

# ECS Knowledge Sharing

Comparison: TLS 1.3 and TLS 1.2



**Entrust Datacard™**  
Trusted Identities | Secure Transactions

# ECS KNOWLEDGE SHARING

## Comparison: TLS 1.3 and TLS 1.2

On August 10th 2018, the Internet Engineering Task Force (IETF) published TLS 1.3 as RFC 8446. This protocol officially became a new standard alongside the existing standard – TLS 1.2.

### What is TLS?

Transport Layer Security (TLS) is a protocol that provides privacy and data integrity between two communicating applications. It's the most widely deployed security protocol used today, and it's used for web browsers and other applications that require data to be securely exchanged over a network, such as file transfers, VPN connections, instant messaging and voice over IP.

### Why has IETF decided to introduce TLS 1.3?

TLS 1.2 has some pitfalls in the form of insecure protocols, ciphers and algorithms, which, even if only a slim possibility, leave room for exploitation. TLS 1.3 doesn't consist of these obsolete components and eliminates the potential risks they cause.

### What advantages does TLS 1.3 have over TLS 1.2?

#### Enhanced Security

TLS 1.3 embraces the less is more philosophy, eliminating support for older, broken forms of cryptography. This means that you can't turn on the potentially vulnerable stuff, even if you try. The list of TLS 1.2 features that have been removed is extensive, and most of the exiled features have been associated with high profile attacks. These include:

- RSA key transport: Doesn't provide perfect forward secrecy
- CBC mode ciphers: Responsible for BEAST and Lucky 13
- RC4 stream cipher: Not secure for use in HTTPS
- SHA-1 hash function: Deprecated in favor of SHA-2
- Arbitrary Diffie-Hellman groups: CVE-2016-0701
- Export ciphers: Responsible for FREAK and LogJam

TLS 1.3 removes the bad crypto smell of these legacy features, making it less likely that attacks on previous versions of the protocol will affect TLS 1.3. This streamlining also makes TLS 1.3 much easier for server operators to configure.

#### Improved Speed

With TLS 1.2, two round-trips are needed to complete the handshake before a request can be sent. Accessing a site over a mobile network can add more than half a second to its load time. With TLS 1.3, the initial handshake is cut in half, requiring only one round trip.

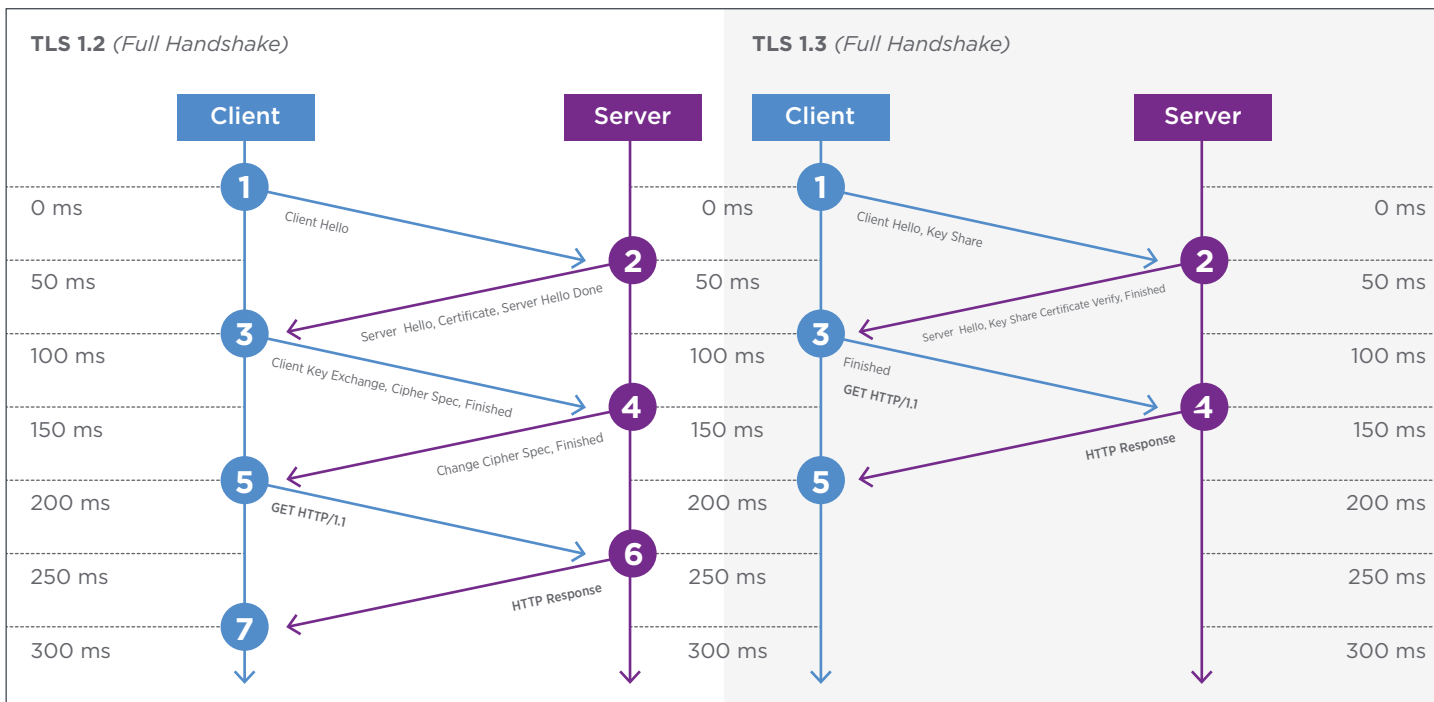
This more efficient handshake is only possible because some of the legacy features present in TLS 1.2 were removed from the protocol. TLS 1.3 also has the additional advantage that, for sites you've recently visited, you can send data on the first message to the server. This is called zero round trip mode (0-RTT) and will result in even faster load times.

# ECS KNOWLEDGE SHARING

## Comparison: TLS 1.3 and TLS 1.2

### What type of TLS certificates can accommodate TLS 1.3?

While the RSA key transport has been removed, the RSA certificates would still be allowed, but the key establishment would be via DHE or ECDHE. One of the currently available in the market for this type of cert is ECC.



### What types of cipher suites support TLS 1.3?

TLS 1.3 requires that you specify the following AEAD (Authenticated Encryption with Associated Data) ciphers. Example of the suites are below:

- TLS13-CHACHA20-POLY1305-SHA256
- TLS13-AES-256-GCM-SHA384
- TLS13-AES-128-GCM-SHA256

### Which internet browsers support TLS 1.3?

- Mozilla Firefox version 57 and onward
- Google Chrome Desktop version 63 and onward
- Google Chrome for Android version 62 and onward
- Safari on OSX High Sierra (enabled manually)

**Note:** As of September 2018, no versions of Microsoft Internet browser or Opera support TLS 1.3.

# ECS KNOWLEDGE SHARING

Comparison: TLS 1.3 and TLS 1.2

## TLS 1.2 and TLS 1.3 handshake comparison

The following is a detailed comparison of the handshake process, as viewed on Wireshark, performed on TLS 1.2 and TLS 1.3.

### I. Overview of the handshake process

TLS 1.2 (Website reference: <https://login.entrust.net>)

No.	Time	Source	Destination	Protocol	Length	Info
73	8.562098	192.168.204.154	216.191.247.148	TLSv1.2	571	Client Hello
116	8.815628	216.191.247.148	192.168.204.154	TLSv1.2	1434	Server Hello
120	8.816115	216.191.247.148	192.168.204.154	TLSv1.2	926	Certificate
122	8.818025	192.168.204.154	216.191.247.148	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
141	9.067844	216.191.247.148	192.168.204.154	TLSv1.2	60	Change Cipher Spec
163	9.513779	192.168.204.154	216.191.247.148	TLSv1.2	99	Encrypted Handshake Message
192	11.221089	192.168.204.154	216.191.247.148	TLSv1.2	999	Application Data
245	11.477458	216.191.247.148	192.168.204.154	TLSv1.2	619	Application Data
247	11.477765	192.168.204.154	216.191.247.148	TLSv1.2	1002	Application Data
273	11.731307	216.191.247.148	192.168.204.154	TLSv1.2	1198	Application Data
280	11.764480	192.168.204.154	216.191.247.148	TLSv1.2	1256	Application Data
295	12.020640	216.191.247.148	192.168.204.154	TLSv1.2	991	Application Data
319	12.944914	192.168.204.154	216.191.247.148	TLSv1.2	1218	Application Data
348	13.211355	216.191.247.148	192.168.204.154	TLSv1.2	590	Application Data
378	13.476516	216.191.247.148	192.168.204.154	TLSv1.2	1434	Application Data
379	13.476517	216.191.247.148	192.168.204.154	TLSv1.2	1471	Application Data
383	13.525672	192.168.204.154	216.191.247.148	TLSv1.2	1351	Application Data

Step	Client	Direction	Message	Direction	Server
1			Client Hello		
2			Server Hello		
3			Certificate		
4			Server Key Exchange		
5			Server Hello Done		
6			Client Key Exchange		
7			Change Cipher Spec		
8			Finished		
9			Change Cipher Spec		
10			Finished		

# ECS KNOWLEDGE SHARING

## Comparison: TLS 1.3 and TLS 1.2

TLS 1.3 (Website reference: <https://www.cloudflare.com>)

No.	Time	Source	Destination	Protocol	Length	Info
135	4.866673	192.168.204.205	198.41.215.162	TLSv1.3	571	Client Hello
137	4.870211	198.41.215.162	192.168.204.205	TLSv1.3	1506	Server Hello, Change Cipher Spec
139	4.870263	198.41.215.162	192.168.204.205	TLSv1.3	483	Application Data
141	4.871355	192.168.204.205	198.41.215.162	TLSv1.3	118	Change Cipher Spec, Application Data
143	4.873424	198.41.215.162	192.168.204.205	TLSv1.3	582	Application Data, Application Data
145	4.937911	192.168.204.205	198.41.215.162	TLSv1.3	140	Application Data
147	4.938448	192.168.204.205	198.41.215.162	TLSv1.3	85	Application Data
148	4.938604	192.168.204.205	198.41.215.162	TLSv1.3	315	Application Data
151	4.940057	198.41.215.162	192.168.204.205	TLSv1.3	85	Application Data

Step	Client	Direction	Message	Direction	Server
1			Client Hello Supported Cipher Suite Guesses Key Agreement Protocol Key Share		
2			Server Hello Key Agreement Protocol Key Share Server Finished		
3			Checks Certificate Generates Keys Client Finished		

# ECS KNOWLEDGE SHARING

## Comparison: TLS 1.3 and TLS 1.2

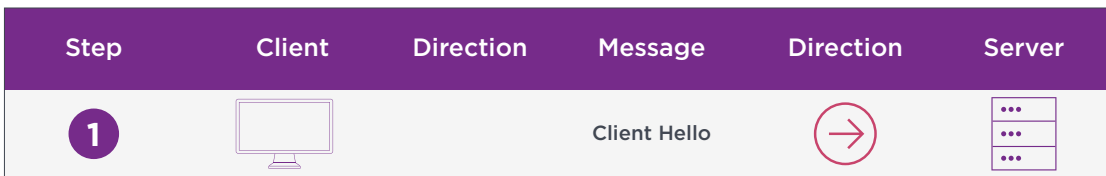
### II. Breakdown of the handshake process

#### TLS 1.2

##### 1. Client Hello

The image shows a Wireshark packet capture of a TLS 1.2 Client Hello message. The packet list pane shows three packets: a Client Hello (73), a Server Hello (116), and a Certificate (120). The packet details pane for packet 73 shows the following structure:

- Frame 73: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface 0
- Ethernet II, Src: Vmware\_d0:b8:3e (00:0c:29:d0:b8:3e), Dst: Vmware\_e1:6b:2b (00:50:56:e1:6b:2b)
- Internet Protocol Version 4, Src: 192.168.204.154, Dst: 216.191.247.148
- Transmission Control Protocol, Src Port: 50757 (50757), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 517
- Secure Sockets Layer
  - 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
        - Session ID Length: 32
        - Session ID: d4119cbab7e0ac8b885f10e6b0705c9a6f042695ff181b8c...
        - Cipher Suites Length: 28
        - Cipher Suites (14 suites)
        - Compression Methods Length: 1
        - Compression Methods (1 method)
        - Extensions Length: 407
        - Extension: server\_name
        - Extension: Extended Master Secret
        - Extension: renegotiation\_info
        - Extension: elliptic\_curves
        - Extension: ec\_point\_formats
        - Extension: SessionTicket TLS
        - Extension: Application Layer Protocol Negotiation
        - Extension: status\_request
        - Extension: Unknown 51
        - Extension: Unknown 43
        - Extension: signature\_algorithms
        - Extension: Unknown 45
        - Extension: Padding



# ECS KNOWLEDGE SHARING

## Comparison: TLS 1.3 and TLS 1.2

### 2. Server Hello

The image shows a Wireshark packet capture window titled 'ssl capture.pcapng'. The main pane displays a list of captured packets. Packet 116 is highlighted, showing a 'Server Hello' message from 216.191.247.148 to 192.168.204.154. The packet details pane is expanded to show the 'Handshake Protocol: Server Hello' structure. The 'Handshake Type' is 'Server Hello (2)' and the 'Version' is 'TLS 1.2 (0x0303)'. The 'Random' field contains a long hexadecimal string. The 'Session ID Length' is 32, and the 'Session ID' is '92c894e2e60d09c67b90ac844e55b04e547ead67e12a5443...'. The 'Cipher Suite' is 'TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc030)'. The 'Compression Method' is 'null (0)'. The 'Extensions Length' is 11, with extensions for 'renegotiation\_info' and 'ec\_point\_formats'.

No.	Time	Source	Destination	Protocol	Length	Info
73	8.562098	192.168.204.154	216.191.247.148	TLSv1.2	571	Client Hello
116	8.815628	216.191.247.148	192.168.204.154	TLSv1.2	1434	Server Hello
120	8.816115	216.191.247.148	192.168.204.154	TLSv1.2	926	Certificate
122	8.818025	192.168.204.154	216.191.247.148	TLSv1.2	188	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
141	9.0678					
163	9.5137					
192	11.221					
245	11.477					
247	11.477					
273	11.731					
280	11.764					
295	12.020					
319	12.944					

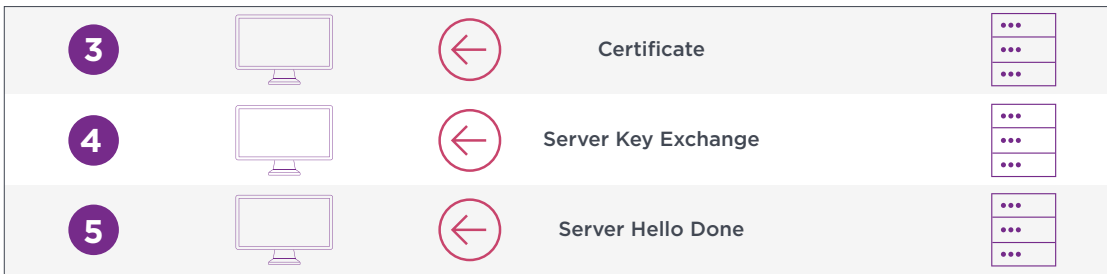
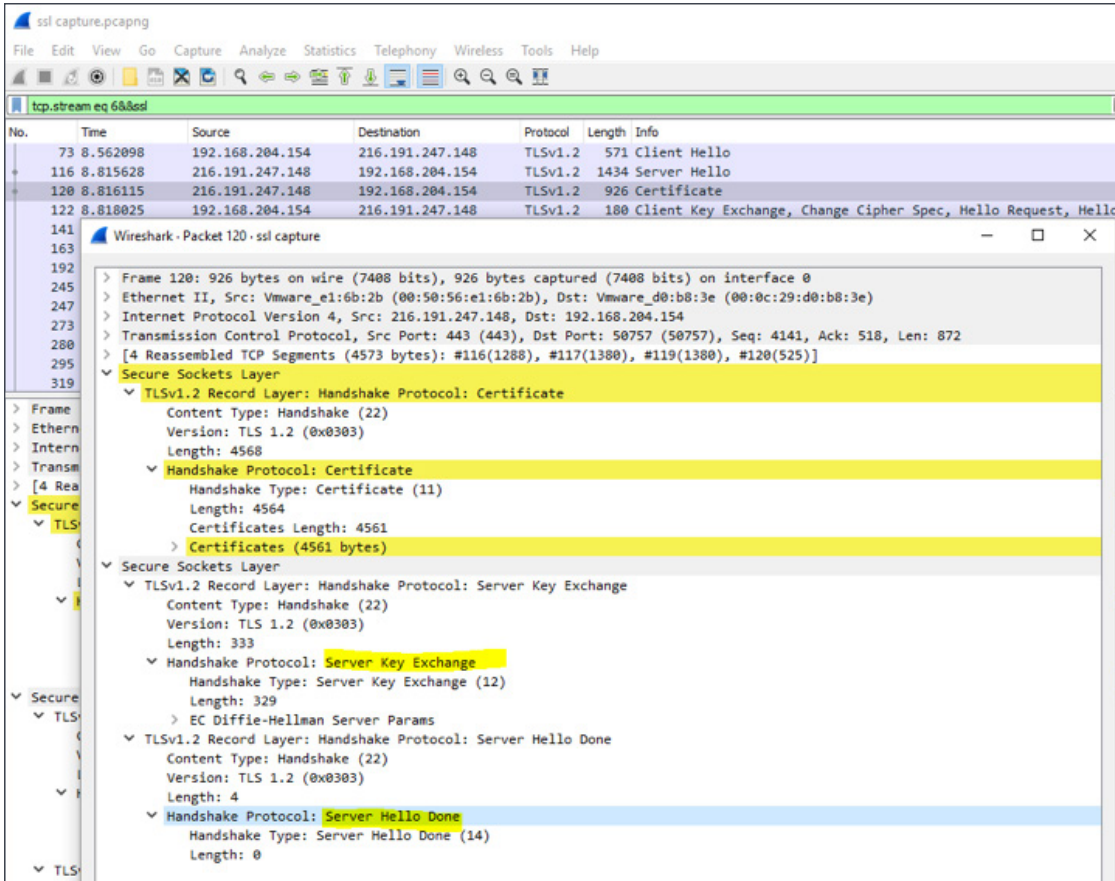
2   Server Hello 

# ECS KNOWLEDGE SHARING

## Comparison: TLS 1.3 and TLS 1.2

### 3. Certificate

- a. Server Key Exchange
- b. Server Hello Done



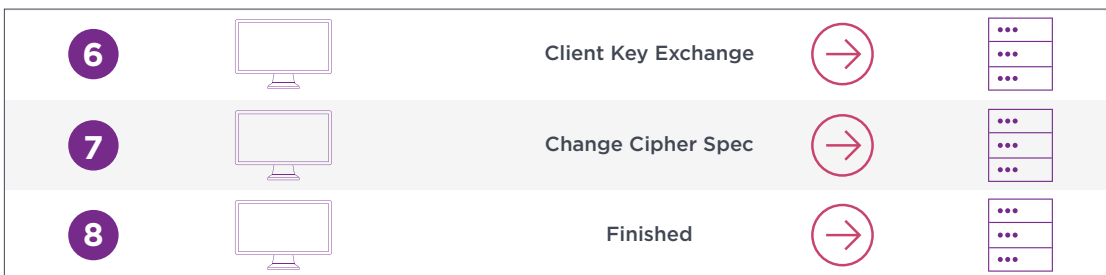
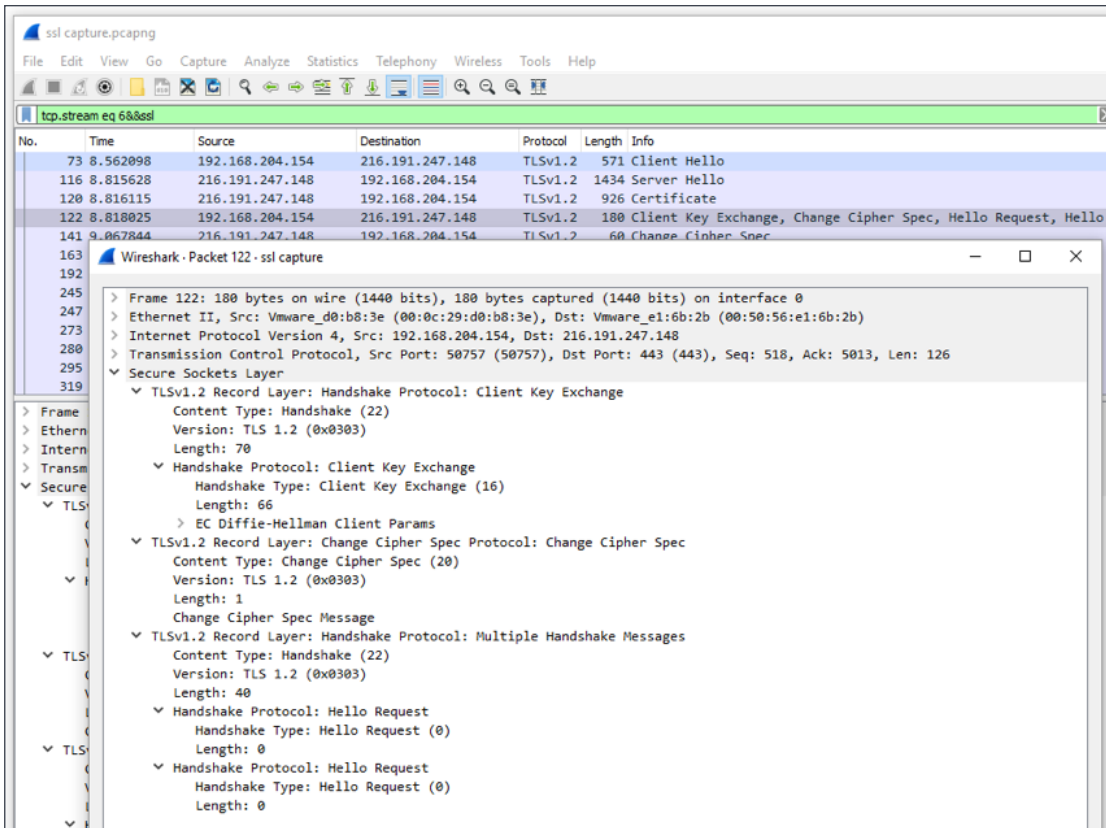


# ECS KNOWLEDGE SHARING

## Comparison: TLS 1.3 and TLS 1.2

### 4. Client Key Exchange

- a. Change Cipher Spec
- b. Finished

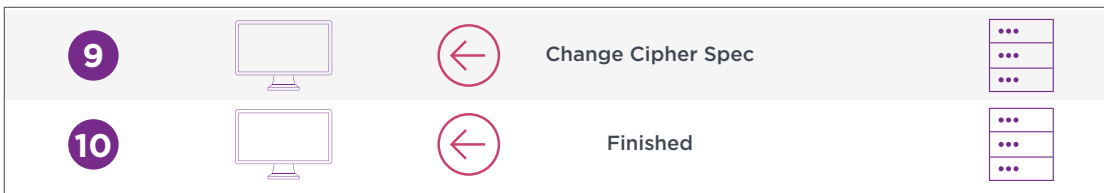
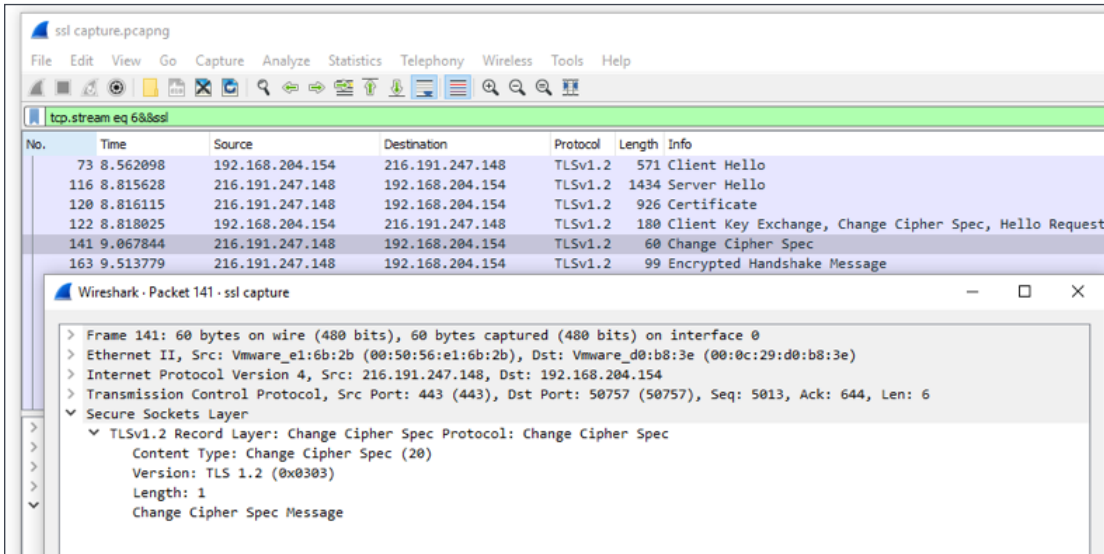


# ECS KNOWLEDGE SHARING

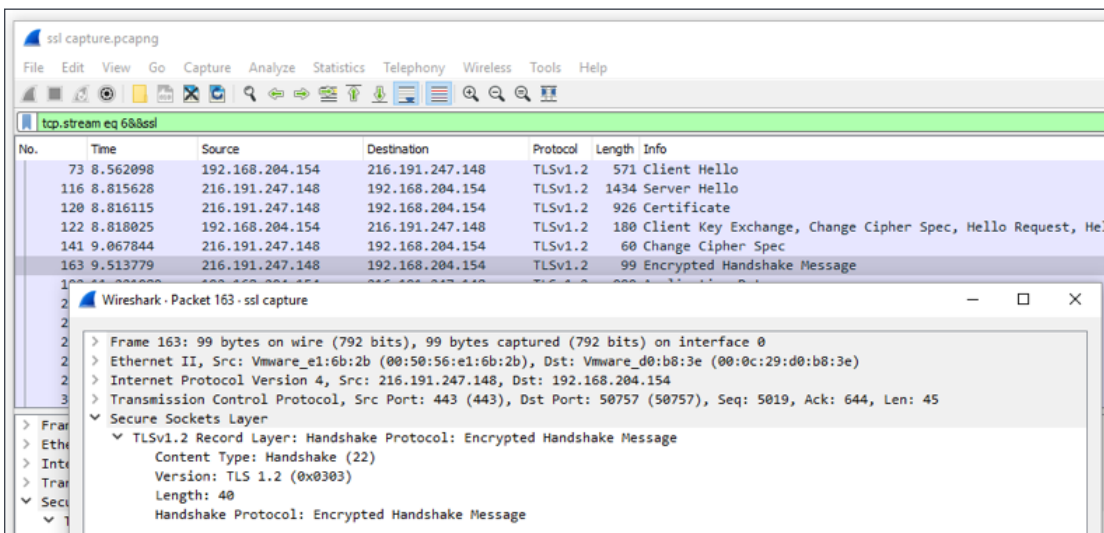
## Comparison: TLS 1.3 and TLS 1.2

### 5. Change Cipher Spec

#### a. Finished



### 6. Encrypted Handshake Message



# ECS KNOWLEDGE SHARING

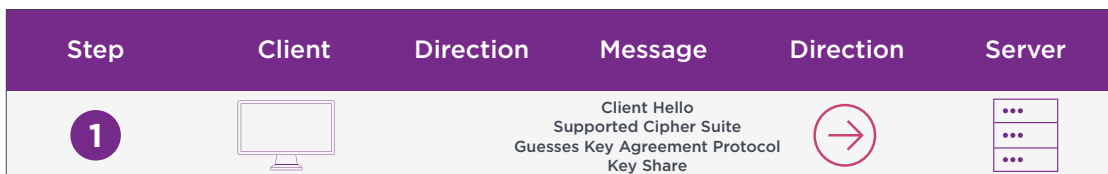
## Comparison: TLS 1.3 and TLS 1.2

### TLS 1.3

1. Client Hello, Supported Cipher Suites, Guesses Key Agreement Protocol, Key Share

The image shows a Wireshark packet capture of a TLS 1.3 Client Hello message. The packet is 571 bytes long and is captured on interface 0. The details pane shows the following structure:

- Secure Sockets Layer
  - TLSv1.3 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: 488ee7183154c2e37876b4dad8ec79ffe4cc658e4a1a8d0d...
      - Session ID Length: 32
      - Session ID: 808dab12a95428d1dd13c6a8b92501a570300d7ac8e500d5...
      - Cipher Suites Length: 34
      - Cipher Suites (17 suites)
      - Compression Methods Length: 1
      - Compression Methods (1 method)
      - Extensions Length: 401
      - Extension: Reserved (GREASE) (len=0)
      - Extension: renegotiation\_info (len=1)
      - Extension: server\_name (len=23)
      - Extension: extended\_master\_secret (len=0)
      - Extension: SessionTicket TLS (len=0)
      - Extension: signature\_algorithms (len=20)
      - Extension: status\_request (len=5)
      - Extension: signed\_certificate\_timestamp (len=0)
      - Extension: application\_layer\_protocol\_negotiation (len=14)
      - Extension: channel\_id (len=0)
      - Extension: ec\_point\_formats (len=2)
      - Extension: key\_share (len=43)
      - Extension: psk\_key\_exchange\_modes (len=2)
      - Extension: supported\_versions (len=11)
      - Extension: supported\_groups (len=10)
      - Extension: Reserved (GREASE) (len=1)
      - Extension: padding (len=201)



# ECS KNOWLEDGE SHARING

## Comparison: TLS 1.3 and TLS 1.2




### 2. Server Hello, Key Agreement Protocol, Key Share, Server Finished

The screenshot shows a Wireshark packet capture of a TLS 1.2 Server Hello message. The packet list pane shows three packets: a Client Hello (571 bytes), a Server Hello (1506 bytes), and Application Data (483 bytes). The packet details pane for packet 137 shows the following structure:

- Frame 137: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits) on interface 0
- Ethernet II, Src: Vmware\_e1:6b:2b (00:50:56:e1:6b:2b), Dst: Vmware\_d0:b8:3e (00:0c:29:d0:b8:3e)
- Internet Protocol Version 4, Src: 198.41.215.162, Dst: 192.168.204.205
- Transmission Control Protocol, Src Port: 443, Dst Port: 49756, Seq: 1, Ack: 518, Len: 1452
- Secure Sockets Layer
  - TLSv1.3 Record Layer: Handshake Protocol: Server Hello
    - Content Type: Handshake (22)
    - Version: TLS 1.2 (0x0303)
    - Length: 122
      - Handshake Protocol: Server Hello
        - Handshake Type: Server Hello (2)
        - Length: 118
        - Version: TLS 1.2 (0x0303)
        - Random: 10c18a16f3c7d5d82abdd35fcdc8d72f43bb627d8aef7a08...
        - Session ID Length: 32
        - Session ID: 808dab12a95428d1dd13c6a8b92501a570300d7ac8e500d5...
        - Cipher Suite: TLS\_AES\_128\_GCM\_SHA256 (0x1301)
        - Compression Method: null (0)
        - Extensions Length: 46
          - Extension: key\_share (len=36)
          - Extension: supported\_versions (len=2)
- TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec

The screenshot shows a Wireshark packet capture of a TLS 1.2 Application Data message. The packet list pane shows three packets: a Client Hello (571 bytes), a Server Hello (1506 bytes), and Application Data (483 bytes). The packet details pane for packet 139 shows the following structure:

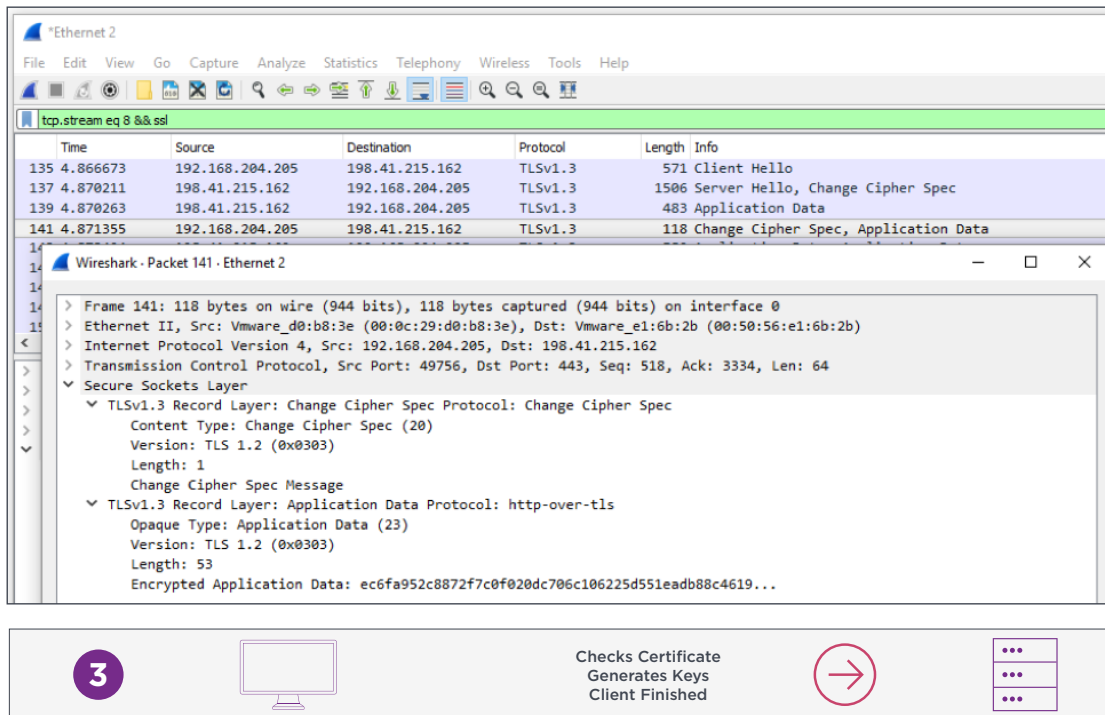
- Frame 139: 483 bytes on wire (3864 bits), 483 bytes captured (3864 bits) on interface 0
- Ethernet II, Src: Vmware\_e1:6b:2b (00:50:56:e1:6b:2b), Dst: Vmware\_d0:b8:3e (00:0c:29:d0:b8:3e)
- Internet Protocol Version 4, Src: 198.41.215.162, Dst: 192.168.204.205
- Transmission Control Protocol, Src Port: 443, Dst Port: 49756, Seq: 2905, Ack: 518, Len: 429
- [3 Reassembled TCP Segments (3200 bytes): #137(1319), #138(1452), #139(429)]
- Secure Sockets Layer
  - TLSv1.3 Record Layer: Application Data Protocol: http-over-tls
    - Opaque Type: Application Data (23)
    - Version: TLS 1.2 (0x0303)
    - Length: 3195
    - Encrypted Application Data: 6f199b6c1195f28bbd4af386293c1ac2772c2c2f0ad8cd51...

2   Server Hello  
Key Agreement Protocol  
Key Share  
Server Finished 

# ECS KNOWLEDGE SHARING

## Comparison: TLS 1.3 and TLS 1.2

### 3. Checks Certificate, Generate Keys, Client Finished



The image displays a Wireshark network capture of a TLS 1.3 handshake. The main capture window shows a list of packets with the following details:

Time	Source	Destination	Protocol	Length	Info
135	4.866673	192.168.204.205	198.41.215.162	TLSv1.3	571 Client Hello
137	4.870211	198.41.215.162	192.168.204.205	TLSv1.3	1506 Server Hello, Change Cipher Spec
139	4.870263	198.41.215.162	192.168.204.205	TLSv1.3	483 Application Data
141	4.871355	192.168.204.205	198.41.215.162	TLSv1.3	118 Change Cipher Spec, Application Data

The packet details pane for packet 141 shows the following structure:

- Frame 141: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
- Ethernet II, Src: Vmware\_d0:b8:3e (00:0c:29:d0:b8:3e), Dst: Vmware\_e1:6b:2b (00:50:56:e1:6b:2b)
- Internet Protocol Version 4, Src: 192.168.204.205, Dst: 198.41.215.162
- Transmission Control Protocol, Src Port: 49756, Dst Port: 443, Seq: 518, Ack: 3334, Len: 64
- Secure Sockets Layer
  - TLSv1.3 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
  - TLSv1.3 Record Layer: Application Data Protocol: http-over-tls
    - Opaque Type: Application Data (23)
    - Version: TLS 1.2 (0x0303)
    - Length: 53
    - Encrypted Application Data: ec6fa952c8872f7c0f020dc706c106225d551eadb88c4619...

**NOTE:** As you can see on the Wireshark log file captured above, TLS 1.3 is definitely simpler and more secure since all the exchange information between the client and server is now encrypted as well as other information such as certificates, key agreement protocols and cipher suites agreement.

## Summary

Just like with HTTP/2, TLS 1.3 is another exciting protocol update that we can expect to benefit from for years to come. Not only will encrypted (HTTPS) connections become faster, but they will also be more secure. Here's to moving the web forward.

## External Reading

If you'd like to learn more about TLS 1.3 and its security improvements, check out some of the recommended reading below.

- F5 DevCentral: [Explaining TLS 1.3](#)
- The SSL Store: [The IETF has FINALLY published TLS 1.3 as RFC 8446](#)
- IETF Datatracker: [The Transport Layer Security \(TLS\) Protocol Version 1.3](#)
- CloudFlare: [Introducing TLS 1.3](#)
- The Inquirer: [IETF drops RSA key transport from TLS 1.3](#)
- The Register: [World celebrates, cyber-snoops cry as TLS 1.3 internet crypto approved](#)
- The SSL Store: [TLS 1.3 Handshake: Taking a Closer Look](#)

## About Entrust Datacard Corporation

Consumers, citizens and employees increasingly expect anywhere-anytime experiences—whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

For more information about Entrust Datacard products and services, call **888-690-2424**, email [sales@entrustdatacard.com](mailto:sales@entrustdatacard.com) or visit [entrustdatacard.com](http://entrustdatacard.com).



### Corporate Headquarters

U.S. Toll-Free Phone: 1-888-690-2424  
International Phone: +1-952-933-1223  
[info@entrustdatacard.com](mailto:info@entrustdatacard.com)  
[entrustdatacard.com](http://entrustdatacard.com)

Entrust Datacard and Datacard are trademarks, hexagon design are registered trademarks and/or service marks of Entrust Datacard Corporation in the United States and/or other countries.

©2018 Entrust Datacard Corporation. All rights reserved. SL19-1019-001