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

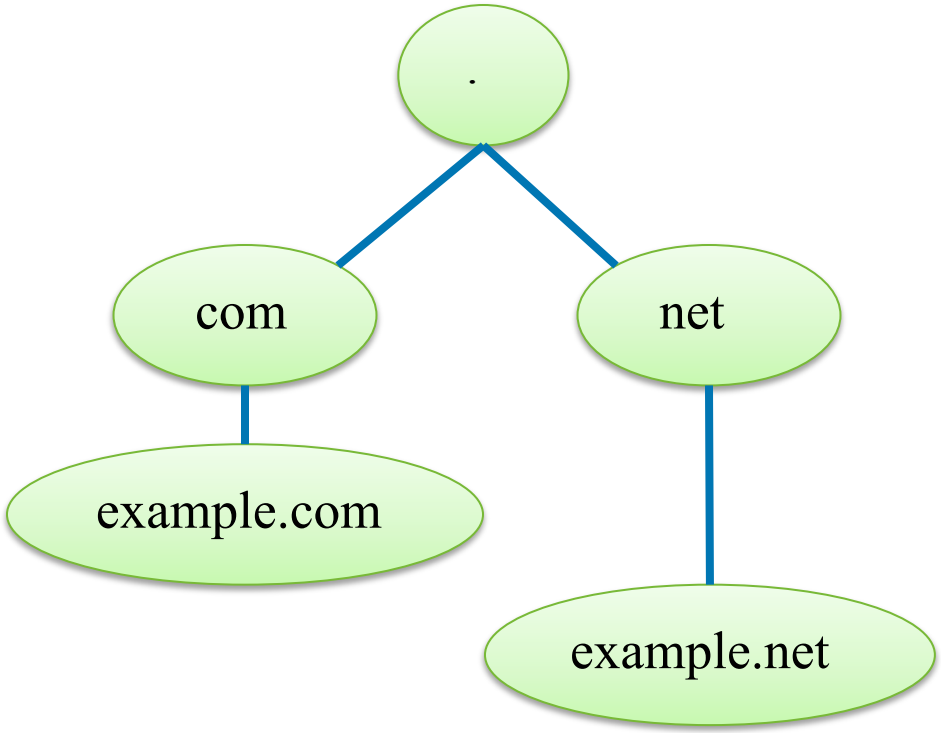
Caveats

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

DNS Overview

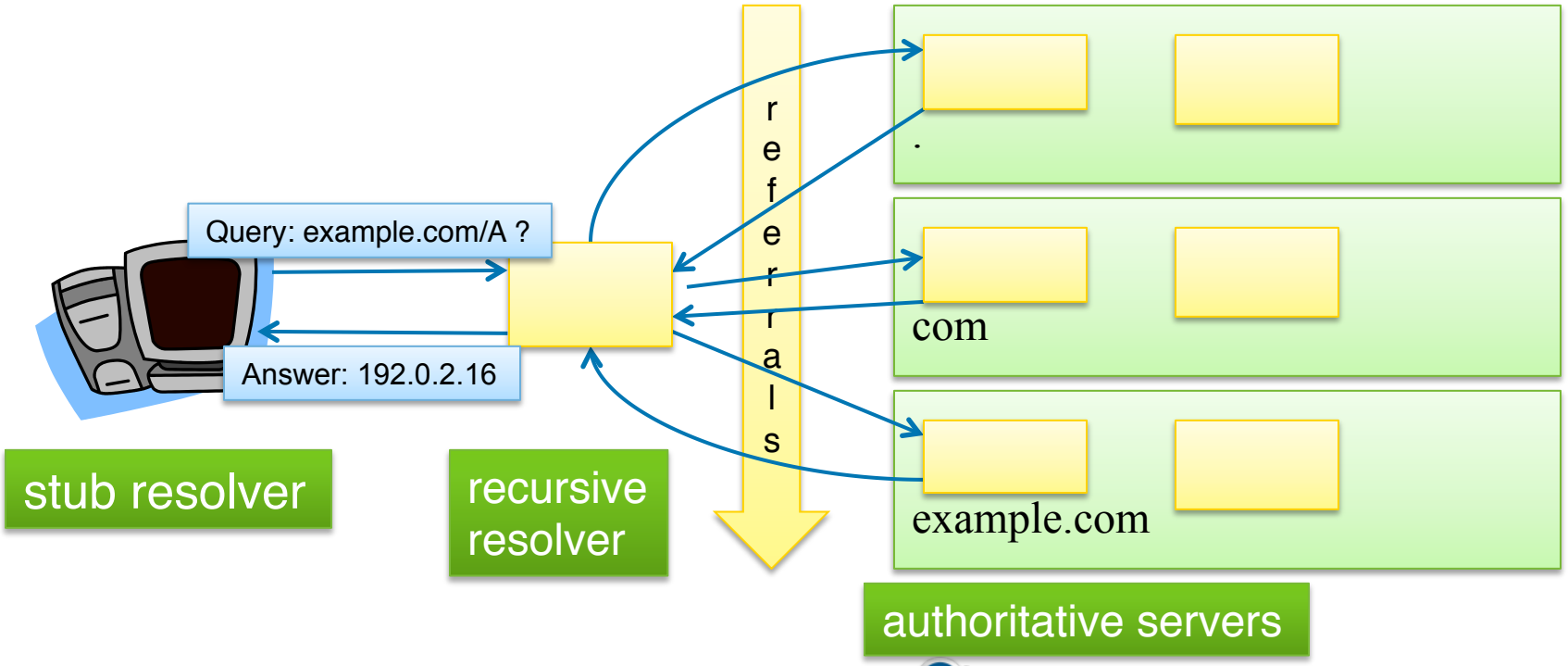
DNS Namespace

- 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

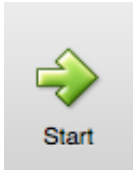
- ***Resolvers*** query ***authoritative servers***
- Queries begin at root zone, resolvers follow downward referrals
- Resolver stops when it receives authoritative answer

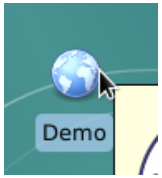


Virtual Environment Initialization

- 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
```

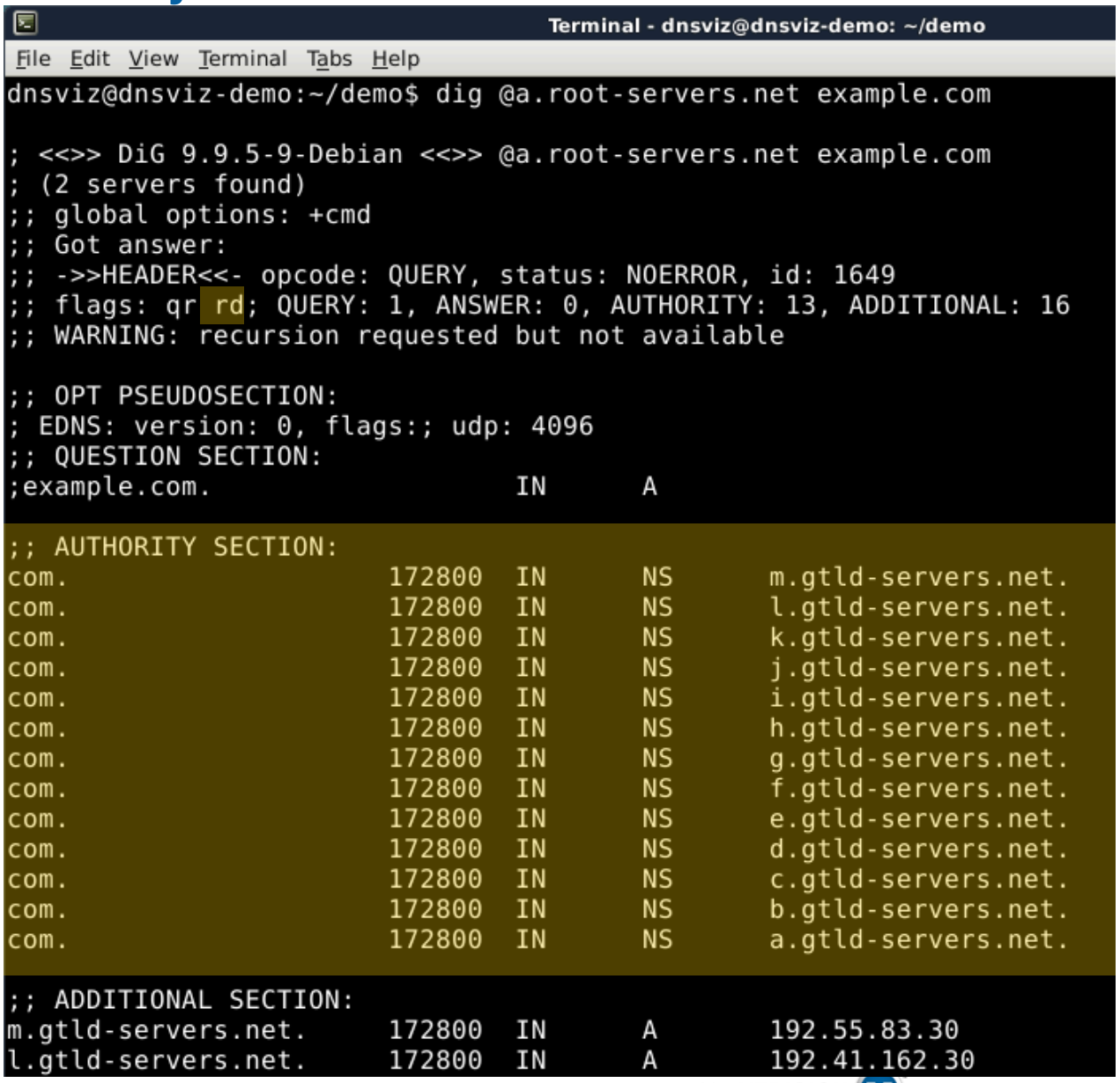
```
$ dig @a.iana-servers.net example.com
```

```
$ 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



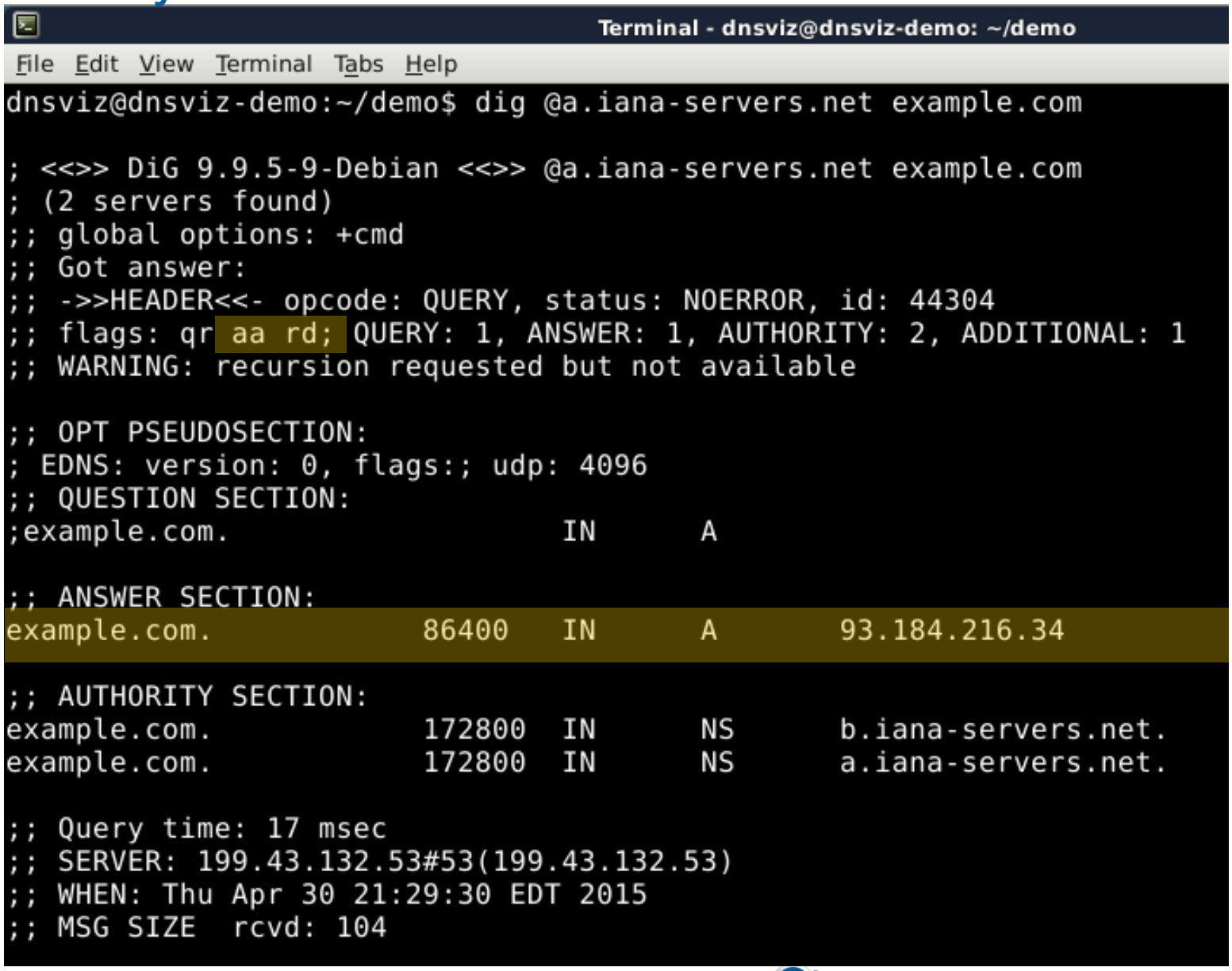
Query a TLD Server

Terminal - dnsviz@dnsviz-demo: ~/demo

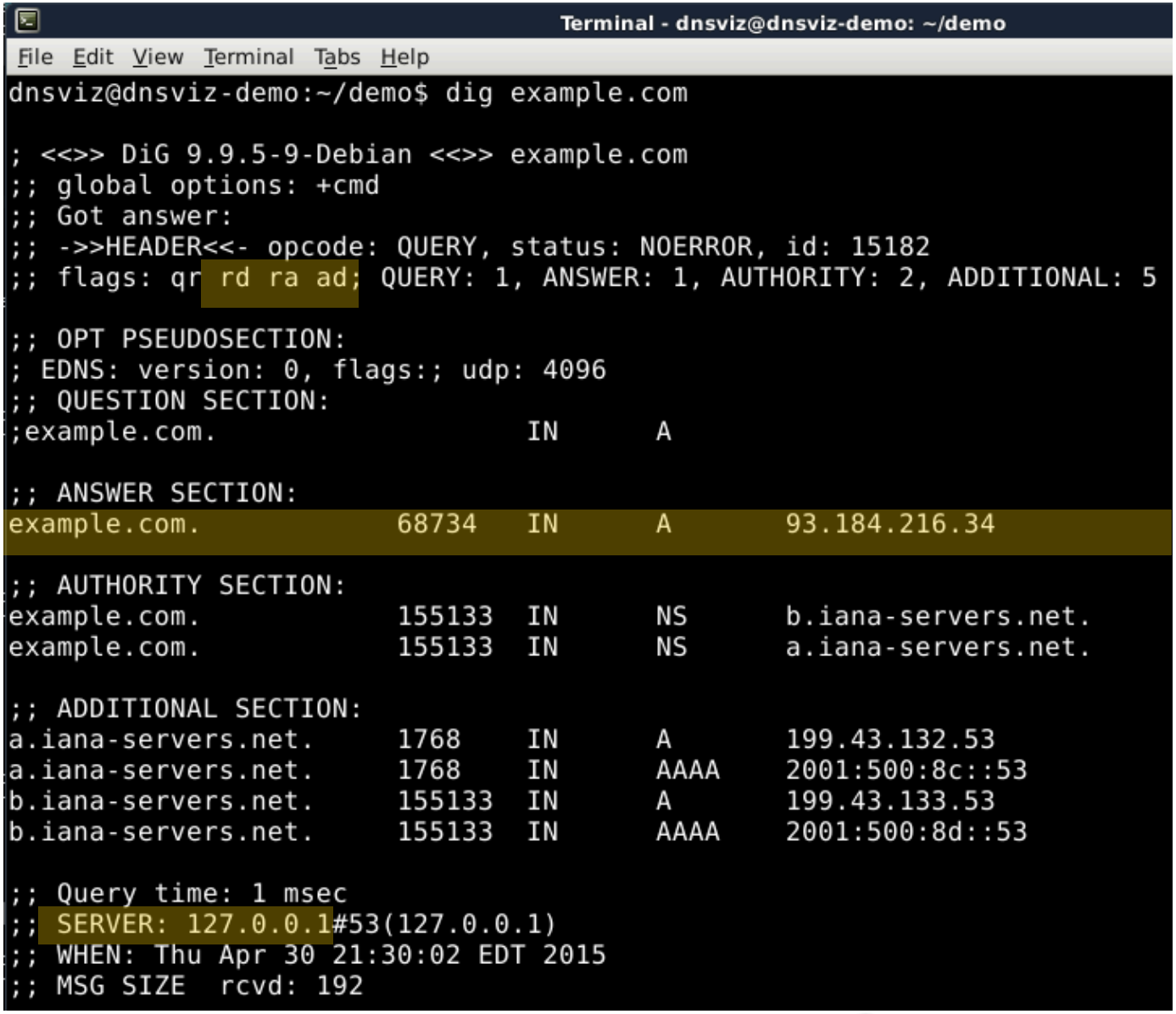
File Edit View Terminal Tabs Help

```
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



Query Local Recursive Resolver



Query for a Non-existent Name

Terminal - dnsviz@dnsviz-demo: ~/demo

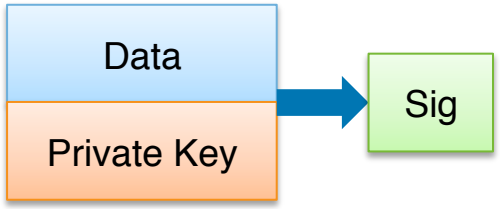
File Edit View Terminal Tabs Help

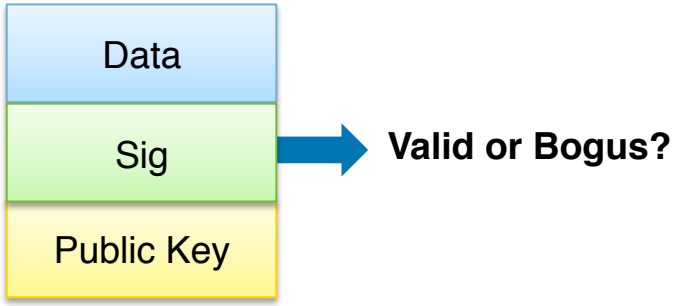
```
dnsviz@dnsviz-demo:~/demo$ dig @a.iana-servers.net foobar.example.com

; <<>> 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

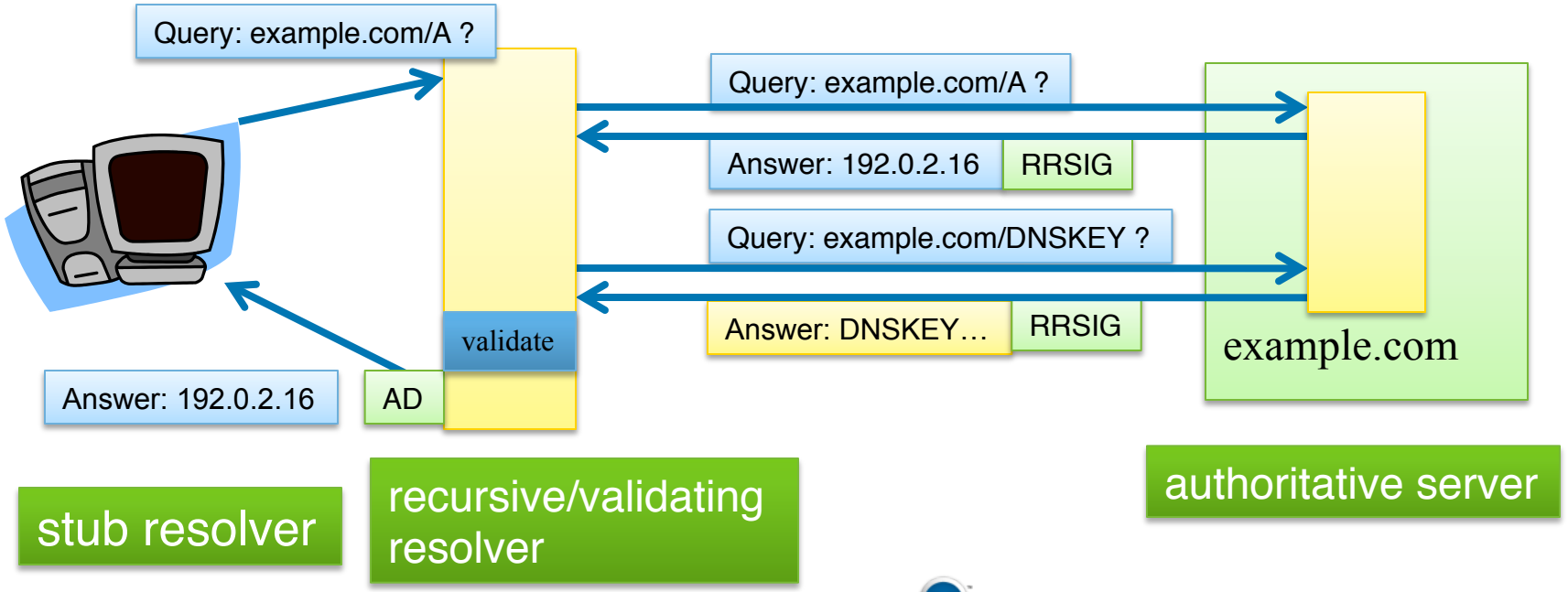
- Keys
  - **Public** Key – advertised to everyone
  - **Private** Key – kept hidden
- Signatures
  - Made by private key
  - Validated with public key
- Validation
  - Consumer uses public key, message, and signature to validate message





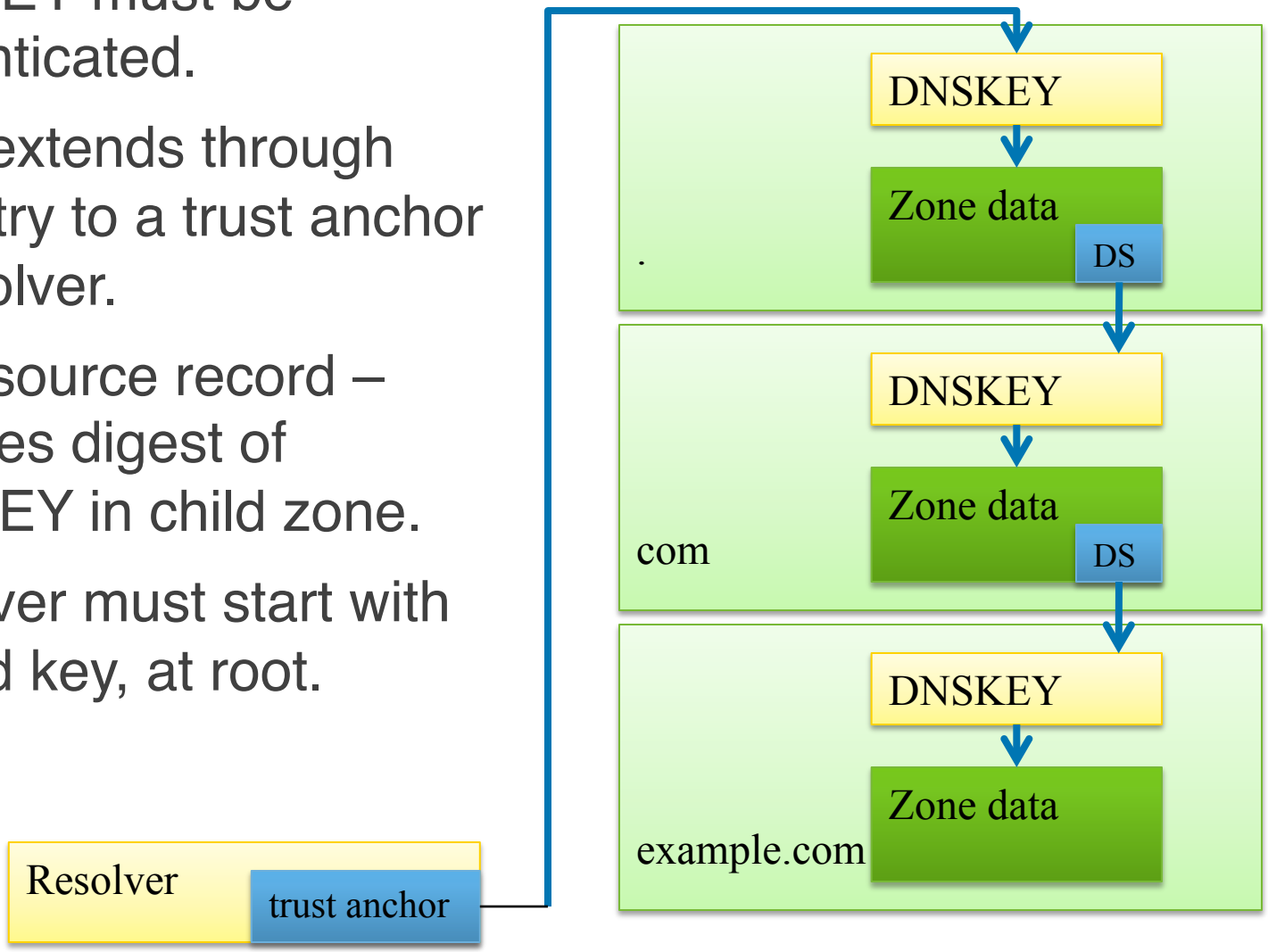
DNS Security Extensions (DNSSEC)

- 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



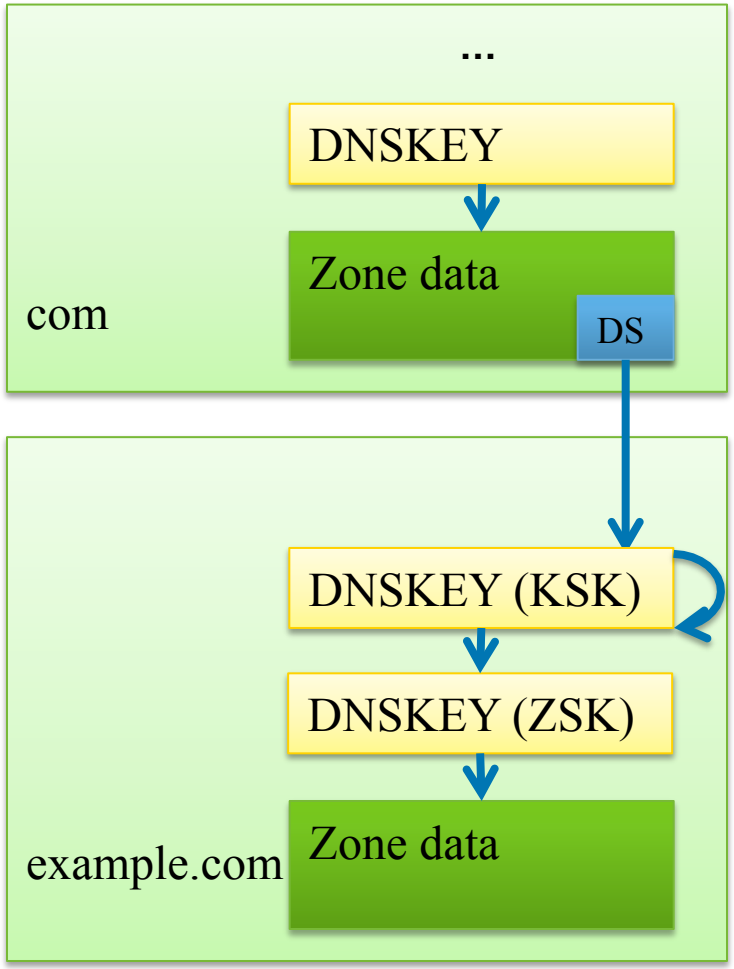
DNSSEC Chain of Trust

- 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.



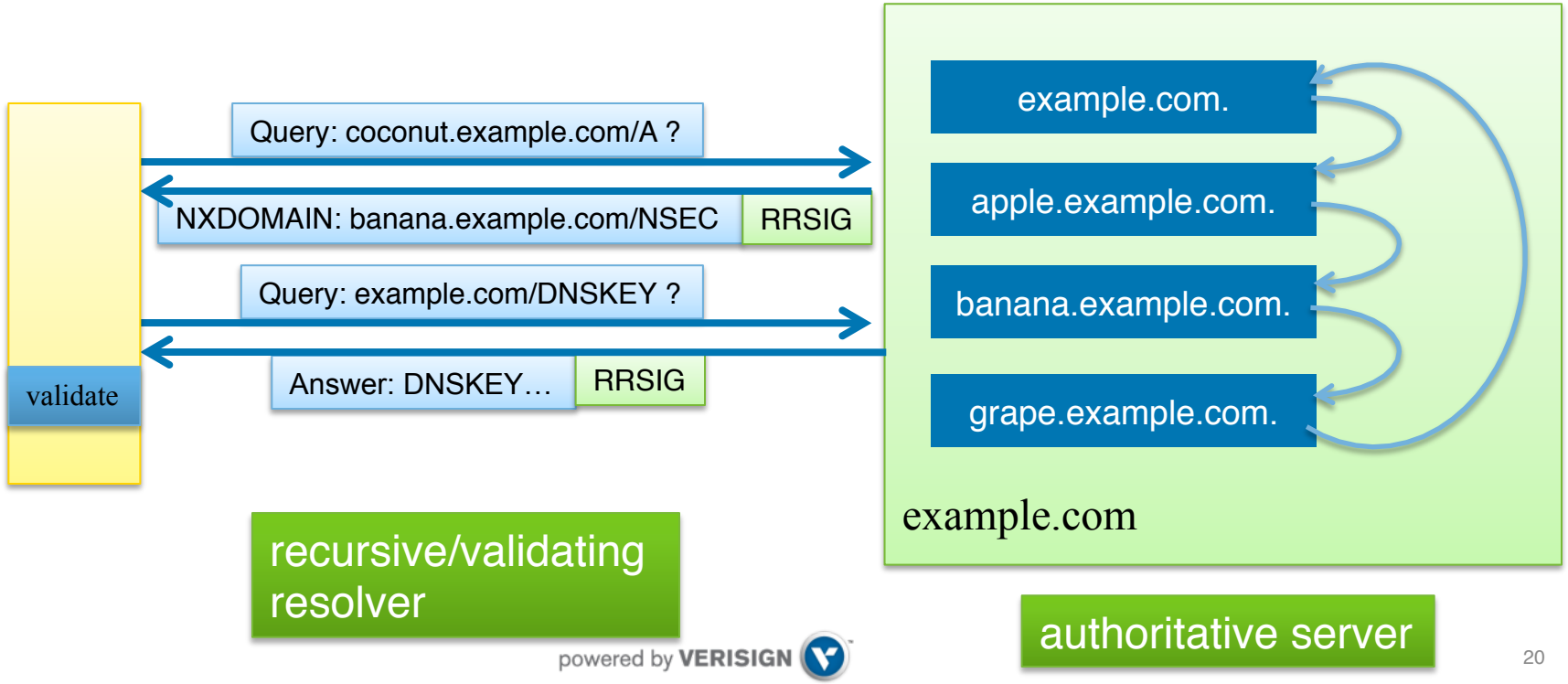
Key Roles – KSK/ZSK

- 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.



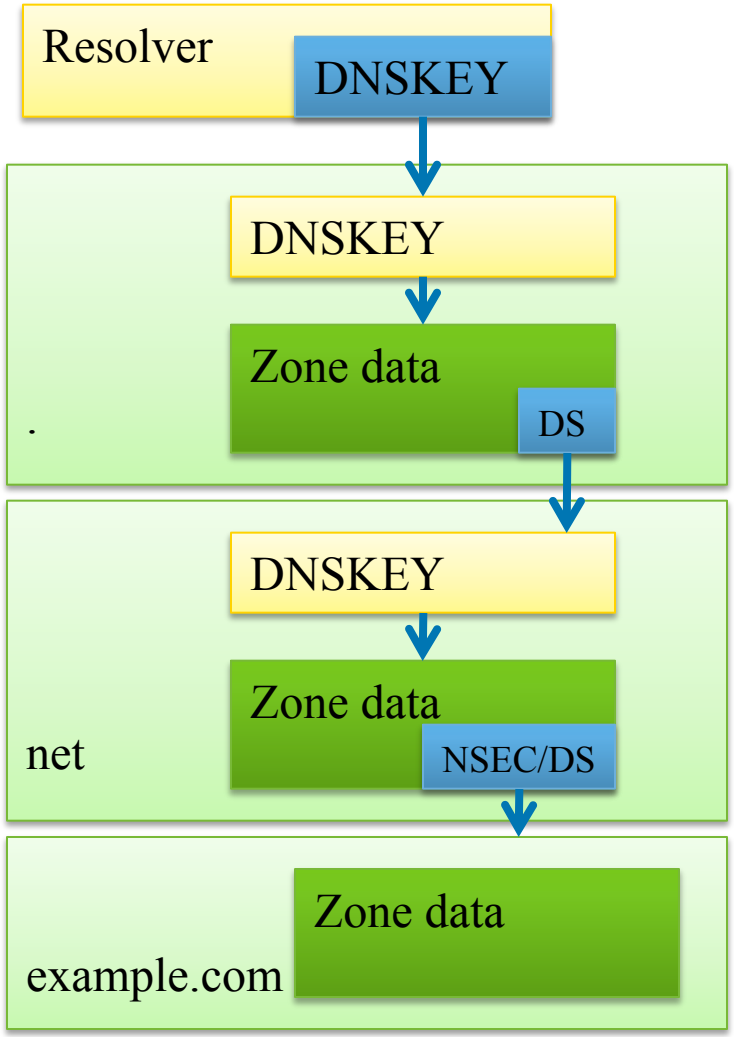
Authenticated Denial of Existence

- 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
```

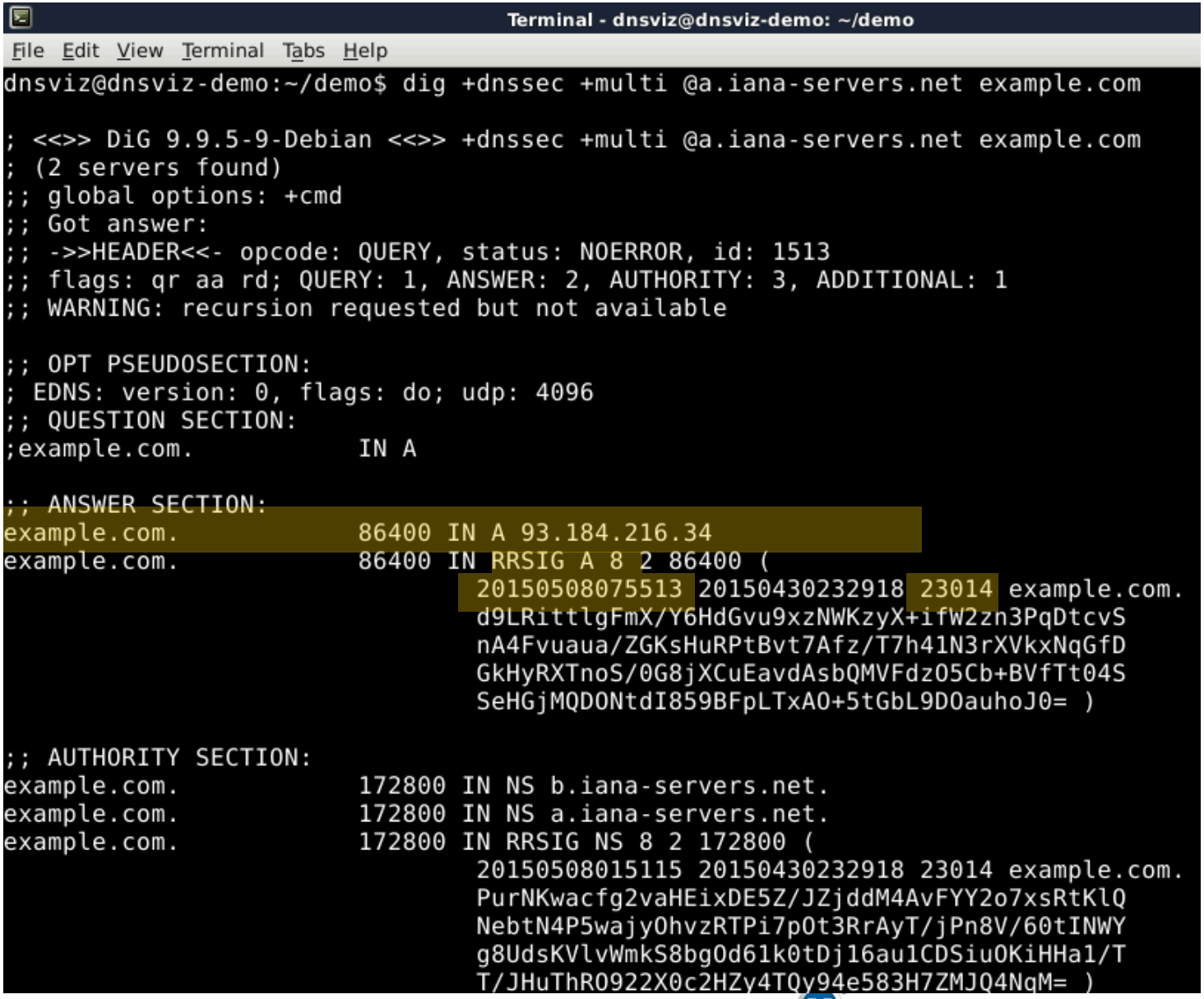
```
$ dig +dnssec +multi @a.gtld-servers.net example.com DS
```

query a "parent" server because we're seeking a DS record

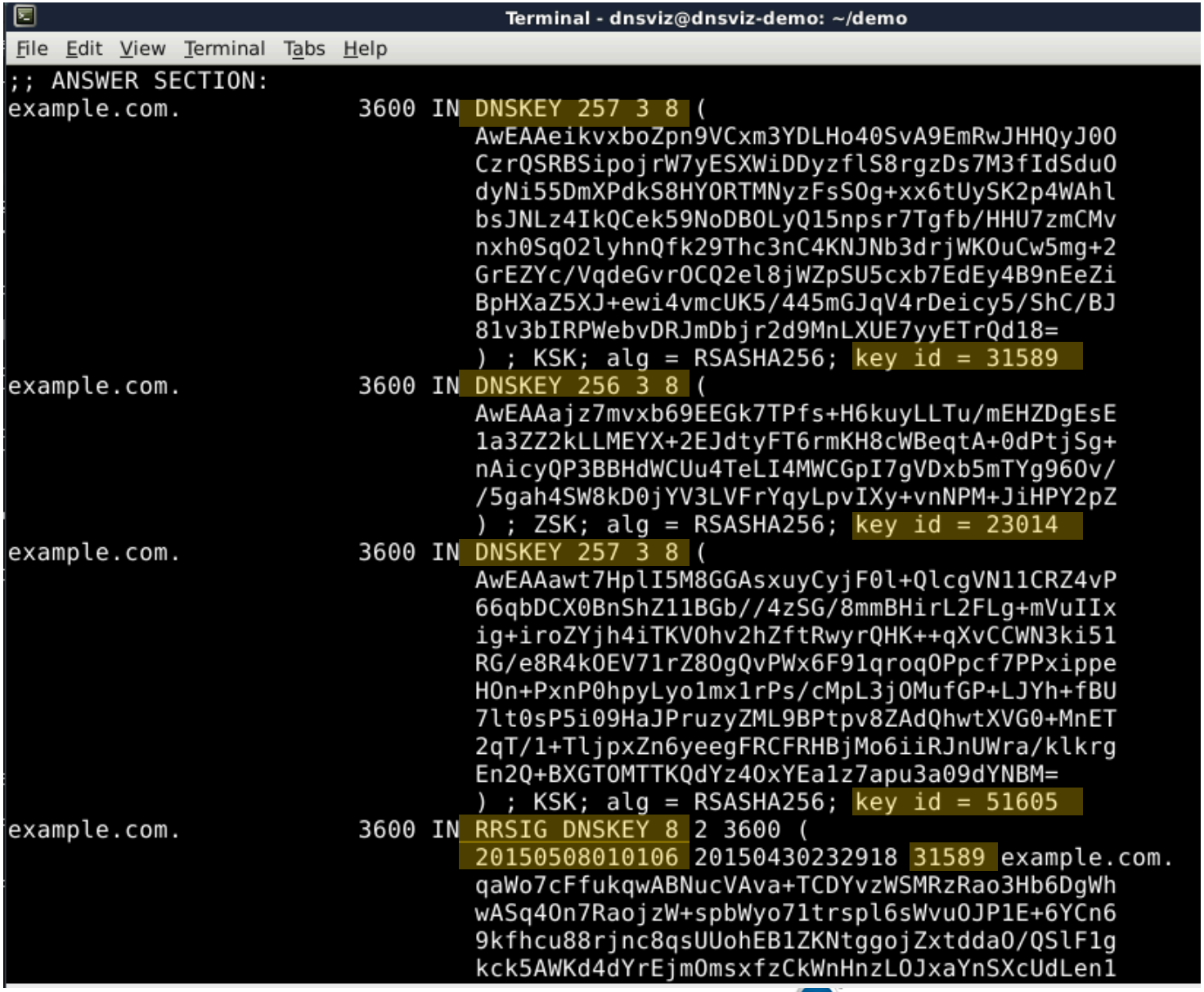
```
$ dig +dnssec +multi example.com
```

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

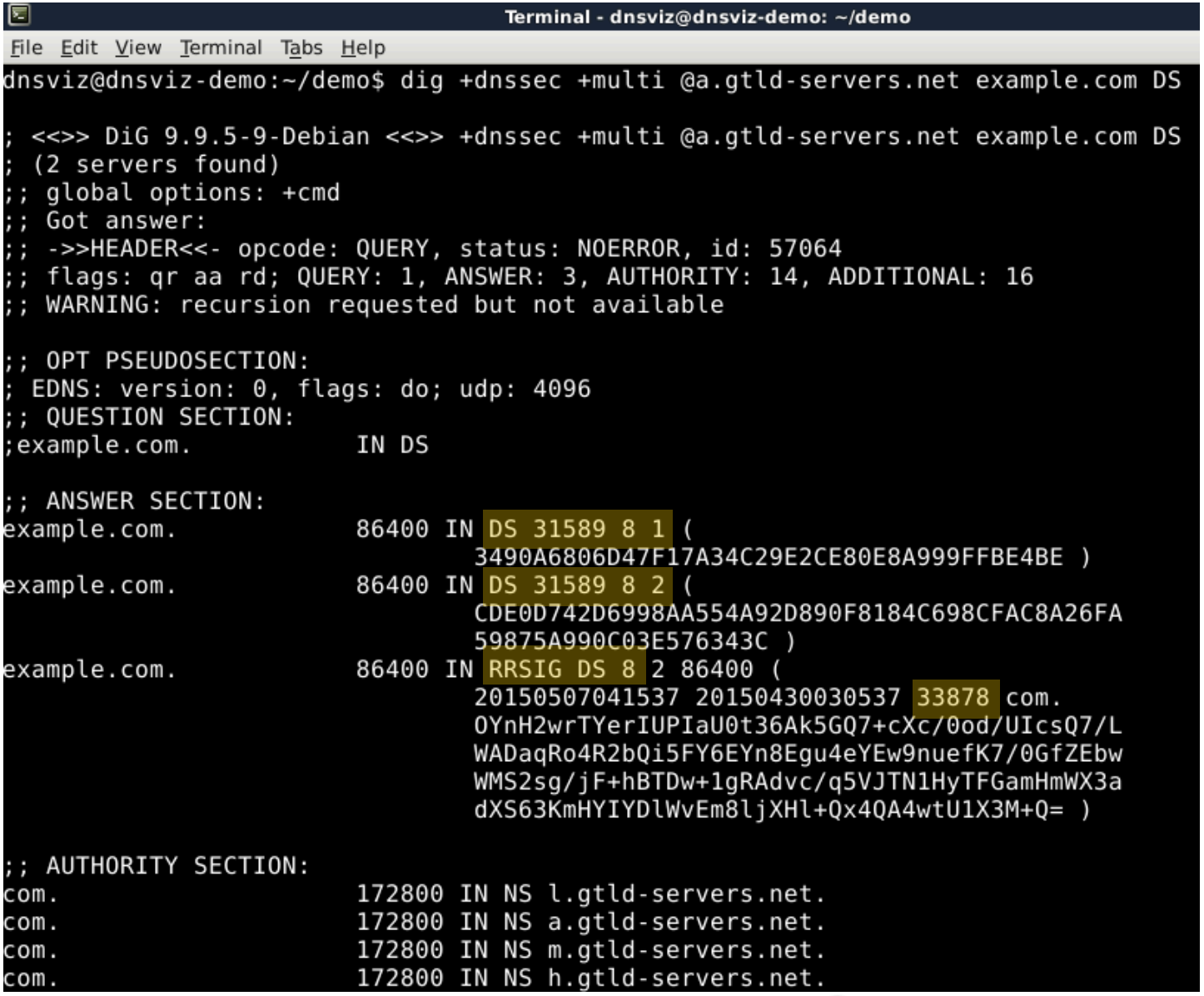
Query for DNSSEC Records (RRSIGs)



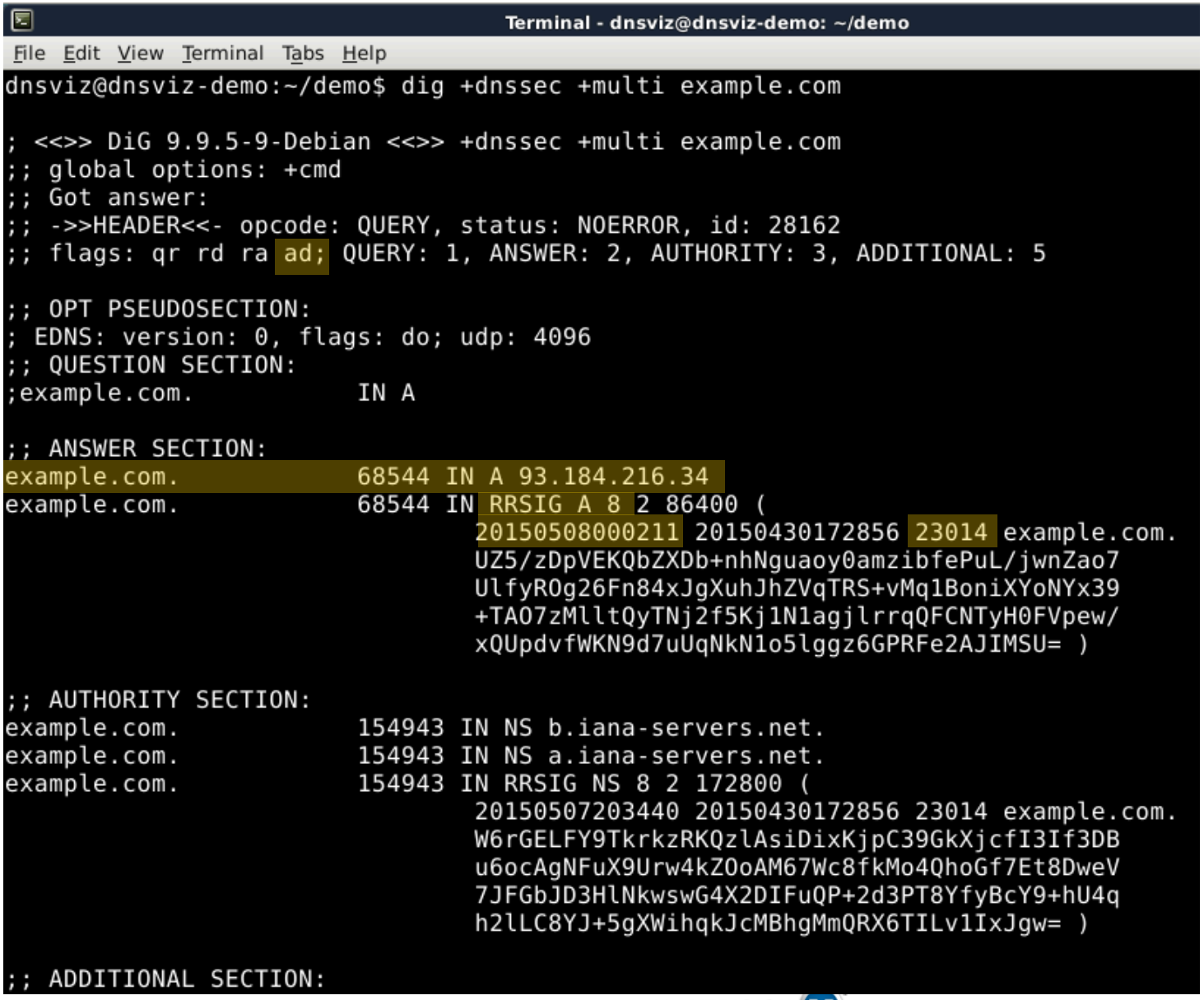
Query for DNSSEC Records (DNSKEY)



Query for DNSSEC Records (DS)



Query for DNSSEC Records



Query For DNSSEC Records (NSEC)

Terminal - dnsviz@dnsviz-demo: ~/demo

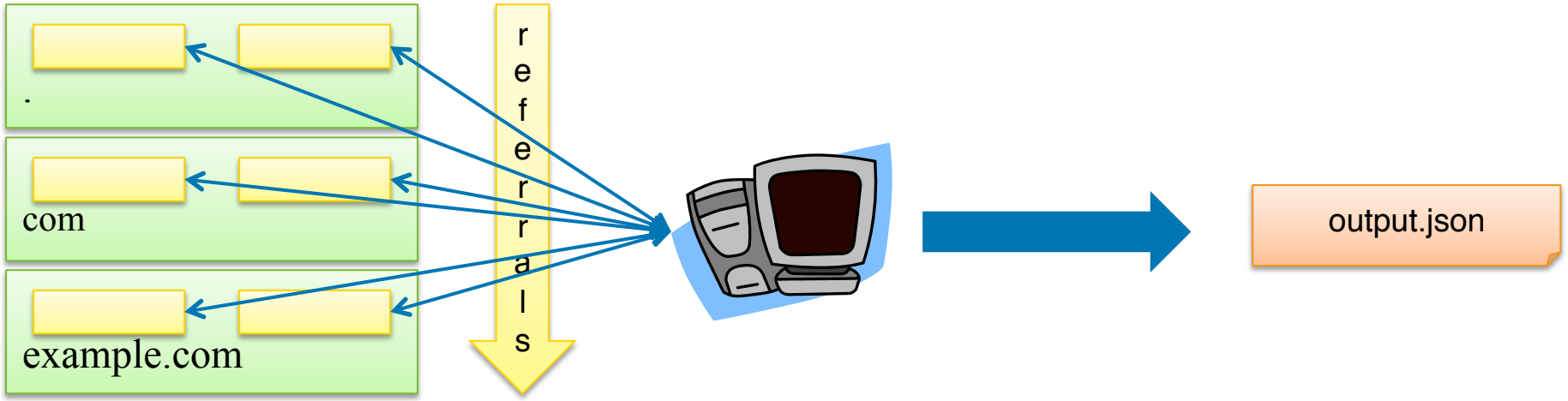
File Edit View Terminal Tabs Help

```
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/JTIBbag9XneTqLofcRFwjyXOrefuLPev
                                ShMn7fzK8O4f0HYXTIYi9oSN30XZkCN3E04Id3Uh4VWU
                                DkMxpEyVgeW1wHQiQto6IHAOOjyresABcifqCyM= )
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

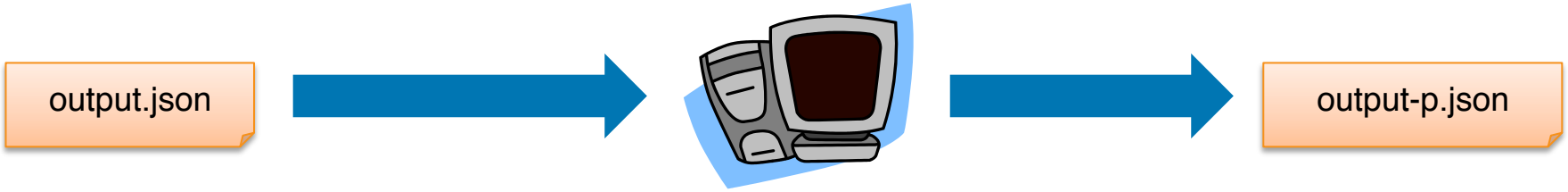
DNS Analysis Using DNSViz (`dnsget` command line)

- 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



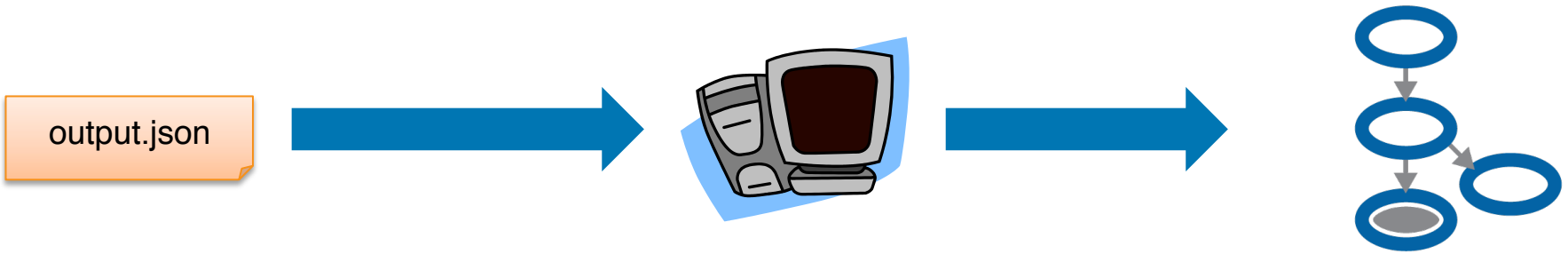
Serialized online analysis (JSON)

```
$ dnsgrok example.com
```

Serialized offline analysis (JSON)

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 `dnsget` 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 `dnsget` 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 `dnsget` Output

example.com.json


```
    },
    "example.com.": {
        "stub": false,
        "analysis_start": "2015-05-01 01:41:59 UTC",
        "analysis_end": "2015-05-01 01:42:00 UTC",
        "clients_ipv4": [
            "10.0.2.15"
        ],
        "clients_ipv6": [],
        "parent": "com.",
        "referral_rdtype": "NS",
        "explicit_delegation": false,
        "nxdomain_name": "s0m8463hu9.example.com.",
        "nxdomain_rdtype": "A",
        "nxrrset_name": "example.com.",
        "nxrrset_rdtype": "CNAME",
        "auth_ns_ip_mapping": {
            "a.iana-servers.net.": [
                "199.43.132.53",
                "2001:500:8c::53"
            ],
            "b.iana-servers.net.": [
                "199.43.133.53",
                "2001:500:8d::53"
            ]
        },
        "queries": [
            {
                "qname": "example.com.",
                "qclass": "IN",
```

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+4cOdK
                                "257 3 8 AwEAAagAIKlVZrpC6Ia7gEzah
                            ],
                            "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 (RSA
            "flags": 256,
            "protocol": 3,
            "algorithm": 8,
            "key": "AwEAAZyIkCwEYeG29NV+4cOdKE4DPng/4BqJe
            "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

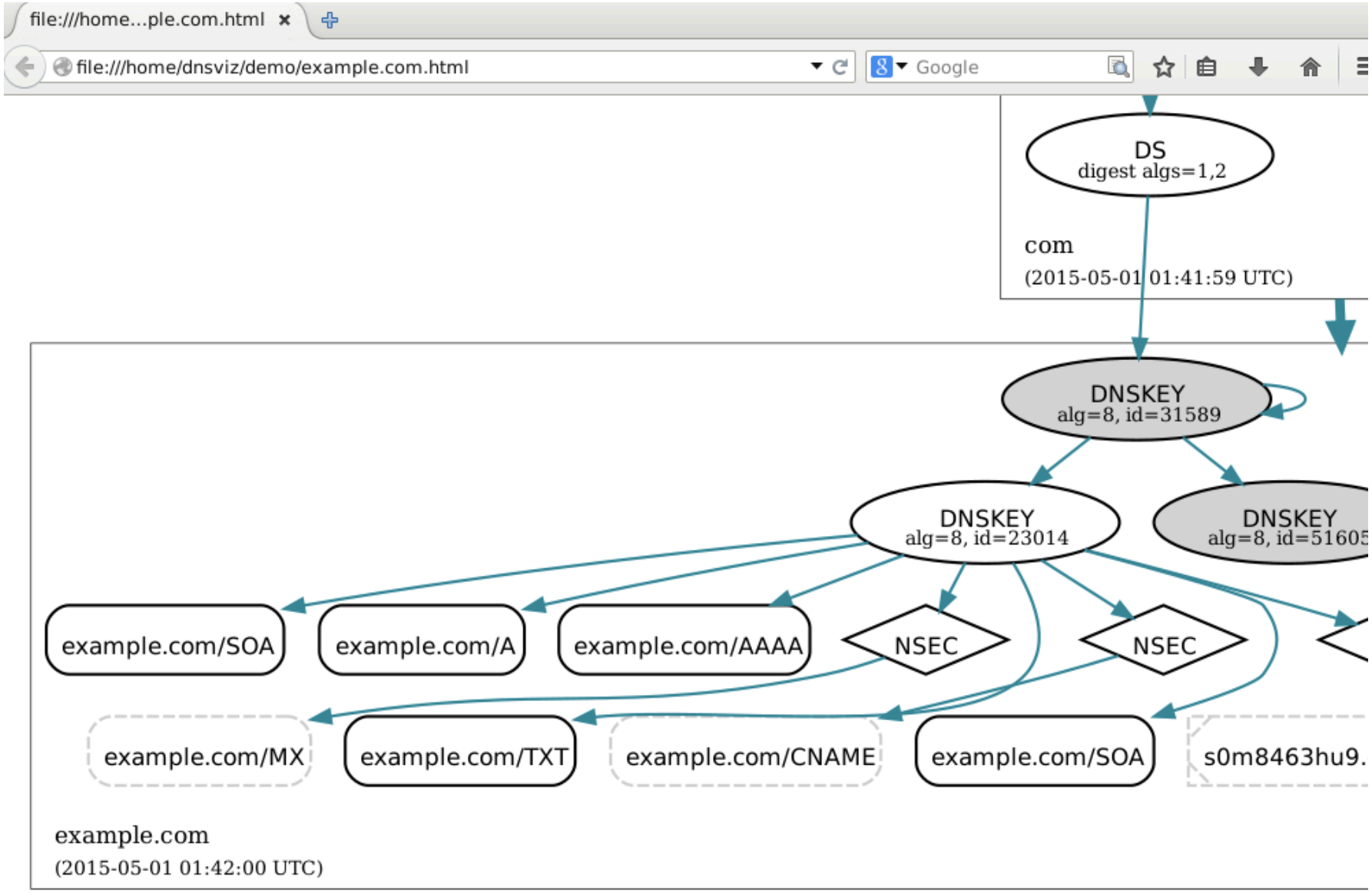

```
{
    ".": {
        "status": "NOERROR",
        "queries": {
            "./IN/DNSKEY": {
                "answer": [
                    {
                        "description": "RRset for ./DNSKEY",
                        "rrsig": [
                            {
                                "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

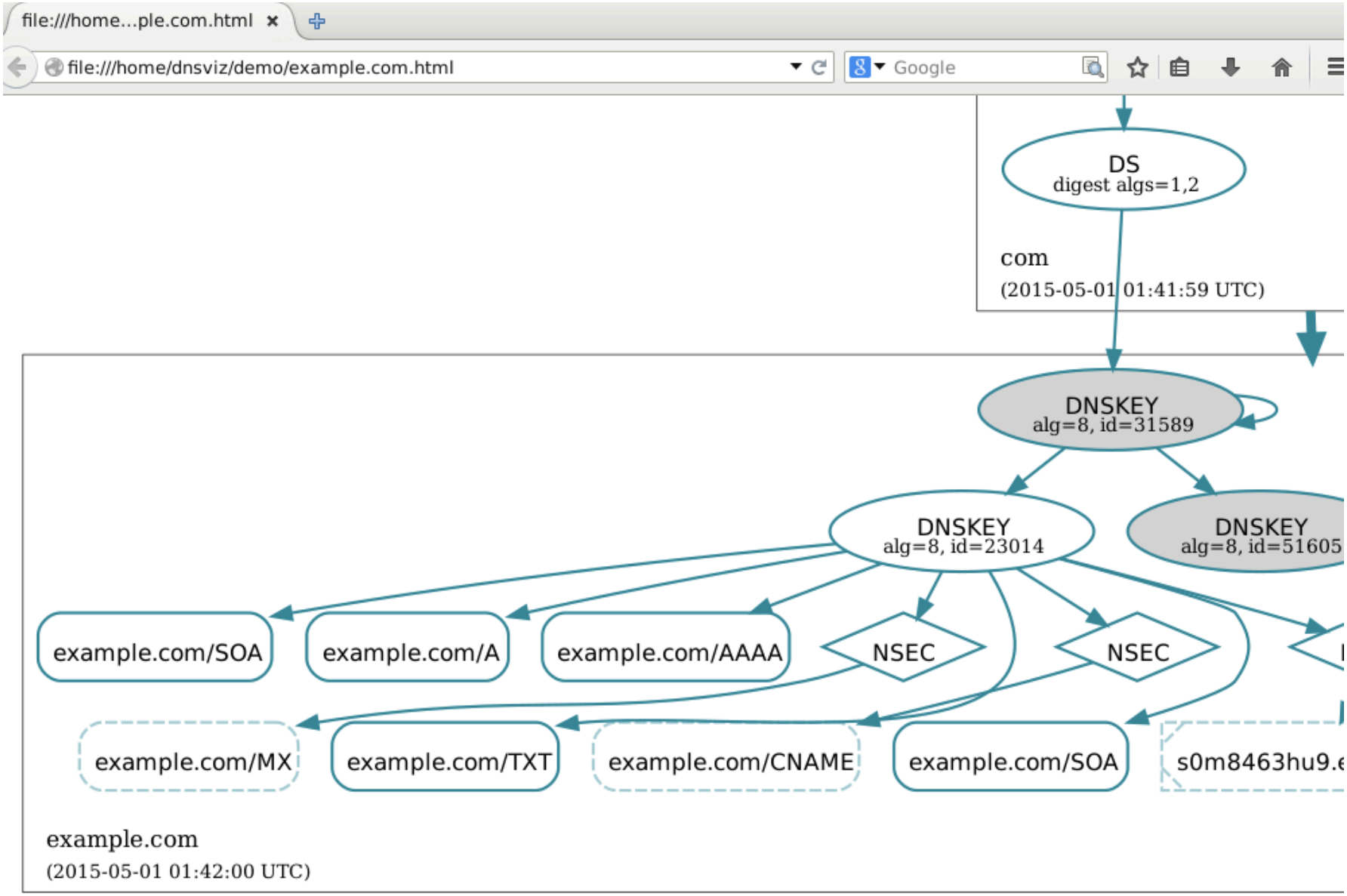
example.com-p1.json


```
            {
                "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

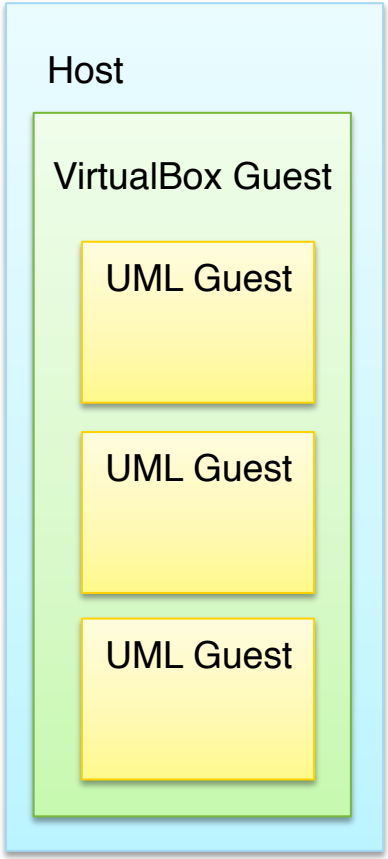


Signing a DNS Zone

Setup Virtual DNS Environment (4.1 – 4.2)

```
$ ./start_all
```

(Wait for all three consoles to come up)



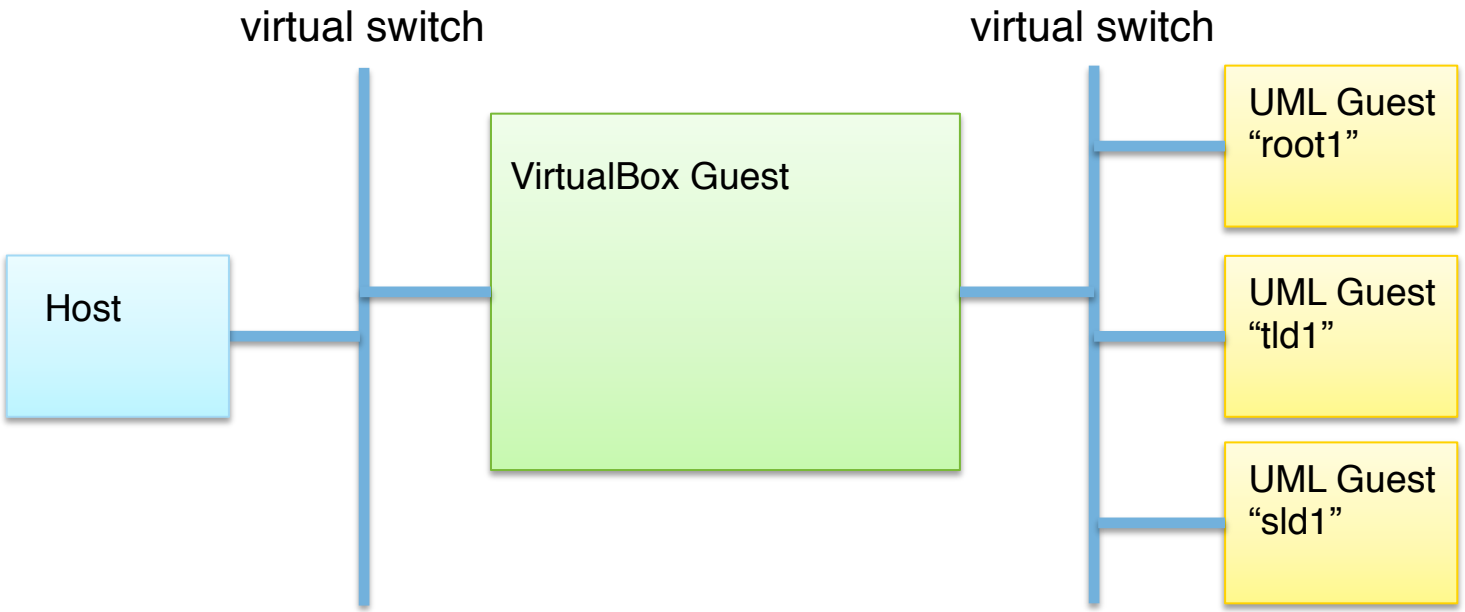
Change directory for all three consoles: root, tld1, sld1

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

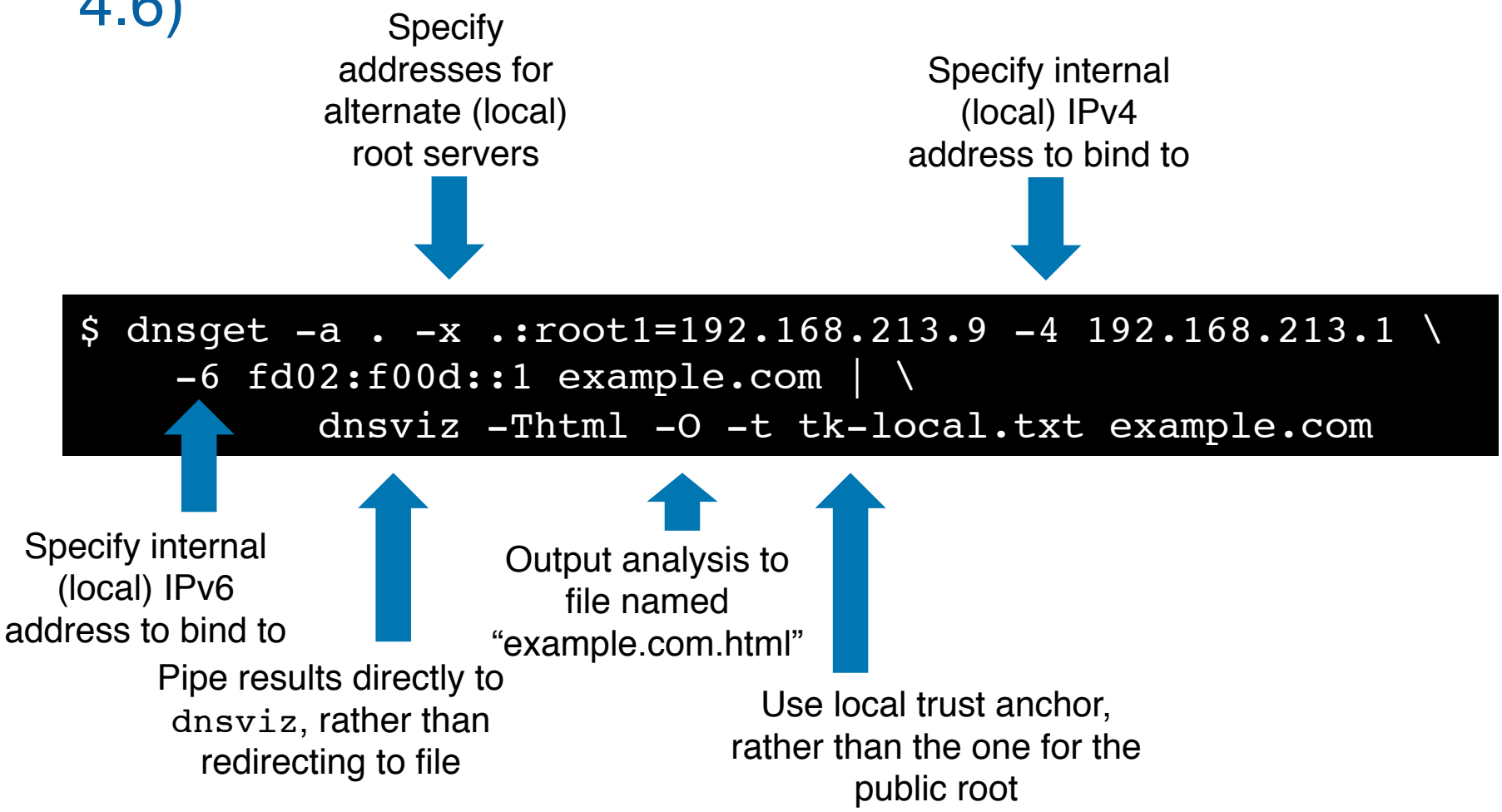
Setup Virtual DNS Environment (4.3)

```
$ ./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)

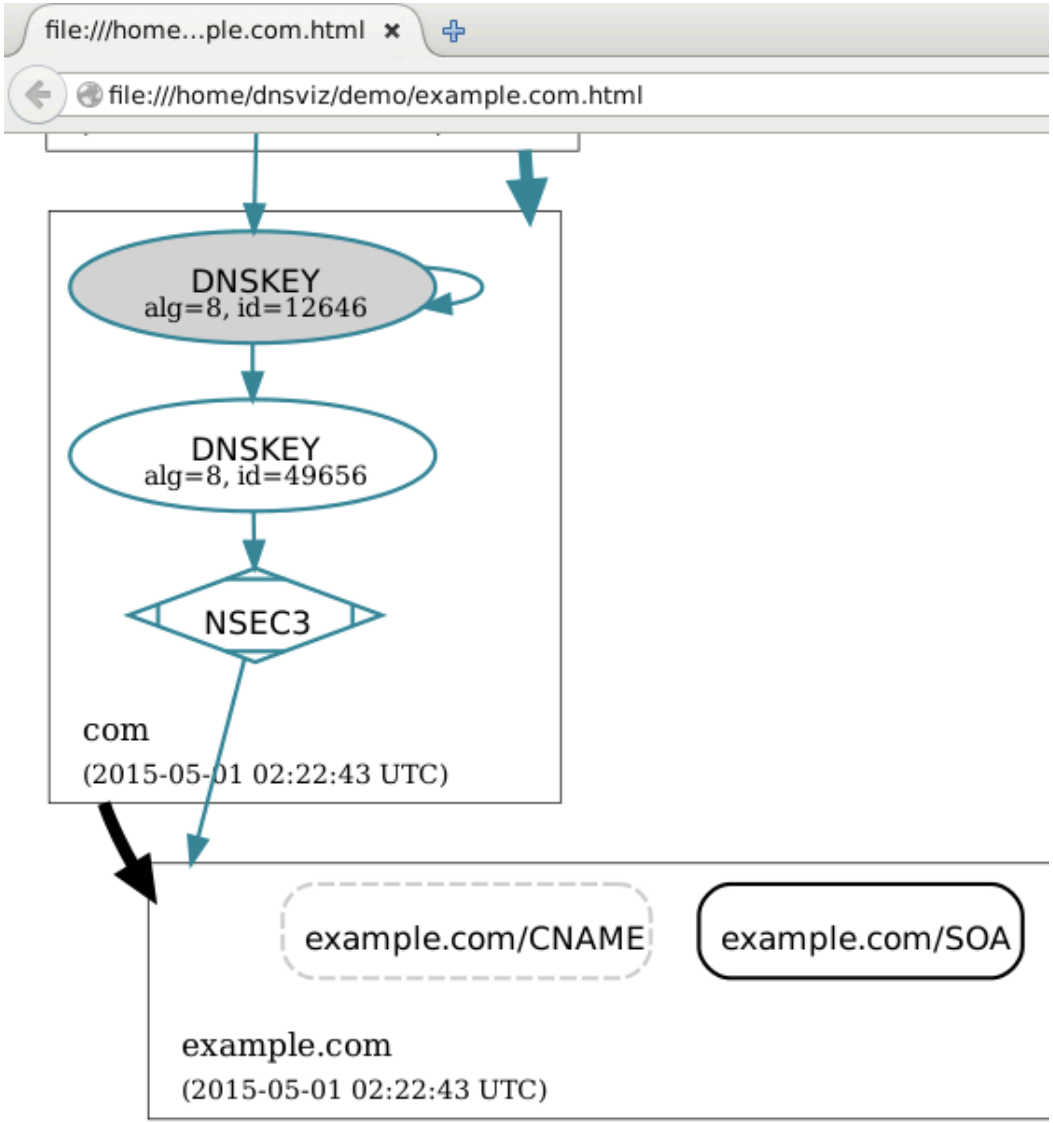



```
$ ./dnsviz_analyze example.com
```

(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
```

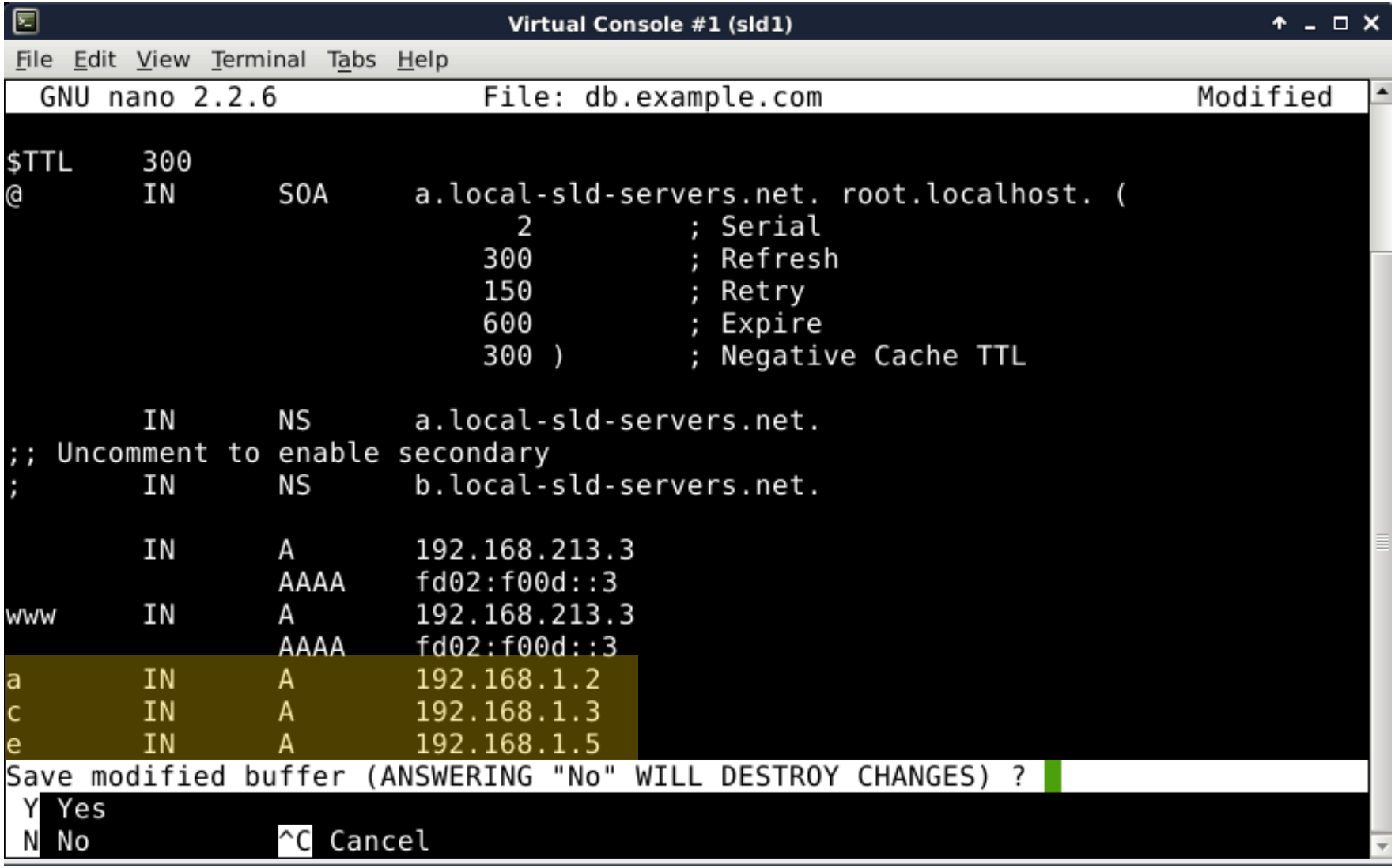
- Reload zone

```
# service bind9 reload
```

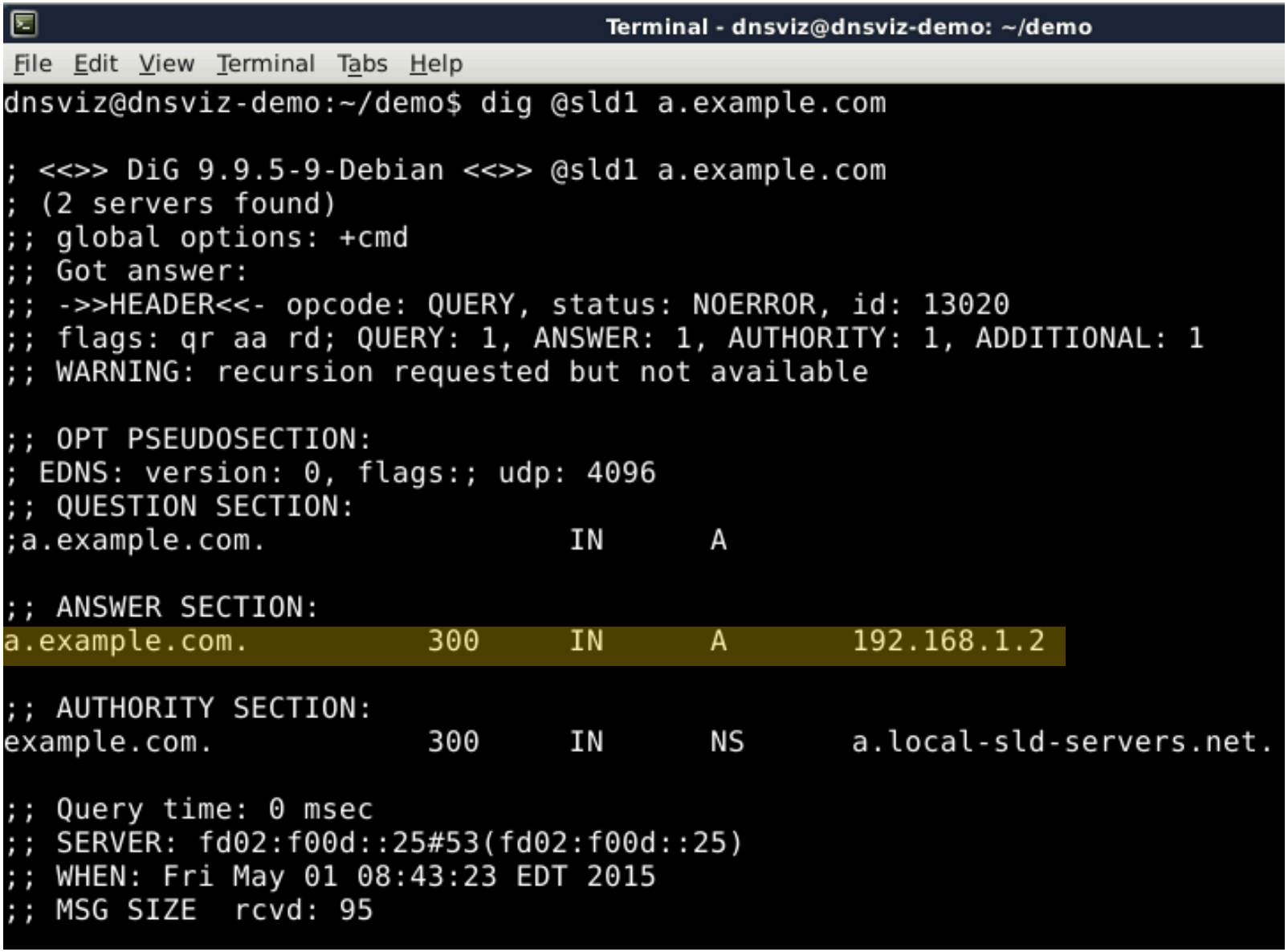
- Check that record shows up (query from VirtualBox guest)

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

Add Records to example.com Zone



Add Records to example.com Zone



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
```

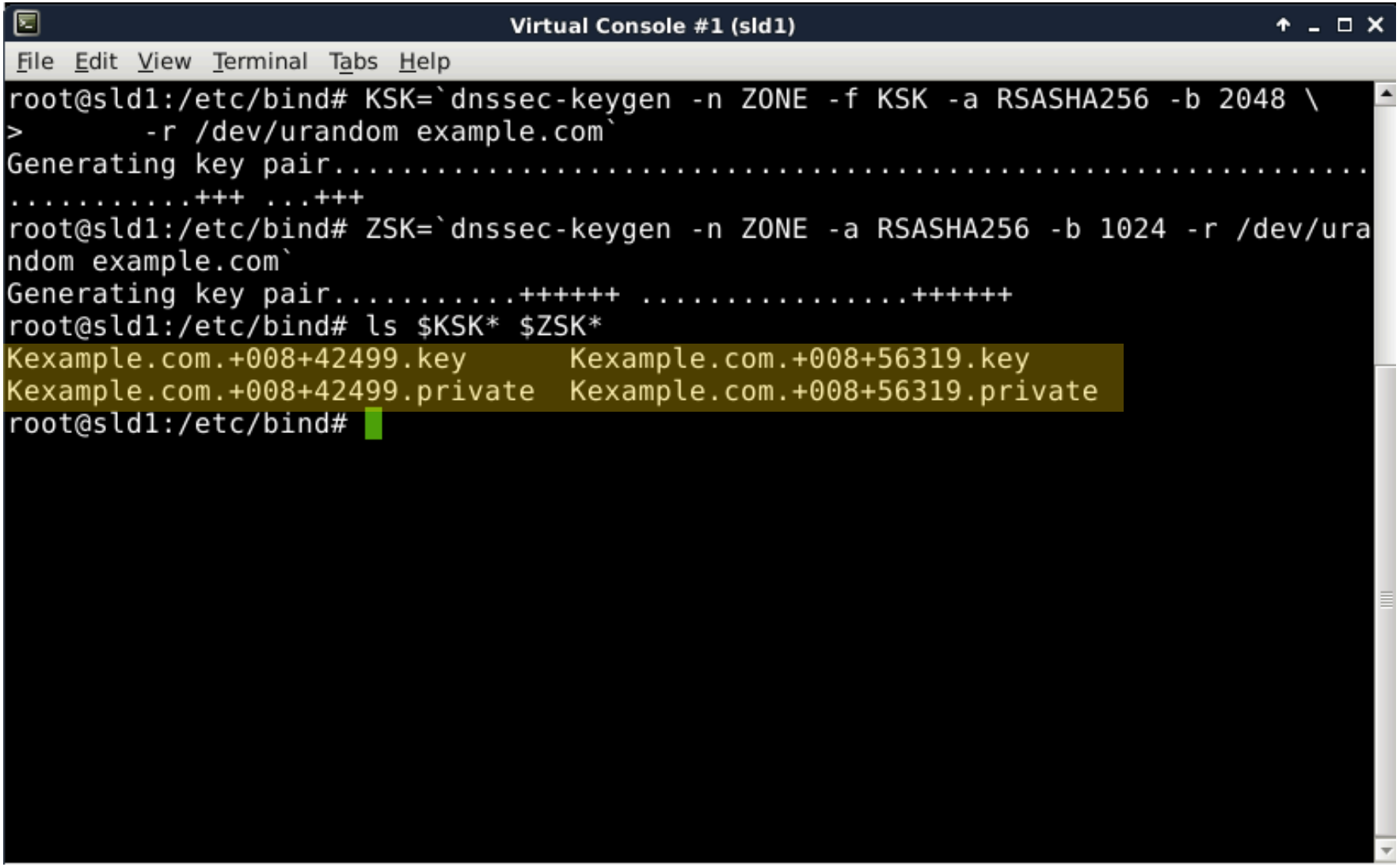
- Re-analyze

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

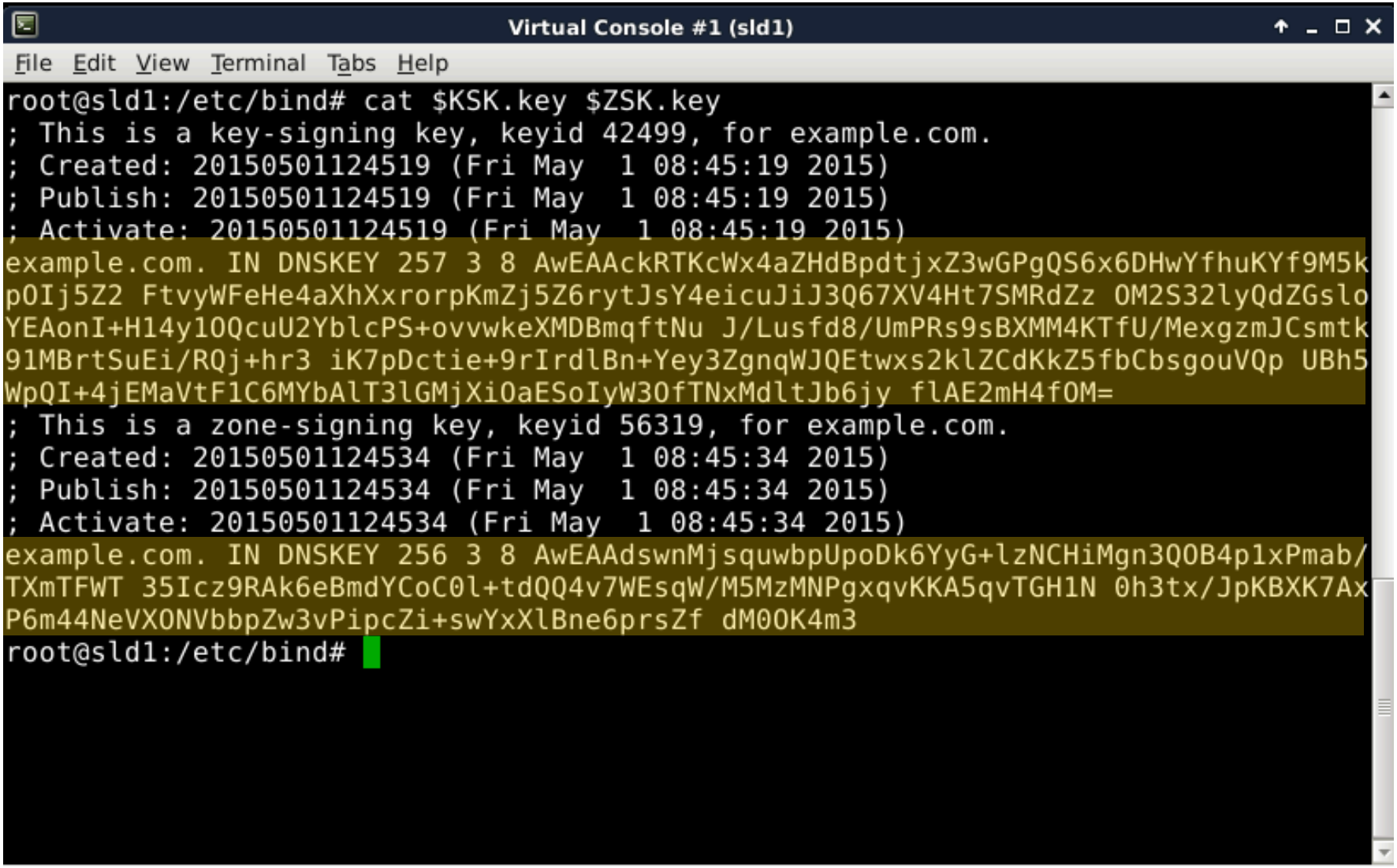
```
$ iceweasel example.com.html &
```

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

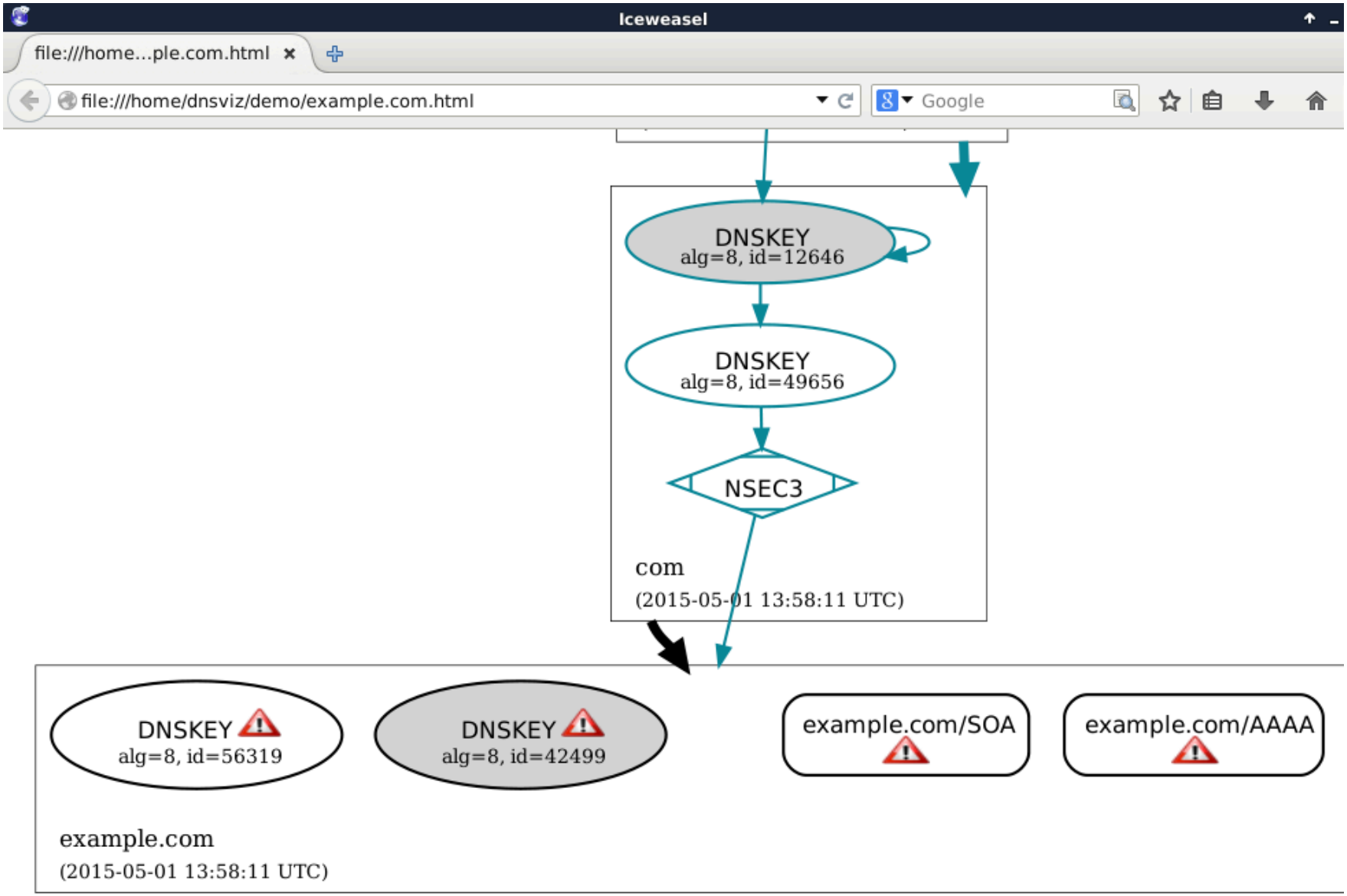
Create DNSSEC keys for example.com



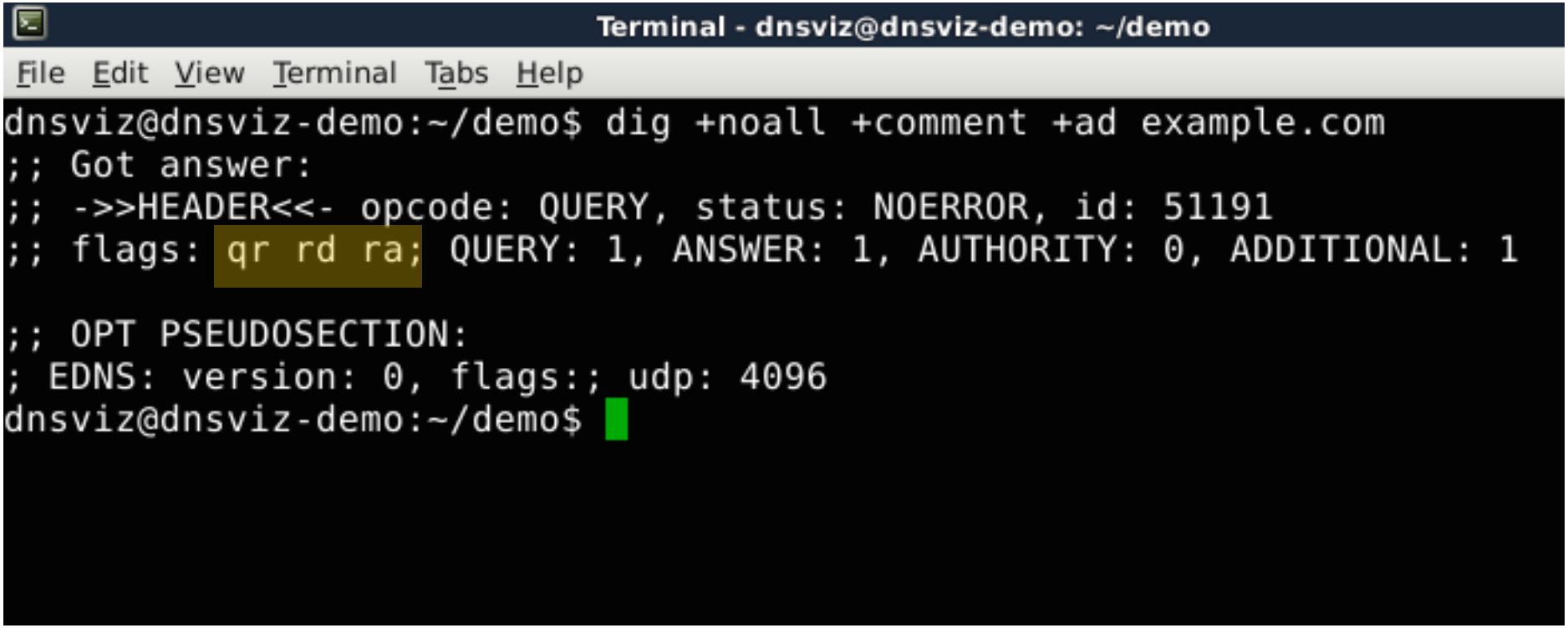
Create DNSSEC keys for example.com



View `dnsviz` Output: DNSKEYs with no RRSIGs



View `dig` Output: no AD bit



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

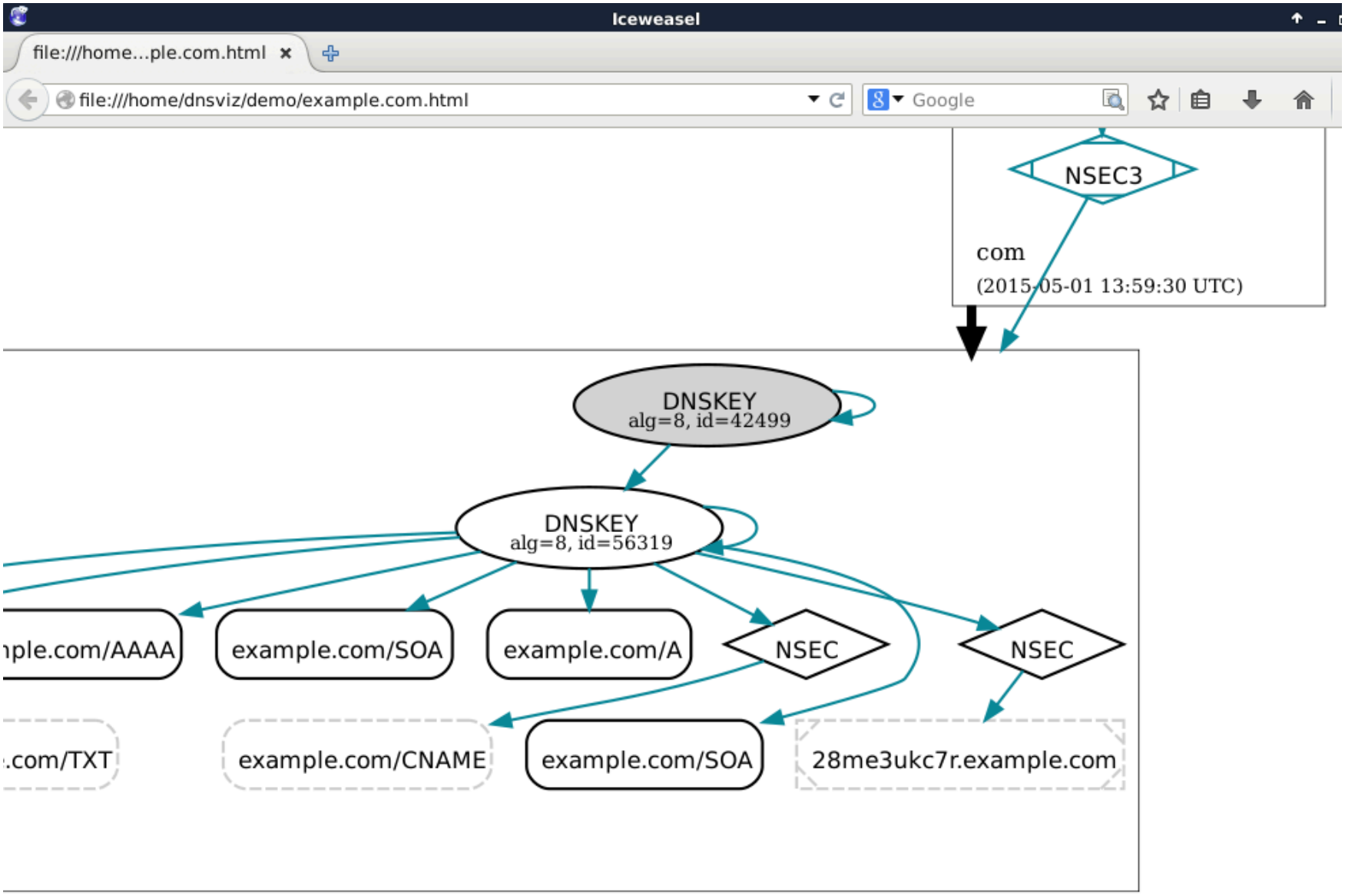
```
# service bind9 reload
```

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

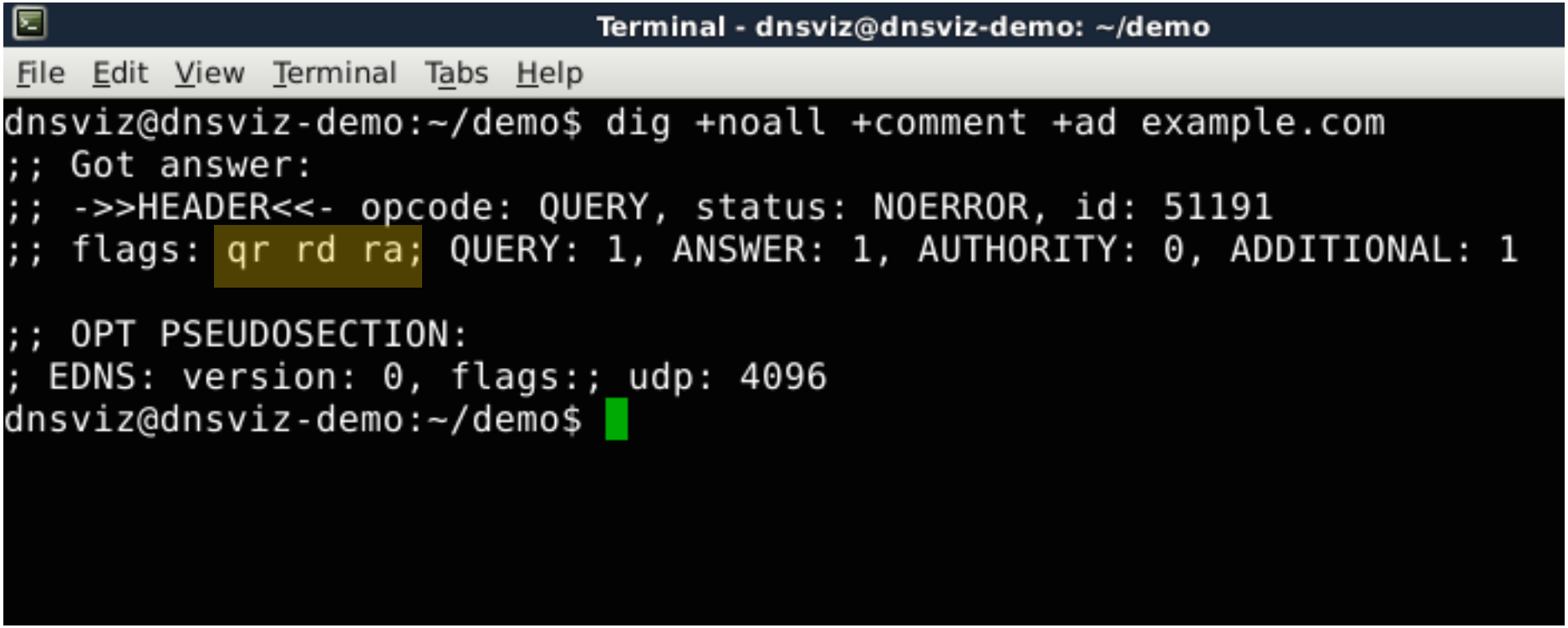
```
$ iceweasel example.com.html &
```

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

View `dnsviz` Output: Signed example.com Zone



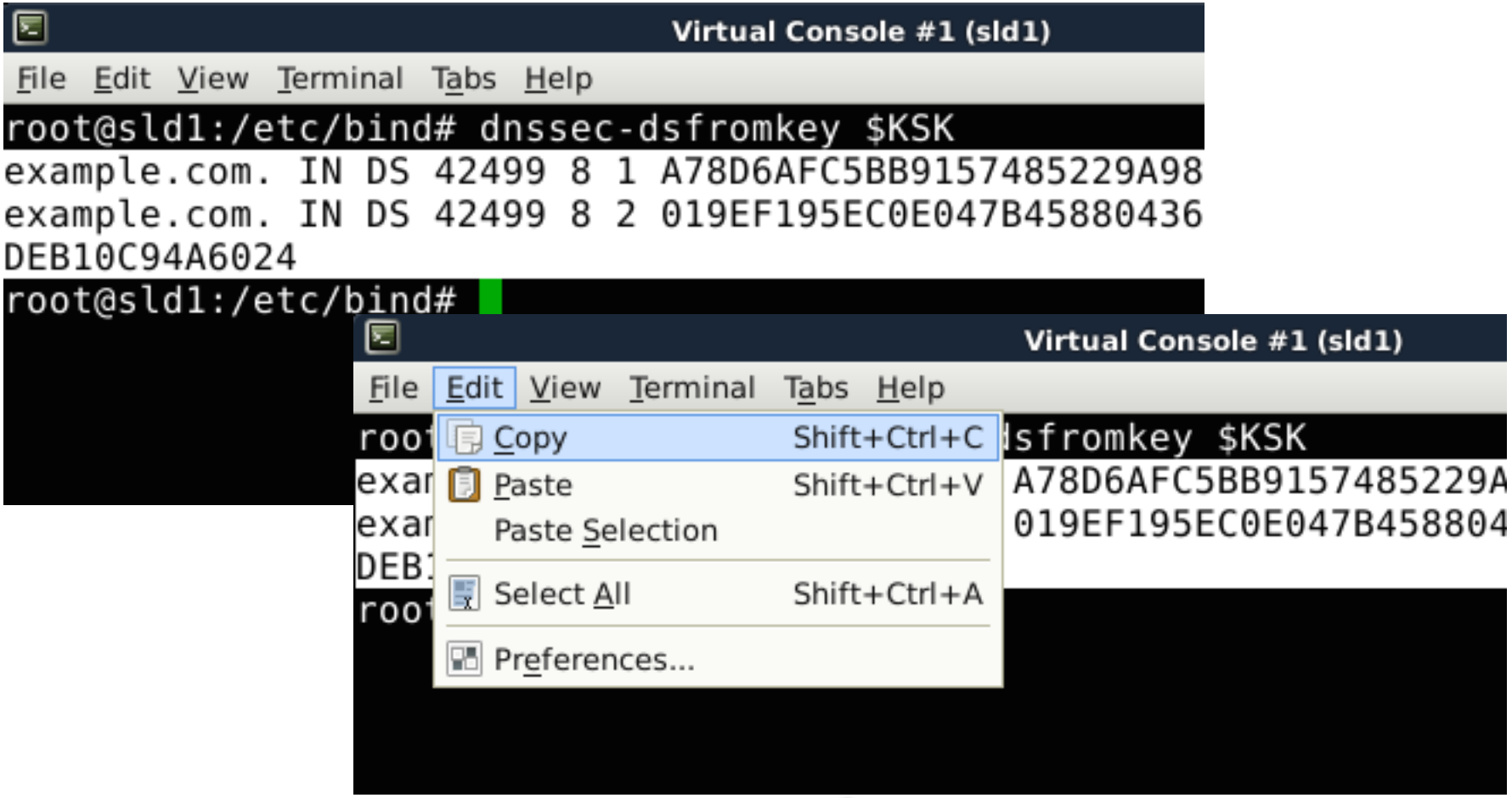
View `dig` Output: no AD bit



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

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

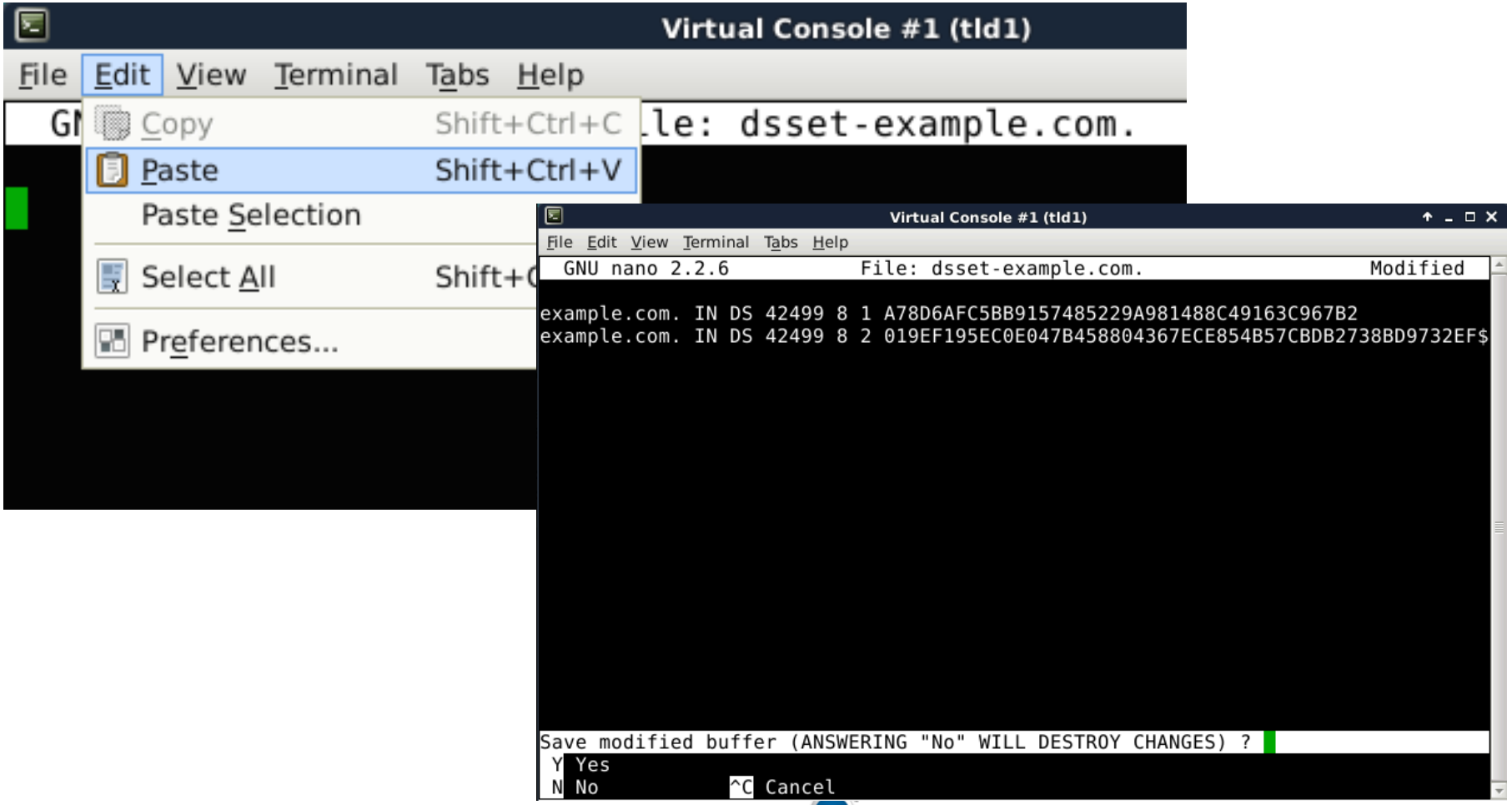
```
# dnssec-dsfromkey $KSK
```



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

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

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



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

- Sign zone (on **tld1**)

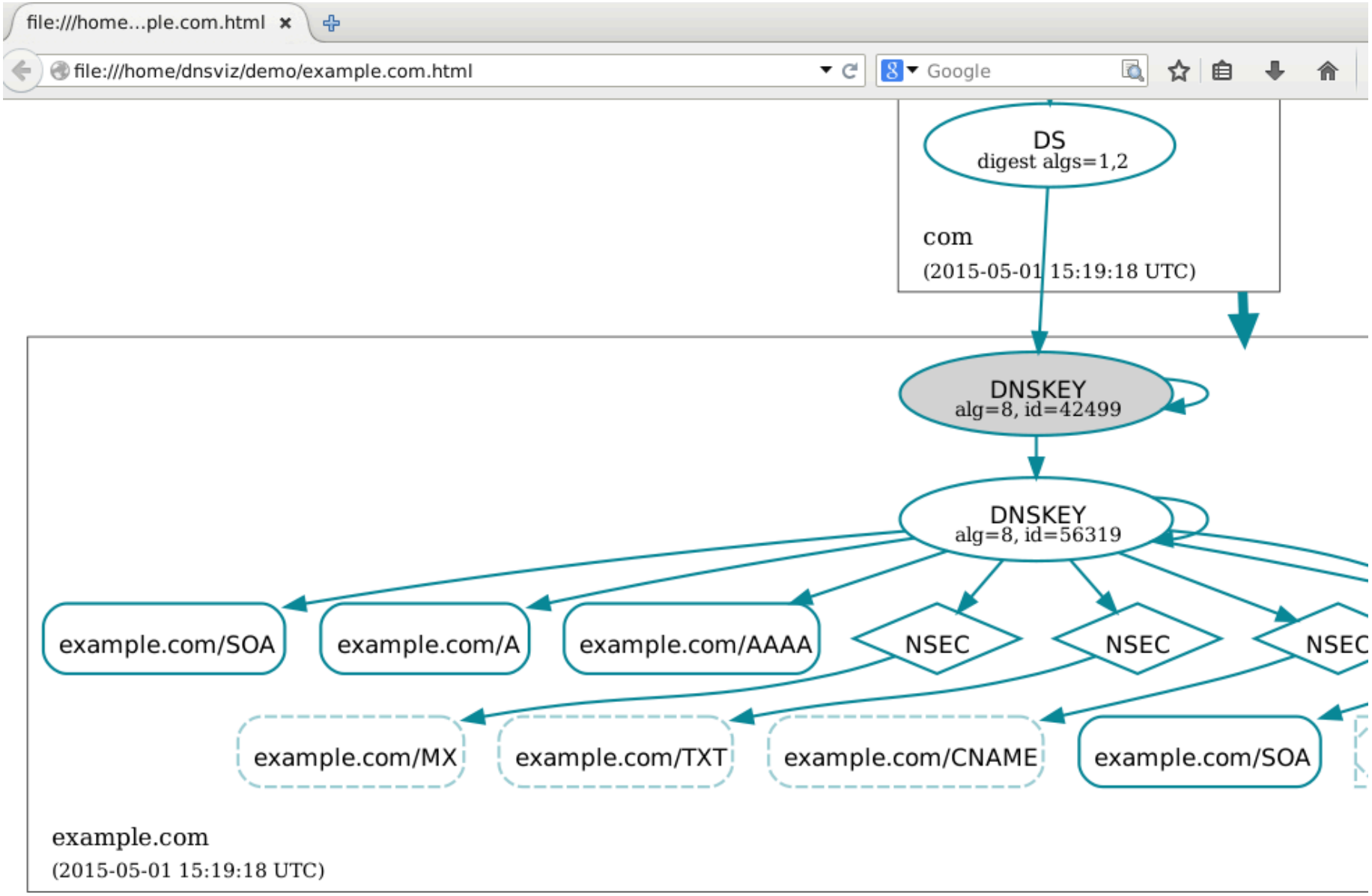
```
# ./resign_tld
```

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

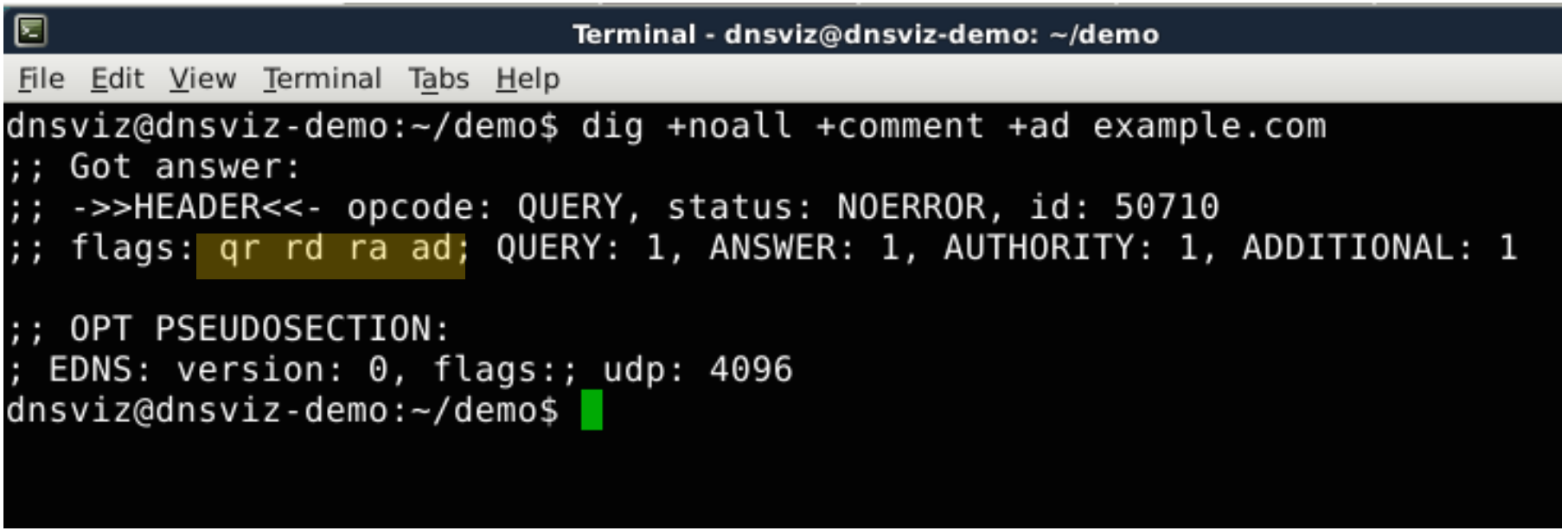
```
$ iceweasel example.com.html &
```

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

View `dnsviz` Output: Full Chain of Trust



View `dig` Output: AD bit



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
```

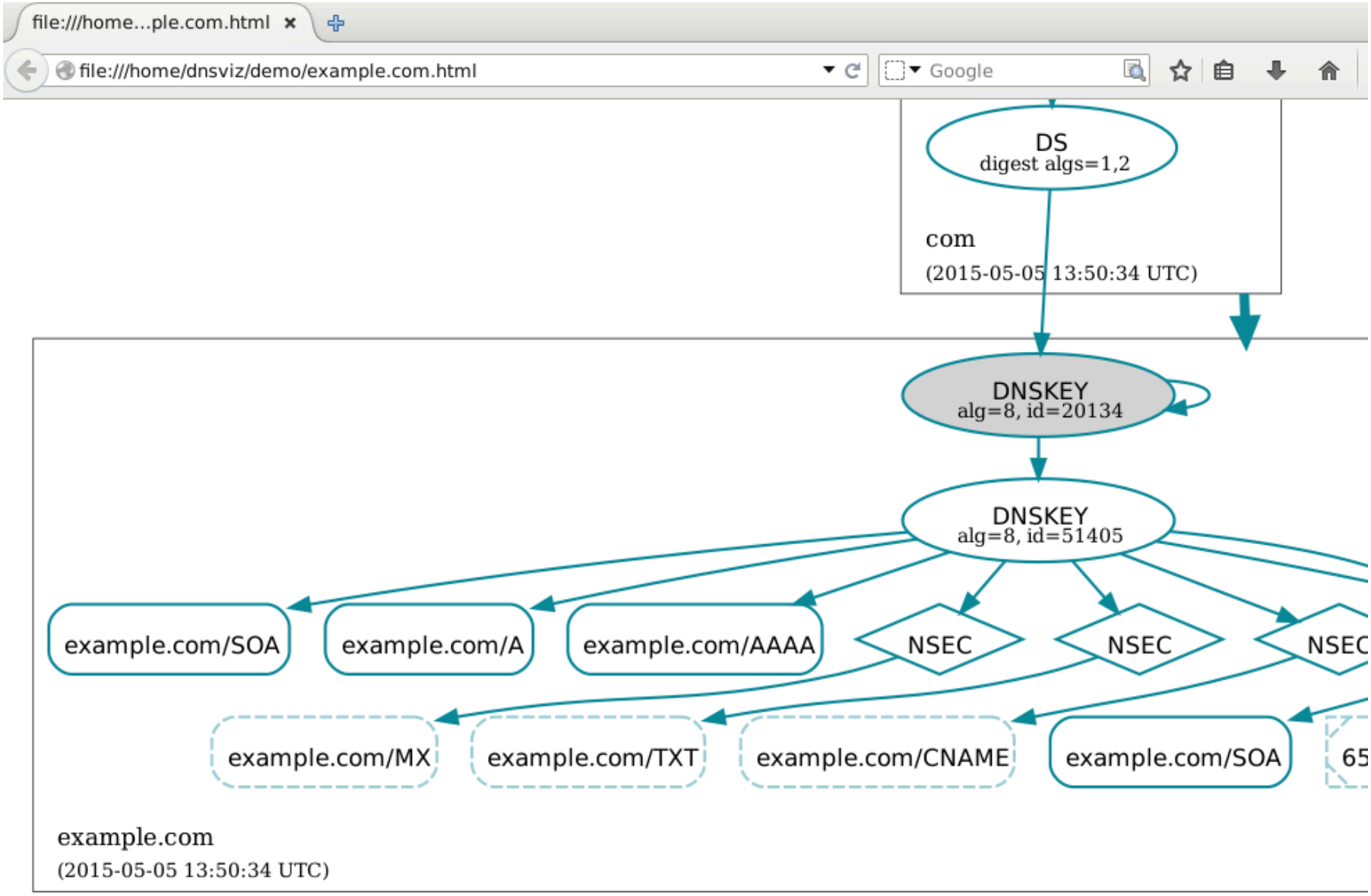
```
# service bind9 reload
```

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

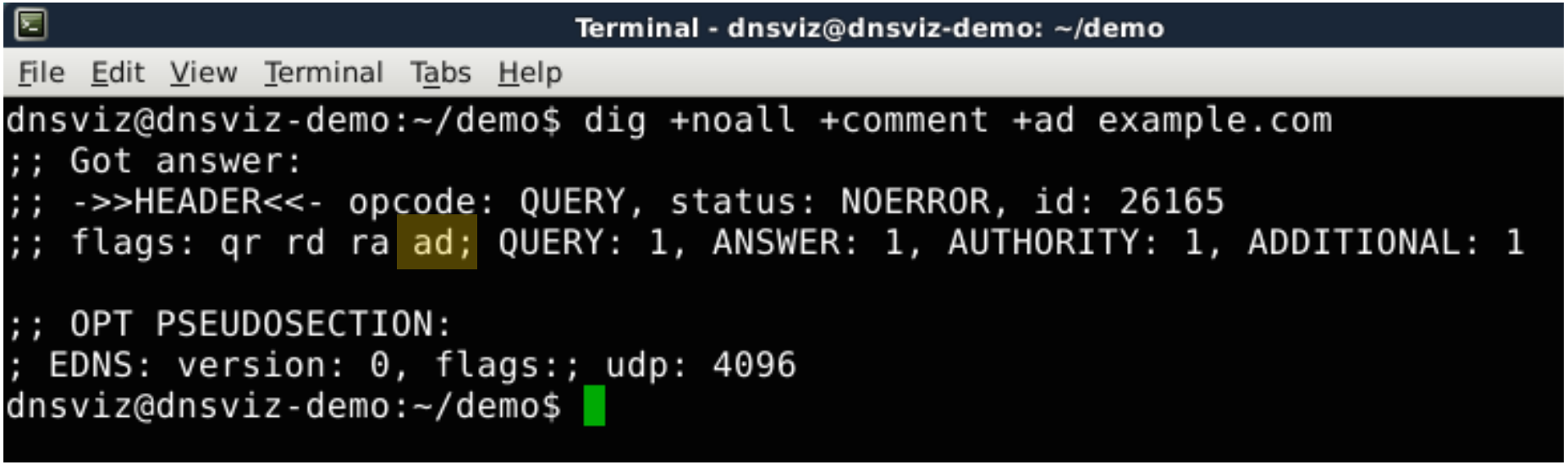
```
$ iceweasel example.com.html &
```

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

View `dnsviz` Output: KSK-only



View `dig` Output: AD bit



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

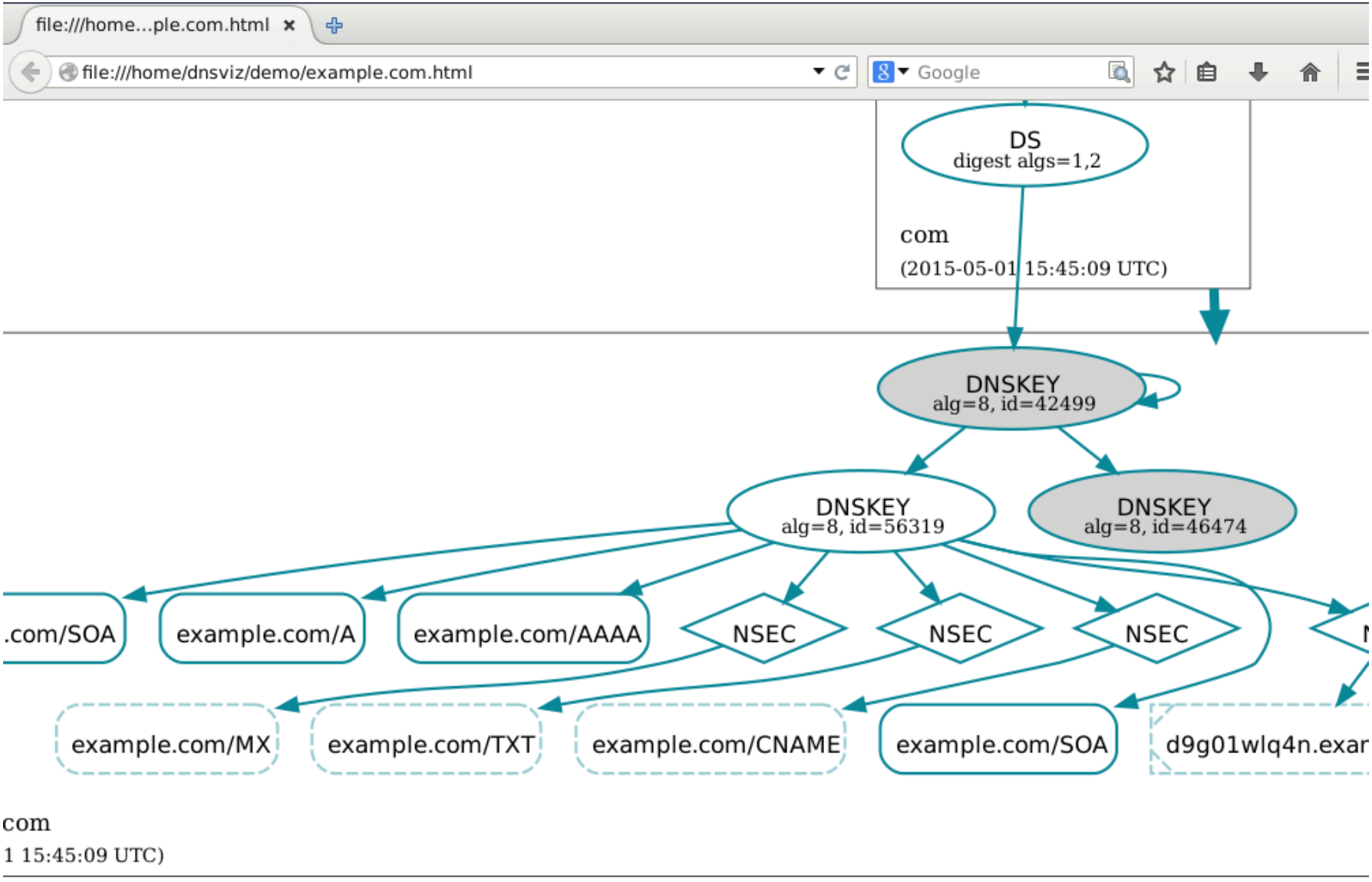
```
# service bind9 reload
```

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

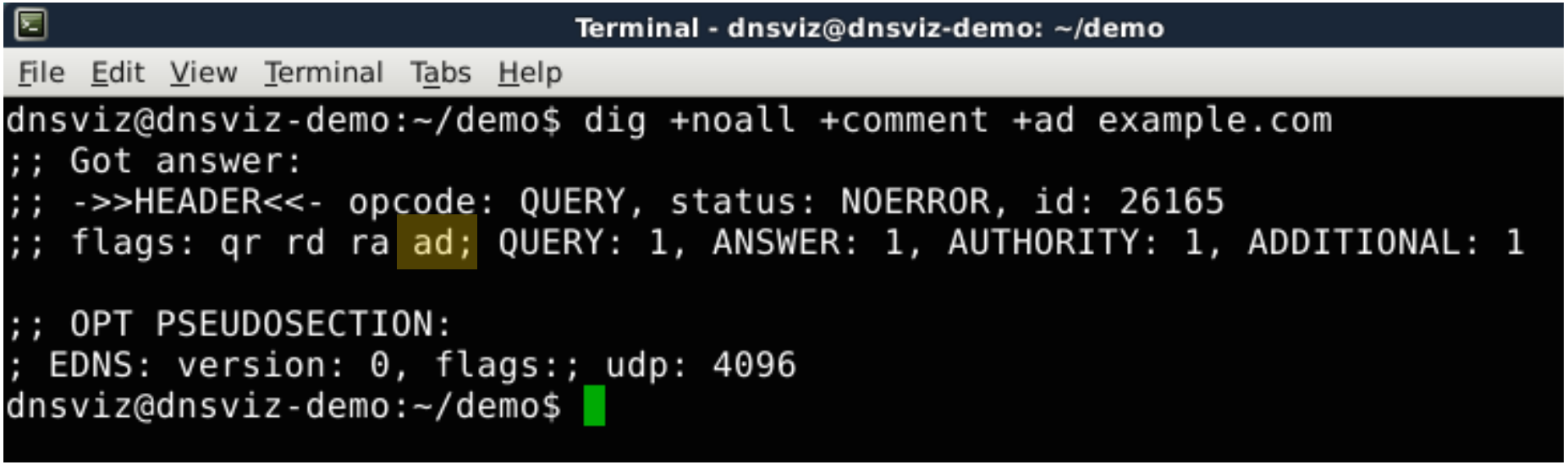
```
$ iceweasel example.com.html &
```

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

View `dnsviz` Output: Standby KSK



View `dig` Output: AD bit



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

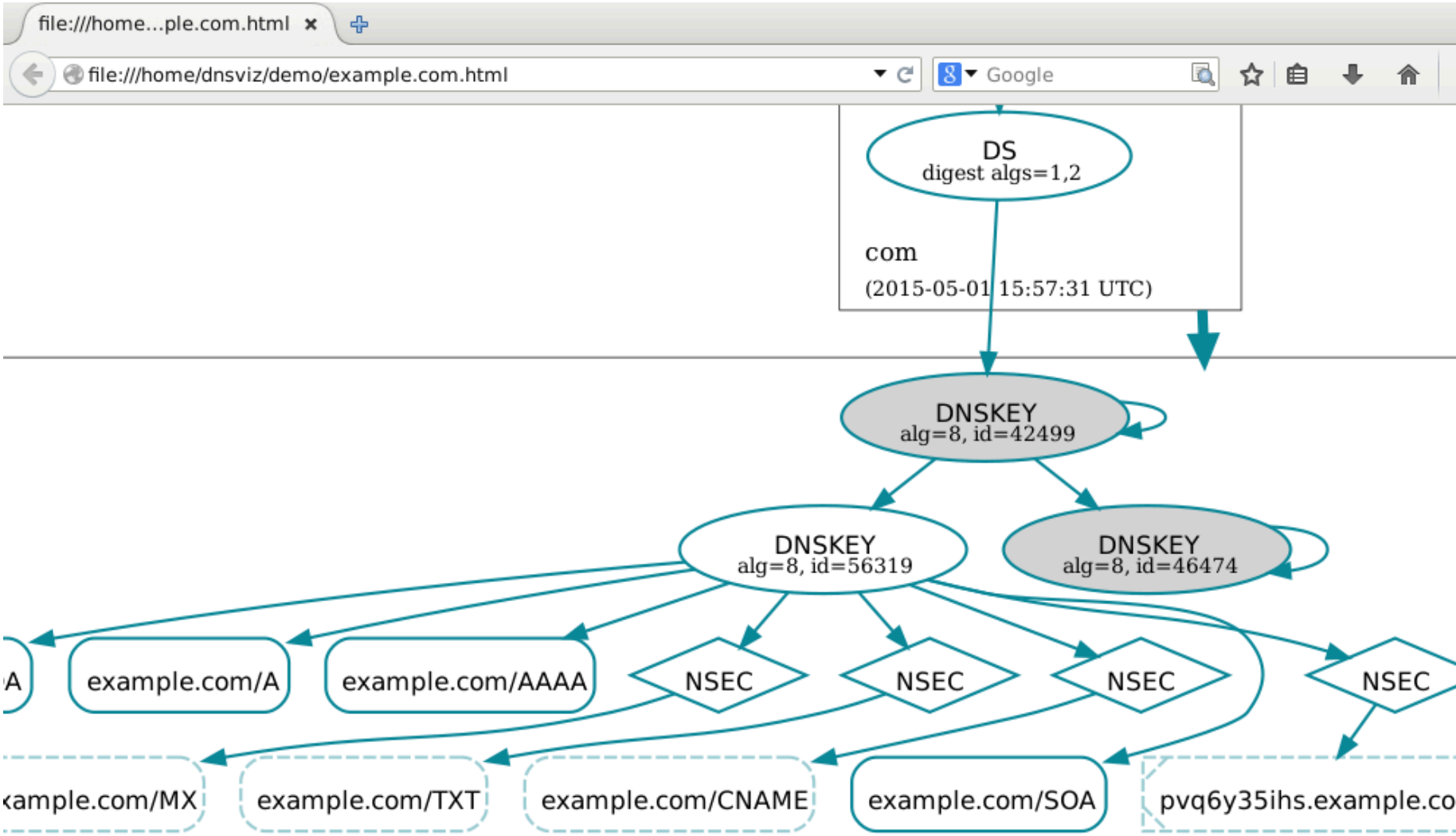
```
# service bind9 reload
```

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

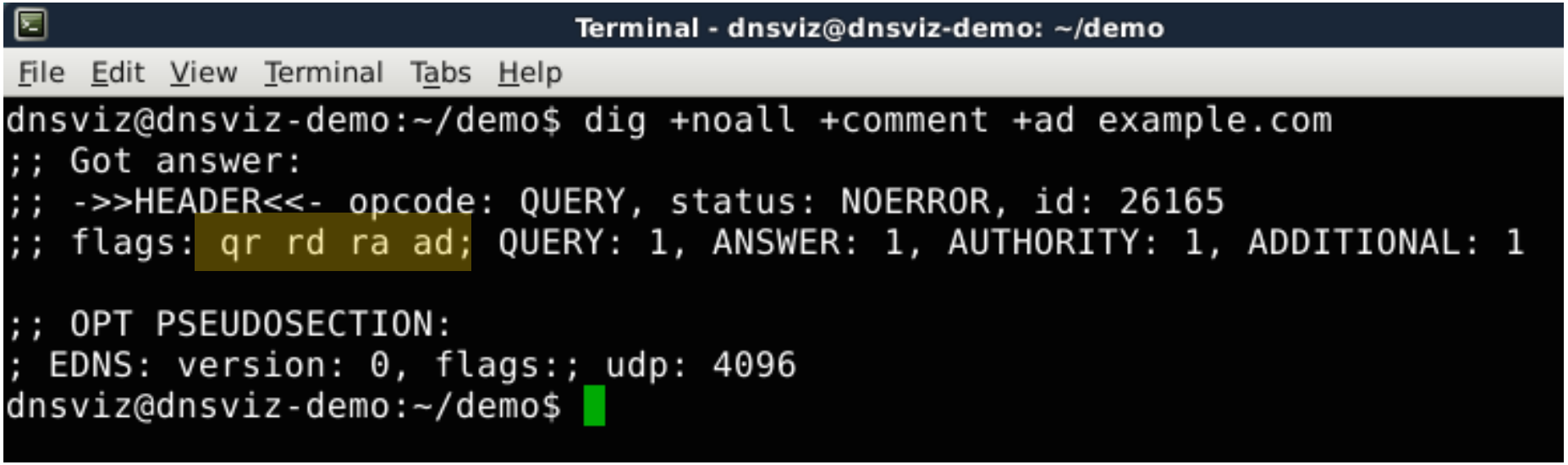
```
$ iceweasel example.com.html &
```

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

View `dnsviz` Output: Multiple KSKs



View `dig` Output: AD bit



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

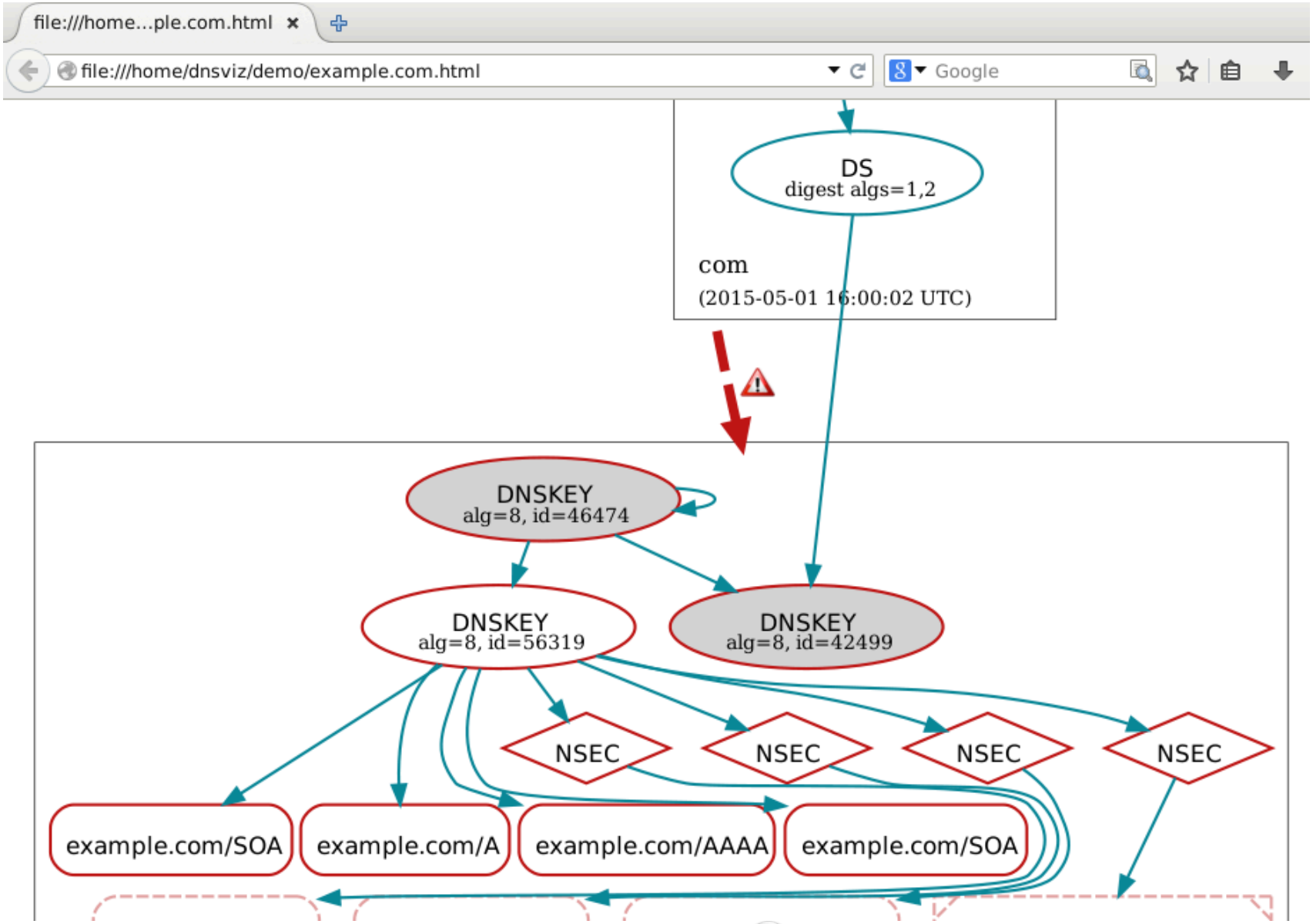
```
# service bind9 reload
```

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

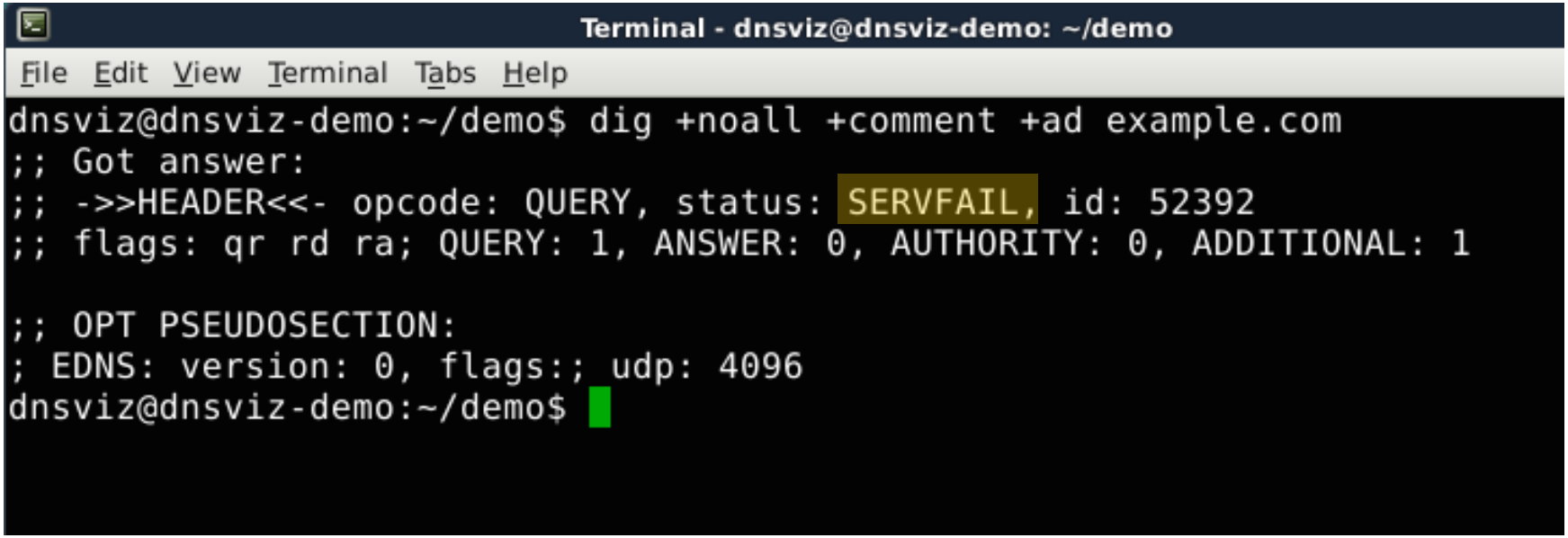
```
$ iceweasel example.com.html &
```

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

View `dnsviz` Output: DS Mismatch



View `dig` Output: SERVFAIL



Tamper with Record Content (9.15 – 9.17)

- Change SOA record:

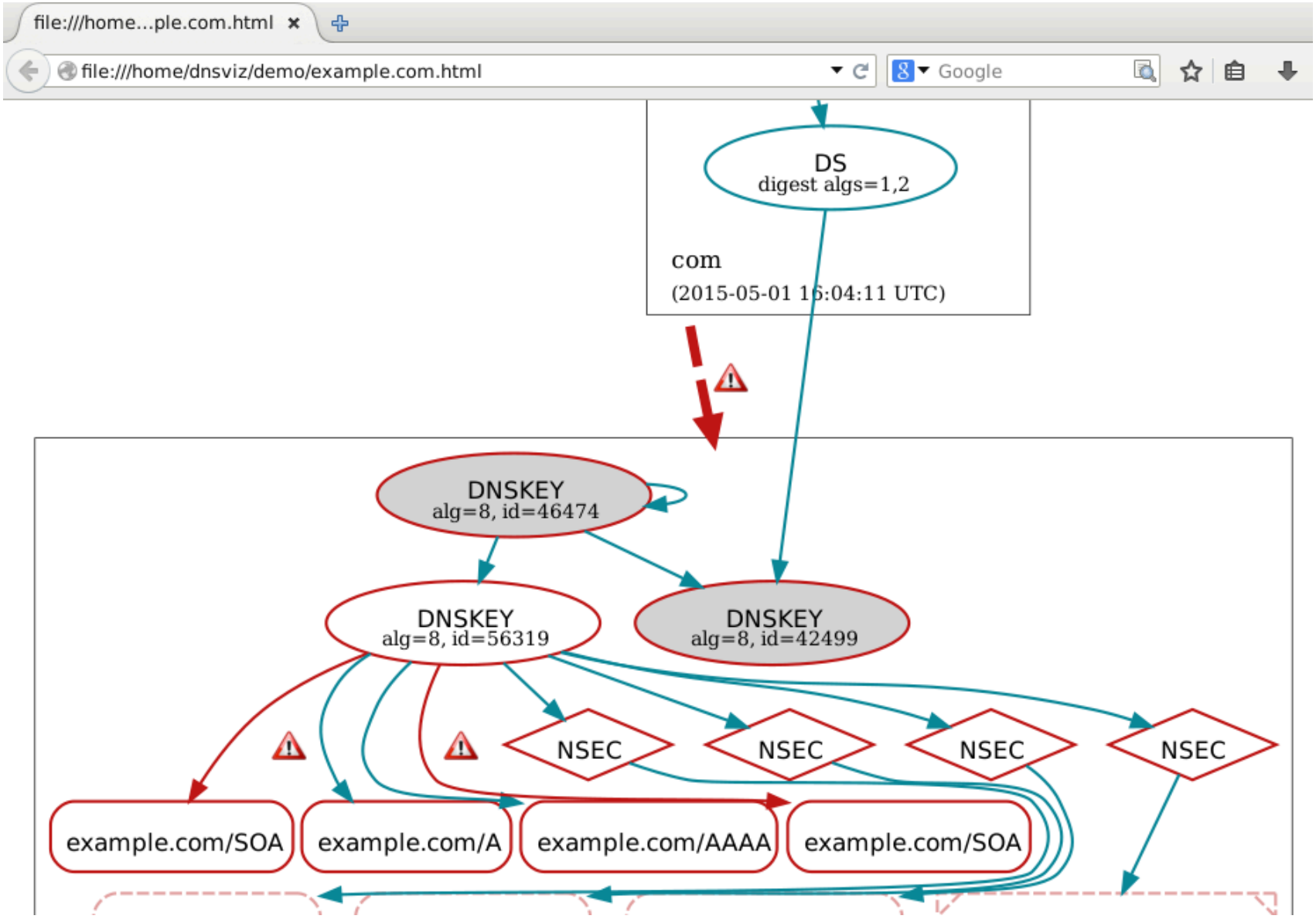
```
# sed -i -e 's/root.localhost/root1.localhost/' \
    db.example.com.signed
```

```
# 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
```

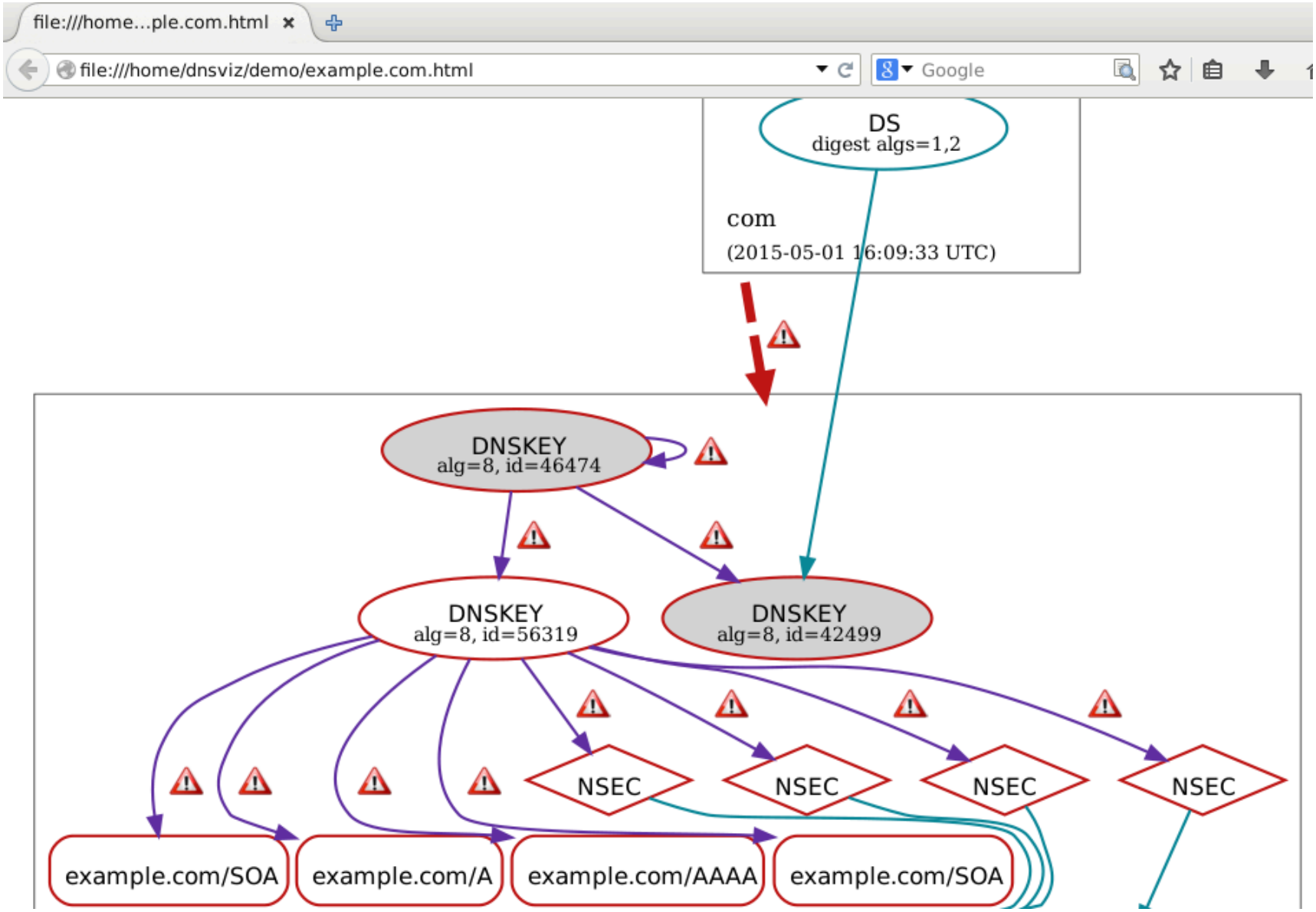
- Reload zone

```
# service bind9 reload
```

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

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

View `dnsviz` Output: Expired RRSIGs



Modify Path MTU (9.22 – 9.23)

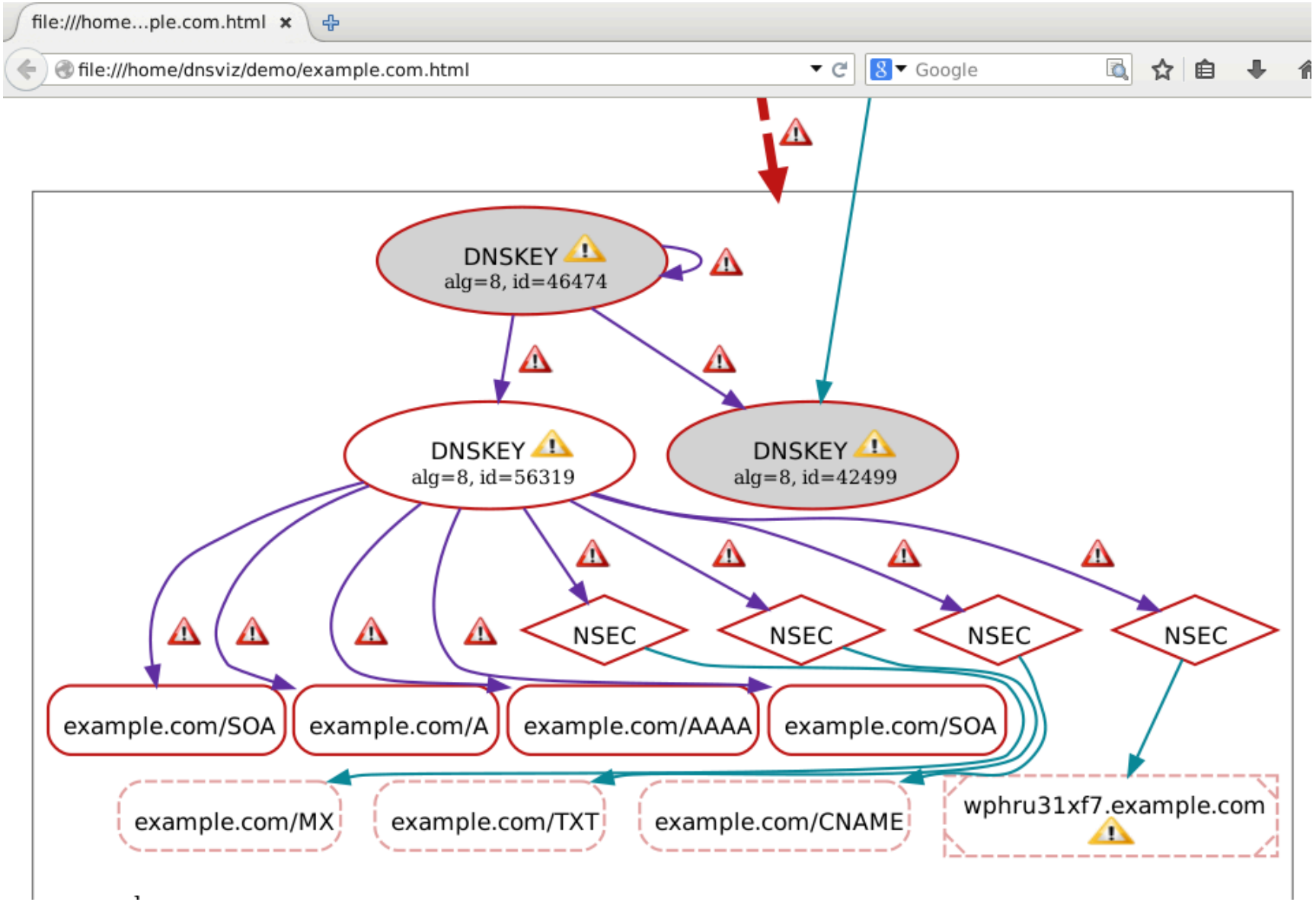
- Drop UDP responses with payloads larger than 512 bytes

```
# 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 `dnsget` 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": "0UGEAAABAAQAAAABB2V4YW1wbGUDY29tAAAwAAHADAA
                        "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 `dnsget` 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 fie
                                            "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 dnsget and dnsviz, e.g., for use with cron

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

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

rm $dnsget_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™