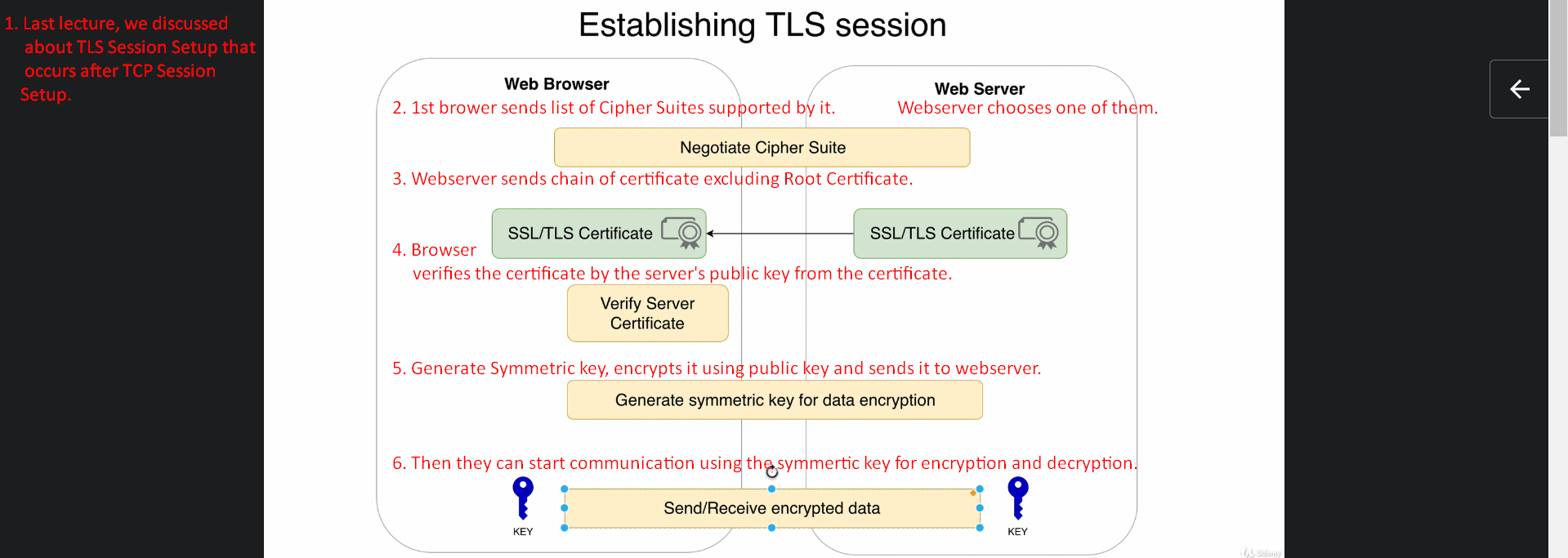
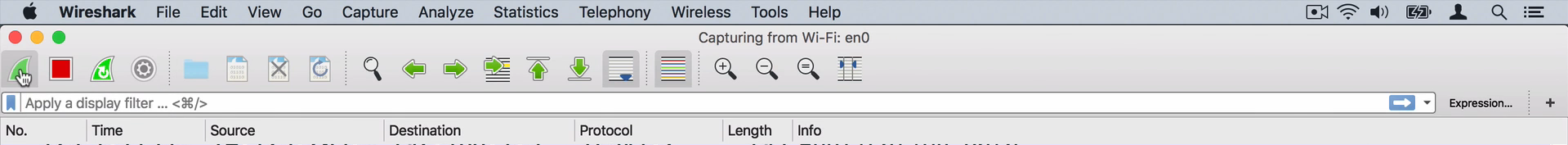
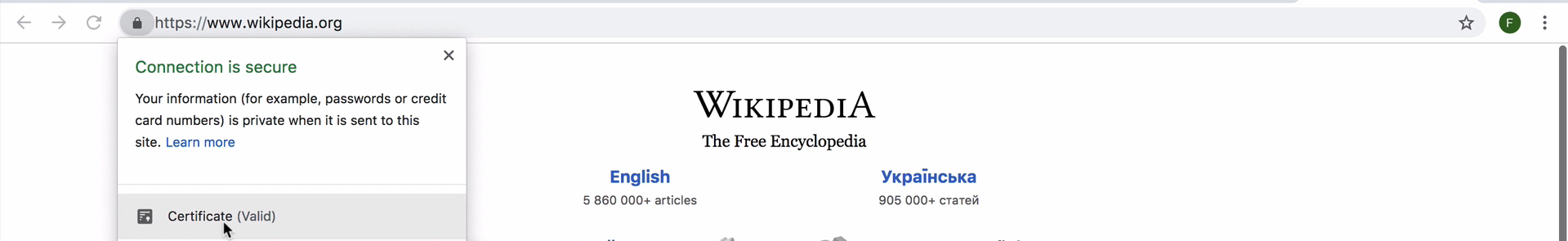
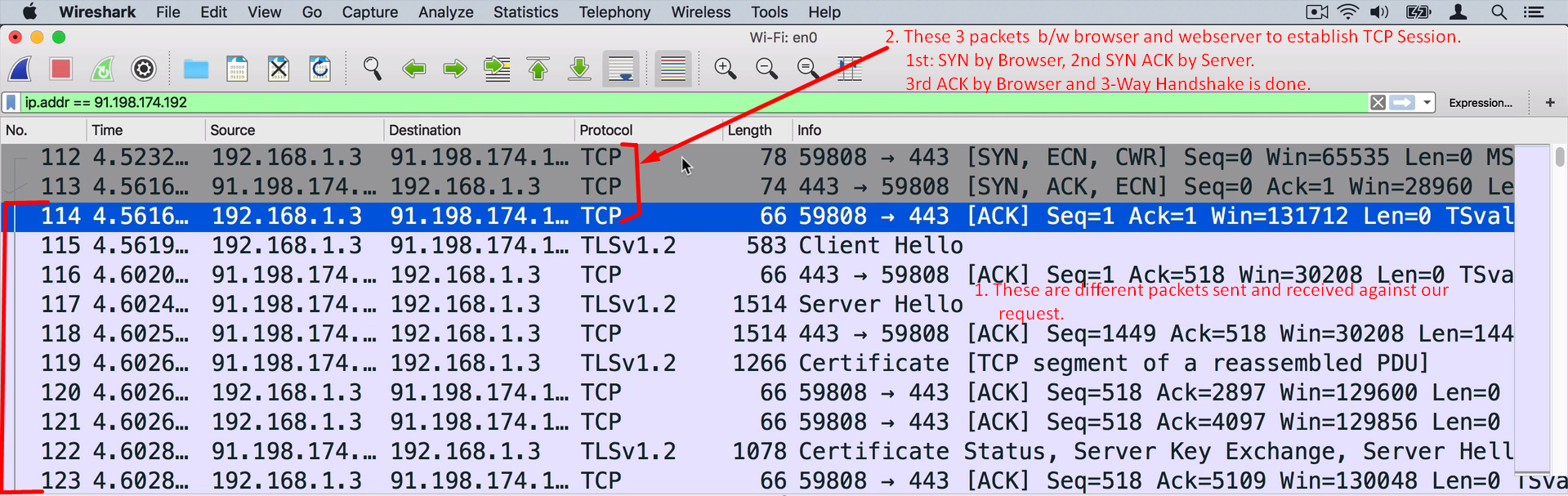
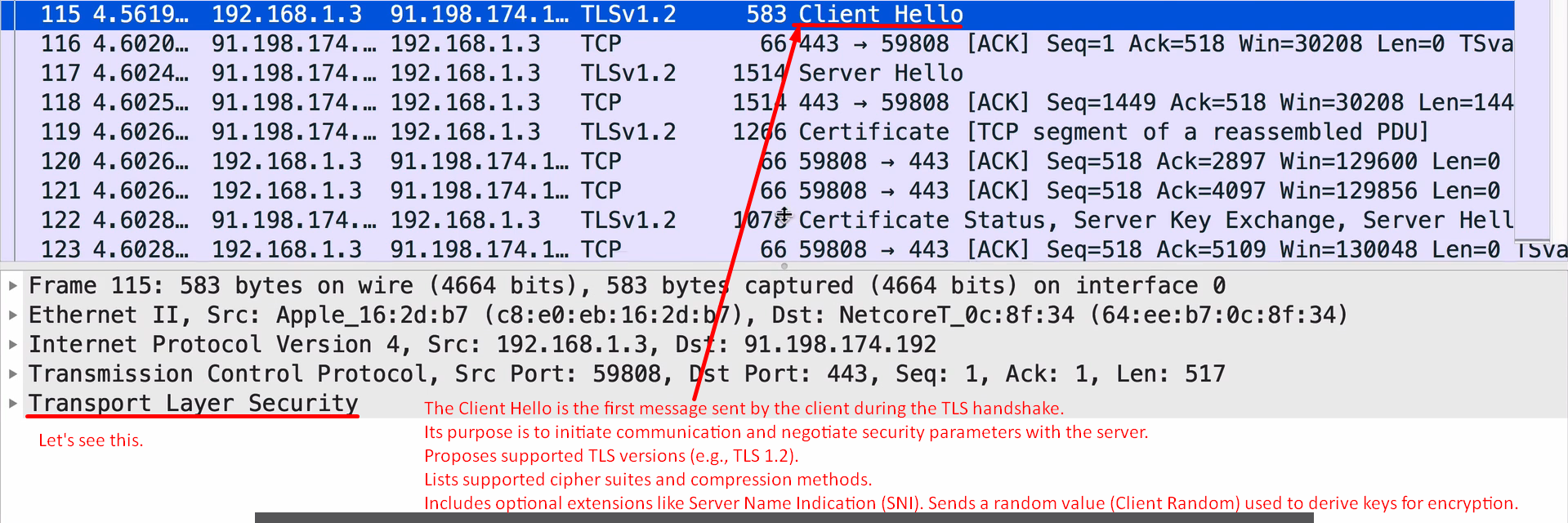
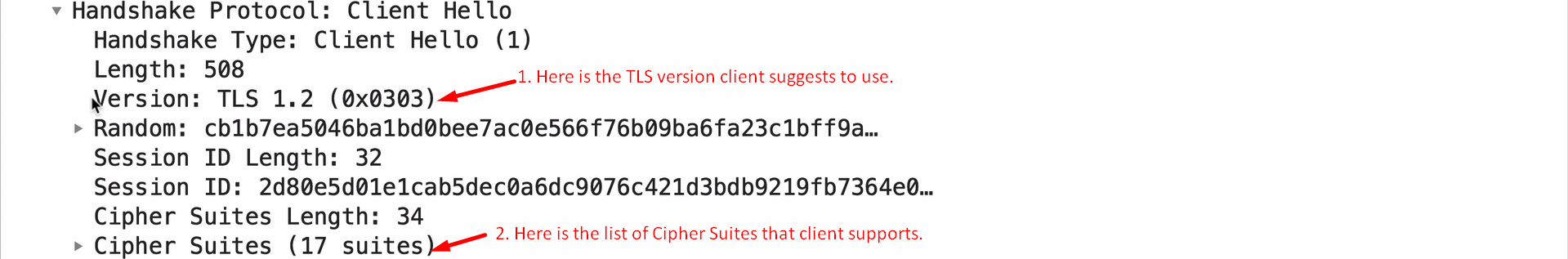
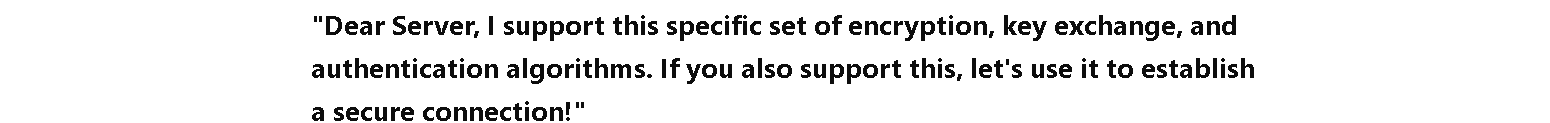
1.   
   Above for Point#4, the browser also checks domain name in the certificate to match with that requested by browser as fake certificate may be served by a man in the middle.
2. Let’s analyse how TLS Session is set up through Wireshark.
3. 
4. 
5. 
6. 
7. 
8. 
9. 
   1. A browser sends a list of Cipher Suite to Server during TLS Handshake to suggest server to use one of them.
   2. That suggested list to server means to say:  
      
   3. TLS\_
      1. TLS: The protocol used for secure communication.
      2. ECDHE (Elliptic Curve Diffie-Hellman Ephemeral) –

Key Exchange Algorithm.

Allows the browser and server to securely **generate** a shared session key.

Ephemeral means the key is temporary and generated for this session only, ensuring forward secrecy.

* + 1. ECDSA (Elliptic Curve Digital Signature Algorithm) –

Authentication Algorithm.

Used to verify the server’s identity with a digital certificate.

Based on Elliptic Curve Cryptography (ECC), providing strong security with smaller key sizes.

* + 1. AES\_256\_GCM (Advanced Encryption Standard, 256-bit, Galois/Counter Mode) –

Encryption Algorithm.

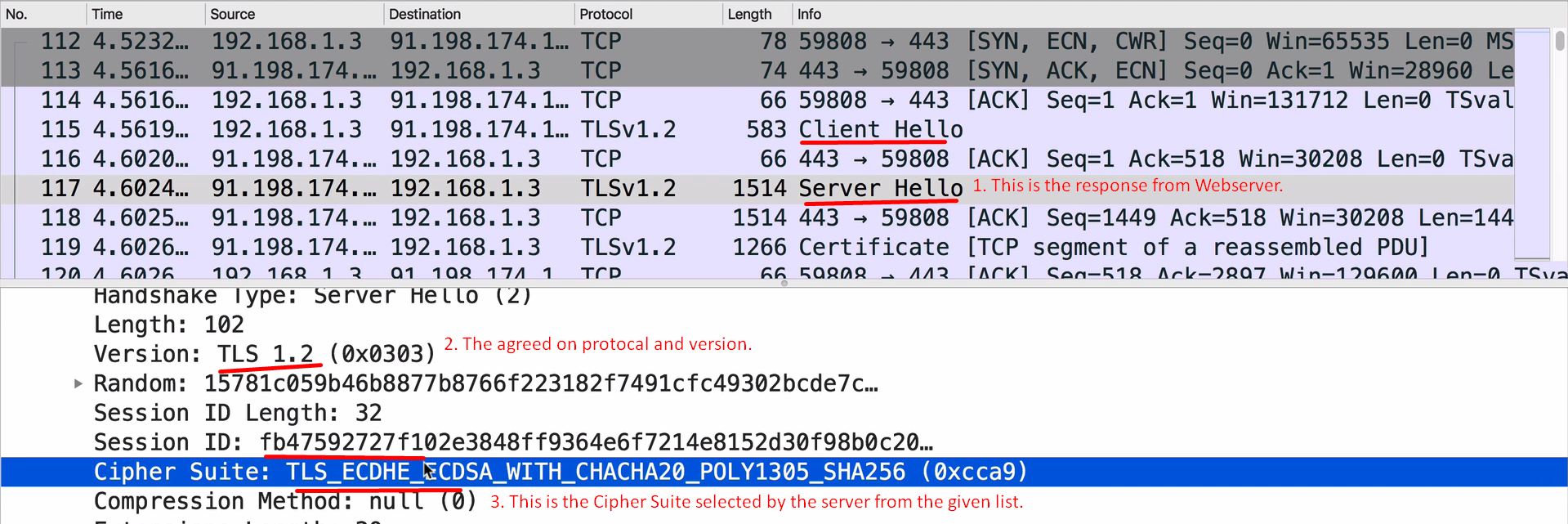
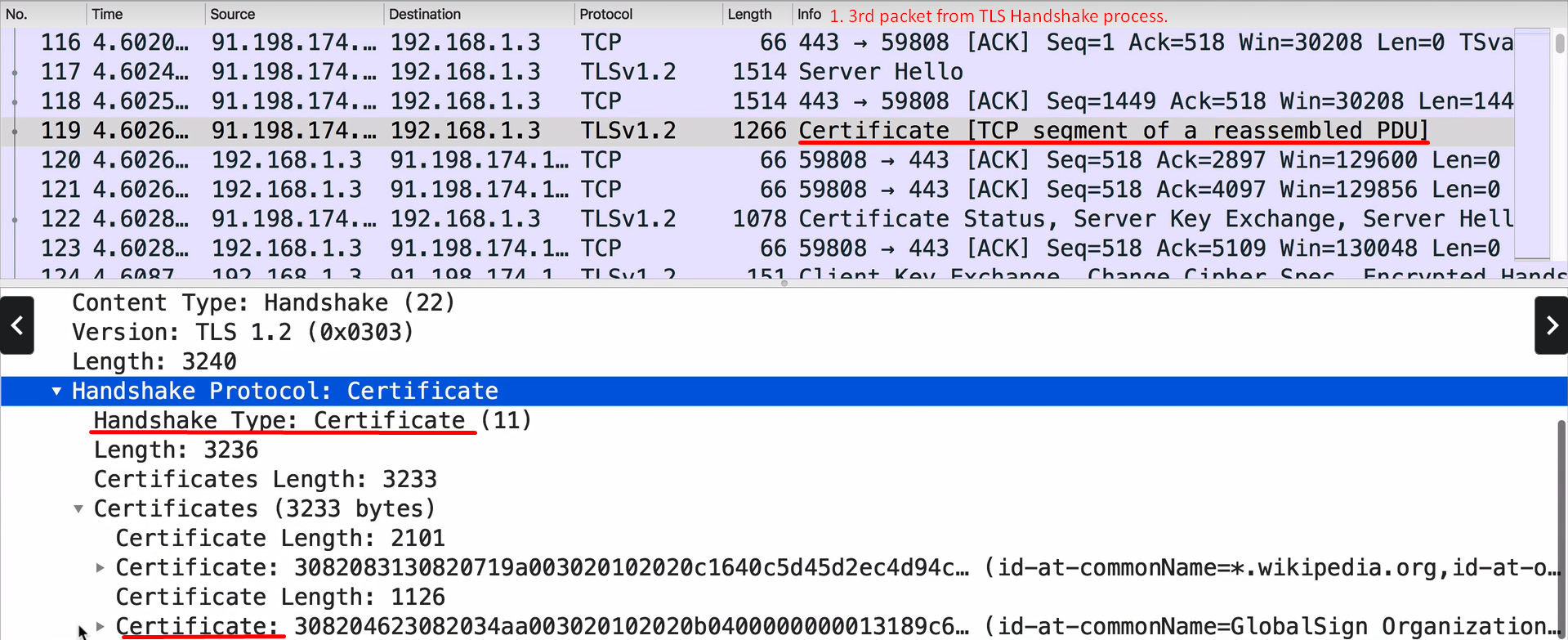
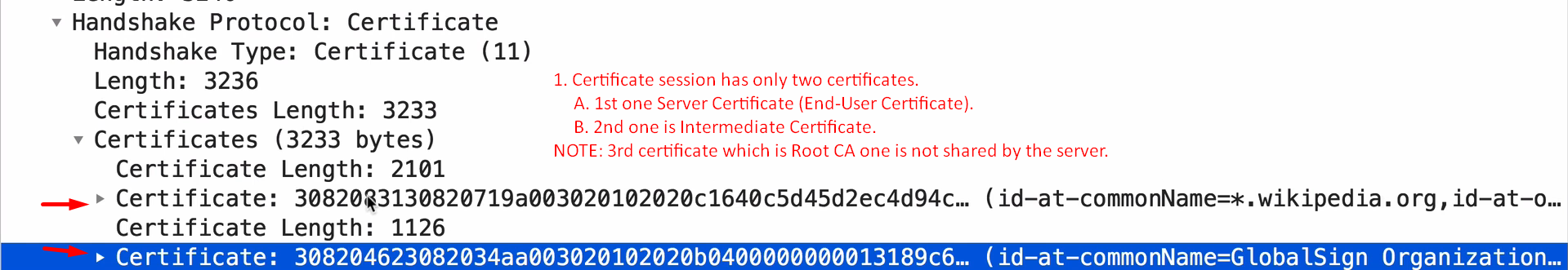
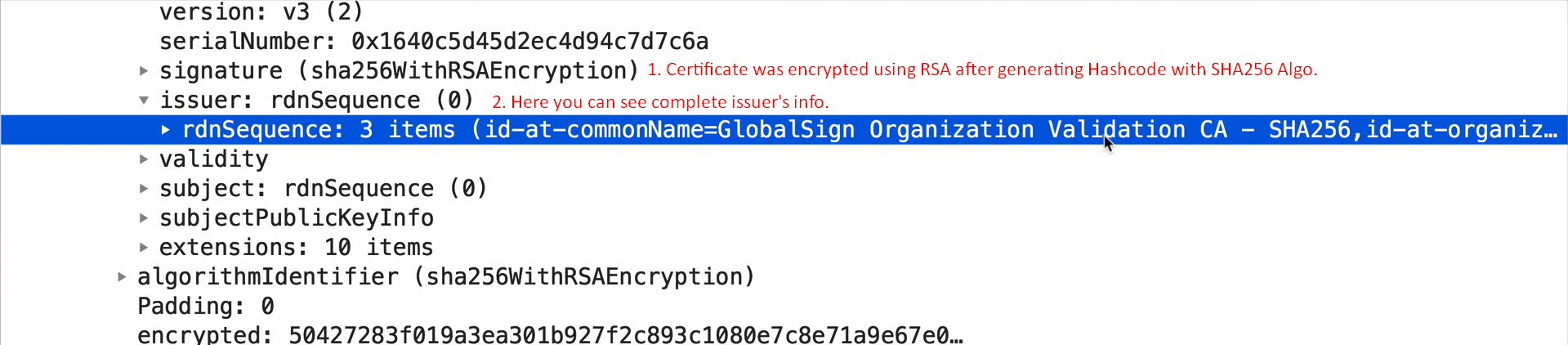
Uses a 256-bit key for strong encryption of data.

GCM (Galois/Counter Mode) adds integrity verification, ensuring data is not tampered with.

* + 1. SHA384 (Secure Hash Algorithm 384-bit) –

Hashing Algorithm for message authentication and integrity checks.

Ensures that the transmitted data is unchanged and authentic.

1. 
2. The following packet comes from server to client computer.   
     
   
3. 
4. Skipped 😊I thought first I need to complete next lectures.