DNS Debugging and monitoring

João Damas
Shane Kerr
Outline

• The basics
• Zone verification
• Instant analysis
• Longer term/ongoing analysis
• Special focus on debugging DNSSEC
The basics

• DNS and errors

• Basic Tools
  – nslookup
  – DiG
  – drill
DNS and errors

- DNS has a very limited set of error/return codes (RCODEs)

### Registry Name: DNS RCODEs

<table>
<thead>
<tr>
<th>Decimal</th>
<th>Name</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>NoError</td>
<td>No Error</td>
<td>[RFC1035]</td>
</tr>
<tr>
<td>1</td>
<td>FormErr</td>
<td>Format Error</td>
<td>[RFC1035]</td>
</tr>
<tr>
<td>2</td>
<td>ServFail</td>
<td>Server Failure</td>
<td>[RFC1035]</td>
</tr>
<tr>
<td>3</td>
<td>NXDomain</td>
<td>Non-Existent Domain</td>
<td>[RFC1035]</td>
</tr>
<tr>
<td>4</td>
<td>NotImp</td>
<td>Not Implemented</td>
<td>[RFC1035]</td>
</tr>
<tr>
<td>5</td>
<td>Refused</td>
<td>Query Refused</td>
<td>[RFC1035]</td>
</tr>
<tr>
<td>6</td>
<td>YXDomain</td>
<td>Name Exists when it should not</td>
<td>[RFC2136]</td>
</tr>
<tr>
<td>7</td>
<td>YXRRSet</td>
<td>RR Set Exists when it should not</td>
<td>[RFC2136]</td>
</tr>
<tr>
<td>8</td>
<td>NXRRSet</td>
<td>RR Set that should exist does not</td>
<td>[RFC2136]</td>
</tr>
<tr>
<td>9</td>
<td>NotAuth</td>
<td>Server Not Authoritative for zone</td>
<td>[RFC2136]</td>
</tr>
<tr>
<td>10</td>
<td>NotZone</td>
<td>Name not contained in zone</td>
<td>[RFC2136]</td>
</tr>
<tr>
<td>11-15</td>
<td>Unassigned</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>BADVERS</td>
<td>Bad OPT Version</td>
<td>[RFC2671]</td>
</tr>
<tr>
<td>16</td>
<td>BADSIG</td>
<td>TSIG Signature Failure</td>
<td>[RFC2845]</td>
</tr>
<tr>
<td>17</td>
<td>BADKEY</td>
<td>Key not recognized</td>
<td>[RFC2845]</td>
</tr>
<tr>
<td>18</td>
<td>BADTIME</td>
<td>Signature out of time window</td>
<td>[RFC2845]</td>
</tr>
<tr>
<td>19</td>
<td>BADMODE</td>
<td>Bad TKEY Mode</td>
<td>[RFC2930]</td>
</tr>
<tr>
<td>20</td>
<td>BADNAME</td>
<td>Duplicate key name</td>
<td>[RFC2930]</td>
</tr>
<tr>
<td>21</td>
<td>BADALG</td>
<td>Algorithm not supported</td>
<td>[RFC2930]</td>
</tr>
<tr>
<td>22</td>
<td>BADTRUNC</td>
<td>Bad Truncation</td>
<td>[RFC4635]</td>
</tr>
<tr>
<td>23-3840</td>
<td>Unassigned</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3841-4095</td>
<td>Reserved for Private Use</td>
<td></td>
<td>[RFC6195]</td>
</tr>
<tr>
<td>4096-65534</td>
<td>Unassigned</td>
<td></td>
<td></td>
</tr>
<tr>
<td>65535</td>
<td>Reserved</td>
<td>can be allocated by Standards Action</td>
<td>[RFC6195]</td>
</tr>
</tbody>
</table>
SERVFAIL

• Generic error for a recursive server
  – now with added DNSSEC flavours
  – any dnssec validation failure is exposed to
    the client as servfail

• on Authoritative servers the most common issue is the server having
  problem accessing the zone data
nslookup

- Been around for a long while in many OSs
- OK for casual use but better to use either of the other tools (DiG or drill)
  - doesn’t really report on what is trying to do
  - use host if all you want is a simple query utility
- General recommendation: DO NOT use for DNS debugging
DiG

• Produced and maintained by ISC as part of BIND 9
  – Very useful all-purpose, full control DNS query tool
  – Install it as part of BIND
  – Get it packaged
• e.g. dnsutils in Ubuntu or Debian
DiG: anatomy of a DNS query

$ dig bondis.org
; <<>> DiG 9.7.0 <<>> bondis.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20717
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
bondis.org. IN A

;; ANSWER SECTION:
bondis.org. 300 IN A 194.176.119.229

;; AUTHORITY SECTION:
bondis.org. 300 IN NS ns.bondis.org.
bondis.org. 300 IN NS borg.c-l-i.net.

;; ADDITIONAL SECTION:
ns.bondis.org. 300 IN A 194.176.119.229
borg.c-l-i.net. 300 IN A 192.16.192.99

;; Query time: 0 msec
;; SERVER: 204.61.225.99#53(204.61.225.99)
;; WHEN: Thu Jan 13 17:59:28 2011
;; MSG SIZE rcvd: 121
$ dig isc.org any +dnssec

; <<>> DiG 9.7.0 <<>> isc.org any +dnssec
;; global options: +cmd

; Got answer:

; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2794

; QUESTION SECTION:
.isc.org.       IN      ANY

; AUTHORITY SECTION:
.          8119    IN      NS      ams.sns-pb.isc.org.isc.org.        8119    IN      NS      ord.sns-pb.isc.org.isc.org.        8119    IN      NS      sfba.sns-pb.isc.org.isc.org.        8119    IN      NS      ns.isc.afilias-nst.info.isc.org.        43122   IN      RRSIG   NS 5 2 43200 20110207233212 20110108233212 26982 isc.org. mo82HW/2bEi4UekDGRd50xUN6Q85Q2llCxVZXJ7HkumyUTEZFzqpix/a CnBYjBvpvAW1rRr/4BTVj33e8tTRgKeV0bT5JG+HVirRAHBISKI+p3ed yNHjYb0PUsN5WD6efiZxGvkFAGWhZRUjSBEiWiIEFWIjjEvV/ywkuGLC uHo=

; ADDITIONAL SECTION:
ns.isc.afilias-nst.info. 721    IN      A       199.254.63.254                  ns.isc.afilias-nst.info. 721    IN      AAAA    2001:500:2c::
ams.sns-pb.isc.org.     6936    IN      A       199.6.1.30                  ams.sns-pb.isc.org.     6937    IN      AAAA    2001:500:60::30
ams.sns-pb.isc.org.     6936    IN      RRSIG   A 5 4 43200 20110207233212 20110108233212 26982 isc.org. aMa15HtsB3q+/Bk4RIO53Z1lhUaQcPH2YhxTMJvMdgAPkUoHOftvenpz G5VIYC +MICO3MJoRuko3N21B8iDvZuMz0pfV9LBBkN2Loy1PQ4enRcM2 dLZjcD4Ycf8OAY/VI/Wt8jUu7h8HeTfCn1U9P1luwFQAtL1K7K4X77Tk ntI=ams.sns-pb.isc.org.     6937    IN      RRSIG   AAAA 5 4 43200 20110207233212 20110108233212 26982 isc.org. DzPQSYGSv3d0I1owD7es9aMQVxB+fPF7xtTPV+vFIBDg27VFDH5C9sDi rpUgTaMTdenb4W1yZWEM8rzIeheibQKYnvAtTMjb40henmJEr/SUXKQK UH+VipzNVnW4f2PJlHBLopEYOVpiXHNV0ChEcrZwRvCWELVE+Yh6x6lS ycY=ord.sns-pb.isc.org.     6936    IN      RRSIG   A 5 4 43200 20110207233212 20110108233212 26982 isc.org. 11ootYvVO9GDfQHZfH6fMhazLCDQAFW+oy91qvihPQ6SQKTRUJv0yF5Q51Af7pqkIagWWnazf8tFmkPK0AxHJMLJUP2ROMFcqJ03e6wNe5NEM2yb PUH4d/kmt+xY5COnYmsq6Tptdb+rM5w43jHj83/ddqI9LQ48Sxq6WpGLtAQ=ord.sns-pb.isc.org.     6936    IN      RRSIG   AAAA 5 4 43200 20110207233212 20110108233212 26982 isc.org. TEe9uq22k1zAauhxfCPFaaggUkip5ltBVEDjRdAcDUiZenKAgsfeJwo1 JN2pkxW0aecawDjDnF2V2W2ekqEdN4C+9UBn76BAgczC0qoRWYBZGdi413+utDlDh/94I4H4BWNhbyxqa1GRphZoay0t1Gay8CdXbGjweS1S3/ob yoY=
DiG

• many options to completely control the query
  – Follow the DNS tree: +trace
  – Expanded format: +multiline
    • does more than the name tells
  – Concise: +short
    • includes only the ANSWER section
      – so if response has now ANSWER, you see nothing.
  – beware, some may be confusing
    • +[no]vc, +bufsize=nnn, +[no]ignore
Using DiG

- By default DiG issues recursive queries (rd bit is set).
  • Most auth servers will say recursion is not available

  $ dig @f.root-servers.net ; <<>> DiG 9.7.2-P3 <<>> @f.root-servers.net; (2 servers found);; global options: +cmd;; Got answer;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16477;; flags: qr aa rd; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 15;; WARNING: recursion requested but not available

  • Some may deny responding to the query.

  ;; Got answer;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 33598

  – Use +norecursion to turn off if you hit this
Using DiG

• check all nameservers for a zone
  +nssearch
DiG and DNSSEC

• Standard DiG will show DNSSEC info if you ask for it (+dnssec option)
• However, for debugging it is much more useful if you compile DiG with the SIGCHASE option
  
  ```
  STD_CDEFINES=-DDIG_SIGCHASE=1
  ```

• If you want to verify the signatures, you need to supply the key
  
  » obtain the root key from a trusted source if possible
  https://data.iana.org/root-anchors/
  or even http://dns.icann.org/ksk/ds19036/
drill

• Written and maintained by NLNet Labs
  – now a part of ldns, a generic DNS library
  – was developed originally with DNSSEC in mind
  – Very similar to DiG in functionality and output format.
  • Choose the one you like better
  – Install ldns or use packaging systems
  • FreeBSD ports
Using drill

• Control over use of EDNS/TCP
  • (-a and -b)

• Trace option attempts DNSSEC validation if it has access to a trust anchor
  – trust anchors can be specified as DNSKEY or as DS
  – e.g. drill -T -k $key
Drill and DiG

- Slightly different syntax respect to DiG

<table>
<thead>
<tr>
<th>Feature</th>
<th>Dig</th>
<th>drill</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNSSEC</td>
<td>+dnssec</td>
<td>-D</td>
</tr>
<tr>
<td>trace</td>
<td>+trace</td>
<td>-t</td>
</tr>
<tr>
<td>chase signatures</td>
<td>+sigchase (1)</td>
<td>-S</td>
</tr>
<tr>
<td>EDNS buf size</td>
<td>+bufsize=nnn</td>
<td>-b nnn</td>
</tr>
<tr>
<td>flags</td>
<td>each has an option</td>
<td>-o xx</td>
</tr>
<tr>
<td>reverse lookup(in-addr)</td>
<td>-x</td>
<td>-x</td>
</tr>
<tr>
<td>Use TCP</td>
<td>+tcp</td>
<td>-t</td>
</tr>
<tr>
<td>Use only UDP</td>
<td>+notcp</td>
<td>-u</td>
</tr>
</tbody>
</table>
drill and DiG - output

$ drill isc.org soa +dnssec; >>> Dig 9.7.2-P3 <<< isc.org soa +dnssec; global options: +cmd; Got answer: ;>

>>>HEADER<<<- opcode: QUERY, rcode: NOERROR, id: 22247; flags: qr rd ra ; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 6 ;; QUESTION SECTION: ;

isc.org.     IN      SOA     ns-int.isc.org. hostmaster.isc.org. 2011010900 7200 3600 24796800 3600; 

$ dig isc.org soa  +dnssec; <<>> DiG 9.7.2-P3 <<>> isc.org soa +dnssec; global options: +cmd; Got answer: ;>

>>>HEADER<<<- opcode: QUERY, rcode: NOERROR, id: 43855; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 6 ;; QUESTION SECTION: ;

isc.org.                42939   IN      SOA     ns-int.isc.org. hostmaster.isc.org. 2011010900 7200 3600 24796800 3600;
Zone verification

• Local tools
  – named-checkzone

• Network services
  – zonecheck.fr
  – dnscheck.iis.se
named-checkzone

• part of BIND
• checks zone file for correctness
• best practice: always run a verification script before loading a zone on a live server
  – can be done off-line, without the server
  – prevents silly mistakes
  – may detect bugs in generation process
• output can be rather verbose
  – tune options to report only errors you care about (e.g. specific glue check types)
named-checkzone: example #1

- $TTL 1H
  $ORIGIN example.org.
  example.org. SOA master hostmaster.example.org. (2012031301 ; serial
  3600 ; refresh (1 hour)
  1800 ; retry (30 minutes)
  864000 ; expire (1 week 3 days)
  600 ; negative TTL (10 minutes)
  )
  
  NS ns1
  NS ns2
  MX 100 smtp
  AAAA 2001:DB8::2
  
  ns1 AAAA 2001:DB8::1
  ns2 AAAA 2001:DB8:8000::1
  smtp AAAA 2001:DB8::2
  www CNAME main
  main AAAA 2001:DB8::2
named-checkzone: example #1

• Execution can be straightforward:
  • $ /usr/sbin/named-checkzone \ 
    > example.org example.org.zone 
  zone example.org/IN: loaded serial 2012031301 
  OK
named-checkzone: example #2

Replace:
  smtp AAAA 2001:DB8::2
With:
  smtp CNAME main

We then see:
  'smtp.example.org' is a CNAME (illegal)

Warning can be disabled by “-M ignore”.
named-checkzone: example #3

• Add:
  • subdomain NS ns1.subdomain
    NS ns2.subdomain
    ns1.subdomain AAAA 2001:DB8::3

• We then see:
  • 'ns1.subdomain.example.org' (out of zone)
    has no addresses records (A or AAAA)
  • 'ns2.subdomain.example.org' has no
    REQUIRED GLUE address records (A or AAAA)
  • 'ns2.subdomain.example.org' (out of zone)
    has no addresses records (A or AAAA)

• Warning can be disabled by “-i local”, but error should remain.
named-checkzone: limitations

• cannot check for some errors
  – forgetting to increment SOA serial number
  – zone truncation
  – typos in out-of-zone names
  – missing or extra '.' at end of names

• does not check for some errors
  – DNSSEC: missing signatures, other errors
  – fully vs. partially lame glue issues
zonecheck.fr

• Developed and maintained by AFNIC (.fr registry)
• Available as
  – online service
  – download
• Online is good for casual use
• Download and install for more control and accessibility
zonecheck.fr

• Local installation can be a bit tedious but offers possibility of tailoring verification policies to registry policies.
• Available as command line tool or local web installation
The ZoneCheck program (freely available [here](#) for download) performs several tests on your zone (i.e., domain) to ensure that it is correct, providing a certain quality to your domain (see the [benefits](#) section).

For detailed information on how to fill this form see the [help](#) section.

### Zone Information

<table>
<thead>
<tr>
<th>Zone</th>
<th>Primary</th>
<th>IPs</th>
<th>Secondary</th>
<th>IPs</th>
<th>Secondary</th>
<th>IPs</th>
<th>Secondary</th>
<th>IPs</th>
<th>Secondary</th>
<th>IPs</th>
<th>Secondary</th>
<th>IPs</th>
<th>Secondary</th>
<th>IPs</th>
<th>Secondary</th>
<th>IPs</th>
</tr>
</thead>
</table>

The time required to completely verify a zone can take from 30 seconds up to 5 minutes depending on the network speed; it generally means we are encountering problems accessing your nameservers (configuration, timeout).

### Options

- **Output**
  - zone summary
  - test name
  - progress bar
  - by severity
  - report format

- **Details**
  - explanations
  - descriptions
  - details
  - nothing
dnscheck.iis.se

• Developed and maintained by IIS (.se registry)
  – Simple and well structured
  – can take some time to go through tests
Instant analysis

• Ready made
  – dnstop

• Toolkits
  – wireshark/tcpdump/libpcap
  – dnscap

• Other
  – DNS-OARC DNS Reply Size Test Server

• Passive DNS
  – ISC SIE, dnslogger
dnstop

• Like top, but for dns queries instead of processes
  – Written by the Measurement Factory

• Download from

<table>
<thead>
<tr>
<th>Sources</th>
<th>Count</th>
<th>%</th>
<th>cum%</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.0.32.242</td>
<td>18</td>
<td>34.6</td>
<td>34.6</td>
</tr>
<tr>
<td>204.152.187.13</td>
<td>11</td>
<td>21.2</td>
<td>55.8</td>
</tr>
<tr>
<td>192.0.36.240</td>
<td>10</td>
<td>19.2</td>
<td>75.0</td>
</tr>
<tr>
<td>204.152.187.14</td>
<td>6</td>
<td>11.5</td>
<td>86.5</td>
</tr>
<tr>
<td>149.20.54.152</td>
<td>4</td>
<td>7.7</td>
<td>94.2</td>
</tr>
<tr>
<td>87.217.89.178</td>
<td>2</td>
<td>3.8</td>
<td>98.1</td>
</tr>
<tr>
<td>204.8.46.130</td>
<td>1</td>
<td>1.9</td>
<td>100.0</td>
</tr>
</tbody>
</table>
dnstop

• Can use standard bpf rules to filter traffic, so you can monitor what you want

• Some common options
  – ignore specific servers (e.g. your own resolvers)
  – ignore specific domains

• May require root or have setuid set to access the interface to capture traffic.
Toolkits

• libpcap/tcpdump/wireshark
  – build your own tools with libpcap
  – use ad-hoc filters
    • example...
  – wireshark is quite good in deciphering packets, including DNS
  – Sometimes too overblown for the job
dnscap

Main features
- Focused on DNS
- Understands both IPv4 and IPv6
- Captures UDP, TCP, and IP fragments.
- Collect only queries, responses, or both
- Collect for only certain source/destination addresses
- Periodically creates new pcap files (-t option)
- Spawns an upload script after closing a pcap file
- Will start and stop collecting at specific times

• Download from https://www.dns-oarc.net/tools/dnscap
dnscap

• Examples of usage....
  – dnscap -i en0 -g (output dig format if using libbind)

• capture file management
  – k executes external command (e.g. gzip)
  – w write files (and specify a basename)
    • the basename gets a timestamp appended
    • the file is in pcap format but reassembly has been done
  – t time limit, to rotate files (also possible based on size)
dnscap

• -x use regular expressions to filter packets
ncap

• pcap substitute
  - performs IP reassembly and generates framing-independent portable output
  - writes output in ncap format
  - can be augmented with modules/plugins to perform specific analysis
Passive DNS

• Collect DNS information as it enters or leaves a nameserver
  – no active DNS role
  – specialised data capture, with tools focused on DNS

• dnslogger

• ISC SIE
libnmsg/dnsqr

- libnmsg implements a generic message format to carry many types of streaming data
- dnsqr is a module for libnmsg designed for Passive DNS capture
- capture, optionally with filters and encapsulates it in nmsg format
- does packet reassembly and can track “flows”
Long term analysis

• Run your own
  – DSC
  – DNS2DB

• Network based services
  – RIPE DNSMON
DSC

- DNS Statistics collector
  - can be tricky to get right
  - does a real good job of collecting and presenting ongoing statistics for your DNS
  - based on packet captures at the servers
    - easy if you run your own servers
  - developed originally by the Measurement Factory for OARC, now maintained by OARC
  - Available as free download
DSC

• Can be used on the DNS servers themselves, using pcap capture
• If load is a concern, capture traffic using a passive tap
• If measuring more than 30-40 nodes, use some logical grouping for processing in multiple servers and merge the results
DNS2DB

• Produced and maintained by IIS (.se)
• Converts raw pcap-files with DNS-traffic to SQLite-databases.
  – Includes basic GUI to look at data.
• Needs libtrace from Waikato University
• Uses Adobe flex to run the front end
DNS2DB

Instructions:
- The first window displays the top 20 domains and servers. The server list 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 resolving for that domain. Double-click on a server to open a window with a list of hosts for that server.
- If you click on a query you will get the servers solving for that domain. A single-click on a row copies the contract to the clipboard.
- When a row is selected in a window you can use the left and right arrows to change the time five minutes. Holding down SHIFT moves hours, holding down CTRL moves days.
- You can search for a domain or server by typing in a text in the text box. You can also change the number of lines that are displayed by selecting another value in the drop-down box.
- You can close a window by clicking on the cross in the top right corner. Double-click on the title bar to hide temporarily or drag them to move them around.
RIPE DNSMON

• Online service available at: http://dnsmon.ripe.net/dns-servmon/

• Shows measurements of DNS servers
  – uses same platform as RIPE Test Traffic

• Data is available with a slight delay
  – Avoids silly usage
  – Immediate data available for subscribers

• Need to learn how to read the graphics
DNSMON: Overview of Domains
DNSMON: Per-Domain View
DNSMON: Per-Server View
RIPE DNSMON: Raw Data

Available via FTP, for example:

+--------------------------------- "DNS"
|                                +------------------------------- test-traffic host originating probe
|                                |                                +------------------------ Unix epoch timestamp of probe
|                                |                                |                                +-- target name server
DNS tt07.ripe.net 1334016000 john.vatican.va 0.000000 3 62083 hostname.bind UNREACH
DNS tt07.ripe.net 1334016000 b.gtld-servers.net 0.001658 1 62111 hostname.bind UNKNOWN
DNS tt07.ripe.net 1334016000 d.nic.at 0.000000 3 62087 id.server UNREACH
DNS tt07.ripe.net 1334016000 f.nic.de 0.000000 3 62085 id.server UNREACH
DNS tt07.ripe.net 1334016000 osiris.namex.it 0.060790 1 62115 hostname.bind osiris.namex.
DNS tt07.ripe.net 1334016001 y.nic.eu 0.001118 1 62121 hostname.bind s2.sth
DNS tt07.ripe.net 1334016001 ns5.dns.net.nz 0.033904 1 62120 id.server
DNS tt07.ripe.net 1334016001 b.ip6-servers.arpa 0.111574 1 62119 id.server inaddr.cjr.dns
DNS tt07.ripe.net 1334016001 a.nic.cl 0.244393 1 62116 id.server merced.nic.cl

  response time ---+  |  attempts ------+  |  port number ----------+  |  query name -----------------+  |  response (answer or error message) ------------------------------------------+
Other useful tools

- **fpdns**
  - fingerprint DNS servers
  - Needs some refresh but is still useful for debugging
    - work ongoing - Verisign+kirei
  - Send various packets to servers and profiles them according to tables of observed behaviour

  ```
  $ fpdns cumin.apnic.net.
  fingerprint (cumin.apnic.net., 202.12.29.59): Nominum ANS
  $ fpdns cumin.apnic.net.
  fingerprint (a.root-servers.net, 198.41.0.4): VeriSign ATLAS
  ```
References

- dig - http://www.isc.org/software/bind
- drill - http://www.nlnetlabs.nl/projects/ldns/
- named-checkzone - http://www.isc.org/software/bind
- zonecheck.fr - http://www.zonecheck.fr/
- dnscheck - http://dnscheck.iis.se/
- https://github.com/dotse/dnscheck
- dnstop - http://dns.measurement-factory.com/tools/dnstop/
- dnslogger - http://www.enyo.de/fw/software/dnslogger/
- dnscap - Download from https://www.dns-oarc.net/tools/dnscap
- DSC - https://www.dns-oarc.net/tools/dsc
- dns2db - https://github.com/dotse/dns2db
- RIPE DNSMON - http://dnsmon.ripe.net/dns-servmon/
- FPDNS - https://github.com/kirei/fpdns
Questions?

joao@isc.org
shane@isc.org