# OCTO and DNS Capture and Analysis

Matt Larson, VP of Research

Joint meeting of the ICANN Board and Technical Experts Group
14 March 2018

# OCTO DNS Data

- Traffic from four root servers: B, D, F and L
  - B, D, F: pcap format
    - Phasing out in 2018
  - L: C-DNS (CBOR based)
  - Post-processed and distilled into plain text format
    - Remarkably useful
    - grep, awk, sed and friends are fast and easy
- *rzkeychange* (DNSCAP plug-in) statistics from 11 root servers
  - High-level statistics
  - RFC8145 trust anchor reports
- Resolver test lab
  - Capture DNS traffic in a controlled environment
- Historic root and TLD zone files

# Research Projects Using DNS Data

- corp/home/mail analysis
- Root KSK roll analysis (RFC8145 data)
- ITHI metrics
- Joint resolver behavior research with APNIC
- DNSSEC deployment statistics
- Validating resolver behavior

- That's just a partial list