**Cryptography & Network Security Lab**

**SSL/TLS Lab**

**Name:** Vaishnavi Santosh Bhajibhakare **PRN**: 2019BTECS00039

**Aim**: To observe SSL/TLS (Secure Sockets Layer/ Transport Layer Security)in action. SSL/TLS is used to secure TCP connections, and it is widely used as part of the secure web:HTTPS is SSL over HTTP

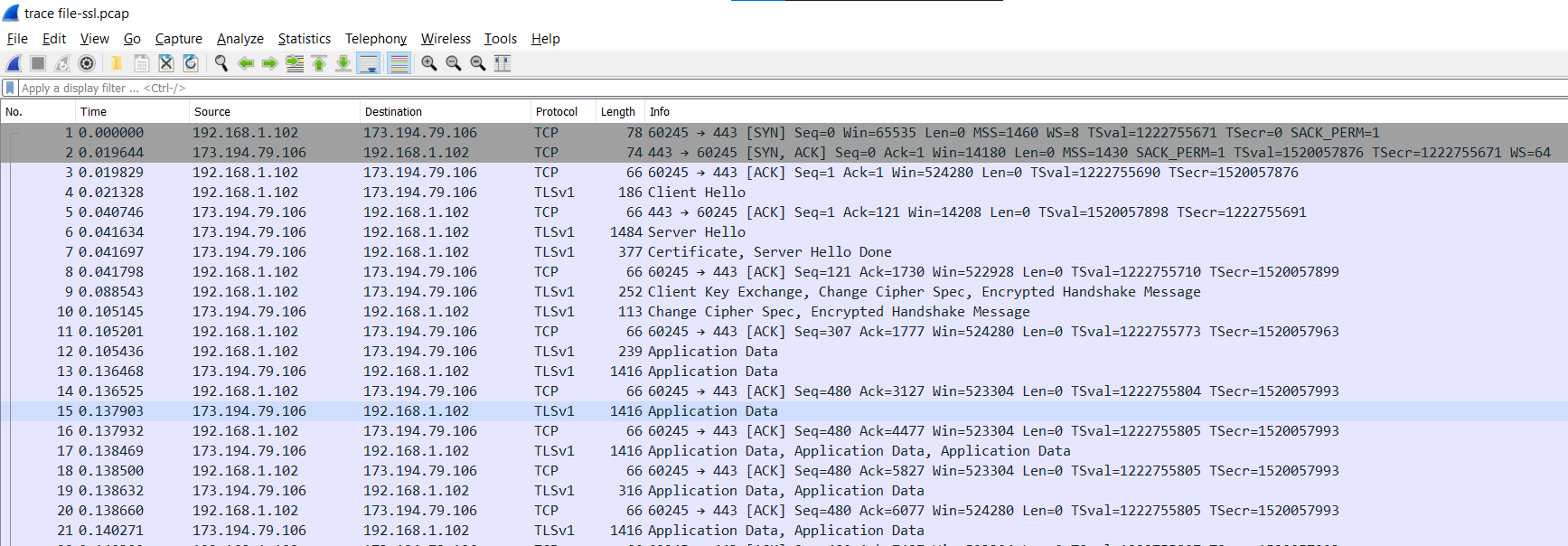
**Theory:** Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

Secure Socket Layer Protocols:

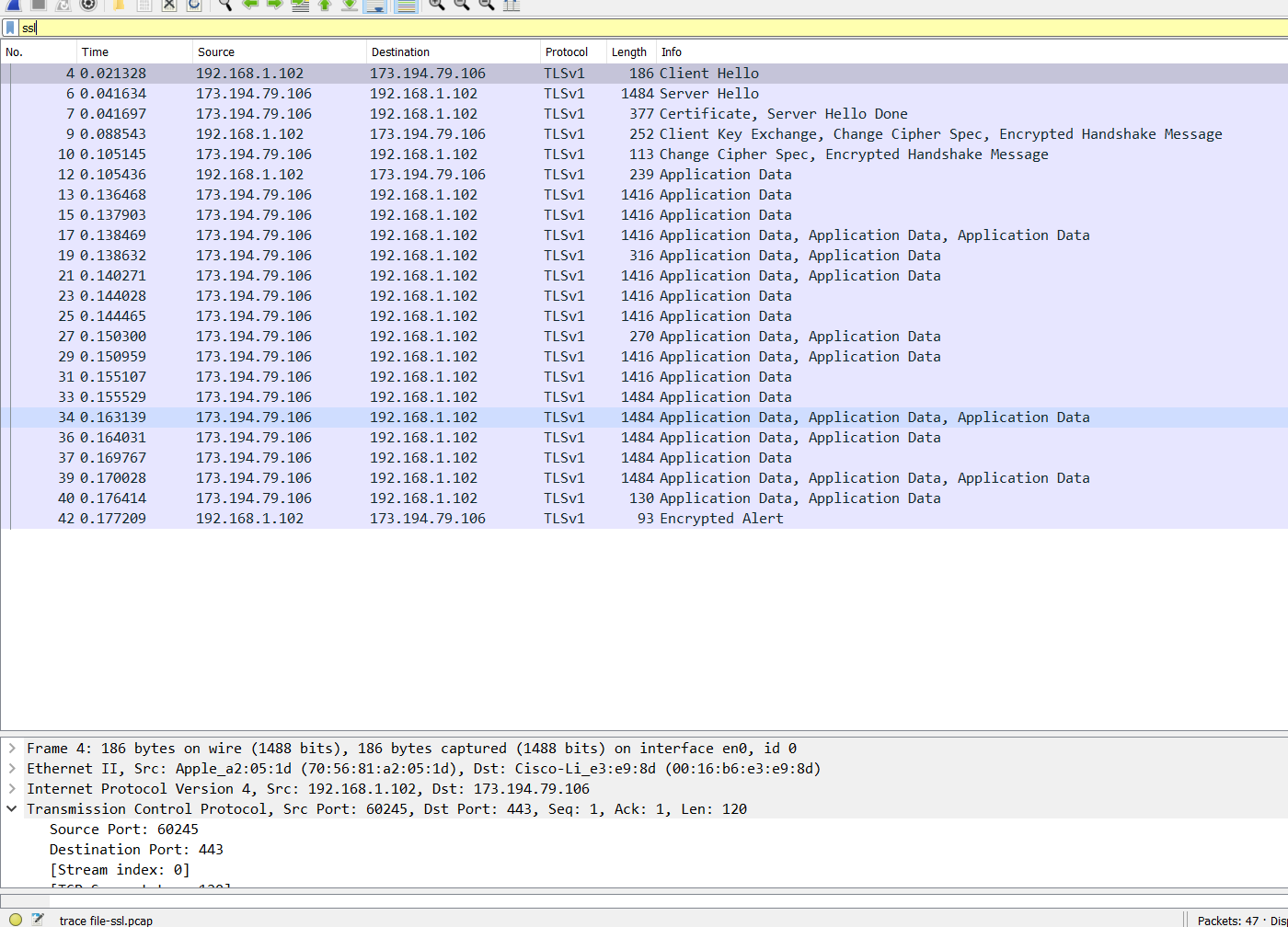
* SSL record protocol
* Handshake protocol
* Change-cipher spec protocol
* Alert protocol

**Procedure:**

**STEP 1:Open a Trace you should use a supplied trace file trace-ssl.pcap.**

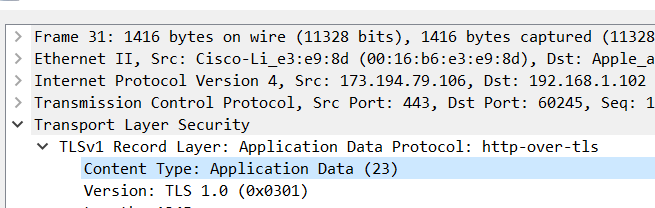


**STEP 2:Inspect the Trace**

****

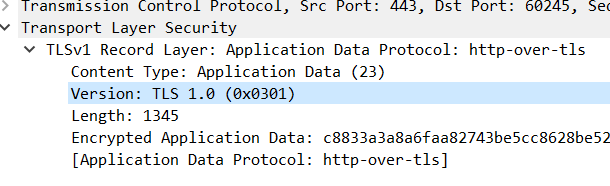
**1. What is the Content Type for a record containing Application Data?**

**>> Content Type**: Application Data (23)



**2. What version constant is used in your trace, and which version of TLS does it represent?**

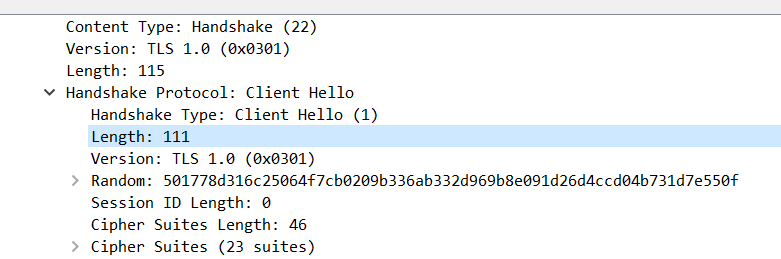
>> **Version: TLS 1.0** (0x0301)



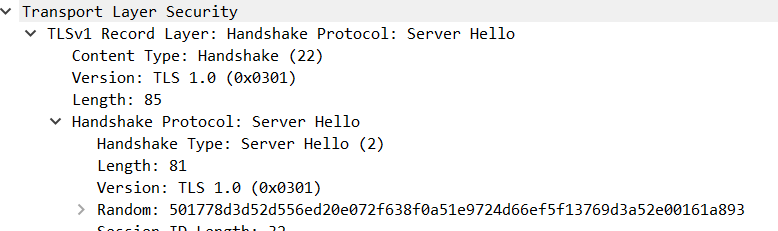
**Step 3: The SSL Handshake**

Hello Message

**1. How long in bytes is the random data in the Hellos? Both the Client and Server include this random data (a nonce) to allow the establishment of session keys.**

>> 

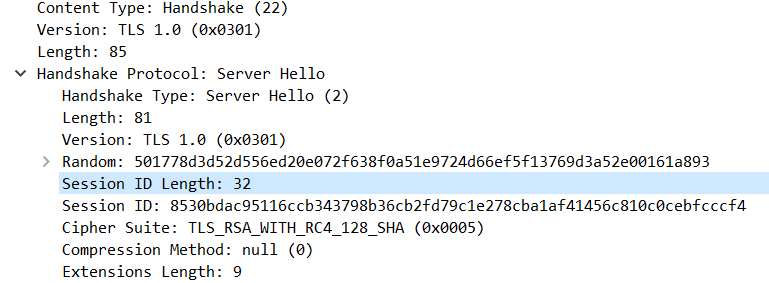
Client Hello Random Data Length in bytes = **111**



Server Hello Random Data Length in bytes = **81**

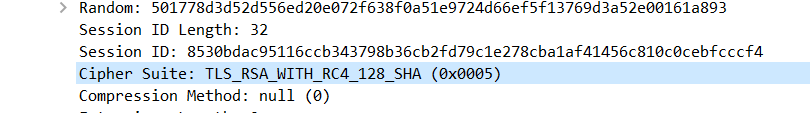
**2. How long in bytes is the session identifier sent by the server?This identifier allows later resumption of the session with an abbreviated handshake when both the client and server indicate the same value. In our case, the client likely sent no session ID as there was nothing to resume.**

ANS:



**Server Session ID:** 8530bdac95116ccb343798b36cb2fd79c1e278cba1af41456c810c0cebfcccf4

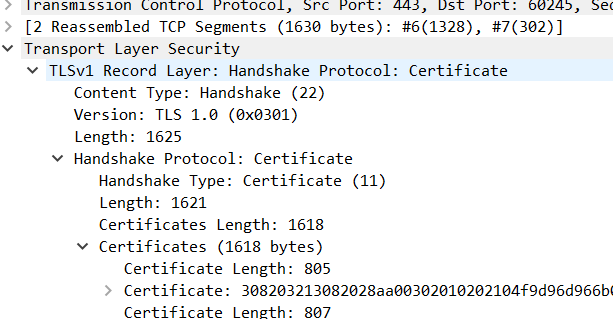
**3. What Cipher suite is chosen by the Server? Give its name and value. The Client will list the different cipher methods it supports, and the Server will pick one of these methods to use.**

****

**Cipher Suite:** TLS\_RSA\_WITH\_RCA\_128\_SHA

Certificate Messages

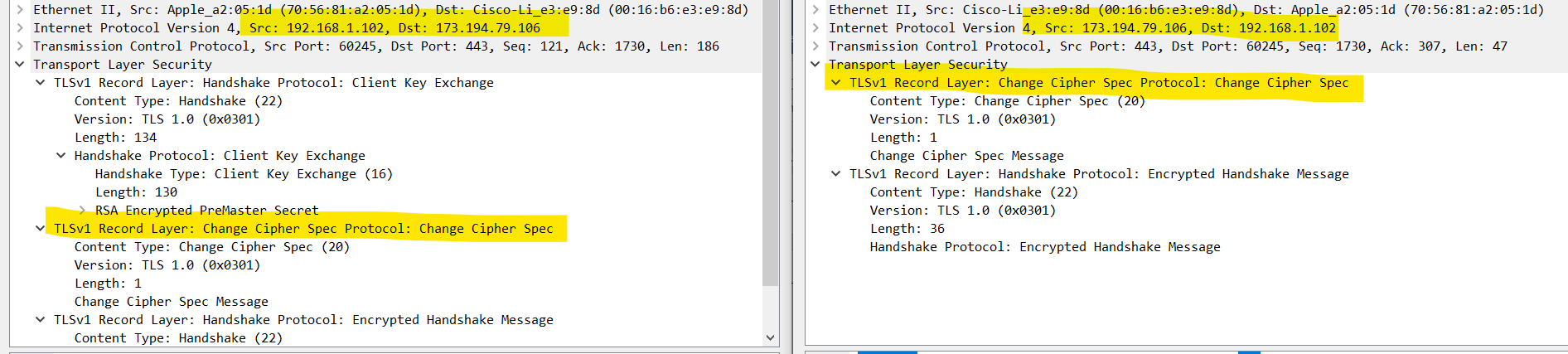
**1. Who sends the Certificate, the client, the server, or both?A certificate is sent by one party to let the other party authenticate that it is who it claims to be. Based on this usage, you should be able to guess who sends the certificate and check the messages in your trace.**



The Server sends the Certificate as the source port is 443, which is the server.

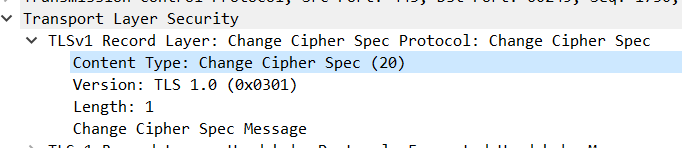
Client Key Exchange and Change Cipher Messages

**1. Who sends the Change Cipher Spec message, the client, the server, or both?**

****

**Both** server and client send the Change Cipher Spec message.

**2. What are the contents carried inside the Change Cipher Spec message? Look past the Content Type and other headers to see the message itself.**

****

**Content Type**: Change Cipher Spec (20)

