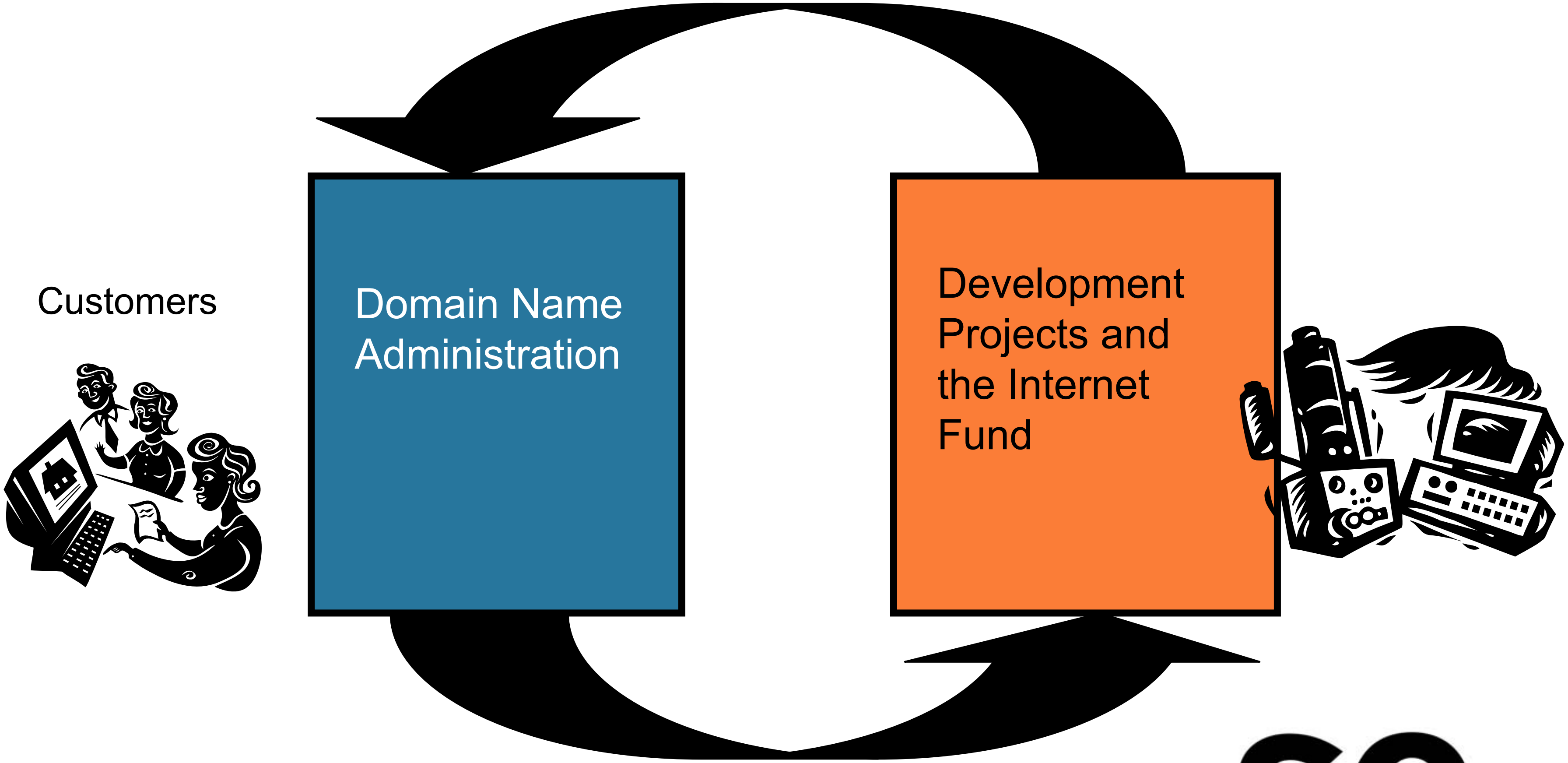
Dns2db

DNS statistics the **.SE** way

Who we are

- .SE (The Internet Infrastructure Foundation) is responsible for the top-level domain for Sweden, .se.
- Non-profit organisation founded in 1997
- Works in the long-term interests of the Internet on assignment from the Swedish Internet community
- 620 000 registered domain names and over 550 new registrations per day
- 34 employees
- Turnover 2006: 64 m SEK
- Regulated by the Law of National Top-level Domains for Sweden on the Internet, which is monitored by the National Post and Telecom Agency (PTS)

.SE' two legs



Customer added value

Customers

Domain Name Administration

Development Projects and the Internet Fund

Profit

Why do traffic analyzis

- Understand traffic flow to secondary servers
- Identify reason for specific peaks

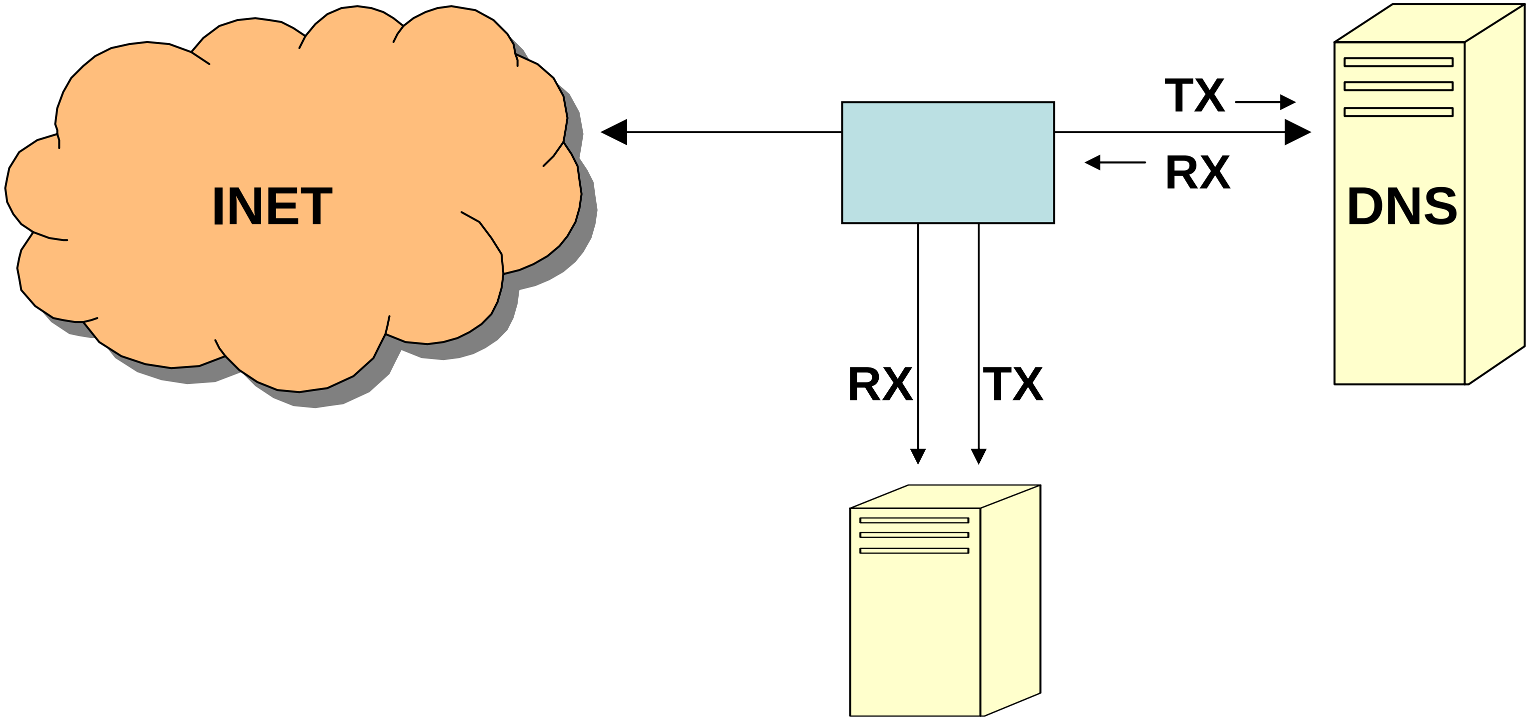
Written from scratch

- Prototype created summer 2005
- Financed by .SE
- Is a new open-source project hosted at iis.se
- Uses ldns from NLnetLabs

  http://www.nlnetlabs.nl/ldns/

.se

Hardware setup



Tcpdump -> Pcap

DNS2DB -> SQL

Installation & setup

- Runs on Linux, FreeBSD (and OSX?)
- Apache webserver
- PHP with pdo_sqlite
- Flash on client

Uses SQL Backend

- Reads Pcap files and store to SQL databases.
- Allows for faster queries due to indexing
- Sqlite3 is our preferred database
- MySQL, PgSQL is planned

Performance

1 hour traffic with 250q/s average

85MB pcap file

pcap->sqlite3=1min 36sec (3.4 GHz)

Indexing time ≈ 1MB/sec (not in ramdisk)

Uses interactive frontend

- GUI written in Adobe Flex
- Server side PHP
- Allows for ”digging in” on traffic data.
- Highly customizable queries/analyzis
- Uses little resources on server

Directory structure

One directory per day

```
$ du -sh *
304M    20070504
2.0G    20070505
759M    20070506
…
…
```

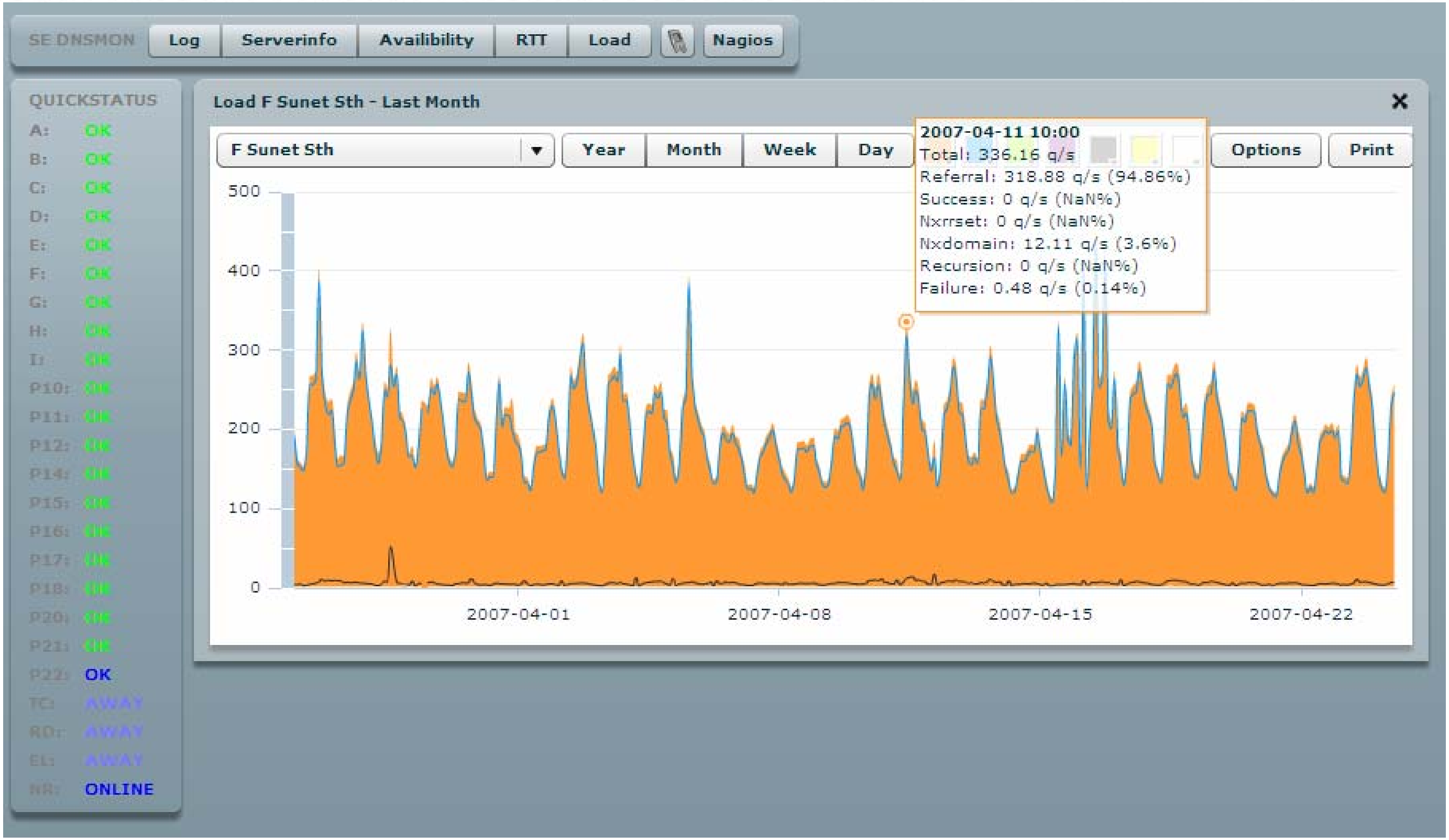
Directory structure

One file per 5 minutes

```
$ du -sh *
6.2M    Fq.20070506_0000.db
1.3M    Fq.20070506_0000.pcap.gz
5.8M    Fq.20070506_0005.db
1.3M    Fq.20070506_0005.pcap.gz
5.6M    Fq.20070506_0010.db
1.3M    Fq.20070506_0010.pcap.gz
5.3M    Fq.20070506_0015.db
1.2M    Fq.20070506_0015.pcap.gz
...
```

Table structure

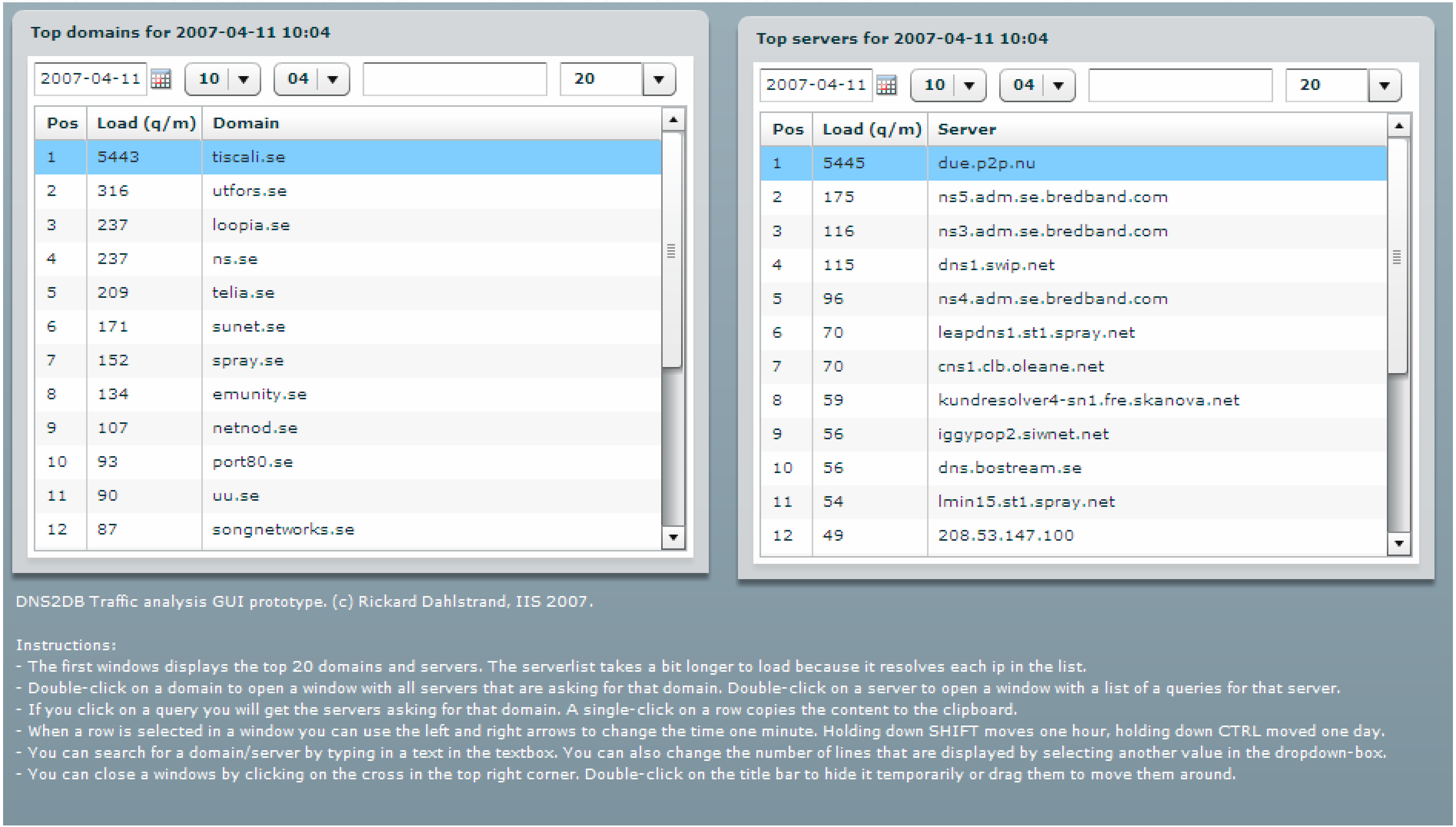
- sqlite> select * from Q limit 1;
- id = 1
- ts = 1178441700
- msg_id = 59483
- Client_num = 2092039856
- Client = 80.1.78.131
- Src_port = 13568
- Qtype = 1
- Qclass = 1
- MsgLen = 27
- Qname = ns1.t3.se.
- Opcode = 0
- Rd = 0
- Opt_RR = 0
- Do = 0
- Version = 0
- E1 = t3.se.
- E2 = 80.1.78.0



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

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%)



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	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

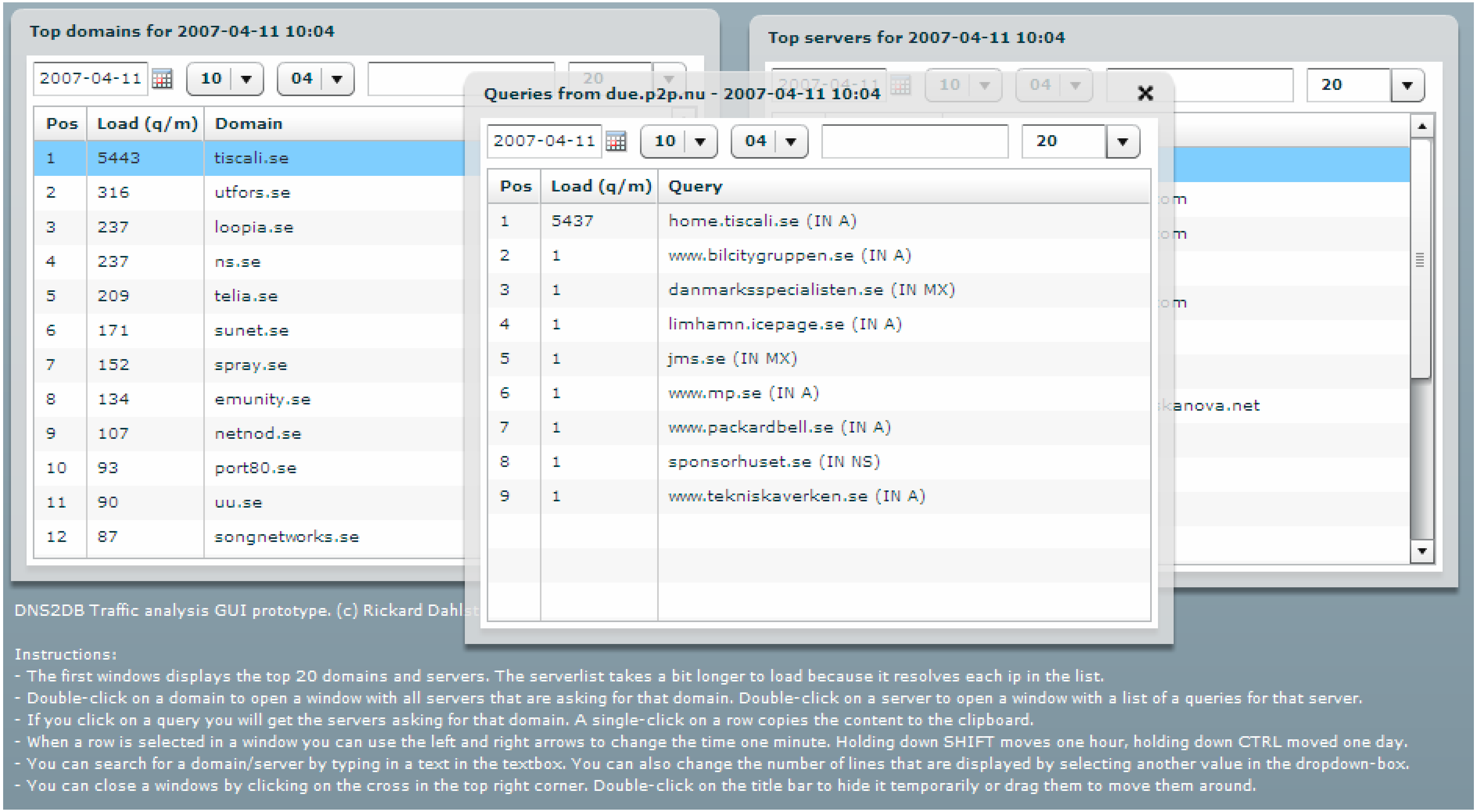
2007-04-11 | 10 | 04 | 20

Pos	Load (q/m)	Server
1	5445	due.p2p.nu
2	175	ns5.adm.se.bredband.com
3	116	ns3.adm.se.bredband.com
4	115	dns1.swip.net
5	96	ns4.adm.se.bredband.com
6	70	leapdns1.st1.spray.net
7	70	cns1.clb.oleane.net
8	59	kundresolver4-sn1.fre.skanova.net
9	56	iggypop2.siwnet.net
10	56	dns.bostream.se
11	54	lmin15.st1.spray.net
12	49	208.53.147.100

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.



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	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

2007-04-11 | 10 | 04 | 20

om
om
om
kanova.net

Queries from due.p2p.nu - 2007-04-11 10:04

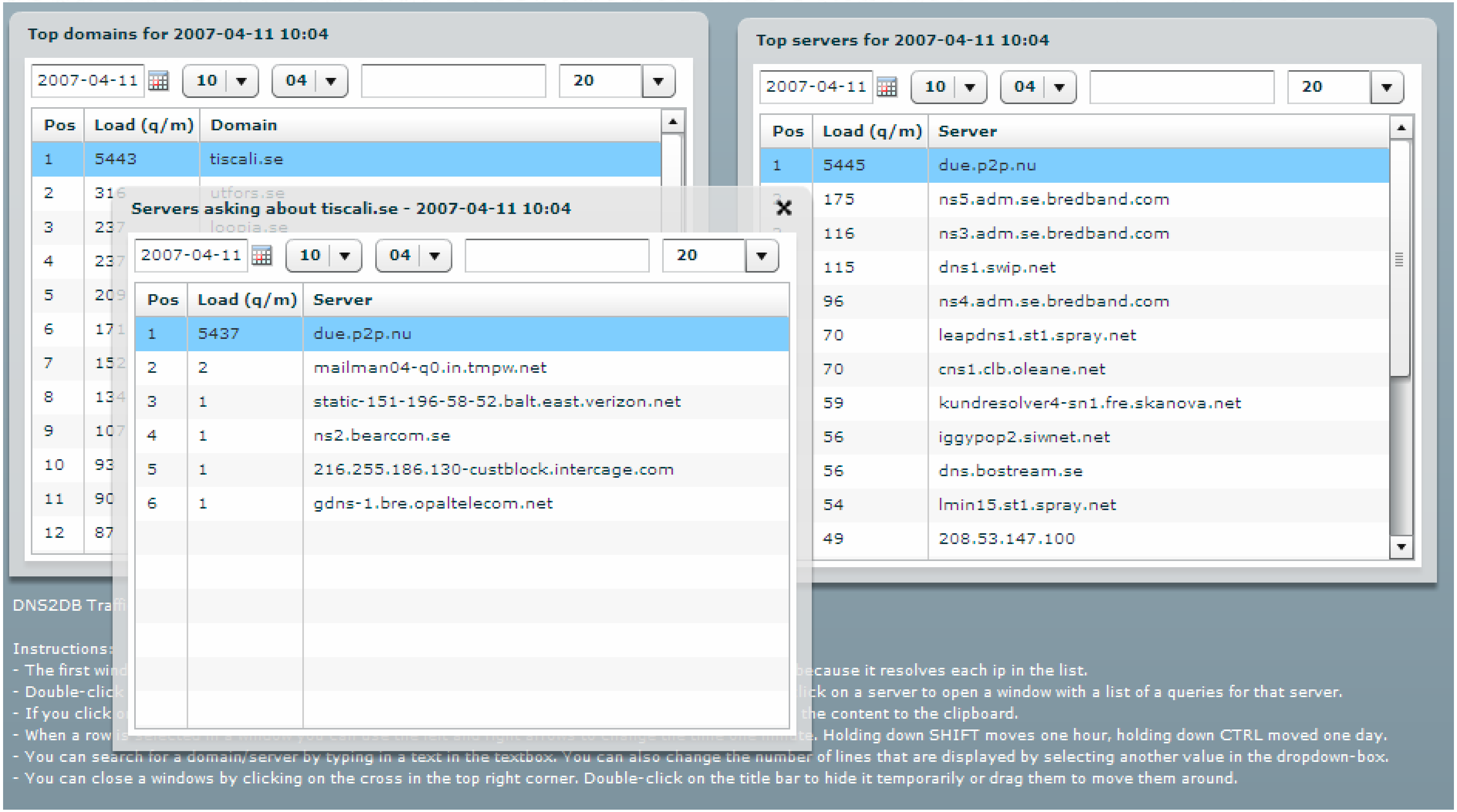
2007-04-11 | 10 | 04 | 20

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 Dahlst

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	

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

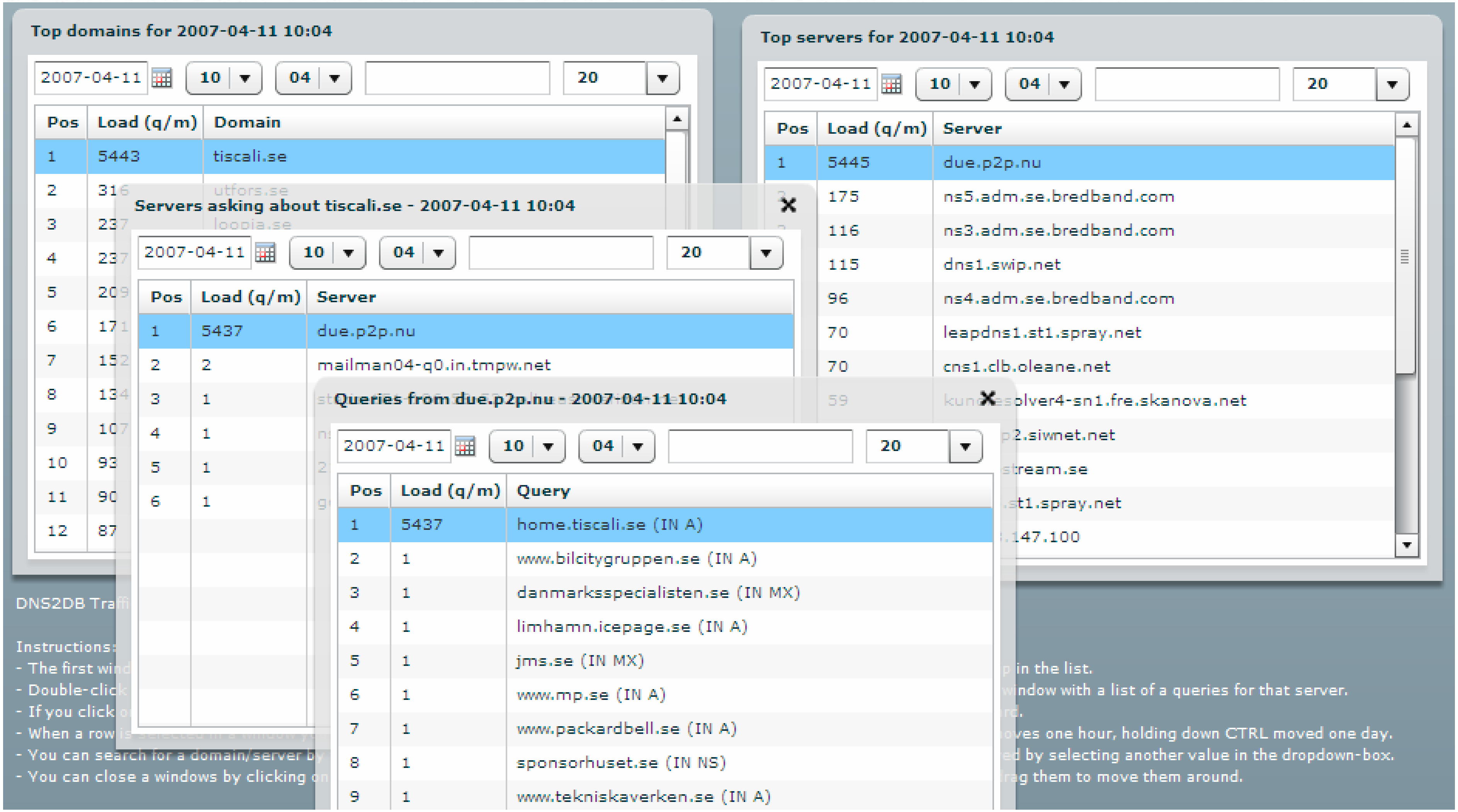
Servers asking about tiscali.se - 2007-04-11 10:04

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

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 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.



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	kun...esolver4-sn1.fre.skanova.net
		...2.siwnet.net
		...stream.se
		...st1.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	st
4	1	n
5	1	2
6	1	g

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 wind ... in the list.
- Double-click ... window with a list of a queries for that server.
- If you click o ... rc.
- When a row is selected in a window y ... oves one hour, holding down CTRL moved one day.
- You can search for a domain/server by ... ed by selecting another value in the dropdown-box.
- You can close a windows by clicking on ... rag them to move them around.

.se

Future

http://opensource.iis.se/trac/dns2db