CVE-2011-4354

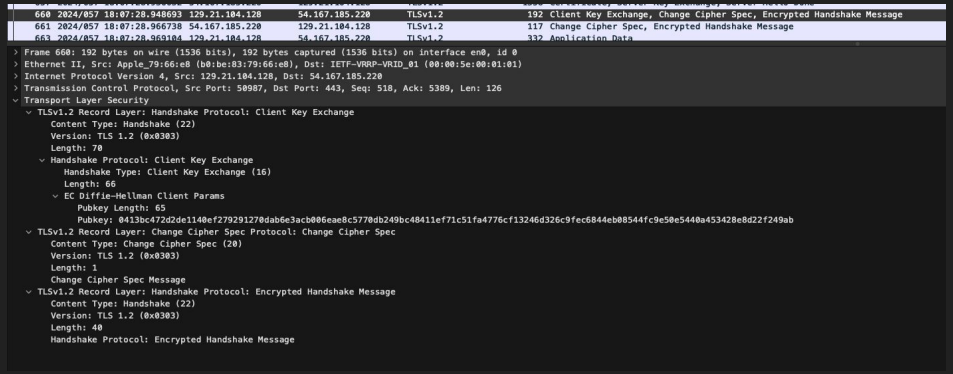
Jonathan Bateman, Hassan Alshehri, Harrison Tarsia

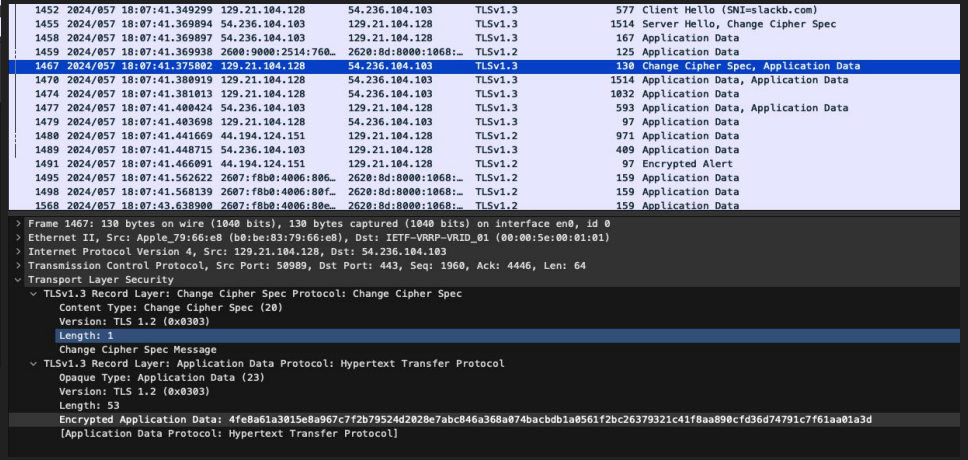
Agenda → We took some risks

- Why CVE-2011-4354?
- ECDHE Review / Intro
- Attack Angle
- TLS in Action & the Handshake (Wirecaps)
- Quiz Questions
- Audience Questions

Why is CVE-2011-4354 important?

- OpenSSL version 0.9.8g
- Implementation vs Efficiency → The Programmers Dilemma
- TLS v1.2 → Why it enables this attack?
  - “Change Cipher Spec” comparison Left (1.2) vs Right (1.3)





ECDHE Overview

- k^i_C & k^i_S → private keys {1 → (n -1)}
- G → generator
  - (initial elliptic crv point)
- Q^i_C & Q^i_S → public keys (over net)
  - Q = [k]G (private key * generator)
- bug?

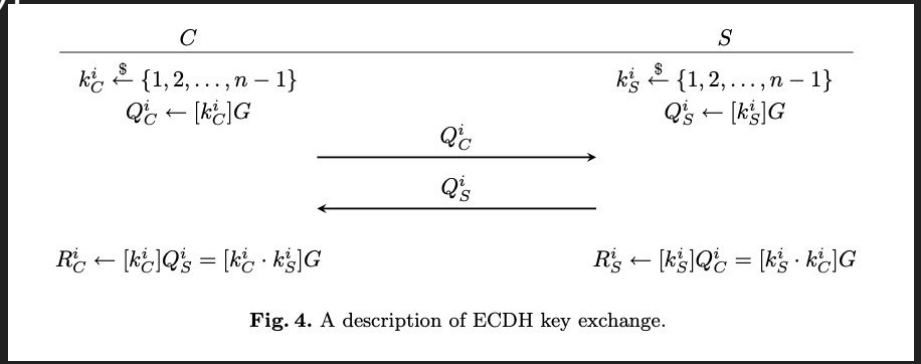


Fig. 4. A description of ECDH key exchange.

- R^i_C & $R^i_S = [k^i_S * k^i_C]G$ → multiply personal private key by opposing public key
  - Shared secret → both client and server have it w/o each other's private key
- Attacker: $Q^i_S Q^i_C = k^i_S * k^i_C * G * G \neq [k^i_S * k^i_C]G$ → Very different

Did devs misunderstand how to implement this algorithm?

Why or Why not?

“This highlights a subtle point: rather than a programming error, the bug is more accurately characterized as a design error. That is , the incorrectly designed refinement is correctly implemented in OpenSSL.”

Attack Angle → blame devs who prioritize optimization

k^i_s

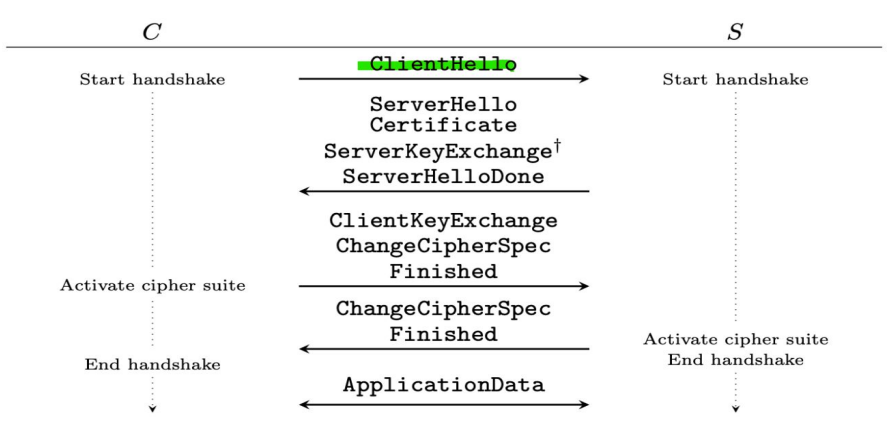
Stays the same!

Client Hello

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	34.107.243.93	192.168.200.146	TLSv1.2	186	Application Data
9	0.013998756	192.168.200.146	34.149.100.209	TLSv1.2	284	Client Hello (SNI=firefox.settings.services.mozilla.com)
11	0.026172994	34.149.100.209	192.168.200.146	TLSv1.2	1466	Server Hello
14	0.026223208	34.149.100.209	192.168.200.146	TLSv1.2	1466	Certificate
15	0.026224444	34.149.100.209	192.168.200.146	TLSv1.2	338	Server Key Exchange, Server Hello Done
18	0.027388200	192.168.200.146	34.149.100.209	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
19	0.038015494	34.149.100.209	192.168.200.146	TLSv1.2	361	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
20	0.038025198	34.149.100.209	192.168.200.146	TLSv1.2	135	Application Data
22	0.038394934	192.168.200.146	34.149.100.209	TLSv1.2	243	Application Data
23	0.038469760	192.168.200.146	34.149.100.209	TLSv1.2	327	Application Data
24	0.038550009	192.168.200.146	34.149.100.209	TLSv1.2	104	Application Data
27	0.048920162	34.149.100.209	192.168.200.146	TLSv1.2	104	Application Data
28	0.050038038	34.149.100.209	192.168.200.146	TLSv1.2	395	Application Data
29	0.050052453	34.149.100.209	192.168.200.146	TLSv1.2	527	Application Data
30	0.050109680	34.149.100.209	192.168.200.146	TLSv1.2	112	Application Data
32	0.050234201	192.168.200.146	34.149.100.209	TLSv1.2	112	Application Data

```
▼ Transport Layer Security
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 213
    ▼ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 209
        Version: TLS 1.2 (0x0303)
      ▶ Random: dfa4d6ee83fbd51d3e4d713b0fa63e6df4a1ced463484447afab367f4ac8b2f9
        Session ID Length: 0
        Cipher Suites Length: 28
      ▼ Cipher Suites (14 suites)
            Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
            Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
            Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
            Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
            Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
            Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
            Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
            Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
            Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
            Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
            Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
            Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
            Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
            Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
        Compression Methods Length: 1
```

```
0000  00 50 56 b0 bb 9e 00 50
0010  01 0e 9f 9d 40 00 40 06
0020  64 d1 ab 8c 01 bb 59 9b
0030  00 fb 7d f9 00 00 01 01
0040  f5 5d 16 03 01 00 d5 01
0050  ee 83 fb d5 1d 3e 4d 71
0060  d4 63 48 44 47 af ab 36
0070  c0 2b c0 2f cc a9 cc a8
0080  c0 13 c0 14 00 9c 00 9d
0090  00 00 00 2a 00 28 00 00
00a0  2e 73 65 74 74 69 6e 67
00b0  65 73 2e 6d 6f 7a 69 6c
00c0  00 00 ff 01 00 01 00 00
00d0  17 00 18 00 19 00 0b 00
00e0  10 00 0e 00 0c 02 68 32
00f0  31 00 05 00 05 01 00 00
0100  04 03 05 03 06 03 08 04
0110  06 01 02 03 02 01 00 1c
```




```
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 213
  ▼ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 209
      Version: TLS 1.2 (0x0303)
    ▶ Random: dfa4d6ee83fbd51d3e4d713b0fa63e6df4a1ced463484447afab367f4ac8b2f9
      Session ID Length: 0
      Cipher Suites Length: 28
    ▶ Cipher Suites (14 suites)
      Compression Methods Length: 1
    ▶ Compression Methods (1 method)
      Extensions Length: 140
    ▶ Extension: server_name (len=42) name=firefox.settings.services.mozilla.com
    ▶ Extension: extended_master_secret (len=0)
    ▶ Extension: renegotiation_info (len=1)
    ▶ Extension: supported_groups (len=10)
    ▶ Extension: ec_point_formats (len=2)
    ▼ Extension: session_ticket (len=0)
        Type: session_ticket (35)
        Length: 0
        Session Ticket: <MISSING>
    ▶ Extension: application_layer_protocol_negotiation (len=14)
    ▶ Extension: status_request (len=5)
    ▶ Extension: signature_algorithms (len=24)
    ▶ Extension: record_size_limit (len=2)
      [JA4: t12d1410h2_c866b44c5a26_b5b8faed2b99]
```

Transport Layer Security (tls), 218 bytes

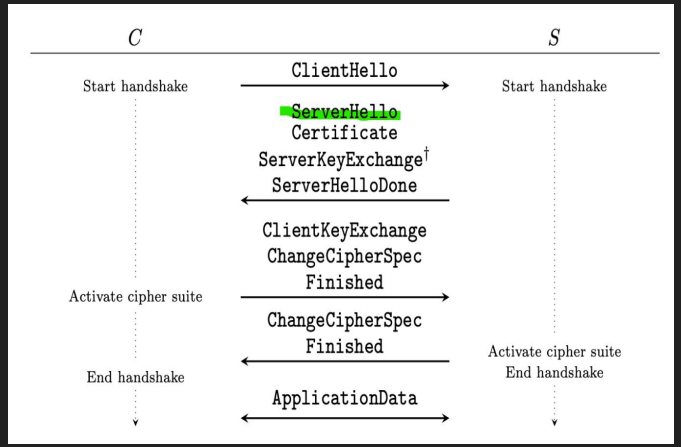
Server Hello - Cipher Suite

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	34.107.243.93	192.168.200.146	TLSv1.2	186	Application Data
9	0.013998756	192.168.200.146	34.149.100.209	TLSv1.2	284	Client Hello (SNI=firefox.settings.services.mozilla.com)
11	0.026172994	34.149.100.209	192.168.200.146	TLSv1.2	1466	Server Hello
14	0.026223208	34.149.100.209	192.168.200.146	TLSv1.2	1466	Certificate
15	0.026224444	34.149.100.209	192.168.200.146	TLSv1.2	338	Server Key Exchange, Server Hello Done
18	0.027388200	192.168.200.146	34.149.100.209	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
19	0.038015494	34.149.100.209	192.168.200.146	TLSv1.2	361	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
20	0.038025198	34.149.100.209	192.168.200.146	TLSv1.2	135	Application Data
22	0.038394934	192.168.200.146	34.149.100.209	TLSv1.2	243	Application Data
23	0.038469760	192.168.200.146	34.149.100.209	TLSv1.2	327	Application Data
24	0.038550009	192.168.200.146	34.149.100.209	TLSv1.2	104	Application Data
27	0.048920162	34.149.100.209	192.168.200.146	TLSv1.2	104	Application Data
28	0.050038038	34.149.100.209	192.168.200.146	TLSv1.2	395	Application Data
29	0.050052453	34.149.100.209	192.168.200.146	TLSv1.2	527	Application Data
30	0.050109680	34.149.100.209	192.168.200.146	TLSv1.2	112	Application Data
32	0.050234201	192.168.200.146	34.149.100.209	TLSv1.2	112	Application Data

```
▸ Frame 11: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits) on interface eth0, id 0
▸ Ethernet II, Src: VMware_b0:bb:9e (00:50:56:b0:bb:9e), Dst: VMware_b0:78:02 (00:50:56:b0:78:02)
▸ Internet Protocol Version 4, Src: 34.149.100.209, Dst: 192.168.200.146
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 43916, Seq: 1, Ack: 219, Len: 1400
▾ Transport Layer Security
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 72
    ▾ Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 68
        Version: TLS 1.2 (0x0303)
      ▸ Random: 65d4d2f640c28f4825f4cae360c3019afa59c9a6eb1f4fa2444f574e47524401
        Session ID Length: 0
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
        Compression Method: null (0)
        Extensions Length: 28
      ▾ Extension: extended_master_secret (len=0)
          Type: extended_master_secret (23)
          Length: 0
      ▸ Extension: renegotiation_info (len=1)
      ▸ Extension: ec_point_formats (len=2)
      ▾ Extension: session_ticket (len=0)
          Type: session_ticket (35)
          Length: 0
          Session Ticket: <MISSING>
      ▸ Extension: application_layer_protocol_negotiation (len=5)
```

```
0060  a6 eb 1f 4f a2 44 4f 57  4e
0070  00 00 1c 00 17 00 00 ff  01
0080  01 00 00 23 00 00 00 10  00
0090  03 03 0f ec 0b 00 0f e8  00
00a0  05 5a 30 82 04 42 a0 03  02
00b0  e3 ad 95 c7 39 2e 35 05  65
00c0  0d 06 09 2a 86 48 86 f7  0d
00d0  31 0b 30 09 06 03 55 04  06
00e0  14 06 03 55 04 0a 13 0d  4c
00f0  63 72 79 70 74 31 0b 30  09
0100  52 33 30 1e 17 0d 32 33  31
0110  30 33 5a 17 0d 32 34 30  33
0120  32 5a 30 26 31 24 30 22  06
0130  65 6d 6f 74 65 2d 73 65  74
0140  6f 7a 69 6c 6c 61 2e 6f  72
0150  06 09 2a 86 48 86 f7 0d  01
0160  0f 00 30 82 01 0a 02 82  01
0170  25 84 0e d8 a3 54 48 4d  e6
0180  1f ba 51 6b 5e f5 83 58  27
0190  b8 02 78 f6 3d de 04 77  9d
01a0  34 aa bb ad d7 79 fc 11  2f
01b0  f7 7a c5 57 f3 d5 47 f3  f8
01c0  52 5e 8a 6e 55 6e f5 33  10
01d0  89 ef 67 de a4 a0 0e 03  08
01e0  dc 65 08 c2 e5 54 13 01  29
01f0  05 52 db cb c8 e0 5b 20  71
0200  06 7b f7 fb a6 6f 28 d0  54
0210  5d 4d d5 e5 06 5a 49 b4  80
0220  59 00 02 25 4c e3 3f 43  1d
0230  8f 06 89 e6 3f ed 5a bd  a5
```

Cipher Suite (tls.handshake.ciphersuite), 2 bytes



Certificate

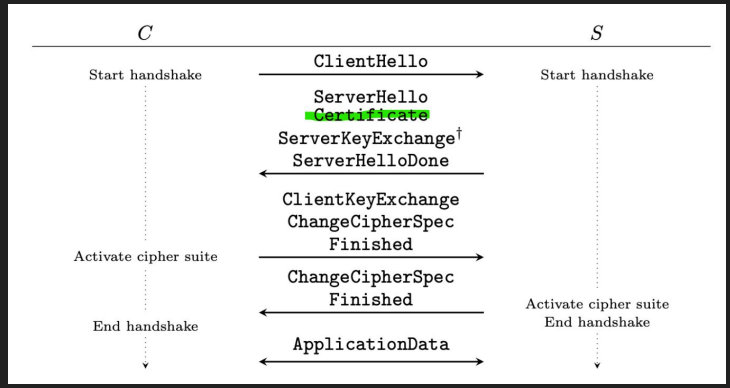
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	34.107.243.93	192.168.200.146	TLSv1.2	186	Application Data
9	0.013998756	192.168.200.146	34.149.100.209	TLSv1.2	284	Client Hello (SNI=firefox.settings.services.mozilla.com)
11	0.026172994	34.149.100.209	192.168.200.146	TLSv1.2	1466	Server Hello
14	0.026223208	34.149.100.209	192.168.200.146	TLSv1.2	1466	Certificate
15	0.026224444	34.149.100.209	192.168.200.146	TLSv1.2	338	Server Key Exchange, Server Hello Done
18	0.027388200	192.168.200.146	34.149.100.209	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
19	0.038015494	34.149.100.209	192.168.200.146	TLSv1.2	361	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
20	0.038025198	34.149.100.209	192.168.200.146	TLSv1.2	135	Application Data
22	0.038394934	192.168.200.146	34.149.100.209	TLSv1.2	243	Application Data
23	0.038469760	192.168.200.146	34.149.100.209	TLSv1.2	327	Application Data
24	0.038550009	192.168.200.146	34.149.100.209	TLSv1.2	104	Application Data
27	0.048920162	34.149.100.209	192.168.200.146	TLSv1.2	104	Application Data
28	0.050038038	34.149.100.209	192.168.200.146	TLSv1.2	395	Application Data
29	0.050052453	34.149.100.209	192.168.200.146	TLSv1.2	527	Application Data
30	0.050109680	34.149.100.209	192.168.200.146	TLSv1.2	112	Application Data
32	0.050234201	192.168.200.146	34.149.100.209	TLSv1.2	112	Application Data

```
▸ Frame 14: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits) on interface eth0, id 0
▸ Ethernet II, Src: VMware_b0:bb:9e (00:50:56:b0:bb:9e), Dst: VMware_b0:78:02 (00:50:56:b0:78:02)
▸ Internet Protocol Version 4, Src: 34.149.100.209, Dst: 192.168.200.146
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 43916, Seq: 2801, Ack: 219, Len: 1400
▸ [3 Reassembled TCP Segments (4081 bytes): #11(1323), #13(1400), #14(1358)]
▾ Transport Layer Security
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 4076
    ▾ Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 4072
        Certificates Length: 4069
      ▾ Certificates (4069 bytes)
          Certificate Length: 1374
        ▾ Certificate [truncated]: 3082055a30820442a003020102021203d198e3ad95c7392e35056581fd8f12af6b300d0…
          ▸ signedCertificate
          ▸ algorithmIdentifier (sha256WithRSAEncryption)
            Padding: 0
            encrypted [truncated]: 3c46201e93c07f1efaeed3063531963cd257c1a8fd4358012c2ae5be5906b941d9d24f…
          Certificate Length: 1306
        ▾ Certificate [truncated]: 30820516308202fea003020102021100912b084acf0c18a753f6d62e25a75f5a300d060…
          ▸ signedCertificate
          ▸ algorithmIdentifier (sha256WithRSAEncryption)
            Padding: 0
            encrypted [truncated]: 85ca4e473ea3f7854485bcd56778b29863ad754d1e963d336572542d81a0eac3edf820…
          Certificate Length: 1380
```

```
0000  00 50 56 b0 78 02 00 50  56
0010  05 ac 80 ca 00 00 7a 06  a9
0020  c8 92 01 bb ab 8c c1 f0  5e
0030  01 05 df 35 00 00 01 01  08
0040  36 93 42 b8 ee 76 aa 3c  64
0050  86 48 86 f7 0d 01 01 0b  05
0060  06 03 55 04 0a 13 1b 44  69
0070  69 67 6e 61 74 75 72 65  20
0080  6f 2e 31 17 30 15 06 03  55
0090  20 52 6f 6f 74 20 43 41  20
00a0  31 30 31 32 30 31 39 31  34
00b0  30 39 33 30 31 38 31 34  30
00c0  09 06 03 55 04 06 13 02  55
00d0  55 04 0a 13 20 49 6e 74  65
00e0  63 75 72 69 74 79 20 52  65
00f0  47 72 6f 75 70 31 15 30  13
0100  49 53 52 47 20 52 6f 6f  74
0110  30 0d 06 09 2a 86 48 86  f7
0120  82 02 0f 00 30 82 02 0a  02
0130  73 f4 14 37 f3 9b 9e 2b  57
0140  38 90 8c 6e 3c e6 57 a0  78
0150  6e f6 00 4f 28 db de 68  86
0160  14 12 6b bf 1f d2 ea 31  9b
0170  f5 dd 79 df b3 b8 ff 12  f1
0180  69 4a 66 66 6c 8f 7e 3c  70
0190  c0 e6 80 ae e2 4b 8f b7  99
01a0  7c 99 48 23 53 e8 38 ae  4f
01b0  8c 80 74 b6 da 2f d0 38  8d
```

Frame (1466 bytes) | Reassembled TC

Transport Layer Security: Protocol



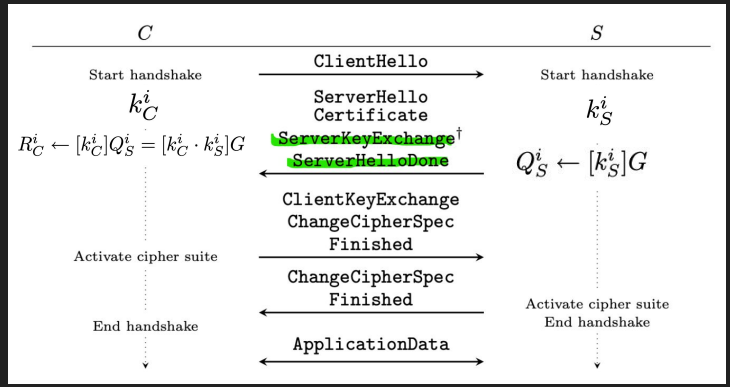
Server Key Exchange, Server Hello Done

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	34.107.243.93	192.168.200.146	TLSv1.2	186	Application Data
9	0.013998756	192.168.200.146	34.149.100.209	TLSv1.2	284	Client Hello (SNI=firefox.settings.services.mozilla.com)
11	0.026172994	34.149.100.209	192.168.200.146	TLSv1.2	1466	Server Hello
14	0.026223208	34.149.100.209	192.168.200.146	TLSv1.2	1466	Certificate
15	0.026224444	34.149.100.209	192.168.200.146	TLSv1.2	338	Server Key Exchange, Server Hello Done
18	0.027388200	192.168.200.146	34.149.100.209	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
19	0.038015494	34.149.100.209	192.168.200.146	TLSv1.2	361	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
20	0.038025198	34.149.100.209	192.168.200.146	TLSv1.2	135	Application Data
22	0.038394934	192.168.200.146	34.149.100.209	TLSv1.2	243	Application Data
23	0.038469760	192.168.200.146	34.149.100.209	TLSv1.2	327	Application Data
24	0.038550009	192.168.200.146	34.149.100.209	TLSv1.2	104	Application Data
27	0.048920162	34.149.100.209	192.168.200.146	TLSv1.2	104	Application Data
28	0.050038038	34.149.100.209	192.168.200.146	TLSv1.2	395	Application Data
29	0.050052453	34.149.100.209	192.168.200.146	TLSv1.2	527	Application Data
30	0.050109680	34.149.100.209	192.168.200.146	TLSv1.2	112	Application Data
32	0.050234201	192.168.200.146	34.149.100.209	TLSv1.2	112	Application Data

```
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 43916, Seq: 4201, Ack: 219, Len: 272
▸ [2 Reassembled TCP Segments (305 bytes): #14(42), #15(263)]
▾ Transport Layer Security
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 300
    ▾ Handshake Protocol: Server Key Exchange
        Handshake Type: Server Key Exchange (12)
        Length: 296
      ▾ EC Diffie-Hellman Server Params
          Curve Type: named_curve (0x03)
          Named Curve: x25519 (0x001d)
          Pubkey Length: 32
          Pubkey: 0efdf852aa8bf95422a98f0247539abb9c7a48d135e41a6c003cc4dab671083b
        ▾ Signature Algorithm: rsa_pss_rsae_sha256 (0x0804)
            Signature Hash Algorithm Hash: Unknown (8)
            Signature Hash Algorithm Signature: SM2 (4)
          Signature Length: 256
          Signature [truncated]: 9e8a3abf096ae6a9f32beec2fe29e0b83d034b47e80ef41c5e5c57e45d1502c046a2f4f77…
▾ Transport Layer Security
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 4
    ▾ Handshake Protocol: Server Hello Done
        Handshake Type: Server Hello Done (14)
        Length: 0
```

```
0000  16 03 03 01 2c 0c 00 01
0010  52 aa 8b f9 54 22 a9 8f
0020  d1 35 e4 1a 6c 00 3c c4
0030  00 9e 8a 3a bf 09 6a e6
0040  b8 3d 03 4b 47 e8 0e f4
0050  c0 46 a2 f4 f7 7d b2 47
0060  ad c8 0d b8 af 4e d3 f7
0070  9f f6 87 ba 57 d6 0d de
0080  c9 fe 74 9d a8 1e d5 62
0090  7c 52 85 9e e5 0c ab de
00a0  1e b4 9e 1d e8 d2 51 a1
00b0  42 66 de 04 70 d6 25 56
00c0  76 b5 b4 73 7d 46 3b 18
00d0  48 13 cb 46 ab 61 14 2f
00e0  29 df 0b 23 b8 8c f1 76
00f0  5a cf 78 db c4 57 57 3f
0100  8a 53 94 64 3b 22 4f 45
0110  d0 e8 7f 6e d3 ad 14 9b
0120  13 02 78 a8 90 41 c2 a4
0130  b1
```

Frame (338 bytes) | Reassembled



Client Key Exchange, Change Cipher Spec, Encrypted Handshake

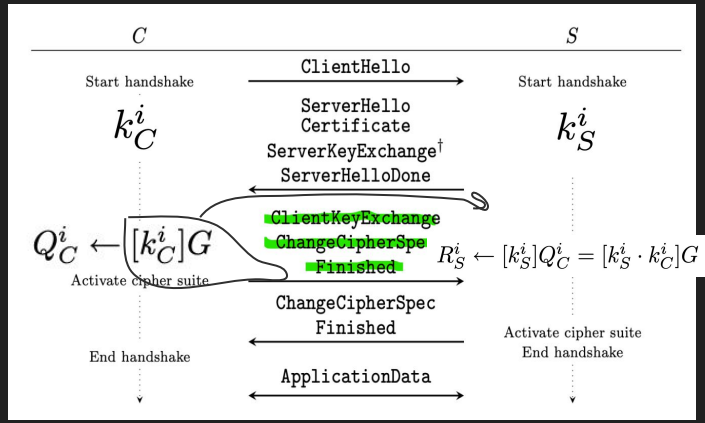
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	34.107.243.93	192.168.200.146	TLSv1.2	186	Application Data
9	0.013998756	192.168.200.146	34.149.100.209	TLSv1.2	284	Client Hello (SNI=firefox.settings.services.mozilla.com)
11	0.026172994	34.149.100.209	192.168.200.146	TLSv1.2	1466	Server Hello
14	0.026223208	34.149.100.209	192.168.200.146	TLSv1.2	1466	Certificate
15	0.026224444	34.149.100.209	192.168.200.146	TLSv1.2	338	Server Key Exchange, Server Hello Done
18	0.027388200	192.168.200.146	34.149.100.209	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
19	0.038015494	34.149.100.209	192.168.200.146	TLSv1.2	361	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
20	0.038025198	34.149.100.209	192.168.200.146	TLSv1.2	135	Application Data
22	0.038394934	192.168.200.146	34.149.100.209	TLSv1.2	243	Application Data
23	0.038469760	192.168.200.146	34.149.100.209	TLSv1.2	327	Application Data
24	0.038550009	192.168.200.146	34.149.100.209	TLSv1.2	104	Application Data
27	0.048920162	34.149.100.209	192.168.200.146	TLSv1.2	104	Application Data
28	0.050038038	34.149.100.209	192.168.200.146	TLSv1.2	395	Application Data
29	0.050052453	34.149.100.209	192.168.200.146	TLSv1.2	527	Application Data
30	0.050109680	34.149.100.209	192.168.200.146	TLSv1.2	112	Application Data
32	0.050234201	192.168.200.146	34.149.100.209	TLSv1.2	112	Application Data

```
▸ Frame 18: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits) on interface eth0, id 0
▸ Ethernet II, Src: VMware_b0:78:02 (00:50:56:b0:78:02), Dst: VMware_b0:bb:9e (00:50:56:b0:bb:9e)
▸ Internet Protocol Version 4, Src: 192.168.200.146, Dst: 34.149.100.209
▸ Transmission Control Protocol, Src Port: 43916, Dst Port: 443, Seq: 219, Ack: 4473, Len: 93
▾ Transport Layer Security
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 37
    ▾ Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 33
      ▾ EC Diffie-Hellman Client Params
          Pubkey Length: 32
          Pubkey: 858de51885ea817d887845a1ae9c49d9053bab9b7c75786542d7b16d5ac00f23
  ▾ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
      Change Cipher Spec Message
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 40
      Handshake Protocol: Encrypted Handshake Message
```

```
0000  00 50 56 b0 bb 9e 00 50  56
0010  00 91 9f a1 40 00 40 06  8a
0020  64 d1 ab 8c 01 bb 59 9b  e5
0030  00 f9 fb 4f 00 00 01 01  08
0040  f5 6a 16 03 03 00 25 10  00
0050  85 ea 81 7d 88 78 45 a1  ae
0060  7c 75 78 65 42 d7 b1 6d  5a
0070  01 01 16 03 03 00 28 00  00
0080  a8 ef 31 43 40 f1 c9 bb  c0
0090  3b 92 0e 44 2d c2 37 50  93
```

Transport Layer Security: Protocol

(attack vector)



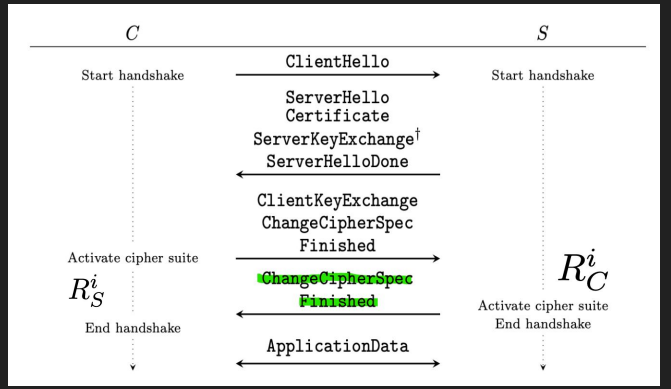
New Session Ticket, Change Cipher Spec, Encrypted Handshake

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	34.107.243.93	192.168.200.146	TLSv1.2	186	Application Data
9	0.013998756	192.168.200.146	34.149.100.209	TLSv1.2	284	Client Hello (SNI=firefox.settings.services.mozilla.com)
11	0.026172994	34.149.100.209	192.168.200.146	TLSv1.2	1466	Server Hello
14	0.026223208	34.149.100.209	192.168.200.146	TLSv1.2	1466	Certificate
15	0.026224444	34.149.100.209	192.168.200.146	TLSv1.2	338	Server Key Exchange, Server Hello Done
18	0.027388200	192.168.200.146	34.149.100.209	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
19	0.038015494	34.149.100.209	192.168.200.146	TLSv1.2	361	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
20	0.038025198	34.149.100.209	192.168.200.146	TLSv1.2	135	Application Data
22	0.038394934	192.168.200.146	34.149.100.209	TLSv1.2	243	Application Data
23	0.038469760	192.168.200.146	34.149.100.209	TLSv1.2	327	Application Data
24	0.038550009	192.168.200.146	34.149.100.209	TLSv1.2	104	Application Data
27	0.048920162	34.149.100.209	192.168.200.146	TLSv1.2	104	Application Data
28	0.050038038	34.149.100.209	192.168.200.146	TLSv1.2	395	Application Data
29	0.050052453	34.149.100.209	192.168.200.146	TLSv1.2	527	Application Data
30	0.050109680	34.149.100.209	192.168.200.146	TLSv1.2	112	Application Data
32	0.050234201	192.168.200.146	34.149.100.209	TLSv1.2	112	Application Data

```
Frame 19: 361 bytes on wire (2888 bits), 361 bytes captured (2888 bits) on interface eth0, id 0
Ethernet II, Src: VMware_b0:bb:9e (00:50:56:b0:bb:9e), Dst: VMware_b0:78:02 (00:50:56:b0:78:02)
Internet Protocol Version 4, Src: 34.149.100.209, Dst: 192.168.200.146
Transmission Control Protocol, Src Port: 443, Dst Port: 43916, Seq: 4473, Ack: 312, Len: 295
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: New Session Ticket
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 239
    Handshake Protocol: New Session Ticket
      Handshake Type: New Session Ticket (4)
      Length: 235
      TLS Session Ticket
        Session Ticket Lifetime Hint: 100800 seconds (1 day, 4 hours)
        Session Ticket Length: 229
        Session Ticket [truncated]: 02c7224989553084fb01df34cf65b1150a502a50efc96942c99e05a29f1d5ab2fb7d63a842e8b47ac08a110e70eba542ef…
  TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.2 (0x0303)
    Length: 1
    Change Cipher Spec Message
  TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 40
    Handshake Protocol: Encrypted Handshake Message
```

```
0000  00 50
0010  01 5b
0020  c8 92
0030  01 0f
0040  36 a6
0050  e5 02
0060  15 0a
0070  b2 f8
0080  42 ef
0090  d4 af
00a0  c7 04
00b0  b5 a9
00c0  b4 67
00d0  06 5a
00e0  88 b9
00f0  23 59
0100  3d 2b
0110  11 3c
0120  98 6c
0130  cb 1f
0140  28 06
0150  8f 06
0160  b3 3e
```

Transport Layer Security: Protocol



Finished message is encrypted with shared secret

Questions?