TLS (SSL)

TLS – Transport Layer Security

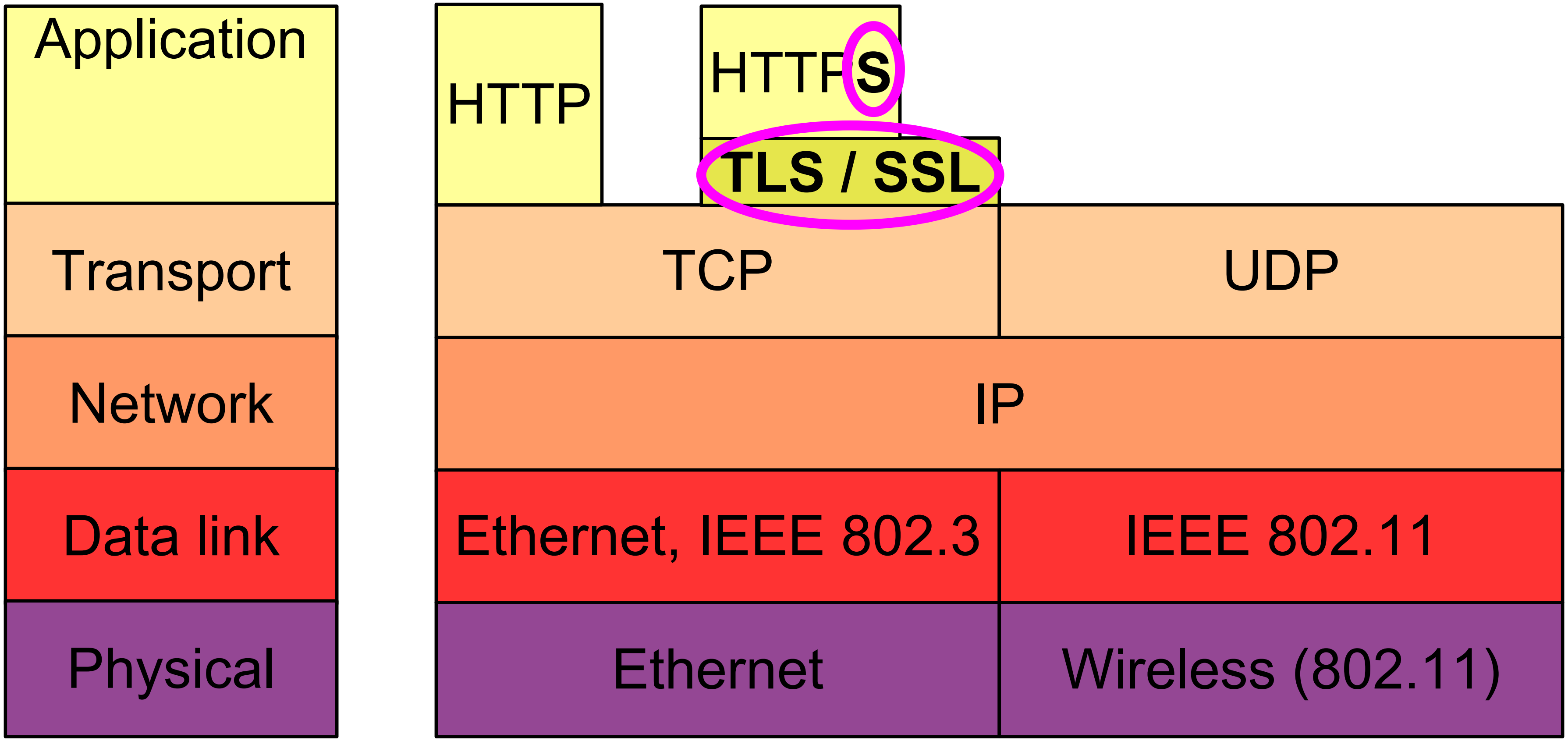
- **Specification**
  - **RFC 5246**, The Transport Layer Security (TLS) Protocol - Version 1.2
  - ftp://ftp.rfc-editor.org/in-notes/rfc5246.txt

- **JAVA Implementation**
  - Java Secure Socket Extension (JSSE)
  - JSSERefGuide.html

TLS – Layers

- **TLS Record Protocol for Connection security**
  - **Privacy:** Symmetric cryptography is used for data encryption. The keys for this symmetric encryption are generated uniquely for each connection and are based on a secret negotiated by another protocol (such as the TLS Handshake Protocol).
  - **Reliability:** Sessage transport includes a message integrity check using a keyed MAC.
- **TLS Handshake Protocol**
  - Authentication of peer's identity
  - Negotiation of shared secret

Security at Layer 4++



TLS Record Layer

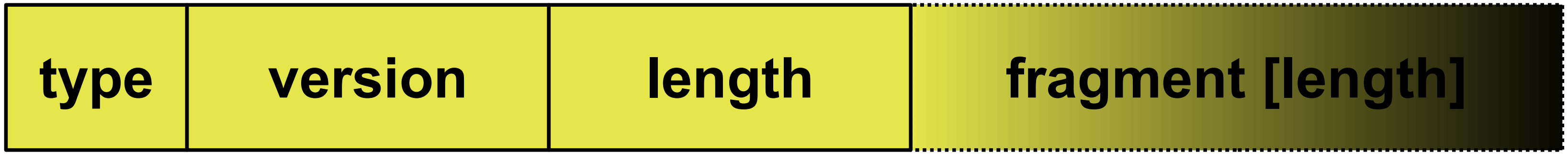
- **Fragmentation**
  - **TLSPlaintext** records of at most 2^{14} bytes length

type	**version**	**length**	**fragment [length]**

- **Record Compression / Decompression**
  - Optional

- **Record Payload Protection**

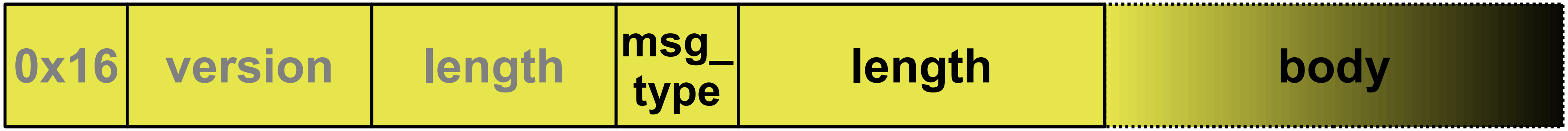
TLS Record Layer – types and versions



0x14	*change_cipher_spec*
0x15	*alert*
0x16	*handshake*
0x17	*application_data*

0x03	0x00	*SSL 3.0*
0x03	0x01	*TLS 1.0*
0x03	0x02	*TLS 1.1*

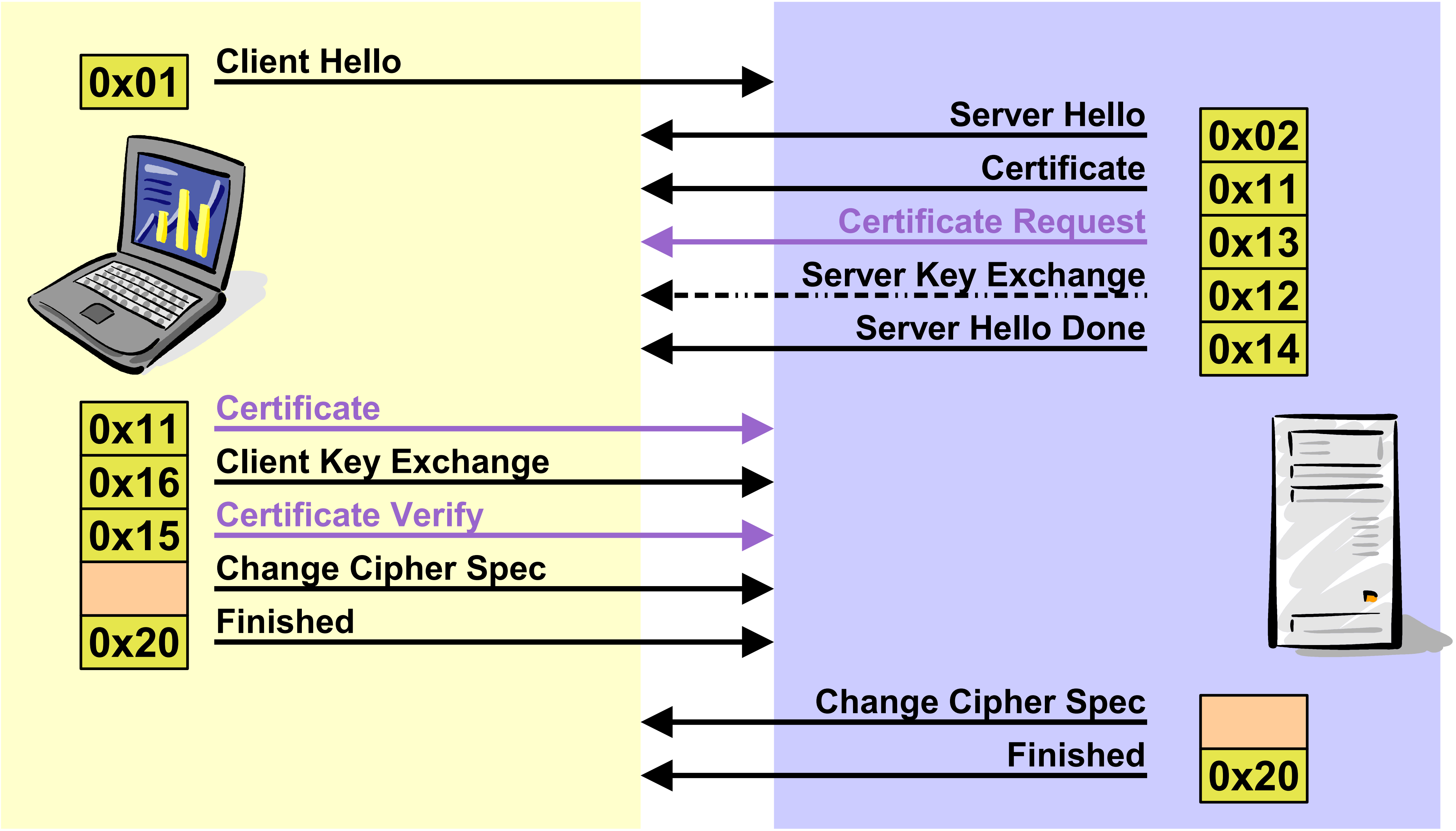
TLS Handshake Protocol



0x16	version	length	msg_type	length	body

0x00	*hello_request*
0x01	*client_hello*
0x02	*server_hello*
0x11	*certificate*
0x12	*server_key_exchange*
0x13	*certificate_request*
0x14	*server_hello_done*
0x15	*certificate_verify*
0x16	*client_key_exchange*
0x20	*finished*

TLS Handshake Protocol



0x01 Client Hello

Server Hello 0x02

Certificate 0x11

Certificate Request 0x13

Server Key Exchange 0x12

Server Hello Done 0x14

0x11 Certificate

0x16 Client Key Exchange

0x15 Certificate Verify

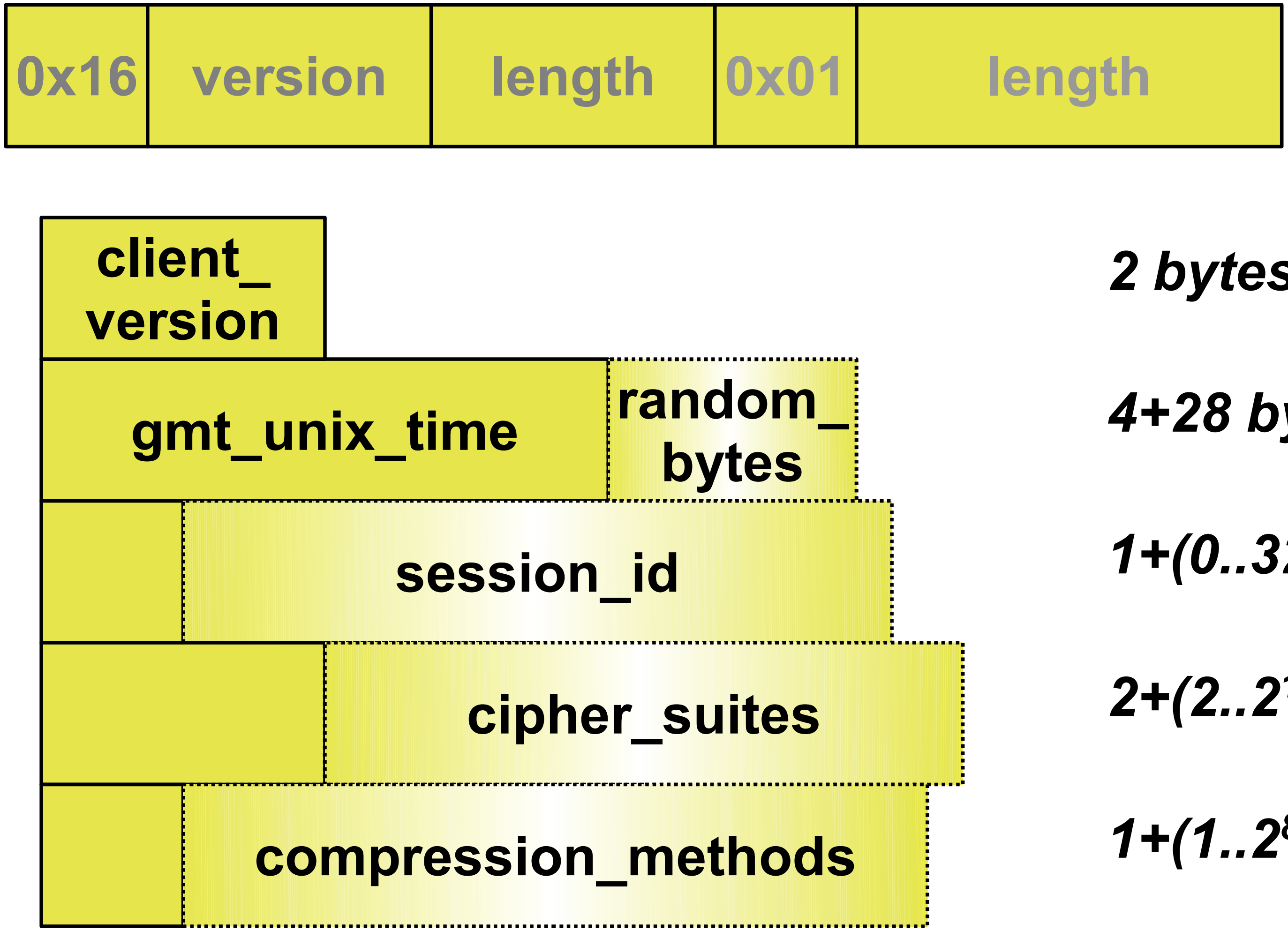
Change Cipher Spec

0x20 Finished

Change Cipher Spec

Finished 0x20

TLS Handshake – Client Hello



0x16 | version | length | 0x01 | length

client_version — 2 bytes

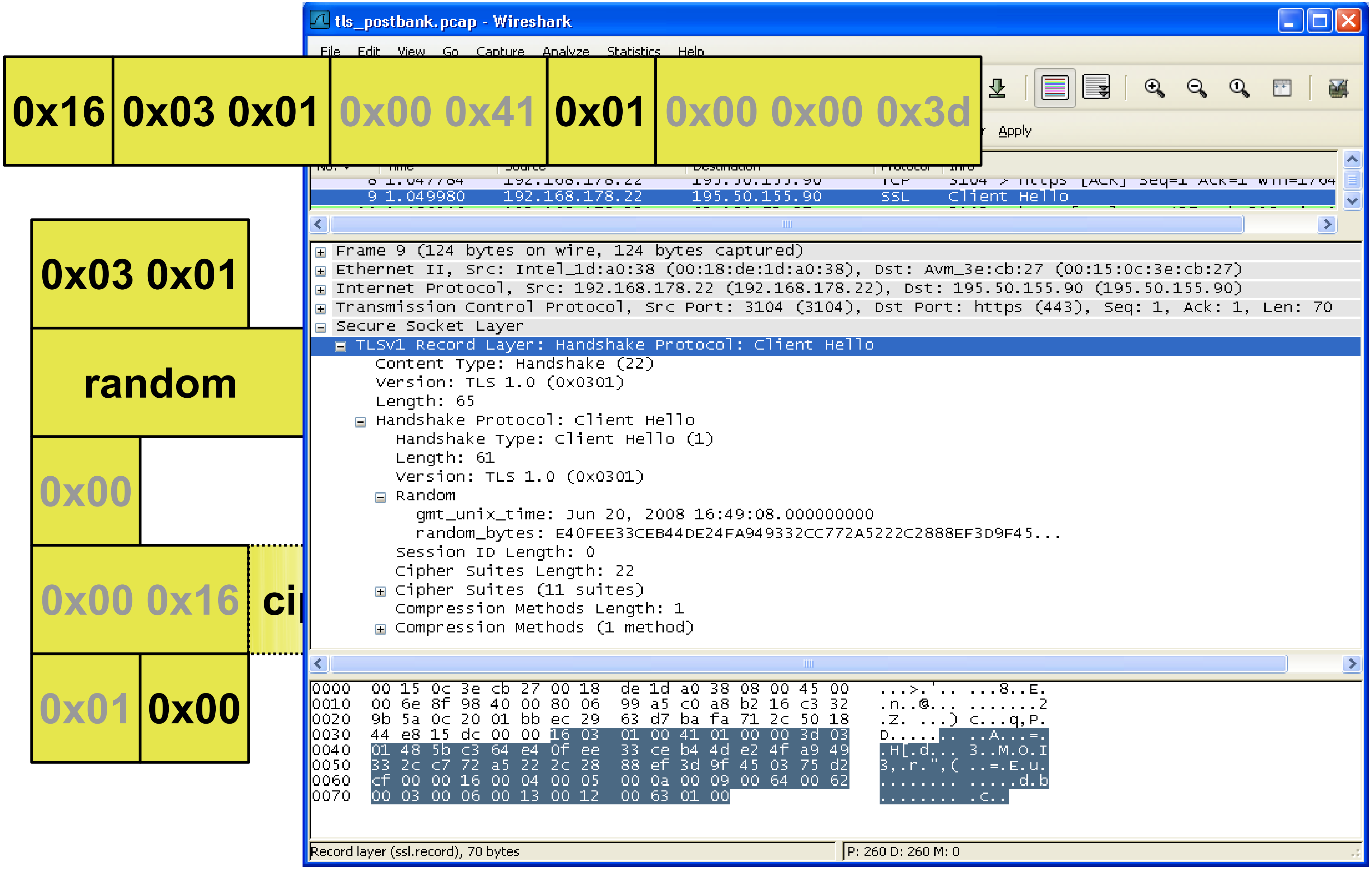
gmt_unix_time, random_bytes — 4+28 bytes

session_id — 1+(0..32) bytes

cipher_suites — 2+(2..2^{16}-1) bytes

compression_methods — 1+(1..2^{8}-1) bytes

TLS Handshake – Client Hello



0x16 | 0x03 0x01 | 0x00 0x41 | 0x01 | 0x00 0x00 0x3d

0x03 0x01

random

0x00

0x00 0x16 | ci

0x01 | 0x00

tls_postbank.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Apply
No. Time Source Destination Protocol Info

```
  8 1.047784  192.168.178.22  195.50.155.90  TCP  3104 > https [ACK] Seq=1 Ack=1 Win=1704
  9 1.049980  192.168.178.22  195.50.155.90  SSL  Client Hello
```

```
⊞ Frame 9 (124 bytes on wire, 124 bytes captured)
⊞ Ethernet II, Src: Intel_1d:a0:38 (00:18:de:1d:a0:38), Dst: Avm_3e:cb:27 (00:15:0c:3e:cb:27)
⊞ Internet Protocol, Src: 192.168.178.22 (192.168.178.22), Dst: 195.50.155.90 (195.50.155.90)
⊞ Transmission Control Protocol, Src Port: 3104 (3104), Dst Port: https (443), Seq: 1, Ack: 1, Len: 70
⊟ Secure Socket Layer
  ⊟ TLSv1 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 65
    ⊟ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 61
        Version: TLS 1.0 (0x0301)
      ⊟ Random
          gmt_unix_time: Jun 20, 2008 16:49:08.000000000
          random_bytes: E40FEE33CEB44DE24FA949332CC772A5222C2888EF3D9F45...
        Session ID Length: 0
        Cipher Suites Length: 22
      ⊞ Cipher Suites (11 suites)
        Compression Methods Length: 1
      ⊞ Compression Methods (1 method)
```

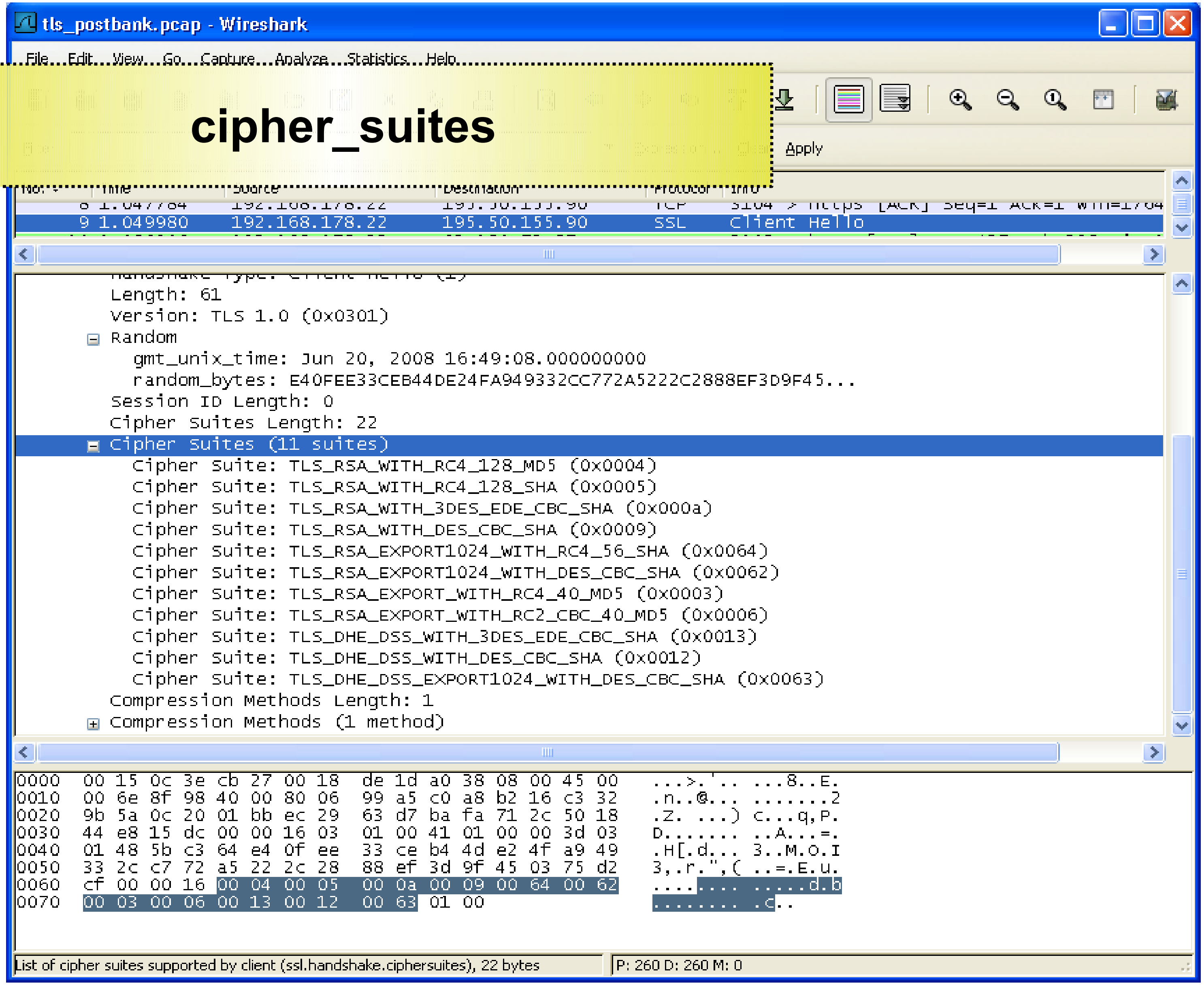
```
0000   00 15 0c 3e cb 27 00 18  de 1d a0 38 08 00 45 00   ...>.'.. ...8..E.
0010   00 6e 8f 98 40 00 80 06  99 a5 c0 a8 b2 16 c3 32   .n..@... .......2
0020   9b 5a 0c 20 01 bb ec 29  63 d7 ba fa 71 2c 50 18   .Z. ...) c...q,P.
0030   44 e8 15 dc 00 00 16 03  01 00 41 01 00 00 3d 03   D....... ..A...=.
0040   01 48 5b c3 64 e4 0f ee  33 ce b4 4d e2 4f a9 49   .H[.d... 3..M.O.I
0050   33 2c c7 72 a5 22 2c 28  88 ef 3d 9f 45 03 75 d2   3,.r.",( ..=.E.u.
0060   cf 00 00 16 00 04 00 05  00 0a 00 09 00 64 00 62   ........ .....d.b
0070   00 03 00 06 00 13 00 12  00 63 01 00               ........ .c..
```

Record layer (ssl.record), 70 bytes | P: 260 D: 260 M: 0

TLS Handshake – Client Hello – Cipher Suites

0x00 0x16

cipher_suites


tls_postbank.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Apply

```
No. -  Time         Source           Destination      Protocol  Info
  8 1.047784     192.168.178.22   195.50.155.90    TCP       3104 > https [ACK] Seq=1 Ack=1 Win=17664
  9 1.049980     192.168.178.22   195.50.155.90    SSL       Client Hello
```

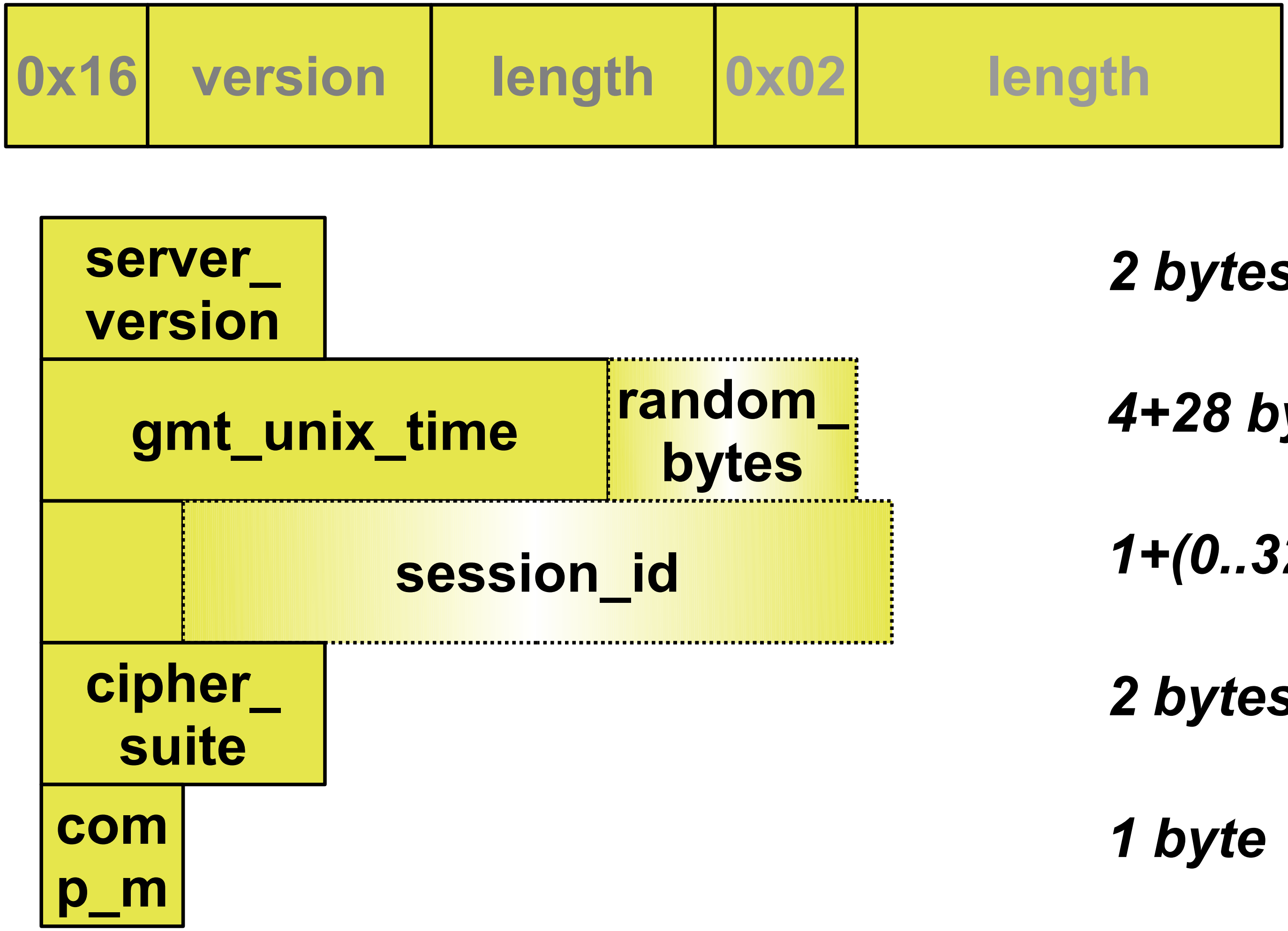
```
    Handshake Type: Client Hello (1)
    Length: 61
    Version: TLS 1.0 (0x0301)
  ⊟ Random
      gmt_unix_time: Jun 20, 2008 16:49:08.000000000
      random_bytes: E40FEE33CEB44DE24FA949332CC772A5222C2888EF3D9F45...
    Session ID Length: 0
    Cipher Suites Length: 22
  ⊟ Cipher Suites (11 suites)
      Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
      Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
      Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
      Cipher Suite: TLS_RSA_WITH_DES_CBC_SHA (0x0009)
      Cipher Suite: TLS_RSA_EXPORT1024_WITH_RC4_56_SHA (0x0064)
      Cipher Suite: TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA (0x0062)
      Cipher Suite: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x0003)
      Cipher Suite: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x0006)
      Cipher Suite: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
      Cipher Suite: TLS_DHE_DSS_WITH_DES_CBC_SHA (0x0012)
      Cipher Suite: TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA (0x0063)
    Compression Methods Length: 1
  ⊞ Compression Methods (1 method)
```

```
0000  00 15 0c 3e cb 27 00 18  de 1d a0 38 08 00 45 00   ...>.'.. ...8..E.
0010  00 6e 8f 98 40 00 80 06  99 a5 c0 a8 b2 16 c3 32   .n..@... .......2
0020  9b 5a 0c 20 01 bb ec 29  63 d7 ba fa 71 2c 50 18   .Z. ...) c...q,P.
0030  44 e8 15 dc 00 00 16 03  01 00 41 01 00 00 3d 03   D....... ..A...=.
0040  01 48 5b c3 64 e4 0f ee  33 ce b4 4d e2 4f a9 49   .H[.d... 3..M.O.I
0050  33 2c c7 72 a5 22 2c 28  88 ef 3d 9f 45 03 75 d2   3,.r.",( ..=.E.u.
0060  cf 00 00 16 00 04 00 05  00 0a 00 09 00 64 00 62   ........ ......d.b
0070  00 03 00 06 00 13 00 12  00 63 01 00              ........ .c..
```

List of cipher suites supported by client (ssl.handshake.ciphersuites), 22 bytes

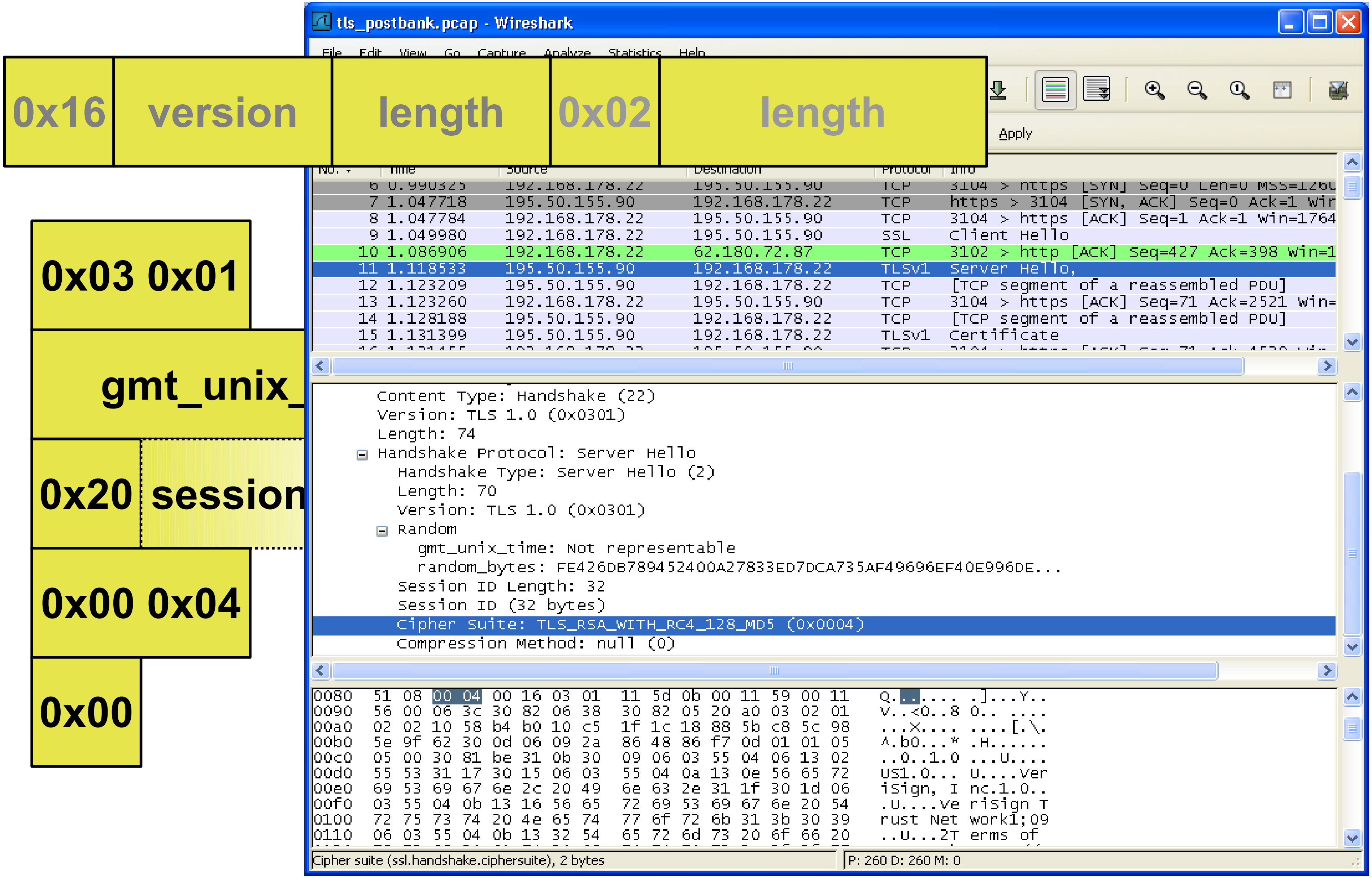
P: 260 D: 260 M: 0

TLS Handshake – Server Hello



0x16 | version | length | 0x02 | length	
server_ version	2 bytes
gmt_unix_time | random_ bytes	4+28 bytes
| session_id	1+(0..32) bytes
cipher_ suite	2 bytes
com p_m	1 byte

TLS Handshake – Server Hello


0x16
version
length
0x02
length
0x03 0x01
gmt_unix_
0x20
session
0x00 0x04
0x00
tls_postbank.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Apply

```
No. -  Time      Source           Destination      Protocol  Info
  6 0.990325  192.168.178.22  195.50.155.90   TCP      3104 > https [SYN] Seq=0 Len=0 MSS=1260
  7 1.047718  195.50.155.90   192.168.178.22  TCP      https > 3104 [SYN, ACK] Seq=0 Ack=1 Win
  8 1.047784  192.168.178.22  195.50.155.90   TCP      3104 > https [ACK] Seq=1 Ack=1 Win=1764
  9 1.049980  192.168.178.22  195.50.155.90   SSL      Client Hello
 10 1.086906  192.168.178.22  62.180.72.87    TCP      3102 > http [ACK] Seq=427 Ack=398 Win=1
 11 1.118533  195.50.155.90   192.168.178.22  TLSv1    Server Hello,
 12 1.123209  195.50.155.90   192.168.178.22  TCP      [TCP segment of a reassembled PDU]
 13 1.123260  192.168.178.22  195.50.155.90   TCP      3104 > https [ACK] Seq=71 Ack=2521 Win=
 14 1.128188  195.50.155.90   192.168.178.22  TCP      [TCP segment of a reassembled PDU]
 15 1.131399  195.50.155.90   192.168.178.22  TLSv1    Certificate
```

```
    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: Not representable
        random_bytes: FE426DB789452400A27833ED7DCA735AF49696EF40E996DE...
      Session ID Length: 32
      Session ID (32 bytes)
      Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
      Compression Method: null (0)
```

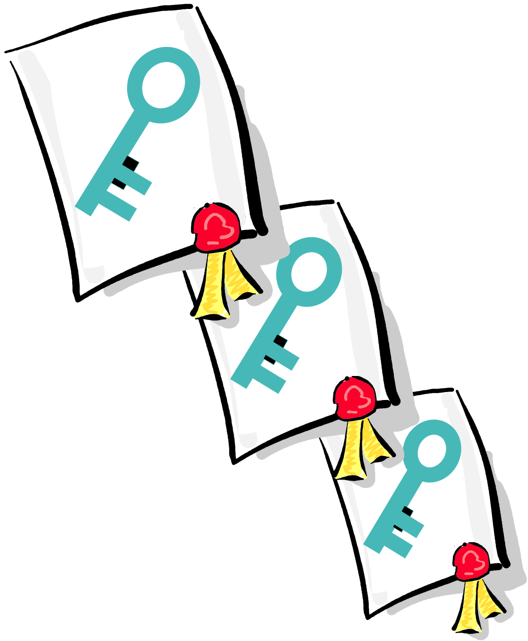
```
0080  51 08 00 04 00 16 03 01  11 5d 0b 00 11 59 00 11   Q....... .]...Y..
0090  56 00 06 3c 30 82 06 38  30 82 05 20 a0 03 02 01   V..<0..8 0.. ....
00a0  02 02 10 58 b4 b0 10 c5  1f 1c 18 88 5b c8 5c 98   ...X.... ....[.\.
00b0  5e 9f 62 30 0d 06 09 2a  86 48 86 f7 0d 01 01 05   ^.b0...* .H......
00c0  05 00 30 81 be 31 0b 30  09 06 03 55 04 06 13 02   ..0..1.0 ...U....
00d0  55 53 31 17 30 15 06 03  55 04 0a 13 0e 56 65 72   US1.0... U....Ver
00e0  69 53 69 67 6e 2c 20 49  6e 63 2e 31 1f 30 1d 06   iSign, I nc.1.0..
00f0  03 55 04 0b 13 16 56 65  72 69 53 69 67 6e 20 54   .U....Ve riSign T
0100  72 75 73 74 20 4e 65 74  77 6f 72 6b 31 3b 30 39   rust Net work1;09
0110  06 03 55 04 0b 13 32 54  65 72 6d 73 20 6f 66 20   ..U...2T erms of
```

Cipher suite (ssl.handshake.ciphersuite), 2 bytes   P: 260 D: 260 M: 0

TLS Handshake – Certificate

0x16	version	length	0x0B	length

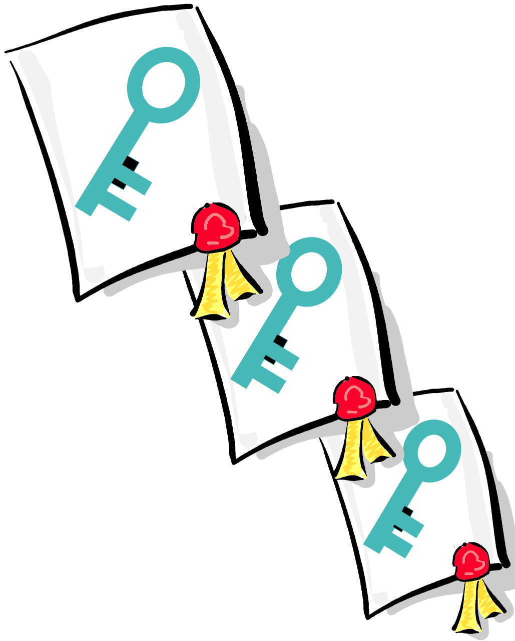
certificate_list

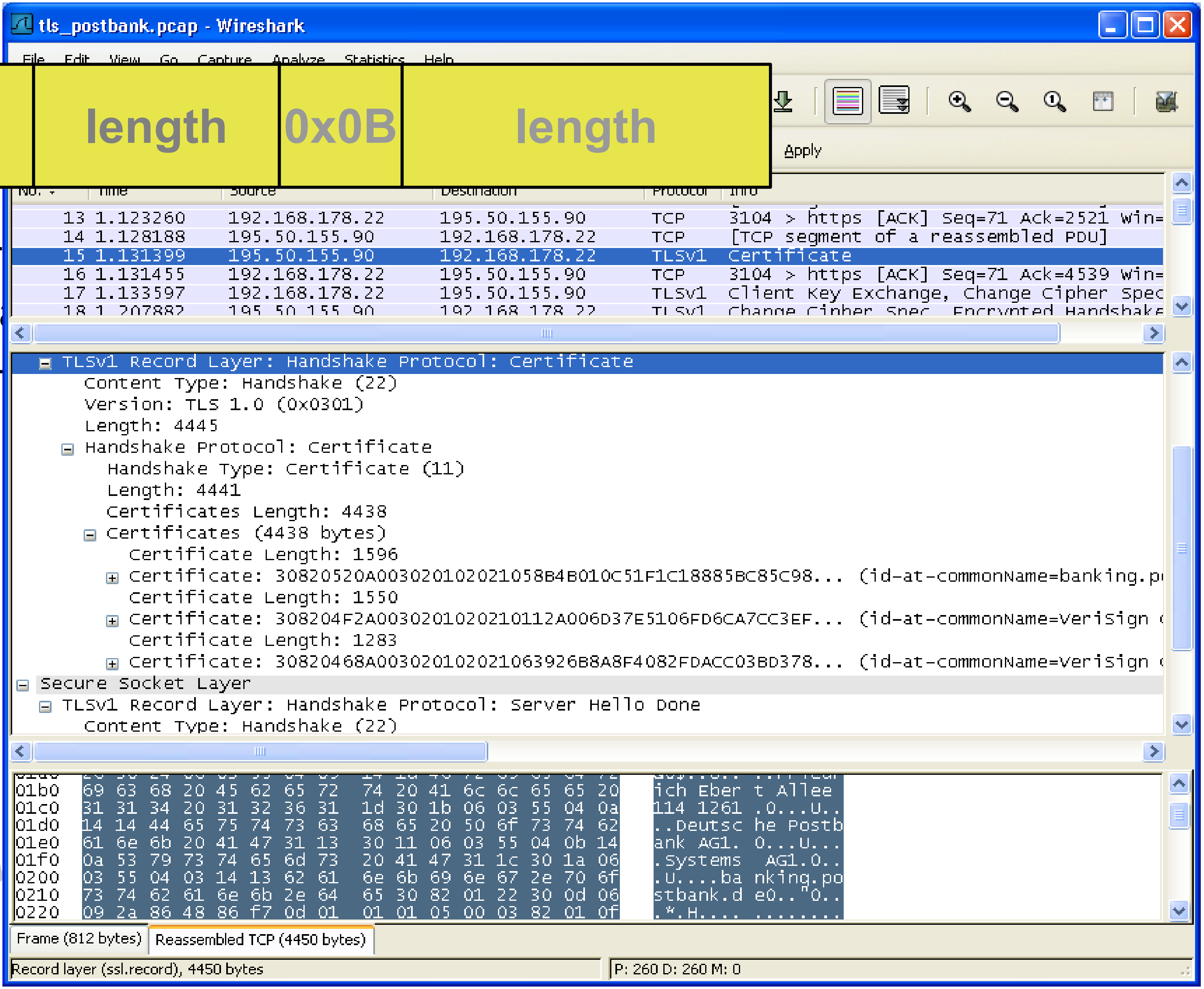


TLS Handshake – Certificate

0x16	version	length	0x0B	length

certifica




tls_postbank.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Apply

```
No. -  Time      Source           Destination      Protocol  Info
 13 1.123260   192.168.178.22   195.50.155.90    TCP       3104 > https [ACK] Seq=71 Ack=2521 Win=
 14 1.128188   195.50.155.90    192.168.178.22   TCP       [TCP segment of a reassembled PDU]
 15 1.131399   195.50.155.90    192.168.178.22   TLSv1     Certificate
 16 1.131455   192.168.178.22   195.50.155.90    TCP       3104 > https [ACK] Seq=71 Ack=4539 Win=
 17 1.133597   192.168.178.22   195.50.155.90    TLSv1     Client Key Exchange, Change Cipher Spec
 18 1.207882   195.50.155.90    192.168.178.22   TLSv1     Change Cipher Spec, Encrypted Handshake
```

```
⊟ TLSv1 Record Layer: Handshake Protocol: Certificate
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 4445
  ⊟ Handshake Protocol: Certificate
      Handshake Type: Certificate (11)
      Length: 4441
      Certificates Length: 4438
    ⊟ Certificates (4438 bytes)
        Certificate Length: 1596
      ⊞ Certificate: 30820520A003020102021058B4B010C51F1C18885BC85C98... (id-at-commonName=banking.po
        Certificate Length: 1550
      ⊞ Certificate: 308204F2A003020102021011 2A006D37E5106FD6CA7CC3EF... (id-at-commonName=VeriSign C
        Certificate Length: 1283
      ⊞ Certificate: 30820468A003020102021063926B8A8F4082FDACC03BD378... (id-at-commonName=VeriSign C
⊟ Secure Socket Layer
  ⊟ TLSv1 Record Layer: Handshake Protocol: Server Hello Done
      Content Type: Handshake (22)
```

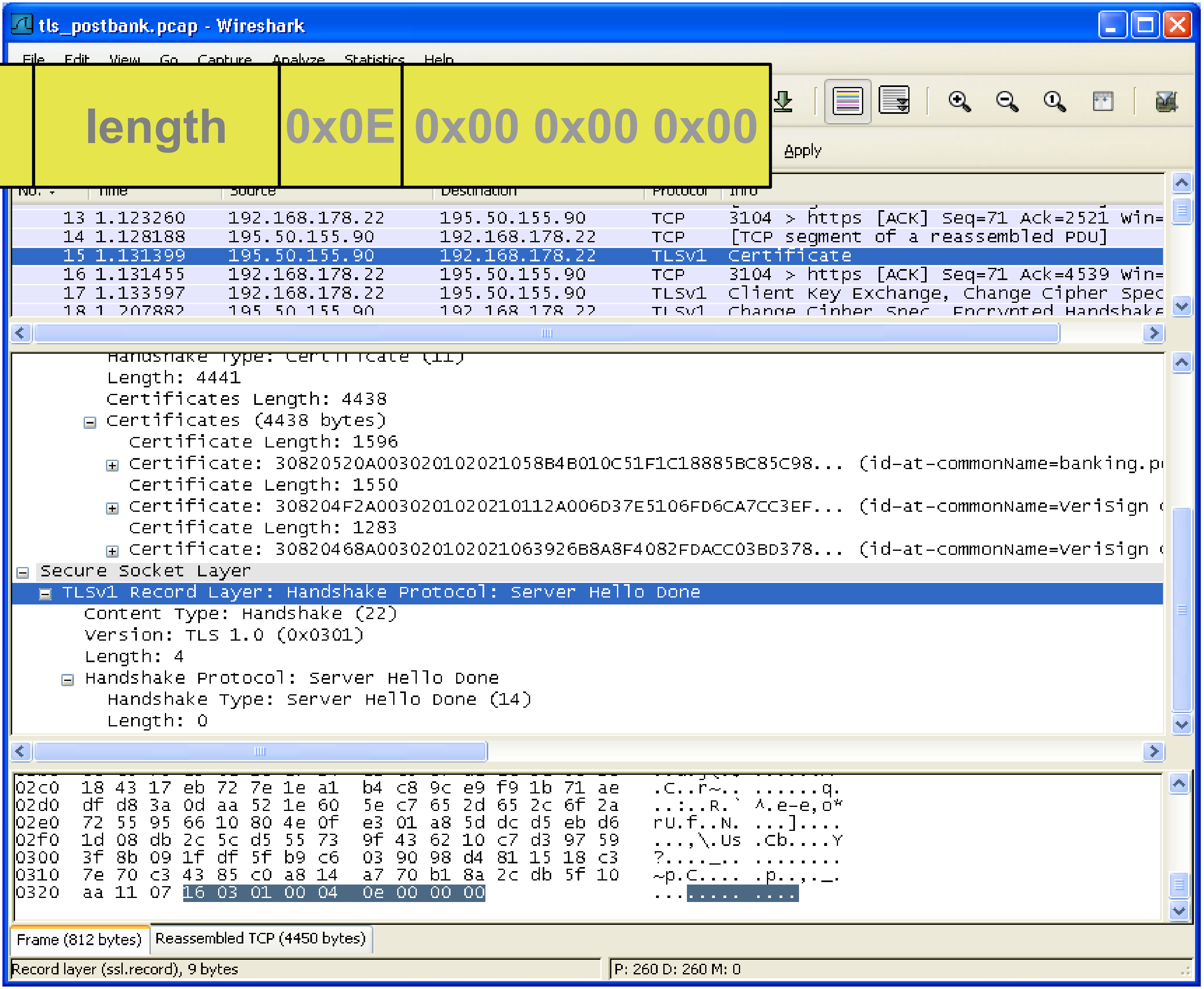
```
01b0  69 63 68 20 45 62 65 72  74 20 41 6c 6c 65 65 20   ich Eber t Allee
01c0  31 31 34 20 31 32 36 31  1d 30 1b 06 03 55 04 0a   114 1261 .0...U..
01d0  14 14 44 65 75 74 73 63  68 65 20 50 6f 73 74 62   ..Deutsc he Postb
01e0  61 6e 6b 20 41 47 31 13  30 11 06 03 55 04 0b 14   ank AG1. 0...U...
01f0  0a 53 79 73 74 65 6d 73  20 41 47 31 1c 30 1a 06   .Systems  AG1.0..
0200  03 55 04 03 14 13 62 61  6e 6b 69 6e 67 2e 70 6f   .U....ba nking.po
0210  73 74 62 61 6e 6b 2e 64  65 30 82 01 22 30 0d 06   stbank.d e0.."0..
0220  09 2a 86 48 86 f7 0d 01  01 01 05 00 03 82 01 0f   .*.H.... ........
```

Frame (812 bytes) | Reassembled TCP (4450 bytes)

Record layer (ssl.record), 4450 bytes | P: 260 D: 260 M: 0

TLS Handshake – Server Hello Done

0x16	version	length	0x0E	0x00 0x00 0x00


tls_postbank.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Apply

```
No.  Time      Source           Destination      Protocol Info
  13 1.123260  192.168.178.22   195.50.155.90    TCP      3104 > https [ACK] Seq=71 Ack=2521 Win=
  14 1.128188  195.50.155.90    192.168.178.22   TCP      [TCP segment of a reassembled PDU]
  15 1.131399  195.50.155.90    192.168.178.22   TLSv1    Certificate
  16 1.131455  192.168.178.22   195.50.155.90    TCP      3104 > https [ACK] Seq=71 Ack=4539 Win=
  17 1.133597  192.168.178.22   195.50.155.90    TLSv1    Client Key Exchange, Change Cipher Spec
  18 1.207882  195.50.155.90    192.168.178.22   TLSv1    Change Cipher Spec, Encrypted Handshake
```

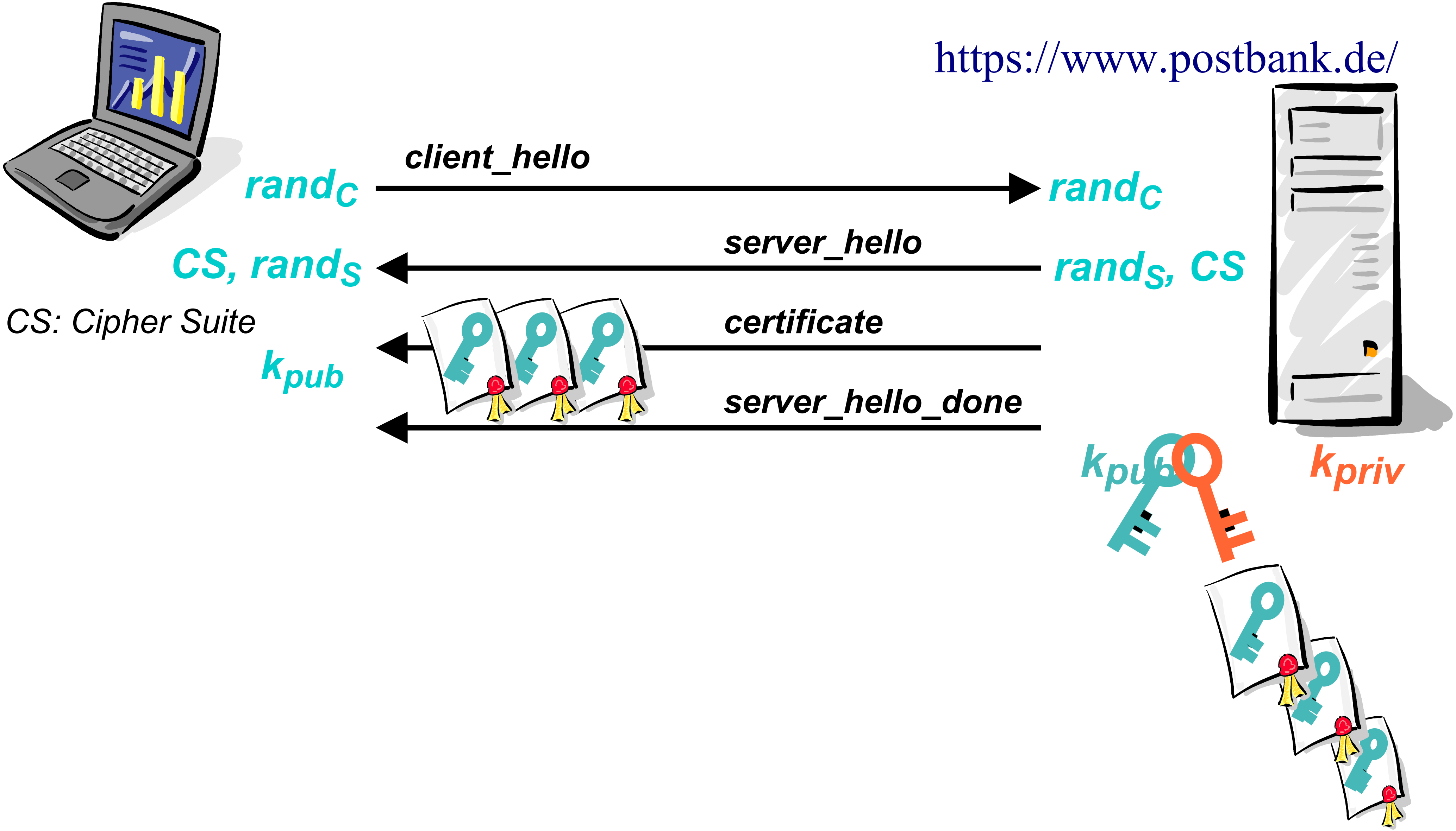
```
        Handshake Type: Certificate (11)
        Length: 4441
        Certificates Length: 4438
      ⊟ Certificates (4438 bytes)
          Certificate Length: 1596
        ⊞ Certificate: 30820520A003020102021058B4B010C51F1C18885BC85C98... (id-at-commonName=banking.p
          Certificate Length: 1550
        ⊞ Certificate: 308204F2A0030201020210112A006D37E5106FD6CA7CC3EF... (id-at-commonName=VeriSign
          Certificate Length: 1283
        ⊞ Certificate: 30820468A00302010202106392 6B8A8F4082FDACC03BD378... (id-at-commonName=VeriSign
⊟ Secure Socket Layer
  ⊟ TLSv1 Record Layer: Handshake Protocol: Server Hello Done
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 4
    ⊟ Handshake Protocol: Server Hello Done
        Handshake Type: Server Hello Done (14)
        Length: 0
```

```
02c0  18 43 17 eb 72 7e 1e a1  b4 c8 9c e9 f9 1b 71 ae   .C..r~.. ......q.
02d0  df d8 3a 0d aa 52 1e 60  5e c7 65 2d 65 2c 6f 2a   ..:..R.` ^.e-e,o*
02e0  72 55 95 66 10 80 4e 0f  e3 01 a8 5d dc d5 eb d6   rU.f..N. ...]....
02f0  1d 08 db 2c 5c d5 55 73  9f 43 62 10 c7 d3 97 59   ...,\.Us .Cb....Y
0300  3f 8b 09 1f df 5f b9 c6  03 90 98 d4 81 15 18 c3   ?...._.. ........
0310  7e 70 c3 43 85 c0 a8 14  a7 70 b1 8a 2c db 5f 10   ~p.C.... .p..,._.
0320  aa 11 07 16 03 01 00 04  0e 00 00 00               ........ ....
```

Frame (812 bytes) | Reassembled TCP (4450 bytes)

Record layer (ssl.record), 9 bytes | P: 260 D: 260 M: 0

TLS – Handshake



https://www.postbank.de/

client_hello

$rand_C$ → $rand_C$

server_hello

$CS, rand_S$ ← $rand_S, CS$

certificate

server_hello_done

CS: Cipher Suite

k_{pub}

k_{pub} k_{priv}

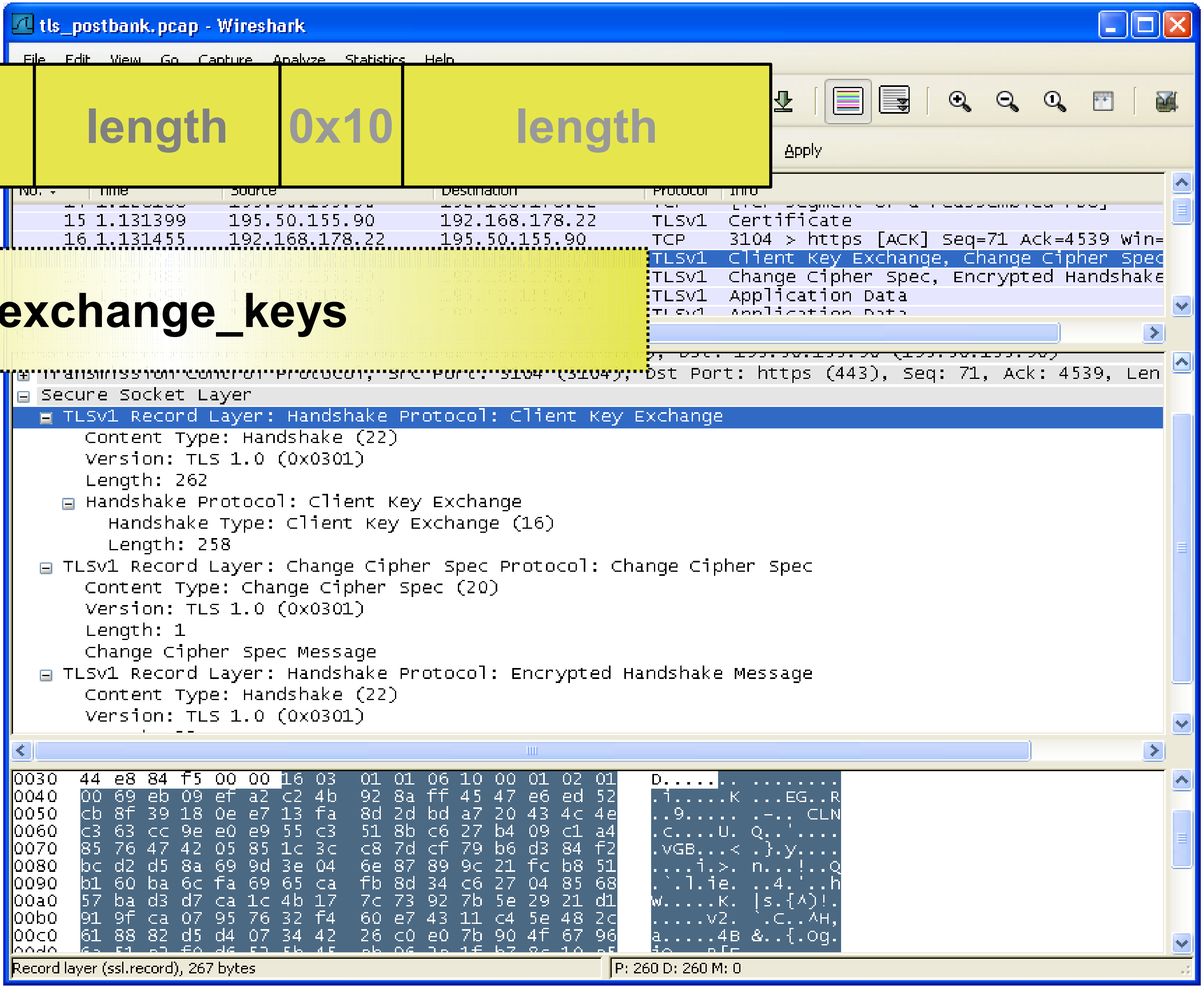
TLS Handshake – Client Key Exchange

0x16 | version | length | 0x10 | length

exchange_keys

RSA:
Encrypted Pre-Master Secret

DH:
Client DH Public


tls_postbank.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Apply
No. Time Source Destination Protocol Info

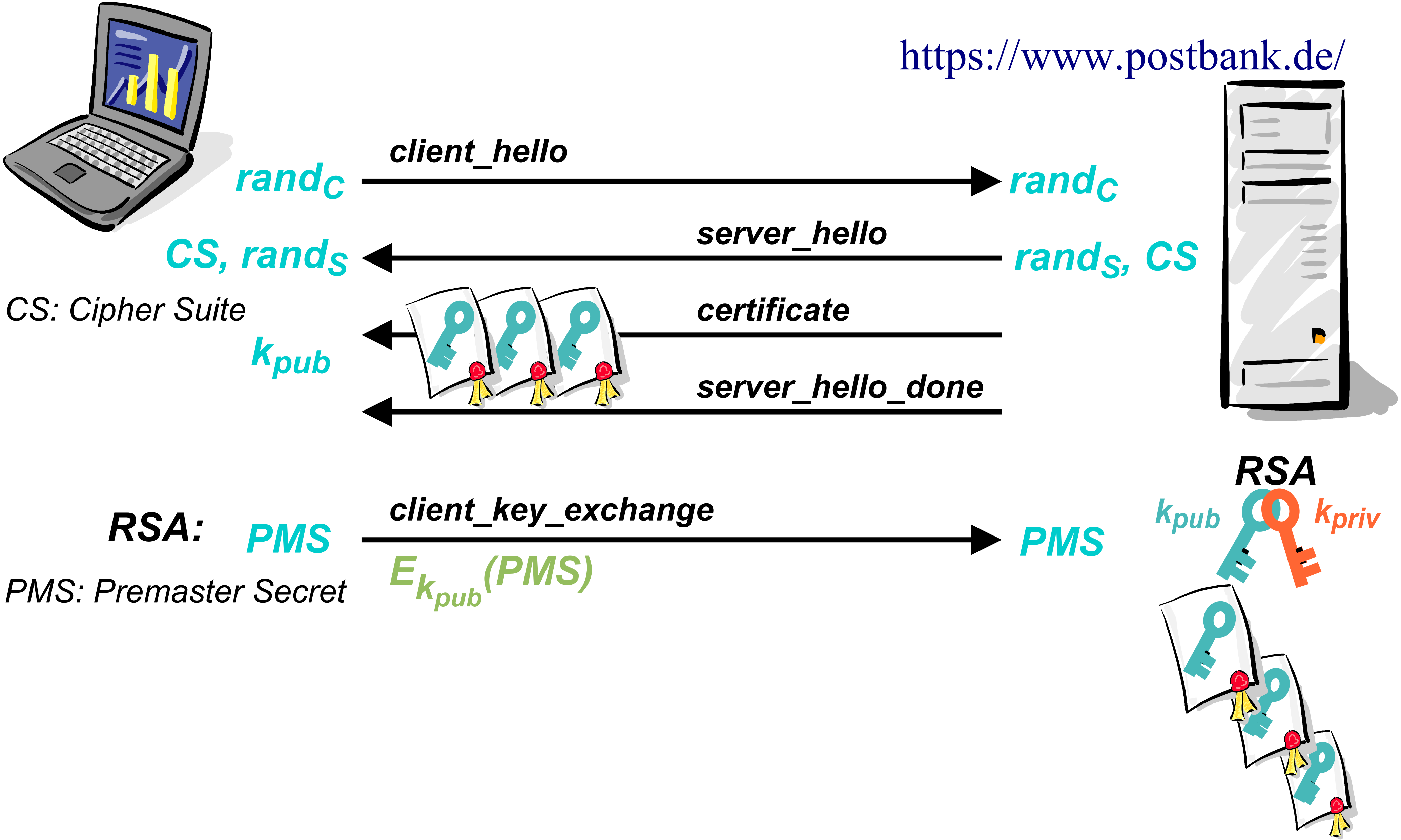
```
15 1.131399   195.50.155.90    192.168.178.22   TLSv1   Certificate
16 1.131455   192.168.178.22   195.50.155.90    TCP     3104 > https [ACK] Seq=71 Ack=4539 Win=
                                                TLSv1   Client Key Exchange, Change Cipher Spec
                                                TLSv1   Change Cipher Spec, Encrypted Handshake
                                                TLSv1   Application Data
```

```
⊞ Transmission Control Protocol, Src Port: 3104 (3104), Dst Port: https (443), Seq: 71, Ack: 4539, Len
⊟ Secure Socket Layer
  ⊟ TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 262
    ⊟ Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 258
  ⊟ TLSv1 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
  ⊟ TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
```

```
0030  44 e8 84 f5 00 00 16 03  01 01 06 10 00 01 02 01   D....... ........
0040  00 69 eb 09 ef a2 c2 4b  92 8a ff 45 47 e6 ed 52   .i.....K ...EG..R
0050  cb 8f 39 18 0e e7 13 fa  8d 2d bd a7 20 43 4c 4e   ..9..... .-.. CLN
0060  c3 63 cc 9e e0 e9 55 c3  51 8b c6 27 b4 09 c1 a4   .c....U. Q..'....
0070  85 76 47 42 05 85 1c 3c  c8 7d cf 79 b6 d3 84 f2   .vGB...< .}.y....
0080  bc d2 d5 8a 69 9d 3e 04  6e 87 89 9c 21 fc b8 51   ....i.>. n...!..Q
0090  b1 60 ba 6c fa 69 65 ca  fb 8d 34 c6 27 04 85 68   .`.l.ie. ..4.'..h
00a0  57 ba d3 d7 ca 1c 4b 17  7c 73 92 7b 5e 29 21 d1   W.....K. |s.{^)!.
00b0  91 9f ca 07 95 76 32 f4  60 e7 43 11 c4 5e 48 2c   .....v2. `.C..^H,
00c0  61 88 82 d5 d4 07 34 42  26 c0 e0 7b 90 4f 67 96   a.....4B &..{.Og.
```

Record layer (ssl.record), 267 bytes | P: 260 D: 260 M: 0

TLS – Handshake (RSA key exchange)



https://www.postbank.de/

client_hello

$rand_C$ → $rand_C$

server_hello

$CS, rand_S$ ← $rand_S, CS$

CS: Cipher Suite

certificate

k_{pub}

server_hello_done

RSA

k_{pub} k_{priv}

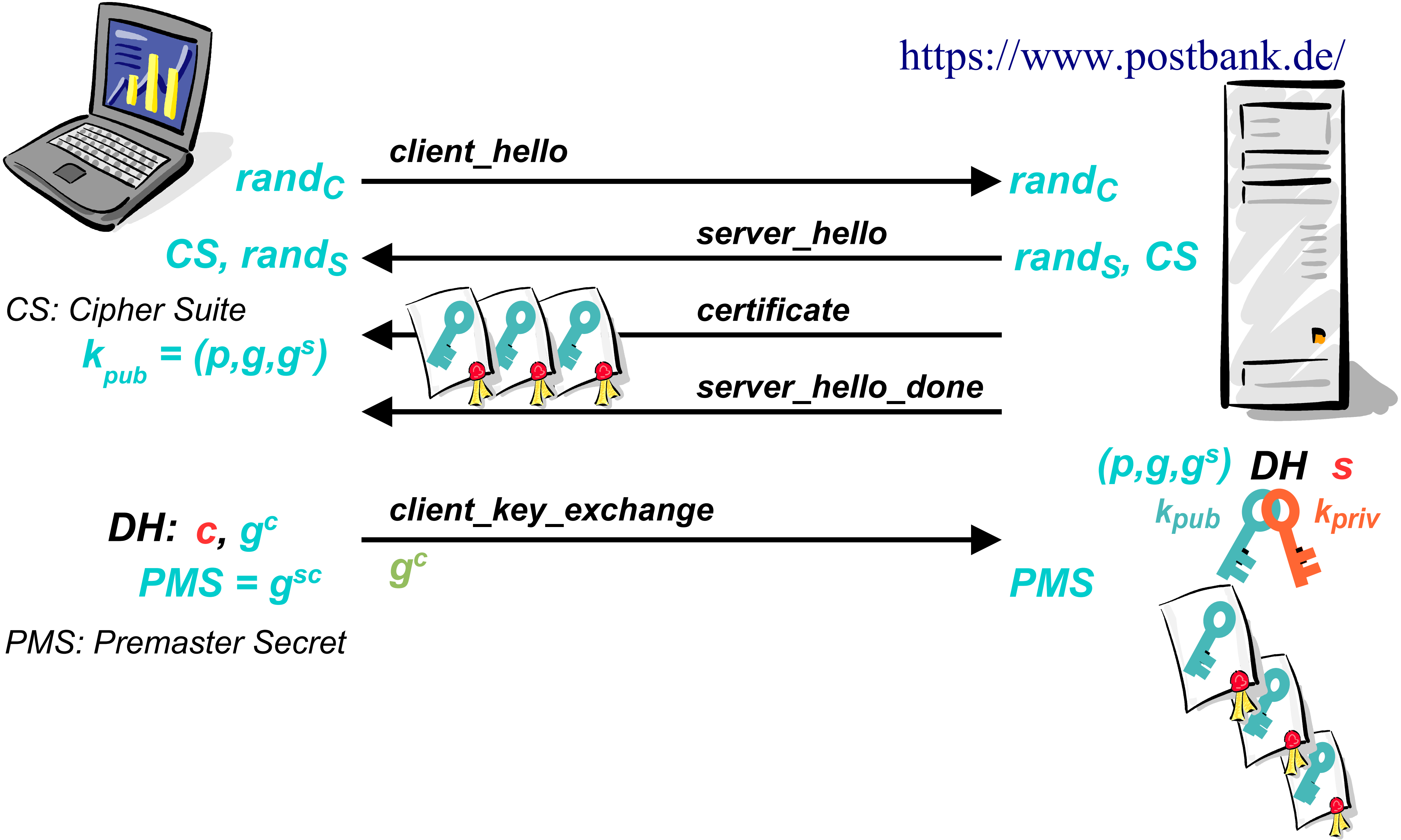
client_key_exchange

RSA: PMS → PMS

$E_{k_{pub}}(PMS)$

PMS: Premaster Secret

TLS – Handshake (DH key exchange)



https://www.postbank.de/

$rand_C$ client_hello → $rand_C$

$CS, rand_S$ ← server_hello $rand_S, CS$

CS: Cipher Suite

$k_{pub} = (p,g,g^s)$ ← certificate

← server_hello_done

(p,g,g^s) DH s

k_{pub} k_{priv}

DH: c, g^c client_key_exchange →

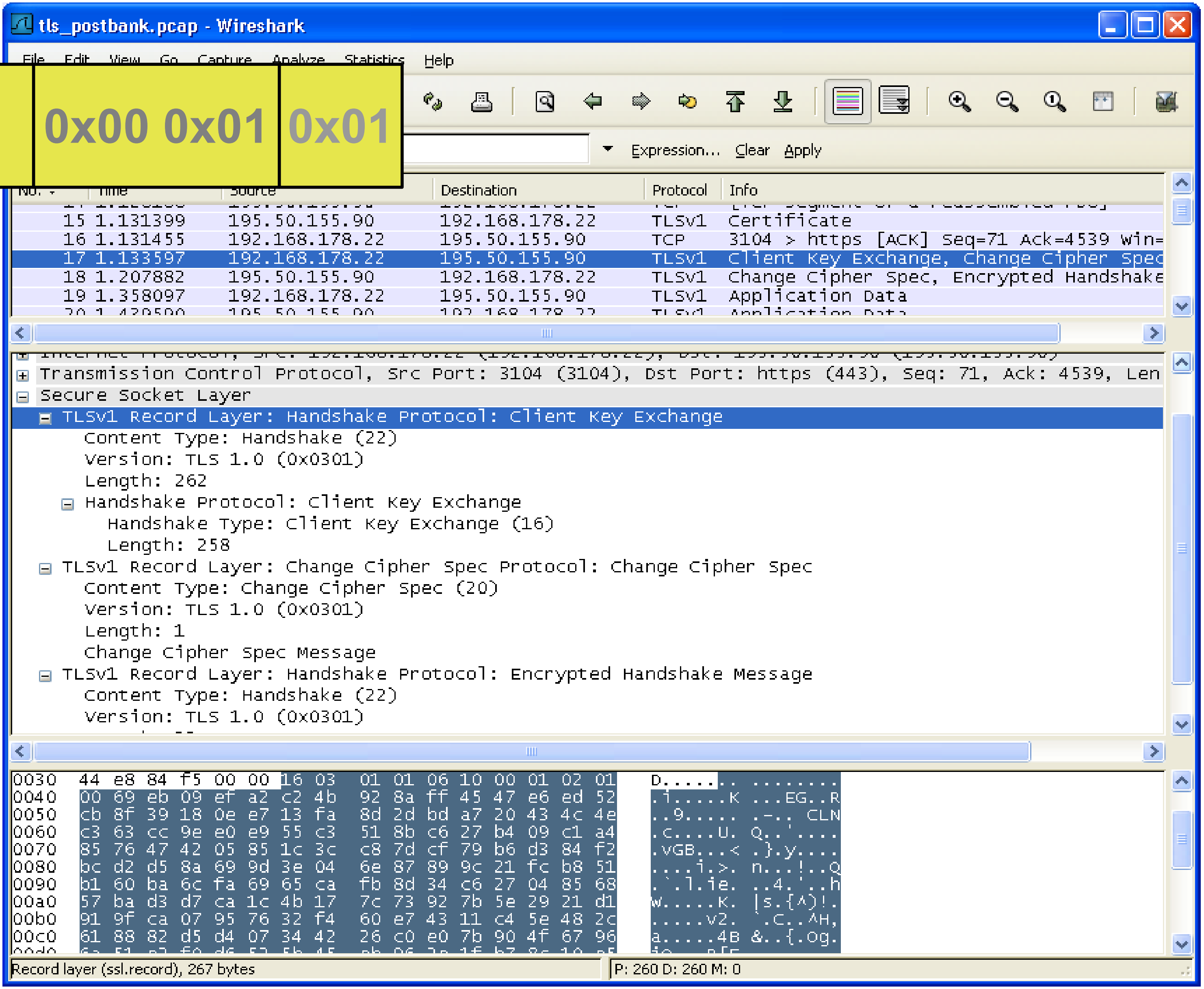
g^c

$PMS = g^{sc}$ PMS

PMS: Premaster Secret

TLS Change Cipher Spec

0x14	version	0x00 0x01	0x01


tls_postbank.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply

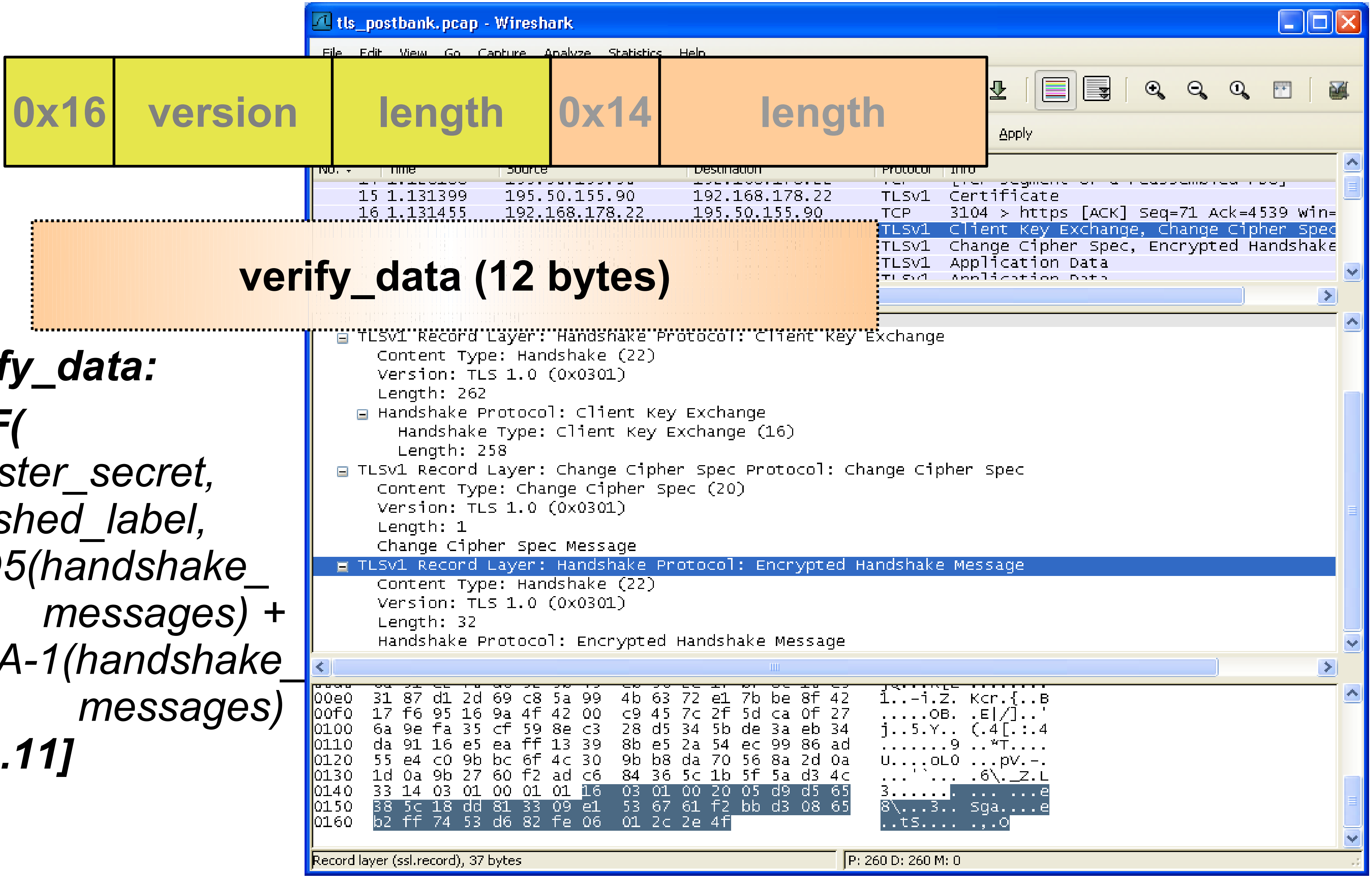
```
No.  Time        Source           Destination      Protocol  Info
15 1.131399  195.50.155.90    192.168.178.22   TLSv1     Certificate
16 1.131455  192.168.178.22   195.50.155.90    TCP       3104 > https [ACK] Seq=71 Ack=4539 Win=
17 1.133597  192.168.178.22   195.50.155.90    TLSv1     Client Key Exchange, Change Cipher Spec
18 1.207882  195.50.155.90    192.168.178.22   TLSv1     Change Cipher Spec, Encrypted Handshake
19 1.358097  192.168.178.22   195.50.155.90    TLSv1     Application Data
```

```
⊞ Transmission Control Protocol, Src Port: 3104 (3104), Dst Port: https (443), Seq: 71, Ack: 4539, Len
⊟ Secure Socket Layer
  ⊟ TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 262
    ⊟ Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 258
  ⊟ TLSv1 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
  ⊟ TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
```

```
0030  44 e8 84 f5 00 00 16 03  01 01 06 10 00 01 02 01   D....... ........
0040  00 69 eb 09 ef a2 c2 4b  92 8a ff 45 47 e6 ed 52   .i.....K ...EG..R
0050  cb 8f 39 18 0e e7 13 fa  8d 2d bd a7 20 43 4c 4e   ..9..... .-.. CLN
0060  c3 63 cc 9e e0 e9 55 c3  51 8b c6 27 b4 09 c1 a4   .c....U. Q..'....
0070  85 76 47 42 05 85 1c 3c  c8 7d cf 79 b6 d3 84 f2   .vGB...< .}.y....
0080  bc d2 d5 8a 69 9d 3e 04  6e 87 89 9c 21 fc b8 51   ....i.>. n...!..Q
0090  b1 60 ba 6c fa 69 65 ca  fb 8d 34 c6 27 04 85 68   .`.l.ie. ..4.'..h
00a0  57 ba d3 d7 ca 1c 4b 17  7c 73 92 7b 5e 29 21 d1   W.....K. |s.{^)!.
00b0  91 9f ca 07 95 76 32 f4  60 e7 43 11 c4 5e 48 2c   .....v2. `.C..^H,
00c0  61 88 82 d5 d4 07 34 42  26 c0 e0 7b 90 4f 67 96   a.....4B &..{.Og.
```

Record layer (ssl.record), 267 bytes | P: 260 D: 260 M: 0

TLS Handshake – Finished (Encrypted)


0x16
version
length
0x14
length
verify_data (12 bytes)
tls_postbank.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Apply
No. Time Source Destination Protocol Info

```
 15 1.131399   195.50.155.90    192.168.178.22   TLSv1   Certificate
 16 1.131455   192.168.178.22   195.50.155.90    TCP     3104 > https [ACK] Seq=71 Ack=4539 Win=
                                                 TLSv1   Client Key Exchange, Change Cipher Spec
                                                 TLSv1   Change Cipher Spec, Encrypted Handshake
                                                 TLSv1   Application Data
```

```
⊟ TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 262
  ⊟ Handshake Protocol: Client Key Exchange
      Handshake Type: Client Key Exchange (16)
      Length: 258
⊟ TLSv1 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
⊟ TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 32
    Handshake Protocol: Encrypted Handshake Message
```

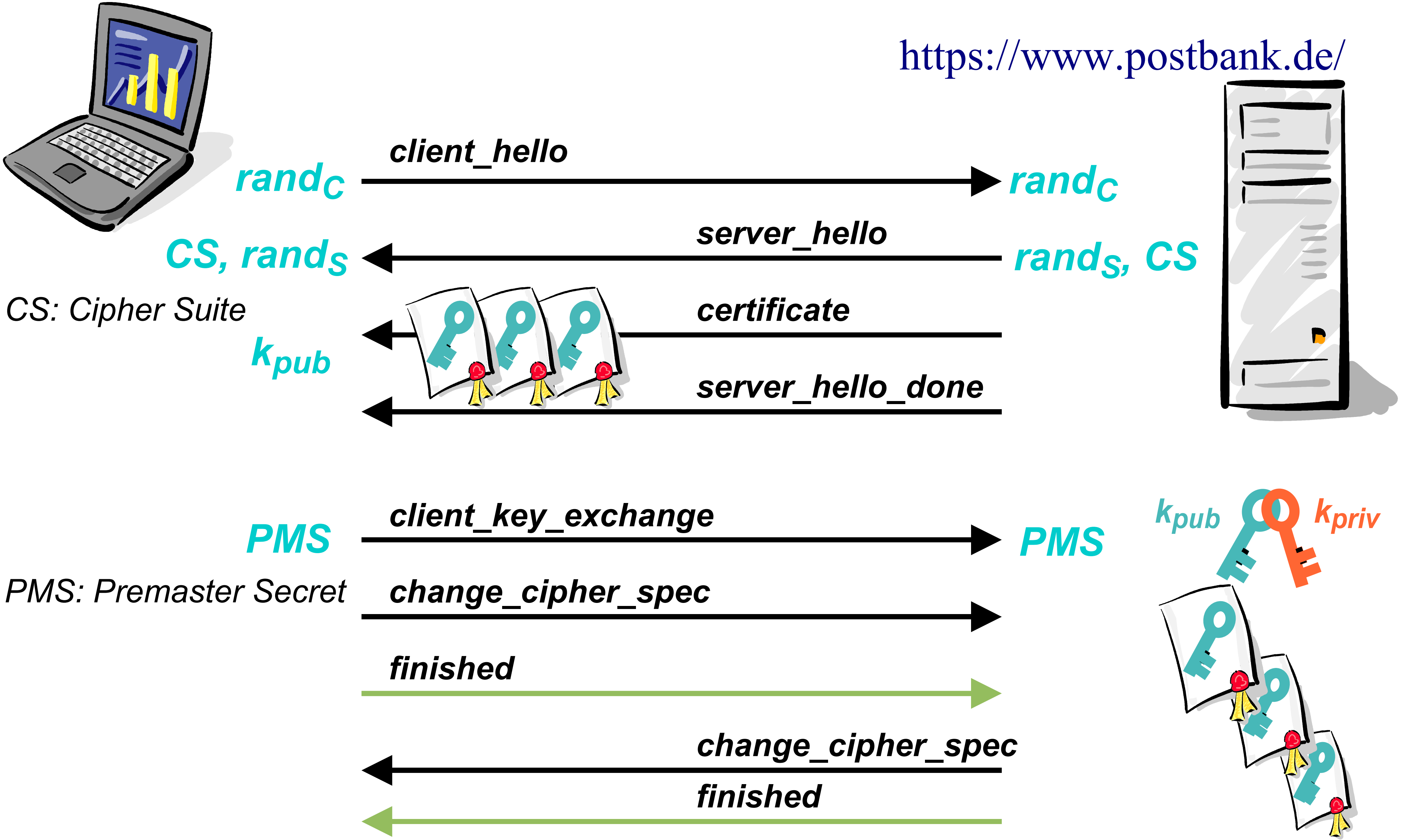
```
00e0  31 87 d1 2d 69 c8 5a 99  4b 63 72 e1 7b be 8f 42   1..-i.Z. Kcr.{..B
00f0  17 f6 95 16 9a 4f 42 00  c9 45 7c 2f 5d ca 0f 27   .....OB. .E|/]..'
0100  6a 9e fa 35 cf 59 8e c3  28 d5 34 5b de 3a eb 34   j..5.Y.. (.4[.:.4
0110  da 91 16 e5 ea ff 13 39  8b e5 2a 54 ec 99 86 ad   .......9 ..*T....
0120  55 e4 c0 9b bc 6f 4c 30  9b b8 da 70 56 8a 2d 0a   U....oL0 ...pV.-.
0130  1d 0a 9b 27 60 f2 ad c6  84 36 5c 1b 5f 5a d3 4c   ...'`... .6\._Z.L
0140  33 14 03 01 00 01 01 16  03 01 00 20 05 d9 d5 65   3....... ... ...e
0150  38 5c 18 dd 81 33 09 e1  53 67 61 f2 bb d3 08 65   8\...3.. Sga....e
0160  b2 ff 74 53 d6 82 fe 06  01 2c 2e 4f               ..tS.... .,.O
```

Record layer (ssl.record), 37 bytes | P: 260 D: 260 M: 0

verify_data:

PRF(
master_secret,
finished_label,
MD5(handshake_messages) +
SHA-1(handshake_messages)
) [0..11]

TLS – Handshake



https://www.postbank.de/

$rand_C$ client_hello *$rand_C$*

CS, $rand_S$ server_hello *$rand_S$, CS*

CS: Cipher Suite

k_{pub} certificate

server_hello_done

k_{pub} *k_{priv}*

PMS client_key_exchange *PMS*

PMS: Premaster Secret

change_cipher_spec

finished

change_cipher_spec

finished

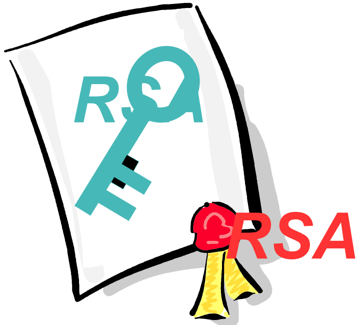
TLS Handshake – Cipher Suites

Initial suite

0x00 0x00	*TLS_NULL_WITH_NULL_NULL*

RSA key exchange suites

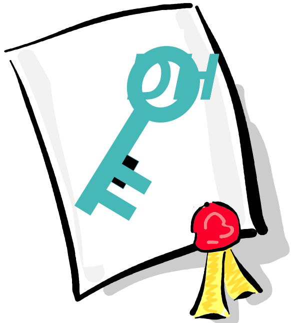
0x00 0x01	*TLS_RSA_WITH_NULL_MD5*
0x00 0x02	*TLS_RSA_WITH_NULL_SHA*
0x00 0x04	*TLS_RSA_WITH_RC4_128_MD5*
0x00 0x05	*TLS_RSA_WITH_RC4_128_SHA*
0x00 0x07	*TLS_RSA_WITH_IDEA_CBC_SHA*
0x00 0x09	*TLS_RSA_WITH_DES_CBC_SHA*
0x00 0x0A	*TLS_RSA_WITH_3DES_EDE_CBC_SHA*



TLS Handshake – Cipher Suites

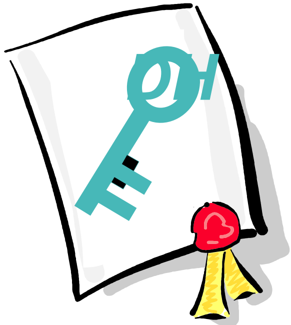
DH key exchange

0x00 0x0C	*TLS_DH_DSS_WITH_DES_CBC_SHA*
0x00 0x0D	*TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA*



DSS

0x00 0x0F	*TLS_DH_RSA_WITH_DES_CBC_SHA*
0x00 0x10	*TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA*

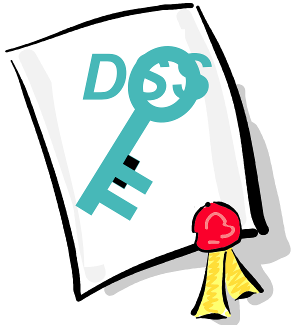


RSA

TLS Handshake – Cipher Suites

DH ephemeral key exchange

0x00 0x12	*TLS_DHE_DSS_WITH_DES_CBC_SHA*
0x00 0x13	*TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA*

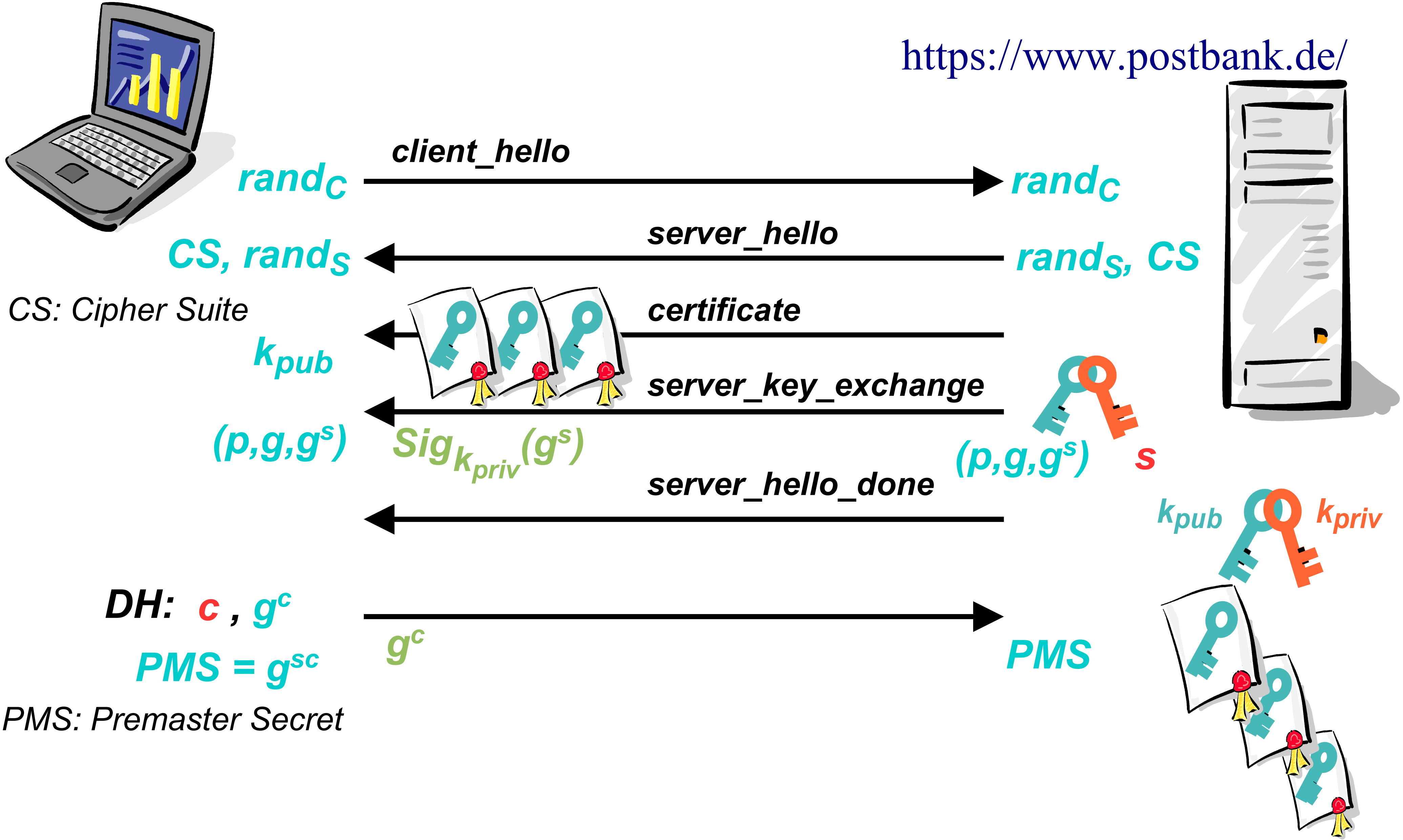


DSS

0x00 0x15	*TLS_DHE_RSA_WITH_DES_CBC_SHA*
0x00 0x16	*TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA*

RSA

TLS – Handshake (DH ephemeral key exchange)



https://www.postbank.de/

client_hello: $rand_C$ → $rand_C$

server_hello: $CS, rand_S$ ← $rand_S, CS$

CS: Cipher Suite

certificate: k_{pub} ←

server_key_exchange: (p,g,g^s) ← $Sig_{k_{priv}}(g^s)$ ← (p,g,g^s) s

k_{pub} k_{priv}

server_hello_done ←

DH: c , g^c

$PMS = g^{sc}$

g^c → PMS

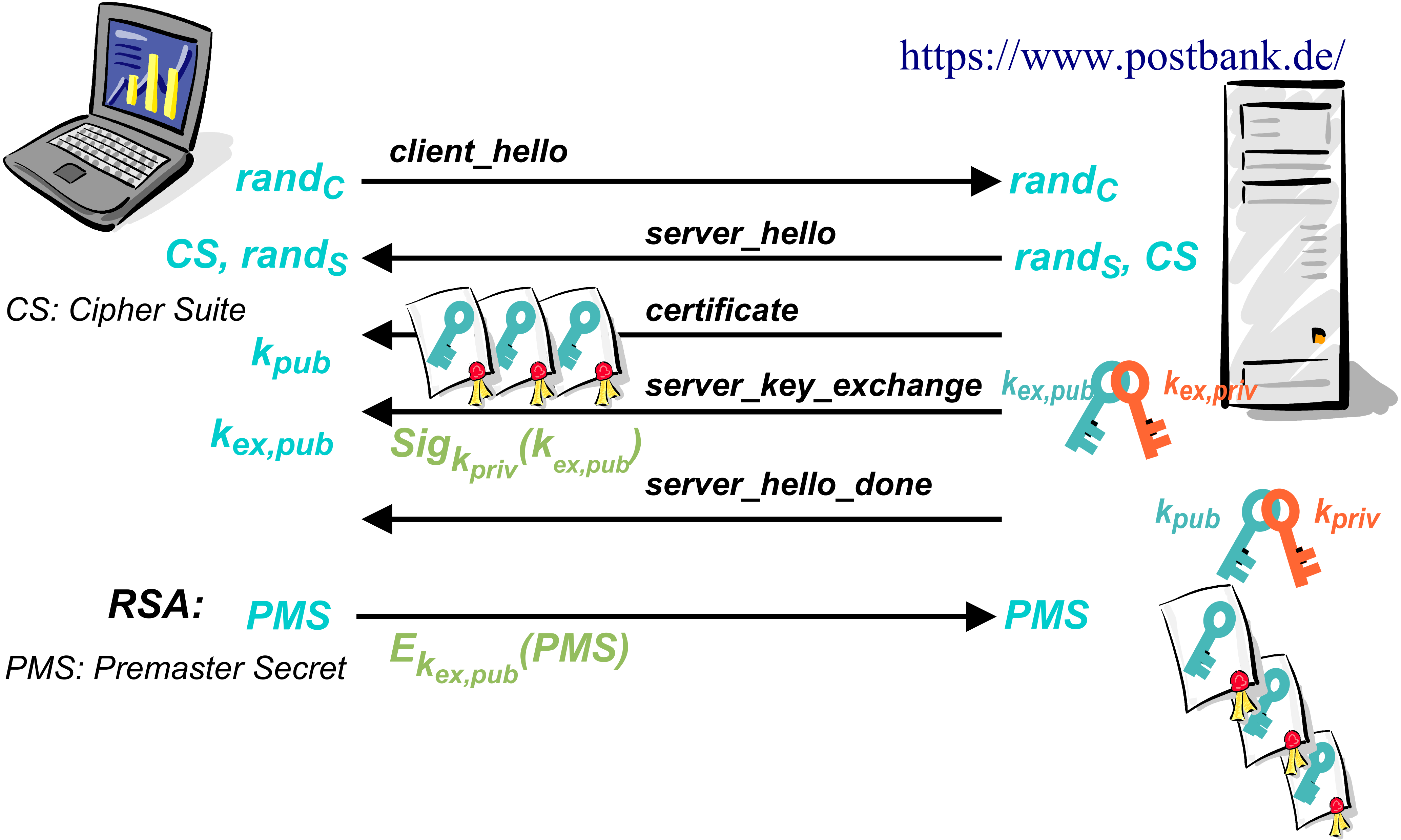
PMS: Premaster Secret

TLS Handshake – Cipher Suites

Export cipher suites (for backward compatibility)

0x00 0x03	*TLS_RSA_EXPORT_WITH_RC4_40_MD5*
0x00 0x06	*TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5*
0x00 0x08	*TLS_RSA_EXPORT_WITH_DES40_CBC_SHA*

TLS Handshake (RSA export key exchange)



https://www.postbank.de/

client_hello

$rand_C$ $rand_C$

server_hello

$CS, rand_S$ $rand_S, CS$

CS: Cipher Suite

certificate

k_{pub}

server_key_exchange

$k_{ex,pub}$ $k_{ex,pub}$ $k_{ex,priv}$

$Sig_{k_{priv}}(k_{ex,pub})$

server_hello_done

k_{pub} k_{priv}

RSA: PMS PMS

$E_{k_{ex,pub}}(PMS)$

PMS: Premaster Secret

TLS Handshake – Cipher Suites

Export cipher suites (for backward compatibility)

0x00 0x0B	*TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA*
0x00 0x0E	*TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA*
0x00 0x11	*TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA*
0x00 0x14	*TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA*
0x00 0x17	*TLS_DH_anon_EXPORT_WITH_RC4_40_MD5*
0x00 0x19	*TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA*

TLS Handshake – Cipher Suites

No authentication (deprecated)

0x00 0x18	*TLS_DH_anon_WITH_RC4_128_MD5*
0x00 0x1A	*TLS_DH_anon_WITH_DES_CBC_SHA*
0x00 0x1B	*TLS_DH_anon_WITH_3DES_EDE_CBC_SHA*

TLS Handshake – Cipher Suites

Kerberos cipher suites (RFC 2712)

0x00 0x1E	*TLS_KRB5_WITH_DES_CBC_SHA*
0x00 0x1F	*TLS_KRB5_WITH_3DES_EDE_CBC_SHA*
0x00 0x20	*TLS_KRB5_WITH_RC4_128_SHA*
0x00 0x21	*TLS_KRB5_WITH_IDEA_CBC_SHA*
0x00 0x22	*TLS_KRB5_WITH_DES_CBC_MD5*
0x00 0x23	*TLS_KRB5_WITH_3DES_EDE_CBC_MD5*
0x00 0x24	*TLS_KRB5_WITH_RC4_128_MD5*
0x00 0x25	*TLS_KRB5_WITH_IDEA_CBC_MD5*

TLS Handshake – Cipher Suites

Kerberos cipher suites (not to be used with TLS 1.1)

0x00 0x26	*TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA*
0x00 0x27	*TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA*
0x00 0x28	*TLS_KRB5_EXPORT_WITH_RC4_40_SHA*
0x00 0x29	*TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5*
0x00 0x2A	*TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5*
0x00 0x2B	*TLS_KRB5_EXPORT_WITH_RC4_40_MD5*

TLS Handshake – Cipher Suites

AES cipher suites (RFC 3268)

0x00 0x2F	*TLS_RSA_WITH_AES_128_CBC_SHA*
0x00 0x30	*TLS_DH_DSS_WITH_AES_128_CBC_SHA*
0x00 0x31	*TLS_DH_RSA_WITH_AES_128_CBC_SHA*
0x00 0x32	*TLS_DHE_DSS_WITH_AES_128_CBC_SHA*
0x00 0x33	*TLS_DHE_RSA_WITH_AES_128_CBC_SHA*
0x00 0x34	*TLS_DH_anon_WITH_AES_128_CBC_SHA*
0x00 0x35	*TLS_RSA_WITH_AES_256_CBC_SHA*
0x00 0x36	*TLS_DH_DSS_WITH_AES_256_CBC_SHA*

TLS Handshake – Cipher Suites

AES cipher suites (RFC 3268), continued

0x00 0x37	*TLS_DH_RSA_WITH_AES_256_CBC_SHA*
0x00 0x38	*TLS_DHE_DSS_WITH_AES_256_CBC_SHA*
0x00 0x39	*TLS_DHE_RSA_WITH_AES_256_CBC_SHA*
0x00 0x3A	*TLS_DH_anon_WITH_AES_256_CBC_SHA*

ECC cipher suites (RFC 4492)