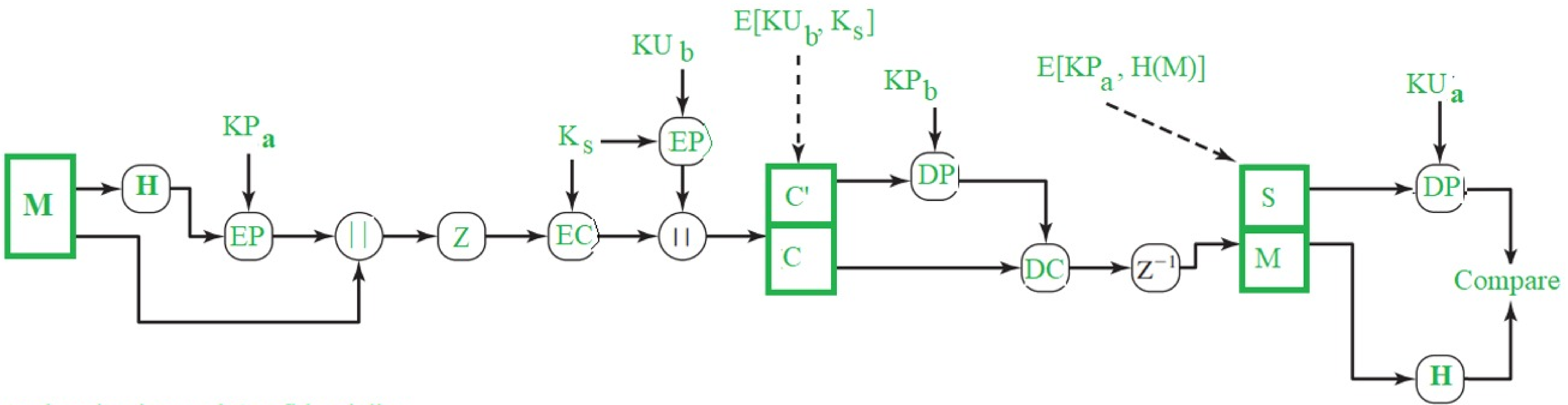
PGP

- PGP stands for Pretty Good Privacy (PGP) which is invented by Phil Zimmermann.
- PGP was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email.
- PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication, and non-repudiation. PGP uses a combination of secret key encryption and public key encryption to provide privacy. Therefore, we can say that the digital signature uses one hash function, one secret key, and two private-public key pairs.
- PGP is an open source and freely available software package for email security.
- PGP provides authentication through the use of Digital Signature.
- It provides confidentiality through the use of symmetric block encryption.
- It provides compression by using the ZIP algorithm, and EMAIL compatibility using the radix-64 encoding scheme.

Following are the steps taken by PGP to create secure e-mail at the sender site:

- The e-mail message is hashed by using a hashing function to create a digest.
- The digest is then encrypted to form a signed digest by using the sender's private key, and then signed digest is added to the original email message.
- The original message and signed digest are encrypted by using a one-time secret key created by the sender.
- The secret key is encrypted by using a receiver's public key.
- Both the encrypted secret key and the encrypted combination of message and digest are sent together.



Authentication and Confidentiality

Introduction of SSL

❑ SSL is developed by Netscape Communication.

❑ ***SSL*** stands for *"**S**ecure **S**ocket **L**ayer".*

❑ **What is SSL?**

- SSL is a protocol for establishing secure links between networked computers.

❑ **Purpose of SSL**

- SSL provides *confidentiality*, *authentication* and *data integrity* in internet communication.
- SSL is the predecessor to the modern TLS encryption used today.

Introduction of SSL

❑ What is an SSL Certificate?

- An SSL certificate is a bit of code on your web server that **provides security for online communications**

HTTP
+
SSL
=
HTTPS
SSL

User

Insecure Connection

Normal HTTP

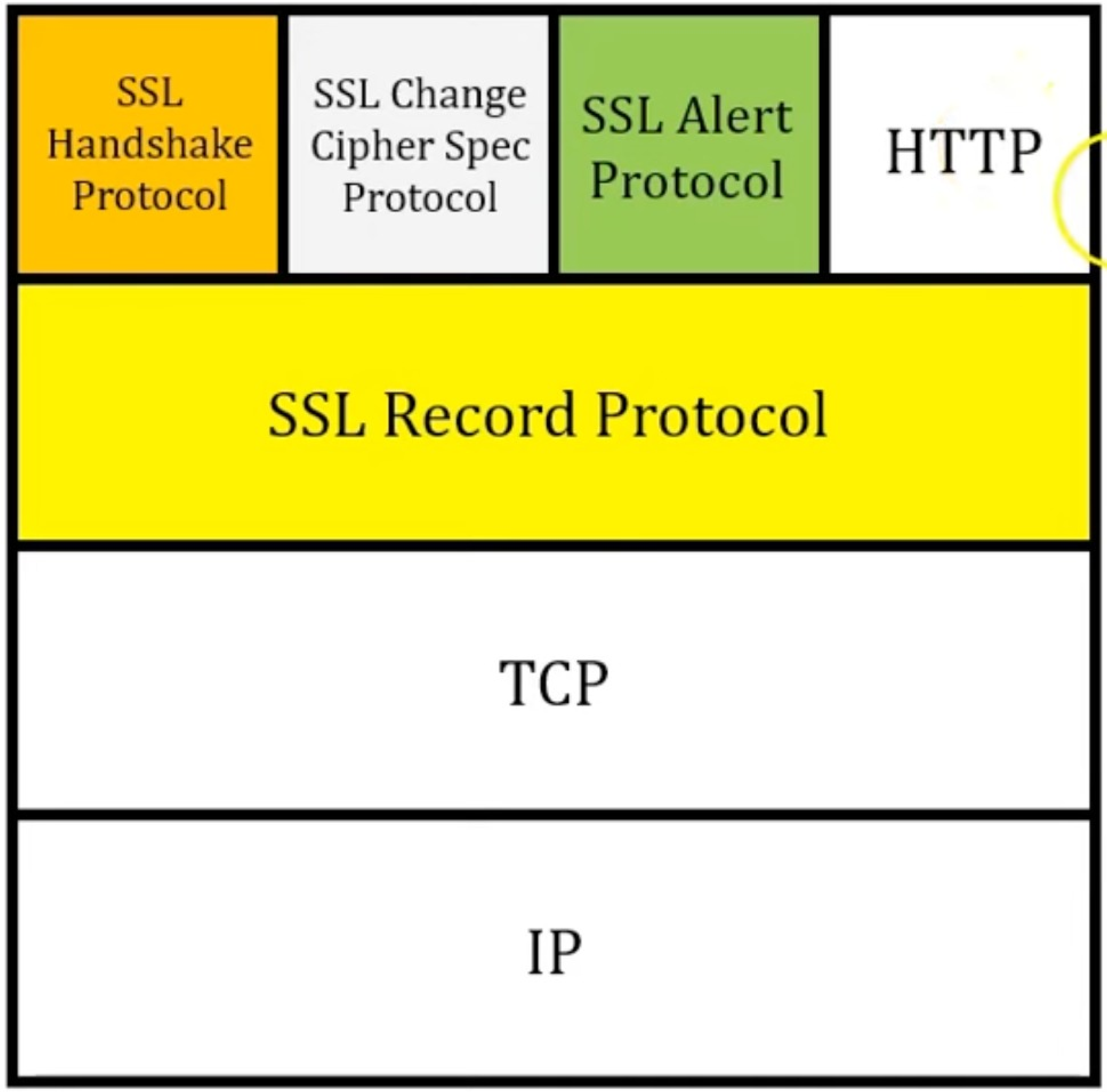
User

Encrypted Connection

Secure HTTPS

SSL Architecture

- **SSL Handshake Protocol:** Connection establishment.
- **SSL Change Spec Protocol:** Use of required cipher techniques for data encryption.
- **SSL Alert Protocol:** alert (warning, error if any) generation.
- **SSL Record Protocol:** encrypted data transmission and encapsulation of the data sent by the higher layer protocols.



SSL Architecture

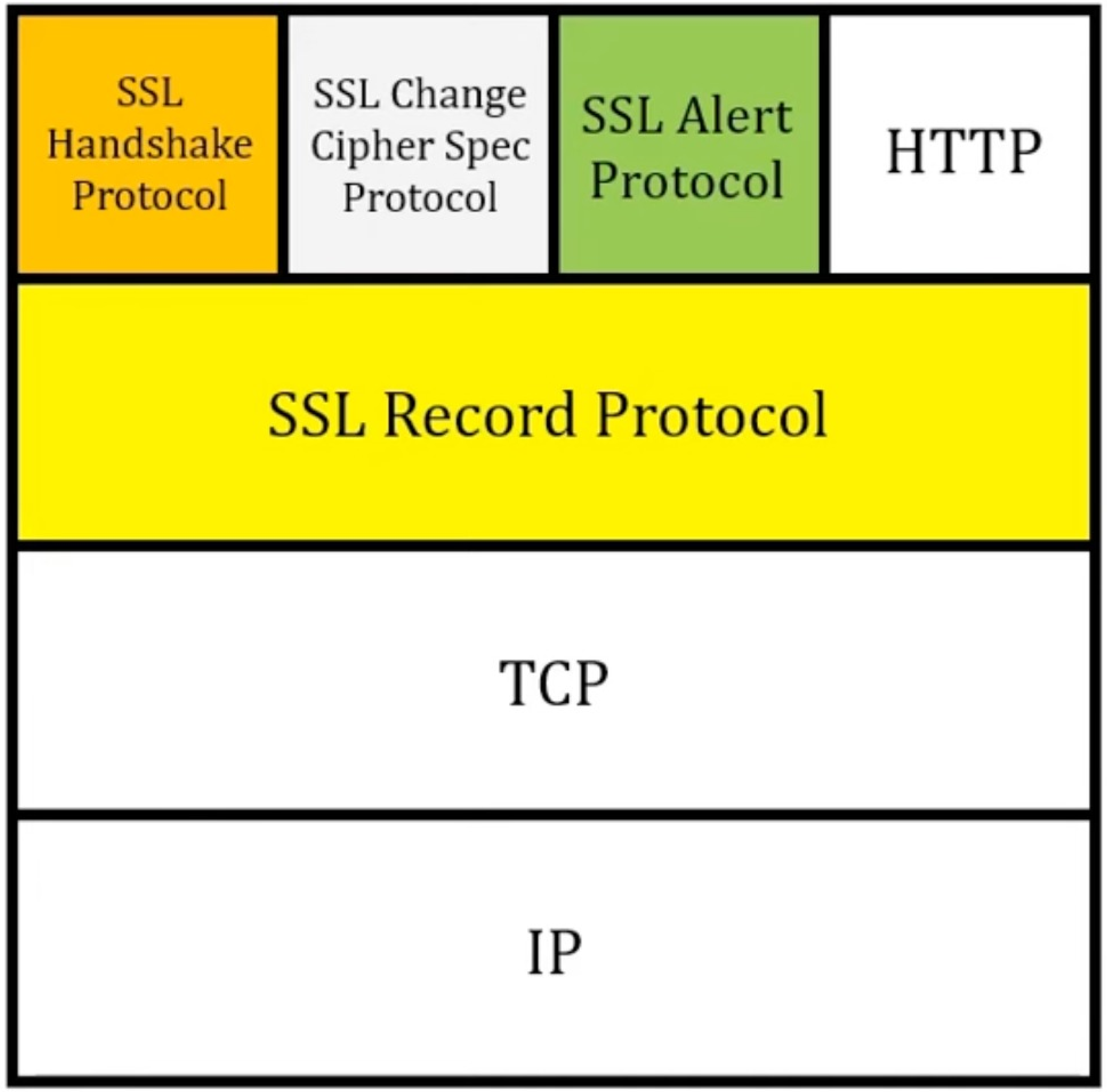
- Two important SSL concepts are the SSL Connection and the SSL Session.

❑ SSL Connection:

- It is a transport that provides a suitable type of service.
- Each connection is *associated* with one *SSL session.*

❑ SSL Session:

- It is a set of cryptographic security parameters which can be shared among multiple *SSL connections*.
- An SSL session is an *association* between a client and a server.



SSL Protocols

❑ SSL has 4 protocols:

- SSL Handshake Protocol
- SSL Change Cipher Spec Protocol
- SSL Alert Protocol

}– **SSL Higher Layer Protocol**

- SSL Record Protocol – **SSL Lower Layer Protocol**

SSL Handshake Protocol

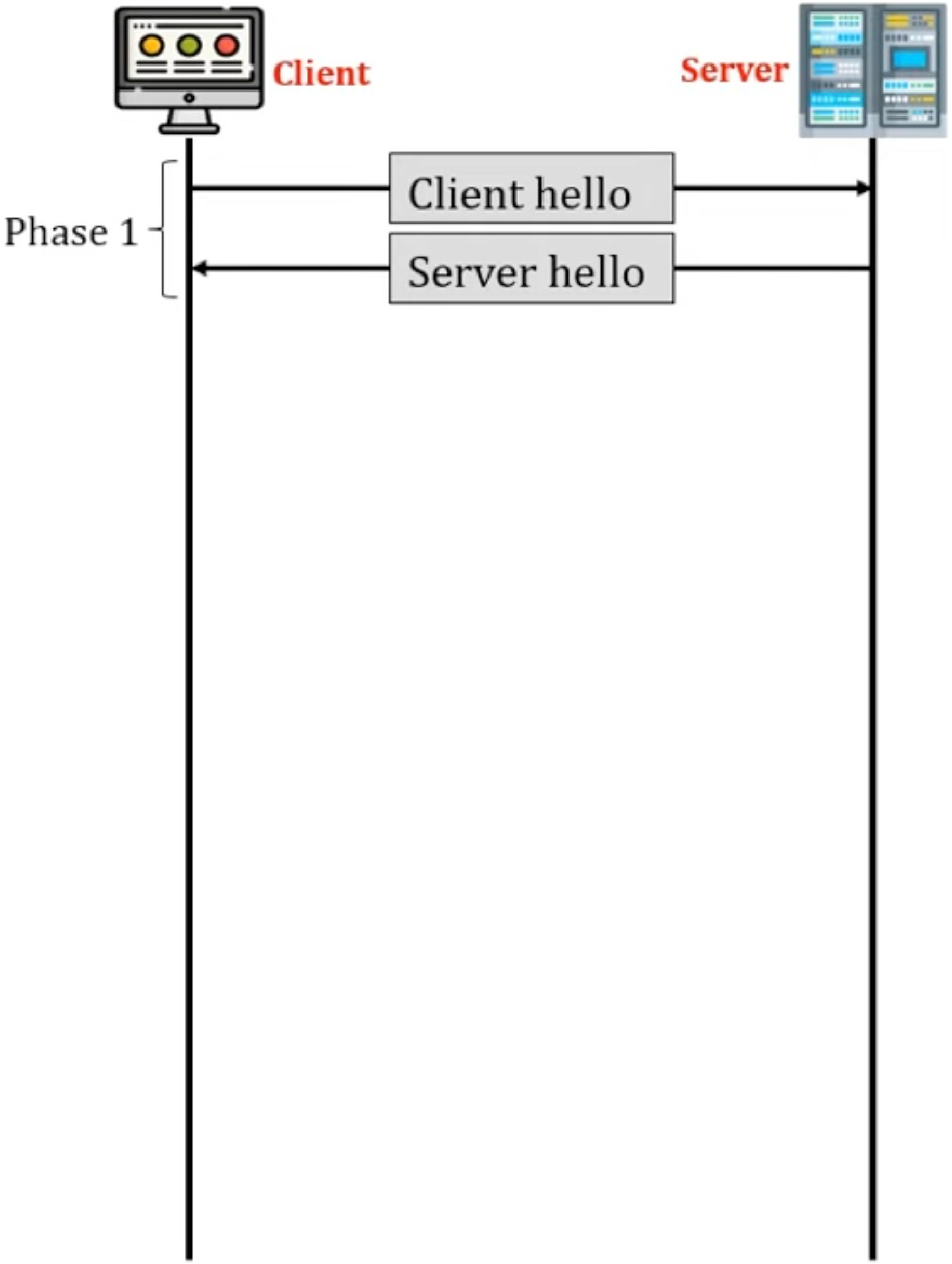
❑ Phase 1: Establishing security capabilities

1. Client Hello:

1. The highest SSL version number which the client can support.
2. A session ID that defines the session.
3. There is a cipher suite parameter that contains the entire cryptographic algorithm which supports client's system.
4. A list of compression methods that can be supported by client system.

2. Server Hello:

1. The highest SSL version number which the server can support.
2. A session ID that defines the session.
3. A cipher suite contains the list of all cryptographic algorithms that is sent by the client which the server will select the algorithm.
4. A list of compression method sent by the client from which the server will select the method.



SSL Handshake Protocol

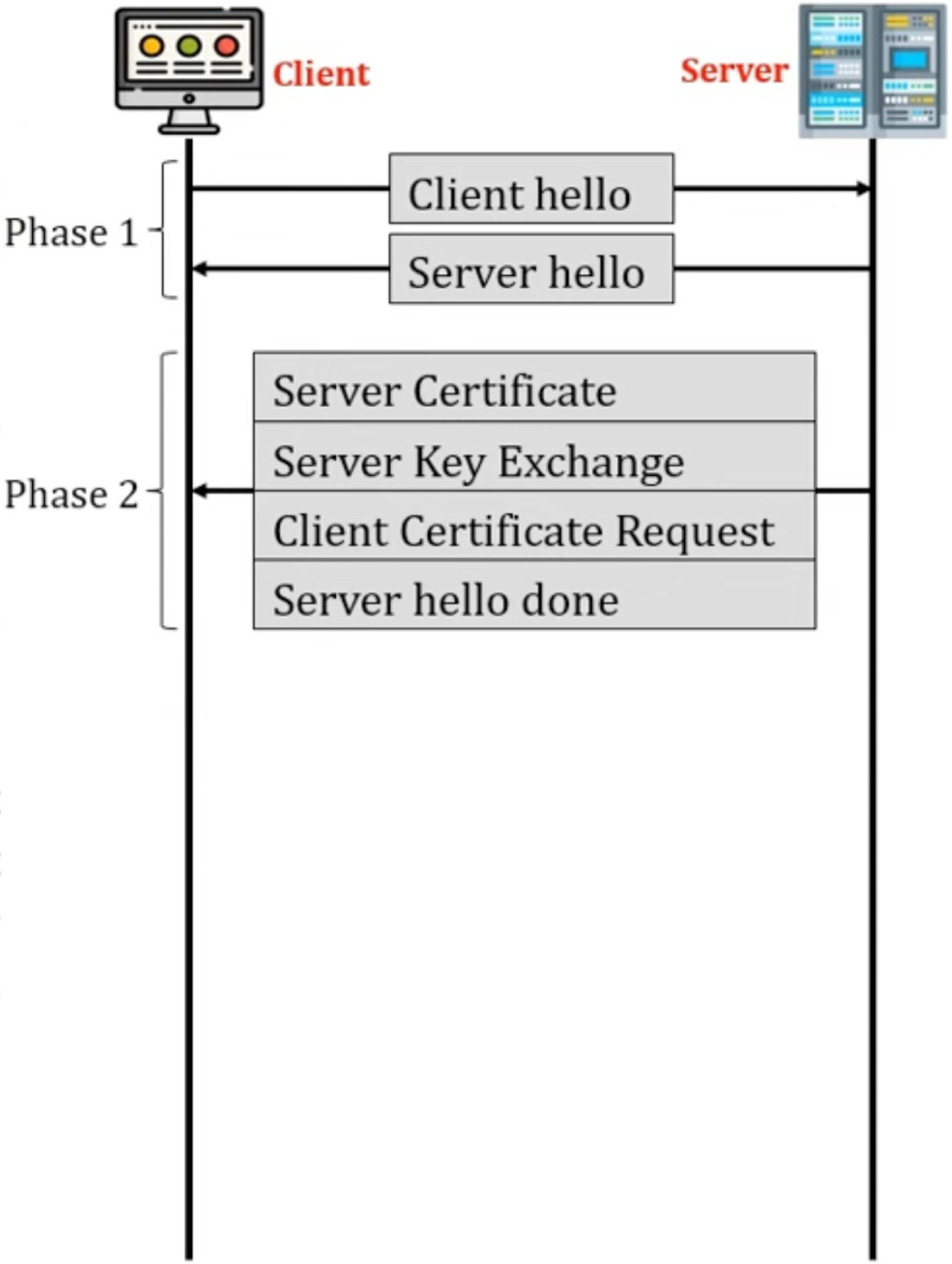
❑ Phase 2: Server Authentication and Key Exchange

- **Certificate:** The server sends a certificate message to authentication itself to the client. If the key exchange algorithm is Diffie-Hellman than no need of authentication.

- **Server key exchange:** This is optional. It is used only if the server doesn't sends its digital certificate to client.

- **Certificate Request:** The server can request for the digital certificate of client. The client's authentication is optional.

- **Server Hello done:** The server message hello done is the last message in phase 2, this indicates to the client that the client can now verify all the certificates received by the server. After this hello message done, the server waits for the client side response in phase 3.



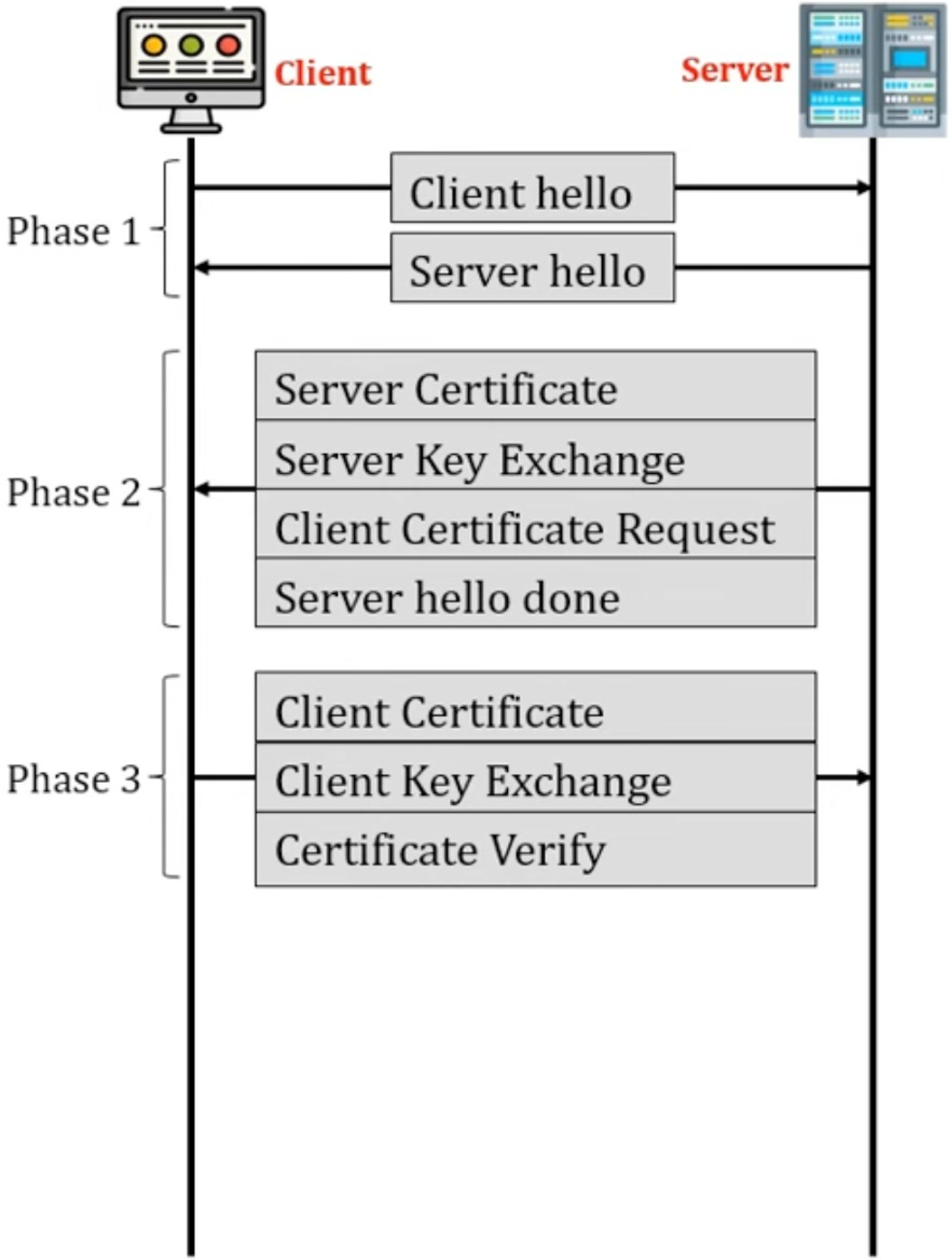
SSL Handshake Protocol

❑ Phase 3: Client Authentication and Key Exchange

1. **Client Certificate:** It is optional, it is only required if the server had requested for the client's digital certificate. If client doesn't have certificate it can be send no certificate message. Then it is upto server's decision whether to continue with the session or to abort the session.

2. **Client key exchange:** The client sends a client key exchange, the contents in this message are based on key exchange algorithms between both the parties.

3. **Certificate Verify:** It is necessary only if the server had asked for client authentication. The client has already sent its certificate to the server. Bit additionally if server wants then the client has to prove that it is authorized holder of the private key. The sever can verify the message with its public key already sent to ensure that the certificate belongs to client.



SSL Handshake Protocol

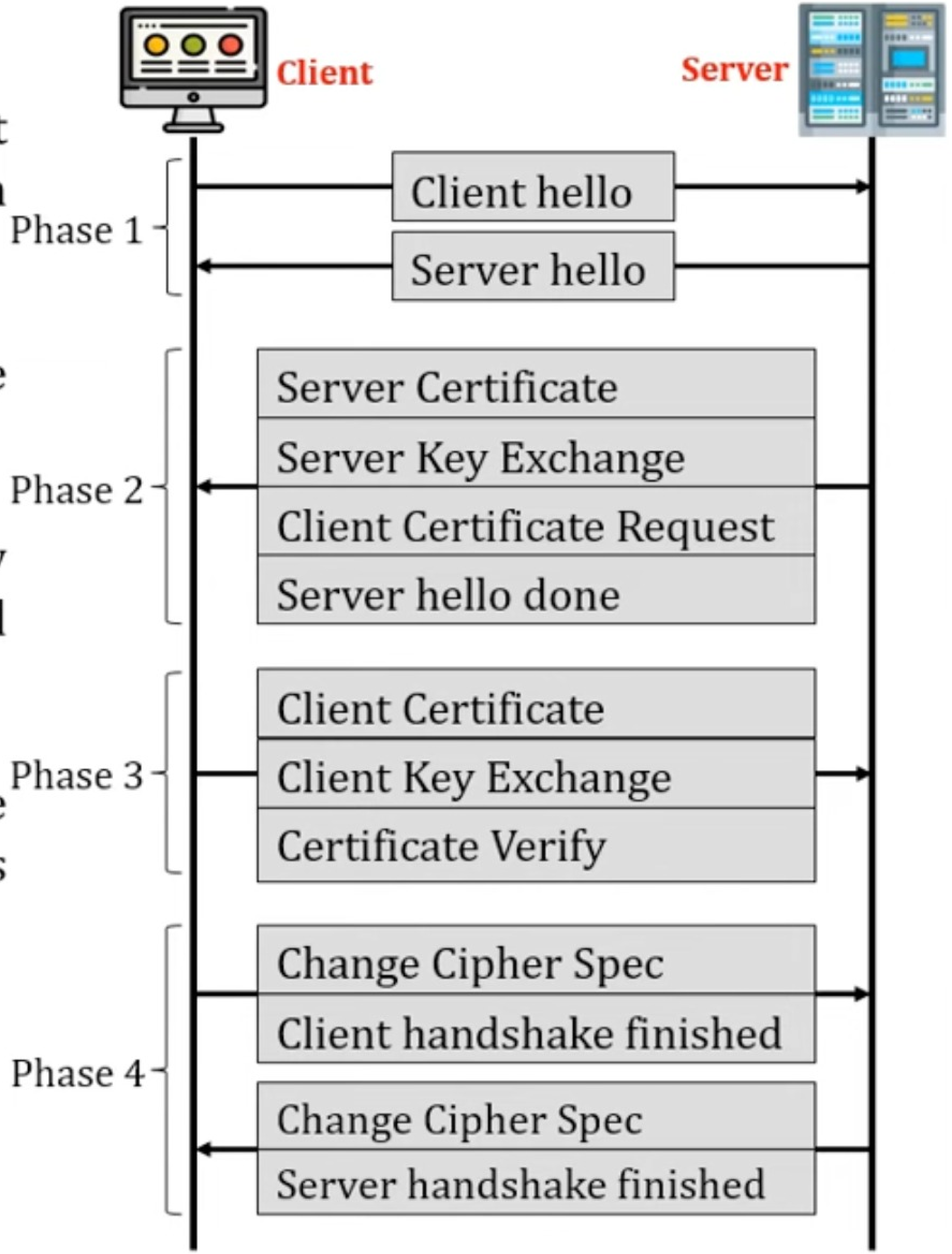
❑ Phase 4: Finish

1. **Change cipher spec:** It is a client side messages telling about the current status of cipher protocols and parameters which has been made active from pending state.

2. **Finished:** This message announce the finish of the handshaking protocol from client side.

3. **Change cipher spec:** This message is sent by server to show that it has made all the pending state of cipher protocols and parameters to active state.

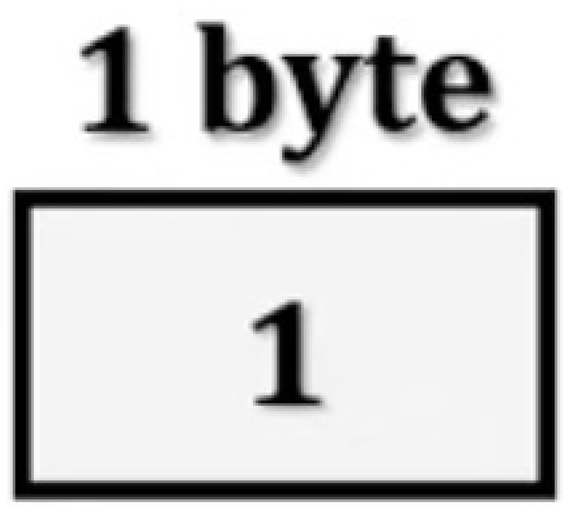
4. **Finished:** This message announce the finish of the handshaking protocol from server and finally handshaking is totally completed.



SSL Change Cipher Spec Protocol

- SSL Change Cipher Spec Protocol is upper layer protocol.

- It is the simplest protocol.



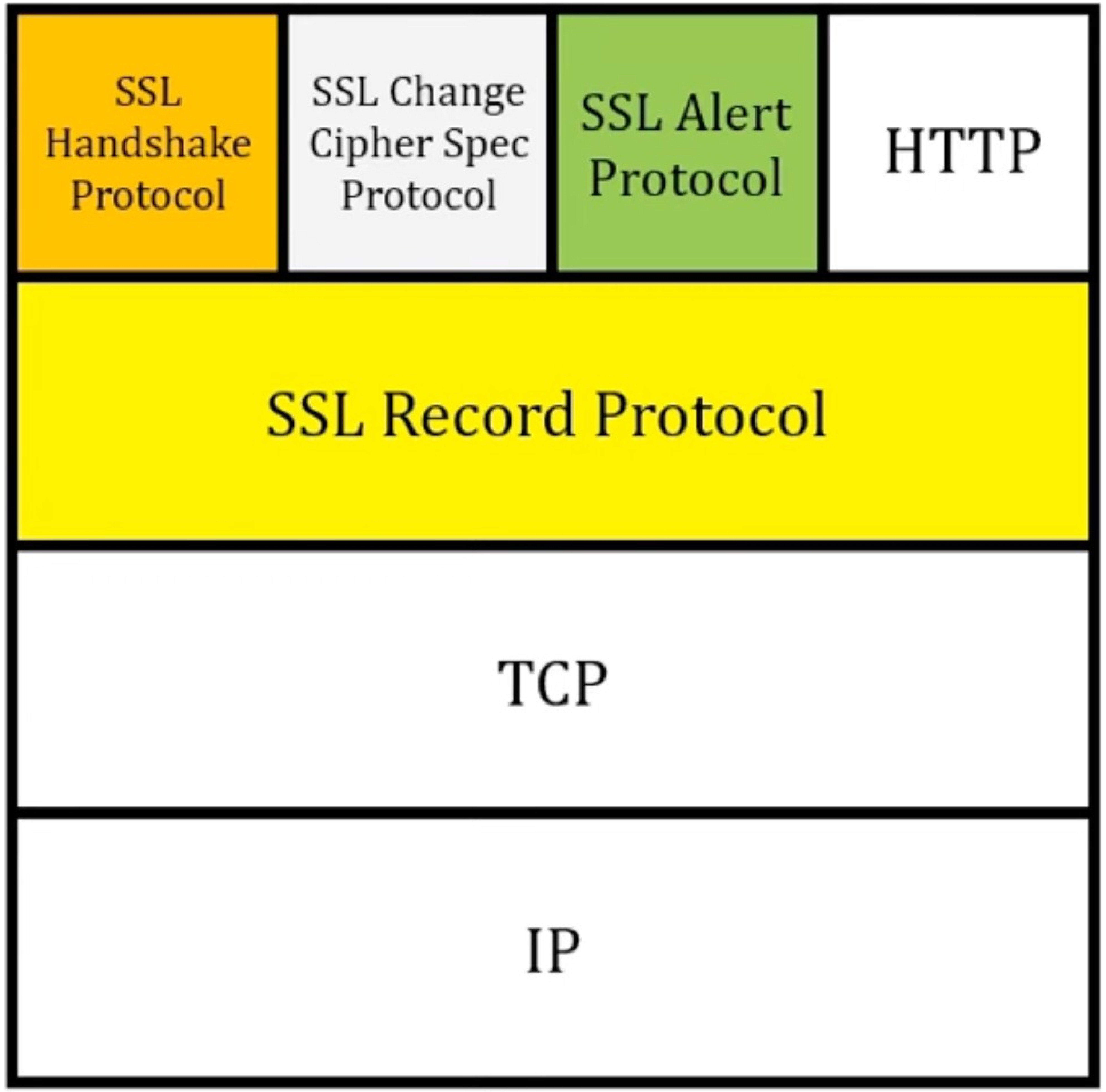
1 byte

1

- This protocol consist of only single byte with value “1”, as shown in figure.

- It consist of single message only.

- It copies pending state to current state, which updates the cipher suite to be used to this connection.



SSL Handshake Protocol

SSL Change Cipher Spec Protocol

SSL Alert Protocol

HTTP

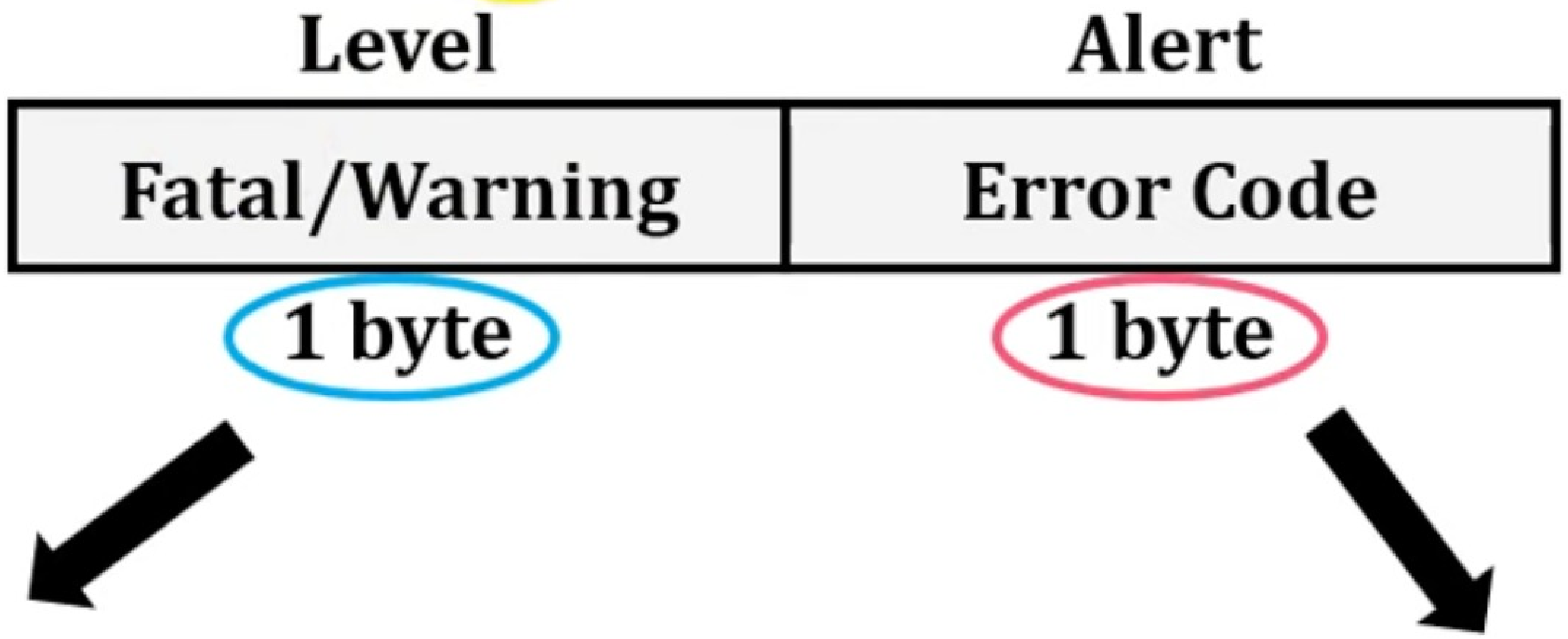
SSL Record Protocol

TCP

IP

SSL Alert Protocol

- Figure Shows Alert Protocol Format



Level	Alert
Fatal/Warning	Error Code
1 byte	1 byte

First “1 byte”: Either “1” or “2”
1 → Warning
2 → Fatal Error

Second “1 byte”: Predefined “Error Code”

SSL Alert Protocol

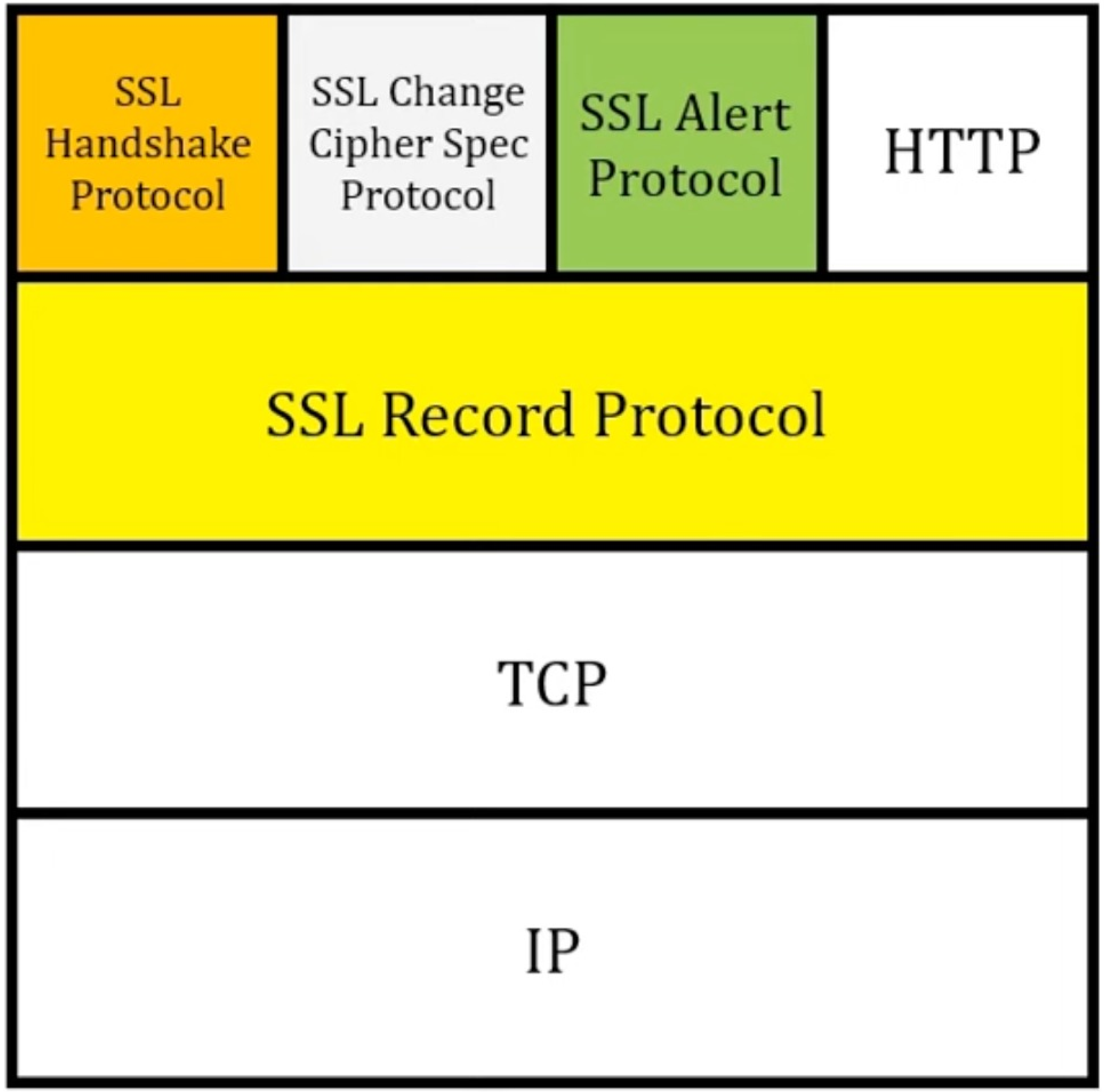
Alert Code	Alert Message	Description
0	close_notify	No more message from sender.
10	unexpected_message	An incorrect message received.
20	bad_record_mac	A wrong MAC received.
30	decompression_failure	Unable to decompress.
40	handshake_failure	Unable to finalize handshake by the sender.
42	bad_certificate	Received a corrupted certificate.
42	No_certificate	Client has no certificate to send to server.
42	certificate_expired	Certificate has expired.

SSL Record Protocol

- SSL Record Protocol is second sub level protocol.

- It also called as lower level protocol.

- SSL Record Protocol provides following services:
  - Encrypted Data Transmission
  - Encapsulation of data
  - Data Confidentiality
  - Data Integrity



SSL Handshake Protocol

SSL Change Cipher Spec Protocol

SSL Alert Protocol

HTTP

SSL Record Protocol

TCP

IP