

1. What is the SSL/TLS version of the Client Hello frame?

Answer: Version: TLS 1.2 (0x0303)

The image shows a Wireshark network traffic capture of an SSL/TLS handshake. The top pane displays a list of packets, with packet 291 highlighted, which is a TLSv1.2 Client Hello frame. The middle pane shows the details of this frame, indicating it is a TLSv1.2 Record Layer: Handshake Protocol: Client Hello. The bottom pane shows the raw packet data in hexadecimal and ASCII. The status bar at the bottom indicates the maximum version supported by the client is TLS 1.2 (0x0303).

No.	Time	Source	Destination	Protocol	Length	Info
281	1541868616.245077	192.168.1.169	172.217.6.196	TCP	1434	59911 → 443 [ACK] Seq=5152 Ack=97206 Win=66048 Len=1380 [TCP segment of a reassembl...
282	1541868616.245086	192.168.1.169	172.217.6.196	TLSv1...	373	Application Data
284	1541868616.283898	172.217.6.196	192.168.1.169	TLSv1...	369	Application Data
291	1541868616.391903	192.168.1.169	52.71.134.97	TLSv1...	571	Client Hello
293	1541868616.397556	52.71.134.97	192.168.1.169	TLSv1...	1514	Server Hello
296	1541868616.397640	52.71.134.97	192.168.1.169	TLSv1...	933	Certificate, Server Key Exchange, Server Hello Done
299	1541868616.398822	192.168.1.169	52.71.134.97	TLSv1...	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
300	1541868616.404054	52.71.134.97	192.168.1.169	TLSv1...	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message

Transmission Control Protocol, Src Port: 59916, Dst Port: 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: 2d941cb63df47aaab110322f040244bbba46192afe768bdb...

0030 01 00 be 3d 00 00 16 03 01 02 00 01 00 01 fc 03
0040 2d 94 1c b6 3d f4 7a aa b1 10 32 2f 04 02 44z ...2/..D
0050 bb ba 46 19 2a fe 76 8b db 33 ad 92 45 d4 5c 1f ..F.*.v. .3..E.\.
0060 5d 20 57 97 74 15 e4 45 97 0e 2a 51 09 4d 13 1d] W-t..E ..*Q-M..
0070 c0 0d 09 ac 40 92 3b c1 4a 75 65 24 be d1 f0 ba ...@.;. Jue\$.
0080 b8 ef 00 22 1a 1a 13 01 13 02 13 03 c0 2b c0 2f ...".... ..+./
0090 c0 2c c0 30 cc a9 cc a8 c0 13 c0 14 00 9c 00 9d ..0....
00a0 00 2f 00 35 00 0a 01 00 01 91 1a 1a 00 00 ff 01 ./5....
00b0 00 01 00 00 00 00 17 00 15 00 00 12 61 75 74 68auth

Maximum version supported by client (ssl.handshake.version), 2 bytes

Packets: 2624 · Displayed: 1306 (49.8%) · Dropped: 0 (0.0%) Profile: Default

11:58 AM 11/10/2018

2. Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?

Answer: Client Hello: Content Type: Handshake (22) – type 22. Handshake Type: Client Hello (1) - type 1

The screenshot shows the Wireshark interface with a network capture on the 'ssl' filter. The packet list pane shows several packets, with packet 291 selected, which is a TLSv1.2 Client Hello. The packet details pane shows the expanded structure of this record:

- Transmission Control Protocol, Src Port: 59916, Dst Port: 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: 2d941cb63df47aaab110322f040244bbba46192afe768bdb...

The packet bytes pane shows the raw data of the selected packet, with the first few bytes highlighted in blue, corresponding to the Client Hello handshake type.

At the bottom of the interface, the status bar indicates: Type of handshake message (ssl.handshake.type), 1 byte. Packets: 2624 · Displayed: 1306 (49.8%) · Dropped: 0 (0.0%) · Profile: Default.

3. Does the ClientHello record contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?

Answer: Then there is 'Random' field which contains a nonce or challenge (in hexadecimal)

3df47aaab110322f040244bbba46192afe768bdb33ad9245...

Wireshark capture of an SSL/TLS handshake. The packet list shows a Client Hello (packet 291) and its details. The details pane for the Client Hello shows the Random field with the value 3df47aaab110322f040244bbba46192afe768bdb33ad9245... The packet bytes pane shows the raw hex and ASCII data.

No.	Time	Source	Destination	Protocol	Length	Info
284	1541868616.283898	172.217.6.196	192.168.1.169	TLSv1...	369	Application Data
291	1541868616.391903	192.168.1.169	52.71.134.97	TLSv1...	571	Client Hello
293	1541868616.397556	52.71.134.97	192.168.1.169	TLSv1...	1514	Server Hello
296	1541868616.397640	52.71.134.97	192.168.1.169	TLSv1...	933	Certificate, Server Key Exchange, Server Hello Done
299	1541868616.398822	192.168.1.169	52.71.134.97	TLSv1...	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
300	1541868616.404054	52.71.134.97	192.168.1.169	TLSv1...	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
301	1541868616.404153	52.71.134.97	192.168.1.169	TLSv1...	123	Application Data
303	1541868616.423953	192.168.1.169	52.71.134.97	TLSv1...	147	Application Data

Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 508
Version: TLS 1.2 (0x0303)
Random: 2d941cb63df47aaab110322f040244bbba46192afe768bdb...
GMT Unix Time: Mar 26, 1994 07:29:58.00000000 Eastern Daylight Time
Random Bytes: 3df47aaab110322f040244bbba46192afe768bdb33ad9245...
Session ID Length: 32
Session ID: 57977415e445970e2a51094d131dc00d09ac40923bc14a75...
Cipher Suites Length: 34
Cipher Suites (17 suites)

0060 5d 20 57 97 74 15 e4 45 97 0e 2a 51 09 4d 13 1d] W-t··E ··*Q·M··
0070 c0 0d 09 ac 40 92 3b c1 4a 75 65 24 be d1 f0 ba ...@·;· Jue\$·...
0080 b8 ef 00 22 1a 1a 13 01 13 02 13 03 c0 2b c0 2f ..."-.....+·/
0090 c0 2c c0 30 cc a9 cc a8 c0 13 c0 14 00 9c 00 9d ·,·0·...·...
00a0 00 2f 00 35 00 0a 01 00 01 91 1a 1a 00 00 ff 01 ·/·5·...·...
00b0 00 01 00 00 00 00 17 00 15 00 00 12 61 75 74 68auth
00c0 2e 67 72 61 6d 6d 61 72 6c 79 2e 63 6f 6d 00 17 .grammar ly.com·
00d0 00 00 00 23 00 00 00 0d 00 14 00 12 04 03 08 04 ...#·...·...
00e0 04 01 05 03 08 05 05 01 08 06 06 01 02 01 00 05·...·...

Identifies the SSL session, allowing later resumption (ssl.handshake.session_id), 32 bytes

Packets: 2624 · Displayed: 1306 (49.8%) · Dropped: 0 (0.0%)

Profile: Default

1:07 PM 11/10/2018

4. Does the ClientHello record advertise the cipher suites it supports? If so, in the first listed suite, what are the public-key algorithm, the symmetric-key algorithm, and the hash algorithm?

Answer: Yes. The first suite uses AES - symmetric algorithm, so it does not have public and private keys - only a shared secret., GCM 128 bites for the symmetric-key cipher and uses the SHA 256 bits hash algorithm.

The image shows a Wireshark capture of a TLS handshake. The packet list shows several packets, with packet 291 (Client Hello) selected. The packet details pane shows the structure of the ClientHello message, including the version (TLS 1.2), random bytes, GMT Unix Time, random bytes, session ID length, session ID, cipher suites length, and a list of cipher suites. The first cipher suite is TLS_AES_128_GCM_SHA256 (0x1301).

Version: TLS 1.2 (0x0303)

- Random: 2d941cb63df47aaab110322f040244bbba46192afe768bdb...
- GMT Unix Time: Mar 26, 1994 07:29:58.000000000 Eastern Daylight Time
- Random Bytes: 3df47aaab110322f040244bbba46192afe768bdb33ad9245...
- Session ID Length: 32
- Session ID: 57977415e445970e2a51094d131dc00d09ac40923bc14a75...
- Cipher Suites Length: 34
- Cipher Suites (17 suites)
 - Cipher Suite: Reserved (GREASE) (0x1a1a)
 - Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
 - Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)

0000 b8 ef 00 22 1a 1a 13 01 13 02 13 03 c0 2b c0 2f ... " ... + /
0090 c0 2c c0 30 cc a9 cc a8 c0 13 c0 14 00 9c 00 9d ... , 0 ...
00a0 00 2f 00 35 00 0a 01 00 01 91 1a 1a 00 00 ff 01 ... / 5 ...
00b0 00 01 00 00 00 00 17 00 15 00 00 12 61 75 74 68 auth
00c0 2e 67 72 61 6d 6d 61 72 6c 79 2e 63 6f 6d 00 17 grammar ly.com ..
00d0 00 00 00 23 00 00 00 0d 00 14 00 12 04 03 08 04 # ..
00e0 04 01 05 03 08 05 05 01 08 06 06 01 02 01 00 05
00f0 00 05 01 00 00 00 00 00 12 00 00 00 10 00 0e 00
0100 0c 02 68 32 08 68 74 74 70 2f 31 2e 31 75 50 00 h2 htt p/1.1uP ..

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

Packets: 2624 · Displayed: 1306 (49.8%) · Dropped: 0 (0.0%) | Profile: Default

12:41 PM 11/10/2018

1. Locate the ServerHello SSL record. Does this record specify a chosen cipher suite? What are the algorithms in the chosen cipher suite?

Answer: Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

In our case elliptic curve diffie-hellman key exchange (ECDHE_RSA) will be used in ephemeral mode (which provides forward secrecy) and this exchange will be authenticated with RSA signature. RSA is used to authenticate the server while ECDHE is used to generate a shared secret between the client and server. GCM 128 bites for the symmetric-key cipher and uses the SHA 256 bits hash algorithm.

The image shows a Wireshark capture of an SSL/TLS handshake. The top pane displays a list of packets, with packet 293 (Server Hello) selected. The middle pane shows the details of the Server Hello message, highlighting the Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f). The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
284	1541868616.283898	172.217.6.196	192.168.1.169	TLSv1...	369	Application Data
291	1541868616.391903	192.168.1.169	52.71.134.97	TLSv1...	571	Client Hello
293	1541868616.397556	52.71.134.97	192.168.1.169	TLSv1...	1514	Server Hello
296	1541868616.397640	52.71.134.97	192.168.1.169	TLSv1...	933	Certificate, Server Key Exchange, Server Hello Done
299	1541868616.398822	192.168.1.169	52.71.134.97	TLSv1...	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
300	1541868616.404054	52.71.134.97	192.168.1.169	TLSv1...	312	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
301	1541868616.404153	52.71.134.97	192.168.1.169	TLSv1...	123	Application Data
303	1541868616.423953	192.168.1.169	52.71.134.97	TLSv1...	147	Application Data

Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 66
Version: TLS 1.2 (0x0303)
> Random: 6a76862cf21c5e9d8aa6110c7f39cbf2a345fa5440988f2f...
Session ID Length: 0
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Compression Method: null (0)
Extensions Length: 26
> Extension: renegotiation_info (len=1)
> Extension: ec_point_formats (len=4)

0060 84 00 c0 2f 00 00 1a ff 01 00 01 00 0b 00 04 .../...
0070 03 00 01 02 00 23 00 00 00 10 00 05 00 03 02 68 ...#...h
0080 32 16 03 03 12 e0 0b 00 12 dc 00 12 d9 00 05 71 2.....q
0090 30 82 05 6d 30 82 04 55 a0 03 02 01 02 02 10 03 0...m0...U...
00a0 f4 45 c1 50 74 bb 1c c6 7e 34 fa 96 84 35 ff 30 :E:Pt...4...5 0
00b0 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00 30 46 ...*H...0F
00c0 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 0f 30 1:0...U...US1 0
00d0 0d 06 03 55 04 0a 13 06 41 6d 61 7a 6f 6e 31 15 ...U...Amazon1
00e0 30 13 06 03 55 04 0b 13 0c 53 65 72 76 65 72 20 0...U...Server

Cipher Suite (ssl.handshake.ciphersuite), 2 bytes | Packets: 2624 · Displayed: 1306 (49.8%) · Dropped: 0 (0.0%) | Profile: Default

IP ADDRESS

The screenshot displays a Windows desktop environment. In the foreground, a Microsoft Word document titled "Document1 - Word" is open, showing a blank page with a ribbon menu. Overlaid on the Word document is a "Select Command Prompt" window. The Command Prompt shows the output of the command `C:\Users\Natalia>ipconfig`. The output details the network configuration for three adapters: two Wireless LAN adapters (Local Area Connection* 1 and 11) and one Ethernet adapter (Bluetooth Network Connection). The IPv4 address for the first Wireless LAN adapter is highlighted as 192.168.1.169. The taskbar at the bottom shows the Start button, task view icon, File Explorer, Google Chrome, Word, and a power icon. The system tray on the right indicates the time is 12:56 PM on 11/10/2018, with the language set to ENG.

AutoSave (Off) Document1 - Word Natalia Ermicio

Select Command Prompt

C:\Users\Natalia>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 1:

Media State : Media disconnected

Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 11:

Media State : Media disconnected

Connection-specific DNS Suffix . :

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : fios-router.home

Link-local IPv6 Address : fe80::a517:91e:236d:6190%18

IPv4 Address. : 192.168.1.169

Subnet Mask : 255.255.255.0

Default Gateway : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

Media State : Media disconnected

Connection-specific DNS Suffix . :

C:\Users\Natalia>

Page 6 of 6 245 words English (United States) 17%

12:56 PM 11/10/2018 ENG