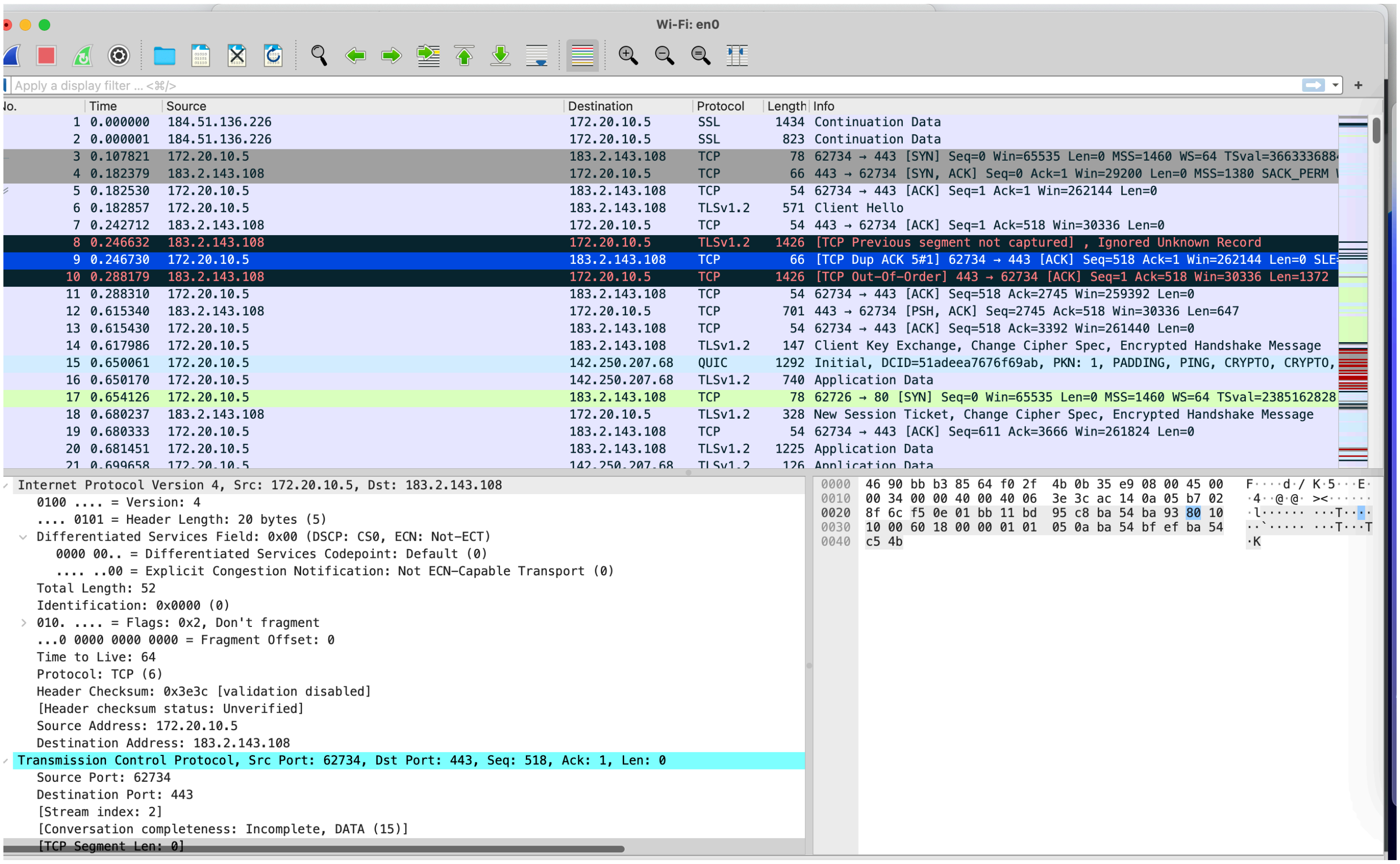
## Any duplicate ack, what's the possible reason?

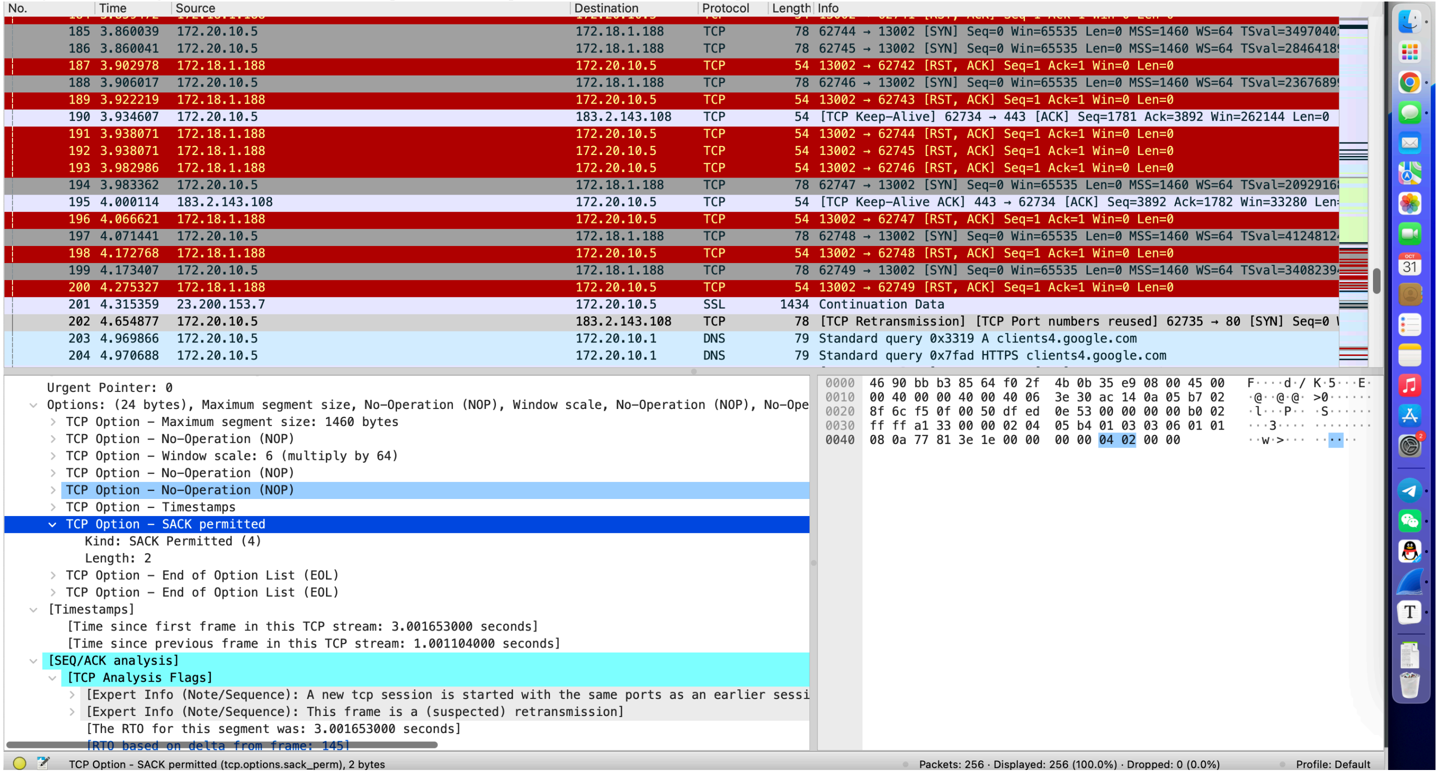


```
No.     Time      Source            Destination     Protocol  Length Info
      1 0.000000  184.51.136.226    172.20.10.5     SSL       1434 Continuation Data
      2 0.000001  184.51.136.226    172.20.10.5     SSL        823 Continuation Data
      3 0.107821  172.20.10.5       183.2.143.108   TCP         78 62734 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=36633368
      4 0.182379  183.2.143.108     172.20.10.5     TCP         66 443 → 62734 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380 SACK_PERM
      5 0.182530  172.20.10.5       183.2.143.108   TCP         54 62734 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
      6 0.182857  172.20.10.5       183.2.143.108   TLSv1.2    571 Client Hello
      7 0.242712  183.2.143.108     172.20.10.5     TCP         54 443 → 62734 [ACK] Seq=1 Ack=518 Win=30336 Len=0
      8 0.246632  183.2.143.108     172.20.10.5     TLSv1.2   1426 [TCP Previous segment not captured] , Ignored Unknown Record
      9 0.246730  172.20.10.5       183.2.143.108   TCP         66 [TCP Dup ACK 5#1] 62734 → 443 [ACK] Seq=518 Ack=1 Win=262144 Len=0 SLE
     10 0.288179  183.2.143.108     172.20.10.5     TCP       1426 [TCP Out-Of-Order] 443 → 62734 [ACK] Seq=1 Ack=518 Win=30336 Len=1372
     11 0.288310  172.20.10.5       183.2.143.108   TCP         54 62734 → 443 [ACK] Seq=518 Ack=2745 Win=259392 Len=0
     12 0.615340  183.2.143.108     172.20.10.5     TCP        701 443 → 62734 [PSH, ACK] Seq=2745 Ack=518 Win=30336 Len=647
     13 0.615430  172.20.10.5       183.2.143.108   TCP         54 62734 → 443 [ACK] Seq=518 Ack=3392 Win=261440 Len=0
     14 0.617986  172.20.10.5       183.2.143.108   TLSv1.2    147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
     15 0.650061  172.20.10.5       142.250.207.68  QUIC      1292 Initial, DCID=51adeea7676f69ab, PKN: 1, PADDING, PING, CRYPTO, CRYPTO,
     16 0.650170  172.20.10.5       142.250.207.68  TLSv1.2    740 Application Data
     17 0.654126  172.20.10.5       183.2.143.108   TCP         78 62726 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2385162828
     18 0.680237  183.2.143.108     172.20.10.5     TLSv1.2    328 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
     19 0.680333  172.20.10.5       183.2.143.108   TCP         54 62734 → 443 [ACK] Seq=611 Ack=3666 Win=261824 Len=0
     20 0.681451  172.20.10.5       183.2.143.108   TLSv1.2   1225 Application Data
     21 0.699658  172.20.10.5       142.250.207.68  TLSv1.2    126 Application Data
```

```
Internet Protocol Version 4, Src: 172.20.10.5, Dst: 183.2.143.108
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 52
  Identification: 0x0000 (0)
  010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: TCP (6)
  Header Checksum: 0x3e3c [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 172.20.10.5
  Destination Address: 183.2.143.108
Transmission Control Protocol, Src Port: 62734, Dst Port: 443, Seq: 518, Ack: 1, Len: 0
  Source Port: 62734
  Destination Port: 443
  [Stream index: 2]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 0]
```

```
0000  46 90 bb b3 85 64 f0 2f  4b 0b 35 e9 08 00 45 00   F····d·/ K·5···E·
0010  00 34 00 00 40 00 40 06  3e 3c ac 14 0a 05 b7 02   ·4··@·@· ><······
0020  8f 6c f5 0e 01 bb 11 bd  95 c8 ba 54 ba 93 80 10   ·l······ ···T····
0030  10 00 60 18 00 00 01 01  05 0a ba 54 bf ef ba 54   ··`····· ···T···T
0040  c5 4b                                              ·K
```

# Any TCP segment with sack permit option and sack option



```
No.     Time      Source          Destination     Protocol Length Info
  185 3.860039  172.20.10.5     172.18.1.188    TCP        78  62744 → 13002 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3497040
  186 3.860041  172.20.10.5     172.18.1.188    TCP        78  62745 → 13002 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2846418
  187 3.902978  172.18.1.188    172.20.10.5     TCP        54  13002 → 62742 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  188 3.906017  172.20.10.5     172.18.1.188    TCP        78  62746 → 13002 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2367689
  189 3.922219  172.18.1.188    172.20.10.5     TCP        54  13002 → 62743 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  190 3.934607  172.20.10.5     183.2.143.108   TCP        54  [TCP Keep-Alive] 62734 → 443 [ACK] Seq=1781 Ack=3892 Win=262144 Len=0
  191 3.938071  172.18.1.188    172.20.10.5     TCP        54  13002 → 62744 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  192 3.938071  172.18.1.188    172.20.10.5     TCP        54  13002 → 62745 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  193 3.982986  172.18.1.188    172.20.10.5     TCP        54  13002 → 62746 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  194 3.983362  172.20.10.5     172.18.1.188    TCP        78  62747 → 13002 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2092916
  195 4.000114  183.2.143.108   172.20.10.5     TCP        54  [TCP Keep-Alive ACK] 443 → 62734 [ACK] Seq=3892 Ack=1782 Win=33280 Len
  196 4.066621  172.18.1.188    172.20.10.5     TCP        54  13002 → 62747 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  197 4.071441  172.20.10.5     172.18.1.188    TCP        78  62748 → 13002 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=4124812
  198 4.172768  172.18.1.188    172.20.10.5     TCP        54  13002 → 62748 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  199 4.173407  172.20.10.5     172.18.1.188    TCP        78  62749 → 13002 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3408239
  200 4.275327  172.18.1.188    172.20.10.5     TCP        54  13002 → 62749 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  201 4.315359  23.200.153.7    172.20.10.5     SSL      1434  Continuation Data
  202 4.654877  172.20.10.5     183.2.143.108   TCP        78  [TCP Retransmission] [TCP Port numbers reused] 62735 → 80 [SYN] Seq=0
  203 4.969866  172.20.10.5     172.20.10.1     DNS        79  Standard query 0x3319 A clients4.google.com
  204 4.970688  172.20.10.5     172.20.10.1     DNS        79  Standard query 0x7fad HTTPS clients4.google.com
```

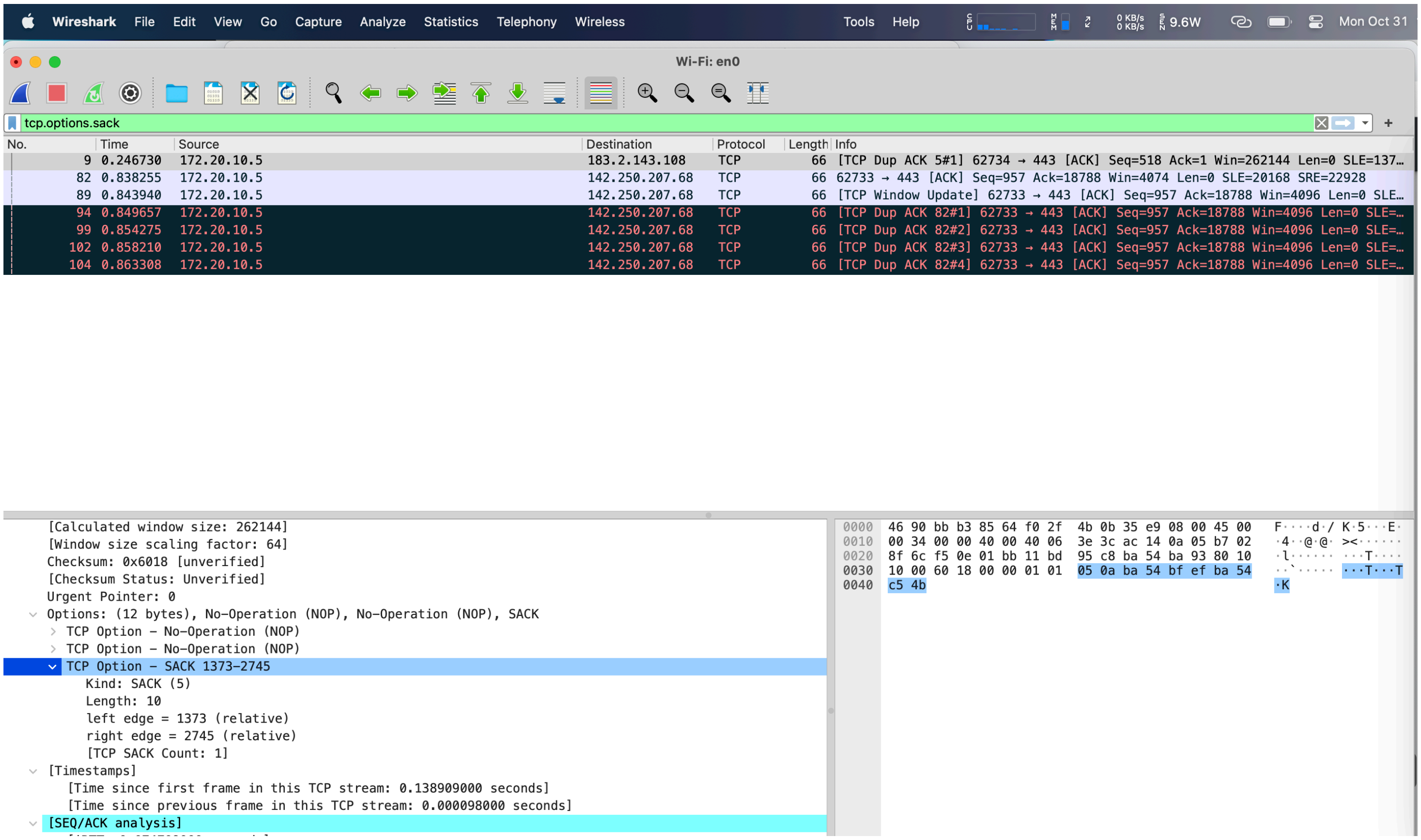
```
    Urgent Pointer: 0
  ⌄ Options: (24 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Ope
    › TCP Option - Maximum segment size: 1460 bytes
    › TCP Option - No-Operation (NOP)
    › TCP Option - Window scale: 6 (multiply by 64)
    › TCP Option - No-Operation (NOP)
    › TCP Option - No-Operation (NOP)
    › TCP Option - Timestamps
    ⌄ TCP Option - SACK permitted
        Kind: SACK Permitted (4)
        Length: 2
    › TCP Option - End of Option List (EOL)
    › TCP Option - End of Option List (EOL)
  ⌄ [Timestamps]
      [Time since first frame in this TCP stream: 3.001653000 seconds]
      [Time since previous frame in this TCP stream: 1.001104000 seconds]
  ⌄ [SEQ/ACK analysis]
    ⌄ [TCP Analysis Flags]
      › [Expert Info (Note/Sequence): A new tcp session is started with the same ports as an earlier sessi
      › [Expert Info (Note/Sequence): This frame is a (suspected) retransmission]
        [The RTO for this segment was: 3.001653000 seconds]
        [RTO based on delta from frame: 145]
```

```
0000  46 90 bb b3 85 64 f0 2f  4b 0b 35 e9 08 00 45 00   F····d·/ K·5···E·
0010  00 40 00 00 40 00 40 06  3e 30 ac 14 0a 05 b7 02   ·@··@·@· >0······
0020  8f 6c f5 0f 00 50 df ed  0e 53 00 00 00 00 b0 02   ·l···P·· ·S······
0030  ff ff a1 33 00 00 02 04  05 b4 01 03 03 06 01 01   ···3···· ········
0040  08 0a 77 81 3e 1e 00 00  00 00 04 02 00 00         ··w·>··· ······
```

TCP Option - SACK permitted (tcp.options.sack_perm), 2 bytes

Packets: 256 · Displayed: 256 (100.0%) · Dropped: 0 (0.0%)

Profile: Default



tcp.options.sack

```
No.     Time      Source          Destination      Protocol Length Info
    9 0.246730  172.20.10.5     183.2.143.108    TCP        66  [TCP Dup ACK 5#1] 62734 → 443 [ACK] Seq=518 Ack=1 Win=262144 Len=0 SLE=137…
   82 0.838255  172.20.10.5     142.250.207.68   TCP        66  62733 → 443 [ACK] Seq=957 Ack=18788 Win=4074 Len=0 SLE=20168 SRE=22928
   89 0.843940  172.20.10.5     142.250.207.68   TCP        66  [TCP Window Update] 62733 → 443 [ACK] Seq=957 Ack=18788 Win=4096 Len=0 SLE…
   94 0.849657  172.20.10.5     142.250.207.68   TCP        66  [TCP Dup ACK 82#1] 62733 → 443 [ACK] Seq=957 Ack=18788 Win=4096 Len=0 SLE=…
   99 0.854275  172.20.10.5     142.250.207.68   TCP        66  [TCP Dup ACK 82#2] 62733 → 443 [ACK] Seq=957 Ack=18788 Win=4096 Len=0 SLE=…
  102 0.858210  172.20.10.5     142.250.207.68   TCP        66  [TCP Dup ACK 82#3] 62733 → 443 [ACK] Seq=957 Ack=18788 Win=4096 Len=0 SLE=…
  104 0.863308  172.20.10.5     142.250.207.68   TCP        66  [TCP Dup ACK 82#4] 62733 → 443 [ACK] Seq=957 Ack=18788 Win=4096 Len=0 SLE=…
```

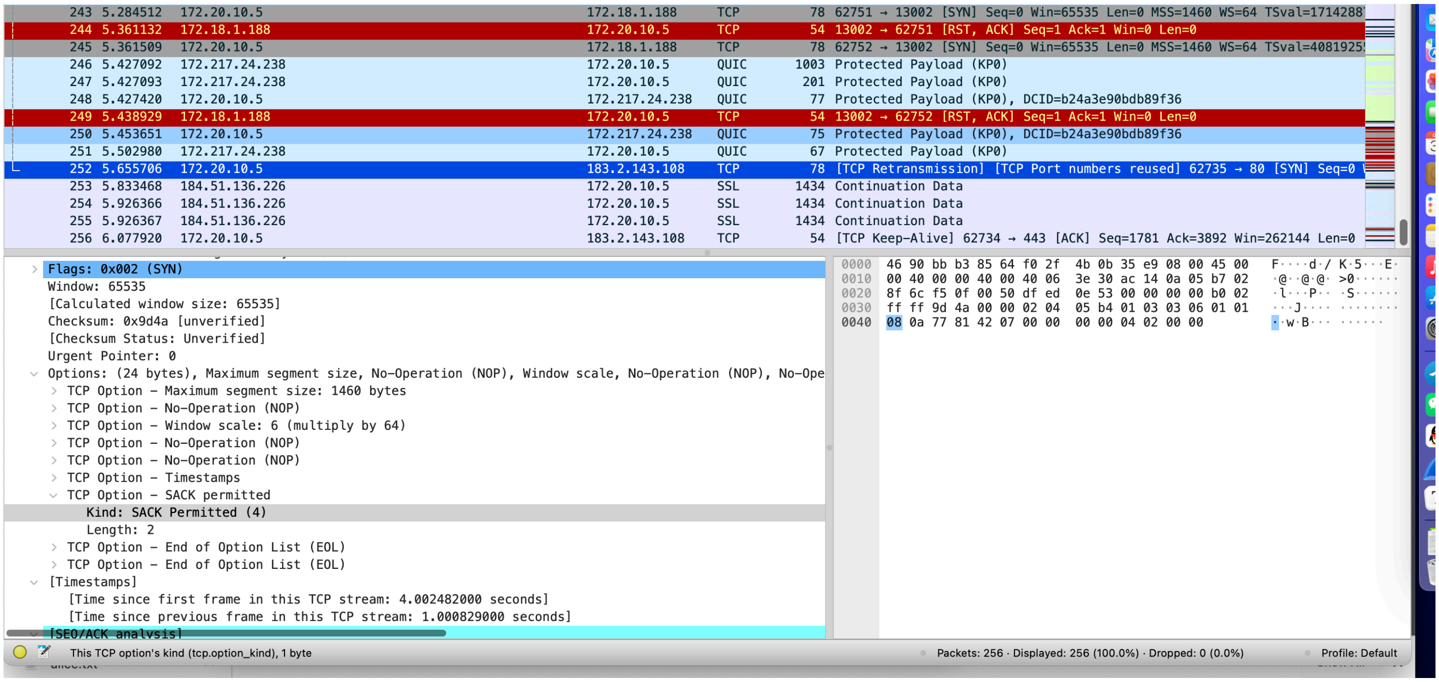
```
    [Calculated window size: 262144]
    [Window size scaling factor: 64]
    Checksum: 0x6018 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ⌄ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), SACK
    › TCP Option - No-Operation (NOP)
    › TCP Option - No-Operation (NOP)
    ⌄ TCP Option - SACK 1373-2745
        Kind: SACK (5)
        Length: 10
        left edge = 1373 (relative)
        right edge = 2745 (relative)
        [TCP SACK Count: 1]
  ⌄ [Timestamps]
      [Time since first frame in this TCP stream: 0.138909000 seconds]
      [Time since previous frame in this TCP stream: 0.000098000 seconds]
  ⌄ [SEQ/ACK analysis]
```

```
0000  46 90 bb b3 85 64 f0 2f  4b 0b 35 e9 08 00 45 00   F····d·/ K·5···E·
0010  00 34 00 00 40 00 40 06  3e 3c ac 14 0a 05 b7 02   ·4··@·@· ><······
0020  8f 6c f5 0e 01 bb 11 bd  95 c8 ba 54 ba 93 80 10   ·l······ ···T····
0030  10 00 60 18 00 00 01 01  05 0a ba 54 bf ef ba 54   ··`····· ···T···T
0040  c5 4b                                              ·K
```

find the segment ranges which is acked in this sack option?

## Any TCP retransmission? Is it retransmission or fast retransmission?

it's retransmission



```
243 5.284512  172.20.10.5      172.18.1.188    TCP    78 62751 → 13002 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1714288
244 5.361132  172.18.1.188     172.20.10.5     TCP    54 13002 → 62751 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
245 5.361509  172.20.10.5      172.18.1.188    TCP    78 62752 → 13002 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=4081925
246 5.427092  172.217.24.238   172.20.10.5     QUIC 1003 Protected Payload (KP0)
247 5.427093  172.217.24.238   172.20.10.5     QUIC  201 Protected Payload (KP0)
248 5.427420  172.20.10.5      172.217.24.238  QUIC   77 Protected Payload (KP0), DCID=b24a3e90bdb89f36
249 5.438929  172.18.1.188     172.20.10.5     TCP    54 13002 → 62752 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
250 5.453651  172.20.10.5      172.217.24.238  QUIC   75 Protected Payload (KP0), DCID=b24a3e90bdb89f36
251 5.502980  172.217.24.238   172.20.10.5     QUIC   67 Protected Payload (KP0)
252 5.655706  172.20.10.5      183.2.143.108   TCP    78 [TCP Retransmission] [TCP Port numbers reused] 62735 → 80 [SYN] Seq=0
253 5.833468  184.51.136.226   172.20.10.5     SSL  1434 Continuation Data
254 5.926366  184.51.136.226   172.20.10.5     SSL  1434 Continuation Data
255 5.926367  184.51.136.226   172.20.10.5     SSL  1434 Continuation Data
256 6.077920  172.20.10.5      183.2.143.108   TCP    54 [TCP Keep-Alive] 62734 → 443 [ACK] Seq=1781 Ack=3892 Win=262144 Len=0
```

```
  > Flags: 0x002 (SYN)
    Window: 65535
    [Calculated window size: 65535]
    Checksum: 0x9d4a [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ∨ Options: (24 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Ope
    > TCP Option - Maximum segment size: 1460 bytes
    > TCP Option - No-Operation (NOP)
    > TCP Option - Window scale: 6 (multiply by 64)
    > TCP Option - No-Operation (NOP)
    > TCP Option - No-Operation (NOP)
    > TCP Option - Timestamps
    ∨ TCP Option - SACK permitted
        Kind: SACK Permitted (4)
        Length: 2
    > TCP Option - End of Option List (EOL)
    > TCP Option - End of Option List (EOL)
  ∨ [Timestamps]
      [Time since first frame in this TCP stream: 4.002482000 seconds]
      [Time since previous frame in this TCP stream: 1.000829000 seconds]
  ∨ [SEQ/ACK analysis]
```

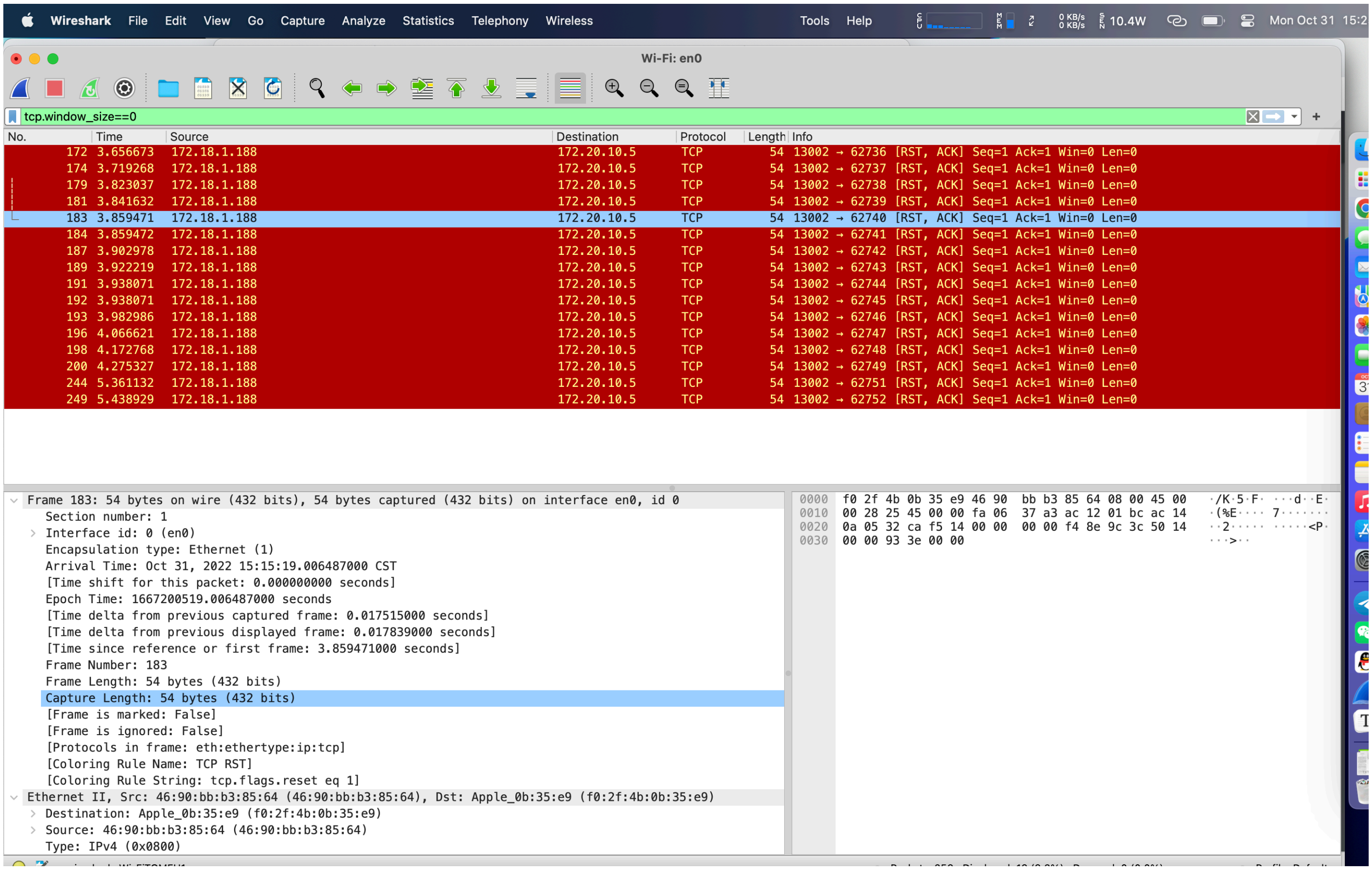
```
0000  46 90 bb b3 85 64 f0 2f  4b 0b 35 e9 08 00 45 00   F····d·/ K·5···E·
0010  00 40 00 00 40 00 40 06  3e 30 ac 14 0a 05 b7 02   ·@··@·@· >0······
0020  8f 6c f5 0f 00 50 df ed  0e 53 00 00 00 00 b0 02   ·l···P·· ·S······
0030  ff ff 9d 4a 00 00 02 04  05 b4 01 03 03 06 01 01   ···J···· ········
0040  08 0a 77 81 42 07 00 00  00 00 04 02 00 00         ··w·B··· ······
```

This TCP option's kind (tcp.option_kind), 1 byte

Packets: 256 · Displayed: 256 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

## Any window size 0 segment, what does it mean? If the window size is 0, what would happened next on this tcp connection?



tcp.window_size==0

```
No.  Time      Source        Destination  Protocol Length Info
172 3.656673  172.18.1.188  172.20.10.5  TCP  54 13002 → 62736 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
174 3.719268  172.18.1.188  172.20.10.5  TCP  54 13002 → 62737 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
179 3.823037  172.18.1.188  172.20.10.5  TCP  54 13002 → 62738 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
181 3.841632  172.18.1.188  172.20.10.5  TCP  54 13002 → 62739 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
183 3.859471  172.18.1.188  172.20.10.5  TCP  54 13002 → 62740 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
184 3.859472  172.18.1.188  172.20.10.5  TCP  54 13002 → 62741 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
187 3.902978  172.18.1.188  172.20.10.5  TCP  54 13002 → 62742 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
189 3.922219  172.18.1.188  172.20.10.5  TCP  54 13002 → 62743 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
191 3.938071  172.18.1.188  172.20.10.5  TCP  54 13002 → 62744 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192 3.938071  172.18.1.188  172.20.10.5  TCP  54 13002 → 62745 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
193 3.982986  172.18.1.188  172.20.10.5  TCP  54 13002 → 62746 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
196 4.066621  172.18.1.188  172.20.10.5  TCP  54 13002 → 62747 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
198 4.172768  172.18.1.188  172.20.10.5  TCP  54 13002 → 62748 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
200 4.275327  172.18.1.188  172.20.10.5  TCP  54 13002 → 62749 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
244 5.361132  172.18.1.188  172.20.10.5  TCP  54 13002 → 62751 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
249 5.438929  172.18.1.188  172.20.10.5  TCP  54 13002 → 62752 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

```
∨ Frame 183: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface en0, id 0
    Section number: 1
  > Interface id: 0 (en0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 31, 2022 15:15:19.006487000 CST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1667200519.006487000 seconds
    [Time delta from previous captured frame: 0.017515000 seconds]
    [Time delta from previous displayed frame: 0.017839000 seconds]
    [Time since reference or first frame: 3.859471000 seconds]
    Frame Number: 183
    Frame Length: 54 bytes (432 bits)
    Capture Length: 54 bytes (432 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: TCP RST]
    [Coloring Rule String: tcp.flags.reset eq 1]
∨ Ethernet II, Src: 46:90:bb:b3:85:64 (46:90:bb:b3:85:64), Dst: Apple_0b:35:e9 (f0:2f:4b:0b:35:e9)
  > Destination: Apple_0b:35:e9 (f0:2f:4b:0b:35:e9)
  > Source: 46:90:bb:b3:85:64 (46:90:bb:b3:85:64)
    Type: IPv4 (0x0800)
```

```
0000  f0 2f 4b 0b 35 e9 46 90  bb b3 85 64 08 00 45 00   ·/K·5·F· ···d··E·
0010  00 28 25 45 00 00 fa 06  37 a3 ac 12 01 bc ac 14   ·(%E···· 7·······
0020  0a 05 32 ca f5 14 00 00  00 00 f4 8e 9c 3c 50 14   ··2····· ·····<P·
0030  00 00 93 3e 00 00                                  ···>··
```

what does it mean?

接受者的windows为0

发送者会检查与接受者的连接是否还存在，并告诉接受者继续连接

**Any TCP window full segment, what does it mean?**

没有full segment，代表发送者发送的数据达到了接受者窗口的上限