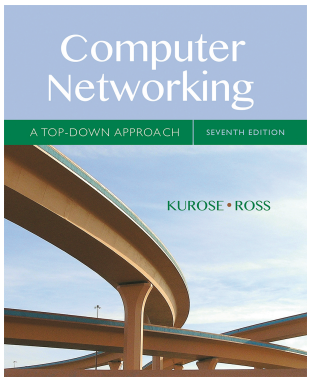
Wireshark Lab: SSL v7.0
SOLUTION

Supplement to *Computer Networking: A Top-Down Approach, 7th ed.,* J.F. Kurose and K.W. Ross

"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb



A Look at the Captured Trace:

staples - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: ssl Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
215	5.974787	192.168.1.104	72.246.122.125	SSLv2	Client Hello
217	6.008484	72.246.122.125	192.168.1.104	TLS	Server Hello, Certificate, Server Hello Done
218	6.010188	192.168.1.104	72.246.122.125	TLS	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
219	6.048457	72.246.122.125	192.168.1.104	TLS	Change Cipher Spec, Encrypted Handshake Message
220	6.048968	192.168.1.104	72.246.122.125	TCP	[TCP segment of a reassembled PDU]
221	6.049053	192.168.1.104	72.246.122.125	TLS	Application Data
224	6.366860	72.246.122.125	192.168.1.104	TLS	Application Data
225	6.367871	72.246.122.125	192.168.1.104	TLS	Application Data
227	6.369293	72.246.122.125	192.168.1.104	TLS	Application Data
228	6.383323	192.168.1.104	72.246.122.125	TCP	[TCP segment of a reassembled PDU]
229	6.383449	192.168.1.104	72.246.122.125	TLS	Application Data
231	7.702870	72.246.122.125	192.168.1.104	TCP	[TCP segment of a reassembled PDU]
236	7.704033	72.246.122.125	192.168.1.104	TLS	Application Data
237	7.725541	192.168.1.104	72.246.122.125	TCP	[TCP segment of a reassembled PDU]
238	7.725667	192.168.1.104	72.246.122.125	TLS	Application Data
240	7.776816	72.246.122.125	192.168.1.104	TLS	Application Data
241	7.792002	192.168.1.104	72.246.122.125	TLS	Application Data

```
⊞ Frame 215 (159 bytes on wire, 159 bytes captured)
⊞ Ethernet II, Src: GemtekTe_86:63:ab (00:90:4b:86:63:ab), Dst: 00:18:3a:2d:8d:a0 (00:18:3a:2d:8d:a0)
⊞ Internet Protocol, Src: 192.168.1.104 (192.168.1.104), Dst: 72.246.122.125 (72.246.122.125)
⊞ Transmission Control Protocol, Src Port: 1310 (1310), Dst Port: https (443), Seq: 1571732215, Ack: 466838551, Len: 105
⊟ Secure Socket Layer
  ⊟ SSLv2 Record Layer: Client Hello
      Length: 103
      Handshake Message Type: Client Hello (1)
      Version: TLS 1.0 (0x0301)
      Cipher Spec Length: 78
      Session ID Length: 0
      Challenge Length: 16
    ⊟ Cipher Specs (26 specs)
        Cipher Spec: SSL2_RC4_128_WITH_MD5 (0x010080)
        Cipher Spec: SSL2_RC2_CBC_128_CBC_WITH_MD5 (0x030080)
        Cipher Spec: SSL2_DES_192_EDE3_CBC_WITH_MD5 (0x0700c0)
        Cipher Spec: SSL2_DES_64_CBC_WITH_MD5 (0x060040)
        Cipher Spec: SSL2_RC4_128_EXPORT40_WITH_MD5 (0x020080)
        Cipher Spec: SSL2_RC2_CBC_128_CBC_WITH_MD5 (0x040080)
        Cipher Spec: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x000039)
```

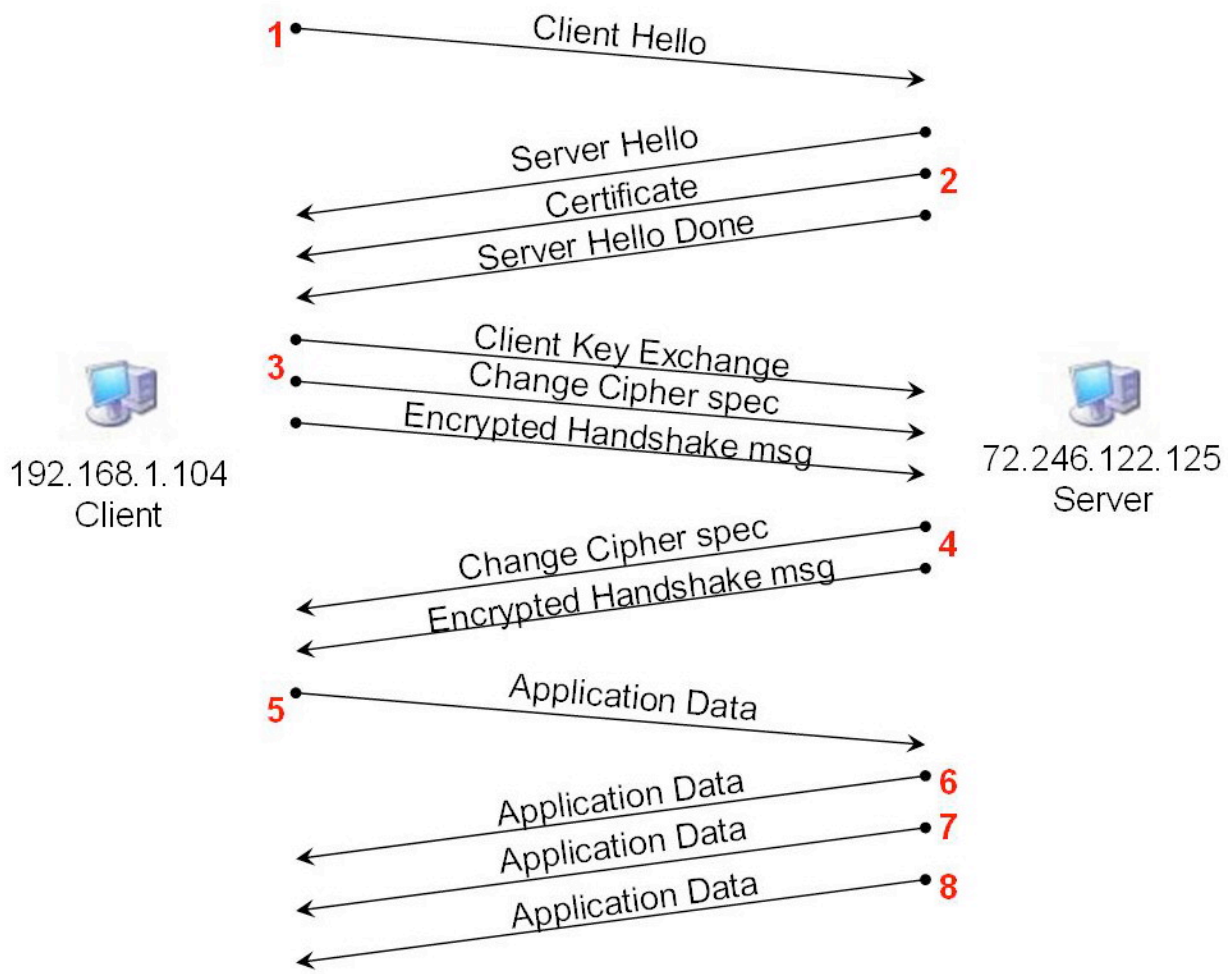
Captured SSL Packets

1. Details of the first 8 captured Ethernet frames (SSL) are listed in the following table:

Frame # in Ethereal	Frame #	Source	Destination	# of SSL Records	List of SSL Records

215	1	192.168.1.104	72.246.122.125	1	Client Hello
217	2	72.246.122.125	192.168.1.104	3	Server Hello Certificate Server Hello Done
218	3	192.168.1.104	72.246.122.125	3	Client Key Exchange Change Cipher spec Encrypted Handshake msg
219	4	72.246.122.125	192.168.1.104	2	Change Cipher spec Encrypted Handshake msg
221	5	192.168.1.104	72.246.122.125	1	Application Data
224	6	72.246.122.125	192.168.1.104	1	Application Data
225	7	72.246.122.125	192.168.1.104	1	Application Data
227	8	72.246.122.125	192.168.1.104	1	Application Data

Details of the first 8 Ethernet Frames for SSL

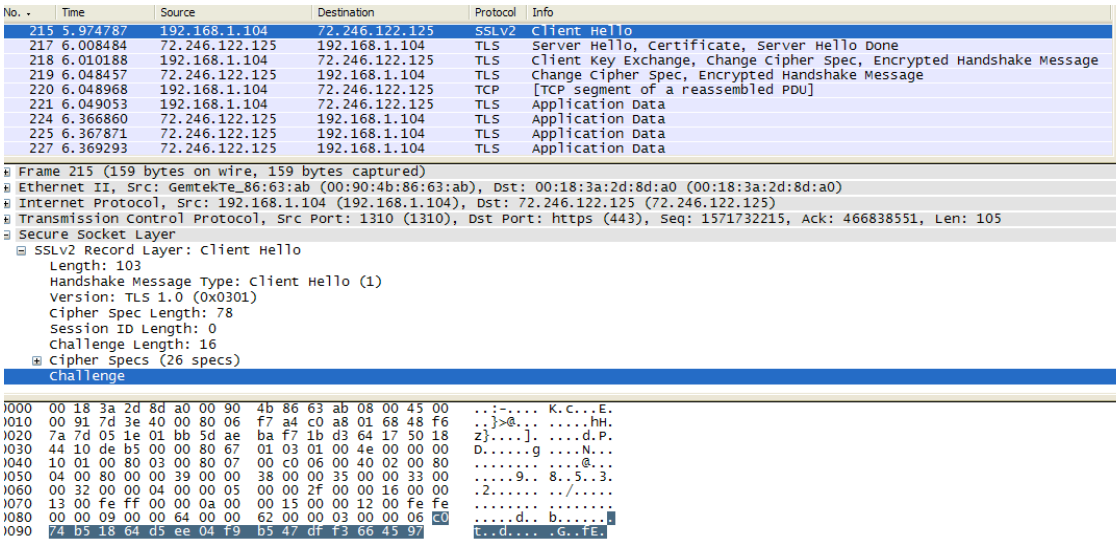


Timing Diagram of the SSL Session

2. Each SSL record begins with the same three fields (content type, version, and length). The values for each SSL record type are listed as follow:

Frame #	SSL Record Types	Content Type	Version	Length
1	Client Hello	Handshake (22)	TLS 1.0 (0x0301)	103
2	Server Hello Certificate Server Hello Done	Handshake (22) Handshake (22) Handshake (22)	TLS 1.0 (0x0301) TLS 1.0 (0x0301) TLS 1.0 (0x0301)	74 989 4
3	Client Key Exchange Change Cipher spec Encrypted Handshake msg	Handshake (22) ChangeCipherSpec(20) Handshake (22)	TLS 1.0 (0x0301) TLS 1.0 (0x0301) TLS 1.0 (0x0301)	134 1 48
4	Change Cipher spec Encrypted Handshake msg	ChangeCipherSpec(20) Handshake (22)	TLS 1.0 (0x0301) TLS 1.0 (0x0301)	1 48
5	Application Data	Application Data (23)	TLS 1.0 (0x0301)	1552
6	Application Data	Application Data (23)	TLS 1.0 (0x0301)	912
7	Application Data	Application Data (23)	TLS 1.0 (0x0301)	32
8	Application Data	Application Data (23)	TLS 1.0 (0x0301)	32

Client Hello Record



Expanded Client Hello Record

3. The value of the content type is Handshake (22) because this is handshake message type (as shown above).

4. Yes, the Client Hello record contains a challenge and its value in HEX is 0xC074B51864D5EE04F9B547DFF3664597

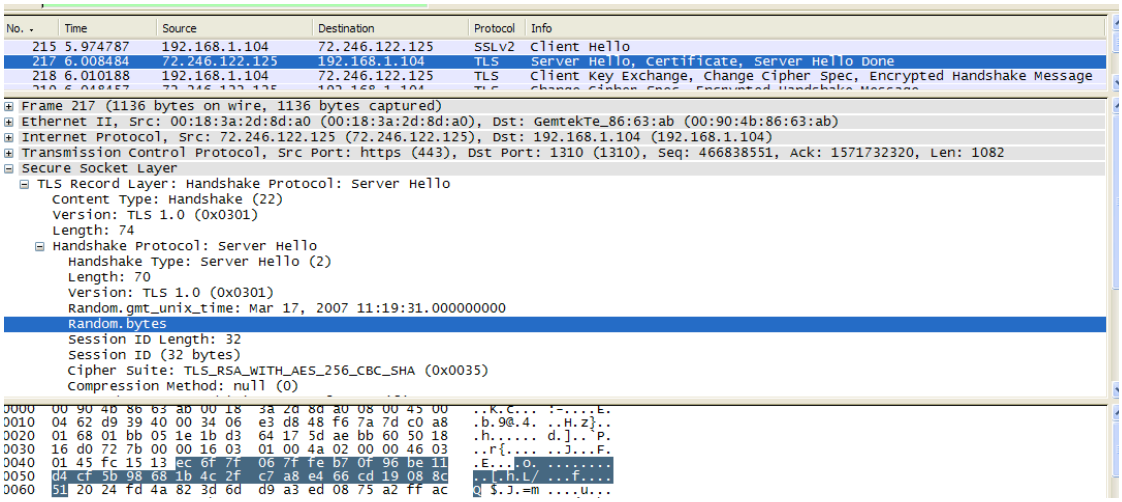
5. Yes, Client Hello record advertises the cipher suite it supports, as shown below.

```
Handshake Message Type: Client Hello (1)
Version: TLS 1.0 (0x0301)
Cipher Spec Length: 78
Session ID Length: 0
Challenge Length: 16
Cipher Specs (26 specs)
  Cipher Spec: SSL2_RC4_128_WITH_MD5 (0x010080)
  Cipher Spec: SSL2_RC2_CBC_128_CBC_WITH_MD5 (0x030080)
  Cipher Spec: SSL2_DES_192_EDE3_CBC_WITH_MD5 (0x0700c0)
  Cipher Spec: SSL2_DES_64_CBC_WITH_MD5 (0x060040)
  Cipher Spec: SSL2_RC4_128_EXPORT40_WITH_MD5 (0x020080)
  Cipher Spec: SSL2_RC2_CBC_128_CBC_WITH_MD5 (0x040080)
  Cipher Spec: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x000039)
  Cipher Spec: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x000038)
  Cipher Spec: TLS_RSA_WITH_AES_256_CBC_SHA (0x000035)
  Cipher Spec: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x000033)
  Cipher Spec: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x000032)
  Cipher Spec: TLS_RSA_WITH_RC4_128_MD5 (0x000004)
  Cipher Spec: TLS_RSA_WITH_RC4_128_SHA (0x000005)
  Cipher Spec: TLS_RSA_WITH_AES_128_CBC_SHA (0x00002f)
  Cipher Spec: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x000016)
  Cipher Spec: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x000013)
  Cipher Spec: SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA (0x00feff)
  Cipher Spec: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x00000a)
  Cipher Spec: TLS_DHE_RSA_WITH_DES_CBC_SHA (0x000015)
  Cipher Spec: TLS_DHE_DSS_WITH_DES_CBC_SHA (0x000012)
  Cipher Spec: SSL_RSA_FIPS_WITH_DES_CBC_SHA (0x00fefe)
  Cipher Spec: TLS_RSA_WITH_DES_CBC_SHA (0x000009)
  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)
Challenge
```

Client Hello Record's Cipher specs

The first listed TLS (SSLv3) cipher spec (highlighted above) is: DHE and RSA (public-key algorithms) with 256-bit CBC AES (symmetric-key) with SHA (hash algorithm).

Server Hello Record



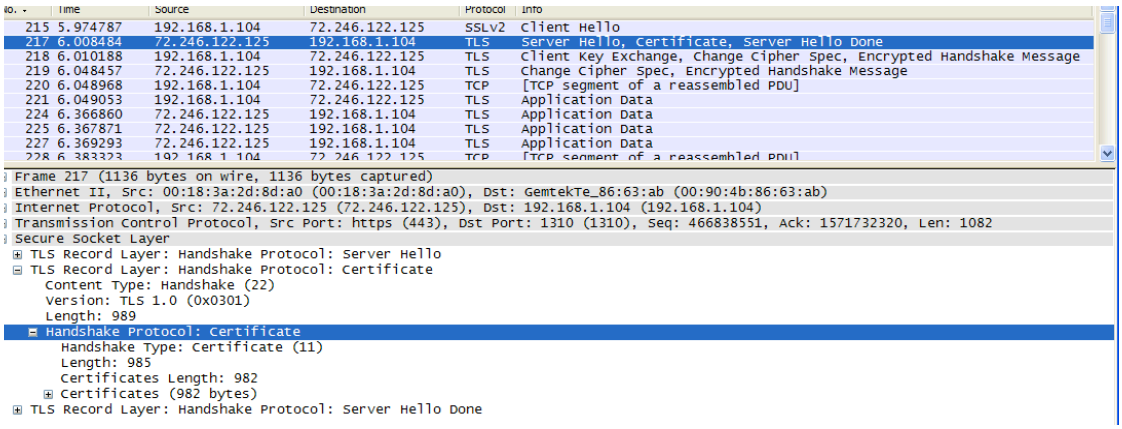
Expanded Server Hello Record

6. Yes, this record specifies a cipher suite. The chosen suite is TLS_RSA_WITH_AES_256_CBC_SHA (0x0035). In other words, RSA (public-key) 256-bit CBC AES (symmetric) and SHA (hash algorithm) are chosen.

7. Yes, this record includes a nonce, as known as Random.bytes, and it is 28 bytes long (as highlighted above). The purpose of the client and server nonces in SSL is to prevent attacker from replaying or reordering records.

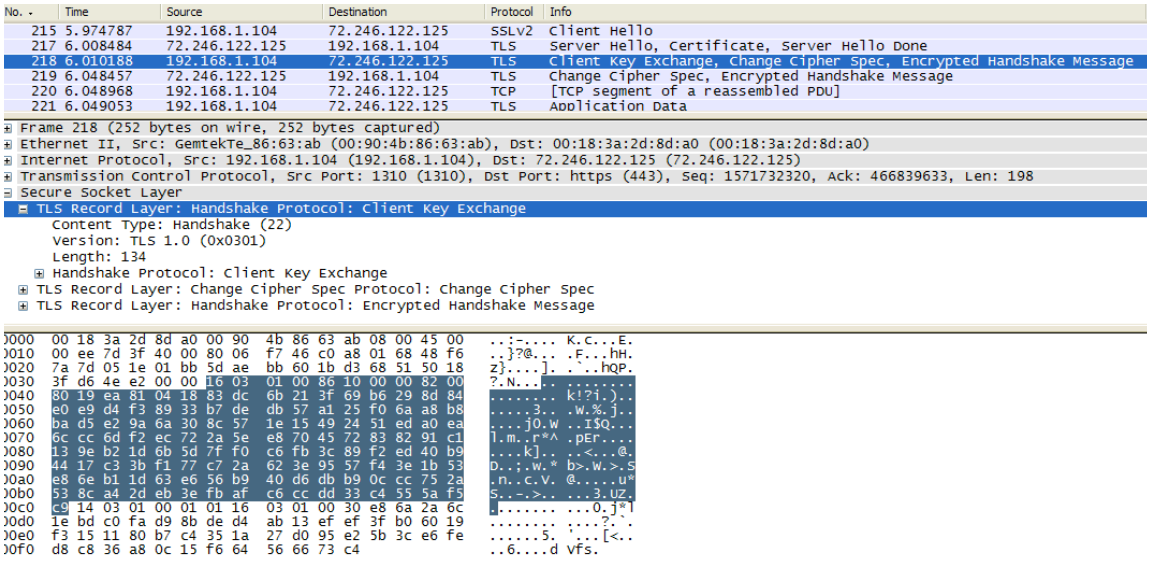
8. Yes, this record includes a Session ID which is 32-bytes long. Its purpose is to allow session resumption, which can significantly reduce the number of time-consuming server handshake to crease a new session ID. In the Client Hello record, a nonzero session ID means that the client to resume its previously established session; and a zero session ID means that the client wishes to establish a new session with the server.

9. Yes, this record contains a certificate. The certificate is 982 bytes long, thus it can fit into a single Ethernet frame.



Expanded Server Hello Record (2)

Client Key Exchange Record

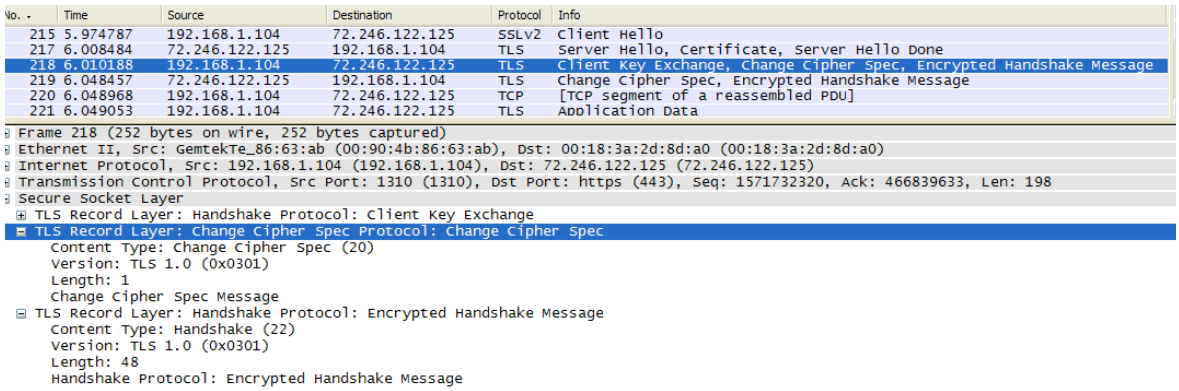


Expanded Client Key Exchange Record

10. Yes, this record contains a pre-master secret (highlighted above). This encrypted pre-master secret is decrypted at the server side and is used to produce a master secret. Then this master secret is used to produces “key block”, which is then sliced and diced into client MAC key, server MAC key, client encryption key, server encryption key, client IV

and serve IV. The secret is encrypted using server's public key. The encrypted secret is 130-byte long.

Change Cipher Spec and Encrypted Handshake Records



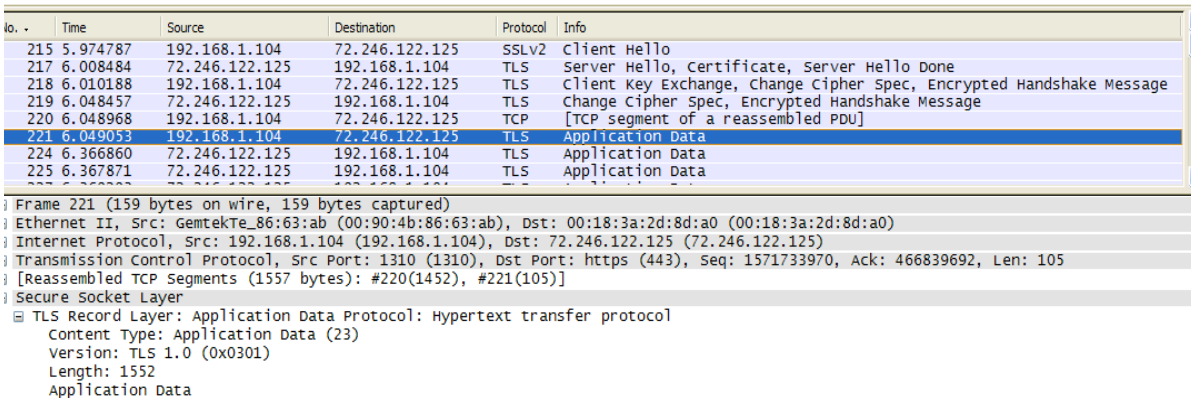
Expanded Change Cipher Spec and Encrypted Handshake Records

11. The purpose of Change Cipher Spec is to indicate change in encryption and authentication algorithms and to update the cipher suite to be used on this connection. This record is only 1 byte long in my trace.

12. The sender of this Encrypted Handshake Records and all handshake messages up to but not including this message are encrypted in record. This information is concatenated and hashed using two hash algorithms, MD5 and SHA. The content of this record is the concatenation of these two hash values. The Encrypted Handshake Record is used to verify that key exchange and authentication processes were successful.

13. Yes, the server also sends its own Change Cipher Spec and Encrypted Handshake records. The only difference is the sender of this record; the sender is now the server while the sender was the client in previous message.

Application Data Records



No.	Time	Source	Destination	Protocol	Info
215	5.974787	192.168.1.104	72.246.122.125	SSLv2	Client Hello
217	6.008484	72.246.122.125	192.168.1.104	TLS	Server Hello, Certificate, Server Hello Done
218	6.010188	192.168.1.104	72.246.122.125	TLS	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
219	6.048457	72.246.122.125	192.168.1.104	TLS	Change Cipher Spec, Encrypted Handshake Message
220	6.048968	192.168.1.104	72.246.122.125	TCP	[TCP segment of a reassembled PDU]
221	6.049053	192.168.1.104	72.246.122.125	TLS	Application Data
224	6.366860	72.246.122.125	192.168.1.104	TLS	Application Data
225	6.367871	72.246.122.125	192.168.1.104	TLS	Application Data

```
Frame 221 (159 bytes on wire, 159 bytes captured)
Ethernet II, Src: GemtekTe_86:63:ab (00:90:4b:86:63:ab), Dst: 00:18:3a:2d:8d:a0 (00:18:3a:2d:8d:a0)
Internet Protocol, Src: 192.168.1.104 (192.168.1.104), Dst: 72.246.122.125 (72.246.122.125)
Transmission Control Protocol, Src Port: 1310 (1310), Dst Port: https (443), Seq: 1571733970, Ack: 466839692, Len: 105
[Reassembled TCP Segments (1557 bytes): #220(1452), #221(105)]
Secure Socket Layer
  TLS Record Layer: Application Data Protocol: Hypertext transfer protocol
      Content Type: Application Data (23)
      Version: TLS 1.0 (0x0301)
      Length: 1552
      Application Data
```

Expanded Application Data Record

14. The application data is encrypted using the specified algorithms in the chosen cipher suite; in my case, RSA (public-key), 256-bit CBC AES (symmetric), and SHA (hash algorithm). Yes, the records containing application data include a MAC; however, Ethereal does not distinguish between the encrypted application data and the MAC.