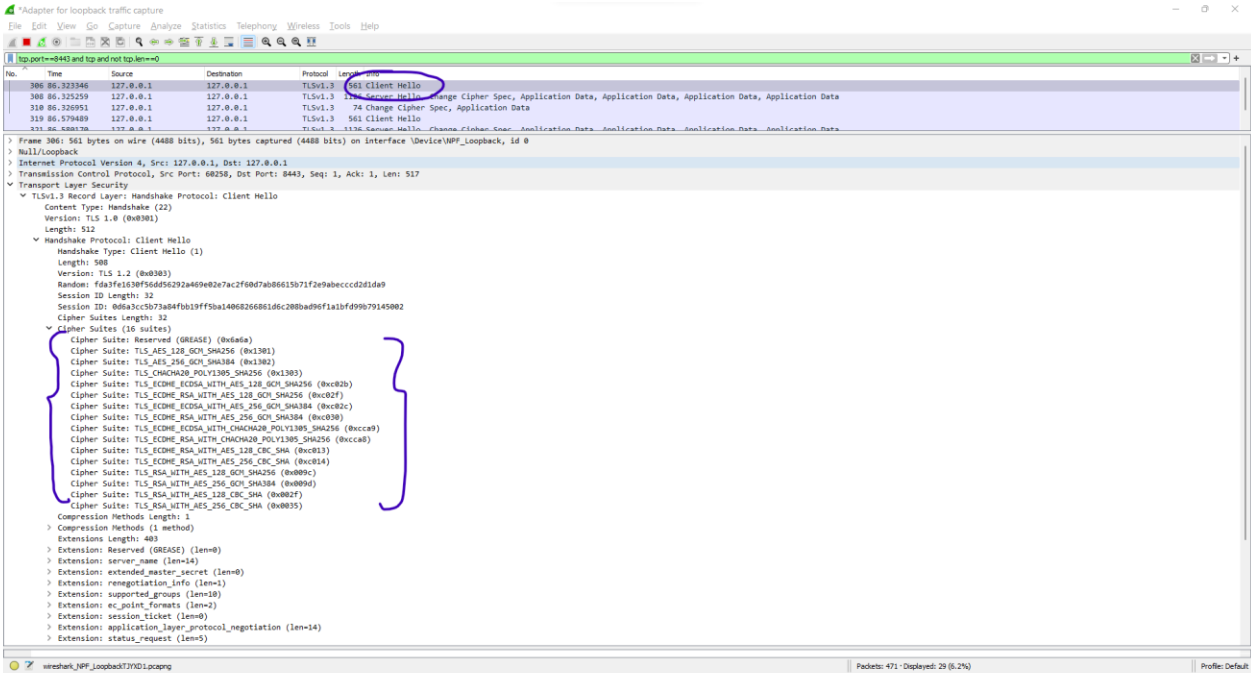
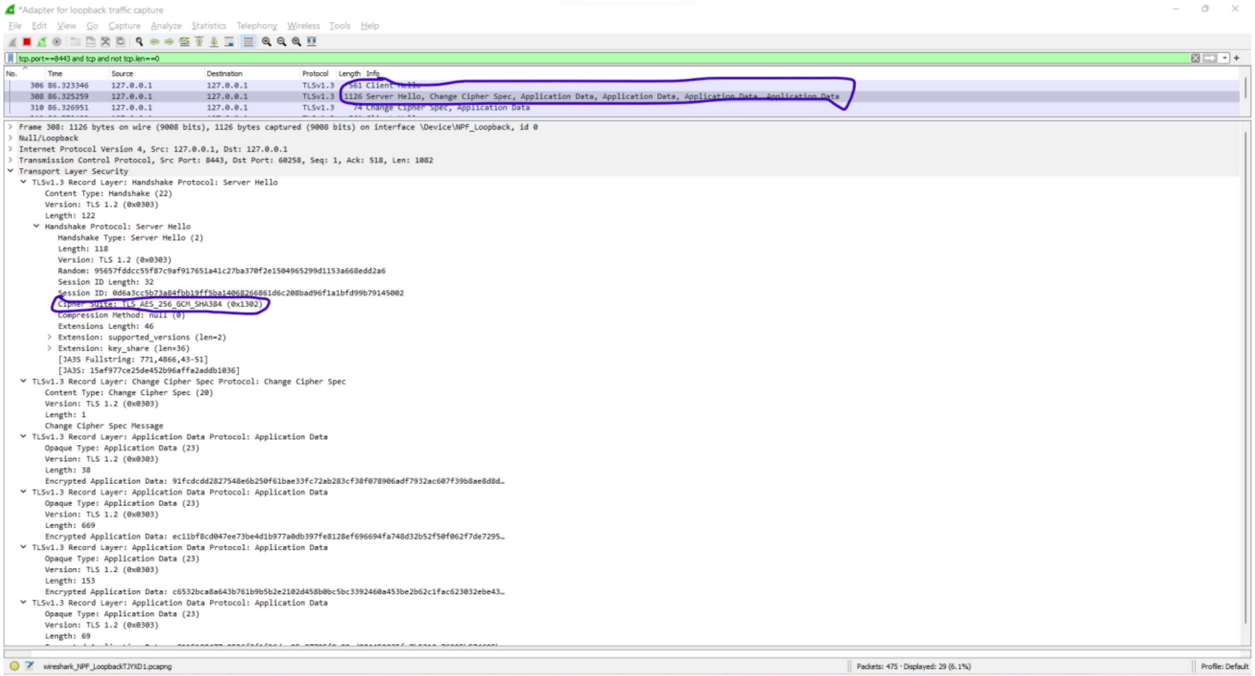
Using Google Chrome

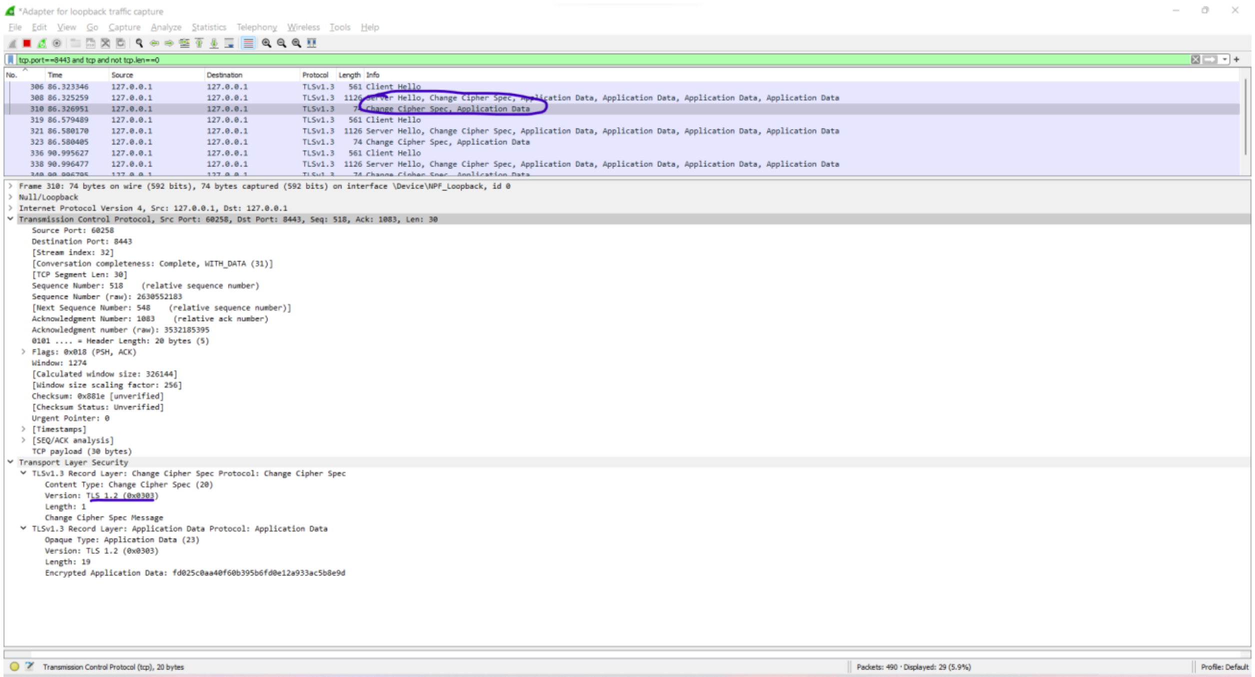
4.a) Provide screen captures of each of the asymmetric key exchange handshake packets


*Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.port==8443 and tcp and not tcp.len==0

No.  Time       Source     Destination  Protocol  Length Info
 306 86.323346  127.0.0.1  127.0.0.1    TLSv1.3    561 Client Hello
 308 86.325259  127.0.0.1  127.0.0.1    TLSv1.3   1126 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
 310 86.326951  127.0.0.1  127.0.0.1    TLSv1.3     74 Change Cipher Spec, Application Data
 319 86.579489  127.0.0.1  127.0.0.1    TLSv1.3    561 Client Hello

> Frame 306: 561 bytes on wire (4488 bits), 561 bytes captured (4488 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 60258, Dst Port: 8443, Seq: 1, Ack: 1, Len: 517
v Transport Layer Security
  v TLSv1.3 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 512
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 508
        Version: TLS 1.2 (0x0303)
        Random: fda3fe1630f56dd56292a469e02e7ac2f60d7ab86615b71f2e9abecccd2d1da9
        Session ID Length: 32
        Session ID: 0d6a3cc5b73a84fbb19ff5ba14068266861d6c208bad96f1a1bfd99b79145002
        Cipher Suites Length: 32
      v Cipher Suites (16 suites)
          Cipher Suite: Reserved (GREASE) (0x6a6a)
          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)
        Compression Methods Length: 1
      > Compression Methods (1 method)
        Extensions Length: 403
      > Extension: Reserved (GREASE) (len=0)
      > Extension: server_name (len=14)
      > Extension: extended_master_secret (len=0)
      > Extension: renegotiation_info (len=1)
      > Extension: supported_groups (len=10)
      > Extension: ec_point_formats (len=2)
      > Extension: session_ticket (len=0)
      > Extension: application_layer_protocol_negotiation (len=14)
      > Extension: status_request (len=5)

wireshark_NPF_LoopbackTJYXD1.pcapng     Packets: 471 · Displayed: 29 (6.2%)     Profile: Default
```


*Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.port==8443 and tcp and not tcp.len==0

No.  Time       Source     Destination  Protocol  Length Info
 306 86.323346  127.0.0.1  127.0.0.1    TLSv1.3    561 Client Hello
 308 86.325259  127.0.0.1  127.0.0.1    TLSv1.3   1126 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data
 310 86.326951  127.0.0.1  127.0.0.1    TLSv1.3     74 Change Cipher Spec, Application Data

> Frame 308: 1126 bytes on wire (9008 bits), 1126 bytes captured (9008 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 8443, Dst Port: 60258, Seq: 1, Ack: 518, Len: 1082
v Transport Layer Security
  v TLSv1.3 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 122
    v Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 118
        Version: TLS 1.2 (0x0303)
        Random: 95657fddcc55f87c9af917651a41c27ba370f2e1504965299d1153a668edd2a6
        Session ID Length: 32
        Session ID: 0d6a3cc5b73a84fbb19ff5ba14068266861d6c208bad96f1a1bfd99b79145002
        Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
        Compression Method: null (0)
        Extensions Length: 46
      > Extension: supported_versions (len=2)
      > Extension: key_share (len=36)
        [JA3S Fullstring: 771,4866,43-51]
        [JA3S: 15af977ce25de452b96affa2addb1036]
  v 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
  v TLSv1.3 Record Layer: Application Data Protocol: Application Data
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 38
      Encrypted Application Data: 91fcdcdd2827548e6b250f61bae33fc72ab283cf38f078906adf7932ac607f39b8ae8d8d…
  v TLSv1.3 Record Layer: Application Data Protocol: Application Data
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 669
      Encrypted Application Data: ec11bf8cd047ee73be4d1b977a0db397fe8128ef696694fa748d32b52f50f062f7de7295…
  v TLSv1.3 Record Layer: Application Data Protocol: Application Data
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 153
      Encrypted Application Data: c6532bca8a643b761b9b5b2e2102d458b0bc5bc3392460a453be2b62c1fac623032ebe43…
  v TLSv1.3 Record Layer: Application Data Protocol: Application Data
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 69

wireshark_NPF_LoopbackTJYXD1.pcapng     Packets: 475 · Displayed: 29 (6.1%)     Profile: Default
```


*Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

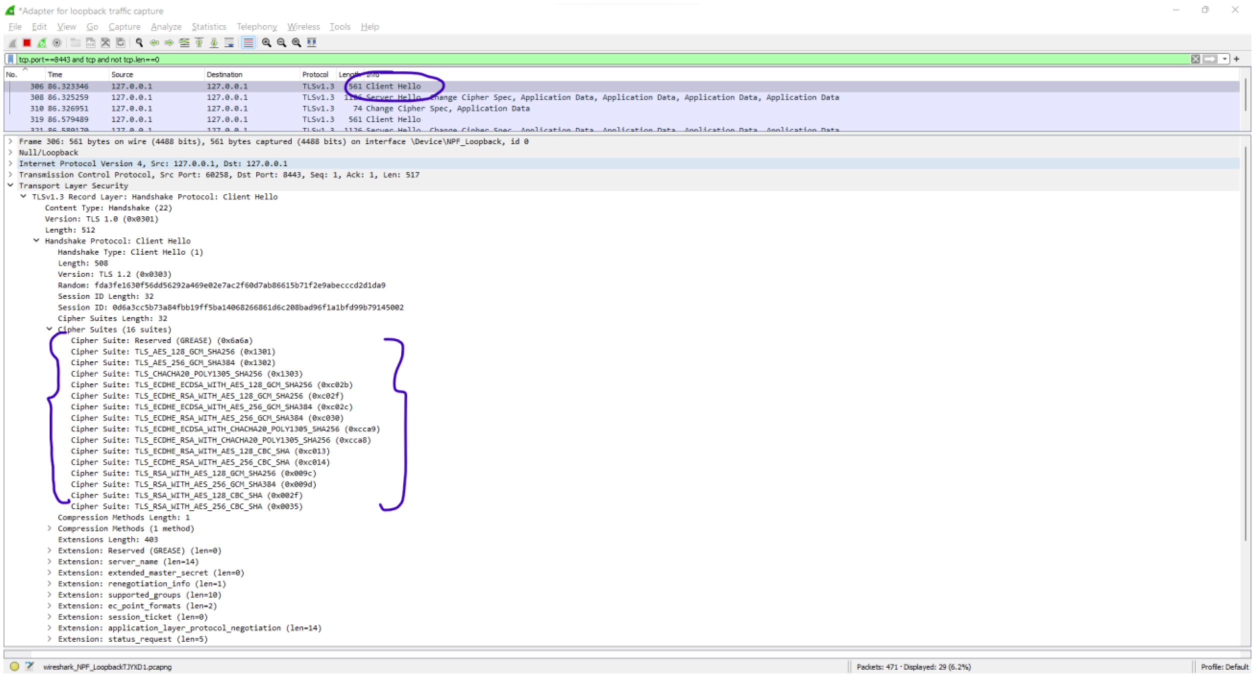
```
tcp.port==8443 and tcp and not tcp.len==0
```

```
No.  Time       Source     Destination  Protocol Length Info
 306 86.323346  127.0.0.1  127.0.0.1    TLSv1.3   561 Client Hello
 308 86.325259  127.0.0.1  127.0.0.1    TLSv1.3  1126 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
 310 86.326951  127.0.0.1  127.0.0.1    TLSv1.3    74 Change Cipher Spec, Application Data
 319 86.579489  127.0.0.1  127.0.0.1    TLSv1.3   561 Client Hello
 321 86.580170  127.0.0.1  127.0.0.1    TLSv1.3  1126 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
 323 86.580405  127.0.0.1  127.0.0.1    TLSv1.3    74 Change Cipher Spec, Application Data
 336 90.995627  127.0.0.1  127.0.0.1    TLSv1.3   561 Client Hello
 338 90.996477  127.0.0.1  127.0.0.1    TLSv1.3  1126 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
 340 90.996795  127.0.0.1  127.0.0.1    TLSv1.3    74 Change Cipher Spec, Application Data
```

```
> Frame 310: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
v Transmission Control Protocol, Src Port: 60258, Dst Port: 8443, Seq: 518, Ack: 1083, Len: 30
    Source Port: 60258
    Destination Port: 8443
    [Stream index: 32]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 30]
    Sequence Number: 518    (relative sequence number)
    Sequence Number (raw): 2630552183
    [Next Sequence Number: 548    (relative sequence number)]
    Acknowledgment Number: 1083    (relative ack number)
    Acknowledgment number (raw): 3532185395
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 1274
    [Calculated window size: 326144]
    [Window size scaling factor: 256]
    Checksum: 0x881e [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (30 bytes)
v Transport Layer Security
  v 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
  v TLSv1.3 Record Layer: Application Data Protocol: Application Data
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 19
      Encrypted Application Data: fd025c0aa40f60b395b6fd0e12a933ac5b8e9d
```

Transmission Control Protocol (tcp), 20 bytes | Packets: 490 · Displayed: 29 (5.9%) | Profile: Default

4.b) Identify the set of cipher suites (screenshot) available in the browser, and the one selected by the server.
Cipher suits avaliable:


*Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

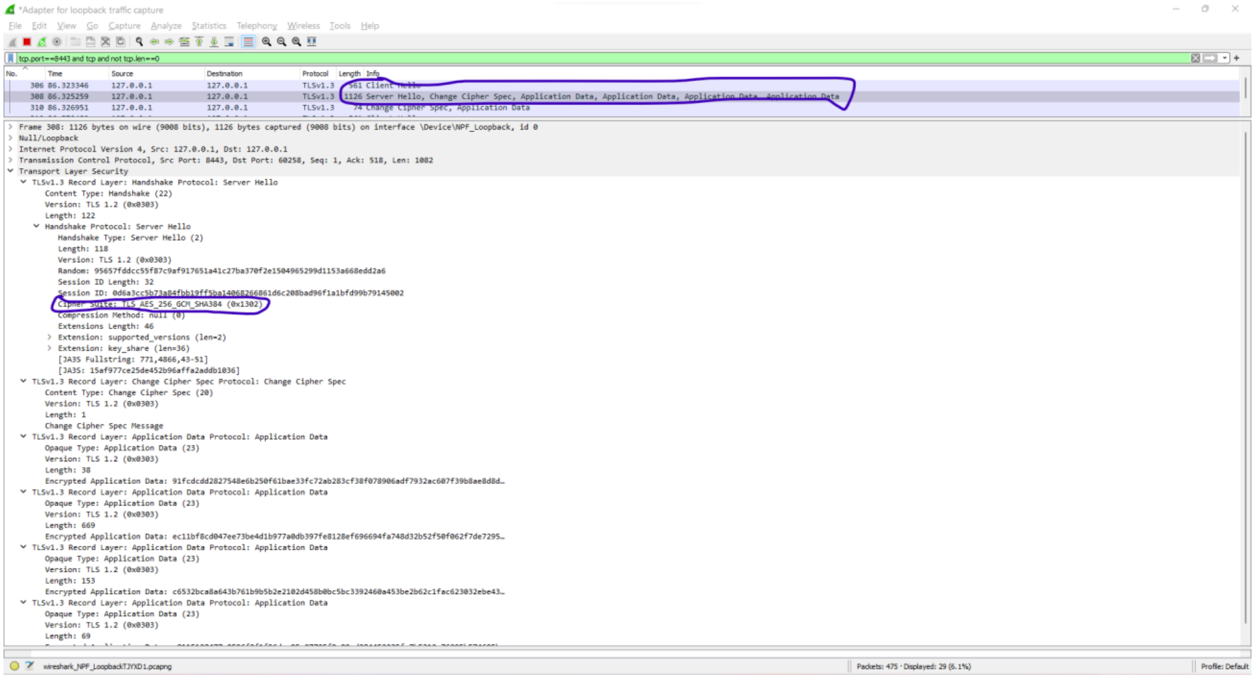
```
tcp.port==8443 and tcp and not tcp.len==0
```

```
No.  Time       Source     Destination  Protocol Length Info
 306 86.323346  127.0.0.1  127.0.0.1    TLSv1.3   561 Client Hello
 308 86.325259  127.0.0.1  127.0.0.1    TLSv1.3  1126 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
 310 86.326951  127.0.0.1  127.0.0.1    TLSv1.3    74 Change Cipher Spec, Application Data
 319 86.579489  127.0.0.1  127.0.0.1    TLSv1.3   561 Client Hello
 321 86.580170  127.0.0.1  127.0.0.1    TLSv1.3  1126 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
```

```
> Frame 306: 561 bytes on wire (4488 bits), 561 bytes captured (4488 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 60258, Dst Port: 8443, Seq: 1, Ack: 1, Len: 517
v Transport Layer Security
  v TLSv1.3 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 512
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 508
        Version: TLS 1.2 (0x0303)
        Random: fda3fe1630f56dd56292a469e02e7ac2f60d7ab86615b71f2e9abecccd2d1da9
        Session ID Length: 32
        Session ID: 0d6a3cc5b73a84fbb19ff5ba14068266861d6c208bad96f1a1bfd99b79145002
        Cipher Suites Length: 32
      v Cipher Suites (16 suites)
          Cipher Suite: Reserved (GREASE) (0x6a6a)
          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)
        Compression Methods Length: 1
      > Compression Methods (1 method)
        Extensions Length: 403
      > Extension: Reserved (GREASE) (len=0)
      > Extension: server_name (len=14)
      > Extension: extended_master_secret (len=0)
      > Extension: renegotiation_info (len=1)
      > Extension: supported_groups (len=10)
      > Extension: ec_point_formats (len=2)
      > Extension: session_ticket (len=0)
      > Extension: application_layer_protocol_negotiation (len=14)
      > Extension: status_request (len=5)
```

wireshark_NPF_LoopbackTJYXD1.pcapng | Packets: 471 · Displayed: 29 (6.2%) | Profile: Default

Selected:



*Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port==8443 and tcp and not tcp.len==0

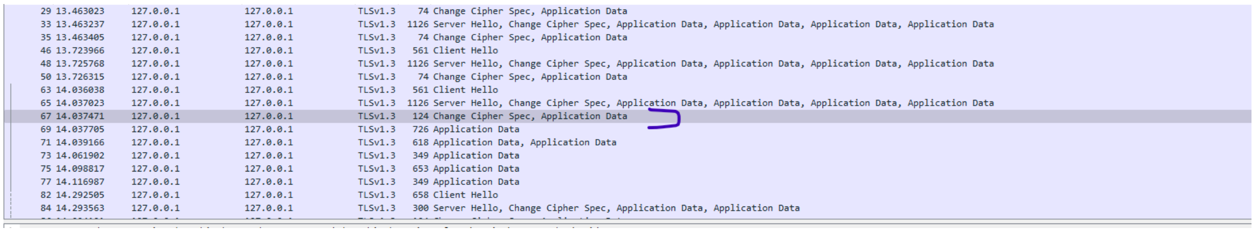
```
No.   Time        Source      Destination  Protocol  Length Info
  306 86.323346   127.0.0.1   127.0.0.1    TLSv1.3    561 Client Hello
  308 86.325259   127.0.0.1   127.0.0.1    TLSv1.3   1126 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
  310 86.326951   127.0.0.1   127.0.0.1    TLSv1.3     74 Change Cipher Spec, Application Data
```

```
> Frame 308: 1126 bytes on wire (9008 bits), 1126 bytes captured (9008 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 8443, Dst Port: 60258, Seq: 1, Ack: 518, Len: 1082
v Transport Layer Security
  v TLSv1.3 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 122
    v Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 118
        Version: TLS 1.2 (0x0303)
        Random: 95657fddcc55f87c9af917651a41c27ba370f2e1504965299d1153a668edd2a6
        Session ID Length: 32
        Session ID: 0d6a3cc5b73a84fbb19ff5ba14068266861d6c208bad96f1a1bfd99b79145002
        Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
        Compression Method: null (0)
        Extensions Length: 46
      > Extension: supported_versions (len=2)
      > Extension: key_share (len=36)
        [JA3S Fullstring: 771,4866,43-51]
        [JA3S: 15af977ce25de452b96affa2addb1036]
  v 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
  v TLSv1.3 Record Layer: Application Data Protocol: Application Data
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 38
      Encrypted Application Data: 91fcdcdd2827548e6b250f61bae33fc72ab283cf38f078906adf7932ac607f39b8ae8d8d…
  v TLSv1.3 Record Layer: Application Data Protocol: Application Data
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 669
      Encrypted Application Data: ec11bf8cd047ee73be4d1b977a0db397fe8128ef696694fa748d32b52f50f062f7de7295…
  v TLSv1.3 Record Layer: Application Data Protocol: Application Data
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 153
      Encrypted Application Data: c6532bca8a643b761b9b5b2e2102d458b0bc5bc3392460a453be2b62c1fac623032ebe43…
  v TLSv1.3 Record Layer: Application Data Protocol: Application Data
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 69
```

wireshark_NPF_LoopbackTJYXD1.pcapng | Packets: 475 · Displayed: 29 (6.1%) | Profile: Default

4.c

Identify the place (packet) in the conversation where the client and server start using symmetric keys and explain why you think this is the place.



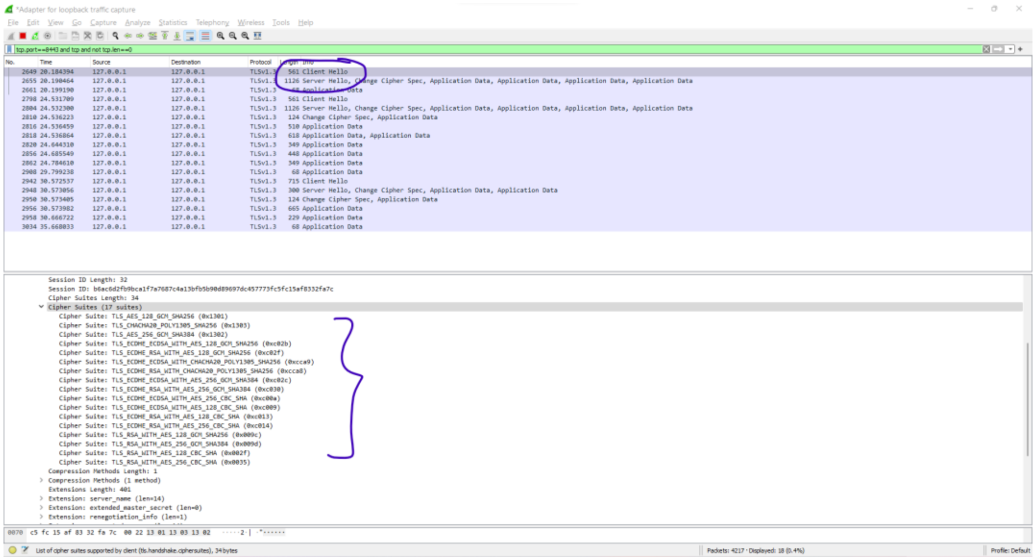
```
   29 13.463023   127.0.0.1   127.0.0.1   TLSv1.3     74 Change Cipher Spec, Application Data
   33 13.463237   127.0.0.1   127.0.0.1   TLSv1.3   1126 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
   35 13.463405   127.0.0.1   127.0.0.1   TLSv1.3     74 Change Cipher Spec, Application Data
   46 13.723966   127.0.0.1   127.0.0.1   TLSv1.3    561 Client Hello
   48 13.725768   127.0.0.1   127.0.0.1   TLSv1.3   1126 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
   50 13.726315   127.0.0.1   127.0.0.1   TLSv1.3     74 Change Cipher Spec, Application Data
   63 14.036038   127.0.0.1   127.0.0.1   TLSv1.3    561 Client Hello
   65 14.037023   127.0.0.1   127.0.0.1   TLSv1.3   1126 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
   67 14.037471   127.0.0.1   127.0.0.1   TLSv1.3    124 Change Cipher Spec, Application Data
   69 14.037705   127.0.0.1   127.0.0.1   TLSv1.3    726 Application Data
   71 14.039166   127.0.0.1   127.0.0.1   TLSv1.3    618 Application Data, Application Data
   73 14.061902   127.0.0.1   127.0.0.1   TLSv1.3    349 Application Data
   75 14.098817   127.0.0.1   127.0.0.1   TLSv1.3    653 Application Data
   77 14.116987   127.0.0.1   127.0.0.1   TLSv1.3    349 Application Data
   82 14.292505   127.0.0.1   127.0.0.1   TLSv1.3    658 Client Hello
   84 14.293563   127.0.0.1   127.0.0.1   TLSv1.3    300 Server Hello, Change Cipher Spec, Application Data, Application Data
```

Assymmetric Encryption : Used for establishing secure connection between client and server.
Symmetric Encryption: Used for communication once secure connection is established.

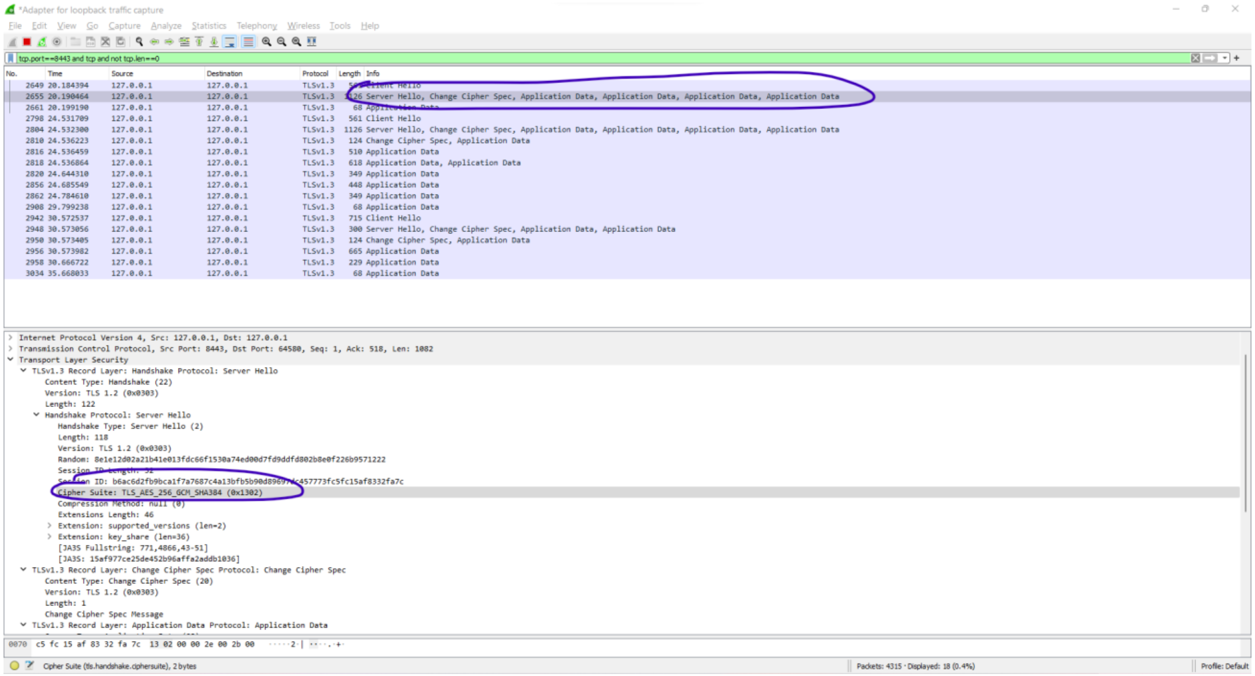
I believe after sending each other Change cipher spec they confirm both have their session keys ready and will now use symmetric encryption for further data transfers [starting at Application Data packet].

Working on Firefox

5.a Provide screen captures of each of the asymmetric key exchange handshake packets


*Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

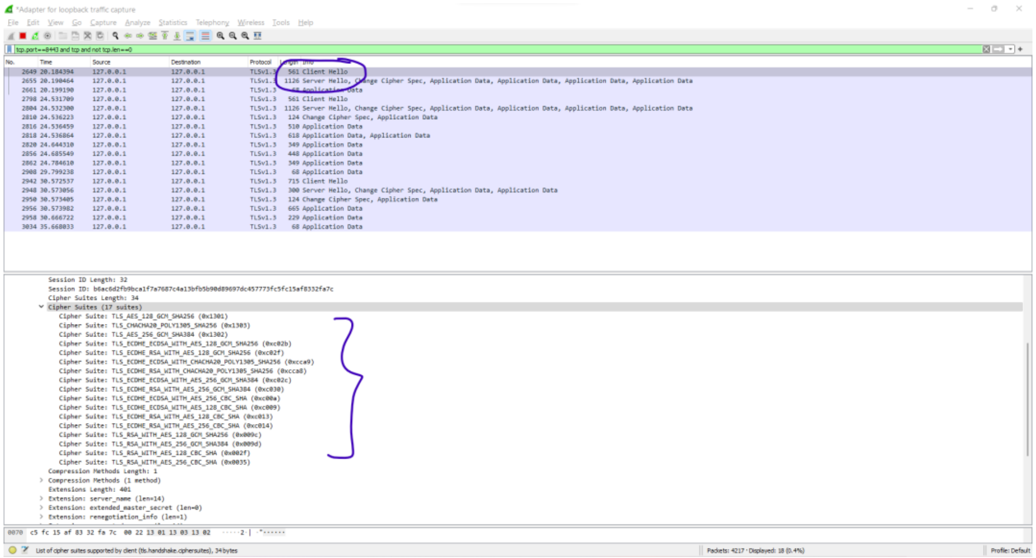
```
tcp.port==8443 and tcp and not tcp.len==0

No.  Time       Source     Destination  Protocol  Length Info
2649 20.184394  127.0.0.1  127.0.0.1    TLSv1.3    561 Client Hello
2655 20.190464  127.0.0.1  127.0.0.1    TLSv1.3   1126 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
2661 20.199190  127.0.0.1  127.0.0.1    TLSv1.3     68 Application Data
2798 24.531709  127.0.0.1  127.0.0.1    TLSv1.3    561 Client Hello
2804 24.532300  127.0.0.1  127.0.0.1    TLSv1.3   1126 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
2810 24.536223  127.0.0.1  127.0.0.1    TLSv1.3    124 Change Cipher Spec, Application Data
2816 24.536459  127.0.0.1  127.0.0.1    TLSv1.3    510 Application Data
2818 24.536864  127.0.0.1  127.0.0.1    TLSv1.3    618 Application Data, Application Data
2820 24.644310  127.0.0.1  127.0.0.1    TLSv1.3    349 Application Data
2856 24.685549  127.0.0.1  127.0.0.1    TLSv1.3    448 Application Data
2862 24.784610  127.0.0.1  127.0.0.1    TLSv1.3    349 Application Data
2908 29.799238  127.0.0.1  127.0.0.1    TLSv1.3     68 Application Data
2942 30.572537  127.0.0.1  127.0.0.1    TLSv1.3    715 Client Hello
2948 30.573056  127.0.0.1  127.0.0.1    TLSv1.3    300 Server Hello, Change Cipher Spec, Application Data, Application Data
2950 30.573405  127.0.0.1  127.0.0.1    TLSv1.3    124 Change Cipher Spec, Application Data
2956 30.573982  127.0.0.1  127.0.0.1    TLSv1.3    665 Application Data
2958 30.666722  127.0.0.1  127.0.0.1    TLSv1.3    229 Application Data
3034 35.668033  127.0.0.1  127.0.0.1    TLSv1.3     68 Application Data

      Session ID Length: 32
      Session ID: b6ac6d2fb9bca1f7a7687c4a13bfb5b90d89697dc457773fc5fc15af8332fa7c
      Cipher Suites Length: 34
    ⌄ Cipher Suites (17 suites)
        Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
        Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
        Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
        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_CHACHA20_POLY1305_SHA256 (0xcca9)
        Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
        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_AES_256_CBC_SHA (0xc00a)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
        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)
      Compression Methods Length: 1
    > Compression Methods (1 method)
      Extensions Length: 401
    > Extension: server_name (len=14)
    > Extension: extended_master_secret (len=0)
    > Extension: renegotiation_info (len=1)

0070  c5 fc 15 af 83 32 fa 7c  00 22 13 01 13 03 13 02   ·····2·| ·"······

List of cipher suites supported by client (tls.handshake.ciphersuites), 34 bytes    Packets: 4217 · Displayed: 18 (0.4%)    Profile: Default
```


*Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.port==8443 and tcp and not tcp.len==0

No.  Time       Source     Destination  Protocol  Length Info
2649 20.184394  127.0.0.1  127.0.0.1    TLSv1.3    561 Client Hello
2655 20.190464  127.0.0.1  127.0.0.1    TLSv1.3   1126 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
2661 20.199190  127.0.0.1  127.0.0.1    TLSv1.3     68 Application Data
2798 24.531709  127.0.0.1  127.0.0.1    TLSv1.3    561 Client Hello
2804 24.532300  127.0.0.1  127.0.0.1    TLSv1.3   1126 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
2810 24.536223  127.0.0.1  127.0.0.1    TLSv1.3    124 Change Cipher Spec, Application Data
2816 24.536459  127.0.0.1  127.0.0.1    TLSv1.3    510 Application Data
2818 24.536864  127.0.0.1  127.0.0.1    TLSv1.3    618 Application Data, Application Data
2820 24.644310  127.0.0.1  127.0.0.1    TLSv1.3    349 Application Data
2856 24.685549  127.0.0.1  127.0.0.1    TLSv1.3    448 Application Data
2862 24.784610  127.0.0.1  127.0.0.1    TLSv1.3    349 Application Data
2908 29.799238  127.0.0.1  127.0.0.1    TLSv1.3     68 Application Data
2942 30.572537  127.0.0.1  127.0.0.1    TLSv1.3    715 Client Hello
2948 30.573056  127.0.0.1  127.0.0.1    TLSv1.3    300 Server Hello, Change Cipher Spec, Application Data, Application Data
2950 30.573405  127.0.0.1  127.0.0.1    TLSv1.3    124 Change Cipher Spec, Application Data
2956 30.573982  127.0.0.1  127.0.0.1    TLSv1.3    665 Application Data
2958 30.666722  127.0.0.1  127.0.0.1    TLSv1.3    229 Application Data
3034 35.668033  127.0.0.1  127.0.0.1    TLSv1.3     68 Application Data

> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 8443, Dst Port: 64580, Seq: 1, Ack: 518, Len: 1082
⌄ Transport Layer Security
  ⌄ 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: 8e1e12d02a21b41e013fdc66f1530a74ed00d7fd9ddfd802b8e0f226b9571222
        Session ID Length: 32
        Session ID: b6ac6d2fb9bca1f7a7687c4a13bfb5b90d89697dc457773fc5fc15af8332fa7c
        Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
        Compression Method: null (0)
        Extensions Length: 46
      > Extension: supported_versions (len=2)
      > Extension: key_share (len=36)
        [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)
      Length: 1
      Change Cipher Spec Message
  ⌄ TLSv1.3 Record Layer: Application Data Protocol: Application Data

0070  c5 fc 15 af 83 32 fa 7c  13 02 00 00 2e 00 2b 00   ·····2·| ····.·+·

Cipher Suite (tls.handshake.ciphersuite), 2 bytes    Packets: 4315 · Displayed: 18 (0.4%)    Profile: Default
```

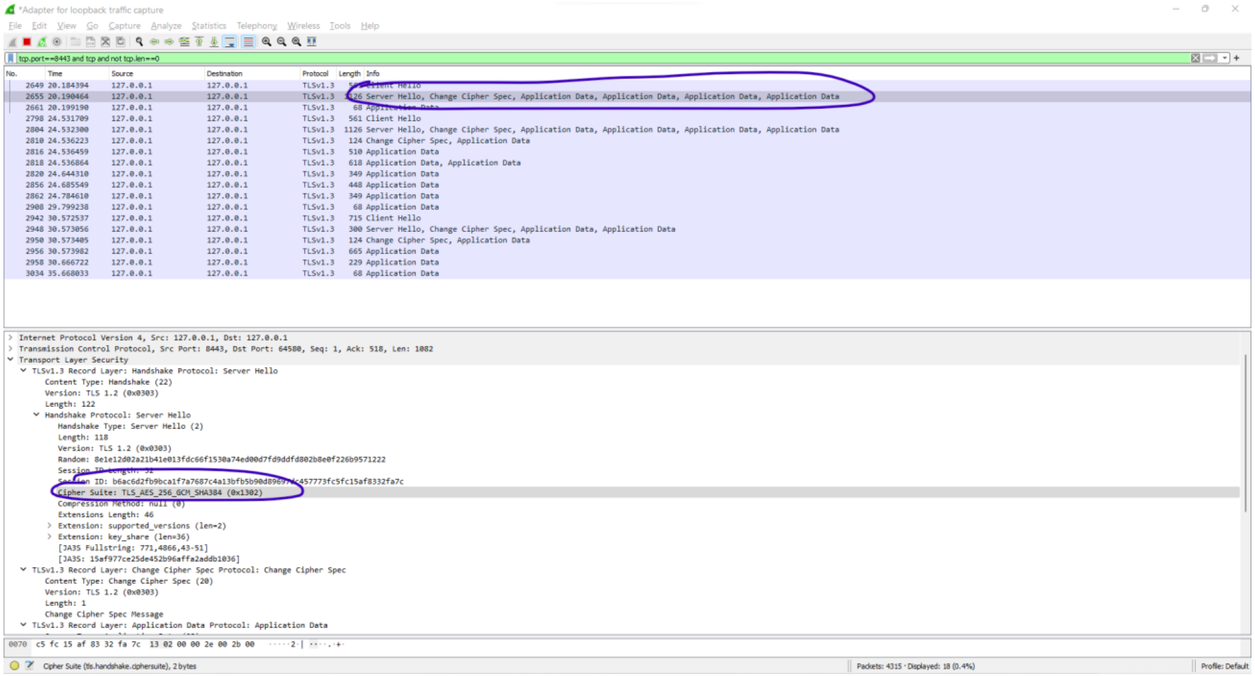
5.b) Identify the set of cipher suites (screenshot) available in the browser, and the one selected by the server.

Cipher suits avaliable:


*Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.port==8443 and tcp and not tcp.len==0

No.  Time       Source     Destination Protocol Length Info
2649 20.184394  127.0.0.1  127.0.0.1   TLSv1.3   561 Client Hello
2655 20.190464  127.0.0.1  127.0.0.1   TLSv1.3  1126 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
2661 20.199190  127.0.0.1  127.0.0.1   TLSv1.3    68 Application Data
2798 24.531709  127.0.0.1  127.0.0.1   TLSv1.3   561 Client Hello
2804 24.532300  127.0.0.1  127.0.0.1   TLSv1.3  1126 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
2810 24.536223  127.0.0.1  127.0.0.1   TLSv1.3   124 Change Cipher Spec, Application Data
2816 24.536459  127.0.0.1  127.0.0.1   TLSv1.3   510 Application Data
2818 24.536864  127.0.0.1  127.0.0.1   TLSv1.3   618 Application Data, Application Data
2820 24.644310  127.0.0.1  127.0.0.1   TLSv1.3   349 Application Data
2856 24.685549  127.0.0.1  127.0.0.1   TLSv1.3   448 Application Data
2862 24.784610  127.0.0.1  127.0.0.1   TLSv1.3   349 Application Data
2908 29.799238  127.0.0.1  127.0.0.1   TLSv1.3    68 Application Data
2942 30.572537  127.0.0.1  127.0.0.1   TLSv1.3   715 Client Hello
2948 30.573056  127.0.0.1  127.0.0.1   TLSv1.3   300 Server Hello, Change Cipher Spec, Application Data, Application Data
2950 30.573405  127.0.0.1  127.0.0.1   TLSv1.3   124 Change Cipher Spec, Application Data
2956 30.573982  127.0.0.1  127.0.0.1   TLSv1.3   665 Application Data
2958 30.666722  127.0.0.1  127.0.0.1   TLSv1.3   229 Application Data
3034 35.668033  127.0.0.1  127.0.0.1   TLSv1.3    68 Application Data

        Session ID Length: 32
        Session ID: b6ac6d2fb9bca1f7a7687c4a13bfb5b90d89697dc457773fc5fc15af8332fa7c
        Cipher Suites Length: 34
      ˅ Cipher Suites (17 suites)
          Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
          Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
          Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
          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_CHACHA20_POLY1305_SHA256 (0xcca9)
          Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
          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_AES_256_CBC_SHA (0xc00a)
          Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
          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)
        Compression Methods Length: 1
      › Compression Methods (1 method)
        Extensions Length: 401
      › Extension: server_name (len=14)
      › Extension: extended_master_secret (len=0)
      › Extension: renegotiation_info (len=1)

0070  c5 fc 15 af 83 32 fa 7c  00 22 13 01 13 03 13 02   ·····2·| ·"······

List of cipher suites supported by client (tls.handshake.ciphersuites), 34 bytes     Packets: 4217 · Displayed: 18 (0.4%)     Profile: Default
```

Selected:

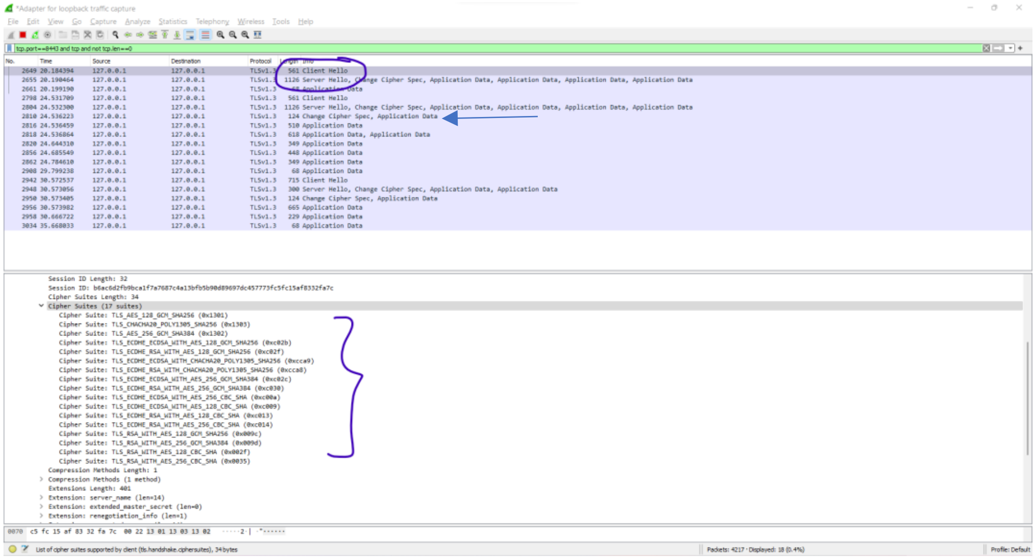

*Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.port==8443 and tcp and not tcp.len==0

No.  Time       Source     Destination Protocol Length Info
2649 20.184394  127.0.0.1  127.0.0.1   TLSv1.3   561 Client Hello
2655 20.190464  127.0.0.1  127.0.0.1   TLSv1.3  1126 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
2661 20.199190  127.0.0.1  127.0.0.1   TLSv1.3    68 Application Data
2798 24.531709  127.0.0.1  127.0.0.1   TLSv1.3   561 Client Hello
2804 24.532300  127.0.0.1  127.0.0.1   TLSv1.3  1126 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
2810 24.536223  127.0.0.1  127.0.0.1   TLSv1.3   124 Change Cipher Spec, Application Data
2816 24.536459  127.0.0.1  127.0.0.1   TLSv1.3   510 Application Data
2818 24.536864  127.0.0.1  127.0.0.1   TLSv1.3   618 Application Data, Application Data
2820 24.644310  127.0.0.1  127.0.0.1   TLSv1.3   349 Application Data
2856 24.685549  127.0.0.1  127.0.0.1   TLSv1.3   448 Application Data
2862 24.784610  127.0.0.1  127.0.0.1   TLSv1.3   349 Application Data
2908 29.799238  127.0.0.1  127.0.0.1   TLSv1.3    68 Application Data
2942 30.572537  127.0.0.1  127.0.0.1   TLSv1.3   715 Client Hello
2948 30.573056  127.0.0.1  127.0.0.1   TLSv1.3   300 Server Hello, Change Cipher Spec, Application Data, Application Data
2950 30.573405  127.0.0.1  127.0.0.1   TLSv1.3   124 Change Cipher Spec, Application Data
2956 30.573982  127.0.0.1  127.0.0.1   TLSv1.3   665 Application Data
2958 30.666722  127.0.0.1  127.0.0.1   TLSv1.3   229 Application Data
3034 35.668033  127.0.0.1  127.0.0.1   TLSv1.3    68 Application Data

› Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
› Transmission Control Protocol, Src Port: 8443, Dst Port: 64580, Seq: 1, Ack: 518, Len: 1082
˅ Transport Layer Security
  ˅ 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: 8e1e12d02a21b41e013fdc66f1530a74ed00d7fd9ddfd802b8e0f226b9571222
        Session ID Length: 32
        Session ID: b6ac6d2fb9bca1f7a7687c4a13bfb5b90d89697dc457773fc5fc15af8332fa7c
        Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
        Compression Method: null (0)
        Extensions Length: 46
      › Extension: supported_versions (len=2)
      › Extension: key_share (len=36)
        [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)
      Length: 1
      Change Cipher Spec Message
  ˅ TLSv1.3 Record Layer: Application Data Protocol: Application Data

0070  c5 fc 15 af 83 32 fa 7c  13 02 00 00 2e 00 2b 00   ·····2·| ····.·+·

Cipher Suite (tls.handshake.ciphersuite), 2 bytes     Packets: 4315 · Displayed: 18 (0.4%)     Profile: Default
```

5c

Identify the place (packet) in the conversation where the client and server start using symmetric keys and explain why you think this is the place.

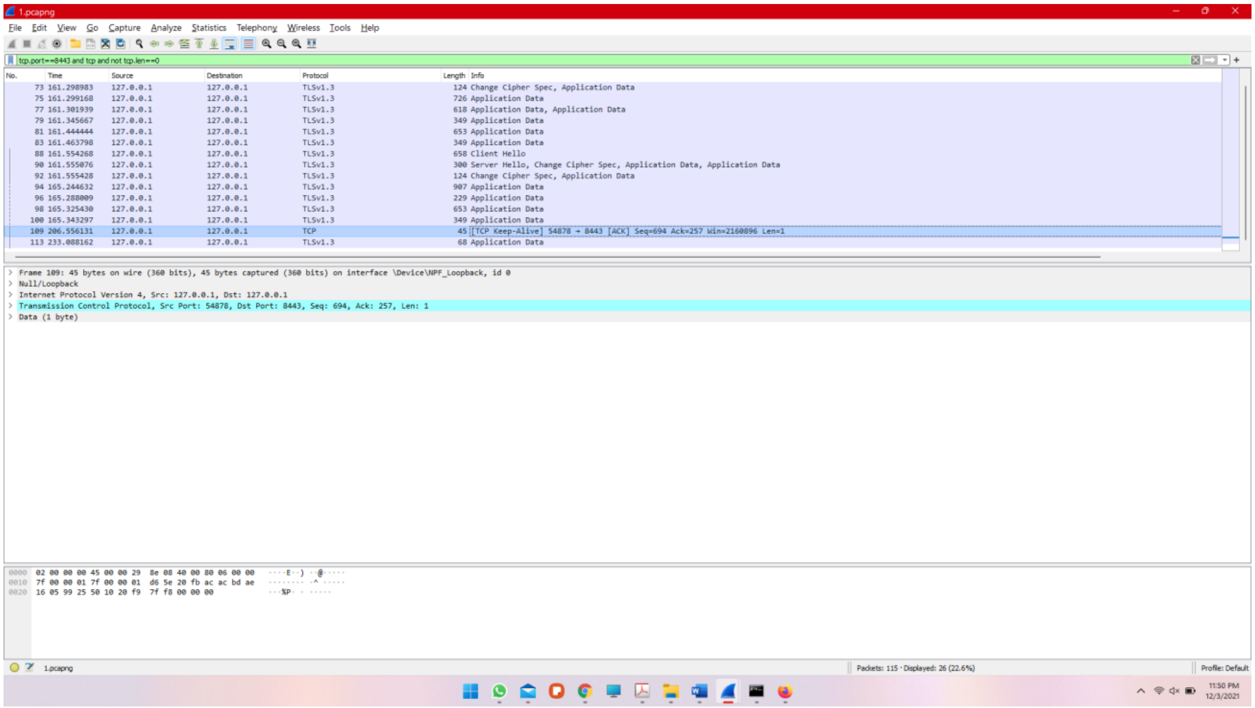
The same point after change cipher spec.


*Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.port==8443 and tcp and not tcp.len==0

No.  Time       Source     Destination  Protocol  Length Info
2649 20.184394  127.0.0.1  127.0.0.1    TLSv1.3    561 Client Hello
2655 20.190464  127.0.0.1  127.0.0.1    TLSv1.3   1126 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
2661 20.199190  127.0.0.1  127.0.0.1    TLSv1.3     68 Application Data
2798 24.531709  127.0.0.1  127.0.0.1    TLSv1.3    561 Client Hello
2804 24.532300  127.0.0.1  127.0.0.1    TLSv1.3   1126 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
2810 24.536223  127.0.0.1  127.0.0.1    TLSv1.3    124 Change Cipher Spec, Application Data
2816 24.536459  127.0.0.1  127.0.0.1    TLSv1.3    510 Application Data
2818 24.536864  127.0.0.1  127.0.0.1    TLSv1.3    618 Application Data, Application Data
2820 24.644310  127.0.0.1  127.0.0.1    TLSv1.3    349 Application Data
2856 24.685549  127.0.0.1  127.0.0.1    TLSv1.3    448 Application Data
2862 24.784610  127.0.0.1  127.0.0.1    TLSv1.3    349 Application Data
2908 29.799238  127.0.0.1  127.0.0.1    TLSv1.3     68 Application Data
2942 30.572537  127.0.0.1  127.0.0.1    TLSv1.3    715 Client Hello
2948 30.573056  127.0.0.1  127.0.0.1    TLSv1.3    300 Server Hello, Change Cipher Spec, Application Data, Application Data
2950 30.573405  127.0.0.1  127.0.0.1    TLSv1.3    124 Change Cipher Spec, Application Data
2956 30.573982  127.0.0.1  127.0.0.1    TLSv1.3    665 Application Data
2958 30.666722  127.0.0.1  127.0.0.1    TLSv1.3    229 Application Data
3034 35.668033  127.0.0.1  127.0.0.1    TLSv1.3     68 Application Data
```

```
    Session ID Length: 32
    Session ID: b6ac6d2fb9bca1f7a7687c4a13bfb5b90d89697dc457773fc5fc15af8332fa7c
    Cipher Suites Length: 34
  v Cipher Suites (17 suites)
      Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
      Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
      Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
      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_CHACHA20_POLY1305_SHA256 (0xcca9)
      Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
      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_AES_256_CBC_SHA (0xc00a)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
      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)
    Compression Methods Length: 1
  > Compression Methods (1 method)
    Extensions Length: 401
  > Extension: server_name (len=14)
  > Extension: extended_master_secret (len=0)
  > Extension: renegotiation_info (len=1)

0070  c5 fc 15 af 83 32 fa 7c  00 22 13 01 13 03 13 02   ·····2·|·"······

List of cipher suites supported by client (tls.handshake.ciphersuites), 34 bytes    Packets: 4217 · Displayed: 18 (0.4%)    Profile: Default
```

6.a In Chrome we can see a Keep-Alive packet. The firefox browser does not keep sending a keep alive packet.


1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
11:50 PM
12/3/2021

```
tcp.port==8443 and tcp and not tcp.len==0

No.  Time        Source     Destination  Protocol  Length Info
 73 161.298983   127.0.0.1  127.0.0.1    TLSv1.3    124 Change Cipher Spec, Application Data
 75 161.299168   127.0.0.1  127.0.0.1    TLSv1.3    726 Application Data
 77 161.301939   127.0.0.1  127.0.0.1    TLSv1.3    618 Application Data, Application Data
 79 161.345667   127.0.0.1  127.0.0.1    TLSv1.3    349 Application Data
 81 161.444444   127.0.0.1  127.0.0.1    TLSv1.3    653 Application Data
 83 161.463798   127.0.0.1  127.0.0.1    TLSv1.3    349 Application Data
 88 161.554268   127.0.0.1  127.0.0.1    TLSv1.3    658 Client Hello
 90 161.555076   127.0.0.1  127.0.0.1    TLSv1.3    300 Server Hello, Change Cipher Spec, Application Data, Application Data
 92 161.555428   127.0.0.1  127.0.0.1    TLSv1.3    124 Change Cipher Spec, Application Data
 94 165.244632   127.0.0.1  127.0.0.1    TLSv1.3    907 Application Data
 96 165.288009   127.0.0.1  127.0.0.1    TLSv1.3    229 Application Data
 98 165.325430   127.0.0.1  127.0.0.1    TLSv1.3    653 Application Data
100 165.343297   127.0.0.1  127.0.0.1    TLSv1.3    349 Application Data
109 206.556131   127.0.0.1  127.0.0.1    TCP         45 [TCP Keep-Alive] 54878 → 8443 [ACK] Seq=694 Ack=257 Win=2160896 Len=1
113 233.088162   127.0.0.1  127.0.0.1    TLSv1.3     68 Application Data

> Frame 109: 45 bytes on wire (360 bits), 45 bytes captured (360 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 54878, Dst Port: 8443, Seq: 694, Ack: 257, Len: 1
> Data (1 byte)

0000  02 00 00 00 45 00 00 29  8e 08 40 00 80 06 00 00   ····E··) ··@·····
0010  7f 00 00 01 7f 00 00 01  d6 5e 20 fb ac ac bd ae   ········ ·^ ·····
0020  16 05 99 25 50 10 20 f9  7f f8 00 00 00            ···%P· · ·····

1.pcapng    Packets: 115 · Displayed: 26 (22.6%)    Profile: Default
```

6.b Chrome has 16 ciphers avaliable and Firefox has 17. The GREASE one in chrome is a chrome specific reserved cipher.

Ciphers 0xc00a and 0xc009 are present in firefox but not in chrome.

Ciphers 0xcca9 and 0xcca8 are present in chrome but not in firefox.

6.c No

7. No, it now uses TLSv1.2 versus TLSv1.3 used in the above examples. TLSv1.3 is relatively new. It is picking up the stream due to faster handshake and other benefits. It also reduces latency for imporving the website perfomance. Moreover, TLS1.3 is not backward compatible with v1.2 – it poses a difficult decision for upgrading of the system. The website seems to be build on a framework that best supports TLSv1.2 and not TLSv1.3.