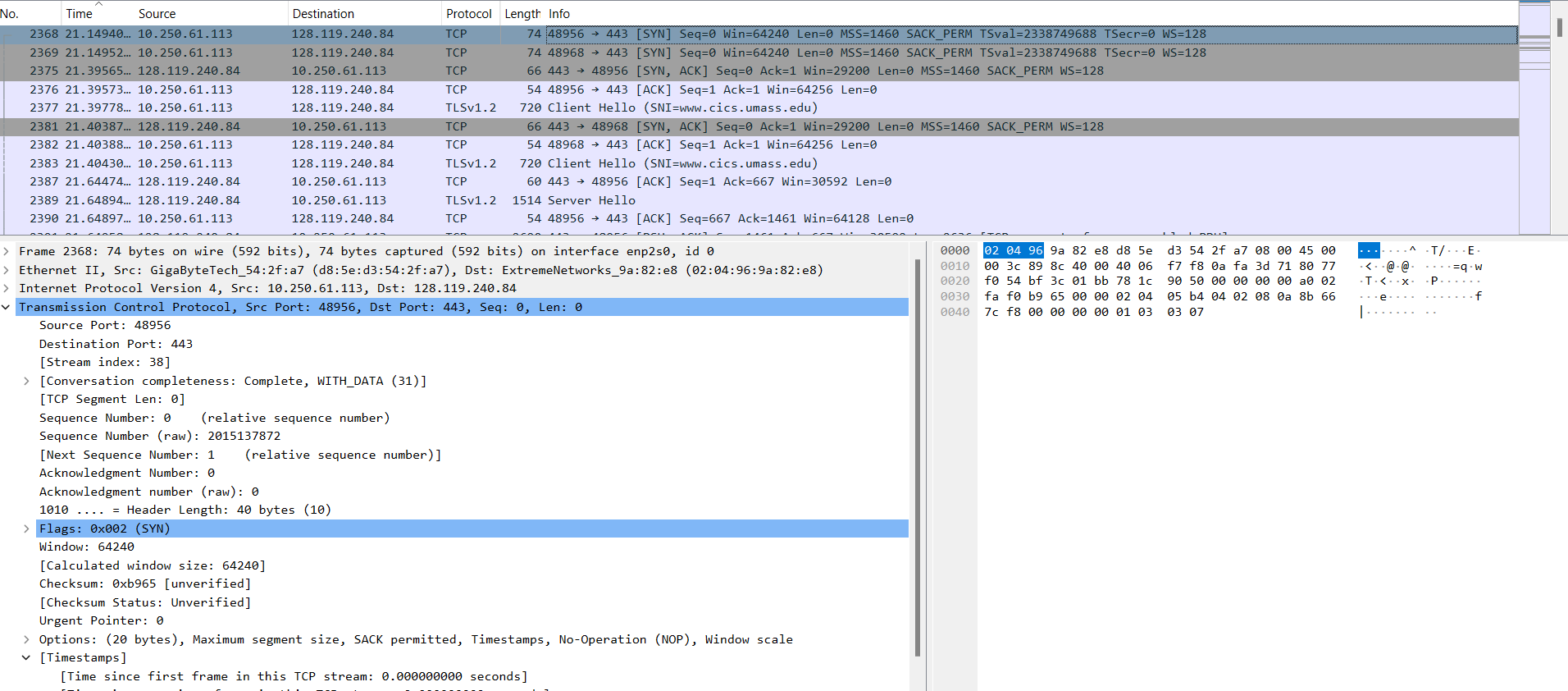
Assignment 13: TLS Protocol

210010020

Part2: A first look at the captured trace

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).

A] Packet Number 2368

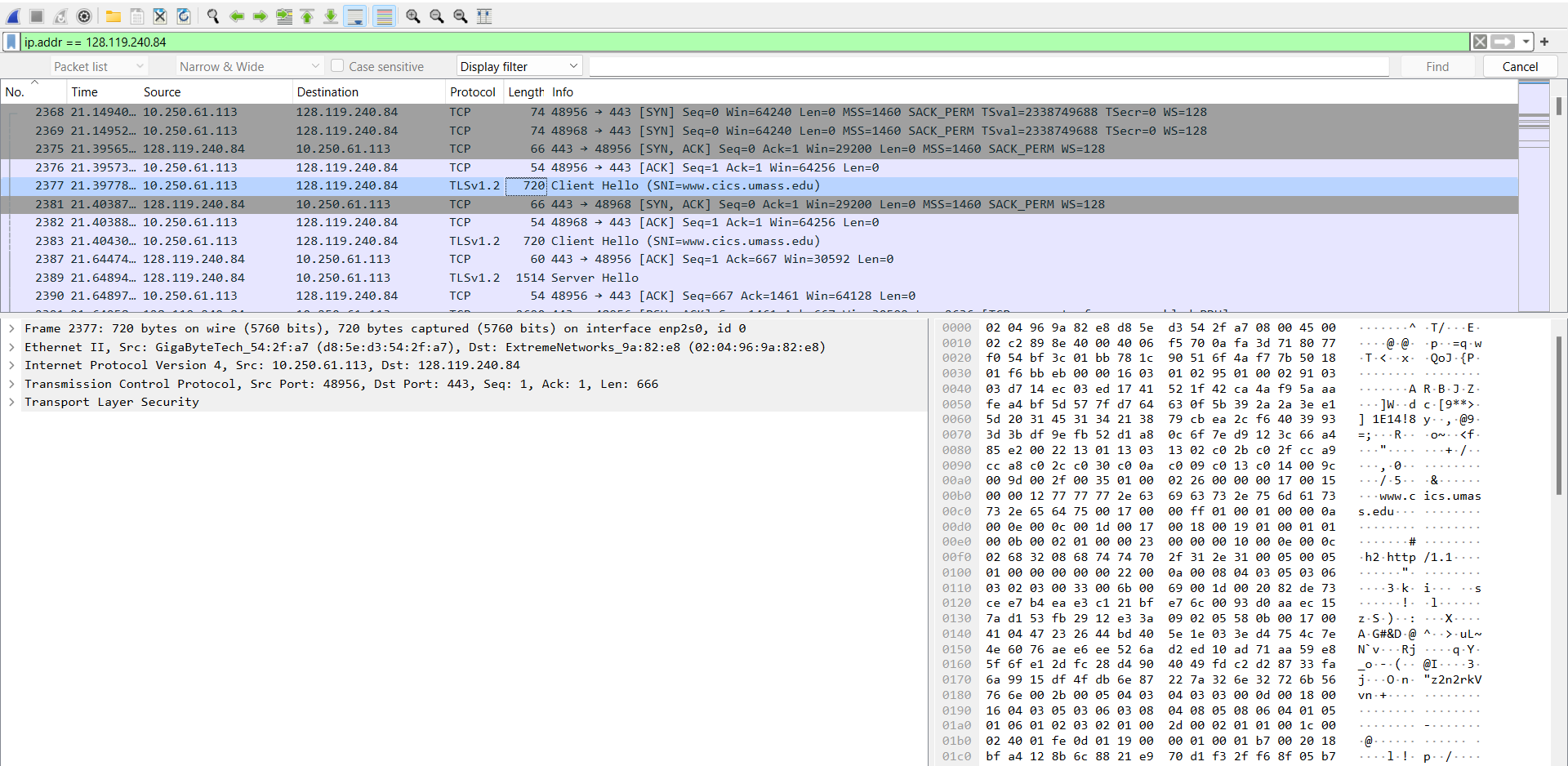


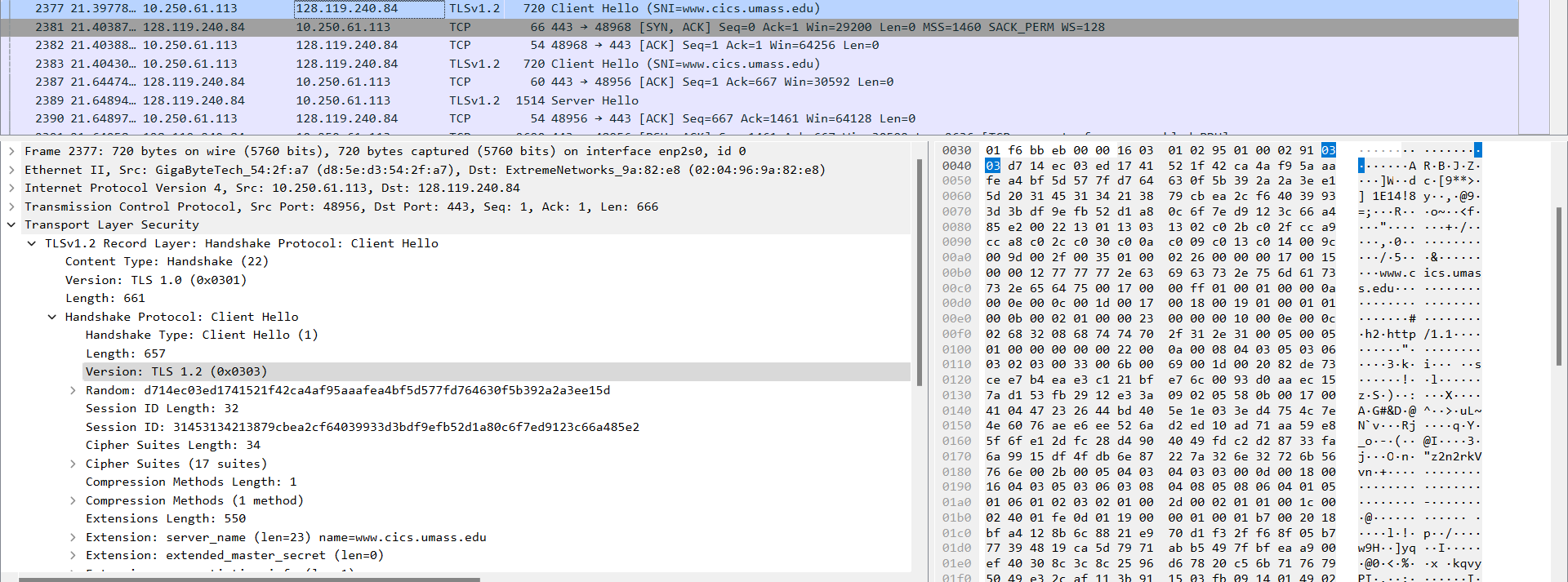
1. Is the TCP connection set up before or after the first TLS message is sent from the client to the server?

A] first TLS message is sent after the TCP connection is set up between the client and the server.

Part-3: The TLS Handshake: Client Hello message

1. What is the packet number in your trace that contains the TLS Client Hello message?

A] packet 2377.  


2. What version of TLS is your client running, as declared in the Client Hello message?  
A] TLS version 0x0301.  
 Inside the handshake field version is 0x0303. This can be seen in the below screenshot.  
 

3. 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 hoid-at-commonName=www.cs.umass.edua HMAC algorithm.

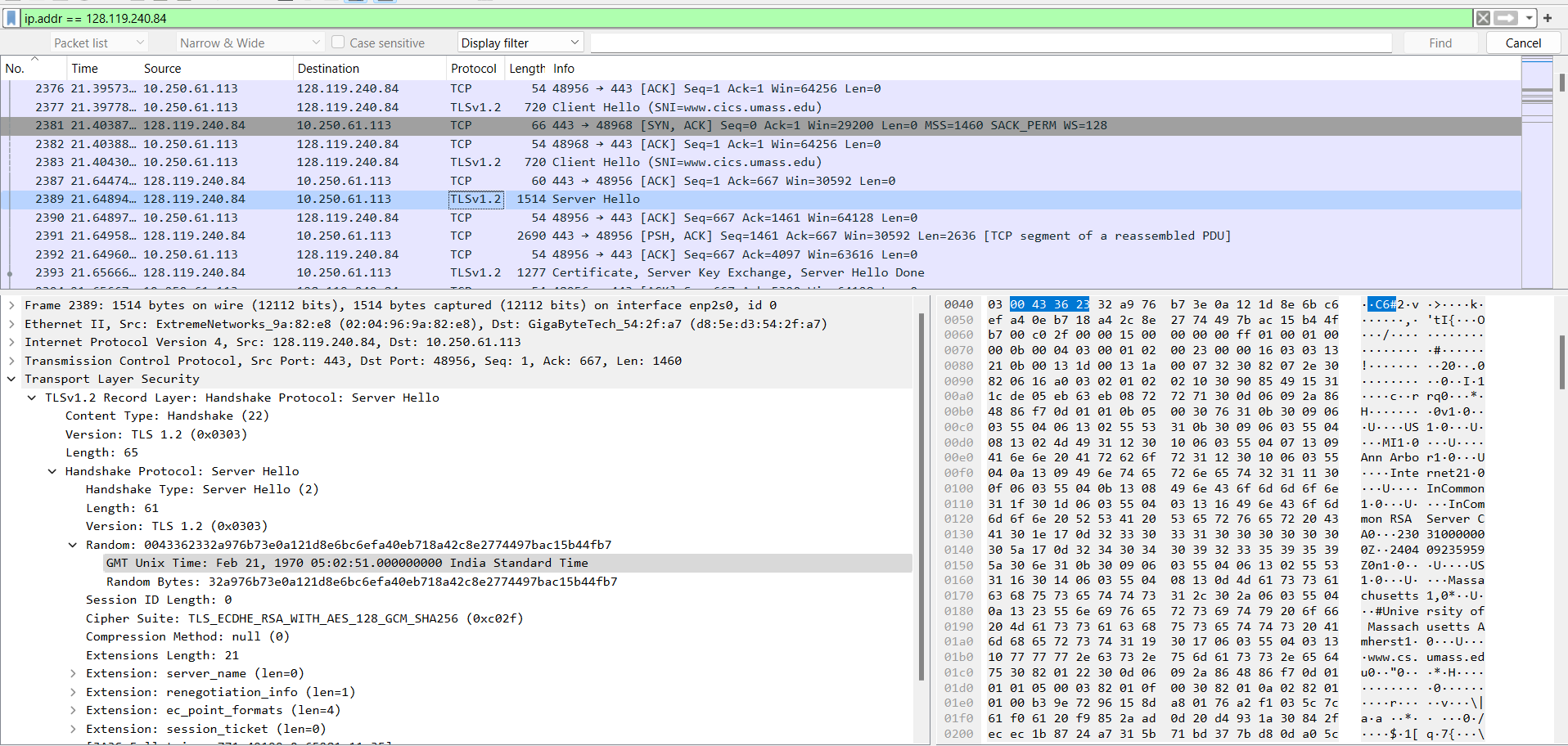
A] As seen in the above figure total of 17 cipher suites can be generated.

4. 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).  
A] The first two digits are the timestamp values **d7**

5. What is the purpose(s) of the “random bytes” field in the Client Hello message? Note: you’ll have to 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).  
A] Helps to distinguish HELLO messages sent between two different clients, to the server. Thus making it unique. The purpose of the client random is to:

* Ensure that each handshake is unique by including a random value.
* Contribute to the generation of session keys for symmetric encryption after the handshake is complete.

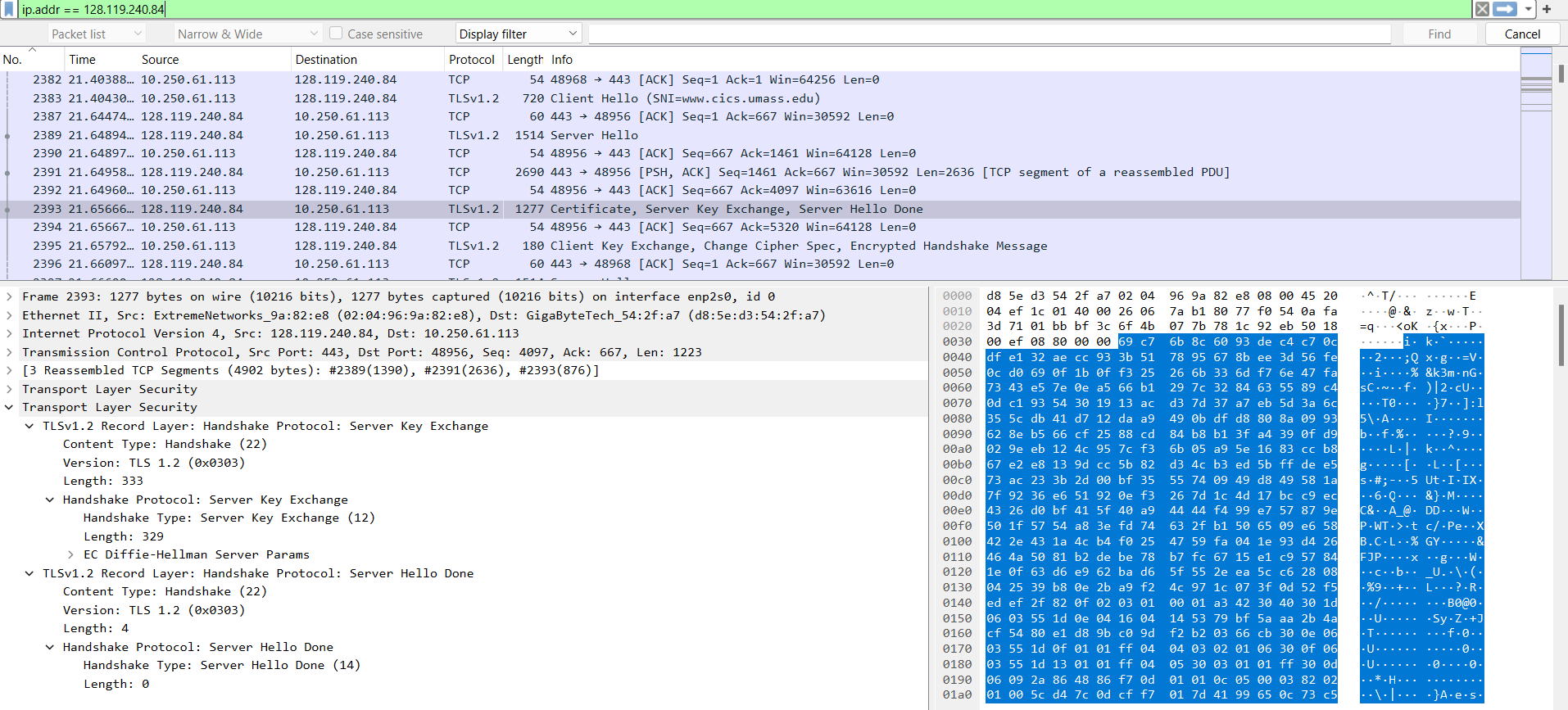
Part-4: The TLS Handshake: Server Hello message

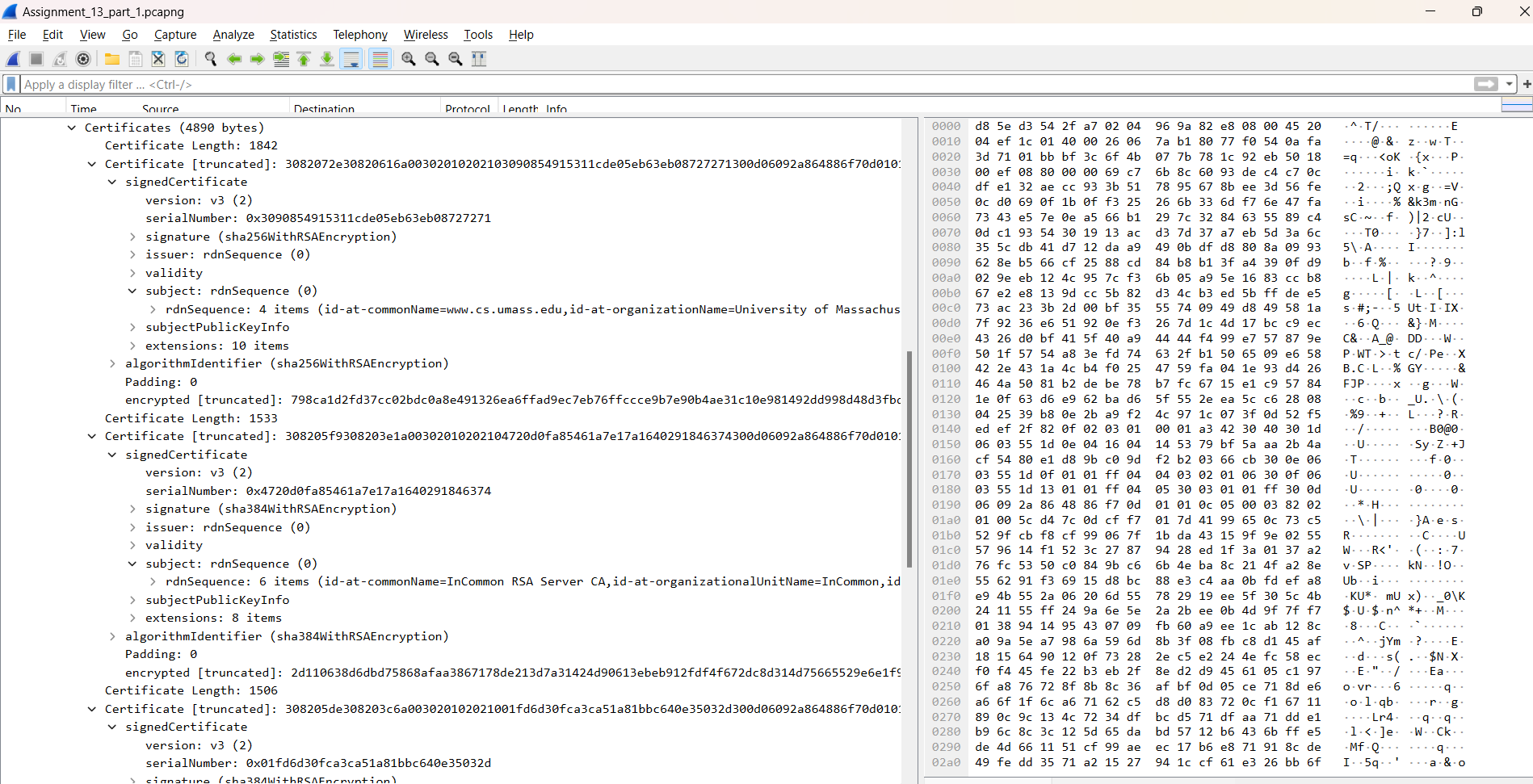
1. What is the packet number in your trace that contains the TLS Server Hello message?   
A] Packet No. 2389  


2. Which cipher suite has been chosen by the server from among those offered in the earlier Client Hello message?  
A] From the available cipher suites the server has chosen   
*Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)*

3. Does the Server Hello message contain random bytes, similar to how the Client Hello message contains random bytes? And if so, what is/are their purpose(s)?  
A] Yes, similar to client the server also contains random bytes. The server random serves the following purposes:

* Distinguishes different handshakes, preventing replay attacks.
* Contributes to session key generation for symmetric encryption.

4. 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)?  
A] 

5. 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-common Name field in the returned certificate.   
A] Total 3 certificates are returned in Packet 2393  
 Not all of them are for cs.umass.edu but for higher authorities that are manage authenticate certification for digital signatures.

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

7. What digital signature algorithm is used by the CA to sign this certificate? Hint: this information can be found in the signature subfield of the SignedCertificate field of the certificate for www.cs.umass.edu.  
A] signature algorithm used by CA authority has used sha256WithRSAEncryption.

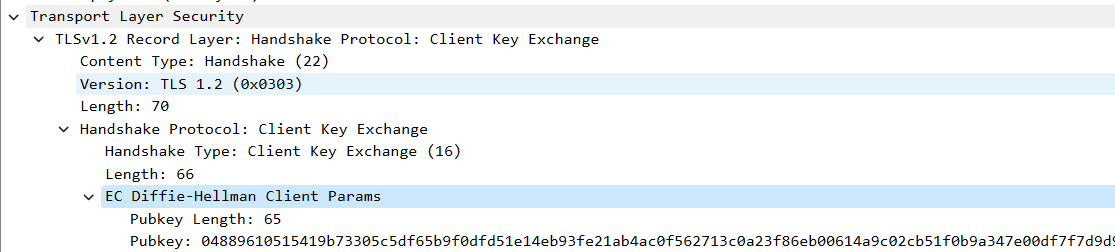
8. Let's take a look at what a real public key looks like! What are the first four hexadecimal digits of the modulus of the public key being used by www.cics.umass.edu? Enter the four hexadecimal digits (without spaces between the hex digits and without any leading '0x' , using lowercase letters where 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.   
A] 00b3

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

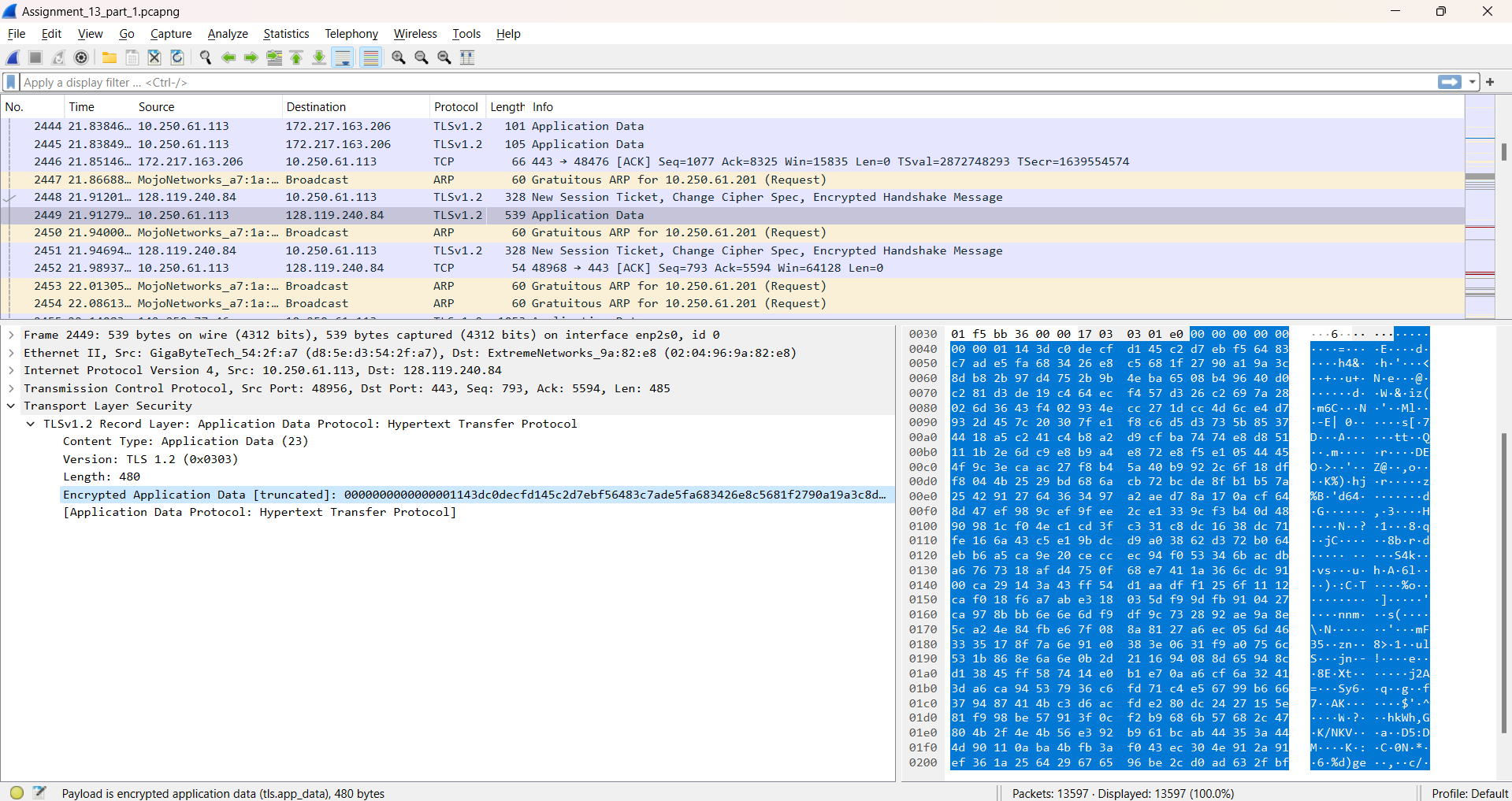
Part-5: The TLS Handshake: wrapping up the handshake

1. 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?   
A] Packet 2395   
  
2. 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?  
A] No

Part-6: Application data

1. What symmetric key cryptography algorithm is being used by the client and server to encrypt application data (in this case, HTTP messages)?   
   A] EF Diffie-Hellman as shown below  
   
2. In which of the TLS messages is this symmetric key cryptography algorithm finally decided and declared?

A] In server hello done packet, packet 2393.

1. What is the packet number in your trace for the first encrypted message carrying application data from client to server?  
   A] packet 2449.
2. 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?  
   A] HTTP GET request is encrypted below  
   
3. Packet number 6545 contains the client-to-server TLS message that shuts down the TLS connection