

DNS Debugging and monitoring

João Damas
Shane Kerr



Outline

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



The basics

- DNS and errors
- Basic Tools
 - nslookup
 - DiG
 - drill



DNS and errors

- DNS has a very limited set of error/return codes (RCODEs)

Registry Name: DNS RCODES

Decimal	Name	Description	Reference
0	NoError	No Error	[RFC1035]
1	FormErr	Format Error	[RFC1035]
2	ServFail	Server Failure	[RFC1035]
3	NXDomain	Non-Existent Domain	[RFC1035]
4	NotImp	Not Implemented	[RFC1035]
5	Refused	Query Refused	[RFC1035]
6	YXDomain	Name Exists when it should not	[RFC2136]
7	YXRSet	RR Set Exists when it should not	[RFC2136]
8	NXRSet	RR Set that should exist does not	[RFC2136]
9	NotAuth	Server Not Authoritative for zone	[RFC2136]
10	NotZone	Name not contained in zone	[RFC2136]
11-15	Unassigned		
16	BADVERS	Bad OPT Version	[RFC2671]
16	BADSIG	TSIG Signature Failure	[RFC2845]
17	BADKEY	Key not recognized	[RFC2845]
18	BADTIME	Signature out of time window	[RFC2845]
19	BADMODE	Bad TKEY Mode	[RFC2930]
20	BADNAME	Duplicate key name	[RFC2930]
21	BADALG	Algorithm not supported	[RFC2930]
22	BADTRUNC	Bad Truncation	[RFC4635]
23-3840	Unassigned		
3841-4095	Reserved for Private Use		[RFC6195]
4096-65534	Unassigned		
65535	Reserved, can be allocated by Standards Action		[RFC6195]

SERVFAIL

- Generic error for a recursive server
 - now with added DNSSEC flavours
 - any dnssec validation failure is exposed to the client as servfail
- on Authoritative servers the most common issue is the server having problem accessing the zone data

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

- 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

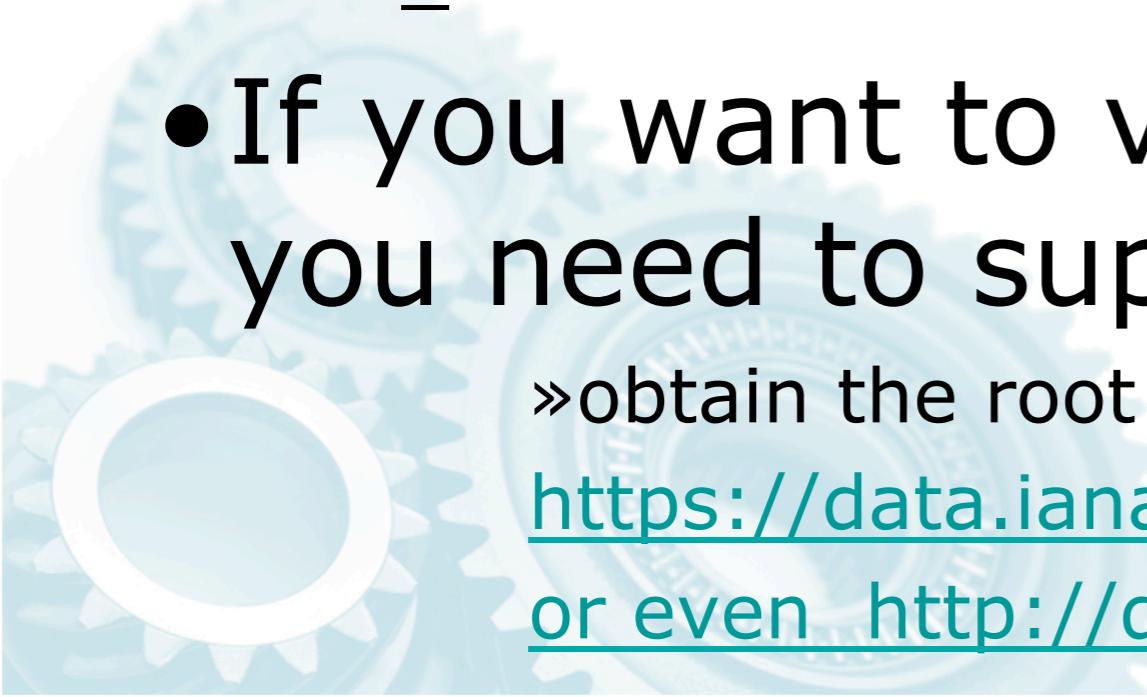
Using DiG

- 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 Idns, 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 Idns 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
 - e.g. `drill -T -k $key`

Drill and DiG

- Slightly different syntax respect to DiG

Feature	DIG	drill
DNSSEC	+dnssec	-D
trace	+trace	-T
chase signatures	+sigchase (1) <small>(1) Must be explicitly compiled in</small>	-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

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 3600isc.org. 42939 IN RRSIG SOA 5 2 43200 20110207233212 20110108233212 26982 isc.org. IKWLI12gYtcFE5zYKvuxRSCKKU0NilpHBy+nsTT8FSVpef1FQsG6F2Zc +FgKrURG7lpfDi2AoHovd6uqsqG2YqFqib2s4lLw8NWCTfRyvZcpJEz+ 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/ 2bEi4UekDGRd50xUN6Q85Q2lICxVZXJ7HkumyUTEZFzqpix/a CnBYjBvpvAW1rRr/4BTvj33e8tTRgKeV0bT5JG +HVirRAHBISKI+p3ed yNHjYb0PUsN5WD6efiZxGvkFAGWhZRUjsBEiWiEFWIjjEvV/ywkuGLC uHo=;; ADDITIONAL SECTION:ns.isc.afilias-nst.info. 36569 IN A 199.254.63.254ns.isc.afilias-nst.info. 36569 IN AAAA 2001:500:2c::254sfba.sns-pb.isc.org. 42393 IN A 149.20.64.3sfba.sns-pb.isc.org. 42392 IN AAAA 2001:4f8:0:2::19sfba.sns-pb.isc.org. 42393 IN RRSIG A 5 4 43200 20110207233212 20110108233212 26982 isc.org. bk/5OoOZuC7m2QVpy4HP8clVUCezNIGMgf3toBjPx7TB++bCJohyAg5 m9Pnz9vaYH9y1/HkKVN/UHYzRRM +TOgKwGvjR5P0jf0Tf6l0QmoASVDI naQgODMWjpO2N5J25afzPaOfnHhYeVhits4ZepxwR/ArdflHppqprtCq SKs=sfba.sns-pb.isc.org. 42392 IN RRSIG AAAA 5 4 43200 20110207233212 20110108233212 26982 isc.org. R6Id3didvV3vBO0LUkiELmrOHh1/GU5jEmddDqanrHGzxgl3/WQRETCX MkQc0MYJ9+uXd9cpHVyjcz1tZCMUtHUsstbupoLm8+GU3ewShSxVYIQm fHsJ89ILaMJjUolg0RQQ7XFBNvTgHDHznmnXrt5gLzhdNJ1V1Yaiy0hC 9kl=;; 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 3600isc.org. 42929 IN RRSIG SOA 5 2 43200 20110207233212 20110108233212 26982 isc.org. IKWLI12gYtcFE5zYKvuxRSCKKU0NilpHBy+nsTT8FSVpef1FQsG6F2Zc +FgKrURG7lpfDi2AoHovd6uqsqG2YqFqib2s4lLw8NWCTfRyvZcpJEz+ ie9SrUgYFuj9iT8R2rVPOD3sMfh4SAZ9Etd0axz0UC/OJcMPQ7xN4AjZ YjA= ;{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. 42973 IN RRSIG NS 5 2 43200 20110207233212 20110108233212 26982 isc.org. mo82HW/ 2bEi4UekDGRd50xUN6Q85Q2lICxVZXJ7HkumyUTEZFzqpix/a CnBYjBvpvAW1rRr/ 4BTvj33e8tTRgKeV0bT5JG+HVirRAHBISKI +p3edyNHjYb0PUsN5WD6efiZxGvkFAGWhZRUjsBEiWiEFWIjjEvV/ywkuGLCuHo= ;{id = 26982};; ADDITIONAL SECTION:ns.isc.afilias-nst.info. 36559 IN A 199.254.63.254ns.isc.afilias-nst.info. 36559 IN AAAA 2001:500:2c::254sfba.sns-pb.isc.org. 42383 IN A 149.20.64.3sfba.sns-pb.isc.org. 42382 IN AAAA 2001:4f8:0:2::19sfba.sns-pb.isc.org. 42383 IN RRSIG A 5 4 43200 20110207233212 20110108233212 26982 isc.org. bk/5OoOZuC7m2QVpy4HP8clVUCezNIGMgf3toBjPx7TB+ +bCJohyAg5m9Pnz9vaYH9y1/HkKVN/UHYzRRM +TOgKwGvjR5P0jf0Tf6l0QmoASVDI naQgODMWjpO2N5J25afzPaOfnHhYeVhits4ZepxwR/ ArdfI HppqprtCqSKs= ;{id = 26982}sfba.sns-pb.isc.org. 42382 IN RRSIG AAAA 5 4 43200 20110207233212 20110108233212 26982 isc.org. R6Id3didvV3vBO0LUkiELmrOHh1/ GU5jEmddDqanrHGzxgl3/ WQRETCXMkQc0MYJ9+uXd9cpHVyjcz1tZCMUtHUsstbupoLm8+GU3ewShSxVYIQmfHsJ89ILa MJjUolg0RQQ7XFBNvTgHDHznmnXrt5gLzhdNJ1V1Yaiy0hC9kl= ;{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 file for correctness
- best practice: always run a verification script before loading a zone on a live server
 - can be done off-line, without the server
 - prevents silly mistakes
 - may detect bugs in generation process
- output can be rather verbose
 - tune options to report only errors you care about (e.g. specific glue check types)

named-checkzone: example #1

- \$TTL 1H
\$ORIGIN example.org.
example.org. SOA master hostmaster.example.org. (
 2012031301 ; serial
 3600 ; refresh (1 hour)
 1800 ; retry (30 minutes)
 864000 ; expire (1 week 3 days)
 600 ; negative TTL (10 minutes)
)
 NS ns1
 NS ns2
 MX 100 smtp
 AAAA 2001:DB8::2
ns1 AAAA 2001:DB8::1
ns2 AAAA 2001:DB8:8000::1
smtp AAAA 2001:DB8::2
www CNAME main
main AAAA 2001:DB8::2

named-checkzone: example #1

- Execution can be straightforward:
- \$ /usr/sbin/named-checkzone \
 > example.org example.org.zone
 zone example.org/IN: loaded serial 2012031301
 OK



named-checkzone: example #2

Replace:

smtp AAAA 2001:DB8::2

With:

smtp CNAME main

We then see:

'smtp.example.org' is a CNAME (illegal)

Warning can be disabled by “-M ignore”.

named-checkzone: example #3

- Add:
 - subdomain NS ns1.subdomain
NS ns2.subdomain
ns1.subdomain AAAA 2001:DB8::3
- We then see:
 - 'ns1.subdomain.example.org' (out of zone)
has no addresses records (A or AAAA)
 - 'ns2.subdomain.example.org' has no
REQUIRED GLUE address records (A or AAAA)
 - 'ns2.subdomain.example.org' (out of zone)
has no addresses records (A or AAAA)
 - Warning can be disabled by "-i local", but error
should remain.

named-checkzone: limitations

- cannot check for some errors
 - forgetting to increment SOA serial number
 - zone truncation
 - typos in out-of-zone names
 - missing or extra '.' at end of names
- does not check for some errors
 - DNSSEC: missing signatures, other errors
 - fully vs. partially lame glue issues

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



The ZoneCheck program (freely available [here](#) for download) performs several tests on your zone (ie: domain) to ensure that it is correct providing a certain quality to your domain (see the [benefit](#) section).

For detailed information on how to fill this form see the [help](#) section.



The time required to completely verify a zone can take from 30 seconds up to **5 minutes** depending on the network speed. If it takes more than a minute it generally means we are encountering problems accessing your nameservers (configuration error or timeout).

Zone information

Zone	IPs
1 Primary	
2 Secondary	

Check! **Clear**

Options

Output		
<input checked="" type="checkbox"/> zone summary	<input type="checkbox"/> test name	<input checked="" type="checkbox"/> explanations
<input checked="" type="radio"/> progress bar	<input type="radio"/> description	<input checked="" type="checkbox"/> details
by severity report	HTML format	English language
Error report		

dnscheck.iis.se

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

The screenshot shows the dnscheck.iis.se interface. At the top, there's an orange 'DNS Check' button. Below it, tabs for 'Domain test' and 'Undelegated domain test' are visible, with 'Domain test' being selected. A text input field contains 'isc.org'. A large green button labeled 'Test now' is present. Below the input field, instructions say 'Enter your domain name in the field above to test the DNS-servers that are used. E.g. "iis.se"'.

A prominent black banner at the bottom displays a green lightbulb icon and the text 'All tests are ok' followed by 'isc.org, 2011-02-16 15:43:48' and 'Test was performed with DNSCheck v1.2'.

The main content area is divided into sections: 'Basic results' (selected) and 'Advanced results'. Under 'Basic results', there are sections for 'Delegation', 'Nameserver' (which lists four servers: ams.sns-pb.isc.org, ns.isc.afiliaas-nst.info, ord.sns-pb.isc.org, sfba.sns-pb.isc.org), 'Consistency', and 'SOA'.

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](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 reassembly 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

libnmsg/dnsqr

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

Long term analysis

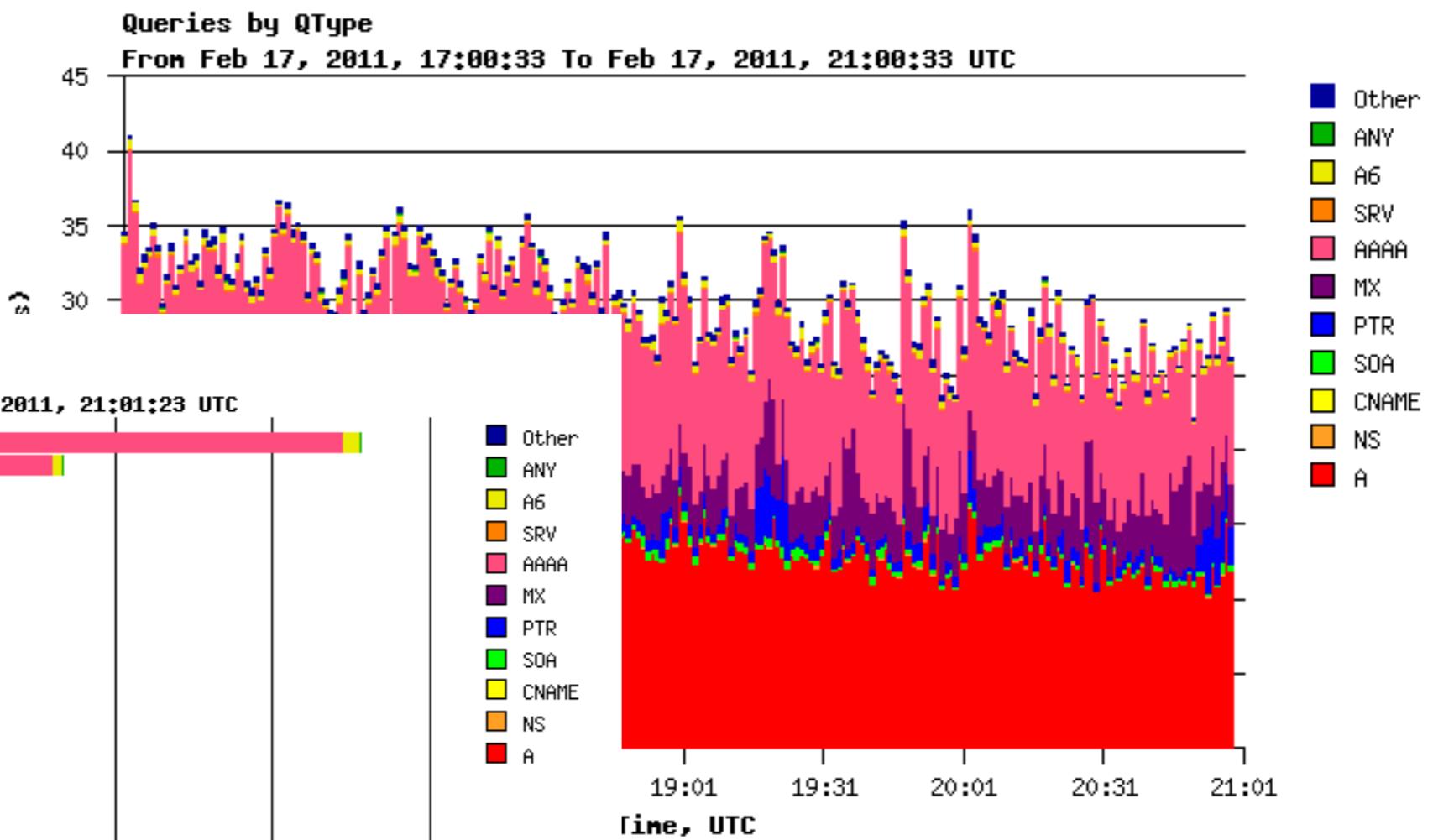
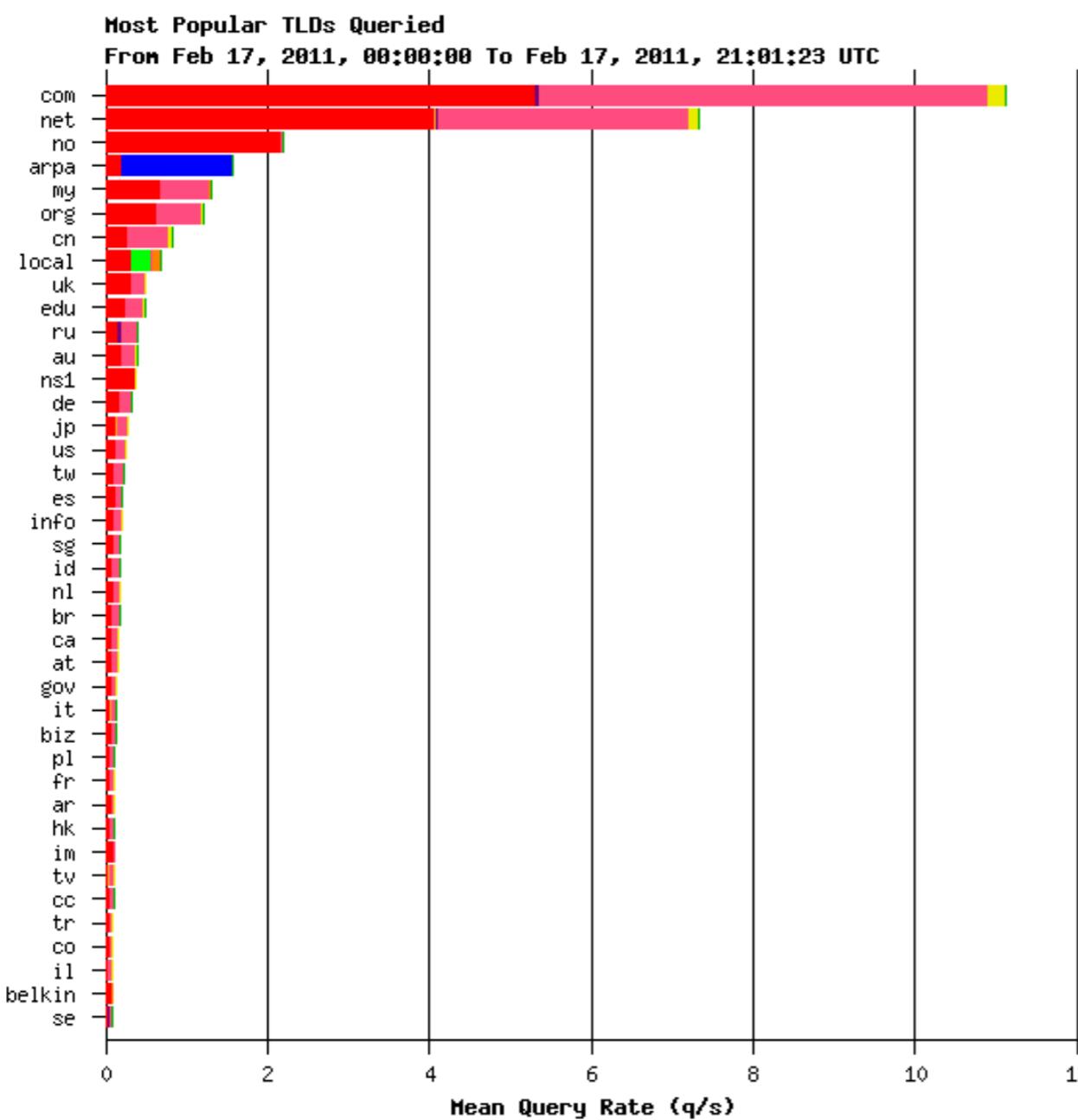
- Run your own
 - DSC
 - DNS2DB
- Network based services
 - RIPE DNSMON



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



DSC

- Can be used on the DNS servers themselves, using pcap capture
- 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

Pos	Load (q/m)	Domain
1	1416	ns.se
2	480	sunet.se
3	307	domainnetwork.se
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	songnetworks.se
11	120	ericsson.se

Top servers for 2009-04-13 08:55

Servers asking about sunet.se - 2009-04-13 08:55

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 rr types for 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 Dahlström 2009

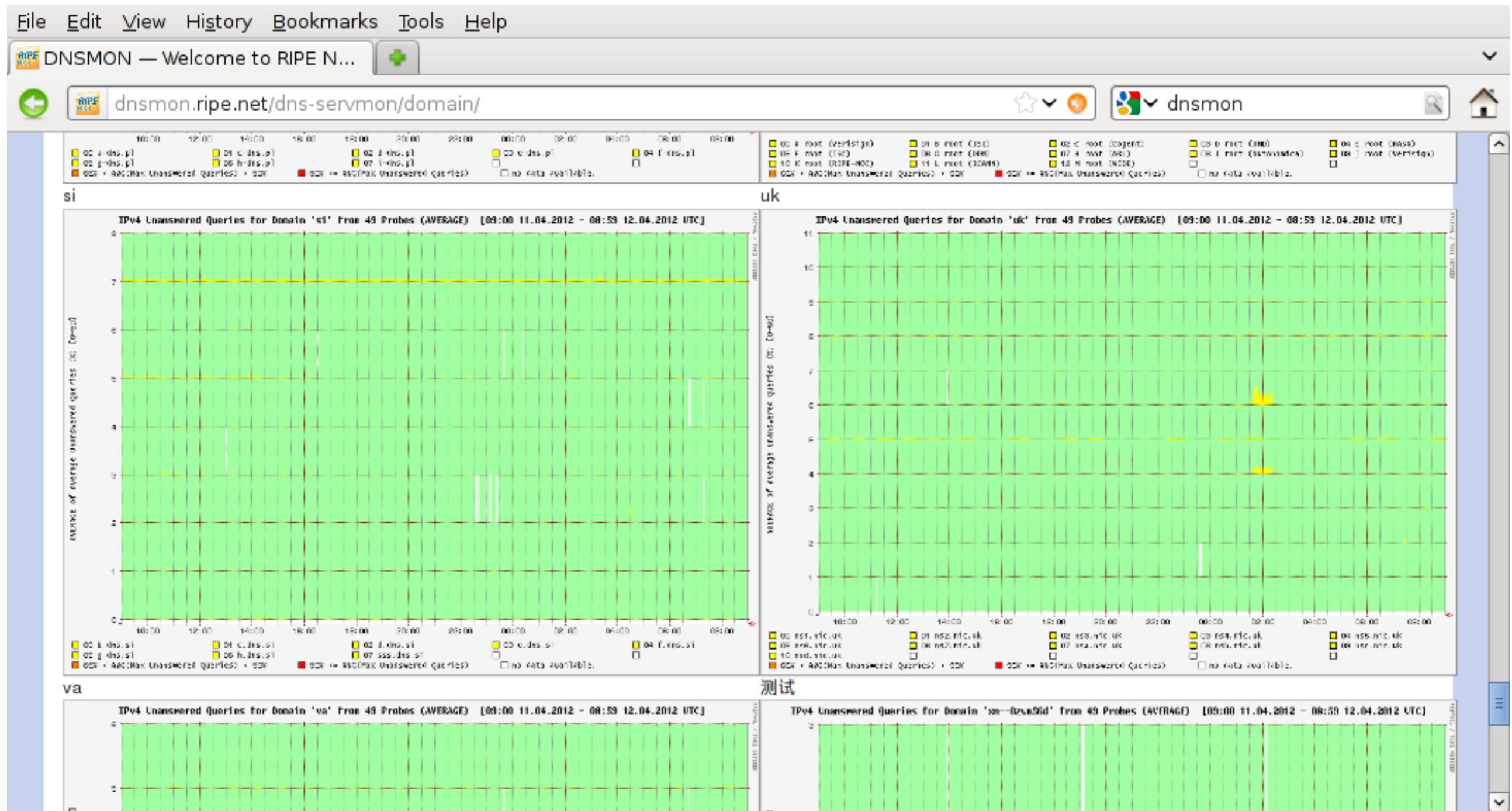
Instructions:

- 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 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.

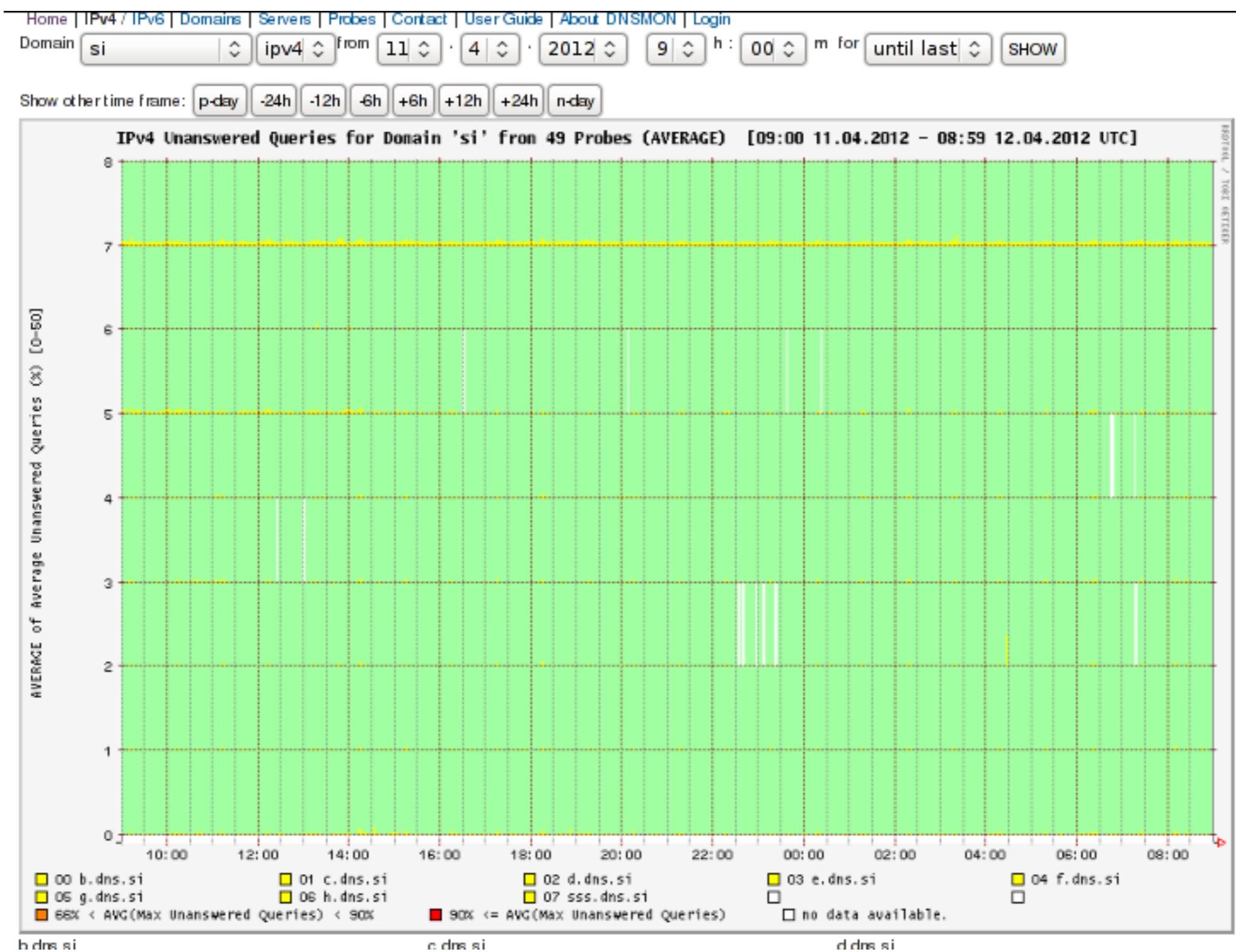
RIPE DNSMON

- Online service available at:
<http://dnsmon.ripe.net/dns-servmon/>
- Shows measurements of DNS servers
 - uses same platform as RIPE Test Traffic
- Data is available with a slight delay
 - Avoids silly usage
 - Immediate data available for subscribers
- Need to learn how to read the graphics

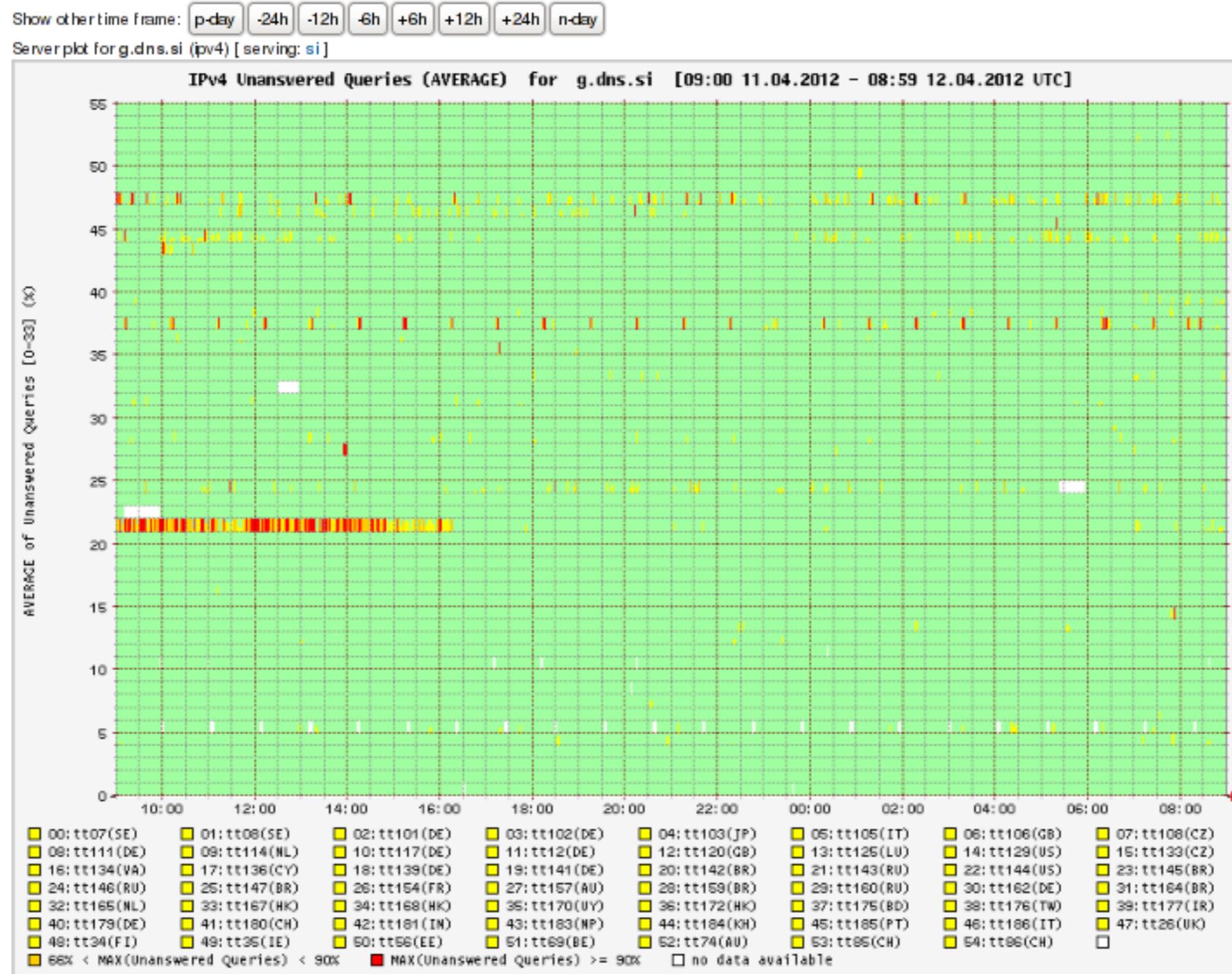
DNSMON: Overview of Domains



DNSMON: Per-Domain View



DNSMON: Per-Server View



RIPE DNSMON: Raw Data

Available via FTP, for example:

<ftp://ftp.ripe.net/test-traffic/dnsmon/data/public/DNS.tt07.ripe.net.20120410>

```
+----- "DNS"
|   +----- test-traffic host originating probe
|   |   +----- Unix epoch timestamp of probe
|   |   |   --- target name server
|
DNS tt07.ripe.net 1334016000 john.vatican.va 0.000000 3 62083 hostname.bind UNREACH
DNS tt07.ripe.net 1334016000 b.gtld-servers.net 0.001658 1 62111 hostname.bind UNKNOWN
DNS tt07.ripe.net 1334016000 d.nic.at 0.000000 3 62087 id.server UNREACH
DNS tt07.ripe.net 1334016000 f.nic.de 0.000000 3 62085 id.server UNREACH
DNS tt07.ripe.net 1334016000 osiris.namex.it 0.060790 1 62115 hostname.bind osiris.namex.
DNS tt07.ripe.net 1334016001 y.nic.eu 0.001118 1 62121 hostname.bind s2.sth
DNS tt07.ripe.net 1334016001 ns5.dns.net.nz 0.033904 1 62120 id.server
DNS tt07.ripe.net 1334016001 b.ip6-servers.arpa 0.111574 1 62119 id.server inaddr.cjr.dns
DNS tt07.ripe.net 1334016001 a.nic.cl 0.244393 1 62116 id.server merced.nic.cl

               |   |   |
               response time --+
               attempts -----+
               port number -----+
               query name -----+
response (answer or error message) -----+
```

Other useful tools

- **fpdns**
 - fingerprint DNS servers
 - Needs some refresh but is still useful for debugging
 - work ongoing - Verisign+kirei
 - 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](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 - <https://github.com/kirei/fpdns>

Questions?

joao@isc.org
shane@isc.org

