ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH

MẠNG MÁY TÍNH THỰC HÀNH - CO3094

Báo cáo:

Lab 8

Giảng viên hướng dẫn: Vũ Thành Tài

Sinh viên: Lê Đức Cường

MSSV: 2210423

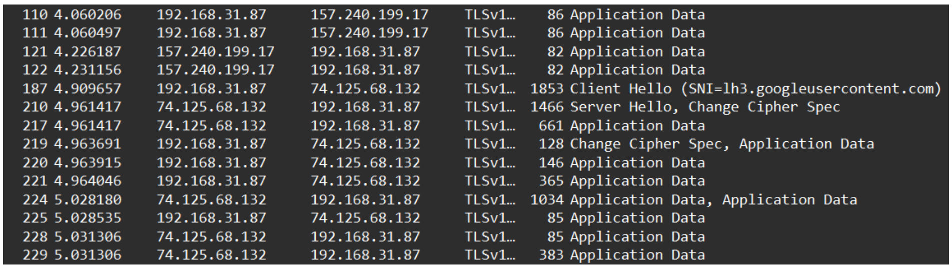
Thành phố Hồ Chí Minh, tháng 4 năm 2025

Mục lục

1 Question 1

For each of the first 8 Ethernet frames, specify the source of the frame (client or server), determine the number of SSL records that are included in the frame, and list the SSL record types that are included in the frame. Draw a timing diagram between client and server, with one arrow for each SSL record.

ANS:



```
110 4.060206    192.168.31.87    157.240.199.17    TLSv1…    86 Application Data
111 4.060497    192.168.31.87    157.240.199.17    TLSv1…    86 Application Data
121 4.226187    157.240.199.17   192.168.31.87     TLSv1…    82 Application Data
122 4.231156    157.240.199.17   192.168.31.87     TLSv1…    82 Application Data
187 4.909657    192.168.31.87    74.125.68.132     TLSv1…  1853 Client Hello (SNI=lh3.googleusercontent.com)
210 4.961417    74.125.68.132    192.168.31.87     TLSv1…  1466 Server Hello, Change Cipher Spec
217 4.961417    74.125.68.132    192.168.31.87     TLSv1…   661 Application Data
219 4.963691    192.168.31.87    74.125.68.132     TLSv1…   128 Change Cipher Spec, Application Data
220 4.963915    192.168.31.87    74.125.68.132     TLSv1…   146 Application Data
221 4.964046    192.168.31.87    74.125.68.132     TLSv1…   365 Application Data
224 5.028180    74.125.68.132    192.168.31.87     TLSv1…  1034 Application Data, Application Data
225 5.028535    192.168.31.87    74.125.68.132     TLSv1…    85 Application Data
228 5.031306    74.125.68.132    192.168.31.87     TLSv1…    85 Application Data
229 5.031306    74.125.68.132    192.168.31.87     TLSv1…   383 Application Data
```

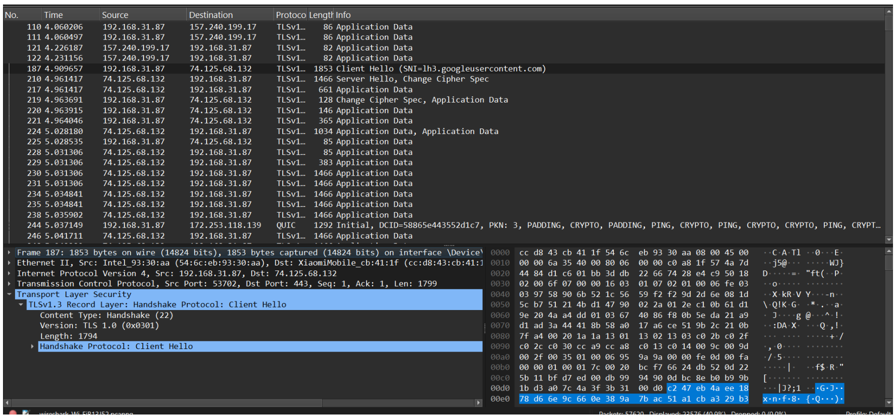
Frame	Source	SSL records	SSL type
110	Client	1	Application data
111	Client	1	Application data
121	Server	1	Application data
122	Server	1	Application data
187	Client	2	Client hello
210	Server	2	Server hello Change Cipher Spec
219	Server	2	Change Cipher Spec Application data

Bảng 1: SSL Records and Types

2 Question 2

Each of the SSL records begins with the same three fields (with possibly different values). One of these fields is "content type" and has length of one byte. List all three fields and their lengths.

ANS:



```
No.   Time      Source          Destination     Protoco Length Info
  110 4.060206  192.168.31.87   157.240.199.17  TLSv1…    86 Application Data
  111 4.060497  192.168.31.87   157.240.199.17  TLSv1…    86 Application Data
  121 4.226187  157.240.199.17  192.168.31.87   TLSv1…    82 Application Data
  122 4.231156  157.240.199.17  192.168.31.87   TLSv1…    82 Application Data
  187 4.909657  192.168.31.87   74.125.68.132   TLSv1…  1853 Client Hello (SNI=lh3.googleusercontent.com)
  210 4.961417  74.125.68.132   192.168.31.87   TLSv1…  1466 Server Hello, Change Cipher Spec
  217 4.961417  74.125.68.132   192.168.31.87   TLSv1…   661 Application Data
  219 4.963691  192.168.31.87   74.125.68.132   TLSv1…   128 Change Cipher Spec, Application Data
  220 4.963915  192.168.31.87   74.125.68.132   TLSv1…   146 Application Data
  221 4.964046  192.168.31.87   74.125.68.132   TLSv1…   365 Application Data
  224 5.028180  74.125.68.132   192.168.31.87   TLSv1…  1034 Application Data, Application Data
  225 5.028535  192.168.31.87   74.125.68.132   TLSv1…    85 Application Data
  228 5.031306  74.125.68.132   192.168.31.87   TLSv1…    85 Application Data
  229 5.031306  74.125.68.132   192.168.31.87   TLSv1…   383 Application Data
  230 5.031306  74.125.68.132   192.168.31.87   TLSv1…  1466 Application Data
  231 5.031306  74.125.68.132   192.168.31.87   TLSv1…  1466 Application Data
  234 5.034841  74.125.68.132   192.168.31.87   TLSv1…  1466 Application Data
  235 5.034841  74.125.68.132   192.168.31.87   TLSv1…  1466 Application Data
  238 5.035902  74.125.68.132   192.168.31.87   TLSv1…  1466 Application Data
  244 5.037149  192.168.31.87   172.253.118.139 QUIC    1292 Initial, DCID=58865e443552d1c7, PKN: 3, PADDING, CRYPTO, PADDING, PING, CRYPTO, PING, CRYPTO, CRYPTO, PING, CRYPT…
  246 5.041711  74.125.68.132   192.168.31.87   TLSv1…  1466 Application Data
```

```
▸ Frame 187: 1853 bytes on wire (14824 bits), 1853 bytes captured (14824 bits) on interface \Device\
▸ Ethernet II, Src: Intel_93:30:aa (54:6c:eb:93:30:aa), Dst: XiaomiMobile_cb:41:1f (cc:d8:43:cb:41:1
▸ Internet Protocol Version 4, Src: 192.168.31.87, Dst: 74.125.68.132
▸ Transmission Control Protocol, Src Port: 53702, Dst Port: 443, Seq: 1, Ack: 1, Len: 1799
▾ Transport Layer Security
  ▾ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 1794
    ▸ Handshake Protocol: Client Hello
```

```
0000  cc d8 43 cb 41 1f 54 6c  eb 93 30 aa 08 00 45 00   ··C·A·Tl ··0···E·
0010  00 00 6a 35 40 00 80 06  00 00 c0 a8 1f 57 4a 7d   ··j5@··· ·····WJ}
0020  44 84 d1 c6 01 bb 3d db  22 66 74 28 e4 c9 50 18   D·····=· "ft(··P·
0030  02 00 6f 07 00 00 16 03  01 07 02 01 00 06 fe 03   ··o····· ········
0040  03 97 58 90 6b 52 1c 56  59 f2 f2 9d 2d 6e 08 1d   ··X·kR·V Y···-n··
0050  5c b7 51 21 4b d1 47 90  02 2a 01 2e c1 0b 61 d1   \·Q!K·G· ·*·.··a·
0060  9e 20 4a a4 dd 01 03 67  40 86 f8 0b 5e da 21 a9   · J····g @···^·!·
0070  d1 ad 3a 44 41 8b 58 a0  17 a6 ce 51 9b 2c 21 0b   ··:DA·X· ···Q·,!·
0080  7f a4 00 20 1a 1a 13 01  13 02 13 03 c0 2b c0 2f   ··· ···· ·····+·/
0090  c0 2c c0 30 cc a9 cc a8  c0 13 c0 14 00 9c 00 9d   ·,·0···· ········
00a0  00 2f 00 35 01 00 06 95  9a 9a 00 00 fe 0d 00 fa   ·/·5···· ········
00b0  00 00 01 00 01 7c 00 20  bc f7 66 24 db 52 0d 22   ·····|·  ··f$·R·"
00c0  5b 11 bf d7 ed 00 db 99  94 90 0d bc 8e b0 b9 9b   [······· ········
00d0  1b d3 a0 7c 4a 3f 3b 31  00 d0 c2 47 eb 4a ee 18   ···|J?;1 ···G·J··
00e0  78 d6 6e 9c 66 0e 38 9a  7b ac 51 a1 cb a3 29 b3   x·n·f·8· {·Q···)·
```

Content Type: 1 byte

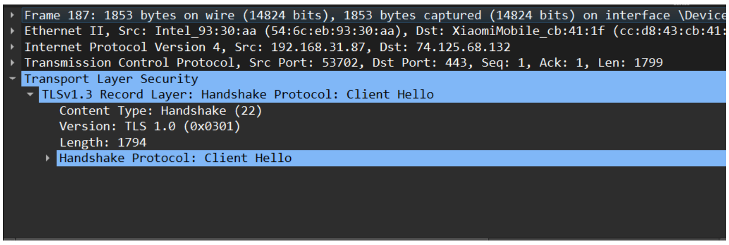
Version: 2 bytes

Length: 2 bytes

3 Question 3

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?

ANS:



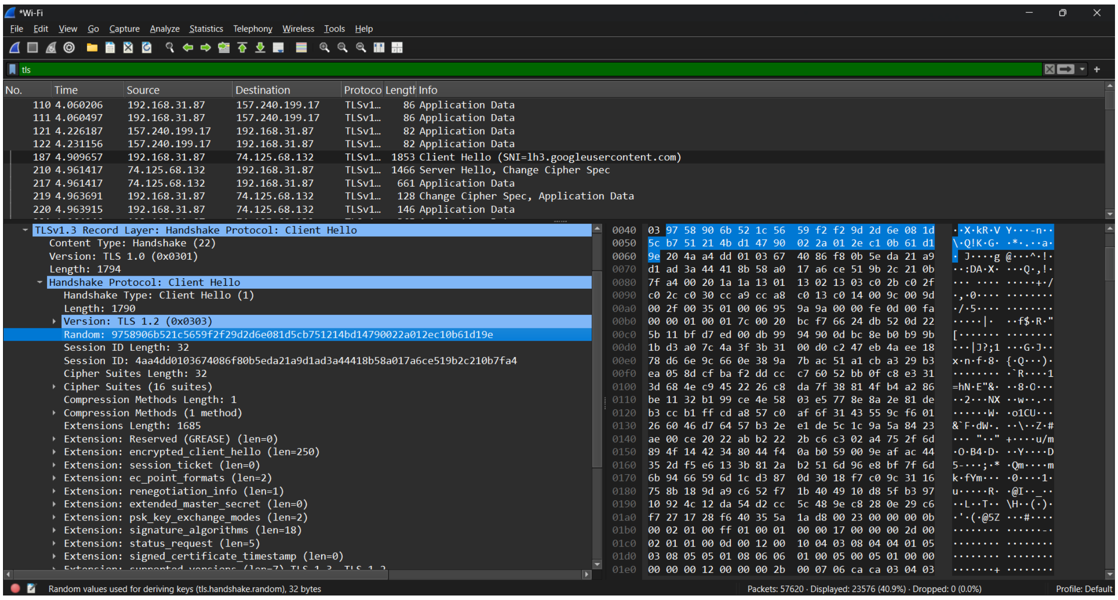
```
▸ Frame 187: 1853 bytes on wire (14824 bits), 1853 bytes captured (14824 bits) on interface \Device
▸ Ethernet II, Src: Intel_93:30:aa (54:6c:eb:93:30:aa), Dst: XiaomiMobile_cb:41:1f (cc:d8:43:cb:41:
▸ Internet Protocol Version 4, Src: 192.168.31.87, Dst: 74.125.68.132
▸ Transmission Control Protocol, Src Port: 53702, Dst Port: 443, Seq: 1, Ack: 1, Len: 1799
▾ Transport Layer Security
  ▾ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 1794
    ▸ Handshake Protocol: Client Hello
```

Handshake (22)

4 Question 4

Does the ClientHello record contain a nonce (also known as a "challenge")? If so, what is the value of the challenge in hexadecimal notation?

ANS:


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

```
No.   Time       Source           Destination      Protoco Length Info
  110 4.060206   192.168.31.87    157.240.199.17   TLSv1…    86 Application Data
  111 4.060497   192.168.31.87    157.240.199.17   TLSv1…    86 Application Data
  121 4.226187   157.240.199.17   192.168.31.87    TLSv1…    82 Application Data
  122 4.231156   157.240.199.17   192.168.31.87    TLSv1…    82 Application Data
  187 4.909657   192.168.31.87    74.125.68.132    TLSv1…  1853 Client Hello (SNI=lh3.googleusercontent.com)
  210 4.961417   74.125.68.132    192.168.31.87    TLSv1…  1466 Server Hello, Change Cipher Spec
  217 4.961417   74.125.68.132    192.168.31.87    TLSv1…   661 Application Data
  219 4.963691   192.168.31.87    74.125.68.132    TLSv1…   128 Change Cipher Spec, Application Data
  220 4.963915   192.168.31.87    74.125.68.132    TLSv1…   146 Application Data
```

```
TLSv1.3 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 1794
    Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 1790
        Version: TLS 1.2 (0x0303)
        Random: 9758906b521c5659f2f29d2d6e081d5cb751214bd14790022a012ec10b61d19e
        Session ID Length: 32
        Session ID: 4aa4dd0103674086f80b5eda21a9d1ad3a44418b58a017a6ce519b2c210b7fa4
        Cipher Suites Length: 32
        Cipher Suites (16 suites)
        Compression Methods Length: 1
        Compression Methods (1 method)
        Extensions Length: 1685
        Extension: Reserved (GREASE) (len=0)
        Extension: encrypted_client_hello (len=250)
        Extension: session_ticket (len=0)
        Extension: ec_point_formats (len=2)
        Extension: renegotiation_info (len=1)
        Extension: extended_master_secret (len=0)
        Extension: psk_key_exchange_modes (len=2)
        Extension: signature_algorithms (len=18)
        Extension: status_request (len=5)
        Extension: signed_certificate_timestamp (len=0)
```

```
0040  03 97 58 90 6b 52 1c 56  59 f2 f2 9d 2d 6e 08 1d   ··X·kR·V Y···-n··
0050  5c b7 51 21 4b d1 47 90  02 2a 01 2e c1 0b 61 d1   \·Q!K·G· ·*·.··a·
0060  9e 20 4a a4 dd 01 03 67  40 86 f8 0b 5e da 21 a9   · J····g @···^·!·
0070  d1 ad 3a 44 41 8b 58 a0  17 a6 ce 51 9b 2c 21 0b   ··:DA·X· ···Q·,!·
0080  7f a4 00 20 1a 1a 13 01  13 02 13 03 c0 2b c0 2f   ··· ···· ·····+·/
0090  c0 2c c0 30 cc a9 cc a8  c0 13 c0 14 00 9c 00 9d   ·,·0···· ········
00a0  00 2f 00 35 01 00 06 95  9a 9a 00 00 fe 0d 00 fa   ·/·5···· ········
00b0  00 00 01 00 01 7c 00 20  bc f7 66 24 db 52 0d 22   ·····|·  ··f$·R·"
00c0  5b 11 bf d7 ed 00 db 99  94 90 0d bc 8e b0 b9 9b   [······· ········
00d0  1b d3 a0 7c 4a 3f 3b 31  00 d0 c2 47 eb 4a ee 18   ···|J?;1 ···G·J··
00e0  78 d6 6e 9c 66 0e 38 9a  7b ac 51 a1 cb a3 29 b3   x·n·f·8· {·Q···)·
00f0  ea 05 8d cf ba f2 dd cc  c7 60 52 bb 0f c8 e3 31   ········ ·`R····1
0100  3d 68 4e c9 45 22 26 c8  da 7f 38 81 4f b4 a2 86   =hN·E"&· ··8·O···
0110  be 11 32 b1 99 ce 4e 58  03 e5 77 8e 8a 2e 81 de   ··2···NX ··w··.··
0120  b3 cc b1 ff cd a8 57 c0  af 6f 31 43 55 9c f6 01   ······W· ·o1CU···
0130  26 60 46 d7 64 57 b3 2e  e1 de 5c 1c 9a 5a 84 23   &`F·dW·. ··\··Z·#
0140  ae 00 ce 20 22 ab b2 22  2b c6 c3 02 a4 75 2f 6d   ··· "··" +····u/m
0150  89 4f 14 42 34 80 44 f4  0a b0 59 00 9e af ac 44   ·O·B4·D· ··Y····D
0160  35 2d f5 e6 13 3b 81 2a  b2 51 6d 96 e8 bf 7f 6d   5-···;·* ·Qm····m
0170  6b 94 66 59 6d 1c d3 87  0d 30 18 f7 c0 9c 31 16   k·fYm··· ·0····1·
0180  75 8b 18 9d a9 c6 52 f7  1b 40 49 10 d8 5f b3 97   u·····R· ·@I··_··
0190  10 92 4c 12 da 54 d2 cc  5c 48 9e c8 28 0e 29 c6   ··L··T·· \H··(·)·
01a0  f7 27 17 28 f6 40 35 5a  1a d8 00 23 00 00 00 0b   ·'·(·@5Z ···#····
01b0  00 02 01 00 ff 01 00 01  00 00 17 00 00 00 2d 00   ········ ······-·
01c0  02 01 01 00 0d 00 12 00  10 04 03 08 04 04 01 05   ········ ········
01d0  03 08 05 05 01 08 06 06  01 00 05 00 05 01 00 00   ········ ········
01e0  00 00 00 12 00 00 00 2b  00 07 06 ca ca 03 04 03   ·······+ ········
```

```
Random values used for deriving keys (tls.handshake.random), 32 bytes
Packets: 57620 · Displayed: 23576 (40.9%) · Dropped: 0 (0.0%)    Profile: Default
```

Yes, the ClientHello record contains a nonce, also known as a challenge. This nonce is found under the field labeled "Random" in the ClientHello handshake message.

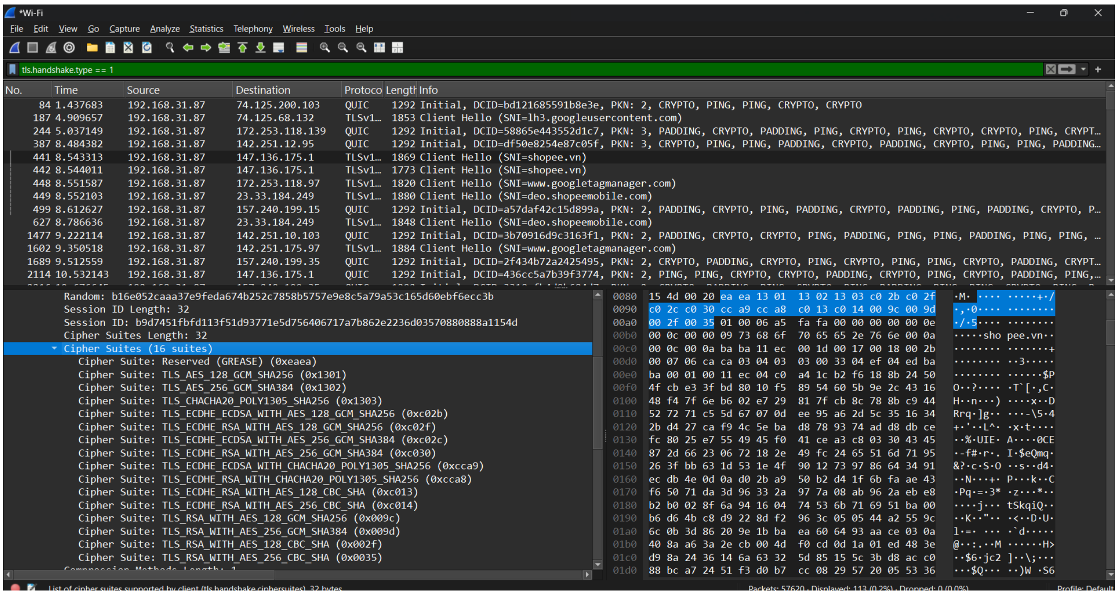
The value of the challenge (nonce) in hexadecimal notation is:

Random: 9758906b521c5659f2f29d2d6e081d5cb751214bd14790022a012ec10b61d19e

5 Question 5

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?

ANS:



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

tls.handshake.type == 1

```
No.   Time       Source         Destination     Protoco Length Info
   84 1.437683   192.168.31.87  74.125.200.103  QUIC    1292 Initial, DCID=bd121685591b8e3e, PKN: 2, CRYPTO, PING, PING, CRYPTO, CRYPTO
  187 4.909657   192.168.31.87  74.125.68.132   TLSv1…  1853 Client Hello (SNI=lh3.googleusercontent.com)
  244 5.037149   192.168.31.87  172.253.118.139 QUIC    1292 Initial, DCID=58865e443552d1c7, PKN: 3, PADDING, CRYPTO, PADDING, PING, CRYPTO, PING, CRYPTO, CRYPTO, PING, CRYPT…
  387 8.484382   192.168.31.87  142.251.12.95   QUIC    1292 Initial, DCID=df50e8254e87c05f, PKN: 3, CRYPTO, PING, PING, PADDING, CRYPTO, PADDING, CRYPTO, PING, PING, PADDING…
  441 8.543313   192.168.31.87  147.136.175.1   TLSv1…  1869 Client Hello (SNI=shopee.vn)
  442 8.544011   192.168.31.87  147.136.175.1   TLSv1…  1773 Client Hello (SNI=shopee.vn)
  448 8.551587   192.168.31.87  172.253.118.97  TLSv1…  1820 Client Hello (SNI=www.googletagmanager.com)
  449 8.552103   192.168.31.87  23.33.184.249   TLSv1…  1880 Client Hello (SNI=deo.shopeemobile.com)
  499 8.612627   192.168.31.87  157.240.199.15  QUIC    1292 Initial, DCID=a57daf42c15d899a, PKN: 2, PADDING, CRYPTO, PING, PADDING, CRYPTO, PADDING, PING, PADDING, CRYPTO, P…
  627 8.786636   192.168.31.87  23.33.184.249   TLSv1…  1848 Client Hello (SNI=deo.shopeemobile.com)
 1477 9.222114   192.168.31.87  142.251.10.103  QUIC    1292 Initial, DCID=3b70916d9c3163f1, PKN: 2, PADDING, CRYPTO, CRYPTO, PING, PADDING, PING, PING, PADDING, PING, PING, …
 1602 9.350518   192.168.31.87  142.251.175.97  TLSv1…  1884 Client Hello (SNI=www.googletagmanager.com)
 1689 9.512559   192.168.31.87  157.240.199.35  QUIC    1292 Initial, DCID=2f434b72a2425495, PKN: 2, CRYPTO, PADDING, CRYPTO, PING, CRYPTO, PING, PING, CRYPTO, PADDING, CRYPT…
 2114 10.532143  192.168.31.87  147.136.175.1   QUIC    1292 Initial, DCID=436cc5a7b39f3774, PKN: 2, PING, PING, CRYPTO, CRYPTO, PADDING, CRYPTO, PING, CRYPTO, PADDING, PING,…
```

```
        Random: b16e052caaa37e9feda674b252c7858b5757e9e8c5a79a53c165d60ebf6ecc3b
        Session ID Length: 32
        Session ID: b9d7451fbfd113f51d93771e5d756406717a7b862e2236d03570880888a1154d
        Cipher Suites Length: 32
      ▾ Cipher Suites (16 suites)
          Cipher Suite: Reserved (GREASE) (0xeaea)
          Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
          Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
          Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
          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_AES_256_GCM_SHA384 (0xc02c)
          Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
          Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
          Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
          Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
          Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
          Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
          Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
          Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
```

```
0080  15 4d 00 20 ea ea 13 01  13 02 13 03 c0 2b c0 2f   ·M· ···· ·····+·/
0090  c0 2c c0 30 cc a9 cc a8  c0 13 c0 14 00 9c 00 9d   ·,·0···· ········
00a0  00 2f 00 35 01 00 06 a5  fa fa 00 00 00 00 00 0e   ·/·5···· ········
00b0  00 0c 00 00 09 73 68 6f  70 65 65 2e 76 6e 00 0a   ·····sho pee.vn··
00c0  00 0c 00 0a ba ba 11 ec  00 1d 00 17 00 18 00 2b   ········ ·······+
00d0  00 07 06 ca ca 03 04 03  03 00 33 04 ef 04 ed ba   ········ ··3·····
00e0  ba 00 01 00 11 ec 04 c0  a4 1c b2 f6 18 8b 24 50   ········ ······$P
00f0  4f cb e3 3f bd 80 10 f5  89 54 60 5b 9e 2c 43 16   O··?···· ·T`[·,C·
0100  48 f4 7f 6e b6 02 e7 29  81 7f cb 8c 78 8b c9 44   H··n···) ····x··D
0110  52 72 71 c5 5d 67 07 0d  ee 95 a6 2d 5c 35 16 34   Rrq·]g·· ···-\5·4
0120  2b d4 27 ca f9 4c 5e ba  d8 78 93 74 ad d8 db ce   +·'··L^· ·x·t····
0130  fc 80 25 e7 55 49 45 f0  41 ce a3 c8 03 30 43 45   ··%·UIE· A····0CE
0140  87 2d 66 23 06 72 18 2e  49 fc 24 65 51 6d 71 95   ·-f#·r·. I·$eQmq·
0150  26 3f bb 63 1d 53 1e 4f  90 12 73 97 86 64 34 91   &?·c·S·O ··s··d4·
0160  ec db 4e 0d 0a d0 2b a9  50 b2 d4 1f 6b fa ae 43   ··N···+· P···k··C
0170  f6 50 71 da 3d 96 33 2a  97 7a 08 ab 96 2a eb e8   ·Pq·=·3* ·z···*··
0180  b2 b0 02 8f 6a 94 16 04  74 53 6b 71 69 51 ba 00   ····j··· tSkqiQ··
0190  b6 d6 4b c8 d9 22 8d f2  96 3c 05 05 44 a2 55 9c   ··K··"·· ·<··D·U·
01a0  6c 0b 3d 86 20 9e 1b ba  ea 60 64 93 aa ce 03 0a   l·=· ··· ·`d·····
01b0  40 8a a6 3a 2e cb 00 4d  f0 cd 0d 1a 01 ed 48 3e   @··:.··M ······H>
01c0  d9 8a 24 36 14 6a 63 32  5d 85 15 5c 3b d8 ac c0   ··$6·jc2 ]··\;···
01d0  88 bc a7 24 51 f3 d0 b7  cc 08 29 57 20 05 53 36   ···$Q··· ··)W ·S6
```

List of cipher suites supported by client (tls.handshake.ciphersuites), 32 bytes

Packets: 57620 · Displayed: 113 (0.2%) · Dropped: 0 (0.0%)

Profile: Default

Yes, the ClientHello record advertises the list of cipher suites that the client supports. These are listed under the "Cipher Suites" field.

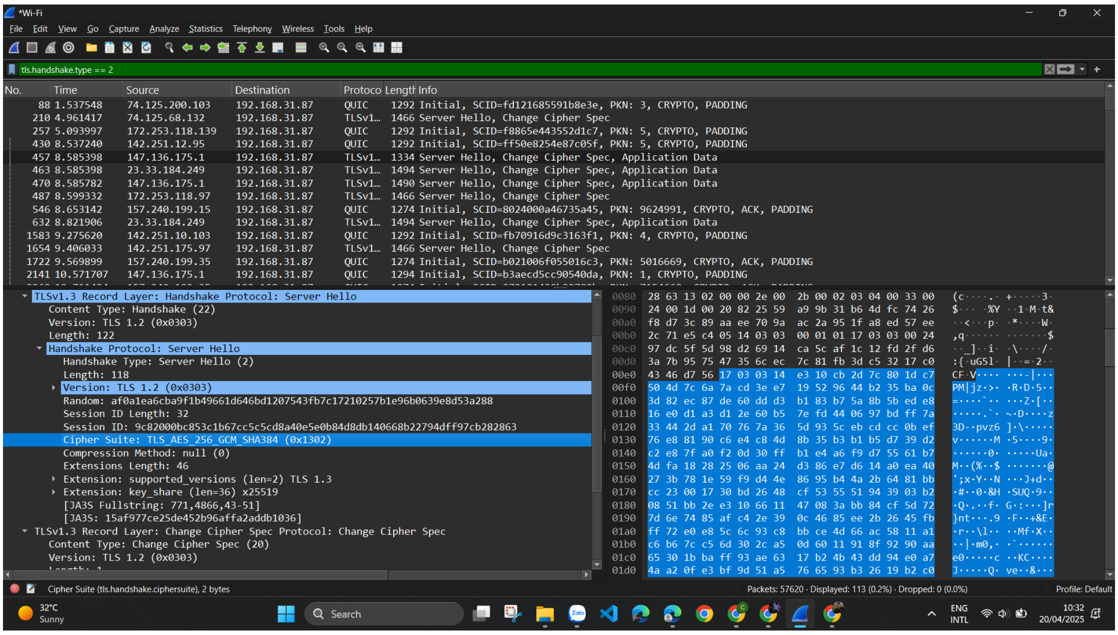
Public key algorithm: RSA, symmetric-key: RC4, hash: MD5

6 Question 6

Locate the ServerHello SSL record. Does this record specify a chosen cipher suite? What are the algorithms in the chosen cipher suite?

ANS:

Yes, the ServerHello record specifies the chosen cipher suite selected by the server from the list provided by the client.



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

tls.handshake.type == 2

```
No.   Time      Source          Destination   Protoco Lengtl Info
   88 1.537548  74.125.200.103  192.168.31.87 QUIC    1292 Initial, SCID=fd121685591b8e3e, PKN: 3, CRYPTO, PADDING
  210 4.961417  74.125.68.132   192.168.31.87 TLSv1…  1466 Server Hello, Change Cipher Spec
  257 5.093997  172.253.118.139 192.168.31.87 QUIC    1292 Initial, SCID=f8865e443552d1c7, PKN: 5, CRYPTO, PADDING
  430 8.537240  142.251.12.95   192.168.31.87 QUIC    1292 Initial, SCID=ff50e8254e87c05f, PKN: 5, CRYPTO, PADDING
  457 8.585398  147.136.175.1   192.168.31.87 TLSv1…  1334 Server Hello, Change Cipher Spec, Application Data
  463 8.585398  23.33.184.249   192.168.31.87 TLSv1…  1494 Server Hello, Change Cipher Spec, Application Data
  470 8.585782  147.136.175.1   192.168.31.87 TLSv1…  1490 Server Hello, Change Cipher Spec, Application Data
  487 8.599332  172.253.118.97  192.168.31.87 TLSv1…  1466 Server Hello, Change Cipher Spec
  546 8.653142  157.240.199.15  192.168.31.87 QUIC    1274 Initial, SCID=8024000a46735a45, PKN: 9624991, CRYPTO, ACK, PADDING
  632 8.821906  23.33.184.249   192.168.31.87 TLSv1…  1494 Server Hello, Change Cipher Spec, Application Data
 1583 9.275620  142.251.10.103  192.168.31.87 QUIC    1292 Initial, SCID=fb70916d9c3163f1, PKN: 4, CRYPTO, PADDING
 1654 9.406033  142.251.175.97  192.168.31.87 TLSv1…  1466 Server Hello, Change Cipher Spec
 1722 9.569899  157.240.199.35  192.168.31.87 QUIC    1274 Initial, SCID=b021006f055016c3, PKN: 5016669, CRYPTO, ACK, PADDING
 2141 10.571707 147.136.175.1   192.168.31.87 QUIC    1294 Initial, SCID=b3aecd5cc90540da, PKN: 1, CRYPTO, PADDING
```

```
TLSv1.3 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 122
    Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 118
        Version: TLS 1.2 (0x0303)
        Random: af0a1ea6cba9f1b49661d646bd1207543fb7c17210257b1e96b0639e8d53a288
        Session ID Length: 32
        Session ID: 9c82000bc853c1b67cc5c5cd8a40e5e0b84d8db140668b22794dff97cb282863
        Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
        Compression Method: null (0)
        Extensions Length: 46
        Extension: supported_versions (len=2) TLS 1.3
        Extension: key_share (len=36) x25519
        [JA3S Fullstring: 771,4866,43-51]
        [JA3S: 15af977ce25de452b96affa2addb1036]
TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.2 (0x0303)
```

```
0080  28 63 13 02 00 00 2e 00  2b 00 02 03 04 00 33 00   (c····.· +·····3·
0090  24 00 1d 00 20 82 25 59  a9 9b 31 b6 4d fc 74 26   $··· ·%Y ··1·M·t&
00a0  f8 d7 3c 89 aa ee 70 9a  ac 2a 95 1f a8 ed 57 ee   ··<···p· ·*····W·
00b0  2c 71 e5 c4 05 14 03 03  00 01 01 17 03 03 00 24   ,q······ ·······$
00c0  97 dc 5f 5d 98 d2 69 14  ca 5c af 1c 12 fd 2f d6   ··_]··i· ·\····/·
00d0  3a 7b 95 75 47 35 6c ec  7c 81 fb 3d c5 32 17 c0   :{·uG5l· |··=·2··
00e0  43 46 d7 56 17 03 03 14  e3 10 cb 2d 7c 80 1d c7   CF·V···· ···-|···
00f0  50 4d 7c 6a 7a cd 3e e7  19 52 96 44 b2 35 ba 0c   PM|jz·>· ·R·D·5··
0100  3d 82 ec 87 de 60 dd d3  b1 83 b7 5a 8b 5b ed e8   =····`·· ···Z·[··
0110  16 e0 d1 a3 d1 2e 60 b5  7e fd 44 06 97 bd ff 7a   ·····.`· ~·D····z
0120  33 44 2d a1 70 76 7a 36  5d 93 5c eb cd cc 0b ef   3D-·pvz6 ]·\·····
0130  76 e8 81 90 c6 e4 c8 4d  8b 35 b3 b1 b5 d7 39 d2   v······M ·5····9·
0140  c2 e8 7f a0 f2 0d 30 ff  b1 e4 a6 f9 d7 55 61 b7   ······0· ·····Ua·
0150  4d fa 18 28 25 06 aa 24  d3 86 e7 d6 14 a0 ea 40   M··(%··$ ·······@
0160  27 3b 78 1e 59 f9 d4 4e  86 95 b4 4a 2b 64 81 bb   ';x·Y··N ···J+d··
0170  cc 23 00 17 30 bd 26 48  cf 53 55 51 94 39 03 b2   ·#··0·&H ·SUQ·9··
0180  08 51 bb 2e e3 10 66 11  47 08 3a bb 84 cf 5d 72   ·Q·.··f· G·:···]r
0190  7d 6e 74 85 af c4 2e 39  0c 46 85 ee 2b 26 45 fb   }nt···.9 ·F··+&E·
01a0  ff 72 e0 e8 5c 6c 93 c8  bb ce 4d 66 ac 58 11 a1   ·r··\l·· ··Mf·X··
01b0  c6 b6 7c c5 6d 30 2c a5  0d 60 11 91 8f 92 90 aa   ··|·m0,· ·`······
01c0  65 30 1b ba ff 93 ae 63  17 b2 4b 43 dd 94 e0 a7   e0·····c ··KC····
01d0  4a a2 0f e3 bf 9d 51 a5  76 65 93 b3 26 19 b2 c0   J·····Q· ve··&···
```

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

Packets: 57620 · Displayed: 113 (0.2%) · Dropped: 0 (0.0%)

Profile: Default

7 Question 7

Does this record include a nonce? If so, how long is it? What is the purpose of the client and server nonces in SSL?

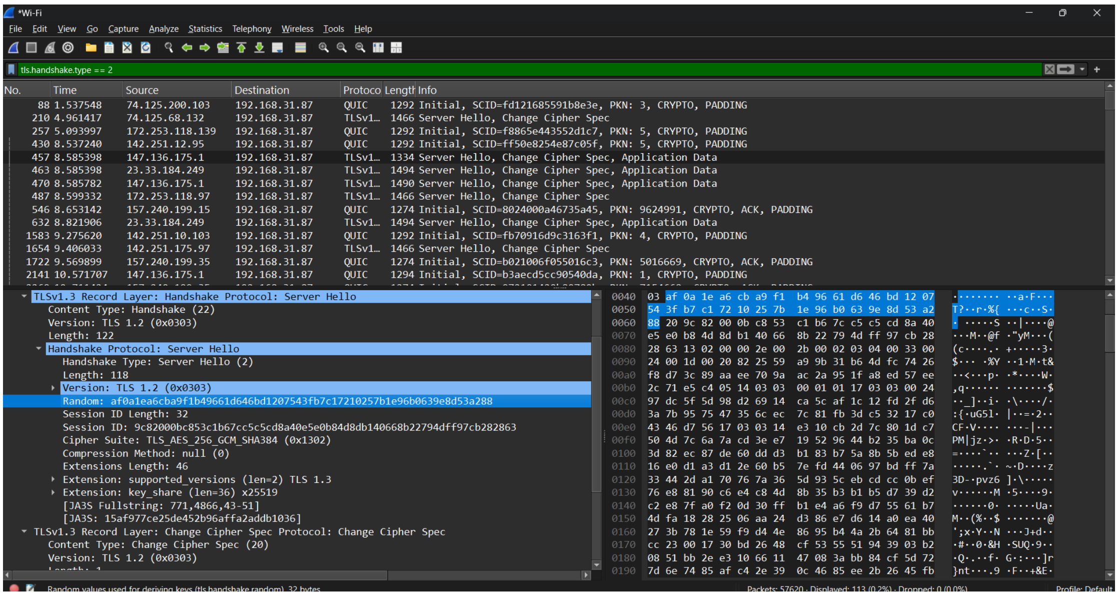
ANS:

Yes, the ServerHello record includes a nonce, also known as the server's random value. This value is located in the "Random" field under the ServerHello handshake message.

- The nonce is 32 bytes (256 bits) in length.
- It is generated randomly by the server and used during key exchange.

Purpose of client and server nonces:

The client and server nonces are used to ensure the uniqueness of each SSL/TLS session and to help in the generation of session keys. Including random values from both parties helps prevent replay attacks and ensures strong cryptographic key derivation.


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

```
tls.handshake.type == 2

No.  Time       Source           Destination    Protoco Length Info
  88 1.537548   74.125.200.103   192.168.31.87  QUIC    1292 Initial, SCID=fd121685591b8e3e, PKN: 3, CRYPTO, PADDING
 210 4.961417   74.125.68.132    192.168.31.87  TLSv1…  1466 Server Hello, Change Cipher Spec
 257 5.093997   172.253.118.139  192.168.31.87  QUIC    1292 Initial, SCID=f8865e443552d1c7, PKN: 5, CRYPTO, PADDING
 430 8.537240   142.251.12.95    192.168.31.87  QUIC    1292 Initial, SCID=ff50e8254e87c05f, PKN: 5, CRYPTO, PADDING
 457 8.585398   147.136.175.1    192.168.31.87  TLSv1…  1334 Server Hello, Change Cipher Spec, Application Data
 463 8.585398   23.33.184.249    192.168.31.87  TLSv1…  1494 Server Hello, Change Cipher Spec, Application Data
 470 8.585782   147.136.175.1    192.168.31.87  TLSv1…  1490 Server Hello, Change Cipher Spec, Application Data
 487 8.599332   172.253.118.97   192.168.31.87  TLSv1…  1466 Server Hello, Change Cipher Spec
 546 8.653142   157.240.199.15   192.168.31.87  QUIC    1274 Initial, SCID=8024000a46735a45, PKN: 9624991, CRYPTO, ACK, PADDING
 632 8.821906   23.33.184.249    192.168.31.87  TLSv1…  1494 Server Hello, Change Cipher Spec, Application Data
1583 9.275620   142.251.10.103   192.168.31.87  QUIC    1292 Initial, SCID=fb70916d9c3163f1, PKN: 4, CRYPTO, PADDING
1654 9.406033   142.251.175.97   192.168.31.87  TLSv1…  1466 Server Hello, Change Cipher Spec
1722 9.569899   157.240.199.35   192.168.31.87  QUIC    1274 Initial, SCID=b021006f055016c3, PKN: 5016669, CRYPTO, ACK, PADDING
2141 10.571707  147.136.175.1    192.168.31.87  QUIC    1294 Initial, SCID=b3aecd5cc90540da, PKN: 1, CRYPTO, PADDING
```

```
TLSv1.3 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 122
    Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 118
        Version: TLS 1.2 (0x0303)
        Random: af0a1ea6cba9f1b49661d646bd1207543fb7c17210257b1e96b0639e8d53a288
        Session ID Length: 32
        Session ID: 9c82000bc853c1b67cc5c5cd8a40e5e0b84d8db140668b22794dff97cb282863
        Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
        Compression Method: null (0)
        Extensions Length: 46
        Extension: supported_versions (len=2) TLS 1.3
        Extension: key_share (len=36) x25519
        [JA3S Fullstring: 771,4866,43-51]
        [JA3S: 15af977ce25de452b96affa2addb1036]
TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.2 (0x0303)
```

```
0040  03 af 0a 1e a6 cb a9 f1  b4 96 61 d6 46 bd 12 07   ········ ··a·F···
0050  54 3f b7 c1 72 10 25 7b  1e 96 b0 63 9e 8d 53 a2   T?··r·%{ ···c··S·
0060  88 20 9c 82 00 0b c8 53  c1 b6 7c c5 c5 cd 8a 40   ·  ·····S ··|····@
0070  e5 e0 b8 4d 8d b1 40 66  8b 22 79 4d ff 97 cb 28   ···M··@f ·"yM···(
0080  28 63 13 02 00 00 2e 00  2b 00 02 03 04 00 33 00   (c·····.· +·····3·
0090  24 00 1d 00 20 82 25 59  a9 9b 31 b6 4d fc 74 26   $··· ·%Y ··1·M·t&
00a0  f8 d7 3c 89 aa ee 70 9a  ac 2a 95 1f a8 ed 57 ee   ··<···p· ·*····W·
00b0  2c 71 e5 c4 05 14 03 03  00 01 01 17 03 03 00 24   ,q······ ·······$
00c0  97 dc 5f 5d 98 d2 69 14  ca 5c af 1c 12 fd 2f d6   ··_]··i· ·\····/·
00d0  3a 7b 95 75 47 35 6c ec  7c 81 fb 3d c5 32 17 c0   :{·uG5l· |··=·2··
00e0  43 46 d7 56 17 03 03 14  e3 10 cb 2d 7c 80 1d c7   CF·V···· ···-|···
00f0  50 4d 7c 6a 7a cd 3e e7  19 52 96 44 b2 35 ba 0c   PM|jz·>· ·R·D·5··
0100  3d 82 ec 87 de 60 dd d3  b1 83 b7 5a 8b 5b ed e8   =····`·· ···Z·[··
0110  16 e0 d1 a3 d1 2e 60 b5  7e fd 44 06 97 bd ff 7a   ·····.`· ~·D····z
0120  33 44 2d a1 70 76 7a 36  5d 93 5c eb cd cc 0b ef   3D-·pvz6 ]·\·····
0130  76 e8 81 90 c6 e4 c8 4d  8b 35 b3 b1 b5 d7 39 d2   v······M ·5····9·
0140  c2 e8 7f a0 f2 0d 30 ff  b1 e4 a6 f9 d7 55 61 b7   ······0· ·····Ua·
0150  4d fa 18 28 25 06 aa 24  d3 86 e7 d6 14 a0 ea 40   M··(%··$ ·······@
0160  27 3b 78 1e 59 f9 d4 4e  86 95 b4 4a 2b 64 81 bb   ';x·Y··N ···J+d··
0170  cc 23 00 17 30 bd 26 48  cf 53 55 51 94 39 03 b2   ·#··0·&H ·SUQ·9··
0180  08 51 bb 2e e3 10 66 11  47 08 3a bb 84 cf 5d 72   ·Q·.··f· G·:···]r
0190  7d 6e 74 85 af c4 2e 39  0c 46 85 ee 2b 26 45 fb   }nt···.9 ·F··+&E·
```

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

Packets: 57620 · Displayed: 113 (0.2%) · Dropped: 0 (0.0%)

Profile: Default

8 Question 8

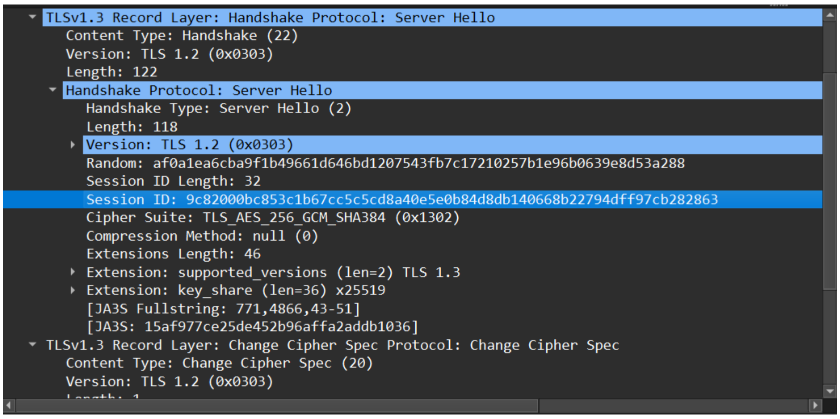
Does this record include a session ID? What is the purpose of the session ID?

ANS:

Yes, the ServerHello record includes a Session ID, which can be found under the "Session ID" field in the ServerHello message.

The session ID is typically 32 bytes or less, depending on the implementation.

Its hexadecimal value is shown in the trace.



```
TLSv1.3 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 122
    Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 118
        Version: TLS 1.2 (0x0303)
        Random: af0a1ea6cba9f1b49661d646bd1207543fb7c17210257b1e96b0639e8d53a288
        Session ID Length: 32
        Session ID: 9c82000bc853c1b67cc5c5cd8a40e5e0b84d8db140668b22794dff97cb282863
        Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
        Compression Method: null (0)
        Extensions Length: 46
        Extension: supported_versions (len=2) TLS 1.3
        Extension: key_share (len=36) x25519
        [JA3S Fullstring: 771,4866,43-51]
        [JA3S: 15af977ce25de452b96affa2addb1036]
TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
    Version: TLS 1.2 (0x0303)
```

9 Question 9

Does this record contain a certificate, or is the certificate included in a separate record. Does the certificate fit into a single Ethernet frame?

ANS:

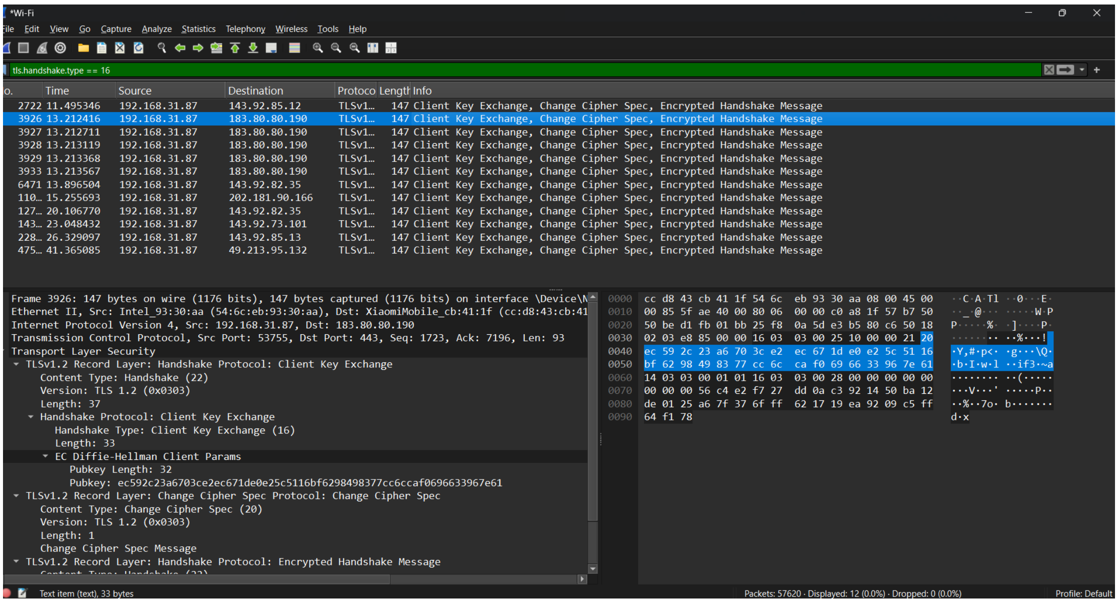
The certificate is not included in the same record as the ServerHello. Instead, it is sent in a separate handshake record labeled as "Certificate".

To determine whether the certificate fits within a single Ethernet frame, you can compare the TLS record length with the frame length.

10 Question 10

Locate the client key exchange record. Does this record contain a pre-master secret? What is this secret used for? Is the secret encrypted? If so, how? How long is the encrypted secret?

ANS:


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

```
tls.handshake.type == 16
```

```
No.   Time      Source         Destination     Protoco Length Info
 2722 11.495346 192.168.31.87  143.92.85.12    TLSv1…  147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 3926 13.212416 192.168.31.87  183.80.80.190   TLSv1…  147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 3927 13.212711 192.168.31.87  183.80.80.190   TLSv1…  147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 3928 13.213119 192.168.31.87  183.80.80.190   TLSv1…  147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 3929 13.213368 192.168.31.87  183.80.80.190   TLSv1…  147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 3933 13.213567 192.168.31.87  183.80.80.190   TLSv1…  147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 6471 13.896504 192.168.31.87  143.92.82.35    TLSv1…  147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 110… 15.255693 192.168.31.87  202.181.90.166  TLSv1…  147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 127… 20.106770 192.168.31.87  143.92.82.35    TLSv1…  147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 143… 23.048432 192.168.31.87  143.92.73.101   TLSv1…  147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 228… 26.329097 192.168.31.87  143.92.85.13    TLSv1…  147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 475… 41.365085 192.168.31.87  49.213.95.132   TLSv1…  147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
```

```
Frame 3926: 147 bytes on wire (1176 bits), 147 bytes captured (1176 bits) on interface \Device\N
Ethernet II, Src: Intel_93:30:aa (54:6c:eb:93:30:aa), Dst: XiaomiMobile_cb:41:1f (cc:d8:43:cb:41
Internet Protocol Version 4, Src: 192.168.31.87, Dst: 183.80.80.190
Transmission Control Protocol, Src Port: 53755, Dst Port: 443, Seq: 1723, Ack: 7196, Len: 93
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 37
    Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 33
      EC Diffie-Hellman Client Params
          Pubkey Length: 32
          Pubkey: ec592c23a6703ce2ec671de0e25c5116bf6298498377cc6ccaf0696633967e61
  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
  TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
```

```
0000  cc d8 43 cb 41 1f 54 6c  eb 93 30 aa 08 00 45 00   ··C·A·Tl ··0···E·
0010  00 85 5f ae 40 00 80 06  00 00 c0 a8 1f 57 b7 50   ··_·@··· ·····W·P
0020  50 be d1 fb 01 bb 25 f8  0a 5d e3 b5 80 c6 50 18   P·····%· ·]····P·
0030  02 03 e8 85 00 00 16 03  03 00 25 10 00 00 21 20   ········ ··%···!
0040  ec 59 2c 23 a6 70 3c e2  ec 67 1d e0 e2 5c 51 16   ·Y,#·p<· ·g···\Q·
0050  bf 62 98 49 83 77 cc 6c  ca f0 69 66 33 96 7e 61   ·b·I·w·l ··if3·~a
0060  14 03 03 00 01 01 16 03  03 00 28 00 00 00 00 00   ········ ··(·····
0070  00 00 00 56 c4 e2 f7 27  dd 0a c3 92 14 50 ba 12   ···V···' ·····P··
0080  de 01 25 a6 7f 37 6f ff  62 17 19 ea 92 09 c5 ff   ··%··7o· b·······
0090  64 f1 78                                          d·x
```

```
Text item (text), 33 bytes          Packets: 57620 · Displayed: 12 (0.0%) · Dropped: 0 (0.0%)          Profile: Default
```

The Client Key Exchange record contains Elliptic Curve Diffie-Hellman (ECDH) parameters, not an RSA-encrypted pre-master secret.

- Instead of sending a pre-master secret encrypted with the server's public key (as in RSA), the client sends an ephemeral public key (Pubkey) to the server.
- In this trace, the public key length is 32 bytes, and the value is shown in hexadecimal.

Purpose of these parameters:

The client and server use these keys to compute a shared secret using the ECDH key exchange algorithm. This shared secret is then used to derive the master secret, which is the basis for session encryption keys.

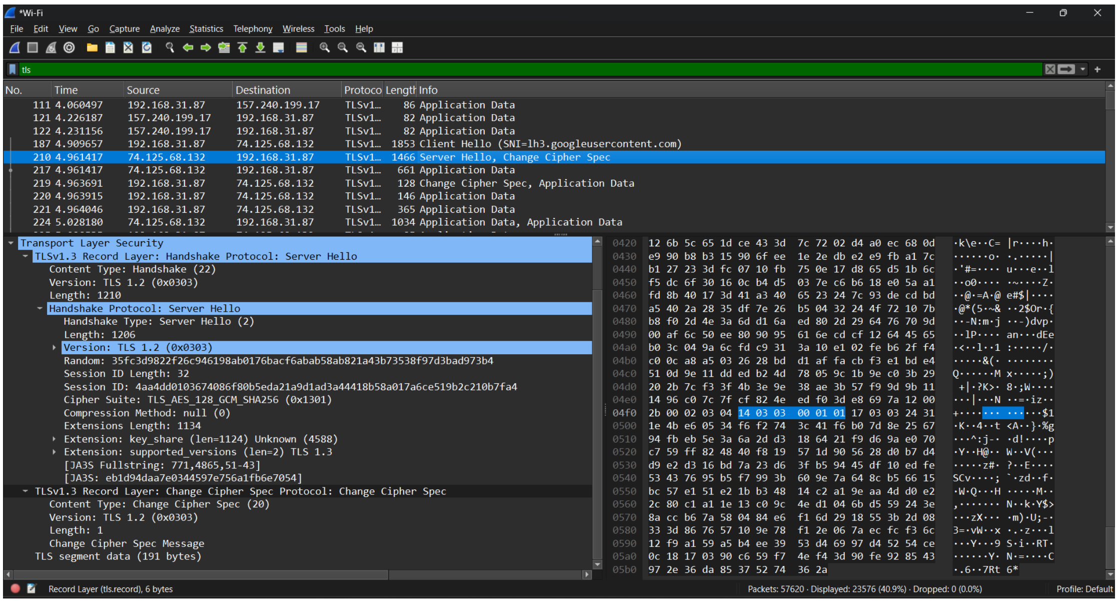
Encryption:

In ECDH, the shared secret is never transmitted. Only the public key is sent, so there's no need to encrypt it. The secrecy relies on the difficulty of the discrete logarithm problem in elliptic curve math.

11 Question 11

What is the purpose of the Change Cipher Spec record? How many bytes is the record in your trace?

ANS:


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

```
No.   Time      Source           Destination      Protoco Length Info
  111 4.060497  192.168.31.87    157.240.199.17   TLSv1…    86 Application Data
  121 4.226187  157.240.199.17   192.168.31.87    TLSv1…    82 Application Data
  122 4.231156  157.240.199.17   192.168.31.87    TLSv1…    82 Application Data
  187 4.909657  192.168.31.87    74.125.68.132    TLSv1…  1853 Client Hello (SNI=lh3.googleusercontent.com)
  210 4.961417  74.125.68.132    192.168.31.87    TLSv1…  1466 Server Hello, Change Cipher Spec
  217 4.961417  74.125.68.132    192.168.31.87    TLSv1…   661 Application Data
  219 4.963691  192.168.31.87    74.125.68.132    TLSv1…   128 Change Cipher Spec, Application Data
  220 4.963915  192.168.31.87    74.125.68.132    TLSv1…   146 Application Data
  221 4.964046  192.168.31.87    74.125.68.132    TLSv1…   365 Application Data
  224 5.028180  74.125.68.132    192.168.31.87    TLSv1…  1034 Application Data, Application Data
```

```
Transport Layer Security
  TLSv1.3 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 1210
    Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 1206
      Version: TLS 1.2 (0x0303)
      Random: 35fc3d9822f26c946198ab0176bacf6abab58ab821a43b73538f97d3bad973b4
      Session ID Length: 32
      Session ID: 4aa4dd0103674086f80b5eda21a9d1ad3a44418b58a017a6ce519b2c210b7fa4
      Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
      Compression Method: null (0)
      Extensions Length: 1134
      Extension: key_share (len=1124) Unknown (4588)
      Extension: supported_versions (len=2) TLS 1.3
      [JA3S Fullstring: 771,4865,51-43]
      [JA3S: eb1d94daa7e0344597e756a1fb6e7054]
  TLSv1.3 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
  TLS segment data (191 bytes)
```

```
0420  12 6b 5c 65 1d ce 43 3d  7c 72 02 d4 a0 ec 68 0d   ·k\e··C= |r····h·
0430  e9 90 b8 b3 15 90 6f ee  1e 2e db e2 e9 fb a1 7c   ······o· ·.·····|
0440  b1 27 23 3d fc 07 10 fb  75 0e 17 d8 65 d5 1b 6c   ·'#=···· u···e··l
0450  f5 dc 6f 30 16 0c b4 d5  03 7e c6 b6 18 e0 5a a1   ··o0···· ·~····Z·
0460  fd 8b 40 17 3d 41 a3 40  65 23 24 7c 93 de cd bd   ··@·=A·@ e#$|····
0470  a5 40 2a 28 35 df 7e 26  b5 04 32 24 4f 72 10 7b   ·@*(5·~& ··2$Or·{
0480  b8 f0 2d 4e 3a 6d d1 6a  ed 80 2d 29 64 76 70 9d   ··-N:m·j ··-)dvp·
0490  00 af 6c 50 ee 80 90 95  61 6e cd cf 12 64 45 65   ··lP···· an···dEe
04a0  b0 3c 04 9a 6c fd c9 31  3a 10 e1 02 fe b6 2f f4   ·<··l··1 :·····/·
04b0  c0 0c a8 a5 03 26 28 bd  d1 af fa cb f3 e1 bd e4   ·····&(· ········
04c0  51 0d 9e 11 dd ed b2 4d  78 05 9c 1b 9e c0 3b 29   Q······M x·····;)
04d0  20 2b 7c f3 3f 4b 3e 9e  38 ae 3b 57 f9 9d 9b 11    +|·?K>· 8·;W····
04e0  14 96 c0 7c 7f cf 82 4e  ed f0 3d e8 69 7a 12 00   ···|···N ··=·iz··
04f0  2b 00 02 03 04 14 03 03  00 01 01 17 03 03 24 31   +······· ······$1
0500  1e 4b e6 05 34 f6 f2 74  3c 41 f6 b0 7d 8e 25 67   ·K··4··t <A··}·%g
0510  94 fb eb 5e 3a 6a 2d d3  18 64 21 f9 d6 9a e0 70   ···^:j-· ·d!····p
0520  c7 59 ff 82 48 40 f8 19  57 1d 90 56 28 d0 b7 d4   ·Y··H@·· W··V(···
0530  d9 e2 d3 16 bd 7a 23 d6  3f b5 94 45 df 10 ed fe   ·····z#· ?··E····
0540  53 43 76 95 b5 f7 99 3b  60 9e 7a 64 8c b5 66 15   SCv····; `·zd··f·
0550  bc 57 e1 51 e2 1b b3 48  14 c2 a1 9e aa 4d d0 e2   ·W·Q···H ·····M··
0560  2c 80 c1 a1 1e 13 c0 9c  4e d1 04 6b d5 59 24 3e   ,······· N··k·Y$>
0570  8a cc b6 7a 58 04 84 e6  f1 6d 29 18 55 3b 2d 08   ···zX··· ·m)·U;-·
0580  33 3d 86 76 57 10 9e 78  f1 2e 06 7a ec fc f3 6c   3=·vW··x ·.·z···l
0590  12 f9 a1 59 a5 b4 ee 39  53 d4 69 97 d4 52 54 ce   ···Y···9 S·i··RT·
05a0  0c 18 17 03 90 c6 59 f7  4e f4 3d 90 fe 92 85 43   ······Y· N·=····C
05b0  97 2e 36 da 85 37 52 74  36 2a                     ·.6··7Rt 6*
```

Record Layer (tls.record), 6 bytes

Packets: 57620 · Displayed: 23576 (40.9%) · Dropped: 0 (0.0%)

Profile: Default

The Change Cipher Spec record is used to indicate that subsequent messages from the client will be encrypted using the newly negotiated cipher suite and session keys derived during the handshake.

- Its purpose is to signal the switch from plaintext handshake messages to encrypted communication.
- It marks the end of the TLS handshake phase on the client side.

In the trace, the Change Cipher Spec record is 1 byte in length, as indicated by:

- Length: 1
- Change Cipher Spec Message

12 Question 12

In the encrypted handshake record, what is being encrypted? How?

ANS:

In the Encrypted Handshake record, the Finished message is being encrypted.

- The Finished message contains a field called verify_data, which is used to verify that both parties have the same session keys and that the handshake was not tampered with.
- This message is encrypted because the client has already sent the Change Cipher Spec, indicating that further messages should be encrypted.

How is it encrypted?

- The encryption is done using the symmetric keys that were derived from the master secret during the handshake.
- The actual encryption method depends on the selected cipher suite. For example:
  - If the cipher suite uses AES-128-GCM, then the record is encrypted using AES in Galois/Counter Mode with built-in authentication.
  - If using AES-CBC, then encryption is done using CBC mode with an HMAC for integrity.

13 Question 13

Does the server also send a change cipher record and an encrypted handshake record to the client? How are those records different from those sent by the client?

ANS:

Yes, the server also sends both a Change Cipher Spec record and an Encrypted Handshake record to the client.

- These records serve the same purpose as those sent by the client:
  - The Change Cipher Spec indicates that the server will now begin encrypting its messages.
  - The Encrypted Handshake Message (Finished) contains the server's verify_data to confirm that the handshake is complete and correct on the server's side.

How are the records different from those sent by the client?

- The structure and purpose are identical, but the content is different:
  - The client and server each generate their own verify_data based on their view of the handshake messages.
  - These values must match expectations on both sides to successfully complete the handshake.

14 Question 14

How is the application data being encrypted? Do the records containing application data include a MAC? Does Wireshark distinguish between the encrypted application data and the MAC?

ANS:

The symmetric encryption algorithm negotiated during the TLS handshake is used to encrypt the application data.

Yes, the records containing application data include a Message Authentication Code (MAC) for integrity verification (unless an authenticated encryption mode like GCM is used, in which case the MAC is integrated).

However, Wireshark does not distinguish between the encrypted application data and the MAC in the packet trace. It displays the entire content as a single block of encrypted data, without separating the MAC from the payload.

15 Question 15

Comment on and explain anything else that you found interesting in the trace.

ANS:

One interesting aspect I observed in the trace is how all application-level data is completely encrypted after the TLS handshake. This highlights the strength of TLS in protecting sensitive information, such as login credentials or payment details, by ensuring that no data is transmitted in plaintext.