Monitoring DNS and DNSSEC

2009-11-06

Niclas Rosell
.SE Registry

Operators

.se

Slaveservers

- 150 servers/instances on the internet:
  - Stockholm, Malmö, Göteborg, Sundsvall, Luleå, Umeå, Amsterdam, Chicago, Los Angeles, Miami, New York, San Fransisco, Ankara, Peking, Bangkok, Bryssel, Colombo, Frankfurt, Helsingfors, Genève, Kuala Lumpur, London, Milano, Mumbai, Oslo, Manilla, Palo Alto, Perth, Doha, Bukarest, Tokyo, Washington, Seattle och Toronto…
- Four different providers, less risk
  - Four different service providers, hardware/software, staff etc.
  - ~6000 queries/second.

.se

Locations of slaveservers

Three important tools

.SE DNSMON based on Nagios

DNSCheck

DNS2db

Monitoring

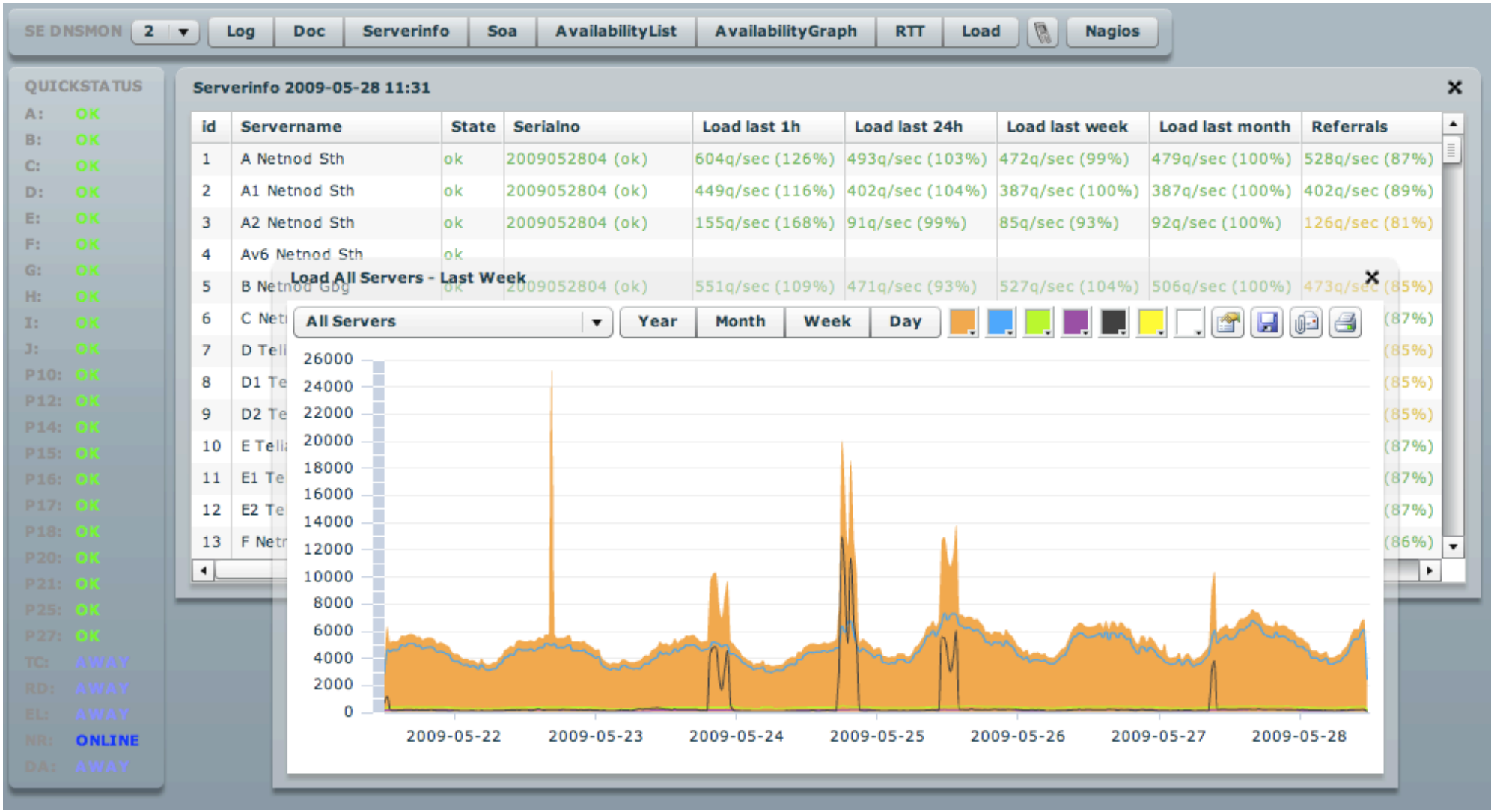
We are monitoring:

- Availability (probe network)
- Query load (Is the load 300% above or 50% below month average)
- Is the zone correct (Is the server running the latest zone file, does it reply correctly, check for usual/unusual domain names etc.)
- DNSSEC (Is dnssec handled correctly, signature expiration, large packets etc) http://opensource.iis.se/trac/dnssec/wiki/DNSSEC-monitor

And various other goodies...

.se

DNSMON GUI


SE DNSMON 2
Log
Doc
Serverinfo
Soa
AvailabilityList
AvailabilityGraph
RTT
Load
Nagios
QUICKSTATUS
A: OK
B: OK
C: OK
D: OK
E: OK
F: OK
G: OK
H: OK
I: OK
J: OK
P10: OK
P12: OK
P14: OK
P15: OK
P16: OK
P17: OK
P18: OK
P20: OK
P21: OK
P25: OK
P27: OK
TC: AWAY
RD: AWAY
EL: AWAY
NR: ONLINE
DA: AWAY
Serverinfo 2009-05-28 11:31
id | Servername | State | Serialno | Load last 1h | Load last 24h | Load last week | Load last month | Referrals
1 | A Netnod Sth | ok | 2009052804 (ok) | 604q/sec (126%) | 493q/sec (103%) | 472q/sec (99%) | 479q/sec (100%) | 528q/sec (87%)
2 | A1 Netnod Sth | ok | 2009052804 (ok) | 449q/sec (116%) | 402q/sec (104%) | 387q/sec (100%) | 387q/sec (100%) | 402q/sec (89%)
3 | A2 Netnod Sth | ok | 2009052804 (ok) | 155q/sec (168%) | 91q/sec (99%) | 85q/sec (93%) | 92q/sec (100%) | 126q/sec (81%)
4 | Av6 Netnod Sth | ok
5 | B Netnod Gbg | ok | 2009052804 (ok) | 551q/sec (109%) | 471q/sec (93%) | 527q/sec (104%) | 506q/sec (100%) | 473q/sec (85%)
6 | C Neti (87%)
7 | D Teli (85%)
8 | D1 Te (85%)
9 | D2 Te (85%)
10 | E Teli (87%)
11 | E1 Te (87%)
12 | E2 Te (87%)
13 | F Netr (86%)
Load All Servers - Last Week
All Servers
Year
Month
Week
Day
26000
24000
22000
20000
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
2009-05-22
2009-05-23
2009-05-24
2009-05-25
2009-05-26
2009-05-27
2009-05-28

DNSSEC Nagios controller module

http://opensource.iis.se/trac/dnssec/wiki/DNSSEC-monitor

checkcommands.cfg

```
define command{

        command_name    check_dnssec

        command_line    $USER1$/nagios_dnssec.pl --zone se --kskcritical=$ARG1$ --kskwarning $ARG2$ --zskcritical=$ARG3$ --zskwarning
$ARG4$ $HOSTADDRESS$

}

define command{

        command_name    check_dnssec_anycast

        command_line    $USER1$/nagios_dnssec.pl --zone se --kskcritical=$ARG1$ --kskwarning $ARG2$ --zskcritical=$ARG3$ --zskwarning
$ARG4$ --dstport=$ARG5$ $HOSTADDRESS$

}
```

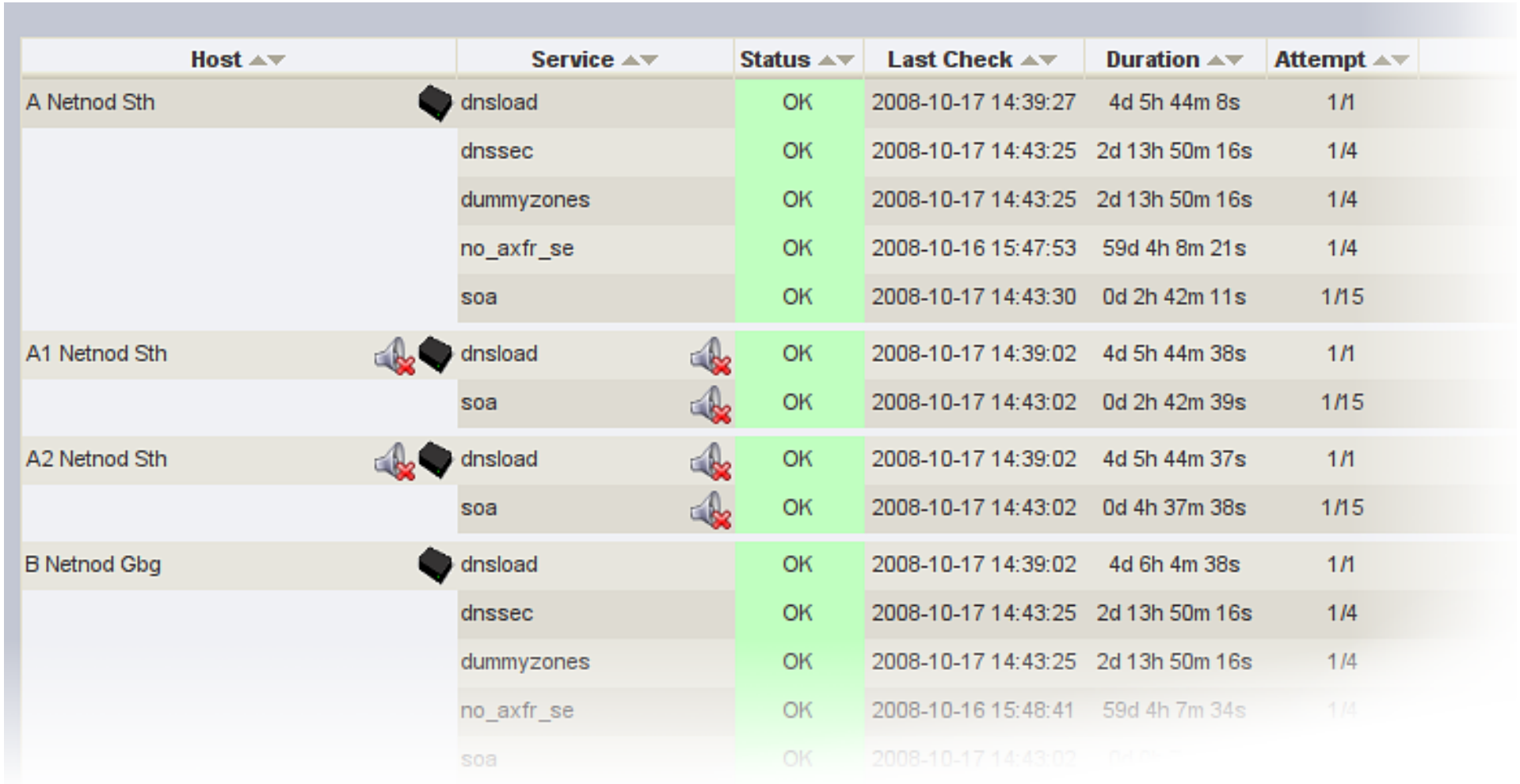
nagios.cfg

```
define service{
                host_name                       host1, host2, host3 ...
        service_description             dnssec
        notifications_enabled           1
        check_command                   check_dnssec!2!4!1!2

}
```

.se

DNSSEC controller in NAGIOS



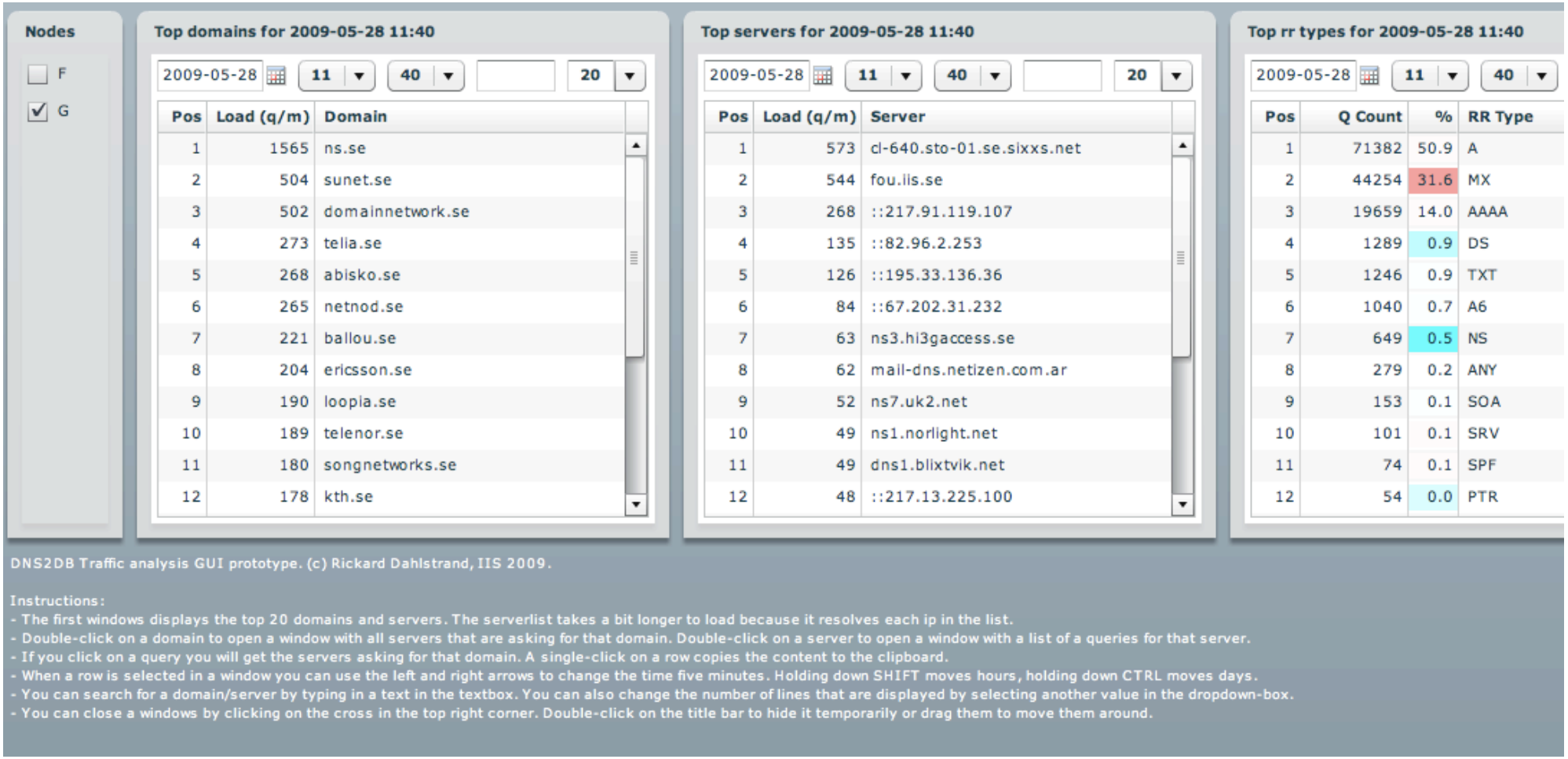
Host	Service	Status	Last Check	Duration	Attempt
A Netnod Sth	dnsload	OK	2008-10-17 14:39:27	4d 5h 44m 8s	1/1
	dnssec	OK	2008-10-17 14:43:25	2d 13h 50m 16s	1/4
	dummyzones	OK	2008-10-17 14:43:25	2d 13h 50m 16s	1/4
	no_axfr_se	OK	2008-10-16 15:47:53	59d 4h 8m 21s	1/4
	soa	OK	2008-10-17 14:43:30	0d 2h 42m 11s	1/15
A1 Netnod Sth	dnsload	OK	2008-10-17 14:39:02	4d 5h 44m 38s	1/1
	soa	OK	2008-10-17 14:43:02	0d 2h 42m 39s	1/15
A2 Netnod Sth	dnsload	OK	2008-10-17 14:39:02	4d 5h 44m 37s	1/1
	soa	OK	2008-10-17 14:43:02	0d 4h 37m 38s	1/15
B Netnod Gbg	dnsload	OK	2008-10-17 14:39:02	4d 6h 4m 38s	1/1
	dnssec	OK	2008-10-17 14:43:25	2d 13h 50m 16s	1/4
	dummyzones	OK	2008-10-17 14:43:25	2d 13h 50m 16s	1/4
	no_axfr_se	OK	2008-10-16 15:48:41	59d 4h 7m 34s	1/4
	soa	OK	2008-10-17 14:43:02	0d 2h 42m 39s	1/15

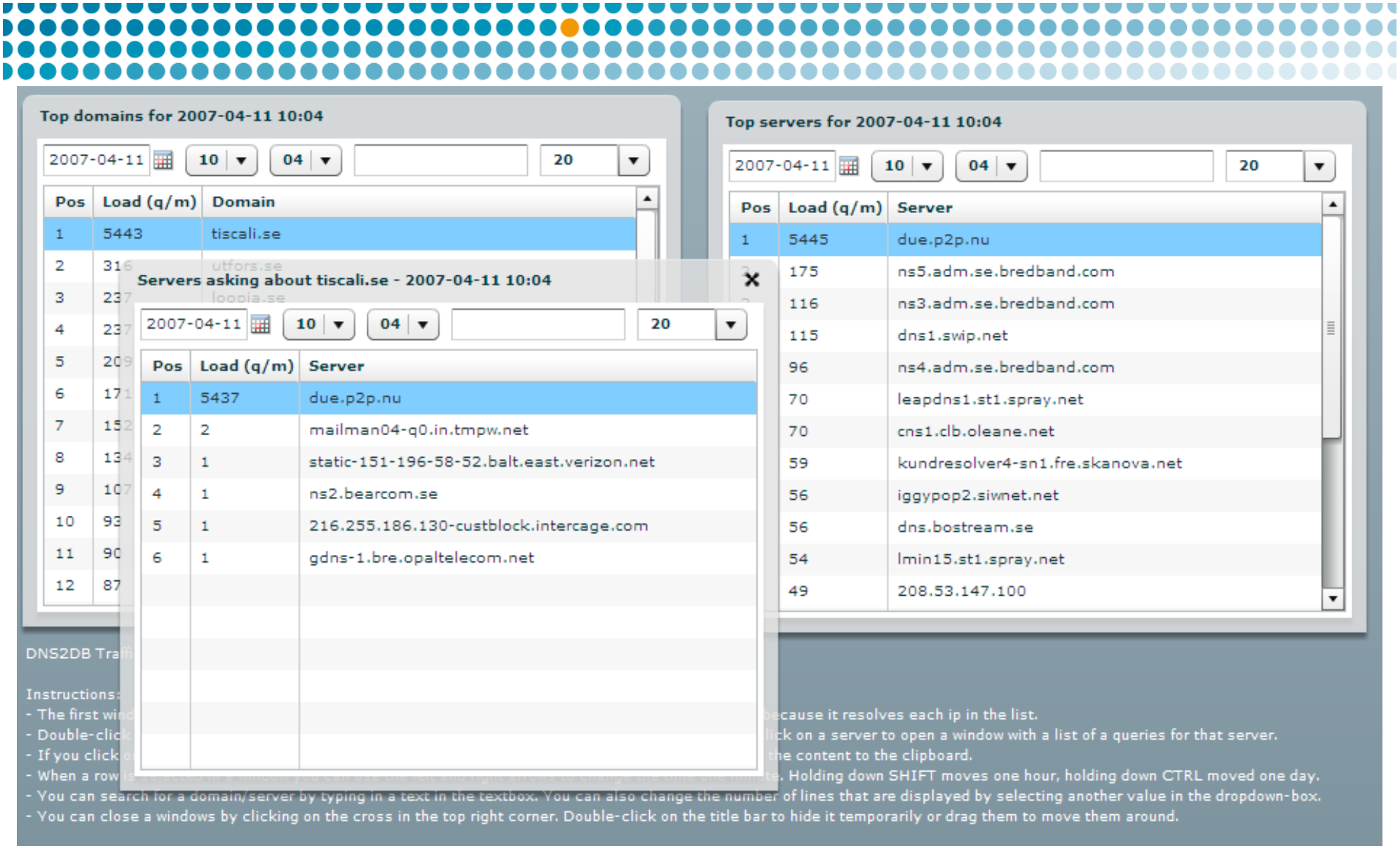
Traffic analyzis – DNS2db

- Collect dns traffic to the .SE slave servers
- Store packets in database for later analyzis
- Possibility to analyze traffic patterns and deviations
- Better understanding of DNS at our level in the DNS hierarchy
- Opensource, available for others root, tld etc.

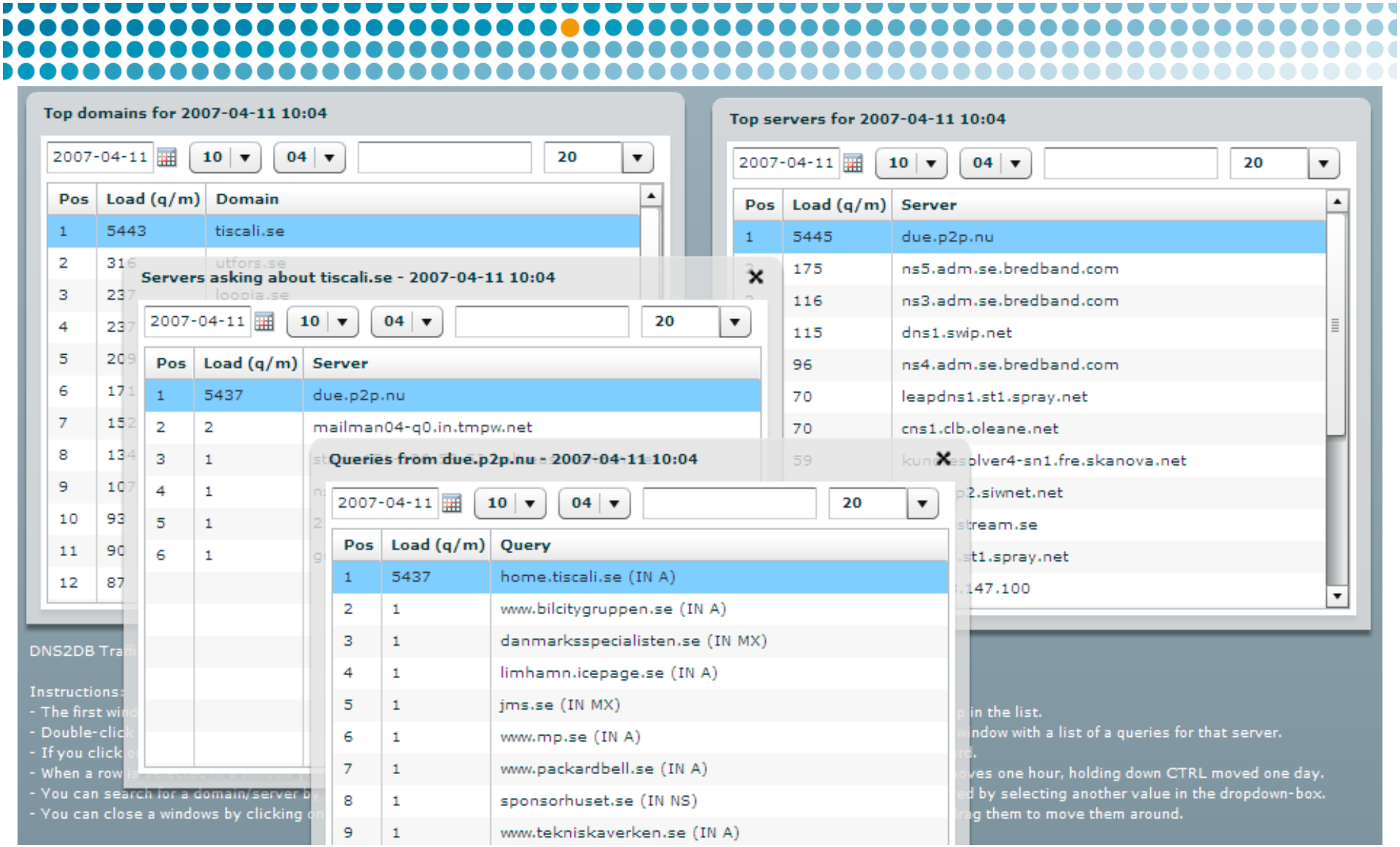
.se

DNS2db GUI


Nodes
F
G
Top domains for 2009-05-28 11:40
2009-05-28
11
40
20
Pos | Load (q/m) | Domain
1 | 1565 | ns.se
2 | 504 | sunet.se
3 | 502 | domainnetwork.se
4 | 273 | telia.se
5 | 268 | abisko.se
6 | 265 | netnod.se
7 | 221 | ballou.se
8 | 204 | ericsson.se
9 | 190 | loopia.se
10 | 189 | telenor.se
11 | 180 | songnetworks.se
12 | 178 | kth.se
Top servers for 2009-05-28 11:40
2009-05-28
11
40
20
Pos | Load (q/m) | Server
1 | 573 | ci-640.sto-01.se.sixxs.net
2 | 544 | fou.iis.se
3 | 268 | ::217.91.119.107
4 | 135 | ::82.96.2.253
5 | 126 | ::195.33.136.36
6 | 84 | ::67.202.31.232
7 | 63 | ns3.hi3gaccess.se
8 | 62 | mail-dns.netizen.com.ar
9 | 52 | ns7.uk2.net
10 | 49 | ns1.norlight.net
11 | 49 | dns1.blixtvik.net
12 | 48 | ::217.13.225.100
Top rr types for 2009-05-28 11:40
2009-05-28
11
40
Pos | Q Count | % | RR Type
1 | 71382 | 50.9 | A
2 | 44254 | 31.6 | MX
3 | 19659 | 14.0 | AAAA
4 | 1289 | 0.9 | DS
5 | 1246 | 0.9 | TXT
6 | 1040 | 0.7 | A6
7 | 649 | 0.5 | NS
8 | 279 | 0.2 | ANY
9 | 153 | 0.1 | SOA
10 | 101 | 0.1 | SRV
11 | 74 | 0.1 | SPF
12 | 54 | 0.0 | PTR
DNS2DB Traffic analysis GUI prototype. (c) Rickard Dahlstrand, IIS 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 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.


Top domains for 2007-04-11 10:04
2007-04-11
10
04
20
Pos
Load (q/m)
Domain
1
5443
tiscali.se
2
316
utfors.se
3
237
loopia.se
4
237
5
209
6
171
7
152
8
134
9
107
10
93
11
90
12
87
Servers asking about tiscali.se - 2007-04-11 10:04
2007-04-11
10
04
20
Pos
Load (q/m)
Server
1
5437
due.p2p.nu
2
2
mailman04-q0.in.tmpw.net
3
1
static-151-196-58-52.balt.east.verizon.net
4
1
ns2.bearcom.se
5
1
216.255.186.130-custblock.intercage.com
6
1
gdns-1.bre.opaltelecom.net
Top servers for 2007-04-11 10:04
2007-04-11
10
04
20
Pos
Load (q/m)
Server
1
5445
due.p2p.nu
175
ns5.adm.se.bredband.com
116
ns3.adm.se.bredband.com
115
dns1.swip.net
96
ns4.adm.se.bredband.com
70
leapdns1.st1.spray.net
70
cns1.clb.oleane.net
59
kundresolver4-sn1.fre.skanova.net
56
iggypop2.siwnet.net
56
dns.bostream.se
54
lmin15.st1.spray.net
49
208.53.147.100
DNS2DB Traffi
Instructions:
- The first wind
because it resolves each ip in the list.
- Double-click
lick on a server to open a window with a list of a queries for that server.
- If you click o
the content to the clipboard.
- When a row is
te. Holding down SHIFT moves one hour, holding down CTRL moved one day.
- 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.

.se


Top domains for 2007-04-11 10:04
2007-04-11
10
04
20
Pos
Load (q/m)
Domain
1
5443
tiscali.se
Top servers for 2007-04-11 10:04
Pos
Load (q/m)
Server
1
5445
due.p2p.nu
175
ns5.adm.se.bredband.com
116
ns3.adm.se.bredband.com
115
dns1.swip.net
96
ns4.adm.se.bredband.com
70
leapdns1.st1.spray.net
70
cns1.clb.oleane.net
Servers asking about tiscali.se - 2007-04-11 10:04
Pos
Load (q/m)
Server
1
5437
due.p2p.nu
2
2
mailman04-q0.in.tmpw.net
3
1
4
1
5
1
6
1
Queries from due.p2p.nu - 2007-04-11 10:04
Pos
Load (q/m)
Query
1
5437
home.tiscali.se (IN A)
2
1
www.bilcitygruppen.se (IN A)
3
1
danmarksspecialisten.se (IN MX)
4
1
limhamn.icepage.se (IN A)
5
1
jms.se (IN MX)
6
1
www.mp.se (IN A)
7
1
www.packardbell.se (IN A)
8
1
sponsorhuset.se (IN NS)
9
1
www.tekniskaverken.se (IN A)
Instructions:
- You can close a windows by clicking
- When a row
- If you click
- Double-click
- The first wind
- You can search for a domain/server b
in the list.
ndow with a list of a queries for that server.
ves one hour, holding down CTRL moved one day.
d by selecting another value in the dropdown-box.
ag them to move them around.

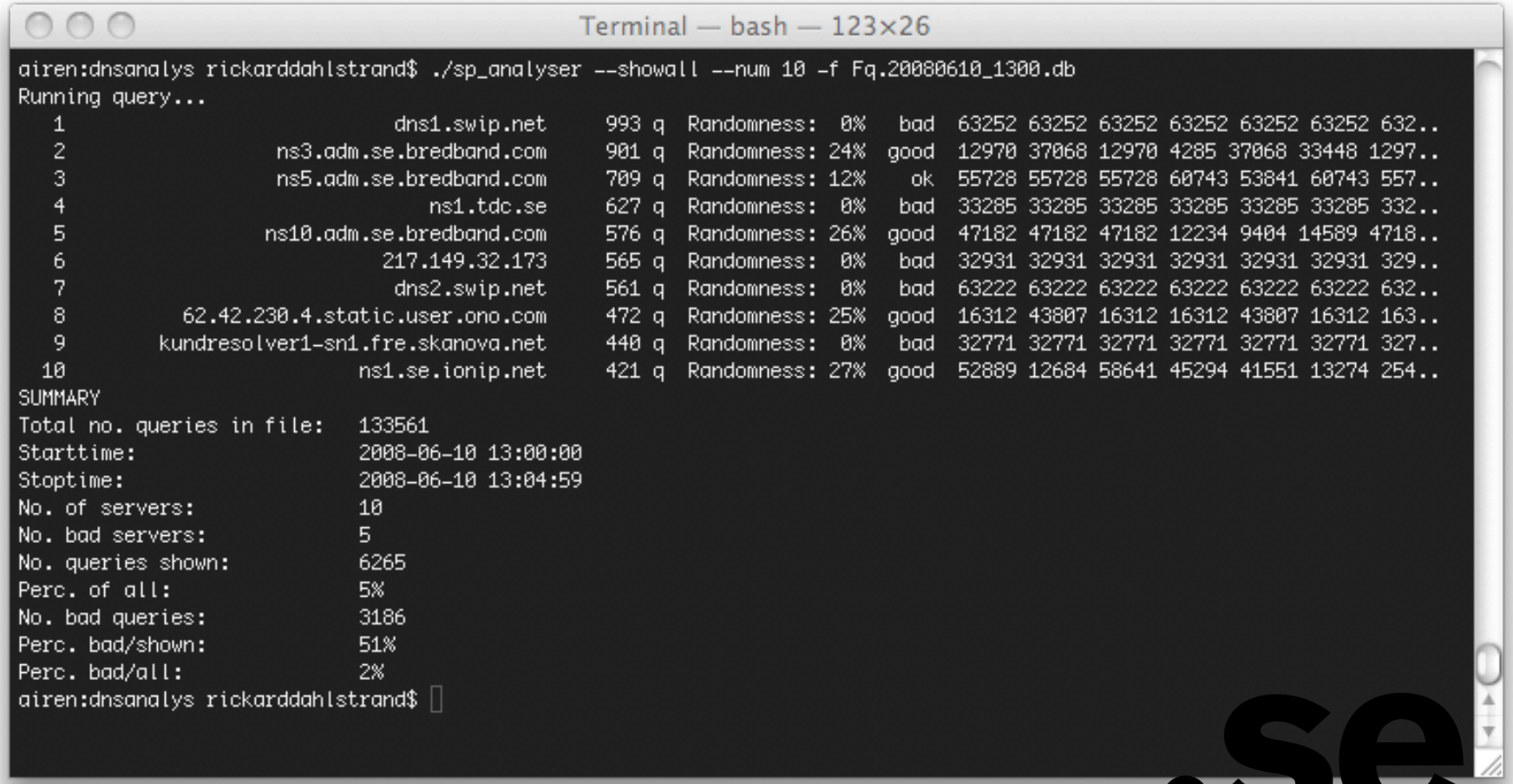
.se

Other possibilities

- Topplists domains/resolvers/qtype
- “Broken” IP-packes (incomplete or non DNS queries)
- Deviations from patterns
- Queries from specific resolver/ specific domain
- Distribution query types/TCP/UDP
- Ipv4/IPv6
- Plotting of origin with GEOIP
- DNSSEC enabled resolvers
- Has the X bit set/unset?

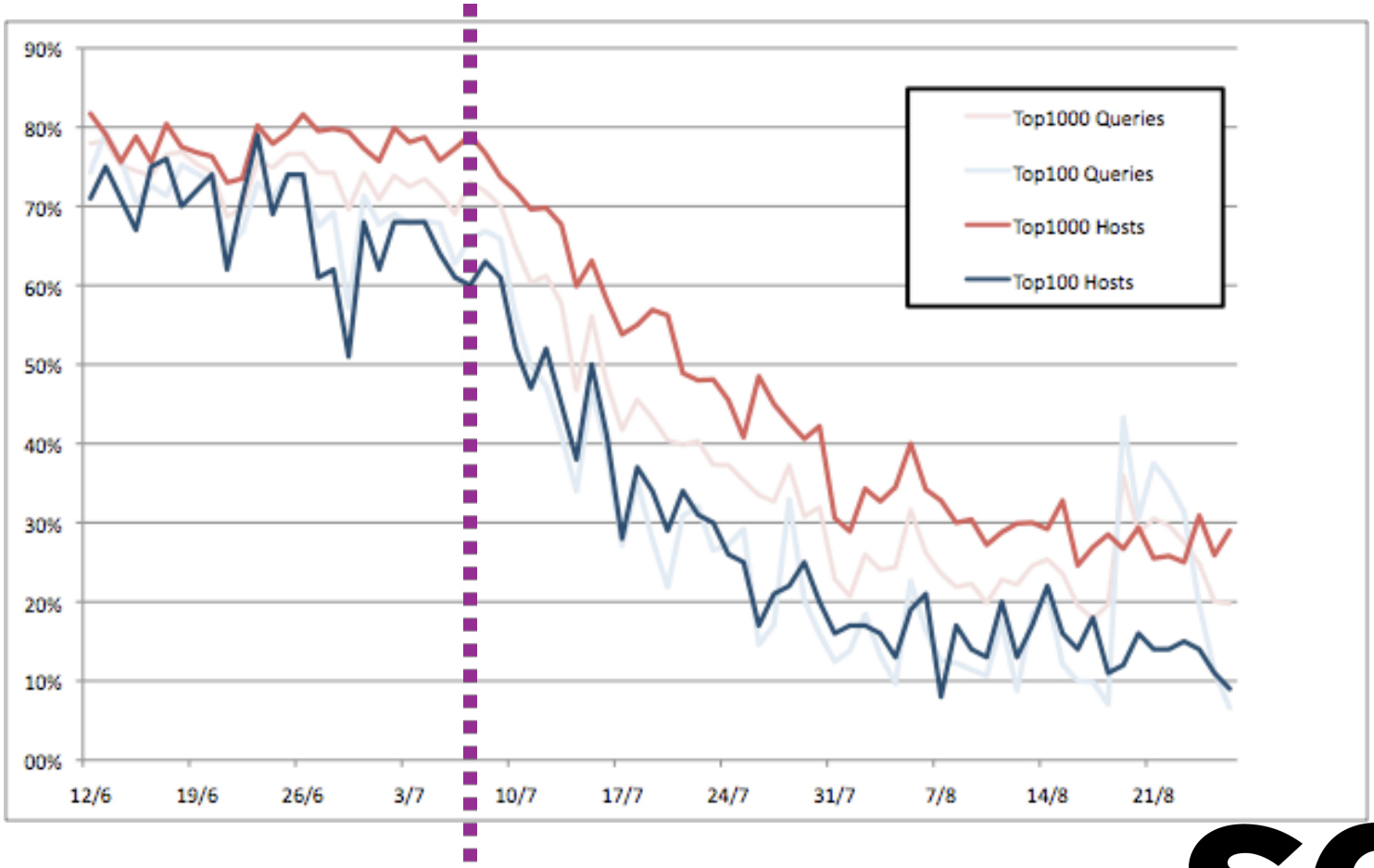
.se

Kaminsky Statistics



.se

Kaminsky Statistics



.se

Questions??

www.iis.se
opensource.iis.se/dns2db
dnscheck.iis.se

.se