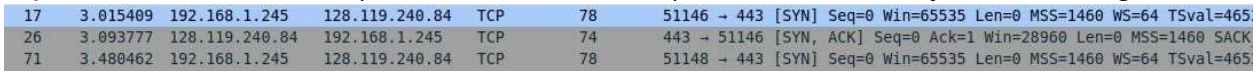
ACN ASSIGNMENT – 8 (TLS)

Name – Aman Singh
Enrollment no. –0801IT221018

1) What is the packet number in your trace that contains the initial TCP SYN message? (By "packet number," we meant the number in the "No." column at the left of the Wireshark display, not the sequence number in the TCP segment itself). **Ans)** The packet no. is 17 of initial TCP SYN message.

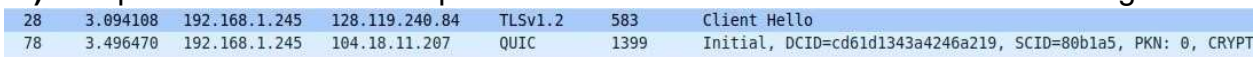
2) Is the TCP connection set up before or after the first TLS message is sent from client to server?

Ans) The TCP handshake (SYN, SYN-ACK, ACK) occurs before any TLS messages**.**



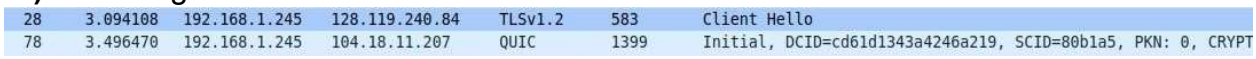
3) What is the packet number in your trace that contains the TLS Client Hello message?

Ans) The packet no. is 28 of the packet that contains the TLS Client Hello message

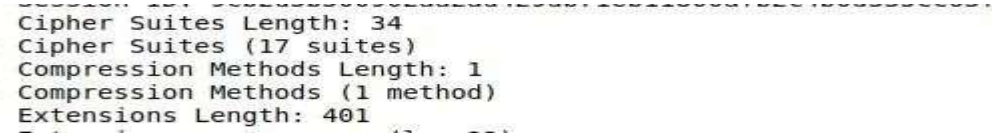


4) What version of TLS is your client running, as declared in the Client Hello message?

Ans) It is using TLSv1.2.



5) How many cipher suites are supported by your client, as declared in the Client Hello message? A cipher suite is a set of related cryptographic algorithms that determine how session keys will be derived, and how data will be encrypted and be digitally signed via a HMAC algorithm.



6) Your client generates and sends a string of "random bytes" to the server in the Client Hello message. What are the first two hexadecimal digits in the random bytes field of the Client Hello message? Enter the two hexadecimal digits (without spaces between the hex digits and without any leading '0x' , using lowercase letters where needed). Hint: be careful to fully dig into the Random field to find the Random Bytes subfield (do not consider the GMT UNIX Time subfield of Random).

Ans) The first two are 4 , 2.

Name – Aman Singh
Enrollment no. –0801IT221018

```
Random: 421623e04b909a780b955b1a679367e8af0312ec2362979794c50c162089004
    GMT Unix Time: Feb 18, 2005 17:20:32.000000000 UTC
    Random Bytes: 4b909a780b955b1a679367e8af0312ec2362979794c50c1620890
Session ID Length: 32
Session ID: 9cb2d5b500902aa2ad429db71eb11800afb2c4b0d335cc63f7bcc8defe8
```

7)What is the purpose(s) of the "random bytes" field in the Client Hello message? Note: you'll have do some searching and reading to get the answer to this question; see section 8.6 and in RFC 5246 (section 8.1 in RFC 5246 in particular).
Ans) The purpose of random bytes field in the client hello message is to generate key and to prevent from relplay attacks.

8) What is the packet number in your trace that contains the TLS Server Hello message?

Ans) The packet number is 32.

```
32   3.172673  128.119.240.84  192.168.1.245  TLSv1.2   1514   Server Hello
80   3.504910  104.18.11.207   192.168.1.245  QUIC      1242   Initial, DCID=80b1a5, SCID=01db9625e7dffc
```

9) Which cipher suite has been chosen by the server from among those offered in the earlier Client Hello message?
Ans)

```
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Compression Method: null (0)
```

10) Does the Server Hello message contain random bytes, similar to how the Client Hello message contained random bytes? And if so, what is/are their purpose(s)?
Ans) similar to the Client Hello message, they help in key generation.

11) What is the packet number in your trace for the TLS message part that contains the public key certificate for the www.cics.umass.edu server (actually the www.cs.umass.edu server)?

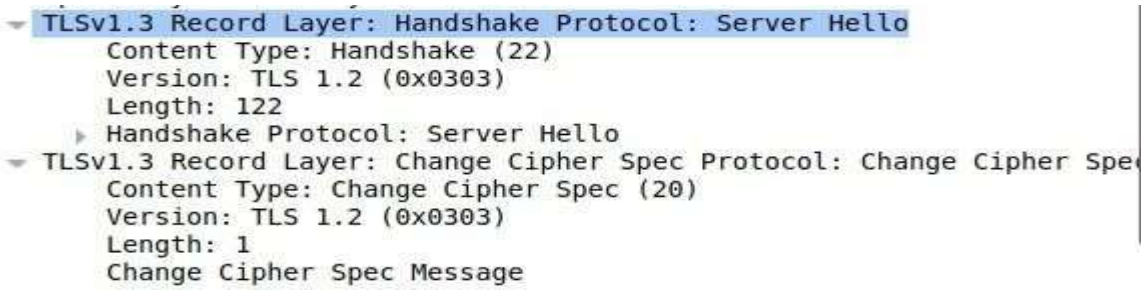
Ans)

```
80    3.504910  104.18.11.207   192.168.1.245  QUIC      1242   Initial, DCID=80b1a5, SCID=01db9625e7dffcd4cddb85242e
103   3.523655  52.222.149.109  192.168.1.245  TLSv1.3   1494   Server Hello, Change Cipher Spec, Application Data
```

12) A server may return more than one certificate. If more than one certificate is returned, are all of these certificates for www.cs.umass.edu? If not all are for www.cs.umass.edu, then who are these other certificates for? You can determine who the certificate is for by checking the id-at-commonName field in the retuned certificate.

Name – Aman Singh
Enrollment no. –0801IT221018

Ans)



13) What is the name of the certification authority that issued the certificate for idat-commonName=www.cs.umass.edu?

Ans)

14) What digital signature algorithm is used by the CA to sign this certificate? Hint: this information can be found in signature subfield of the SignedCertificate field of the certificate for www.cs.umass.edu.

Ans)

15) Let's take a look at what a real public key looks like! What are the first four hexadecimal digits of the modulus of the public key being used by www.cics.umass.edu? Enter the four hexadecimal digits (without spaces between the hex digits and without any leading '0x' , using lowercase letters where needed, and including any leading 0s after '0x'). Hint: this information can be found in subjectPublicKeyInfo subfield of the SignedCertificate field of the certificate for www.cs.umass.edu.

Ans)

16) Look in your trace to find messages between the client and a CA to get the CA's public key information, so that the client can verify that the CA-signed certificate sent by the server is indeed valid and has not been forged or altered. Do you see such message in your trace? If so, what is the number in the trace of the first packet sent from your client to the CA? If not, explain why the client did not contact the CA.

Ans)

17) What is the packet number in your trace for the TLS message part that contains the Server Hello Done TLS record? **Ans)**

Name – Aman Singh
Enrollment no. –0801IT221018

974	5.764296	179.60.192.36	192.168.1.245	TLSv1.3	1446	Server Hello, Change Cipher Spec, Application Data
1022	6.025403	179.60.192.36	192.168.1.245	QUIC	1274	Initial, DCID=e5b12a, SCID=7313c33e9879955c, PKN: 132

18) What is the packet number in your trace for the TLS message that contains the public key information, Change Cipher Spec, and Encrypted Handshake message, being sent from client to server?

Ans)

39	3.185548	192.168.1.245	128.119.240.84	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted
565	4.810423	192.168.1.245	18.189.133.49	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted

19) Does the client provide its own CA-signed public key certificate back to the server? If so, what is the packet number in your trace containing your client's certificate?

Ans)

20) What symmetric key cryptography algorithm is being used by the client and server to encrypt application data (in this case, HTTP messages)?

Ans)

```
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Compression Method: null (0)
```

21) In which of the TLS messages is this symmetric key cryptography algorithm finally decided and declared? **Ans)**

32	3.172673	128.119.240.84	192.168.1.245	TLSv1.2	1514	Server Hello
80	3.504910	104.18.11.207	192.168.1.245	QUIC	1242	Initial, DCID=80b1a5,
103	3.523655	52.222.149.109	192.168.1.245	TLSv1.3	1494	Server Hello, Change C

22) What is the packet number in your trace for the first encrypted message carrying application data from client to server?

Ans)

7	1.536919	34.226.161.166	192.168.1.245	TLSv1.2	599	Application Data
41	3.267670	192.168.1.245	128.119.240.84	TLSv1.2	970	Application Data
42	3.355274	128.119.240.84	192.168.1.245	TLSv1.2	1514	Application Data, Ap

23) What do you think the content of this encrypted application-data is, given that this trace was generated by fetching the homepage of www.cics.umass.edu?

Ans) It is likely to contain the content of homepage of www.cics.umass.edu and also some additional resources likes images, javascript code etc.

24) What packet number contains the client-to-server TLS message that shuts down the TLS connection? Because TLS messages are encrypted in our

358	4.428470	192.168.1.245	128.119.240.84	TLSv1.2	97
403	4.506718	128.119.240.84	192.168.1.245	TLSv1.2	97