

# **CNS Assignment**

## **SSL Wireshark Assignment**

**Harsh Agarwal**  
**CS15BTECH11019**

1)

- a) Frame 1
  - Source : client (192.168.117.63)
  - No of SSL records : 1
  - SSL Type : Handshake(22) Client Hello
- b) Frame 2
  - Source : server(216.58.196.36)
  - No of SSL records : 1
  - SSL Type : Handshake(22) Server Hello
- c) Frame 3
  - Source : server(216.58.196.36)
  - No of SSL records : 3
  - SSL Type : Handshake(22) Certificate, Handshake(22) Server Key Exchange, Handshake(22) Server Hello Done
- d) Frame 4
  - Source : client (192.168.117.63)
  - No of SSL records : 1
  - SSL Type : Handshake(22) Client Hello
- e) Frame 5
  - Source : server(216.58.196.36)
  - No of SSL records : 1
  - SSL Type : Handshake(22) Server Hello
- f) Frame 6
  - Source : server(216.58.196.36)
  - No of SSL records : 3
  - SSL Type : Handshake(22) Certificate, Handshake(22) Server Key Exchange, Handshake(22) Server Hello Done
- g) Frame 7
  - Source : client(192.168.117.63)
  - No of SSL records : 3
  - SSL Type : Handshake(22) Client Key Exchange, Change Cipher Spec(20), Handshake(22) Encrypted Handshake Message
- h) Frame 8
  - Source : server(216.58.196.36)
  - No of SSL records : 3

## SSL Type : Handshake(22) New Session Ticket, Change Cipher Spec(20), Handshake(22) Encrypted Handshake Message

### Timing Diagram

Client                      Server

```

→Client Hello→
←Server Hello←
←Certificate←
←Server Key Exchange←
←Server Hello Done←
→Client Hello→
←Server Hello←
←Certificate←
←Server Key Exchange←
←Server Hello Done←
→Client Key Exchange→
→Change Cipher Spec→
→Encrypted Handshake Message→
←New Session Ticket←
←Change Cipher Spec←
←Encrypted Handshake Message←
  
```

No.	Time	Source	Destination	Protocol	Length	Info
210	10.191680	192.168.117.63	216.58.196.36	TLSv1.2	257	Client Hello
220	10.344479	216.58.196.36	192.168.117.63	TLSv1.2	1434	Server Hello
224	10.344618	216.58.196.36	192.168.117.63	TLSv1.2	482	Certificate, Server Key Exchange, Server Hello Done
234	10.498240	192.168.117.63	216.58.196.36	TLSv1.2	257	Client Hello
236	10.565193	216.58.196.36	192.168.117.63	TLSv1.2	1434	Server Hello
240	10.565343	216.58.196.36	192.168.117.63	TLSv1.2	482	Certificate, Server Key Exchange, Server Hello Done
242	10.575245	192.168.117.63	216.58.196.36	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake M...
256	10.635163	216.58.196.36	192.168.117.63	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Handshake Me...
259	10.649530	192.168.117.63	216.58.196.36	TLSv1.2	243	Application Data
260	10.649601	192.168.117.63	216.58.196.36	TLSv1.2	904	Application Data
269	10.894751	216.58.196.36	192.168.117.63	TLSv1.2	296	[TCP Spurious Retransmission], Encrypted Handshake Message, C...
273	11.119687	216.58.196.36	192.168.117.63	TLSv1.2	135	Application Data
275	11.119842	216.58.196.36	192.168.117.63	TLSv1.2	104	Application Data
277	11.119972	192.168.117.63	216.58.196.36	TLSv1.2	104	Application Data
279	11.144938	216.58.196.36	192.168.117.63	TLSv1.2	535	Application Data
280	11.144985	216.58.196.36	192.168.117.63	TLSv1.2	214	Application Data, Application Data
281	11.145011	216.58.196.36	192.168.117.63	TLSv1.2	112	Application Data
283	11.145982	192.168.117.63	216.58.196.36	TLSv1.2	112	Application Data
290	11.500973	192.168.117.63	54.191.90.208	TLSv1.2	997	[TCP Previous segment not captured], Application Data
295	11.641675	192.168.117.63	103.68.220.61	TLSv1.2	260	Client Hello
297	11.675280	103.68.220.61	192.168.117.63	TLSv1.2	1434	Server Hello
301	11.675480	103.68.220.61	192.168.117.63	TLSv1.2	1049	Certificate, Server Key Exchange, Server Hello Done
303	11.678624	192.168.117.63	103.68.220.61	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake M...
308	11.699362	192.168.117.63	103.68.220.61	TLSv1.2	585	Application Data

Frame 210: 257 bytes on wire (2056 bits), 257 bytes captured (2056 bits) on interface 0  
 Ethernet II, Src: Dell 7d:fc:24 (34:e6:d7:7d:fc:24), Dst: HewlettP a9:8b:f8 (5c:8a:38:a9:8b:f8)  
 Internet Protocol Version 4, Src: 192.168.117.63, Dst: 216.58.196.36  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 243  
 Identification: 0x9f3b (40763)  
 Flags: 0x02 (Don't Fragment)  
 Fragment offset: 0  
 Time to live: 64  
 Protocol: TCP (6)  
 Header checksum: 0xc882 [validation disabled]  
 [Header checksum status: Unverified]

0000 5c 8a 38 a9 8b f8 34 e6 d7 7d fc 24 08 00 45 00 \.8...4. .).\$.E.

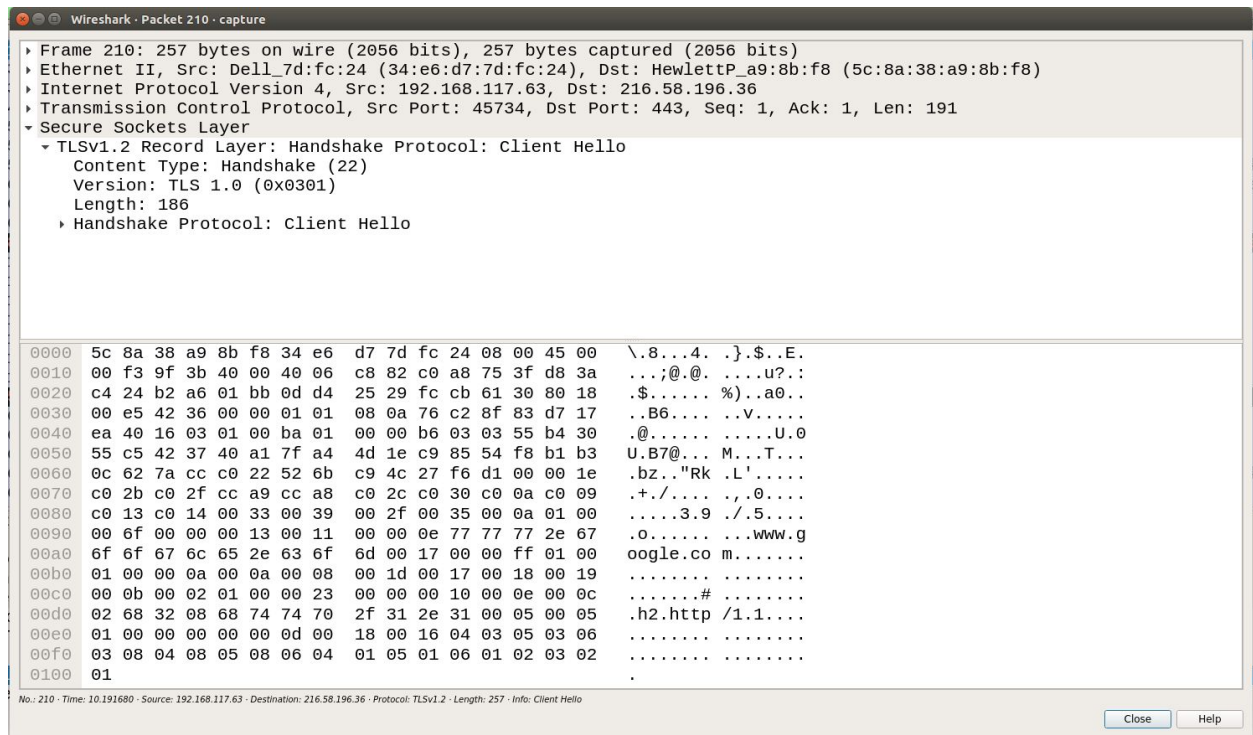
2)

Content Type :: 1 bytes

Version :: 2 bytes

Length :: 2 bytes

### 3) Client Hello's Content Type is Handshake(22)



### 4)

In packet noonce is shown by Random field which contains GMT Unix Time and Random Bytes

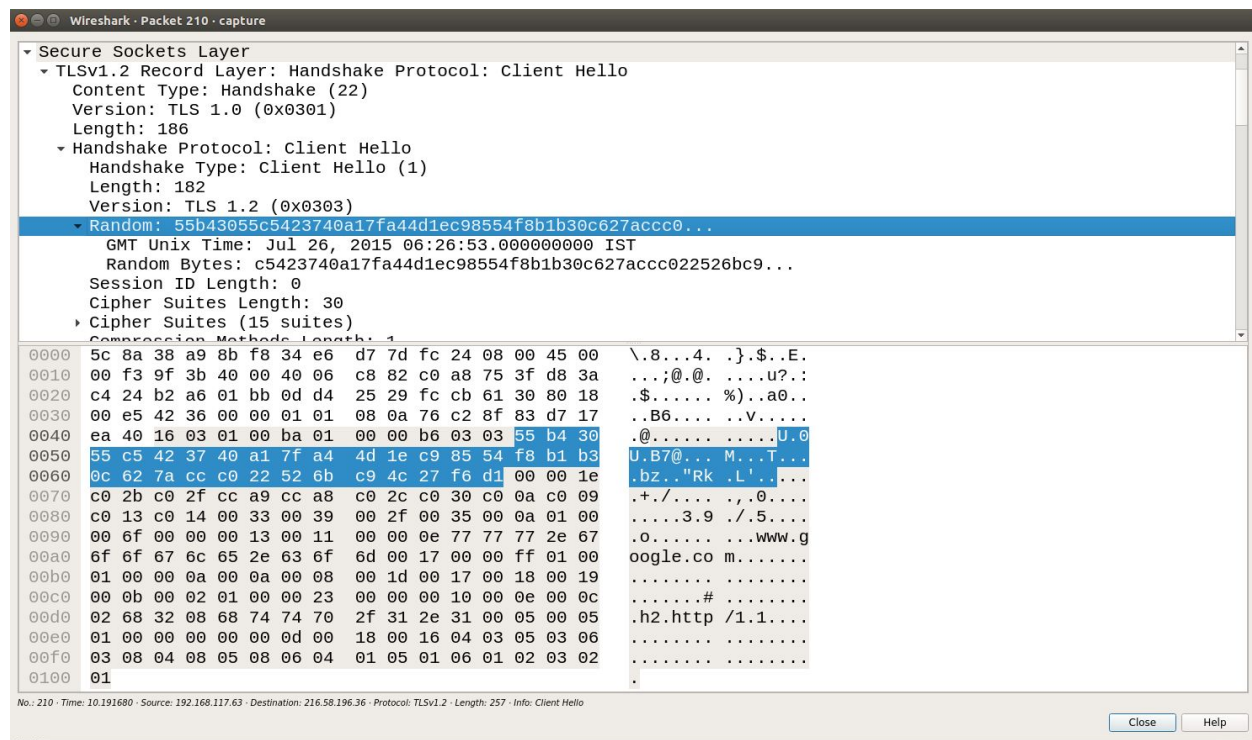
Complete Random Field :: 55 b4 30 55 c5 42 37 40 a1 7f a4 4d 1e c9 85 54

0010 f8 b1 b3 0c 62 7a cc c0 22 52 6b c9 4c 27 f6 d1

GMT Unix Time :: 55 b4 30 55

Random Bytes :: c5 42 37 40 a1 7f a4 4d 1e c9 85 54

0010 f8 b1 b3 0c 62 7a cc c0 22 52 6b c9 4c 27 f6 d1



5)

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02b)  
Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)  
Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xcca9)  
Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xcca8)  
Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc02c)  
Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc030)  
Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA (0xc00a)  
Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA (0xc009)  
Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xc013)  
Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xc014)  
Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x0033)  
Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0039)  
Cipher Suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x002f)  
Cipher Suite: TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035)  
Cipher Suite: TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (0x000a)  
Public-Key algorithm :: RSA, ECDSA(Elliptic Curve Digital Signature Algorithm)  
Symmetric-Key Algorithm :: AES\_128\_GCM, CHACHA20\_POLY1305  
Hash Algorithm :: SHA256, SHA384, SHA

210.10.191680	192.168.117.63	216.58.196.36	TLSv1.2	257 Client Hello
220.10.344470	216.58.196.36	192.168.117.63	TLSv1.2	1434 Server Hello
224.10.344618	216.58.196.36	192.168.117.63	TLSv1.2	482 Certificate, Server Key Exchange, Server Hello Done
234.10.408240	192.168.117.63	216.58.196.36	TLSv1.2	257 Client Hello

```

Version: TLS 1.0 (0x0301)
Length: 186
  Handshake Protocol: Client Hello
  Handshake Type: Client Hello (1)
  Length: 182
  Version: TLS 1.2 (0x0303)
  Random: 55b49b55c5423740a17fa44d1ec98554f8b1b30c627acc0...
  GMT Unix Time: Jul 26, 2015 06:26:53.000000000 IST
  Random Bytes: c5423740a17fa44d1ec98554f8b1b30c627acc022526bc9...
  Session ID Length: 0
  Cipher Suites Length: 30
  Cipher Suites (45 suites)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
    Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
    Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
    Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
    Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
    Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
    Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
  Compression Methods Length: 1

```

## 6) Chosen cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256

TLS - the protocol used

ECDHE - the key exchange mechanism - elliptic curve diffie-hellman key exchange

ECDSA - the algorithm of the authentication key - Elliptic Curve Digital Signature Algorithm

AES - the symmetric encryption algorithm - Advanced Encryption Standard

128 - the key size of the above

GCM - the mode of the above - Galois/Counter Mode (GCM)

SHA256 - the MAC used by the algorithm - Secure Hash Algorithm-256

Length: 68
Version: TLS 1.2 (0x0303)
Random: 5acfa9df875d5e29960a54726d7b781ffa37face4e21e4fe...
GMT Unix Time: Apr 13, 2018 00:17:59.000000000 IST
Random Bytes: 875d5e29960a54726d7b781ffa37face4e21e4fe36d09754...
Session ID Length: 0
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Compression Method: null (0)
Extensions Length: 28
Extension: renegotiation_info (len=1)
Type: renegotiation_info (65281)

## 7) Yes nonce is there - 32 bytes

Purpose :: A *nonce* is a unique value chosen by an entity in a protocol, and it is used to protect that entity against replay attacks. It is often a random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks.

## 8) No there is no session ID

Purpose :: A session ID is a unique number that a Web site's server assigns a specific user for the duration of that user's visit (session). The session ID can be stored as a cookie, form field, or URL. As session IDs are often used to identify a user that has logged into a website.

## 9) Certificate is in a different record. Yes certificate fits into a single frame.



```

220 10 3444f9 210 08 190 36 192 188 117 83 TLSv1.2 1434 Server Hello
224 10 344618 216 58 196 36 192 168 117 83 TLSv1.2 482 Certificate, Server Hello Done
234 10 2a892a 192 168 117 83 216 68 106 36 TLSv1.2 257 Client Hello
+ TLSv1.2 Record Layer: Handshake Protocol: Certificate
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 2948
+ Handshake Protocol: Certificate
  Handshake Type: Certificate (11)
  Length: 2936
  Certificates Length: 2933
+ Certificates (2933 bytes)
  Certificate Length: 959
+ Certificate: 30820428308292a2a0830820102020815faa276d9d7fd7630... (id-at-commonName=www.google.com,id-at-organizationName=Google Inc,id-at-localityName=Mountain View,id-at-countryName=US)
+ Certificate: 30820428308292a2a083082010202100100212588bfa59a7... (id-at-commonName=Google Internet Authority G2,id-at-organizationName=Google Inc,id-at-countryName=US)
+ Certificate: 3082037d508202e6a0830820102020312b6b300d6692a86... (id-at-commonName=GeoTrust Global CA,id-at-organizationName=GeoTrust Inc.,id-at-countryName=US)
+ Secure Sockets Layer
+ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 116
+ Handshake Protocol: Server Key Exchange
  Handshake Type: Server Key Exchange (12)
  Length: 112
+ EC Diffie-Hellman Server Params
+ TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 4
+ Handshake Protocol: Server Hello Done

```

X.509 certificate ::

MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIlb3DQEBBQUAME4xCzAJBgNVBAYTAIVT  
MRAwDgYDVQQKEwdFcXVpZmF4MS0wKwYDVQQLExRfCvXpZmF4IFNlYy3VyZSBDZXJ0  
aWZpY2F0ZSBDbXRob3JpdHkwHhcNMDIwNTIxMDQwMDAwWHcNMTgwODIxMDQwMDAw  
WjBCMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNMR2VvVHJ1c3QgSW5jLjEjbMBkGA1UE  
AxMSR2VvVHJ1c3QgR2xvYmFsIENBMIIBlJANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB  
CgKCAQEA2swYYzD99BcjGIZ+W988bdDjkcbd4kdS8odhM+KhDtgpPtTSEHCljaWC9m  
OSm9BXilnTjoBbdqfnGk5sRgprDvgOSJKA+eJdbtg/OtpHHmMICGDUUna2YRplu  
T8rxh0PBFpVXLVDviS2Aelet8u5fa9IAjbkU+BQVNdnARqN7csiRv8IVK83Qlz6c  
JmTM386DGXHKTubU1XupGc1V3sjs0l44U+VcT4wt/IAjNvxm5suOpDkZALeVAjmR  
Cw7+OC7RHQWa9k0+bw8HHA8sHo9gOeL6NIMTOdReJivbPagUvTLrGAMoUgRx5asz  
PeE4uwc2hGKceeoWMPRfwCvocWvk+QIDAQABo4HwMIHtMB8GA1UdIwQYMBaAFEjm  
aPr0rKV10fylyAQTZoyKJ/UMB0GA1UdDgQWBBAephohYn7qwVkDBF9qn1luMrM  
TjAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjA6BgNVHR8EMzAxMC+g  
LaArhilodHRwOi8vY3JsLmdlb3RydXN0LmNvbS9jcmxzL3NIY3VyZWZhbmNyYDBO  
BgNVHSAERzBFMEMGBFUdIAAwOza5BggrBgEFBQCcARYtaHR0cHM6Ly93d3cuZ2Vv  
dHJ1c3QuY29tL3Jlc291cmNlcy9yZXBvc2l0b3J5MA0GCSqGSIlb3DQEBBQUAA4GB  
AHbhEm5OSxYShjAGsoElz/Alx8dxmfmbuwu3UOX//8PDITtZDOLC5MH0Y0FWDomrL  
NhGc6Ehmo21/uBPUR/6LWLxz/K7ZGzlZOKuXNBsqItLroxwUCEm2u+WR74M26x1W  
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S

-----END CERTIFICATE-----

a) Public key length :: 2048 bits

b) Public key encryption algorithm :: rsaEncryption

c) Signature Algorithm :: sha1WithRSAEncryption

d) SignatureValue ::

AHbhEm5OSxYShjAGsoElz/Alx8dxmbuwu3UOx//8PDITtZDOLC5MH0Y0FWDomrLNhGc6Eh  
mo21/uBPUR/6LWlxz/K7ZGzIZOKuXNBSqItLroxwUCEm2u+WR74M26x1Wb8ravHNjkOR/ez4iy  
z0H7V84dJzjA1BOoa+Y7mHyhD8S

e) Certificate issuer ::

Issuer: C=US, O=Equifax, OU=Equifax Secure Certificate Authority

f) Common name and Alternative name (if any) ::

DNS Name: [www.onlinesbi.com](http://www.onlinesbi.com)

g) Key usage and purpose of the certificate ::

Critical

Certificate Sign, CRL Sign

10)

It is used to provide greater consistency between TLS cipher suites. This and 2 nonces above are used to generate the master key.

This uses Diffie Hellman Key exchange.

Length : 32 bit

Key shared by client to server :: Pubkey:

27:ac:1b:61:0c:e1:3e:15:47:4f:67:a2:e7:8c:62:11:2c:37:1c:90:83:57:5a:9d:0d:07:82:0f:7b:6f:43:3  
e

Actually, this is part of the DH exchange. This will go to server and finally both client and server will have same key . This key is the pre-master secret. It is not explicitly mentioned in the packet but calculated on both hosts.

11) The change cipher spec protocol is used to change the encryption being used by the client and server. It is used as part of the handshake process to switch to symmetric key encryption.

Length :: 6 bytes

12) A finished message is being encrypted using the symmetric keys negotiated earlier. This includes a sender code. If this message can be decrypted properly, then we are good to go and can start encrypting traffic

13) Yes.

Server has different sender code which is hashed to become the message payload . This is different from client finished message as client will send his own code.

14)

Message is encrypted using agreed symmetric keys & algorithms.

Yes a MAC is there with each record for every application data message.

No, Wireshark doesn't distinguish.

15)

The thing I found on this wireshark Lab is different SSL Record types, the different encryption and decryption, algorithms, new session ticket , how application data is encrypted , how SSL closes the connection.

16)

No.	Time	Source	Destination	Protocol	Length	Info
214	10.275593	192.168.117.63	216.58.196.36	TCP	257	[TCP Out-Of-Order] 45734 → 443 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=191 TSval=1992462...
215	10.288266	192.168.117.63	216.58.196.36	TCP	74	45736 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1992462388 TSecr=0...
219	10.335721	216.58.196.36	192.168.117.63	TCP	66	443 → 45734 [ACK] Seq=1 Ack=193 Win=43520 Len=0 TSval=3608668879 TSecr=1992462295
220	10.344479	216.58.196.36	192.168.117.63	TLSv1.2	1424	Server Hello
221	10.344524	192.168.117.63	216.58.196.36	TCP	54	45734 → 443 [RST] Seq=193 Win=0 Len=0
222	10.344566	216.58.196.36	192.168.117.63	TCP	1434	443 → 45734 [ACK] Seq=1369 Ack=193 Win=43520 Len=1368 TSval=3608668889 TSecr=19924622...
223	10.344604	192.168.117.63	216.58.196.36	TCP	54	45734 → 443 [RST] Seq=193 Win=0 Len=0
224	10.344618	216.58.196.36	192.168.117.63	TLSv1.2	482	Certificate, Server Key Exchange, Server Hello Done
225	10.344629	192.168.117.63	216.58.196.36	TCP	54	45734 → 443 [RST] Seq=193 Win=0 Len=0
226	10.344633	216.58.196.36	192.168.117.63	TCP	66	443 → 45734 [FIN, ACK] Seq=3153 Ack=193 Win=43520 Len=0 TSval=3608668889 TSecr=199246...
227	10.344646	192.168.117.63	216.58.196.36	TCP	54	45734 → 443 [RST] Seq=193 Win=0 Len=0
228	10.345041	216.58.196.36	192.168.117.63	TCP	74	443 → 45736 [SYN, ACK] Seq=0 Ack=1 Win=42408 Len=0 MSS=1380 SACK_PERM=1 TSval=3382536...
229	10.345065	192.168.117.63	216.58.196.36	TCP	54	45736 → 443 [RST] Seq=1 Win=0 Len=0
231	10.430497	192.168.117.63	216.58.196.36	TCP	74	45736 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1992462450 TSecr=0...
232	10.497891	216.58.196.36	192.168.117.63	TCP	74	443 → 45738 [SYN, ACK] Seq=0 Ack=1 Win=42408 Len=0 MSS=1380 SACK_PERM=1 TSval=2777188...
233	10.497952	192.168.117.63	216.58.196.36	TCP	66	45738 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1992462517 TSecr=2777180436
234	10.498240	192.168.117.63	216.58.196.36	TLSv1.2	257	Client Hello
235	10.557811	216.58.196.36	192.168.117.63	TCP	66	443 → 45738 [ACK] Seq=1 Ack=192 Win=43520 Len=0 TSval=2777180495 TSecr=1992462518
236	10.565193	216.58.196.36	192.168.117.63	TLSv1.2	1424	Server Hello
237	10.565268	192.168.117.63	216.58.196.36	TCP	66	45738 → 443 [ACK] Seq=192 Ack=1369 Win=32128 Len=0 TSval=1992462585 TSecr=2777180502
238	10.565298	216.58.196.36	192.168.117.63	TCP	1434	443 → 45738 [ACK] Seq=1369 Ack=192 Win=43520 Len=1368 TSval=2777180502 TSecr=19924625...
239	10.565328	192.168.117.63	216.58.196.36	TCP	66	45738 → 443 [ACK] Seq=192 Ack=2737 Win=35072 Len=0 TSval=1992462585 TSecr=2777180502
240	10.565343	216.58.196.36	192.168.117.63	TLSv1.2	482	Certificate, Server Key Exchange, Server Hello Done
241	10.565305	192.168.117.63	216.58.196.36	TCP	66	45738 → 443 [ACK] Seq=192 Ack=3153 Win=37760 Len=0 TSval=1992462585 TSecr=2777180502
242	10.575245	192.168.117.63	216.58.196.36	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
243	10.635163	216.58.196.36	192.168.117.63	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
244	10.649530	192.168.117.63	216.58.196.36	TLSv1.2	243	Application Data
245	10.649661	192.168.117.63	216.58.196.36	TLSv1.2	904	Application Data
246	10.674503	192.168.117.63	216.58.196.36	TCP	904	[TCP Retransmission] 45738 → 443 [PSH, ACK] Seq=462 Ack=3383 Win=40576 Len=838 TSval=...
249	10.894751	192.168.117.63	216.58.196.36	TCP	296	[TCP Spurious Retransmission] , Encrypted Handshake Message, Change Cipher Spec, Encr...
270	10.894821	192.168.117.63	216.58.196.36	TCP	78	[TCP Dup ACK 259#1] 45738 → 443 [ACK] Seq=1300 Ack=3383 Win=40576 Len=0 TSval=1992462...
272	11.059585	192.168.117.63	216.58.196.36	TCP	1081	[TCP Retransmission] 45738 → 443 [PSH, ACK] Seq=285 Ack=3383 Win=40576 Len=1015 TSval=...
273	11.119687	216.58.196.36	192.168.117.63	TLSv1.2	135	Application Data
274	11.119709	192.168.117.63	216.58.196.36	TCP	66	45738 → 443 [ACK] Seq=1300 Ack=3452 Win=40576 Len=0 TSval=1992463139 TSecr=2777180957
275	11.119842	216.58.196.36	192.168.117.63	TLSv1.2	104	Application Data
276	11.119877	192.168.117.63	216.58.196.36	TCP	66	45738 → 443 [ACK] Seq=1300 Ack=3490 Win=40576 Len=0 TSval=1992463139 TSecr=2777180957
277	11.119972	192.168.117.63	216.58.196.36	TLSv1.2	104	Application Data
279	11.144938	216.58.196.36	192.168.117.63	TLSv1.2	535	Application Data
280	11.144985	216.58.196.36	192.168.117.63	TLSv1.2	214	Application Data, Application Data
281	11.145011	216.58.196.36	192.168.117.63	TLSv1.2	112	Application Data
282	11.145883	192.168.117.63	216.58.196.36	TCP	66	45738 → 443 [ACK] Seq=1338 Ack=4153 Win=45952 Len=0 TSval=1992463164 TSecr=27771809082
283	11.145982	192.168.117.63	216.58.196.36	TLSv1.2	112	Application Data
285	11.285518	216.58.196.36	192.168.117.63	TCP	66	443 → 45738 [ACK] Seq=4153 Ack=1384 Win=45568 Len=0 TSval=27771809143 TSecr=1992463139

Ethernet II, Src: Dell17d:fc:24 (34:b6:d7:7d:fc:24), Dst: HewlettP\_a9:8b:f8 (5c:8a:38:a9:8b:f8)  
Internet Protocol Version 4, Src: 192.168.117.63, Dst: 216.58.196.36  
Transmission Control Protocol, Src Port: 45734, Dst Port: 443, Seq: 1, Ack: 1, Len: 191

0000 5c 8a 38 a9 8b f8 34 e6 d7 7d fc 24 08 00 45 00 \. . . . 4 . . . \$. . E .

capture Packets: 2345 · Displayed: 49 (2.1%) · Load time: 0.0/78 Profile: Default

Total 49 packets are exchanged in the entire session (displayed at bottom)

Duration of HTTPS session :: 0.929925 sec

17)

Using nonces and pre\_master , master\_secret is found using PRF (pseudo-random function).

Pseudo Code :

master\_secret = PRF(pre\_master\_secret, "master secret", ClientHello.random + ServerHello.random)

PRF(secret, label, seed) = P\_<hash>(secret, label + seed)



$$P\_hash(secret, seed) = HMAC\_hash(secret, A(1) + seed) +$$

$$HMAC\_hash(secret, A(2) + seed) +$$

$$HMAC\_hash(secret, A(3) + seed) +$$

$$A(0) = seed$$

$$A(i) = HMAC\_hash(secret, A(i-1))$$

Algorithm :: label + client-nonce+ server-noonce is calculated and treated as seed. Then secret and seed is hashed sequentially until 48 bytes string is obtained. This is the master key. From the master key the following are derived

- client\_write\_MAC\_key
- server\_write\_MAC\_key
- client\_write\_key
- Server\_write\_key

The master\_secret is found using PRF- the same way as premaster\_key. This is repeated until sufficient length is obtained to get the 4 diff keys

```
key_block = PRF(SecurityParameters.master_secret,
    "key expansion",
    SecurityParameters.server_random +
    SecurityParameters.client_random);
```

The browser does these things for us.