Modern Education Society's
Wadia College of Engineering, Pune

NAME OF STUDENT:	**CLASS:**
SEMESTER/YEAR:	**ROLL NO:**
DATE OF PERFORMANCE:	**DATE OF SUBMISSION:**
EXAMINED BY:	**EXPERIMENT NO:**

Assignment No. 14 (Group - C)

Title: Capture and study SSL protocol packet.

Objectives:

Understand working of SSL Protocol

Problem Statement:

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

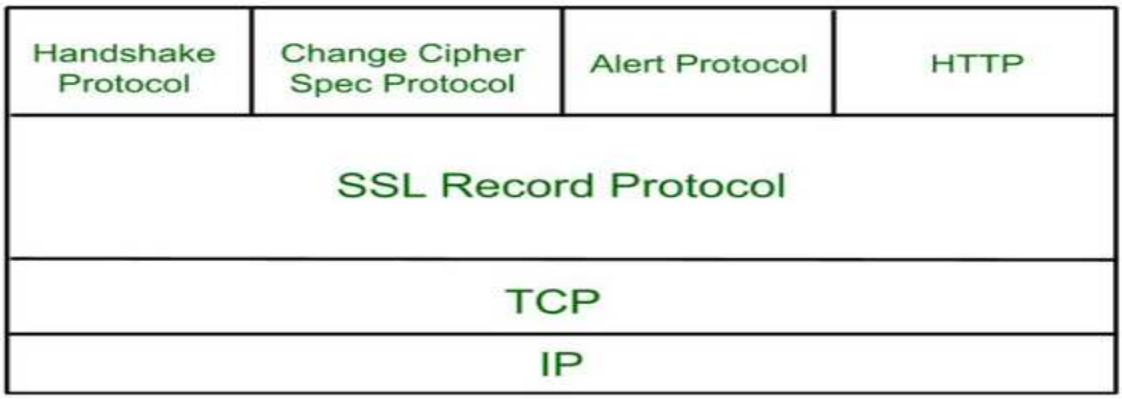
Outcomes:

Understands working of SSL Protocol

Tools Required:

Software: wireshark

Theory:

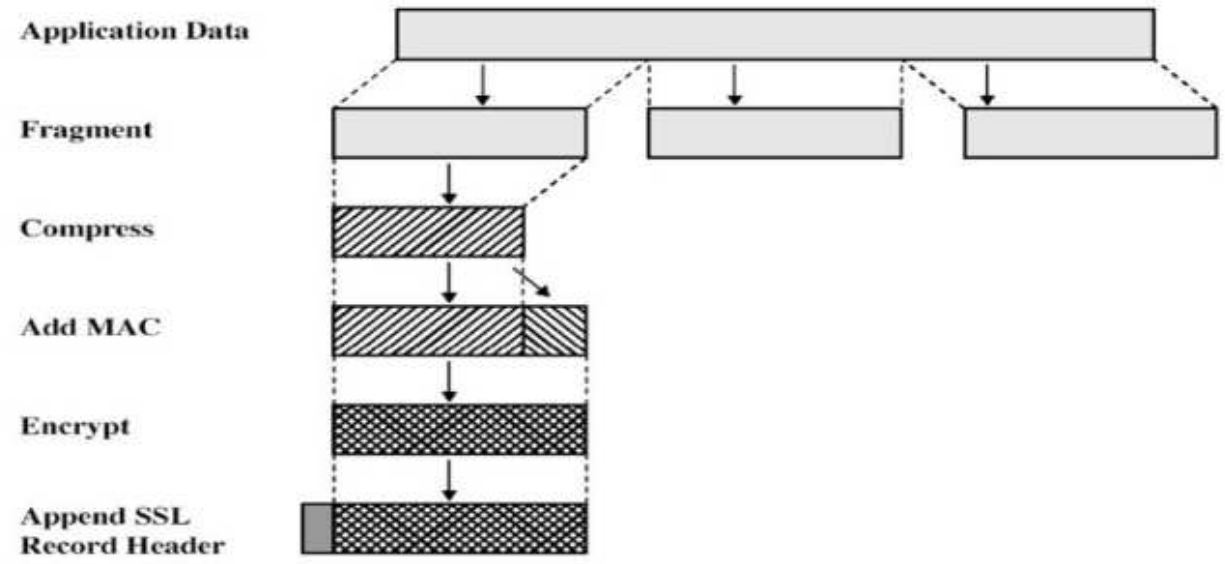


SSL Record Protocol:

SSL Record provides two services to SSL connection.

- Confidentiality
- Message Integrity

In the SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message Digest) is appended. After that encryption of the data is done and in last SSL header is appended to the data.



Conclusion :

Thus we have undestood how DHCP is working.

Questions:-

1.What Is The Dhcp Process For Client Machine?

2.List Some Benefits Of Using Dhcp?

3.What Is A Mac Address?

4.What Is Dhcp Spoofing?

Fig. 2 SSL Record Protocol Operation

Change Cipher Spec Protocol

This consists of a single message which consists of a single byte with the value 1. Thisis used to cause the pending state to be copied into the current state which updates thecipher suite to be used on this connection.

Alert Protocol

This protocol is used to convey SSL-related alerts to the peer entity. It consists of twobytes the first of which takes the values 1 (warning) or 2 (fatal). If the level is fatal SSLimmediately terminates the connection. The second byte contains a code that indicates the specific alert.

Handshake Protocol

This is the most complex part of SSL and allows the server and client to authenticateeach other and to negotiate an encryption and MAC algorithm and cryptographic keysto be used to protect data sent in an SSL record. This protocol is used before anyapplication data is sent. It consists of a series of messages exchanged by the client and server.

Each message has threefields:

1.Type (1 byte): Indicates one of 10 messages such as “hellorequest”

2.Length (3 bytes): The length of the message in bytes.

3.Content(≥0byte): The parameters associated with this message such version ofSSL being used.

The Handshake Protocol consists of four phases:

1.Establish security capabilities including protocol version, session ID, ciphersuite, compression method and initial random numbers. This phase consists ofthe clienthello and serverhello

messages which contain the following (this isfor the client however it’s a little different for the server):

Version: The highest SSL version understood by client

Random: 32-bit timestamp and 28 byte nonce.

Session ID: A variable length session identifier.

CipherSuite: List of cryptoalgorithms supported by client in decreasing or-der of preference. Both key exchange and CipherSpec (this includes fieldssuch as CipherAlgorithm, MacAlgorithm, CipherType, HashSize, Key Ma-terial and IV Size) are defined.

Compression Method: List of methods supported by client

2.Server may send certificate, key exchange, and request certificate it also signalsend of hello message phase. The certificate sent is one of a chain of X.509 cer-tificates discussed earlier in the course. The serverkey exchange is sent only ifrequired. A certificate may be requested from the client if needs be by certifi-caterequest.3.Upon receipt of the serverdone message, the client should verify that the serverprovided a valid certificate, if required, and check that the serverhello parame-ters are acceptable. If all is satisfactory, the client sends one or more messages back to the server. The client sends certificate if requested (if none available thenit sends a nocertificate alert instead). Next the client sends clientkeyexchangemessage . Finally, the client may send certificate verification.4.Change cipher suite and finish handshake protocol. The secure connection isnow setup and the client and server may begin to exchange application layer data.

Handsahke Protocol Action:-

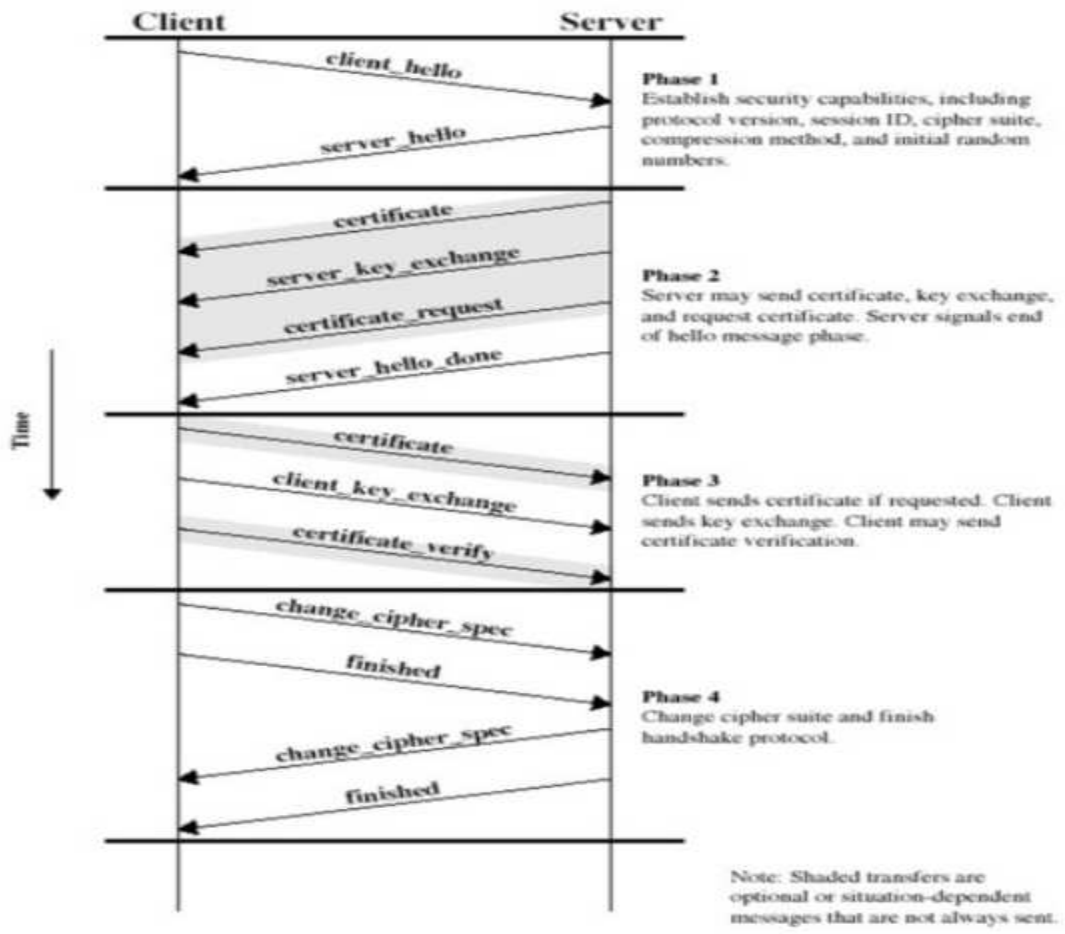


Fig 3. Handshake Protocol

Conclusion :

Understands SSL protocol

Question:

Q. 1. Enlist all the protocols in SSL

Q. 2. How Handshake protocol ? Explain with suitable diagram.

Reference:

http://www.facweb.iitkgp.ac.in/~sourav/SSL.pdf