Dns2db

DNS traffic statistics and by **.SE**

Written from scratch

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

.se

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

.se

Uses interactive frontend

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

.se

Performance

1 hour traffic with 250q/s average

85MB pcap file

pcap->sqlite3 ≈ 45 sec (HP DL380G4)

.se

Installation & setup

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

- Log rotation and job control from cron

.se

Directory structure

One directory per day

```
[niclas@snok /logg/dns2db]$ du -sh *
2.2G    2007-03-24
2.1G    2007-03-25
2.7G    2007-03-26
2.7G    2007-03-27
2.7G    2007-03-28
...
...
```

.se

Directory structure

One file per minute (time intervall configurable)

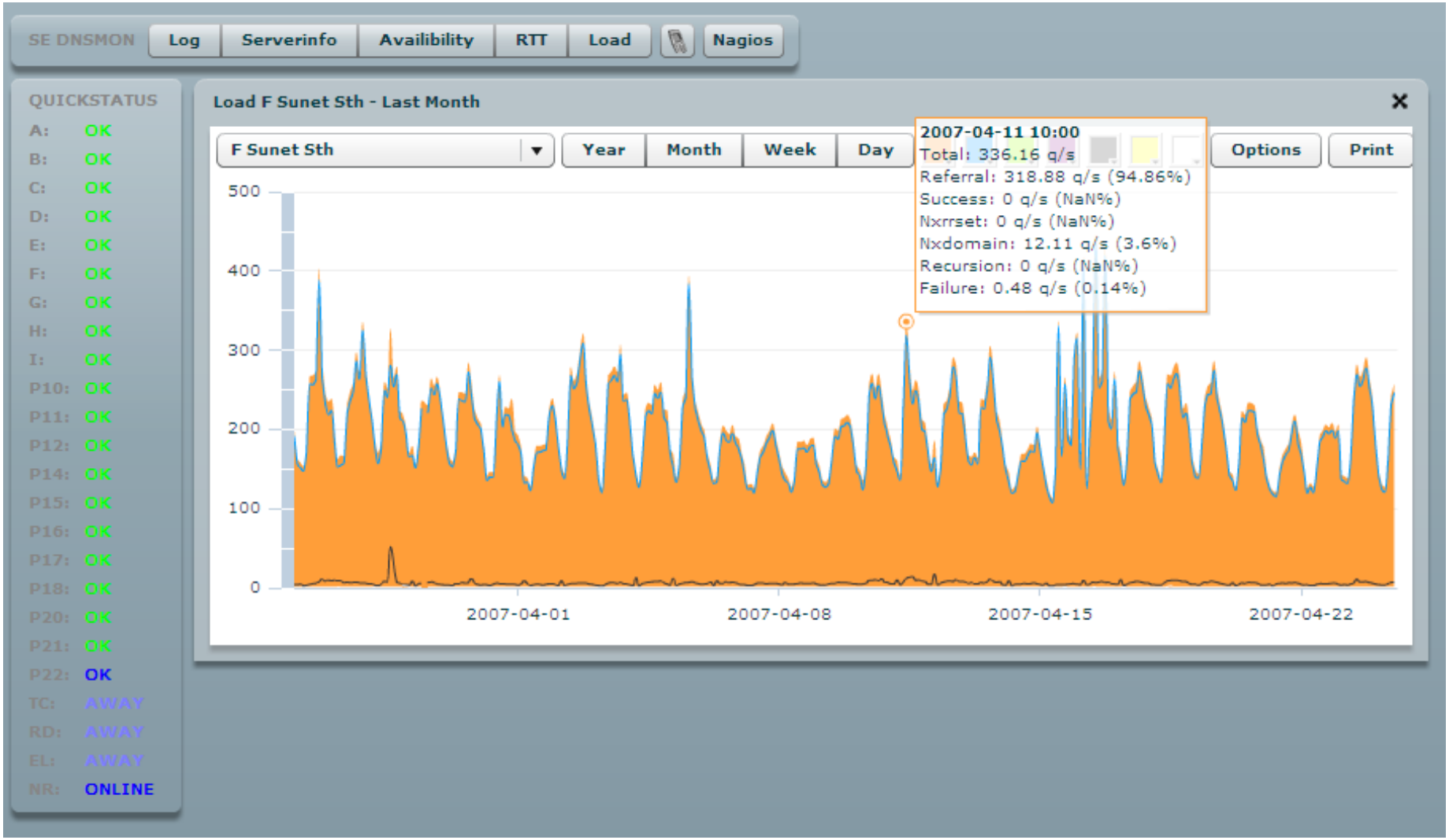
```
[niclas@snok /logg/dns2db/2007-04-22]$ du -sh *
1.4M    DSC.2007-04-22_00_00.db
1.3M    DSC.2007-04-22_00_01.db
1.4M    DSC.2007-04-22_00_02.db
1.4M    DSC.2007-04-22_00_03.db
1.4M    DSC.2007-04-22_00_04.db
1.5M    DSC.2007-04-22_00_05.db
...
...
```

.se

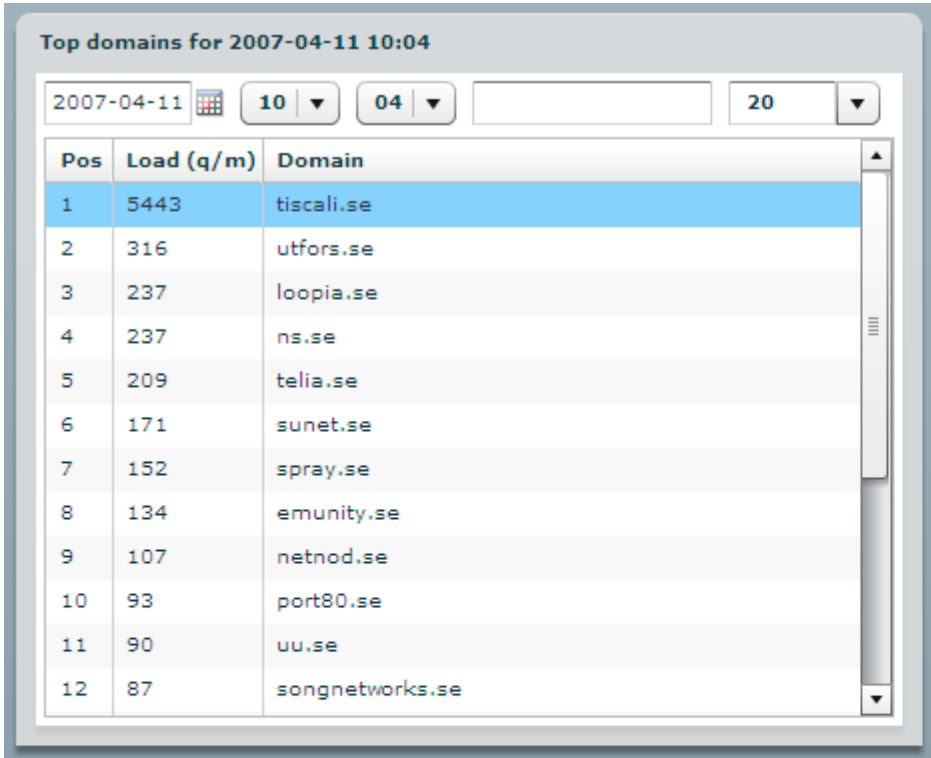
Table structure

- sqlite> select * from Q limit 1;
- id = 1
- ts = 1177417198
- msg_id = 13897
- Client_num = 117578696
- Client = 200.27.2.7
- Src_port = 32951
- Qtype = 1
- Qclass = 1
- MsgLen = 43
- Qname = dns2.utfors.se
- Opcode = 0
- Rd = 0
- Opt_RR = 1
- Do = 0
- Version = 0
- E1 = utfors.se
- E2 = 200.27.2.0

.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

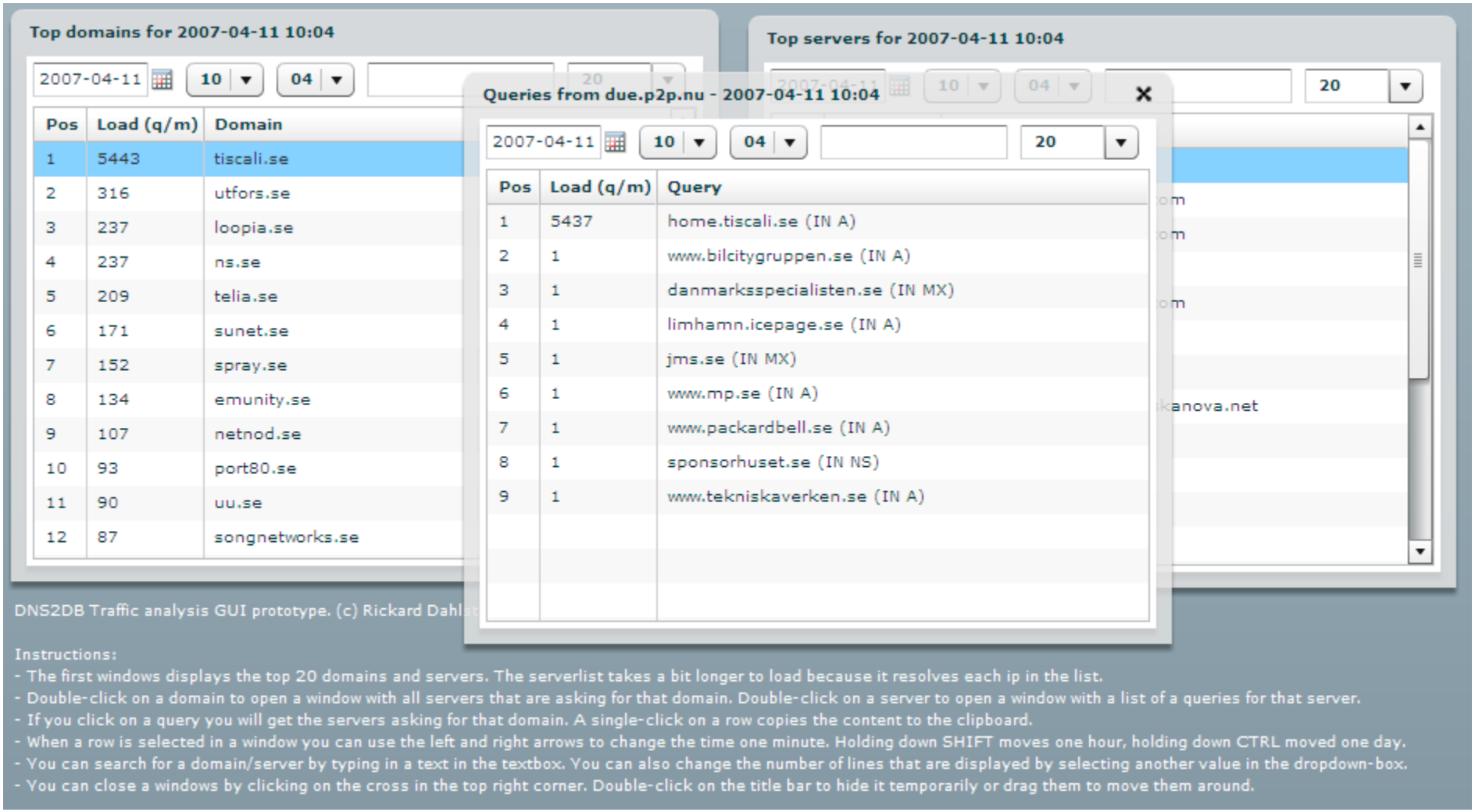


DNS2DB Traffic analysis GUI prototype. (c) Rickard Dahlstrand, IIS 2007.

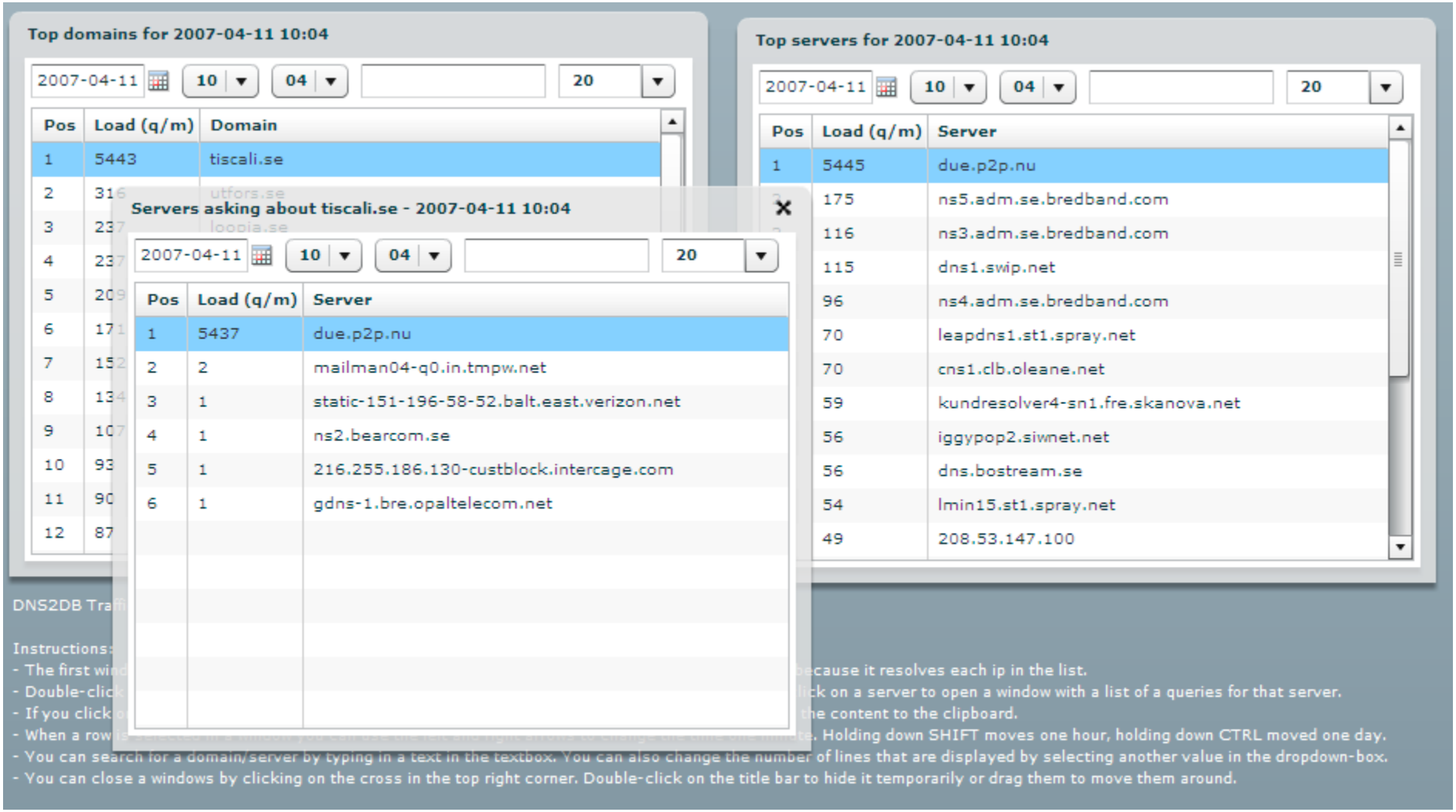
Instructions:

- 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.

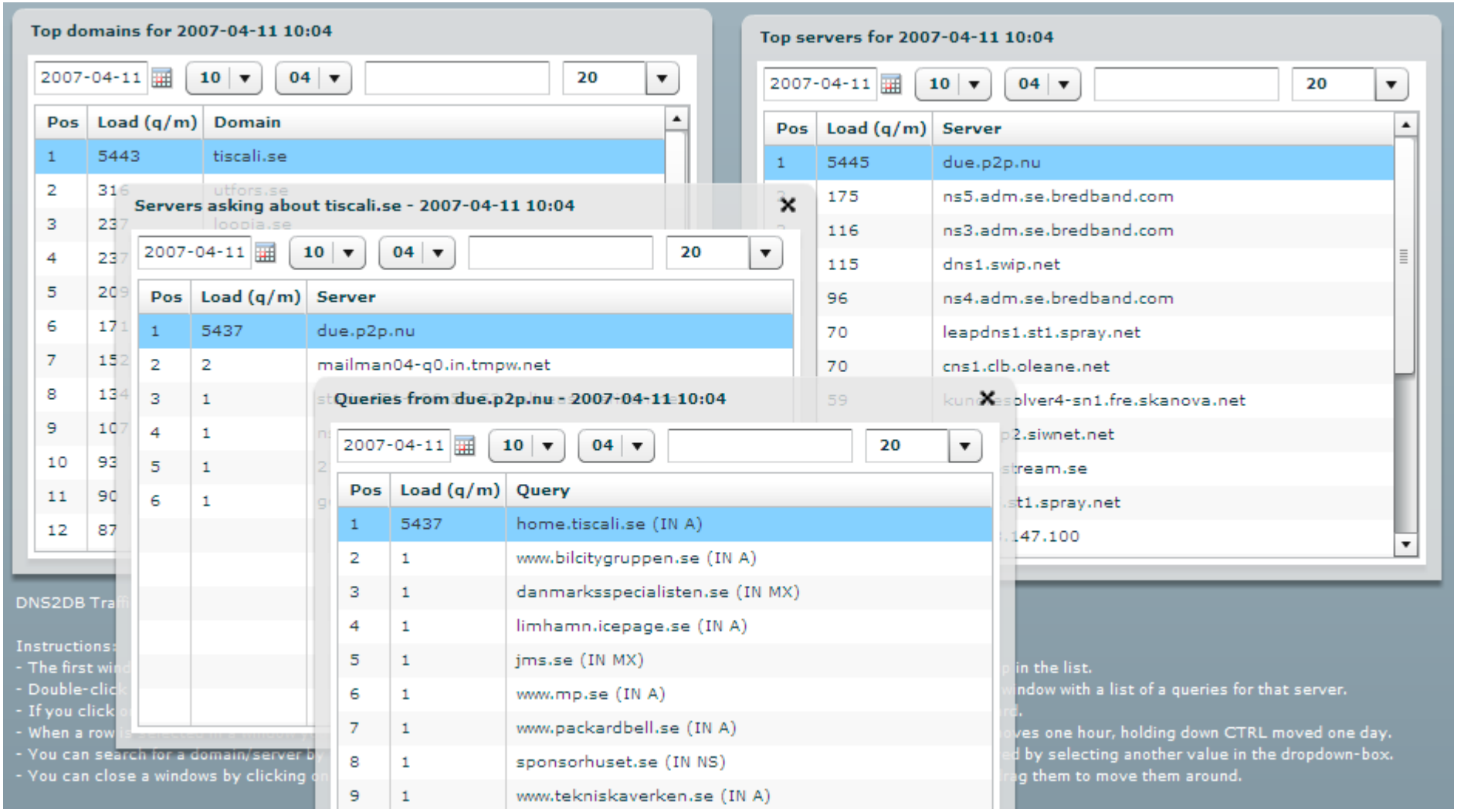
.se


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
ecause 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
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)
DNS2DB Traffi
Instructions:
- The first win
- Double-click
- If you click
- When a row
- You can search for a domain/server b
- You can close a windows by clicking
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.

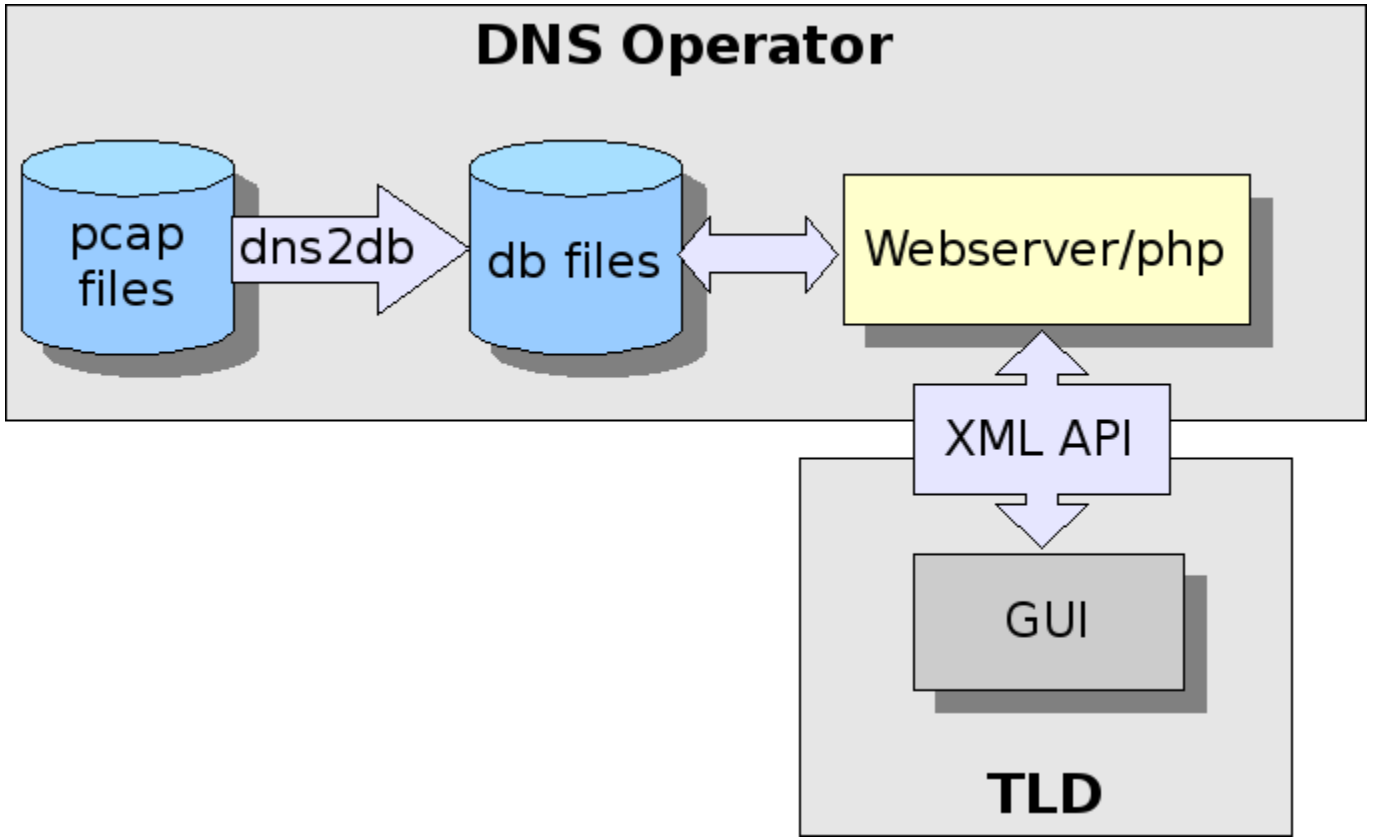
.se

Progress the last two months

- Convertion of TCP packets
- Ipv6
- 2x performance in conversion

.se

How to implement.


DNS Operator
pcap files
dns2db
db files
Webserver/php
XML API
GUI
TLD

.se

Future

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

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