TLS
Internet-Draft
Intended status: Standards Track
Expires: June 7, 2018

M. Thomson
Mozilla

December 4, 2017

Example Handshake Traces for TLS 1.3
draft-ietf-tls-tls13-vectors-03

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 https://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 June 7, 2018.

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):  b4 bb 49 8f 82 79 30 3d 98 08 36 39 9b 36 c6 98 8c
   0c 68 de 55 e1 bd b8 26 d3 90 1a 24 61 ea fd 2d e4 9a 91 d0 15 ab
   bc 9a 95 13 7a ce 6c 1a f1 9e aa 6a f9 8c 7c ed 43 12 09 98 e1 87
   a8 0e e0 cc b0 52 4b 1b 01 8c 3e 0b 63 26 4d 44 9a 6d 38 e2 2a 5f
   da 43 08 46 74 80 30 53 0e f0 46 1c 8c a9 d9 ef bf ae 8e a6 d1 d0
   3e 2b d1 93 ef f0 ab 9a 80 02 c4 74 28 a6 d3 5a 8d 88 d7 9f 7f 1e
   3f

public exponent:  01 00 01
```

```
   private exponent:  04 de a7 05 d4 3a 6e a7 20 9d d8 07 21 11 a8 3c 81
      e3 22 a5 92 78 b3 34 80 64 1e af 7c 0a 69 85 b8 e3 1c 44 f6 de 62
      e1 b4 c2 30 9f 61 26 e7 7b 7c 41 e9 23 31 4b bf a3 88 13 05 dc 12
      17 f1 6c 81 9c e5 38 e9 22 f3 69 82 8d 0e 57 19 5d 8c 84 88 46 02
```



```
      07 b2 fa a7 26 bc f7 08 bb d7 db 7f 67 9f 89 34 92 fc 2a 62 2e 08
      97 0a ac 44 1c e4 e0 c3 08 8d f2 5a e6 79 23 3d f8 a3 bd a2 ff 99
      41

   prime1:  e4 35 fb 7c c8 37 37 75 6d ac ea 96 ab 7f 59 a2 cc 10 69 db
      7d eb 19 0e 17 e3 3a 53 2b 27 3f 30 a3 27 aa 0a aa bc 58 cd 67 46
      6a f9 84 5f ad c6 75 fe 09 4a f9 2c 4b d1 f2 c1 bc 33 dd 2e 05 15

   prime2:  ca bd 3b c0 e0 43 86 64 c8 d4 cc 9f 99 97 7a 94 d9 bb fe ad
      8e 43 87 0a ba e3 f7 eb 8b 4e 0e ee 8a f1 d9 b4 71 9b a6 19 6c f2
      cb ba ee eb f8 b3 49 0a fe 9e 9f fa 74 a8 8a a5 1f c6 45 62 93 03

   exponent1:  3f 57 34 5c 27 fe 1b 68 7e 6e 76 16 27 b7 8b 1b 82 64 33
      dd 76 0f a0 be a6 a6 ac f3 94 90 aa 1b 47 cd a4 86 9d 68 f5 84 dd
      5b 50 29 bd 32 09 3b 82 58 66 1f e7 15 02 5e 5d 70 a4 5a 08 d3 d3
      19

   exponent2:  18 3d a0 13 63 bd 2f 28 85 ca cb dc 99 64 bf 47 64 f1 51
      76 36 f8 64 01 28 6f 71 89 3c 52 cc fe 40 a6 c2 3d 0d 08 6b 47 c6
      fb 10 d8 fd 10 41 e0 4d ef 7e 9a 40 ce 95 7c 41 77 94 e1 04 12 d1
      39

   coefficient:  83 9c a9 a0 85 e4 28 6b 2c 90 e4 66 99 7a 2c 68 1f 21
      33 9a a3 47 78 14 e4 de c1 18 33 05 0e d5 0d d1 3c c0 38 04 8a 43
      c5 9b 2a cc 41 68 89 c0 37 66 5f e5 af a6 05 96 9f 8c 01 df a5 ca
      96 9d
```

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.

{client} create an ephemeral x25519 key pair:

private key (32 octets): b1 6a 3c 97 a7 19 0b ec c4 00 2a 2f be
80 40 b5 99 45 df 0b bd 0c e1 ba db f4 aa 6d 4f 0f a1 9e

public key (32 octets): 78 e5 89 74 13 f1 71 53 c7 0c f3 3f a3 4c
84 97 72 4b da b4 f5 7f 9d 01 c9 53 f5 88 f0 30 46 61

{client} send a ClientHello handshake message

{client} send handshake record:

payload (190 octets): 01 00 00 ba 03 03 c4 e2 ea b7 cc 4b bb 43
7d fa b4 7c a5 6a f8 a0 db 07 2b 90 e5 36 f9 c4 a4 9f ac 89 84
9c 10 b2 00 00 06 13 01 13 03 13 02 01 00 00 8b 00 00 00 0b 00
09 00 00 06 73 65 72 76 65 72 ff 01 00 01 00 00 0a 00 14 00 12
00 1d 00 17 00 18 00 19 01 00 01 01 01 02 01 03 01 04 00 23 00
00 00 28 00 26 00 24 00 1d 00 20 78 e5 89 74 13 f1 71 53 c7 0c
f3 3f a3 4c 84 97 72 4b da b4 f5 7f 9d 01 c9 53 f5 88 f0 30 46
61 00 2b 00 03 02 7f 16 00 0d 00 20 00 1e 04 03 05 03 06 03 02
03 08 04 08 05 08 06 04 01 05 01 06 01 02 01 04 02 05 02 06 02
02 02 00 2d 00 02 01 01

ciphertext (195 octets): 16 03 01 00 be 01 00 00 ba 03 03 c4 e2
ea b7 cc 4b bb 43 7d fa b4 7c a5 6a f8 a0 db 07 2b 90 e5 36 f9
c4 a4 9f ac 89 84 9c 10 b2 00 00 06 13 01 13 03 13 02 01 00 00
8b 00 00 00 0b 00 09 00 00 06 73 65 72 76 65 72 ff 01 00 01 00
00 0a 00 14 00 12 00 1d 00 17 00 18 00 19 01 00 01 01 01 02 01
03 01 04 00 23 00 00 00 28 00 26 00 24 00 1d 00 20 78 e5 89 74
13 f1 71 53 c7 0c f3 3f a3 4c 84 97 72 4b da b4 f5 7f 9d 01 c9
53 f5 88 f0 30 46 61 00 2b 00 03 02 7f 16 00 0d 00 20 00 1e 04
03 05 03 06 03 02 03 08 04 08 05 08 06 04 01 05 01 06 01 02 01
04 02 05 02 06 02 02 02 00 2d 00 02 01 01

{server} extract secret "early":

salt: (absent)

ikm (32 octets): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```
   secret (32 octets):  33 ad 0a 1c 60 7e c0 3b 09 e6 cd 98 93 68 0c
      e2 10 ad f3 00 aa 1f 26 60 e1 b2 2e 10 f1 70 f9 2a

{server}  create an ephemeral x25519 key pair:

   private key (32 octets):  20 eb 30 48 af fc bf 2b ff 56 df b5 1e
      93 4d 78 a0 f5 d2 38 29 41 70 b1 0e ea 18 31 69 68 8b 65

   public key (32 octets):  ee 31 96 ca 63 98 21 a1 7b 51 68 ab 61 0d
      70 57 d2 b2 50 84 89 1f 87 ef 26 cf 0c 26 84 e5 d6 7e

{server}  send a ServerHello handshake message

{server}  derive secret for handshake "tls13 derived":

   PRK (32 octets):  33 ad 0a 1c 60 7e c0 3b 09 e6 cd 98 93 68 0c e2
      10 ad f3 00 aa 1f 26 60 e1 b2 2e 10 f1 70 f9 2a
```



```
   hash (32 octets):  e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24
      27 ae 41 e4 64 9b 93 4c a4 95 99 1b 78 52 b8 55

   info (49 octets):  00 20 0d 74 6c 73 31 33 20 64 65 72 69 76 65 64
      20 e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24 27 ae 41 e4
      64 9b 93 4c a4 95 99 1b 78 52 b8 55

   output (32 octets):  6f 26 15 a1 08 c7 02 c5 67 8f 54 fc 9d ba b6
      97 16 c0 76 18 9c 48 25 0c eb ea c3 57 6c 36 11 ba

{server}  extract secret "handshake":

   salt (32 octets):  6f 26 15 a1 08 c7 02 c5 67 8f 54 fc 9d ba b6 97
      16 c0 76 18 9c 48 25 0c eb ea c3 57 6c 36 11 ba

   ikm (32 octets):  61 d3 4a ad f2 5e 22 3a 2c e6 fb 59 f8 a0 f9 d1
      d7 5f 18 87 df b0 6c 0f ff f8 47 6d c3 c5 0f 47

   secret (32 octets):  79 07 c2 82 34 f1 6c a8 71 a4 6b eb 25 da 54
      7f dc 8a ab 96 d1 4e ef f8 0f 5b 12 f9 ad 8a c9 d6

{server}  derive secret "tls13 c hs traffic":
```

```
      PRK (32 octets):  79 07 c2 82 34 f1 6c a8 71 a4 6b eb 25 da 54 7f
         dc 8a ab 96 d1 4e ef f8 0f 5b 12 f9 ad 8a c9 d6

      hash (32 octets):  2a 63 e9 0b 84 e5 c9 79 80 56 98 41 19 3b 80 94
         22 19 36 52 19 ad 23 90 b6 80 64 c2 ae bb 09 69

      info (54 octets):  00 20 12 74 6c 73 31 33 20 63 20 68 73 20 74 72
         61 66 66 69 63 20 2a 63 e9 0b 84 e5 c9 79 80 56 98 41 19 3b 80
         94 22 19 36 52 19 ad 23 90 b6 80 64 c2 ae bb 09 69

      output (32 octets):  40 2b 60 6f 3c b0 c8 5b 6d bf fb fd a9 df 79
         14 58 4a 0e b9 21 1b b5 e9 0b a4 81 f2 5c 4b 94 e2

   {server}  derive secret "tls13 s hs traffic":

      PRK (32 octets):  79 07 c2 82 34 f1 6c a8 71 a4 6b eb 25 da 54 7f
         dc 8a ab 96 d1 4e ef f8 0f 5b 12 f9 ad 8a c9 d6

      hash (32 octets):  2a 63 e9 0b 84 e5 c9 79 80 56 98 41 19 3b 80 94
         22 19 36 52 19 ad 23 90 b6 80 64 c2 ae bb 09 69

      info (54 octets):  00 20 12 74 6c 73 31 33 20 73 20 68 73 20 74 72
         61 66 66 69 63 20 2a 63 e9 0b 84 e5 c9 79 80 56 98 41 19 3b 80
         94 22 19 36 52 19 ad 23 90 b6 80 64 c2 ae bb 09 69
```



```
      output (32 octets):  a2 c1 53 5b 55 26 42 8b 49 cb e6 cc 3c 19 23
         7c 37 4e 94 db 25 6c 96 4d 4d 13 76 a9 de 1a c5 12

   {server}  derive secret for master "tls13 derived":

      PRK (32 octets):  79 07 c2 82 34 f1 6c a8 71 a4 6b eb 25 da 54 7f
         dc 8a ab 96 d1 4e ef f8 0f 5b 12 f9 ad 8a c9 d6

      hash (32 octets):  e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24
         27 ae 41 e4 64 9b 93 4c a4 95 99 1b 78 52 b8 55

      info (49 octets):  00 20 0d 74 6c 73 31 33 20 64 65 72 69 76 65 64
         20 e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24 27 ae 41 e4
         64 9b 93 4c a4 95 99 1b 78 52 b8 55
```

```
   output (32 octets):  44 50 97 b3 09 4b 9c e8 35 af 72 02 5d 0f d3
      80 ae 2b ae 88 06 08 f6 b2 b9 92 42 92 eb 04 71 d1

{server}  extract secret "master":

   salt (32 octets):  44 50 97 b3 09 4b 9c e8 35 af 72 02 5d 0f d3 80
      ae 2b ae 88 06 08 f6 b2 b9 92 42 92 eb 04 71 d1

   ikm (32 octets):  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

   secret (32 octets):  23 07 37 68 ca 09 44 ef de d6 a1 fd 17 3e 7a
      1f a7 51 b2 1b 6b f2 07 66 1c b2 94 bc 29 f4 49 c7

{server}  send handshake record:

   payload (90 octets):  02 00 00 56 03 03 8e 58 c0 e7 0c 99 2d 7f fc
      80 98 eb dc 67 ba 85 05 e4 2e 44 05 bf 77 23 95 49 24 7a b2 ba
      20 3c 00 13 01 00 00 2e 00 28 00 24 00 1d 00 20 ee 31 96 ca 63
      98 21 a1 7b 51 68 ab 61 0d 70 57 d2 b2 50 84 89 1f 87 ef 26 cf
      0c 26 84 e5 d6 7e 00 2b 00 02 7f 16

   ciphertext (95 octets):  16 03 03 00 5a 02 00 00 56 03 03 8e 58 c0
      e7 0c 99 2d 7f fc 80 98 eb dc 67 ba 85 05 e4 2e 44 05 bf 77 23
      95 49 24 7a b2 ba 20 3c 00 13 01 00 00 2e 00 28 00 24 00 1d 00
      20 ee 31 96 ca 63 98 21 a1 7b 51 68 ab 61 0d 70 57 d2 b2 50 84
      89 1f 87 ef 26 cf 0c 26 84 e5 d6 7e 00 2b 00 02 7f 16

{server}  send a EncryptedExtensions handshake message

{server}  send a Certificate handshake message

{server}  send a CertificateVerify handshake message
```



```
{server}  calculate finished "tls13 finished":

   PRK (32 octets):  a2 c1 53 5b 55 26 42 8b 49 cb e6 cc 3c 19 23 7c
      37 4e 94 db 25 6c 96 4d 4d 13 76 a9 de 1a c5 12

   hash (0 octets):  (empty)

   info (18 octets):  00 20 0e 74 6c 73 31 33 20 66 69 6e 69 73 68 65
```

```
      64 00

   output (32 octets):  d2 7d 01 ab e2 d9 d6 68 98 dc 10 f8 5d 92 2f
      d6 ff f5 1d b8 80 f4 af 64 52 b7 1c 05 c3 fc 42 67

{server}  send a Finished handshake message

{server}  send handshake record:

   payload (651 octets):  08 00 00 1e 00 1c 00 0a 00 14 00 12 00 1d
      00 17 00 18 00 19 01 00 01 01 01 02 01 03 01 04 00 00 00 00 0b
      00 01 b9 00 00 01 b5 00 01 b0 30 82 01 ac 30 82 01 15 a0 03 02
      01 02 02 01 02 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00 30
      0e 31 0c 30 0a 06 03 55 04 03 13 03 72 73 61 30 1e 17 0d 31 36
      30 37 33 30 30 31 32 33 35 39 5a 17 0d 32 36 30 37 33 30 30 31
      32 33 35 39 5a 30 0e 31 0c 30 0a 06 03 55 04 03 13 03 72 73 61
      30 81 9f 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 81 8d
      00 30 81 89 02 81 81 00 b4 bb 49 8f 82 79 30 3d 98 08 36 39 9b
      36 c6 98 8c 0c 68 de 55 e1 bd b8 26 d3 90 1a 24 61 ea fd 2d e4
      9a 91 d0 15 ab bc 9a 95 13 7a ce 6c 1a f1 9e aa 6a f9 8c 7c ed
      43 12 09 98 e1 87 a8 0e e0 cc b0 52 4b 1b 01 8c 3e 0b 63 26 4d
      44 9a 6d 38 e2 2a 5f da 43 08 46 74 80 30 53 0e f0 46 1c 8c a9
      d9 ef bf ae 8e a6 d1 d0 3e 2b d1 93 ef f0 ab 9a 80 02 c4 74 28
      a6 d3 5a 8d 88 d7 9f 7f 1e 3f 02 03 01 00 01 a3 1a 30 18 30 09
      06 03 55 1d 13 04 02 30 00 30 0b 06 03 55 1d 0f 04 04 03 02 05
      a0 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00 03 81 81 00 85
      aa d2 a0 e5 b9 27 6b 90 8c 65 f7 3a 72 67 17 06 18 a5 4c 5f 8a
      7b 33 7d 2d f7 a5 94 36 54 17 f2 ea e8 f8 a5 8c 8f 81 72 f9 31
      9c f3 6b 7f d6 c5 5b 80 f2 1a 03 01 51 56 72 60 96 fd 33 5e 5e
      67 f2 db f1 02 70 2e 60 8c ca e6 be c1 fc 63 a4 2a 99 be 5c 3e
      b7 10 7c 3c 54 e9 b9 eb 2b d5 20 3b 1c 3b 84 e0 a8 b2 f7 59 40
      9b a3 ea c9 d9 1d 40 2d cc 0c c8 f8 96 12 29 ac 91 87 b4 2b 4d
      e1 00 00 0f 00 00 84 08 04 00 80 35 dc 65 98 6e 5d 7a 91 25 7a
      91 01 85 5d 87 54 9c 1b 0d 19 6b 6c 19 da a2 67 38 30 ff 73 a4
      51 ab 79 48 55 ca c3 40 e8 48 fd 10 5a 96 ed b4 23 48 99 8c d9
      ac 0d f6 63 d8 92 7e 88 67 25 57 0a 41 52 28 af 19 67 a2 2d 9b
      4d 36 7b b0 90 e4 f0 76 ea 5f a4 7d c5 7c ac 77 cb e6 21 7f 3e
      fa 6f 10 53 12 9e b9 1a cb 05 48 c6 38 16 89 8d 36 79 8d 6a c0
      38 89 c4 13 c9 27 de df f9 39 d0 58 8c 14 00 00 20 4a 81 42 ca
```



```
      b4 49 41 89 68 94 06 27 07 e6 92 d6 32 a8 6a 12 4c be 2a 81 6b
```

```
      3d ef a1 b3 15 40 db

   ciphertext (673 octets):  17 03 03 02 9c 6f 0c 3d 25 89 2d 11 1b
      9e 10 b7 bf 9e cb 09 ec 5e 87 75 53 b3 15 3e b9 80 12 4c 44 59
      58 b1 71 01 41 8b 00 d8 f0 2f af cc 55 ba 06 25 88 ba 53 0e f0
      9a 8f b4 c7 d6 de 1f 8b 7e b8 d8 b6 d2 1e 01 34 a9 75 74 ae 71
      2d 5c b6 c1 5d 19 b3 47 c7 8a 88 4a 71 ff b8 c2 e7 60 02 22 16
      a7 93 8f 10 81 8c 3f 81 16 b4 5a 39 79 d0 9d 72 52 e3 b4 4f 10
      ae 68 f5 a6 1b 31 d8 e0 b4 15 f8 09 7d d5 14 f1 ba d1 49 dc bc
      e5 cb 35 48 55 f6 1d 56 08 c7 b9 d5 85 9a d9 f4 e2 02 84 45 5d
      9d ab 37 d5 6e 09 5e bd 88 68 89 a2 36 3f c9 7b 16 62 06 63 7c
      ca 01 ab 37 7e 9d 3f 3d 06 4f 6a fc 87 22 1a bf e6 d5 23 27 e9
      96 91 6e d4 a3 ed 24 9d 5e 71 04 44 dc 78 64 e4 31 6d a8 01 83
      b0 cc 0c 3b 38 0a 0a 87 a8 36 17 13 86 c7 f1 b8 db 0b 15 30 a4
      39 6c 1a d4 53 2a 60 7a 55 31 90 63 83 f7 bb 9c cc 20 da a8 ec
      47 af 17 e5 7e d6 fc c5 f0 61 b7 cb 5a 42 6d 96 96 19 3f e4 a5
      13 56 82 a2 2e 0c 3f a2 26 9f 0a bf c6 31 6a 19 6f e8 7c f8 91
      29 b7 7c 43 41 ae 6c 12 b6 c5 70 d6 fb b5 46 0f f7 c6 5d a5 80
      b1 17 0c 49 12 e4 bd b5 9b 2d 14 f2 7a 05 35 3e 51 d2 18 a3 60
      15 4c bf 08 f2 9c 64 4b 28 8f 3d 42 4e e8 ea bb f1 26 fd 6b e4
      b2 b0 f1 97 5f e4 73 a3 df a8 83 78 bd 5b ea ce ee 52 0e 6e 2d
      c7 40 8e 83 8f 34 36 29 c1 a4 a3 dd fa 58 c3 c3 f8 08 5a 79 3a
      f2 49 38 3d e5 51 a8 a9 50 4a ea 31 31 28 27 ad d1 0c ed b3 39
      e4 a2 32 11 85 aa 27 6f 76 2b 0a 6b cd 9e f8 f8 2c 0f de ac 3b
      60 d6 5d 10 94 99 b9 1f 19 4b 88 4a cd c7 b0 d6 3b 8c f6 f0 d8
      cb ab f1 3c a9 96 69 42 e1 6a 3d 75 24 ad f3 3e ee e5 de e8 91
      6b 57 31 c3 6e 21 1a 2d fb fb 65 60 07 91 3b 51 c5 a0 97 50 df
      a9 70 8d 38 e0 a2 0b 5c ee c9 58 4b c7 aa 83 70 94 b9 6e fd 55
      b0 7a c3 72 00 42 4c f9 eb 54 2d 53 b5 6e 71 32 33 83 c1 93 f2
      cd f6 22 08 35 48 07 a0 19 3e cd 23 78 ed dd 72 74 27 fe 9d f9
      d0 46 28 b8 9c 38 0b 3b 83 b5 e6 95 cf ba 2d 8d 2f 30 ce 0e 19
      17 ee 05 2e 7e c9 4d 4d da 39 b6 93 e0 1e a9 68 ad 95 1d 40 cc
      99 66 82 0e 7a 95 ff 17 e0 fd 0b 4d d0 d2 a8 70 d0 b5 ab d9 10
      79 5a 3e d7 2d 66 54 ba e0 a7 3a 85 fc dc 9b f8 98 53 82 8c 2c
      4e 07 51 be e6 e4 a7 de 11

{server}  derive secret "tls13 c ap traffic":

   PRK (32 octets):  23 07 37 68 ca 09 44 ef de d6 a1 fd 17 3e 7a 1f
      a7 51 b2 1b 6b f2 07 66 1c b2 94 bc 29 f4 49 c7

   hash (32 octets):  ad 7f 35 b9 42 29 61 a5 31 91 f1 be 86 0e 47 19
      77 4f e9 ee c7 0e d5 3f 29 fa ec af b1 f2 9c 0b

   info (54 octets):  00 20 12 74 6c 73 31 33 20 63 20 61 70 20 74 72
      61 66 66 69 63 20 ad 7f 35 b9 42 29 61 a5 31 91 f1 be 86 0e 47
      19 77 4f e9 ee c7 0e d5 3f 29 fa ec af b1 f2 9c 0b
```

```
      output (32 octets):  4f c9 93 4a 78 39 af bf b1 ad 4a 09 f9 13 90
         aa 58 f8 16 40 60 8d 63 86 38 78 c0 b9 9f 6c da aa

   {server}  derive secret "tls13 s ap traffic":

      PRK (32 octets):  23 07 37 68 ca 09 44 ef de d6 a1 fd 17 3e 7a 1f
         a7 51 b2 1b 6b f2 07 66 1c b2 94 bc 29 f4 49 c7

      hash (32 octets):  ad 7f 35 b9 42 29 61 a5 31 91 f1 be 86 0e 47 19
         77 4f e9 ee c7 0e d5 3f 29 fa ec af b1 f2 9c 0b

      info (54 octets):  00 20 12 74 6c 73 31 33 20 73 20 61 70 20 74 72
         61 66 66 69 63 20 ad 7f 35 b9 42 29 61 a5 31 91 f1 be 86 0e 47
         19 77 4f e9 ee c7 0e d5 3f 29 fa ec af b1 f2 9c 0b

      output (32 octets):  71 9b 77 1c 5c 65 41 32 a7 25 1f 09 12 92 f7
         68 b6 d8 9f af 36 f3 1f 79 44 05 00 fc 16 68 b2 b7

   {server}  derive secret "tls13 exp master":

      PRK (32 octets):  23 07 37 68 ca 09 44 ef de d6 a1 fd 17 3e 7a 1f
         a7 51 b2 1b 6b f2 07 66 1c b2 94 bc 29 f4 49 c7

      hash (32 octets):  ad 7f 35 b9 42 29 61 a5 31 91 f1 be 86 0e 47 19
         77 4f e9 ee c7 0e d5 3f 29 fa ec af b1 f2 9c 0b

      info (52 octets):  00 20 10 74 6c 73 31 33 20 65 78 70 20 6d 61 73
         74 65 72 20 ad 7f 35 b9 42 29 61 a5 31 91 f1 be 86 0e 47 19 77
         4f e9 ee c7 0e d5 3f 29 fa ec af b1 f2 9c 0b

      output (32 octets):  9d 07 cc 4a ef bc c1 f1 75 81 54 ac 1a ba 78
         8b 0e d5 f3 1b bc 7f a4 ca dd ce 7a 09 7a 3e 25 42

   {client}  extract secret "early":

      salt:  (absent)

      ikm (32 octets):  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
         00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      secret (32 octets):  33 ad 0a 1c 60 7e c0 3b 09 e6 cd 98 93 68 0c
         e2 10 ad f3 00 aa 1f 26 60 e1 b2 2e 10 f1 70 f9 2a

   {client}  derive secret for handshake "tls13 derived":

      PRK (32 octets):  33 ad 0a 1c 60 7e c0 3b 09 e6 cd 98 93 68 0c e2
```

hash (32 octets): e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24
27 ae 41 e4 64 9b 93 4c a4 95 99 1b 78 52 b8 55

info (49 octets): 00 20 0d 74 6c 73 31 33 20 64 65 72 69 76 65 64
20 e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24 27 ae 41 e4
64 9b 93 4c a4 95 99 1b 78 52 b8 55

output (32 octets): 6f 26 15 a1 08 c7 02 c5 67 8f 54 fc 9d ba b6
97 16 c0 76 18 9c 48 25 0c eb ea c3 57 6c 36 11 ba

{client} extract secret "handshake":

salt (32 octets): 6f 26 15 a1 08 c7 02 c5 67 8f 54 fc 9d ba b6 97
16 c0 76 18 9c 48 25 0c eb ea c3 57 6c 36 11 ba

ikm (32 octets): 61 d3 4a ad f2 5e 22 3a 2c e6 fb 59 f8 a0 f9 d1
d7 5f 18 87 df b0 6c 0f ff f8 47 6d c3 c5 0f 47

secret (32 octets): 79 07 c2 82 34 f1 6c a8 71 a4 6b eb 25 da 54
7f dc 8a ab 96 d1 4e ef f8 0f 5b 12 f9 ad 8a c9 d6

{client} derive secret "tls13 c hs traffic" (same as server)

{client} derive secret "tls13 s hs traffic" (same as server)

{client} derive secret for master "tls13 derived" (same as server)

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

{client} calculate finished "tls13 finished" (same as server)

{client} derive secret "tls13 c ap traffic" (same as server)

{client} derive secret "tls13 s ap traffic" (same as server)

{client} derive secret "tls13 exp master" (same as server)

{client} calculate finished "tls13 finished":

```
      PRK (32 octets):  40 2b 60 6f 3c b0 c8 5b 6d bf fb fd a9 df 79 14
         58 4a 0e b9 21 1b b5 e9 0b a4 81 f2 5c 4b 94 e2

      hash (0 octets):  (empty)

      info (18 octets):  00 20 0e 74 6c 73 31 33 20 66 69 6e 69 73 68 65
         64 00
```



```
      output (32 octets):  47 af c3 66 da 4c 2d 41 64 19 fe c6 f7 af f1
         3c 58 9b 56 a2 6a da e0 b6 f3 7a 8d f5 2e a1 d9 33

   {client}  send a Finished handshake message

   {client}  send handshake record:

      payload (36 octets):  14 00 00 20 3a d4 3d b6 d0 42 77 0c 3f 79 f7
         a9 1a cc 0a 41 1f 1b 92 21 f0 3f 9d 2a 6b 92 c4 d1 54 51 19 ed

      ciphertext (58 octets):  17 03 03 00 35 32 d7 1d 7f 1b 8e f2 da f3
         58 4c 6c 09 c7 4a ed 85 6e 75 59 4e 6f 14 67 4c d9 48 f2 69 ab
         c1 cc 0e b7 bb 10 45 51 78 88 83 8f 51 34 75 a2 59 ef 80 9b 0f
         94 1f

   {client}  derive secret "tls13 res master":

      PRK (32 octets):  23 07 37 68 ca 09 44 ef de d6 a1 fd 17 3e 7a 1f
         a7 51 b2 1b 6b f2 07 66 1c b2 94 bc 29 f4 49 c7

      hash (32 octets):  2d eb 11 8e 31 f3 d3 8b 38 de 1f cc 26 46 d2 21
         ac e6 1f 97 fa 79 75 92 23 7a 65 9c 2b 6b 93 51

      info (52 octets):  00 20 10 74 6c 73 31 33 20 72 65 73 20 6d 61 73
         74 65 72 20 2d eb 11 8e 31 f3 d3 8b 38 de 1f cc 26 46 d2 21 ac
         e6 1f 97 fa 79 75 92 23 7a 65 9c 2b 6b 93 51

      output (32 octets):  ba dd 11 ad f0 7b 59 f9 d1 90 56 1e 4e 69 d6
         5d 2d 0c cc 92 3b 08 4a cd 70 6e 00 cd 54 e6 5b 70

   {server}  calculate finished "tls13 finished" (same as client)
```

{server} derive secret "tls13 res master" (same as client)

{server} generate resumption secret "tls13 resumption":

PRK (32 octets): ba dd 11 ad f0 7b 59 f9 d1 90 56 1e 4e 69 d6 5d
2d 0c cc 92 3b 08 4a cd 70 6e 00 cd 54 e6 5b 70

hash (2 octets): 00 00

info (22 octets): 00 20 10 74 6c 73 31 33 20 72 65 73 75 6d 70 74
69 6f 6e 02 00 00

output (32 octets): 20 b3 ed 07 48 14 86 03 09 cd 47 fb 81 0b 36
9c f1 86 b7 09 7c b7 76 ff 57 f8 a7 ce 12 18 fa fa

{server} send a NewSessionTicket handshake message

{server} send handshake record:

payload (205 octets): 04 00 00 c9 00 00 00 1e 1a 46 fe 8d 02 00
00 00 b2 f7 34 a8 af 18 42 36 ce f0 ae ea b1 00 00 00 00 68 2d
66 eb 29 13 c9 eb 94 c6 9a 57 51 5d df 2f 00 70 c2 f3 4f 9b 2e
d5 a5 30 91 16 c9 d7 4f ca eb 2b f8 87 51 9a a5 5a 7c 83 ff 27
fd c3 72 ba ec 38 7d be 58 8e d6 27 4b 1f f5 13 6c eb 68 ea 4a
39 ce 79 08 7c 6e 75 42 b4 9c 7c 0e 4b 97 fc 2a 29 73 27 71 8b
29 bf 63 6a dd 4e 6b 46 a4 1d f2 3f 45 01 28 80 20 b2 6c e5 75
d4 c9 f1 87 eb e5 48 07 1b 51 19 8c 4b 10 f9 4c f7 ce 94 aa 08
17 a7 2a a8 86 64 63 d9 d7 7f 9c db 81 e6 27 82 c1 33 2e 22 0c
55 2c dc 44 48 4b e7 ee f7 64 3d c3 8d 00 08 00 2a 00 04 00 00
04 00

ciphertext (227 octets): 17 03 03 00 de ce 84 1b 08 4c ba 5c 21
cd 70 f7 30 28 18 7c c9 a0 e9 e5 b8 88 f8 d0 ca 5a f7 7d df 96
eb cd fd 1e 70 c6 8b a2 44 a9 64 3d c8 c2 b3 9c 93 3d 0e a9 1a
8d 7a 35 df db 3d c3 45 57 bb eb e8 0c a4 0b 64 b8 45 cd 04 b2
18 2e 73 59 f5 53 60 0b 1b 1f 8a c1 29 fd 3c f5 eb 79 91 3a e4
27 02 a3 10 a7 17 5d e1 15 c7 fd 77 00 06 54 2d cf 8a 7a 94 53
8d 96 d9 71 72 02 28 4b ed af f5 ff ec a0 23 10 92 12 3e a6 b0
bc 12 99 ae c3 a9 8c 44 27 e4 35 7c 38 16 d0 a6 c5 d0 93 aa d5
9c 09 5c 99 76 91 b5 88 cc 3c 10 8e 95 d7 f8 39 f9 ec 2c a5 18
2c 80 53 12 a1 c2 d0 32 88 80 97 c1 4e 38 5a 3c c5 e9 37 0e b6
49 08 05 4b 52 64 4e 35 09 2a 34 4a 74 77 b8 bb be fb 22 a8 ff

```
      c3 9e 84 ac

{client}  generate resumption secret "tls13 resumption" (same as
   server)

{client}  send application_data record:

   payload (50 octets):  00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e
      0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23
      24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31

   ciphertext (72 octets):  17 03 03 00 43 18 8a fa 7b 29 8e 8d ef c3
      eb 5e f8 2f dc 60 92 3b b5 5c ca 31 a5 64 63 df ec 71 7a aa 99
      77 9c c6 1f bf ca 90 73 b9 95 51 73 a0 b7 1c 1b f2 b9 2d b0 60
      73 e9 65 5b 64 3e 12 ef 76 d8 c8 86 91 12 aa 35

{server}  send application_data record:

   payload (50 octets):  00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e
      0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23
      24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31
```



```
   ciphertext (72 octets):  17 03 03 00 43 d8 27 0a 4b 0b a6 c0 74 c3
      83 0b 15 58 a1 cb 89 13 e2 21 d7 08 33 ee 02 74 58 e2 46 11 a0
      d4 7f 9c d3 bd 66 ce 03 13 db 71 8e e4 d0 ef bc 3f 8a 4d 7e 35
      04 3c 46 48 40 d8 7d eb 66 b7 7d 40 df 36 aa 7d

{client}  send alert record:

   payload (2 octets):  01 00

   ciphertext (24 octets):  17 03 03 00 13 d5 92 9a 67 ba 50 4f 19 3a
      59 7d 3a ab 2d c3 f9 04 12 7d

{server}  send alert record:

   payload (2 octets):  01 00

   ciphertext (24 octets):  17 03 03 00 13 69 ed b3 40 6d 1e 57 51 97
      75 4a c9 27 19 e0 5d 71 18 67
```

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): 25 ee 23 7a 20 17 98 ee e8 7f 37 60 53 e1 28 50 9a be 65 e7 87 34 4f f2 b9 ff 9d 04 fd 13 8a fa

public key (32 octets): fa 5d e3 00 e6 9f 05 d6 19 a4 28 fc fb 02 88 b5 57 b6 40 6a 26 fc 51 13 c0 4e 4a 3c 86 9a 44 14

{client} extract secret "early":

salt: (absent)

ikm (32 octets): 20 b3 ed 07 48 14 86 03 09 cd 47 fb 81 0b 36 9c f1 86 b7 09 7c b7 76 ff 57 f8 a7 ce 12 18 fa fa

secret (32 octets): 35 10 b5 e7 47 ce ef 42 b1 fe ff e7 a7 4f dc 0f 52 a5 ee fc a2 b6 76 b0 82 4e 06 17 c8 64 56 16

{client} send a ClientHello handshake message

{client} calculate finished "tls13 finished":

PRK (32 octets): de 0c 49 be 25 cd 0a b1 79 a9 d1 be e0 5a c0 cc a0 3d 51 10 4f cc ac db 13 12 b6 35 40 5a db 2c

hash (0 octets): (empty)

info (18 octets): 00 20 0e 74 6c 73 31 33 20 66 69 6e 69 73 68 65 64 00

output (32 octets): e6 12 24 d1 ef b4 01 4b 18 aa e8 db 83 4e 12 5b da e8 e8 bf f1 17 2f a6 a8 8c 35 39 77 c6 5a 68

{client} send handshake record:

payload (512 octets): 01 00 01 fc 03 03 f4 74 90 c6 31 61 6b 80
01 47 e5 62 01 b1 13 6d b0 04 92 f7 e8 d9 56 2a 77 fb f9 77 1d
8a a4 6c 00 00 06 13 01 13 03 13 02 01 00 01 cd 00 00 00 0b 00
09 00 00 06 73 65 72 76 65 72 ff 01 00 01 00 00 0a 00 14 00 12
00 1d 00 17 00 18 00 19 01 00 01 01 01 02 01 03 01 04 00 28 00
26 00 24 00 1d 00 20 fa 5d e3 00 e6 9f 05 d6 19 a4 28 fc fb 02
88 b5 57 b6 40 6a 26 fc 51 13 c0 4e 4a 3c 86 9a 44 14 00 2a 00
00 00 2b 00 03 02 7f 16 00 0d 00 20 00 1e 04 03 05 03 06 03 02
03 08 04 08 05 08 06 04 01 05 01 06 01 02 01 04 02 05 02 06 02
02 02 00 2d 00 02 01 01 00 15 00 5d 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 29 00 dd 00 b8 00 b2 f7 34 a8 af 18 42 36 ce f0 ae ea b1 00
00 00 00 68 2d 66 eb 29 13 c9 eb 94 c6 9a 57 51 5d df 2f 00 70
c2 f3 4f 9b 2e d5 a5 30 91 16 c9 d7 4f ca eb 2b f8 87 51 9a a5
5a 7c 83 ff 27 fd c3 72 ba ec 38 7d be 58 8e d6 27 4b 1f f5 13
6c eb 68 ea 4a 39 ce 79 08 7c 6e 75 42 b4 9c 7c 0e 4b 97 fc 2a
29 73 27 71 8b 29 bf 63 6a dd 4e 6b 46 a4 1d f2 3f 45 01 28 80
20 b2 6c e5 75 d4 c9 f1 87 eb e5 48 07 1b 51 19 8c 4b 10 f9 4c
f7 ce 94 aa 08 17 a7 2a a8 86 64 63 d9 d7 7f 9c db 81 e6 27 82
c1 33 2e 22 0c 55 2c dc 44 48 4b e7 ee f7 64 3d c3 8d 1a 46 fe
90 00 21 20 34 60 d2 6b d5 55 86 97 91 90 dd 6d 8f 25 3d f3 fa
d7 d1 64 61 28 f3 d9 3d 51 57 21 3b 90 86 b3

ciphertext (517 octets): 16 03 01 02 00 01 00 01 fc 03 03 f4 74
90 c6 31 61 6b 80 01 47 e5 62 01 b1 13 6d b0 04 92 f7 e8 d9 56
2a 77 fb f9 77 1d 8a a4 6c 00 00 06 13 01 13 03 13 02 01 00 01
cd 00 00 00 0b 00 09 00 00 06 73 65 72 76 65 72 ff 01 00 01 00
00 0a 00 14 00 12 00 1d 00 17 00 18 00 19 01 00 01 01 01 02 01
03 01 04 00 28 00 26 00 24 00 1d 00 20 fa 5d e3 00 e6 9f 05 d6
19 a4 28 fc fb 02 88 b5 57 b6 40 6a 26 fc 51 13 c0 4e 4a 3c 86
9a 44 14 00 2a 00 00 00 2b 00 03 02 7f 16 00 0d 00 20 00 1e 04
03 05 03 06 03 02 03 08 04 08 05 08 06 04 01 05 01 06 01 02 01

04 02 05 02 06 02 02 02 00 2d 00 02 01 01 00 15 00 5d 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 29 00 dd 00 b8 00 b2 f7 34 a8 af 18 42 36
      ce f0 ae ea b1 00 00 00 00 68 2d 66 eb 29 13 c9 eb 94 c6 9a 57
      51 5d df 2f 00 70 c2 f3 4f 9b 2e d5 a5 30 91 16 c9 d7 4f ca eb
      2b f8 87 51 9a a5 5a 7c 83 ff 27 fd c3 72 ba ec 38 7d be 58 8e
      d6 27 4b 1f f5 13 6c eb 68 ea 4a 39 ce 79 08 7c 6e 75 42 b4 9c
      7c 0e 4b 97 fc 2a 29 73 27 71 8b 29 bf 63 6a dd 4e 6b 46 a4 1d
      f2 3f 45 01 28 80 20 b2 6c e5 75 d4 c9 f1 87 eb e5 48 07 1b 51
      19 8c 4b 10 f9 4c f7 ce 94 aa 08 17 a7 2a a8 86 64 63 d9 d7 7f
      9c db 81 e6 27 82 c1 33 2e 22 0c 55 2c dc 44 48 4b e7 ee f7 64
      3d c3 8d 1a 46 fe 90 00 21 20 34 60 d2 6b d5 55 86 97 91 90 dd
      6d 8f 25 3d f3 fa d7 d1 64 61 28 f3 d9 3d 51 57 21 3b 90 86 b3

{client}  derive secret "tls13 c e traffic":

   PRK (32 octets):  35 10 b5 e7 47 ce ef 42 b1 fe ff e7 a7 4f dc 0f
      52 a5 ee fc a2 b6 76 b0 82 4e 06 17 c8 64 56 16

   hash (32 octets):  89 4e e7 2f 01 a8 67 e9 cc 87 5a 19 44 22 10 8a
      e9 51 45 f9 43 b0 89 1f 3c ab 07 4f 12 fa c4 0a

   info (53 octets):  00 20 11 74 6c 73 31 33 20 63 20 65 20 74 72 61
      66 66 69 63 20 89 4e e7 2f 01 a8 67 e9 cc 87 5a 19 44 22 10 8a
      e9 51 45 f9 43 b0 89 1f 3c ab 07 4f 12 fa c4 0a

   output (32 octets):  7b dd 21 10 35 33 b9 d8 2b ae 6c 26 be 3e 78
      e9 bd 37 91 42 96 24 db e0 a6 b3 9c e5 bf 69 eb 23

{client}  derive secret "tls13 e exp master":

   PRK (32 octets):  35 10 b5 e7 47 ce ef 42 b1 fe ff e7 a7 4f dc 0f
      52 a5 ee fc a2 b6 76 b0 82 4e 06 17 c8 64 56 16

   hash (32 octets):  89 4e e7 2f 01 a8 67 e9 cc 87 5a 19 44 22 10 8a
      e9 51 45 f9 43 b0 89 1f 3c ab 07 4f 12 fa c4 0a

   info (54 octets):  00 20 12 74 6c 73 31 33 20 65 20 65 78 70 20 6d
      61 73 74 65 72 20 89 4e e7 2f 01 a8 67 e9 cc 87 5a 19 44 22 10
      8a e9 51 45 f9 43 b0 89 1f 3c ab 07 4f 12 fa c4 0a

   output (32 octets):  da 05 9b c4 d7 bd 6e 30 45 b3 df d8 ab c8 68
      1b 22 47 6f 44 b4 54 22 75 12 af a9 af c0 60 3f c1

{client}  send application_data record:
```

payload (6 octets): 41 42 43 44 45 46

ciphertext (28 octets): 17 03 03 00 17 d8 3a 80 c1 65 49 bf 19 49 38 a3 9c c1 54 a1 8b a7 cb bb a7 bf 02 e0

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

{server} calculate finished "tls13 finished" (same as client)

{server} create an ephemeral x25519 key pair:

private key (32 octets): a3 41 34 2b 44 be 43 fa 13 b5 a2 fa 30 6a d7 24 ef 7f 73 a0 87 ac be 4a 79 10 82 b6 00 cd 08 b5

public key (32 octets): 66 62 56 0e 42 6c b1 13 d5 63 b1 69 e9 72 b5 c4 81 dd b6 cc f2 a5 79 39 ed d2 4b a9 e9 b6 2f 5f

{server} derive secret "tls13 c e traffic" (same as client)

{server} derive secret "tls13 e exp master" (same as client)

{server} send a ServerHello handshake message

{server} derive secret for handshake "tls13 derived":

PRK (32 octets): 35 10 b5 e7 47 ce ef 42 b1 fe ff e7 a7 4f dc 0f 52 a5 ee fc a2 b6 76 b0 82 4e 06 17 c8 64 56 16

hash (32 octets): e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24 27 ae 41 e4 64 9b 93 4c a4 95 99 1b 78 52 b8 55

info (49 octets): 00 20 0d 74 6c 73 31 33 20 64 65 72 69 76 65 64 20 e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24 27 ae 41 e4 64 9b 93 4c a4 95 99 1b 78 52 b8 55

output (32 octets): 3c 5b 59 45 89 ee 0f a2 f1 18 d3 98 fc 3c 3e 50 f7 13 21 65 bc 5e 20 1a 97 da df 8e 36 ad 16 ba

{server} extract secret "handshake":

salt (32 octets): 3c 5b 59 45 89 ee 0f a2 f1 18 d3 98 fc 3c 3e 50 f7 13 21 65 bc 5e 20 1a 97 da df 8e 36 ad 16 ba

ikm (32 octets): ca 49 06 0d 44 b4 58 b8 e2 6f b7 2a 18 6e bc 44 6b a8 e4 0e 8f b1 39 5c c7 f7 56 59 ee 86 f8 54

secret (32 octets): 6b a5 c1 83 92 4b a3 2c e0 99 85 c9 11 f2 97

```
bb 0a 7c de 27 63 1a 6f 2e e8 88 25 19 88 f3 07 54
```


{server} derive secret "tls13 c hs traffic":

PRK (32 octets): 6b a5 c1 83 92 4b a3 2c e0 99 85 c9 11 f2 97 bb
0a 7c de 27 63 1a 6f 2e e8 88 25 19 88 f3 07 54

hash (32 octets): ef 88 42 5a 0d c1 df 66 77 f6 2d de 3e 93 79 b6
39 83 b3 a0 89 66 db aa d7 d4 c9 c6 b1 79 b3 b7

info (54 octets): 00 20 12 74 6c 73 31 33 20 63 20 68 73 20 74 72
61 66 66 69 63 20 ef 88 42 5a 0d c1 df 66 77 f6 2d de 3e 93 79
b6 39 83 b3 a0 89 66 db aa d7 d4 c9 c6 b1 79 b3 b7

output (32 octets): a2 ba 52 84 b4 0e 7d 65 af af 93 c0 93 06 dd
e4 70 98 a4 ee 28 4c f4 6e 0b 59 09 fe 25 8c a6 4f

{server} derive secret "tls13 s hs traffic":

PRK (32 octets): 6b a5 c1 83 92 4b a3 2c e0 99 85 c9 11 f2 97 bb
0a 7c de 27 63 1a 6f 2e e8 88 25 19 88 f3 07 54

hash (32 octets): ef 88 42 5a 0d c1 df 66 77 f6 2d de 3e 93 79 b6
39 83 b3 a0 89 66 db aa d7 d4 c9 c6 b1 79 b3 b7

info (54 octets): 00 20 12 74 6c 73 31 33 20 73 20 68 73 20 74 72
61 66 66 69 63 20 ef 88 42 5a 0d c1 df 66 77 f6 2d de 3e 93 79
b6 39 83 b3 a0 89 66 db aa d7 d4 c9 c6 b1 79 b3 b7

output (32 octets): 58 6f 1a b9 cb 2d 93 70 66 1a 1e 0b c9 fc 8c
39 1a 34 67 b9 9e bd 58 16 c1 8c 46 a5 28 6e 96 77

{server} derive secret for master "tls13 derived":

PRK (32 octets): 6b a5 c1 83 92 4b a3 2c e0 99 85 c9 11 f2 97 bb
0a 7c de 27 63 1a 6f 2e e8 88 25 19 88 f3 07 54

hash (32 octets): e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24
27 ae 41 e4 64 9b 93 4c a4 95 99 1b 78 52 b8 55

info (49 octets): 00 20 0d 74 6c 73 31 33 20 64 65 72 69 76 65 64
20 e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24 27 ae 41 e4

```
      64 9b 93 4c a4 95 99 1b 78 52 b8 55

   output (32 octets):  78 31 58 10 11 a6 70 a2 ce 59 0b 80 b8 e5 44
      12 35 49 d6 bd 44 3c f6 9e 80 e8 0a 7e 38 93 d7 7e

{server}  extract secret "master":
```



```
   salt (32 octets):  78 31 58 10 11 a6 70 a2 ce 59 0b 80 b8 e5 44 12
      35 49 d6 bd 44 3c f6 9e 80 e8 0a 7e 38 93 d7 7e

   ikm (32 octets):  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

   secret (32 octets):  6b 06 1b 95 b3 81 1d 3a 8a a8 3d a0 1d f0 e6
      d5 c3 be 43 d8 3b 18 b3 bc b8 e8 52 78 14 2b 11 9c

{server}  send handshake record:

   payload (96 octets):  02 00 00 5c 03 03 4b 98 9e 4c 47 ca 09 2a 18
      78 78 ae 45 7f d5 85 6e dc a0 f7 ae cf 00 4e d0 20 3a fe 0d 57
      e3 86 00 13 01 00 00 34 00 29 00 02 00 00 00 28 00 24 00 1d 00
      20 66 62 56 0e 42 6c b1 13 d5 63 b1 69 e9 72 b5 c4 81 dd b6 cc
      f2 a5 79 39 ed d2 4b a9 e9 b6 2f 5f 00 2b 00 02 7f 16

   ciphertext (101 octets):  16 03 03 00 60 02 00 00 5c 03 03 4b 98
      9e 4c 47 ca 09 2a 18 78 78 ae 45 7f d5 85 6e dc a0 f7 ae cf 00
      4e d0 20 3a fe 0d 57 e3 86 00 13 01 00 00 34 00 29 00 02 00 00
      00 28 00 24 00 1d 00 20 66 62 56 0e 42 6c b1 13 d5 63 b1 69 e9
      72 b5 c4 81 dd b6 cc f2 a5 79 39 ed d2 4b a9 e9 b6 2f 5f 00 2b
      00 02 7f 16

{server}  send a EncryptedExtensions handshake message

{server}  calculate finished "tls13 finished":

   PRK (32 octets):  58 6f 1a b9 cb 2d 93 70 66 1a 1e 0b c9 fc 8c 39
      1a 34 67 b9 9e bd 58 16 c1 8c 46 a5 28 6e 96 77

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

```
   info (18 octets):  00 20 0e 74 6c 73 31 33 20 66 69 6e 69 73 68 65
      64 00

   output (32 octets):  98 90 9d e6 86 66 b5 12 80 1c 41 c6 3b 20 f9
      fc 1f 7f 8f e1 19 64 75 d2 07 48 66 e3 a1 5d 14 15

{server}  send a Finished handshake message

{server}  send handshake record:

   payload (74 octets):  08 00 00 22 00 20 00 0a 00 14 00 12 00 1d 00
      17 00 18 00 19 01 00 01 01 01 02 01 03 01 04 00 00 00 00 00 2a
      00 00 14 00 00 20 c9 f5 11 e0 94 08 c2 b3 ff b5 ac 45 3c 7c 0a
      65 c0 8c 28 c9 bc 4f 38 54 46 91 9e b8 fd 84 7c e0
```



```
   ciphertext (96 octets):  17 03 03 00 5b f5 a6 a6 20 f2 db 4e 20 1f
      22 8d 73 b4 15 d8 5e a9 76 e1 55 27 5f 2d 89 a4 96 68 d7 be 48
      9a 8b 85 20 5d 0b 59 30 79 e6 0e 10 6e 15 67 29 c2 11 90 0a de
      1f 72 32 67 d8 c8 2b f5 dd 40 bb c5 63 99 1e bc 01 1e 49 14 ea
      3a ee 25 37 3e eb 31 00 36 c8 f4 44 be 45 16 4d 3a 50 5d

{server}  derive secret "tls13 c ap traffic":

   PRK (32 octets):  6b 06 1b 95 b3 81 1d 3a 8a a8 3d a0 1d f0 e6 d5
      c3 be 43 d8 3b 18 b3 bc b8 e8 52 78 14 2b 11 9c

   hash (32 octets):  bc be 0c 61 2f 39 63 e4 2c 49 6c b3 03 e9 59 89
      ba 96 f6 21 00 34 f4 63 05 b9 75 2a 53 d9 a7 dd

   info (54 octets):  00 20 12 74 6c 73 31 33 20 63 20 61 70 20 74 72
      61 66 66 69 63 20 bc be 0c 61 2f 39 63 e4 2c 49 6c b3 03 e9 59
      89 ba 96 f6 21 00 34 f4 63 05 b9 75 2a 53 d9 a7 dd

   output (32 octets):  c9 d1 12 6d be c2 7c a1 72 21 37 3f ef 10 4e
      cf a0 6d c4 a1 c4 5c 1d 55 3f 2b 1a 84 16 b4 6e cb

{server}  derive secret "tls13 s ap traffic":

   PRK (32 octets):  6b 06 1b 95 b3 81 1d 3a 8a a8 3d a0 1d f0 e6 d5
      c3 be 43 d8 3b 18 b3 bc b8 e8 52 78 14 2b 11 9c
```

```
   hash (32 octets):  bc be 0c 61 2f 39 63 e4 2c 49 6c b3 03 e9 59 89
      ba 96 f6 21 00 34 f4 63 05 b9 75 2a 53 d9 a7 dd

   info (54 octets):  00 20 12 74 6c 73 31 33 20 73 20 61 70 20 74 72
      61 66 66 69 63 20 bc be 0c 61 2f 39 63 e4 2c 49 6c b3 03 e9 59
      89 ba 96 f6 21 00 34 f4 63 05 b9 75 2a 53 d9 a7 dd

   output (32 octets):  aa 91 af 99 99 34 3a 32 8e cf ad 72 cb be e1
      20 71 d7 79 b3 8a 3d 18 5a 7d c7 c4 e7 f8 33 33 1c

{server}  derive secret "tls13 exp master":

   PRK (32 octets):  6b 06 1b 95 b3 81 1d 3a 8a a8 3d a0 1d f0 e6 d5
      c3 be 43 d8 3b 18 b3 bc b8 e8 52 78 14 2b 11 9c

   hash (32 octets):  bc be 0c 61 2f 39 63 e4 2c 49 6c b3 03 e9 59 89
      ba 96 f6 21 00 34 f4 63 05 b9 75 2a 53 d9 a7 dd

   info (52 octets):  00 20 10 74 6c 73 31 33 20 65 78 70 20 6d 61 73
      74 65 72 20 bc be 0c 61 2f 39 63 e4 2c 49 6c b3 03 e9 59 89 ba
      96 f6 21 00 34 f4 63 05 b9 75 2a 53 d9 a7 dd
```



```
   output (32 octets):  3d 65 4f f5 ca 07 87 85 69 31 01 cc 71 0f 46
      e2 93 5b 5e c4 61 14 ca bb 08 35 41 a0 84 66 d1 84

{client}  derive secret for handshake "tls13 derived":

   PRK (32 octets):  35 10 b5 e7 47 ce ef 42 b1 fe ff e7 a7 4f dc 0f
      52 a5 ee fc a2 b6 76 b0 82 4e 06 17 c8 64 56 16

   hash (32 octets):  e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24
      27 ae 41 e4 64 9b 93 4c a4 95 99 1b 78 52 b8 55

   info (49 octets):  00 20 0d 74 6c 73 31 33 20 64 65 72 69 76 65 64
      20 e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24 27 ae 41 e4
      64 9b 93 4c a4 95 99 1b 78 52 b8 55

   output (32 octets):  3c 5b 59 45 89 ee 0f a2 f1 18 d3 98 fc 3c 3e
      50 f7 13 21 65 bc 5e 20 1a 97 da df 8e 36 ad 16 ba

{client}  extract secret "handshake":
```

salt (32 octets): 3c 5b 59 45 89 ee 0f a2 f1 18 d3 98 fc 3c 3e 50
f7 13 21 65 bc 5e 20 1a 97 da df 8e 36 ad 16 ba

ikm (32 octets): ca 49 06 0d 44 b4 58 b8 e2 6f b7 2a 18 6e bc 44
6b a8 e4 0e 8f b1 39 5c c7 f7 56 59 ee 86 f8 54

secret (32 octets): 6b a5 c1 83 92 4b a3 2c e0 99 85 c9 11 f2 97
bb 0a 7c de 27 63 1a 6f 2e e8 88 25 19 88 f3 07 54

{client} derive secret "tls13 c hs traffic" (same as server)

{client} derive secret "tls13 s hs traffic" (same as server)

{client} derive secret for master "tls13 derived" (same as server)

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

{client} calculate finished "tls13 finished" (same as server)

{client} derive secret "tls13 c ap traffic" (same as server)

{client} derive secret "tls13 s ap traffic" (same as server)

{client} derive secret "tls13 exp master" (same as server)

{client} send a EndOfEarlyData handshake message

{client} send handshake record:

payload (4 octets): 05 00 00 00

ciphertext (26 octets): 17 03 03 00 15 1d ee d3 9b 27 ff 4f 3c 92
2f fd ef 73 89 56 5e cc 79 d1 13 71

{client} calculate finished "tls13 finished":

PRK (32 octets): a2 ba 52 84 b4 0e 7d 65 af af 93 c0 93 06 dd e4
70 98 a4 ee 28 4c f4 6e 0b 59 09 fe 25 8c a6 4f

hash (0 octets): (empty)

```
   info (18 octets):  00 20 0e 74 6c 73 31 33 20 66 69 6e 69 73 68 65
      64 00

   output (32 octets):  67 02 97 87 4f 08 e5 10 32 72 a8 be 0c 6d c3
      b4 39 6e 82 28 34 62 6b 21 e6 be 28 b9 d4 b4 35 05

{client}  send a Finished handshake message

{client}  send handshake record:

   payload (36 octets):  14 00 00 20 60 c3 2e 99 5e c1 0d d0 1d 73 79
      e3 eb f1 9f 75 ef 74 0b 18 d4 24 06 c9 62 db 37 a4 53 74 9d 76

   ciphertext (58 octets):  17 03 03 00 35 b1 a4 2d de c8 7d 6a 62 17
      a5 53 19 3b 47 a6 6c 32 b4 51 ab f8 48 dc df 68 21 3b 44 21 76
      a9 e5 9b 8e cf 5e 1a fe d8 94 43 9a 9d f0 c3 a2 4b da ac 97 fc
      34 55

{client}  derive secret "tls13 res master":

   PRK (32 octets):  6b 06 1b 95 b3 81 1d 3a 8a a8 3d a0 1d f0 e6 d5
      c3 be 43 d8 3b 18 b3 bc b8 e8 52 78 14 2b 11 9c

   hash (32 octets):  04 5f 9f 6c d4 c6 84 65 a7 79 f4 89 b7 13 57 7f
      42 e9 91 c1 b7 b7 34 db 01 28 a5 7b 88 35 41 27

   info (52 octets):  00 20 10 74 6c 73 31 33 20 72 65 73 20 6d 61 73
      74 65 72 20 04 5f 9f 6c d4 c6 84 65 a7 79 f4 89 b7 13 57 7f 42
      e9 91 c1 b7 b7 34 db 01 28 a5 7b 88 35 41 27

   output (32 octets):  40 7b 7c fa 1a 5d cd 73 e2 75 a6 80 13 16 68
      24 4e a8 88 64 19 a6 fe cc 01 f5 7b df d5 5d 15 2a

{server}  calculate finished "tls13 finished" (same as client)

{server}  derive secret "tls13 res master" (same as client)
```



```
{client}  send application_data record:

   payload (50 octets):  00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e
      0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23
      24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31
```

ciphertext (72 octets): 17 03 03 00 43 89 8d 41 41 71 76 9c 87 23
f5 46 43 1e c6 80 49 5a fa a6 ac 32 5d 66 2f a5 9d 93 5a 99 d2
f5 94 63 b8 d9 cd d3 c1 b1 36 79 08 1d d0 98 7c 4d 26 40 9a bd
40 ca d0 be a6 d5 95 85 01 b1 fc 02 15 08 6d b9

{server} send application_data record:

payload (50 octets): 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e
0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23
24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31

ciphertext (72 octets): 17 03 03 00 43 8e 95 04 14 52 07 ad 99 f9
26 b4 7c 28 f6 0f a5 31 b9 7d 35 4f 55 ac fe 46 59 b0 37 f1 94
6e 6a 8d c8 da f7 a9 fc 36 27 02 3f c1 df 0b a1 8c a5 90 11 fc
2f 39 96 ea bc 2f 6d 50 85 93 d6 0b 23 87 d4 bc

{client} send alert record:

payload (2 octets): 01 00

ciphertext (24 octets): 17 03 03 00 13 e4 f4 3b 1b 15 b0 75 40 6c
2f 32 68 61 99 82 35 6d 78 53

{server} send alert record:

payload (2 octets): 01 00

ciphertext (24 octets): 17 03 03 00 13 06 18 b6 94 51 58 6b 0d b9
6c 39 08 0f 6b d7 d1 f1 0b 41

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): 52 99 b5 dc 31 26 3d a4 eb 70 79 f3 f9
29 68 d5 1e ce c2 0c 3b aa 64 67 f2 d8 d2 c2 49 88 09 10

```
   public key (32 octets):  9e d2 81 f2 d1 e0 f8 c3 99 a4 90 a8 6a cd
      71 9d 46 56 77 db dc b4 45 1f 97 39 e1 22 40 8a d4 32

{client}  send a ClientHello handshake message

{client}  send handshake record:

   payload (174 octets):  01 00 00 aa 03 03 24 cc 22 ad 4c 8b 8c ed
      c8 e7 ee ac 95 93 1b 24 9d 3a dd 7d 98 c5 e0 d8 35 f5 d7 81 0d
      fb b1 80 00 00 06 13 01 13 03 13 02 01 00 00 7b 00 00 00 0b 00
      09 00 00 06 73 65 72 76 65 72 ff 01 00 01 00 00 0a 00 08 00 06
      00 1d 00 17 00 18 00 28 00 26 00 24 00 1d 00 20 9e d2 81 f2 d1
      e0 f8 c3 99 a4 90 a8 6a cd 71 9d 46 56 77 db dc b4 45 1f 97 39
      e1 22 40 8a d4 32 00 2b 00 03 02 7f 16 00 0d 00 20 00 1e 04 03
      05 03 06 03 02 03 08 04 08 05 08 06 04 01 05 01 06 01 02 01 04
      02 05 02 06 02 02 02 00 2d 00 02 01 01

   ciphertext (179 octets):  16 03 01 00 ae 01 00 00 aa 03 03 24 cc
      22 ad 4c 8b 8c ed c8 e7 ee ac 95 93 1b 24 9d 3a dd 7d 98 c5 e0
      d8 35 f5 d7 81 0d fb b1 80 00 00 06 13 01 13 03 13 02 01 00 00
      7b 00 00 00 0b 00 09 00 00 06 73 65 72 76 65 72 ff 01 00 01 00
      00 0a 00 08 00 06 00 1d 00 17 00 18 00 28 00 26 00 24 00 1d 00
      20 9e d2 81 f2 d1 e0 f8 c3 99 a4 90 a8 6a cd 71 9d 46 56 77 db
      dc b4 45 1f 97 39 e1 22 40 8a d4 32 00 2b 00 03 02 7f 16 00 0d
      00 20 00 1e 04 03 05 03 06 03 02 03 08 04 08 05 08 06 04 01 05
      01 06 01 02 01 04 02 05 02 06 02 02 02 00 2d 00 02 01 01

{server}  send a ServerHello handshake message

{server}  send handshake record:

   payload (176 octets):  02 00 00 ac 03 03 cf 21 ad 74 e5 9a 61 11
      be 1d 8c 02 1e 65 b8 91 c2 a2 11 16 7a bb 8c 5e 07 9e 09 e2 c8
      a8 33 9c 00 13 01 00 00 84 00 28 00 02 00 17 00 2c 00 74 00 72
      3c c7 0f 98 68 ee 6d bc bb 7b 7c 21 00 00 00 00 73 d2 77 2a 29
      c9 93 b4 e0 c3 78 de 45 9e 99 ea 00 30 97 19 7d a5 86 38 74 31
      85 03 d3 dd e2 41 7d 5f b7 8c 92 76 13 14 10 ea a9 2e 9e 8a f5
      4e a0 92 86 7b 67 7d 64 4f 96 d8 c5 fd 48 30 d1 70 dd 1b 3f 8a
      85 17 ab ee 19 60 52 d8 e4 29 3d 62 f0 3b 6d 29 b6 88 4b 7c 00
      cc 5e 6c e7 ac 36 47 0e a7 00 2b 00 02 7f 16

   ciphertext (181 octets):  16 03 03 00 b0 02 00 00 ac 03 03 cf 21
      ad 74 e5 9a 61 11 be 1d 8c 02 1e 65 b8 91 c2 a2 11 16 7a bb 8c
      5e 07 9e 09 e2 c8 a8 33 9c 00 13 01 00 00 84 00 28 00 02 00 17
      00 2c 00 74 00 72 3c c7 0f 98 68 ee 6d bc bb 7b 7c 21 00 00 00
      00 73 d2 77 2a 29 c9 93 b4 e0 c3 78 de 45 9e 99 ea 00 30 97 19
      7d a5 86 38 74 31 85 03 d3 dd e2 41 7d 5f b7 8c 92 76 13 14 10
      ea a9 2e 9e 8a f5 4e a0 92 86 7b 67 7d 64 4f 96 d8 c5 fd 48 30
```

```
      d1 70 dd 1b 3f 8a 85 17 ab ee 19 60 52 d8 e4 29 3d 62 f0 3b 6d
      29 b6 88 4b 7c 00 cc 5e 6c e7 ac 36 47 0e a7 00 2b 00 02 7f 16
```

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

```
   private key (32 octets):  e5 d7 d7 16 54 b7 0d 85 b7 ef f8 ff 9f
      b4 10 f8 cc 6d 5c 0d 46 cb 4f 3c 96 28 61 c5 20 88 5d e0

   public key (65 octets):  04 17 35 66 97 92 26 4a 94 82 cf 17 8e 99
      0a e8 49 a3 55 2f 71 ec b8 4c 7b 02 2b 84 f0 57 eb b9 03 a2 e7
      ad 9d 2f 7d 44 e3 59 1a d0 04 33 a6 b2 d8 6d 57 9a af 1b 6a 2b
      01 72 df 0e 6e 00 08 7a bb
```

{client} send a ClientHello handshake message

{client} send handshake record:

```
   payload (512 octets):  01 00 01 fc 03 03 24 cc 22 ad 4c 8b 8c ed
      c8 e7 ee ac 95 93 1b 24 9d 3a dd 7d 98 c5 e0 d8 35 f5 d7 81 0d
      fb b1 80 00 00 06 13 01 13 03 13 02 01 00 01 cd 00 00 00 0b 00
      09 00 00 06 73 65 72 76 65 72 ff 01 00 01 00 00 0a 00 08 00 06
      00 1d 00 17 00 18 00 28 00 47 00 45 00 17 00 41 04 17 35 66 97
      92 26 4a 94 82 cf 17 8e 99 0a e8 49 a3 55 2f 71 ec b8 4c 7b 02
      2b 84 f0 57 eb b9 03 a2 e7 ad 9d 2f 7d 44 e3 59 1a d0 04 33 a6
      b2 d8 6d 57 9a af 1b 6a 2b 01 72 df 0e 6e 00 08 7a bb 00 2b 00
      03 02 7f 16 00 0d 00 20 00 1e 04 03 05 03 06 03 02 03 08 04 08
      05 08 06 04 01 05 01 06 01 02 01 04 02 05 02 06 02 02 02 00 2c
      00 74 00 72 3c c7 0f 98 68 ee 6d bc bb 7b 7c 21 00 00 00 00 73
      d2 77 2a 29 c9 93 b4 e0 c3 78 de 45 9e 99 ea 00 30 97 19 7d a5
      86 38 74 31 85 03 d3 dd e2 41 7d 5f b7 8c 92 76 13 14 10 ea a9
      2e 9e 8a f5 4e a0 92 86 7b 67 7d 64 4f 96 d8 c5 fd 48 30 d1 70
      dd 1b 3f 8a 85 17 ab ee 19 60 52 d8 e4 29 3d 62 f0 3b 6d 29 b6
      88 4b 7c 00 cc 5e 6c e7 ac 36 47 0e a7 00 2d 00 02 01 01 00 15
      00 b5 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
      ciphertext (517 octets):  16 03 03 02 00 01 00 01 fc 03 03 24 cc
         22 ad 4c 8b 8c ed c8 e7 ee ac 95 93 1b 24 9d 3a dd 7d 98 c5 e0
         d8 35 f5 d7 81 0d fb b1 80 00 00 06 13 01 13 03 13 02 01 00 01
         cd 00 00 00 0b 00 09 00 00 06 73 65 72 76 65 72 ff 01 00 01 00
         00 0a 00 08 00 06 00 1d 00 17 00 18 00 28 00 47 00 45 00 17 00
```

```
         41 04 17 35 66 97 92 26 4a 94 82 cf 17 8e 99 0a e8 49 a3 55 2f
         71 ec b8 4c 7b 02 2b 84 f0 57 eb b9 03 a2 e7 ad 9d 2f 7d 44 e3
         59 1a d0 04 33 a6 b2 d8 6d 57 9a af 1b 6a 2b 01 72 df 0e 6e 00
         08 7a bb 00 2b 00 03 02 7f 16 00 0d 00 20 00 1e 04 03 05 03 06
         03 02 03 08 04 08 05 08 06 04 01 05 01 06 01 02 01 04 02 05 02
         06 02 02 02 00 2c 00 74 00 72 3c c7 0f 98 68 ee 6d bc bb 7b 7c
         21 00 00 00 00 73 d2 77 2a 29 c9 93 b4 e0 c3 78 de 45 9e 99 ea
         00 30 97 19 7d a5 86 38 74 31 85 03 d3 dd e2 41 7d 5f b7 8c 92
         76 13 14 10 ea a9 2e 9e 8a f5 4e a0 92 86 7b 67 7d 64 4f 96 d8
         c5 fd 48 30 d1 70 dd 1b 3f 8a 85 17 ab ee 19 60 52 d8 e4 29 3d
         62 f0 3b 6d 29 b6 88 4b 7c 00 cc 5e 6c e7 ac 36 47 0e a7 00 2d
         00 02 01 01 00 15 00 b5 00 00 00 00 00 00 00 00 00 00 00 00 00
         00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
         00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
         00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
         00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
         00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
         00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
         00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
         00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

   {server}  extract secret "early":

      salt:  (absent)

      ikm (32 octets):  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
         00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      secret (32 octets):  33 ad 0a 1c 60 7e c0 3b 09 e6 cd 98 93 68 0c
         e2 10 ad f3 00 aa 1f 26 60 e1 b2 2e 10 f1 70 f9 2a

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

      private key (32 octets):  b1 6d 06 d1 40 ff d5 a9 3b b1 bf 4d 58
         d7 3d 97 06 62 b9 a5 50 25 ca 63 bc b1 b4 f6 75 ac 73 15
```

```
   public key (65 octets):  04 89 cf b4 c1 91 61 f7 0e b1 5a 43 81 40
      02 13 53 46 37 bd b4 fe d0 20 a9 2e 59 d9 58 10 ff eb e3 a8 dd
      bd f2 e2 cc 65 71 fe 17 df 28 3a 37 22 f1 23 f3 32 fc b0 cb 3d
      8b bb 9f 0b 65 e0 07 46 ae

{server}  send a ServerHello handshake message

{server}  derive secret for handshake "tls13 derived":

   PRK (32 octets):  33 ad 0a 1c 60 7e c0 3b 09 e6 cd 98 93 68 0c e2
      10 ad f3 00 aa 1f 26 60 e1 b2 2e 10 f1 70 f9 2a
```



```
   hash (32 octets):  e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24
      27 ae 41 e4 64 9b 93 4c a4 95 99 1b 78 52 b8 55

   info (49 octets):  00 20 0d 74 6c 73 31 33 20 64 65 72 69 76 65 64
      20 e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24 27 ae 41 e4
      64 9b 93 4c a4 95 99 1b 78 52 b8 55

   output (32 octets):  6f 26 15 a1 08 c7 02 c5 67 8f 54 fc 9d ba b6
      97 16 c0 76 18 9c 48 25 0c eb ea c3 57 6c 36 11 ba

{server}  extract secret "handshake":

   salt (32 octets):  6f 26 15 a1 08 c7 02 c5 67 8f 54 fc 9d ba b6 97
      16 c0 76 18 9c 48 25 0c eb ea c3 57 6c 36 11 ba

   ikm (32 octets):  ba 1c d6 f8 aa 98 a2 de ff b7 ba bb 8e 52 4d 2f
      d3 e8 2d 5c ff 5d 7b e3 0a 20 80 ef 62 6a 92 b3

   secret (32 octets):  8e f8 e6 41 ab fd 33 02 a2 4a c0 03 d0 98 2a
      3e 6e ef cd 99 46 ed 19 82 b8 1b 4d e2 ab c8 7d e8

{server}  derive secret "tls13 c hs traffic":

   PRK (32 octets):  8e f8 e6 41 ab fd 33 02 a2 4a c0 03 d0 98 2a 3e
      6e ef cd 99 46 ed 19 82 b8 1b 4d e2 ab c8 7d e8

   hash (32 octets):  87 73 ef 3f d6 03 64 ff ab 64 c5 f1 66 f8 30 09
      c2 9e c6 70 16 76 e5 cc 60 b5 1a 2f 2a dd 9e 27
```

```
   info (54 octets):  00 20 12 74 6c 73 31 33 20 63 20 68 73 20 74 72
      61 66 66 69 63 20 87 73 ef 3f d6 03 64 ff ab 64 c5 f1 66 f8 30
      09 c2 9e c6 70 16 76 e5 cc 60 b5 1a 2f 2a dd 9e 27

   output (32 octets):  1e af b2 10 3a c5 96 e5 a8 67 3e ae 2c 42 0c
      ff b2 d9 45 99 d9 00 08 94 0b db a8 8c a7 71 26 26

{server}  derive secret "tls13 s hs traffic":

   PRK (32 octets):  8e f8 e6 41 ab fd 33 02 a2 4a c0 03 d0 98 2a 3e
      6e ef cd 99 46 ed 19 82 b8 1b 4d e2 ab c8 7d e8

   hash (32 octets):  87 73 ef 3f d6 03 64 ff ab 64 c5 f1 66 f8 30 09
      c2 9e c6 70 16 76 e5 cc 60 b5 1a 2f 2a dd 9e 27

   info (54 octets):  00 20 12 74 6c 73 31 33 20 73 20 68 73 20 74 72
      61 66 66 69 63 20 87 73 ef 3f d6 03 64 ff ab 64 c5 f1 66 f8 30
      09 c2 9e c6 70 16 76 e5 cc 60 b5 1a 2f 2a dd 9e 27
```



```
   output (32 octets):  82 54 e1 25 3f 75 bf a5 bb 5c 4e f2 b1 bb 79
      73 e0 b7 b8 32 51 31 2b ce 86 30 8e a1 27 b5 52 e0

{server}  derive secret for master "tls13 derived":

   PRK (32 octets):  8e f8 e6 41 ab fd 33 02 a2 4a c0 03 d0 98 2a 3e
      6e ef cd 99 46 ed 19 82 b8 1b 4d e2 ab c8 7d e8

   hash (32 octets):  e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24
      27 ae 41 e4 64 9b 93 4c a4 95 99 1b 78 52 b8 55

   info (49 octets):  00 20 0d 74 6c 73 31 33 20 64 65 72 69 76 65 64
      20 e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24 27 ae 41 e4
      64 9b 93 4c a4 95 99 1b 78 52 b8 55

   output (32 octets):  91 74 25 ca 4f 3e 40 22 e2 e6 bb 99 25 f2 f7
      08 e9 7c 1c 75 56 cd e8 63 52 1f 40 b3 c8 2f 49 36

{server}  extract secret "master":

   salt (32 octets):  91 74 25 ca 4f 3e 40 22 e2 e6 bb 99 25 f2 f7 08
```

```
      e9 7c 1c 75 56 cd e8 63 52 1f 40 b3 c8 2f 49 36

   ikm (32 octets):  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

   secret (32 octets):  5f 5f 3a b7 4a c0 3b 74 79 0f 0f 40 33 f9 e9
      3c 18 44 95 ac 41 03 a9 f2 2d 43 d8 dc 57 86 a2 95

{server}  send handshake record:

   payload (123 octets):  02 00 00 77 03 03 eb 62 5e d0 a8 a3 3c 5f
      a3 c2 77 5a eb a4 c6 2a 4f 31 71 f2 ff ea e4 ea 53 38 27 30 41
      6f f7 3a 00 13 01 00 00 4f 00 28 00 45 00 17 00 41 04 89 cf b4
      c1 91 61 f7 0e b1 5a 43 81 40 02 13 53 46 37 bd b4 fe d0 20 a9
      2e 59 d9 58 10 ff eb e3 a8 dd bd f2 e2 cc 65 71 fe 17 df 28 3a
      37 22 f1 23 f3 32 fc b0 cb 3d 8b bb 9f 0b 65 e0 07 46 ae 00 2b
      00 02 7f 16

   ciphertext (128 octets):  16 03 03 00 7b 02 00 00 77 03 03 eb 62
      5e d0 a8 a3 3c 5f a3 c2 77 5a eb a4 c6 2a 4f 31 71 f2 ff ea e4
      ea 53 38 27 30 41 6f f7 3a 00 13 01 00 00 4f 00 28 00 45 00 17
      00 41 04 89 cf b4 c1 91 61 f7 0e b1 5a 43 81 40 02 13 53 46 37
      bd b4 fe d0 20 a9 2e 59 d9 58 10 ff eb e3 a8 dd bd f2 e2 cc 65
      71 fe 17 df 28 3a 37 22 f1 23 f3 32 fc b0 cb 3d 8b bb 9f 0b 65
      e0 07 46 ae 00 2b 00 02 7f 16

{server}  send a EncryptedExtensions handshake message
```



```
{server}  send a Certificate handshake message

{server}  send a CertificateVerify handshake message

{server}  calculate finished "tls13 finished":

   PRK (32 octets):  82 54 e1 25 3f 75 bf a5 bb 5c 4e f2 b1 bb 79 73
      e0 b7 b8 32 51 31 2b ce 86 30 8e a1 27 b5 52 e0

   hash (0 octets):  (empty)

   info (18 octets):  00 20 0e 74 6c 73 31 33 20 66 69 6e 69 73 68 65
      64 00
```

output (32 octets): a3 3a 40 a0 16 61 06 92 2f 96 9d 66 28 69 0e
ad 71 29 6b 1c 9f 44 14 64 e8 f4 c4 c2 33 14 10 15

{server} send a Finished handshake message

{server} send handshake record:

payload (639 octets): 08 00 00 12 00 10 00 0a 00 08 00 06 00 17
00 18 00 1d 00 00 00 00 0b 00 01 b9 00 00 01 b5 00 01 b0 30 82
01 ac 30 82 01 15 a0 03 02 01 02 02 01 02 30 0d 06 09 2a 86 48
86 f7 0d 01 01 0b 05 00 30 0e 31 0c 30 0a 06 03 55 04 03 13 03
72 73 61 30 1e 17 0d 31 36 30 37 33 30 30 31 32 33 35 39 5a 17
0d 32 36 30 37 33 30 30 31 32 33 35 39 5a 30 0e 31 0c 30 0a 06
03 55 04 03 13 03 72 73 61 30 81 9f 30 0d 06 09 2a 86 48 86 f7
0d 01 01 01 05 00 03 81 8d 00 30 81 89 02 81 81 00 b4 bb 49 8f
82 79 30 3d 98 08 36 39 9b 36 c6 98 8c 0c 68 de 55 e1 bd b8 26
d3 90 1a 24 61 ea fd 2d e4 9a 91 d0 15 ab bc 9a 95 13 7a ce 6c
1a f1 9e aa 6a f9 8c 7c ed 43 12 09 98 e1 87 a8 0e e0 cc b0 52
4b 1b 01 8c 3e 0b 63 26 4d 44 9a 6d 38 e2 2a 5f da 43 08 46 74
80 30 53 0e f0 46 1c 8c a9 d9 ef bf ae 8e a6 d1 d0 3e 2b d1 93
ef f0 ab 9a 80 02 c4 74 28 a6 d3 5a 8d 88 d7 9f 7f 1e 3f 02 03
01 00 01 a3 1a 30 18 30 09 06 03 55 1d 13 04 02 30 00 30 0b 06
03 55 1d 0f 04 04 03 02 05 a0 30 0d 06 09 2a 86 48 86 f7 0d 01
01 0b 05 00 03 81 81 00 85 aa d2 a0 e5 b9 27 6b 90 8c 65 f7 3a
72 67 17 06 18 a5 4c 5f 8a 7b 33 7d 2d f7 a5 94 36 54 17 f2 ea
e8 f8 a5 8c 8f 81 72 f9 31 9c f3 6b 7f d6 c5 5b 80 f2 1a 03 01
51 56 72 60 96 fd 33 5e 5e 67 f2 db f1 02 70 2e 60 8c ca e6 be
c1 fc 63 a4 2a 99 be 5c 3e b7 10 7c 3c 54 e9 b9 eb 2b d5 20 3b
1c 3b 84 e0 a8 b2 f7 59 40 9b a3 ea c9 d9 1d 40 2d cc 0c c8 f8
96 12 29 ac 91 87 b4 2b 4d e1 00 00 0f 00 00 84 08 04 00 80 96
ac 87 45 e8 60 64 a1 18 d3 35 75 88 1c c7 db 99 b7 ad 5c f6 42
04 2f 0c 6a 4c 65 42 d6 15 3e f7 b4 71 2d 9f 9f 7c 16 7a 9c fe
1b 9f 7a e7 41 4b ff 4c d1 3c dd 81 1d ce 07 ce 22 7b f2 ec 74
38 e9 22 6e 7d da 00 0e f8 34 85 60 ed 21 6b 28 a8 bc 6d b6 10

3c aa 96 00 d8 84 7c a6 f0 ea 40 64 da 4f 7d 6d c7 b5 98 ff 54
36 a0 4e 01 7d e3 2c 12 eb f3 2e 55 3b e2 60 3e 0f 63 20 63 42
b8 14 00 00 20 a4 98 49 23 dd 33 35 94 bd 90 4b 9e 80 1b c1 88
73 31 57 ba 4b 16 c7 62 cd a9 f6 f3 0f e9 a6 88

ciphertext (661 octets): 17 03 03 02 90 11 09 c2 d4 04 4a ea 1f
e6 a7 d0 e1 52 4a 86 e6 b3 fd 43 3a 4a 86 8a 8c 10 1a 58 ab b3

```
      38 1e 66 c6 9a bc b0 0d c0 ba d7 b4 9c c3 24 55 aa 28 c8 e5 13
      13 a0 9b 4f 19 fc 3c b9 9b 35 5e 8a 4a fc 74 84 c4 c6 d4 de 32
      d5 75 01 4c 53 71 48 ce 7d df 31 d9 3a f5 fb f1 ac dd b8 c7 13
      32 e7 ce d7 7a 2f 4d e0 16 dd 98 5a 2c ec 06 8a e2 49 fd a9 bc
      a4 d7 23 19 5a df d8 b8 03 95 00 e9 e1 d6 c6 01 20 6a 6a 85 33
      56 1a ab ca f5 cc f2 e2 b7 c5 9e 74 75 1a 41 ca 95 15 03 26 a8
      f2 25 56 7f bb 9f ad 99 39 b6 d6 ca a2 47 90 05 d9 4b b8 95 18
      ca 63 84 cf 66 dd 97 36 2f 8c 40 13 26 d4 22 d5 3f bd 68 1b 14
      09 16 ec 14 31 45 32 49 04 dd 7f 63 26 96 81 a1 36 f2 e6 15 f4
      7e e9 e3 2a a3 25 2e 0c 3b 1d 47 a9 92 63 50 b4 98 5b 96 51 ef
      c5 14 80 09 61 6d 75 df dd e9 33 1f e2 ae e5 44 c4 a1 40 10 2a
      db c1 12 d4 45 1e 1b 90 46 02 9e 71 b9 36 60 49 c9 ac aa 36 82
      79 f0 dc 27 00 bb 15 1d 96 6d 2d 71 a7 55 44 6a 74 9f 3f fb 2b
      10 11 0d 2f 9d c2 1e f7 1d b7 2b 53 ae 2b a8 70 70 f2 79 15 b8
      a3 4a 4c 92 03 70 36 3b f7 75 98 a8 99 3d 6d 97 45 53 f7 6a 83
      dd e2 a5 5c 30 10 ed bf 86 ec 45 6c 5e 12 f4 fb 28 3f d5 25 e2
      2b f8 4e 28 03 41 9a 1f 5c 0d 83 7c e5 bc b1 8c 36 18 06 35 c1
      d3 28 30 f4 af f6 60 7a 72 81 1e 4e 19 02 b1 c0 88 4e 3c 97 dd
      44 3f 69 5e e3 fe 76 db 3e cc d4 36 ae 87 0f 7f 1d b1 3e 00 cc
      41 9c c4 5a 44 69 29 92 c2 e1 62 41 fb 31 d4 ed e3 95 77 2b 31
      fd e3 cc 4d b3 27 64 0f 48 d8 3f 63 5f 95 be f6 7f b3 60 c3 c9
      8e db d6 ae 57 4f ae d0 dc 59 38 20 b2 48 3e 6f 2d ae 39 51 5d
      9c 54 b9 d1 66 5a 7c ac 02 16 fa 32 55 0a a4 46 a5 e3 7c 9d af
      54 ed 38 71 39 eb 85 47 cc 53 13 7b 02 37 4b 4a 03 4d 38 18 69
      57 81 da 2a 23 ec 82 b5 81 98 3d 69 5b 84 37 94 07 cc 87 dc 85
      4e 0d 06 3e 6d 62 d2 3c 97 97 5e 91 7d b6 d5 21 82 83 a2 e8 15
      16 43 37 5f 0b a1 84 59 91 ed 6f 40 9a 68 31 b5 7a 1c 5d dd 88
      fe b6 e9 cc 66 ee 1f 3c 28 60 f6 1d f0 f8 1e bb 3b 0a 87 2d 0c
      2d 00 ae 84 44 5f 47 89 31 7d 02 e1 b6 75 a8 db cc 45 66 34 28
      95 ff 20 77 d8 9d 20 2d 86 43 22 be 4c c6 b3 f0 bf df

{server}  derive secret "tls13 c ap traffic":

   PRK (32 octets):  5f 5f 3a b7 4a c0 3b 74 79 0f 0f 40 33 f9 e9 3c
      18 44 95 ac 41 03 a9 f2 2d 43 d8 dc 57 86 a2 95

   hash (32 octets):  62 05 ce 54 b4 21 f2 e9 c4 2e ed 68 3d 19 12 89
      cd 9b 1f 9a 84 4d 94 c2 3e 95 b8 94 cc 4e 8a 42
```

```
   info (54 octets):  00 20 12 74 6c 73 31 33 20 63 20 61 70 20 74 72
      61 66 66 69 63 20 62 05 ce 54 b4 21 f2 e9 c4 2e ed 68 3d 19 12
      89 cd 9b 1f 9a 84 4d 94 c2 3e 95 b8 94 cc 4e 8a 42

   output (32 octets):  de 2e 40 35 e0 1c 52 ea e4 d5 b8 b3 46 50 c3
      32 04 53 6b 07 03 09 21 e4 31 95 37 b4 a0 90 1e e0

{server}  derive secret "tls13 s ap traffic":

   PRK (32 octets):  5f 5f 3a b7 4a c0 3b 74 79 0f 0f 40 33 f9 e9 3c
      18 44 95 ac 41 03 a9 f2 2d 43 d8 dc 57 86 a2 95

   hash (32 octets):  62 05 ce 54 b4 21 f2 e9 c4 2e ed 68 3d 19 12 89
      cd 9b 1f 9a 84 4d 94 c2 3e 95 b8 94 cc 4e 8a 42

   info (54 octets):  00 20 12 74 6c 73 31 33 20 73 20 61 70 20 74 72
      61 66 66 69 63 20 62 05 ce 54 b4 21 f2 e9 c4 2e ed 68 3d 19 12
      89 cd 9b 1f 9a 84 4d 94 c2 3e 95 b8 94 cc 4e 8a 42

   output (32 octets):  14 ff 87 2f 92 e2 e2 5c c2 18 e0 15 bf db f7
      b9 1d b3 42 c7 20 00 e2 bd 1d 5c 08 06 d7 56 ab 4d

{server}  derive secret "tls13 exp master":

   PRK (32 octets):  5f 5f 3a b7 4a c0 3b 74 79 0f 0f 40 33 f9 e9 3c
      18 44 95 ac 41 03 a9 f2 2d 43 d8 dc 57 86 a2 95

   hash (32 octets):  62 05 ce 54 b4 21 f2 e9 c4 2e ed 68 3d 19 12 89
      cd 9b 1f 9a 84 4d 94 c2 3e 95 b8 94 cc 4e 8a 42

   info (52 octets):  00 20 10 74 6c 73 31 33 20 65 78 70 20 6d 61 73
      74 65 72 20 62 05 ce 54 b4 21 f2 e9 c4 2e ed 68 3d 19 12 89 cd
      9b 1f 9a 84 4d 94 c2 3e 95 b8 94 cc 4e 8a 42

   output (32 octets):  10 9f ba 7b bc 8d 86 f3 f8 56 bf d6 a1 0e f3
      c2 fb f6 8c 6e 06 70 1b ab 97 6b a8 0c bf 00 12 d5

{client}  extract secret "early":

   salt:  (absent)

   ikm (32 octets):  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

   secret (32 octets):  33 ad 0a 1c 60 7e c0 3b 09 e6 cd 98 93 68 0c
      e2 10 ad f3 00 aa 1f 26 60 e1 b2 2e 10 f1 70 f9 2a

{client}  derive secret for handshake "tls13 derived":
```

```
      PRK (32 octets):  33 ad 0a 1c 60 7e c0 3b 09 e6 cd 98 93 68 0c e2
         10 ad f3 00 aa 1f 26 60 e1 b2 2e 10 f1 70 f9 2a

      hash (32 octets):  e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24
         27 ae 41 e4 64 9b 93 4c a4 95 99 1b 78 52 b8 55

      info (49 octets):  00 20 0d 74 6c 73 31 33 20 64 65 72 69 76 65 64
         20 e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24 27 ae 41 e4
         64 9b 93 4c a4 95 99 1b 78 52 b8 55

      output (32 octets):  6f 26 15 a1 08 c7 02 c5 67 8f 54 fc 9d ba b6
         97 16 c0 76 18 9c 48 25 0c eb ea c3 57 6c 36 11 ba

   {client}  extract secret "handshake":

      salt (32 octets):  6f 26 15 a1 08 c7 02 c5 67 8f 54 fc 9d ba b6 97
         16 c0 76 18 9c 48 25 0c eb ea c3 57 6c 36 11 ba

      ikm (32 octets):  ba 1c d6 f8 aa 98 a2 de ff b7 ba bb 8e 52 4d 2f
         d3 e8 2d 5c ff 5d 7b e3 0a 20 80 ef 62 6a 92 b3

      secret (32 octets):  8e f8 e6 41 ab fd 33 02 a2 4a c0 03 d0 98 2a
         3e 6e ef cd 99 46 ed 19 82 b8 1b 4d e2 ab c8 7d e8

   {client}  derive secret "tls13 c hs traffic" (same as server)

   {client}  derive secret "tls13 s hs traffic" (same as server)

   {client}  derive secret for master "tls13 derived" (same as server)

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

   {client}  calculate finished "tls13 finished" (same as server)

   {client}  derive secret "tls13 c ap traffic" (same as server)

   {client}  derive secret "tls13 s ap traffic" (same as server)

   {client}  derive secret "tls13 exp master" (same as server)

   {client}  calculate finished "tls13 finished":

      PRK (32 octets):  1e af b2 10 3a c5 96 e5 a8 67 3e ae 2c 42 0c ff
```

```
      b2 d9 45 99 d9 00 08 94 0b db a8 8c a7 71 26 26

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



```
   info (18 octets):  00 20 0e 74 6c 73 31 33 20 66 69 6e 69 73 68 65
      64 00

   output (32 octets):  19 3b 17 c6 19 fb 94 85 1f 97 91 db 7b 9a 9e
      03 9d 4f 81 96 9a 93 71 02 06 4b 45 a3 be e9 a3 12

{client}  send a Finished handshake message

{client}  send handshake record:

   payload (36 octets):  14 00 00 20 3c 9c 63 c4 72 e5 d6 ab 04 4d 14
      59 2e 5a d8 a2 ef 4c 1d 70 f7 f7 7a 13 3c 8d cc fc 05 a6 df 52

   ciphertext (58 octets):  17 03 03 00 35 cd db d8 39 c3 4d 8d b2 a1
      fc 58 5e 55 78 f6 5f ec 70 81 d6 95 00 88 09 02 5c 0c 9d 4f 87
      5a f9 e7 10 d7 52 a2 0a 3d 2c 59 86 7e 92 6e b4 39 52 e2 8f 91
      83 da

{client}  derive secret "tls13 res master":

   PRK (32 octets):  5f 5f 3a b7 4a c0 3b 74 79 0f 0f 40 33 f9 e9 3c
      18 44 95 ac 41 03 a9 f2 2d 43 d8 dc 57 86 a2 95

   hash (32 octets):  cb 0c c7 bc 35 ef 49 7c be e7 ea fa 2b ff a2 2f
      8d a5 b8 28 5e 83 35 48 0c 33 65 81 32 22 2c c2

   info (52 octets):  00 20 10 74 6c 73 31 33 20 72 65 73 20 6d 61 73
      74 65 72 20 cb 0c c7 bc 35 ef 49 7c be e7 ea fa 2b ff a2 2f 8d
      a5 b8 28 5e 83 35 48 0c 33 65 81 32 22 2c c2

   output (32 octets):  18 8c 90 bc 6f a9 7a 8d d5 55 1d 80 b1 ae 18
      42 4c f3 e2 f6 90 bc 70 54 e3 6b 33 3f 17 30 17 f3

{server}  calculate finished "tls13 finished" (same as client)

{server}  derive secret "tls13 res master" (same as client)
```

{client} send alert record:

payload (2 octets): 01 00

ciphertext (24 octets): 17 03 03 00 13 93 21 5e 8c f7 98 69 b6 9a 28 57 8f 90 f4 c6 94 6e 5c 9b

{server} send alert record:

payload (2 octets): 01 00

ciphertext (24 octets): 17 03 03 00 13 4a b5 80 73 c0 a8 93 de 17 76 47 6d ec d2 5e 97 84 e3 d1

6. Client Authentication

In this example, the server requests client authentication. The client uses a certificate with an RSA key, the server uses an ECDSA certificate with a P-256 key.

{client} create an ephemeral x25519 key pair:

private key (32 octets): a4 0d c1 93 0c 00 af 0e 9d 3b c2 6c f9 0f 5e ee 7d ba 97 17 1f 53 2b 71 7f ef bf bf 87 08 38 c9

public key (32 octets): d5 dd 20 0f ad 08 39 7b 40 f3 e6 14 45 24 0c 75 78 5e b2 e5 0b 72 7c 5a 04 91 64 0d c1 2c 3a 0e

{client} send a ClientHello handshake message

{client} send handshake record:

payload (186 octets): 01 00 00 b6 03 03 a3 ce 03 a9 0c 76 17 79 2d ee d9 6e 55 b1 6a b8 fc 10 91 2c 67 f3 3d db d1 50 b3 25 d5 ca d6 58 00 00 06 13 01 13 03 13 02 01 00 00 87 00 00 00 0b 00 09 00 00 06 73 65 72 76 65 72 ff 01 00 01 00 00 0a 00 14 00 12 00 1d 00 17 00 18 00 19 01 00 01 01 01 02 01 03 01 04 00 28 00 26 00 24 00 1d 00 20 d5 dd 20 0f ad 08 39 7b 40 f3 e6 14 45 24 0c 75 78 5e b2 e5 0b 72 7c 5a 04 91 64 0d c1 2c 3a 0e 00 2b 00 03 02 7f 16 00 0d 00 20 00 1e 04 03 05 03 06 03 02 03 08 04 08

```
      05 08 06 04 01 05 01 06 01 02 01 04 02 05 02 06 02 02 02 00 2d
      00 02 01 01
```

```
   ciphertext (191 octets):  16 03 01 00 ba 01 00 00 b6 03 03 a3 ce
      03 a9 0c 76 17 79 2d ee d9 6e 55 b1 6a b8 fc 10 91 2c 67 f3 3d
      db d1 50 b3 25 d5 ca d6 58 00 00 06 13 01 13 03 13 02 01 00 00
      87 00 00 00 0b 00 09 00 00 06 73 65 72 76 65 72 ff 01 00 01 00
      00 0a 00 14 00 12 00 1d 00 17 00 18 00 19 01 00 01 01 01 02 01
      03 01 04 00 28 00 26 00 24 00 1d 00 20 d5 dd 20 0f ad 08 39 7b
      40 f3 e6 14 45 24 0c 75 78 5e b2 e5 0b 72 7c 5a 04 91 64 0d c1
      2c 3a 0e 00 2b 00 03 02 7f 16 00 0d 00 20 00 1e 04 03 05 03 06
      03 02 03 08 04 08 05 08 06 04 01 05 01 06 01 02 01 04 02 05 02
      06 02 02 02 00 2d 00 02 01 01
```

```
{server}  extract secret "early":
```

```
   salt:  (absent)
```



```
   ikm (32 octets):  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
   secret (32 octets):  33 ad 0a 1c 60 7e c0 3b 09 e6 cd 98 93 68 0c
      e2 10 ad f3 00 aa 1f 26 60 e1 b2 2e 10 f1 70 f9 2a
```

```
{server}  create an ephemeral x25519 key pair:
```

```
   private key (32 octets):  01 f2 df a3 5d 2f f7 47 3c b2 b2 85 25
      74 2d a0 58 a0 35 c7 f8 21 bc 86 bf c2 11 72 16 be cc aa
```

```
   public key (32 octets):  b5 89 13 10 62 da ed c2 12 1b b7 5c 36 88
      0b 71 12 c1 96 7f fe 17 db 5f a7 ef ef 22 90 90 1e 3d
```

```
{server}  send a ServerHello handshake message
```

```
{server}  derive secret for handshake "tls13 derived":
```

```
   PRK (32 octets):  33 ad 0a 1c 60 7e c0 3b 09 e6 cd 98 93 68 0c e2
      10 ad f3 00 aa 1f 26 60 e1 b2 2e 10 f1 70 f9 2a
```

```
   hash (32 octets):  e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24
```

```
      27 ae 41 e4 64 9b 93 4c a4 95 99 1b 78 52 b8 55

   info (49 octets):  00 20 0d 74 6c 73 31 33 20 64 65 72 69 76 65 64
      20 e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24 27 ae 41 e4
      64 9b 93 4c a4 95 99 1b 78 52 b8 55

   output (32 octets):  6f 26 15 a1 08 c7 02 c5 67 8f 54 fc 9d ba b6
      97 16 c0 76 18 9c 48 25 0c eb ea c3 57 6c 36 11 ba

{server}  extract secret "handshake":

   salt (32 octets):  6f 26 15 a1 08 c7 02 c5 67 8f 54 fc 9d ba b6 97
      16 c0 76 18 9c 48 25 0c eb ea c3 57 6c 36 11 ba

   ikm (32 octets):  94 2f 83 fa ee 2f ad ad 24 2e eb fb c7 a6 6d 5e
      c7 71 04 b1 3c d4 97 e0 b1 0d 9d 70 69 1d e8 6a

   secret (32 octets):  53 d7 91 87 9a 6b 33 f3 86 45 35 3b 3e 03 49
      e5 e0 88 e4 0b 6c 37 00 12 0c 80 04 25 d3 d5 e9 9f

{server}  derive secret "tls13 c hs traffic":

   PRK (32 octets):  53 d7 91 87 9a 6b 33 f3 86 45 35 3b 3e 03 49 e5
      e0 88 e4 0b 6c 37 00 12 0c 80 04 25 d3 d5 e9 9f
```



```
   hash (32 octets):  7a a6 f3 63 a4 49 35 45 a9 31 9b da 72 05 59 8c
      e1 5c bc 83 48 40 ce 04 c0 0e 8f 96 0b 27 80 7b

   info (54 octets):  00 20 12 74 6c 73 31 33 20 63 20 68 73 20 74 72
      61 66 66 69 63 20 7a a6 f3 63 a4 49 35 45 a9 31 9b da 72 05 59
      8c e1 5c bc 83 48 40 ce 04 c0 0e 8f 96 0b 27 80 7b

   output (32 octets):  e8 d4 bb 93 8c a3 de 6d 1d 7c 78 01 a5 57 20
      aa df cd 34 2d c8 a4 47 04 1d 21 7c 83 c8 df f3 94

{server}  derive secret "tls13 s hs traffic":

   PRK (32 octets):  53 d7 91 87 9a 6b 33 f3 86 45 35 3b 3e 03 49 e5
      e0 88 e4 0b 6c 37 00 12 0c 80 04 25 d3 d5 e9 9f
```

```
   hash (32 octets):  7a a6 f3 63 a4 49 35 45 a9 31 9b da 72 05 59 8c
      e1 5c bc 83 48 40 ce 04 c0 0e 8f 96 0b 27 80 7b

   info (54 octets):  00 20 12 74 6c 73 31 33 20 73 20 68 73 20 74 72
      61 66 66 69 63 20 7a a6 f3 63 a4 49 35 45 a9 31 9b da 72 05 59
      8c e1 5c bc 83 48 40 ce 04 c0 0e 8f 96 0b 27 80 7b

   output (32 octets):  8b fc e8 b0 11 4e ac cd 83 64 68 b5 e4 60 30
      fd 32 1c 37 20 7a 41 cd 22 66 4f 56 53 14 f2 1e 05

{server}  derive secret for master "tls13 derived":

   PRK (32 octets):  53 d7 91 87 9a 6b 33 f3 86 45 35 3b 3e 03 49 e5
      e0 88 e4 0b 6c 37 00 12 0c 80 04 25 d3 d5 e9 9f

   hash (32 octets):  e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24
      27 ae 41 e4 64 9b 93 4c a4 95 99 1b 78 52 b8 55

   info (49 octets):  00 20 0d 74 6c 73 31 33 20 64 65 72 69 76 65 64
      20 e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24 27 ae 41 e4
      64 9b 93 4c a4 95 99 1b 78 52 b8 55

   output (32 octets):  6f d8 3c 95 03 f0 45 fb a0 08 69 a3 23 22 28
      0f 38 85 3f cd 95 15 f1 3c e5 09 60 f0 e6 00 24 84

{server}  extract secret "master":

   salt (32 octets):  6f d8 3c 95 03 f0 45 fb a0 08 69 a3 23 22 28 0f
      38 85 3f cd 95 15 f1 3c e5 09 60 f0 e6 00 24 84

   ikm (32 octets):  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```



```
   secret (32 octets):  86 05 00 52 9e e3 a6 0a 26 44 3e 62 2a 4c 00
      0a b3 ff 0d ea 05 05 5c c3 ed f3 bf 01 f7 11 db ba

{server}  send handshake record:

   payload (90 octets):  02 00 00 56 03 03 0b 21 fe 7a 05 5c 66 77 67
      7b 21 e0 7d fc 22 f9 65 92 1c 5c 3e 0c c8 85 b1 71 5e 2e 01 a8
      91 3d 00 13 01 00 00 2e 00 28 00 24 00 1d 00 20 b5 89 13 10 62
```

```
      da ed c2 12 1b b7 5c 36 88 0b 71 12 c1 96 7f fe 17 db 5f a7 ef
      ef 22 90 90 1e 3d 00 2b 00 02 7f 16

   ciphertext (95 octets):  16 03 03 00 5a 02 00 00 56 03 03 0b 21 fe
      7a 05 5c 66 77 67 7b 21 e0 7d fc 22 f9 65 92 1c 5c 3e 0c c8 85
      b1 71 5e 2e 01 a8 91 3d 00 13 01 00 00 2e 00 28 00 24 00 1d 00
      20 b5 89 13 10 62 da ed c2 12 1b b7 5c 36 88 0b 71 12 c1 96 7f
      fe 17 db 5f a7 ef ef 22 90 90 1e 3d 00 2b 00 02 7f 16

{server}  send a EncryptedExtensions handshake message

{server}  send a CertificateRequest handshake message

{server}  send a Certificate handshake message

{server}  send a CertificateVerify handshake message

{server}  calculate finished "tls13 finished":

   PRK (32 octets):  8b fc e8 b0 11 4e ac cd 83 64 68 b5 e4 60 30 fd
      32 1c 37 20 7a 41 cd 22 66 4f 56 53 14 f2 1e 05

   hash (0 octets):  (empty)

   info (18 octets):  00 20 0e 74 6c 73 31 33 20 66 69 6e 69 73 68 65
      64 00

   output (32 octets):  23 48 7f 1e 47 29 a3 ef 3d fb e1 61 bd 0c d1
      c0 42 51 86 74 be 62 54 5b f1 62 25 7a d7 d9 4e 9d

{server}  send a Finished handshake message

{server}  send handshake record:

   payload (512 octets):  08 00 00 1e 00 1c 00 0a 00 14 00 12 00 1d
      00 17 00 18 00 19 01 00 01 01 01 02 01 03 01 04 00 00 00 00 0d
      00 00 27 00 00 24 00 0d 00 20 00 1e 04 03 05 03 06 03 02 03 08
      04 08 05 08 06 04 01 05 01 06 01 02 01 04 02 05 02 06 02 02 02
      0b 00 01 3b 00 00 01 37 00 01 32 30 82 01 2e 30 81 d5 a0 03 02
      01 02 02 01 07 30 0a 06 08 2a 86 48 ce 3d 04 03 02 30 13 31 11
```



```
      30 0f 06 03 55 04 03 13 08 65 63 64 73 61 32 35 36 30 1e 17 0d
```

```
      31 36 30 37 33 30 30 31 32 34 30 30 5a 17 0d 32 36 30 37 33 30
      30 31 32 34 30 30 5a 30 13 31 11 30 0f 06 03 55 04 03 13 08 65
      63 64 73 61 32 35 36 30 59 30 13 06 07 2a 86 48 ce 3d 02 01 06
      08 2a 86 48 ce 3d 03 01 07 03 42 00 04 08 d5 30 16 15 75 f4 cf
      e7 f1 54 ee 34 48 18 00 86 00 1e 88 43 1a 79 ee 62 ee 6e 2f 83
      ef 38 ba 61 e9 fb 37 f3 4e 00 7a 7d f4 d2 f5 b5 6d 1f 04 ec e4
      5d 62 1f 46 84 06 f5 c3 a1 51 58 94 8d d0 a3 1a 30 18 30 09 06
      03 55 1d 13 04 02 30 00 30 0b 06 03 55 1d 0f 04 04 03 02 07 80
      30 0a 06 08 2a 86 48 ce 3d 04 03 02 03 48 00 30 45 02 21 00 df
      30 fd 45 07 f5 ed d2 2c 1a 6f f8 6d b4 79 ca 69 3f ee ca 3b 71
      b3 f9 ef 55 6b 29 37 c0 59 4d 02 20 62 e2 a4 72 50 d3 20 fe a8
      3c 7e 2d cb 5b 76 a5 0e 02 00 c0 9a db d1 3f ee 94 6e 51 3e 01
      1d 11 00 00 0f 00 00 4c 04 03 00 48 30 46 02 21 00 f7 46 ae b2
      e0 10 2f 37 94 0d d8 90 2b 0a 80 63 33 b7 63 69 06 28 9b ae f0
      a9 7d 92 12 ab 14 30 02 21 00 a7 81 31 62 2d 82 7b ce 23 d5 04
      c7 f8 1e 2a 78 d7 fb d6 59 fa 09 e1 e7 4c 5a 74 b9 b0 e5 5f 3e
      14 00 00 20 c6 c0 d6 02 f0 3c e5 92 6c 9e 53 05 04 a0 0a 5f d5
      40 97 5d de c4 6a fd 8a 18 fa 20 85 17 08 d6

   ciphertext (534 octets):  17 03 03 02 11 17 bf 02 f6 e5 be bf f8
      97 3f de b8 5f 0c cd 77 d7 5e 02 12 69 d8 47 5d 82 a4 26 74 bf
      e3 6c c7 a2 89 6f 63 42 3a aa 5f e2 b2 f8 96 6a 85 61 cb 25 f4
      c4 e2 8e c2 df 74 64 85 cf 64 fd f4 28 e6 fb c9 02 49 89 3a 62
      a8 15 c5 7a f9 8d 03 73 44 4f 90 85 40 1c e2 5f 4b fb 30 e9 99
      85 6a b0 eb 87 70 ef b0 1a cb 7e 30 c3 be d5 3d a3 03 32 b7 dc
      1b 31 78 89 49 a8 05 71 4a 06 81 75 4b 41 d4 57 93 c8 b8 28 29
      b1 9f 6a fa ea b5 bc c1 78 3d 0b 5e 39 63 03 67 7e fc 73 26 5a
      2c 0c cc 07 02 6f e0 98 46 3b 7e e1 d7 c7 e9 81 ff 7c 89 61 d0
      9d e7 fc be 92 77 98 25 98 a5 e9 0f 53 3a 23 5e 1a e3 81 01 fc
      87 07 69 3e c3 ff 90 47 75 52 87 91 74 65 d3 a6 44 12 2c 73 6c
      1f e5 98 a2 a9 45 87 c3 d2 4f b8 6a d2 18 97 2d 99 38 c0 89 42
      ce 28 64 20 db a4 3a 39 84 46 55 5f 3b 12 d0 84 5b e9 c8 fe 0c
      8d 71 f6 99 97 b7 08 b7 51 9c 7b 78 70 98 5d ad 45 89 40 a5 8f
      e4 1a 93 be 45 1f 31 08 42 7a d7 fd 3a 6f 27 ef e0 9f 35 d4 ad
      b3 a5 61 b3 41 87 ad 07 59 90 ac a8 b1 4c ec 21 cd c3 1b 78 e8
      bb b8 e0 30 d7 f7 c8 0c 56 dc 7c 2f f8 b5 53 0f 95 8c 0f ab 81
      3b c8 3e b3 d7 a9 72 5d 36 0f b2 d8 33 7c df c9 3c b3 d7 ed ea
      ea 75 75 cd cc 43 64 a1 a9 f2 19 e4 ae a9 3c c0 6e 2a 31 51 a8
      c7 f0 ef 15 16 a2 fd 34 1a bf b5 b3 9f 32 7c 6b 31 54 33 6e 5c
      6e 94 ed 2c c2 ca 95 ff 69 d4 25 48 3c 63 d2 a4 04 60 b0 03 c0
      4a b6 f5 bf 0e dc 3c 4e 66 21 a7 6f ff ff 1a 4d ae 84 7b 17 b8
      e5 ea 2b b5 47 e0 5f e3 8a 0f dc 63 78 fd cf 45 5c b9 92 17 8f
      e6 12 9d bd a3 49 a4 c5 6c d3 1e 04 ab bc 4c 5d 2d f5 0d 0c 06
      04 75 ec 11 8b 0e 3d 82 f0 79 cb 5e ec 44 1f c1 f1 78 88 db f7
      9b 04 f4 fa 89 39 ab be 4f 65 c4 b6 26 43 5c c8 dc
```

{server} derive secret "tls13 c ap traffic":

```
      PRK (32 octets):  86 05 00 52 9e e3 a6 0a 26 44 3e 62 2a 4c 00 0a
         b3 ff 0d ea 05 05 5c c3 ed f3 bf 01 f7 11 db ba

      hash (32 octets):  35 56 64 82 3a 07 6c 67 8f 60 11 3d f2 c4 fa 18
         3e 44 c0 0b 0a 94 38 c7 93 d2 96 e9 2a 76 e3 06

      info (54 octets):  00 20 12 74 6c 73 31 33 20 63 20 61 70 20 74 72
         61 66 66 69 63 20 35 56 64 82 3a 07 6c 67 8f 60 11 3d f2 c4 fa
         18 3e 44 c0 0b 0a 94 38 c7 93 d2 96 e9 2a 76 e3 06

      output (32 octets):  49 94 c4 1b d3 5f 90 84 9c da c8 1c ee eb 48
         cf 0a 25 08 9c da 15 66 d0 c8 51 ce 42 67 55 0e 42

   {server}  derive secret "tls13 s ap traffic":

      PRK (32 octets):  86 05 00 52 9e e3 a6 0a 26 44 3e 62 2a 4c 00 0a
         b3 ff 0d ea 05 05 5c c3 ed f3 bf 01 f7 11 db ba

      hash (32 octets):  35 56 64 82 3a 07 6c 67 8f 60 11 3d f2 c4 fa 18
         3e 44 c0 0b 0a 94 38 c7 93 d2 96 e9 2a 76 e3 06

      info (54 octets):  00 20 12 74 6c 73 31 33 20 73 20 61 70 20 74 72
         61 66 66 69 63 20 35 56 64 82 3a 07 6c 67 8f 60 11 3d f2 c4 fa
         18 3e 44 c0 0b 0a 94 38 c7 93 d2 96 e9 2a 76 e3 06

      output (32 octets):  04 94 45 e6 ca b5 c5 4c 87 af 8a d9 c9 4f c1
         28 14 f5 4c 22 bb c4 6a 08 5e 9e 3f 55 91 1e 77 0c

   {server}  derive secret "tls13 exp master":

      PRK (32 octets):  86 05 00 52 9e e3 a6 0a 26 44 3e 62 2a 4c 00 0a
         b3 ff 0d ea 05 05 5c c3 ed f3 bf 01 f7 11 db ba

      hash (32 octets):  35 56 64 82 3a 07 6c 67 8f 60 11 3d f2 c4 fa 18
         3e 44 c0 0b 0a 94 38 c7 93 d2 96 e9 2a 76 e3 06

      info (52 octets):  00 20 10 74 6c 73 31 33 20 65 78 70 20 6d 61 73
         74 65 72 20 35 56 64 82 3a 07 6c 67 8f 60 11 3d f2 c4 fa 18 3e
         44 c0 0b 0a 94 38 c7 93 d2 96 e9 2a 76 e3 06

      output (32 octets):  84 69 2c 16 37 b0 91 ce 55 73 7a bc e2 46 9b
         74 5c f4 77 80 ea d7 68 be 99 35 59 2c 16 0d 0d 57

   {client}  extract secret "early":

      salt:  (absent)
```

```
      ikm (32 octets):  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
         00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      secret (32 octets):  33 ad 0a 1c 60 7e c0 3b 09 e6 cd 98 93 68 0c
         e2 10 ad f3 00 aa 1f 26 60 e1 b2 2e 10 f1 70 f9 2a

   {client}  derive secret for handshake "tls13 derived":

      PRK (32 octets):  33 ad 0a 1c 60 7e c0 3b 09 e6 cd 98 93 68 0c e2
         10 ad f3 00 aa 1f 26 60 e1 b2 2e 10 f1 70 f9 2a

      hash (32 octets):  e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24
         27 ae 41 e4 64 9b 93 4c a4 95 99 1b 78 52 b8 55

      info (49 octets):  00 20 0d 74 6c 73 31 33 20 64 65 72 69 76 65 64
         20 e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24 27 ae 41 e4
         64 9b 93 4c a4 95 99 1b 78 52 b8 55

      output (32 octets):  6f 26 15 a1 08 c7 02 c5 67 8f 54 fc 9d ba b6
         97 16 c0 76 18 9c 48 25 0c eb ea c3 57 6c 36 11 ba

   {client}  extract secret "handshake":

      salt (32 octets):  6f 26 15 a1 08 c7 02 c5 67 8f 54 fc 9d ba b6 97
         16 c0 76 18 9c 48 25 0c eb ea c3 57 6c 36 11 ba

      ikm (32 octets):  94 2f 83 fa ee 2f ad ad 24 2e eb fb c7 a6 6d 5e
         c7 71 04 b1 3c d4 97 e0 b1 0d 9d 70 69 1d e8 6a

      secret (32 octets):  53 d7 91 87 9a 6b 33 f3 86 45 35 3b 3e 03 49
         e5 e0 88 e4 0b 6c 37 00 12 0c 80 04 25 d3 d5 e9 9f

   {client}  derive secret "tls13 c hs traffic" (same as server)

   {client}  derive secret "tls13 s hs traffic" (same as server)

   {client}  derive secret for master "tls13 derived" (same as server)

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

{client} calculate finished "tls13 finished" (same as server)

{client} derive secret "tls13 c ap traffic" (same as server)

{client} derive secret "tls13 s ap traffic" (same as server)

{client} derive secret "tls13 exp master" (same as server)

{client} send a Certificate handshake message

{client} send a CertificateVerify handshake message

{client} calculate finished "tls13 finished":

PRK (32 octets): e8 d4 bb 93 8c a3 de 6d 1d 7c 78 01 a5 57 20 aa df cd 34 2d c8 a4 47 04 1d 21 7c 83 c8 df f3 94

hash (0 octets): (empty)

info (18 octets): 00 20 0e 74 6c 73 31 33 20 66 69 6e 69 73 68 65 64 00

output (32 octets): 03 c1 ff eb e1 ec af c1 16 94 42 a3 5f b7 8c 4a f4 3d 55 4e c8 5b 94 ae 3f e9 18 3f 54 55 f1 84

{client} send a Finished handshake message

{client} send handshake record:

payload (623 octets): 0b 00 01 bf 00 00 01 bb 00 01 b6 30 82 01 b2 30 82 01 1b a0 03 02 01 02 02 01 01 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00 30 11 31 0f 30 0d 06 03 55 04 03 13 06 63 6c 69 65 6e 74 30 1e 17 0d 31 36 30 37 33 30 30 31 32 33 35 39 5a 17 0d 32 36 30 37 33 30 30 31 32 33 35 39 5a 30 11 31 0f 30 0d 06 03 55 04 03 13 06 63 6c 69 65 6e 74 30 81 9f 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 81 8d 00 30 81 89 02 81 81 00 c3 81 75 e0 04 a6 8d 09 3f 82 3b 9c 37 9d 20 1f bc 0b b7 a1 c7 91 90 5e 3f bf 76 84 7e 44 e7 51 eb bc d3 60 bd 94 5c 81 e5 22 2b cc 88 46 d3 a8 a0 f9 3e 9b f5 be ba bd 92 ed f1 de 1f f1 90 21 70 3e 7a b6 c0 90 15 13 f9 7e 39 b1 11 f0 9c 93 48 97 1c

```
      7b 21 19 84 a7 54 cd 45 fe 09 5a f0 ea 42 36 82 9b cc f7 a7 fe
      9b 28 88 e7 8a b4 77 69 0a 5b 9e 1c cb e9 1c 6a 4a 0f 97 a7 e0
      28 42 01 02 03 01 00 01 a3 1a 30 18 30 09 06 03 55 1d 13 04 02
      30 00 30 0b 06 03 55 1d 0f 04 04 03 02 07 80 30 0d 06 09 2a 86
      48 86 f7 0d 01 01 0b 05 00 03 81 81 00 1a 7a 5a 01 85 32 b0 22
      af 07 67 d4 86 16 0c ff 2d 16 7a 19 15 d2 38 35 b5 45 94 91 6d
      c6 80 be 5d 2e 62 60 76 c5 d5 27 22 eb cc 77 5d 7d 99 f9 80 be
      2f c9 4d 34 ac f6 cc 00 ba 90 cb cf b0 60 8a a1 e7 e3 97 1e f0
      c0 7a 41 d4 7a d8 34 5d 1f 81 fe 41 8a 1c f4 10 54 42 9f d2 17
      bd 77 7d c1 cf 08 f0 5d f9 07 99 c6 59 36 1e 0f 1a 8e e4 ac 0f
      78 97 42 0b db c8 23 da 80 a2 f2 ba 23 08 1c 00 00 0f 00 00 84
      08 04 00 80 84 10 d9 4d 75 9a c5 a1 87 9c 61 71 49 48 04 09 7f
      9d 94 6f 41 e0 02 2a 66 ee 8e 0d 3b bc f4 37 c2 6f db cb 1d b6
      69 45 94 f9 01 71 82 e2 80 5c 1a 68 24 e1 06 d1 86 dd 42 37 53
      60 89 14 3d 06 12 ec 33 08 50 2c d5 a1 54 3e 82 fb 9d b5 58 7e
      54 07 6e 18 7a d6 ad 9b 89 35 42 a7 54 1d f0 47 49 7f fb 6c e2
```



```
      5d df f8 fd e7 ed 8a 67 98 f2 b7 de 1f a8 d9 f9 67 76 15 3a 3d
      01 9c 5a cc af 97 14 00 00 20 49 3e e4 87 b7 fc 2b f5 19 b7 cd
      2b 6b 33 b5 0f 5b e6 d5 23 37 a4 96 2e 39 d0 ec 13 92 f0 76 80

   ciphertext (645 octets):  17 03 03 02 80 4d 75 ab 8f 1d 72 06 a6
      3e 00 ac cd 41 c6 aa d6 3f e1 4d df 20 42 8f 59 68 d7 fc 60 61
      2f d2 5f f6 49 ae 82 c6 2e 3b 1e 6b 0d 07 d4 26 ae d4 3f a8 1f
      c2 76 15 43 92 5d 9a 8c 53 57 b2 0d 5d f1 7d fe 67 7d 8f df 7c
      b3 5f 07 48 02 a0 c5 5a 12 31 de a8 d4 27 1d fa 5f 5d 65 21 a4
      f4 67 c4 78 5d b0 54 1d f1 fb 84 8f 8b 01 e6 8d cb 9c 63 a3 86
      3a 6b d3 e8 8d b5 a3 67 34 53 2d f3 68 b0 f5 7a 12 b5 65 94 b2
      e1 6b 69 4e 5c e6 c1 e6 f3 ab 6f 1f a0 a9 f5 40 e3 80 2d 6b f2
      4f eb e4 2b 72 1f 13 ab 80 90 f1 54 e4 14 54 72 f9 1b 9a fe d6
      c5 b4 51 39 7e a0 fd 19 8c 04 48 af 73 44 42 91 57 43 11 53 4d
      22 91 07 65 9b 88 00 5c f0 51 db 32 70 83 44 4c 2c 00 14 e9 22
      a2 bd 94 a2 c9 d8 40 70 7b 4c 76 0c 56 ff 09 36 b1 b7 ad 8c 76
      f7 bf c2 dc 8b 75 19 d2 29 ad 7b a5 6d 0a 16 12 d0 56 f8 78 da
      5a b9 91 c9 ce 3d d0 44 62 8c 5a 0f ab 4d 51 14 af 7f 95 7e f1
      f5 27 05 6b 5d 16 0e 8b b2 ad 6d b0 a9 3b e2 3c 5f 68 7e 0a 28
      ec 76 32 a2 1f 24 4f 9e ac 1d 04 4f f9 2d 3c 1f b1 8e f8 1a bb
      cf 38 08 24 d4 cb 1c e4 51 7a d6 c1 45 f0 56 8b 41 b9 36 26 65
      68 ac 23 1e c9 48 eb b3 32 1f 5f b0 14 36 21 af 9b 3c e7 51 7b
      08 88 e0 71 c6 17 4b 7b 05 a7 bf ce a2 d9 e2 50 16 1a f7 0f 93
      73 a9 c2 fc 2d 41 06 85 52 38 bc 54 f0 78 40 6c 75 82 7a 46 1e
      c2 c3 59 19 f6 75 16 44 fd ce b6 11 31 3e f5 57 09 b5 2b 32 69
```

```
      24 12 32 92 d1 bd 9d 1d 19 2f 6d 4d d6 bd e8 f3 c8 2c 30 49 f4
      f6 dd f7 4d 18 4d 72 76 57 9f ce 90 a6 6b bd 6b 50 17 82 6d cd
      0d 31 25 bc a5 47 df b2 f9 ab 53 43 fd a4 2a bb eb 5b f9 ca 6d
      02 45 8e 7e 7b af 21 04 70 e5 e6 93 ee a4 c2 ca 50 2f e8 e6 d4
      78 7b 57 18 6d 85 40 7d df 0d 5e 0c 8a be 1a 73 46 d6 cd 30 86
      5a c5 fc 9d f2 d3 8e 84 1e f3 67 91 be e0 dd 3a 1a 95 b9 c3 2d
      3e 8e 97 04 c8 7b fe bd 35 ea f5 cb db 4a 72 32 46 82 04 a5 75
      63 2c ed 27 76 70 6c d5 02 a5 66 d1 30 c1 ab 40 9a 1c e4 ab 08
      c5 8c 04 ae 75 33 94 8b 63 4b ff 14 54 b6 91 a1 e9 88 c6 de 54
      85 7e 12 05 65 fc bc 6e 3d 01 ed fa 7a ab c5 f9 2c 45 b4 df 22
      50 c0

{client}  derive secret "tls13 res master":

   PRK (32 octets):  86 05 00 52 9e e3 a6 0a 26 44 3e 62 2a 4c 00 0a
      b3 ff 0d ea 05 05 5c c3 ed f3 bf 01 f7 11 db ba

   hash (32 octets):  7f 2d 4e 12 6e 73 62 ae 2f ea 3c b9 1f 32 ec b0
      f7 ba 7f 60 c4 ee a4 41 0f 80 26 dc 33 25 77 88

   info (52 octets):  00 20 10 74 6c 73 31 33 20 72 65 73 20 6d 61 73
      74 65 72 20 7f 2d 4e 12 6e 73 62 ae 2f ea 3c b9 1f 32 ec b0 f7
      ba 7f 60 c4 ee a4 41 0f 80 26 dc 33 25 77 88
```



```
   output (32 octets):  42 f1 0b 54 0d ee 84 7b 5b 1c 5b 0d 89 2c f7
      11 7d 9a 13 9b 89 20 64 88 a3 52 eb ee d8 cb 6f 90

{server}  calculate finished "tls13 finished" (same as client)

{server}  derive secret "tls13 res master" (same as client)

{client}  send alert record:

   payload (2 octets):  01 00

   ciphertext (24 octets):  17 03 03 00 13 70 16 fa 95 9e 65 31 0b cf
      54 11 09 dd 74 cc 4b bd 42 95

{server}  send alert record:

   payload (2 octets):  01 00
```

```
   ciphertext (24 octets):  17 03 03 00 13 92 e3 7d 92 18 1a 14 ec cf
      3e 35 13 f4 54 63 4f b1 70 d9
```

7. 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.

8. References

8.1. Normative References

[I-D.ietf-tls-tls13]
Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", draft-ietf-tls-tls13-22 (work in progress), November 2017.

8.2. 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, <https://www.rfc-editor.org/info/rfc7748>.

8.3. URIs

[1] https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS

Appendix A. Acknowledgements

This draft is generated using tests that were written for NSS [1]. 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