**Tevin Jeffrey**

**Wireshark Lab 8**

**1. For each of the first 8 Ethernet frames, specify the source of the frame (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. Draw a timing diagram between client and server, with one arrow for each SSL record.**

**2. Each of the SSL records begins with the same three fields (with possibly different values). One of these fields is “content type” and has length of one byte. List all three fields and their lengths.**

**ClientHello Record:**

**3. Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?**

**4. Does the ClientHello record contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?**

**5. 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?**

**ServerHello Record:**

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

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

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

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

**Client Key Exchange Record:**

**10. 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?**

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

**11. What is the purpose of the Change Cipher Spec record? How many bytes is the record in your trace?**

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

**13. Does the server also send a change cipher record and an encrypted handshake record to the client? How are those records different from those sent by the client?**

**Application Data**

**14. How is the application data being encrypted? Do the records containing application data include a MAC? Does Wireshark distinguish between the encrypted application data and the MAC?**

**15. Comment on and explain anything else that you found interesting in the trace.**