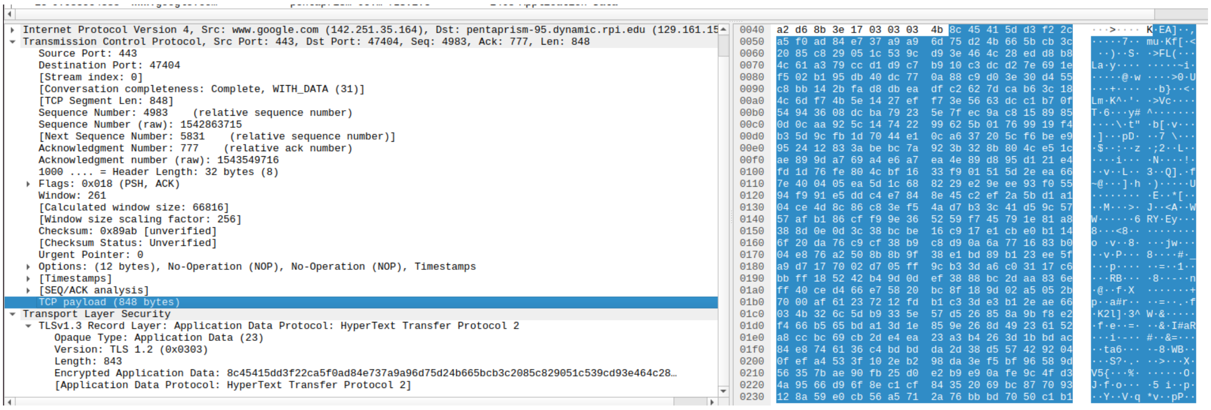
PART1:

1. list the essential packets No. used for TCP/TLS1.3 handshakes and write down their message types.
   There should be total 5 or 6 packets.
   A:
   1. Packet N0.1: Message Type: SYN
   2. Packet NO.2 ; Message Type: SYN / ACK
   3. Packet NO.3 ; Message Type: ACK
   4. Packet NO.4 ; Message Type: Client Hello
   5. Packet NO.6 ; Message Type: Server Hello, Change Cipher Spec
   6. Packet NO.12 ; Message Type: Change Cipher Spec

2. Pick an application data packet and write down its No. What's the payload you can find in that packet?
   A:
   Packet NO.22 ; Payload:

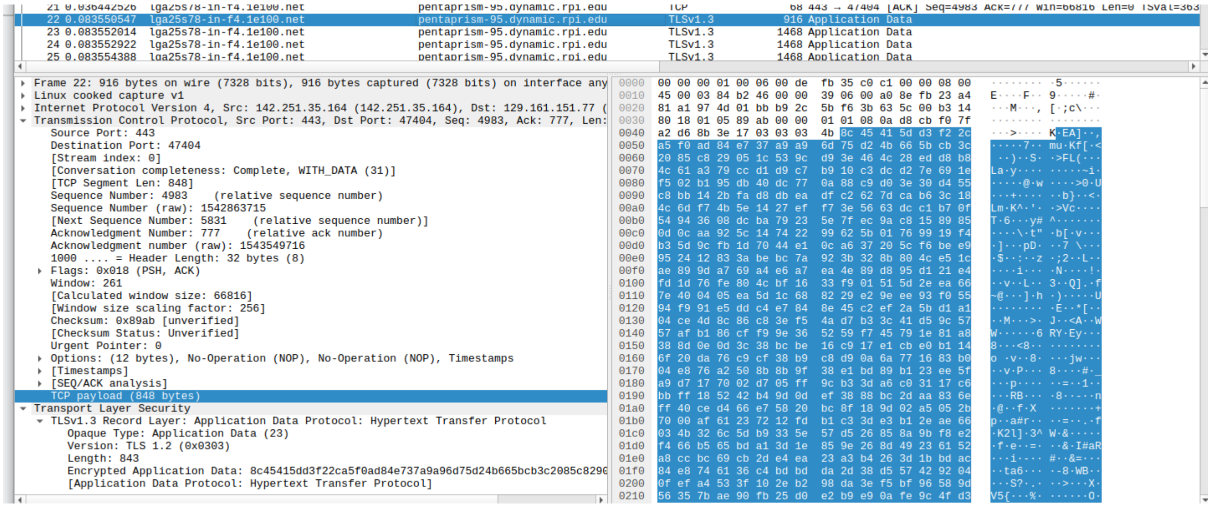


```
▸ Internet Protocol Version 4, Src: www.google.com (142.251.35.164), Dst: pentaprism-95.dynamic.rpi.edu (129.161.15
▾ Transmission Control Protocol, Src Port: 443, Dst Port: 47404, Seq: 4983, Ack: 777, Len: 848
    Source Port: 443
    Destination Port: 47404
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 848]
    Sequence Number: 4983    (relative sequence number)
    Sequence Number (raw): 1542863715
    [Next Sequence Number: 5831    (relative sequence number)]
    Acknowledgment Number: 777    (relative ack number)
    Acknowledgment number (raw): 1543549716
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x018 (PSH, ACK)
    Window: 261
    [Calculated window size: 66816]
    [Window size scaling factor: 256]
    Checksum: 0x89ab [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
    TCP payload (848 bytes)
▾ Transport Layer Security
  ▾ TLSv1.3 Record Layer: Application Data Protocol: HyperText Transfer Protocol 2
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 843
      Encrypted Application Data: 8c45415dd3f22ca5f0ad84e737a9a96d75d24b665bcb3c2085c829051c539cd93e464c28…
      [Application Data Protocol: HyperText Transfer Protocol 2]
```

```
0040  a2 d6 8b 3e 17 03 03 03  4b 8c 45 41 5d d3 f2 2c   ···>···· K·EA]··,
0050  a5 f0 ad 84 e7 37 a9 a9  6d 75 d2 4b 66 5b cb 3c   ·····7·· mu·Kf[·<
0060  20 85 c8 29 05 1c 53 9c  d9 3e 46 4c 28 ed d8 b8    ··)··S· ·>FL(···
0070  4c 61 a3 79 cc d1 d9 c7  b9 10 c3 dc d2 7e 69 1e   La·y···· ·····~i·
0080  f5 02 b1 95 db 40 dc 77  0a 88 c9 d0 3e 30 d4 55   ·····@·w ····>0·U
0090  c8 bb 14 2b fa d8 db ea  df c2 62 7d ca b6 3c 18   ···+···· ··b}··<·
00a0  4c 6d f7 4b 5e 14 27 ef  f7 3e 56 63 dc c1 b7 0f   Lm·K^·'· ·>Vc····
00b0  54 94 36 08 dc ba 79 23  5e 7f ec 9a c8 15 89 85   T·6···y# ^·······
00c0  0d 0c aa 92 5c 14 74 22  99 62 5b 01 76 99 19 f4   ····\·t" ·b[·v···
00d0  b3 5d 9c fb 1d 70 44 e1  0c a6 37 20 5c f6 be e9   ·]···pD· ··7 \···
00e0  95 24 12 83 3a be bc 7a  92 3b 32 8b 80 4c e5 1c   ·$··:··z ·;2··L··
00f0  ae 89 9d a7 69 a4 e6 a7  ea 4e 89 d8 95 d1 21 e4   ····i··· ·N····!·
0100  fd 1d 76 fe 80 4c bf 16  33 f9 01 51 5d 2e ea 66   ··v··L·· 3··Q].·f
0110  7e 40 04 05 ea 5d 1c 68  82 29 e2 9e ee 93 f0 55   ~@···]·h ·)·····U
0120  94 f9 91 e5 dd c4 e7 84  8e 45 c2 ef 2a 5b d1 a1   ········ ·E··*[··
0130  04 ce 4d 8c 86 c8 3e f5  4a d7 b3 3c 41 d5 9c 57   ··M···>· J··<A··W
0140  57 af b1 86 cf f9 9e 36  52 59 f7 45 79 1e 81 a8   W······6 RY·Ey···
0150  38 8d 0e 0d 3c 38 bc be  16 c9 17 e1 cb e0 b1 14   8···<8·· ········
0160  6f 20 da 76 c9 cf 38 b9  c8 d9 0a 6a 77 16 83 b0   o ·v··8· ···jw···
0170  04 e8 76 a2 50 8b 8b 9f  38 e1 bd 89 b1 23 ee 5f   ··v·P··· 8····#·_
0180  a9 d7 17 70 02 d7 05 ff  9c b3 3d a6 c0 31 17 c6   ···p···· ··=··1··
0190  bb ff 18 52 42 b4 9d 0d  ef 38 88 bc 2d aa 83 6e   ···RB··· ·8··-··n
01a0  ff 40 ce d4 66 e7 58 20  bc 8f 18 9d 02 a5 05 2b   ·@··f·X  ·······+
01b0  70 00 af 61 23 72 12 fd  b1 c3 3d e3 b1 2e ae 66   p··a#r·· ··=··.·f
01c0  03 4b 32 6c 5d b9 33 5e  57 d5 26 85 8a 9b f8 e2   ·K2l]·3^ W·&·····
01d0  f4 66 b5 65 bd a1 3d 1e  85 9e 26 8d 49 23 61 52   ·f·e··=· ··&·I#aR
01e0  a8 cc bc 69 cb 2d e4 ea  23 a3 b4 26 3d 1b bd ac   ···i·-·· #··&=···
01f0  84 e8 74 61 36 c4 bd bd  da 2d 38 d5 57 42 92 04   ··ta6··· ·-8·WB··
0200  0f ef a4 53 3f 10 2e b2  98 da 3e f5 bf 96 58 9d   ···S?·.· ··>···X·
0210  56 35 7b ae 90 fb 25 d0  e2 b9 e9 0a fe 9c 4f d3   V5{···%· ······O·
0220  4a 95 66 d9 6f 8e c1 cf  84 35 20 69 bc 87 70 93   J·f·o··· ·5 i··p·
0230  12 8a 59 e0 cb 56 a5 71  2a 76 bb bd 70 50 c1 b1   ··Y··V·q *v··pP··
```

3. Now it is the time to use the keys to decrypt the traffic. go to Preferences->Protocols->TLS->(Pre)-Master_scret log file. Select the part1keys.txt you generated before. Compare with the payload you saw before in your selected application data packet , what's the difference?
   A:
   The packets are decrypted by the txt file.

Before decryption:

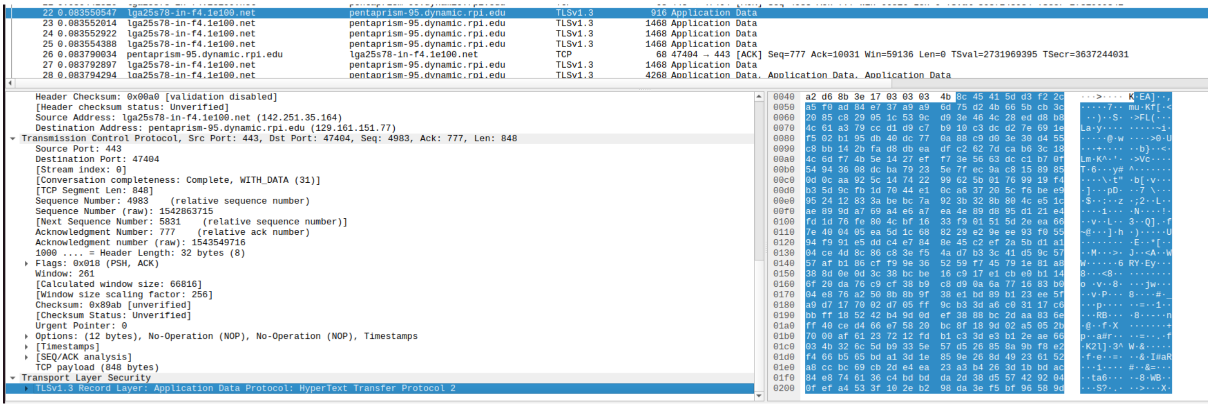


```
   21 0.036442526  lga25s78-in-f4.1e100.net       pentaprism-95.dynamic.rpi.edu   TCP         68 443 → 47404 [ACK] Seq=4983 Ack=777 Win=66816 Len=0 TSval=363
   22 0.083550547  lga25s78-in-f4.1e100.net       pentaprism-95.dynamic.rpi.edu   TLSv1.3    916 Application Data
   23 0.083552014  lga25s78-in-f4.1e100.net       pentaprism-95.dynamic.rpi.edu   TLSv1.3   1468 Application Data
   24 0.083552922  lga25s78-in-f4.1e100.net       pentaprism-95.dynamic.rpi.edu   TLSv1.3   1468 Application Data
   25 0.083554388  lga25s78-in-f4.1e100.net       pentaprism-95.dynamic.rpi.edu   TLSv1.3   1468 Application Data
```

```
▸ Frame 22: 916 bytes on wire (7328 bits), 916 bytes captured (7328 bits) on interface any
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 142.251.35.164 (142.251.35.164), Dst: 129.161.151.77 (
▾ Transmission Control Protocol, Src Port: 443, Dst Port: 47404, Seq: 4983, Ack: 777, Len:
    Source Port: 443
    Destination Port: 47404
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 848]
    Sequence Number: 4983    (relative sequence number)
    Sequence Number (raw): 1542863715
    [Next Sequence Number: 5831    (relative sequence number)]
    Acknowledgment Number: 777    (relative ack number)
    Acknowledgment number (raw): 1543549716
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x018 (PSH, ACK)
    Window: 261
    [Calculated window size: 66816]
    [Window size scaling factor: 256]
    Checksum: 0x89ab [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
    TCP payload (848 bytes)
▾ Transport Layer Security
  ▾ TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 843
      Encrypted Application Data: 8c45415dd3f22ca5f0ad84e737a9a96d75d24b665bcb3c2085c8290
      [Application Data Protocol: Hypertext Transfer Protocol]
```

```
0000  00 00 00 01 00 06 00 de  fb 35 c0 c1 00 00 08 00   ········ ·5······
0010  45 00 03 84 b2 46 00 00  39 06 00 a0 8e fb 23 a4   E····F·· 9·····#·
0020  81 a1 97 4d 01 bb b9 2c  5b f6 3b 63 5c 00 b3 14   ···M···, [·;c\···
0030  80 18 01 05 89 ab 00 00  01 01 08 0a d8 cb f0 7f   ········ ········
0040  a2 d6 8b 3e 17 03 03 03  4b 8c 45 41 5d d3 f2 2c   ···>···· K·EA]··,
0050  a5 f0 ad 84 e7 37 a9 a9  6d 75 d2 4b 66 5b cb 3c   ·····7·· mu·Kf[·<
0060  20 85 c8 29 05 1c 53 9c  d9 3e 46 4c 28 ed d8 b8    ··)··S· ·>FL(···
0070  4c 61 a3 79 cc d1 d9 c7  b9 10 c3 dc d2 7e 69 1e   La·y···· ·····~i·
0080  f5 02 b1 95 db 40 dc 77  0a 88 c9 d0 3e 30 d4 55   ·····@·w ····>0·U
0090  c8 bb 14 2b fa d8 db ea  df c2 62 7d ca b6 3c 18   ···+···· ··b}··<·
00a0  4c 6d f7 4b 5e 14 27 ef  f7 3e 56 63 dc c1 b7 0f   Lm·K^·'· ·>Vc····
00b0  54 94 36 08 dc ba 79 23  5e 7f ec 9a c8 15 89 85   T·6···y# ^·······
00c0  0d 0c aa 92 5c 14 74 22  99 62 5b 01 76 99 19 f4   ····\·t" ·b[·v···
00d0  b3 5d 9c fb 1d 70 44 e1  0c a6 37 20 5c f6 be e9   ·]···pD· ··7 \···
00e0  95 24 12 83 3a be bc 7a  92 3b 32 8b 80 4c e5 1c   ·$··:··z ·;2··L··
00f0  ae 89 9d a7 69 a4 e6 a7  ea 4e 89 d8 95 d1 21 e4   ····i··· ·N····!·
0100  fd 1d 76 fe 80 4c bf 16  33 f9 01 51 5d 2e ea 66   ··v··L·· 3··Q].·f
0110  7e 40 04 05 ea 5d 1c 68  82 29 e2 9e ee 93 f0 55   ~@···]·h ·)·····U
0120  94 f9 91 e5 dd c4 e7 84  8e 45 c2 ef 2a 5b d1 a1   ········ ·E··*[··
0130  04 ce 4d 8c 86 c8 3e f5  4a d7 b3 3c 41 d5 9c 57   ··M···>· J··<A··W
0140  57 af b1 86 cf f9 9e 36  52 59 f7 45 79 1e 81 a8   W······6 RY·Ey···
0150  38 8d 0e 0d 3c 38 bc be  16 c9 17 e1 cb e0 b1 14   8···<8·· ········
0160  6f 20 da 76 c9 cf 38 b9  c8 d9 0a 6a 77 16 83 b0   o ·v··8· ···jw···
0170  04 e8 76 a2 50 8b 8b 9f  38 e1 bd 89 b1 23 ee 5f   ··v·P··· 8····#·_
0180  a9 d7 17 70 02 d7 05 ff  9c b3 3d a6 c0 31 17 c6   ···p···· ··=··1··
0190  bb ff 18 52 42 b4 9d 0d  ef 38 88 bc 2d aa 83 6e   ···RB··· ·8··-··n
01a0  ff 40 ce d4 66 e7 58 20  bc 8f 18 9d 02 a5 05 2b   ·@··f·X  ·······+
01b0  70 00 af 61 23 72 12 fd  b1 c3 3d e3 b1 2e ae 66   p··a#r·· ··=··.·f
01c0  03 4b 32 6c 5d b9 33 5e  57 d5 26 85 8a 9b f8 e2   ·K2l]·3^ W·&·····
01d0  f4 66 b5 65 bd a1 3d 1e  85 9e 26 8d 49 23 61 52   ·f·e··=· ··&·I#aR
01e0  a8 cc bc 69 cb 2d e4 ea  23 a3 b4 26 3d 1b bd ac   ···i·-·· #··&=···
01f0  84 e8 74 61 36 c4 bd bd  da 2d 38 d5 57 42 92 04   ··ta6··· ·-8·WB··
0200  0f ef a4 53 3f 10 2e b2  98 da 3e f5 bf 96 58 9d   ···S?·.· ··>···X·
0210  56 35 7b ae 90 fb 25 d0  e2 b9 e9 0a fe 9c 4f d3   V5{···%· ······O·
```

After decryption:



```
   22 0.083550547  lga25s78-in-f4.1e100.net       pentaprism-95.dynamic.rpi.edu   TLSv1.3    916 Application Data
   23 0.083552014  lga25s78-in-f4.1e100.net       pentaprism-95.dynamic.rpi.edu   TLSv1.3   1468 Application Data
   24 0.083552922  lga25s78-in-f4.1e100.net       pentaprism-95.dynamic.rpi.edu   TLSv1.3   1468 Application Data
   25 0.083554388  lga25s78-in-f4.1e100.net       pentaprism-95.dynamic.rpi.edu   TLSv1.3   1468 Application Data
   26 0.083790034  pentaprism-95.dynamic.rpi.edu  lga25s78-in-f4.1e100.net        TCP         68 47404 → 443 [ACK] Seq=777 Ack=10031 Win=59136 Len=0 TSval=2731969395 TSecr=3637244031
   27 0.083792897  lga25s78-in-f4.1e100.net       pentaprism-95.dynamic.rpi.edu   TLSv1.3   1468 Application Data
   28 0.083794294  lga25s78-in-f4.1e100.net       pentaprism-95.dynamic.rpi.edu   TLSv1.3   4268 Application Data, Application Data, Application Data
```

```
    Header Checksum: 0x00a0 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: lga25s78-in-f4.1e100.net (142.251.35.164)
    Destination Address: pentaprism-95.dynamic.rpi.edu (129.161.151.77)
▾ Transmission Control Protocol, Src Port: 443, Dst Port: 47404, Seq: 4983, Ack: 777, Len: 848
    Source Port: 443
    Destination Port: 47404
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 848]
    Sequence Number: 4983    (relative sequence number)
    Sequence Number (raw): 1542863715
    [Next Sequence Number: 5831    (relative sequence number)]
    Acknowledgment Number: 777    (relative ack number)
    Acknowledgment number (raw): 1543549716
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x018 (PSH, ACK)
    Window: 261
    [Calculated window size: 66816]
    [Window size scaling factor: 256]
    Checksum: 0x89ab [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
    TCP payload (848 bytes)
▾ Transport Layer Security
  ▸ TLSv1.3 Record Layer: Application Data Protocol: HyperText Transfer Protocol 2
```

```
0040  a2 d6 8b 3e 17 03 03 03  4b 8c 45 41 5d d3 f2 2c   ···>···· K·EA]··,
0050  a5 f0 ad 84 e7 37 a9 a9  6d 75 d2 4b 66 5b cb 3c   ·····7·· mu·Kf[·<
0060  20 85 c8 29 05 1c 53 9c  d9 3e 46 4c 28 ed d8 b8    ··)··S· ·>FL(···
0070  4c 61 a3 79 cc d1 d9 c7  b9 10 c3 dc d2 7e 69 1e   La·y···· ·····~i·
0080  f5 02 b1 95 db 40 dc 77  0a 88 c9 d0 3e 30 d4 55   ·····@·w ····>0·U
0090  c8 bb 14 2b fa d8 db ea  df c2 62 7d ca b6 3c 18   ···+···· ··b}··<·
00a0  4c 6d f7 4b 5e 14 27 ef  f7 3e 56 63 dc c1 b7 0f   Lm·K^·'· ·>Vc····
00b0  54 94 36 08 dc ba 79 23  5e 7f ec 9a c8 15 89 85   T·6···y# ^·······
00c0  0d 0c aa 92 5c 14 74 22  99 62 5b 01 76 99 19 f4   ····\·t" ·b[·v···
00d0  b3 5d 9c fb 1d 70 44 e1  0c a6 37 20 5c f6 be e9   ·]···pD· ··7 \···
00e0  95 24 12 83 3a be bc 7a  92 3b 32 8b 80 4c e5 1c   ·$··:··z ·;2··L··
00f0  ae 89 9d a7 69 a4 e6 a7  ea 4e 89 d8 95 d1 21 e4   ····i··· ·N····!·
0100  fd 1d 76 fe 80 4c bf 16  33 f9 01 51 5d 2e ea 66   ··v··L·· 3··Q].·f
0110  7e 40 04 05 ea 5d 1c 68  82 29 e2 9e ee 93 f0 55   ~@···]·h ·)·····U
0120  94 f9 91 e5 dd c4 e7 84  8e 45 c2 ef 2a 5b d1 a1   ········ ·E··*[··
0130  04 ce 4d 8c 86 c8 3e f5  4a d7 b3 3c 41 d5 9c 57   ··M···>· J··<A··W
0140  57 af b1 86 cf f9 9e 36  52 59 f7 45 79 1e 81 a8   W······6 RY·Ey···
0150  38 8d 0e 0d 3c 38 bc be  16 c9 17 e1 cb e0 b1 14   8···<8·· ········
0160  6f 20 da 76 c9 cf 38 b9  c8 d9 0a 6a 77 16 83 b0   o ·v··8· ···jw···
0170  04 e8 76 a2 50 8b 8b 9f  38 e1 bd 89 b1 23 ee 5f   ··v·P··· 8····#·_
0180  a9 d7 17 70 02 d7 05 ff  9c b3 3d a6 c0 31 17 c6   ···p···· ··=··1··
0190  bb ff 18 52 42 b4 9d 0d  ef 38 88 bc 2d aa 83 6e   ···RB··· ·8··-··n
01a0  ff 40 ce d4 66 e7 58 20  bc 8f 18 9d 02 a5 05 2b   ·@··f·X  ·······+
01b0  70 00 af 61 23 72 12 fd  b1 c3 3d e3 b1 2e ae 66   p··a#r·· ··=··.·f
01c0  03 4b 32 6c 5d b9 33 5e  57 d5 26 85 8a 9b f8 e2   ·K2l]·3^ W·&·····
01d0  f4 66 b5 65 bd a1 3d 1e  85 9e 26 8d 49 23 61 52   ·f·e··=· ··&·I#aR
01e0  a8 cc bc 69 cb 2d e4 ea  23 a3 b4 26 3d 1b bd ac   ···i·-·· #··&=···
01f0  84 e8 74 61 36 c4 bd bd  da 2d 38 d5 57 42 92 04   ··ta6··· ·-8·WB··
0200  0f ef a4 53 3f 10 2e b2  98 da 3e f5 bf 96 58 9d   ···S?·.· ··>···X·
```

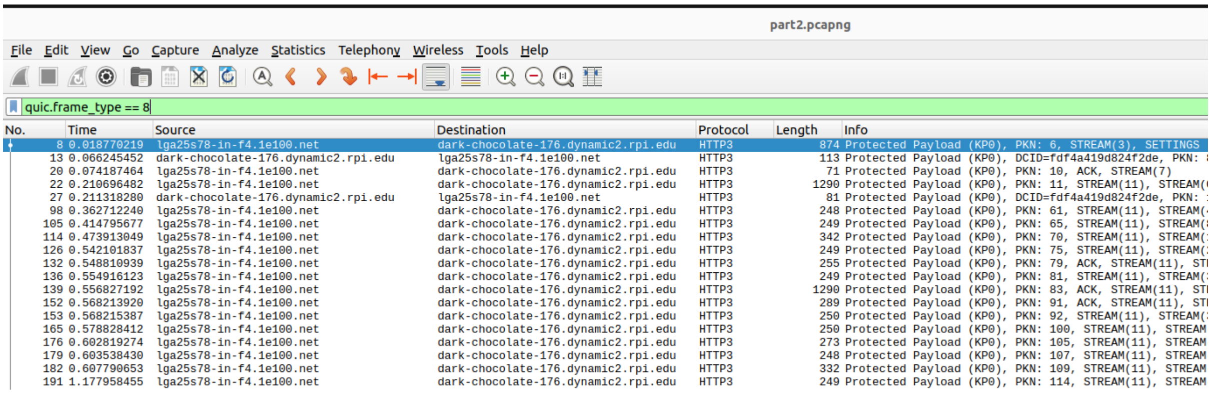
4. Continue to find a packet No. that contains plain text HTTP header method :GET. Write down the packet No. and all other header fields and values in the packet.
   A:
   :GET: Packet N0.14

PART2:

1. List the No. of packets that contains TLS hello messages, and describe how you find them.
   A:
   Filter by “tls.handshake.type == 1”, which corresponds with “Client Hello” message.
   Packet NO.1

2. List the all the frame types in the QUIC packet that contains clienthello message.
   A:
   CRYPTO

3. Do you see any stream frame types in payload packets? If you see it, list packet No. If not, explain why.
   A:
   Filtered packets with “quic.frame_type == 8”.
   All the packets shown in snapshot are steam frame types in payload packets.


part2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

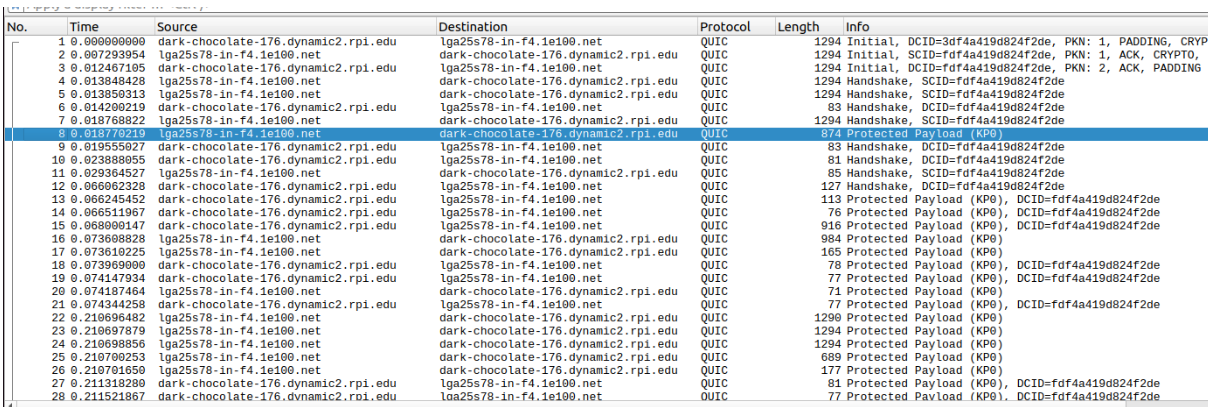
```
quic.frame_type == 8

No.   Time        Source                                Destination                           Protocol  Length Info
    8 0.018770219 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  HTTP3        874 Protected Payload (KP0), PKN: 6, STREAM(3), SETTINGS
   13 0.066245452 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             HTTP3        113 Protected Payload (KP0), DCID=fdf4a419d824f2de, PKN:
   20 0.074187464 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  HTTP3         71 Protected Payload (KP0), PKN: 10, ACK, STREAM(7)
   22 0.210696482 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  HTTP3       1290 Protected Payload (KP0), PKN: 11, STREAM(11), STREAM(
   27 0.211318280 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             HTTP3         81 Protected Payload (KP0), DCID=fdf4a419d824f2de, PKN:
   98 0.362712240 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  HTTP3        248 Protected Payload (KP0), PKN: 61, STREAM(11), STREAM(
  105 0.414795677 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  HTTP3        249 Protected Payload (KP0), PKN: 65, STREAM(11), STREAM(
  114 0.473913049 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  HTTP3        342 Protected Payload (KP0), PKN: 70, STREAM(11), STREAM(
  126 0.542101837 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  HTTP3        249 Protected Payload (KP0), PKN: 75, STREAM(11), STREAM(
  132 0.548810939 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  HTTP3        255 Protected Payload (KP0), PKN: 79, ACK, STREAM(11), ST
  136 0.554916123 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  HTTP3        249 Protected Payload (KP0), PKN: 81, STREAM(11), STREAM(
  139 0.556827192 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  HTTP3       1290 Protected Payload (KP0), PKN: 83, ACK, STREAM(11), ST
  152 0.568213920 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  HTTP3        289 Protected Payload (KP0), PKN: 91, ACK, STREAM(11), ST
  153 0.568215387 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  HTTP3        250 Protected Payload (KP0), PKN: 92, STREAM(11), STREAM(
  165 0.578828412 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  HTTP3        250 Protected Payload (KP0), PKN: 100, STREAM(11), STREAM
  176 0.602819274 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  HTTP3        273 Protected Payload (KP0), PKN: 105, STREAM(11), STREAM
  179 0.603538430 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  HTTP3        248 Protected Payload (KP0), PKN: 107, STREAM(11), STREAM
  182 0.607790653 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  HTTP3        332 Protected Payload (KP0), PKN: 109, STREAM(11), STREAM
  191 1.177958455 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  HTTP3        249 Protected Payload (KP0), PKN: 114, STREAM(11), STREAM
```

4. Now repeat the same decryption step by using part2keys.txt. Look for any packet that contains plain text HTTP header. If you find one, write down the Packet No. If not, explain why.

   A:

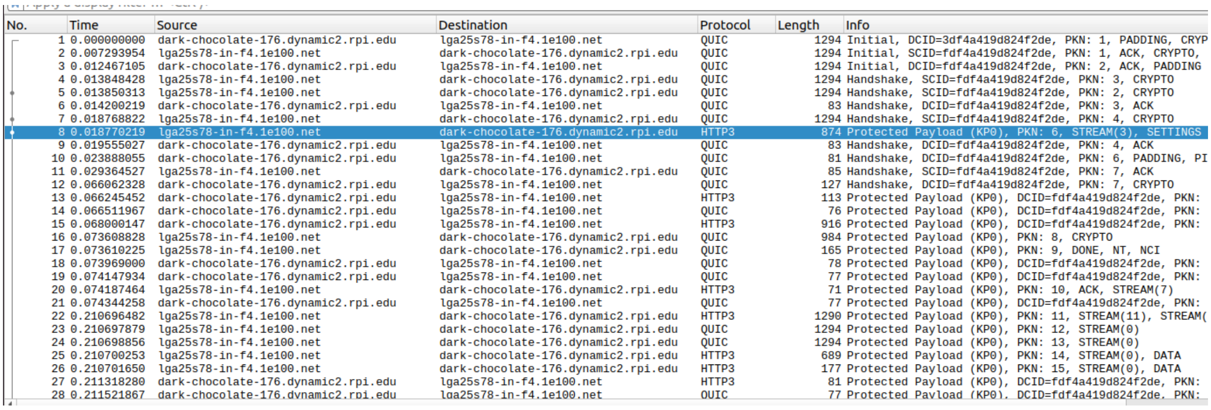
   After decryption, some of the QUIC becomes HTTPS3 (as packet NO.8), and the stream frame showed up.

   Before decryption:



```
No.   Time        Source                                Destination                           Protocol  Length Info
    1 0.000000000 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC        1294 Initial, DCID=3df4a419d824f2de, PKN: 1, PADDING, CRYP
    2 0.007293954 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC        1294 Initial, SCID=fdf4a419d824f2de, PKN: 1, ACK, CRYPTO,
    3 0.012467105 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC        1294 Initial, DCID=fdf4a419d824f2de, PKN: 2, ACK, PADDING
    4 0.013848428 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC        1294 Handshake, SCID=fdf4a419d824f2de
    5 0.013850313 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC        1294 Handshake, SCID=fdf4a419d824f2de
    6 0.014200219 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC          83 Handshake, DCID=fdf4a419d824f2de
    7 0.018768822 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC        1294 Handshake, SCID=fdf4a419d824f2de
    8 0.018770219 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC         874 Protected Payload (KP0)
    9 0.019555027 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC          83 Handshake, DCID=fdf4a419d824f2de
   10 0.023888055 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC          81 Handshake, DCID=fdf4a419d824f2de
   11 0.029364527 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC          85 Handshake, SCID=fdf4a419d824f2de
   12 0.066062328 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC         127 Handshake, DCID=fdf4a419d824f2de
   13 0.066245452 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC         113 Protected Payload (KP0), DCID=fdf4a419d824f2de
   14 0.066511967 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC          76 Protected Payload (KP0), DCID=fdf4a419d824f2de
   15 0.068000147 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC         916 Protected Payload (KP0), DCID=fdf4a419d824f2de
   16 0.073608828 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC         984 Protected Payload (KP0)
   17 0.073610225 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC         165 Protected Payload (KP0)
   18 0.073969000 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC          78 Protected Payload (KP0), DCID=fdf4a419d824f2de
   19 0.074147934 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC          77 Protected Payload (KP0), DCID=fdf4a419d824f2de
   20 0.074187464 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC          71 Protected Payload (KP0)
   21 0.074344258 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC          77 Protected Payload (KP0), DCID=fdf4a419d824f2de
   22 0.210696482 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC        1290 Protected Payload (KP0)
   23 0.210697879 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC        1294 Protected Payload (KP0)
   24 0.210698856 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC        1294 Protected Payload (KP0)
   25 0.210700253 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC         689 Protected Payload (KP0)
   26 0.210701650 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC         177 Protected Payload (KP0)
   27 0.211318280 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC          81 Protected Payload (KP0), DCID=fdf4a419d824f2de
   28 0.211521867 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC          77 Protected Payload (KP0), DCID=fdf4a419d824f2de
```

   After decryption:



```
No.   Time        Source                                Destination                           Protocol  Length Info
    1 0.000000000 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC        1294 Initial, DCID=3df4a419d824f2de, PKN: 1, PADDING, CRYP
    2 0.007293954 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC        1294 Initial, SCID=fdf4a419d824f2de, PKN: 1, ACK, CRYPTO,
    3 0.012467105 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC        1294 Initial, DCID=fdf4a419d824f2de, PKN: 2, ACK, PADDING
    4 0.013848428 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC        1294 Handshake, SCID=fdf4a419d824f2de, PKN: 3, CRYPTO
    5 0.013850313 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC        1294 Handshake, SCID=fdf4a419d824f2de, PKN: 2, CRYPTO
    6 0.014200219 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC          83 Handshake, DCID=fdf4a419d824f2de, PKN: 3, ACK
    7 0.018768822 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC        1294 Handshake, SCID=fdf4a419d824f2de, PKN: 4, CRYPTO
    8 0.018770219 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  HTTP3        874 Protected Payload (KP0), PKN: 6, STREAM(3), SETTINGS
    9 0.019555027 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC          83 Handshake, DCID=fdf4a419d824f2de, PKN: 4, ACK
   10 0.023888055 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC          81 Handshake, DCID=fdf4a419d824f2de, PKN: 6, PADDING, PI
   11 0.029364527 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC          85 Handshake, SCID=fdf4a419d824f2de, PKN: 7, ACK
   12 0.066062328 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC         127 Handshake, DCID=fdf4a419d824f2de, PKN: 7, CRYPTO
   13 0.066245452 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             HTTP3        113 Protected Payload (KP0), DCID=fdf4a419d824f2de, PKN:
   14 0.066511967 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC          76 Protected Payload (KP0), DCID=fdf4a419d824f2de, PKN:
   15 0.068000147 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             HTTP3        916 Protected Payload (KP0), DCID=fdf4a419d824f2de, PKN:
   16 0.073608828 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC         984 Protected Payload (KP0), PKN: 8, CRYPTO
   17 0.073610225 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC         165 Protected Payload (KP0), PKN: 9, DONE, NT, NCI
   18 0.073969000 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC          78 Protected Payload (KP0), DCID=fdf4a419d824f2de, PKN:
   19 0.074147934 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC          77 Protected Payload (KP0), DCID=fdf4a419d824f2de, PKN:
   20 0.074187464 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  HTTP3         71 Protected Payload (KP0), PKN: 10, ACK, STREAM(7)
   21 0.074344258 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC          77 Protected Payload (KP0), DCID=fdf4a419d824f2de, PKN:
   22 0.210696482 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  HTTP3       1290 Protected Payload (KP0), PKN: 11, STREAM(11), STREAM(
   23 0.210697879 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC        1294 Protected Payload (KP0), PKN: 12, STREAM(0)
   24 0.210698856 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  QUIC        1294 Protected Payload (KP0), PKN: 13, STREAM(0)
   25 0.210700253 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  HTTP3        689 Protected Payload (KP0), PKN: 14, STREAM(0), DATA
   26 0.210701650 lga25s78-in-f4.1e100.net             dark-chocolate-176.dynamic2.rpi.edu  HTTP3        177 Protected Payload (KP0), PKN: 15, STREAM(0), DATA
   27 0.211318280 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             HTTP3         81 Protected Payload (KP0), DCID=fdf4a419d824f2de, PKN:
   28 0.211521867 dark-chocolate-176.dynamic2.rpi.edu  lga25s78-in-f4.1e100.net             QUIC          77 Protected Payload (KP0), DCID=fdf4a419d824f2de, PKN:
```