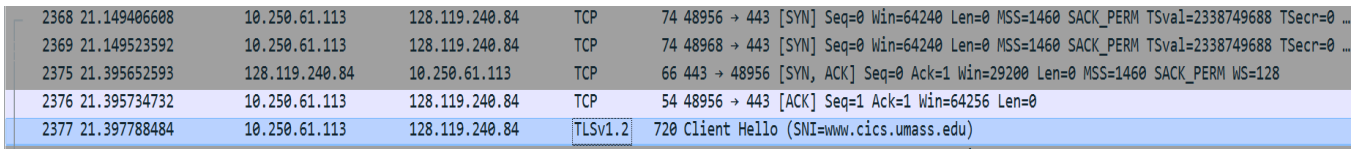
Assignment 13

Part-2

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



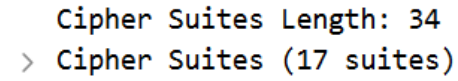
2. After a TCP connection has been established through a TCP handshake, The TLS handshake takes place.

Part-3

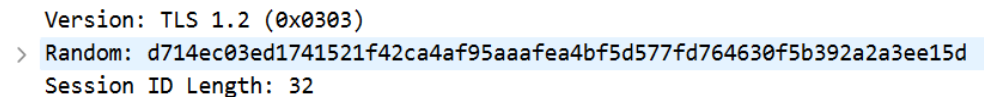
1. The packet number in trace that contains the TLS Client Hello Message is: **2377**

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.

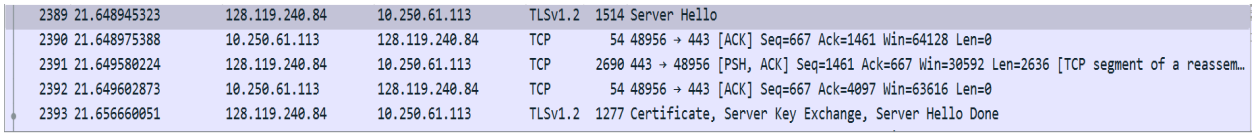


4. The first two hexadecimal digits in the random bytes field of the Client Hello message are: **d7**



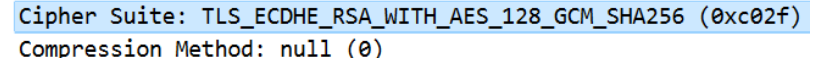
5. The premaster secret is created using the random bytes. That is, a shared secret key known as the pre master key is created by combining the random bytes with additional information sent during the TLS handshake.

Part-4



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)



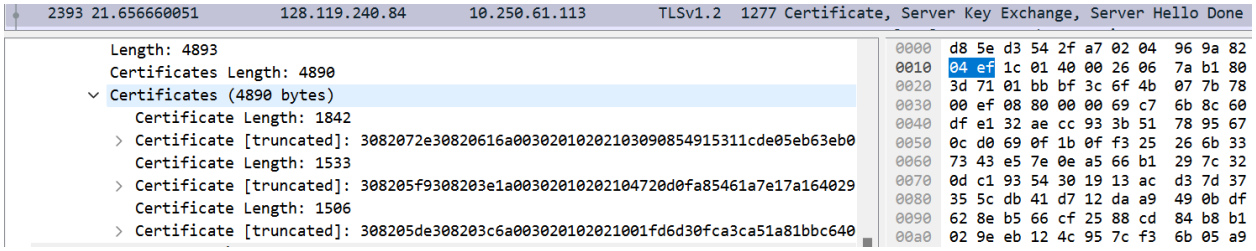
3. Yes, the server Hello message contains random bytes, similar to how the Client Hello message contained random bytes. The purpose of the random bytes is to provide assurance that the person you want to connect with is genuinely present and participating in the conversation, rather than just playing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

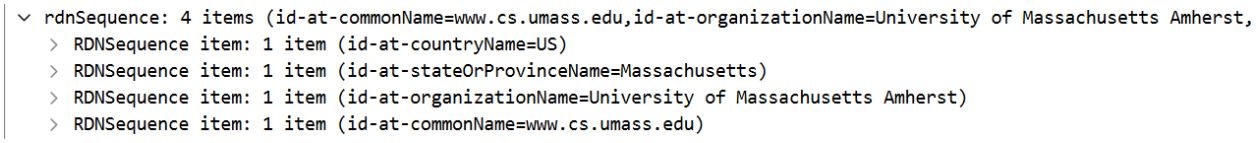
5. The server return **3 certificates**, These are not all for www.cs.umass.edu

The certificates are for:

- InCommon RSA Server CA
- USERTrust RSA Certification Authority

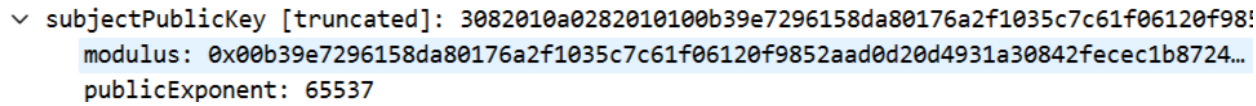


6. The name of the certification authority that issued the certificate for id-at-commonName=www.cs.umass.edu is **University of Massachusetts Amherst**



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

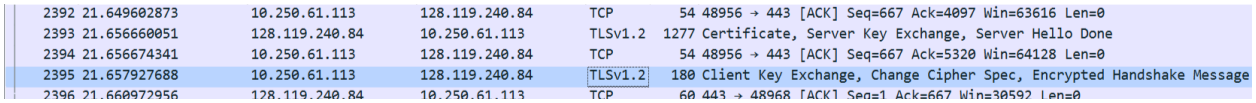
8. The first 4 hexadecimal digits of the modulus of the public key being used by www.cics.umass.edu are: **00b3**



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**



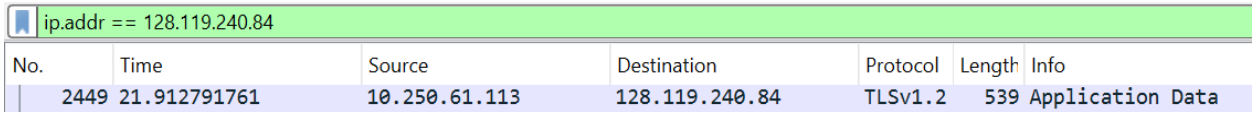
2. No. the client doesn't provide its own CA-signed public key certificate back to the server.

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.



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**