SE 4472

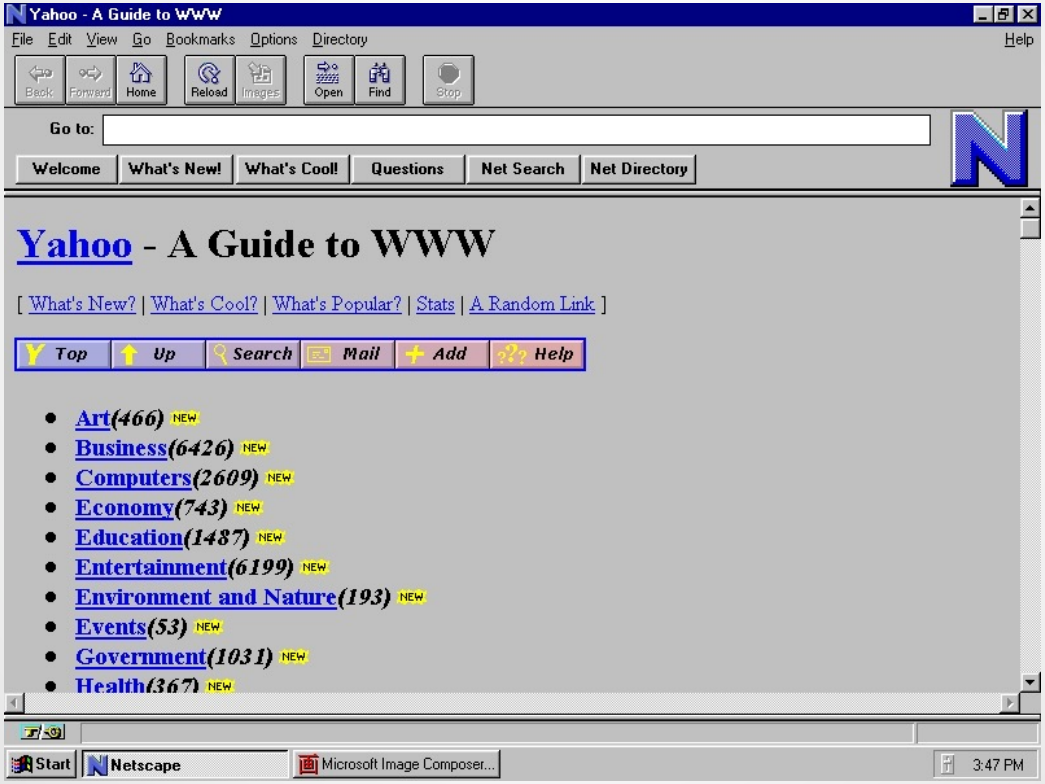
Information Security

Putting it all together:

Transport Layer Security (TLS)

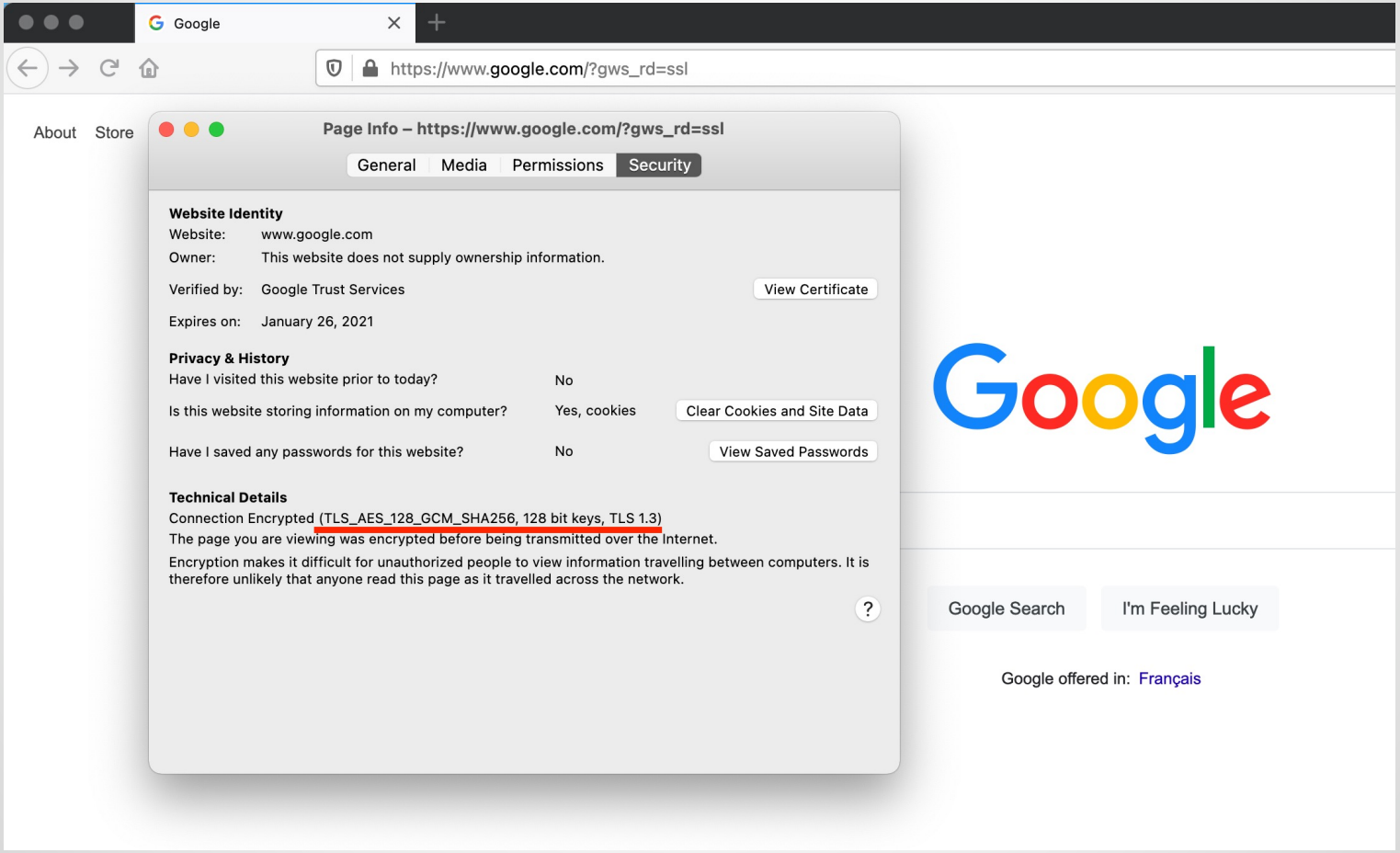
Western Engineering

Security at the Transport Layer



Where we started in this course: no security

Security at the Transport Layer



Where we've ended up in this course: practical security

Security at the Transport Layer

- TLS is the protocol that secures the web
- Combines all the concepts you've learned about so far
- HTTPS: HTTP-over-TLS
  - Eavesdropper can see you exchanging bits with a server
  - Eavesdropper cannot see Session and Presentation and Application-layer information:
    - Cannot see URL (e.g.,uwo.ca/welcome.html)
    - Cannot see cookies/auth tokens
    - Cannot see page contents

SSL/TLS History

- Secure Sockets Layer (SSL)
  - 1.0 – not released. Originally written by Taher Elgamal.
  - 2.0 – 1995. MITM possible through cipher downgrade attacks. Disallowed by IETF in 2011 (RFC 6176)
  - 3.0 – 1996. Major redesign. SHA-1 introduced. POODLE attack (Sept 2014)
- Transport Layer Security (TLS)
  - 1.0 – 1999. Different key derivation functions (HMAC)
  - 1.1 – 2006. Better IV handling mitigates CBC-mode attacks (BEAST)
  - 1.2 – 2008. SHA-256. AES-GCM
  - 1.3 – 2018. Deprecate RSA Kx. Requires forward-secrecy, authenticated encryption. Eliminates MD5, 3DES, SHA-1, CBC mode

TLS Handshake

TLS Handshake

Phases:

- Phase 1: Agree on security capabilities/parameters
- Phase 2: Public key exchange and public-key authentication (via certificates/PKI)
- Phase 3: Shared-secret and sub-key derivation
- Phase 4: Symmetric-key handshake authenication

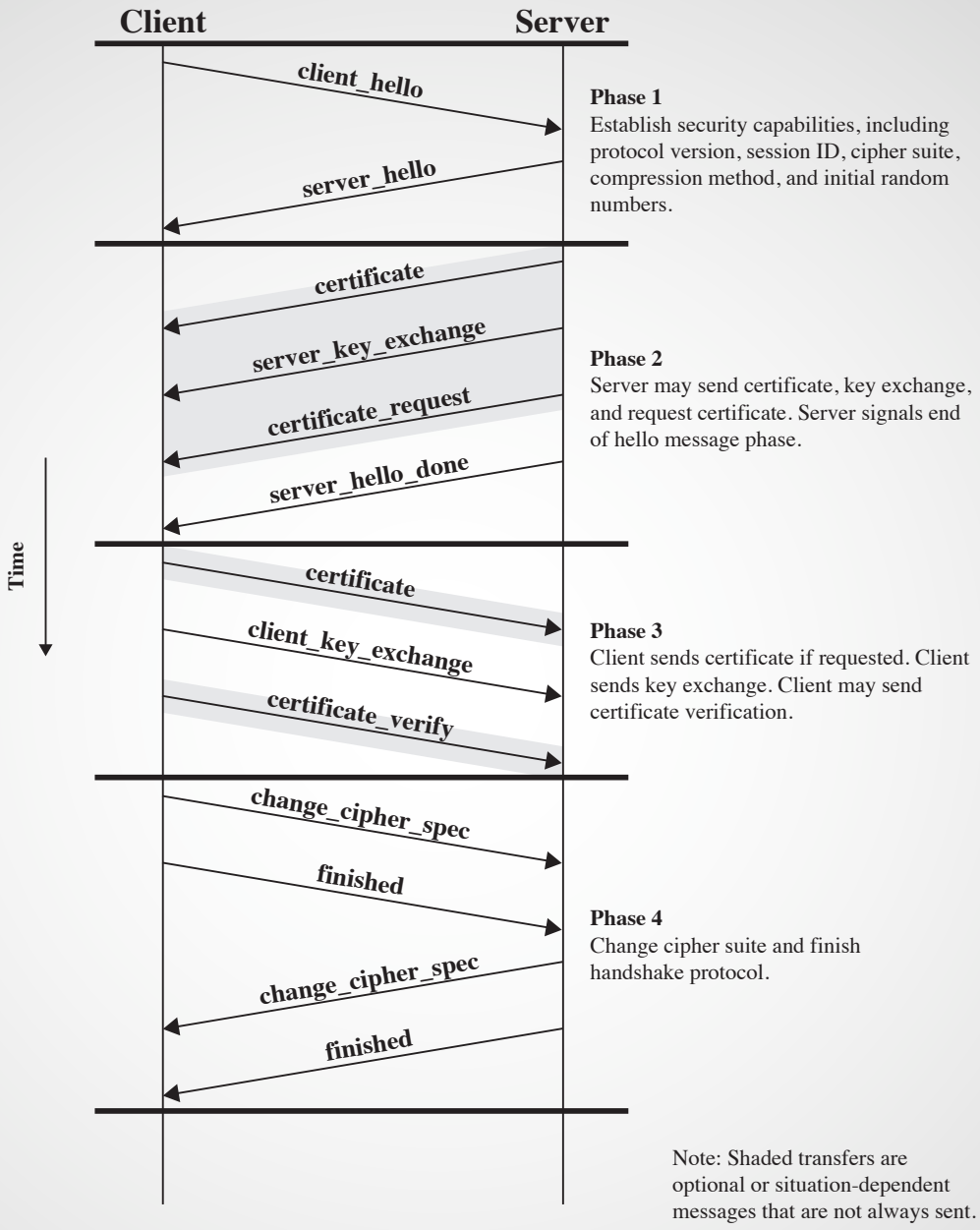


Figure 17.6 Handshake Protocol Action

Source: William Stallings. Cryptography and Network Security.

Phase 1: Security Capabilities

- Client_Hello
  - Highest SSL/TLS version supported
  - Client nonce
  - Session ID
- Server_Hello
  - Highest SSL/TLS version supported
  - Appropriate ciphersuite
    - Kx (e.g., DHE/ECDHE)
    - Cipher algorithm (e.g., AES-GCM)
    - Hash function (e.g., SHA256)
  - Server nonce

TLS Ciphersuites

Example: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

- Key agreement
  - RSA, DHE, ECDHE
- Signature scheme
  - RSA, DSA, ECDSA
- Block cipher and mode of operation
  - AES_256_CBC, 3DES_EDE, AES-GCM (i.e., AES in CTR), CHACHA20_POLY1305
- Hash function
  - SHA1, SHA256, SHA512

Firefox’s Ciphersuite Preferences

Cipher Suites (in order of preference)

TLS_AES_128_GCM_SHA256 (0x1301) Forward Secrecy	128
TLS_CHACHA20_POLY1305_SHA256 (0x1303) Forward Secrecy	256
TLS_AES_256_GCM_SHA384 (0x1302) Forward Secrecy	256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) Forward Secrecy	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) Forward Secrecy	128
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) Forward Secrecy	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) Forward Secrecy	256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) Forward Secrecy	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) Forward Secrecy	256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) **WEAK**	256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) **WEAK**	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) **WEAK**	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) **WEAK**	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) **WEAK**	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK**	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) **WEAK**	112

(1) When a browser supports SSL 2, its SSL 2-only suites are shown only on the very first connection to this site. To see the suites, close all browser windows, then open this exact page directly. Don't refresh.

TLS Ciphersuites

- The hash function is used as a pseudo-random function to derive sub-keys and as a MAC to authenticate certain messages
- What about this:
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - What is the key agreement method? What is the signature scheme? What is the Cipher?
  - What is the MAC?

Phase 2: Authentication and Public-key Exchange

- Certificate message
  - Server sends certificate chain
- Server_key_exchange
  - If using DHE/ECDHE, server sends its public key and signature

Client checks certificate chain, and signature on Pk if using DHE/ECDHE

Phase 3: Key Exchange/Derivation

1. Exchange *pre-master secret*

- If using RSA for Kx
  - Client generates 48-byte *pre-master secret*, encrypts with public key and sends to server
- If using DHE/ECDHE
  - Parties compute Diffie-Hellman shared secret (becomes *pre-master secret*)

2. Derive *master secret*

3. Derive symmetric keys
   - Use key derivation function to derive key material (see next slide)

Pseudo-random Function (PRF)

- TLS makes use of an HMAC as a PRF
- Used to expand secrets into keys
- Recall HMAC(K,m) accepts a message and a key
- First we define P_hash, which takes a secret (and a seed value) and expands it into a desired number of bytes:

```
P_hash(secret, seed) = HMAC_hash(secret, A(1) + seed) +
                       HMAC_hash(secret, A(2) + seed) +
                       HMAC_hash(secret, A(3) + seed) + ...
```

where + indicates concatenation.

A() is defined as:

```
A(0) = seed
A(i) = HMAC_hash(secret, A(i-1))
```

Pseudo-random Function (PRF)

- The PRF is constructed as follows:

  PRF(secret, label, seed) = P_<hash>(secret, label + seed)

- The label is a UTF-8 string. For example, the label "slithy toves" would be represent the following bytes:

  73 6C 69 74 68 79 20 74 6F 76 65 73

Master Secret

- Derived from the pre-master secret (either RSA or Diffie-Hellman shared secret):

```
master_secret = PRF(pre_master_secret, "master secret",
                    ClientHello.random + ServerHello.random)
                    [0..47];
```

- Used to generate the “key block”:

```
key_block = PRF(SecurityParameters.master_secret,
                "key expansion",
                SecurityParameters.server_random +
                SecurityParameters.client_random);
```

Key Block

- The key block consists of all the values used in the symmetric-key operations
- TLS generates separate keys for client and sever (though both ends have all keys):

client_write_MAC_key[SecurityParameters.mac_key_length]
server_write_MAC_key[SecurityParameters.mac_key_length]
client_write_key[SecurityParameters.enc_key_length]
server_write_key[SecurityParameters.enc_key_length]

Phase 4: Finished

- Parties exchange Finished messages
- An HMAC'd copy of everything the client (resp. the server) has seen in the handshake so far

  PRF(master_secret, finished_label, Hash(handshake_messages))

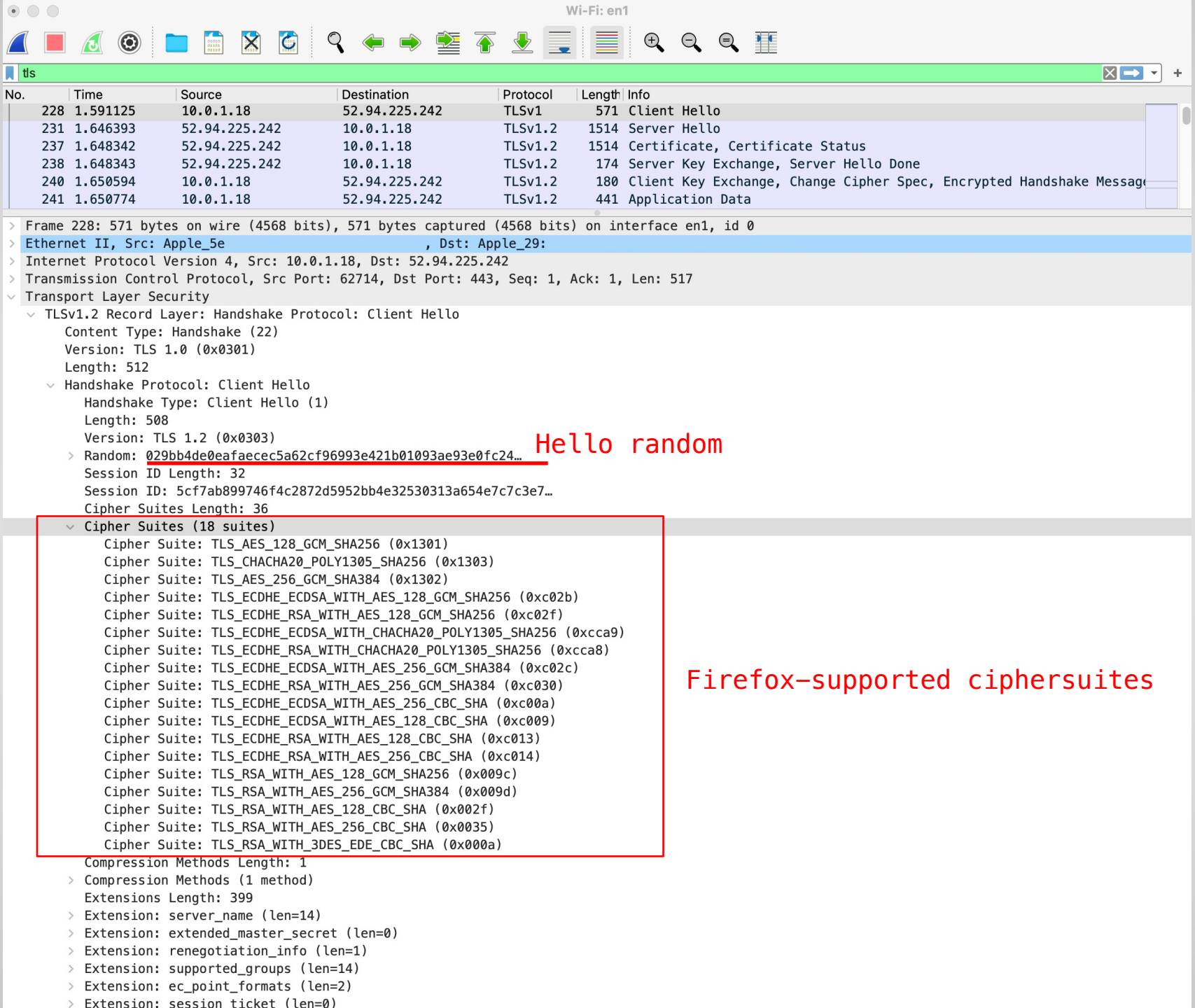
- Prevents a variety of subtle man-in-the-middle attacks
- Once client (resp. server) sends its Finished message and receives and validates the Finished message from its peer, it can start using the TLS connection.

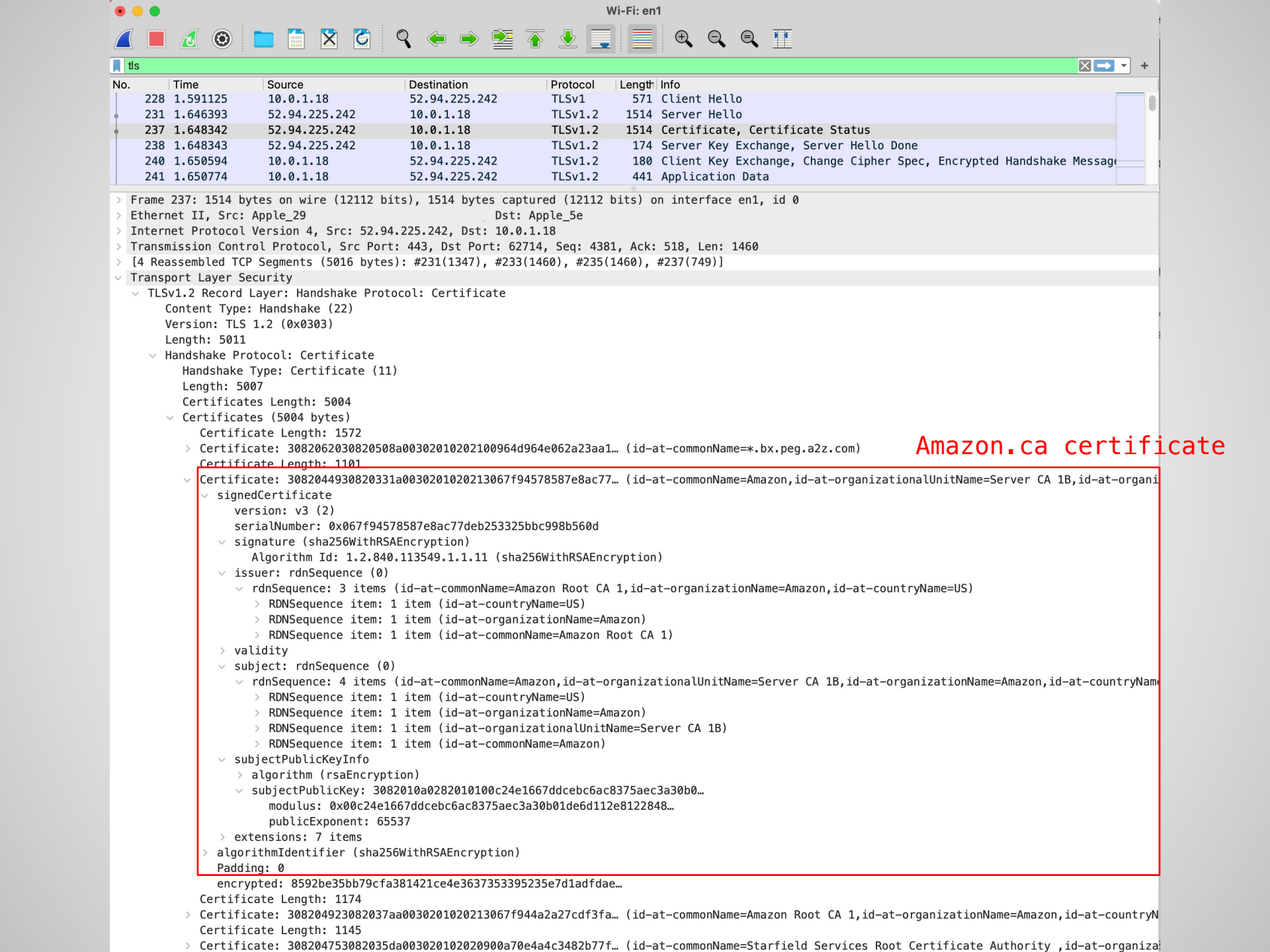
Wireshark

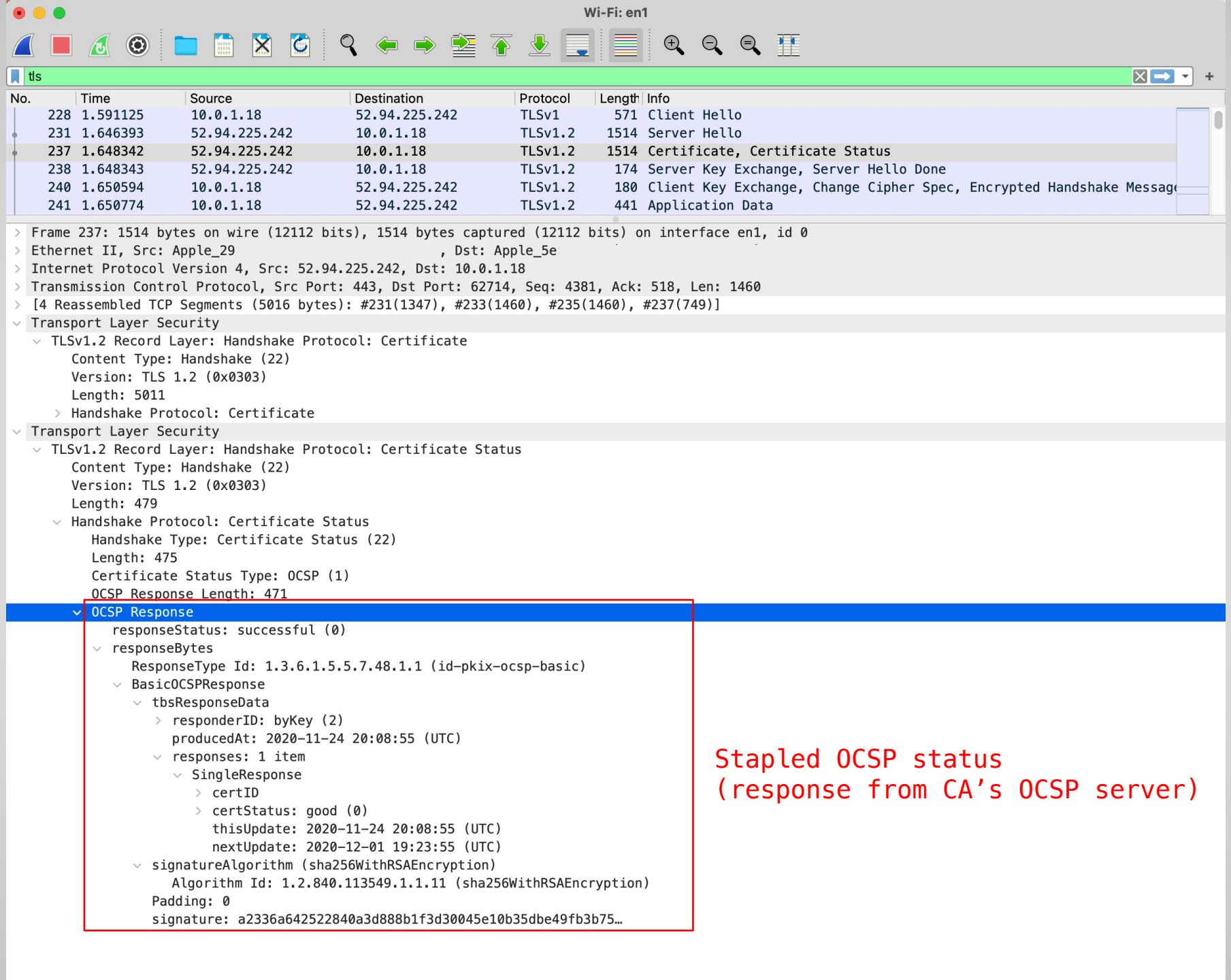
Let's see a TLS handshake in Wireshark

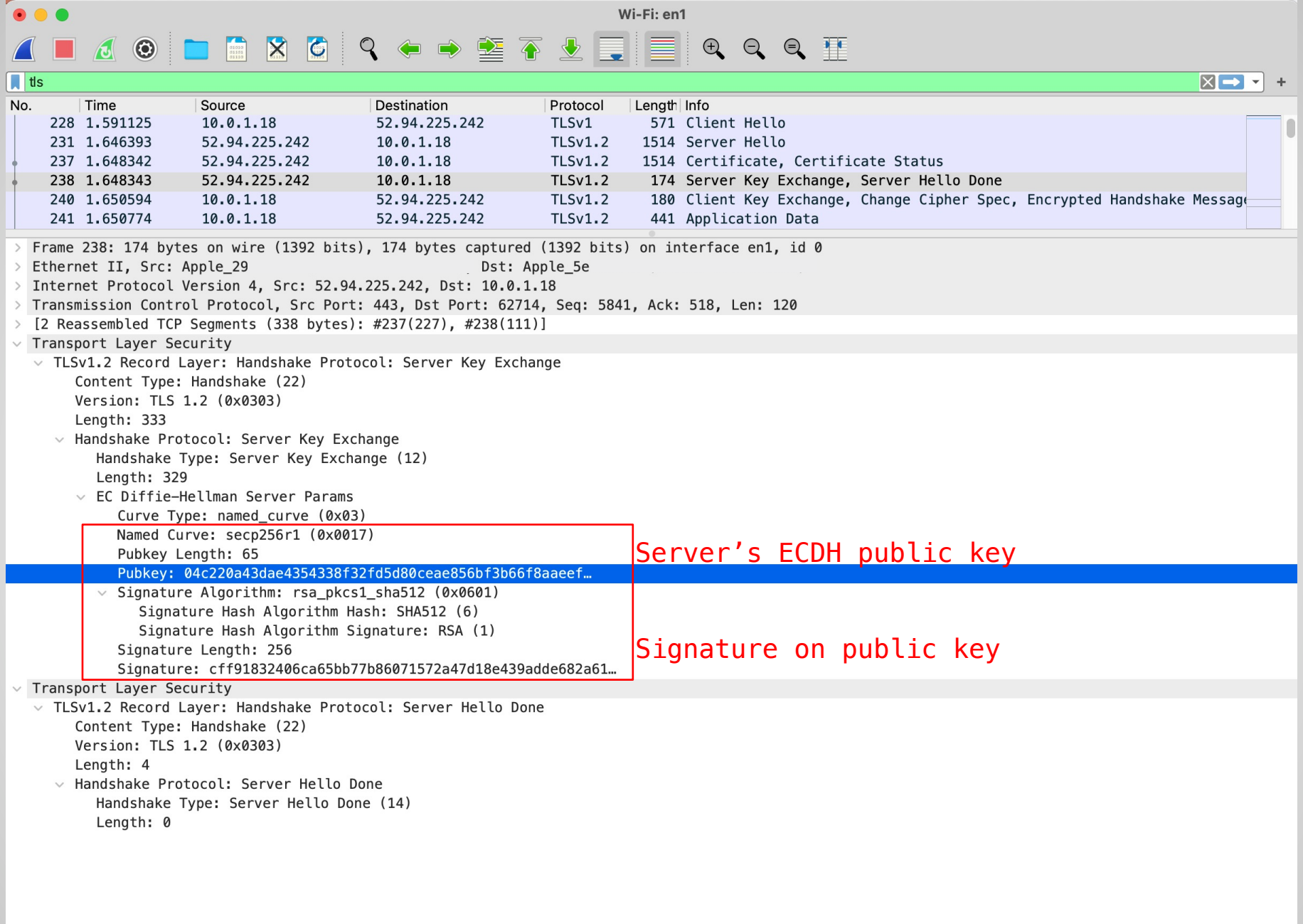
Between:

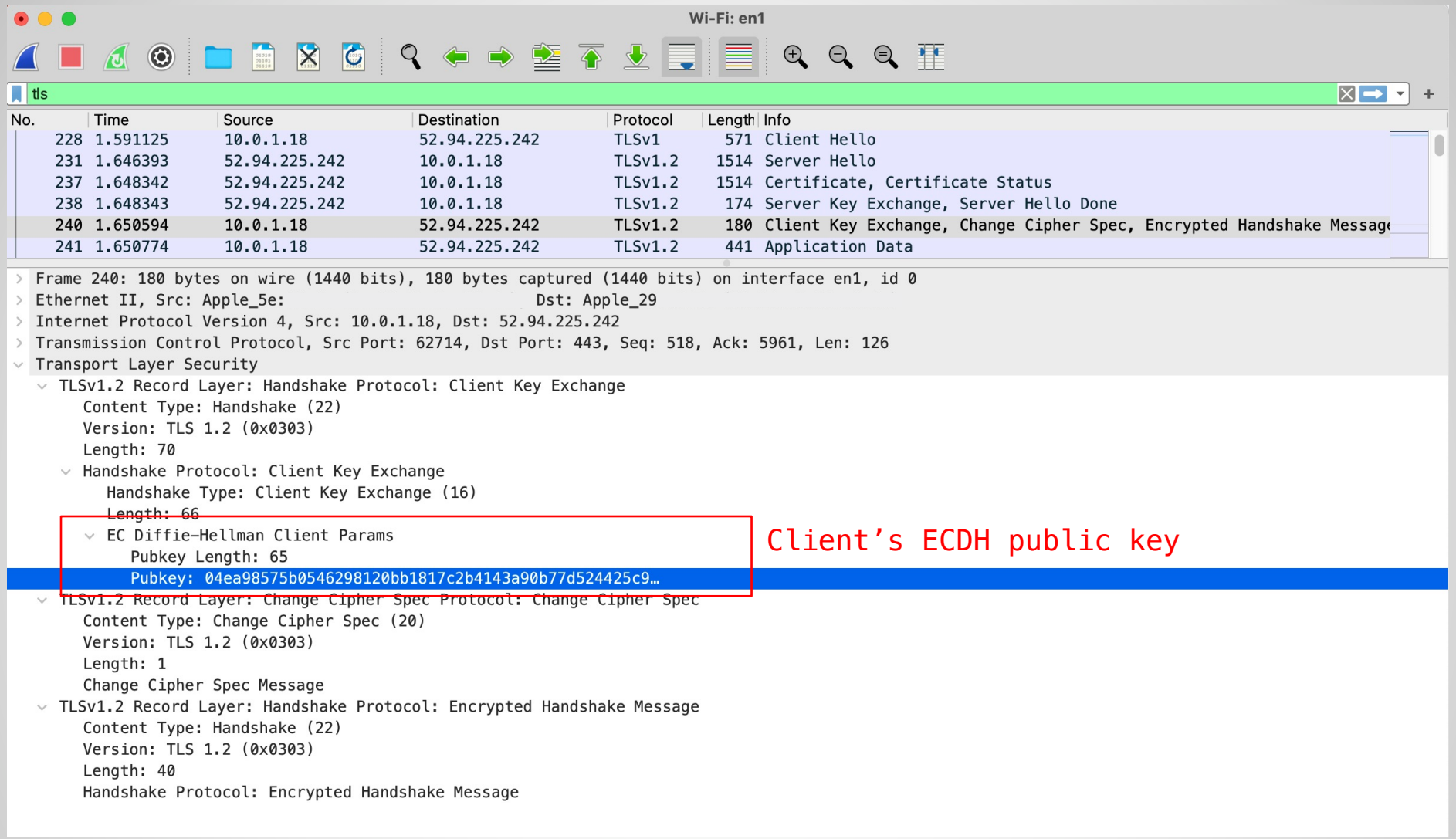
- Laptop using Firefox (10.0.1.18)
- Amazon.ca (52.94.225.242)

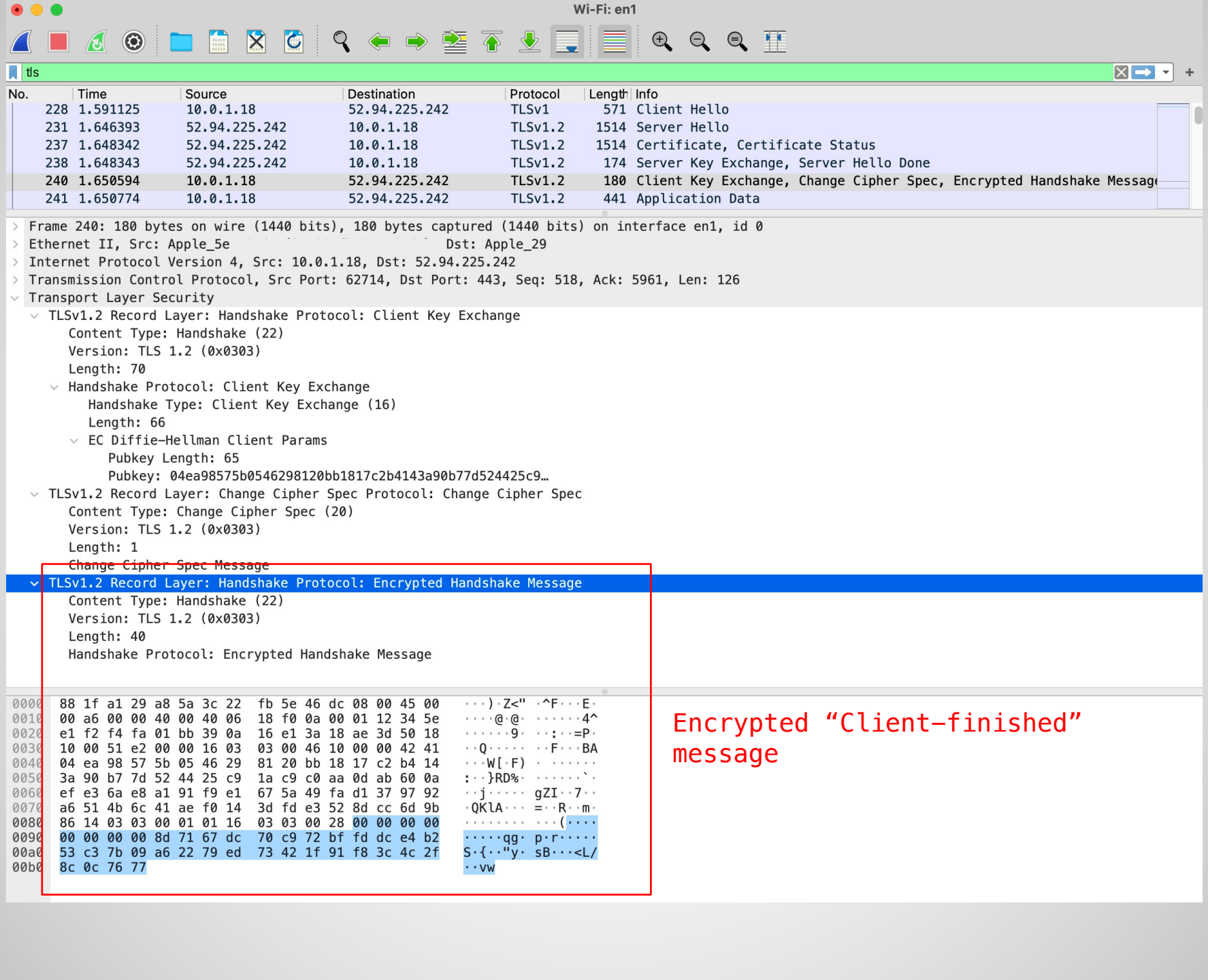

Wi-Fi: en1
tls
No. Time Source Destination Protocol Length Info
228 1.591125 10.0.1.18 52.94.225.242 TLSv1 571 Client Hello
231 1.646393 52.94.225.242 10.0.1.18 TLSv1.2 1514 Server Hello
237 1.648342 52.94.225.242 10.0.1.18 TLSv1.2 1514 Certificate, Certificate Status
238 1.648343 52.94.225.242 10.0.1.18 TLSv1.2 174 Server Key Exchange, Server Hello Done
240 1.650594 10.0.1.18 52.94.225.242 TLSv1.2 180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
241 1.650774 10.0.1.18 52.94.225.242 TLSv1.2 441 Application Data
Frame 228: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface en1, id 0
Ethernet II, Src: Apple_5e , Dst: Apple_29:
Internet Protocol Version 4, Src: 10.0.1.18, Dst: 52.94.225.242
Transmission Control Protocol, Src Port: 62714, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 512
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 508
Version: TLS 1.2 (0x0303)
Random: 029bb4de0eafaecec5a62cf96993e421b01093ae93e0fc24…
Hello random
Session ID Length: 32
Session ID: 5cf7ab899746f4c2872d5952bb4e32530313a654e7c7c3e7…
Cipher Suites Length: 36
Cipher Suites (18 suites)
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
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)
Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
Firefox-supported ciphersuites
Compression Methods Length: 1
Compression Methods (1 method)
Extensions Length: 399
Extension: server_name (len=14)
Extension: extended_master_secret (len=0)
Extension: renegotiation_info (len=1)
Extension: supported_groups (len=14)
Extension: ec_point_formats (len=2)
Extension: session_ticket (len=0)

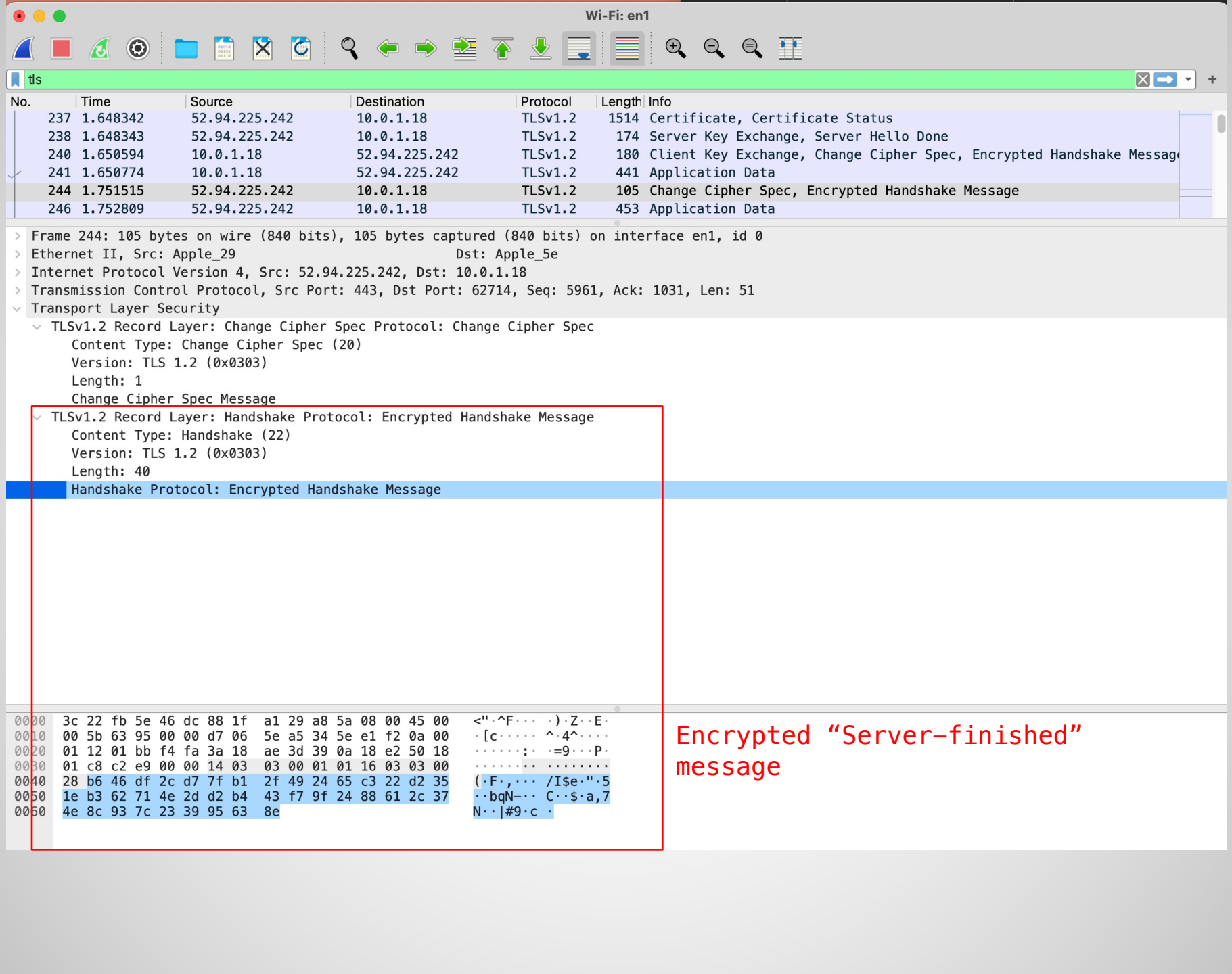

Wi-Fi: en1
tls
No. Time Source Destination Protocol Length Info
228 1.591125 10.0.1.18 52.94.225.242 TLSv1 571 Client Hello
231 1.646393 52.94.225.242 10.0.1.18 TLSv1.2 1514 Server Hello
237 1.648342 52.94.225.242 10.0.1.18 TLSv1.2 1514 Certificate, Certificate Status
238 1.648343 52.94.225.242 10.0.1.18 TLSv1.2 174 Server Key Exchange, Server Hello Done
240 1.650594 10.0.1.18 52.94.225.242 TLSv1.2 180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
241 1.650774 10.0.1.18 52.94.225.242 TLSv1.2 441 Application Data
Frame 237: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en1, id 0
Ethernet II, Src: Apple_29 Dst: Apple_5e
Internet Protocol Version 4, Src: 52.94.225.242, Dst: 10.0.1.18
Transmission Control Protocol, Src Port: 443, Dst Port: 62714, Seq: 4381, Ack: 518, Len: 1460
[4 Reassembled TCP Segments (5016 bytes): #231(1347), #233(1460), #235(1460), #237(749)]
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Certificate
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 5011
Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 5007
Certificates Length: 5004
Certificates (5004 bytes)
Certificate Length: 1572
Certificate: 3082062030820508a0030201020210096 4d964e062a23aa1… (id-at-commonName=*.bx.peg.a2z.com)
Certificate Length: 1101
Certificate: 308204430820331a0030201020213067f94578587e8ac77… (id-at-commonName=Amazon,id-at-organizationalUnitName=Server CA 1B,id-at-organi
signedCertificate
version: v3 (2)
serialNumber: 0x067f94578587e8ac77deb253325bbc998b560d
signature (sha256WithRSAEncryption)
Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
issuer: rdnSequence (0)
rdnSequence: 3 items (id-at-commonName=Amazon Root CA 1,id-at-organizationName=Amazon,id-at-countryName=US)
RDNSequence item: 1 item (id-at-countryName=US)
RDNSequence item: 1 item (id-at-organizationName=Amazon)
RDNSequence item: 1 item (id-at-commonName=Amazon Root CA 1)
validity
subject: rdnSequence (0)
rdnSequence: 4 items (id-at-commonName=Amazon,id-at-organizationalUnitName=Server CA 1B,id-at-organizationName=Amazon,id-at-countryNam
RDNSequence item: 1 item (id-at-countryName=US)
RDNSequence item: 1 item (id-at-organizationName=Amazon)
RDNSequence item: 1 item (id-at-organizationalUnitName=Server CA 1B)
RDNSequence item: 1 item (id-at-commonName=Amazon)
subjectPublicKeyInfo
algorithm (rsaEncryption)
subjectPublicKey: 3082010a0282010100c24e1667ddcebc6ac8375aec3a30b0…
modulus: 0x00c24e1667ddcebc6ac8375aec3a30b01de6d112e8122848…
publicExponent: 65537
extensions: 7 items
algorithmIdentifier (sha256WithRSAEncryption)
Padding: 0
encrypted: 8592be35bb79cfa381421ce4e3637353395235e7d1adfdae…
Certificate Length: 1174
Certificate: 308204923082037aa0030201020213067f944a2a27cdf3fa… (id-at-commonName=Amazon Root CA 1,id-at-organizationName=Amazon,id-at-countryN
Certificate Length: 1145
Certificate: 308204753082035da003020102020900a70e4a4c3482b77f… (id-at-commonName=Starfield Services Root Certificate Authority ,id-at-organiza
Amazon.ca certificate


Wi-Fi: en1
tls
No. Time Source Destination Protocol Length Info
228 1.591125 10.0.1.18 52.94.225.242 TLSv1 571 Client Hello
231 1.646393 52.94.225.242 10.0.1.18 TLSv1.2 1514 Server Hello
237 1.648342 52.94.225.242 10.0.1.18 TLSv1.2 1514 Certificate, Certificate Status
238 1.648343 52.94.225.242 10.0.1.18 TLSv1.2 174 Server Key Exchange, Server Hello Done
240 1.650594 10.0.1.18 52.94.225.242 TLSv1.2 180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
241 1.650774 10.0.1.18 52.94.225.242 TLSv1.2 441 Application Data
Frame 237: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en1, id 0
Ethernet II, Src: Apple_29 , Dst: Apple_5e
Internet Protocol Version 4, Src: 52.94.225.242, Dst: 10.0.1.18
Transmission Control Protocol, Src Port: 443, Dst Port: 62714, Seq: 4381, Ack: 518, Len: 1460
[4 Reassembled TCP Segments (5016 bytes): #231(1347), #233(1460), #235(1460), #237(749)]
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Certificate
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 5011
Handshake Protocol: Certificate
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Certificate Status
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 479
Handshake Protocol: Certificate Status
Handshake Type: Certificate Status (22)
Length: 475
Certificate Status Type: OCSP (1)
OCSP Response Length: 471
OCSP Response
responseStatus: successful (0)
responseBytes
ResponseType Id: 1.3.6.1.5.5.7.48.1.1 (id-pkix-ocsp-basic)
BasicOCSPResponse
tbsResponseData
responderID: byKey (2)
producedAt: 2020-11-24 20:08:55 (UTC)
responses: 1 item
SingleResponse
certID
certStatus: good (0)
thisUpdate: 2020-11-24 20:08:55 (UTC)
nextUpdate: 2020-12-01 19:23:55 (UTC)
signatureAlgorithm (sha256WithRSAEncryption)
Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
Padding: 0
signature: a2336a642522840a3d888b1f3d30045e10b35dbe49fb3b75…
Stapled OCSP status
(response from CA's OCSP server)


Wi-Fi: en1
tls
No. Time Source Destination Protocol Length Info
228 1.591125 10.0.1.18 52.94.225.242 TLSv1 571 Client Hello
231 1.646393 52.94.225.242 10.0.1.18 TLSv1.2 1514 Server Hello
237 1.648342 52.94.225.242 10.0.1.18 TLSv1.2 1514 Certificate, Certificate Status
238 1.648343 52.94.225.242 10.0.1.18 TLSv1.2 174 Server Key Exchange, Server Hello Done
240 1.650594 10.0.1.18 52.94.225.242 TLSv1.2 180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
241 1.650774 10.0.1.18 52.94.225.242 TLSv1.2 441 Application Data
Frame 238: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface en1, id 0
Ethernet II, Src: Apple_29 Dst: Apple_5e
Internet Protocol Version 4, Src: 52.94.225.242, Dst: 10.0.1.18
Transmission Control Protocol, Src Port: 443, Dst Port: 62714, Seq: 5841, Ack: 518, Len: 120
[2 Reassembled TCP Segments (338 bytes): #237(227), #238(111)]
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 333
Handshake Protocol: Server Key Exchange
Handshake Type: Server Key Exchange (12)
Length: 329
EC Diffie-Hellman Server Params
Curve Type: named_curve (0x03)
Named Curve: secp256r1 (0x0017)
Pubkey Length: 65
Pubkey: 04c220a43dae4354338f32fd5d80ceae856bf3b66f8aaeef…
Signature Algorithm: rsa_pkcs1_sha512 (0x0601)
Signature Hash Algorithm Hash: SHA512 (6)
Signature Hash Algorithm Signature: RSA (1)
Signature Length: 256
Signature: cff91832406ca65bb77b86071572a47d18e439adde682a61…
Server’s ECDH public key
Signature on public key
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


Wi-Fi: en1
tls
No. Time Source Destination Protocol Length Info
228 1.591125 10.0.1.18 52.94.225.242 TLSv1 571 Client Hello
231 1.646393 52.94.225.242 10.0.1.18 TLSv1.2 1514 Server Hello
237 1.648342 52.94.225.242 10.0.1.18 TLSv1.2 1514 Certificate, Certificate Status
238 1.648343 52.94.225.242 10.0.1.18 TLSv1.2 174 Server Key Exchange, Server Hello Done
240 1.650594 10.0.1.18 52.94.225.242 TLSv1.2 180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
241 1.650774 10.0.1.18 52.94.225.242 TLSv1.2 441 Application Data
Frame 240: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface en1, id 0
Ethernet II, Src: Apple_5e: Dst: Apple_29
Internet Protocol Version 4, Src: 10.0.1.18, Dst: 52.94.225.242
Transmission Control Protocol, Src Port: 62714, Dst Port: 443, Seq: 518, Ack: 5961, Len: 126
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 70
Handshake Protocol: Client Key Exchange
Handshake Type: Client Key Exchange (16)
Length: 66
EC Diffie-Hellman Client Params
Pubkey Length: 65
Pubkey: 04ea98575b0546298120bb1817c2b4143a90b77d524425c9…
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
Client’s ECDH public key


Wi-Fi: en1
tls
No. Time Source Destination Protocol Length Info
228 1.591125 10.0.1.18 52.94.225.242 TLSv1 571 Client Hello
231 1.646393 52.94.225.242 10.0.1.18 TLSv1.2 1514 Server Hello
237 1.648342 52.94.225.242 10.0.1.18 TLSv1.2 1514 Certificate, Certificate Status
238 1.648343 52.94.225.242 10.0.1.18 TLSv1.2 174 Server Key Exchange, Server Hello Done
240 1.650594 10.0.1.18 52.94.225.242 TLSv1.2 180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
241 1.650774 10.0.1.18 52.94.225.242 TLSv1.2 441 Application Data
Frame 240: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface en1, id 0
Ethernet II, Src: Apple_5e Dst: Apple_29
Internet Protocol Version 4, Src: 10.0.1.18, Dst: 52.94.225.242
Transmission Control Protocol, Src Port: 62714, Dst Port: 443, Seq: 518, Ack: 5961, Len: 126
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 70
Handshake Protocol: Client Key Exchange
Handshake Type: Client Key Exchange (16)
Length: 66
EC Diffie-Hellman Client Params
Pubkey Length: 65
Pubkey: 04ea98575b0546298120bb1817c2b4143a90b77d524425c9…
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 88 1f a1 29 a8 5a 3c 22 fb 5e 46 dc 08 00 45 00
0010 00 a6 00 00 40 00 40 06 18 f0 0a 00 01 12 34 5e
0020 e1 f2 f4 fa 01 bb 39 0a 16 e1 3a 18 ae 3d 50 18
0030 10 00 51 e2 00 00 16 03 03 00 46 10 00 00 42 41
0040 04 ea 98 57 5b 05 46 29 81 20 bb 18 17 c2 b4 14
0050 3a 90 b7 7d 52 44 25 c9 1a c9 c0 aa 0d ab 60 0a
0060 ef e3 6a e8 a1 91 f9 e1 67 5a 49 fa d1 37 97 92
0070 a6 51 4b 6c 41 ae f0 14 3d fd e3 52 8d cc 6d 9b
0080 86 14 03 03 00 01 01 16 03 03 00 28 00 00 00 00
0090 00 00 00 00 8d 71 67 dc 70 c9 72 bf fd dc e4 b2
00a0 53 c3 7b 09 a6 22 79 ed 73 42 1f 91 f8 3c 4c 2f
00b0 8c 0c 76 77
Encrypted “Client-finished” message


Wi-Fi: en1
tls
No. Time Source Destination Protocol Length Info
237 1.648342 52.94.225.242 10.0.1.18 TLSv1.2 1514 Certificate, Certificate Status
238 1.648343 52.94.225.242 10.0.1.18 TLSv1.2 174 Server Key Exchange, Server Hello Done
240 1.650594 10.0.1.18 52.94.225.242 TLSv1.2 180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
241 1.650774 10.0.1.18 52.94.225.242 TLSv1.2 441 Application Data
244 1.751515 52.94.225.242 10.0.1.18 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message
246 1.752809 52.94.225.242 10.0.1.18 TLSv1.2 453 Application Data
Frame 244: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface en1, id 0
Ethernet II, Src: Apple_29 Dst: Apple_5e
Internet Protocol Version 4, Src: 52.94.225.242, Dst: 10.0.1.18
Transmission Control Protocol, Src Port: 443, Dst Port: 62714, Seq: 5961, Ack: 1031, Len: 51
Transport Layer Security
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 3c 22 fb 5e 46 dc 88 1f a1 29 a8 5a 08 00 45 00
0010 00 5b 63 95 00 00 d7 06 5e a5 34 5e e1 f2 0a 00
0020 01 12 01 bb f4 fa 3a 18 ae 3d 39 0a 18 e2 50 18
0030 01 c8 c2 e9 00 00 14 03 03 00 01 01 16 03 03 00
0040 28 b6 46 df 2c d7 7f b1 2f 49 24 65 c3 22 d2 35
0050 1e b3 62 71 4e 2d d2 b4 43 f7 9f 24 88 61 2c 37
0060 4e 8c 93 7c 23 39 95 63 8e
Encrypted “Server-finished” message