HTTP
Internet-Draft
Intended status: Standards Track
Expires: May 17, 2017

M. Thomson
Mozilla

November 13, 2016

Example Handshake Traces for TLS 1.3
draft-thomson-tls-tls13-vectors-01

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.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 17, 2017.

Copyright Notice

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):  03bd8bca70c19f65 7e897e366dbe21a4
      66e4924af6082dbd f573827bcdde5def
```

```
      public key (32 octets):  2a981db6cdd02a06 c1763102c9e74136
         5ac4e6f72b3176a6 bd6a3523d3ec0f4c

   {client}  send a ClientHello handshake message

   {client}  send record:

      cleartext (512 octets):  010001fc0303ce05 cfa3d92170cbc246
         5cdc3e3a2f577f6e ac809361708ab244 b07d8fad86160000
         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
         1d00202a981db6cd d02a06c1763102c9 e741365ac4e6f72b
         3176a6bd6a3523d3 ec0f4c002b000706 7f1203030302000d
         0020001e04030503 0603020308040805 0806040105010601
         0201040205020602 0202002d00020101

      ciphertext (517 octets):  1603010200010001 fc0303ce05cfa3d9
         2170cbc2465cdc3e 3a2f577f6eac8093 61708ab244b07d8f
         ad861600003e1301 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 0000000000000000
      0000000000000000 0000000000000000 0000000b00090000
      06736572766572ff 01000100000a0014 0012001d00170018
      0019010001010102 01030104000b0002 0100002300000028
      00260024001d0020 2a981db6cdd02a06 c1763102c9e74136
      5ac4e6f72b3176a6 bd6a3523d3ec0f4c 002b0007067f1203
      030302000d002000 1e04030503060302 0308040805080604
      0105010601020104 0205020602020200 2d00020101
```

{server} extract secret "early":

salt (0 octets): (empty)

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): 0cc3d0a7806ef6bc df69be30c6855597 7b51e0f5edbf1d1c c7b28eead93b34b4

public key (32 octets): 9c1b0a7421919a73 cb57b3a0ad9d6805 861a9c47e11df863 9d25323b79ce201c

{server} send a ServerHello handshake message

{server} extract secret "handshake":

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

ikm (32 octets): 0dfa4c5e11a6f606 d4b75f138412d85a 4b2da0d5f981ffc1 d2e8ceff2e00a12c

secret (32 octets): 1b3f45dcdc375a9a e91bf34d669f24c7

```
      53132f1d394553af bfffe6568a27e22c

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

      PRK (32 octets):  1b3f45dcdc375a9a e91bf34d669f24c7
         53132f1d394553af bfffe6568a27e22c

      handshake hash (32 octets):  79027f438271dba2 d8e207b6e36a5180
         bdd916869ab43f24 f2e2fa98b2db135c

      info (76 octets):  002028544c532031 2e332c20636c6965
         6e742068616e6473 68616b6520747261 6666696320736563
         7265742079027f43 8271dba2d8e207b6 e36a5180bdd91686
         9ab43f24f2e2fa98 b2db135c

      output (32 octets):  f737c2b29be2ef48 9d145dd3df485103
         86e812edcf799925 27e9ad5479967193

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

      PRK (32 octets):  1b3f45dcdc375a9a e91bf34d669f24c7
         53132f1d394553af bfffe6568a27e22c

      handshake hash (32 octets):  79027f438271dba2 d8e207b6e36a5180
         bdd916869ab43f24 f2e2fa98b2db135c
```



```
      info (76 octets):  002028544c532031 2e332c2073657276
         65722068616e6473 68616b6520747261 6666696320736563
         7265742079027f43 8271dba2d8e207b6 e36a5180bdd91686
         9ab43f24f2e2fa98 b2db135c

      output (32 octets):  3550ca3a8c219272 9cc385313e3bc832
         92a14f4ecb3d2b92 18ea7907c67ab3a7

   {server}  extract secret "master":

      salt (32 octets):  1b3f45dcdc375a9a e91bf34d669f24c7
         53132f1d394553af bfffe6568a27e22c

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

```
   secret (32 octets):  cab4645a3995d0d8 5bea9942596284e7
      2058a3d4d8f3e0d9 885aa92c517ad9e4

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

   PRK (32 octets):  3550ca3a8c219272 9cc385313e3bc832
      92a14f4ecb3d2b92 18ea7907c67ab3a7

   key info (16 octets):  00100c544c532031 2e332c206b657900

   key output (16 octets):  d2dd45f87ad87801 a85ac38187f9023b

   iv info (15 octets):  000c0b544c532031 2e332c20697600

   iv output (12 octets):  f0a14f808692cef8 7a3daf70

{server}  send record:

   cleartext (82 octets):  0200004e7f1220b9 c9201cd171a15abb
      a4e7eddcf3e8488e 7192ffe01ea5c19f 3d4b52ffeebe1301
      002800280024001d 00209c1b0a742191 9a73cb57b3a0ad9d
      6805861a9c47e11d f8639d25323b79ce 201c

   ciphertext (87 octets):  1603010052020000 4e7f1220b9c9201c
      d171a15abba4e7ed dcf3e8488e7192ff e01ea5c19f3d4b52
      ffeebe1301002800 280024001d00209c 1b0a7421919a73cb
      57b3a0ad9d680586 1a9c47e11df8639d 25323b79ce201c

{server}  send a EncryptedExtensions handshake message

{server}  send a Certificate handshake message
```



```
{server}  send a CertificateVerify handshake message

{server}  calculate finished:

   PRK (32 octets):  3550ca3a8c219272 9cc385313e3bc832
      92a14f4ecb3d2b92 18ea7907c67ab3a7

   handshake hash (0 octets):  (empty)
```

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

      output (32 octets):  1ba8c586468bb93d cd9264e62929e77d
         eba36e5bfc5e06ad 029f667448e5e6c8

   {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 0000840804008013 4e22eac57321ab47
         db6b38b2992cec2d d79bd065a034a9af 6b9e3d03475e4309
         e6523ccdf055453f b480804a3a7e9962 29eb28e734f6702b
         ea2b32149899ac04 3a4b44468197868d a77147ce9f73c054
         3c4e3fc33e306cac 8506faa80a959c5f 1edccbee76eda1ad
         7a4fa440de35dcb8 7e82ec94e8725355 ce7507713a609e14
         0000207304bb7332 1f01b71dd94622fa e98daf634490d220
         e4c8f3ffa2559911 a56e51
```



```
      ciphertext (673 octets):  170301029c40ae92 071a3a548b26af31
```

```
      e116dfc0ba454921 0b17e70da16cfbda 9ccdad844d94264a
      9ae65b786b3eaf0d e20aa89c6babb448 b6f32d07f2335842
      96eefe19316bd979 659472ee8567cb01 d70b0366cddb3c60
      eb9e1d789a3691dc 254c14de73f4f201 00504544ce184d44
      547e124b1f18303b 4859f8f2e2b04423 d23a866b43866374
      d54af41649d25f4a 3ec2cecd5d4e6de1 b24953440b46fbb7
      4c1dbec6fbb1f16b c21d4aa0e1e936a4 9c07127e19719bc6
      52a2f0b7f8df4a15 0b2b3c9e9e353d6e d101970ddc611aba
      d0632c6793f9379c 9d06846c311fcbd6 f85edd569b8782c4
      c5f62294c4611ae6 0f83230a53aa95e3 bcbed204f19a7a1d
      b83c0fbfec1edd2c 17498fa7b5aa2321 248a92592d891e49
      47df6bcef52f4481 797d032ad332046a 384abece6454b3e3
      56d7249bfa569679 3c7f7d3048dc87fa 7409a4691887caaf
      0982c402b902d699 f62dc4d5e153f13e 8589e4a6206c7f74
      eb26ddefbb92309f b753decfea972dec 7de02eda9c6d26ac
      d7be53a8aa20f1a9 3f082ae6eb927a6a 1b7bd9153551aedf
      af94f61dd4cb9355 ad7ab09f615d9f92 c21712c732c0e7e1
      17797f38cbdc184e 3a65e15a89f46cb3 624f5fdb8dbbd275
      f2c8492f8d95bdbd 8d1dc1b9f21107bd 433acbbac247239c
      073a2f24a4a9f807 4f325f277d579b6b ff0269ff19aed380
      9a9ddd21dd29c136 3c9dc44812dd41d2 111f9c2e8342046c
      14133b853262676f 15e94de18660e04a e5c0c661ea43559a
      f5842e161c83dd29 f64508b2ec3e635a 2134fc0e1a39d3ec
      b51dcddfcf8382c8 8ffe2a737842ad1d e7fe505b6c4d1673
      870f6fc2a0f2f797 2acaee368a1599d6 4ba18798f10333f9
      779bd5b05f9b084d 03dab2f3d80c2eb7 4ec70c9866ea31c1
      8b491cd597aae3e9 41205fcc38a3a10c e8c0269f02ccc9c5
      1278e25f1a0f0731 a9

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

   PRK (32 octets):  cab4645a3995d0d8 5bea9942596284e7
      2058a3d4d8f3e0d9 885aa92c517ad9e4

   handshake hash (32 octets):  16756399da565370 337a4ede5774b9e6
      0bf328086272dc39 3b8b1d8ba6e6ebbb

   info (78 octets):  00202a544c532031 2e332c20636c6965
      6e74206170706c69 636174696f6e2074 7261666669632073
      6563726574201675 6399da565370337a 4ede5774b9e60bf3
      28086272dc393b8b 1d8ba6e6ebbb

   output (32 octets):  2a1d25e6f9f13f92 e4b482fa06bc4447
      1218368d2d4e03e0 504d4e342b16ff8f

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

PRK (32 octets): cab4645a3995d0d8 5bea9942596284e7
2058a3d4d8f3e0d9 885aa92c517ad9e4

handshake hash (32 octets): 16756399da565370 337a4ede5774b9e6
0bf328086272dc39 3b8b1d8ba6e6ebbb

info (78 octets): 00202a544c532031 2e332c2073657276
6572206170706c69 636174696f6e2074 7261666669632073
6563726574201675 6399da565370337a 4ede5774b9e60bf3
28086272dc393b8b 1d8ba6e6ebbb

output (32 octets): 56231ff04300e7f7 4964da88c8bbdf12
42a31ade351ce974 46598d28632e79ca

{server} derive secret "exporter master secret":

PRK (32 octets): cab4645a3995d0d8 5bea9942596284e7
2058a3d4d8f3e0d9 885aa92c517ad9e4

handshake hash (32 octets): 16756399da565370 337a4ede5774b9e6
0bf328086272dc39 3b8b1d8ba6e6ebbb

info (67 octets): 00201f544c532031 2e332c206578706f
72746572206d6173 7465722073656372 65742016756399da
565370337a4ede57 74b9e60bf3280862 72dc393b8b1d8ba6 e6ebbb

output (32 octets): 407265d811f66c24 30de0832fbc4bd25
719a4736301f1312 98fd9107653a78f2

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

PRK (32 octets): 56231ff04300e7f7 4964da88c8bbdf12
42a31ade351ce974 46598d28632e79ca

key info (16 octets): 00100c544c532031 2e332c206b657900

key output (16 octets): 3381f6b3f94500f1 6226de440193e858

iv info (15 octets): 000c0b544c532031 2e332c20697600

iv output (12 octets): 4f1d73cc1d465eb3 0021c41f

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

PRK (32 octets): f737c2b29be2ef48 9d145dd3df485103
86e812edcf799925 27e9ad5479967193

key info (16 octets): 00100c544c532031 2e332c206b657900

key output (16 octets): 40e1201d75d41962 7f04c88530a15c9d

iv info (15 octets): 000c0b544c532031 2e332c20697600

iv output (12 octets): a0f073f3b35e18f9 6969696b

{client} extract secret "early":

salt (0 octets): (empty)

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): 0dfa4c5e11a6f606 d4b75f138412d85a
4b2da0d5f981ffc1 d2e8ceff2e00a12c

secret (32 octets): 1b3f45dcdc375a9a e91bf34d669f24c7
53132f1d394553af bfffe6568a27e22c

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

PRK (32 octets): 1b3f45dcdc375a9a e91bf34d669f24c7
53132f1d394553af bfffe6568a27e22c

handshake hash (32 octets): 79027f438271dba2 d8e207b6e36a5180
bdd916869ab43f24 f2e2fa98b2db135c

info (76 octets): 002028544c532031 2e332c20636c6965
6e742068616e6473 68616b6520747261 6666696320736563
7265742079027f43 8271dba2d8e207b6 e36a5180bdd91686
9ab43f24f2e2fa98 b2db135c

```
      output (32 octets):  f737c2b29be2ef48 9d145dd3df485103
         86e812edcf799925 27e9ad5479967193

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

      PRK (32 octets):  1b3f45dcdc375a9a e91bf34d669f24c7
         53132f1d394553af bfffe6568a27e22c
```



```
      handshake hash (32 octets):  79027f438271dba2 d8e207b6e36a5180
         bdd916869ab43f24 f2e2fa98b2db135c

      info (76 octets):  002028544c532031 2e332c2073657276
         65722068616e6473 68616b6520747261 6666696320736563
         7265742079027f43 8271dba2d8e207b6 e36a5180bdd91686
         9ab43f24f2e2fa98 b2db135c

      output (32 octets):  3550ca3a8c219272 9cc385313e3bc832
         92a14f4ecb3d2b92 18ea7907c67ab3a7

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

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

      PRK (32 octets):  3550ca3a8c219272 9cc385313e3bc832
         92a14f4ecb3d2b92 18ea7907c67ab3a7

      key info (16 octets):  00100c544c532031 2e332c206b657900

      key output (16 octets):  d2dd45f87ad87801 a85ac38187f9023b

      iv info (15 octets):  000c0b544c532031 2e332c20697600

      iv output (12 octets):  f0a14f808692cef8 7a3daf70

   {client}  calculate finished:

      PRK (32 octets):  3550ca3a8c219272 9cc385313e3bc832
         92a14f4ecb3d2b92 18ea7907c67ab3a7

      handshake hash (0 octets):  (empty)
```

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

   output (32 octets):  1ba8c586468bb93d cd9264e62929e77d
      eba36e5bfc5e06ad 029f667448e5e6c8

{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):  cab4645a3995d0d8 5bea9942596284e7
      2058a3d4d8f3e0d9 885aa92c517ad9e4

   handshake hash (32 octets):  16756399da565370 337a4ede5774b9e6
      0bf328086272dc39 3b8b1d8ba6e6ebbb
```



```
   info (78 octets):  00202a544c532031 2e332c20636c6965
      6e74206170706c69 636174696f6e2074 7261666669632073
      6563726574201675 6399da565370337a 4ede5774b9e60bf3
      28086272dc393b8b 1d8ba6e6ebbb

   output (32 octets):  2a1d25e6f9f13f92 e4b482fa06bc4447
      1218368d2d4e03e0 504d4e342b16ff8f

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

   PRK (32 octets):  cab4645a3995d0d8 5bea9942596284e7
      2058a3d4d8f3e0d9 885aa92c517ad9e4

   handshake hash (32 octets):  16756399da565370 337a4ede5774b9e6
      0bf328086272dc39 3b8b1d8ba6e6ebbb

   info (78 octets):  00202a544c532031 2e332c2073657276
      6572206170706c69 636174696f6e2074 7261666669632073
      6563726574201675 6399da565370337a 4ede5774b9e60bf3
      28086272dc393b8b 1d8ba6e6ebbb

   output (32 octets):  56231ff04300e7f7 4964da88c8bbdf12
      42a31ade351ce974 46598d28632e79ca

{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): f737c2b29be2ef48 9d145dd3df485103
      86e812edcf799925 27e9ad5479967193

   handshake hash (0 octets): (empty)

   info (21 octets): 002011544c532031 2e332c2066696e69 7368656400

   output (32 octets): ea2fe9596714c959 d1cdd8f8cd893b96
      6429ee678bc7105e a10e6b4c03e2425a

{client} send a Finished handshake message

{client} send record:

   cleartext (36 octets): 1400002078367856 d3c8cc4e0a95eb98
      906ca7a48bd3cc70 29f48bd4ae0dc91a b903ca89

   ciphertext (58 octets): 1703010035fa15e9 2daa21cd05d8f9c3
      152a61748d9aaf04 9da559718e583f95 aacecad657b52a65
      62da09a5819e864d 86ac2989360a1eb2 2795

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

   PRK (32 octets): 2a1d25e6f9f13f92 e4b482fa06bc4447
      1218368d2d4e03e0 504d4e342b16ff8f

   key info (16 octets): 00100c544c532031 2e332c206b657900

   key output (16 octets): eb23a804904b80ba 4fe8399e09b1ce42

   iv info (15 octets): 000c0b544c532031 2e332c20697600

   iv output (12 octets): efa8c50c06b9c9b8 c483e174

{client} derive secret "resumption master secret":

```
   PRK (32 octets):  cab4645a3995d0d8 5bea9942596284e7
      2058a3d4d8f3e0d9 885aa92c517ad9e4

   handshake hash (32 octets):  e74cc34c780d9562 b1b3e7321f2ebcb0
      e6646246dbae060d 5d1335ac5f8db917

   info (69 octets):  002021544c532031 2e332c2072657375
      6d7074696f6e206d 6173746572207365 6372657420e74cc3
      4c780d9562b1b3e7 321f2ebcb0e66462 46dbae060d5d1335 ac5f8db917

   output (32 octets):  05438edfa0f6e663 0d7a9ffe81dc6773
      6d753a4ee351a79d 296975918b16039e

{server}  calculate finished:

   PRK (32 octets):  f737c2b29be2ef48 9d145dd3df485103
      86e812edcf799925 27e9ad5479967193

   handshake hash (0 octets):  (empty)

   info (21 octets):  002011544c532031 2e332c2066696e69 7368656400

   output (32 octets):  ea2fe9596714c959 d1cdd8f8cd893b96
      6429ee678bc7105e a10e6b4c03e2425a

{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 4abe594b00924e53
      5321cadc96238da0 9caf9b02fecafdd6 5e3e418f03e43772
      cf512ed806610050 3b1c08abbbf298a9 d138ce821dd12fe1
      710e2137cd12e6a8 5cd3fd7f73706e7f 5dddefb87c1ef838
      24638464099c9d13 63e3c64ed2075c16 b8ccd8e524a6bbd7
      a6a6e34ea1579782 b15bbe7dfed5c0c0 d980fb330f9d8ab2
      52ffe7be1277d418 b6828ead4dae3b30 d448442417ef76af
```

```
      0008002e00040002 0000

   ciphertext (192 octets):  17030100bb45a662 6fa13b66ce2c5b3e
      f807e299a118296f 26a2dd9ec7487a06 73e2460d4c79f400
      87dcd014c59c5137 9c90d26b4e4f9bb2 b78f5b6761594f01
      3ff3e4c78d836905 229eac811c4ef8b2 faa89867e9ffc586
      f7f03c216591aa5e 620eac3c62dfe60f 846036bd7ecc4464
      b584af184e9644e9 4ee1d7834dba408a 51cbe4248004796e
      d9c558e0f5f96115 a6f6ba487e17d16a 2e20a3d3a650a9a0
      70fb53d9da82864b 5621d77650bd0c79 47e9889917b53d05
      15627c72b0ded521

{client}  send record:

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

   ciphertext (72 octets):  1703010043e30617 8ad97f74bb64f35e
      af3c39846b83aef8 472cbc9046749b81 a949dfb12cfbc65c
      babd20ade92c1f94 4605892ceeb12fde e8a927bce77c8303
      6ac5a794a8f54a69

{server}  send record:

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

   ciphertext (72 octets):  1703010043467d99 a807dbf778e6ffd8
      be52456c70665f89 0811ef2f3c495d5b be983feedab0c251
      dde596bc7e2b1359 09ec9f9166fb0152 e8c16a84e4b10392
      56467f9538be4463

{client}  send record:

   cleartext (2 octets):  0100
```



```
   ciphertext (24 octets):  17030100136bdf60 847ba6fb650da36e
      872adc684a4af2e8

{server}  send record:
```

cleartext (2 octets): 0100

ciphertext (24 octets): 1703010013621b7c c1962cd8a70109fe
e68a52efedf87d2e

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): 0944d93ff58c924f a9d8915d05ab99cb
48eb9d3c932710a6 e44feb46b1ded481

public key (32 octets): 2c1a71f7cedf5fad 8e8433be7c85533a
615a8d1140c8984d bfdf5391e18b4e74

{client} extract secret "early":

salt (0 octets): (empty)

ikm (32 octets): 05438edfa0f6e663 0d7a9ffe81dc6773
6d753a4ee351a79d 296975918b16039e

secret (32 octets): 99853a47f018f8b2 123e742a14b06549
87fd96262ec8b893 e3dc5c087dc10f4f

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

PRK (32 octets): 99853a47f018f8b2 123e742a14b06549
87fd96262ec8b893 e3dc5c087dc10f4f

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

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

output (32 octets): 1590d475bebda581 fd7d7008a92140d9
baf1b75bfcb7e033 a736591ecba7bb42

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

PRK (32 octets): 99853a47f018f8b2 123e742a14b06549
87fd96262ec8b893 e3dc5c087dc10f4f

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

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

output (32 octets): 399ca522c8bdbd22 9a1db3f4f97632d4
250ed6ecd5568419 6ba9953033956f94

{client} send a ClientHello handshake message

{client} calculate finished:

PRK (32 octets): 1590d475bebda581 fd7d7008a92140d9
baf1b75bfcb7e033 a736591ecba7bb42

handshake hash (0 octets): (empty)

info (21 octets): 002011544c532031 2e332c2066696e69 7368656400

output (32 octets): fe36c444491b0082 e4683625da4dcadf
99aebd2dab5a1621 ae25542ec266d6a7

{client} send record:

cleartext (512 octets): 010001fc030302d2 254d2bde0890e202
8ebb36a14a128bce bc498d9ebcc5eaf0 c1d258cc0a290000
3e130113031302c0 2bc02fcca9cca8c0 0ac009c013c023c0
27c014009eccaa00 3300320067003900 38006b0016001300
9c002f003c003500 3d000a0005000401 0001950015003b00
0000000000000000 0000000000000000 0000000000000000
0000000000000000 0000000000000000 0000000000000000
0000000000000000 00000000000b0009 0000067365727665
72ff01000100000a 00140012001d0017 0018001901000101
010201030104000b 0002010000280026 0024001d00202c1a
71f7cedf5fad8e84 33be7c85533a615a 8d1140c8984dbfdf
5391e18b4e74002a 0000002b0007067f 1203030302000d00
20001e0403050306 0302030804080508 0604010501060102
0104020502060202 02002d0002010100 2900bd009800924e
535321cadc96238d a09caf9b02fecafd d65e3e418f03e437

```
      e1710e2137cd12e6 a85cd3fd7f73706e 7f5dddefb87c1ef8
      3824638464099c9d 1363e3c64ed2075c 16b8ccd8e524a6bb
      d7a6a6e34ea15797 82b15bbe7dfed5c0 c0d980fb330f9d8a
      b252ffe7be1277d4 18b6828ead4dae3b 30d448442417ef76
      af4abe594b002120 56d264e68d59a053 7d872a47a2f0a72d
      5051f1aa5dcbbc5d a1e43ec781580e0a

   ciphertext (517 octets):  1603010200010001 fc030302d2254d2b
      de0890e2028ebb36 a14a128bcebc498d 9ebcc5eaf0c1d258
      cc0a2900003e1301 13031302c02bc02f cca9cca8c00ac009
      c013c023c027c014 009eccaa00330032 006700390038006b
      00160013009c002f 003c0035003d000a 0005000401000195
      0015003b00000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 0000000000000000
      0000000000000000 0000000000000000 00000b0009000006
      736572766572ff01 000100000a001400 12001d0017001800
      1901000101010201 030104000b000201 0000280026002400
      1d00202c1a71f7ce df5fad8e8433be7c 85533a615a8d1140
      c8984dbfdf5391e1 8b4e74002a000000 2b0007067f120303
      0302000d0020001e 0403050306030203 0804080508060401
      0501060102010402 050206020202002d 00020101002900bd
      009800924e535321 cadc96238da09caf 9b02fecafdd65e3e
      418f03e43772cf51 2ed8066100503b1c 08abbbf298a9d138
      ce821dd12fe1710e 2137cd12e6a85cd3 fd7f73706e7f5ddd
      efb87c1ef8382463 8464099c9d1363e3 c64ed2075c16b8cc
      d8e524a6bbd7a6a6 e34ea1579782b15b be7dfed5c0c0d980
      fb330f9d8ab252ff e7be1277d418b682 8ead4dae3b30d448
      442417ef76af4abe 594b00212056d264 e68d59a0537d872a
      47a2f0a72d5051f1 aa5dcbbc5da1e43e c781580e0a

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

   PRK (32 octets):  99853a47f018f8b2 123e742a14b06549
      87fd96262ec8b893 e3dc5c087dc10f4f

   handshake hash (32 octets):  5abe42e4bb8e0bcf f118e9e02e78c793
      c0f8bf0461a62ce4 5a7c541edf06c204

   info (72 octets):  002024544c532031 2e332c20636c6965
      6e74206561726c79 2074726166666963 2073656372657420
```

5abe42e4bb8e0bcf f118e9e02e78c793 c0f8bf0461a62ce4
5a7c541edf06c204

output (32 octets): 560df53cb4604f16 954e5f63869fcf11
d656be054f92c803 f93017a506032016

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

PRK (32 octets): 560df53cb4604f16 954e5f63869fcf11
d656be054f92c803 f93017a506032016

key info (16 octets): 00100c544c532031 2e332c206b657900

key output (16 octets): ee1188babbf83c53 5f8fa55f8f8a20a7

iv info (15 octets): 000c0b544c532031 2e332c20697600

iv output (12 octets): 22a3d48298c8b820 bef80201

{client} send record:

cleartext (6 octets): 414243444546

ciphertext (28 octets): 1703010017c07b71 c7200dab007e9ebc
45c182721f06cd88 6bf785ab

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

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

PRK (32 octets): 99853a47f018f8b2 123e742a14b06549
87fd96262ec8b893 e3dc5c087dc10f4f

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

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

output (32 octets): 1590d475bebda581 fd7d7008a92140d9

baf1b75bfcb7e033 a736591ecba7bb42

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

PRK (32 octets): 99853a47f018f8b2 123e742a14b06549
87fd96262ec8b893 e3dc5c087dc10f4f

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

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

output (32 octets): 399ca522c8bdbd22 9a1db3f4f97632d4
250ed6ecd5568419 6ba9953033956f94

{server} calculate finished:

PRK (32 octets): 1590d475bebda581 fd7d7008a92140d9
baf1b75bfcb7e033 a736591ecba7bb42

handshake hash (0 octets): (empty)

info (21 octets): 002011544c532031 2e332c2066696e69 7368656400

output (32 octets): fe36c444491b0082 e4683625da4dcadf
99aebd2dab5a1621 ae25542ec266d6a7

{server} create an ephemeral x25519 key pair:

private key (32 octets): 084cf2ecb7e94256 f575cd6e3dde2f21
9c4f9029143e4f6a 85e86700b7d5eb77

public key (32 octets): 7897ec11458a449d 3c73f5e3846c5062
8c35faa8876e602e 996c2620deafbe0d

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

```
{server}  send a ServerHello handshake message

{server}  extract secret "handshake":

   salt (32 octets):  99853a47f018f8b2 123e742a14b06549
      87fd96262ec8b893 e3dc5c087dc10f4f

   ikm (32 octets):  7edd226788b92bf9 3b2b33396e06ef84
      059693fa9c199da2 3f41224c2b84e97d

   secret (32 octets):  6423cd6207ff4ea4 7b73af91b6f8db82
      706e5ee4691b27ca 3c743445186ed12c

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

   PRK (32 octets):  6423cd6207ff4ea4 7b73af91b6f8db82
      706e5ee4691b27ca 3c743445186ed12c

   handshake hash (32 octets):  a80310ec3b531838 1c8db6495965f2fa
      cf9ca85a391fcf37 d85cadd1bc7443d4
```



```
   info (76 octets):  002028544c532031 2e332c20636c6965
      6e742068616e6473 68616b6520747261 6666696320736563
      72657420a80310ec 3b5318381c8db649 5965f2facf9ca85a
      391fcf37d85cadd1 bc7443d4

   output (32 octets):  d60ef6f4d7eda53d cc21d02d26ebd575
      f9663f84ef4af32e 5bed4fbb6af833e0

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

   PRK (32 octets):  6423cd6207ff4ea4 7b73af91b6f8db82
      706e5ee4691b27ca 3c743445186ed12c

   handshake hash (32 octets):  a80310ec3b531838 1c8db6495965f2fa
      cf9ca85a391fcf37 d85cadd1bc7443d4

   info (76 octets):  002028544c532031 2e332c2073657276
      65722068616e6473 68616b6520747261 6666696320736563
      72657420a80310ec 3b5318381c8db649 5965f2facf9ca85a
```

```
      391fcf37d85cadd1 bc7443d4

   output (32 octets):  c41576b7adda04fb eb128b8cb48e4b46
      e9954abc6dd2dfc3 0856d028dedcfdd7

{server}  extract secret "master":

   salt (32 octets):  6423cd6207ff4ea4 7b73af91b6f8db82
      706e5ee4691b27ca 3c743445186ed12c

   ikm (32 octets):  0000000000000000 0000000000000000
      0000000000000000 0000000000000000

   secret (32 octets):  838095f760b7ff7a 207ff3c3c818e6f9
      86c87db36fcf063f 09e8451dc55b97e2

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

   PRK (32 octets):  c41576b7adda04fb eb128b8cb48e4b46
      e9954abc6dd2dfc3 0856d028dedcfdd7

   key info (16 octets):  00100c544c532031 2e332c206b657900

   key output (16 octets):  3b6b7a6360a82cf2 5bf22e59e3d170c3

   iv info (15 octets):  000c0b544c532031 2e332c20697600

   iv output (12 octets):  3e94717fb3af82cd e82642b9
```



```
{server}  send record:

   cleartext (88 octets):  020000547f124f9b fff8d7d6e5e445e8
      67330150aa680274 59e8d59262ac183e a8d7e5b9c4981301
      002e002900020000 00280024001d0020 7897ec11458a449d
      3c73f5e3846c5062 8c35faa8876e602e 996c2620deafbe0d

   ciphertext (93 octets):  1603010058020000 547f124f9bfff8d7
      d6e5e445e8673301 50aa68027459e8d5 9262ac183ea8d7e5
      b9c4981301002e00 2900020000002800 24001d00207897ec
      11458a449d3c73f5 e3846c50628c35fa a8876e602e996c26 20deafbe0d
```

```
{server}  send a EncryptedExtensions handshake message

{server}  calculate finished:

   PRK (32 octets):  c41576b7adda04fb eb128b8cb48e4b46
      e9954abc6dd2dfc3 0856d028dedcfdd7

   handshake hash (0 octets):  (empty)

   info (21 octets):  002011544c532031 2e332c2066696e69 7368656400

   output (32 octets):  675bd9b07376e6a6 56ef9fbe9297ce8a
      cabbc804e1001d0d c4a810b918aad2d3

{server}  send a Finished handshake message

{server}  send record:

   cleartext (74 octets):  080000220020000a 00140012001d0017
      0018001901000101 0102010301040000 0000002a00001400
      00206b2d3c33b880 827d22789897cf52 ced3a06fd4a1b927
      106cad93e8145ecf e9ee

   ciphertext (96 octets):  170301005b29076d 479ff50c63291217
      5bc8d31b77425359 8be825a729656425 3acf12baa202f07a
      29c686489aa76bb5 d8b1bb64d6502ee9 7954302c4a8a528f
      f27506e35fabb67b 7bf7623cfb23ac56 24942c10ffbae8a7
      79ffcec31860a481

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

   PRK (32 octets):  838095f760b7ff7a 207ff3c3c818e6f9
      86c87db36fcf063f 09e8451dc55b97e2

   handshake hash (32 octets):  25678f29cd74c323 e2c410f6163f1560
      8bbe70f367f330f9 f316a3b91a98a5cb
```



```
   info (78 octets):  00202a544c532031 2e332c20636c6965
      6e74206170706c69 636174696f6e2074 7261666669632073
      6563726574202567 8f29cd74c323e2c4 10f6163f15608bbe
      70f367f330f9f316 a3b91a98a5cb
```

```
   output (32 octets):  642d05445f11316d d9f94a0b64af1f07
      37ca6429219cd7fb 1f33c4b2fe3ab632

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

   PRK (32 octets):  838095f760b7ff7a 207ff3c3c818e6f9
      86c87db36fcf063f 09e8451dc55b97e2

   handshake hash (32 octets):  25678f29cd74c323 e2c410f6163f1560
      8bbe70f367f330f9 f316a3b91a98a5cb

   info (78 octets):  00202a544c532031 2e332c2073657276
      6572206170706c69 636174696f6e2074 7261666669632073
      6563726574202567 8f29cd74c323e2c4 10f6163f15608bbe
      70f367f330f9f316 a3b91a98a5cb

   output (32 octets):  125f0e573a686d07 92ed788646fedd3e
      4407728929607077 745cd1a98f240daa

{server}  derive secret "exporter master secret":

   PRK (32 octets):  838095f760b7ff7a 207ff3c3c818e6f9
      86c87db36fcf063f 09e8451dc55b97e2

   handshake hash (32 octets):  25678f29cd74c323 e2c410f6163f1560
      8bbe70f367f330f9 f316a3b91a98a5cb

   info (67 octets):  00201f544c532031 2e332c206578706f
      72746572206d6173 7465722073656372 65742025678f29cd
      74c323e2c410f616 3f15608bbe70f367 f330f9f316a3b91a 98a5cb

   output (32 octets):  94afc03877de24ce 1a14ecd098ad891c
      5d54b37369bc98f8 3c136fb7f56e1490

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

   PRK (32 octets):  125f0e573a686d07 92ed788646fedd3e
      4407728929607077 745cd1a98f240daa

   key info (16 octets):  00100c544c532031 2e332c206b657900

   key output (16 octets):  dab117e37b791fec 925a71f88c376fa6
```

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

   iv output (12 octets):  bbe980ebee1ba6c0 38a2e244

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

{client}  extract secret "handshake":

   salt (32 octets):  99853a47f018f8b2 123e742a14b06549
      87fd96262ec8b893 e3dc5c087dc10f4f

   ikm (32 octets):  7edd226788b92bf9 3b2b33396e06ef84
      059693fa9c199da2 3f41224c2b84e97d

   secret (32 octets):  6423cd6207ff4ea4 7b73af91b6f8db82
      706e5ee4691b27ca 3c743445186ed12c

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

   PRK (32 octets):  6423cd6207ff4ea4 7b73af91b6f8db82
      706e5ee4691b27ca 3c743445186ed12c

   handshake hash (32 octets):  a80310ec3b531838 1c8db6495965f2fa
      cf9ca85a391fcf37 d85cadd1bc7443d4

   info (76 octets):  002028544c532031 2e332c20636c6965
      6e742068616e6473 68616b6520747261 6666696320736563
      72657420a80310ec 3b5318381c8db649 5965f2facf9ca85a
      391fcf37d85cadd1 bc7443d4

   output (32 octets):  d60ef6f4d7eda53d cc21d02d26ebd575
      f9663f84ef4af32e 5bed4fbb6af833e0

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

   PRK (32 octets):  6423cd6207ff4ea4 7b73af91b6f8db82
      706e5ee4691b27ca 3c743445186ed12c

   handshake hash (32 octets):  a80310ec3b531838 1c8db6495965f2fa
      cf9ca85a391fcf37 d85cadd1bc7443d4

   info (76 octets):  002028544c532031 2e332c2073657276
      65722068616e6473 68616b6520747261 6666696320736563
      72657420a80310ec 3b5318381c8db649 5965f2facf9ca85a
      391fcf37d85cadd1 bc7443d4
```

```
      output (32 octets):  c41576b7adda04fb eb128b8cb48e4b46
         e9954abc6dd2dfc3 0856d028dedcfdd7

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

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

      PRK (32 octets):  c41576b7adda04fb eb128b8cb48e4b46
         e9954abc6dd2dfc3 0856d028dedcfdd7

      key info (16 octets):  00100c544c532031 2e332c206b657900

      key output (16 octets):  3b6b7a6360a82cf2 5bf22e59e3d170c3

      iv info (15 octets):  000c0b544c532031 2e332c20697600

      iv output (12 octets):  3e94717fb3af82cd e82642b9

   {client}  calculate finished:

      PRK (32 octets):  c41576b7adda04fb eb128b8cb48e4b46
         e9954abc6dd2dfc3 0856d028dedcfdd7

      handshake hash (0 octets):  (empty)

      info (21 octets):  002011544c532031 2e332c2066696e69 7368656400

      output (32 octets):  675bd9b07376e6a6 56ef9fbe9297ce8a
         cabbc804e1001d0d c4a810b918aad2d3

   {client}  send record:

      cleartext (2 octets):  0101

      ciphertext (24 octets):  17030100130aba56 52f18ac0971329d7
         5fa54b8d4477f693

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

      PRK (32 octets):  d60ef6f4d7eda53d cc21d02d26ebd575
         f9663f84ef4af32e 5bed4fbb6af833e0
```

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

      key output (16 octets):  bd8d8cc78152c42f 15b5d2ae85d85391

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



```
      iv output (12 octets):  9e379b5677dda474 9dd45fd5

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

      PRK (32 octets):  838095f760b7ff7a 207ff3c3c818e6f9
         86c87db36fcf063f 09e8451dc55b97e2

      handshake hash (32 octets):  25678f29cd74c323 e2c410f6163f1560
         8bbe70f367f330f9 f316a3b91a98a5cb

      info (78 octets):  00202a544c532031 2e332c20636c6965
         6e74206170706c69 636174696f6e2074 7261666669632073
         6563726574202567 8f29cd74c323e2c4 10f6163f15608bbe
         70f367f330f9f316 a3b91a98a5cb

      output (32 octets):  642d05445f11316d d9f94a0b64af1f07
         37ca6429219cd7fb 1f33c4b2fe3ab632

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

      PRK (32 octets):  838095f760b7ff7a 207ff3c3c818e6f9
         86c87db36fcf063f 09e8451dc55b97e2

      handshake hash (32 octets):  25678f29cd74c323 e2c410f6163f1560
         8bbe70f367f330f9 f316a3b91a98a5cb

      info (78 octets):  00202a544c532031 2e332c2073657276
         6572206170706c69 636174696f6e2074 7261666669632073
         6563726574202567 8f29cd74c323e2c4 10f6163f15608bbe
         70f367f330f9f316 a3b91a98a5cb

      output (32 octets):  125f0e573a686d07 92ed788646fedd3e
         4407728929607077 745cd1a98f240daa

   {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): d60ef6f4d7eda53d cc21d02d26ebd575
      f9663f84ef4af32e 5bed4fbb6af833e0

   handshake hash (0 octets): (empty)

   info (21 octets): 002011544c532031 2e332c2066696e69 7368656400

   output (32 octets): 9d18ee7c846ea450 0c9884d3b3741107
      1cb93b42db69a46c 101e65e976a20417

{client} send a Finished handshake message

{client} send record:

   cleartext (36 octets): 1400002055f849f1 a03006f7ec3d5384
      aba84782b4c37df3 d3c7b92543d5e8b0 24b38aea

   ciphertext (58 octets): 170301003561ad40 384d8ffd77d6ea42
      28ca06247041fccf edc89e8f4f575a3b 79a01e61f6d3961a
      5a6251e79594620a 62067c3a245dff64 b2fe

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

   PRK (32 octets): 642d05445f11316d d9f94a0b64af1f07
      37ca6429219cd7fb 1f33c4b2fe3ab632

   key info (16 octets): 00100c544c532031 2e332c206b657900

   key output (16 octets): ed504bf560f8c1e6 867659dd6527cdfa

   iv info (15 octets): 000c0b544c532031 2e332c20697600

   iv output (12 octets): 005434eeaac2d2b6 b3dc186d

{client} derive secret "resumption master secret":

PRK (32 octets): 838095f760b7ff7a 207ff3c3c818e6f9
86c87db36fcf063f 09e8451dc55b97e2

handshake hash (32 octets): 10e631557cc36de9 c9e1698cd932420d
8388263513d401f0 a8a2d5bbf8ab8500

info (69 octets): 002021544c532031 2e332c2072657375
6d7074696f6e206d 6173746572207365 637265742010e631
557cc36de9c9e169 8cd932420d838826 3513d401f0a8a2d5 bbf8ab8500

output (32 octets): ddb7ba1feb09673a ebc36db7e08c410b
de864b2eb7be9bda ded9be89bac6649c

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

PRK (32 octets): d60ef6f4d7eda53d cc21d02d26ebd575
f9663f84ef4af32e 5bed4fbb6af833e0

key info (16 octets): 00100c544c532031 2e332c206b657900

key output (16 octets): bd8d8cc78152c42f 15b5d2ae85d85391

iv info (15 octets): 000c0b544c532031 2e332c20697600

iv output (12 octets): 9e379b5677dda474 9dd45fd5

{server} calculate finished:

PRK (32 octets): d60ef6f4d7eda53d cc21d02d26ebd575
f9663f84ef4af32e 5bed4fbb6af833e0

handshake hash (0 octets): (empty)

info (21 octets): 002011544c532031 2e332c2066696e69 7368656400

output (32 octets): 9d18ee7c846ea450 0c9884d3b3741107
1cb93b42db69a46c 101e65e976a20417

{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): 1703010043215c81 57730ca2101ad6ee
      50335a7216d5565e 3391c1d920b4c126 4285994032dbe9bc
      f077bfdd6f0fa1c9 e0c610c0b74605b2 a24448e4a7cb45ef
      8b0193ea95b4d860

{server} send record:

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

   ciphertext (72 octets): 17030100434255b4 8f15b947f760ed76
      29e130e5d4aaabea 7d06fa74fd3c9901 0997853776caf2c6
      5c8ccc6e33567dc7 f4ac50467eddf42c c76241aeda237a07
      422ac51a643773e9

{client} send record:

   cleartext (2 octets): 0100

   ciphertext (24 octets): 1703010013422dd5 2ef4a92aaac69e06
      6846b7e507d4a2ca

{server} send record:

   cleartext (2 octets): 0100

   ciphertext (24 octets): 1703010013c6f797 8bf3ce7e86f54ffe
      a9edc9e61dfdd967

5. 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.

6. 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.

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