UKNOF37
Manchester
April 2017

OARC's DNS Software Tools Suite

Keith Mitchell,
Jerry Lundström

https://www.dns-oarc.net/

OARC's Mission

The Domain Name System Operations Analysis and Research Center (DNS-OARC) is a non-profit, membership organisation that seeks to improve the security, stability, and understanding of the Internet's DNS infrastructure.

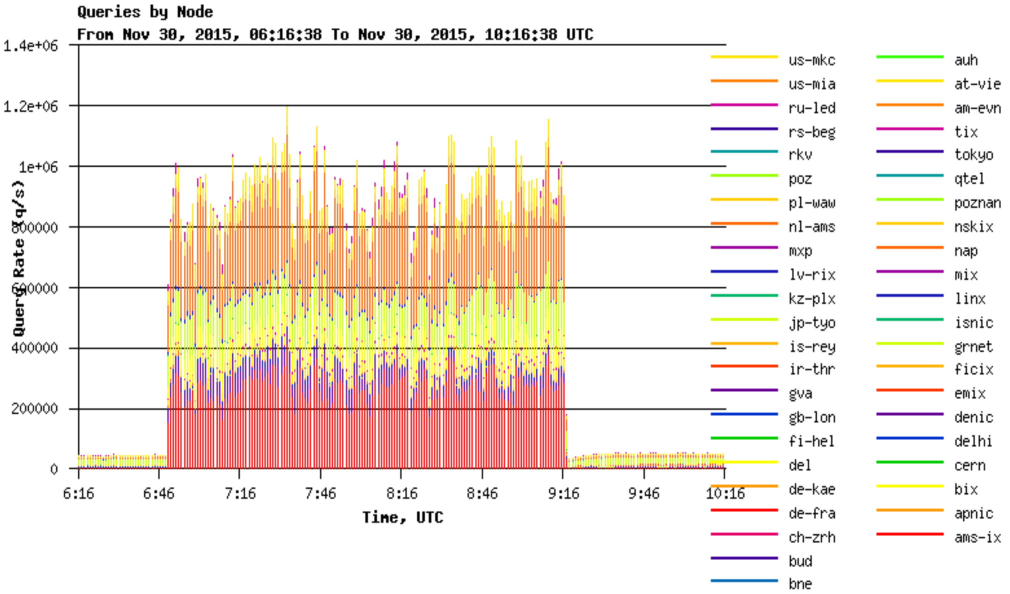
DNS-OARC's mission is to:

- *promote and conduct research with operational relevance through data collection and analysis*
- *offer useful services and tools*
- *build relationships among its community of members*
- *facilitate an environment where information can be shared responsibly*
- *enable knowledge transfer by organizing open workshops*
- *increase public awareness of the DNS's significance*

DNS-OARC
Domain Name System Operations Analysis and Research Center

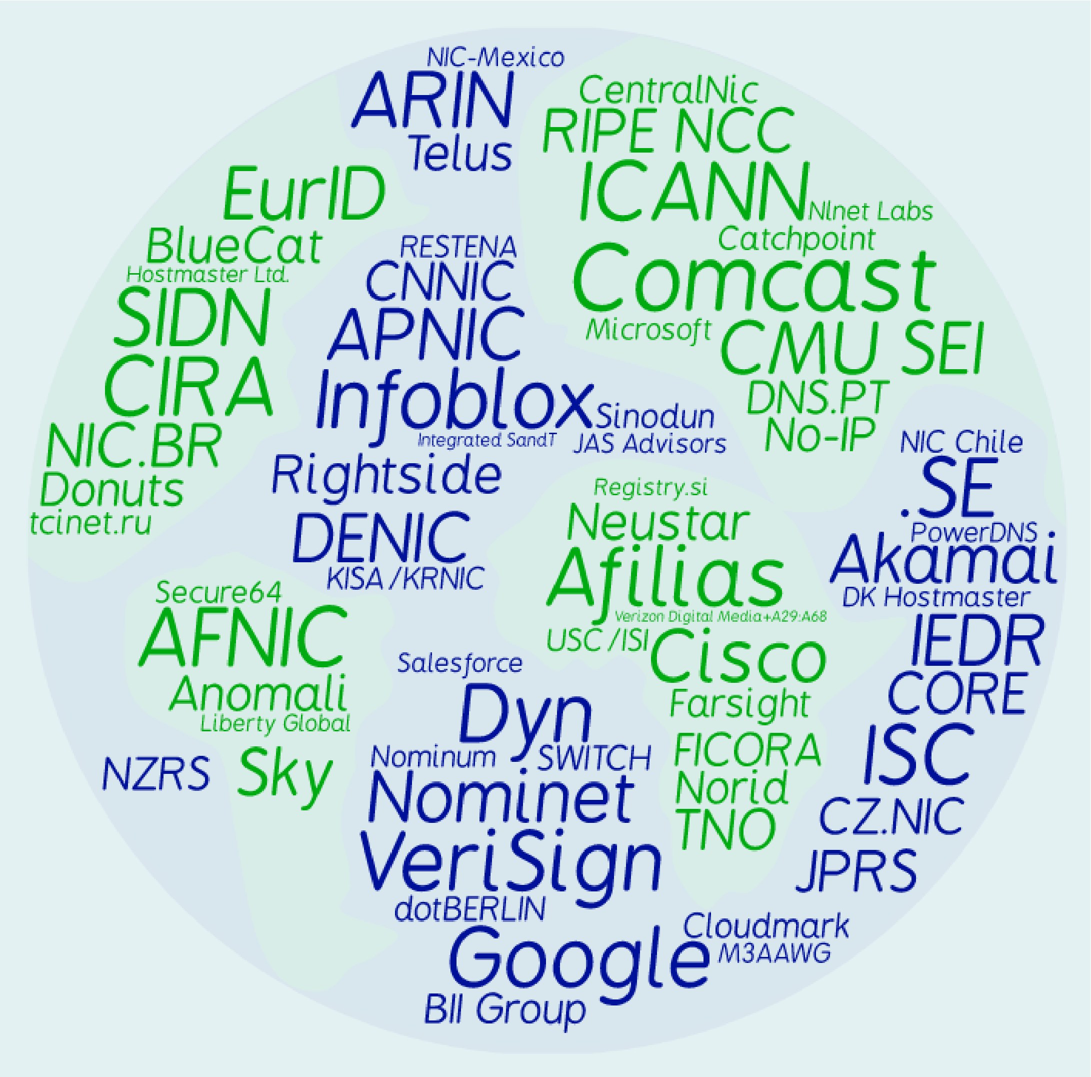
..or to put it another way:

- Yet more bad stuff has been happening to the DNS lately



- DNS is uniquely positioned to be all of victim, vector, and solution to abuse

DNS-OARC
Domain Name System Operations Analysis and Research Center



OARC's Members

DNS-OARC

Domain Name System Operations Analysis and Research Center

OARC Governance

- Independent legal entity
- Diverse member base
- Financially self-supporting
  - ~$700k annual revenue ~= expenses
- Self-governing, neutral
- Elected Board reflecting member interests
- Contracted Executive Staff
  - funds 75% of Keith's time, 20% of Denesh's
- Volunteer workshop Programme Committee
- *501(c)3* non-profit public benefit corporation

Recent Achievements

- Re-located California primary infrastructure site
- Set up new resilient site in Ottawa, Canada
- First workshop in LAC Region
- Brought over 500TB of new storage capacity online
- 2017 “day-in-the-life” (DITL) data gathering just completed
- Special DITL for Root ZSK size increase
- Major Website update
- New Software Engineer:
  - modernized and consolidated existing tools
  - started new development projects

OARC Infrastructure

- Primary site at Hurricane Electric, Fremont, California
  - 10Gb/s Ethernet core
  - over 800TB storage capacity
  - peering at SFMIX exchange (AS64238)
  - data analysis servers
- New Secondary site at CIRA and OttIX in Ottawa, Canada
  - complete dataset mirror
  - planning to consolidate into single site
- Additional development/resilience servers donated & hosted by Netnod in Stockholm, Sweden

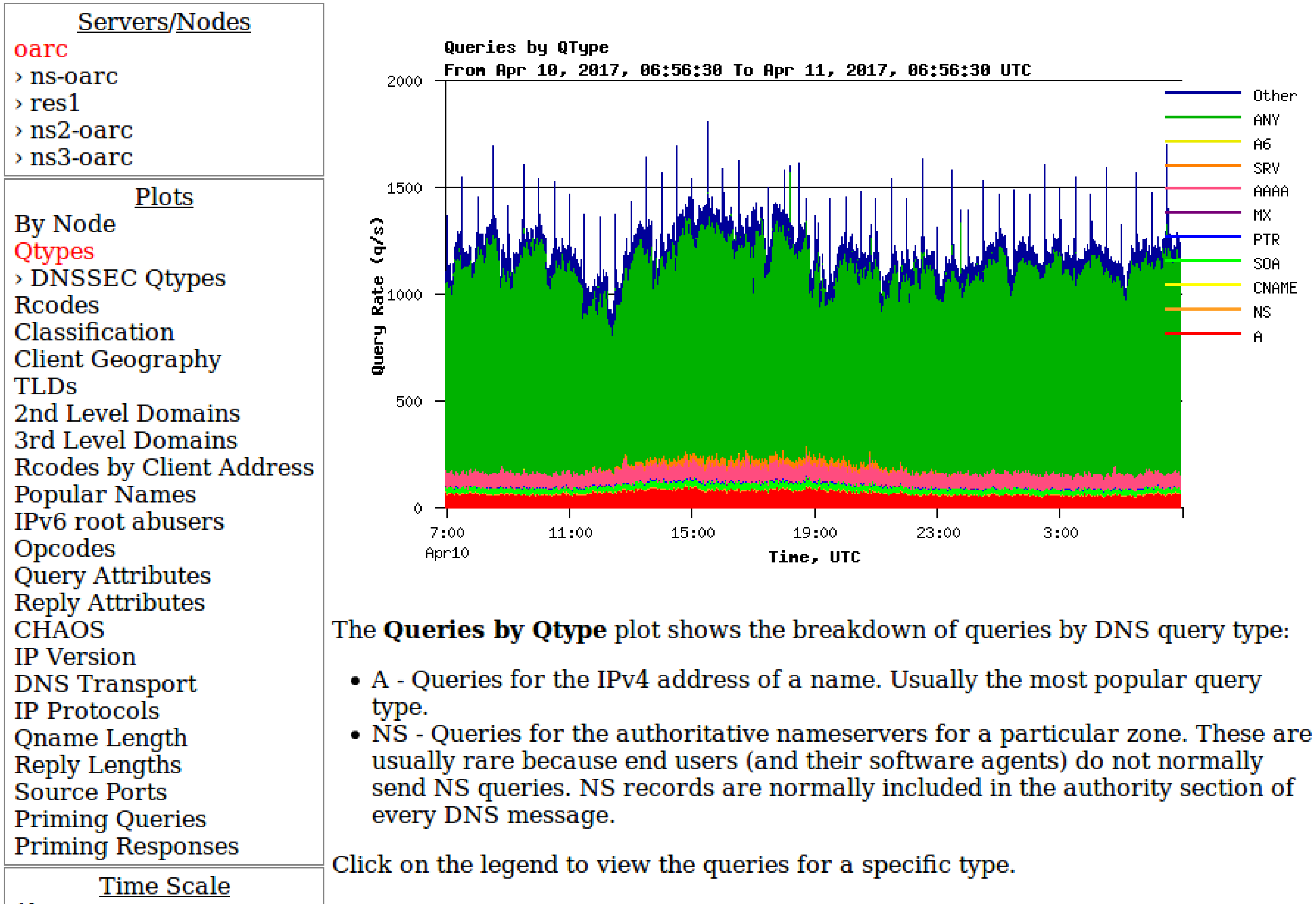
Software Development Environment

- Git/GitHub https://github.com/DNS-OARC
- Uses autoconf/automake/libtool, Semantic Versioning 2.0.0, conforms to FHS 3.0, man-pages
- Continuous Integration using Jenkins and Travis-CI
- Coverity Scan for code analysis
- Compatibility testing on Debian, Ubuntu, CentOS, FreeBSD and OpenBSD
- Packages for Debian, Ubuntu and CentOS

Domain Statistics Collector

- DSC is a tool for collecting and exploring statistics from busy DNS servers
- Uses *libpcap* to sniff network traffic
- Stores aggregated data for the Presenter
- Is configurable to allow the operator to capture any kind of data that they choose

DSC Presenter



The **Queries by Qtype** plot shows the breakdown of queries by DNS query type:

- A - Queries for the IPv4 address of a name. Usually the most popular query type.
- NS - Queries for the authoritative nameservers for a particular zone. These are usually rare because end users (and their software agents) do not normally send NS queries. NS records are normally included in the authority section of every DNS message.

Click on the legend to view the queries for a specific type.

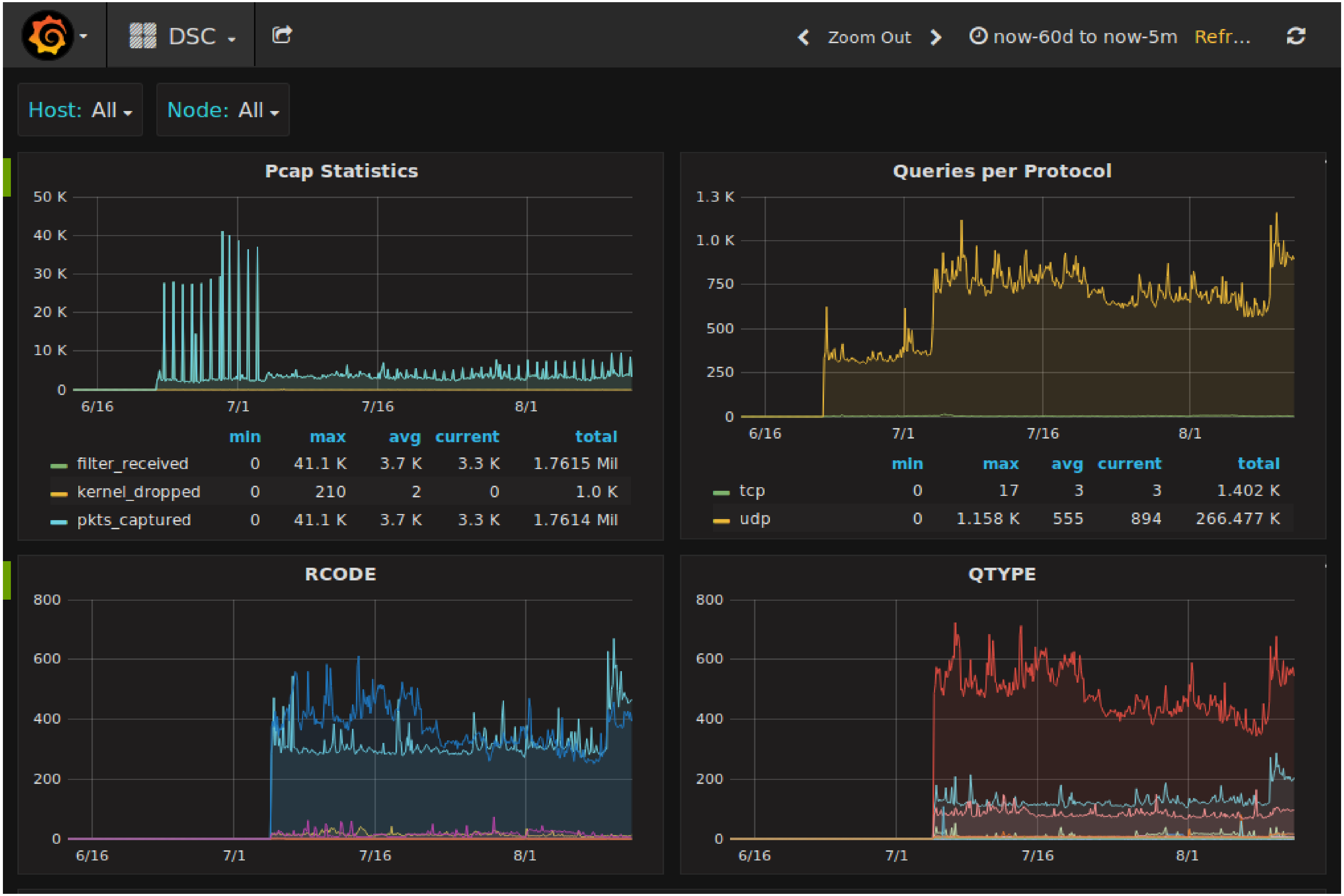
DNS-OARC
Domain Name System Operations Analysis and Research Center

DSC Evolution

- Grafana replacement for DSC Presenter
- *dsc-datatool*, a tool for converting, exporting, merging and transforming DSC data
- Development site at: https://dev.dns-oarc.net/dsc-grafana

DSC Visualisation Improvement

- Use existing visualisation tools
- Use cases: (1) Operational (2) Research
- Preliminary support for Grafana to cover operational needs, time series data covering QPS for total or per QTYPE/RCODE etc
- Evaluating Elastic/Kibana for Research, complex graphs like client port and subnet distribution, geo-location etc



Pcap Statistics

	min	max	avg	current	total
filter_received	0	41.1 K	3.7 K	3.3 K	1.7615 Mil
kernel_dropped	0	210	2	0	1.0 K
pkts_captured	0	41.1 K	3.7 K	3.3 K	1.7614 Mil

Queries per Protocol

	min	max	avg	current	total
tcp	0	17	3	3	1.402 K
udp	0	1.158 K	555	894	266.477 K

DNS-OARC

Domain Name System Operations Analysis and Research Center

dsc-datatool

- Converts, merges, exports, transforms and enriches DSC XML/DAT data
- Currently in development, support for reading DSC XML and exporting to Graphite and InfluxDB
- Transformers:
    - *Labler* – label number based data such as QTYPE/RCODE
    - *ReRanger* – recompile ranges such as ports and subnets
- Generators: GeoIP and IP Authority enrichment

DSC Grafana / dsc-datatool

- Test site available at:

  https://dev.dns-oarc.net/dsc-grafana/dashboard/db/dsc

  Uses live data from the public DSC collection

- Wiki article on how to set it up:

  https://github.com/DNS-OARC/dsc-datatool/wiki/Setting-up-a-test-Grafana

DNSCAP

- *dnscap* is a network capture utility similar to *tcpdump*, but has a number of features tailored to DNS transactions and protocol options
- DNS-OARC uses *dnscap* for DITL data collections
- License moved from ISC to DNS-OARC in 2016

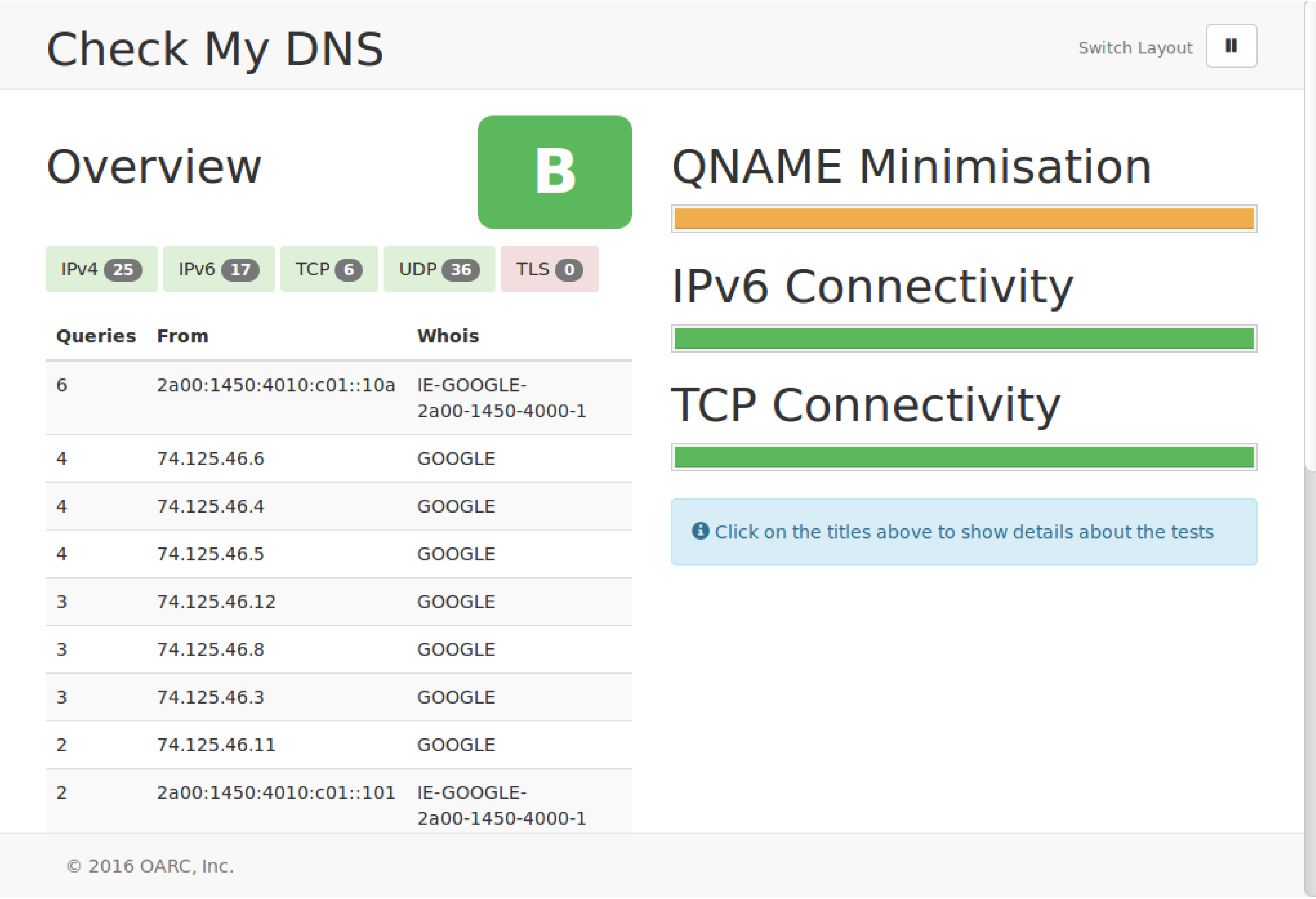
DNS-OARC
Domain Name System Operations Analysis and Research Center

Check My DNS

- A web application to test the resolvers of the client by generating lookups from the browser to a custom developed DNS server
- Initiation, status and results accessed by an API
- Currently tests for: DNSSEC, IPv6, QNAME minimisation and TCP
- All results are stored locally and available for OARC members

Check My DNS

- Future tests: Reply Size, DNS Entropy, DNSSEC algorithms, AD/Z bit compliance, EDNS, DNSSEC key sizes, “ENT was here!”, IPv6 only mid-delegation, Glueless zones, IPv6 fragmentation, NAT64/DNS64 …
  (disclaimer: everything may not be possible to check)
- “dig @... test.dn TXT” support when possible



Check My DNS

Overview

B

Queries	From	Whois
6	2a00:1450:4010:c01::10a	IE-GOOGLE-2a00-1450-4000-1
4	74.125.46.6	GOOGLE
4	74.125.46.4	GOOGLE
4	74.125.46.5	GOOGLE
3	74.125.46.12	GOOGLE
3	74.125.46.8	GOOGLE
3	74.125.46.3	GOOGLE
2	74.125.46.11	GOOGLE
2	2a00:1450:4010:c01::101	IE-GOOGLE-2a00-1450-4000-1

QNAME Minimisation

IPv6 Connectivity

TCP Connectivity

ℹ Click on the titles above to show details about the tests

Check My DNS

- Current status:
  Reimplementation in Go underway to increase performance from ~400 QPS to >50k QPS and to make it possible to run at locations around the world
- Upcoming feature:
  Run as plug-in on any website to see how your visitors' DNS resolvers operate

DNS Replay Tool (drool)

- drool replays DNS traffic from packet capture (PCAP) files and sends it to a specified server
- Options to manipulate timing between packets, loop packets infinitely or N iterations … and more to come !
- Considering hosting member-contributed sample traffic library

DNS Replay Tool (drool)

```
$ src/drool -vv -c 'text:timing ignore; client_pool target "127.0.0.1" "53"; client_pool
skip_reply; client_pool sendas udp; context client_pools 3;' -r ~/dns.pcap
core info: setup signal handling
core info: initialize pcap-thread
core info: start
core info: end
core info: runtime 0.160850035 seconds
core info: saw 286868 packets, 1783450/pps
core info: sent 173686 packets, 1079801/pps 39/abpp
core info: dropped 12580 packets
core info: ignored 100602 packets
```

dumdumd

- High performance UDP/TCP server that ... just drops everything you send to it
- Used during the development of drool to the the network code
- Uses libev and/or libuv
- Able to receive ~1 million UDP PPS using EV and ~1.1 million using UV

Helper Libraries

- Shared code between projects moved to git submodules as helper libraries
- *pcap-thread* - PCAP helper library with POSIX threads support and transport layer callbacks
- *omg-dns* - Helper library for parsing valid / invalid / broken / malformed DNS packets
- *parseconf* - Conf parser helper library
- *sllq* - Semi Lock-Less Queue

OARC Workshops

- OARC26
  - Madrid, Spain, 14-15 May
  - Co-located with ICANN GDD, RoW, DNS Symposium
  - https://indico.dns-oarc.net/event/26/

- OARC27
  - San Jose, California, 29-30 September
  - Co-located with NANOG71, ARIN40
  - https://indico.dns-oarc.net/event/27/

Why Become an OARC Member ?

- Access to, and participation in, the world's premier community of DNS technical experts
- Influence and fund development of open tools and services to support your infrastructure operations
- Share and analyze an unequaled DNS dataset to generate new insights into global Internet operations
- Use of community co-ordination resources to respond to incidents and threats
- Support a trusted, neutral technical party free of vested interests in the DNS space

DNS-OARC
Domain Name System Operations Analysis and Research Center

Questions/ Discussion