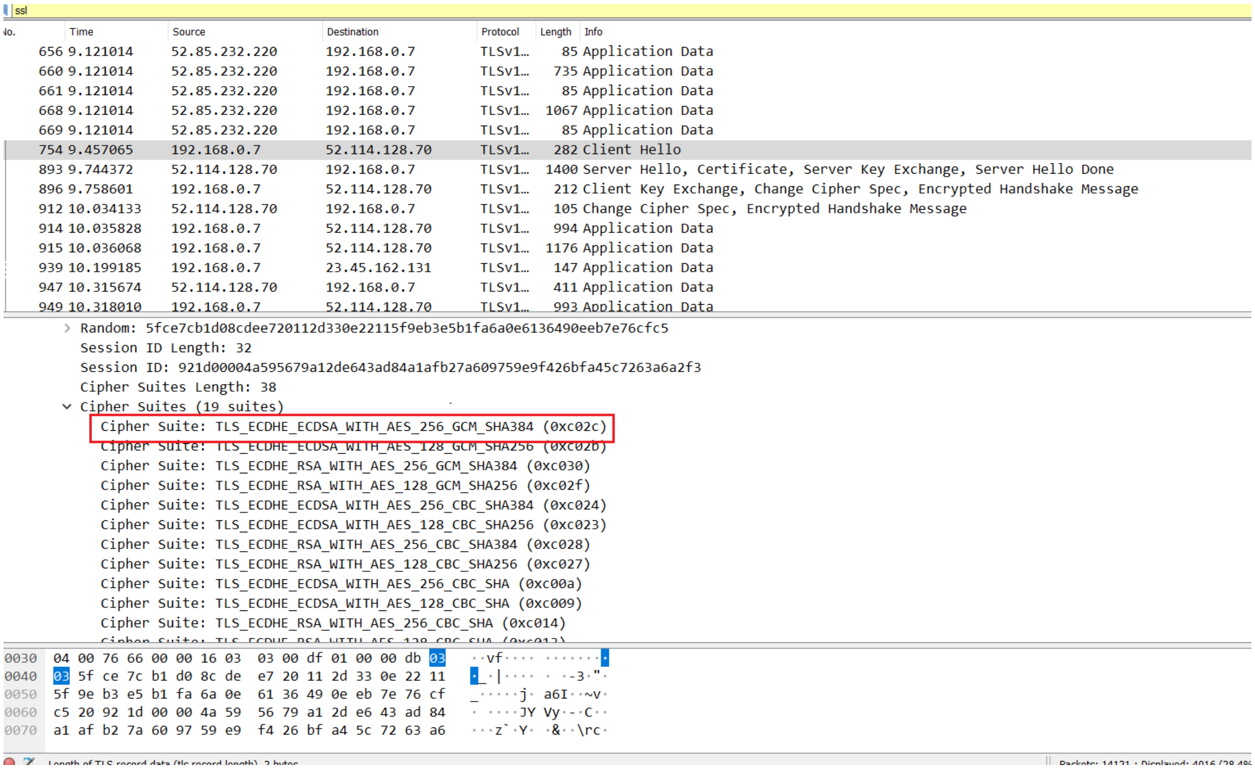
LAB-9

1.What are the cipher suites advertised by client hello record? How do you identify the client hello record?

Cipher suites: They are set cryptographic algorithms.



```
ssl
No.  Time       Source          Destination     Protocol  Length Info
 656 9.121014   52.85.232.220   192.168.0.7     TLSv1…      85 Application Data
 660 9.121014   52.85.232.220   192.168.0.7     TLSv1…     735 Application Data
 661 9.121014   52.85.232.220   192.168.0.7     TLSv1…      85 Application Data
 668 9.121014   52.85.232.220   192.168.0.7     TLSv1…    1067 Application Data
 669 9.121014   52.85.232.220   192.168.0.7     TLSv1…      85 Application Data
 754 9.457065   192.168.0.7     52.114.128.70   TLSv1…     282 Client Hello
 893 9.744372   52.114.128.70   192.168.0.7     TLSv1…    1400 Server Hello, Certificate, Server Key Exchange, Server Hello Done
 896 9.758601   192.168.0.7     52.114.128.70   TLSv1…     212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 912 10.034133  52.114.128.70   192.168.0.7     TLSv1…     105 Change Cipher Spec, Encrypted Handshake Message
 914 10.035828  192.168.0.7     52.114.128.70   TLSv1…     994 Application Data
 915 10.036068  192.168.0.7     52.114.128.70   TLSv1…    1176 Application Data
 939 10.199185  192.168.0.7     23.45.162.131   TLSv1…     147 Application Data
 947 10.315674  52.114.128.70   192.168.0.7     TLSv1…     411 Application Data
 949 10.318010  192.168.0.7     52.114.128.70   TLSv1…     993 Application Data
```

```
  > Random: 5fce7cb1d08cdee720112d330e22115f9eb3e5b1fa6a0e6136490eeb7e76cfc5
    Session ID Length: 32
    Session ID: 921d00004a595679a12de643ad84a1afb27a609759e9f426bfa45c7263a6a2f3
    Cipher Suites Length: 38
  v 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)
      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)
```

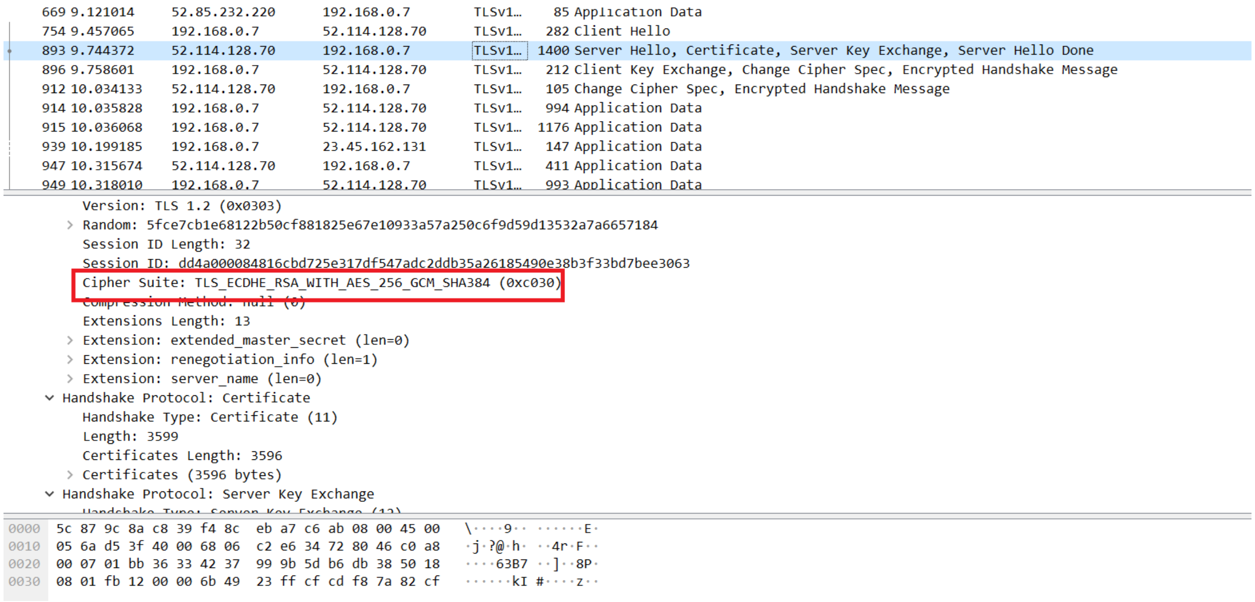
```
0030  04 00 76 66 00 00 16 03  03 00 df 01 00 00 db 03   ··vf····  ········
0040  03 5f ce 7c b1 d0 8c de  e7 20 11 2d 33 0e 22 11   ·_·|····  · ·-3·"·
0050  5f 9e b3 e5 b1 fa 6a 0e  61 36 49 0e eb 7e 76 cf   _·····j·  a6I··~v·
0060  c5 20 92 1d 00 00 4a 59  56 79 a1 2d e6 43 ad 84   · ····JY  Vy·-·C··
0070  a1 af b2 7a 60 97 59 e9  f4 26 bf a4 5c 72 63 a6   ···z`·Y·  ·&··\rc·
```

```
Length of TLS record data (tls.record.length), 2 bytes        Packets: 14121 · Displayed: 4016 (28.4%
```

The client has so many cipher suites. The first cipher suite is:

Public key algorithm: ECDHE_ECDSA
Symmetric-key algorithm: AES_256
MAC algorithm: GCM_SHA384

2. What cipher suite is picked by the server hello? How do you identify the server Hello record?



```
669 9.121014    52.85.232.220    192.168.0.7      TLSv1…    85 Application Data
754 9.457065    192.168.0.7      52.114.128.70    TLSv1…   282 Client Hello
893 9.744372    52.114.128.70    192.168.0.7      TLSv1…  1400 Server Hello, Certificate, Server Key Exchange, Server Hello Done
896 9.758601    192.168.0.7      52.114.128.70    TLSv1…   212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
912 10.034133   52.114.128.70    192.168.0.7      TLSv1…   105 Change Cipher Spec, Encrypted Handshake Message
914 10.035828   192.168.0.7      52.114.128.70    TLSv1…   994 Application Data
915 10.036068   192.168.0.7      52.114.128.70    TLSv1…  1176 Application Data
939 10.199185   192.168.0.7      23.45.162.131    TLSv1…   147 Application Data
947 10.315674   52.114.128.70    192.168.0.7      TLSv1…   411 Application Data
949 10.318010   192.168.0.7      52.114.128.70    TLSv1…   993 Application Data
```

```
        Version: TLS 1.2 (0x0303)
      > Random: 5fce7cb1e68122b50cf881825e67e10933a57a250c6f9d59d13532a7a6657184
        Session ID Length: 32
        Session ID: dd4a000084816cbd725e317df547adc2ddb35a26185490e38b3f33bd7bee3063
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
        Compression Method: null (0)
        Extensions Length: 13
      > Extension: extended_master_secret (len=0)
      > Extension: renegotiation_info (len=1)
      > Extension: server_name (len=0)
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 3599
        Certificates Length: 3596
      > Certificates (3596 bytes)
    v Handshake Protocol: Server Key Exchange
        Handshake Type: Server Key Exchange (12)
```

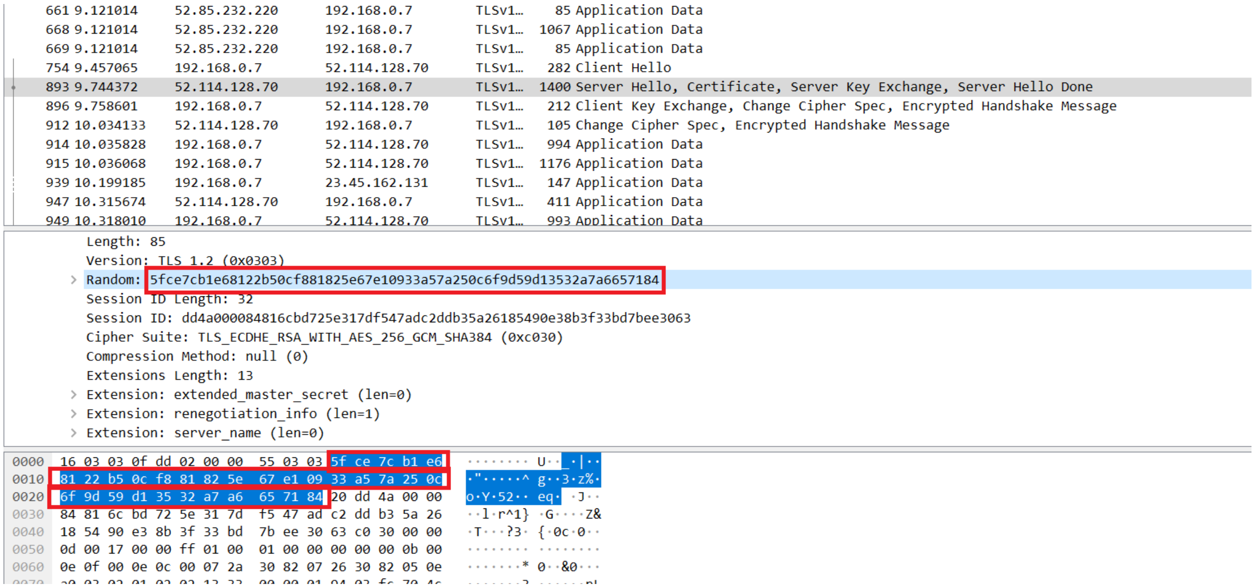
```
0000  5c 87 9c 8a c8 39 f4 8c  eb a7 c6 ab 08 00 45 00   \····9·· ······E·
0010  05 6a d5 3f 40 00 68 06  c2 e6 34 72 80 46 c0 a8   ·j·?@·h· ··4r·F··
0020  00 07 01 bb 36 33 42 37  99 9b 5d b6 db 38 50 18   ····63B7 ··]··8P·
0030  08 01 fb 12 00 00 6b 49  23 ff cf cd f8 7a 82 cf   ······kI #····z··
```

Server side picked one of the cipher suites from client.

Public key algorithm: ECDHE_RSA
Symmetric-key algorithm: AES_256
MAC algorithm: GCM_SHA384

3. Does the server hello contain a nonce? What is its value? Does it have a certificate? How many bytes long?

> A: Yes, the server hello contains a nonce. Its value is 32 bits. No, there is no certificate in this record. The certificate is in the separate record.

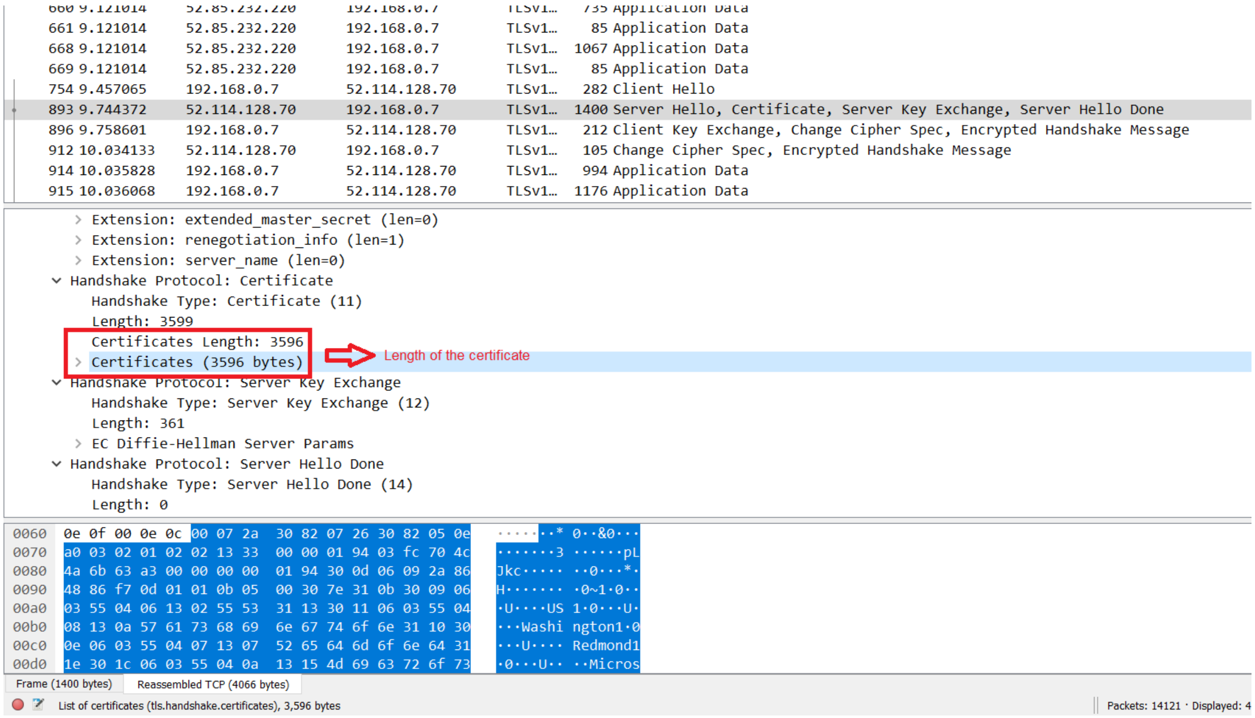


```
661 9.121014     52.85.232.220     192.168.0.7       TLSv1…    85 Application Data
668 9.121014     52.85.232.220     192.168.0.7       TLSv1…  1067 Application Data
669 9.121014     52.85.232.220     192.168.0.7       TLSv1…    85 Application Data
754 9.457065     192.168.0.7       52.114.128.70     TLSv1…   282 Client Hello
893 9.744372     52.114.128.70     192.168.0.7       TLSv1…  1400 Server Hello, Certificate, Server Key Exchange, Server Hello Done
896 9.758601     192.168.0.7       52.114.128.70     TLSv1…   212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
912 10.034133    52.114.128.70     192.168.0.7       TLSv1…   105 Change Cipher Spec, Encrypted Handshake Message
914 10.035828    192.168.0.7       52.114.128.70     TLSv1…   994 Application Data
915 10.036068    192.168.0.7       52.114.128.70     TLSv1…  1176 Application Data
939 10.199185    192.168.0.7       23.45.162.131     TLSv1…   147 Application Data
947 10.315674    52.114.128.70     192.168.0.7       TLSv1…   411 Application Data
949 10.318010    192.168.0.7       52.114.128.70     TLSv1…   993 Application Data
```

```
        Length: 85
        Version: TLS 1.2 (0x0303)
      > Random: 5fce7cb1e68122b50cf881825e67e10933a57a250c6f9d59d13532a7a6657184
        Session ID Length: 32
        Session ID: dd4a000084816cbd725e317df547adc2ddb35a26185490e38b3f33bd7bee3063
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
        Compression Method: null (0)
        Extensions Length: 13
      > Extension: extended_master_secret (len=0)
      > Extension: renegotiation_info (len=1)
      > Extension: server_name (len=0)
```

```
0000  16 03 03 0f dd 02 00 00  55 03 03 5f ce 7c b1 e6   ········ U··_·|··
0010  81 22 b5 0c f8 81 82 5e  67 e1 09 33 a5 7a 25 0c   ·"·····^ g··3·z%·
0020  6f 9d 59 d1 35 32 a7 a6  65 71 84 20 dd 4a 00 00   o·Y·52·· eq· ·J··
0030  84 81 6c bd 72 5e 31 7d  f5 47 ad c2 dd b3 5a 26   ··l·r^1} ·G····Z&
0040  18 54 90 e3 8b 3f 33 bd  7b ee 30 63 c0 30 00 00   ·T···?3· {·0c·0··
0050  0d 00 17 00 00 ff 01 00  01 00 00 00 00 00 0b 00   ········ ········
0060  0e 0f 00 0e 0c 00 07 2a  30 82 07 26 30 82 05 0e   ·······* 0··&0···
```

Certificate:



```
660 9.121014     52.85.232.220     192.168.0.7       TLSv1…   735 Application Data
661 9.121014     52.85.232.220     192.168.0.7       TLSv1…    85 Application Data
668 9.121014     52.85.232.220     192.168.0.7       TLSv1…  1067 Application Data
669 9.121014     52.85.232.220     192.168.0.7       TLSv1…    85 Application Data
754 9.457065     192.168.0.7       52.114.128.70     TLSv1…   282 Client Hello
893 9.744372     52.114.128.70     192.168.0.7       TLSv1…  1400 Server Hello, Certificate, Server Key Exchange, Server Hello Done
896 9.758601     192.168.0.7       52.114.128.70     TLSv1…   212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
912 10.034133    52.114.128.70     192.168.0.7       TLSv1…   105 Change Cipher Spec, Encrypted Handshake Message
914 10.035828    192.168.0.7       52.114.128.70     TLSv1…   994 Application Data
915 10.036068    192.168.0.7       52.114.128.70     TLSv1…  1176 Application Data
```

```
      > Extension: extended_master_secret (len=0)
      > Extension: renegotiation_info (len=1)
      > Extension: server_name (len=0)
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 3599
        Certificates Length: 3596
      > Certificates (3596 bytes)
    v Handshake Protocol: Server Key Exchange
        Handshake Type: Server Key Exchange (12)
        Length: 361
      > EC Diffie-Hellman Server Params
    v Handshake Protocol: Server Hello Done
        Handshake Type: Server Hello Done (14)
        Length: 0
```

Length of the certificate

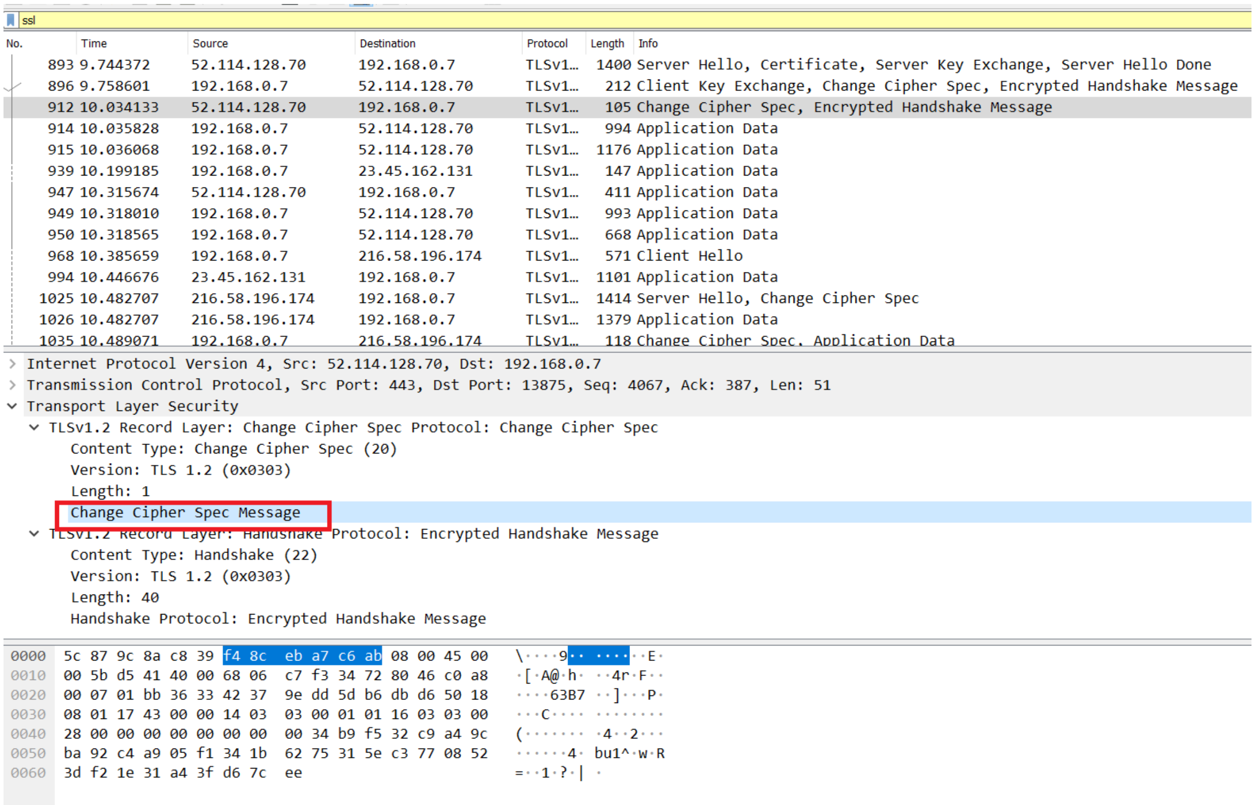
```
0060  0e 0f 00 0e 0c 00 07 2a  30 82 07 26 30 82 05 0e   ·······* 0··&0···
0070  a0 03 02 01 02 02 13 33  00 00 01 94 03 fc 70 4c   ·······3 ······pL
0080  4a 6b 63 a3 00 00 00 00  01 94 30 0d 06 09 2a 86   Jkc····· ··0···*·
0090  48 86 f7 0d 01 01 0b 05  00 30 7e 31 0b 30 09 06   H······· ·0~1·0··
00a0  03 55 04 06 13 02 55 53  31 13 30 11 06 03 55 04   ·U····US 1·0···U·
00b0  08 13 0a 57 61 73 68 69  6e 67 74 6f 6e 31 10 30   ···Washi ngton1·0
00c0  0e 06 03 55 04 07 13 07  52 65 64 6d 6f 6e 64 31   ···U···· Redmond1
00d0  1e 30 1c 06 03 55 04 0a  13 15 4d 69 63 72 6f 73   ·0···U·· ··Micros
```

List of certificates (tls.handshake.certificates), 3,596 bytes

Packets: 14121 · Displayed: 4

4. Observe what is done by the change cipher spec and authentication algorithms. Is it possible to capture the application data? Why?

- The Change Cipher Spec record is used to indicate the content of the next SSL records will be encrypted.



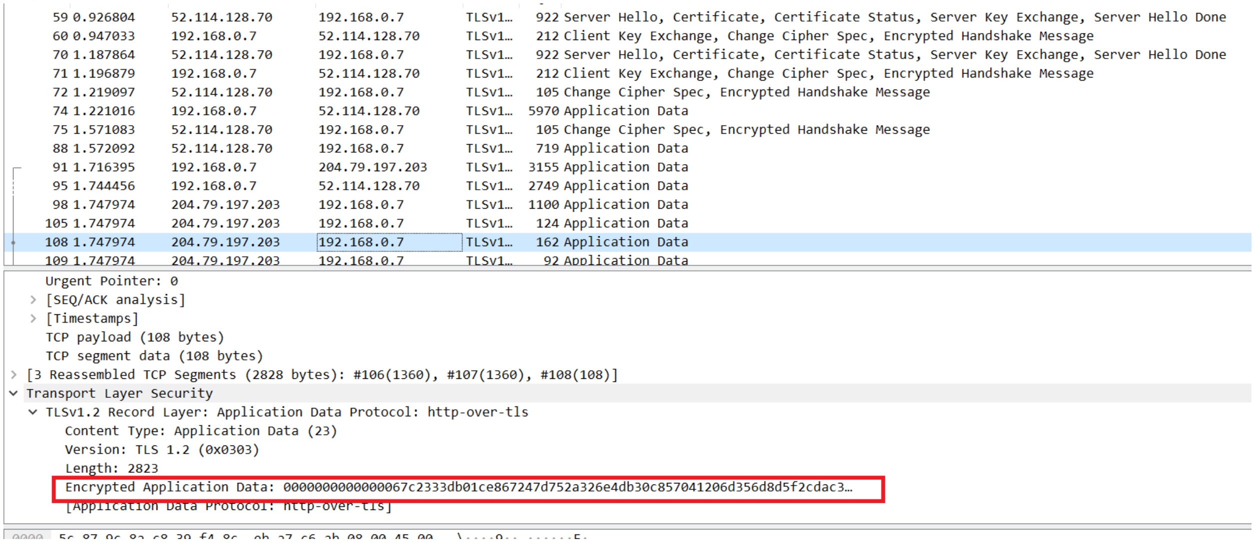
ssl

```
No.      Time        Source            Destination       Protocol  Length Info
  893 9.744372     52.114.128.70     192.168.0.7       TLSv1…    1400 Server Hello, Certificate, Server Key Exchange, Server Hello Done
  896 9.758601     192.168.0.7       52.114.128.70     TLSv1…     212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  912 10.034133    52.114.128.70     192.168.0.7       TLSv1…     105 Change Cipher Spec, Encrypted Handshake Message
  914 10.035828    192.168.0.7       52.114.128.70     TLSv1…     994 Application Data
  915 10.036068    192.168.0.7       52.114.128.70     TLSv1…    1176 Application Data
  939 10.199185    192.168.0.7       23.45.162.131     TLSv1…     147 Application Data
  947 10.315674    52.114.128.70     192.168.0.7       TLSv1…     411 Application Data
  949 10.318010    192.168.0.7       52.114.128.70     TLSv1…     993 Application Data
  950 10.318565    192.168.0.7       52.114.128.70     TLSv1…     668 Application Data
  968 10.385659    192.168.0.7       216.58.196.174    TLSv1…     571 Client Hello
  994 10.446676    23.45.162.131     192.168.0.7       TLSv1…    1101 Application Data
 1025 10.482707    216.58.196.174    192.168.0.7       TLSv1…    1414 Server Hello, Change Cipher Spec
 1026 10.482707    216.58.196.174    192.168.0.7       TLSv1…    1379 Application Data
 1035 10.489071    192.168.0.7       216.58.196.174    TLSv1…     118 Change Cipher Spec, Application Data
```

```
> Internet Protocol Version 4, Src: 52.114.128.70, Dst: 192.168.0.7
> Transmission Control Protocol, Src Port: 443, Dst Port: 13875, Seq: 4067, Ack: 387, Len: 51
v Transport Layer Security
  v TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
      Change Cipher Spec Message
  v TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 40
      Handshake Protocol: Encrypted Handshake Message
```

```
0000  5c 87 9c 8a c8 39 f4 8c  eb a7 c6 ab 08 00 45 00   \····9·· ······E·
0010  00 5b d5 41 40 00 68 06  c7 f3 34 72 80 46 c0 a8   ·[·A@·h· ··4r·F··
0020  00 07 01 bb 36 33 42 37  9e dd 5d b6 db d6 50 18   ····63B7 ··]···P·
0030  08 01 17 43 00 00 14 03  03 00 01 01 16 03 03 00   ···C···· ········
0040  28 00 00 00 00 00 00 00  00 34 b9 f5 32 c9 a4 9c   (······· ·4··2···
0050  ba 92 c4 a9 05 f1 34 1b  62 75 31 5e c3 77 08 52   ······4· bu1^·w·R
0060  3d f2 1e 31 a4 3f d6 7c  ee                        =··1·?·| ·
```

- We cannot get the application data because it is encrypted. The symmetric encryption algorithm is used to encrypt the application data



```
   59 0.926804     52.114.128.70     192.168.0.7       TLSv1…     922 Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
   60 0.947033     192.168.0.7       52.114.128.70     TLSv1…     212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   70 1.187864     52.114.128.70     192.168.0.7       TLSv1…     922 Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
   71 1.196879     192.168.0.7       52.114.128.70     TLSv1…     212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   72 1.219097     52.114.128.70     192.168.0.7       TLSv1…     105 Change Cipher Spec, Encrypted Handshake Message
   74 1.221016     192.168.0.7       52.114.128.70     TLSv1…    5970 Application Data
   75 1.571083     52.114.128.70     192.168.0.7       TLSv1…     105 Change Cipher Spec, Encrypted Handshake Message
   88 1.572092     52.114.128.70     192.168.0.7       TLSv1…     719 Application Data
   91 1.716395     192.168.0.7       204.79.197.203    TLSv1…    3155 Application Data
   95 1.744456     192.168.0.7       52.114.128.70     TLSv1…    2749 Application Data
   98 1.747974     204.79.197.203    192.168.0.7       TLSv1…    1100 Application Data
  105 1.747974     204.79.197.203    192.168.0.7       TLSv1…     124 Application Data
  108 1.747974     204.79.197.203    192.168.0.7       TLSv1…     162 Application Data
  109 1.747974     204.79.197.203    192.168.0.7       TLSv1…      92 Application Data
```

```
    Urgent Pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (108 bytes)
    TCP segment data (108 bytes)
> [3 Reassembled TCP Segments (2828 bytes): #106(1360), #107(1360), #108(108)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 2823
      Encrypted Application Data: 0000000000000067c2333db01ce867247d752a326e4db30c857041206d356d8d5f2cdac3…
      [Application Data Protocol: http-over-tls]
```

```
0000  5c 87 9c 8a c8 39 f4 8c  eb a7 c6 ab 08 00 45 00   \····9·· ······E·
```