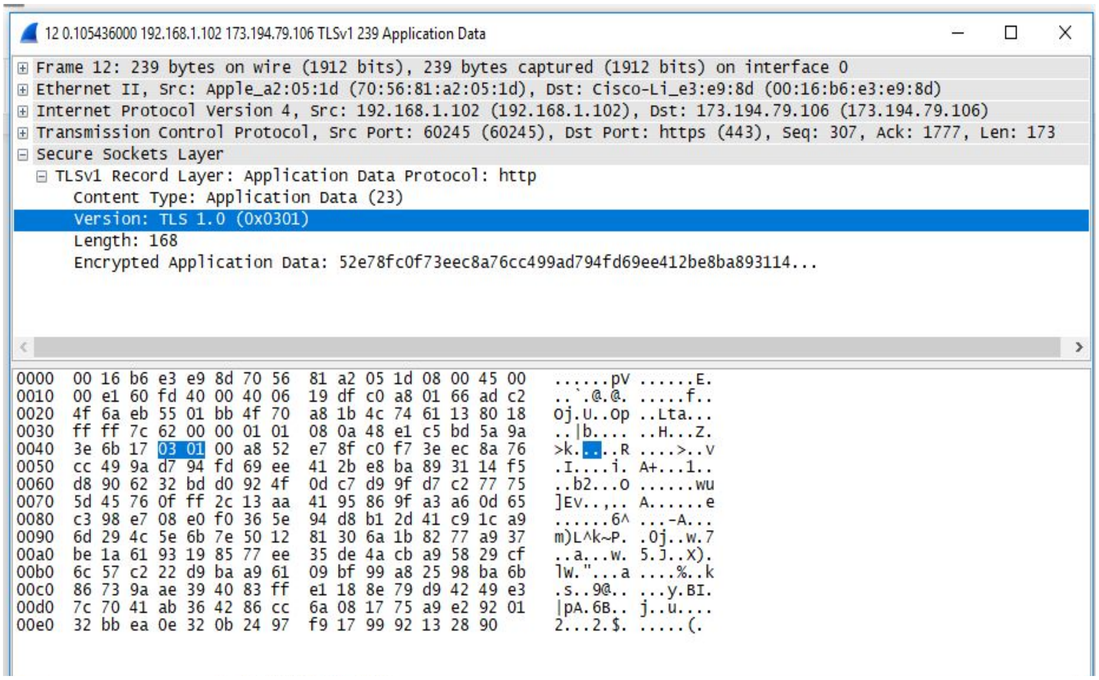
Secure Socket Layer(SSL)

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



12 0.105436000 192.168.1.102 173.194.79.106 TLSv1 239 Application Data

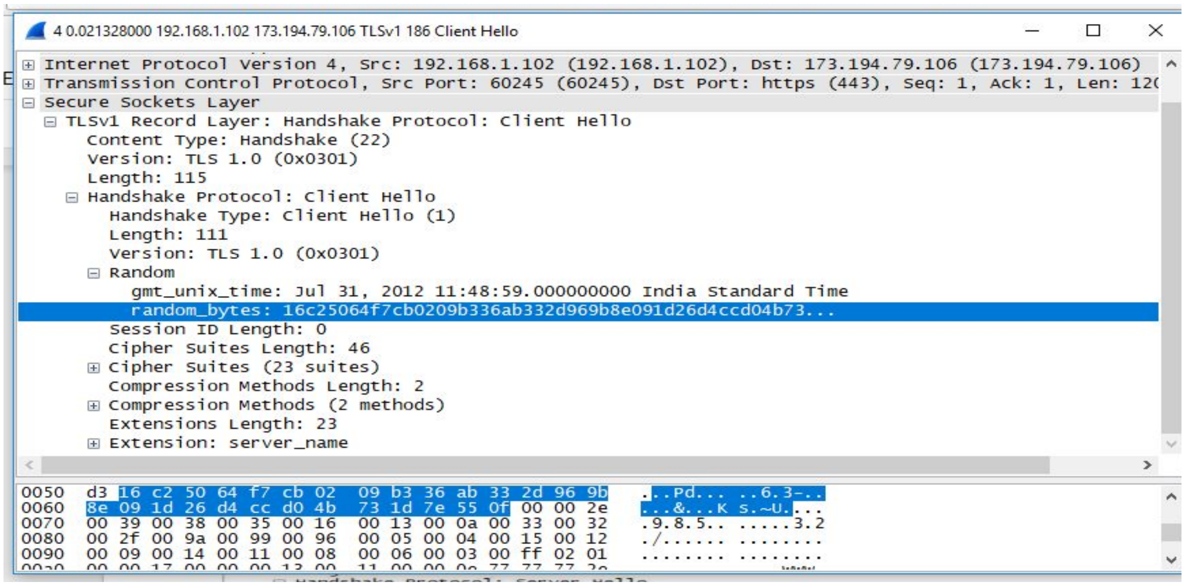
```
⊞ Frame 12: 239 bytes on wire (1912 bits), 239 bytes captured (1912 bits) on interface 0
⊞ Ethernet II, Src: Apple_a2:05:1d (70:56:81:a2:05:1d), Dst: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d)
⊞ Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 173.194.79.106 (173.194.79.106)
⊞ Transmission Control Protocol, Src Port: 60245 (60245), Dst Port: https (443), Seq: 307, Ack: 1777, Len: 173
⊟ Secure Sockets Layer
  ⊟ TLSv1 Record Layer: Application Data Protocol: http
      Content Type: Application Data (23)
      Version: TLS 1.0 (0x0301)
      Length: 168
      Encrypted Application Data: 52e78fc0f73eec8a76cc499ad794fd69ee412be8ba893114...
```

```
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.$. .....(.
```

2.What version constant is used in your trace, and which version of TLS does it represent?
ANS:TLS 1.0(0x0301)

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.

Client Hello random data:

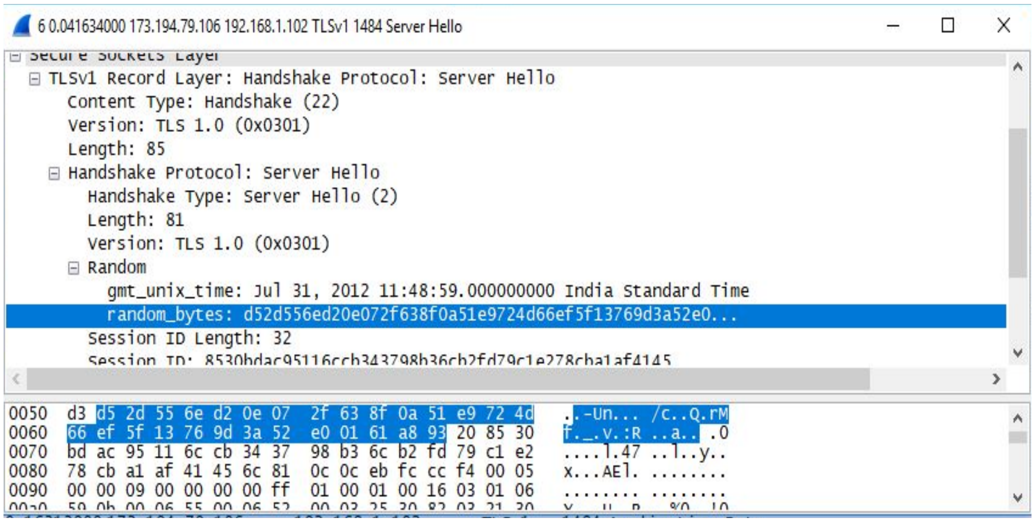


4 0.021328000 192.168.1.102 173.194.79.106 TLSv1 186 Client Hello

```
⊞ Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 173.194.79.106 (173.194.79.106)
⊞ Transmission Control Protocol, Src Port: 60245 (60245), Dst Port: https (443), Seq: 1, Ack: 1, Len: 12(
⊟ Secure Sockets Layer
  ⊟ 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
          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
      ⊞ Compression Methods (2 methods)
        Extensions Length: 23
      ⊞ Extension: server_name
```

```
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   ........ ........
```

Server Hello random data:



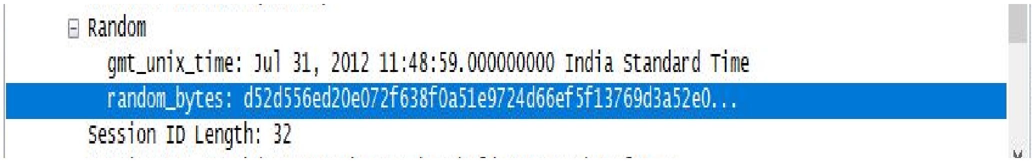
6 0.041634000 173.194.79.106 192.168.1.102 TLSv1 1484 Server Hello

```
⊟ Secure Sockets Layer
  ⊟ 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
          gmt_unix_time: Jul 31, 2012 11:48:59.000000000 India Standard Time
          random_bytes: d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e0...
        Session ID Length: 32
        Session ID: 8530bdac95116ccb343798b36cb2fd79c1e278cba1af4145
```

```
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   ........ ........
```

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.

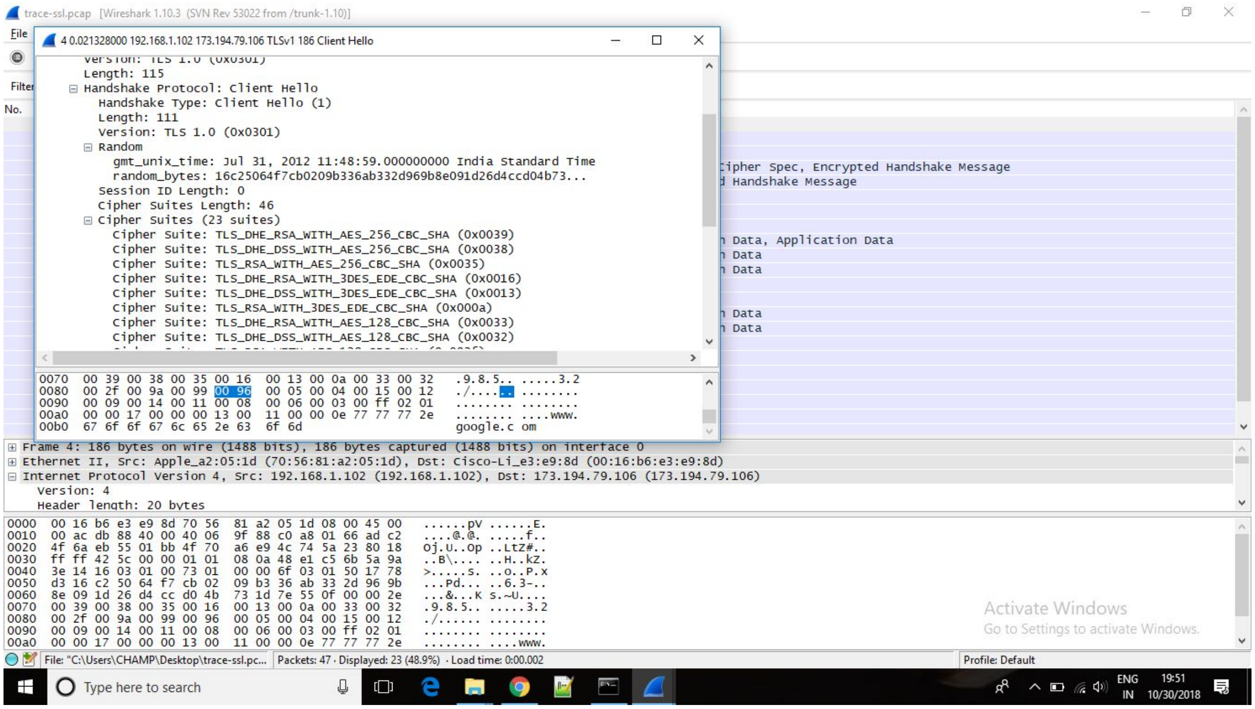
ANS:Session id length: 32



```
⊟ Random
    gmt_unix_time: Jul 31, 2012 11:48:59.000000000 India Standard Time
    random_bytes: d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e0...
  Session ID Length: 32
```

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.

Client cipher suite:



trace-ssl.pcap [Wireshark 1.10.3 (SVN Rev 53022 from /trunk-1.10)]

4 0.021328000 192.168.1.102 173.194.79.106 TLSv1 186 Client Hello

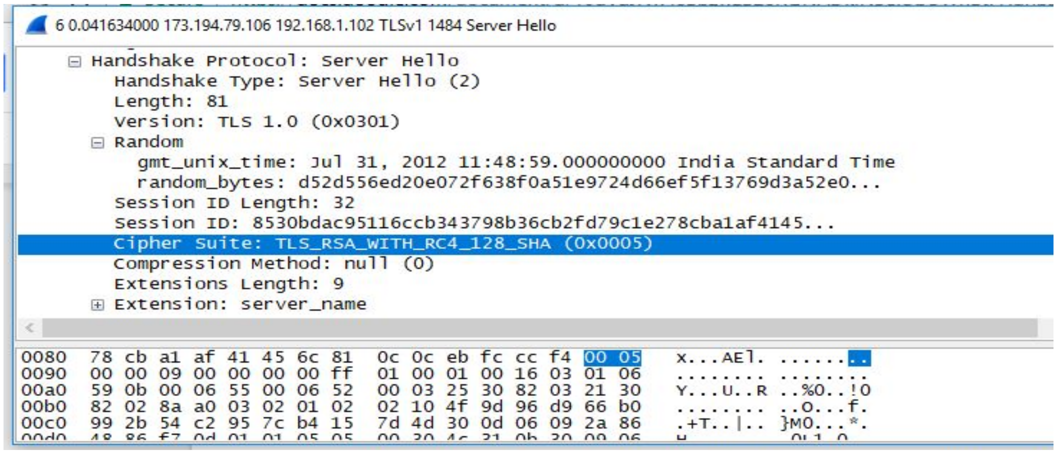
```
    Version: TLS 1.0 (0x0301)
    Length: 115
  ⊟ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 111
      Version: TLS 1.0 (0x0301)
    ⊟ Random
        gmt_unix_time: Jul 31, 2012 11:48:59.000000000 India Standard Time
        random_bytes: 16c25064f7cb0209b336ab332d969b8e091d26d4ccd04b73...
      Session ID Length: 0
      Cipher Suites Length: 46
    ⊟ Cipher Suites (23 suites)
        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)

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
```

```
ipher Spec, Encrypted Handshake Message
d Handshake Message
n Data, Application Data
n Data
n Data
n Data
n Data
```

```
⊞ Frame 4: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface 0
⊞ Ethernet II, Src: Apple_a2:05:1d (70:56:81:a2:05:1d), Dst: Cisco-Li_e3:e9:8d (00:16:b6:e3:e9:8d)
⊟ Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 173.194.79.106 (173.194.79.106)
    Version: 4
    Header length: 20 bytes

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.
```

File: "C:\Users\CHAMP\Desktop\trace-ssl.pc... Packets: 47 · Displayed: 23 (48.9%) · Load time: 0:00.002 Profile: Default

Server cipher suite:



6 0.041634000 173.194.79.106 192.168.1.102 TLSv1 1484 Server Hello

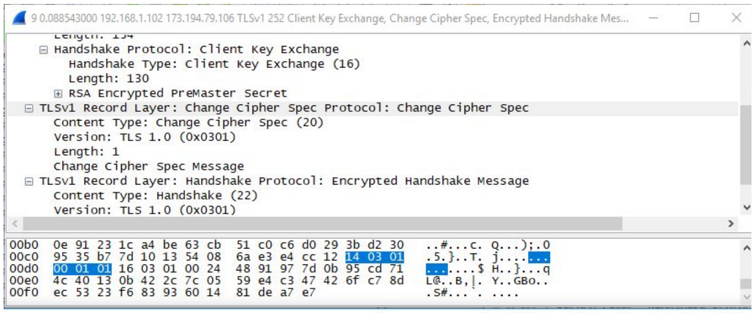
```
⊟ Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 81
    Version: TLS 1.0 (0x0301)
  ⊟ Random
      gmt_unix_time: Jul 31, 2012 11:48:59.000000000 India Standard Time
      random_bytes: d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e0...
    Session ID Length: 32
    Session ID: 8530bdac95116ccb343798b36cb2fd79c1e278cba1af4145...
    Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
    Compression Method: null (0)
    Extensions Length: 9
  ⊞ Extension: server_name

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...*.
```

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.

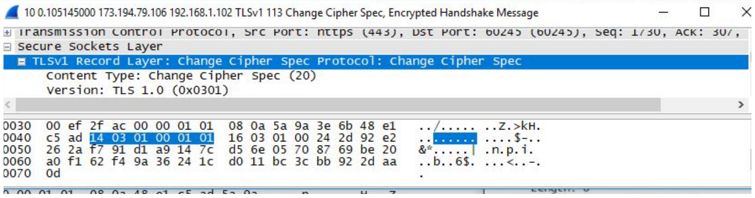
ANS: Server Sends the certificate to authenticate connection.

7.Who sends the Change Cipher Spec message, the client, the server, or both?
ANS: Both

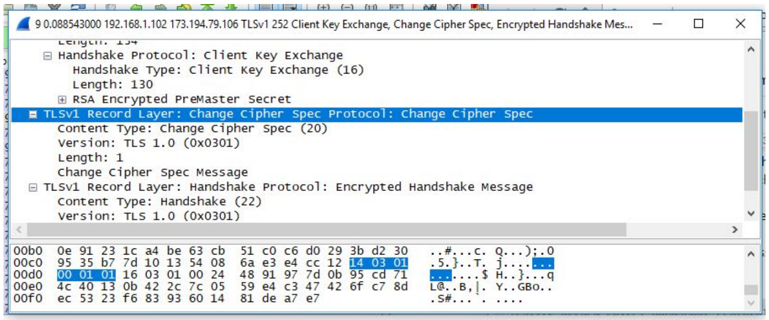
Client cipher spec and server cipher spec:



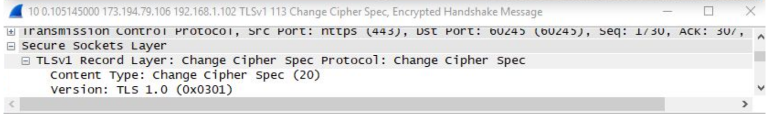
```
9 0.088543000 192.168.1.102 173.194.79.106 TLSv1 252 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mes...
      Length: 134
    ⊟ Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 130
      ⊞ RSA Encrypted PreMaster Secret
  ⊟ 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
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)

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#...`. ....
```



```
10 0.105145000 173.194.79.106 192.168.1.102 TLSv1 113 Change Cipher Spec, Encrypted Handshake Message
⊞ Transmission Control Protocol, Src Port: https (443), Dst Port: 60245 (60245), Seq: 1730, Ack: 307,
⊟ Secure Sockets Layer
  ⊟ TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.0 (0x0301)

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                                                 .
```



```
9 0.088543000 192.168.1.102 173.194.79.106 TLSv1 252 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mes...
      Length: 134
    ⊟ Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 130
      ⊞ RSA Encrypted PreMaster Secret
  ⊟ 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
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)

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#...`. ....
```



```
10 0.105145000 173.194.79.106 192.168.1.102 TLSv1 113 Change Cipher Spec, Encrypted Handshake Message
⊞ Transmission Control Protocol, Src Port: https (443), Dst Port: 60245 (60245), Seq: 1730, Ack: 307,
⊟ Secure Sockets Layer
  ⊟ TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.0 (0x0301)
```

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.

ANS: Content type , TLS Version , Length, Change Cipher Spec message