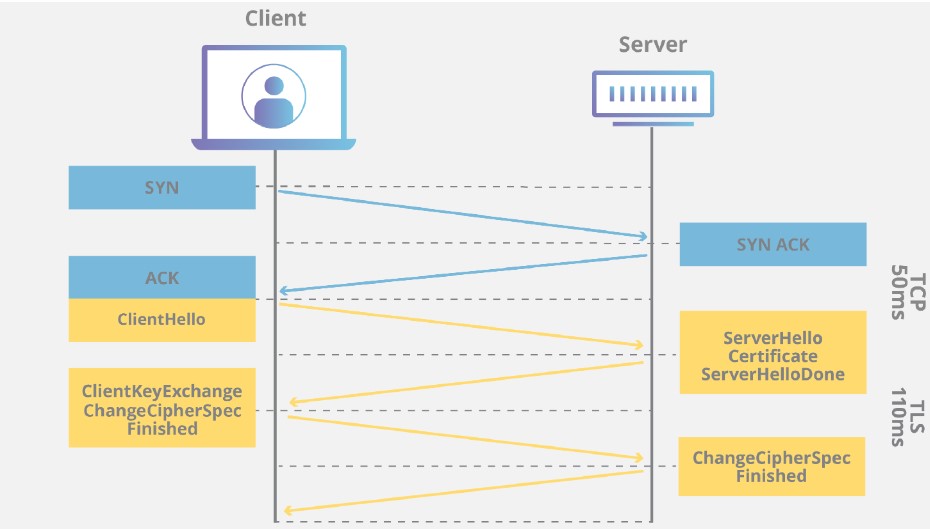
Name: Rithik Sarvesh Bharathiraja

UID: 120395246

Course: ENPM693

Task: Homework 6

Part – 1



This is a packet capture of the conversation between the client and badssl.com

Client hello

Following important parameters are sent to the server in the client\_hello message

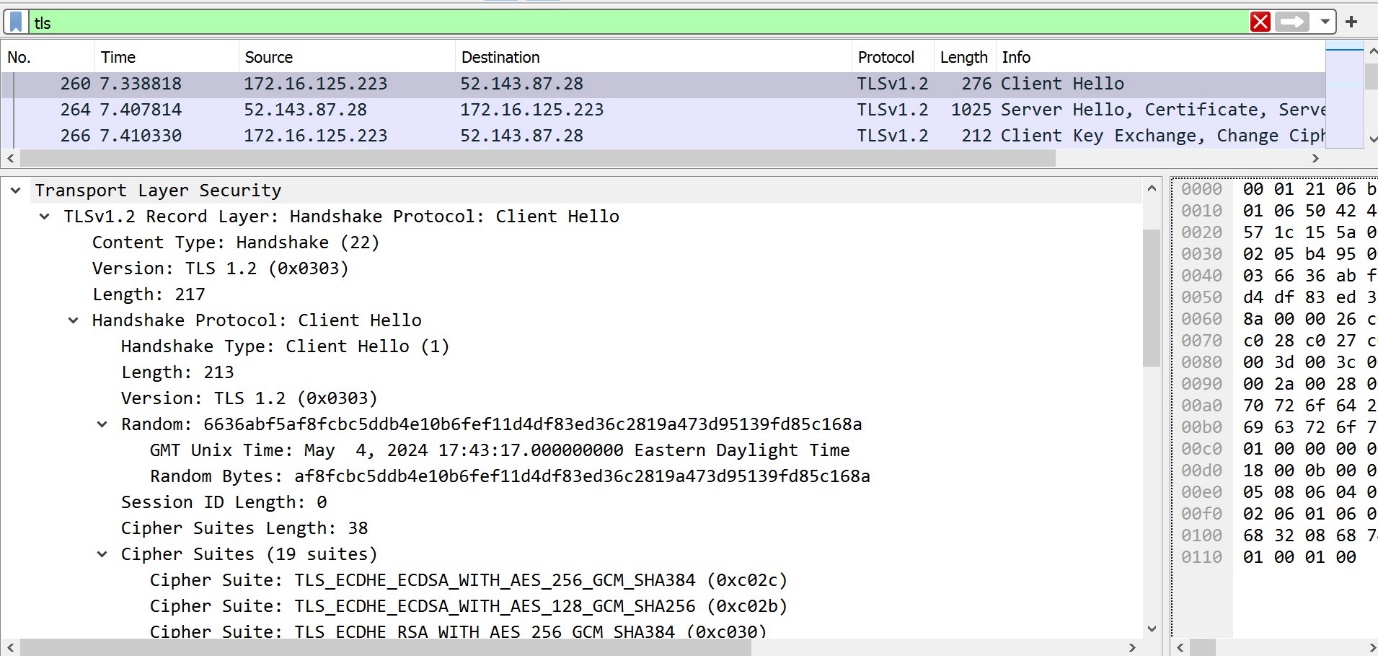
Version – TLS version

Timestamp – to prevent replay attack

random bytes - generated by the client

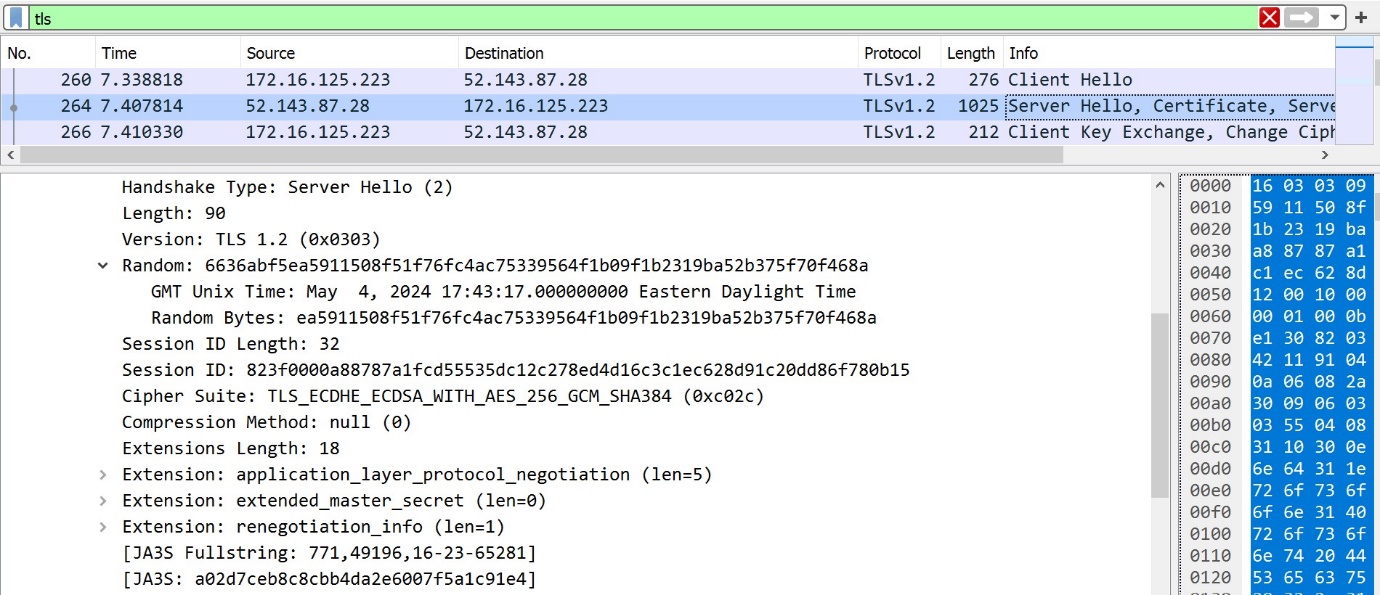
Session ID – To check whether the connection was established already.

Cipher suites – The types of cipher suites supported by the client

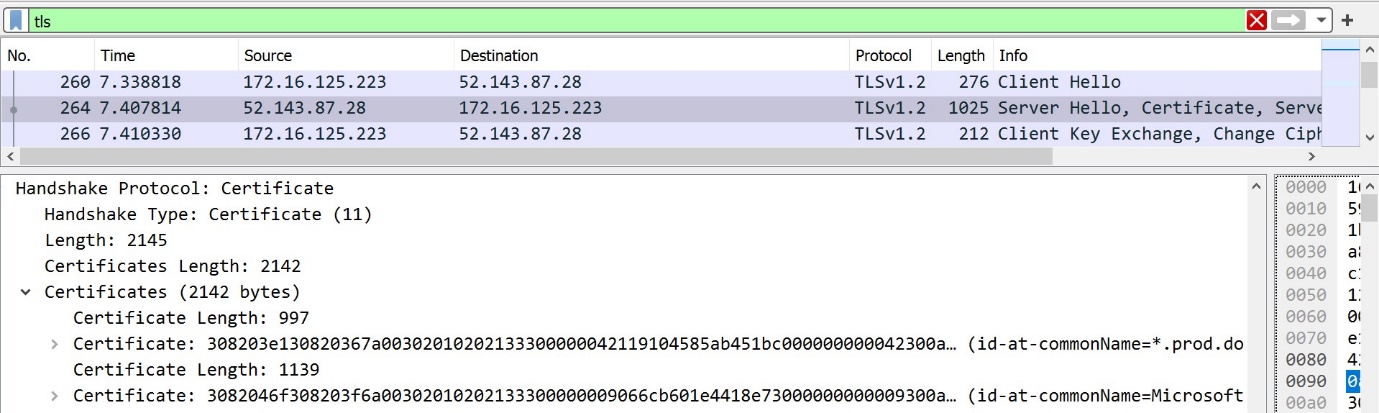


Server hello

In response to client hello, server sends the server\_hello message. In this, server chooses the cipher suite and sends that to the client. Along with that, session is established and unique session ID is generated and sent to the client.



After server\_hello, the server sends its certificate to the client.



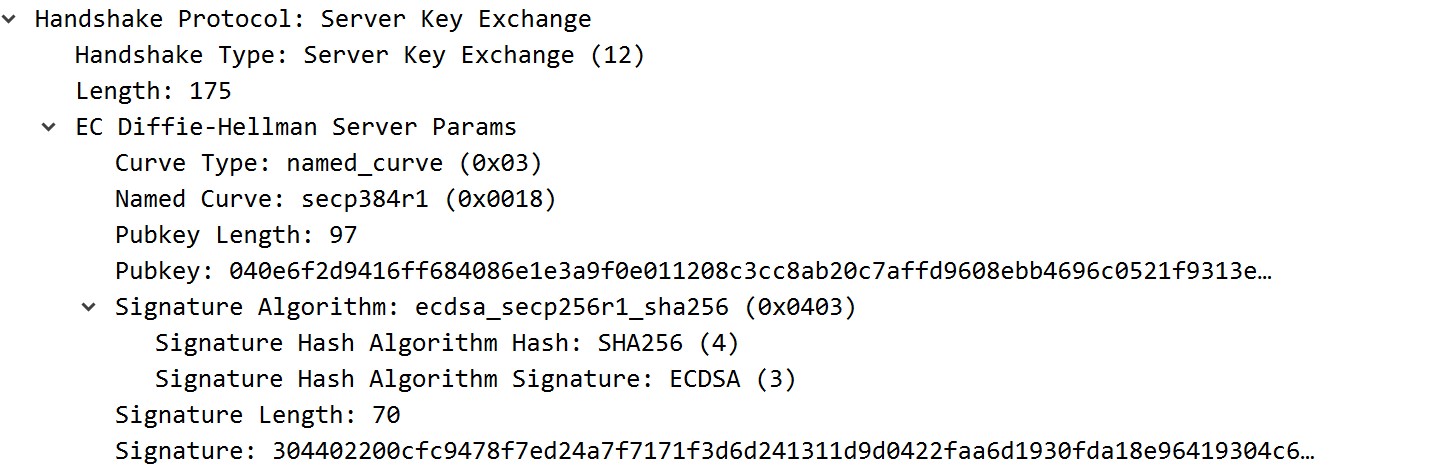
In certificate, it comes up with various important parameters like

* Signature
* Issuer
* Validity
* Subject

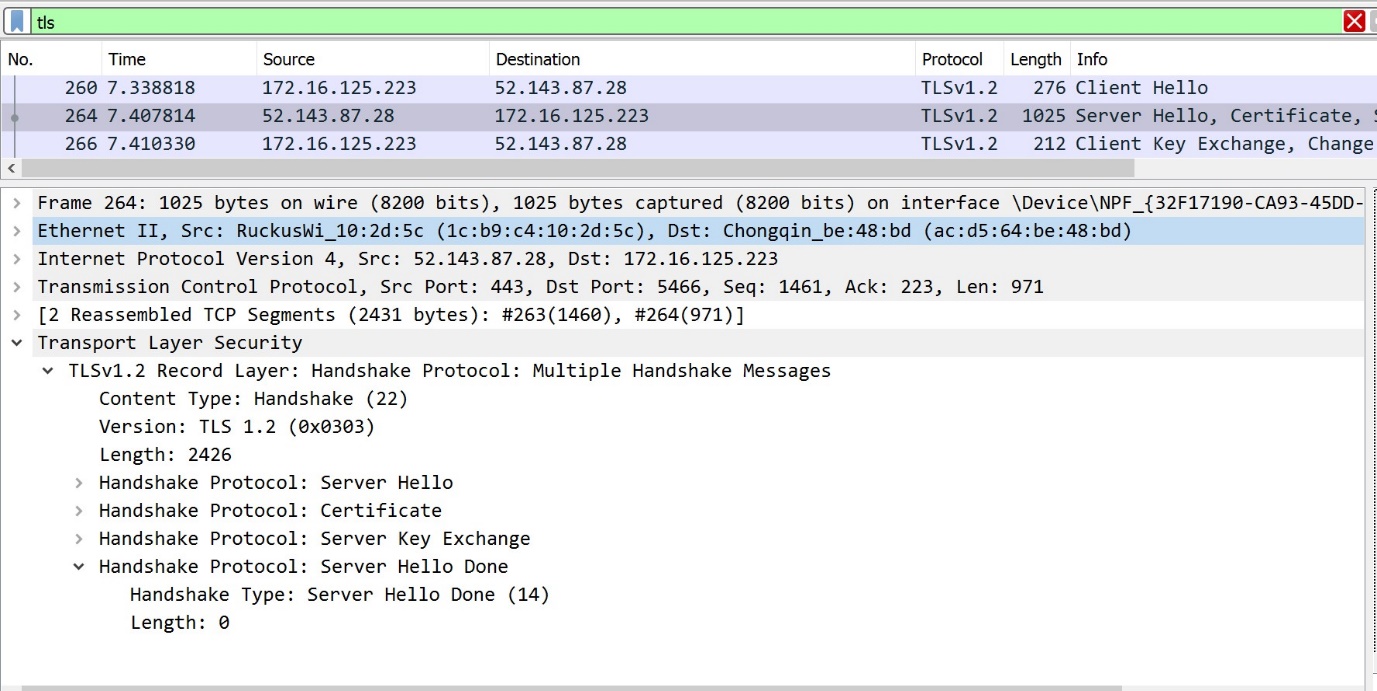




To exchange keys, server sends the key exchange algorithm and its parameter.

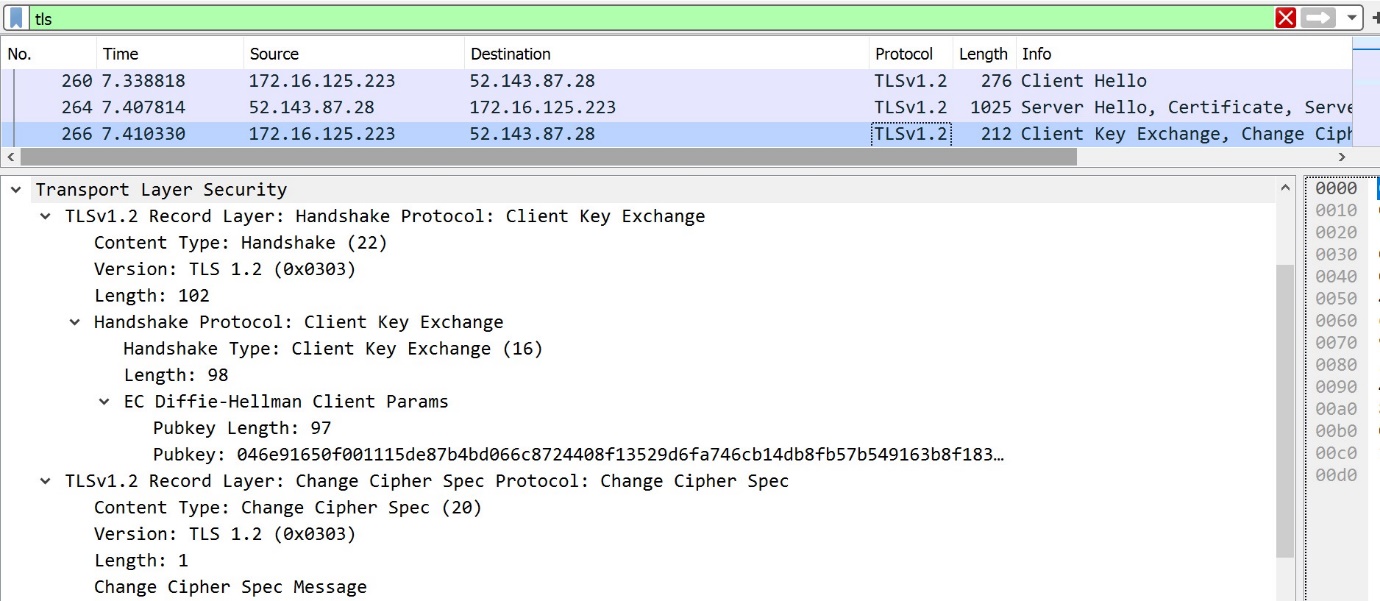


At last, the server sends the server\_hello\_done message to mark the end of server hello



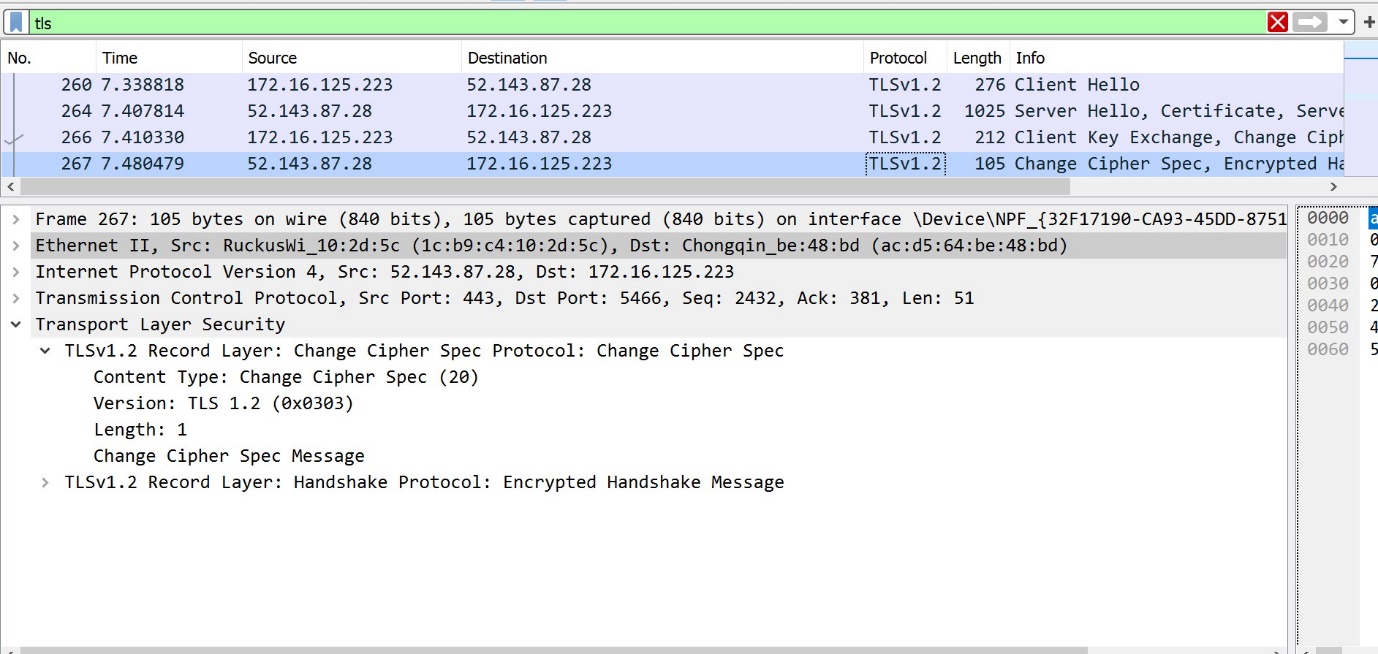
Client key exchange and cipher change spec

In response, the client sends its parameter for key exchange and it acknowledges that the server has chosen a cipher suite.



Server reply

Server acknowledges the client’s acknowledgement and starts sending in the data after that.



Part 2

After following the given steps, packet capture was done after accessing https://www.iplt20.com website. Using the sslkeylog.txt, wireshark decrypts the data sent in the https. At the end, readable html tags were found in the below tab.

