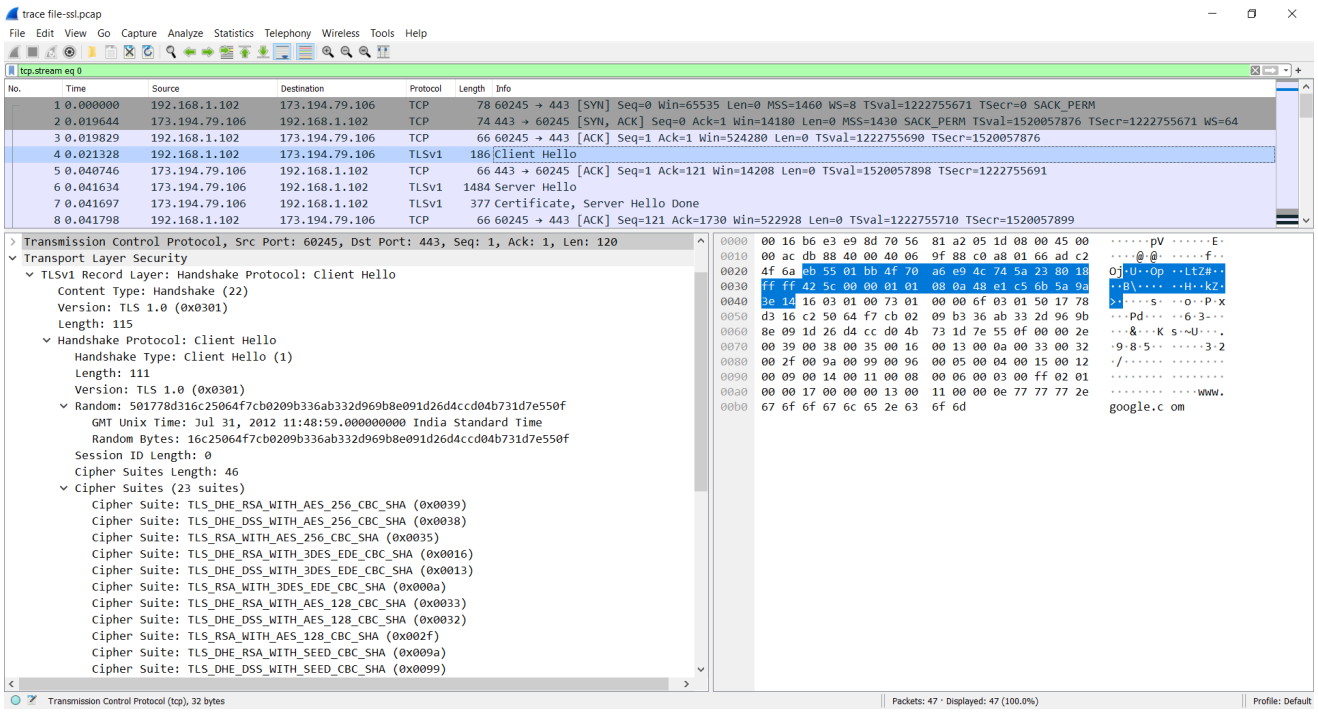
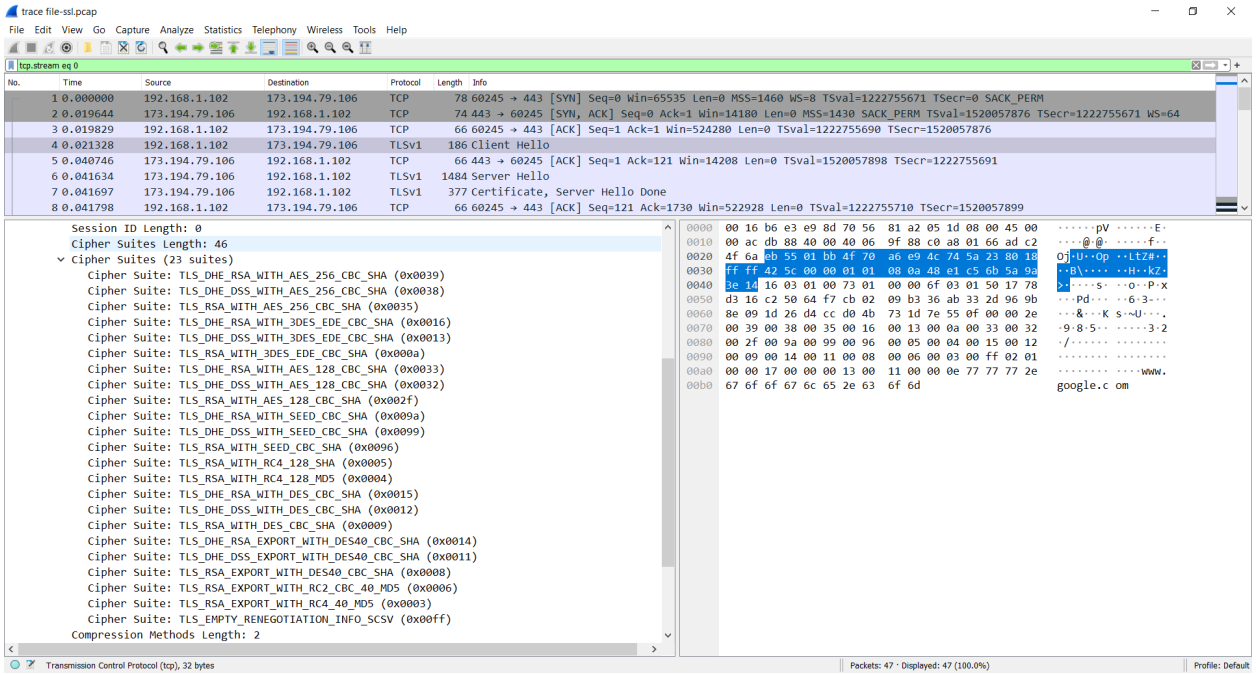
Cryptography and Network Security Lab

Name: Shrutika Rajendra Adhav
PRN : 2019BTECS00027
Batch : B1

Examining TLS Client Hello packet :

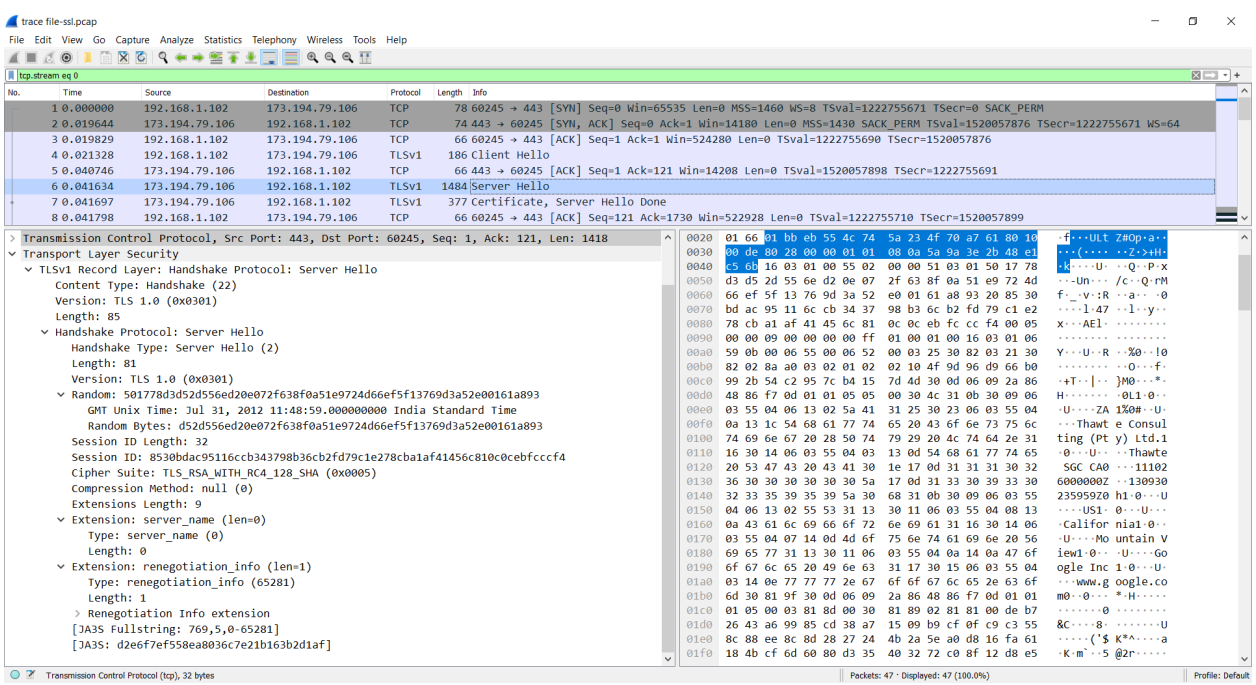


Examining Client Hello packet for possible encryption,hashing algorithms cipher suites :

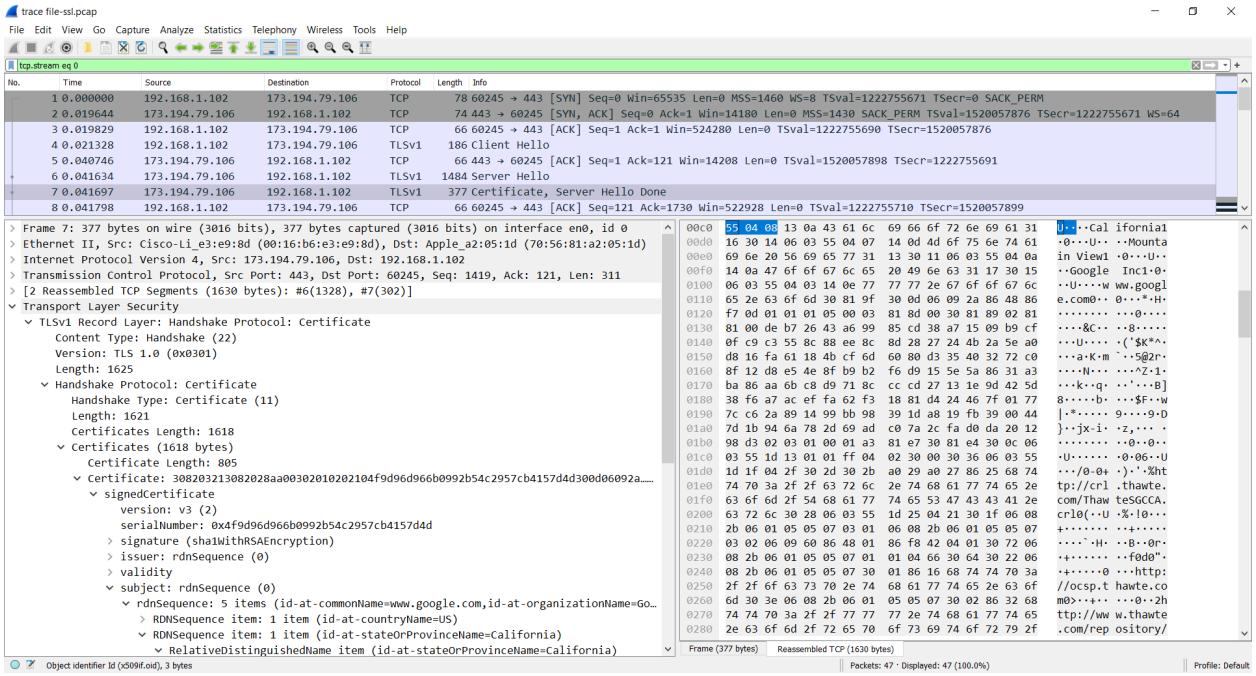


Examining Server Hello message for cipher suite:

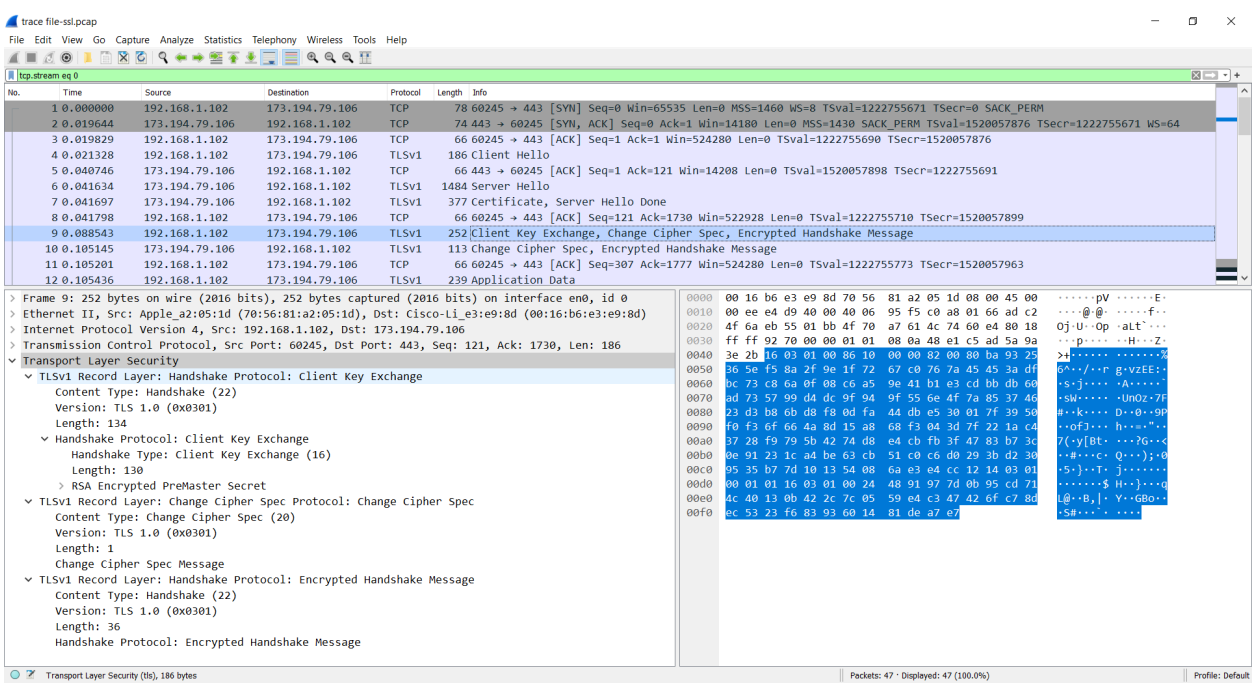
Cipher suite used here: TLS_RSA_WITH_RC4_128_SHA (0x0005)



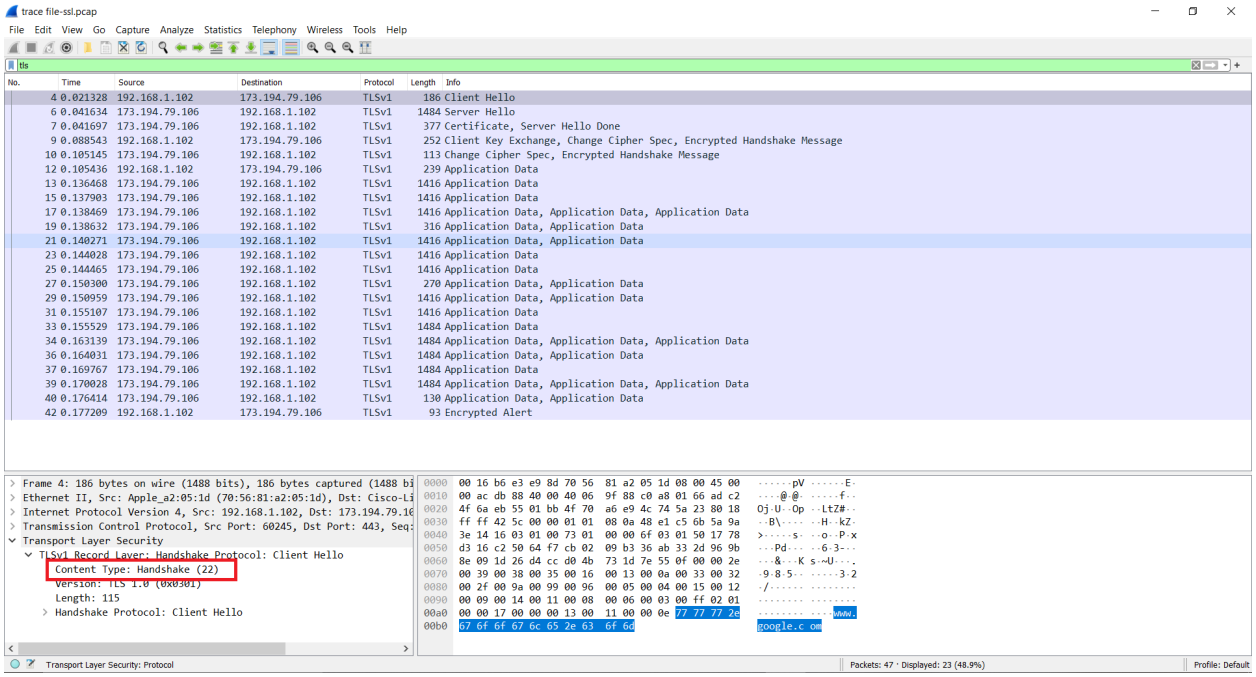
Examining server certificate packet for certificate details :



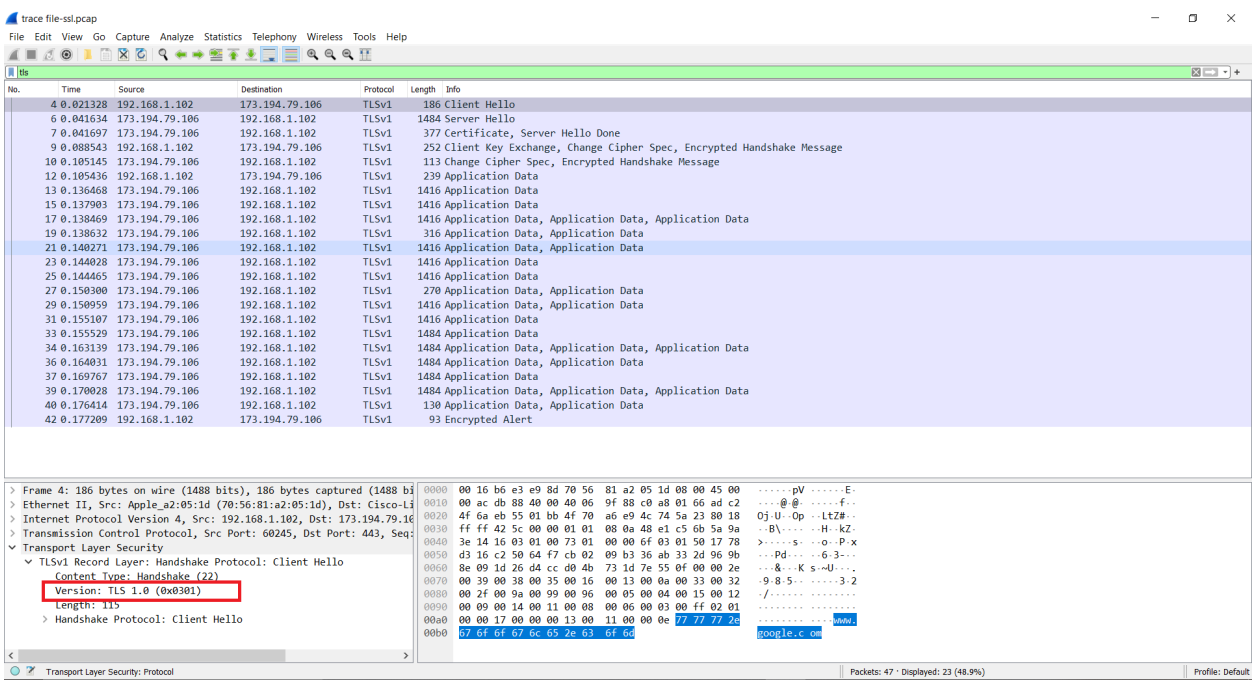
Examining client key exchange packet for encryption of further packets:



1. What is the Content Type for a record containing Application Data?
Ans: The content type is Handshake (22)

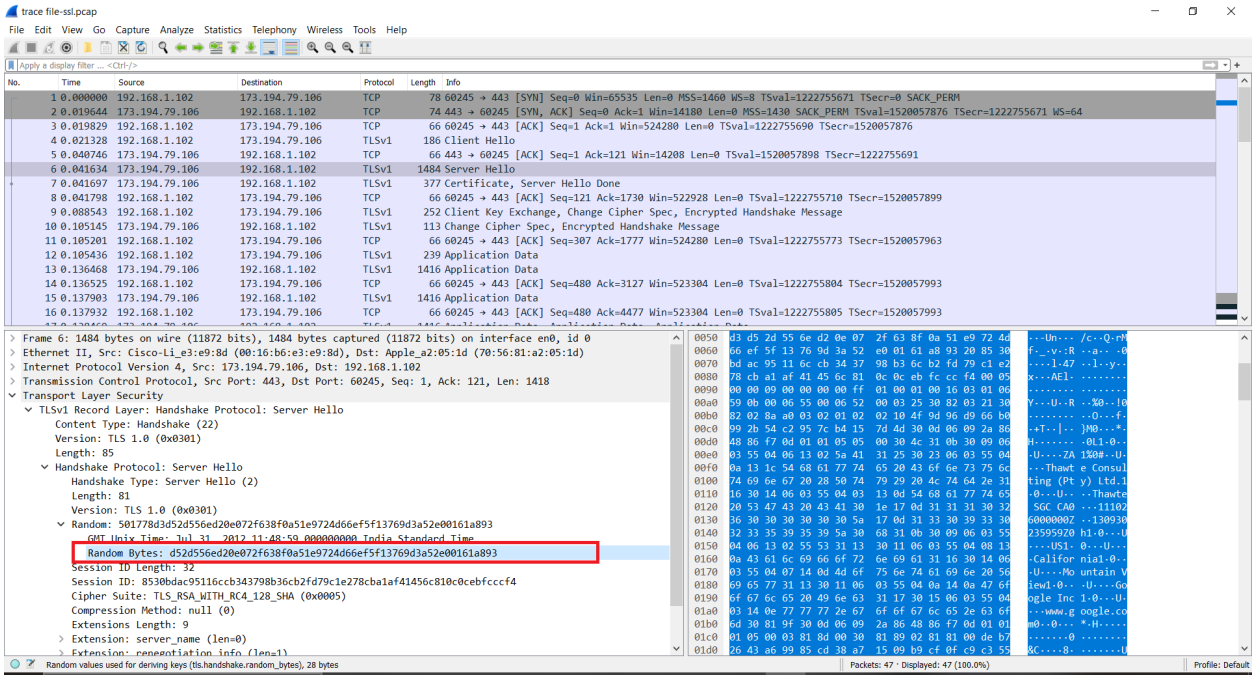


2. What version constant is used in your trace, and which version of TLS does it represent?
Ans: The TLS version used is TLS 1.0 (0x0301)



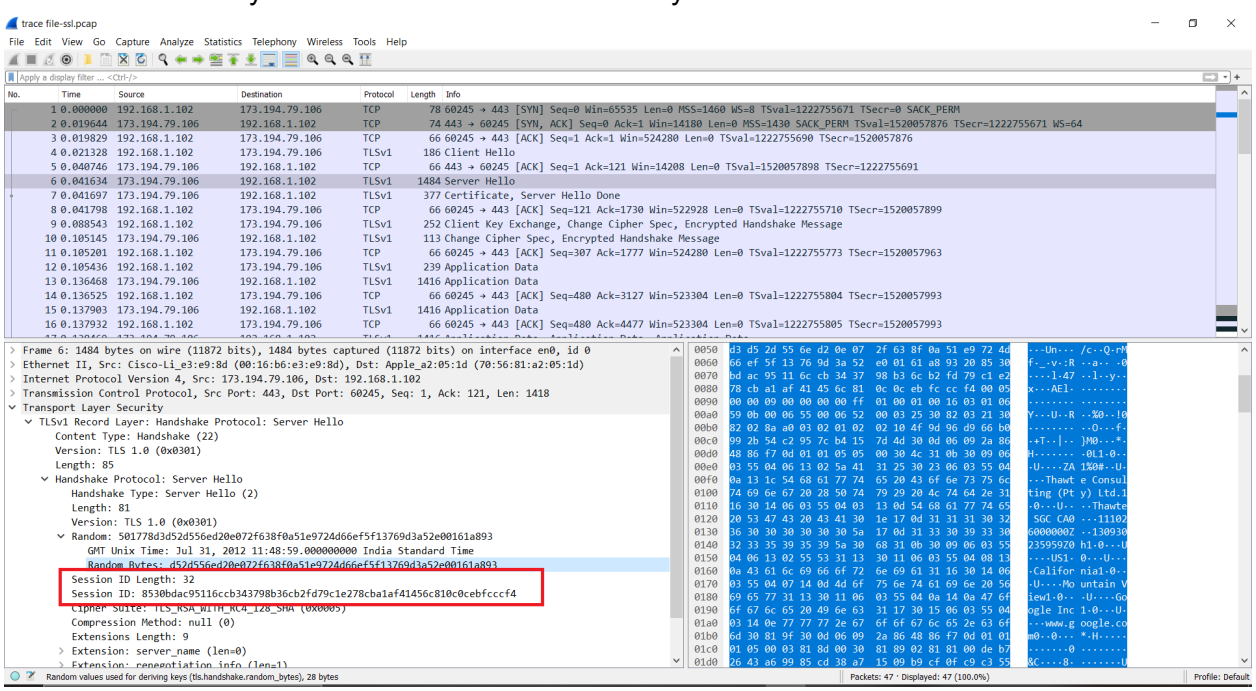
3. How long in bytes is the random data in the Hellos? Both the Client and Server include this random data (a nonce) to allow the establishment of session keys.

Ans : The random bytes is 28 hex characters of 14 bytes



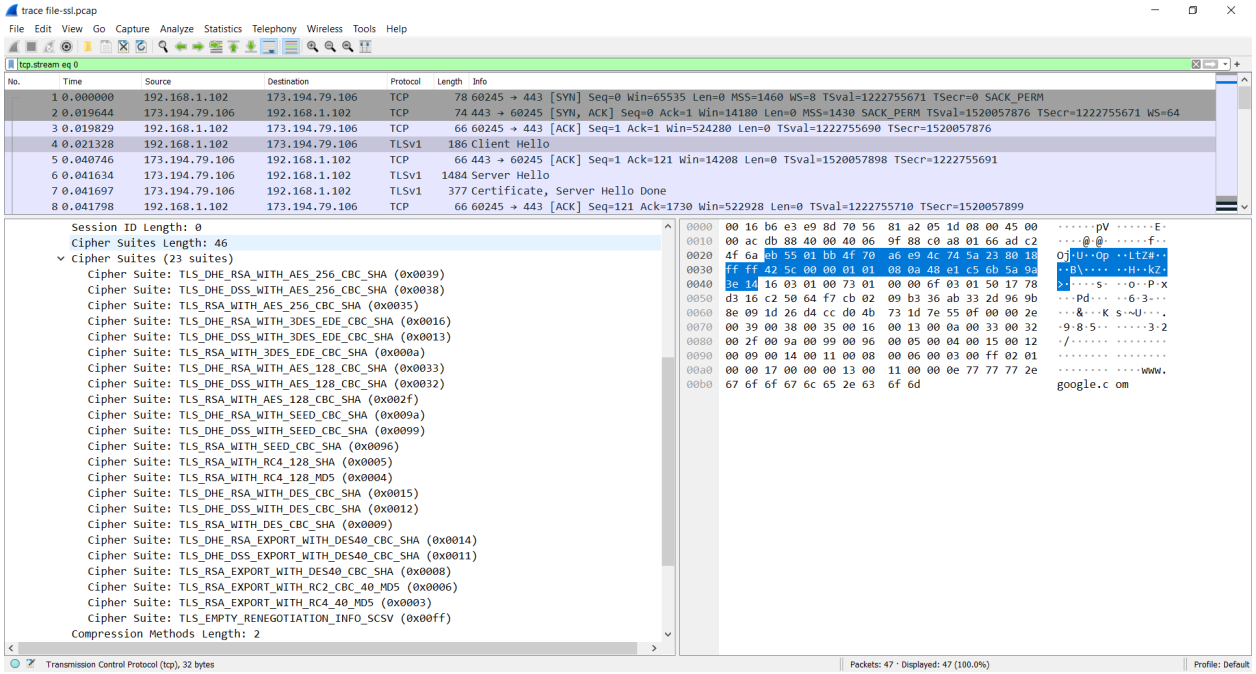
4. How long in bytes is the session identifier sent by the server?This identifier allows later resumption of the session with an abbreviated handshake when both the client and server indicate the same value. In our case, the client likely sent no session ID as there was nothing to resume.

Ans: The random bytes is 32 hex characters of 16 bytes



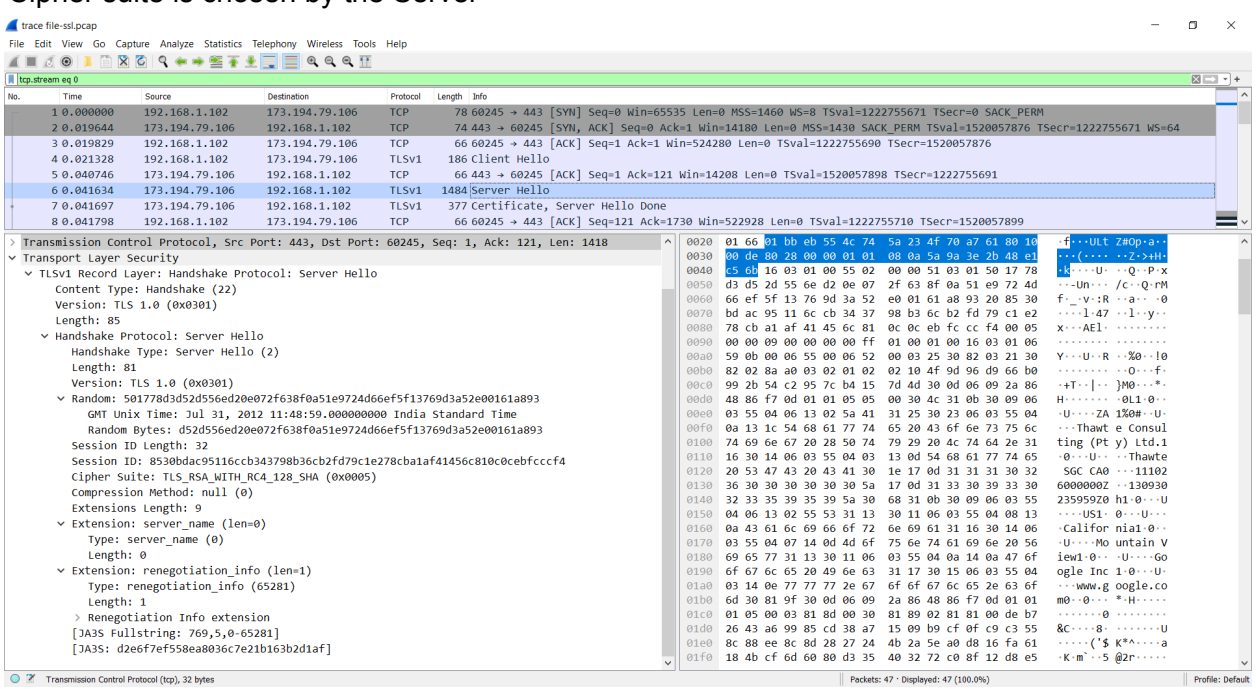
6. What Cipher suite is chosen by the Server? Give its name and value. The Client will list the different cipher methods it supports, and the Server will pick one of these methods to use.

Ans: The Client will list the different cipher methods it supports



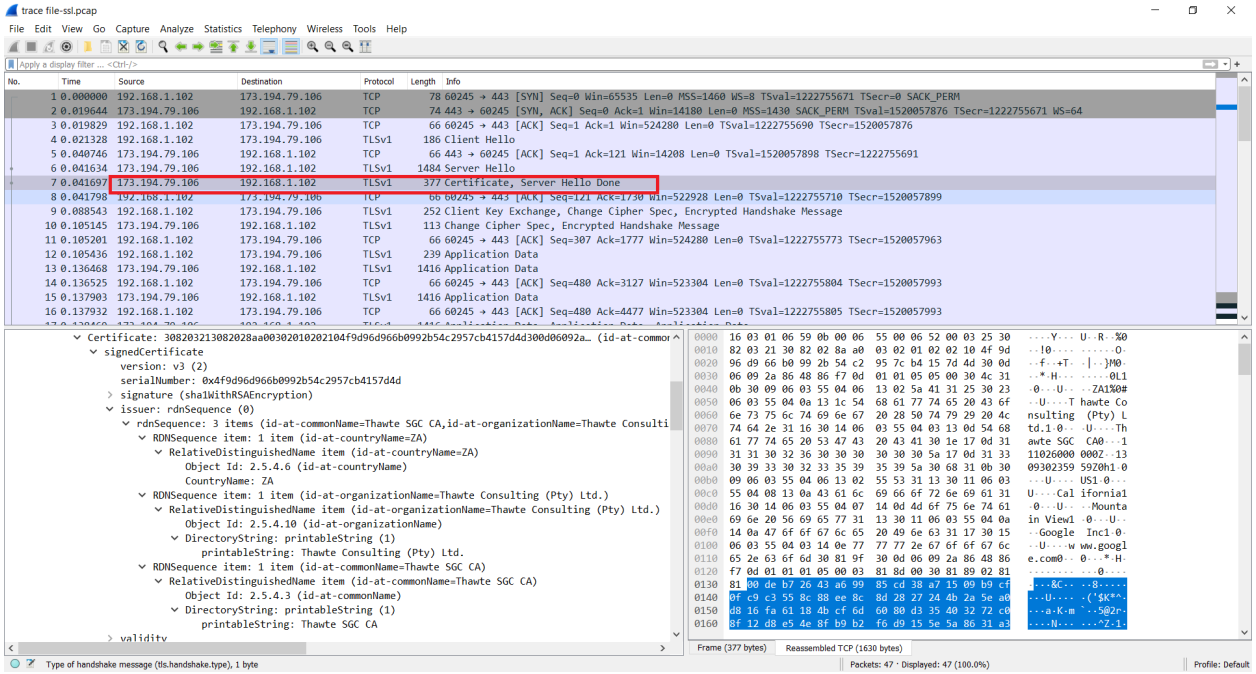
Cipher suite used here: TLS_RSA_WITH_RC4_128_SHA (0x0005)

Cipher suite is chosen by the Server



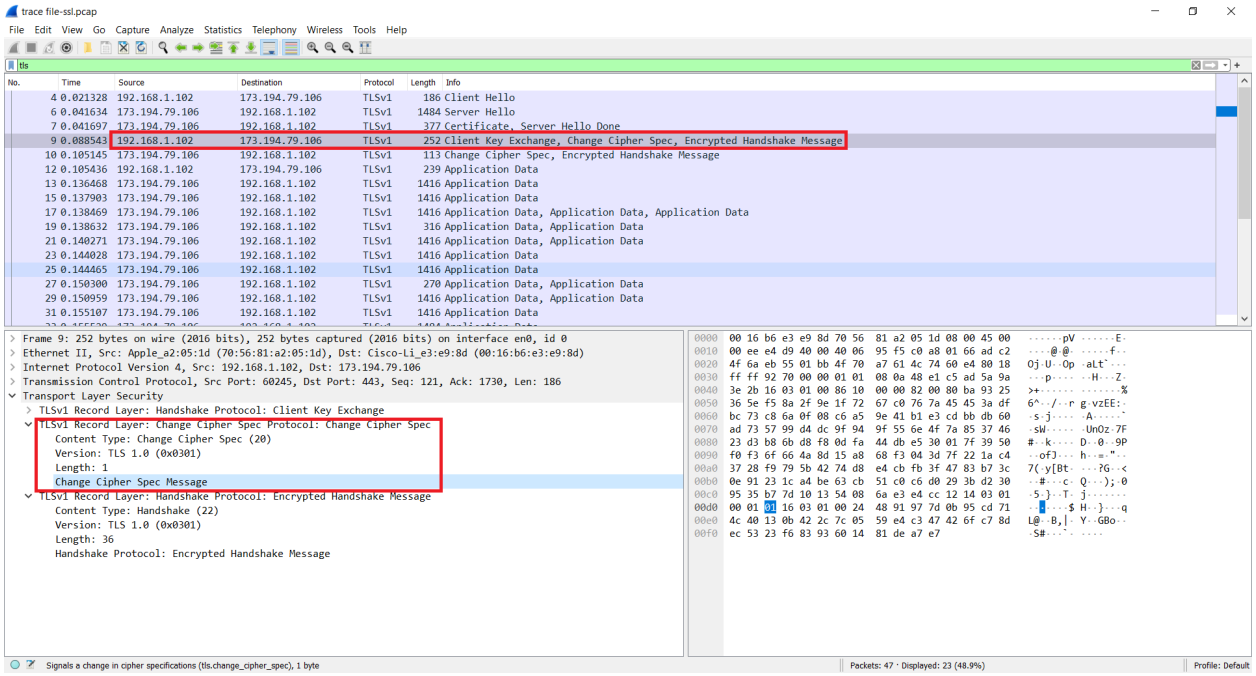
7. Who sends the Certificate, the client, the server, or both?A certificate is sent by one party to let the other party authenticate that it is who it claims to be. Based on this usage, you should be able to guess who sends the certificate and check the messages in your trace

Ans: The certificate is sent by the server

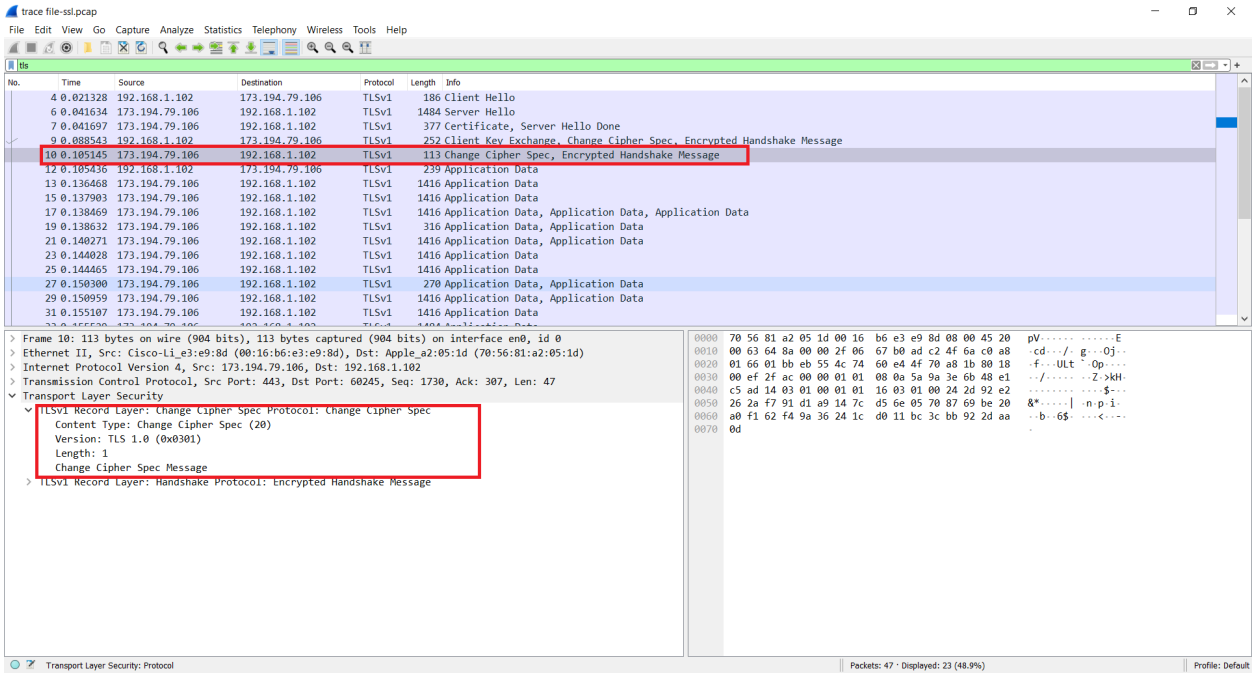


8.Who sends the Change Cipher Spec message, the client, the server, or both?

Ans: The client sends the change cipher spec message first



Server change cipher spec message



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

Ans: