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)

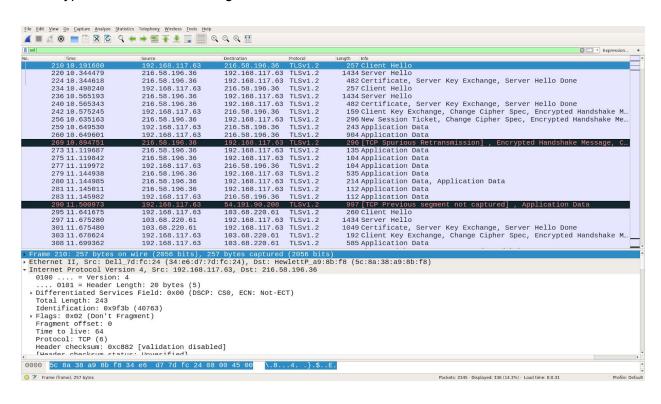
No of SSL records: 3

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←



Version :: 2 bytes Length :: 2 bytes

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

```
😣 🖨 🗈 Wireshark • Packet 210 • capture

    Frame 210: 257 bytes on wire (2056 bits), 257 bytes captured (2056 bits)
    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

 > Transmission Control Protocol, Src Port: 45734, Dst Port: 443, Seq: 1, Ack: 1, Len: 191
 → Secure Sockets Layer
   * TLSv1.2 Record Layer: Handshake Protocol: Client Hello
       Content Type: Handshake (22)
       Version: TLS 1.0 (0x0301)
       Length: 186
     Handshake Protocol: Client Hello
                                      d7 7d fc 24 08 00 45 00
                                                                     \.8...4. .}.$..E.
        5c 8a 38 a9 8b f8 34 e6
                                      c8 82 c0 a8 75 3f d8 3a
25 29 fc cb 61 30 80 18
                                                                    ...;@.@. ....u?.:
.$..... %)..ao..
  0010 00 f3 9f 3b 40 00 40 06
  0020 c4 24 b2 a6 01 bb 0d d4
                                                                     ..B6.... ..v....
  0030 00 e5 42 36 00 00 01 01
                                      08 0a 76 c2 8f 83 d7 17
  0040 ea 40 16 03 01 00 ba 01
                                      00 00 b6 03 03 55 b4 30
                                                                     .@.....U.0
                                                                    U.B7@... M...T...
.bz.."Rk .L'....
  0050
        55 c5 42 37 40 a1 7f a4
                                      4d 1e c9 85 54 f8 b1 b3
  0060 0c 62 7a cc c0 22 52 6b
                                      c9 4c 27 f6 d1 00 00 1e
                                                                     .+./.... .,.0....
....3.9 ./.5....
  0070 c0 2b c0 2f cc a9 cc a8
                                      c0 2c c0 30 c0 0a c0 09
  9989 c0 13 c0 14 99 33 99 39
                                      00 2f 00 35 00 0a 01 00
  0090 00 6f 00 00 00 13 00 11
                                      00 00 0e 77 77 77 2e 67
                                                                     .o..... ...www.g
                                                                    oogle.co m.....
  00a0 6f 6f 67 6c 65 2e 63 6f
                                      6d 00 17 00 00 ff 01 00
  00b0 01 00 00 0a 00 0a 00 08
                                      00 1d 00 17 00 18 00 19
                                                                    00 0b 00 02 01 00 00 23
                                      00 00 00 10 00 0e 00 0c
  00d0 02 68 32 08 68 74 74 70
                                     2f 31 2e 31 00 05 00 05
                                                                     .h2.http /1.1....
  00e0 01 00 00 00 00 00 0d 00
                                     18 00 16 04 03 05 03 06
  00f0 03 08 04 08 05 08 06 04 01 05 01 06 01 02 03 02
                                                                     0100 01
 No.: 210 · Time: 10.191680 · Source: 192.168.117.63 · Destination: 216.58.196.36 · Protocol: TLSv1.2 · Length: 257 · Info: Client Helio
                                                                                                                          Close Help
```

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

```
Secure Sockets Laver
 TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 186
   - Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
       Length: 182
      Version: TLS 1.2 (0x0303)
        GMT Unix Time: Jul 26, 2015 06:26:53.000000000 IST
        Random Bytes: c5423740a17fa44d1ec98554f8b1b30c627accc022526bc9...
      Session TD Length: 0
      Cipher Suites Length:
     → Cipher Suites (15 suites)
      5c 8a 38 a9 8b f8 34 e6 d
                                  d7 7d fc 24 08 00 45 00
                                                                \.8...4. .}.$..E.
                                  c8 82 c0 a8 75 3f d8 3a
                                                                ...;@.@. ...u?.:
.$..... %)..ao..
0010 00 f3 9f 3b 40 00 40 06
0020 c4 24 b2 a6 01 bb 0d d4
                                  25 29 fc cb 61 30 80 18
0030 00 e5 42 36 00 00 01 01
                                  08 0a 76 c2 8f 83 d7 17
                                                                ..B6.... ..v....
      ea 40 16 03 01 00 ba 01
                                  00 00 b6 03 03 55
                                                                .@....<mark>.. .....</mark>U.
                    40 a1
                                  c9 4c 27 f6 d1 00 00 1e
0060
                                                                          .,.0...
      c0 2b c0 2f cc a9 cc a8
                                  c0 2c c0 30 c0 0a c0 09
0080
      c0 13 c0 14 00 33 00 39
                                  00 2f 00 35 00 0a 01 00
                                                                .....3.9 ./.5...
      00 6f 00 00 00 13 00 11
                                  00 00 0e 77 77 77 2e 67
                                                                .o..... ...www.g
      6f 6f 67 6c 65 2e 63 6f
                                  6d 00 17 00 00 ff 01 00
00a0
                                                                oogle.co m.....
      01 00 00 0a 00 0a 00 08
                                  00 1d 00 17 00 18 00 19
                                                                . . . . . . . . . . . . . . . . . .
      00 0b 00 02 01 00 00 23
                                  00 00 00 10 00 0e 00 0c
      02 68 32 08 68 74 74 70
                                  2f 31 2e 31 00 05 00 05
                                                                .h2.http /1.1....
      01 00 00 00 00 00 0d 00
                                  18 00 16 04 03 05 03 06
00e0
                                                                . . . . . . . . . . . . . . . . . . .
00f0 03 08 04 08 05 08 06 04
                                  01 05 01 06 01 02 03 02
                                                                . . . . . . . . . . . . . . . . . . .
0100 01
lo.: 210 · Time: 10.191680 · Source: 192.168.117.63 · Destination: 216.58.196.36 · Protocol: TLSv1.2 · Length: 257 · Info: Client Hell
                                                                                                                   Close
```

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

```
229 19.191680 192.468.117.63 216.58.196.36 192.168.117.63 11.591.2 1434 Server Hello
224 19.344618 216.58.196.36 192.168.117.63 11.591.2 482 Certificate, Server Key Exchange, Server Hello Done
234 19.344618 216.58.196.36 192.168.117.63 11.591.2 482 Certificate, Server Key Exchange, Server Hello Done
241 19.344618 216.58.196.36 192.168.117.63 11.591.2 257.01ent Hello
Length: 186

+ Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 182
Version: TLS 1.2 (0x0383)

* Random: S5b43055C5423740a17fa44diec98554f8b1b30c627accc0...
GMT Unix Time: Jul 26, 2015 06:26:53.000000000 IST
Random Sytes: C5423740a17fa44diec98554f8b1b30c627accc022526b9...
Session ID Length: 0

* Clipher Sultes Length: 30

* Clipher Sultes Length: 30

* Clipher Sulte: TLS ECOHE ECOSA WITH AES 128 GCM SHA256 (0x028)
Clipher Sulte: TLS ECOHE ECOSA WITH CHACHA29 Poly130S SHA256 (0x028)
Clipher Sulte: TLS ECOHE ECOSA WITH CHACHA29 Poly130S SHA256 (0x028)
Clipher Sulte: TLS ECOHE ECOSA WITH AES 256 GCM SHA286 (0x028)
Clipher Sulte: TLS ECOHE ECOSA WITH AES 256 GCM SHA284 (0x028)
Clipher Sulte: TLS ECOHE ECOSA WITH AES 256 GCM SHA284 (0x028)
Clipher Sulte: TLS ECOHE ECOSA WITH AES 256 GCM SHA284 (0x028)
Clipher Sulte: TLS ECOHE ECOSA WITH AES 128 GCC SHA (0x0000)
Clipher Sulte: TLS ECOHE ECOSA WITH AES 128 GCC SHA (0x0000)
Clipher Sulte: TLS ECOHE ECOSA WITH AES 128 GCC SHA (0x0000)
Clipher Sulte: TLS ECOHE ECOSA WITH AES 128 GCC SHA (0x0001)
Clipher Sulte: TLS ECOHE ECOSA WITH AES 128 GCC SHA (0x0001)
Clipher Sulte: TLS ECOHE ECOSA WITH AES 128 GCC SHA (0x0001)
Clipher Sulte: TLS ECOHE ECOSA WITH AES 128 GCC SHA (0x0001)
Clipher Sulte: TLS ECOHE ECOSA WITH AES 128 GCC SHA (0x0001)
Clipher Sulte: TLS ECOHE ECOSA WITH AES 128 GCC SHA (0x0001)
Clipher Sulte: TLS ECOHE ECOSA WITH AES 128 GCC SHA (0x0001)
Clipher Sulte: TLS ECOHE ECOSA WITH AES 128 GCC SHA (0x0001)
Clipher Sulte: TLS ECOHE ECOSA WITH AES 128 GCC SHA (0x0001)
Clipher Sulte: TLS ECOHE ECOSA WITH AES 128 GCC SHA (0x0001)
Clipher Sulte: TLS ECOHE ECOSA WITH AES 128 GCC SHA
```

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 (0x0363)

Random: Sacfaodf075d5c29960a54726d7b781ffa37facc4e21e4fe...

GMT Unix Time: Apr 13, 2018 06:17:59.000000000 IST

Random Bytes: 875d5c29960a54726d7b781ffa37facc4e21e4fe36d09754...
Session ID Length: 0

Cipher Suite: TLS_ECOHE_ECOSA_WITH_AES_128_GCM_SHA256 (0xc602b)

Compression Method: null (0)

Extensions Length: 28

Extension: renegotiation_info (len=1)

Type: renegotiation_info (65281)
```

7) Yes noonce 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.

Infact 3 SSL records are in the frame along with certificate



10)

X.509 certificate ::

----BEGIN CERTIFICATE-----

MIIDfTCCAuaqAwIBAqIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBqNVBAYTAIVT MRAwDgYDVQQKEwdFcXVpZmF4MS0wKwYDVQQLEyRFcXVpZmF4IFNIY3VyZSBDZXJ0 aWZpY2F0ZSBBdXRob3JpdHkwHhcNMDIwNTIxMDQwMDAwWhcNMTgwODIxMDQwMDAw WjBCMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNR2VvVHJ1c3QqSW5jLjEbMBkGA1UE AxMSR2VvVHJ1c3QqR2xvYmFsIENBMIIBIjANBqkqhkiG9w0BAQEFAAOCAQ8AMIIB CgKCAQEA2swYYzD99BcjGlZ+W988bDjkcbd4kdS8odhM+KhDtgPpTSEHCljaWC9m OSm9BXiLnTjoBbdgfnGk5sRgprDvgOSJKA+eJdbtg/OtppHHmMlCGDUUna2YRplu T8rxh0PBFpVXLVDviS2Aelet8u5fa9IAjbkU+BQVNdnARqN7csiRv8IVK83QIz6c JmTM386DGXHKTubU1XupGc1V3sjs0I44U+VcT4wt/IAjNvxm5suOpDkZALeVAjmR Cw7+OC7RHQWa9k0+bw8HHa8sHo9gOeL6NIMTOdReJivbPagUvTLrGAMoUgRx5asz PeE4uwc2hGKceeoWMPRfwCvocWvk+QIDAQABo4HwMIHtMB8GA1UdlwQYMBaAFEjm aPkr0rKV10fYlyAQTzOYkJ/UMB0GA1UdDqQWBBTAephojYn7gwVkDBF9gn1luMrM TjAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjA6BgNVHR8EMzAxMC+g LaArhilodHRwOi8vY3JsLmdlb3RydXN0LmNvbS9jcmxzL3NlY3VyZWNhLmNybDBO BgNVHSAERzBFMEMGBFUdIAAwOzA5BggrBgEFBQcCARYtaHR0cHM6Ly93d3cuZ2Vv dHJ1c3QuY29tL3Jlc291cmNlcy9yZXBvc2l0b3J5MA0GCSqGSlb3DQEBBQUAA4GB AHbhEm5OSxYShjAGsoElz/Alx8dxfmbuwu3UOx//8PDITtZDOLC5MH0Y0FWDomrL NhGc6Ehmo21/uBPUR/6LWlxz/K7ZGzIZOKuXNBSqltLroxwUCEm2u+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/Alx8dxfmbuwu3UOx//8PDITtZDOLC5MH0Y0FWDomrLNhGc6Eh mo21/uBPUR/6LWlxz/K7ZGzlZOKuXNBSqltLroxwUCEm2u+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

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 noonces 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

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 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)

219 10.335771 216.58.196.36 192.168.117.63 1CP 74.45 220 10.344479 216.58.196.36 192.168.117.63 1CP 66.44 221 10.344524 192.168.117.63 216.58.196.36 1CP 54.45 222 10.344566 216.58.196.36 121.68.196.36 1CP 143.4 222 10.344566 216.58.196.36 121.68.196.36 1CP 143.4 223 10.344564 192.168.117.63 216.58.196.36 1CP 143.4 224 10.344618 216.58.196.36 121.68.117.63 1CP 143.4 224 10.344618 216.58.196.36 121.68.117.63 1CP 143.4 225 10.345629 192.168.147.63 216.58.196.36 1CP 64.4 226 10.34563 121.65.147.63 121.58.196.36 1CP 64.4 227 10.34451 121.65.147.63 121.68.17.63 1CP 64.4 228 10.345641 122.165.147.63 121.68.17.63 1CP 64.4 228 10.345651 121.68.106.36 121.68.17.63 1CP 64.4 228 10.345651 121.68.106.36 121.68.17.63 1CP 64.4 228 10.345651 121.68.106.36 121.68.17.63 1CP 74.4 229 10.345651 121.68.106.36 121.68.17.63 1CP 74.4 220 10.345651 121.68.17.63 121.68.17.63 1CP 74.4 221.68.17.63 121.68.17.63 121.68.17.63 1CP 74.4 222 10.345651 121.68.17.63 121.68.17.63 1CP 74.4 223 10.497652 122.168.17.63 121.68.17.63 1CP 74.4 224 10.35651 121.68.17.63 121.68.17.63 121.68.17.63 1CP 74.4 224 10.35651 121.68.17.63 121.68.17.63 121.68.17.63 1CP 74.4 224 10.35651 121.68.17.63 121.68.17.63 121.68.17.63 1CP 74.4 224 10.48626 122.168.17.63 121.68.17.63 1CP 74.4 224 10.55651 121.68.16.17.63 121.68.17.63 121.68.17.63 1CP 74.4 224 10.55651 121.68.17.63 121.68.17.63 1CP 74.4 225 10.35651 121.68.17.63 121.68.17.63 1CP 74.4 226 10.35651 121.68.17.63 121.68.17.63 1CP 74.4 227 10.35651 121.68.17.63 121.68.17.63 1CP 74.4 228 10.55653 121.68.17.63 121.68.17.63 1CP 74.4 229 10.55653 121.68.17.63 121.68.17.63 1CP 74.4 229 10.55653 121.68.17.63 121.68.17.63 1CP 143.4 220 10.55654 121.68.17.63 121.68.17.63 1CP 143.4 220 10.55654 121.68.17.63 121.68.17.63 1CP 143.4 220 10.55654 121.68.17.63 121.68.17.63 121.68.17.63 1CP 143.4 220 10.55654 121.68.17.63 121.68.17.63 121.58.196.36 1CP 143.4 220 10.55654 121.68.17.63 121.68.17.63 121.58.196.36 1CP 143.4 220 10.55654 121.68.17.63 121	
219 10.335771 216.58.196.36 192.168.117.63 1CP 74.45 220 10.344479 216.58.196.36 192.168.117.63 1CP 66.44 221 10.344524 192.168.117.63 216.58.196.36 1CP 54.45 222 10.344566 216.58.196.36 121.68.196.36 1CP 143.4 222 10.344566 216.58.196.36 121.68.196.36 1CP 143.4 223 10.344564 192.168.117.63 216.58.196.36 1CP 143.4 224 10.344618 216.58.196.36 121.68.117.63 1CP 143.4 224 10.344618 216.58.196.36 121.68.117.63 1CP 143.4 225 10.345629 192.168.147.63 216.58.196.36 1CP 64.4 226 10.34563 121.65.147.63 121.58.196.36 1CP 64.4 227 10.34451 121.65.147.63 121.68.17.63 1CP 64.4 228 10.345641 122.165.147.63 121.68.17.63 1CP 64.4 228 10.345651 121.68.106.36 121.68.17.63 1CP 64.4 228 10.345651 121.68.106.36 121.68.17.63 1CP 64.4 228 10.345651 121.68.106.36 121.68.17.63 1CP 74.4 229 10.345651 121.68.106.36 121.68.17.63 1CP 74.4 220 10.345651 121.68.17.63 121.68.17.63 1CP 74.4 221.68.17.63 121.68.17.63 121.68.17.63 1CP 74.4 222 10.345651 121.68.17.63 121.68.17.63 1CP 74.4 223 10.497652 122.168.17.63 121.68.17.63 1CP 74.4 224 10.35651 121.68.17.63 121.68.17.63 121.68.17.63 1CP 74.4 224 10.35651 121.68.17.63 121.68.17.63 121.68.17.63 1CP 74.4 224 10.35651 121.68.17.63 121.68.17.63 121.68.17.63 1CP 74.4 224 10.48626 122.168.17.63 121.68.17.63 1CP 74.4 224 10.55651 121.68.16.17.63 121.68.17.63 121.68.17.63 1CP 74.4 224 10.55651 121.68.17.63 121.68.17.63 1CP 74.4 225 10.35651 121.68.17.63 121.68.17.63 1CP 74.4 226 10.35651 121.68.17.63 121.68.17.63 1CP 74.4 227 10.35651 121.68.17.63 121.68.17.63 1CP 74.4 228 10.55653 121.68.17.63 121.68.17.63 1CP 74.4 229 10.55653 121.68.17.63 121.68.17.63 1CP 74.4 229 10.55653 121.68.17.63 121.68.17.63 1CP 143.4 220 10.55654 121.68.17.63 121.68.17.63 1CP 143.4 220 10.55654 121.68.17.63 121.68.17.63 1CP 143.4 220 10.55654 121.68.17.63 121.68.17.63 121.68.17.63 1CP 143.4 220 10.55654 121.68.17.63 121.68.17.63 121.58.196.36 1CP 143.4 220 10.55654 121.68.17.63 121.68.17.63 121.58.196.36 1CP 143.4 220 10.55654 121.68.17.63 121	
229 10.335721 216.58.196.36 192.168.117.63 TCP 66 42 221 10.344524 192.168.196.36 192.168.117.63 TCP 54 48 222 10.344524 192.168.196.36 192.168.117.63 TCP 54 48 222 10.344564 192.168.196.36 192.168.117.63 TCP 143 44 222 10.344564 192.168.196.36 192.168.117.63 TCP 143 44 222 10.344564 192.168.196.36 192.168.117.63 TCP 143 44 222 10.344564 192.168.196.36 192.168.117.63 TCP 54 48 224 10.344564 192.168.196.36 192.168.117.63 TCP 54 48 224 10.344564 192.168.196.36 192.168.117.63 TCP 54 48 226 10.34563 192.168.117.63 192.168.117.63 TCP 56 48 226 10.34564 192.168.117.63 192.168.117.63 TCP 74 49 229 10.34561 192.168.117.63 192.168.117.63 TCP 66 49 224 10.49894 192.168.117.63 192.168.117.63 TCP 66 49 224 10.49895 192.168.117.63 192.168.117.63 TCP 66 49 224 10.4985 192.168.117.63 192.168.117.	CP Out-Of-Order] 45734 → 443 [PSH, ACK] Seq=1 Ack=1 Win=29312 Len=191 TSval=1992
229 10.344479 216.58.196.36 126.58.196.36 1CP 54 4 222 10.344564 192.166.117.63 216.58.196.36 1CP 1434 4 222 10.344566 216.58.196.36 127.63 126.58.196.36 1CP 1434 4 223 10.344604 192.166.117.63 216.58.196.36 1CP 54 4 224 10.344618 216.58.196.36 126.58.196.36 1CP 54 4 225 10.344628 216.58.196.36 122.168.117.63 1CP 64 225 10.344628 126.58.196.36 122.168.117.63 1CP 64 222 10.345641 122.168.117.63 126.58.196.36 102.168.117.63 1CP 74 4 222 10.345641 122.168.117.63 122.168.117.63 1CP 74 4 223 10.345641 122.168.117.63 122.168.117.63 1CP 74 4 223 10.345641 122.168.117.63 122.168.117.63 102.16	736 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1992462308 TSec
221 10. 344524 192.168.117.63 216.58.196.36 TCP 54.48 223 10. 344604 192.168.117.63 216.58.196.36 TCP 54.49 223 10. 344604 192.168.117.63 216.58.196.36 TCP 54.49 224 10. 344618 216.58.196.36 192.168.117.63 TLSV1.2 482 CC 225 10. 344629 192.168.117.63 216.58.196.36 TCP 54.49 226 10. 344629 192.168.117.63 216.58.196.36 TCP 54.49 227 10. 344646 192.168.117.63 216.58.196.36 TCP 54.49 229 10. 345964 216.58.196.36 192.168.117.63 TCP 54.49 229 10. 345965 192.168.117.63 216.58.196.36 TCP 54.49 229 10. 58586 192.168.117.63 216.58.196.36 TCP 54.49 229 10. 58586 192.168.117.63 216.58.196.36 TCP 56.49 239 10. 585282 192.168.117.63 216.58.196.36 TCP 56.49 239 10. 585286 192.168.117.63 216.58.196.36 TCP 56.49 239 10. 585286 192.168.117.63 216.58.196.36 TCP 56.49 239 10. 585286 192.168.117.63 216.58.196.36 TCP 56.49 240 10. 585345 216.58.196.36 192.168.117.63 TCP 66.49 241 10. 585345 216.58.196.36 192.168.117.63 TCP 66.49 240 10. 585345 216.58.196.36 TCP 66.49 240 10. 585545 216.58.196.36 TCP 66.49 240 10. 585545 216.58	3 → 45734 [ACK] Seq=1 Ack=193 Win=43520 Len=0 TSval=3608668879 TSecr=1992462295
222 10.344586 216.58.196.36 126.51.76.3 162.166.117.63 1CP 1434 42.224 10.344618 216.58.196.36 122.168.117.63 1CP 54.4 22.25 10.344628 216.58.196.36 122.168.117.63 1CP 54.4 22.26 10.344628 216.58.196.36 122.168.117.63 1CP 64.4 22.27 10.344624 122.168.117.63 126.58.196.36 122.168.117.63 1CP 54.4 22.27 10.344624 122.168.117.63 126.58.196.36 122.168.117.63 1CP 74.4 22.27 10.345641 122.168.117.63 126.58.196.36 122.168.117.63 1CP 74.4 22.29 10.345641 122.168.117.63 126.58.196.36 1CP 74.4 22.29 10.345624 122.168.117.63 126.58.196.36 1CP 74.4 22.29 10.345625 122.168.196.36 122.168.117.63 1CP 12.29 12	rver Hello
223 10, 344694 192,168,117,63 216,58,196,36 TCP 54 48 224 10, 344629 192,168,117,63 216,58,196,38 TCP 54 48 227 10, 344629 192,168,117,63 216,58,196,38 TCP 56 48 227 10, 344646 192,168,196,36 192,168,117,63 102,168,117,63 TCP 54 48 229 10, 345641 216,58,196,38 192,168,117,63 TCP 54 48 229 10, 345665 192,168,117,63 216,58,196,38 TCP 54 48 229 10, 345665 192,168,117,63 216,58,196,38 TCP 54 48 232 10, 497891 216,58,196,36 192,168,117,63 216,58,196,38 TCP 74 49 232 10, 497891 216,58,196,36 192,168,117,63 216,58,196,36 TCP 74 49 232 10, 498791 216,58,196,36 192,168,117,63 TCP 74 49 232 10, 5957951 192,168,117,63 216,58,196,36 TCP 74 49 232 10, 5957951 192,168,117,63 216,58,196,36 TCP 74 49 232 10, 5957951 192,168,117,63 216,58,196,36 TCP 74 49 232 10, 5957951 192,158,196,36 192,168,117,63 TCP 74 49 232 10, 595266 192,168,117,63 216,58,196,36 TCP 74 49 239 10, 595266 192,168,117,63 216,58,196,36 TCP 74 49 24 10, 595343 216,58,196,36 192,168,117,63 TCP 1434 49 24 10, 595343 216,58,196,36 192,168,117,63 TCP 1434 49 24 10, 595343 216,58,196,36 192,168,117,63 TCP 1434 49 24 10, 595343 216,58,196,36 192,168,117,63 TCP 144 49 22 10, 595345 216,58,196,36 TCP 166,48 196,36 TCP 166,48 196,36 TCP 167 10, 10, 10, 10, 10, 10, 10, 10, 10, 10,	734 → 443 [RST] Seq=193 Win=0 Len=0
224 10. 344618 216.58.196.36 120.168.117.63 TLSV1.2 482 CC 225 10. 344633 216.58.196.36 120.168.117.63 TCP 66 42 223 10. 344643 122.165.81.196.36 120.168.117.63 TCP 66 42 223 10. 345641 216.58.196.36 120.168.117.63 TCP 74 42 223 10. 345641 121.658.196.36 TCP 74 42 223 10. 345651 121.658.196.36 TCP 74 42 224 10. 346651 121.658.196.36 TCP 74 42 224 10. 346651 121.658.196.36 TCP 74 42 225 121.658.196.36 TCP 74 66 42	3 → 45734 [ACK] Seq=1369 Ack=193 Win=43520 Len=1368 TSval=3608668889 TSecr=19924 734 → 443 [RST] Seg=193 Win=0 Len=0
225 16. 344629 192,168,117,63 216,58,196,36 TCP 54.48 227 16. 344646 192,168,117,63 192,168,117,63 102,168,1	rtificate, Server Key Exchange, Server Hello Done
226 10. 344633 216.58.196.36 120.168.117.63 TCP 66 42 229 10. 345641 216.58.196.36 120.168.117.63 120.168.117.63 TCP 74 42 229 10. 345661 120.168.117.63 1216.58.196.36 TCP 74 42 229 10. 345661 120.168.117.63 1216.58.196.36 TCP 74 42 229 10. 345665 120.168.117.63 1216.58.196.36 TCP 74 42 229 10. 345691 120.168.117.63 120.168.117.63 TCP 120.168.117.	734 - 443 [RST] Seq=193 Win=0 Len=0
227 16. 344646 192.168.117.63 216.58.196.36 TCP 54.4 229 16. 345665 192.168.117.63 216.58.196.38 TCP 54.4 229 16. 345665 192.168.117.63 216.58.196.38 TCP 54.4 232 16. 497891 216.58.196.36 192.168.117.63 TCP 74.4 232 16. 497891 216.58.196.36 192.168.196.36 TCP 74.4 232 16. 497891 216.58.196.36 192.168.196.36 TCP 66.4 234 10. 498246 192.168.117.63 216.58.196.36 TCP 66.4 234 10. 498246 192.168.117.63 192.168.117.63 TCP 66.4 235 10. 557511 216.58.196.36 192.168.117.63 TCP 66.4 236 10. 565193 216.58.196.36 192.168.117.63 TCP 66.4 238 10. 565258 192.168.117.63 216.58.196.36 TCP 66.4 238 10. 565258 192.168.117.63 216.58.196.36 TCP 66.4 241 10. 565343 216.58.196.36 192.168.117.63 TCP 66.4 241 10. 565345 192.168.117.63 216.58.196.36 TCP 66.4 242 10. 575245 192.168.117.63 216.58.196.36 TCP 66.4 247 10. 565348 192.168.117.63 216.58.196.36 TCP 66.4 247 10. 565348 192.168.117.63 116.17.63 TCP 243.4 249 10. 565348 192.168.117.63 116.17.63 TCP 66.4 247 10. 565348 192.168.117.63 116.17.63 TCP 66.4 247 10. 5655848 192.168.117.63 116.17.63 TCP 66.4 247 10. 1676848 192.168.17.63 116.17.63 TCP 66.4 247 10. 16768 192.168.17.63 116.18.17.63 TCP 66	3 → 45734 [FIN, ACK] Seq=3153 Ack=193 Win=43520 Len=0 TSval=3608668889 TSecr=199
229 18.345665 192.168.117.63 216.58.196.36 TCP 54.48 231 10.497891 216.58.196.36 216.58.196.36 TCP 74.44 233 10.497891 216.58.196.36 192.168.117.63 216.58.196.36 TCP 74.42 233 10.497891 216.58.196.36 121.68.117.63 216.58.196.36 TCP 66.44 234 10.498246 192.168.117.63 216.58.196.36 TLSVI.2 257 C 236 10.565193 216.58.196.36 192.168.117.63 TCP 66.4 237 10.565268 192.168.117.63 216.58.196.36 TCP 66.4 238 10.565298 216.58.196.36 192.168.117.63 TCP 64.4 249 10.565326 192.168.117.63 216.58.196.36 TCP 66.4 241 10.565326 192.168.117.63 216.58.196.36 TCP 66.4 241 10.565365 192.168.117.63 216.58.196.36 TCP 66.4 242 10.565363 192.168.117.63 115.58.196.36 TCP 66.4 241 10.565365 192.168.117.63 216.58.196.36	734 → 443 [RST] Seq=193 Win=0 Len=0
233 16.498497 192.168.117.63 216.58.196.36 TCP 74 44 233 16.497952 192.168.117.63 216.58.196.36 TCP 66 44 233 16.497952 192.168.117.63 216.58.196.36 TCP 66 44 233 16.497952 192.168.117.63 216.58.196.36 TCP 66 44 235 16.557811 216.58.196.36 192.168.191.63 TCP 66 42 235 16.557811 216.58.196.36 192.168.117.63 TCP 66 42 237 16.552599 216.55 196.36 192.168.117.63 TCP 66 42 237 16.552599 216.55 196.36 192.168.117.63 TCP 66 42 237 16.552589 126.56 196.36 192.168.117.63 TCP 68 42 237 16.552589 126.56 196.36 192.168.117.63 TCP 68 42 249 16.552543 216.58 196.36 192.168.117.63 TCP 66 42 241 16.552543 192.168.117.63 126.58.196.36 TCP 66 42 241 16.552545 192.168.117.63 216.58.196.36 TCP 66 42 242 16.552545 192.168.117.63 216.58.196.36 TCP 66 42 242 16.649536 192.168.117.63 216.58.196.36 TCP 66 43 2559 16.649536 192.168.117.63 216.58.196.36 TLSV1.2 199 CC 256 16.649536 192.168.117.63 126.58.196.36 TLSV1.2 296 NC 256 16.649536 192.168.117.63 126.58.196.36 TLSV1.2 296 NC 256 16.649536 192.168.117.63 126.58.196.36 TLSV1.2 296 NC 257 16.11987 192.188.117.63 192.168.117.63 TLSV1.2 296 NC 257 16.11987 192.188.117.63 192.168.107.63 TLSV1.2 194 A2 257 11.11987 192.188.117.63 192.188.107.63 TLSV1.2 194 A2 276 11.11987 192.188.117.63 192.188.117.63 TLSV1.2 55 A2 276 11.11987 192.188.117.63 192.188.117.63 TLSV1.2 55 A2 276 11.11987 192.188.117.63 192.188.117.63 TLSV1.2 55 A2 277 11.119849 216.58.196.36 192.188.117.63 TLSV1.2 55 A2 278 11.119897 192.188.117.63 192.188.117.63 TLSV1.2 55 A2 278 11.119897 192.188.117.63 192.188	3 → 45736 [SYN, ACK] Seq=0 Ack=1 Win=42408 Len=0 MSS=1380 SACK_PERM=1 TSval=3382
233 10.497691 216.58.196.36 192.168.117.63 TCP 74 42 233 10.497952 192.168.117.63 216.58.196.36 TCP 66 43 234 10.498249 192.168.117.63 216.58.196.36 TLSVI.2 257 C. 236 10.557611 216.58.196.36 192.168.117.63 TCP 66 42 236 10.565193 216.58.196.36 192.168.117.63 TCP 66 42 237 10.565268 192.166.117.63 216.58.196.36 TCP 66 43 239 10.565298 216.58.196.36 192.168.117.63 TCP 1434 42 239 10.565298 216.58.196.36 192.168.117.63 TCP 1434 42 240 10.565343 216.58.196.36 192.168.117.63 TCP 66 42 110.565343 216.58.196.36 192.168.117.63 TCP 66 42 110.565343 216.58.196.36 192.168.117.63 TCP 66 42 110.565343 216.58.196.36 192.168.117.63 TCP 66 42 10.565343 192.168.117.63 216.58.196.36 TCP 66 42 10.575245 192.168.117.63 216.58.196.36 TCP 66 42 10.575245 192.168.117.63 216.58.196.36 TLSVI.2 199 C. 242 10.575245 192.168.117.63 216.58.196.36 TLSVI.2 296 N. 69 10.649530 192.168.117.63 216.58.196.36 TLSVI.2 243 A1 226.16.77.1669 192.168.117.63 216.58.196.36 TCP 66 42 270 11.655681 192.168.117.63 216.58.196.36 TCP 10.575149 192.168.117.63 216.58.196.36 TCP 10.575149 192.168.117.63 216.58.196.36 TCP 66 42 272 11.169598 192.168.117.63 216.58.196.36 TCP 66 42 273 11.119769 192.168.117.63 216.58.196.36 TCP 66 42 273 11.11977 192.168.117.63 216.58.196.36 TCP 66 42 273 11.11977 192.168.117.63 216.58.196.36 TCP 66 42 273 11.11977 192.168.117.63 216.58.196.36 TCP 66 42 277 11.119797 192.168.117.63 216.58.196.36 TCP 66 42 277 11.119799 192.168.117.63 216.58.196.36 TCP 66 42 277 11.119979 192.168.117.63 216.58.196.36 TCP 66 42 277 11.119979 192.168.117.63 216.58.	736 → 443 [RST] Seq=1 Win=0 Len=0
233 10.497952 192.168.117.63 216.58.196.36 TCP 66 44 234 10.495240 192.168.117.63 216.58.196.36 TLSV1.2 257 CL 235 10.557811 216.58.196.36 192.168.117.63 TCP 66 44 236 10.555919 216.558.196.36 192.168.117.63 TCP 66 47 237 10.565268 192.168.196.36 192.168.117.63 TCP 66 48 239 10.565268 192.168.196.36 192.168.117.63 TCP 66 48 239 10.565259 216.58.196.36 192.168.117.63 TCP 66 48 249 10.565259 192.168.117.63 216.58.196.36 TCP 66 49 249 10.565251 192.168.117.63 216.58.196.36 TCP 66 49 249 10.565251 192.168.117.63 216.58.196.36 TCP 66 49 249 10.565251 192.168.117.63 216.58.196.36 TCP 10.56526 192.168.117.63 216.58.196.36 TCP 10.56526 192.168.117.63 216.58.196.36 TCP 10.56526 192.168.117.63 216.58.196.36 TLSV1.2 199 CC 10.69536 192.168.117.63 216.58.196.36 TLSV1.2 199 CC 10.69536 192.168.117.63 216.58.196.36 TLSV1.2 296 NC 10.69536 192.168.117.63 216.58.196.36 TLSV1.2 296 NC 10.69536 192.168.117.63 216.58.196.36 TLSV1.2 296 NC 10.69536 192.168.117.63 216.58.196.36 TLSV1.2 294 AV 10.771669 192.168.117.63 216.58.196.36 TLSV1.2 296 NC 10.69536 192.168.117.63 192.168.117.63 192.168.117.63 192.168.117.63 192.168.117.63 192.168.117.63 192.168.117.63 192.168.117.63 192.168.117.63 192.168.117.63 192.168.117.63 TLSV1.2 296 NC 10.69546 192.168.117.63 192.168.117.63 TLSV1.2 194 AV 10.77169 192.168.117.63 192.168.107.63 TLSV1.2 194 AV 10.77169 192.168.117.63 192.168.117.63 192.168.117.63 TLSV1.2 194 AV 10.77169 192.168.117.63 192.168.117.63 192.168.117.63 TLSV1.2 194 AV 10.77169 192.168.117.63 192.16	738 - 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1992462458 TSec
234 10. 498249 192. 168. 117. 63 126. 58. 196. 38 TLSVI. 2 257 C. 236 10. 557511 216. 58. 196. 38 192. 168. 117. 63 TCP 66 44 236 10. 655193 216. 58. 196. 36 192. 168. 117. 63 TCP 66 42 237 10. 565268 192. 168. 117. 63 216. 58. 196. 36 TCP 66 43 238 10. 565298 216. 56. 196. 36 192. 168. 197. 63 TCP 1434 42 241 10. 565342 216. 58. 196. 36 192. 168. 196. 36 TCP 66 44 110. 565343 216. 58. 196. 36 192. 168. 196. 36 TCP 66 44 110. 565343 216. 58. 196. 36 192. 168. 196. 36 TCP 66 44 110. 565343 216. 58. 196. 36 192. 168. 196. 36 TCP 66 44 10. 565343 216. 58. 196. 36 192. 168. 196. 36 TCP 66 44 10. 565343 216. 58. 196. 36 192. 168. 196. 36 TCP 66 44 10. 565343 216. 58. 196. 36 TCP 66 44 10. 565343 216. 58. 196. 36 TCP 66 44 10. 565345 216. 58. 196. 36 TCP 242 10. 575245 192. 168. 117. 63 216. 58. 196. 36 TLSVI. 2 159 C. 242 10. 575245 192. 168. 117. 63 192. 168. 117. 63 TLSVI. 2 243 A1 10. 565340 192. 168. 117. 63 192. 168. 117. 63 TLSVI. 2 243 A1 10. 565340 192. 168. 117. 63 16. 50. 196. 36 TLSVI. 2 243 A1 10. 565340 192. 168. 117. 63 116. 50. 196. 36 TCP 903 TCP 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.	3 → 45738 [SYN, ACK] Seq=0 Ack=1 Win=42408 Len=0 MSS=1380 SACK_PERM=1 TSval=2777
236 10. 557811	738 - 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1992462517 TSecr=2777108436
236 10.565193 216.58.196.36 192.168.117.63 TLSV1.2 1434 St 237 10.565268 192.168.117.63 216.58.196.36 TCP 66 45 238 10.565298 216.56.196.36 192.168.117.63 TCP 1434 4- 239 10.565298 216.56.196.36 192.168.196.36 TCP 66 45 240 10.565343 216.58.196.36 192.168.197.63 TCP 66 45 241 10.565343 216.58.196.36 192.168.117.63 TCP 66 45 242 10.575245 192.168.117.63 216.58.196.36 TCP 66 45 260 10.575245 192.168.117.63 216.58.196.36 TLSV1.2 199 CC 126 10.635163 216.58.196.36 192.168.117.63 TLSV1.2 245 MC 10.575245 192.168.117.63 216.58.196.36 TLSV1.2 245 MC 10.649539 192.168.117.63 216.59.196.36 TLSV1.2 245 MC 10.649539 192.168.117.63 216.59.196.36 TLSV1.2 245 MC 10.649539 192.168.117.63 216.59.196.36 TCP 904 TCP 10.649539 192.168.117.63 216.58.196.36 TCP 904 TCP 10.549549 192.168.117.63 216.58.196.36 TCP 904 TCP 10.549549 192.168.117.63 192.168.117.63 TCP 904 TCP 10.549549 192.168.117.63 192.168.117.63 TCP 904 TCP 10.549549 192.168.117.63 192.168.117.63 TCP 904 TCP 904 TCP 10.549549 192.168.117.63 192.168.117.63 TCP 904 TCP 904 TCP 10.549549 192.168.117.63 192.168.117.63 TCP 904 T	ient Hello
237 10. 565268 192.168.117.63 216.58.196.36 TCP 66 44 239 10. 565258 216.56.196.36 192.168.117.63 TCP 1434 44 24 61. 565343 216.58.196.36 192.168.117.63 TCP 66 45 249 10. 565343 216.58.196.36 192.168.117.63 TLSV1.2 240 12. 565345 216.58.196.36 192.168.117.63 TLSV1.2 296 12. 565 10. 635163 216.58.196.36 192.168.117.63 TLSV1.2 296 NC 259 10. 649530 192.168.117.63 216.58.196.36 TLSV1.2 296 NC 259 10. 649530 192.168.117.63 216.58.196.36 TLSV1.2 294 AC 261.575.169 10. 649581 192.168.117.63 126.58.196.36 TLSV1.2 294 AC 261.63.196.36 TLSV1.2 294 AC 276 TLSV1.2 294 TLSV1.2 294 TLSV1.2 294 TLSV1.2 294 TLSV1.2 294 TLSV1.2 295 TLSV1.2 294 T	3 → 45738 [ACK] Seq=1 Ack=192 Win=43520 Len=0 TSval=2777108495 TSecr=1992462518
238 16.565298 216.56.196.36 192.166.117.63 TCP 1434 4-239 10.565228 192.166.117.63 216.56.196.36 TCP 66 44 24 10.565343 216.58.196.36 192.168.117.63 TCP 165.117.63 TCP 165	rver нешо 738 → 443 [ACK] Seq=192 Ack=1369 Win=32128 Len=0 TSval=1992462585 TSecr=27771085
239 10. 565228 192. 168. 117. 63 126. 58. 196. 36 TCP 66 44 249 10. 565343 216. 58. 196. 36 129. 168. 117. 63 TLSV1. 2 482 CC 241 10. 565365 192. 168. 117. 63 216. 58. 196. 36 TCP 66 45 242 10. 575245 192. 168. 117. 63 216. 58. 196. 36 TCP 66 45 242 10. 575245 192. 168. 117. 63 216. 58. 196. 36 TLSV1. 2 296 N 259 10. 649530 192. 168. 117. 63 216. 58. 196. 36 TLSV1. 2 296 N 259 10. 649501 192. 168. 117. 63 216. 58. 196. 36 TLSV1. 2 294 A 264 10. 57166 192. 158. 117. 63 216. 58. 196. 36 TLSV1. 2 294 A 264 10. 77166 192. 158. 117. 63 216. 58. 196. 36 TLSV1. 2 296 N 264 10. 77166 192. 158. 117. 63 216. 58. 196. 36 TLSV1. 2 296 N 264 10. 77168 192. 158. 117. 63 216. 58. 196. 36 TLSV1. 2 296 N 264 10. 77168 192. 158. 117. 63 216. 58. 196. 36 TCP 78 TLSV1. 2 296 TLSV1.	730 → 443 [ACK] Seq=1369 ACK=1369 WIN=32120 Len=1368 TSval=2777108502 TSecr=19924
246 10. 565343 216. 58. 196. 36 192. 168. 117. 63 TLSV1. 2 482 Ct 241 10. 565545 192. 168. 117. 63 216. 58. 196. 36 TCP 66 44 10. 575245 192. 168. 117. 63 216. 58. 196. 36 TLSV1. 2 159 Ct 256 10. 635163 216. 58. 196. 36 192. 168. 117. 63 TLSV1. 2 296 Nt 259 10. 649530 192. 168. 117. 63 216. 58. 196. 36 TLSV1. 2 243 At 260 10. 649630 192. 168. 117. 63 216. 58. 196. 36 TLSV1. 2 243 At 260 10. 649651 192. 168. 117. 63 216. 58. 196. 36 TLSV1. 2 244 At 260 10. 649651 192. 168. 117. 63 216. 58. 196. 36 TLSV1. 2 244 At 260 10. 649651 192. 168. 117. 63 216. 58. 196. 36 TCP 994 [1.2] 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.	738 → 443 [ACK] Seq=192 Ack=192 Win=35072 Len=0 TSval=1992462585 TSecr=27771085
241 10. 565365 192. 168. 117. 63 216. 58. 196. 38 TCP 66 44 242 10. 575245 192. 168. 117. 63 216. 58. 196. 38 TLSV1. 2 296 N 259 10. 649530 192. 168. 117. 63 216. 58. 196. 38 TLSV1. 2 296 N 259 10. 649530 192. 168. 117. 63 216. 58. 196. 38 TLSV1. 2 294 N 269 10. 649601 192. 168. 117. 63 216. 58. 196. 38 TLSV1. 2 994 N 269 10. 649601 212. 158. 117. 63 216. 58. 196. 38 TLSV1. 2 994 N 269 10. 894751 216. 58. 196. 38 126. 58. 196. 38 TCP 994 TCP 16. 894821 192. 168. 117. 63 216. 58. 196. 38 TCP 187 18. 197 18. 197 197 192. 168. 117. 63 196. 58. 196. 38 TCP 66 44 276 11. 119877 192. 168. 117. 63 192. 168. 117. 63 TLSV1. 2 194 N 276 11. 149438 216. 58. 196. 38 TCP 164. 176. 38 TLSV1. 2 194 N 279 11. 149485 216. 58. 196. 38 TCP 15. 17. 63 TLSV1. 2 194 N 279 11. 149485 216. 58. 196. 38 TCP 15. 196. 38 TCP 18. 177. 63 TLSV1. 2 194 N 279 11. 14948 216. 58. 196. 38 TCP 18. 177. 63 TLSV1. 2 194 N 279 11. 14948 216. 58. 196. 38 TCP 18. 177. 63 TLSV1. 2 194 N 279 11. 14948 216. 58. 196. 38 TCP 18. 177. 63 TLSV1. 2 194 N 279 11. 149485 216. 58. 196. 38 TCP 18. 177. 63 TLSV1. 2 194 N 279 11. 149485 216. 58. 196. 38 TCP 18. 177. 63 TLSV1. 2 194 N 279 11. 149485 216. 58. 196. 38 TCP 18. 177. 63 TLSV1. 2 194 N 279 11. 149485 216. 58. 196. 38 TCP 18. 177. 63 TLSV1. 2 194 N 279 11. 149485 216. 58. 196. 38 TCP 18. 177. 63 TLSV1. 2 194 N 279 11. 149485 216. 58. 196. 38 TCP 18. 177. 63 TLSV1. 2 194 N 279 11. 149485 216. 58. 196. 38 TCP 18. 177. 63 TLSV1. 2 194 N 279 11. 149485 216. 58. 196. 38 TCP 18. 177. 63 TLSV1. 2 194 N 279 11. 149485 216. 58. 196. 38 TCP 18. 177. 63 TLSV1. 2 194 N 279 11. 149485 21	rtificate, Server Kev Exchange, Server Hello Done
242 10. 575245 192. 168. 117. 63 216. 58. 196. 36 TLSV1. 2 159 C. 256 10. 635163 216. 58. 196. 36 192. 168. 117. 63 TLSV1. 2 296 N. 259 10. 649530 192. 168. 117. 63 216. 58. 196. 36 TLSV1. 2 243 AJ 269 10. 6496901 192. 168. 117. 63 216. 58. 196. 36 TLSV1. 2 243 AJ 264 10. 771669 192. 198. 117. 63 216. 58. 196. 36 TLSV1. 2 994 [7.6] 10. 10. 10. 10. 10. 10. 10. 10. 10. 10.	738 → 443 [ACK] Seq=192 Ack=3153 Win=37760 Len=0 TSval=1992462585 TSecr=27771085
256 10, 635163 216, 58, 196, 36 192, 168, 117, 63 TLSV1, 2 296 N 259 10, 649691 192, 168, 117, 63 216, 58, 196, 36 TLSV1, 2 994 A 264 10, 649691 192, 168, 117, 63 216, 58, 196, 36 TLSV1, 2 994 A 264 18, 771669 192, 168, 117, 63 216, 58, 196, 36 TLSV1, 2 296 F 269 18, 894751 216, 58, 196, 36 192, 168, 117, 63 TLSV1, 2 296 F 279 11, 898985 192, 168, 117, 63 216, 58, 196, 36 TCP 181 F 274 11, 119769 192, 168, 117, 63 192, 168, 117, 63 TLSV1, 2 195 F 275 11, 119877 192, 168, 117, 63 192, 168, 117, 63 TCP 66 48 276 11, 119877 192, 168, 117, 63 126, 58, 196, 36 TCP 66 48 277 11, 11979 192, 168, 117, 63 216, 58, 196, 36 TCP 66 48 279 11, 144938 216, 58, 196, 36 192, 168, 117, 63 TLSV1, 2 194 A 279 18, 149498 216, 58, 196, 36 192, 166, 117, 63 TLSV1, 2 194 A 270 16, 117, 6	ient Key Exchange, Change Cipher Spec, Encrypted Handshake Message
269 10, 649691 192, 168, 117, 63 216, 58, 196, 36 TLSV1, 2 994 A 264 10, 7716169 192, 168, 117, 63 216, 58, 196, 36 TCP 994 [269 10, 894751 216, 58, 196, 36 192, 168, 117, 63 TLSV1, 2 296 [279 11, 898981 192, 168, 117, 63 216, 58, 196, 36 TCP 1981 [273 11, 119687 216, 58, 196, 36 192, 168, 117, 63 TLSV1, 2 195 M 274 11, 119769 192, 168, 117, 63 126, 58, 196, 36 TCP 66 48 275 11, 119877 192, 168, 117, 63 192, 168, 117, 63 TLSV1, 2 194 A 276 11, 119877 192, 168, 117, 63 216, 58, 196, 36 TCP 66 48 277 11, 11979 192, 168, 117, 63 216, 58, 196, 36 TCP 66 49 279 11, 144938 216, 58, 196, 36 192, 168, 117, 63 TLSV1, 2 194 A 280 11, 144938 216, 58, 196, 36 192, 168, 117, 63 TLSV1, 2 214 A 280 11, 144948 216, 58, 196, 36 192, 168, 117, 63 TLSV1, 2 214 A	w Session Ticket, Change Cipher Spec, Encrypted Handshake Message
284 18, 771669 192, 168, 117, 63 216, 58, 196, 36 TCP 994 [286 18, 884571 216, 58, 196, 36 192, 168, 117, 63 TLSV1, 2 296 [276 10, 884621 192, 168, 117, 63 216, 58, 196, 36 TCP 78 [272 11, 695985 192, 168, 117, 63 216, 58, 196, 36 TCP 78 [273 11, 119687 216, 58, 196, 36 192, 168, 117, 63 TCP 66 44 [275 11, 11974 192, 168, 117, 63 192, 168, 117, 63 TLSV1, 2 194, 74 [276 11, 119972 192, 168, 117, 63 216, 58, 196, 36 TCP 66 45 [277 11, 119972 192, 168, 117, 63 216, 58, 196, 36 TCP 66 45 [279 11, 144938 216, 58, 196, 36 192, 168, 117, 63 TLSV1, 2 194, 74 [288 11, 1449485 216, 58, 196, 36 192, 168, 117, 63 TLSV1, 2 535 Af 188 117, 64985 216, 58, 196, 36 192, 168, 117, 63 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 192, 166, 117, 63 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 192, 166, 117, 63 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 192, 166, 117, 63 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 192, 166, 117, 63 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 192, 166, 117, 63 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 192, 166, 117, 63 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 192, 166, 117, 63 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 192, 166, 117, 63 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 192, 166, 117, 63 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36 TLSV1, 2 214 Af 188 117, 64985 216, 58, 196, 36	plication Data
269 18. 894751 216. 58. 196. 36 192. 168. 117. 63 TLSV1.2 296 170 279 18. 894821 192. 168. 117. 63 216. 58. 196. 36 TCP 78 17 272 11. 189898 192. 168. 117. 63 216. 58. 196. 36 TCP 1981 17 273 11. 119687 216. 58. 196. 36 192. 168. 117. 63 TLSV1. 2 158 h 275 11. 119442 216. 58. 196. 36 192. 168. 117. 63 TLSV1. 2 194 h 276 11. 119677 192. 168. 117. 63 126. 58. 196. 36 TCP 66 48 277 11. 11979 192. 168. 117. 63 216. 58. 196. 36 TCP 66 48 279 11. 144938 216. 58. 196. 36 192. 168. 117. 63 TLSV1. 2 53 A 280 11. 1449485 216. 58. 196. 36 192. 168. 117. 63 TLSV1. 2 53 A 280 11. 1449485 216. 58. 196. 36 192. 168. 117. 63 TLSV1. 2 214 A	plication Data
276 16, 894821 192, 168, 117, 63 216, 58, 196, 36 TCP 78 272 11, 689885 192, 198, 117, 63 216, 58, 196, 36 TCP 1931 273 11, 119887 216, 58, 196, 36 192, 168, 117, 63 TCP 1931 274 11, 119799 192, 168, 117, 63 216, 58, 196, 36 TCP 66 44 275 11, 119942 216, 58, 196, 36 192, 168, 117, 63 TLSV1, 2 194, M 276 11, 119977 192, 168, 117, 63 216, 58, 196, 36 TCP 66 48 277 11, 149938 216, 58, 196, 36 192, 168, 117, 63 TLSV1, 2 194, M 288 11, 144938 216, 58, 196, 36 192, 168, 117, 63 TLSV1, 2 536, M 288 11, 1449485 216, 58, 196, 36 192, 166, 117, 63 TLSV1, 2 214, M	CP Retransmission] 45738 → 443 [PSH, ACK] Seq=462 Ack=3383 Win=40576 Len=838 TSV
272 11, 169585 192,168,117,63 216,58,196,38 TCP 1931 273 11, 119687 216,58,196,38 192,168,117,63 152,168,117,63 TLSV1,2 158 h 274 11,119769 192,168,117,63 216,58,196,38 TCP 66 48 276 11,119877 192,168,117,63 122,168,117,63 TLSV1,2 194 h 277 11,119972 192,168,117,63 216,58,196,38 TCP 66 48 279 11,144938 216,58,196,38 192,168,117,63 TLSV1,2 535 M 280 11,1449498 216,58,196,38 192,168,117,63 TLSV1,2 535 M 280 11,1449485 216,58,196,38 192,168,117,63 TLSV1,2 525 M	CP Spurious Retransmission] , Encrypted Handshake Message, Change Cipher Spec, E
273 11. 119687 216.58.196.36 192.168.117.63 TLSV1.2 125 Å 274 11. 11975 192.168.117.63 216.58.196.36 TCP 66 44 275 11. 119842 216.58.196.36 192.168.117.63 TLSV1.2 104 Å 276 11. 119877 192.168.117.63 216.58.196.36 TCP 66 44 277 11. 119972 192.168. 117.63 216.58.196.36 TLSV1.2 104 Å 279 11. 144938 216.58.196.36 192.168.117.63 TLSV1.2 53 Å 280 11. 1449485 216.58.196.36 192.166.117.63 TLSV1.2 214 Å	CP Dup ACK 259#1] 45738 - 443 [ACK] Seq=1300 Ack=3383 Win=40576 Len=0 TSval=1992
274 11.119769 192.168.117.63 216.58.196.36 TCP 66.4 275 11.119842 216.58.196.36 192.168.117.63 TLSV1.2 194 M 276 11.119877 192.168.117.63 216.58.196.36 TCP 66.44 277 11.119972 192.168.117.63 216.58.196.36 TLSV1.2 194 M 279 11.144938 216.58.196.36 192.168.117.63 TLSV1.2 535 M 280 11.1449485 216.58.196.36 192.166.117.63 TLSV1.2 214 M 281 11.149495 216.58.196.36 192.166.117.63 TLSV1.2 214 M	CP Retransmission] 45738 443 [PSH, ACK] Seq=285 Ack=3383 Win=40576 Len=1015 TS plication Data
275 11, 119842 216, 58, 196, 36 192, 168, 117, 63 TLSV1, 2 194 Aj 276 11, 119877 192, 168, 117, 63 216, 58, 196, 36 TCP 66 4t 277 11, 119972 192, 168, 117, 63 216, 58, 196, 36 TLSV1, 2 194 Aj 279 11, 144938 216, 58, 196, 36 192, 168, 117, 63 TLSV1, 2 535 Aj 280 11, 1449485 216, 58, 196, 36 192, 168, 117, 63 TLSV1, 2 214 Aj	prication bata 738 → 443 [ACK] Seq=1300 Ack=3452 Win=40576 Len=0 TSval=1992463139 TSecr=2777109
276 11. 119877 192. 168. 117. 63 216. 58. 196. 36 TCP 66. 4½ 277 11. 11972 192. 168. 117. 63 216. 58. 196. 36 TLSV1. 2 194. A 279 11. 144938 216. 58. 196. 36 192. 168. 117. 63 TLSV1. 2 535 A 280 11. 1449485 216. 58. 196. 36 192. 168. 117. 63 TLSV1. 2 214 A	olication Data
277 11.119972 192.168.117.63 216.58.196.36 TLSV1.2 194 Ag 279 11.144938 216.58.196.36 192.168.117.63 TLSV1.2 535 Ag 280 11.144995 216.58.196.36 192.168.117.63 TLSV1.2 214 Ag	738 → 443 [ACK] Seq=1300 Ack=3490 Win=40576 Len=0 TSval=1992463139 TSecr=2777109
279 11.144938 216.58.196.36 192.168.117.63 TLSV1.2 535 A 280 11.144985 216.58.196.36 192.168.117.63 TLSV1.2 214 A	plication Data
	plication Data
	plication Data, Application Data
	plication Data
	738 → 443 [ACK] Seq=1338 Ack=4153 Win=45952 Len=0 TSval=1992463164 TSecr=2777109
	plication Data
285 11.205518 216.58.196.36 192.168.117.63 TCP 66 44	3 → 45738 [ACK] Seq=4153 Ack=1384 Win=45568 Len=0 TSval=2777109143 TSecr=1992463
et II, Src: Dell_7d:fc:24 (34:e6:d7:7d:fc:24), Dst: HewlettP_a9:8b:f8 (5c:8a:38:a9:8	o:f8)
net Protocol Version 4, Src: 192.168.117.63, Dst: 216.58.196.36 Dission Control Protocol, Src Port: 45734, Dst Port: 443, Seq: 1, Ack: 1, Len: 191	

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

Duration of HTTPS session :: 0.929925 sec

17)

Using noonces 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.