Name: Rutikesh Sawant

Batch: B2

Subject: CNS Lab

PRN: 2019BTECS00034

Assignment 17

Aim: To observe SSL/TLS (Secure Sockets Layer/ Transport Layer Security)in action. SSL/TLS is used to secure TCP connections, and it is widely used as part of the secure web: HTTPS is SSL over HTTP.

2 STEP 1: Open a Trace you should use a supplied trace file trace-ssl.pcap.
File → Open → open from folder containing file.

3 STEP 2: Inspect the Trace
Now we are ready to look at the details of some SSL messages. To begin, enter and apply a
display filter of ssl.This filter will help to simplify the display by showing only SSL and TLS
messages. It will exclude other TCP segments that are part of the trace, such as Acks and
connection open/close. Select a TLS message somewhere in the middle of your trace for
which the Info field reads Application Data, and expand its Secure Sockets Layer block(by

using triangular icon on left side). Application Data is a generic TLS message carrying
contents for the application, such as the web page. It is a good place for us to start looking
at TLS messages. Look for the following protocol blocks and fields in the message

• The lower layer protocol blocks are TCP and IP because SSL runs on top of TCP/IP.

• The SSL layer contains a TLS Record Layer. This is the foundational sublayer for TLS. All messages contain records. Expand this block to see its details.

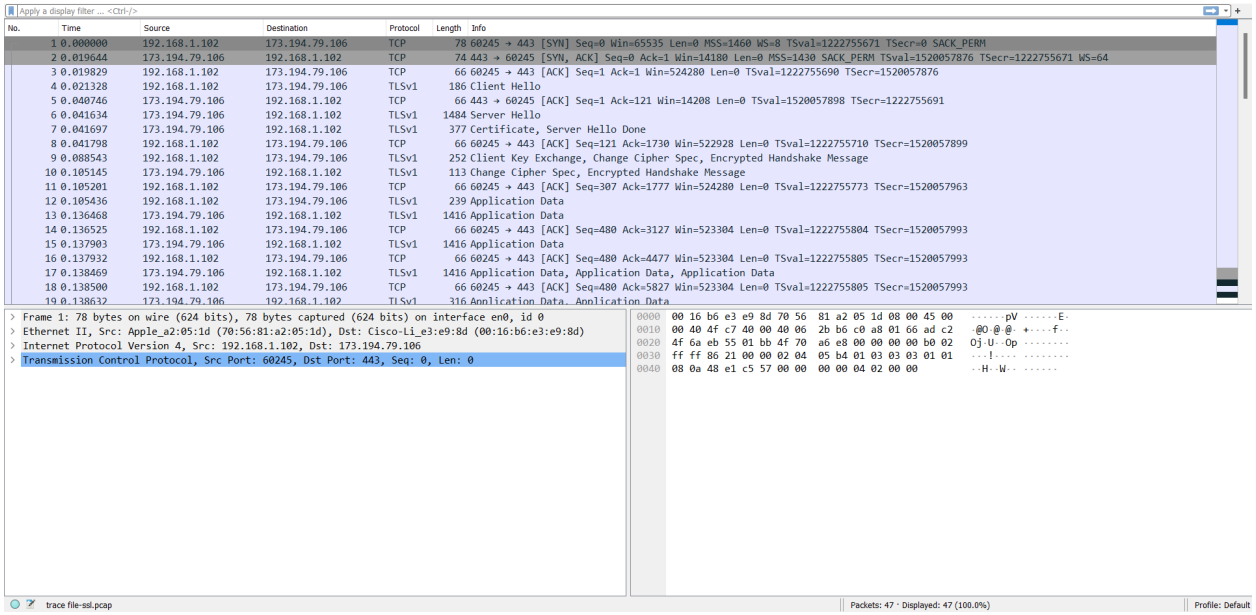
• Each record starts with a Content Type field. This tells us what is in the contents of the record. Then comes a Version identifier.It will be a constant value for the SSL
connection.

• It is followed by a Length field giving the length of the record.

• Last comes the contents of the record. Application Data records are sent after SSL has secured the connection, so the contents will show up as encrypted data.

Note that, unlike other protocols we will see such as DNS, there may be multiple records in
a single mes-sage. Each record will show up as its own block. Look at the Info column, and
you will see messages with more than one block.

Answer the following questions to show your understanding of SSL records:



1. What is the Content Type for a record containing Application Data?:

Content Type: Hanshake(22)

2. What version constant is used in your trace, and which version of TLS does it represent?

Version : 1.0 (0x0301)

4 Step 3: The SSL Handshake

An important part of SSL is the initial handshake that establishes a secure connection.

The handshake proceeds in several phases. There are slight differences for different

versions of TLS and depending on the encryption scheme that is in use. The usual outline

for a brand new connection is:

• Client (the browser) and Server(the web server) both send their Hellos

• Server sends its certificate to Client to authenticate (and optionally asks for Client

Certificate)

• Client sends keying information and signals a switch to encrypted data.

• Server signals a switch to encrypted data.

• Both Client and Server send encrypted data.

• An Alert is used to tell the other party that the connection is closing. Note that there is also a mechanism to resume sessions for repeat connections between the same

client and server to skip most of steps b and c.

4.1 Hello Message

Find and inspect the details of the Client Hello and Server Hello messages, including

expanding the Hand- shake protocol block within the TLS Record. For these initial

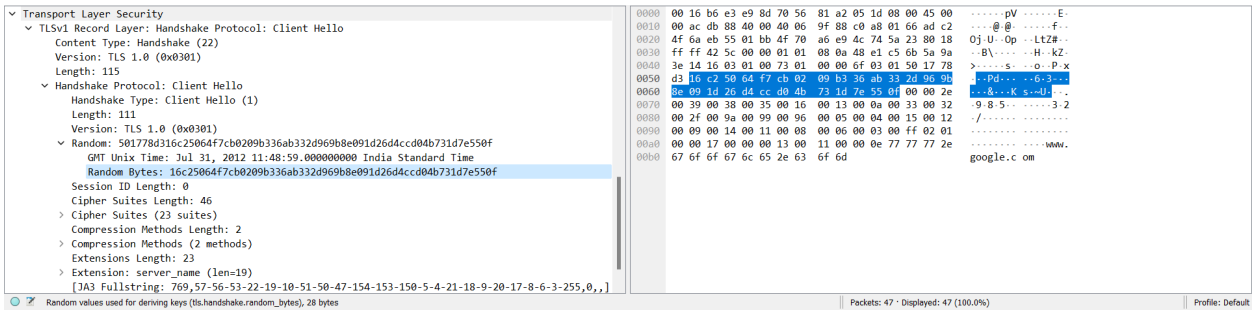
messages, an encryption scheme is not yet established so the contents of the record are

visible to us. They contain details of the secure connection setup in a Handshake protocol format.

Answer the following questions.

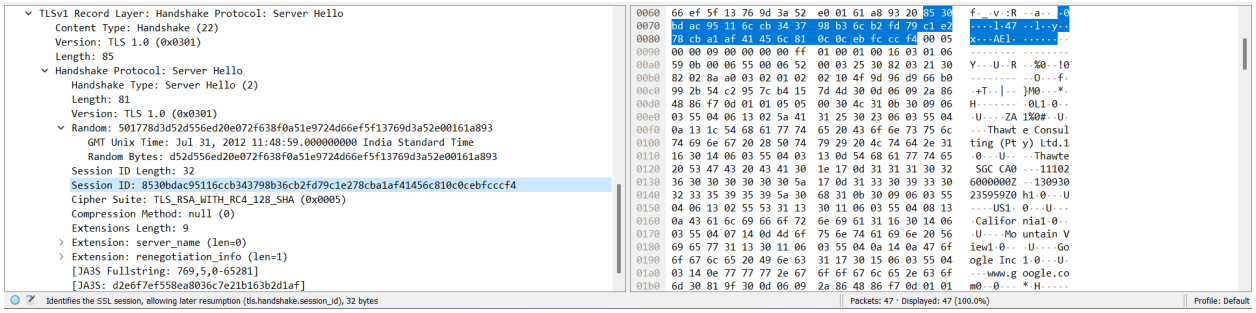
1. How long in bytes is the random data in the Hellos? Both the Client and Server include this random data (a nonce) to allow the establishment of session keys.

→ Length of random Bytes: 28



2. How long in bytes is the session identifier sent by the server? This identifier allows later resumption of the session with an abbreviated handshake when both the client and server indicate the same value. In our case, the client likely sent no session ID as there was nothing to resume.

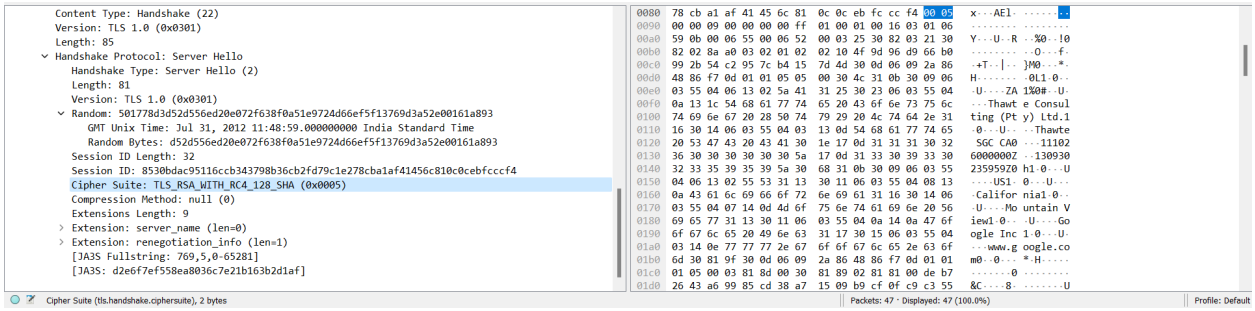
→ Session Identifier Length: 32 (Bytes 110 - 141)



3. What Cipher suite is chosen by the Server? Give its name and value. The Client will list the different cipher methods it supports, and the Server will pick one of these methods to use.

→ Cipher Suite used by the Server is:

Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)



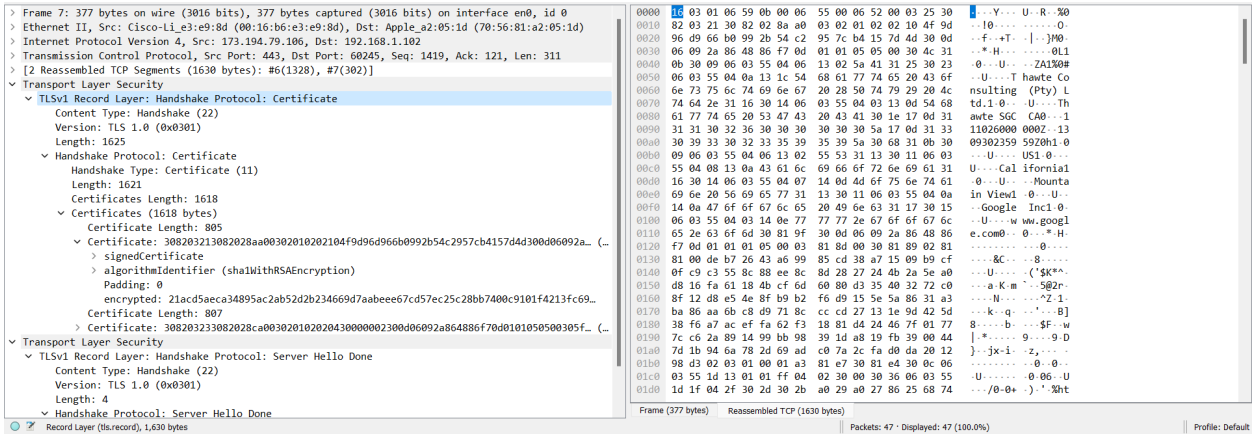
4.2 Certificate Messages

Next, find and inspect the details of the Certificate message, including expanding the Handshake proto-col block within the TLS Record. As with the Hellos, the contents of the Certificate message are visible because an encryption scheme is not yet established. It should come after the Hello messages.

Answer the following questions:

1. Who sends the Certificate, the client, the server, or both?A certificate is sent by one party to let the other party authenticate that it is who it claims to be. Based on this usage, you should be able to guess who sends the certificate and check the messages in your trace.

→ In this packet tract only server is sending its certificate. But there might be the case that the server could ask the client to provide its own certificate for the identity of the client.



A Certificate message will contain one or more certificates, as needed for one party to verify the identity of the other party from its roots of trust certificates. You can inspect those certificates in your browser.

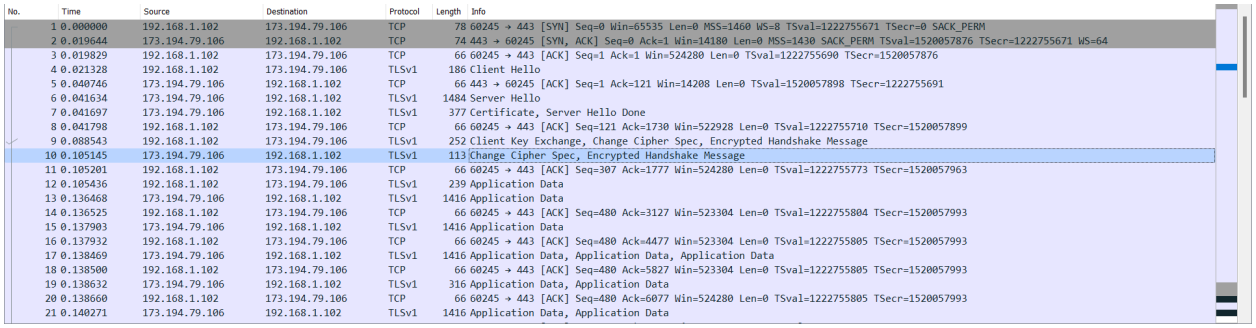
4.3 Client Key Exchange and Change Cipher Messages

Find and inspect the details of the Client Key Exchange and Change Cipher messages, expanding their various details. The key exchange message is sent to pass keying information so that both sides will have the same secret session key. The change cipher message signal a switch to a new encryption scheme to the other party. This means that it is the last unencrypted message sent by the party.

Answer the following questions:

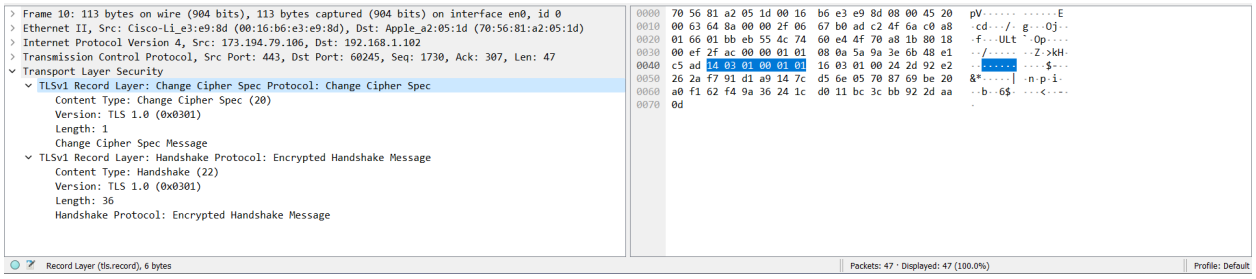
1. Who sends the Change Cipher Spec message, the client, the server, or both?

→ The change cipher spec message is sent by both client and server. Client sent it first.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	173.194.79.106	TCP	78	60245 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=1222755671 TSecr=0 SACK_PERM
2	0.019644	173.194.79.106	192.168.1.102	TCP	74	443 → 60245 [SYN, ACK] Seq=0 Ack=1 Win=14180 Len=0 MSS=1430 SACK_PERM TSval=1520057876 TSecr=1222755671 WS=64
3	0.019829	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=1 Ack=1 Win=524280 Len=0 TSval=1222755690 TSecr=1520057876
4	0.021328	192.168.1.102	173.194.79.106	TLSv1	186	Client Hello
5	0.040746	173.194.79.106	192.168.1.102	TCP	66	443 → 60245 [ACK] Seq=1 Ack=121 Win=14208 Len=0 TSval=1520057898 TSecr=1222755691
6	0.041634	173.194.79.106	192.168.1.102	TLSv1	1484	Server Hello
7	0.041697	173.194.79.106	192.168.1.102	TLSv1	377	Certificate, Server Hello Done
8	0.041798	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=121 Ack=1730 Win=522928 Len=0 TSval=1222755710 TSecr=1520057899
9	0.088543	192.168.1.102	173.194.79.106	TLSv1	252	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	0.105145	173.194.79.106	192.168.1.102	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
11	0.105201	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=307 Ack=1777 Win=524280 Len=0 TSval=1222755773 TSecr=1520057963
12	0.105436	192.168.1.102	173.194.79.106	TLSv1	239	Application Data
13	0.136468	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data
14	0.136525	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=480 Ack=3127 Win=523304 Len=0 TSval=1222755804 TSecr=1520057993
15	0.137903	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data
16	0.137932	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=480 Ack=4477 Win=523304 Len=0 TSval=1222755805 TSecr=1520057993
17	0.138469	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data, Application Data, Application Data
18	0.138500	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=480 Ack=5827 Win=523304 Len=0 TSval=1222755805 TSecr=1520057993
19	0.138632	173.194.79.106	192.168.1.102	TLSv1	316	Application Data, Application Data
20	0.138660	192.168.1.102	173.194.79.106	TCP	66	60245 → 443 [ACK] Seq=480 Ack=6077 Win=524280 Len=0 TSval=1222755805 TSecr=1520057993
21	0.140271	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data, Application Data

2. What are the contents carried inside the Change Cipher Spec message? Look past the Content Type and other headers to see the message itself.



```
> Frame 10: 113 bytes on wire (904 bits), 113 bytes captured (904 bits) on interface en0, id 0
> Ethernet II, Src: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d), Dst: Apple_a2:05:1d (70:56:81:a2:05:1d)
> Internet Protocol Version 4, Src: 173.194.79.106, Dst: 192.168.1.102
> Transmission Control Protocol, Src Port: 443, Dst Port: 60245, Seq: 1730, Ack: 307, Len: 47
v Transport Layer Security
  v TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.0 (0x0301)
      Length: 1
      Change Cipher Spec Message
  v TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 36
      Handshake Protocol: Encrypted Handshake Message
```

```
0000  70 56 81 a2 05 1d 00 16  b6 e3 e9 8d 08 00 45 20   pV·····  ·····E
0010  00 63 64 8a 00 00 2f 06  67 b0 ad c2 4f 6a c0 a8   ·cd···/· g···Oj··
0020  01 66 01 bb eb 55 4c 74  60 e4 4f 70 a8 1b 80 18   ·f···ULt `·Op····
0030  00 ef 2f ac 00 00 01 01  08 0a 5a 9a 3e 6b 48 e1   ··/····· ··Z·>kH·
0040  c5 ad 14 03 01 00 01 01  16 03 01 00 24 2d 92 e2   ········ ····$-··
0050  26 2a f7 91 d1 a9 14 7c  d5 6e 05 70 87 69 be 20   &*·····| ·n·p·i·
0060  a0 f1 62 f4 9a 36 24 1c  d0 11 bc 3c bb 92 2d aa   ··b··6$· ···<··-·
0070  0d                                                 ·
```

Record Layer (tls.record), 6 bytes | Packets: 47 · Displayed: 47 (100.0%) | Profile: Default

→ The Change Cipher Spec Message contains following Fiels:

- Content Type
- Version
- Length
- change cipher spec message