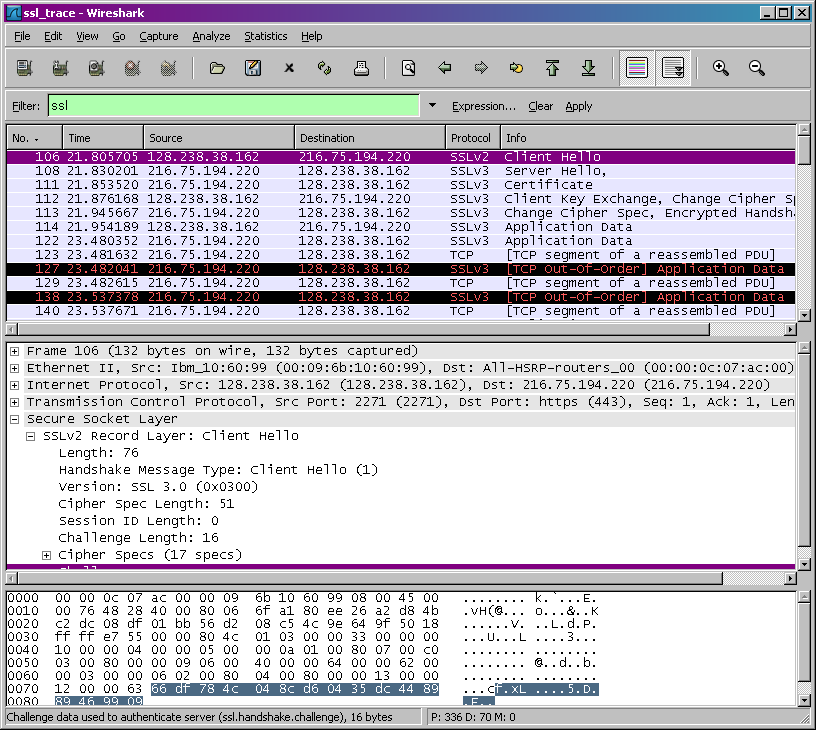
|  |  |
| --- | --- |
| Wireshark Lab:  SSL v8.0  Supplement to *Computer Networking: A Top-Down Approach, 8th ed.,* J.F. Kurose and K.W. Ross  *“Tell me and I forget. Show me and I remember. Involve me and I understand.”* Chinese proverb  © 2005-2020, J.F Kurose and K.W. Ross, All Rights Reserved | *A picture containing outdoor, water, bridge, building  Description automatically generated* |

In this lab, we’ll investigate the Secure Sockets Layer (SSL) protocol, focusing on the SSL records sent over a TCP connection. We’ll do so by analyzing a trace of the SSL records sent between your host and an e-commerce server. We’ll investigate the various SSL record types as well as the fields in the SSL messages. You may want to review Section 8.6 in the text[[1]](#footnote-1). We are currently developing a Wireshark Lab that will cover TLS – whose treatment in the 8th edition of our text replaces the coverage of SSL.



1. Capturing packets in an SSL session

The first step is to capture the packets in an SSL session. To do this, you should go to your favorite e-commerce site and begin the process of purchasing an item (but terminating before making the actual purpose!). After capturing the packets with Wireshark, you should set the filter so that it displays only the Ethernet frames that contain SSL records sent from and received by your host. (An SSL record is the same thing as an SSL message.) You should obtain something like screenshot on the previous page.

If you have difficulty creating a trace, you should download the zip file [http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip](http://gaia.cs.umass.edu/ethereal-labs/ethereal-traces.zip) and extract the *ssl-ethereal-trace-1* packet trace.

2. A look at the captured trace

Your Wireshark GUI should be displaying only the Ethernet frames that have SSL records. It is important to keep in mind that an Ethernet frame may contain one or more SSL records. (This is very different from HTTP, for which each frame contains either one complete HTTP message or a portion of a HTTP message.) Also, an SSL record may not completely fit into an Ethernet frame, in which case multiple frames will be needed to carry the record.

Whenever possible, when answering a question below, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout[[2]](#footnote-2) to explain your answer. To print a packet, use *File->Print*, choose *Selected packet only*, choose *Packet summary line,* and select the minimum amount of packet detail that you need to answer the question

Week 13 Questions

These are the questions from the lab. Put your answers on these pages using a contrasting font color. When you are finished, copy the answers to a separate document and submit it through the submission link.

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.

Diagram

Description automatically generated

1. 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.

Content Type = 1 byte  
   SSL Version = 2 bytes  
   Length = 2 bytes

ClientHello Record:

1. 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? 1
2. Does the ClientHello record contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?

66 df 78 4c 04 8c d6  05 35 dc 44 89 89 46 99 09.

1. 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? Yes, the Client displays its supported cyber suites.  The first listed suite is TLS\_RSA.  The symmetric , public and hash algorithms are RC4, 128 and MD5, respectively.

ServerHello Record:

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

 TLS\_RSA, the algorithms are RC4, 128 and MD5

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

It includes a nonce of 32 bits.  The purpose is thransmitted, the nonces will show that they are duplicates and should be ignored or the connection should be dropped.

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

Yes, session ID would prevent Trudy from inserting a false message across the connection

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

Yes,  Because the size of the certificate(2684 bytes) is larger than the maximum payload size of an Ethernet Frame (1500 bytes), the certificate must be contained in multiple frames

Client Key Exchange Record:

1. 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?

The Client Key record encrypts the Pre-Master Secret (PMS) with the server’s public key.  This is used to verify that both parties completely understand the encryption method that will be used in the further communication, which will all be encrypted.  The encrypted secret is 56 bytes.

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

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

The Change Cipher Spec record tells the other party what Cipher version to use for future encrypted data. The length is 1 byte

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

the client takes the PMS and encrypts it using the cipher agreement from the previous messages.

1. 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?

The server also sends the change cipher record and encrypted handshake. The PMS encryption should return the same handshake message, so there is no difference other than the clients Key Exchange Record.

Application Data

1. 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?

The application data is encrypted according to the server’s agreed on encryption method. Every message between client and server is accompanied with a Message Authentication Code (MAC).  Wireshark doesn’t distinguish this from the encrypted data.

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

Basicaclly, It helps those communications in the lab establish truest but using SSL

1. References to figures and sections for this SSL lab are for the 7th edition of our text, *Computer Networks, A Top-down Approach, 7th ed.,* J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2016. [↑](#footnote-ref-1)
2. What do we mean by “annotate”? If you hand in a paper copy, please highlight where in the printout you’ve found the answer and add some text (preferably with a colored pen) noting what you found in what you ‘ve highlight. If you hand in an electronic copy, it would be great if you could also highlight and annotate. [↑](#footnote-ref-2)