I had trouble creating an SSL trace, so I used the one provided.

1.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Frame | Source | Destination | Time | SSL Count | SSL Type |
| 106 | 128.238.38.162 | 216.75.194.220 | 21.805705 | 1 | Client Hello |
| 108 | 216.75.194.220 | 128.238.38.162 | 21.830201 | 1 | Server Hello |
| 111 | 216.75.194.220 | 128.238.38.162 | 21.853520 | 2 | Certificate, Server Hello Done |
| 112 | 128.238.38.162 | 216.75.194.220 | 21.876168 | 3 | Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message |
| 113 | 216.75.194.220 | 128.238.38.162 | 21.945667 | 2 | Change Cipher Spec, Encrypted Handshake Message |
| 114 | 128.238.38.162 | 216.75.194.220 | 21.954189 | 1 | Application Data |
| 122 | 216.75.194.220 | 128.238.38.162 | 23.480352 | 1 | Application Data |
| 149 | 216.75.194.220 | 128.238.38.162 | 23.559497 | 1 | Application Data |

Client: 128.238.38.162

Oldest

Server: 216.75.194.220

2.

Server

Client

Content Type: 1 byte

Version: 2 bytes

Newest

Length: 2 bytes

**ClientHello Record:**

Graphical user interface, text, application

Description automatically generated

3.

The content type value in the Client Hello record is SSLv2 Record Layer, this means that SSLv2 protocol is being used for this handshake.

4.

Yes, it does contain a nonce(challenge).

66 df 78 4c 04 8c d6 04 35 dc 44 89 89 46 99 09

5.

Cipher Spec: TLS\_RSA\_WITH\_RC4\_128\_MD5 (0x000004)

Public-Key Algorithm: RSA

Symmetric-Key Algorithm: RC4-128

Hash Algorithm: MD5

**ServerHello Record:**

Graphical user interface, text, application

Description automatically generated

6.

Yes, it does have a chosen cipher suite.

Cipher Suite: TLS\_RSA\_WITH\_RC4\_128\_MD5 (0x0004)

Public-Key Algorithm: RSA

Symmetric-Key Algorithm: RC4-128

Hash Algorithm: MD5

7.

Random: 0000000042dbed248b8831d04cc98c26e5badc4e267c391944f0f070ece57745

Yes, it does include a nonce. It is a 32-byte value.

The purpose of the client and server nonces in SSL are to use them to establish a shared secret key that can then be used for the subsequent communication between them. The nonces are generated to be unique to that interaction as a random generated value and they are used so that the communication is not vulnerable to a replay attack.

8.

Session ID: 1bad05faba02ea92c64c54be4547c32f3e3ca63d3a0c86ddad694b45682da22f

Yes, it does include a session ID. The purpose of the session ID is to enable the client and server to resume a previous session. When the client initiates a new session it can then include the session ID in the Client Hello message and if the server has the matching session ID then the session can be resumed. This helps to save time and resources by avoiding having to re-complete the SSL handshake.

9.

Graphical user interface, text, application, email

Description automatically generated

The certificate is included in a separate record in this case, the record is “Certificate, Server Hello Done”. This certificate does fit into a single Ethernet frame in this case, this usually depends on the MTU of the network and the size of the certificate, but this certificate fits into one frame. This certificate has a length of 2687 in the packet.

**Client Key Exchange Record:**

Graphical user interface, text, application, email

Description automatically generated

10.

This record does contain a pre-master secret. The secret is used to establish the shared secret key between the client and the server to subsequently encrypt data exchanged between them. It is encrypted using RSA encryption. The length of the pre-master secret is 128 bytes.

Encrypted PreMaster: bc49494729aa2590477fd059056ae78956c77b12af08b47c609e61f104b0fbf83e41c08d…

**Change Cipher Spec Record (sent by client) and Encrypted Handshake Record:**

**Graphical user interface, application, Word

Description automatically generated**

11.

The Change Cipher Spec record’s purpose is to signal a switch in the encryption algorithm used for the communication between the client and the server. This message informs the other party that any further data will be encrypted with a different key than was previously being used. This is usually done during the handshake process once the client and server agree on what encryption algorithms will be used. In this record trace, just the Change Cipher Spec record has a length of 1 byte.

12.

The record is encrypted and contains a series of handshake messages using the established session key. It is encrypted so we do not know the exact contents but most likely contained is the server’s certificate, cryptographic parameters such as the algorithm being used, and any other optional handshake messages between the client and server such as a client key exchange method. The handshake message is encrypted using the session keys that are used to generate a symmetric encryption key using an encryption method such as AES. The length of the Encrypted Handshake Message is 56 bytes which means that there are multiple handshake messages that have been encrypted using the established session key.

13.

Yes, the server also sends a Change Cipher Spec record and a Handshake Message to the client during the handshake process. The Change Cipher Spec record sent by the server has the same format as the one sent by the client so those do not differ other than being sent by the server instead of the client. The Handshake Message is in the same format as well containing the handshake messages that are encrypted using the established session key. The encryption format will be the same as the client record, the only difference is that the handshake messages contained will be different since it is coming from the server not the client. Even though they are pretty much the same, it is necessary to ensure that the same encryption parameters are being used by both parties to have secure communication.

**Bonus Question:**

Graphical user interface, text, application, email

Description automatically generated

(1)

The key exchange is using TLSv1.2 as the protocol and starts with the Client Hello message then continues similarly compared the previous SSL examples above. There is the Server Hello packet, Certificate, Server Key Exchange, Server Hello Done packet where the server sends the certificate to the client(me). Then the Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message packet from the client to the server followed by the same packet coming from the server later on in packet number 9128.



(2)

Yes a digital certificate was used and it was the digital certificate of the server.

Graphical user interface, text, application

Description automatically generated