**Question 1:**

For each of the first 8 Ethernet frames (after you apply SSL filter, i.e., frame 106), specify 1) the frame number, 2) frame source (client or server), determine the number of SSL records that are included in the frame, and list the SSL record types that are included in the frame.

**Hint:** You may need to see the details of each frame.

|  |  |  |  |
| --- | --- | --- | --- |
| Frame No. | Source | No. of SSL Records | Record Type |

|  |  |  |  |
| --- | --- | --- | --- |
| **Frame No.** | **Source** | **No. of SSL Records** | **Record Type** |
| 106 | 128.238.38.162 | 1 | Client Hello (SSLv2) |
| 108 | 216.75.194.220 | 1 | Server Hello (SSLv3) |
| 111 | 216.75.194.220 | 2 | Certificate (SSLv3)  Server Hello Done (SSLv3) |
| 112 | 128.238.38.162 | 3 | Client Key Exchange (SSLv3)  Change Cipher Spec (SSLv3)  Encrypted Handshake Message (SSLv3) |
| 113 | 216.75.194.220 | 2 | Change Cipher Spec (SSLv3)  Encrypted Handshake Message (SSLv3) |
| 114 | 128.238.38.162 | 1 | http-over-tls (SSLv3) |
| 122 | 216.75.194.220 | 1 | http-over-tls (SSLv3) |
| 149 | 216.75.194.220 | 1 | http-over-tls (SSLv3) |

**Question 2:**

Draw a timing diagram between client and server, with one arrow for each SSL record. (You can upload a picture of your drawing)

A piece of paper with writing on it

Description automatically generated with medium confidence

**Question 3:**

Answer the following questions about **ClientHello**:

Locate the ClientHello Record. Does the ClientHello record contain a nonce (also known as a "challenge")? If so, what is the value of the challenge in hexadecimal notation?

**Hint:** Pick any ClientHello frame that you see, i.e., frame 106. You may need to print the raw information by adding option –T jsonraw to the command, which will print the details in JSON with some raw information in hexadecimal.

*Answer:*

Yes, it does contain Challenge.

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

**Question 4:**

Answer the following questions about **ClientHello**:

Does the ClientHello record advertise the cyber suites it supports? If so, in the first listed suite, what are the public-key algorithm, the symmetric-key algorithm, and the hash algorithm?

**Answer:**

Yes, the Client Hello record advertise the Cyber Suits it supported.

Text

Description automatically generatedPublic-key Algorithm:

* RSA

Symmetric-key Algorithm:

* RC4

Hash Algorithm:

* MD5

**Question 5:**

Answer the following questions about **ServerHello**:

Locate the **ServerHello**SSL Record. Does this record specify a chosen cipher suite? What are the algorithms in the chosen cipher suite?

**Answer:**

Yes, the chosen cipher Suite is TLS\_RSA\_WITH\_RC4\_128\_MD5

Graphical user interface, text, application, email

Description automatically generated

**Question 6:**

Answer the following questions about **ServerHello**:

Does this **ServerHello** record include a nonce? If so, how long is it? What is the purpose of the client and server nonces in SSL?

**Answer text**

**Question 7:**

Does this **ServerHello** record include a session ID? What is the purpose of the session ID?

**Question 8:**

Does this **ServerHello** record contain a certificate, or is the certificate included in a separate record. Does the certificate fit into a single Ethernet frame?

**Question 9:**

Answer the following questions about encryption:

Locate the Client key exchange record. Does this record contain a pre-master secret? What is this secret used for? Is the secret encrypted? If so, how? How long is the encrypted secret?

**Question 10:**

What is the purpose of the **Change Cipher Spec** **record** (sent by client)? How many bytes is the record in your trace?

**Question 11:**

In the **Encrypted handshake record**, what is being encrypted? How?

**Question 12:**

Does the **Server** also send a **Change cipher record** and an **Encrypted hand shake record** to the client? How are those records different from those sent by the client?

**Question 13:**

How is the Application Data being encrypted? Do the records containing application data include a MAC? Does TShark distinguish between the encrypted application data and the MAC?