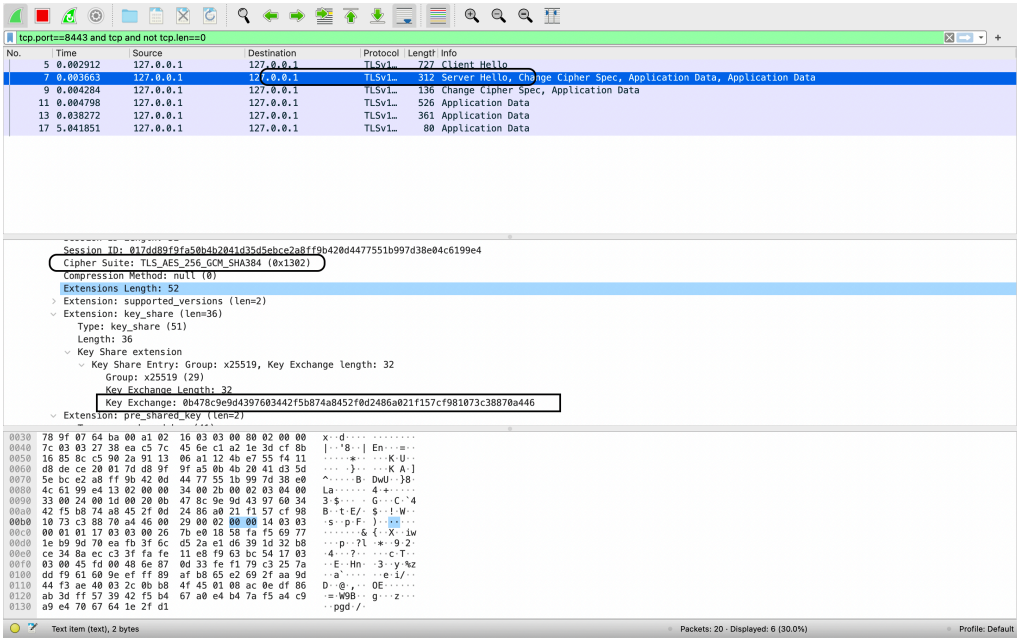
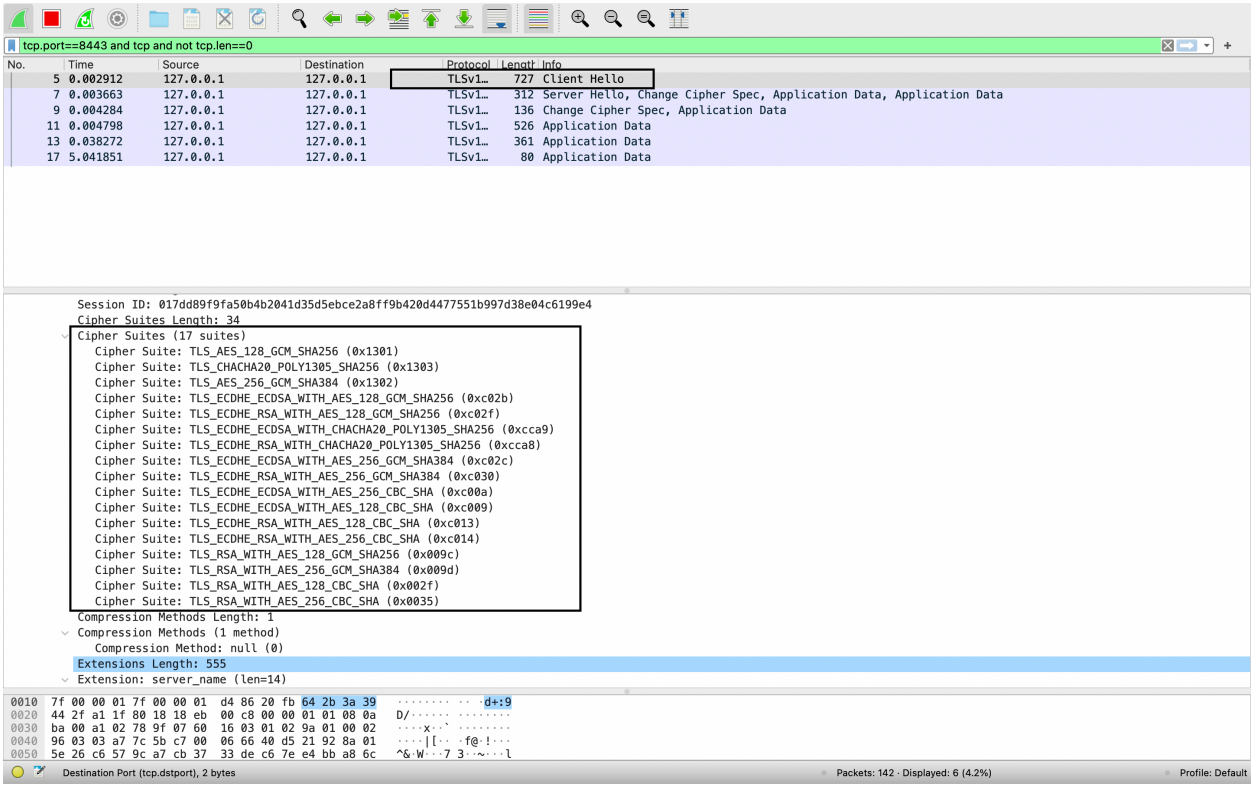
Wireshark sniffing for Firefox Browser packets of https://localhost:8443/

1. Asymmetric key exchange between server to client when ServerHello packet is sent.



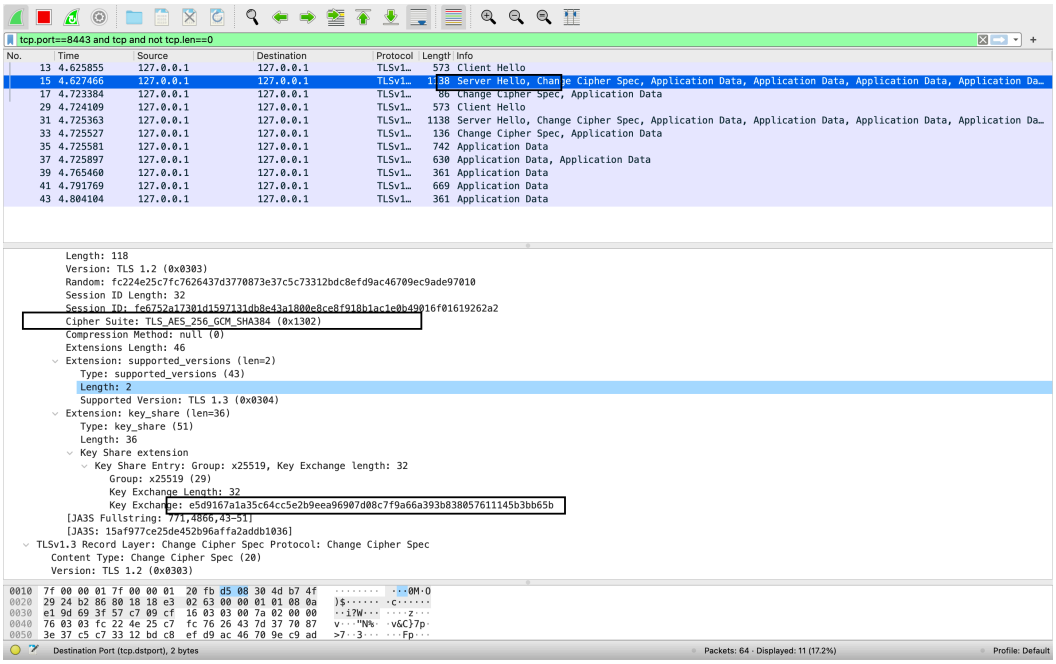
2. Cypher suites available with browser are sent to the server with ClientHello Packet



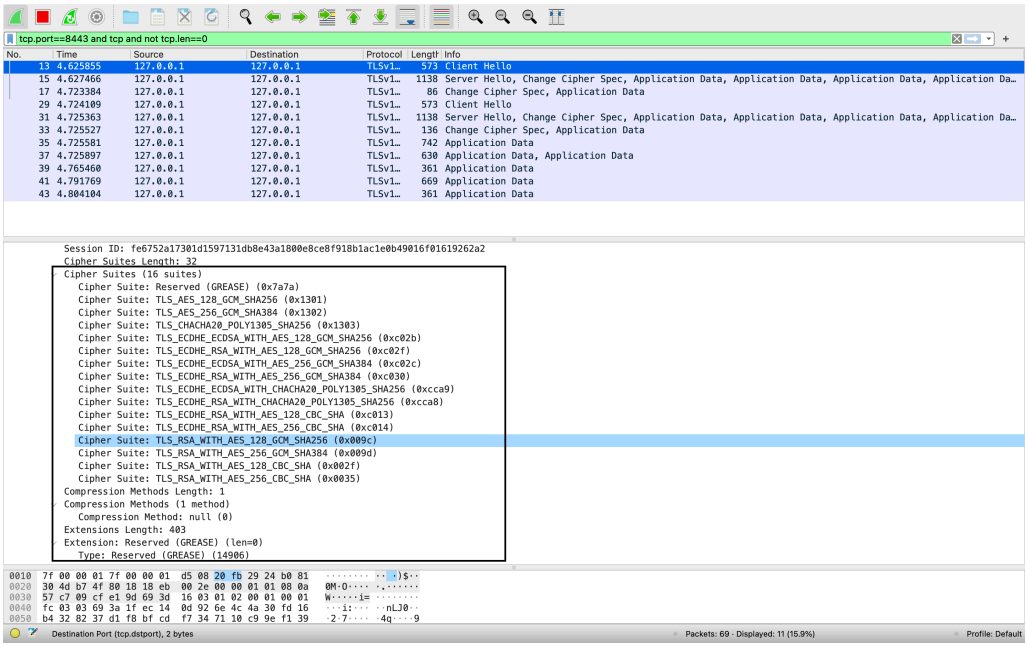
3. There is no exchange of symmetric key between the server and client on Firefox browser.

Wireshark sniffing for Google Chrome Browser packets of https://localhost:8443/

1.Asymmetric key exchange between server to client when ServerHello packet is sent.



2. Cypher suites available with browser are sent to the server with ClientHello Packet



3. There is no exchange of symmetric key between the server and client on Firefox browser.

6. A
However, in google chrome the TCP handshake happens twice. This is attributed because chrome sends the second clienthello message with GREASE extension which is google proprietary protocol

6.B
There is an extra cypher suite available of GREASE in google chromes cypher suite.

6.C
The cypher protocol selected for both browsers is the same.

7.
Yes, the cypher used for communication was the same - TLS_AES_256_GCM_SHA384.
However, there was an exchange of keys for symmetric key between client and server which was not present on localhost network.
This I believe was done due to exchange of certificate on the server for verification which proceeded with symmetric key exchange.
Furthermore, I did the testing with Firefox as a browser, thus could see the keyexchange packet being sent regularly. This was with the change of port listening on server from 443 to 546** as allocated by server for the new tcp connection.