

Name: Siddhi Lokhande  
PRN NO: 2019BTECS00014

## **Assignment: 16**

### **Title:**

SSL/TLS Handshake Analysis using Wireshark

### **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

### **Theory:**

- Wireshark is a free and open-source packet analyzer.
- It is used for network troubleshooting, analysis, software and communications protocol development, and education.
- Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.
- Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix- like operating systems, and Microsoft Windows.
- There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU



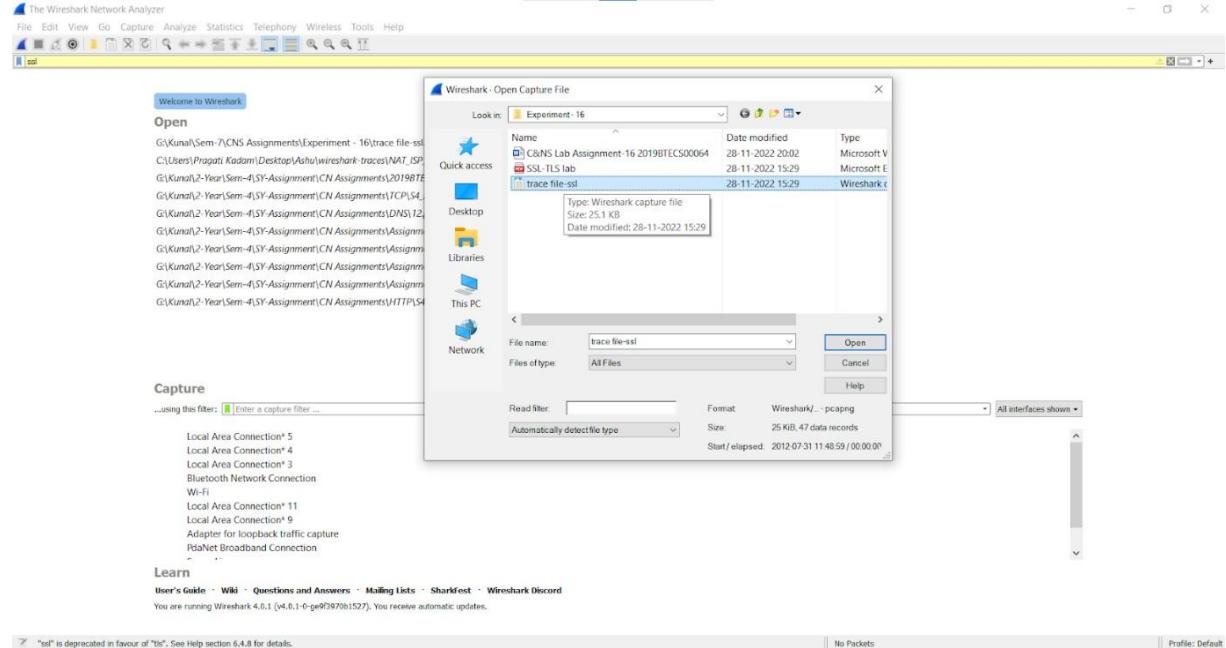
Edit with WPS Office

General Public License version 2 or any later version.

## Use of Wireshark

**Step 1:** Open a Trace you should use a supplied trace file trace-ssl.pcap.

File → Open → open from folder containing file



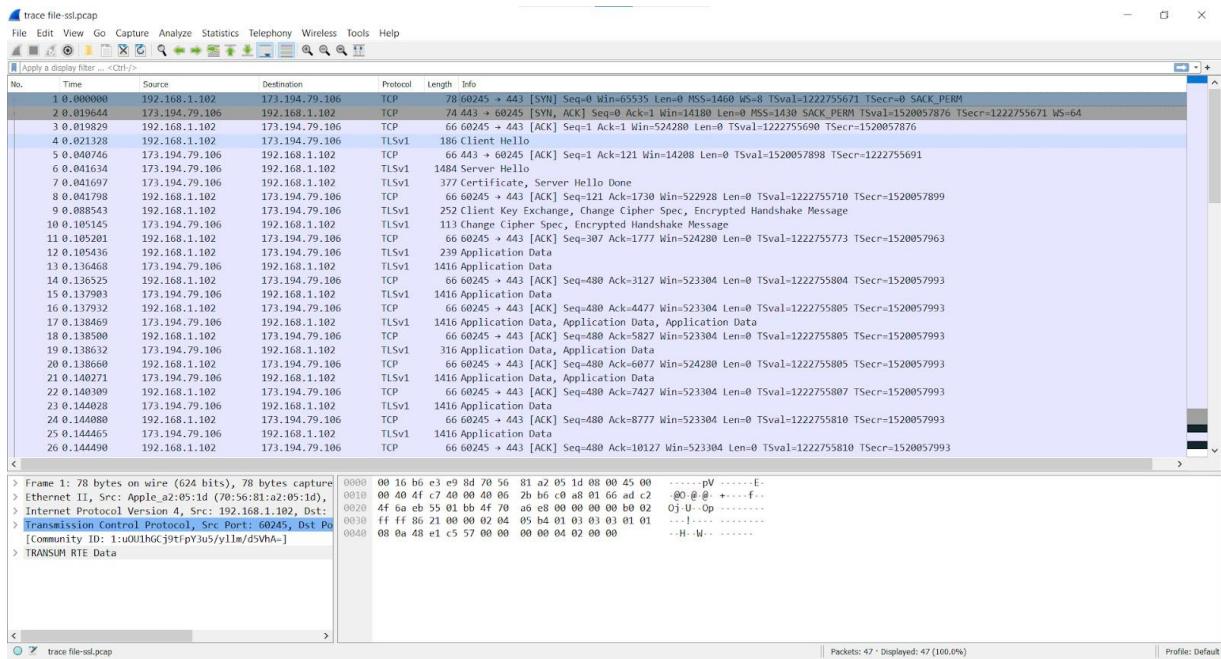
**Step 2:** Inspect the Trace

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 Acknowledgments 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).

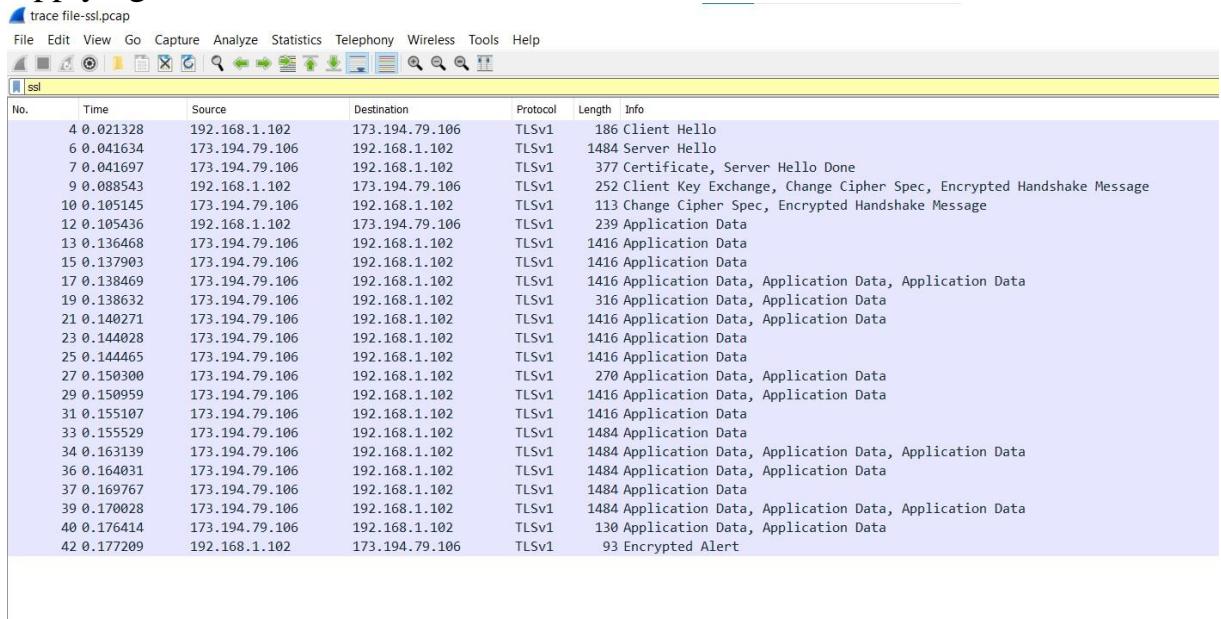
Application Data is a generic TLS message carrying contents for the application, such as the web page. It is a good place for us to start looking at TLS messages. Look for the following protocol blocks and fields in the message



Edit with WPS Office



## Applying SSL Filter



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



Edit with WPS Office

- 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 message. Each record will show up as its own block. Look at the Info column, and you will see messages with more than one block.

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

trace file:ssl.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No. Time Source Destination Protocol Length Info

No.	Time	Source	Destination	Protocol	Length	Info
4	0.021328	192.168.1.102	173.194.79.106	TLSv1	186	Client Hello
5	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
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
12	0.195436	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
15	0.137903	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data
17	0.138469	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data, Application Data, Application Data
19	0.138632	173.194.79.106	192.168.1.102	TLSv1	316	Application Data, Application Data
21	0.139271	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data, Application Data
23	0.144028	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data
25	0.144465	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data
27	0.150300	173.194.79.106	192.168.1.102	TLSv1	270	Application Data, Application Data
29	0.150959	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data, Application Data
31	0.151507	173.194.79.106	192.168.1.102	TLSv1	1416	Application Data
33	0.155529	173.194.79.106	192.168.1.102	TLSv1	1484	Application Data
34	0.161319	173.194.79.106	192.168.1.102	TLSv1	1484	Application Data, Application Data, Application Data
36	0.164031	173.194.79.106	192.168.1.102	TLSv1	1484	Application Data, Application Data
37	0.169767	173.194.79.106	192.168.1.102	TLSv1	1484	Application Data
39	0.170028	173.194.79.106	192.168.1.102	TLSv1	1484	Application Data, Application Data, Application Data
40	0.176414	173.194.79.106	192.168.1.102	TLSv1	130	Application Data, Application Data
42	0.177209	192.168.1.102	173.194.79.106	TLSv1	93	Encrypted Alert

Urgent Pointer: 0

> Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

> [Timestamps]

> [SEQ/ACK analysis]

CTP payload (137 bytes)

▼ Transport Layer Security

▼ TLSv1 Record Layer: Application Data Protocol: Hypertext Transfer Protocol

Content Type: Application Data (23)

Version: TLS 1.0 (0x0301)

Length: 168

Encrypted Application Data: 52e7f6ff0f72eecc876cc499ad794fd69ee412bb0e8a893114f5d8906232bdd...  
[Application Data Protocol: Hypertext Transfer Protocol]

[Community ID: 1:00000000000000000000000000000000]

▼ TRANSMISSION CONTROL PROTOCOL

0000: 80 16 b6 e3 e9 8d 70 56 81 a9 05 1d 08 08 45 00

0010: 00 01 e1 60 fd ff 40 00 06 93 f9 c0 86 65 ad 20

0020: 44 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

0030: ff ff 7c 62 00 00 01 01 08 08 49 e1 c5 bd 5a 94

0040: 3e 6b 17 03 01 00 a8 52 7f 8f c6 f7 3e ec 8a 76

0050: c5 49 9a d7 69 ee 41 2b e8 ba 8a 31 14 f5

0060: d8 9b 62 32 bd d0 92 4f 0d c7 d9 9f d7 c2 77 75

0070: 5d 45 76 ff ff 2c 13 aa 41 95 86 9f a3 0d 65

0080: c3 98 e7 08 00 10 36 5e 94 d8 b1 2d 41 c9 1c a9

0090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00a0: be 14 8a 5b 00 77 22 35 de 4a 29 58 00 00 00 00

00b0: 57 c3 22 9a 0a 61 09 b6 99 00 25 68 00 00 00 00

00c0: 86 73 9a 39 40 83 ff e1 18 8e 79 d9 42 49 e3

00d0: 7c 70 41 ab 36 42 86 cc 6a 08 17 75 a9 e2 92 01

00e0: 32 bb ea e3 32 8b 24 97 f9 17 99 92 13 28 90

.....

0..pV .....E  
0..@ ..L..  
0..j ..L..  
0..z ..H..Z.  
0..k ..R ..>..  
I..i ..A+..1  
I..b2 ..0 ..w  
I..Ev ..A ..-e  
.....6 ..A ..-e  
0..LM+P ..(8) ..7  
0..m ..w ..X ..Y  
0..l ..w ..X ..Y  
s..10 ..y ..B1  
pA..GB ..j ..u..  
2..2..S ..(..

Packets: 47 - Displayed: 23 (48.9%)

Profile: Default

```

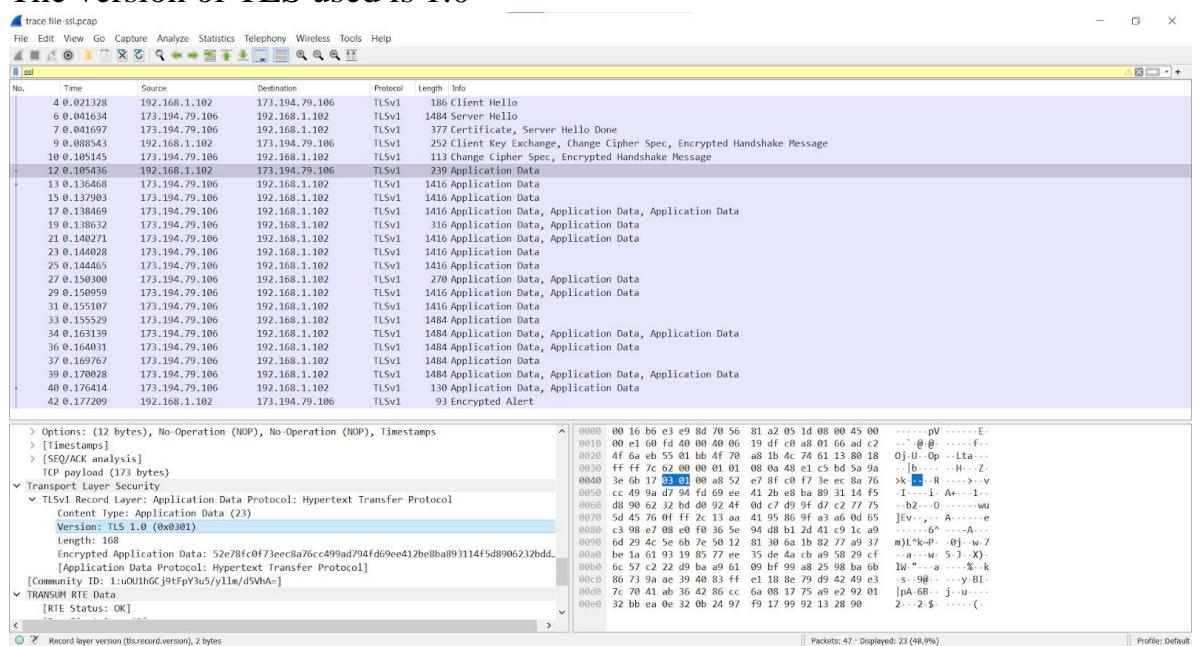
Urgent Pointer: 0
> Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
> [Timestamps]
> [SEQ/ACK analysis]
TCP payload (173 bytes)
▼ Transport Layer Security
  ▼ TLSv1 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
    Content Type: Application Data (23)
    Version: TLS 1.0 (0x0301)
    Length: 168
    Encrypted Application Data: 52e78fc0f73eec8a76cc499ad794fd69ee412be8ba893114f5d8906232bdd...
      [Application Data Protocol: Hypertext Transfer Protocol]
      [Community ID: 1:uOUlhGCj9tFpY3u5/y1lm/d5VhA=]
  ▼ TRANSUM RTE Data

```

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

Ans:

The version of TLS used is 1.0



Edit with WPS Office

```

    > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    > [Timestamps]
    > [SEQ/ACK analysis]
    TCP payload (173 bytes)
    ▼ Transport Layer Security
        ▼ TLSv1 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
            Content Type: Application Data (23)
            Version: TLS 1.0 (0x0301)
            Length: 168
            Encrypted Application Data: 52e78fc0f73eec8a76cc499ad794fd69ee412be8ba893114f5d8906232bdd..
            [Application Data Protocol: Hypertext Transfer Protocol]
            [Community ID: 1:u0U1hGCj9tFpY3u5/yllm/d5VhA=]
    ▼ TRANSM RTE Data
        [RTE Status: OK]

```

### Step 3: 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.

### 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.

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.

Ans:

## Client:

Trace file: stlcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No. Time Source Destination Protocol Length Info

1 4.021328 192.168.1.102 173.194.79.106 TLSv1 186 Client Hello

2 6.041634 173.194.79.106 192.168.1.102 TLSv1 1484 Server Hello

3 7.041697 173.194.79.106 192.168.1.102 TLSv1 377 Certificate, Server Hello Done

4 9.088543 192.168.1.102 173.194.79.106 TLSv1 252 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

5 10.195145 173.194.79.106 192.168.1.102 TLSv1 113 Change Cipher Spec, Encrypted Handshake Message

6 12.0195436 192.168.1.102 173.194.79.106 TLSv1 239 Application Data

7 13.0136468 173.194.79.106 192.168.1.102 TLSv1 1416 Application Data

8 15.0137903 173.194.79.106 192.168.1.102 TLSv1 1416 Application Data

9 17.0138469 173.194.79.106 192.168.1.102 TLSv1 1416 Application Data, Application Data, Application Data

10 19.0138632 173.194.79.106 192.168.1.102 TLSv1 316 Application Data, Application Data

11 21.0140271 173.194.79.106 192.168.1.102 TLSv1 1416 Application Data, Application Data

12 23.0140316 173.194.79.106 192.168.1.102 TLSv1 1416 Application Data

13 25.0144665 173.194.79.106 192.168.1.102 TLSv1 1416 Application Data

14 27.0150300 173.194.79.106 192.168.1.102 TLSv1 200 Application Data, Application Data

15 29.0150959 173.194.79.106 192.168.1.102 TLSv1 1416 Application Data, Application Data

16 31.0155107 173.194.79.106 192.168.1.102 TLSv1 1416 Application Data

17 33.0155529 173.194.79.106 192.168.1.102 TLSv1 1404 Application Data

18 34.0163139 173.194.79.106 192.168.1.102 TLSv1 1484 Application Data, Application Data, Application Data

19 36.0164031 173.194.79.106 192.168.1.102 TLSv1 1484 Application Data, Application Data

20 37.0169767 173.194.79.106 192.168.1.102 TLSv1 1484 Application Data

21 39.0170028 173.194.79.106 192.168.1.102 TLSv1 1484 Application Data, Application Data, Application Data

22 40.0176414 173.194.79.106 192.168.1.102 TLSv1 130 Application Data, Application Data

23 42.0177209 192.168.1.102 173.194.79.106 TLSv1 93 Encrypted Alert

TCP payload (120 bytes)

Transport Layer Security

TLSv1 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 115

Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 111

Version: TLS 1.0 (0x0301)

Random: 501778d316c25064f7cb0209b336ab332d969b8e091d26d4cc04b731d7e550f

GMT Unix Time: Jul 31, 2012 11:48:59.000000000 India Standard Time

Random Bytes: 16c25064f7cb0209b336ab332d969b8e091d26d4cc04b731d7e550f

Session ID Length: 0

Record layer version (tlv.record.version), 2 bytes

Packets: 47 · Displayed: 23 (48.9%)

Profile: Default

No. Time Source Destination Protocol Length Info

1 0000 00 16 b6 e3 c9 8d 70 56 81 a2 05 1d 08 00 00 45 00 ..pV .....E.

2 0010 00 04 ab d8 80 00 00 06 9f 88 c0 a8 01 56 ad c2 ..@ B.....F..

3 0020 4f 6a eb 55 01 bb Af 70 a6 9c 74 5a 23 88 18 0j U-Op -LT#-.

4 0030 ff 42 5c 00 00 01 01 08 0a 49 c1 c5 6b 5a 9a ..BV....-H-KZ-

5 0040 3e 14 16 03 01 00 73 01 00 00 6f 03 01 50 17 78 > ..S...-o-P-X

6 0050 d3 16 c2 50 64 f7 cb 02 09 b3 36 ab 33 d2 96 9b ...-PD-..-6-3-.

7 0060 8e 09 1d 26 44 cc 00 4b 73 1d 7e 55 0f 00 00 2e ...-&-K S-U-

8 0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 12 /-/-....

9 0080 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 12 /-8-5-....3-2

10 0090 00 00 00 14 00 11 00 00 00 00 00 00 00 03 00 ff 02 01 /-/....

11 00a0 00 00 12 00 00 00 12 00 11 00 00 00 00 00 00 00 77 77 2e .....-MM.

12 00b0 67 6f 6f 67 6c 05 2e 63 6f 6d google.c om

## Server:

trace file-ssl.cap

File Edit View Go Capture Analyze Statistics Telephone Wireless Tools Help

No. Time Source Destination Protocol Length Info

4	0.021328	192.168.1.102	173.194.79.106	TLSv1	180 Client Hello
5	0.021634	173.194.79.106	192.168.1.102	TLSv1	180 Server Hello
6	0.021637	173.194.79.106	192.168.1.102	TLSv1	377 Certificate, Server Hello Done
9	0.08543	173.194.79.106	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
12	0.105436	192.168.1.102	173.194.79.106	TLSv1	230 Application Data
13	0.136468	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
15	0.137993	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
17	0.138469	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data, Application Data, Application Data
19	0.138632	173.194.79.106	192.168.1.102	TLSv1	316 Application Data, Application Data
21	0.140271	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data, Application Data
23	0.144028	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
25	0.144465	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
27	0.150300	173.194.79.106	192.168.1.102	TLSv1	270 Application Data, Application Data
29	0.150959	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data, Application Data
31	0.155107	173.194.79.106	192.168.1.102	TLSv1	1416 Application Data
32	0.155529	173.194.79.106	192.168.1.102	TLSv1	1484 Application Data
34	0.161339	173.194.79.106	192.168.1.102	TLSv1	1484 Application Data, Application Data, Application Data
36	0.164031	173.194.79.106	192.168.1.102	TLSv1	1484 Application Data, Application Data
37	0.169767	173.194.79.106	192.168.1.102	TLSv1	1484 Application Data
39	0.170028	173.194.79.106	192.168.1.102	TLSv1	1484 Application Data, Application Data, Application Data
40	0.176414	173.194.79.106	192.168.1.102	TLSv1	130 Application Data, Application Data
42	0.177209	192.168.1.102	173.194.79.106	TLSv1	93 Encrypted Alert

[Reassembled PDU in frame: 2] TCP segment data (1328 bytes)

Transport Layer Security

- TLsv1 Record Layer: Handshake Protocol: Server Hello
  - Content Type: Handshake (22)
  - Version: TLS 1.0 (0x0301)
  - Length: 85
- Handshake Protocol: Server Hello
  - Handshake Type: Server Hello (2)
  - Length: 81
  - Version: TLS 1.0 (0x0301)
- Random: 501778d3d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893
  - GMT Unix Time: Jul 31, 2012 11:48:59.000000000 India Standard Time
  - Random Bytes: d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893

Random values used for deriving keys (tlshandshake.random), 32 bytes

[Reassembled PDU in frame: 7]

TCP segment data (1328 bytes)

Transport Layer Security

- TLsv1 Record Layer: Handshake Protocol: Server Hello
  - Content Type: Handshake (22)
  - Version: TLS 1.0 (0x0301)
  - Length: 85
- Handshake Protocol: Server Hello
  - Handshake Type: Server Hello (2)
  - Length: 81
  - Version: TLS 1.0 (0x0301)
- Random: 501778d3d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893
  - GMT Unix Time: Jul 31, 2012 11:48:59.000000000 India Standard Time
  - Random Bytes: d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893

Profile: Default



Edit with WPS Office

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.

Ans:

Server:

Length of Session ID is 32

The screenshot shows a Wireshark capture of a TLS handshake. The session details pane at the bottom indicates a session ID length of 32 bytes. The packet list shows the exchange of Client Hello, Server Hello, Certificate, Change Cipher Spec, and Application Data frames. The bytes pane shows the raw hex and ASCII data for the session ID field.

No.	Time	Source	Destination	Protocol	Length	Info
4.0.021328	192.168.1.182	173.194.79.106	TLSv1	106	Client Hello	
6.0.041634	173.194.79.106	192.168.1.182	TLSv1	1484	Server Hello	
7.0.041697	173.194.79.106	192.168.1.182	TLSv1	377	Certificate, Server Hello Done	
9.0.038543	192.168.1.182	173.194.79.106	TLSv1	252	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message	
10.0.105145	173.194.79.106	192.168.1.182	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message	
12.0.105436	192.168.1.182	173.194.79.106	TLSv1	239	Application Data	
13.0.136468	173.194.79.106	192.168.1.182	TLSv1	1416	Application Data	
15.0.137983	173.194.79.106	192.168.1.182	TLSv1	1416	Application Data	
17.0.138469	173.194.79.106	192.168.1.182	TLSv1	1416	Application Data, Application Data, Application Data	
19.0.138632	173.194.79.106	192.168.1.182	TLSv1	316	Application Data, Application Data	
21.0.140271	173.194.79.106	192.168.1.182	TLSv1	1416	Application Data, Application Data	
23.0.144028	173.194.79.106	192.168.1.182	TLSv1	1416	Application Data	
25.0.144465	173.194.79.106	192.168.1.182	TLSv1	1416	Application Data	
27.0.150300	173.194.79.106	192.168.1.182	TLSv1	270	Application Data, Application Data	
29.0.150959	173.194.79.106	192.168.1.182	TLSv1	1416	Application Data	
31.0.155107	173.194.79.106	192.168.1.182	TLSv1	1416	Application Data	
33.0.155529	173.194.79.106	192.168.1.182	TLSv1	1484	Application Data	
34.0.163139	173.194.79.106	192.168.1.182	TLSv1	1484	Application Data, Application Data, Application Data	
36.0.164031	173.194.79.106	192.168.1.182	TLSv1	1484	Application Data, Application Data	
37.0.169767	173.194.79.106	192.168.1.182	TLSv1	1484	Application Data	
39.0.170028	173.194.79.106	192.168.1.182	TLSv1	1484	Application Data, Application Data, Application Data	
40.0.176414	173.194.79.106	192.168.1.182	TLSv1	130	Application Data, Application Data	
42.0.177209	192.168.1.182	173.194.79.106	TLSv1	93	Encrypted Alert	

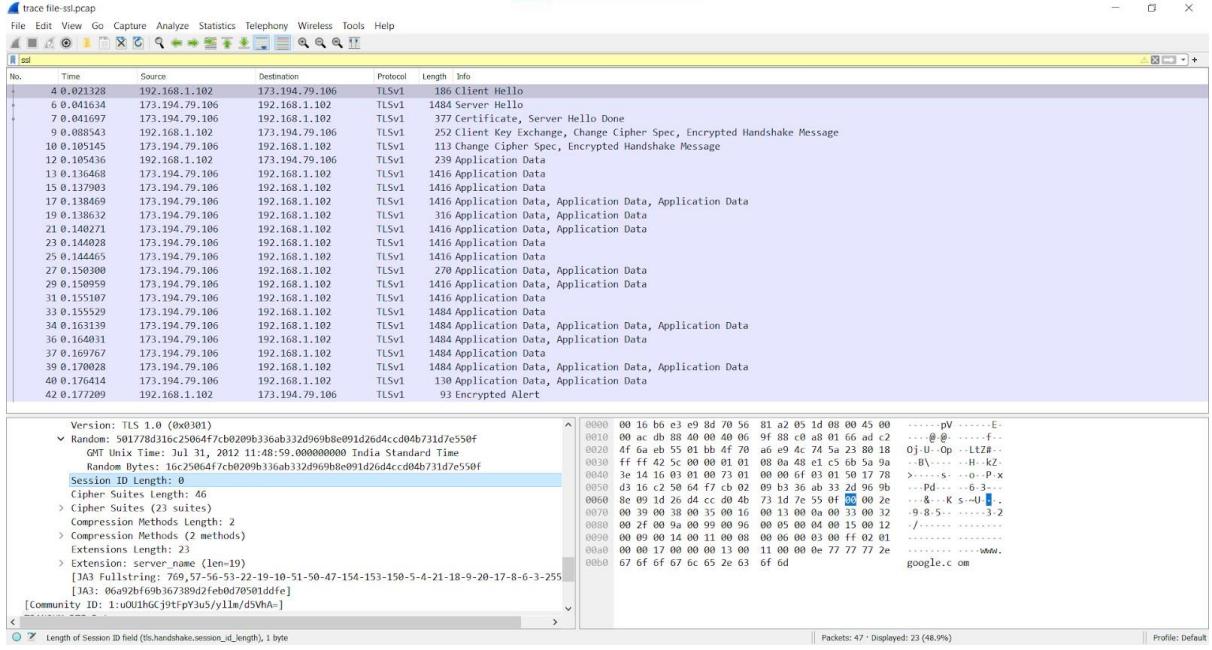
**Handshake Protocol: Server Hello**  
**Handshake Type: Server Hello (2)**  
**Length: 81**  
**Version: TLS 1.0 (0x0301)**  
**Random: 501778d3d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893**  
**GMT Unix Time: Jul 31, 2012 11:48:59.000000000 India Standard Time**  
**Random Bytes: d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893**  
**Session ID Length: 32**  
**Session ID: 8530bdac95116ccb343798b36cb2fd79c1e278cba1af41456c810c0cebfcccf4**  
**Cipher Suite: TLS\_RSA\_WITH\_RC4\_128\_SHA (0x0005)**  
**Compression Method: null (0)**  
**Extensions Length: 9**  
> Extension: server\_name (len=0)  
> Extension: renegotiation\_info (len=1)

Client:

Length of Session ID is 0



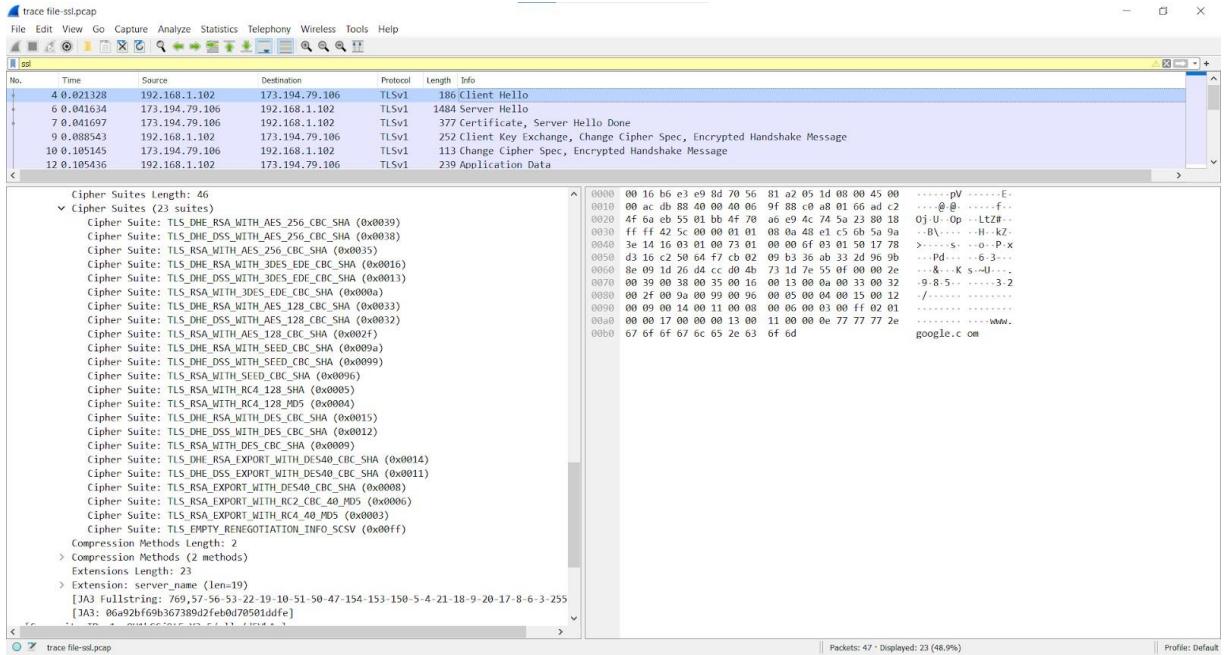
Edit with WPS Office



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.

Ans:

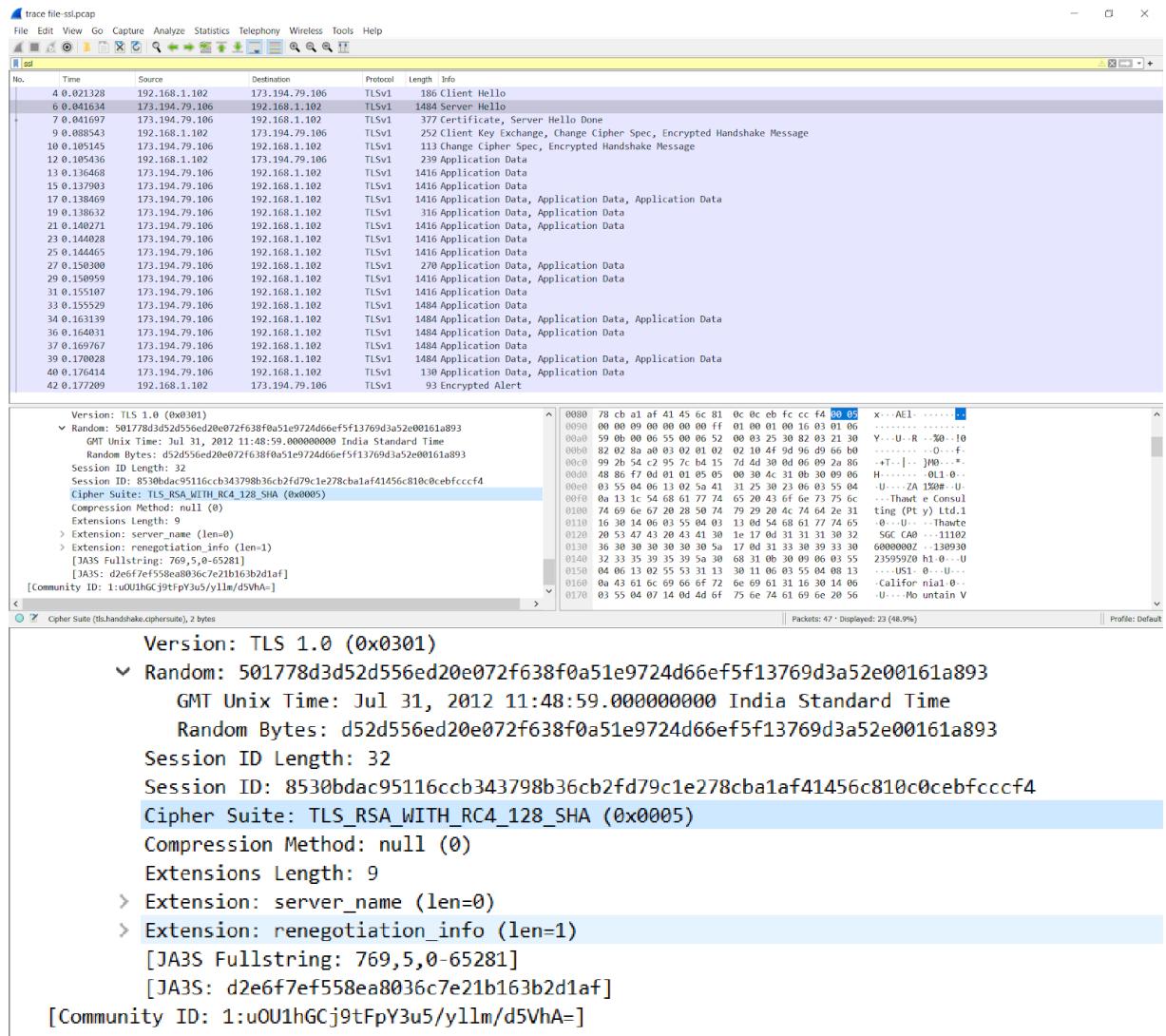
Client:



Server:



Edit with WPS Office



## Certificate Messages:

Next, find and inspect the details of the Certificate message, including expanding the Handshake protocol 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.

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.



Edit with WPS Office

Ans:

## The Server sends Certificate to the client

Two screenshots of Wireshark showing network traffic for a TLS handshake. The top screenshot shows the initial Client Hello and Server Hello messages, followed by the Certificate message from the server. The bottom screenshot shows the continuation of the handshake, including the Client Key Exchange and Change Cipher Spec messages.

**Trace file: ssl.pcap**

No. Time Source Destination Protocol Length Info

4 0.021328 192.168.1.102 173.194.79.106 TLSv1 186 Client Hello

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

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

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

15 0.137983 173.194.79.106 192.168.1.102 TLSv1 1416 Application Data

17 0.138469 173.194.79.106 192.168.1.102 TLSv1 1416 Application Data, Application Data, Application Data

19 0.138632 173.194.79.106 192.168.1.102 TLSv1 316 Application Data, Application Data

21 0.140271 173.194.79.106 192.168.1.102 TLSv1 1416 Application Data, Application Data

23 0.144028 173.194.79.106 192.168.1.102 TLSv1 1416 Application Data

25 0.144465 173.194.79.106 192.168.1.102 TLSv1 1416 Application Data

27 0.150300 173.194.79.106 192.168.1.102 TLSv1 270 Application Data, Application Data

29 0.150959 173.194.79.106 192.168.1.102 TLSv1 1416 Application Data, Application Data

31 0.155107 173.194.79.106 192.168.1.102 TLSv1 1416 Application Data

33 0.155529 173.194.79.106 192.168.1.102 TLSv1 1484 Application Data

34 0.163139 173.194.79.106 192.168.1.102 TLSv1 1484 Application Data, Application Data, Application Data

36 0.164031 173.194.79.106 192.168.1.102 TLSv1 1484 Application Data, Application Data

37 0.169767 173.194.79.106 192.168.1.102 TLSv1 1484 Application Data

39 0.170028 173.194.79.106 192.168.1.102 TLSv1 1484 Application Data, Application Data, Application Data

40 0.176414 173.194.79.106 192.168.1.102 TLSv1 130 Application Data, Application Data

42 0.177209 192.168.1.102 173.194.79.106 TLSv1 93 Encrypted Alert

**Trace file: ssl.pcap**

No. Time Source Destination Protocol Length Info

4 0.021328 192.168.1.102 173.194.79.106 TLSv1 186 Client Hello

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

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

12 0.105436 192.168.1.102 173.194.79.106 TLSv1 239 Application Data

[Checksum Status: Unverified]  
Urgent Pointer: 0  
> Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps  
> [Timestamps]  
> [SEQ/ACK analysis]  
TCP payload (311 bytes)  
TCP segment data (302 bytes)  
> [2 Reassembled TCP Segments (1630 bytes): #6(1328), #7(302)]  
TCP segment data (302 bytes)

**Transport Layer Security**

> TLSv1 Record Layer: Handshake Protocol: Certificate

Content Type: Handshake (22)  
Version: TLS 1.0 (0x0301)  
Length: 1625

> Handshake Protocol: Certificate

Handshake Type: Certificate (11)  
Length: 1621  
Certificates length: 1618

> Certificates (1618 bytes)

Certificate Length: 805  
> Certificate: 308203213082028aa00302010202104f9d96d966b0992b54c2957cb4157dd4d3000d06092a864886f70d01010500305  
Certificate Length: 807  
> Certificate: 308203233082028ca003020102020430000020300d06092a864886f70d01010500305

> Transport Layer Security

> TLSv1 Record Layer: Handshake Protocol: Server Hello Done

Frame (377 bytes) Reassembled TCF (1630 bytes)

Packets: 47 • Displayed: 23 (48.9%)

**Trace file: ssl.pcap**

No. Time Source Destination Protocol Length Info

4 0.021328 192.168.1.102 173.194.79.106 TLSv1 186 Client Hello

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

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

12 0.105436 192.168.1.102 173.194.79.106 TLSv1 239 Application Data

[Checksum Status: Unverified]  
Urgent Pointer: 0  
> Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps  
> [Timestamps]  
> [SEQ/ACK analysis]  
TCP payload (311 bytes)  
TCP segment data (302 bytes)  
> [2 Reassembled TCP Segments (1630 bytes): #6(1328), #7(302)]  
TCP segment data (302 bytes)

**Transport Layer Security**

> TLSv1 Record Layer: Handshake Protocol: Certificate

Content Type: Handshake (22)  
Version: TLS 1.0 (0x0301)  
Length: 1625

> Handshake Protocol: Certificate

Handshake Type: Certificate (11)  
Length: 1621  
Certificates length: 1618

> Certificates (1618 bytes)

Certificate Length: 805  
> Certificate: 308203213082028aa00302010202104f9d96d966b0992b54c2957cb4157dd4d3000d06092a864886f70d01010500305  
Certificate Length: 807  
> Certificate: 308203233082028ca003020102020430000020300d06092a864886f70d01010500305

> Transport Layer Security

> TLSv1 Record Layer: Handshake Protocol: Server Hello Done

Content Type: Handshake (22)  
Version: TLS 1.0 (0x0301)  
Length: 4

> Handshake Protocol: Server Hello Done

Handshake Type: Server Hello Done (14)  
Length: 0

[Community ID: 1:oU1hGcj9tFpY3u5/y1lm/d5VhA=]

Frame (377 bytes) Reassembled TCF (1630 bytes)

Packets: 47 • Displayed: 23 (48.9%)

|| Profile: Default

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.

## 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



Edit with WPS Office

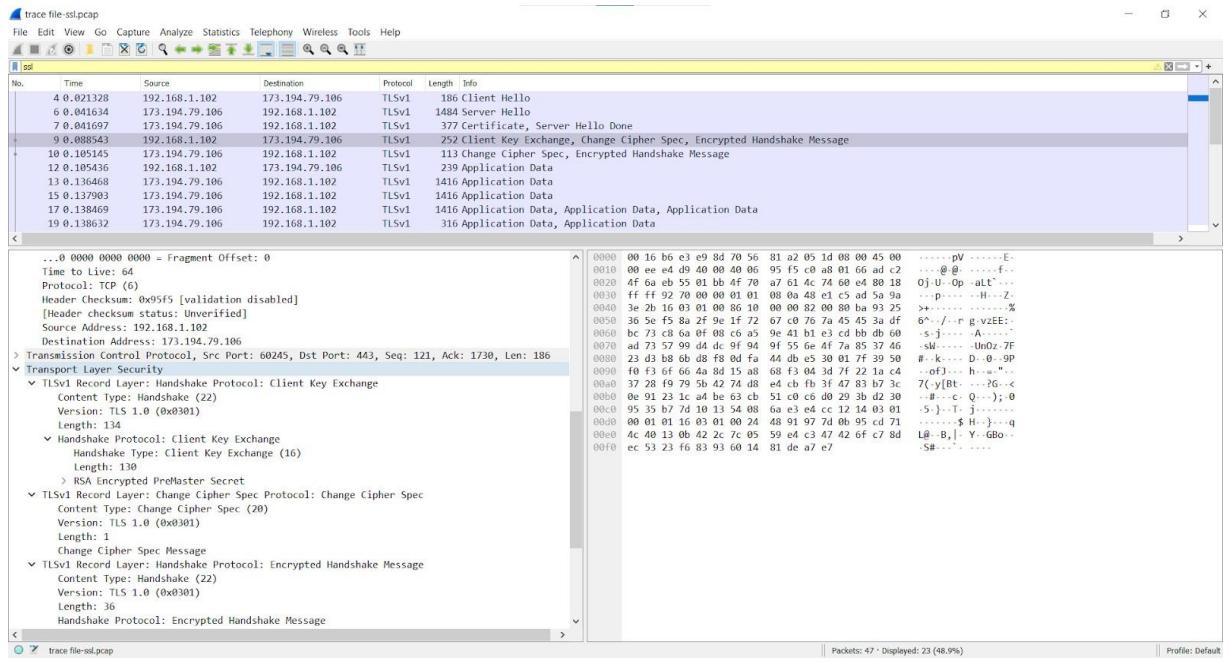
switch to a new encryption scheme to the other party. This means that it is the last unencrypted message sent by the party.

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

Ans:

Both the server and the client sends the Change Cipher Spec Message

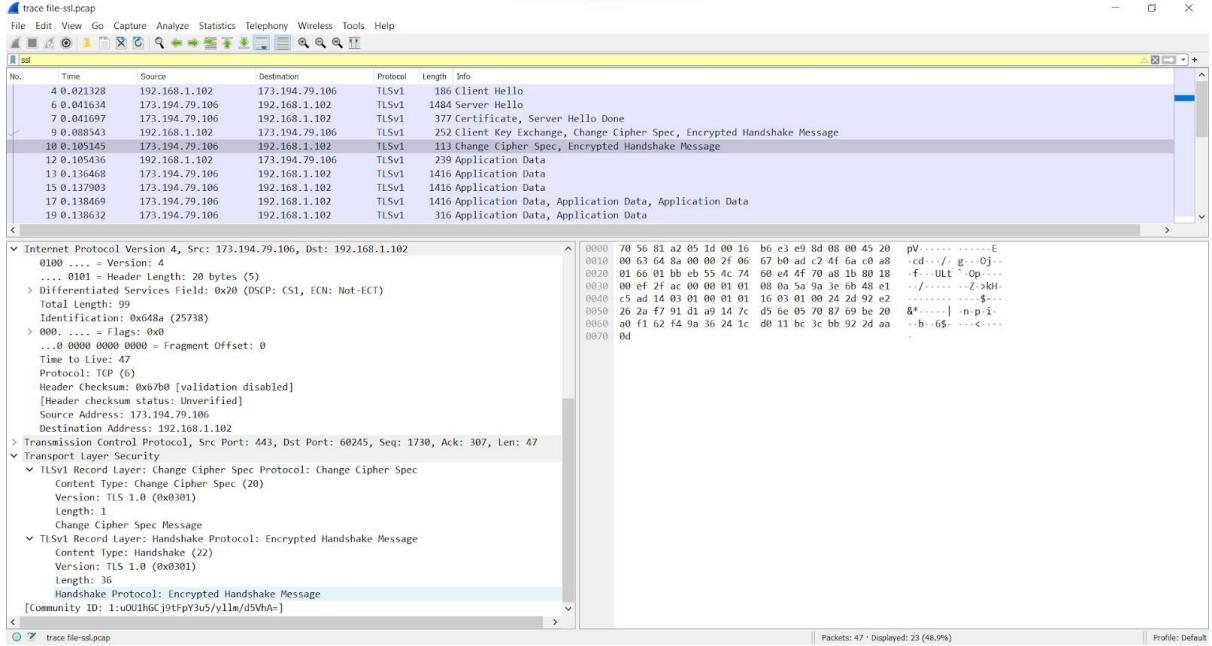
Client:



Server:

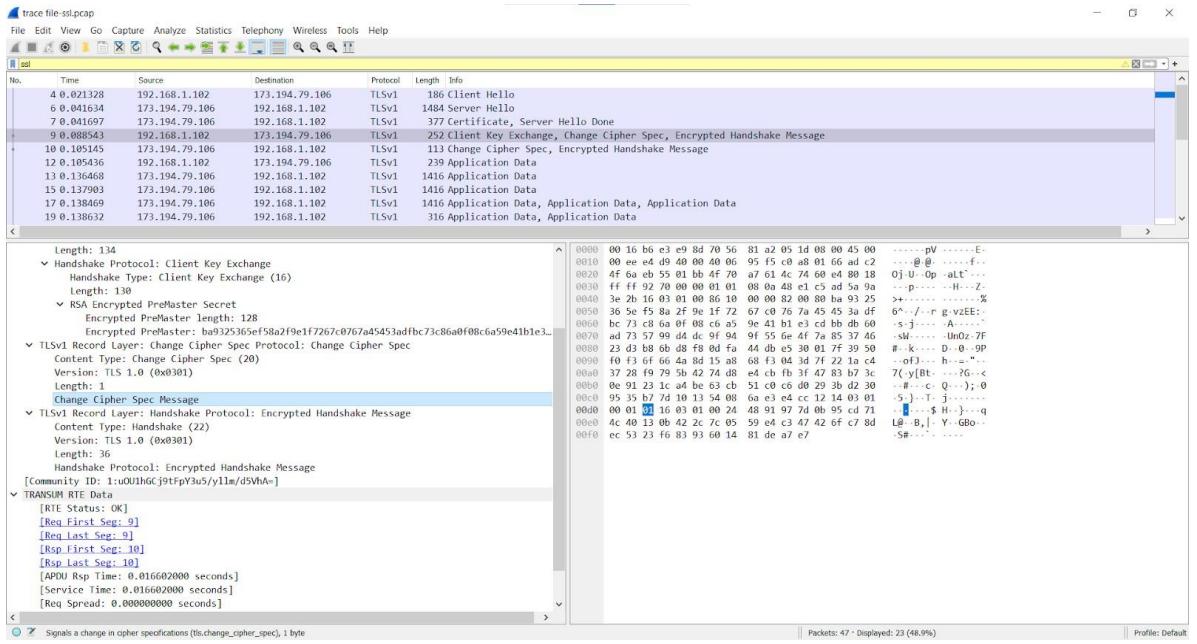


Edit with WPS Office

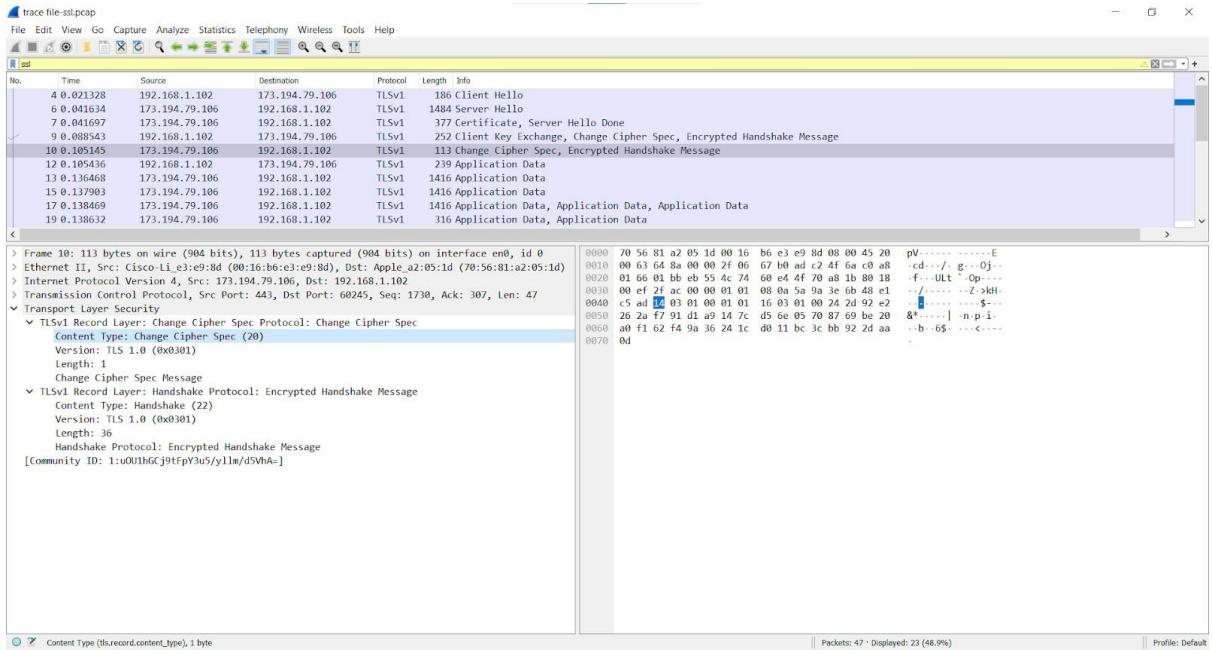


2. What are the contents carried inside the Change Cipher Spec message? Look past the Content Type and other headers to see the message itself.

Ans:



Edit with WPS Office



## Conclusion:

Performed the experiment successfully.

Wireshark is used to analyse the packets of various protocols such as TCP, UDP, SSL, TLS, etc.



Edit with WPS Office