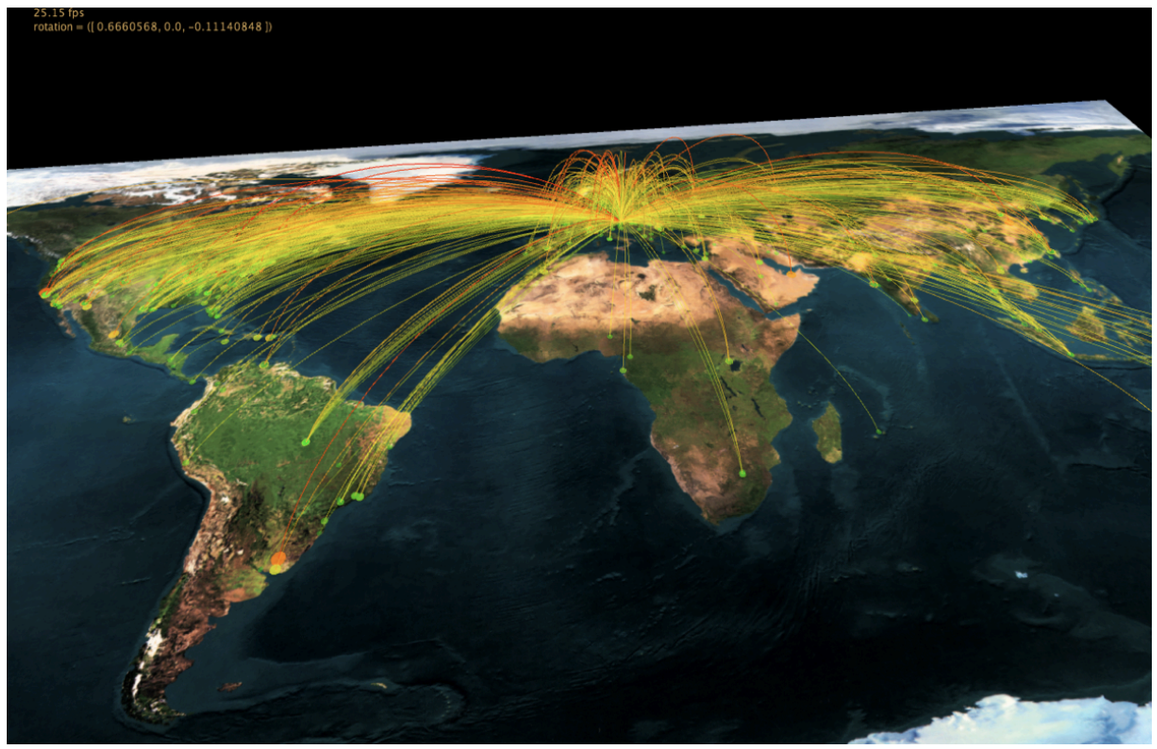
Passive DNS @ CERT.at
("pDNS")

contact:
L. Aaron Kaplan <kaplan@cert.at>
Tel: +43 1 505 64 16 / 78

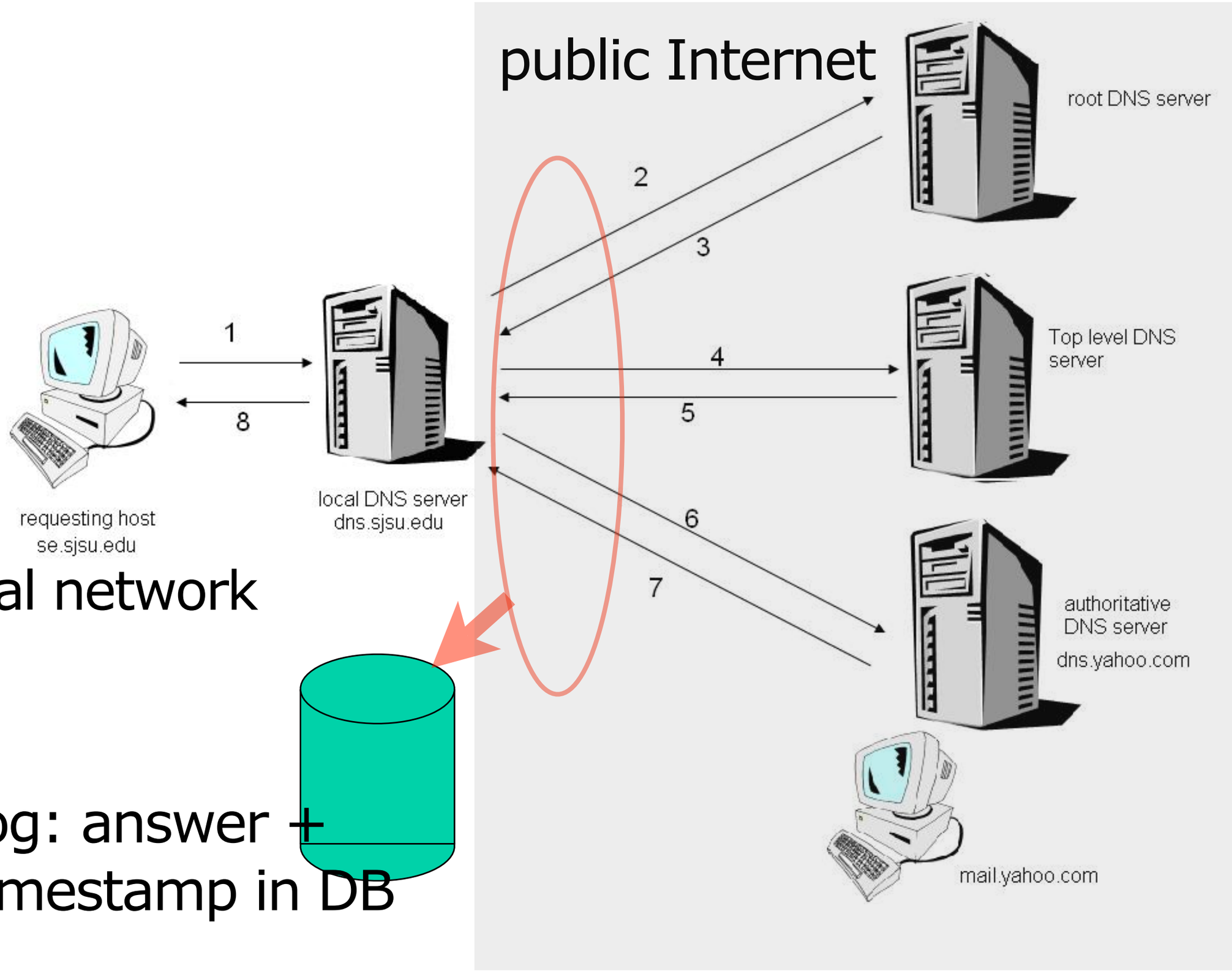
Idea & credits: Florian Weimer, BFK

pDNS @ CERT.at

- passive DNS: Idea to capture the DNS **answers** and give them a timestamp.
- Dataprotection -> omit src IPs (of client)!
- CERT.at + UniWien implemented a pDNS server: nmsg + C code + postgresql 9.0
- Optimized for **speed!** (~ 20 msec for a complex answer).
- 100% compatible with BFK pDNS.
- Cooperating with other pDNS servers
- webinterface, whois
- **Looking for sensors!**



pDNS @ CERT.at: Diagram



internal network

Log: answer +
Timestamp in DB

pDNS - new User Interface

CERT.at

CERT.at / ACOnet
DNS History

131.130.0.0/16 [Go] [Reset] [X]

Format: ○ Whois ○ csv ◉ HTML

Options: ☐ Sensor info ☐ Exact domain

List only: ☐ NXDOMAIN ☐ A ☐ NS ☐ CNAME ☐ SOA ☐ PTR ☐ MX ☐ TXT ☐ AAAA

Sort: [ ] desc ☐ , [ ] desc ☐ , [ ] desc ☐

```
% CERT.at / ACOnet DNS replicator WHOIS server, version 2.0.
% (C) 2011 All rights reserved.
% Authors: L. Aaron Kaplan <kaplan AT cert.at>
%          Achim Adam      <achim.adam AT univie.ac.at>
%
% 10000 elements (10000), 4.1737s
```

LEFT	RTYPE	RIGHT	FIRST-SEEN	LAST-SEEN	COUNT-SEEN
059c37b917f1ad2846b26bd6e11f0c0b.dnsscanner.org	A	131.130.250.130	2010-11-30 11:43:49	2010-11-30 11:43:49	1
0.at.pool.ntp.org	A	131.130.251.107	2010-09-16 16:54:07	2011-04-27 09:12:04	40
0.centos.pool.ntp.org	A	131.130.251.107	2010-07-21 08:33:21	2010-11-04 12:24:27	3
0.debian.pool.ntp.org	[illegible]	131.130.251.107	[illegible]	2011-04-28 21:48:01	1433
0.europe.[illegible]	A	131.130.251.107	2010-07-24 22:40:02	2011-01-06 21:45:[illegible]	6
[illegible]fedora.pool.ntp.org	A	131.130.[illegible]107	2010-07-19 0[illegible]:17:00	2011-04-2[illegible] 10:06:26	[illegible]
0.freebsd.pool.nt[illegible]	A	[illegible].130.[illegible]107	[illegible]	[illegible] 09:2[illegible]	6
[illegible] pool.ntp.org	A	131.130.251.107	2010-07-16 19:00:07	2011-04-14 [illegible]:14:00	[illegible]
0.opensuse.pool.[illegible]	A	131.130.251.107	2010-08-18 17:02:46	[illegible]	2
0.palm.pool.ntp.org	[illegible]	[illegible]	[illegible]	2011-03-15 16:51:40	1
0.pool.ntp.org	A	131.130.251.107	2010-07-17 00:52:08	2011-04-27 08:14:29	482
0.rhel.pool.ntp.org	A	131.130.251.107	2010-08-13 19:53:18	2011-03-18 07:29:51	40
0.ubuntu.pool.ntp.org	A	131.130.251.107	2011-04-27 14:43:44	2011-04-27 14:43:44	1
0.vmware.pool.ntp.org	A	131.130.251.107	2010-10-20 09:26:29	2010-10-20 09:26:29	1
0.xenclient.pool.ntp.org	A	131.130.251.107	2010-10-08 12:52:11	2010-10-08 14:16:50	2
100.23.177.202.u-914740bd847beca4.d-9dd954bb2bac5080.b20e	A	131.130.2.52	2010-07-20 16:21:50	2010-07-20 16:21:50	1

domaine, record type, IP, timeframe(from - last), count_seen

pDNS @CERT.at - Example

- Step 1: netblock: 193.104.XX.0/24. AS12XX / Vladimir BLABLAvich - suspected BP host
- Step 2: ask pDNS

```
rr-name: pharmazoria.com
rr-type: A
rr-address: 193.104.XX.164
seen-first: 2009-12-03 17:16:39
seen-last: 2009-12-30 12:33:43

rr-name: www.genericmedsusa.com
rr-type: A
rr-address: 193.104.XX.162
seen-first: 2009-12-16 16:04:07
seen-last: 2009-12-21 11:47:22
```

- lots of shady domain names

```
rr-name:
ns2.federalbankofnevada.com
rr-type: A
rr-address: 193.104.XX.69
seen-first: 2010-02-17 09:57:25
seen-last: 2010-02-21 12:04:29

rr-name: ns1.pronewmedia.com
rr-type: A
rr-address: 193.104.XX.67
seen-first: 2010-02-17 09:22:17
seen-last: 2010-02-22 19:51:36

rr-name: ns2.pronewmedia.com
rr-type: A
rr-address: 193.104.XX.67
seen-first: 2010-02-17 09:22:17
seen-last: 2010-02-22 19:51:36
```

Join! We want sensors.

Get access to the DB!