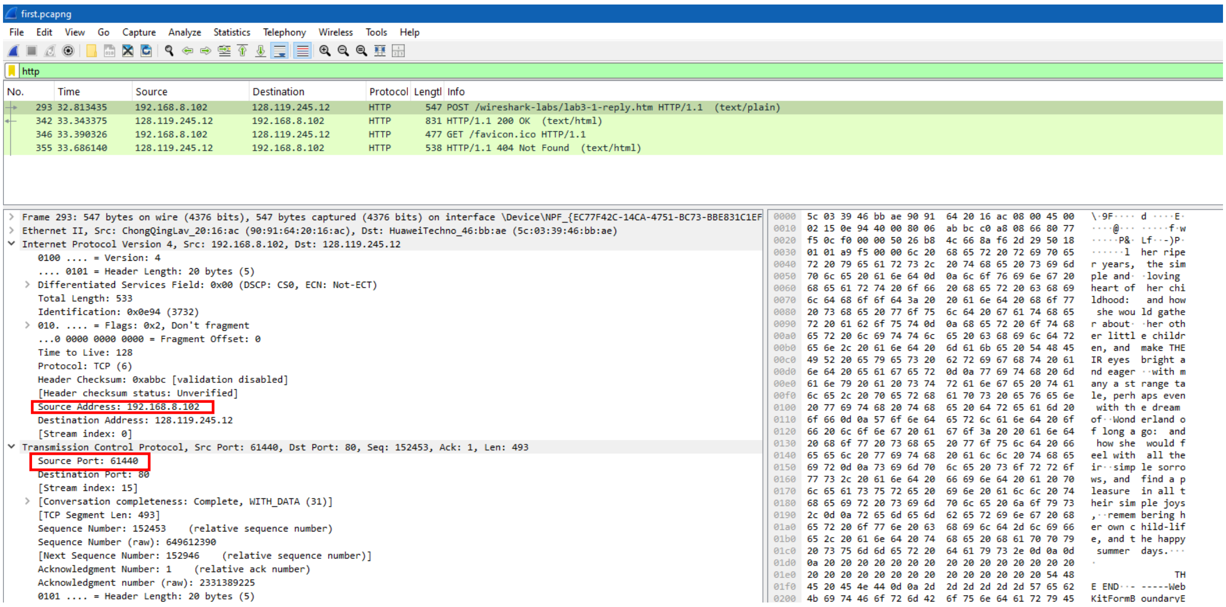
Activity04 - Wireshark Lab 04 - Wireshark TCP

1. *What is the IP address and TCP port number used by the client computer (source) that is transferring the alice.txt file to gaia.cs.umass.edu?*

- Client IP – 192.168.8.102
- Client port – 61440



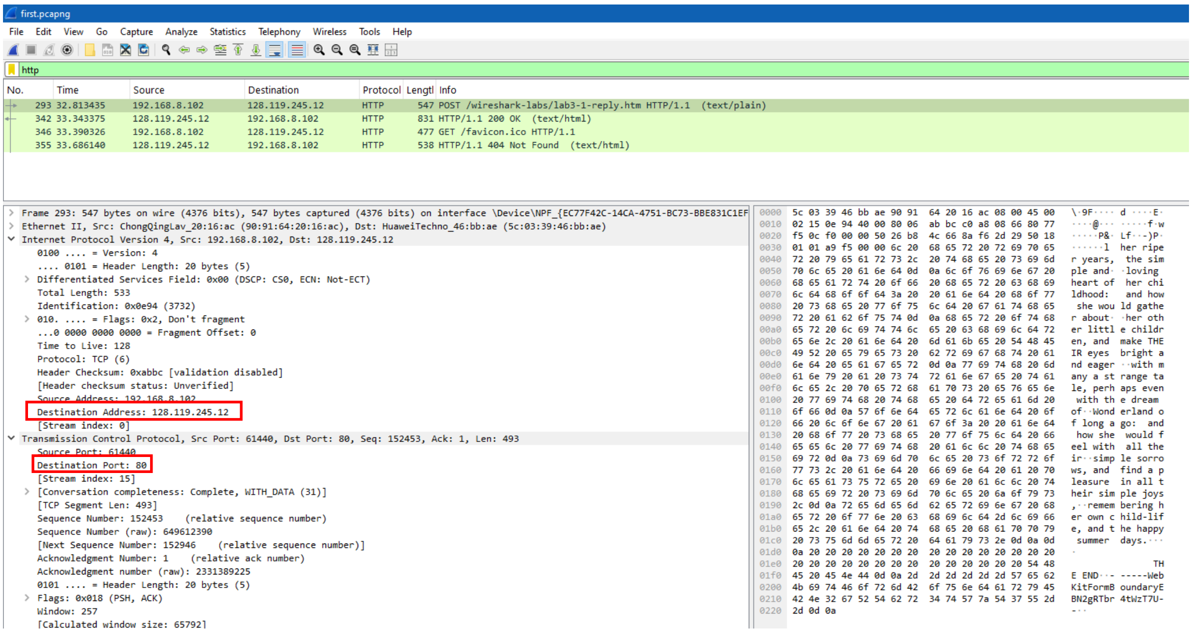
```
No.    Time        Source           Destination      Protocol Lengtl Info
   293 32.813435   192.168.8.102    128.119.245.12   HTTP      547 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)
   342 33.343375   128.119.245.12   192.168.8.102    HTTP      831 HTTP/1.1 200 OK  (text/html)
   346 33.390326   192.168.8.102    128.119.245.12   HTTP      477 GET /favicon.ico HTTP/1.1
   355 33.686140   128.119.245.12   192.168.8.102    HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 293: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface \Device\NPF_{EC77F42C-14CA-4751-BC73-BBE831C1EF
> Ethernet II, Src: ChongQingLav_20:16:ac (90:91:64:20:16:ac), Dst: HuaweiTechno_46:bb:ae (5c:03:39:46:bb:ae)
v Internet Protocol Version 4, Src: 192.168.8.102, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 533
    Identification: 0x0e94 (3732)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xabbc [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.8.102
    Destination Address: 128.119.245.12
    [Stream index: 0]
v Transmission Control Protocol, Src Port: 61440, Dst Port: 80, Seq: 152453, Ack: 1, Len: 493
    Source Port: 61440
    Destination Port: 80
    [Stream index: 15]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 493]
    Sequence Number: 152453    (relative sequence number)
    Sequence Number (raw): 649612390
    [Next Sequence Number: 152946    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2331389225
    0101 .... = Header Length: 20 bytes (5)
```

```
0000  5c 03 39 46 bb ae 90 91  64 20 16 ac 08 00 45 00   \·9F···· d ····E·
0010  02 15 0e 94 40 00 80 06  ab bc c0 a8 08 66 80 77   ····@··· ·····f·w
0020  f5 0c f0 00 00 50 26 b8  4c 66 8a f6 2d 29 50 18   ·····P&· Lf··-)P·
0030  01 01 a9 f5 00 00 6c 20  68 65 72 20 72 69 70 65   ······l  her ripe
0040  72 20 79 65 61 72 73 2c  20 74 68 65 20 73 69 6d   r years,  the sim
0050  70 6c 65 20 61 6e 64 0d  0a 6c 6f 76 69 6e 67 20   ple and· ·loving 
0060  68 65 61 72 74 20 6f 66  20 68 65 72 20 63 68 69   heart of  her chi
0070  6c 64 68 6f 6f 64 3a 20  20 61 6e 64 20 68 6f 77   ldhood:   and how
0080  20 73 68 65 20 77 6f 75  6c 64 20 67 61 74 68 65    she wou ld gathe
0090  72 20 61 62 6f 75 74 0d  0a 68 65 72 20 6f 74 68   r about· ·her oth
00a0  65 72 20 6c 69 74 74 6c  65 20 63 68 69 6c 64 72   er littl e childr
00b0  65 6e 2c 20 61 6e 64 20  6d 61 6b 65 20 54 48 45   en, and  make THE
00c0  49 52 20 65 79 65 73 20  62 72 69 67 68 74 20 61   IR eyes  bright a
00d0  6e 64 20 65 61 67 65 72  0d 0a 77 69 74 68 20 6d   nd eager ··with m
00e0  61 6e 79 20 61 20 73 74  72 61 6e 67 65 20 74 61   any a st range ta
00f0  6c 65 2c 20 70 65 72 68  61 70 73 20 65 76 65 6e   le, perh aps even
0100  20 77 69 74 68 20 74 68  65 20 64 72 65 61 6d 20    with th e dream 
0110  6f 66 0d 0a 57 6f 6e 64  65 72 6c 61 6e 64 20 6f   of··Wond erland o
0120  66 20 6c 6f 6e 67 20 61  67 6f 3a 20 20 61 6e 64   f long a go:  and
0130  20 68 6f 77 20 73 68 65  20 77 6f 75 6c 64 20 66    how she  would f
0140  65 65 6c 20 77 69 74 68  20 61 6c 6c 20 74 68 65   eel with  all the
0150  69 72 0d 0a 73 69 6d 70  6c 65 20 73 6f 72 72 6f   ir··simp le sorro
0160  77 73 2c 20 61 6e 64 20  66 69 6e 64 20 61 20 70   ws, and  find a p
0170  6c 65 61 73 75 72 65 20  69 6e 20 61 6c 6c 20 74   leasure  in all t
0180  68 65 69 72 20 73 69 6d  70 6c 65 20 6a 6f 79 73   heir sim ple joys
0190  2c 0d 0a 72 65 6d 65 6d  62 65 72 69 6e 67 20 68   ,··remem bering h
01a0  65 72 20 6f 77 6e 20 63  68 69 6c 64 2d 6c 69 66   er own c hild-lif
01b0  65 2c 20 61 6e 64 20 74  68 65 20 68 61 70 70 79   e, and t he happy
01c0  20 73 75 6d 6d 65 72 20  64 61 79 73 2e 0d 0a 0d    summer  days.···
01d0  0a 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20   ·
01e0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 54 48                 TH
01f0  45 20 45 4e 44 0d 0a 2d  2d 2d 2d 2d 2d 57 65 62   E END··- -----Web
0200  4b 69 74 46 6f 72 6d 42  6f 75 6e 64 61 72 79 45   KitFormB oundaryE
```

2. *What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?*

- Server IP – 128.119.245.12
- Server port - 80



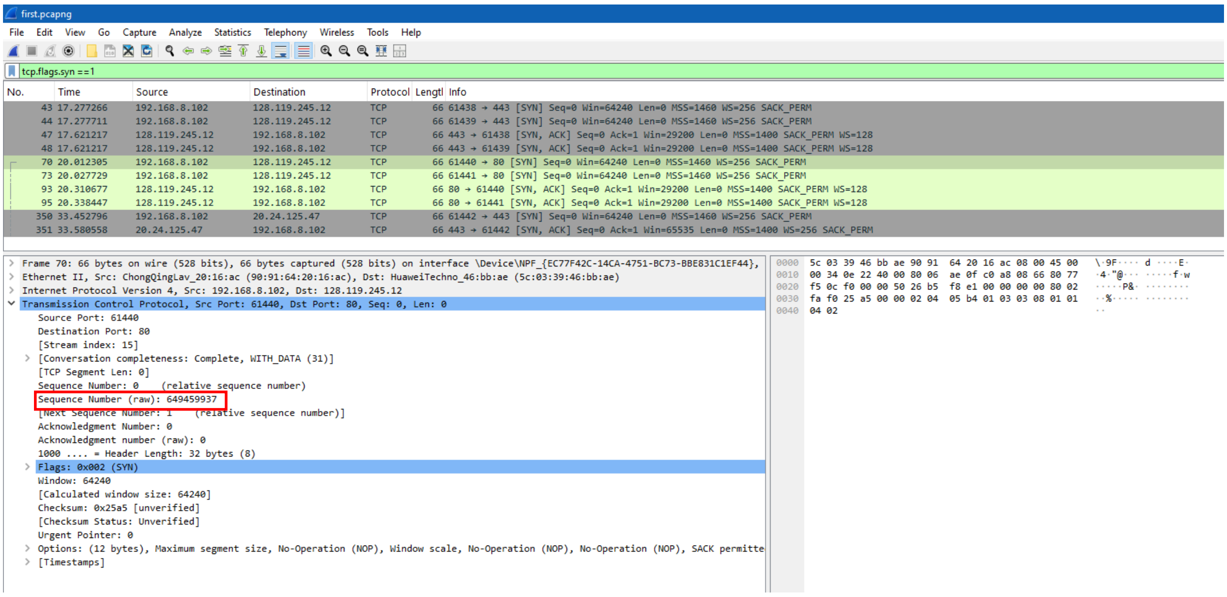
```
No.    Time        Source           Destination      Protocol Lengtl Info
   293 32.813435   192.168.8.102    128.119.245.12   HTTP      547 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)
   342 33.343375   128.119.245.12   192.168.8.102    HTTP      831 HTTP/1.1 200 OK  (text/html)
   346 33.390326   192.168.8.102    128.119.245.12   HTTP      477 GET /favicon.ico HTTP/1.1
   355 33.686140   128.119.245.12   192.168.8.102    HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 293: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface \Device\NPF_{EC77F42C-14CA-4751-BC73-BBE831C1EF
> Ethernet II, Src: ChongQingLav_20:16:ac (90:91:64:20:16:ac), Dst: HuaweiTechno_46:bb:ae (5c:03:39:46:bb:ae)
v Internet Protocol Version 4, Src: 192.168.8.102, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 533
    Identification: 0x0e94 (3732)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xabbc [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.8.102
    Destination Address: 128.119.245.12
    [Stream index: 0]
v Transmission Control Protocol, Src Port: 61440, Dst Port: 80, Seq: 152453, Ack: 1, Len: 493
    Source Port: 61440
    Destination Port: 80
    [Stream index: 15]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 493]
    Sequence Number: 152453    (relative sequence number)
    Sequence Number (raw): 649612390
    [Next Sequence Number: 152946    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2331389225
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 257
    [Calculated window size: 65792]
```

```
0000  5c 03 39 46 bb ae 90 91  64 20 16 ac 08 00 45 00   \·9F···· d ····E·
0010  02 15 0e 94 40 00 80 06  ab bc c0 a8 08 66 80 77   ····@··· ·····f·w
0020  f5 0c f0 00 00 50 26 b8  4c 66 8a f6 2d 29 50 18   ·····P&· Lf··-)P·
0030  01 01 a9 f5 00 00 6c 20  68 65 72 20 72 69 70 65   ······l  her ripe
0040  72 20 79 65 61 72 73 2c  20 74 68 65 20 73 69 6d   r years,  the sim
0050  70 6c 65 20 61 6e 64 0d  0a 6c 6f 76 69 6e 67 20   ple and· ·loving 
0060  68 65 61 72 74 20 6f 66  20 68 65 72 20 63 68 69   heart of  her chi
0070  6c 64 68 6f 6f 64 3a 20  20 61 6e 64 20 68 6f 77   ldhood:   and how
0080  20 73 68 65 20 77 6f 75  6c 64 20 67 61 74 68 65    she wou ld gathe
0090  72 20 61 62 6f 75 74 0d  0a 68 65 72 20 6f 74 68   r about· ·her oth
00a0  65 72 20 6c 69 74 74 6c  65 20 63 68 69 6c 64 72   er littl e childr
00b0  65 6e 2c 20 61 6e 64 20  6d 61 6b 65 20 54 48 45   en, and  make THE
00c0  49 52 20 65 79 65 73 20  62 72 69 67 68 74 20 61   IR eyes  bright a
00d0  6e 64 20 65 61 67 65 72  0d 0a 77 69 74 68 20 6d   nd eager ··with m
00e0  61 6e 79 20 61 20 73 74  72 61 6e 67 65 20 74 61   any a st range ta
00f0  6c 65 2c 20 70 65 72 68  61 70 73 20 65 76 65 6e   le, perh aps even
0100  20 77 69 74 68 20 74 68  65 20 64 72 65 61 6d 20    with th e dream 
0110  6f 66 0d 0a 57 6f 6e 64  65 72 6c 61 6e 64 20 6f   of··Wond erland o
0120  66 20 6c 6f 6e 67 20 61  67 6f 3a 20 20 61 6e 64   f long a go:  and
0130  20 68 6f 77 20 73 68 65  20 77 6f 75 6c 64 20 66    how she  would f
0140  65 65 6c 20 77 69 74 68  20 61 6c 6c 20 74 68 65   eel with  all the
0150  69 72 0d 0a 73 69 6d 70  6c 65 20 73 6f 72 72 6f   ir··simp le sorro
0160  77 73 2c 20 61 6e 64 20  66 69 6e 64 20 61 20 70   ws, and  find a p
0170  6c 65 61 73 75 72 65 20  69 6e 20 61 6c 6c 20 74   leasure  in all t
0180  68 65 69 72 20 73 69 6d  70 6c 65 20 6a 6f 79 73   heir sim ple joys
0190  2c 0d 0a 72 65 6d 65 6d  62 65 72 69 6e 67 20 68   ,··remem bering h
01a0  65 72 20 6f 77 6e 20 63  68 69 6c 64 2d 6c 69 66   er own c hild-lif
01b0  65 2c 20 61 6e 64 20 74  68 65 20 68 61 70 70 79   e, and t he happy
01c0  20 73 75 6d 6d 65 72 20  64 61 79 73 2e 0d 0a 0d    summer  days.···
01d0  0a 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20   ·
01e0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 54 48                 TH
01f0  45 20 45 4e 44 0d 0a 2d  2d 2d 2d 2d 2d 57 65 62   E END··- -----Web
0200  4b 69 74 46 6f 72 6d 42  6f 75 6e 64 61 72 79 45   KitFormB oundaryE
0210  42 4e 32 67 52 54 62 72  34 74 57 7a 54 37 55 2d   BN2gRTbr 4tWzT7U-
0220  2d 0d 0a                                           -··
```

3. *What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu?*

- Sequence number (raw) – 649459937


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

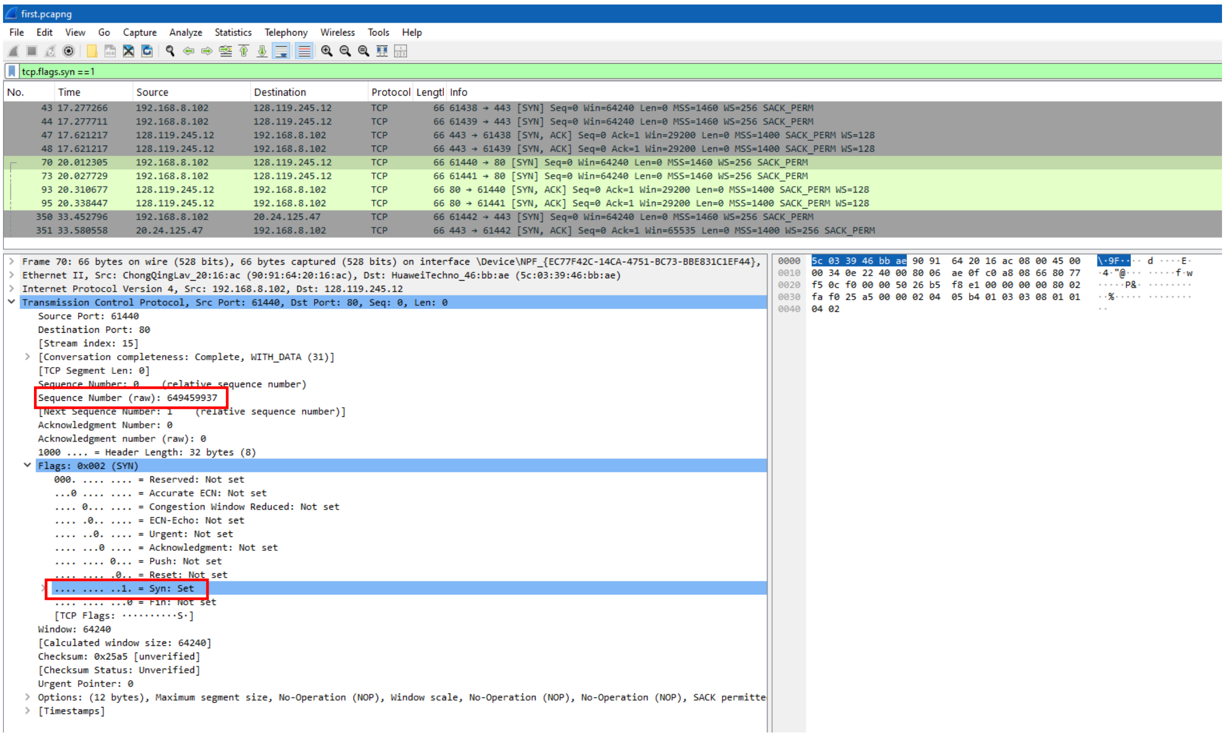
```
tcp.flags.syn ==1

No.     Time        Source          Destination     Protocol Lengtl Info
     43 17.277266   192.168.8.102   128.119.245.12  TCP      66 61438 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
     44 17.277711   192.168.8.102   128.119.245.12  TCP      66 61439 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
     47 17.621217   128.119.245.12  192.168.8.102   TCP      66 443 → 61438 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
     48 17.621217   128.119.245.12  192.168.8.102   TCP      66 443 → 61439 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
     70 20.012305   192.168.8.102   128.119.245.12  TCP      66 61440 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
     73 20.027729   192.168.8.102   128.119.245.12  TCP      66 61441 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
     93 20.310677   128.119.245.12  192.168.8.102   TCP      66 80 → 61440 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
     95 20.338447   128.119.245.12  192.168.8.102   TCP      66 80 → 61441 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
    350 33.452796   192.168.8.102   20.24.125.47    TCP      66 61442 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
    351 33.580558   20.24.125.47    192.168.8.102   TCP      66 443 → 61442 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM
```

```
> Frame 70: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{EC77F42C-14CA-4751-BC73-BBE831C1EF44},
> Ethernet II, Src: ChongQingLav_20:16:ac (90:91:64:20:16:ac), Dst: HuaweiTechno_46:bb:ae (5c:03:39:46:bb:ae)
> Internet Protocol Version 4, Src: 192.168.8.102, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 61440, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 61440
    Destination Port: 80
    [Stream index: 15]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 649459937
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x25a5 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitte
  > [Timestamps]
```

```
0000  5c 03 39 46 bb ae 90 91  64 20 16 ac 08 00 45 00   \·9F····d·····E·
0010  00 34 0e 22 40 00 80 06  ae 0f c0 a8 08 66 80 77   ·4·"@········f·w
0020  f5 0c f0 00 00 50 26 b5  f8 e1 00 00 00 00 80 02   ·····P&·········
0030  fa f0 25 a5 00 00 02 04  05 b4 01 03 03 08 01 01   ··%·············
0040  04 02                                              ··
```

What is it in this TCP segment that identifies the segment as a SYN segment?

- The SYN flag (0x002) is set in the Flags field.
  - SYN flag: Set to 1.
  - ACK flag: Set to 0.


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

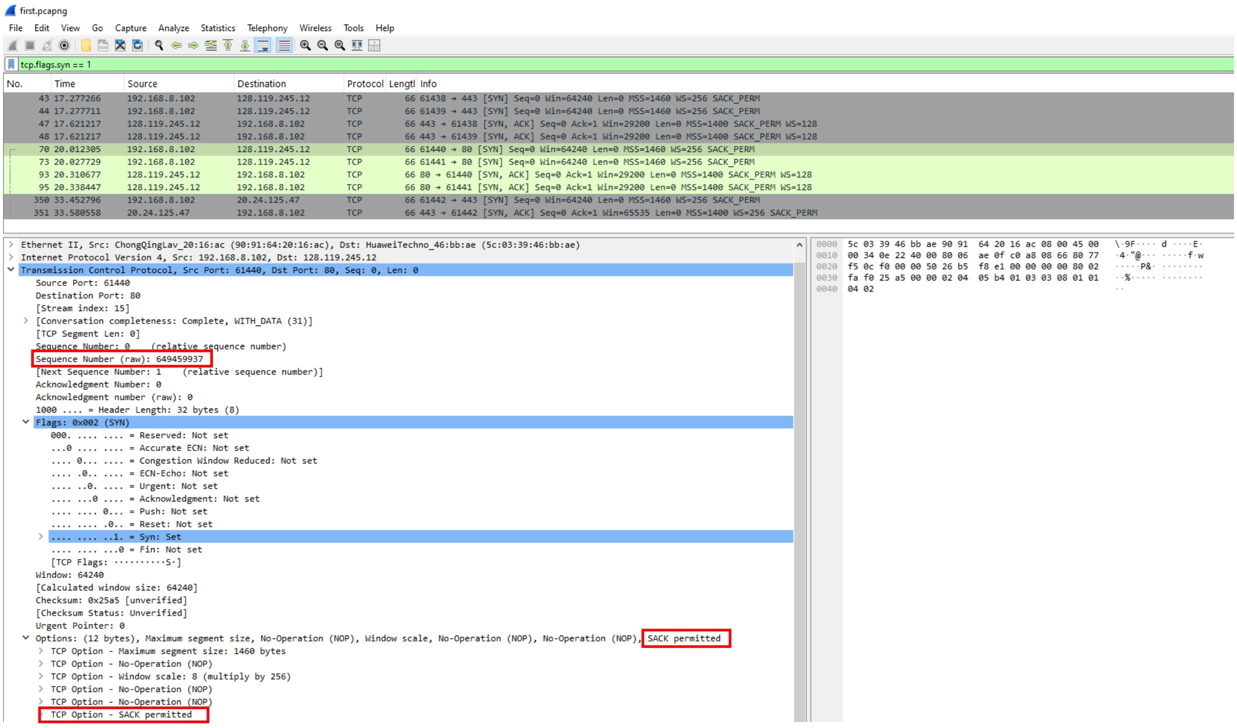
```
tcp.flags.syn ==1

No.     Time        Source          Destination     Protocol Lengtl Info
     43 17.277266   192.168.8.102   128.119.245.12  TCP      66 61438 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
     44 17.277711   192.168.8.102   128.119.245.12  TCP      66 61439 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
     47 17.621217   128.119.245.12  192.168.8.102   TCP      66 443 → 61438 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
     48 17.621217   128.119.245.12  192.168.8.102   TCP      66 443 → 61439 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
     70 20.012305   192.168.8.102   128.119.245.12  TCP      66 61440 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
     73 20.027729   192.168.8.102   128.119.245.12  TCP      66 61441 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
     93 20.310677   128.119.245.12  192.168.8.102   TCP      66 80 → 61440 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
     95 20.338447   128.119.245.12  192.168.8.102   TCP      66 80 → 61441 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
    350 33.452796   192.168.8.102   20.24.125.47    TCP      66 61442 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
    351 33.580558   20.24.125.47    192.168.8.102   TCP      66 443 → 61442 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM
```

```
> Frame 70: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{EC77F42C-14CA-4751-BC73-BBE831C1EF44},
> Ethernet II, Src: ChongQingLav_20:16:ac (90:91:64:20:16:ac), Dst: HuaweiTechno_46:bb:ae (5c:03:39:46:bb:ae)
> Internet Protocol Version 4, Src: 192.168.8.102, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 61440, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 61440
    Destination Port: 80
    [Stream index: 15]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 649459937
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  v Flags: 0x002 (SYN)
       000. .... .... = Reserved: Not set
       ...0 .... .... = Accurate ECN: Not set
       .... 0... .... = Congestion Window Reduced: Not set
       .... .0.. .... = ECN-Echo: Not set
       .... ..0. .... = Urgent: Not set
       .... ...0 .... = Acknowledgment: Not set
       .... .... 0... = Push: Not set
       .... .... .0.. = Reset: Not set
     > .... .... ..1. = Syn: Set
       .... .... ...0 = Fin: Not set
       [TCP Flags: ··········S·]
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x25a5 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitte
  > [Timestamps]
```

```
0000  5c 03 39 46 bb ae 90 91  64 20 16 ac 08 00 45 00   \·9F····d·····E·
0010  00 34 0e 22 40 00 80 06  ae 0f c0 a8 08 66 80 77   ·4·"@········f·w
0020  f5 0c f0 00 00 50 26 b5  f8 e1 00 00 00 00 80 02   ·····P&·········
0030  fa f0 25 a5 00 00 02 04  05 b4 01 03 03 08 01 01   ··%·············
0040  04 02                                              ··
```

Will the TCP receiver in this session be able to use Selective Acknowledgments?

- Yes, because the SACK_PERM (Selective Acknowledgment Permitted) option is present.


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

tcp.flags.syn == 1

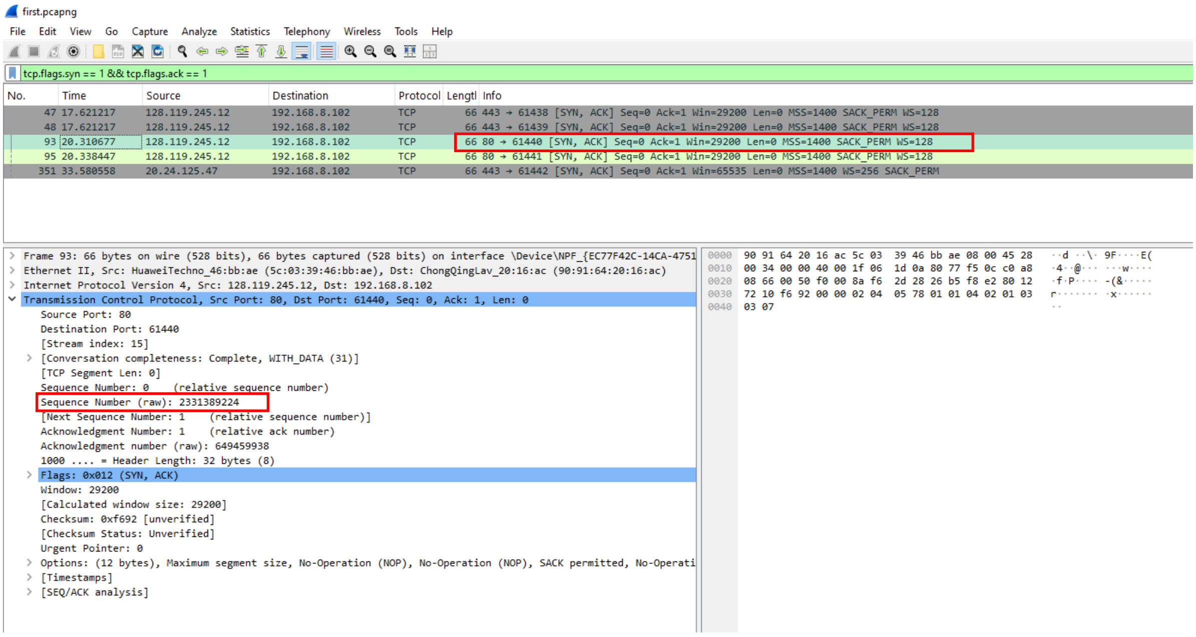
```
No.  Time       Source          Destination     Protocol Lengtl Info
  43 17.277266  192.168.8.102   128.119.245.12  TCP      66 61438 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  44 17.277711  192.168.8.102   128.119.245.12  TCP      66 61439 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  47 17.621217  128.119.245.12  192.168.8.102   TCP      66 443 → 61438 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
  48 17.621217  128.119.245.12  192.168.8.102   TCP      66 443 → 61439 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
  70 20.012305  192.168.8.102   128.119.245.12  TCP      66 61440 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  73 20.027729  192.168.8.102   128.119.245.12  TCP      66 61441 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  93 20.310677  128.119.245.12  192.168.8.102   TCP      66 80 → 61440 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
  95 20.338447  128.119.245.12  192.168.8.102   TCP      66 80 → 61441 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
 350 33.452796  192.168.8.102   20.24.125.47    TCP      66 61442 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 351 33.580558  20.24.125.47    192.168.8.102   TCP      66 443 → 61442 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM
```

```
> Ethernet II, Src: ChongQingLav_20:16:ac (90:91:64:20:16:ac), Dst: HuaweiTechno_46:bb:ae (5c:03:39:46:bb:ae)
> Internet Protocol Version 4, Src: 192.168.8.102, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 61440, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 61440
    Destination Port: 80
    [Stream index: 15]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 649459937
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  v Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Accurate ECN: Not set
      .... 0... .... = Congestion Window Reduced: Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    > .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ··········S·]
    Window: 64240
    [Calculated window size: 64240]
    Checksum: 0x25a5 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  v Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
    > TCP Option - Maximum segment size: 1460 bytes
    > TCP Option - No-Operation (NOP)
    > TCP Option - Window scale: 8 (multiply by 256)
    > TCP Option - No-Operation (NOP)
    > TCP Option - No-Operation (NOP)
    > TCP Option - SACK permitted
```

```
0000  5c 03 39 46 bb ae 90 91  64 20 16 ac 08 00 45 00   \·9F···· d ····E·
0010  00 34 0e 22 40 00 80 06  ae 0f c0 a8 08 66 80 77   ·4·"@··· ·····f·w
0020  f5 0c f0 00 00 50 26 b5  f8 e1 00 00 00 00 80 02   ·····P&· ········
0030  fa f0 25 a5 00 00 02 04  05 b4 01 03 03 08 01 01   ··%····· ········
0040  04 02                                              ··
```

4. *What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN?*

- Sequence number – 0 (relative number)
- Sequence number (raw) – 2331389224


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

tcp.flags.syn == 1 && tcp.flags.ack == 1

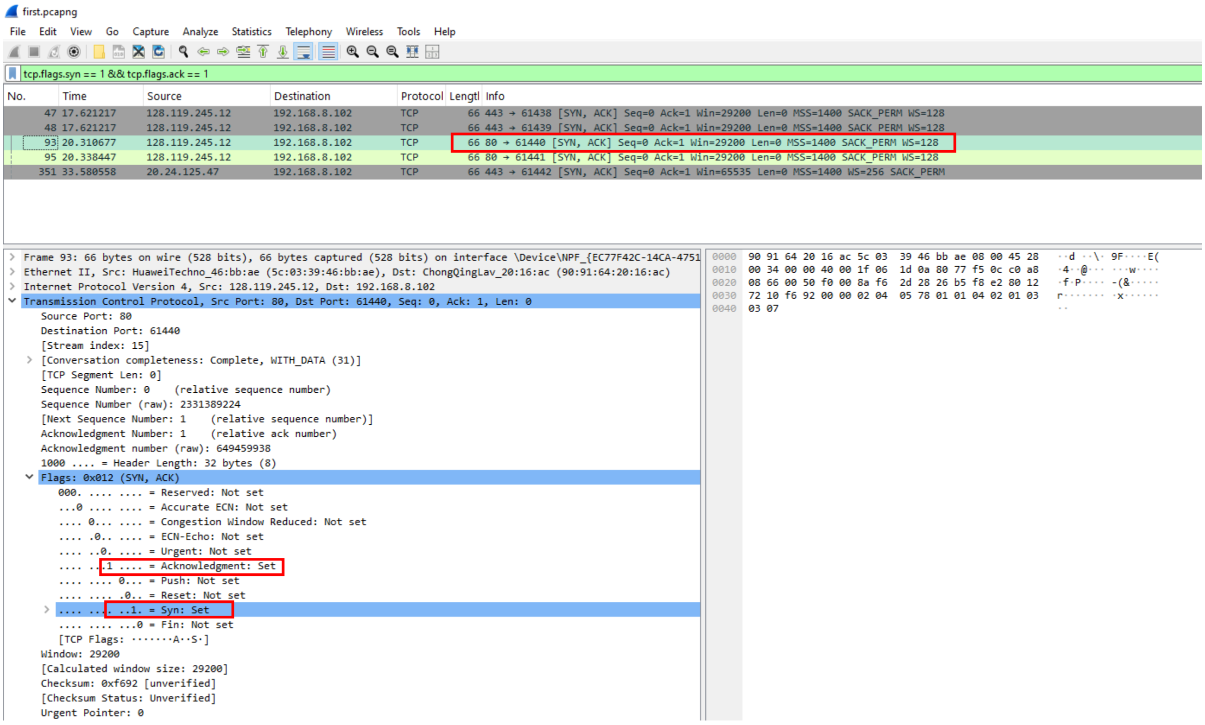
```
No.  Time       Source          Destination     Protocol Lengtl Info
  47 17.621217  128.119.245.12  192.168.8.102   TCP      66 443 → 61438 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
  48 17.621217  128.119.245.12  192.168.8.102   TCP      66 443 → 61439 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
  93 20.310677  128.119.245.12  192.168.8.102   TCP      66 80 → 61440 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
  95 20.338447  128.119.245.12  192.168.8.102   TCP      66 80 → 61441 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
 351 33.580558  20.24.125.47    192.168.8.102   TCP      66 443 → 61442 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM
```

```
> Frame 93: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{EC77F42C-14CA-4751
> Ethernet II, Src: HuaweiTechno_46:bb:ae (5c:03:39:46:bb:ae), Dst: ChongQingLav_20:16:ac (90:91:64:20:16:ac)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.8.102
v Transmission Control Protocol, Src Port: 80, Dst Port: 61440, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 61440
    [Stream index: 15]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2331389224
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 649459938
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x012 (SYN, ACK)
    Window: 29200
    [Calculated window size: 29200]
    Checksum: 0xf692 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operati
  > [Timestamps]
  > [SEQ/ACK analysis]
```

```
0000  90 91 64 20 16 ac 5c 03  39 46 bb ae 08 00 45 28   ··d ··\· 9F····E(
0010  00 34 00 00 40 00 1f 06  1d 0a 80 77 f5 0c c0 a8   ·4··@··· ···w····
0020  08 66 00 50 f0 00 8a f6  2d 28 26 b5 f8 e2 80 12   ·f·P···· -(&·····
0030  72 10 f6 92 00 00 02 04  05 78 01 01 04 02 01 03   r······· ·x······
0040  03 07                                              ··
```

What is it in the segment that identifies the segment as a SYNACK segment?

- The segment is identified as a SYNACK segment by the TCP flags:
  - ✓ SYN flag: Set to 1.
  - ✓ ACK flag: Set to 1.
- The presence of both flags (SYN=1 and ACK=1) in the TCP header identifies the segment as a SYNACK segment.


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

tcp.flags.syn == 1 && tcp.flags.ack == 1

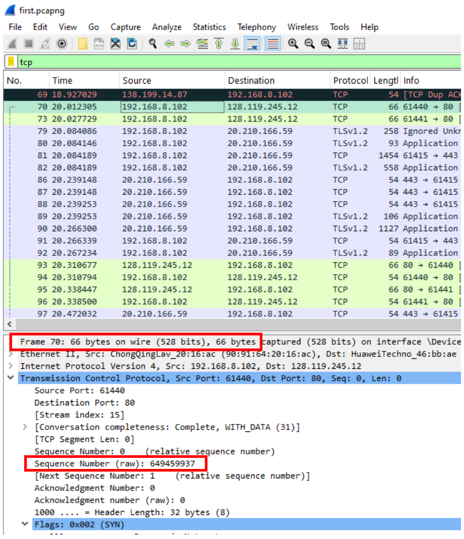
```
No.   Time       Source          Destination     Protocol Lengtl Info
   47 17.621217  128.119.245.12  192.168.8.102   TCP          66 443 → 61438 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
   48 17.621217  128.119.245.12  192.168.8.102   TCP          66 443 → 61439 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
   93 20.310677  128.119.245.12  192.168.8.102   TCP          66 80 → 61440 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
   95 20.338447  128.119.245.12  192.168.8.102   TCP          66 80 → 61441 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
  351 33.580558  20.24.125.47    192.168.8.102   TCP          66 443 → 61442 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM
```

```
> Frame 93: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{EC77F42C-14CA-4751
> Ethernet II, Src: HuaweiTechno_46:bb:ae (5c:03:39:46:bb:ae), Dst: ChongQingLav_20:16:ac (90:91:64:20:16:ac)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.8.102
v Transmission Control Protocol, Src Port: 80, Dst Port: 61440, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 61440
    [Stream index: 15]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2331389224
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 649459938
    1000 .... = Header Length: 32 bytes (8)
  v Flags: 0x012 (SYN, ACK)
       000. .... .... = Reserved: Not set
       ...0 .... .... = Accurate ECN: Not set
       .... 0... .... = Congestion Window Reduced: Not set
       .... .0.. .... = ECN-Echo: Not set
       .... ..0. .... = Urgent: Not set
       .... ...1 .... = Acknowledgment: Set
       .... .... 0... = Push: Not set
       .... .... .0.. = Reset: Not set
     > .... .... ..1. = Syn: Set
       .... .... ...0 = Fin: Not set
       [TCP Flags: ·······A··S·]
    Window: 29200
    [Calculated window size: 29200]
    Checksum: 0xf692 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
```

```
0000  90 91 64 20 16 ac 5c 03  39 46 bb ae 08 00 45 28   ··d ··\· 9F····E(
0010  00 34 00 00 40 00 1f 06  1d 0a 80 77 f5 0c c0 a8   ·4··@··· ···w····
0020  08 66 00 50 f0 00 8a f6  2d 28 26 b5 f8 e2 80 12   ·f·P···· -(&·····
0030  72 10 f6 92 00 00 02 04  05 78 01 01 04 02 01 03   r······· ·x······
0040  03 07                                              ··
```

What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value?

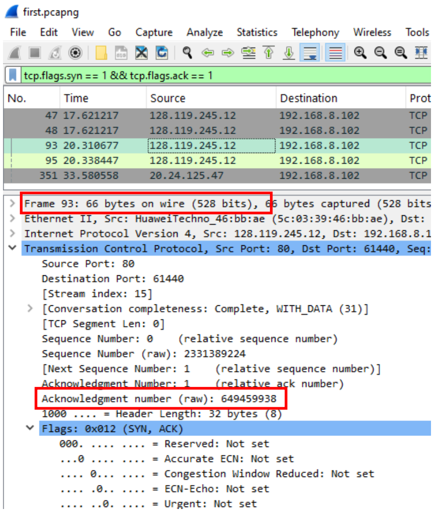
- Acknowledgement Number (raw): 649459938
- It was calculated as Client's Initial Sequence Number + 1 (649459937+ 1 = 649459938)


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

tcp

```
No.   Time       Source          Destination     Protocol Lengtl Info
   69 18.927029  138.199.14.87   192.168.8.102   TCP          54 [TCP Dup ACK
   70 20.012305  192.168.8.102   128.119.245.12  TCP          66 61440 → 80 [
   73 20.027729  192.168.8.102   128.119.245.12  TCP          66 61441 → 80 [
   79 20.084086  192.168.8.102   20.210.166.59   TLSv1.2     258 Ignored Unkr
   80 20.084146  192.168.8.102   20.210.166.59   TLSv1.2      93 Application
   81 20.084189  192.168.8.102   20.210.166.59   TCP        1454 61415 → 443
   82 20.084189  192.168.8.102   20.210.166.59   TLSv1.2     558 Application
   86 20.239148  20.210.166.59   192.168.8.102   TCP          54 443 → 61415
   87 20.239148  20.210.166.59   192.168.8.102   TCP          54 443 → 61415
   88 20.239253  20.210.166.59   192.168.8.102   TCP          54 443 → 61415
   89 20.239253  20.210.166.59   192.168.8.102   TLSv1.2     106 Application
   90 20.266300  20.210.166.59   192.168.8.102   TLSv1.2    1127 Application
   91 20.266339  192.168.8.102   20.210.166.59   TCP          54 61415 → 443
   92 20.267234  192.168.8.102   20.210.166.59   TLSv1.2      89 Application
   93 20.310677  128.119.245.12  192.168.8.102   TCP          66 80 → 61440 [
   94 20.310794  192.168.8.102   128.119.245.12  TCP          54 61440 → 80 [
   95 20.338447  128.119.245.12  192.168.8.102   TCP          66 80 → 61441 [
   96 20.338500  192.168.8.102   128.119.245.12  TCP          54 61441 → 80 [
   97 20.472032  20.210.166.59   192.168.8.102   TCP          54 443 → 61415
```

```
> Frame 70: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device
> Ethernet II, Src: ChongQingLav_20:16:ac (90:91:64:20:16:ac), Dst: HuaweiTechno_46:bb:ae
> Internet Protocol Version 4, Src: 192.168.8.102, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 61440, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 61440
    Destination Port: 80
    [Stream index: 15]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 649459937
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  v Flags: 0x002 (SYN)
```


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

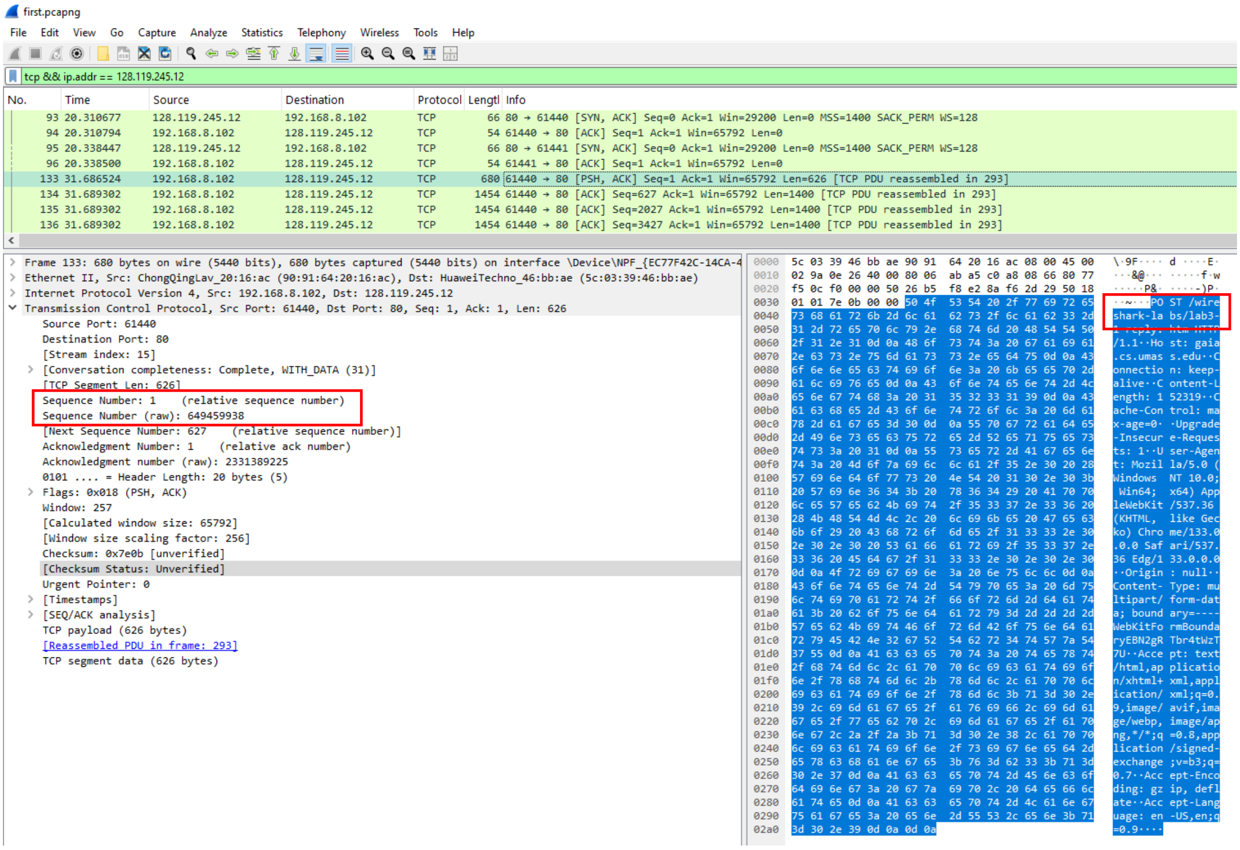
tcp.flags.syn == 1 && tcp.flags.ack == 1

```
No.   Time       Source          Destination     Prot
   47 17.621217  128.119.245.12  192.168.8.102   TCP
   48 17.621217  128.119.245.12  192.168.8.102   TCP
   93 20.310677  128.119.245.12  192.168.8.102   TCP
   95 20.338447  128.119.245.12  192.168.8.102   TCP
  351 33.580558  20.24.125.47    192.168.8.102   TCP
```

```
> Frame 93: 66 bytes on wire (528 bits), 66 bytes captured (528 bits
> Ethernet II, Src: HuaweiTechno_46:bb:ae (5c:03:39:46:bb:ae), Dst:
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.8.1
v Transmission Control Protocol, Src Port: 80, Dst Port: 61440, Seq:
    Source Port: 80
    Destination Port: 61440
    [Stream index: 15]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2331389224
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 649459938
    1000 .... = Header Length: 32 bytes (8)
  v Flags: 0x012 (SYN, ACK)
       000. .... .... = Reserved: Not set
       ...0 .... .... = Accurate ECN: Not set
       .... 0... .... = Congestion Window Reduced: Not set
       .... .0.. .... = ECN-Echo: Not set
       .... ..0. .... = Urgent: Not set
```

5. *What is the sequence number of the TCP segment containing the header of the HTTP POST command?*

- The sequence number of the **TCP segment is 1** (relative sequence number) or **649459938** (raw sequence number).



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

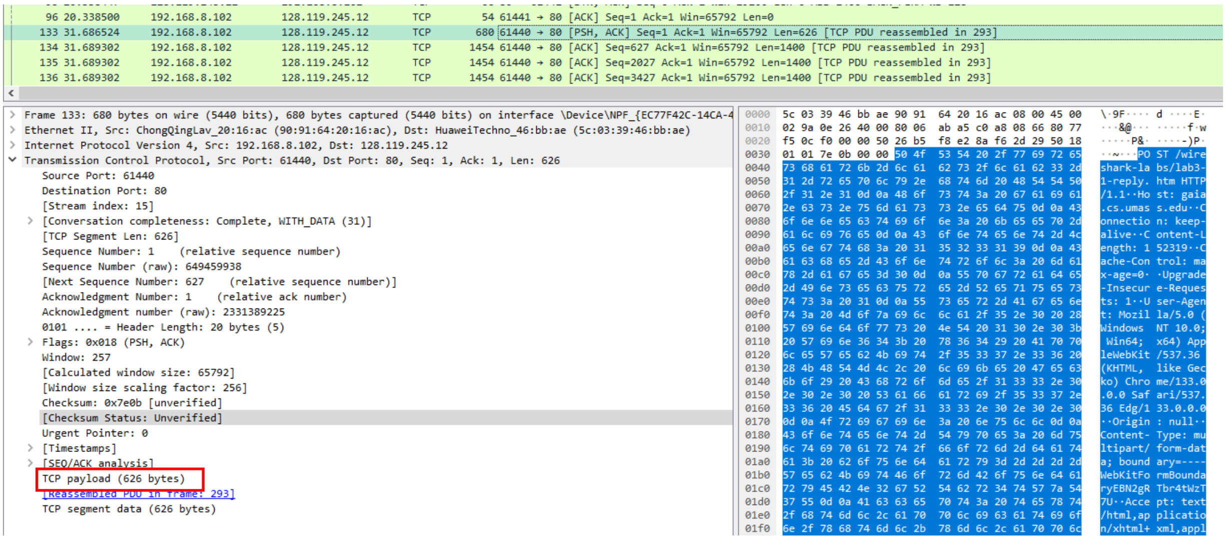
```
tcp && ip.addr == 128.119.245.12

No.   Time       Source          Destination     Protocol Lengtl Info
   93 20.310677  128.119.245.12  192.168.8.102   TCP        66 80 → 61440 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
   94 20.310794  192.168.8.102   128.119.245.12  TCP        54 61440 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
   95 20.338447  128.119.245.12  192.168.8.102   TCP        66 80 → 61441 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
   96 20.338500  192.168.8.102   128.119.245.12  TCP        54 61441 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
  133 31.686524  192.168.8.102   128.119.245.12  TCP       680 61440 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65792 Len=626 [TCP PDU reassembled in 293]
  134 31.689302  192.168.8.102   128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=627 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
  135 31.689302  192.168.8.102   128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=2027 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
  136 31.689302  192.168.8.102   128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=3427 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
```

```
> Frame 133: 680 bytes on wire (5440 bits), 680 bytes captured (5440 bits) on interface \Device\NPF_{EC77F42C-14CA-4
> Ethernet II, Src: ChongQingLav_20:16:ac (90:91:64:20:16:ac), Dst: HuaweiTechno_46:bb:ae (5c:03:39:46:bb:ae)
> Internet Protocol Version 4, Src: 192.168.8.102, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 61440, Dst Port: 80, Seq: 1, Ack: 1, Len: 626
    Source Port: 61440
    Destination Port: 80
    [Stream index: 15]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 626]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 649459938
    [Next Sequence Number: 627    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2331389225
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 257
    [Calculated window size: 65792]
    [Window size scaling factor: 256]
    Checksum: 0x7e0b [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (626 bytes)
    [Reassembled PDU in frame: 293]
    TCP segment data (626 bytes)
```

```
0000  5c 03 39 46 bb ae 90 91  64 20 16 ac 08 00 45 00   \·9F···· d ····E·
0010  02 9a 0e 26 40 00 80 06  ab a5 c0 a8 08 66 80 77   ···&@··· ·····f·w
0020  f5 0c f0 00 00 50 26 b5  f8 e2 8a f6 2d 29 50 18   ·····P&· ····-)P·
0030  01 01 7e 0b 00 00 50 4f  53 54 20 2f 77 69 72 65   ··~···PO ST /wire
0040  73 68 61 72 6b 2d 6c 61  62 73 2f 6c 61 62 33 2d   shark-la bs/lab3-
0050  31 2d 72 65 70 6c 79 2e  68 74 6d 20 48 54 54 50   1-reply. htm HTTP
0060  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 67 61 69 61   /1.1··Ho st: gaia
0070  2e 63 73 2e 75 6d 61 73  73 2e 65 64 75 0d 0a 43   .cs.umas s.edu··C
0080  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b 65 65 70 2d   onnectio n: keep-
0090  61 6c 69 76 65 0d 0a 43  6f 6e 74 65 6e 74 2d 4c   alive··C ontent-L
00a0  65 6e 67 74 68 3a 20 31  35 32 33 31 39 0d 0a 43   ength: 1 52319··C
00b0  61 63 68 65 2d 43 6f 6e  74 72 6f 6c 3a 20 6d 61   ache-Con trol: ma
00c0  78 2d 61 67 65 3d 30 0d  0a 55 70 67 72 61 64 65   x-age=0· ·Upgrade
00d0  2d 49 6e 73 65 63 75 72  65 2d 52 65 71 75 65 73   -Insecur e-Reques
00e0  74 73 3a 20 31 0d 0a 55  73 65 72 2d 41 67 65 6e   ts: 1··U ser-Agen
00f0  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
0100  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows  NT 10.0;
0110  20 57 69 6e 36 34 3b 20  78 36 34 29 20 41 70 70    Win64;  x64) App
0120  6c 65 57 65 62 4b 69 74  2f 35 33 37 2e 33 36 20   leWebKit /537.36 
0130  28 4b 48 54 4d 4c 2c 20  6c 69 6b 65 20 47 65 63   (KHTML,  like Gec
0140  6b 6f 29 20 43 68 72 6f  6d 65 2f 31 33 33 2e 30   ko) Chro me/133.0
0150  2e 30 2e 30 20 53 61 66  61 72 69 2f 35 33 37 2e   .0.0 Saf ari/537.
0160  33 36 20 45 64 67 2f 31  33 33 2e 30 2e 30 2e 30   36 Edg/1 33.0.0.0
0170  0d 0a 4f 72 69 67 69 6e  3a 20 6e 75 6c 6c 0d 0a   ··Origin : null··
0180  43 6f 6e 74 65 6e 74 2d  54 79 70 65 3a 20 6d 75   Content- Type: mu
0190  6c 74 69 70 61 72 74 2f  66 6f 72 6d 2d 64 61 74   ltipart/ form-dat
01a0  61 3b 20 62 6f 75 6e 64  61 72 79 3d 2d 2d 2d 2d   a; bound ary=----
01b0  57 65 62 4b 69 74 46 6f  72 6d 42 6f 75 6e 64 61   WebKitFo rmBounda
01c0  72 79 45 42 4e 32 67 52  54 62 72 34 74 57 7a 54   ryEBN2gR Tbr4tWzT
01d0  37 55 0d 0a 41 63 63 65  70 74 3a 20 74 65 78 74   7U··Acce pt: text
01e0  2f 68 74 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   /html,ap plicatio
01f0  6e 2f 78 68 74 6d 6c 2b  78 6d 6c 2c 61 70 70 6c   n/xhtml+ xml,appl
0200  69 63 61 74 69 6f 6e 2f  78 6d 6c 3b 71 3d 30 2e   ication/ xml;q=0.
0210  39 2c 69 6d 61 67 65 2f  61 76 69 66 2c 69 6d 61   9,image/ avif,ima
0220  67 65 2f 77 65 62 70 2c  69 6d 61 67 65 2f 61 70   ge/webp, image/ap
0230  6e 67 2c 2a 2f 2a 3b 71  3d 30 2e 38 2c 61 70 70   ng,*/*;q =0.8,app
0240  6c 69 63 61 74 69 6f 6e  2f 73 69 67 6e 65 64 2d   lication /signed-
0250  65 78 63 68 61 6e 67 65  3b 76 3d 62 33 3b 71 3d   exchange ;v=b3;q=
0260  30 2e 37 0d 0a 41 63 63  65 70 74 2d 45 6e 63 6f   0.7··Acc ept-Enco
0270  64 69 6e 67 3a 20 67 7a  69 70 2c 20 64 65 66 6c   ding: gz ip, defl
0280  61 74 65 0d 0a 41 63 63  65 70 74 2d 4c 61 6e 67   ate··Acc ept-Lang
0290  75 61 67 65 3a 20 65 6e  2d 55 53 2c 65 6e 3b 71   uage: en -US,en;q
02a0  3d 30 2e 39 0d 0a 0d 0a                            =0.9····
```

How many bytes of data are contained in the payload (data) field of this TCP segment?

- **TCP payload - 626 bytes**



```
   96 20.338500  192.168.8.102   128.119.245.12  TCP        54 61441 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
  133 31.686524  192.168.8.102   128.119.245.12  TCP       680 61440 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65792 Len=626 [TCP PDU reassembled in 293]
  134 31.689302  192.168.8.102   128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=627 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
  135 31.689302  192.168.8.102   128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=2027 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
  136 31.689302  192.168.8.102   128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=3427 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
```

```
> Frame 133: 680 bytes on wire (5440 bits), 680 bytes captured (5440 bits) on interface \Device\NPF_{EC77F42C-14CA-4
> Ethernet II, Src: ChongQingLav_20:16:ac (90:91:64:20:16:ac), Dst: HuaweiTechno_46:bb:ae (5c:03:39:46:bb:ae)
> Internet Protocol Version 4, Src: 192.168.8.102, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 61440, Dst Port: 80, Seq: 1, Ack: 1, Len: 626
    Source Port: 61440
    Destination Port: 80
    [Stream index: 15]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 626]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 649459938
    [Next Sequence Number: 627    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2331389225
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 257
    [Calculated window size: 65792]
    [Window size scaling factor: 256]
    Checksum: 0x7e0b [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (626 bytes)
    [Reassembled PDU in frame: 293]
    TCP segment data (626 bytes)
```

```
0000  5c 03 39 46 bb ae 90 91  64 20 16 ac 08 00 45 00   \·9F···· d ····E·
0010  02 9a 0e 26 40 00 80 06  ab a5 c0 a8 08 66 80 77   ···&@··· ·····f·w
0020  f5 0c f0 00 00 50 26 b5  f8 e2 8a f6 2d 29 50 18   ·····P&· ····-)P·
0030  01 01 7e 0b 00 00 50 4f  53 54 20 2f 77 69 72 65   ··~···PO ST /wire
0040  73 68 61 72 6b 2d 6c 61  62 73 2f 6c 61 62 33 2d   shark-la bs/lab3-
0050  31 2d 72 65 70 6c 79 2e  68 74 6d 20 48 54 54 50   1-reply. htm HTTP
0060  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 67 61 69 61   /1.1··Ho st: gaia
0070  2e 63 73 2e 75 6d 61 73  73 2e 65 64 75 0d 0a 43   .cs.umas s.edu··C
0080  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b 65 65 70 2d   onnectio n: keep-
0090  61 6c 69 76 65 0d 0a 43  6f 6e 74 65 6e 74 2d 4c   alive··C ontent-L
00a0  65 6e 67 74 68 3a 20 31  35 32 33 31 39 0d 0a 43   ength: 1 52319··C
00b0  61 63 68 65 2d 43 6f 6e  74 72 6f 6c 3a 20 6d 61   ache-Con trol: ma
00c0  78 2d 61 67 65 3d 30 0d  0a 55 70 67 72 61 64 65   x-age=0· ·Upgrade
00d0  2d 49 6e 73 65 63 75 72  65 2d 52 65 71 75 65 73   -Insecur e-Reques
00e0  74 73 3a 20 31 0d 0a 55  73 65 72 2d 41 67 65 6e   ts: 1··U ser-Agen
00f0  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
0100  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows  NT 10.0;
0110  20 57 69 6e 36 34 3b 20  78 36 34 29 20 41 70 70    Win64;  x64) App
0120  6c 65 57 65 62 4b 69 74  2f 35 33 37 2e 33 36 20   leWebKit /537.36 
0130  28 4b 48 54 4d 4c 2c 20  6c 69 6b 65 20 47 65 63   (KHTML,  like Gec
0140  6b 6f 29 20 43 68 72 6f  6d 65 2f 31 33 33 2e 30   ko) Chro me/133.0
0150  2e 30 2e 30 20 53 61 66  61 72 69 2f 35 33 37 2e   .0.0 Saf ari/537.
0160  33 36 20 45 64 67 2f 31  33 33 2e 30 2e 30 2e 30   36 Edg/1 33.0.0.0
0170  0d 0a 4f 72 69 67 69 6e  3a 20 6e 75 6c 6c 0d 0a   ··Origin : null··
0180  43 6f 6e 74 65 6e 74 2d  54 79 70 65 3a 20 6d 75   Content- Type: mu
0190  6c 74 69 70 61 72 74 2f  66 6f 72 6d 2d 64 61 74   ltipart/ form-dat
01a0  61 3b 20 62 6f 75 6e 64  61 72 79 3d 2d 2d 2d 2d   a; bound ary=----
01b0  57 65 62 4b 69 74 46 6f  72 6d 42 6f 75 6e 64 61   WebKitFo rmBounda
01c0  72 79 45 42 4e 32 67 52  54 62 72 34 74 57 7a 54   ryEBN2gR Tbr4tWzT
01d0  37 55 0d 0a 41 63 63 65  70 74 3a 20 74 65 78 74   7U··Acce pt: text
01e0  2f 68 74 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   /html,ap plicatio
01f0  6e 2f 78 68 74 6d 6c 2b  78 6d 6c 2c 61 70 70 6c   n/xhtml+ xml,appl
```

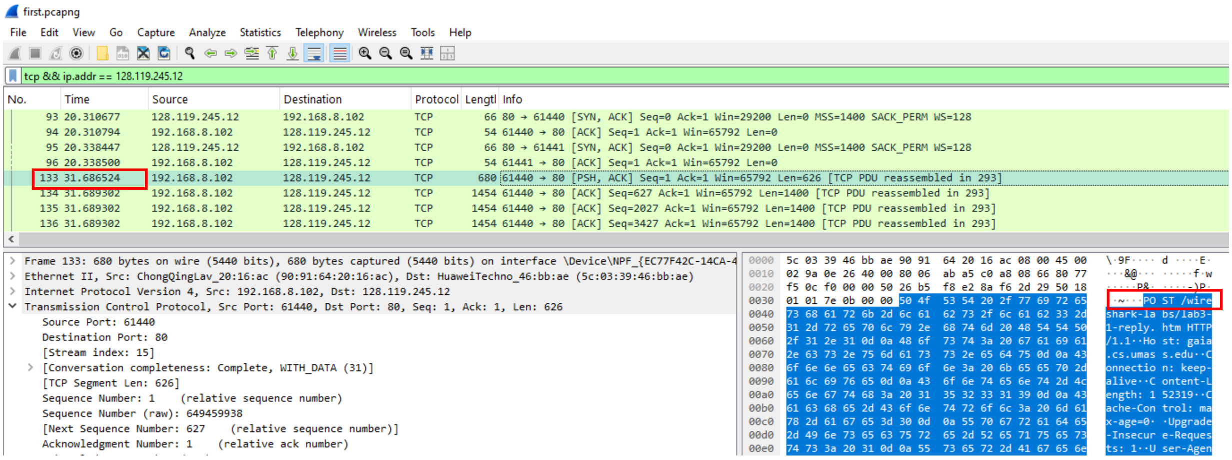
Did all of the data in the transferred file alice.txt fit into this single segment?

- **No**, it was divided into multiple segments.

6. *Consider the TCP segment containing the HTTP "POST" as the first segment in the data transfer part of the TCP connection.*

At what time was the first segment (the one containing the HTTP POST) in the data-transfer part of the TCP connection sent?

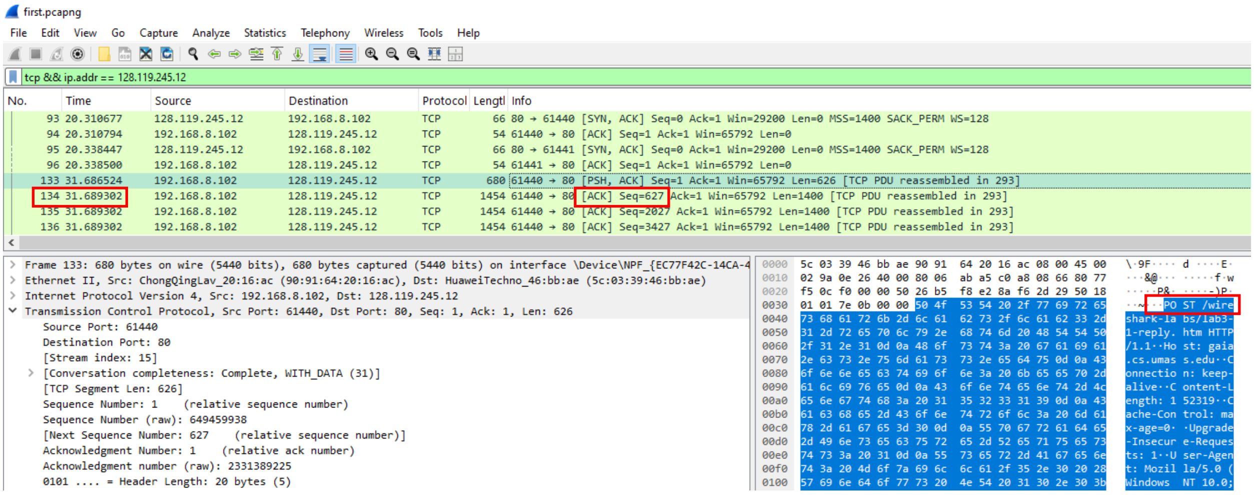
- The first segment containing the HTTP "POST" was sent at **31.686524 seconds**


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

```
tcp && ip.addr == 128.119.245.12

No.  Time       Source          Destination     Protocol Lengtl Info
  93 20.310677  128.119.245.12  192.168.8.102   TCP        66 80 → 61440 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
  94 20.310794  192.168.8.102   128.119.245.12  TCP        54 61440 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
  95 20.338447  128.119.245.12  192.168.8.102   TCP        66 80 → 61441 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
  96 20.338500  192.168.8.102   128.119.245.12  TCP        54 61441 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
 133 31.686524  192.168.8.102   128.119.245.12  TCP       680 61440 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65792 Len=626 [TCP PDU reassembled in 293]
 134 31.689302  192.168.8.102   128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=627 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
 135 31.689302  192.168.8.102   128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=2027 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
 136 31.689302  192.168.8.102   128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=3427 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]

> Frame 133: 680 bytes on wire (5440 bits), 680 bytes captured (5440 bits) on interface \Device\NPF_{EC77F42C-14CA-4
> Ethernet II, Src: ChongQingLav_20:16:ac (90:91:64:20:16:ac), Dst: HuaweiTechno_46:bb:ae (5c:03:39:46:bb:ae)
> Internet Protocol Version 4, Src: 192.168.8.102, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 61440, Dst Port: 80, Seq: 1, Ack: 1, Len: 626
    Source Port: 61440
    Destination Port: 80
    [Stream index: 15]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 626]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 649459938
    [Next Sequence Number: 627    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)

0000  5c 03 39 46 bb ae 90 91  64 20 16 ac 08 00 45 00   \·9F···· d ····E·
0010  02 9a 0e 26 40 00 80 06  ab a5 c0 a8 08 66 80 77   ···&@··· ·····f·w
0020  f5 0c f0 00 00 50 26 b5  f8 e2 8a f6 2d 29 50 18   ·····P&· ····-)P·
0030  01 01 7e 0b 00 00 50 4f  53 54 20 2f 77 69 72 65   ··~···PO ST /wire
0040  73 68 61 72 6b 2d 6c 61  62 73 2f 6c 61 62 33 2d   shark-la bs/lab3-
0050  31 2d 72 65 70 6c 79 2e  68 74 6d 20 48 54 54 50   1-reply. htm HTTP
0060  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 67 61 69 61   /1.1··Ho st: gaia
0070  2e 63 73 2e 75 6d 61 73  73 2e 65 64 75 0d 0a 43   .cs.umas s.edu··C
0080  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b 65 65 70 2d   onnectio n: keep-
0090  61 6c 69 76 65 0d 0a 43  6f 6e 74 65 6e 74 2d 4c   alive··C ontent-L
00a0  65 6e 67 74 68 3a 20 31  35 32 33 31 39 0d 0a 43   ength: 1 52319··C
00b0  61 63 68 65 2d 43 6f 6e  74 72 6f 6c 3a 20 6d 61   ache-Con trol: ma
00c0  78 2d 61 67 65 3d 30 0d  0a 55 70 67 72 61 64 65   x-age=0· ·Upgrade
00d0  2d 49 6e 73 65 63 75 72  65 2d 52 65 71 75 65 73   -Insecur e-Reques
00e0  74 73 3a 20 31 0d 0a 55  73 65 72 2d 41 67 65 6e   ts: 1··U ser-Agen
```

At what time was the ACK for this first data-containing segment received?

- The ACK for the first data-containing segment (HTTP POST) was received at: **31.689302 seconds**


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

```
tcp && ip.addr == 128.119.245.12

No.  Time       Source          Destination     Protocol Lengtl Info
  93 20.310677  128.119.245.12  192.168.8.102   TCP        66 80 → 61440 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
  94 20.310794  192.168.8.102   128.119.245.12  TCP        54 61440 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
  95 20.338447  128.119.245.12  192.168.8.102   TCP        66 80 → 61441 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128
  96 20.338500  192.168.8.102   128.119.245.12  TCP        54 61441 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
 133 31.686524  192.168.8.102   128.119.245.12  TCP       680 61440 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65792 Len=626 [TCP PDU reassembled in 293]
 134 31.689302  192.168.8.102   128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=627 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
 135 31.689302  192.168.8.102   128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=2027 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
 136 31.689302  192.168.8.102   128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=3427 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]

> Frame 133: 680 bytes on wire (5440 bits), 680 bytes captured (5440 bits) on interface \Device\NPF_{EC77F42C-14CA-4
> Ethernet II, Src: ChongQingLav_20:16:ac (90:91:64:20:16:ac), Dst: HuaweiTechno_46:bb:ae (5c:03:39:46:bb:ae)
> Internet Protocol Version 4, Src: 192.168.8.102, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 61440, Dst Port: 80, Seq: 1, Ack: 1, Len: 626
    Source Port: 61440
    Destination Port: 80
    [Stream index: 15]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 626]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 649459938
    [Next Sequence Number: 627    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2331389225
    0101 .... = Header Length: 20 bytes (5)

0000  5c 03 39 46 bb ae 90 91  64 20 16 ac 08 00 45 00   \·9F···· d ····E·
0010  02 9a 0e 26 40 00 80 06  ab a5 c0 a8 08 66 80 77   ···&@··· ·····f·w
0020  f5 0c f0 00 00 50 26 b5  f8 e2 8a f6 2d 29 50 18   ·····P&· ····-)P·
0030  01 01 7e 0b 00 00 50 4f  53 54 20 2f 77 69 72 65   ··~···PO ST /wire
0040  73 68 61 72 6b 2d 6c 61  62 73 2f 6c 61 62 33 2d   shark-la bs/lab3-
0050  31 2d 72 65 70 6c 79 2e  68 74 6d 20 48 54 54 50   1-reply. htm HTTP
0060  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 67 61 69 61   /1.1··Ho st: gaia
0070  2e 63 73 2e 75 6d 61 73  73 2e 65 64 75 0d 0a 43   .cs.umas s.edu··C
0080  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b 65 65 70 2d   onnectio n: keep-
0090  61 6c 69 76 65 0d 0a 43  6f 6e 74 65 6e 74 2d 4c   alive··C ontent-L
00a0  65 6e 67 74 68 3a 20 31  35 32 33 31 39 0d 0a 43   ength: 1 52319··C
00b0  61 63 68 65 2d 43 6f 6e  74 72 6f 6c 3a 20 6d 61   ache-Con trol: ma
00c0  78 2d 61 67 65 3d 30 0d  0a 55 70 67 72 61 64 65   x-age=0· ·Upgrade
00d0  2d 49 6e 73 65 63 75 72  65 2d 52 65 71 75 65 73   -Insecur e-Reques
00e0  74 73 3a 20 31 0d 0a 55  73 65 72 2d 41 67 65 6e   ts: 1··U ser-Agen
00f0  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
0100  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows  NT 10.0;
```

What is the RTT for this first data-containing segment?

RTT = Time ACK received - Time packet sent

RTT = 31.689302 - 31.686524

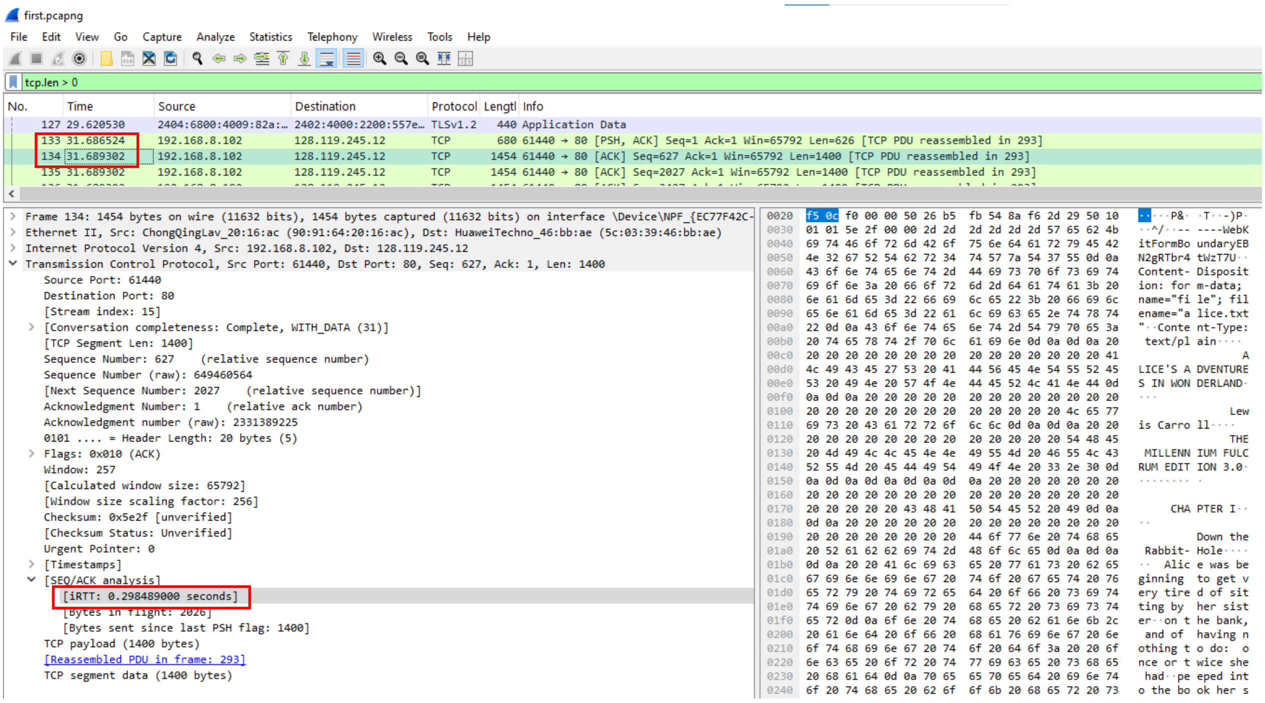
= 0.002778 seconds (or 2.778 ms)

RTT of Frame 133–134 (~2.778 ms)

- This is the **measured RTT for the first data packet** (Frame 133) and its **ACK (Frame 134)**.
- It shows the time **between sending data and receiving an acknowledgment**.

iRTT (0.298489 sec) in Frame 134

- **iRTT is the Initial RTT estimated by Wireshark**.
- It is usually based on the **TCP handshake (SYN-SYN/ACK-ACK packets)**.
- It estimates how long it takes for the **first connection setup**.



tcp.len > 0

```
No.   Time       Source                Destination          Protocol Lengtl Info
  127 29.620530  2404:6800:4009:82a:…  2402:4000:2200:557e… TLSv1.2   440 Application Data
  133 31.686524  192.168.8.102         128.119.245.12       TCP       680 61440 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65792 Len=626 [TCP PDU reassembled in 293]
  134 31.689302  192.168.8.102         128.119.245.12       TCP      1454 61440 → 80 [ACK] Seq=627 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
  135 31.689302  192.168.8.102         128.119.245.12       TCP      1454 61440 → 80 [ACK] Seq=2027 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
```

```
> Frame 134: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface \Device\NPF_{EC77F42C-
> Ethernet II, Src: ChongQingLav_20:16:ac (90:91:64:20:16:ac), Dst: HuaweiTechno_46:bb:ae (5c:03:39:46:bb:ae)
> Internet Protocol Version 4, Src: 192.168.8.102, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 61440, Dst Port: 80, Seq: 627, Ack: 1, Len: 1400
     Source Port: 61440
     Destination Port: 80
     [Stream index: 15]
   > [Conversation completeness: Complete, WITH_DATA (31)]
     [TCP Segment Len: 1400]
     Sequence Number: 627    (relative sequence number)
     Sequence Number (raw): 649460564
     [Next Sequence Number: 2027    (relative sequence number)]
     Acknowledgment Number: 1    (relative ack number)
     Acknowledgment number (raw): 2331389225
     0101 .... = Header Length: 20 bytes (5)
   > Flags: 0x010 (ACK)
     Window: 257
     [Calculated window size: 65792]
     [Window size scaling factor: 256]
     Checksum: 0x5e2f [unverified]
     [Checksum Status: Unverified]
     Urgent Pointer: 0
   > [Timestamps]
   v [SEQ/ACK analysis]
        [iRTT: 0.298489000 seconds]
        [Bytes in flight: 2026]
        [Bytes sent since last PSH flag: 1400]
     TCP payload (1400 bytes)
     [Reassembled PDU in frame: 293]
     TCP segment data (1400 bytes)
```

```
0020  f5 0c f0 00 00 50 26 b5  fb 54 8a f6 2d 29 50 10   ·····P&· ·T··-)P·
0030  01 01 5e 2f 00 00 2d 2d  2d 2d 2d 2d 57 65 62 4b   ··^/··-- ----WebK
0040  69 74 46 6f 72 6d 42 6f  75 6e 64 61 72 79 45 42   itFormBo undaryEB
0050  4e 32 67 52 54 62 72 34  74 57 7a 54 37 55 0d 0a   N2gRTbr4 tWzT7U··
0060  43 6f 6e 74 65 6e 74 2d  44 69 73 70 6f 73 69 74   Content- Disposit
0070  69 6f 6e 3a 20 66 6f 72  6d 2d 64 61 74 61 3b 20   ion: for m-data; 
0080  6e 61 6d 65 3d 22 66 69  6c 65 22 3b 20 66 69 6c   name="fi le"; fil
0090  65 6e 61 6d 65 3d 22 61  6c 69 63 65 2e 74 78 74   ename="a lice.txt
00a0  22 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   "··Conte nt-Type:
00b0  20 74 65 78 74 2f 70 6c  61 69 6e 0d 0a 0d 0a 20    text/pl ain···· 
00c0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 41                  A
00d0  4c 49 43 45 27 53 20 41  44 56 45 4e 54 55 52 45   LICE'S A DVENTURE
00e0  53 20 49 4e 20 57 4f 4e  44 45 52 4c 41 4e 44 0d   S IN WON DERLAND·
00f0  0a 0d 0a 20 20 20 20 20  20 20 20 20 20 20 20 20   ···              
0100  20 20 20 20 20 20 20 20  20 20 20 20 20 4c 65 77                Lew
0110  69 73 20 43 61 72 72 6f  6c 6c 0d 0a 0d 0a 20 20   is Carro ll····  
0120  20 20 20 20 20 20 20 20  20 20 20 20 20 54 48 45                THE
0130  20 4d 49 4c 4c 45 4e 4e  49 55 4d 20 46 55 4c 43    MILLENN IUM FULC
0140  52 55 4d 20 45 44 49 54  49 4f 4e 20 33 2e 30 0d   RUM EDIT ION 3.0·
0150  0a 0d 0a 0d 0a 0d 0a 0d  0a 20 20 20 20 20 20 20   ········ ·       
0160  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20                    
0170  20 20 20 20 20 43 48 41  50 54 45 52 20 49 0d 0a        CHA PTER I··
0180  0d 0a 20 20 20 20 20 20  20 20 20 20 20 20 20 20   ··               
0190  20 20 20 20 20 20 20 20  44 6f 77 6e 20 74 68 65            Down the
01a0  20 52 61 62 62 69 74 2d  48 6f 6c 65 0d 0a 0d 0a    Rabbit- Hole····
01b0  0d 0a 20 20 41 6c 69 63  65 20 77 61 73 20 62 65   ··  Alic e was be
01c0  67 69 6e 6e 69 6e 67 20  74 6f 20 67 65 74 20 76   ginning  to get v
01d0  65 72 79 20 74 69 72 65  64 20 6f 66 20 73 69 74   ery tire d of sit
01e0  74 69 6e 67 20 62 79 20  68 65 72 20 73 69 73 74   ting by  her sist
01f0  65 72 0d 0a 6f 6e 20 74  68 65 20 62 61 6e 6b 2c   er··on t he bank,
0200  20 61 6e 64 20 6f 66 20  68 61 76 69 6e 67 20 6e    and of  having n
0210  6f 74 68 69 6e 67 20 74  6f 20 64 6f 3a 20 20 6f   othing t o do:  o
0220  6e 63 65 20 6f 72 20 74  77 69 63 65 20 73 68 65   nce or t wice she
0230  20 68 61 64 0d 0a 70 65  65 70 65 64 20 69 6e 74    had··pe eped int
0240  6f 20 74 68 65 20 62 6f  6f 6b 20 68 65 72 20 73   o the bo ok her s
```

What is the RTT value the second data-carrying TCP segment and its ACK?

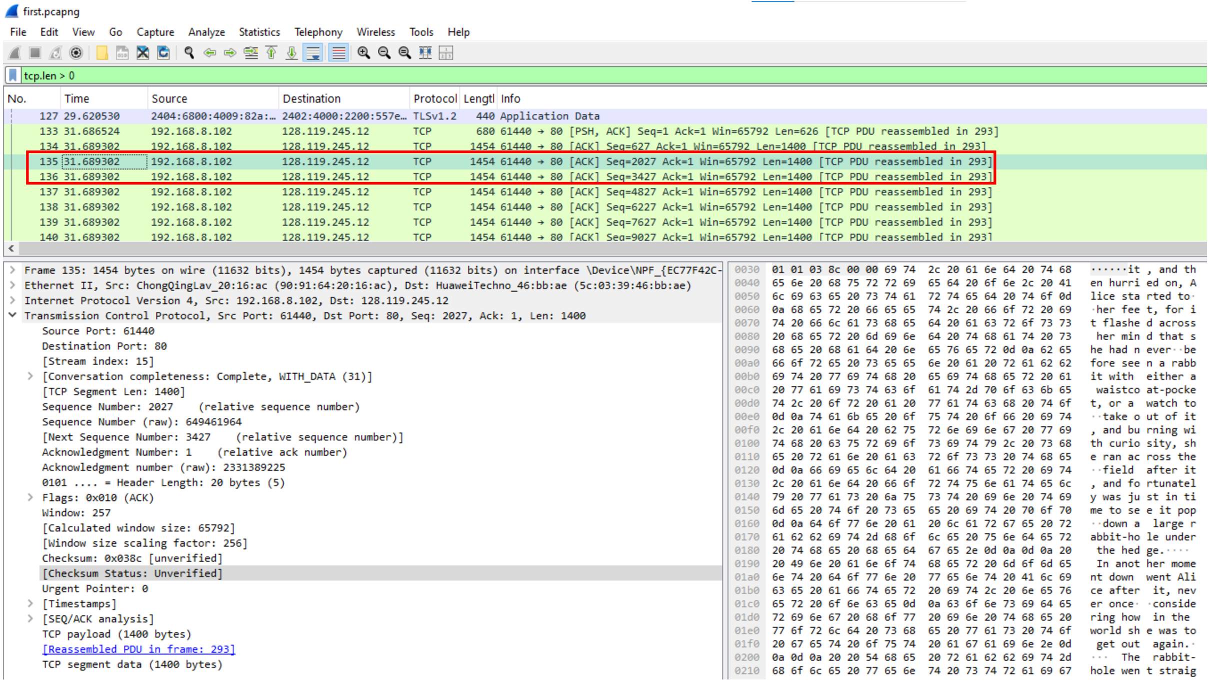
- Frame 135 carries data with Seq=2027.
- The ACK for this should acknowledge **Seq=3427 (2027 + 1400).**
- Look for the first ACK that acknowledges 3427.

RTT = Timestamp(Frame 136) - Timestamp(Frame 135)

= 31.689302 - 31.689302

= 0seconds

- Frame 135 has a timestamp of **31.689302 sec.**
- The ACK (for Seq=3427) has the same timestamp, then **RTT = 0 sec.**



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

```
tcp.len > 0

No.   Time        Source                  Destination             Protocol Lengtl Info
  127 29.620530   2404:6800:4009:82a:…   2402:4000:2200:557e…   TLSv1.2   440 Application Data
  133 31.686524   192.168.8.102           128.119.245.12          TCP       680 61440 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65792 Len=626 [TCP PDU reassembled in 293]
  134 31.689302   192.168.8.102           128.119.245.12          TCP      1454 61440 → 80 [ACK] Seq=627 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
  135 31.689302   192.168.8.102           128.119.245.12          TCP      1454 61440 → 80 [ACK] Seq=2027 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
  136 31.689302   192.168.8.102           128.119.245.12          TCP      1454 61440 → 80 [ACK] Seq=3427 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
  137 31.689302   192.168.8.102           128.119.245.12          TCP      1454 61440 → 80 [ACK] Seq=4827 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
  138 31.689302   192.168.8.102           128.119.245.12          TCP      1454 61440 → 80 [ACK] Seq=6227 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
  139 31.689302   192.168.8.102           128.119.245.12          TCP      1454 61440 → 80 [ACK] Seq=7627 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
  140 31.689302   192.168.8.102           128.119.245.12          TCP      1454 61440 → 80 [ACK] Seq=9027 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
```

```
> Frame 135: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface \Device\NPF_{EC77F42C-
> Ethernet II, Src: ChongQingLav_20:16:ac (90:91:64:20:16:ac), Dst: HuaweiTechno_46:bb:ae (5c:03:39:46:bb:ae)
> Internet Protocol Version 4, Src: 192.168.8.102, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 61440, Dst Port: 80, Seq: 2027, Ack: 1, Len: 1400
    Source Port: 61440
    Destination Port: 80
    [Stream index: 15]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 1400]
    Sequence Number: 2027    (relative sequence number)
    Sequence Number (raw): 649461964
    [Next Sequence Number: 3427    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2331389225
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window: 257
    [Calculated window size: 65792]
    [Window size scaling factor: 256]
    Checksum: 0x038c [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (1400 bytes)
    [Reassembled PDU in frame: 293]
    TCP segment data (1400 bytes)
```

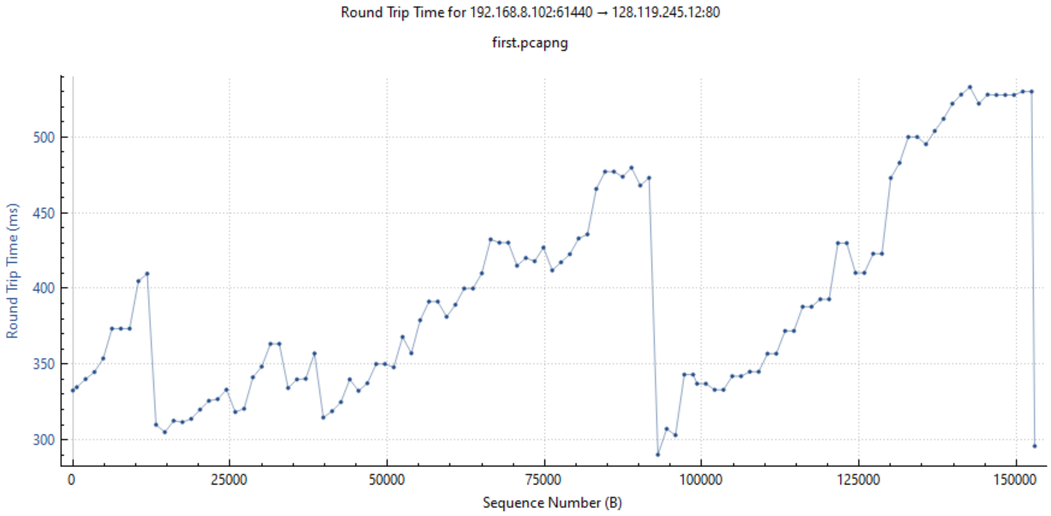
```
0030  01 01 03 8c 00 00 69 74  2c 20 61 6e 64 20 74 68   ······it , and th
0040  65 6e 20 68 75 72 72 69  65 64 20 6f 6e 2c 20 41   en hurri ed on, A
0050  6c 69 63 65 20 73 74 61  72 74 65 64 20 74 6f 0d   lice sta rted to·
0060  0a 68 65 72 20 66 65 65  74 2c 20 66 6f 72 20 69   ·her fee t, for i
0070  74 20 66 6c 61 73 68 65  64 20 61 63 72 6f 73 73   t flashe d across
0080  20 68 65 72 20 6d 69 6e  64 20 74 68 61 74 20 73    her min d that s
0090  68 65 20 68 61 64 20 6e  65 76 65 72 0d 0a 62 65   he had n ever··be
00a0  66 6f 72 65 20 73 65 65  6e 20 61 20 72 61 62 62   fore see n a rabb
00b0  69 74 20 77 69 74 68 20  65 69 74 68 65 72 20 61   it with  either a
00c0  20 77 61 69 73 74 63 6f  61 74 2d 70 6f 63 6b 65    waistco at-pocke
00d0  74 2c 20 6f 72 20 61 20  77 61 74 63 68 20 74 6f   t, or a  watch to
00e0  0d 0a 74 61 6b 65 20 6f  75 74 20 6f 66 20 69 74   ··take o ut of it
00f0  2c 20 61 6e 64 20 62 75  72 6e 69 6e 67 20 77 69   , and bu rning wi
0100  74 68 20 63 75 72 69 6f  73 69 74 79 2c 20 73 68   th curio sity, sh
0110  65 20 72 61 6e 20 61 63  72 6f 73 73 20 74 68 65   e ran ac ross the
0120  0d 0a 66 69 65 6c 64 20  61 66 74 65 72 20 69 74   ··field  after it
0130  2c 20 61 6e 64 20 66 6f  72 74 75 6e 61 74 65 6c   , and fo rtunatel
0140  79 20 77 61 73 20 6a 75  73 74 20 69 6e 20 74 69   y was ju st in ti
0150  6d 65 20 74 6f 20 73 65  65 20 69 74 20 70 6f 70   me to se e it pop
0160  0d 0a 64 6f 77 6e 20 61  20 6c 61 72 67 65 20 72   ··down a  large r
0170  61 62 62 69 74 2d 68 6f  6c 65 20 75 6e 64 65 72   abbit-ho le under
0180  20 74 68 65 20 68 65 64  67 65 2e 0d 0a 0d 0a 20    the hed ge.····
0190  20 49 6e 20 61 6e 6f 74  68 65 72 20 6d 6f 6d 65    In anot her mome
01a0  6e 74 20 64 6f 77 6e 20  77 65 6e 74 20 41 6c 69   nt down  went Ali
01b0  63 65 20 61 66 74 65 72  20 69 74 2c 20 6e 65 76   ce after  it, nev
01c0  65 72 20 6f 6e 63 65 0d  0a 63 6f 6e 73 69 64 65   er once· ·conside
01d0  72 69 6e 67 20 68 6f 77  20 69 6e 20 74 68 65 20   ring how  in the
01e0  77 6f 72 6c 64 20 73 68  65 20 77 61 73 20 74 6f   world sh e was to
01f0  20 67 65 74 20 6f 75 74  20 61 67 61 69 6e 2e 0d    get out  again.·
0200  0a 0d 0a 20 20 54 68 65  20 72 61 62 62 69 74 2d   ···  The  rabbit-
0210  68 6f 6c 65 20 77 65 6e  74 20 73 74 72 61 69 67   hole wen t straig
```

What is the EstimatedRTT value (see Section 3.5.3, in the text) after the ACK for the second data-carrying segment is received?

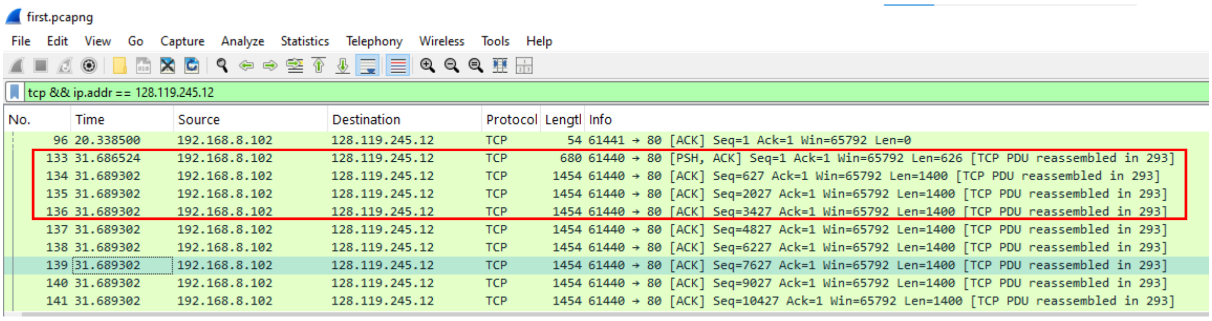
EstimatedRTT = (1-α) × Estimated + α × SampleRTT

- α=0.125
- **Initial EstimatedRTT** = **Measured RTT of the first segment** = **2.778 ms**
- **SampleRTT for the second segment** = **0 ms**

EstimatedRTT = (1- 0.125) × 2.778 + 0.125 × 0
EstimatedRTT = (0.875)×2.778
<u>EstimatedRTT = 2.430ms</u>



7. *What is the length (header plus payload) of each of the first four data-carrying TCP segments?*


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

tcp && ip.addr == 128.119.245.12

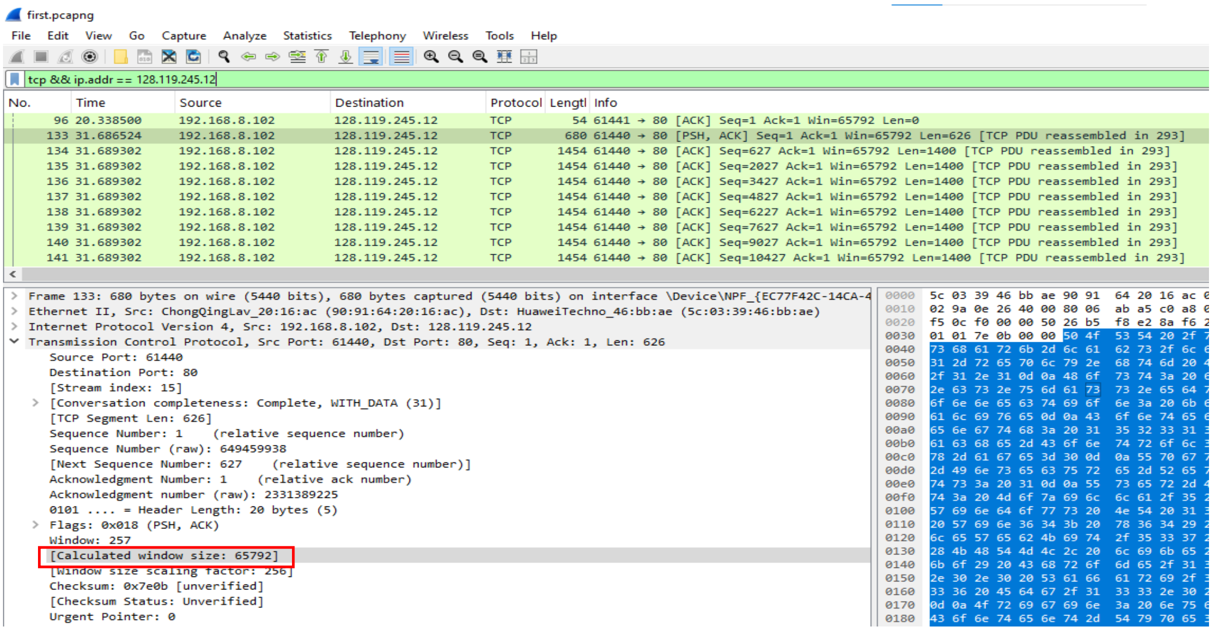
```
No.  Time       Source         Destination     Protocol Lengtl Info
  96 20.338500  192.168.8.102  128.119.245.12  TCP        54 61441 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
 133 31.686524  192.168.8.102  128.119.245.12  TCP       680 61440 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65792 Len=626 [TCP PDU reassembled in 293]
 134 31.689302  192.168.8.102  128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=627 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
 135 31.689302  192.168.8.102  128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=2027 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
 136 31.689302  192.168.8.102  128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=3427 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
 137 31.689302  192.168.8.102  128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=4827 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
 138 31.689302  192.168.8.102  128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=6227 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
 139 31.689302  192.168.8.102  128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=7627 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
 140 31.689302  192.168.8.102  128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=9027 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
 141 31.689302  192.168.8.102  128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=10427 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
```

Segment	**Sequence No**	**TCP Payload Length**	**TCP Header Length**	**Length**
Frame No - 133	Seq= 1	626 bytes	20 bytes	646bytes
Frame No - 134	Seq= 627	1400 bytes	20 bytes	1420 bytes
Frame No - 135	Seq= 2027	1400bytes	20 bytes	1420 bytes
Frame No - 136	Seq= 3427	1400 bytes	20 bytes	1420 bytes

8. *What is the minimum amount of available buffer space advertised to the client by gaia.cs.umass.edu among these first four data-carrying TCP segments?*

Frame No	**ACK for Seq No**	**Calculated Window**
133	ACK for Seq=1	65792 bytes
134	ACK for Seq=627	65792 bytes
135	ACK for Seq=2027	65792 bytes
136	ACK for Seq=3427	65792 bytes

The **minimum advertised buffer space** among these four data-carrying segments is **65 792 bytes**.


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

tcp && ip.addr == 128.119.245.12

```
No.  Time       Source         Destination     Protocol Lengtl Info
  96 20.338500  192.168.8.102  128.119.245.12  TCP        54 61441 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
 133 31.686524  192.168.8.102  128.119.245.12  TCP       680 61440 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65792 Len=626 [TCP PDU reassembled in 293]
 134 31.689302  192.168.8.102  128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=627 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
 135 31.689302  192.168.8.102  128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=2027 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
 136 31.689302  192.168.8.102  128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=3427 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
 137 31.689302  192.168.8.102  128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=4827 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
 138 31.689302  192.168.8.102  128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=6227 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
 139 31.689302  192.168.8.102  128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=7627 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
 140 31.689302  192.168.8.102  128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=9027 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
 141 31.689302  192.168.8.102  128.119.245.12  TCP      1454 61440 → 80 [ACK] Seq=10427 Ack=1 Win=65792 Len=1400 [TCP PDU reassembled in 293]
```

```
> Frame 133: 680 bytes on wire (5440 bits), 680 bytes captured (5440 bits) on interface \Device\NPF_{EC77F42C-14CA-4
> Ethernet II, Src: ChongQingLav_20:16:ac (90:91:64:20:16:ac), Dst: HuaweiTechno_46:bb:ae (5c:03:39:46:bb:ae)
> Internet Protocol Version 4, Src: 192.168.8.102, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 61440, Dst Port: 80, Seq: 1, Ack: 1, Len: 626
    Source Port: 61440
    Destination Port: 80
    [Stream index: 15]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 626]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 649459938
    [Next Sequence Number: 627    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2331389225
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 257
    [Calculated window size: 65792]
    [Window size scaling factor: 256]
    Checksum: 0x7e0b [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
```

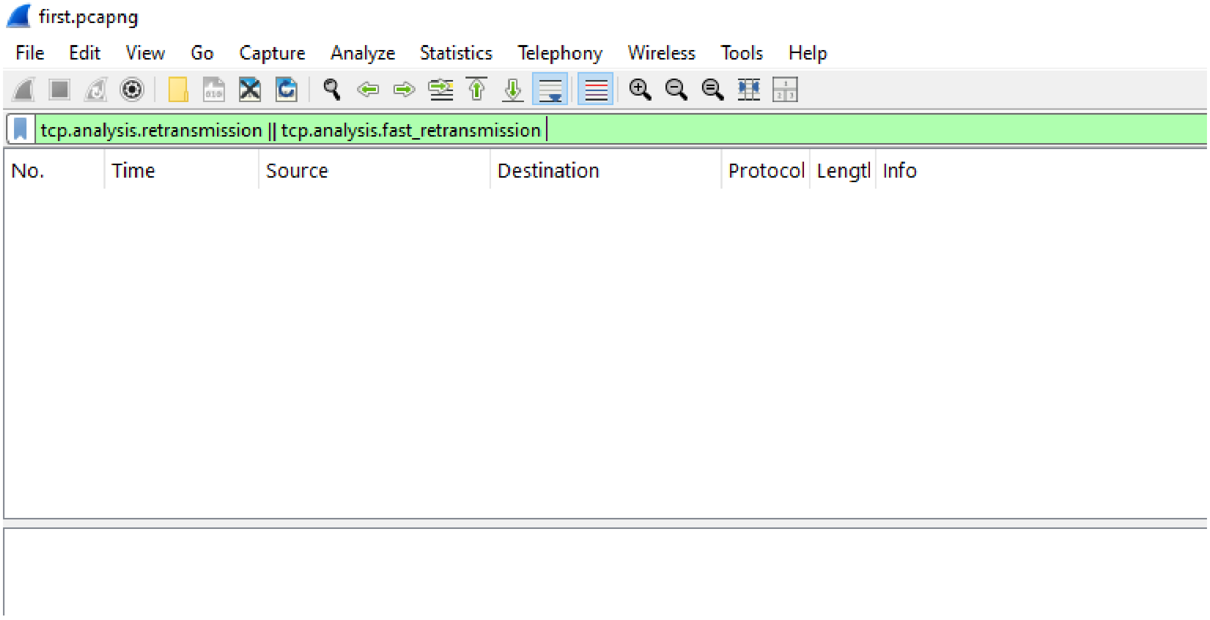
```
0000  5c 03 39 46 bb ae 90 91  64 20 16 ac
0010  02 9a 0e 26 40 00 80 06  ab a5 c0 a8
0020  f5 0c f0 00 00 50 26 b5  f8 e2 8a f6
0030  01 01 7e 0b 00 00 50 4f  53 54 20 2f
0040  73 68 61 72 6b 2d 6c 61  62 73 2f 6c
0050  31 2d 72 65 70 6c 79 2e  68 74 6d 20
0060  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20
0070  2e 63 73 2e 75 6d 61 73  73 2e 65 64
0080  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b
0090  61 6c 69 76 65 0d 0a 43  6f 6e 74 65
00a0  65 6e 67 74 68 3a 20 31  35 32 33 31
00b0  61 63 68 65 2d 43 6f 6e  74 72 6f 6c
00c0  78 2d 61 67 65 3d 30 0d  0a 55 70 67
00d0  2d 49 6e 73 65 63 75 72  65 2d 52 65
00e0  74 73 3a 20 31 0d 0a 55  73 65 72 2d
00f0  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35
0100  57 69 6e 64 6f 77 73 20  4e 54 20 31
0110  20 57 69 6e 36 34 3b 20  78 36 34 29
0120  6c 65 57 65 62 4b 69 74  2f 35 33 37
0130  28 4b 48 54 4d 4c 2c 20  6c 69 6b 65
0140  6b 6f 29 20 43 68 72 6f  6d 65 2f 31
0150  2e 30 2e 30 20 53 61 66  61 72 69 2f
0160  33 36 20 45 64 67 2f 31  33 33 2e 30
0170  0d 0a 4f 72 69 67 69 6e  3a 20 6e 75
0180  43 6f 6e 74 65 6e 74 2d  54 79 70 65
```

Does the lack of receiver buffer space ever throttle the sender for these first four data carrying segments?

- The lack of receiver buffer space does not throttle the sender for the first four data-carrying TCP segments.

9. *Are there any retransmitted segments in the trace file? What did you check for (in the trace) in order to answer this question?*

- No retransmitted segments were detected in the trace file. This was confirmed using Wireshark filters and by manually inspecting sequence numbers and duplicate ACKs.



tcp.analysis.retransmission || tcp.analysis.fast_retransmission

No.	Time	Source	Destination	Protocol	Lengtl	Info

10. *How much data does the receiver typically acknowledge in an ACK among the first ten data-carrying segments sent from the client to gaia.cs.umass.edu?*

- The receiver (128.119.245.12) typically acknowledges **2800 bytes** in each ACK.
- This indicates that the receiver is **ACKing every two received segments** (each segment is 1400 bytes).

Can you identify cases where the receiver is ACKing every other received segment (see Table 3.2 in the text) among these first ten data-carrying segments?

- **Yes.** The receiver does **not** send an ACK for every single segment.
- Instead, it acknowledges every **two** segments (after receiving **2800 bytes**).
- This is a **delayed ACK strategy** used to reduce the number of ACK packets.

11. *What is the throughput (bytes transferred per unit time) for the TCP connection?*

- Each segment carries **1400 bytes** of data.
- The receiver acknowledges **every two segments (2800 bytes per ACK)**.
- Counting from frame **133 to 256**, we estimate about **50 data segments** were sent.
- Total estimated data: **50 × 1400 = 70,000 bytes**

Calculate Time Duration

- **Start Time** : 31.686524 sec
- **End Time** : 32.711167 sec
- **Duration** : 32.711167 - 31.686524 = 1.0246 sec

Compute Throughput

Throughput = Total Bytes Transferred/Time Duration
Throughput = 70 000 bytes / 1.0246 sec
Throughput ≈ 68,324 bytes/sec ≈ 66.7 KB/sec

✓ The **TCP throughput is approximately 66.7 KB/sec (68,324 bytes/sec)**.

Explain how you calculated this value.

✓ This is calculated by dividing the **total data transferred (70,000 bytes)** by the **time duration (1.0246 sec)**.

12. *Use the Time-Sequence-Graph(Stevens) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Consider the "fleets" of packets sent around t = 0.025, t = 0.053, t = 0.082 and t = 0.1. Comment on whether this looks as if TCP is in its slow start phase, congestion avoidance phase or some other phase. Figure 6 shows a slightly different view of this data.*

- The observed packet transmission pattern **(3, 6, 12, 24)** strongly indicates that **TCP is in the Slow Start phase**, a fundamental part of **TCP's Congestion Control Mechanism**.
- During Slow Start, **TCP exponentially increases the congestion window (CWND) per Round-Trip Time (RTT)** by doubling the number of segments sent with each successful **Acknowledgment (ACK)**. This allows TCP to quickly probe the available bandwidth. The burst patterns at **t = 0.025s, t = 0.053s, t = 0.082s, and t = 0.1s** confirm this behavior, demonstrating the rapid expansion of CWND.
- Initially, **CWND starts small (often 1 MSS)** but grows multiplicatively (CWND = CWND × 2 per RTT) until it reaches a predefined **slow start threshold (ssthresh)**. When CWND surpasses **ssthresh**, TCP transitions into **Congestion Avoidance**, where the growth rate becomes linear rather than exponential.

13. *These “fleets” of segments appear to have some periodicity. What can you say about the period?*

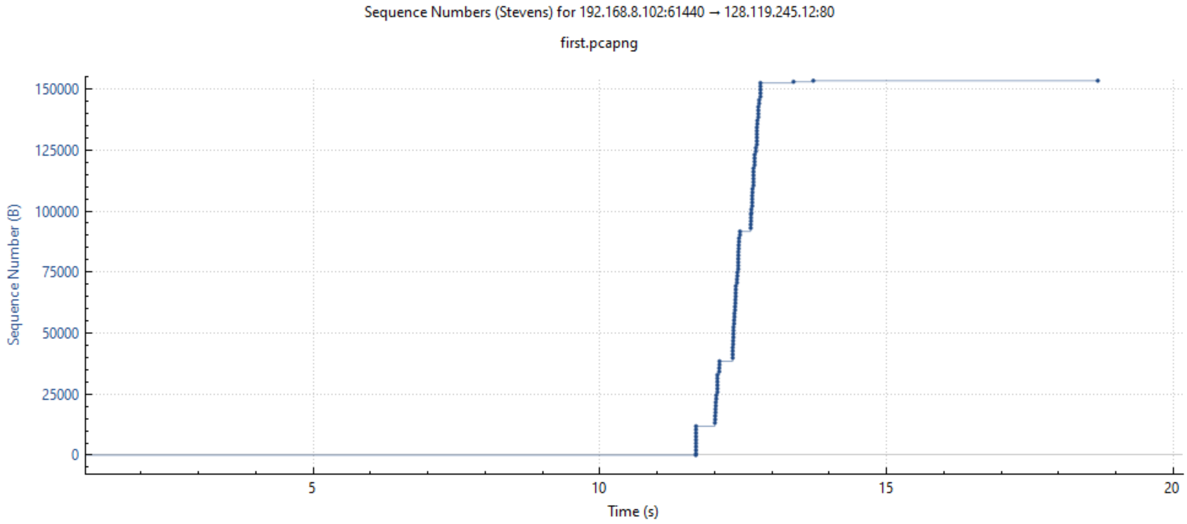
The **periodicity of the fleets of segments** in the **Time-Sequence Graph (Stevens)** suggests that the segments are being sent in bursts at **regular intervals**, corresponding to **the Round-Trip Time (RTT) of the TCP connection**.

Each fleet of packets appears at approximately:

- **t = 0.025s**
- **t = 0.053s**
- **t = 0.082s**
- **t = 0.1s**

By analyzing these timestamps, we observe that the fleets are spaced by approximately **0.025s to 0.03s**, which likely corresponds to the **RTT of the connection**.

14. *Answer each of two questions above for the trace that you have gathered when you transferred a file from your computer to gaia.cs.umass.edu*



Use the Time-Sequence-Graph(Stevens) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Consider the “fleets” of packets sent around t = 0.025, t = 0.053, t = 0.082 and t = 0.1. Comment on whether this looks as if TCP is in its slow start phase, congestion avoidance phase or some other phase.

- The pattern suggests TCP is in the **Slow Start phase**, as indicated by the exponential growth in segment transmission.

These “fleets” of segments appear to have some periodicity. What can you say about the period?

- The periodicity (~0.025s - 0.03s) corresponds to the **RTT**, which determines when new bursts of packets are sent.