DNS Debugging and monitoring

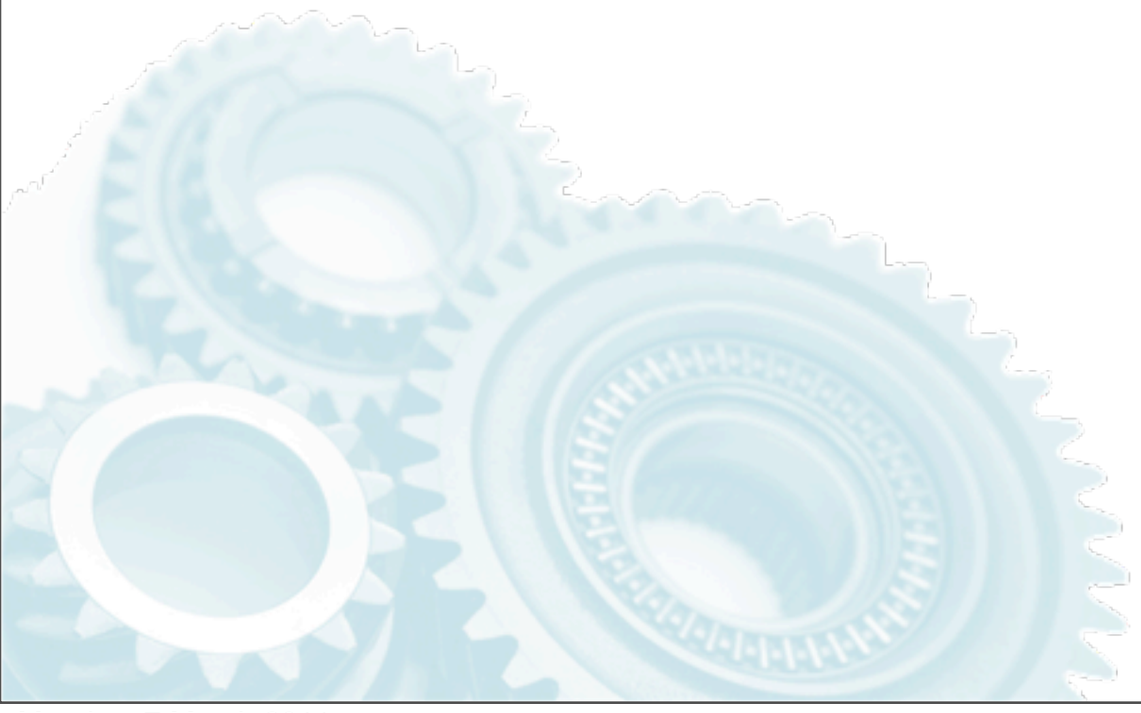
João Damas

Outline

- The basics
- Zone verification
- Instant analysis
- Longer term/ongoing analysis
- Special focus on debugging DNSSEC

The basics

- nslookup
- DiG
- drill



nslookup

- Been around for a long while in many OSs
- OK for casual use but better to use either of the other tools (DiG or drill)
  - doesn't really report on what is trying to do
  - use ***host*** if all you want is a simple query utility
  - general recommendation: **DO NOT** use for DNS debugging

DiG

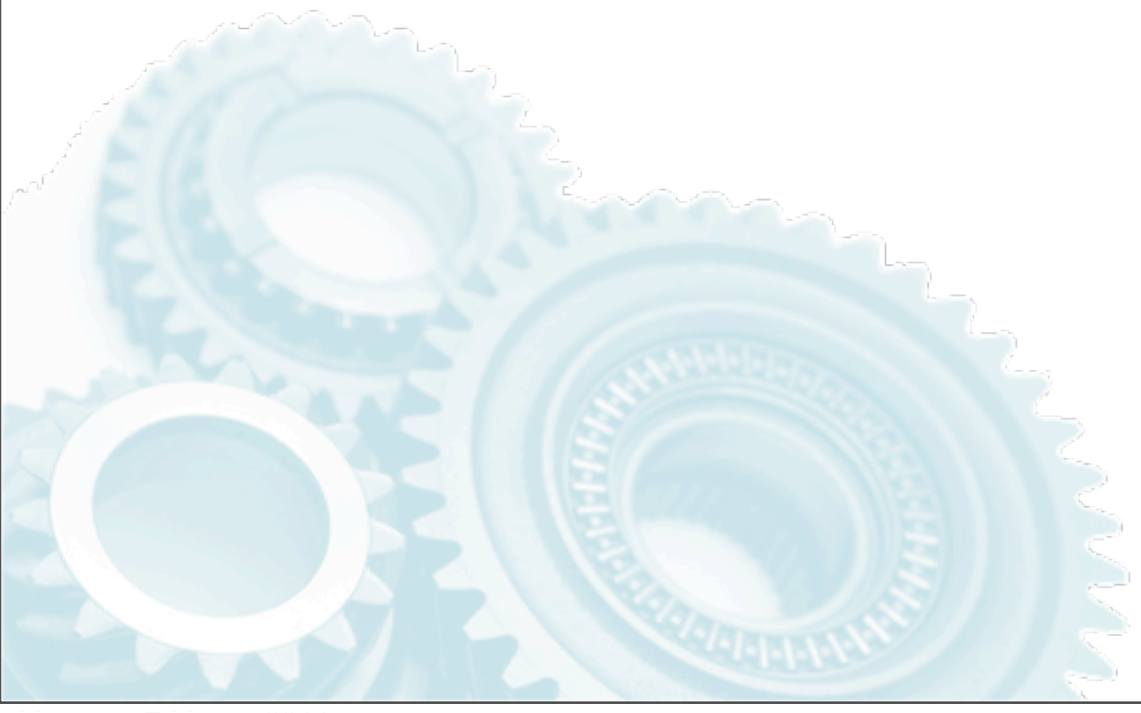
- Produced and maintained by ISC as part of BIND 9
  - –Very useful all-purpose, full control DNS query tool
  - –Install it as part of BIND
  - –Get it packaged
    - e.g. dnsutils in Ubuntu or Debian

DiG: anatomy of a DNS query

```
$ dig bondis.org

; <<>> DiG 9.7.0 <<>> bondis.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20717
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
;; QUESTION SECTION:
;bondis.org.                    IN      A
;; ANSWER SECTION:
bondis.org.             300     IN      A       194.176.119.229
;; AUTHORITY SECTION:
bondis.org.             300     IN      NS      ns.bondis.org.
bondis.org.             300     IN      NS      borg.c-l-i.net.
;; ADDITIONAL SECTION:
ns.bondis.org.          300     IN      A       194.176.119.229
borg.c-l-i.net.         300     IN      A       192.16.192.99
;; Query time: 0 msec
;; SERVER: 204.61.225.99#53(204.61.225.99)
;; WHEN: Thu Jan 13 17:59:28 2011
;; MSG SIZE  rcvd: 121
```

DiG

```
$ dig isc.org any +dnssec

; <<>> DiG 9.7.0 <<>> isc.org any +dnssec

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2794

;; flags: qr rd ra; QUERY: 1, ANSWER: 10, AUTHORITY: 5, ADDITIONAL: 11
```



DiG

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;isc.org.                       IN      ANY
```

DiG

;; ANSWER SECTION:

isc.org. 43122 IN RRSIG A 5 2 43200 20110207233212 20110108233212 26982 isc.org. oGQRMM
+BQOYtqHBUG0pwwhmNKiXY49ncQPw9UJrIKpEYHoZpSZhvLGrX QgtKuUQi5dOBOR8QeAoQ9IoV0tuSNmlEk+Fi2EFvouDP8WPgLpc7Y86R
ovfA0NjpYtIbranjm6B/Dv9Wc0v1Yv/eFFxL+AJ8F2e4UnVXxMOP7dP0 BDM=

isc.org. 43122 IN A 149.20.64.42

isc.org. 8119 IN NS ams.sns-pb.isc.org.

isc.org. 8119 IN NS ns.isc.afilias-nst.info.

isc.org. 8119 IN NS ord.sns-pb.isc.org.

isc.org. 8119 IN NS sfba.sns-pb.isc.org.

isc.org. 43122 IN RRSIG NS 5 2 43200 20110207233212 20110108233212 26982 isc.org. mo82HW/
2bEi4UekDGRd50xUN6Q85Q2llCxVZXJ7HkumyUTEZFzqpix/a CnBYjBvpvAW1rRr/4BTVj33e8tTRgKeV0bT5JG+HVirRAHBISKI+p3ed
yNHjYb0PUsN5WD6efiZxGvkFAGWhZRUjSBEiWiIEFWIjjEvV/ywkuGLC uHo=

isc.org. 51319 IN RRSIG DS 7 2 86400 20110123165115 20110109155115 1743 org. N3g2hkYL
+cuSnNBT16sGz1WonF4esYR3awgSVSckBwND8uZTse9G6q14 +8b81zuXcqVSCJuWoRuOVkJ8aE28qPzx8S+SVEw5Gm+gXk4xJuIkkW5J
c6rlivi7copPuN9KhS2Rbs8aq4SutAG3STRUg8OnlneAXXt/PTBZD84i Kt4=

isc.org. 51319 IN DS 12892 5 2 F1E184C0E1D615D20EB3C223ACED3B03C773DD952D5F0EB5C777586D E18DA6B5

isc.org. 51319 IN DS 12892 5 1 982113D08B4C6A1D9F6AEE1E2237AEF69F3F9759

DiG

;; AUTHORITY SECTION:

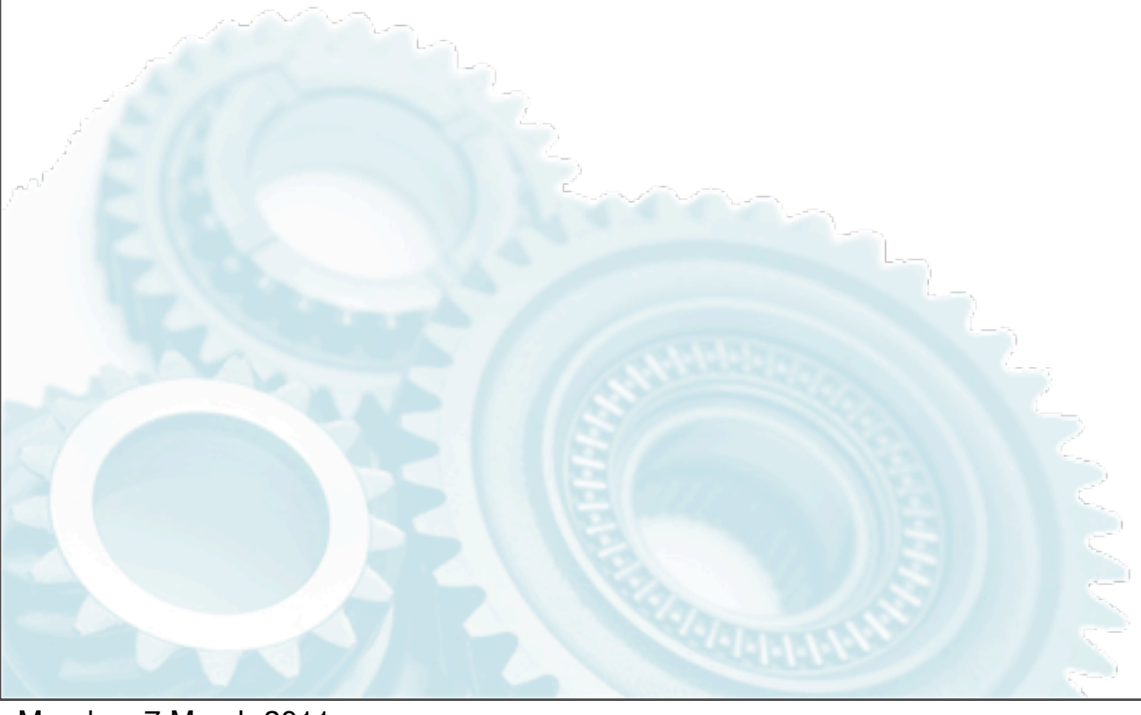
isc.org. 8119 IN NS ams.sns-pb.isc.org.

isc.org. 8119 IN NS ord.sns-pb.isc.org.

isc.org. 8119 IN NS sfba.sns-pb.isc.org.

isc.org. 8119 IN NS ns.isc.afilias-nst.info.

isc.org. 43122 IN RRSIG NS 5 2 43200 20110207233212 20110108233212 26982 isc.org. mo82HW/
2bEi4UekDGRd50xUN6Q85Q2llCxVZXJ7HkumyUTEZFzqpix/a CnBYjBvpvAW1rRr/4BTVj33e8tTRgKeV0bT5JG+HVirRAHBISKI
+p3ed yNHjYb0PUsN5WD6efiZxGvkFAGWhZRUjSBEiWiIEFWIjjEvV/ywkuGLC uHo=



DiG

;; ADDITIONAL SECTION:

ns.isc.afilias-nst.info. 721 IN A 199.254.63.254

ns.isc.afilias-nst.info. 721 IN AAAA 2001:500:2c::254

ams.sns-pb.isc.org. 6936 IN A 199.6.1.30

ams.sns-pb.isc.org. 6937 IN AAAA 2001:500:60::30

ord.sns-pb.isc.org. 6936 IN A 199.6.0.30

ord.sns-pb.isc.org. 6936 IN AAAA 2001:500:71::30

ams.sns-pb.isc.org. 6936 IN RRSIG A 5 4 43200 20110207233212 20110108233212 26982 isc.org. aMa15HtsB3q+/
Bk4RIO53Z1lhUaQcPH2YhxTMJvMdgAPkUoHOftvenpz G5VIYC+MICO3MJoRuko3N21B8iDvZuMz0pfV9LBBkN2Loy1PQ4enRcM2 dLZjcD4Ycf8OAY/
VI/Wt8jUu7h8HeTfCn1U9P1luwFQAtL1K7K4X77Tk ntI=

ams.sns-pb.isc.org. 6937 IN RRSIG AAAA 5 4 43200 20110207233212 20110108233212 26982 isc.org.
DzPQSYGSv3d0I1owD7es9aMQVxB+fPF7xtTPV+vFIBDg27VFDH5C9sDi rpUgTaMTdenb4W1yZWEM8rzIeheibQKYnvAtTMjb40henmJEr/SUXKQK UH
+VipzNVnW4f2PJlHBLopEYOVpiXHNV0ChEcrZwRvCWELVE+Yh6x6lS ycY=

ord.sns-pb.isc.org. 6936 IN RRSIG A 5 4 43200 20110207233212 20110108233212 26982 isc.org.
11ootYvVO9GDfQHZfH6fMhazLCDQAFW+oy91qvihPQ6SQKTRUJv0yF5Q 51Af7pqkIagWWnazf8tFmkPK0AxHJMLJUP2ROMFcqJ03e6wNe5NEM2yb
PUH4d/kmt+xY5COnYmsq6Tptdb+rM5w43jHj83/ddqI9LQ48Sxq6WpGL tAQ=

ord.sns-pb.isc.org. 6936 IN RRSIG AAAA 5 4 43200 20110207233212 20110108233212 26982 isc.org.
TEe9uq22k1zAauhxfCPFaaggUkip5ltBVEDjRdAcDUiZenKAgsfeJwo1 JN2pkxW0aecawDjDnF2V2W2ekqEdN4C+9UBn76BAgczC0qoRWYBZGdi4
13+utDlDh/94I4H4BWNhbyxqa1GRphZoay0t1Gay8CdXbGjweS1S3/ob yoY=

DiG

```
;; Query time: 1 msec
;; SERVER: 204.62.249.35#53(204.62.249.35)
;; WHEN: Thu Jan 13 21:42:00 2011
;; MSG SIZE  rcvd: 1755
```

DiG

- many options to completely control the query
  - Follow the DNS tree: +trace
  - Expanded format: +multiline
    - does more than the name tells
  - Concise: +short
    - includes only the **ANSWER** section
      - so if response has now ANSWER, you see nothing.
  - beware, some may be confusing
    - +[no]vc, +bufsize=*nnn*, +[no]ignore

Using DiG

–By default DiG issues recursive queries (rd bit is set).

- Most auth servers will say recursion is not available

```
$ dig @f.root-servers.net

; <<>> DiG 9.7.2-P3 <<>> @f.root-servers.net
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16477
;; flags: qr aa rd; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL:
15
;; WARNING: recursion requested but not available
```

- Some may deny responding to the query.

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 33598
```

–Use +norecurse to turn off if you hit this

Using DiG

- check all nameservers for a zone

  +nssearch

DiG and DNSSEC

- Standard DiG will show DNSSEC info if you ask for it (+dnssec option)
- However, for debugging it is much more useful if you compile DiG with the SIGCHASE option
  - STD_CDEFINES='-DDIG_SIGCHASE=1' ./configure
- If you want to verify the signatures, you need to supply the key
  - »obtain the root key from a trusted source if possible
    https://data.iana.org/root-anchors/
    or even http://dns.icann.org/ksk/ds19036/

drill

- Written and maintained by NLNet Labs
  - –now a part of ldns, a generic DNS library
  - –was developed originally with DNSSEC in mind
  - –Very similar to DiG in functionality and output format.
    - Choose the one you like better
  - –Install ldns or use packaging systems
    - FreeBSD ports

Using drill

- Control over use of EDNS/TCP
  - (-a and -b)
- Trace option attempts DNSSEC validation if it has access to a trust anchor
  - trust anchors can be specified as DNSKEY or as DS

Drill and DiG

- Slightly different syntax respect to DiG

Feature	DiG	drill
DNSSEC	+dnssec	-D
trace	+trace	-T
chase signatures	+sigchase (1)	-S
EDNS buf size	+bufsize=*nnn*	-b *nnn*
flags	each has an option	-o *xx*
reverse lookup(in-addr)	-x	-x
Use TCP	+tcp	-t
Use only UDP	+notcp	-u

(1) Must be explicitly compiled in

drill and DiG - output

```
$ dig isc.org soa  +dnssec
; <<>> DiG 9.7.2-P3 <<>> isc.org soa +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43855
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;isc.org.                       IN      SOA

;; ANSWER SECTION:
isc.org.                42939   IN      SOA     ns-int.isc.org. hostmaster.isc.org. 2011010900 7200 3600 24796800
3600
isc.org.                42939   IN      RRSIG   SOA 5 2 43200 20110207233212 20110108233212 26982 isc.org.
IKWLI12gYtcFE5zYKvuxRSCKKU0NiIpHBy+nsTT8FSVpef1FQsG6F2Zc
+FgKrURG7IpfDi2AoHovd6uqsqG2YqFqib2s4lLw8NWCtfRyvZcpJEz+
ie9SrUgYFuj9iT8R2rVPOD3sMfH4SAZ9Etd0axz0UC/OJcMPQ7xN4AjZ YjA=

;; AUTHORITY SECTION:
isc.org.                366     IN      NS      sfba.sns-pb.isc.org.
isc.org.                366     IN      NS      ns.isc.afilias-nst.info.
isc.org.                366     IN      NS      ord.sns-pb.isc.org.
isc.org.                366     IN      NS      ams.sns-pb.isc.org.
isc.org.                42983   IN      RRSIG   NS 5 2 43200 20110207233212 20110108233212 26982 isc.org.
mo82HW/2bEi4UekDGRd50xUN6Q85Q2llCxVZXJ7HkumyUTEZFzqpix/a CnBYjBvpvAW1rRr/
4BTVj33e8tTRgKeV0bT5JG+HVirRAHBISKI+p3ed
yNHjYb0PUsN5WD6efiZxGvkFAGWhZRUjSBEiWiIEFWIjjEvV/ywkuGLC uHo=

;; ADDITIONAL SECTION:
ns.isc.afilias-nst.info. 36569  IN      A       199.254.63.254
ns.isc.afilias-nst.info. 36569  IN      AAAA    2001:500:2c::254
sfba.sns-pb.isc.org.    42393   IN      A       149.20.64.3
sfba.sns-pb.isc.org.    42392   IN      AAAA    2001:4f8:0:2::19
sfba.sns-pb.isc.org.    42393   IN      RRSIG   A 5 4 43200 20110207233212 20110108233212 26982 isc.org.
bk/5OoOZuC7m2QVpy4HP8cIVUCezNIGMgfu3toBjPx7TB++bCJohyAg5 m9Pnz9vaYH9y1/HkKVN/UHYzRRM
+TOgKwGvjR5P0jf0Tf6l0QmoASVDI naQgODMWjpO2N5J25afzPaOfnHhYeVhits4ZepxwR/ArdfIHppqprtCq
SKs=
sfba.sns-pb.isc.org.    42392   IN      RRSIG   AAAA 5 4 43200 20110207233212 20110108233212 26982
isc.org. R6Id3didvV3vBO0LUkiELmrOHh1/GU5jEmdDDqanrHGzxgI3/WQRETCX
MkQc0MYJ9+uXd9cpHVyjcz1tZCMUtHUsstbupoLm8+GU3ewShSxVYlQm
fHsJ89lLaMJjUolg0RQQ7XFBnvTgHDHznmnXrt5gLzhdNJ1V1Yaiy0hC 9kI=

;; Query time: 1 msec
;; SERVER: 204.62.249.35#53(204.62.249.35)
;; WHEN: Fri Jan 14 11:51:14 2011
;; MSG SIZE  rcvd: 945
```

```
$  drill -D isc.org soa
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 22247
;; flags: qr rd ra ; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 6
;; QUESTION SECTION:
;; isc.org.     IN      SOA

;; ANSWER SECTION:
isc.org.        42929   IN      SOA     ns-int.isc.org. hostmaster.isc.org. 2011010900 7200 3600
24796800 3600
isc.org.        42929   IN      RRSIG   SOA 5 2 43200 20110207233212 20110108233212 26982
isc.org. IKWLI12gYtcFE5zYKvuxRSCKKU0NiIpHBy+nsTT8FSVpef1FQsG6F2Zc
+FgKrURG7IpfDi2AoHovd6uqsqG2YqFqib2s4lLw8NWCtfRyvZcpJEz
+ie9SrUgYFuj9iT8R2rVPOD3sMfH4SAZ9Etd0axz0UC/OJcMPQ7xN4AjZYjA= ;{id = 26982}

;; AUTHORITY SECTION:
isc.org.        356     IN      NS      sfba.sns-pb.isc.org.
isc.org.        356     IN      NS      ns.isc.afilias-nst.info.
isc.org.        356     IN      NS      ams.sns-pb.isc.org.
isc.org.        356     IN      NS      ord.sns-pb.isc.org.
isc.org.        42973   IN      RRSIG   NS 5 2 43200 20110207233212 20110108233212 26982
isc.org. mo82HW/2bEi4UekDGRd50xUN6Q85Q2llCxVZXJ7HkumyUTEZFzqpix/
aCnBYjBvpvAW1rRr/4BTVj33e8tTRgKeV0bT5JG+HVirRAHBISKI
+p3edyNHjYb0PUsN5WD6efiZxGvkFAGWhZRUjSBEiWiIEFWIjjEvV/ywkuGLCuHo= ;{id =
26982}

;; ADDITIONAL SECTION:
ns.isc.afilias-nst.info.        36559   IN      A       199.254.63.254
ns.isc.afilias-nst.info.        36559   IN      AAAA    2001:500:2c::254
sfba.sns-pb.isc.org.    42383   IN      A       149.20.64.3
sfba.sns-pb.isc.org.    42382   IN      AAAA    2001:4f8:0:2::19
sfba.sns-pb.isc.org.    42383   IN      RRSIG   A 5 4 43200 20110207233212 20110108233212
26982 isc.org. bk/5OoOZuC7m2QVpy4HP8cIVUCezNIGMgfu3toBjPx7TB+
+bCJohyAg5m9Pnz9vaYH9y1/HkKVN/UHYzRRM
+TOgKwGvjR5P0jf0Tf6l0QmoASVDInaQgODMWjpO2N5J25afzPaOfnHhYeVhits4ZepxwR/
ArdfIHppqprtCqSKs= ;{id = 26982}
sfba.sns-pb.isc.org.    42382   IN      RRSIG   AAAA 5 4 43200 20110207233212
20110108233212 26982 isc.org. R6Id3didvV3vBO0LUkiELmrOHh1/GU5jEmdDDqanrHGzxgI3/
WQRETCXMkQc0MYJ9+uXd9cpHVyjcz1tZCMUtHUsstbupoLm8+GU3ewShSxVYlQmfHsJ89lL
aMJjUolg0RQQ7XFBnvTgHDHznmnXrt5gLzhdNJ1V1Yaiy0hC9kI= ;{id = 26982}

;; Query time: 0 msec
;; EDNS: version 0; flags: do ; udp: 4096
;; SERVER: 204.62.249.35
;; WHEN: Fri Jan 14 11:51:23 2011
;; MSG SIZE  rcvd: 945
```

Zone verification

- Local tools
  - named-checkzone
- Network services
  - zonecheck.fr
  - dnscheck.iis.se

named-checkzone

- Part of bind
  - –checks zone contents from a file in a disk
  - –Good practice to always run a verification script before loading the zone on the server
    - •can be done off-line, without loading the server
    - •prevents silly mistakes, may detect bugs in generation process
  - –can be rather verbose
    - •tune options to report only errors you care about (e.g. types of glue)

named-checkzone

- options to control what MX Records are acceptable (e.g. addresses or CNAME)
- Tricky part are the glue checks
  - –sibling glue, local checks, full checks

otherexample.xx NS ns3.example.xx
otherexample.xx NS ns4.example.xx

example.xx NS ns1.otherexample.xx
example.xx NS ns2.otherexample.xx

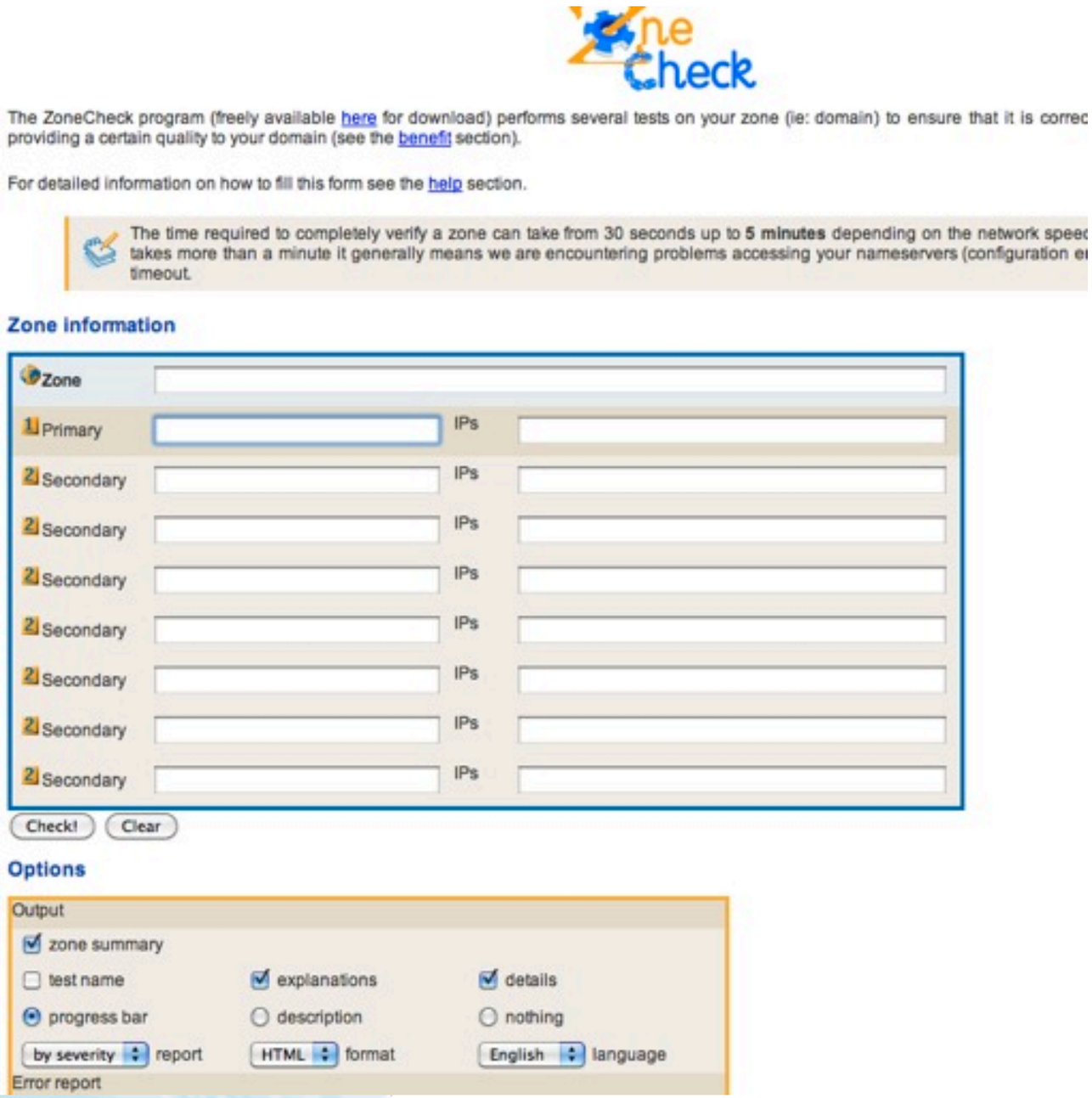
zonecheck.fr

- Developed and maintained by AFNIC (.fr registry)
- Available as
  - online service
  - download
- Online is good for casual use
- Download and install for more control and accessibility

zonecheck.fr

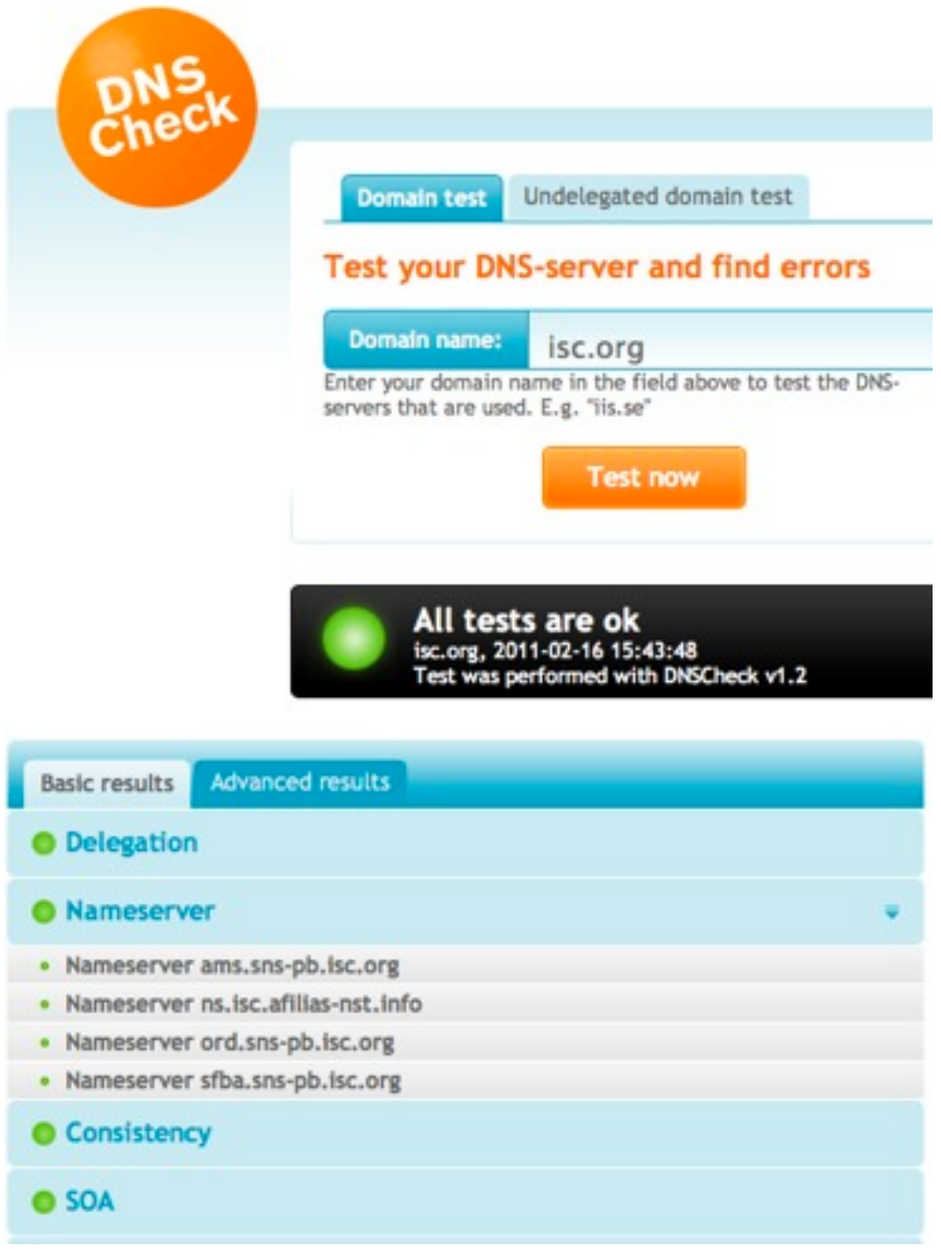
- Local installation can be a bit tedious but offers possibility of tailoring verification policies to registry policies.
- Available as command line tool or local web installation

Zonecheck.fr



dnscheck.iis.se

- Developed and maintained by IIS (.se registry)
  - Simple and well structured
  - can take some time to go through tests



Instant analysis

- Ready made
  - –dnstop
- Toolkits
  - –wireshark/tcpdump/libpcap
  - –dnscap
- Other
  - –DNS-OARC DNS Reply Size Test Server
- Passive DNS
  - –ISC SIE, dnslogger

dnstop

- Like *top*, but for dns queries instead of processes
  - Written by the *Measurement Factory*
- download from
  - http://dns.measurement-factory.com/tools/dnstop/source.html

```
Queries: 0 new, 52 total
Sun Jan 16 15:10:03 2011

Sources              Count      %   cum%
-------------- --------- ------ ------
192.0.32.242            18   34.6   34.6
204.152.187.13          11   21.2   55.8
192.0.36.240            10   19.2   75.0
204.152.187.14           6   11.5   86.5
149.20.54.152            4    7.7   94.2
87.217.89.178            2    3.8   98.1
204.8.46.130             1    1.9  100.0
```

dnstop

- Can use standard bpf rules to filter traffic, so you can monitor what you want
- Some common options
  - ignore specific servers (e.g. your own resolvers)
  - ignore specific domains
- May require root or have setuid set to access the interface to capture traffic.

Toolkits

- libpcap/tcpdump/wireshark
  - build your own tools with libpcap
  - use ad-hoc filters
    - example...
  - wireshark is quite good in deciphering packets, including DNS
  - Sometimes too overblown for the job

dnscap

Main features

- Focused on DNS
- Understands both IPv4 and IPv6
- Captures UDP, TCP, and **IP fragments**.
- Collect only queries, responses, or both
- Collect for only certain source/destination addresses
- Periodically creates new pcap files (-t option)
- Spawns an upload script after closing a pcap file
- Will start and stop collecting at specific times

- Download from https://www.dns-oarc.net/tools/dnscap

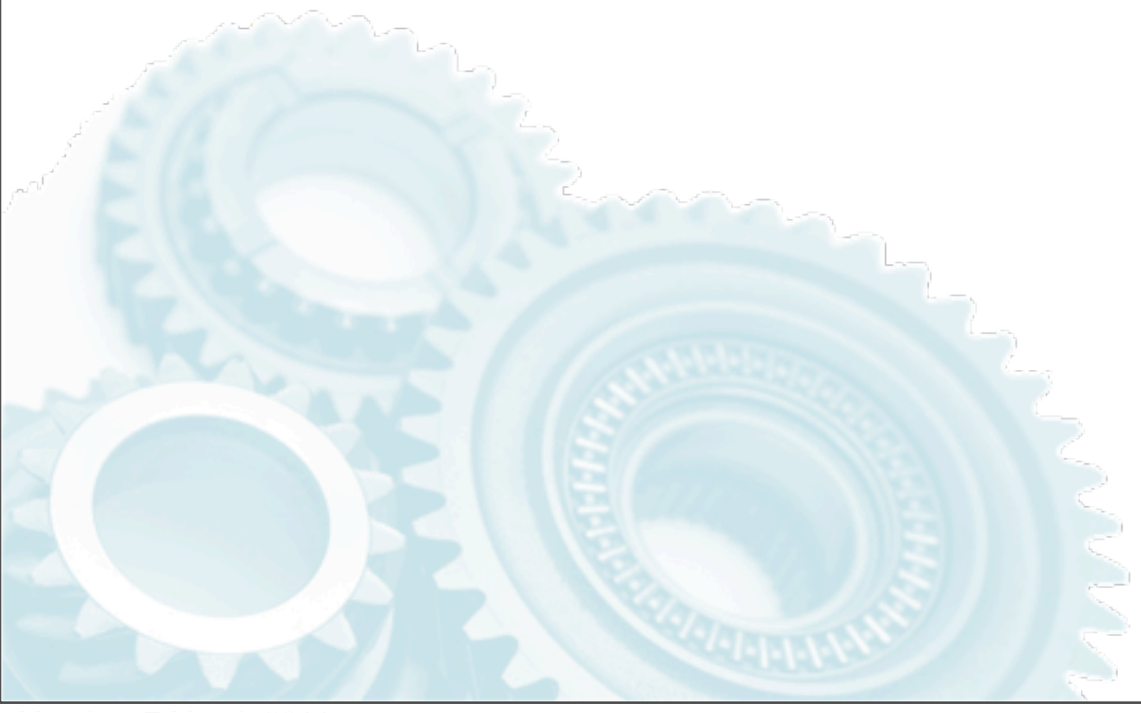
dnscap

- Examples of usage....
  - –dnscap -i en0 -g (output dig format if using libbind)

- capture file management
  - –k executes external command (e.g. gzip)
  - –w write files (and specify a basename)
    - the basename gets a timestamp appended
    - the file is in pcap format but reassemblyu has been done
  - –t time limit, to rotate files (also possible based on size)

dnscap

- -x use regular expressions to filter packets



ncap

- pcap substitute
  - performs IP reassembly and generates framing-independent portable output
  - writes output in ncap format
  - can be augmented with modules/plugins to perform specific analysis

Passive DNS

- Collect DNS information as it enters or leaves a nameserver
  - no active DNS role
  - specialised data capture, with tools focused on DNS
- dnslogger
- ISC SIE

dnslogger

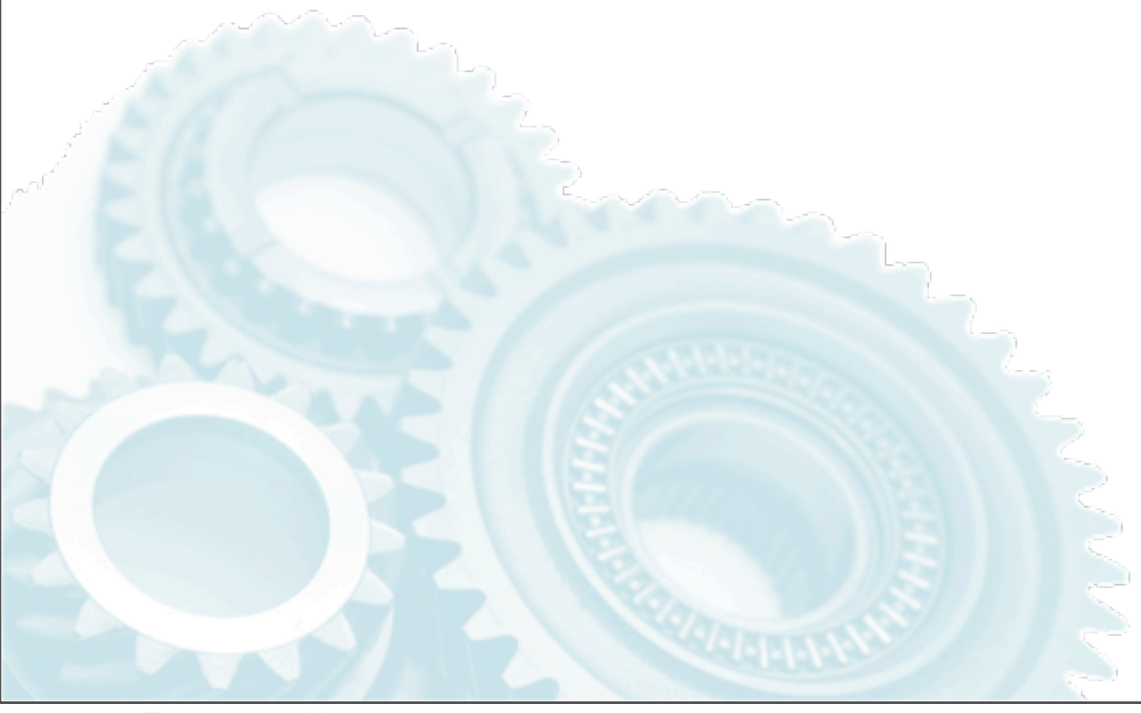
- Can be used to reconstruct a zone from observed DNS messages in a network

libnmsg/dnsqr

- libnmsg implements a generic message format to carry many types of streaming data
- dnsqr is a module for libnmsg desgined for Passive DNS capture
- capture, optionally with filters and encapsulates it in nmsg format
- does packet reassembly and can track "flows"

Long term analysis

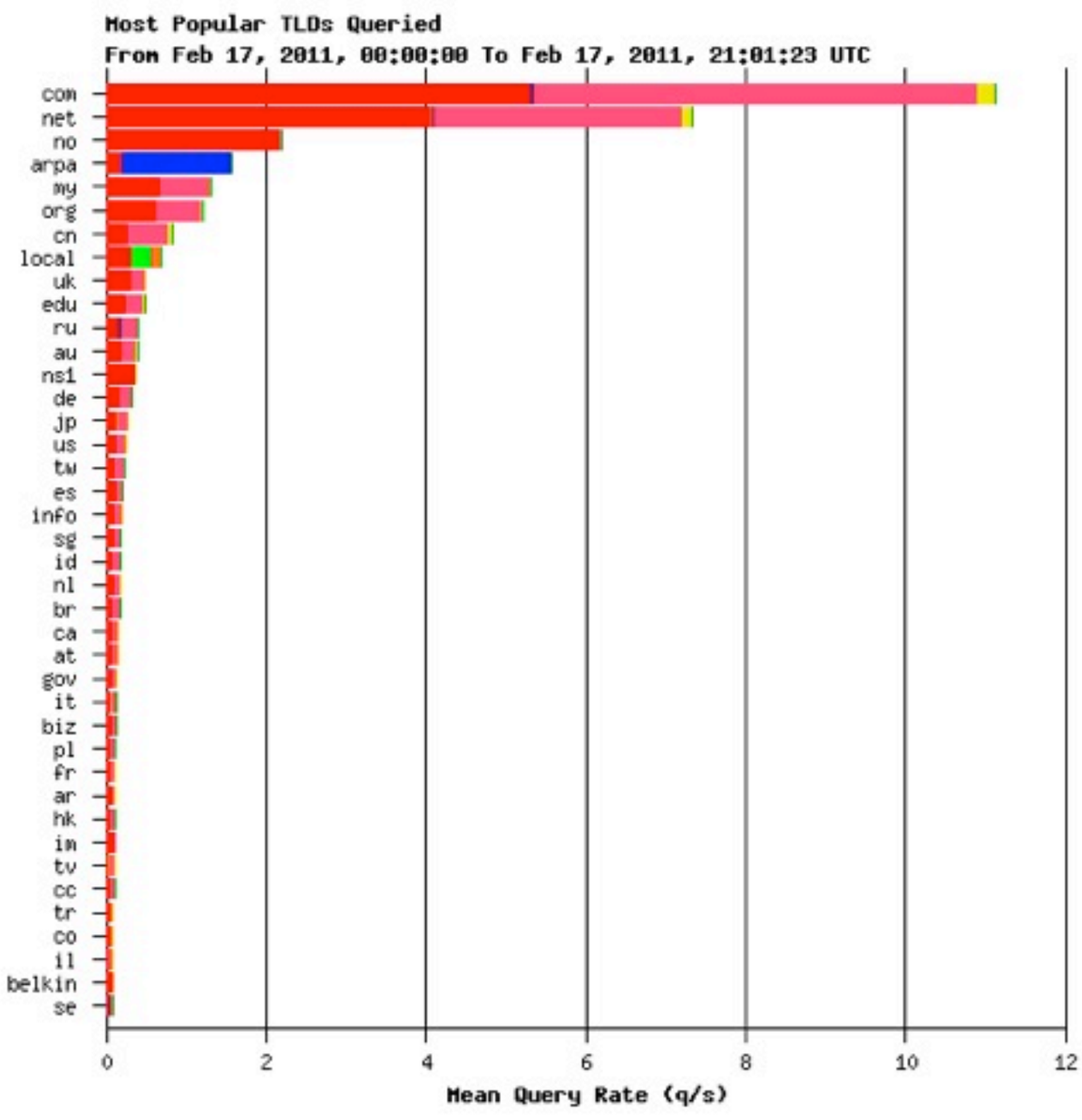
- Run your own
  - DSC
  - DNS2DB
- Network based services
  - RIPE DNSMON

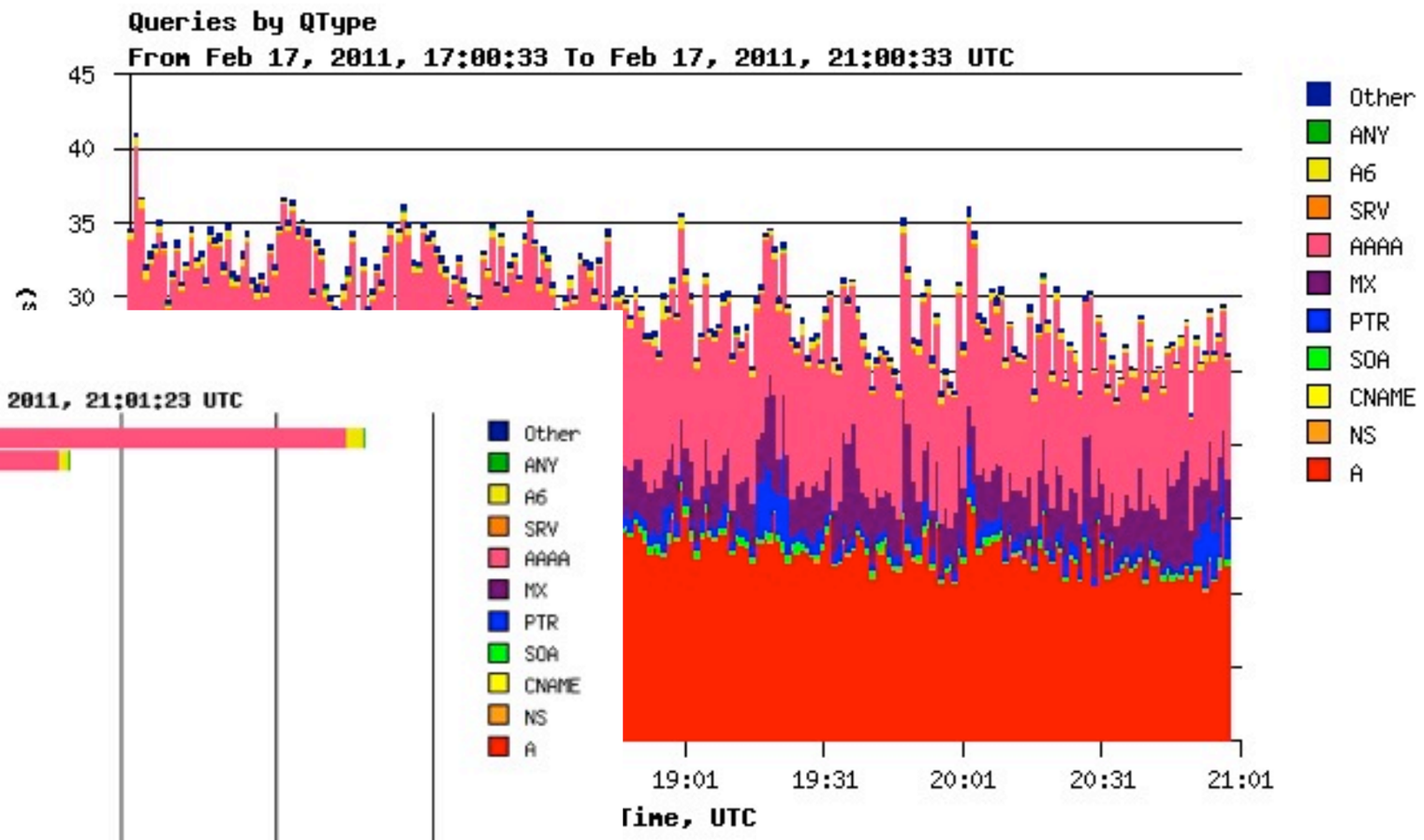


DSC

- DNS Statistics collector
  - –can be tricky to get right
  - –does a real good job of collecting and presenting ongoing statistics for your DNS
  - –based on packet captures at the servers
    - easy if you run your own servers
  - –developed originally by the *Measurement Factory* for OARC, now maintained by OARC
  - –Available as free download

DSC


Most Popular TLDs Queried
From Feb 17, 2011, 00:00:00 To Feb 17, 2011, 21:01:23 UTC
com
net
no
arpa
my
org
cn
local
uk
edu
ru
au
ns1
de
jp
us
tw
es
info
sg
id
nl
br
ca
at
gov
it
biz
pl
fr
ar
hk
im
tv
cc
tr
co
il
belkin
se
0
2
4
6
8
10
12
Mean Query Rate (q/s)


Queries by QType
From Feb 17, 2011, 17:00:33 To Feb 17, 2011, 21:00:33 UTC
45
40
35
30
Other
ANY
A6
SRV
AAAA
MX
PTR
SOA
CNAME
NS
A
19:01
19:31
20:01
20:31
21:01
Time, UTC

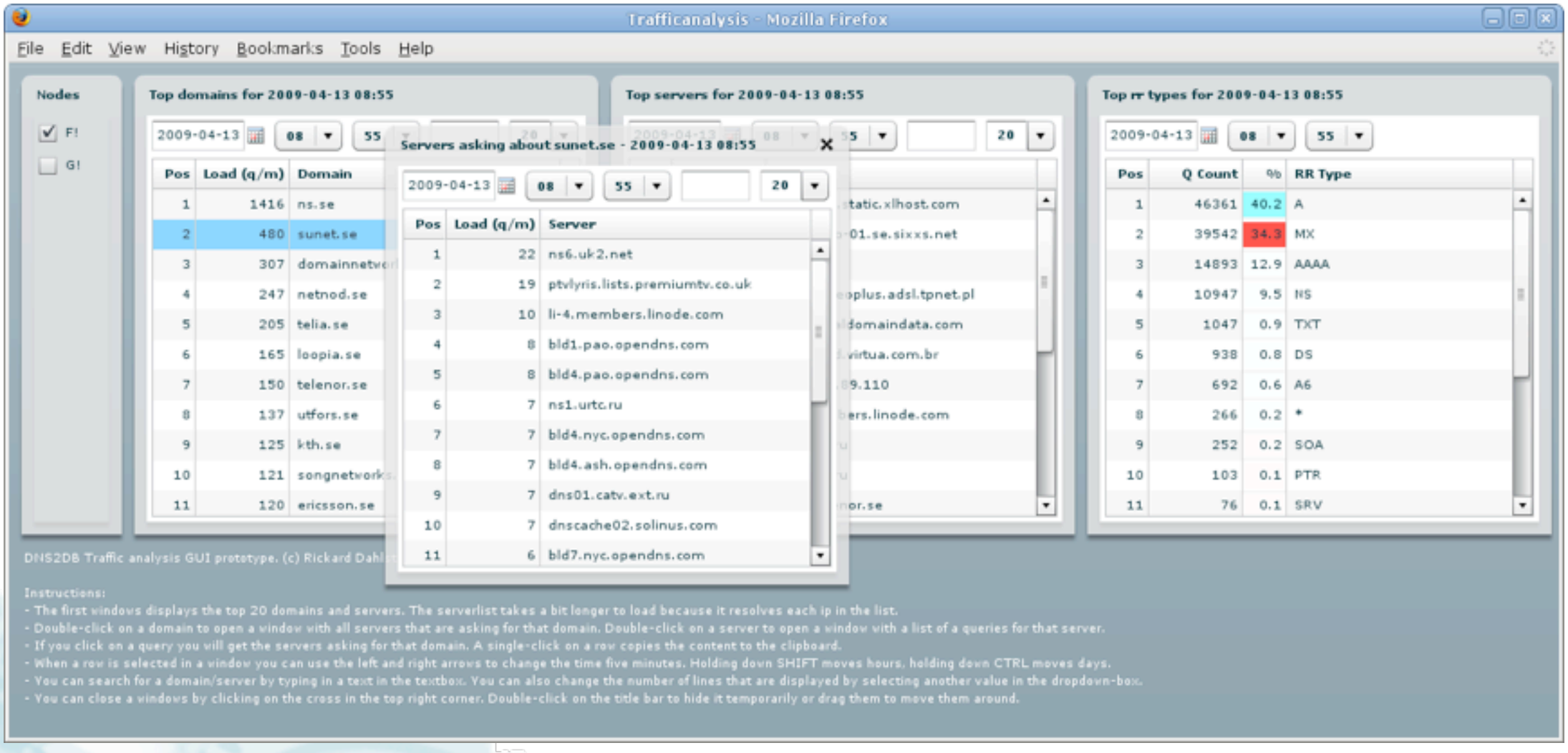
DSC

- Can be used on the DNS servers themselves, using pcap catpure
- if load is a concern, capture traffic using a passive tap
- If measuring more than 30-40 nodes, use some logical grouping for processing in multiple servers and merge the results

DNS2DB

- Produced and maintained by IIS (.se)
- converts raw pcap-files with DNS-traffic to SQLite-databases.
  - –includes basic GUI to look at data.
- Needs libtrace from Waikato University
- Uses Adobe flex to run the front end

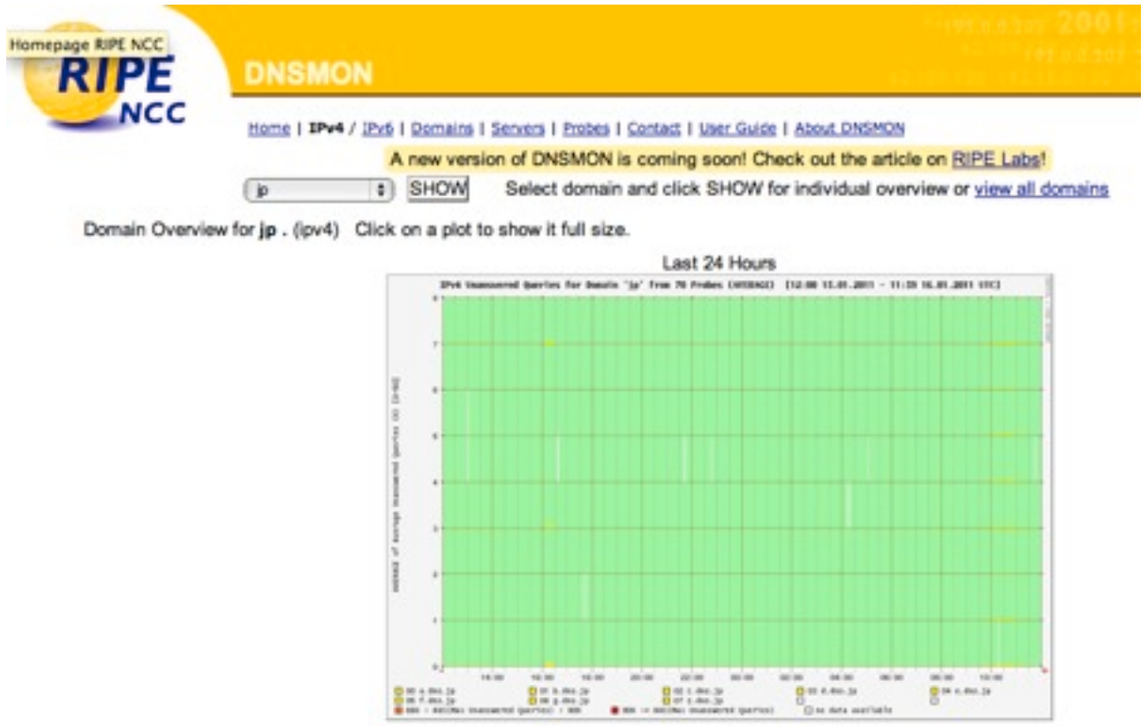
DNS2DB


Trafficanalysis - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Nodes
F!
G!
Top domains for 2009-04-13 08:55
2009-04-13 08 55 20
Pos Load (q/m) Domain
1 1416 ns.se
2 480 sunet.se
3 307 domainnetwo
4 247 netnod.se
5 205 telia.se
6 165 loopia.se
7 150 telenor.se
8 137 utfors.se
9 125 kth.se
10 121 songnetwork
11 120 ericsson.se
Servers asking about sunet.se - 2009-04-13 08:55
2009-04-13 08 55 20
Pos Load (q/m) Server
1 22 ns6.uk2.net
2 19 ptvlyris.lists.premiumtv.co.uk
3 10 li-4.members.linode.com
4 8 bld1.pao.opendns.com
5 8 bld4.pao.opendns.com
6 7 ns1.urtc.ru
7 7 bld4.nyc.opendns.com
8 7 bld4.ash.opendns.com
9 7 dns01.catv.ext.ru
10 7 dnscache02.solinus.com
11 6 bld7.nyc.opendns.com
Top servers for 2009-04-13 08:55
20
tatic.xlhost.com
01.se.sixxs.net
oplus.adsl.tpnet.pl
domaindata.com
virtua.com.br
9.110
ers.linode.com
or.se
Top rr types for 2009-04-13 08:55
2009-04-13 08 55
Pos Q Count % RR Type
1 46361 40.2 A
2 39542 34.3 MX
3 14893 12.9 AAAA
4 10947 9.5 NS
5 1047 0.9 TXT
6 938 0.8 DS
7 692 0.6 A6
8 266 0.2 *
9 252 0.2 SOA
10 103 0.1 PTR
11 76 0.1 SRV
DNS2DB Traffic analysis GUI prototype. (c) Rickard Dahl
Instructions:
- The first windows displays the top 20 domains and servers. The serverlist takes a bit longer to load because it resolves each ip in the list.
- Double-click on a domain to open a window with all servers that are asking for that domain. Double-click on a server to open a window with a list of a queries for that server.
- If you click on a query you will get the servers asking for that domain. A single-click on a row copies the content to the clipboard.
- When a row is selected in a window you can use the left and right arrows to change the time five minutes. Holding down SHIFT moves hours, holding down CTRL moves days.
- You can search for a domain/server by typing in a text in the textbox. You can also change the number of lines that are displayed by selecting another value in the dropdown-box.
- You can close a windows by clicking on the cross in the top right corner. Double-click on the title bar to hide it temporarily or drag them to move them around.

RIPE DNSMON

- Online service available at
  - http://dnsmon.ripe.net/dns-servmon/
- Shows measurements of DNS servers from selected sites (uses same platform as RIPE Test Trafffic)
- Data is available with a slight delay to avoid silly usage.
- Need to get used to read the graphics

RIPE DNSMON


Homepage RIPE NCC
RIPE NCC
DNSMON
Home | IPv4 / IPv6 | Domains | Servers | Probes | Contact | User Guide | About DNSMON
A new version of DNSMON is coming soon! Check out the article on RIPE Labs!
jp
SHOW
Select domain and click SHOW for individual overview or view all domains
Domain Overview for jp . (ipv4) Click on a plot to show it full size.
Last 24 Hours

Other useful tools

- fpdns
  - fingerprint DNS servers
  - Needs some refresh but is still useful for debugging
  - Send various packets to servers and profiles them according to tables of observed behaviour

$ fpdns cumin.apnic.net.

fingerprint (cumin.apnic.net., 202.12.29.59): Nominum ANS

$ fpdns cumin.apnic.net.

fingerprint (a.root-servers.net, 198.41.0.4): VeriSign ATLAS

References

- dig - http://www.isc.org/software/bind
- drill - http://www.nlnetlabs.nl/projects/ldns/
- named-checkzone - http://www.isc.org/software/bind
- zonecheck.fr - http://www.zonecheck.fr/
- dnscheck - http://dnscheck.iis.se/
- https://github.com/dotse/dnscheck
- dnstop - http://dns.measurement-factory.com/tools/dnstop/
- dnslogger - http://www.enyo.de/fw/software/dnslogger/
- dnscap - Download from https://www.dns-oarc.net/tools/dnscap
- DSC - https://www.dns-oarc.net/tools/dsc
- dns2db - https://github.com/dotse/dns2db
- RIPE DNSMON - http://dnsmon.ripe.net/dns-servmon/
- FPDNS - http://code.google.com/p/fpdns/

Questions?

joao@isc.org