

# Using Splunk To Monitor Network Connectivity and Quality

Douglas Muth

Twitter: @dmuth

<https://www.dmuth.org/>



None of the things I am about to say should be considered as speaking for Splunk, and definitely not for my employer.

You interrupted my tachyon detection grid



for THIS?



# How My Obsession Started

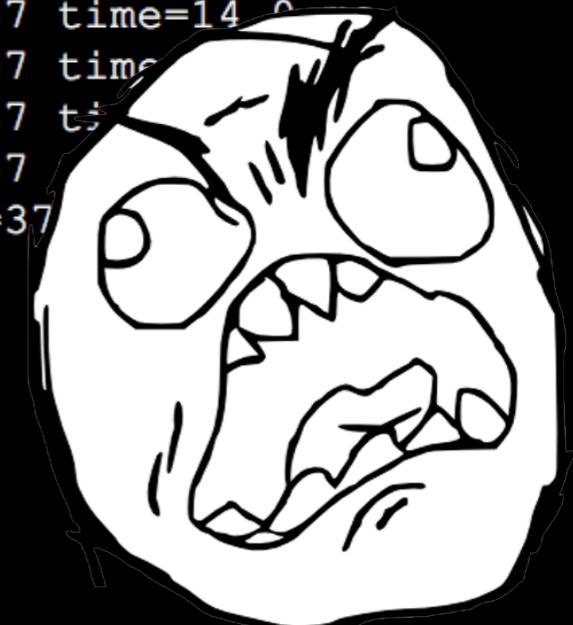
```
root@9472fb8370bd:/# ping -c 10 google.com
PING google.com (172.217.6.206) 56(84) bytes of data.
64 bytes from lga25s54-in-f206.1e100.net (172.217.6.206): icmp_seq=1 ttl=37 time=20.9 ms
64 bytes from lga25s54-in-f206.1e100.net (172.217.6.206): icmp_seq=2 ttl=37 time=13.2 ms
64 bytes from lga25s54-in-f206.1e100.net (172.217.6.206): icmp_seq=3 ttl=37 time=13.9 ms
64 bytes from lga25s54-in-f206.1e100.net (172.217.6.206): icmp_seq=4 ttl=37 time=13.7 ms
64 bytes from lga25s54-in-f206.1e100.net (172.217.6.206): icmp_seq=5 ttl=37 time=294 ms
64 bytes from lga25s54-in-f206.1e100.net (172.217.6.206): icmp_seq=6 ttl=37 time=14.0 ms
64 bytes from lga25s54-in-f206.1e100.net (172.217.6.206): icmp_seq=7 ttl=37 time=13.7 ms
64 bytes from lga25s54-in-f206.1e100.net (172.217.6.206): icmp_seq=8 ttl=37 time=13.6 ms
64 bytes from lga25s54-in-f206.1e100.net (172.217.6.206): icmp_seq=9 ttl=37 time=13.8 ms
64 bytes from lga25s54-in-f206.1e100.net (172.217.6.206): icmp_seq=10 ttl=37 time=12.9 ms

--- google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9015ms
rtt min/avg/max/mdev = 12.925/42.447/294.451/84.030 ms
```

# How My Obsession Started

```
root@9472fb8370bd:/# ping -c 10 google.com
PING google.com (172.217.6.206) 56(84) bytes of data.
64 bytes from lga25s54-in-f206.1e100.net (172.217.6.206): icmp_seq=1 ttl=37 time=20.9 ms
64 bytes from lga25s54-in-f206.1e100.net (172.217.6.206): icmp_seq=2 ttl=37 time=13.2 ms
64 bytes from lga25s54-in-f206.1e100.net (172.217.6.206): icmp_seq=3 ttl=37 time=13.9 ms
64 bytes from lga25s54-in-f206.1e100.net (172.217.6.206): icmp_seq=4 ttl=37 time=13.7 ms
64 bytes from lga25s54-in-f206.1e100.net (172.217.6.206): icmp_seq=5 ttl=37 time=294 ms
64 bytes from lga25s54-in-f206.1e100.net (172.217.6.206): icmp_seq=6 ttl=37 time=14.0 ms
64 bytes from lga25s54-in-f206.1e100.net (172.217.6.206): icmp_seq=7 ttl=37 time=13.9 ms
64 bytes from lga25s54-in-f206.1e100.net (172.217.6.206): icmp_seq=8 ttl=37 time=13.8 ms
64 bytes from lga25s54-in-f206.1e100.net (172.217.6.206): icmp_seq=9 ttl=37 time=13.7 ms
64 bytes from lga25s54-in-f206.1e100.net (172.217.6.206): icmp_seq=10 ttl=37 time=13.7 ms

--- google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9015ms
rtt min/avg/max/mdev = 12.925/42.447/294.451/84.030 ms
```



# Let's Do This A Little Longer

```
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=289 ttl=37 time=15.9 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=290 ttl=37 time=13.4 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=291 ttl=37 time=13.8 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=292 ttl=37 time=13.0 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=293 ttl=37 time=13.1 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=294 ttl=37 time=12.5 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=295 ttl=37 time=13.3 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=296 ttl=37 time=12.9 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=297 ttl=37 time=12.6 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=298 ttl=37 time=18.2 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=299 ttl=37 time=12.9 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=300 ttl=37 time=13.3 ms

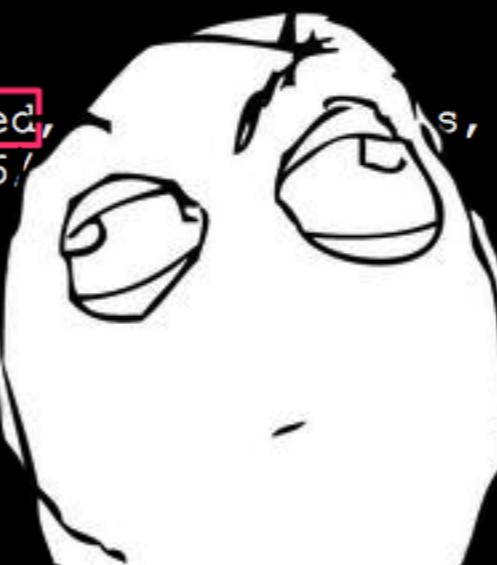
--- google.com ping statistics ---
300 packets transmitted, 297 received, 1% packet loss, time 299638ms
rtt min/avg/max/mdev = 12.145/13.656/28.737/2.012 ms
```

# Let's Do This A Little Longer

```
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=289 ttl=37 time=15.9 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=290 ttl=37 time=13.4 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=291 ttl=37 time=13.8 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=292 ttl=37 time=13.0 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=293 ttl=37 time=13.1 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=294 ttl=37 time=12.5 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=295 ttl=37 time=13.3 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=296 ttl=37 time=12.9 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=297 ttl=37 time=12.6 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=298 ttl=37 time=18.2 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=299 ttl=37 time=12.9 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): icmp_seq=300 ttl=37 time=13.3 ms
```

```
--- google.com ping statistics ---
```

```
300 packets transmitted, 297 received, 0% packet loss, time 299638ms
rtt min/avg/max/mdev = 12.145/13.656/
```

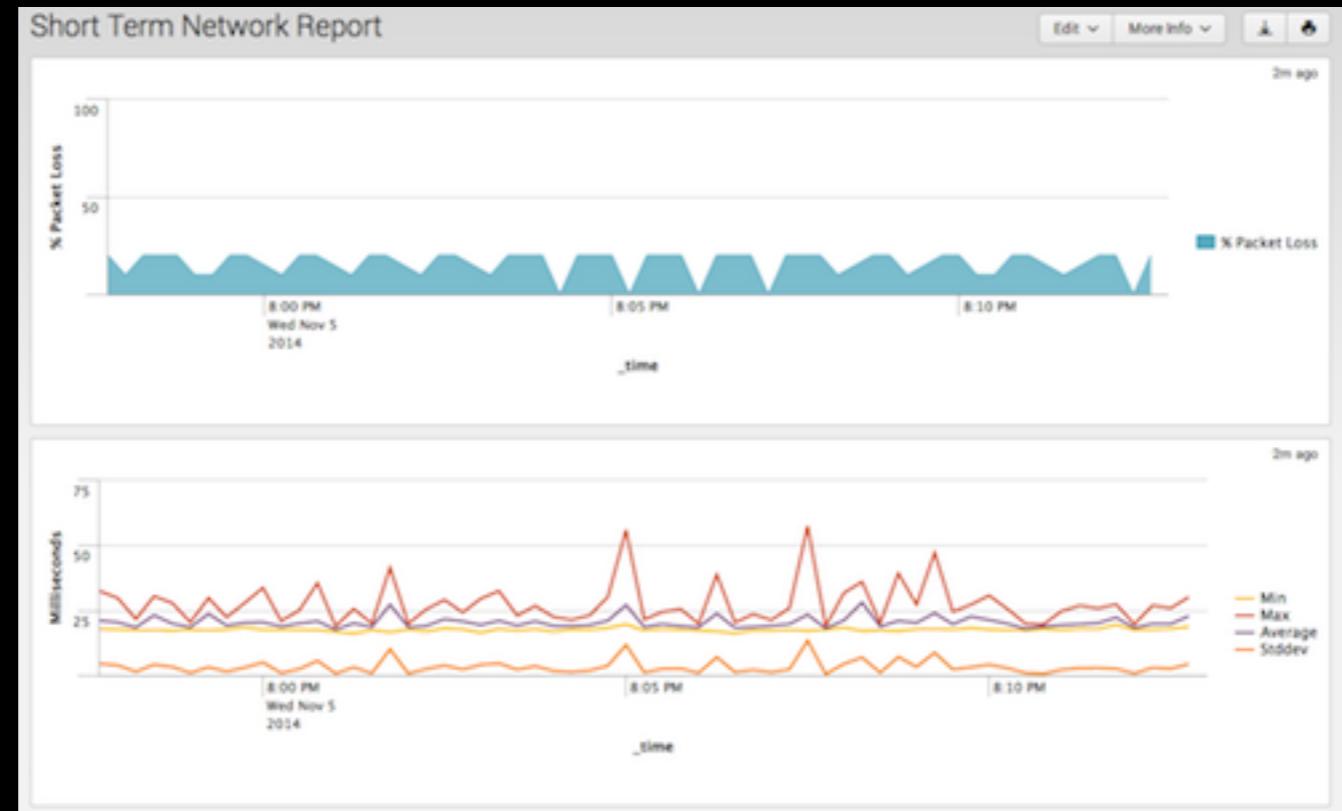


# How About MTR?

```
Sat Oct 20 13:55:18 EDT 2018
Running 'mtr -4 --report --report-cycles 10 google.com'...
Start: Sat Oct 20 13:55:18 2018
HOST: CheetahCollector.localdomain Loss% Snt Last Avg Best Wrst StDev
 1.|-- ubnt           0.0% 10  0.6  0.5  0.4  0.6  0.0
 2.|-- 10.0.0.1        0.0% 10  0.7  1.0  0.7  1.4  0.0
 3.|-- 96.120.76.109   0.0% 10  8.6  8.6  7.3  11.0 0.9
 4.|-- xe-10-2-0-32767-sur01.bal 0.0% 10 11.6  8.6  7.7  11.6 1.1
 5.|-- be-8-ar03.newcastle.de.pa 0.0% 10  9.5 10.0  9.2  11.6 0.5
 6.|-- be-202-ar03.ivyland.pa.pa 0.0% 10  9.6 10.0  9.1  12.2 0.8
 7.|-- 69.241.64.98      0.0% 10 11.4 12.3 11.3 13.7 0.5
 8.|-- ???            100.0 10  0.0  0.0  0.0  0.0  0.0
 9.|-- 108.170.227.210   0.0% 10 12.1 12.9 11.9 17.2 1.5
10.|-- 108.170.248.99   0.0% 10 12.2 13.5 11.7 20.7 2.6
11.|-- 209.85.255.52     0.0% 10 13.3 13.4 12.8 14.5 0.3
12.|-- 209.85.254.138   0.0% 10 12.8 14.7 12.6 20.9 2.8
13.|-- 108.170.248.1     0.0% 10 14.1 14.3 13.3 14.9 0.3
14.|-- 72.14.234.65      0.0% 10 14.8 13.6 12.4 14.8 0.5
15.|-- lga25s61-in-f14.1e100.net 0.0% 10 13.4 12.9 12.3 13.6 0.0
```

- MTR was a nice idea, but ultimately didn't pan out

# My First Attempt With Splunk



- You had to install Splunk manually
- Reproducible builds were a challenge

# Docker to the Rescue!



# Docker to the Rescue!

- Docker lets you partition processes (and filesystems) from each other.

# Docker to the Rescue!

- Docker lets you partition processes (and filesystems) from each other.
- I wanted something easy to stand up

# Docker to the Rescue!

- Docker lets you partition processes (and filesystems) from each other.
- I wanted something easy to stand up
- I wanted something my manager could stand up (he has)

# Docker to the Rescue!

- Docker lets you partition processes (and filesystems) from each other.
- I wanted something easy to stand up
- I wanted something my manager could stand up (he has)
- ```
docker run -p 8000:8000 \
-v $(pwd)/splunk-data:/opt/splunk/var/lib/splunk/defaultdb \
dmuth1/splunk-network-health-check
```

# Let's Monitor Multiple Hosts

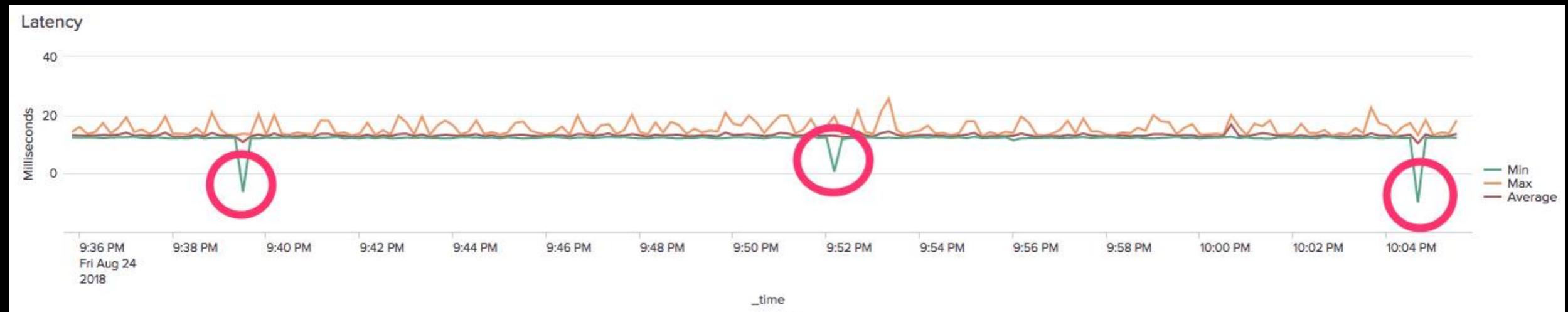
- Ping had issues
- Could only ping one host at a time
- Pinging multiple hosts created spikes in load every 10 seconds when the process exited and was restarted.
- ...and that's no good. This is meant to be run on laptops!

# Maybe fping is a good idea?

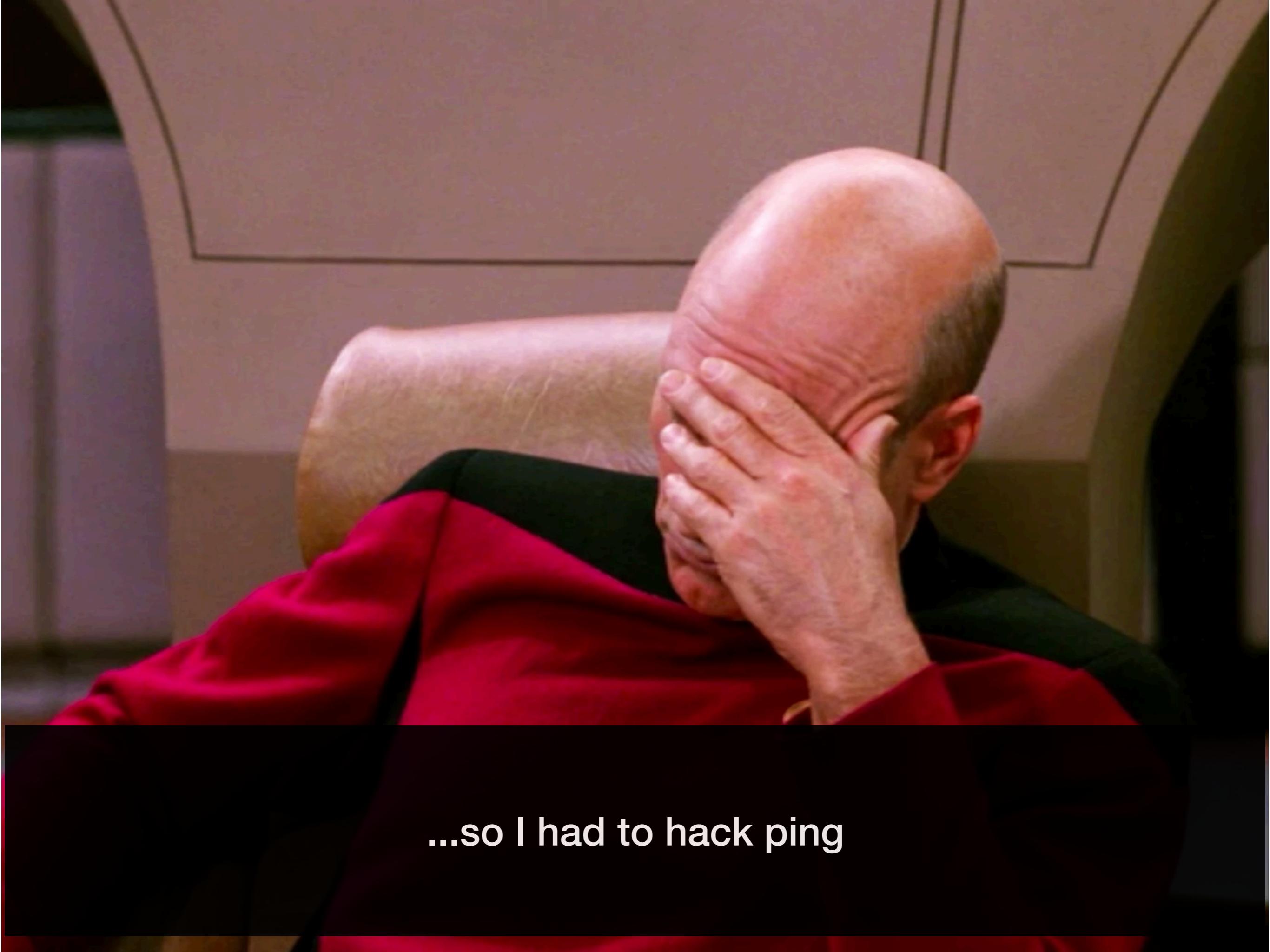
```
[CheetahCollector:~] $ fping -c 4 1.1.1.1 8.8.8.8 google.com cnn.com
1.1.1.1    : [0], 84 bytes, 12.7 ms (12.7 avg, 0% loss)
8.8.8.8    : [0], 84 bytes, 12.5 ms (12.5 avg, 0% loss)
google.com  : [0], 84 bytes, 12.4 ms (12.4 avg, 0% loss)
cnn.com    : [0], 84 bytes, 11.8 ms (11.8 avg, 0% loss)
1.1.1.1    : [1], 84 bytes, 12.1 ms (12.4 avg, 0% loss)
8.8.8.8    : [1], 84 bytes, 11.6 ms (12.1 avg, 0% loss)
google.com  : [1], 84 bytes, 12.2 ms (12.3 avg, 0% loss)
cnn.com    : [1], 84 bytes, 11.6 ms (11.7 avg, 0% loss)
1.1.1.1    : [2], 84 bytes, 12.1 ms (12.3 avg, 0% loss)
8.8.8.8    : [2], 84 bytes, 12.8 ms (12.3 avg, 0% loss)
google.com  : [2], 84 bytes, 11.9 ms (12.2 avg, 0% loss)
cnn.com    : [2], 84 bytes, 11.6 ms (11.7 avg, 0% loss)
1.1.1.1    : [3], 84 bytes, 12.2 ms (12.2 avg, 0% loss)
8.8.8.8    : [3], 84 bytes, 12.1 ms (12.3 avg, 0% loss)
google.com  : [3], 84 bytes, 19.9 ms (14.1 avg, 0% loss)
cnn.com    : [3], 84 bytes, 11.7 ms (11.7 avg, 0% loss)

1.1.1.1    : xmt/rcv/%loss = 4/4/0%, min/avg/max = 12.1/12.2/12.7
8.8.8.8    : xmt/rcv/%loss = 4/4/0%, min/avg/max = 11.6/12.3/12.8
google.com  : xmt/rcv/%loss = 4/4/0%, min/avg/max = 11.9/14.1/19.9
cnn.com    : xmt/rcv/%loss = 4/4/0%, min/avg/max = 11.6/11.7/11.8
```

# Maybe fping is a good idea?



- ...if you like time travel!

A close-up photograph of a man with a shaved head, wearing a dark green jacket over a red shirt. He is sitting in a light-colored armchair, holding his head in his hands with his fingers covering his eyes. His expression appears to be one of distress or exhaustion. The background is a plain, light-colored wall.

...so I had to hack ping

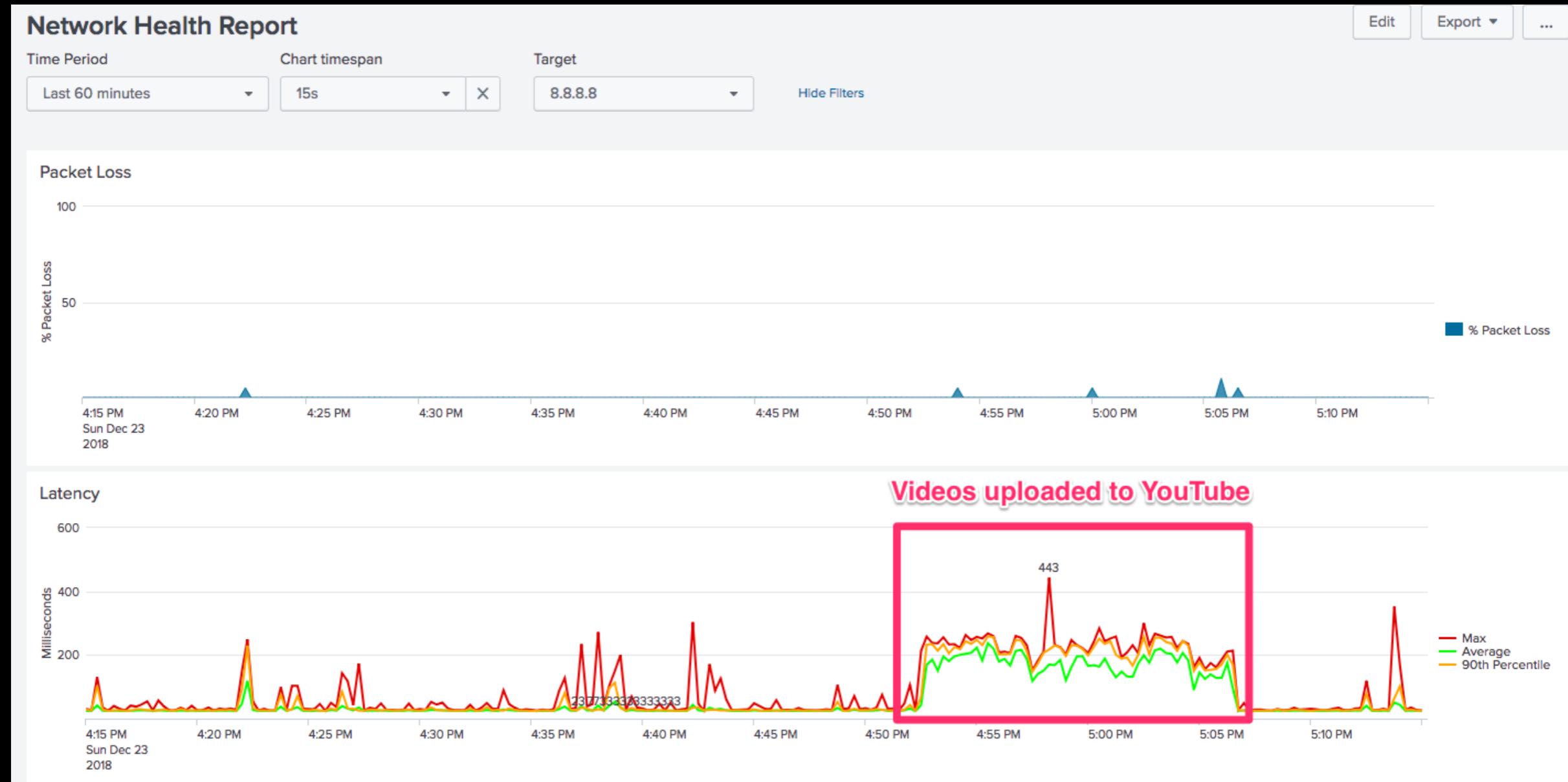
# How ping behaves now

```
root@9472fb8370bd:/mnt/splunk-app/bin# /iputils/ping google.com
PING google.com (172.217.11.46) 56(84) bytes of data.
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): target=google.com icmp_seq=1 ttl=37 time=12.7 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): target=google.com icmp_seq=2 ttl=37 time=12.9 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): target=google.com icmp_seq=3 ttl=37 time=13.1 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): target=google.com icmp_seq=4 ttl=37 time=14.5 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): target=google.com icmp_seq=5 ttl=37 time=12.6 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): target=google.com icmp_seq=6 ttl=37 time=12.9 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): target=google.com icmp_seq=7 ttl=37 time=12.9 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): target=google.com icmp_seq=8 ttl=37 time=14.6 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): target=google.com icmp_seq=9 ttl=37 time=12.10 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): target=google.com icmp_seq=10 ttl=37 time=12.8 ms
target=google.com transmitted=10 received=10
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): target=google.com icmp_seq=11 ttl=37 time=12.8 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): target=google.com icmp_seq=12 ttl=37 time=13.5 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): target=google.com icmp_seq=13 ttl=37 time=13.6 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): target=google.com icmp_seq=14 ttl=37 time=12.3 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): target=google.com icmp_seq=15 ttl=37 time=20.9 ms
64 bytes from lga25s61-in-f14.1e100.net (172.217.11.46): target=google.com icmp_seq=16 ttl=37 time=12.2 ms
```

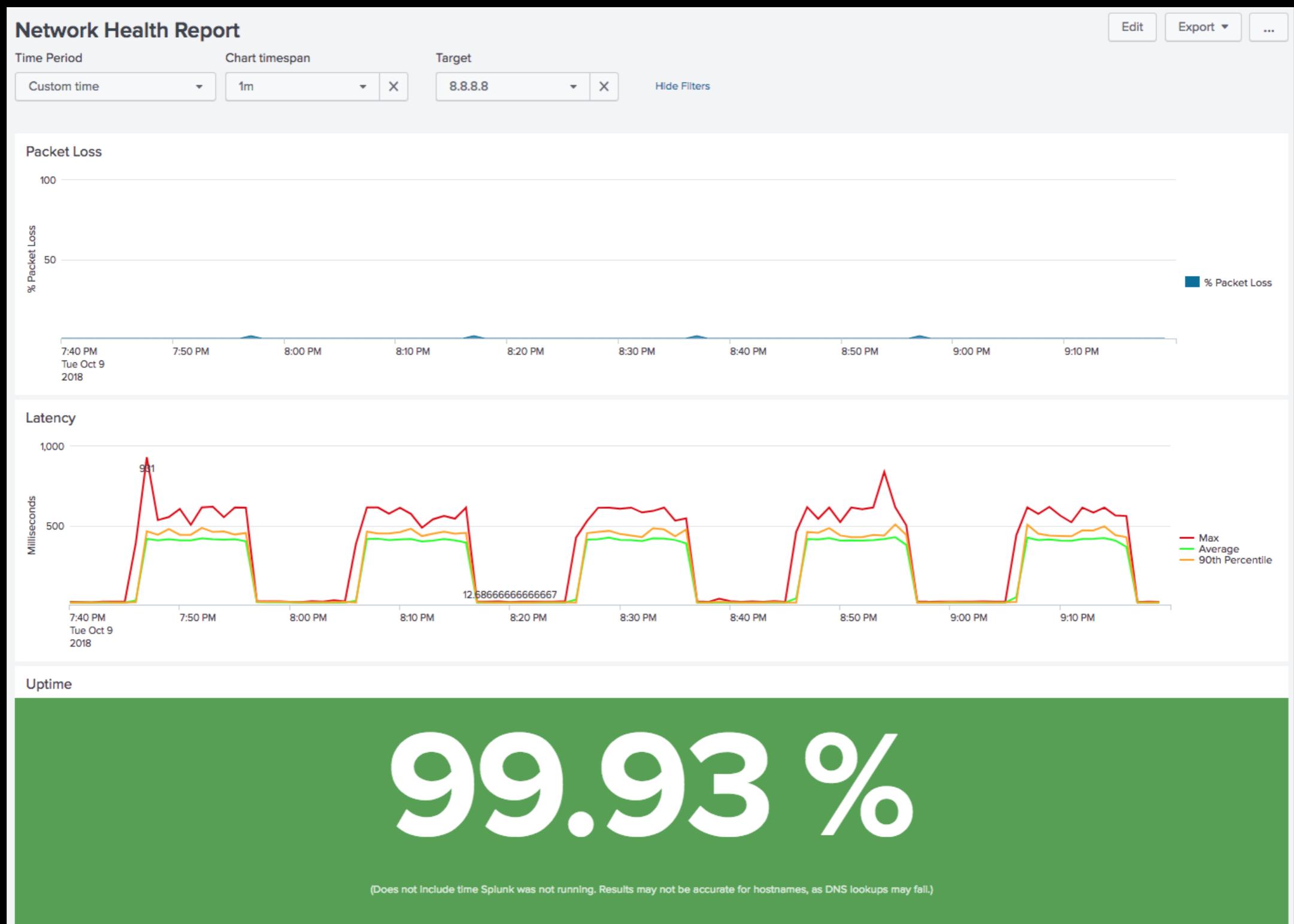
- Runs normally, but prints a checkpoint every 10 s
- Also lets me track individual packets, get percentiles, etc.

# In The Real World

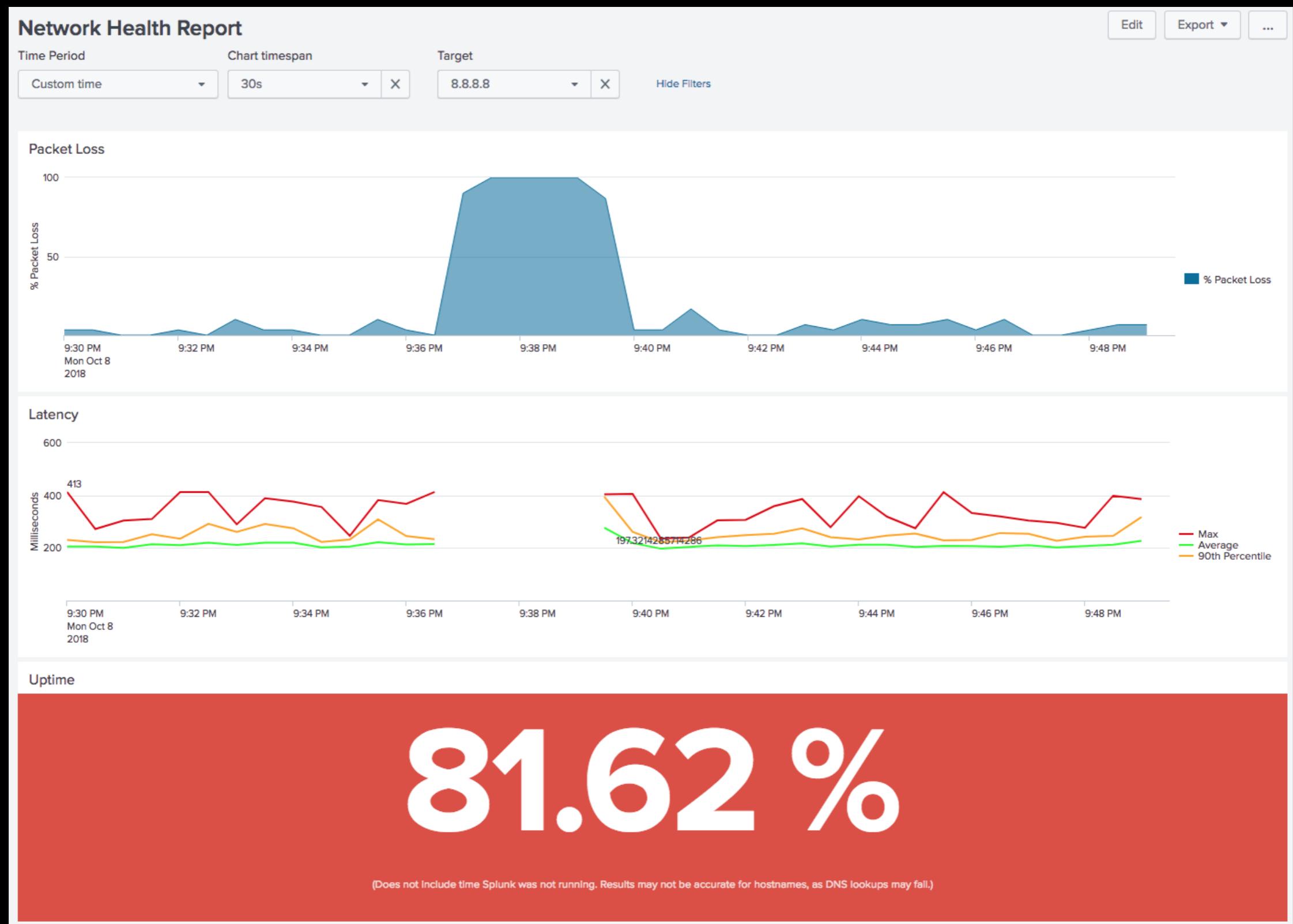
# Uploading Video to YouTube



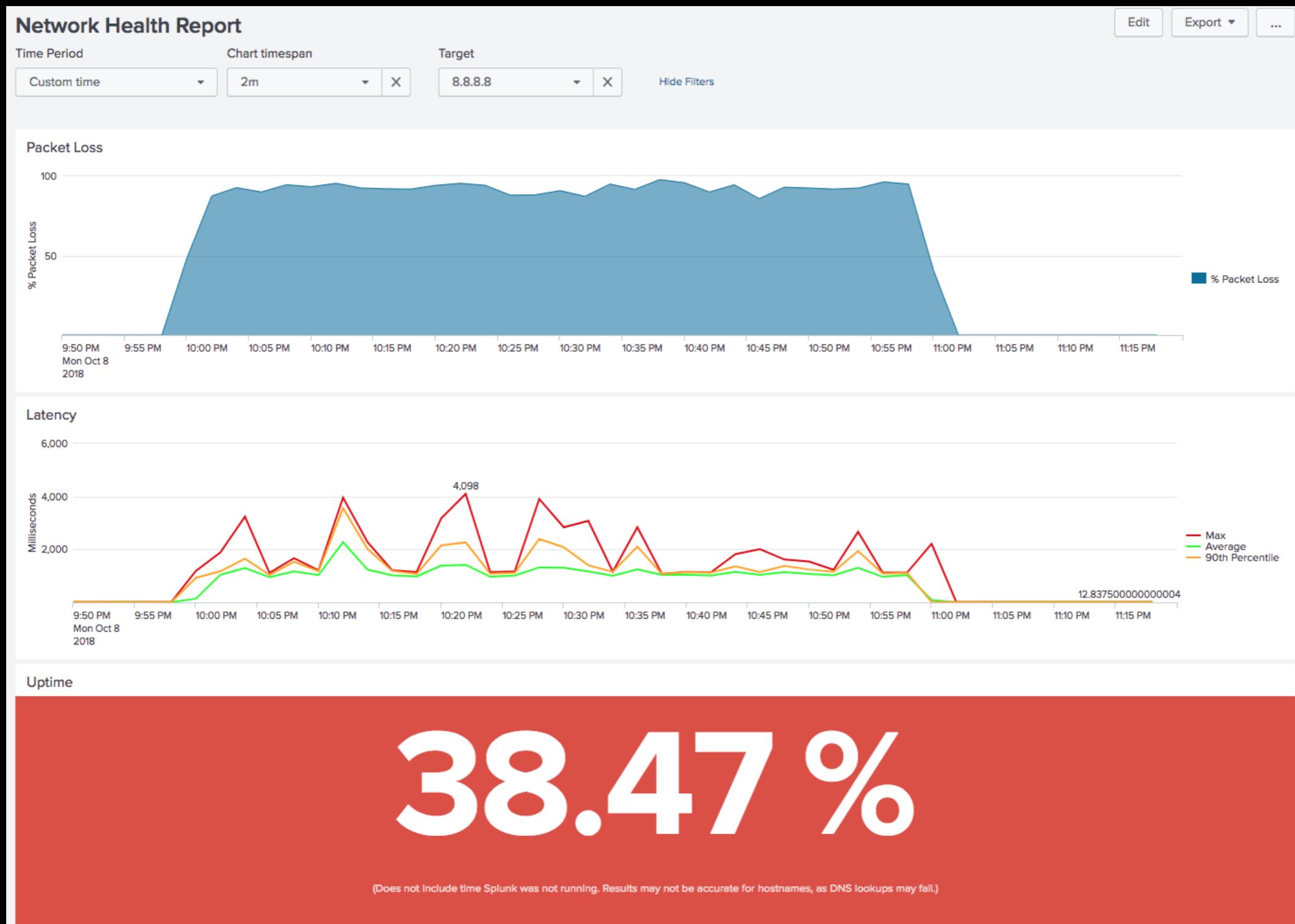
# When Firewalls Go Bad



# Train Tunnels



# Internet Outages





# Live Demo

# What Comes Next?

- Support for TCP/UDP ports?
- Support for HTTP/HTTPS?
  - ...less often than once per second?

# Additional Resources

- [github.com/dmuth/splunk-network-health-check](https://github.com/dmuth/splunk-network-health-check)
- [github.com/dmuth/splunk-lab](https://github.com/dmuth/splunk-lab)
- [github.com/dmuth/presentations](https://github.com/dmuth/presentations)
- [docker.com](https://docker.com)
- Twitter: @dmuth
- Web: <http://www.dmuth.org/>

# Questions?