CSE 3111: Computer Networking Lab

TCP LAB

Wireshark TCP Analysis

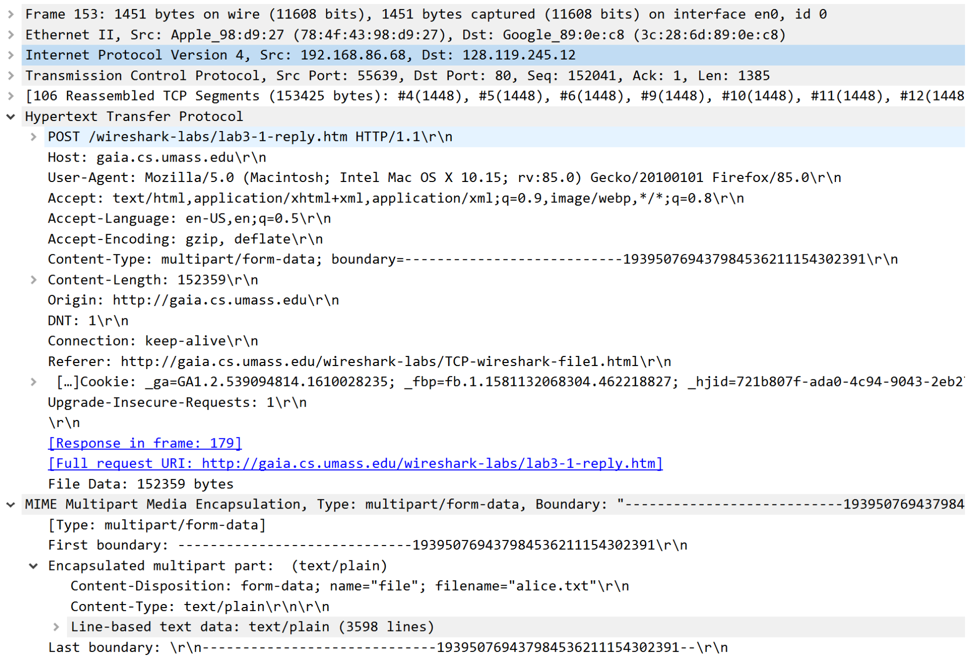
H.M. Mehedi Hasan(13)
Abu Bakar Siddique(47)

1. Client IP and TCP Port

Question:

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`? To answer this question, it's probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the "details of the selected packet header window".

Answer:



```
Frame 153: 1451 bytes on wire (11608 bits), 1451 bytes captured (11608 bits) on interface en0, id 0
Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Google_89:0e:c8 (3c:28:6d:89:0e:c8)
Internet Protocol Version 4, Src: 192.168.86.68, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55639, Dst Port: 80, Seq: 152041, Ack: 1, Len: 1385
[106 Reassembled TCP Segments (153425 bytes): #4(1448), #5(1448), #6(1448), #9(1448), #10(1448), #11(1448), #12(1448
Hypertext Transfer Protocol
  POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:85.0) Gecko/20100101 Firefox/85.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Content-Type: multipart/form-data; boundary=---------------------------193950769437984536211154302391\r\n
  Content-Length: 152359\r\n
  Origin: http://gaia.cs.umass.edu\r\n
  DNT: 1\r\n
  Connection: keep-alive\r\n
  Referer: http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html\r\n
   […]Cookie: _ga=GA1.2.539094814.1610028235; _fbp=fb.1.1581132068304.462218827; _hjid=721b807f-ada0-4c94-9043-2eb2
  Upgrade-Insecure-Requests: 1\r\n
  \r\n
  [Response in frame: 179]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/lab3-1-reply.htm]
  File Data: 152359 bytes
MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "---------------------------193950769437984
  [Type: multipart/form-data]
  First boundary: -----------------------------193950769437984536211154302391\r\n
  Encapsulated multipart part:  (text/plain)
    Content-Disposition: form-data; name="file"; filename="alice.txt"\r\n
    Content-Type: text/plain\r\n\r\n
    Line-based text data: text/plain (3598 lines)
  Last boundary: \r\n-----------------------------193950769437984536211154302391--\r\n
```

Client IP: `192.168.86.68`

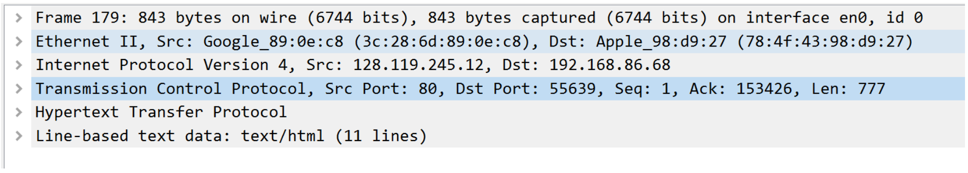
TCP Port: `55639`

2. Server IP and Port

Question:

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

Answer:



```
Frame 179: 843 bytes on wire (6744 bits), 843 bytes captured (6744 bits) on interface en0, id 0
Ethernet II, Src: Google_89:0e:c8 (3c:28:6d:89:0e:c8), Dst: Apple_98:d9:27 (78:4f:43:98:d9:27)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.86.68
Transmission Control Protocol, Src Port: 80, Dst Port: 55639, Seq: 1, Ack: 153426, Len: 777
Hypertext Transfer Protocol
Line-based text data: text/html (11 lines)
```

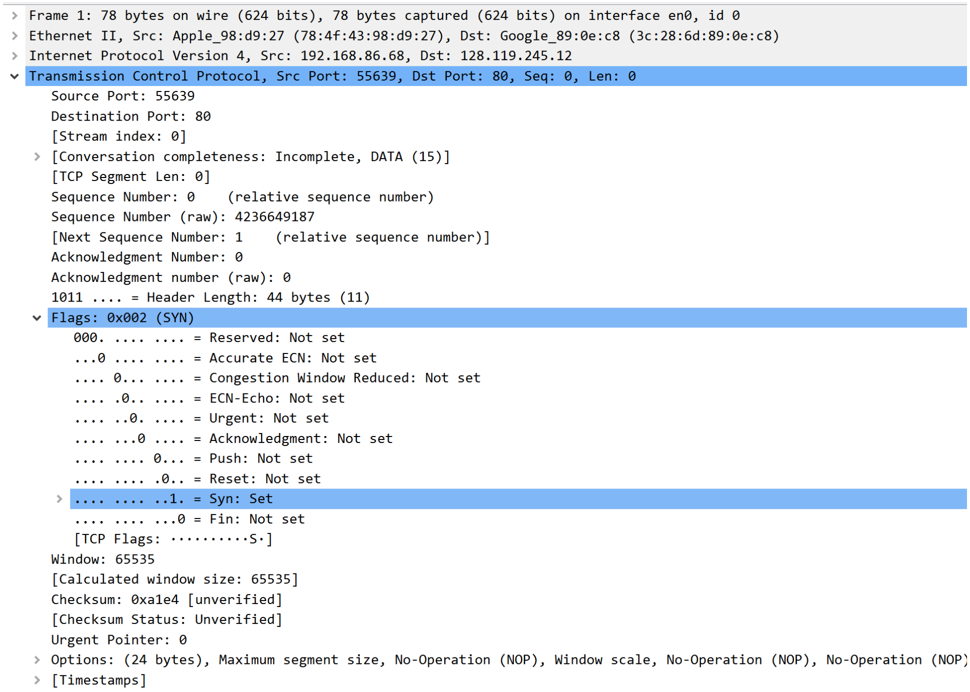
Server IP: 128.119.245.12
Sending: 55639
Receiving: 80

3. TCP SYN Segment

Question:

What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client and server? What identifies the segment as a SYN? Will the receiver be able to use Selective Acknowledgments (SACK)?

Answer:



```
> Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface en0, id 0
> Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Google_89:0e:c8 (3c:28:6d:89:0e:c8)
> Internet Protocol Version 4, Src: 192.168.86.68, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 55639, Dst Port: 80, Seq: 0, Len: 0
     Source Port: 55639
     Destination Port: 80
     [Stream index: 0]
   > [Conversation completeness: Incomplete, DATA (15)]
     [TCP Segment Len: 0]
     Sequence Number: 0    (relative sequence number)
     Sequence Number (raw): 4236649187
     [Next Sequence Number: 1    (relative sequence number)]
     Acknowledgment Number: 0
     Acknowledgment number (raw): 0
     1011 .... = Header Length: 44 bytes (11)
   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: 65535
     [Calculated window size: 65535]
     Checksum: 0xa1e4 [unverified]
     [Checksum Status: Unverified]
     Urgent Pointer: 0
   > Options: (24 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP)
   > [Timestamps]
```

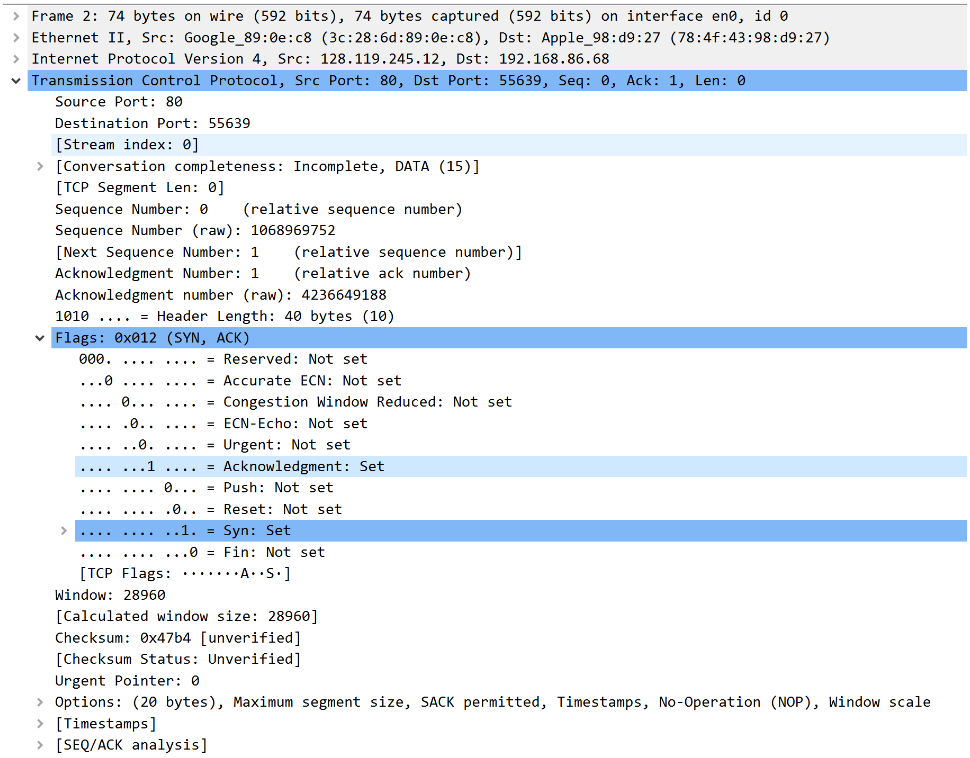
Sequence Number (Raw): 4236649187
Flags: 0x002 (SYN)
Yes, in the TCP Options, the “SACK Permitted” option appears.

4. TCP SYN-ACK Segment

Question:

What is the sequence number of the SYN-ACK segment sent by the server? What identifies it as a SYN-ACK? What is the value of the Acknowledgment field in the SYN-ACK segment, and how was it determined?

Answer:



```
> Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface en0, id 0
> Ethernet II, Src: Google_89:0e:c8 (3c:28:6d:89:0e:c8), Dst: Apple_98:d9:27 (78:4f:43:98:d9:27)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.86.68
v Transmission Control Protocol, Src Port: 80, Dst Port: 55639, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 55639
    [Stream index: 0]
  > [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1068969752
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 4236649188
    1010 .... = Header Length: 40 bytes (10)
  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: 28960
    [Calculated window size: 28960]
    Checksum: 0x47b4 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
  > [Timestamps]
  > [SEQ/ACK analysis]
```

SYN-ACK Sequence Number (Raw): `1068969752`
Flags: `0x012 (SYN, ACK)`
Acknowledgment Number (Raw): `4236649188`

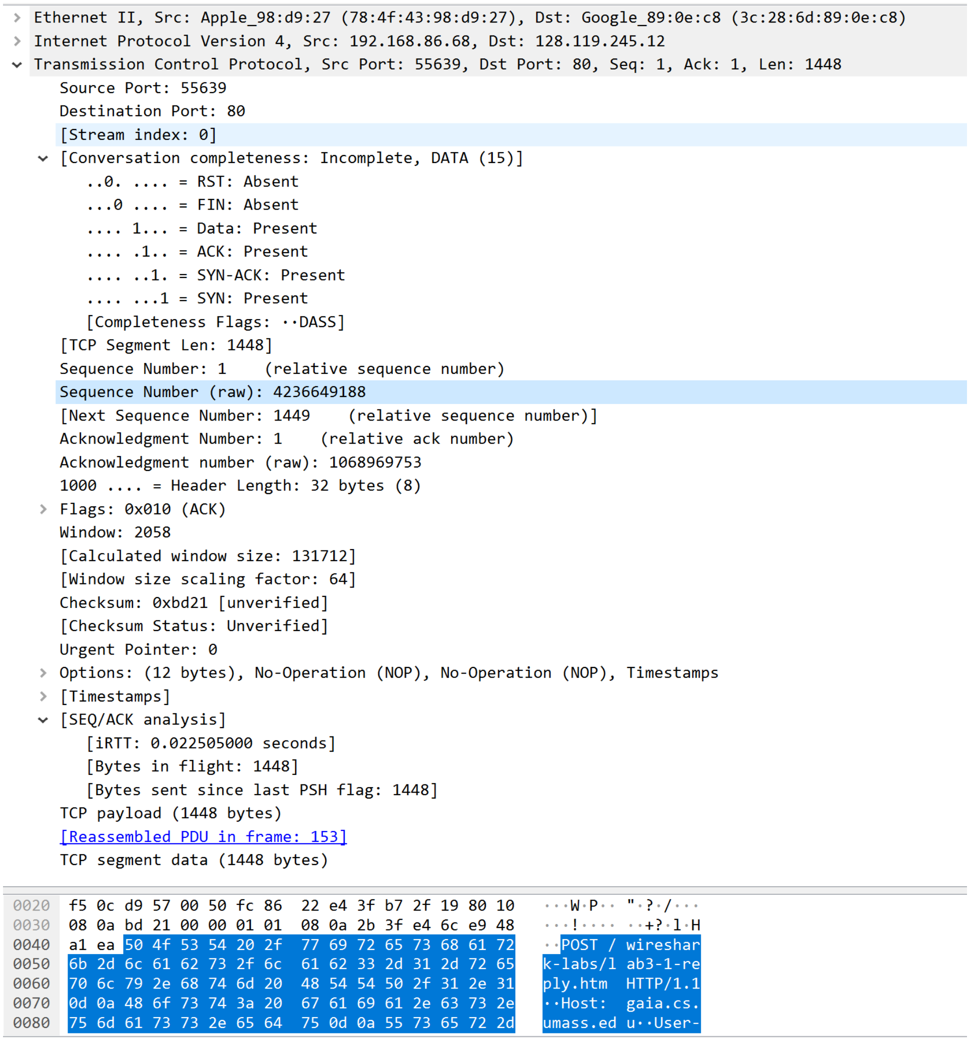
$$\text{Ack}_{\text{raw}} = \text{Client Initial Seq} + 1 = 4236649187 + 1 = 4236649188$$

The acknowledgment is derived from the client's initial sequence number.

5. HTTP POST Command Segment

Question:
What is the sequence number of the TCP segment containing the HTTP POST command? How many bytes of data are contained in the payload of this TCP segment? Did all of the data in the file fit into this single segment?

Answer:



```
›  Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Google_89:0e:c8 (3c:28:6d:89:0e:c8)
›  Internet Protocol Version 4, Src: 192.168.86.68, Dst: 128.119.245.12
⌄  Transmission Control Protocol, Src Port: 55639, Dst Port: 80, Seq: 1, Ack: 1, Len: 1448
      Source Port: 55639
      Destination Port: 80
      [Stream index: 0]
   ⌄  [Conversation completeness: Incomplete, DATA (15)]
         ..0. .... = RST: Absent
         ...0 .... = FIN: Absent
         .... 1... = Data: Present
         .... .1.. = ACK: Present
         .... ..1. = SYN-ACK: Present
         .... ...1 = SYN: Present
         [Completeness Flags: ··DASS]
      [TCP Segment Len: 1448]
      Sequence Number: 1    (relative sequence number)
      Sequence Number (raw): 4236649188
      [Next Sequence Number: 1449    (relative sequence number)]
      Acknowledgment Number: 1    (relative ack number)
      Acknowledgment number (raw): 1068969753
      1000 .... = Header Length: 32 bytes (8)
   ›  Flags: 0x010 (ACK)
      Window: 2058
      [Calculated window size: 131712]
      [Window size scaling factor: 64]
      Checksum: 0xbd21 [unverified]
      [Checksum Status: Unverified]
      Urgent Pointer: 0
   ›  Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
   ›  [Timestamps]
   ⌄  [SEQ/ACK analysis]
         [iRTT: 0.022505000 seconds]
         [Bytes in flight: 1448]
         [Bytes sent since last PSH flag: 1448]
      TCP payload (1448 bytes)
      [Reassembled PDU in frame: 153]
      TCP segment data (1448 bytes)

0020  f5 0c d9 57 00 50 fc 86  22 e4 3f b7 2f 19 80 10   ···W·P··  "·?·/···
0030  08 0a bd 21 00 00 01 01  08 0a 2b 3f e4 6c e9 48   ···!····  ··+?·l·H
0040  a1 ea 50 4f 53 54 20 2f  77 69 72 65 73 68 61 72   ··POST /  wireshar
0050  6b 2d 6c 61 62 73 2f 6c  61 62 33 2d 31 2d 72 65   k-labs/l  ab3-1-re
0060  70 6c 79 2e 68 74 6d 20  48 54 54 50 2f 31 2e 31   ply.htm   HTTP/1.1
0070  0d 0a 48 6f 73 74 3a 20  67 61 69 61 2e 63 73 2e   ··Host:   gaia.cs.
0080  75 6d 61 73 73 2e 65 64  75 0d 0a 55 73 65 72 2d   umass.ed  u··User-
```

Sequence Number (Raw): `4236649188`, Relative: `1`

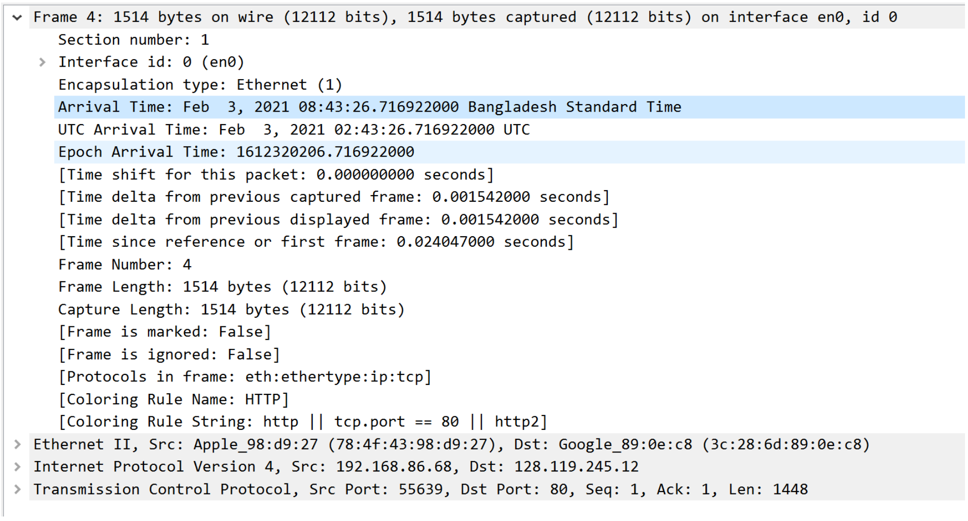
TCP Payload: `1448 bytes`

No, the `POST` request (including `alice.txt`) spans multiple TCP segments (106 reassembled, total 153,425 bytes).

6. RTT Calculations

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

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

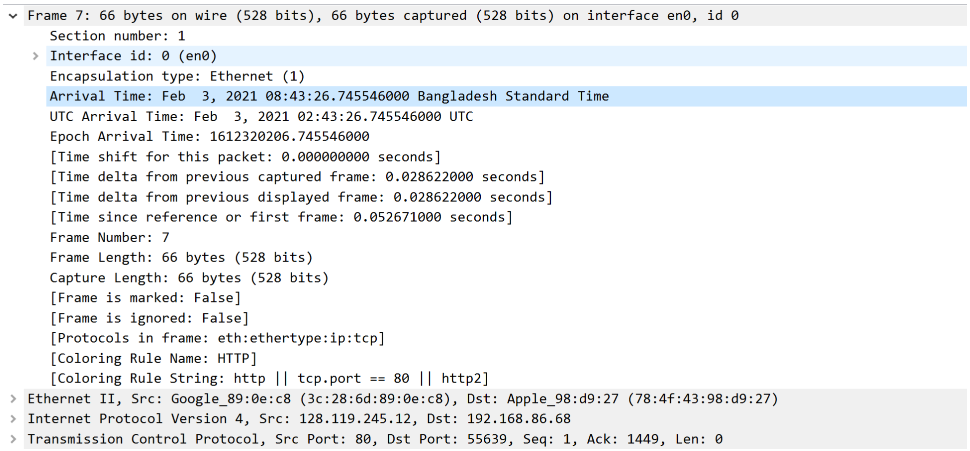


```
⌄ Frame 4: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0, id 0
     Section number: 1
   › Interface id: 0 (en0)
     Encapsulation type: Ethernet (1)
     Arrival Time: Feb  3, 2021 08:43:26.716922000 Bangladesh Standard Time
     UTC Arrival Time: Feb  3, 2021 02:43:26.716922000 UTC
     Epoch Arrival Time: 1612320206.716922000
     [Time shift for this packet: 0.000000000 seconds]
     [Time delta from previous captured frame: 0.001542000 seconds]
     [Time delta from previous displayed frame: 0.001542000 seconds]
     [Time since reference or first frame: 0.024047000 seconds]
     Frame Number: 4
     Frame Length: 1514 bytes (12112 bits)
     Capture Length: 1514 bytes (12112 bits)
     [Frame is marked: False]
     [Frame is ignored: False]
     [Protocols in frame: eth:ethertype:ip:tcp]
     [Coloring Rule Name: HTTP]
     [Coloring Rule String: http || tcp.port == 80 || http2]
› Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Google_89:0e:c8 (3c:28:6d:89:0e:c8)
› Internet Protocol Version 4, Src: 192.168.86.68, Dst: 128.119.245.12
› Transmission Control Protocol, Src Port: 55639, Dst Port: 80, Seq: 1, Ack: 1, Len: 1448
```

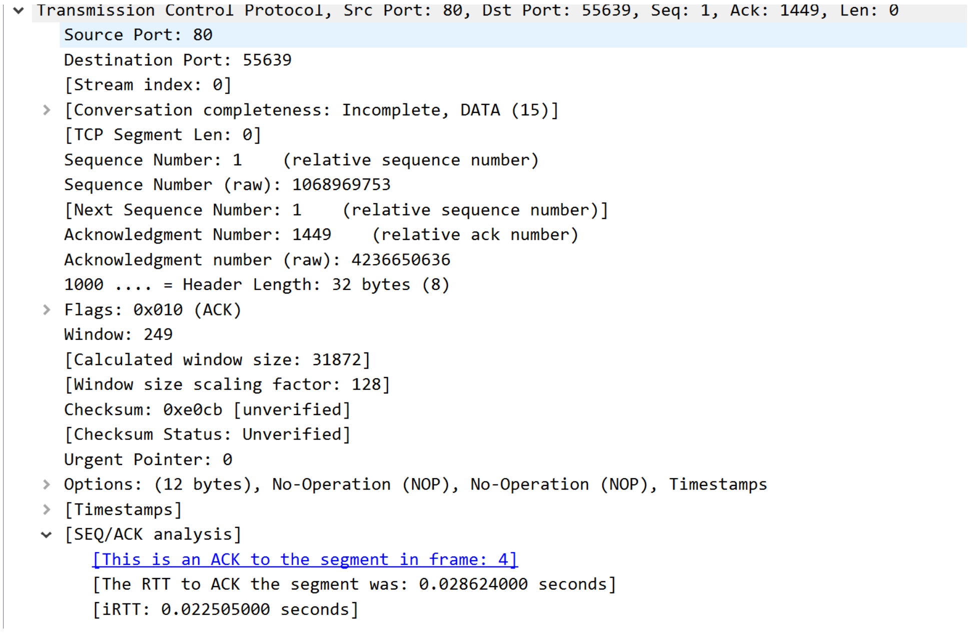
Figure: *Time of First Segment (Frame 4)*

Answer: Feb 3, 2021 08:43:26.716922000 BST

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



```
⌄ Frame 7: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0
     Section number: 1
   › Interface id: 0 (en0)
     Encapsulation type: Ethernet (1)
     Arrival Time: Feb  3, 2021 08:43:26.745546000 Bangladesh Standard Time
     UTC Arrival Time: Feb  3, 2021 02:43:26.745546000 UTC
     Epoch Arrival Time: 1612320206.745546000
     [Time shift for this packet: 0.000000000 seconds]
     [Time delta from previous captured frame: 0.028622000 seconds]
     [Time delta from previous displayed frame: 0.028622000 seconds]
     [Time since reference or first frame: 0.052671000 seconds]
     Frame Number: 7
     Frame Length: 66 bytes (528 bits)
     Capture Length: 66 bytes (528 bits)
     [Frame is marked: False]
     [Frame is ignored: False]
     [Protocols in frame: eth:ethertype:ip:tcp]
     [Coloring Rule Name: HTTP]
     [Coloring Rule String: http || tcp.port == 80 || http2]
› Ethernet II, Src: Google_89:0e:c8 (3c:28:6d:89:0e:c8), Dst: Apple_98:d9:27 (78:4f:43:98:d9:27)
› Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.86.68
› Transmission Control Protocol, Src Port: 80, Dst Port: 55639, Seq: 1, Ack: 1449, Len: 0
```

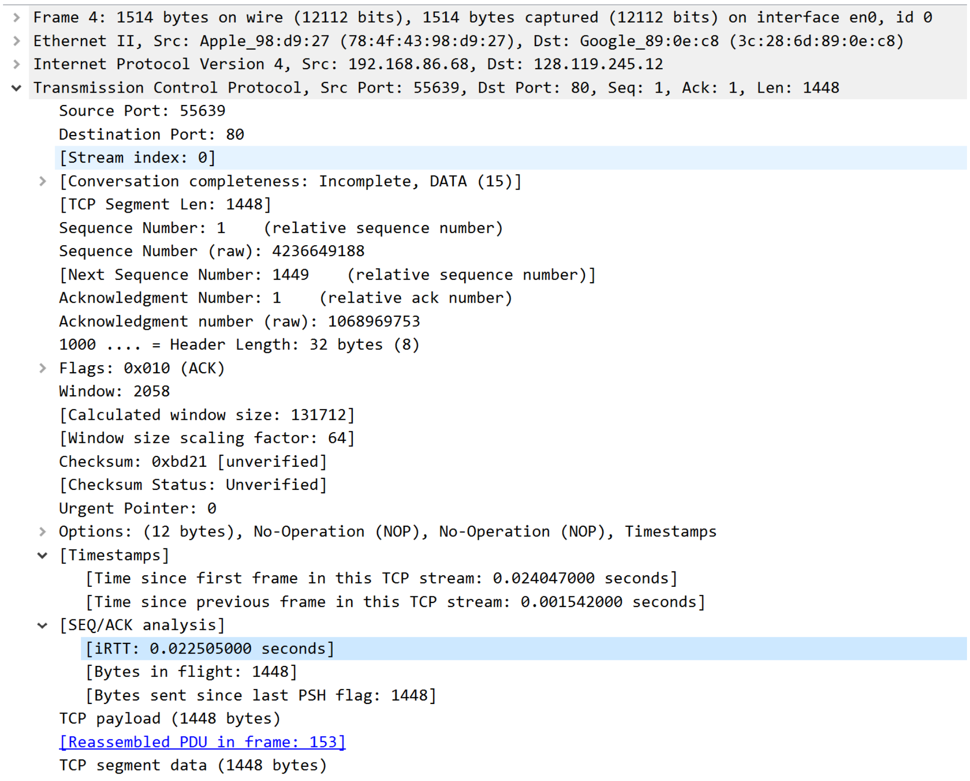


```
⌄ Transmission Control Protocol, Src Port: 80, Dst Port: 55639, Seq: 1, Ack: 1449, Len: 0
    Source Port: 80
    Destination Port: 55639
    [Stream index: 0]
  › [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1068969753
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1449    (relative ack number)
    Acknowledgment number (raw): 4236650636
    1000 .... = Header Length: 32 bytes (8)
  › Flags: 0x010 (ACK)
    Window: 249
    [Calculated window size: 31872]
    [Window size scaling factor: 128]
    Checksum: 0xe0cb [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  › Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  › [Timestamps]
  ⌄ [SEQ/ACK analysis]
       [This is an ACK to the segment in frame: 4]
       [The RTT to ACK the segment was: 0.028624000 seconds]
       [iRTT: 0.022505000 seconds]
```

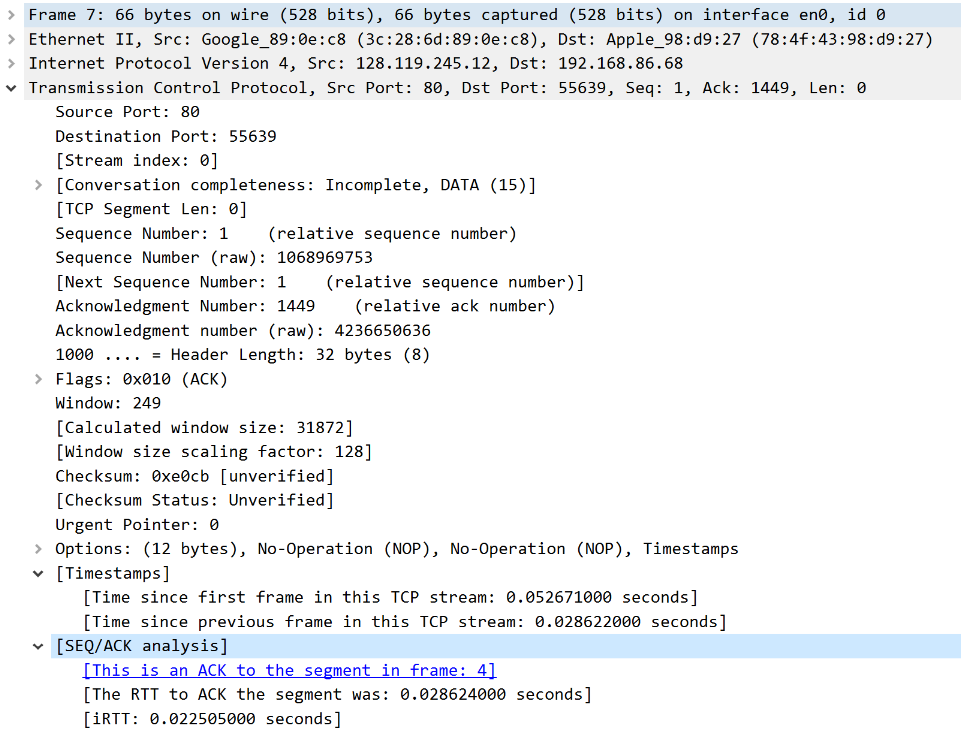
Figure: *Time of ACK (Frame 7)*

Answer: Feb 3, 2021 08:43:26.745546000 BST

c) What is the RTT for this first data-containing segment? (First data segment Frame 4 and First ACK Frame 7)



```
› Frame 4: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0, id 0
› Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Google_89:0e:c8 (3c:28:6d:89:0e:c8)
› Internet Protocol Version 4, Src: 192.168.86.68, Dst: 128.119.245.12
⌄ Transmission Control Protocol, Src Port: 55639, Dst Port: 80, Seq: 1, Ack: 1, Len: 1448
    Source Port: 55639
    Destination Port: 80
    [Stream index: 0]
  › [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 1448]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 4236649188
    [Next Sequence Number: 1449    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1068969753
    1000 .... = Header Length: 32 bytes (8)
  › Flags: 0x010 (ACK)
    Window: 2058
    [Calculated window size: 131712]
    [Window size scaling factor: 64]
    Checksum: 0xbd21 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  › Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ⌄ [Timestamps]
       [Time since first frame in this TCP stream: 0.024047000 seconds]
       [Time since previous frame in this TCP stream: 0.001542000 seconds]
  ⌄ [SEQ/ACK analysis]
       [iRTT: 0.022505000 seconds]
       [Bytes in flight: 1448]
       [Bytes sent since last PSH flag: 1448]
    TCP payload (1448 bytes)
    [Reassembled PDU in frame: 153]
    TCP segment data (1448 bytes)
```



```
> Frame 7: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0
> Ethernet II, Src: Google_89:0e:c8 (3c:28:6d:89:0e:c8), Dst: Apple_98:d9:27 (78:4f:43:98:d9:27)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.86.68
v Transmission Control Protocol, Src Port: 80, Dst Port: 55639, Seq: 1, Ack: 1449, Len: 0
     Source Port: 80
     Destination Port: 55639
     [Stream index: 0]
   > [Conversation completeness: Incomplete, DATA (15)]
     [TCP Segment Len: 0]
     Sequence Number: 1    (relative sequence number)
     Sequence Number (raw): 1068969753
     [Next Sequence Number: 1    (relative sequence number)]
     Acknowledgment Number: 1449    (relative ack number)
     Acknowledgment number (raw): 4236650636
     1000 .... = Header Length: 32 bytes (8)
   > Flags: 0x010 (ACK)
     Window: 249
     [Calculated window size: 31872]
     [Window size scaling factor: 128]
     Checksum: 0xe0cb [unverified]
     [Checksum Status: Unverified]
     Urgent Pointer: 0
   > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
   v [Timestamps]
        [Time since first frame in this TCP stream: 0.052671000 seconds]
        [Time since previous frame in this TCP stream: 0.028622000 seconds]
   v [SEQ/ACK analysis]
        [This is an ACK to the segment in frame: 4]
        [The RTT to ACK the segment was: 0.028624000 seconds]
        [iRTT: 0.022505000 seconds]
```

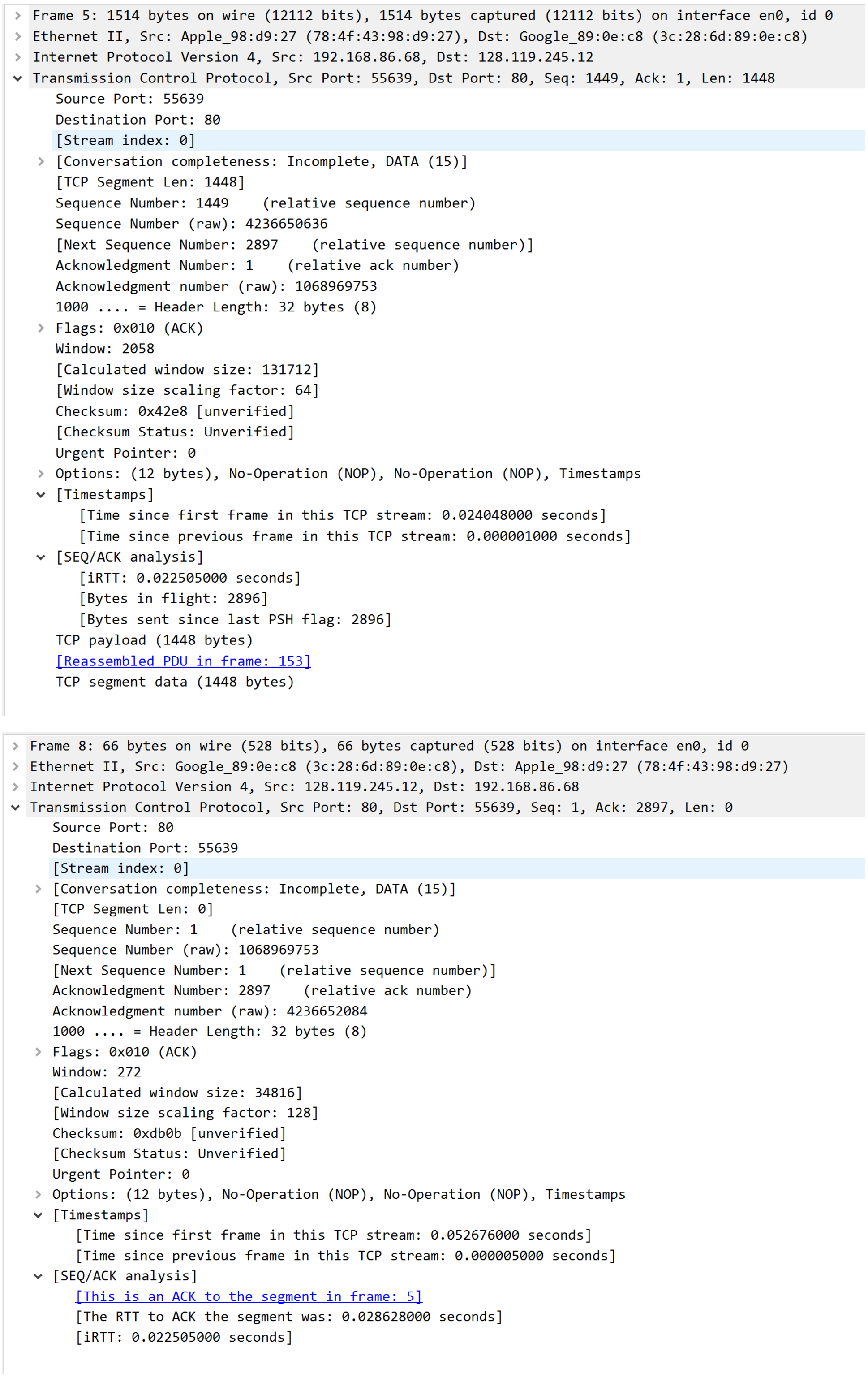
Figure: *RTT for First Data Segment*

$$\text{RTT} = \text{Time}_{ACK} - \text{Time}_{DataSegment}$$

$$\text{RTT} = 0.052671000 - 0.024047000 = 0.028624000 \text{ s}$$

Answer: RTT = `0.028624000 s`

d) What is the RTT value of the second data-carrying TCP segment and its ACK? (2nd data segment Frame 4 and the 2nd ACK Frame 8)



```
> Frame 5: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0, id 0
> Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Google_89:0e:c8 (3c:28:6d:89:0e:c8)
> Internet Protocol Version 4, Src: 192.168.86.68, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 55639, Dst Port: 80, Seq: 1449, Ack: 1, Len: 1448
    Source Port: 55639
    Destination Port: 80
    [Stream index: 0]
  > [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 1448]
    Sequence Number: 1449    (relative sequence number)
    Sequence Number (raw): 4236650636
    [Next Sequence Number: 2897    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1068969753
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x010 (ACK)
    Window: 2058
    [Calculated window size: 131712]
    [Window size scaling factor: 64]
    Checksum: 0x42e8 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  v [Timestamps]
      [Time since first frame in this TCP stream: 0.024048000 seconds]
      [Time since previous frame in this TCP stream: 0.000001000 seconds]
  v [SEQ/ACK analysis]
      [iRTT: 0.022505000 seconds]
      [Bytes in flight: 2896]
      [Bytes sent since last PSH flag: 2896]
    TCP payload (1448 bytes)
    [Reassembled PDU in frame: 153]
    TCP segment data (1448 bytes)
```

```
> Frame 8: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0
> Ethernet II, Src: Google_89:0e:c8 (3c:28:6d:89:0e:c8), Dst: Apple_98:d9:27 (78:4f:43:98:d9:27)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.86.68
v Transmission Control Protocol, Src Port: 80, Dst Port: 55639, Seq: 1, Ack: 2897, Len: 0
    Source Port: 80
    Destination Port: 55639
    [Stream index: 0]
  > [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1068969753
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 2897    (relative ack number)
    Acknowledgment number (raw): 4236652084
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x010 (ACK)
    Window: 272
    [Calculated window size: 34816]
    [Window size scaling factor: 128]
    Checksum: 0xdb0b [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  v [Timestamps]
      [Time since first frame in this TCP stream: 0.052676000 seconds]
      [Time since previous frame in this TCP stream: 0.000005000 seconds]
  v [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 5]
      [The RTT to ACK the segment was: 0.028628000 seconds]
      [iRTT: 0.022505000 seconds]
```

Figure: *RTT for Second Data Segment*

$$\text{RTT} = 0.052676000 - 0.024048000 = 0.028628000 \text{ s}$$

Answer: RTT = `0.028628000 s`

e) What is the EstimatedRTT value (see Section 3.5.3 in the text) after the ACK for the second data-carrying segment is received? Assume that in making this calculation after the received of the ACK for the second segment, that the initial value of EstimatedRTT is equal to the measured RTT for the first segment, and then is computed using the EstimatedRTT equation on page 242, and a value of $\alpha = 0.125$.

$$\text{EstimatedRTT} = (1-\alpha) \times \text{RTT}_{\text{prev}} + \alpha \times \text{SampleRTT}$$

Where $\alpha = 0.125$

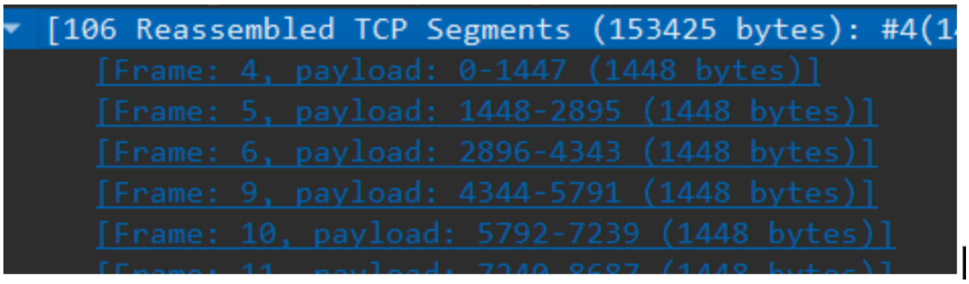
$$\text{EstimatedRTT} = 0.875(0.028624000) + 0.125(0.028628000) = 0.0286245 \text{ s}$$

Answer: Estimated RTT = `0.0286245 s`

7. Segment Lengths

Question:
What is the length (header plus payload) of each of the first four data-carrying TCP segments?

Answer:



```
[106 Reassembled TCP Segments (153425 bytes): #4(1
    [Frame: 4, payload: 0-1447 (1448 bytes)]
    [Frame: 5, payload: 1448-2895 (1448 bytes)]
    [Frame: 6, payload: 2896-4343 (1448 bytes)]
    [Frame: 9, payload: 4344-5791 (1448 bytes)]
    [Frame: 10, payload: 5792-7239 (1448 bytes)]
    [Frame: 11, payload: 7240-8687 (1448 bytes)]
```

TCP Header = 32 bytes
Payload = 1448 bytes
Each segment: 1448 + 32 = 1480 bytes

8. Receiver Buffer Space

Question:
What is the minimum amount of available buffer space advertised to the client among the first four data-carrying TCP segments? Does lack of receiver buffer space throttle the sender?

Answer:

ACK 1 (Frame 7)	31,872 bytes
ACK 2 (Frame 8)	34,816 bytes
ACK 3 (Frame 13)	37,760 bytes
ACK 4 (Frame 16)	40,576 bytes

Minimum Advertised Buffer Space = `34,816 bytes`

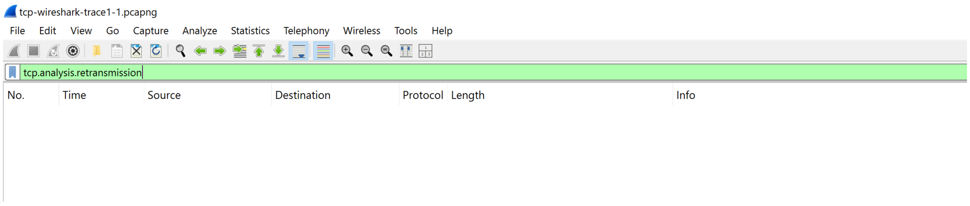
No throttling occurred; ample buffer space was available.

9. Retransmissions

Question:

Are there any retransmitted segments in the trace file? What did you check to confirm?

Answer:



tcp-wireshark-trace1-1.pcapng

tcp.analysis.retransmission

```
No.   Time   Source   Destination   Protocol  Length   Info
```

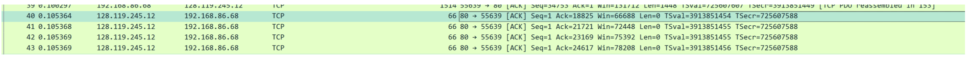
No retransmitted segments were found. Verified by checking for duplicate TCP sequence numbers and retransmission flags.

10. ACK Analysis

Question:

How much data does the receiver typically acknowledge in an ACK among the first ten data-carrying segments? Are there cases where the receiver ACKs every other segment?

Answer:



```
39 0.100297  192.168.86.68   128.119.245.12  TCP  1514 55639 → 80 [ACK] Seq=34753 Ack=1 Win=131712 Len=1448 TSval=725607607 TSecr=3913851449 [TCP PDU reassembled in 153]
40 0.105364  128.119.245.12  192.168.86.68   TCP    66 80 → 55639 [ACK] Seq=1 Ack=18825 Win=66688 Len=0 TSval=3913851454 TSecr=725607588
41 0.105368  128.119.245.12  192.168.86.68   TCP    66 80 → 55639 [ACK] Seq=1 Ack=21721 Win=72448 Len=0 TSval=3913851455 TSecr=725607588
42 0.105369  128.119.245.12  192.168.86.68   TCP    66 80 → 55639 [ACK] Seq=1 Ack=23169 Win=75392 Len=0 TSval=3913851455 TSecr=725607588
43 0.105369  128.119.245.12  192.168.86.68   TCP    66 80 → 55639 [ACK] Seq=1 Ack=24617 Win=78208 Len=0 TSval=3913851456 TSecr=725607588
```

Each segment: `1448 bytes`.

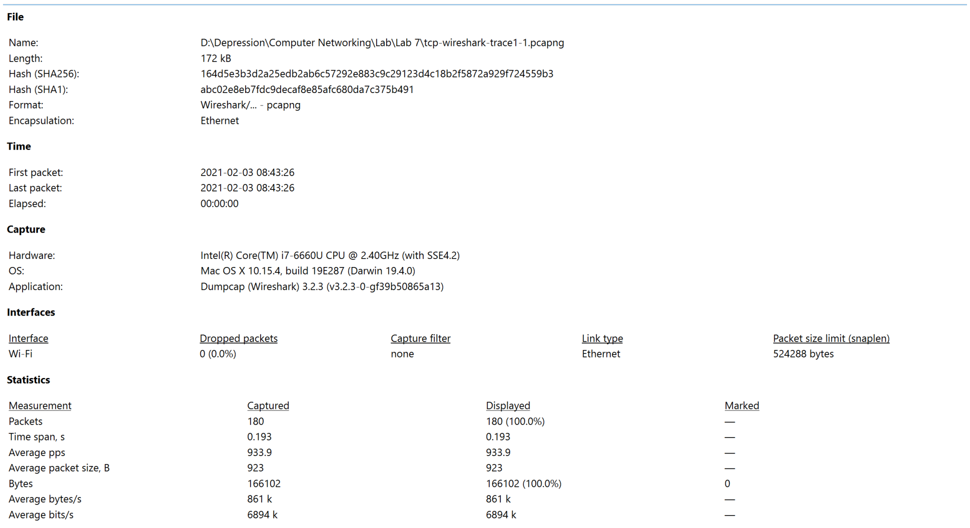
Receiver typically acknowledges one segment (1448 bytes) per ACK.

Yes, in some cases, every other segment is acknowledged (e.g., ACK 25 covers segments 24 and 25).

11. Throughput

Question:

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



File

Name:	D:\Depression\Computer Networking\Lab\Lab 7\tcp-wireshark-trace1-1.pcapng
Length:	172 kB
Hash (SHA256):	164d5e3b3d2a25edb2ab6c57292e883c9c29123d4c18b2f5872a929f724559b3
Hash (SHA1):	abc02e8eb7fdc9decaf8e85afc680da7c375b491
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2021-02-03 08:43:26
Last packet:	2021-02-03 08:43:26
Elapsed:	00:00:00

Capture

Hardware:	Intel(R) Core(TM) i7-6660U CPU @ 2.40GHz (with SSE4.2)
OS:	Mac OS X 10.15.4, build 19E287 (Darwin 19.4.0)
Application:	Dumpcap (Wireshark) 3.2.3 (v3.2.3-0-gf39b50865a13)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Wi-Fi	0 (0.0%)	none	Ethernet	524288 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	180	180 (100.0%)	—
Time span, s	0.193	0.193	—
Average pps	933.9	933.9	—
Average packet size, B	923	923	—
Bytes	166102	166102 (100.0%)	0
Average bytes/s	861 k	861 k	—
Average bits/s	6894 k	6894 k	—

$$\text{Throughput} = \frac{\text{Total Data Transferred}}{\text{Total Time}} = \frac{166102\ \text{Bytes}}{0.193\ \text{s}} = 860632.12\ \text{Bytes/s}$$

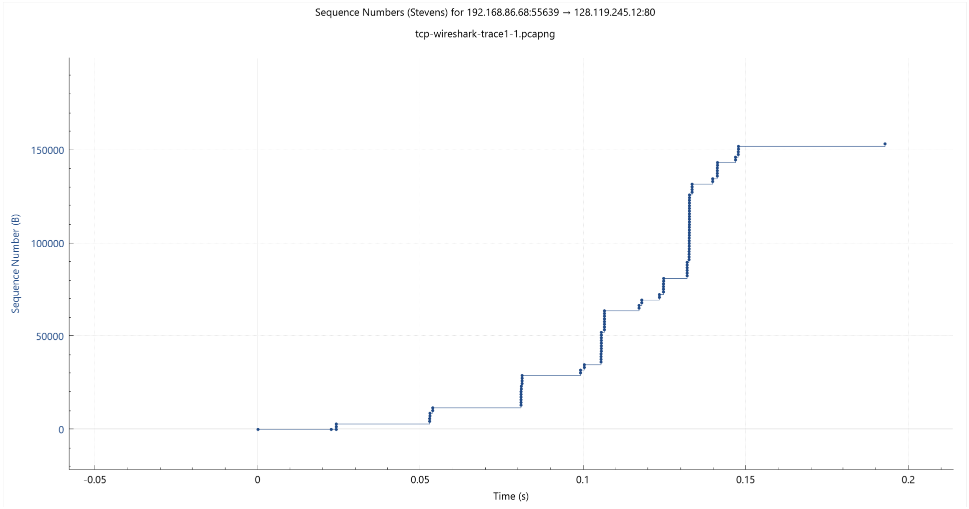
Answer: Throughput `860.63 KB/s`

12. Time-Sequence Graph (Stevens)

Question:

Analyze the Time-Sequence graph (Stevens) of the segments sent from the client to the server. Does it indicate slow start, congestion avoidance, or another phase?

Answer:



The stair-step pattern with exponentially increasing bursts indicates TCP is in the **Slow Start Phase**.

13. Periodicity of Fleets

Question:
These “fleets” of segments appear periodic. What can you say about their period?

Answer:
The period of these ”fleets” or bursts of segments is determined by the Round-Trip Time (RTT) of the connection.ACKs don’t add much because the receiver acks every other segment almost immediately once two segments arrive.
Based on a visual inspection of the graphs (the consistent stepping in the slow start phase), the RTT for this connection is estimated to be around 25 milliseconds (0.050s - 0.025s) = 0.025s.

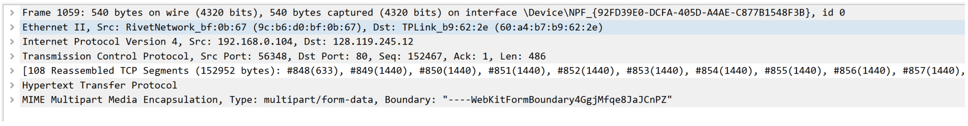
14. File Transfer from User’s Own Capture

Question:
Answer the above questions for the trace you gathered transferring a file from your computer to `gaia.cs.umass.edu`.

URL: `https://www-net.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html`

Question: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`? To answer this question, it’s probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the “details of the selected packet header window”.

Answer:

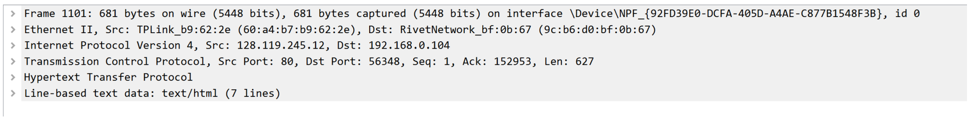


```
> Frame 1059: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{92FD39E0-DCFA-405D-A4AE-C877B1548F3B}, id 0
> Ethernet II, Src: RivetNetwork_bf:0b:67 (9c:b6:d0:bf:0b:67), Dst: TPLink_b9:62:2e (60:a4:b7:b9:62:2e)
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 56348, Dst Port: 80, Seq: 152467, Ack: 1, Len: 486
> [108 Reassembled TCP Segments (152952 bytes): #848(633), #849(1440), #850(1440), #851(1440), #852(1440), #853(1440), #854(1440), #855(1440), #856(1440), #857(1440),
> Hypertext Transfer Protocol
> MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "----WebKitFormBoundary4GgjMfqe8JaJCnPZ"
```

- Client IP: `192.168.0.104`, Source Port: `56348`

Question: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?

Answer:



```
> Frame 1101: 681 bytes on wire (5448 bits), 681 bytes captured (5448 bits) on interface \Device\NPF_{92FD39E0-DCFA-405D-A4AE-C877B1548F3B}, id 0
> Ethernet II, Src: TPLink_b9:62:2e (60:a4:b7:b9:62:2e), Dst: RivetNetwork_bf:0b:67 (9c:b6:d0:bf:0b:67)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.104
> Transmission Control Protocol, Src Port: 80, Dst Port: 56348, Seq: 1, Ack: 152953, Len: 627
> Hypertext Transfer Protocol
> Line-based text data: text/html (7 lines)
```

- Server IP: `128.119.245.12`, Sending: `56348`, Receiving: `80`