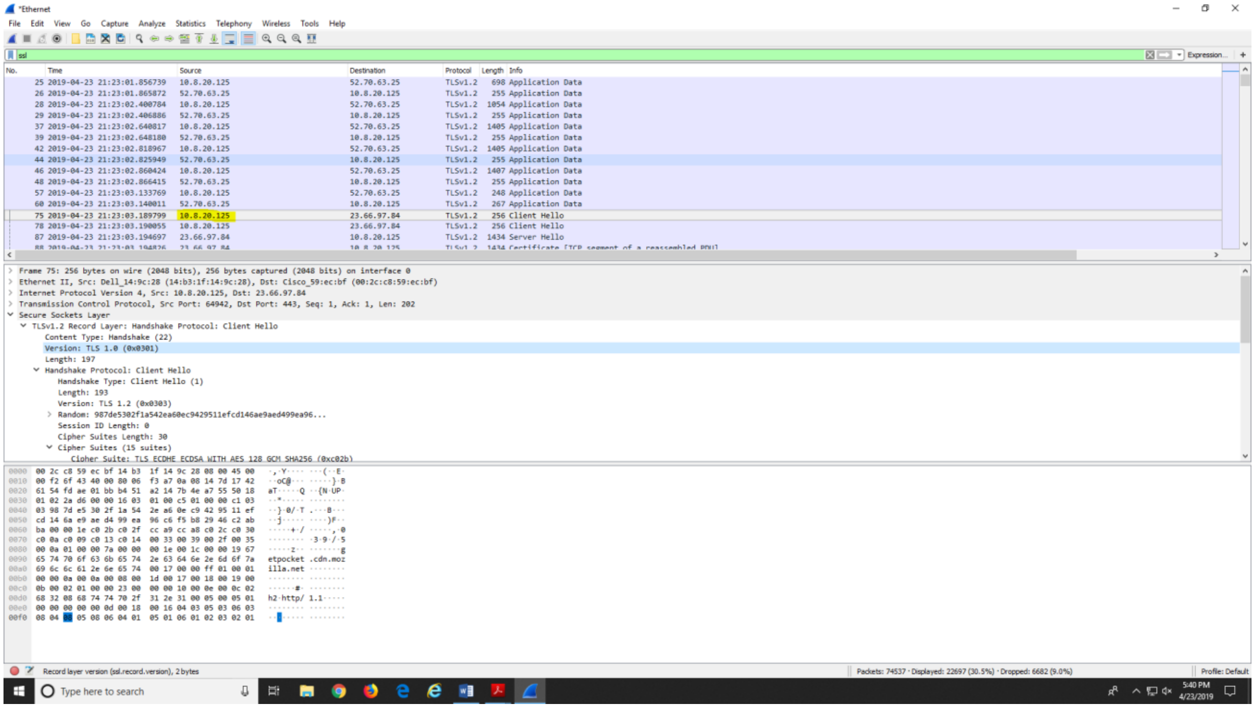
Ameen Almakrami

IT-520-A

Enterprise Infrastructure & Networking

The IP address is 10.8.20.2.125


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssl
Expression...

```
No.   Time                          Source          Destination     Protocol  Length  Info
   25 2019-04-23 21:23:01.856739   10.8.20.125     52.70.63.25     TLSv1.2    698 Application Data
   26 2019-04-23 21:23:01.865872   52.70.63.25     10.8.20.125     TLSv1.2    255 Application Data
   28 2019-04-23 21:23:02.400784   10.8.20.125     52.70.63.25     TLSv1.2   1054 Application Data
   29 2019-04-23 21:23:02.406886   52.70.63.25     10.8.20.125     TLSv1.2    255 Application Data
   37 2019-04-23 21:23:02.640817   10.8.20.125     52.70.63.25     TLSv1.2   1405 Application Data
   39 2019-04-23 21:23:02.648180   52.70.63.25     10.8.20.125     TLSv1.2    255 Application Data
   42 2019-04-23 21:23:02.818967   10.8.20.125     52.70.63.25     TLSv1.2   1405 Application Data
   44 2019-04-23 21:23:02.825949   52.70.63.25     10.8.20.125     TLSv1.2    255 Application Data
   46 2019-04-23 21:23:02.860424   10.8.20.125     52.70.63.25     TLSv1.2   1407 Application Data
   48 2019-04-23 21:23:02.866415   52.70.63.25     10.8.20.125     TLSv1.2    255 Application Data
   57 2019-04-23 21:23:03.133769   10.8.20.125     52.70.63.25     TLSv1.2    248 Application Data
   60 2019-04-23 21:23:03.140011   52.70.63.25     10.8.20.125     TLSv1.2    267 Application Data
   75 2019-04-23 21:23:03.189799   10.8.20.125     23.66.97.84     TLSv1.2    256 Client Hello
   78 2019-04-23 21:23:03.190055   10.8.20.125     23.66.97.84     TLSv1.2    256 Client Hello
   87 2019-04-23 21:23:03.194697   23.66.97.84     10.8.20.125     TLSv1.2   1434 Server Hello
   88 2019-04-23 21:23:03.194826   23.66.97.84     10.8.20.125     TLSv1.2   1434 Certificate [TCP segment of a reassembled PDU]
```

```
> Frame 75: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits) on interface 0
> Ethernet II, Src: Dell_14:9c:28 (14:b3:1f:14:9c:28), Dst: Cisco_59:ec:bf (00:2c:c8:59:ec:bf)
> Internet Protocol Version 4, Src: 10.8.20.125, Dst: 23.66.97.84
> Transmission Control Protocol, Src Port: 64942, Dst Port: 443, Seq: 1, Ack: 1, Len: 202
v Secure Sockets Layer
  v TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 197
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 193
        Version: TLS 1.2 (0x0303)
      > Random: 987de5302f1a542ea60ec9429511efcd146ae9aed499ea96...
        Session ID Length: 0
        Cipher Suites Length: 30
      v Cipher Suites (15 suites)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
```

```
0000  00 2c c8 59 ec bf 14 b3  1f 14 9c 28 08 00 45 00   ·,·Y···· ···(··E·
0010  00 f2 6f 43 40 00 80 06  f3 a7 0a 08 14 7d 17 42   ··oC@··· ·····}·B
0020  61 54 fd ae 01 bb b4 51  a2 14 7b 4e a7 55 50 18   aT·····Q ··{N·UP·
0030  01 02 2a d6 00 00 16 03  01 00 c5 01 00 00 c1 03   ··*····· ········
0040  03 98 7d e5 30 2f 1a 54  2e a6 0e c9 42 95 11 ef   ··}·0/·T .···B···
0050  cd 14 6a e9 ae d4 99 ea  96 c6 f5 b8 29 46 c2 ab   ··j····· ····)F··
0060  ba 00 00 1e c0 2b c0 2f  cc a9 cc a8 c0 2c c0 30   ·····+·/ ·····,·0
0070  c0 0a c0 09 c0 13 c0 14  00 33 00 39 00 2f 00 35   ········ ·3·9·/·5
0080  00 0a 01 00 00 7a 00 00  00 1e 00 1c 00 00 19 67   ·····z·· ·······g
0090  65 74 70 6f 63 6b 65 74  2e 63 64 6e 2e 6d 6f 7a   etpocket .cdn.moz
00a0  69 6c 6c 61 2e 6e 65 74  00 17 00 00 ff 01 00 01   illa.net ········
00b0  00 00 0a 00 0a 00 08 00  1d 00 17 00 18 00 19 00   ········ ········
00c0  0b 00 02 01 00 00 23 00  00 00 10 00 0e 00 0c 02   ······#· ········
00d0  68 32 08 68 74 74 70 2f  31 2e 31 00 05 00 05 01   h2·http/ 1.1·····
00e0  00 00 00 00 00 0d 00 18  00 16 04 03 05 03 06 03   ········ ········
00f0  08 04 08 05 08 06 04 01  05 01 06 01 02 03 02 01   ········ ········
```

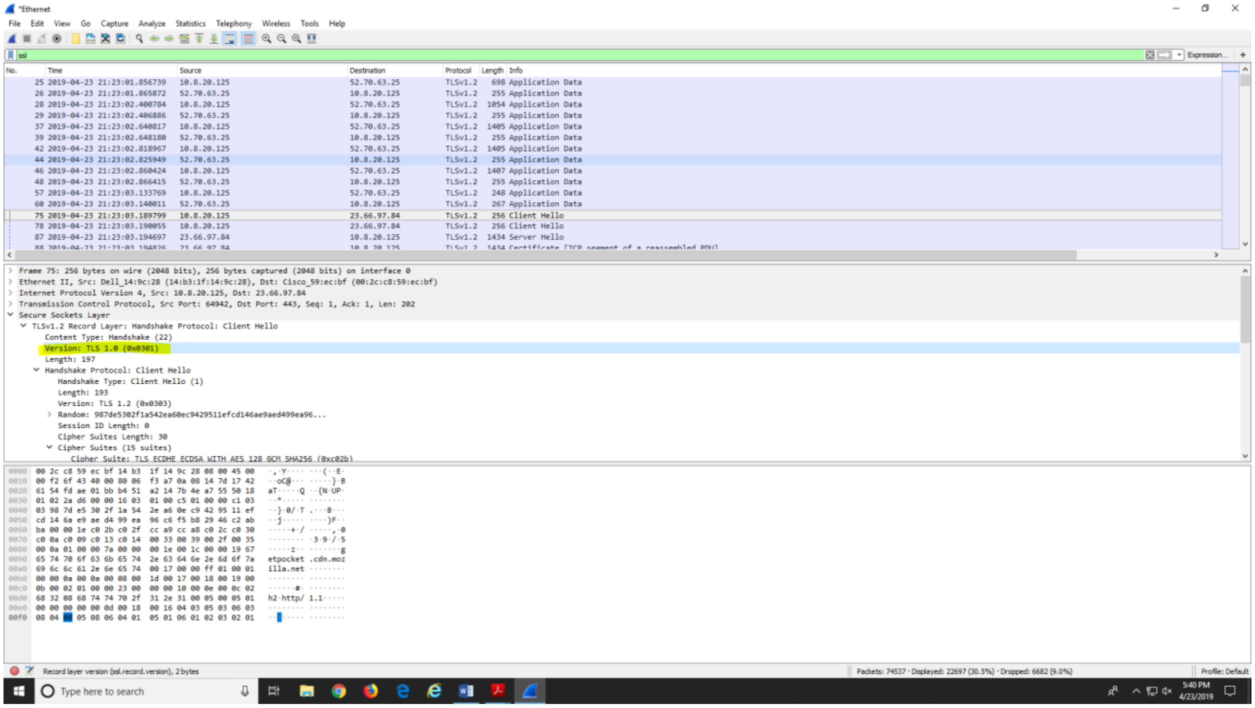
Record layer version (ssl.record.version), 2 bytes

Packets: 74537 · Displayed: 22697 (30.5%) · Dropped: 6682 (9.0%)

Profile: Default

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

Its TLS 1.0(0x0301)


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+
Type here to search
5:40 PM
4/23/2019

Filter: ssl

```
No.   Time                          Source         Destination    Protocol Length Info
   25 2019-04-23 21:23:01.856739    10.8.20.125    52.70.63.25    TLSv1.2   698 Application Data
   26 2019-04-23 21:23:01.865872    52.70.63.25    10.8.20.125    TLSv1.2   255 Application Data
   28 2019-04-23 21:23:02.400784    10.8.20.125    52.70.63.25    TLSv1.2  1054 Application Data
   29 2019-04-23 21:23:02.406886    52.70.63.25    10.8.20.125    TLSv1.2   255 Application Data
   37 2019-04-23 21:23:02.640817    10.8.20.125    52.70.63.25    TLSv1.2  1405 Application Data
   39 2019-04-23 21:23:02.648180    52.70.63.25    10.8.20.125    TLSv1.2   255 Application Data
   42 2019-04-23 21:23:02.818967    10.8.20.125    52.70.63.25    TLSv1.2  1405 Application Data
   44 2019-04-23 21:23:02.825949    52.70.63.25    10.8.20.125    TLSv1.2   255 Application Data
   46 2019-04-23 21:23:02.860424    10.8.20.125    52.70.63.25    TLSv1.2  1407 Application Data
   48 2019-04-23 21:23:02.866415    52.70.63.25    10.8.20.125    TLSv1.2   255 Application Data
   57 2019-04-23 21:23:03.133769    10.8.20.125    52.70.63.25    TLSv1.2   248 Application Data
   60 2019-04-23 21:23:03.140011    52.70.63.25    10.8.20.125    TLSv1.2   267 Application Data
   75 2019-04-23 21:23:03.189799    10.8.20.125    23.66.97.84    TLSv1.2   256 Client Hello
   78 2019-04-23 21:23:03.190055    10.8.20.125    23.66.97.84    TLSv1.2   256 Client Hello
   87 2019-04-23 21:23:03.194697    23.66.97.84    10.8.20.125    TLSv1.2  1434 Server Hello
   88 2019-04-23 21:23:03.194826    23.66.97.84    10.8.20.125    TLSv1.2  1434 Certificate [TCP segment of a reassembled PDU]
```

```
> Frame 75: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits) on interface 0
> Ethernet II, Src: Dell_14:9c:28 (14:b3:1f:14:9c:28), Dst: Cisco_59:ec:bf (00:2c:c8:59:ec:bf)
> Internet Protocol Version 4, Src: 10.8.20.125, Dst: 23.66.97.84
> Transmission Control Protocol, Src Port: 64942, Dst Port: 443, Seq: 1, Ack: 1, Len: 202
v Secure Sockets Layer
  v TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 197
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 193
        Version: TLS 1.2 (0x0303)
      > Random: 987de5302f1a542ea60ec9429511efcd146ae9aed499ea96...
        Session ID Length: 0
        Cipher Suites Length: 30
      v Cipher Suites (15 suites)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
```

```
0000  00 2c c8 59 ec bf 14 b3  1f 14 9c 28 08 00 45 00   ·,·Y···· ···(··E·
0010  00 f2 6f 43 40 00 80 06  f3 a7 0a 08 14 7d 17 42   ··oC@··· ·····}·B
0020  61 54 fd ae 01 bb b4 51  a2 14 7b 4e a7 55 50 18   aT·····Q ··{N·UP·
0030  01 02 2a d6 00 00 16 03  01 00 c5 01 00 00 c1 03   ··*····· ········
0040  03 98 7d e5 30 2f 1a 54  2e a6 0e c9 42 95 11 ef   ··}·0/·T .···B···
0050  cd 14 6a e9 ae d4 99 ea  96 c6 f5 b8 29 46 c2 ab   ··j····· ····)F··
0060  ba 00 00 1e c0 2b c0 2f  cc a9 cc a8 c0 2c c0 30   ·····+·/ ·····,·0
0070  c0 0a c0 09 c0 13 c0 14  00 33 00 39 00 2f 00 35   ········ ·3·9·/·5
0080  00 0a 01 00 00 7a 00 00  00 1e 00 1c 00 00 19 67   ·····z·· ·······g
0090  65 74 70 6f 63 6b 65 74  2e 63 64 6e 2e 6d 6f 7a   etpocket .cdn.moz
00a0  69 6c 6c 61 2e 6e 65 74  00 17 00 00 ff 01 00 01   illa.net ········
00b0  00 00 0a 00 0a 00 08 00  1d 00 17 00 18 00 19 00   ········ ········
00c0  0b 00 02 01 00 00 23 00  00 00 10 00 0e 00 0c 02   ······#· ········
00d0  68 32 08 68 74 74 70 2f  31 2e 31 00 05 00 05 01   h2·http/ 1.1·····
00e0  00 00 00 00 00 0d 00 18  00 16 04 03 05 03 06 03   ········ ········
00f0  08 04 08 05 08 06 04 01  05 01 06 01 02 03 02 01   ········ ········
```

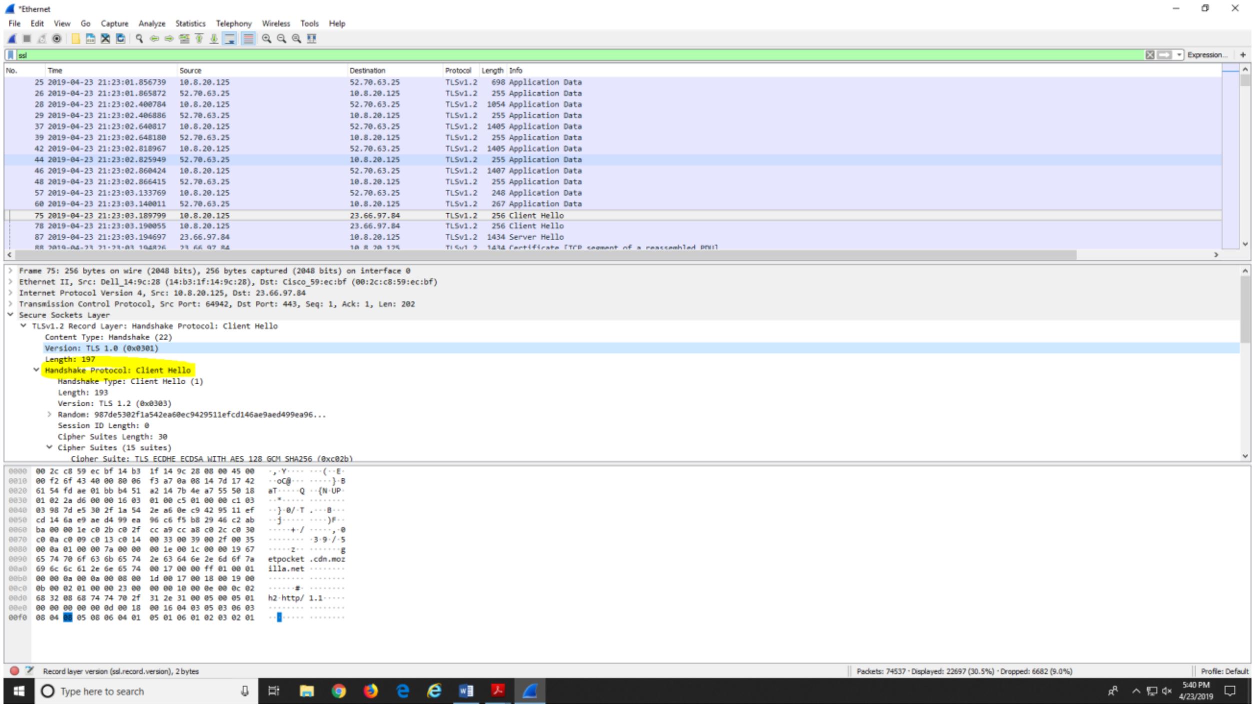
Record layer version (ssl.record.version), 2 bytes

Packets: 74537 · Displayed: 22697 (30.5%) · Dropped: 6682 (9.0%)

Profile: Default

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

Its Handshake protocol: client Hello



```
No.   Time                        Source          Destination     Protocol  Length Info
   25 2019-04-23 21:23:01.856739  10.8.20.125     52.70.63.25     TLSv1.2    698 Application Data
   26 2019-04-23 21:23:01.865872  52.70.63.25     10.8.20.125     TLSv1.2    255 Application Data
   28 2019-04-23 21:23:02.400784  10.8.20.125     52.70.63.25     TLSv1.2   1054 Application Data
   29 2019-04-23 21:23:02.406886  52.70.63.25     10.8.20.125     TLSv1.2    255 Application Data
   37 2019-04-23 21:23:02.640817  10.8.20.125     52.70.63.25     TLSv1.2   1405 Application Data
   39 2019-04-23 21:23:02.648180  52.70.63.25     10.8.20.125     TLSv1.2    255 Application Data
   42 2019-04-23 21:23:02.818967  10.8.20.125     52.70.63.25     TLSv1.2   1405 Application Data
   44 2019-04-23 21:23:02.825949  52.70.63.25     10.8.20.125     TLSv1.2    255 Application Data
   46 2019-04-23 21:23:02.860424  10.8.20.125     52.70.63.25     TLSv1.2   1407 Application Data
   48 2019-04-23 21:23:02.866415  52.70.63.25     10.8.20.125     TLSv1.2    255 Application Data
   57 2019-04-23 21:23:03.133769  10.8.20.125     52.70.63.25     TLSv1.2    248 Application Data
   60 2019-04-23 21:23:03.140011  52.70.63.25     10.8.20.125     TLSv1.2    267 Application Data
   75 2019-04-23 21:23:03.189799  10.8.20.125     23.66.97.84     TLSv1.2    256 Client Hello
   78 2019-04-23 21:23:03.190055  10.8.20.125     23.66.97.84     TLSv1.2    256 Client Hello
   87 2019-04-23 21:23:03.194697  23.66.97.84     10.8.20.125     TLSv1.2   1434 Server Hello
   88 2019-04-23 21:23:03.194826  23.66.97.84     10.8.20.125     TLSv1.2   1434 Certificate [TCP segment of a reassembled PDU]
```

```
> Frame 75: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits) on interface 0
> Ethernet II, Src: Dell_14:9c:28 (14:b3:1f:14:9c:28), Dst: Cisco_59:ec:bf (00:2c:c8:59:ec:bf)
> Internet Protocol Version 4, Src: 10.8.20.125, Dst: 23.66.97.84
> Transmission Control Protocol, Src Port: 64942, Dst Port: 443, Seq: 1, Ack: 1, Len: 202
v Secure Sockets Layer
  v TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 197
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 193
        Version: TLS 1.2 (0x0303)
      > Random: 987de5302f1a542ea60ec9429511efcd146ae9aed499ea96...
        Session ID Length: 0
        Cipher Suites Length: 30
      v Cipher Suites (15 suites)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
```

```
0000  00 2c c8 59 ec bf 14 b3  1f 14 9c 28 08 00 45 00   ·,·Y···· ···(··E·
0010  00 f2 6f 43 40 00 80 06  f3 a7 0a 08 14 7d 17 42   ··oC@··· ·····}·B
0020  61 54 fd ae 01 bb b4 51  a2 14 7b 4e a7 55 50 18   aT·····Q ··{N·UP·
0030  01 02 2a d6 00 00 16 03  01 00 c5 01 00 00 c1 03   ··*····· ········
0040  03 98 7d e5 30 2f 1a 54  2e a6 0e c9 42 95 11 ef   ··}·0/·T .···B···
0050  cd 14 6a e9 ae d4 99 ea  96 c6 f5 b8 29 46 c2 ab   ··j····· ····)F··
0060  ba 00 00 1e c0 2b c0 2f  cc a9 cc a8 c0 2c c0 30   ·····+·/ ·····,·0
0070  c0 0a c0 09 c0 13 c0 14  00 33 00 39 00 2f 00 35   ········ ·3·9·/·5
0080  00 0a 01 00 00 7a 00 00  00 1e 00 1c 00 00 19 67   ·····z·· ·······g
0090  65 74 70 6f 63 6b 65 74  2e 63 64 6e 2e 6d 6f 7a   etpocket .cdn.moz
00a0  69 6c 6c 61 2e 6e 65 74  00 17 00 00 ff 01 00 01   illa.net ········
00b0  00 00 0a 00 0a 00 08 00  1d 00 17 00 18 00 19 00   ········ ········
00c0  0b 00 02 01 00 00 23 00  00 00 10 00 0e 00 0c 02   ······#· ········
00d0  68 32 08 68 74 74 70 2f  31 2e 31 00 05 00 05 01   h2·http/ 1.1·····
00e0  00 00 00 00 00 0d 00 18  00 16 04 03 05 03 06 03   ········ ········
00f0  08 04 08 05 08 06 04 01  05 01 06 01 02 03 02 01   ········ ········
```

Record layer version (ssl.record.version), 2 bytes

Packets: 74537 · Displayed: 22697 (30.5%) · Dropped: 6682 (9.0%)

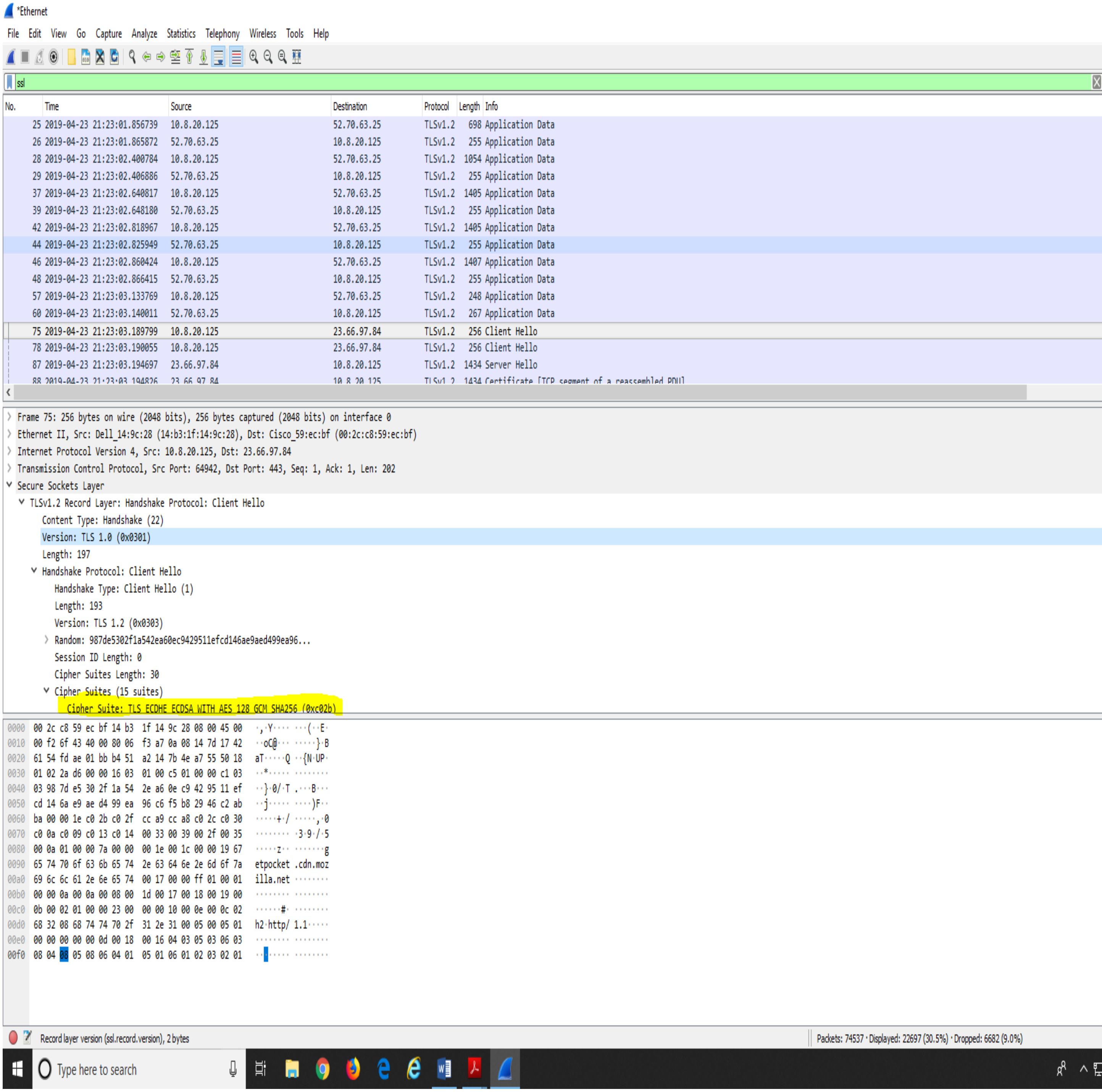
Profile: Default

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

Mine does not show challenge in hexadecimal notation.

4. Does the Client Hello 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?

public key ECDSA symmetric key AES 128 GCM hash algorithm SHA256


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Type here to search

```
ssl
```

```
No.   Time                        Source         Destination    Protocol  Length Info
   25 2019-04-23 21:23:01.856739  10.8.20.125    52.70.63.25    TLSv1.2    698 Application Data
   26 2019-04-23 21:23:01.865872  52.70.63.25    10.8.20.125    TLSv1.2    255 Application Data
   28 2019-04-23 21:23:02.400784  10.8.20.125    52.70.63.25    TLSv1.2   1054 Application Data
   29 2019-04-23 21:23:02.406886  52.70.63.25    10.8.20.125    TLSv1.2    255 Application Data
   37 2019-04-23 21:23:02.640817  10.8.20.125    52.70.63.25    TLSv1.2   1405 Application Data
   39 2019-04-23 21:23:02.648180  52.70.63.25    10.8.20.125    TLSv1.2    255 Application Data
   42 2019-04-23 21:23:02.818967  10.8.20.125    52.70.63.25    TLSv1.2   1405 Application Data
   44 2019-04-23 21:23:02.825949  52.70.63.25    10.8.20.125    TLSv1.2    255 Application Data
   46 2019-04-23 21:23:02.860424  10.8.20.125    52.70.63.25    TLSv1.2   1407 Application Data
   48 2019-04-23 21:23:02.866415  52.70.63.25    10.8.20.125    TLSv1.2    255 Application Data
   57 2019-04-23 21:23:03.133769  10.8.20.125    52.70.63.25    TLSv1.2    248 Application Data
   60 2019-04-23 21:23:03.140011  52.70.63.25    10.8.20.125    TLSv1.2    267 Application Data
   75 2019-04-23 21:23:03.189799  10.8.20.125    23.66.97.84    TLSv1.2    256 Client Hello
   78 2019-04-23 21:23:03.190055  10.8.20.125    23.66.97.84    TLSv1.2    256 Client Hello
   87 2019-04-23 21:23:03.194697  23.66.97.84    10.8.20.125    TLSv1.2   1434 Server Hello
   88 2019-04-23 21:23:03.194826  23.66.97.84    10.8.20.125    TLSv1.2   1434 Certificate [TCP segment of a reassembled PDU]
```

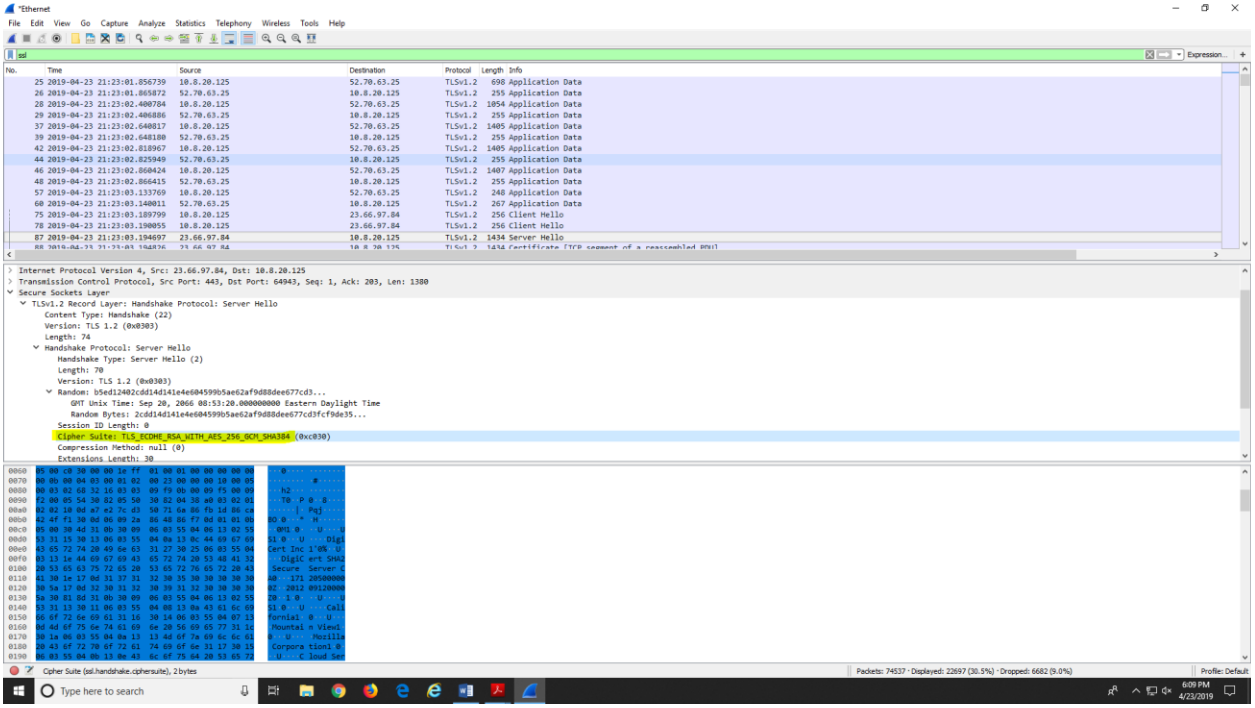
```
> Frame 75: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits) on interface 0
> Ethernet II, Src: Dell_14:9c:28 (14:b3:1f:14:9c:28), Dst: Cisco_59:ec:bf (00:2c:c8:59:ec:bf)
> Internet Protocol Version 4, Src: 10.8.20.125, Dst: 23.66.97.84
> Transmission Control Protocol, Src Port: 64942, Dst Port: 443, Seq: 1, Ack: 1, Len: 202
v Secure Sockets Layer
  v TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 197
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 193
        Version: TLS 1.2 (0x0303)
      > Random: 987de5302f1a542ea60ec9429511efcd146ae9aed499ea96...
        Session ID Length: 0
        Cipher Suites Length: 30
      v Cipher Suites (15 suites)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
```

```
0000  00 2c c8 59 ec bf 14 b3  1f 14 9c 28 08 00 45 00   ·,·Y···· ···(··E·
0010  00 f2 6f 43 40 00 80 06  f3 a7 0a 08 14 7d 17 42   ··oC@··· ·····}·B
0020  61 54 fd ae 01 bb b4 51  a2 14 7b 4e a7 55 50 18   aT·····Q ··{N·UP·
0030  01 02 2a d6 00 00 16 03  01 00 c5 01 00 00 c1 03   ··*····· ········
0040  03 98 7d e5 30 2f 1a 54  2e a6 0e c9 42 95 11 ef   ··}·0/·T .···B···
0050  cd 14 6a e9 ae d4 99 ea  96 c6 f5 b8 29 46 c2 ab   ··j····· ····)F··
0060  ba 00 00 1e c0 2b c0 2f  cc a9 cc a8 c0 2c c0 30   ·····+·/ ·····,·0
0070  c0 0a c0 09 c0 13 c0 14  00 33 00 39 00 2f 00 35   ········ ·3·9·/·5
0080  00 0a 01 00 00 7a 00 00  00 1e 00 1c 00 00 19 67   ·····z·· ·······g
0090  65 74 70 6f 63 6b 65 74  2e 63 64 6e 2e 6d 6f 7a   etpocket .cdn.moz
00a0  69 6c 6c 61 2e 6e 65 74  00 17 00 00 ff 01 00 01   illa.net ········
00b0  00 00 0a 00 0a 00 08 00  1d 00 17 00 18 00 19 00   ········ ········
00c0  0b 00 02 01 00 00 23 00  00 00 10 00 0e 00 0c 02   ······#· ········
00d0  68 32 08 68 74 74 70 2f  31 2e 31 00 05 00 05 01   h2·http/ 1.1·····
00e0  00 00 00 00 00 0d 00 18  00 16 04 03 05 03 06 03   ········ ········
00f0  08 04 08 05 08 06 04 01  05 01 06 01 02 03 02 01   ········ ········
```

```
Record layer version (ssl.record.version), 2 bytes        Packets: 74537 · Displayed: 22697 (30.5%) · Dropped: 6682 (9.0%)
```

1. Locate the Server Hello SSL record. Does this record specify a chosen cipher suite? What are the algorithms in the chosen cipher suite?
   Public key

Public key RSA, symmetric key AES, hash SHA384



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssl
Expression…

```
No.    Time                         Source          Destination     Protocol  Length Info
    25 2019-04-23 21:23:01.856739   10.8.20.125     52.70.63.25     TLSv1.2    698 Application Data
    26 2019-04-23 21:23:01.865872   52.70.63.25     10.8.20.125     TLSv1.2    255 Application Data
    28 2019-04-23 21:23:02.400784   10.8.20.125     52.70.63.25     TLSv1.2   1054 Application Data
    29 2019-04-23 21:23:02.406886   52.70.63.25     10.8.20.125     TLSv1.2    255 Application Data
    37 2019-04-23 21:23:02.640817   10.8.20.125     52.70.63.25     TLSv1.2   1405 Application Data
    39 2019-04-23 21:23:02.648180   52.70.63.25     10.8.20.125     TLSv1.2    255 Application Data
    42 2019-04-23 21:23:02.818967   10.8.20.125     52.70.63.25     TLSv1.2   1405 Application Data
    44 2019-04-23 21:23:02.825949   52.70.63.25     10.8.20.125     TLSv1.2    255 Application Data
    46 2019-04-23 21:23:02.860424   10.8.20.125     52.70.63.25     TLSv1.2   1407 Application Data
    48 2019-04-23 21:23:02.866415   52.70.63.25     10.8.20.125     TLSv1.2    255 Application Data
    57 2019-04-23 21:23:03.133769   10.8.20.125     52.70.63.25     TLSv1.2    248 Application Data
    60 2019-04-23 21:23:03.140011   52.70.63.25     10.8.20.125     TLSv1.2    267 Application Data
    75 2019-04-23 21:23:03.189799   10.8.20.125     23.66.97.84     TLSv1.2    256 Client Hello
    78 2019-04-23 21:23:03.190055   10.8.20.125     23.66.97.84     TLSv1.2    256 Client Hello
    87 2019-04-23 21:23:03.194697   23.66.97.84     10.8.20.125     TLSv1.2   1434 Server Hello
    88 2019-04-23 21:23:03.194826   23.66.97.84     10.8.20.125     TLSv1.2   1434 Certificate [TCP segment of a reassembled PDU]
```

```
> Internet Protocol Version 4, Src: 23.66.97.84, Dst: 10.8.20.125
> Transmission Control Protocol, Src Port: 443, Dst Port: 64943, Seq: 1, Ack: 203, Len: 1380
v Secure Sockets Layer
  v TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 74
    v Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 70
        Version: TLS 1.2 (0x0303)
      v Random: b5ed12402cdd14d141e4e604599b5ae62af9d88dee677cd3...
          GMT Unix Time: Sep 20, 2066 08:53:20.000000000 Eastern Daylight Time
          Random Bytes: 2cdd14d141e4e604599b5ae62af9d88dee677cd3fcf9de35...
        Session ID Length: 0
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
        Compression Method: null (0)
        Extensions Length: 30
```

```
0060  05 00 c0 30 00 00 1e ff  01 00 01 00 00 00 00 00   ...0.... ........
0070  00 0b 00 04 03 00 01 02  00 23 00 00 00 10 00 05   ........ .#......
0080  00 03 02 68 32 16 03 03  09 f9 0b 00 09 f5 00 09   ...h2... ........
0090  f2 00 05 54 30 82 05 50  30 82 04 38 a0 03 02 01   ...T0..P 0..8....
00a0  02 02 10 0d a7 e2 7c d3  50 71 6a 86 fb 1d 86 ca   ......|. Pqj.....
00b0  42 4f f1 30 0d 06 09 2a  86 48 86 f7 0d 01 01 0b   BO.0...* .H......
00c0  05 00 30 4d 31 0b 30 09  06 03 55 04 06 13 02 55   ..0M1.0. ..U....U
00d0  53 31 15 30 13 06 03 55  04 0a 13 0c 44 69 67 69   S1.0...U ....Digi
00e0  43 65 72 74 20 49 6e 63  31 27 30 25 06 03 55 04   Cert Inc 1'0%..U.
00f0  03 13 1e 44 69 67 69 43  65 72 74 20 53 48 41 32   ...DigiC ert SHA2
0100  20 53 65 63 75 72 65 20  53 65 72 76 65 72 20 43    Secure  Server C
0110  41 30 1e 17 0d 31 37 31  32 30 35 30 30 30 30 30   A0...171 20500000
0120  30 5a 17 0d 32 30 31 32  30 39 31 32 30 30 30 30   0Z..2012 09120000
0130  5a 30 81 8d 31 0b 30 09  06 03 55 04 06 13 02 55   Z0..1.0. ..U....U
0140  53 31 13 30 11 06 03 55  04 08 13 0a 43 61 6c 69   S1.0...U ....Cali
0150  66 6f 72 6e 69 61 31 16  30 14 06 03 55 04 07 13   fornia1. 0...U...
0160  0d 4d 6f 75 6e 74 61 69  6e 20 56 69 65 77 31 1c   .Mountai n View1.
0170  30 1a 06 03 55 04 0a 13  13 4d 6f 7a 69 6c 6c 61   0...U... .Mozilla
0180  20 43 6f 72 70 6f 72 61  74 69 6f 6e 31 17 30 15    Corpora tion1.0.
0190  06 03 55 04 0b 13 0e 43  6c 6f 75 64 20 53 65 72   ..U....C loud Ser
```

Cipher Suite (ssl.handshake.ciphersuite), 2 bytes | Packets: 74537 · Displayed: 22697 (30.5%) · Dropped: 6682 (9.0%) | Profile: Default