Monitoring DNS and DNSSEC

2008-10-23

Niclas Rosell

Three important tools

.SE DNSMON based on Nagios

DNSCheck

DNS2db

ombud

.se

.se

Databas

1. Registrant orders changes.

2. .SE:s registrar forwards the request to the registry.

3. .SE updates the database with changes

4. New zonefile generated 12 times/day

5. New zonefile is sent to master server

Internet

6. New zonefile is sent to distribution pionts

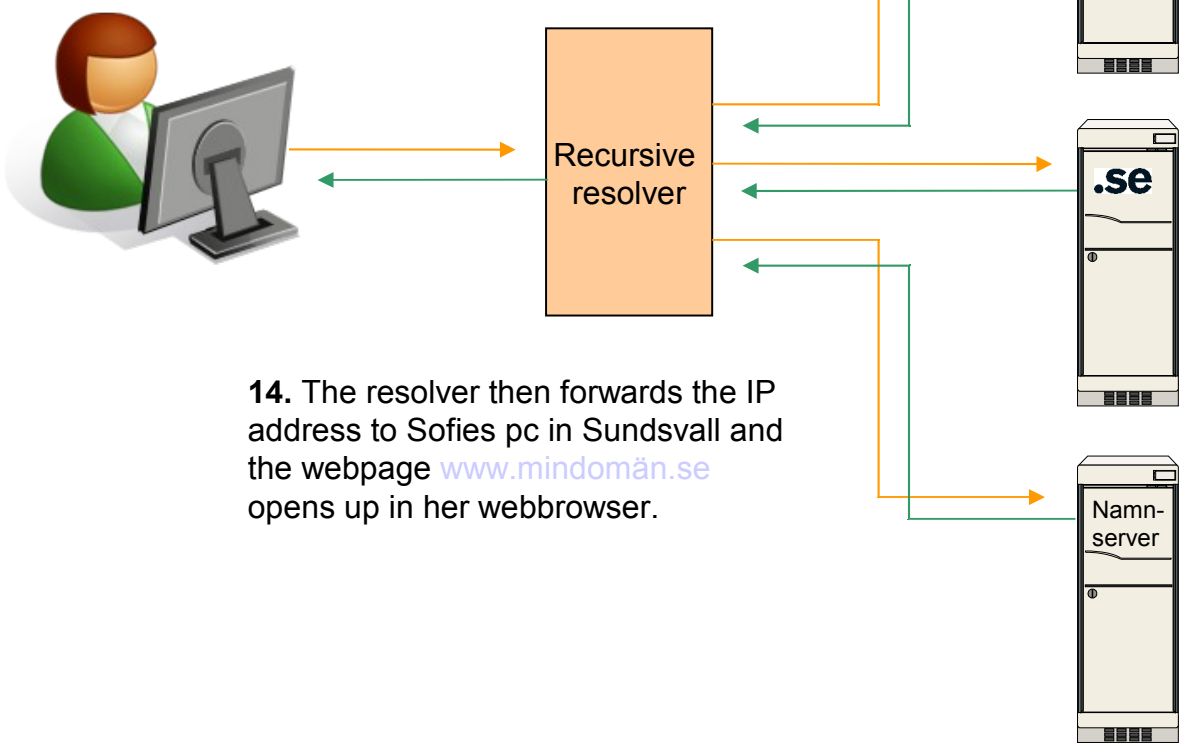
7. The zonefile is distributed to slaveservers.

8. .The .SE slaveserver are ready to answer queries for the .se zone from anywhere ont the internet

.se

9. Sofie in Sundsvall types www.mindomän.se in her webbrowser.

10. The query for the IP adress for www.mindomän.se is sent to a recursive resolver.



11. The resolver queries one of the root servers which points the way to the .SE:s DNS-servers since the domain ends with ’.se’.

12. The resolver then queries one of .SE:s slavservrar on the Internet which point to the nameserver responible for mindomän.se.

13. The resolver then queries the nameserver for mindomän.se, which replies with the IP adress for www.mindomän.se.

14. The resolver then forwards the IP address to Sofies pc in Sundsvall and the webpage www.mindomän.se opens up in her webbrowser.

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.
- Ca 4000 queries/second. (345 million/day)

.se

Monitoring

- We are monitoring:
  - Availability (probe network)
  - Load (Is the load above or below month average, load for certain types of queries.)
  - 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, large packets etc) http://opensource.iis.se/trac/dnssec/wiki/DNSSEC-monitor
  - And various other goodies...
- Alarms via sms/mail to .SE operations & operators/partners.

.se

DNSSEC 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 $ZONE$ --kskcritical=$ARG1$
--kskwarning $ARG2$ --zskcritical=$ARG3$ --zskwarning $ARG4$ $HOSTADDRESS$
}
```

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 4h 37m 38s	1/15

DNSCheck

Project Manager: Einar Lönn

Department for Domain Product and DNS Operation

Einar.Lonn@iis.se

DNSCheck history

- The previous version of DNSCheck (http://www.dnscheck.se) was developed by Patrik Fältström, Frobbit AB, on behalf of .SE.
- The new version of DNSCheck (http://dnscheck.iis.se) has been developed by Jakob Schlyter, Kirei. The primary reasons why we decided to rebuild the code was that we needed better control (it's now modular code and open source) and also a more user-friendly interface (The new GUI has been written in PHP instead of pure html).

.se

What does DNSCheck do?

- DNSCheck is a program that was designed to help people check, measure and hopefully also understand the workings of the Domain Name System, DNS. When a domain (aka zone) is submitted to DNSCheck it will investigate the domain's general health by traversing the DNS from root (.) to the TLD (Top Level Domain, like .SE) to eventually the nameserver(s) that holds the information about the specified domain (like iis.se). Some other sanity checks, for example measuring host connectivity, validity of IP-addresses and control of DNSSEC signatures will also be performed.

What makes DNSCheck special?

- Checks previously used name servers in redelegations done after February 2007 (only .SE-zones though)
- Checks the full .SE-zone periodically
- Clarifies any found warnings/errors
- Saves history for tests done / domain
- Advanced tab for techies
- Written as modular code which helps reuse of whatever functions that are needed elsewhere
- Open source

Built for tomorrow

- Fully capable of running all checks that are performed over IPv4 over IPv6. (Note however that for http://dnscheck.iis.se these are not run today, this is because the location of the DNSCheck-server does not have IPv6 connectivety yet).

- Complete validation of the chain of trust, including some other checks like the presence of secure algorithms, of DNSSEC.

.se

DNSCheck – Phase 1

- The first phase of DNSCheck's development with the GUI built by Pingdom was released in version v0.7 the 9:th of September.
- This version, in turn, has been greatly improved and the current running version, v0.81, is running on http://dnscheck.iis.se since October 8:th.

- ***Demo v0.81***

.se

DNSCheck – Phase 2

- Even though the current version of DNSCheck explains the errors found as well as possible there's always room for improvements. With the help of E-Centret (www.ecentret.se) we want to, in Phase 2, make DNSCheck so user-friendly that even people without any real knowledge of what DNS is should be able to use and learn from it. Call it an interactive "DNS school".

.se

Want to test from home?

Adress to current running DNSCheck (v0.81) – http://dnscheck.iis.se

Adress to the source code of the new DNSCheck - http://opensource.iis.se/trac/dnscheck

Adress to the developers of the GUI – http://www.pingdom.se

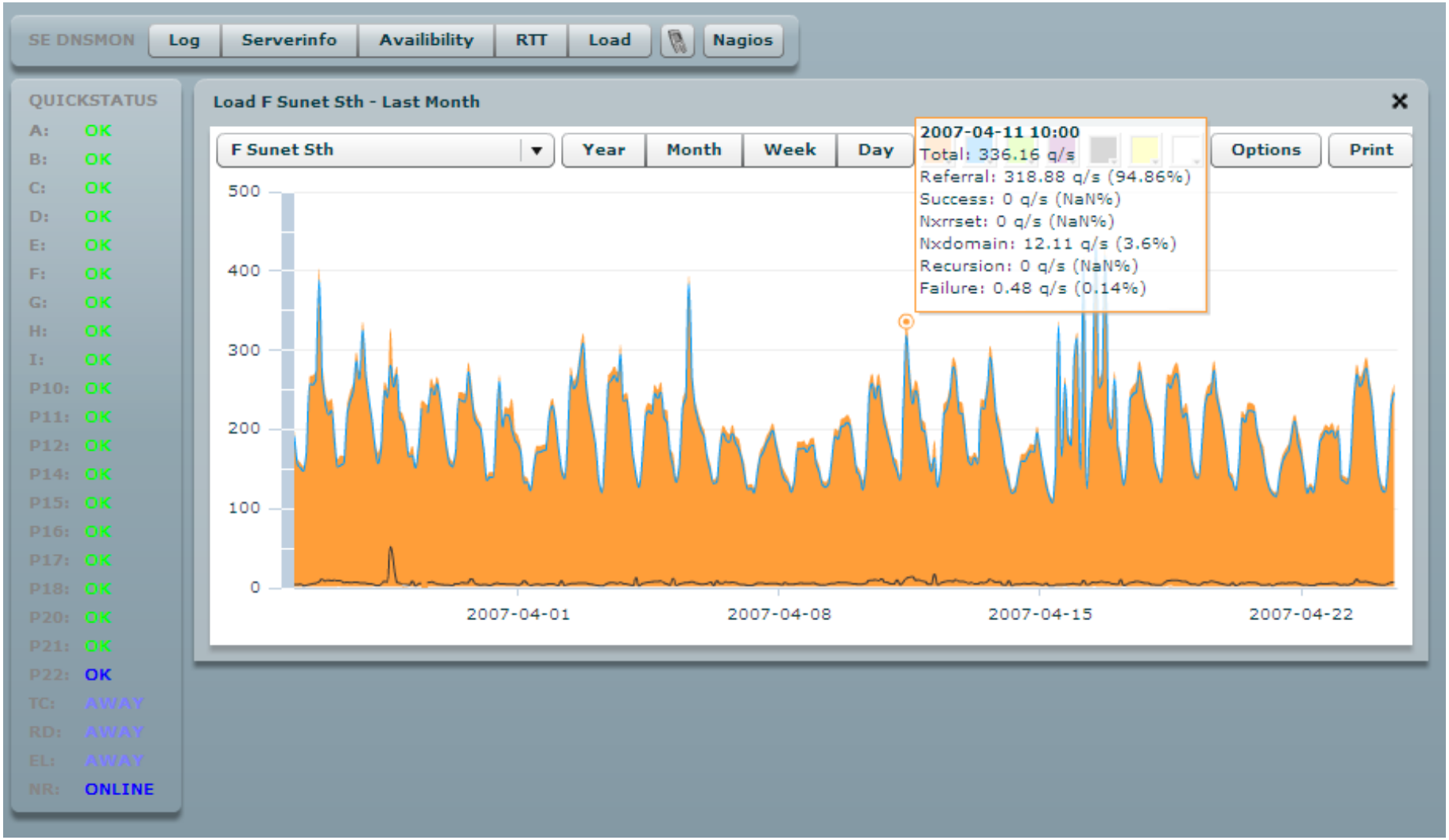
Adress to the previously used DNSCheck – http://www.dnscheck.se

.se

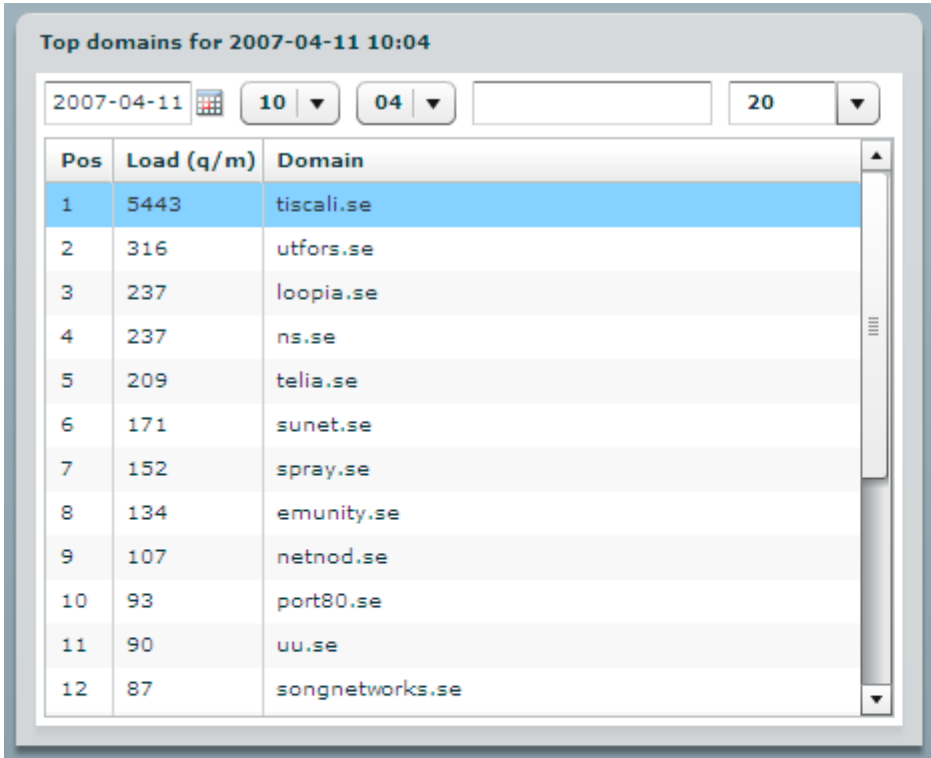
Traffic analyzis – DNS2db

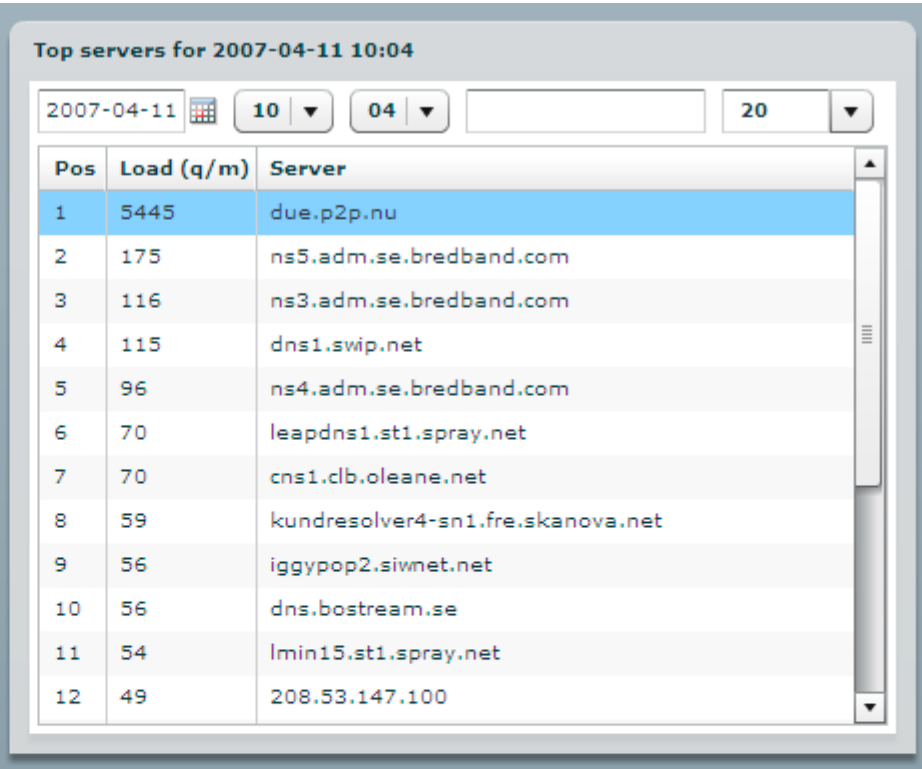
- Collect dns traffic to the .SE slave servers
- Store packets in database for later analyzis
- Possibility to analyze traffic patterns and deviations
- Better understanding of DNS at our level in the DNS hierarchy
- Opensource, available for others root, tld etc.

.se


SE DNSMON
Log
Serverinfo
Availibility
RTT
Load
Nagios
QUICKSTATUS
A: OK
B: OK
C: OK
D: OK
E: OK
F: OK
G: OK
H: OK
I: OK
P10: OK
P11: OK
P12: OK
P14: OK
P15: OK
P16: OK
P17: OK
P18: OK
P20: OK
P21: OK
P22: OK
TC: AWAY
RD: AWAY
EL: AWAY
NR: ONLINE
Load F Sunet Sth - Last Month
F Sunet Sth
Year
Month
Week
Day
Options
Print
2007-04-11 10:00
Total: 336.16 q/s
Referral: 318.88 q/s (94.86%)
Success: 0 q/s (NaN%)
Nxrrset: 0 q/s (NaN%)
Nxdomain: 12.11 q/s (3.6%)
Recursion: 0 q/s (NaN%)
Failure: 0.48 q/s (0.14%)
500
400
300
200
100
0
2007-04-01
2007-04-08
2007-04-15
2007-04-22

.se



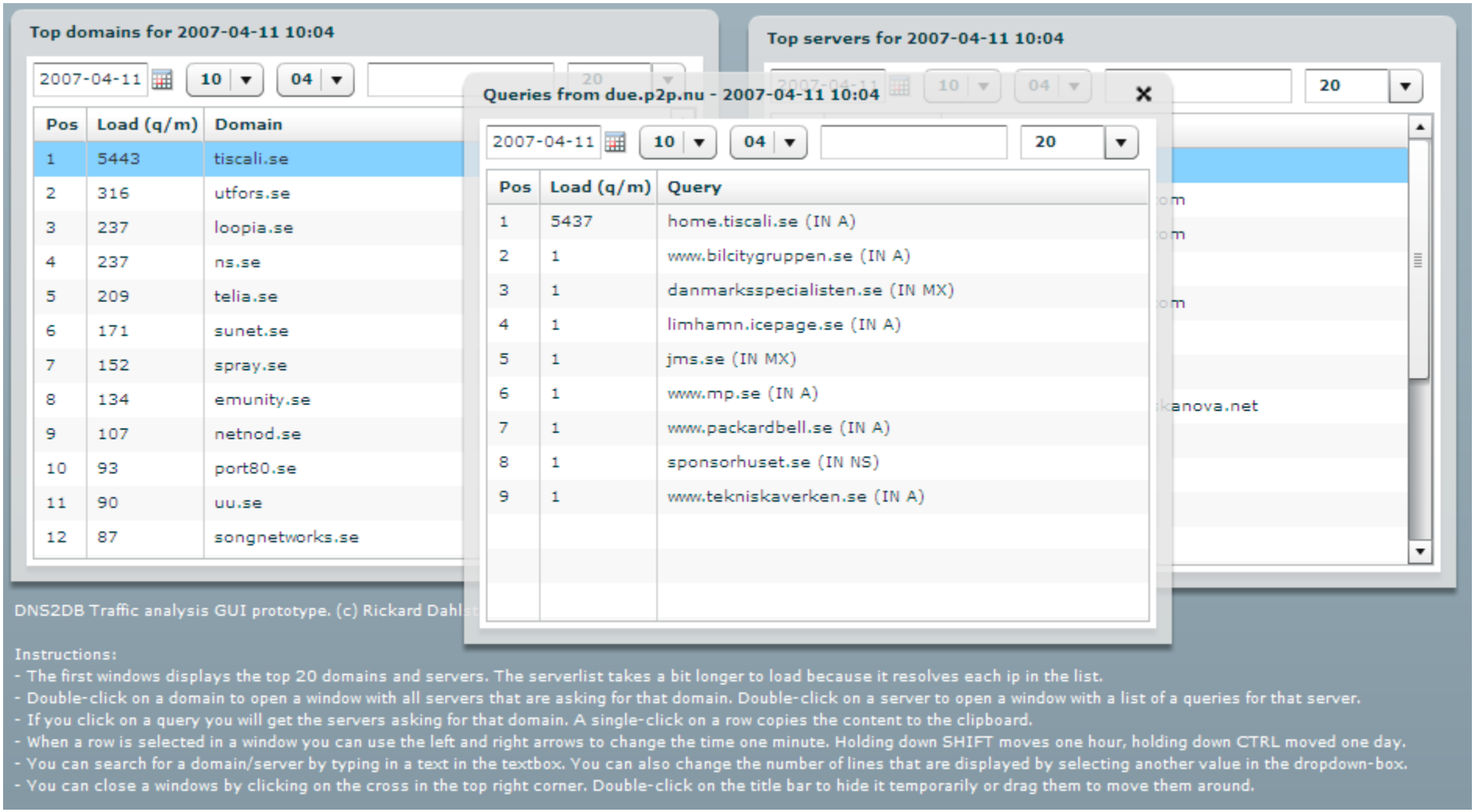


DNS2DB Traffic analysis GUI prototype. (c) Rickard Dahlstrand, IIS 2007.

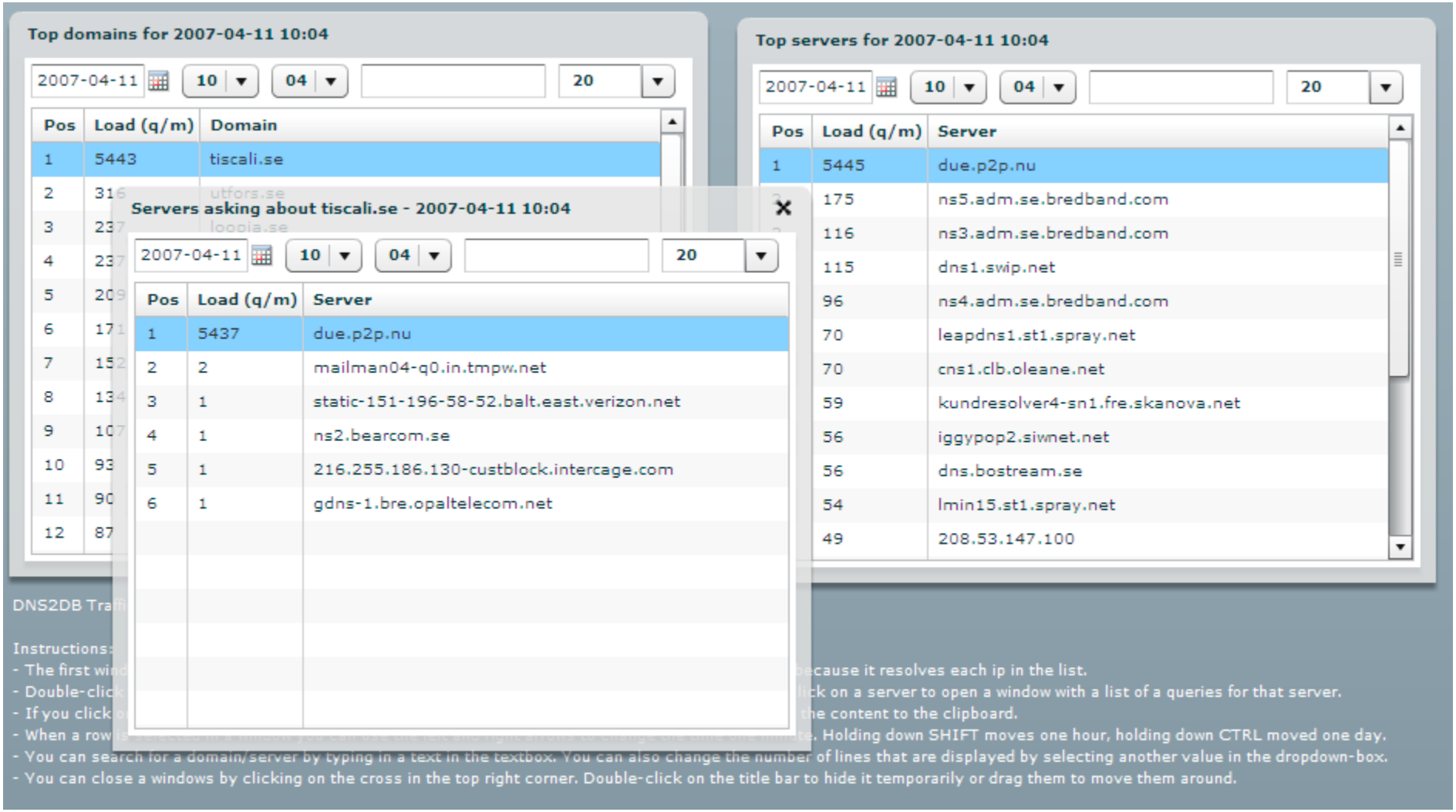
Instructions:

- 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 one minute. 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.

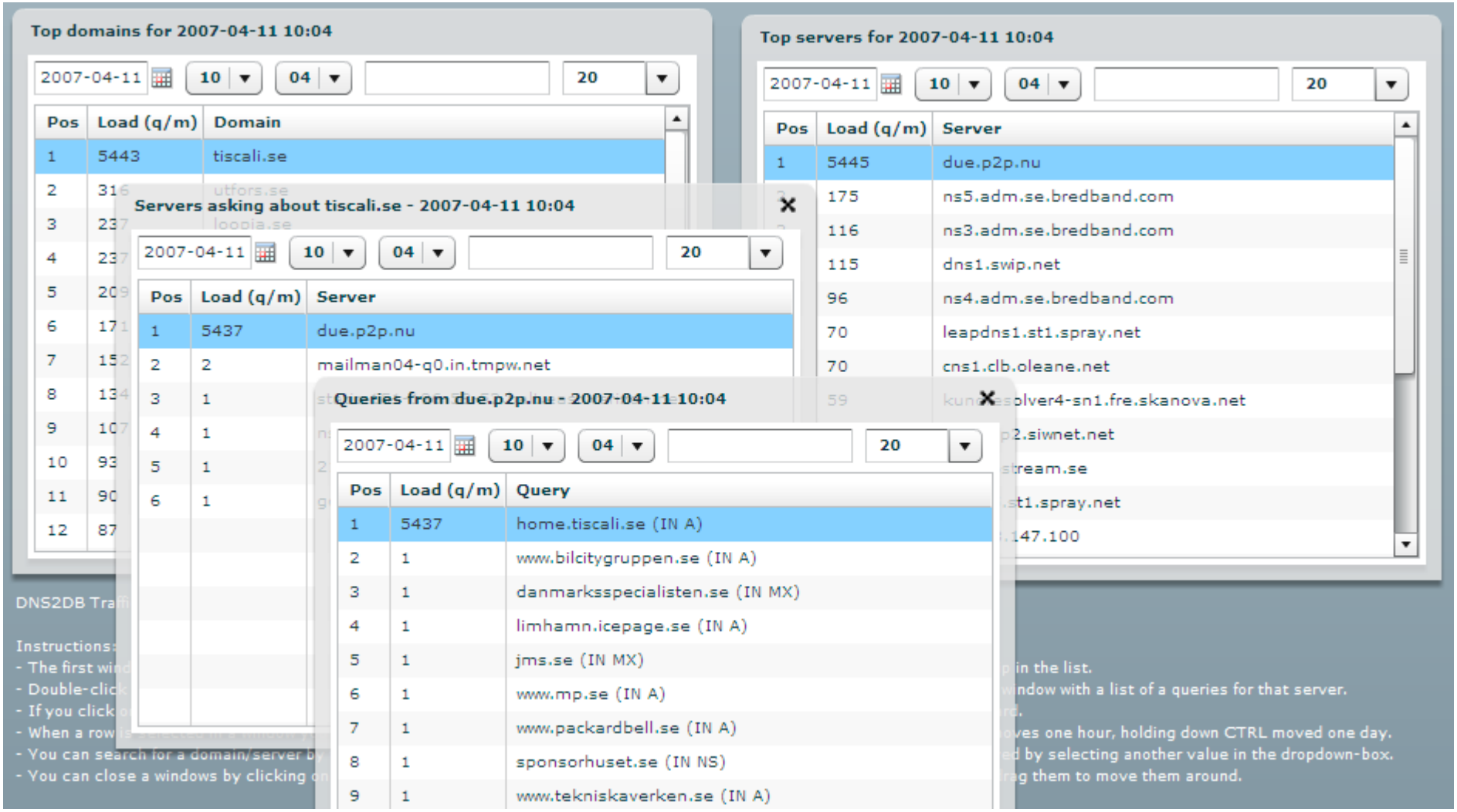
.se


Top domains for 2007-04-11 10:04
2007-04-11
10
04
Pos
Load (q/m)
Domain
1 5443 tiscali.se
2 316 utfors.se
3 237 loopia.se
4 237 ns.se
5 209 telia.se
6 171 sunet.se
7 152 spray.se
8 134 emunity.se
9 107 netnod.se
10 93 port80.se
11 90 uu.se
12 87 songnetworks.se
Top servers for 2007-04-11 10:04
20
Queries from due.p2p.nu - 2007-04-11 10:04
2007-04-11
10
04
20
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)
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 one minute. 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
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 wi
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
he 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
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
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
kunda.resolver4-sn1.fre.skanova.net
2.siwnet.net
tream.se
t1.spray.net
147.100
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
4
1
5
1
6
1
Queries from due.p2p.nu - 2007-04-11 10:04
2007-04-11
10
04
20
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)
DNS2DB Traffi
Instructions:
- The first win
- Double-click
- If you click o
- When a row is
- You can search for a domain/server b
- You can close a windows by clicking on
in the list.
ndow with a list of a queries for that server.
rd.
ves one hour, holding down CTRL moved one day.
d by selecting another value in the dropdown-box.
rag 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
- DNSSEC
- Has the X bit set/unset?

.se

Example of generic statistics

DNS2DB quick report generator

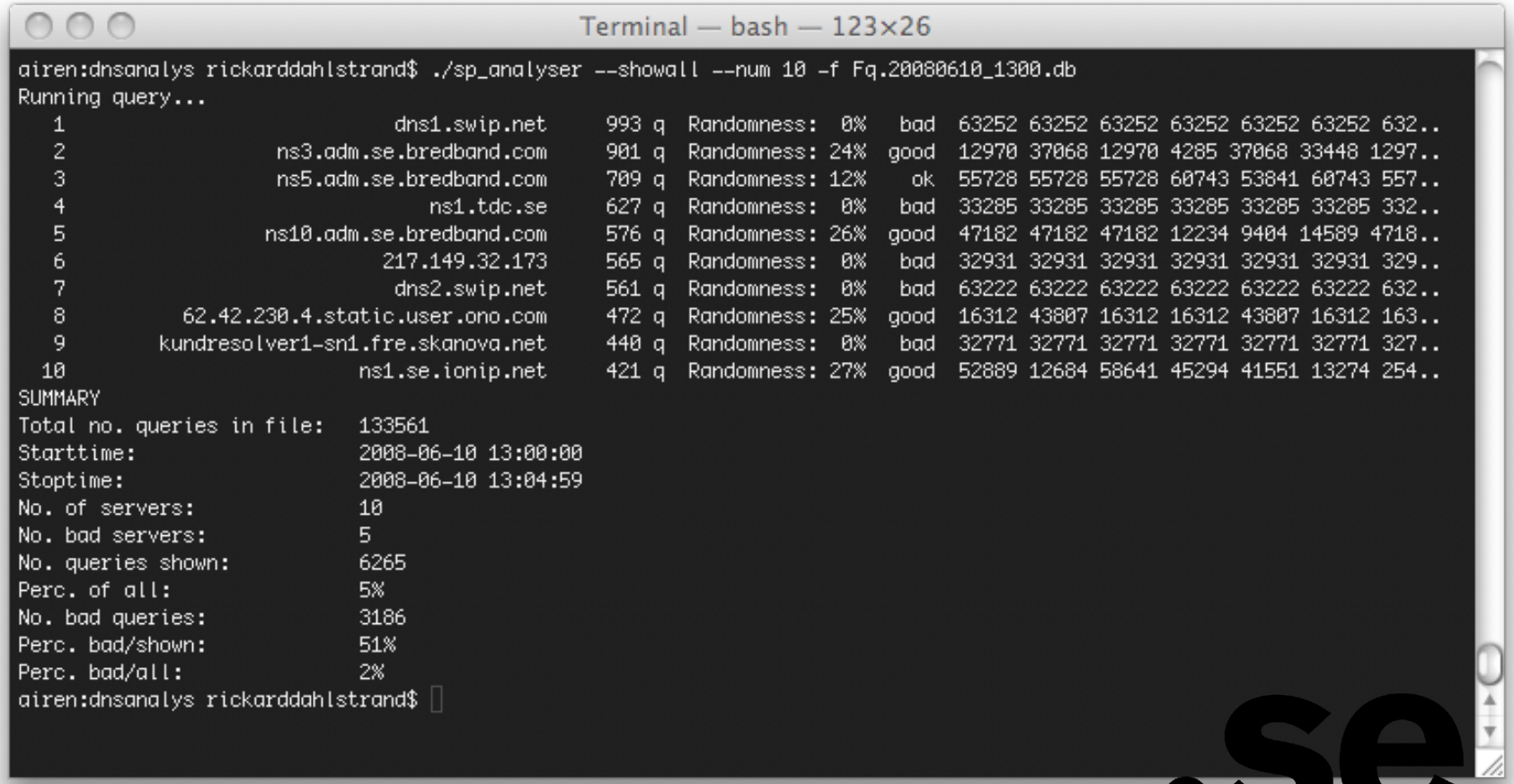
Generating report for database G.NS.SE-200807100010

DateTime	200807100010
Total number of queries:	52972
Packets over UDP:	52697
Percent packets UDP:	99.48
Packets over TCP:	275
Percent packets TCP:	.51
Packets over IPv4:	51899
Number of clients over IPv4:	18061
Packets over IPv6:	1073
Number of clients over IPv6:	196
Percent Clients over IPv6:	1.07

A	29151
AAAA	6777
A6	1051
NS	177
SOA	114
MX	13659
DS	109
RRSIG	1
NSEC	0
DNSKEY	89

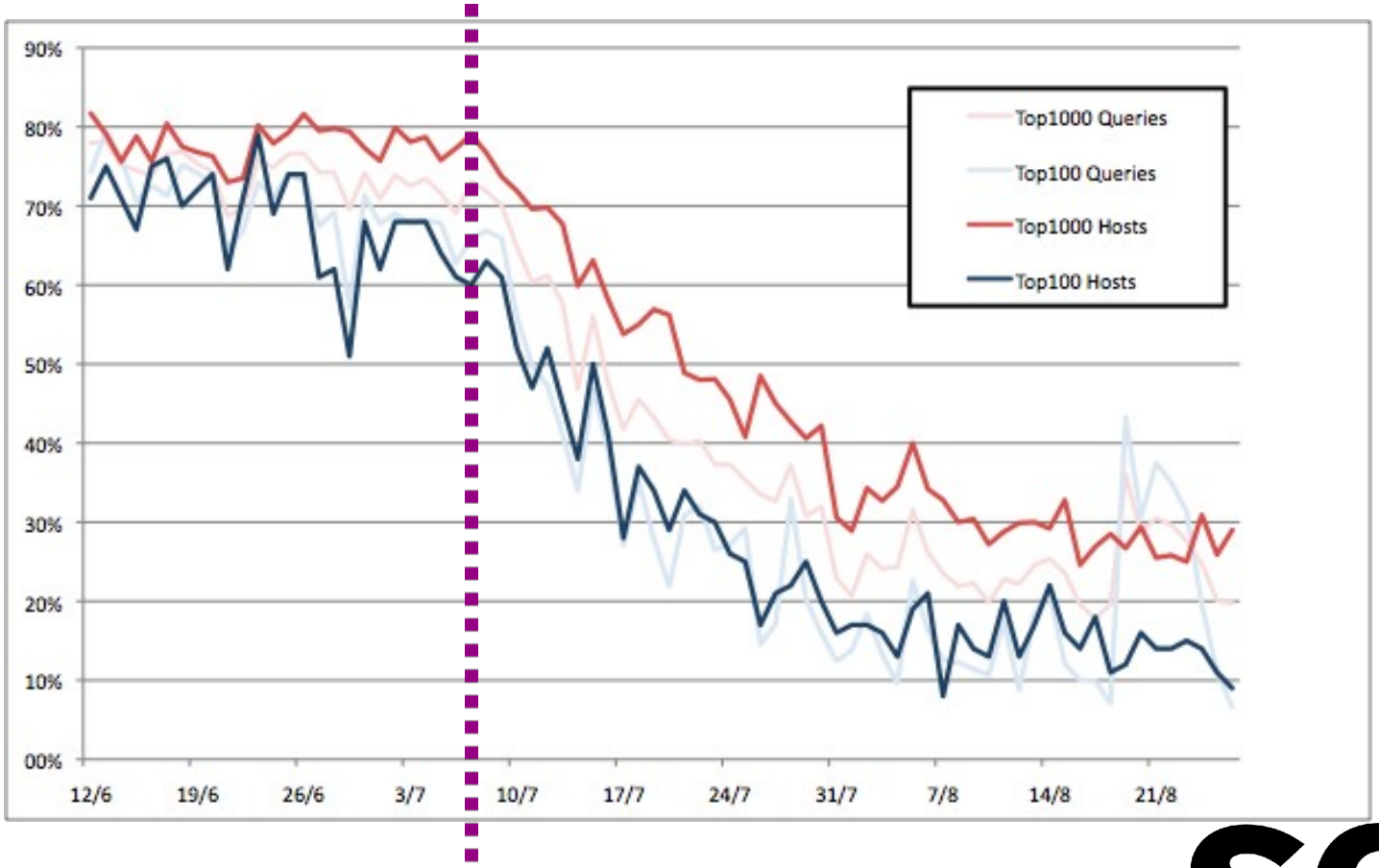
Unhandled packets: 275

Kaminsky Statistics



.se

Kaminsky Statistics



.se

Questions??

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