SSL/TLS Lab

Title : SSL/TLS Lab

PRN : 2017BTECS000215

Theory :

SSL (Secure Sockets Layer) and its successor, TLS (Transport Layer Security), are protocols for establishing authenticated and encrypted links between networked computers. The most common and well-known use of SSL/TLS is secure web browsing via the HTTPS protocol. A properly-configured public HTTPS website includes an SSL/TLS certificate that is signed by a publicly trusted Certification Authority.

Users visiting an HTTPS website can be assured of :

- *Authenticity*

  The server presenting the certificate is in possession of the private key that matches the public key in the certificate.

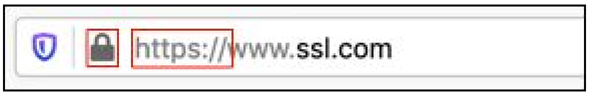
- *Integrity*

  Documents signed by the certificate (e.g. web pages) have not been altered in transit by a man in the middle.

- *Encryption*

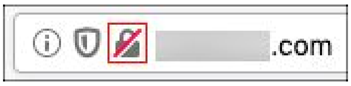
  Communications between the client and server are encrypted.

Website with SSL



https://www.ssl.com

Website without SSL

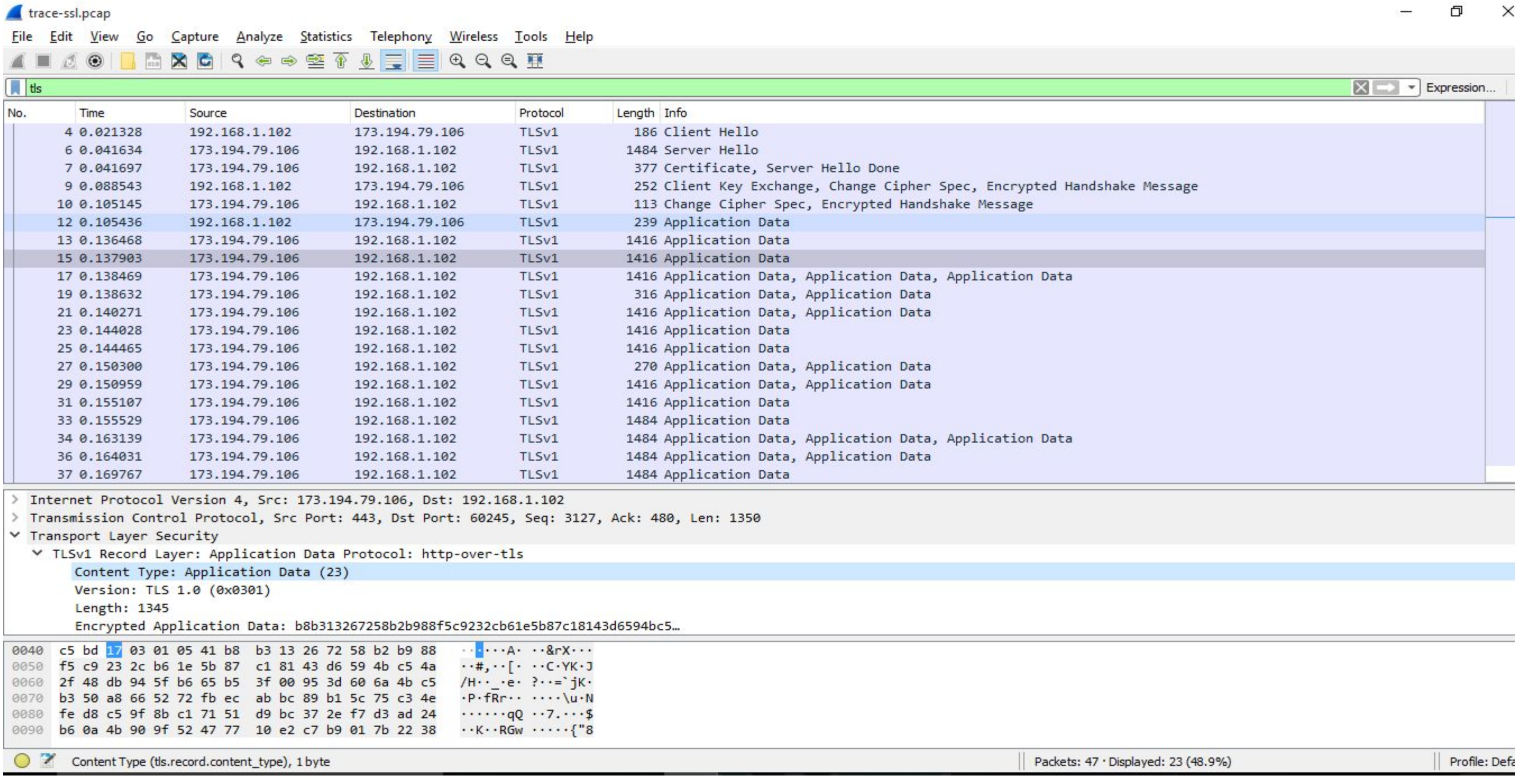


.com

Questions and Answers :

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

Answer : Application data


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

```
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
```

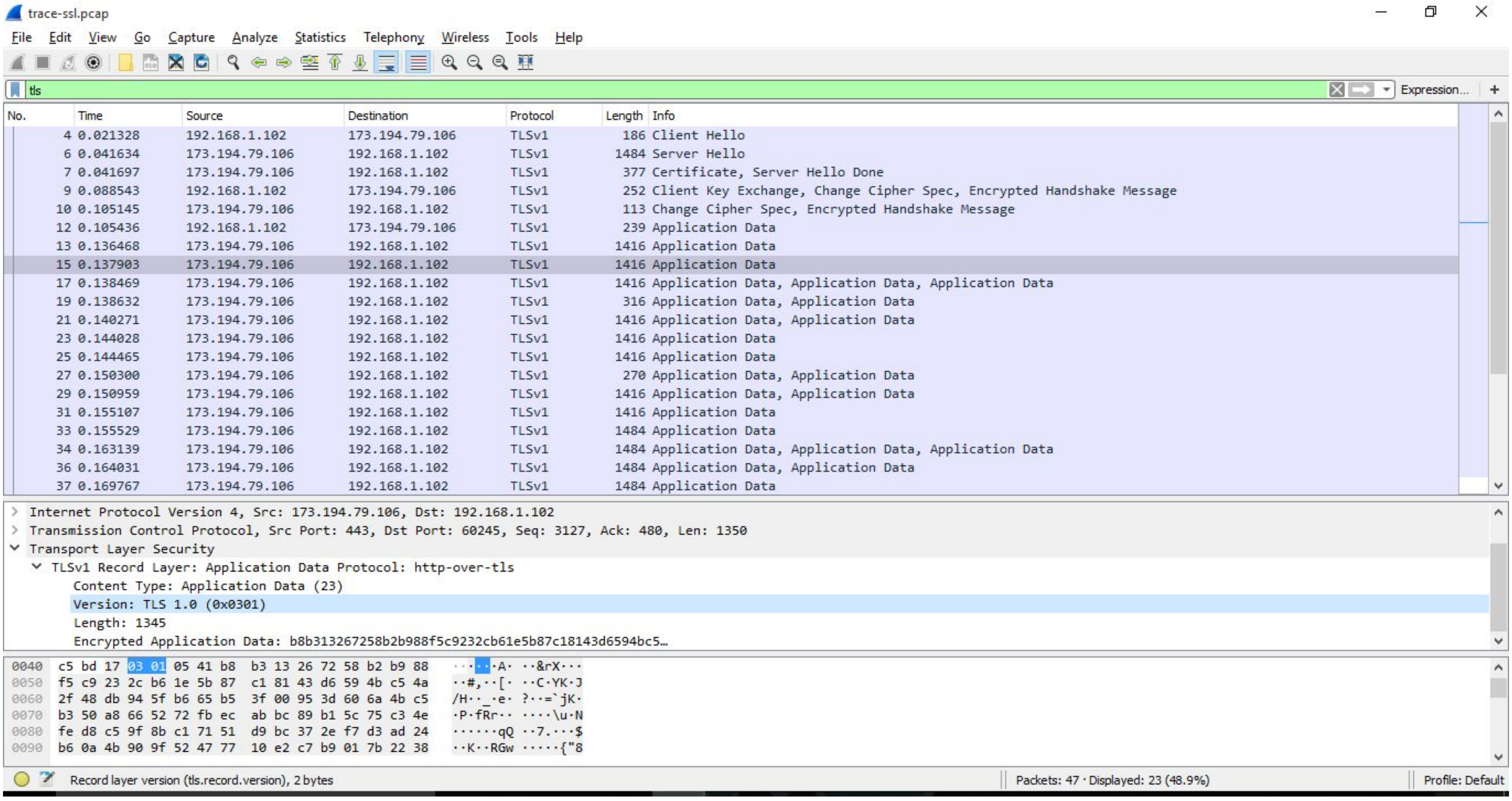
```
> Internet Protocol Version 4, Src: 173.194.79.106, Dst: 192.168.1.102
> Transmission Control Protocol, Src Port: 443, Dst Port: 60245, Seq: 3127, Ack: 480, Len: 1350
v Transport Layer Security
  v TLSv1 Record Layer: Application Data Protocol: http-over-tls
      Content Type: Application Data (23)
      Version: TLS 1.0 (0x0301)
      Length: 1345
      Encrypted Application Data: b8b313267258b2b988f5c9232cb61e5b87c18143d6594bc5…
```

```
0040  c5 bd 17 03 01 05 41 b8  b3 13 26 72 58 b2 b9 88   ·······A· ··&rX···
0050  f5 c9 23 2c b6 1e 5b 87  c1 81 43 d6 59 4b c5 4a   ··#,··[· ··C·YK·J
0060  2f 48 db 94 5f b6 65 b5  3f 00 95 3d 60 6a 4b c5   /H··_·e· ?··=`jK·
0070  b3 50 a8 66 52 72 fb ec  ab bc 89 b1 5c 75 c3 4e   ·P·fRr·· ····\u·N
0080  fe d8 c5 9f 8b c1 71 51  d9 bc 37 2e f7 d3 ad 24   ······qQ ··7.···$
0090  b6 0a 4b 90 9f 52 47 77  10 e2 c7 b9 01 7b 22 38   ··K··RGw ·····{"8
```

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

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

Answer : TLS 1.0


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

```
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
```

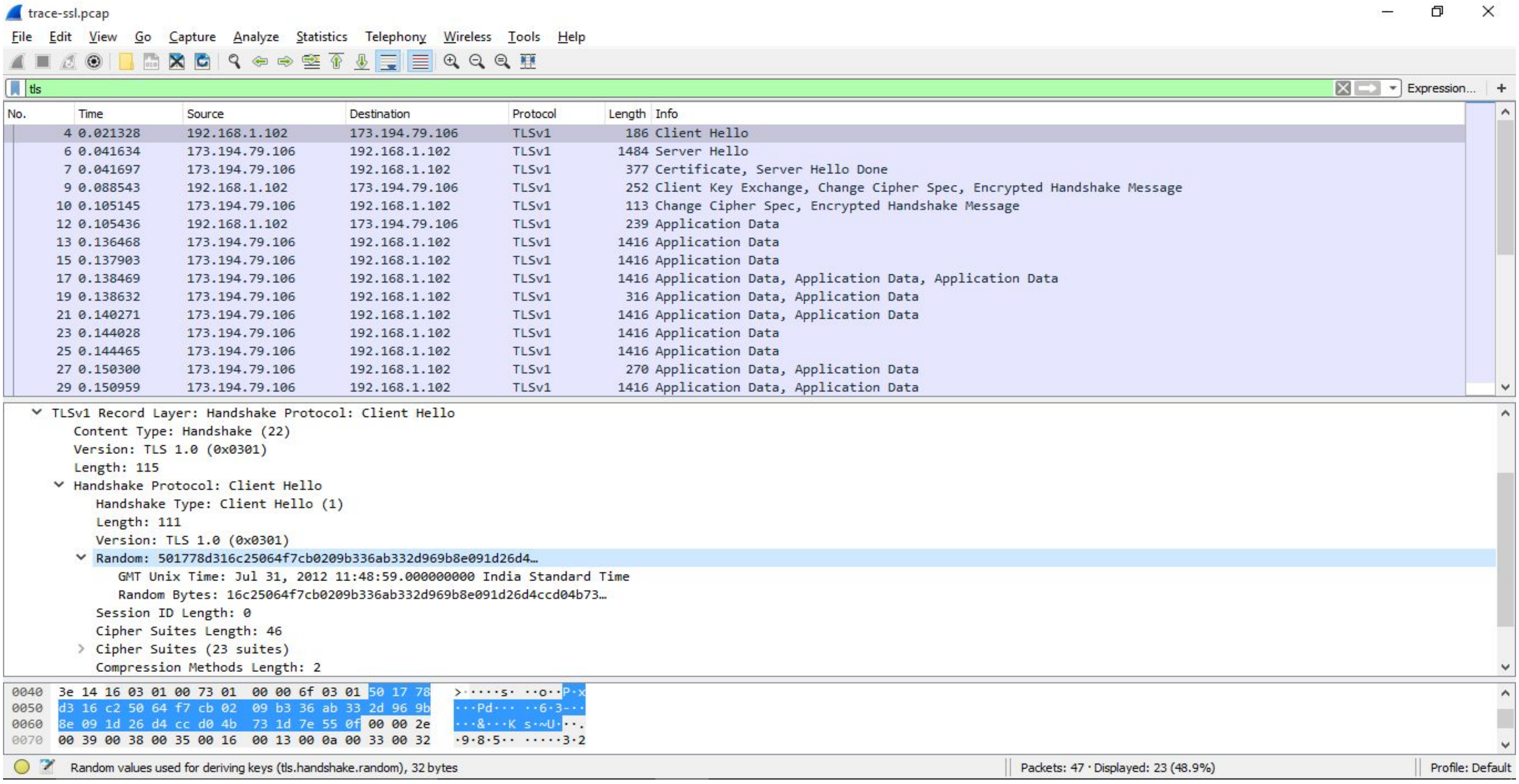
```
> Internet Protocol Version 4, Src: 173.194.79.106, Dst: 192.168.1.102
> Transmission Control Protocol, Src Port: 443, Dst Port: 60245, Seq: 3127, Ack: 480, Len: 1350
v Transport Layer Security
  v TLSv1 Record Layer: Application Data Protocol: http-over-tls
      Content Type: Application Data (23)
      Version: TLS 1.0 (0x0301)
      Length: 1345
      Encrypted Application Data: b8b313267258b2b988f5c9232cb61e5b87c18143d6594bc5…
```

```
0040  c5 bd 17 03 01 05 41 b8  b3 13 26 72 58 b2 b9 88   ·······A· ··&rX···
0050  f5 c9 23 2c b6 1e 5b 87  c1 81 43 d6 59 4b c5 4a   ··#,··[· ··C·YK·J
0060  2f 48 db 94 5f b6 65 b5  3f 00 95 3d 60 6a 4b c5   /H··_·e· ?··=`jK·
0070  b3 50 a8 66 52 72 fb ec  ab bc 89 b1 5c 75 c3 4e   ·P·fRr·· ····\u·N
0080  fe d8 c5 9f 8b c1 71 51  d9 bc 37 2e f7 d3 ad 24   ······qQ ··7.···$
0090  b6 0a 4b 90 9f 52 47 77  10 e2 c7 b9 01 7b 22 38   ··K··RGw ·····{"8
```

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

Q.3) 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.

Answer : 32 bytes

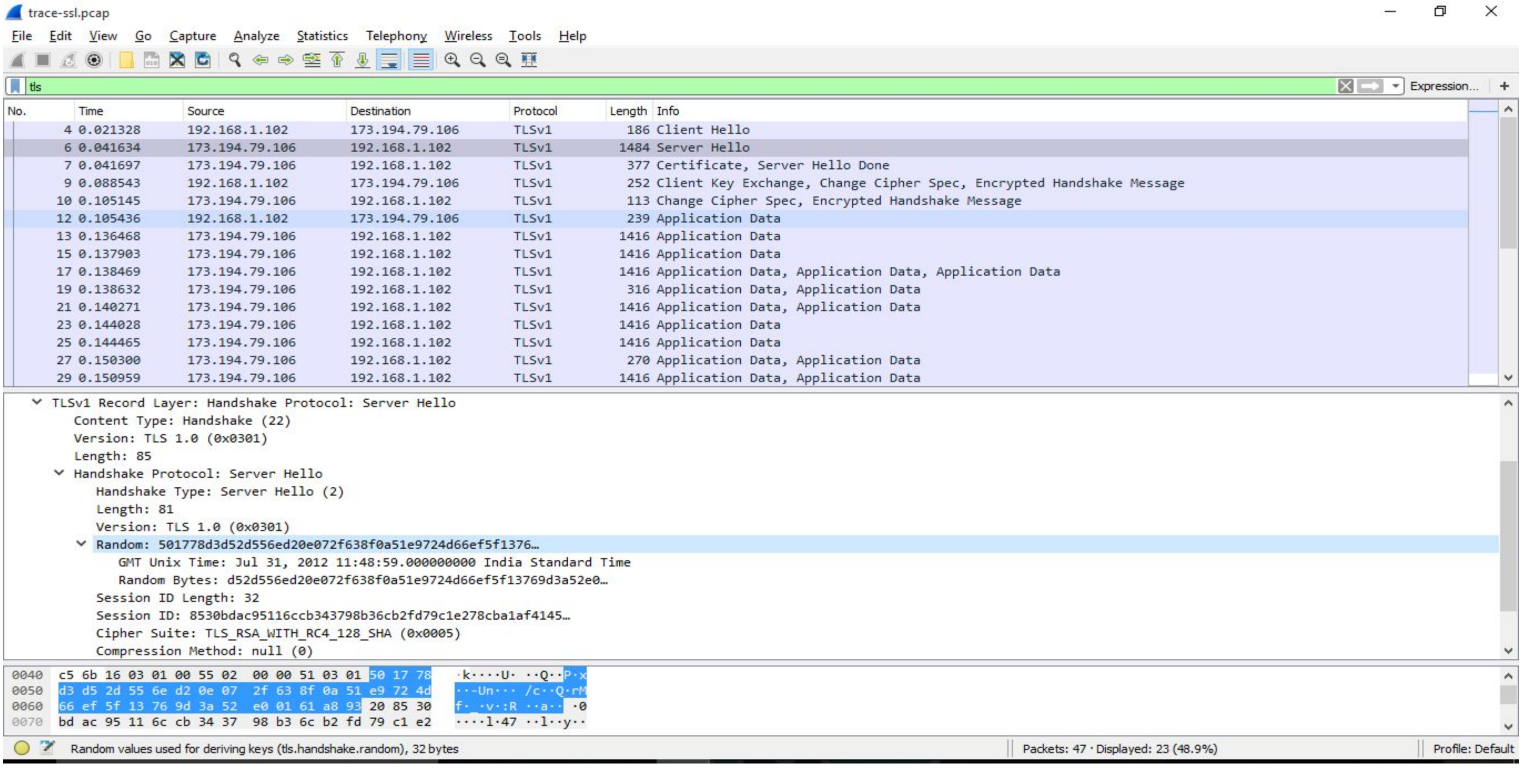

trace-ssl.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls
Expression…
+

```
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
```

```
  ˅ TLSv1 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 115
    ˅ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 111
        Version: TLS 1.0 (0x0301)
      ˅ Random: 501778d316c25064f7cb0209b336ab332d969b8e091d26d4…
          GMT Unix Time: Jul 31, 2012 11:48:59.000000000 India Standard Time
          Random Bytes: 16c25064f7cb0209b336ab332d969b8e091d26d4ccd04b73…
        Session ID Length: 0
        Cipher Suites Length: 46
      › Cipher Suites (23 suites)
        Compression Methods Length: 2
```

```
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
```

Random values used for deriving keys (tls.handshake.random), 32 bytes | Packets: 47 · Displayed: 23 (48.9%) | Profile: Default


trace-ssl.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls
Expression…
+

```
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
```

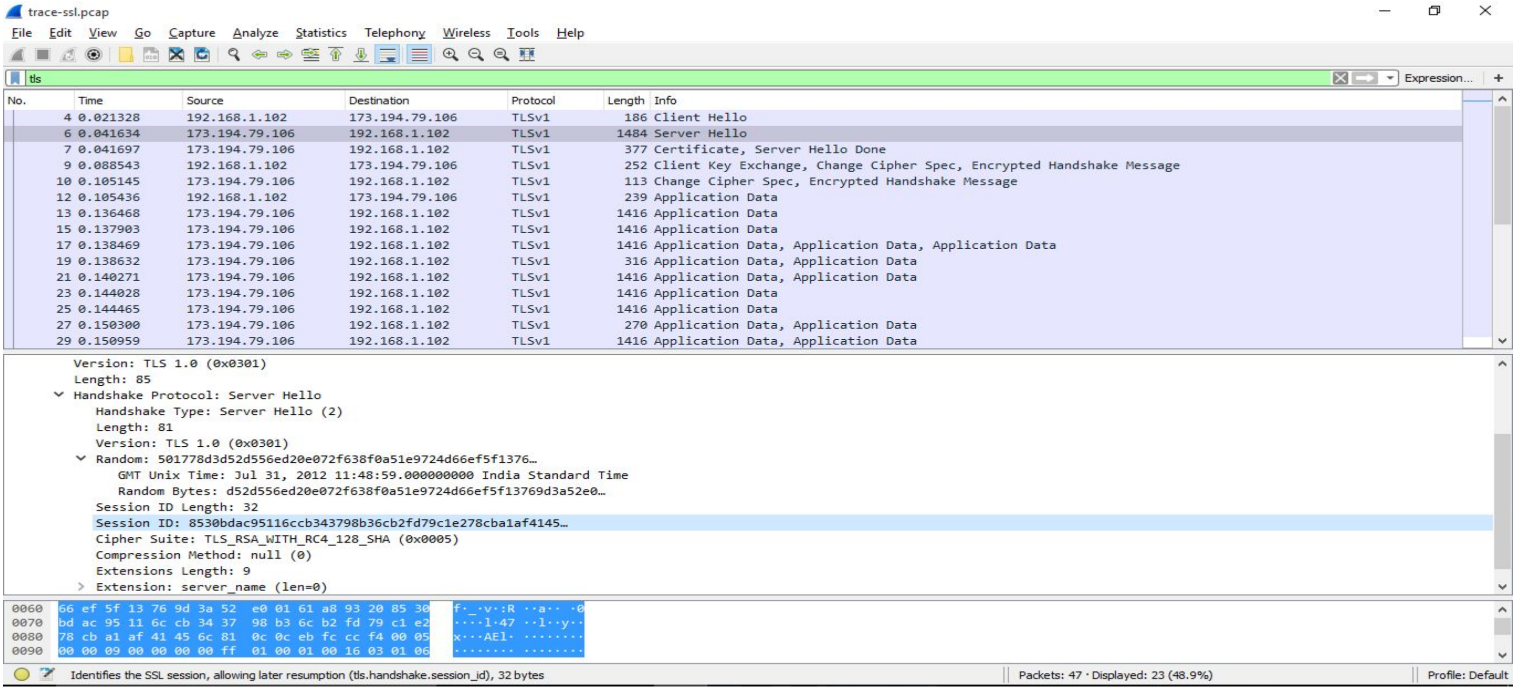
```
  ˅ TLSv1 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 85
    ˅ Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 81
        Version: TLS 1.0 (0x0301)
      ˅ Random: 501778d3d52d556ed20e072f638f0a51e9724d66ef5f1376…
          GMT Unix Time: Jul 31, 2012 11:48:59.000000000 India Standard Time
          Random Bytes: d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e0…
        Session ID Length: 32
        Session ID: 8530bdac95116ccb343798b36cb2fd79c1e278cba1af4145…
        Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
        Compression Method: null (0)
```

```
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··
```

Random values used for deriving keys (tls.handshake.random), 32 bytes | Packets: 47 · Displayed: 23 (48.9%) | Profile: Default

Q.4) 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.

Answer : 32 bytes


trace-ssl.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls
Expression…
+

```
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
```

```
    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: 501778d3d52d556ed20e072f638f0a51e9724d66ef5f1376…
        GMT Unix Time: Jul 31, 2012 11:48:59.000000000 India Standard Time
        Random Bytes: d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e0…
      Session ID Length: 32
      Session ID: 8530bdac95116ccb343798b36cb2fd79c1e278cba1af4145…
      Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
      Compression Method: null (0)
      Extensions Length: 9
    > Extension: server_name (len=0)
```

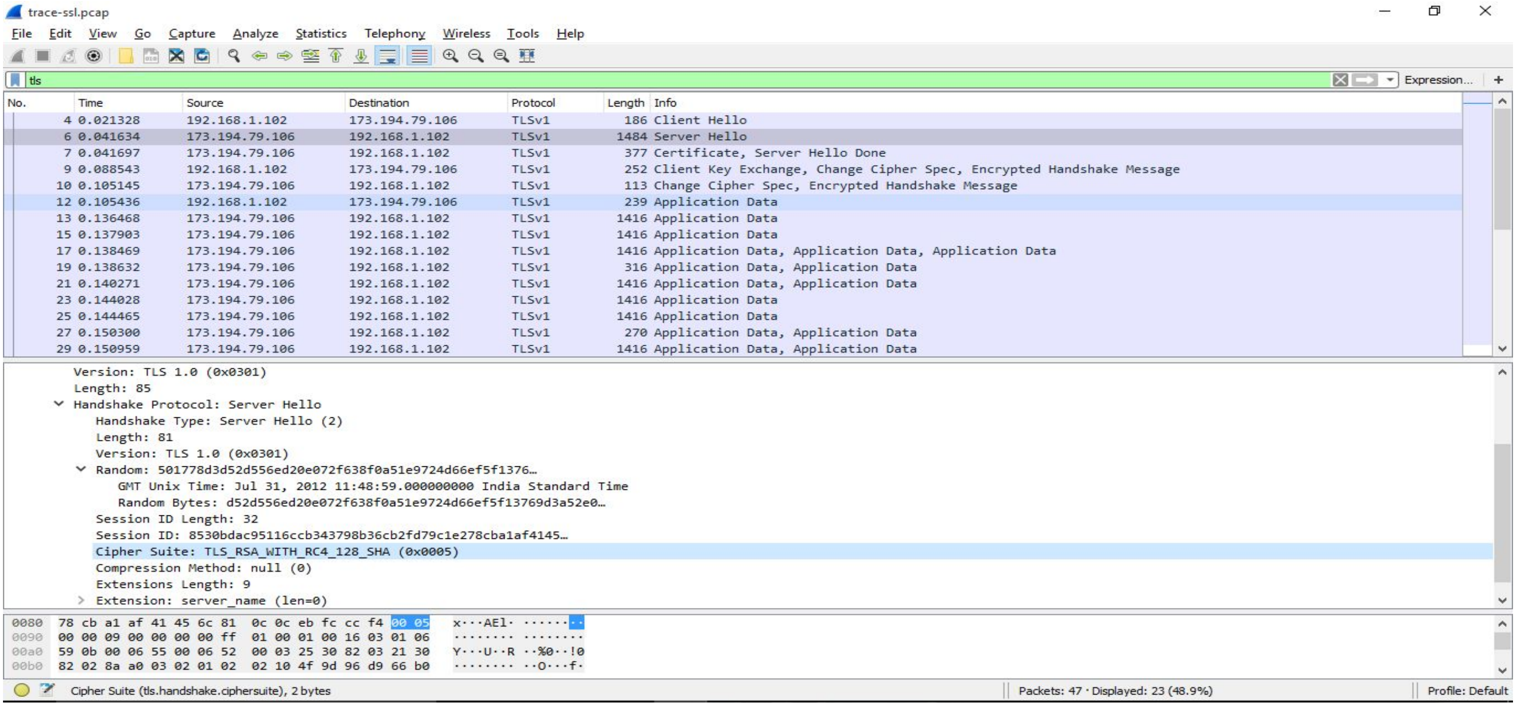
```
0060  66 ef 5f 13 76 9d 3a 52  e0 01 61 a8 93 20 85 30   f·_·v·:R ··a·· ·0
0070  bd ac 95 11 6c cb 34 37  98 b3 6c b2 fd 79 c1 e2   ····l·47 ··l··y··
0080  78 cb a1 af 41 45 6c 81  0c 0c eb fc cc f4 00 05   x···AEl· ········
0090  00 00 09 00 00 00 00 ff  01 00 01 00 16 03 01 06   ········ ········
```

Identifies the SSL session, allowing later resumption (tls.handshake.session_id), 32 bytes | Packets: 47 · Displayed: 23 (48.9%) | Profile: Default

Q.5) 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.

Answer : *Cipher suite name :* TLS_RSA_WITH_RC4_128_SHA

Cipher suite value : 5


trace-ssl.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls
Expression…
+

```
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
```

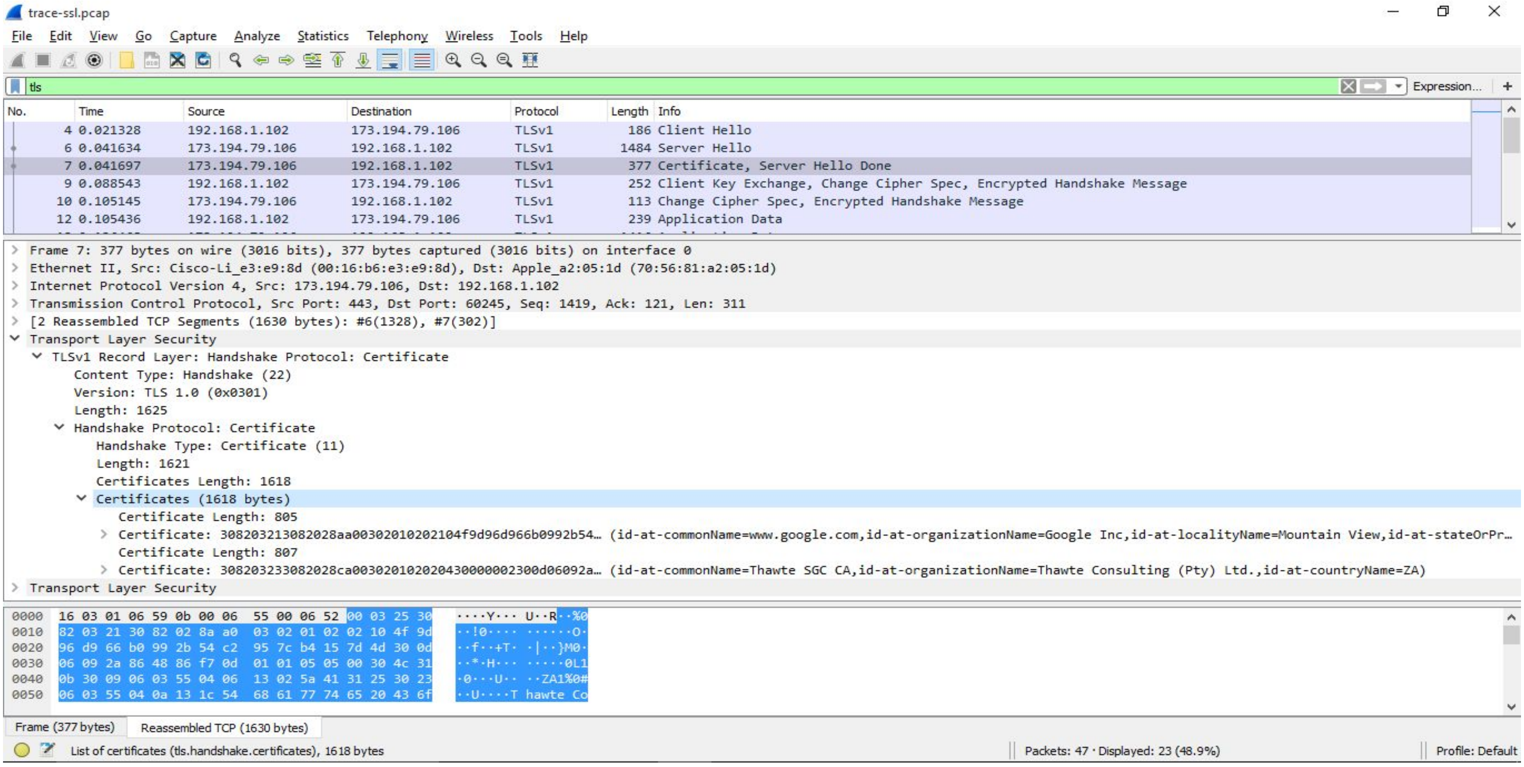
```
    Version: TLS 1.0 (0x0301)
    Length: 85
  v Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 81
      Version: TLS 1.0 (0x0301)
    v Random: 501778d3d52d556ed20e072f638f0a51e9724d66ef5f1376…
        GMT Unix Time: Jul 31, 2012 11:48:59.000000000 India Standard Time
        Random Bytes: d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e0…
      Session ID Length: 32
      Session ID: 8530bdac95116ccb343798b36cb2fd79c1e278cba1af4145…
      Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
      Compression Method: null (0)
      Extensions Length: 9
    > Extension: server_name (len=0)
```

```
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·
```

Cipher Suite (tls.handshake.ciphersuite), 2 bytes | Packets: 47 · Displayed: 23 (48.9%) | Profile: Default

Q.6) 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.

Answer : Server sends the certificate to the client.



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

tls

```
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
```

```
> Frame 7: 377 bytes on wire (3016 bits), 377 bytes captured (3016 bits) on interface 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: 308203213082028aa00302010202104f9d96d966b0992b54… (id-at-commonName=www.google.com,id-at-organizationName=Google Inc,id-at-localityName=Mountain View,id-at-stateOrPr…
          Certificate Length: 807
        > Certificate: 308203233082028ca003020102020430000002300d06092a… (id-at-commonName=Thawte SGC CA,id-at-organizationName=Thawte Consulting (Pty) Ltd.,id-at-countryName=ZA)
> Transport Layer Security
```

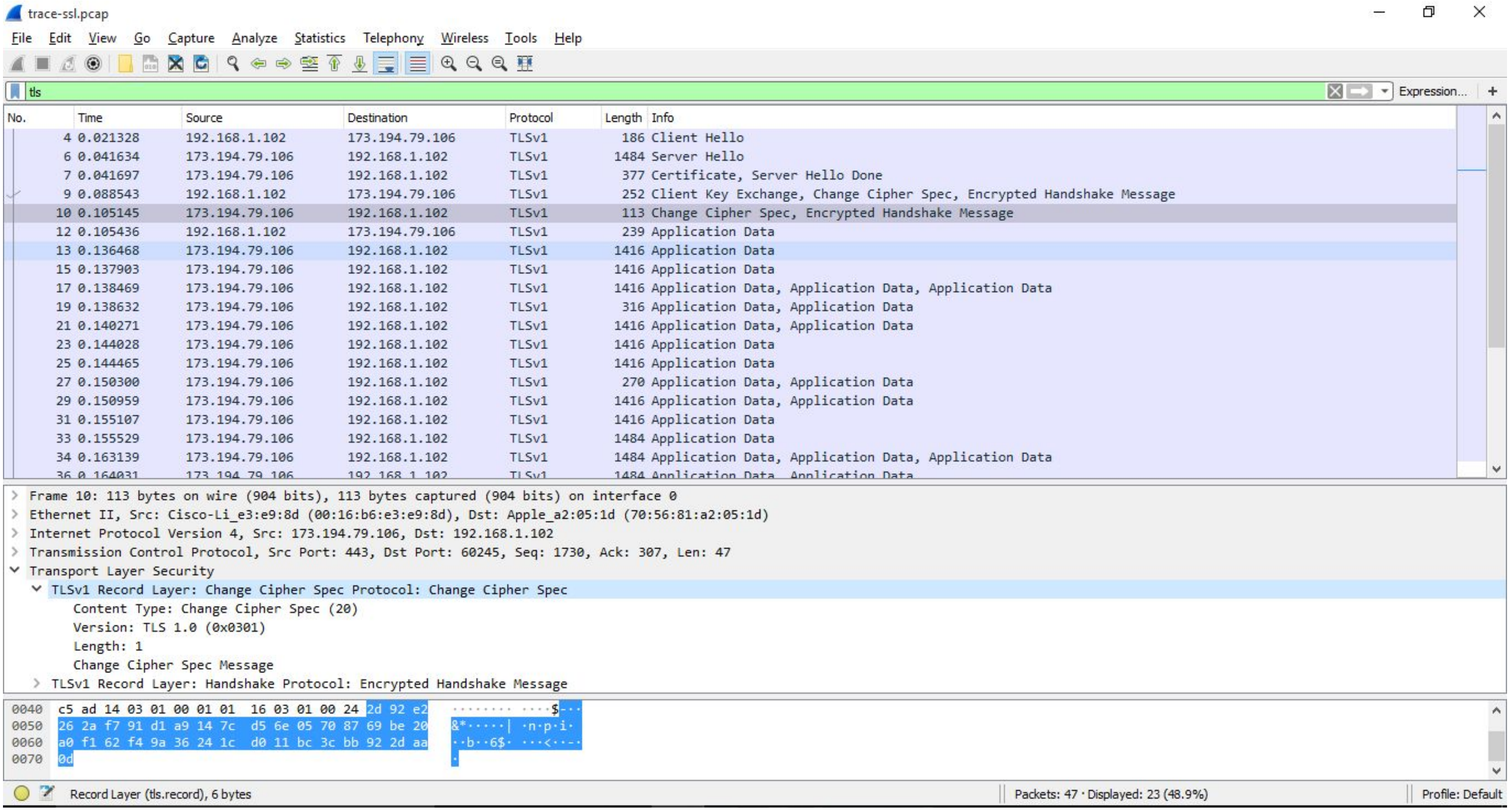
```
0000  16 03 01 06 59 0b 00 06  55 00 06 52 00 03 25 30   ····Y··· U··R··%0
0010  82 03 21 30 82 02 8a a0  03 02 01 02 02 10 4f 9d   ··!0···· ······O·
0020  96 d9 66 b0 99 2b 54 c2  95 7c b4 15 7d 4d 30 0d   ··f··+T· ·|··}M0·
0030  06 09 2a 86 48 86 f7 0d  01 01 05 05 00 30 4c 31   ··*·H··· ·····0L1
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
```

Frame (377 bytes) Reassembled TCP (1630 bytes)

List of certificates (tls.handshake.certificates), 1618 bytes | Packets: 47 · Displayed: 23 (48.9%) | Profile: Default

Q.7) Who sends the Change Cipher Spec message, the client, the server, or both?

Answer : Server sends the Change Cipher Spec message to the client.



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

tls

```
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
```

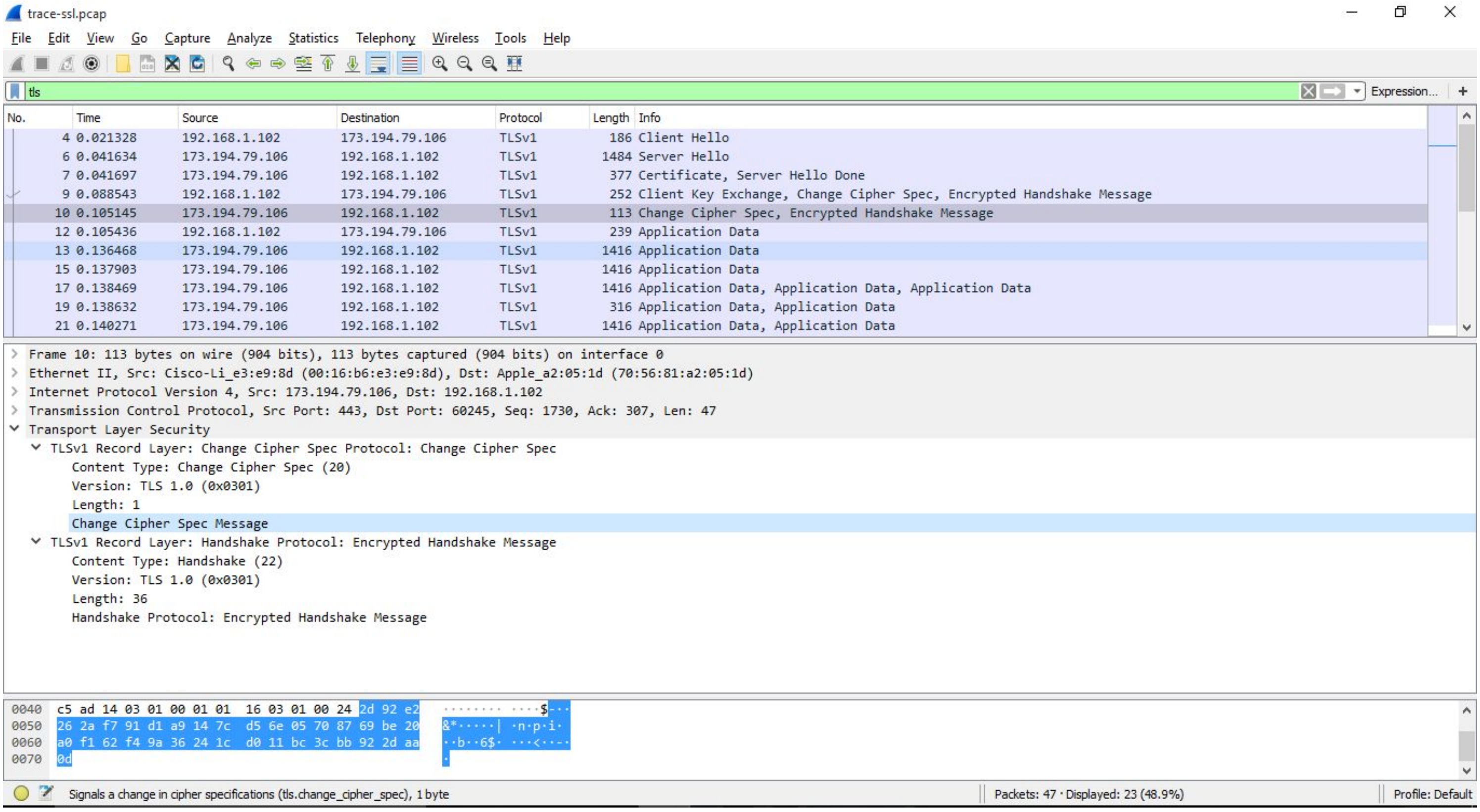
```
> Frame 10: 113 bytes on wire (904 bits), 113 bytes captured (904 bits) on interface 0
> Ethernet II, Src: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d), Dst: Apple_a2:05:1d (70:56:81:a2:05:1d)
> Internet Protocol Version 4, Src: 173.194.79.106, Dst: 192.168.1.102
> Transmission Control Protocol, Src Port: 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
  > TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
```

```
0040  c5 ad 14 03 01 00 01 01  16 03 01 00 24 2d 92 e2   ········ ····$-··
0050  26 2a f7 91 d1 a9 14 7c  d5 6e 05 70 87 69 be 20   &*·····| ·n·p·i·
0060  a0 f1 62 f4 9a 36 24 1c  d0 11 bc 3c bb 92 2d aa   ··b··6$· ···<··-·
0070  0d                                                 ·
```

Record Layer (tls.record), 6 bytes | Packets: 47 · Displayed: 23 (48.9%) | Profile: Default

Q.8) What are the contents carried inside the Change Cipher Spec message? Look past the Content Type and other headers to see the message itself.

Answer : It contains the keying information that signals a change in the cipher specifications so that both sides will have the same secret session key.


trace-ssl.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tls
Expression…
+

```
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
```

```
> Frame 10: 113 bytes on wire (904 bits), 113 bytes captured (904 bits) on interface 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
```

```
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                                                 ·
```

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

Conclusion :

We observed SSL/TLS (Secure Sockets Layer/ Transport Layer Security) in action using WireShark.