Ariel Salazar

IT 520 – Lab7

April 15th, 2019

Instructions:

Capture your packets in an SSL session. To do this, you should go to your favorite e-commerce site and begin the process of purchasing an item (but terminating before making the actual purpose!). After capturing the packets with Wireshark, you should set the filter so that it displays only the Ethernet frames that contain SSL records sent from and received by your host. (An SSL record is the same thing as an SSL message.)

Your Wireshark GUI should be displaying only the Ethernet frames that have SSL records. It is important to keep in mind that an Ethernet frame may contain one or more SSL records. (This is very different from HTTP, for which each frame contains either one complete HTTP message or a portion of a HTTP message.) Also, an SSL record may not completely fit into an Ethernet frame, in which case multiple frames will be needed to carry the record. Locate the "Client Hello" and "Server Hello" frame and use the frames to answer the questions.

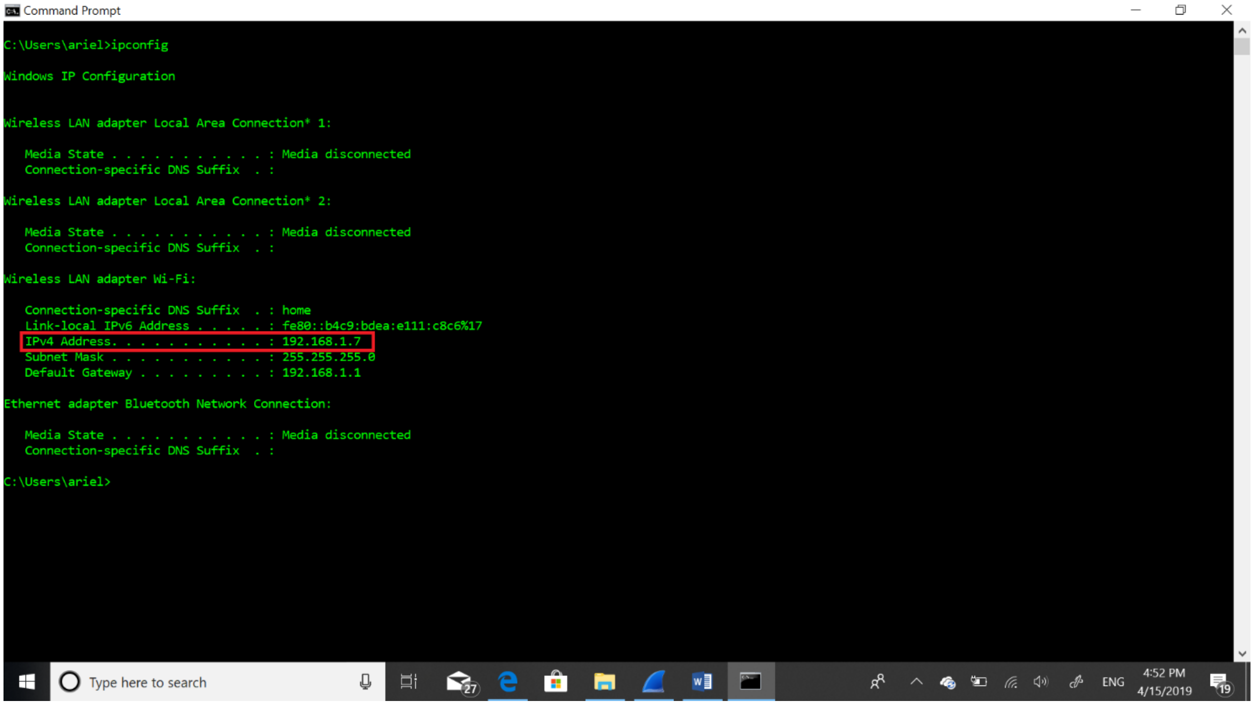
- (For each of these questions, take a screenshot of Wireshark, and attach it to your answer) - Questions without Full Screenshot will not be graded. A lab submission template is available on canvas. Your screenshot should indicate the time and date on your computer.

- Include a terminal screenshot showing computer IP address on the front page before Question 1, and a full PRINT of the HTTP OK message as the last page.

Lab will NOT be graded if either of these two is missing.

Questions:

Computer IP address: 192.168.1.7

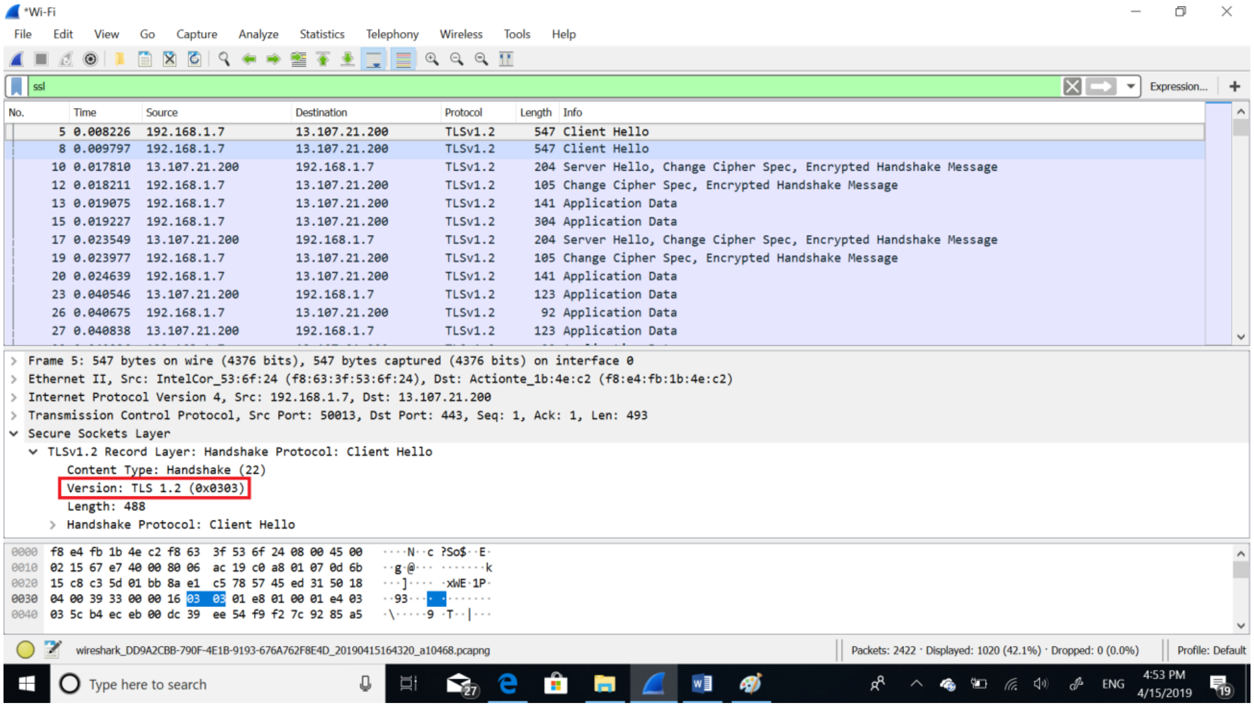


```
C:\Users\ariel>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : home
   Link-local IPv6 Address . . . . . : fe80::b4c9:bdea:e111:c8c6%17
   IPv4 Address. . . . . . . . . . . : 192.168.1.7
   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\ariel>
```

Client Hello Record:

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

Version: TLS 1.2 (0x0303)



ssl

```
No.  Time      Source        Destination   Protocol Length Info
   5 0.008226  192.168.1.7   13.107.21.200 TLSv1.2   547 Client Hello
   8 0.009797  192.168.1.7   13.107.21.200 TLSv1.2   547 Client Hello
  10 0.017810  13.107.21.200 192.168.1.7   TLSv1.2   204 Server Hello, Change Cipher Spec, Encrypted Handshake Message
  12 0.018211  192.168.1.7   13.107.21.200 TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
  13 0.019075  192.168.1.7   13.107.21.200 TLSv1.2   141 Application Data
  15 0.019227  192.168.1.7   13.107.21.200 TLSv1.2   304 Application Data
  17 0.023549  13.107.21.200 192.168.1.7   TLSv1.2   204 Server Hello, Change Cipher Spec, Encrypted Handshake Message
  19 0.023977  192.168.1.7   13.107.21.200 TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
  20 0.024639  192.168.1.7   13.107.21.200 TLSv1.2   141 Application Data
  23 0.040546  13.107.21.200 192.168.1.7   TLSv1.2   123 Application Data
  26 0.040675  192.168.1.7   13.107.21.200 TLSv1.2    92 Application Data
  27 0.040838  13.107.21.200 192.168.1.7   TLSv1.2   123 Application Data
```

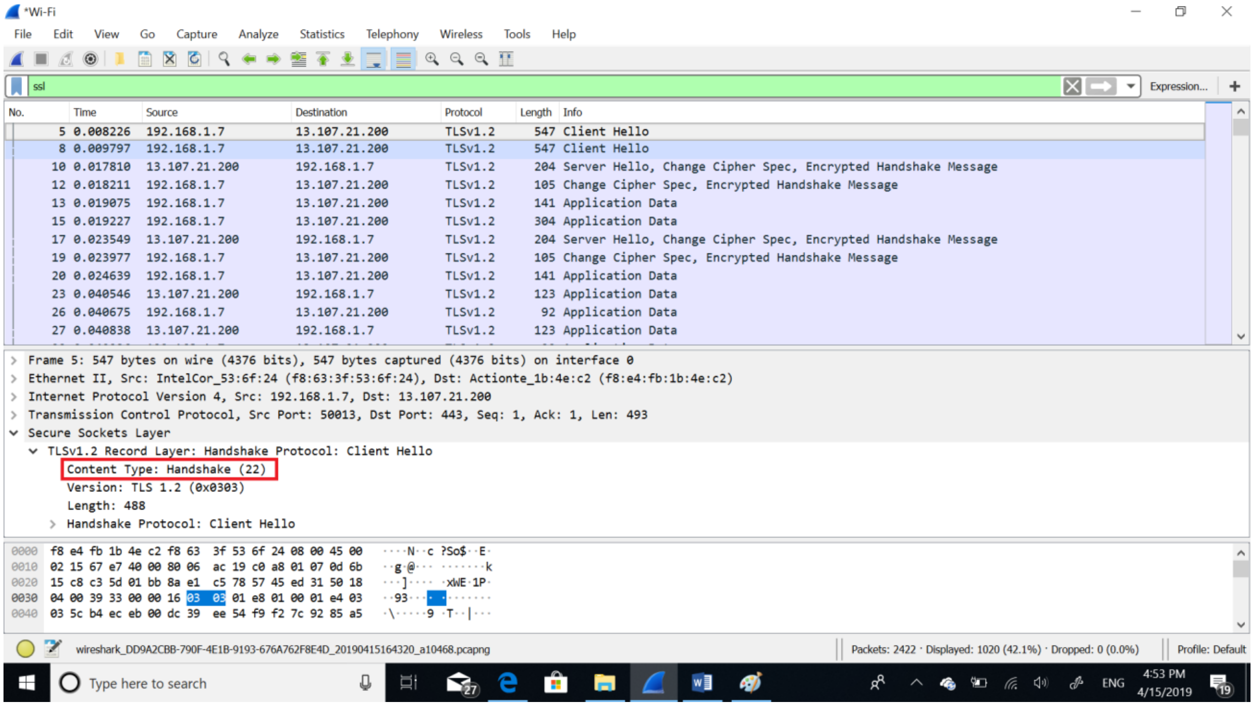
```
> Frame 5: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface 0
> Ethernet II, Src: IntelCor_53:6f:24 (f8:63:3f:53:6f:24), Dst: Actionte_1b:4e:c2 (f8:e4:fb:1b:4e:c2)
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 13.107.21.200
> Transmission Control Protocol, Src Port: 50013, Dst Port: 443, Seq: 1, Ack: 1, Len: 493
v Secure Sockets Layer
  v TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 488
    > Handshake Protocol: Client Hello
```

```
0000  f8 e4 fb 1b 4e c2 f8 63  3f 53 6f 24 08 00 45 00   ····N··c ?So$··E·
0010  02 15 67 e7 40 00 80 06  ac 19 c0 a8 01 07 0d 6b   ··g·@··· ·······k
0020  15 c8 c3 5d 01 bb 8a e1  c5 78 57 45 ed 31 50 18   ···]···· ·xWE·1P·
0030  04 00 39 33 00 00 16 03  03 01 e8 01 00 01 e4 03   ··93···· ········
0040  03 5c b4 ec eb 00 dc 39  ee 54 f9 f2 7c 92 85 a5   ·\·····9 ·T··|···
```

wireshark_DD9A2CBB-790F-4E1B-9193-676A762F8E4D_20190415164320_a10468.pcapng | Packets: 2422 · Displayed: 1020 (42.1%) · 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?

Content Type: Handshake (22)



```
No.   Time      Source          Destination     Protocol  Length Info
    5 0.008226  192.168.1.7     13.107.21.200   TLSv1.2   547 Client Hello
    8 0.009797  192.168.1.7     13.107.21.200   TLSv1.2   547 Client Hello
   10 0.017810  13.107.21.200   192.168.1.7     TLSv1.2   204 Server Hello, Change Cipher Spec, Encrypted Handshake Message
   12 0.018211  192.168.1.7     13.107.21.200   TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
   13 0.019075  192.168.1.7     13.107.21.200   TLSv1.2   141 Application Data
   15 0.019227  192.168.1.7     13.107.21.200   TLSv1.2   304 Application Data
   17 0.023549  13.107.21.200   192.168.1.7     TLSv1.2   204 Server Hello, Change Cipher Spec, Encrypted Handshake Message
   19 0.023977  192.168.1.7     13.107.21.200   TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
   20 0.024639  192.168.1.7     13.107.21.200   TLSv1.2   141 Application Data
   23 0.040546  13.107.21.200   192.168.1.7     TLSv1.2   123 Application Data
   26 0.040675  192.168.1.7     13.107.21.200   TLSv1.2    92 Application Data
   27 0.040838  13.107.21.200   192.168.1.7     TLSv1.2   123 Application Data
```

```
> Frame 5: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface 0
> Ethernet II, Src: IntelCor_53:6f:24 (f8:63:3f:53:6f:24), Dst: Actionte_1b:4e:c2 (f8:e4:fb:1b:4e:c2)
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 13.107.21.200
> Transmission Control Protocol, Src Port: 50013, Dst Port: 443, Seq: 1, Ack: 1, Len: 493
v Secure Sockets Layer
  v TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 488
    > Handshake Protocol: Client Hello
```

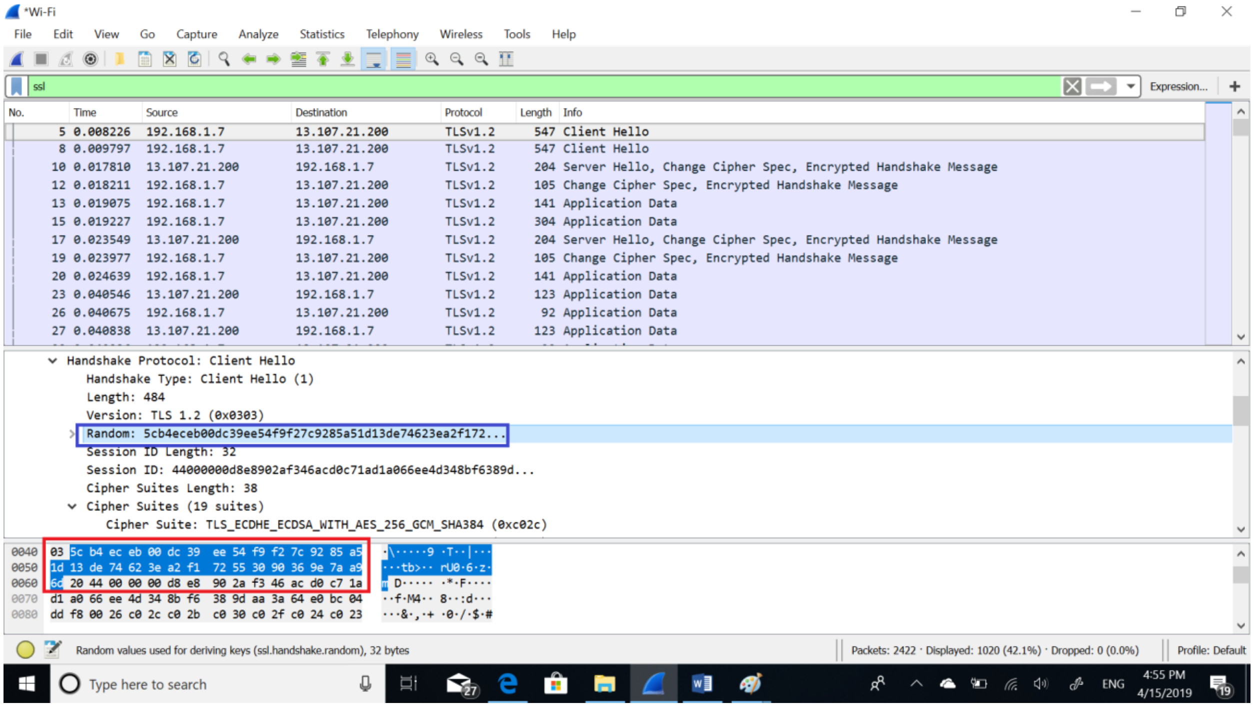
```
0000  f8 e4 fb 1b 4e c2 f8 63  3f 53 6f 24 08 00 45 00   ····N··c ?So$··E·
0010  02 15 67 e7 40 00 80 06  ac 19 c0 a8 01 07 0d 6b   ··g·@··· ·······k
0020  15 c8 c3 5d 01 bb 8a e1  c5 78 57 45 ed 31 50 18   ···]···· ·xWE·1P·
0030  04 00 39 33 00 00 16 03  03 01 e8 01 00 01 e4 03   ··93···· ········
0040  03 5c b4 ec eb 00 dc 39  ee 54 f9 f2 7c 92 85 a5   ·\·····9 ·T··|···
```

wireshark_DD9A2CBB-790F-4E1B-9193-676A762F8E4D_20190415164320_a10468.pcapng | Packets: 2422 · Displayed: 1020 (42.1%) · 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?

This ClientHello record doesn't contain a nonce or "challenge" variable with that name. However, there is a value called "random" value that has the same function that "challenge". The value is:

5c b4 ec eb 00 dc 39 ee 54 f9 f2 7c 92 85 a5 1d 13 de 74 62 3e a2 f1 72 55 30 90 36 9e 7a a9 6d



ssl

```
No.  Time      Source         Destination    Protocol  Length Info
   5 0.008226  192.168.1.7    13.107.21.200  TLSv1.2   547 Client Hello
   8 0.009797  192.168.1.7    13.107.21.200  TLSv1.2   547 Client Hello
  10 0.017810  13.107.21.200  192.168.1.7    TLSv1.2   204 Server Hello, Change Cipher Spec, Encrypted Handshake Message
  12 0.018211  192.168.1.7    13.107.21.200  TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
  13 0.019075  192.168.1.7    13.107.21.200  TLSv1.2   141 Application Data
  15 0.019227  192.168.1.7    13.107.21.200  TLSv1.2   304 Application Data
  17 0.023549  13.107.21.200  192.168.1.7    TLSv1.2   204 Server Hello, Change Cipher Spec, Encrypted Handshake Message
  19 0.023977  192.168.1.7    13.107.21.200  TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
  20 0.024639  192.168.1.7    13.107.21.200  TLSv1.2   141 Application Data
  23 0.040546  13.107.21.200  192.168.1.7    TLSv1.2   123 Application Data
  26 0.040675  192.168.1.7    13.107.21.200  TLSv1.2    92 Application Data
  27 0.040838  13.107.21.200  192.168.1.7    TLSv1.2   123 Application Data
```

```
  ˅ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 484
      Version: TLS 1.2 (0x0303)
    > Random: 5cb4eceb00dc39ee54f9f27c9285a51d13de74623ea2f172...
      Session ID Length: 32
      Session ID: 44000000d8e8902af346acd0c71ad1a066ee4d348bf6389d...
      Cipher Suites Length: 38
    ˅ Cipher Suites (19 suites)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
```

```
0040  03 5c b4 ec eb 00 dc 39  ee 54 f9 f2 7c 92 85 a5   ·\·····9 ·T··|···
0050  1d 13 de 74 62 3e a2 f1  72 55 30 90 36 9e 7a a9   ···tb>·· rU0·6·z·
0060  6d 20 44 00 00 00 d8 e8  90 2a f3 46 ac d0 c7 1a   m D····· ·*·F····
0070  d1 a0 66 ee 4d 34 8b f6  38 9d aa 3a 64 e0 bc 04   ··f·M4·· 8··:d···
0080  dd f8 00 26 c0 2c c0 2b  c0 30 c0 2f c0 24 c0 23   ···&·,·+ ·0·/·$·#
```

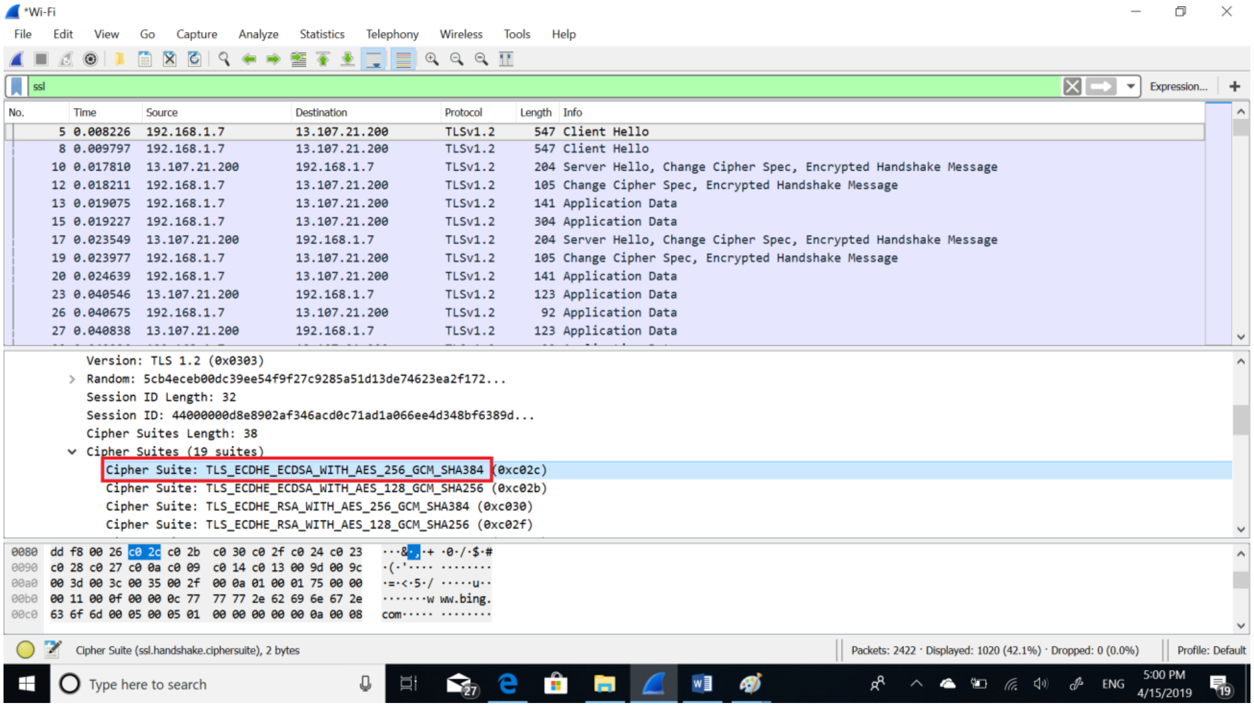
Random values used for deriving keys (ssl.handshake.random), 32 bytes

Packets: 2422 · Displayed: 1020 (42.1%) · 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, the ClientHello record advertise the cyber suites it supports. The first listed suite uses ECDHE and ECDSA as public-key algorithm, AES as symmetric-key algorithm and GCM as hash algorithm.



ssl

```
No.  Time      Source         Destination    Protocol  Length Info
   5 0.008226  192.168.1.7    13.107.21.200  TLSv1.2   547 Client Hello
   8 0.009797  192.168.1.7    13.107.21.200  TLSv1.2   547 Client Hello
  10 0.017810  13.107.21.200  192.168.1.7    TLSv1.2   204 Server Hello, Change Cipher Spec, Encrypted Handshake Message
  12 0.018211  192.168.1.7    13.107.21.200  TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
  13 0.019075  192.168.1.7    13.107.21.200  TLSv1.2   141 Application Data
  15 0.019227  192.168.1.7    13.107.21.200  TLSv1.2   304 Application Data
  17 0.023549  13.107.21.200  192.168.1.7    TLSv1.2   204 Server Hello, Change Cipher Spec, Encrypted Handshake Message
  19 0.023977  192.168.1.7    13.107.21.200  TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
  20 0.024639  192.168.1.7    13.107.21.200  TLSv1.2   141 Application Data
  23 0.040546  13.107.21.200  192.168.1.7    TLSv1.2   123 Application Data
  26 0.040675  192.168.1.7    13.107.21.200  TLSv1.2    92 Application Data
  27 0.040838  13.107.21.200  192.168.1.7    TLSv1.2   123 Application Data
```

```
      Version: TLS 1.2 (0x0303)
    > Random: 5cb4eceb00dc39ee54f9f27c9285a51d13de74623ea2f172...
      Session ID Length: 32
      Session ID: 44000000d8e8902af346acd0c71ad1a066ee4d348bf6389d...
      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)
```

```
0080  dd f8 00 26 c0 2c c0 2b  c0 30 c0 2f c0 24 c0 23   ···&·,·+ ·0·/·$·#
0090  c0 28 c0 27 c0 0a c0 09  c0 14 c0 13 00 9d 00 9c   ·(·'···· ········
00a0  00 3d 00 3c 00 35 00 2f  00 0a 01 00 01 75 00 00   ·=·<·5·/ ·····u··
00b0  00 11 00 0f 00 00 0c 77  77 77 2e 62 69 6e 67 2e   ·······w ww.bing.
00c0  63 6f 6d 00 05 00 05 01  00 00 00 00 00 0a 00 08   com····· ········
```

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

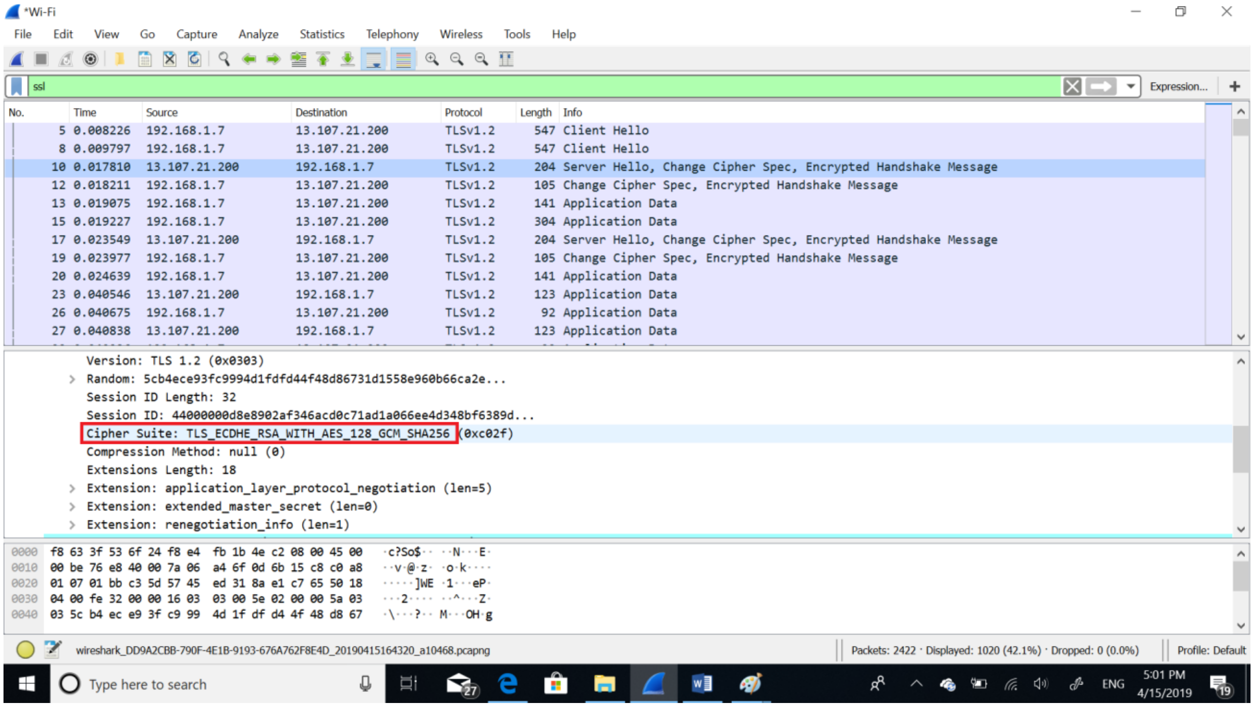
Packets: 2422 · Displayed: 1020 (42.1%) · Dropped: 0 (0.0%)

Profile: Default

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?

Yes, this record specifies a chosen cipher suite. It uses ECDHE and RSA as public key algorithm, AES as a symmetric-key algorithm and GCM as a hash algorithm.



```
No.   Time      Source          Destination     Protocol  Length Info
    5 0.008226  192.168.1.7     13.107.21.200   TLSv1.2    547 Client Hello
    8 0.009797  192.168.1.7     13.107.21.200   TLSv1.2    547 Client Hello
   10 0.017810  13.107.21.200   192.168.1.7     TLSv1.2    204 Server Hello, Change Cipher Spec, Encrypted Handshake Message
   12 0.018211  192.168.1.7     13.107.21.200   TLSv1.2    105 Change Cipher Spec, Encrypted Handshake Message
   13 0.019075  192.168.1.7     13.107.21.200   TLSv1.2    141 Application Data
   15 0.019227  192.168.1.7     13.107.21.200   TLSv1.2    304 Application Data
   17 0.023549  13.107.21.200   192.168.1.7     TLSv1.2    204 Server Hello, Change Cipher Spec, Encrypted Handshake Message
   19 0.023977  192.168.1.7     13.107.21.200   TLSv1.2    105 Change Cipher Spec, Encrypted Handshake Message
   20 0.024639  192.168.1.7     13.107.21.200   TLSv1.2    141 Application Data
   23 0.040546  13.107.21.200   192.168.1.7     TLSv1.2    123 Application Data
   26 0.040675  192.168.1.7     13.107.21.200   TLSv1.2     92 Application Data
   27 0.040838  13.107.21.200   192.168.1.7     TLSv1.2    123 Application Data
```

```
      Version: TLS 1.2 (0x0303)
    > Random: 5cb4ece93fc9994d1fdfd44f48d86731d1558e960b66ca2e...
      Session ID Length: 32
      Session ID: 44000000d8e8902af346acd0c71ad1a066ee4d348bf6389d...
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
      Compression Method: null (0)
      Extensions Length: 18
    > Extension: application_layer_protocol_negotiation (len=5)
    > Extension: extended_master_secret (len=0)
    > Extension: renegotiation_info (len=1)
```

```
0000  f8 63 3f 53 6f 24 f8 e4  fb 1b 4e c2 08 00 45 00   ·c?So$·· ··N···E·
0010  00 be 76 e8 40 00 7a 06  a4 6f 0d 6b 15 c8 c0 a8   ··v·@·z· ·o·k····
0020  01 07 01 bb c3 5d 57 45  ed 31 8a e1 c7 65 50 18   ·····]WE ·1···eP·
0030  04 00 fe 32 00 00 16 03  03 00 5e 02 00 00 5a 03   ···2···· ··^···Z·
0040  03 5c b4 ec e9 3f c9 99  4d 1f df d4 4f 48 d8 67   ·\···?·· M···OH·g
```

```
wireshark_DD9A2CBB-790F-4E1B-9193-676A762F8E4D_20190415164320_a10468.pcapng   Packets: 2422 · Displayed: 1020 (42.1%) · Dropped: 0 (0.0%)   Profile: Default
```