

Abdullah Alrfeedi  
Lab 8  
IT-520

My IP address is (192.168.0.4).

The image shows a Wireshark network traffic capture of a TLS handshake. The packet list on the left shows several packets, with packet 1870 (Client Hello) highlighted. The packet details pane on the right shows the structure of the Client Hello message, including the TLS version (3.1), random values, session ID, cipher suites, and compression methods. The packet bytes pane at the bottom shows the raw data of the Client Hello message in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1844	24.040268	2001:559:19:85::13...	2601:140:8600:18a0...	TLSv1...	1514	Application Data [TCP segment of a reassembled PDU]
1845	24.040308	2001:559:19:85::13...	2601:140:8600:18a0...	TLSv1...	1371	Application Data, Application Data
1852	24.045223	65.55.44.109	192.168.0.4	TLSv1...	105	Change Cipher Spec, Encrypted Handshake Message
1870	24.164605	192.168.0.4	52.204.250.175	TLSv1...	571	Client Hello
1877	24.215316	52.204.250.175	192.168.0.4	TLSv1...	1514	Server Hello
1878	24.215579	52.204.250.175	192.168.0.4	TLSv1...	1514	Certificate [TCP segment of a reassembled PDU]
1880	24.215734	52.204.250.175	192.168.0.4	TLSv1...	205	Server Key Exchange, Server Hello Done
1882	24.219637	192.168.0.4	52.204.250.175	TLSv1...	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1884	24.220415	192.168.0.4	52.204.250.175	TLSv1...	907	Application Data
1891	24.245330	192.168.0.4	23.53.216.181	TLSv1...	571	Client Hello

Frame 1870: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface 0  
Ethernet II, Src: Apple\_13:0e:7c (88:1f:a1:13:0e:7c), Dst: Netgear\_8c:a7:cb (dc:ef:09:8c:a7:cb)  
Internet Protocol Version 4, Src: 192.168.0.4, Dst: 52.204.250.175  
Transmission Control Protocol, Src Port: 52968, Dst Port: 443, Seq: 1, Ack: 1, Len: 517  
Transport Layer Security

Random values used for deriving keys (tls.handshake.random), 32 bytes

Page 1 of 6 178 words English (United States)

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

The SSL/TLS version of the Client Hello frame is (TLS 1.0).

The image shows a Wireshark network packet capture of an SSL/TLS handshake. The packet list on the left shows several frames, with frame 1870 (Client Hello) selected. The packet details pane on the right shows the structure of the Client Hello frame, with the 'Version: TLS 1.0 (0x0301)' field highlighted in a red box. The packet bytes pane at the bottom shows the raw hex and ASCII data of the frame.

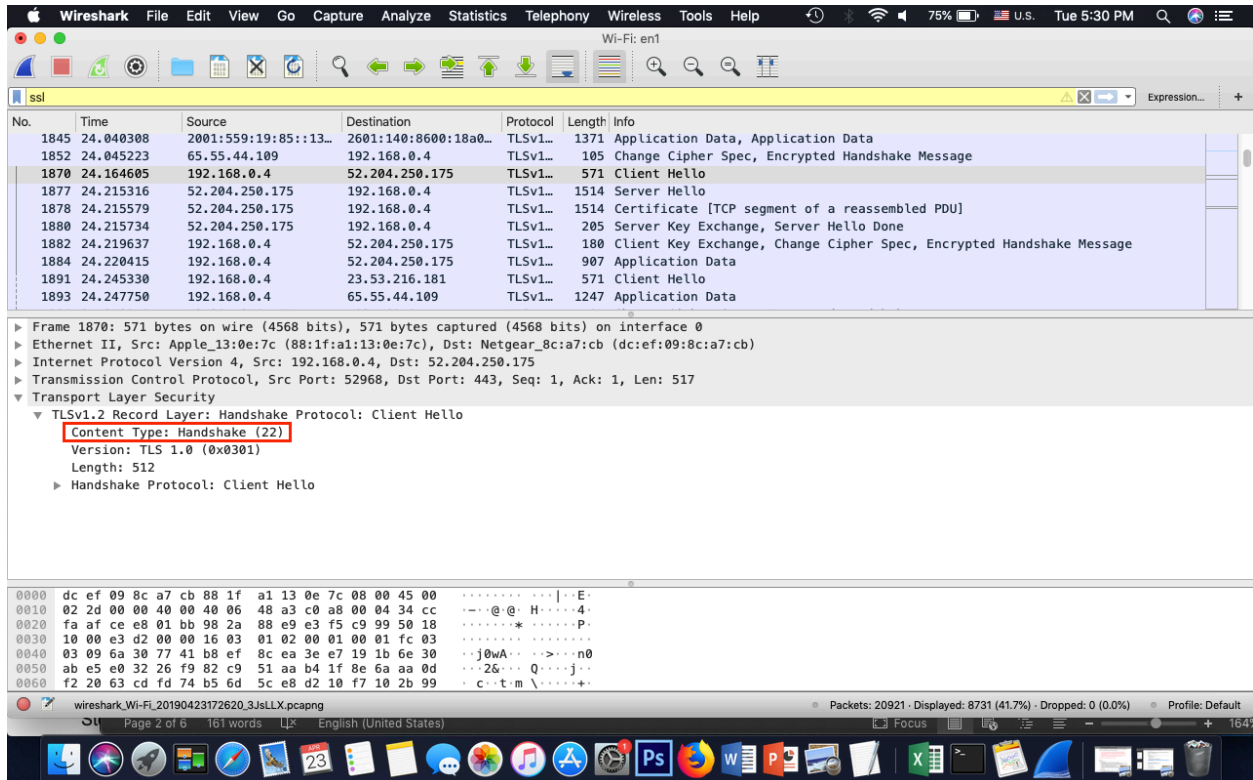
No.	Time	Source	Destination	Protocol	Length	Info
1845	24.040308	2001:559:19:85::13...	2601:140:8600:18a0...	TLSv1...	1371	Application Data, Application Data
1852	24.045223	65.55.44.109	192.168.0.4	TLSv1...	105	Change Cipher Spec, Encrypted Handshake Message
1870	24.164605	192.168.0.4	52.204.250.175	TLSv1...	571	Client Hello
1877	24.215316	52.204.250.175	192.168.0.4	TLSv1...	1514	Server Hello
1878	24.215579	52.204.250.175	192.168.0.4	TLSv1...	1514	Certificate [TCP segment of a reassembled PDU]
1880	24.215734	52.204.250.175	192.168.0.4	TLSv1...	205	Server Key Exchange, Server Hello Done
1882	24.219637	192.168.0.4	52.204.250.175	TLSv1...	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1884	24.220415	192.168.0.4	52.204.250.175	TLSv1...	907	Application Data
1891	24.245330	192.168.0.4	23.53.216.181	TLSv1...	571	Client Hello
1893	24.247750	192.168.0.4	65.55.44.109	TLSv1...	1247	Application Data

Frame 1870: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface 0  
Ethernet II, Src: Apple\_13:0e:7c (88:1f:a1:13:0e:7c), Dst: Netgear\_8c:a7:cb (dc:ef:09:8c:a7:cb)  
Internet Protocol Version 4, Src: 192.168.0.4, Dst: 52.204.250.175  
Transmission Control Protocol, Src Port: 52968, 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

0000 dc ef 09 8c a7 cb 88 1f a1 13 0e 7c 08 00 45 00 .....E.  
0010 02 2d 00 00 40 00 40 06 48 a3 c0 a8 00 04 34 cc ...@.H....4.  
0020 fa af ce e8 01 bb 98 2a 88 e9 e3 f5 c9 99 50 18 .....\*.....P.  
0030 10 00 e3 d2 00 00 16 03 01 02 00 01 00 01 fc 03 .....  
0040 03 09 6a 30 77 41 b8 ef 8c ea 3e e7 19 1b 6e 30 ...j0wA...>...n0  
0050 ab e5 e0 32 26 f9 82 c9 51 aa b4 1f 8e 6a aa 0d ...26...Q....j..  
0060 f2 20 63 cd fd 74 b5 6d 5c e8 d2 10 f7 10 2b 99 ...c..t.m \.....+

- 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?

The value of the content type is **Handshake (22)**.



The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The status bar at the top right shows the system time as Tue 5:30 PM and battery level at 75%.

The main packet list pane shows a series of network packets. Packet 1870 is highlighted, showing a TLSv1.2 Client Hello message. The packet details pane on the right shows the expanded structure of this packet:

- Frame 1870: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface 0
- Ethernet II, Src: Apple\_13:0e:7c (88:1f:a1:13:0e:7c), Dst: Netgear\_8c:a7:cb (dc:ef:09:8c:a7:cb)
- Internet Protocol Version 4, Src: 192.168.0.4, Dst: 52.204.250.175
- Transmission Control Protocol, Src Port: 52968, 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

The bottom pane shows the raw packet data in hexadecimal and ASCII format.

- 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?

Yes, it does. It is (096a307741b8ef8cea3ee...).

The image shows a Wireshark network packet capture of a TLS handshake. The packet list on the left shows several packets, with packet 1870 (Client Hello) selected. The packet details pane on the right shows the structure of the Client Hello message. The 'Random' field is highlighted with a red box, showing the value 096a307741b8ef8cea3ee7191b6e30abe5e03226f982c951. The packet bytes pane at the bottom shows the raw hexadecimal and ASCII data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
1844	24.040268	2001:559:19:85::13...	2601:140:8600:18a0...	TLSv1...	1514	Application Data [TCP segment of a reassembled PDU]
1845	24.040308	2001:559:19:85::13...	2601:140:8600:18a0...	TLSv1...	1371	Application Data, Application Data
1852	24.045223	65.55.44.109	192.168.0.4	TLSv1...	105	Change Cipher Spec, Encrypted Handshake Message
1870	24.164605	192.168.0.4	52.204.250.175	TLSv1...	571	Client Hello
1877	24.215316	52.204.250.175	192.168.0.4	TLSv1...	1514	Server Hello
1878	24.215579	52.204.250.175	192.168.0.4	TLSv1...	1514	Certificate [TCP segment of a reassembled PDU]
1880	24.215734	52.204.250.175	192.168.0.4	TLSv1...	205	Server Key Exchange, Server Hello Done
1882	24.219637	192.168.0.4	52.204.250.175	TLSv1...	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1884	24.220415	192.168.0.4	52.204.250.175	TLSv1...	907	Application Data
1891	24.245330	192.168.0.4	23.53.216.181	TLSv1...	571	Client Hello

Length: 508  
Version: TLS 1.2 (0x0303)  
Random: 096a307741b8ef8cea3ee7191b6e30abe5e03226f982c951  
GMT Unix Time: Jan 2, 1975 23:09:27.000000000 EST  
Random Bytes: 41b8ef8cea3ee7191b6e30abe5e03226f982c951aab41f8e...  
Session ID Length: 32  
Session ID: 63cdfd74b56d5ce8d210f7102b99c97459396b918a0cd526...  
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)

0040 03 09 6a 30 77 41 b8 ef 8c ea 3e e7 19 1b 6e 30 .j0wA...>...n0  
0050 ab e5 e0 32 26 f9 82 c9 51 aa b4 1f 8e 6a aa 0d ..26...Q...j...  
0060 f2 20 63 cd fd 74 b5 6d 5c e8 d2 10 f7 10 2b 99 .c..t.m\.....+..  
0070 c9 74 59 39 6b 91 8a 0c d5 26 d0 84 a3 31 9b 45 .tY9k...&...1.E  
0080 52 44 00 24 13 01 13 03 13 02 c0 2b c0 2f cc a9 RD\$....+./...  
0090 cc a8 c0 2c c0 30 c0 0a c0 09 c0 13 c0 14 00 33 ...0... ..3  
00a0 00 39 00 2f 00 35 00 0a 01 00 01 8f 00 00 00 13 .9./..S.....

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?

Yes, it does.

- Public-Key algorithm is (AES).
- The symmetric-key algorithm is (GCM).
- The hash algorithm is (SHA256).

The image shows a Wireshark capture of an SSL/TLS handshake. The top pane displays a list of packets, with the ClientHello packet (No. 1870) selected. The bottom pane shows the details of the ClientHello message, including the Session ID, Cipher Suites Length, and a list of supported Cipher Suites. The first cipher suite listed is TLS\_AES\_128\_GCM\_SHA256 (0x1301), which is highlighted with a red box. The bottom pane also shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1845	24.040308	2001:559:19:85::13..	2601:140:8600:18a0..	TLsv1..	1371	Application Data, Application Data
1852	24.045223	65.55.44.109	192.168.0.4	TLsv1..	105	Change Cipher Spec, Encrypted Handshake Message
1870	24.164605	192.168.0.4	52.204.250.175	TLsv1..	571	Client Hello
1877	24.215316	52.204.250.175	192.168.0.4	TLsv1..	1514	Server Hello
1878	24.215579	52.204.250.175	192.168.0.4	TLsv1..	1514	Certificate [TCP segment of a reassembled PDU]
1880	24.215734	52.204.250.175	192.168.0.4	TLsv1..	205	Server Key Exchange, Server Hello Done
1882	24.219637	192.168.0.4	52.204.250.175	TLsv1..	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1884	24.220415	192.168.0.4	52.204.250.175	TLsv1..	907	Application Data
1891	24.245330	192.168.0.4	23.53.216.181	TLsv1..	571	Client Hello
1893	24.247750	192.168.0.4	65.55.44.109	TLsv1..	1247	Application Data

Random: 096a3077410be78ce3ee71910e30ade3e052207962c951..  
Session ID Length: 32  
Session ID: 63cdfd74b56d5ce8d210f7102b99c97459396b918a0cd526..  
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 (0xc0ca8)  
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)

0000 dc ef 09 8c a7 cb 88 1f a1 13 0e 7c 08 00 45 00 .....E  
0010 02 2d 00 00 40 00 40 06 48 a3 c0 a8 00 04 34 cc ...@.H...4  
0020 fa af ce e8 01 bb 98 2a 88 e9 e3 f5 c9 99 50 18 .....\*.....P  
0030 10 00 e3 d2 00 00 16 03 01 02 00 01 00 01 fc 03 .....n0  
0040 03 09 6a 30 77 41 b8 ef 8c ea 3e e7 19 1b 6e 30 ...j0wA...>...n0  
0050 ab e5 e0 32 26 f9 82 c9 51 aa b4 1f 8e 6a aa 0d ...26...Q...j...  
0060 f2 20 63 cd fd 74 b5 6d 5c e8 d2 10 f7 10 2b 99 ...c..t..m\.....+

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

Yes, it does. They are (TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256).

The image shows a Wireshark network packet capture of an SSL/TLS handshake. The packet list on the left shows several records, with the 'Server Hello' record (No. 1877) selected. The details pane on the right shows the structure of the ServerHello message, including the TLS version, random, session ID, and cipher suite. The cipher suite is highlighted with a red box: 'Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)'. The bottom of the image shows the macOS dock with various application icons.

No.	Time	Source	Destination	Protocol	Length	Info
1845	24.040308	2001:559:19:85::13...	2601:140:8600:18a0...	TLSv1...	1371	Application Data, Application Data
1852	24.045223	65.55.44.109	192.168.0.4	TLSv1...	105	Change Cipher Spec, Encrypted Handshake Message
1870	24.164605	192.168.0.4	52.204.250.175	TLSv1...	571	Client Hello
1877	24.215316	52.204.250.175	192.168.0.4	TLSv1...	1514	Server Hello
1878	24.215579	52.204.250.175	192.168.0.4	TLSv1...	1514	Certificate [TCP segment of a reassembled PDU]
1880	24.215734	52.204.250.175	192.168.0.4	TLSv1...	205	Server Key Exchange, Server Hello Done
1882	24.219637	192.168.0.4	52.204.250.175	TLSv1...	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1884	24.220415	192.168.0.4	52.204.250.175	TLSv1...	907	Application Data
1891	24.245330	192.168.0.4	23.53.216.181	TLSv1...	571	Client Hello
1893	24.247750	192.168.0.4	65.55.44.109	TLSv1...	1247	Application Data

Content Type: Handshake (22)  
Version: TLS 1.2 (0x0303)  
Length: 89  
Handshake Protocol: Server Hello  
Handshake Type: Server Hello (2)  
Length: 85  
Version: TLS 1.2 (0x0303)  
Random: e72cfac08031c4dd419d05dc4e8856d0972731792b2900d...  
Session ID Length: 32  
Session ID: ed60271055cf51d311a4df37702f95a3897ea176599445f6...  
Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)  
Compression Method: null (0)  
Extensions Length: 13  
Extension: renegotiation\_info (len=1)  
Extension: ec\_point\_formats (len=4)

There is no HTTP OK message.!

The image shows a Wireshark network traffic capture on a macOS system. The interface includes a menu bar at the top with options like File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu bar is a toolbar with various icons for packet analysis. The main display area is divided into three panes. The top pane shows a list of captured packets, with two packets selected: packet 169 (OCSP Request, 460 bytes) and packet 172 (OCSP Response, 1191 bytes). The middle pane shows the details of the selected packet, which is an OCSP Response. The bottom pane shows the raw packet data in hexadecimal and ASCII format. The status bar at the bottom indicates that 20921 packets were captured, 2 were displayed, and 0 were dropped.

No.	Time	Source	Destination	Protocol	Length	Info
169...	93.744559	2601:140:8600:18a0...	2606:4700::6812:19...	OCSP	460	Request
172...	93.798740	2606:4700::6812:19...	2601:140:8600:18a0...	OCSP	1191	Response

Frame 16989: 460 bytes on wire (3680 bits), 460 bytes captured (3680 bits) on interface 0  
Ethernet II, Src: Apple\_13:0e:7c (88:1f:a1:13:0e:7c), Dst: Netgear\_8c:a7:cb (dc:ef:09:8c:a7:cb)  
Internet Protocol Version 6, Src: 2601:140:8600:18a0:a562:33b2:e3b9:6046, Dst: 2606:4700::6812:19f3  
Transmission Control Protocol, Src Port: 53103, Dst Port: 80, Seq: 1, Ack: 1, Len: 386  
Hypertext Transfer Protocol  
Online Certificate Status Protocol

0000 dc ef 09 8c a7 cb 88 1f a1 13 0e 7c 86 dd 60 03 .....  
0010 75 b8 01 96 06 40 26 01 01 40 86 00 18 a0 a5 62 u...@S...@...b  
0020 33 b2 e3 b9 60 46 26 06 47 00 00 00 00 00 00 3...`F&...G...  
0030 00 00 68 12 19 f3 cf 6f 00 50 cf 50 78 7f 04 2b ..h...o...P:Px...+  
0040 27 2a 50 18 10 00 23 15 00 00 50 4f 53 54 20 2f '\*P...#...POST /  
0050 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a HTTP/1.1..Host:  
0060 20 6f 63 73 70 2e 6d 73 6f 63 73 70 2e 63 6f 6d ocsp.ms ocsp.com

Hypertext Transfer Protocol: Protocol  
Page 7 of 7 184 words English (United States)  
Packets: 20921 - Displayed: 2 (0.0%) - Dropped: 0 (0.0%) Profile: Default  
Focus 180%