

DNS as a Defense Vector

Dr. Paul Vixie, CEO
Farsight Security
Ruxcon, 2015-10-25

Topic

DNS Itself

Internet as Territory

- But what **is** the internet?
 - “It's the largest equivalence class in the reflexive transitive symmetric closure of the relationship *can be reached by an IP packet from.*”
 - (Seth Breidbart)
- IP addresses, IP packets, underlie everything
- We overlay IP with many things, e.g., *the web*
- Most important overlay (for security) is: DNS

DNS as Map

- Most everything we do on the Internet...
 - B2C Web, B2B Web, E-mail, I-M, *<your idea here>*
 - ...relies on TCP/IP, and begins with a DNS lookup
- Mobile Internet is dominated by search...
 - ...but search itself relies extensively upon DNS
- DNS has a rigorous internal structure
 - Things that are in fact related, *are* related in DNS
 - You can have *whois* privacy, but not DNS privacy

Criminal DNS

- The Internet has been a great accelerator of human civilization
 - Sadly, the criminals came along for the ride
- Online crime is impossible without DNS
 - Cheap throw-away domain names
 - DNS registrars and servers in bad neighborhoods
 - *Whois* privacy or simply bad *whois* data
- *Nature, to be commanded, must be obeyed.*
 - (Francis Bacon)

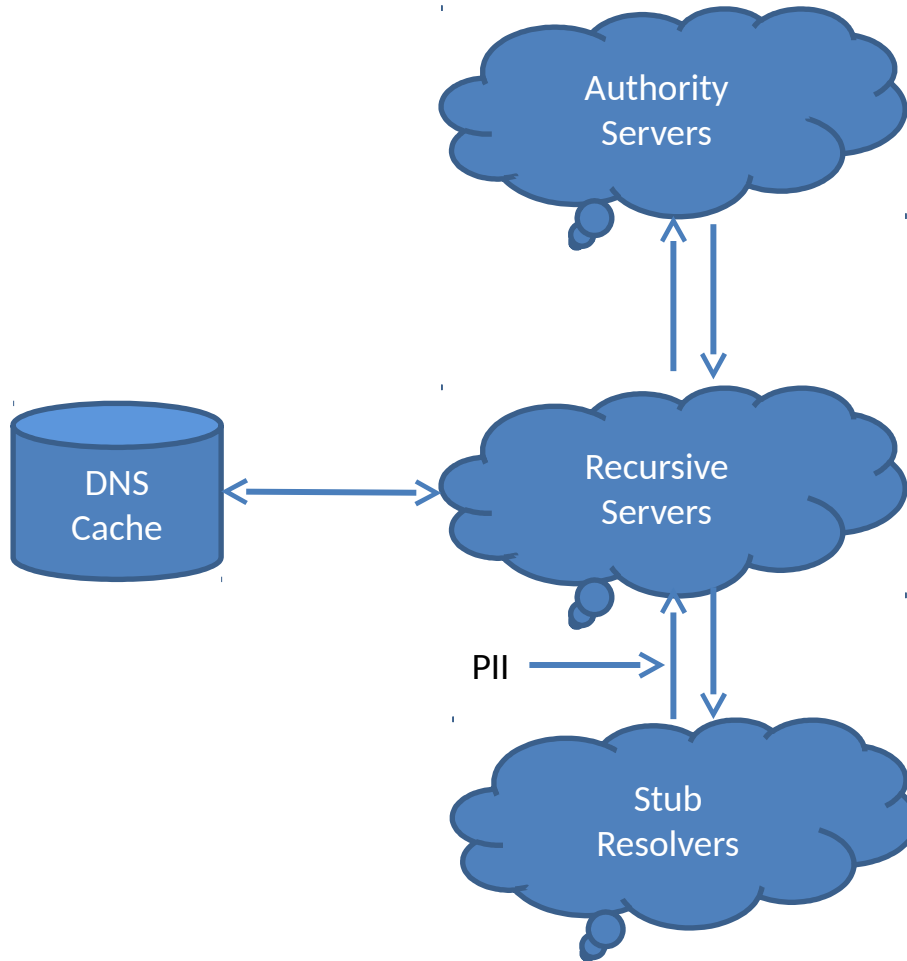
So, About that Internal Structure

- Domain names are grouped into *zones*
 - Like *root* zone, or “COM”, or “EXAMPLE.COM”
- A *zone* has one or more *name servers*
 - Like “COM. NS a.gtld-servers.net.”
- Each *name server* has one or more *addresses*
 - Like “a.gtld-servers.net. A 192.5.6.30”
- Other domain names also have *addresses*
 - Like “www.apnic.net. A 203.119.102.244”
- IP *addresses* are grouped into *netblocks*
 - Like “192.5.6.0/24” or “203.119.102.240/28”

DNS Security Features

- TSIG secures heavy weight transactions
 - Like UPDATE, IXFR/AXFR; but not QUERY
- DNSSEC secures data end-to-end
 - Zone is signed; responses contain signatures
 - Zone has keys; these are signed in parent zone
 - QUERY initiator can validate signatures
 - Requires universally trusted *root signing key*
- Use TSIG and DNSSEC: they work, they'll help
 - But: our actual topic today lies elsewhere

DNS Data Flow



13 root servers,
~250 Cctld's,
~15 old Gtld's,
~2000 new Gtld's,
~500M 2LD/etc

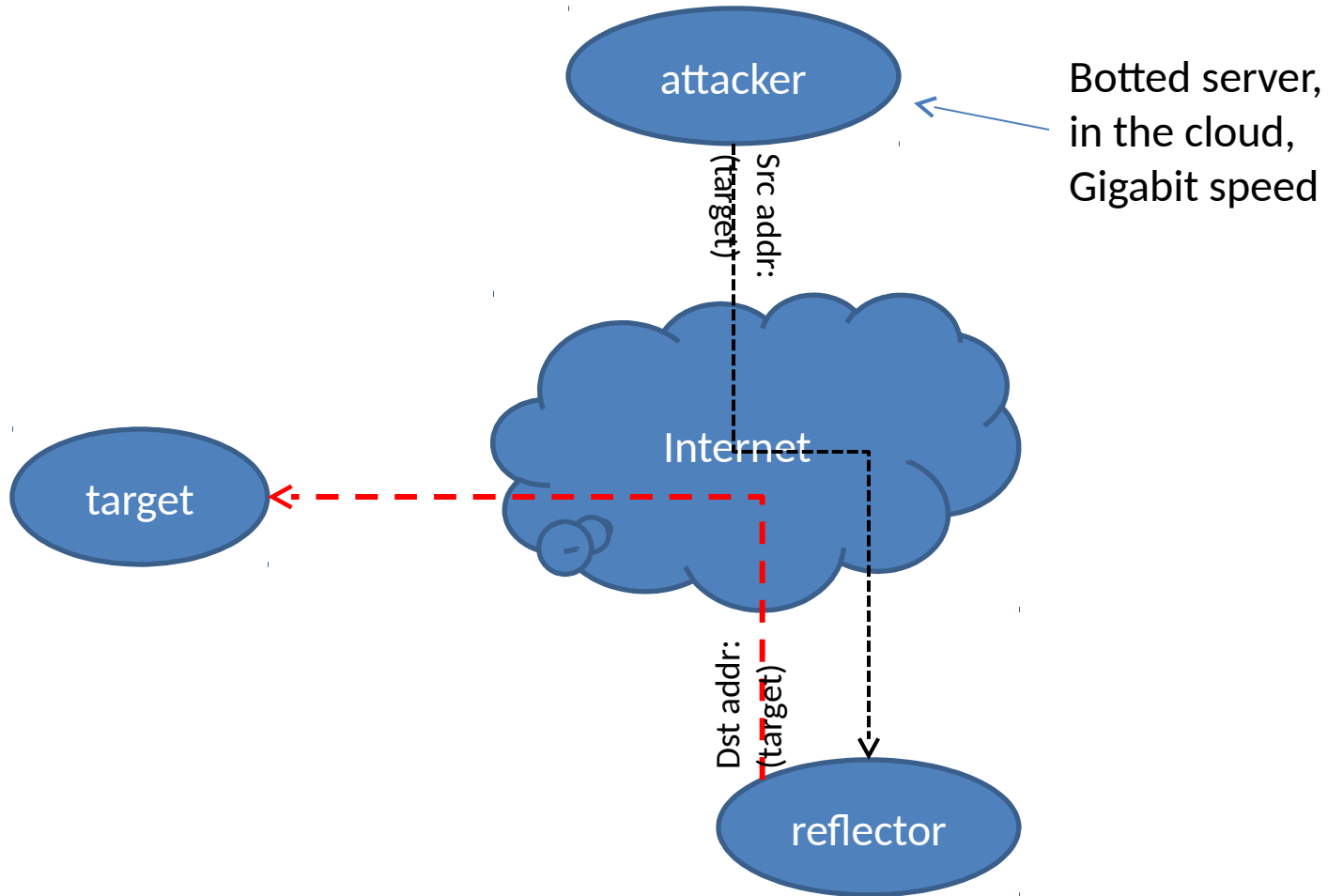
Campus,
Enterprise,
OpenDNS,
GoogleDNS

Servers, Laptops,
Smartphones,
embedded devs

Topic

DNS As Abused

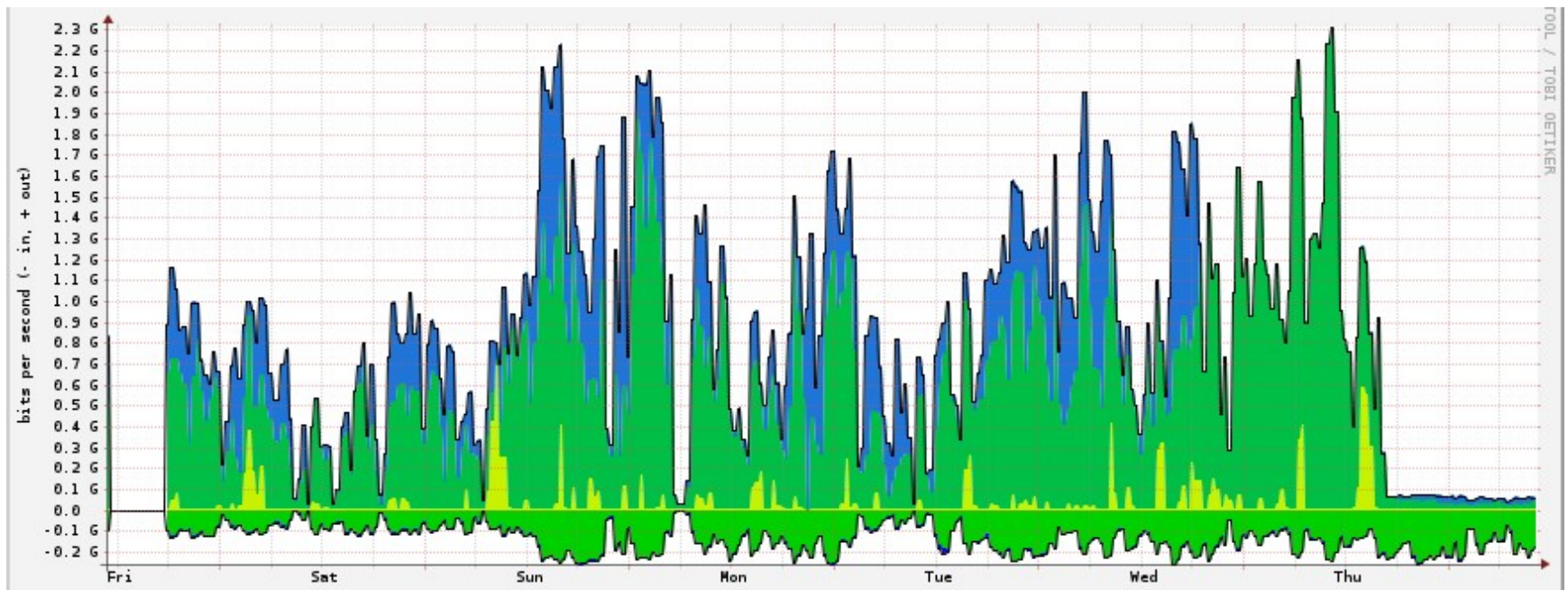
Spoofed Source Attacks



DNS Response Rate Limiting (RRL)

- If you run a DNS content (“authority”) server, it has to be massively overprovisioned
- Because OPN’s don’t have SAV, your server is a purpose-built DNS DDoS reflecting amplifier
- BIND and NSD now support DNS RRL, which accurately guesses what’s safe to drop
- Your authority servers need this, whereas your recursive servers need to be firewalled off

RRL In Action: Afilias



“...too cheap to meter”

- SpamAssassin as a teaching tool
 - For example: dotted quads in body as spamsign
- RRP and EPP: solving “the .COM problem”
 - Running a race to the bottom (cheaper; sooner)
- Quantity and fluidity having only one purpose
 - 30 seconds? Really?
- Fitting Sturgeon’s revelation
 - “90% of <thing> is crap”

Takedown: Far End Tactics

- Since we can't prevent it...
 - ...we'll have to evolve coping strategies
- Takedown as a Service (TaaS?)
 - Yes, you can outsource this now
- A new profit center! (.TK)
 - “Kill all you want, we'll make more!”
- Whack-a-mole as a Service (WaaS?)
 - Incrementalism breeds better criminals

Firewalls: Near End Tactics

- If we can't prevent it and takedown is hard...
 - ...then we'll have to fight them at our threshold
- We can filter IP+port, URL, and now even DNS
 - But, bad guys are endlessly mobile and numerous
 - Thus, the Internet creates another new industry!
- We can't afford manual configuration
 - So, firewall config now follows a pub-sub model

Response Policy Zones: High Level

- Uses DNS zones to carry DNS Firewall policy
 - R-P-Z = Response Policy Zones
- Pub-sub is handled by NOTIFY/TSIG/IXFR
 - Many publishers, many subscribers, one format
- Subscribe to multiple external feeds
 - And create your own, for local policy reasons
- Simple failure or walled garden, as you choose
 - We call this “taking back the DNS”

RPZ Capabilities

- Triggers (RR owners):
 - If the query name is \$X
 - If the response contains an address in CIDR \$X
 - If any NS name is \$X
 - If any NS address is in CIDR \$X
 - If the query source address is in CIDR \$X
- Actions (RR data):
 - Synthesize NXDOMAIN
 - Synthesize CNAME
 - Synthesize NODATA
 - Synthesize an answer
 - Answer with the truth

Why Use RPZ?

- Easy stuff:
 - Block access to DGA C&C's
 - Block access to known phish/driveby
 - Block e-mail if envelope/header is spammy
- More interesting stuff:
 - Block DNS A/AAAA records in bad address space
 - E.g., import Cymru Bogons or Spamhaus DROP list
 - Block domains having some computable attribute
 - E.g., Farsight Newly Observed Domains (NOD) list

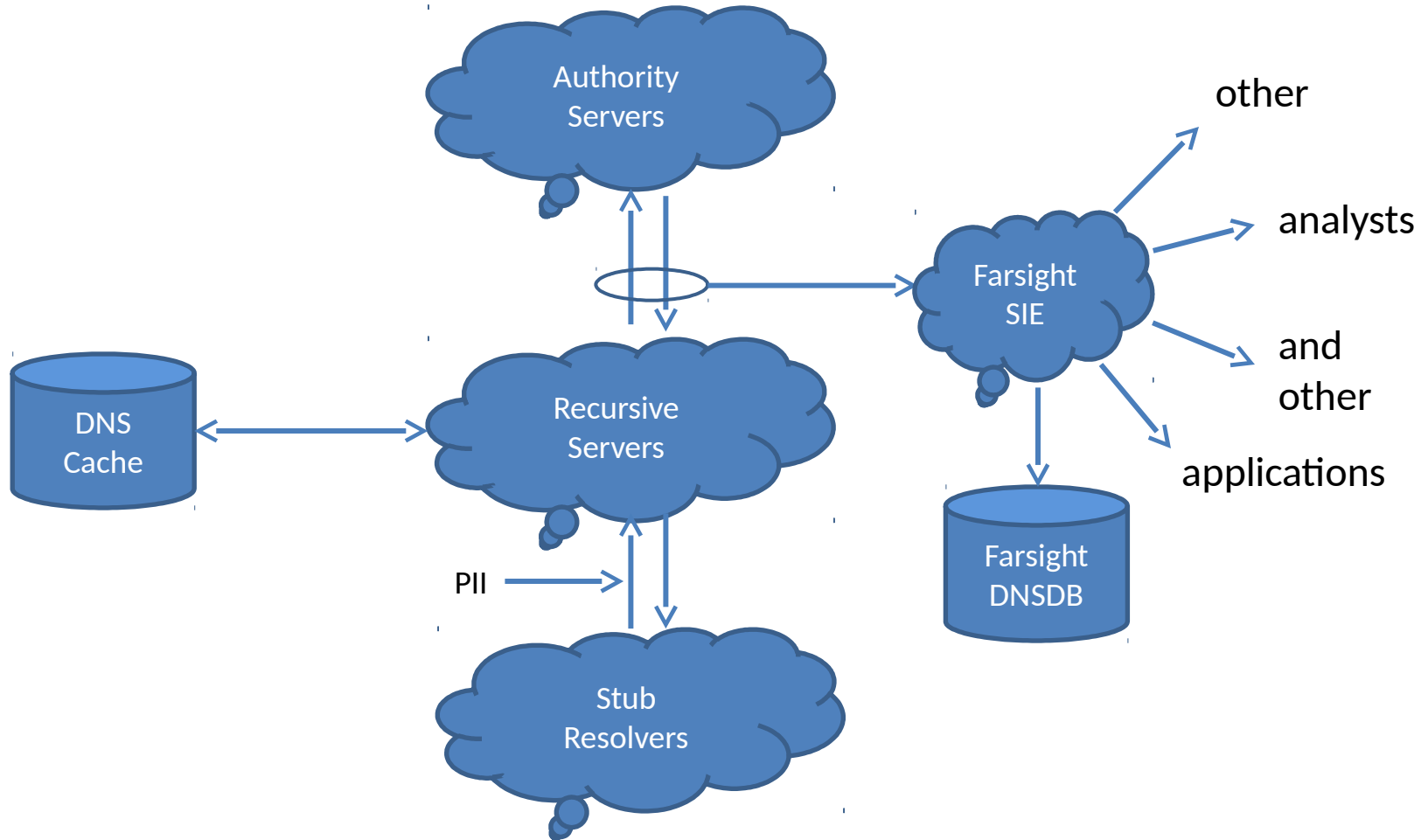
Key RPZ Takeaways

- Implications:
 - Open market for producers and consumers
 - Differentiated service at a global scale
 - Instantaneous wide area takedown
- Deployment:
 - The RPZ standard is open and unencumbered
 - So far implemented only in BIND (PowerDNS, Knot: soon)
 - BIND RPZ performance is not unreasonable (~5% QPS loss)
 - New features will be backward compatible
 - This is not an IETF standard

Topic

DNS As Observed

Passive DNS Data Flow



Owner Lookup, Show History

```
$ dnsdb_query -r vix.com/ns/vix.com
...
;; record times: 2010-07-04 16:14:12 \
                .. 2013-05-12 00:55:59
;; count: 2221563; bailiwick: vix.com.
vix.com.  NS  ns.sql1.vix.com.
vix.com.  NS  ns1.isc-sns.net.
vix.com.  NS  ns2.isc-sns.com.
vix.com.  NS  ns3.isc-sns.info.

;; record times: 2013-10-18 06:30:10 \
                .. 2014-02-28 18:13:10
;; count: 330; bailiwick: vix.com.
vix.com.  NS  buy.internettraffic.com.
vix.com.  NS  sell.internettraffic.com.
```

Owner Wildcards (left or right side)

```
$ dnsdb_query -r \*.vix.com/a | fgrep 24.104.150
internal.cat.lah1.vix.com.  A  24.104.150.1
ss.vix.com.                 A  24.104.150.2
gutentag.vix.com.          A  24.104.150.3
lah1z.vix.com.             A  24.104.150.4
mm.vix.com.                A  24.104.150.11
ww.vix.com.                A  24.104.150.12
external.cat.lah1.vix.com. A  24.104.150.33
wireless.cat.lah1.vix.com. A  24.104.150.65
wireless.ss.vix.com.       A  24.104.150.66
ap-kit.lah1.vix.com.       A  24.104.150.67
cat.lah1.vix.com.          A  24.104.150.225
vix.com.                   A  24.104.150.231
deadrat.lah1.vix.com.      A  24.104.150.232
ns-maps.vix.com.          A  24.104.150.232
ns.lah1.vix.com.          A  24.104.150.234
```

Data Lookup, By Name

```
$ ./dnsdb_query -n ss.vix.su/mx
vix.su.                MX    10  ss.vix.su.
dns-ok.us.            MX     0  ss.vix.su.
mibh.com.            MX     0  ss.vix.su.
iengines.com.       MX     0  ss.vix.su.
toomanydatsuns.com. MX     0  ss.vix.su.
farsightsecurity.com. MX    10  ss.vix.su.
anog.net.           MX     0  ss.vix.su.
mibh.net.           MX     0  ss.vix.su.
tisf.net.          MX    10  ss.vix.su.
iengines.net.      MX     0  ss.vix.su.
al.org.            MX     0  ss.vix.su.
vixie.org.         MX     0  ss.vix.su.
redbarn.org.       MX     0  ss.vix.su.
benedelman.org.    MX     0  ss.vix.su.
```


Data Lookup, by IP Address

```
$ dnsdb_query -r ic.fbi.gov/mx  
ic.fbi.gov.  MX  10 mail.ic.fbi.gov.
```

```
$ dnsdb_query -r mail.ic.fbi.gov/a  
mail.ic.fbi.gov.  A  153.31.119.142
```

```
$ dnsdb_query -i 153.31.119.142  
ic.fbi.gov.      A  153.31.119.142  
mail.ic.fbi.gov. A  153.31.119.142  
mail.ncijtf.fbi.gov. A  153.31.119.142
```

Data Lookup, by IP Address Block

```
$ dnsdb_query -i 153.31.119.0/24 | grep -v infragard
vpn.dev2.leo.gov.      A 153.31.119.70
mail.leo.gov.         A 153.31.119.132
www.biometriccoe.gov. A 153.31.119.135
www.leo.gov.          A 153.31.119.136
cgate.leo.gov.        A 153.31.119.136
www.infraguard.net.   A 153.31.119.138
infraguard.org.       A 153.31.119.138
www.infraguard.org.   A 153.31.119.138
mx.leo.gov.           A 153.31.119.140
ic.fbi.gov.           A 153.31.119.142
mail.ic.fbi.gov.      A 153.31.119.142
mail.ncijtf.fbi.gov.  A 153.31.119.142
```

Technical Formatting Notes

- These slides show a DNS output conversion
 - The real output is in JSON format, i.e.:

```
$ dnsdb_query -r f.root-servers.net/a/root-servers.net
;; record times: 2010-06-24 03:10:38 .. 2014-03-05 01:22:56
;; count: 715301521; bailiwick: root-servers.net.
f.root-servers.net.  A  192.5.5.241
```

```
$ dnsdb_query -r f.root-servers.net/a/root-servers.net -j
{"count": 715301521, "time_first": 1277349038, "rrtype":
"A", "rrname": "f.root-servers.net.", "bailiwick": "root-
servers.net.", "rdata": ["192.5.5.241"], "time_last":
1393982576}
```

DNSDB Deployment Notes

- FSI Passive DNS sensor is open source (PCAP)
 - ‘dnstap’ is coming soon, for server embedding
- The FSI DNSDB API is open (now an IETF I-D)
 - FSI, 360 Networks, NIC.AT all operate servers
- FSI DNSDB is quasi-commercial:
 - Full grant for students (with advisor’s approval)
 - Partial grant for those who operate sensors for us
 - Commercially available for use, resale, embedding

Limited Bibliography

<https://www.farsightsecurity.com/>
<http://www.redbarn.org/dns/ratelimits>
<http://dnsrcp.info/>
<https://dnsdb.info/>
<https://dnstap.info/>