Monitoring The Second Level: Valid Use or Child Abuse?

Canadian Internet Registration Authority (CIRA)
Jacob Zack
DNS Administrator
DNS-OARC @ Teddington, UK, March 2012

Lack of Visibility

- As part of our DNSSEC deployment strategy, we decided there was a need for far greater visibility into the second-level of .CA:
  - How many delegations are broken now?
  - How many delegations will break under DNSSEC?
  - How many delegations rely on DNS servers in currently unsigned TLD's?
  - Which DNS hosting providers and/or registrars implementing DNSSEC en-masse would have the largest effect on uptake of the new DNSSEC product?

What We Knew Already

- Almost 1.9 million total .CA delegations
- Almost 97,000 DNS servers referenced in zone file
- Over 4.2 million domain<->DNS server relationships
- Some delegations will be broken
- Some delegations will be broken and working
- Packets get lost occasionally
- I am an awesome programmer

What We Learned First

- Spawning 4.2 million nslookup's takes forever (joke!)
- Spawning 4.2 million dig's is faster! (still joking!)
- Net::DNS is totally the solution (wish I were joking)
- Some DNS is broken in ways I couldn't imagine
- I am only a slightly above average programmer

What We Learned Next

- Far more wild-carding exists than we'd all hoped
- A domain can appear working despite responding "NOTIMP" to an SOA query
- A domain can have a CNAME at apex and still be "working"-ish
- All of this breaks Net::DNS when you don't expect it
- I am only an average programmer

Try 1: One-off Reports

- One query per relationship, one retry if no response
- Failure prone (ie: temporary network issues)
- Instantly outdated
- More than one run required, diffs
- Results logged to .CSV file, stats via grep
- Created more questions than answers
- Clearly a more robust solution was needed

Next Generation Requirements

- Multiple querying clients in multiple locations
- Database back-end
- Automated importing of new relationships
- History keeping
- Web-based front-end
- Version control

Client Methodology

- Select $x (5000) least recently assigned relationships
- Look up hostname of DNS server using Net::DNS::Resolver::Recurse search()
- Look up SOA record using DNS server IP Net::DNS::Resolver send($domain, 'SOA', 'IN')
- Update results table
- Update serialhistory table if required
- Update errorhistory table if required

Web-based Display of Data (dom)

.CA Looking Glass

Domain: Submit

Nameserver: Submit

Recent Scans

DOMAIN: cira.ca.

Nameserver	Last Scan	Scan Source	Response Time	SOAOK	Error Code	Serial	Refresh	Retry	Expire	MinTTL	Last .CA zone
ns01.cira.ca.	2012-03-14 08:20:10	FOGBUGZ.CRP	0.0125	Y	PROPER - NOERROR	2012030900	1800	900	604800	300	2012031411
sns-pb.isc.org.	2012-03-14 03:55:35	LOCALHOST	0.0216	Y	PROPER - NOERROR	2012030900	1800	900	604800	300	2012031411
ns02.cira.ca.	2012-03-14 02:06:09	FOGBUGZ.CRP	0.0102	Y	PROPER - NOERROR	2012030900	1800	900	604800	300	2012031411

Serial History

Change Date	Nameserver	Scan Source	New Serial	Last .CA zone

Status History

Change Date	Nameserver	Scan Source	Old Status -> New Status	Last .CA zone

Serial History

Change Date	Nameserver	Scan Source	New Serial	Last .CA zone
2012-03-14 11:33:44	ns1.server269.com.	LOCALHOST	1331715606	2012031411
2012-03-14 00:00:57	ns1.server269.com.	LOCALHOST	1331663282	2012031411
2012-03-13 15:47:47	ns2.server269.com.	FOGBUGZ.CRP	1331663282	2012031411

Status History

Change Date	Nameserver	Scan Source	Old Status -> New Status	Last .CA zone
2012-03-14 02:46:38	ns1.dreamhost.com.	FOGBUGZ.CRP	[PROPER - NOERROR] -> [NORESPONSE - query timed out]	2012031411
2012-03-13 15:49:40	ns2.dreamhost.com.	LOCALHOST	[NORESPONSE - query timed out] -> [PROPER - NOERROR]	2012031411

Web-based Display of Data (NS)

.CA Looking Glass

Domain: Submit

Nameserver: Submit

Nameserver Stats

NAMESERVER: ns01.cira.ca.				
Total Delegations	Good Delegations	Bad Delegations	Average Response Time	Download Data as .CSV
113	72 (63.72%)	41 (36.28%)	0.0106 seconds	REPORT-ns01.cira.ca.-NS.csv

Passed Tests

Domain Name	Last Scanned	Scan Source	Error Code	Last .CA zone
unmilliondomaine.ca.	2012-03-14 12:58:50	LOCALHOST	PROPER - NOERROR	2012031411
net-day.ca.	2012-03-14 12:38:39	LOCALHOST	PROPER - NOERROR	2012031411
wwwcira.ca.	2012-03-14 11:36:49	FOGBUGZ.CRP	PROPER - NOERROR	2012031411
consultationidn.ca.	2012-03-14 11:11:06	FOGBUGZ.CRP	PROPER - NOERROR	2012031411
onewebday.ca.	2012-03-14 11:05:30	FOGBUGZ.CRP	PROPER - NOERROR	2012031411
internetdaycanada.ca.	2012-03-14 11:05:30	FOGBUGZ.CRP	PROPER - NOERROR	2012031411
lejourwebcanada.ca.	2012-03-14 11:02:02	LOCALHOST	PROPER - NOERROR	2012031411
journeeweb.ca.	2012-03-14 10:46:09	FOGBUGZ.CRP	PROPER - NOERROR	2012031411
aceiadhesion.ca.	2012-03-14 10:40:59	FOGBUGZ.CRP	PROPER - NOERROR	2012031411
webdays.ca.	2012-03-14 10:32:16	FOGBUGZ.CRP	PROPER - NOERROR	2012031411
september22.ca.	2012-03-14 10:28:12	LOCALHOST	PROPER - NOERROR	2012031411
internet-day.ca.	2012-03-14 10:23:57	LOCALHOST	PROPER - NOERROR	2012031411
ficanadien.ca.	2012-03-14 10:21:45	FOGBUGZ.CRP	PROPER - NOERROR	2012031411
milliondomaine.ca.	2012-03-14 10:19:24	FOGBUGZ.CRP	PROPER - NOERROR	2012031411
cirablogs.ca.	2012-03-14 10:01:47	LOCALHOST	PROPER - NOERROR	2012031411
impactawards.ca.	2012-03-14 09:21:48	LOCALHOST	PROPER - NOERROR	2012031411
jourweb.ca.	2012-03-14 09:07:37	FOGBUGZ.CRP	PROPER - NOERROR	2012031411
internetday.ca.	2012-03-14 08:58:21	LOCALHOST	PROPER - NOERROR	2012031411
get-your.ca.	2012-03-14 08:33:49	LOCALHOST	PROPER - NOERROR	2012031411
montrezvotre.ca.	2012-03-14 08:32:42	LOCALHOST	PROPER - NOERROR	2012031411
webday.ca.	2012-03-14 08:31:15	FOGBUGZ.CRP	PROPER - NOERROR	2012031411

Failed Tests

Domain Name	Last Scanned	Scan Source	Error Code	Last .CA zone
25years.ca.	2012-03-14 12:56:57	LOCALHOST	NOANSWER - REFUSED	2012031411
onsepc.ca.	2012-03-14 12:56:55	LOCALHOST	NOANSWER - REFUSED	2012031411
cirablogging.ca.	2012-03-14 12:56:54	LOCALHOST	NOANSWER - REFUSED	2012031411
canadianinternetforum.ca.	2012-03-14 12:41:19	LOCALHOST	NOANSWER - REFUSED	2012031411
youdontwanta.ca.	2012-03-14 11:53:05	LOCALHOST	NOANSWER - REFUSED	2012031411
bunboy.ca.	2012-03-14 10:47:50	FOGBUGZ.CRP	NOANSWER - REFUSED	2012031411
canadiensbranches.ca.	2012-03-14 10:21:45	FOGBUGZ.CRP	NOANSWER - REFUSED	2012031411
thecafecanada.ca.	2012-03-14 10:07:24	LOCALHOST	NOANSWER - REFUSED	2012031411
e164.ca.	2012-03-14 09:57:18	LOCALHOST	NOANSWER - REFUSED	2012031411
thecirablogs.ca.	2012-03-14 09:29:32	FOGBUGZ.CRP	NOANSWER - REFUSED	2012031411
byronholland.ca.	2012-03-14 09:09:34	FOGBUGZ.CRP	NOANSWER - REFUSED	2012031411
cira-blogs.ca.	2012-03-14 09:07:38	FOGBUGZ.CRP	NOANSWER - REFUSED	2012031411
cira-blog.ca.	2012-03-14 08:52:30	FOGBUGZ.CRP	NOANSWER - REFUSED	2012031411
icann45.ca.	2012-03-14 08:46:12	FOGBUGZ.CRP	NOANSWER - REFUSED	2012031411
canadianlikeyou.ca.	2012-03-14 08:28:45	LOCALHOST	NOANSWER - REFUSED	2012031411
icanntoronto.ca.	2012-03-14 07:59:31	LOCALHOST	NOANSWER - REFUSED	2012031411
cira-blogging.ca.	2012-03-14 07:23:01	LOCALHOST	NOANSWER - REFUSED	2012031411
thecirablog.ca.	2012-03-14 07:22:21	LOCALHOST	NOANSWER - REFUSED	2012031411
stateofinternet.ca.	2012-03-14 05:45:27	LOCALHOST	NOANSWER - REFUSED	2012031411
amiamember.ca.	2012-03-14 05:12:25	FOGBUGZ.CRP	NOANSWER - REFUSED	2012031411
larrytheleaderinlamps.ca.	2012-03-14 05:09:38	LOCALHOST	NOANSWER - REFUSED	2012031411

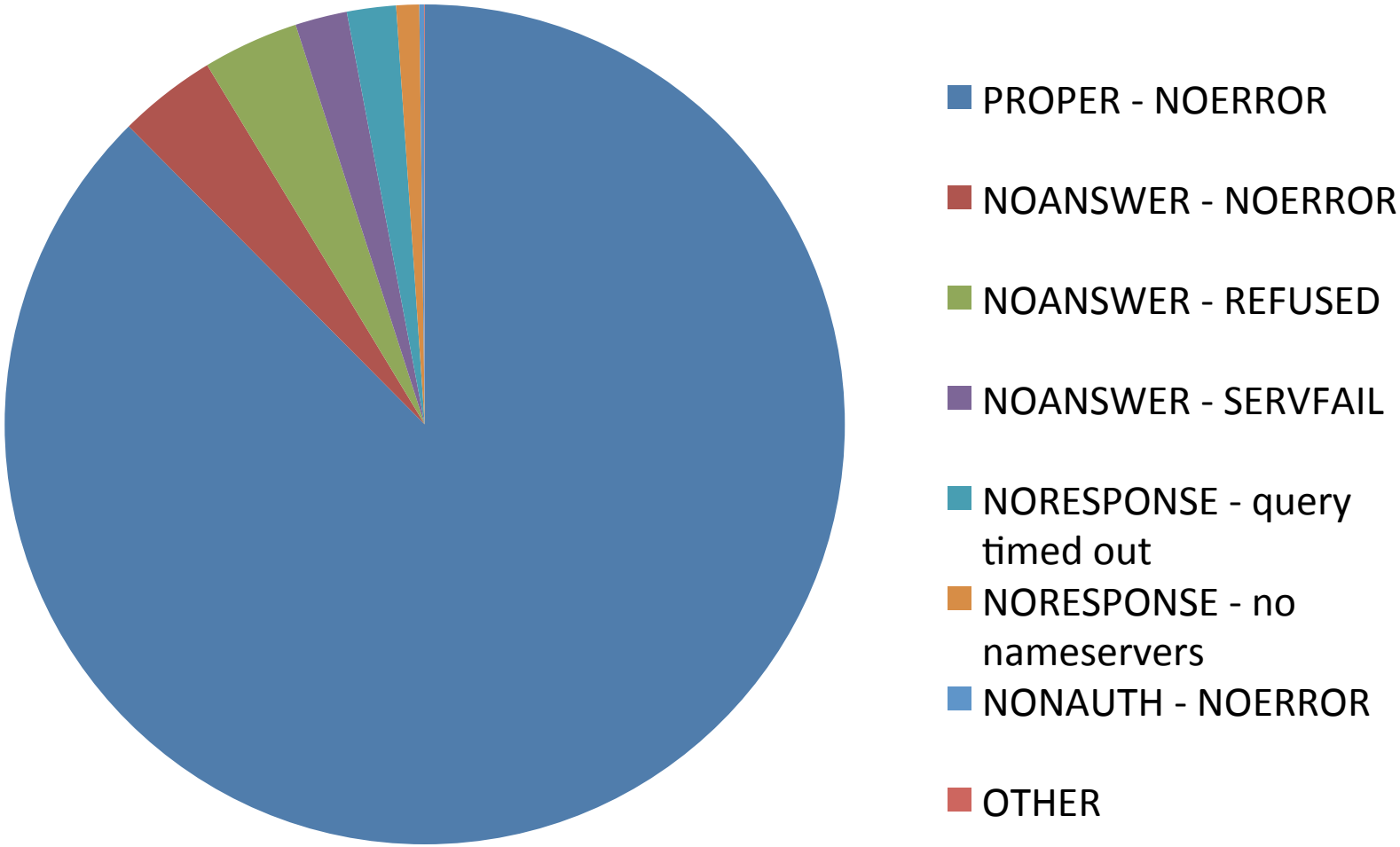
Current Status

- Currently two client machines on same network
- Each relationship queried every ~8 hours
- About 12 million DNS queries/day
- Manual importing of latest zone every few days
- 32bit server with 4Gig of RAM hosting mySQL
- ~10 seconds search result load times

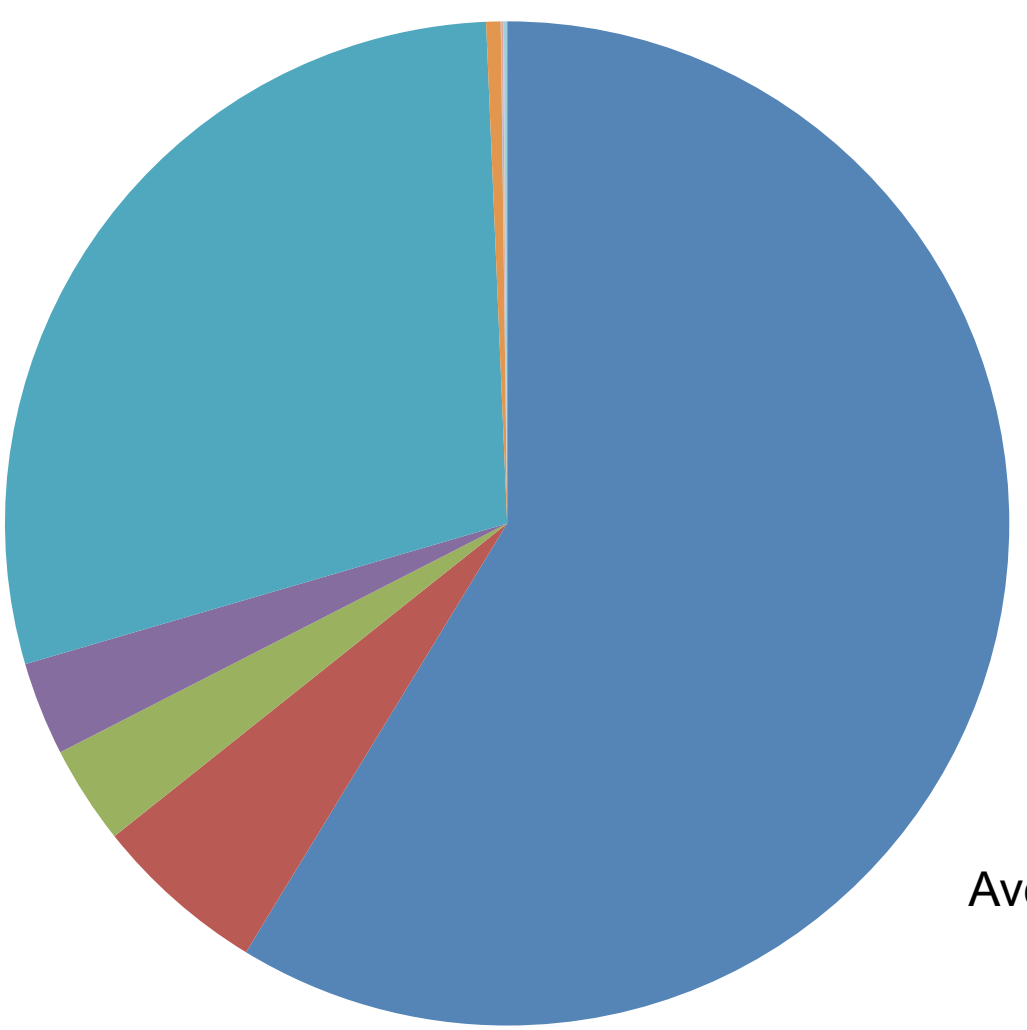
Future Steps

- Clients in Vancouver, Montreal, Ottawa, Toronto
- Per-site mySQL databases
- Automatic importing of latest zone file hourly
- Dynamically created pie charts and graphs
- Faster search result load times
- Alerting, Trending, etc.
- Customer Service/Registrar Troubleshooting Tool

SOA Query Test Results



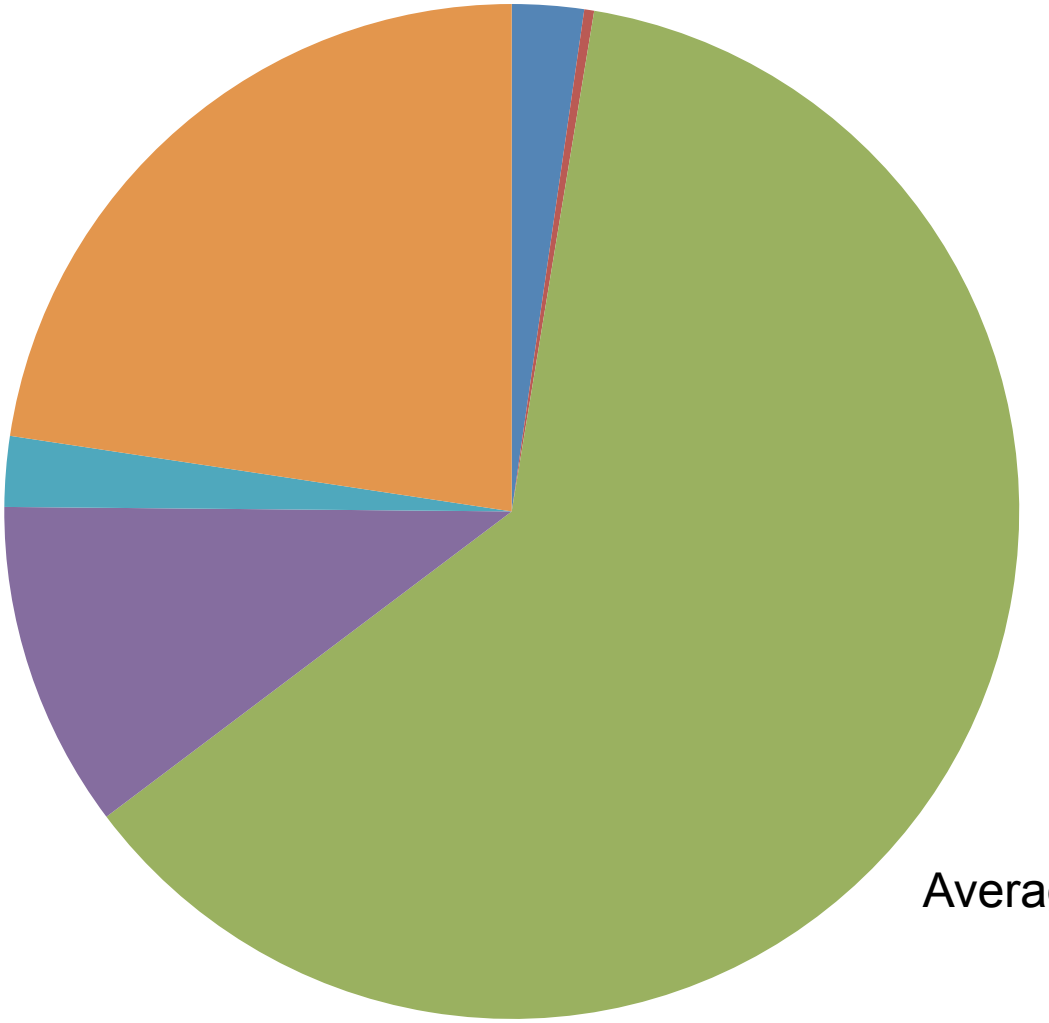
Min TTLs



Average: 30818 seconds

8.56 hours

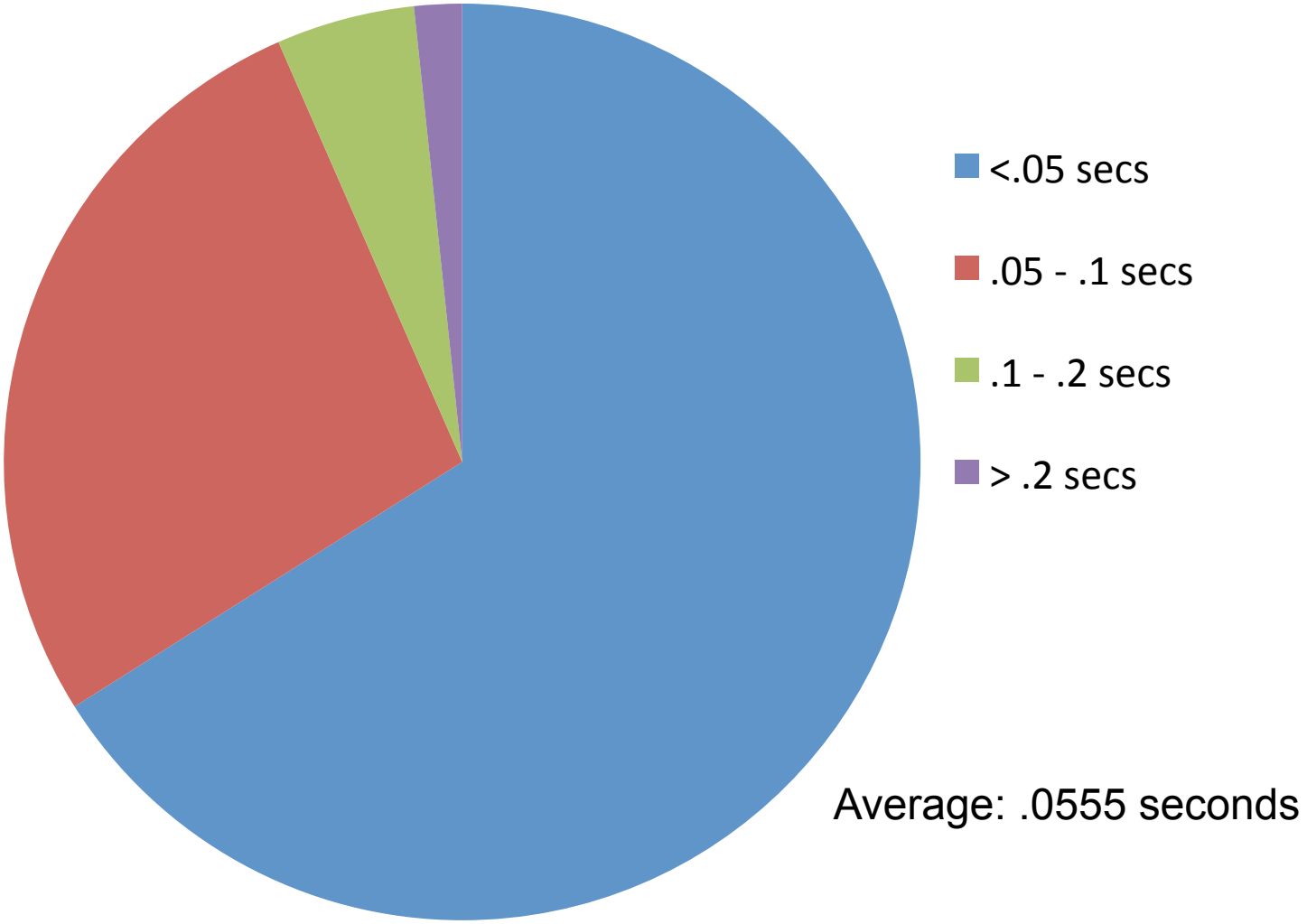
Expire Times



Average: 1295407 seconds

14.99 days

Response Times



Average: .0555 seconds

Questions/Comments

- Is this valid research?
- Is this child abuse?
- Is any other TLD monitoring the second level?
- Does PERL count as a programming language?
- Are pie charts the lowest form of chartery?
- Your question here! ($25 USD)