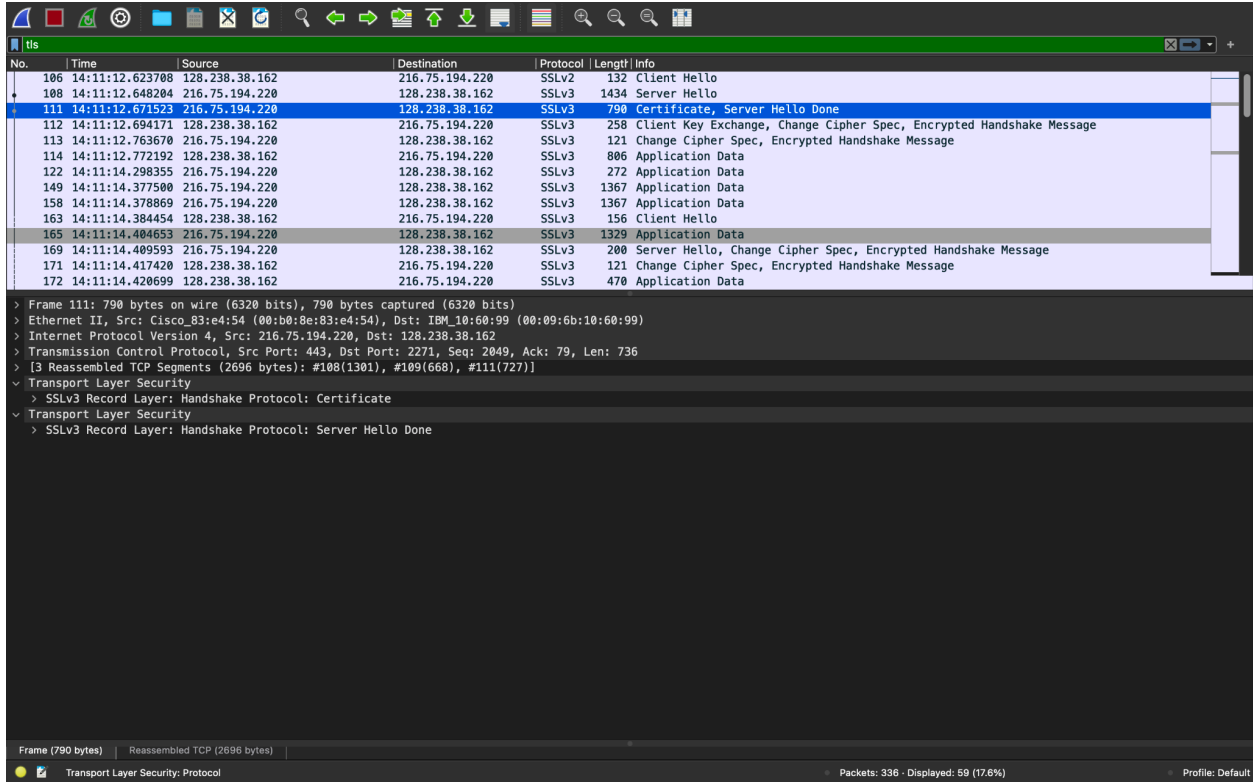


# Foundation of Computer Networks - Wireshark Project

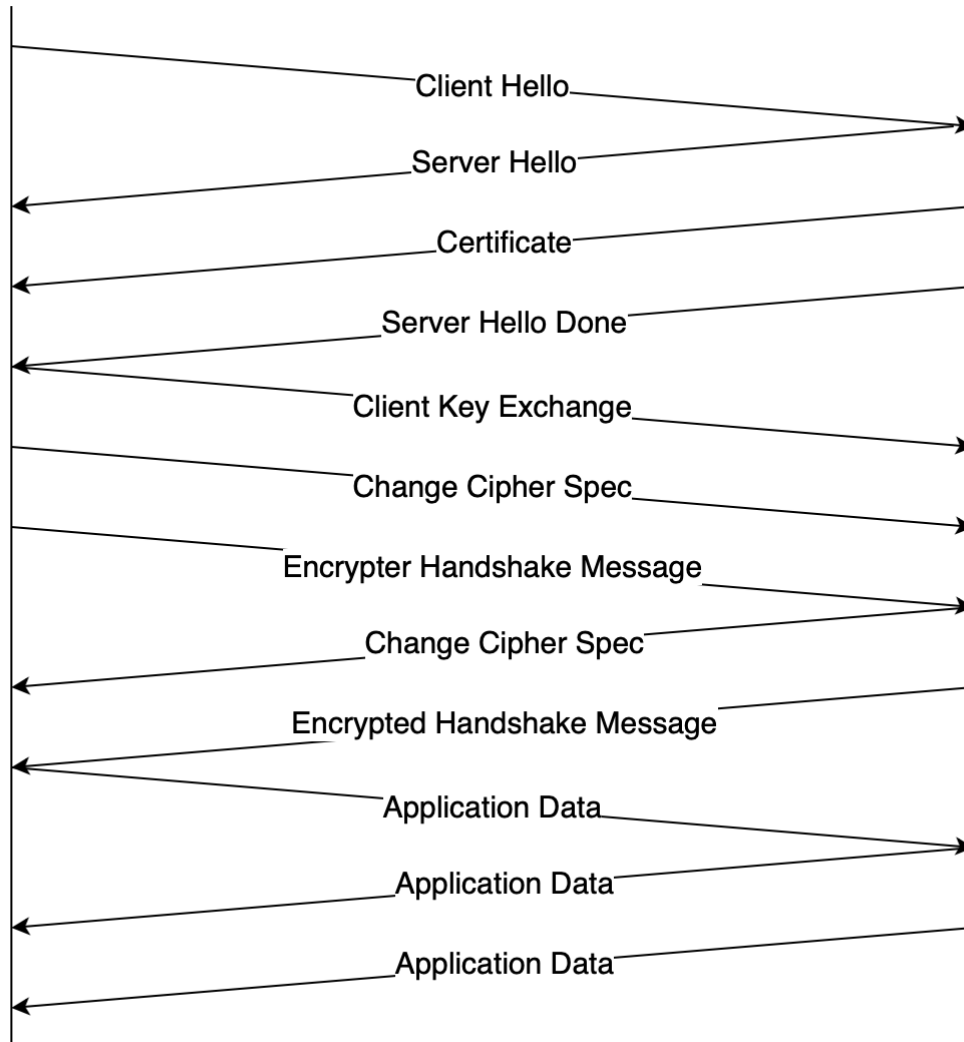
## Bhavin Oza (bo2115)



1).

Frame	Source	SSL Count	SSL Type
106	128.238.38.162	1	Client Hello
108	216.75.194.220	1	Server Hello
111	216.75.194.220	2	Certificate, Server Hello Done
112	128.238.38.162	3	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
113	216.75.194.220	2	Change Cipher Spec, Encrypted Handshake Message
114	128.238.38.162	1	Application Data
122	216.75.194.220	1	Application Data
149	216.75.194.220	1	Application Data

**Foundation of Computer Networks - Wireshark Project**  
**Bhavin Oza (bo2115)**



2). Content Type is 1 byte

Version is 2 bytes

Length is 2 bytes

3). The value of Content Type is 22

## Foundation of Computer Networks - Wireshark Project

Bhavin Oza (bo2115)

```
Window: 65535
[Calculated window size: 65535]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0xe755 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [Timestamps]
> [SEQ/ACK analysis]
TCP payload (78 bytes)
- Transport Layer Security
  - SSLv2 Record Layer: Client Hello
    [Version: SSL 2.0 (0x0002)]
    Length: 76
    Handshake Message Type: Client Hello (1)
    Version: SSL 3.0 (0x0300)
    Cipher Spec Length: 51
    Session ID Length: 0
    Challenge Length: 16
    > Cipher Specs (17 specs)
      Challenge
0000 00 00 0c 07 ac 00 00 09 6b 10 60 99 08 00 45 00 ..... k`...E.
0010 00 76 48 28 40 00 80 06 6f a1 80 ee 26 a2 d8 4b .vH(@...o...&..K
0020 c2 dc 08 df 01 bb 56 d2 08 c5 4c 9e 64 9f 50 18 .....V...L..d..P.
0030 ff ff e7 55 00 00 80 4c 01 03 00 00 33 00 00 00 ...U...L...3...
0040 10 00 00 04 00 00 05 00 00 0a 01 00 80 07 00 c0 .....
0050 03 00 80 00 00 09 06 00 40 00 00 64 00 00 62 00 ..... @..d..b.
0060 00 03 00 00 06 02 00 80 04 00 80 00 00 13 00 00 .....
0070 12 00 00 63 66 df 78 4c 04 8c d6 04 35 dc 44 89 ...cf.xL...5.D.
0080 89 46 99 09 ..F..
```

4). Yes.

The value of Challenge is 66 df 78 4c 04 8c d6 04 35 dc 44 89 89 46 99 09

# Foundation of Computer Networks - Wireshark Project

## Bhavin Oza (bo2115)

The image shows a Wireshark packet capture of a TLS handshake. The packet list on the left shows packets 106 through 172. The selected packet 106 is a Client Hello. The packet details pane on the right shows the TLS handshake structure, including the Client Hello, Server Hello, Certificate, Server Hello Done, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message, Application Data, and Client Hello. The packet bytes pane at the bottom shows the raw data of the Client Hello, including the challenge data used to authenticate the server.

No.	Time	Source	Destination	Protocol	Length	Info
106	14:11:12.623708	128.238.38.162	216.75.194.220	SSLv2	132	Client Hello
108	14:11:12.648204	216.75.194.220	128.238.38.162	SSLv3	1434	Server Hello
111	14:11:12.671523	216.75.194.220	128.238.38.162	SSLv3	798	Certificate, Server Hello Done
112	14:11:12.694171	128.238.38.162	216.75.194.220	SSLv3	258	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
113	14:11:12.763670	216.75.194.220	128.238.38.162	SSLv3	121	Change Cipher Spec, Encrypted Handshake Message
114	14:11:12.772192	128.238.38.162	216.75.194.220	SSLv3	806	Application Data
122	14:11:14.298355	216.75.194.220	128.238.38.162	SSLv3	272	Application Data
149	14:11:14.377500	216.75.194.220	128.238.38.162	SSLv3	1367	Application Data
158	14:11:14.378869	216.75.194.220	128.238.38.162	SSLv3	1367	Application Data
163	14:11:14.384454	128.238.38.162	216.75.194.220	SSLv3	156	Client Hello
165	14:11:14.484653	216.75.194.220	128.238.38.162	SSLv3	1329	Application Data
169	14:11:14.489593	216.75.194.220	128.238.38.162	SSLv3	208	Server Hello, Change Cipher Spec, Encrypted Handshake Message
171	14:11:14.417420	128.238.38.162	216.75.194.220	SSLv3	121	Change Cipher Spec, Encrypted Handshake Message
172	14:11:14.420699	128.238.38.162	216.75.194.220	SSLv3	478	Application Data

Challenge Length: 16

✓ Cipher Specs (17 specs)

- Cipher Spec: TLS\_RSA\_WITH\_RC4\_128\_MD5 (0x000004)
- Cipher Spec: TLS\_RSA\_WITH\_RC4\_128\_SHA (0x000005)
- Cipher Spec: TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (0x00000a)
- Cipher Spec: SSL2\_RC4\_128\_WITH\_MD5 (0x010000)
- Cipher Spec: SSL2\_DES\_192\_EDE3\_CBC\_WITH\_MD5 (0x0700c0)
- Cipher Spec: SSL2\_RC2\_128\_CBC\_WITH\_MD5 (0x030080)
- Cipher Spec: TLS\_RSA\_WITH\_DES\_CBC\_SHA (0x000009)
- Cipher Spec: SSL2\_DES\_64\_CBC\_WITH\_MD5 (0x000040)
- Cipher Spec: TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA (0x000064)
- Cipher Spec: TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA (0x000062)
- Cipher Spec: TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 (0x000003)
- Cipher Spec: TLS\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5 (0x000006)
- Cipher Spec: SSL2\_RC4\_128\_EXPORT40\_WITH\_MD5 (0x020080)
- Cipher Spec: SSL2\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5 (0x040080)
- Cipher Spec: TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA (0x000013)
- Cipher Spec: TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA (0x000012)
- Cipher Spec: TLS\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA (0x000063)

Challenge

```
0000 00 00 0c 07 ac 00 00 09 6b 10 60 99 08 00 45 00 .....k....E
0010 00 76 48 28 40 00 80 06 6f a1 80 ee 26 a2 d8 4b ..VH(@...a...K
0020 c2 dc 00 df 01 bb 55 d2 00 c5 4e 9e 64 9f 50 18 ....V...L..d..P
0030 ff ff e7 55 00 00 00 4c 01 03 00 00 33 00 00 00 ...U...L...3...
0040 10 00 00 04 00 00 05 00 00 0a 01 00 00 07 00 c0 .....@...d...b
0050 03 00 00 00 00 09 06 00 40 00 00 64 00 00 62 00 .....@...d...b
0060 00 03 00 00 06 02 00 80 04 00 80 00 13 00 00 .....@...d...b
0070 12 00 00 63 66 df 78 4c 04 8c d6 04 35 dc 44 89 ...cf..xL...5..D
0080 89 46 99 09 .....F..
```

Challenge data used to authenticate server (tls.handshake.challenge), 16 bytes

Packets: 336 - Displayed: 59 (17.6%)

Profile: Default

5). Yes.

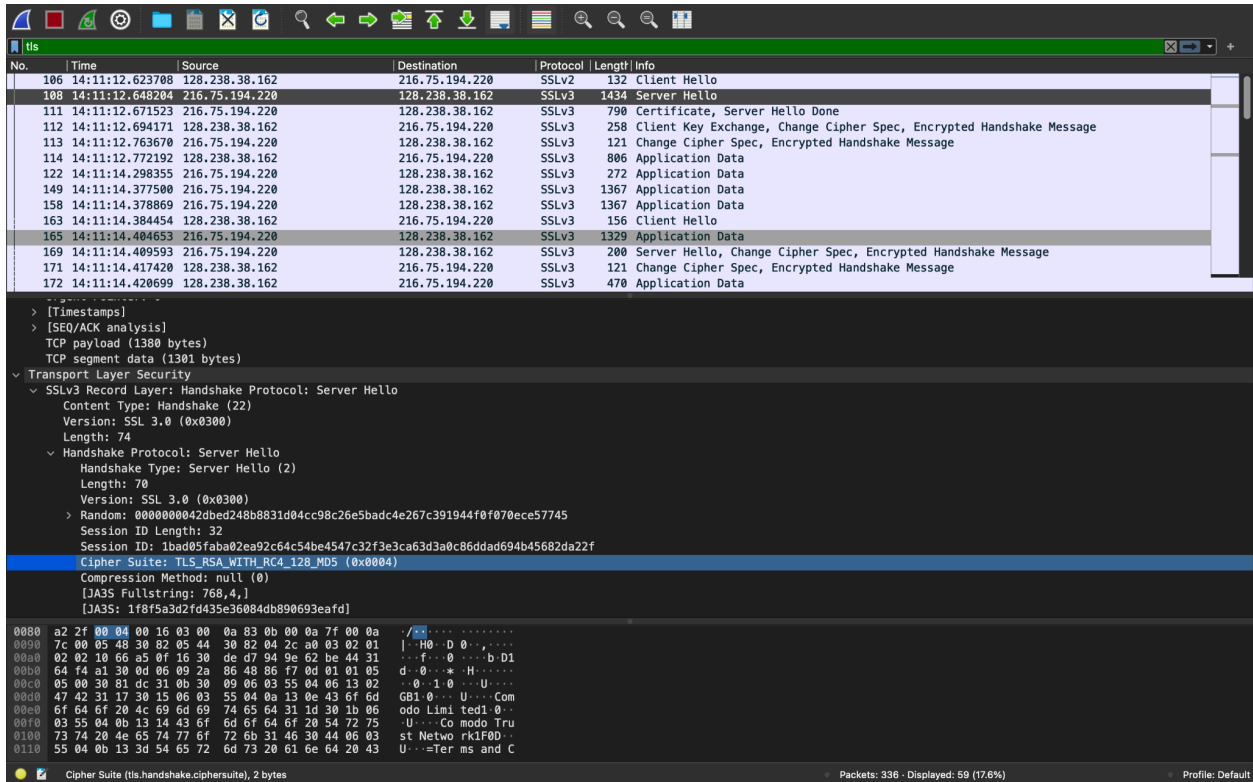
RSA for public cryptography algorithm.

RC4 for symmetric key cipher

MD5 hash algorithm

# Foundation of Computer Networks - Wireshark Project

## Bhavin Oza (bo2115)

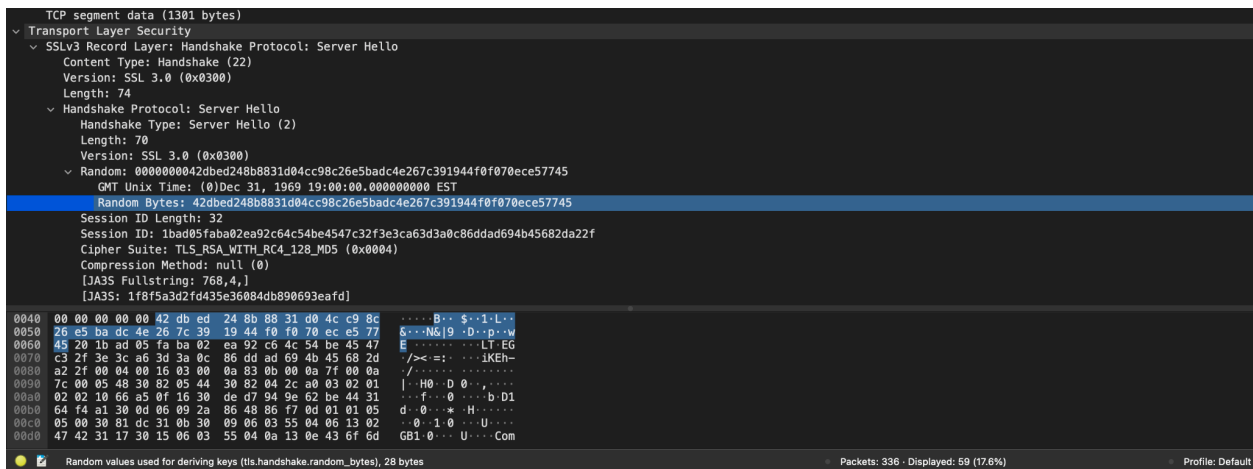


6). Yes.

RSA for public cryptography algorithm

RC4 for symmetric key cipher

MD5 hash algorithm



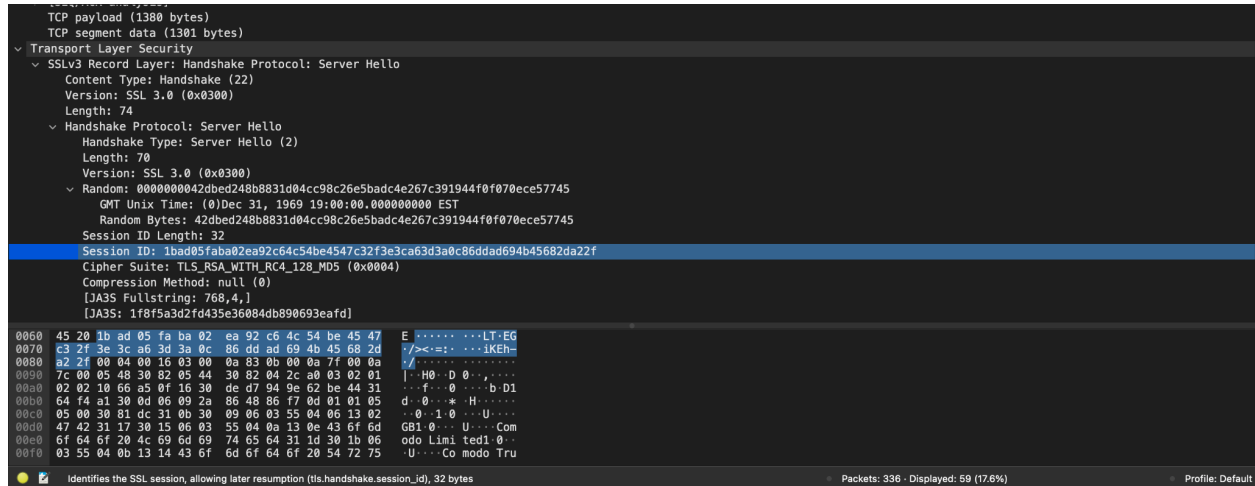
7). Yes.

The nonce is known as random bytes as shown above, which is 28 bytes long

The purpose of the nonce is to avoid replay attacks.

# Foundation of Computer Networks - Wireshark Project

## Bhavin Oza (bo2115)

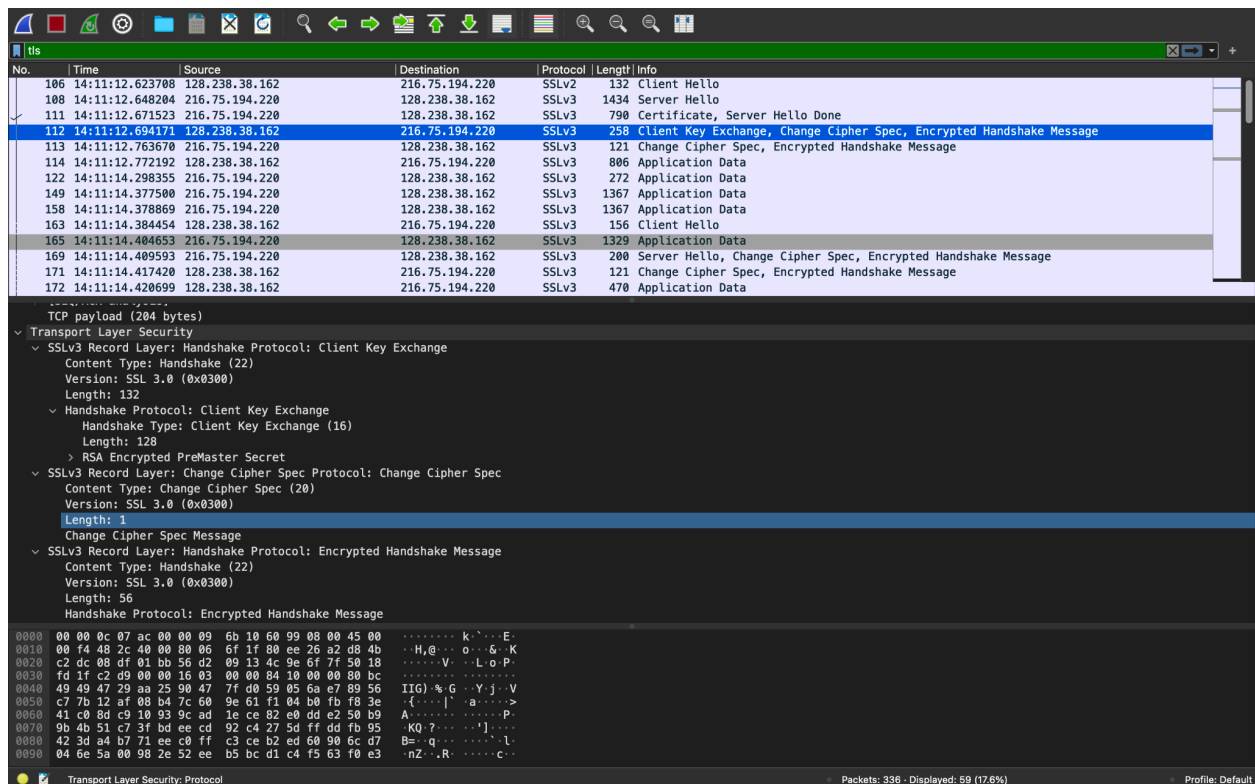


8). Yes, and the session ID is 32 bytes long

The purpose of the Session ID is it provides a persistent identifier for the SSL session. The client may resume the same session later by using server provided session ID

9). No.

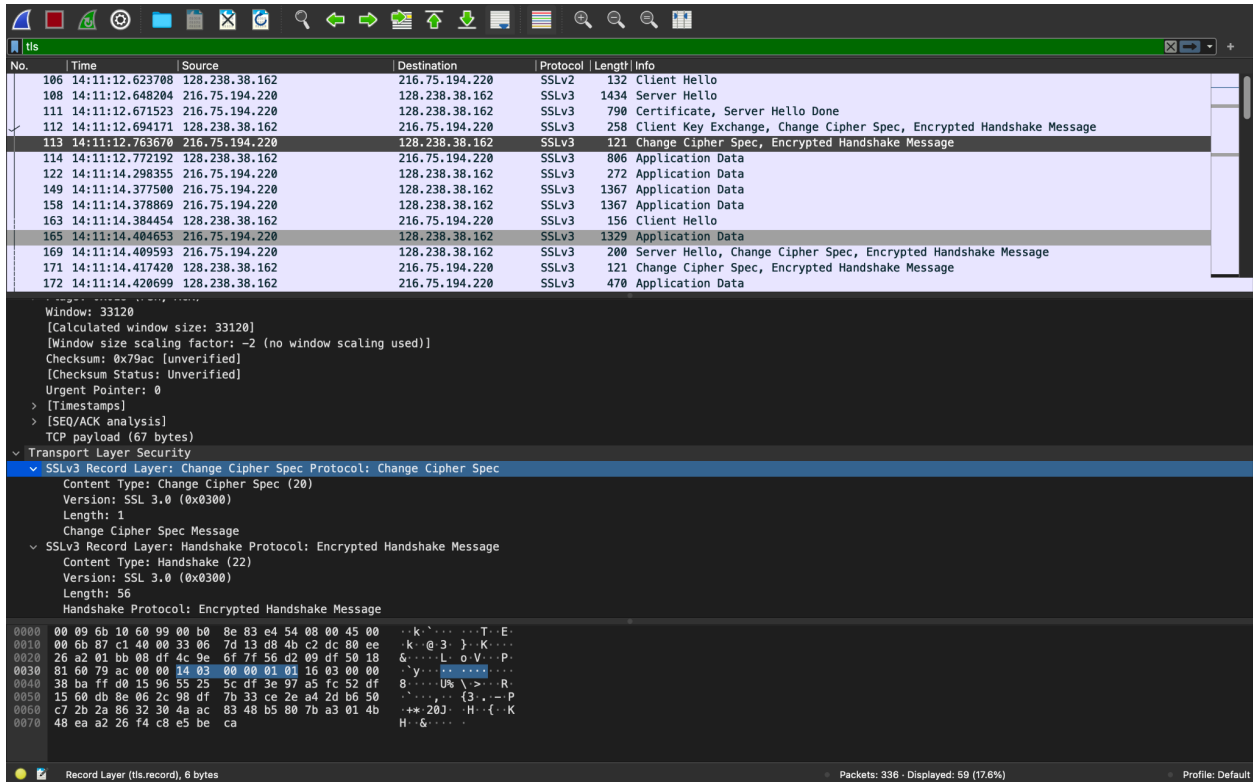
The certificate is in another record



10). Yes. The client and server share the same master key and it is 128 bytes long

## Foundation of Computer Networks - Wireshark Project

### Bhavin Oza (bo2115)



11). The purpose of the Change Cipher Spec is to indicate that the content will be encrypted by the client and sent.

The length is 1 byte long.

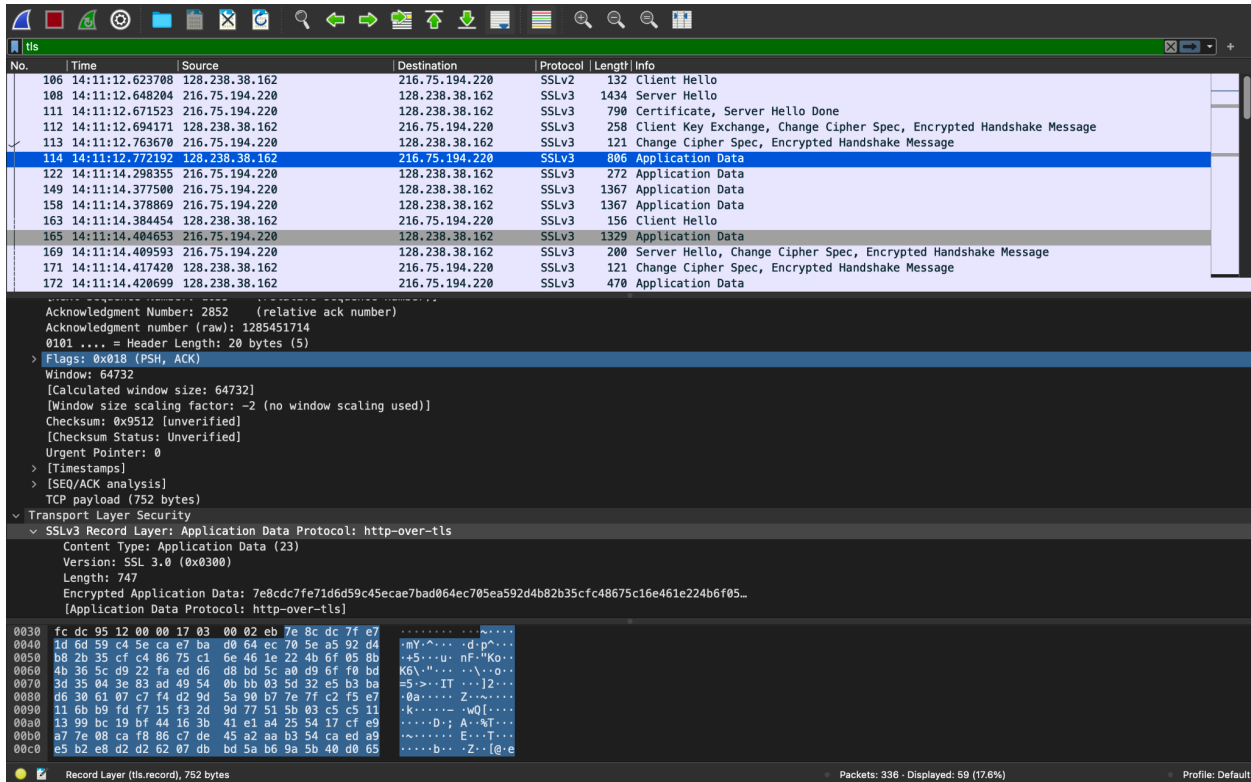
12). MAC address of all the previous handshake are encrypted, and sent from client to server

13). Yes

The difference is that the sender is server and previous the client was sender

## Foundation of Computer Networks - Wireshark Project

### Bhavin Oza (bo2115)



14).

Application data is being encrypted using one of the cipher suite algorithms chosen in the handshake phase.

Yes it includes MAC.

Yes, the wireshark distinguishes between encrypted application data and the MAC

15). The first client hello message is sent by SSLv2 and the others are sent by SSLv3.

The certificate is sent only in the first handshake process, after the first handshake client sends only a nonce.

The server sends the encrypted handshake and change cipher spec record to the client.