HTTP
Internet-Draft
Intended status: Standards Track
Expires: July 7, 2017

M. Thomson
Mozilla

January 3, 2017

# Example Handshake Traces for TLS 1.3
# draft-ietf-tls-tls13-vectors-00

Abstract

Examples of TLS 1.3 handshakes are shown. Private keys and inputs are provided so that these handshakes might be reproduced. Intermediate values, including secrets, traffic keys and ivs are shown so that implementations might be checked incrementally against these values.

Table of Contents



## 1. Introduction

TLS 1.3 [I-D.ietf-tls-tls13] defines a new key schedule and a number new cryptographic operations. This document includes sample handshakes that show all intermediate values. This allows an implementation to be verified incrementally, examining inputs and outputs of each cryptographic computation independently.

Private keys are included with the traces so that implementations can be checked by importing these values and verifying that the same outputs are produced.

## 2. Private Keys

Ephemeral private keys are shown as they are generated in the traces.

The server in most examples uses an RSA certificate with a private key of:

```
modulus (public):  b4bb498f8279303d 980836399b36c698 8c0c68de55e1bdb8
   26d3901a2461eafd 2de49a91d015abbc 9a95137ace6c1af1
   9eaa6af98c7ced43 120998e187a80ee0 ccb0524b1b018c3e
   0b63264d449a6d38 e22a5fda43084674 8030530ef0461c8c
   a9d9efbfae8ea6d1 d03e2bd193eff0ab 9a8002c47428a6d3
   5a8d88d79f7f1e3f

public exponent:  010001

private exponent:  04dea705d43a6ea7 209dd8072111a83c 81e322a59278b334
   80641eaf7c0a6985 b8e31c44f6de62e1 b4c2309f6126e77b
   7c41e923314bbfa3 881305dc1217f16c 819ce538e922f369
   828d0e57195d8c84 88460207b2faa726 bcf708bbd7db7f67
   9f893492fc2a622e 08970aac441ce4e0 c3088df25ae67923
   3df8a3bda2ff9941
```

prime1: e435fb7cc8373775 6dacea96ab7f59a2 cc1069db7deb190e
17e33a532b273f30 a327aa0aaabc58cd 67466af9845fadc6
75fe094af92c4bd1 f2c1bc33dd2e0515

prime2: cabd3bc0e0438664 c8d4cc9f99977a94 d9bbfead8e43870a
bae3f7eb8b4e0eee 8af1d9b4719ba619 6cf2cbbaeeebf8b3
490afe9e9ffa74a8 8aa51fc645629303

exponent1: 3f57345c27fe1b68 7e6e761627b78b1b 826433dd760fa0be
a6a6acf39490aa1b 47cda4869d68f584 dd5b5029bd32093b
8258661fe715025e 5d70a45a08d3d319

exponent2: 183da01363bd2f28 85cacbdc9964bf47 64f1517636f86401
286f71893c52ccfe 40a6c23d0d086b47 c6fb10d8fd1041e0
4def7e9a40ce957c 417794e10412d139

coefficient: 839ca9a085e4286b 2c90e466997a2c68 1f21339aa3477814
e4dec11833050ed5 0dd13cc038048a43 c59b2acc416889c0
37665fe5afa60596 9f8c01dfa5ca969d

## 3. Simple 1-RTT Handshake

In this example, the simplest possible handshake is completed. The server is authenticated, but the client remains anonymous. After connecting, a few application data octets are exchanged. The server sends a session ticket that permits the use of 0-RTT in any resumed session.

Note: This example doesn't include the calculation of the exporter secret. Support for that will be added to NSS soon.

{client} create an ephemeral x25519 key pair:

private key (32 octets): 00b4198a84ed6a7c 218702891735239d
40b7c66505330364 3d3c67f7458ecbc9

public key (32 octets): 35e58b160db6124f 01a1d2475a22b72a
bd6896701eed4c7e fd6124ee231ba458

{client} send a ClientHello handshake message

{client} send record:

cleartext (512 octets): 010001fc03039a46 4db650dcc81fed6f
1fea635f15861574 c0ed0bfb5778de77 24fb927c5ef10000
3e130113031302c0 2bc02fcca9cca8c0 0ac009c013c023c0
27c014009eccaa00 3300320067003900 38006b0016001300
9c002f003c003500 3d000a0005000401 000195001500fc00

```
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000b00 0900000673657276
      6572ff0100010000 0a00140012001d00 1700180019010001
      0101020103010400 0b00020100002300 0000280026002400
      1d002035e58b160d b6124f01a1d2475a 22b72abd6896701e
      ed4c7efd6124ee23 1ba458002b000706 7f1203030302000d
      0020001e04030503 0603020308040805 0806040105010601
      0201040205020602 0202002d00020101

   ciphertext (517 octets):  1603010200010001 fc03039a464db650
      dcc81fed6f1fea63 5f15861574c0ed0b fb5778de7724fb92
      7c5ef100003e1301 13031302c02bc02f cca9cca8c00ac009
      c013c023c027c014 009eccaa00330032 006700390038006b
      00160013009c002f 003c0035003d000a 0005000401000195
      001500fc00000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000b00090000
      06736572766572ff 01000100000a0014 0012001d00170018
      0019010001010102 01030104000b0002 0100002300000028
      00260024001d0020 35e58b160db6124f 01a1d2475a22b72a
      bd6896701eed4c7e fd6124ee231ba458 002b0007067f1203
      030302000d002000 1e04030503060302 0308040805080604
      0105010601020104 0205020602020200 2d00020101

{server}  extract secret "early":

   salt:  (absent)

   ikm (32 octets):  0000000000000000 0000000000000000
      0000000000000000 0000000000000000
```

```
      secret (32 octets):  33ad0a1c607ec03b 09e6cd9893680ce2
         10adf300aa1f2660 e1b22e10f170f92a

   {server}  create an ephemeral x25519 key pair:

      private key (32 octets):  03d43f48ed52076f 4ce9bab73d1f39ec
         689cf304075829f5 2b90f9f13bea6f34

      public key (32 octets):  a20ed1b7f2d96a7f 12568f0e460bb0fc
         86dc8d1db6c07d6b 10d4dc74aaac9219

   {server}  send a ServerHello handshake message

   {server}  extract secret "handshake":

      salt (32 octets):  33ad0a1c607ec03b 09e6cd9893680ce2
         10adf300aa1f2660 e1b22e10f170f92a

      ikm (32 octets):  c08acc73ba101d7f ea86d223de32d9fc
         4948e14549368059 4b83b0a109f83649

      secret (32 octets):  31168cad69862a80 c6f6bfd42897d0fe
         23c406a12e652a8d 3ae4217694f49844

   {server}  derive secret "client handshake traffic secret":

      PRK (32 octets):  31168cad69862a80 c6f6bfd42897d0fe
         23c406a12e652a8d 3ae4217694f49844

      handshake hash (32 octets):  52c04472bdfe9297 72c98b91cf425f78
         f47659be9d4a7d68 b9e29d162935e9b9

      info (76 octets):  002028544c532031 2e332c20636c6965
         6e742068616e6473 68616b6520747261 6666696320736563
         7265742052c04472 bdfe929772c98b91 cf425f78f47659be
         9d4a7d68b9e29d16 2935e9b9

      output (32 octets):  6c6f274b1eae09b8 bbd2039b7eb56147
         201a5e19288a3fd5 04fa52b1178a6e93

   {server}  derive secret "server handshake traffic secret":

      PRK (32 octets):  31168cad69862a80 c6f6bfd42897d0fe
         23c406a12e652a8d 3ae4217694f49844

      handshake hash (32 octets):  52c04472bdfe9297 72c98b91cf425f78
         f47659be9d4a7d68 b9e29d162935e9b9
```

```
      info (76 octets):  002028544c532031 2e332c2073657276
         65722068616e6473 68616b6520747261 6666696320736563
         7265742052c04472 bdfe929772c98b91 cf425f78f47659be
         9d4a7d68b9e29d16 2935e9b9

      output (32 octets):  b2c2663ed59e833b 17c68823516f11f1
         cb311855045d3ce4 6bfe8ac8889268d9

   {server}  extract secret "master":

      salt (32 octets):  31168cad69862a80 c6f6bfd42897d0fe
         23c406a12e652a8d 3ae4217694f49844

      ikm (32 octets):  0000000000000000 0000000000000000
         0000000000000000 0000000000000000

      secret (32 octets):  24bc43c2d11c895e b2d5f78b6fdf9cf5
         a50c336573b2d2e9 6d4d5cc82a64c0e9

   {server}  send record:

      cleartext (82 octets):  0200004e7f1298e3 4364038683391cbe
         c1039aa0fba2f496 d8c8e6327151cc94 bbc5ef7390751301
         002800280024001d 0020a20ed1b7f2d9 6a7f12568f0e460b
         b0fc86dc8d1db6c0 7d6b10d4dc74aaac 9219

      ciphertext (87 octets):  1603010052020000 4e7f1298e3436403
         8683391cbec1039a a0fba2f496d8c8e6 327151cc94bbc5ef
         7390751301002800 280024001d0020a2 0ed1b7f2d96a7f12
         568f0e460bb0fc86 dc8d1db6c07d6b10 d4dc74aaac9219

   {server}  derive write traffic keys using label "handshake data":

      PRK (32 octets):  b2c2663ed59e833b 17c68823516f11f1
         cb311855045d3ce4 6bfe8ac8889268d9

      key info (16 octets):  00100c544c532031 2e332c206b657900

      key output (16 octets):  acd79b9ecb64a1ab 61b77b11a03eb976

      iv info (15 octets):  000c0b544c532031 2e332c20697600

      iv output (12 octets):  a353bfcdf9695a2a 09c2e293

   {server}  send a EncryptedExtensions handshake message

   {server}  send a Certificate handshake message
```

```
   {server}  send a CertificateVerify handshake message

   {server}  calculate finished:

      PRK (32 octets):  b2c2663ed59e833b 17c68823516f11f1
         cb311855045d3ce4 6bfe8ac8889268d9

      handshake hash (0 octets):  (empty)

      info (21 octets):  002011544c532031 2e332c2066696e69 7368656400

      output (32 octets):  6378b7e68a7b3a12 8c3de8df9346e410
         9fdf04ca088904df 69115284c9e34d8a

   {server}  send a Finished handshake message

   {server}  send record:

      cleartext (651 octets):  0800001e001c000a 00140012001d0017
         0018001901000101 0102010301040000 00000b0001b90000
         01b50001b0308201 ac30820115a00302 0102020102300d06
         092a864886f70d01 010b0500300e310c 300a060355040313
         03727361301e170d 3136303733303031 323335395a170d32
         3630373330303132 3335395a300e310c 300a060355040313
         0372736130819f30 0d06092a864886f7 0d01010105000381
         8d00308189028181 00b4bb498f827930 3d980836399b36c6
         988c0c68de55e1bd b826d3901a2461ea fd2de49a91d015ab
         bc9a95137ace6c1a f19eaa6af98c7ced 43120998e187a80e
         e0ccb0524b1b018c 3e0b63264d449a6d 38e22a5fda430846
         748030530ef0461c 8ca9d9efbfae8ea6 d1d03e2bd193eff0
         ab9a8002c47428a6 d35a8d88d79f7f1e 3f0203010001a31a
         301830090603551d 1304023000300b06 03551d0f04040302
         05a0300d06092a86 4886f70d01010b05 000381810085aad2
         a0e5b9276b908c65 f73a7267170618a5 4c5f8a7b337d2df7
         a594365417f2eae8 f8a58c8f8172f931 9cf36b7fd6c55b80
         f21a030151567260 96fd335e5e67f2db f102702e608ccae6
         bec1fc63a42a99be 5c3eb7107c3c54e9 b9eb2bd5203b1c3b
         84e0a8b2f759409b a3eac9d91d402dcc 0cc8f8961229ac91
         87b42b4de100000f 000084080400808d 8d5ed7ee8e4fa552
         aaa1279b8f5c39e4 394cf20e8c53ef1a de12f9bd92337169
         b218e4746b19817c bdef9410151cbf31 43ecc1c075076d97
         71379ccca365ce01 d0dcce2ba1ea4a5e 4e37f362594574c3
         e6cb1a4afcfa3547 ce08155de7a6cc3d b9752478913db105
         47cf2013b24f3fcd 61a2dbe6d2a7dc25 97ddf880ec1f5814
         00002051f933cd8e fe503845c33b8711 9fc67d4991b6ffa9
         f520ae0b1a37f7ea bb2ecc
```

```
      ciphertext (673 octets):  170301029c4e1f34 2dba17a54a09f7a1
         8ffb2c6a29df17a6 db843044c52861bf 78988527ce366159
         e6a24871b704d2b9 fade56488921796d 719173a753bdfec8
         0554c8c15e128695 450ccfdde1204ffd 2fb1ecdcd87b8070
         644eb5a6b86ec951 aba3ed314754a2f3 14d4d2620b92da1f
         28f24b9559d76b67 a7b35c17cc231ba5 77a94fb2be59c74f
         84c8c78bf5faf4cb b2f8a37091580743 3c67d9f4e1b1923a
         3969b85a2ae9064e 34e84363aae43aa9 f58717836a017b9c
         33c3ad733c2fd3ce 288ae362764403d0 102a371047d9e49d
         f9b30596262b1704 f0e9839fff5641ba a7041a4bcf9e4d46
         7108922fc0ea0bc1 48dab2ebdd155f51 76c632be04a7c610
         3fbc92754dba7962 4f8a09f8e8d65c17 eee87f98636fbc93
         bb734674b80d183c da904200a20d8f15 0a214902b6953209
         aa2431c3973bda3b d92a33878baca7b9 0507f433a55f2fe8
         f0db81898ebacf31 b68eaabfa27c39b6 a2453a322c005030
         4e60bf53f0402b38 65b43fe5a7454c13 17a2dc76d1323fb1
         aa553996876a0dfe 8e789d6adf3dc85b 0636bb58a96e6aad
         851e7a6fc1dfa796 ec65e33bf9e3c05d 6de35f11e1f32731
         fb9550a60cb75e90 9345eb0edb81f99f cad883cb41d4a3ef
         7cbe671b92a8176b 472772be401b83a4 99b06b7ab0a1d9cd
         795e5ba0b67ce2d6 5c45565028824aa2 08797f405bbcf243
         27dd69a1d986032f 544b15d110e4d8c4 681cb85c09960adb
         57fb9723eef0e0bb 275552af25fbdfc1 a4215adf14a9dba2
         4462dd095f1a78f5 6ed6db3de139936f 14b091ab7f4adc81
         c277e68bfb6fd925 d92c06c0a4ddd105 9c071073a8a2e987
         f98948599f27bf6d 1f4369ac6c5a3323 2932fb8aa52ec4e1
         85790dff0ef5eee0 13b4e90b5bc1cd4a c42b7ce82d856cc0
         f5d1c80400e68d61 b434cec56d437141 1e31849d4cf88862
         8ba288548df6a19e c4

   {server}  derive secret "client application traffic secret":

      PRK (32 octets):  24bc43c2d11c895e b2d5f78b6fdf9cf5
         a50c336573b2d2e9 6d4d5cc82a64c0e9

      handshake hash (32 octets):  f610f8a56a05fab4 c6fef3579180d575
         79c1a24e01fe709d 97bd49750576c241

      info (78 octets):  00202a544c532031 2e332c20636c6965
         6e74206170706c69 636174696f6e2074 7261666669632073
         656372657420f610 f8a56a05fab4c6fe f3579180d57579c1
         a24e01fe709d97bd 49750576c241

      output (32 octets):  d0886eee6eef4411 5c74ba22e546e115
         752832743916a01b 1d6a60517bbf2997

   {server}  derive secret "server application traffic secret":
```

```
      PRK (32 octets):  24bc43c2d11c895e b2d5f78b6fdf9cf5
         a50c336573b2d2e9 6d4d5cc82a64c0e9

      handshake hash (32 octets):  f610f8a56a05fab4 c6fef3579180d575
         79c1a24e01fe709d 97bd49750576c241

      info (78 octets):  00202a544c532031 2e332c2073657276
         6572206170706c69 636174696f6e2074 7261666669632073
         656372657420f610 f8a56a05fab4c6fe f3579180d57579c1
         a24e01fe709d97bd 49750576c241

      output (32 octets):  b8dac8d7e56af263 b53ff4cc720ce286
         41053666877dc200 d3abec0b60ab4a4f

   {server}  derive secret "exporter master secret":

      PRK (32 octets):  24bc43c2d11c895e b2d5f78b6fdf9cf5
         a50c336573b2d2e9 6d4d5cc82a64c0e9

      handshake hash (32 octets):  f610f8a56a05fab4 c6fef3579180d575
         79c1a24e01fe709d 97bd49750576c241

      info (67 octets):  00201f544c532031 2e332c206578706f
         72746572206d6173 7465722073656372 657420f610f8a56a
         05fab4c6fef35791 80d57579c1a24e01 fe709d97bd497505 76c241

      output (32 octets):  5f52032864fadbcc 0d87afb4cafc7f53
         3393e51a2cca21fa 2f31a99b0e07f6c4

   {server}  derive write traffic keys using label "application data":

      PRK (32 octets):  b8dac8d7e56af263 b53ff4cc720ce286
         41053666877dc200 d3abec0b60ab4a4f

      key info (16 octets):  00100c544c532031 2e332c206b657900

      key output (16 octets):  5fa2db5d9b4c104d 51217b0c144f35b7

      iv info (15 octets):  000c0b544c532031 2e332c20697600

      iv output (12 octets):  cbbd55b839920e04 e1d775ab

   {server}  derive read traffic keys using label "handshake data":

      PRK (32 octets):  6c6f274b1eae09b8 bbd2039b7eb56147
         201a5e19288a3fd5 04fa52b1178a6e93

      key info (16 octets):  00100c544c532031 2e332c206b657900
```

```
      key output (16 octets):  86a3c174990039e0 81d021981c5f1465

      iv info (15 octets):  000c0b544c532031 2e332c20697600

      iv output (12 octets):  53fa86476124ba4a db28355c

   {client}  extract secret "early":

      salt:  (absent)

      ikm (32 octets):  0000000000000000 0000000000000000
         0000000000000000 0000000000000000

      secret (32 octets):  33ad0a1c607ec03b 09e6cd9893680ce2
         10adf300aa1f2660 e1b22e10f170f92a

   {client}  extract secret "handshake":

      salt (32 octets):  33ad0a1c607ec03b 09e6cd9893680ce2
         10adf300aa1f2660 e1b22e10f170f92a

      ikm (32 octets):  c08acc73ba101d7f ea86d223de32d9fc
         4948e14549368059 4b83b0a109f83649

      secret (32 octets):  31168cad69862a80 c6f6bfd42897d0fe
         23c406a12e652a8d 3ae4217694f49844

   {client}  derive secret "client handshake traffic secret":

      PRK (32 octets):  31168cad69862a80 c6f6bfd42897d0fe
         23c406a12e652a8d 3ae4217694f49844

      handshake hash (32 octets):  52c04472bdfe9297 72c98b91cf425f78
         f47659be9d4a7d68 b9e29d162935e9b9

      info (76 octets):  002028544c532031 2e332c20636c6965
         6e742068616e6473 68616b6520747261 6666696320736563
         7265742052c04472 bdfe929772c98b91 cf425f78f47659be
         9d4a7d68b9e29d16 2935e9b9

      output (32 octets):  6c6f274b1eae09b8 bbd2039b7eb56147
         201a5e19288a3fd5 04fa52b1178a6e93

   {client}  derive secret "server handshake traffic secret":

      PRK (32 octets):  31168cad69862a80 c6f6bfd42897d0fe
         23c406a12e652a8d 3ae4217694f49844
```

handshake hash (32 octets): 52c04472bdfe9297 72c98b91cf425f78
f47659be9d4a7d68 b9e29d162935e9b9

info (76 octets): 002028544c532031 2e332c2073657276
65722068616e6473 68616b6520747261 6666696320736563
7265742052c04472 bdfe929772c98b91 cf425f78f47659be
9d4a7d68b9e29d16 2935e9b9

output (32 octets): b2c2663ed59e833b 17c68823516f11f1
cb311855045d3ce4 6bfe8ac8889268d9

{client} extract secret "master" (same as server)

{client} derive read traffic keys using label "handshake data":

PRK (32 octets): b2c2663ed59e833b 17c68823516f11f1
cb311855045d3ce4 6bfe8ac8889268d9

key info (16 octets): 00100c544c532031 2e332c206b657900

key output (16 octets): acd79b9ecb64a1ab 61b77b11a03eb976

iv info (15 octets): 000c0b544c532031 2e332c20697600

iv output (12 octets): a353bfcdf9695a2a 09c2e293

{client} calculate finished:

PRK (32 octets): b2c2663ed59e833b 17c68823516f11f1
cb311855045d3ce4 6bfe8ac8889268d9

handshake hash (0 octets): (empty)

info (21 octets): 002011544c532031 2e332c2066696e69 7368656400

output (32 octets): 6378b7e68a7b3a12 8c3de8df9346e410
9fdf04ca088904df 69115284c9e34d8a

{client} derive write traffic keys using label "handshake data"
(same as server read traffic keys)

{client} derive secret "client application traffic secret":

PRK (32 octets): 24bc43c2d11c895e b2d5f78b6fdf9cf5
a50c336573b2d2e9 6d4d5cc82a64c0e9

handshake hash (32 octets): f610f8a56a05fab4 c6fef3579180d575
79c1a24e01fe709d 97bd49750576c241

```
      info (78 octets):  00202a544c532031 2e332c20636c6965
         6e74206170706c69 636174696f6e2074 7261666669632073
         656372657420f610 f8a56a05fab4c6fe f3579180d57579c1
         a24e01fe709d97bd 49750576c241

      output (32 octets):  d0886eee6eef4411 5c74ba22e546e115
         752832743916a01b 1d6a60517bbf2997

   {client}  derive secret "server application traffic secret":

      PRK (32 octets):  24bc43c2d11c895e b2d5f78b6fdf9cf5
         a50c336573b2d2e9 6d4d5cc82a64c0e9

      handshake hash (32 octets):  f610f8a56a05fab4 c6fef3579180d575
         79c1a24e01fe709d 97bd49750576c241

      info (78 octets):  00202a544c532031 2e332c2073657276
         6572206170706c69 636174696f6e2074 7261666669632073
         656372657420f610 f8a56a05fab4c6fe f3579180d57579c1
         a24e01fe709d97bd 49750576c241

      output (32 octets):  b8dac8d7e56af263 b53ff4cc720ce286
         41053666877dc200 d3abec0b60ab4a4f

   {client}  derive secret "exporter master secret" (same as server)

   {client}  derive read traffic keys using label "application data"
      (same as server write traffic keys)

   {client}  calculate finished:

      PRK (32 octets):  6c6f274b1eae09b8 bbd2039b7eb56147
         201a5e19288a3fd5 04fa52b1178a6e93

      handshake hash (0 octets):  (empty)

      info (21 octets):  002011544c532031 2e332c2066696e69 7368656400

      output (32 octets):  f28fcafbd1390f7c 5d0a306095890ee3
         e62d071262778959 6388fc228d67abac

   {client}  send a Finished handshake message

   {client}  send record:

      cleartext (36 octets):  140000201a5eb0ba 5f92f34ed0059d64
         cedd2a7d208f25f0 0e28138117fb3974 d415776a
```

```
      ciphertext (58 octets):  1703010035161e94 818226d7bd618063
         0804644debc52bdd 661034243217ac45 a084228c82086baa
         4893ecfc969624d6 8e19d88c3e67ccb4 8bdf

   {client}  derive write traffic keys using label "application data":

      PRK (32 octets):  d0886eee6eef4411 5c74ba22e546e115
         752832743916a01b 1d6a60517bbf2997

      key info (16 octets):  00100c544c532031 2e332c206b657900

      key output (16 octets):  7c0d9bd5eced0f0c cc541dd3b7775490

      iv info (15 octets):  000c0b544c532031 2e332c20697600

      iv output (12 octets):  41b32fd4039bf79c 1762e25c

   {client}  derive secret "resumption master secret":

      PRK (32 octets):  24bc43c2d11c895e b2d5f78b6fdf9cf5
         a50c336573b2d2e9 6d4d5cc82a64c0e9

      handshake hash (32 octets):  aa0b1e200d4fff65 669d70b742e99143
         5bc93874ca864420 620acf75242fb0c3

      info (69 octets):  002021544c532031 2e332c2072657375
         6d7074696f6e206d 6173746572207365 6372657420aa0b1e
         200d4fff65669d70 b742e991435bc938 74ca864420620acf 75242fb0c3

      output (32 octets):  0a3495607f1f8cda df1ca4ca7fb1fe10
         19d122e324eeb81d 8d372d3c6f27ca17

   {server}  calculate finished:

      PRK (32 octets):  6c6f274b1eae09b8 bbd2039b7eb56147
         201a5e19288a3fd5 04fa52b1178a6e93

      handshake hash (0 octets):  (empty)

      info (21 octets):  002011544c532031 2e332c2066696e69 7368656400

      output (32 octets):  f28fcafbd1390f7c 5d0a306095890ee3
         e62d071262778959 6388fc228d67abac

   {server}  derive read traffic keys using label "application data"
      (same as client write traffic keys)

   {server}  derive secret "resumption master secret" (same as client)
```

```
   {server}  send a SessionTicket handshake message

   {server}  send record:

      cleartext (170 octets):  040000a60002a300 50fabab700924e53
         5321e5c102aa2498 52ac81f080bc62bd 5e696a0d8a2130e9
         80e37b9035aa0050 403a09451c497f08 25609bac976c59f2
         d53f159051d2fc5f cf4bd68ae4886dd9 a05144d07c5a2646
         177e94015f764edd 5ecf3b7ea4042f29 a6225092b11ba8ec
         20e17c5c6fff9a38 c56cf2373b2bd538 60e5b0b983e82aa2
         ae72cb225b9d6951 67ed0963cceabfa1 09e1b2e5104fec34
         0008002e00040002 0000

      ciphertext (192 octets):  17030100bbe6b3e9 89df694688f29f5d
         a42d9f56053fc6d2 f73ee23accad26f9 599ee4dcf4e0cf9e
         de80128b48156a65 e5e47dee679a8401 1234862b6728fb12
         be5198d5c023d6f2 0c355fc417a5eade 1aff0bf9ecba14c8
         7277ea7aeb30055e a4d9b37bc12f7517 27ca7a1efc9285f8
         ed5e9e3be42ff475 30f2b7347a90618b 6f7f4eba9b8b6564
         f2159fcfcf09e4b6 2b4b09bb129e7c76 5c877966ca66e5cd
         a84cdb6087a07fc0 50c97f275568623c 5d0f459d2b1133d1
         d5d37cd441192da7

   {client}  send record:

      cleartext (50 octets):  0001020304050607 08090a0b0c0d0e0f
         1011121314151617 18191a1b1c1d1e1f 2021222324252627
         28292a2b2c2d2e2f 3031

      ciphertext (72 octets):  170301004341b540 bf5adeaf9d209001
         9f0733e281964724 526678a1946852cf 6f586dffacf1151d
         bf7c9262ef6ae960 4a423fff339fd7e4 0cc3e7604ae661f0
         afa2f775c3668867

   {server}  send record:

      cleartext (50 octets):  0001020304050607 08090a0b0c0d0e0f
         1011121314151617 18191a1b1c1d1e1f 2021222324252627
         28292a2b2c2d2e2f 3031

      ciphertext (72 octets):  17030100438c3168 1fb21f820ef0603c
         dc3b9d3deedeb2bb 615aa418fb2590a0 9b0dec00c2299feb
         17c4206f89ab28d2 7a605e288ac9bd69 657593addd1046be
         51b23940f8746634

   {client}  send record:

      cleartext (2 octets):  0100
```

ciphertext (24 octets): 17030100131ce9b1 f21ba236bca94455
ab2aad71c666534a

{server} send record:

cleartext (2 octets): 0100

ciphertext (24 octets): 1703010013aabcdb 9d293d23fb00deb7
11b562afeddffeed

## 4. Resumed 0-RTT Handshake

This handshake resumes from the handshake in Section 3. Since the server provided a session ticket that permitted 0-RTT, and the client is configured for 0-RTT, the client is able to send 0-RTT data.

{client} create an ephemeral x25519 key pair:

private key (32 octets): 04c04b641580df25 c7515df0ad895903
2deb52cddaf1f16f 013ef18a59baf88a

public key (32 octets): 248c256578c6418e 6c533ec1878cc84b
cfbca6b5e61d6993 8ac34888faf5df47

{client} extract secret "early":

salt: (absent)

ikm (32 octets): 0a3495607f1f8cda df1ca4ca7fb1fe10
19d122e324eeb81d 8d372d3c6f27ca17

secret (32 octets): 4134d8d48b05dfef 4658fc13f653b21b
40426eca75a84eab 87900d991db9abfd

{client} derive secret "resumption psk binder key":

PRK (32 octets): 4134d8d48b05dfef 4658fc13f653b21b
40426eca75a84eab 87900d991db9abfd

handshake hash (32 octets): e3b0c44298fc1c14 9afbf4c8996fb924
27ae41e4649b934c a495991b7852b855

info (70 octets): 002022544c532031 2e332c2072657375
6d7074696f6e2070 736b2062696e6465 72206b657920e3b0
c44298fc1c149afb f4c8996fb92427ae 41e4649b934ca495 991b7852b855

output (32 octets): 17f4f2e4a585caa6 7dc5fe0fcd009df8
a425cbda95f6e05d 1b0d7d81c28b7b8c

```
   {client}  derive secret "early exporter master secret":

      PRK (32 octets):  4134d8d48b05dfef 4658fc13f653b21b
         40426eca75a84eab 87900d991db9abfd

      handshake hash (32 octets):  e3b0c44298fc1c14 9afbf4c8996fb924
         27ae41e4649b934c a495991b7852b855

      info (73 octets):  002025544c532031 2e332c206561726c
         79206578706f7274 6572206d61737465 7220736563726574
         20e3b0c44298fc1c 149afbf4c8996fb9 2427ae41e4649b93
         4ca495991b7852b8 55

      output (32 octets):  4b3490267b142ccb 9979c56caad0c2f1
         c0941899c9169414 bd4ec1977a706f3c

   {client}  send a ClientHello handshake message

   {client}  calculate finished:

      PRK (32 octets):  17f4f2e4a585caa6 7dc5fe0fcd009df8
         a425cbda95f6e05d 1b0d7d81c28b7b8c

      handshake hash (0 octets):  (empty)

      info (21 octets):  002011544c532031 2e332c2066696e69 7368656400

      output (32 octets):  2a22df8df852efc1 5265e5b5424db5a7
         7a13e3433681189b 71d685515f6b8988

   {client}  send record:

      cleartext (512 octets):  010001fc030367bc 45e51e4ea55af6f7
         0c84056f69d8f14c ac08c88417c9116a 30cb54965bb70000
         3e130113031302c0 2bc02fcca9cca8c0 0ac009c013c023c0
         27c014009eccaa00 3300320067003900 38006b0016001300
         9c002f003c003500 3d000a0005000401 0001950015003b00
         0000000000000000 0000000000000000 0000000000000000
         0000000000000000 0000000000000000 0000000000000000
         0000000000000000 000000000000b0009 0000067365727665
         72ff01000100000a 00140012001d0017 0018001901000101
         010201030104000b 0002010000280026 0024001d0020248c
         256578c6418e6c53 3ec1878cc84bcfbc a6b5e61d69938ac3
         4888faf5df47002a 0000002b0007067f 1203030302000d00
         20001e0403050306 0302030804080508 0604010501060102
         0104020502060202 02002d0002010100 2900bd009800924e
         535321e5c102aa24 9852ac81f080bc62 bd5e696a0d8a2130
         e980e37b9035aa00 50403a09451c497f 0825609bac976c59
```

```
      f2d53f159051d2fc 5fcf4bd68ae4886d d9a05144d07c5a26
      46177e94015f764e dd5ecf3b7ea4042f 29a6225092b11ba8
      ec20e17c5c6fff9a 38c56cf2373b2bd5 3860e5b0b983e82a
      a2ae72cb225b9d69 5167ed0963cceabf a109e1b2e5104fec
      3450fababb002120 b63b26e73c9662e6 db5a9c9608f4df50
      ae547ece1b50a359 7de5f7298f86d213

   ciphertext (517 octets):  1603010200010001 fc030367bc45e51e
      4ea55af6f70c8405 6f69d8f14cac08c8 8417c9116a30cb54
      965bb700003e1301 13031302c02bc02f cca9cca8c00ac009
      c013c023c027c014 009eccaa00330032 006700390038006b
      00160013009c002f 003c0035003d000a 0005000401000195
      0015003b00000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 00000b0009000006
      736572766572ff01 000100000a001400 12001d0017001800
      1901000101010201 030104000b000201 0000280026002400
      1d0020248c256578 c6418e6c533ec187 8cc84bcfbca6b5e6
      1d69938ac34888fa f5df47002a000000 2b0007067f120303
      0302000d0020001e 0403050306030203 0804080508060401
      0501060102010402 050206020202002d 00020101002900bd
      009800924e535321 e5c102aa249852ac 81f080bc62bd5e69
      6a0d8a2130e980e3 7b9035aa0050403a 09451c497f082560
      9bac976c59f2d53f 159051d2fc5fcf4b d68ae4886dd9a051
      44d07c5a2646177e 94015f764edd5ecf 3b7ea4042f29a622
      5092b11ba8ec20e1 7c5c6fff9a38c56c f2373b2bd53860e5
      b0b983e82aa2ae72 cb225b9d695167ed 0963cceabfa109e1
      b2e5104fec3450fa babb002120b63b26 e73c9662e6db5a9c
      9608f4df50ae547e ce1b50a3597de5f7 298f86d213

{client}  derive secret "client early traffic secret":

   PRK (32 octets):  4134d8d48b05dfef 4658fc13f653b21b
      40426eca75a84eab 87900d991db9abfd

   handshake hash (32 octets):  f112c74dce3549fb 905c28fe797b54c2
      5d7e66e999e3d2c4 7bdfe302d8eec019

   info (72 octets):  002024544c532031 2e332c20636c6965
      6e74206561726c79 2074726166666963 2073656372657420
      f112c74dce3549fb 905c28fe797b54c2 5d7e66e999e3d2c4
      7bdfe302d8eec019

   output (32 octets):  c7626bf3ab56db2a bad7e3f9147acff2
      2aece599a57831b3 ba76db92b5b4e281

{client}  derive write traffic keys using label "early application
   data":
```

```
      PRK (32 octets):  c7626bf3ab56db2a bad7e3f9147acff2
         2aece599a57831b3 ba76db92b5b4e281

      key info (16 octets):  00100c544c532031 2e332c206b657900

      key output (16 octets):  fd649610caac6474 2a757c31668e4dee

      iv info (15 octets):  000c0b544c532031 2e332c20697600

      iv output (12 octets):  e3b86ee7f121da48 6734c5fa

   {client}  send record:

      cleartext (6 octets):  414243444546

      ciphertext (28 octets):  170301001761fc9c 67e6ffedb4f96e10
         76090e4f6accbf3c c67a8270

   {server}  extract secret "early" (same as client)

   {server}  derive secret "resumption psk binder key":

      PRK (32 octets):  4134d8d48b05dfef 4658fc13f653b21b
         40426eca75a84eab 87900d991db9abfd

      handshake hash (32 octets):  e3b0c44298fc1c14 9afbf4c8996fb924
         27ae41e4649b934c a495991b7852b855

      info (70 octets):  002022544c532031 2e332c2072657375
         6d7074696f6e2070 736b2062696e6465 72206b657920e3b0
         c44298fc1c149afb f4c8996fb92427ae 41e4649b934ca495 991b7852b855

      output (32 octets):  17f4f2e4a585caa6 7dc5fe0fcd009df8
         a425cbda95f6e05d 1b0d7d81c28b7b8c

   {server}  derive secret "early exporter master secret":

      PRK (32 octets):  4134d8d48b05dfef 4658fc13f653b21b
         40426eca75a84eab 87900d991db9abfd

      handshake hash (32 octets):  e3b0c44298fc1c14 9afbf4c8996fb924
         27ae41e4649b934c a495991b7852b855

      info (73 octets):  002025544c532031 2e332c206561726c
         79206578706f7274 6572206d61737465 7220736563726574
         20e3b0c44298fc1c 149afbf4c8996fb9 2427ae41e4649b93
         4ca495991b7852b8 55
```

```
      output (32 octets):  4b3490267b142ccb 9979c56caad0c2f1
         c0941899c9169414 bd4ec1977a706f3c

   {server}  calculate finished:

      PRK (32 octets):  17f4f2e4a585caa6 7dc5fe0fcd009df8
         a425cbda95f6e05d 1b0d7d81c28b7b8c

      handshake hash (0 octets):  (empty)

      info (21 octets):  002011544c532031 2e332c2066696e69 7368656400

      output (32 octets):  2a22df8df852efc1 5265e5b5424db5a7
         7a13e3433681189b 71d685515f6b8988

   {server}  create an ephemeral x25519 key pair:

      private key (32 octets):  063a96b0215d7e47 08de2984730c25f9
         292938093f701623 58f55b2e417ba725

      public key (32 octets):  fd8ed5f9bb812fd9 854227d656768386
         0b40b1cf93456dce 603f02de5b4a881a

   {server}  derive secret "client early traffic secret" (same as
      client)

   {server}  send a ServerHello handshake message

   {server}  extract secret "handshake":

      salt (32 octets):  4134d8d48b05dfef 4658fc13f653b21b
         40426eca75a84eab 87900d991db9abfd

      ikm (32 octets):  8137f1033479e363 c531d475456a399c
         b60c5e1f13c28f5d dc761b9eac5afc66

      secret (32 octets):  2b4389f45c4c468c 1f94bf7bb6b99546
         a33c35f4c3a57a35 6dccbe99d3d56302

   {server}  derive secret "client handshake traffic secret":

      PRK (32 octets):  2b4389f45c4c468c 1f94bf7bb6b99546
         a33c35f4c3a57a35 6dccbe99d3d56302

      handshake hash (32 octets):  2fd2f168296a08d7 1a1c693b3340f152
         9326ca31c3795190 504e1d0a1261a79d
```

```
      info (76 octets):  002028544c532031 2e332c20636c6965
         6e742068616e6473 68616b6520747261 6666696320736563
         726574202fd2f168 296a08d71a1c693b 3340f1529326ca31
         c3795190504e1d0a 1261a79d

      output (32 octets):  5f9c7ffdc773eaa8 f11886ee8d5bc62e
         5bf9acb23983a321 271960d54daa730c

   {server}  derive secret "server handshake traffic secret":

      PRK (32 octets):  2b4389f45c4c468c 1f94bf7bb6b99546
         a33c35f4c3a57a35 6dccbe99d3d56302

      handshake hash (32 octets):  2fd2f168296a08d7 1a1c693b3340f152
         9326ca31c3795190 504e1d0a1261a79d

      info (76 octets):  002028544c532031 2e332c2073657276
         65722068616e6473 68616b6520747261 6666696320736563
         726574202fd2f168 296a08d71a1c693b 3340f1529326ca31
         c3795190504e1d0a 1261a79d

      output (32 octets):  eedd9ba9252944fa 8ccd415fe8897fbe
         035fbbfbb3f0afbf 71ed64d7f2278cbd

   {server}  extract secret "master":

      salt (32 octets):  2b4389f45c4c468c 1f94bf7bb6b99546
         a33c35f4c3a57a35 6dccbe99d3d56302

      ikm (32 octets):  0000000000000000 0000000000000000
         0000000000000000 0000000000000000

      secret (32 octets):  5d995a2374a68417 22518bedfcfcd627
         855c8fb4e18a8759 4416b19c3c4e485d

   {server}  send record:

      cleartext (88 octets):  020000547f12eb07 b4e06753eeef8160
         4e669a35df1850c2 632e80850807693a 2c6f4bba48421301
         002e002900020000 00280024001d0020 fd8ed5f9bb812fd9
         854227d656768386 0b40b1cf93456dce 603f02de5b4a881a

      ciphertext (93 octets):  1603010058020000 547f12eb07b4e067
         53eeef81604e669a 35df1850c2632e80 850807693a2c6f4b
         ba48421301002e00 2900020000002800 24001d0020fd8ed5
         f9bb812fd9854227 d6567683860b40b1 cf93456dce603f02 de5b4a881a

   {server}  derive write traffic keys using label "handshake data":
```

```
      PRK (32 octets):  eedd9ba9252944fa 8ccd415fe8897fbe
         035fbbfbb3f0afbf 71ed64d7f2278cbd

      key info (16 octets):  00100c544c532031 2e332c206b657900

      key output (16 octets):  33ebfd906881cf62 6df5af4e11583167

      iv info (15 octets):  000c0b544c532031 2e332c20697600

      iv output (12 octets):  bee0ca11151aecb4 c09f53a4

   {server}  send a EncryptedExtensions handshake message

   {server}  calculate finished:

      PRK (32 octets):  eedd9ba9252944fa 8ccd415fe8897fbe
         035fbbfbb3f0afbf 71ed64d7f2278cbd

      handshake hash (0 octets):  (empty)

      info (21 octets):  002011544c532031 2e332c2066696e69 7368656400

      output (32 octets):  0fbc2652ef380d5e ea99467b0f7f8dd0
         8f9448439634a056 ebe4f673b6a6df60

   {server}  send a Finished handshake message

   {server}  send record:

      cleartext (74 octets):  080000220020000a 00140012001d0017
         0018001901000101 0102010301040000 0000002a00001400
         00202187c7f5b8f2 b388d5ac262db202 fca236b5bc85cbac
         5817aa547ade36d2 15ed

      ciphertext (96 octets):  170301005b706a6b 6b735ee383176d5b
         79f53c208dbc9637 4da9a2e1660f8993 3901920f749de18a
         1988eb9cc5838969 106b05690618419e db0ebd23ac400ef3
         290afea3e3d6c250 ec2ae7c599e2eb81 df4e546b797e55e4
         84b34d8eb4c99c7b

   {server}  derive secret "client application traffic secret":

      PRK (32 octets):  5d995a2374a68417 22518bedfcfcd627
         855c8fb4e18a8759 4416b19c3c4e485d

      handshake hash (32 octets):  653d913f16296ff2 630594dd59260083
         98b1541e334b77e7 5b3aef7988aa68cc
```

```
      info (78 octets):  00202a544c532031 2e332c20636c6965
         6e74206170706c69 636174696f6e2074 7261666669632073
         656372657420653d 913f16296ff26305 94dd5926008398b1
         541e334b77e75b3a ef7988aa68cc

      output (32 octets):  09d0215a03cb3192 b7701429d46a21df
         a9d70f7bb8191c94 f7643679dde02858

   {server}  derive secret "server application traffic secret":

      PRK (32 octets):  5d995a2374a68417 22518bedfcfcd627
         855c8fb4e18a8759 4416b19c3c4e485d

      handshake hash (32 octets):  653d913f16296ff2 630594dd59260083
         98b1541e334b77e7 5b3aef7988aa68cc

      info (78 octets):  00202a544c532031 2e332c2073657276
         6572206170706c69 636174696f6e2074 7261666669632073
         656372657420653d 913f16296ff26305 94dd5926008398b1
         541e334b77e75b3a ef7988aa68cc

      output (32 octets):  149a37433868240f e334f16978655b84
         f5a41ac33a8bee94 9ccb9210296fd966

   {server}  derive secret "exporter master secret":

      PRK (32 octets):  5d995a2374a68417 22518bedfcfcd627
         855c8fb4e18a8759 4416b19c3c4e485d

      handshake hash (32 octets):  653d913f16296ff2 630594dd59260083
         98b1541e334b77e7 5b3aef7988aa68cc

      info (67 octets):  00201f544c532031 2e332c206578706f
         72746572206d6173 7465722073656372 657420653d913f16
         296ff2630594dd59 26008398b1541e33 4b77e75b3aef7988 aa68cc

      output (32 octets):  5db5664ff5226633 6585be23b68f2d9a
         921d7311026df10e 1df2774d9da2eec7

   {server}  derive write traffic keys using label "application data":

      PRK (32 octets):  149a37433868240f e334f16978655b84
         f5a41ac33a8bee94 9ccb9210296fd966

      key info (16 octets):  00100c544c532031 2e332c206b657900

      key output (16 octets):  820f92209ecf5f71 e4a967edd13fd065
```

```
      iv info (15 octets):  000c0b544c532031 2e332c20697600

      iv output (12 octets):  5d1478071afaadcb d44ea6cd

   {server}  derive read traffic keys using label "early application
      data" (same as client write traffic keys)

   {client}  extract secret "handshake":

      salt (32 octets):  4134d8d48b05dfef 4658fc13f653b21b
         40426eca75a84eab 87900d991db9abfd

      ikm (32 octets):  8137f1033479e363 c531d475456a399c
         b60c5e1f13c28f5d dc761b9eac5afc66

      secret (32 octets):  2b4389f45c4c468c 1f94bf7bb6b99546
         a33c35f4c3a57a35 6dccbe99d3d56302

   {client}  derive secret "client handshake traffic secret":

      PRK (32 octets):  2b4389f45c4c468c 1f94bf7bb6b99546
         a33c35f4c3a57a35 6dccbe99d3d56302

      handshake hash (32 octets):  2fd2f168296a08d7 1a1c693b3340f152
         9326ca31c3795190 504e1d0a1261a79d

      info (76 octets):  002028544c532031 2e332c20636c6965
         6e742068616e6473 68616b6520747261 6666696320736563
         726574202fd2f168 296a08d71a1c693b 3340f1529326ca31
         c3795190504e1d0a 1261a79d

      output (32 octets):  5f9c7ffdc773eaa8 f11886ee8d5bc62e
         5bf9acb23983a321 271960d54daa730c

   {client}  derive secret "server handshake traffic secret":

      PRK (32 octets):  2b4389f45c4c468c 1f94bf7bb6b99546
         a33c35f4c3a57a35 6dccbe99d3d56302

      handshake hash (32 octets):  2fd2f168296a08d7 1a1c693b3340f152
         9326ca31c3795190 504e1d0a1261a79d

      info (76 octets):  002028544c532031 2e332c2073657276
         65722068616e6473 68616b6520747261 6666696320736563
         726574202fd2f168 296a08d71a1c693b 3340f1529326ca31
         c3795190504e1d0a 1261a79d
```

```
      output (32 octets):  eedd9ba9252944fa 8ccd415fe8897fbe
         035fbbfbb3f0afbf 71ed64d7f2278cbd

   {client}  extract secret "master" (same as server)

   {client}  derive read traffic keys using label "handshake data":

      PRK (32 octets):  eedd9ba9252944fa 8ccd415fe8897fbe
         035fbbfbb3f0afbf 71ed64d7f2278cbd

      key info (16 octets):  00100c544c532031 2e332c206b657900

      key output (16 octets):  33ebfd906881cf62 6df5af4e11583167

      iv info (15 octets):  000c0b544c532031 2e332c20697600

      iv output (12 octets):  bee0ca11151aecb4 c09f53a4

   {client}  calculate finished:

      PRK (32 octets):  eedd9ba9252944fa 8ccd415fe8897fbe
         035fbbfbb3f0afbf 71ed64d7f2278cbd

      handshake hash (0 octets):  (empty)

      info (21 octets):  002011544c532031 2e332c2066696e69 7368656400

      output (32 octets):  0fbc2652ef380d5e ea99467b0f7f8dd0
         8f9448439634a056 ebe4f673b6a6df60

   {client}  send record:

      cleartext (2 octets):  0101

      ciphertext (24 octets):  170301001329e1af f008e8f9cb64ef78
         5cb26aa4140396b8

   {client}  derive write traffic keys using label "handshake data":

      PRK (32 octets):  5f9c7ffdc773eaa8 f11886ee8d5bc62e
         5bf9acb23983a321 271960d54daa730c

      key info (16 octets):  00100c544c532031 2e332c206b657900

      key output (16 octets):  505a5542bb68c323 0316fedd6a6ef04f

      iv info (15 octets):  000c0b544c532031 2e332c20697600
```

```
      iv output (12 octets):  024cb0bcf2c8d436 cfa3a739

   {client}  derive secret "client application traffic secret":

      PRK (32 octets):  5d995a2374a68417 22518bedfcfcd627
         855c8fb4e18a8759 4416b19c3c4e485d

      handshake hash (32 octets):  653d913f16296ff2 630594dd59260083
         98b1541e334b77e7 5b3aef7988aa68cc

      info (78 octets):  00202a544c532031 2e332c20636c6965
         6e74206170706c69 636174696f6e2074 7261666669632073
         656372657420653d 913f16296ff26305 94dd5926008398b1
         541e334b77e75b3a ef7988aa68cc

      output (32 octets):  09d0215a03cb3192 b7701429d46a21df
         a9d70f7bb8191c94 f7643679dde02858

   {client}  derive secret "server application traffic secret":

      PRK (32 octets):  5d995a2374a68417 22518bedfcfcd627
         855c8fb4e18a8759 4416b19c3c4e485d

      handshake hash (32 octets):  653d913f16296ff2 630594dd59260083
         98b1541e334b77e7 5b3aef7988aa68cc

      info (78 octets):  00202a544c532031 2e332c2073657276
         6572206170706c69 636174696f6e2074 7261666669632073
         656372657420653d 913f16296ff26305 94dd5926008398b1
         541e334b77e75b3a ef7988aa68cc

      output (32 octets):  149a37433868240f e334f16978655b84
         f5a41ac33a8bee94 9ccb9210296fd966

   {client}  derive secret "exporter master secret" (same as server)

   {client}  derive read traffic keys using label "application data"
      (same as server write traffic keys)

   {client}  calculate finished:

      PRK (32 octets):  5f9c7ffdc773eaa8 f11886ee8d5bc62e
         5bf9acb23983a321 271960d54daa730c

      handshake hash (0 octets):  (empty)

      info (21 octets):  002011544c532031 2e332c2066696e69 7368656400
```

```
      output (32 octets):  1b4d3b86f9361dec 4ebb14c934750dd8
         a35f44362f8cf631 a5f839b73cd08961

   {client}  send a Finished handshake message

   {client}  send record:

      cleartext (36 octets):  14000020e43a4478 62b160d1d64f872e
         c81914ac97d6d282 9a2bdea8847b8137 5e0379ee

      ciphertext (58 octets):  1703010035ae8c37 e2d3e0083135eb7d
         35f3ef2d375b4898 fb49295699912130 6c6b367a31cb8563
         87aaad029c1b9218 b53ea4be043bd7fc 2cc1

   {client}  derive write traffic keys using label "application data":

      PRK (32 octets):  09d0215a03cb3192 b7701429d46a21df
         a9d70f7bb8191c94 f7643679dde02858

      key info (16 octets):  00100c544c532031 2e332c206b657900

      key output (16 octets):  979ea306b9b7de91 0adc3c8c72473d6a

      iv info (15 octets):  000c0b544c532031 2e332c20697600

      iv output (12 octets):  a55a4b237184c78c 535b0a22

   {client}  derive secret "resumption master secret":

      PRK (32 octets):  5d995a2374a68417 22518bedfcfcd627
         855c8fb4e18a8759 4416b19c3c4e485d

      handshake hash (32 octets):  a3da757d83c4474f 68222e715e52cdea
         38616f3dab5e9496 2e97536a54efdac8

      info (69 octets):  002021544c532031 2e332c2072657375
         6d7074696f6e206d 6173746572207365 6372657420a3da75
         7d83c4474f68222e 715e52cdea38616f 3dab5e94962e9753 6a54efdac8

      output (32 octets):  8b587b9e8ad75697 b59f164ff6fbdce4
         ae176b9d14ea8edb d1ad4429485ce9c6

   {server}  derive read traffic keys using label "handshake data":

      PRK (32 octets):  5f9c7ffdc773eaa8 f11886ee8d5bc62e
         5bf9acb23983a321 271960d54daa730c

      key info (16 octets):  00100c544c532031 2e332c206b657900
```

```
      key output (16 octets):  505a5542bb68c323 0316fedd6a6ef04f

      iv info (15 octets):  000c0b544c532031 2e332c20697600

      iv output (12 octets):  024cb0bcf2c8d436 cfa3a739

   {server}  calculate finished:

      PRK (32 octets):  5f9c7ffdc773eaa8 f11886ee8d5bc62e
         5bf9acb23983a321 271960d54daa730c

      handshake hash (0 octets):  (empty)

      info (21 octets):  002011544c532031 2e332c2066696e69 7368656400

      output (32 octets):  1b4d3b86f9361dec 4ebb14c934750dd8
         a35f44362f8cf631 a5f839b73cd08961

   {server}  derive read traffic keys using label "application data"
      (same as client write traffic keys)

   {server}  derive secret "resumption master secret" (same as client)

   {client}  send record:

      cleartext (50 octets):  0001020304050607 08090a0b0c0d0e0f
         1011121314151617 18191a1b1c1d1e1f 2021222324252627
         28292a2b2c2d2e2f 3031

      ciphertext (72 octets):  170301004367c3e4 c2e178aaad5b95f6
         9e41c757ad5575a1 745e2c4c9a8d0088 86d502a466d3f8e4
         86ee73134e3c740a 683a405ac408b1dc 21a4b22caacd90a0
         58e5f9d98285c204

   {server}  send record:

      cleartext (50 octets):  0001020304050607 08090a0b0c0d0e0f
         1011121314151617 18191a1b1c1d1e1f 2021222324252627
         28292a2b2c2d2e2f 3031

      ciphertext (72 octets):  170301004362928f 4bc451d13e46e29a
         9c1b684a0bf984ed 257be4155f3d97dc 727689e84a152fb6
         2f9103041a5dd045 34959f28fe6017dc 1b3c9d8293b2456d
         2eb3775029f7bd8a

   {client}  send record:

      cleartext (2 octets):  0100
```

ciphertext (24 octets): 17030100139d41ac 5ed9b4f06ae44f09
1c7ae9cc9e6d9793

{server} send record:

cleartext (2 octets): 0100

ciphertext (24 octets): 170301001308d06f 582c7d7294ee1b96
9aca936f2ced5471

## 5. HelloRetryRequest

In this example, the client initiates a handshake with an X25519 [RFC7748] share. The server however prefers P-256 [FIPS186] and sends a HelloRetryRequest that requires the client to generate a key share on the P-256 curve.

{client} create an ephemeral x25519 key pair:

private key (32 octets): 0a0cb6f0d87f01e3 46cd092736e1b5b7
9dc623ed53d5d030 2c46cacc61913e17

public key (32 octets): 05efa94d13f5adcd 14219379d5a37dbc
e4721d9294e572c6 651aeb761838815b

{client} send a ClientHello handshake message

{client} send record:

cleartext (174 octets): 010000aa0303d9e9 898df63d43adbe64
a2634f0b63bcdc40 19a3e526bc013a60 42e05b14555c0000
0613011303130201 00007b0000000b00 0900000673657276
6572ff0100010000 0a00080006001d00 1700180028002600
24001d002005efa9 4d13f5adcd142193 79d5a37dbce4721d
9294e572c6651aeb 761838815b002b00 03027f12000d0020
001e040305030603 0203080408050806 0401050106010201
0402050206020202 002d00020101

ciphertext (179 octets): 16030100ae010000 aa0303d9e9898df6
3d43adbe64a2634f 0b63bcdc4019a3e5 26bc013a6042e05b
14555c0000061301 130313020100007b 0000000b00090000
06736572766572ff 01000100000a0008 0006001d00170018
002800260024001d 002005efa94d13f5 adcd14219379d5a3
7dbce4721d9294e5 72c6651aeb761838 815b002b0003027f
12000d0020001e04 0305030603020308 0408050806040105
0106010201040205 0206020202002d00 020101

{server} send a HelloRetryRequest handshake message

```
   {server}  send record:

      cleartext (14 octets):  0600000a7f120006 002800020017

      ciphertext (19 octets):  160301000e060000 0a7f120006002800 020017

   {client}  create an ephemeral P-256 key pair:

      private key (32 octets):  11fa48d153c917ff d89dff13140760a1
         36265d399fa9f10e 2d766d42a6c84e90

      public key (65 octets):  041e5a785f5417fb 18db4293843534a5
         c0ba6e744baa6846 d0b32f4e9ea39227 24a08f2adb09f071
         f81402e7fd8ca33b 76abe1cd556fd3e8 fe20e0fd2e8202f9 69

   {client}  send a ClientHello handshake message

   {client}  send record:

      cleartext (207 octets):  010000cb0303d9e9 898df63d43adbe64
         a2634f0b63bcdc40 19a3e526bc013a60 42e05b14555c0000
         0613011303130201 00009c0000000b00 0900000673657276
         6572ff0100010000 0a00080006001d00 1700180028004700
         4500170041041e5a 785f5417fb18db42 93843534a5c0ba6e
         744baa6846d0b32f 4e9ea3922724a08f 2adb09f071f81402
         e7fd8ca33b76abe1 cd556fd3e8fe20e0 fd2e8202f969002b
         0003027f12000d00 20001e0403050306 0302030804080508
         0604010501060102 0104020502060202 02002d00020101

      ciphertext (212 octets):  16030100cf010000 cb0303d9e9898df6
         3d43adbe64a2634f 0b63bcdc4019a3e5 26bc013a6042e05b
         14555c0000061301 130313020100009c 0000000b00090000
         06736572766572ff 01000100000a0008 0006001d00170018
         0028004700450017 0041041e5a785f54 17fb18db42938435
         34a5c0ba6e744baa 6846d0b32f4e9ea3 922724a08f2adb09
         f071f81402e7fd8c a33b76abe1cd556f d3e8fe20e0fd2e82
         02f969002b000302 7f12000d0020001e 0403050306030203
         0804080508060401 0501060102010402 050206020202002d 00020101

   {server}  extract secret "early":

      salt:  (absent)

      ikm (32 octets):  0000000000000000 0000000000000000
         0000000000000000 0000000000000000

      secret (32 octets):  33ad0a1c607ec03b 09e6cd9893680ce2
         10adf300aa1f2660 e1b22e10f170f92a
```

```
   {server}  create an ephemeral P-256 key pair:

      private key (32 octets):  ff265d2062c70725 ca22513e1e6841ff
         475e8a00421f0818 186edd1c0080cc6a

      public key (65 octets):  048a4d09cde58dbc 041955b9a41a43c1
         696dc5429ffa96f9 cd194a863ac782f1 8159f072b4f61021
         5d86407dd7368b75 4ab2e64f2c1b3f9d 457c264e2b1781a3 6b

   {server}  send a ServerHello handshake message

   {server}  extract secret "handshake":

      salt (32 octets):  33ad0a1c607ec03b 09e6cd9893680ce2
         10adf300aa1f2660 e1b22e10f170f92a

      ikm (32 octets):  6551f8de88be4c85 a6ec245d84aa63d5
         ce85c9fdeb9398b9 b35512d372637253

      secret (32 octets):  ead65db5900e7b73 cc49689cfed1039d
         7a2f34b865915e9f a9c47c5fe6e551a8

   {server}  derive secret "client handshake traffic secret":

      PRK (32 octets):  ead65db5900e7b73 cc49689cfed1039d
         7a2f34b865915e9f a9c47c5fe6e551a8

      handshake hash (32 octets):  a5ad44690729db79 d84d7637a8f2915a
         54ab8f4cd52d2862 591392fe3255e1af

      info (76 octets):  002028544c532031 2e332c20636c6965
         6e742068616e6473 68616b6520747261 6666696320736563
         72657420a5ad4469 0729db79d84d7637 a8f2915a54ab8f4c
         d52d2862591392fe 3255e1af

      output (32 octets):  c6cfd0de3536e43c cb8522fa10d9deff
         ff1753ebf96a7d97 c6c8ccc501e57ad0

   {server}  derive secret "server handshake traffic secret":

      PRK (32 octets):  ead65db5900e7b73 cc49689cfed1039d
         7a2f34b865915e9f a9c47c5fe6e551a8

      handshake hash (32 octets):  a5ad44690729db79 d84d7637a8f2915a
         54ab8f4cd52d2862 591392fe3255e1af

      info (76 octets):  002028544c532031 2e332c2073657276
         65722068616e6473 68616b6520747261 6666696320736563
```

```
      72657420a5ad4469 0729db79d84d7637 a8f2915a54ab8f4c
      d52d2862591392fe 3255e1af

   output (32 octets):  b20106ffa8a023ba be8534eb03dd3683
      fafa594b2e9c9465 0856b64c3f318939

{server}  extract secret "master":

   salt (32 octets):  ead65db5900e7b73 cc49689cfed1039d
      7a2f34b865915e9f a9c47c5fe6e551a8

   ikm (32 octets):  0000000000000000 0000000000000000
      0000000000000000 0000000000000000

   secret (32 octets):  bf6d13ecadf8826f fed70fa62c0bf904
      d6067a7b6c4e0362 6172eec87a71b5a2

{server}  send record:

   cleartext (115 octets):  0200006f7f1296ff 693075d8465651a9
      c28773f549654220 6ba390199b9c9975 45d9a12666151301
      0049002800450017 0041048a4d09cde5 8dbc041955b9a41a
      43c1696dc5429ffa 96f9cd194a863ac7 82f18159f072b4f6
      10215d86407dd736 8b754ab2e64f2c1b 3f9d457c264e2b17 81a36b

   ciphertext (120 octets):  1603010073020000 6f7f1296ff693075
      d8465651a9c28773 f5496542206ba390 199b9c997545d9a1
      2666151301004900 2800450017004104 8a4d09cde58dbc04
      1955b9a41a43c169 6dc5429ffa96f9cd 194a863ac782f181
      59f072b4f610215d 86407dd7368b754a b2e64f2c1b3f9d45
      7c264e2b1781a36b

{server}  derive write traffic keys using label "handshake data":

   PRK (32 octets):  b20106ffa8a023ba be8534eb03dd3683
      fafa594b2e9c9465 0856b64c3f318939

   key info (16 octets):  00100c544c532031 2e332c206b657900

   key output (16 octets):  f1c0114cbc1391f0 023187ab7ab4eac1

   iv info (15 octets):  000c0b544c532031 2e332c20697600

   iv output (12 octets):  b28638f5018dbb8f 6b5d1314

{server}  send a EncryptedExtensions handshake message

{server}  send a Certificate handshake message
```

```
   {server}  send a CertificateVerify handshake message

   {server}  calculate finished:

      PRK (32 octets):  b20106ffa8a023ba be8534eb03dd3683
         fafa594b2e9c9465 0856b64c3f318939

      handshake hash (0 octets):  (empty)

      info (21 octets):  002011544c532031 2e332c2066696e69 7368656400

      output (32 octets):  7b88ebd4056b7e68 d2477433058cf559
         15ffa712d01141fd a135a49b7e3f7a56

   {server}  send a Finished handshake message

   {server}  send record:

      cleartext (639 octets):  080000120010000a 0008000600170018
         001d000000000b00 01b9000001b50001 b0308201ac308201
         15a0030201020201 02300d06092a8648 86f70d01010b0500
         300e310c300a0603 5504031303727361 301e170d31363037
         3330303132333539 5a170d3236303733 303031323335395a
         300e310c300a0603 5504031303727361 30819f300d06092a
         864886f70d010101 050003818d003081 8902818100b4bb49
         8f8279303d980836 399b36c6988c0c68 de55e1bdb826d390
         1a2461eafd2de49a 91d015abbc9a9513 7ace6c1af19eaa6a
         f98c7ced43120998 e187a80ee0ccb052 4b1b018c3e0b6326
         4d449a6d38e22a5f da43084674803053 0ef0461c8ca9d9ef
         bfae8ea6d1d03e2b d193eff0ab9a8002 c47428a6d35a8d88
         d79f7f1e3f020301 0001a31a30183009 0603551d13040230
         00300b0603551d0f 0404030205a0300d 06092a864886f70d
         01010b0500038181 0085aad2a0e5b927 6b908c65f73a7267
         170618a54c5f8a7b 337d2df7a5943654 17f2eae8f8a58c8f
         8172f9319cf36b7f d6c55b80f21a0301 5156726096fd335e
         5e67f2dbf102702e 608ccae6bec1fc63 a42a99be5c3eb710
         7c3c54e9b9eb2bd5 203b1c3b84e0a8b2 f759409ba3eac9d9
         1d402dcc0cc8f896 1229ac9187b42b4d e100000f00008408
         040080a2427ae5f8 0c99ee8e72b7ddee b2f512458f7f6325
         1b8a77ace3b1577a ac9a8fcd73bb6a33 5a3446d66b2debb7
         f90d6eb8701f3ab1 69793295b34251b9 e6d5fe0251478e8a
         6ab8b79651ea64c9 b598c8628893c867 9b7400177bc5e457
         a539316b5ebd7d08 f380593f0541d781 f0dd28b41a062aad
         e8bf20074c6eda9c 01c75b140000208e 0bdf3cb16b0b2560
         51b37de6704e005d 2a4600cd0c38cae9 0a79eac6ed1bf1

      ciphertext (661 octets):  170301029081de4f cfd700da4573d570
         5942f14a11e569aa 9aacc95260520102 6f74f2b2ad6abe08
```

```
      7b53a4940ff94208 9e02d3159b1c6f11 75d7fcb51abad6fd
      d4f7ff4af6590b47 16c1d90e1031e1a1 e32079f531108c6b
      9f79d6120319e0a3 73010e82d780a8f9 c3fdf8474840cdb6
      7e4943d3808a27cd 5d9375c766a95ef4 8393c235d83ad26a
      20628671793f75df aa0be78b11fed206 6506d19a769d9d32
      adc0437784994359 ef5e452609353670 1c46004cf6fc252e
      546e797238c73b94 b073461158301f78 1498917c32dc0ece
      658a53790c667397 f7744775c2bef907 b5f7d5677b2e57fe
      7c4bfd43c7ad1ee4 6fd400c3d3c3c05f e8775f055263e98a
      692b49a818d0f698 4400c1db2f429fa8 9fb61d523398e1d0
      2bc5c393027146c0 f326032d18cb8283 473f2b6d554df942
      c7b1a0050694c7b2 bf31a816f7ff77f1 d7db873dbb6e4646
      acabfa73c317a34c e6212a3469f549e6 cde71ab229a6f220
      acda60832b510663 02a23d02c734bd5e 71b04fb248ca47ba
      0c7b1fd28fee9b5d 86e6b1a6a2a1a43e 3831210519f54134
      c96486d11ef3125f 74969785690487e0 aa5c0a310ebf9d31
      95ec5543af8a6ffb 710eb0a90285960d c1ccdc10ecee9669
      9171e97eae526a17 205012ab6f262e44 31ae9a70ff2ed7bd
      966ef6bd4563f56a 7a14970dcabf97ae 7e4354db1ea27548
      c55c11542ad07bcd 6f47a7143b86c4e6 678ce7dc6d51a1b7
      75687644d6526efa 3c864f592819e7b7 f9f1bbc02ed8821a
      e66019b240b41f5e ebf9475069700030 7122f7c8a8d6c0da
      a264c63183238d72 0eacb86879fab9ba 8a673c51a52c8284
      75e3211223cd2238 bd8b8a934af3e4dd e10e788df23ad6d8
      51d68b78082ac667 a854356415e7858b e526307332990d8c
      c38a5dc4cfc22a2c a2bdd9126a2ce13d 7015264921

{server}  derive secret "client application traffic secret":

   PRK (32 octets):  bf6d13ecadf8826f fed70fa62c0bf904
      d6067a7b6c4e0362 6172eec87a71b5a2

   handshake hash (32 octets):  dd0da93863ed291f 518b94a83093da6b
      8edd2d25470c20cd c3becba4eee76c49

   info (78 octets):  00202a544c532031 2e332c20636c6965
      6e74206170706c69 636174696f6e2074 7261666669632073
      656372657420dd0d a93863ed291f518b 94a83093da6b8edd
      2d25470c20cdc3be cba4eee76c49

   output (32 octets):  a754e4ccfbb7363d fdc7a57028da0867
      f804f958c38caead 1e656380d64fd662

{server}  derive secret "server application traffic secret":

   PRK (32 octets):  bf6d13ecadf8826f fed70fa62c0bf904
      d6067a7b6c4e0362 6172eec87a71b5a2
```

handshake hash (32 octets): dd0da93863ed291f 518b94a83093da6b
8edd2d25470c20cd c3becba4eee76c49

info (78 octets): 00202a544c532031 2e332c2073657276
6572206170706c69 636174696f6e2074 7261666669632073
656372657420dd0d a93863ed291f518b 94a83093da6b8edd
2d25470c20cdc3be cba4eee76c49

output (32 octets): fa2a2be1efe55357 c112071aa4a62c3f
ec646fa0d7883092 fc9087dc5405c7a4

{server} derive secret "exporter master secret":

PRK (32 octets): bf6d13ecadf8826f fed70fa62c0bf904
d6067a7b6c4e0362 6172eec87a71b5a2

handshake hash (32 octets): dd0da93863ed291f 518b94a83093da6b
8edd2d25470c20cd c3becba4eee76c49

info (67 octets): 00201f544c532031 2e332c206578706f
72746572206d6173 7465722073656372 657420dd0da93863
ed291f518b94a830 93da6b8edd2d2547 0c20cdc3becba4ee e76c49

output (32 octets): f8538fa665addfe5 a88955dd68be1d39
874aa7a07f5c999d 6658f47a498029b7

{server} derive write traffic keys using label "application data":

PRK (32 octets): fa2a2be1efe55357 c112071aa4a62c3f
ec646fa0d7883092 fc9087dc5405c7a4

key info (16 octets): 00100c544c532031 2e332c206b657900

key output (16 octets): 5e7915cfd47985ac cedca500e9d65e13

iv info (15 octets): 000c0b544c532031 2e332c20697600

iv output (12 octets): b0b11ff319194dc7 c1ba7a3e

{server} derive read traffic keys using label "handshake data":

PRK (32 octets): c6cfd0de3536e43c cb8522fa10d9deff
ff1753ebf96a7d97 c6c8ccc501e57ad0

key info (16 octets): 00100c544c532031 2e332c206b657900

key output (16 octets): 9a9244d62def9bb2 0e9486b71569fdd3

```
      iv info (15 octets):  000c0b544c532031 2e332c20697600

      iv output (12 octets):  564fe61b06a369d1 665cd57a

   {client}  extract secret "early":

      salt:  (absent)

      ikm (32 octets):  0000000000000000 0000000000000000
         0000000000000000 0000000000000000

      secret (32 octets):  33ad0a1c607ec03b 09e6cd9893680ce2
         10adf300aa1f2660 e1b22e10f170f92a

   {client}  extract secret "handshake":

      salt (32 octets):  33ad0a1c607ec03b 09e6cd9893680ce2
         10adf300aa1f2660 e1b22e10f170f92a

      ikm (32 octets):  6551f8de88be4c85 a6ec245d84aa63d5
         ce85c9fdeb9398b9 b35512d372637253

      secret (32 octets):  ead65db5900e7b73 cc49689cfed1039d
         7a2f34b865915e9f a9c47c5fe6e551a8

   {client}  derive secret "client handshake traffic secret":

      PRK (32 octets):  ead65db5900e7b73 cc49689cfed1039d
         7a2f34b865915e9f a9c47c5fe6e551a8

      handshake hash (32 octets):  a5ad44690729db79 d84d7637a8f2915a
         54ab8f4cd52d2862 591392fe3255e1af

      info (76 octets):  002028544c532031 2e332c20636c6965
         6e742068616e6473 68616b6520747261 6666696320736563
         72657420a5ad4469 0729db79d84d7637 a8f2915a54ab8f4c
         d52d2862591392fe 3255e1af

      output (32 octets):  c6cfd0de3536e43c cb8522fa10d9deff
         ff1753ebf96a7d97 c6c8ccc501e57ad0

   {client}  derive secret "server handshake traffic secret":

      PRK (32 octets):  ead65db5900e7b73 cc49689cfed1039d
         7a2f34b865915e9f a9c47c5fe6e551a8

      handshake hash (32 octets):  a5ad44690729db79 d84d7637a8f2915a
         54ab8f4cd52d2862 591392fe3255e1af
```

```
      info (76 octets):  002028544c532031 2e332c2073657276
         65722068616e6473 68616b6520747261 6666696320736563
         72657420a5ad4469 0729db79d84d7637 a8f2915a54ab8f4c
         d52d2862591392fe 3255e1af

      output (32 octets):  b20106ffa8a023ba be8534eb03dd3683
         fafa594b2e9c9465 0856b64c3f318939

   {client}  extract secret "master" (same as server)

   {client}  derive read traffic keys using label "handshake data":

      PRK (32 octets):  b20106ffa8a023ba be8534eb03dd3683
         fafa594b2e9c9465 0856b64c3f318939

      key info (16 octets):  00100c544c532031 2e332c206b657900

      key output (16 octets):  f1c0114cbc1391f0 023187ab7ab4eac1

      iv info (15 octets):  000c0b544c532031 2e332c20697600

      iv output (12 octets):  b28638f5018dbb8f 6b5d1314

   {client}  calculate finished:

      PRK (32 octets):  b20106ffa8a023ba be8534eb03dd3683
         fafa594b2e9c9465 0856b64c3f318939

      handshake hash (0 octets):  (empty)

      info (21 octets):  002011544c532031 2e332c2066696e69 7368656400

      output (32 octets):  7b88ebd4056b7e68 d2477433058cf559
         15ffa712d01141fd a135a49b7e3f7a56

   {client}  derive write traffic keys using label "handshake data"
      (same as server read traffic keys)

   {client}  derive secret "client application traffic secret":

      PRK (32 octets):  bf6d13ecadf8826f fed70fa62c0bf904
         d6067a7b6c4e0362 6172eec87a71b5a2

      handshake hash (32 octets):  dd0da93863ed291f 518b94a83093da6b
         8edd2d25470c20cd c3becba4eee76c49

      info (78 octets):  00202a544c532031 2e332c20636c6965
         6e74206170706c69 636174696f6e2074 7261666669632073
```

```
         656372657420dd0d a93863ed291f518b 94a83093da6b8edd
         2d25470c20cdc3be cba4eee76c49

      output (32 octets):  a754e4ccfbb7363d fdc7a57028da0867
         f804f958c38caead 1e656380d64fd662

   {client}  derive secret "server application traffic secret":

      PRK (32 octets):  bf6d13ecadf8826f fed70fa62c0bf904
         d6067a7b6c4e0362 6172eec87a71b5a2

      handshake hash (32 octets):  dd0da93863ed291f 518b94a83093da6b
         8edd2d25470c20cd c3becba4eee76c49

      info (78 octets):  00202a544c532031 2e332c2073657276
         6572206170706c69 636174696f6e2074 7261666669632073
         656372657420dd0d a93863ed291f518b 94a83093da6b8edd
         2d25470c20cdc3be cba4eee76c49

      output (32 octets):  fa2a2be1efe55357 c112071aa4a62c3f
         ec646fa0d7883092 fc9087dc5405c7a4

   {client}  derive secret "exporter master secret" (same as server)

   {client}  derive read traffic keys using label "application data"
      (same as server write traffic keys)

   {client}  calculate finished:

      PRK (32 octets):  c6cfd0de3536e43c cb8522fa10d9deff
         ff1753ebf96a7d97 c6c8ccc501e57ad0

      handshake hash (0 octets):  (empty)

      info (21 octets):  002011544c532031 2e332c2066696e69 7368656400

      output (32 octets):  621f7d1de488a6bb 3874e3a03ded00e0
         4c9bd054c85b95e3 b65e7423ac3f3b88

   {client}  send a Finished handshake message

   {client}  send record:

      cleartext (36 octets):  14000020fc53f1be b1436fb968319299
         a9e3b6088cc99e42 178c77337bc52786 d084882f
```

```
      ciphertext (58 octets):  170301003543adad e592362412fb77d7
         28b181c01b77cd62 a661e4125e6f9851 826e418f4c292ec6
         3254e8b0342d65db 8a7f074eed527ea6 98a6

   {client}  derive write traffic keys using label "application data":

      PRK (32 octets):  a754e4ccfbb7363d fdc7a57028da0867
         f804f958c38caead 1e656380d64fd662

      key info (16 octets):  00100c544c532031 2e332c206b657900

      key output (16 octets):  0e2e7a8db77587cf 18388def90b15063

      iv info (15 octets):  000c0b544c532031 2e332c20697600

      iv output (12 octets):  56140ec2f82b9649 b0eefbfa

   {client}  derive secret "resumption master secret":

      PRK (32 octets):  bf6d13ecadf8826f fed70fa62c0bf904
         d6067a7b6c4e0362 6172eec87a71b5a2

      handshake hash (32 octets):  ad82e98953633398 4f4733bdac834b98
         63d05680cfb820cf c07c923029af4642

      info (69 octets):  002021544c532031 2e332c2072657375
         6d7074696f6e206d 6173746572207365 6372657420ad82e9
         89536333984f4733 bdac834b9863d056 80cfb820cfc07c92 3029af4642

      output (32 octets):  8a4f85ba26bb67b7 0df06509177d7e91
         8808eccada5604b1 61e378fe0803c374

   {server}  calculate finished:

      PRK (32 octets):  c6cfd0de3536e43c cb8522fa10d9deff
         ff1753ebf96a7d97 c6c8ccc501e57ad0

      handshake hash (0 octets):  (empty)

      info (21 octets):  002011544c532031 2e332c2066696e69 7368656400

      output (32 octets):  621f7d1de488a6bb 3874e3a03ded00e0
         4c9bd054c85b95e3 b65e7423ac3f3b88

   {server}  derive read traffic keys using label "application data"
      (same as client write traffic keys)

   {server}  derive secret "resumption master secret" (same as client)
```

{client} send record:

cleartext (2 octets): 0100

ciphertext (24 octets): 17030100131ef5c9 e7205f31a1edf9b1
3600fec1271e4f5d

{server} send record:

cleartext (2 octets): 0100

ciphertext (24 octets): 170301001350ff6e 907c508b6b191ff6
094faf4c0b32d6a8

## 6. Security Considerations

It probably isn't a good idea to use the private key here. If it weren't for the fact that it is too small to provide any meaningful security, it is now very well known.

## 7. References

### 7.1. Normative References

[I-D.ietf-tls-tls13]
Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", draft-ietf-tls-tls13-18 (work in progress), October 2016.

### 7.2. Informative References

[FIPS186] National Institute of Standards and Technology (NIST), "Digital Signature Standard (DSS)", NIST PUB 186-4 , July 2013.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <http://www.rfc-editor.org/info/rfc7748>.

## Appendix A. Acknowledgements

None of this would have been possible without Franziskus Kiefer, Eric Rescorla and Tim Taubert, who did a lot of the work in NSS.

Author's Address

Martin Thomson
Mozilla

Email: martin.thomson@gmail.com