Team USA & Friends

Monitoring DNS Propagation Times

Team USA & Friends

USA

Merc

Shane

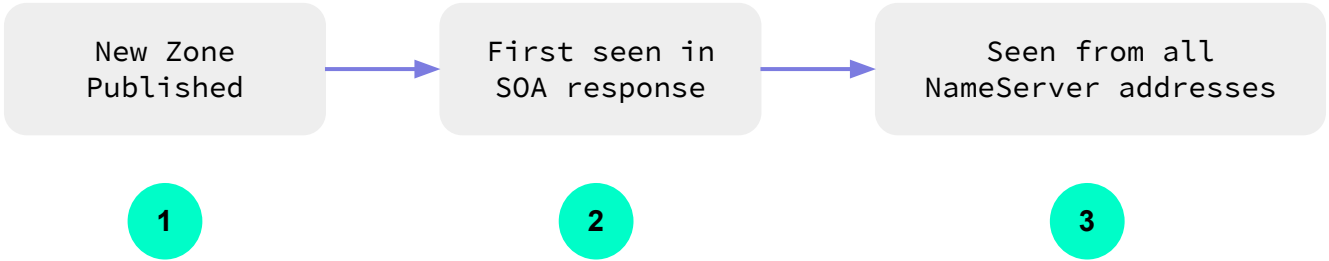
Friends

Tom

Kai

How consistent is DNS?

Mapping dns propagation times



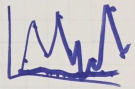
Mapping dns propagation times

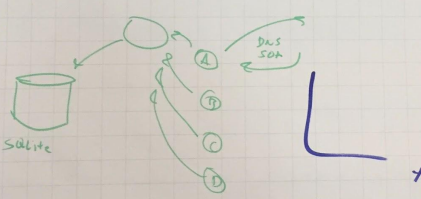
GOALS

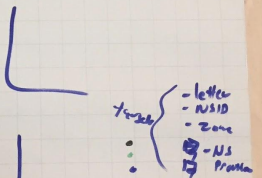
- ~~MULTIPLE SITES~~
- ✓ ARBITRARY DOMAINS (ANY# RECORDS?)
- VISUALIZATION
- ✓ COMPARE w/ OTHER DATA SETS
- ✓ ROBUSTNESS ☺
- ✓ PER-MACHINE INFO

ZONE

SRC IP (NSID, DST IP); serial 1 2; time first 10 21; time last ~~35~~ 22 21



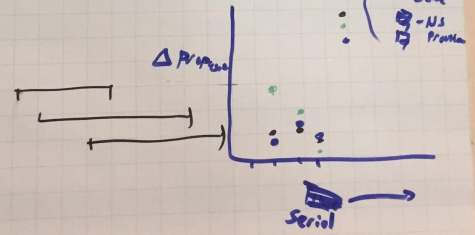




- letter
- NSID
- zone
- NS
- Prefix

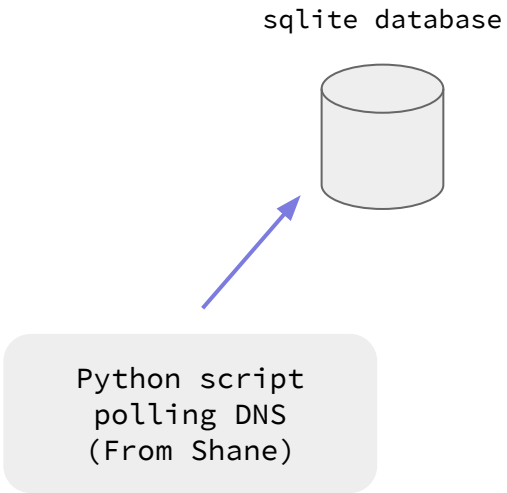
- time
- target
- propagation Δ
- instance
-

A
D
C
.
.

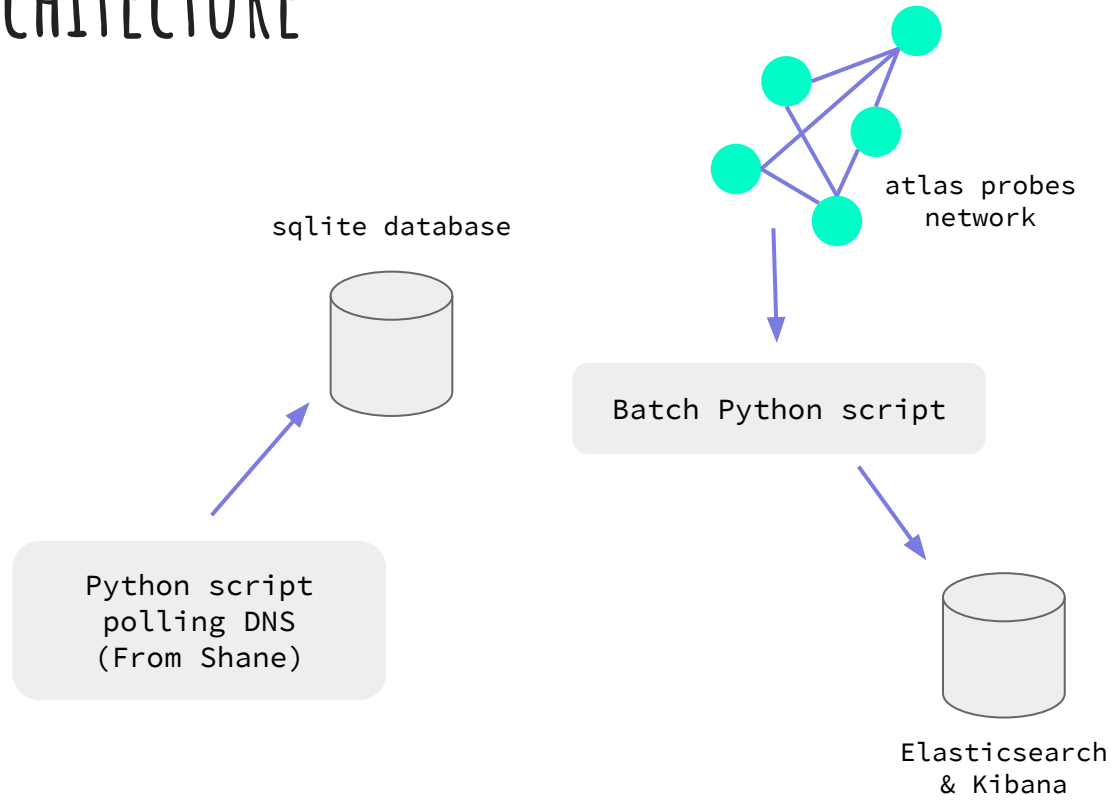


STAPLES

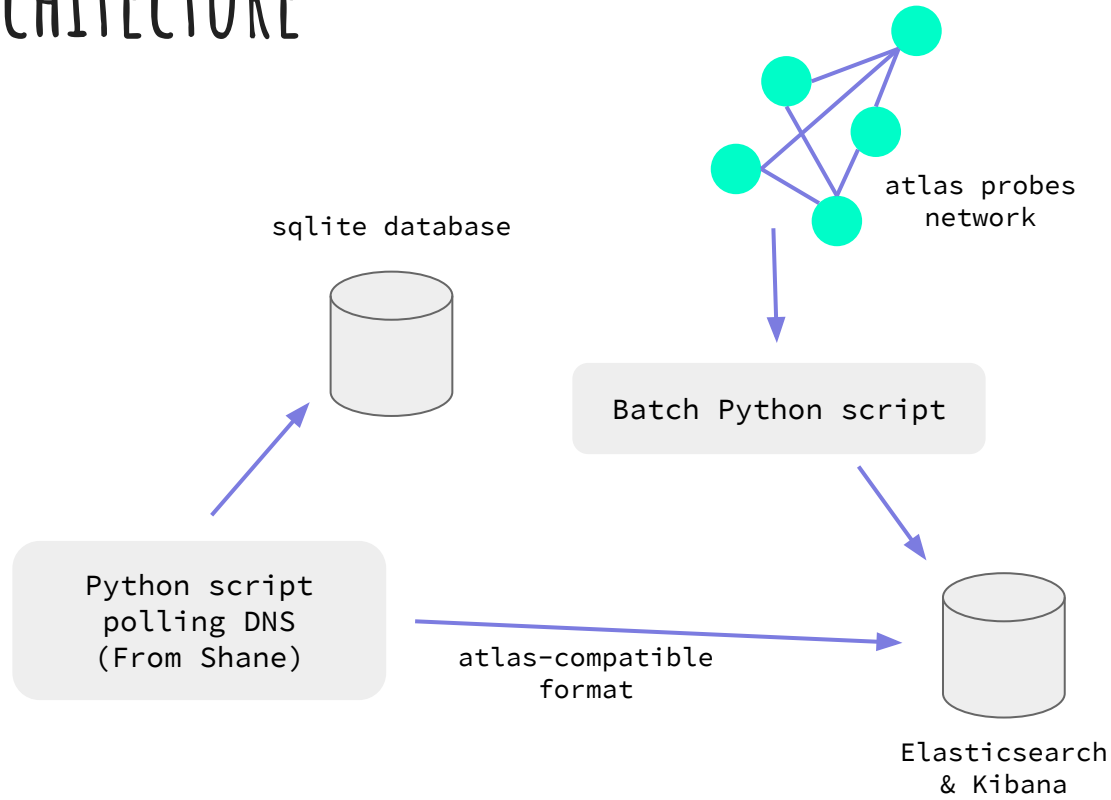
Data architecture



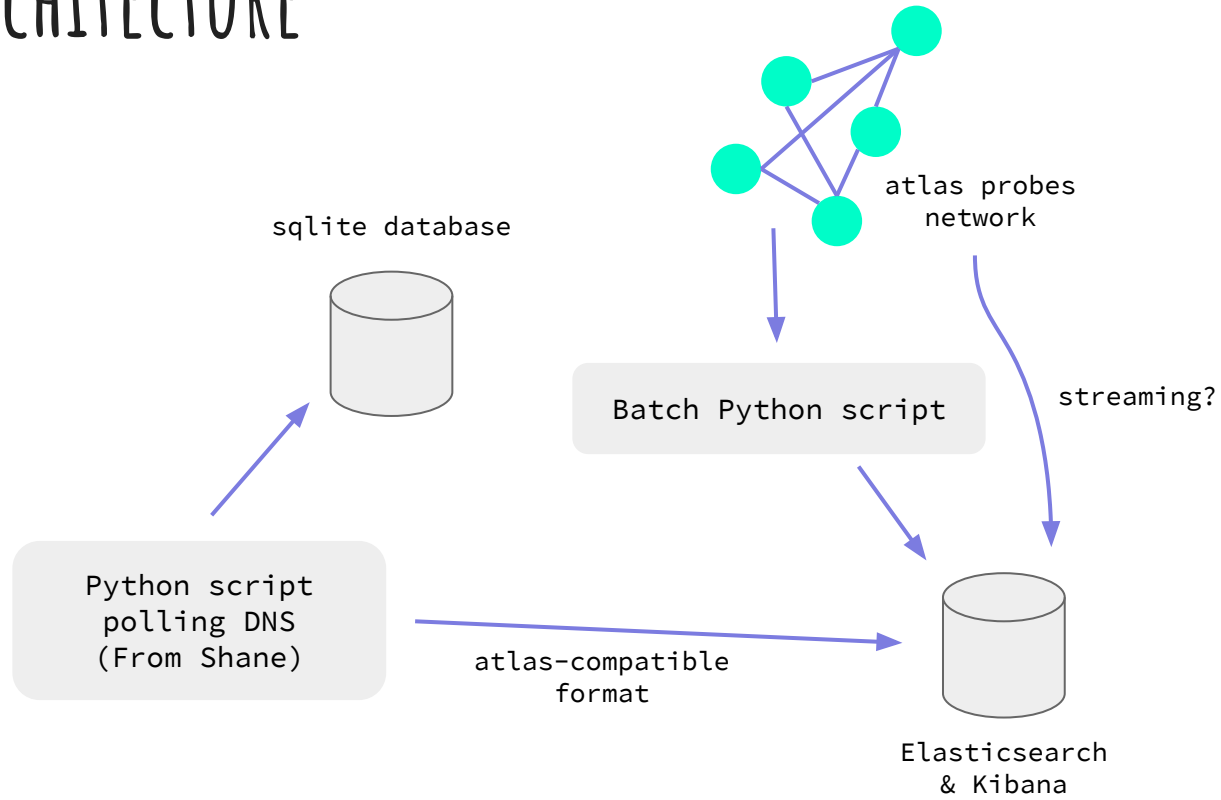
Data architecture



Data architecture



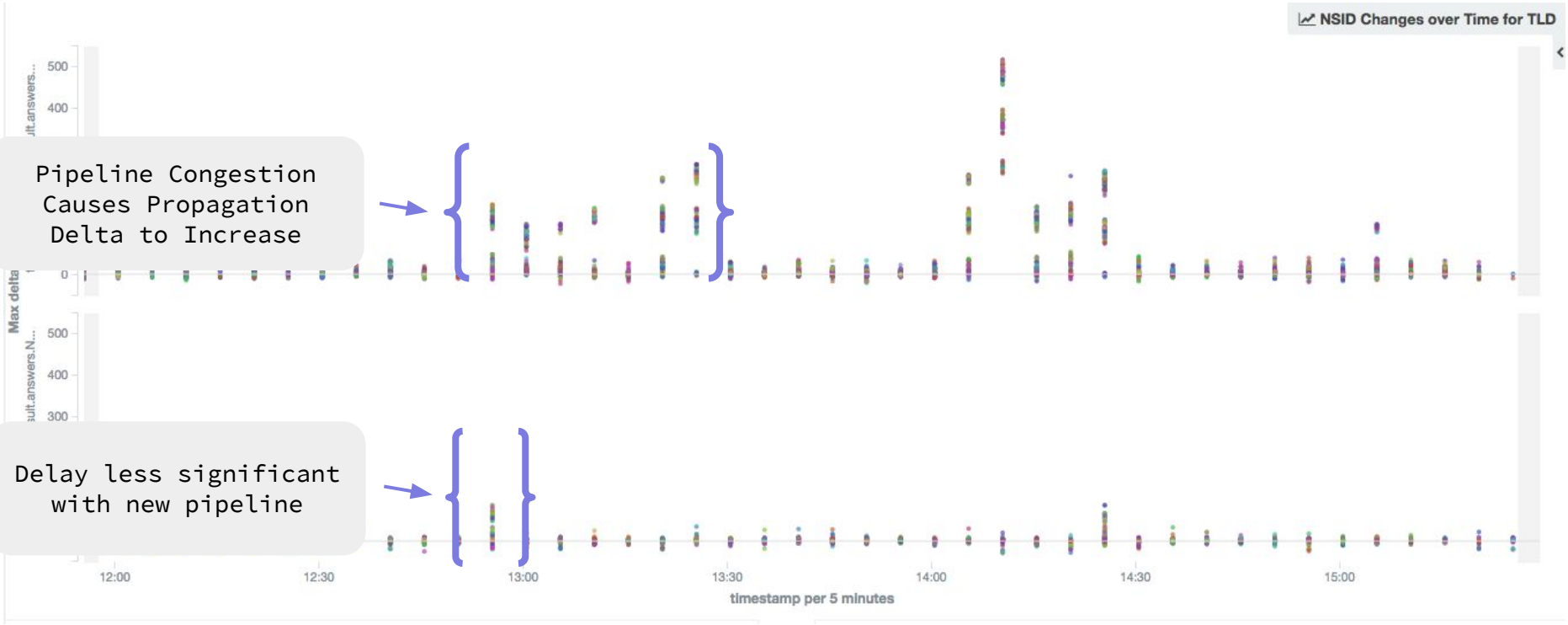
Data architecture



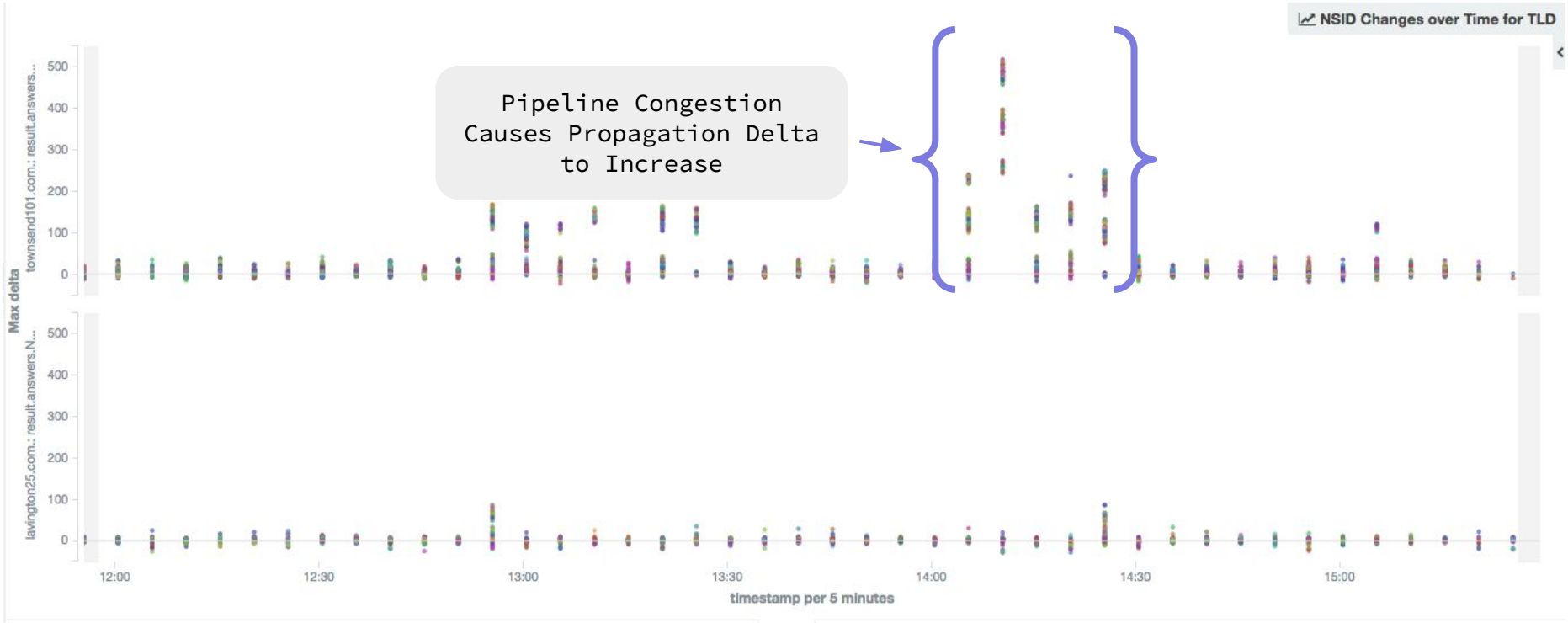
Sources for SOA data

- Root SOA Serial
  - Root propagation is tracked as part of the RSSAC Root Operator Analytics standard (interesting to compare, though)
- TLD SOA Serial
  - We collected data from DNSMON **com.** Measurements (for all GTLD NSs)
- Custom SOA Serial
  - Example: Cloudflare DNS monitoring with a frequently changing serial

Real Propagation Delay Issue Detection

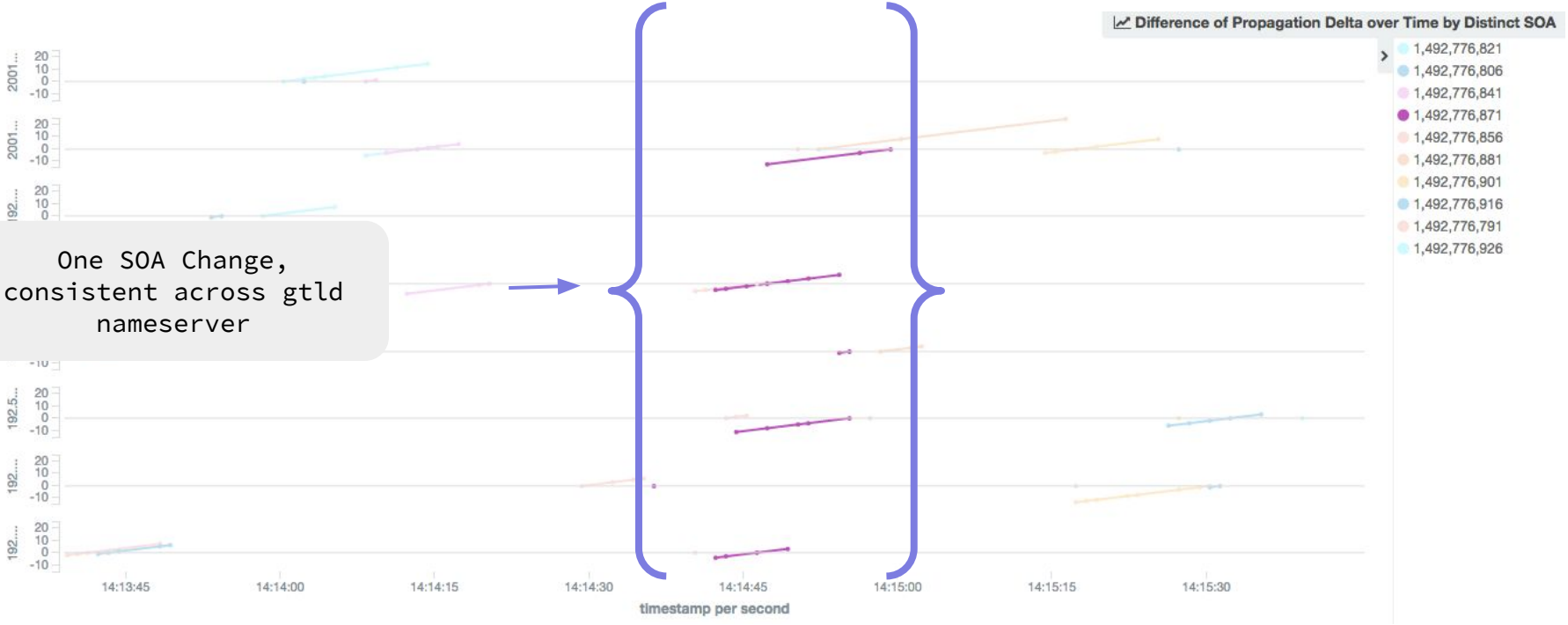


Real Propagation Delay Issue Detection



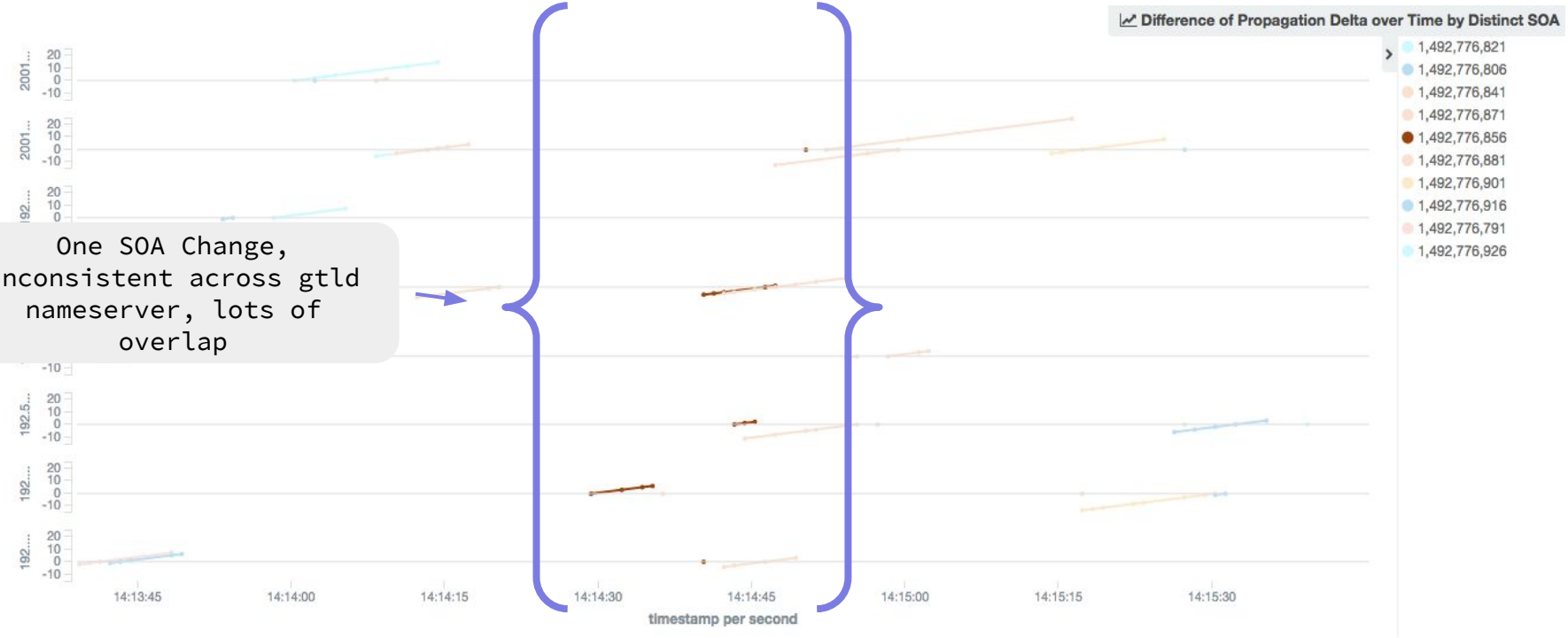
Consistency Issues Across GTLD Servers

One SOA Change, consistent across gtld nameserver



Consistency Issues Across GTLD Servers

One SOA Change, inconsistent across gtld nameserver, lots of overlap



Curious findings

- EDNS3 NSID Flag
  - Built-in Atlas measurements don’t contain NSID data
  - Some big TLDs (com, uk, …) don’t provide NSID

- Root SOA Serials
  - Generally 2-3 updates a day
  - Often serials from a few days ago cropping up from a few NS

THANKS!