

# Cryptography and Network Security Lab

Name: Shrutika Rajendra Adhav

PRN : 2019BTECS00027

Batch : B1

## Examining TLS Client Hello packet :

The image shows a Wireshark packet capture of a TLS Client Hello packet. The packet list on the left shows a sequence of packets: a SYN packet, a SYN-ACK packet, an ACK packet, and then the TLS Client Hello packet (packet 4). The packet details pane on the left shows the structure of the TLS Client Hello packet, including the Handshake Protocol, Version (TLS 1.0), Length (115), and various cipher suites. The packet bytes pane on the right shows the raw data of the packet, including the TLS record header and the Client Hello message.

Packet 4: TLSv1 186 Client Hello

Content Type: Handshake (22)  
Version: TLS 1.0 (0x0301)  
Length: 115

Handshake Protocol: Client Hello  
Handshake Type: Client Hello (1)  
Length: 111  
Version: TLS 1.0 (0x0301)

Random: 501778d316c25064f7cb0209b336ab332d969b8e091d26d4ccd04b731d7e550f  
GMT Unix Time: Jul 31, 2012 11:48:59.000000000 India Standard Time  
Random Bytes: 16c25064f7cb0209b336ab332d969b8e091d26d4ccd04b731d7e550f  
Session ID Length: 0  
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)

Packet bytes: 0000 00 16 b6 e3 e9 8d 70 56 81 a2 05 1d 00 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..k2..  
0040 1e 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 9f 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 0e 77 77 77 2e .....www..  
00b0 6f 6f 6f 6f 6c 65 2e 63 6f 6d google.c om

## Examining Client Hello packet for possible encryption, hashing algorithms cipher suites :

The image shows a Wireshark packet capture of a TLS Client Hello packet. The packet list on the left shows the following packets:

- No. 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
- No. 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
- No. 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
- No. 4: 0.021328 192.168.1.102 → 173.194.79.106 TLSv1 186 Client Hello
- No. 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
- No. 6: 0.041634 173.194.79.106 → 192.168.1.102 TLSv1 1484 Server Hello
- No. 7: 0.041697 173.194.79.106 → 192.168.1.102 TLSv1 377 Certificate, Server Hello Done
- No. 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

The details pane for the Client Hello packet (No. 4) shows the following structure:

- 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)
  - 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

The packet bytes pane shows the raw data of the Client Hello packet, including the TLS record header and the Client Hello structure.

## Examining Server Hello message for cipher suite:

Cipher suite used here: TLS\_RSA\_WITH\_RC4\_128\_SHA (0x0005)

The image shows a Wireshark packet capture of a TLS Server Hello packet. The packet list on the left shows the following packets:

- No. 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
- No. 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
- No. 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
- No. 4: 0.021328 192.168.1.102 → 173.194.79.106 TLSv1 186 Client Hello
- No. 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
- No. 6: 0.041634 173.194.79.106 → 192.168.1.102 TLSv1 1484 Server Hello
- No. 7: 0.041697 173.194.79.106 → 192.168.1.102 TLSv1 377 Certificate, Server Hello Done
- No. 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

The details pane for the Server Hello packet (No. 6) shows the following structure:

- Transmission Control Protocol, Src Port: 443, Dst Port: 60245, Seq: 1, Ack: 121, Len: 1418
- Transport Layer Security
  - TLSv1 Record Layer: Handshake Protocol: Server Hello
  - Content Type: Handshake (22)
  - Version: TLS 1.0 (0x0301)
  - Length: 85
  - Handshake Protocol: Server Hello
  - Handshake Type: Server Hello (2)
  - Length: 81
  - Version: TLS 1.0 (0x0301)
  - Random: 501778d3d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893
  - GMT Unix Time: Jul 31, 2012 11:48:59.000000000 India Standard Time
  - Random Bytes: d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893
  - Session ID Length: 32
  - Session ID: 8530bdac95116cb343798b36cb2fd79c1e278cbaf41456c810c0ebfccc4
  - Cipher Suite: TLS\_RSA\_WITH\_RC4\_128\_SHA (0x0005)
  - Compression Method: null (0)
  - Extensions Length: 9
  - Extension: server\_name (len=0)
  - Type: server\_name (0)
  - Length: 0
  - Extension: renegotiation\_info (len=1)
  - Type: renegotiation\_info (65281)
  - Length: 1
  - Renegotiation Info extension
  - [JA3S Fullstring: 769,5,0-65281]
  - [JA3S: d2e6f7ef558ea8036c7e21b163b2d1af]

The packet bytes pane shows the raw data of the Server Hello packet, including the TLS record header and the Server Hello structure.

## Examining server certificate packet for certificate details :

trace file-ssl.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 0

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	TLVSV1	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	TLVSV1	1484	Server Hello
7	0.041697	173.194.79.106	192.168.1.102	TLVSV1	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

> Frame 7: 377 bytes on wire (3016 bits), 377 bytes captured (3016 bits) on interface en0, id 0  
> Ethernet II, Src: Cisco-Li\_e3:e9:8d (00:16:b6:e3:e9:8d), Dst: Apple\_a2:05:1d (70:56:81:a2:05:1d)  
> Internet Protocol Version 4, Src: 173.194.79.106, Dst: 192.168.1.102  
> Transmission Control Protocol, Src Port: 443, Dst Port: 60245, Seq: 1419, Ack: 121, Len: 311  
> [2 Reassembled TCP Segments (1630 bytes): #6(1328), #7(302)]

Transport Layer Security

- TLVSV1 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: 308203213082028aa0302010202104f9d9d966b0992b54c2957cb4157d4d300d6092a.....
      - signedCertificate
        - version: v3 (2)
        - serialNumber: 0x4f9d9d966b0992b54c2957cb4157d4d
        - signature (sha1WithRSAEncryption)
        - issuer: rdnSequence (0)
        - validity
          - subject: rdnSequence (0)
          - rdnSequence: 5 items (id-at-commonName=www.google.com,id-at-organizationName=Go...
            - rdnSequence item: 1 item (id-at-countryName=US)
            - rdnSequence item: 1 item (id-at-stateOrProvinceName=California)
            - relativeDistinguishedName item (id-at-stateOrProvinceName=California)

## Examining client key exchange packet for encryption of further packets:

trace file-ssl.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 0

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	TLVSV1	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	TLVSV1	1484	Server Hello
7	0.041697	173.194.79.106	192.168.1.102	TLVSV1	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	TLVSV1	252	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	0.105145	173.194.79.106	192.168.1.102	TLVSV1	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	TLVSV1	239	Application Data

> Frame 9: 252 bytes on wire (2016 bits), 252 bytes captured (2016 bits) on interface en0, id 0  
> Ethernet II, Src: Apple\_a2:05:1d (70:56:81:a2:05:1d), Dst: Cisco-Li\_e3:e9:8d (00:16:b6:e3:e9:8d)  
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 173.194.79.106  
> Transmission Control Protocol, Src Port: 60245, Dst Port: 443, Seq: 121, Ack: 1730, Len: 186  
> Transport Layer Security

- TLVSV1 Record Layer: Handshake Protocol: Client Key Exchange
  - Content Type: Handshake (22)
  - Version: TLS 1.0 (0x0301)
  - Length: 134
- Handshake Protocol: Client Key Exchange
  - Handshake Type: Client Key Exchange (16)
  - Length: 130
  - RSA Encrypted PreMaster Secret
- TLVSV1 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
- TLVSV1 Record Layer: Handshake Protocol: Encrypted Handshake Message
  - Content Type: Handshake (22)
  - Version: TLS 1.0 (0x0301)
  - Length: 36
  - Handshake Protocol: Encrypted Handshake Message

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

Ans: The content type is Handshake (22)

The image shows a Wireshark packet capture of a TLS handshake. The packet list on the left shows a series of packets from 192.168.1.102 to 173.194.79.106. The packet details pane on the right shows the 'Transport Layer Security' protocol selected, with the 'Handshake Protocol: Client Hello' record expanded. The 'Content Type: Handshake (22)' is highlighted in a red box. The 'Version: TLS 1.0 (0x0301)' is also highlighted in a red box. The packet bytes pane on the right shows the raw data of the Client Hello message, including the 'pV' field and the 'Google.c.o' domain name.

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

Ans: The TLS version used is TLS 1.0 (0x0301)

The image shows a Wireshark packet capture of a TLS handshake, similar to the first image. The packet list on the left shows a series of packets from 192.168.1.102 to 173.194.79.106. The packet details pane on the right shows the 'Transport Layer Security' protocol selected, with the 'Handshake Protocol: Client Hello' record expanded. The 'Content Type: Handshake (22)' is highlighted in a red box. The 'Version: TLS 1.0 (0x0301)' is also highlighted in a red box. The packet bytes pane on the right shows the raw data of the Client Hello message, including the 'pV' field and the 'Google.c.o' domain name.

### 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.

Ans : The random bytes is 28 hex characters of 14 bytes

The image shows a Wireshark packet capture of a TLSv1 Handshake Protocol: Server Hello. The packet is captured on interface en0, id 0, from 192.168.1.102 to 173.194.79.106. The packet details pane shows the following structure:

- Frame 6: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 bits) on interface en0, id 0
- Ethernet II, Src: Cisco-Li\_e3:e9:8d (00:16:b6:e3:e9:8d), Dst: Apple\_a2:05:1d (70:56:81:a2:05:1d)
- Internet Protocol Version 4, Src: 173.194.79.106, Dst: 192.168.1.102
- Transmission Control Protocol, Src Port: 443, Dst Port: 60245, Seq: 1, Ack: 121, Len: 1418
- Transport Layer Security
  - TLSv1 Record Layer: Handshake Protocol: Server Hello
    - Content Type: Handshake (22)
    - Version: TLS 1.0 (0x0301)
    - Length: 85
    - Handshake Protocol: Server Hello
      - Handshake Type: Server Hello (2)
      - Length: 81
      - Version: TLS 1.0 (0x0301)
      - Random bytes: d52d556ed20e72f638f8a51e9724d66ef5f13769d3a52e00161a893 (highlighted in red)
      - Session ID Length: 32
      - Session ID: 8530bdac95116cb343798b36cb2fd79c1e278cbaf41456c810c0ebfccc4
      - 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)

### 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: The random bytes is 32 hex characters of 16 bytes

The image shows a Wireshark packet capture of a TLSv1 Handshake Protocol: Server Hello. The packet is captured on interface en0, id 0, from 192.168.1.102 to 173.194.79.106. The packet details pane shows the following structure:

- Frame 6: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 bits) on interface en0, id 0
- Ethernet II, Src: Cisco-Li\_e3:e9:8d (00:16:b6:e3:e9:8d), Dst: Apple\_a2:05:1d (70:56:81:a2:05:1d)
- Internet Protocol Version 4, Src: 173.194.79.106, Dst: 192.168.1.102
- Transmission Control Protocol, Src Port: 443, Dst Port: 60245, Seq: 1, Ack: 121, Len: 1418
- Transport Layer Security
  - TLSv1 Record Layer: Handshake Protocol: Server Hello
    - Content Type: Handshake (22)
    - Version: TLS 1.0 (0x0301)
    - Length: 85
    - Handshake Protocol: Server Hello
      - Handshake Type: Server Hello (2)
      - Length: 81
      - Version: TLS 1.0 (0x0301)
      - Random bytes: d52d556ed20e72f638f8a51e9724d66ef5f13769d3a52e00161a893 (highlighted in red)
      - Session ID Length: 32
      - Session ID: 8530bdac95116cb343798b36cb2fd79c1e278cbaf41456c810c0ebfccc4 (highlighted in red)
      - 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)

**6. 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:** The Client will list the different cipher methods it supports

trace file-ssl.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 0

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

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)  
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

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 bb 55 01 bb 2f 70 a6 e9 4c 74 5a 23 80 18 0jU~Op~L1Z~  
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 15 00 12 ~9~8~5~...~3~2  
0080 00 2f 00 9a 00 99 00 06 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 google.c om ~www.  
00b0 67 6f 6f 67 6c 65 2e 63 6f 6d

Transmission Control Protocol (tcp), 32 bytes

Packets: 47 · Displayed: 47 (100.0%)

Profile: Default

Cipher suite used here: TLS\_RSA\_WITH\_RC4\_128\_SHA (0x0005)

Cipher suite is chosen by the Server

trace file-ssl.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 0

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

> Transmission Control Protocol, Src Port: 443, Dst Port: 60245, Seq: 1, Ack: 121, Len: 1418

> Transport Layer Security

> TLSv1 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 85

> Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 81

Version: TLS 1.0 (0x0301)

Random: 501778d3d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893

GMT Unix time: Jul 31, 2012 11:48:59.000000000 India Standard Time

Random Bytes: d52d556ed20e072f638f0a51e9724d66ef5f13769d3a52e00161a893

Session ID Length: 32

Session ID: 8530bdac95116cb343798b36cb2fd79c1e278cbaf41456c810c0ebfccf4

Cipher Suite: TLS\_RSA\_WITH\_RC4\_128\_SHA (0x0005)

Compression Method: null (0)

Extensions Length: 9

> Extension: server\_name (len=0)

Type: server\_name (0)

Length: 0

> Extension: renegotiation\_info (len=1)

Type: renegotiation\_info (65281)

Length: 1

> Renegotiation Info extension

[JA3S Fullstring: 769,5,0-65281]

[JA3S: d2e6f7ef558ea8036c7e21b163b2d1af]

0000 01 66 81 bb eb 55 4c 74 5a 23 4f 70 87 61 80 10 f.....ULT z00~  
0010 30 de 80 28 00 00 01 01 00 00 5a 9a 3c 2b 48 e1 ~0.....Z~>H~  
0020 3e 14 16 03 01 00 55 02 00 00 51 03 01 50 17 78 ~.~U.....Q~P~x  
0030 d3 d5 2d 55 6e d2 0e 07 2f 63 8f 0a 51 e9 72 4d f~Un~v~R ~a~c~Q~M  
0040 66 ef 5f 13 76 9d 3a 52 e0 01 61 a8 93 20 85 30 f~v~v~R ~a~a~c~  
0050 bd ac 95 11 6c cb 34 37 98 b3 6c b2 fd 79 c1 e2 ~1~47~1~y~  
0060 78 cb a1 af 41 45 6c 81 0c 0c eb fc cc f4 00 05 x~AEL.....  
0070 00 00 09 00 00 00 00 ff 01 00 01 00 16 03 01 06 ~.....  
0080 59 0b 00 06 55 00 06 52 00 03 25 30 82 03 21 30 Y~U~R ~X~0~l0  
0090 82 02 8a a0 03 02 01 02 02 10 4f 9d 9e 69 6b 60 ~.....O~f~  
00a0 99 2b 54 c2 95 7c b4 15 7d ad 30 0d 06 09 2a 86 ~+T~|~}~M~\*~  
00b0 48 86 f7 0d 01 01 05 05 00 30 4c 31 0b 30 09 06 H.....0L1~0~  
00c0 03 55 04 06 13 02 5a 41 31 25 30 23 06 03 55 04 ~U.....ZA 1X0~U~  
00d0 0a 13 1c 54 68 61 77 74 65 20 43 6f 6e 73 75 6c ~Thawt~e Consul  
00e0 74 69 6e 67 20 28 50 74 79 29 20 4c 74 64 2e 31 ting (Pt y) Ltd.1  
00f0 16 30 14 06 03 55 04 03 13 0d 54 68 61 77 74 65 ~0~U.....Thawte  
0100 20 53 47 43 20 43 41 30 1e 17 0d 31 31 31 30 32 SGC CA0 ~11102  
0110 36 30 30 30 30 30 30 5a 17 0d 31 33 30 39 33 30 6000000Z ~130930  
0120 32 33 35 39 35 39 5a 30 68 31 00 30 09 06 03 55 23595920 h1~0~U  
0130 04 06 13 02 55 53 31 13 30 11 06 03 55 04 08 13 ~US1~0~U~  
0140 0a 43 61 6c 69 66 6f 72 6e 69 61 31 16 30 14 06 ~Callifor nia1~0~  
0150 03 55 04 07 14 0d 4d 6f 75 6e 74 61 69 6e 20 56 ~U~U~Mo untain V~  
0160 69 65 77 31 13 30 11 06 03 55 04 0a 14 0a 47 6f iew1~0~U~U~Go  
0170 6f 67 6c 65 20 49 6e 63 31 17 30 15 06 03 55 04 ogle Inc 1~0~U~  
0180 03 14 0e 77 77 77 2e 67 6f 6f 6f 6c 65 2e 63 6f ~www.g oogle.co  
0190 6d 30 81 9f 30 0d 06 09 2a 86 48 86 f7 0d 01 01 m0~0~0~\*~H~  
01a0 01 05 00 03 81 8d 00 30 81 89 02 81 81 00 de b7 ~  
01b0 26 43 ae 99 85 cd 38 a7 15 09 b9 cf 0f c9 c3 55 &C~8~  
01c0 8c 88 ee 8c 8d 28 27 24 4b 2a 5e a0 d8 16 fa 61 ~('S K^~a~  
01d0 18 4b cf 6d 60 80 d3 35 40 32 72 c0 8f 12 d8 e5 ~K~m~S ~2r~

Transmission Control Protocol (tcp), 32 bytes

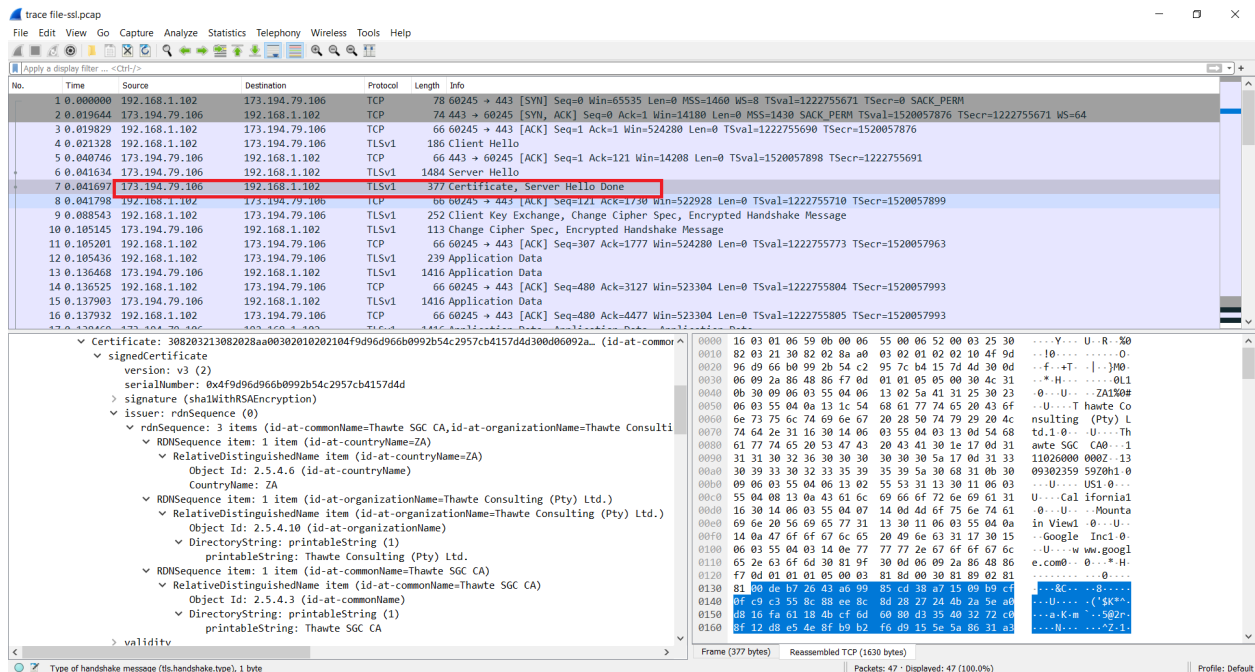
Packets: 47 · Displayed: 47 (100.0%)

Profile: Default



**7. 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 certificate is sent by the server



The image shows a Wireshark packet capture of a TLS handshake. The packet list on the left shows the following packets:

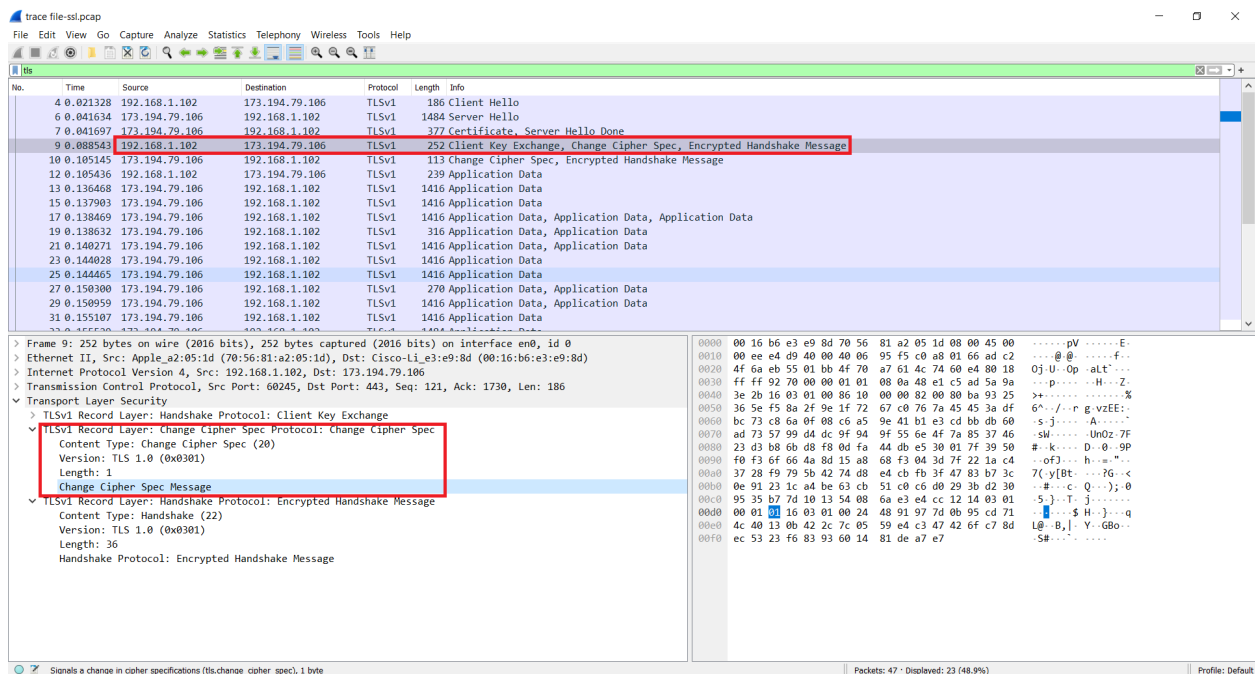
- No. 1: 0.000000 192.168.1.102 → 173.194.79.106 TCP 78 60245 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=0 TSval=1222755671 TSecr=0 SACK\_PERM
- No. 2: 0.019644 173.194.79.106 → 192.168.1.102 TCP 74 443 → 60245 [SYN, ACK] Seq=0 Ack=1 Win=14180 Len=0 MSS=1430 SACK\_PERM TSval=1520057876 TSecr=1222755671 WS=64
- No. 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
- No. 4: 0.021328 192.168.1.102 → 173.194.79.106 TLSv1 186 Client Hello
- No. 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
- No. 6: 0.041634 173.194.79.106 → 192.168.1.102 TLSv1 1484 Server Hello
- No. 7: 0.041697 173.194.79.106 → 192.168.1.102 TLSv1 377 Certificate, Server Hello Done
- No. 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
- No. 9: 0.088543 192.168.1.102 → 173.194.79.106 TLSv1 252 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
- No. 10: 0.105145 173.194.79.106 → 192.168.1.102 TLSv1 113 Change Cipher Spec, Encrypted Handshake Message
- No. 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
- No. 12: 0.105436 192.168.1.102 → 173.194.79.106 TLSv1 239 Application Data
- No. 13: 0.136468 173.194.79.106 → 192.168.1.102 TLSv1 1416 Application Data
- No. 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
- No. 15: 0.137903 173.194.79.106 → 192.168.1.102 TLSv1 1416 Application Data
- No. 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

The packet details pane for packet 7 shows the following structure:

- Certificate: 308203213082028a0030201020104f9d96d96b0992b54c2957cb4157d4d300d06092a. (id-at-commonName)
- signedCertificate
  - version: v3 (2)
  - serialNumber: 0x4f9d96d96b0992b54c2957cb4157d4d
  - signature (sha1WithRSAEncryption)
  - issuer: rdnSequence (0)
    - rdnSequence: 3 items (id-at-commonName=Thawte SGC CA,id-at-organizationName=Thawte Consulting)
    - RelativeDistinguishedName item (id-at-countryName=ZA)
      - Object Id: 2.5.4.6 (id-at-countryName)
      - CountryName: ZA
    - RelativeDistinguishedName item (id-at-organizationName=Thawte Consulting (Pty) Ltd.)
      - Object Id: 2.5.4.10 (id-at-organizationName)
      - DirectoryString: printableString (1)
        - printableString: Thawte Consulting (Pty) Ltd.
    - RelativeDistinguishedName item (id-at-commonName=Thawte SGC CA)
      - Object Id: 2.5.4.3 (id-at-commonName)
      - DirectoryString: printableString (1)
        - printableString: Thawte SGC CA

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

**Ans:** The client sends the change cipher spec message first



The image shows a Wireshark packet capture of a TLS handshake. The packet list on the left shows the following packets:

- No. 4: 0.021328 192.168.1.102 → 173.194.79.106 TLSv1 186 Client Hello
- No. 6: 0.041634 173.194.79.106 → 192.168.1.102 TLSv1 1484 Server Hello
- No. 7: 0.041697 173.194.79.106 → 192.168.1.102 TLSv1 377 Certificate, Server Hello Done
- No. 8: 0.088543 192.168.1.102 → 173.194.79.106 TLSv1 252 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
- No. 9: 0.105145 173.194.79.106 → 192.168.1.102 TLSv1 113 Change Cipher Spec, Encrypted Handshake Message
- No. 10: 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
- No. 12: 0.105436 192.168.1.102 → 173.194.79.106 TLSv1 239 Application Data
- No. 13: 0.136468 173.194.79.106 → 192.168.1.102 TLSv1 1416 Application Data
- No. 15: 0.137903 173.194.79.106 → 192.168.1.102 TLSv1 1416 Application Data
- No. 17: 0.138469 173.194.79.106 → 192.168.1.102 TLSv1 1416 Application Data, Application Data, Application Data
- No. 19: 0.138632 173.194.79.106 → 192.168.1.102 TLSv1 316 Application Data, Application Data
- No. 21: 0.140271 173.194.79.106 → 192.168.1.102 TLSv1 1416 Application Data, Application Data
- No. 23: 0.144028 173.194.79.106 → 192.168.1.102 TLSv1 1416 Application Data
- No. 25: 0.144665 173.194.79.106 → 192.168.1.102 TLSv1 1416 Application Data
- No. 27: 0.150300 173.194.79.106 → 192.168.1.102 TLSv1 270 Application Data, Application Data
- No. 29: 0.150959 173.194.79.106 → 192.168.1.102 TLSv1 1416 Application Data, Application Data
- No. 31: 0.155107 173.194.79.106 → 192.168.1.102 TLSv1 1416 Application Data

The packet details pane for packet 9 shows the following structure:

- Frame 9: 252 bytes on wire (2016 bits), 252 bytes captured (2016 bits) on interface en0, id 0
- Ethernet II, Src: Apple-a2:05:1d (70:56:81:a2:05:1d), Dst: Cisco-Li\_e3:e9:8d (00:16:b6:e3:e9:8d)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 173.194.79.106
- Transmission Control Protocol, Src Port: 60245, Dst Port: 443, Seq: 121, Ack: 1730, Len: 186
- Transport Layer Security
  - Handshake Protocol: Client Key Exchange
  - TLSv1 Record Layer: Handshake Protocol: Change Cipher Spec
    - Content Type: Change Cipher Spec (20)
    - Version: TLS 1.0 (0x0301)
    - Length: 1
    - Change Cipher Spec Message
  - Handshake Protocol: Encrypted Handshake Message
    - Content Type: Handshake (22)
    - Version: TLS 1.0 (0x0301)
    - Length: 36
    - Handshake Protocol: Encrypted Handshake Message

## Server change cipher spec message

The screenshot shows a Wireshark capture of a TLS handshake. The packet list on the left highlights packet 10, which is a 'Change Cipher Spec, Encrypted Handshake Message' from the server (192.168.1.102) to the client (173.194.79.106). The packet details pane on the right shows the 'Transport Layer Security' protocol tree. Under 'TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec', the 'Content Type: Change Cipher Spec (20)' is highlighted. The 'Version: TLS 1.0 (0x0301)' and 'Length: 1' are also visible. The packet bytes pane on the far right shows the raw data of the message.

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

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  
▼ Transport Layer Security  
    ▼ 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

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...0j..  
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 4b 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.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:

The screenshot shows a Wireshark capture of a TLS handshake. The packet list on the left highlights packet 10, which is a 'Change Cipher Spec, Encrypted Handshake Message' from the server (192.168.1.102) to the client (173.194.79.106). The packet details pane on the right shows the 'Transport Layer Security' protocol tree. Under 'TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec', the 'Content Type: Change Cipher Spec (20)' is highlighted. The 'Version: TLS 1.0 (0x0301)' and 'Length: 1' are also visible. The packet bytes pane on the far right shows the raw data of the message.

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

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  
▼ Transport Layer Security  
    ▼ 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

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...0j..  
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 4b 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