

Name: Rushikesh Kazbhai Palde
Roll No. 31258

Date	Page No.
/ / 20	

①

Assignment No. 12 (C4)

DOI: 03-12-2021

Title :- Study of SSL

Problem statement :-

To study the SSL protocol by capturing the packets using Wireshark tool while visiting any SSL secured website (banking, e-commerce etc.).

Pre-requisites :-

Knowledge of protocols, Wireshark :-

Objectives :-

- (i) To learn use of SSL protocol -
- (ii) To understand importance of SSL protocol -

Learning Outcomes :-

After completion of the assignment, students will be able to understand the use and importance of SSL protocol.

THEORY :-

SSL stands for Secure Socket Layer. It is an encryption method used to prevent anyone other than webserver and the user from eavesdropping on the transmission of sensitive personal or financial information.

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

SSL certificates :-

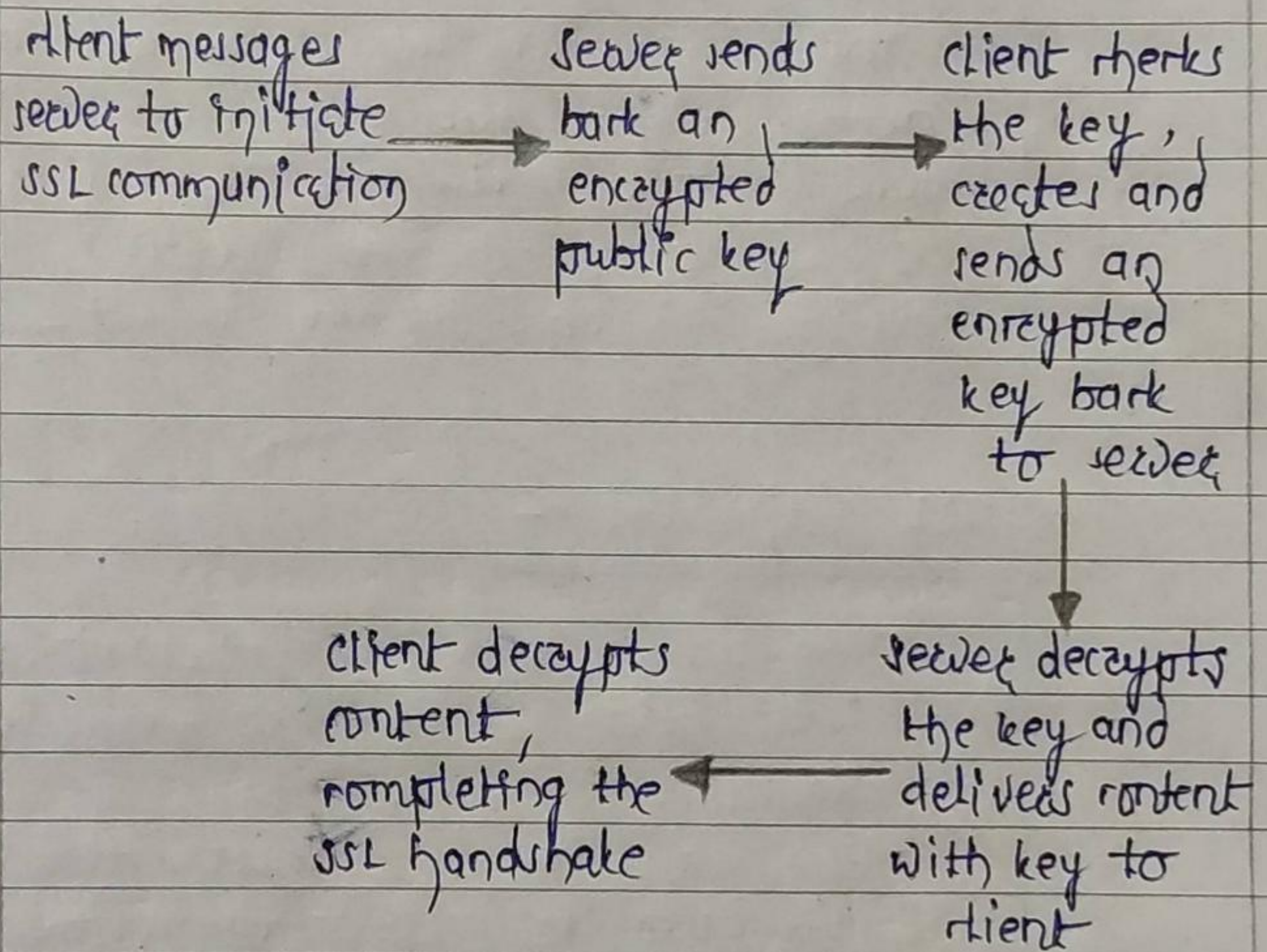
They are an essential component of the data encryption process that makes internet transactions secure.

They are digital passports that provide authentication to protect the confidentiality and integrity of website communication with browsers.

The SSL certificate's 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. Any organisations

that engages in e-commerce must have a SSL certificate on its webserver to ensure safety of customer and company information as well as the security of financial transactions.

Working :-



CONCLUSION :-

Successfully studied the SSL protocol with the help of Wireshark -

OUTPUT :-

The image shows a Wireshark packet capture of a TLS handshake. The filter is set to 'ip.addr==52.95.120.67'. The packets are as follows:

No.	Time	Source	Destination	Protocol	Length	Info
12010	99.619139	100.80.11.89	52.95.120.67	TCP	54	53497 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
12011	99.619406	100.80.11.89	52.95.120.67	TLSv1.2	571	Client Hello
12015	99.747671	52.95.120.67	100.80.11.89	TCP	60	[TCP Window Update] 443 → 53497 [ACK] Seq=1 Ack=1 Win=27136 Len=0
12016	99.749543	52.95.120.67	100.80.11.89	TCP	60	443 → 53497 [ACK] Seq=1 Ack=518 Win=28160 Len=0
12017	99.750617	52.95.120.67	100.80.11.89	TLSv1.2	1514	Server Hello
12018	99.750617	52.95.120.67	100.80.11.89	TCP	1514	443 → 53497 [ACK] Seq=1461 Ack=518 Win=28160 Len=1460 [TCP segment of a reassembled PDU]
12019	99.750617	52.95.120.67	100.80.11.89	TCP	1514	443 → 53497 [ACK] Seq=2921 Ack=518 Win=28160 Len=1460 [TCP segment of a reassembled PDU]
12020	99.750617	52.95.120.67	100.80.11.89	TLSv1.2	1514	Certificate, Certificate Status
12021	99.750617	52.95.120.67	100.80.11.89	TLSv1.2	293	Server Key Exchange, Server Hello Done
12022	99.750701	100.80.11.89	52.95.120.67	TCP	54	53497 → 443 [ACK] Seq=518 Ack=6080 Win=131328 Len=0
12023	99.753109	100.80.11.89	52.95.120.67	TLSv1.2	61	Alert (Level: Fatal, Description: Certificate Unknown)
12024	99.753186	100.80.11.89	52.95.120.67	TCP	54	53497 → 443 [FIN, ACK] Seq=525 Ack=6080 Win=131328 Len=0