Pingbeat:
Y'know, for pings!

Joshua Rich
Technical Support
Engineer
February 2016

elastic


U.B. B

Ping theory

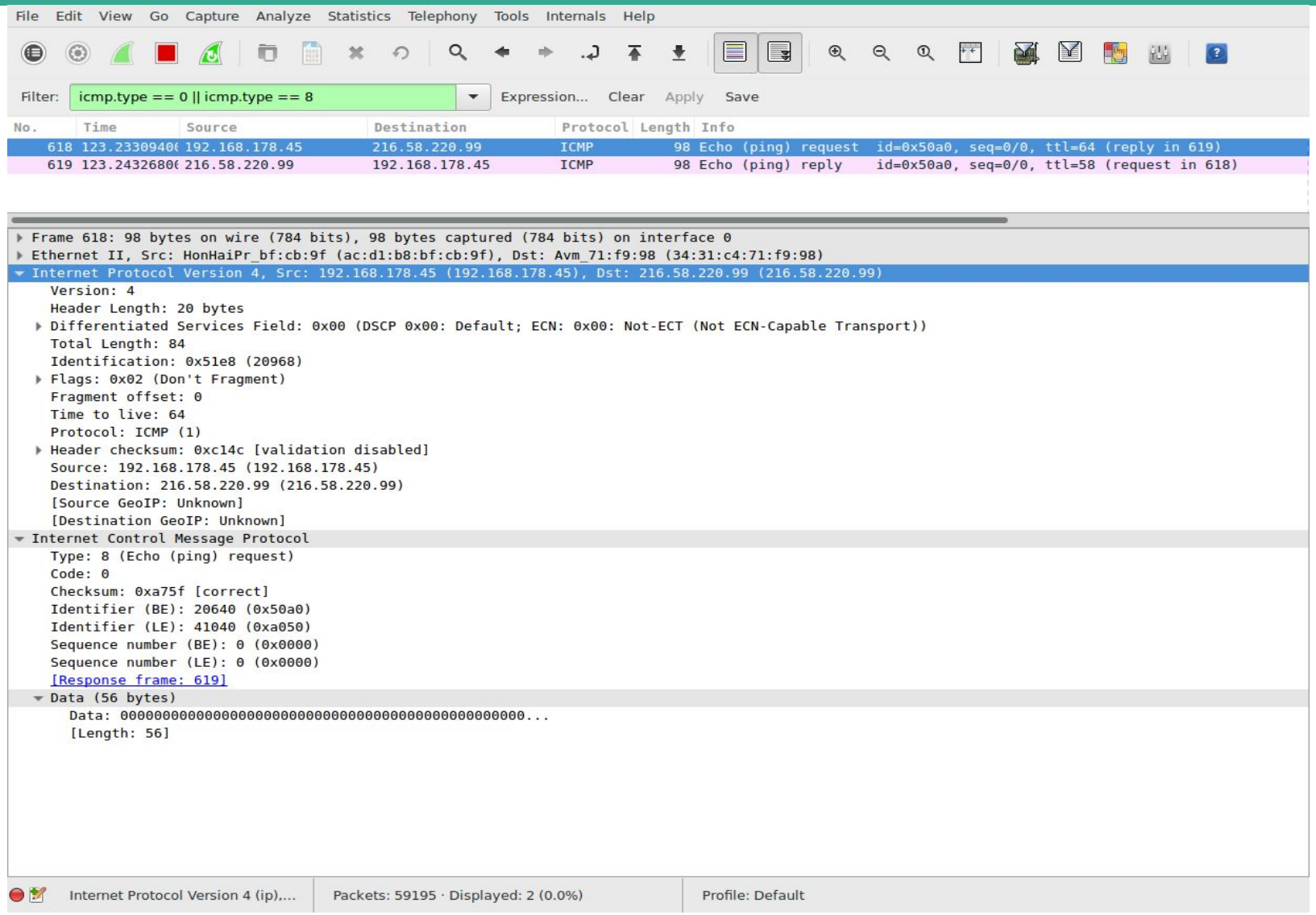
1. Source creates an ICMP *echo-request* and sends this to the target.
   a. Contains an ***identifier*** and ***sequence number*** to keep track of this specific ping request
2. Source records the timestamp of when the *echo-request* was sent.
3. Target receives the source *echo-request* and creates their own ICMP *echo-reply*, sending this back to the source.
   a. Contains the ***identifier*** and ***sequence number*** in addition to a timestamp of when the message was sent back.
4. Source receives the *echo-reply* and calculates Round-Trip Time (RTT) based on recorded timestamps.

What happens if the target doesn't respond?

- Requests are retried after a configured timeout period.
- After configured number of retries, source gives up and records packet loss.

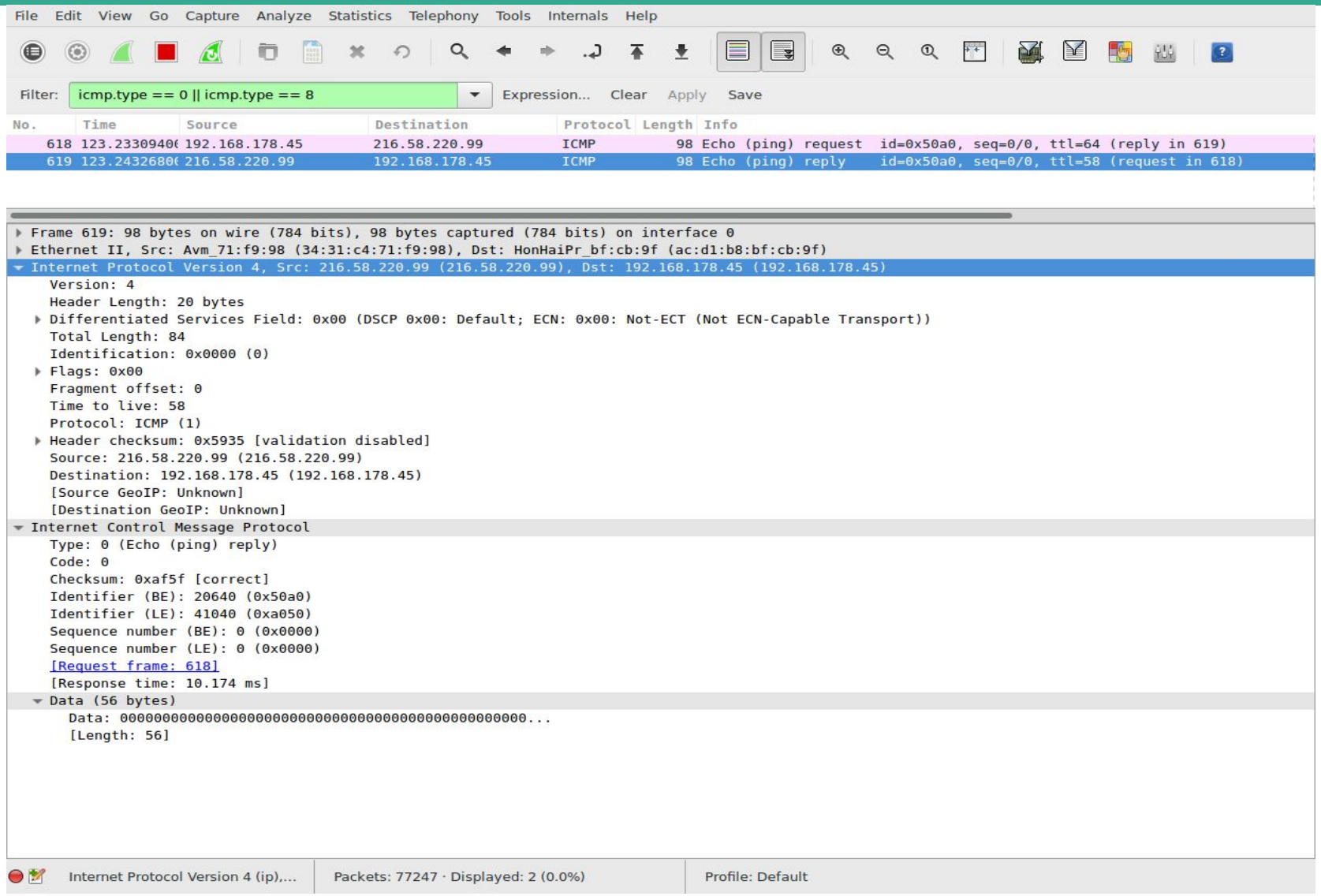
Copyright Elastic 2015 Copying, publishing and/or distributing without written permission is strictly prohibited

ICMP *echo-request* in Wireshark



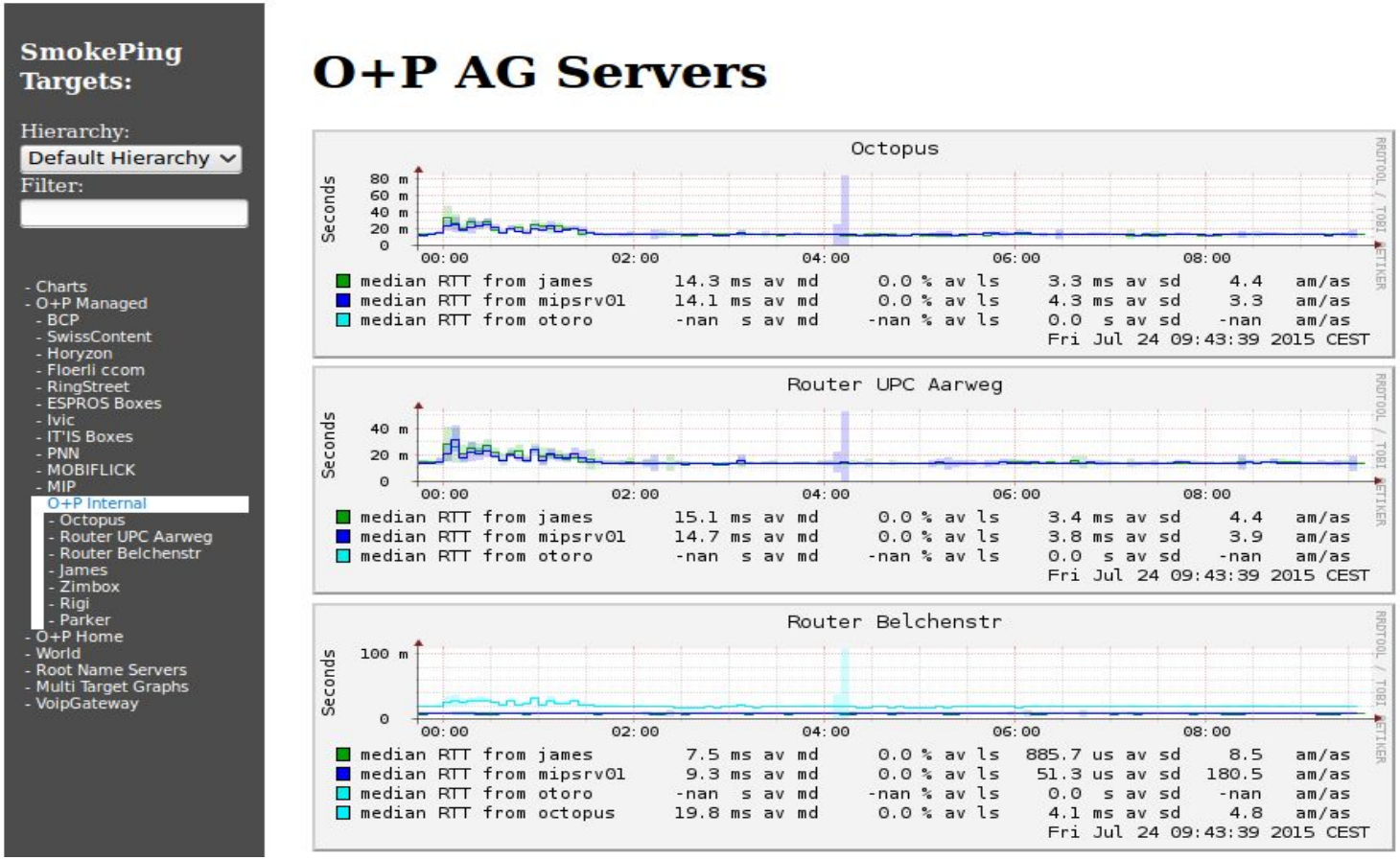
Copyright Elastic 2015 Copying, publishing and/or distributing without written permission is strictly prohibited

ICMP *echo-reply* in Wireshark



Copyright Elastic 2015 Copying, publishing and/or distributing without written permission is strictly prohibited

Inspiration



Smokeping - the venerable goto network monitor in NOCs...

Copyright Elastic 2015 Copying, publishing and/or distributing without written permission is strictly prohibited

Pingbeat

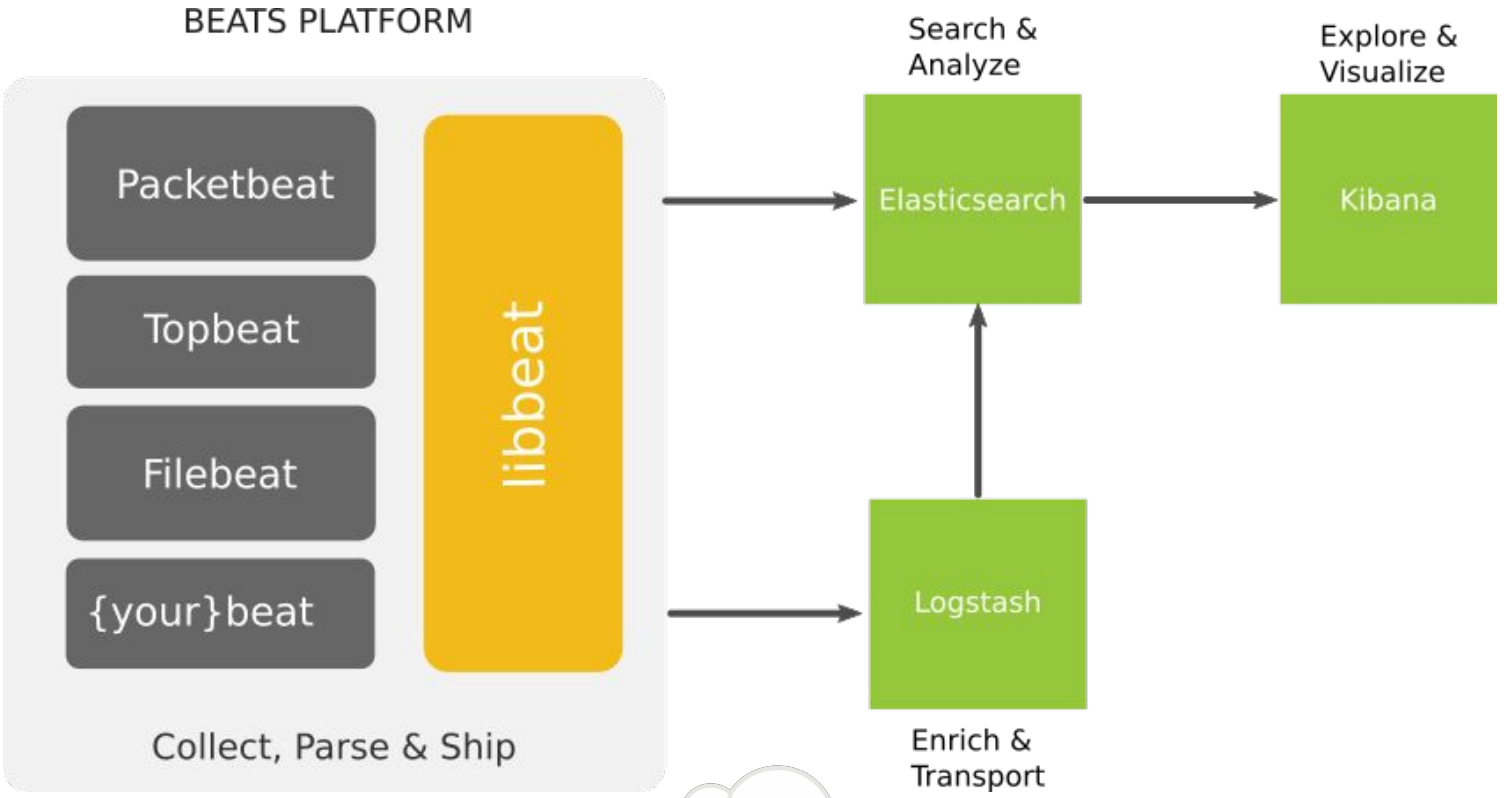
A lightweight network monitoring probe

(based on)

Copyright Elastic 2015 Copying, publishing and/or distributing without written permission is strictly prohibited

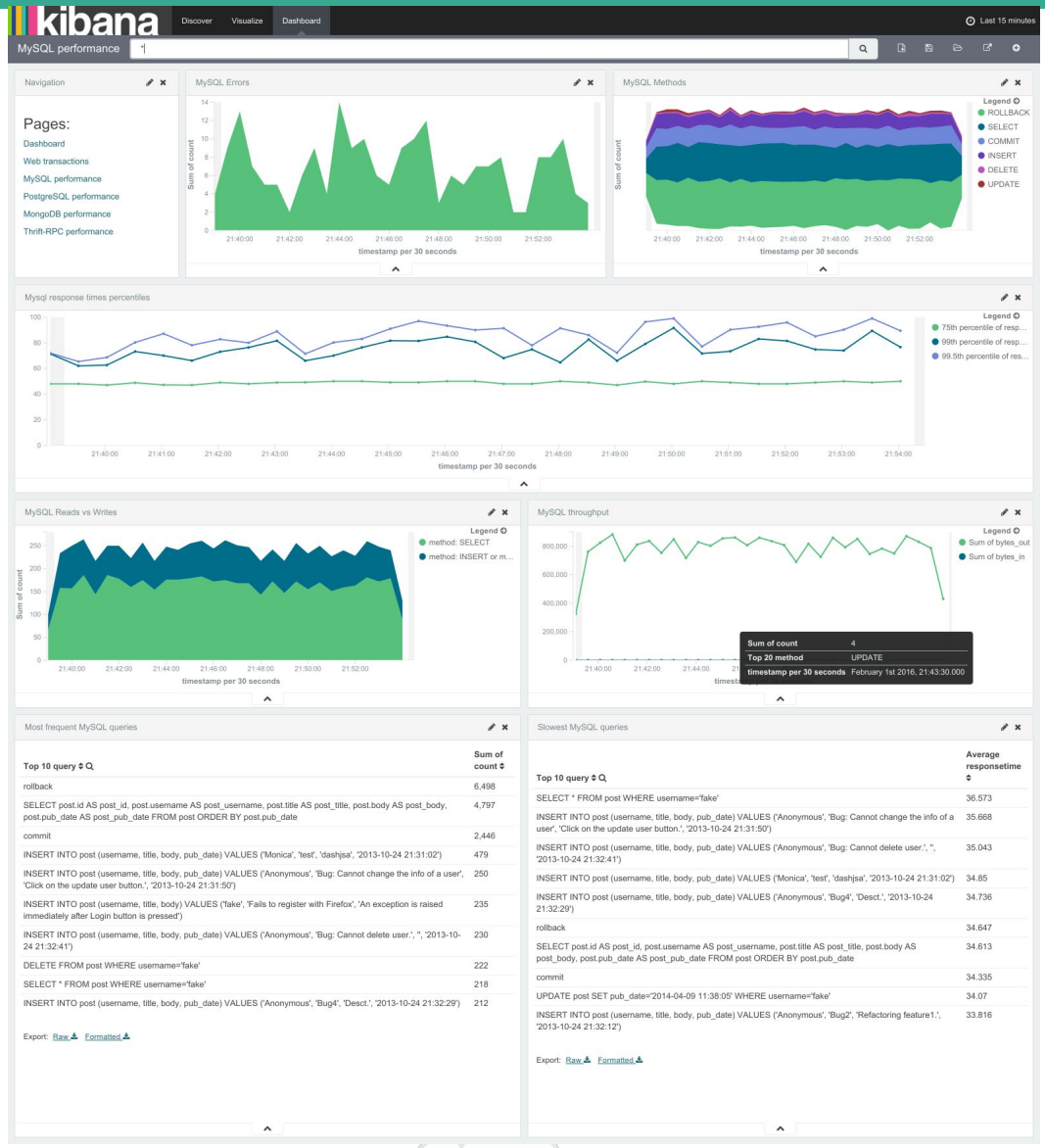
What are beats?

- Beats are lightweight shippers that capture all sorts of operational data from your servers and ship it to Logstash and Elasticsearch.
- They use a common open-source platform, libbeat, that makes it easy to write your own beat.
- Written in Go.
- Designed to be small on memory and CPU.



Copyright Elastic 2015 Copying, publishing and/or distributing without written permission is strictly prohibited

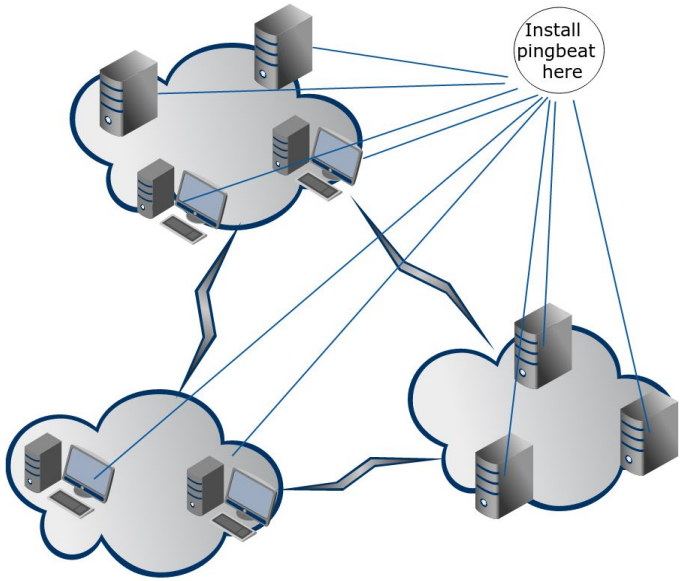
Check out a demo at demo.elastic.co!



Copyright Elastic 2015 Copying, publishing and/or distributing without written permission is strictly prohibited

What is Pingbeat?

- Complement the packetbeat high-level application protocol analysis with more low-level network protocol metrics.
- Single binary, single YAML config file needed (easy to deploy).
- Supports any outputs that libbeats supports.
  - e.g., Elasticsearch, Logstash, Redis and file outputs.
- No need to install Logstash for each probe! Just one binary and one config file!
- Small memory footprint (10-15 MB RSS) and fast ping response.
- Ideally install in many places in your network to get a world-view of latency across the network.



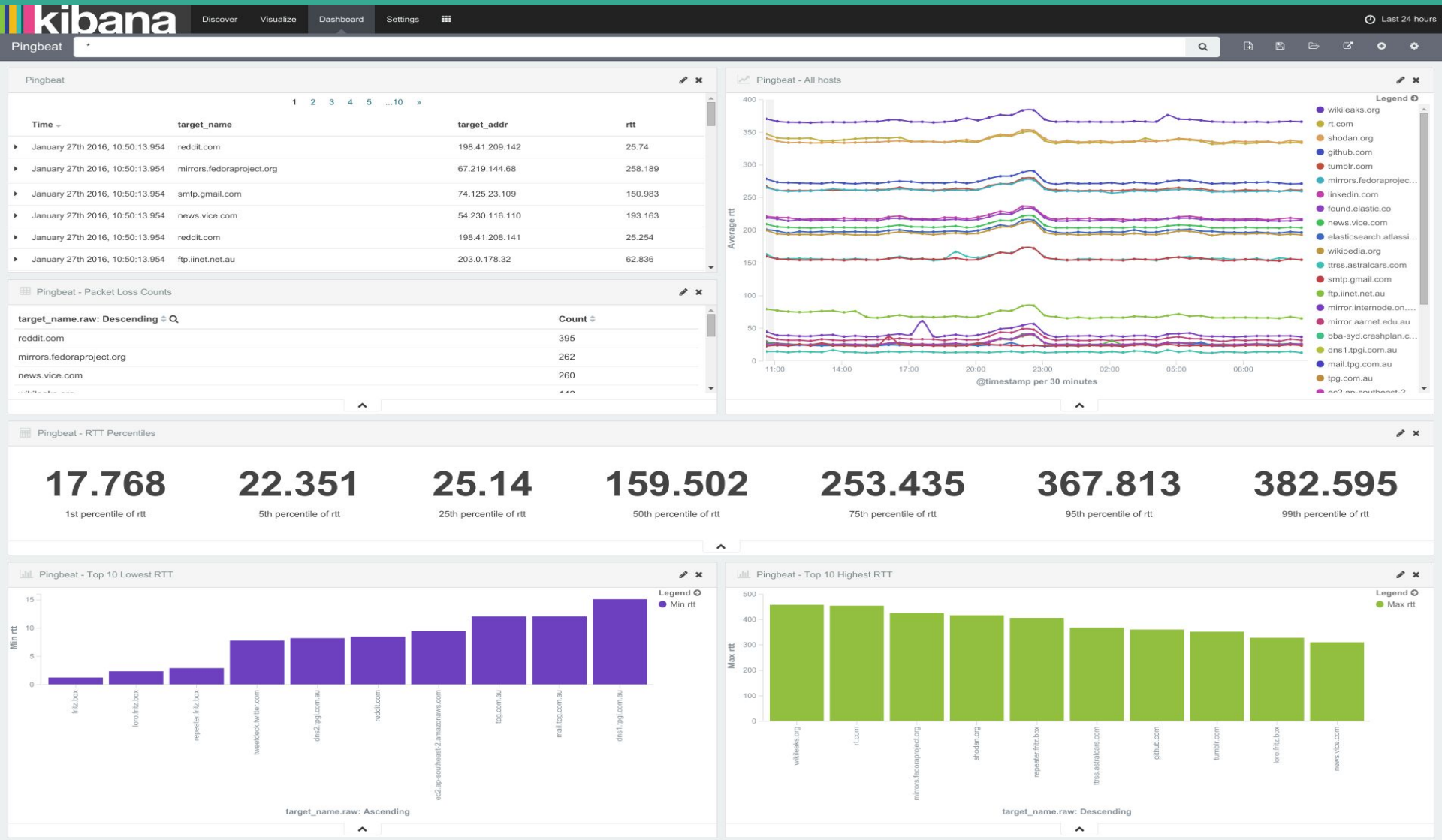
Available now!

https://github.com/joshuar/pingbeat

go get github.com/joshuar/pingbeat

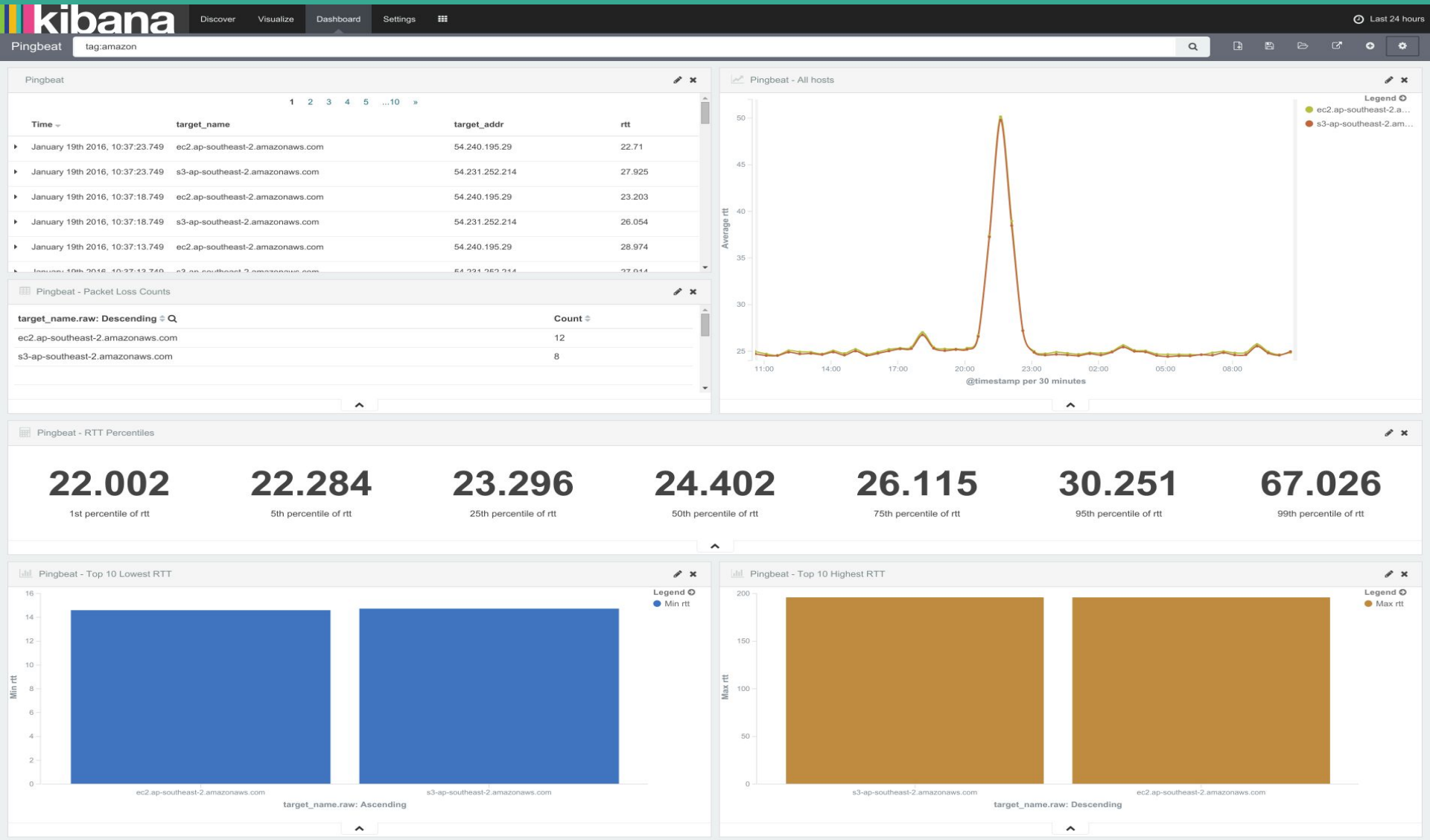
Copyright Elastic 2015 Copying, publishing and/or distributing without written permission is strictly prohibited

Pingbeat Dashboard



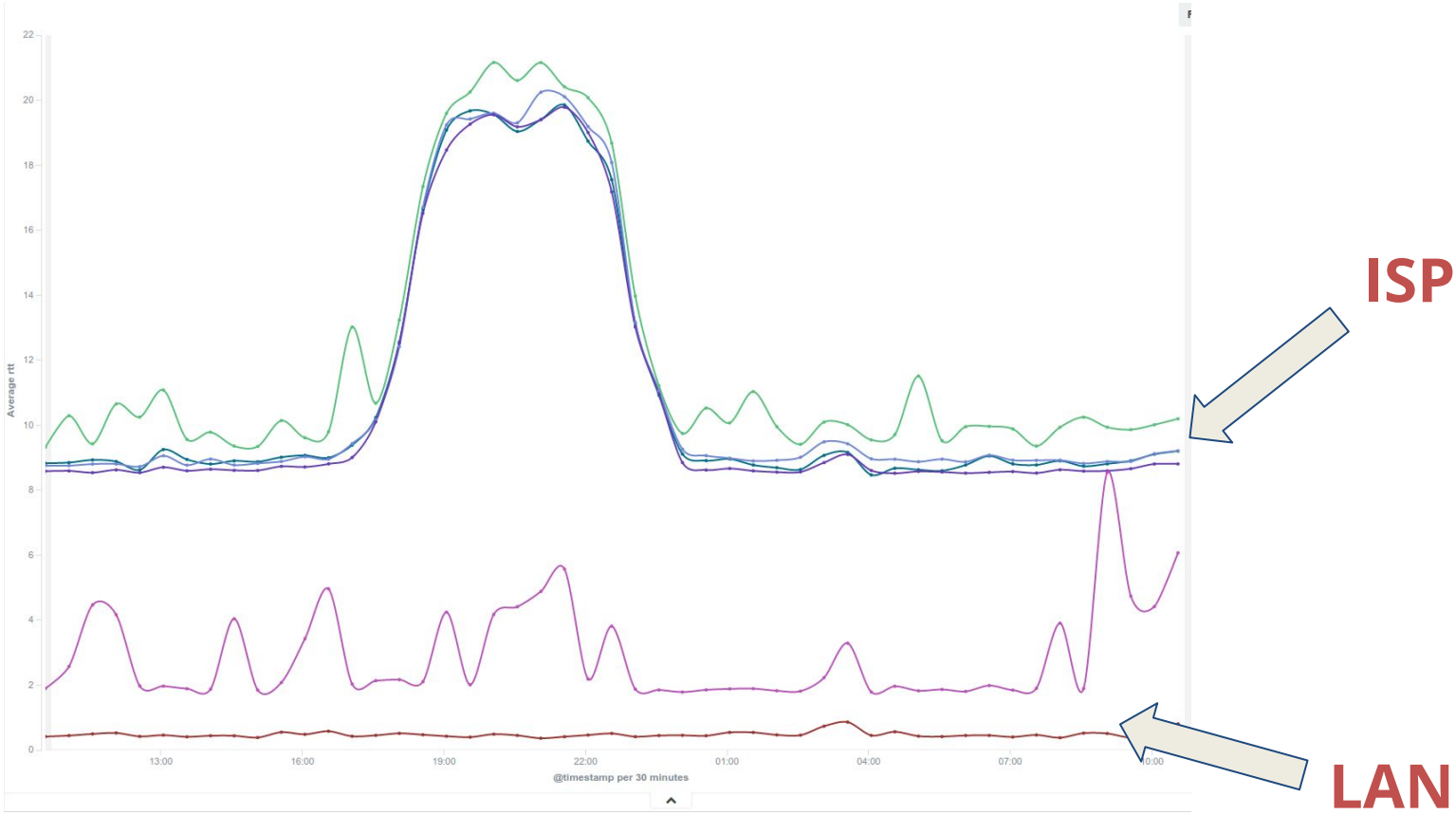
Copyright Elastic 2015 Copying, publishing and/or distributing without written permission is strictly prohibited

Pingbeat Dashboard



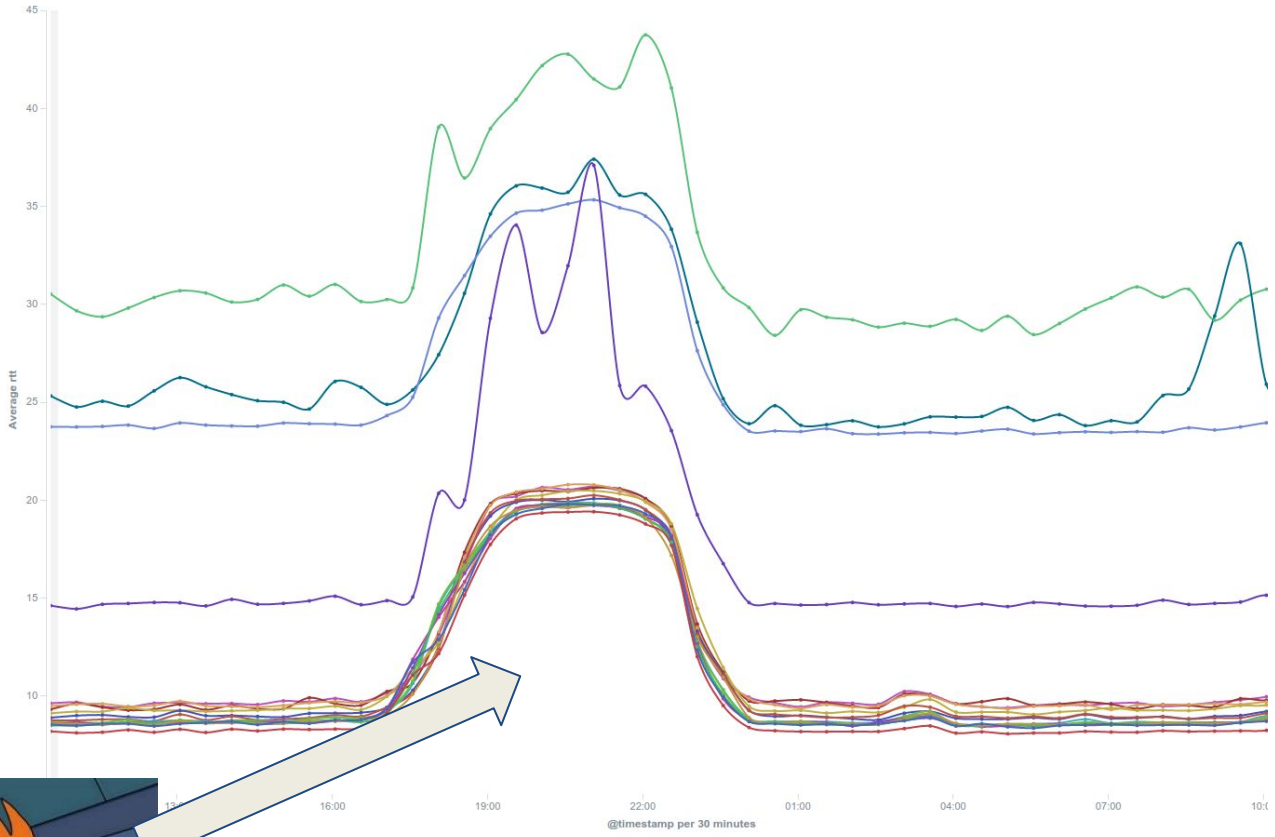
Copyright Elastic 2015 Copying, publishing and/or distributing without written permission is strictly prohibited

Filtering to my LAN and ISP hosts...



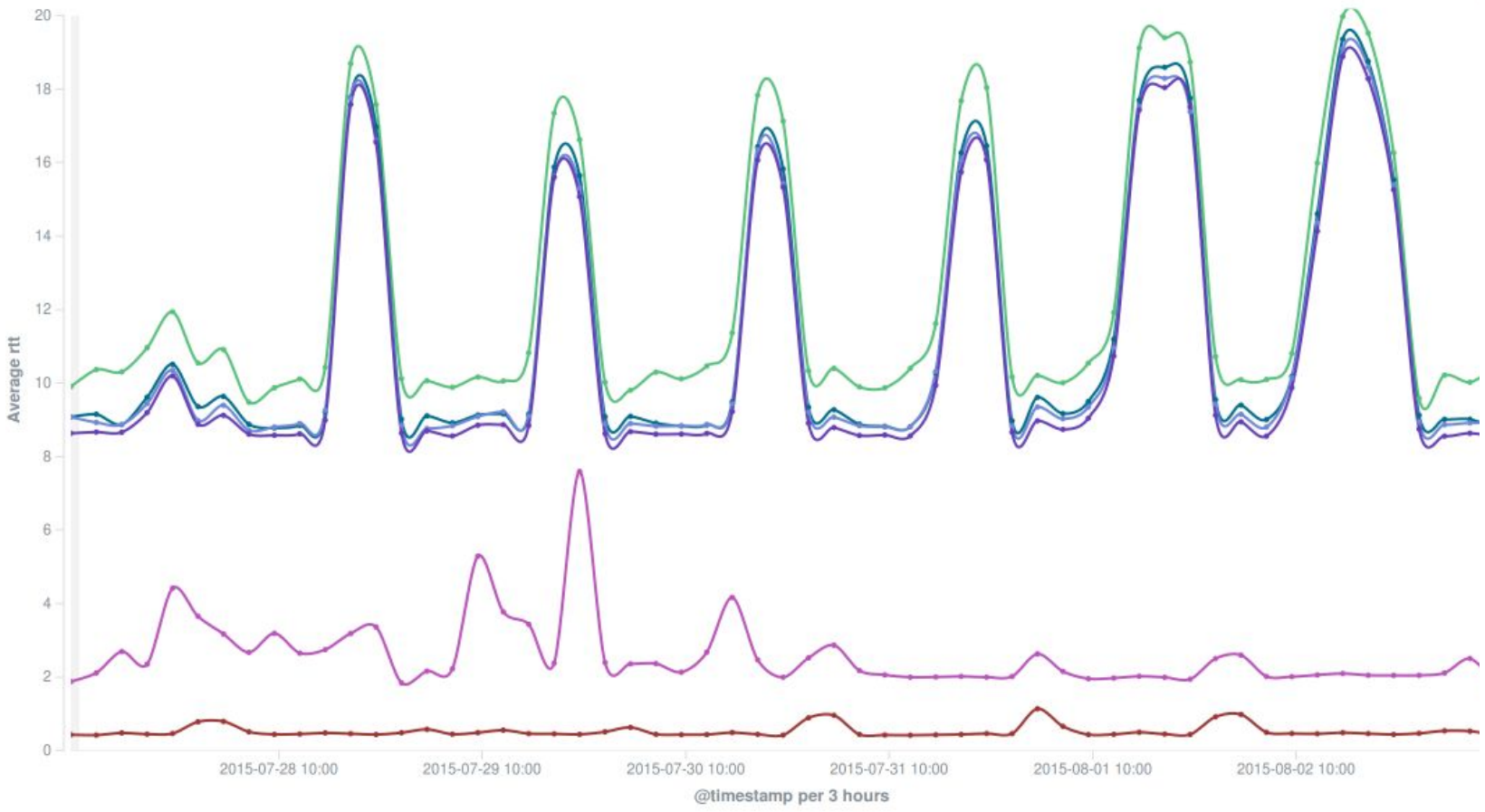
Copyright Elastic 2015 Copying, publishing and/or distributing without written permission is strictly prohibited

Filtering to everything else…



Copyright Elastic 2015 Copying, publishing and/or distributing without written permission is strictly prohibited

The Netflix effect...



Copyright Elastic 2015 Copying, publishing and/or distributing without written permission is strictly prohibited

If you like Pingbeat, you may also like:

- **Unifedbeat**
  - https://github.com/cleesmith/unifiedbeat
  - *Index into ElasticSearch the alert records from network intrusion detection software.*
- **Nagioscheckbeat**
  - https://github.com/PhaedrusTheGreek/nagioscheckbeat
  - *Index Nagios checks into Elasticsearch*
- **Factbeat**
  - https://github.com/jarpy/factbeat
  - *Ship Facter facts to Elasticsearch*
- **Hsbeat**
  - https://github.com/YaSuenag/hsbeat
  - *Index JVM stats/metrics to Elasticsearch*

Copyright Elastic 2015 Copying, publishing and/or distributing without written permission is strictly prohibited

Want to learn more?

Tutorial: The Power of Open Data with ELK

Thursday 10:40am, D2.211

elastic