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.

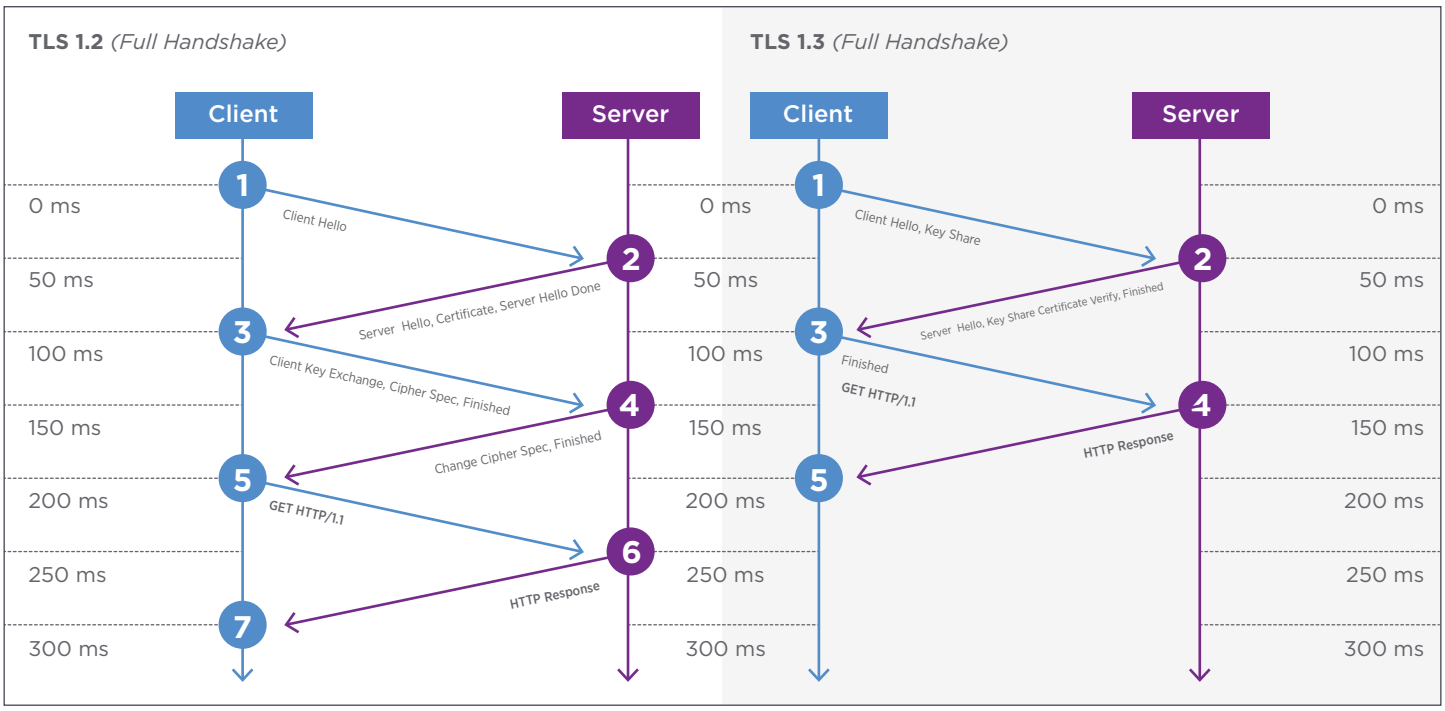
Improved Speed

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.

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)

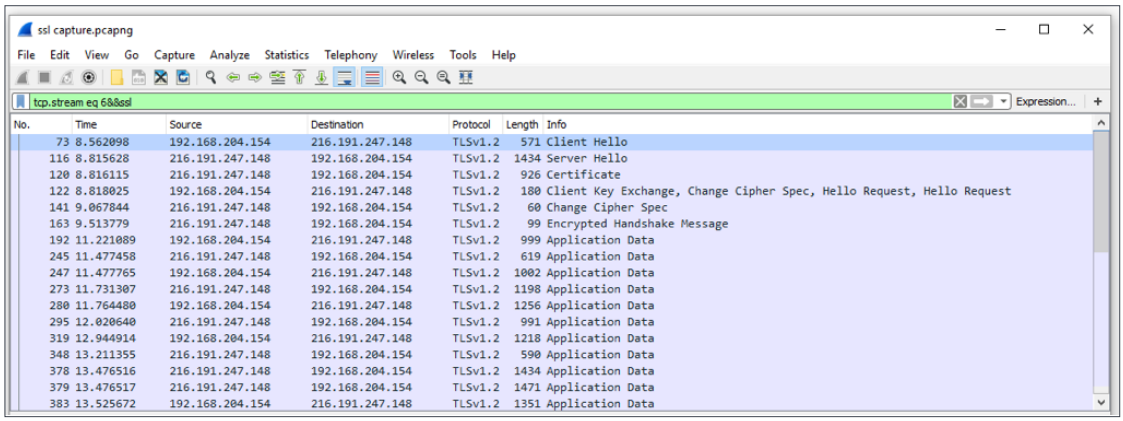
Note: ***As of September 2018, no versions of Microsoft Internet browser or Opera support TLS 1.3.***

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)



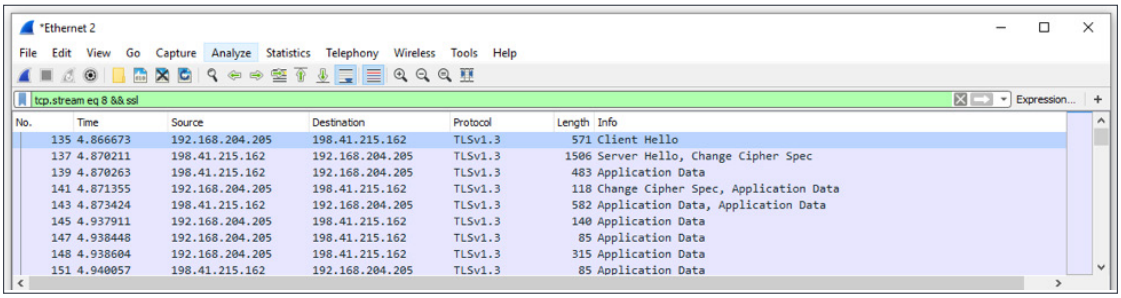
No.	Time	Source	Destination	Protocol	Length	Info
73	8.562098	192.168.204.154	216.191.247.148	TLSv1.2	571	Client Hello
116	8.815628	216.191.247.148	192.168.204.154	TLSv1.2	1434	Server Hello
120	8.816115	216.191.247.148	192.168.204.154	TLSv1.2	926	Certificate
122	8.818025	192.168.204.154	216.191.247.148	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	216.191.247.148	192.168.204.154	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

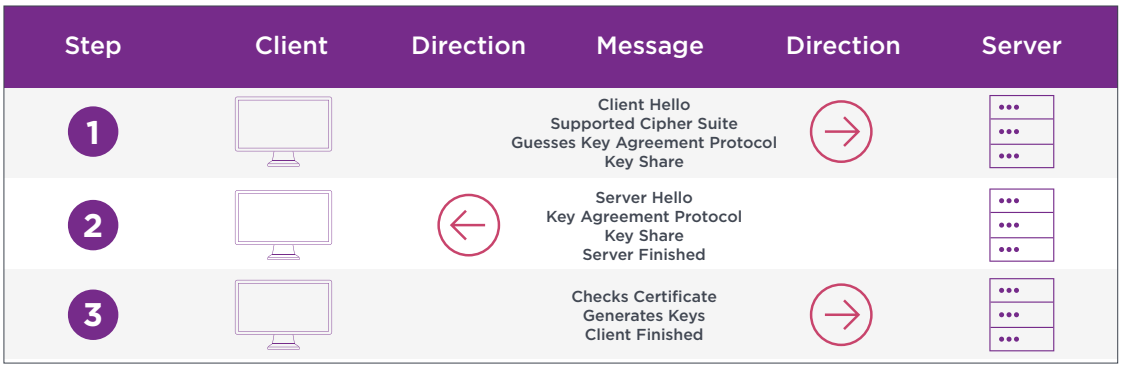
Step	Client	Direction	Message	Direction	Server
1			Client Hello	→	
2		←	Server Hello		
3		←	Certificate		
4		←	Server Key Exchange		
5		←	Server Hello Done		
6			Client Key Exchange	→	
7			Change Cipher Spec	→	
8			Finished	→	
9		←	Change Cipher Spec		
10		←	Finished		

ECS KNOWLEDGE SHARING

Comparison: TLS 1.3 and TLS 1.2

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

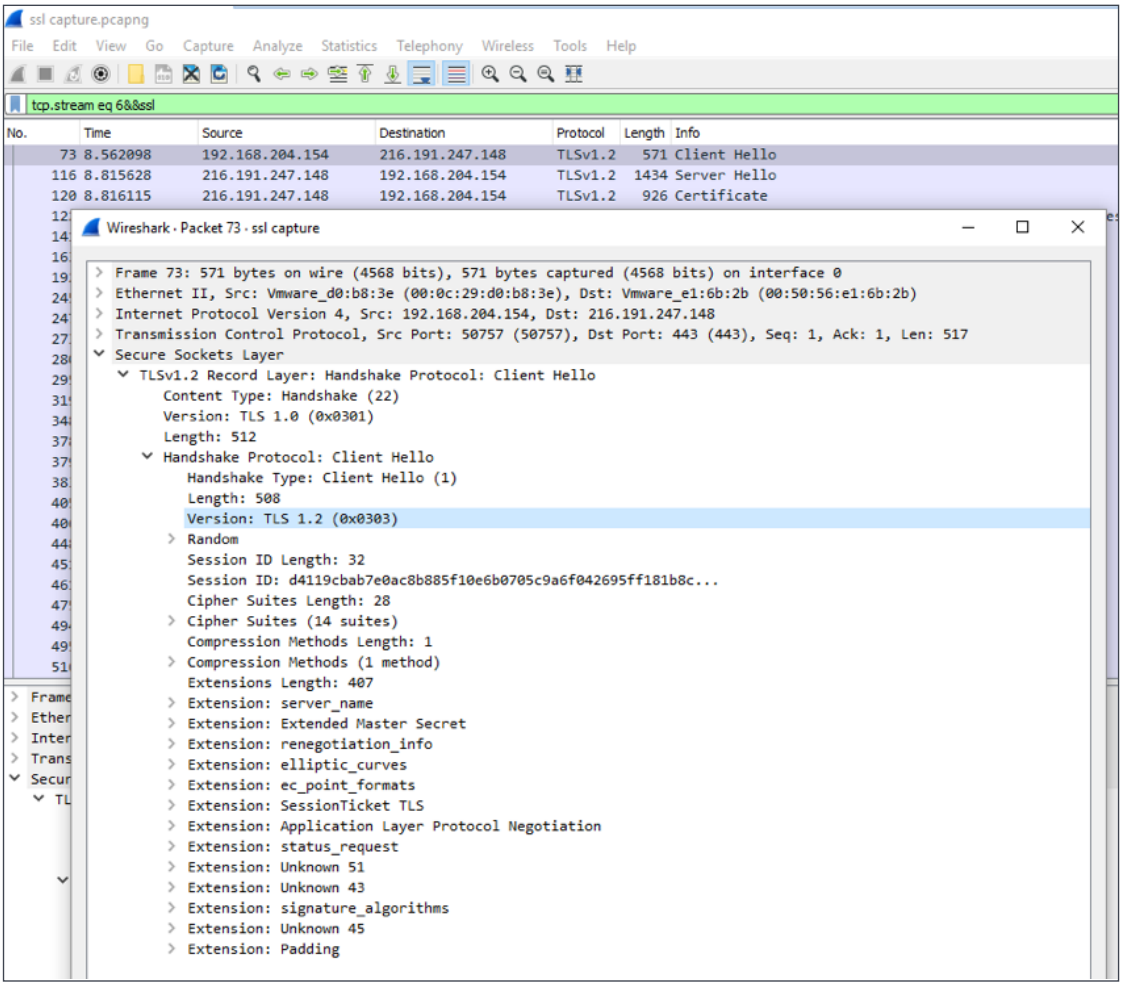




II. Breakdown of the handshake process

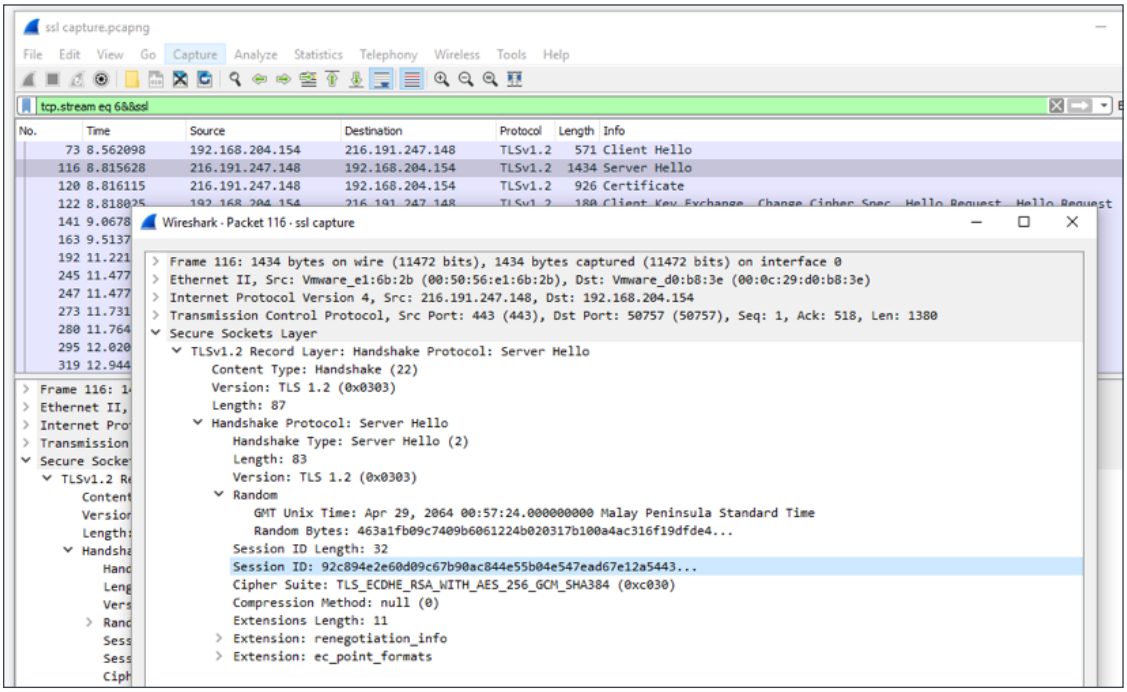
TLS 1.2

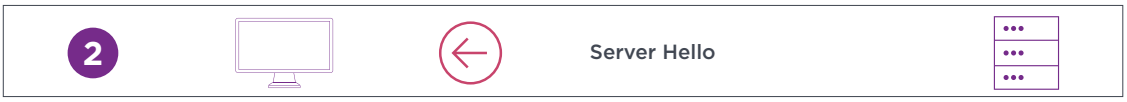
1. Client Hello



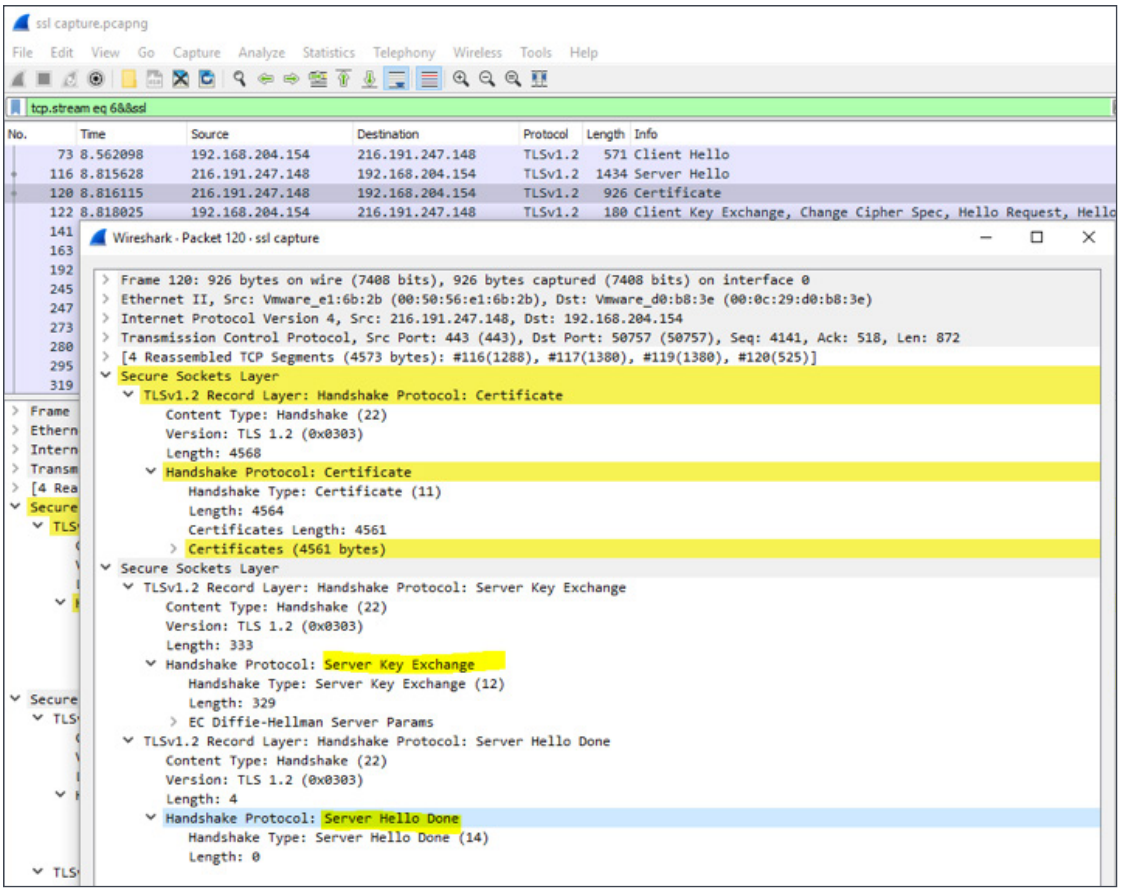
Step	Client	Direction	Message	Direction	Server
1			Client Hello	→	

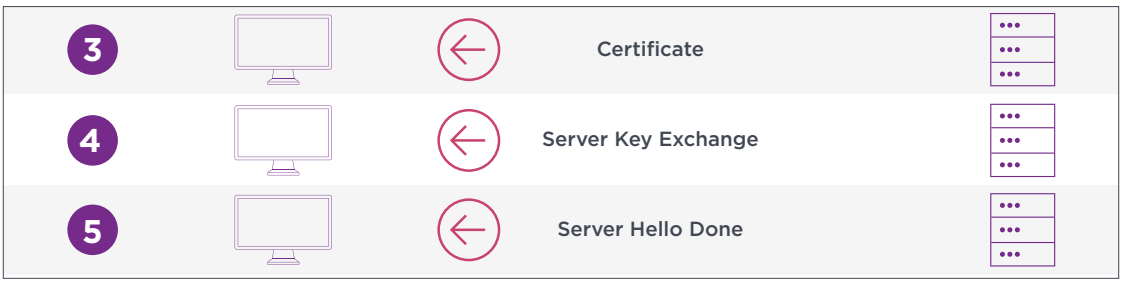
2. Server Hello



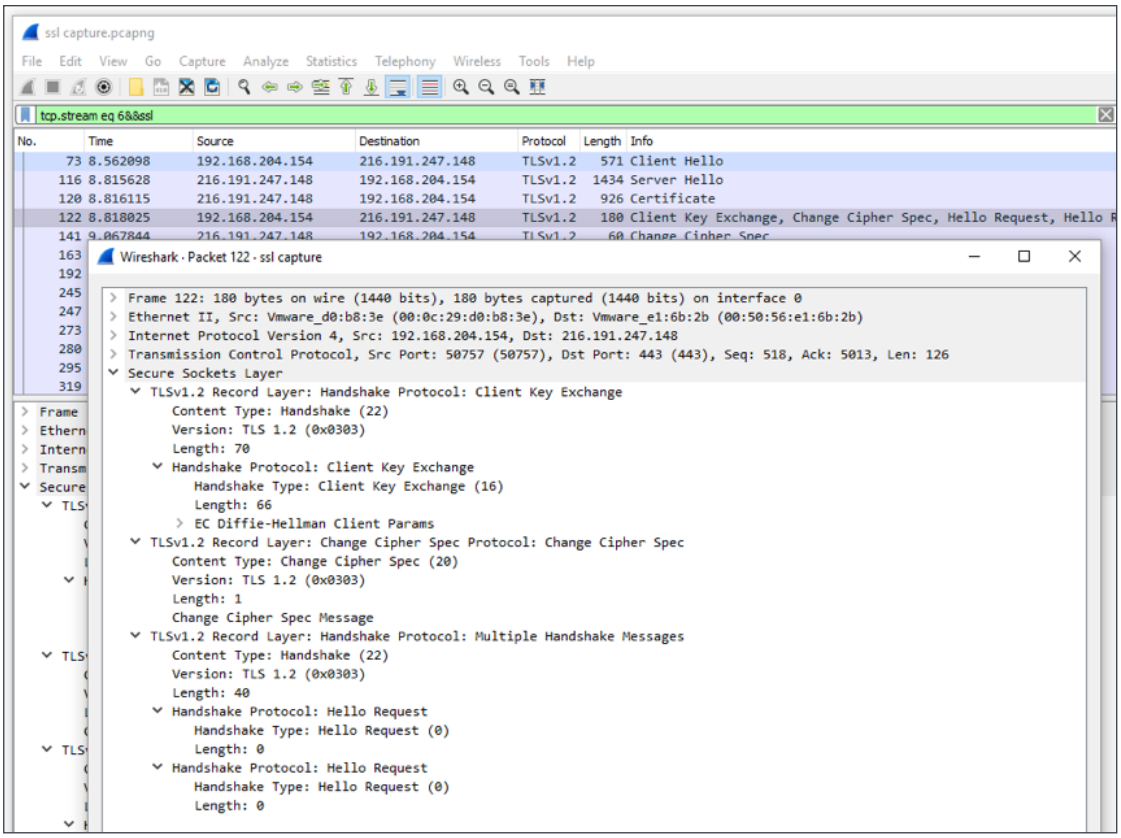


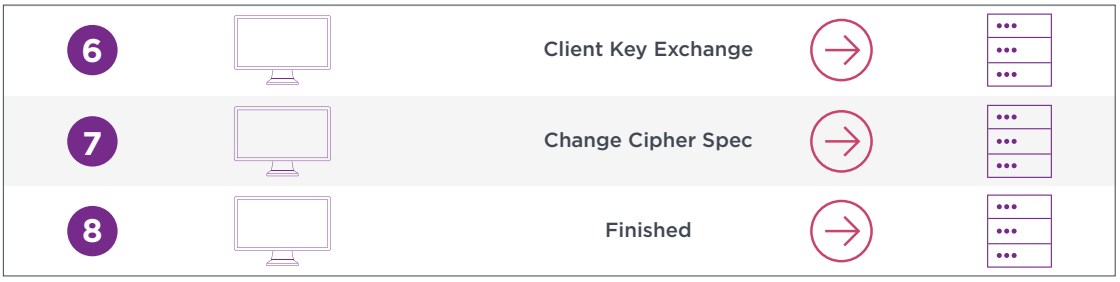
3. Certificate
    a. Server Key Exchange
    b. Server Hello Done





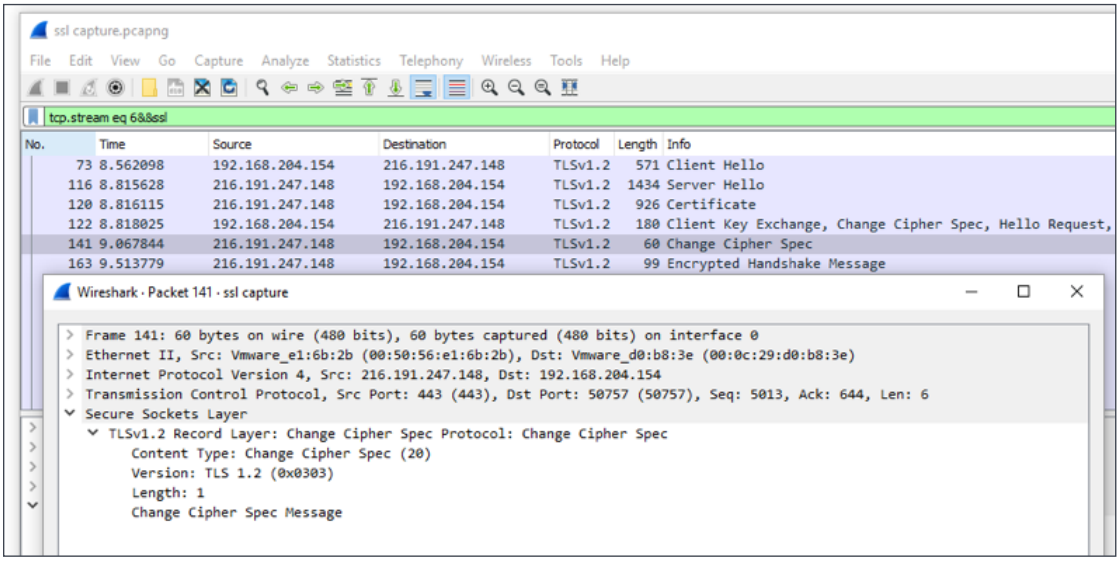
4. Client Key Exchange
    a. Change Cipher Spec
    b. Finished

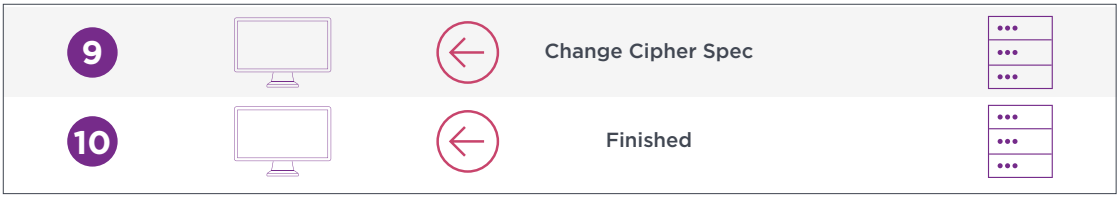




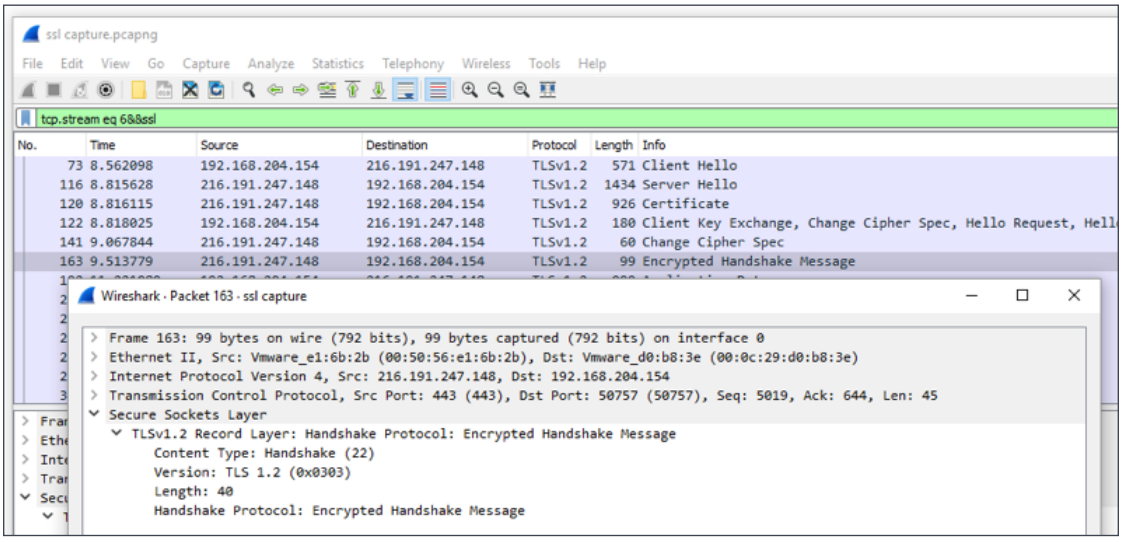
5. Change Cipher Spec

   a. Finished





6. Encrypted Handshake Message

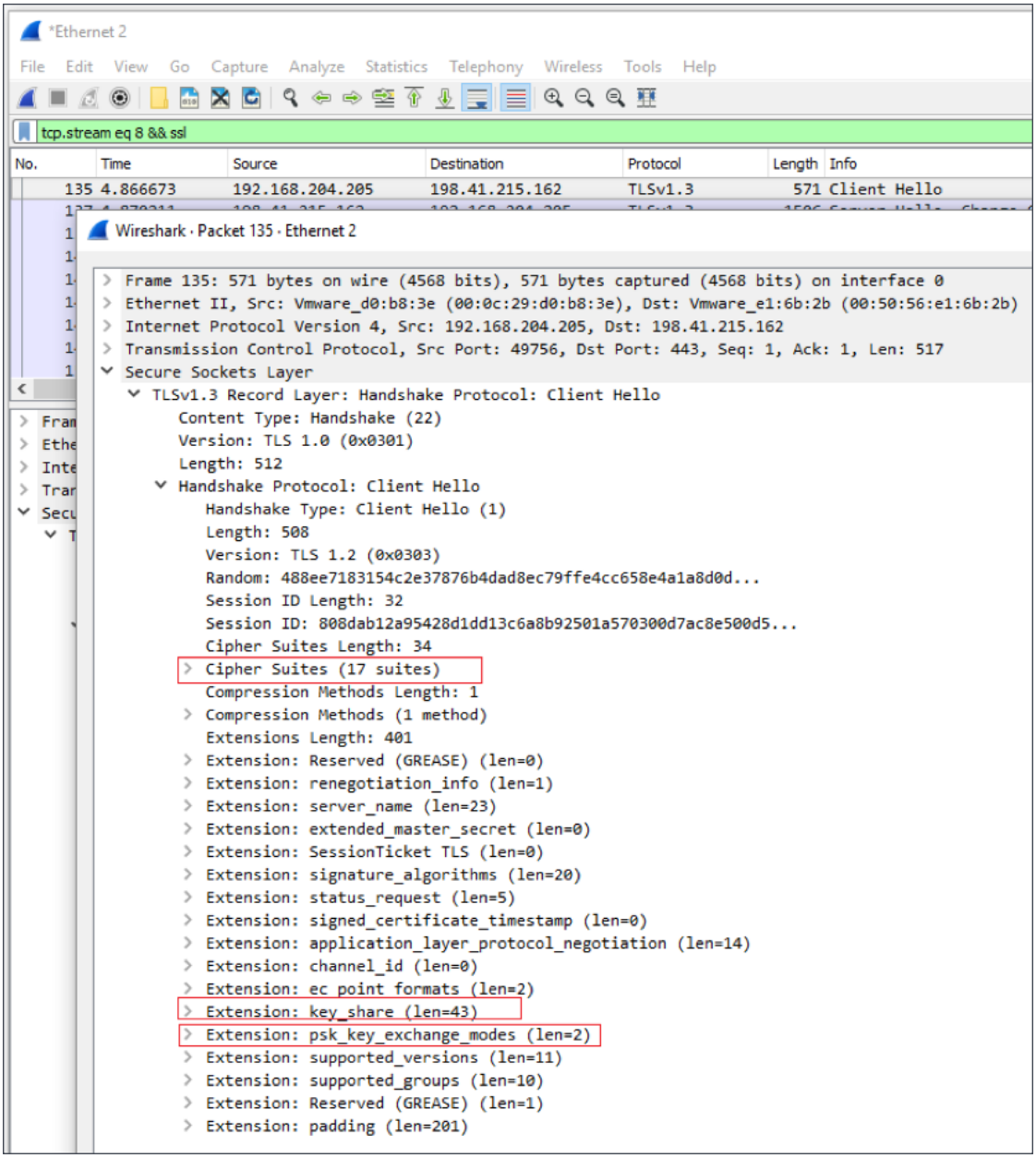


ECS KNOWLEDGE SHARING

Comparison: TLS 1.3 and TLS 1.2

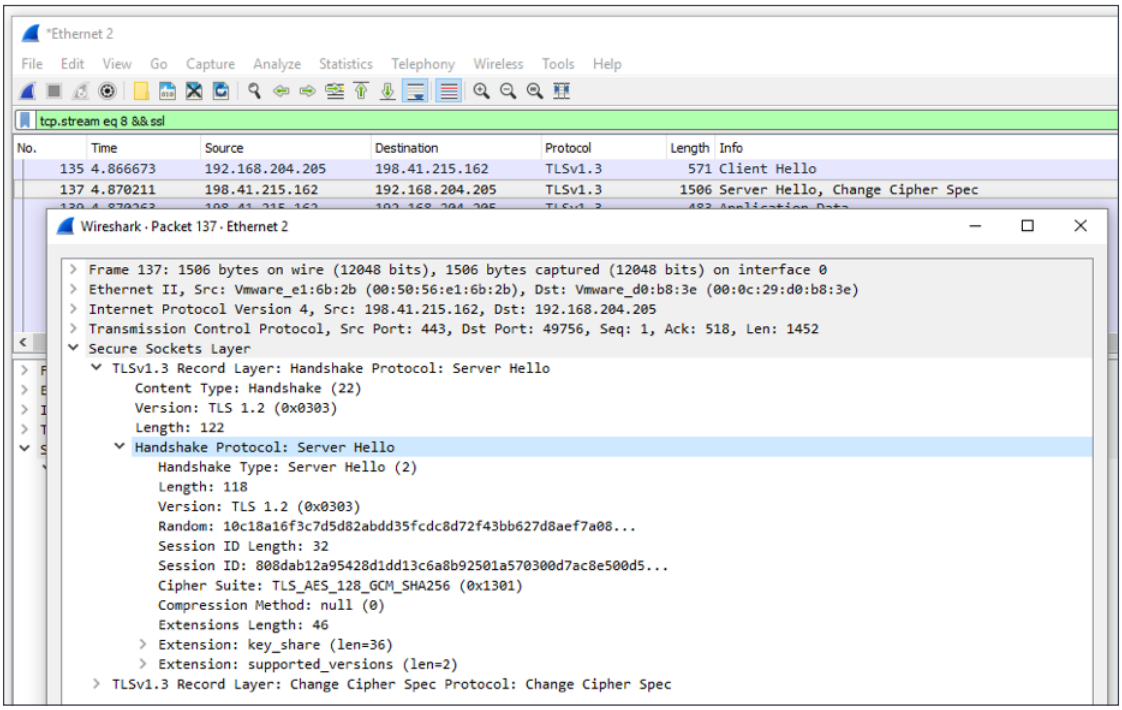
TLS 1.3

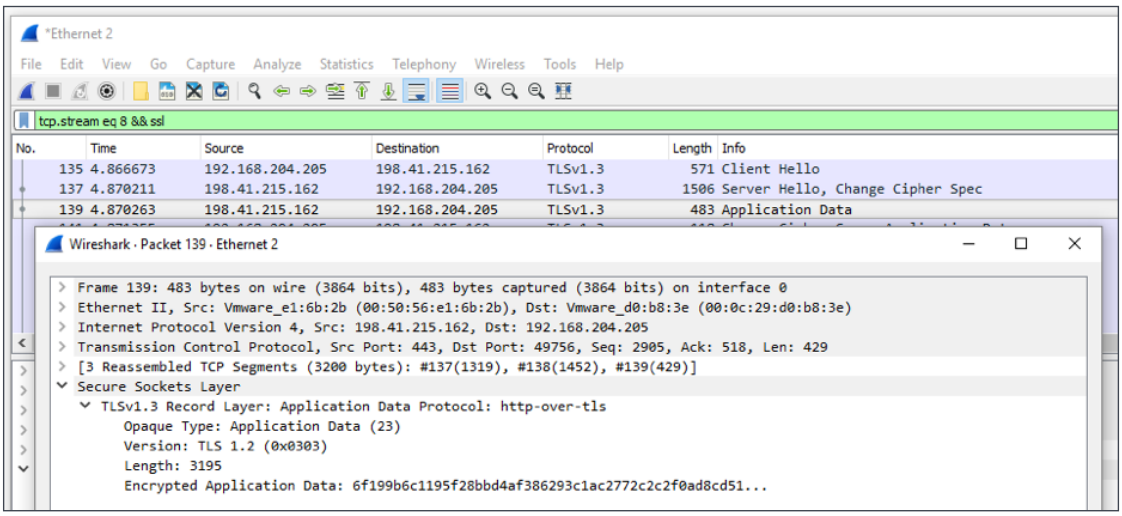
1. Client Hello, Supported Cipher Suites, Guesses Key Agreement Protocol, Key Share



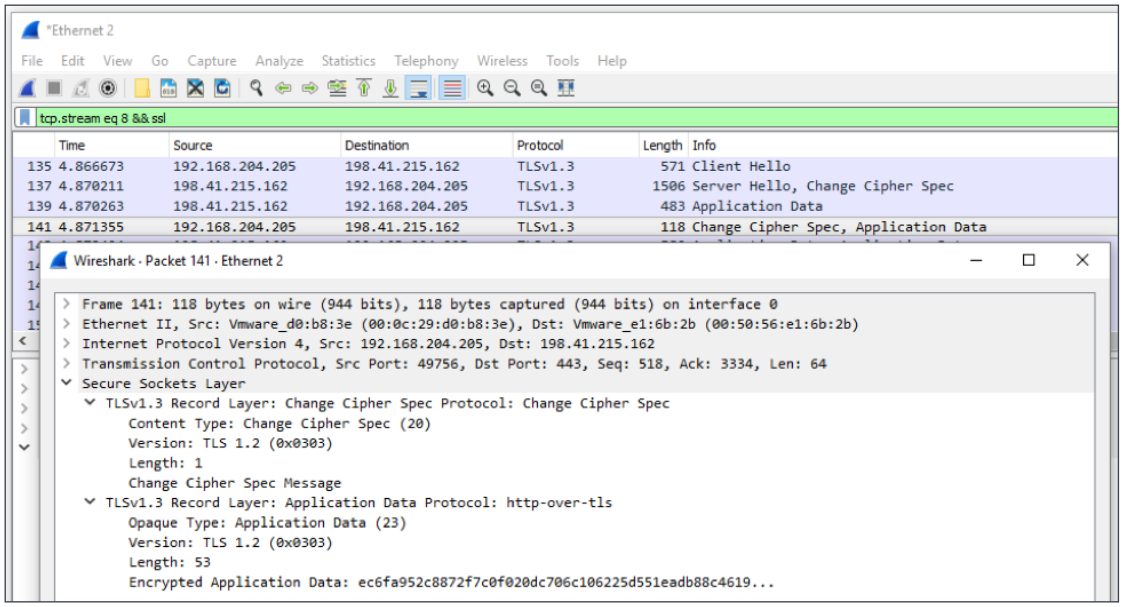
Step	Client	Direction	Message	Direction	Server
1			Client Hello Supported Cipher Suite Guesses Key Agreement Protocol Key Share	→	

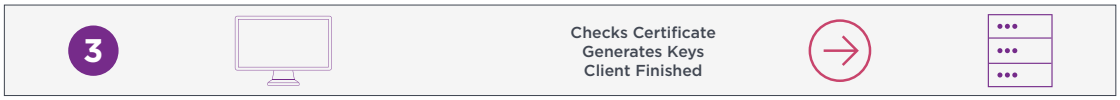
2. Server Hello, Key Agreement Protocol, Key Share, Server Finished





3. Checks Certificate, Generate Keys, Client Finished





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** or visit **entrustdatacard.com**.

Entrust Datacard™

Corporate Headquarters

U.S. Toll-Free Phone: 1-888-690-2424
International Phone: +1-952-933-1223
info@entrustdatacard.com
entrustdatacard.com