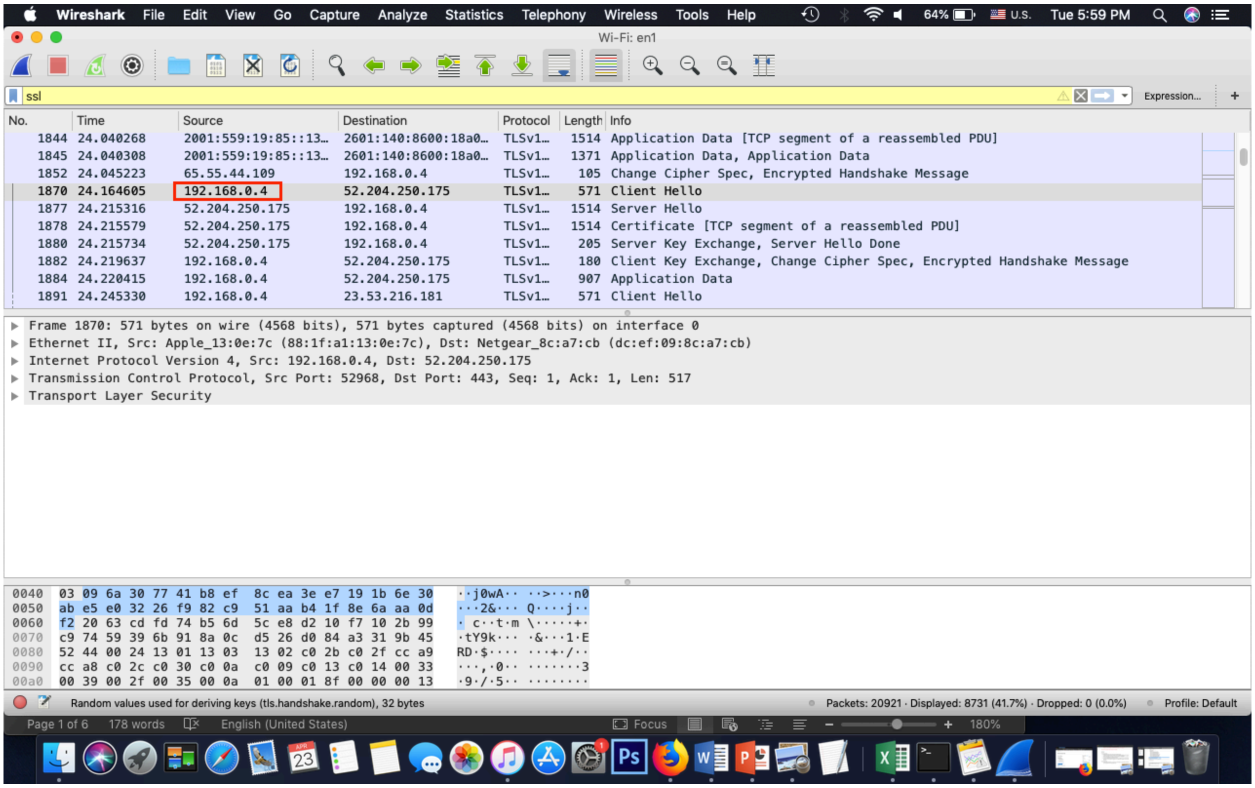
Abdullah Alrfeedi
Lab 8
IT-520

My IP address is (192.168.0.4).


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
64% U.S. Tue 5:59 PM
Wi-Fi: en1
Expression...
+

ssl

```
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
```

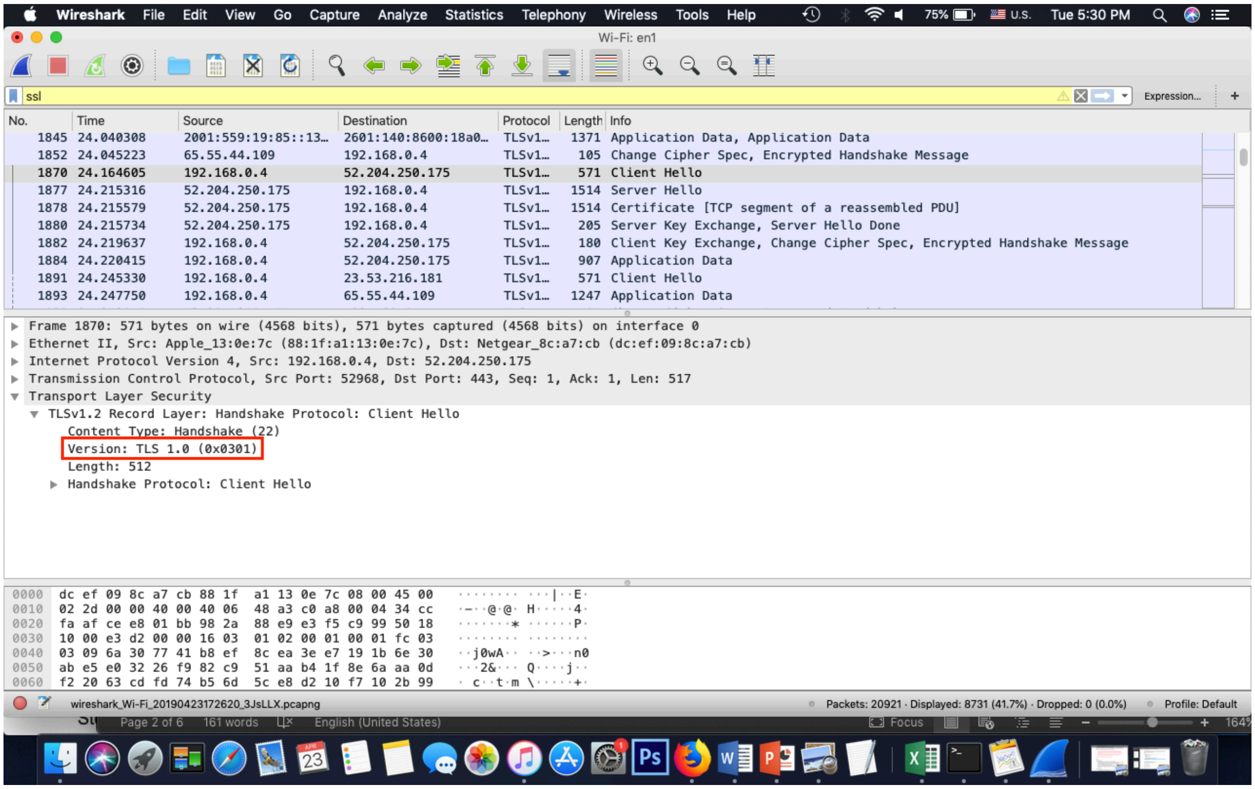
```
0040  03 09 6a 30 77 41 b8 ef  8c ea 3e e7 19 1b 6e 30   ··j0wA·· ··>···n0
0050  ab e5 e0 32 26 f9 82 c9  51 aa b4 1f 8e 6a aa 0d   ···2&··· Q····j··
0060  f2 20 63 cd fd 74 b5 6d  5c e8 d2 10 f7 10 2b 99   · c··t·m \·····+·
0070  c9 74 59 39 6b 91 8a 0c  d5 26 d0 84 a3 31 9b 45   ·tY9k··· ·&···1·E
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·/·5·· ········
```

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

Packets: 20921 · Displayed: 8731 (41.7%) · Dropped: 0 (0.0%)   Profile: Default

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

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



ssl

```
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
```

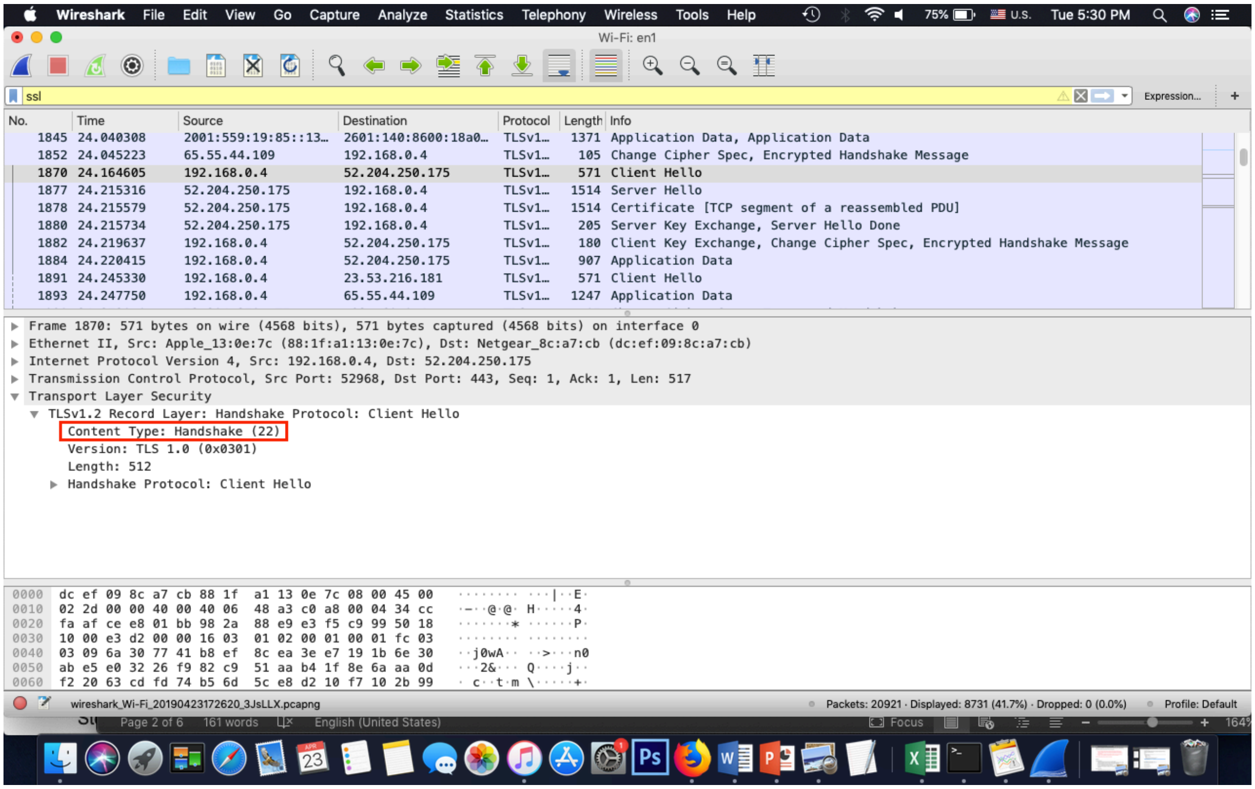
```
0000  dc ef 09 8c a7 cb 88 1f  a1 13 0e 7c 08 00 45 00   ········ ···|··E·
0010  02 2d 00 00 40 00 40 06  48 a3 c0 a8 00 04 34 cc   ·–··@·@· H·····4·
0020  fa af ce e8 01 bb 98 2a  88 e9 e3 f5 c9 99 50 18   ·······* ······P·
0030  10 00 e3 d2 00 00 16 03  01 02 00 01 00 01 fc 03   ········ ········
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   ···2&··· Q····j··
0060  f2 20 63 cd fd 74 b5 6d  5c e8 d2 10 f7 10 2b 99   · c··t·m \·····+·
```

wireshark_Wi-Fi_20190423172620_3JsLLX.pcapng

Packets: 20921 · Displayed: 8731 (41.7%) · Dropped: 0 (0.0%)   Profile: Default

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).


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
75% U.S. Tue 5:30 PM
Wi-Fi: en1
ssl
Expression…
+

```
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
```

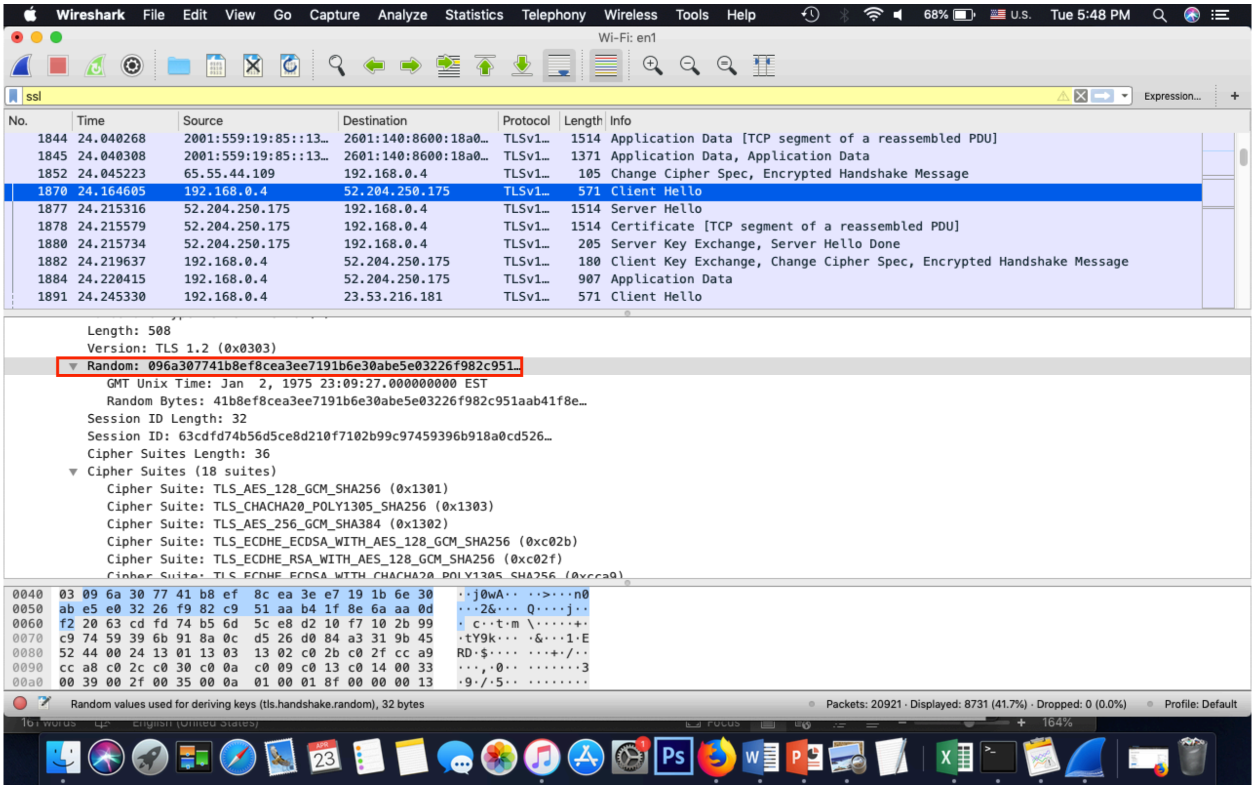
```
▶ Frame 1870: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface 0
▶ Ethernet II, Src: Apple_13:0e:7c (88:1f:a1:13:0e:7c), Dst: Netgear_8c:a7:cb (dc:ef:09:8c:a7:cb)
▶ Internet Protocol Version 4, Src: 192.168.0.4, Dst: 52.204.250.175
▶ Transmission Control Protocol, Src Port: 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   ···2&··· Q····j··
0060  f2 20 63 cd fd 74 b5 6d  5c e8 d2 10 f7 10 2b 99   · c··t·m \·····+·
```

wireshark_Wi-Fi_20190423172620_3JsLLX.pcapng
Packets: 20921 · Displayed: 8731 (41.7%) · Dropped: 0 (0.0%)
Profile: Default
Page 2 of 6
161 words
English (United States)
Focus
164%

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….).



Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
68% U.S. Tue 5:48 PM
Wi-Fi: en1
Expression…

ssl

```
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   ···2&···  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·/·5··  ········
```

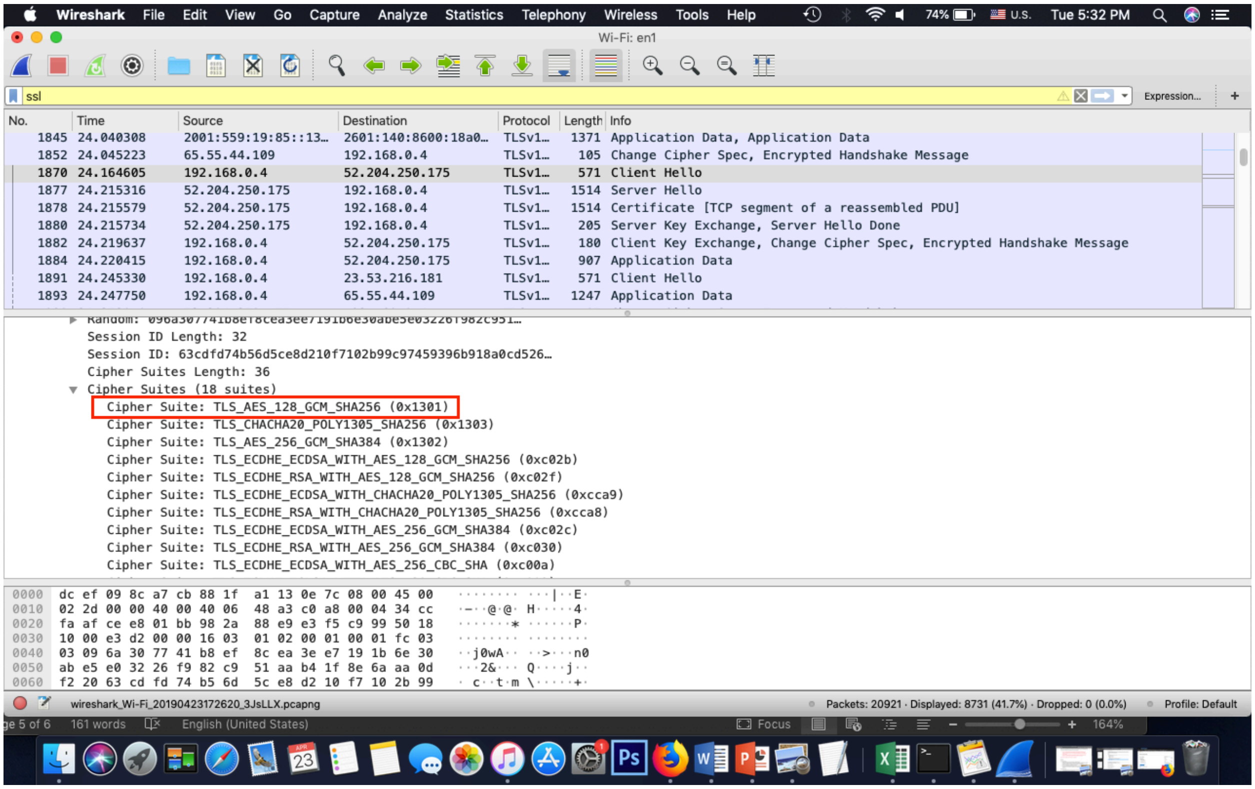
Random values used for deriving keys (tls.handshake.random), 32 bytes

Packets: 20921 · Displayed: 8731 (41.7%) · Dropped: 0 (0.0%) · Profile: Default

4) Does the ClientHello record advertise the cyber 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).



ssl

```
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: 096a307741b8ef8cea3ee7191b6e30abe5e03226f982c951…
      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 (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)
```

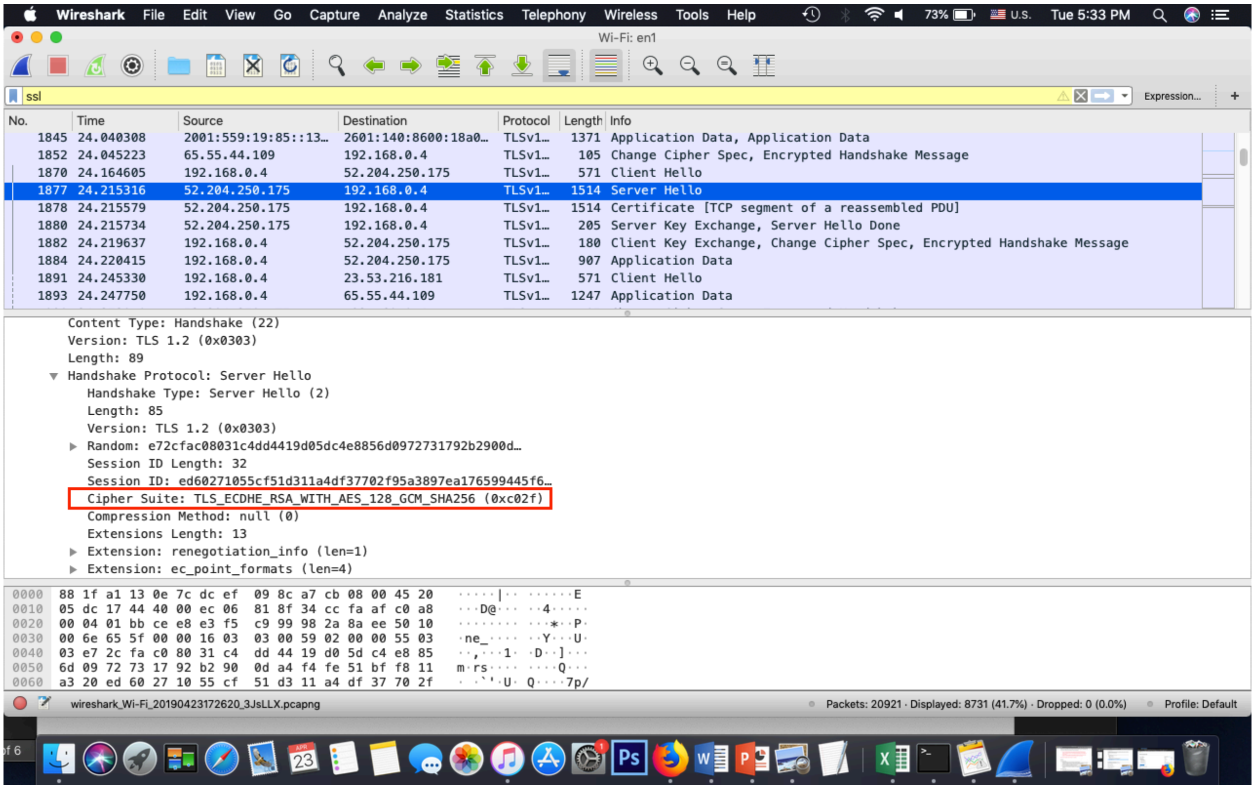
```
0000  dc ef 09 8c a7 cb 88 1f  a1 13 0e 7c 08 00 45 00   ········ ···|··E·
0010  02 2d 00 00 40 00 40 06  48 a3 c0 a8 00 04 34 cc   ·-··@·@· H·····4·
0020  fa af ce e8 01 bb 98 2a  88 e9 e3 f5 c9 99 50 18   ·······* ······P·
0030  10 00 e3 d2 00 00 16 03  01 02 00 01 00 01 fc 03   ········ ········
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   ···2&··· Q····j··
0060  f2 20 63 cd fd 74 b5 6d  5c e8 d2 10 f7 10 2b 99   · c··t·m \·····+·
```

wireshark_Wi-Fi_20190423172620_3JsLLX.pcapng   Packets: 20921 · Displayed: 8731 (41.7%) · Dropped: 0 (0.0%)   Profile: Default

ge 5 of 6   161 words   English (United States)   Focus   164%

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).



ssl

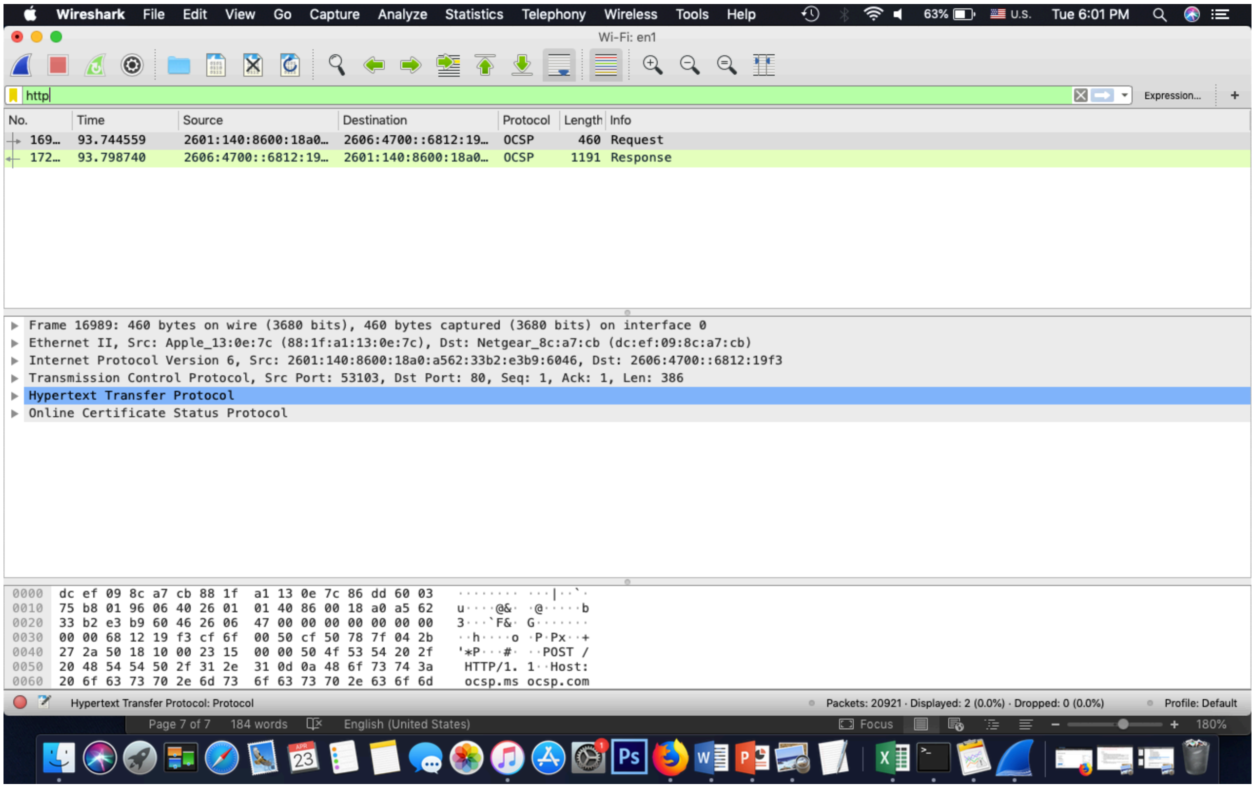
```
No.   Time       Source              Destination         Protocol Length Info
 1845 24.040308  2001:559:19:85::13… 2601:140:8600:18a0… TLSv1…   1371 Application Data, Application Data
 1852 24.045223  65.55.44.109        192.168.0.4         TLSv1…    105 Change Cipher Spec, Encrypted Handshake Message
 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: e72cfac08031c4dd4419d05dc4e8856d0972731792b2900d…
      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)
```

```
0000  88 1f a1 13 0e 7c dc ef  09 8c a7 cb 08 00 45 20   ·····|·· ······E
0010  05 dc 17 44 40 00 ec 06  81 8f 34 cc fa af c0 a8   ···D@··· ··4·····
0020  00 04 01 bb ce e8 e3 f5  c9 99 98 2a 8a ee 50 10   ········ ···*··P·
0030  00 6e 65 5f 00 00 16 03  03 00 59 02 00 00 55 03   ·ne_···· ··Y···U·
0040  03 e7 2c fa c0 80 31 c4  dd 44 19 d0 5d c4 e8 85   ··,···1· ·D··]···
0050  6d 09 72 73 17 92 b2 90  0d a4 f4 fe 51 bf f8 11   m·rs···· ····Q···
0060  a3 20 ed 60 27 10 55 cf  51 d3 11 a4 df 37 70 2f   · ·`'·U· Q····7p/
```

wireshark_Wi-Fi_20190423172620_3JsLLX.pcapng   Packets: 20921 · Displayed: 8731 (41.7%) · Dropped: 0 (0.0%)   Profile: Default

There is no HTTP OK message.!



http

```
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····@&· ·@·····b
0020  33 b2 e3 b9 60 46 26 06  47 00 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

Packets: 20921 · Displayed: 2 (0.0%) · Dropped: 0 (0.0%)

Profile: Default