Shubham Chomate
Roll. No. 31118

Assignment-12

Problem statement: To study SSL protocol by capturing the packets using wireshark while visiting any SSL secured website. To study IPsec & protocol by capturing data packet in wire shark.

Pre-requisite:
knowledge of protocols & wireshark.

Learning objectives:
Learn use & importance of SSL.

Theory:

SSL stands for Secure Socket layer. It is an encryption method used to prevent anyone other than webserver & the user from evesdropping on the transmission of sensitive personal | financial information.

This encryption can secure a connection between website & a browser (or) an email host & client. Integrating SSL into webpage improves security by reducing risk identity theft.

SSL certificates:

1) They are an essential component of the data encryption process that makes internet transaction secure.

2) They are digital passports that provide authentication to protect the confidentiality & integrity

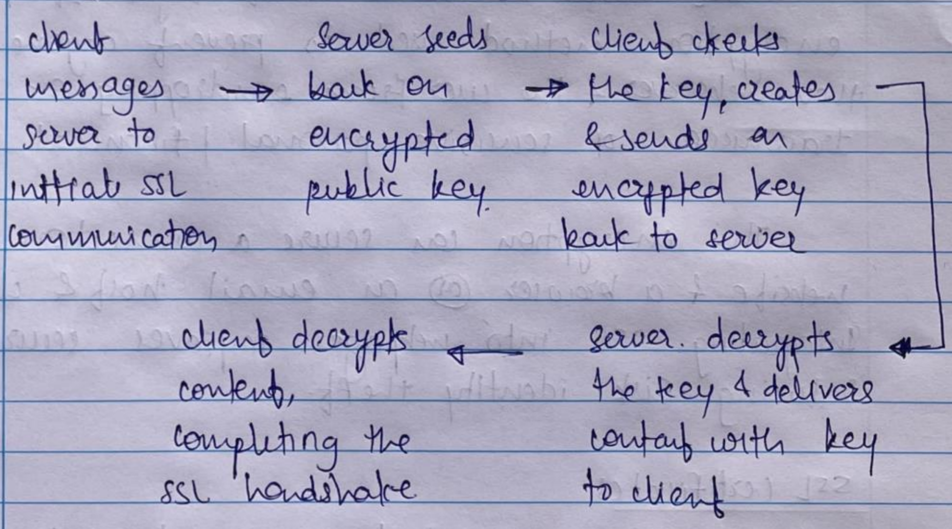
of website communication with browser.

3) The SSL certificates job is to initiate secure sessions with user's browser via the secure socket layer protocol.

This secure connection cannot be established without SSL certificate, which digitally connects company information to a cryptographic key.

4) Any organization that engages in e-commerce must have an SSL-certificate on it's webserver to ensure safety of customer & company information as well as security of financial transactions.

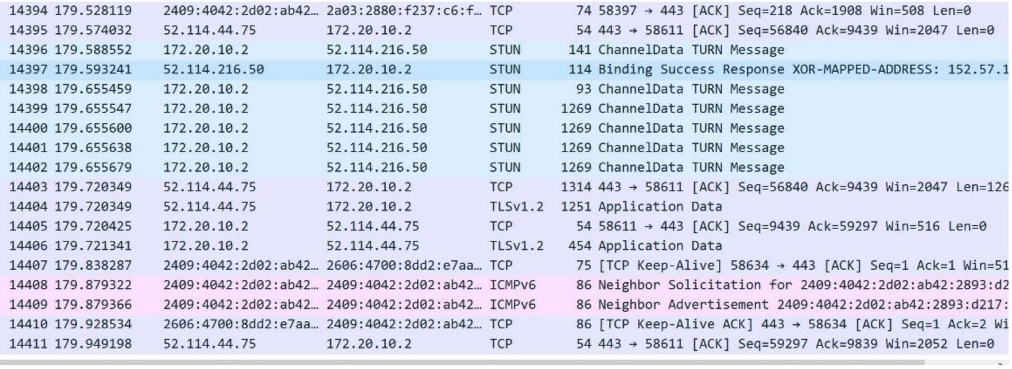
Working:



client messages server to initiate SSL communication → Server sends back an encrypted public key. → client checks the key, creates & sends an encrypted key back to server → server decrypts the key & delivers content with key to client → client decrypts content, completing the SSL handshake

Conclusion:

In this study assignment, I have successfully studied the SSL protocol with the help of wireshark



```
14394 179.528119    2409:4042:2d02:ab42… 2a03:2880:f237:c6:f… TCP       74 58397 → 443 [ACK] Seq=218 Ack=1908 Win=508 Len=0
14395 179.574032    52.114.44.75         172.20.10.2          TCP       54 443 → 58611 [ACK] Seq=56840 Ack=9439 Win=2047 Len=0
14396 179.588552    172.20.10.2          52.114.216.50        STUN     141 ChannelData TURN Message
14397 179.593241    52.114.216.50        172.20.10.2          STUN     114 Binding Success Response XOR-MAPPED-ADDRESS: 152.57.1
14398 179.655459    172.20.10.2          52.114.216.50        STUN      93 ChannelData TURN Message
14399 179.655547    172.20.10.2          52.114.216.50        STUN    1269 ChannelData TURN Message
14400 179.655600    172.20.10.2          52.114.216.50        STUN    1269 ChannelData TURN Message
14401 179.655638    172.20.10.2          52.114.216.50        STUN    1269 ChannelData TURN Message
14402 179.655679    172.20.10.2          52.114.216.50        STUN    1269 ChannelData TURN Message
14403 179.720349    52.114.44.75         172.20.10.2          TCP     1314 443 → 58611 [ACK] Seq=56840 Ack=9439 Win=2047 Len=126
14404 179.720349    52.114.44.75         172.20.10.2          TLSv1.2 1251 Application Data
14405 179.720425    172.20.10.2          52.114.44.75         TCP       54 58611 → 443 [ACK] Seq=9439 Ack=59297 Win=516 Len=0
14406 179.721341    172.20.10.2          52.114.44.75         TLSv1.2  454 Application Data
14407 179.838287    2409:4042:2d02:ab42… 2606:4700:8dd2:e7aa… TCP       75 [TCP Keep-Alive] 58634 → 443 [ACK] Seq=1 Ack=1 Win=51
14408 179.879322    2409:4042:2d02:ab42… 2409:4042:2d02:ab42… ICMPv6    86 Neighbor Solicitation for 2409:4042:2d02:ab42:2893:d2
14409 179.879366    2409:4042:2d02:ab42… 2409:4042:2d02:ab42… ICMPv6    86 Neighbor Advertisement 2409:4042:2d02:ab42:2893:d217:
14410 179.928534    2606:4700:8dd2:e7aa… 2409:4042:2d02:ab42… TCP       86 [TCP Keep-Alive ACK] 443 → 58634 [ACK] Seq=1 Ack=2 Wi
14411 179.949198    52.114.44.75         172.20.10.2          TCP       54 443 → 58611 [ACK] Seq=59297 Ack=9839 Win=2052 Len=0
```