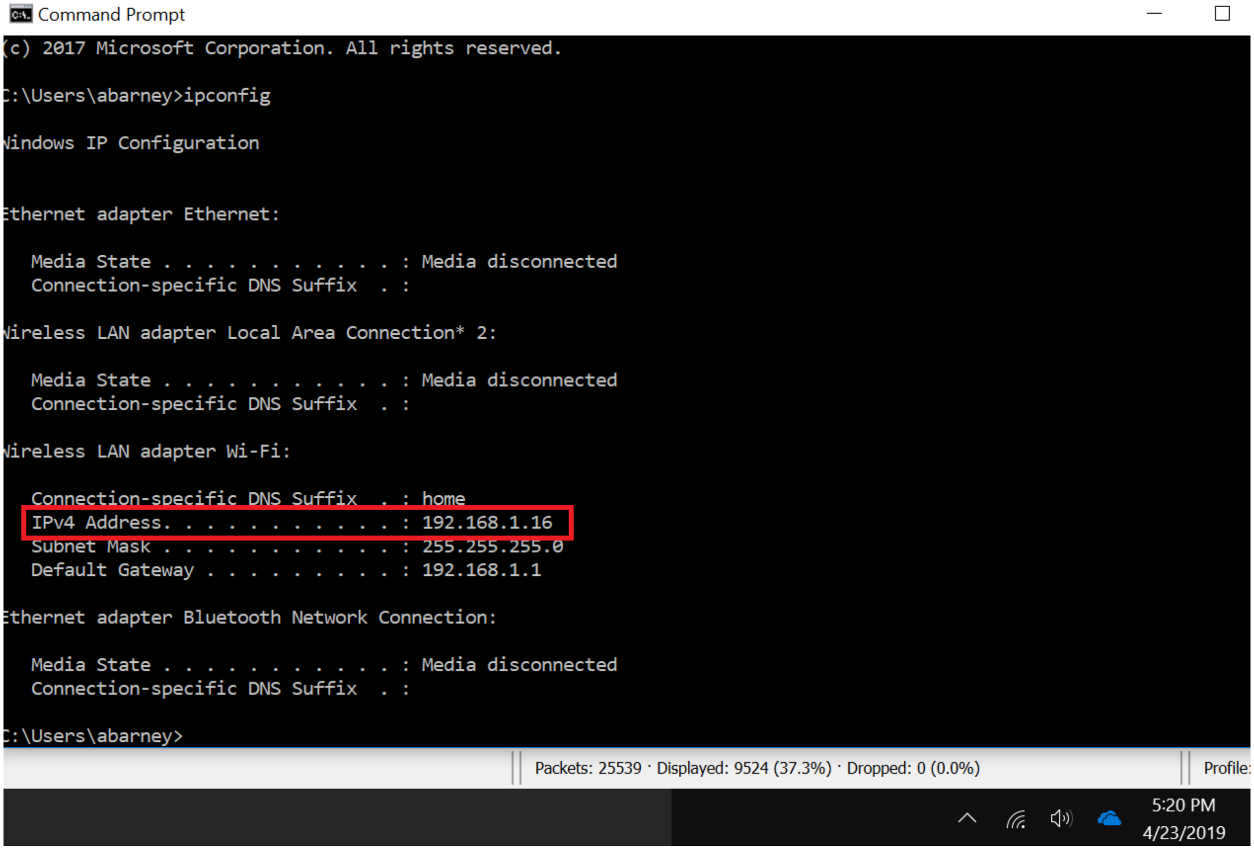
Lab 8

IP: 192.168.1.16

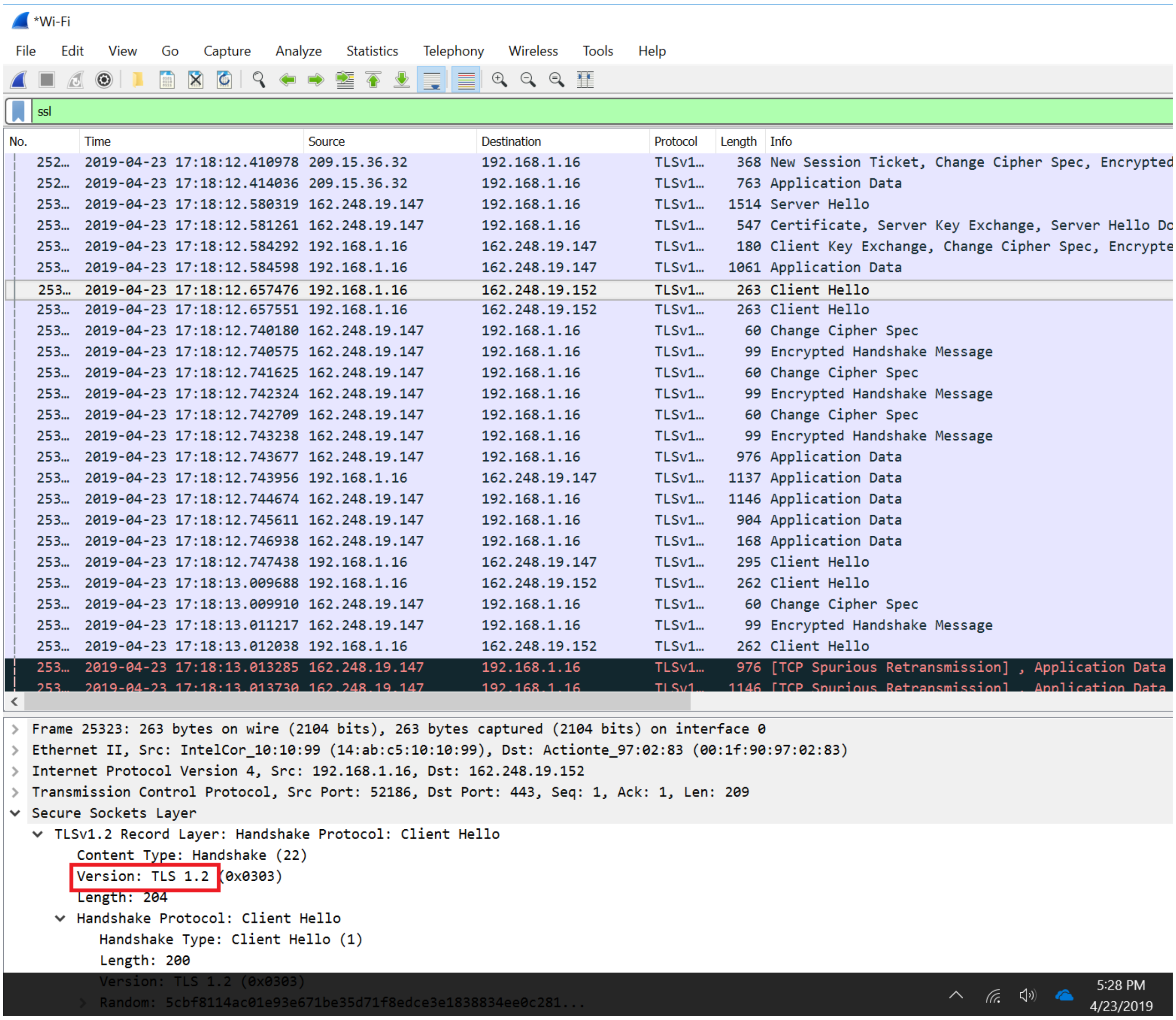


```
(c) 2017 Microsoft Corporation. All rights reserved.

:\Users\abarney>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : home
   IPv4 Address. . . . . . . . . . . : 192.168.1.16
   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  . :

:\Users\abarney>
```

Packets: 25539 · Displayed: 9524 (37.3%) · Dropped: 0 (0.0%)

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

TSL 1.2

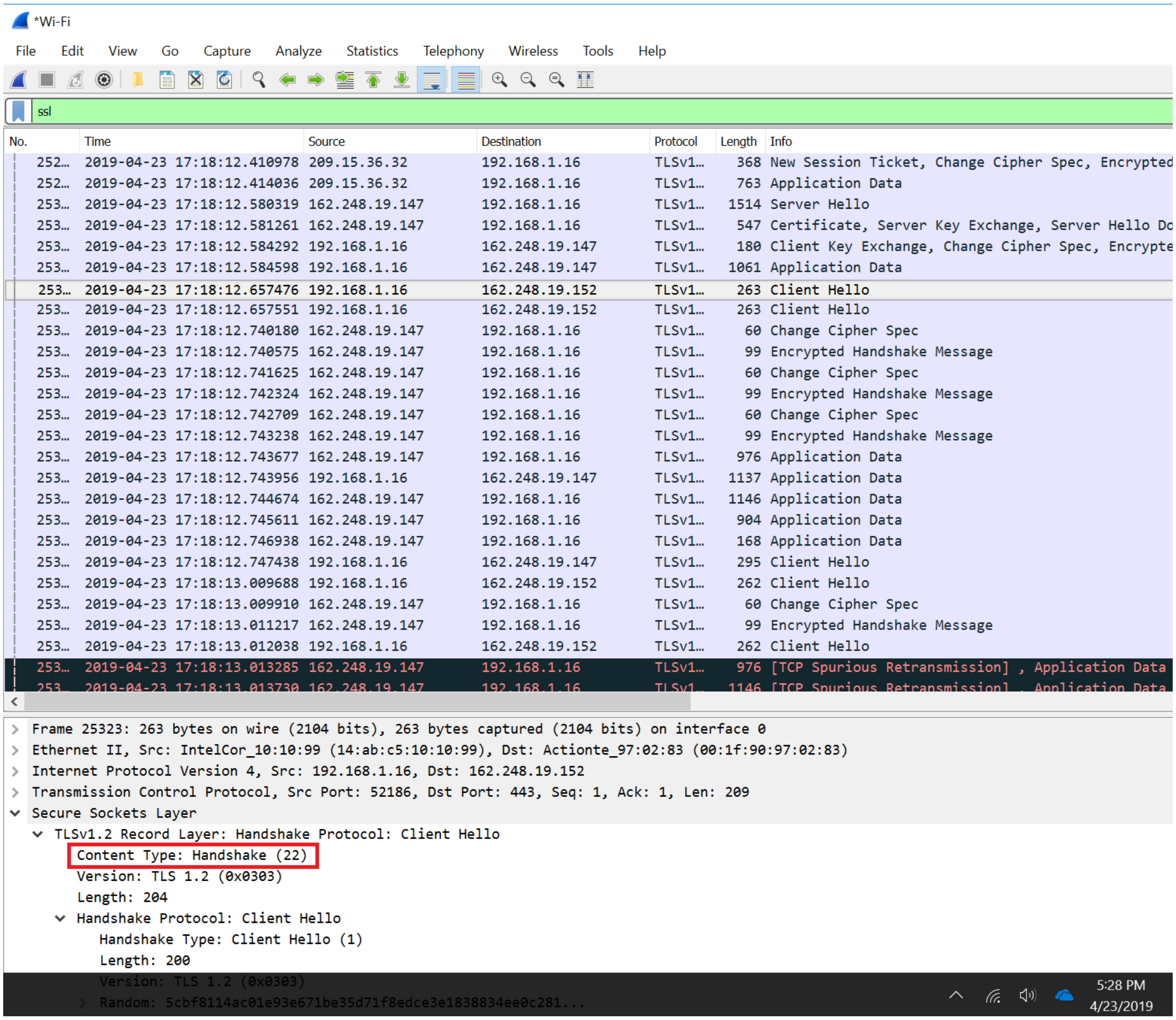

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssl
5:28 PM
4/23/2019

```
No.   Time                        Source          Destination     Protocol Length Info
252…  2019-04-23 17:18:12.410978 209.15.36.32    192.168.1.16    TLSv1…    368 New Session Ticket, Change Cipher Spec, Encrypted
252…  2019-04-23 17:18:12.414036 209.15.36.32    192.168.1.16    TLSv1…    763 Application Data
253…  2019-04-23 17:18:12.580319 162.248.19.147  192.168.1.16    TLSv1…   1514 Server Hello
253…  2019-04-23 17:18:12.581261 162.248.19.147  192.168.1.16    TLSv1…    547 Certificate, Server Key Exchange, Server Hello Do
253…  2019-04-23 17:18:12.584292 192.168.1.16    162.248.19.147  TLSv1…    180 Client Key Exchange, Change Cipher Spec, Encrypte
253…  2019-04-23 17:18:12.584598 192.168.1.16    162.248.19.147  TLSv1…   1061 Application Data
253…  2019-04-23 17:18:12.657476 192.168.1.16    162.248.19.152  TLSv1…    263 Client Hello
253…  2019-04-23 17:18:12.657551 192.168.1.16    162.248.19.152  TLSv1…    263 Client Hello
253…  2019-04-23 17:18:12.740180 162.248.19.147  192.168.1.16    TLSv1…     60 Change Cipher Spec
253…  2019-04-23 17:18:12.740575 162.248.19.147  192.168.1.16    TLSv1…     99 Encrypted Handshake Message
253…  2019-04-23 17:18:12.741625 162.248.19.147  192.168.1.16    TLSv1…     60 Change Cipher Spec
253…  2019-04-23 17:18:12.742324 162.248.19.147  192.168.1.16    TLSv1…     99 Encrypted Handshake Message
253…  2019-04-23 17:18:12.742709 162.248.19.147  192.168.1.16    TLSv1…     60 Change Cipher Spec
253…  2019-04-23 17:18:12.743238 162.248.19.147  192.168.1.16    TLSv1…     99 Encrypted Handshake Message
253…  2019-04-23 17:18:12.743677 162.248.19.147  192.168.1.16    TLSv1…    976 Application Data
253…  2019-04-23 17:18:12.743956 192.168.1.16    162.248.19.147  TLSv1…   1137 Application Data
253…  2019-04-23 17:18:12.744674 162.248.19.147  192.168.1.16    TLSv1…   1146 Application Data
253…  2019-04-23 17:18:12.745611 162.248.19.147  192.168.1.16    TLSv1…    904 Application Data
253…  2019-04-23 17:18:12.746938 162.248.19.147  192.168.1.16    TLSv1…    168 Application Data
253…  2019-04-23 17:18:12.747438 192.168.1.16    162.248.19.147  TLSv1…    295 Client Hello
253…  2019-04-23 17:18:13.009688 192.168.1.16    162.248.19.152  TLSv1…    262 Client Hello
253…  2019-04-23 17:18:13.009910 162.248.19.147  192.168.1.16    TLSv1…     60 Change Cipher Spec
253…  2019-04-23 17:18:13.011217 162.248.19.147  192.168.1.16    TLSv1…     99 Encrypted Handshake Message
253…  2019-04-23 17:18:13.012038 192.168.1.16    162.248.19.152  TLSv1…    262 Client Hello
253…  2019-04-23 17:18:13.013285 162.248.19.147  192.168.1.16    TLSv1…    976 [TCP Spurious Retransmission] , Application Data
253…  2019-04-23 17:18:13.013730 162.248.19.147  192.168.1.16    TLSv1…   1146 [TCP Spurious Retransmission] , Application Data
```

```
> Frame 25323: 263 bytes on wire (2104 bits), 263 bytes captured (2104 bits) on interface 0
> Ethernet II, Src: IntelCor_10:10:99 (14:ab:c5:10:10:99), Dst: Actionte_97:02:83 (00:1f:90:97:02:83)
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 162.248.19.152
> Transmission Control Protocol, Src Port: 52186, Dst Port: 443, Seq: 1, Ack: 1, Len: 209
v Secure Sockets Layer
  v TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 204
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 200
        Version: TLS 1.2 (0x0303)
      > Random: 5cbf8114ac01e93e671be35d71f8edce3e1838834ee0c281...
```

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?

Handshake (22)

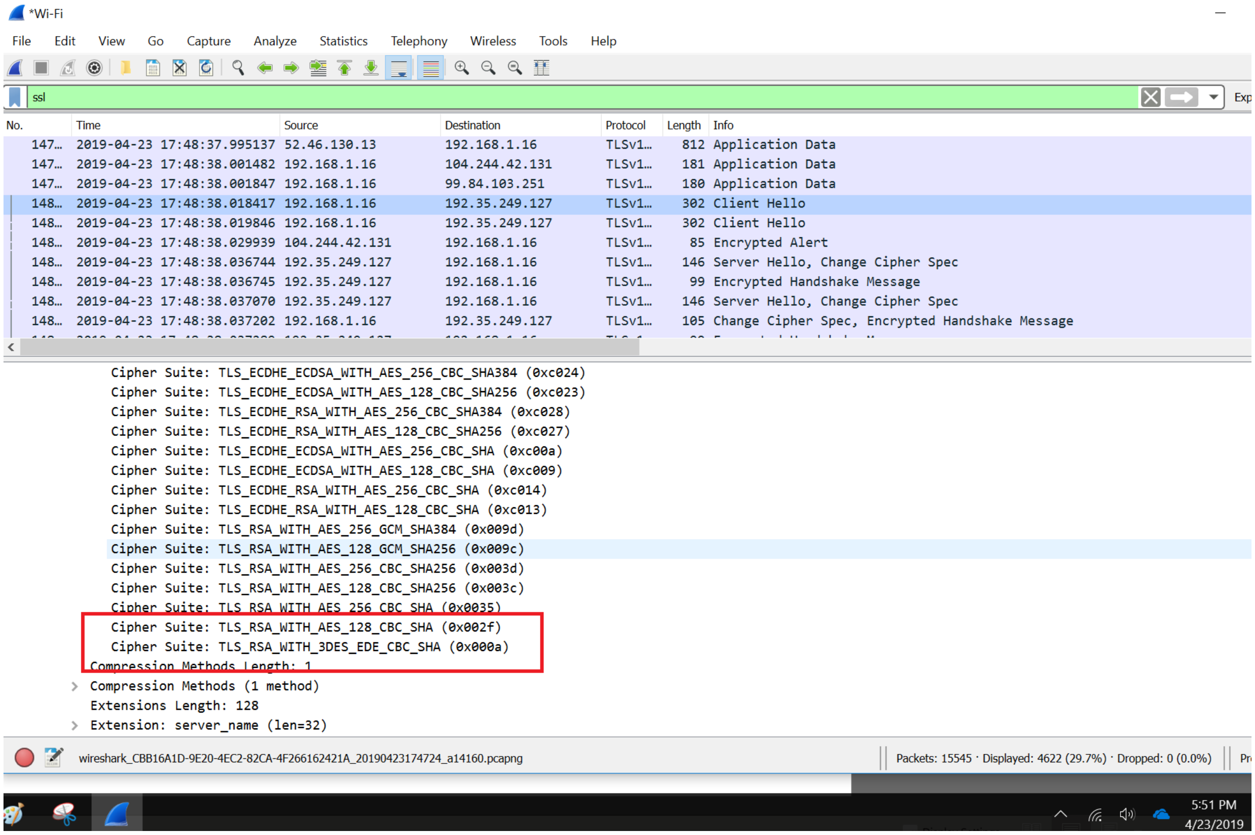

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssl
5:28 PM
4/23/2019

```
No.   Time                        Source          Destination     Protocol  Length Info
252…  2019-04-23 17:18:12.410978  209.15.36.32    192.168.1.16    TLSv1…    368 New Session Ticket, Change Cipher Spec, Encrypted
252…  2019-04-23 17:18:12.414036  209.15.36.32    192.168.1.16    TLSv1…    763 Application Data
253…  2019-04-23 17:18:12.580319  162.248.19.147  192.168.1.16    TLSv1…   1514 Server Hello
253…  2019-04-23 17:18:12.581261  162.248.19.147  192.168.1.16    TLSv1…    547 Certificate, Server Key Exchange, Server Hello Do
253…  2019-04-23 17:18:12.584292  192.168.1.16    162.248.19.147  TLSv1…    180 Client Key Exchange, Change Cipher Spec, Encrypte
253…  2019-04-23 17:18:12.584598  192.168.1.16    162.248.19.147  TLSv1…   1061 Application Data
253…  2019-04-23 17:18:12.657476  192.168.1.16    162.248.19.152  TLSv1…    263 Client Hello
253…  2019-04-23 17:18:12.657551  192.168.1.16    162.248.19.152  TLSv1…    263 Client Hello
253…  2019-04-23 17:18:12.740180  162.248.19.147  192.168.1.16    TLSv1…     60 Change Cipher Spec
253…  2019-04-23 17:18:12.740575  162.248.19.147  192.168.1.16    TLSv1…     99 Encrypted Handshake Message
253…  2019-04-23 17:18:12.741625  162.248.19.147  192.168.1.16    TLSv1…     60 Change Cipher Spec
253…  2019-04-23 17:18:12.742324  162.248.19.147  192.168.1.16    TLSv1…     99 Encrypted Handshake Message
253…  2019-04-23 17:18:12.742709  162.248.19.147  192.168.1.16    TLSv1…     60 Change Cipher Spec
253…  2019-04-23 17:18:12.743238  162.248.19.147  192.168.1.16    TLSv1…     99 Encrypted Handshake Message
253…  2019-04-23 17:18:12.743677  162.248.19.147  192.168.1.16    TLSv1…    976 Application Data
253…  2019-04-23 17:18:12.743956  192.168.1.16    162.248.19.147  TLSv1…   1137 Application Data
253…  2019-04-23 17:18:12.744674  162.248.19.147  192.168.1.16    TLSv1…   1146 Application Data
253…  2019-04-23 17:18:12.745611  162.248.19.147  192.168.1.16    TLSv1…    904 Application Data
253…  2019-04-23 17:18:12.746938  162.248.19.147  192.168.1.16    TLSv1…    168 Application Data
253…  2019-04-23 17:18:12.747438  192.168.1.16    162.248.19.147  TLSv1…    295 Client Hello
253…  2019-04-23 17:18:13.009688  192.168.1.16    162.248.19.152  TLSv1…    262 Client Hello
253…  2019-04-23 17:18:13.009910  162.248.19.147  192.168.1.16    TLSv1…     60 Change Cipher Spec
253…  2019-04-23 17:18:13.011217  162.248.19.147  192.168.1.16    TLSv1…     99 Encrypted Handshake Message
253…  2019-04-23 17:18:13.012038  192.168.1.16    162.248.19.152  TLSv1…    262 Client Hello
253…  2019-04-23 17:18:13.013285  162.248.19.147  192.168.1.16    TLSv1…    976 [TCP Spurious Retransmission] , Application Data
253…  2019-04-23 17:18:13.013730  162.248.19.147  192.168.1.16    TLSv1…   1146 [TCP Spurious Retransmission] , Application Data
```

```
> Frame 25323: 263 bytes on wire (2104 bits), 263 bytes captured (2104 bits) on interface 0
> Ethernet II, Src: IntelCor_10:10:99 (14:ab:c5:10:10:99), Dst: Actionte_97:02:83 (00:1f:90:97:02:83)
> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 162.248.19.152
> Transmission Control Protocol, Src Port: 52186, Dst Port: 443, Seq: 1, Ack: 1, Len: 209
v Secure Sockets Layer
    v TLSv1.2 Record Layer: Handshake Protocol: Client Hello
        Content Type: Handshake (22)
        Version: TLS 1.2 (0x0303)
        Length: 204
      v Handshake Protocol: Client Hello
          Handshake Type: Client Hello (1)
          Length: 200
          Version: TLS 1.2 (0x0303)
        > Random: 5cbf8114ac01e93e671be35d71f8edce3e1838834ee0c281...
```

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?

No nonce or “challenge” found


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Exp

```
ssl
```

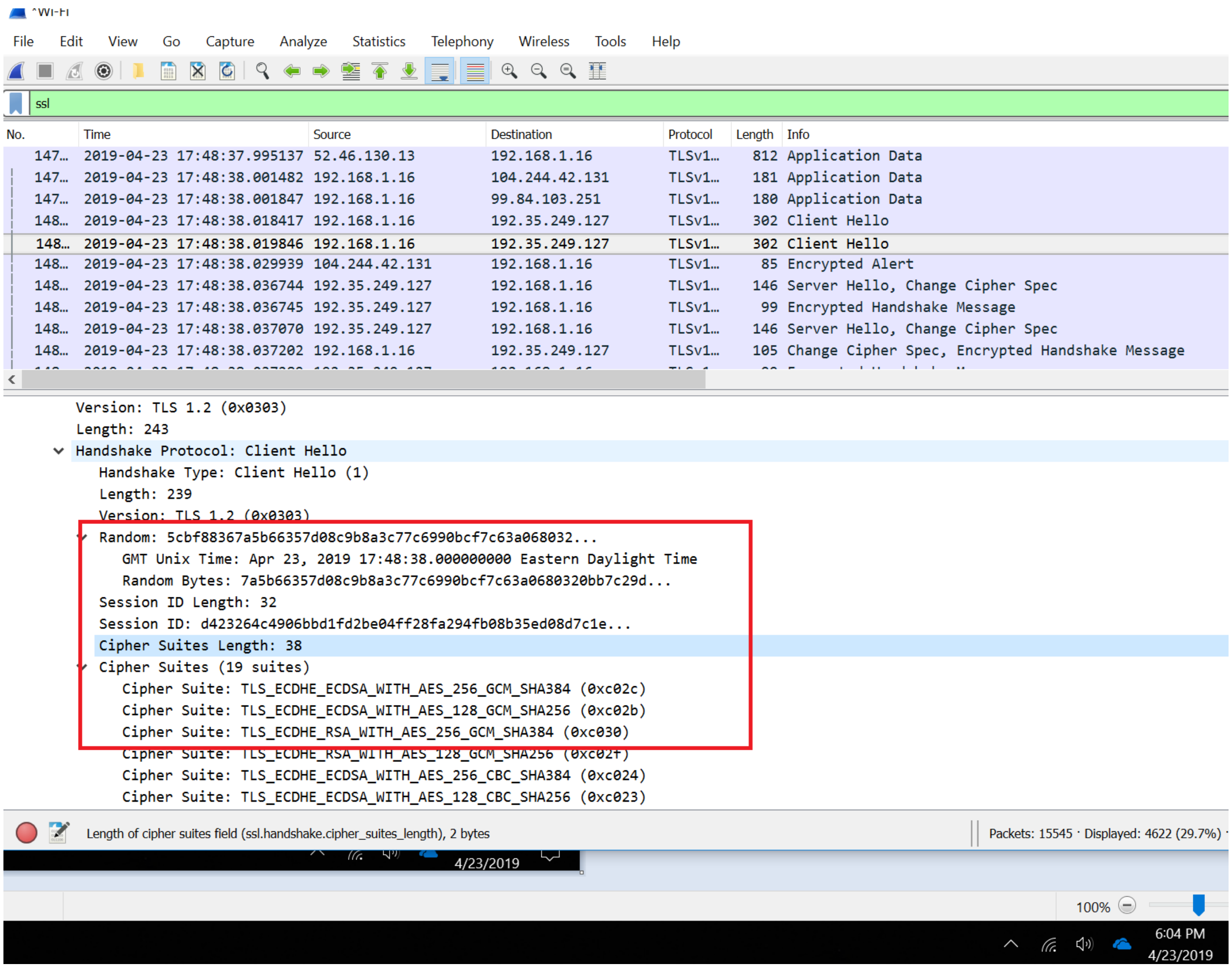
```
No.   Time                       Source          Destination     Protocol  Length Info
147…  2019-04-23 17:48:37.995137 52.46.130.13    192.168.1.16    TLSv1…    812 Application Data
147…  2019-04-23 17:48:38.001482 192.168.1.16    104.244.42.131  TLSv1…    181 Application Data
147…  2019-04-23 17:48:38.001847 192.168.1.16    99.84.103.251   TLSv1…    180 Application Data
148…  2019-04-23 17:48:38.018417 192.168.1.16    192.35.249.127  TLSv1…    302 Client Hello
148…  2019-04-23 17:48:38.019846 192.168.1.16    192.35.249.127  TLSv1…    302 Client Hello
148…  2019-04-23 17:48:38.029939 104.244.42.131  192.168.1.16    TLSv1…     85 Encrypted Alert
148…  2019-04-23 17:48:38.036744 192.35.249.127  192.168.1.16    TLSv1…    146 Server Hello, Change Cipher Spec
148…  2019-04-23 17:48:38.036745 192.35.249.127  192.168.1.16    TLSv1…     99 Encrypted Handshake Message
148…  2019-04-23 17:48:38.037070 192.35.249.127  192.168.1.16    TLSv1…    146 Server Hello, Change Cipher Spec
148…  2019-04-23 17:48:38.037202 192.168.1.16    192.35.249.127  TLSv1…    105 Change Cipher Spec, Encrypted Handshake Message
```

```
            Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
            Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
            Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
            Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
            Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
            Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
            Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
            Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
            Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
            Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
            Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
            Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
            Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
            Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
            Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
         Compression Methods Length: 1
       > Compression Methods (1 method)
         Extensions Length: 128
       > Extension: server_name (len=32)
```

```
wireshark_CBB16A1D-9E20-4EC2-82CA-4F266162421A_20190423174724_a14160.pcapng    Packets: 15545 · Displayed: 4622 (29.7%) · Dropped: 0 (0.0%)    Pr
```

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?

ClientHello record does not advertise the cyber suites it supports.



```
No.   Time                        Source          Destination     Protocol  Length  Info
147…  2019-04-23 17:48:37.995137  52.46.130.13    192.168.1.16    TLSv1…     812    Application Data
147…  2019-04-23 17:48:38.001482  192.168.1.16    104.244.42.131  TLSv1…     181    Application Data
147…  2019-04-23 17:48:38.001847  192.168.1.16    99.84.103.251   TLSv1…     180    Application Data
148…  2019-04-23 17:48:38.018417  192.168.1.16    192.35.249.127  TLSv1…     302    Client Hello
148…  2019-04-23 17:48:38.019846  192.168.1.16    192.35.249.127  TLSv1…     302    Client Hello
148…  2019-04-23 17:48:38.029939  104.244.42.131  192.168.1.16    TLSv1…      85    Encrypted Alert
148…  2019-04-23 17:48:38.036744  192.35.249.127  192.168.1.16    TLSv1…     146    Server Hello, Change Cipher Spec
148…  2019-04-23 17:48:38.036745  192.35.249.127  192.168.1.16    TLSv1…      99    Encrypted Handshake Message
148…  2019-04-23 17:48:38.037070  192.35.249.127  192.168.1.16    TLSv1…     146    Server Hello, Change Cipher Spec
148…  2019-04-23 17:48:38.037202  192.168.1.16    192.35.249.127  TLSv1…     105    Change Cipher Spec, Encrypted Handshake Message
```

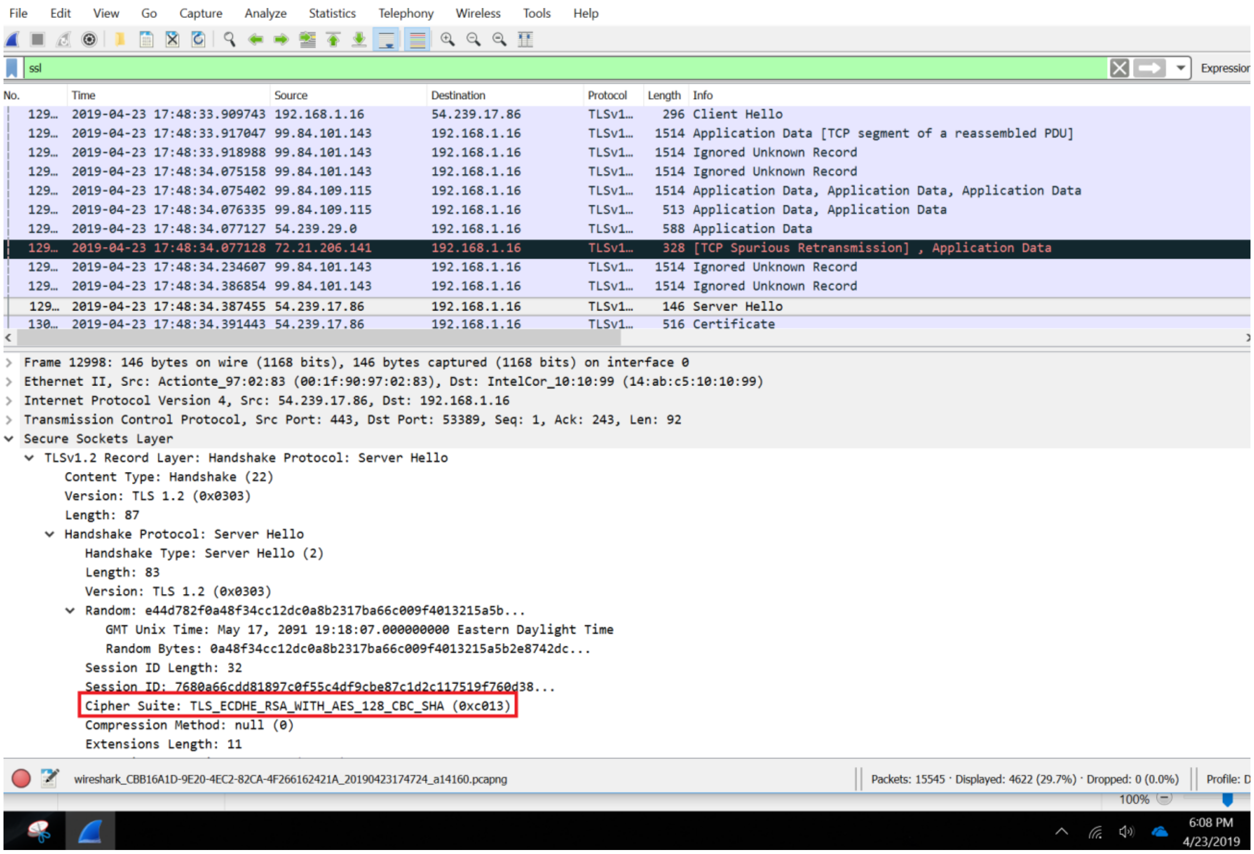
```
      Version: TLS 1.2 (0x0303)
      Length: 243
    ⌄ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 239
        Version: TLS 1.2 (0x0303)
      ⌄ Random: 5cbf88367a5b66357d08c9b8a3c77c6990bcf7c63a068032...
          GMT Unix Time: Apr 23, 2019 17:48:38.000000000 Eastern Daylight Time
          Random Bytes: 7a5b66357d08c9b8a3c77c6990bcf7c63a0680320bb7c29d...
        Session ID Length: 32
        Session ID: d423264c4906bbd1fd2be04ff28fa294fb08b35ed08d7c1e...
        Cipher Suites Length: 38
      ⌄ Cipher Suites (19 suites)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
          Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
          Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
```

Length of cipher suites field (ssl.handshake.cipher_suites_length), 2 bytes

Packets: 15545 · Displayed: 4622 (29.7%)

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

TLS, RSA and AES and SHA



ssl

```
No.    Time                        Source          Destination     Protocol  Length  Info
  129… 2019-04-23 17:48:33.909743 192.168.1.16    54.239.17.86    TLSv1…     296 Client Hello
  129… 2019-04-23 17:48:33.917047 99.84.101.143   192.168.1.16    TLSv1…    1514 Application Data [TCP segment of a reassembled PDU]
  129… 2019-04-23 17:48:33.918988 99.84.101.143   192.168.1.16    TLSv1…    1514 Ignored Unknown Record
  129… 2019-04-23 17:48:34.075158 99.84.101.143   192.168.1.16    TLSv1…    1514 Ignored Unknown Record
  129… 2019-04-23 17:48:34.075402 99.84.109.115   192.168.1.16    TLSv1…    1514 Application Data, Application Data, Application Data
  129… 2019-04-23 17:48:34.076335 99.84.109.115   192.168.1.16    TLSv1…     513 Application Data, Application Data
  129… 2019-04-23 17:48:34.077127 54.239.29.0     192.168.1.16    TLSv1…     588 Application Data
  129… 2019-04-23 17:48:34.077128 72.21.206.141   192.168.1.16    TLSv1…     328 [TCP Spurious Retransmission] , Application Data
  129… 2019-04-23 17:48:34.234607 99.84.101.143   192.168.1.16    TLSv1…    1514 Ignored Unknown Record
  129… 2019-04-23 17:48:34.386854 99.84.101.143   192.168.1.16    TLSv1…    1514 Ignored Unknown Record
  129… 2019-04-23 17:48:34.387455 54.239.17.86    192.168.1.16    TLSv1…     146 Server Hello
  130… 2019-04-23 17:48:34.391443 54.239.17.86    192.168.1.16    TLSv1…     516 Certificate
```

```
> Frame 12998: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface 0
> Ethernet II, Src: Actionte_97:02:83 (00:1f:90:97:02:83), Dst: IntelCor_10:10:99 (14:ab:c5:10:10:99)
> Internet Protocol Version 4, Src: 54.239.17.86, Dst: 192.168.1.16
> Transmission Control Protocol, Src Port: 443, Dst Port: 53389, Seq: 1, Ack: 243, Len: 92
v Secure Sockets Layer
  v TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 87
    v Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 83
        Version: TLS 1.2 (0x0303)
      v Random: e44d782f0a48f34cc12dc0a8b2317ba66c009f4013215a5b...
          GMT Unix Time: May 17, 2091 19:18:07.000000000 Eastern Daylight Time
          Random Bytes: 0a48f34cc12dc0a8b2317ba66c009f4013215a5b2e8742dc...
        Session ID Length: 32
        Session ID: 7680a66cdd81897c0f55c4df9cbe87c1d2c117519f760d38...
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
        Compression Method: null (0)
        Extensions Length: 11
```

wireshark_CBB16A1D-9E20-4EC2-82CA-4F266162421A_20190423174724_a14160.pcapng

Packets: 15545 · Displayed: 4622 (29.7%) · Dropped: 0 (0.0%)

Profile: D

```
No.     Time                          Source                Destination           Protocol Length Info
  12998 2019-04-23 17:48:34.387455    54.239.17.86          192.168.1.16          TLSv1.2   146    Server Hello
Frame 12998: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface 0
Ethernet II, Src: Actionte_97:02:83 (00:1f:90:97:02:83), Dst: IntelCor_10:10:99 (14:ab:c5:10:10:99)
Internet Protocol Version 4, Src: 54.239.17.86, Dst: 192.168.1.16
Transmission Control Protocol, Src Port: 443, Dst Port: 53389, Seq: 1, Ack: 243, Len: 92
Secure Sockets Layer
    TLSv1.2 Record Layer: Handshake Protocol: Server Hello
        Content Type: Handshake (22)
        Version: TLS 1.2 (0x0303)
        Length: 87
        Handshake Protocol: Server Hello
            Handshake Type: Server Hello (2)
            Length: 83
            Version: TLS 1.2 (0x0303)
            Random: e44d782f0a48f34cc12dc0a8b2317ba66c009f4013215a5b...
                GMT Unix Time: May 17, 2091 19:18:07.000000000 Eastern Daylight Time
                Random Bytes: 0a48f34cc12dc0a8b2317ba66c009f4013215a5b2e8742dc...
            Session ID Length: 32
            Session ID: 7680a66cdd81897c0f55c4df9cbe87c1d2c117519f760d38...
            Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
            Compression Method: null (0)
            Extensions Length: 11
            Extension: ec_point_formats (len=2)
            Extension: renegotiation_info (len=1)
```