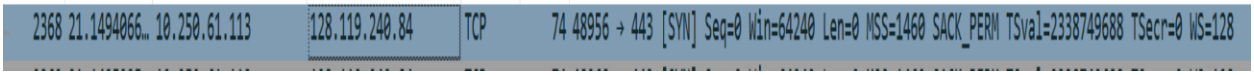
CS-315 COMPUTER NETWORKS LAB-13 (TLS)

Part-2

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

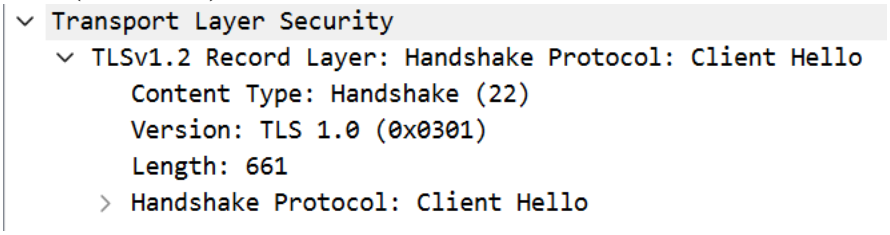


2. The TCP connection is set up before the first TLS message is sent from the client to the server.

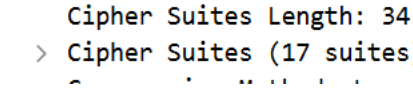
Part-3

1. The packet number in your trace that contains the TLS Client Hello message is 2377.

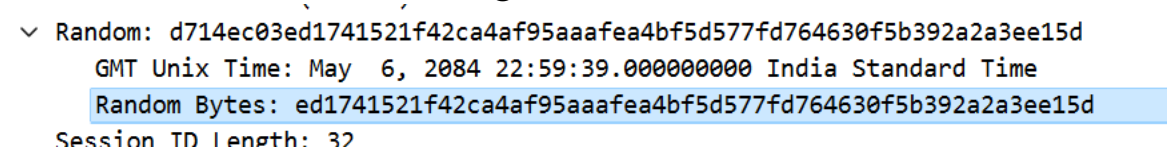
2. The version of TLS as declared in the Client Hello message is TLS 1.0 (0x0301) of TLSv1.2.



3. 17 Cipher suites are supported by your client, as declared in the Client Hello message.



4. The first two hexadecimal digits: ed.

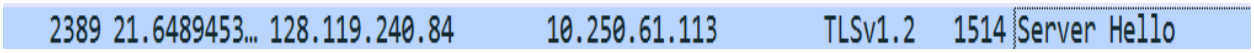


5. The random bytes in the Client Hello message play a crucial role in establishing a secure TLS connection by providing randomness, aiding in version negotiation, facilitating session resumption, and

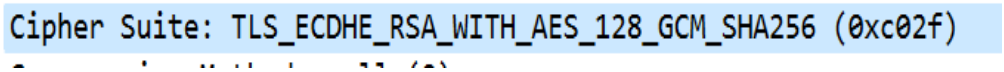
contributing to the generation of key material. It serves several important functions within the TLS handshake. It ensures cryptographic parameters are generated with sufficient randomness, guards against replay attacks, enhances the entropy of session keys, and assists in uniquely identifying connections during the handshake phase.

Part-4

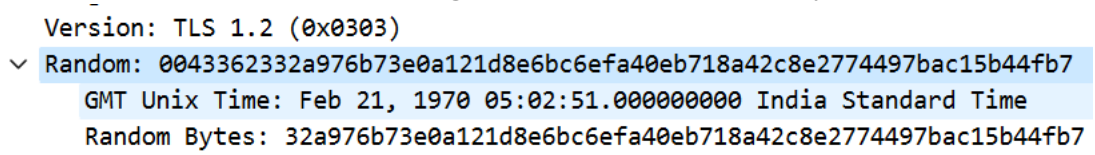
1. The packet number in your trace that contains the TLS Server Hello message is 2389.



2. The cipher suite that has been chosen by the server is TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(0xc02f).



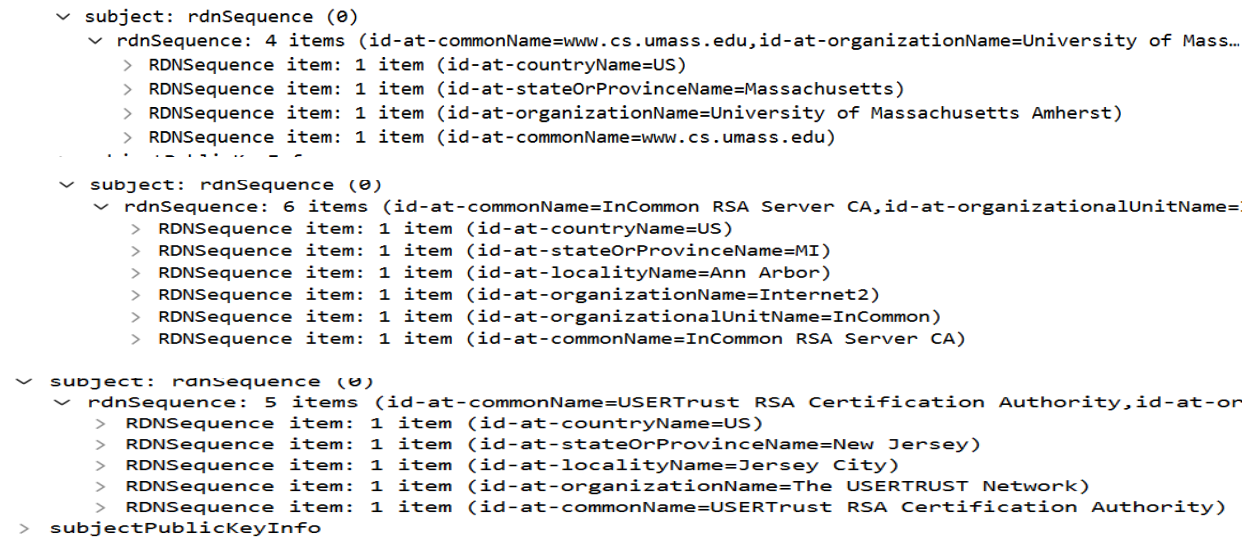
3. Yes, the Server Hello message contains random bytes, similar to how the Client Hello message contains random bytes.



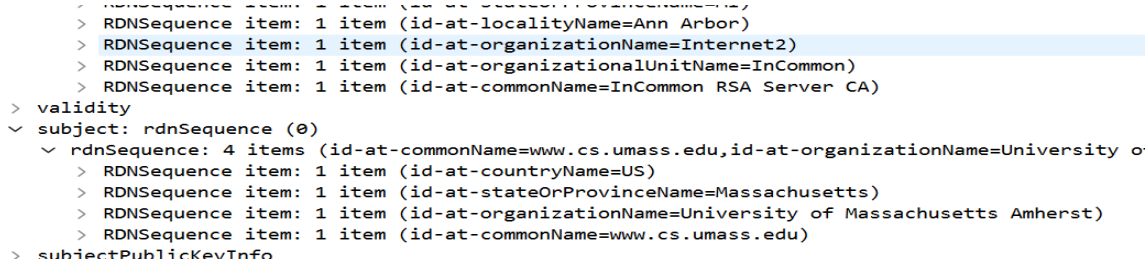
The random bytes in the Client Hello message play a crucial role in establishing a secure TLS connection by providing randomness, aiding in version negotiation, facilitating session resumption, and contributing to the generation of key material. It serves several important functions within the TLS handshake. It ensures cryptographic parameters are generated with sufficient randomness, guards against replay attacks, enhances the entropy of session keys, and assists in uniquely identifying connections during the handshake phase.

4. 2393 is the packet number in the trace for the TLS message part that contains the public key certificate for the www.cics.umass.edu server.

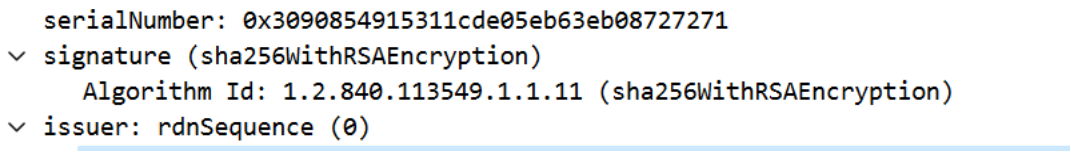
5. The server returns 3 certificates. No, not all certificates are for www.cs.umass.edu. The other two certificates are for InCommon RSA Server CA and USERTrust RSA Certification Authority.



6. The name of the certification authority that issued the certificate for id-at-commonName=www.cs.umass.edu is InCommon RSA Server CA.



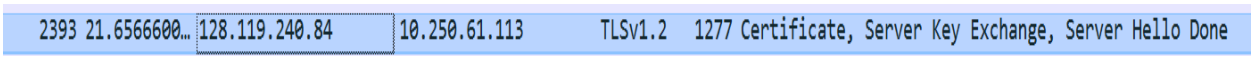
7. The signature algorithm used is sha256WithRSAEncryption with Algorithm Id: 1.2.840.113549.1.1.11.



8. The first four hexadecimal digits of the modulus of the public key being used by www.cics.umass.edu is 00b3.

```
      > RDNSequence item: 1 item (id-at-commonName=www.cs.umass.edu)
  v subjectPublicKeyInfo
    > algorithm (rsaEncryption)
    v subjectPublicKey [truncated]: 3082010a0282010100b39e7296158da80176a2f1035c7c61f06120f9852a
        modulus: 0x00b39e7296158da80176a2f1035c7c61f06120f9852aad0d20d4931a30842fecec1b8724…
        publicExponent: 65537
```

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



Part-5

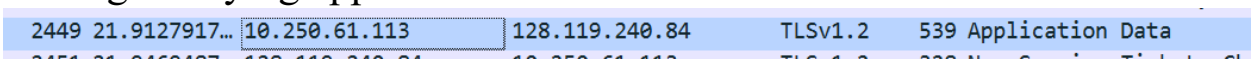
1. 2395 is the packet number in your trace for the TLS message that contains the public key information, Change Cipher Spec, and Encrypted Handshake message, being sent from client to server.
2. No, the client does not provide its own CA-signed public key certificate back to the server.

Part-6

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

```
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
```

2. This symmetric key cryptography algorithm is finally decided and declared in the Client Hello and Server Hello messages in the Cipher Suite Step of TLS handshake.
3. 2449 is the packet number in your trace for the first encrypted message carrying application data from client to server.



4. The content of this encrypted application data is content based on the homepage and it is encrypted as this trace was collected while fetching the homepage of www.cics.umass.edu.
5. Packet number 6545 contains the client-to-server TLS message that shuts down the TLS connection.