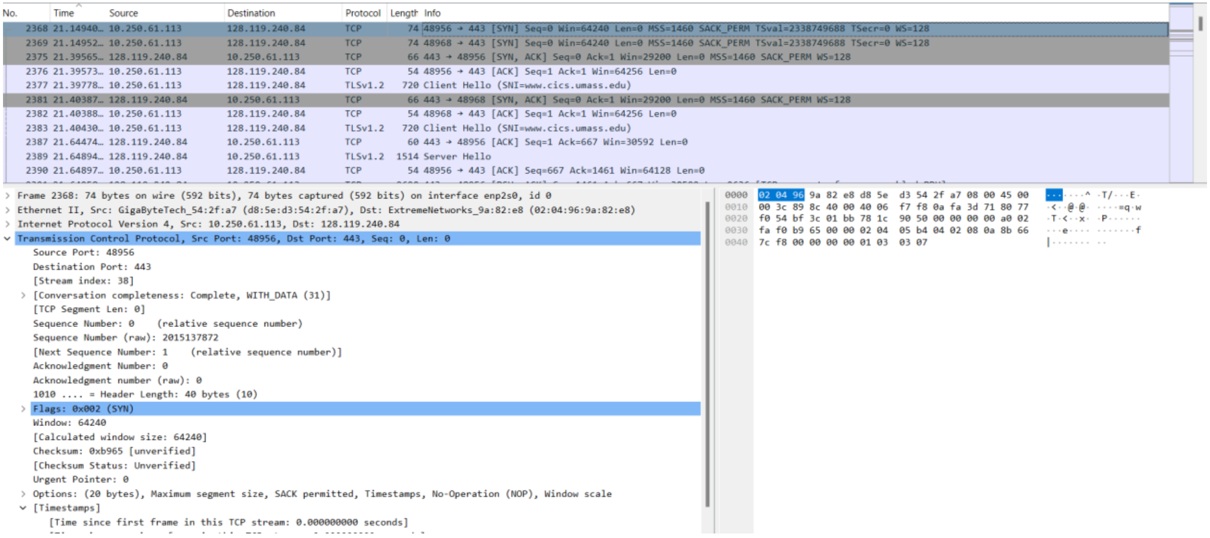
Assignment 13: TLS Protocol

210010020

Part2: A first look at the captured trace

1. What is the packet number in your trace that contains the initial TCP SYN message? (By “packet number,” we meant the number in the “No.” column at the left of the Wireshark display, not the sequence number in the TCP segment itself).

   A] Packet Number 2368



```
No.   Time        Source          Destination     Protocol Length Info
 2368 21.14940…  10.250.61.113   128.119.240.84  TCP        74 48956 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2338749688 TSecr=0 WS=128
 2369 21.14952…  10.250.61.113   128.119.240.84  TCP        74 48968 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2338749688 TSecr=0 WS=128
 2375 21.39565…  128.119.240.84  10.250.61.113   TCP        66 443 → 48956 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
 2376 21.39573…  10.250.61.113   128.119.240.84  TCP        54 48956 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
 2377 21.39778…  10.250.61.113   128.119.240.84  TLSv1.2   720 Client Hello (SNI=www.cics.umass.edu)
 2381 21.40387…  128.119.240.84  10.250.61.113   TCP        66 443 → 48968 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
 2382 21.40388…  10.250.61.113   128.119.240.84  TCP        54 48968 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
 2383 21.40430…  10.250.61.113   128.119.240.84  TLSv1.2   720 Client Hello (SNI=www.cics.umass.edu)
 2387 21.64474…  128.119.240.84  10.250.61.113   TCP        60 443 → 48956 [ACK] Seq=1 Ack=667 Win=30592 Len=0
 2389 21.64894…  128.119.240.84  10.250.61.113   TLSv1.2  1514 Server Hello
 2390 21.64897…  10.250.61.113   128.119.240.84  TCP        54 48956 → 443 [ACK] Seq=667 Ack=1461 Win=64128 Len=0
```

```
> Frame 2368: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface enp2s0, id 0
> Ethernet II, Src: GigaByteTech_54:2f:a7 (d8:5e:d3:54:2f:a7), Dst: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8)
> Internet Protocol Version 4, Src: 10.250.61.113, Dst: 128.119.240.84
v Transmission Control Protocol, Src Port: 48956, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 48956
    Destination Port: 443
    [Stream index: 38]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2015137872
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1010 .... = Header Length: 40 bytes (10)
  > Flags: 0x002 (SYN)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0xb965 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
  v [Timestamps]
      [Time since first frame in this TCP stream: 0.000000000 seconds]
```

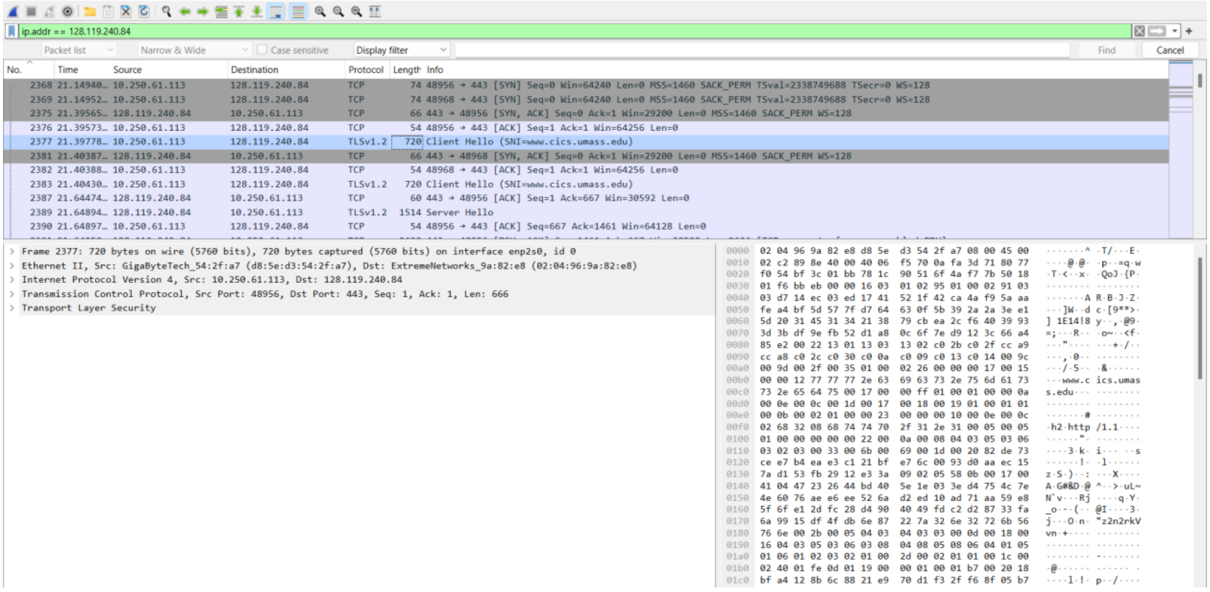
```
0000  02 04 96 9a 82 e8 d8 5e  d3 54 2f a7 08 00 45 00   ·······^ ·T/···E·
0010  00 3c 89 8c 40 00 40 06  f7 f8 0a fa 3d 71 80 77   ·<··@·@· ····=q·w
0020  f0 54 bf 3c 01 bb 78 1c  90 50 00 00 00 00 a0 02   ·T·<··x· ·P······
0030  fa f0 b9 65 00 00 02 04  05 b4 04 02 08 0a 8b 66   ···e···· ·······f
0040  7c f8 00 00 00 00 01 03  03 07                     |······· ··
```

2. Is the TCP connection set up before or after the first TLS message is sent from the client to the server?
   A] first TLS message is sent after the TCP connection is set up between the client and the server.

Part-3: The TLS Handshake: Client Hello message

1. What is the packet number in your trace that contains the TLS Client Hello message?

A] packet 2377.

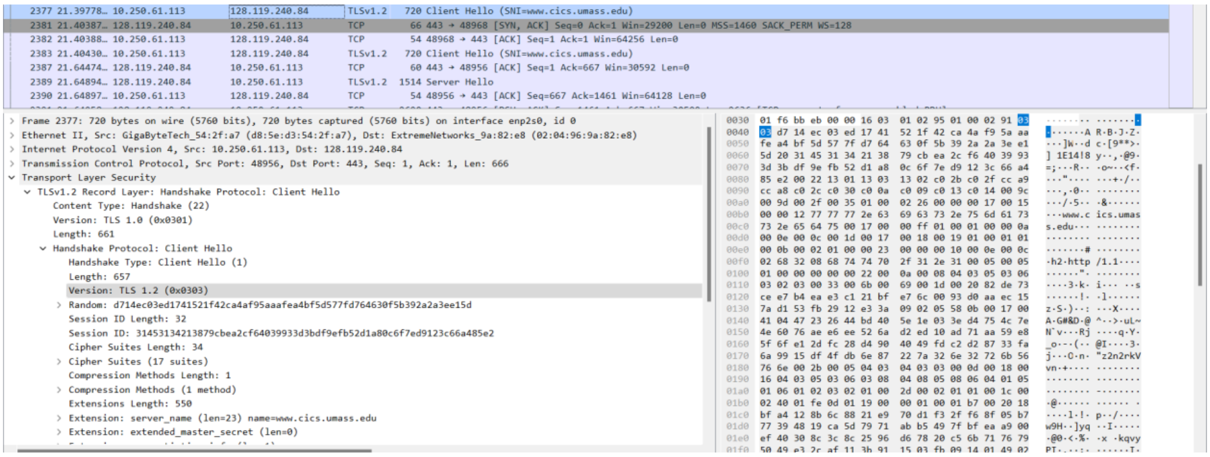


```
ip.addr == 128.119.240.84

No.   Time        Source           Destination      Protocol Length Info
 2368 21.14940… 10.250.61.113    128.119.240.84   TCP        74 48956 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2338749688 TSecr=0 WS=128
 2369 21.14952… 10.250.61.113    128.119.240.84   TCP        74 48968 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2338749688 TSecr=0 WS=128
 2375 21.39565… 128.119.240.84   10.250.61.113    TCP        66 443 → 48956 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
 2376 21.39573… 10.250.61.113    128.119.240.84   TCP        54 48956 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
 2377 21.39778… 10.250.61.113    128.119.240.84   TLSv1.2   720 Client Hello (SNI=www.cics.umass.edu)
 2381 21.40387… 128.119.240.84   10.250.61.113    TCP        66 443 → 48968 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
 2382 21.40388… 10.250.61.113    128.119.240.84   TCP        54 48968 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
 2383 21.40430… 10.250.61.113    128.119.240.84   TLSv1.2   720 Client Hello (SNI=www.cics.umass.edu)
 2387 21.64474… 128.119.240.84   10.250.61.113    TCP        60 443 → 48956 [ACK] Seq=1 Ack=667 Win=30592 Len=0
 2389 21.64894… 128.119.240.84   10.250.61.113    TLSv1.2  1514 Server Hello
 2390 21.64897… 10.250.61.113    128.119.240.84   TCP        54 48956 → 443 [ACK] Seq=667 Ack=1461 Win=64128 Len=0

> Frame 2377: 720 bytes on wire (5760 bits), 720 bytes captured (5760 bits) on interface enp2s0, id 0
> Ethernet II, Src: GigaByteTech_54:2f:a7 (d8:5e:d3:54:2f:a7), Dst: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8)
> Internet Protocol Version 4, Src: 10.250.61.113, Dst: 128.119.240.84
> Transmission Control Protocol, Src Port: 48956, Dst Port: 443, Seq: 1, Ack: 1, Len: 666
> Transport Layer Security

0000  02 04 96 9a 82 e8 d8 5e  d3 54 2f a7 08 00 45 00   ·······^ ·T/···E·
0010  02 c2 89 8e 40 00 40 06  f5 70 0a fa 3d 71 80 77   ····@·@· ·p··=q·w
0020  f0 54 bf 3c 01 bb 78 1c  90 51 6f 4a f7 7b 50 18   ·T·<··x· ·QoJ·{P·
0030  01 f6 bb eb 00 00 16 03  01 02 95 01 00 02 91 03   ········ ········
0040  03 d7 14 ec 03 ed 17 41  52 1f 42 ca 4a f9 5a aa   ·······A R·B·J·Z·
0050  fe a4 bf 5d 57 7f d7 64  63 0f 5b 39 2a 2a 3e e1   ···]W··d c·[9**>·
0060  5d 20 31 45 31 34 21 38  79 cb ea 2c f6 40 39 93   ] 1E14!8 y··,·@9·
0070  3d 3b df 9e fb 52 d1 a8  0c 6f 7e d9 12 3c 66 a4   =;···R·· ·o~··<f·
0080  85 e2 00 22 13 01 13 03  13 02 c0 2b c0 2f cc a9   ···"···· ···+·/··
0090  cc a8 c0 2c c0 30 c0 0a  c0 09 c0 13 c0 14 00 9c   ···,·0·· ········
00a0  00 9d 00 2f 00 35 01 00  02 26 00 00 00 17 00 15   ···/·5·· ·&······
00b0  00 00 12 77 77 77 2e 63  69 63 73 2e 75 6d 61 73   ···www.c ics.umas
00c0  73 2e 65 64 75 00 17 00  00 ff 01 00 01 00 00 0a   s.edu··· ········
00d0  00 0e 00 0c 00 1d 00 17  00 18 00 19 01 00 01 01   ········ ········
00e0  00 0b 00 02 01 00 00 23  00 00 00 10 00 0e 00 0c   ·······# ········
00f0  02 68 32 08 68 74 74 70  2f 31 2e 31 00 05 00 05   ·h2·http /1.1····
0100  01 00 00 00 00 00 22 00  0a 00 08 04 03 05 03 06   ······"· ········
0110  03 02 03 00 33 00 6b 00  69 00 1d 00 20 82 de 73   ····3·k· i··· ··s
0120  ce e7 b4 ea e3 c1 21 bf  e7 6c 00 93 d0 aa ec 15   ······!· ·l······
0130  7a d1 53 fb 29 12 e3 3a  09 02 05 58 0b 00 17 00   z·S·)··: ···X····
0140  41 04 47 23 26 44 bd 40  5e 1e 03 3e d4 75 4c 7e   A·G#&D·@ ^··>·uL~
0150  4e 60 76 ae e6 ee 52 6a  d2 ed 10 ad 71 aa 59 e8   N`v···Rj ····q·Y·
0160  5f 6f e1 2d fc 28 d4 90  40 49 fd c2 d2 87 33 fa   _o·-·(·· @I····3·
0170  6a 99 15 df 4f db 6e 87  22 7a 32 6e 32 72 6b 56   j···O·n· "z2n2rkV
0180  76 6e 00 2b 00 05 04 03  04 03 03 00 0d 00 18 00   vn·+···· ········
0190  16 04 03 05 03 06 03 08  04 08 05 08 06 04 01 05   ········ ········
01a0  01 06 01 02 03 02 01 00  2d 00 02 01 01 00 1c 00   ········ -·······
01b0  02 40 01 fe 0d 01 19 00  00 01 00 01 b7 00 20 18   ·@······ ······ ·
01c0  bf a4 12 8b 6c 88 21 e9  70 d1 f3 2f f6 8f 05 b7   ····l·!· p··/····
```

2. What version of TLS is your client running, as declared in the Client Hello message?

A] TLS version 0x0301.

Inside the handshake field version is 0x0303. This can be seen in the below screenshot.



```
 2377 21.39778… 10.250.61.113    128.119.240.84   TLSv1.2   720 Client Hello (SNI=www.cics.umass.edu)
 2381 21.40387… 128.119.240.84   10.250.61.113    TCP        66 443 → 48968 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
 2382 21.40388… 10.250.61.113    128.119.240.84   TCP        54 48968 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
 2383 21.40430… 10.250.61.113    128.119.240.84   TLSv1.2   720 Client Hello (SNI=www.cics.umass.edu)
 2387 21.64474… 128.119.240.84   10.250.61.113    TCP        60 443 → 48956 [ACK] Seq=1 Ack=667 Win=30592 Len=0
 2389 21.64894… 128.119.240.84   10.250.61.113    TLSv1.2  1514 Server Hello
 2390 21.64897… 10.250.61.113    128.119.240.84   TCP        54 48956 → 443 [ACK] Seq=667 Ack=1461 Win=64128 Len=0

> Frame 2377: 720 bytes on wire (5760 bits), 720 bytes captured (5760 bits) on interface enp2s0, id 0
> Ethernet II, Src: GigaByteTech_54:2f:a7 (d8:5e:d3:54:2f:a7), Dst: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8)
> Internet Protocol Version 4, Src: 10.250.61.113, Dst: 128.119.240.84
> Transmission Control Protocol, Src Port: 48956, Dst Port: 443, Seq: 1, Ack: 1, Len: 666
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 661
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 657
        Version: TLS 1.2 (0x0303)
      > Random: d714ec03ed1741521f42ca4af95aaafea4bf5d577fd764630f5b392a2a3ee15d
        Session ID Length: 32
        Session ID: 31453134213879cbea2cf64039933d3bdf9efb52d1a80c6f7ed9123c66a485e2
        Cipher Suites Length: 34
      > Cipher Suites (17 suites)
        Compression Methods Length: 1
      > Compression Methods (1 method)
        Extensions Length: 550
      > Extension: server_name (len=23) name=www.cics.umass.edu
      > Extension: extended_master_secret (len=0)

0030  01 f6 bb eb 00 00 16 03  01 02 95 01 00 02 91 03   ········ ········
0040  03 d7 14 ec 03 ed 17 41  52 1f 42 ca 4a f9 5a aa   ·······A R·B·J·Z·
0050  fe a4 bf 5d 57 7f d7 64  63 0f 5b 39 2a 2a 3e e1   ···]W··d c·[9**>·
0060  5d 20 31 45 31 34 21 38  79 cb ea 2c f6 40 39 93   ] 1E14!8 y··,·@9·
0070  3d 3b df 9e fb 52 d1 a8  0c 6f 7e d9 12 3c 66 a4   =;···R·· ·o~··<f·
0080  85 e2 00 22 13 01 13 03  13 02 c0 2b c0 2f cc a9   ···"···· ···+·/··
0090  cc a8 c0 2c c0 30 c0 0a  c0 09 c0 13 c0 14 00 9c   ···,·0·· ········
00a0  00 9d 00 2f 00 35 01 00  02 26 00 00 00 17 00 15   ···/·5·· ·&······
00b0  00 00 12 77 77 77 2e 63  69 63 73 2e 75 6d 61 73   ···www.c ics.umas
00c0  73 2e 65 64 75 00 17 00  00 ff 01 00 01 00 00 0a   s.edu··· ········
00d0  00 0e 00 0c 00 1d 00 17  00 18 00 19 01 00 01 01   ········ ········
00e0  00 0b 00 02 01 00 00 23  00 00 00 10 00 0e 00 0c   ·······# ········
00f0  02 68 32 08 68 74 74 70  2f 31 2e 31 00 05 00 05   ·h2·http /1.1····
0100  01 00 00 00 00 00 22 00  0a 00 08 04 03 05 03 06   ······"· ········
0110  03 02 03 00 33 00 6b 00  69 00 1d 00 20 82 de 73   ····3·k· i··· ··s
0120  ce e7 b4 ea e3 c1 21 bf  e7 6c 00 93 d0 aa ec 15   ······!· ·l······
0130  7a d1 53 fb 29 12 e3 3a  09 02 05 58 0b 00 17 00   z·S·)··: ···X····
0140  41 04 47 23 26 44 bd 40  5e 1e 03 3e d4 75 4c 7e   A·G#&D·@ ^··>·uL~
0150  4e 60 76 ae e6 ee 52 6a  d2 ed 10 ad 71 aa 59 e8   N`v···Rj ····q·Y·
0160  5f 6f e1 2d fc 28 d4 90  40 49 fd c2 d2 87 33 fa   _o·-·(·· @I····3·
0170  6a 99 15 df 4f db 6e 87  22 7a 32 6e 32 72 6b 56   j···O·n· "z2n2rkV
0180  76 6e 00 2b 00 05 04 03  04 03 03 00 0d 00 18 00   vn·+···· ········
0190  16 04 03 05 03 06 03 08  04 08 05 08 06 04 01 05   ········ ········
01a0  01 06 01 02 03 02 01 00  2d 00 02 01 01 00 1c 00   ········ -·······
01b0  02 40 01 fe 0d 01 19 00  00 01 00 01 b7 00 20 18   ·@······ ······ ·
01c0  bf a4 12 8b 6c 88 21 e9  70 d1 f3 2f f6 8f 05 b7   ····l·!· p··/····
01d0  77 39 48 19 ca 5d 79 71  ab b5 49 7f bf ea a9 00   w9H··]yq ··I·····
01e0  ef 40 30 8c 3c 8c 25 96  d6 78 20 c5 6b 71 76 79   ·@0·<·%· ·x ·kqvy
01f0  50 49 e3 2c af 11 3b 91  15 03 fb 09 14 01 49 02   PI·,··;· ······I·
```

3. How many cipher suites are supported by your client, as declared in the Client Hello message? A cipher suite is a set of related cryptographic algorithms that determine how session keys will be derived, and hoid-at-commonName=www.cs.umass.edua HMAC algorithm.

A] As seen in the above figure total of 17 cipher suites can be generated.

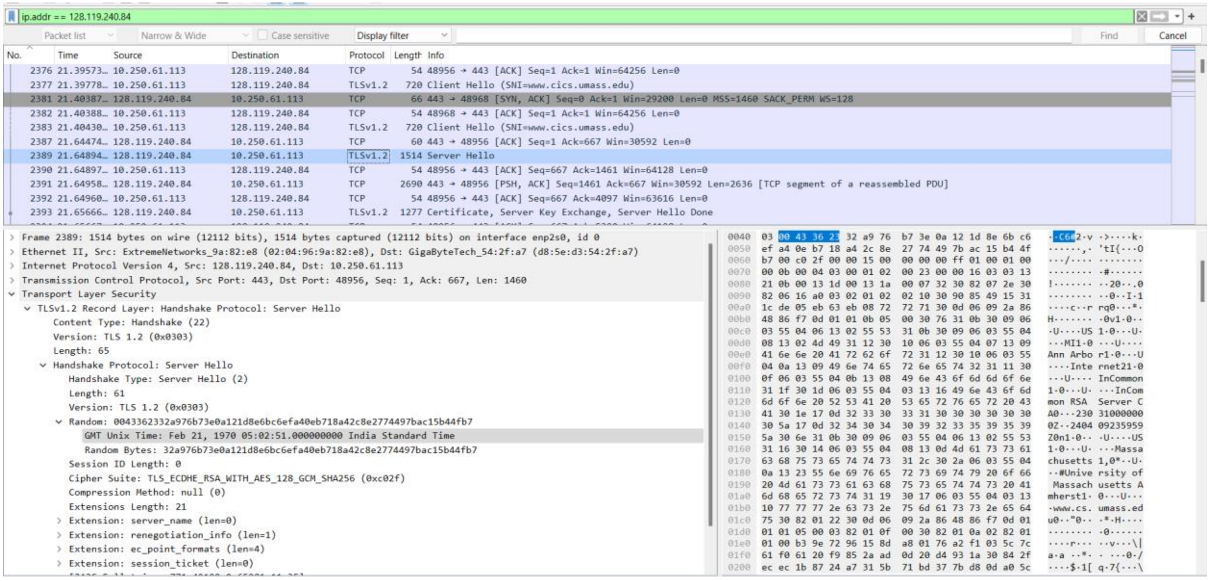
4. Your client generates and sends a string of "random bytes" to the server in the Client Hello message. What are the first two hexadecimal digits in the random bytes field of the Client Hello message? Enter the two hexadecimal digits (without spaces between the hex digits and without any leading '0x', using lowercase letters where needed). Hint: be careful to fully dig into the Random field to find the Random Bytes subfield (do not consider the GMT UNIX Time subfield of Random).
A] The first two digits are the timestamp values **d7**

5. What is the purpose(s) of the "random bytes" field in the Client Hello message? Note: you'll have to do some searching and reading to get the answer to this question; see section 8.6 and in RFC 5246 (section 8.1 in RFC 5246 in particular).
A] Helps to distinguish HELLO messages sent between two different clients, to the server. Thus making it unique. The purpose of the client random is to:

- Ensure that each handshake is unique by including a random value.
- Contribute to the generation of session keys for symmetric encryption after the handshake is complete.

Part-4: The TLS Handshake: Server Hello message

1. What is the packet number in your trace that contains the TLS Server Hello message?
A] Packet No. 2389



ip.addr == 128.119.240.84

```
No.   Time         Source           Destination      Protocol Length Info
 2376 21.39573…   10.250.61.113    128.119.240.84   TCP        54 48956 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
 2377 21.39778…   10.250.61.113    128.119.240.84   TLSv1.2   720 Client Hello (SNI=www.cics.umass.edu)
 2381 21.40387…   128.119.240.84   10.250.61.113    TCP        66 443 → 48968 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
 2382 21.40388…   10.250.61.113    128.119.240.84   TCP        54 48968 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
 2383 21.40430…   10.250.61.113    128.119.240.84   TLSv1.2   720 Client Hello (SNI=www.cics.umass.edu)
 2387 21.64474…   128.119.240.84   10.250.61.113    TCP        60 443 → 48956 [ACK] Seq=1 Ack=667 Win=30592 Len=0
 2389 21.64894…   128.119.240.84   10.250.61.113    TLSv1.2  1514 Server Hello
 2390 21.64897…   10.250.61.113    128.119.240.84   TCP        54 48956 → 443 [ACK] Seq=667 Ack=1461 Win=64128 Len=0
 2391 21.64958…   128.119.240.84   10.250.61.113    TCP      2690 443 → 48956 [PSH, ACK] Seq=1461 Ack=667 Win=30592 Len=2636 [TCP segment of a reassembled PDU]
 2392 21.64960…   10.250.61.113    128.119.240.84   TCP        54 48956 → 443 [ACK] Seq=667 Ack=4097 Win=63616 Len=0
 2393 21.65666…   128.119.240.84   10.250.61.113    TLSv1.2  1277 Certificate, Server Key Exchange, Server Hello Done
```

```
> Frame 2389: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface enp2s0, id 0
> Ethernet II, Src: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8), Dst: GigaByteTech_54:2f:a7 (d8:5e:d3:54:2f:a7)
> Internet Protocol Version 4, Src: 128.119.240.84, Dst: 10.250.61.113
> Transmission Control Protocol, Src Port: 443, Dst Port: 48956, Seq: 1, Ack: 667, Len: 1460
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 65
    v Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 61
        Version: TLS 1.2 (0x0303)
      v Random: 0043362332a976b73e0a121d8e6bc6efa40eb718a42c8e2774497bac15b44fb7
          GMT Unix Time: Feb 21, 1970 05:02:51.000000000 India Standard Time
          Random Bytes: 32a976b73e0a121d8e6bc6efa40eb718a42c8e2774497bac15b44fb7
        Session ID Length: 0
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
        Compression Method: null (0)
        Extensions Length: 21
      > Extension: server_name (len=0)
      > Extension: renegotiation_info (len=1)
      > Extension: ec_point_formats (len=4)
      > Extension: session_ticket (len=0)
```

```
0040  03 00 43 36 23 32 a9 76  b7 3e 0a 12 1d 8e 6b c6   ··C6#2·v ·>····k·
0050  ef a4 0e b7 18 a4 2c 8e  27 74 49 7b ac 15 b4 4f   ······,· 'tI{···O
0060  b7 00 c0 2f 00 00 15 00  00 00 00 ff 01 00 01 00   ···/···· ········
0070  00 0b 00 04 03 00 01 02  00 23 00 00 16 03 03 13   ········ ·#······
0080  21 0b 00 13 1d 00 13 1a  00 07 32 30 82 07 2e 30   !······· ··20··.0
0090  82 06 16 a0 03 02 01 02  02 10 30 90 85 49 15 31   ········ ··0··I·1
00a0  1c de 05 eb 63 eb 08 72  72 71 30 0d 06 09 2a 86   ····c··r rq0···*·
00b0  48 86 f7 0d 01 01 0b 05  00 30 76 31 0b 30 09 06   H······· ·0v1·0··
00c0  03 55 04 06 13 02 55 53  31 0b 30 09 06 03 55 04   ·U····US 1·0···U·
00d0  08 13 02 4d 49 31 12 30  10 06 03 55 04 07 13 09   ···MI1·0 ···U····
00e0  41 6e 6e 20 41 72 62 6f  72 31 12 30 10 06 03 55   Ann Arbo r1·0···U
00f0  04 0a 13 09 49 6e 74 65  72 6e 65 74 32 31 11 30   ····Inte rnet21·0
0100  0f 06 03 55 04 0b 13 08  49 6e 43 6f 6d 6d 6f 6e   ···U···· InCommon
0110  31 1f 30 1d 06 03 55 04  03 13 16 49 6e 43 6f 6d   1·0···U· ···InCom
0120  6d 6f 6e 20 52 53 41 20  53 65 72 76 65 72 20 43   mon RSA  Server C
0130  41 30 1e 17 0d 32 33 30  33 31 30 30 30 30 30 30   A0···230 31000000
0140  30 5a 17 0d 32 34 30 34  30 39 32 33 35 39 35 39   0Z··2404 09235959
0150  5a 30 6e 31 0b 30 09 06  03 55 04 06 13 02 55 53   Z0n1·0·· ·U····US
0160  31 16 30 14 06 03 55 04  08 13 0d 4d 61 73 73 61   1·0···U· ···Massa
0170  63 68 75 73 65 74 74 73  31 2c 30 2a 06 03 55 04   chusetts 1,0*··U·
0180  0a 13 23 55 6e 69 76 65  72 73 69 74 79 20 6f 66   ··#Unive rsity of
0190  20 4d 61 73 73 61 63 68  75 73 65 74 74 73 20 41    Massach usetts A
01a0  6d 68 65 72 73 74 31 19  30 17 06 03 55 04 03 13   mherst1· 0···U···
01b0  10 77 77 77 2e 63 73 2e  75 6d 61 73 73 2e 65 64   ·www.cs. umass.ed
01c0  75 30 82 01 22 30 0d 06  09 2a 86 48 86 f7 0d 01   u0··"0·· ·*·H····
01d0  01 01 05 00 03 82 01 0f  00 30 82 01 0a 02 82 01   ········ ·0······
01e0  01 00 b3 9e 72 96 15 8d  a8 01 76 a2 f1 03 5c 7c   ····r··· ··v···\|
01f0  61 f0 61 20 f9 85 2a ad  0d 20 d4 93 1a 30 84 2f   a·a ··*· · ···0·/
0200  ec ec 1b 87 24 a7 31 5b  71 bd 37 7b d8 0d a0 5c   ····$·1[ q·7{···\
```

2. Which cipher suite has been chosen by the server from among those offered in the earlier Client Hello message?
A] From the available cipher suites the server has chosen
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

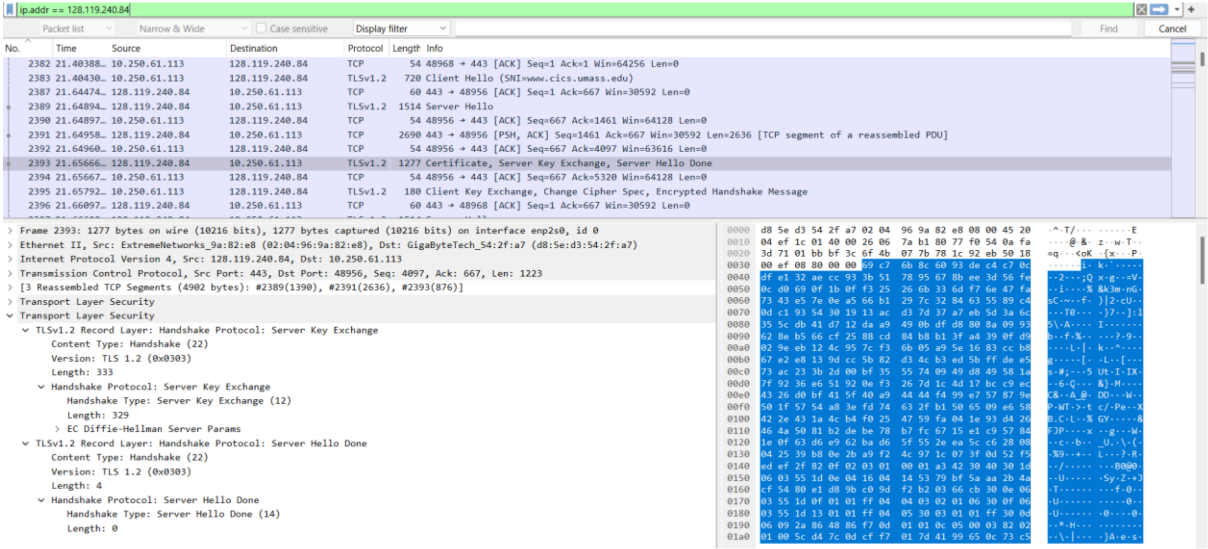
3. Does the Server Hello message contain random bytes, similar to how the Client Hello message contains random bytes? And if so, what is/are their purpose(s)?

A] Yes, similar to client the server also contains random bytes. The server random serves the following purposes:

- Distinguishes different handshakes, preventing replay attacks.
- Contributes to session key generation for symmetric encryption.

4. What is the packet number in your trace for the TLS message part that contains the public key certificate for the www.cics.umass.edu server (actually the www.cs.umass.edu server)?

A]



```
ip.addr == 128.119.240.84
```

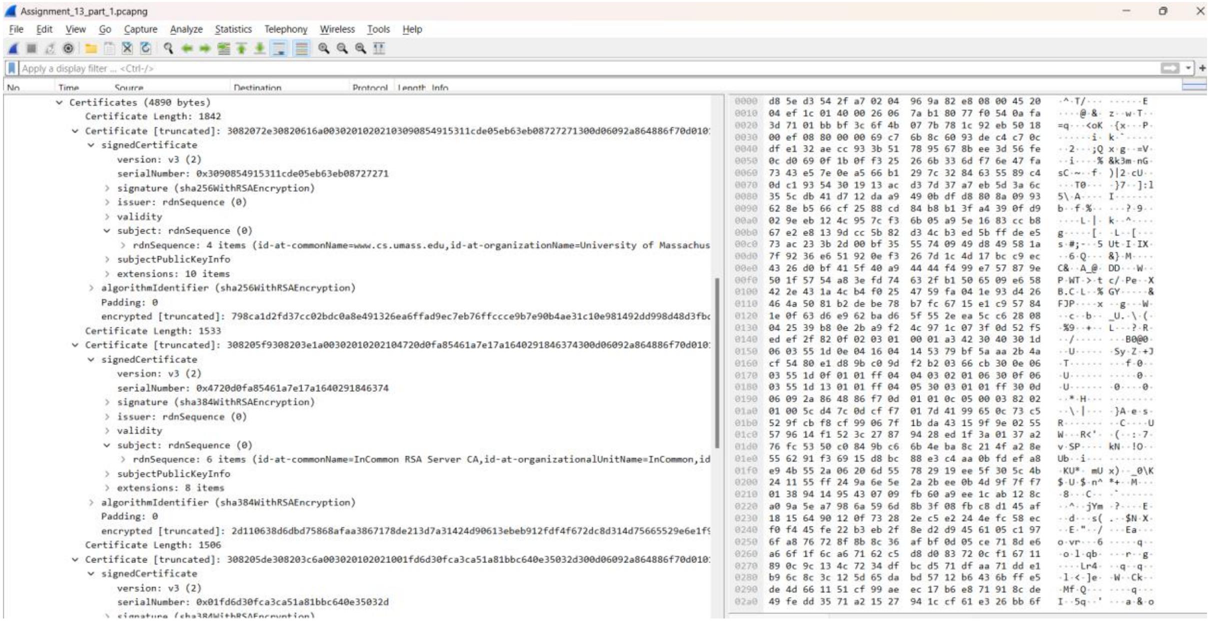
```
No.   Time        Source          Destination     Protocol Length Info
 2382 21.40388… 10.250.61.113   128.119.240.84  TCP        54 48968 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
 2383 21.40430… 10.250.61.113   128.119.240.84  TLSv1.2   720 Client Hello (SNI=www.cics.umass.edu)
 2387 21.64474… 128.119.240.84  10.250.61.113   TCP        60 443 → 48956 [ACK] Seq=1 Ack=667 Win=30592 Len=0
 2389 21.64894… 128.119.240.84  10.250.61.113   TLSv1.2  1514 Server Hello
 2390 21.64897… 10.250.61.113   128.119.240.84  TCP        54 48956 → 443 [ACK] Seq=667 Ack=1461 Win=64128 Len=0
 2391 21.64958… 128.119.240.84  10.250.61.113   TCP      2690 443 → 48956 [PSH, ACK] Seq=1461 Ack=667 Win=30592 Len=2636 [TCP segment of a reassembled PDU]
 2392 21.64960… 10.250.61.113   128.119.240.84  TCP        54 48956 → 443 [ACK] Seq=667 Ack=4097 Win=63616 Len=0
 2393 21.65666… 128.119.240.84  10.250.61.113   TLSv1.2  1277 Certificate, Server Key Exchange, Server Hello Done
 2394 21.65667… 10.250.61.113   128.119.240.84  TCP        54 48956 → 443 [ACK] Seq=667 Ack=5320 Win=64128 Len=0
 2395 21.65792… 10.250.61.113   128.119.240.84  TLSv1.2   180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 2396 21.66097… 128.119.240.84  10.250.61.113   TCP        60 443 → 48968 [ACK] Seq=1 Ack=667 Win=30592 Len=0
```

```
> Frame 2393: 1277 bytes on wire (10216 bits), 1277 bytes captured (10216 bits) on interface enp2s0, id 0
> Ethernet II, Src: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8), Dst: GigaByteTech_54:2f:a7 (d8:5e:d3:54:2f:a7)
> Internet Protocol Version 4, Src: 128.119.240.84, Dst: 10.250.61.113
> Transmission Control Protocol, Src Port: 443, Dst Port: 48956, Seq: 4097, Ack: 667, Len: 1223
> [3 Reassembled TCP Segments (4902 bytes): #2389(1390), #2391(2636), #2393(876)]
> Transport Layer Security
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 333
    v Handshake Protocol: Server Key Exchange
        Handshake Type: Server Key Exchange (12)
        Length: 329
      > EC Diffie-Hellman Server Params
  v TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 4
    v Handshake Protocol: Server Hello Done
        Handshake Type: Server Hello Done (14)
        Length: 0
```

```
0000  d8 5e d3 54 2f a7 02 04  96 9a 82 e8 08 00 45 20   ·^·T/··· ······E
0010  04 ef 1c 01 40 00 26 06  7a b1 80 77 f0 54 0a fa   ····@·&· z··w·T··
0020  3d 71 01 bb bf 3c 6f 4b  07 7b 78 1c 92 eb 50 18   =q···<oK ·{x···P·
0030  00 ef 08 80 00 00 69 c7  6b 8c 60 93 de c4 c7 0c   ······i· k·`·····
0040  df e1 32 ae cc 93 3b 51  78 95 67 8b ee 3d 56 fe   ··2···;Q x·g··=V·
0050  0c d0 69 0f 1b 0f f3 25  26 6b 33 6d f7 6e 47 fa   ··i····% &k3m·nG·
0060  73 43 e5 7e 0e a5 66 b1  29 7c 32 84 63 55 89 c4   sC·~··f· )|2·cU··
0070  0d c1 93 54 30 19 13 ac  d3 7d 37 a7 eb 5d 3a 6c   ···T0··· ·}7··]:l
0080  35 5c db 41 d7 12 da a9  49 0b df d8 80 8a 09 93   5\·A···· I·······
0090  62 8e b5 66 cf 25 88 cd  84 b8 b1 3f a4 39 0f d9   b··f·%·· ···?·9··
00a0  02 9e eb 12 4c 95 7c f3  6b 05 a9 5e 16 83 cc b8   ····L·|· k··^····
00b0  67 e2 e8 13 9d cc 5b 82  d3 4c b3 ed 5b ff de e5   g·····[· ·L··[···
00c0  73 ac 23 3b 2d 00 bf 35  55 74 09 49 d8 49 58 1a   s·#;-··5 Ut·I·IX·
00d0  7f 92 36 e6 51 92 0e f3  26 7d 1c 4d 17 bc c9 ec   ··6·Q··· &}·M····
00e0  43 26 d0 bf 41 5f 40 a9  44 44 f4 99 e7 57 87 9e   C&··A_@· DD···W··
00f0  50 1f 57 54 a8 3e fd 74  63 2f b1 50 65 09 e6 58   P·WT·>·t c/·Pe··X
0100  42 2e 43 1a 4c b4 f0 25  47 59 fa 04 1e 93 d4 26   B.C·L··% GY·····&
0110  46 4a 50 81 b2 de be 78  b7 fc 67 15 e1 c9 57 84   FJP····x ··g···W·
0120  1e 0f 63 d6 e9 62 ba d6  5f 55 2e ea 5c c6 28 08   ··c··b·· _U.·\·(·
0130  04 25 39 b8 0e 2b a9 f2  4c 97 1c 07 3f 0d 52 f5   ·%9··+·· L···?·R·
0140  ed ef 2f 82 0f 02 03 01  00 01 a3 42 30 40 30 1d   ··/····· ···B0@0·
0150  06 03 55 1d 0e 04 16 04  14 53 79 bf 5a aa 2b 4a   ··U····· ·Sy·Z·+J
0160  cf 54 80 e1 d8 9b c0 9d  f2 b2 03 66 cb 30 0e 06   ·T······ ···f·0··
0170  03 55 1d 0f 01 01 ff 04  04 03 02 01 06 30 0f 06   ·U······ ·····0··
0180  03 55 1d 13 01 01 ff 04  05 30 03 01 01 ff 30 0d   ·U······ ·0····0·
0190  06 09 2a 86 48 86 f7 0d  01 01 0c 05 00 03 82 02   ··*·H··· ········
01a0  01 00 5c d4 7c 0d cf f7  01 7d 41 99 65 0c 73 c5   ··\·|··· ·}A·e·s·
```

5. A server may return more than one certificate. If more than one certificate is returned, are all of these certificates for www.cs.umass.edu? If not all are for www.cs.umass.edu, then who are these other certificates for? You can determine who the certificate is for by checking the id-at-common Name field in the returned certificate.

A] Total 3 certificates are returned in Packet 2393



Assignment_13_part_1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
No. Time Source Destination Protocol Length Info

```
v Certificates (4890 bytes)
    Certificate Length: 1842
  v Certificate [truncated]: 3082072e30820616a00302010202103090854915311cde05eb63eb08727271300d06092a864886f70d010
    v signedCertificate
        version: v3 (2)
        serialNumber: 0x3090854915311cde05eb63eb08727271
      > signature (sha256WithRSAEncryption)
      > issuer: rdnSequence (0)
      > validity
      v subject: rdnSequence (0)
        > rdnSequence: 4 items (id-at-commonName=www.cs.umass.edu,id-at-organizationName=University of Massachus
      > subjectPublicKeyInfo
      > extensions: 10 items
    > algorithmIdentifier (sha256WithRSAEncryption)
      Padding: 0
      encrypted [truncated]: 798ca1d2fd37cc02bdc0a8e491326ea6ffad9ec7eb76ffccce9b7e90b4ae31c10e981492dd998d48d3fbc
    Certificate Length: 1533
  v Certificate [truncated]: 308205f9308203e1a00302010202104720d0fa85461a7e17a1640291846374300d06092a864886f70d010
    v signedCertificate
        version: v3 (2)
        serialNumber: 0x4720d0fa85461a7e17a1640291846374
      > signature (sha384WithRSAEncryption)
      > issuer: rdnSequence (0)
      > validity
      v subject: rdnSequence (0)
        > rdnSequence: 6 items (id-at-commonName=InCommon RSA Server CA,id-at-organizationalUnitName=InCommon,id
      > subjectPublicKeyInfo
      > extensions: 8 items
    > algorithmIdentifier (sha384WithRSAEncryption)
      Padding: 0
      encrypted [truncated]: 2d110638d6dbd75868afaa3867178de213d7a31424d90613ebeb912fdf4f672dc8d314d75665529e6e1f
    Certificate Length: 1506
  v Certificate [truncated]: 308205de308203c6a003020102021001fd6d30fca3ca51a81bbc640e35032d300d06092a864886f70d010
    v signedCertificate
        version: v3 (2)
        serialNumber: 0x01fd6d30fca3ca51a81bbc640e35032d
      > signature (sha384WithRSAEncryption)
```

```
0000  d8 5e d3 54 2f a7 02 04  96 9a 82 e8 08 00 45 20   ·^·T/··· ······E
0010  04 ef 1c 01 40 00 26 06  7a b1 80 77 f0 54 0a fa   ····@·&· z··w·T··
0020  3d 71 01 bb bf 3c 6f 4b  07 7b 78 1c 92 eb 50 18   =q···<oK ·{x···P·
0030  00 ef 08 80 00 00 69 c7  6b 8c 60 93 de c4 c7 0c   ······i· k·`·····
0040  df e1 32 ae cc 93 3b 51  78 95 67 8b ee 3d 56 fe   ··2···;Q x·g··=V·
0050  0c d0 69 0f 1b 0f f3 25  26 6b 33 6d f7 6e 47 fa   ··i····% &k3m·nG·
0060  73 43 e5 7e 0e a5 66 b1  29 7c 32 84 63 55 89 c4   sC·~··f· )|2·cU··
0070  0d c1 93 54 30 19 13 ac  d3 7d 37 a7 eb 5d 3a 6c   ···T0··· ·}7··]:l
0080  35 5c db 41 d7 12 da a9  49 0b df d8 80 8a 09 93   5\·A···· I·······
0090  62 8e b5 66 cf 25 88 cd  84 b8 b1 3f a4 39 0f d9   b··f·%·· ···?·9··
00a0  02 9e eb 12 4c 95 7c f3  6b 05 a9 5e 16 83 cc b8   ····L·|· k··^····
00b0  67 e2 e8 13 9d cc 5b 82  d3 4c b3 ed 5b ff de e5   g·····[· ·L··[···
00c0  73 ac 23 3b 2d 00 bf 35  55 74 09 49 d8 49 58 1a   s·#;-··5 Ut·I·IX·
00d0  7f 92 36 e6 51 92 0e f3  26 7d 1c 4d 17 bc c9 ec   ··6·Q··· &}·M····
00e0  43 26 d0 bf 41 5f 40 a9  44 44 f4 99 e7 57 87 9e   C&··A_@· DD···W··
00f0  50 1f 57 54 a8 3e fd 74  63 2f b1 50 65 09 e6 58   P·WT·>·t c/·Pe··X
0100  42 2e 43 1a 4c b4 f0 25  47 59 fa 04 1e 93 d4 26   B.C·L··% GY·····&
0110  46 4a 50 81 b2 de be 78  b7 fc 67 15 e1 c9 57 84   FJP····x ··g···W·
0120  1e 0f 63 d6 e9 62 ba d6  5f 55 2e ea 5c c6 28 08   ··c··b·· _U.·\·(·
0130  04 25 39 b8 0e 2b a9 f2  4c 97 1c 07 3f 0d 52 f5   ·%9··+·· L···?·R·
0140  ed ef 2f 82 0f 02 03 01  00 01 a3 42 30 40 30 1d   ··/····· ···B0@0·
0150  06 03 55 1d 0e 04 16 04  14 53 79 bf 5a aa 2b 4a   ··U····· ·Sy·Z·+J
0160  cf 54 80 e1 d8 9b c0 9d  f2 b2 03 66 cb 30 0e 06   ·T······ ···f·0··
0170  03 55 1d 0f 01 01 ff 04  04 03 02 01 06 30 0f 06   ·U······ ·····0··
0180  03 55 1d 13 01 01 ff 04  05 30 03 01 01 ff 30 0d   ·U······ ·0····0·
0190  06 09 2a 86 48 86 f7 0d  01 01 0c 05 00 03 82 02   ··*·H··· ········
01a0  01 00 5c d4 7c 0d cf f7  01 7d 41 99 65 0c 73 c5   ··\·|··· ·}A·e·s·
01b0  52 9f cb f8 cf 99 06 7f  1b da 43 15 9f 9e 02 55   R······· ··C····U
01c0  57 96 14 f1 52 3c 27 87  94 28 ed 1f 3a 01 37 a2   W···R<'· ·(··:·7·
01d0  76 fc 53 50 c0 84 9b c6  6b 4e ba 8c 21 4f a2 8e   v·SP···· kN··!O··
01e0  55 62 91 f3 69 15 d8 bc  88 e3 c4 aa 0b fd ef a8   Ub··i··· ········
01f0  e9 4b 55 2a 06 20 6d 55  78 29 19 ee 5f 30 5c 4b   ·KU*· mU x)··_0\K
0200  24 11 55 ff 24 9a 6e 5e  2a 2b ee 0b 4d 9f 7f f7   $·U·$·n^ *+··M···
0210  01 38 94 14 95 43 07 09  fb 60 a9 ee 1c ab 12 8c   ·8···C·· ·`······
0220  a0 9a 5e a7 98 6a 59 6d  8b 3f 08 fb c8 d1 45 af   ··^··jYm ·?····E·
0230  18 15 64 90 12 0f 73 28  2e c5 e2 24 4e fc 58 ec   ··d···s( .··$N·X·
0240  f0 f4 45 fe 22 b3 eb 2f  8e d2 d9 45 61 05 c1 97   ··E·"··/ ···Ea···
0250  6f a8 76 72 8f 8b 8c 36  af bf 0d 05 ce 71 8d e6   o·vr···6 ·····q··
0260  a6 6f 1f 6c a6 71 62 c5  d8 d0 83 72 0c f1 67 11   ·o·l·qb· ···r··g·
0270  89 0c 9c 13 4c 72 34 df  bc d5 71 df aa 71 dd e1   ····Lr4· ··q··q··
0280  b9 6c 8c 3c 12 5d 65 da  bd 57 12 b6 43 6b ff e5   ·l·<·]e· ·W··Ck··
0290  de 4d 66 11 51 cf 99 ae  ec 17 b6 e8 71 91 8c de   ·Mf·Q··· ····q···
02a0  49 fe dd 35 71 a2 15 27  94 1c cf 61 e3 26 bb 6f   I··5q··' ···a·&·o
```

Not all of them are for cs.umass.edu but for higher authorities that are manage authenticate certification for digital signatures.

6. What is the name of the certification authority that issued the certificate for id-at-commonName=www.cs.umass.edu?
A] InCommon RSA Server CA

7. What digital signature algorithm is used by the CA to sign this certificate? Hint: this information can be found in the signature subfield of the SignedCertificate field of the certificate for www.cs.umass.edu.
A] signature algorithm used by CA authority has used sha256WithRSAEncryption.

8. Let's take a look at what a real public key looks like! What are the first four hexadecimal digits of the modulus of the public key being used by www.cics.umass.edu? Enter the four hexadecimal digits (without spaces between the hex digits and without any leading '0x' , using lowercase letters where needed, and including any leading 0s after '0x'). Hint: this information can be found in subjectPublicKeyInfo subfield of the SignedCertificate field of the certificate for www.cs.umass.edu.
A] 00b3

9. What is the packet number in your trace for the TLS message part that contains the Server Hello Done TLS record?
A] Packet 2393

Part-5: The TLS Handshake: wrapping up the handshake

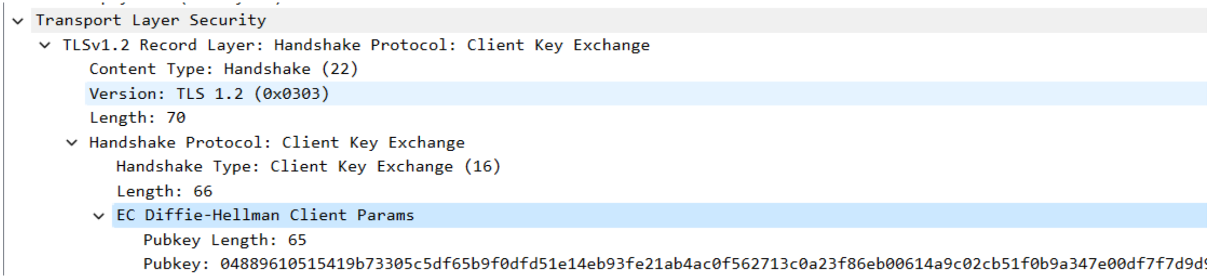
1. What is the packet number in your trace for the TLS message that contains the public key information, Change Cipher Spec, and Encrypted Handshake message, being sent from client to server?
A] Packet 2395

2. Does the client provide its own CA-signed public key certificate back to the server? If so, what is the packet number in your trace containing your client's certificate?
A] No

Part-6: Application data

1. What symmetric key cryptography algorithm is being used by the client and server to encrypt application data (in this case, HTTP messages)?

A] EF Diffie-Hellman as shown below

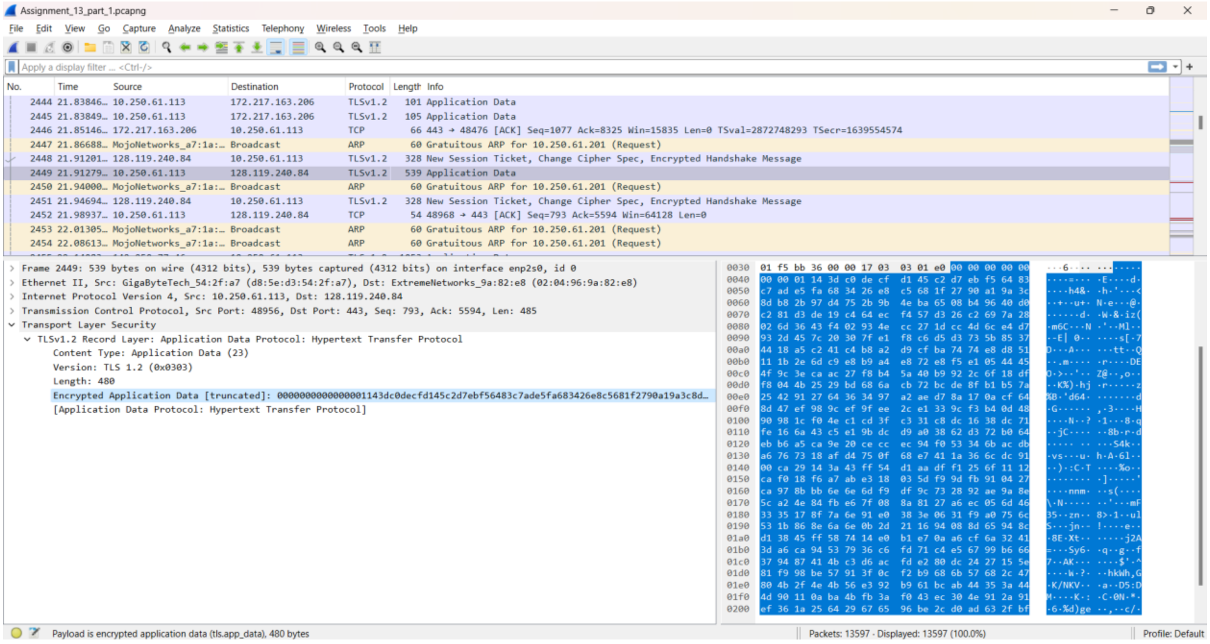


```
⌄ Transport Layer Security
  ⌄ TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 70
    ⌄ Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 66
      ⌄ EC Diffie-Hellman Client Params
          Pubkey Length: 65
          Pubkey: 04889610515419b73305c5df65b9f0dfd51e14eb93fe21ab4ac0f562713c0a23f86eb00614a9c02cb51f0b9a347e00df7f7d9d
```

2. In which of the TLS messages is this symmetric key cryptography algorithm finally decided and declared?
   A] In server hello done packet, packet 2393.

3. What is the packet number in your trace for the first encrypted message carrying application data from client to server?
   A] packet 2449.

4. What do you think the content of this encrypted application data is, given that this trace was generated by fetching the homepage of www.cics.umass.edu?
   A] HTTP GET request is encrypted below



Assignment_13_part_1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source                Destination      Protocol  Length Info
 2444 21.83846… 10.250.61.113         172.217.163.206  TLSv1.2   101 Application Data
 2445 21.83849… 10.250.61.113         172.217.163.206  TLSv1.2   105 Application Data
 2446 21.85146… 172.217.163.206       10.250.61.113    TCP        66 443 → 48476 [ACK] Seq=1077 Ack=8325 Win=15835 Len=0 TSval=2872748293 TSecr=1639554574
 2447 21.86688… MojoNetworks_a7:1a:… Broadcast        ARP        60 Gratuitous ARP for 10.250.61.201 (Request)
 2448 21.91201… 128.119.240.84        10.250.61.113    TLSv1.2   328 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
 2449 21.91279… 10.250.61.113         128.119.240.84   TLSv1.2   539 Application Data
 2450 21.94000… MojoNetworks_a7:1a:… Broadcast        ARP        60 Gratuitous ARP for 10.250.61.201 (Request)
 2451 21.94694… 128.119.240.84        10.250.61.113    TLSv1.2   328 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
 2452 21.98937… 10.250.61.113         128.119.240.84   TCP        54 48968 → 443 [ACK] Seq=793 Ack=5594 Win=64128 Len=0
 2453 22.01305… MojoNetworks_a7:1a:… Broadcast        ARP        60 Gratuitous ARP for 10.250.61.201 (Request)
 2454 22.08613… MojoNetworks_a7:1a:… Broadcast        ARP        60 Gratuitous ARP for 10.250.61.201 (Request)
```

```
> Frame 2449: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits) on interface enp2s0, id 0
> Ethernet II, Src: GigaByteTech_54:2f:a7 (d8:5e:d3:54:2f:a7), Dst: ExtremeNetworks_9a:82:e8 (02:04:96:9a:82:e8)
> Internet Protocol Version 4, Src: 10.250.61.113, Dst: 128.119.240.84
> Transmission Control Protocol, Src Port: 48956, Dst Port: 443, Seq: 793, Ack: 5594, Len: 485
⌄ Transport Layer Security
  ⌄ TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 480
      Encrypted Application Data [truncated]: 0000000000000001143dc0decfd145c2d7ebf56483c7ade5fa683426e8c5681f2790a19a3c8d…
      [Application Data Protocol: Hypertext Transfer Protocol]
```

```
0030  01 f5 bb 36 00 00 17 03  03 01 e0 00 00 00 00 00   ···6···· ·····
0040  00 00 01 14 3d c0 de cf  d1 45 c2 d7 eb f5 64 83   ····=··· ·E····d·
0050  c7 ad e5 fa 68 34 26 e8  c5 68 1f 27 90 a1 9a 3c   ····h4&· ·h·'···<
0060  8d b8 2b 97 d4 75 2b 9b  4e ba 65 08 b4 96 40 d0   ··+··u+· N·e···@·
0070  c2 81 d3 de 19 c4 64 ec  f4 57 d3 26 c2 69 7a 28   ······d· ·W·&·iz(
0080  02 6d 36 43 f4 02 93 4e  cc 27 1d cc 4d 6c e4 d7   ·m6C···N ·'··Ml··
0090  93 2d 45 7c 20 30 7f e1  f8 c6 d5 d3 73 5b 85 37   ·-E| 0·· ····s[·7
00a0  44 18 a5 c2 41 c4 b8 a2  d9 cf ba 74 74 e8 d8 51   D···A··· ···tt··Q
00b0  11 1b 2e 6d c9 e8 b9 a4  e8 72 e8 f5 e1 05 44 45   ···.m··· ·r····DE
00c0  4f 9c 3e ca ac 27 f8 b4  5a 40 b9 92 2c 6f 18 df   O·>··'·· Z@··,o··
00d0  f8 04 4b 25 29 bd 68 6a  cb 72 bc de 8f b1 b5 7a   ··K%)·hj ·r·····z
00e0  25 42 91 27 64 36 34 97  a2 ae d7 8a 17 0a cf 64   %B·'d64· ·······d
00f0  8d 47 ef 98 9c ef 9f ee  2c e1 33 9c f3 b4 0d 48   ·G······ ,·3····H
0100  90 98 1c f0 4e c1 cd 3f  c3 31 c8 dc 16 38 dc 71   ····N··? ·1···8·q
0110  fe 16 6a 43 c5 e1 9b dc  d9 a0 38 62 d3 72 b0 64   ··jC···· ··8b·r·d
0120  eb b6 a5 ca 9e 20 ce cc  ec 94 f0 53 34 6b ac db   ····· ·· ···S4k··
0130  a6 76 73 18 af d4 75 0f  68 e7 41 1a 36 6c dc 91   ·vs···u· h·A·6l··
0140  00 ca 29 14 3a 43 ff 54  d1 aa df f1 25 6f 11 12   ··)·:C·T ····%o··
0150  ca f0 18 f6 a7 ab e3 18  03 5d f9 9d fb 91 04 27   ········ ·]·····'
0160  ca 97 8b bb 6e 6e 6d f9  df 9c 73 28 92 ae 9a 8e   ····nnm· ··s(····
0170  5c a2 4e 84 fb e6 7f 08  8a 81 27 a6 ec 05 6d 46   \·N····· ··'···mF
0180  33 35 17 8f 7a 6e 91 e0  38 3e 06 31 f9 a0 75 6c   35··zn·· 8>·1··ul
0190  53 1b 86 8e 6a 6e 0b 2d  21 16 94 08 8d 65 94 8c   S···jn·- !····e··
01a0  d1 38 45 ff 58 74 14 e0  b1 e7 0a a6 cf 6a 32 41   ·8E·Xt·· ·····j2A
01b0  3d a6 ca 94 53 79 36 c6  fd 71 c4 e5 67 99 b6 66   =···Sy6· ·q··g··f
01c0  37 94 87 41 4b c3 d6 ac  fd e2 80 dc 24 27 15 5e   7··AK··· ····$'·^
01d0  81 f9 98 be 57 91 3f 0c  f2 b9 68 6b 57 68 2c 47   ····W·?· ··hkWh,G
01e0  80 4b 2f 4e 4b 56 e3 92  b9 61 bc ab 44 35 3a 44   ·K/NKV·· ·a··D5:D
01f0  4d 90 11 0a ba 4b fb 3a  f0 43 ec 30 4e 91 2a 91   M····K·: ·C·0N·*·
0200  ef 36 1a 25 64 29 67 65  96 be 2c d0 ad 63 2f bf   ·6·%d)ge ··,··c/·
```

Payload is encrypted application data (tls.app_data), 480 bytes | Packets: 13597 · Displayed: 13597 (100.0%) | Profile: Default

5. Packet number 6545 contains the client-to-server TLS message that shuts down the TLS connection