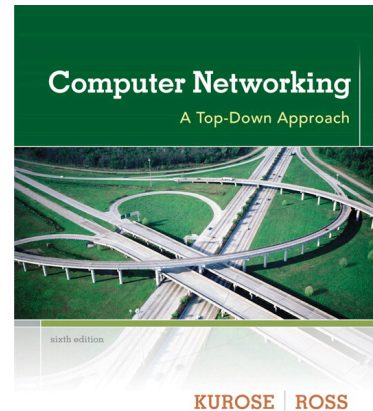


Wireshark Lab: SSL v6.0

Supplement to *Computer Networking: A Top-Down Approach*,
6th 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

© 2005-21012, J.F Kurose and K.W. Ross, All Rights Reserved



A Look at the Captured Trace:

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)

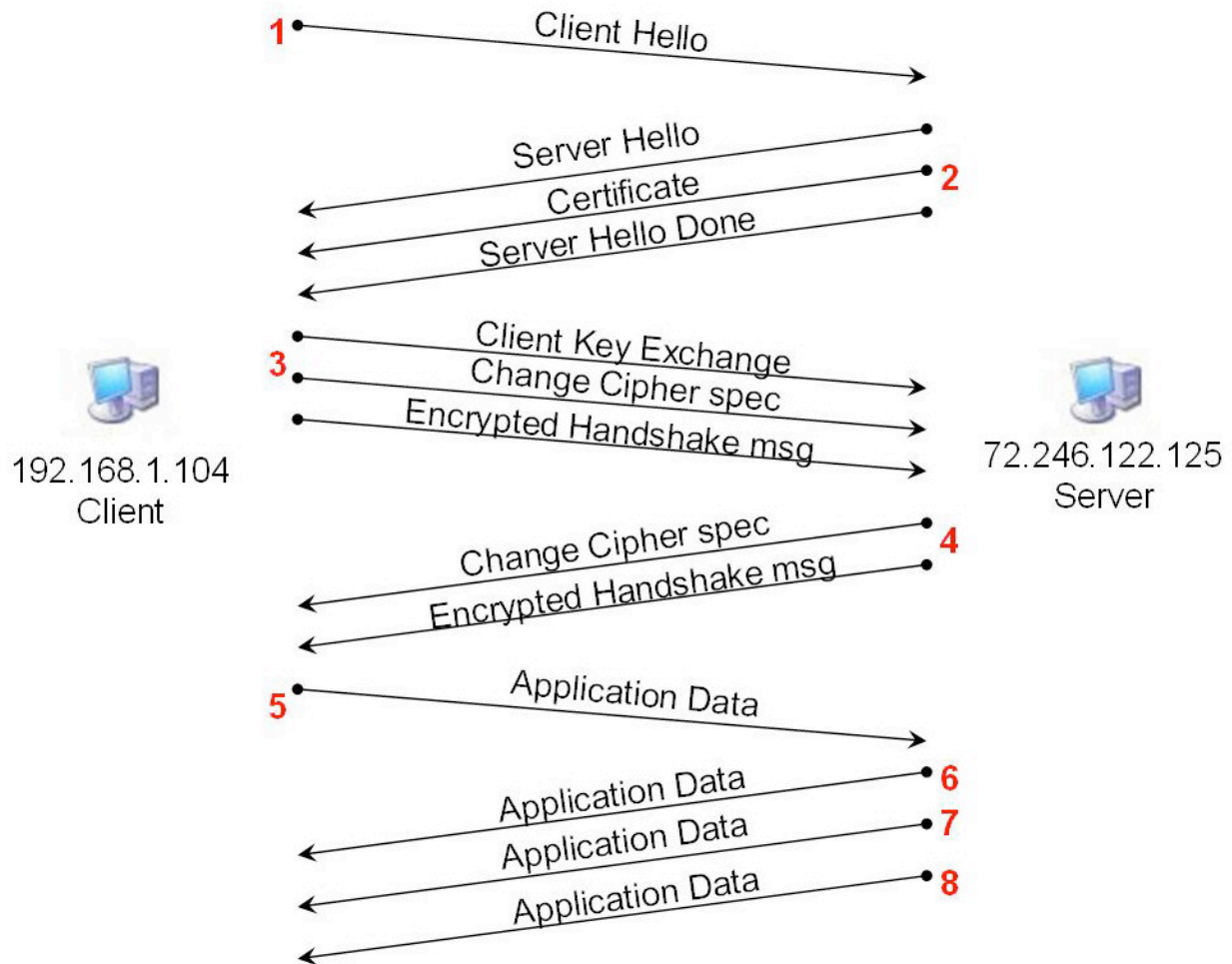
Captured SSL Packets

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

Frame #	Frame	Source	Destination	# of SSL	List of SSL Records
---------	-------	--------	-------------	----------	---------------------

in Ethereal	#			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

- 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	Handshake (22)	TLS 1.0 (0x0301)	74
	Certificate	Handshake (22)	TLS 1.0 (0x0301)	989
	Server Hello Done	Handshake (22)	TLS 1.0 (0x0301)	4
3	Client Key Exchange	Handshake (22)	TLS 1.0 (0x0301)	134
	Change Cipher spec	ChangeCipherSpec(20)	TLS 1.0 (0x0301)	1
	Encrypted Handshake msg	Handshake (22)	TLS 1.0 (0x0301)	48
4	Change Cipher spec	ChangeCipherSpec(20)	TLS 1.0 (0x0301)	1
	Encrypted Handshake msg	Handshake (22)	TLS 1.0 (0x0301)	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

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
# 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) Challenge					
0000	00 18 3a 2d 8d a0 00 90	4b 86 63 ab 08 00 45 00	...K.C...E.		
0010	00 91 7d 3e 40 00 80 06	f7 a4 c0 a8 01 68 48 f6	..>@... ..hH.		
0020	7a 7d 05 1e 01 bb 5d ae	ba f7 1b d3 64 17 50 18	Z}....].d.P.		
0030	44 10 de b5 00 00 80 67	01 03 01 00 4e 00 00 00	D.....gN...		
0040	10 01 00 80 03 00 80 07	00 c0 06 00 40 02 00 80@...		
0050	04 00 80 00 00 39 00 00	38 00 00 35 00 00 33 009.. 8..5..3.		
0060	00 32 00 00 04 00 00 05	00 00 2f 00 00 16 00 00	.2......./.....		
0070	13 00 fe ff 00 00 0a 00	00 15 00 00 12 00 fe fef.e		
0080	00 00 09 00 00 64 00 00	62 00 00 03 00 00 06 c0d..b.....		
0090	74 b5 18 64 d5 ee 04 f9	b5 47 df f3 66 45 97	t..d.... .G..fE.		

Expanded Client Hello Record

- The value of the content type is Handshake (22) because this is handshake message type (as shown above).
- Yes, the Client Hello record contains a challenge and its value in HEX is 0xC074B51864D5EE04F9B547DFF3664597
- 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

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	6.010457	72.246.122.125	192.168.1.104	TLS	Change Cipher Spec, Encrypted Handshake Message
# Frame 217 (1136 bytes on wire, 1136 bytes captured)					
# Ethernet II, Src: 00:18:3a:2d:8d:a0 (00:18:3a:2d:8d:a0), Dst: GemtekTe-86:63:ab (00:90:4b:86:63:ab)					
# Internet Protocol, Src: 72.246.122.125 (72.246.122.125), Dst: 192.168.1.104 (192.168.1.104)					
# Transmission Control Protocol, Src Port: https (443), Dst Port: 1310 (1310), Seq: 466838551, Ack: 1571732320, Len: 1082					
❑ Secure Socket Layer					
❑ TLS Record Layer: Handshake Protocol: Server Hello					
Content Type: Handshake (22)					
Version: TLS 1.0 (0x0301)					
Length: 74					
❑ Handshake Protocol: Server Hello					
Handshake Type: Server Hello (2)					
Length: 70					
Version: TLS 1.0 (0x0301)					
Random.gmt_unix_time: Mar 17, 2007 11:19:31.000000000					
Random.bytes					
Session ID Length: 32					
Session ID (32 bytes)					
Cipher suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)					
Compression Method: null (0)					
0000	00 90 4b 86 63 ab 00 18	3a 2d 8d a0 08 00 45 00	..K.C... :...E.		
0010	04 62 d9 39 40 00 34 06	e3 d8 48 f6 7a 7d c0 a8	.b.9@.4. .H.z}..		
0020	01 68 01 bb 05 1e 1b d3	64 17 5d ae bb 60 50 18	.h..... d.]... P.		
0030	16 d0 72 7b 00 00 16 03	01 00 4a 02 00 00 46 03	..P[.....J...F.		
0040	01 45 fc 15 13 ec 6f 7f	06 7f fe b7 0f 96 be 11	.E...o.		
0050	04 cf 5b 98 68 1b 4c 2f	c7 a8 e4 66 cd 19 08 8c	..[.h.L/ ...f....		
0060	51 20 24 fd 4a 82 3d 6d	d9 a3 ed 08 75 a2 ff ac	q \$.J.=mu...		

Expanded Server Hello Record

- 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.
- 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 create 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.

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	6.383273	192.168.1.104	72.246.122.125	TCP	[TCP segment of a reassembled PDU]

Frame 217 (1136 bytes on wire, 1136 bytes captured)

Ethernet II, Src: 00:18:3a:2d:8d:a0 (00:18:3a:2d:8d:a0), Dst: GemtekTe_86:63:ab (00:90:4b:86:63:ab)

Internet Protocol, Src: 72.246.122.125 (72.246.122.125), Dst: 192.168.1.104 (192.168.1.104)

Transmission Control Protocol, Src Port: https (443), Dst Port: 1310 (1310), Seq: 466838551, Ack: 1571732320, Len: 1082

Secure Socket Layer

- TLS Record Layer: Handshake Protocol: Server Hello
- TLS Record Layer: Handshake Protocol: Certificate
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 989
- Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 985
 - Certificates Length: 982
 - Certificates (982 bytes)
- TLS Record Layer: Handshake Protocol: Server Hello Done

Expanded Server Hello Record (2)

Client Key Exchange Record

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

Frame 218 (252 bytes on wire, 252 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: 1571732320, Ack: 466839633, Len: 198

Secure Socket Layer

- TLS Record Layer: Handshake Protocol: Client Key Exchange
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 134
- Handshake Protocol: Client Key Exchange
- TLS Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
- TLS Record Layer: Handshake Protocol: Encrypted Handshake Message

```

0000 00 18 3a 2d 8d a0 00 90 4b 86 63 ab 08 00 45 00  ..-... K.C...E.
0010 00 ee 7d 3f 40 00 80 06 f7 46 c0 a8 01 68 48 f6  ..}?....F...hh.
0020 7a 7d 05 1e 01 bb 5d ae bb 60 1b d3 68 51 50 18  z}....}. ...hQP.
0030 3f d6 4e e2 00 00 10 03 01 00 38 10 00 00 82 00  ?N....
0040 80 19 ea 81 04 18 b3 dc 6b 21 3f 69 b6 29 8d b4  .....k[?].
0050 e0 e9 d4 f3 89 33 b7 de db 57 a1 25 f0 6a a8 b8  .....3...w.%}.
0060 ba d5 e2 9a 6a 30 8c 57 1e 15 49 24 51 ed a0 ea  ....j0.w...ISQ..
0070 6c cc 6d f2 ec 72 2a 5e 08 70 45 72 83 82 91 c1  l.m.r*^..PER....
0080 13 9e b2 1d 6b 5d 7f f0 c6 fb 3c 89 f2 ed 40 b9  ....k]...<...@.
0090 44 17 c3 3b f1 77 c7 2a 62 3e 95 57 f4 3e 1b 53  D.;.w.* b>.w>.S
00a0 e8 6e b1 1d 63 e6 56 b9 40 d6 db b9 0c cc 75 2a  .n..c.v. @....u*
00b0 53 8c ad 2d ab 3e fb af c6 cc dd 33 c4 55 5a f5  S...>...3..UZ.
00c0 c3 14 03 01 00 01 01 16 03 01 00 30 e8 6a 2a 6c  .....0..j?
00d0 1e bd c0 fa d9 8b de d4 ab 13 ef ef 3f b0 60 19  .....?..?..
00e0 f3 15 11 80 b7 c4 35 1a 27 d0 95 e2 5b 3c e6 fe  ....S....[<...
00f0 d8 c8 36 a8 0c 15 f6 64 56 66 73 c4                ..6....d vfs.

```

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 produce “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

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

Frame 218 (252 bytes on wire, 252 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: 1571732320, Ack: 466839633, Len: 198
Secure Socket Layer
TLS Record Layer: Handshake Protocol: Client Key Exchange
TLS Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
Content Type: Change Cipher Spec (20)
Version: TLS 1.0 (0x0301)
Length: 1
Change Cipher Spec Message
TLS Record Layer: Handshake Protocol: Encrypted Handshake Message
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 48
Handshake Protocol: Encrypted Handshake Message

Expanded Change Cipher Spec and Encrypted Handshake Records

- 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.
- 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.
- 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

- 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.