SharkFest'17 US

Analysis Visualizations

Robert Bullen
Blue Cross and Blue Shield of Minnesota

SharkFest'17 US • Carnegie Mellon University • June 19-22, 2017

Agenda

Included

- Create firewall latency charts using tshark & Excel
- Show examples of successful visualizations
- Explain the tcptrace chart and view examples

Excluded

- Review Wireshark‘s I/O Graphs

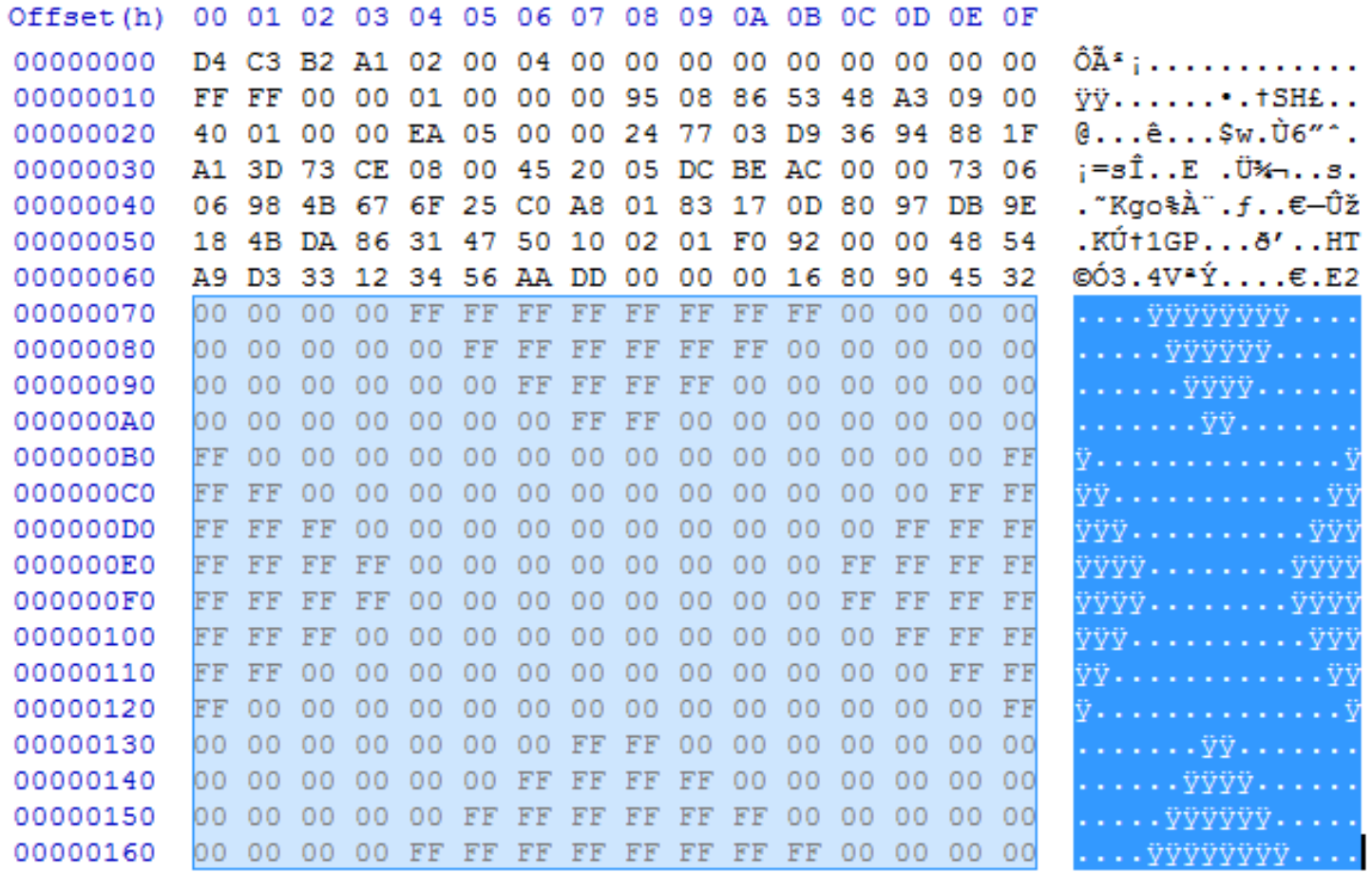
Visualizing Problems Helps An Analyst

- Avoid capturing or mining excessive traffic
- Digest more packets much quicker
- Identify macro patterns and spot anomalies
- Direct (or even avoid) analysis efforts
- Explain the problem to others
- Prove or disprove hypotheses or corrective measures

An Unexpected Visualization

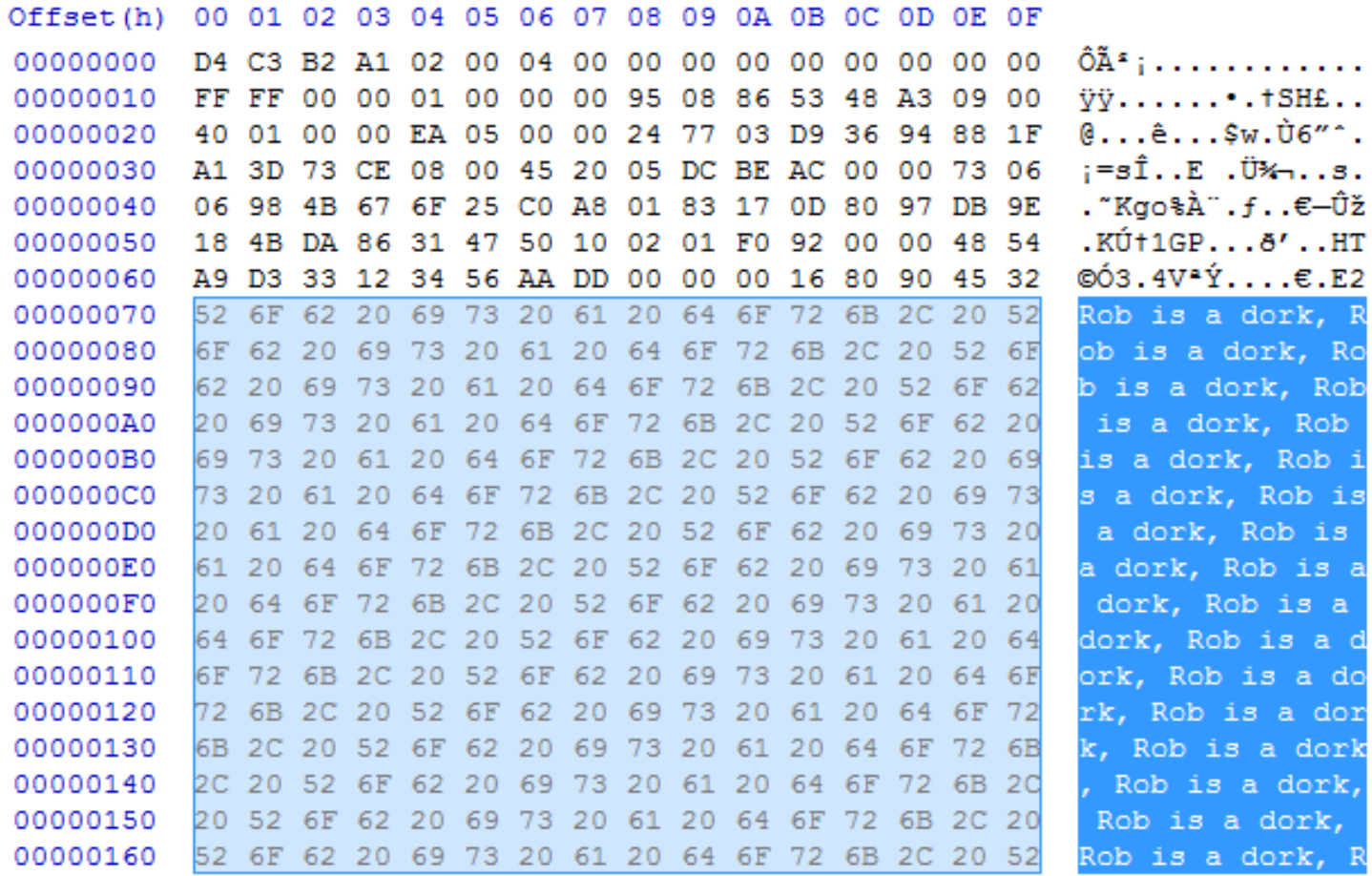
VNC Cursor

A Surprisingly Obvious Packet



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	D4	C3	B2	A1	02	00	04	00	00	00	00	00	00	00	00	00
00000010	FF	FF	00	00	01	00	00	00	95	08	86	53	48	A3	09	00
00000020	40	01	00	00	EA	05	00	00	24	77	03	D9	36	94	88	1F
00000030	A1	3D	73	CE	08	00	45	20	05	DC	BE	AC	00	00	73	06
00000040	06	98	4B	67	6F	25	C0	A8	01	83	17	0D	80	97	DB	9E
00000050	18	4B	DA	86	31	47	50	10	02	01	F0	92	00	00	48	54
00000060	A9	D3	33	12	34	56	AA	DD	00	00	00	16	80	90	45	32
00000070	00	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	00	00	00	00
00000080	00	00	00	00	00	FF	FF	FF	FF	FF	FF	00	00	00	00	00
00000090	00	00	00	00	00	00	FF	FF	FF	FF	00	00	00	00	00	00
000000A0	00	00	00	00	00	00	00	FF	FF	00	00	00	00	00	00	00
000000B0	FF	00	00	00	00	00	00	00	00	00	00	00	00	00	00	FF
000000C0	FF	FF	00	00	00	00	00	00	00	00	00	00	00	00	FF	FF
000000D0	FF	FF	FF	00	00	00	00	00	00	00	00	00	00	FF	FF	FF
000000E0	FF	FF	FF	FF	00	00	00	00	00	00	00	00	FF	FF	FF	FF
000000F0	FF	FF	FF	FF	00	00	00	00	00	00	00	00	FF	FF	FF	FF
00000100	FF	FF	FF	00	00	00	00	00	00	00	00	00	00	FF	FF	FF
00000110	FF	FF	00	00	00	00	00	00	00	00	00	00	00	00	FF	FF
00000120	FF	00	00	00	00	00	00	00	00	00	00	00	00	00	00	FF
00000130	00	00	00	00	00	00	00	FF	FF	00	00	00	00	00	00	00
00000140	00	00	00	00	00	00	FF	FF	FF	FF	00	00	00	00	00	00
00000150	00	00	00	00	00	FF	FF	FF	FF	FF	FF	00	00	00	00	00
00000160	00	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	00	00	00	00

An Alternative Viewpoint

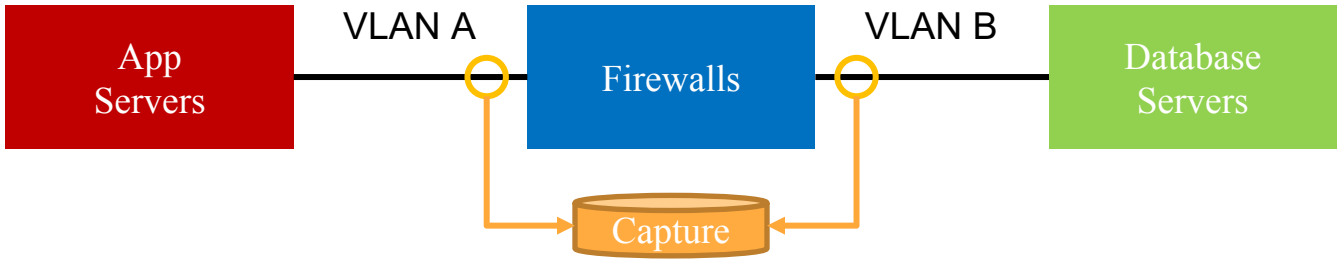


Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	D4	C3	B2	A1	02	00	04	00	00	00	00	00	00	00	00	00	ÔÃ²¡.....
00000010	FF	FF	00	00	01	00	00	00	95	08	86	53	48	A3	09	00	ÿÿ.....•.†SH£..
00000020	40	01	00	00	EA	05	00	00	24	77	03	D9	36	94	88	1F	@...ê...$w.Ù6”ˆ.
00000030	A1	3D	73	CE	08	00	45	20	05	DC	BE	AC	00	00	73	06	¡=sÎ..E .Ü¾¬..s.
00000040	06	98	4B	67	6F	25	C0	A8	01	83	17	0D	80	97	DB	9E	.˜Kgo%À¨.ƒ..€—Ûž
00000050	18	4B	DA	86	31	47	50	10	02	01	F0	92	00	00	48	54	.KÚ†1GP...ð’..HT
00000060	A9	D3	33	12	34	56	AA	DD	00	00	00	16	80	90	45	32	©Ó3.4V²Ý....€.E2
00000070	52	6F	62	20	69	73	20	61	20	64	6F	72	6B	2C	20	52	Rob is a dork, R
00000080	6F	62	20	69	73	20	61	20	64	6F	72	6B	2C	20	52	6F	ob is a dork, Ro
00000090	62	20	69	73	20	61	20	64	6F	72	6B	2C	20	52	6F	62	b is a dork, Rob
000000A0	20	69	73	20	61	20	64	6F	72	6B	2C	20	52	6F	62	20	is a dork, Rob
000000B0	69	73	20	61	20	64	6F	72	6B	2C	20	52	6F	62	20	69	is a dork, Rob i
000000C0	73	20	61	20	64	6F	72	6B	2C	20	52	6F	62	20	69	73	s a dork, Rob is
000000D0	20	61	20	64	6F	72	6B	2C	20	52	6F	62	20	69	73	20	a dork, Rob is
000000E0	61	20	64	6F	72	6B	2C	20	52	6F	62	20	69	73	20	61	a dork, Rob is a
000000F0	20	64	6F	72	6B	2C	20	52	6F	62	20	69	73	20	61	20	dork, Rob is a
00000100	64	6F	72	6B	2C	20	52	6F	62	20	69	73	20	61	20	64	dork, Rob is a d
00000110	6F	72	6B	2C	20	52	6F	62	20	69	73	20	61	20	64	6F	ork, Rob is a do
00000120	72	6B	2C	20	52	6F	62	20	69	73	20	61	20	64	6F	72	rk, Rob is a dor
00000130	6B	2C	20	52	6F	62	20	69	73	20	61	20	64	6F	72	6B	k, Rob is a dork
00000140	2C	20	52	6F	62	20	69	73	20	61	20	64	6F	72	6B	2C	, Rob is a dork,
00000150	20	52	6F	62	20	69	73	20	61	20	64	6F	72	6B	2C	20	Rob is a dork,
00000160	52	6F	62	20	69	73	20	61	20	64	6F	72	6B	2C	20	52	Rob is a dork, R

Firewall Latency Charts

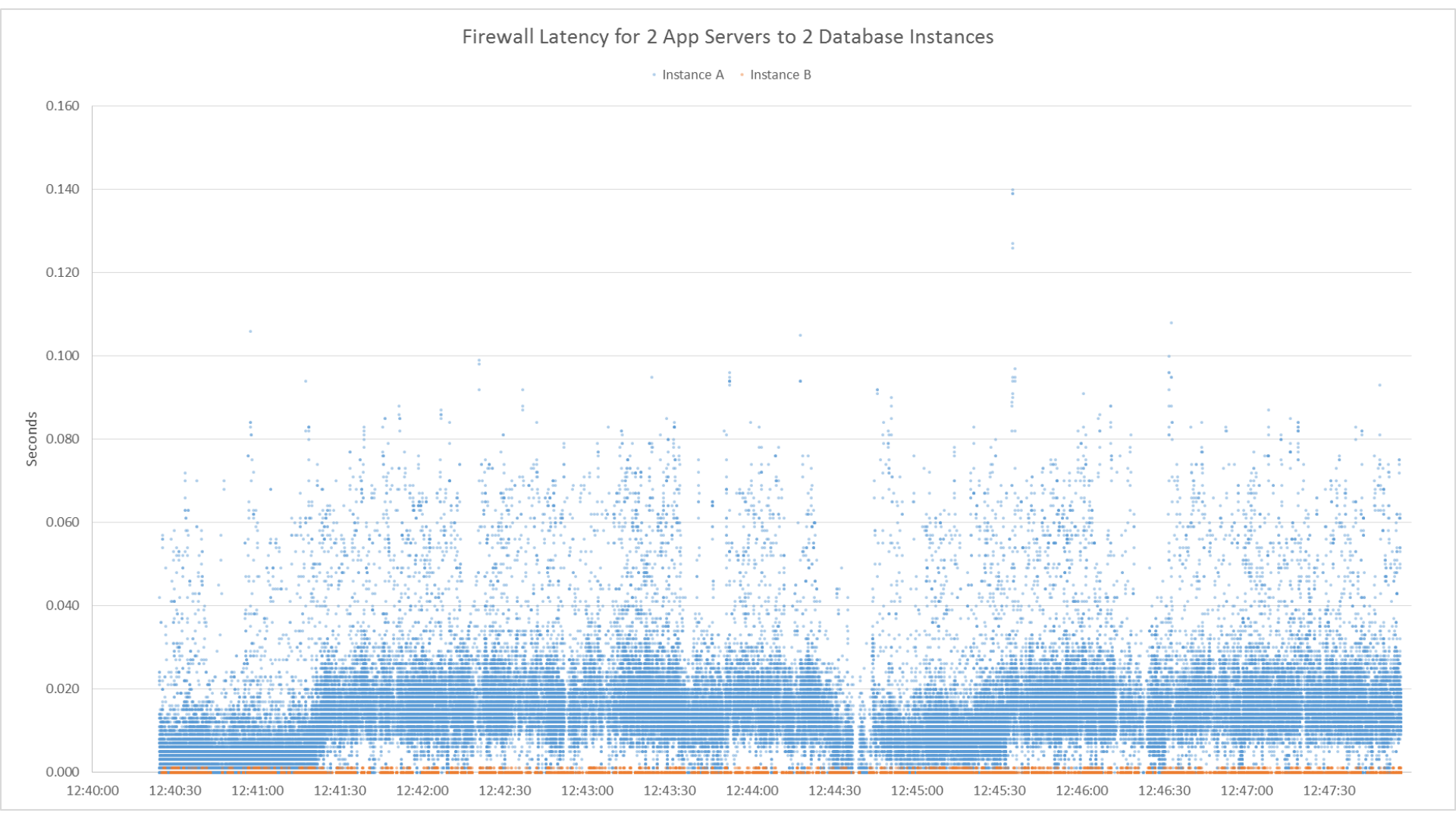
The Situation

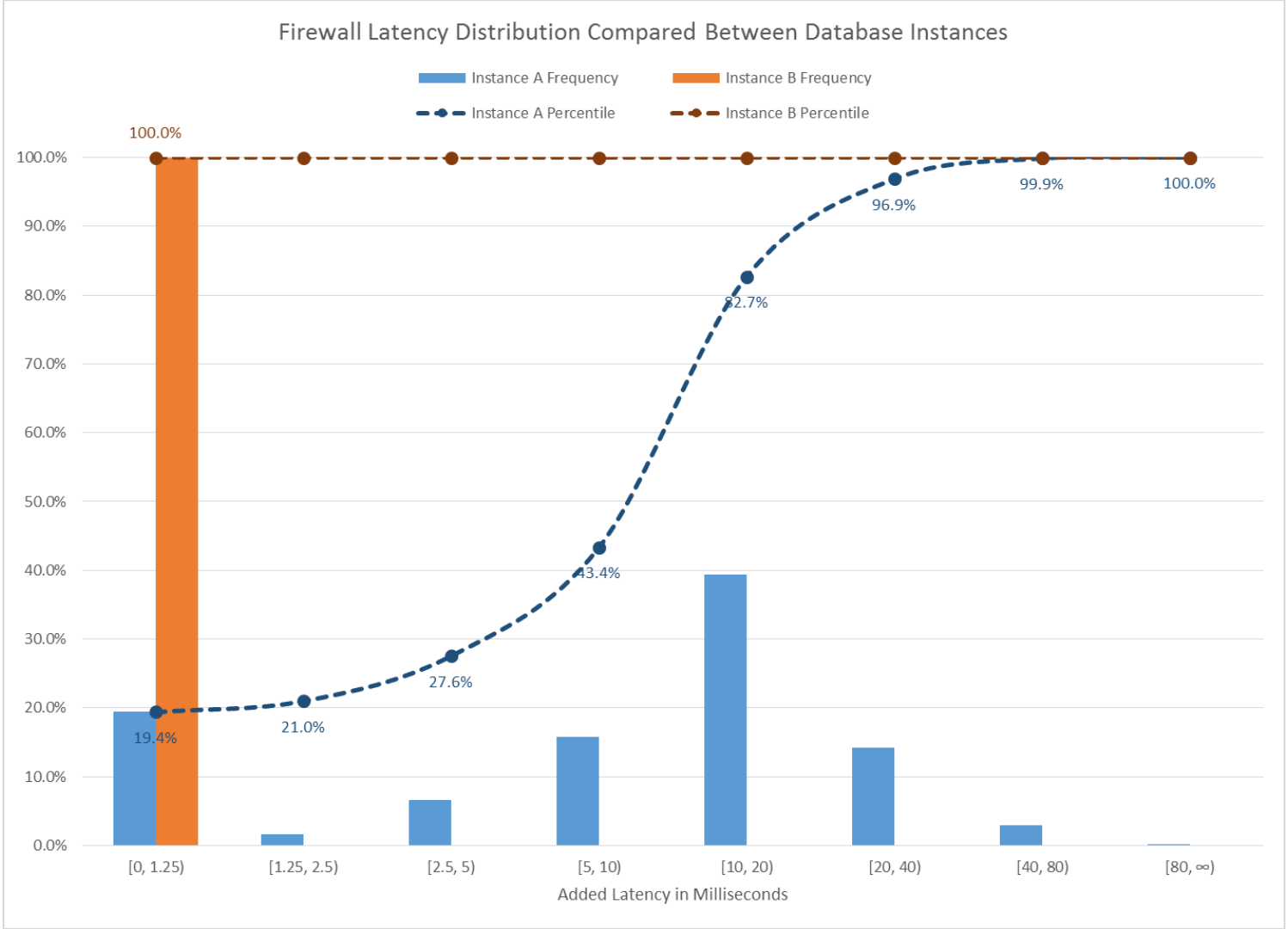
- App server to database queries slowed to a crawl
- App server and database tiers are in their own VRFs separated by firewalls
- Firewall team reported no recent changes had been applied

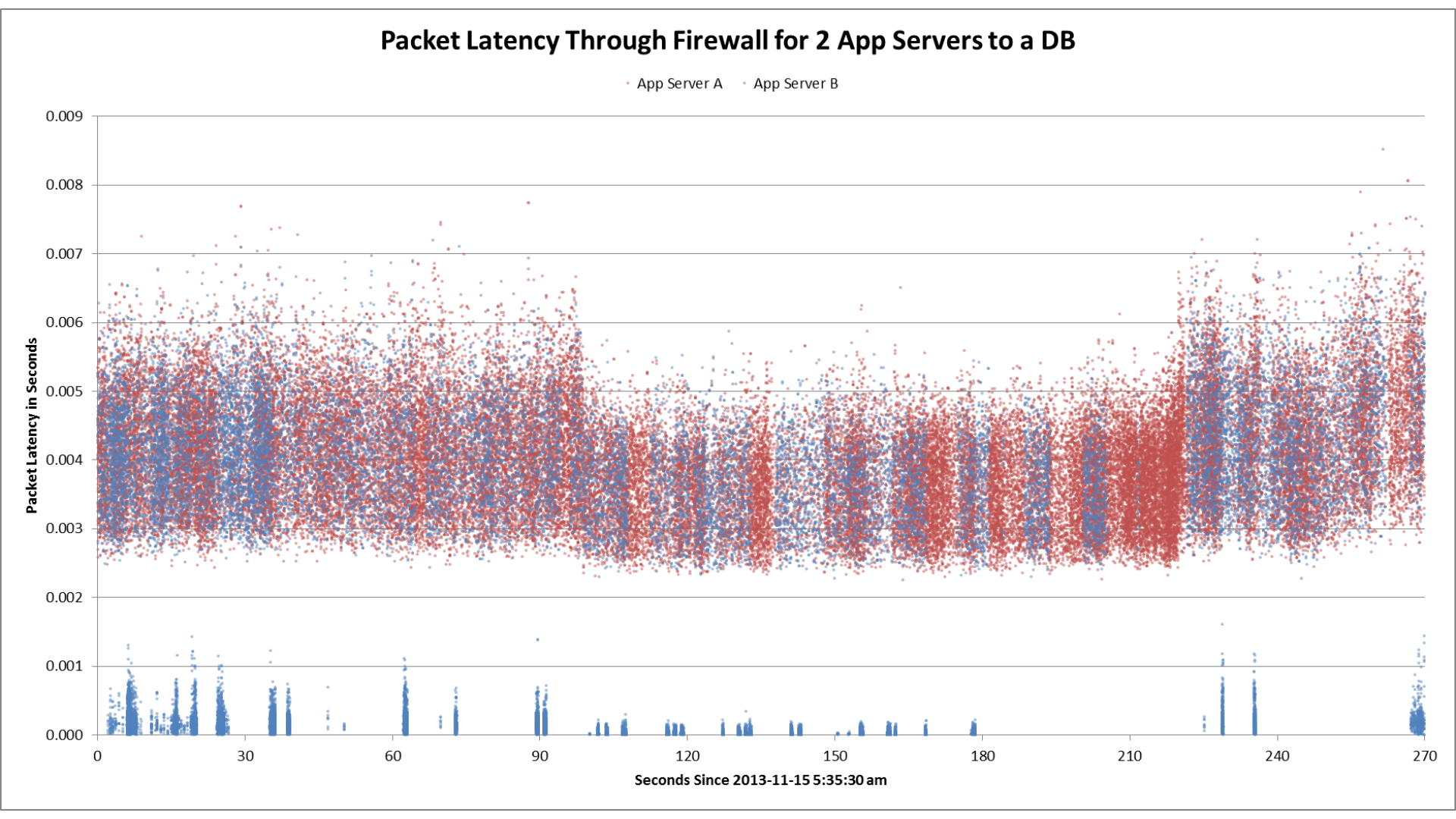


Demo

```
#!/usr/bin/env bash

INPUT_FILE='Firewall Latency.pcapng'
OUTPUT_FILE='Firewall Latency.csv'

if [[ ! -f "${OUTPUT_FILE}" ]]; then

    # Output the trace file's packet count and capture duration.
    echo
    capinfos -c -u "${INPUT_FILE}"
    echo

    # Process the trace file.
    echo -n "Processing '${INPUT_FILE}' to '${OUTPUT_FILE}'..."
    tshark -r "${INPUT_FILE}"\
        -T fields -E header=yes\
        -e frame.number -e frame.time_relative -e ip.id -e tcp.seq\
        -o tcp.relative_sequence_numbers:FALSE\
        > "${OUTPUT_FILE}"
    echo "done."
    echo

else

    echo
    echo "'${OUTPUT_FILE}' already exists"
    echo

fi
```


Firewall Latency for 2 App Servers to 2 Database Instances
Instance A
Instance B
Seconds
0.160
0.140
0.120
0.100
0.080
0.060
0.040
0.020
0.000
12:40:00
12:40:30
12:41:00
12:41:30
12:42:00
12:42:30
12:43:00
12:43:30
12:44:00
12:44:30
12:45:00
12:45:30
12:46:00
12:46:30
12:47:00
12:47:30


Firewall Latency Distribution Compared Between Database Instances
Instance A Frequency
Instance B Frequency
Instance A Percentile
Instance B Percentile
100.0%
100.0%
90.0%
80.0%
70.0%
60.0%
50.0%
40.0%
30.0%
20.0%
10.0%
0.0%
19.4%
21.0%
27.6%
43.4%
72.7%
96.9%
99.9%
100.0%
[0, 1.25)
[1.25, 2.5)
[2.5, 5)
[5, 10)
[10, 20)
[20, 40)
[40, 80)
[80, ∞)
Added Latency in Milliseconds


Packet Latency Through Firewall for 2 App Servers to a DB
App Server A
App Server B
0.009
0.008
0.007
0.006
0.005
0.004
0.003
0.002
0.001
0.000
Packet Latency in Seconds
0
30
60
90
120
150
180
210
240
270
Seconds Since 2013-11-15 5:35:30 am

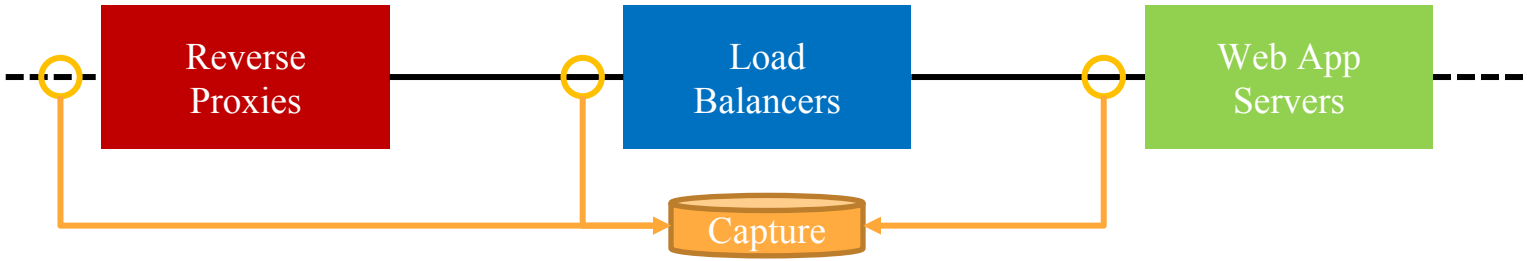
Visualization Accomplishments

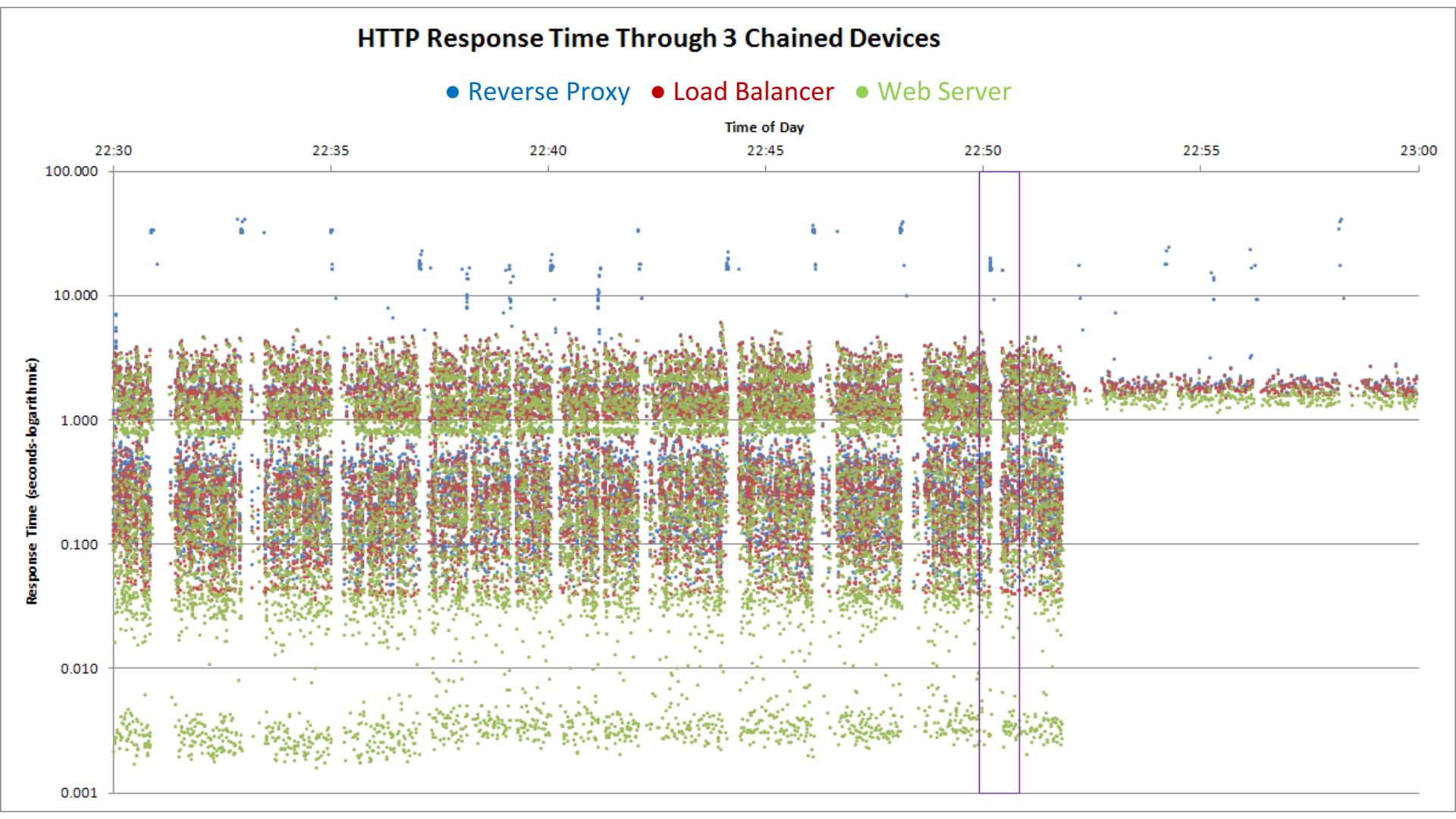
- ✓ Avoid capturing or mining excessive traffic
- ✓ Digest more packets much quicker
- ✓ Identify macro patterns and spot anomalies
- ✓ Direct or avoid analysis efforts
- ✓ Explain the problem to others
- ✓ Prove or disprove hypotheses or corrective measures

Web App Load Testing Performance Problem

The Situation

- Load testing a web application revealed mostly good performance but a small percentage of abysmal response times not specific to any particular operation.
- Web app server logs showed acceptable performance at all times for all operations
- The infrastructure consisted of two sets of appliances in front of the servers:




HTTP Response Time Through 3 Chained Devices
Reverse Proxy
Load Balancer
Web Server
Time of Day
22:30
22:35
22:40
22:45
22:50
22:55
23:00
100.000
10.000
1.000
0.100
0.010
0.001
Response Time (seconds-logarithmic)

Example

```
#!/usr/bin/env bash

INPUT_FILE='Load Test.pcapng'
OUTPUT_FILE='Load Test.csv'

if [[ ! -f "${OUTPUT_FILE}" ]]; then

    # Process the trace file.
    echo -n "Processing '${INPUT_FILE}' to '${OUTPUT_FILE}'..."
    tshark -r "${INPUT_FILE}"\
        -Y 'http.time'
        -T fields -E header=yes\
        -e frame.number -e frame.time_relative -e ip.src -e http.time\
        > "${OUTPUT_FILE}"
    echo "done."
    echo

else

    echo
    echo "'${OUTPUT_FILE}' already exists"
    echo

fi
```

Visualization Accomplishments

- ❑ Avoid capturing or mining excessive traffic
- ✓ Digest more packets much quicker
- ✓ Identify macro patterns and spot anomalies
- ✓ Direct or avoid analysis efforts
- ✓ Explain the problem to others
- ❑ Prove or disprove hypotheses or corrective measures

Check Keying Station Image Load Delays

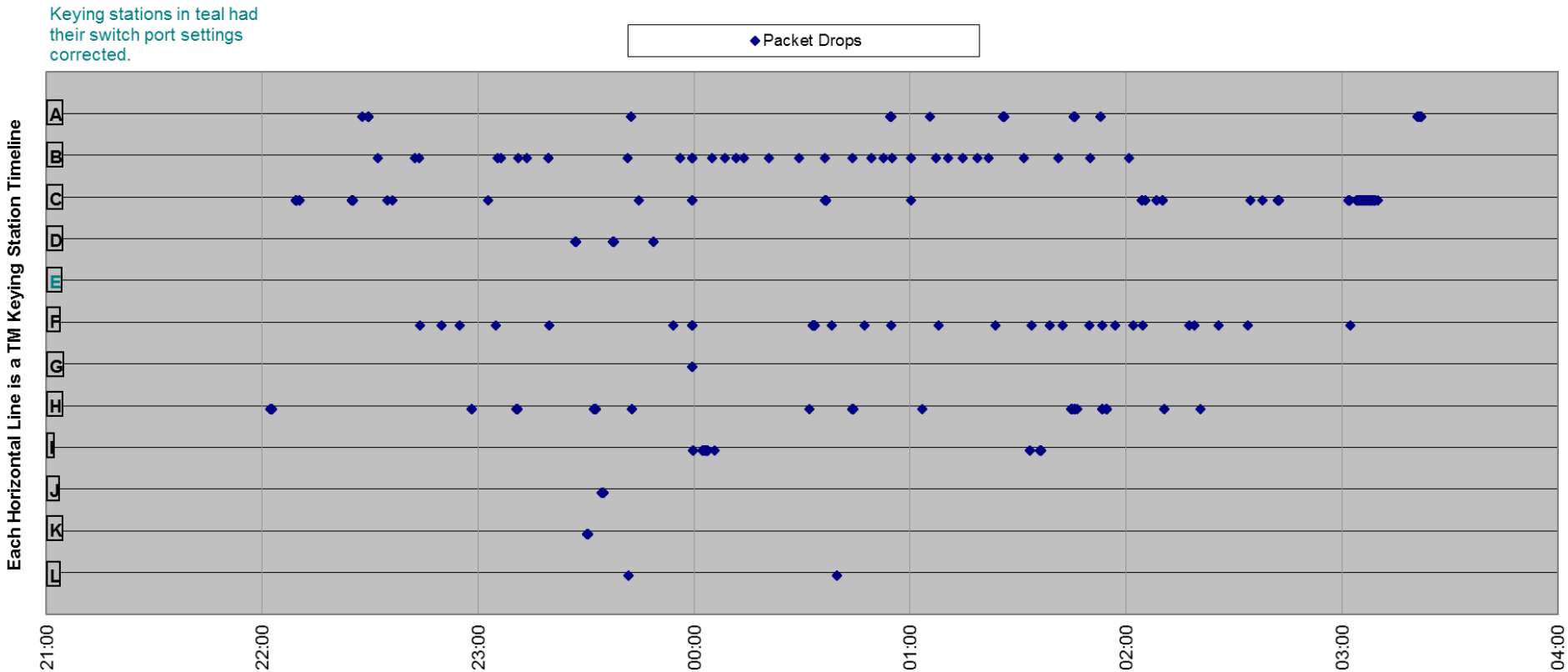
The Situation

- For bank checks that aren't machine readable, operators review check images and manually key in data
- Operators were reporting occasional image load delays that slow down their performance, which in turn impacts their department's metrics and individuals' compensation

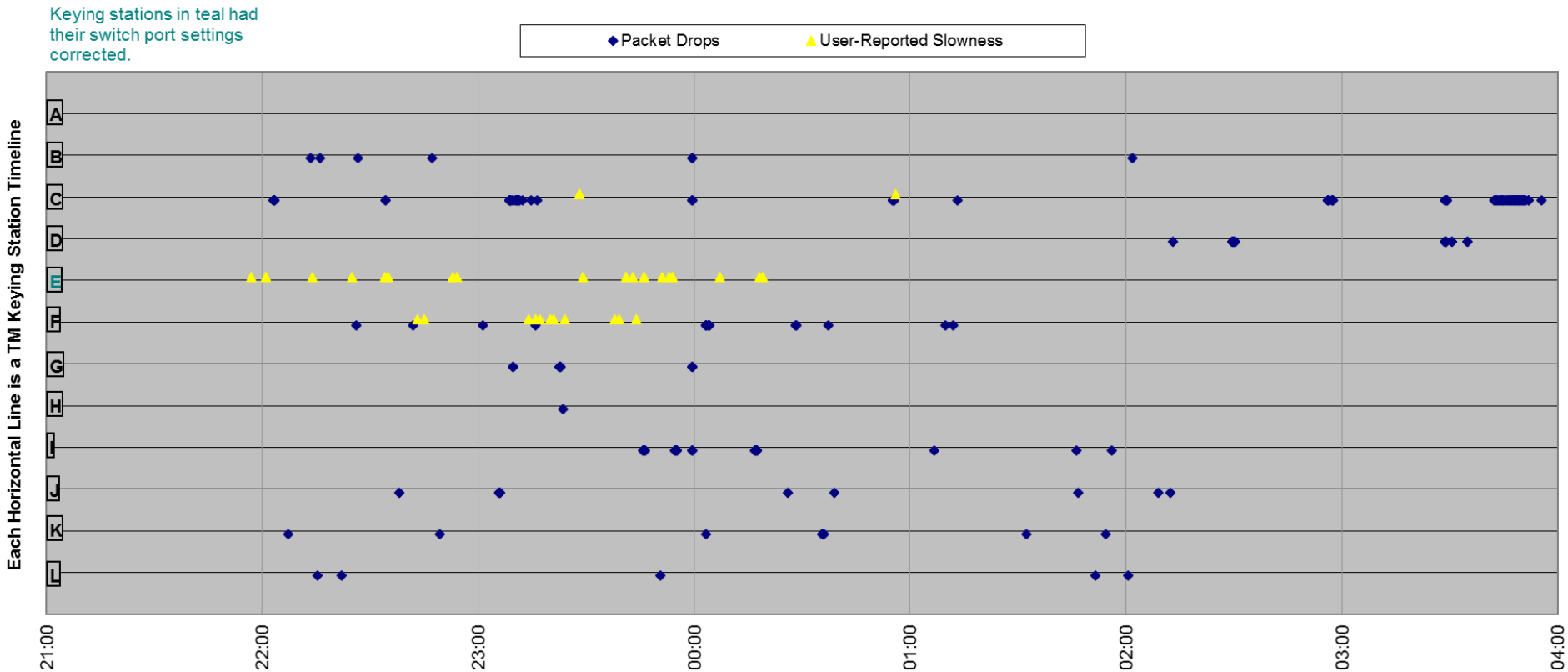
The Challenges

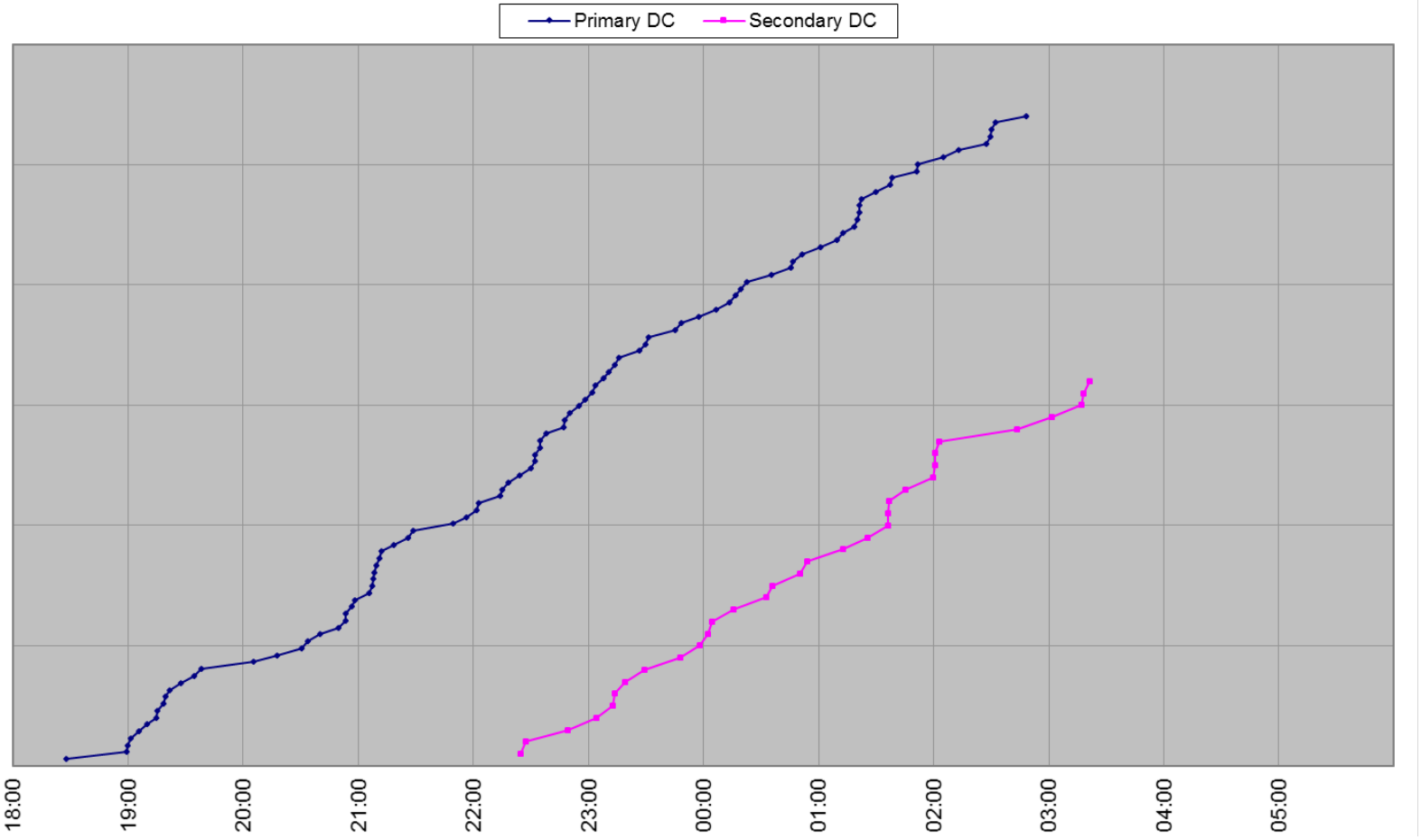
- Tickets are created when slowdowns are reported, but without helpful analysis information like accurate timings—**Packet mining timeline guesswork**
- There are two keying station sites geographically separated from the application & image servers, meaning that separate captures must be taken in at least two of the three locations—**Multi-point capture correlation with differing timestamps**
- Operator-to-app server assignment is non-deterministic, and images are spread across many image servers, which is also non-deterministic—**Don't know what mining filters to provide until after starting to look at packets**
- The protocol is proprietary, so no decodes—**Looking at packets just got a lot harder**

Timelines of Keying Station Packet Drops

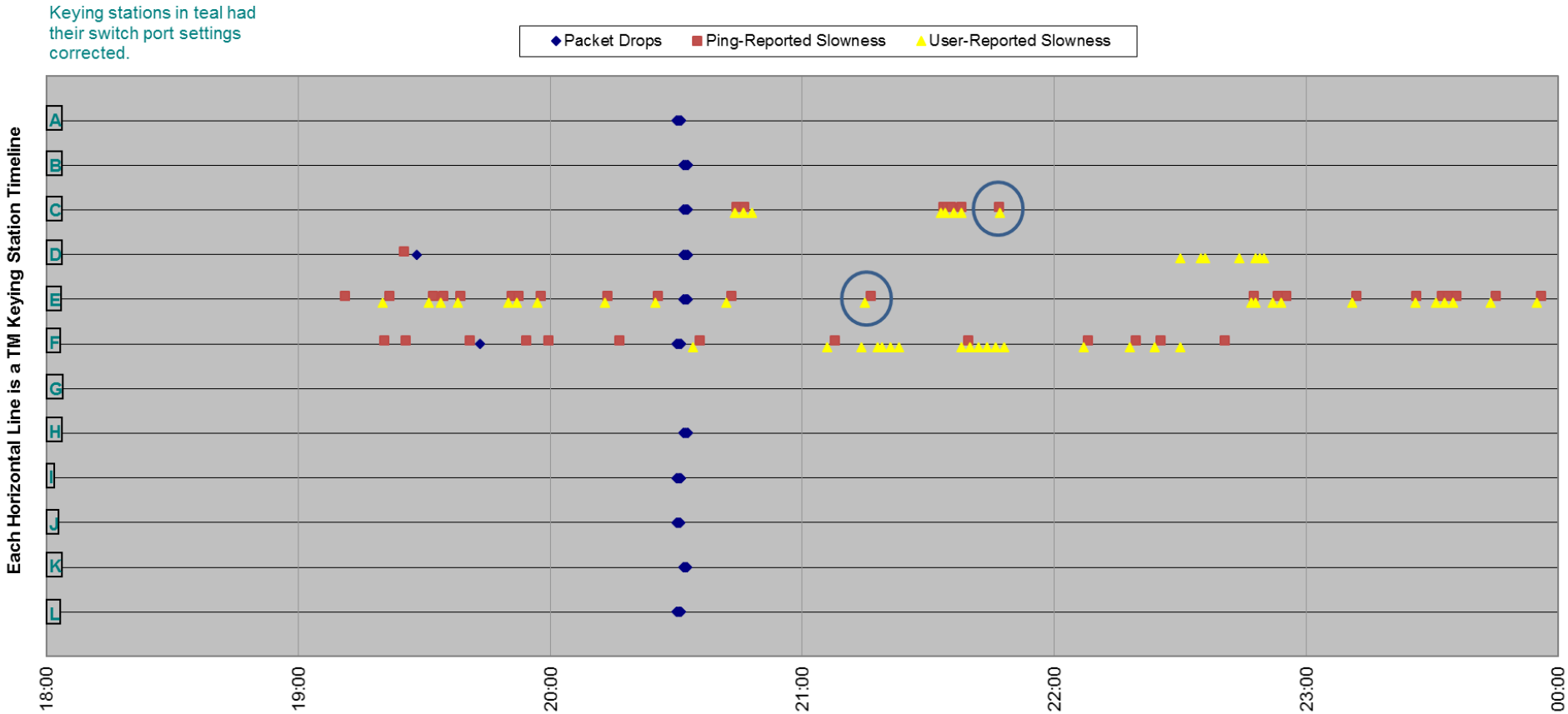


Timelines of Keying Station Packet Drops and User-Reported Slowness




Reports of Keying Station Slowness over Time by Data Center
Primary DC
Secondary DC
18:00
19:00
20:00
21:00
22:00
23:00
00:00
01:00
02:00
03:00
04:00
05:00

Timelines of Keying Station Packet Drops and Reported Slowness



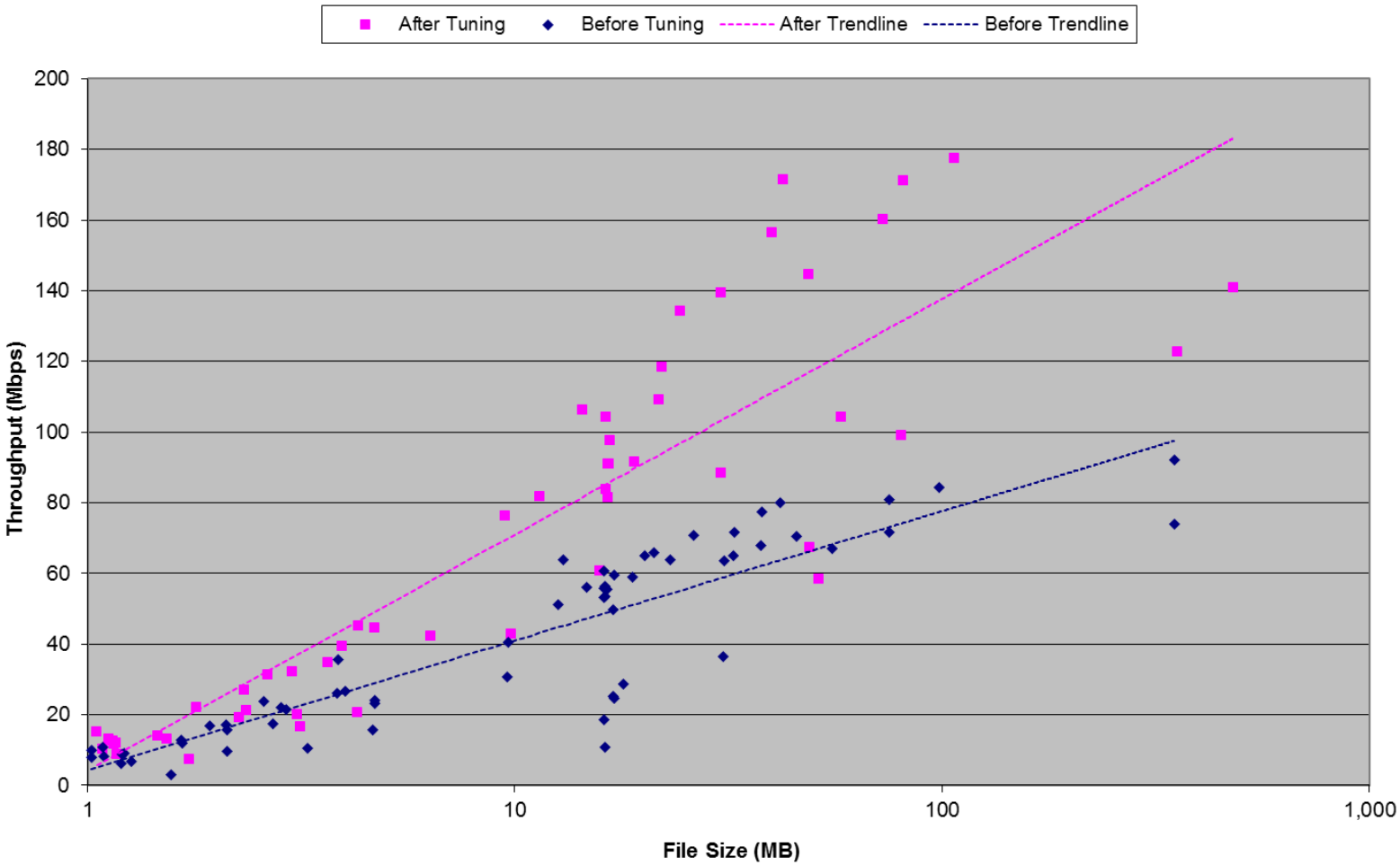
Visualization Accomplishments

- ✓ Avoid capturing or mining excessive traffic
- ✓ Digest more packets much quicker
- ✓ Identify macro patterns and spot anomalies
- ✓ Direct or avoid analysis efforts
- ✓ Explain the problem to others
- ✓ Prove or disprove hypotheses or corrective measures

File Transfer Tuning Validation

The Situation

- We recommended increasing TCP window sizes to improve file transfer throughput
- Did it work?


Comparison of File Transfer Performance Before and After Tuning
After Tuning
Before Tuning
After Trendline
Before Trendline
Throughput (Mbps)
200
180
160
140
120
100
80
60
40
20
0
1
10
100
1,000
File Size (MB)

Visualization Accomplishments

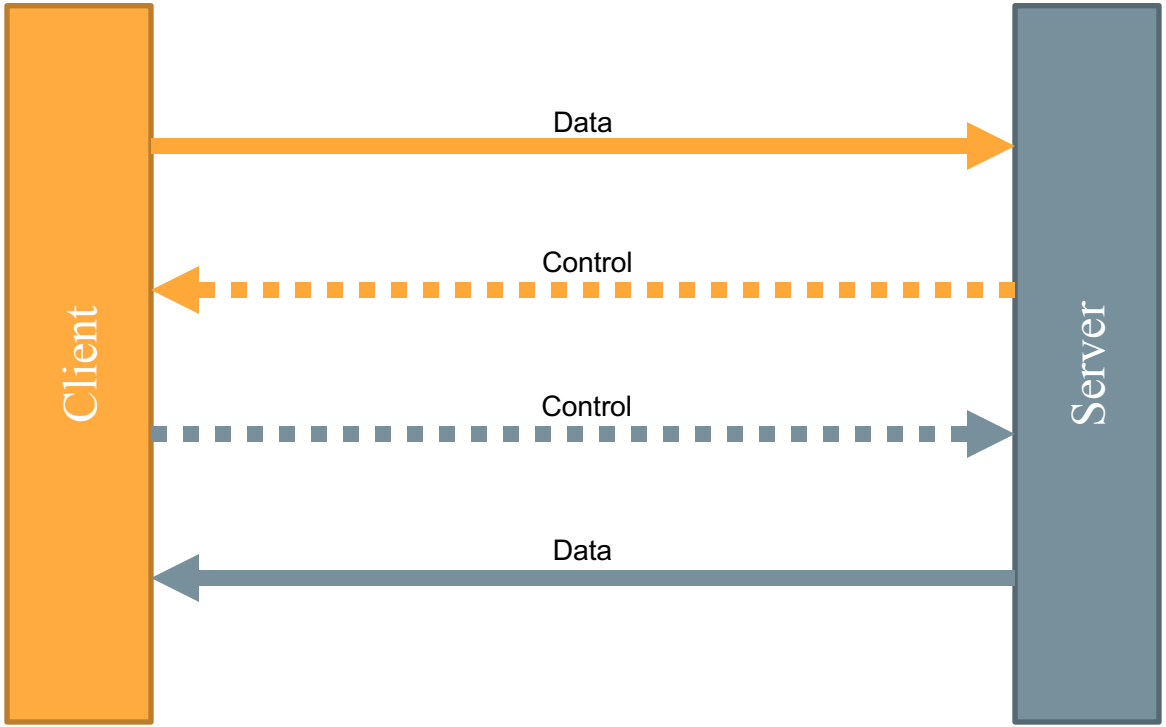
- ✓ Avoid capturing or mining excessive traffic
- ❑ Digest more packets much quicker
- ✓ Identify macro patterns and spot anomalies
- ✓ Direct or avoid analysis efforts
- ✓ Explain the problem to others
- ✓ Prove or disprove hypotheses or corrective measures

Introducing tcptrace

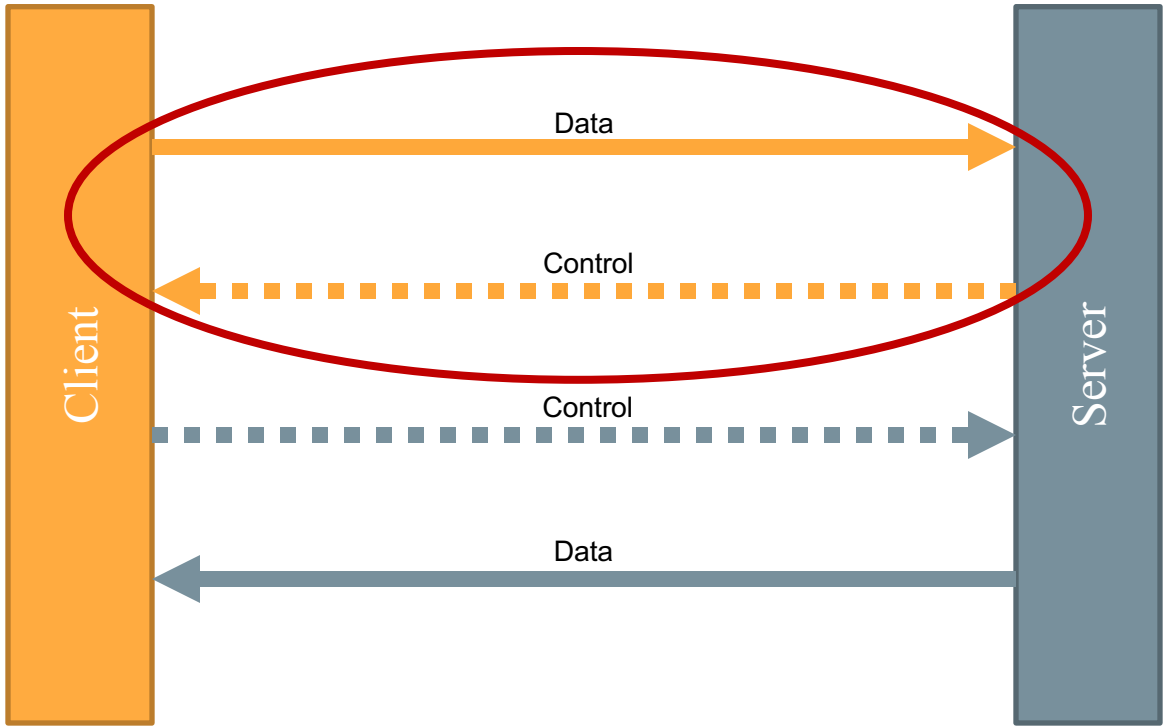
tcptrace

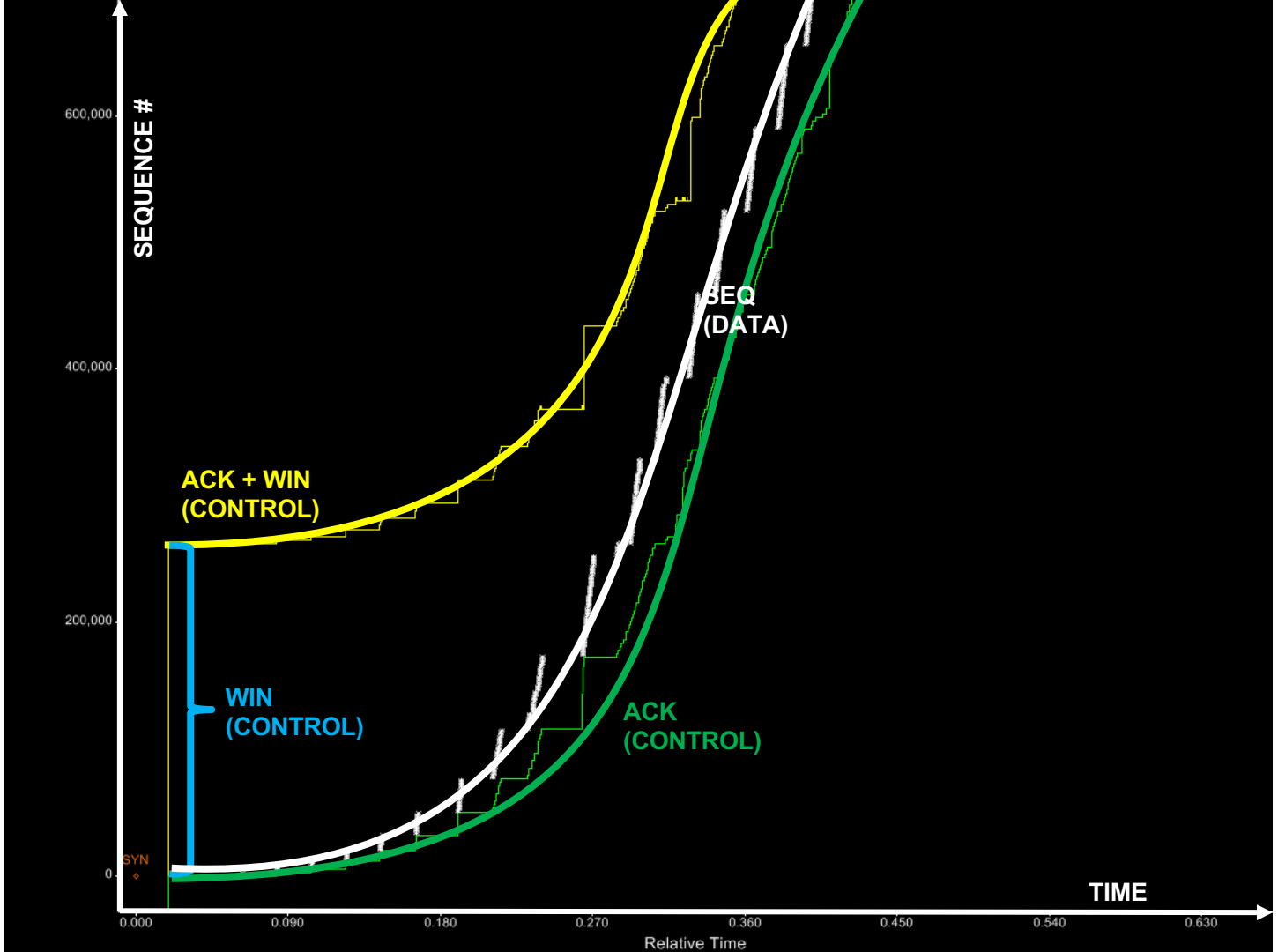
- http://www.tcptrace.org—"*tcptrace* is a tool written by Shawn Ostermann at Ohio University, for analysis of [packet capture] files."
- tcptrace creates a variety of charts, many of which are also implemented in Wireshark's Statistics | TCP Stream Graphs menu.
- The Time Sequence chart is by far the coolest (IMHO), and is oftentimes termed a tcptrace chart.

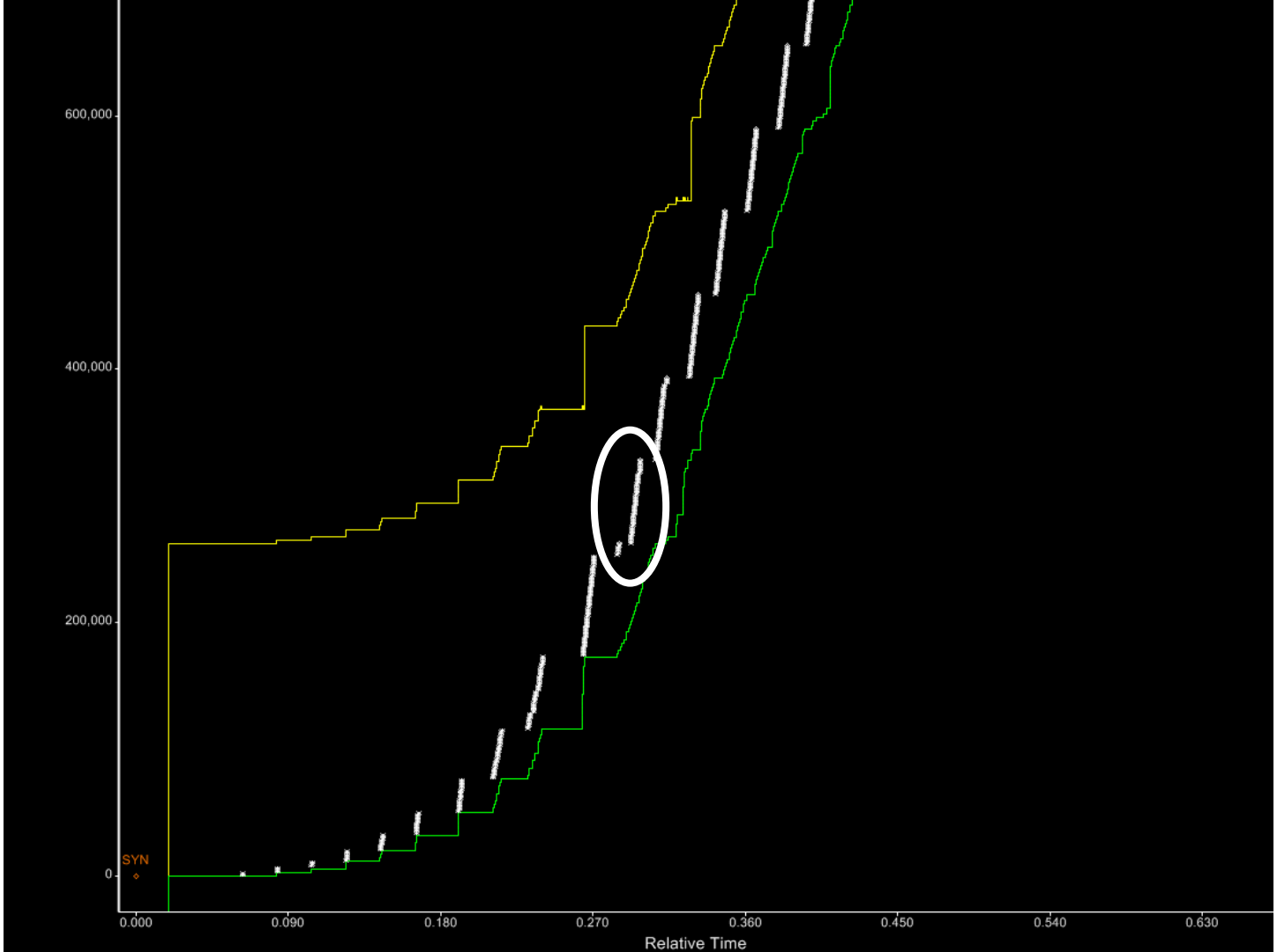
TCP Bidirectionality

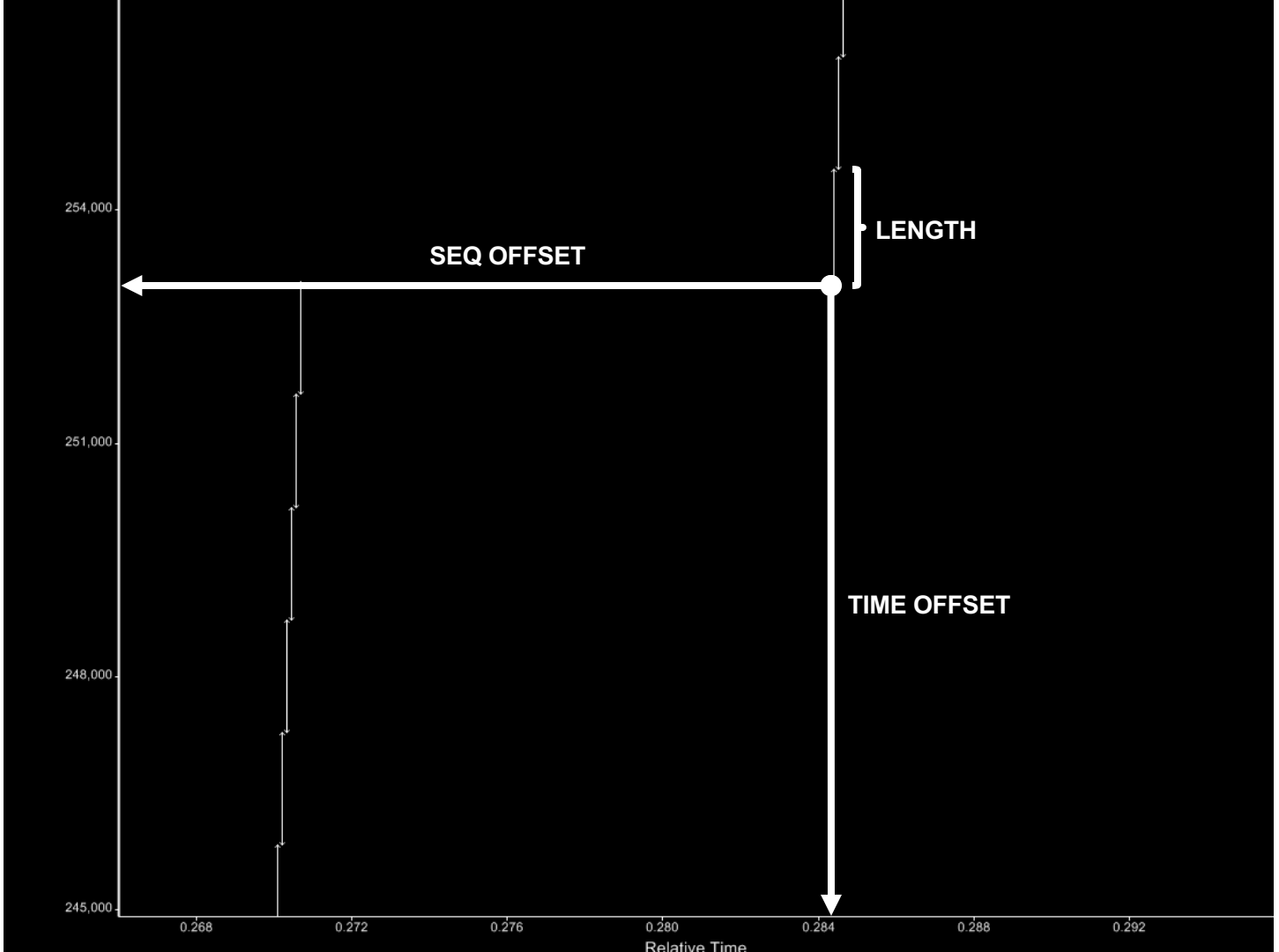


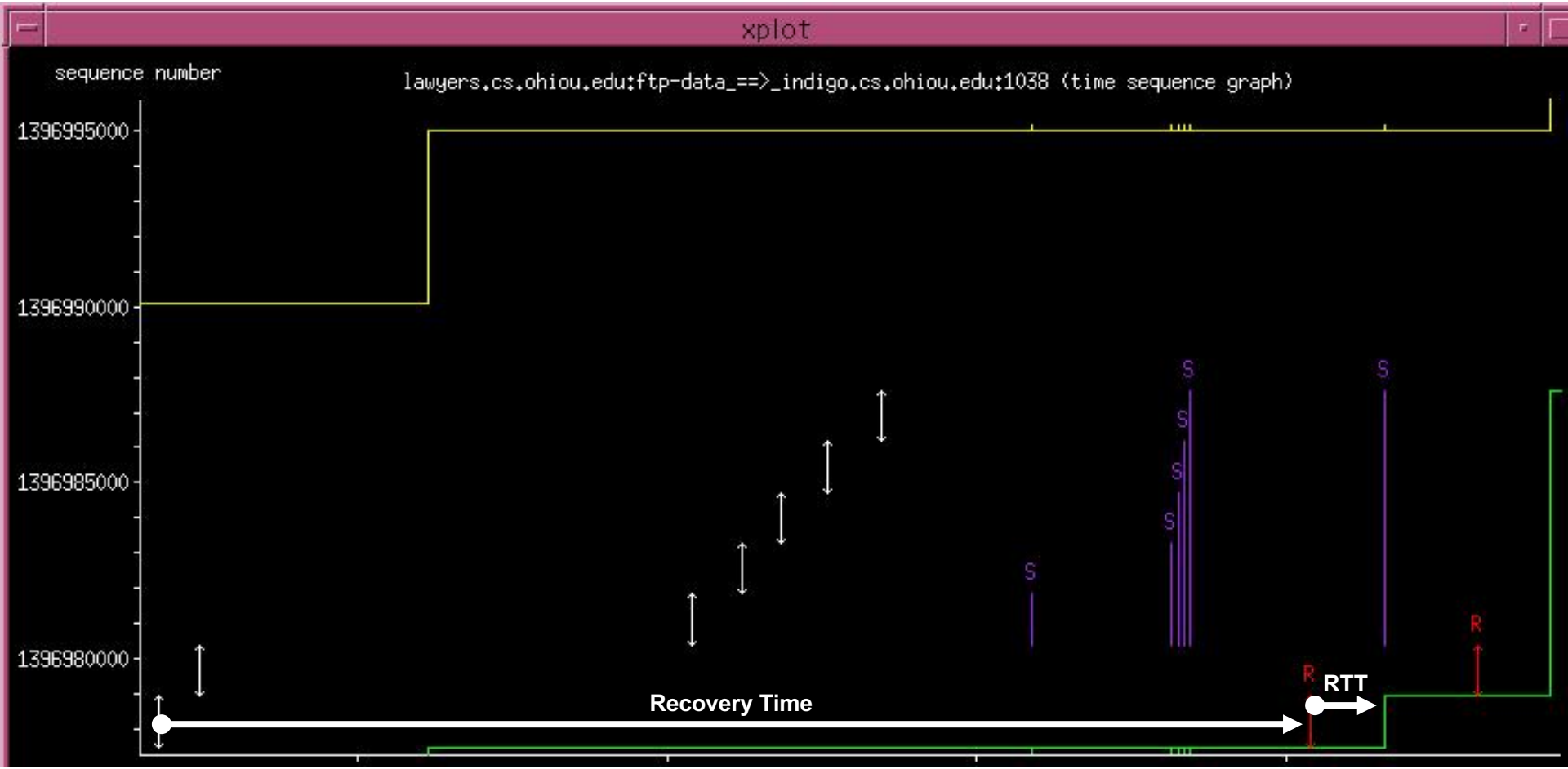
tcptrace is a Unidirectional Visualization

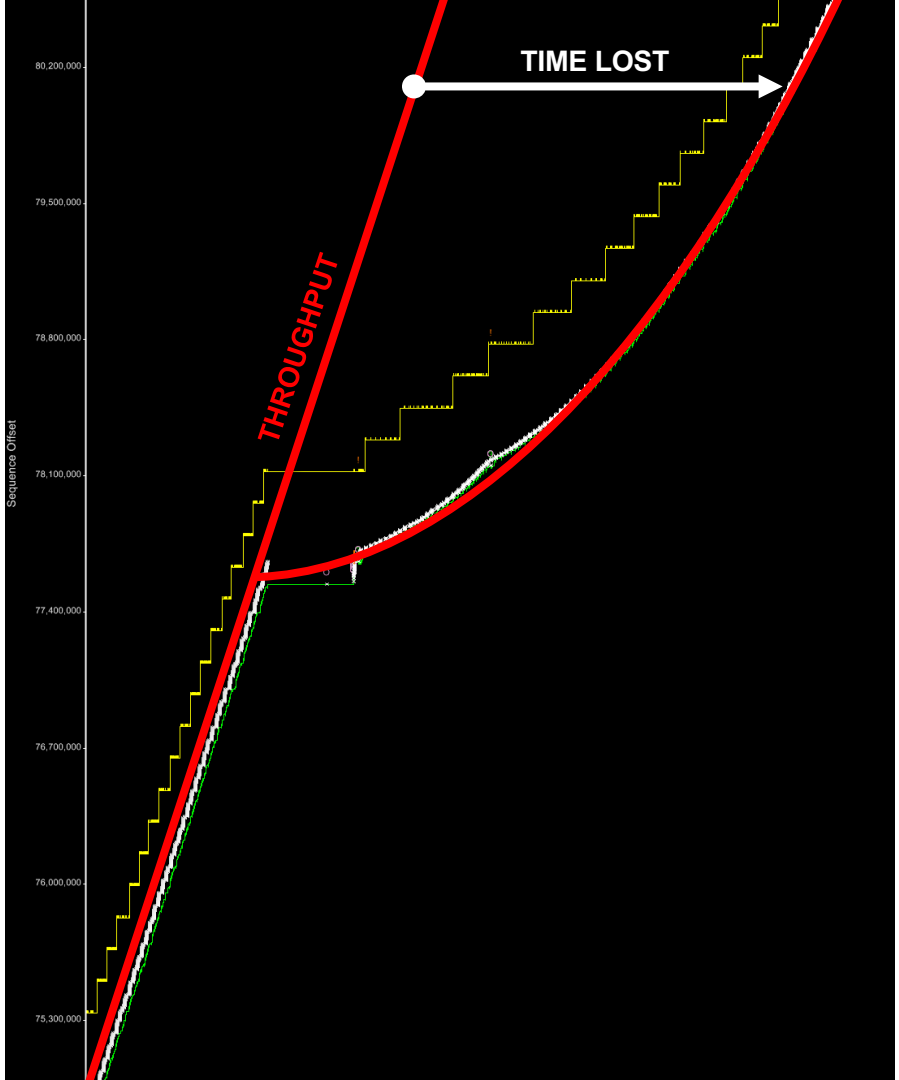



SEQUENCE #
600,000
400,000
200,000
0
SYN
ACK + WIN
(CONTROL)
WIN
(CONTROL)
SEQ
(DATA)
ACK
(CONTROL)
TIME
0.000
0.090
0.180
0.270
0.360
0.450
0.540
0.630
Relative Time


600,000
400,000
200,000
0
SYN
0.000
0.090
0.180
0.270
0.360
0.450
0.540
0.630
Relative Time


254,000
251,000
248,000
245,000
SEQ OFFSET
LENGTH
TIME OFFSET
0.268
0.272
0.276
0.280
0.284
0.288
0.292
Relative Time

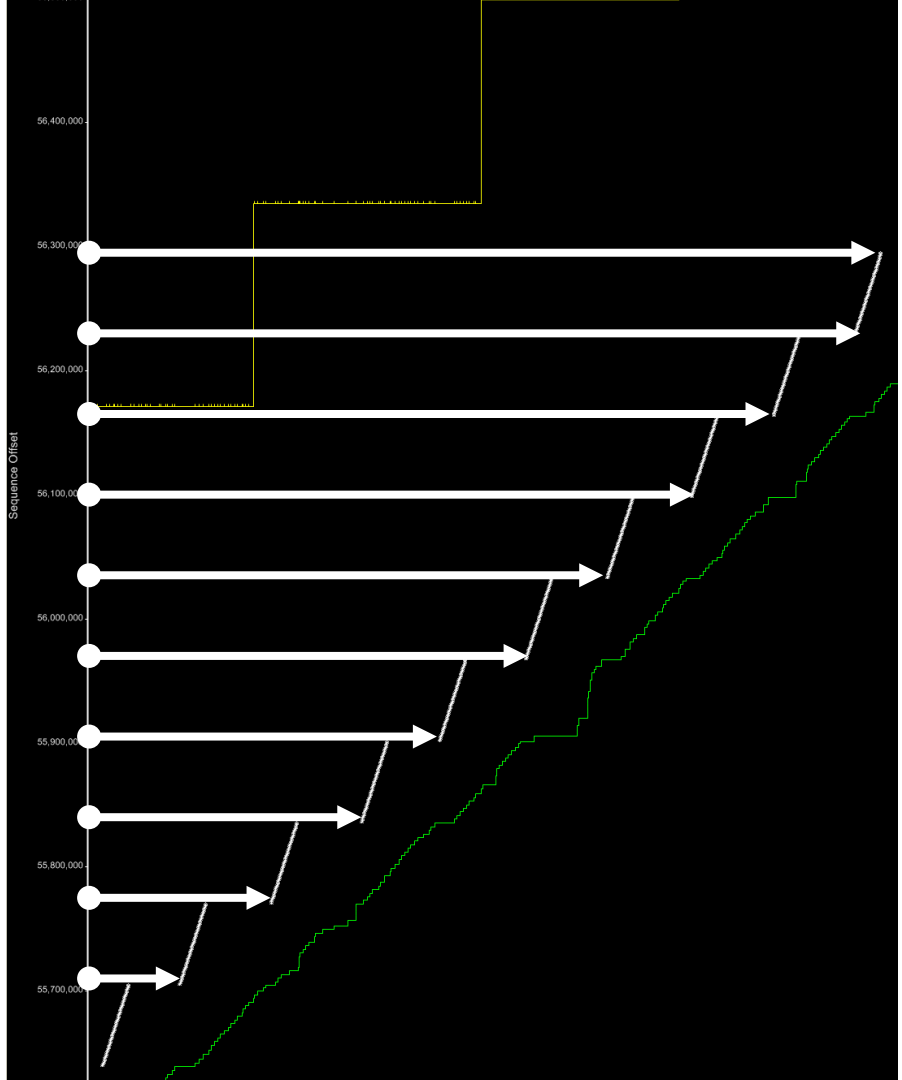

xplot
sequence number
lawyers.cs.ohiou.edu:ftp-data_==>_indigo.cs.ohiou.edu:1038 (time sequence graph)
1396995000
1396990000
1396985000
1396980000
S
S
S
S
S
S
R
R
RTT
Recovery Time

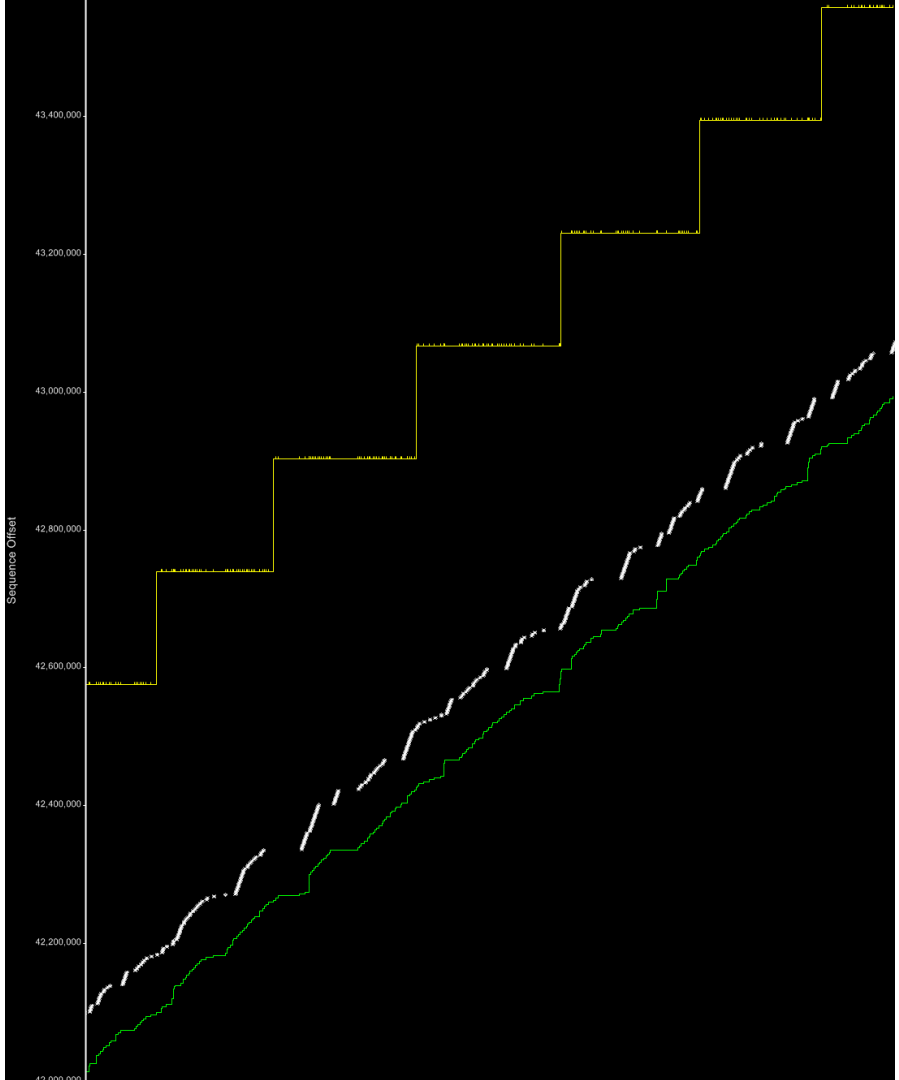

TIME LOST
THROUGHPUT
Sequence Offset
80,200,000
79,500,000
78,800,000
78,100,000
77,400,000
76,700,000
76,000,000
75,300,000

FTP File Transfer
Realizing Poor Throughput

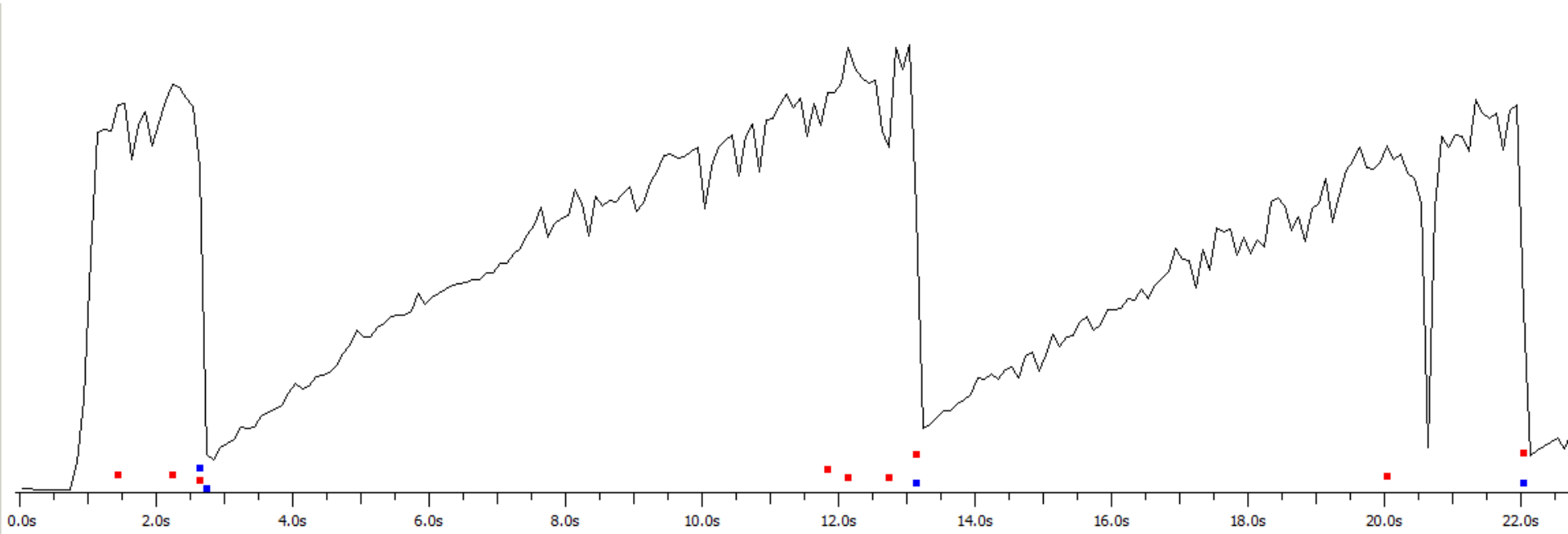
Packet	Source	Destination	Size	Absolute Time	Delta Time	Protocol	Summary	Expe
1	10.42.232.217	192.168.125.65	1518	15:45:05.669427000		FTP Data	Src= 2859,Dst= 20,.A....,S=3701143293,L= 1448,A=2240505265,W=65535	
2	10.42.232.217	192.168.125.65	1518	15:45:05.669550000	0.000123000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701144741,L= 1448,A=2240505265,W=65535	
3	192.168.125.65	10.42.232.217	70	15:45:05.669632000	0.000082000	FTP Data	Src= 20,Dst= 2859,.A....,S=2240505265,L= 0,A=3701070518,W=16996	
4	10.42.232.217	192.168.125.65	1518	15:45:05.669673000	0.000041000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701146189,L= 1448,A=2240505265,W=65535	
5	10.42.232.217	192.168.125.65	1518	15:45:05.669796000	0.000123000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701147637,L= 1448,A=2240505265,W=65535	
6	10.42.232.217	192.168.125.65	1518	15:45:05.669919000	0.000123000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701149085,L= 1448,A=2240505265,W=65535	
7	10.42.232.217	192.168.125.65	1518	15:45:05.670043000	0.000124000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701150533,L= 1448,A=2240505265,W=65535	
8	10.42.232.217	192.168.125.65	1518	15:45:05.670165000	0.000122000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701151981,L= 1448,A=2240505265,W=65535	
9	10.42.232.217	192.168.125.65	1518	15:45:05.670288000	0.000123000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701153429,L= 1448,A=2240505265,W=65535	
10	192.168.125.65	10.42.232.217	70	15:45:05.670328000	0.000040000	FTP Data	Src= 20,Dst= 2859,.A....,S=2240505265,L= 0,A=3701073414,W=16906	
11	10.42.232.217	192.168.125.65	1518	15:45:05.670411000	0.000083000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701154877,L= 1448,A=2240505265,W=65535	
12	10.42.232.217	192.168.125.65	1518	15:45:05.670534000	0.000123000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701156325,L= 1448,A=2240505265,W=65535	
13	10.42.232.217	192.168.125.65	1518	15:45:05.670658000	0.000124000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701157773,L= 1448,A=2240505265,W=65535	
14	10.42.232.217	192.168.125.65	1518	15:45:05.670780000	0.000122000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701159221,L= 1448,A=2240505265,W=65535	
15	192.168.125.65	10.42.232.217	70	15:45:05.670897000	0.000117000	FTP Data	Src= 20,Dst= 2859,.A....,S=2240505265,L= 0,A=3701076310,W=16815	
16	10.42.232.217	192.168.125.65	1518	15:45:05.670903000	0.000006000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701160669,L= 1448,A=2240505265,W=65535	
17	10.42.232.217	192.168.125.65	1518	15:45:05.671026000	0.000123000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701162117,L= 1448,A=2240505265,W=65535	
18	10.42.232.217	192.168.125.65	1518	15:45:05.671149000	0.000123000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701163565,L= 1448,A=2240505265,W=65535	
19	10.42.232.217	192.168.125.65	1518	15:45:05.671273000	0.000124000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701165013,L= 1448,A=2240505265,W=65535	
20	10.42.232.217	192.168.125.65	1518	15:45:05.671396000	0.000123000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701166461,L= 1448,A=2240505265,W=65535	
21	10.42.232.217	192.168.125.65	1518	15:45:05.671518000	0.000122000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701167909,L= 1448,A=2240505265,W=65535	
22	192.168.125.65	10.42.232.217	70	15:45:05.671570000	0.000052000	FTP Data	Src= 20,Dst= 2859,.A....,S=2240505265,L= 0,A=3701079206,W=16725	
23	10.42.232.217	192.168.125.65	1518	15:45:05.671642000	0.000072000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701169357,L= 1448,A=2240505265,W=65535	
24	10.42.232.217	192.168.125.65	1518	15:45:05.671765000	0.000123000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701170805,L= 1448,A=2240505265,W=65535	
25	10.42.232.217	192.168.125.65	1518	15:45:05.671888000	0.000123000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701172253,L= 1448,A=2240505265,W=65535	
26	10.42.232.217	192.168.125.65	1518	15:45:05.672011000	0.000123000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701173701,L= 1448,A=2240505265,W=65535	
27	10.42.232.217	192.168.125.65	1518	15:45:05.672134000	0.000123000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701175149,L= 1448,A=2240505265,W=65535	
28	10.42.232.217	192.168.125.65	1518	15:45:05.672257000	0.000123000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701176597,L= 1448,A=2240505265,W=65535	
29	10.42.232.217	192.168.125.65	445	15:45:05.672269000	0.000012000	FTP Data	Src= 2859,Dst= 20,.AP...,S=3701178045,L= 375,A=2240505265,W=65535	
30	192.168.125.65	10.42.232.217	70	15:45:05.672630000	0.000361000	FTP Data	Src= 20,Dst= 2859,.A....,S=2240505265,L= 0,A=3701082102,W=16634	
31	192.168.125.65	10.42.232.217	70	15:45:05.673112000	0.000482000	FTP Data	Src= 20,Dst= 2859,.A....,S=2240505265,L= 0,A=3701084998,W=16544	
32	192.168.125.65	10.42.232.217	70	15:45:05.673963000	0.000851000	FTP Data	Src= 20,Dst= 2859,.A....,S=2240505265,L= 0,A=3701089342,W=16408	
33	192.168.125.65	10.42.232.217	70	15:45:05.674447000	0.000484000	FTP Data	Src= 20,Dst= 2859,.A....,S=2240505265,L= 0,A=3701092238,W=16318	
34	192.168.125.65	10.42.232.217	70	15:45:05.674924000	0.000477000	FTP Data	Src= 20,Dst= 2859,.A....,S=2240505265,L= 0,A=3701095134,W=16227	
35	192.168.125.65	10.42.232.217	70	15:45:05.676558000	0.001634000	FTP Data	Src= 20,Dst= 2859,.A....,S=2240505265,L= 0,A=3701099478,W=16091	
36	192.168.125.65	10.42.232.217	70	15:45:05.677125000	0.000567000	FTP Data	Src= 20,Dst= 2859,.A....,S=2240505265,L= 0,A=3701102374,W=16001	
37	192.168.125.65	10.42.232.217	70	15:45:05.678264000	0.001139000	FTP Data	Src= 20,Dst= 2859,.A....,S=2240505265,L= 0,A=3701105270,W=15910	
38	192.168.125.65	10.42.232.217	70	15:45:05.679714000	0.001450000	FTP Data	Src= 20,Dst= 2859,.A....,S=2240505265,L= 0,A=3701108166,W=15820	
39	192.168.125.65	10.42.232.217	70	15:45:05.680395000	0.000681000	FTP Data	Src= 20,Dst= 2859,.A....,S=2240505265,L= 0,A=3701111062,W=15729	
40	192.168.125.65	10.42.232.217	70	15:45:05.682117000	0.001722000	FTP Data	Src= 20,Dst= 2859,.A....,S=2240505265,L= 0,A=3701112885,W=15672	
41	10.42.232.217	192.168.125.65	1518	15:45:05.682703000	0.000586000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701178420,L= 1448,A=2240505265,W=65535	
42	10.42.232.217	192.168.125.65	1518	15:45:05.682826000	0.000123000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701179868,L= 1448,A=2240505265,W=65535	
43	10.42.232.217	192.168.125.65	1518	15:45:05.682949000	0.000123000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701181316,L= 1448,A=2240505265,W=65535	
44	10.42.232.217	192.168.125.65	1518	15:45:05.683072000	0.000123000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701182764,L= 1448,A=2240505265,W=65535	
45	10.42.232.217	192.168.125.65	1518	15:45:05.683195000	0.000123000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701184212,L= 1448,A=2240505265,W=65535	
46	10.42.232.217	192.168.125.65	1518	15:45:05.683319000	0.000124000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701185660,L= 1448,A=2240505265,W=65535	
47	10.42.232.217	192.168.125.65	1518	15:45:05.683441000	0.000122000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701187108,L= 1448,A=2240505265,W=65535	
48	10.42.232.217	192.168.125.65	1518	15:45:05.683564000	0.000123000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701188556,L= 1448,A=2240505265,W=65535	
49	10.42.232.217	192.168.125.65	1518	15:45:05.683687000	0.000123000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701190004,L= 1448,A=2240505265,W=65535	
50	10.42.232.217	192.168.125.65	1518	15:45:05.683811000	0.000124000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701191452,L= 1448,A=2240505265,W=65535	
51	10.42.232.217	192.168.125.65	1518	15:45:05.683933000	0.000122000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701192900,L= 1448,A=2240505265,W=65535	
52	10.42.232.217	192.168.125.65	1518	15:45:05.684057000	0.000124000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701194348,L= 1448,A=2240505265,W=65535	
53	10.42.232.217	192.168.125.65	1518	15:45:05.684179000	0.000122000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701195796,L= 1448,A=2240505265,W=65535	
54	10.42.232.217	192.168.125.65	1518	15:45:05.684303000	0.000124000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701197244,L= 1448,A=2240505265,W=65535	
55	10.42.232.217	192.168.125.65	1518	15:45:05.684426000	0.000123000	FTP Data	Src= 2859,Dst= 20,.A....,S=3701198692,L= 1448,A=2240505265,W=65535	

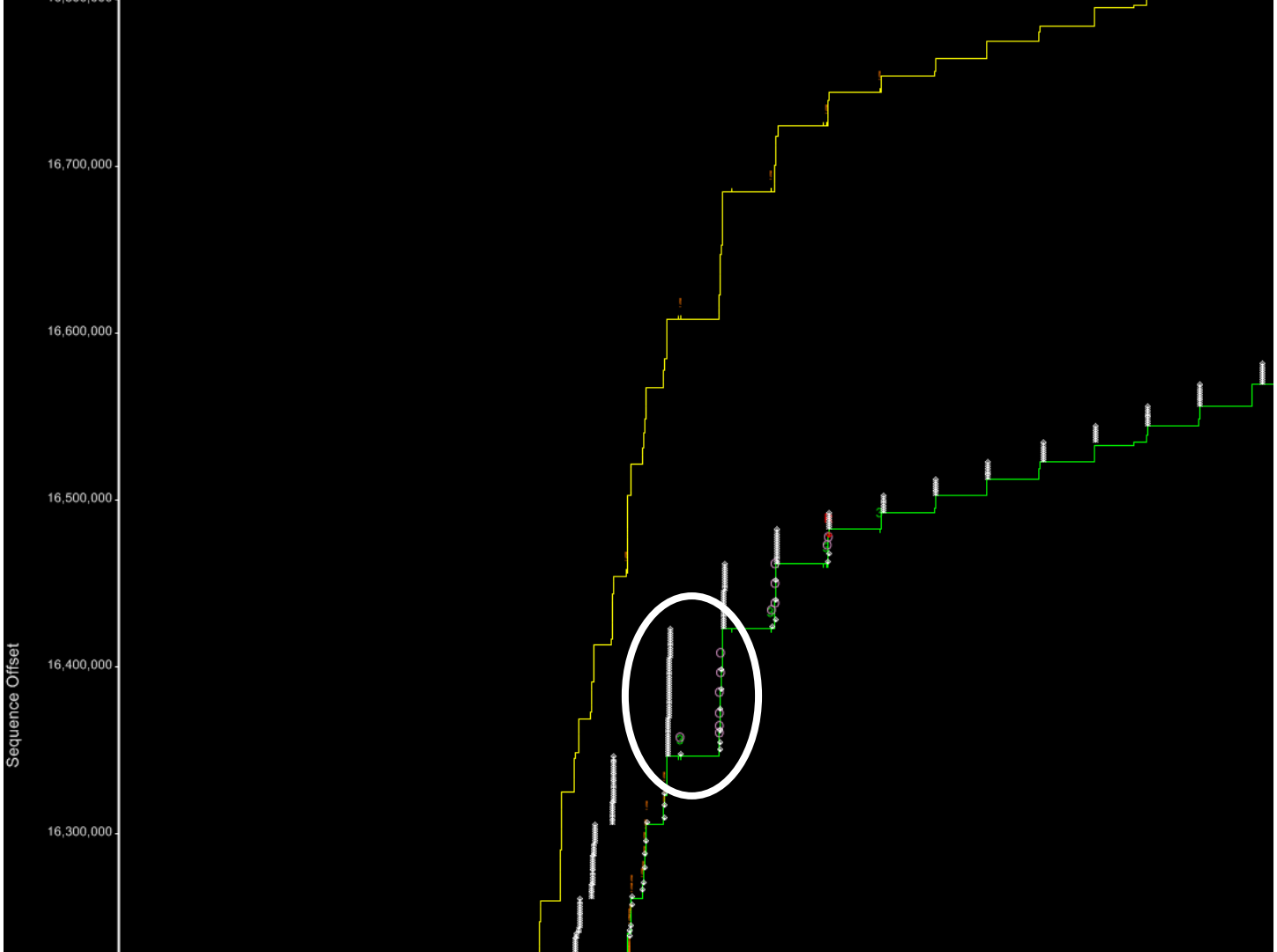
Packet	Absolute Time	Delta Time	PacketVisualizer	Ack For	Summary	Expert
7654	15:45:07.920991000	0.000592000			IP L= 1500 TCP .A.... S= 7440582 L= 1448 O=A W=65535	
7655	15:45:07.921114000	0.000123000			IP L= 1500 TCP .A.... S= 7442030 L= 1448 O=A W=65535	
7656	15:45:07.921238000	0.000124000			IP L= 1500 TCP .A.... S= 7443478 L= 1448 O=A W=65535	
7657	15:45:07.921361000	0.000123000			IP L= 1500 TCP .A.... S= 7444926 L= 1448 O=A W=65535	
7658	15:45:07.921483000	0.000122000			IP L= 1500 TCP .A.... S= 7446374 L= 1448 O=A W=65535	
7659	15:45:07.921606000	0.000123000			IP L= 1500 TCP .A.... S= 7447822 L= 1448 O=A W=65535	
7660	15:45:07.921729000	0.000123000			IP L= 1500 TCP .A.... S= 7449270 L= 1448 O=A W=65535	
7661	15:45:07.921852000	0.000123000			IP L= 1500 TCP .A.... S= 7450718 L= 1448 O=A W=65535	
7662	15:45:07.921976000	0.000124000			IP L= 1500 TCP .A.... S= 7452166 L= 1448 O=A W=65535	
7663	15:45:07.922099000	0.000123000			IP L= 1500 TCP .A.... S= 7453614 L= 1448 O=A W=65535	
7664	15:45:07.922221000	0.000122000			IP L= 1500 TCP .A.... S= 7455062 L= 1448 O=A W=65535	
7665	15:45:07.922344000	0.000123000			IP L= 1500 TCP .A.... S= 7456510 L= 1448 O=A W=65535	
7666	15:45:07.922468000	0.000124000			IP L= 1500 TCP .A.... S= 7457958 L= 1448 O=A W=65535	
7667	15:45:07.922590000	0.000122000			IP L= 1500 TCP .A.... S= 7459406 L= 1448 O=A W=65535	
7668	15:45:07.922714000	0.000124000			IP L= 1500 TCP .A.... S= 7460854 L= 1448 O=A W=65535	
7669	15:45:07.922837000	0.000123000			IP L= 1500 TCP .A.... S= 7462302 L= 1448 O=A W=65535	
7670	15:45:07.922960000	0.000123000			IP L= 1500 TCP .A.... S= 7463750 L= 1448 O=A W=65535	
7671	15:45:07.923083000	0.000123000			IP L= 1500 TCP .A.... S= 7465198 L= 1448 O=A W=65535	
7672	15:45:07.923206000	0.000123000			IP L= 1500 TCP .A.... S= 7466646 L= 1448 O=A W=65535	
7673	15:45:07.923510000	0.000304000		7587	IP L= 52 TCP .A.... 7377943=A L= 0 S= 0 W=19624	
7674	15:45:07.923522000	0.000012000		7589	IP L= 52 TCP .A.... 7380839=A L= 0 S= 0 W=19533	
7675	15:45:07.923765000	0.000243000			IP L= 1500 TCP .A.... S= 7468094 L= 1448 O=A W=65535	
7676	15:45:07.923887000	0.000122000			IP L= 1500 TCP .A.... S= 7469542 L= 1448 O=A W=65535	
7677	15:45:07.924011000	0.000124000			IP L= 1500 TCP .A.... S= 7470990 L= 1448 O=A W=65535	
7678	15:45:07.924134000	0.000123000			IP L= 1500 TCP .A.... S= 7472438 L= 1448 O=A W=65535	
			0.001000000			
			0.002000000			
7679	15:45:07.926264000	0.002130000		7591	IP L= 52 TCP .A.... 7383735=A L= 0 S= 0 W=19443	
7680	15:45:07.926516000	0.000252000			IP L= 1500 TCP .A.... S= 7473886 L= 1448 O=A W=65535	
7681	15:45:07.926639000	0.000123000			IP L= 1500 TCP .A.... S= 7475334 L= 1448 O=A W=65535	
7682	15:45:07.927099000	0.000460000		7593	IP L= 52 TCP .A.... 7386631=A L= 0 S= 0 W=19352	
7683	15:45:07.927359000	0.000260000			IP L= 1500 TCP .A.... S= 7476782 L= 1448 O=A W=65535	
7684	15:45:07.927484000	0.000125000			IP L= 1500 TCP .A.... S= 7478230 L= 1448 O=A W=65535	
			0.001000000			
7685	15:45:07.929204000	0.001720000		7595	IP L= 52 TCP .A.... 7389527=A L= 0 S= 0 W=19262	
7686	15:45:07.929456000	0.000252000			IP L= 1500 TCP .A.... S= 7479678 L= 1448 O=A W=65535	
7687	15:45:07.929579000	0.000123000			IP L= 1500 TCP .A.... S= 7481126 L= 1448 O=A W=65535	
			0.001000000			
7688	15:45:07.930887000	0.001308000		7597	IP L= 52 TCP .A.... 7392423=A L= 0 S= 0 W=19171	
7689	15:45:07.931139000	0.000252000			IP L= 1500 TCP .A.... S= 7482574 L= 1448 O=A W=65535	
7690	15:45:07.931262000	0.000123000			IP L= 1500 TCP .A.... S= 7484022 L= 1448 O=A W=65535	
7691	15:45:07.931870000	0.000608000		7599	IP L= 52 TCP .A.... 7395319=A L= 0 S= 0 W=19081	
7692	15:45:07.931886000	0.000016000		7601	IP L= 52 TCP .A.... 7399663=A L= 0 S= 0 W=18945	
7693	15:45:07.931899000	0.000013000		7604	IP L= 52 TCP .A.... 7402559=A L= 0 S= 0 W=18855	
7694	15:45:07.931916000	0.000017000		7612	IP L= 52 TCP .A.... 7405455=A L= 0 S= 0 W=18764	
7695	15:45:07.931923000	0.000007000		7616	IP L= 52 TCP .A.... 7408351=A L= 0 S= 0 W=18674	
7696	15:45:07.931930000	0.000007000		7618	IP L= 52 TCP .A.... 7411247=A L= 0 S= 0 W=18583	
7697	15:45:07.932029000	0.000099000		7620	IP L= 52 TCP .A.... 7414143=A L= 0 S= 0 W=18493	
7698	15:45:07.932124000	0.000095000			IP L= 1500 TCP .A.... S= 7485470 L= 1448 O=A W=65535	

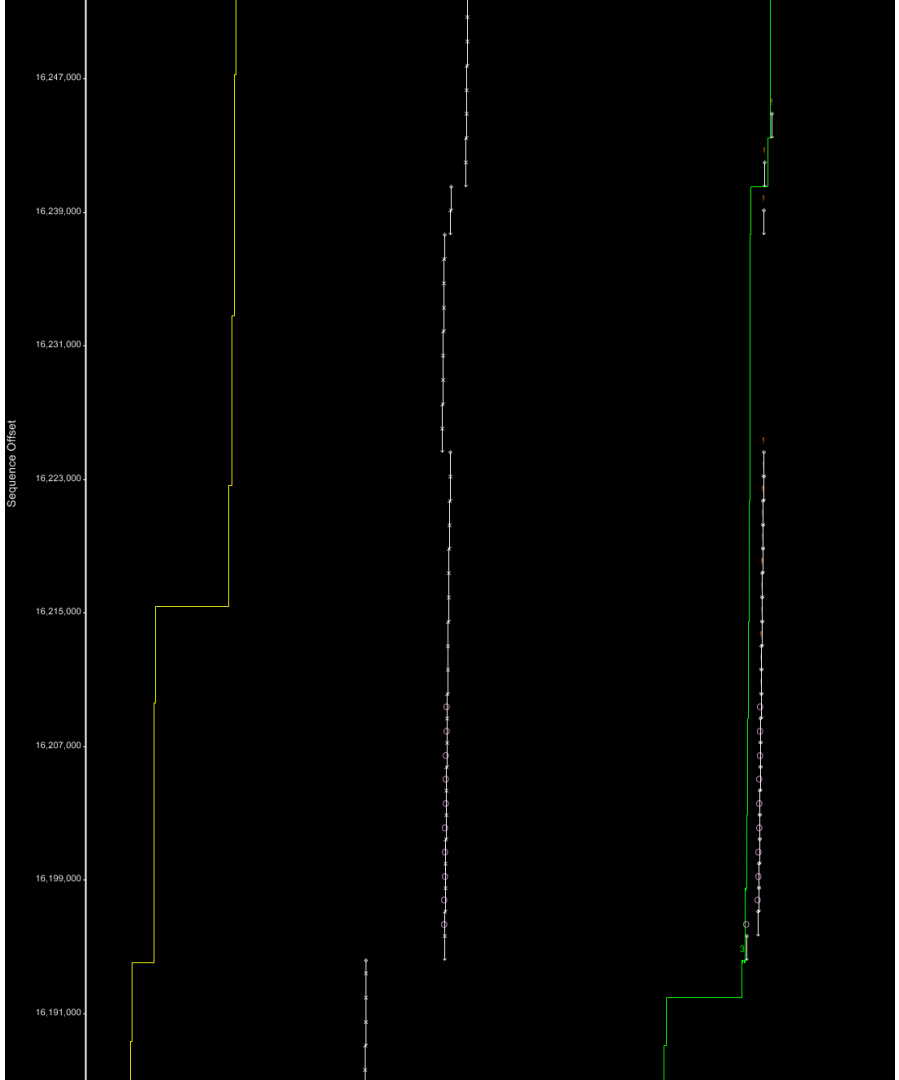

56,400,000
56,300,000
56,200,000
Sequence Offset
56,100,000
56,000,000
55,900,000
55,800,000
55,700,000


Sequence Offset
43,400,000
43,200,000
43,000,000
42,800,000
42,600,000
42,400,000
42,200,000

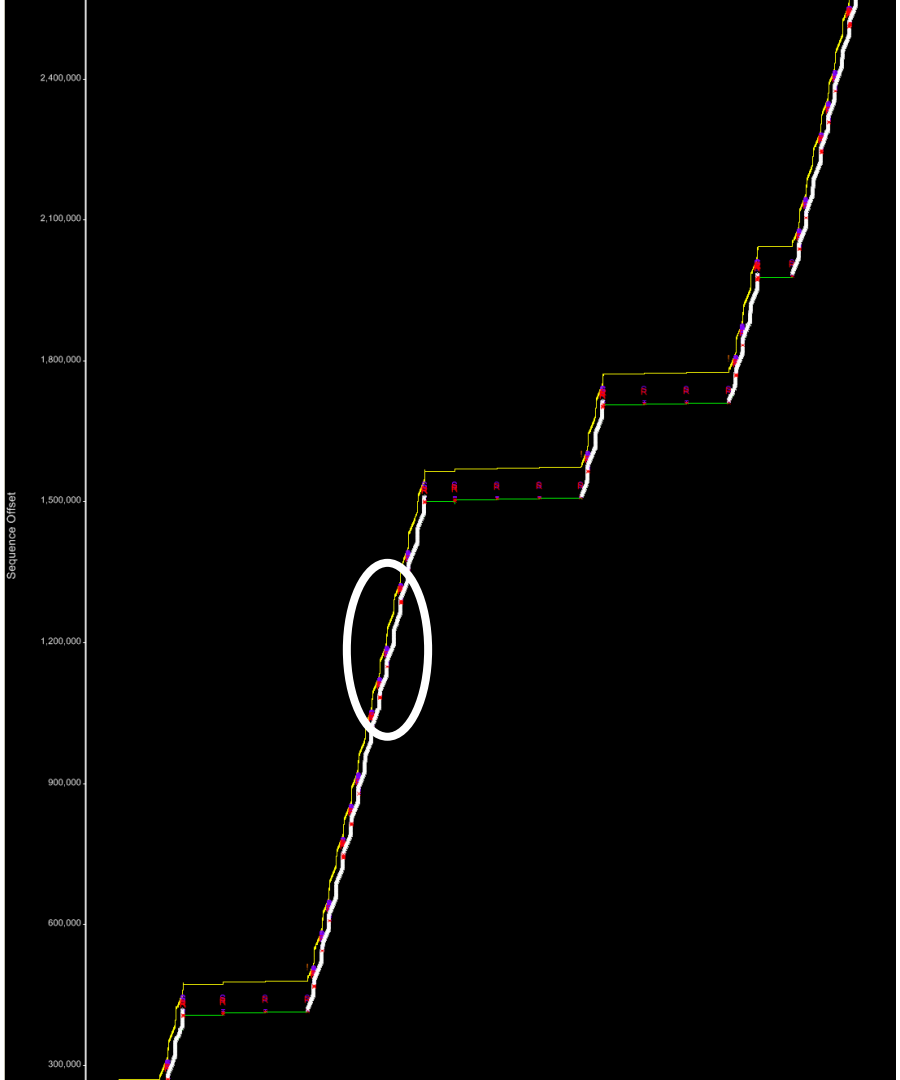
Mainframe Sending Segments Out-of-Order

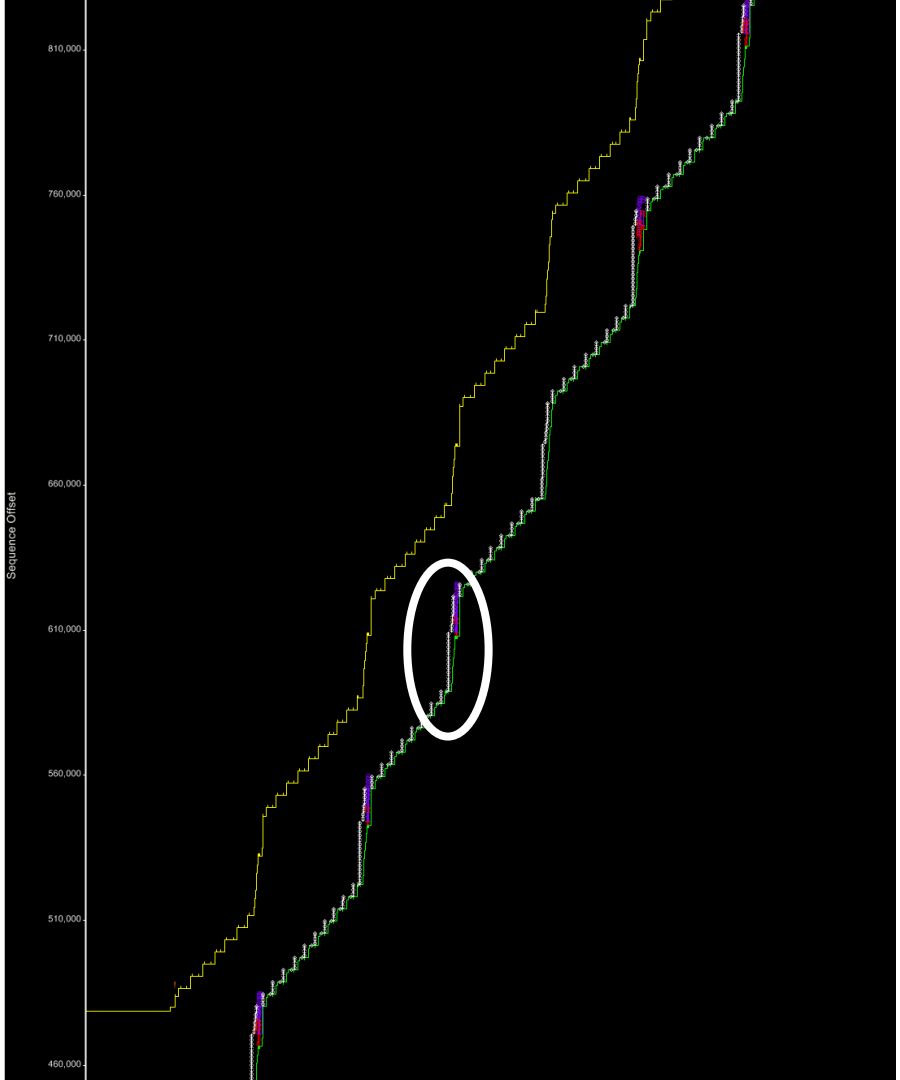

0.0s
2.0s
4.0s
6.0s
8.0s
10.0s
12.0s
14.0s
16.0s
18.0s
20.0s
22.0s

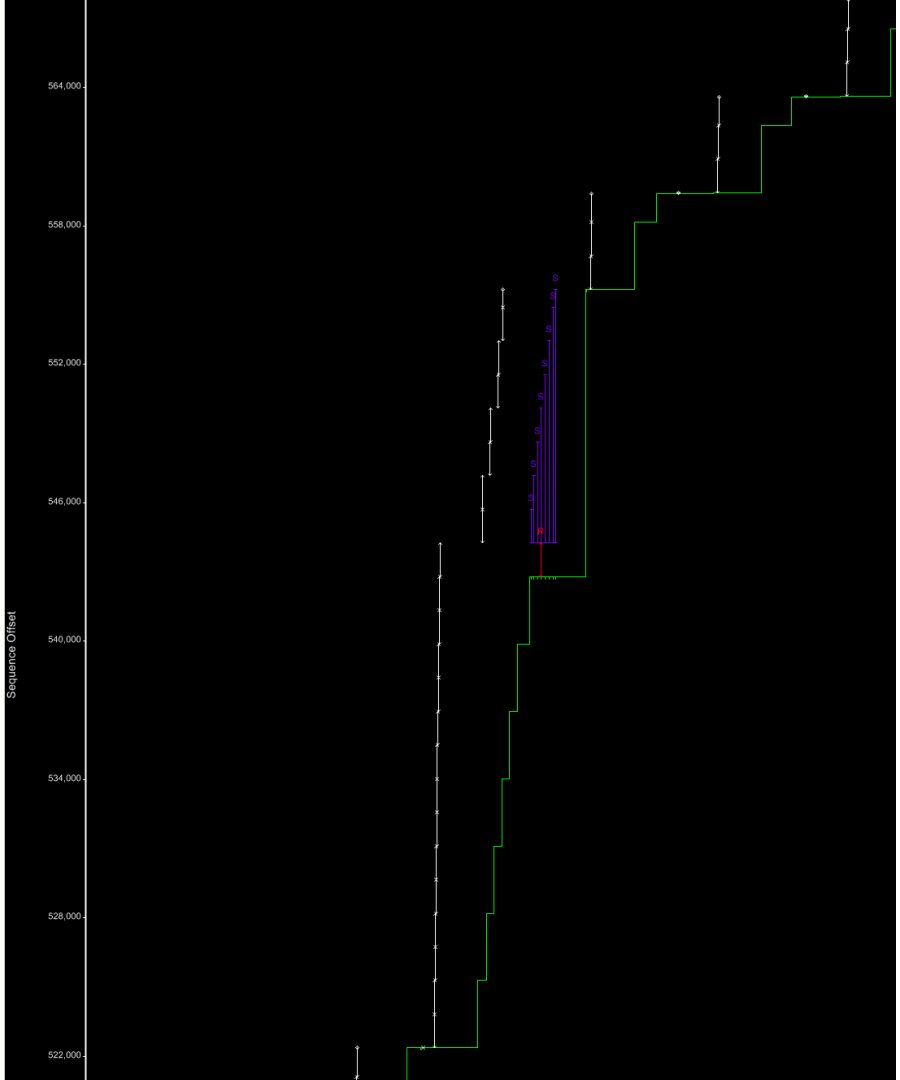

16,700,000
16,600,000
16,500,000
16,400,000
16,300,000
Sequence Offset

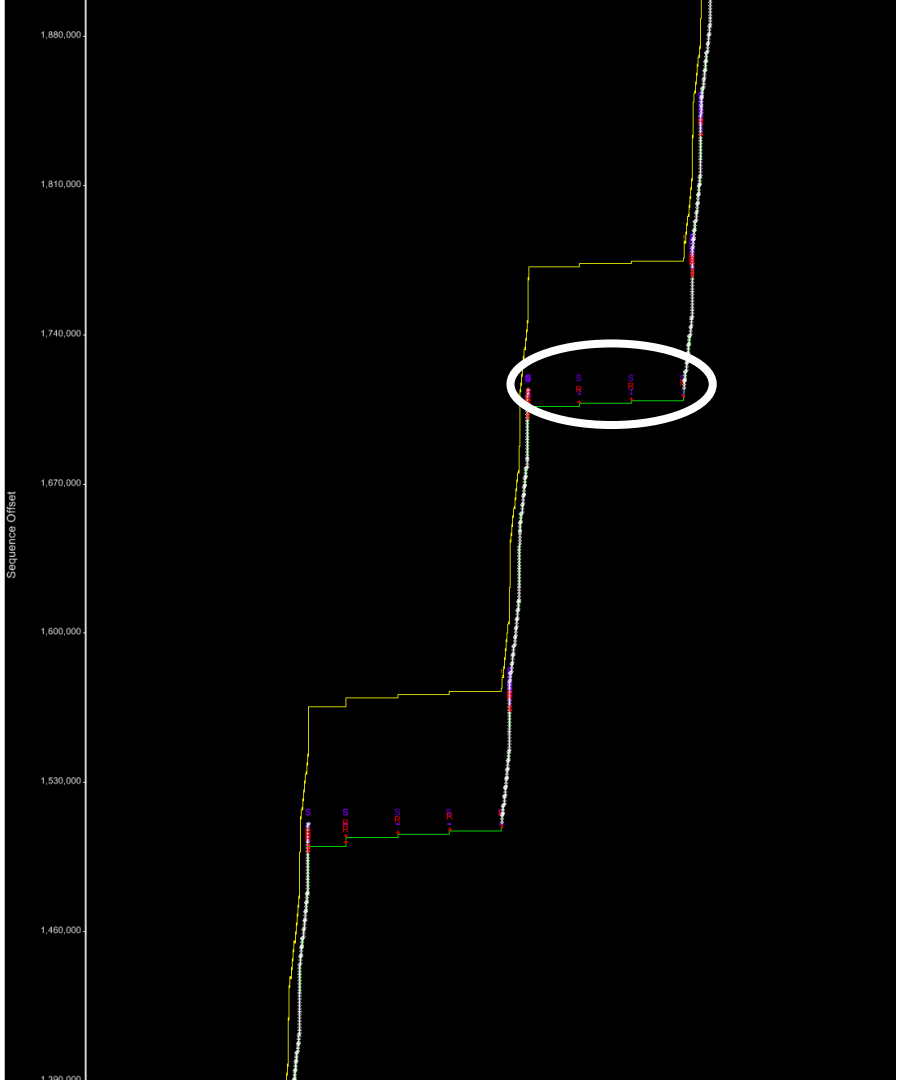

Sequence Offset
16,247,000
16,239,000
16,231,000
16,223,000
16,215,000
16,207,000
16,199,000
16,191,000

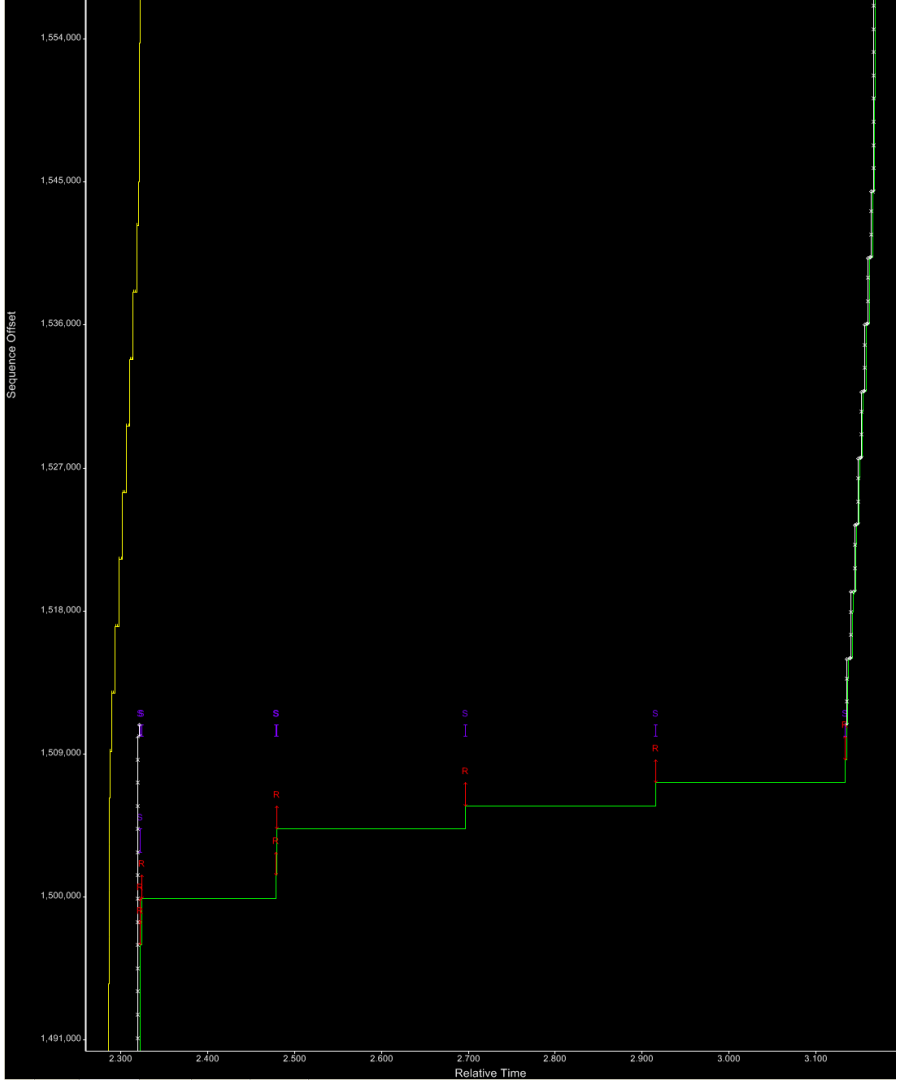
SMB File Transfer Overrunning a Switch Buffer


Sequence Offset
2,400,000
2,100,000
1,800,000
1,500,000
1,200,000
900,000
600,000
300,000


Sequence Offset
810,000
760,000
710,000
660,000
610,000
560,000
510,000
460,000


564,000
558,000
552,000
546,000
540,000
534,000
528,000
522,000
Sequence Offset


Sequence Offset
1,880,000
1,810,000
1,740,000
1,670,000
1,600,000
1,530,000
1,460,000


Sequence Offset
1,554,000
1,545,000
1,536,000
1,527,000
1,518,000
1,509,000
1,500,000
1,491,000
2.300
2.400
2.500
2.600
2.700
2.800
2.900
3.000
3.100
Relative Time
S
R