HTTP
Internet-Draft
Intended status: Standards Track
Expires: May 1, 2017

M. Thomson
Mozilla

October 28, 2016

Example Handshake Traces for TLS 1.3
draft-thomson-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.

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 1, 2017.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 2
2. Private Keys 2
3. Simple 1-RTT Handshake 3
4. Resumed 0-RTT Handshake 14
5. Security Considerations 25
6. Normative References 25
Appendix A. Acknowledgements 25
Author's Address 26

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.

Note: This version of the document shows vectors from version -16 of the draft. It will be updated when NSS is updated to -18 (real soon now).

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):  075e1d4503195c00 61e75a39738e7f88
         08cdcceb84fc36ec aae01a327d05010b

      public key (32 octets):  e122b20099cbe505 9a9bbe5880e02ed6
         525d6f72f8f7afab b87a32dbe9e23022

   {client}  send a ClientHello handshake message

   {client}  send record:

      cleartext (250 octets):  010000f603034a77 2c764c3313f344b2
         f4fae943e816fe5a f3eac74809c21e2c 24989f3e8c520000
```

```
         3e130113031302c0 2bc02fcca9cca8c0 0ac009c013c023c0
         27c014009eccaa00 3300320067003900 38006b0016001300
         9c002f003c003500 3d000a0005000401 00008f0000000b00
         0900000673657276 6572ff0100010000 0a00140012001d00
         1700180019010001 0101020103010400 0b00020100002300
         0000280026002400 1d0020e122b20099 cbe5059a9bbe5880
         e02ed6525d6f72f8 f7afabb87a32dbe9 e23022002b000706
         7f1003030302000d 0020001e04030503 0603020308040805
         0806040105010601 0201040205020602 0202

      ciphertext (255 octets):  16030100fa010000 f603034a772c764c
         3313f344b2f4fae9 43e816fe5af3eac7 4809c21e2c24989f
         3e8c5200003e1301 13031302c02bc02f cca9cca8c00ac009
         c013c023c027c014 009eccaa00330032 006700390038006b
         00160013009c002f 003c0035003d000a 000500040100008f
         0000000b00090000 06736572766572ff 01000100000a0014
         0012001d00170018 0019010001010102 01030104000b0002
         0100002300000028 00260024001d0020 e122b20099cbe505
         9a9bbe5880e02ed6 525d6f72f8f7afab b87a32dbe9e23022
         002b0007067f1003 030302000d002000 1e04030503060302
         0308040805080604 0105010601020104 02050206020202

   {server}  create an ephemeral x25519 key pair:

      private key (32 octets):  06730e3ab71702bc 322472986e421ba2
         320db29fb0c67d7a 1bf21a4f06c9f115

      public key (32 octets):  e2816da24ed31838 bd876b0a344b2793
         dead2350adda23fb 5193787ae608f647

   {server}  extract secret "early":

      salt (0 octets):  (empty)

      ikm (32 octets):  0000000000000000 0000000000000000
         0000000000000000 0000000000000000

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

   {server}  send a ServerHello handshake message

   {server}  extract secret "handshake":

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

```
      ikm (32 octets):  ad602096bc9ed914 61b83c950382a9d4
         1829059264f563a1 59c87cec790b0333

      secret (32 octets):  b75d555586220fea 3e6eb1e1243c8f7e
         20e5af8cee1799e0 31b7efefff43c8b1

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

      handshake hash (64 octets):  48d89c6276fa205b 0eb068ac122fb05b
         1e010350db32eae9 59cbe6addf25a67e 66687aadf862bd77
         6c8fc18b8e9f8e20 089714856ee233b3 902a591d0d5f2925

      PRK (32 octets):  b75d555586220fea 3e6eb1e1243c8f7e
         20e5af8cee1799e0 31b7efefff43c8b1

      info (108 octets):  002028544c532031 2e332c20636c6965
         6e742068616e6473 68616b6520747261 6666696320736563
         7265744048d89c62 76fa205b0eb068ac 122fb05b1e010350
         db32eae959cbe6ad df25a67e66687aad f862bd776c8fc18b
         8e9f8e2008971485 6ee233b3902a591d 0d5f2925

      output (32 octets):  7f9ee8ff500bdb58 6780934edddd288e
         1600a2083ab2ece6 0dc339845e158678

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

      handshake hash (64 octets):  48d89c6276fa205b 0eb068ac122fb05b
         1e010350db32eae9 59cbe6addf25a67e 66687aadf862bd77
         6c8fc18b8e9f8e20 089714856ee233b3 902a591d0d5f2925

      PRK (32 octets):  b75d555586220fea 3e6eb1e1243c8f7e
         20e5af8cee1799e0 31b7efefff43c8b1

      info (108 octets):  002028544c532031 2e332c2073657276
         65722068616e6473 68616b6520747261 6666696320736563
         7265744048d89c62 76fa205b0eb068ac 122fb05b1e010350
         db32eae959cbe6ad df25a67e66687aad f862bd776c8fc18b
         8e9f8e2008971485 6ee233b3902a591d 0d5f2925

      output (32 octets):  d7fa33c70916f980 d2097d211158c6dc
         b3aaa9899cfe0acf 10bc5334d9083866

   {server}  extract secret "master":

      salt (32 octets):  b75d555586220fea 3e6eb1e1243c8f7e
         20e5af8cee1799e0 31b7efefff43c8b1
```

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

      secret (32 octets):  6304ef9c9685cfd5 940af49d657cc6b8
         942889b94a4fafef b0d3f181c440028c

   {server}  send record:

      cleartext (86 octets):  020000527f102ac7 df3c5e246509294f
         5cd617339959743c 8d34c0f28b6f3c57 c02e77014b901301
         002c000d00000028 0024001d0020e281 6da24ed31838bd87
         6b0a344b2793dead 2350adda23fb5193 787ae608f647

      ciphertext (91 octets):  1603010056020000 527f102ac7df3c5e
         246509294f5cd617 339959743c8d34c0 f28b6f3c57c02e77
         014b901301002c00 0d00000028002400 1d0020e2816da24e
         d31838bd876b0a34 4b2793dead2350ad da23fb5193787ae6 08f647

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

      PRK (32 octets):  d7fa33c70916f980 d2097d211158c6dc
         b3aaa9899cfe0acf 10bc5334d9083866

      key info (41 octets):  001025544c532031 2e332c2068616e64
         7368616b65206b65 7920657870616e73 696f6e2c206b6579 00

      key output (16 octets):  d9e91353d9fc4516 3218909ab937fddb

      iv info (40 octets):  000c24544c532031 2e332c2068616e64
         7368616b65206b65 7920657870616e73 696f6e2c20697600

      iv output (12 octets):  7c880c98fe14487b aec110ee

   {server}  send a EncryptedExtensions handshake message

   {server}  send a Certificate handshake message

   {server}  send a CertificateVerify handshake message

   {server}  send a Finished handshake message

   {server}  send record:

      cleartext (649 octets):  0800001e001c000a 00140012001d0017
         0018001901000101 0102010301040000 00000b0001b70000
         01b30001b0308201 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
      87b42b4de10f0000 840804008050421a 381f73d2f29ad569
      3f93bc456fd7024f 189b98ddb73be484 0509b16ba4e91973
      156e97328919568f 6458edae49c0620a 636fb689f53d3eea
      3b6474ba54b2f851 b0ca038bbd1b603e c0a337526fb47ff6
      fd2fdebbfd81a8a4 5da64b115175c243 76c48fbb9fe5e30f
      be81dce81afc8d33 1b4ec72487f58701 ce979ece6e140000
      2005729a74d99f80 61a1e0d75f6d5cef 88d26fa95661aa81
      db6cc2bf99a25b75 07

   ciphertext (671 octets):  170301029aca54b6 a40203d951b0d14f
      9573fc3b918db939 fe3b7d8d1ca90163 870a9fa0687b7451
      96893091919525a3 586bebddc81d0c64 14ad78a337af2dde
      585361126008e5a3 1c377c05056cd994 7fc8682a0d4e12cf
      eee9b2ba99b7fc6b d7ec8a167be1c675 26395c8486d00ea9
      b704c6776847d3e2 f5e80a014593116a 8e317aab896a9c24
      757069f0a627882f 291dc6c5ad46520c 1c9ddc40ca6c1632
      c38f7d0b6e0e6b56 3094a14ee9da6862 a470d2335e3afcd8
      146be77ef8477c78 b54bdfeb847dffae ac6a41ce697674a9
      24f24006aae67391 bcdc6298a4c267c5 71ba244f92c039fe
      9bbc2ca94d199e20 3b45f6a3f90acbe9 0f48a18c28a2cdfb
      3aa376a2d4e8d131 6fae0dee5b0c6317 3726c02c63ad7513
      2af36f10c49c33f9 228b8d17abdfd7c2 db649bbb05309095
      5b71294b9405bec9 f02121a2826de9e3 ed606f92c6a98290
      7aae17417e75af9f 8f8d20b15623647d 951e4c7e9a0f9423
      7a7080b1c50a7d1f ff5a9e827674e02e ca0732f6cbad41d5
      021fdf33ca1140fc 37b2f9f92b93c12e f32f1199864c9acc
      c1db416403a51f71 a8a12174cf0fcb96 d7c8301f405bd35f
      a454167f27191885 b62a38e9a8610dba 8a12a63ff6ab3ff8
      6475fced4bf26460 bd47d5e3a9fc96c8 1a5b95b9710cd699
      eb34255fa528d061 4cbd9acac2966635 dea58e1c3174de8b
      46e66cb09a9f0f56 d7fb01e7cbaf3e91 d565482bf1caf6c2
      b6ad6f405c444f6a 9f12b7a26ce59aa9 594fa88319133bcb
```

```
         45fb6808116bb185 f284663cb7a93cf3 7abf77869c29bed6
         531355b921def46c 10a307248deaa5c3 7698d9fa582e9d8a
         dd76bb66a12464a2 593a2f36097bd279 a9d2a33611c835fc
         b66c47a2d6274f02 9f1dae41075ff72d c490b460e16ce7c0
         0372cb171c318825 15be0cf49954228b 07ca8df5f1afaeac
         824a3901f46ba0

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

      handshake hash (64 octets):  ff0df9baa81cb6f3 63c49c82a47d1760
         a4f8f3a3ff5e5bc0 908ed79828a2307b 66687aadf862bd77
         6c8fc18b8e9f8e20 089714856ee233b3 902a591d0d5f2925

      PRK (32 octets):  6304ef9c9685cfd5 940af49d657cc6b8
         942889b94a4fafef b0d3f181c440028c

      info (110 octets):  00202a544c532031 2e332c20636c6965
         6e74206170706c69 636174696f6e2074 7261666669632073
         656372657440ff0d f9baa81cb6f363c4 9c82a47d1760a4f8
         f3a3ff5e5bc0908e d79828a2307b6668 7aadf862bd776c8f
         c18b8e9f8e200897 14856ee233b3902a 591d0d5f2925

      output (32 octets):  97e11121ec208603 baf556083a0846a7
         d3865e129dfd431e f58ed67ef3294ea0

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

      handshake hash (64 octets):  ff0df9baa81cb6f3 63c49c82a47d1760
         a4f8f3a3ff5e5bc0 908ed79828a2307b 66687aadf862bd77
         6c8fc18b8e9f8e20 089714856ee233b3 902a591d0d5f2925

      PRK (32 octets):  6304ef9c9685cfd5 940af49d657cc6b8
         942889b94a4fafef b0d3f181c440028c

      info (110 octets):  00202a544c532031 2e332c2073657276
         6572206170706c69 636174696f6e2074 7261666669632073
         656372657440ff0d f9baa81cb6f363c4 9c82a47d1760a4f8
         f3a3ff5e5bc0908e d79828a2307b6668 7aadf862bd776c8f
         c18b8e9f8e200897 14856ee233b3902a 591d0d5f2925

      output (32 octets):  99ad63e5f7e3fd34 ac5e25c72d40ccb2
         0d00b15ac72af67d 45f51b58af21bb6b

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

      PRK (32 octets):  99ad63e5f7e3fd34 ac5e25c72d40ccb2
         0d00b15ac72af67d 45f51b58af21bb6b
```

```
      key info (48 octets):  00102c544c532031 2e332c206170706c
         69636174696f6e20 64617461206b6579 20657870616e7369
         6f6e2c206b657900

      key output (16 octets):  6169499247a881de 7229cd410dc39148

      iv info (47 octets):  000c2b544c532031 2e332c206170706c
         69636174696f6e20 64617461206b6579 20657870616e7369
         6f6e2c20697600

      iv output (12 octets):  e9a71b94ce8a906f 80318b27

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

      PRK (32 octets):  7f9ee8ff500bdb58 6780934edddd288e
         1600a2083ab2ece6 0dc339845e158678

      key info (41 octets):  001025544c532031 2e332c2068616e64
         7368616b65206b65 7920657870616e73 696f6e2c206b6579 00

      key output (16 octets):  3d44490aa0bf7393 15c50de02eb3675b

      iv info (40 octets):  000c24544c532031 2e332c2068616e64
         7368616b65206b65 7920657870616e73 696f6e2c20697600

      iv output (12 octets):  82decae60afb84cb 6692e045

   {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):  ad602096bc9ed914 61b83c950382a9d4
         1829059264f563a1 59c87cec790b0333

      secret (32 octets):  b75d555586220fea 3e6eb1e1243c8f7e
         20e5af8cee1799e0 31b7efefff43c8b1
```

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

   handshake hash (64 octets):  48d89c6276fa205b 0eb068ac122fb05b
      1e010350db32eae9 59cbe6addf25a67e 66687aadf862bd77
      6c8fc18b8e9f8e20 089714856ee233b3 902a591d0d5f2925

   PRK (32 octets):  b75d555586220fea 3e6eb1e1243c8f7e
      20e5af8cee1799e0 31b7efefff43c8b1

   info (108 octets):  002028544c532031 2e332c20636c6965
      6e742068616e6473 68616b6520747261 6666696320736563
      7265744048d89c62 76fa205b0eb068ac 122fb05b1e010350
      db32eae959cbe6ad df25a67e66687aad f862bd776c8fc18b
      8e9f8e2008971485 6ee233b3902a591d 0d5f2925

   output (32 octets):  7f9ee8ff500bdb58 6780934edddd288e
      1600a2083ab2ece6 0dc339845e158678

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

   handshake hash (64 octets):  48d89c6276fa205b 0eb068ac122fb05b
      1e010350db32eae9 59cbe6addf25a67e 66687aadf862bd77
      6c8fc18b8e9f8e20 089714856ee233b3 902a591d0d5f2925

   PRK (32 octets):  b75d555586220fea 3e6eb1e1243c8f7e
      20e5af8cee1799e0 31b7efefff43c8b1

   info (108 octets):  002028544c532031 2e332c2073657276
      65722068616e6473 68616b6520747261 6666696320736563
      7265744048d89c62 76fa205b0eb068ac 122fb05b1e010350
      db32eae959cbe6ad df25a67e66687aad f862bd776c8fc18b
      8e9f8e2008971485 6ee233b3902a591d 0d5f2925

   output (32 octets):  d7fa33c70916f980 d2097d211158c6dc
      b3aaa9899cfe0acf 10bc5334d9083866

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

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

   PRK (32 octets):  d7fa33c70916f980 d2097d211158c6dc
      b3aaa9899cfe0acf 10bc5334d9083866

   key info (41 octets):  001025544c532031 2e332c2068616e64
      7368616b65206b65 7920657870616e73 696f6e2c206b6579 00

   key output (16 octets):  d9e91353d9fc4516 3218909ab937fddb
```

```
      iv info (40 octets):  000c24544c532031 2e332c2068616e64
         7368616b65206b65 7920657870616e73 696f6e2c20697600

      iv output (12 octets):  7c880c98fe14487b aec110ee

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

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

      handshake hash (64 octets):  ff0df9baa81cb6f3 63c49c82a47d1760
         a4f8f3a3ff5e5bc0 908ed79828a2307b 66687aadf862bd77
         6c8fc18b8e9f8e20 089714856ee233b3 902a591d0d5f2925

      PRK (32 octets):  6304ef9c9685cfd5 940af49d657cc6b8
         942889b94a4fafef b0d3f181c440028c

      info (110 octets):  00202a544c532031 2e332c20636c6965
         6e74206170706c69 636174696f6e2074 7261666669632073
         656372657440ff0d f9baa81cb6f363c4 9c82a47d1760a4f8
         f3a3ff5e5bc0908e d79828a2307b6668 7aadf862bd776c8f
         c18b8e9f8e200897 14856ee233b3902a 591d0d5f2925

      output (32 octets):  97e11121ec208603 baf556083a0846a7
         d3865e129dfd431e f58ed67ef3294ea0

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

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

   {client}  send a Finished handshake message

   {client}  send record:

      cleartext (36 octets):  1400002066eb0ee7 18d53e225f390198
         cb11e509fa9b7a47 5631cc4bda677d8d 2cf83bcd

      ciphertext (58 octets):  1703010035f3a571 37af8ee7be72190f
         b3e3597bd91f5d47 eae71f3f0ac738bf 27c3352d1994095a
         bb3b0237762044b9 c792c6ba692dfe59 4354

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

      PRK (32 octets):  97e11121ec208603 baf556083a0846a7
         d3865e129dfd431e f58ed67ef3294ea0
```

```
      key info (48 octets):  00102c544c532031 2e332c206170706c
         69636174696f6e20 64617461206b6579 20657870616e7369
         6f6e2c206b657900

      key output (16 octets):  e49f80706175ac01 dbbf084bfb4c1e52

      iv info (47 octets):  000c2b544c532031 2e332c206170706c
         69636174696f6e20 64617461206b6579 20657870616e7369
         6f6e2c20697600

      iv output (12 octets):  371f77d48eafc897 7f2bc95a

   {client}  derive secret "resumption master secret":

      handshake hash (64 octets):  6565a715d091d3e9 b9459f063075589a
         2bc00ba70008cc8f 98aabc8e6820aca1 66687aadf862bd77
         6c8fc18b8e9f8e20 089714856ee233b3 902a591d0d5f2925

      PRK (32 octets):  6304ef9c9685cfd5 940af49d657cc6b8
         942889b94a4fafef b0d3f181c440028c

      info (101 octets):  002021544c532031 2e332c2072657375
         6d7074696f6e206d 6173746572207365 63726574406565a7
         15d091d3e9b9459f 063075589a2bc00b a70008cc8f98aabc
         8e6820aca166687a adf862bd776c8fc1 8b8e9f8e20089714
         856ee233b3902a59 1d0d5f2925

      output (32 octets):  39ba24cd46a6a039 92281635246613af
         bf91ca4a3f0ec2c9 0aafd99c441f7b5e

   {server}  derive read traffic keys using label "application data key
      expansion" (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 0101010000924e53
         53216ffddf432e46 e04edd3964cda3f3 50651903277c3a25
         9ec4661515360050 cf3e329e2bd535a9 62d66cdcaa31777a
         35f8cf6579f194fa d530346815c95bae a68f17c1573aa34c
         0b279ce1bfc02c4f f5fef1b022033911 78fadda4b941b657
         72a1cf139ed70ae2 c178cbd80d5408bb 4e635422667e5d15
         a4065d15687f3b80 9fc5a2682df6f538 57ba2c70cdfbe30a
         00080001000492f5 741d
```

```
      ciphertext (192 octets):  17030100bb6e9e08 968779b20df43113
         ae8de08b64ce7399 8c5d172d7c35ead5 05828f494e9f9380
         3d963a50899cd3a9 bf7c8d05c5b6ff31 6d7bd5276f34695c
         62bd2ae07649b44e 561c892dbcec0e12 589fd86cd100e54a
         a454edf944bbb37f 471372176e3f42f0 d0743e718bd508a0
         1ff4419853d85639 91deaadf7e8f6e87 dea06197a0bd5ee2
         960a7c7d97354c46 039bb1053cc3bd64 6a4a631fa5dec790
         f54315dc613d24f8 49cb8173624056ce 837d602babdb6f03
         7c10d4ff8c0d687c

   {client}  send record:

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

      ciphertext (72 octets):  1703010043b20a2d ed0ab1f75406210a
         47c90bdc2005accd a938dea9d89ae18f e0d4ee831f31d30c
         22dfdf4cd54ef9b5 8d41175801c59f11 2174c4741262d95e
         ebce282c57885a6d

   {server}  send record:

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

      ciphertext (72 octets):  1703010043f3ce38 bdf2d147bc67a732
         86fd7aa19ab042fe 50a6de46fb66f9cd 205ccde487149928
         f72e56ab2b345770 6a574fe3964ea45b 5f20ae76e33819f7
         c54d7fdbb50bf7aa

   {client}  send record:

      cleartext (2 octets):  0100

      ciphertext (24 octets):  1703010013d60d81 f25a39b000df86f5
         0a29f040ef22f42a

   {server}  send record:

      cleartext (2 octets):  0100

      ciphertext (24 octets):  1703010013b8ba60 16a056a597287382
         226c61b64b545c87
```

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):  01c5c60e33afeed5 a0f82c5e4ca515fa
      6ebcda9c7f50ee64 7414fa1c22728b03

   public key (32 octets):  1206a37e316cf704 99d848efd024caaf
      c4b5050647f8aef2 27d81cf446082515

{client}  send a ClientHello handshake message

{client}  extract secret "early":

   salt (0 octets):  (empty)

   ikm (32 octets):  afdb6b1d2cc77780 d80026ca6d61b50e
      d7facf76ffd647ae f5565bf072da5420

   secret (32 octets):  50b55777d9078122 7376f3701a850c21
      040983207b0c2469 9580e18ba29bd5f6

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

   handshake hash (64 octets):  44dd22c46277ede3 eac3a2dc694d8cb4
      20504c75e9aa00ec 418b6ca7d5555b71 ffc65d93ccb7b739
      b3f1ba164a8c1893 4e069aa123889906 2188e39045f3d821

   PRK (32 octets):  50b55777d9078122 7376f3701a850c21
      040983207b0c2469 9580e18ba29bd5f6

   info (104 octets):  002024544c532031 2e332c20636c6965
      6e74206561726c79 2074726166666963 2073656372657440
      44dd22c46277ede3 eac3a2dc694d8cb4 20504c75e9aa00ec
      418b6ca7d5555b71 ffc65d93ccb7b739 b3f1ba164a8c1893
      4e069aa123889906 2188e39045f3d821

   output (32 octets):  af68f3b851db647a 50ccd03afb94d52e
      8f1349a66f56f54d 683ca3a9900ed295

{client}  send record:

   cleartext (512 octets):  010001fc030346bd 529e51ffb4df6f6b
      99049413c1b719d7 be796c195f3ce005 4d2866c5dd370000
```

```
         3e130113031302c0 2bc02fcca9cca8c0 0ac009c013c023c0
         27c014009eccaa00 3300320067003900 38006b0016001300
         9c002f003c003500 3d000a0005000401 0001950000000b00
         0900000673657276 6572ff0100010000 0a00140012001d00
         1700180019010001 0101020103010400 0b00020100002800
         260024001d002012 06a37e316cf70499 d848efd024caafc4
         b5050647f8aef227 d81cf44608251500 29009a0098010101
         0000924e5353216f fddf432e46e04edd 3964cda3f3506519
         03277c3a259ec466 1515360050cf3e32 9e2bd535a962d66c
         dcaa31777a35f8cf 6579f194fad53034 6815c95baea68f17
         c1573aa34c0b279c e1bfc02c4ff5fef1 b02203391178fadd
         a4b941b65772a1cf 139ed70ae2c178cb d80d5408bb4e6354
         22667e5d15a4065d 15687f3b809fc5a2 682df6f53857ba2c
         70cdfbe30a002a00 0492f5741d002b00 07067f1003030302
         000d0020001e0403 0503060302030804 0805080604010501
         0601020104020502 0602020200150060 0000000000000000
         0000000000000000 0000000000000000 0000000000000000
         0000000000000000 0000000000000000 0000000000000000
         0000000000000000 0000000000000000 0000000000000000
         0000000000000000 0000000000000000

      ciphertext (517 octets):  1603010200010001 fc030346bd529e51
         ffb4df6f6b990494 13c1b719d7be796c 195f3ce0054d2866
         c5dd3700003e1301 13031302c02bc02f cca9cca8c00ac009
         c013c023c027c014 009eccaa00330032 006700390038006b
         00160013009c002f 003c0035003d000a 0005000401000195
         0000000b00090000 06736572766572ff 01000100000a0014
         0012001d00170018 0019010001010102 01030104000b0002
         0100002800260024 001d00201206a37e 316cf70499d848ef
         d024caafc4b50506 47f8aef227d81cf4 460825150029009a
         0098010101000092 4e5353216ffddf43 2e46e04edd3964cd
         a3f350651903277c 3a259ec466151536 0050cf3e329e2bd5
         35a962d66cdcaa31 777a35f8cf6579f1 94fad530346815c9
         5baea68f17c1573a a34c0b279ce1bfc0 2c4ff5fef1b02203
         391178fadda4b941 b65772a1cf139ed7 0ae2c178cbd80d54
         08bb4e635422667e 5d15a4065d15687f 3b809fc5a2682df6
         f53857ba2c70cdfb e30a002a000492f5 741d002b0007067f
         1003030302000d00 20001e0403050306 0302030804080508
         0604010501060102 0104020502060202 0200150060000000
         0000000000000000 0000000000000000 0000000000000000
         0000000000000000 0000000000000000 0000000000000000
         0000000000000000 0000000000000000 0000000000000000
         0000000000000000 0000000000000000 0000000000

   {client}  derive write traffic keys using label "early handshake key
      expansion":
```

```
      PRK (32 octets):  af68f3b851db647a 50ccd03afb94d52e
         8f1349a66f56f54d 683ca3a9900ed295

      key info (47 octets):  00102b544c532031 2e332c206561726c
         792068616e647368 616b65206b657920 657870616e73696f
         6e2c206b657900

      key output (16 octets):  eee93d2d1de2b7aa 0939dd335a5389ed

      iv info (46 octets):  000c2a544c532031 2e332c206561726c
         792068616e647368 616b65206b657920 657870616e73696f 6e2c20697600

      iv output (12 octets):  acef44f1be5aab86 64a9749a

   {client}  send a Finished handshake message

   {client}  send record:

      cleartext (36 octets):  140000205b3a3d1b 354919bcea11c379
         edf28d2e780fe28a 0f9d4c5bb3f104b4 30a4ba70

      ciphertext (58 octets):  17030100356c5477 611b08bfe7b2493f
         f05e70873262ae65 cb663667b93931b1 93f36c372e3c5483
         c6a49fc10096b367 09075f2dd5f3f36f 564f

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

      PRK (32 octets):  af68f3b851db647a 50ccd03afb94d52e
         8f1349a66f56f54d 683ca3a9900ed295

      key info (54 octets):  001032544c532031 2e332c206561726c
         79206170706c6963 6174696f6e206461 7461206b65792065
         7870616e73696f6e 2c206b657900

      key output (16 octets):  c713c8bb3ff78315 b982cfb9a07c80b0

      iv info (53 octets):  000c31544c532031 2e332c206561726c
         79206170706c6963 6174696f6e206461 7461206b65792065
         7870616e73696f6e 2c20697600

      iv output (12 octets):  3750adac15984d62 31053f36

   {client}  send record:

      cleartext (6 octets):  414243444546
```

```
      ciphertext (28 octets):  17030100170a9923 e64e0860d54570f8
         d31b86197fd67248 d38cd32f

   {server}  create an ephemeral x25519 key pair:

      private key (32 octets):  0df26b2e9c055b1f bb96b97718ef6f1a
         5549839aff3e3f6a 60b6b356ff631611

      public key (32 octets):  e6c6574f90c8d810 e002c083efa8d895
         389061c5bcd71c63 6f5ae1daf0b30112

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

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

   {server}  derive read traffic keys using label "early handshake key
      expansion":

      PRK (32 octets):  af68f3b851db647a 50ccd03afb94d52e
         8f1349a66f56f54d 683ca3a9900ed295

      key info (47 octets):  00102b544c532031 2e332c206561726c
         792068616e647368 616b65206b657920 657870616e73696f
         6e2c206b657900

      key output (16 octets):  eee93d2d1de2b7aa 0939dd335a5389ed

      iv info (46 octets):  000c2a544c532031 2e332c206561726c
         792068616e647368 616b65206b657920 657870616e73696f 6e2c20697600

      iv output (12 octets):  acef44f1be5aab86 64a9749a

   {server}  send a ServerHello handshake message

   {server}  extract secret "handshake":

      salt (32 octets):  50b55777d9078122 7376f3701a850c21
         040983207b0c2469 9580e18ba29bd5f6

      ikm (32 octets):  5a2925fe53a03d94 3ae4e2c64dc2bc06
         2c916390403174ac fc64892091e56550

      secret (32 octets):  eff9edc8b2b872d3 e34214189cb5f10a
         45c873eef248f458 15c693215bbc2277

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

```
      handshake hash (64 octets):  4a158002aa771132 1d86db9554a8cac1
         f27fa052ab3f8356 1aefa6e1eadc336f ffc65d93ccb7b739
         b3f1ba164a8c1893 4e069aa123889906 2188e39045f3d821

      PRK (32 octets):  eff9edc8b2b872d3 e34214189cb5f10a
         45c873eef248f458 15c693215bbc2277

      info (108 octets):  002028544c532031 2e332c20636c6965
         6e742068616e6473 68616b6520747261 6666696320736563
         726574404a158002 aa7711321d86db95 54a8cac1f27fa052
         ab3f83561aefa6e1 eadc336fffc65d93 ccb7b739b3f1ba16
         4a8c18934e069aa1 238899062188e390 45f3d821

      output (32 octets):  f14973e577eff04c a6795e3f4c1b7752
         901b6e4fbde4ac02 e17e067f08d052f1

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

      handshake hash (64 octets):  4a158002aa771132 1d86db9554a8cac1
         f27fa052ab3f8356 1aefa6e1eadc336f ffc65d93ccb7b739
         b3f1ba164a8c1893 4e069aa123889906 2188e39045f3d821

      PRK (32 octets):  eff9edc8b2b872d3 e34214189cb5f10a
         45c873eef248f458 15c693215bbc2277

      info (108 octets):  002028544c532031 2e332c2073657276
         65722068616e6473 68616b6520747261 6666696320736563
         726574404a158002 aa7711321d86db95 54a8cac1f27fa052
         ab3f83561aefa6e1 eadc336fffc65d93 ccb7b739b3f1ba16
         4a8c18934e069aa1 238899062188e390 45f3d821

      output (32 octets):  e6e9623c5c3d0023 c64f84145fca6a63
         736f3c8e37ba71da d139daf40f8e4ec0

   {server}  extract secret "master":

      salt (32 octets):  eff9edc8b2b872d3 e34214189cb5f10a
         45c873eef248f458 15c693215bbc2277

      ikm (32 octets):  0000000000000000 0000000000000000
         0000000000000000 0000000000000000

      secret (32 octets):  faecb2e5b0bef416 13d0ff2ae3441ca9
         408b0074cbbea3a2 c270e1cb4a2578cc

   {server}  send record:
```

```
      cleartext (88 octets):  020000547f101750 d392fda7530a72ee
         97ec5c43731022b2 168b2ddd967ed3be 04ddbdee74631301
         002e002900020000 00280024001d0020 e6c6574f90c8d810
         e002c083efa8d895 389061c5bcd71c63 6f5ae1daf0b30112

      ciphertext (93 octets):  1603010058020000 547f101750d392fd
         a7530a72ee97ec5c 43731022b2168b2d dd967ed3be04ddbd
         ee74631301002e00 2900020000002800 24001d0020e6c657
         4f90c8d810e002c0 83efa8d895389061 c5bcd71c636f5ae1 daf0b30112

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

      PRK (32 octets):  e6e9623c5c3d0023 c64f84145fca6a63
         736f3c8e37ba71da d139daf40f8e4ec0

      key info (41 octets):  001025544c532031 2e332c2068616e64
         7368616b65206b65 7920657870616e73 696f6e2c206b6579 00

      key output (16 octets):  64cff1125fc9090b b3ebb29cf49b26a1

      iv info (40 octets):  000c24544c532031 2e332c2068616e64
         7368616b65206b65 7920657870616e73 696f6e2c20697600

      iv output (12 octets):  6292d575366424a0 80f01a22

   {server}  send a EncryptedExtensions handshake message

   {server}  send a Finished handshake message

   {server}  send record:

      cleartext (74 octets):  080000220020000a 00140012001d0017
         0018001901000101 0102010301040000 0000002a00001400
         00206a8db5af860c 85fee7da54cf130a 8fbb7d48563b457c
         6c48bf58e649877f 4241

      ciphertext (96 octets):  170301005bf374b2 5eb166088968e7d5
         fdd0a28ed3411f92 7b4e3fa412bde6c5 ce0ed3627c24b60e
         d67a87dd33444e78 8489c2edcc2b02c5 f520d81e1ab1bdc2
         8c2f9eef9c17a646 0d7043fe958a831b bfe82671b356f6bc
         d1bf43290b8d05a3

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

      handshake hash (64 octets):  055666b5e4969791 a49484a3bc0e44db
         db8ac3e18a5dfe8b cc3d700a78d04b90 ffc65d93ccb7b739
         b3f1ba164a8c1893 4e069aa123889906 2188e39045f3d821
```

```
      PRK (32 octets):  faecb2e5b0bef416 13d0ff2ae3441ca9
         408b0074cbbea3a2 c270e1cb4a2578cc

      info (110 octets):  00202a544c532031 2e332c20636c6965
         6e74206170706c69 636174696f6e2074 7261666669632073
         6563726574400556 66b5e4969791a494 84a3bc0e44dbdb8a
         c3e18a5dfe8bcc3d 700a78d04b90ffc6 5d93ccb7b739b3f1
         ba164a8c18934e06 9aa1238899062188 e39045f3d821

      output (32 octets):  4c9f3438c915bc4d 0a8a66ec606bed75
         db479d3853d995f1 bc2b97274abf4494

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

      handshake hash (64 octets):  055666b5e4969791 a49484a3bc0e44db
         db8ac3e18a5dfe8b cc3d700a78d04b90 ffc65d93ccb7b739
         b3f1ba164a8c1893 4e069aa123889906 2188e39045f3d821

      PRK (32 octets):  faecb2e5b0bef416 13d0ff2ae3441ca9
         408b0074cbbea3a2 c270e1cb4a2578cc

      info (110 octets):  00202a544c532031 2e332c2073657276
         6572206170706c69 636174696f6e2074 7261666669632073
         6563726574400556 66b5e4969791a494 84a3bc0e44dbdb8a
         c3e18a5dfe8bcc3d 700a78d04b90ffc6 5d93ccb7b739b3f1
         ba164a8c18934e06 9aa1238899062188 e39045f3d821

      output (32 octets):  8045d1d46cc35dfa 71b8ded37d54fc72
         afd5ccdaaed73a24 13cdea56a0e363d4

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

      PRK (32 octets):  8045d1d46cc35dfa 71b8ded37d54fc72
         afd5ccdaaed73a24 13cdea56a0e363d4

      key info (48 octets):  00102c544c532031 2e332c206170706c
         69636174696f6e20 64617461206b6579 20657870616e7369
         6f6e2c206b657900

      key output (16 octets):  8bef5ef0dfa457f1 fcc656c8c187dba9

      iv info (47 octets):  000c2b544c532031 2e332c206170706c
         69636174696f6e20 64617461206b6579 20657870616e7369
         6f6e2c20697600

      iv output (12 octets):  d38dc8e37a7c9464 7e4f4cb5
```

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

{client}  extract secret "handshake":

   salt (32 octets):  50b55777d9078122 7376f3701a850c21
      040983207b0c2469 9580e18ba29bd5f6

   ikm (32 octets):  5a2925fe53a03d94 3ae4e2c64dc2bc06
      2c916390403174ac fc64892091e56550

   secret (32 octets):  eff9edc8b2b872d3 e34214189cb5f10a
      45c873eef248f458 15c693215bbc2277

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

   handshake hash (64 octets):  4a158002aa771132 1d86db9554a8cac1
      f27fa052ab3f8356 1aefa6e1eadc336f ffc65d93ccb7b739
      b3f1ba164a8c1893 4e069aa123889906 2188e39045f3d821

   PRK (32 octets):  eff9edc8b2b872d3 e34214189cb5f10a
      45c873eef248f458 15c693215bbc2277

   info (108 octets):  002028544c532031 2e332c20636c6965
      6e742068616e6473 68616b6520747261 6666696320736563
      726574404a158002 aa7711321d86db95 54a8cac1f27fa052
      ab3f83561aefa6e1 eadc336fffc65d93 ccb7b739b3f1ba16
      4a8c18934e069aa1 238899062188e390 45f3d821

   output (32 octets):  f14973e577eff04c a6795e3f4c1b7752
      901b6e4fbde4ac02 e17e067f08d052f1

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

   handshake hash (64 octets):  4a158002aa771132 1d86db9554a8cac1
      f27fa052ab3f8356 1aefa6e1eadc336f ffc65d93ccb7b739
      b3f1ba164a8c1893 4e069aa123889906 2188e39045f3d821

   PRK (32 octets):  eff9edc8b2b872d3 e34214189cb5f10a
      45c873eef248f458 15c693215bbc2277

   info (108 octets):  002028544c532031 2e332c2073657276
      65722068616e6473 68616b6520747261 6666696320736563
      726574404a158002 aa7711321d86db95 54a8cac1f27fa052
      ab3f83561aefa6e1 eadc336fffc65d93 ccb7b739b3f1ba16
      4a8c18934e069aa1 238899062188e390 45f3d821
```

```
      output (32 octets):  e6e9623c5c3d0023 c64f84145fca6a63
         736f3c8e37ba71da d139daf40f8e4ec0

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

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

      PRK (32 octets):  e6e9623c5c3d0023 c64f84145fca6a63
         736f3c8e37ba71da d139daf40f8e4ec0

      key info (41 octets):  001025544c532031 2e332c2068616e64
         7368616b65206b65 7920657870616e73 696f6e2c206b6579 00

      key output (16 octets):  64cff1125fc9090b b3ebb29cf49b26a1

      iv info (40 octets):  000c24544c532031 2e332c2068616e64
         7368616b65206b65 7920657870616e73 696f6e2c20697600

      iv output (12 octets):  6292d575366424a0 80f01a22

   {client}  send record:

      cleartext (2 octets):  0101

      ciphertext (24 octets):  1703010013687eb4 9a969a751172cf83
         fb367fc3e6554ff2

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

      PRK (32 octets):  f14973e577eff04c a6795e3f4c1b7752
         901b6e4fbde4ac02 e17e067f08d052f1

      key info (41 octets):  001025544c532031 2e332c2068616e64
         7368616b65206b65 7920657870616e73 696f6e2c206b6579 00

      key output (16 octets):  a73add6f2e57fc83 c79573d270cc6509

      iv info (40 octets):  000c24544c532031 2e332c2068616e64
         7368616b65206b65 7920657870616e73 696f6e2c20697600

      iv output (12 octets):  d61dd1b8a247c421 c244041f

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

```
      handshake hash (64 octets):  055666b5e4969791 a49484a3bc0e44db
         db8ac3e18a5dfe8b cc3d700a78d04b90 ffc65d93ccb7b739
         b3f1ba164a8c1893 4e069aa123889906 2188e39045f3d821

      PRK (32 octets):  faecb2e5b0bef416 13d0ff2ae3441ca9
         408b0074cbbea3a2 c270e1cb4a2578cc

      info (110 octets):  00202a544c532031 2e332c20636c6965
         6e74206170706c69 636174696f6e2074 7261666669632073
         6563726574400556 66b5e4969791a494 84a3bc0e44dbdb8a
         c3e18a5dfe8bcc3d 700a78d04b90ffc6 5d93ccb7b739b3f1
         ba164a8c18934e06 9aa1238899062188 e39045f3d821

      output (32 octets):  4c9f3438c915bc4d 0a8a66ec606bed75
         db479d3853d995f1 bc2b97274abf4494

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

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

   {client}  send a Finished handshake message

   {client}  send record:

      cleartext (36 octets):  140000208a5ff8f5 2a3e97eaaa1feb1c
         0ee058d9b923c788 592c46fcdd240e5d 17a80d40

      ciphertext (58 octets):  170301003551e152 cd27816eb07f79e8
         9c71bf328d373b5b b8390821a319a957 03b3a563f0042de9
         713c82a48cd42321 4c7efa9806153dec 62de

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

      PRK (32 octets):  4c9f3438c915bc4d 0a8a66ec606bed75
         db479d3853d995f1 bc2b97274abf4494

      key info (48 octets):  00102c544c532031 2e332c206170706c
         69636174696f6e20 64617461206b6579 20657870616e7369
         6f6e2c206b657900

      key output (16 octets):  aeffc85a70981079 9828a861b510d20a

      iv info (47 octets):  000c2b544c532031 2e332c206170706c
         69636174696f6e20 64617461206b6579 20657870616e7369
         6f6e2c20697600
```

```
      iv output (12 octets):  a240fcfee10fc824 5f977745

   {client}  derive secret "resumption master secret":

      handshake hash (64 octets):  86dd36a494000932 c9f58c7410cff699
         2b53f90b2e457196 cb0a62a306fabc32 ffc65d93ccb7b739
         b3f1ba164a8c1893 4e069aa123889906 2188e39045f3d821

      PRK (32 octets):  faecb2e5b0bef416 13d0ff2ae3441ca9
         408b0074cbbea3a2 c270e1cb4a2578cc

      info (101 octets):  002021544c532031 2e332c2072657375
         6d7074696f6e206d 6173746572207365 637265744086dd36
         a494000932c9f58c 7410cff6992b53f9 0b2e457196cb0a62
         a306fabc32ffc65d 93ccb7b739b3f1ba 164a8c18934e069a
         a1238899062188e3 9045f3d821

      output (32 octets):  a42c624281007958 cf5b386cdeea9505
         78f5a4e8ce376e5b 5e1cc521f50a8e13

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

      PRK (32 octets):  f14973e577eff04c a6795e3f4c1b7752
         901b6e4fbde4ac02 e17e067f08d052f1

      key info (41 octets):  001025544c532031 2e332c2068616e64
         7368616b65206b65 7920657870616e73 696f6e2c206b6579 00

      key output (16 octets):  a73add6f2e57fc83 c79573d270cc6509

      iv info (40 octets):  000c24544c532031 2e332c2068616e64
         7368616b65206b65 7920657870616e73 696f6e2c20697600

      iv output (12 octets):  d61dd1b8a247c421 c244041f

   {server}  derive read traffic keys using label "application data key
      expansion" (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):  1703010043002960 3d4a0b22d5c35dbe
         6b57d8015fbe1364 a6eb5047be44ddb7 9c52225b97d85854
         59322c960eb231a5 99464c714b5a3a5e 06dd664311d9d4ac
         182853c7597e7a9d

   {server}  send record:

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

      ciphertext (72 octets):  170301004387d132 c8efbcd1bb57be5b
         1b8bdd232247d909 45f87d6076a8f110 addb8c27ba05b107
         28e5b103aaac58ce 4b6693dbf77066ed a8168a4f6df78d8f
         4f9a743dc72b3156

   {client}  send record:

      cleartext (2 octets):  0100

      ciphertext (24 octets):  17030100136a2ffa 499ba7a94e2cc32d
         e33f03e69da02d0e

   {server}  send record:

      cleartext (2 octets):  0100

      ciphertext (24 octets):  1703010013e01536 07df77f766766ee3
         b61e6746db71bbed
```

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