Cryptography & Network Security Lab

PRN/ Roll No: 2019BTECS00090

Full name: Udaykumar Gadikar

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

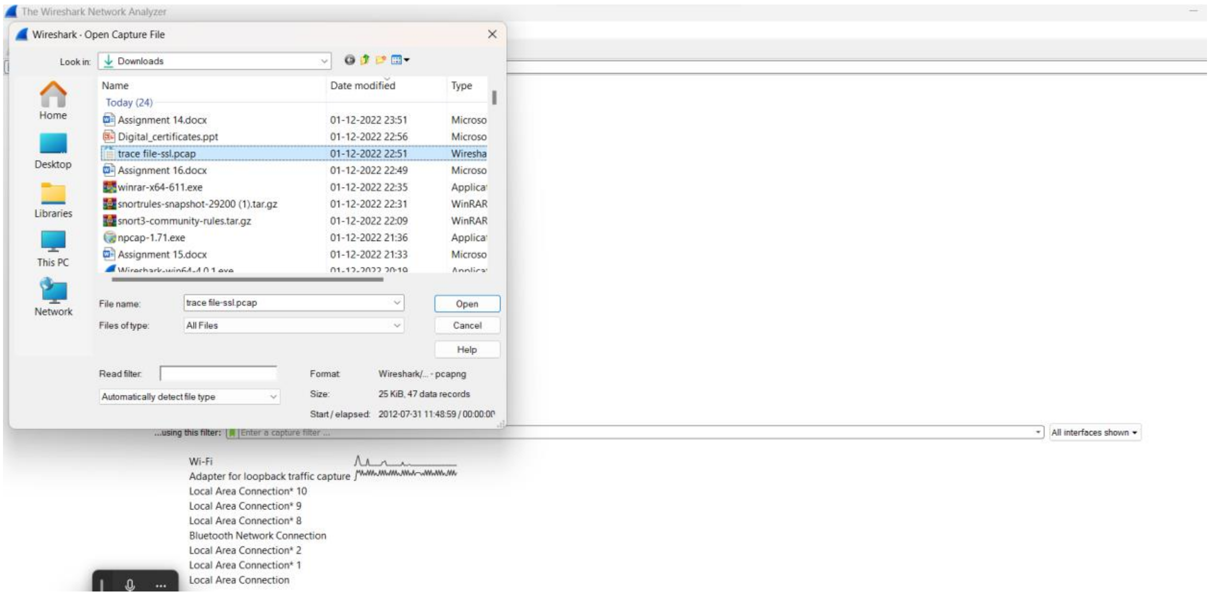
Theory:

- Wireshark is a free and open-source packet 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 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



Name	Date modified	Type
Today (24)		
Assignment 14.docx	01-12-2022 23:51	Microso
Digital_certificates.ppt	01-12-2022 22:56	Microso
trace file-ssl.pcap	01-12-2022 22:51	Wiresha
Assignment 16.docx	01-12-2022 22:49	Microso
winrar-x64-611.exe	01-12-2022 22:35	Applica
snortrules-snapshot-29200 (1).tar.gz	01-12-2022 22:31	WinRAR
snort3-community-rules.tar.gz	01-12-2022 22:09	WinRAR
npcap-1.71.exe	01-12-2022 21:36	Applica
Assignment 15.docx	01-12-2022 21:33	Microso
Wireshark-win64-4.0.1.exe	01-12-2022 20:19	Applica

File name: trace file-ssl.pcap

Files of type: All Files

Read filter:

Automatically detect file type

Format: Wireshark/... - pcapng

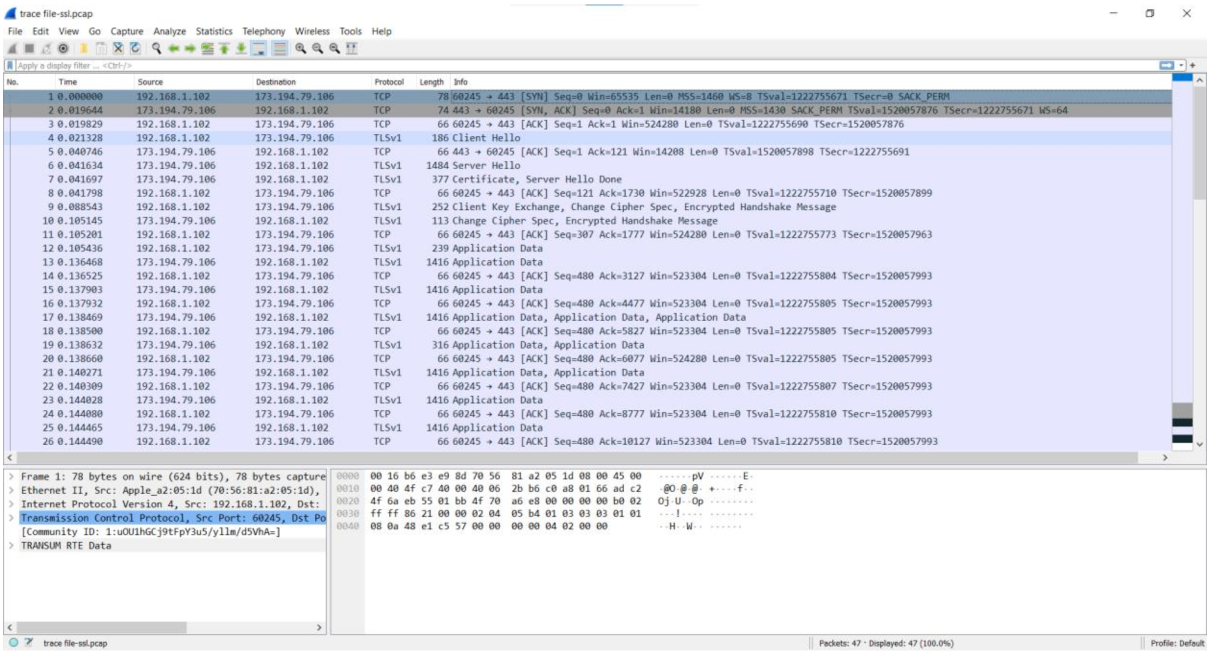
Size: 25 KiB, 47 data records

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

...using this filter: Enter a capture filter ...

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

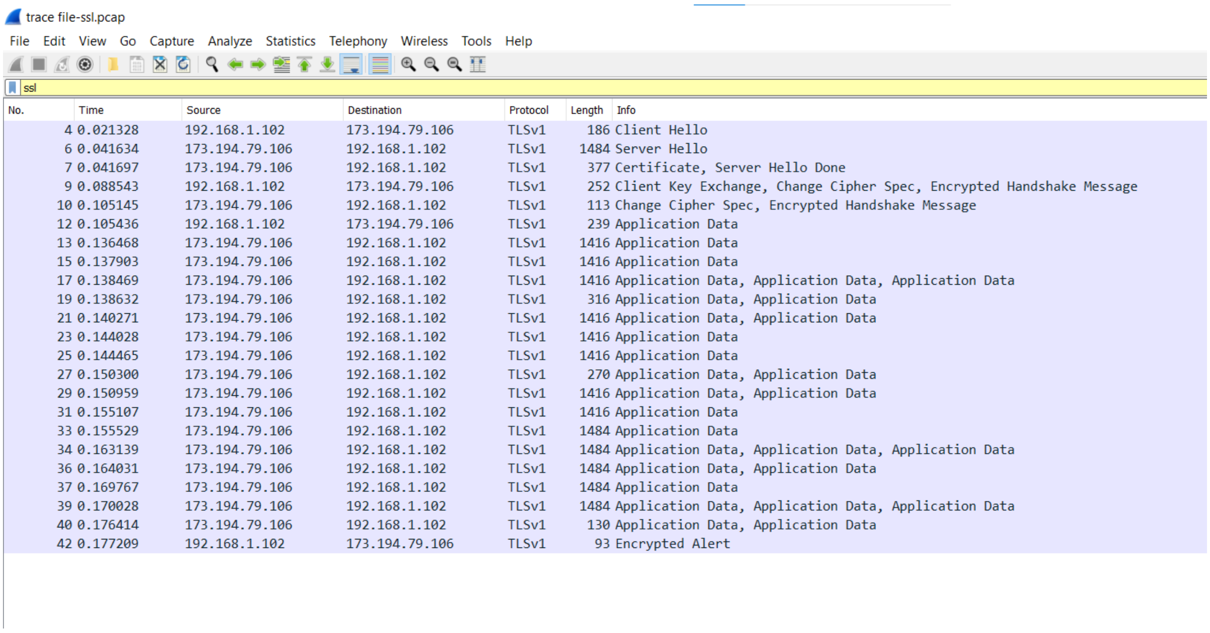


```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  192.168.1.102   173.194.79.106  TCP        78 60245 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=8 TSval=1222755671 TSecr=0 SACK_PERM
   2 0.019644  173.194.79.106  192.168.1.102   TCP        74 443 → 60245 [SYN, 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 capture
> Ethernet II, Src: Apple_a2:05:1d (70:56:81:a2:05:1d),
> Internet Protocol Version 4, Src: 192.168.1.102, Dst:
> Transmission Control Protocol, Src Port: 60245, Dst Po
  [Community ID: 1:uOU1hGCj9tFpY3u5/yllm/d5VhA=]
> TRANSUM RTE Data
```

```
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
```

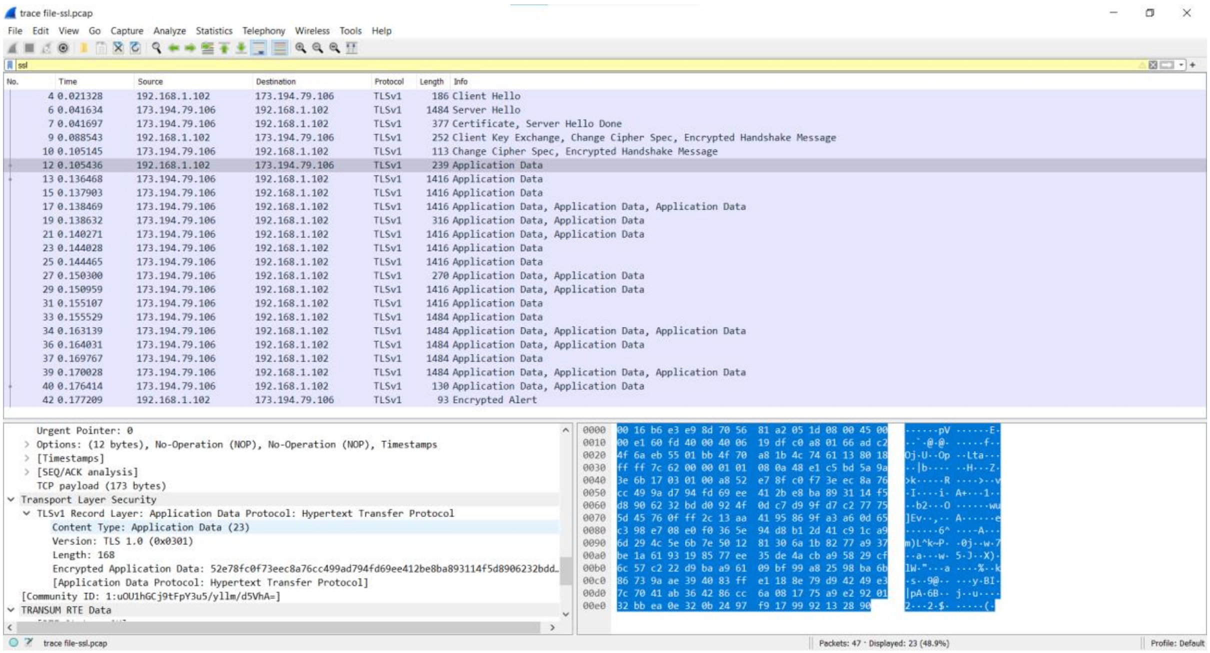
- The lower layer protocol blocks are TCP and IP because SSL runs on top of TCP/IP.]
- The SSL layer contains a TLS Record Layer. This is the foundational sublayer for TLS. All messages contain records. Expand this block to see its details.
- Each record starts with a Content Type field. This tells us 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:

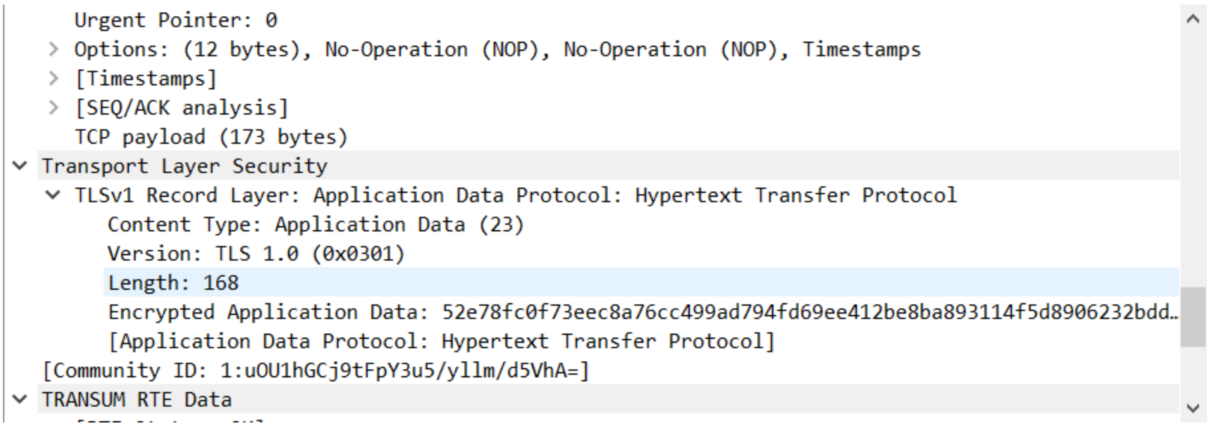
The Content Type is Application Data.


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
```

```
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (173 bytes)
v Transport Layer Security
  v 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=]
v TRANSUM RTE Data
```

```
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····
00e0  32 bb ea 0e 32 0b 24 97  f9 17 99 92 13 28 90      2···2·$· ·····(·
```

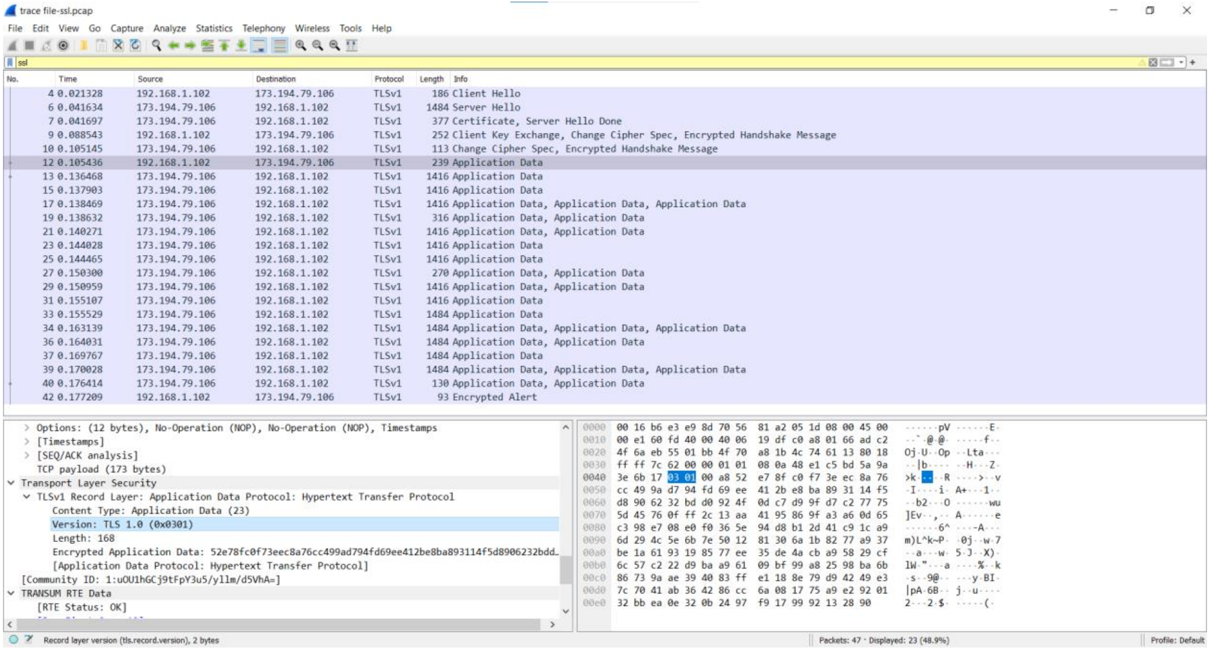


```
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (173 bytes)
v Transport Layer Security
  v TLSv1 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Content Type: Application 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=]
v 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

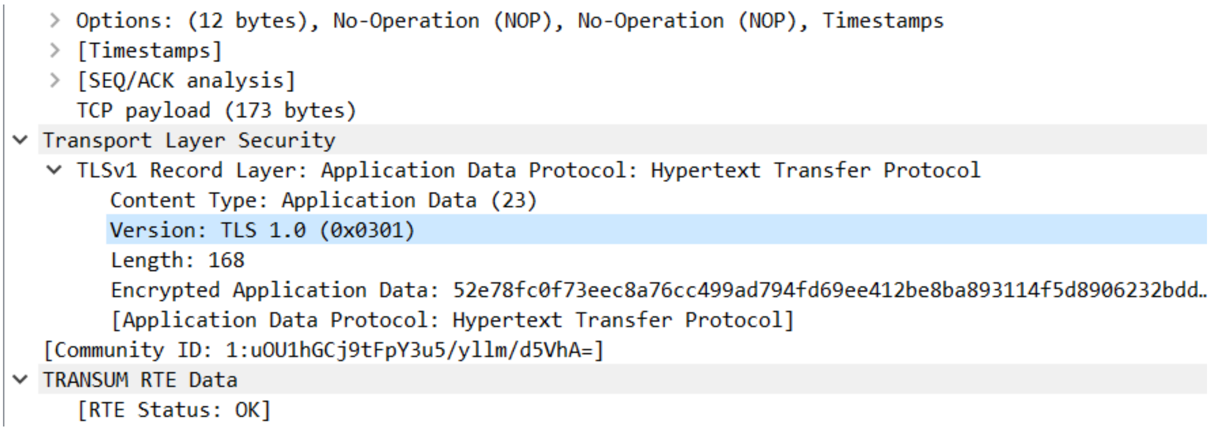

trace file-ssl.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssl

```
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
```

```
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (173 bytes)
v Transport Layer Security
  v 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=]
v TRANSUM RTE Data
    [RTE Status: OK]
```

```
0000  00 16 b6 e3 e9 8d 70 56  81 a2 05 1d 08 00 45 00
0010  00 e1 60 fd 40 00 40 06  19 df c0 a8 01 66 ad c2
0020  4f 6a eb 55 01 bb 4f 70  a8 1b 4c 74 61 13 80 18
0030  ff ff 7c 62 00 00 01 01  08 0a 48 e1 c5 bd 5a 9a
0040  3e 6b 17 03 01 00 a8 52  e7 8f c0 f7 3e ec 8a 76
0050  cc 49 9a d7 94 fd 69 ee  41 2b e8 ba 89 31 14 f5
0060  d8 90 62 32 bd d0 92 4f  0d c7 d9 9f d7 c2 77 75
0070  5d 45 76 0f ff 2c 13 aa  41 95 86 9f a3 a6 0d 65
0080  c3 98 e7 08 e0 f0 36 5e  94 d8 b1 2d 41 c9 1c a9
0090  6d 29 4c 5e 6b 7e 50 12  81 30 6a 1b 82 77 a9 37
00a0  be 1a 61 93 19 85 77 ee  35 de 4a cb a9 58 29 cf
00b0  6c 57 c2 22 d9 ba a9 61  09 bf 99 a8 25 98 ba 6b
00c0  86 73 9a ae 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 0e 32 0b 24 97  f9 17 99 92 13 28 90
```

Record layer version (tls.record.version), 2 bytes | Packets: 47 · Displayed: 23 (48.9%) | Profile: Default



```
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (173 bytes)
v Transport Layer Security
  v 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=]
v TRANSUM 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.

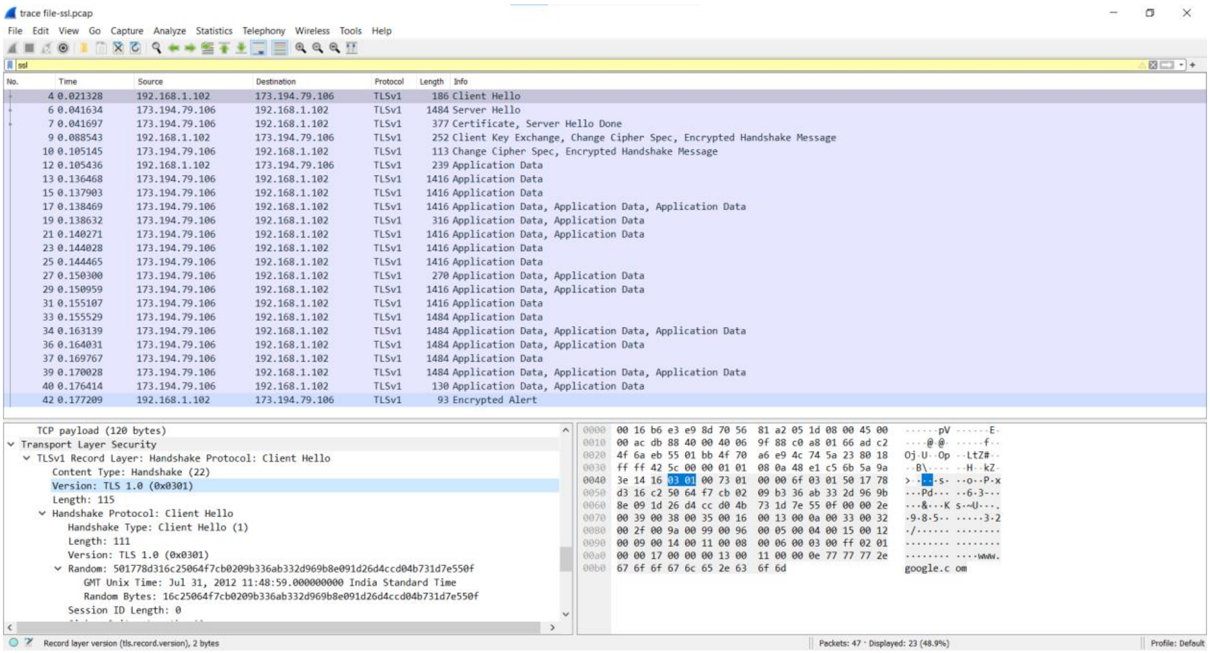
Hello Message

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
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
```

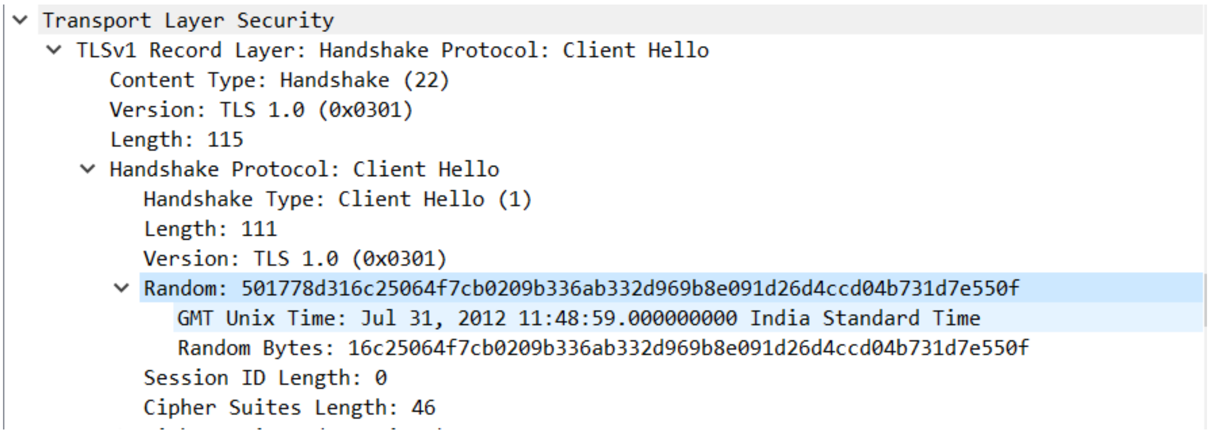
```
    TCP payload (120 bytes)
v Transport Layer Security
  v TLSv1 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 115
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 111
        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
```

```
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-··
0060  8e 09 1d 26 d4 cc d0 4b  73 1d 7e 55 0f 00 00 2e   ···&···K s·~U···.
0070  00 39 00 38 00 35 00 16  00 13 00 0a 00 33 00 32   ·9·8·5·· ·····3·2
0080  00 2f 00 9a 00 99 00 96  00 05 00 04 00 15 00 12   ·/······ ········
0090  00 09 00 14 00 11 00 08  00 06 00 03 00 ff 02 01   ········ ········
00a0  00 00 17 00 00 00 13 00  11 00 00 0e 77 77 77 2e   ········ ····www.
00b0  67 6f 6f 67 6c 65 2e 63  6f 6d                     google.c om
```

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

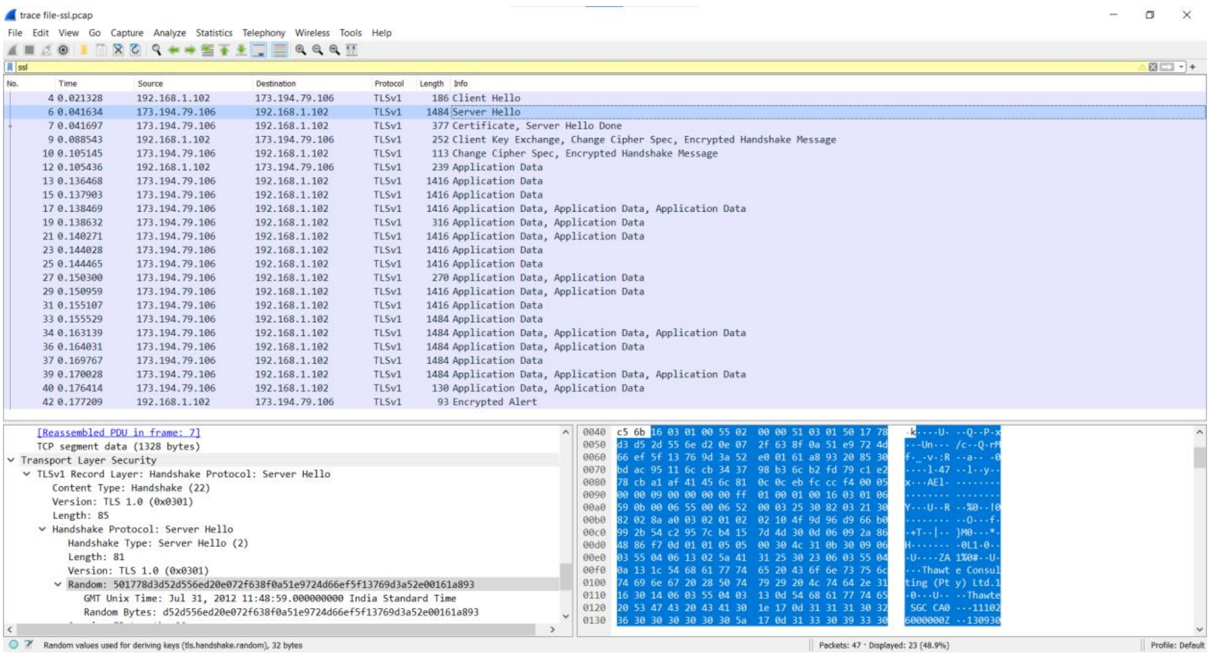
Packets: 47 · Displayed: 23 (48.9%)

Profile: Default



```
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
```

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, 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
```

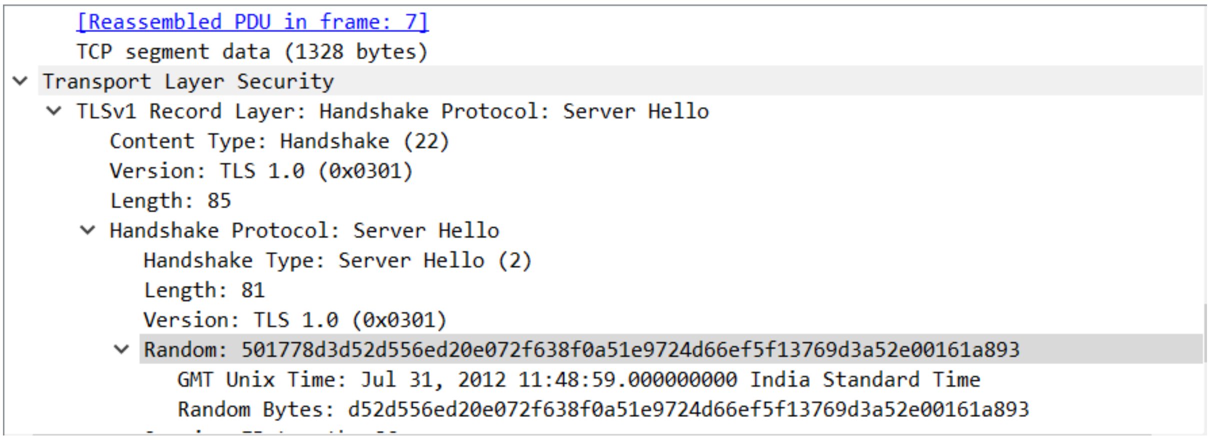
```
    [Reassembled PDU in frame: 7]
    TCP segment data (1328 bytes)
v Transport Layer Security
  v TLSv1 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 85
    v Handshake Protocol: Server Hello
        Handshake Type: 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
```

```
0040  c5 6b 16 03 01 00 55 02  00 00 51 03 01 50 17 78   ·k····U· ··Q··P·x
0050  d3 d5 2d 55 6e d2 0e 07  2f 63 8f 0a 51 e9 72 4d   ··-Un··· /c··Q·rM
0060  66 ef 5f 13 76 9d 3a 52  e0 01 61 a8 93 20 85 30   f·_·v·:R ··a·· ·0
0070  bd ac 95 11 6c cb 34 37  98 b3 6c b2 fd 79 c1 e2   ····l·47 ··l··y··
0080  78 cb a1 af 41 45 6c 81  0c 0c eb fc cc f4 00 05   x···AEl· ········
0090  00 00 09 00 00 00 00 ff  01 00 01 00 16 03 01 06   ········ ········
00a0  59 0b 00 06 55 00 06 52  00 03 25 30 82 03 21 30   Y···U··R ··%0··!0
00b0  82 02 8a a0 03 02 01 02  02 10 4f 9d 96 d9 66 b0   ········ ··O···f·
00c0  99 2b 54 c2 95 7c b4 15  7d 4d 30 0d 06 09 2a 86   ·+T··|·· }M0···*·
00d0  48 86 f7 0d 01 01 05 05  00 30 4c 31 0b 30 09 06   H······· ·0L1·0··
00e0  03 55 04 06 13 02 5a 41  31 25 30 23 06 03 55 04   ·U····ZA 1%0#··U·
00f0  0a 13 1c 54 68 61 77 74  65 20 43 6f 6e 73 75 6c   ···Thawt e Consul
0100  74 69 6e 67 20 28 50 74  79 29 20 4c 74 64 2e 31   ting (Pt y) Ltd.1
0110  16 30 14 06 03 55 04 03  13 0d 54 68 61 77 74 65   ·0···U·· ··Thawte
0120  20 53 47 43 20 43 41 30  1e 17 0d 31 31 31 30 32    SGC CA0 ···11102
0130  36 30 30 30 30 30 30 5a  17 0d 31 33 30 39 33 30   6000000Z ··130930
```

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

Packets: 47 · Displayed: 23 (48.9%)

Profile: Default



```
    [Reassembled PDU in frame: 7]
    TCP segment data (1328 bytes)
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
```

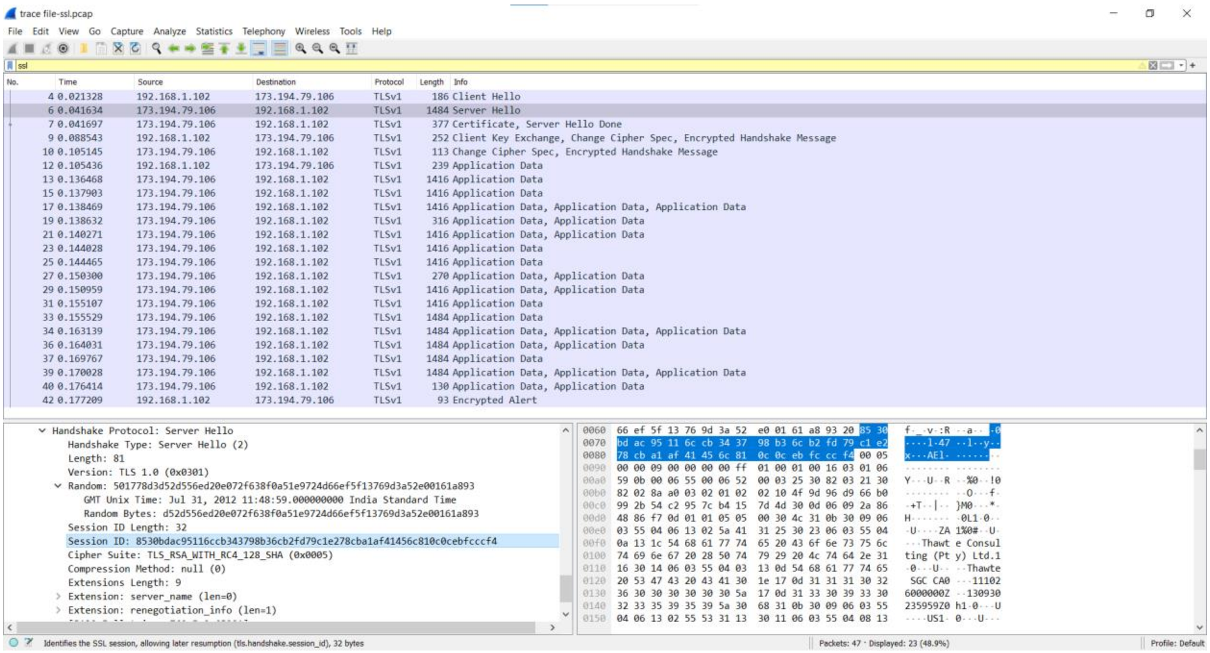
2. How long in bytes is the session identifier sent by the server?This identifier allows later resumption of the session with an abbreviated

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



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
```

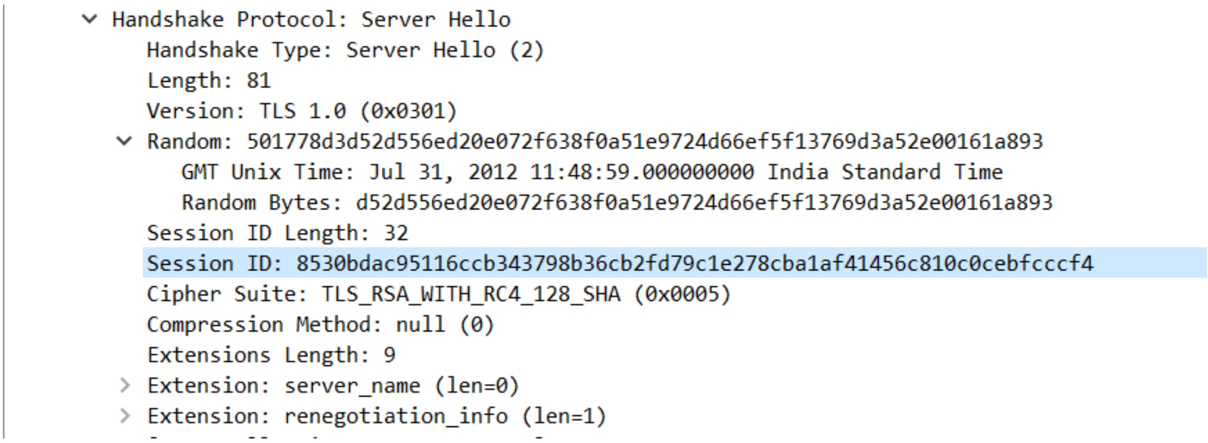
```
  v Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 81
      Version: TLS 1.0 (0x0301)
    v Random: 501778d3d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893
        GMT Unix Time: Jul 31, 2012 11:48:59.000000000 India Standard Time
        Random Bytes: 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)
```

```
0060  66 ef 5f 13 76 9d 3a 52  e0 01 61 a8 93 20 85 30   f·_·v·:R ··a·· ·0
0070  bd ac 95 11 6c cb 34 37  98 b3 6c b2 fd 79 c1 e2   ····l·47 ··l··y··
0080  78 cb a1 af 41 45 6c 81  0c 0c eb fc cc f4 00 05   x···AEl· ········
0090  00 00 09 00 00 00 00 ff  01 00 01 00 16 03 01 06   ········ ········
00a0  59 0b 00 06 55 00 06 52  00 03 25 30 82 03 21 30   Y···U··R ··%0··!0
00b0  82 02 8a a0 03 02 01 02  02 10 4f 9d 96 d9 66 b0   ········ ··O···f·
00c0  99 2b 54 c2 95 7c b4 15  7d 4d 30 0d 06 09 2a 86   ·+T··|·· }M0···*·
00d0  48 86 f7 0d 01 01 05 05  00 30 4c 31 0b 30 09 06   H······· ·0L1·0··
00e0  03 55 04 06 13 02 5a 41  31 25 30 23 06 03 55 04   ·U····ZA 1%0#··U·
00f0  0a 13 1c 54 68 61 77 74  65 20 43 6f 6e 73 75 6c   ···Thawt e Consul
0100  74 69 6e 67 20 28 50 74  79 29 20 4c 74 64 2e 31   ting (Pt y) Ltd.1
0110  16 30 14 06 03 55 04 03  13 0d 54 68 61 77 74 65   ·0···U·· ··Thawte
0120  20 53 47 43 20 43 41 30  1e 17 0d 31 31 31 30 32    SGC CA0 ···11102
0130  36 30 30 30 30 30 30 5a  17 0d 31 33 30 39 33 30   6000000Z ··130930
0140  32 33 35 39 35 39 5a 30  68 31 0b 30 09 06 03 55   235959Z0 h1·0···U
0150  04 06 13 02 55 53 31 13  30 11 06 03 55 04 08 13   ····US1· 0···U···
```

Identifies the SSL session, allowing later resumption (tls.handshake.session_id), 32 bytes

Packets: 47 · Displayed: 23 (48.9%)

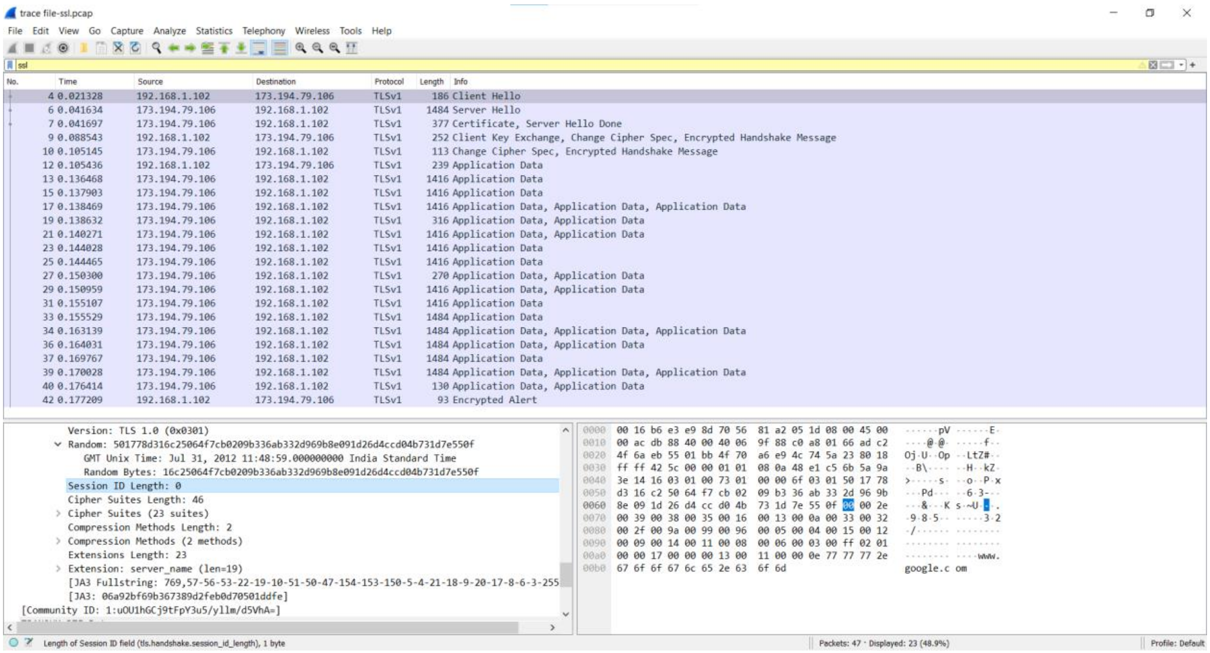
Profile: Default



```
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)
```

Client:

Length of Session ID is 0


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
```

```
      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
      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
      [JA3: 06a92bf69b367389d2feb0d70501ddfe]
  [Community ID: 1:uOU1hGCj9tFpY3u5/yllm/d5VhA=]
```

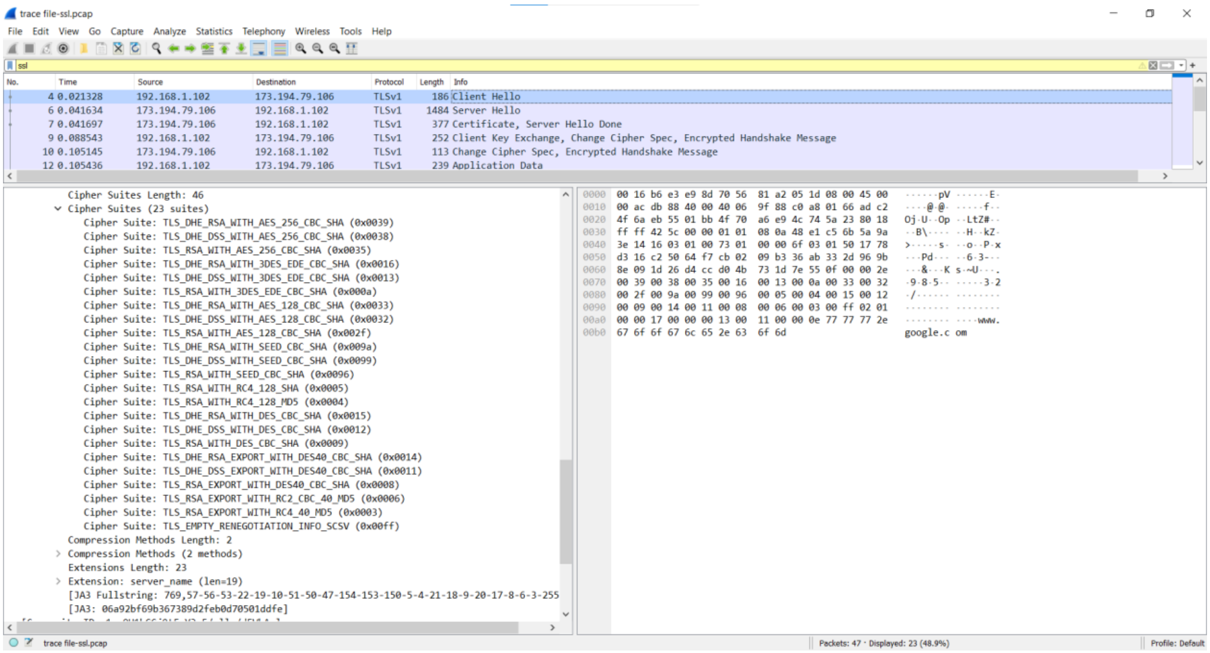
```
0000  00 16 b6 e3 e9 8d 70 56  81 a2 05 1d 08 00 45 00   ······pV ······E·
0010  00 ac db 88 40 00 40 06  9f 88 c0 a8 01 66 ad c2   ····@·@· ·····f··
0020  4f 6a eb 55 01 bb 4f 70  a6 e9 4c 74 5a 23 80 18   Oj·U··Op ··LtZ#··
0030  ff ff 42 5c 00 00 01 01  08 0a 48 e1 c5 6b 5a 9a   ··B\···· ··H··kZ·
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-··
0060  8e 09 1d 26 d4 cc d0 4b  73 1d 7e 55 0f 00 00 2e   ···&···K s·~U···.
0070  00 39 00 38 00 35 00 16  00 13 00 0a 00 33 00 32   ·9·8·5·· ·····3·2
0080  00 2f 00 9a 00 99 00 96  00 05 00 04 00 15 00 12   ·/······ ········
0090  00 09 00 14 00 11 00 08  00 06 00 03 00 ff 02 01   ········ ········
00a0  00 00 17 00 00 00 13 00  11 00 00 0e 77 77 77 2e   ········ ····www.
00b0  67 6f 6f 67 6c 65 2e 63  6f 6d                     google.c om
```

Length of Session ID field (tls.handshake.session_id_length), 1 byte | Packets: 47 · Displayed: 23 (48.9%) | Profile: Default

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:


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

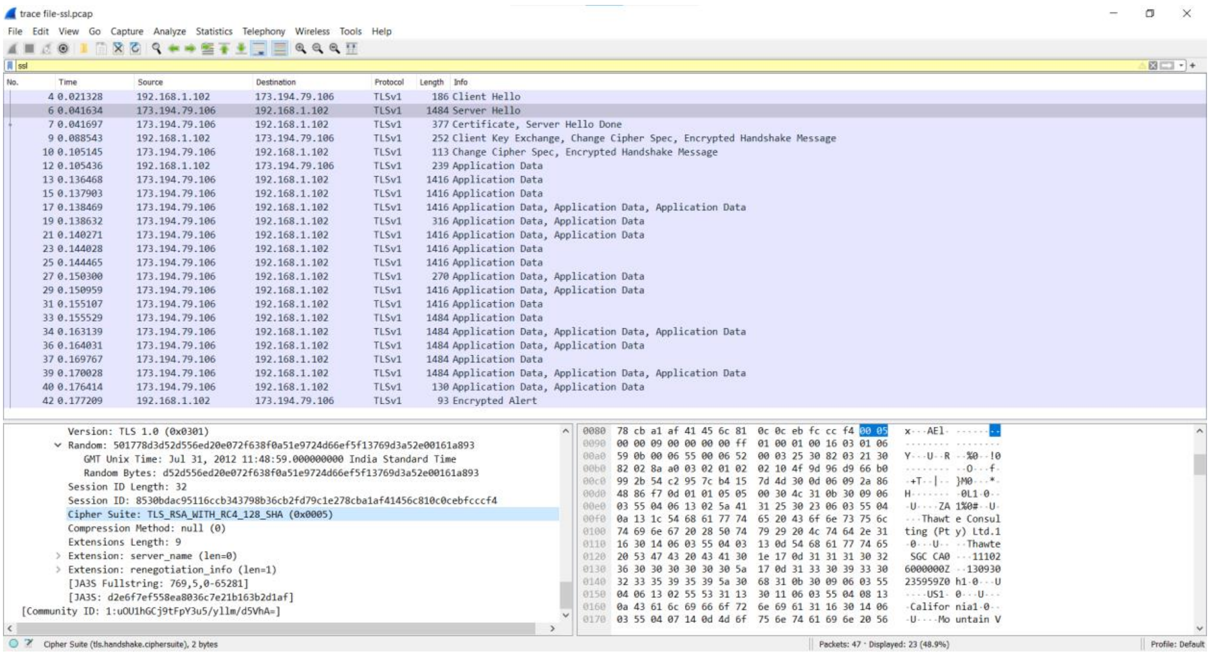
```
No.  Time      Source          Destination     Protocol Length Info
   4 0.021328  192.168.1.102   173.194.79.106  TLSv1     186 Client Hello
   6 0.041634  173.194.79.106  192.168.1.102   TLSv1    1484 Server Hello
   7 0.041697  173.194.79.106  192.168.1.102   TLSv1     377 Certificate, Server 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
```

```
      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
    › 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
      [JA3: 06a92bf69b367389d2feb0d70501ddfe]
```

```
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-··
0060  8e 09 1d 26 d4 cc d0 4b  73 1d 7e 55 0f 00 00 2e   ···&···K s·~U···.
0070  00 39 00 38 00 35 00 16  00 13 00 0a 00 33 00 32   ·9·8·5·· ·····3·2
0080  00 2f 00 9a 00 99 00 96  00 05 00 04 00 15 00 12   ·/······ ········
0090  00 09 00 14 00 11 00 08  00 06 00 03 00 ff 02 01   ········ ········
00a0  00 00 17 00 00 00 13 00  11 00 00 0e 77 77 77 2e   ········ ····www.
00b0  67 6f 6f 67 6c 65 2e 63  6f 6d                     google.c om
```

trace file-ssl.pcap | Packets: 47 · Displayed: 23 (48.9%) | Profile: Default

Server:


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
```

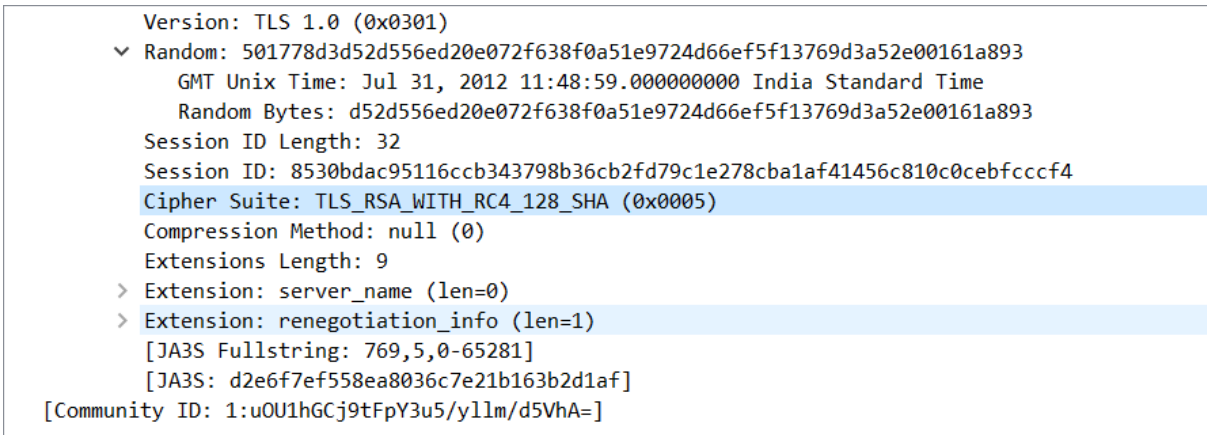
```
        Version: TLS 1.0 (0x0301)
      ˅ Random: 501778d3d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893
            GMT Unix Time: Jul 31, 2012 11:48:59.000000000 India Standard Time
            Random Bytes: d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893
        Session ID Length: 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)
        [JA3S Fullstring: 769,5,0-65281]
        [JA3S: d2e6f7ef558ea8036c7e21b163b2d1af]
    [Community ID: 1:uOU1hGCj9tFpY3u5/yllm/d5VhA=]
```

```
0080  78 cb a1 af 41 45 6c 81  0c 0c eb fc cc f4 00 05   x···AEl· ······ ··
0090  00 00 09 00 00 00 00 ff  01 00 01 00 16 03 01 06   ········ ········
00a0  59 0b 00 06 55 00 06 52  00 03 25 30 82 03 21 30   Y···U··R ··%0··!0
00b0  82 02 8a a0 03 02 01 02  02 10 4f 9d 96 d9 66 b0   ········ ··O···f·
00c0  99 2b 54 c2 95 7c b4 15  7d 4d 30 0d 06 09 2a 86   ·+T··|·· }M0···*·
00d0  48 86 f7 0d 01 01 05 05  00 30 4c 31 0b 30 09 06   H······· ·0L1·0··
00e0  03 55 04 06 13 02 5a 41  31 25 30 23 06 03 55 04   ·U····ZA 1%0#··U·
00f0  0a 13 1c 54 68 61 77 74  65 20 43 6f 6e 73 75 6c   ···Thawt e Consul
0100  74 69 6e 67 20 28 50 74  79 29 20 4c 74 64 2e 31   ting (Pt y) Ltd.1
0110  16 30 14 06 03 55 04 03  13 0d 54 68 61 77 74 65   ·0···U·· ··Thawte
0120  20 53 47 43 20 43 41 30  1e 17 0d 31 31 31 30 32    SGC CA0 ···11102
0130  36 30 30 30 30 30 30 5a  17 0d 31 33 30 39 33 30   6000000Z ··130930
0140  32 33 35 39 35 39 5a 30  68 31 0b 30 09 06 03 55   235959Z0 h1·0···U
0150  04 06 13 02 55 53 31 13  30 11 06 03 55 04 08 13   ····US1· 0···U···
0160  0a 43 61 6c 69 66 6f 72  6e 69 61 31 16 30 14 06   ·Califor nia1·0··
0170  03 55 04 07 14 0d 4d 6f  75 6e 74 61 69 6e 20 56   ·U····Mo untain V
```

Cipher Suite (tls.handshake.ciphersuite), 2 bytes

Packets: 47 · Displayed: 23 (48.9%)

Profile: Default



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

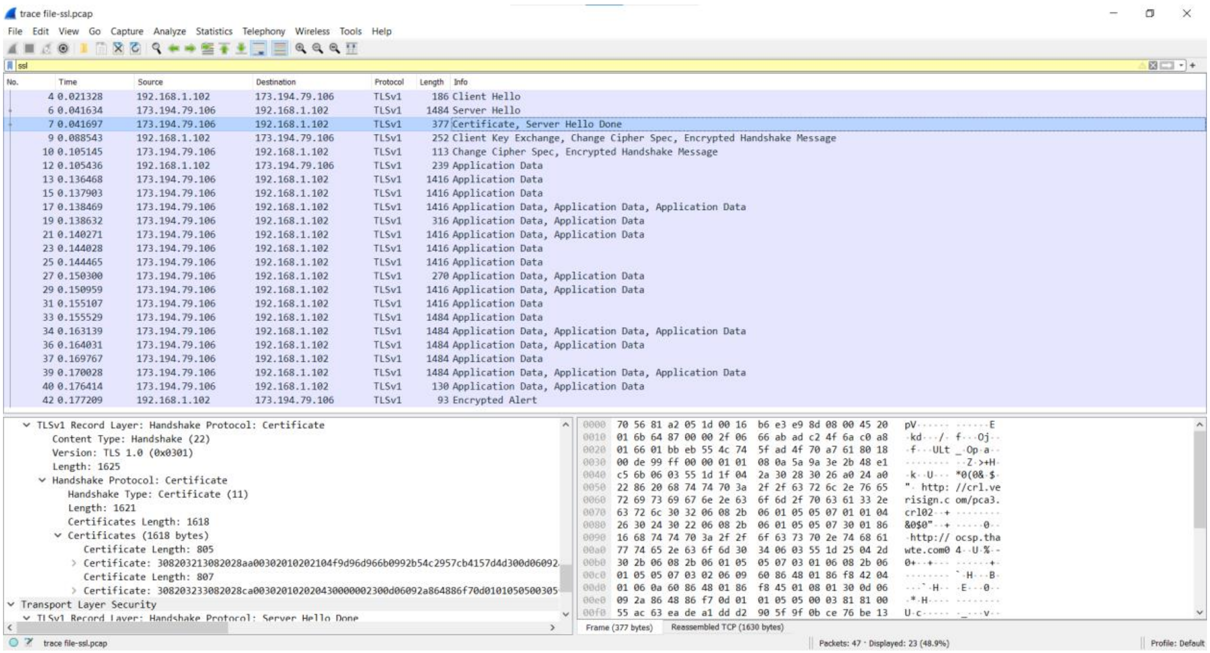
Certificate Messages:

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



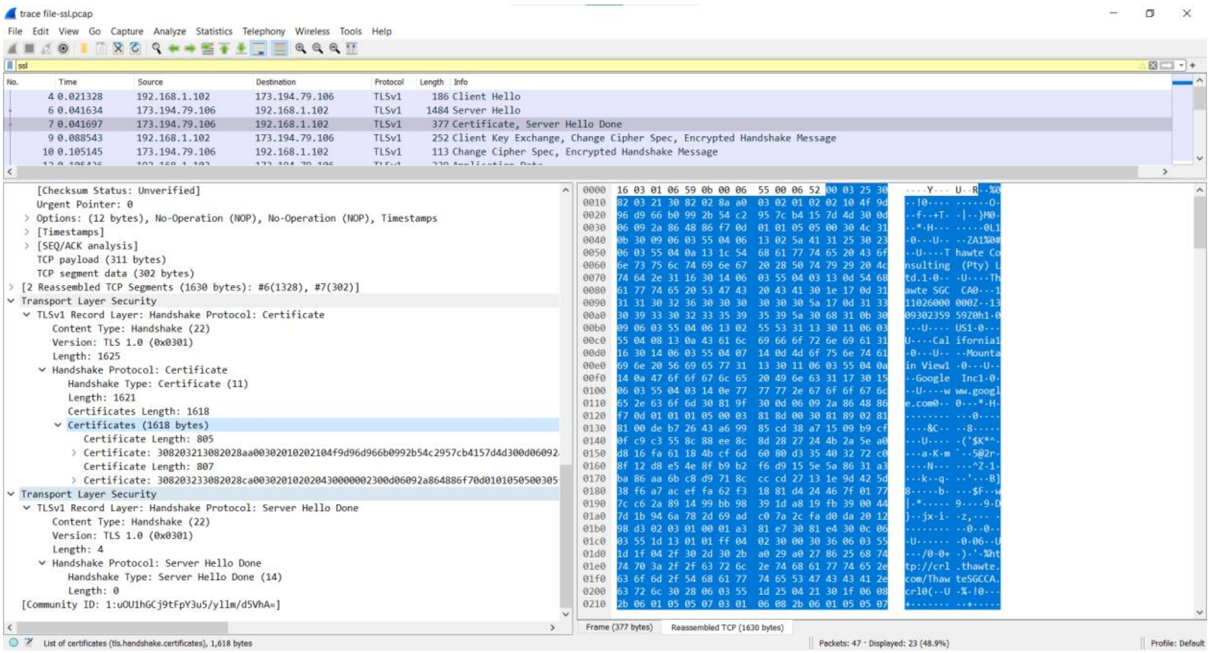
trace file-ssl.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssl

```
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
```

```
  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: 308203213082028aa00302010202104f9d96d966b0992b54c2957cb4157d4d300d06092
           Certificate Length: 807
         > Certificate: 308203233082028ca003020102020430000002300d06092a864886f70d0101050500305
Transport Layer Security
  TLSv1 Record Layer: Handshake Protocol: Server Hello Done
```

```
0000  70 56 81 a2 05 1d 00 16  b6 e3 e9 8d 08 00 45 20   pV······ ······E
0010  01 6b 64 87 00 00 2f 06  66 ab ad c2 4f 6a c0 a8   ·kd···/· f···Oj··
0020  01 66 01 bb eb 55 4c 74  5f ad 4f 70 a7 61 80 18   ·f···ULt _·Op·a··
0030  00 de 99 ff 00 00 01 01  08 0a 5a 9a 3e 2b 48 e1   ········ ··Z·>+H·
0040  c5 6b 06 03 55 1d 1f 04  2a 30 28 30 26 a0 24 a0   ·k··U··· *0(0&·$·
0050  22 86 20 68 74 74 70 3a  2f 2f 63 72 6c 2e 76 65   "· http: //crl.ve
0060  72 69 73 69 67 6e 2e 63  6f 6d 2f 70 63 61 33 2e   risign.c om/pca3.
0070  63 72 6c 30 32 06 08 2b  06 01 05 05 07 01 01 04   crl02··+ ········
0080  26 30 24 30 22 06 08 2b  06 01 05 05 07 30 01 86   &0$0"··+ ·····0··
0090  16 68 74 74 70 3a 2f 2f  6f 63 73 70 2e 74 68 61   ·http:// ocsp.tha
00a0  77 74 65 2e 63 6f 6d 30  34 06 03 55 1d 25 04 2d   wte.com0 4··U·%·-
00b0  30 2b 06 08 2b 06 01 05  05 07 03 01 06 08 2b 06   0+··+··· ······+·
00c0  01 05 05 07 03 02 06 09  60 86 48 01 86 f8 42 04   ········ `·H···B·
00d0  01 06 0a 60 86 48 01 86  f8 45 01 08 01 30 0d 06   ···`·H·· ·E···0··
00e0  09 2a 86 48 86 f7 0d 01  01 05 05 00 03 81 81 00   ·*·H···· ········
00f0  55 ac 63 ea de a1 dd d2  90 5f 9f 0b ce 76 be 13   U·c····· ·_···v··
```

Frame (377 bytes)
Reassembled TCP (1630 bytes)
trace file-ssl.pcap
Packets: 47 · Displayed: 23 (48.9%)
Profile: Default



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
```

```
    [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)]
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: 308203213082028aa00302010202104f9d96d966b0992b54c2957cb4157d4d300d06092
           Certificate Length: 807
         > Certificate: 308203233082028ca003020102020430000002300d06092a864886f70d0101050500305
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:uOU1hGCj9tFpY3u5/yllm/d5VhA=]
```

```
0000  16 03 01 06 59 0b 00 06  55 00 06 52 00 03 25 30   ····Y··· U··R··%0
0010  82 03 21 30 82 02 8a a0  03 02 01 02 02 10 4f 9d   ··!0···· ······O·
0020  96 d9 66 b0 99 2b 54 c2  95 7c b4 15 7d 4d 30 0d   ··f··+T· ·|··}M0·
0030  06 09 2a 86 48 86 f7 0d  01 01 05 05 00 30 4c 31   ··*·H··· ·····0L1
0040  0b 30 09 06 03 55 04 06  13 02 5a 41 31 25 30 23   ·0···U·· ··ZA1%0#
0050  06 03 55 04 0a 13 1c 54  68 61 77 74 65 20 43 6f   ··U····T hawte Co
0060  6e 73 75 6c 74 69 6e 67  20 28 50 74 79 29 20 4c   nsulting  (Pty) L
0070  74 64 2e 31 16 30 14 06  03 55 04 03 13 0d 54 68   td.1·0·· ·U····Th
0080  61 77 74 65 20 53 47 43  20 43 41 30 1e 17 0d 31   awte SGC  CA0···1
0090  31 31 30 32 36 30 30 30  30 30 30 5a 17 0d 31 33   11026000 000Z··13
00a0  30 39 33 30 32 33 35 39  35 39 5a 30 68 31 0b 30   09302359 59Z0h1·0
00b0  09 06 03 55 04 06 13 02  55 53 31 13 30 11 06 03   ···U···· US1·0···
00c0  55 04 08 13 0a 43 61 6c  69 66 6f 72 6e 69 61 31   U····Cal ifornia1
00d0  16 30 14 06 03 55 04 07  14 0d 4d 6f 75 6e 74 61   ·0···U·· ··Mounta
00e0  69 6e 20 56 69 65 77 31  13 30 11 06 03 55 04 0a   in View1 ·0···U··
00f0  14 0a 47 6f 6f 67 6c 65  20 49 6e 63 31 17 30 15   ··Google  Inc1·0·
0100  06 03 55 04 03 14 0e 77  77 77 2e 67 6f 6f 67 6c   ··U····w ww.googl
0110  65 2e 63 6f 6d 30 81 9f  30 0d 06 09 2a 86 48 86   e.com0·· 0···*·H·
0120  f7 0d 01 01 01 05 00 03  81 8d 00 30 81 89 02 81   ········ ···0····
0130  81 00 de b7 26 43 a6 99  85 cd 38 a7 15 09 b9 cf   ····&C·· ··8·····
0140  0f c9 c3 55 8c 88 ee 8c  8d 28 27 24 4b 2a 5e a0   ···U···· ·('$K*^·
0150  d8 16 fa 61 18 4b cf 6d  60 80 d3 35 40 32 72 c0   ···a·K·m `··5@2r·
0160  8f 12 d8 e5 4e 8f b9 b2  f6 d9 15 5e 5a 86 31 a3   ····N··· ···^Z·1·
0170  ba 86 aa 6b c8 d9 71 8c  cc cd 27 13 1e 9d 42 5d   ···k··q· ··'···B]
0180  38 f6 a7 ac ef fa 62 f3  18 81 d4 24 46 7f 01 77   8·····b· ···$F··w
0190  7c c6 2a 89 14 99 bb 98  39 1d a8 19 fb 39 00 44   |·*····· 9····9·D
01a0  7d 1b 94 6a 78 2d 69 ad  c0 7a 2c fa d0 da 20 12   }··jx-i· ·z,··· ·
01b0  98 d3 02 03 01 00 01 a3  81 e7 30 81 e4 30 0c 06   ········ ··0··0··
01c0  03 55 1d 13 01 01 ff 04  02 30 00 30 36 06 03 55   ·U······ ·0·06··U
01d0  1d 1f 04 2f 30 2d 30 2b  a0 29 a0 27 86 25 68 74   ···/0-0+ ·)·'·%ht
01e0  74 70 3a 2f 2f 63 72 6c  2e 74 68 61 77 74 65 2e   tp://crl .thawte.
01f0  63 6f 6d 2f 54 68 61 77  74 65 53 47 43 43 41 2e   com/Thaw teSGCCA.
0200  63 72 6c 30 28 06 03 55  1d 25 04 21 30 1f 06 08   crl0(··U ·%·!0···
0210  2b 06 01 05 05 07 03 01  06 08 2b 06 01 05 05 07   +······· ··+·····
```

Frame (377 bytes)
Reassembled TCP (1630 bytes)
List of certificates (tls.handshake.certificates), 1,618 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

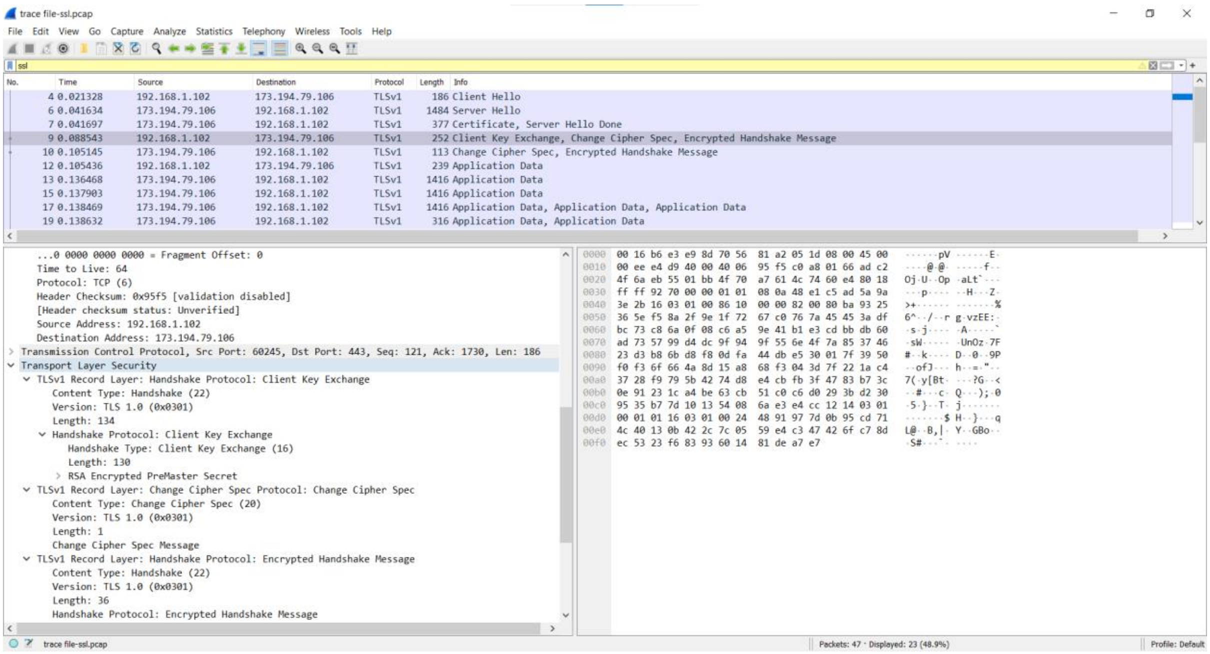
Find and inspect the details of the Client Key Exchange and Change Cipher messages, expanding their various details. The key exchange message is sent to pass keying information so that both sides will have the same secret session key. The change cipher message signal a switch to a new encryption scheme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

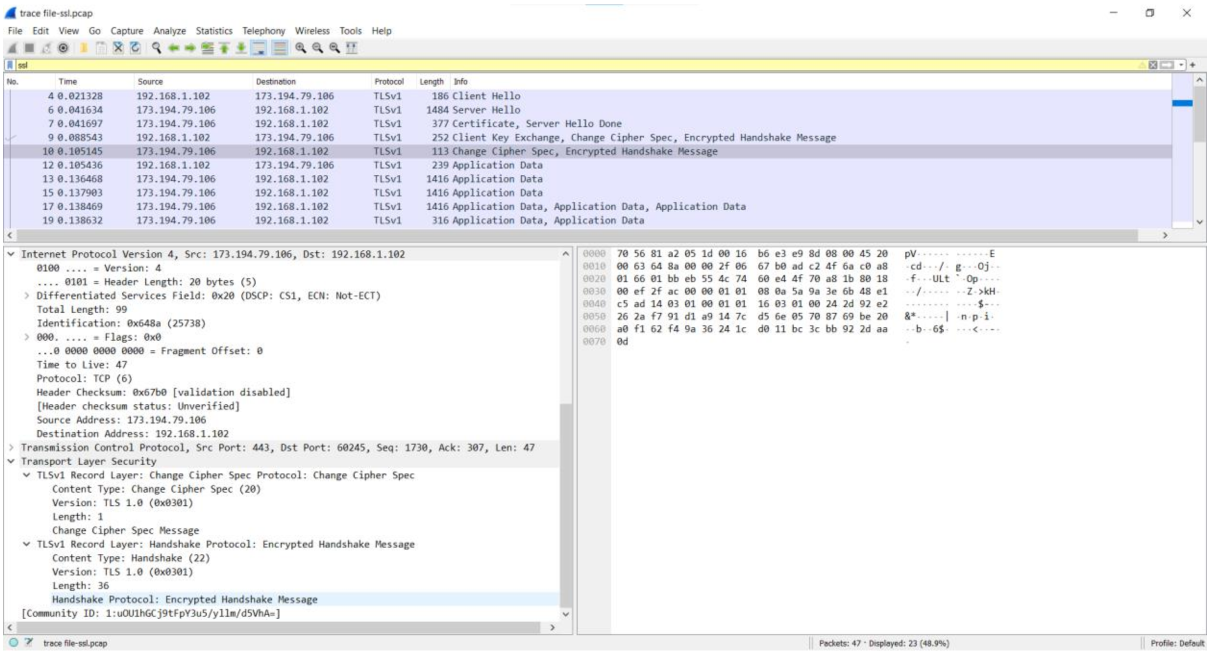

trace file-ssl.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssl

```
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
```

```
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x95f5 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 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#···`· ····
```

Server:



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

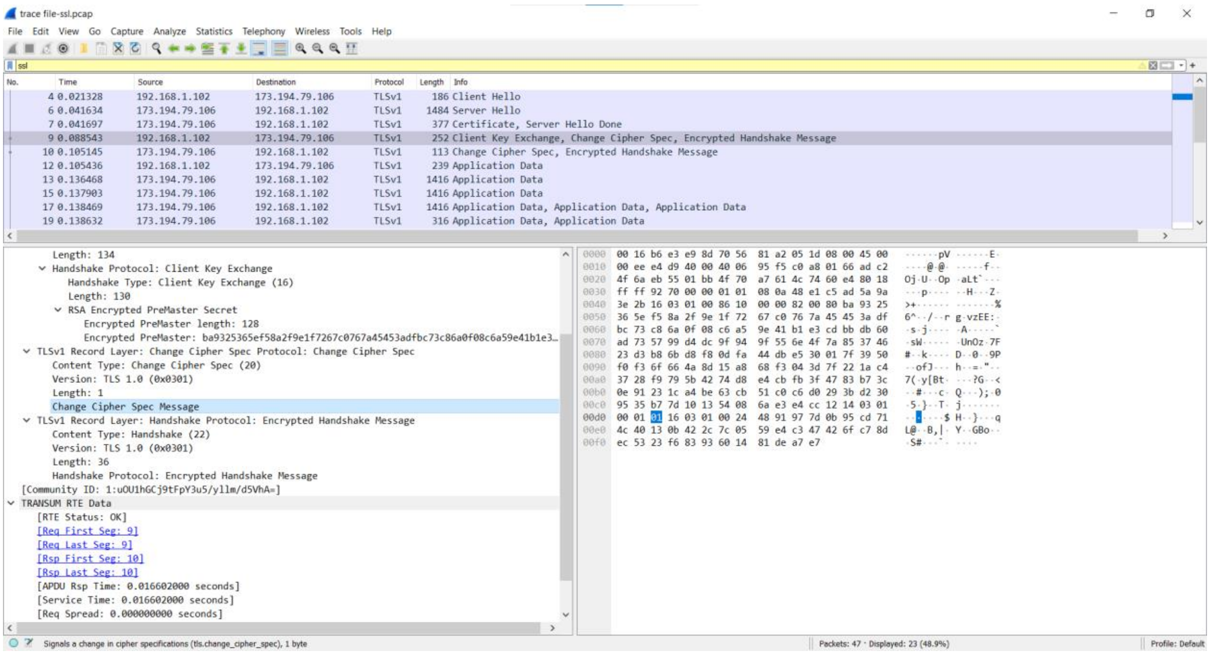
```
No.   Time      Source          Destination     Protocol Length Info
    4 0.021328  192.168.1.102   173.194.79.106  TLSv1     186 Client Hello
    6 0.041634  173.194.79.106  192.168.1.102   TLSv1    1484 Server Hello
    7 0.041697  173.194.79.106  192.168.1.102   TLSv1     377 Certificate, Server 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
```

```
v Internet Protocol Version 4, Src: 173.194.79.106, Dst: 192.168.1.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
    Total Length: 99
    Identification: 0x648a (25738)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 47
    Protocol: TCP (6)
    Header Checksum: 0x67b0 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 173.194.79.106
    Destination Address: 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
  [Community ID: 1:uOU1hGCj9tFpY3u5/yllm/d5VhA=]
```

```
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                                                 ·
```

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:



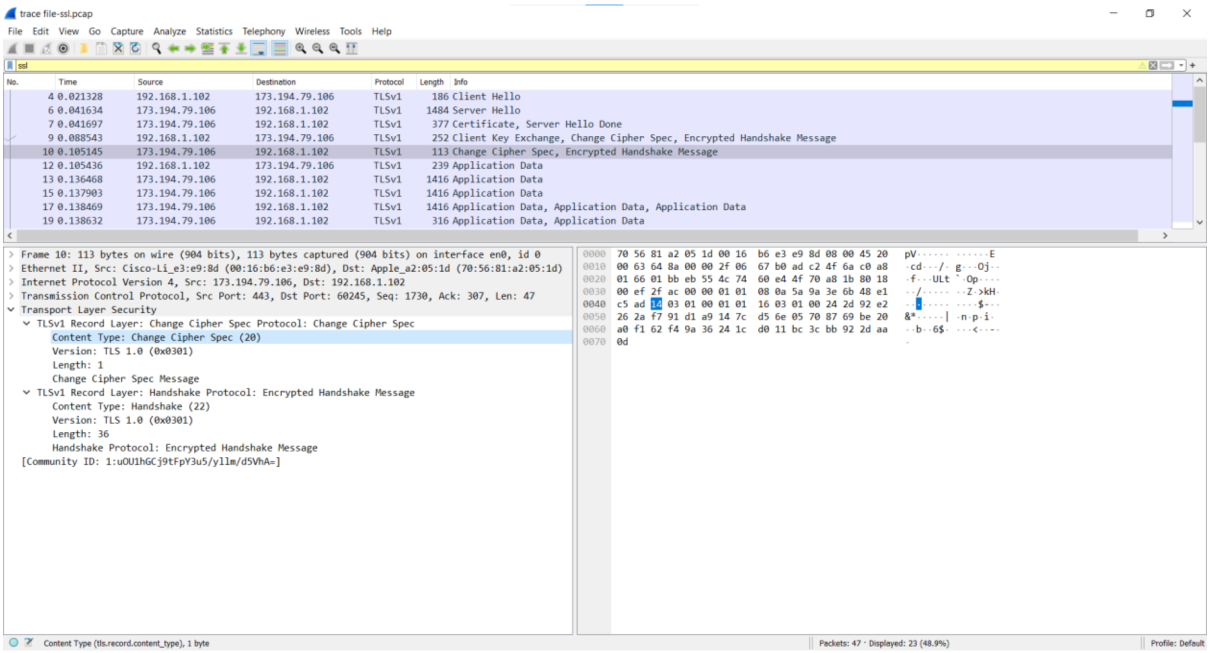
trace file-ssl.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssl

```
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
```

```
      Length: 134
    v Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 130
      v RSA Encrypted PreMaster Secret
          Encrypted PreMaster length: 128
          Encrypted PreMaster: ba9325365ef58a2f9e1f7267c0767a45453adfbc73c86a0f08c6a59e41b1e3…
  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
  [Community ID: 1:uOU1hGCj9tFpY3u5/yllm/d5VhA=]
v TRANSUM RTE Data
    [RTE Status: OK]
    [Req First Seg: 9]
    [Req Last Seg: 9]
    [Rsp First Seg: 10]
    [Rsp Last Seg: 10]
    [APDU Rsp Time: 0.016602000 seconds]
    [Service Time: 0.016602000 seconds]
    [Req Spread: 0.000000000 seconds]
```

```
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#···`· ····
```

Signals a change in cipher specifications (tls.change_cipher_spec), 1 byte
Packets: 47 · Displayed: 23 (48.9%)
Profile: Default



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
```

```
> 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
  [Community ID: 1:uOU1hGCj9tFpY3u5/yllm/d5VhA=]
```

```
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                                                 ·
```

Content Type (tls.record.content_type), 1 byte
Packets: 47 · Displayed: 23 (48.9%)
Profile: Default

Conclusion:

Performed the experiment successfully.

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