Google

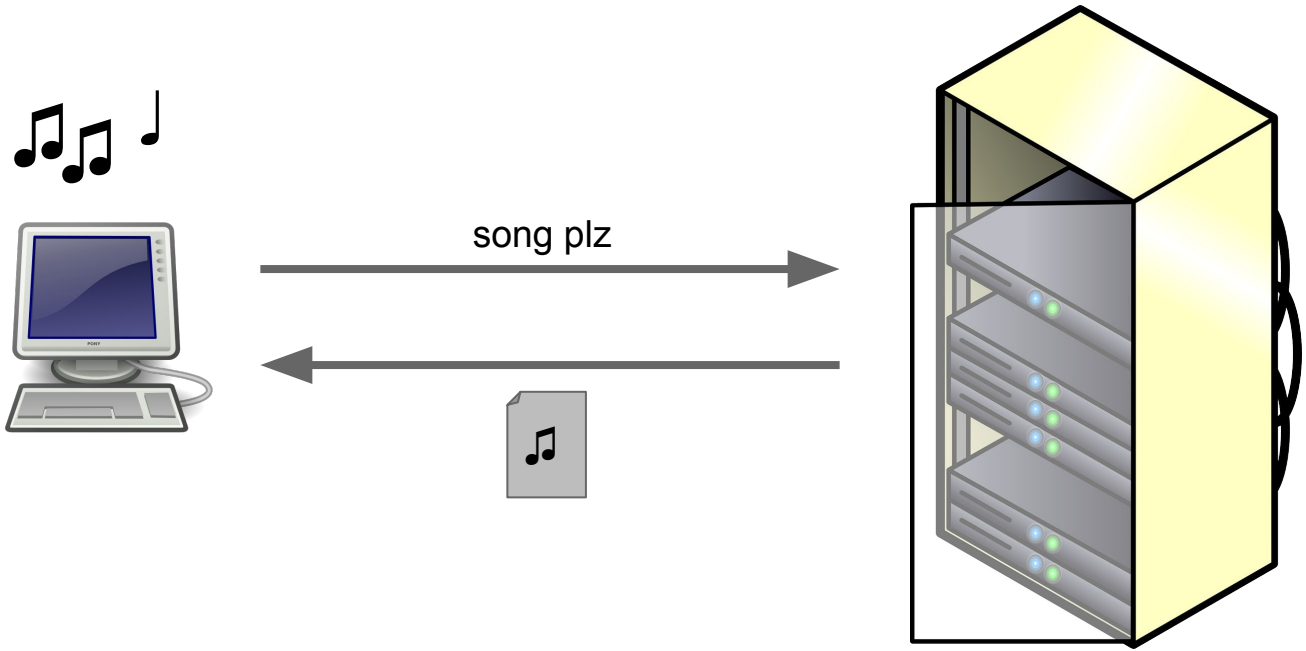
Real-time packet analysis at scale

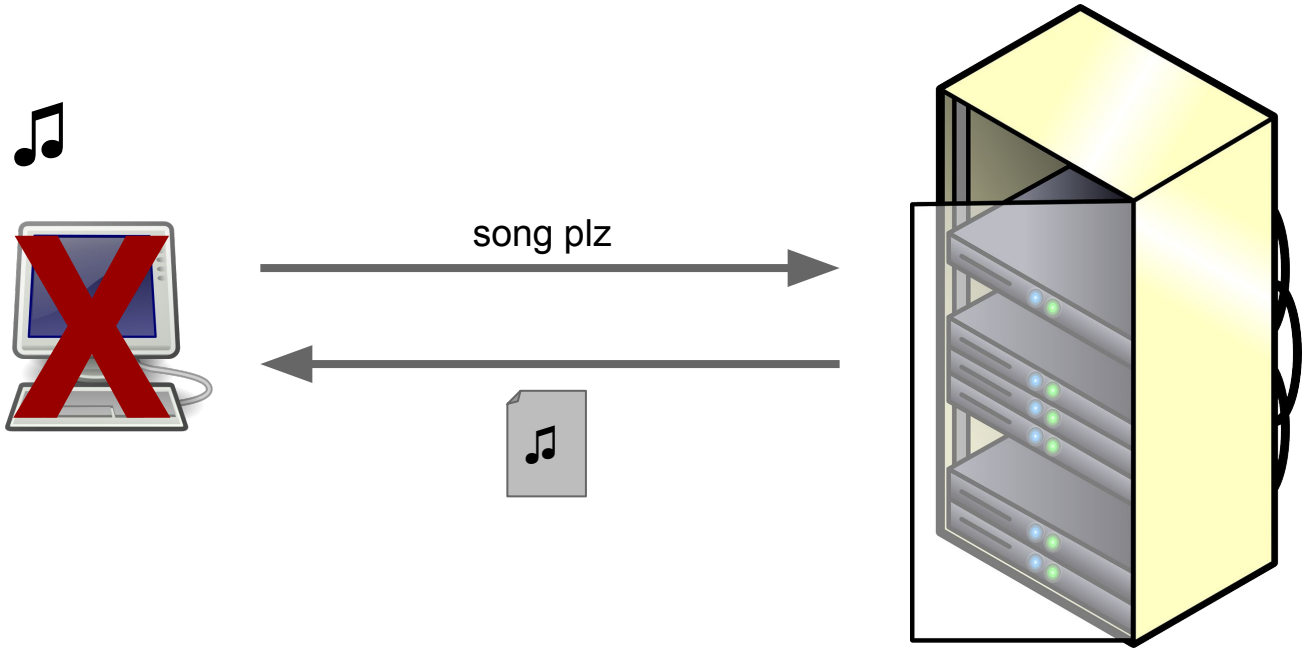
Douglas Creager
@dcreager

Monitorama PDX 2017

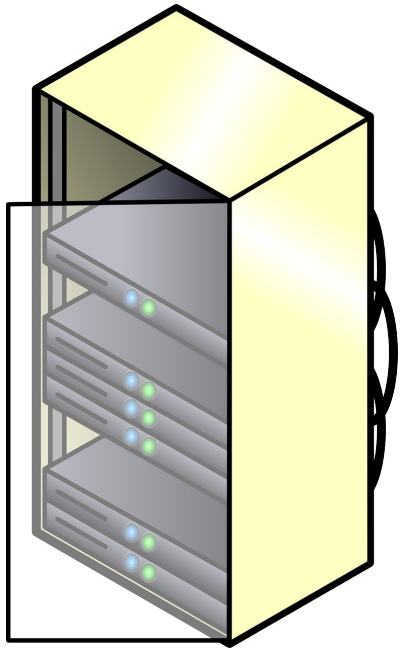
Packet captures are useful.

You won’t need to change your monitoring stack.

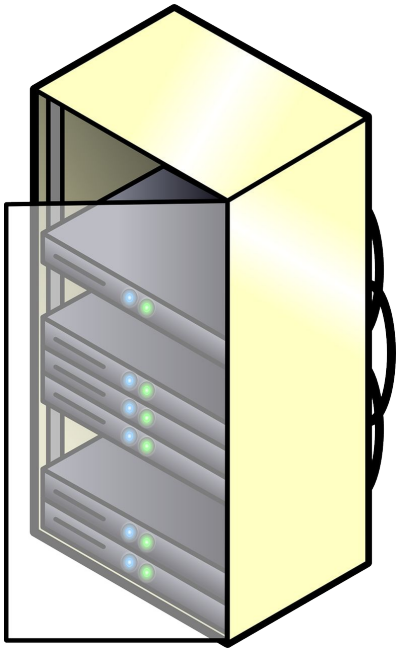

song plz


song plz


Throughput
(C) FHGPHOTO

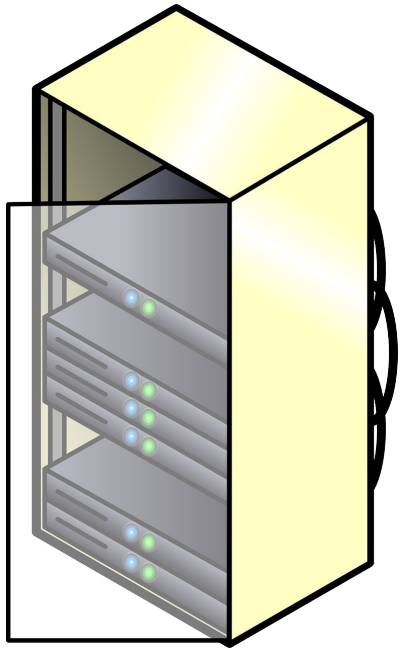


128 Kb/s

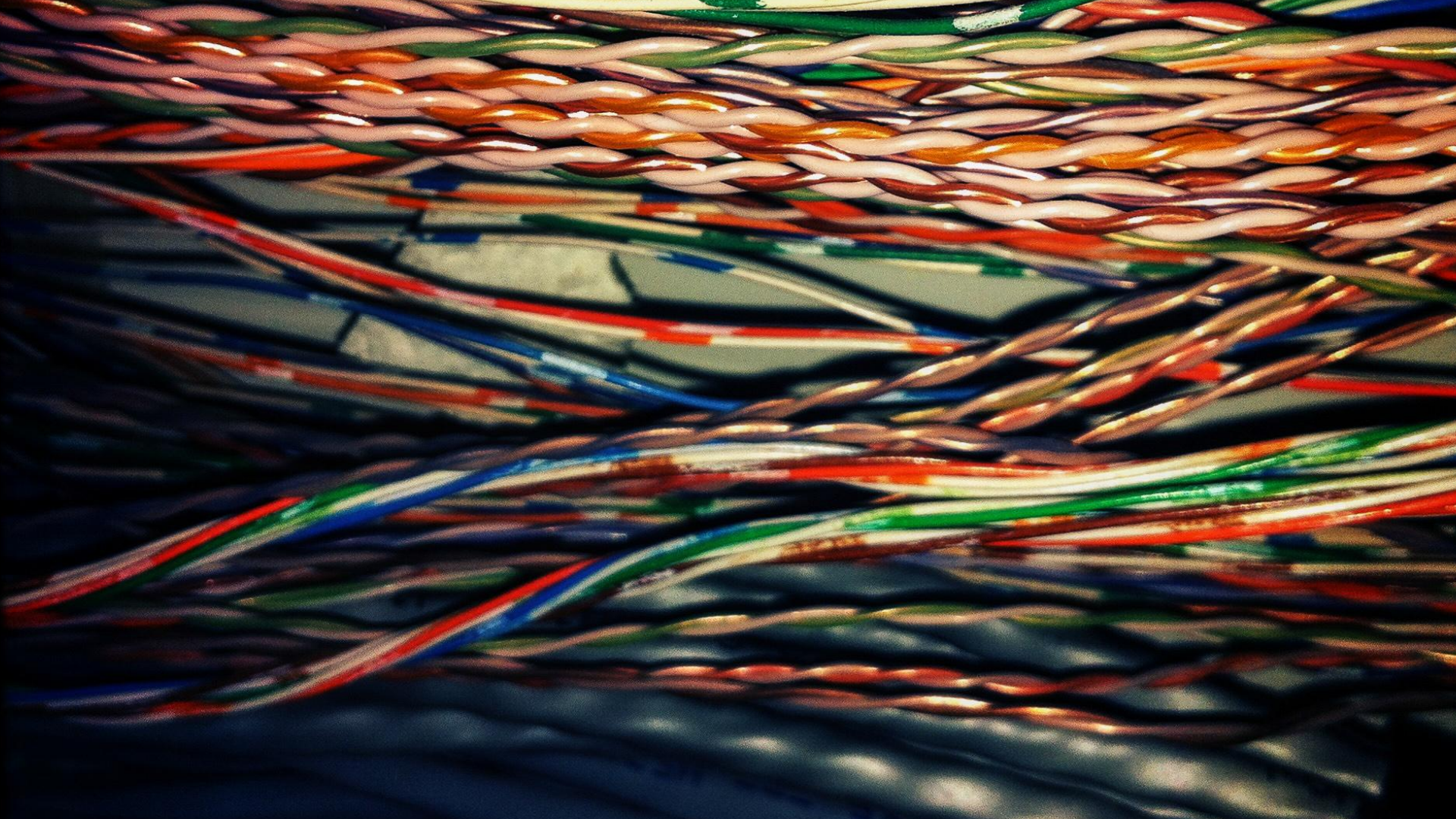


10 MB / 320 second = 250 Kb/s

?



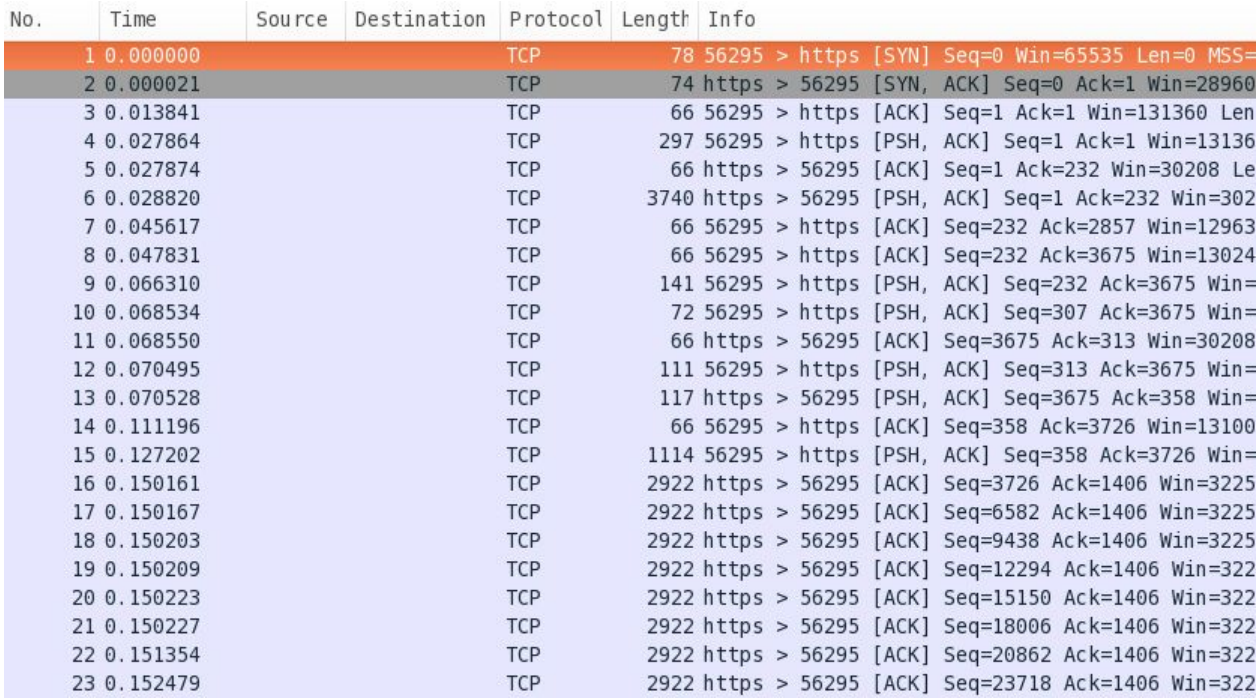

Vantage point




Flow data

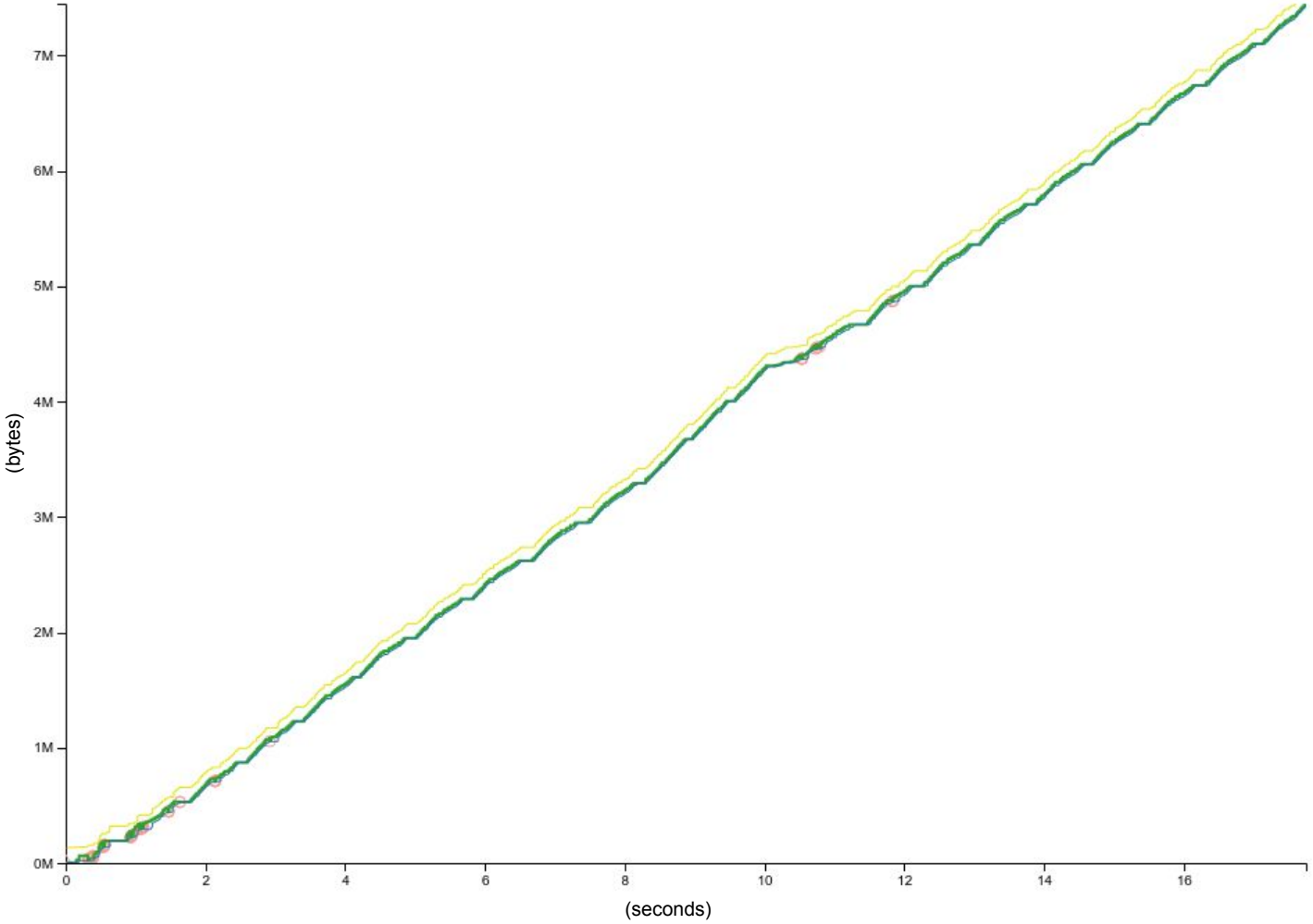
captures

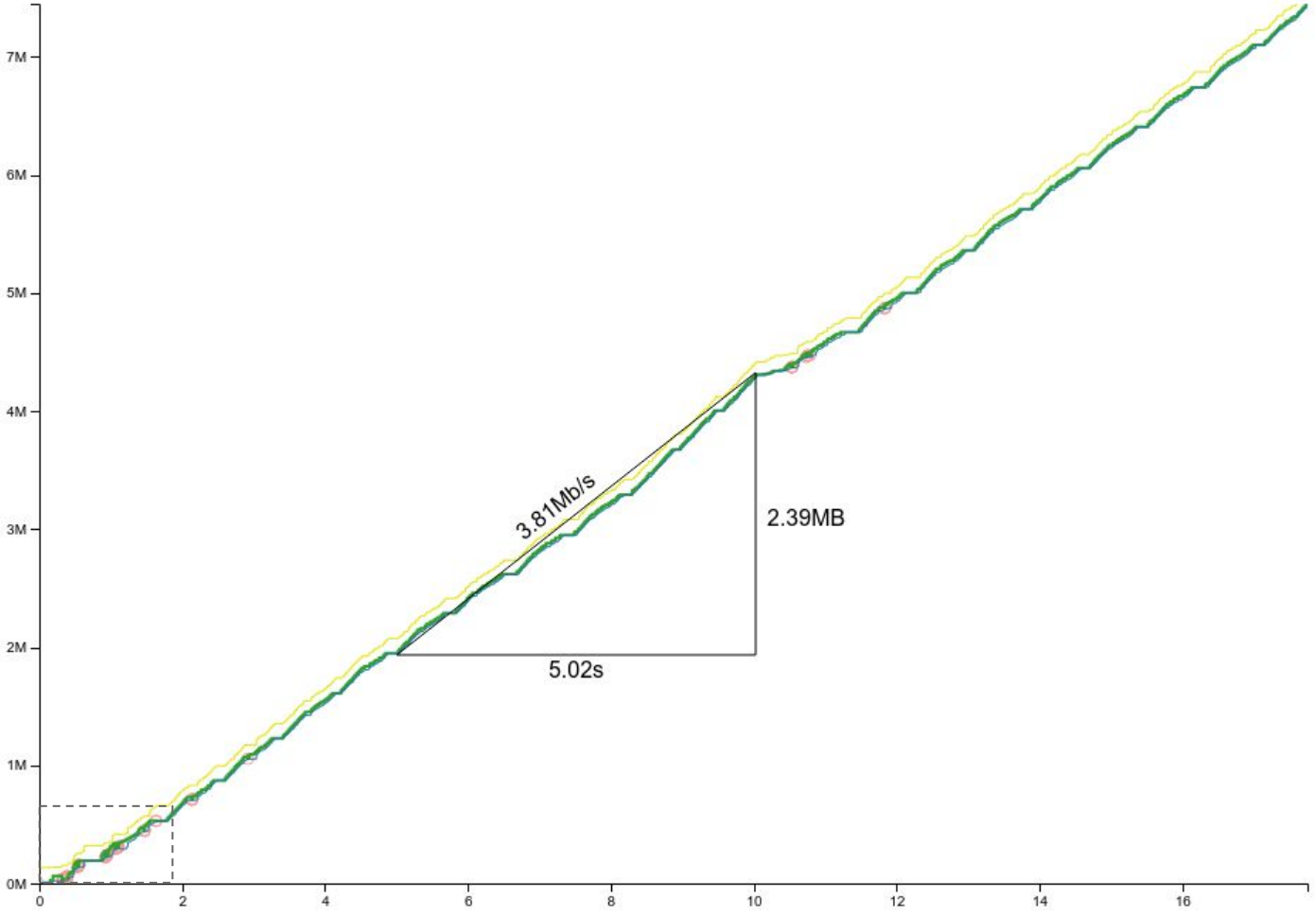

PACKET.
ROBIN.
WILD WOODBINE CIGARETTES
W.D.&H.O.WILLS
HILL'S
SPECIAL
SUNRIPE
CIGARETTES
CHOICE GOLDEN VIRGINIA
The Spinet House
"TENNER"
(MEDIUM)
LARGE SIZE
PLAYER'S No 6
PLAYER'S No 3
Extra Quality Cigarettes.
20 Pieces
NAVY
CIGARETTES
"MEDIUM"
WOODBINE
"Park Drive"
Cigarettes
GALLAHER'S
The Three Castles Cigarettes
W.D.& H.O.Wills
MEDIUM STRENGTH.
"CAPSTAN"
Navy Cut
Cigarettes
PICCADILLY
Number One
A LARGE SIZE CIGARETTE OF FINE QUALITY
PLAYERS
BACHELOR
10 SENIOR SERVICE 10

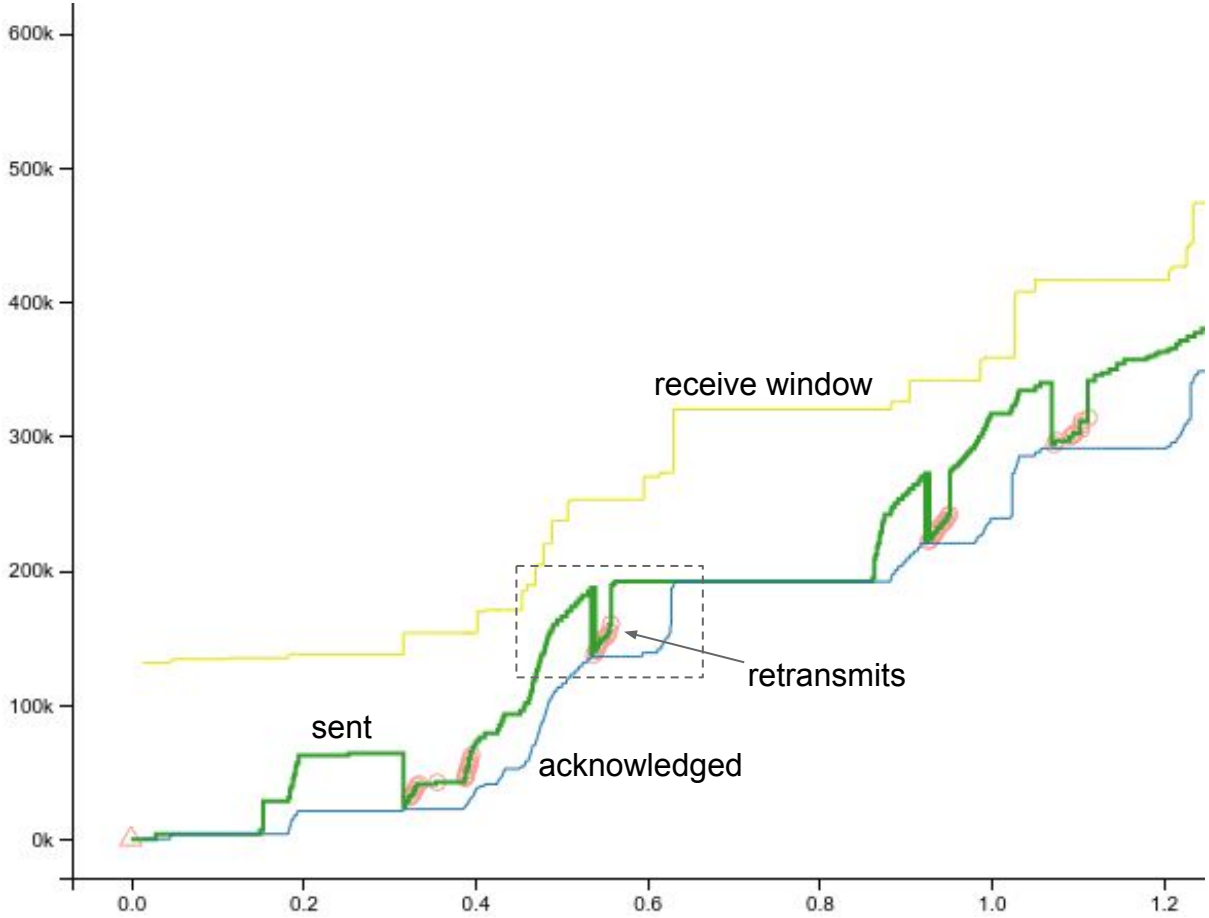


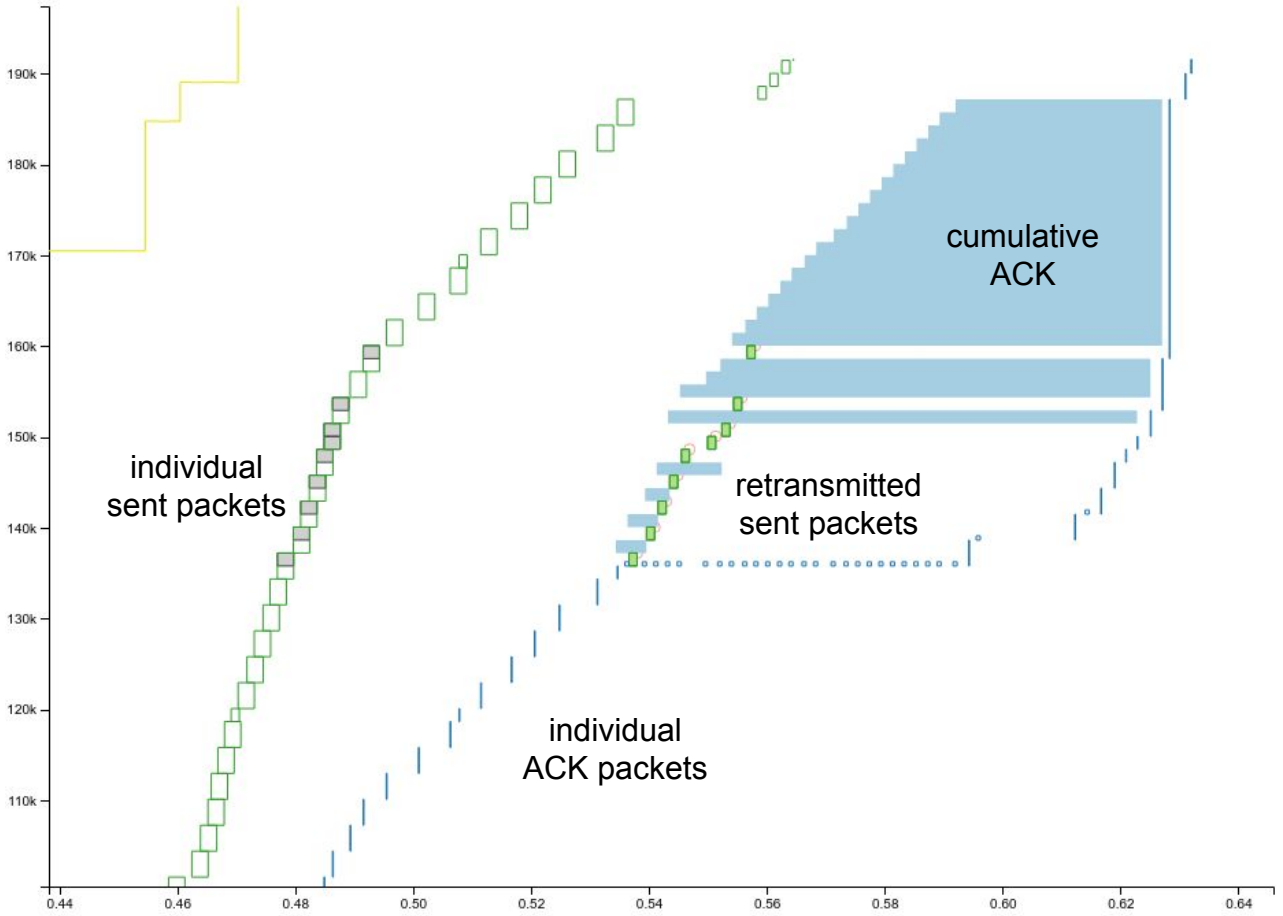
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000			TCP	78	56295 > https [SYN] Seq=0 Win=65535 Len=0 MSS=
2	0.000021			TCP	74	https > 56295 [SYN, ACK] Seq=0 Ack=1 Win=28960
3	0.013841			TCP	66	56295 > https [ACK] Seq=1 Ack=1 Win=131360 Len
4	0.027864			TCP	297	56295 > https [PSH, ACK] Seq=1 Ack=1 Win=13136
5	0.027874			TCP	66	https > 56295 [ACK] Seq=1 Ack=232 Win=30208 Le
6	0.028820			TCP	3740	https > 56295 [PSH, ACK] Seq=1 Ack=232 Win=302
7	0.045617			TCP	66	56295 > https [ACK] Seq=232 Ack=2857 Win=12963
8	0.047831			TCP	66	56295 > https [ACK] Seq=232 Ack=3675 Win=13024
9	0.066310			TCP	141	56295 > https [PSH, ACK] Seq=232 Ack=3675 Win=
10	0.068534			TCP	72	56295 > https [PSH, ACK] Seq=307 Ack=3675 Win=
11	0.068550			TCP	66	https > 56295 [ACK] Seq=3675 Ack=313 Win=30208
12	0.070495			TCP	111	56295 > https [PSH, ACK] Seq=313 Ack=3675 Win=
13	0.070528			TCP	117	https > 56295 [PSH, ACK] Seq=3675 Ack=358 Win=
14	0.111196			TCP	66	56295 > https [ACK] Seq=358 Ack=3726 Win=13100
15	0.127202			TCP	1114	56295 > https [PSH, ACK] Seq=358 Ack=3726 Win=
16	0.150161			TCP	2922	https > 56295 [ACK] Seq=3726 Ack=1406 Win=3225
17	0.150167			TCP	2922	https > 56295 [ACK] Seq=6582 Ack=1406 Win=3225
18	0.150203			TCP	2922	https > 56295 [ACK] Seq=9438 Ack=1406 Win=3225
19	0.150209			TCP	2922	https > 56295 [ACK] Seq=12294 Ack=1406 Win=322
20	0.150223			TCP	2922	https > 56295 [ACK] Seq=15150 Ack=1406 Win=322
21	0.150227			TCP	2922	https > 56295 [ACK] Seq=18006 Ack=1406 Win=322
22	0.151354			TCP	2922	https > 56295 [ACK] Seq=20862 Ack=1406 Win=322
23	0.152479			TCP	2922	https > 56295 [ACK] Seq=23718 Ack=1406 Win=322

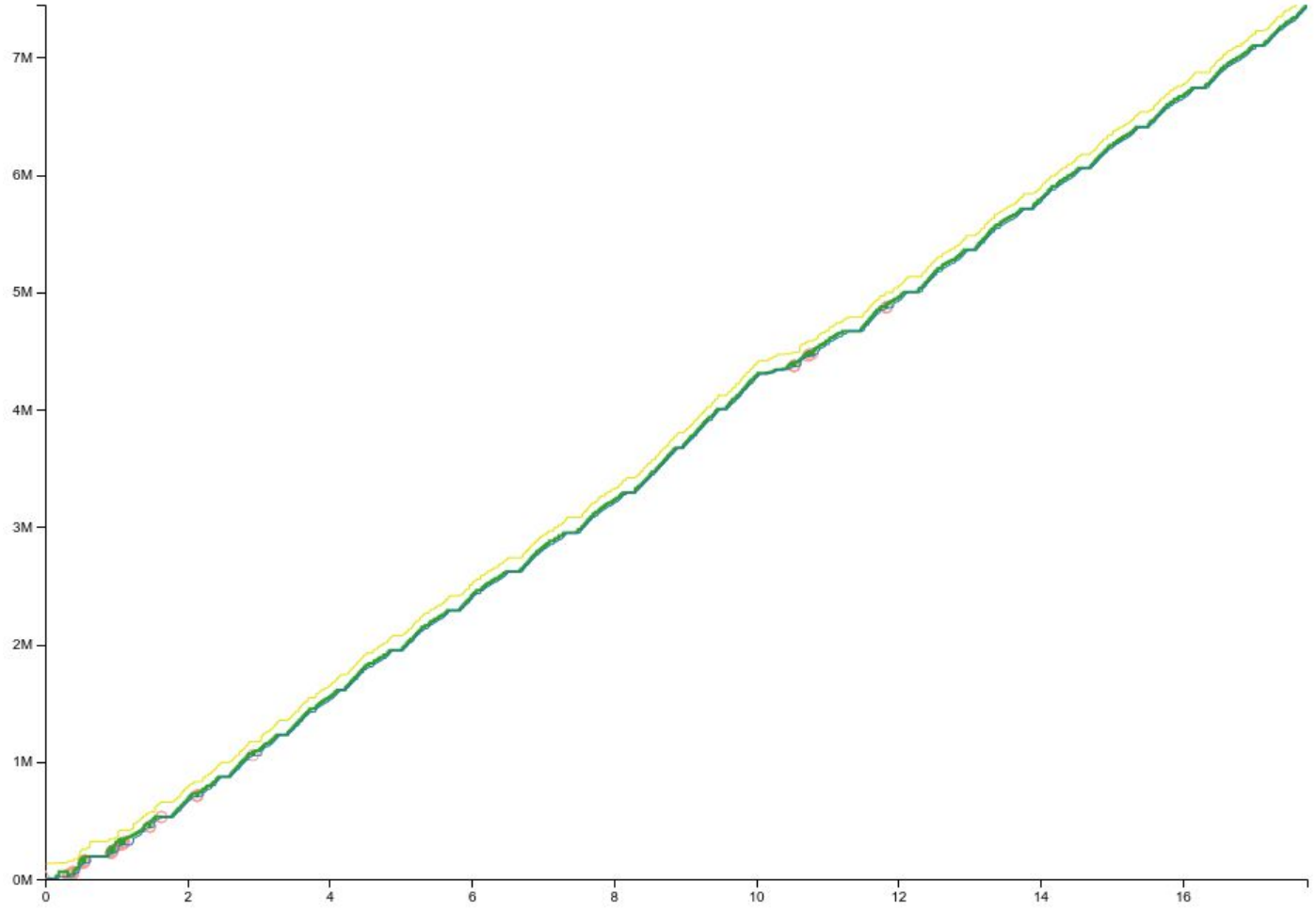
What’s the throughput?

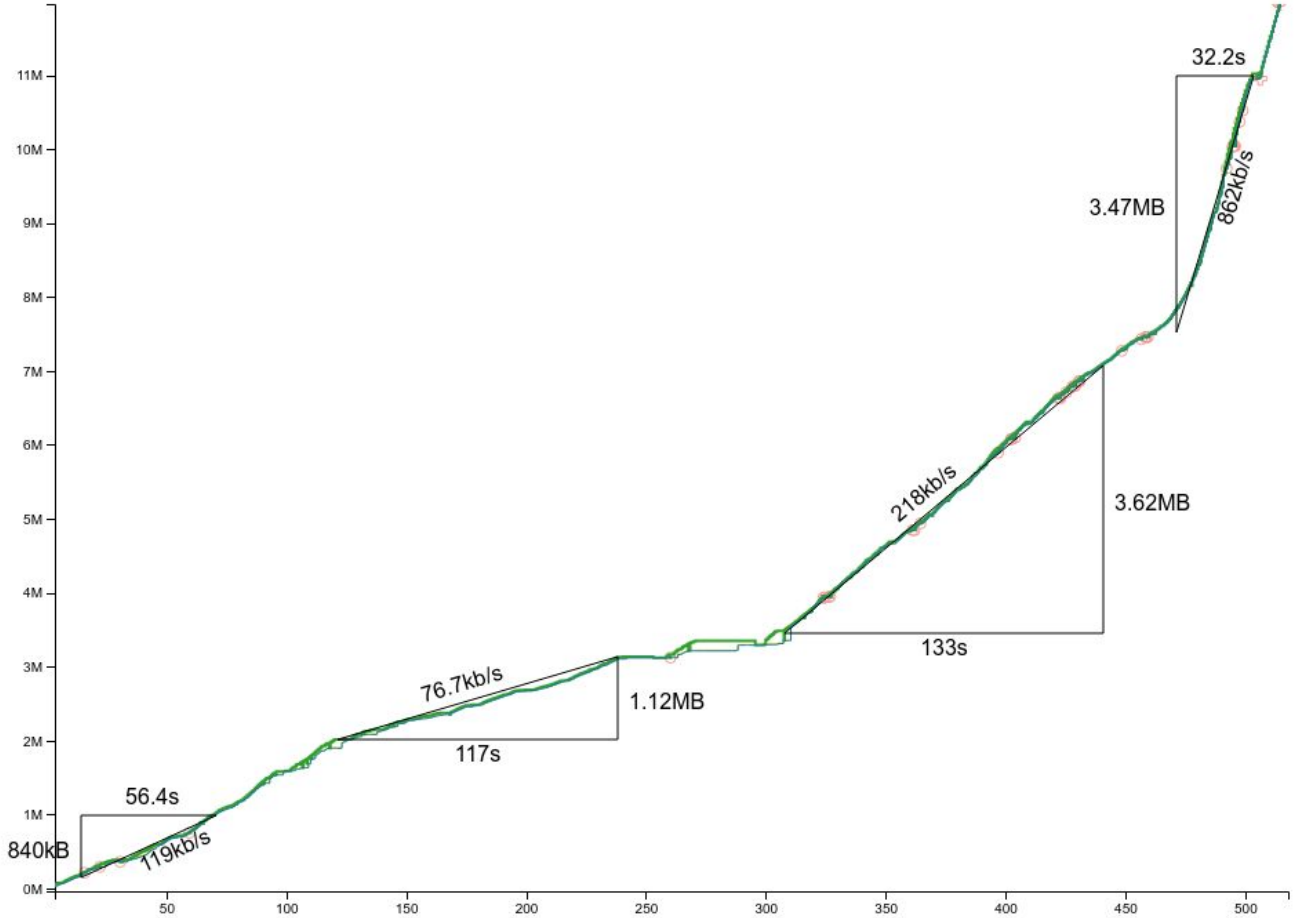

7M
6M
5M
4M
3M
2M
1M
0M
(bytes)
0
2
4
6
8
10
12
14
16
(seconds)

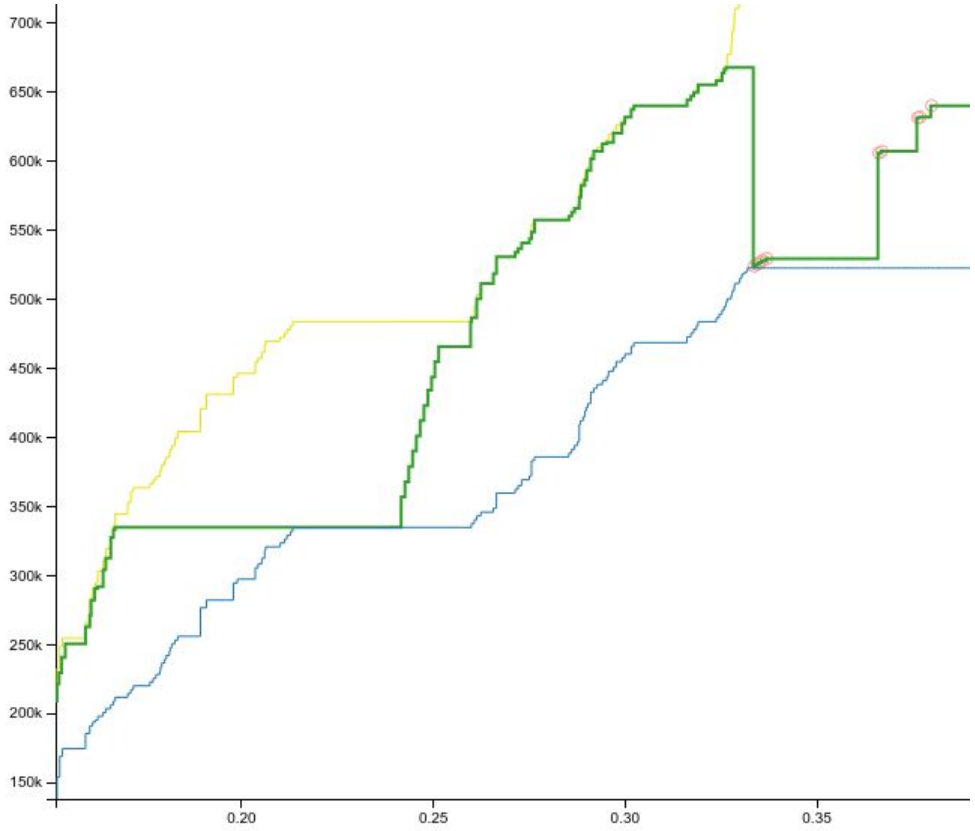



600k
500k
400k
300k
200k
100k
0k
0.0
0.2
0.4
0.6
0.8
1.0
1.2
receive window
retransmits
sent
acknowledged

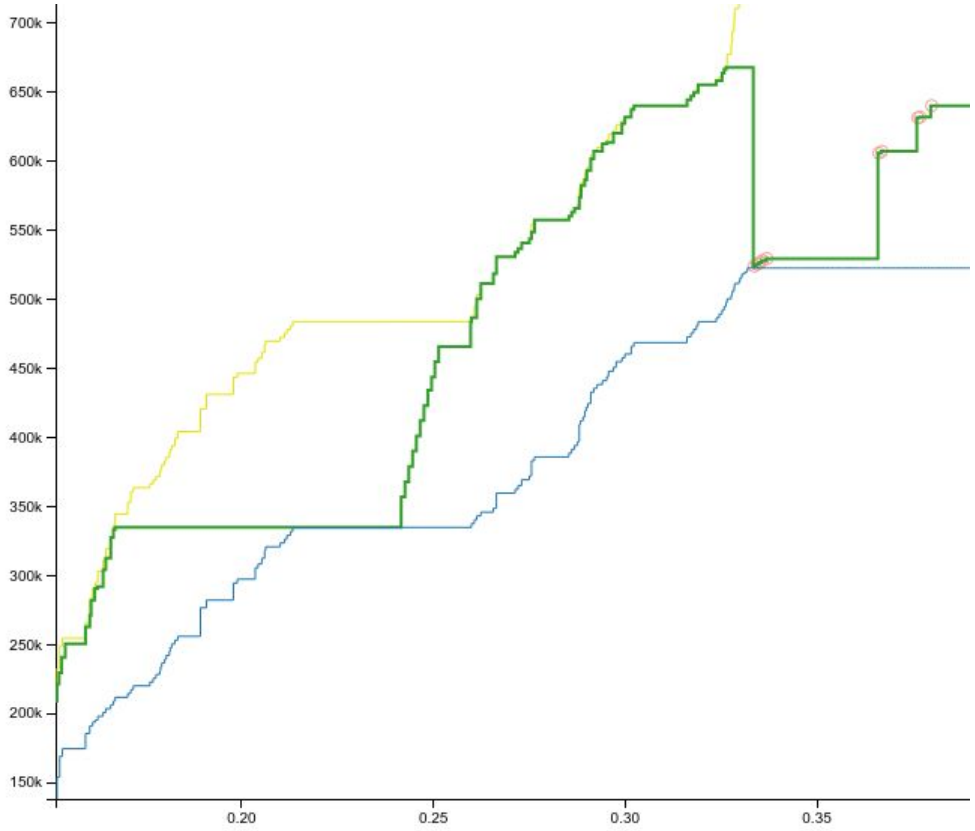

190k
180k
170k
160k
150k
140k
130k
120k
110k
0.44
0.46
0.48
0.50
0.52
0.54
0.56
0.58
0.60
0.62
0.64
cumulative
ACK
individual
sent packets
retransmitted
sent packets
individual
ACK packets

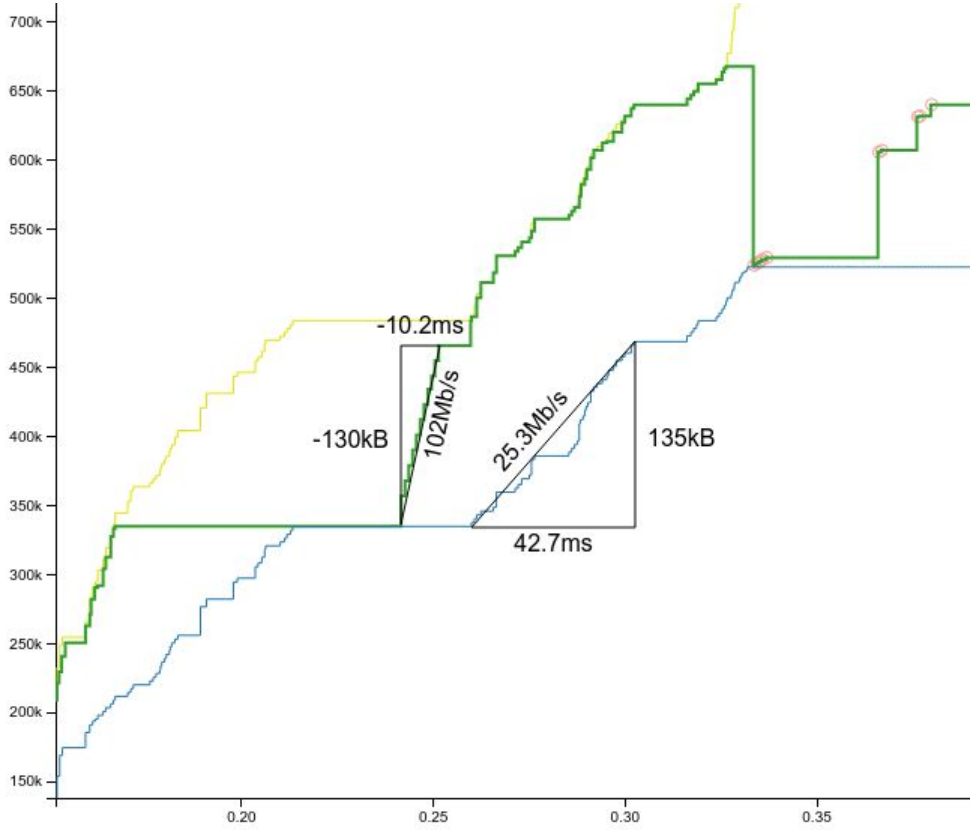



11M
10M
9M
8M
7M
6M
5M
4M
3M
2M
1M
0M
50
100
150
200
250
300
350
400
450
500
840kB
56.4s
119kb/s
76.7kb/s
117s
1.12MB
218kb/s
133s
3.62MB
32.2s
3.47MB
862kb/s

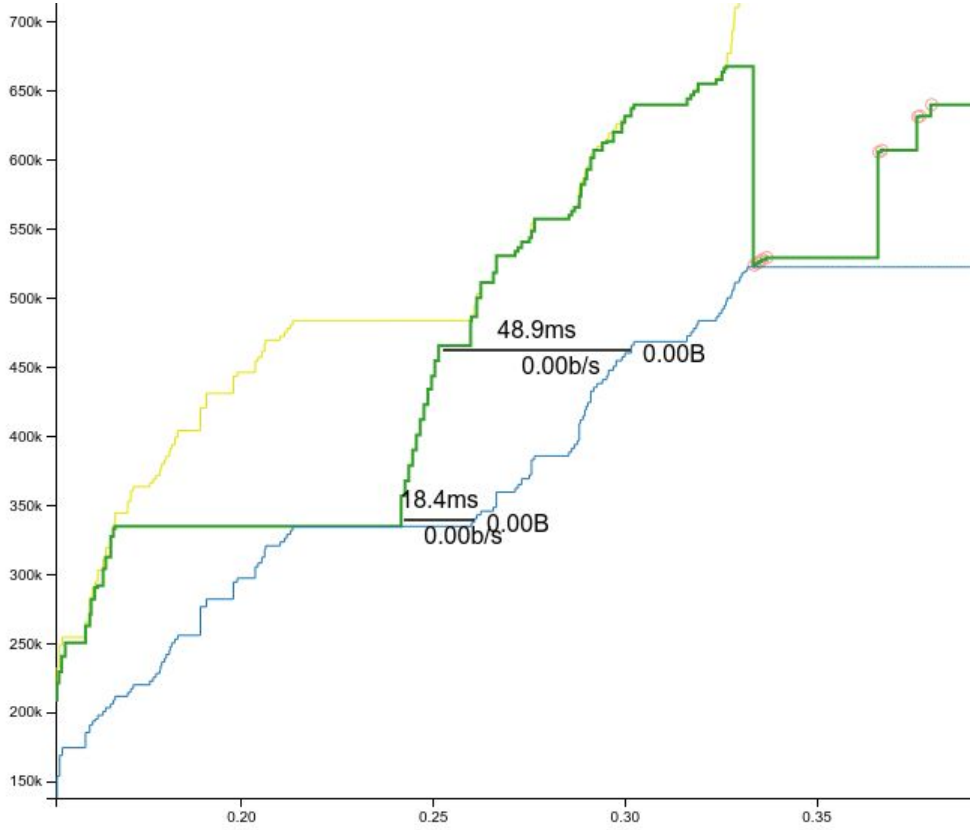

700k
650k
600k
550k
500k
450k
400k
350k
300k
250k
200k
150k
0.20
0.25
0.30
0.35


Bufferbloat


700k
650k
600k
550k
500k
450k
400k
350k
300k
250k
200k
150k
0.20
0.25
0.30
0.35


700k
650k
600k
550k
500k
450k
400k
350k
300k
250k
200k
150k
0.20
0.25
0.30
0.35
-10.2ms
-130kB
102Mb/s
25.3Mb/s
135kB
42.7ms

Latency


700k
650k
600k
550k
500k
450k
400k
350k
300k
250k
200k
150k
0.20
0.25
0.30
0.35
48.9ms
0.00b/s
0.00B
18.4ms
0.00b/s
0.00B


Look for interesting patterns


Collect some packets


LEVEL 1
tcpdump


LEVEL 2
libpcap


Add to your existing
monitoring stack

```
{"start_timestamp": "2017-05-22 13:23:00.325632Z",
 "end_timestamp": "2017-05-22 13:23:05.957626Z",
 "client_country": "US", "server_zone": "us-east1",
 "blackholed": true, "bufferbloat": true,
 "non_idle_throughput_mbps": 1.2}
```

```
{"start_timestamp": "2017-05-22 13:23:00.325632Z",
 "end_timestamp": "2017-05-22 13:23:05.957626Z",
 "client_country": "US", "server_zone": "us-east1",
 "blackholed": true, "bufferbloat": true,
 "non_idle_throughput_mbps": 1.2}
```

```
{"start_timestamp": "2017-05-22 13:23:00.325632Z",
 "end_timestamp": "2017-05-22 13:23:05.957626Z",
 "client_country": "US", "server_zone": "us-east1",
 "blackholed": true, "bufferbloat": true,
 "non_idle_throughput_mbps": 1.2}
```

```
{"start_timestamp": "2017-05-22 13:23:00.325632Z",
 "end_timestamp": "2017-05-22 13:23:05.957626Z",
 "client_country": "US", "server_zone": "us-east1",
 "blackholed": true, "bufferbloat": true,
 "non_idle_throughput_mbps": 1.2}
```

Conclusions

Packet captures are useful.

You won’t need to change your monitoring stack.

Image credits

All images licensed under CC BY 2.0, https://creativecommons.org/licenses/by/2.0/, unless otherwise noted

§3-10, Computer icon by Tango Project, public domain: https://commons.wikimedia.org/wiki/File:Computer.svg

§3-10, Server rack icon, CC0, https://creativecommons.org/publicdomain/zero/1.0/: https://pixabay.com/en/server-mount-icon-rack-computer-98402/

§5, Detail of “Hyper-Sky” by FHG: https://flic.kr/p/2ZXjk4

§10, Detail of “Observation point” by Franck Michel: https://flic.kr/p/qMjiQ8

§11, Detail of “Networking” by Andrew Malone: https://flic.kr/p/nmLheP

§12-13, Detail of “Flow” by Kalle Gustafsson: https://flic.kr/p/arV528

§14, Detail of “Collection of Old Cigarette Packets” by David Wright: https://flic.kr/p/7F4xRE

§15, Detail of “South Beach flood” by maxstrz: https://flic.kr/p/6u5fXb

§24, Detail of “Spicy Toad” by Cory Denton: https://flic.kr/p/oWh7dW

§27, Detail of “Stopwatch” by William Warby: https://flic.kr/p/62hNF6

§29, Detail of “tidal pattern 1” by david: https://flic.kr/p/sqiJKP

§30, Detail of “Coca-Cola Bottling Plant” by Simon Berry: https://flic.kr/p/e1ZZZP

§31, Detail of “Chick” by Tom Coppen: https://flic.kr/p/8KpAtn

§32, Detail of “hen” by dlp: https://flic.kr/p/8bDsG6

§33, Detail of “monitors” by Samuel Mann: https://flic.kr/p/5rfHm5

§38, Detail of “...in the name of love” by Chrishna: https://flic.kr/p/64gcDZ