DNS Nameserver Database
Now at OARC

Duane Wessels
The Measurement Factory/CAIDA

WIDE+CAIDA Workshop #9
January 19, 2008

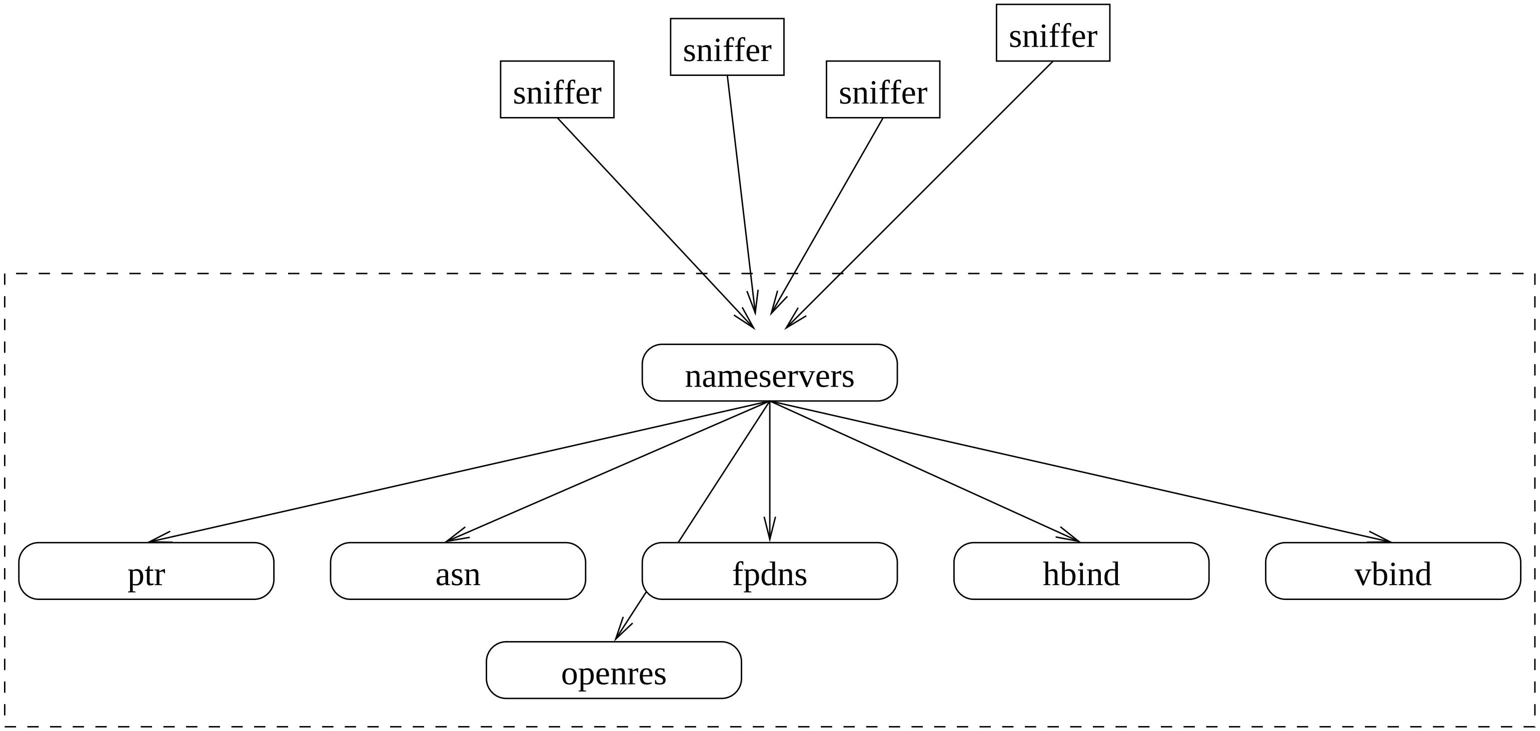
Motivation

- Measurement Factory and CAIDA were doing periodic surveys of nameservers, collecting information such as:
  - *fpdns* fingerprint
  - VERSION.BIND
  - HOSTNAME.BIND
  - PTR record
  - TCP support
- Also had separate survey/database of open resolvers.
- Wanted to turn periodic surveys into continuously updating database.
- Has been running for a year or so now.
- Recently transitioned to OARC.

Database Tables

- nameservers: Nameserver IP addresses
- names: DNS Names
- glue: “Glue” records
- fpdns: fingerprint
- hbind: hostname.bind records
- vbind: version.bind records
- asn: AS number
- ptr: PTR record
- openres: openresolver test result

Flow


sniffer
sniffer
sniffer
sniffer
nameservers
ptr
asn
fpdns
hbind
vbind
openres

Flow

- passive sniffers send nameserver IP addresses and DNS names to the database.
- nameservers are checked for aliveness by querying for one of (a.root-servers.net, www.google.com, localhost).
- Unresponsive nameservers are not probed any further.

Freshners

- Most of the tables have “freshner” scripts that run continuously and keep the tables up-to-date.
- For example, the fpdns freshner re-fingerprints a nameserver every 7 days.

Sample Database Queries I

- Find some ISC-hosted nameservers:

```
SELECT ptr.addr,ptr.ptrname
  FROM ptr,asn
  WHERE asn.asn=1280
  AND ptr.addr=asn.addr ;

      addr       |             ptrname
-----------------+--------------------------------
 204.152.191.230 | <no answers>
 204.152.188.30  | lah1z.vix.com
 204.152.186.173 | packman-ha.isc.org
 204.152.186.179 | art.net
 204.152.186.144 | white.flame.org
 204.152.185.196 | <no answers>
 204.152.184.202 | ns-us1.nic.at
 204.152.184.203 | obsd.isc.org
 204.152.186.45  | klapaucius.zer0.org
 204.152.186.50  | boole.openldap.org
 204.152.186.51  | galois.openldap.org
 204.152.186.52  | cantor.openldap.org
 204.152.186.58  | proxy8.monitor.dal.net
```

Sample Database Queries II

- Who runs Nominet software?

```
SELECT vbind.addr,ptr.ptrname,vbind_seq.str
  FROM vbind,vbind_seq,ptr
  WHERE vbind_seq.str like 'Nominum%'
  AND vbind_seq.id=vbind.vbind_id
  AND vbind.addr=ptr.addr ;

      addr       |             ptrname              |           str
-----------------+----------------------------------+-------------------------
 192.220.125.193 | ns2.onlyhosting.net              | Nominum ANS 2.5.0.0
 192.220.125.164 | ns2.hileytech.net                | Nominum ANS 2.5.0.0
 212.74.78.48    | ns2.colt-telecom.nl              | Nominum ANS 2.8.0.0
 202.166.27.108  | ad202.166.27.108.magix.com.sg    | Nominum ANS 2.8.1.2
 192.220.125.129 | ns2.wanderers.com                | Nominum ANS 2.5.0.0
 192.220.125.64  | ns2.axinet.com                   | Nominum ANS 2.5.0.0
 212.74.78.17    | ns0.be.colt.net                  | Nominum ANS 2.8.0.0
 192.220.125.87  | ns2.warbler.com                  | Nominum ANS 2.5.0.0
 192.220.125.19  | nsb.ntx.net                      | Nominum ANS 2.5.0.0
 192.220.124.141 | dns1.webhost.be                  | Nominum ANS 2.5.0.0
```

Sample Database Queries III

- Which nameservers have IPv6 addresses?

```
SELECT name,v6
  FROM glue
  WHERE v6!= '{}' ;

          name           |                 v6
-------------------------+-----------------------------------
 jupiter.luon.net        | {2001:888:1d84::}
 ns1.uninet.net.id       | {2001:dc6:ff8e::1}
 ns1.es.net              | {2001:400:14:2::10}
 bofh.it                 | {2001:1418:13::42}
 dns2.nhinetworks.com    | {::ffff:204.251.15.190}
 ns01.lindos.ch          | {2001:1b50::82:195:225:110}
 dns1.consulintel.com    | {2a01:48:20:0:200:1cff:feb5:c535}
 mx-in.itb.ac.id         | {2001:d30:3:0:202:44ff:fe35:228c}
 dns.koli.uni-miskolc.hu | {2001:738:6001:3f00::1}
 skm.shonan.bunkyo.ac.jp | {2001:200:166:2001::2}
```

Fingerprints For Everyone

- fpdns fingerprints are served as a “DNSBL”:

  ```
  $ dig +short 241.5.5.192.fpdns.measurement-factory.com txt
  "ISC BIND 9.2.3rc1 -- 9.4.0a0"
  ```

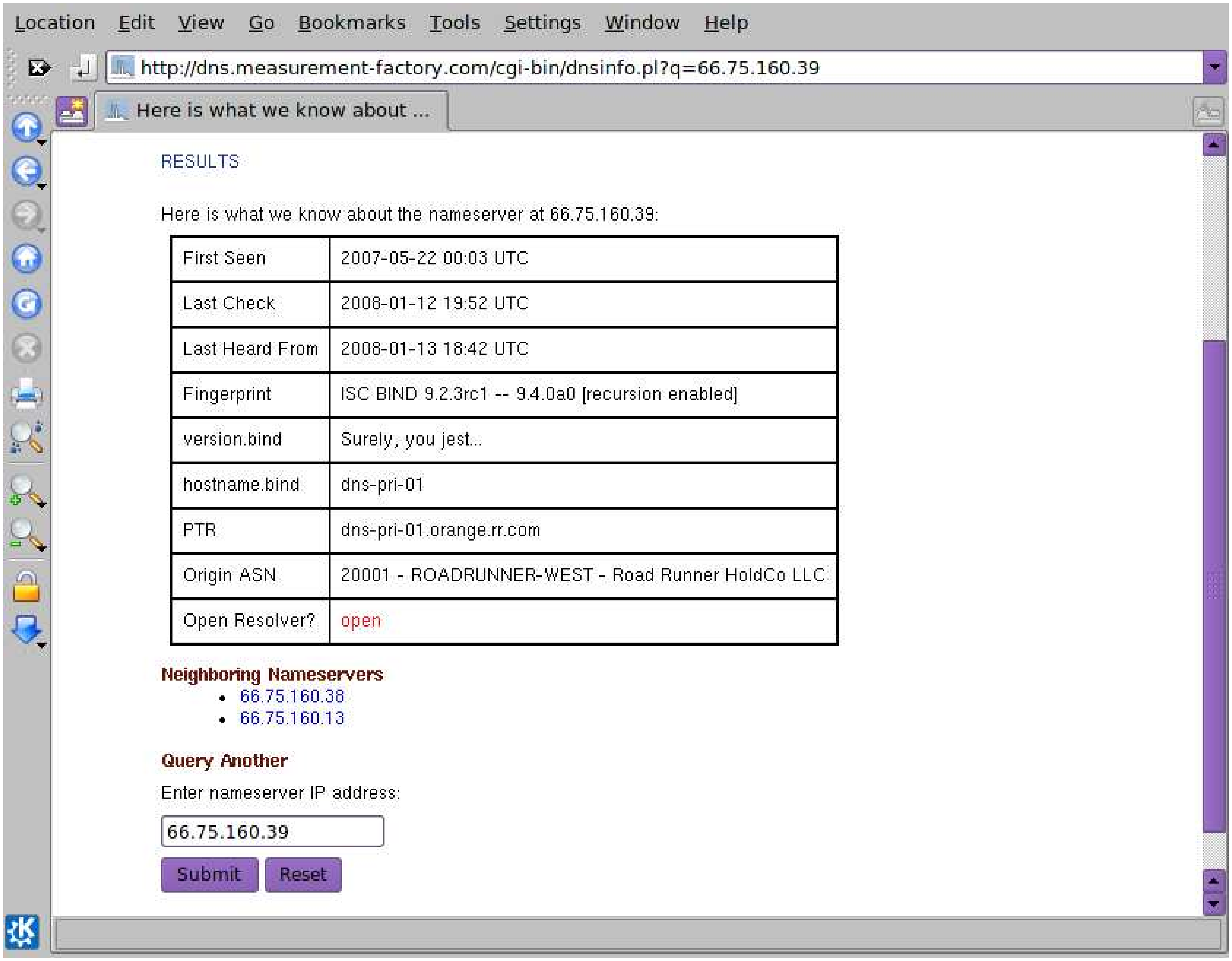
- Could also serve additional data this way.

Is My Resolver Open?

- dig it:

```
$ dig +short amiopen.openresolvers.org txt
"Your resolver at 66.75.164.90 is CLOSED"
```

dnsinfo.pl



Location Edit View Go Bookmarks Tools Settings Window Help
http://dns.measurement-factory.com/cgi-bin/dnsinfo.pl?q=66.75.160.39
Here is what we know about ...

RESULTS

Here is what we know about the nameserver at 66.75.160.39:

First Seen	2007-05-22 00:03 UTC
Last Check	2008-01-12 19:52 UTC
Last Heard From	2008-01-13 18:42 UTC
Fingerprint	ISC BIND 9.2.3rc1 -- 9.4.0a0 [recursion enabled]
version.bind	Surely, you jest...
hostname.bind	dns-pri-01
PTR	dns-pri-01.orange.rr.com
Origin ASN	20001 - ROADRUNNER-WEST - Road Runner HoldCo LLC
Open Resolver?	open

Neighboring Nameservers

- 66.75.160.38
- 66.75.160.13

Query Another

Enter nameserver IP address:

66.75.160.39

Future Work

- Document database and how OARC members and public can utilize it.
- Use ISC's SIE to feed database with addresses, zones, and names.
  - To the extent that this little database can take the increased load
- Add tables and code to track relationships between name-servers and zones they serve.
- Keep track of whether a nameserver is used to serve authoritative data, as a caching resolver (sorry, iterative mode resolver), or both.

The End