DNS Debugging and monitoring

João Damas
Outline

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

• nslookup
• DiG
• drill
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

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20717
;; flags: qr aa rd ra

;; 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
;; flags: qr rd ra; QUERY: 1, ANSWER: 10, AUTHORITY: 5, ADDITIONAL: 11
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;isc.org. IN ANY
 ;; ANSWER SECTION:

isc.org. 43122 IN RRSIG A 5 2 43200 20110207233212 20110108233212 26982 isc.org. oGQRMM +BQOYtqHBUG0pwwhmNKixY49ncQPw9UjrIKpEYHoZpSZhvLGRX QgtKuUQi5dOBOR8QeAoQ9IoV0tuSNmlEk+Ft2EFvouD8WPgPlpc7Y86R o/va0NjpYtIbranjm6B/Dv9Wc0v1Yv/eFFxL+AJ8F2e4UnVXxMOP7dPo BDM=

isc.org. 43122 IN A 149.20.64.42

isc.org. 8119 IN NS ams.sns-pb.isc.org.

isc.org. 8119 IN NS ns.isc.afilias-nst.info.

isc.org. 8119 IN NS ord.sns-pb.isc.org.

isc.org. 8119 IN NS sfba.sns-pb.isc.org.

isc.org. 43122 IN RRSIG NS 5 2 43200 20110207233212 20110108233212 26982 isc.org. mo82HW/2bEi4UekDGRd50xUN6Q85Q2lCvVXJ7HkumyUTEZFzqpix/a CnBYjByvpAW1rRr/4BTvJ33e8tTRgKeV0bT5JG+HVrRAHBISKI+p3ed yNHjYb0PU65NWD6efiZxGvkFAGWhZRUjSBElWIIEFWljEvV/ywkuGLC uHo=

isc.org. 51319 IN RRSIG DS 7 2 86400 20110123165115 20110109155115 1743 org. N3g2hkYL+cuSmNBT16sGz1WonF4esYR3awgSVScbWnND8uZTse9G6q14 +8b81zuXcqVSCJuWoRuOVkJ8aE28qPzx8S+SVEw5Gm+gXk4xJuIkW5J c6rlivi7copPuN9KhS2Rbs8aq4SutAG3STRug8OnlineAXxt/PTBDZ84i Kt4=

isc.org. 51319 IN DS 12892 5 2 F1E184C0E1D615D20EB3C223ACED3B03C773DD952D50EB5C777586D E18DA6B5

isc.org. 51319 IN DS 12892 5 1 982113D08B4C6A1D9F6AEE1E2237A6F69F3F9759
;; AUTHORITY SECTION:
isc.org. 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/2bEi4UekDGRd50xUN6Q85Q2lICxVZxJ7HkumyUTEZFzqpix/a CnBYjBvpvAW1rRr/4BTvJ33e8tTRgKeV0bT5JG+HVrRAHBISKI+p3ed yNHjYb0PUeN5WD6efiZxGvkFAGWhZRUjSBEiWiEFWljjEvV/ywkuGLC uH0=
;; 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::254
ams.sns-pb.isc.org. 6936 IN A 199.6.1.30
ams.sns-pb.isc.org. 6937 IN AAAA 2001:500:60::30
ord.sns-pb.isc.org. 6936 IN A 199.6.0.30
ord.sns-pb.isc.org. 6936 IN AAAA 2001:500:71::30
ams.sns-pb.isc.org. 6936 IN RRSIG A 5 4 3200 20110207233212 20110108233212 26982 isc.org. aMa15HtsB3q+/Bk4RIO53Z1lhUaQcPH2YhxTMJvMdgAPkUoH0ftvenpz G5VIYC+MICO3MJoRuko3N21B8iDvZuMz0pfV9LBBkN2Loy1PQ4enRcM2 dLZjcD4Ycf8OAY/VI/Wt8jUU7h8HeTfCn1U9P1lwFQAtl1K7K4X77TkJntI=
ams.sns-pb.isc.org. 6937 IN RRSIG AAAA 5 4 3200 20110207233212 20110108233212 26982 isc.org. DzPQSYGSv3d011owD7es9aMQVxxB+fPF7xtTPV+vF18Bdg27VFDH5C9sDi rpUgTaMTdenb4W1yZWEM8rzIeheibQKYnvAtTMjb40henmJEr/SUXKQK UH+VIpzNVnW4f2PJHBLopEYOViXHNV0ChEcrZwRvCWELVE+Yh6x6lS ycY=
ord.sns-pb.isc.org. 6936 IN RRSIG A 5 4 3200 20110207233212 20110108233212 26982 isc.org. 11ootYvVO9GDfQHZfH6fHzazLCDQAFW+oy91qvihPQ6SQKTRUJv0yF5Q 51Af7pqklagWWnazf8tFmkPK0AxHJMLJUP2ROMFcqJ03e6wNe5NEM2yb PUH4d/kmt+xY5CoNYmsq6Tptdb+rM5w43jHj83/ddqI9LQ48Sxq6WpGL tAQ=
ord.sns-pb.isc.org. 6936 IN RRSIG AAAA 5 4 3200 20110207233212 20110108233212 26982 isc.org. TEe9uq22k1z1AauhxfCPFaaaglUkip5ltBVEDjRdAcDuZenKAgsef3wo1 JN2pkkxW0aecawDjDnF2V2W2ekqEdN4C+9UBn76BAgczC0qoRWWBZGdi4 13+utDIrh/94I4H4BWNhbyxqa1GRphZoay0t1Gay8CdXbGjweS1S3/ob yoY=
;; Query time: 1 msec
;; SERVER: 204.62.249.35#53(204.62.249.35)
;; WHEN: Thu Jan 13 21:42:00 2011
;; MSG SIZE  rcvd: 1755
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 +norecurse 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
  
  ```bash
  STD_CDEFINES='-DDIG_SIGCHASE=1' ./configure
  ```

- 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
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>

(1) Must be explicitly compiled in
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: 43855
        flags: qr rd ra ; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 7

        OPT PSEUDOSECTION:
        EDNS: version: 0, flags: do ; udp: 4096

        QUESTION SECTION:
        isc.org. IN SOA

        ANSWER SECTION:
        isc.org. 42939 IN SOA ns-int.isc.org. hostmaster.isc.org. 2011010900 7200 3600 24796800 3600
        isc.org. 42939 IN RRSIG SOA 5 2 43200 20110207233212 20110108233212 26982
        isc.org. 366 IN NS ns.isc.afilias-nst.info.
        isc.org. 42983 IN RRSIG NS 5 2 43200 20110207233212 20110108233212 26982

        ADDITIONAL SECTION:
        ns.isc.afilias-nst.info. 36569 IN A 199.254.63.254
        ns.isc.afilias-nst.info. 36569 IN AAAA 2001:500:2c::254
        sfba.sns-pb.isc.org. 42393 IN A 199.254.63.254
        sfba.sns-pb.isc.org. 42393 IN AAAA 2001:500:2c::254
        sfba.sns-pb.isc.org. 42383 IN A 149.20.64.3
        sfba.sns-pb.isc.org. 42383 IN AAAA 2001:48:0:2::19
        sfba.sns-pb.isc.org. 42383 IN RRSIG A 5 4 43200 20110207233212 20110108233212 26982
        sfba.sns-pb.isc.org. 42383 IN RRSIG A 5 4 43200 20110207233212 20110108233212 26982
        sfba.sns-pb.isc.org. 42383 IN RRSIG A 5 4 43200 20110207233212 20110108233212 26982
        sfba.sns-pb.isc.org. 42383 IN RRSIG A 5 4 43200 20110207233212 20110108233212 26982
        sfba.sns-pb.isc.org. 42383 IN RRSIG A 5 4 43200 20110207233212 20110108233212 26982

$ 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: 22247
        flags: qr rd ra ; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 6

        QUESTION SECTION:
        isc.org. IN SOA

        ANSWER SECTION:
        isc.org. 22247 IN SOA ns-int.isc.org. hostmaster.isc.org. 2011010900 7200 3600 24796800 3600
        isc.org. 22247 IN RRSIG SOA 5 2 43200 20110207233212 20110108233212 26982

        AUTHORITY SECTION:
        isc.org. 356 IN NS ns.isc.afilias-nst.info.

        ADDITIONAL SECTION:
        ns.isc.afilias-nst.info. 36559 IN A 199.254.63.254
        ns.isc.afilias-nst.info. 36559 IN AAAA 2001:500:2c::254
        sfba.sns-pb.isc.org. 42382 IN A 149.20.64.3
        sfba.sns-pb.isc.org. 42382 IN AAAA 2001:48:0:2::19

$ drill -D isc.org soa
; ->>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

; ANSWER SECTION:
; isc.org. 22247 IN SOA ns-int.isc.org. hostmaster.isc.org. 2011010900 7200 3600 24796800 3600
; isc.org. 22247 IN RRSIG SOA 5 2 43200 20110207233212 20110108233212 26982

; AUTHORITY SECTION:
; isc.org. 356 IN NS sfba.sns-pb.isc.org.
; isc.org. 356 IN NS ns.isc.afilias-nst.info.
; isc.org. 356 IN NS ord.sn-spb.isc.org.

; ADDITIONAL SECTION:
; ns.isc.afilias-nst.info. 36569 IN A 199.254.63.254
; ns.isc.afilias-nst.info. 36569 IN AAAA 2001:500:2c::254
; sfba.sns-pb.isc.org. 42383 IN A 149.20.64.3
; sfba.sns-pb.isc.org. 42382 IN AAAA 2001:48:0:2::19

Monday, 7 March 2011
Zone verification

• Local tools
  – named-checkzone

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

• Part of bind
  – checks zone contents from a file in a disk
  – Good practice to always run a verification script before loading the zone on the server
    • can be done off-line, without loading the server
    • prevents silly mistakes, may detect bugs in generation process
  – can be rather verbose
    • tune options to report only errors you care about (e.g. types of glue)
named-checkzone

• options to control what MX Records are acceptable (e.g. addresses or CNAME)
• Tricky part are the glue checks
  – sibling glue, local checks, full checks

otherexample.xx NS ns3.example.xx
otherexample.xx NS ns4.example.xx

example.xx NS ns1.otherexample.xx
example.xx NS ns2.otherexample.xx
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
• 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
Zone information

| Zone | Primary |  | IPs |  | Secondary |  | IPs |  | Secondary |  | IPs |  | Secondary |  | IPs |  | Secondary |  | IPs |  | Secondary |  | IPs |  | Secondary |  | IPs |  | Secondary |  
|------|---------|---|-----|---|-----------|---|-----|---|-----------|---|-----|---|-----------|---|-----|---|-----------|---|-----|---|-----------|---|-----|---|-----------|---|-----|---|

Options

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

The ZoneCheck program (freely available [here](#) for download) performs several tests on your zone (ie: domain) to ensure that it is correct providing a certain quality to your domain (see the benefit section).

For detailed information on how to fill this form see the help section.

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

• 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
  - [http://dns.measurement-factory.com/tools/dnstop/source.html](http://dns.measurement-factory.com/tools/dnstop/source.html)

Queries: 0 new, 52 total
Sun Jan 16 15:10:03 2011

<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

- 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
dnslogger

- Can be used to reconstruct a zone from observed DNS messages in a network
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 asking for that domain. Double-click on a server to open a window with a list of 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 five minutes. Holding down SHIFT moves hours; holding down CTRL moves days.
- 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 window 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.
RIPE DNSMON

• Online service available at
  – http://dnsmon.ripe.net/dns-servmon/
• Shows measurements of DNS servers from selected sites (uses same platform as RIPE Test Traffic)
• Data is available with a slight delay to avoid silly usage.
• Need to get used to read the graphics
RIPE DNSMON

Domain Overview for jp . (ipv4) Click on a plot to show it full size.

Last 24 Hours
Other useful tools

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

```bash
$ 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 - http://code.google.com/p/fpdns/
Questions?

joao@isc.org