C&NS Lab Assignment 16

Onkar Santosh Gavali (2019BTECS00037)

Batch B2

# Index

SSL and TLS

* Explain SSL and TLS

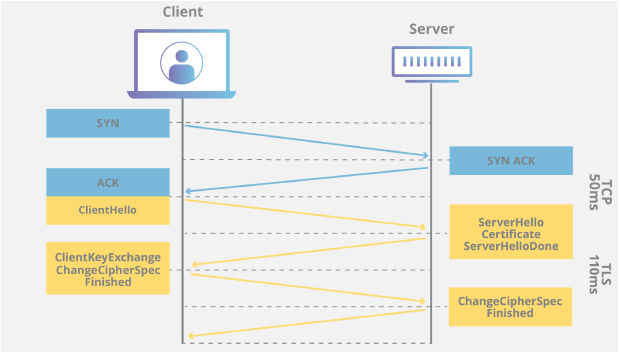
# 

# 

# SSL and TLS

**SSL** (Secure Sockets Layer) and its successor, TLS (Transport Layer Security), are protocols for establishing authenticated and encrypted links between networked computers. Although the SSL protocol was deprecated with the release of TLS 1.0 in 1999, it is still common to refer to these related technologies as “SSL” or “SSL/TLS.” The most current version is TLS 1.3, defined in RFC 8446

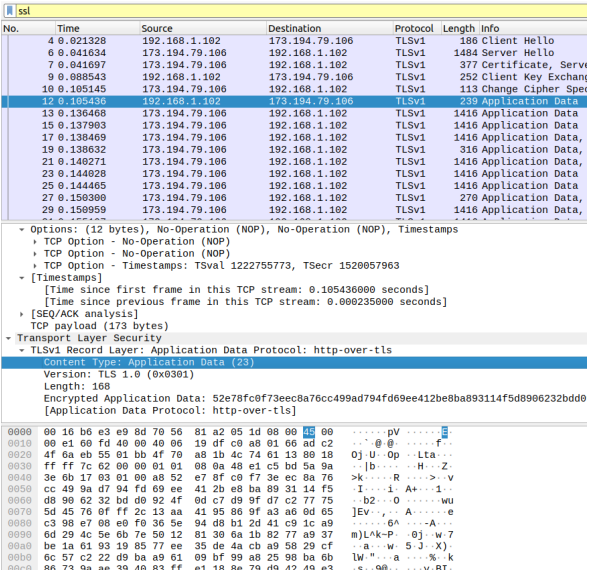
**TLS** (Transport Layer Security), released in 1999, is the successor to the SSL (Secure Sockets Layer) protocol for authentication and encryption. TLS 1.3 is defined in in RFC 8446 (August 2018).



# Questions:

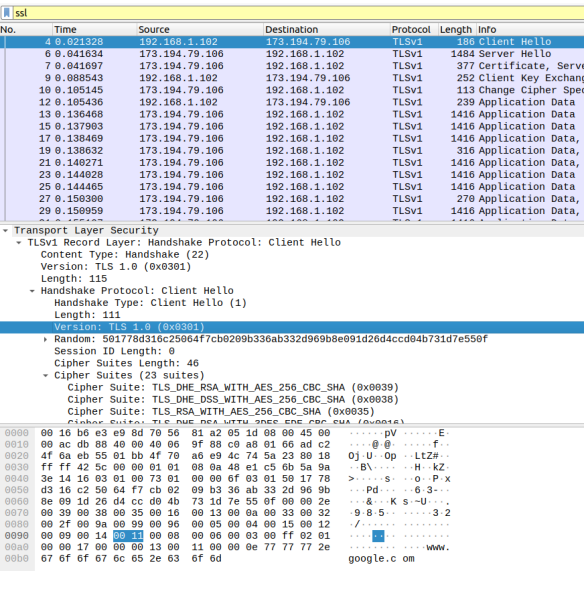
# 1. What is the Content-Type for a record containing Application Data?

# Content-Type is: Application Data (23)



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

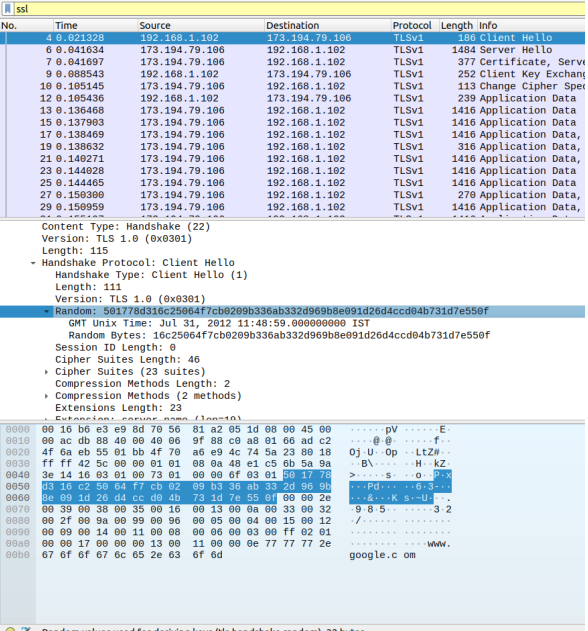
Ans: TLS version : 1.0 TLS version constant: 0x0301



**4.1 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.**

Ans: Length of Random data filed: 32 bytes

# 



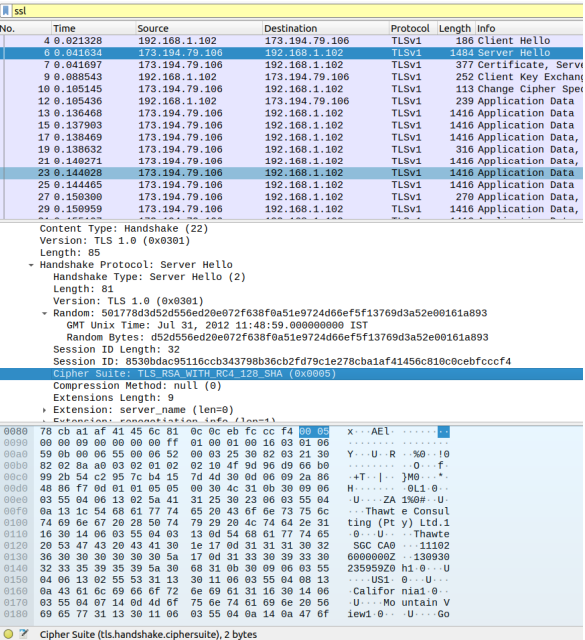
**2. How long in bytes is the session identifier sent by the server?This identifier allows later resumption of the session with an abbreviated handshake when both the client and server indicate the same value. In our case, the client likely sent no session ID as there was nothing to resume.**

Ans: Session ID length : 32

# 

**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.**

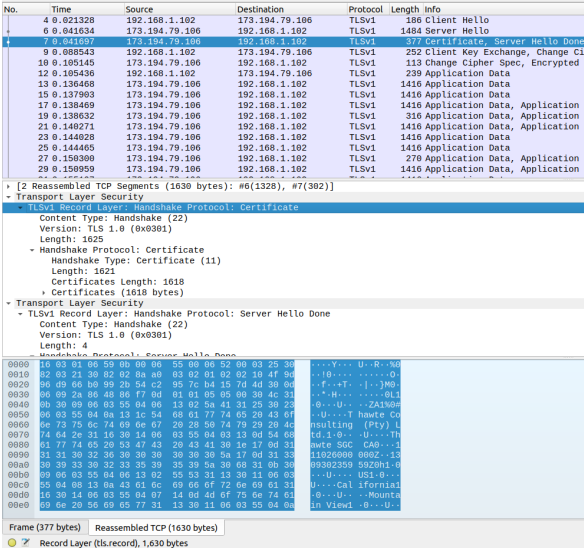
Ans: Cipher Suit name: TLS\_RSA\_WITH\_RC4\_128\_SHA (0x0005)



**4.2 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.

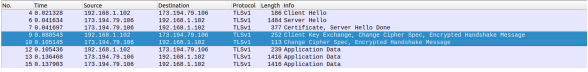
Ans: Server sends the certificate



**4.3 Client Key Exchange and Change Cipher Messages**

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

Ans: Both server and client sends 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**

Ans: Change Cipher Spec message contains: Content Type, Version, Length and Change Cipher Spec Message

