Troubleshooting DNSSEC

a few handles to get you started

NLnet Labs

Toolbag

- dig
- drill
- unbound-host
- Packet analysis
  - wireshark
  - tcpdump
  - dnscap (in combination with the above)

NLnet Labs

Try to understand the wire

- A DNS Packet has a header and 4 sections:
  - Question
  - Answer
  - Authoritative
  - Additional

HEADER

ID															
QDCOUNT															
ANCOUNT															
NSCOUNT															
ARCOUNT															

NLnet Labs

Header

FLAGS

RCODE

Query (0)
Response (1)

Opcode

Flag	Description
AA	Authoritative Answer
TC	Truncated Response
RD	Recursion Desired
RA	Recursion Allowed
	Reserved
AD	Authentic Data
CD	Checking Disabled

Hexadecimal	Name	Description
0	NoError	No Error
1	FormErr	Format Error
2	ServFail	Server Failure
3	NXDomain	Non-Existent Domain
4	NotImp	Not Implemented
5	Refused	Query Refused
6	YXDomain	Name Exists when it should not
7	YXRRSet	RR Set Exists when it should not
8	NXRRSet	RR Set that should exist does not
9	NotAuth	Server Not Authoritative for zone
10	NotZone	Name not contained in zone
11-15	Unassigned	

0	Query	[RFC1035]
1	IQuery (Inverse Query, Obsolete)	[RFC3425]
2	Status	[RFC1035]
3	Unassigned	
4	Notify	[RFC1996]
5	Update	[RFC2136]
6-15	Unassigned	

NLnet Labs

```
; <<>> DiG 9.7.0b2 <<>> @a0.org.afilias-nst.info. org NS +dnssec
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49574
;; flags: qr aa rd; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 13
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;org.                    IN NS

;; ANSWER SECTION:
org.                 86400 IN NS b0.org.afilias-nst.org.
org.                 86400 IN NS d0.org.afilias-nst.org.
org.                 86400 IN NS a0.org.afilias-nst.info.
org.                 86400 IN NS a2.org.afilias-nst.info.
org.                 86400 IN NS b2.org.afilias-nst.org.
org.                 86400 IN NS c0.org.afilias-nst.info.
org.                 86400 IN RRSIG NS 7 1 86400 20100415154437 (
                             20100401144437 47948 org.
                             BSO2Encp2iwdCtge[illegible]
                             gGIpy7HRamerEg7fQ+PWvxr3F0k/zTUdFifRi1paOHbG
                             MRfvOG9XHskSxoUqxwi2jRAIXWYmXz3A/NsjgoJVsIEj
                             3DWGP43cTJMoOsS68qmK7CbbyLrSTRdg6/d/mK4= )

;; ADDITIONAL SECTION:
a0.org.afilias-nst.info. 86400 IN A 199.19.56.1
a0.org.afilias-nst.info. 86400 IN AAAA 2001:500:e::1
a2.org.afilias-nst.info. 86400 IN A 199.249.112.1
a2.org.afilias-nst.info. 86400 IN AAAA 2001:500:40::1
b0.org.afilias-nst.org. 86400 IN A 199.19.54.1
b0.org.afilias-nst.org. 86400 IN AAAA 2001:500:c::1
b2.org.afilias-nst.org. 86400 IN A 199.249.120.1
b2.org.afilias-nst.org. 86400 IN AAAA 2001:500:48::1
c0.org.afilias-nst.info. 86400 IN A 199.19.53.1
c0.org.afilias-nst.info. 86400 IN AAAA 2001:500:b::1
d0.org.afilias-nst.org. 86400 IN A 199.19.57.1
d0.org.afilias-nst.org. 86400 IN AAAA 2001:500:f::1

;; Query time: 409 msec
;; SERVER: 2001:500:e::1#53(2001:500:e::1)
;; WHEN: Thu Apr  8 08:44:33 2010
;; MSG SIZE  rcvd: 597
```

Request DNS information

Question to Authoritative Nameserver

Question Section

Answer Section

Authority Section

NLnet Labs

```
203 26.001005   213.154.224.48   194.85.252.62   DNS   Standard query A ns.majordomo.ru
```

```
▷ Frame 203 (86 bytes on wire, 86 bytes captured)
▷ Ethernet II, Src: 3com_bc:24:1b (00:10:4b:bc:24:1b), Dst: PcEngine_15:9a:d4 (00:0d:b9:15:9a:d4)
▷ Internet Protocol, Src: 213.154.224.48 (213.154.224.48), Dst: 194.85.252.62 (194.85.252.62)
▷ User Datagram Protocol, Src Port: 50285 (50285), Dst Port: domain (53)
▽ Domain Name System (query)
    [Response In: 204]
    Transaction ID: 0x9a3a
  ▽ Flags: 0x0010 (Standard query)
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...0 .... .... = Recursion desired: Don't do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...1 .... = Non-authenticated data OK: Non-authenticated data is acceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▽ Queries
    ▷ ns.majordomo.ru: type A, class IN
  ▽ Additional records
    ▽ <Root>: type OPT
        Name: <Root>
        Type: OPT (EDNS0 option)
        UDP payload size: 4096
        Higher bits in extended RCODE: 0x0
        EDNS0 version: 0
      ▽ Z: 0x8000
          Bit 0 (DO bit): 1 (Accepts DNSSEC security RRs)
          Bits 1-15: 0x0 (reserved)
        Data length: 0
```

OPT RR: EDNS

```
0000  00 0d b9 15 9a d4 00 10  4b bc 24 1b 08 00 45 00   ........ K.$...E.
0010  00 48 f2 cd 00 00 40 11  13 78 d5 9a e0 30 c2 55   .H....@. .x...0.U
```

EDNS

- Communicate ability to deal with 512+ IP packets (fragmentation buffers)
- Communicate willingness to receive DNSSEC resource records
  - Space for much more resource

NLnet Labs

Deeper Understanding?

- http://www.iana.org/assignments/dns-parameters
- follow the links to to the RFCs

NLnet Labs

What Can Go Wrong

Possible Failures

- Local Configuration
- Secure Delegation Failure
- True validation failure
- Transport problems

NLnet Labs

Local Configuration

- Time:
  DNSSEC is critically dependent on time.
  Check your NTP configuration
- use **`date -u "+%Y%m%d%H%M%S"`**
- Check signature validity times

NLnet Labs

```
; <<>> DiG 9.7.0b2 <<>> @a0.org.afilias-nst.info. org NS +dnssec
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49574
;; flags: qr aa rd; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 13
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;org.                    IN NS

;; ANSWER SECTION:
org.                    86400 IN NS b0.org.afilias-nst.org.
org.                    86400 IN NS d0.org.afilias-nst.org.
org.                    86400 IN NS a0.org.afilias-nst.info.
org.                    86400 IN NS a2.org.afilias-nst.info.
org.                    86400 IN NS b2.org.afilias-nst.org.
org.                    86400 IN NS c0.org.afilias-nst.info.
org.                    86400 IN RRSIG NS 7 1 86400 20100415154437 (
                              20100401144437 47948 org.
                              BSO2Encp2iwdCtgeKXCyi0PsVZFU8ai1zInCveqPxBuW
                              gGIpy7HRamerEg7fQ+PWvxr3F0k/zTUdFifRi1paOHbG
                              MRfvOG9XHskSxoUqxwi2jRAIXWYmXz3A/NsjgoJVsIEj
                              3DWGP43cTJMoOsS68qmK7CbbyLrSTRdg6/d/mK4= )

;; ADDITIONAL SECTION:
a0.org.afilias-nst.info. 86400 IN A 199.19.56.1
a0.org.afilias-nst.info. 86400 IN AAAA 2001:500:e::1
a2.org.afilias-nst.info. 86400 IN A 199.249.112.1
a2.org.afilias-nst.info. 86400 IN AAAA 2001:500:40::1
b0.org.afilias-nst.org. 86400 IN A 199.19.54.1
b0.org.afilias-nst.org. 86400 IN AAAA 2001:500:c::1
b2.org.afilias-nst.org. 86400 IN A 199.249.120.1
b2.org.afilias-nst.org. 86400 IN AAAA 2001:500:48::1
c0.org.afilias-nst.info. 86400 IN A 199.19.53.1
c0.org.afilias-nst.info. 86400 IN AAAA 2001:500:b::1
d0.org.afilias-nst.org. 86400 IN A 199.19.57.1
d0.org.afilias-nst.org. 86400 IN AAAA 2001:500:f::1

;; Query time: 409 msec
;; SERVER: 2001:500:e::1#53(2001:500:e::1)
;; WHEN: Thu Apr  8 08:44:33 2010
;; MSG SIZE  rcvd: 597
```

against authoritative server

SIGNATURE validity

```
$ date -u "+%Y%m%d%H%M%S"
20100408095947
```

NLnet Labs

Secure delegations

- Secure delegations: Look for the DS
  - Matching Key IDs?
  - NSEC proof?
  - Hard to do manually

Looking at the chain of trust

- CLI based
  - drill -T or drill -S (trace or chace)
  - dig +sigchace
- Web Based
  - dnsviz: http://dnsviz.net/
  - debugger: http://dnssec-debugger.verisignlabs.com/

NLnet Labs

drill -S

```
;; Chasing: example.net. SOA


DNSSEC Trust tree:
example.net. (SOA)
|---example.net. (DNSKEY keytag: 17000)
    |---example.net. (DNSKEY keytag: 49656)
    |---example.net. (DS keytag: 49656)
        |---net. (DNSKEY keytag: 62972)
            |---net. (DNSKEY keytag: 13467)
            |---net. (DS keytag: 13467)
                |---. (DNSKEY keytag: 63380)
                    |---. (DNSKEY keytag: 63276)
;; Chase successful
```

NLnet Labs

drill -T

drill -T -k < root.ksk > example.net SOA

```
;; Domain: .
[T] . 100 IN DNSKEY 256 3 5 ;{id = 63380 (zsk), size = 1024b}
. 100 IN DNSKEY 257 3 5 ;{id = 63276 (ksk), size = 1280b}
Checking if signing key is trusted:
New key: .      100     IN      DNSKEY  256 3 5 AQPQyahTOOaR/Pi6p ... Q== ;{id = 63380 (zsk), size = 1024b}
        Trusted key: .  3600    IN      DNSKEY  257 3 5 AQOv6tbkmW+ ... 1iY/ ;{id = 63276 (ksk), size = 1280b}
        Trusted key: .  100     IN      DNSKEY  256 3 5 AQPQyahTOOaR/ ... MiBmsMQ== ;{id = 63380 (zsk), size = 1024b}
Key is now trusted!
        Trusted key: .  100     IN      DNSKEY  257 3 5 AQOv6tbkmW+1 ... 1iY/ ;{id = 63276 (ksk), size = 1280b}
[T] net. 100 IN DS 13467 5 2 ec9b094786b82c46aa3054c7352b59904b697119d515b4ea536ec3dd9a10ed81
net. 100 IN DS 13467 5 1 de01426e08ddb9186502ccc1081390cd7da0e178
;; Domain: net.
[T] net. 100 IN DNSKEY 256 3 5 ;{id = 62972 (zsk), size = 1024b}
net. 100 IN DNSKEY 257 3 5 ;{id = 13467 (ksk), size = 1280b}
Checking if signing key is trusted:
New key: net.   100     IN      DNSKEY  256 3 5 AQPVP6Je ... 8h3J3Gw== ;{id = 62972 (zsk), size = 1024b}
        Trusted key: .  3600    IN      DNSKEY  257 3 5 AQOv6tbkmW+ ...  1iY/ ;{id = 63276 (ksk), size = 1280b}
        Trusted key: .  100     IN      DNSKEY  256 3 5 AQPQyahT ... msMQ== ;{id = 63380 (zsk), size = 1024b}
        Trusted key: .  100     IN      DNSKEY  257 3 5 AQOv6tbkmW ... oewi1iY/ ;{id = 63276 (ksk), size = 1280b}
        Trusted key: net.       100     IN      DNSKEY  256 3 5 AQPVP6 ... 3J3Gw== ;{id = 62972 (zsk), size = 1024b}
Key is now trusted!
        Trusted key: net.       100     IN      DNSKEY  257 3 5 AQOsAH77.... QuH ;{id = 13467 (ksk), size = 1280b}
[T] example.net. 100 IN DS 49656 5 1 3850efb913aec66275bca53221587d445702397e
example.net. 100 IN DS 49656 5 2 9e06b299abe811d699e077fff990ff5a1b496c914deb22697ba22a1da31f0a6e
;; Domain: example.net.
[T] example.net. 100 IN DNSKEY 256 3 5 ;{id = 17000 (zsk), size = 1024b}
example.net. 100 IN DNSKEY 257 3 5 ;{id = 49656 (ksk), size = 1280b}
[T] example.net.        100     IN      SOA     ns.example.net. olaf.nlnetlabs.nl. 2002050501 100 200 604800 100
;;[S] self sig OK; [B] bogus; [T] trusted
```

NLnet Labs

External views

- DNSVIZ: http://dnsviz.net/
- Verisign's DNSSEC Debugger: http://dnssec-debugger.verisignlabs.com/
- Secspider: http://secspider.cs.ucla.edu/

NLnet Labs

Sandia National Laboratories

DNSViz Home » bert.secret-wg.org

DNSViz

Go to domain name... Go »

A DNS visualization tool

bert.secret-wg.org
(Updated: Wed, 7 Apr 2010 12:54:05 -0700. Update now)

DNSSEC | Servers | Analyze

— DNSSEC options (show) —

Notices

Domain names

Untrusted (2)

DNSKEY/DS RRs

Trusted (7)

Untrusted (6)

Delegation status

Secure (1)

Insecure (2)

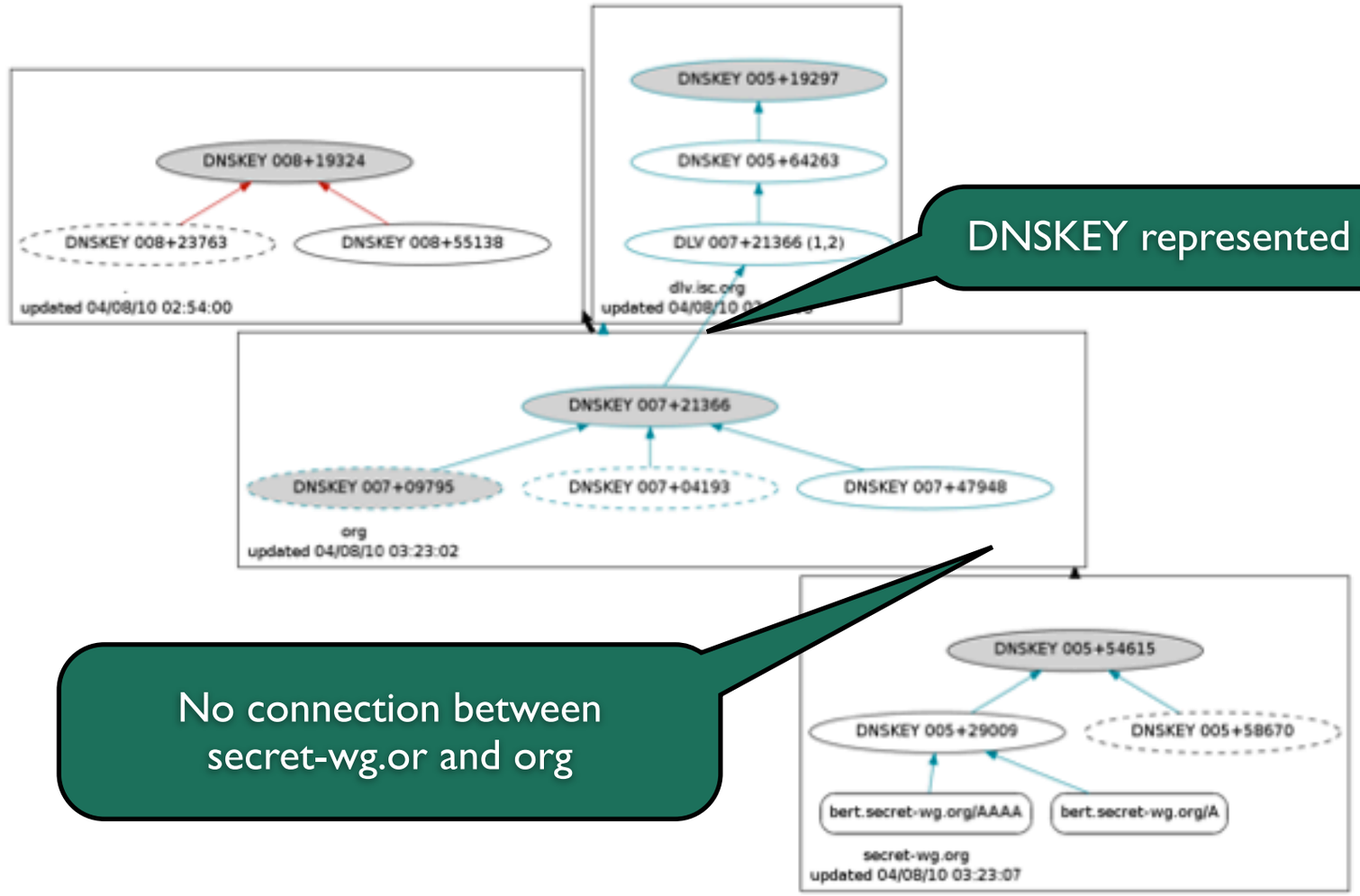
DNSKEY legend

Published only

SEP bit set

Revoke bit set

DNSSEC authentication chain



Same zone different, after secure delegation

VERISIGN™ LABS

Domain Name: bert.secret-wg.org Detail: more(+) / less(-) Time: 2012-02-03 15:18:01 UTC, NTP stratum 3

Analyzing DNSSEC problems for bert.secret-wg.org

.	Found 2 DNSKEY records for . DS=19036/SHA1 verifies DNSKEY=19036/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
org	Found 2 DS records for org in the . zone Found 1 RRSIGs over DS RRset RRSIG=51201 and DNSKEY=51201 verifies the DS RRset Found 4 DNSKEY records for org DS=21366/SHA1 verifies DNSKEY=21366/SEP Found 2 RRSIGs over DNSKEY RRset RRSIG=21366 and DNSKEY=21366/SEP verifies the DNSKEY RRset
secret-wg.org	Found 2 DS records for secret-wg.org in the org zone Found 1 RRSIGs over DS RRset RRSIG=55440 and DNSKEY=55440 verifies the DS RRset Found 4 DNSKEY records for secret-wg.org DS=18786/SHA256 verifies DNSKEY=18786/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=18786 and DNSKEY=18786/SEP verifies the DNSKEY RRset bert.secret-wg.org A RR has value 213.154.224.48 Found 1 RRSIGs over A RRset RRSIG=46673 and DNSKEY=46673 verifies the A RRset

Connection between secret-wg.or and org exist

Move your mouse over any ⊗ or ⚠ symbols for remediation hints.

Want a second opinion? Test bert.secret-wg.org at dnsviz.net.

  VeriSign Labs DNSSEC Analyzer r43 2012-01-30 23:05:50

SecSpider

http://secspider.cs.ucla.edu/

Google

SecSpider

SecSpider the DNSSEC Monitoring Project

Home | Blog | Documentation | Trust-Anchors | Pollers | GPG Key

Check out our new sister-project Vantages with libvdns, `dnsfunnel`, and `vantaged`!

We now have TA files for both modern resolvers and older instances of BIND that don't support all key types on our Trust Anchors Page

Search for zone:

Zone: Submit

To add a zone for monitoring, please submit below:

Zone to add: secret-wg.org Submit

Vouch for or against a zone's production status

For more information, questions, or comments please contact:
Eric Osterweil (*eoster@cs.ucla.edu*)
Dan Massey (*massey@cs.colostate.edu*)
Lixia Zhang (*lixia@cs.ucla.edu*)

DNSSEC Deployment status as of: *Wed Dec 14 06:41:56 2011 UTC*

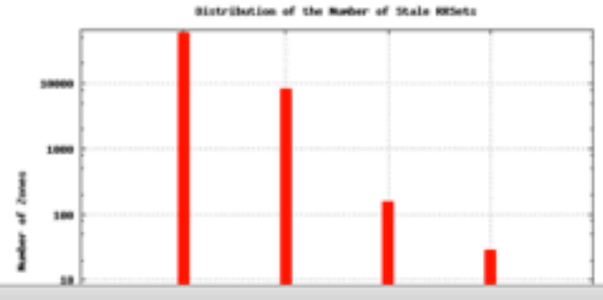
Deployment Metrics:

[What are these?]

Availability Metric: 0.743

Verifiability Metric: 0.423

Validity Metric: < 0.932, 0.937 >



NLnet Labs

DNSSEC Zone stats

http://secspider.cs.ucla.edu/secret-wg-org--zone.html

Google

DNSSEC Zone stats

Zone **secret-wg.org.** status as of: Wed Dec 14 06:41:56 2011 UTC
Seen by 7/9 active pollers.

Reason for Monitoring this Zone:

DNSKEY Availability	Stale RRsets
1	0

Parent Zone: org.

Data files for:
DS records (signed)
DNSKEY records (signed)

Trust Anchor:

Consistency:	Name:
6/9	.
1/9	org.

Summary:

Property:	Status:
EDNS0 capable	Yes
DNSSEC deployed	Yes
Production zone	Yes
User Production	N/A

DNSKEY PMTU Walk Summary

From poller #	PMTU problem for DNSKEYs?	Packet size that worked
0	No	Any
1	No	Any
2	No	Any
3	No	Any
4	No	Any
5	No	Any
6	No	Any
7	No	Any
8	No	Any

Name Servers:

Consistency:	Online:	NS Name:	NS IP:	Server Version:	First Queried:	Last Queried:	NS Serial Number:	EDNS0 Capable:	DNSSEC Deployed:	Pointed to by Which Zone (Parent/Authoritative/Both)?
7/9	Yes	mcvax.nlnetlabs.nl.	192.16.197.229	NSD 3.2.8	Sun May 29 14:49:08 2011 UTC	Thu Nov 17 02:07:21 2011 UTC	501	Yes	Yes	Parent
7/9	Yes	sec2.authdns.ripe.net.	193.0.9.4	9.7.3-P3	Sun Jul 11 04:47:00 2010 UTC	Thu Nov 17 02:07:22 2011 UTC	501	Yes	Yes	Both
6/9	Yes	ns.secret-wg.org.	213.154.224.48	NSD 3.2.8	Tue Aug 22 19:15:39 2006 UTC	Thu Nov 17 02:07:24 2011 UTC	501	Yes	Yes	Both
7/9	Yes	open.nlnetlabs.nl.	213.154.224.1	NSD 3.2.8	Wed Apr 26 22:11:23 2006 UTC	Thu Nov 17 02:07:23 2011 UTC	501	Yes	Yes	Both

DS Records from parent zone:
Consistency: 7/9

Key Tag:	Digest:	Verified (Yes/No):
SECRET-WG.ORG. 18786	6B4D6BE52905E7C45086 8C44C905F3ABB59A5934 457F2F517F240F2D2F62 456C	Yes
SECRET-WG.ORG. 18786	BD9CB32D9C35DA3C4D60 C3314C4BD99F22FDB082	Yes

DNSKEYs:
Consistency: 7/9

Key Verified (Yes/No/Unknown):	Key Tag:	Key Type:	Algorithm:	Key:
Yes	secret-wg.org. 18786	KSK	RSASHA1-NSEC3-SHA1	AwEAAcwokMwQhDhIggcA 97E7FI5NbisKJ+YvftLe mmbU93YP26IpIGkpJdQ OiMAdWJtkW+LAuVNrUTm bZyZaL1QUhE9WdslVW5L pVTjSWBn2C2DP9X3ZlIM hfvYTO3ztz6cBn5xlcBq 5VdVBopo+zIkbhcjsM07 UsDkcOIfs/Bnm6nus2BD EtWCc7Uf61A/KI+lwbjM p5044/nMY/BH7CxXvZ7s w5cHBPwfK2V4LPj0ejGO /qc+8IZIp2y7asIbYX2h FIfib56Z35W9Kj8z2HUI z8T8lqnqg5B3QKZXtQH7 azRR02QOIYWKBv7sm6Re PKvCMGTQr82+/mq2t0Rj kRm/sDc=
Yes	secret-wg.org. 39573	ZSK	RSASHA1-NSEC3-SHA1	AwEAAZ5J25d6vBat5T2I qBiKnIsPbiKyN0KIxzui tauC6r40pJJ6MFNC1K5t CMM6zZx1WfU0dtzWclch I16vyeG3ce/3bYHn20GI RXq3L9jr00noWSKGUYW7 b33hb0PYR35ei6wQumJl SYmYbkkeTn0tv/1uKVDD ayvl70JRquaMjrgI
Yes	secret-wg.org. 61595	ZSK	RSASHA1-NSEC3-SHA1	AwEAAcG3GlPcfOyRep40 Lxsyzy0+dYKoXsS6w4Gf 120sVOI2CWeacE3EfqfH YJN0e61PkAeYZJNFxIqF TbrP/t7vXfQyq0T0jXdZ fKUkltKWYaglIe5323L6 95v4pGI49o865btY3gjD NBbWV43WGpV/5FYwLfq8 5RlpjpMHKwZxuJjH

RRSIGs	Key Used:	Inception:	Expiration:
	secret-wg.org. 18786	Mon Nov 14 08:33:41 2011 UTC	Sun Nov 27 23:38:43 2011 UTC

.net Labs

orted License.

Case Study

- NASA DS Rollover failure impacting Comcast: http://www.dnssec.comcast.net/DNSSEC_Validation_Failure_NASAGOV_20120118_FINAL.pdf

looking at a validating server

- So you got a SERVAIL
  - dig +cd will disable checking
    - you get an answer?
    - likely validation failure

Transport problems

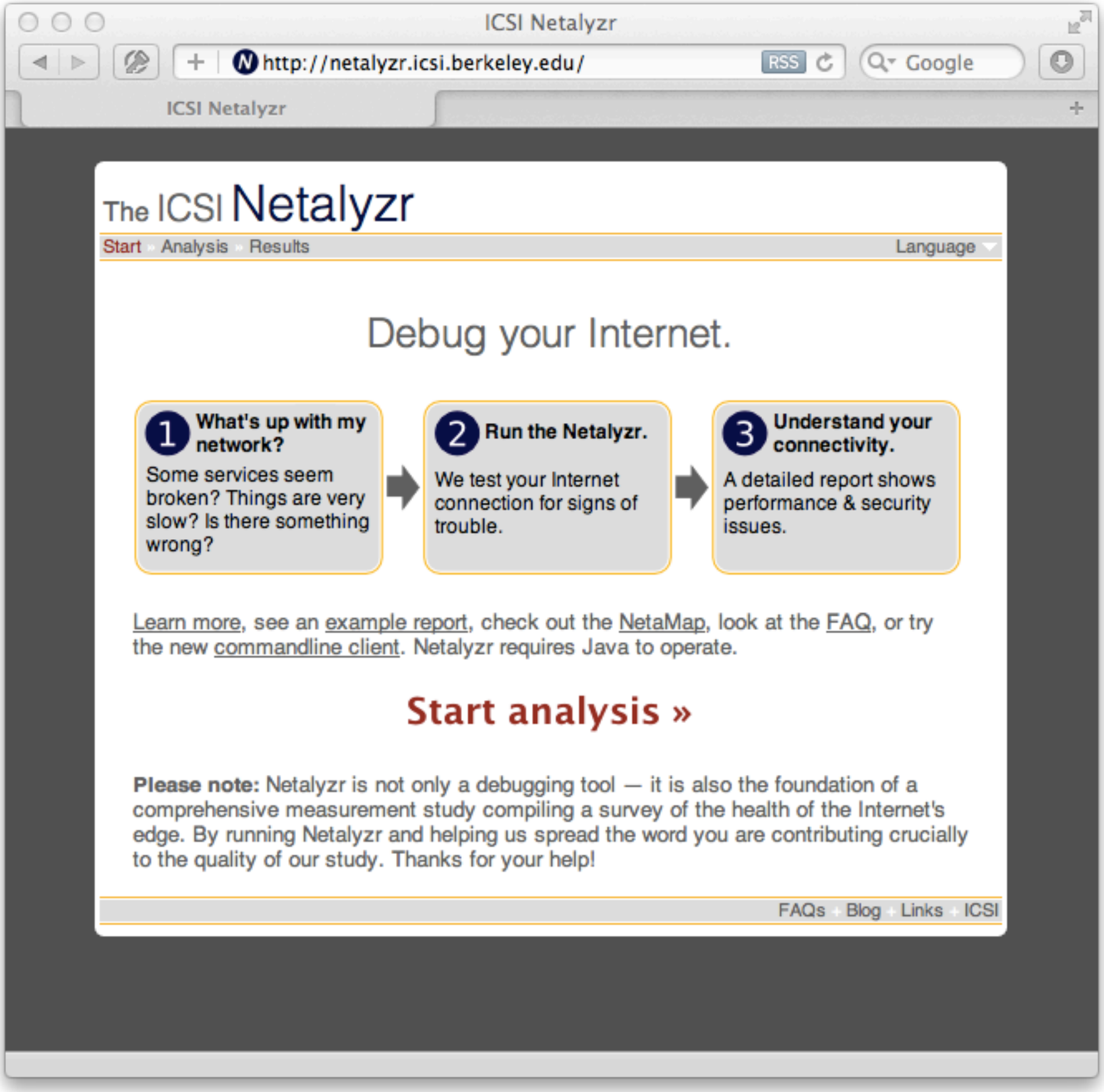
- If responses grow beyond 512octets:
  - UDP may see fragmentation and dropped fragments (firewalls etc)
  - fragmentation problems on path?
  - Fallback to TCP
    - Port 53 TCP sometimes blocked

NLnet Labs

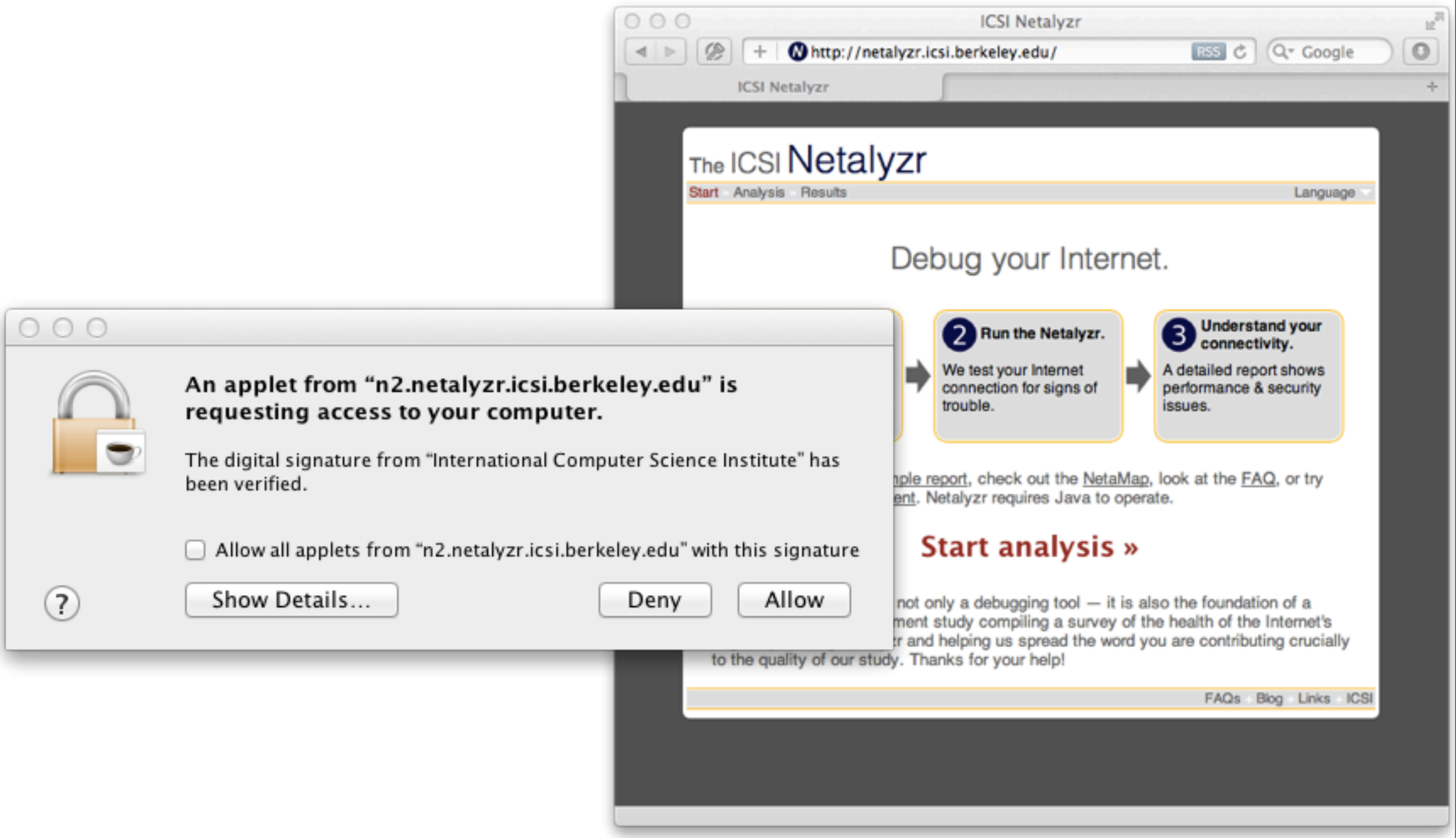
Does the network support DNSSEC?

- One tool you could use for a quick assesment:
- http://netalyzr.icsi.berkeley.edu/
    - you contribute to good science too!

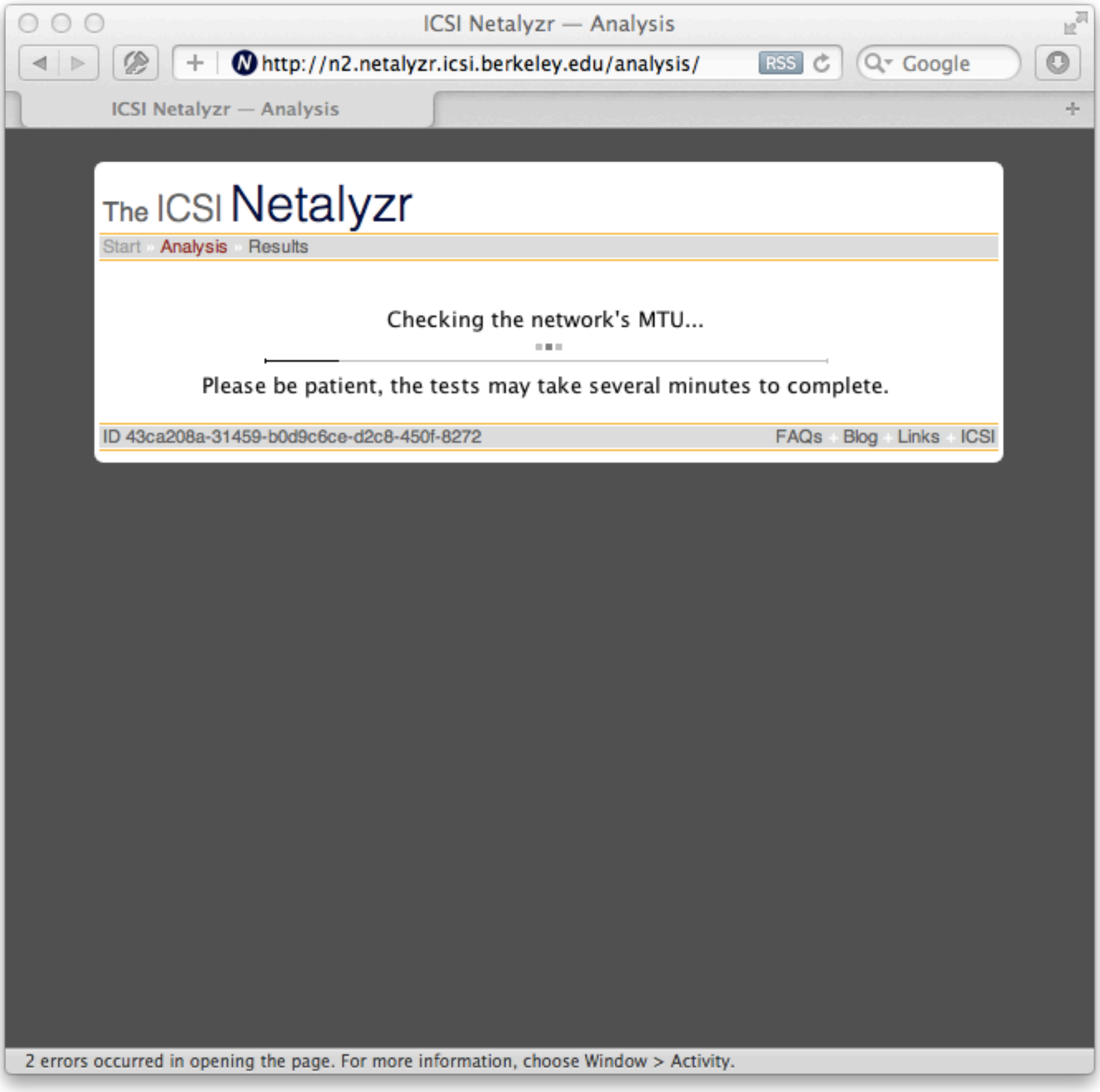
NLnet Labs



NLnet Labs



NLnet Labs



ICSI Netalyzr — Results

http://n1.netalyzr.icsi.berkeley.edu/summary/id=43ca253f-11779-1d6e982f-7d3b-4301-ad2

ICSI Netalyzr — Results

The ICSI Netalyzr

Start » Analysis » Results

Result Summary +/– (help)

[redacted].nl / [redacted].83

Recorded at 04:14 EST (09:14 UTC), Feb 14 2012. Permalink. Client/server transcript.

Summary of Noteworthy Events –

Minor Aberrations

- Network packet buffering may be excessive ↓
- We received unexpected and possibly dangerous results when looking up important names ↓
- The path between our system and your network does not appear to handle fragmented IPv6 traffic properly ↓

Address-based Tests +

- NAT detection (?): No NAT Detected
- Local Network Interfaces (?): OK
- DNS-based host information (?): OK

Reachability Tests +

- TCP connectivity (?): OK
- UDP connectivity (?): OK
- Traceroute (?): OK
- Path MTU (?): OK

NLnet Labs

DNS Tests –

Restricted domain DNS lookup (?): OK

We can successfully look up a name which resolves to the same IP address as our webserver. This means we are able to conduct many of the tests on your DNS server.

Unrestricted domain DNS lookup (?): OK

We can successfully look up arbitrary names from within the Java applet. This means we are able to conduct all test on your DNS server.

Direct DNS support (?): OK

All tested DNS types were received OK.

Direct EDNS support (?): OK

EDNS-enabled requests for small responses are answered successfully.

EDNS-enabled requests for medium-sized responses are answered successfully.

EDNS-enabled requests for large responses are answered successfully.

DNS resolver address (?): OK

The IP address of your ISP's DNS Resolver is 213.154.224.59, which resolves to alpha.nlnetlabs.nl.

DNS resolver properties (?): Lookup latency 240ms

Your ISP's DNS resolver requires 240 msec to conduct an external lookup. It takes 200 msec for your ISP's DNS resolver to lookup a name on our server.

Your resolver correctly uses TCP requests when necessary.

Your resolver is using QTYPE=A for default queries.

Your host or resolver also performs IPv6 queries in addition to IPv4 queries.

Your DNS resolver requests DNSSEC records.

Your DNS resolver advertises the ability to accept DNS packets of up to 4096 bytes.

Your DNS resolver can successfully receive a smaller (~1400 byte) DNS response.

Your DNS resolver can successfully receive a large (>1500 byte) DNS response.

Your DNS resolver can successfully accept large responses.

Your resolver does not use 0x20 randomization, but will pass names in a case-sensitive

NLnet Labs

On your server

- val-log-level:
  - val-log-level: 0 - prints nothing
  - val-log-level: 1 - print queries that fail
  - val-log-level: 2 - print reason why it failed

- remember **`unbound-control set_option`**?

NLnet Labs

```
Apr 08 12:31:06 unbound[853:0] info: validation failure
<dnssec1.gsa.dnsops.gov. A IN>: signature expired from 159.142.174.98
for key gsa.dnsops.gov. while building chain of trust


Apr 08 10:28:01 unbound[853:0] info: validation failure
<barney.llnl.dnsops.gov. SOA IN>: No DNSKEY record from 128.115.249.61
for key barney.llnl.dnsops.gov. while building chain of trust
```

NLnet Labs

Unbound-host

- unbound-host tool is useful for taking a first stab
- Runs the unbound validator from the command line
  - unbound-host -v -f trustanchor example.com
  - prints the val-log-level 2 error message if it fails.
  - with -C it can read unbound.conf for settings.
  - with -d (or -dddd) you get a high verbosity trace

NLnet Labs

Remedies

- Clean your cache in case of problems locally
- Bind:
  - `rndc flush`
  - `rndc flushname`
- Unbound
  - `unbound-control flush`
  - `unbound-control flush_zone`
  - `unbound-control flush_infra`

NLnet Labs