

Final Year B. Tech., Sem VII 2022-23

## Cryptography And Network Security Lab

Assignment submission

PRN No: 2019BTECS00077

Full name: Avinash Biradar

Batch: B7

Assignment: 16

Title of assignment: SSL/TLS Handshake Analysis using  
Wireshark

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 analyser.
- 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

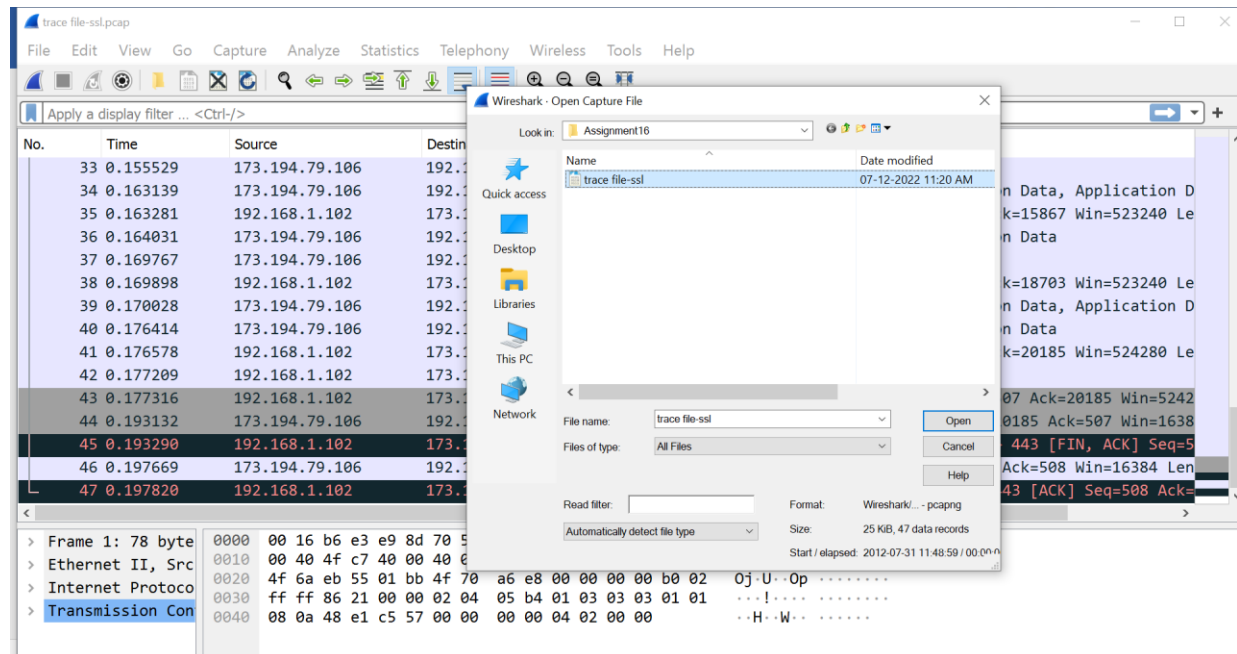
on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows.

- 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 General Public License version 2 or any later version.

## Use of Wireshark

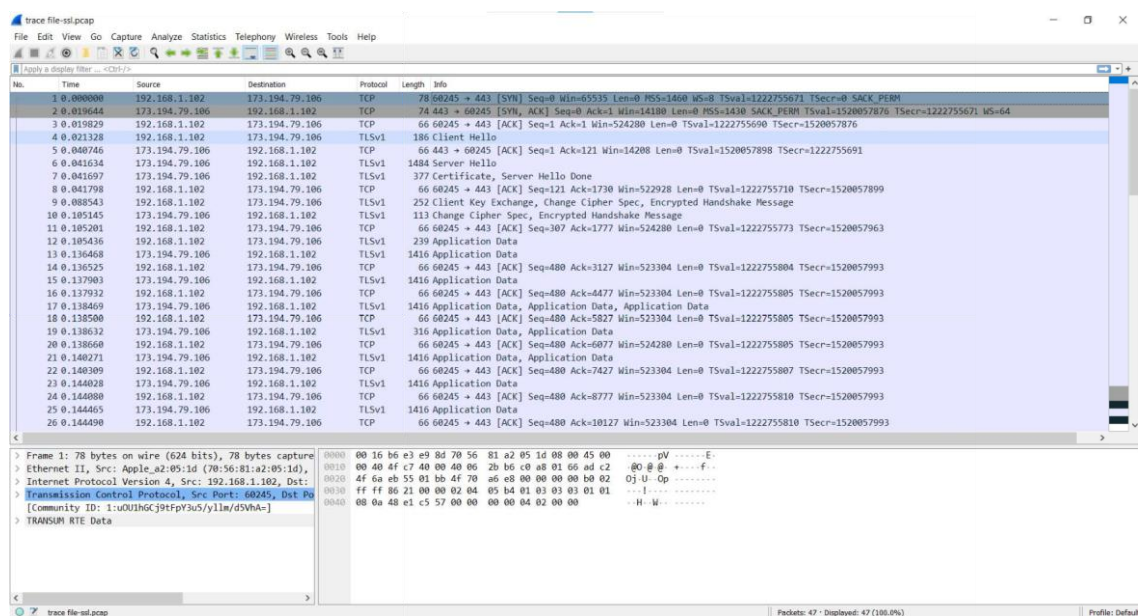
Step 1: Open a Trace you should use a supplied trace file trace-ssl.pcap.

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 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



Applying SSL Filter

trace file-ssl.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl

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	0.137903	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	0.140271	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

- 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 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.

The image shows a Wireshark capture of a TLS handshake and application data exchange. The handshake sequence is as follows:

- 4.0.021328: 192.168.1.102 to 173.194.79.106, TLSv1, 186 Client Hello
- 6.0.041634: 173.194.79.106 to 192.168.1.102, TLSv1, 1484 Server Hello
- 7.0.041697: 173.194.79.106 to 192.168.1.102, TLSv1, 377 Certificate, Server Hello Done
- 9.0.088541: 192.168.1.102 to 173.194.79.106, TLSv1, 252 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
- 10.0.105145: 173.194.79.106 to 192.168.1.102, TLSv1, 113 Change Cipher Spec, Encrypted Handshake Message
- 12.0.105436: 192.168.1.102 to 173.194.79.106, TLSv1, 239 Application Data
- 13.0.136468: 173.194.79.106 to 192.168.1.102, TLSv1, 1416 Application Data
- 15.0.137903: 173.194.79.106 to 192.168.1.102, TLSv1, 1416 Application Data
- 17.0.138469: 173.194.79.106 to 192.168.1.102, TLSv1, 1416 Application Data, Application Data, Application Data
- 19.0.138632: 173.194.79.106 to 192.168.1.102, TLSv1, 316 Application Data, Application Data
- 21.0.140271: 173.194.79.106 to 192.168.1.102, TLSv1, 1416 Application Data, Application Data
- 23.0.144028: 173.194.79.106 to 192.168.1.102, TLSv1, 1416 Application Data
- 25.0.144465: 173.194.79.106 to 192.168.1.102, TLSv1, 1416 Application Data
- 27.0.150300: 173.194.79.106 to 192.168.1.102, TLSv1, 270 Application Data, Application Data
- 29.0.150959: 173.194.79.106 to 192.168.1.102, TLSv1, 1416 Application Data, Application Data
- 31.0.155107: 173.194.79.106 to 192.168.1.102, TLSv1, 1416 Application Data
- 33.0.155529: 173.194.79.106 to 192.168.1.102, TLSv1, 1484 Application Data
- 34.0.163139: 173.194.79.106 to 192.168.1.102, TLSv1, 1484 Application Data, Application Data, Application Data
- 36.0.164031: 173.194.79.106 to 192.168.1.102, TLSv1, 1484 Application Data, Application Data
- 37.0.169767: 173.194.79.106 to 192.168.1.102, TLSv1, 1484 Application Data, Application Data
- 39.0.170928: 173.194.79.106 to 192.168.1.102, TLSv1, 1484 Application Data, Application Data, Application Data
- 40.0.176414: 173.194.79.106 to 192.168.1.102, TLSv1, 130 Application Data, Application Data
- 42.0.177209: 192.168.1.102 to 173.194.79.106, TLSv1, 93 Encrypted Alert

The detailed view of the TLSv1 Record Layer (packet 12) shows the following structure:

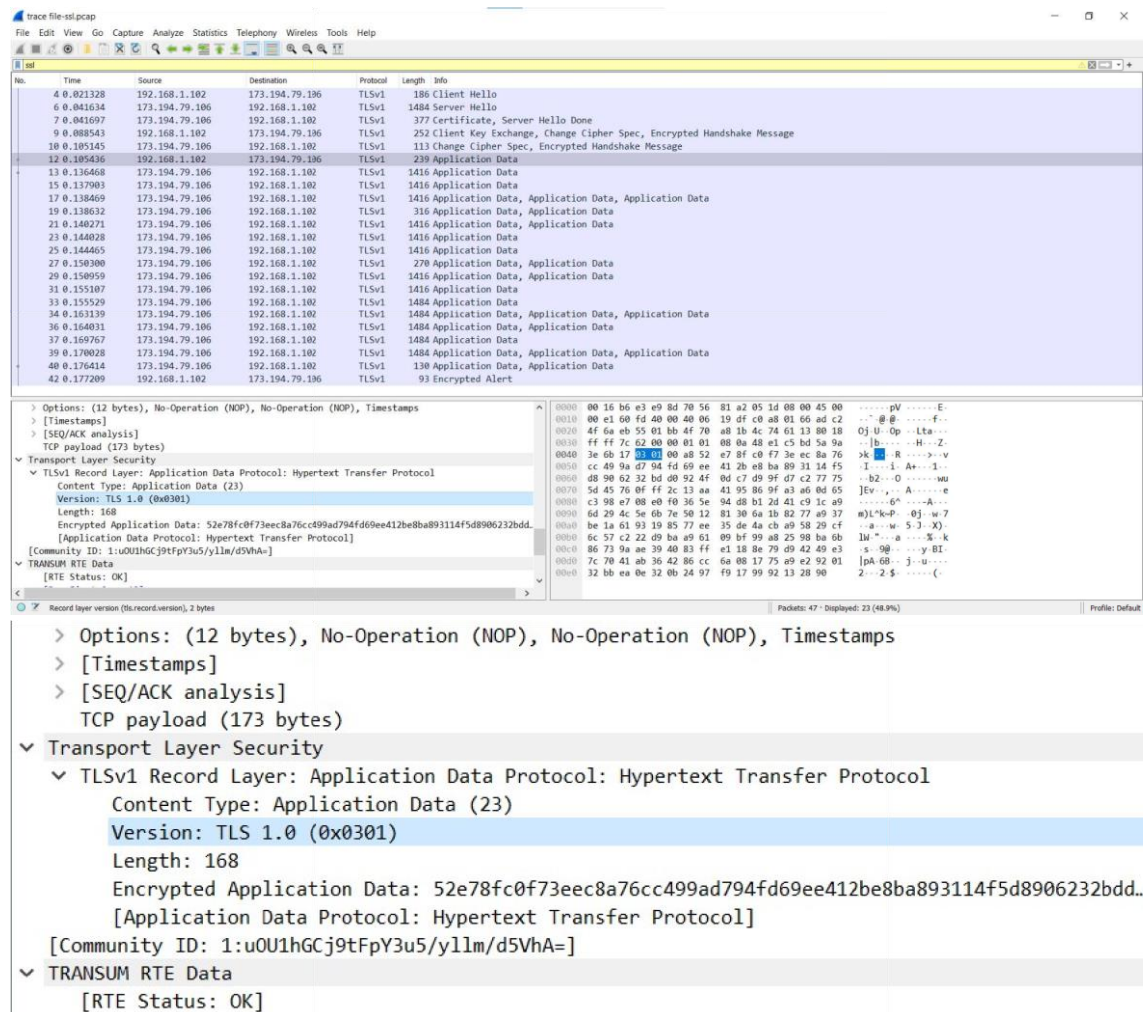
- Urgent Pointer: 0
- Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
- [Timestamps]
- [SEQ/ACK analysis]
- TCP payload (173 bytes)
- Transport Layer Security
  - TLSv1 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
    - Content Type: Application Data (23)
    - Version: TLS 1.0 (0x0301)
    - Length: 168
    - Encrypted Application Data: 52e78fc0f73ecc8a76cc499ad794fd69ee412be8ba893114f5d8906232bdd..
    - [Application Data Protocol: Hypertext Transfer Protocol]
    - [Community ID: 1:uOU1hGcJ9tFpY3u5/yllm/d5VhA=]
  - TRANSMISSION 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



The image displays a Wireshark packet capture of a TLS 1.0 handshake and subsequent application data exchange. The top pane shows a list of 42 packets. The bottom pane provides a detailed view of the selected packet (No. 12), showing the TLSv1 Record Layer structure.

**Packet List:**

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	0.137988	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	0.161339	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

**Packet Details (No. 12):**

- 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:uOU1hGCj9tFpY3u5/yllm/d5VhA=]
  - TRANSMISSION 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:ssl.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
4	0.021328	192.168.1.102	173.194.79.136	TLSv1	186	Client Hello
6	0.041634	173.194.79.136	192.168.1.102	TLSv1	1484	Server Hello
7	0.041697	173.194.79.136	192.168.1.102	TLSv1	377	Certificate, Server Hello Done
9	0.088541	192.168.1.102	173.194.79.136	TLSv1	252	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	0.105145	173.194.79.136	192.168.1.102	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
12	0.105436	192.168.1.102	173.194.79.136	TLSv1	239	Application Data
13	0.136468	173.194.79.136	192.168.1.102	TLSv1	1416	Application Data
15	0.137903	173.194.79.136	192.168.1.102	TLSv1	1416	Application Data
17	0.138469	173.194.79.136	192.168.1.102	TLSv1	1416	Application Data, Application Data, Application Data
19	0.138632	173.194.79.136	192.168.1.102	TLSv1	316	Application Data, Application Data
21	0.140271	173.194.79.136	192.168.1.102	TLSv1	1416	Application Data, Application Data
23	0.144028	173.194.79.136	192.168.1.102	TLSv1	1416	Application Data
25	0.144465	173.194.79.136	192.168.1.102	TLSv1	1416	Application Data
27	0.150300	173.194.79.136	192.168.1.102	TLSv1	270	Application Data, Application Data
29	0.150959	173.194.79.136	192.168.1.102	TLSv1	1416	Application Data, Application Data
31	0.155107	173.194.79.136	192.168.1.102	TLSv1	1416	Application Data
33	0.155529	173.194.79.136	192.168.1.102	TLSv1	1484	Application Data
34	0.163139	173.194.79.136	192.168.1.102	TLSv1	1484	Application Data, Application Data, Application Data
36	0.164031	173.194.79.136	192.168.1.102	TLSv1	1484	Application Data, Application Data
37	0.169767	173.194.79.136	192.168.1.102	TLSv1	1484	Application Data
39	0.170928	173.194.79.136	192.168.1.102	TLSv1	1484	Application Data, Application Data, Application Data
40	0.176414	173.194.79.136	192.168.1.102	TLSv1	130	Application Data, Application Data
42	0.177209	192.168.1.102	173.194.79.136	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: 501778d316c25064f7cb0209b336ab332d969b8e091d26d4ccd04b731d7e550f
      - GMT Unix Time: Jul 31, 2012 11:48:59.000000000 India Standard Time
      - Random Bytes: 16c25064f7cb0209b336ab332d969b8e091d26d4ccd04b731d7e550f
      - Session ID Length: 0

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

Packets: 47 - Displayed: 23 (48.9%)

Profile: Default

Server:



**Reassembled PDU in frame: 71**

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

- 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:

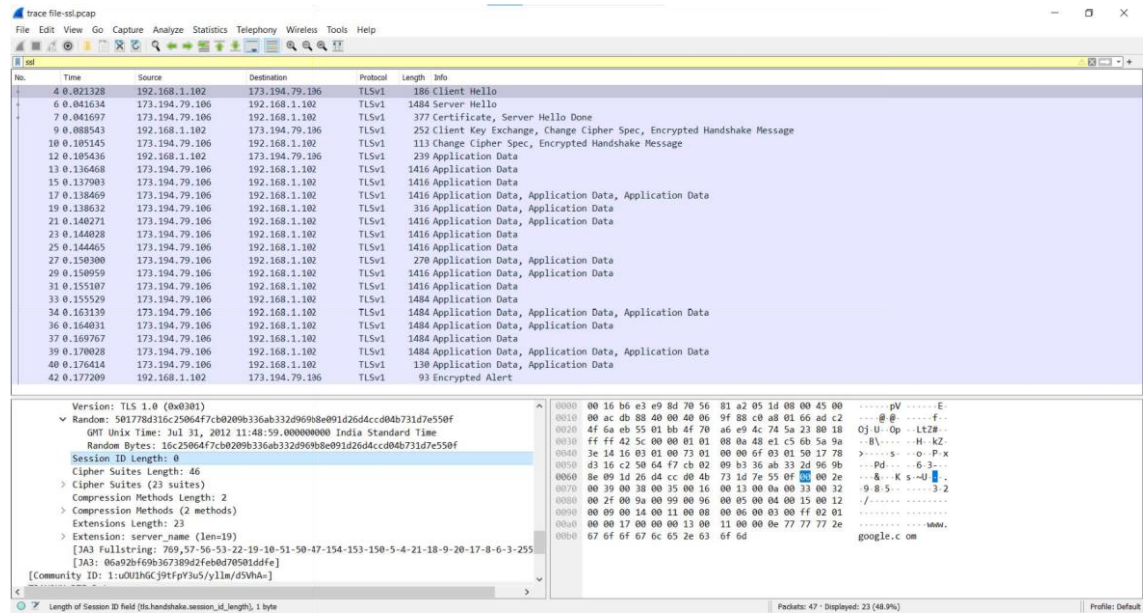
Server:

Length of Session ID is 32

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:

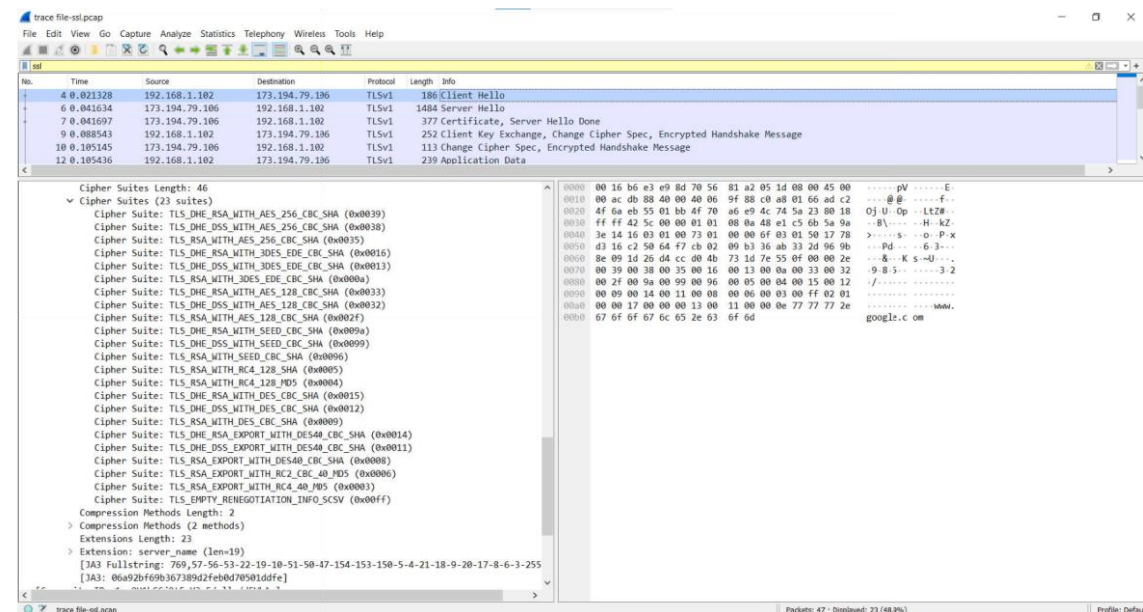
Length of Session ID is 0



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:



The image shows a Wireshark packet capture of a TLS handshake. The top pane displays a list of packets, and the bottom pane shows the expanded details of a TLS record.

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
4	0.021328	192.168.1.102	173.194.79.136	TLSv1	186	Client Hello
6	0.041634	173.194.79.136	192.168.1.102	TLSv1	1484	Server Hello
7	0.041697	173.194.79.136	192.168.1.102	TLSv1	377	Certificate, Server Hello Done
9	0.088541	192.168.1.102	173.194.79.136	TLSv1	252	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	0.105145	173.194.79.136	192.168.1.102	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message
12	0.105436	192.168.1.102	173.194.79.136	TLSv1	239	Application Data
13	0.136468	173.194.79.136	192.168.1.102	TLSv1	1416	Application Data
15	0.137903	173.194.79.136	192.168.1.102	TLSv1	1416	Application Data
17	0.138469	173.194.79.136	192.168.1.102	TLSv1	1416	Application Data, Application Data, Application Data
19	0.138632	173.194.79.136	192.168.1.102	TLSv1	316	Application Data, Application Data
21	0.140271	173.194.79.136	192.168.1.102	TLSv1	1416	Application Data, Application Data
23	0.144028	173.194.79.136	192.168.1.102	TLSv1	1416	Application Data
25	0.144465	173.194.79.136	192.168.1.102	TLSv1	1416	Application Data
27	0.150300	173.194.79.136	192.168.1.102	TLSv1	270	Application Data, Application Data
29	0.150959	173.194.79.136	192.168.1.102	TLSv1	1416	Application Data, Application Data
31	0.155107	173.194.79.136	192.168.1.102	TLSv1	1416	Application Data
33	0.155529	173.194.79.136	192.168.1.102	TLSv1	1484	Application Data
34	0.163139	173.194.79.136	192.168.1.102	TLSv1	1484	Application Data, Application Data, Application Data
36	0.164031	173.194.79.136	192.168.1.102	TLSv1	1484	Application Data, Application Data
37	0.169767	173.194.79.136	192.168.1.102	TLSv1	1484	Application Data
39	0.170928	173.194.79.136	192.168.1.102	TLSv1	1484	Application Data, Application Data, Application Data
40	0.176414	173.194.79.136	192.168.1.102	TLSv1	130	Application Data, Application Data
42	0.177209	192.168.1.102	173.194.79.136	TLSv1	93	Encrypted Alert

**Packet Details:**

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: 8530bdac95116ccb343798b36cb2fd79c1e278cba1af41456c810c0ebfccc4
- 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)
- [JA3S Fullstring: 769,5,0-65281]
- [JA3S: d2e6f7ef558ea8036c7e21b163b2d1af]
- [Community ID: 1:uOU1hGCj9tFpY3u5/yllm/d5VhA=]

**Packet Bytes:**

0000 78 cb a1 af 41 45 6c 81 0c 0e eb fc cc f4 05 x: AEL .....  
0001 00 00 09 00 00 00 00 ff 01 00 01 00 15 03 01 06 .....  
0002 50 00 00 00 55 00 00 52 00 03 25 30 82 03 21 30 Y...U.R...50...10  
0003 82 02 8a a0 03 02 01 02 02 10 4f 9d 96 09 66 b0 .....  
0004 99 2b 54 c2 95 7c b4 15 7d 4d 30 0d 06 09 2a 86 +T...J00...  
0005 48 86 f7 0d 01 01 05 05 00 30 4c 31 00 30 09 06 H....0110  
0006 03 55 04 06 13 02 5a 41 31 25 30 23 06 03 55 04 U...ZA130#...U  
0007 0a 13 1c 54 68 61 77 74 65 20 43 6f 6e 73 75 6c ...Thaut e Consul  
0100 74 69 6e 67 20 28 50 74 79 29 20 4c 74 64 2e 31 ting (Pt y) Ltd.1  
0101 16 30 14 06 03 55 04 03 13 0d 54 68 61 77 74 05 0...U...Thaute  
0102 20 53 47 43 20 43 41 30 1e 17 0d 31 31 31 30 32 SGC CAB ...11102  
0103 36 30 30 30 30 30 30 5a 17 0d 31 33 30 39 33 30 60000002...130930  
0104 32 33 35 39 35 39 5a 30 68 31 0b 30 09 06 03 55 23595920 h1 0...U  
0105 04 06 13 02 55 53 31 13 30 11 06 03 55 04 08 13 US1 0...U...  
0106 0a 43 61 6c 69 66 6f 72 6e 69 61 31 16 30 14 06 Califor nial 0...  
0107 83 55 04 07 14 0d 4d 6f 75 6e 74 61 69 6e 20 56 U...Mo untain V

## 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.

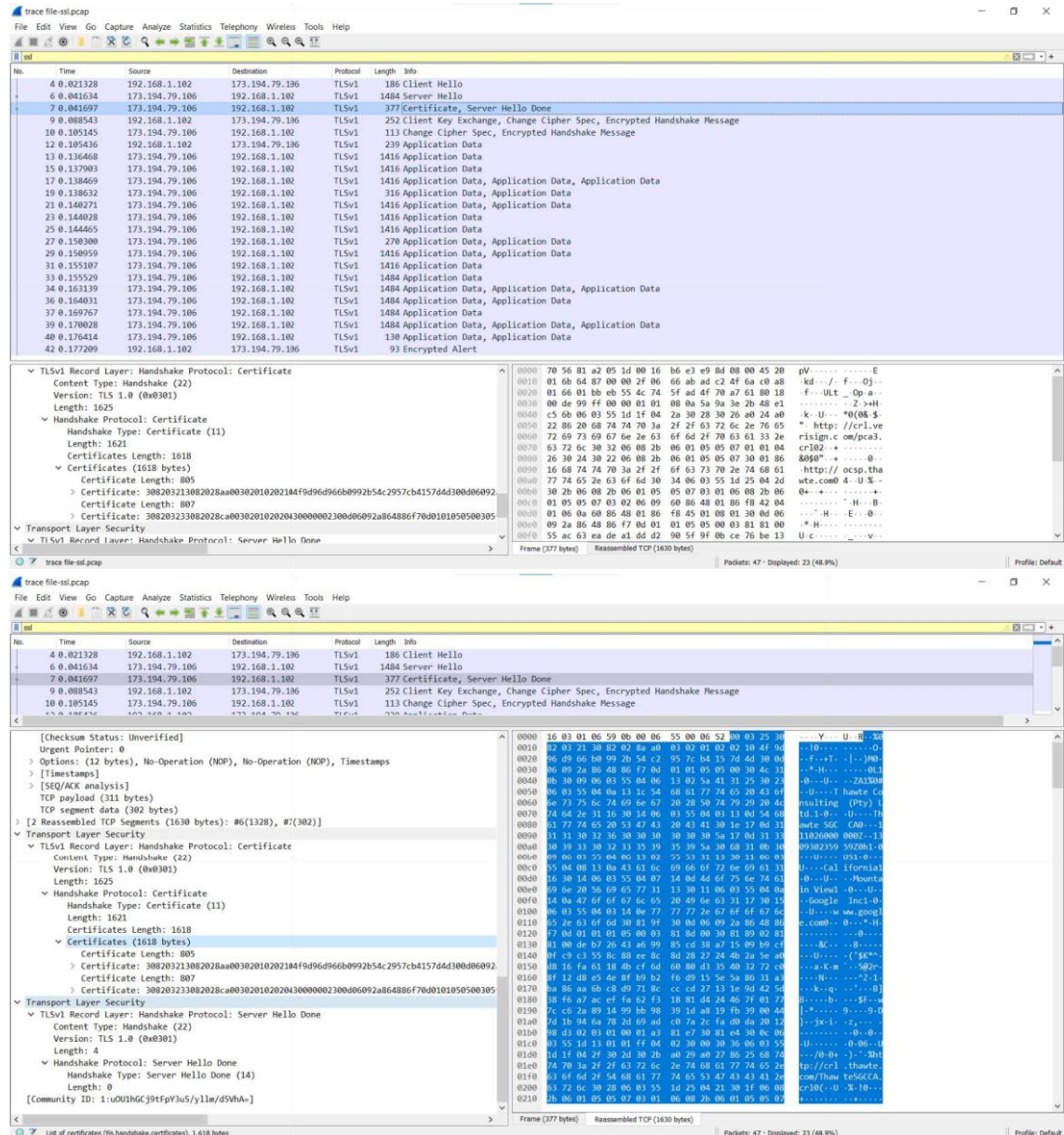
1. Who sends the Certificate, the client, the server, or both? A certificate is sent by one party to let the other party authenticate that it is who it claims

to be. Based on this usage, you should be able to guess who sends the certificate and check the messages in your trace.

Ans:

The Server sends Certificate to 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.

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.

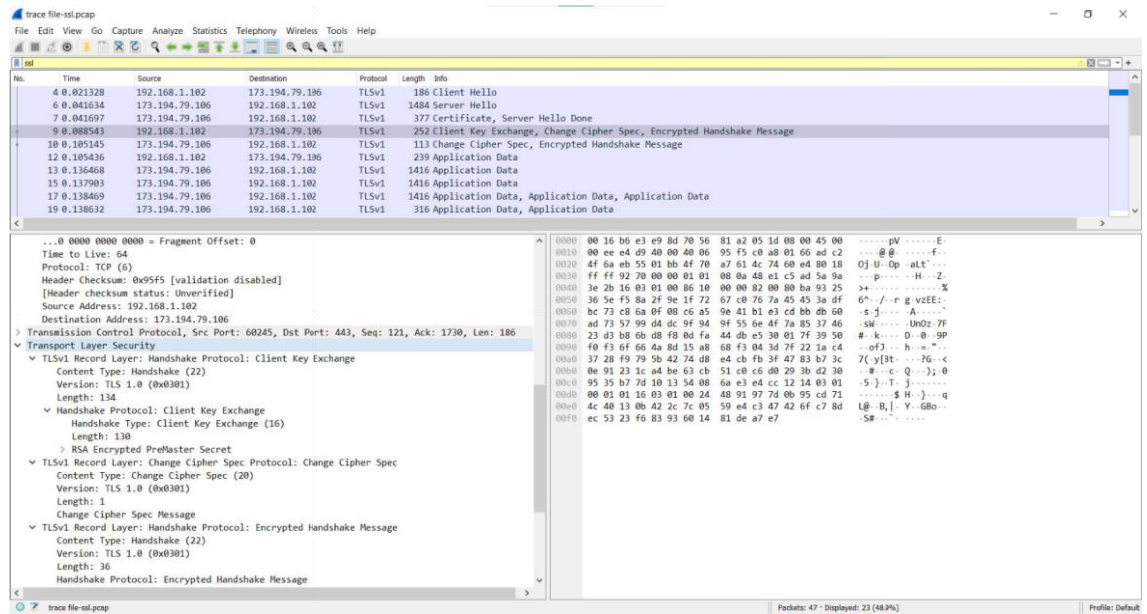


1. Who sends the Change Cipher Spec message, the client, the server, or both?

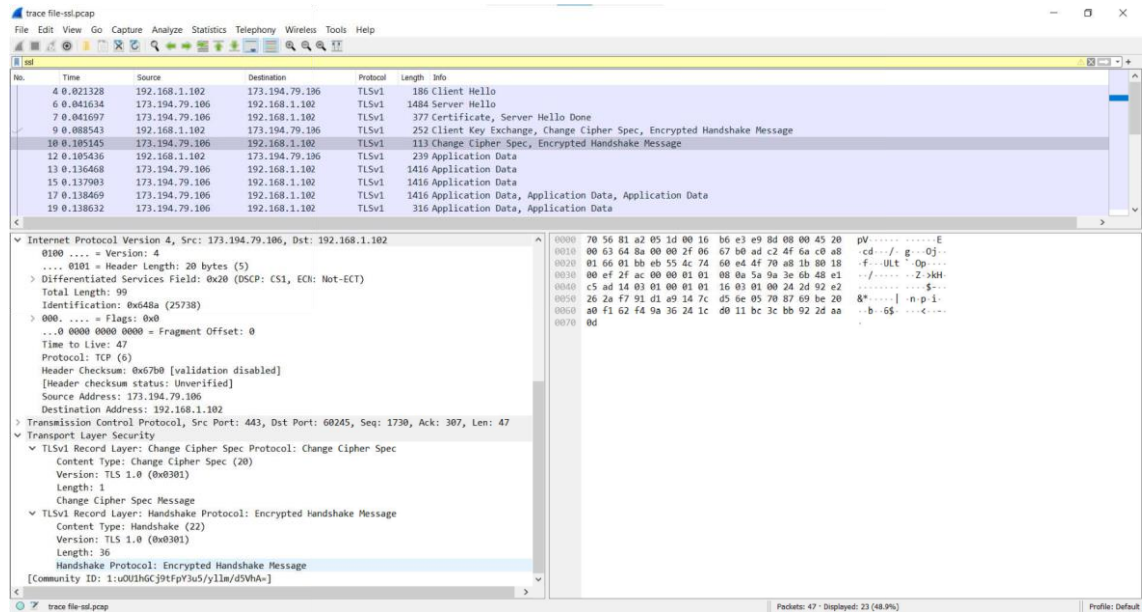
Ans:

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

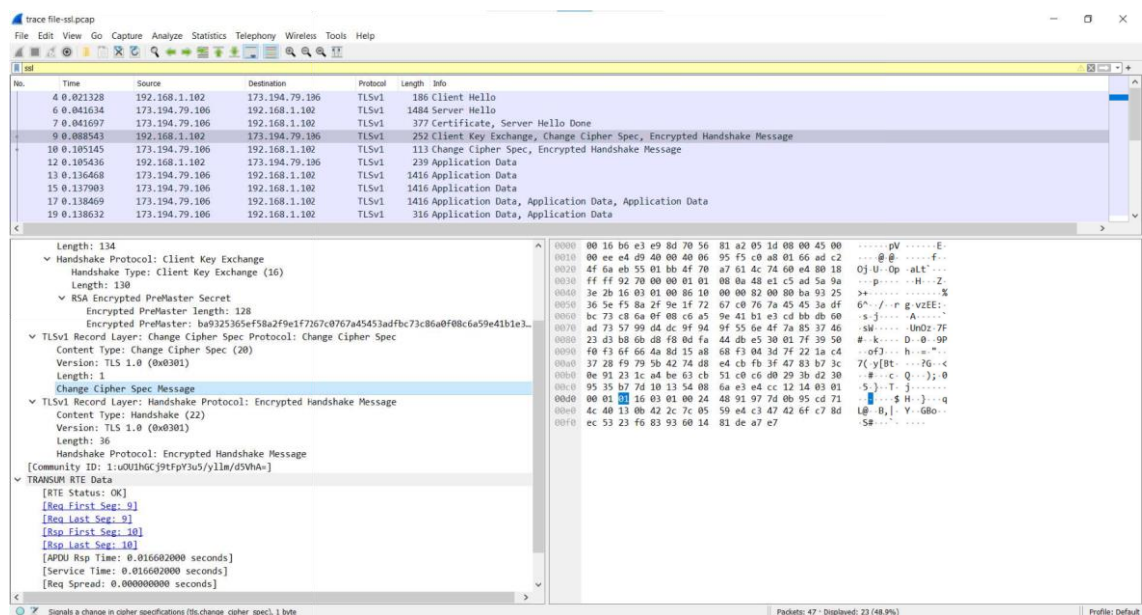
Client:

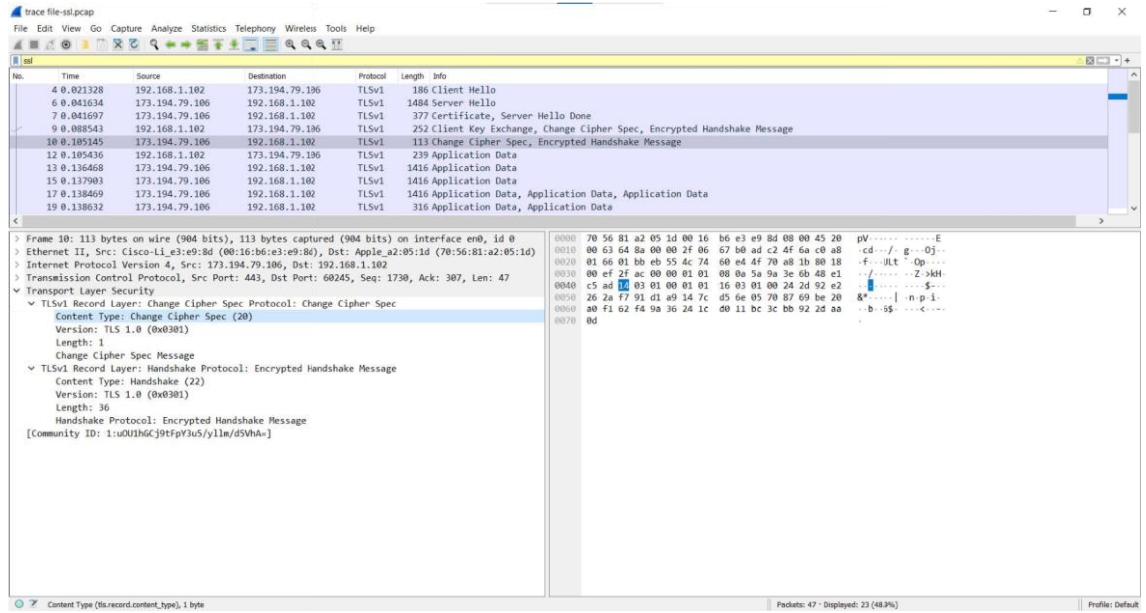


Server:



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:





## Conclusion:

Performed the experiment successfully.

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