



VERISIGN®

Hands-on DNSSEC with DNSViz

Casey Deccio, Verisign Labs

RIPE 70, Amsterdam

May 11, 2015

Preparation

- Demo and exercises available at:
 - <http://dnsviz.net/demo/>
- Includes links to the following:
 - VirtualBox software
 - VirtualBox demo image
 - Tutorial exercises

Objectives

- Understand the basics of DNS and DNSSEC
- Become familiar with DNS server and analysis tools
 - DiG
 - BIND
 - DNSViz
- Learn how tools might be used to routinely analyze/monitor your DNS health

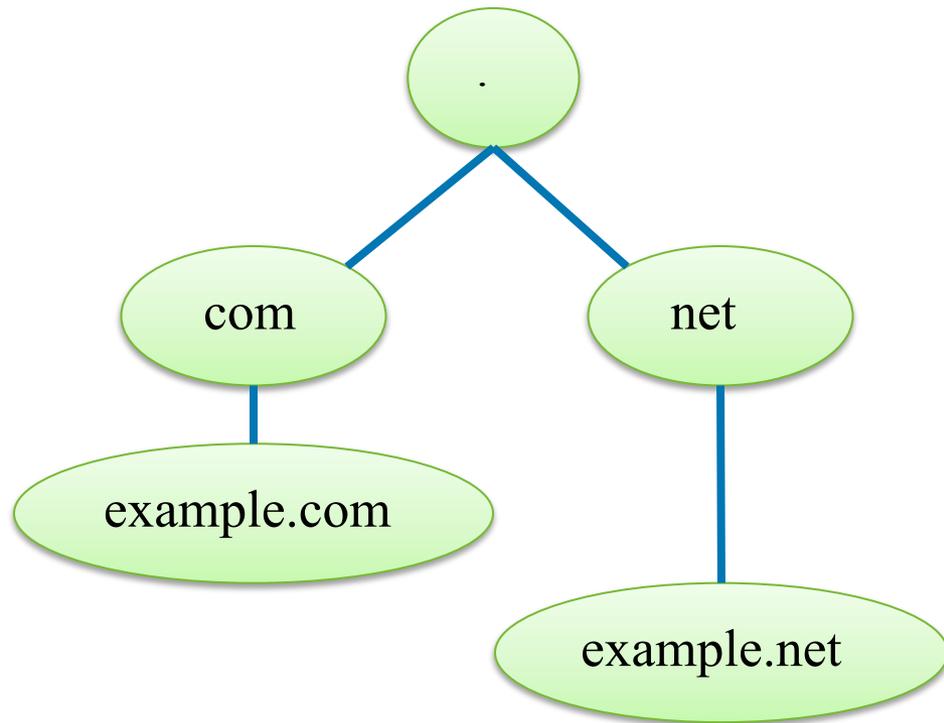
Caveats

- The exercises range from novice-level to advanced.
- Many of the exercises are more to facilitate understanding than efficiency.
- The exercises are meant for learning DNS/DNSSEC and related tools, but do not cover all details for proper DNS/DNSSEC maintenance.

DNS Overview

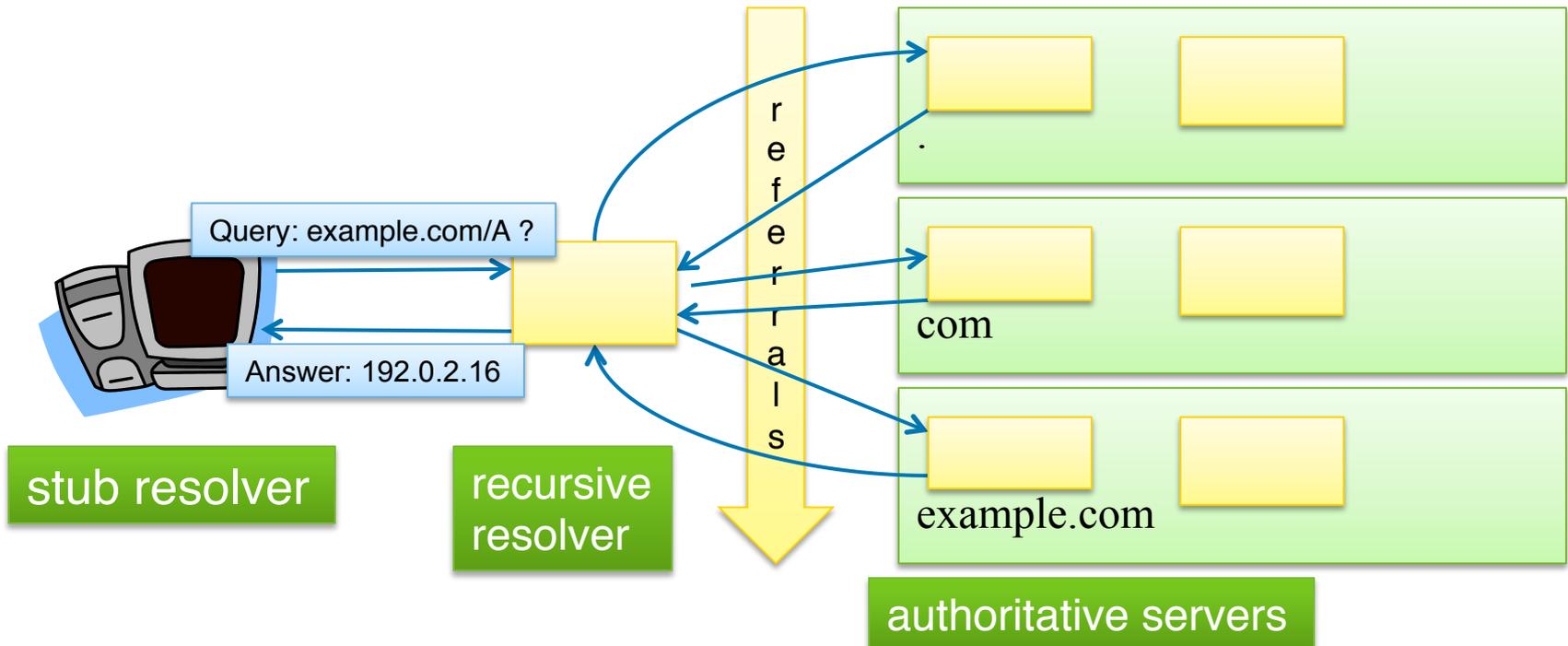
DNS Namespace

- Namespace is organized hierarchically
- DNS **root** is top of namespace
- **Zones** are autonomously managed pieces of DNS namespace
- Subdomain namespace is delegated to child zones



DNS Name Resolution

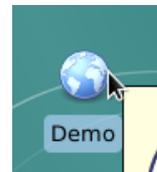
- **Resolvers** query **authoritative servers**
- Queries begin at root zone, resolvers follow downward referrals
- Resolver stops when it receives authoritative answer



Virtual Environment Initialization

- Unzip dnsviz-demo-v1.zip
- Open dnsviz-demo-v1/dnsviz-demo-v1.vbox

- “Start” VM
- Enlarge screen
- Double-click “demo” icon



- (Exercises 0.1 – 0.2)
 - Open “Terminal Emulator”
 - Change to “demo” directory



```
$ cd demo
```

Query DNS Servers (1.1 – 1.5)

```
$ dig @a.root-servers.net example.com
```



query a specific server
(rather than querying your
configured resolver)



no record type specified,
so default type
“A” (address) is used

```
$ dig @a.gtld-servers.net example.com
```

```
$ dig @a.iana-servers.net example.com
```

```
$ dig www.example.com
```



no server is explicitly
designated, so query
goes to local resolver

```
$ dig @a.iana-servers.net foobar.example.com
```

Query a root Server

```
Terminal - dnsviz@dnsviz-demo: ~/demo
File Edit View Terminal Tabs Help
dnsviz@dnsviz-demo:~/demo$ dig @a.root-servers.net example.com

; <<>> DiG 9.9.5-9-Debian <<>> @a.root-servers.net example.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1649
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 16
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;example.com.                IN      A

;; AUTHORITY SECTION:
com.      172800  IN      NS      m.gtld-servers.net.
com.      172800  IN      NS      l.gtld-servers.net.
com.      172800  IN      NS      k.gtld-servers.net.
com.      172800  IN      NS      j.gtld-servers.net.
com.      172800  IN      NS      i.gtld-servers.net.
com.      172800  IN      NS      h.gtld-servers.net.
com.      172800  IN      NS      g.gtld-servers.net.
com.      172800  IN      NS      f.gtld-servers.net.
com.      172800  IN      NS      e.gtld-servers.net.
com.      172800  IN      NS      d.gtld-servers.net.
com.      172800  IN      NS      c.gtld-servers.net.
com.      172800  IN      NS      b.gtld-servers.net.
com.      172800  IN      NS      a.gtld-servers.net.

;; ADDITIONAL SECTION:
m.gtld-servers.net.  172800  IN      A      192.55.83.30
l.gtld-servers.net.  172800  IN      A      192.41.162.30
```

Query a TLD Server

```
Terminal - dnsviz@dnsviz-demo: ~/demo
File Edit View Terminal Tabs Help
dnsviz@dnsviz-demo:~/demo$ dig @a.gtld-servers.net example.com

; <<>> DiG 9.9.5-9-Debian <<>> @a.gtld-servers.net example.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64763
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 5
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;example.com.                IN      A

;; AUTHORITY SECTION:
example.com.                172800  IN      NS      a.iana-servers.net.
example.com.                172800  IN      NS      b.iana-servers.net.

;; ADDITIONAL SECTION:
a.iana-servers.net.        172800  IN      A       199.43.132.53
a.iana-servers.net.        172800  IN      AAAA    2001:500:8c::53
b.iana-servers.net.        172800  IN      A       199.43.133.53
b.iana-servers.net.        172800  IN      AAAA    2001:500:8d::53

;; Query time: 91 msec
;; SERVER: 192.5.6.30#53(192.5.6.30)
;; WHEN: Thu Apr 30 21:27:16 EDT 2015
;; MSG SIZE rcvd: 176
```

Query an SLD Server

```
Terminal - dnsviz@dnsviz-demo: ~/demo
File Edit View Terminal Tabs Help
dnsviz@dnsviz-demo:~/demo$ dig @a.iana-servers.net example.com

; <<>> DiG 9.9.5-9-Debian <<>> @a.iana-servers.net example.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 44304
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;example.com.                IN      A

;; ANSWER SECTION:
example.com.                 86400  IN      A      93.184.216.34

;; AUTHORITY SECTION:
example.com.                 172800 IN      NS     b.iana-servers.net.
example.com.                 172800 IN      NS     a.iana-servers.net.

;; Query time: 17 msec
;; SERVER: 199.43.132.53#53(199.43.132.53)
;; WHEN: Thu Apr 30 21:29:30 EDT 2015
;; MSG SIZE rcvd: 104
```

Query Local Recursive Resolver

```
Terminal - dnsviz@dnsviz-demo: ~/demo
File Edit View Terminal Tabs Help
dnsviz@dnsviz-demo:~/demo$ dig example.com

; <<>> DiG 9.9.5-9-Debian <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15182
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;example.com.                IN      A

;; ANSWER SECTION:
example.com.                68734   IN      A      93.184.216.34

;; AUTHORITY SECTION:
example.com.                155133  IN      NS     b.iana-servers.net.
example.com.                155133  IN      NS     a.iana-servers.net.

;; ADDITIONAL SECTION:
a.iana-servers.net.        1768    IN      A      199.43.132.53
a.iana-servers.net.        1768    IN      AAAA   2001:500:8c::53
b.iana-servers.net.        155133  IN      A      199.43.133.53
b.iana-servers.net.        155133  IN      AAAA   2001:500:8d::53

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Apr 30 21:30:02 EDT 2015
;; MSG SIZE rcvd: 192
```

Query for a Non-existent Name

```
Terminal - dnsviz@dnsviz-demo: ~/demo
File Edit View Terminal Tabs Help
dnsviz@dnsviz-demo:~/demo$ dig @a.iana-servers.net foobar.example.com

; <<>> DiG 9.9.5-9-Debian <<>> @a.iana-servers.net foobar.example.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 36564
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;foobar.example.com.          IN      A

;; AUTHORITY SECTION:
example.com.                  3600    IN      SOA     sns.dns.icann.org. noc.d
0 3600 1209600 3600

;; Query time: 12 msec
;; SERVER: 199.43.132.53#53(199.43.132.53)
;; WHEN: Thu Apr 30 21:30:41 EDT 2015
;; MSG SIZE rcvd: 104
```

DNSSEC Overview

Public Key Cryptography

- Keys

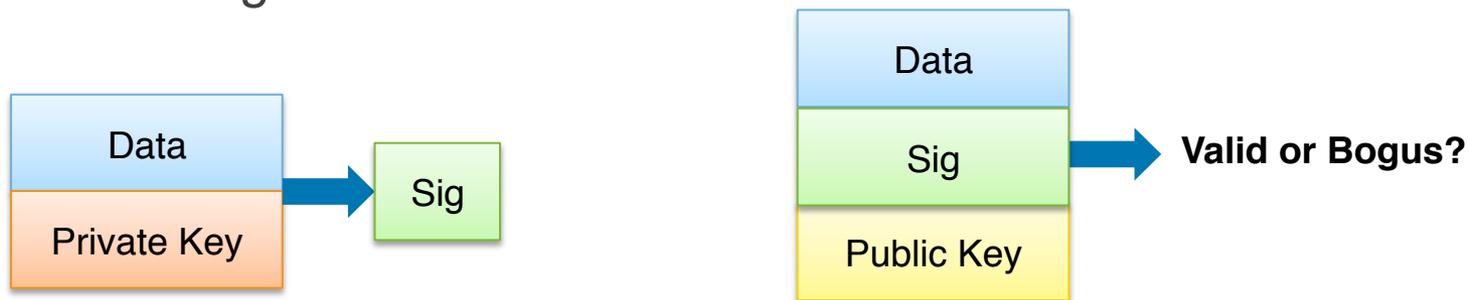
- **Public** Key – advertised to everyone
- **Private** Key – kept hidden

- Signatures

- Made by private key
- Validated with public key

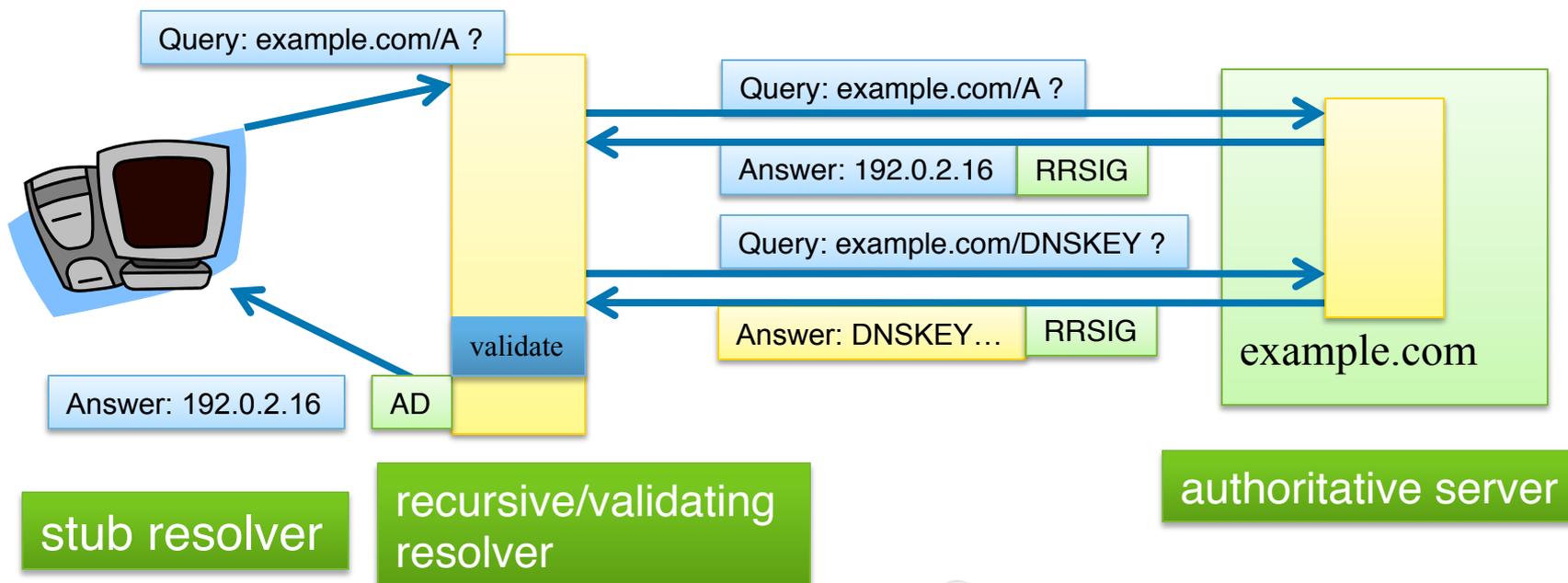
- Validation

- Consumer uses public key, message, and signature to validate message



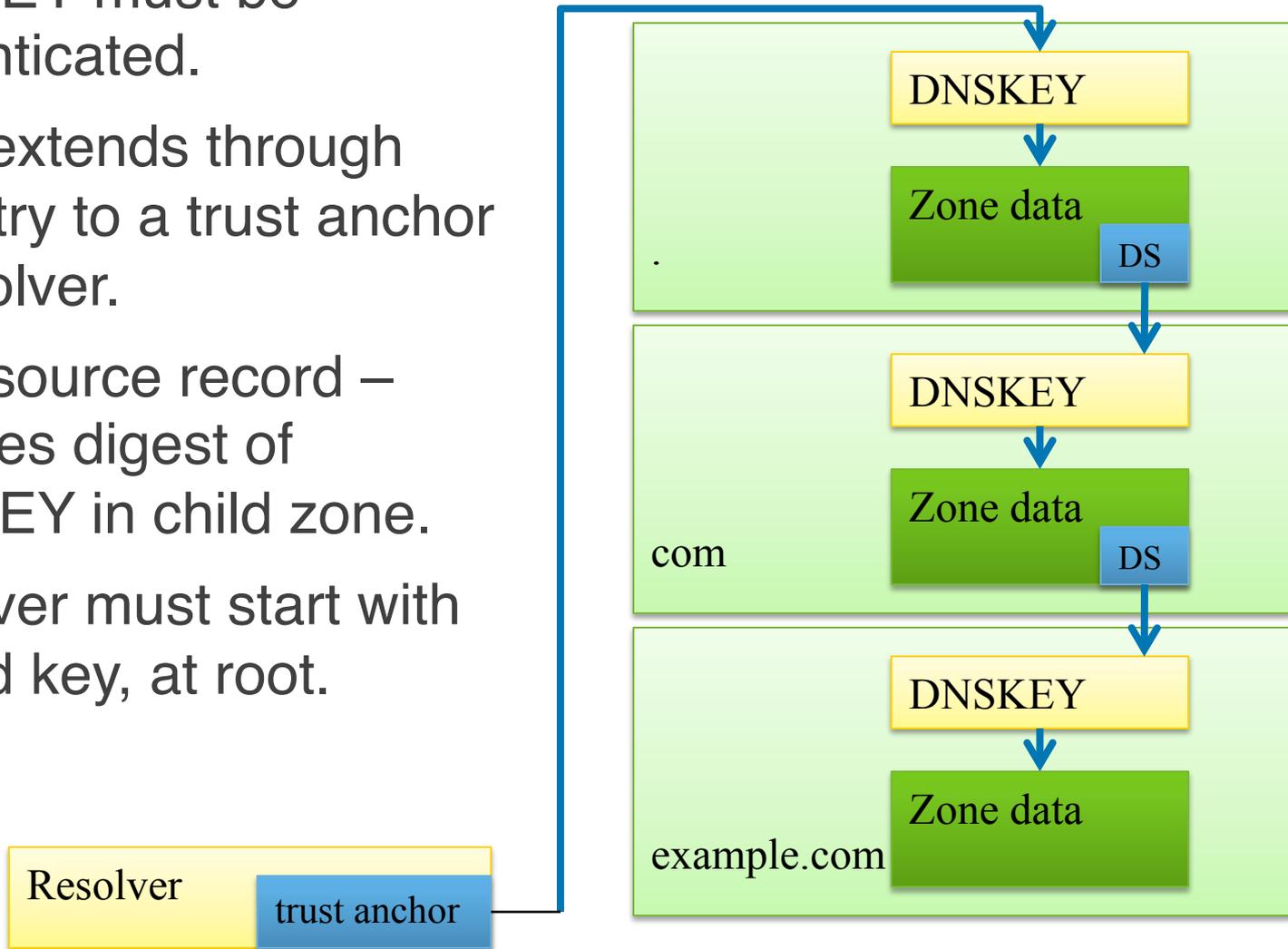
DNS Security Extensions (DNSSEC)

- DNS data signed with private keys
- Signatures (RRSIGs) and public keys (DNSKEYs) published in zone data
- Resolver response
 - If authentic: Authenticated data (AD) bit is set
 - If bogus: SERVFAIL message is returned



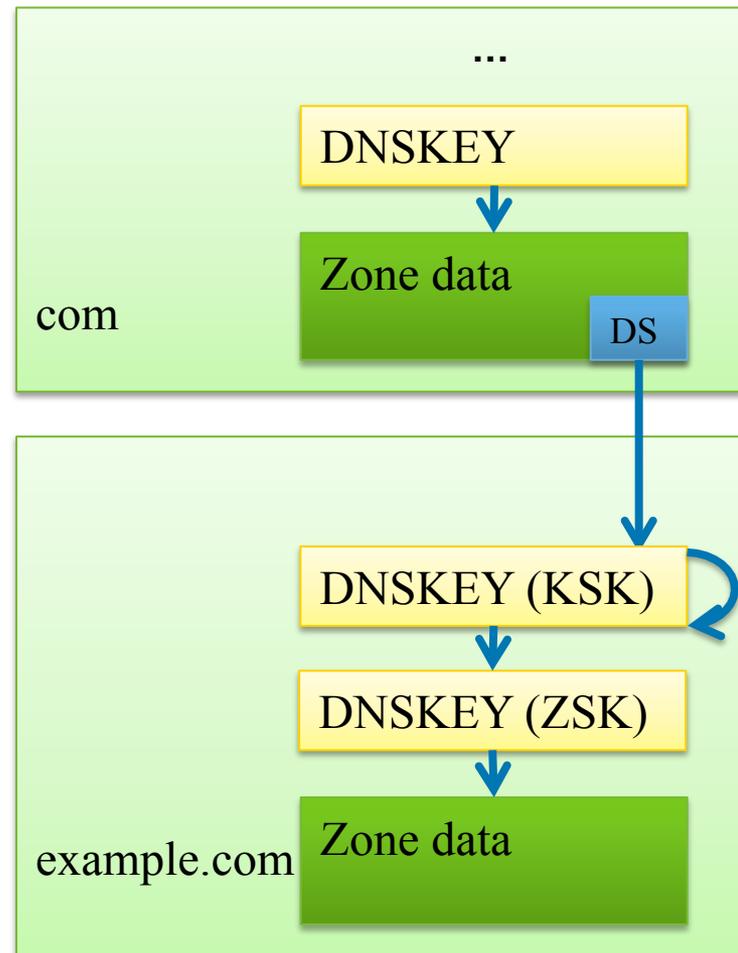
DNSSEC Chain of Trust

- DNSKEY must be authenticated.
- Trust extends through ancestry to a trust anchor at resolver.
- DS resource record – provides digest of DNSKEY in child zone.
- Resolver must start with trusted key, at root.



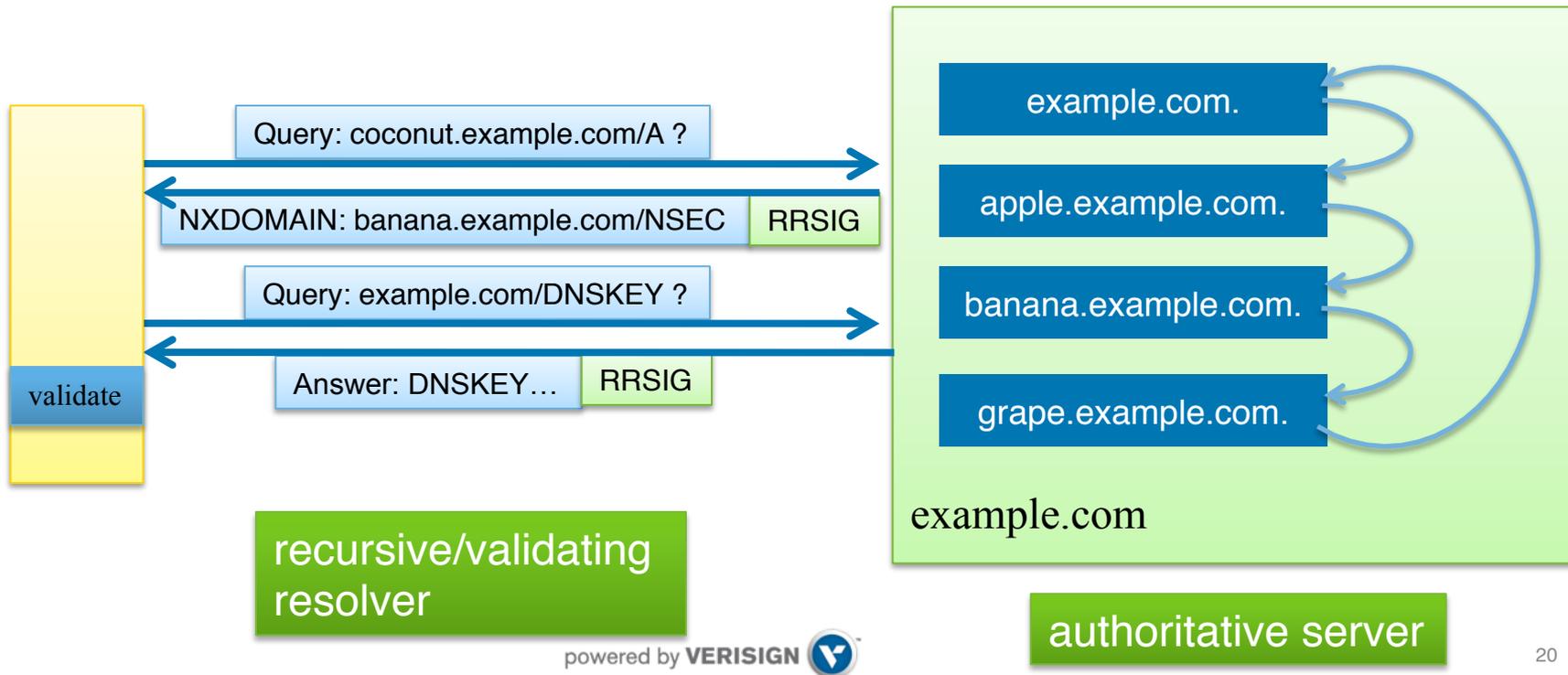
Key Roles – KSK/ZSK

- DNSKEY RRset usually has multiple keys, often with split roles.
- KSK (Key signing key)
 - Signs (only) the DNSKEY RRset.
 - Corresponds to DS records in parent, providing “secure entry point” into zone.
- ZSK (Zone signing key)
 - Signs the rest of the zone.



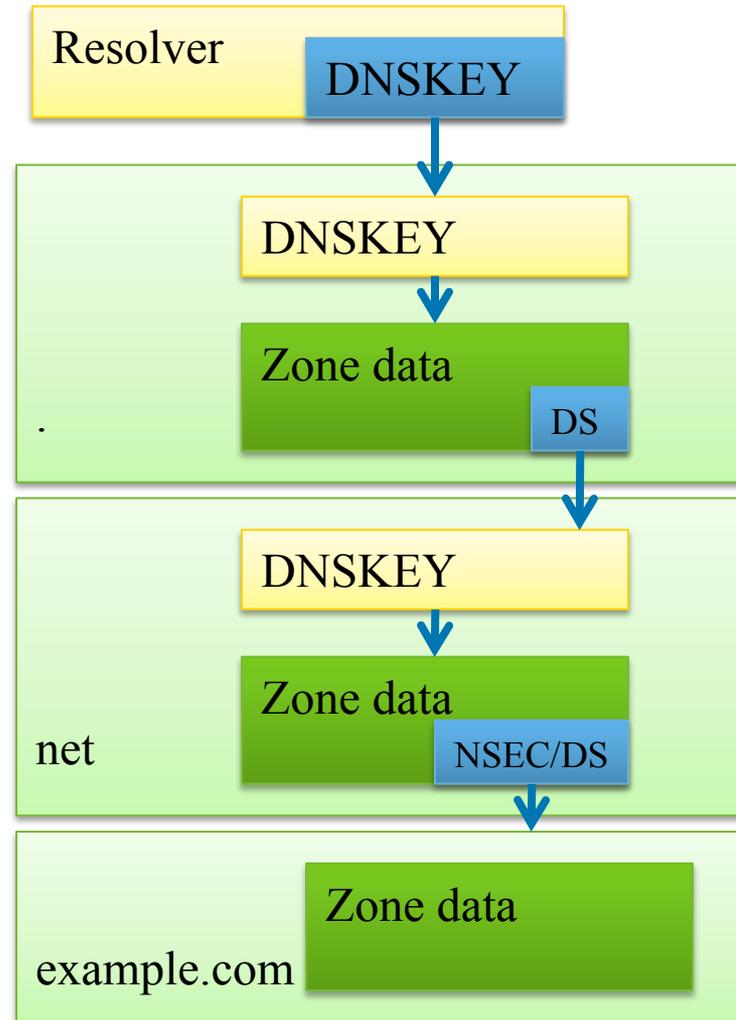
Authenticated Denial of Existence

- How do you prove something doesn't exist?
- “Chain” of names of zone formed using NSEC records.
- NSEC records form comprehensive chain of names (and their record types) in zone in canonical ordering.
- Server uses NSEC records to prove non-existence.



Insecure delegations

- How can DNSSEC be deployed incrementally?
- If child zone is unsigned, resolver must be able to prove it is insecure.
- NSEC resource records provide proof of absence of DS.



Zone Enumeration and NSEC3

- NSEC records allow enumeration of entire zone contents.
- NSEC3 standard introduces *hashed* denial of existence.
 - Joint effort between Verisign, Nominet (.uk), and DENIC (.de).
- Chain is of *hashes* of names, not *names* themselves.
(a hash is the output of a one-way cryptographic function.)



Query for DNSSEC Records (2.1 – 2.5)

```
$ dig +dnssec +multi @a.iana-servers.net example.com
```



include DNSSEC records in response (e.g., RRSIG)
present response in multi-line format with comments (for readability)

query for records of type “DNSKEY” (DNSSEC public key) instead of the default, “A” (address)



```
$ dig +dnssec +multi @a.iana-servers.net example.com DNSKEY
```

```
$ dig +dnssec +multi @a.gtld-servers.net example.com DS
```



query a “parent” server because we’re seeking a DS record

```
$ dig +dnssec +multi example.com
```

```
$ dig +dnssec +multi @a.iana-servers.net foobar.example.com
```

Query for DNSSEC Records (RRSIGs)

```
Terminal - dnsviz@dnsviz-demo: ~/demo
File Edit View Terminal Tabs Help
dnsviz@dnsviz-demo:~/demo$ dig +dnssec +multi @a.iana-servers.net example.com
; <<>> DiG 9.9.5-9-Debian <<>> +dnssec +multi @a.iana-servers.net example.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1513
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
example.com.                IN A

;; ANSWER SECTION:
example.com.                86400 IN A 93.184.216.34
example.com.                86400 IN RRSIG A 8 2 86400 (
                             20150508075513 20150430232918 23014 example.com.
                             d9LRittlgFmX/Y6HdGvu9xzNWKzyX+ifW2zn3PqDtcvS
                             nA4Fvuaua/ZGKsHuRPtBvt7Afz/T7h41N3rXVknNqGfD
                             GkHyRXTnoS/0G8jXCuEavdAsbQMVFdZ05Cb+BVfTt04S
                             SeHGjMQD0NtdI859BFpLTxA0+5tGbL9D0auhoJ0= )

;; AUTHORITY SECTION:
example.com.                172800 IN NS b.iana-servers.net.
example.com.                172800 IN NS a.iana-servers.net.
example.com.                172800 IN RRSIG NS 8 2 172800 (
                             20150508015115 20150430232918 23014 example.com.
                             PurNKwacfg2vaHEixDE5Z/JZjddM4AvFYY2o7xsRtKlQ
                             NebtN4P5wajy0hvzRTPi7p0t3RrAyT/jPn8V/60tINWY
                             g8UdsKvlvWmkS8bg0d61k0tDj16au1CDSiu0KiHHa1/T
                             T/JHuThR0922X0c2HZy4TQy94e583H7ZMJQ4NqM= )
```

Query for DNSSEC Records (DNSKEY)

```
Terminal - dnsviz@dnsviz-demo: ~/demo
File Edit View Terminal Tabs Help
;; ANSWER SECTION:
example.com.      3600 IN DNSKEY 257 3 8 (
    AwEAAaikvxboZpn9VCxm3YDLHo40SvA9EmRwJHHQyJ00
    CzrQSRBSipojrW7yESXWiDDyzfLS8rgzDs7M3fIdSdu0
    dyNi55DmXPdkS8HYORTMNyzFsS0g+xx6tUySK2p4WAhl
    bsJNLz4IkQCek59NoDB0LyQ15npsr7Tgfb/HHU7zmCMv
    nxh0Sq02lyhnQfk29Thc3nC4KNJNb3drjWK0uCW5mg+2
    GrEZYc/VqdeGvr0CQ2el8jWZpSU5cxb7EdEy4B9nEeZi
    BpHXaZ5XJ+ewi4vmcUK5/445mGJqV4rDeicy5/ShC/BJ
    81v3bIRPWebvDRJmDbjr2d9MnLXUE7yyETrQd18=
    ) ; KSK; alg = RSASHA256; key id = 31589
example.com.      3600 IN DNSKEY 256 3 8 (
    AwEAAajz7mvxb69EEGk7TPfs+H6kuyLLTu/mEHZDgEsE
    1a3ZZ2kLLMEYX+2EJdtyFT6rmKH8cWBeqtA+0dPtjSg+
    nAicyQP3BBHdWCUu4TeLI4MwCGpI7gVDxb5mTYg960v/
    /5gah4SW8kD0jYV3LVFrYqyLpvIXy+vnNPM+JiHPY2pZ
    ) ; ZSK; alg = RSASHA256; key id = 23014
example.com.      3600 IN DNSKEY 257 3 8 (
    AwEAAawt7HpLI5M8GGAsxuyCyjF0l+QlCGVN11CRZ4vP
    66qbDCX0BnShZ11Bgb//4zSG/8mmBHirL2FLg+mVuIix
    ig+iroZYjh4iTKV0hv2hZftRwyrQHK++qXvCCWN3ki51
    RG/e8R4k0EV71rZ80gQvPWx6F91qroq0Ppcf7PPxippe
    H0n+PxnP0hpyLyolmx1rPs/cMpl3j0MufGP+LJYh+fBU
    7lt0sP5i09HaJPruzyZML9BPtpv8ZAdQhwtXVG0+MnET
    2qT/1+TljpxZn6yeegFRCFRHBjMo6iiRjnuWra/klkrg
    En2Q+BXGT0MTTKQdYz40xYEa1z7apu3a09dYnBM=
    ) ; KSK; alg = RSASHA256; key id = 51605
example.com.      3600 IN RRSIG DNSKEY 8 2 3600 (
    20150508010106 20150430232918 31589 example.com.
    qaWo7cFfukqwABNucVAva+TCDYvzWSMRzRao3Hb6DgWh
    wASq40n7RaojzW+spbWyo71trspl6sWvu0JP1E+6YCN6
    9kfhcu88rjnc8qsUUohEB1ZKNtggojZxtdda0/QSlF1g
    kck5AWKd4dYrEjm0msxfzCkWnHnzL0JxaYnSXCudLen1
```

Query for DNSSEC Records (DS)

```
Terminal - dnsviz@dnsviz-demo: ~/demo
File Edit View Terminal Tabs Help
dnsviz@dnsviz-demo:~/demo$ dig +dnssec +multi @a.gtld-servers.net example.com DS
; <<>> DiG 9.9.5-9-Debian <<>> +dnssec +multi @a.gtld-servers.net example.com DS
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57064
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 14, ADDITIONAL: 16
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;example.com.          IN DS

;; ANSWER SECTION:
example.com.          86400 IN DS 31589 8 1 (
                      3490A6806D47F17A34C29E2CE80E8A999FFBE4BE )
example.com.          86400 IN DS 31589 8 2 (
                      CDE0D742D6998AA554A92D890F8184C698CFAC8A26FA
                      59875A990C03E576343C )
example.com.          86400 IN RRSIG DS 8 2 86400 (
                      20150507041537 20150430030537 33878 com.
                      0YnH2wrTYerIUPIaU0t36Ak5GQ7+cXc/0od/UIcsQ7/L
                      WADaqRo4R2bQi5FY6EYn8Egu4eYEw9nuefK7/0GfZEbw
                      WMS2sg/jF+hBTDw+lgRAdvC/q5VJTN1HyTFGamHmWX3a
                      dXS63KmHYIYDlWvEm8ljXHL+Qx4QA4wtU1X3M+Q= )

;; AUTHORITY SECTION:
com.                  172800 IN NS l.gtld-servers.net.
com.                  172800 IN NS a.gtld-servers.net.
com.                  172800 IN NS m.gtld-servers.net.
com.                  172800 IN NS h.gtld-servers.net.
```

Query for DNSSEC Records

```
Terminal - dnsviz@dnsviz-demo: ~/demo
File Edit View Terminal Tabs Help
dnsviz@dnsviz-demo:~/demo$ dig +dnssec +multi example.com

; <<>> DiG 9.9.5-9-Debian <<>> +dnssec +multi example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28162
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;example.com.                IN A

;; ANSWER SECTION:
example.com.                 68544 IN A 93.184.216.34
example.com.                 68544 IN RRSIG A 8 2 86400 (
                             20150508000211 20150430172856 23014 example.com.
                             UZ5/zDpVEKQbZXDb+nhNguaoy0amzibfePuL/jwnZao7
                             UlfyR0g26Fn84xJgXuhJhZVqTRS+vMq1BoniXYoNYx39
                             +TA07zMlltQyTNj2f5Kj1N1agjlrqQFCNTyH0FVpew/
                             xQUpdvfWKN9d7uUqNkN1o5lggz6GPRFe2AJIMSU= )

;; AUTHORITY SECTION:
example.com.                 154943 IN NS b.iana-servers.net.
example.com.                 154943 IN NS a.iana-servers.net.
example.com.                 154943 IN RRSIG NS 8 2 172800 (
                             20150507203440 20150430172856 23014 example.com.
                             W6rGELFY9TkrkzRKQzLAsiDixKjpc39GkXjcfI3If3DB
                             u6ocAgNFuX9Urw4kZ0oAM67Wc8fkMo4QhoGf7Et8DweV
                             7JFGbJD3HlNkswG4X2DIFuQP+2d3PT8YfyBcY9+hU4q
                             h2lLC8YJ+5gXWihqkJcMBhgMmQRX6TILv1IxJgw= )

;; ADDITIONAL SECTION:
```

Query For DNSSEC Records (NSEC)

```
Terminal - dnsviz@dnsviz-demo: ~/demo
File Edit View Terminal Tabs Help
dnsviz@dnsviz-demo:~/demo$ dig +dnssec +multi @a.iana-servers.net foobar.example.com
; <<>> DiG 9.9.5-9-Debian <<>> +dnssec +multi @a.iana-servers.net foobar.example.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 46161
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1
;; WARNING: recursion requested but not available

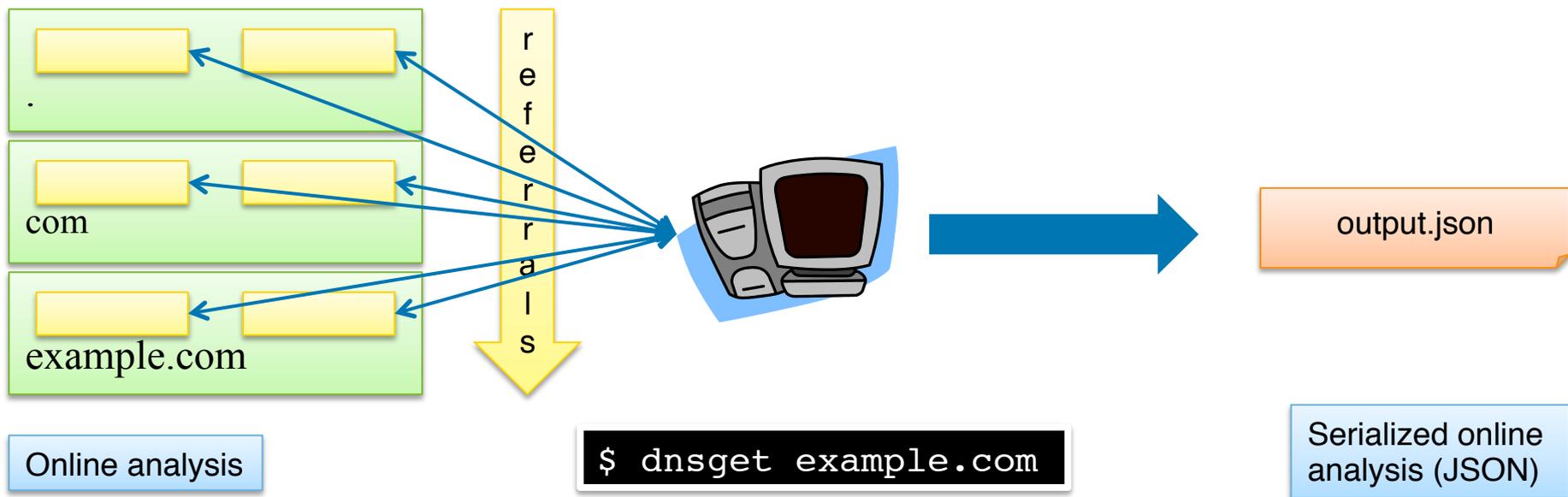
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;foobar.example.com.      IN A

;; AUTHORITY SECTION:
example.com.              3600 IN SOA sns.dns.icann.org. noc.dns.icann.org. (
                           2014121768 ; serial
                           7200      ; refresh (2 hours)
                           3600      ; retry (1 hour)
                           1209600   ; expire (2 weeks)
                           3600      ; minimum (1 hour)
                           )
example.com.              3600 IN RRSIG SOA 8 2 3600 (
                           20150508092402 20150430232918 23014 example.com.
                           if9lkxlgzM7MpCoEmZcRuTDJstIK4wUTyk3FyV96jpLi
                           XzaaGwMBCFc/JTIBbag9XneTqLofcRFwjyX0refuLPev
                           ShMn7fzK804f0HYXTiYi9oSN30XZkCN3E04Id3Uh4VWU
                           DkMxpEyVgeW1wHQiQto6IHA00jyresABcifqCyM= )
example.com.              3600 IN NSEC www.example.com. A NS SOA TXT AAAA RRSIG NSEC DNSKEY
example.com.              3600 IN RRSIG NSEC 8 2 3600 (
                           20150508090714 20150430232918 23014 example.com.
                           Gk85kZ3lUW+pdYXfG72ye4RF5TG9QPU316nWS8AnSDJQ
```

DNSViz

DNS Analysis Using DNSViz (dnstool command line)

- Queries issued
 - Referral queries – to learn delegation NS records from parent
 - NS queries – to learn authoritative NS records
 - DNSKEY/DS queries – for building a DNSSEC chain
 - A/AAAA/TXT/MX/SOA queries
 - Diagnostic queries (special handling of errors, etc.)
- All servers queried
 - IPv4/IPv6
 - UDP/TCP



DNS Analysis Using DNSViz (dnsgrok command line)

- Responses analyzed (offline)

- Responsiveness

- Query timeouts
- Network errors
- EDNS/fragmentation capabilities

- Consistency

- Across servers
- Between DNSKEY/RRSIG
- Between DNSKEY/DS

- Correctness

- RRSIG

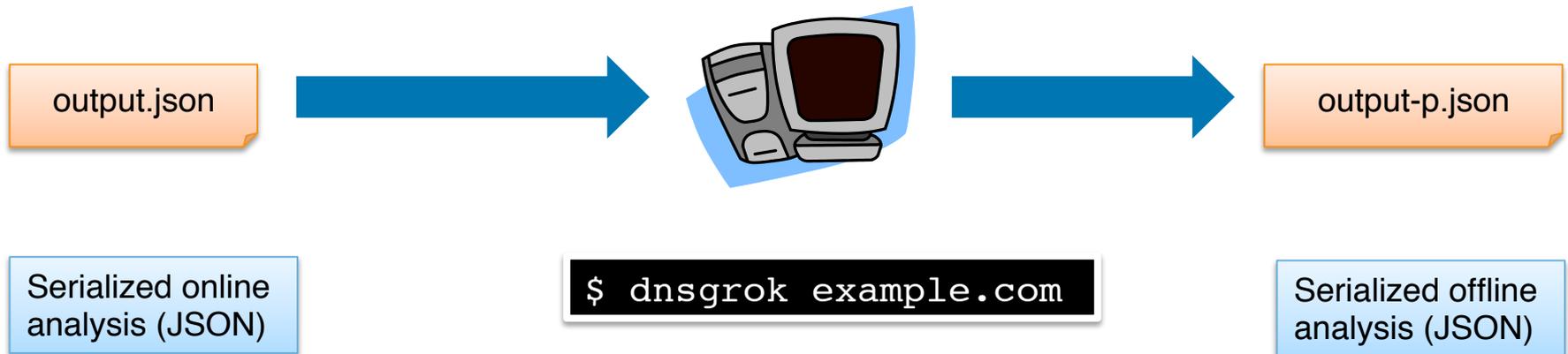
- Expiration/inception dates
- Cryptographic signature

- DS

- Cryptographic hash

- Negative responses

- NSEC proof correctness
- SOA record correctness



DNS Analysis Using DNSViz (dnsviz command line)

- Responses analyzed (offline)

- Responsiveness

- Query timeouts
- Network errors
- EDNS/fragmentation capabilities

- Consistency

- Across servers
- Between DNSKEY/RRSIG
- Between DNSKEY/DS

- Correctness

- RRSIG

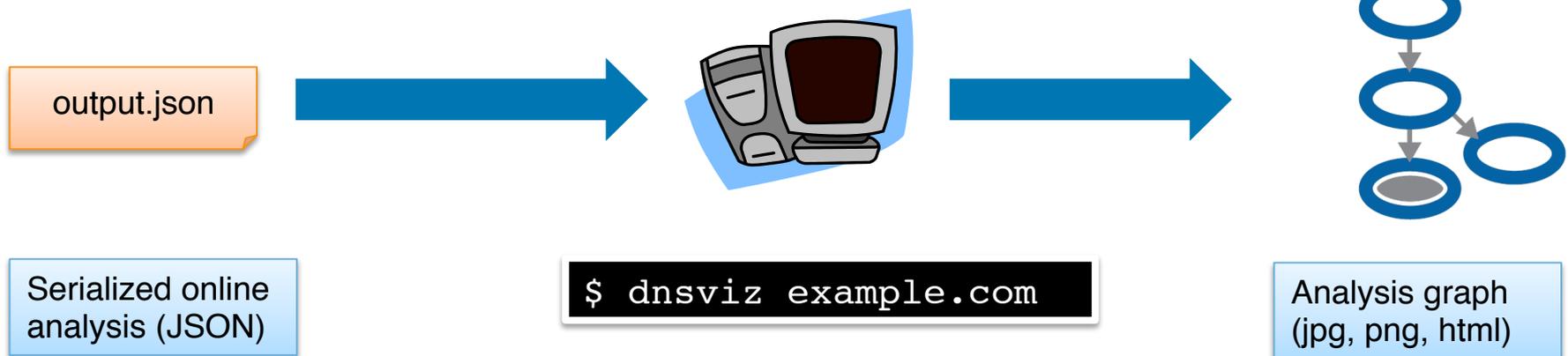
- Expiration/inception dates
- Cryptographic signature

- DS

- Cryptographic hash

- Negative responses

- NSEC proof correctness
- SOA record correctness



Analyze Using dnsget (3.1 – 3.2)

```
$ dnsget -a . -p example.com > example.com.json
```



follow referrals
from root (“.”) to
analyze name



make the output
“pretty” (for
readability)



store analysis in file
called
“example.com.json”

```
$ medit example.com.json &
```

Analyze Using dnsgrok (3.3 – 3.4)

make the output
“pretty” (for readability)



read analysis from
“example.com.json”



```
$ dnsgrok -p example.com < example.com.json \  
> example.com-p.json
```



store analysis in file called
“example.com-p.json”

```
$ medit example.com-p.json
```

Analyze Using dnsgrok (3.5 – 3.6)

show only
information that is
of priority “info” or
higher



```
$ dnsgrok -l info -p example.com < example.com.json \  
> example.com-p1.json
```

```
$ medit example.com-p1.json
```

Analyze Using dnsgrok (3.7)

show only
information that is
of priority "error" or
higher



display output (if
any) to screen,
instead of
redirecting to file



```
$ dnsgrok -l error -p example.com < example.com.json
```

Analyze Using dnsviz (3.8 – 3.11)

```
$ dnsviz -Thtml example.com < example.com.json \  
> example.com.html
```



output interactive
HTML format

```
$ iceweasel example.com.html &
```

```
$ dnsviz -Thtml -t tk.txt example.com < example.com.json \  
> example.com.html
```



anchor trust
with root KSK

```
$ iceweasel example.com.html &
```

View dnstget Output

example.com.json

```
{
  ".": {
    "stub": false,
    "analysis_start": "2015-05-01 01:41:58 UTC",
    "analysis_end": "2015-05-01 01:41:58 UTC",
    "clients_ipv4": [
      "10.0.2.15"
    ],
    "clients_ipv6": [],
    "referral_rdtype": "NS",
    "explicit_delegation": false,
    "auth_ns_ip_mapping": {
      "a.root-servers.net.": [
        "198.41.0.4",
        "2001:503:ba3e::2:30"
      ],
      "b.root-servers.net.": [
        "192.228.79.201",
        "2001:500:84::b"
      ],
      "c.root-servers.net.": [
        "192.33.4.12",
        "2001:500:2::c"
      ],
      "d.root-servers.net.": [
        "199.7.91.13",
        "2001:500:2d::d"
      ],
      "e.root-servers.net.": [
        "192.203.230.10"
      ],
    }
  }
}
```

View dnstget Output

```
example.com.json
{
  "202.12.27.33",
  "2001:dc3::35"
},
"queries": [
  {
    "qname": ".",
    "qclass": "IN",
    "qtype": "NS",
    "options": {
      "flags": 0,
      "edns_version": 0,
      "edns_max_udp_payload": 4096,
      "edns_flags": 32768,
      "edns_options": [],
      "tcp": false
    },
    "responses": {
      "128.63.2.53": {
        "10.0.2.15": {
          "message": "+WCEAAABAA4AAAAZAAACAAEAAAIAAQAH6QAAFAF",
          "msg_size": 913,
          "response_time": 0.045,
          "history": []
        }
      },
      "192.5.5.241": {
        "10.0.2.15": {
          "message": "T++EAAABAA4AAAAZAAACAAEAAAIAAQAH6QAAFAF",
          "msg_size": 913,
          "response_time": 0.088,

```


View dnsgrok Output

```
example.com-p.json
{
  ".": {
    "status": "NOERROR",
    "queries": {
      "./IN/DNSKEY": {
        "answer": [
          {
            "description": "RRset for ./DNSKEY",
            "rrset": {
              "name": ".",
              "ttl": 172800,
              "type": "DNSKEY",
              "rdata": [
                "256 3 8 AwEAAZyIkCwEYeG29NV+4c0dK",
                "257 3 8 AwEAAgAIKlVZrpC6Ia7gEzah"
              ]
            },
            "servers": [
              "128.63.2.53",
              "192.5.5.241",
              "192.33.4.12",
              "192.36.148.17",
              "192.58.128.30",
              "192.112.36.4",
              "192.203.230.10",
              "192.228.79.201",
              "193.0.14.129",
              "198.41.0.4",
              "199.7.83.42",
              "199.7.91.13",
              "202.12.27.33"
            ]
          }
        ]
      }
    }
  }
}
```

View dnsgrok Output

```
example.com-p.json
}
}
},
"dnskey": [
  {
    "description": "DNSKEY for . (algorithm 8 (RS)
    "flags": 256,
    "protocol": 3,
    "algorithm": 8,
    "key": "AwEAAZyIkCwEYeG29NV+4c0dKE4DPng/4BqJec
    "meta": {
      "ttl": 172800,
      "key_length": 1024,
      "key_tag": 48613
    },
    "servers": [
      "128.63.2.53",
      "192.5.5.241",
      "192.33.4.12",
      "192.36.148.17",
      "192.58.128.30",
      "192.112.36.4",
      "192.203.230.10",
      "192.228.79.201",
      "193.0.14.129",
      "198.41.0.4",
      "199.7.83.42",
      "199.7.91.13",
      "202.12.27.33"
    ]
  }
]
```

View dnsgrok Output

example.com-p.json

```
    },
  ],
  "s0m8463hu9.example.com./IN/A": {
    "nxdomain": [
      {
        "proof": [
          {
            "description": "NSEC record(s) proving the non-existence (NX)",
            "nsec": [
              {
                "description": "RRset for example.com./NSEC",
                "rrset": {
                  "name": "example.com.",
                  "ttl": 3600,
                  "type": "NSEC",
                  "rdata": [
                    "www.example.com. A NS SOA TXT AAAA RRSIG NS"
                  ]
                }
              },
            ],
            "rrsig": [
              {
                "description": "RRSIG covering example.com./",
                "rdata": {
                  "signer": "example.com.",
                  "algorithm": 8,
                  "key_tag": 23014,
                  "original_ttl": 3600,
                  "labels": 2,
                  "inception": "2015-04-30 23:29:18 UTC",
                  "expiration": "2015-05-08 09:07:14 UTC",

```

View dnsgrok Output

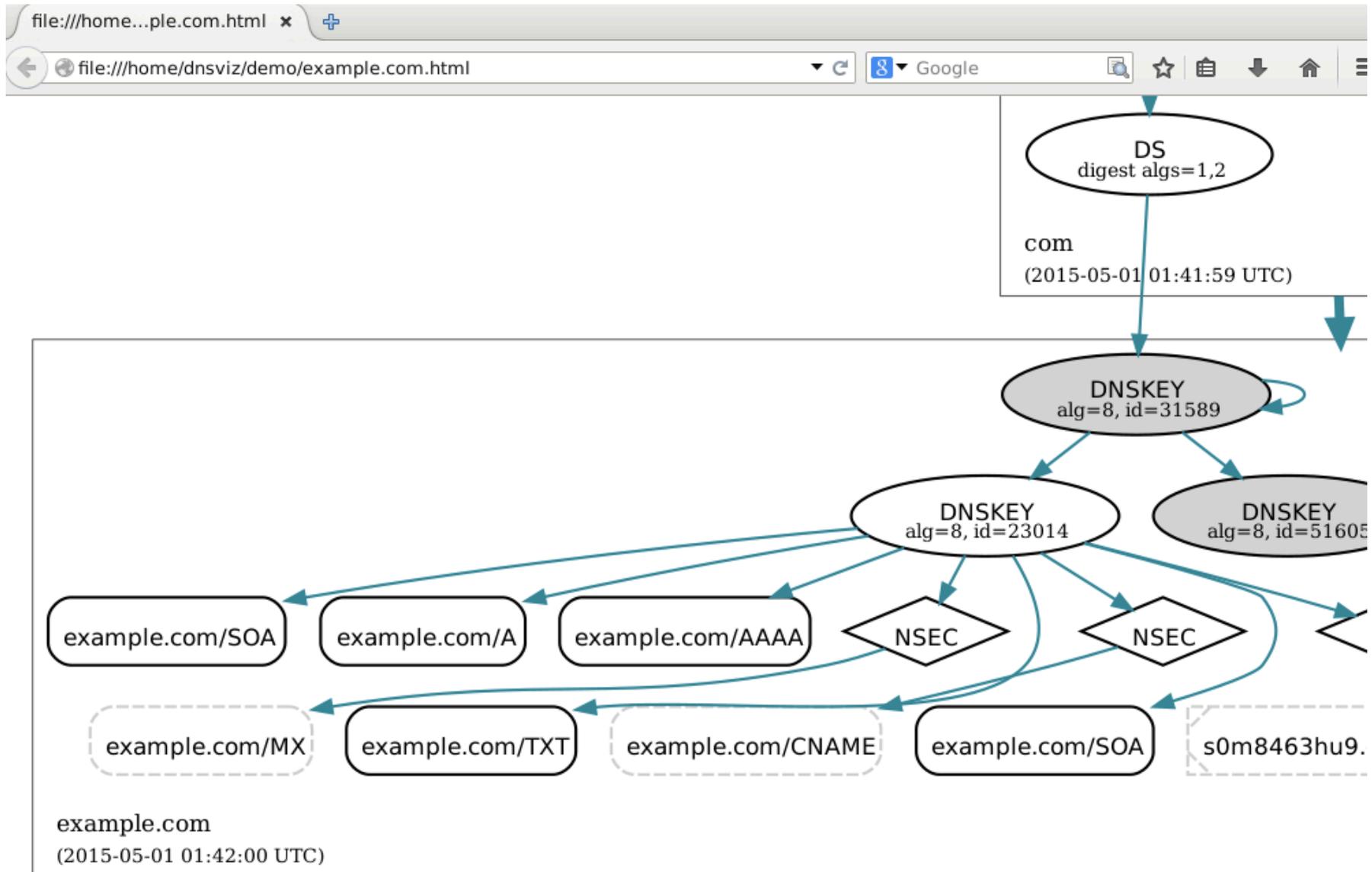
```
example.com-p1.json
{
  ".": {
    "status": "NOERROR",
    "queries": {
      "./IN/DNSKEY": {
        "answer": [
          {
            "description": "RRset for ./DNSKEY",
            "rrsig": [
              {
                "description": "RRSIG covering ./DNSKEY",
                "status": "VALID"
              }
            ]
          }
        ]
      }
    }
  },
  "dnskey": [
    {
      "description": "DNSKEY for . (algorithm 8 (RSA/SHA-256), key tag 48613)"
    },
    {
      "description": "DNSKEY for . (algorithm 8 (RSA/SHA-256), key tag 19036)"
    }
  ]
},
  "com.": {
    "status": "NOERROR",
    "queries": {
      "com./IN/DS": {
```

View dnsgrok Output

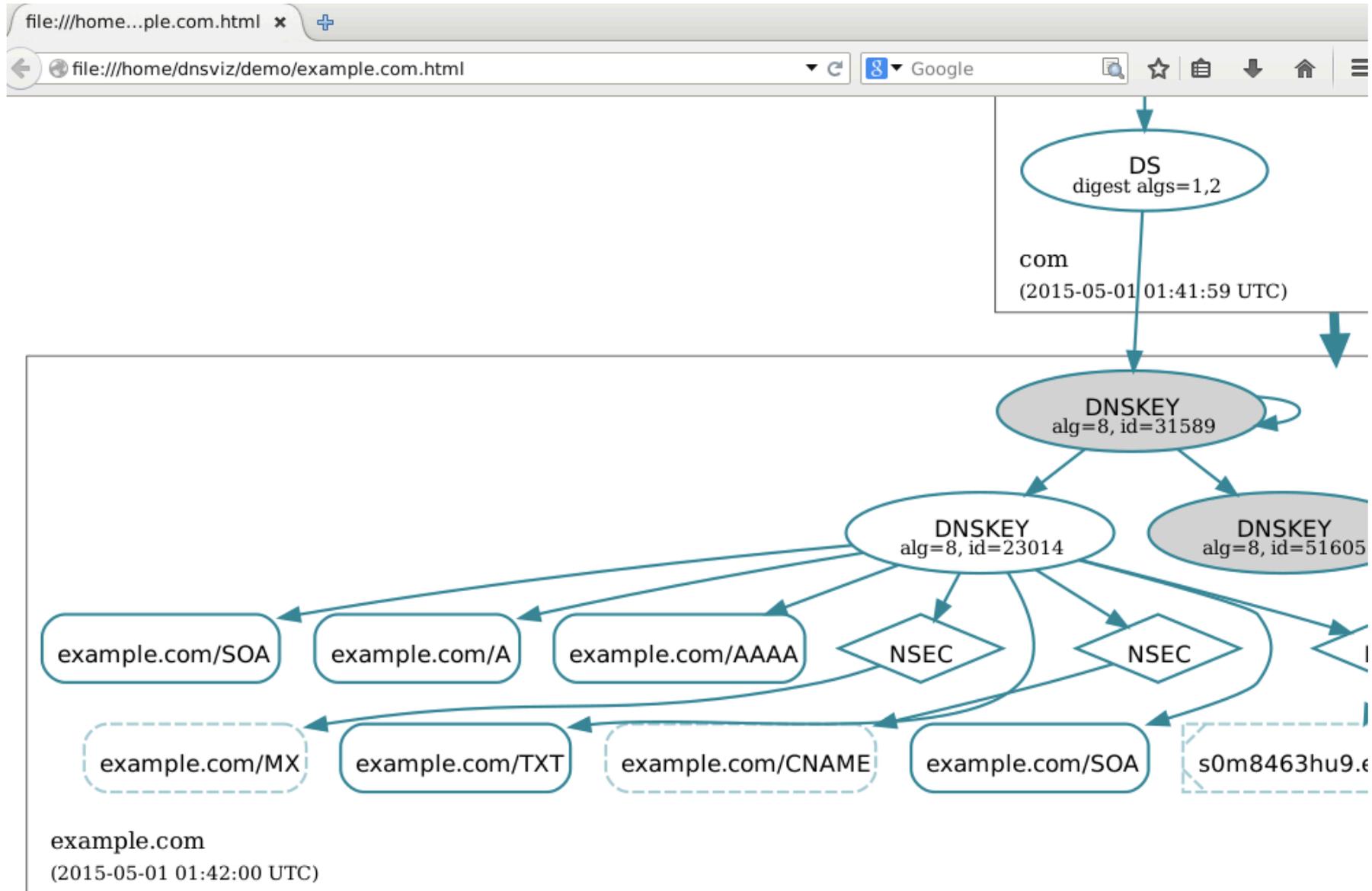
example.com-pl.json

```
{
  "description": "DNSKEY for com. (algorithm 8 (RSA/SHA-256), key tag 33878)"
},
"delegation": {
  "ds": [
    {
      "description": "DS record(s) corresponding to DNSKEY for com. (algorithm
      "status": "VALID"
    }
  ],
  "status": "SECURE"
}
},
"example.com.": {
  "status": "NOERROR",
  "queries": {
    "example.com./IN/A": {
      "answer": [
        {
          "description": "RRset for example.com./A",
          "rrsig": [
            {
              "description": "RRSIG covering example.com./A",
              "status": "VALID"
            }
          ]
        }
      ]
    }
  ]
},
"example.com./IN/NS": {
```

View dnsviz Output



View dnsviz Output



Signing a DNS Zone

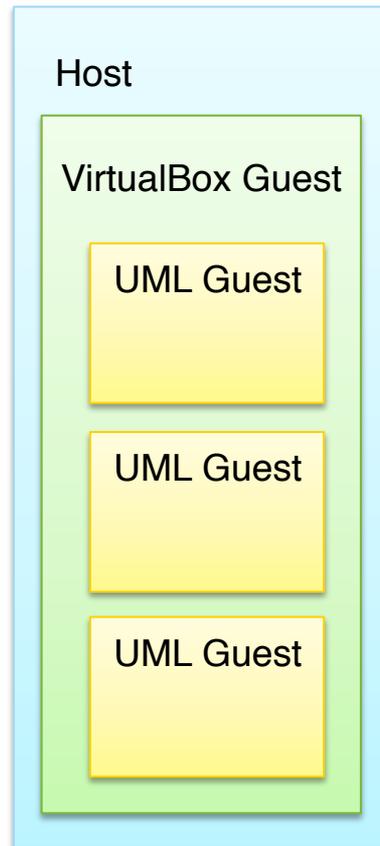
Setup Virtual DNS Environment (4.1 – 4.2)

```
$ ./start_all
```

(Wait for all three
consoles to come up)

Change directory for
all three consoles:
root, tld1, sld1

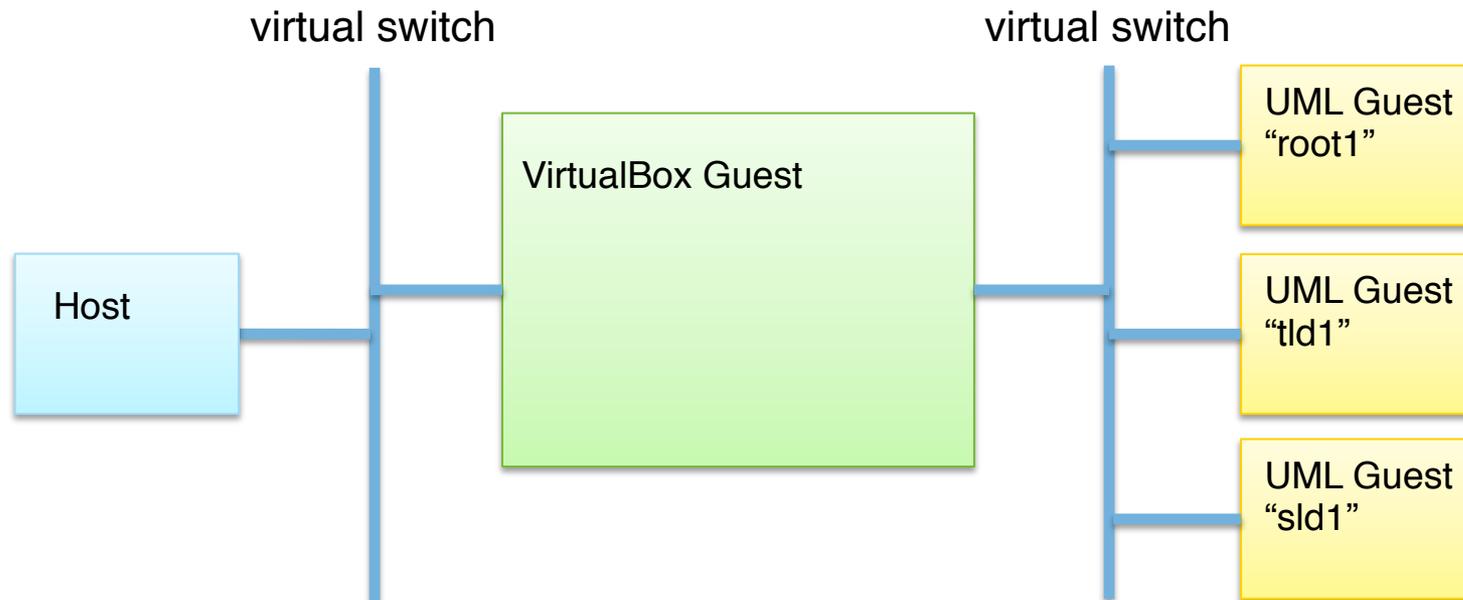
```
$ cd /etc/bind
```



Setup Virtual DNS Environment (4.3)

```
$ ./dns_change_root local
```

(point DNS root hints and trusted keys to internal root server)



Analyze example.com in Local Environment (4.4 – 4.6)

Specify addresses for alternate (local) root servers



Specify internal (local) IPv4 address to bind to



```
$ dnsget -a . -x .:root1=192.168.213.9 -4 192.168.213.1 \  
-6 fd02:f00d::1 example.com | \  
dnsviz -Thtml -O -t tk-local.txt example.com
```



Specify internal (local) IPv6 address to bind to

Pipe results directly to dnsviz, rather than redirecting to file

Output analysis to file named "example.com.html"

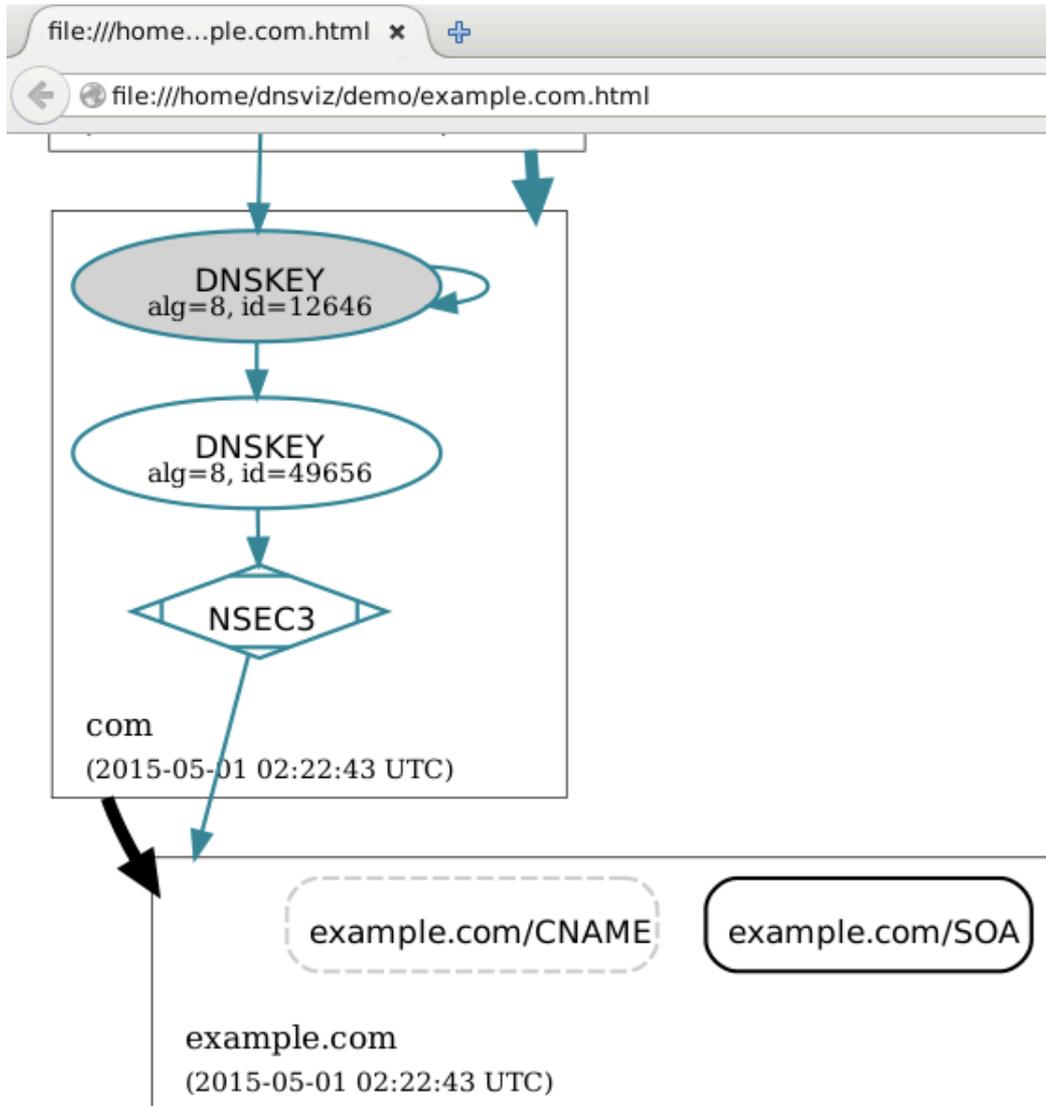
Use local trust anchor, rather than the one for the public root

```
$ ./dnsviz_analyze example.com
```

(script included for simplification)

```
$ iceweasel example.com.html &
```

View dnsviz Output



Add Records to example.com Zone (5.1 – 5.4)

- Add A records for names “a”, “c”, and “e” (on **sld1**)
(hint: see existing record for “www”)

```
# nano db.example.com
```

or

```
# vi db.example.com
```

- Check zone

```
# named-checkzone example.com db.example.com
```

- Reload zone

```
# service bind9 reload
```

- Check that record shows up (query from VirtualBox guest)

```
$ dig @sld1 a.example.com
```

Add Records to example.com Zone

```
Virtual Console #1 (sld1)
File Edit View Terminal Tabs Help
GNU nano 2.2.6 File: db.example.com Modified
$TTL      300
@         IN      SOA      a.local-sld-servers.net. root.localhost. (
                        2          ; Serial
                        300         ; Refresh
                        150         ; Retry
                        600         ; Expire
                        300 )       ; Negative Cache TTL

         IN      NS       a.local-sld-servers.net.
;; Uncomment to enable secondary
;         IN      NS       b.local-sld-servers.net.

         IN      A        192.168.213.3
         AAAA     fd02:f00d::3
www      IN      A        192.168.213.3
         AAAA     fd02:f00d::3
a        IN      A        192.168.1.2
c        IN      A        192.168.1.3
e        IN      A        192.168.1.5
Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?
Y Yes
N No      ^C Cancel
```

Add Records to example.com Zone

```
Terminal - dnsviz@dnsviz-demo: ~/demo
File Edit View Terminal Tabs Help
dnsviz@dnsviz-demo:~/demo$ dig @sld1 a.example.com

; <<>> DiG 9.9.5-9-Debian <<>> @sld1 a.example.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13020
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;a.example.com.                IN      A

;; ANSWER SECTION:
a.example.com.                 300    IN      A      192.168.1.2

;; AUTHORITY SECTION:
example.com.                   300    IN      NS     a.local-sld-servers.net.

;; Query time: 0 msec
;; SERVER: fd02:f00d::25#53(fd02:f00d::25)
;; WHEN: Fri May 01 08:43:23 EDT 2015
;; MSG SIZE rcvd: 95
```

Create DNSSEC Keys for example.com Zone (6.1 – 6.3)

(on **sld1**)

Set the “SEP”
bit for this
DNSKEY



Use algorithm
RSASHA256
for signing



Create a
2048-bit key



```
# KSK=`dnssec-keygen -n ZONE -f KSK -a RSASHA256 -b 2048 \  
-r /dev/urandom example.com`
```

No “SEP” bit
here



Create a
1024-bit key



```
# ZSK=`dnssec-keygen -n ZONE -a RSASHA256 -b 1024 \  
-r /dev/urandom example.com`
```

```
# ls $KSK* $ZSK*
```

Add DNSKEY Records to example.com Zone (6.4 – 6.9)

- Look at DNSKEY records (on **sld1**):

```
# cat Kexample.com*key
```

- Add DNSKEY records to zone

```
# cat Kexample.com*key >> db.example.com
```

- Reload zone

```
# service bind9 reload
```

- Re-analyze

```
$ ./dnsviz_analyze example.com
```

```
$ iceweasel example.com.html &
```

```
$ dig +noall +comment +ad example.com
```

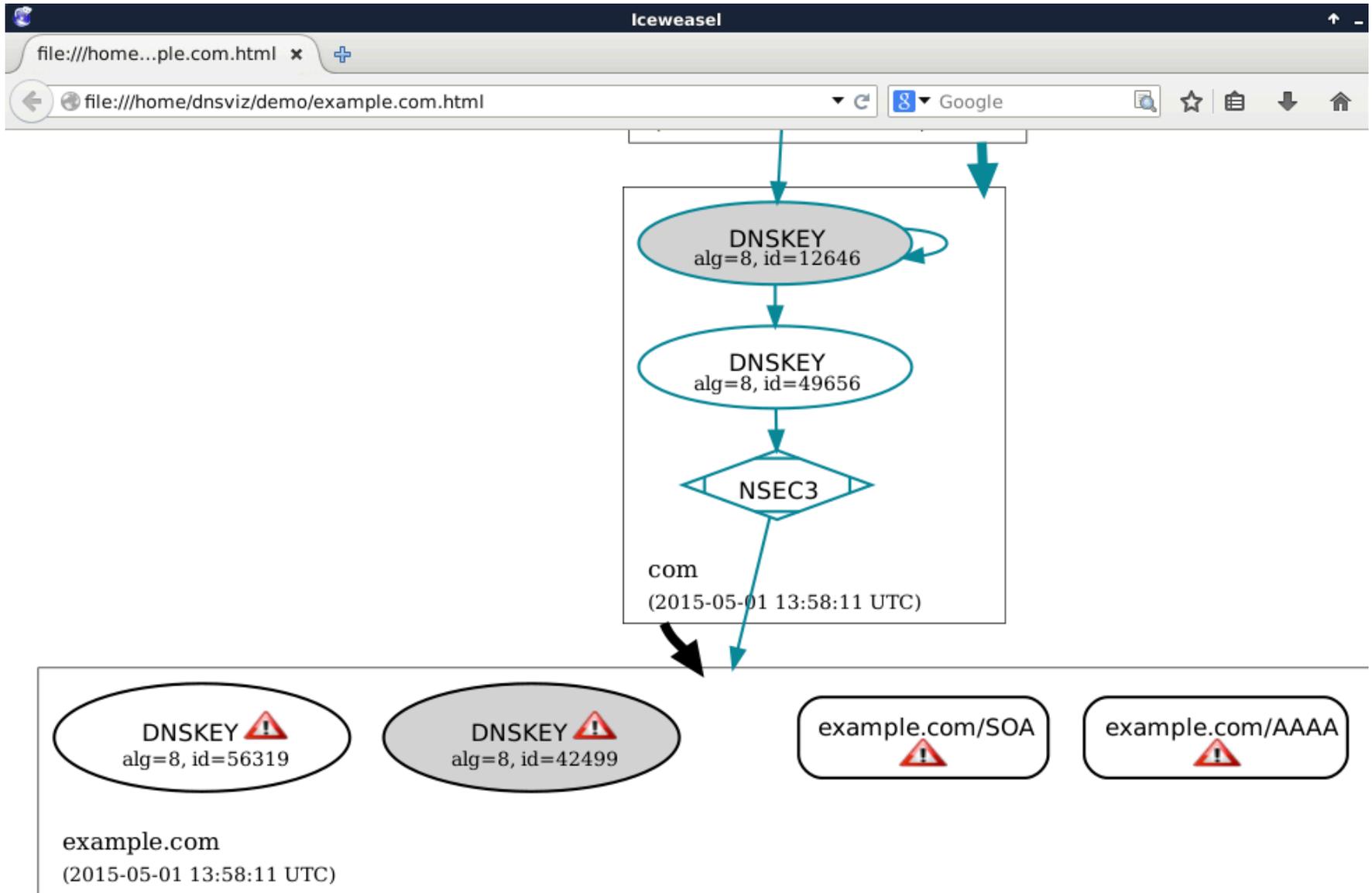
Create DNSSEC keys for example.com

```
Virtual Console #1 (sld1)
File Edit View Terminal Tabs Help
root@sld1:/etc/bind# KSK=`dnssec-keygen -n ZONE -f KSK -a RSASHA256 -b 2048 \
> -r /dev/urandom example.com`
Generating key pair.....
.....+++ ...+++
root@sld1:/etc/bind# ZSK=`dnssec-keygen -n ZONE -a RSASHA256 -b 1024 -r /dev/ura
ndom example.com`
Generating key pair.....+++++ .....+++++
root@sld1:/etc/bind# ls $KSK* $ZSK*
Kexample.com.+008+42499.key      Kexample.com.+008+56319.key
Kexample.com.+008+42499.private  Kexample.com.+008+56319.private
root@sld1:/etc/bind# █
```

Create DNSSEC keys for example.com

```
Virtual Console #1 (sld1)
File Edit View Terminal Tabs Help
root@sld1:/etc/bind# cat $KSK.key $ZSK.key
; This is a key-signing key, keyid 42499, for example.com.
; Created: 20150501124519 (Fri May 1 08:45:19 2015)
; Publish: 20150501124519 (Fri May 1 08:45:19 2015)
; Activate: 20150501124519 (Fri May 1 08:45:19 2015)
example.com. IN DNSKEY 257 3 8 AwEAAckRTKcWx4aZHdBpdtjxZ3wGPgQS6x6DHwYfhuKYf9M5k
p0Ij5Z2 FtvYwFeHe4aXhXrorpKmZj5Z6rytJsY4eicuJiJ3Q67XV4Ht7SMRdZz 0M2S32lyQdZGslo
YEAonI+H14y10QcuU2YblcPS+ovvwkeXMDBmqftNu J/Lusfd8/UmPRs9sBXMM4KTfU/MexgzmJCsmtk
91MBrtSuEi/RQj+hr3 iK7pDctie+9rIrdlBn+Yey3ZgnqWJQEtwxS2klZCdKkZ5fbCbsgouVQp UBh5
WpQI+4jEMaVtF1C6MYbAlT3lGMjXi0aESoIyW30fTNxMdlTjB6jy flAE2mH4f0M=
; This is a zone-signing key, keyid 56319, for example.com.
; Created: 20150501124534 (Fri May 1 08:45:34 2015)
; Publish: 20150501124534 (Fri May 1 08:45:34 2015)
; Activate: 20150501124534 (Fri May 1 08:45:34 2015)
example.com. IN DNSKEY 256 3 8 AwEAAAdswNMsquwbpUpoDk6YyG+lzNCHiMgn3Q0B4p1xPmab/
TXmTFWT 35Icz9RAk6eBmdYCoC0l+tdQQ4v7WESqW/M5MzMNpGxqvKKA5qvTGH1N 0h3tx/JpKBXK7Ax
P6m44NeVX0NVbbpZw3vPipcZi+swYxXlBne6prsZf dM00K4m3
root@sld1:/etc/bind#
```

View dnsviz Output: DNSKEYs with no RRSIGs



View dig Output: no AD bit

```
Terminal - dnsviz@dnsviz-demo: ~/demo
File Edit View Terminal Tabs Help
dnsviz@dnsviz-demo:~/demo$ dig +noall +comment +ad example.com
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51191
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
dnsviz@dnsviz-demo:~/demo$
```

Sign Records in example.com Zone (7.1 – 7.4)

- Sign zone (**sld1**)  Use pseudo-random entropy source (**not for production use**)

```
# dnssec-signzone -r /dev/urandom \  
-k $KSK -o example.com db.example.com $ZSK
```

 Sign only DNSKEY records with this key

 Sign entire zone with this key

- Point named.conf to signed zone file

```
# sed -i -e 's:/db.example.com:&.signed:' named.conf.local
```

- Reload zone

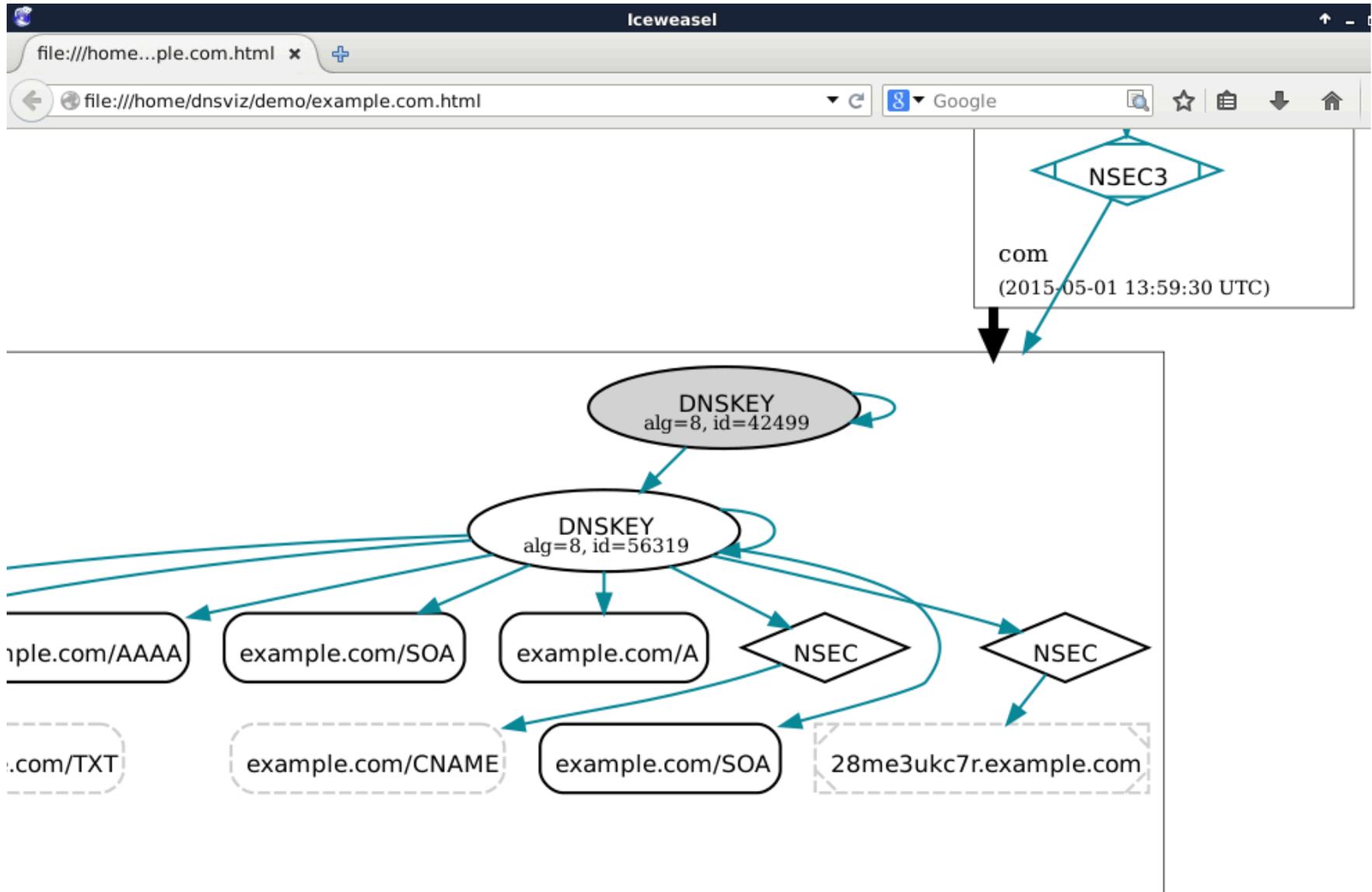
```
# service bind9 reload
```

```
$ ./dnsviz_analyze example.com
```

```
$ iceweasel example.com.html &
```

```
$ dig +noall +comment +ad example.com
```

View dnsviz Output: Signed example.com Zone



View dig Output: no AD bit

```
Terminal - dnsviz@dnsviz-demo: ~/demo
File Edit View Terminal Tabs Help
dnsviz@dnsviz-demo:~/demo$ dig +noall +comment +ad example.com
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51191
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
dnsviz@dnsviz-demo:~/demo$ █
```

Generate DS Records for example.com (8.1 – 8.2)

- Create/copy DS records (on **sld1**)

```
# dnssec-dsfromkey $KSK
```

```
Virtual Console #1 (sld1)
File Edit View Terminal Tabs Help
root@sld1:/etc/bind# dnssec-dsfromkey $KSK
example.com. IN DS 42499 8 1 A78D6AFC5BB9157485229A98
example.com. IN DS 42499 8 2 019EF195EC0E047B45880436
DEB10C94A6024
root@sld1:/etc/bind#
```

```
Virtual Console #1 (sld1)
File Edit View Terminal Tabs Help
root@sld1:/etc/bind# dnssec-dsfromkey $KSK
example.com. IN DS 42499 8 1 A78D6AFC5BB9157485229A98
example.com. IN DS 42499 8 2 019EF195EC0E047B45880436
DEB10C94A6024
root@sld1:/etc/bind#
```

Add DS Records for example.com (8.3a – 8.3c)

- Add DS records to “example” zone (on **tld1**)

```
# nano dsset-example.com.
```

The image shows a Virtual Console window titled "Virtual Console #1 (tld1)". The main window displays the nano editor with the file "dsset-example.com." open. A context menu is open over the editor, showing options: Copy (Shift+Ctrl+C), Paste (Shift+Ctrl+V), Paste Selection, Select All (Shift+), and Preferences... The nano editor content shows two lines of text:

```
example.com. IN DS 42499 8 1 A78D6AFC5BB9157485229A981488C49163C967B2
example.com. IN DS 42499 8 2 019EF195EC0E047B458804367ECE854B57CBDB2738BD9732EF$
```

A confirmation dialog is displayed at the bottom of the nano editor, asking: "Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?". The options are Y Yes, N No, and ^C Cancel.

Sign Records in “example.com” Zone (8.4 – 8.5)

- Sign zone (on **tld1**)

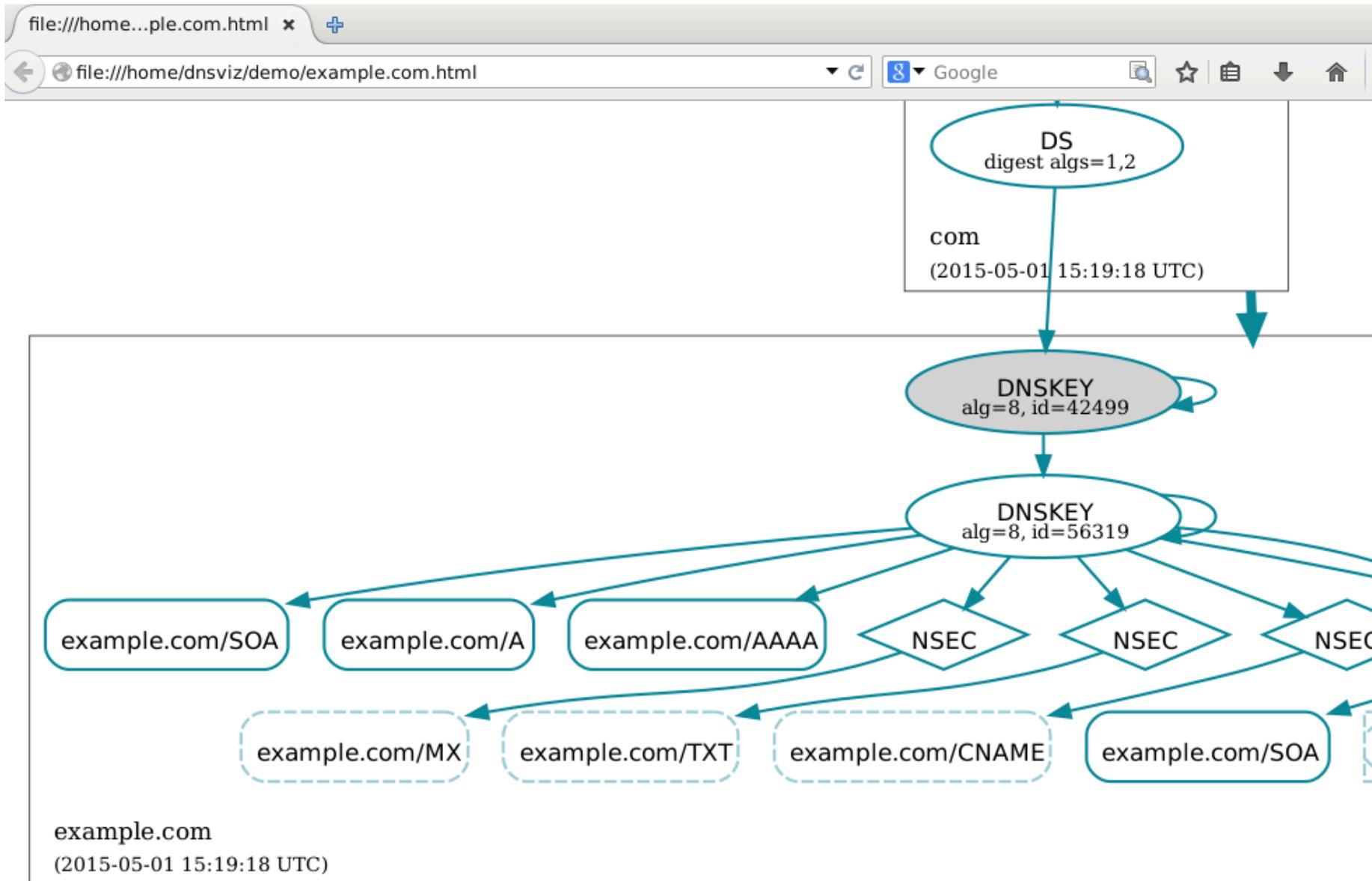
```
# ./resign_tld
```

```
$ ./dnsviz_analyze example.com
```

```
$ iceweasel example.com.html &
```

```
$ dig +noall +comment +ad example.com
```

View dnsviz Output: Full Chain of Trust



View dig Output: AD bit

```
Terminal - dnsviz@dnsviz-demo: ~/demo
File Edit View Terminal Tabs Help
dnsviz@dnsviz-demo:~/demo$ dig +noall +comment +ad example.com
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50710
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
dnsviz@dnsviz-demo:~/demo$
```

Fun with DNSViz

Use KSK to Only Sign DNSKEY RRset (9.1 – 9.3)

Don't sign zone
data with KSK



```
# dnssec-signzone -x -r /dev/urandom \  
-k $KSK -o example.com db.example.com $ZSK
```

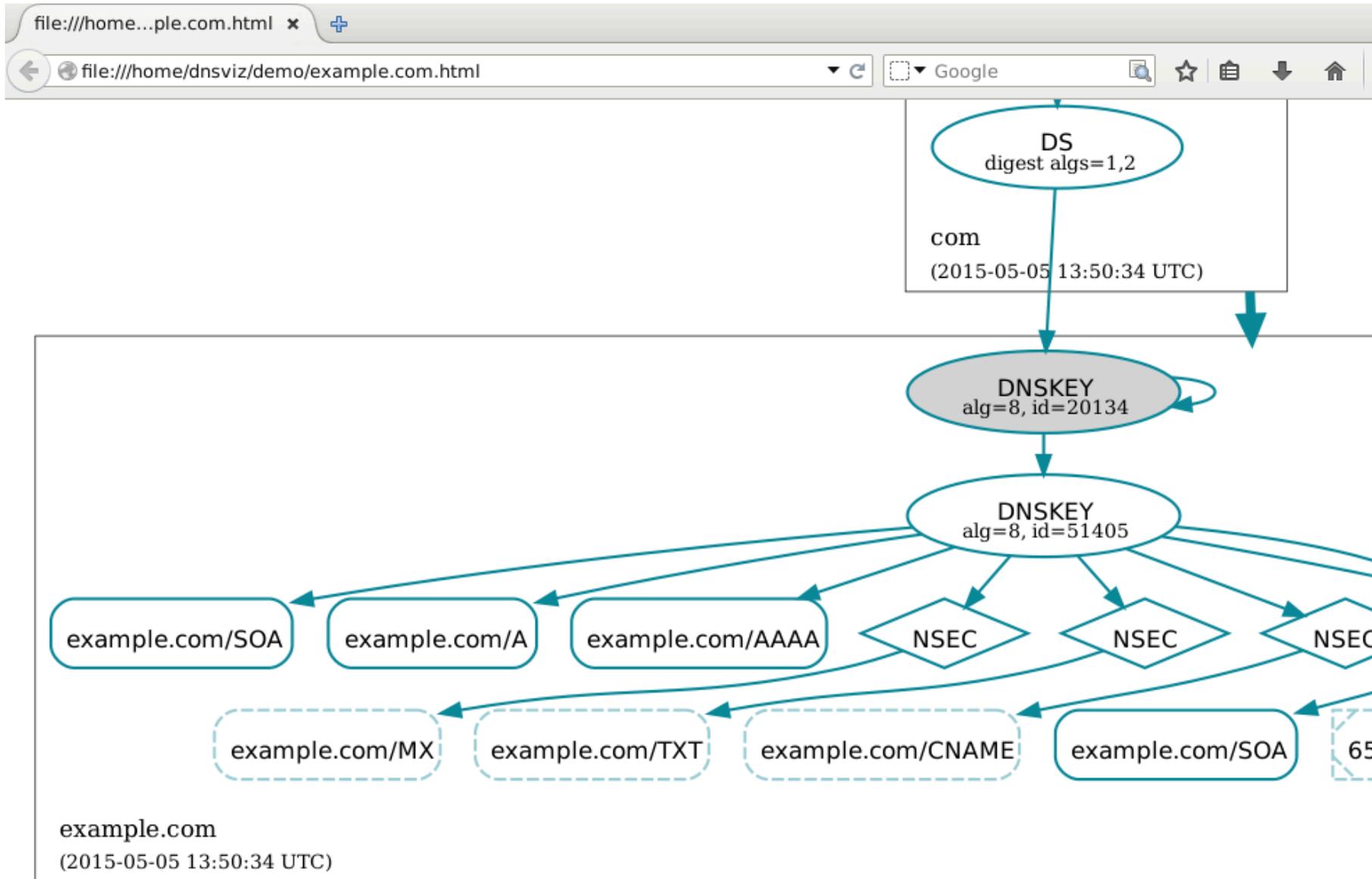
```
# service bind9 reload
```

```
$ ./dnsviz_analyze example.com
```

```
$ iceweasel example.com.html &
```

```
$ dig +noall +comment +ad example.com
```

View dnsviz Output: KSK-only



View dig Output: AD bit

```
Terminal - dnsviz@dnsviz-demo: ~/demo
File Edit View Terminal Tabs Help
dnsviz@dnsviz-demo:~/demo$ dig +noall +comment +ad example.com
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26165
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
dnsviz@dnsviz-demo:~/demo$
```

Add New KSK to example.com Zone (9.4 – 9.8)

- Generate new KSK:

```
# NEWKSK=`dnssec-keygen -n ZONE -f KSK -a RSASHA256 -b 2048 \  
-r /dev/urandom example.com`
```

```
# cat $NEWKSK.key >> db.example.com
```

- Re-sign zone:

```
# dnssec-signzone -x -r /dev/urandom \  
-k $KSK -o example.com db.example.com $ZSK
```

- Reload zone

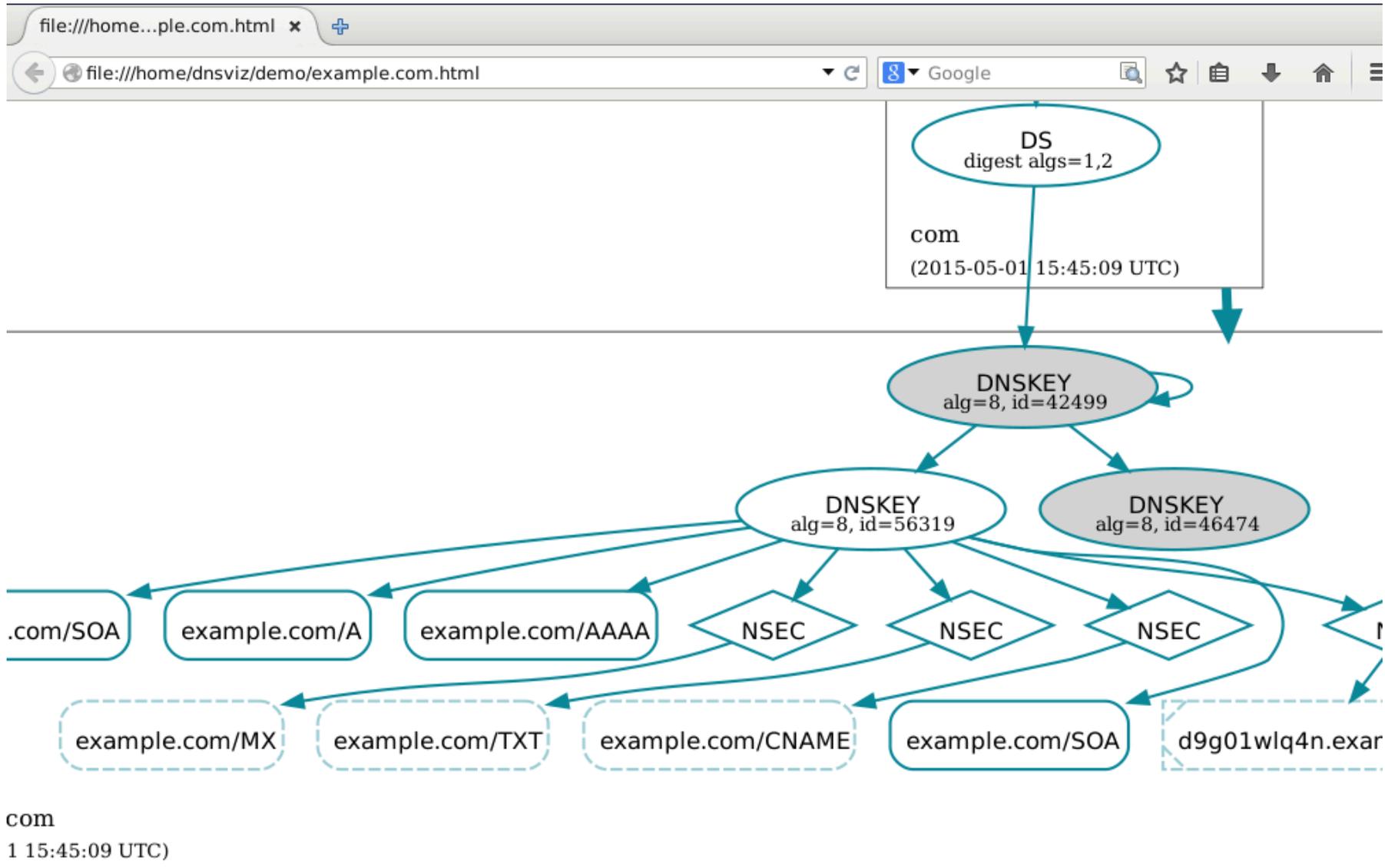
```
# service bind9 reload
```

```
$ ./dnsviz_analyze example.com
```

```
$ iceweasel example.com.html &
```

```
$ dig +noall +comment +ad example.com
```

View dnsviz Output: Standby KSK



View dig Output: AD bit

```
Terminal - dnsviz@dnsviz-demo: ~/demo
File Edit View Terminal Tabs Help
dnsviz@dnsviz-demo:~/demo$ dig +noall +comment +ad example.com
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26165
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
dnsviz@dnsviz-demo:~/demo$ █
```

Add New KSK to example.com Zone (9.9 – 9.11)

- Re-sign zone with two KSKs:

```
# dnssec-signzone -x -r /dev/urandom \  
-k $KSK -k $NEWKSK -o example.com db.example.com $ZSK
```

- Reload zone

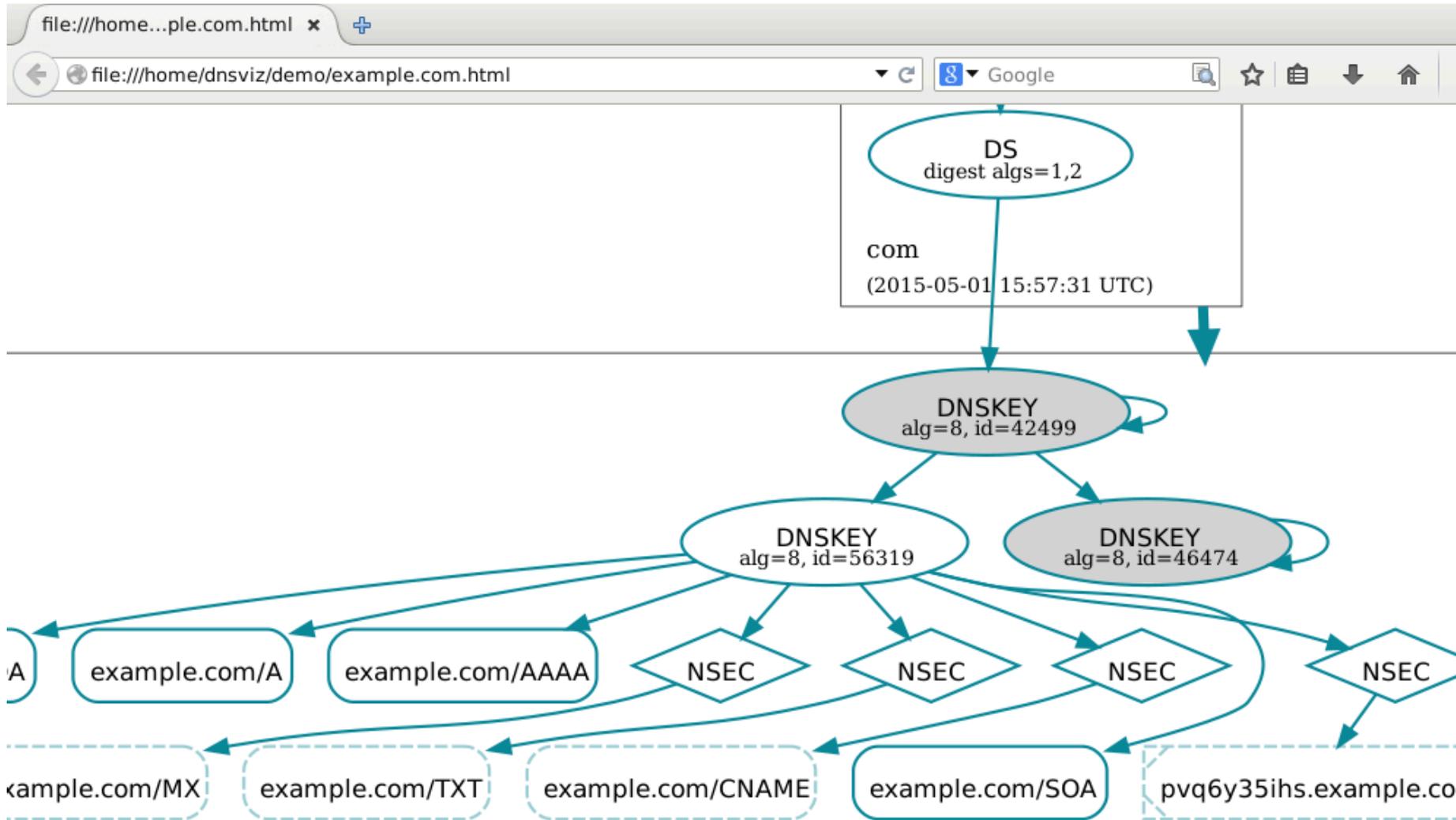
```
# service bind9 reload
```

```
$ ./dnsviz_analyze example.com
```

```
$ iceweasel example.com.html &
```

```
$ dig +noall +comment +ad example.com
```

View dnsviz Output: Multiple KSKs



View dig Output: AD bit

```
Terminal - dnsviz@dnsviz-demo: ~/demo
File Edit View Terminal Tabs Help
dnsviz@dnsviz-demo:~/demo$ dig +noall +comment +ad example.com
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26165
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
dnsviz@dnsviz-demo:~/demo$ █
```

Change KSK for example.com Zone (9.12 – 9.14)

- Sign with only the second KSK:

```
# dnssec-signzone -x -r /dev/urandom \  
-k $NEWKSK -o example.com db.example.com $ZSK
```

- Reload zone

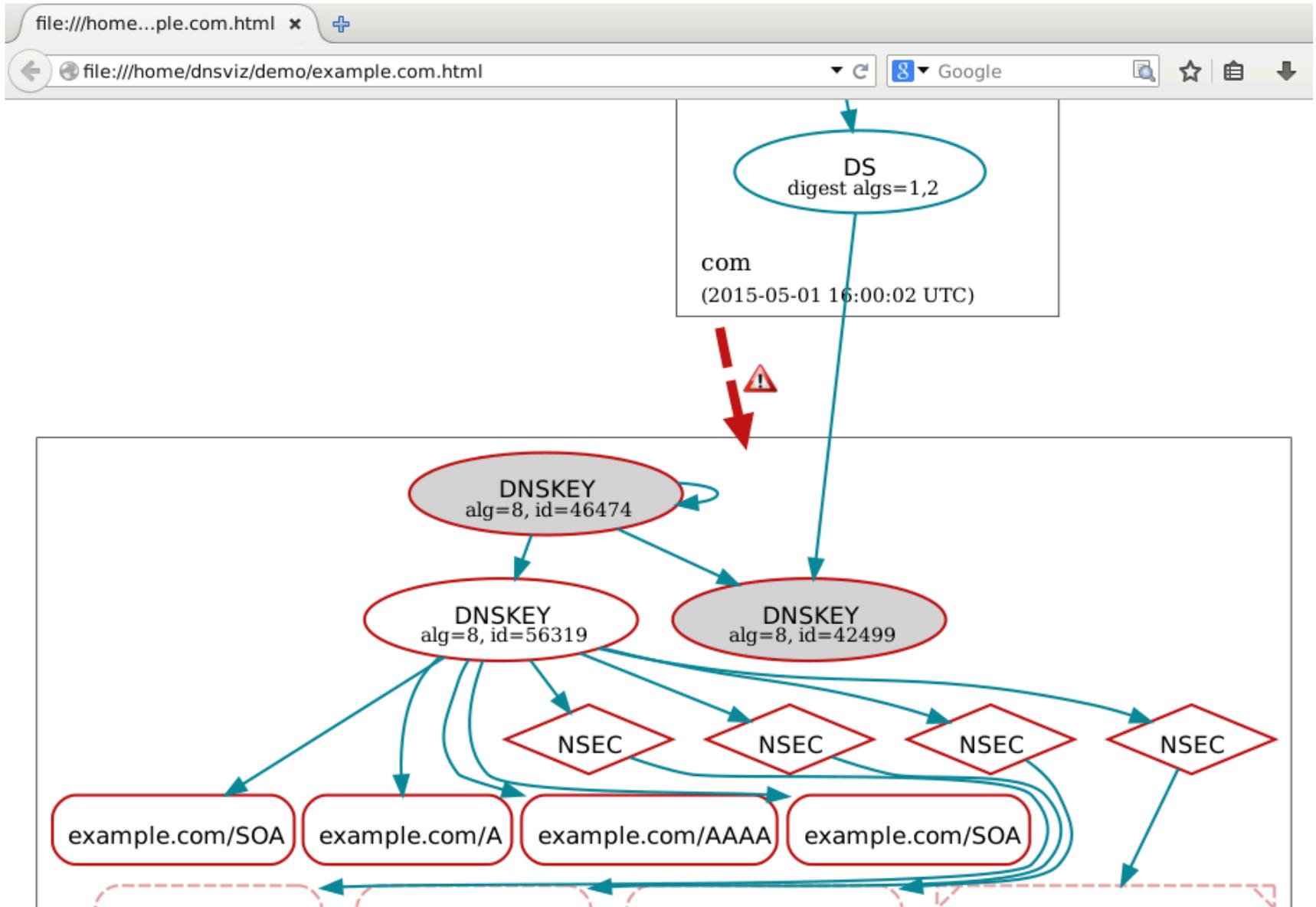
```
# service bind9 reload
```

```
$ ./dnsviz_analyze example.com
```

```
$ iceweasel example.com.html &
```

```
$ dig +noall +comment +ad example.com
```

View dnsviz Output: DS Mismatch



View dig Output: SERVFAIL

```
Terminal - dnsviz@dnsviz-demo: ~/demo
File Edit View Terminal Tabs Help
dnsviz@dnsviz-demo:~/demo$ dig +noall +comment +ad example.com
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 52392
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
dnsviz@dnsviz-demo:~/demo$
```

Tamper with Record Content (9.15 – 9.17)

- Change SOA record:

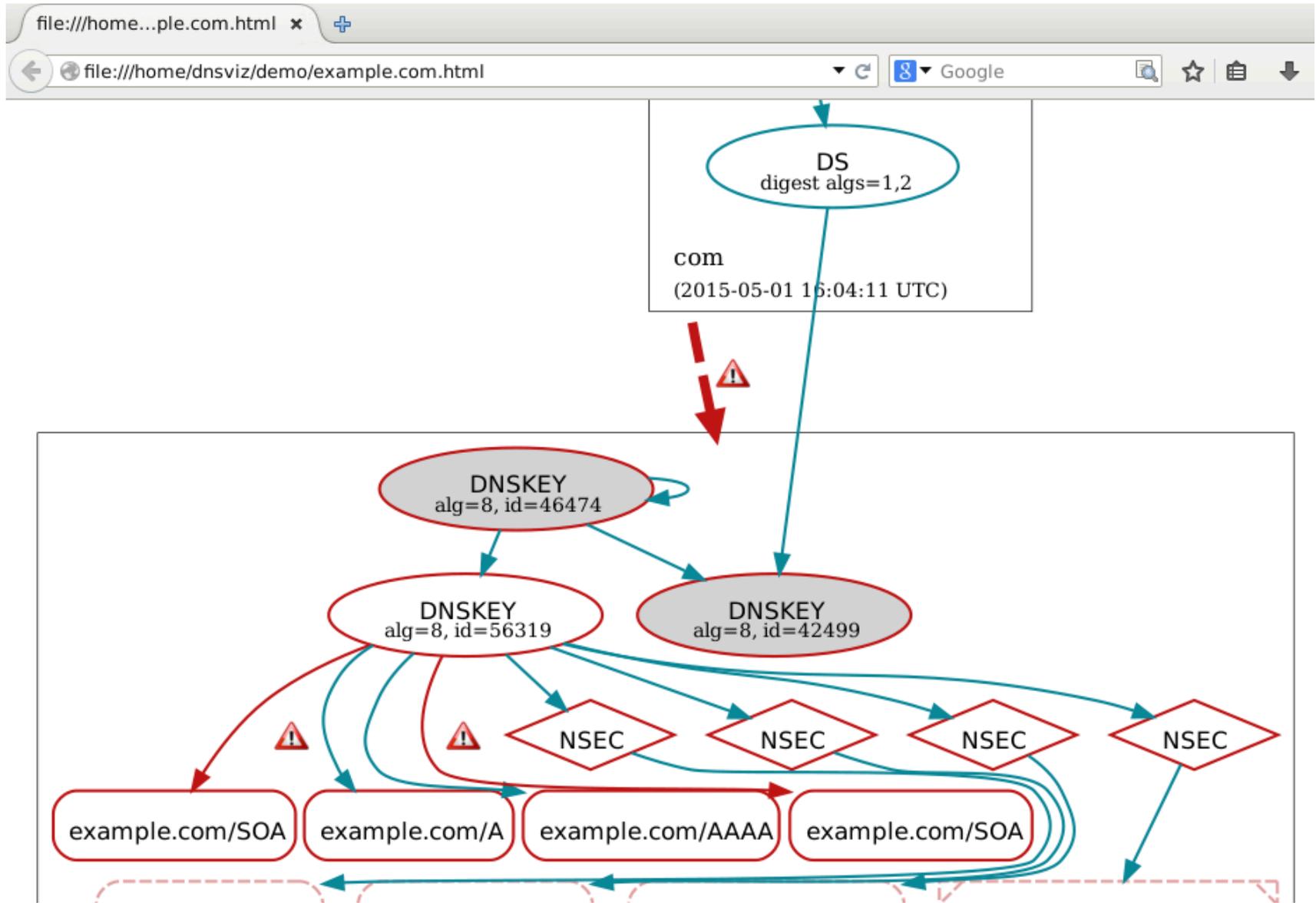
```
# sed -i -e 's/root.localhost/root1.localhost/' \
  db.example.com.signed
```

```
# service bind9 reload
```

```
$ ./dnsviz_analyze example.com
```

```
$ iceweasel example.com.html &
```

View dnsviz Output: Invalid Signatures



Change RRSIG Expiration (9.18 – 9.21)

- Set the RRSIG expiration explicitly to 1 second from “now”

```
# dnssec-signzone -x -e now+1 -r /dev/urandom \  
-k $NEWKSK -o example.com db.example.com $ZSK
```

- Manipulate (again) SOA record

```
# sed -i -e 's/root.localhost/root1.localhost/' \  
db.example.com.signed
```

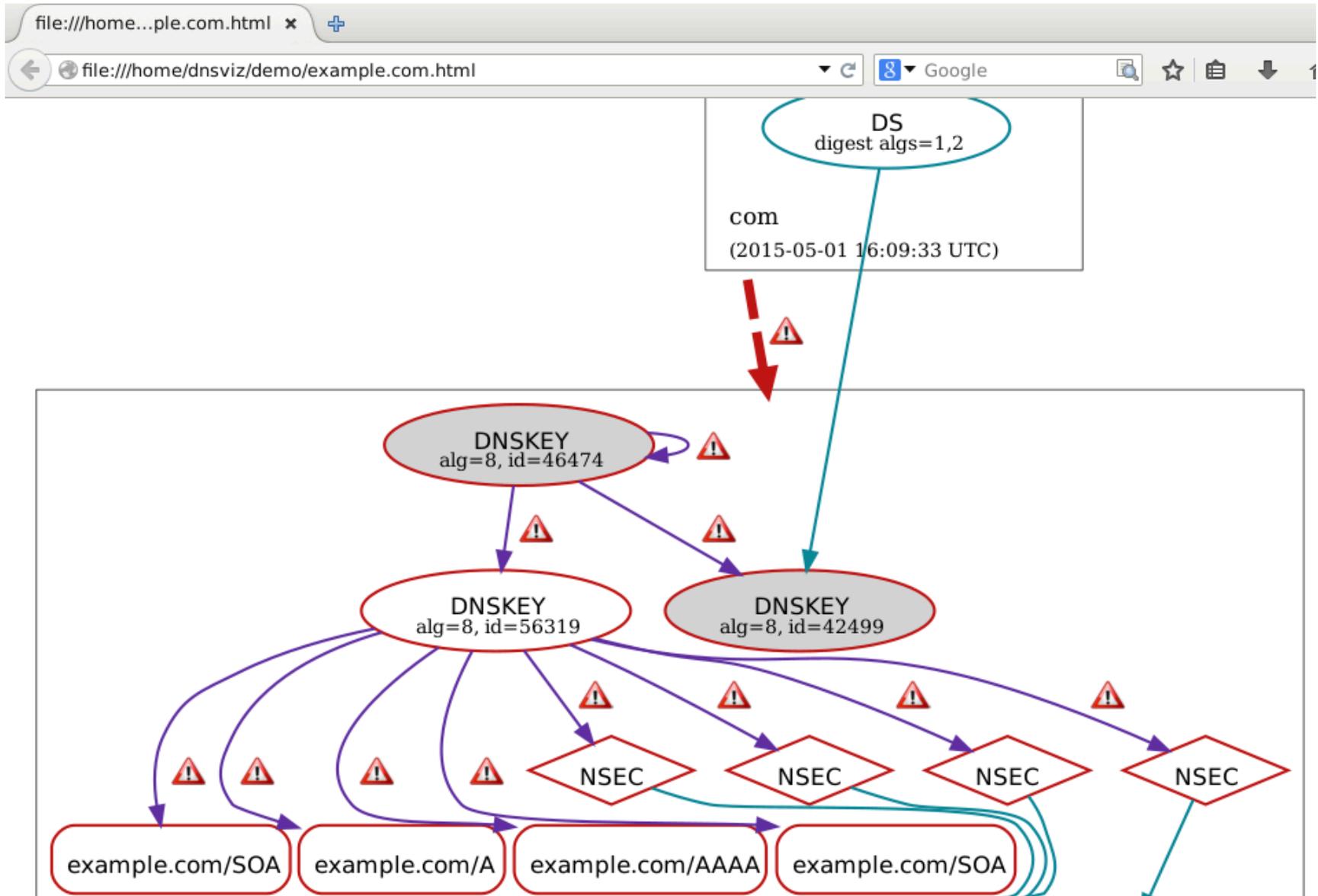
- Reload zone

```
# service bind9 reload
```

```
$ ./dnsviz_analyze example.com
```

```
$ iceweasel example.com.html &
```

View dnsviz Output: Expired RRSIGs



Modify Path MTU (9.22 – 9.23)

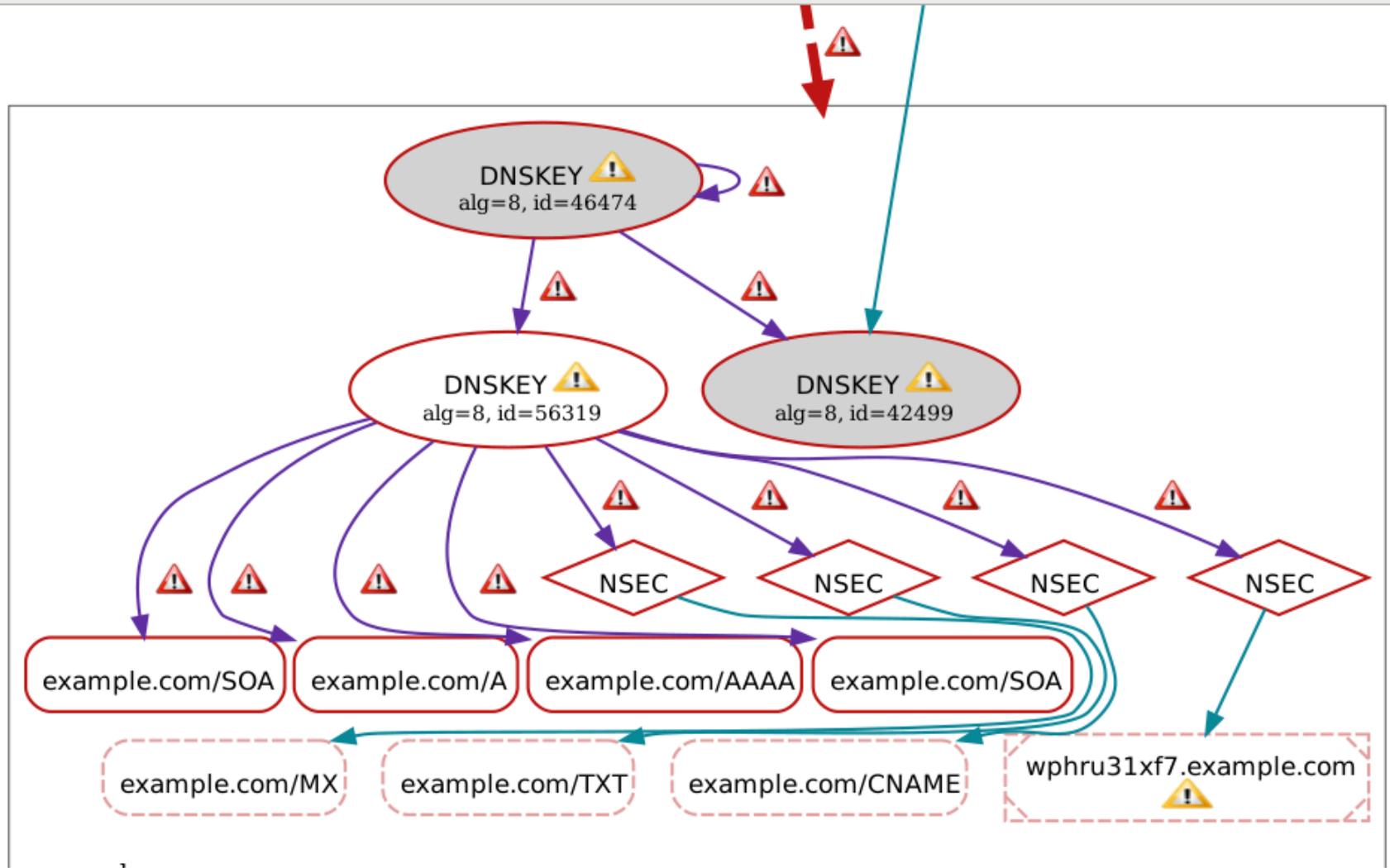
- Drop UDP responses with payloads larger than 512 bytes

```
# iptables -A OUTPUT -p udp --sport 53 \  
-m length --length 540:65535 -j DROP
```

```
$ ./dnsviz_analyze example.com
```

```
$ iceweasel example.com.html &
```

View dnsviz Output: Low PMTU



DNSViz Programmatic Analysis

dnsget Revisited (10.1 – 10.2)

```
$ ./dnsget_default example.com > example.com-broken.json
```

```
$ medit example.com-broken.json &
```

or

```
$ vi example.com-broken.json
```

dnsgrok Revisited (10.3 – 10.4)

```
$ ./dnsgrok -l warning -p example.com < example.com-broken.json \  
> example.com-broken-p.json
```

```
$ medit example.com-broken-p.json &
```

or

```
$ vi example.com-broken-p.json
```

View dnstool Output: Diagnostic Query History

example.com-broken.json

```
},
{
  "qname": "example.com.",
  "qclass": "IN",
  "qtype": "DNSKEY",
  "options": {
    "flags": 0,
    "edns_version": 0,
    "edns_max_udp_payload": 4096,
    "edns_flags": 32768,
    "edns_options": [],
    "tcp": false
  },
  "responses": {
    "192.168.213.25": {
      "192.168.213.1": {
        "message": "0UGEAAAABAAQAAAABB2V4YW1wbGUDY29tAAAwAAHADAA",
        "msg_size": 1039,
        "response_time": 0.001,
        "history": [
          {
            "response_time": 1.001,
            "cause": "TIMEOUT",
            "action": "NO_CHANGE"
          },
          {
            "response_time": 1.001,
            "cause": "TIMEOUT",
            "action": "NO_CHANGE"
          }
        ]
      }
    }
  }
}
```

View dnstget Output: Diagnostic Query History

example.com-broken.json

```
    "tcp": false
  },
  "responses": {
    "192.168.213.25": {
      "192.168.213.1": {
        "message": "0UGEAAABAAQAAAABB2V4YW1wbGUDY29tAAAwAAHADAAwA/",
        "msg_size": 1039,
        "response_time": 0.001,
        "history": [
          {
            "response_time": 1.001,
            "cause": "TIMEOUT",
            "action": "NO_CHANGE"
          },
          {
            "response_time": 1.001,
            "cause": "TIMEOUT",
            "action": "NO_CHANGE"
          },
          {
            "response_time": 1.002,
            "cause": "TIMEOUT",
            "action": "NO_CHANGE"
          },
          {
            "response_time": 2.001,
            "cause": "TIMEOUT",
            "action": "CHANGE_UDP_MAX_PAYLOAD",
            "action_arg": 512
          }
        ]
      }
    }
  }
}
```

View dnsgrok Output: Errors, Warnings, Statuses

```
example.com-broken-p.json
{
  "example.com.": {
    "queries": {
      "example.com./IN/A": {
        "answer": [
          {
            "rrsig": [
              {
                "description": "RRSIG covering example.com./A",
                "status": "EXPIRED",
                "servers": [
                  "192.168.213.25",
                  "fd02:f00d::25"
                ],
                "errors": [
                  {
                    "description": "The Signature Expiration field of th",
                    "code": "EXPIRATION_IN_PAST"
                  }
                ]
              }
            ]
          }
        ]
      },
      "example.com./IN/NS": {
        "answer": [
          {
            "rrsig": [
              {
                "description": "RRSIG covering example.com./NS".
```

View dnsgrok Output: Errors, Warnings, Statuses

```
example.com-broken-p.json
{
  "soa": [
    {
      "rrsig": [
        {
          "description": "RRSIG covering example.com./SOA",
          "status": "EXPIRED",
          "servers": [
            "192.168.213.25",
            "fd02:f00d::25"
          ],
          "errors": [
            {
              "description": "The Signature Expiration file",
              "code": "EXPIRATION_IN_PAST"
            },
            {
              "description": "The cryptographic signature",
              "code": "SIGNATURE_INVALID"
            }
          ]
        }
      ]
    }
  ]
}
```

View dnsgrok Output: Errors, Warnings, Statuses

example.com-broken-p.json

```
    },
    "delegation": {
      "status": "BOGUS",
      "errors": [
        {
          "description": "No valid RRSIGs made by a key corresponding to a DS R
          "code": "NO_SEP",
          "servers": [
            "192.168.213.25",
            "fd02:f00d::25"
          ]
        },
        {
          "description": "The DS RRset for the zone included algorithm 8 (RSASH
          "code": "MISSING_SEP_FOR_ALG",
          "servers": [
            "192.168.213.25",
            "fd02:f00d::25"
          ]
        }
      ]
    }
  }
}
```

Monitoring with DNSViz

- Sample script uses combination of dnstool and dnsviz, e.g., for use with cron

```
#!/bin/sh
name=$1
date=`date +%Y%m%d%H%M%S`
dnstool_out=/tmp/$name-dnstool-$date.json
dnsgrok_out=/tmp/$name-dnsgrok-$date.json
dnsviz_out=/tmp/$name-dnsviz-$date.png

dnstool -d 0 $name > $dnstool_out
dnsgrok -l warning -p $name < $dnstool_out > $dnsgrok_out
if (( $( stat -c %s $dnsgrok_out ) > 0 )); then
    dnsviz -Tpng -o $dnsviz_out $name $name < $dnstool_out
    gzip $dnstool_out
    cat $dnsgrok_out | \
    mutt -s "Problems with $name" -a $dnsviz_out $dnstool_out.gz -- \
        joe@example.com
fi

rm $dnstool_out* $dnsgrok_out $dnsviz_out
```

Summary

- Understanding and analyzing DNS and DNSSEC can be complex.
- DiG, BIND, DNSViz, and other tools can aid in understanding, troubleshooting, and monitoring.
- Maintain and monitor your DNS zones!

Further Information on DNSViz

- Source: <https://github.com/dnsviz/dnsviz> (License: GPLv2)
- Online version: <http://dnsviz.net/>
- Mailing list: <https://groups.google.com/d/forum/dnsviz-users>

powered by



VERISIGN™