packet 2368 is a TCP SYN message from 10.250.61.113 to 128.119.240.84. The bottom pane shows the details of packet 2368, which is a Transmission Control Protocol (TCP) segment. The details pane shows the source port as 48956, destination port as 443, and the sequence number as 0. The flags field shows SYN. The window size is 64240. The checksum is 0xb965 (unverified). The urgent pointer is 0. The options field shows (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale, and Timestamps. The packet is 12 bytes (tcp.flags) and 2 bytes (tcp.options).

No.	Time	Source	Destination	Protocol	Length	Info
2368	17:03:58.11950	10.250.61.113	128.119.240.84	TCP	74	48956 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=23387
2375	17:03:58.36575	128.119.240.84	10.250.61.113	TCP	66	443 → 48956 [SYN, ACK] Seq=0 Ack=1 Win=29280 Len=0 MSS=1460 SACK_PERM
2376	17:03:58.36583	10.250.61.113	128.119.240.84	TCP	54	48956 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
2377	17:03:58.36788	10.250.61.113	128.119.240.84	TLSv1.2	720	Client Hello (SNI=www.cics.umass.edu)
2381	17:03:58.37396	128.119.240.84	10.250.61.113	TCP	66	443 → 48956 [SYN, ACK] Seq=0 Ack=1 Win=29280 Len=0 MSS=1460 SACK_PERM
2382	17:03:58.37398	10.250.61.113	128.119.240.84	TCP	54	48956 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
2383	17:03:58.37440	10.250.61.113	128.119.240.84	TLSv1.2	720	Client Hello (SNI=www.cics.umass.edu)
2387	17:03:58.61484	128.119.240.84	10.250.61.113	TCP	68	443 → 48956 [ACK] Seq=1 Ack=667 Win=38592 Len=0
2389	17:03:58.61904	128.119.240.84	10.250.61.113	TLSv1.2	1514	Server Hello
2390	17:03:58.61907	10.250.61.113	128.119.240.84	TCP	54	48956 → 443 [ACK] Seq=667 Ack=1461 Win=64128 Len=0
2391	17:03:58.61967	128.119.240.84	10.250.61.113	TCP	2690	443 → 48956 [PSH, ACK] Seq=1461 Ack=667 Win=38592 Len=2636 [TCP segmen
2392	17:03:58.61970	10.250.61.113	128.119.240.84	TCP	54	48956 → 443 [ACK] Seq=667 Ack=4897 Win=63616 Len=0
2393	17:03:58.62675	128.119.240.84	10.250.61.113	TLSv1.2	1277	Certificate, Server Key Exchange, Server Hello Done
2394	17:03:58.62677	10.250.61.113	128.119.240.84	TCP	54	48956 → 443 [ACK] Seq=667 Ack=5320 Win=64128 Len=0
2395	17:03:58.62802	10.250.61.113	128.119.240.84	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2396	17:03:58.63107	128.119.240.84	10.250.61.113	TCP	68	443 → 48956 [ACK] Seq=1 Ack=667 Win=38592 Len=0
2397	17:03:58.63610	128.119.240.84	10.250.61.113	TLSv1.2	1514	Server Hello
2398	17:03:58.63610	10.250.61.113	128.119.240.84	TCP	54	48956 → 443 [ACK] Seq=667 Ack=1461 Win=64128 Len=0
2399	17:03:58.63673	128.119.240.84	10.250.61.113	TCP	1514	443 → 48956 [ACK] Seq=1461 Ack=667 Win=38592 Len=1468 [TCP segment of
2400	17:03:58.63674	10.250.61.113	128.119.240.84	TCP	54	48956 → 443 [ACK] Seq=667 Ack=2921 Win=64128 Len=0
2401	17:03:58.63720	128.119.240.84	10.250.61.113	TCP	1230	443 → 48956 [PSH, ACK] Seq=2921 Ack=667 Win=38592 Len=1176 [TCP segmen
2402	17:03:58.63721	10.250.61.113	128.119.240.84	TCP	54	48956 → 443 [ACK] Seq=667 Ack=4897 Win=64128 Len=0
2403	17:03:58.65466	128.119.240.84	10.250.61.113	TLSv1.2	1277	Certificate, Server Key Exchange, Server Hello Done
2404	17:03:58.65469	10.250.61.113	128.119.240.84	TCP	54	48956 → 443 [ACK] Seq=667 Ack=5320 Win=64128 Len=0
2405	17:03:58.65752	10.250.61.113	128.119.240.84	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2406	17:03:58.68211	128.119.240.84	10.250.61.113	TLSv1.2	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message

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.

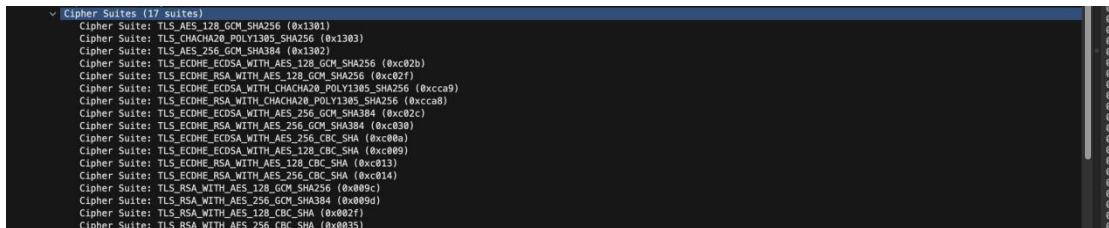
The image shows a Wireshark packet capture of a network connection. The top pane displays a list of packets. Packet 2377 is a TLS Client Hello message from 10.250.61.113 to 128.119.240.84. The bottom pane shows the details of packet 2377, which is a TLSv1.2 record layer. The details pane shows the source port as 48956, destination port as 443, and the sequence number as 1. The flags field shows SYN. The window size is 64240. The checksum is 0xb965 (unverified). The urgent pointer is 0. The options field shows (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale, and Timestamps. The packet is 12 bytes (tcp.flags) and 2 bytes (tcp.options).

No.	Time	Source	Destination	Protocol	Length	Info
2377	17:03:58.36788	10.250.61.113	128.119.240.84	TLSv1.2	720	Client Hello (SNI=www.cics.umass.edu)
2381	17:03:58.37396	128.119.240.84	10.250.61.113	TCP	66	443 → 48956 [SYN, ACK] Seq=0 Ack=1 Win=29280 Len=0 MSS=1460 SACK_PERM
2382	17:03:58.37398	10.250.61.113	128.119.240.84	TCP	54	48956 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0

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.



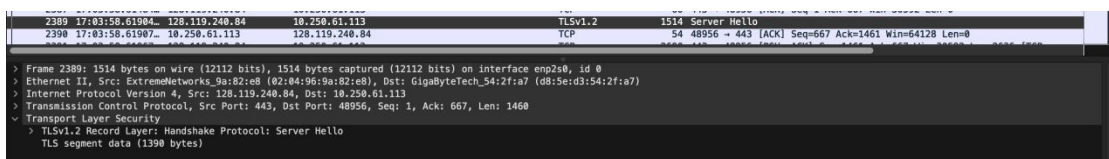
```
▼ Cipher Suites (17 suites)
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc030)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc031)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x0090)
Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
```

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.



```
2389 17:03:58.619041 128.119.240.84 10.250.61.113 TLSv1.2 1514 Server Hello
2390 17:03:58.619071 18.250.61.113 128.119.240.84 TCP 54 48956 → 443 [ACK] Seq=667 Ack=1461 Win=64128 Len=0

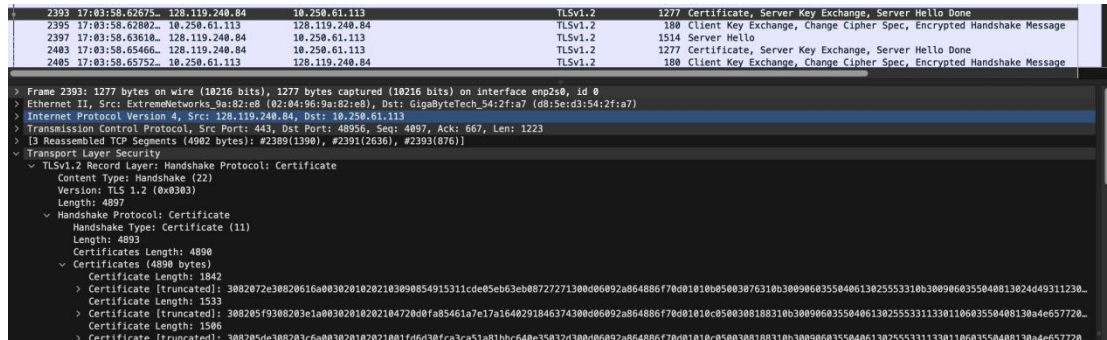
> Frame 2389: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface enp2s8, id 0
> Ethernet II, Src: ExtremeNetworks_9a:18:2e:a8 (02:04:9b:9a:18:2e:a8), Dst: GigabyteTech_94:2f:a7 (08:5e:d3:54:2f:a7)
> Internet Protocol Version 4, Src: 128.119.240.84, Dst: 10.250.61.113
> Transmission Control Protocol, Src Port: 443, Dst Port: 48956, Seq: 1, Ack: 667, Len: 1460
> Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    TLS segment data (1398 bytes)
```

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.

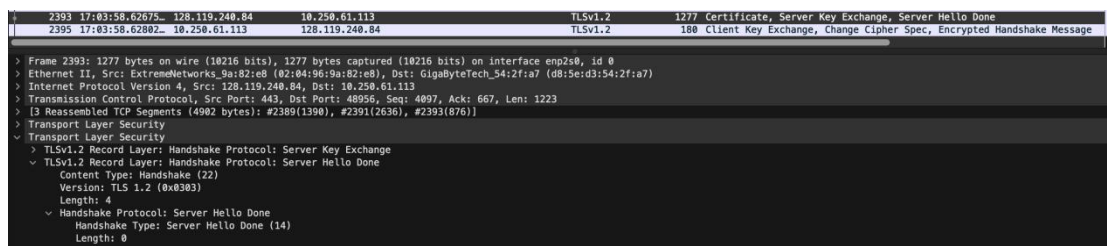
4.



The image shows a Wireshark packet capture of a TLS handshake. The top section lists several packets: 2393 (17:03:58.62675- 128.119.240.84 to 10.250.61.113) is a TLSv1.2 1277 Certificate, Server Key Exchange, Server Hello Done; 2395 (17:03:58.62802- 10.250.61.113 to 128.119.240.84) is a TLSv1.2 188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message; 2397 (17:03:58.63610- 128.119.240.84 to 10.250.61.113) is a TLSv1.2 1514 Server Hello; 2403 (17:03:58.65466- 128.119.240.84 to 10.250.61.113) is a TLSv1.2 1277 Certificate, Server Key Exchange, Server Hello Done; and 2405 (17:03:58.65752- 10.250.61.113 to 128.119.240.84) is a TLSv1.2 188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message. The main pane shows the details of packet 2393, which is a TLSv1.2 Record Layer: Handshake Protocol: Certificate. The content type is Handshake (22), version is TLS 1.2 (0x0303), and length is 4897. The handshake type is Certificate (11). The length is 4893. The certificates length is 4890. The certificates (4890 bytes) section shows a certificate (length 1842) which is truncated, and a certificate (length 1533) which is also truncated. The certificate (length 1506) is truncated. The certificate (length 1506) is truncated.

Packet No. 2393 contains the public key certificate for [www.cics.umass.edu](http://www.cics.umass.edu) server.

5. 3 certificates are returned, only one of these certificates is for [www.cs.umass.edu](http://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](http://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](http://www.cs.umass.edu)
- 9.



The image shows a Wireshark packet capture of a TLS handshake. The top section lists several packets: 2393 (17:03:58.62675- 128.119.240.84 to 10.250.61.113) is a TLSv1.2 1277 Certificate, Server Key Exchange, Server Hello Done; 2395 (17:03:58.62802- 10.250.61.113 to 128.119.240.84) is a TLSv1.2 188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message; 2397 (17:03:58.63610- 128.119.240.84 to 10.250.61.113) is a TLSv1.2 1514 Server Hello; 2403 (17:03:58.65466- 128.119.240.84 to 10.250.61.113) is a TLSv1.2 1277 Certificate, Server Key Exchange, Server Hello Done; and 2405 (17:03:58.65752- 10.250.61.113 to 128.119.240.84) is a TLSv1.2 188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message. The main pane shows the details of packet 2393, which is a TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange. The content type is Handshake (22), version is TLS 1.2 (0x0303), and length is 4. The handshake type is Server Hello Done (14). The length is 0.

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
> Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 70
    > Handshake Protocol: Client Key Exchange
      Handshake Type: Client Key Exchange (16)
      Length: 66
      > EC Diffie-Hellman Client Params
  > 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
  > 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:

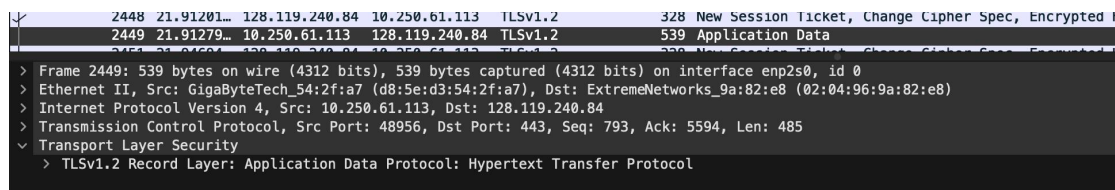
1.

```
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 Handshake Message
> 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)]
> Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: Certificate
  > Transport Layer Security
    > TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 333
      > 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.

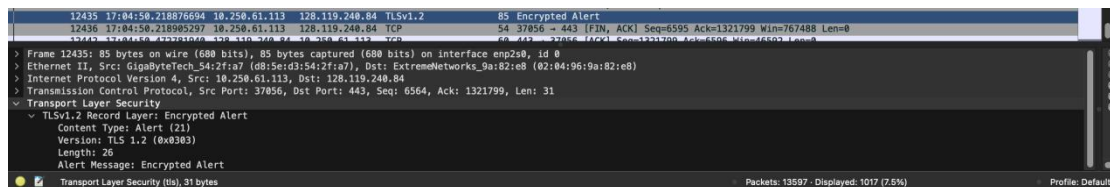
3.



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](http://www.cs.umass.edu) server after which we do not find any communication between these two.