BU-9 Wireshark Charts & IO Graphs

18 June 2009

Ray Tompkins

Founder & CEO | gearbit

Get it in Gear

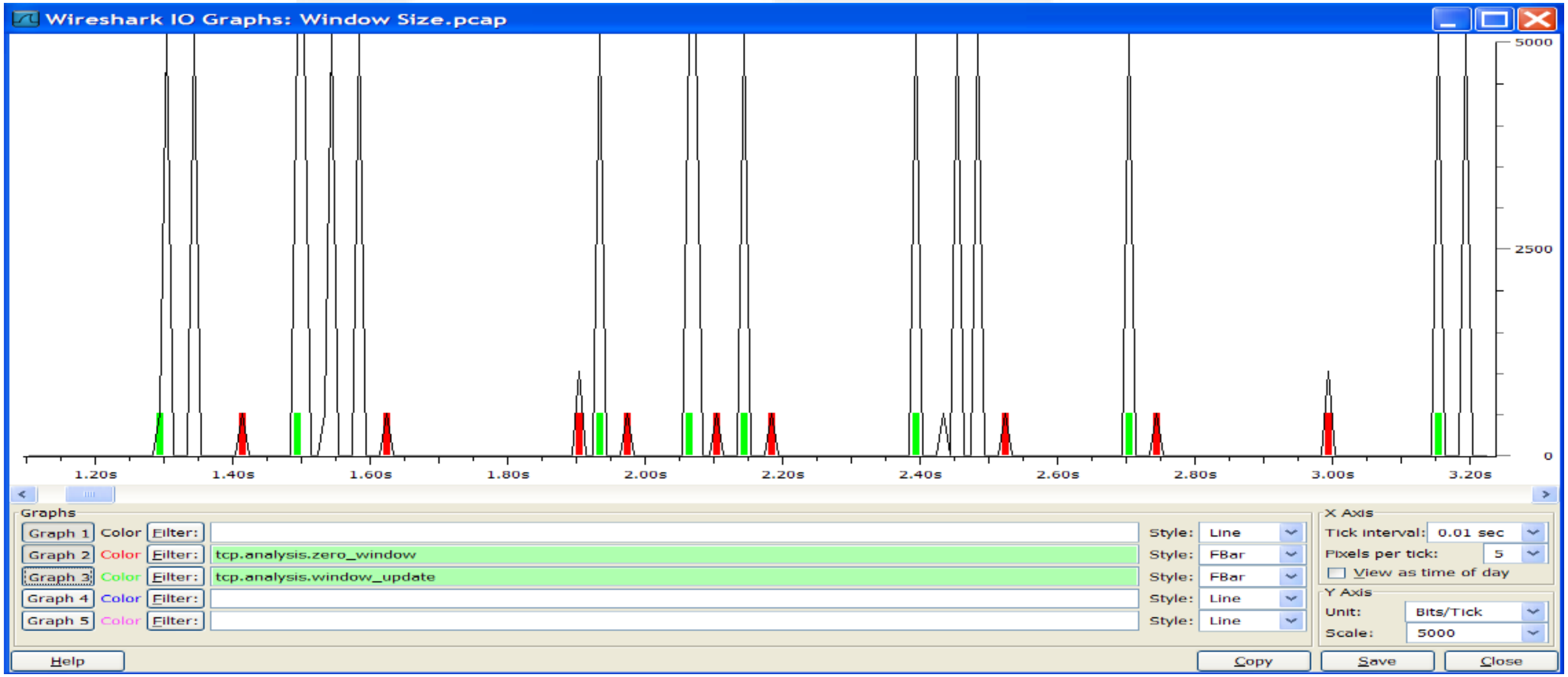
SHARKFEST **'09**

Stanford University

June 15-18, 2009

Wireshark Charts & IO Graphs

- How to find and then graph performance problems
- How you can see solid proof what's the problem
- Displaying graphs so others can visibly see the problem



Wireshark IO Graphs: Window Size.pcap

Graphs

Graph 1	Color	Filter:		Style: Line
Graph 2	Color	Filter:	tcp.analysis.zero_window	Style: FBar
Graph 3	Color	Filter:	tcp.analysis.window_update	Style: FBar
Graph 4	Color	Filter:		Style: Line
Graph 5	Color	Filter:		Style: Line

X Axis

Tick interval: 0.01 sec

Pixels per tick: 5

□ View as time of day

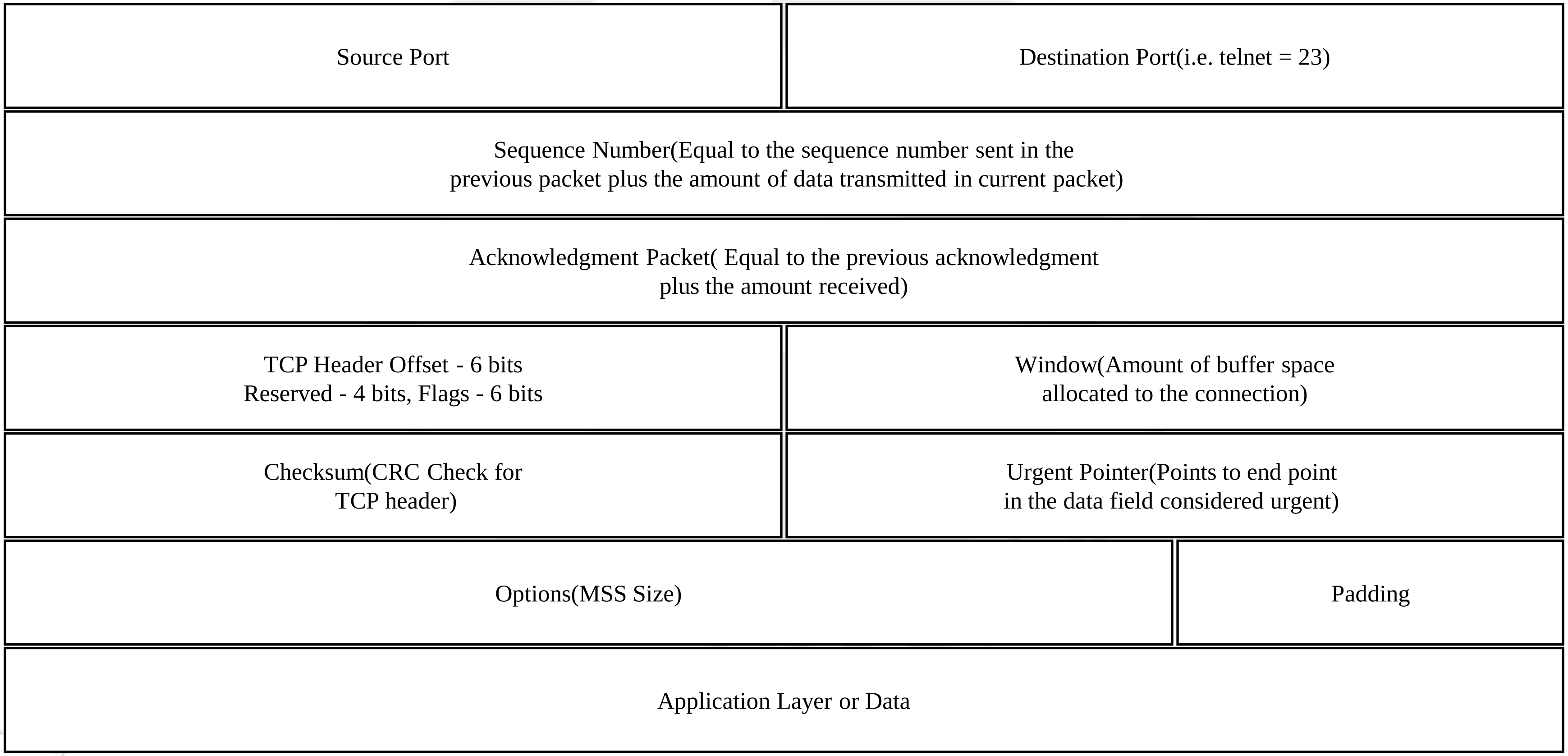
Y Axis

Unit: Bits/Tick

Scale: 5000

TCP Overview

TCP Header



Source Port | Destination Port(i.e. telnet = 23)

Sequence Number(Equal to the sequence number sent in the previous packet plus the amount of data transmitted in current packet)

Acknowledgment Packet(Equal to the previous acknowledgment plus the amount received)

TCP Header Offset - 6 bits
Reserved - 4 bits, Flags - 6 bits | Window(Amount of buffer space allocated to the connection)

Checksum(CRC Check for TCP header) | Urgent Pointer(Points to end point in the data field considered urgent)

Options(MSS Size) | Padding

Application Layer or Data

TCP Overview

Connection Oriented: Before data can be transferred, a TCP connection must be established.

Full Duplex: Every TCP conversation has two logical pipes; an outgoing and incoming pipe.

Reliable: All data is sequenced and lost packets are detected and retransmitted.

Byte Stream: TCP views data transmitted over a pipe as a continuous stream of Bytes.

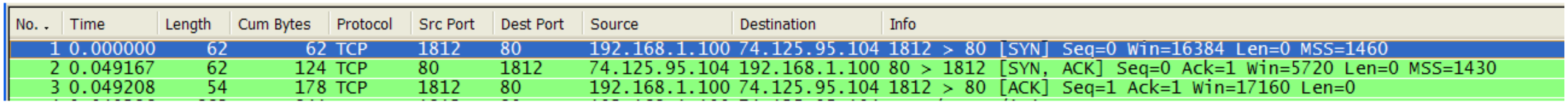
Sender and Receiver Flow Control: A TCP Window is used to avoid sending too much data. This will be discussed in more detail in a later slide.

Segmentation: TCP will segment any application data so that it will fit within the IP MTU.

TCP Overview

- TCP 2 WAY HANDSHAKE

- The delta value between frames 1 and 2 can be used as a TCP transport connect baseline value.

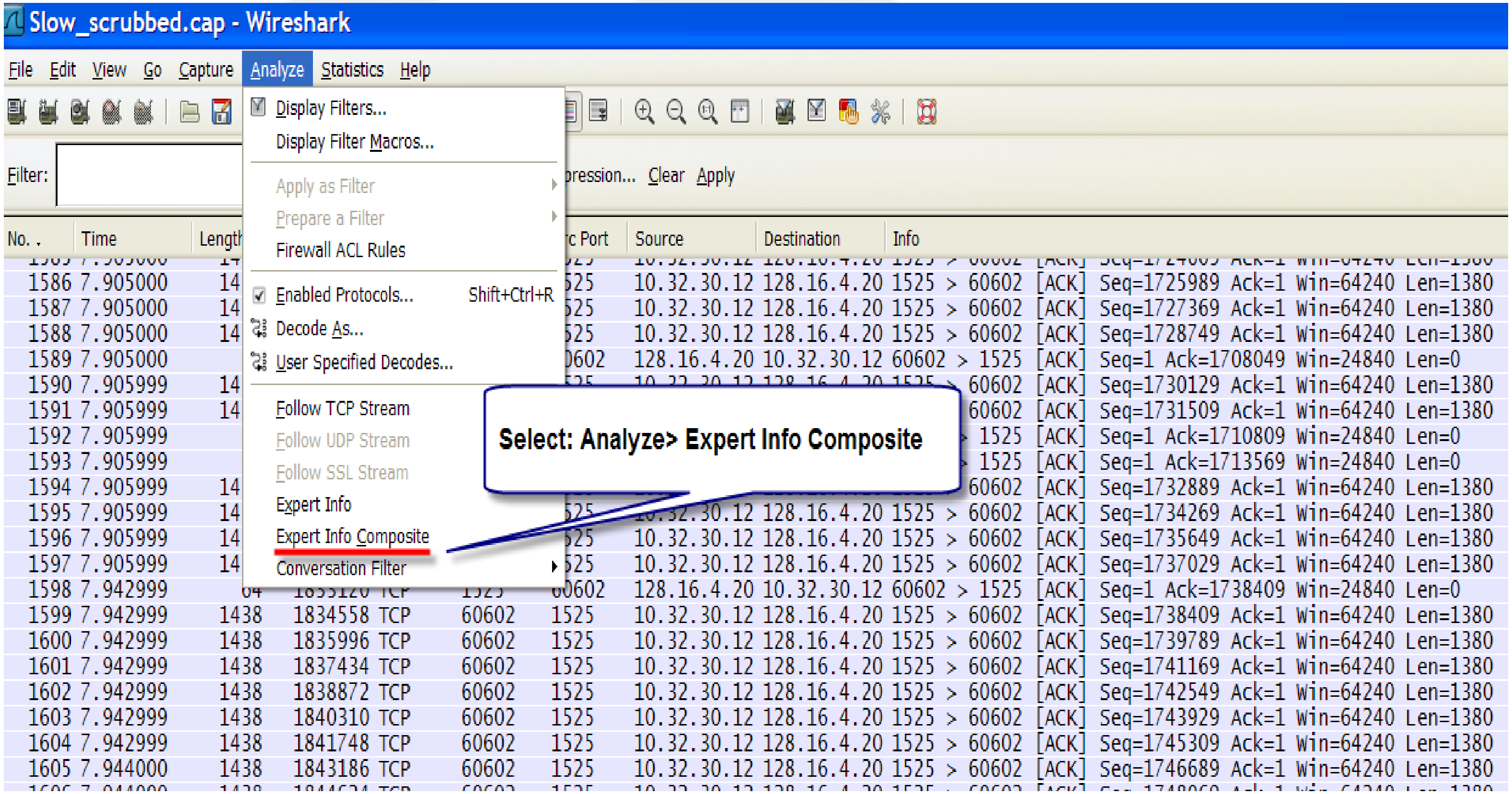


No.	Time	Length	Cum Bytes	Protocol	Src Port	Dest Port	Source	Destination	Info
1	0.000000	62	62	TCP	1812	80	192.168.1.100	74.125.95.104	1812 > 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460
2	0.049167	62	124	TCP	80	1812	74.125.95.104	192.168.1.100	80 > 1812 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
3	0.049208	54	178	TCP	1812	80	192.168.1.100	74.125.95.104	1812 > 80 [ACK] Seq=1 Ack=1 Win=17160 Len=0

- Other important information gathered from this handshake:
  - Window Size
  - SACK
  - Maximum Segment Size
  - Window Scale Option value

Indentifying Zero Window Size

- **Select: Analysis>Expert Info Composite**

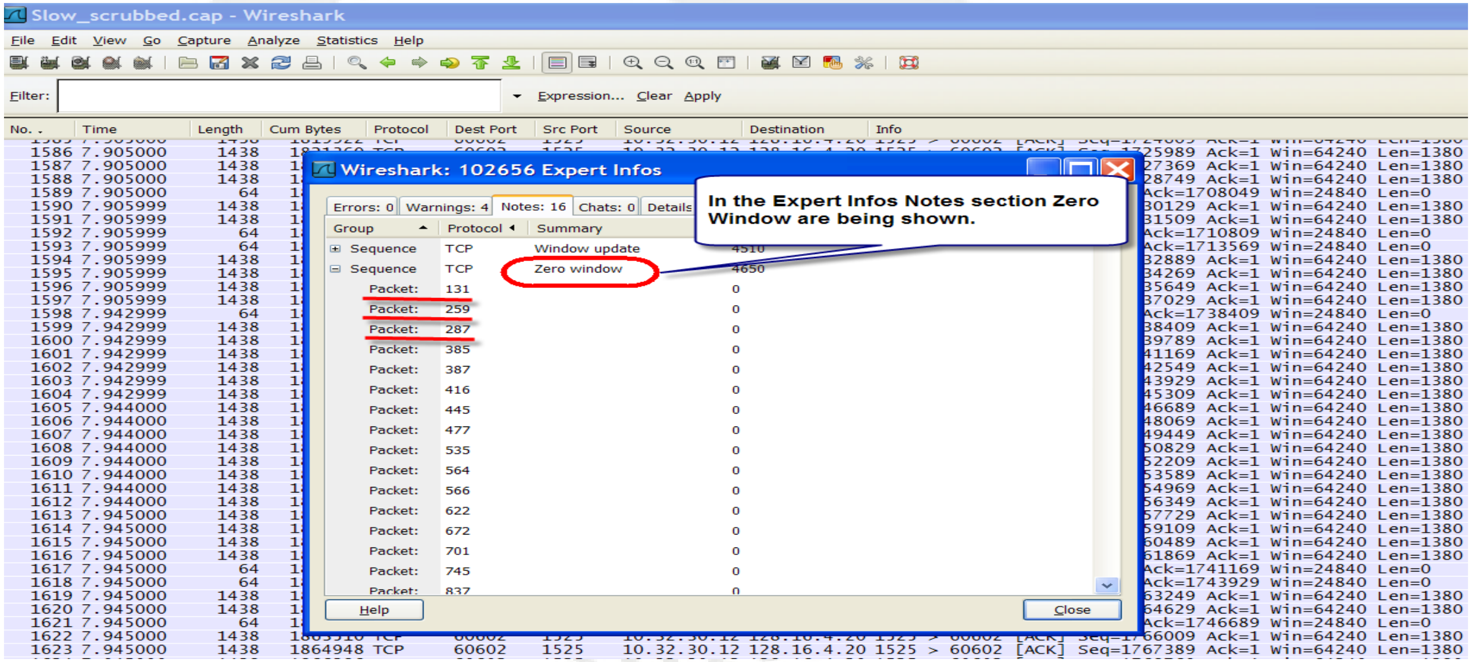


```
No. .  Time     Length                              c Port  Source       Destination  Info
1586 7.905000   14                                  525     10.32.30.12  128.16.4.20  1525 > 60602 [ACK] Seq=1725989 Ack=1 Win=64240 Len=1380
1587 7.905000   14                                  525     10.32.30.12  128.16.4.20  1525 > 60602 [ACK] Seq=1727369 Ack=1 Win=64240 Len=1380
1588 7.905000   14                                  525     10.32.30.12  128.16.4.20  1525 > 60602 [ACK] Seq=1728749 Ack=1 Win=64240 Len=1380
1589 7.905000                                       0602    128.16.4.20  10.32.30.12  60602 > 1525 [ACK] Seq=1 Ack=1708049 Win=24840 Len=0
1590 7.905999   14                                                                          60602 [ACK] Seq=1730129 Ack=1 Win=64240 Len=1380
1591 7.905999   14                                                                          60602 [ACK] Seq=1731509 Ack=1 Win=64240 Len=1380
1592 7.905999                                                                               1525 [ACK] Seq=1 Ack=1710809 Win=24840 Len=0
1593 7.905999                                                                               1525 [ACK] Seq=1 Ack=1713569 Win=24840 Len=0
1594 7.905999   14                                                                          60602 [ACK] Seq=1732889 Ack=1 Win=64240 Len=1380
1595 7.905999   14                                  525                  128.16.4.20  1525 > 60602 [ACK] Seq=1734269 Ack=1 Win=64240 Len=1380
1596 7.905999   14                                  525     10.32.30.12  128.16.4.20  1525 > 60602 [ACK] Seq=1735649 Ack=1 Win=64240 Len=1380
1597 7.905999   14                                  525     10.32.30.12  128.16.4.20  1525 > 60602 [ACK] Seq=1737029 Ack=1 Win=64240 Len=1380
1598 7.942999                                       60602   128.16.4.20  10.32.30.12  60602 > 1525 [ACK] Seq=1 Ack=1738409 Win=24840 Len=0
1599 7.942999   1438    1834558 TCP     60602       1525    10.32.30.12  128.16.4.20  1525 > 60602 [ACK] Seq=1738409 Ack=1 Win=64240 Len=1380
1600 7.942999   1438    1835996 TCP     60602       1525    10.32.30.12  128.16.4.20  1525 > 60602 [ACK] Seq=1739789 Ack=1 Win=64240 Len=1380
1601 7.942999   1438    1837434 TCP     60602       1525    10.32.30.12  128.16.4.20  1525 > 60602 [ACK] Seq=1741169 Ack=1 Win=64240 Len=1380
1602 7.942999   1438    1838872 TCP     60602       1525    10.32.30.12  128.16.4.20  1525 > 60602 [ACK] Seq=1742549 Ack=1 Win=64240 Len=1380
1603 7.942999   1438    1840310 TCP     60602       1525    10.32.30.12  128.16.4.20  1525 > 60602 [ACK] Seq=1743929 Ack=1 Win=64240 Len=1380
1604 7.942999   1438    1841748 TCP     60602       1525    10.32.30.12  128.16.4.20  1525 > 60602 [ACK] Seq=1745309 Ack=1 Win=64240 Len=1380
1605 7.944000   1438    1843186 TCP     60602       1525    10.32.30.12  128.16.4.20  1525 > 60602 [ACK] Seq=1746689 Ack=1 Win=64240 Len=1380
```

Select: Analyze> Expert Info Composite

Indentifying Zero Window Size

- Wireshark shows expert condition by protocol. TCP Zero Window



Slow_scrubbed.cap - Wireshark

File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. .  Time       Length  Cum Bytes  Protocol  Dest Port  Src Port  Source   Destination   Info
1586 7.905000     1438    1                                                   25989 Ack=1 Win=64240 Len=1380
1587 7.905000     1438    1                                                   27369 Ack=1 Win=64240 Len=1380
1588 7.905000     1438    1                                                   28749 Ack=1 Win=64240 Len=1380
1589 7.905000       64    1                                                   Ack=1708049 Win=24840 Len=0
1590 7.905999     1438    1                                                   30129 Ack=1 Win=64240 Len=1380
1591 7.905999     1438    1                                                   31509 Ack=1 Win=64240 Len=1380
1592 7.905999       64    1                                                   Ack=1710809 Win=24840 Len=0
1593 7.905999       64    1                                                   Ack=1713569 Win=24840 Len=0
1594 7.905999     1438    1                                                   32889 Ack=1 Win=64240 Len=1380
1595 7.905999     1438    1                                                   34269 Ack=1 Win=64240 Len=1380
1596 7.905999     1438    1                                                   35649 Ack=1 Win=64240 Len=1380
1597 7.905999     1438    1                                                   37029 Ack=1 Win=64240 Len=1380
1598 7.942999       64    1                                                   Ack=1738409 Win=24840 Len=0
1599 7.942999     1438    1                                                   38409 Ack=1 Win=64240 Len=1380
1600 7.942999     1438    1                                                   39789 Ack=1 Win=64240 Len=1380
1601 7.942999     1438    1                                                   41169 Ack=1 Win=64240 Len=1380
1602 7.942999     1438    1                                                   42549 Ack=1 Win=64240 Len=1380
1603 7.942999     1438    1                                                   43929 Ack=1 Win=64240 Len=1380
1604 7.942999     1438    1                                                   45309 Ack=1 Win=64240 Len=1380
1605 7.944000     1438    1                                                   46689 Ack=1 Win=64240 Len=1380
1606 7.944000     1438    1                                                   48069 Ack=1 Win=64240 Len=1380
1607 7.944000     1438    1                                                   49449 Ack=1 Win=64240 Len=1380
1608 7.944000     1438    1                                                   50829 Ack=1 Win=64240 Len=1380
1609 7.944000     1438    1                                                   52209 Ack=1 Win=64240 Len=1380
1610 7.944000     1438    1                                                   53589 Ack=1 Win=64240 Len=1380
1611 7.944000     1438    1                                                   54969 Ack=1 Win=64240 Len=1380
1612 7.944000     1438    1                                                   56349 Ack=1 Win=64240 Len=1380
1613 7.945000     1438    1                                                   57729 Ack=1 Win=64240 Len=1380
1614 7.945000     1438    1                                                   59109 Ack=1 Win=64240 Len=1380
1615 7.945000     1438    1                                                   60489 Ack=1 Win=64240 Len=1380
1616 7.945000     1438    1                                                   61869 Ack=1 Win=64240 Len=1380
1617 7.945000       64    1                                                   Ack=1741169 Win=24840 Len=0
1618 7.945000       64    1                                                   Ack=1743929 Win=24840 Len=0
1619 7.945000     1438    1                                                   63249 Ack=1 Win=64240 Len=1380
1620 7.945000     1438    1                                                   64629 Ack=1 Win=64240 Len=1380
1621 7.945000       64    1                                                   Ack=1746689 Win=24840 Len=0
1622 7.945000     1438                                                        66009 Ack=1 Win=64240 Len=1380
1623 7.945000     1438    1864948 TCP  60602  1525  10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=1767389 Ack=1 Win=64240 Len=1380
```

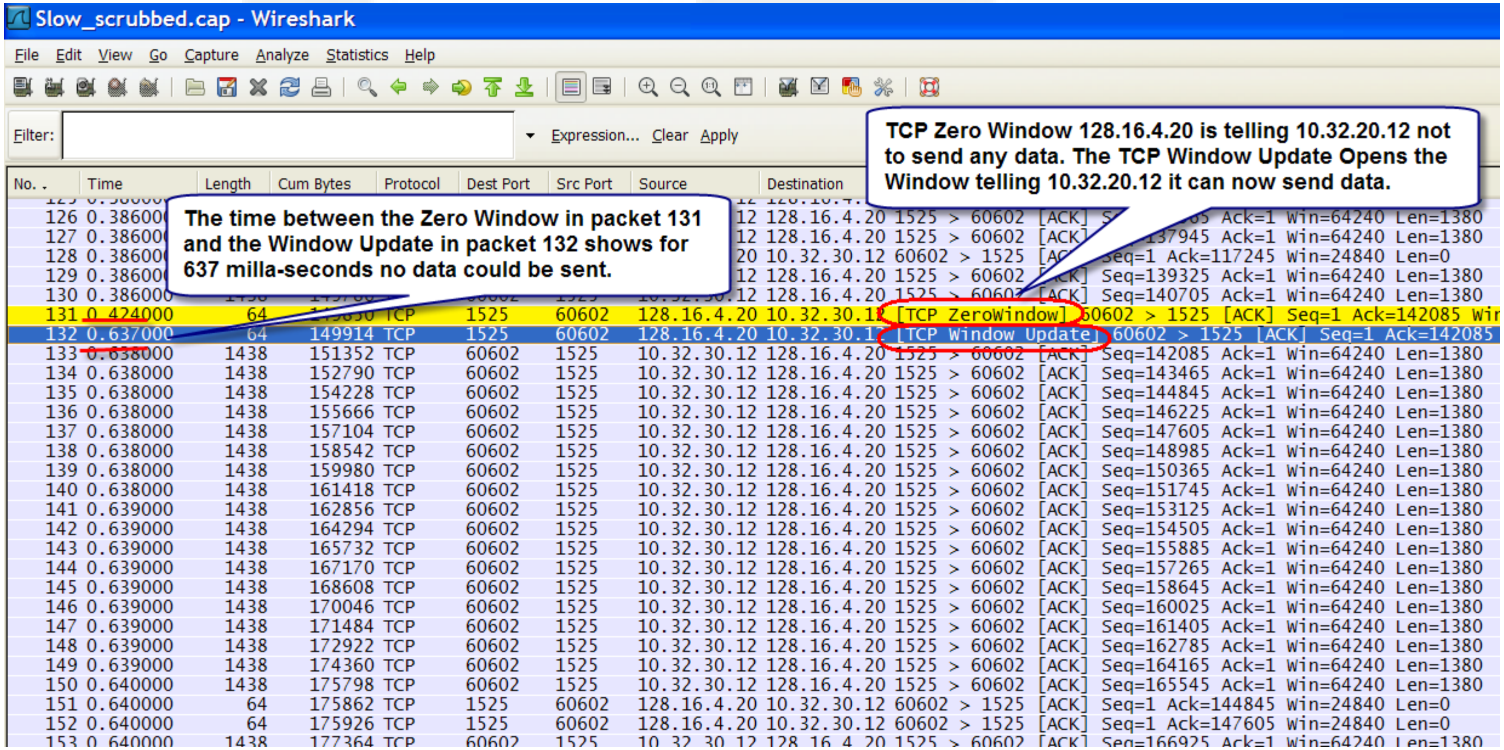
Wireshark: 102656 Expert Infos

```
Group  ▲      Protocol ◂   Summary
⊞ Sequence    TCP          Window update     4510
⊟ Sequence    TCP          Zero window       4650
    Packet:   131                            0
    Packet:   259                            0
    Packet:   287                            0
    Packet:   385                            0
    Packet:   387                            0
    Packet:   416                            0
    Packet:   445                            0
    Packet:   477                            0
    Packet:   535                            0
    Packet:   564                            0
    Packet:   566                            0
    Packet:   622                            0
    Packet:   672                            0
    Packet:   701                            0
    Packet:   745                            0
    Packet:   837                            0
```

In the Expert Infos Notes section Zero Window are being shown.

Indentifying Zero Window Size

- TCP Zero Window followed by TCP Windows Update


Slow_scrubbed.cap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

TCP Zero Window 128.16.4.20 is telling 10.32.20.12 not to send any data. The TCP Window Update Opens the Window telling 10.32.20.12 it can now send data.

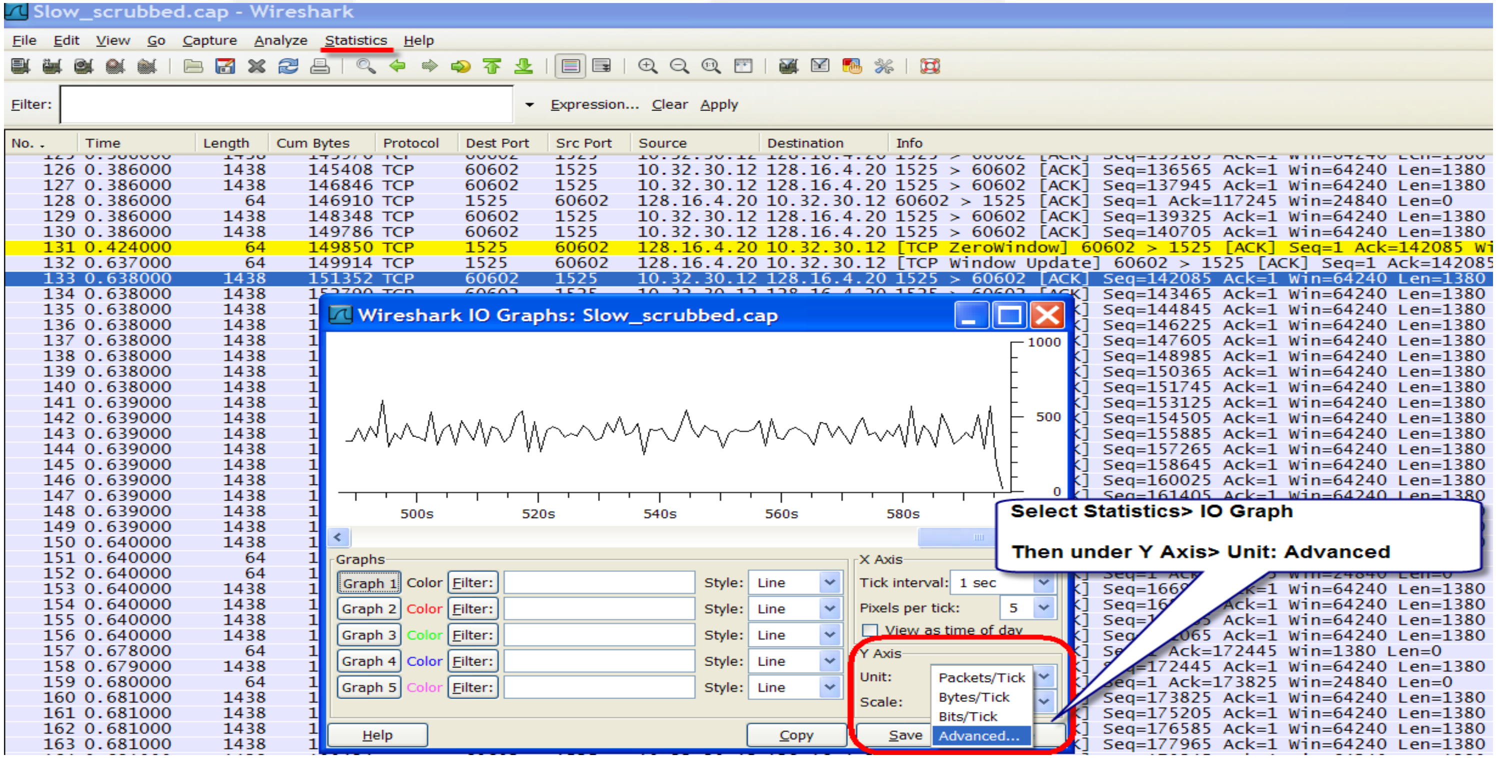
The time between the Zero Window in packet 131 and the Window Update in packet 132 shows for 637 milla-seconds no data could be sent.

```
No. .  Time     Length Cum Bytes Protocol Dest Port Src Port Source      Destination
126 0.38600                                               12 128.16.4.20 1525 > 60602 [ACK] S        65 Ack=1 Win=64240 Len=1380
127 0.38600                                               12 128.16.4.20 1525 > 60602 [ACK]      37945 Ack=1 Win=64240 Len=1380
128 0.38600                                               20 10.32.30.12 60602 > 1525 [A      Seq=1 Ack=117245 Win=24840 Len=0
129 0.38600                                               12 128.16.4.20 1525 > 60602    CK] Seq=139325 Ack=1 Win=64240 Len=1380
130 0.386000                                              12 128.16.4.20 1525 > 6060  [ACK] Seq=140705 Ack=1 Win=64240 Len=1380
131 0.424000     64 149850 TCP    1525   60602  128.16.4.20 10.32.30.12 [TCP ZeroWindow] 60602 > 1525 [ACK] Seq=1 Ack=142085 Wir
132 0.637000     64 149914 TCP    1525   60602  128.16.4.20 10.32.30.12 [TCP Window Update] 60602 > 1525 [ACK] Seq=1 Ack=142085
133 0.638000   1438 151352 TCP    60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=142085 Ack=1 Win=64240 Len=1380
134 0.638000   1438 152790 TCP    60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=143465 Ack=1 Win=64240 Len=1380
135 0.638000   1438 154228 TCP    60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=144845 Ack=1 Win=64240 Len=1380
136 0.638000   1438 155666 TCP    60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=146225 Ack=1 Win=64240 Len=1380
137 0.638000   1438 157104 TCP    60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=147605 Ack=1 Win=64240 Len=1380
138 0.638000   1438 158542 TCP    60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=148985 Ack=1 Win=64240 Len=1380
139 0.638000   1438 159980 TCP    60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=150365 Ack=1 Win=64240 Len=1380
140 0.638000   1438 161418 TCP    60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=151745 Ack=1 Win=64240 Len=1380
141 0.639000   1438 162856 TCP    60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=153125 Ack=1 Win=64240 Len=1380
142 0.639000   1438 164294 TCP    60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=154505 Ack=1 Win=64240 Len=1380
143 0.639000   1438 165732 TCP    60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=155885 Ack=1 Win=64240 Len=1380
144 0.639000   1438 167170 TCP    60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=157265 Ack=1 Win=64240 Len=1380
145 0.639000   1438 168608 TCP    60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=158645 Ack=1 Win=64240 Len=1380
146 0.639000   1438 170046 TCP    60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=160025 Ack=1 Win=64240 Len=1380
147 0.639000   1438 171484 TCP    60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=161405 Ack=1 Win=64240 Len=1380
148 0.639000   1438 172922 TCP    60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=162785 Ack=1 Win=64240 Len=1380
149 0.639000   1438 174360 TCP    60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=164165 Ack=1 Win=64240 Len=1380
150 0.640000   1438 175798 TCP    60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=165545 Ack=1 Win=64240 Len=1380
151 0.640000     64 175862 TCP    1525   60602  128.16.4.20 10.32.30.12 60602 > 1525 [ACK] Seq=1 Ack=144845 Win=24840 Len=0
152 0.640000     64 175926 TCP    1525   60602  128.16.4.20 10.32.30.12 60602 > 1525 [ACK] Seq=1 Ack=147605 Win=24840 Len=0
153 0.640000   1438 177364 TCP    60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=166925 Ack=1 Win=64240 Len=1380
```

gearbit
Get it in Gear

Indentifying Zero Window Size

- Select: Statistics
  Then under Y Axis Units: select Advanced


Slow_scrubbed.cap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
Wireshark IO Graphs: Slow_scrubbed.cap
1000
500
0
500s
520s
540s
560s
580s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: Style: Line
Graph 3 Color Filter: Style: Line
Graph 4 Color Filter: Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
□ View as time of day
Y Axis
Unit:
Scale:
Packets/Tick
Bytes/Tick
Bits/Tick
Advanced...
Help
Copy
Save

```
No. .  Time      Length  Cum Bytes  Protocol  Dest Port  Src Port  Source       Destination  Info
126 0.386000  1438  145408 TCP  60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=136565 Ack=1 Win=64240 Len=1380
127 0.386000  1438  146846 TCP  60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=137945 Ack=1 Win=64240 Len=1380
128 0.386000    64  146910 TCP  1525   60602  128.16.4.20 10.32.30.12 60602 > 1525 [ACK] Seq=1 Ack=117245 Win=24840 Len=0
129 0.386000  1438  148348 TCP  60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=139325 Ack=1 Win=64240 Len=1380
130 0.386000  1438  149786 TCP  60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=140705 Ack=1 Win=64240 Len=1380
131 0.424000    64  149850 TCP  1525   60602  128.16.4.20 10.32.30.12 [TCP ZeroWindow] 60602 > 1525 [ACK] Seq=1 Ack=142085 Wi
132 0.637000    64  149914 TCP  1525   60602  128.16.4.20 10.32.30.12 [TCP Window Update] 60602 > 1525 [ACK] Seq=1 Ack=142085
133 0.638000  1438  151352 TCP  60602  1525   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=142085 Ack=1 Win=64240 Len=1380
134 0.638000  1438  1                                        Seq=143465 Ack=1 Win=64240 Len=1380
135 0.638000  1438  1                                        Seq=144845 Ack=1 Win=64240 Len=1380
136 0.638000  1438  1                                        Seq=146225 Ack=1 Win=64240 Len=1380
137 0.638000  1438  1                                        Seq=147605 Ack=1 Win=64240 Len=1380
138 0.638000  1438  1                                        Seq=148985 Ack=1 Win=64240 Len=1380
139 0.638000  1438  1                                        Seq=150365 Ack=1 Win=64240 Len=1380
140 0.638000  1438  1                                        Seq=151745 Ack=1 Win=64240 Len=1380
141 0.639000  1438  1                                        Seq=153125 Ack=1 Win=64240 Len=1380
142 0.639000  1438  1                                        Seq=154505 Ack=1 Win=64240 Len=1380
143 0.639000  1438  1                                        Seq=155885 Ack=1 Win=64240 Len=1380
144 0.639000  1438  1                                        Seq=157265 Ack=1 Win=64240 Len=1380
145 0.639000  1438  1                                        Seq=158645 Ack=1 Win=64240 Len=1380
146 0.639000  1438  1                                        Seq=160025 Ack=1 Win=64240 Len=1380
147 0.639000  1438  1                                        Seq=161405 Ack=1 Win=64240 Len=1380
148 0.639000  1438  1
149 0.639000  1438  1
150 0.640000  1438  1
151 0.640000    64  1
152 0.640000    64  1
153 0.640000  1438  1                                        Seq=1669     k=1 Win=64240 Len=1380
154 0.640000  1438  1                                        Seq=16       Ack=1 Win=64240 Len=1380
155 0.640000  1438  1                                        Seq=1        Ack=1 Win=64240 Len=1380
156 0.640000  1438  1                                        Seq    2065 Ack=1 Win=64240 Len=1380
157 0.678000    64  1                                        Se     Ack=172445 Win=1380 Len=0
158 0.679000  1438  1                                           =172445 Ack=1 Win=64240 Len=1380
159 0.680000    64  1                                         eq=1 Ack=173825 Win=24840 Len=0
160 0.681000  1438  1                                        Seq=173825 Ack=1 Win=64240 Len=1380
161 0.681000  1438  1                                        Seq=175205 Ack=1 Win=64240 Len=1380
162 0.681000  1438  1                                        Seq=176585 Ack=1 Win=64240 Len=1380
163 0.681000  1438  1                                        Seq=177965 Ack=1 Win=64240 Len=1380
```

Select Statistics> IO Graph

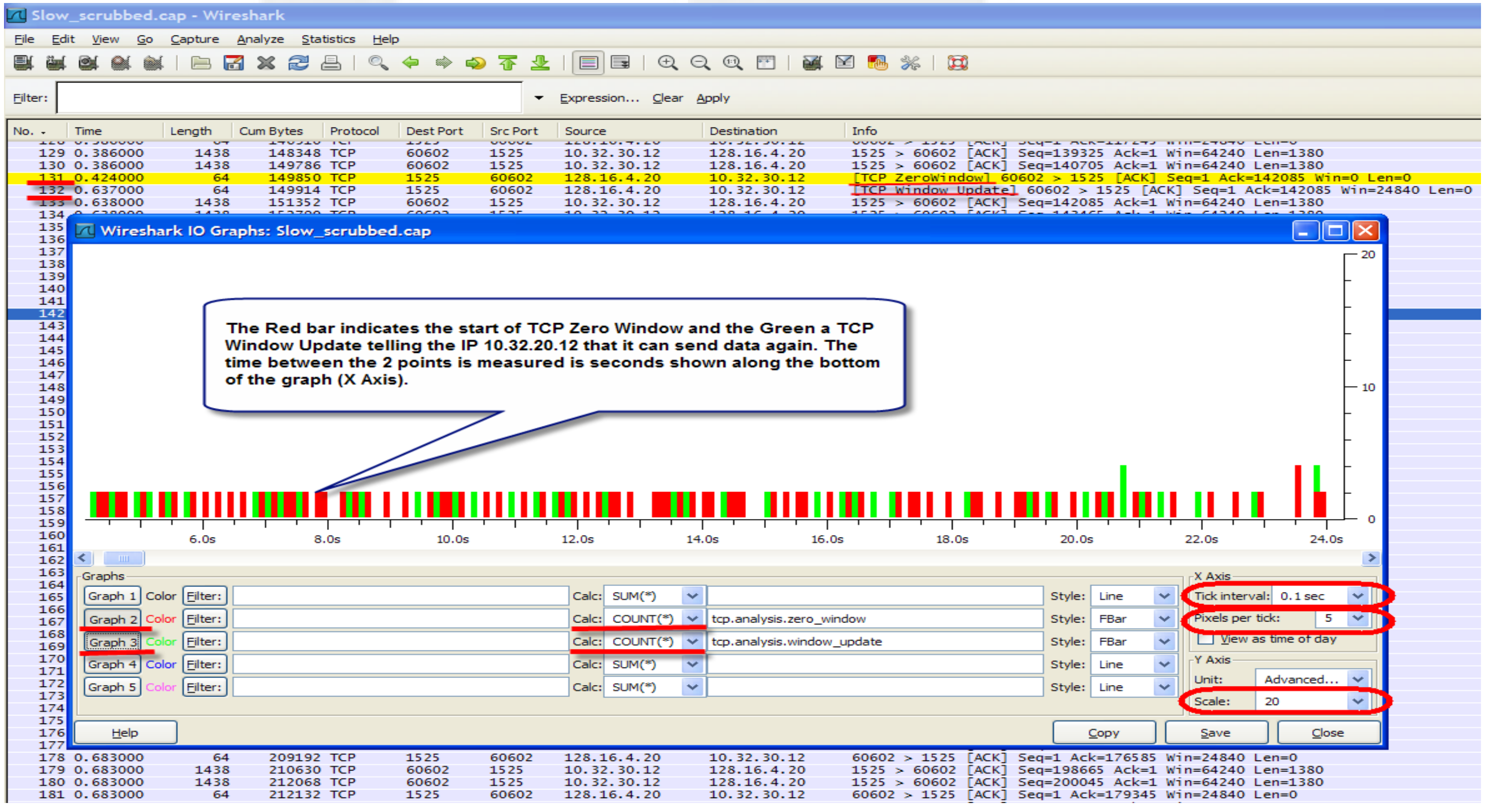
Then under Y Axis> Unit: Advanced

Indentifying Zero Window Size

- Modify X Axes & Y Axes

  X Axes: Tick Interval 0.1 sec, Pixels per tick 5

  Y Axes: Scale 20


Slow_scrubbed.cap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
Wireshark IO Graphs: Slow_scrubbed.cap
20
10
0
6.0s
8.0s
10.0s
12.0s
14.0s
16.0s
18.0s
20.0s
22.0s
24.0s
Help
Copy
Save
Close

```
No. -  Time      Length  Cum Bytes Protocol Dest Port Src Port Source        Destination   Info
129 0.386000     1438    148348 TCP      60602     1525     10.32.30.12   128.16.4.20   1525 > 60602 [ACK] Seq=139325 Ack=1 Win=64240 Len=1380
130 0.386000     1438    149786 TCP      60602     1525     10.32.30.12   128.16.4.20   1525 > 60602 [ACK] Seq=140705 Ack=1 Win=64240 Len=1380
131 0.424000       64    149850 TCP      1525      60602    128.16.4.20   10.32.30.12   [TCP ZeroWindow] 60602 > 1525 [ACK] Seq=1 Ack=142085 Win=0 Len=0
132 0.637000       64    149914 TCP      1525      60602    128.16.4.20   10.32.30.12   [TCP Window Update] 60602 > 1525 [ACK] Seq=1 Ack=142085 Win=24840 Len=0
133 0.638000     1438    151352 TCP      60602     1525     10.32.30.12   128.16.4.20   1525 > 60602 [ACK] Seq=142085 Ack=1 Win=64240 Len=1380
...
178 0.683000       64    209192 TCP      1525      60602    128.16.4.20   10.32.30.12   60602 > 1525 [ACK] Seq=1 Ack=176585 Win=24840 Len=0
179 0.683000     1438    210630 TCP      60602     1525     10.32.30.12   128.16.4.20   1525 > 60602 [ACK] Seq=198665 Ack=1 Win=64240 Len=1380
180 0.683000     1438    212068 TCP      60602     1525     10.32.30.12   128.16.4.20   1525 > 60602 [ACK] Seq=200045 Ack=1 Win=64240 Len=1380
181 0.683000       64    212132 TCP      1525      60602    128.16.4.20   10.32.30.12   60602 > 1525 [ACK] Seq=1 Ack=179345 Win=24840 Len=0
```

The Red bar indicates the start of TCP Zero Window and the Green a TCP Window Update telling the IP 10.32.20.12 that it can send data again. The time between the 2 points is measured is seconds shown along the bottom of the graph (X Axis).

Graphs

			Calc:		Style:
Graph 1	Color	Filter:	SUM(*)		Line
Graph 2	Color	Filter:	COUNT(*)	tcp.analysis.zero_window	FBar
Graph 3	Color	Filter:	COUNT(*)	tcp.analysis.window_update	FBar
Graph 4	Color	Filter:	SUM(*)		Line
Graph 5	Color	Filter:	SUM(*)		Line

X Axis

Tick interval: 0.1 sec

Pixels per tick: 5

□ View as time of day

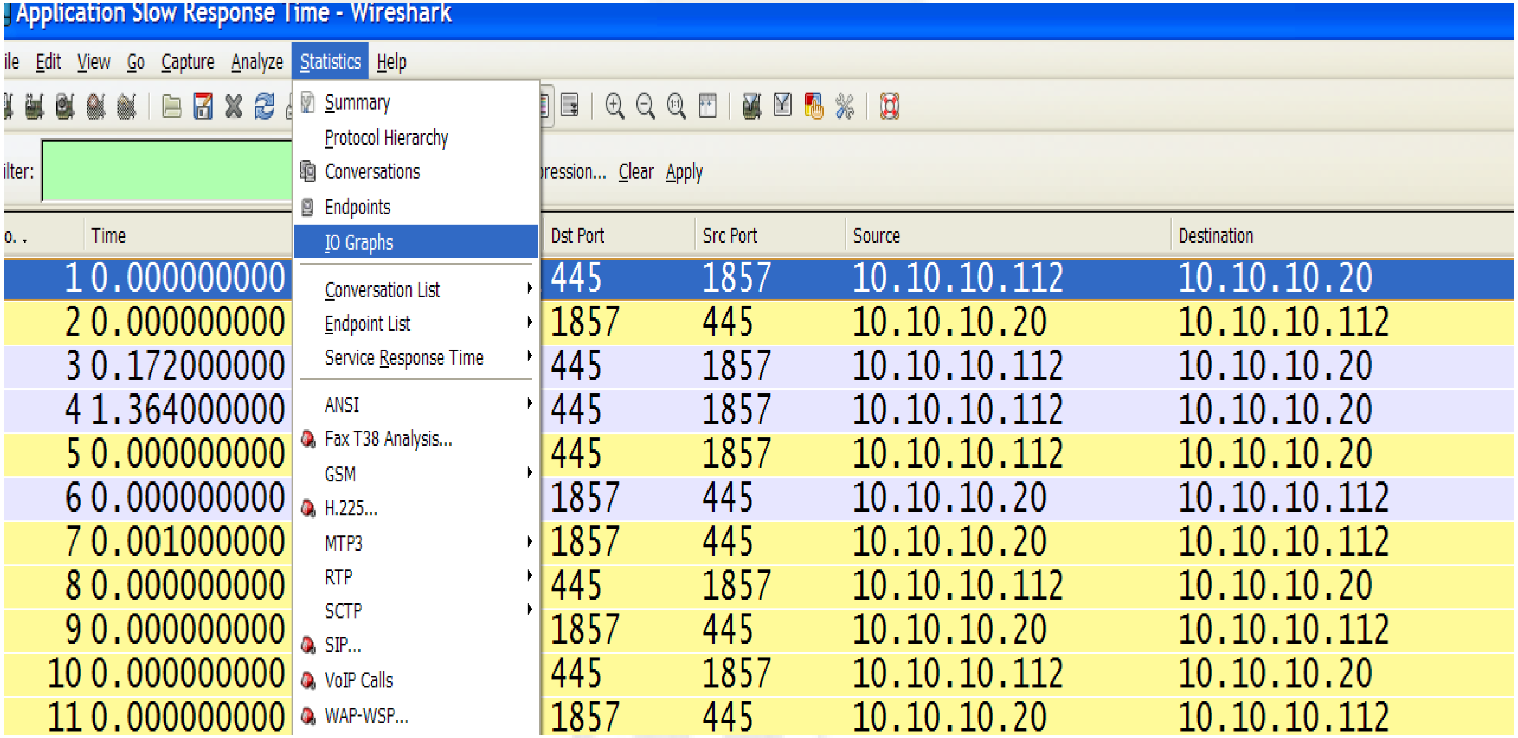
Y Axis

Unit: Advanced...

Scale: 20

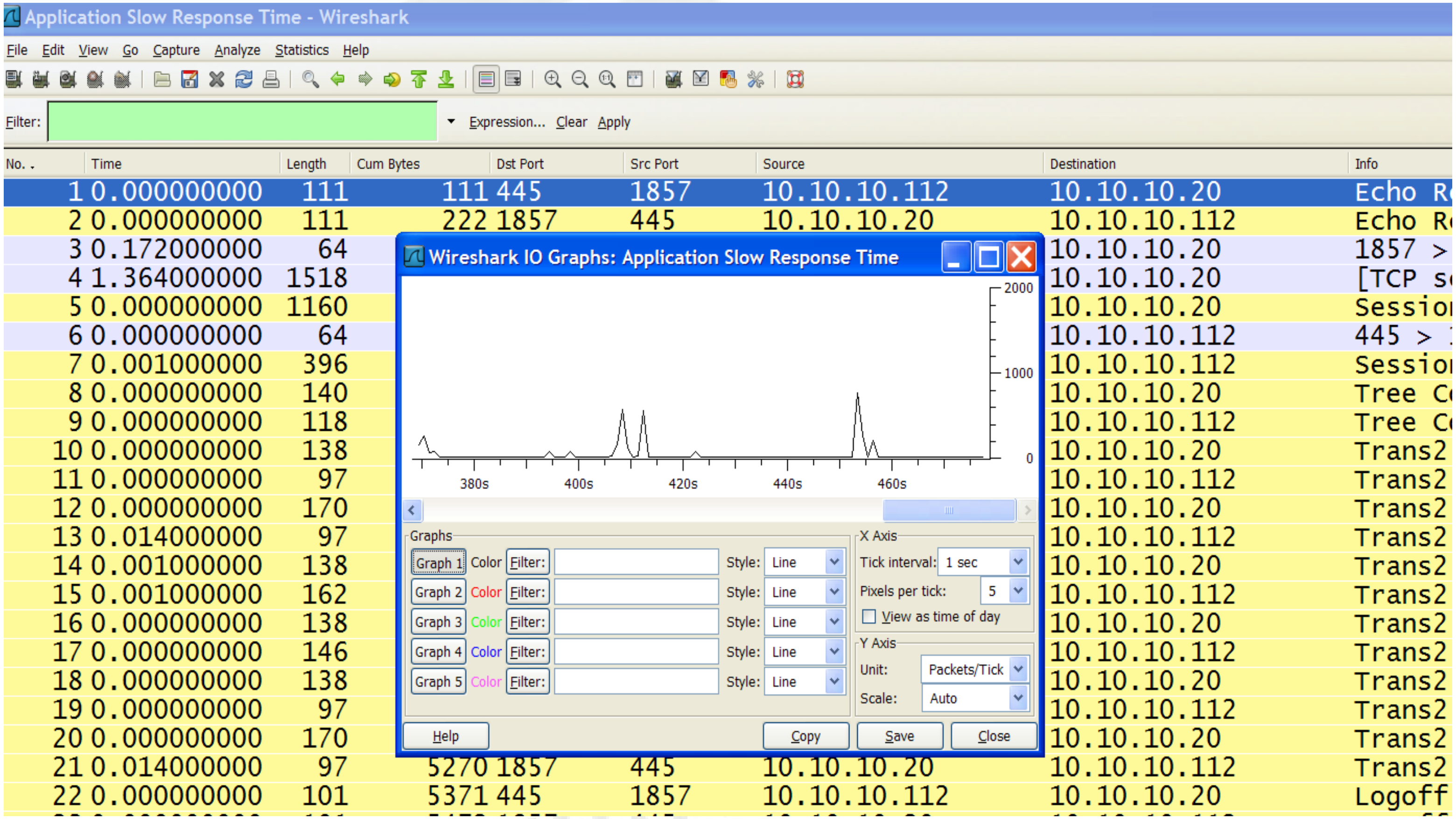
Response Time IO Graph

- Statistics IO Graph



o.	Time	Dst Port	Src Port	Source	Destination
1	0.000000000	445	1857	10.10.10.112	10.10.10.20
2	0.000000000	1857	445	10.10.10.20	10.10.10.112
3	0.172000000	445	1857	10.10.10.112	10.10.10.20
4	1.364000000	445	1857	10.10.10.112	10.10.10.20
5	0.000000000	445	1857	10.10.10.112	10.10.10.20
6	0.000000000	1857	445	10.10.10.20	10.10.10.112
7	0.001000000	1857	445	10.10.10.20	10.10.10.112
8	0.000000000	445	1857	10.10.10.112	10.10.10.20
9	0.000000000	1857	445	10.10.10.20	10.10.10.112
10	0.000000000	445	1857	10.10.10.112	10.10.10.20
11	0.000000000	1857	445	10.10.10.20	10.10.10.112

Response Time IO Graph



Application Slow Response Time - Wireshark

File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

No.	Time	Length	Cum Bytes	Dst Port	Src Port	Source	Destination	Info
1	0.000000000	111	111	445	1857	10.10.10.112	10.10.10.20	Echo R
2	0.000000000	111	222	1857	445	10.10.10.20	10.10.10.112	Echo R
3	0.172000000	64					10.10.10.20	1857 >
4	1.364000000	1518					10.10.10.20	[TCP s
5	0.000000000	1160					10.10.10.20	Sessio
6	0.000000000	64					10.10.10.112	445 >
7	0.001000000	396					10.10.10.112	Sessio
8	0.000000000	140					10.10.10.20	Tree C
9	0.000000000	118					10.10.10.112	Tree C
10	0.000000000	138					10.10.10.20	Trans2
11	0.000000000	97					10.10.10.112	Trans2
12	0.000000000	170					10.10.10.20	Trans2
13	0.014000000	97					10.10.10.112	Trans2
14	0.001000000	138					10.10.10.20	Trans2
15	0.001000000	162					10.10.10.112	Trans2
16	0.000000000	138					10.10.10.20	Trans2
17	0.000000000	146					10.10.10.112	Trans2
18	0.000000000	138					10.10.10.20	Trans2
19	0.000000000	97					10.10.10.112	Trans2
20	0.000000000	170					10.10.10.20	Trans2
21	0.014000000	97	5270	1857	445	10.10.10.20	10.10.10.112	Trans2
22	0.000000000	101	5371	445	1857	10.10.10.112	10.10.10.20	Logoff

Wireshark IO Graphs: Application Slow Response Time

Graphs

Graph 1	Color	Filter:		Style:	Line
Graph 2	Color	Filter:		Style:	Line
Graph 3	Color	Filter:		Style:	Line
Graph 4	Color	Filter:		Style:	Line
Graph 5	Color	Filter:		Style:	Line

X Axis

Tick interval: 1 sec

Pixels per tick: 5

□ View as time of day

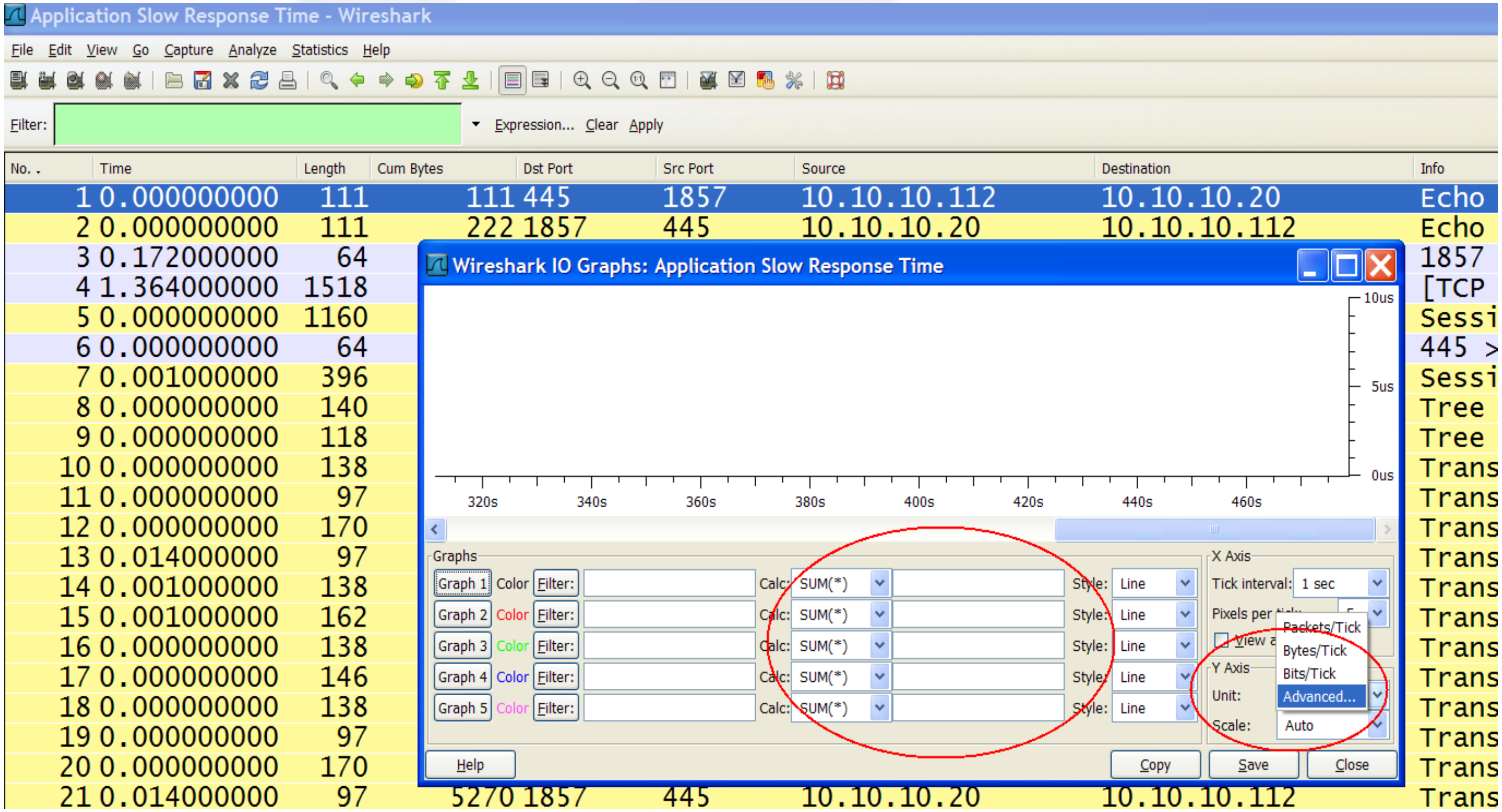
Y Axis

Unit: Packets/Tick

Scale: Auto

Response Time IO Graph

- Advanced tab



Application Slow Response Time - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

No.	Time	Length	Cum Bytes	Dst Port	Src Port	Source	Destination	Info
1	0.000000000	111	111	445	1857	10.10.10.112	10.10.10.20	Echo
2	0.000000000	111	222	1857	445	10.10.10.20	10.10.10.112	Echo
3	0.172000000	64						1857
4	1.364000000	1518						[TCP
5	0.000000000	1160						Sessi
6	0.000000000	64						445 >
7	0.001000000	396						Sessi
8	0.000000000	140						Tree
9	0.000000000	118						Tree
10	0.000000000	138						Trans
11	0.000000000	97						Trans
12	0.000000000	170						Trans
13	0.014000000	97						Trans
14	0.001000000	138						Trans
15	0.001000000	162						Trans
16	0.000000000	138						Trans
17	0.000000000	146						Trans
18	0.000000000	138						Trans
19	0.000000000	97						Trans
20	0.000000000	170						Trans
21	0.014000000	97	5270	1857	445	10.10.10.20	10.10.10.112	Trans

Wireshark IO Graphs: Application Slow Response Time

Graphs

Graph 1	Color	Filter:	Calc: SUM(*)		Style: Line
Graph 2	Color	Filter:	Calc: SUM(*)		Style: Line
Graph 3	Color	Filter:	Calc: SUM(*)		Style: Line
Graph 4	Color	Filter:	Calc: SUM(*)		Style: Line
Graph 5	Color	Filter:	Calc: SUM(*)		Style: Line

X Axis

Tick interval: 1 sec

Pixels per tick: 5

□ View a

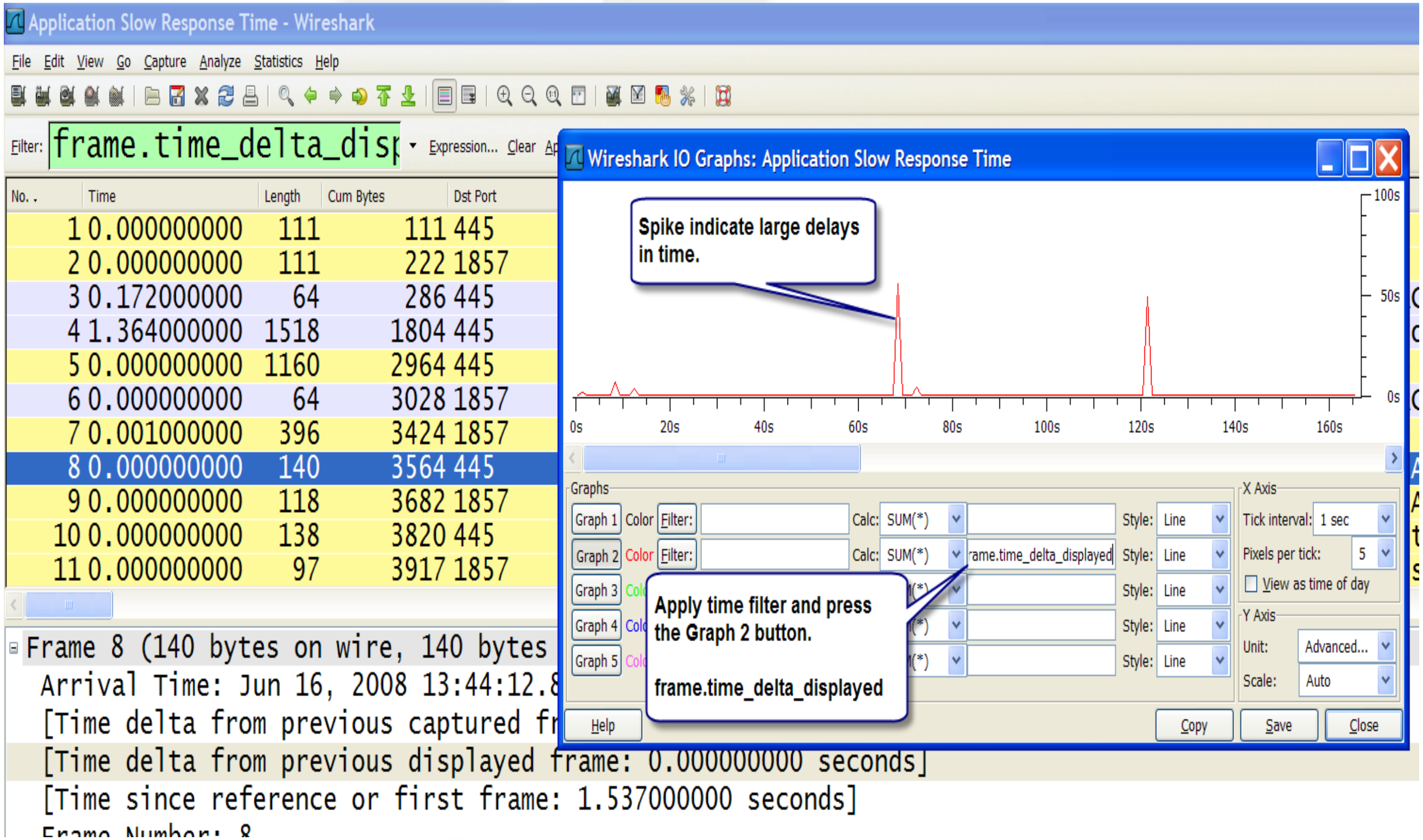
Y Axis

Unit: Advanced...

Scale: Auto

Response Time IO Graph

Advanced tab-Apply-frame.time_delta_displayed


Application Slow Response Time - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Ap
Wireshark IO Graphs: Application Slow Response Time
100s
50s
0s
0s 20s 40s 60s 80s 100s 120s 140s 160s
Graphs
X Axis
Y Axis
Help
Copy
Save
Close

Filter: frame.time_delta_disp

No.	Time	Length	Cum Bytes	Dst Port
1	0.000000000	111	111	445
2	0.000000000	111	222	1857
3	0.172000000	64	286	445
4	1.364000000	1518	1804	445
5	0.000000000	1160	2964	445
6	0.000000000	64	3028	1857
7	0.001000000	396	3424	1857
8	0.000000000	140	3564	445
9	0.000000000	118	3682	1857
10	0.000000000	138	3820	445
11	0.000000000	97	3917	1857

```
⊟ Frame 8 (140 bytes on wire, 140 bytes
    Arrival Time: Jun 16, 2008 13:44:12.8
    [Time delta from previous captured fr
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 1.537000000 seconds]
    Frame Number: 8
```

Spike indicate large delays in time.

Graph	Color	Filter	Calc		Style
Graph 1	Color	Filter:	SUM(*)		Line
Graph 2	Color	Filter:	SUM(*)	rame.time_delta_displayed	Line
Graph 3	Col		(*)		Line
Graph 4	Col		(*)		Line
Graph 5	Col		(*)		Line

X Axis
Tick interval: 1 sec
Pixels per tick: 5
☐ View as time of day

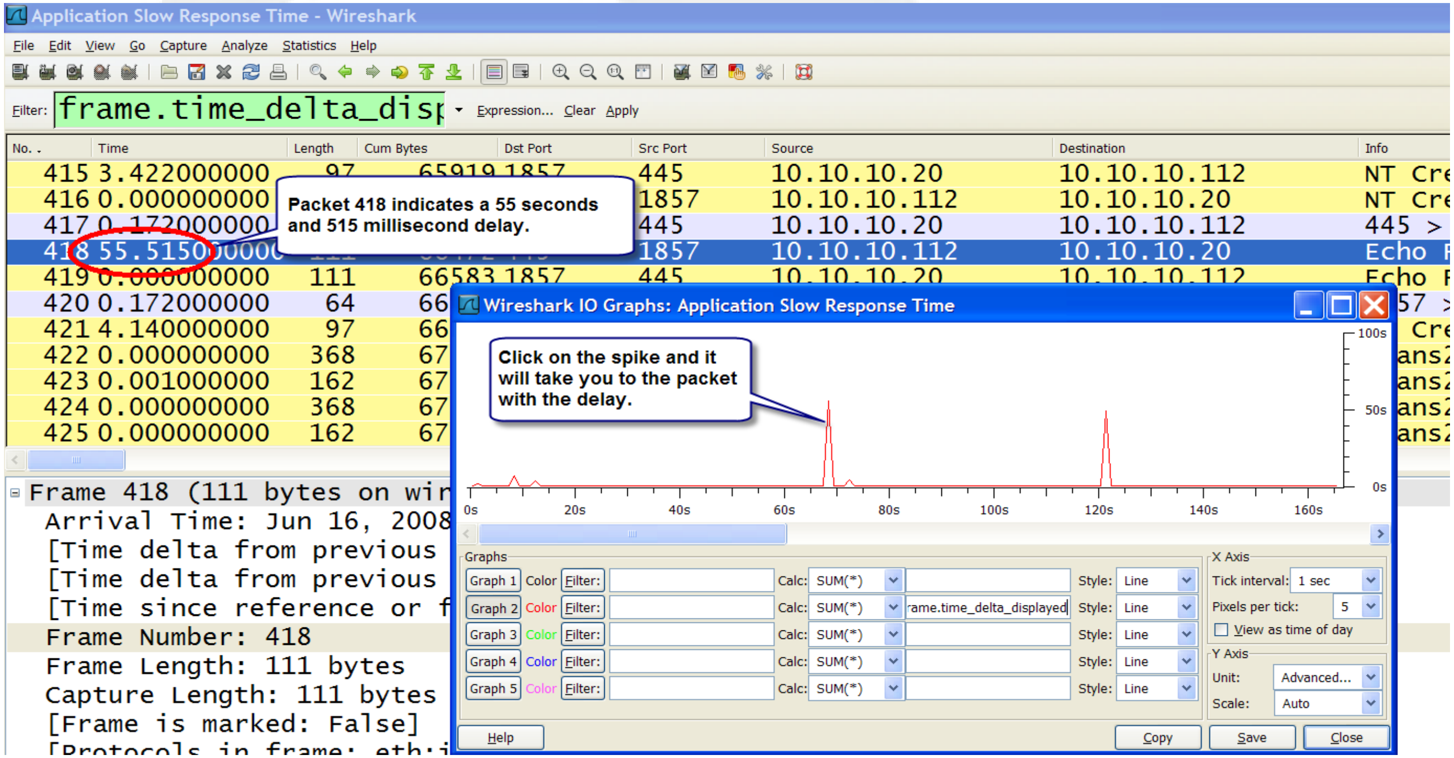
Y Axis
Unit: Advanced...
Scale: Auto

Apply time filter and press the Graph 2 button.

frame.time_delta_displayed

Response Time IO Graph

- Click on the spike and it will take you to the packet with the delay



Application Slow Response Time - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: frame.time_delta_disp

Expression... Clear Apply

```
No. .  Time          Length  Cum Bytes  Dst Port  Src Port  Source         Destination    Info
  415  3.422000000     97    65919      1857      445       10.10.10.20    10.10.10.112   NT Cre
  416  0.000000000                                1857      10.10.10.112   10.10.10.20    NT Cre
  417  0.172000000                                445       10.10.10.20    10.10.10.112   445 >
  418  55.5150000                                 1857      10.10.10.112   10.10.10.20    Echo R
  419  0.000000000    111    66583      1857      445       10.10.10.20    10.10.10.112   Echo R
  420  0.172000000     64    66                                                           57 >
  421  4.140000000     97    66                                                           Cre
  422  0.000000000    368    67                                                           ans2
  423  0.001000000    162    67                                                           ans2
  424  0.000000000    368    67                                                           ans2
  425  0.000000000    162    67                                                           ans2
```

Packet 418 indicates a 55 seconds and 515 millisecond delay.

```
⊟ Frame 418 (111 bytes on wir
    Arrival Time: Jun 16, 2008
    [Time delta from previous
    [Time delta from previous
    [Time since reference or f
    Frame Number: 418
    Frame Length: 111 bytes
    Capture Length: 111 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:i
```

Wireshark IO Graphs: Application Slow Response Time

Click on the spike and it will take you to the packet with the delay.

Graphs

Graph 1	Color	Filter:		Calc:	SUM(*)		Style: Line
Graph 2	Color	Filter:		Calc:	SUM(*)	rame.time_delta_displayed	Style: Line
Graph 3	Color	Filter:		Calc:	SUM(*)		Style: Line
Graph 4	Color	Filter:		Calc:	SUM(*)		Style: Line
Graph 5	Color	Filter:		Calc:	SUM(*)		Style: Line

X Axis

Tick interval: 1 sec

Pixels per tick: 5

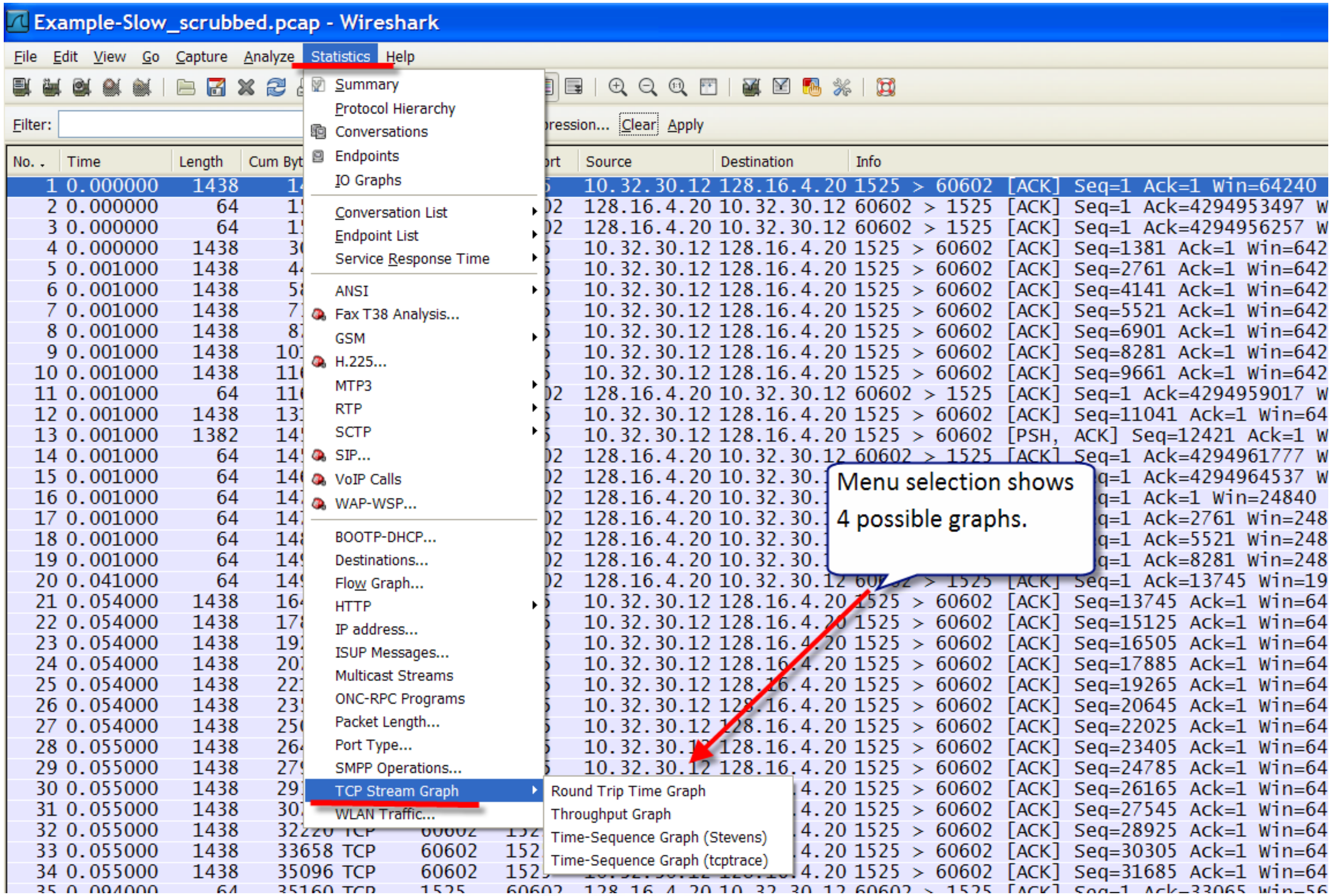
☐ View as time of day

Y Axis

Unit: Advanced...

Scale: Auto

TCP Stream Graphs



```
No. .  Time      Length  Cum Byt              rt   Source      Destination Info
 1 0.000000  1438    14                 5   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=1 Ack=1 Win=64240
 2 0.000000    64    15                 02  128.16.4.20 10.32.30.12 60602 > 1525 [ACK] Seq=1 Ack=4294953497 W
 3 0.000000    64    15                 02  128.16.4.20 10.32.30.12 60602 > 1525 [ACK] Seq=1 Ack=4294956257 W
 4 0.000000  1438    3                  5   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=1381 Ack=1 Win=642
 5 0.001000  1438    44                 5   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=2761 Ack=1 Win=642
 6 0.001000  1438    5                  5   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=4141 Ack=1 Win=642
 7 0.001000  1438    7                  5   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=5521 Ack=1 Win=642
 8 0.001000  1438    8                  5   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=6901 Ack=1 Win=642
 9 0.001000  1438    10                 5   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=8281 Ack=1 Win=642
10 0.001000  1438    11                 5   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=9661 Ack=1 Win=642
11 0.001000    64    11                 02  128.16.4.20 10.32.30.12 60602 > 1525 [ACK] Seq=1 Ack=4294959017 W
12 0.001000  1438    13                 5   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=11041 Ack=1 Win=64
13 0.001000  1382    14                 5   10.32.30.12 128.16.4.20 1525 > 60602 [PSH, ACK] Seq=12421 Ack=1 W
14 0.001000    64    14                 02  128.16.4.20 10.32.30.12 60602 > 1525 [ACK] Seq=1 Ack=4294961777 W
15 0.001000    64    14                 02  128.16.4.20 10.32.30.                      q=1 Ack=4294964537 W
16 0.001000    64    14                 02  128.16.4.20 10.32.30.                      q=1 Ack=1 Win=24840
17 0.001000    64    14                 02  128.16.4.20 10.32.30.                      q=1 Ack=2761 Win=248
18 0.001000    64    14                 02  128.16.4.20 10.32.30.                      q=1 Ack=5521 Win=248
19 0.001000    64    14                 02  128.16.4.20 10.32.30.                      q=1 Ack=8281 Win=248
20 0.041000    64    14                 02  128.16.4.20 10.32.30.12 60     > 1525 [ACK] Seq=1 Ack=13745 Win=19
21 0.054000  1438    16                 5   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=13745 Ack=1 Win=64
22 0.054000  1438    17                 5   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=15125 Ack=1 Win=64
23 0.054000  1438    19                 5   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=16505 Ack=1 Win=64
24 0.054000  1438    20                 5   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=17885 Ack=1 Win=64
25 0.054000  1438    22                 5   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=19265 Ack=1 Win=64
26 0.054000  1438    23                 5   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=20645 Ack=1 Win=64
27 0.054000  1438    25                 5   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=22025 Ack=1 Win=64
28 0.055000  1438    26                 5   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=23405 Ack=1 Win=64
29 0.055000  1438    27                 5   10.32.30.12 128.16.4.20 1525 > 60602 [ACK] Seq=24785 Ack=1 Win=64
30 0.055000  1438    29                                       4.20 1525 > 60602 [ACK] Seq=26165 Ack=1 Win=64
31 0.055000  1438    30                                       4.20 1525 > 60602 [ACK] Seq=27545 Ack=1 Win=64
32 0.055000  1438    32220 TCP   60602  152                   4.20 1525 > 60602 [ACK] Seq=28925 Ack=1 Win=64
33 0.055000  1438    33658 TCP   60602  152                   4.20 1525 > 60602 [ACK] Seq=30305 Ack=1 Win=64
34 0.055000  1438    35096 TCP   60602  152                   4.20 1525 > 60602 [ACK] Seq=31685 Ack=1 Win=64
35 0.094000    64    35160 TCP   1525   60602 128.16.4.20 10.32.30.12 60602 > 1525 [ACK] Seq=1 Ack=33065 Win=56
```

Menu selection shows 4 possible graphs.

TCP Stream Graphs

- **Round Trip Time Graph**: shows the round trip time for ACKs over time.

- **Through Put Graph**: measures through put using TCP sequence numbers.

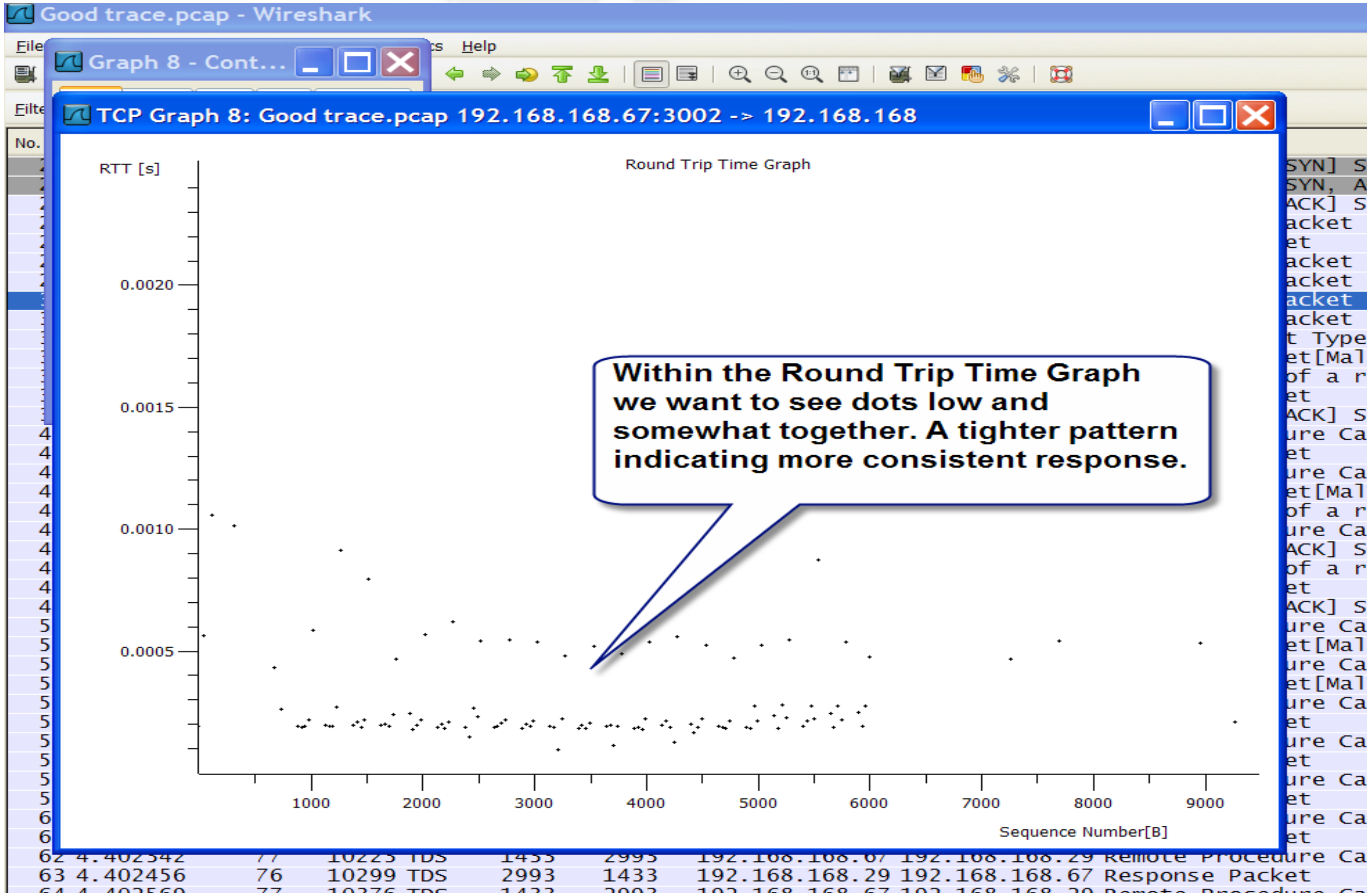
- **Time-Sequence Graph (Stevens):** a graph of TCP sequence numbers versus time. This helps us see if traffic is moving along without interruption, packet loss or long delays.

  Reference: TCP/IP Illustrated by W. Richard Stevens

- **Time-Sequence Graph (tcptrace):** a graph of TCP sequence numbers versus time. It also keeps track of the ACK values received from the other endpoint and tracks the receive window advertised from the other endpoint.

  Reference: tcptrace is a tool written by Shawn Ostermann at Ohio University see www.tcptrace.org

TCP Steam Graphs-Round Trip



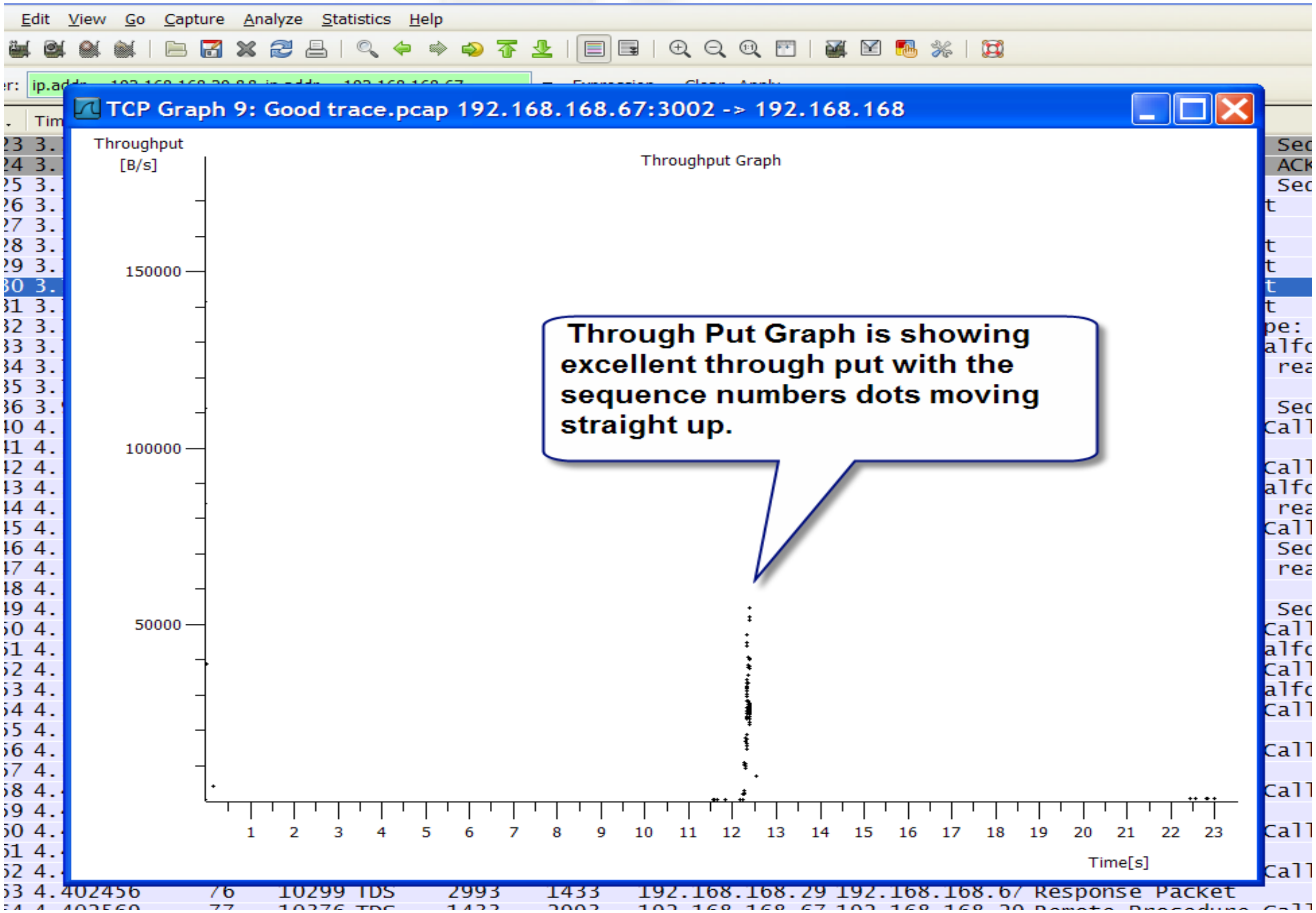
```
63 4.402456    76   10299 TDS    2993   1433   192.168.168.29 192.168.168.67 Response Packet
```

Within the Round Trip Time Graph we want to see dots low and somewhat together. A tighter pattern indicating more consistent response.

gearbit

Get it in Gear

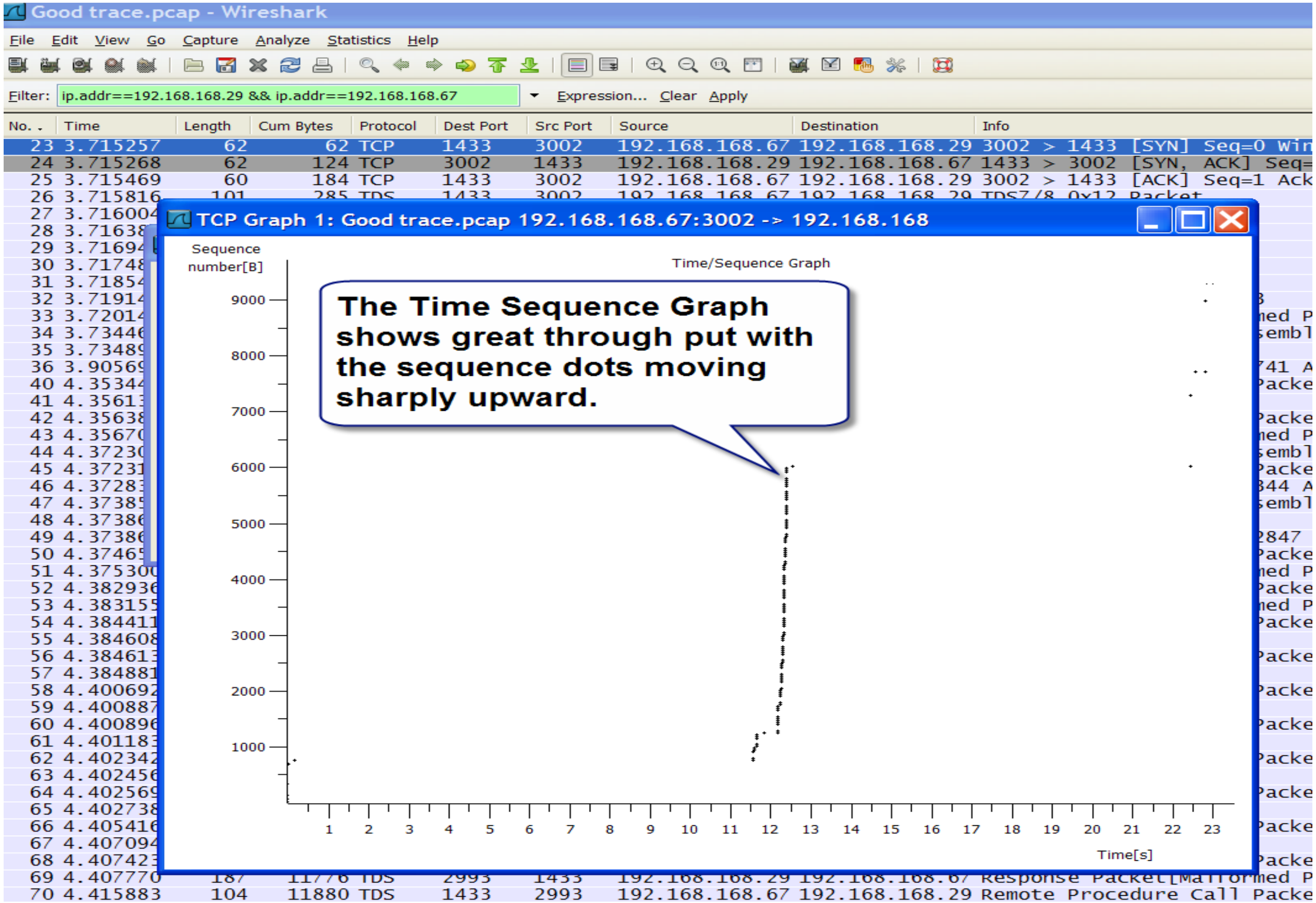
TCP Stream Graphs-Through Put



```
53 4.402456    76    10299 TDS    2993    1433    192.168.168.29 192.168.168.67 Response Packet
```

Through Put Graph is showing excellent through put with the sequence numbers dots moving straight up.

TCP Stream Graphs-Time Sequence

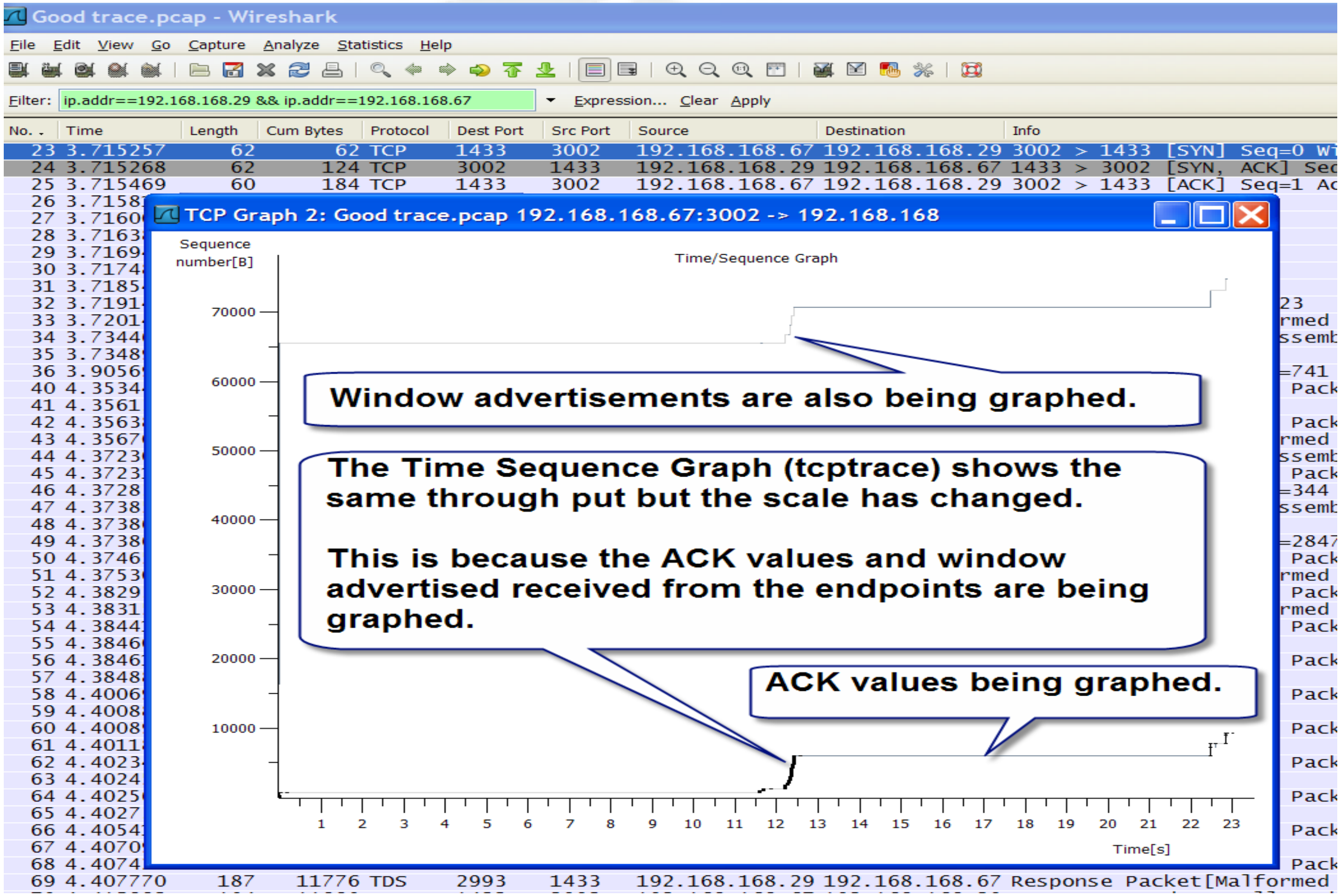


Good trace.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: ip.addr==192.168.168.29 && ip.addr==192.168.168.67
Expression... Clear Apply
TCP Graph 1: Good trace.pcap 192.168.168.67:3002 -> 192.168.168
Sequence number[B]
Time/Sequence Graph
9000
8000
7000
6000
5000
4000
3000
2000
1000
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
Time[s]

```
No. .  Time        Length  Cum Bytes  Protocol  Dest Port  Src Port  Source          Destination     Info
 23 3.715257       62         62 TCP      1433       3002      192.168.168.67 192.168.168.29 3002 > 1433 [SYN] Seq=0 Win
 24 3.715268       62        124 TCP      3002       1433      192.168.168.29 192.168.168.67 1433 > 3002 [SYN, ACK] Seq=
 25 3.715469       60        184 TCP      1433       3002      192.168.168.67 192.168.168.29 3002 > 1433 [ACK] Seq=1 Ack
 26 3.715816      101        285 TDS      1433       3002      192.168.168.67 192.168.168.29 TDS7/8 0x12 Packet
 27 3.716004
 28 3.71638
 29 3.71694
 30 3.71748
 31 3.71854
 32 3.71914                                                                                   3
 33 3.72014                                                                                   ned P
 34 3.73446                                                                                   sembl
 35 3.73489
 36 3.90569                                                                                   741 A
 40 4.35344                                                                                   Packe
 41 4.35613
 42 4.35638                                                                                   Packe
 43 4.35670                                                                                   ned P
 44 4.37230                                                                                   sembl
 45 4.37231                                                                                   Packe
 46 4.37283                                                                                   344 A
 47 4.37385                                                                                   sembl
 48 4.37386
 49 4.37386                                                                                   2847
 50 4.37465                                                                                   Packe
 51 4.375300                                                                                  ned P
 52 4.382936                                                                                  Packe
 53 4.383155                                                                                  ned P
 54 4.384411                                                                                  Packe
 55 4.384608
 56 4.384613                                                                                  Packe
 57 4.384881
 58 4.400692                                                                                  Packe
 59 4.400887
 60 4.400896                                                                                  Packe
 61 4.401183
 62 4.402342                                                                                  Packe
 63 4.402456
 64 4.402569                                                                                  Packe
 65 4.402738
 66 4.405416                                                                                  Packe
 67 4.407094
 68 4.407423                                                                                  Packe
 69 4.407770      187      11776 TDS      2993       1433      192.168.168.29 192.168.168.67 Response Packet[Malformed P
 70 4.415883      104      11880 TDS      1433       2993      192.168.168.67 192.168.168.29 Remote Procedure Call Packe
```

The Time Sequence Graph shows great through put with the sequence dots moving sharply upward.

TCP Stream Graphs-TCPTrace


Good trace.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply
TCP Graph 2: Good trace.pcap 192.168.168.67:3002 -> 192.168.168
Sequence number[B]
Time/Sequence Graph
70000
60000
50000
40000
30000
20000
10000
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
Time[s]

Filter: ip.addr==192.168.168.29 && ip.addr==192.168.168.67

```
No. .  Time        Length  Cum Bytes  Protocol  Dest Port  Src Port  Source          Destination     Info
 23 3.715257        62        62 TCP    1433       3002      192.168.168.67 192.168.168.29 3002 > 1433 [SYN] Seq=0 Wi
 24 3.715268        62       124 TCP    3002       1433      192.168.168.29 192.168.168.67 1433 > 3002 [SYN, ACK] Sec
 25 3.715469        60       184 TCP    1433       3002      192.168.168.67 192.168.168.29 3002 > 1433 [ACK] Seq=1 Ac
 26 3.7158
 27 3.7160
 28 3.7163
 29 3.7169
 30 3.7174
 31 3.7185
 32 3.7191                                                                                        23
 33 3.7201                                                                                        rmed
 34 3.7344                                                                                        ssemb
 35 3.7348
 36 3.9056                                                                                        =741
 40 4.3534                                                                                         Pack
 41 4.3561
 42 4.3563                                                                                         Pack
 43 4.3567                                                                                        rmed
 44 4.3723                                                                                        ssemb
 45 4.3723                                                                                         Pack
 46 4.3728                                                                                        =344
 47 4.3738                                                                                        ssemb
 48 4.3738
 49 4.3738                                                                                        =2847
 50 4.3746                                                                                         Pack
 51 4.3753                                                                                        rmed
 52 4.3829                                                                                         Pack
 53 4.3831                                                                                        rmed
 54 4.3844                                                                                         Pack
 55 4.3846
 56 4.3846                                                                                         Pack
 57 4.3848
 58 4.4006                                                                                         Pack
 59 4.4008
 60 4.4008                                                                                         Pack
 61 4.4011
 62 4.4023                                                                                         Pack
 63 4.4024
 64 4.4025                                                                                         Pack
 65 4.4027
 66 4.4054                                                                                         Pack
 67 4.4070
 68 4.4074                                                                                         Pack
 69 4.407770       187     11776 TDS    2993       1433      192.168.168.29 192.168.168.67 Response Packet[Malformed
```

Window advertisements are also being graphed.

The Time Sequence Graph (tcptrace) shows the same through put but the scale has changed.

This is because the ACK values and window advertised received from the endpoints are being graphed.

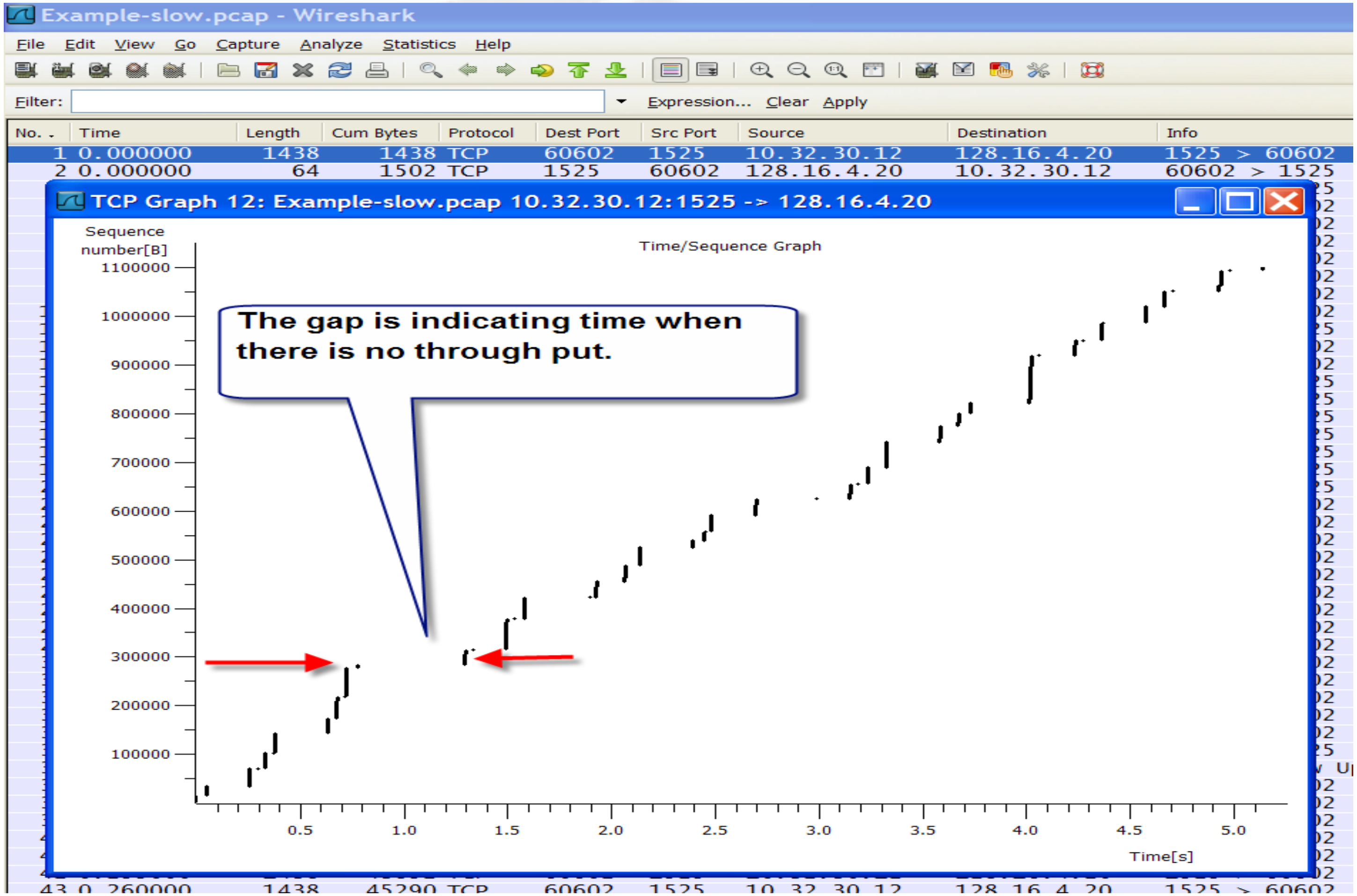
ACK values being graphed.

TCP Stream-How to View Keys

How to View Keys

• Takes you to the packet within the trace file	Ctrl + left mouse click
• Magnifies a portions of the graph	Ctrl + right mouse click
• Zoom In	Left mouse click
• Zoom Out	Shift + left mouse click
• Allows you to move the graph around	Right Mouse Click

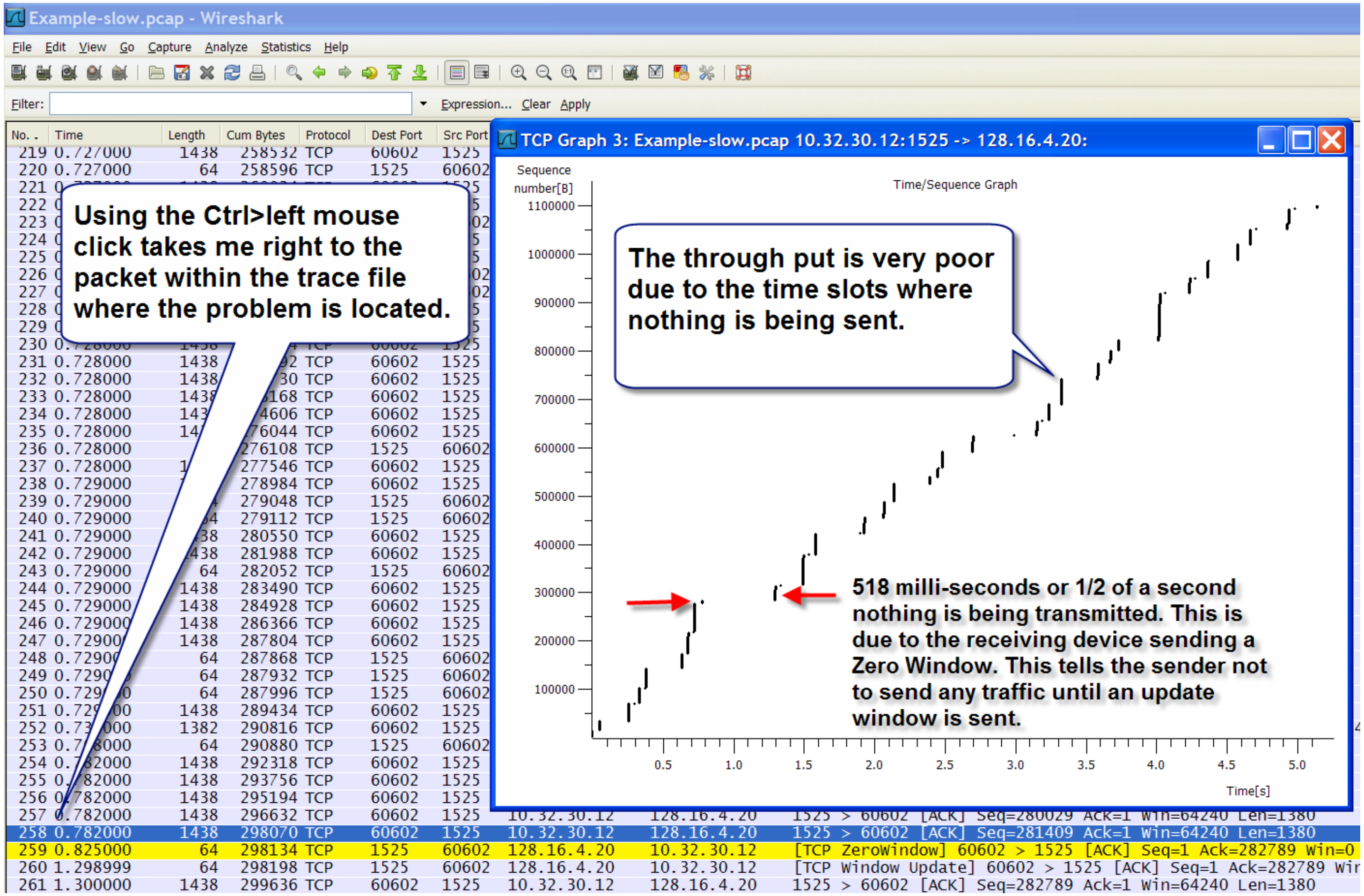
TCP Stream Graphs- Time Sequence Graph (Stevens)


Example-slow.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
TCP Graph 12: Example-slow.pcap 10.32.30.12:1525 -> 128.16.4.20
Time/Sequence Graph
Sequence number[B]
1100000
1000000
900000
800000
700000
600000
500000
400000
300000
200000
100000
0.5
1.0
1.5
2.0
2.5
3.0
3.5
4.0
4.5
5.0
Time[s]

No.	Time	Length	Cum Bytes	Protocol	Dest Port	Src Port	Source	Destination	Info
1	0.000000	1438	1438	TCP	60602	1525	10.32.30.12	128.16.4.20	1525 > 60602
2	0.000000	64	1502	TCP	1525	60602	128.16.4.20	10.32.30.12	60602 > 1525
43	0.260000	1438	45290	TCP	60602	1525	10.32.30.12	128.16.4.20	1525 > 60602

The gap is indicating time when there is no through put.

TCP Stream Graphs-Locate the Packet


Example-slow.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
TCP Graph 3: Example-slow.pcap 10.32.30.12:1525 -> 128.16.4.20:
Sequence number[B]
Time/Sequence Graph
1100000
1000000
900000
800000
700000
600000
500000
400000
300000
200000
100000
0.5
1.0
1.5
2.0
2.5
3.0
3.5
4.0
4.5
5.0
Time[s]

Using the Ctrl>left mouse click takes me right to the packet within the trace file where the problem is located.

The through put is very poor due to the time slots where nothing is being sent.

518 milli-seconds or 1/2 of a second nothing is being transmitted. This is due to the receiving device sending a Zero Window. This tells the sender not to send any traffic until an update window is sent.

```
No. . Time      Length  Cum Bytes Protocol Dest Port Src Port
219 0.727000    1438    258532 TCP    60602    1525
220 0.727000      64    258596 TCP    1525     60602
221 0                                          525
222 0                                          5
223 0                                          02
224 0                                          5
225 0                                          5
226 0                                          02
227 0                                          02
228 0                                          5
229 0                                          5
230 0.                                         525
231 0.728000    1438        92 TCP    60602    1525
232 0.728000    1438        30 TCP    60602    1525
233 0.728000    1438       168 TCP    60602    1525
234 0.728000    143       4606 TCP    60602    1525
235 0.728000    14       76044 TCP    60602    1525
236 0.728000            276108 TCP    1525     60602
237 0.728000    1       277546 TCP    60602    1525
238 0.729000            278984 TCP    60602    1525
239 0.729000       4    279048 TCP    1525     60602
240 0.729000      64    279112 TCP    1525     60602
241 0.729000     438    280550 TCP    60602    1525
242 0.729000     438    281988 TCP    60602    1525
243 0.729000      64    282052 TCP    1525     60602
244 0.729000    1438    283490 TCP    60602    1525
245 0.729000    1438    284928 TCP    60602    1525
246 0.729000    1438    286366 TCP    60602    1525
247 0.72900     1438    287804 TCP    60602    1525
248 0.7290        64    287868 TCP    1525     60602
249 0.7290  0     64    287932 TCP    1525     60602
250 0.729  0      64    287996 TCP    1525     60602
251 0.72  00    1438    289434 TCP    60602    1525
252 0.73  000   1382    290816 TCP    60602    1525
253 0.7 8000      64    290880 TCP    1525     60602
254 0. 82000    1438    292318 TCP    60602    1525
255 0. 82000    1438    293756 TCP    60602    1525
256 0 782000    1438    295194 TCP    60602    1525
257 0.782000    1438    296632 TCP    60602    1525   10.32.30.12  128.16.4.20  1525 > 60602 [ACK] Seq=280029 Ack=1 Win=64240 Len=1380
258 0.782000    1438    298070 TCP    60602    1525   10.32.30.12  128.16.4.20  1525 > 60602 [ACK] Seq=281409 Ack=1 Win=64240 Len=1380
259 0.825000      64    298134 TCP    1525     60602  128.16.4.20  10.32.30.12  [TCP ZeroWindow] 60602 > 1525 [ACK] Seq=1 Ack=282789 Win=0
260 1.298999      64    298198 TCP    1525     60602  128.16.4.20  10.32.30.12  [TCP Window Update] 60602 > 1525 [ACK] Seq=1 Ack=282789 Wir
261 1.300000    1438    299636 TCP    60602    1525   10.32.30.12  128.16.4.20  1525 > 60602 [ACK] Seq=282789 Ack=1 Win=64240 Len=1380
```

gearbit
Get it in Gear

How to contact us at gearbit

Ray Tompkins

info09@gearbit.com
www.gearbit.com