Debugging SSL/TLS Connections

Understanding SSL/TLS connection problems can sometimes be difficult, especially when it is not clear what messages are actually being sent and received. The SunJSSE has a built-in debug facility and is activated by the System property `javax.net.debug`.

What follows is a brief example how to read the debug output. Please be aware that the output is non-standard, and may change from release to release. We are using the default SunJSSE X509KeyManager and X509TrustManager which prints debug information.

This example assumes a basic understanding of the SSL/TLS protocol. Please see the The SSL Protocol Overview section of the JSSE Reference Guide for more information on the protocols (handshake messages, etc.).

In this example, we connect using the `SSLSocketClientWithClientAuth` sample application to a simple HTTPS server that requires client authentication, then send a HTTPS request and receive the reply.

```
java  -Djavax.net.debug=all  \
    -Djavax.net.ssl.trustStore=trustStore
    SSLSocketClientWithClientAuth bongos 2001 /index.html
```

First, the X509KeyManager is initialized and discovers there is one keyEntry in the supplied KeyStore for a subject called "duke". If a server requests a client to authenticate itself, the X509KeyManager will search its list of keyEntries for an appropriate credential.

```
***
found key for : duke
chain [0] = [
[
  Version: V1
  Subject: CN=Duke, OU= , O="Oracle and/or its affiliates.",
  L=Cupertino, ST=CA, C=US
  Signature Algorithm: MD5withRSA, OID = 1.2.840.113549.1.1.4

  Key:  Sun RSA public key, 1024 bits
  modulus: 134968166047563266914058280571444028986498087544923991226919517
  667593269213420979048109900052353578998293280426361122296881234393722020
  704208851688212064483570055963805034839797994154526862998272017486468599
  962268346037652120279791547218281230795146025359480589335682217749874703
  510467348902637769973696151441
  public exponent: 65537
  Validity: [From: Tue May 22 16:46:46 PDT 2001,
              To: Sun May 22 16:46:46 PDT 2011]
  Issuer: CN=Duke, OU= , O="Oracle and/or its affiliates.",
  L=Cupertino, ST=CA, C=US
  SerialNumber: [    3b0afa66]

]
  Algorithm: [MD5withRSA]
  Signature:
0000: 5F B5 62 E9 A0 26 1D 8E   A2 7E 7C 02 08 36 3A 3E  _.b..&.......6:>
0010: C9 C2 45 03 DD F9 BC 06   FC 25 CF 30 92 91 B1 4E  ..E......%.0...N
0020: 62 17 08 48 14 68 80 CF   DD 89 11 EA 92 7F CE DD  b..H.h..........
0030: B4 FD 12 A8 71 C7 9E D7   C3 D0 E3 BD BB DE 20 92  ....q......... .
0040: C2 3B C8 DE CB 25 23 C0   8B B6 92 B9 0B 64 80 63  .;...%#......d.c
0050: D9 09 25 2D 7A CF 0A 31   B6 E9 CA C1 37 93 BC 0D  ..%-z..1....7...
0060: 4E 74 95 4F 58 31 DA AC   DF D8 BD 89 BD AF EC C8  Nt.OX1..........
```

```
0070: 2D 18 A2 BC B2 15 4F B7   28 6F D3 00 E1 72 9B 6C  -.....O.(o...r.l

]
***
```

The X509TrustManager is next initialized, and finds a certificate for a Certificate Authority (CA) named "JSSE Test CA". Any server presenting **valid** credentials signed by this CA will be trusted.

```
trustStore is: trustkeys
trustStore type is : jks
trustStore provider is :
init truststore
adding as trusted cert:
  Subject: CN=JSSE Test CA, OU=JWS, O=Sun,
      L=Santa Clara, ST=CA, C=US
  Issuer:  CN=JSSE Test CA, OU=JWS, O=Sun,
      L=Santa Clara, ST=CA, C=US
  Algorithm: RSA; Serial number: 0x0
  Valid from Mon Jul 19 13:30:15 PDT 2004 until Fri Dec 05 12:30:15 PST 2031
```

We finish some additional initialization code, and after this, we are now finally ready to make the connection to the server.

```
trigger seeding of SecureRandom
done seeding SecureRandom
export control - checking the cipher suites
export control - no cached value available...
export control - storing legal entry into cache...
%% No cached client session
```

The connection to the server is made, and we see the initial ClientHello message, which contains:

- random information to initialize the cryptographic routines,
- the SessionID, which if non-null, would be used in reestablishing a previous session,
- the list of ciphersuites that the client requests,
- and no compression algorithms.

This is followed by the output of various filters, such as encapsulating the TLSv1 header into the SSLv2Hello header format (See setEnabledProtocols()).

```
*** ClientHello, TLSv1
RandomCookie:  GMT: 1073239164 bytes = { 10, 80, 71, 86, 124, 135, 104,
151, 72, 153, 70, 28, 97, 232, 160, 217, 146, 178, 87, 255, 122, 147, 83,
197, 60, 187, 227, 76 }
Session ID:  {}
Cipher Suites: [SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA,
SSL_RSA_WITH_DES_CBC_SHA, SSL_DHE_RSA_WITH_DES_CBC_SHA,
SSL_DHE_DSS_WITH_DES_CBC_SHA, SSL_RSA_EXPORT_WITH_RC4_40_MD5,
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA, SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA,
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA]
Compression Methods:  { 0 }
***
[write] MD5 and SHA1 hashes:  len = 73
0000: 01 00 00 45 03 01 40 F8   54 7C 0A 50 47 56 7C 87  ...E..@.T..PGV..
0010: 68 97 48 99 46 1C 61 E8   A0 D9 92 B2 57 FF 7A 93  h.H.F.a.....W.z.
0020: 53 C5 3C BB E3 4C 00 00   1E 00 04 00 05 00 2F 00  S.<..L......../.
0030: 33 00 32 00 0A 00 16 00   13 00 09 00 15 00 12 00  3.2.............
0040: 03 00 08 00 14 00 11 01   00                       .........
main, WRITE: TLSv1 Handshake, length = 73
```

```
[write] MD5 and SHA1 hashes:  len = 98
0000: 01 03 01 00 39 00 00 00   20 00 00 04 01 00 80 00  ....9... .......
0010: 00 05 00 00 2F 00 00 33   00 00 32 00 00 0A 07 00  ..../..3..2.....
0020: C0 00 00 16 00 00 13 00   00 09 06 00 40 00 00 15  ............@...
0030: 00 00 12 00 00 03 02 00   80 00 00 08 00 00 14 00  ................
0040: 00 11 40 F8 54 7C 0A 50   47 56 7C 87 68 97 48 99  ..@.T..PGV..h.H.
0050: 46 1C 61 E8 A0 D9 92 B2   57 FF 7A 93 53 C5 3C BB  F.a.....W.z.S.<.
0060: E3 4C                                              .L
main, WRITE: SSLv2 client hello message, length = 98
```

Section labeled "[Raw write]" represent the actual data sent to the raw output object (in this case, an OutputStream).

```
[Raw write]: length = 100
0000: 80 62 01 03 01 00 39 00   00 00 20 00 00 04 01 00  .b....9... .....
0010: 80 00 00 05 00 00 2F 00   00 33 00 00 32 00 00 0A  ....../..3..2...
0020: 07 00 C0 00 00 16 00 00   13 00 00 09 06 00 40 00  ..............@.
0030: 00 15 00 00 12 00 00 03   02 00 80 00 00 08 00 00  ................
0040: 14 00 00 11 40 F8 54 7C   0A 50 47 56 7C 87 68 97  ....@.T..PGV..h.
0050: 48 99 46 1C 61 E8 A0 D9   92 B2 57 FF 7A 93 53 C5  H.F.a.....W.z.S.
0060: 3C BB E3 4C                                       <..L
```

After sending the initial ClientHello, we wait for the server's response, a ServerHello. "[Raw read]" displays the raw data read from the input device (InputStream), before any processing has been performed.

```
[Raw read]: length = 5
0000: 16 03 01 06 F0                                     .....
[Raw read]: length = 1776
0000: 02 00 00 46 03 01 40 FC   31 10 79 AB 17 66 FA 8B  ...F..@.1.y..f..
0010: 3F AA FD 5E 48 23 FA 90   31 D8 3C B9 A3 2C 8C F5  ?..^H#..1.<..,..
0020: E9 81 9B A2 63 6C 20 40   FC 31 10 BD 8D A5 91 06  ....cl @.1......
0030: 8B E1 E6 80 C6 5A 5C D9   8D 0A AE CA 58 4A BA 36  .....Z\.....XJ.6
0040: B1 3D 04 8D 82 21 B4 00   04 00 0B 00 06 1B 00 06  .=...!..........
0050: 18 00 03 11 30 82 03 0D   30 82 02 76 A0 03 02 01  ....0...0..v....
0060: 02 02 01 01 30 0D 06 09   2A 86 48 86 F7 0D 01 01  ....0...*.H.....
0070: 04 05 00 30 63 31 0B 30   09 06 03 55 04 06 13 02  ...0c1.0...U....
0080: 55 53 31 0B 30 09 06 03   55 04 08 13 02 43 41 31  US1.0...U....CA1
0090: 14 30 12 06 03 55 04 07   13 0B 53 61 6E 74 61 20  .0...U....Santa
00A0: 43 6C 61 72 61 31 0C 30   0A 06 03 55 04 0A 13 03  Clara1.0...U....
00B0: 53 75 6E 31 0C 30 0A 06   03 55 04 0B 13 03 4A 57  Sun1.0...U....JW
00C0: 53 31 15 30 13 06 03 55   04 03 13 0C 4A 53 53 45  S1.0...U....JSSE
00D0: 20 54 65 73 74 20 43 41   30 1E 17 0D 30 34 30 37   Test CA0...0407
00E0: 31 39 32 30 33 30 35 31   5A 17 0D 33 31 31 32 30  19203051Z..31120
00F0: 35 32 30 33 30 35 31 5A   30 48 31 0B 30 09 06 03  5203051Z0H1.0...
0100: 55 04 06 13 02 55 53 31   0B 30 09 06 03 55 04 08  U....US1.0...U..
0110: 13 02 43 41 31 0C 30 0A   06 03 55 04 0A 13 03 53  ..CA1.0...U....S
0120: 75 6E 31 0D 30 0B 06 03   55 04 0B 13 04 4A 61 76  un1.0...U....Jav
0130: 61 31 0F 30 0D 06 03 55   04 03 13 06 62 6F 6E 67  a1.0...U....bong
0140: 6F 73 30 81 9F 30 0D 06   09 2A 86 48 86 F7 0D 01  os0..0...*.H....
0150: 01 01 05 00 03 81 8D 00   30 81 89 02 81 81 00 CC  ........0.......
0160: 09 74 CB 43 AB 6D ED F6   35 AA 0E 49 29 D9 E0 F0  .t.C.m..5..I)...
0170: A1 D5 E2 3E 8F 5E C5 CE   F4 DE C1 A4 F3 CB 8C 45  ...>.^.........E
0180: 0B 0F 6E 21 E1 00 65 CB   3C D1 5C EF 6A FB 5D 96  ..n!..e.<.\.j.].
0190: 93 F4 71 41 41 45 FF 37   86 4C AB F9 EA 9A 3F A5  ..qAAE.7.L....?.
01A0: 82 60 BF 0A 81 84 C9 3E   AC 0F 3D 20 3D AC A0 69  .`.....>..= =..i
01B0: EF CA 4A A7 94 AD C8 A5   CE 37 66 52 D1 25 43 CB  ..J......7fR.%C.
01C0: 10 44 07 1E 93 74 D9 68   01 D7 06 48 C9 0D 52 2D  .D...t.h...H..R-
01D0: D5 6A 2E A6 48 4C 59 E2   5C C6 C1 5C C8 4C 1B 02  .j..HLY.\..\.L..
01E0: 03 01 00 01 A3 81 EB 30   81 E8 30 09 06 03 55 1D  .......0..0...U.
01F0: 13 04 02 30 00 30 2C 06   09 60 86 48 01 86 F8 42  ...0.0,..`.H...B
0200: 01 0D 04 1F 16 1D 4F 70   65 6E 53 53 4C 20 47 65  ......OpenSSL Ge
0210: 6E 65 72 61 74 65 64 20   43 65 72 74 69 66 69 63  nerated Certific
0220: 61 74 65 30 1D 06 03 55   1D 0E 04 16 04 14 58 D7  ate0...U......X.
0230: 3A A9 37 AA 3E 14 27 FC   EC CC 45 08 04 8E 2A 8B  :.7.>.'...E...*.
```

```
0240: 77 28 30 81 8D 06 03 55   1D 23 04 81 85 30 81 82  w(0....U.#...0..
0250: 80 14 08 A3 7E 35 96 15   FA B0 F5 1B 5F CD 4F 54  .....5......_.OT
0260: EF 31 33 70 E4 A7 A1 67   A4 65 30 63 31 0B 30 09  .13p...g.e0c1.0.
0270: 06 03 55 04 06 13 02 55   53 31 0B 30 09 06 03 55  ..U....US1.0...U
0280: 04 08 13 02 43 41 31 14   30 12 06 03 55 04 07 13  ....CA1.0...U...
0290: 0B 53 61 6E 74 61 20 43   6C 61 72 61 31 0C 30 0A  .Santa Clara1.0.
02A0: 06 03 55 04 0A 13 03 53   75 6E 31 0C 30 0A 06 03  ..U....Sun1.0...
02B0: 55 04 0B 13 03 4A 57 53   31 15 30 13 06 03 55 04  U....JWS1.0...U.
02C0: 03 13 0C 4A 53 53 45 20   54 65 73 74 20 43 41 82  ...JSSE Test CA.
02D0: 01 00 30 0D 06 09 2A 86   48 86 F7 0D 01 01 04 05  ..0...*.H.......
02E0: 00 03 81 81 00 05 3E 17   DA F2 05 CB 4E 9E BF 12  ......>.....N...
02F0: CE 13 76 FF B2 FB 7F 9C   3D 45 28 43 6C 98 28 E3  ..v.....=E(Cl.(.
0300: 92 17 C2 C6 F1 62 CA 60   C2 B0 EC E6 7E 4C 2F C2  .....b.`.....L/.
0310: 40 FE 06 CB 34 60 B1 F4   26 1C E8 46 39 24 E1 8A  @...4`..&..F9$..
0320: 71 F2 13 90 A4 0A 7B 0B   13 AB 51 68 53 D9 7A 31  q.........QhS.z1
0330: 5A C1 7E 3C 44 2C 49 70   57 25 F9 18 FE 5D A5 42  Z..a.).1F....'y@v
0350: 97 B6 25 19 BE 6C 6A 92   DC EF 11 BE E7 4A FF 2A  ..%..lj......J.*
0360: E6 D6 AC 39 31 00 03 01   30 82 02 FD 30 82 02 66  ...91...0...0..f
0370: A0 03 02 01 02 02 01 00   30 0D 06 09 2A 86 48 86  ........0...*.H.
0380: F7 0D 01 01 04 05 00 30   63 31 0B 30 09 06 03 55  .......0c1.0...U
0390: 04 06 13 02 55 53 31 0B   30 09 06 03 55 04 08 13  ....US1.0...U...
03A0: 02 43 41 31 14 30 12 06   03 55 04 07 13 0B 53 61  .CA1.0...U....Sa
03B0: 6E 74 61 20 43 6C 61 72   61 31 0C 30 0A 06 03 55  nta Clara1.0...U
03C0: 04 0A 13 03 53 75 6E 31   0C 30 0A 06 03 55 04 0B  ....Sun1.0...U..
03D0: 13 03 4A 57 53 31 15 30   13 06 03 55 04 03 13 0C  ..JWS1.0...U....
03E0: 4A 53 53 45 20 54 65 73   74 20 43 41 30 1E 17 0D  JSSE Test CA0...
03F0: 30 34 30 37 31 39 32 30   33 30 31 35 5A 17 0D 33  040719203015Z..3
0400: 31 31 32 30 35 32 30 33   30 31 35 5A 30 63 31 0B  11205203015Z0c1.
0410: 30 09 06 03 55 04 06 13   02 55 53 31 0B 30 09 06  0...U....US1.0..
0420: 03 55 04 08 13 02 43 41   31 14 30 12 06 03 55 04  .U....CA1.0...U.
0430: 07 13 0B 53 61 6E 74 61   20 43 6C 61 72 61 31 0C  ...Santa Clara1.
0440: 30 0A 06 03 55 04 0A 13   03 53 75 6E 31 0C 30 0A  0...U....Sun1.0.
0450: 06 03 55 04 0B 13 03 4A   57 53 31 15 30 13 06 03  ..U....JWS1.0...
0460: 55 04 03 13 0C 4A 53 53   45 20 54 65 73 74 20 43  U....JSSE Test C
0470: 41 30 81 9F 30 0D 06 09   2A 86 48 86 F7 0D 01 01  A0..0...*.H.....
0480: 01 05 00 03 81 8D 00 30   81 89 02 81 81 00 9A 0A  .......0........
0490: B6 45 66 D5 DE 4A D9 3C   8C AC A6 B5 A5 88 B4 CF  .Ef..J.<........
04A0: 14 E1 A6 1B 25 25 4F 44   C9 1F 22 38 32 29 CF A1  ....%%OD.."82)..
04B0: 7C 18 30 93 DC 2B EC 2B   67 EE 2E 08 66 2D 0F 47  ..0..+.+g...f-.G
04C0: E0 12 3A DC E0 03 E9 65   16 F6 18 C6 16 14 56 24  ..:....e......V$
04D0: 55 7D 32 3E F9 66 A2 DD   55 EB 4D 0A 67 C7 5D 21  U.2>.f..U.M.g.]!
04E0: 9B 29 EA 2E 51 C5 83 A3   55 FF 35 CA A6 99 8F 46  .)..Q...U.5....F
04F0: F8 8E 56 BB A2 B1 39 83   D8 61 42 79 E0 95 78 FA  ..V...9..aBy..x.
0500: C6 E3 65 B0 FD 74 2D 64   51 71 04 F2 A1 91 02 03  ..e..t-dQq......
0510: 01 00 01 A3 81 C0 30 81   BD 30 1D 06 03 55 1D 0E  ......0..0...U..
0520: 04 16 04 14 08 A3 7E 35   96 15 FA B0 F5 1B 5F CD  .......5......_.
0530: 4F 54 EF 31 33 70 E4 A7   30 81 8D 06 03 55 1D 23  OT.13p..0....U.#
0540: 04 81 85 30 81 82 80 14   08 A3 7E 35 96 15 FA B0  ...0.......5....
0550: F5 1B 5F CD 4F 54 EF 31   33 70 E4 A7 A1 67 A4 65  .._.OT.13p...g.e
0560: 30 63 31 0B 30 09 06 03   55 04 06 13 02 55 53 31  0c1.0...U....US1
0570: 0B 30 09 06 03 55 04 08   13 02 43 41 31 14 30 12  .0...U....CA1.0.
0580: 06 03 55 04 07 13 0B 53   61 6E 74 61 20 43 6C 61  ..U....Santa Cla
0590: 72 61 31 0C 30 0A 06 03   55 04 0A 13 03 53 75 6E  ra1.0...U....Sun
05A0: 31 0C 30 0A 06 03 55 04   0B 13 03 4A 57 53 31 15  1.0...U....JWS1.
05B0: 30 13 06 03 55 04 03 13   0C 4A 53 53 45 20 54 65  0...U....JSSE Te
05C0: 73 74 20 43 41 82 01 00   30 0C 06 03 55 1D 13 04  st CA...0...U...
05D0: 05 30 03 01 01 FF 30 0D   06 09 2A 86 48 86 F7 0D  .0....0...*.H...
05E0: 01 01 04 05 00 03 81 81   00 73 6A 46 A2 05 E3 D8  .........sjF....
05F0: 6E 5C F4 18 A2 74 BC CF   EB 0C 5B FF 81 1C 28 85  n\...t....[...(.
0600: C7 FA E4 ED 5C 4F 71 22   FB 26 E3 01 3D 0C 10 AA  ....\Oq".&..=...
0610: BB 3E 90 ED 0E 1F 0C 9B   B1 8C 49 6A 51 E4 C3 52  .>........IjQ..R
0620: D6 FB 42 6C B4 A9 A9 57   A5 84 00 42 6D 37 37 6D  ..Bl...W...Bm77m
0630: C7 6C 23 BC DC 60 D1 9D   6F B3 75 47 3A 15 33 1A  .l#..`..o.uG:.3.
0640: EC 90 09 9D F9 EB BD 88   96 E7 1D 41 BC 01 8D CA  ...........A....
0650: 88 D9 5B 04 09 8F 3E EA   C8 15 A0 AA 4E 85 95 AE  ..[...>.....N...
```

```
0660: 2F 0E 31 92 AC 3C FB 2F   C4 0D 00 00 7F 02 01 02  /.1..</........
0670: 00 7A 00 78 30 76 31 0B   30 09 06 03 55 04 06 13  .z.x0v1.0...U...
0680: 02 55 53 31 0B 30 09 06   03 55 04 08 13 02 43 41  .US1.0...U....CA
0690: 31 12 30 10 06 03 55 04   07 13 09 43 75 70 65 72  1.0...U....Cuper
06A0: 74 69 6E 6F 31 1F 30 1D   06 03 55 04 0A 13 16 53  tino1.0...U....S
06B0: 75 6E 20 4D 69 63 72 6F   73 79 73 74 65 6D 73 2C  un Microsystems,
06C0: 20 49 6E 63 2E 31 16 30   14 06 03 55 04 0B 13 0D   Inc.1.0...U....
06D0: 4A 61 76 61 20 53 6F 66   74 77 61 72 65 31 0D 30   1.0
06E0: 0B 06 03 55 04 03 13 04   44 75 6B 65 0E 00 00 00  ...U....Duke....
main, READ: TLSv1 Handshake, length = 1776
```

The data is unpackaged, and if the message is in the SSL/TLS format, it is parsed into a ServerHello. If you connected to a non-SSL/TLS socket (plaintext?), the received data will not be in SSL/TLS format, and you'll have problems connecting.

The ServerHello specifies several things:

- The server's random data, also used to initialize the cryptographic algorithms,
- the identifier of this session (if the client wants to try to rejoin this session using a different connection, it can send this ID in its ClientHello. If the client session ID equals the server session ID, an abbreviated handshake takes place, and the previously established parameters are used),
- the selected cipher suite,
- and the compression method (none in this case).

Lastly note that the ServerHello has specified that the connection should use "TLSv1", rather than "SSLv3."

```
*** ServerHello, TLSv1
RandomCookie:  GMT: 1073492240 bytes = { 121, 171, 23, 102, 250, 139, 63,
170, 253, 94, 72, 35, 250, 144, 49, 216, 60, 185, 163, 44, 140, 245, 233,
129, 155, 162, 99, 108 }
Session ID:  {64, 252, 49, 16, 189, 141, 165, 145, 6, 139, 225, 230, 128,
198, 90, 92, 217, 141, 10, 174, 202, 88, 74, 186, 54, 177, 61, 4, 141, 130,
33, 180}
Cipher Suite: SSL_RSA_WITH_RC4_128_MD5
Compression Method: 0
***
%% Created:  [Session-1, SSL_RSA_WITH_RC4_128_MD5]
** SSL_RSA_WITH_RC4_128_MD5
[read] MD5 and SHA1 hashes:  len = 74
0000: 02 00 00 46 03 01 40 FC   31 10 79 AB 17 66 FA 8B  ...F..@.1.y..f..
0010: 3F AA FD 5E 48 23 FA 90   31 D8 3C B9 A3 2C 8C F5  ?..^H#..1.<..,..
0020: E9 81 9B A2 63 6C 20 40   FC 31 10 BD 8D A5 91 06  ....cl @.1......
0030: 8B E1 E6 80 C6 5A 5C D9   8D 0A AE CA 58 4A BA 36  .....Z\.....XJ.6
0040: B1 3D 04 8D 82 21 B4 00   04 00                    .=...!....
```

The server next identifies itself to the client by passing a Certificate chain. In this example, we have a certificate for the subject "bongos", signed by the issuer "JSSE Test CA". We know that "JSSE Test CA" is a trusted CA, so if the certificate chain verifies correctly by our X509TrustManager, we can accept this connection.

There are many different ways of establishing trust, so if the default X509TrustManager is not doing the types of trust management you need, you can supply your own X509TrustManager to the SSLContext.

```
*** Certificate chain
chain [0] = [
[
  Version: V3
  Subject:
  CN=bongos, OU=Java, O=Sun, ST=CA, C=US
  Signature Algorithm: MD5withRSA, OID = 1.2.840.113549.1.1.4
```

```
  Key:  Sun RSA public key, 1024 bits
  modulus: 14327961070042705070421670273499528365070663811882665735630808 7
  6825527511655401266650701950067469181937023139008360638020454483927712 74
  4630883451578086701901220171538216429856302880176292949308004459397211 28
  7352506685156197369336485485120479417080181309269859368945120633978166 02
  6238679764747637831108662589 71
  public exponent: 65537
  Validity: [From: Mon Jul 19 13:30:51 PDT 2004,
              To: Fri Dec 05 12:30:51 PST 2031]
  Issuer: CN=JSSE Test CA, OU=JWS, O=Sun,
      L=Santa Clara, ST=CA, C=US
  SerialNumber: [    01]

Certificate Extensions: 3

[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 58 D7 3A A9 37 AA 3E 14   27 FC EC CC 45 08 04 8E  X.:.7.>.'...E...
0010: 2A 8B 77 28                                        *.w(
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 08 A3 7E 35 96 15 FA B0   F5 1B 5F CD 4F 54 EF 31  ...5......_.OT.1
0010: 33 70 E4 A7                                        3p..
]

[CN=JSSE Test CA, OU=JWS, O=Sun, L=Santa Clara, ST=CA, C=US]
SerialNumber: [    00]
]

[3]: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
CA:false
PathLen: undefined
]

]
  Algorithm: [MD5withRSA]
  Signature:
0000: 05 3E 17 DA F2 05 CB 4E   9E BF 12 CE 13 76 FF B2  .>.....N.....v..
0010: FB 7F 9C 3D 45 28 43 6C   98 28 E3 92 17 C2 C6 F1  ...=E(Cl.(......
0020: 62 CA 60 C2 B0 EC E6 7E   4C 2F C2 40 FE 06 CB 34  b.`.....L/.@...4
0030: 60 B1 F4 26 1C E8 46 39   24 E1 8A 71 F2 13 90 A4  `..&..F9$..q....
0040: 0A 7B 0B 13 AB 51 68 53   D9 7A 31 5A C1 7E 3C 44  .....QhS.z1Z..a.)
0060: A3 31 46 02 C6 D2 8C 27   79 40 76 97 B6 25 19 BE  .1F....'y@v..%..
0070: 6C 6A 92 DC EF 11 BE E7   4A FF 2A E6 D6 AC 39 31  lj......J.*...91

]
chain [1] = [
[
  Version: V3
  Subject: CN=JSSE Test CA, OU=JWS, O=Sun,
      L=Santa Clara, ST=CA, C=US
  Signature Algorithm: MD5withRSA, OID = 1.2.840.113549.1.1.4

  Key:  Sun RSA public key, 1024 bits
  modulus: 10817186131493429492364685225820109325361946029981813523048104 0
  6159230251491951681404582386292517269502203988897225907405520797828645 77
  9768386917518414496799016441833172038241438039400378831991937758399347 67
  3045603138417168692847457691572930131882466015632719598242900730951507 30
  5053290119569861456365209931 69
```

```
  public exponent: 65537
  Validity: [From: Mon Jul 19 13:30:15 PDT 2004,
              To: Fri Dec 05 12:30:15 PST 2031]
  Issuer: CN=JSSE Test CA, OU=JWS, O=Sun,
      L=Santa Clara, ST=CA, C=US
  SerialNumber: [    00]

Certificate Extensions: 3
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 08 A3 7E 35 96 15 FA B0   F5 1B 5F CD 4F 54 EF 31  ...5......_.OT.1
0010: 33 70 E4 A7                                        3p..
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 08 A3 7E 35 96 15 FA B0   F5 1B 5F CD 4F 54 EF 31  ...5......_.OT.1
0010: 33 70 E4 A7                                        3p..
]

[CN=JSSE Test CA, OU=JWS, O=Sun, L=Santa Clara, ST=CA, C=US]
SerialNumber: [    00]
]

[3]: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
CA:true
PathLen:2147483647
]

]
  Algorithm: [MD5withRSA]
  Signature:
0000: 73 6A 46 A2 05 E3 D8 6E   5C F4 18 A2 74 BC CF EB  sjF....n\...t...
0010: 0C 5B FF 81 1C 28 85 C7   FA E4 ED 5C 4F 71 22 FB  .[...(.....\Oq".
0020: 26 E3 01 3D 0C 10 AA BB   3E 90 ED 0E 1F 0C 9B B1  &..=....>.......
0030: 8C 49 6A 51 E4 C3 52 D6   FB 42 6C B4 A9 A9 57 A5  .IjQ..R..Bl...W.
0040: 84 00 42 6D 37 37 6D C7   6C 23 BC DC 60 D1 9D 6F  ..Bm77m.l#..`..o
0050: B3 75 47 3A 15 33 1A EC   90 09 9D F9 EB BD 88 96  .uG:.3..........
0060: E7 1D 41 BC 01 8D CA 88   D9 5B 04 09 8F 3E EA C8  ..A......[...>..
0070: 15 A0 AA 4E 85 95 AE 2F   0E 31 92 AC 3C FB 2F C4  ...N.../.1..<./.

]
```

We recoginise this cert! We can trust it, and continue on with the handshake.

```
***
Found trusted certificate:
[
[
  Version: V3
  Subject: CN=JSSE Test CA, OU=JWS, O=Sun, L=Santa Clara, ST=CA, C=US
  Signature Algorithm: MD5withRSA, OID = 1.2.840.113549.1.1.4

  Key:  Sun RSA public key, 1024 bits
  modulus: 108171861314934294923646852258201093253619460299818135230481040
  615923025149195168140458238629251726950220398889722590740552079782864577
  976838691751841449679901644183317203824143803940037883199193775839934767
  304560313841716869284745769157293013188246601563271959824290073095150730
  505329011956986145636520993169
  public exponent: 65537
```

```
  Validity: [From: Mon Jul 19 13:30:15 PDT 2004,
              To: Fri Dec 05 12:30:15 PST 2031]
  Issuer: CN=JSSE Test CA, OU=JWS, O=Sun, L=Santa Clara, ST=CA, C=US
  SerialNumber: [    00]

Certificate Extensions: 3
[1]: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 08 A3 7E 35 96 15 FA B0   F5 1B 5F CD 4F 54 EF 31  ...5......_.OT.1
0010: 33 70 E4 A7                                        3p..
]
]

[2]: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 08 A3 7E 35 96 15 FA B0   F5 1B 5F CD 4F 54 EF 31  ...5......_.OT.1
0010: 33 70 E4 A7                                        3p..
]

[CN=JSSE Test CA, OU=JWS, O=Sun, L=Santa Clara, ST=CA, C=US]
SerialNumber: [    00]
]

[3]: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
CA:true
PathLen:2147483647
]

]
  Algorithm: [MD5withRSA]
  Signature:
0000: 73 6A 46 A2 05 E3 D8 6E   5C F4 18 A2 74 BC CF EB  sjF....n\...t...
0010: 0C 5B FF 81 1C 28 85 C7   FA E4 ED 5C 4F 71 22 FB  .[...(.....\Oq".
0020: 26 E3 01 3D 0C 10 AA BB   3E 90 ED 0E 1F 0C 9B B1  &..=....>.......
0030: 8C 49 6A 51 E4 C3 52 D6   FB 42 6C B4 A9 A9 57 A5  .IjQ..R..Bl...W.
0040: 84 00 42 6D 37 37 6D C7   6C 23 BC DC 60 D1 9D 6F  ..Bm77m.l#..`..o
0050: B3 75 47 3A 15 33 1A EC   90 09 9D F9 EB BD 88 96  .uG:.3..........
0060: E7 1D 41 BC 01 8D CA 88   D9 5B 04 09 8F 3E EA C8  ..A......[...>..
0070: 15 A0 AA 4E 85 95 AE 2F   0E 31 92 AC 3C FB 2F C4  ...N.../.1..<./.

]
```

We read the next few bytes of the handshake...

```
[read] MD5 and SHA1 hashes:  len = 1567
0000: 0B 00 06 1B 00 06 18 00   03 11 30 82 03 0D 30 82  ..........0...0.
0010: 02 76 A0 03 02 01 02 02   01 01 30 0D 06 09 2A 86  .v........0...*.
0020: 48 86 F7 0D 01 01 04 05   00 30 63 31 0B 30 09 06  H........0c1.0..
0030: 03 55 04 06 13 02 55 53   31 0B 30 09 06 03 55 04  .U....US1.0...U.
0040: 08 13 02 43 41 31 14 30   12 06 03 55 04 07 13 0B  ...CA1.0...U....
0050: 53 61 6E 74 61 20 43 6C   61 72 61 31 0C 30 0A 06  Santa Clara1.0..
0060: 03 55 04 0A 13 03 53 75   6E 31 0C 30 0A 06 03 55  .U....Sun1.0...U
0070: 04 0B 13 03 4A 57 53 31   15 30 13 06 03 55 04 03  ....JWS1.0...U..
0080: 13 0C 4A 53 53 45 20 54   65 73 74 20 43 41 30 1E  ..JSSE Test CA0.
0090: 17 0D 30 34 30 37 31 39   32 30 33 30 35 31 5A 17  ..040719203051Z.
00A0: 0D 33 31 31 32 30 35 32   30 33 30 35 31 5A 30 48  .311205203051Z0H
00B0: 31 0B 30 09 06 03 55 04   06 13 02 55 53 31 0B 30  1.0...U....US1.0
00C0: 09 06 03 55 04 08 13 02   43 41 31 0C 30 0A 06 03  ...U....CA1.0...
00D0: 55 04 0A 13 03 53 75 6E   31 0D 30 0B 06 03 55 04  U....Sun1.0...U.
00E0: 0B 13 04 4A 61 76 61 31   0F 30 0D 06 03 55 04 03  ...Java1.0...U..
00F0: 13 06 62 6F 6E 67 6F 73   30 81 9F 30 0D 06 09 2A  ..bongos0..0...*
```

```
0100: 86 48 86 F7 0D 01 01 01   05 00 03 81 8D 00 30 81  .H............0.
0110: 89 02 81 81 00 CC 09 74   CB 43 AB 6D ED F6 35 AA  .......t.C.m..5.
0120: 0E 49 29 D9 E0 F0 A1 D5   E2 3E 8F 5E C5 CE F4 DE  .I).....>.^....
0130: C1 A4 F3 CB 8C 45 0B 0F   6E 21 E1 00 65 CB 3C D1  .....E..n!..e.<.
0140: 5C EF 6A FB 5D 96 93 F4   71 41 41 45 FF 37 86 4C  \.j.]...qAAE.7.L
0150: AB F9 EA 9A 3F A5 82 60   BF 0A 81 84 C9 3E AC 0F  ....?..`.....>..
0160: 3D 20 3D AC A0 69 EF CA   4A A7 94 AD C8 A5 CE 37  = =..i..J......7
0170: 66 52 D1 25 43 CB 10 44   07 1E 93 74 D9 68 01 D7  fR.%C..D...t.h..
0180: 06 48 C9 0D 52 2D D5 6A   2E A6 48 4C 59 E2 5C C6  .H..R-.j..HLY.\.
0190: C1 5C C8 4C 1B 02 03 01   00 01 A3 81 EB 30 81 E8  .\.L.........0..
01A0: 30 09 06 03 55 1D 13 04   02 30 00 30 2C 06 09 60  0...U....0.0,..`
01B0: 86 48 01 86 F8 42 01 0D   04 1F 16 1D 4F 70 65 6E  .H...B......Open
01C0: 53 53 4C 20 47 65 6E 65   72 61 74 65 64 20 43 65  SSL Generated Ce
01D0: 72 74 69 66 69 63 61 74   65 30 1D 06 03 55 1D 0E  rtificate0...U..
01E0: 04 16 04 14 58 D7 3A A9   37 AA 3E 14 27 FC EC CC  ....X.:.7.>.'...
01F0: 45 08 04 8E 2A 8B 77 28   30 81 8D 06 03 55 1D 23  E...*.w(0....U.#
0200: 04 81 85 30 81 82 80 14   08 A3 7E 35 96 15 FA B0  ...0.......5....
0210: F5 1B 5F CD 4F 54 EF 31   33 70 E4 A7 A1 67 A4 65  .._.OT.13p...g.e
0220: 30 63 31 0B 30 09 06 03   55 04 06 13 02 55 53 31  0c1.0...U....US1
0230: 0B 30 09 06 03 55 04 08   13 02 43 41 31 14 30 12  .0...U....CA1.0.
0240: 06 03 55 04 07 13 0B 53   61 6E 74 61 20 43 6C 61  ..U....Santa Cla
0250: 72 61 31 0C 30 0A 06 03   55 04 0A 13 03 53 75 6E  ra1.0...U....Sun
0260: 31 0C 30 0A 06 03 55 04   0B 13 03 4A 57 53 31 15  1.0...U....JWS1.
0270: 30 13 06 03 55 04 03 13   0C 4A 53 53 45 20 54 65  0...U....JSSE Te
0280: 73 74 20 43 41 82 01 00   30 0D 06 09 2A 86 48 86  st CA...0...*.H.
0290: F7 0D 01 01 04 05 00 03   81 81 00 05 3E 17 DA F2  ............>...
02A0: 05 CB 4E 9E BF 12 CE 13   76 FF B2 FB 7F 9C 3D 45  ..N.....v.....=E
02B0: 28 43 6C 98 28 E3 92 17   C2 C6 F1 62 CA 60 C2 B0  (Cl.(......b.`..
02C0: EC E6 7E 4C 2F C2 40 FE   06 CB 34 60 B1 F4 26 1C  ...L/.@...4`..&.
02D0: E8 46 39 24 E1 8A 71 F2   13 90 A4 0A 7B 0B 13 AB  .F9$..q.........
02E0: 51 68 53 D9 7A 31 5A C1   7E 3C 44 2C 49 70 57 25  QhS.z1Z..a.).1F..
0300: D2 8C 27 79 40 76 97 B6   25 19 BE 6C 6A 92 DC EF  ..'y@v..%..lj...
0310: 11 BE E7 4A FF 2A E6 D6   AC 39 31 00 03 01 30 82  ...J.*...91...0.
0320: 02 FD 30 82 02 66 A0 03   02 01 02 02 01 00 30 0D  ..0..f........0.
0330: 06 09 2A 86 48 86 F7 0D   01 01 04 05 00 30 63 31  ..*.H........0c1
0340: 0B 30 09 06 03 55 04 06   13 02 55 53 31 0B 30 09  .0...U....US1.0.
0350: 06 03 55 04 08 13 02 43   41 31 14 30 12 06 03 55  ..U....CA1.0...U
0360: 04 07 13 0B 53 61 6E 74   61 20 43 6C 61 72 61 31  ....Santa Clara1
0370: 0C 30 0A 06 03 55 04 0A   13 03 53 75 6E 31 0C 30  .0...U....Sun1.0
0380: 0A 06 03 55 04 0B 13 03   4A 57 53 31 15 30 13 06  ...U....JWS1.0..
0390: 03 55 04 03 13 0C 4A 53   53 45 20 54 65 73 74 20  .U....JSSE Test
03A0: 43 41 30 1E 17 0D 30 34   30 37 31 39 32 30 33 30  CA0...0407192030
03B0: 31 35 5A 17 0D 33 31 31   32 30 35 32 30 33 30 31  15Z..31120520301
03C0: 35 5A 30 63 31 0B 30 09   06 03 55 04 06 13 02 55  5Z0c1.0...U....U
03D0: 53 31 0B 30 09 06 03 55   04 08 13 02 43 41 31 14  S1.0...U....CA1.
03E0: 30 12 06 03 55 04 07 13   0B 53 61 6E 74 61 20 43  0...U....Santa C
03F0: 6C 61 72 61 31 0C 30 0A   06 03 55 04 0A 13 03 53  lara1.0...U....S
0400: 75 6E 31 0C 30 0A 06 03   55 04 0B 13 03 4A 57 53  un1.0...U....JWS
0410: 31 15 30 13 06 03 55 04   03 13 0C 4A 53 53 45 20  1.0...U....JSSE
0420: 54 65 73 74 20 43 41 30   81 9F 30 0D 06 09 2A 86  Test CA0..0...*.
0430: 48 86 F7 0D 01 01 01 05   00 03 81 8D 00 30 81 89  H............0..
0440: 02 81 81 00 9A 0A B6 45   66 D5 DE 4A D9 3C 8C AC  .......Ef..J.<..
0450: A6 B5 A5 88 B4 CF 14 E1   A6 1B 25 25 4F 44 C9 1F  ..........%%OD..
0460: 22 38 32 29 CF A1 7C 18   30 93 DC 2B EC 2B 67 EE  "82)....0..+.+g.
0470: 2E 08 66 2D 0F 47 E0 12   3A DC E0 03 E9 65 16 F6  ..f-.G..:....e..
0480: 18 C6 16 14 56 24 55 7D   32 3E F9 66 A2 DD 55 EB  ....V$U.2>.f..U.
0490: 4D 0A 67 C7 5D 21 9B 29   EA 2E 51 C5 83 A3 55 FF  M.g.]!.)..Q...U.
04A0: 35 CA A6 99 8F 46 F8 8E   56 BB A2 B1 39 83 D8 61  5....F..V...9..a
04B0: 42 79 E0 95 78 FA C6 E3   65 B0 FD 74 2D 64 51 71  By..x...e..t-dQq
04C0: 04 F2 A1 91 02 03 01 00   01 A3 81 C0 30 81 BD 30  ............0..0
04D0: 1D 06 03 55 1D 0E 04 16   04 14 08 A3 7E 35 96 15  ...U.........5..
04E0: FA B0 F5 1B 5F CD 4F 54   EF 31 33 70 E4 A7 30 81  ...._.OT.13p..0.
04F0: 8D 06 03 55 1D 23 04 81   85 30 81 82 80 14 08 A3  ...U.#...0......
0500: 7E 35 96 15 FA B0 F5 1B   5F CD 4F 54 EF 31 33 70  .5......_.OT.13p
0510: E4 A7 A1 67 A4 65 30 63   31 0B 30 09 06 03 55 04  ...g.e0c1.0...U.
```

```
0520: 06 13 02 55 53 31 0B 30   09 06 03 55 04 08 13 02  ...US1.0...U....
0530: 43 41 31 14 30 12 06 03   55 04 07 13 0B 53 61 6E  CA1.0...U....San
0540: 74 61 20 43 6C 61 72 61   31 0C 30 0A 06 03 55 04  ta Clara1.0...U.
0550: 0A 13 03 53 75 6E 31 0C   30 0A 06 03 55 04 0B 13  ...Sun1.0...U...
0560: 03 4A 57 53 31 15 30 13   06 03 55 04 03 13 0C 4A  .JWS1.0...U....J
0570: 53 53 45 20 54 65 73 74   20 43 41 82 01 00 30 0C  SSE Test CA...0.
0580: 06 03 55 1D 13 04 05 30   03 01 01 FF 30 0D 06 09  ..U....0....0...
0590: 2A 86 48 86 F7 0D 01 01   04 05 00 03 81 81 00 73  *.H............s
05A0: 6A 46 A2 05 E3 D8 6E 5C   F4 18 A2 74 BC CF EB 0C  jF....n\...t....
05B0: 5B FF 81 1C 28 85 C7 FA   E4 ED 5C 4F 71 22 FB 26  [...(.....\Oq".&
05C0: E3 01 3D 0C 10 AA BB 3E   90 ED 0E 1F 0C 9B B1 8C  ..=....>........
05D0: 49 6A 51 E4 C3 52 D6 FB   42 6C B4 A9 A9 57 A5 84  IjQ..R..Bl...W..
05E0: 00 42 6D 37 37 6D C7 6C   23 BC DC 60 D1 9D 6F B3  .Bm77m.l#..`..o.
05F0: 75 47 3A 15 33 1A EC 90   09 9D F9 EB BD 88 96 E7  uG:.3...........
0600: 1D 41 BC 01 8D CA 88 D9   5B 04 09 8F 3E EA C8 15  .A......[...>...
0610: A0 AA 4E 85 95 AE 2F 0E   31 92 AC 3C FB 2F C4     ..N.../.1..<./.
```

...and parse it to find that it's a CertificateRequest message.

The server is asking the client to identify itself with a X509 certificate subject having the common name (CN=) "Duke". The server's X509TrustManager has the option of rejecting any credentials provided by the client (or lack thereof). In a real-world situation, you'd probably use a certificate signed by a CA, and the list of trusted CA's would be included in this message instead.

Lastly, we receive the ServerHelloDone message, which signals to the client that the server has finished sending its part of the handshake.

```
*** CertificateRequest
Cert Types: RSA, DSS,
Cert Authorities:
CN=Duke, OU= , O="Oracle and/or its affiliates.",
L=Cupertino, ST=CA, C=US>
[read] MD5 and SHA1 hashes:  len = 131
0000: 0D 00 00 7F 02 01 02 00   7A 00 78 30 76 31 0B 30  ........z.x0v1.0
0010: 09 06 03 55 04 06 13 02   55 53 31 0B 30 09 06 03  ...U....US1.0...
0020: 55 04 08 13 02 43 41 31   12 30 10 06 03 55 04 07  U....CA1.0...U..
0030: 13 09 43 75 70 65 72 74   69 6E 6F 31 1F 30 1D 06  ..Cupertino1.0..
0040: 03 55 04 0A 13 16 53 75   6E 20 4D 69 63 72 6F 73  .U....Sun Micros
0050: 79 73 74 65 6D 73 2C 20   49 6E 63 2E 31 16 30 14  ystems, Inc.1.0.
0060: 06 03 55 04 0B 13 0D 4A   61 76 61 20 53 6F 66 74  ..U....Java Soft
0070: 77 61 72 65 31 0D 30 0B   06 03 55 04 03 13 04 44  ware1.0...U....D
0080: 75 6B 65                                           uke
*** ServerHelloDone
[read] MD5 and SHA1 hashes:  len = 4
0000: 0E 00 00 00                                        ....
```

We need to send client credentials back to the server, so the client's X509KeyManager is now consulted. We look for a match between the list of accepted issuers (above), and the certificates we have in our KeyStore. In this case (luckily?), there is a match: we have credentials for "duke". It's now up to the server's X509TrustManager to decide whether to accept these credentials.

```
matching alias: duke
*** Certificate chain
chain [0] = [
[
  Version: V1
  Subject: CN=Duke, OU= , O="Oracle and/or its affiliates.",
  L=Cupertino, ST=CA, C=US
  Signature Algorithm: MD5withRSA, OID = 1.2.840.113549.1.1.4

  Key:  Sun RSA public key, 1024 bits
  modulus: 134968166047563266914058280571444028986498087544923991226919517
```

```
  667593269213420979048109900052353578998293280426361122296881234393722020
  704208851688212064483570055963805034839797994154526862998272017486468599
  962268346037652120279791547218281230795146025359480589335682217749874703
  510467348902637769973696151441
  public exponent: 65537
  Validity: [From: Tue May 22 16:46:46 PDT 2001,
              To: Sun May 22 16:46:46 PDT 2011]
  Issuer: CN=Duke, OU= , O="Oracle and/or its affiliates.",
  L=Cupertino, ST=CA, C=US
  SerialNumber: [    3b0afa66]

]
  Algorithm: [MD5withRSA]
  Signature:
0000: 5F B5 62 E9 A0 26 1D 8E   A2 7E 7C 02 08 36 3A 3E  _.b..&.......6:>
0010: C9 C2 45 03 DD F9 BC 06   FC 25 CF 30 92 91 B1 4E  ..E......%.0...N
0020: 62 17 08 48 14 68 80 CF   DD 89 11 EA 92 7F CE DD  b..H.h..........
0030: B4 FD 12 A8 71 C7 9E D7   C3 D0 E3 BD BB DE 20 92  ....q......... .
0040: C2 3B C8 DE CB 25 23 C0   8B B6 92 B9 0B 64 80 63  .;...%#......d.c
0050: D9 09 25 2D 7A CF 0A 31   B6 E9 CA C1 37 93 BC 0D  ..%-z..1....7...
0060: 4E 74 95 4F 58 31 DA AC   DF D8 BD 89 BD AF EC C8  Nt.OX1..........
0070: 2D 18 A2 BC B2 15 4F B7   28 6F D3 00 E1 72 9B 6C  -.....O.(o...r.l

]
***
```

In the case of this particular cipher suite, we must now pass a message called a ClientKeyExchange, which helps establish a shared secret between the two parties.

All of this data is eventually collected and written to the raw device.

```
*** ClientKeyExchange, RSA PreMasterSecret, TLSv1
Random Secret:  { 3, 1, 132, 84, 245, 214, 235, 245, 168, 8, 186, 250,
122, 34, 97, 45, 117, 220, 64, 232, 152, 249, 14, 178, 135, 128, 184,
26, 143, 104, 37, 184, 81, 208, 84, 69, 97, 138, 80, 201, 187, 14, 57,
83, 69, 120, 190, 121 }
[write] MD5 and SHA1 hashes:  len = 754
0000: 0B 00 02 68 00 02 65 00   02 62 30 82 02 5E 30 82  ...h..e..b0..^0.
0010: 01 C7 02 04 3B 0A FA 66   30 0D 06 09 2A 86 48 86  ....;..f0...*.H.
0020: F7 0D 01 01 04 05 00 30   76 31 0B 30 09 06 03 55  .......0v1.0...U
0030: 04 06 13 02 55 53 31 0B   30 09 06 03 55 04 08 13  ....US1.0...U...
0040: 02 43 41 31 12 30 10 06   03 55 04 07 13 09 43 75  .CA1.0...U....Cu
0050: 70 65 72 74 69 6E 6F 31   1F 30 1D 06 03 55 04 0A  pertino1.0...U..
0060: 13 16 53 75 6E 20 4D 69   63 72 6F 73 79 73 74 65  ..Sun Microsyste
0070: 6D 73 2C 20 49 6E 63 2E   31 16 30 14 06 03 55 04  ms, Inc.1.0...U.
0080: 0B 13 0D 4A 61 76 61 20   53 6F 66 74 77 61 72 65  ...
0090: 31 0D 30 0B 06 03 55 04   03 13 04 44 75 6B 65 30  1.0...U....Duke0
00A0: 1E 17 0D 30 31 30 35 32   32 32 33 34 36 34 36 5A  ...010522234646Z
00B0: 17 0D 31 31 30 35 32 32   32 33 34 36 34 36 5A 30  ..110522234646Z0
00C0: 76 31 0B 30 09 06 03 55   04 06 13 02 55 53 31 0B  v1.0...U....US1.
00D0: 30 09 06 03 55 04 08 13   02 43 41 31 12 30 10 06  0...U....CA1.0..
00E0: 03 55 04 07 13 09 43 75   70 65 72 74 69 6E 6F 31  .U....Cupertino1
00F0: 1F 30 1D 06 03 55 04 0A   13 16 53 75 6E 20 4D 69  .0...U....Sun Mi
0100: 63 72 6F 73 79 73 74 65   6D 73 2C 20 49 6E 63 2E  crosystems, Inc.
0110: 31 16 30 14 06 03 55 04   0B 13 0D 4A 61 76 61 20  1.0...U....Java
0120: 53 6F 66 74 77 61 72 65   31 0D 30 0B 06 03 55 04  Software1.0...U.
0130: 03 13 04 44 75 6B 65 30   81 9F 30 0D 06 09 2A 86  ...Duke0..0...*.
0140: 48 86 F7 0D 01 01 01 05   00 03 81 8D 00 30 81 89  H............0..
0150: 02 81 81 00 C0 33 77 E7   1F D0 CE CE BD 43 2F 8D  .....3w......C/.
0160: EB C6 D3 07 A9 00 F5 75   4D C8 4B 04 52 42 EE 69  .......uM.K.RB.i
0170: F3 30 E9 A0 C6 07 B7 C8   55 2D B9 5B 57 7A 4C AD  .0......U-.[WzL.
0180: 1A 30 63 5C 7D 6D 16 BF   ED 54 13 49 8A 1B E6 29  .0c\.m...T.I...)
0190: 26 20 85 F9 5E 2B 2F A7   12 9C 98 2D 83 F6 EE B1  & ..^+/....-....
01A0: 85 68 DA B5 8E 4C 1D 2D   8E 21 97 B0 30 C8 3A 57  .h...L.-.!..0.:W
```

```
01B0: F4 E1 18 9E F6 98 B2 D5   3D 8E D5 2B 09 E2 E1 A0  ........=..+....
01C0: 49 C1 A6 43 CE EA 57 7F   3B 5C 3A C9 BA DB B7 F0  I..C..W.;\:.....
01D0: 89 69 BF 91 02 03 01 00   01 30 0D 06 09 2A 86 48  .i.......0...*.H
01E0: 86 F7 0D 01 01 04 05 00   03 81 81 00 5F B5 62 E9  ............_.b.
01F0: A0 26 1D 8E A2 7E 7C 02   08 36 3A 3E C9 C2 45 03  .&.......6:>..E.
0200: DD F9 BC 06 FC 25 CF 30   92 91 B1 4E 62 17 08 48  .....%.0...Nb..H
0210: 14 68 80 CF DD 89 11 EA   92 7F CE DD B4 FD 12 A8  .h..............
0220: 71 C7 9E D7 C3 D0 E3 BD   BB DE 20 92 C2 3B C8 DE  q.........  ..;..
0230: CB 25 23 C0 8B B6 92 B9   0B 64 80 63 D9 09 25 2D  .%#......d.c..%-
0240: 7A CF 0A 31 B6 E9 CA C1   37 93 BC 0D 4E 74 95 4F  z..1....7...Nt.O
0250: 58 31 DA AC DF D8 BD 89   BD AF EC C8 2D 18 A2 BC  X1..........-...
0260: B2 15 4F B7 28 6F D3 00   E1 72 9B 6C 10 00 00 82  ..O.(o...r.l....
0270: 00 80 4E DD E7 77 F1 91   6B 31 4E FA D6 61 D9 69  ..N..w..k1N..a.i
0280: 82 BD 22 40 83 FD 76 E6   FF A7 18 95 A0 04 28 0D  ..."@..v.......(.
0290: 0D F7 44 6F 0C 42 4F 17   77 A0 99 56 2A 13 77 28  ..Do.BO.w..V*.w(
02A0: 0B 09 48 C1 B9 8C 09 ED   9F C6 2E 32 18 DB BD ED  ..H........2....
02B0: AF C3 AB E7 AD 8F DF 9E   AB 07 43 B4 50 EF 74 98  ..........C.P.t.
02C0: EA FC E8 4D C9 DA FC B0   B2 C7 D4 83 50 B5 84 B8  ...M........P...
02D0: 44 86 7B 5D 8A C2 F8 04   80 06 E6 84 42 33 B2 EE  D..]........B3..
02E0: 05 E6 D3 48 0E 23 E5 1F   63 4C 53 98 B8 8C 45 BA  ...H.#..cLS...E.
02F0: C8 19                                              ..
main, WRITE: TLSv1 Handshake, length = 754
[Raw write]: length = 759
0000: 16 03 01 02 F2 0B 00 02   68 00 02 65 00 02 62 30  ........h..e..b0
0010: 82 02 5E 30 82 01 C7 02   04 3B 0A FA 66 30 0D 06  ..^0.....;..f0..
0020: 09 2A 86 48 86 F7 0D 01   01 04 05 00 30 76 31 0B  .*.H........0v1.
0030: 30 09 06 03 55 04 06 13   02 55 53 31 0B 30 09 06  0...U....US1.0..
0040: 03 55 04 08 13 02 43 41   31 12 30 10 06 03 55 04  .U....CA1.0...U.
0050: 07 13 09 43 75 70 65 72   74 69 6E 6F 31 1F 30 1D  ...Cupertino1.0.
0060: 06 03 55 04 0A 13 16 53   75 6E 20 4D 69 63 72 6F  ..U....Sun Micro
0070: 73 79 73 74 65 6D 73 2C   20 49 6E 63 2E 31 16 30  systems, Inc.1.0
0080: 14 06 03 55 04 0B 13 0D   4A 61 76 61 20 53 6F 66  ...U....Java Sof
0090: 74 77 61 72 65 31 0D 30   0B 06 03 55 04 03 13 04  tware1.0...U....
00A0: 44 75 6B 65 30 1E 17 0D   30 31 30 35 32 32 32 33  Duke0...01052223
00B0: 34 36 34 36 5A 17 0D 31   31 30 35 32 32 32 33 34  4646Z..110522234
00C0: 36 34 36 5A 30 76 31 0B   30 09 06 03 55 04 06 13  646Z0v1.0...U...
00D0: 02 55 53 31 0B 30 09 06   03 55 04 08 13 02 43 41  .US1.0...U....CA
00E0: 31 12 30 10 06 03 55 04   07 13 09 43 75 70 65 72  1.0...U....Cuper
00F0: 74 69 6E 6F 31 1F 30 1D   06 03 55 04 0A 13 16 53  tino1.0...U....S
0100: 75 6E 20 4D 69 63 72 6F   73 79 73 74 65 6D 73 2C  un Microsystems,
0110: 20 49 6E 63 2E 31 16 30   14 06 03 55 04 0B 13 0D   Inc.1.0...U....
0120: 4A 61 76 61 20 53 6F 66   74 77 61 72 65 31 0D 30   1.0
0130: 0B 06 03 55 04 03 13 04   44 75 6B 65 30 81 9F 30  ...U....Duke0..0
0140: 0D 06 09 2A 86 48 86 F7   0D 01 01 01 05 00 03 81  ...*.H..........
0150: 8D 00 30 81 89 02 81 81   00 C0 33 77 E7 1F D0 CE  ..0.......3w....
0160: CE BD 43 2F 8D EB C6 D3   07 A9 00 F5 75 4D C8 4B  ..C/........uM.K
0170: 04 52 42 EE 69 F3 30 E9   A0 C6 07 B7 C8 55 2D B9  .RB.i.0......U-.
0180: 5B 57 7A 4C AD 1A 30 63   5C 7D 6D 16 BF ED 54 13  [WzL..0c\.m...T.
0190: 49 8A 1B E6 29 26 20 85   F9 5E 2B 2F A7 12 9C 98  I...)& ..^+/....
01A0: 2D 83 F6 EE B1 85 68 DA   B5 8E 4C 1D 2D 8E 21 97  -.....h...L.-.!.
01B0: B0 30 C8 3A 57 F4 E1 18   9E F6 98 B2 D5 3D 8E D5  .0.:W........=..
01C0: 2B 09 E2 E1 A0 49 C1 A6   43 CE EA 57 7F 3B 5C 3A  +....I..C..W.;\:
01D0: C9 BA DB B7 F0 89 69 BF   91 02 03 01 00 01 30 0D  ......i.......0.
01E0: 06 09 2A 86 48 86 F7 0D   01 01 04 05 00 03 81 81  ..*.H...........
01F0: 00 5F B5 62 E9 A0 26 1D   8E A2 7E 7C 02 08 36 3A  ._.b..&.......6:
0200: 3E C9 C2 45 03 DD F9 BC   06 FC 25 CF 30 92 91 B1  >..E......%.0...
0210: 4E 62 17 08 48 14 68 80   CF DD 89 11 EA 92 7F CE  Nb..H.h.........
0220: DD B4 FD 12 A8 71 C7 9E   D7 C3 D0 E3 BD BB DE 20  .....q.........
0230: 92 C2 3B C8 DE CB 25 23   C0 8B B6 92 B9 0B 64 80  ..;...%#......d.
0240: 63 D9 09 25 2D 7A CF 0A   31 B6 E9 CA C1 37 93 BC  c..%-z..1....7..
0250: 0D 4E 74 95 4F 58 31 DA   AC DF D8 BD 89 BD AF EC  .Nt.OX1.........
0260: C8 2D 18 A2 BC B2 15 4F   B7 28 6F D3 00 E1 72 9B  .-.....O.(o...r.
0270: 6C 10 00 00 82 00 80 4E   DD E7 77 F1 91 6B 31 4E  l......N..w..k1N
0280: FA D6 61 D9 69 82 BD 22   40 83 FD 76 E6 FF A7 18  ..a.i.."@..v....
0290: 95 A0 04 28 0D 0D F7 44   6F 0C 42 4F 17 77 A0 99  ...(...Do.BO.w..
```

```
02A0: 56 2A 13 77 28 0B 09 48   C1 B9 8C 09 ED 9F C6 2E  V*.w(..H........
02B0: 32 18 DB BD ED AF C3 AB   E7 AD 8F DF 9E AB 07 43  2..............C
02C0: B4 50 EF 74 98 EA FC E8   4D C9 DA FC B0 B2 C7 D4  .P.t....M.......
02D0: 83 50 B5 84 B8 44 86 7B   5D 8A C2 F8 04 80 06 E6  .P...D..].......
02E0: 84 42 33 B2 EE 05 E6 D3   48 0E 23 E5 1F 63 4C 53  .B3.....H.#..cLS
02F0: 98 B8 8C 45 BA C8 19                               ...E...
```

At this point, we have everything we need to generate the actual secrets.

```
SESSION KEYGEN:
PreMaster Secret:
0000: 03 01 84 54 F5 D6 EB F5   A8 08 BA FA 7A 22 61 2D  ...T........z"a-
0010: 75 DC 40 E8 98 F9 0E B2   87 80 B8 1A 8F 68 25 B8  u.@..........h%.
0020: 51 D0 54 45 61 8A 50 C9   BB 0E 39 53 45 78 BE 79  Q.TEa.P...9SEx.y
CONNECTION KEYGEN:
Client Nonce:
0000: 40 FC 30 AE 2D 63 84 BB   C5 4B 27 FD 58 21 CA 90  @.0.-c...K'.X!..
0010: 05 F6 A7 7B 37 BB 72 E1   FC 1D 1B 6A F5 1C C8 9F  ....7.r....j....
Server Nonce:
0000: 40 FC 31 10 79 AB 17 66   FA 8B 3F AA FD 5E 48 23  @.1.y..f..?..^H#
0010: FA 90 31 D8 3C B9 A3 2C   8C F5 E9 81 9B A2 63 6C  ..1.<..,......cl
Master Secret:
0000: B0 00 22 34 59 03 16 B7   7A 6C 56 9B 89 D2 7A CC  .."4Y...zlV...z.
0010: F3 85 55 59 3A 14 76 3D   54 BF EB 3F E0 2F B1 4B  ..UY:.v=T..?./.K
0020: 79 8C 75 A9 78 55 6C 8E   A2 14 60 B7 45 EB 77 B2  y.u.xUl...`.E.w.
Client MAC write Secret:
0000: 85 F0 56 F8 07 1D B1 89   89 D0 E1 33 3C CA 63 F9  ..V........3<.c.
Server MAC write Secret:
0000: 1E 4D D1 D3 0A 78 EE B7   4F EC 15 79 B2 59 18 40  .M...x..O..y.Y.@
Client write key:
0000: 10 D0 D6 C2 D9 B7 62 CB   2C 74 BF 5F 85 3C 6F E7  ......b.,t._.
```

Send a quick confirmation to the server verifying that we know the private key corresponding to the client certificate we just sent.

```
*** CertificateVerify
[write] MD5 and SHA1 hashes:  len = 134
0000: 0F 00 00 82 00 80 45 41   43 4B 47 1D F0 EE D1 14  ......EACKG.....
0010: AE F9 B3 2C 1F B9 FE 7B   3E 91 50 C5 0F F1 57 4F  ...,....>.P...WO
0020: 55 F1 4B C3 79 16 A8 F1   72 6B 10 CA CC 83 02 FC  U.K.y...rk......
0030: 97 3D 04 29 44 4C 58 74   84 94 19 63 BB 8A 2C 78  .=.)DLXt...c..,x
0040: 43 A0 DD 5E 54 52 AA 97   15 92 1C 39 6B 10 2E BF  C..^TR.....9k...
0050: F2 DA AE 2D 8F FB 50 44   9E E2 1F 7D C9 C5 CB A0  ...-..PD........
0060: 31 A0 F9 AA 93 2D 1B 07   1B FA E0 EE 95 E7 88 D7  1....-..........
0070: AD 4A 3A 40 DC FB DF 9E   EB 75 04 14 E2 F2 BB DC  .J:@.....u......
0080: 1B 7E 6E D5 8C 62                                  ..n..b
main, WRITE: TLSv1 Handshake, length = 134
[Raw write]: length = 139
0000: 16 03 01 00 86 0F 00 00   82 00 80 45 41 43 4B 47  ...........EACKG
0010: 1D F0 EE D1 14 AE F9 B3   2C 1F B9 FE 7B 3E 91 50  ........,....>.P
0020: C5 0F F1 57 4F 55 F1 4B   C3 79 16 A8 F1 72 6B 10  ...WOU.K.y...rk.
0030: CA CC 83 02 FC 97 3D 04   29 44 4C 58 74 84 94 19  ......=.)DLXt...
0040: 63 BB 8A 2C 78 43 A0 DD   5E 54 52 AA 97 15 92 1C  c..,xC..^TR.....
0050: 39 6B 10 2E BF F2 DA AE   2D 8F FB 50 44 9E E2 1F  9k......-..PD...
0060: 7D C9 C5 CB A0 31 A0 F9   AA 93 2D 1B 07 1B FA E0  .....1....-.....
0070: EE 95 E7 88 D7 AD 4A 3A   40 DC FB DF 9E EB 75 04  ......J:@.....u.
0080: 14 E2 F2 BB DC 1B 7E 6E   D5 8C 62                 .......n..b
```

Almost finished! Tell the server we're changing to the newly established cipher suite. All further messages will be encrypted using the parameters we just established. We send an encrypted Finished message to verify everything worked.

```
main, WRITE: TLSv1 Change Cipher Spec, length = 1
[Raw write]: length = 6
0000: 14 03 01 00 01 01                                      ......
*** Finished
verify_data:  { 242, 98, 66, 170, 124, 124, 204, 231, 73, 15, 237, 172 }
***
[write] MD5 and SHA1 hashes:  len = 16
0000: 14 00 00 0C F2 62 42 AA   7C 7C CC E7 49 0F ED AC  .....bB.....I...
Padded plaintext before ENCRYPTION:  len = 32
0000: 14 00 00 0C F2 62 42 AA   7C 7C CC E7 49 0F ED AC  .....bB.....I...
0010: FA 06 3C 9F 8C 41 1D ED   2B 06 D0 5A ED 31 F2 80  ..<..A..+..Z.1..
main, WRITE: TLSv1 Handshake, length = 32
```

Note next that when the message above is actually written to the raw output device (following the 5 bytes of header information), the message is now encrypted.

```
[Raw write]: length = 37
0000: 16 03 01 00 20 15 8C 25   BA 4E 73 F5 27 79 49 B1  .... ..%.Ns.'yI.
0010: E9 F5 7E C8 48 A7 D3 A6   9B BD 6F 8E A5 8E 2B B7  ....H.....o...+.
0020: EE DC BD F4 D7                                     .....
```

We now wait for the server to send the same (Change Cipher Spec/Finshed), so we can know it completed negotiations successfully.

```
[Raw read]: length = 5
0000: 14 03 01 00 01                                     .....
[Raw read]: length = 1
0000: 01                                                 .
main, READ: TLSv1 Change Cipher Spec, length = 1
[Raw read]: length = 5
0000: 16 03 01 00 20                                     ....
[Raw read]: length = 32
0000: 1F F5 FA C8 79 20 CE 91   AA 68 7F 6C F3 5A DB 7B  ....y ...h.l.Z..
0010: A5 1C 31 1F 6F 41 50 C5   C6 25 25 8D 48 50 3F F1  ..1.oAP..%%.HP?.
main, READ: TLSv1 Handshake, length = 32
Padded plaintext after DECRYPTION:  len = 32
0000: 14 00 00 0C 07 38 46 5F   62 AD 41 B3 DC 79 30 FD  .....8F_b.A..y0.
0010: 34 F2 3B 54 1C D4 68 0E   92 0B 9C 7E ED 47 9F 3B  4.;T..h......G.;
*** Finished
verify_data:  { 7, 56, 70, 95, 98, 173, 65, 179, 220, 121, 48, 253 }
***
[read] MD5 and SHA1 hashes:  len = 16
0000: 14 00 00 0C 07 38 46 5F   62 AD 41 B3 DC 79 30 FD  .....8F_b.A..y0.
```

Everything completed successfully! Let's cache the established session in case we want to reestablish this session after this connection is dropped.

At this point, a SSL/TLS client should examine the credentials of the peer to make sure that it is communicating with the expected server. A HttpsURLConnection would check the hostname and call HostnameVerifier if there was a problem, but the raw SSLSocket doesn't. This verification should be done by hand, but we're ignoring this for now.

So, after all that, we're finally ready to exchange application data. We send a "GET /index.html HTTP1.1" command.

```
%% Cached client session: [Session-1, SSL_RSA_WITH_RC4_128_MD5]
Padded plaintext before ENCRYPTION:  len = 42
0000: 47 45 54 20 2F 69 6E 64   65 78 2E 68 74 6D 6C 20  GET /index.html
0010: 48 54 54 50 2F 31 2E 31   0A 0A CA CB D1 10 9D 0E  HTTP/1.1........
0020: 13 3C D9 66 6B 9E 36 87   ED 9B                    .<.fk.6...
main, WRITE: TLSv1 Application Data, length = 42
```

Note again the data over the wire is encrypted (skipping the 5 header bytes).

```
[Raw write]: length = 47
0000: 17 03 01 00 2A 8A E9 EC   2C 8D 19 B6 E2 50 C1 E2  ....*...,....P..
0010: 22 1A C0 97 95 23 99 E1   20 DD F3 2A B4 DC 14 57  "....#.. ..*...W
0020: 32 71 58 98 01 BE 70 11   A3 FC 8E 3A 7C 8D BF     2qX...p....:...
```

We get the application data back. First the HTTPS header, then the actual data.

```
[Raw read]: length = 5
0000: 17 03 01 00 50                                     ....P
[Raw read]: length = 80
0000: 70 10 0D D6 FA ED 51 FC   C2 7E CE 24 2E F1 2F F7  p.....Q....$../.
0010: E7 CD A5 D6 2D 1B 10 FD   48 56 9C 1B B5 EC 8F 1E  ....-...HV......
0020: DB DA F9 83 62 52 15 38   70 4B C1 85 13 EF CA 17  ....bR.8pK......
0030: 89 37 D3 45 C0 88 BB 92   63 F6 9C DE 69 E6 60 3E  .7.E....c...i.`>
0040: 1F F7 4D C1 56 61 79 01   49 55 FB 38 6B 16 81 BC  ..M.Vay.IU.8k...
main, READ: TLSv1 Application Data, length = 80
Padded plaintext after DECRYPTION:  len = 80
0000: 48 54 54 50 2F 31 2E 30   20 32 30 30 20 4F 4B 0D  HTTP/1.0 200 OK.
0010: 0A 43 6F 6E 74 65 6E 74   2D 4C 65 6E 67 74 68 3A  .Content-Length:
0020: 20 35 38 0D 0A 43 6F 6E   74 65 6E 74 2D 54 79 70   58..Content-Typ
0030: 65 3A 20 74 65 78 74 2F   68 74 6D 6C 0D 0A 0D 0A  e: text/html....
0040: 40 18 A1 FF 1D 5A D4 55   98 DB E3 95 01 A0 91 AF  @....Z.U........
HTTP/1.0 200 OK
Content-Length: 58
Content-Type: text/html
[Raw read]: length = 5
0000: 17 03 01 00 4A                                     ....J
[Raw read]: length = 74
0000: 75 DA F2 58 C3 5E 58 DE   14 AD FE 71 A3 78 07 58  u..X.^X....q.x.X
0010: EB E9 2B A2 D7 82 5C 6E   C9 9C 58 84 D7 A8 C6 F8  ..+...\n..X.....
0020: DE C6 5B BA 10 59 DF CC   11 AE 35 F7 C7 0F F6 C2  ..[..Y....5.....
0030: 3E 67 4E 95 30 AA 91 0B   E4 4F 5C C7 BF 50 AC 61  >gN.0....O\..P.a
0040: 87 B7 80 75 F0 81 F1 00   63 C9                    ...u....c.
main, READ: TLSv1 Application Data, length = 74
Padded plaintext after DECRYPTION:  len = 74
0000: 3C 48 54 4D 4C 3E 0A 3C   48 31 3E 48 65 6C 6C 6F  <HTML>.<H1>Hello
0010: 20 57 6F 72 6C 64 3C 2F   48 31 3E 0A 54 68 65 20   World</H1>.The
0020: 74 65 73 74 20 69 73 20   63 6F 6D 70 6C 65 74 65  test is complete
0030: 21 0A 3C 2F 48 54 4D 4C   3E 0A 38 2E 68 72 F1 47  !.</HTML>.8.hr.G
0040: E8 56 D1 EA A6 FC 3C 30   6F F3                    .V....<0o.
 <HTML>
<H1>Hello World<H1>
The test is complete!
<HTML>
```

Read from the socket again to see if there is any more data. We get a close_notify message, which means this connection is shutting down properly. We send our own in turn, then close the socket.

```
[Raw read]: length = 5
0000: 15 03 01 00 12                                     .....
[Raw read]: length = 18
0000: 09 AB 95 00 43 8D C8 7C   83 18 EB C4 8C 99 43 A6  ....C.........C.
0010: 76 49                                              vI
main, READ: TLSv1 Alert, length = 18
Padded plaintext after DECRYPTION:  len = 18
0000: 01 00 FA 44 D5 57 71 5C   CC C7 D9 D0 04 23 10 D8  ...D.Wq\.....#..
0010: 21 7B                                              !.
main, RECV TLSv1 ALERT:  warning, close_notify
main, called closeInternal(false)
main, SEND TLSv1 ALERT:  warning, description = close_notify
Padded plaintext before ENCRYPTION:  len = 18
0000: 01 00 8A 2C A2 36 9C 88   22 50 6E BC 95 3B B2 C4  ...,.6.."Pn..;..
```

```
0010: FE F2                                              ..
main, WRITE: TLSv1 Alert, length = 18
[Raw write]: length = 23
0000: 15 03 01 00 12 19 BE 10   8D FA F1 CA DD AB CC 91  ................
0010: 2E 49 08 71 2B C1 05                               .I.q+..
main, called close()
main, called closeInternal(true)
main, called close()
main, called closeInternal(true)
main, called close()
main, called closeInternal(true)
```