SEM - VII - 2022-23

CNS Lab

B1 - 2019BTECS00094 - Sweety Shrawan Gupta

Assignment 16

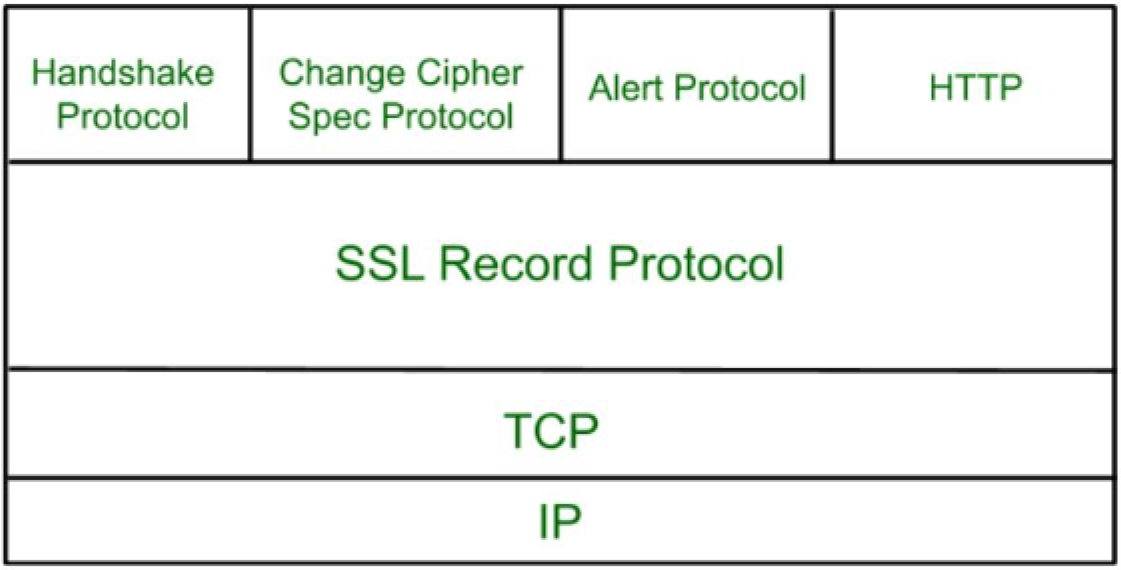
Title:- SSL/TLS Handshake Analysis using Wireshark

Aim:- To observe SSL/TLS (Secure Sockets Layer / Transport Layer Security) in action.

Theory:-

- SSL/TLS is used to secure TCP connections, and it is widely used as part of the secure web: HTTPS is SSL over HTTP .
- Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server.
- SSL encrypts the link between a web server and a browser which ensures that all data passed between them remains private and free from attack.
- Secure Socket Layer Protocols:
    a. SSL record protocol
    b. Handshake protocol
    c. Change-cipher spec protocol
    d. Alert protocol

SSL Protocol Stack:



Objectives of SSL

The goals of SSL are as follows –

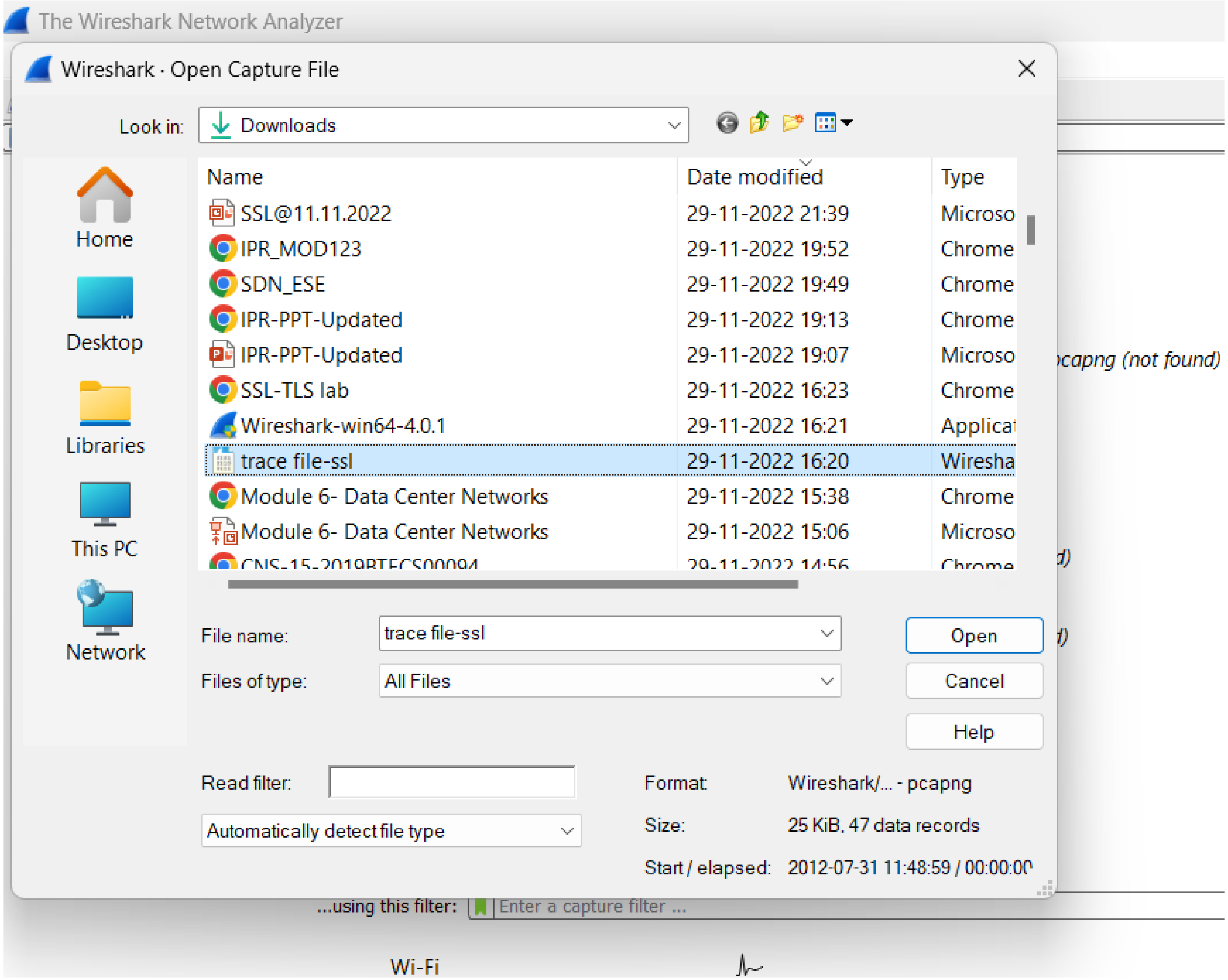
- ***Data integrity*** – Information is safe from tampering. The SSL Record Protocol, SSL Handshake Protocol, SSL Change CipherSpec Protocol, and SSL Alert Protocol maintain data privacy.
- ***Client-server authentication*** – The SSL protocol authenticates the client and server using standard cryptographic procedures.
- SSL is the forerunner of Transport Layer Security (TLS), a cryptographic technology for secure data transfer over the Internet.

- Wireshark is a free and open-source packet analyzer.
- It is used for network troubleshooting, analysis, software and communications protocol development, and education.

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



The Wireshark Network Analyzer

Wireshark · Open Capture File

Look in: Downloads

Name	Date modified	Type
SSL@11.11.2022	29-11-2022 21:39	Microso
IPR_MOD123	29-11-2022 19:52	Chrome
SDN_ESE	29-11-2022 19:49	Chrome
IPR-PPT-Updated	29-11-2022 19:13	Chrome
IPR-PPT-Updated	29-11-2022 19:07	Microso
SSL-TLS lab	29-11-2022 16:23	Chrome
Wireshark-win64-4.0.1	29-11-2022 16:21	Applicat
trace file-ssl	29-11-2022 16:20	Wiresha
Module 6- Data Center Networks	29-11-2022 15:38	Chrome
Module 6- Data Center Networks	29-11-2022 15:06	Microso
CNS-15-2019BTECS00094	29-11-2022 14:56	Chrome

File name: trace file-ssl

Files of type: All Files

Read filter:

Automatically detect file type

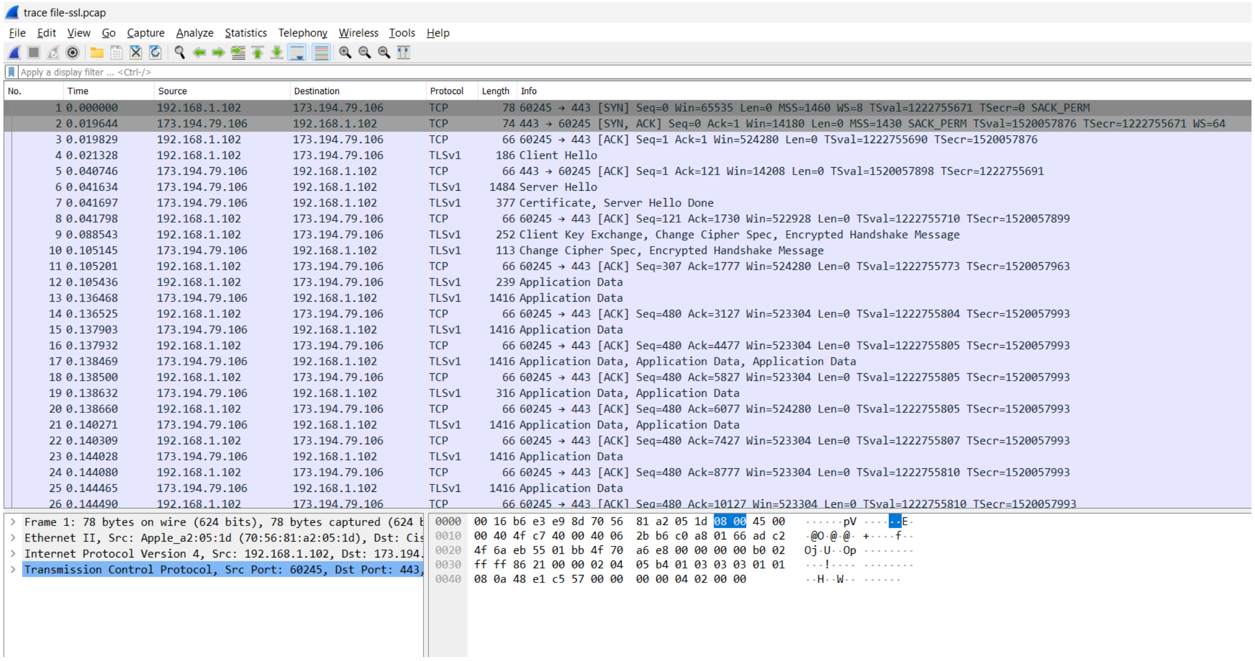
Format: Wireshark/... - pcapng

Size: 25 KiB, 47 data records

Start / elapsed: 2012-07-31 11:48:59 / 00:00:00

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

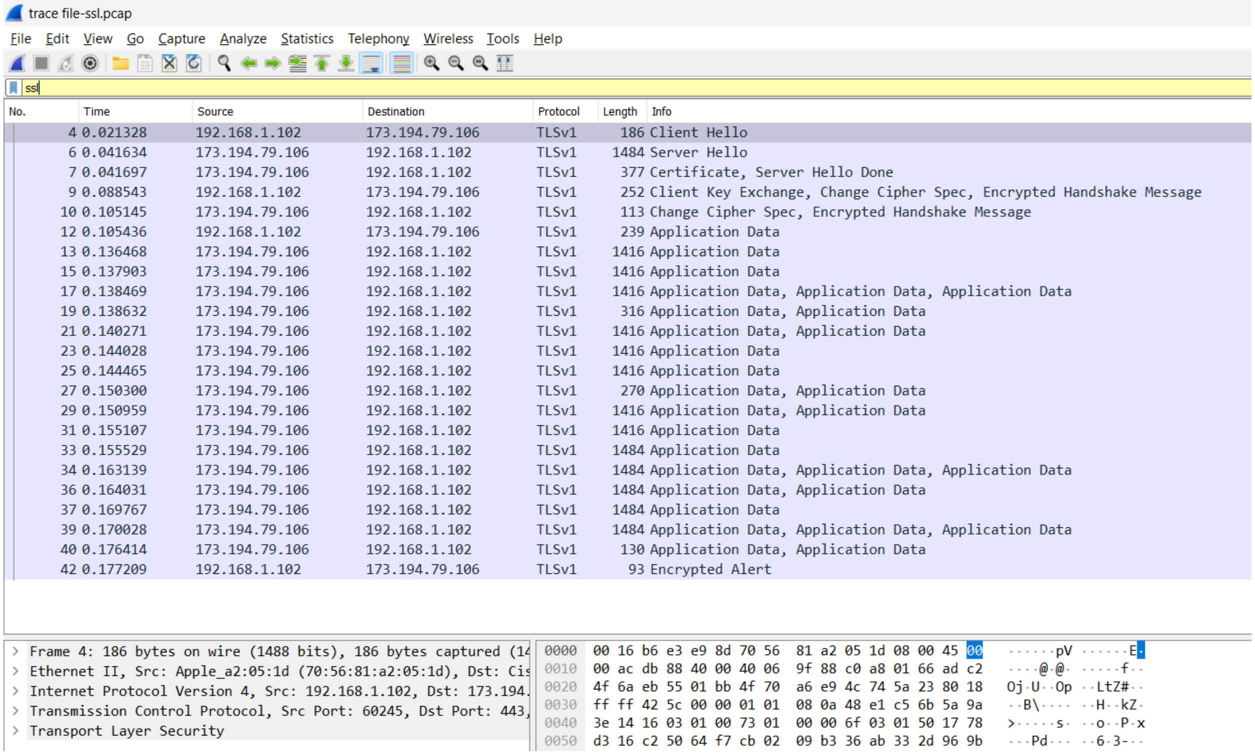

trace file-ssl.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
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
  22 0.140309  192.168.1.102   173.194.79.106  TCP        66 60245 → 443 [ACK] Seq=480 Ack=7427 Win=523304 Len=0 TSval=1222755807 TSecr=1520057993
  23 0.144028  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
  24 0.144080  192.168.1.102   173.194.79.106  TCP        66 60245 → 443 [ACK] Seq=480 Ack=8777 Win=523304 Len=0 TSval=1222755810 TSecr=1520057993
  25 0.144465  173.194.79.106  192.168.1.102   TLSv1    1416 Application Data
  26 0.144490  192.168.1.102   173.194.79.106  TCP        66 60245 → 443 [ACK] Seq=480 Ack=10127 Win=523304 Len=0 TSval=1222755810 TSecr=1520057993
```

```
> Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 b
> Ethernet II, Src: Apple_a2:05:1d (70:56:81:a2:05:1d), Dst: Cis
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 173.194.
> Transmission Control Protocol, Src Port: 60245, Dst Port: 443,
```

```
0000  00 16 b6 e3 e9 8d 70 56  81 a2 05 1d 08 00 45 00   ······pV ······E·
0010  00 40 4f c7 40 00 40 06  2b b6 c0 a8 01 66 ad c2   ·@O·@·@· +····f··
0020  4f 6a eb 55 01 bb 4f 70  a6 e8 00 00 00 00 b0 02   Oj·U··Op ········
0030  ff ff 86 21 00 00 02 04  05 b4 01 03 03 03 01 01   ···!···· ········
0040  08 0a 48 e1 c5 57 00 00  00 00 04 02 00 00         ··H··W·· ······
```

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
```

```
> Frame 4: 186 bytes on wire (1488 bits), 186 bytes captured (14
> Ethernet II, Src: Apple_a2:05:1d (70:56:81:a2:05:1d), Dst: Cis
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 173.194.
> Transmission Control Protocol, Src Port: 60245, Dst Port: 443,
> Transport Layer Security
```

```
0000  00 16 b6 e3 e9 8d 70 56  81 a2 05 1d 08 00 45 00   ······pV ······E·
0010  00 ac db 88 40 00 40 06  9f 88 c0 a8 01 66 ad c2   ····@·@· ·····f··
0020  4f 6a eb 55 01 bb 4f 70  a6 e9 4c 74 5a 23 80 18   Oj·U··Op ··LtZ#··
0030  ff ff 42 5c 00 00 01 01  08 0a 48 e1 c5 6b 5a 9a   ··B\···· ··H··kZ·
0040  3e 14 16 03 01 00 73 01  00 00 6f 03 01 50 17 78   >·····s· ··o··P·x
0050  d3 16 c2 50 64 f7 cb 02  09 b3 36 ab 33 2d 96 9b   ···Pd··· ··6·3-··
```

- 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.

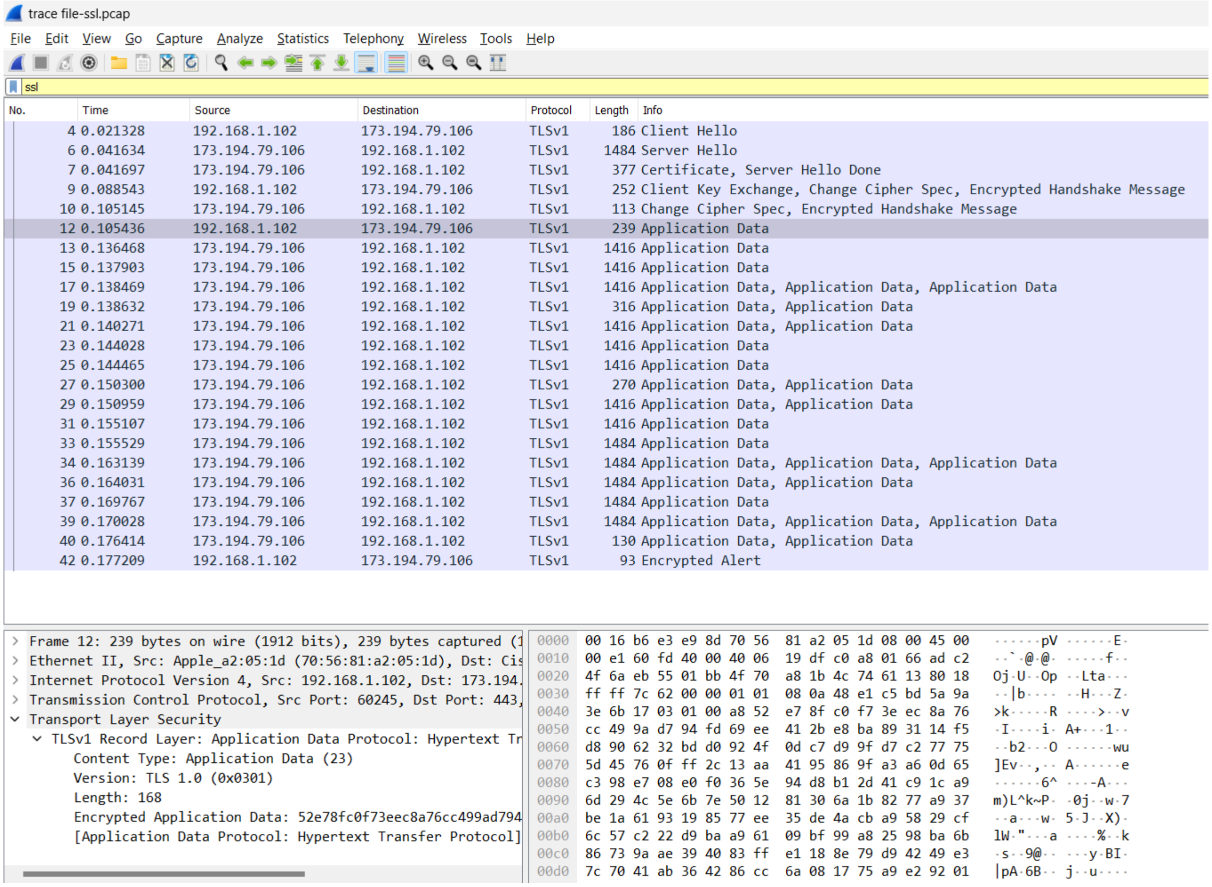
  Last comes the contents of the record. Application Data records are sent after SSL has secured the connection, so the contents will show up as encrypted data.

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.

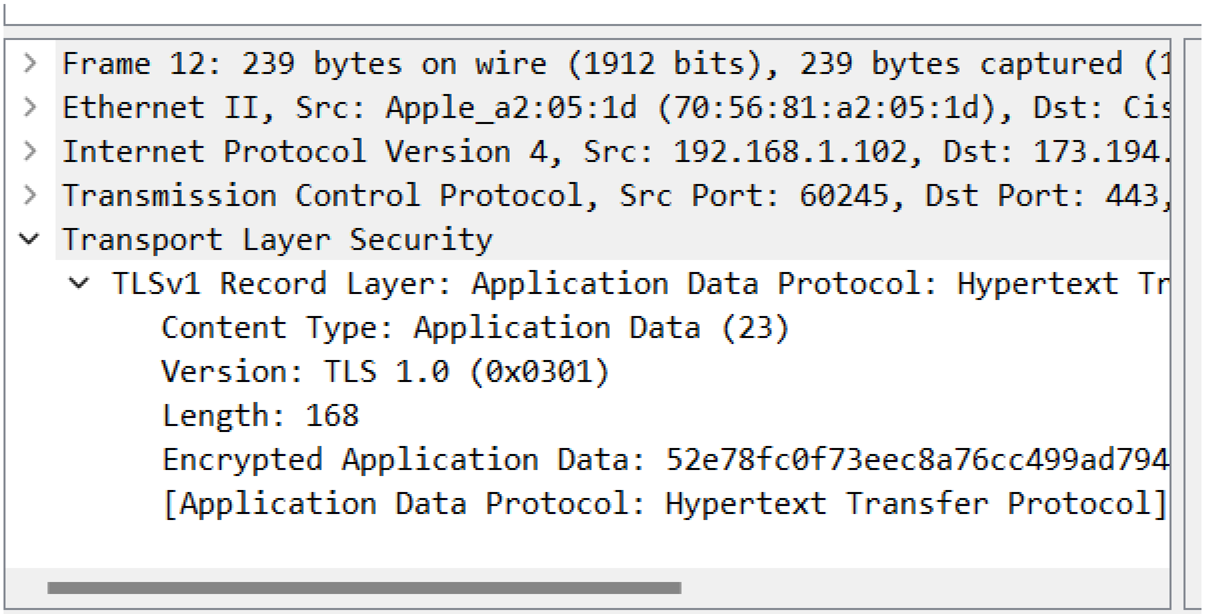

trace file-ssl.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

```
> Frame 12: 239 bytes on wire (1912 bits), 239 bytes captured (1
> Ethernet II, Src: Apple_a2:05:1d (70:56:81:a2:05:1d), Dst: Cis
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 173.194.
> Transmission Control Protocol, Src Port: 60245, Dst Port: 443,
v Transport Layer Security
  v TLSv1 Record Layer: Application Data Protocol: Hypertext Tr
      Content Type: Application Data (23)
      Version: TLS 1.0 (0x0301)
      Length: 168
      Encrypted Application Data: 52e78fc0f73eec8a76cc499ad794
      [Application Data Protocol: Hypertext Transfer Protocol]
```

```
0000  00 16 b6 e3 e9 8d 70 56  81 a2 05 1d 08 00 45 00   ······pV ······E·
0010  00 e1 60 fd 40 00 40 06  19 df c0 a8 01 66 ad c2   ··`·@·@· ·····f··
0020  4f 6a eb 55 01 bb 4f 70  a8 1b 4c 74 61 13 80 18   Oj·U··Op ··Lta···
0030  ff ff 7c 62 00 00 01 01  08 0a 48 e1 c5 bd 5a 9a   ··|b···· ··H···Z·
0040  3e 6b 17 03 01 00 a8 52  e7 8f c0 f7 3e ec 8a 76   >k·····R ····>··v
0050  cc 49 9a d7 94 fd 69 ee  41 2b e8 ba 89 31 14 f5   ·I····i· A+···1··
0060  d8 90 62 32 bd d0 92 4f  0d c7 d9 9f d7 c2 77 75   ··b2···O ······wu
0070  5d 45 76 0f ff 2c 13 aa  41 95 86 9f a3 a6 0d 65   ]Ev··,·· A······e
0080  c3 98 e7 08 e0 f0 36 5e  94 d8 b1 2d 41 c9 1c a9   ······6^ ···-A···
0090  6d 29 4c 5e 6b 7e 50 12  81 30 6a 1b 82 77 a9 37   m)L^k~P· ·0j··w·7
00a0  be 1a 61 93 19 85 77 ee  35 de 4a cb a9 58 29 cf   ··a···w· 5·J··X)·
00b0  6c 57 c2 22 d9 ba a9 61  09 bf 99 a8 25 98 ba 6b   lW·"···a ····%··k
00c0  86 73 9a ae 39 40 83 ff  e1 18 8e 79 d9 42 49 e3   ·s··9@·· ···y·BI·
00d0  7c 70 41 ab 36 42 86 cc  6a 08 17 75 a9 e2 92 01   |pA·6B·· j··u····
```

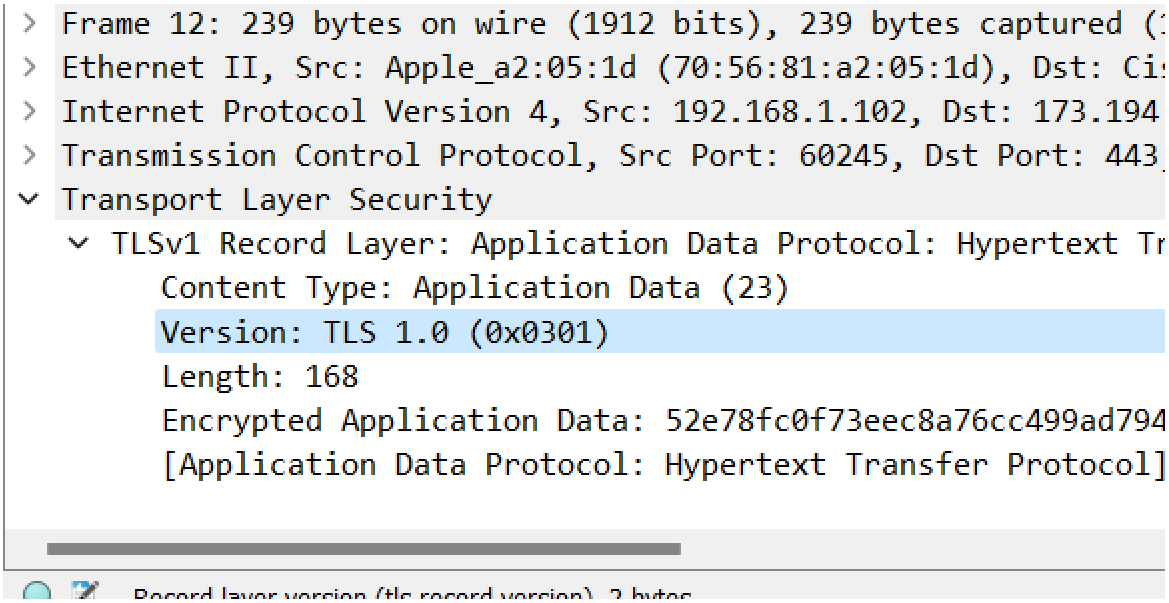


```
> Frame 12: 239 bytes on wire (1912 bits), 239 bytes captured (1
> Ethernet II, Src: Apple_a2:05:1d (70:56:81:a2:05:1d), Dst: Cis
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 173.194.
> Transmission Control Protocol, Src Port: 60245, Dst Port: 443,
v Transport Layer Security
    v TLSv1 Record Layer: Application Data Protocol: Hypertext Tr
        Content Type: Application Data (23)
        Version: TLS 1.0 (0x0301)
        Length: 168
        Encrypted Application Data: 52e78fc0f73eec8a76cc499ad794
        [Application Data Protocol: Hypertext Transfer Protocol]
```

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



```
> Frame 12: 239 bytes on wire (1912 bits), 239 bytes captured (
> Ethernet II, Src: Apple_a2:05:1d (70:56:81:a2:05:1d), Dst: Ci
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 173.194
> Transmission Control Protocol, Src Port: 60245, Dst Port: 443
v Transport Layer Security
  v TLSv1 Record Layer: Application Data Protocol: Hypertext Tr
      Content Type: Application Data (23)
      Version: TLS 1.0 (0x0301)
      Length: 168
      Encrypted Application Data: 52e78fc0f73eec8a76cc499ad794
      [Application Data Protocol: Hypertext Transfer Protocol]
```

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

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.

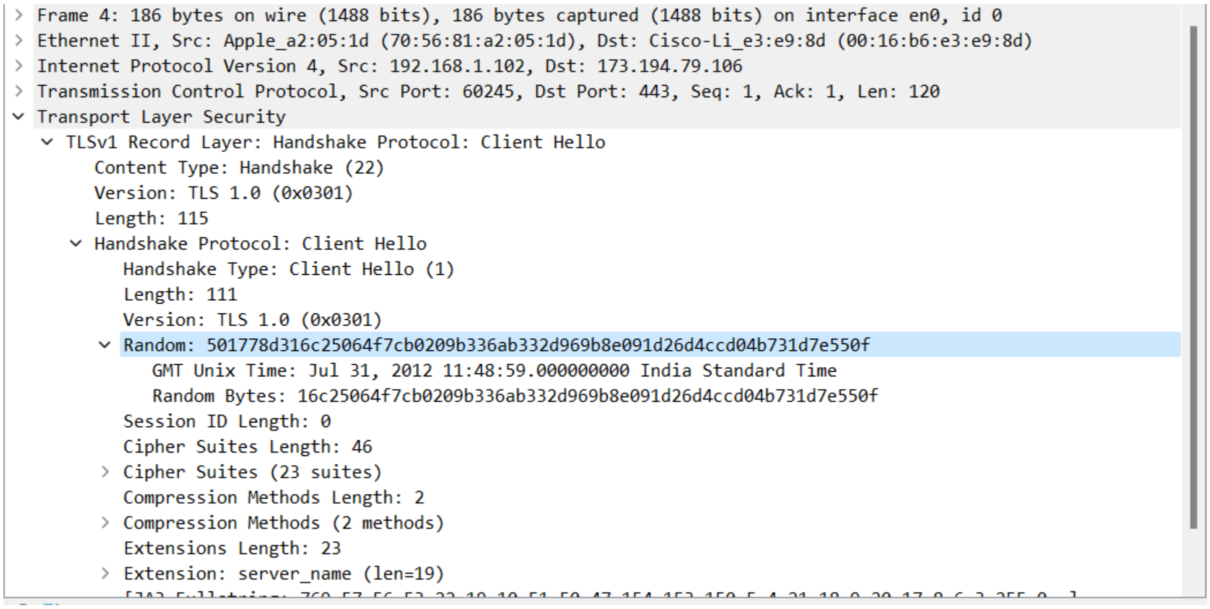
Hello Message

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 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.

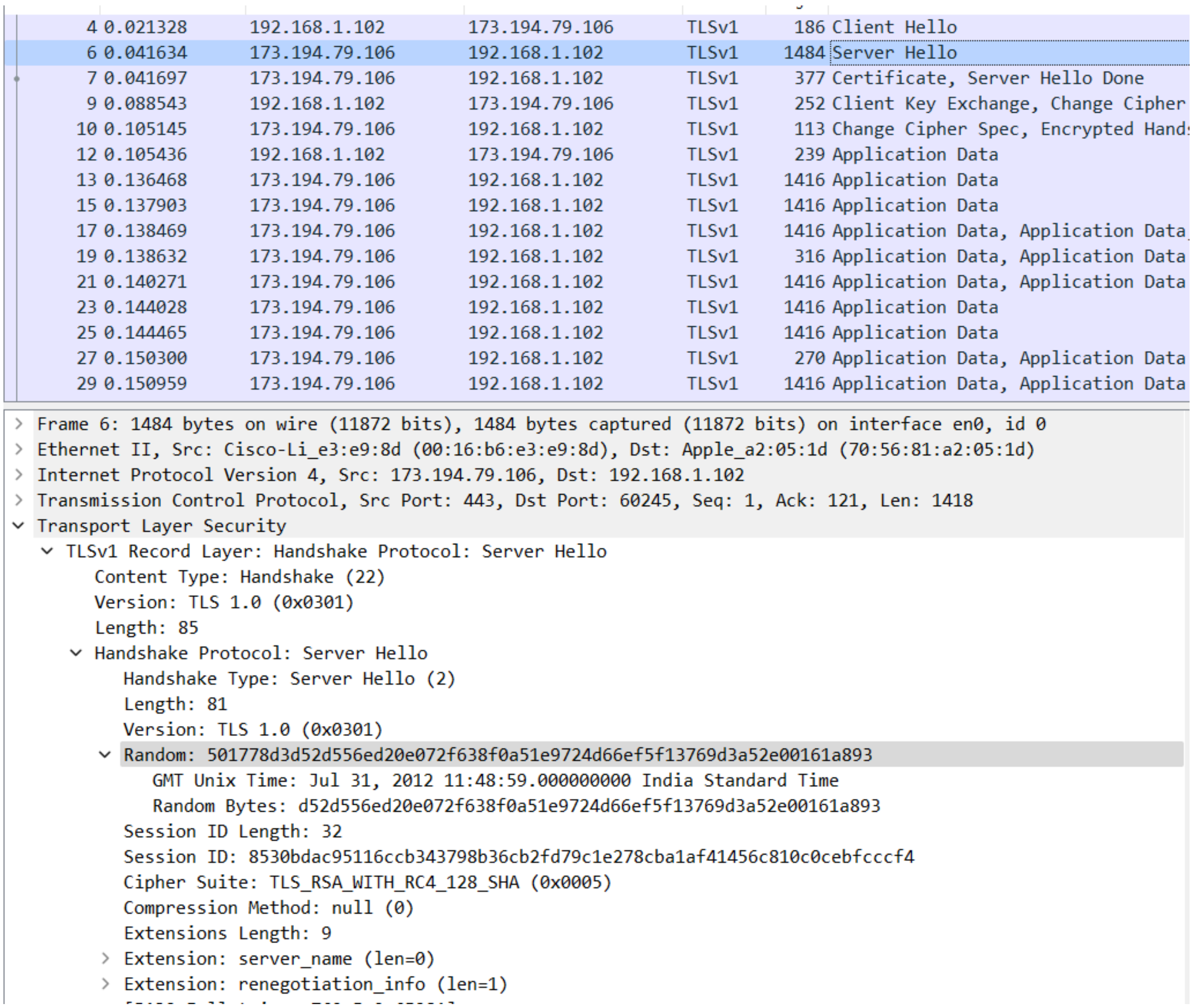
Ans:

Client:



```
> Frame 4: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface en0, id 0
> Ethernet II, Src: Apple_a2:05:1d (70:56:81:a2:05:1d), Dst: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 173.194.79.106
> Transmission Control Protocol, Src Port: 60245, Dst Port: 443, Seq: 1, Ack: 1, Len: 120
v Transport Layer Security
  v TLSv1 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 115
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 111
        Version: TLS 1.0 (0x0301)
      v Random: 501778d316c25064f7cb0209b336ab332d969b8e091d26d4ccd04b731d7e550f
          GMT Unix Time: Jul 31, 2012 11:48:59.000000000 India Standard Time
          Random Bytes: 16c25064f7cb0209b336ab332d969b8e091d26d4ccd04b731d7e550f
        Session ID Length: 0
        Cipher Suites Length: 46
      > Cipher Suites (23 suites)
        Compression Methods Length: 2
      > Compression Methods (2 methods)
        Extensions Length: 23
      > Extension: server_name (len=19)
        [JA3 Fullstring: 769,57-56-53-22-19-10-51-50-47-154-153-150-5-4-21-18-9-20-17-8-6-3-255,0,...]
```

Server:



```
   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
  10 0.105145   173.194.79.106   192.168.1.102    TLSv1    113 Change Cipher Spec, Encrypted Hand:
  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,
  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
```

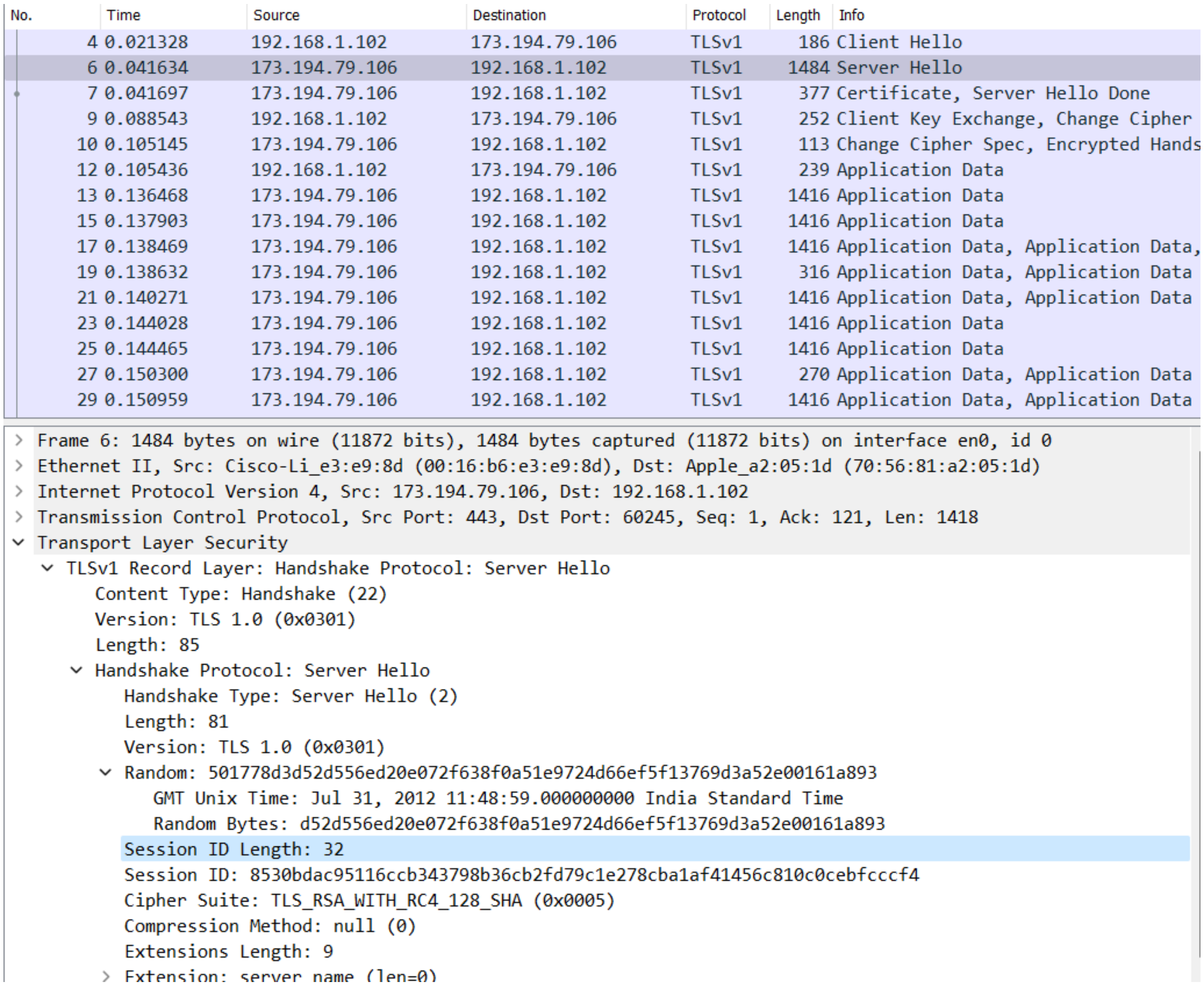
```
> Frame 6: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 bits) on interface en0, id 0
> Ethernet II, Src: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d), Dst: Apple_a2:05:1d (70:56:81:a2:05:1d)
> Internet Protocol Version 4, Src: 173.194.79.106, Dst: 192.168.1.102
> Transmission Control Protocol, Src Port: 443, Dst Port: 60245, Seq: 1, Ack: 121, Len: 1418
v Transport Layer Security
  v TLSv1 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 85
    v Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 81
        Version: TLS 1.0 (0x0301)
      v 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)
```

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 if Session ID is 32

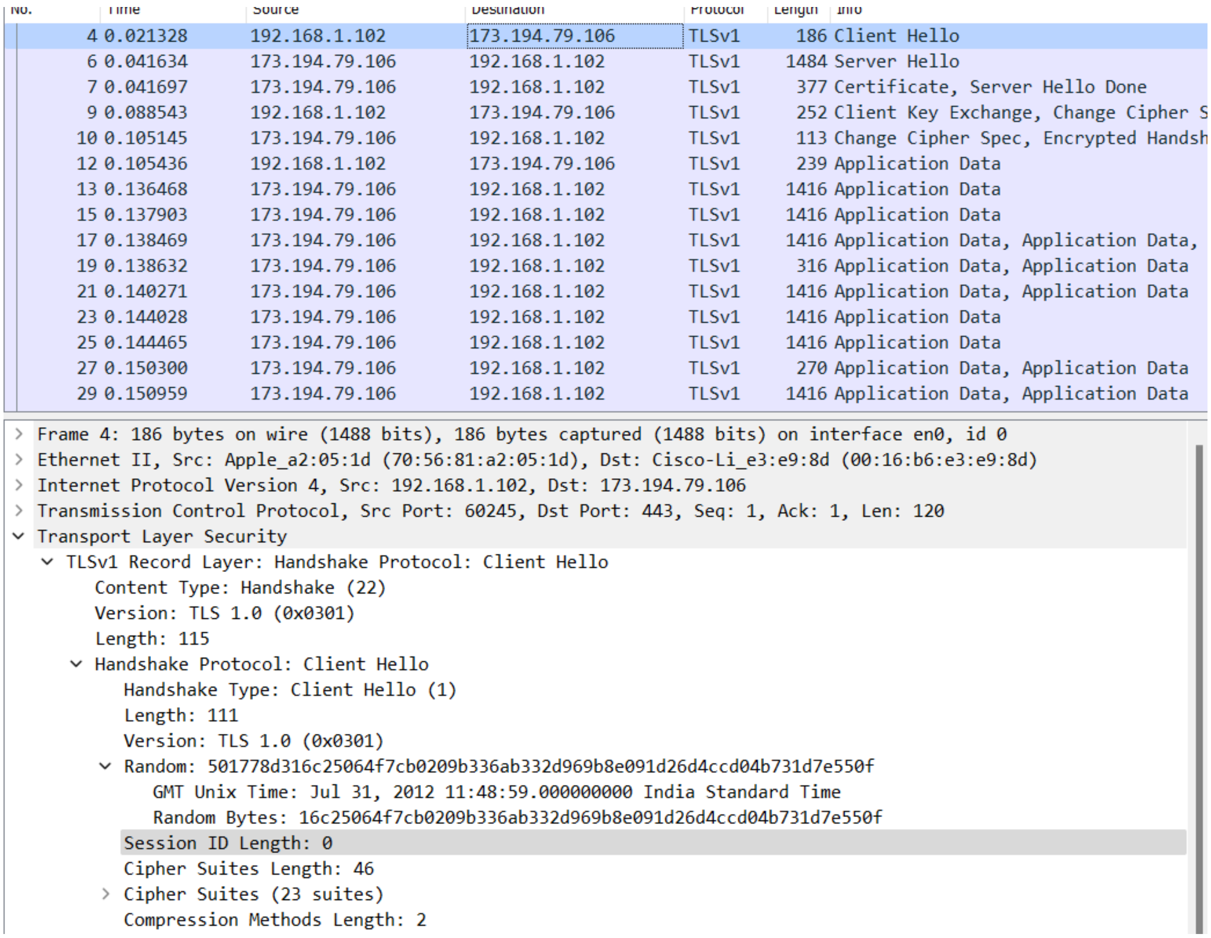


No.	Time	Source	Destination	Protocol	Length	Info
4	0.021328	192.168.1.102	173.194.79.106	TLSv1	186	Client Hello
6	0.041634	173.194.79.106	192.168.1.102	TLSv1	1484	Server Hello
7	0.041697	173.194.79.106	192.168.1.102	TLSv1	377	Certificate, Server Hello Done
9	0.088543	192.168.1.102	173.194.79.106	TLSv1	252	Client Key Exchange, Change Cipher
10	0.105145	173.194.79.106	192.168.1.102	TLSv1	113	Change Cipher Spec, Encrypted Hands
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,
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

```
> Frame 6: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 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: 1, Ack: 121, Len: 1418
v Transport Layer Security
  v TLSv1 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 85
    v Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 81
        Version: TLS 1.0 (0x0301)
      v 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)
```

Client:

Length of Session ID is 0



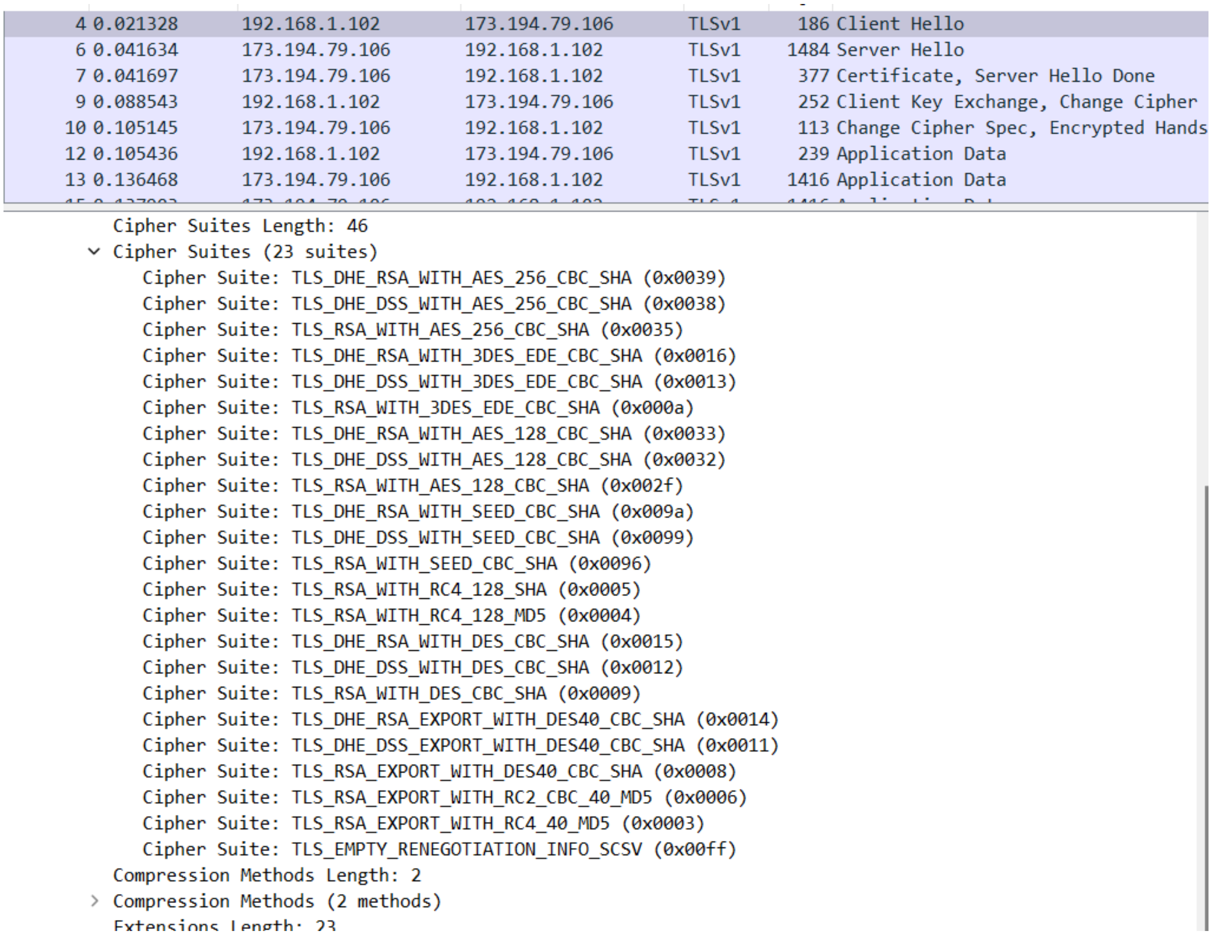
```
No.  Time       Source          Destination     Protocol  Length Info
   4 0.021328   192.168.1.102   173.194.79.106  TLSv1      186 Client Hello
   6 0.041634   173.194.79.106  192.168.1.102   TLSv1     1484 Server Hello
   7 0.041697   173.194.79.106  192.168.1.102   TLSv1      377 Certificate, Server Hello Done
   9 0.088543   192.168.1.102   173.194.79.106  TLSv1      252 Client Key Exchange, Change Cipher S
  10 0.105145   173.194.79.106  192.168.1.102   TLSv1      113 Change Cipher Spec, Encrypted Handsh
  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,
  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
```

```
> Frame 4: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface en0, id 0
> Ethernet II, Src: Apple_a2:05:1d (70:56:81:a2:05:1d), Dst: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 173.194.79.106
> Transmission Control Protocol, Src Port: 60245, Dst Port: 443, Seq: 1, Ack: 1, Len: 120
v Transport Layer Security
  v TLSv1 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 115
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 111
        Version: TLS 1.0 (0x0301)
      v Random: 501778d316c25064f7cb0209b336ab332d969b8e091d26d4ccd04b731d7e550f
          GMT Unix Time: Jul 31, 2012 11:48:59.000000000 India Standard Time
          Random Bytes: 16c25064f7cb0209b336ab332d969b8e091d26d4ccd04b731d7e550f
        Session ID Length: 0
        Cipher Suites Length: 46
      > Cipher Suites (23 suites)
        Compression Methods Length: 2
```

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:

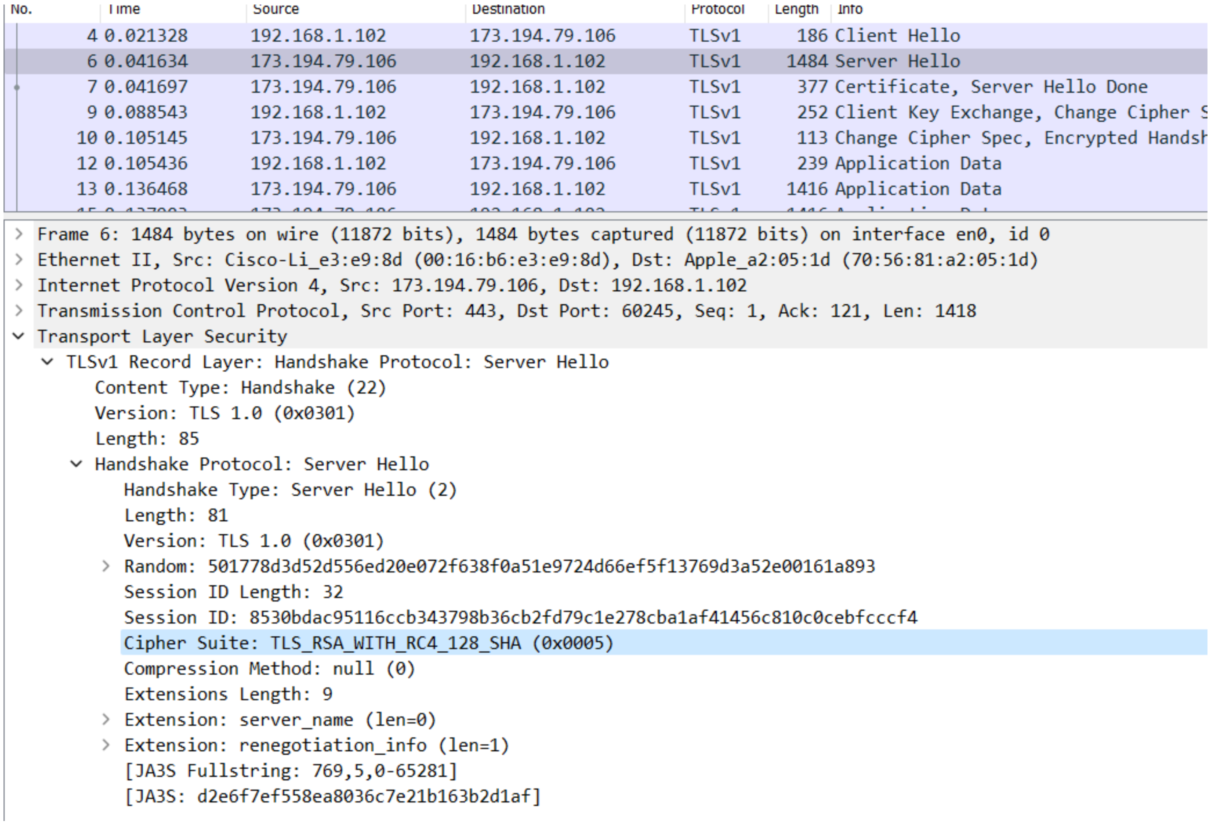
Client:



```
  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
 10 0.105145   173.194.79.106  192.168.1.102    TLSv1    113 Change Cipher Spec, Encrypted Hands
 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
```

```
    Cipher Suites Length: 46
  ˅ Cipher Suites (23 suites)
      Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
      Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
      Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
      Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
      Cipher Suite: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
      Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
      Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
      Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
      Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
      Cipher Suite: TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x009a)
      Cipher Suite: TLS_DHE_DSS_WITH_SEED_CBC_SHA (0x0099)
      Cipher Suite: TLS_RSA_WITH_SEED_CBC_SHA (0x0096)
      Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
      Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
      Cipher Suite: TLS_DHE_RSA_WITH_DES_CBC_SHA (0x0015)
      Cipher Suite: TLS_DHE_DSS_WITH_DES_CBC_SHA (0x0012)
      Cipher Suite: TLS_RSA_WITH_DES_CBC_SHA (0x0009)
      Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0x0014)
      Cipher Suite: TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA (0x0011)
      Cipher Suite: TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0x0008)
      Cipher Suite: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x0006)
      Cipher Suite: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x0003)
      Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
    Compression Methods Length: 2
  › Compression Methods (2 methods)
    Extensions Length: 23
```

Server:



```
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 S
         10 0.105145      173.194.79.106    192.168.1.102     TLSv1       113 Change Cipher Spec, Encrypted Handsh
         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

> Frame 6: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 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: 1, Ack: 121, Len: 1418
v Transport Layer Security
  v TLSv1 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 85
    v Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 81
        Version: TLS 1.0 (0x0301)
      > Random: 501778d3d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893
        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)
        [JA3S Fullstring: 769,5,0-65281]
        [JA3S: d2e6f7ef558ea8036c7e21b163b2d1af]
```

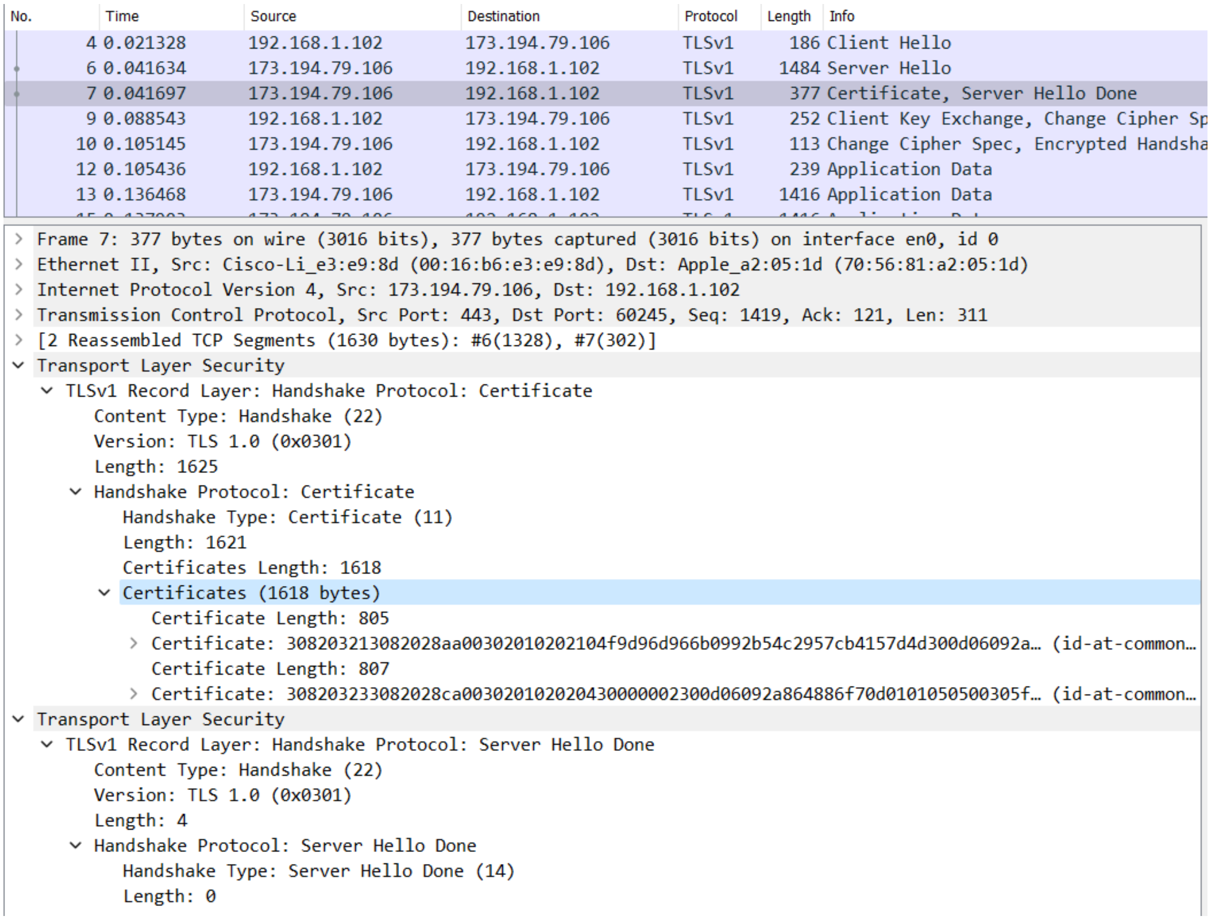
Certificate Messages:

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



```
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 Sp
        10 0.105145    173.194.79.106   192.168.1.102    TLSv1      113 Change Cipher Spec, Encrypted Handsha
        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
```

```
> Frame 7: 377 bytes on wire (3016 bits), 377 bytes captured (3016 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: 1419, Ack: 121, Len: 311
> [2 Reassembled TCP Segments (1630 bytes): #6(1328), #7(302)]
v Transport Layer Security
  v TLSv1 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 1625
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 1621
        Certificates Length: 1618
      v Certificates (1618 bytes)
          Certificate Length: 805
        > Certificate: 308203213082028aa00302010202104f9d96d966b0992b54c2957cb4157d4d300d06092a… (id-at-common…
          Certificate Length: 807
        > Certificate: 308203233082028ca003020102020430000002300d06092a864886f70d0101050500305f… (id-at-common…
v Transport Layer Security
  v TLSv1 Record Layer: Handshake Protocol: Server Hello Done
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 4
    v Handshake Protocol: Server Hello Done
        Handshake Type: Server Hello Done (14)
        Length: 0
```

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

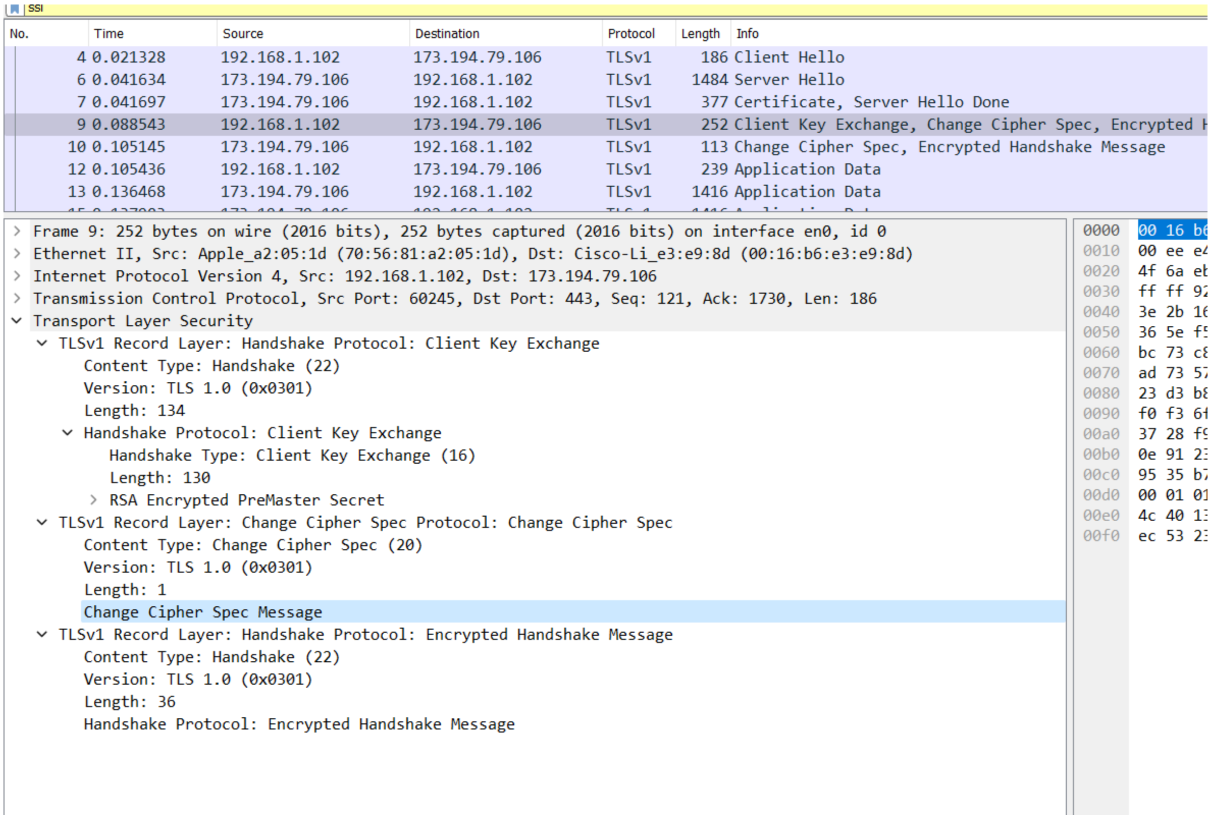
Find and inspect the details of the Client Key Exchange and Change Cipher messages, expanding their various details. The key exchange message is sent to pass keying information so that both sides will have the same secret session key. The change cipher message signal a switch to a new encryption scheme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

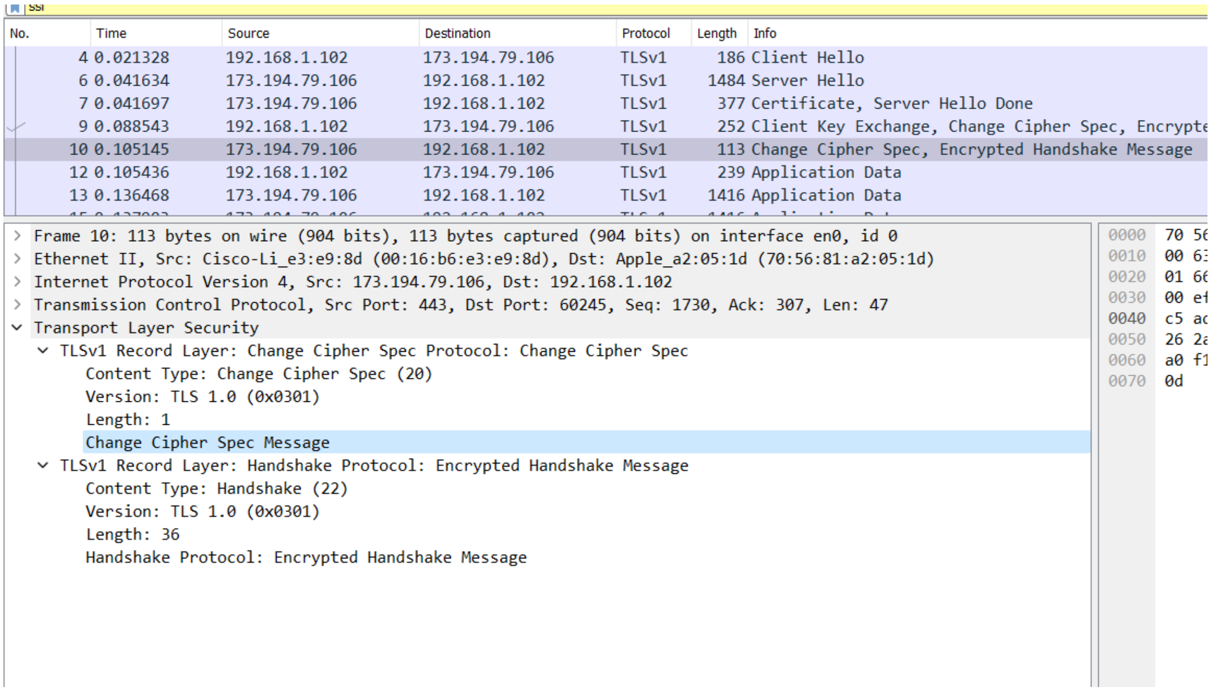


```
ssl
No.     Time       Source          Destination     Protocol  Length  Info
      4 0.021328   192.168.1.102   173.194.79.106  TLSv1      186 Client Hello
      6 0.041634   173.194.79.106  192.168.1.102   TLSv1     1484 Server Hello
      7 0.041697   173.194.79.106  192.168.1.102   TLSv1      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 H
     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
```

```
> Frame 9: 252 bytes on wire (2016 bits), 252 bytes captured (2016 bits) on interface en0, id 0
> Ethernet II, Src: Apple_a2:05:1d (70:56:81:a2:05:1d), Dst: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 173.194.79.106
> Transmission Control Protocol, Src Port: 60245, Dst Port: 443, Seq: 121, Ack: 1730, Len: 186
v Transport Layer Security
  v TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 134
    v Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 130
      > RSA Encrypted PreMaster Secret
  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  00 16 b
0010  00 ee e
0020  4f 6a e
0030  ff ff 9
0040  3e 2b 1
0050  36 5e f
0060  bc 73 c
0070  ad 73 5
0080  23 d3 b
0090  f0 f3 6
00a0  37 28 f
00b0  0e 91 2
00c0  95 35 b
00d0  00 01 0
00e0  4c 40 1
00f0  ec 53 2
```

Server:



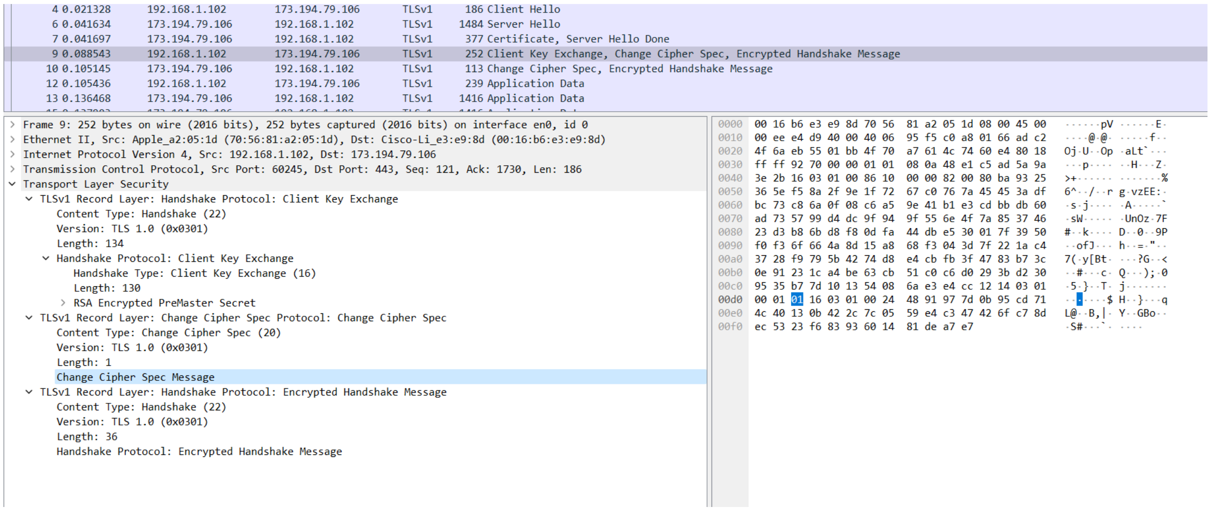
```
ssl
No.    Time       Source           Destination      Protocol  Length  Info
    4 0.021328    192.168.1.102    173.194.79.106   TLSv1      186 Client Hello
    6 0.041634    173.194.79.106   192.168.1.102    TLSv1     1484 Server Hello
    7 0.041697    173.194.79.106   192.168.1.102    TLSv1      377 Certificate, Server Hello Done
    9 0.088543    192.168.1.102    173.194.79.106   TLSv1      252 Client Key Exchange, Change Cipher Spec, Encrypte
   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
```

```
> 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
0010  00 63
0020  01 66
0030  00 ef
0040  c5 ac
0050  26 2a
0060  a0 f1
0070  0d
```

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.

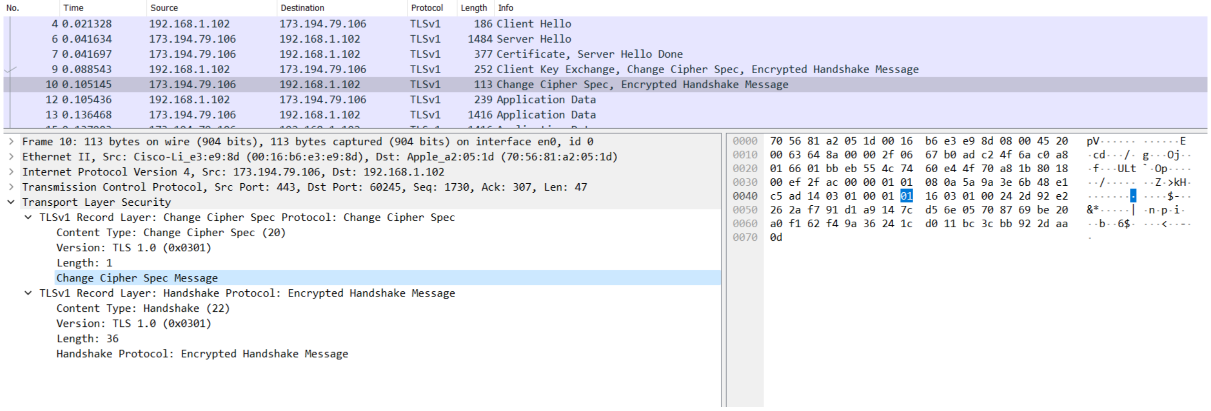
Ans:



```
    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
```

```
> Frame 9: 252 bytes on wire (2016 bits), 252 bytes captured (2016 bits) on interface en0, id 0
> Ethernet II, Src: Apple_a2:05:1d (70:56:81:a2:05:1d), Dst: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 173.194.79.106
> Transmission Control Protocol, Src Port: 60245, Dst Port: 443, Seq: 121, Ack: 1730, Len: 186
v Transport Layer Security
  v TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 134
    v Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 130
      > RSA Encrypted PreMaster Secret
  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  00 16 b6 e3 e9 8d 70 56  81 a2 05 1d 08 00 45 00   ······pV ······E·
0010  00 ee e4 d9 40 00 40 06  95 f5 c0 a8 01 66 ad c2   ····@·@· ·····f··
0020  4f 6a eb 55 01 bb 4f 70  a7 61 4c 74 60 e4 80 18   Oj·U··Op ·aLt`···
0030  ff ff 92 70 00 00 01 01  08 0a 48 e1 c5 ad 5a 9a   ···p···· ··H···Z·
0040  3e 2b 16 03 01 00 86 10  00 00 82 00 80 ba 93 25   >+······ ·······%
0050  36 5e f5 8a 2f 9e 1f 72  67 c0 76 7a 45 45 3a df   6^··/··r g·vzEE:·
0060  bc 73 c8 6a 0f 08 c6 a5  9e 41 b1 e3 cd bb db 60   ·s·j···· ·A·····`
0070  ad 73 57 99 d4 dc 9f 94  9f 55 6e 4f 7a 85 37 46   ·sW····· ·UnOz·7F
0080  23 d3 b8 6b d8 f8 0d fa  44 db e5 30 01 7f 39 50   #··k···· D··0··9P
0090  f0 f3 6f 66 4a 8d 15 a8  68 f3 04 3d 7f 22 1a c4   ··ofJ··· h··=·"··
00a0  37 28 f9 79 5b 42 74 d8  e4 cb fb 3f 47 83 b7 3c   7(·y[Bt· ···?G··<
00b0  0e 91 23 1c a4 be 63 cb  51 c0 c6 d0 29 3b d2 30   ··#···c· Q···);·0
00c0  95 35 b7 7d 10 13 54 08  6a e3 e4 cc 12 14 03 01   ·5·}··T· j·······
00d0  00 01 01 16 03 01 00 24  48 91 97 7d 0b 95 cd 71   ·······$ H··}···q
00e0  4c 40 13 0b 42 2c 7c 05  59 e4 c3 47 42 6f c7 8d   L@··B,|· Y··GBo··
00f0  ec 53 23 f6 83 93 60 14  81 de a7 e7               ·S#···`· ····
```



```
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
```

```
> 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                                                 ·
```

Conclusion:

Performed the experiment successfully.

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