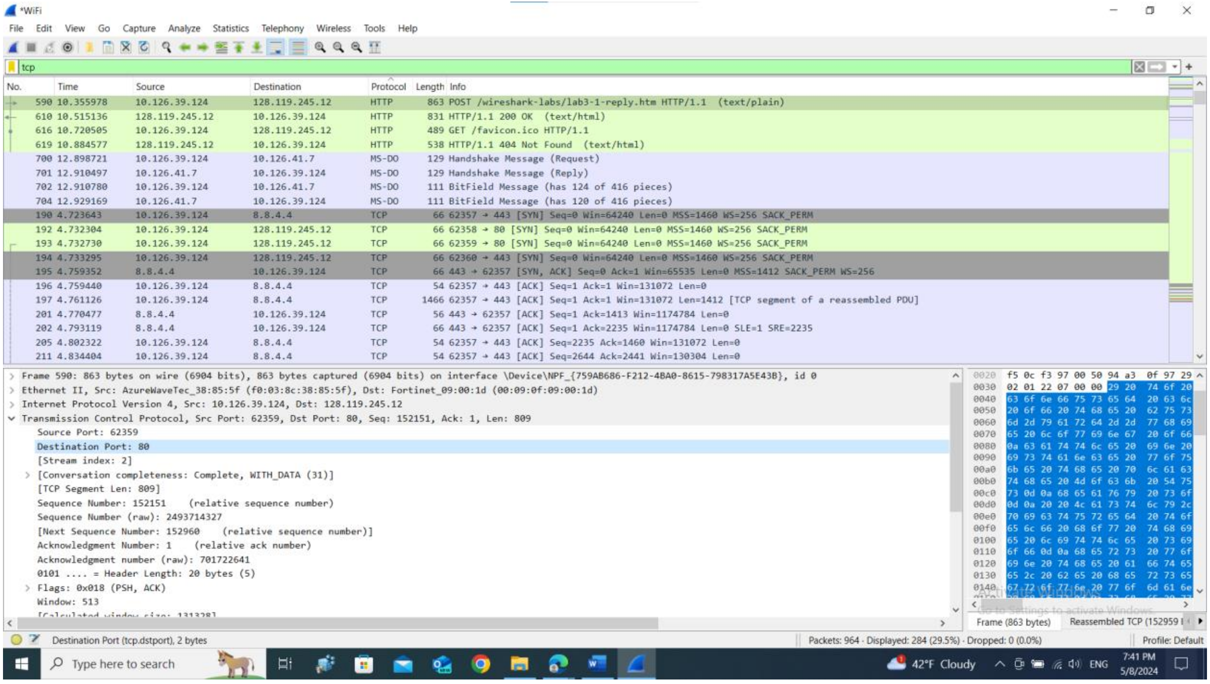
1. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu?



*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

```
No.   Time        Source          Destination     Protocol Length Info
  590 10.355978   10.126.39.124   128.119.245.12  HTTP      863 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)
  610 10.515136   128.119.245.12  10.126.39.124   HTTP      831 HTTP/1.1 200 OK  (text/html)
  616 10.720505   10.126.39.124   128.119.245.12  HTTP      489 GET /favicon.ico HTTP/1.1
  619 10.884577   128.119.245.12  10.126.39.124   HTTP      538 HTTP/1.1 404 Not Found  (text/html)
  700 12.898721   10.126.39.124   10.126.41.7     MS-DO     129 Handshake Message (Request)
  701 12.910497   10.126.41.7     10.126.39.124   MS-DO     129 Handshake Message (Reply)
  702 12.910780   10.126.39.124   10.126.41.7     MS-DO     111 BitField Message (has 124 of 416 pieces)
  704 12.929169   10.126.41.7     10.126.39.124   MS-DO     111 BitField Message (has 120 of 416 pieces)
  190 4.723643    10.126.39.124   8.8.4.4         TCP        66 62357 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  192 4.732304    10.126.39.124   128.119.245.12  TCP        66 62358 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  193 4.732730    10.126.39.124   128.119.245.12  TCP        66 62359 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  194 4.733295    10.126.39.124   128.119.245.12  TCP        66 62360 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  195 4.759352    8.8.4.4         10.126.39.124   TCP        66 443 → 62357 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
  196 4.759440    10.126.39.124   8.8.4.4         TCP        54 62357 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
  197 4.761126    10.126.39.124   8.8.4.4         TCP      1466 62357 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=1412 [TCP segment of a reassembled PDU]
  201 4.770477    8.8.4.4         10.126.39.124   TCP        56 443 → 62357 [ACK] Seq=1 Ack=1413 Win=1174784 Len=0
  202 4.793119    8.8.4.4         10.126.39.124   TCP        66 443 → 62357 [ACK] Seq=1 Ack=2235 Win=1174784 Len=0 SLE=1 SRE=2235
  205 4.802322    10.126.39.124   8.8.4.4         TCP        54 62357 → 443 [ACK] Seq=2235 Ack=1460 Win=131072 Len=0
  211 4.834404    10.126.39.124   8.8.4.4         TCP        54 62357 → 443 [ACK] Seq=2644 Ack=2441 Win=130304 Len=0
```

```
> Frame 590: 863 bytes on wire (6904 bits), 863 bytes captured (6904 bits) on interface \Device\NPF_{759AB686-F212-4BA0-8615-798317A5E43B}, id 0
> Ethernet II, Src: AzureWaveTec_38:85:5f (f0:03:8c:38:85:5f), Dst: Fortinet_09:00:1d (00:09:0f:09:00:1d)
> Internet Protocol Version 4, Src: 10.126.39.124, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 62359, Dst Port: 80, Seq: 152151, Ack: 1, Len: 809
    Source Port: 62359
    Destination Port: 80
    [Stream index: 2]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 809]
    Sequence Number: 152151    (relative sequence number)
    Sequence Number (raw): 2493714327
    [Next Sequence Number: 152960    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 701722641
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 513
```

```
0020  f5 0c f3 97 00 50 94 a3  0f 97 29
0030  02 01 22 07 00 00 29 20  74 6f 20
0040  63 6f 6e 66 75 73 65 64  20 63 6c
0050  20 6f 66 20 74 68 65 20  62 75 73
0060  6d 2d 79 61 72 64 2d 2d  77 68 69
0070  65 20 6c 6f 77 69 6e 67  20 6f 66
0080  0a 63 61 74 74 6c 65 20  69 6e 20
0090  69 73 74 61 6e 63 65 20  77 6f 75
00a0  6b 65 20 74 68 65 20 70  6c 61 63
00b0  74 68 65 20 4d 6f 63 6b  20 54 75
00c0  73 0d 0a 68 65 61 76 79  20 73 6f
00d0  0d 0a 20 20 4c 61 73 74  6c 79 2c
00e0  70 69 63 74 75 72 65 64  20 74 6f
00f0  65 6c 66 20 68 6f 77 20  74 68 69
0100  65 20 6c 69 74 74 6c 65  20 73 69
0110  6f 66 0d 0a 68 65 72 73  20 77 6f
0120  69 6e 20 74 68 65 20 61  66 74 65
0130  65 2c 20 62 65 20 68 65  72 73 65
0140  67 72 6f 77 6e 20 77 6f  6d 61 6e
```

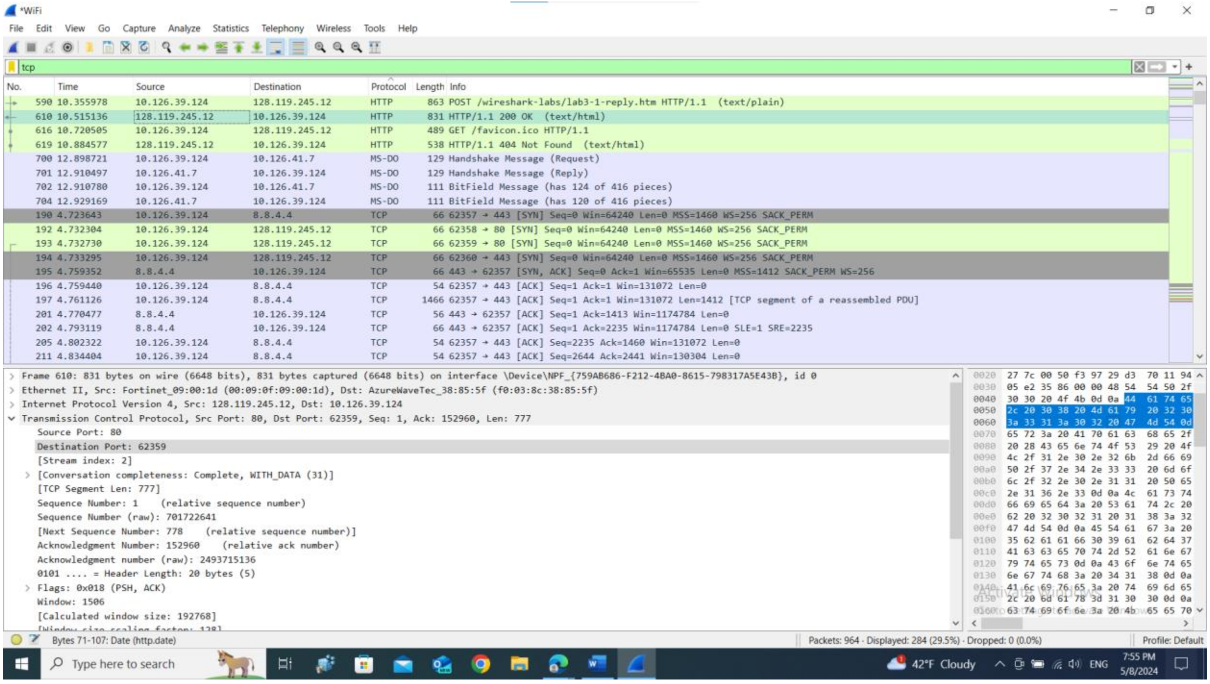
Frame (863 bytes) Reassembled TCP (152959 I

Destination Port (tcp.dstport), 2 bytes

Packets: 964 · Displayed: 284 (29.5%) · Dropped: 0 (0.0%)

Profile: Default

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?



*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

```
No.   Time        Source          Destination     Protocol Length Info
  590 10.355978   10.126.39.124   128.119.245.12  HTTP      863 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)
  610 10.515136   128.119.245.12  10.126.39.124   HTTP      831 HTTP/1.1 200 OK  (text/html)
  616 10.720505   10.126.39.124   128.119.245.12  HTTP      489 GET /favicon.ico HTTP/1.1
  619 10.884577   128.119.245.12  10.126.39.124   HTTP      538 HTTP/1.1 404 Not Found  (text/html)
  700 12.898721   10.126.39.124   10.126.41.7     MS-DO     129 Handshake Message (Request)
  701 12.910497   10.126.41.7     10.126.39.124   MS-DO     129 Handshake Message (Reply)
  702 12.910780   10.126.39.124   10.126.41.7     MS-DO     111 BitField Message (has 124 of 416 pieces)
  704 12.929169   10.126.41.7     10.126.39.124   MS-DO     111 BitField Message (has 120 of 416 pieces)
  190 4.723643    10.126.39.124   8.8.4.4         TCP        66 62357 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  192 4.732304    10.126.39.124   128.119.245.12  TCP        66 62358 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  193 4.732730    10.126.39.124   128.119.245.12  TCP        66 62359 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  194 4.733295    10.126.39.124   128.119.245.12  TCP        66 62360 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  195 4.759352    8.8.4.4         10.126.39.124   TCP        66 443 → 62357 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
  196 4.759440    10.126.39.124   8.8.4.4         TCP        54 62357 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
  197 4.761126    10.126.39.124   8.8.4.4         TCP      1466 62357 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=1412 [TCP segment of a reassembled PDU]
  201 4.770477    8.8.4.4         10.126.39.124   TCP        56 443 → 62357 [ACK] Seq=1 Ack=1413 Win=1174784 Len=0
  202 4.793119    8.8.4.4         10.126.39.124   TCP        66 443 → 62357 [ACK] Seq=1 Ack=2235 Win=1174784 Len=0 SLE=1 SRE=2235
  205 4.802322    10.126.39.124   8.8.4.4         TCP        54 62357 → 443 [ACK] Seq=2235 Ack=1460 Win=131072 Len=0
  211 4.834404    10.126.39.124   8.8.4.4         TCP        54 62357 → 443 [ACK] Seq=2644 Ack=2441 Win=130304 Len=0
```

```
> Frame 610: 831 bytes on wire (6648 bits), 831 bytes captured (6648 bits) on interface \Device\NPF_{759AB686-F212-4BA0-8615-798317A5E43B}, id 0
> Ethernet II, Src: Fortinet_09:00:1d (00:09:0f:09:00:1d), Dst: AzureWaveTec_38:85:5f (f0:03:8c:38:85:5f)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.126.39.124
v Transmission Control Protocol, Src Port: 80, Dst Port: 62359, Seq: 1, Ack: 152960, Len: 777
    Source Port: 80
    Destination Port: 62359
    [Stream index: 2]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 777]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 701722641
    [Next Sequence Number: 778    (relative sequence number)]
    Acknowledgment Number: 152960    (relative ack number)
    Acknowledgment number (raw): 2493715136
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 1506
    [Calculated window size: 192768]
```

```
0020  27 7c 00 50 f3 97 29 d3  70 11 94
0030  05 e2 35 86 00 00 48 54  54 50 2f
0040  30 30 20 4f 4b 0d 0a 44  61 74 65
0050  2c 20 30 38 20 4d 61 79  20 32 30
0060  3a 33 31 3a 30 32 20 47  4d 54 0d
0070  65 72 3a 20 41 70 61 63  68 65 2f
0080  20 28 43 65 6e 74 4f 53  29 20 4f
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69
00a0  50 2f 37 2e 34 2e 33 33  20 6d 6f
00b0  6c 2f 32 2e 30 2e 31 31  20 50 65
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74
00d0  66 69 65 64 3a 20 53 61  74 2c 20
00e0  62 20 32 30 32 31 20 31  38 3a 32
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20
0100  35 62 61 61 66 30 39 61  62 64 37
0110  41 63 63 65 70 74 2d 52  61 6e 67
0120  79 74 65 73 0d 0a 43 6f  6e 74 65
0130  6e 67 74 68 3a 20 34 31  38 0d 0a
0140  41 6c 69 76 65 3a 20 74  69 6d 65
0150  2c 20 6d 61 78 3d 31 30  30 0d 0a
0160  63 74 69 6f 6e 3a 20 4b  65 65 70
```

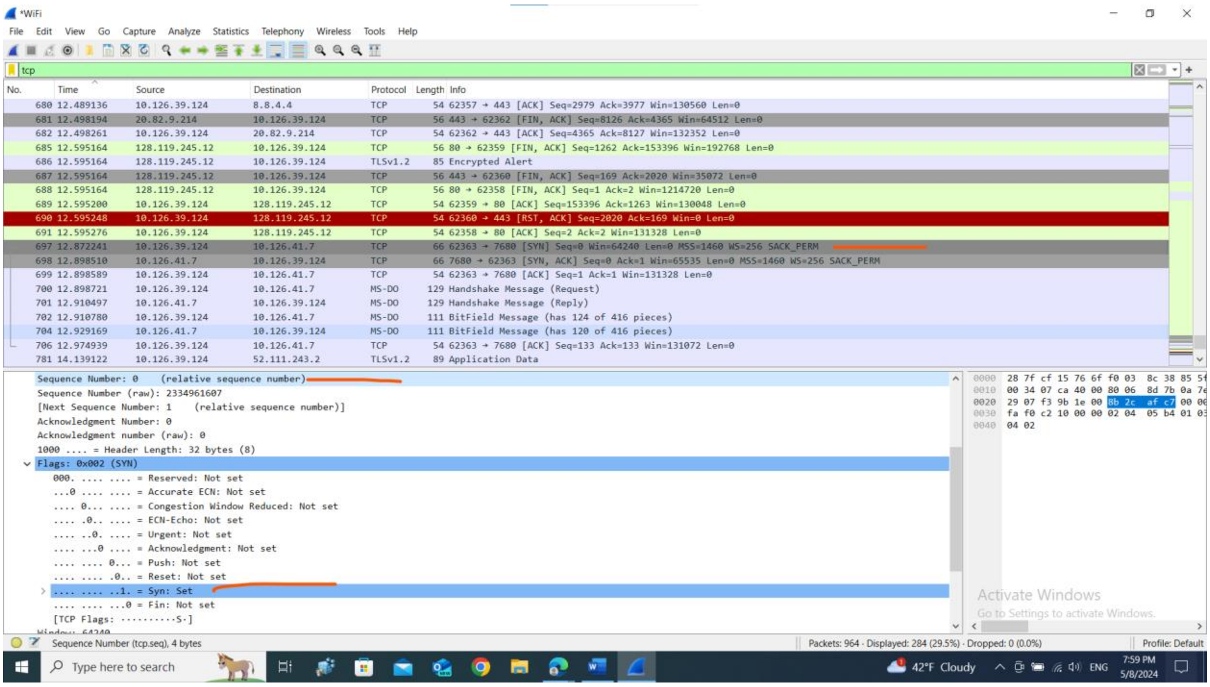
Bytes 71-107: Date (http.date)

Packets: 964 · Displayed: 284 (29.5%) · Dropped: 0 (0.0%)

Profile: Default

4. 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? What is it

in the segment that identifies the segment as a SYN segment?


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.  Time       Source          Destination     Protocol Length Info
 680 12.489136  10.126.39.124   8.8.4.4         TCP       54 62357 → 443 [ACK] Seq=2979 Ack=3977 Win=130560 Len=0
 681 12.498194  20.82.9.214     10.126.39.124   TCP       56 443 → 62362 [FIN, ACK] Seq=8126 Ack=4365 Win=64512 Len=0
 682 12.498261  10.126.39.124   20.82.9.214     TCP       54 62362 → 443 [ACK] Seq=4365 Ack=8127 Win=132352 Len=0
 685 12.595164  128.119.245.12  10.126.39.124   TCP       56 80 → 62359 [FIN, ACK] Seq=1262 Ack=153396 Win=192768 Len=0
 686 12.595164  128.119.245.12  10.126.39.124   TLSv1.2   85 Encrypted Alert
 687 12.595164  128.119.245.12  10.126.39.124   TCP       56 443 → 62360 [FIN, ACK] Seq=169 Ack=2020 Win=35072 Len=0
 688 12.595164  128.119.245.12  10.126.39.124   TCP       56 80 → 62358 [FIN, ACK] Seq=1 Ack=2 Win=1214720 Len=0
 689 12.595200  10.126.39.124   128.119.245.12  TCP       54 62359 → 80 [ACK] Seq=153396 Ack=1263 Win=130048 Len=0
 690 12.595248  10.126.39.124   128.119.245.12  TCP       54 62360 → 443 [RST, ACK] Seq=2020 Ack=169 Win=0 Len=0
 691 12.595276  10.126.39.124   128.119.245.12  TCP       54 62358 → 80 [ACK] Seq=2 Ack=2 Win=131328 Len=0
 697 12.872241  10.126.39.124   10.126.41.7     TCP       66 62363 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 698 12.898510  10.126.41.7     10.126.39.124   TCP       66 7680 → 62363 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 699 12.898589  10.126.39.124   10.126.41.7     TCP       54 62363 → 7680 [ACK] Seq=1 Ack=1 Win=131328 Len=0
 700 12.898721  10.126.39.124   10.126.41.7     MS-DO    129 Handshake Message (Request)
 701 12.910497  10.126.41.7     10.126.39.124   MS-DO    129 Handshake Message (Reply)
 702 12.910780  10.126.39.124   10.126.41.7     MS-DO    111 BitField Message (has 124 of 416 pieces)
 704 12.929169  10.126.41.7     10.126.39.124   MS-DO    111 BitField Message (has 120 of 416 pieces)
 706 12.974939  10.126.39.124   10.126.41.7     TCP       54 62363 → 7680 [ACK] Seq=133 Ack=133 Win=131072 Len=0
 781 14.139122  10.126.39.124   52.111.243.2    TLSv1.2   89 Application Data
```

```
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2334961607
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  ∨ 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
```

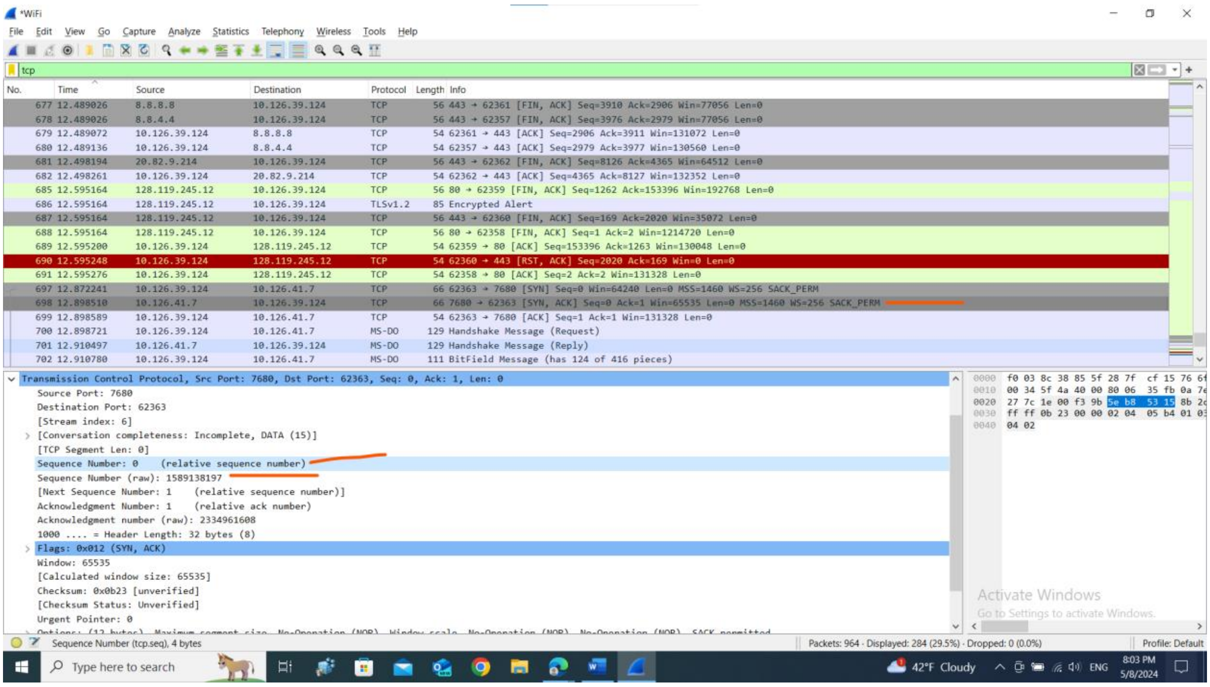
```
0000  28 7f cf 15 76 6f f0 03  8c 38 85 5f
0010  00 34 07 ca 40 00 80 06  8d 7b 0a 7e
0020  29 07 f3 9b 1e 00 8b 2c  af c7 00 00
0030  fa f0 c2 10 00 00 02 04  05 b4 01 03
0040  04 02
```

Sequence Number (tcp.seq), 4 bytes

Packets: 964 · Displayed: 284 (29.5%) · Dropped: 0 (0.0%)

Profile: Default

5. What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.  Time       Source          Destination     Protocol Length Info
 677 12.489026  8.8.8.8         10.126.39.124   TCP       56 443 → 62361 [FIN, ACK] Seq=3910 Ack=2906 Win=77056 Len=0
 678 12.489026  8.8.4.4         10.126.39.124   TCP       56 443 → 62357 [FIN, ACK] Seq=3976 Ack=2979 Win=77056 Len=0
 679 12.489072  10.126.39.124   8.8.8.8         TCP       54 62361 → 443 [ACK] Seq=2906 Ack=3911 Win=131072 Len=0
 680 12.489136  10.126.39.124   8.8.4.4         TCP       54 62357 → 443 [ACK] Seq=2979 Ack=3977 Win=130560 Len=0
 681 12.498194  20.82.9.214     10.126.39.124   TCP       56 443 → 62362 [FIN, ACK] Seq=8126 Ack=4365 Win=64512 Len=0
 682 12.498261  10.126.39.124   20.82.9.214     TCP       54 62362 → 443 [ACK] Seq=4365 Ack=8127 Win=132352 Len=0
 685 12.595164  128.119.245.12  10.126.39.124   TCP       56 80 → 62359 [FIN, ACK] Seq=1262 Ack=153396 Win=192768 Len=0
 686 12.595164  128.119.245.12  10.126.39.124   TLSv1.2   85 Encrypted Alert
 687 12.595164  128.119.245.12  10.126.39.124   TCP       56 443 → 62360 [FIN, ACK] Seq=169 Ack=2020 Win=35072 Len=0
 688 12.595164  128.119.245.12  10.126.39.124   TCP       56 80 → 62358 [FIN, ACK] Seq=1 Ack=2 Win=1214720 Len=0
 689 12.595200  10.126.39.124   128.119.245.12  TCP       54 62359 → 80 [ACK] Seq=153396 Ack=1263 Win=130048 Len=0
 690 12.595248  10.126.39.124   128.119.245.12  TCP       54 62360 → 443 [RST, ACK] Seq=2020 Ack=169 Win=0 Len=0
 691 12.595276  10.126.39.124   128.119.245.12  TCP       54 62358 → 80 [ACK] Seq=2 Ack=2 Win=131328 Len=0
 697 12.872241  10.126.39.124   10.126.41.7     TCP       66 62363 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 698 12.898510  10.126.41.7     10.126.39.124   TCP       66 7680 → 62363 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 699 12.898589  10.126.39.124   10.126.41.7     TCP       54 62363 → 7680 [ACK] Seq=1 Ack=1 Win=131328 Len=0
 700 12.898721  10.126.39.124   10.126.41.7     MS-DO    129 Handshake Message (Request)
 701 12.910497  10.126.41.7     10.126.39.124   MS-DO    129 Handshake Message (Reply)
 702 12.910780  10.126.39.124   10.126.41.7     MS-DO    111 BitField Message (has 124 of 416 pieces)
```

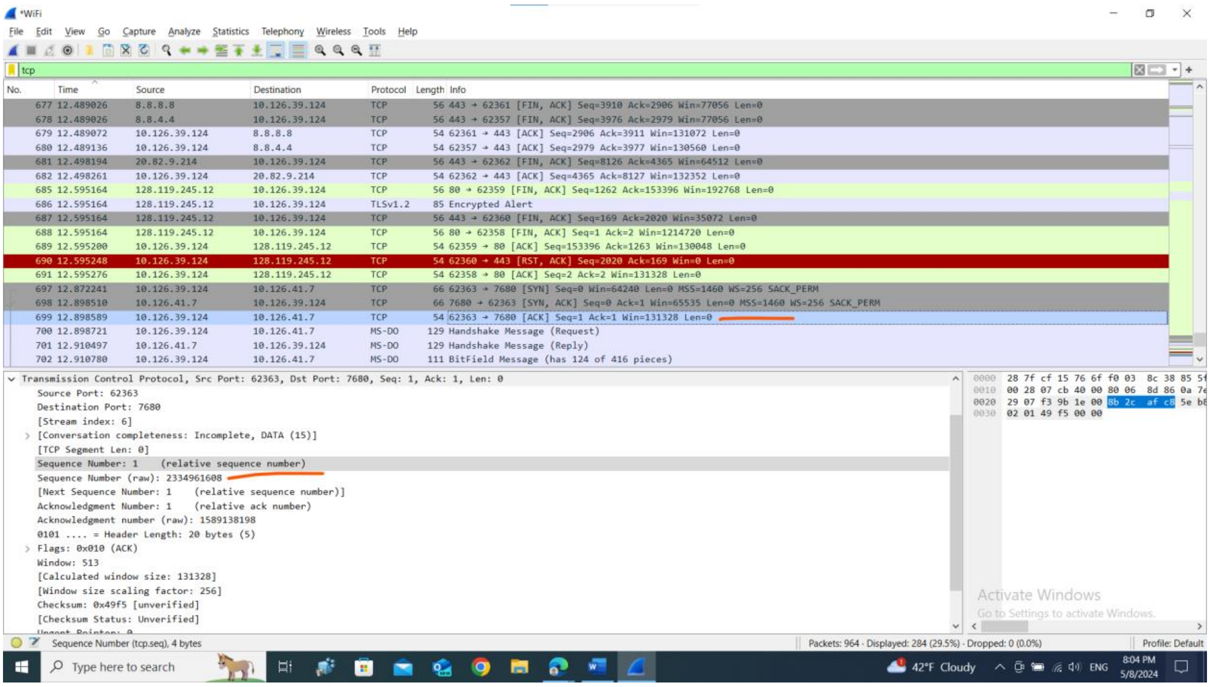
```
∨ Transmission Control Protocol, Src Port: 7680, Dst Port: 62363, Seq: 0, Ack: 1, Len: 0
    Source Port: 7680
    Destination Port: 62363
    [Stream index: 6]
  > [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1589138197
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2334961608
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x012 (SYN, ACK)
    Window: 65535
    [Calculated window size: 65535]
    Checksum: 0x0b23 [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 permitted
```

```
0000  f0 03 8c 38 85 5f 28 7f  cf 15 76 6f
0010  00 34 5f 4a 40 00 80 06  35 fb 0a 7e
0020  27 7c 1e 00 f3 9b 5e b8  53 15 8b 2c
0030  ff ff 0b 23 00 00 02 04  05 b4 01 03
0040  04 02
```

Sequence Number (tcp.seq), 4 bytes

Packets: 964 · Displayed: 284 (29.5%) · Dropped: 0 (0.0%)

Profile: Default


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.   Time        Source          Destination     Protocol Length Info
  677 12.489026   8.8.8.8         10.126.39.124   TCP       56 443 → 62361 [FIN, ACK] Seq=3910 Ack=2906 Win=77056 Len=0
  678 12.489026   8.8.4.4         10.126.39.124   TCP       56 443 → 62357 [FIN, ACK] Seq=3976 Ack=2979 Win=77056 Len=0
  679 12.489072   10.126.39.124   8.8.8.8         TCP       54 62361 → 443 [ACK] Seq=2906 Ack=3911 Win=131072 Len=0
  680 12.489136   10.126.39.124   8.8.4.4         TCP       54 62357 → 443 [ACK] Seq=2979 Ack=3977 Win=130560 Len=0
  681 12.498194   20.82.9.214     10.126.39.124   TCP       56 443 → 62362 [FIN, ACK] Seq=8126 Ack=4365 Win=64512 Len=0
  682 12.498261   10.126.39.124   20.82.9.214     TCP       54 62362 → 443 [ACK] Seq=4365 Ack=8127 Win=132352 Len=0
  685 12.595164   128.119.245.12  10.126.39.124   TCP       56 80 → 62359 [FIN, ACK] Seq=1262 Ack=153396 Win=192768 Len=0
  686 12.595164   128.119.245.12  10.126.39.124   TLSv1.2   85 Encrypted Alert
  687 12.595164   128.119.245.12  10.126.39.124   TCP       56 443 → 62360 [FIN, ACK] Seq=169 Ack=2020 Win=35072 Len=0
  688 12.595164   128.119.245.12  10.126.39.124   TCP       56 80 → 62358 [FIN, ACK] Seq=1 Ack=2 Win=1214720 Len=0
  689 12.595200   10.126.39.124   128.119.245.12  TCP       54 62359 → 80 [ACK] Seq=153396 Ack=1263 Win=130048 Len=0
  690 12.595248   10.126.39.124   128.119.245.12  TCP       54 62360 → 443 [RST, ACK] Seq=2020 Ack=169 Win=0 Len=0
  691 12.595276   10.126.39.124   128.119.245.12  TCP       54 62358 → 80 [ACK] Seq=2 Ack=2 Win=131328 Len=0
  697 12.872241   10.126.39.124   10.126.41.7     TCP       66 62363 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  698 12.898510   10.126.41.7     10.126.39.124   TCP       66 7680 → 62363 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
  699 12.898589   10.126.39.124   10.126.41.7     TCP       54 62363 → 7680 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  700 12.898721   10.126.39.124   10.126.41.7     MS-DO    129 Handshake Message (Request)
  701 12.910497   10.126.41.7     10.126.39.124   MS-DO    129 Handshake Message (Reply)
  702 12.910780   10.126.39.124   10.126.41.7     MS-DO    111 BitField Message (has 124 of 416 pieces)
```

```
v Transmission Control Protocol, Src Port: 62363, Dst Port: 7680, Seq: 1, Ack: 1, Len: 0
    Source Port: 62363
    Destination Port: 7680
    [Stream index: 6]
  > [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2334961608
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1589138198
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window: 513
    [Calculated window size: 131328]
    [Window size scaling factor: 256]
    Checksum: 0x49f5 [unverified]
    [Checksum Status: Unverified]
```

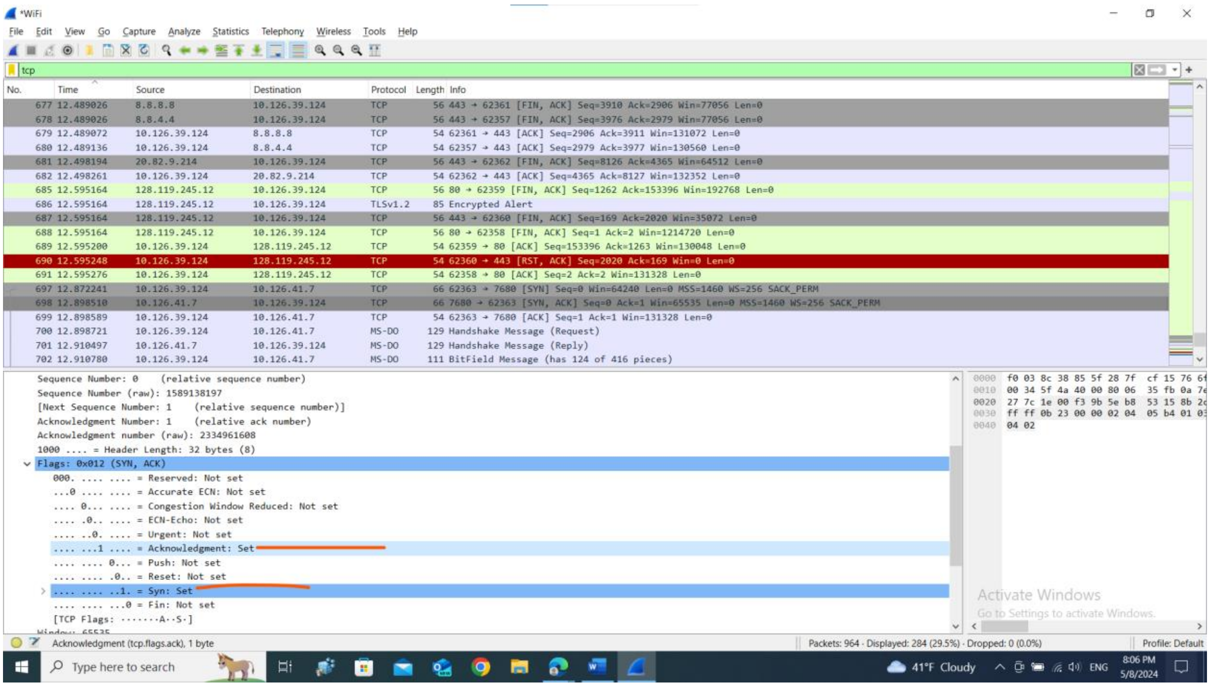
```
0000  28 7f cf 15 76 6f f0 03  8c 38 85 5f
0010  00 28 07 cb 40 00 80 06  8d 86 0a 7e
0020  29 07 f3 9b 1e 00 8b 2c  af c8 5e b8
0030  02 01 49 f5 00 00
```

Sequence Number (tcp.seq), 4 bytes

Packets: 964 · Displayed: 284 (29.5%) · Dropped: 0 (0.0%)

Profile: Default

Activate Windows
Go to Settings to activate Windows.
Type here to search
42°F Cloudy
ENG
8:04 PM
5/8/2024


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.   Time        Source          Destination     Protocol Length Info
  677 12.489026   8.8.8.8         10.126.39.124   TCP       56 443 → 62361 [FIN, ACK] Seq=3910 Ack=2906 Win=77056 Len=0
  678 12.489026   8.8.4.4         10.126.39.124   TCP       56 443 → 62357 [FIN, ACK] Seq=3976 Ack=2979 Win=77056 Len=0
  679 12.489072   10.126.39.124   8.8.8.8         TCP       54 62361 → 443 [ACK] Seq=2906 Ack=3911 Win=131072 Len=0
  680 12.489136   10.126.39.124   8.8.4.4         TCP       54 62357 → 443 [ACK] Seq=2979 Ack=3977 Win=130560 Len=0
  681 12.498194   20.82.9.214     10.126.39.124   TCP       56 443 → 62362 [FIN, ACK] Seq=8126 Ack=4365 Win=64512 Len=0
  682 12.498261   10.126.39.124   20.82.9.214     TCP       54 62362 → 443 [ACK] Seq=4365 Ack=8127 Win=132352 Len=0
  685 12.595164   128.119.245.12  10.126.39.124   TCP       56 80 → 62359 [FIN, ACK] Seq=1262 Ack=153396 Win=192768 Len=0
  686 12.595164   128.119.245.12  10.126.39.124   TLSv1.2   85 Encrypted Alert
  687 12.595164   128.119.245.12  10.126.39.124   TCP       56 443 → 62360 [FIN, ACK] Seq=169 Ack=2020 Win=35072 Len=0
  688 12.595164   128.119.245.12  10.126.39.124   TCP       56 80 → 62358 [FIN, ACK] Seq=1 Ack=2 Win=1214720 Len=0
  689 12.595200   10.126.39.124   128.119.245.12  TCP       54 62359 → 80 [ACK] Seq=153396 Ack=1263 Win=130048 Len=0
  690 12.595248   10.126.39.124   128.119.245.12  TCP       54 62360 → 443 [RST, ACK] Seq=2020 Ack=169 Win=0 Len=0
  691 12.595276   10.126.39.124   128.119.245.12  TCP       54 62358 → 80 [ACK] Seq=2 Ack=2 Win=131328 Len=0
  697 12.872241   10.126.39.124   10.126.41.7     TCP       66 62363 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  698 12.898510   10.126.41.7     10.126.39.124   TCP       66 7680 → 62363 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
  699 12.898589   10.126.39.124   10.126.41.7     TCP       54 62363 → 7680 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  700 12.898721   10.126.39.124   10.126.41.7     MS-DO    129 Handshake Message (Request)
  701 12.910497   10.126.41.7     10.126.39.124   MS-DO    129 Handshake Message (Reply)
  702 12.910780   10.126.39.124   10.126.41.7     MS-DO    111 BitField Message (has 124 of 416 pieces)
```

```
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1589138197
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2334961608
    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·]
```

```
0000  f0 03 8c 38 85 5f 28 7f  cf 15 76 6f
0010  00 34 5f 4a 40 00 80 06  35 fb 0a 7e
0020  27 7c 1e 00 f3 9b 5e b8  53 15 8b 2c
0030  ff ff 0b 23 00 00 02 04  05 b4 01 03
0040  04 02
```

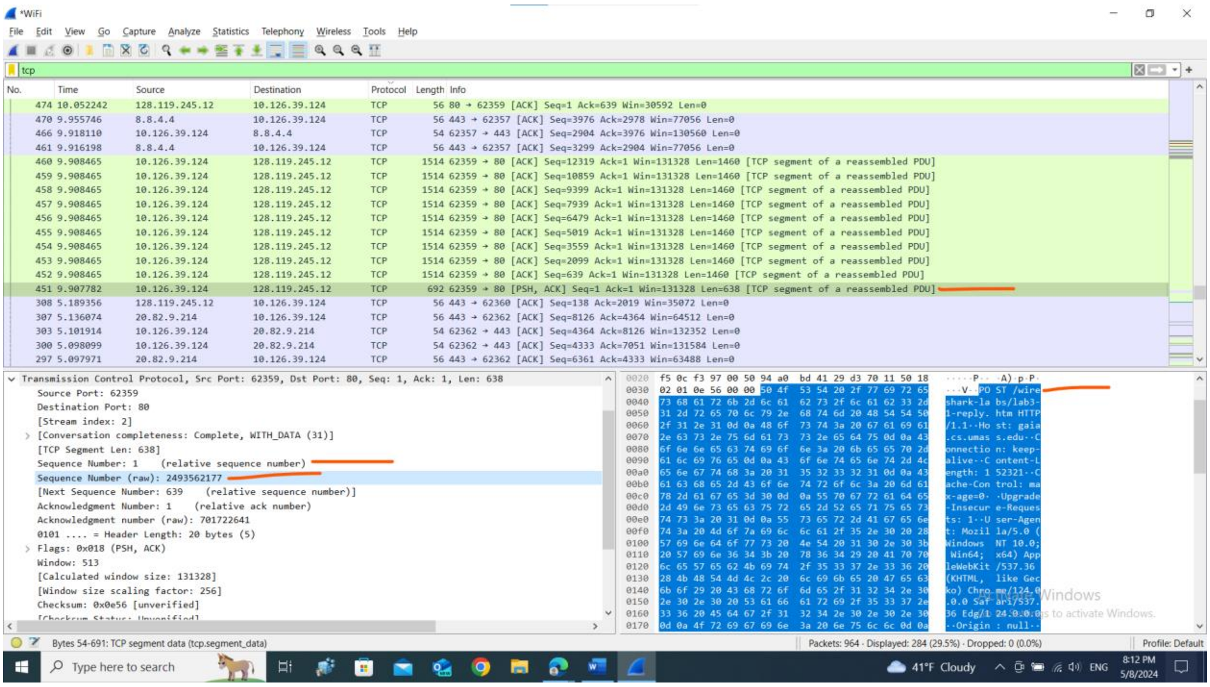
Acknowledgment (tcp.flags.ack), 1 byte

Packets: 964 · Displayed: 284 (29.5%) · Dropped: 0 (0.0%)

Profile: Default

6. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a

segment with a “POST” within its DATA field.



```
tcp
No.   Time       Source          Destination     Protocol Length Info
  474 10.052242  128.119.245.12  10.126.39.124   TCP        56 80 → 62359 [ACK] Seq=1 Ack=639 Win=30592 Len=0
  470 9.955746   8.8.4.4         10.126.39.124   TCP        56 443 → 62357 [ACK] Seq=3976 Ack=2978 Win=77056 Len=0
  466 9.918110   10.126.39.124   8.8.4.4         TCP        54 62357 → 443 [ACK] Seq=2904 Ack=3976 Win=130560 Len=0
  461 9.916198   8.8.4.4         10.126.39.124   TCP        56 443 → 62357 [ACK] Seq=3299 Ack=2904 Win=77056 Len=0
  460 9.908465   10.126.39.124   128.119.245.12  TCP      1514 62359 → 80 [ACK] Seq=12319 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
  459 9.908465   10.126.39.124   128.119.245.12  TCP      1514 62359 → 80 [ACK] Seq=10859 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
  458 9.908465   10.126.39.124   128.119.245.12  TCP      1514 62359 → 80 [ACK] Seq=9399 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
  457 9.908465   10.126.39.124   128.119.245.12  TCP      1514 62359 → 80 [ACK] Seq=7939 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
  456 9.908465   10.126.39.124   128.119.245.12  TCP      1514 62359 → 80 [ACK] Seq=6479 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
  455 9.908465   10.126.39.124   128.119.245.12  TCP      1514 62359 → 80 [ACK] Seq=5019 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
  454 9.908465   10.126.39.124   128.119.245.12  TCP      1514 62359 → 80 [ACK] Seq=3559 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
  453 9.908465   10.126.39.124   128.119.245.12  TCP      1514 62359 → 80 [ACK] Seq=2099 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
  452 9.908465   10.126.39.124   128.119.245.12  TCP      1514 62359 → 80 [ACK] Seq=639 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
  451 9.907782   10.126.39.124   128.119.245.12  TCP       692 62359 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=638 [TCP segment of a reassembled PDU]
  308 5.189356   128.119.245.12  10.126.39.124   TCP        56 443 → 62360 [ACK] Seq=138 Ack=2019 Win=35072 Len=0
  307 5.136074   20.82.9.214     10.126.39.124   TCP        56 443 → 62362 [ACK] Seq=8126 Ack=4364 Win=64512 Len=0
  303 5.101914   10.126.39.124   20.82.9.214     TCP        54 62362 → 443 [ACK] Seq=4364 Ack=8126 Win=132352 Len=0
  300 5.098099   10.126.39.124   20.82.9.214     TCP        54 62362 → 443 [ACK] Seq=4333 Ack=7051 Win=131584 Len=0
  297 5.097971   20.82.9.214     10.126.39.124   TCP        56 443 → 62362 [ACK] Seq=6361 Ack=4333 Win=63488 Len=0
```

```
Transmission Control Protocol, Src Port: 62359, Dst Port: 80, Seq: 1, Ack: 1, Len: 638
    Source Port: 62359
    Destination Port: 80
    [Stream index: 2]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 638]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2493562177
    [Next Sequence Number: 639    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 701722641
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 513
    [Calculated window size: 131328]
    [Window size scaling factor: 256]
    Checksum: 0x0e56 [unverified]
```

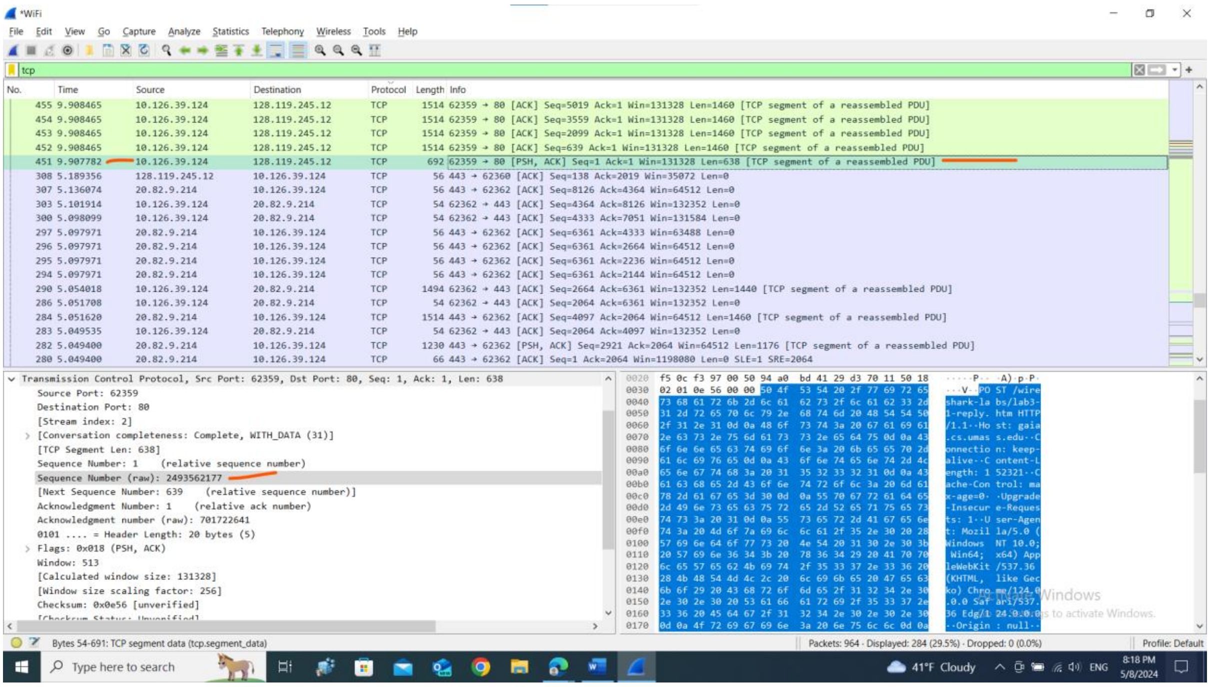
```
0020  f5 0c f3 97 00 50 94 a0  bd 41 29 d3 70 11 50 18   ·····P·· ·A)·p·P·
0030  02 01 0e 56 00 00 50 4f  53 54 20 2f 77 69 72 65   ···V··PO ST /wire
0040  73 68 61 72 6b 2d 6c 61  62 73 2f 6c 61 62 33 2d   shark-la bs/lab3-
0050  31 2d 72 65 70 6c 79 2e  68 74 6d 20 48 54 54 50   1-reply. htm HTTP
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 32 31 0d 0a 43   ength: 1 52321··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 32 34 2e 30   ko) Chro me/124.0
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  32 34 2e 30 2e 30 2e 30   36 Edg/1 24.0.0.0
0170  0d 0a 4f 72 69 67 69 6e  3a 20 6e 75 6c 6c 0d 0a   ··Origin : null··
```

Bytes 54-691: TCP segment data (tcp.segment_data)

Packets: 964 · Displayed: 284 (29.5%) · Dropped: 0 (0.0%)

Profile: Default

7. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the …..



```
tcp
No.   Time       Source          Destination     Protocol Length Info
  455 9.908465   10.126.39.124   128.119.245.12  TCP      1514 62359 → 80 [ACK] Seq=5019 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
  454 9.908465   10.126.39.124   128.119.245.12  TCP      1514 62359 → 80 [ACK] Seq=3559 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
  453 9.908465   10.126.39.124   128.119.245.12  TCP      1514 62359 → 80 [ACK] Seq=2099 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
  452 9.908465   10.126.39.124   128.119.245.12  TCP      1514 62359 → 80 [ACK] Seq=639 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
  451 9.907782   10.126.39.124   128.119.245.12  TCP       692 62359 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=638 [TCP segment of a reassembled PDU]
  308 5.189356   128.119.245.12  10.126.39.124   TCP        56 443 → 62360 [ACK] Seq=138 Ack=2019 Win=35072 Len=0
  307 5.136074   20.82.9.214     10.126.39.124   TCP        56 443 → 62362 [ACK] Seq=8126 Ack=4364 Win=64512 Len=0
  303 5.101914   10.126.39.124   20.82.9.214     TCP        54 62362 → 443 [ACK] Seq=4364 Ack=8126 Win=132352 Len=0
  300 5.098099   10.126.39.124   20.82.9.214     TCP        54 62362 → 443 [ACK] Seq=4333 Ack=7051 Win=131584 Len=0
  297 5.097971   20.82.9.214     10.126.39.124   TCP        56 443 → 62362 [ACK] Seq=6361 Ack=4333 Win=63488 Len=0
  296 5.097971   20.82.9.214     10.126.39.124   TCP        56 443 → 62362 [ACK] Seq=6361 Ack=2664 Win=64512 Len=0
  295 5.097971   20.82.9.214     10.126.39.124   TCP        56 443 → 62362 [ACK] Seq=6361 Ack=2236 Win=64512 Len=0
  294 5.097971   20.82.9.214     10.126.39.124   TCP        56 443 → 62362 [ACK] Seq=6361 Ack=2144 Win=64512 Len=0
  290 5.054018   10.126.39.124   20.82.9.214     TCP      1494 62362 → 443 [ACK] Seq=2664 Ack=6361 Win=132352 Len=1440 [TCP segment of a reassembled PDU]
  286 5.051708   10.126.39.124   20.82.9.214     TCP        54 62362 → 443 [ACK] Seq=2064 Ack=6361 Win=132352 Len=0
  284 5.051620   20.82.9.214     10.126.39.124   TCP      1514 443 → 62362 [ACK] Seq=4097 Ack=2064 Win=64512 Len=1460 [TCP segment of a reassembled PDU]
  283 5.049535   10.126.39.124   20.82.9.214     TCP        54 62362 → 443 [ACK] Seq=2064 Ack=4097 Win=132352 Len=0
  282 5.049400   20.82.9.214     10.126.39.124   TCP      1230 443 → 62362 [PSH, ACK] Seq=2921 Ack=2064 Win=64512 Len=1176 [TCP segment of a reassembled PDU]
  280 5.049400   20.82.9.214     10.126.39.124   TCP        66 443 → 62362 [ACK] Seq=1 Ack=2064 Win=1198080 Len=0 SLE=1 SRE=2064
```

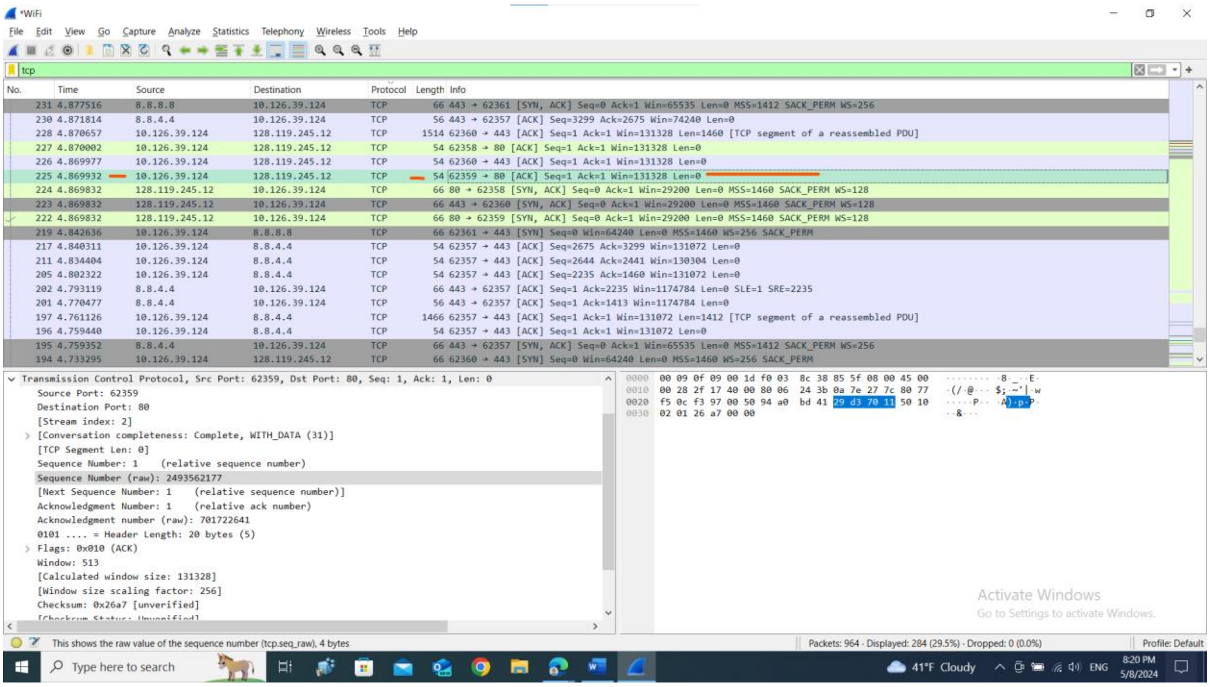
```
Transmission Control Protocol, Src Port: 62359, Dst Port: 80, Seq: 1, Ack: 1, Len: 638
    Source Port: 62359
    Destination Port: 80
    [Stream index: 2]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 638]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2493562177
    [Next Sequence Number: 639    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 701722641
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 513
    [Calculated window size: 131328]
    [Window size scaling factor: 256]
    Checksum: 0x0e56 [unverified]
```

```
0020  f5 0c f3 97 00 50 94 a0  bd 41 29 d3 70 11 50 18   ·····P·· ·A)·p·P·
0030  02 01 0e 56 00 00 50 4f  53 54 20 2f 77 69 72 65   ···V··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 32 31 0d 0a 43   ength: 1 52321··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 32 34 2e 30   ko) Chro me/124.0
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  32 34 2e 30 2e 30 2e 30   36 Edg/1 24.0.0.0
0170  0d 0a 4f 72 69 67 69 6e  3a 20 6e 75 6c 6c 0d 0a   ··Origin : null··
```

Bytes 54-691: TCP segment data (tcp.segment_data)

Packets: 964 · Displayed: 284 (29.5%) · Dropped: 0 (0.0%)

Profile: Default


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.   Time      Source          Destination     Protocol Length Info
  231 4.877516  8.8.8.8         10.126.39.124   TCP      66 443 → 62361 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
  230 4.871814  8.8.4.4         10.126.39.124   TCP      56 443 → 62357 [ACK] Seq=3299 Ack=2675 Win=74240 Len=0
  228 4.870657  10.126.39.124   128.119.245.12  TCP    1514 62360 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
  227 4.870002  10.126.39.124   128.119.245.12  TCP      54 62358 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  226 4.869977  10.126.39.124   128.119.245.12  TCP      54 62360 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  225 4.869932  10.126.39.124   128.119.245.12  TCP      54 62359 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  224 4.869832  128.119.245.12  10.126.39.124   TCP      66 80 → 62358 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
  223 4.869832  128.119.245.12  10.126.39.124   TCP      66 443 → 62360 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
  222 4.869832  128.119.245.12  10.126.39.124   TCP      66 80 → 62359 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
  219 4.842636  10.126.39.124   8.8.8.8         TCP      66 62361 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  217 4.840311  10.126.39.124   8.8.4.4         TCP      54 62357 → 443 [ACK] Seq=2675 Ack=3299 Win=131072 Len=0
  211 4.834404  10.126.39.124   8.8.4.4         TCP      54 62357 → 443 [ACK] Seq=2644 Ack=2441 Win=130304 Len=0
  205 4.802322  10.126.39.124   8.8.4.4         TCP      54 62357 → 443 [ACK] Seq=2235 Ack=1460 Win=131072 Len=0
  202 4.793119  8.8.4.4         10.126.39.124   TCP      66 443 → 62357 [ACK] Seq=1 Ack=2235 Win=1174784 Len=0 SLE=1 SRE=2235
  201 4.770477  8.8.4.4         10.126.39.124   TCP      56 443 → 62357 [ACK] Seq=1 Ack=1413 Win=1174784 Len=0
  197 4.761126  10.126.39.124   8.8.4.4         TCP    1466 62357 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=1412 [TCP segment of a reassembled PDU]
  196 4.759440  10.126.39.124   8.8.4.4         TCP      54 62357 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
  195 4.759352  8.8.4.4         10.126.39.124   TCP      66 443 → 62357 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
  194 4.733295  10.126.39.124   128.119.245.12  TCP      66 62360 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
```

```
v Transmission Control Protocol, Src Port: 62359, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
    Source Port: 62359
    Destination Port: 80
    [Stream index: 2]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2493562177
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 701722641
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window: 513
    [Calculated window size: 131328]
    [Window size scaling factor: 256]
    Checksum: 0x26a7 [unverified]
    [Checksum Status: Unverified]
```

```
0000  00 09 0f 09 00 1d f0 03  8c 38 85 5f 08 00 45 00   ········ ·8·_··E·
0010  00 28 2f 17 40 00 80 06  24 3b 0a 7e 27 7c 80 77   ·(/·@··· $;·~'|·w
0020  f5 0c f3 97 00 50 94 a0  bd 41 29 d3 70 11 50 10   ·····P·· ·A)·p·P·
0030  02 01 26 a7 00 00                                  ··&···
```

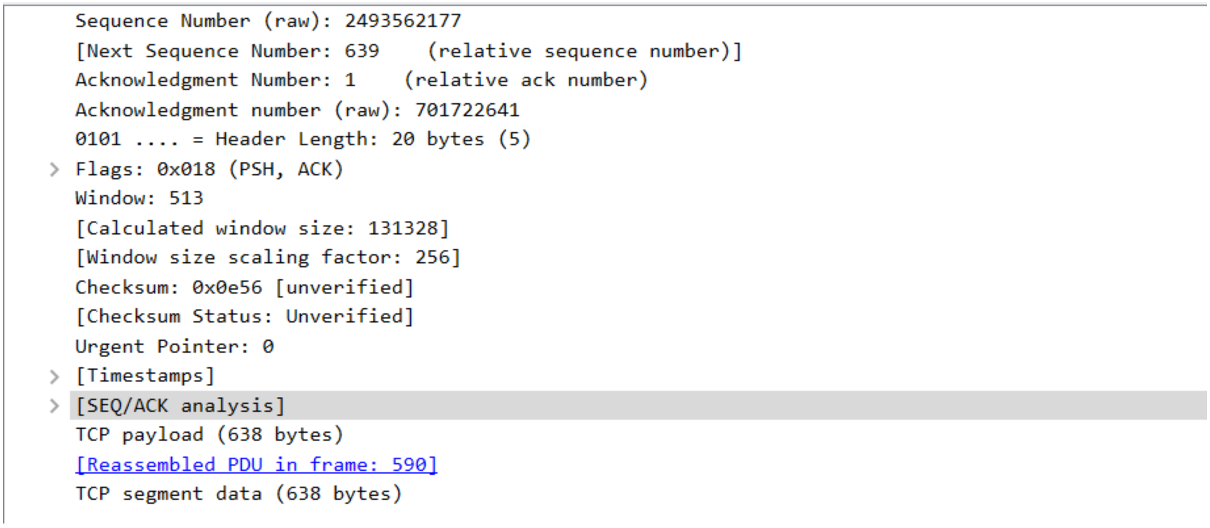
This shows the raw value of the sequence number (tcp.seq_raw), 4 bytes

Packets: 964 · Displayed: 284 (29.5%) · Dropped: 0 (0.0%)

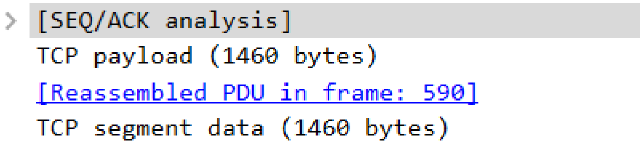
Profile: Default

RTT = receive time – send time .

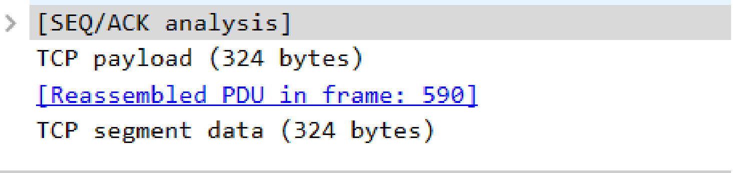
8. What is the length of each of the first six TCP segments?



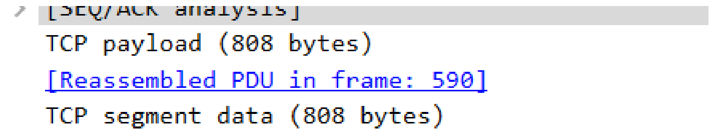
```
    Sequence Number (raw): 2493562177
    [Next Sequence Number: 639    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 701722641
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 513
    [Calculated window size: 131328]
    [Window size scaling factor: 256]
    Checksum: 0x0e56 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (638 bytes)
    [Reassembled PDU in frame: 590]
    TCP segment data (638 bytes)
```



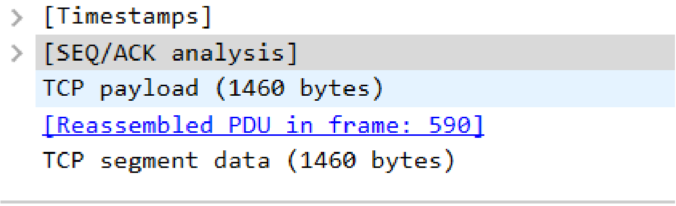
```
> [SEQ/ACK analysis]
  TCP payload (1460 bytes)
  [Reassembled PDU in frame: 590]
  TCP segment data (1460 bytes)
```



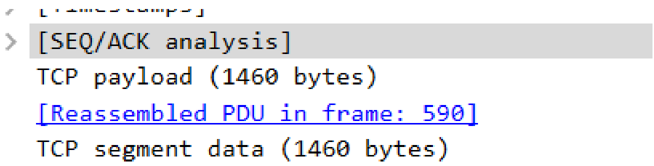
```
> [SEQ/ACK analysis]
  TCP payload (324 bytes)
  [Reassembled PDU in frame: 590]
  TCP segment data (324 bytes)
```



```
> [SEQ/ACK analysis]
  TCP payload (808 bytes)
  [Reassembled PDU in frame: 590]
  TCP segment data (808 bytes)
```

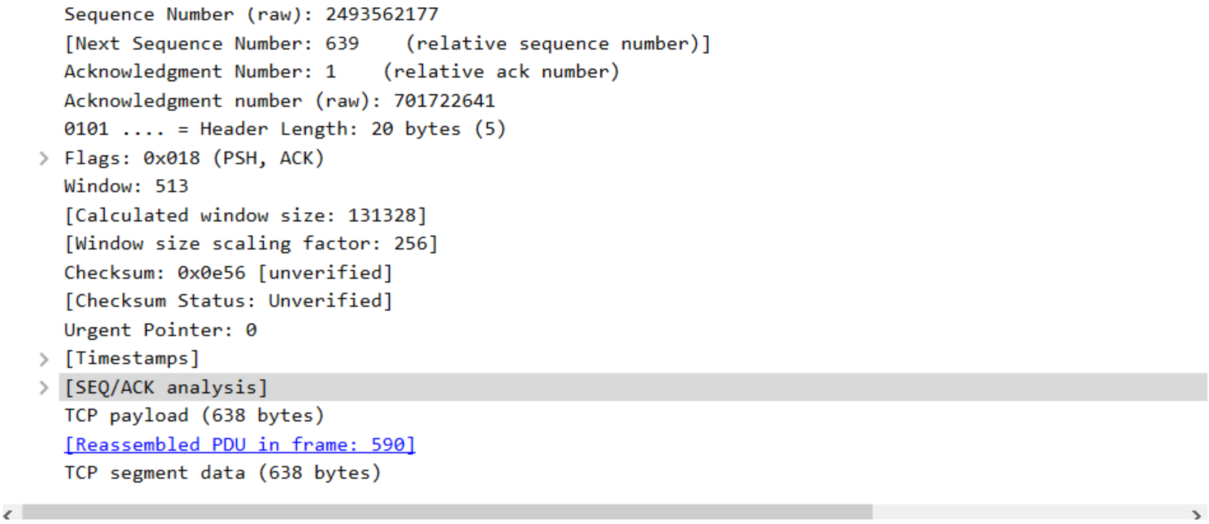


```
> [Timestamps]
> [SEQ/ACK analysis]
  TCP payload (1460 bytes)
  [Reassembled PDU in frame: 590]
  TCP segment data (1460 bytes)
```



```
> [Timestamps]
> [SEQ/ACK analysis]
  TCP payload (1460 bytes)
  [Reassembled PDU in frame: 590]
  TCP segment data (1460 bytes)
```

9. What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?



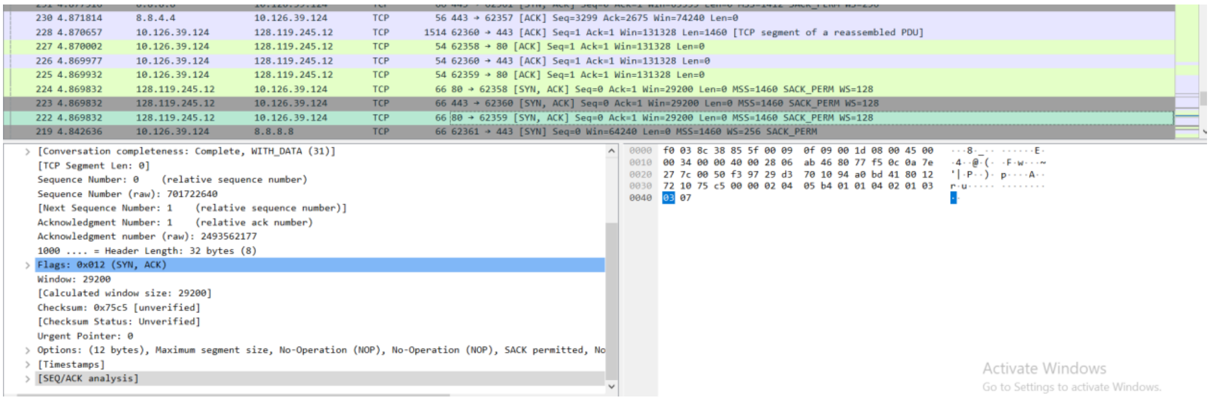
```
  Sequence Number (raw): 2493562177
  [Next Sequence Number: 639    (relative sequence number)]
  Acknowledgment Number: 1    (relative ack number)
  Acknowledgment number (raw): 701722641
  0101 .... = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
  Window: 513
  [Calculated window size: 131328]
  [Window size scaling factor: 256]
  Checksum: 0x0e56 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
> [Timestamps]
> [SEQ/ACK analysis]
  TCP payload (638 bytes)
  [Reassembled PDU in frame: 590]
  TCP segment data (638 bytes)
```

No ..segment length less then window size

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

Ans. No. I check the source port .

11. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is ACKing every other received segment

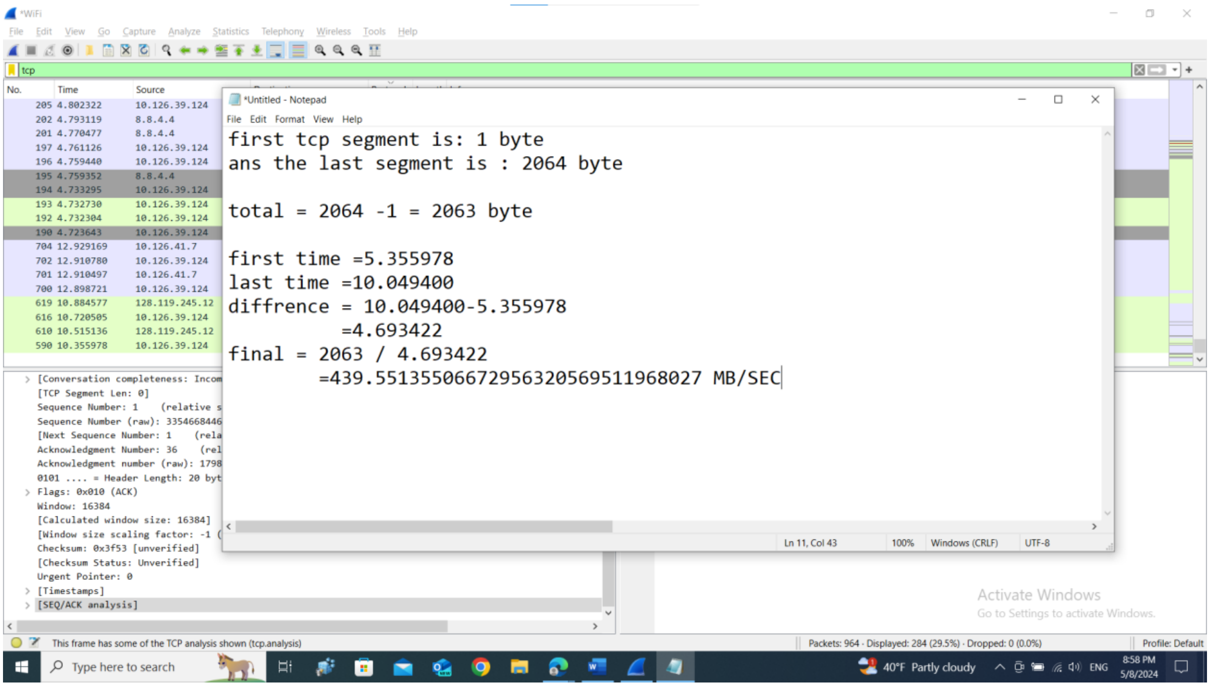


```
230 4.871814  8.8.4.4         10.126.39.124   TCP    56 443 → 62357 [ACK] Seq=3299 Ack=2675 Win=74240 Len=0
228 4.870657  10.126.39.124   128.119.245.12  TCP  1514 62360 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=1460 [TCP segment of a reassembled PDU]
227 4.870002  10.126.39.124   128.119.245.12  TCP    54 62358 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
226 4.869977  10.126.39.124   128.119.245.12  TCP    54 62360 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
225 4.869932  10.126.39.124   128.119.245.12  TCP    54 62359 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
224 4.869832  128.119.245.12  10.126.39.124   TCP    66 80 → 62358 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
223 4.869832  128.119.245.12  10.126.39.124   TCP    66 443 → 62360 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
222 4.869832  128.119.245.12  10.126.39.124   TCP    66 80 → 62359 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
219 4.842636  10.126.39.124   8.8.8.8         TCP    66 62361 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
```

```
> [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 0    (relative sequence number)
  Sequence Number (raw): 701722640
  [Next Sequence Number: 1    (relative sequence number)]
  Acknowledgment Number: 1    (relative ack number)
  Acknowledgment number (raw): 2493562177
  1000 .... = Header Length: 32 bytes (8)
> Flags: 0x012 (SYN, ACK)
  Window: 29200
  [Calculated window size: 29200]
  Checksum: 0x75c5 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
> Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No
> [Timestamps]
> [SEQ/ACK analysis]
```

```
0000  f0 03 8c 38 85 5f 00 09  0f 09 00 1d 08 00 45 00   ···8·_·· ······E·
0010  00 34 00 00 40 00 28 06  ab 46 80 77 f5 0c 0a 7e   ·4··@·(· ·F·w···~
0020  27 7c 00 50 f3 97 29 d3  70 10 94 a0 bd 41 80 12   '|·P··)· p····A··
0030  72 10 75 c5 00 00 02 04  05 b4 01 01 04 02 01 03   r·u····· ········
0040  03 07                                              ·
```

12. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value



*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No.
Time
Source

```
205 4.802322   10.126.39.124
202 4.793119   8.8.4.4
201 4.770477   8.8.4.4
197 4.761126   10.126.39.124
196 4.759440   10.126.39.124
195 4.759352   8.8.4.4
194 4.733295   10.126.39.124
193 4.732730   10.126.39.124
192 4.732304   10.126.39.124
190 4.723643   10.126.39.124
704 12.929169  10.126.41.7
702 12.910780  10.126.39.124
701 12.910497  10.126.41.7
700 12.898721  10.126.39.124
619 10.884577  128.119.245.12
616 10.720505  10.126.39.124
610 10.515136  128.119.245.12
590 10.355978  10.126.39.124
```

```
> [Conversation completeness: Incom
  [TCP Segment Len: 0]
  Sequence Number: 1    (relative s
  Sequence Number (raw): 3354668446
  [Next Sequence Number: 1    (rela
  Acknowledgment Number: 36    (rel
  Acknowledgment number (raw): 1798
  0101 .... = Header Length: 20 byt
> Flags: 0x010 (ACK)
  Window: 16384
  [Calculated window size: 16384]
  [Window size scaling factor: -1 (
  Checksum: 0x3f53 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
> [Timestamps]
> [SEQ/ACK analysis]
```

```
first tcp segment is: 1 byte
ans the last segment is : 2064 byte

total = 2064 -1 = 2063 byte

first time =5.355978
last time =10.049400
diffrence = 10.049400-5.355978
           =4.693422
final = 2063 / 4.693422
        =439.55135506672956320569511968027 MB/SEC
```

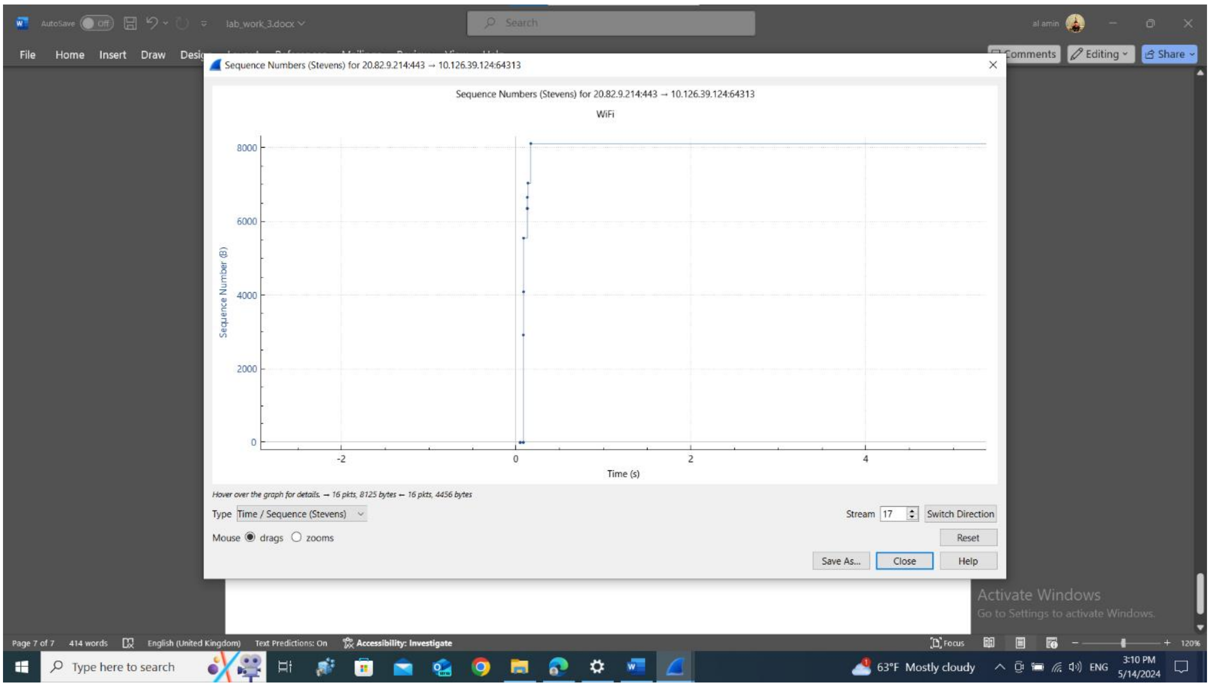
This frame has some of the TCP analysis shown (tcp.analysis)

Packets: 964 · Displayed: 284 (29.5%) · Dropped: 0 (0.0%)

Profile: Default

13. 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. Can you identify where TCP's slowstart phase begins and ends, and where congestion avoidance takes over? Comment on ways in which the measured data differs from the idealized behavior of TCP that we've

studied in the text.



Sequence Numbers (Stevens) for 20.82.9.214:443 → 10.126.39.124:64313

Sequence Numbers (Stevens) for 20.82.9.214:443 → 10.126.39.124:64313
WiFi
Sequence Number (B)
8000
6000
4000
2000
0
-2
0
2
4
Time (s)

Hover over the graph for details. → 16 pkts, 8125 bytes ← 16 pkts, 4456 bytes

Type Time / Sequence (Stevens)

Stream 17

Mouse ● drags ○ zooms

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?
    Ans. Already answer in the avobe.