



VERISIGN®

Multi-Vantage Point DNS Diagnostics and Measurement

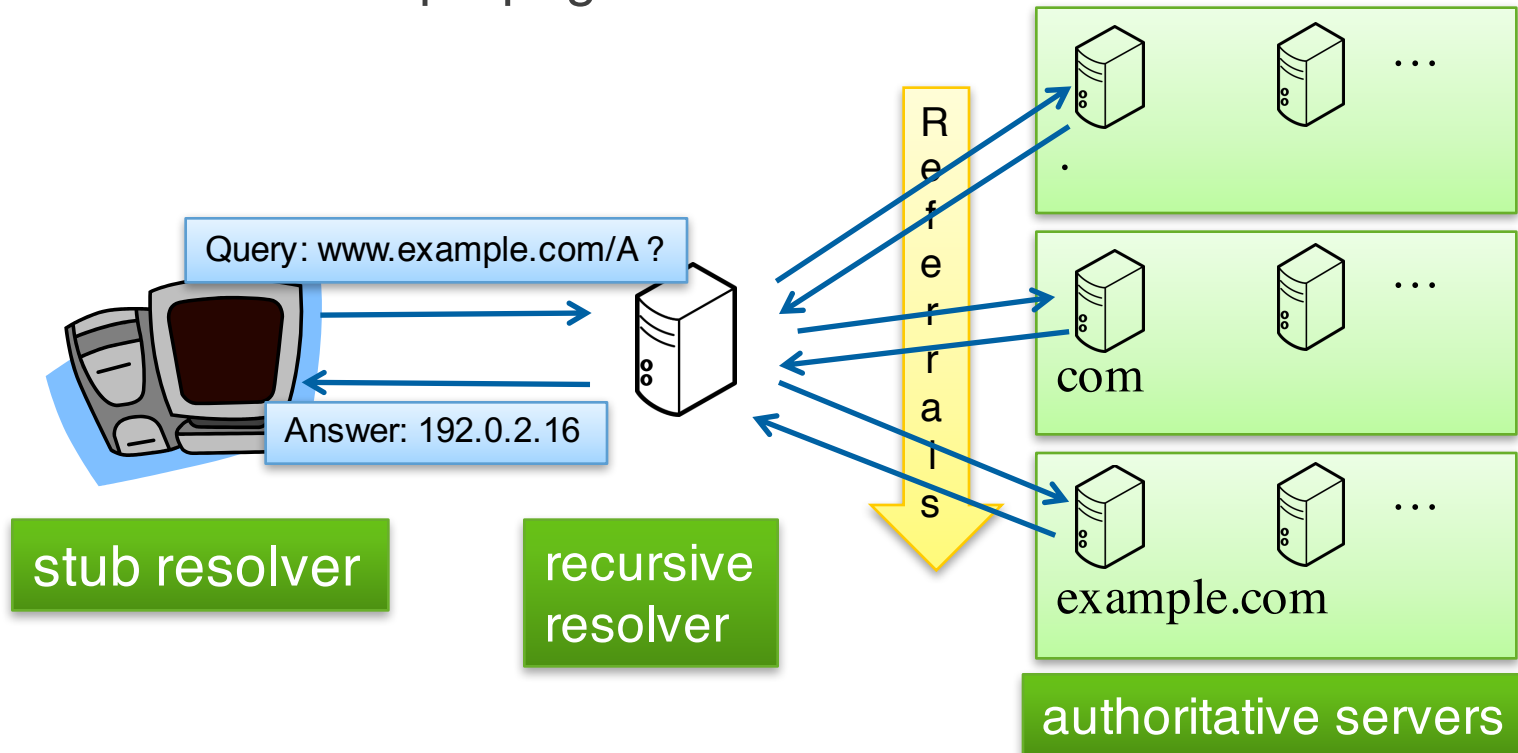
Casey Deccio, Verisign Labs

NANOG 67, Chicago

June 14, 2016

DNS Name Resolution in a Nutshell

- Stub resolver queries recursive resolver for a name.
- Recursive resolver asks authoritative servers.
- Authoritative servers refer recursive resolvers to server that can answer.
- Answers are propagated back to stub.



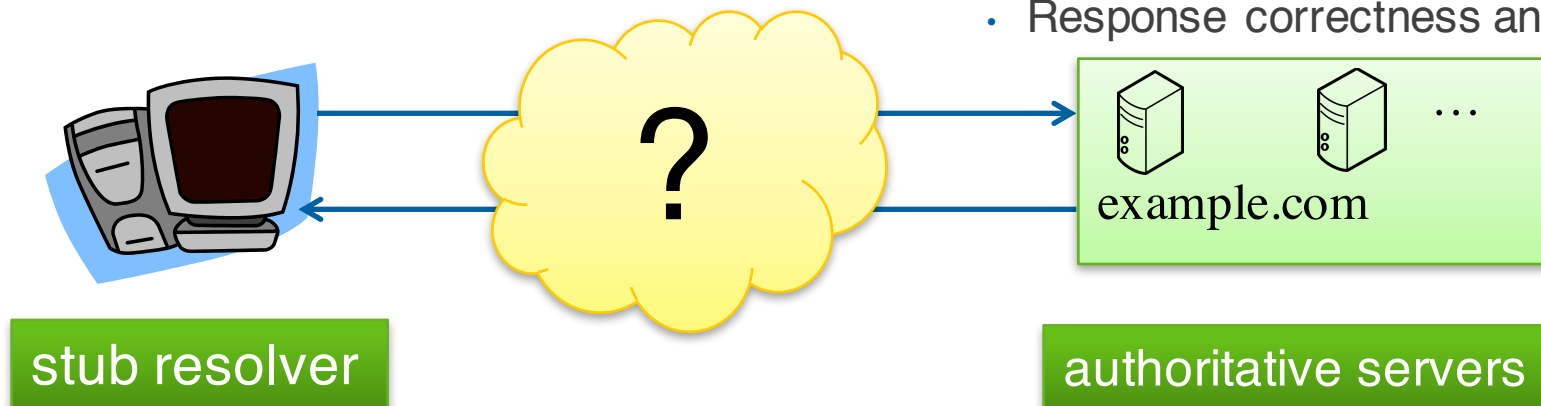
The Path Between Stub and Authoritative

Paths

- Recursive resolver(s)
- Middleboxes
- Firewalls
- NATs
- IPv4/IPv6 network paths / anycast
- Authoritative servers

Potential Issues

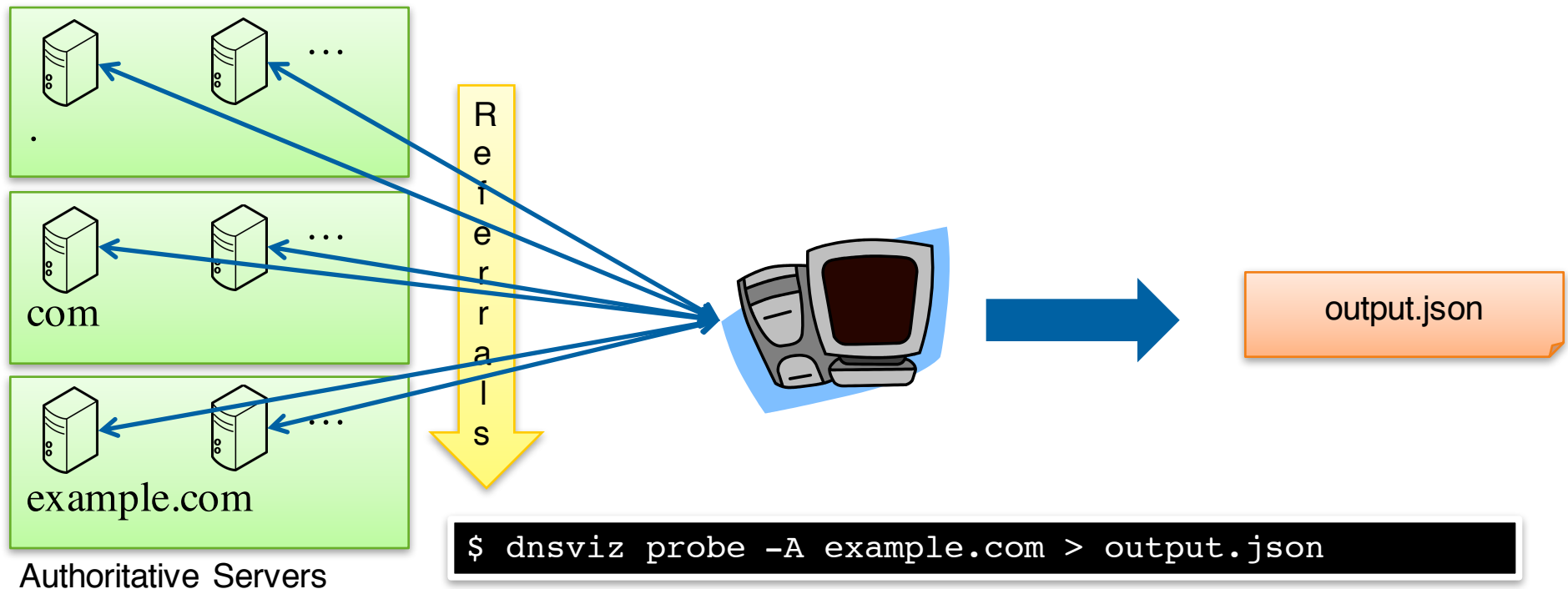
- TCP/UDP connectivity
- Response latency
- Path/server EDNS capabilities: version, options, flags
- DNSSEC records
- Large/fragmented packets
- Record types
- Response correctness and consistency



Authoritative DNS Queries with DNSViz:

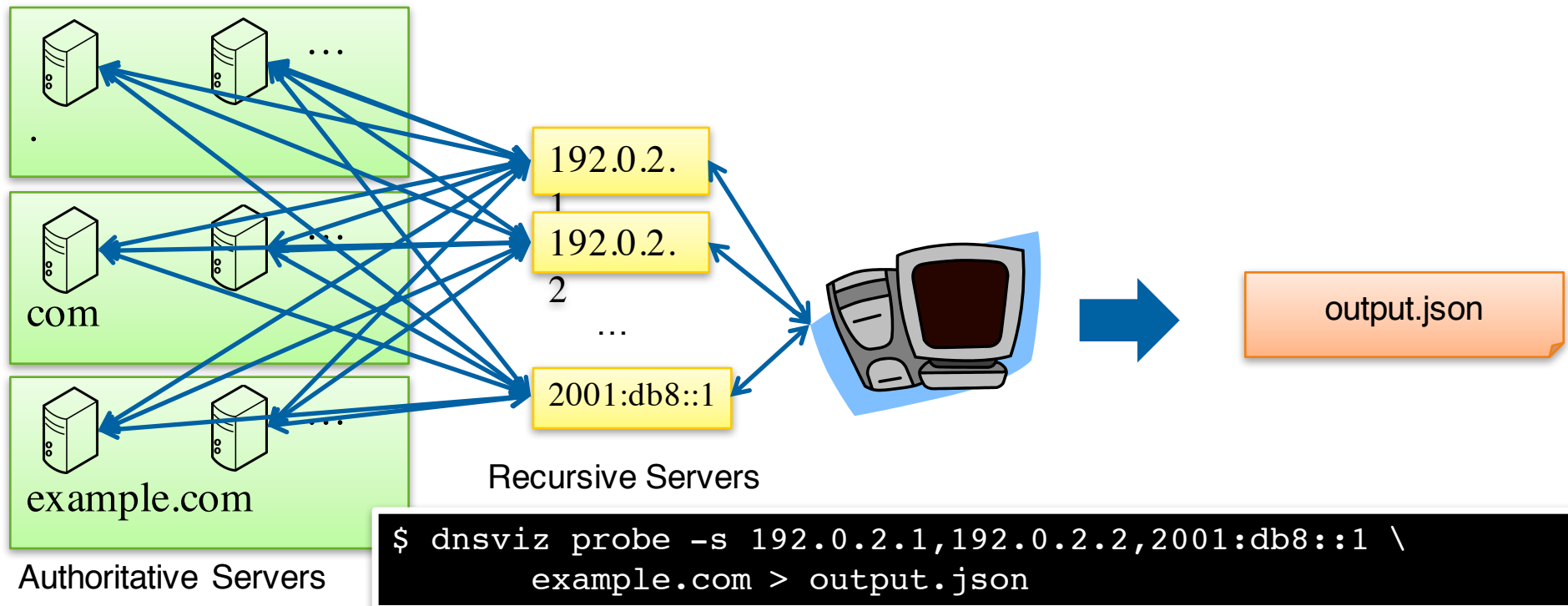
`dnsviz probe -A`

- Queries issued towards authoritative servers
(optionally, following referrals all the way from root)
- All server addresses queried
 - IPv4/IPv6
 - UDP/TCP



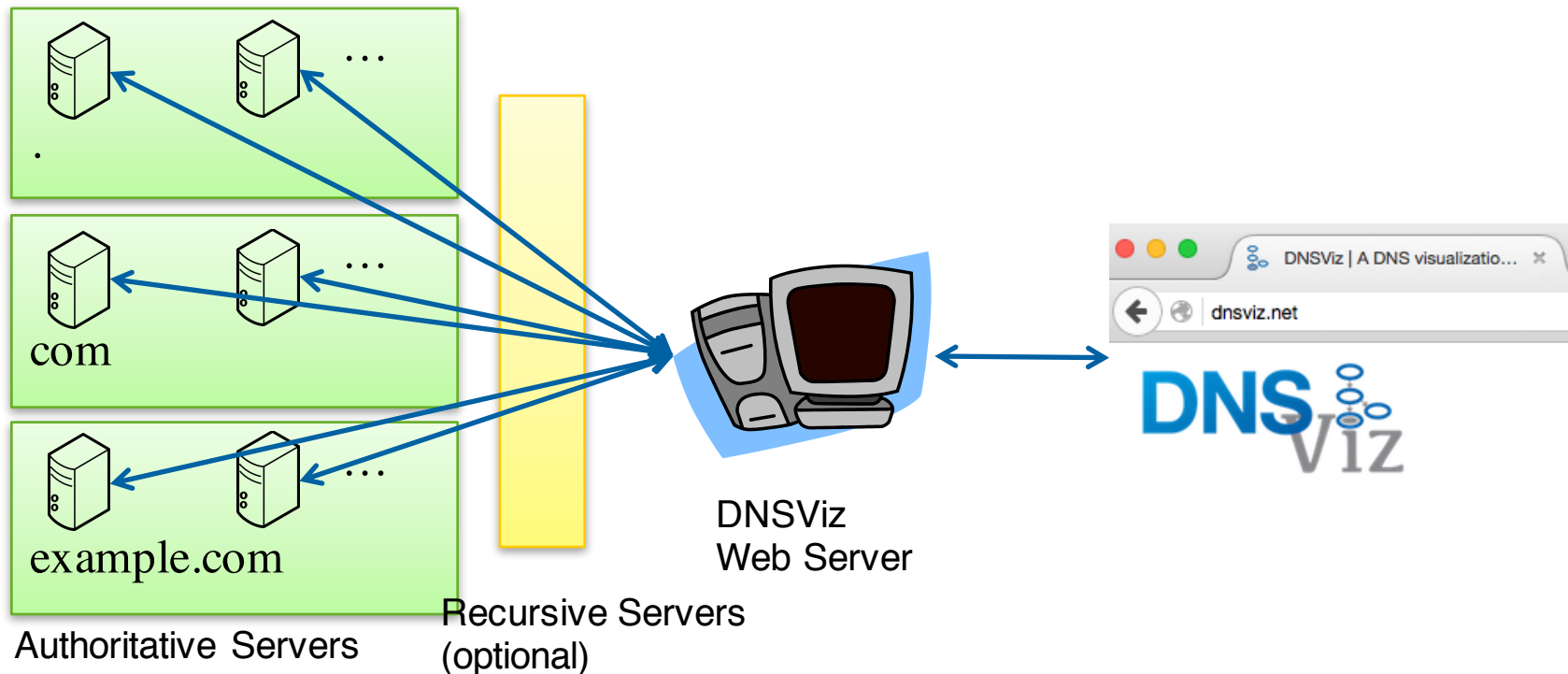
Recursive DNS Queries with DNSViz (default): `dnsviz probe`

- Queries issued towards recursive servers (all the way to the root, by default)
- Default recursive servers used if none specified.

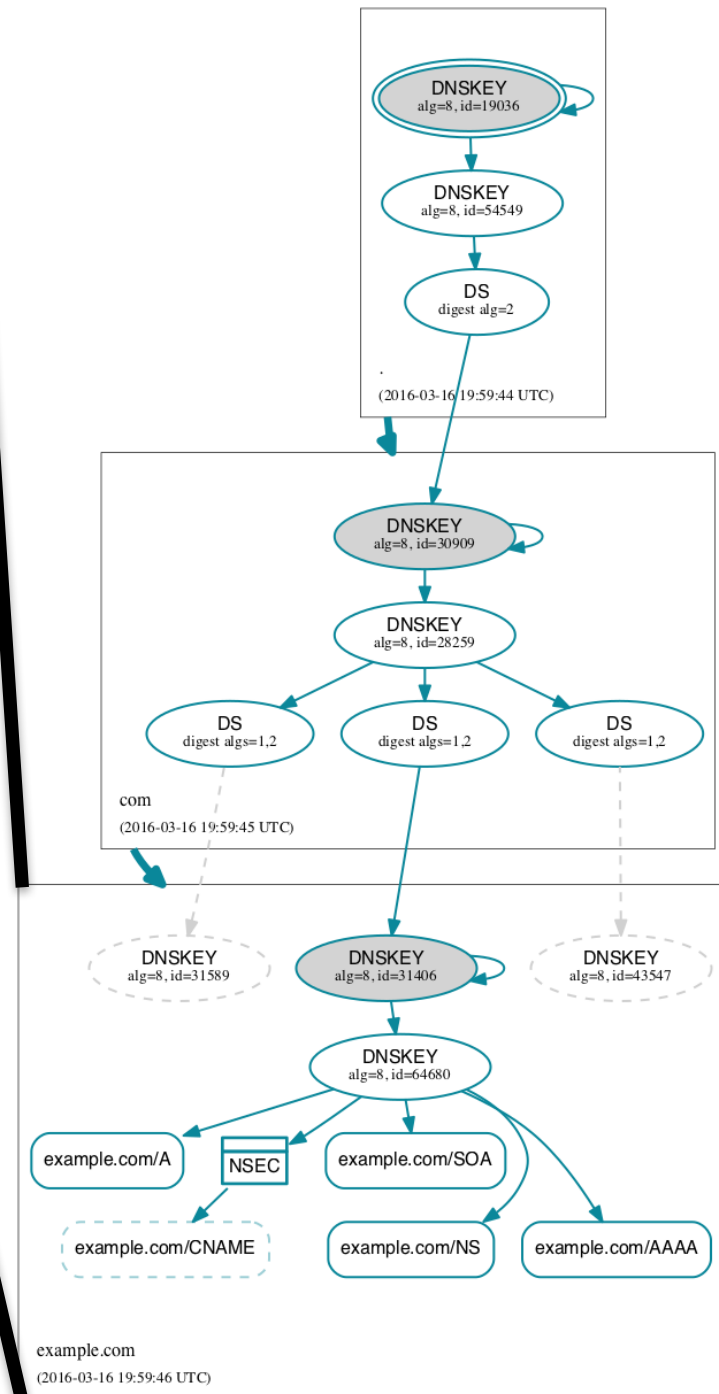
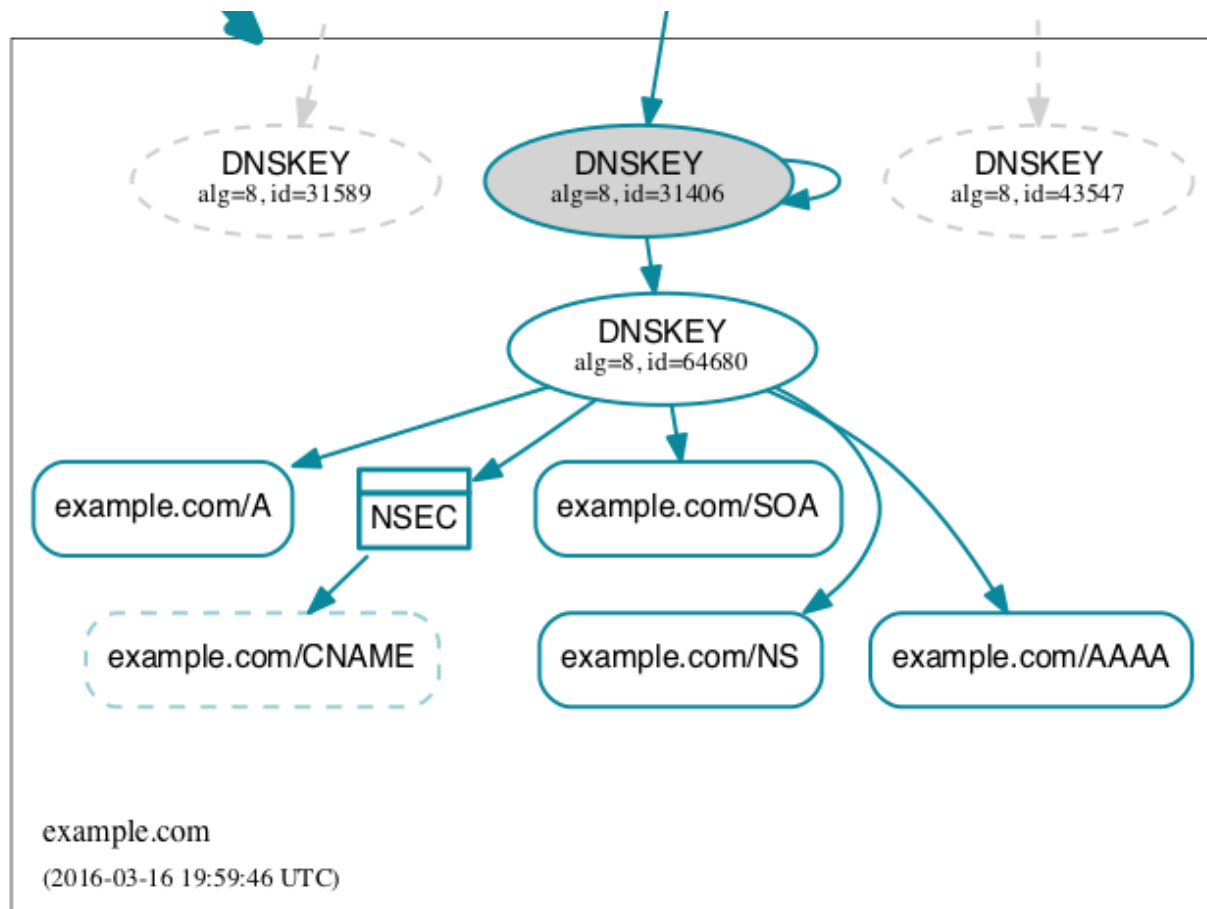


DNSViz Web Interface – Authoritative or Recursive Analysis

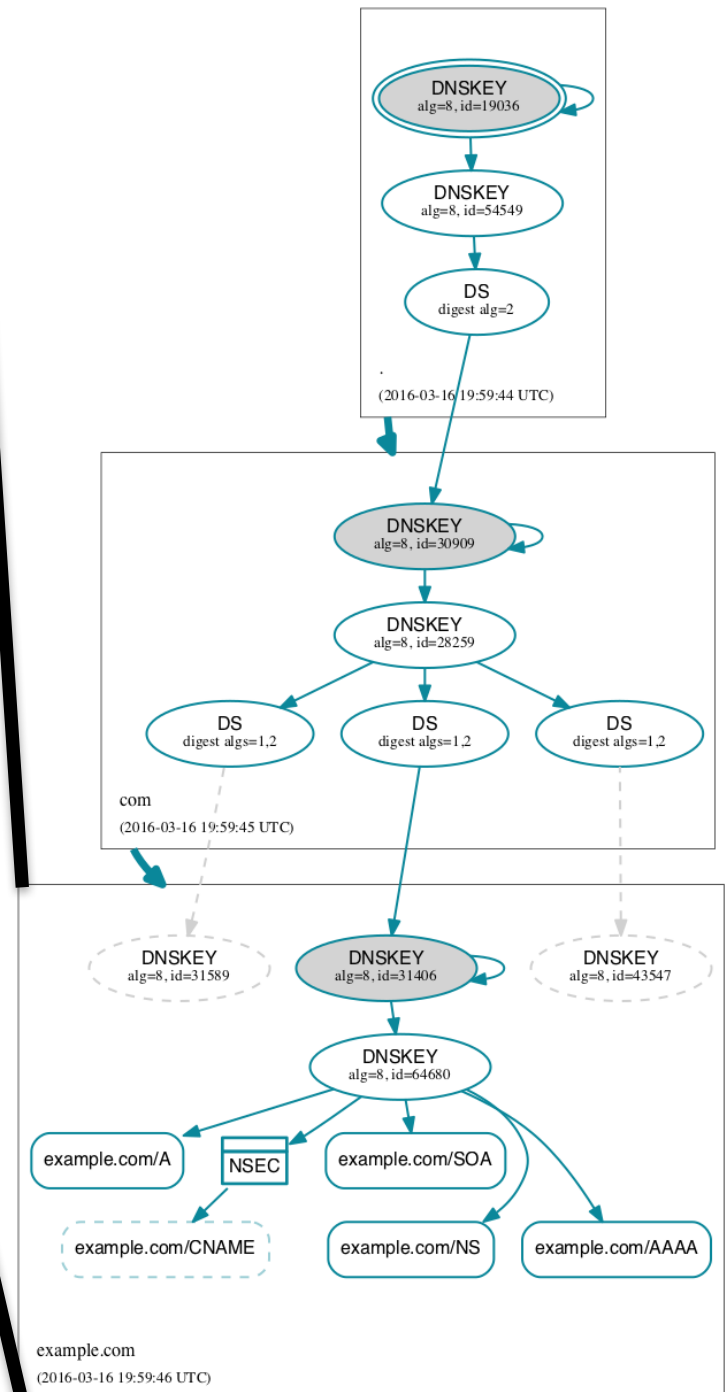
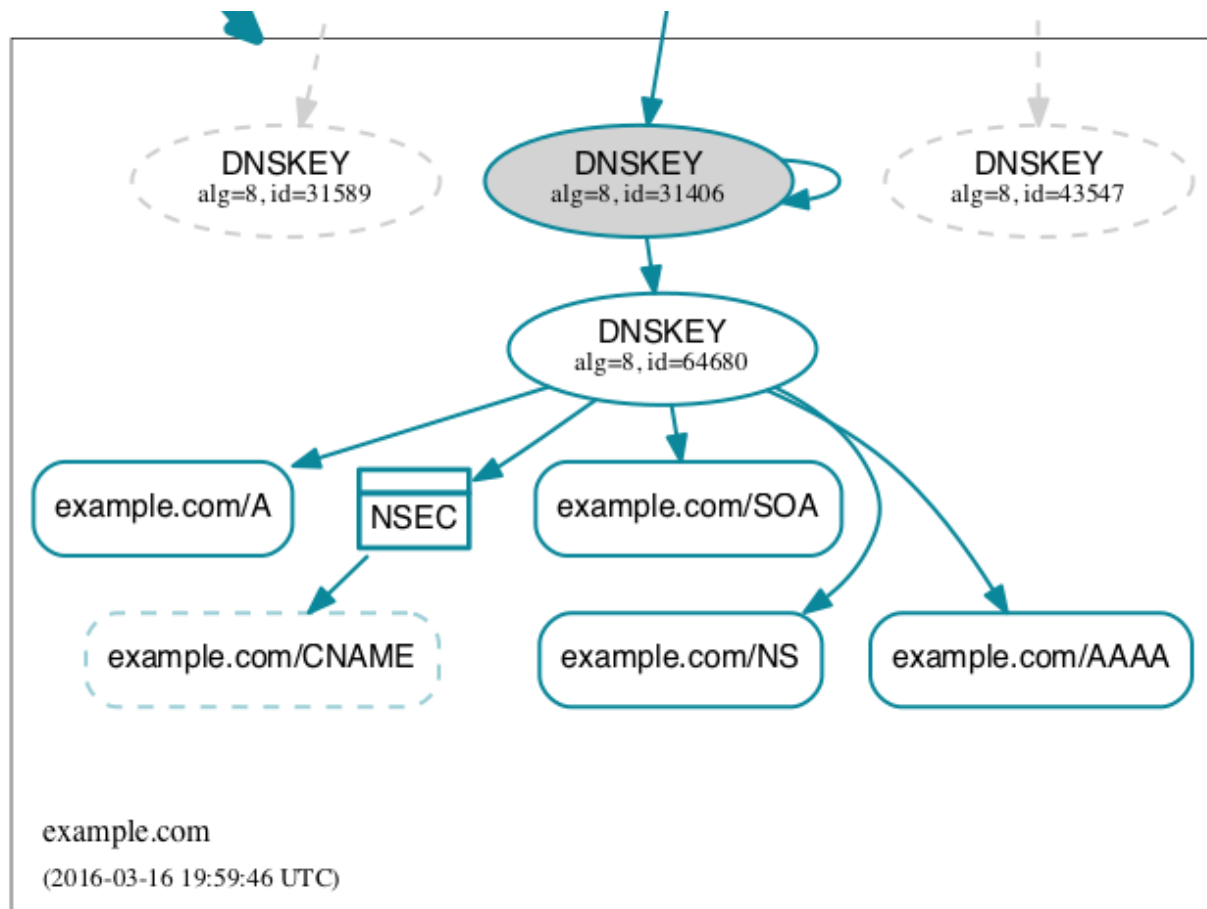
- Select “authoritative” or “recursive” analysis from analysis form.



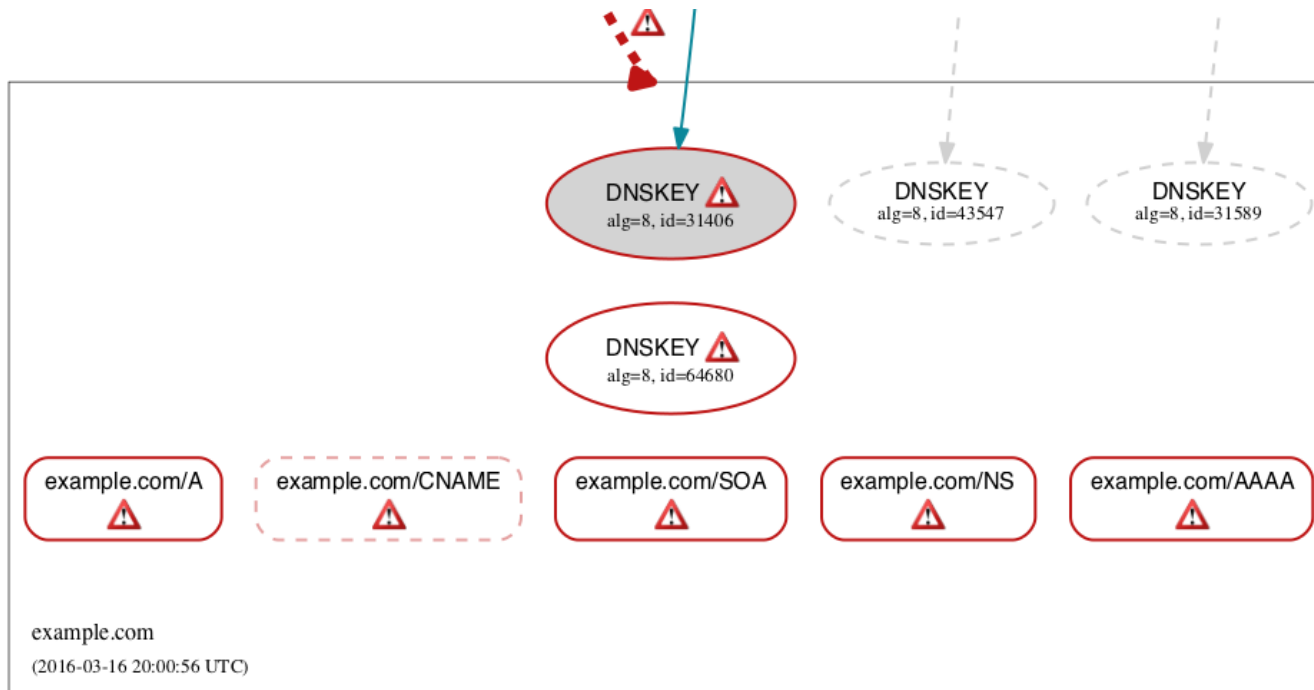
Example – Authoritative View



Example – Recursive View #1

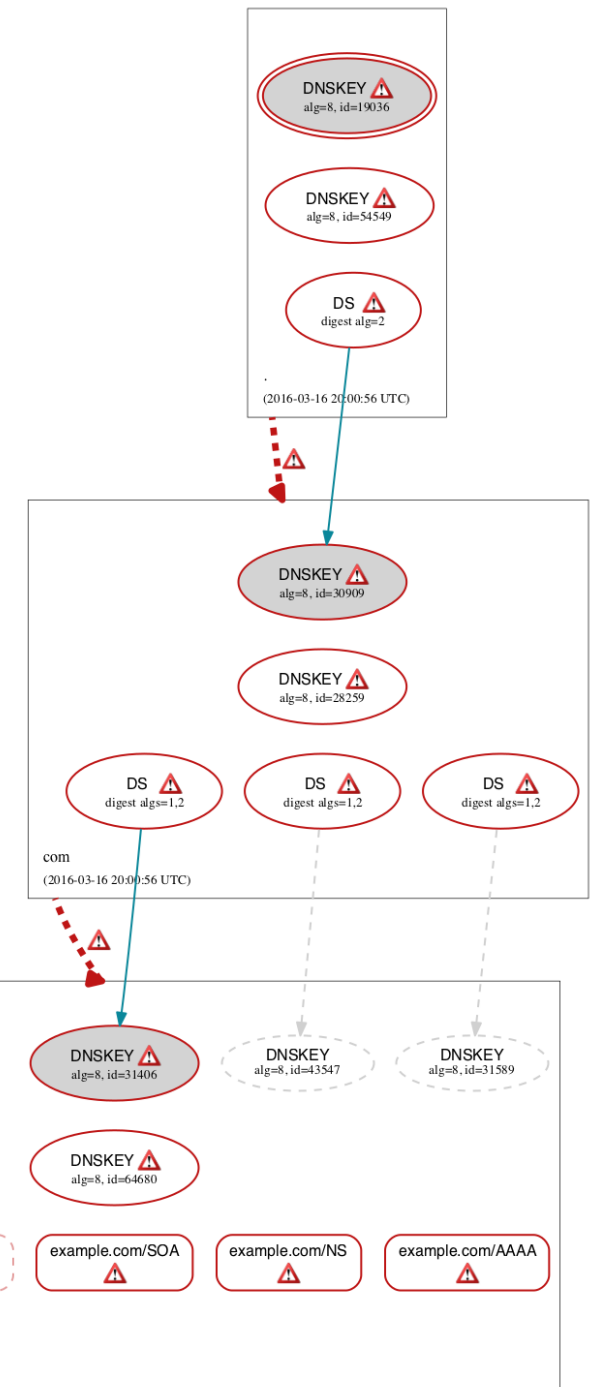


Example – Recursive View #2

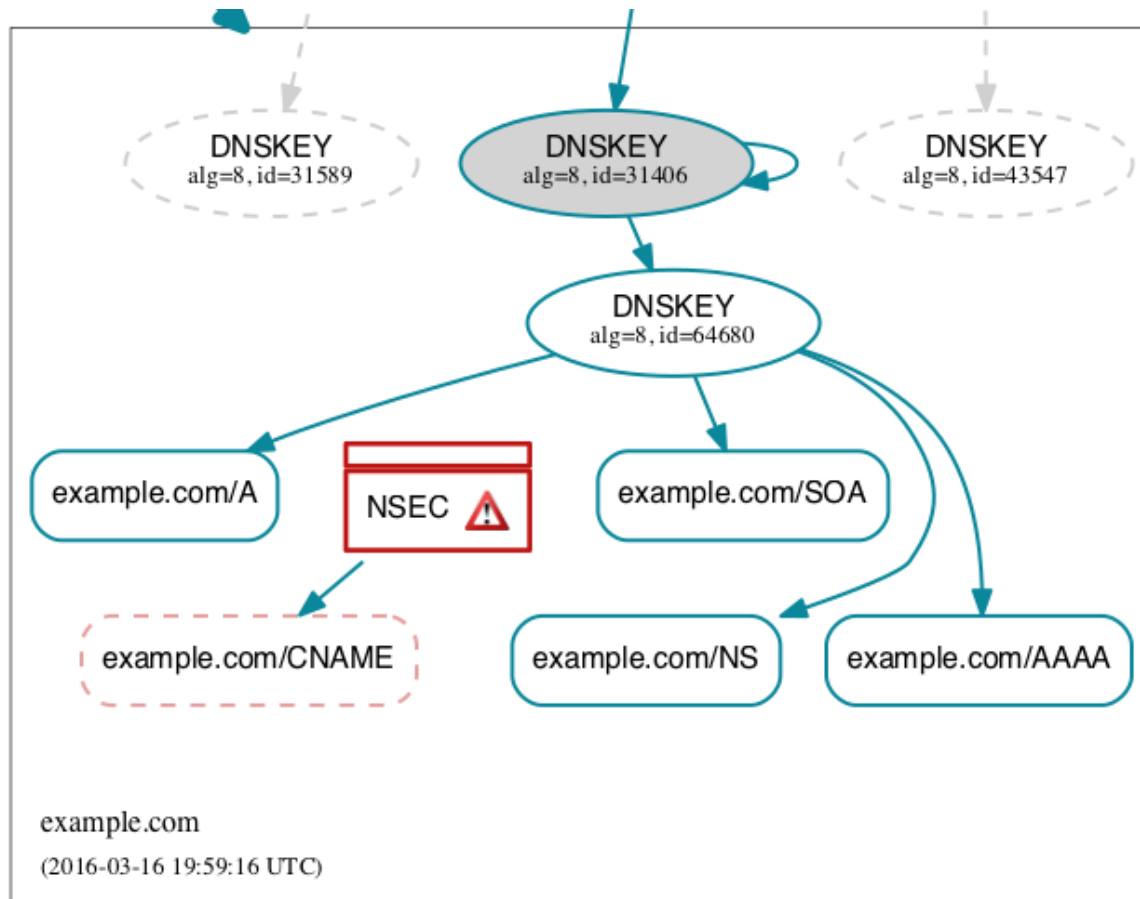


Problem:

- No DNSSEC records returned

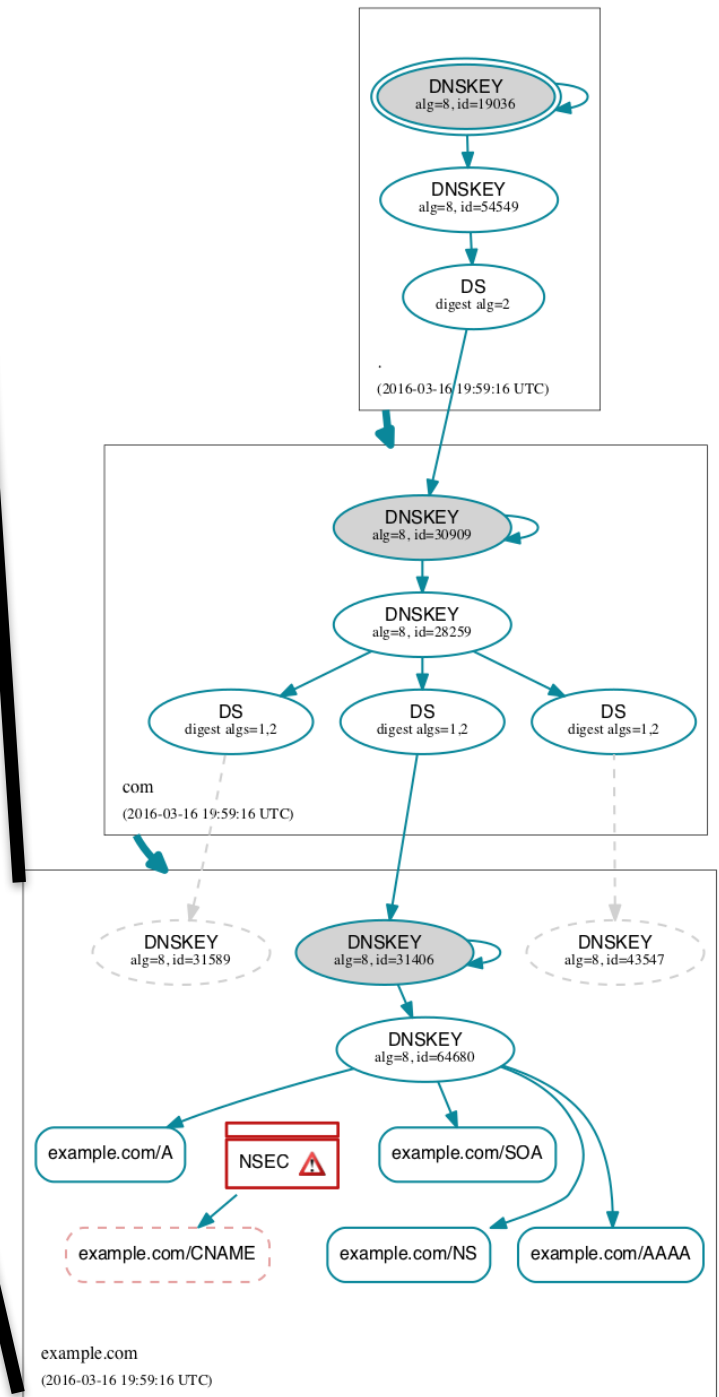


Example – Recursive View #3



Problem:

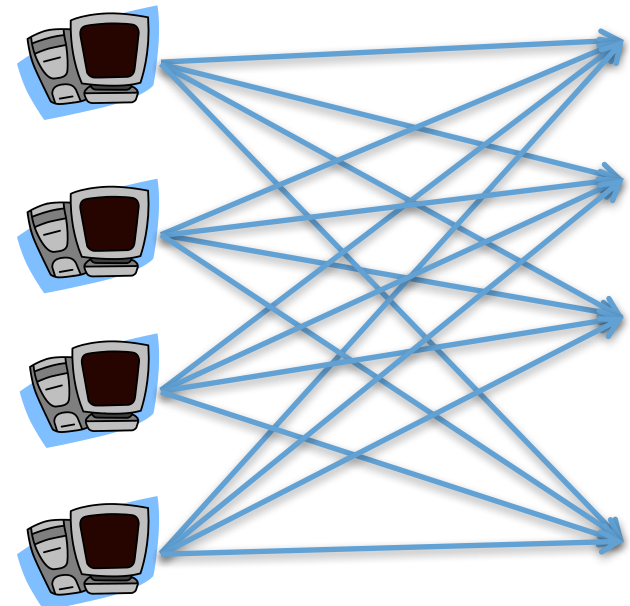
- No RRSIG records returned to cover NSEC(3)



Measuring from Other Vantage Points

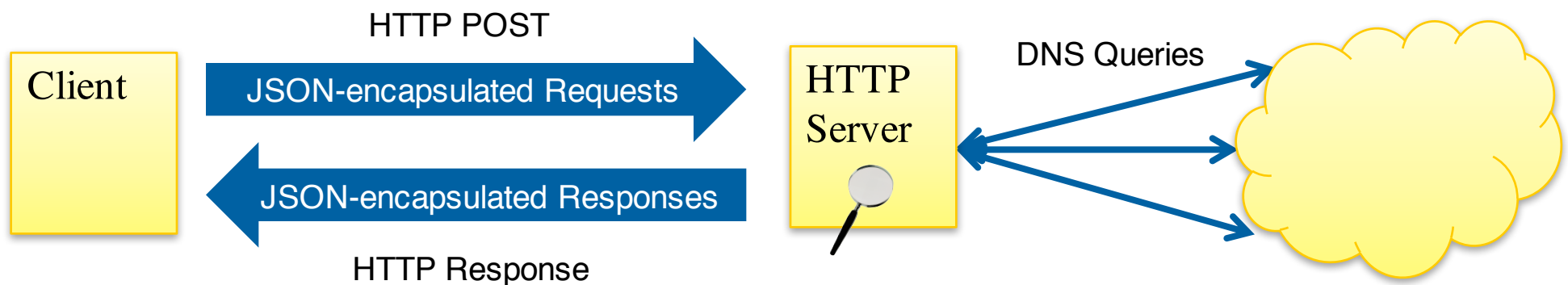
- Considerations

- Platform access – full shell vs. API
- Queries/tests – canned vs. custom
- Availability of probes
 - Number
 - Location
- Synchronous vs. asynchronous execution
- Sequential progressive diagnostics



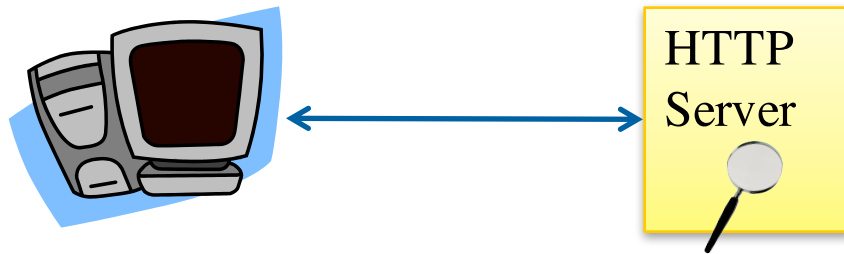
DNS Looking Glass – Over HTTP

- Client encapsulates requests using JSON.
- Requests are sent to HTTP server as data to HTTP POST request.
 - DNS message and remote server/port are included.
- HTTP server issues DNS queries specified (in parallel).
- Responses are returned from HTTP server as content of HTTP response.



DNSViz Proof-of-concept Looking Glass

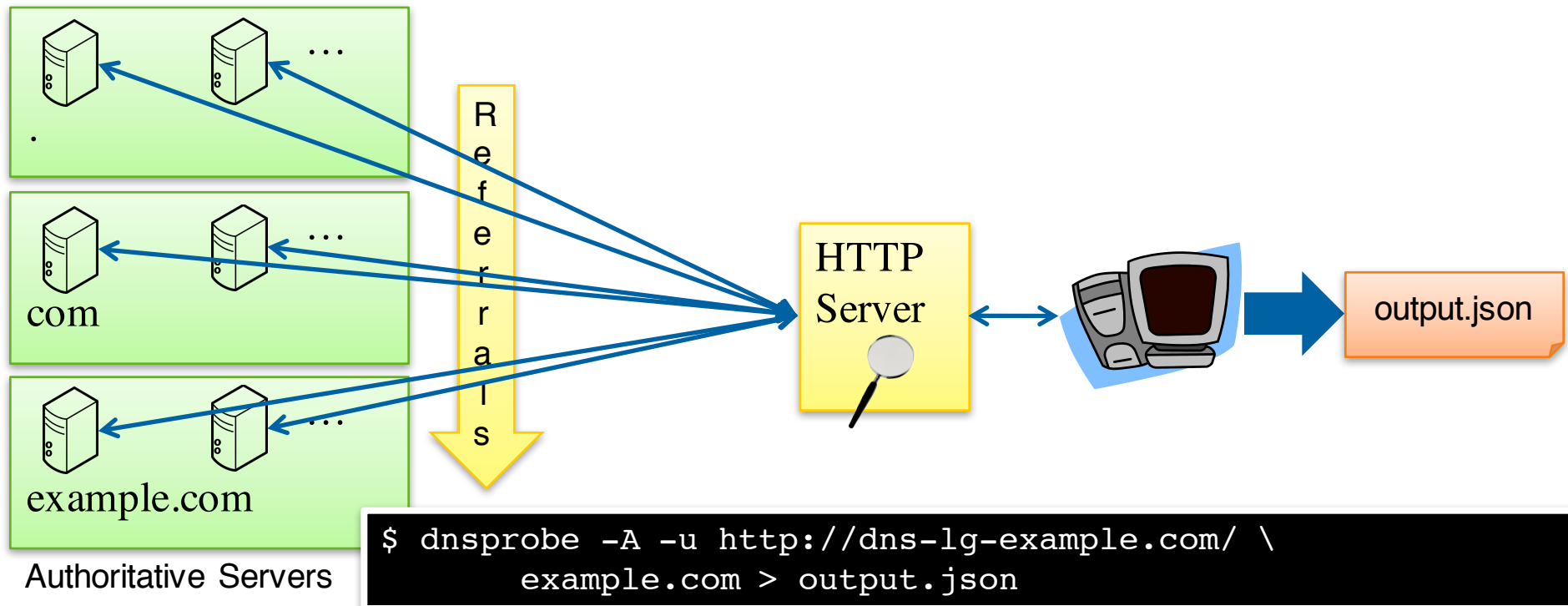
- Client/server components included with DNSViz source:
 - <https://github.com/dnsviz/dnsviz>
- Server:
 - `contrib/dnsviz-lg.cgi`
(requires DNSViz installation)
- Client:
 - `contrib/digviz`
(behaves similar to ISC `dig`)



```
$ digviz +lg=http://dns-lg-example.com/dnsviz-lg.cgi @192.0.2.1
```

Authoritative DNS Queries Using a Looking Glass: `dnsviz probe -A -u <URL>`

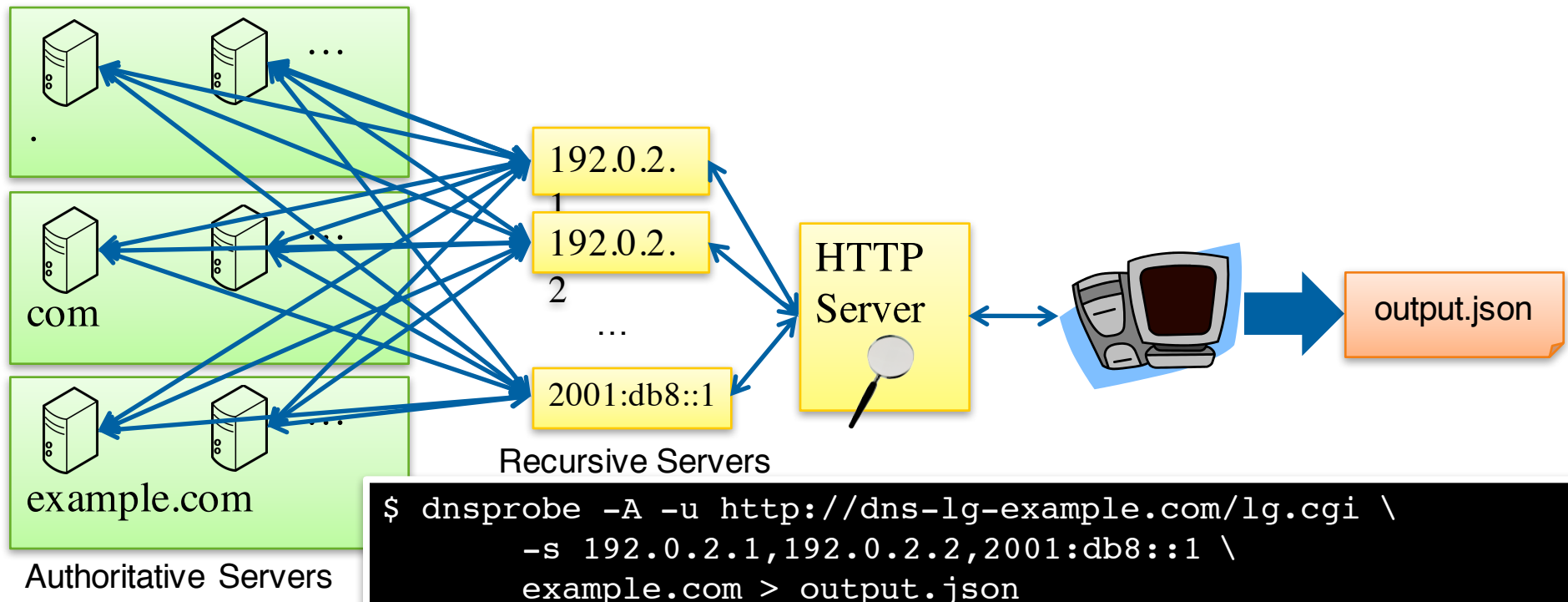
- Queries issued towards authoritative servers (optionally, all the way from root)
- All servers addresses queried
 - IPv4/IPv6
 - UDP/TCP



Recursive DNS Queries Using a Looking Glass:

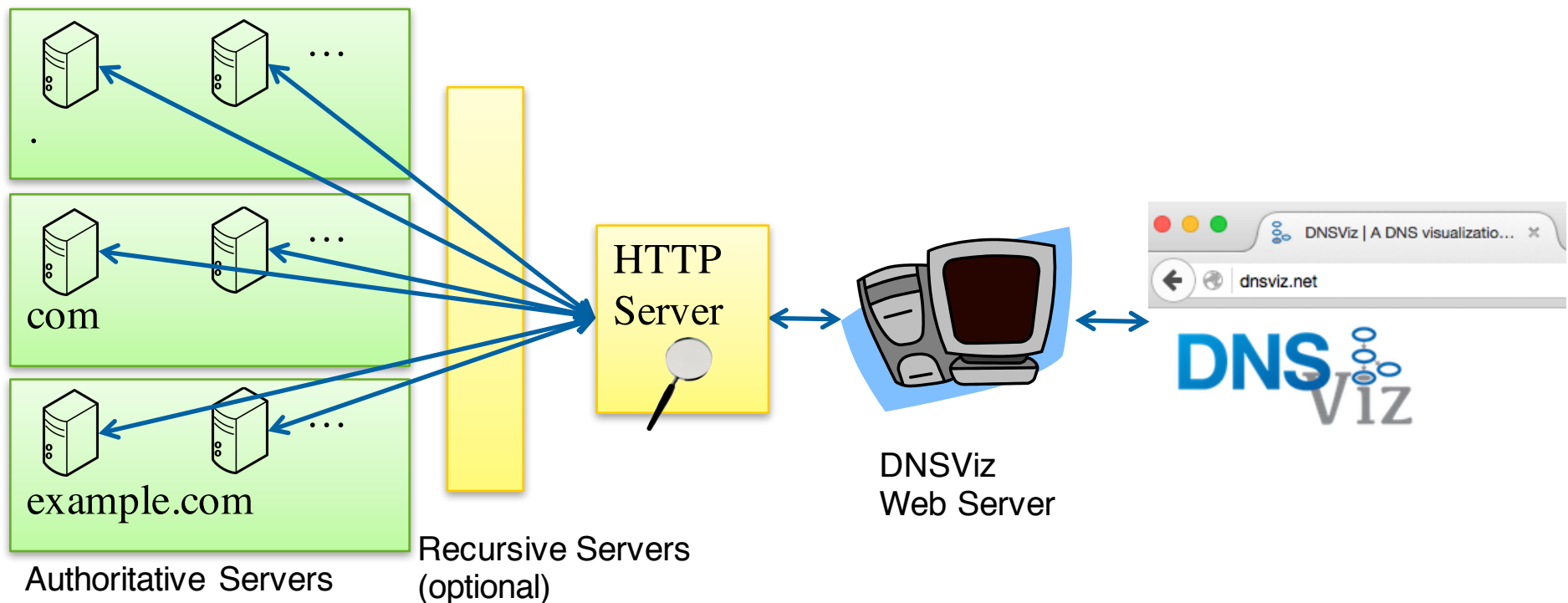
`dnsviz probe -u <URL>`

- Queries issued towards recursive servers (all the way to the root, by default)



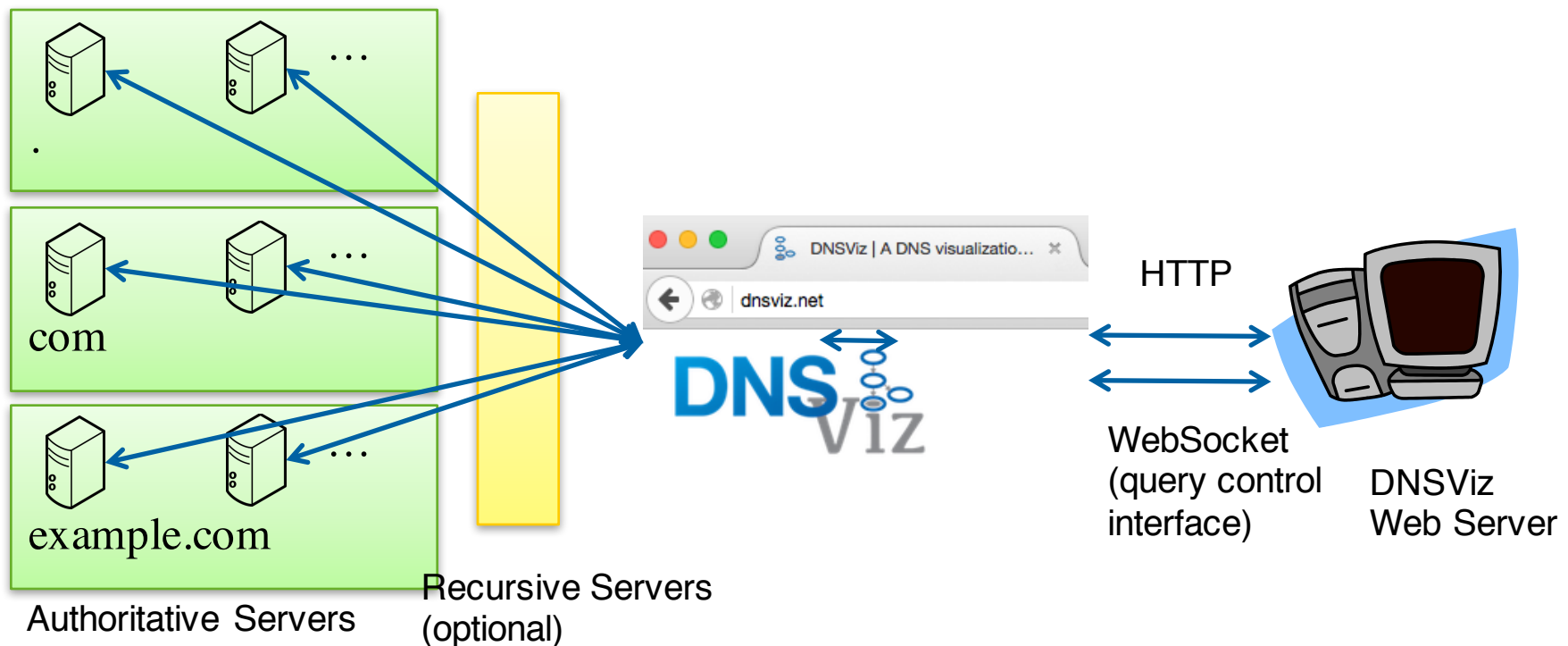
DNSViz Web Interface – Third-party Looking Glass

- Select “third-party” location from analysis form.
- Server uses HTTP-based DNS looking glass.



DNSViz Web Interface – Client-side Looking Glass

- Select “third-party” location from analysis form.
- Java app(let) connects to server using WebSocket.
- Diagnostic DNS queries issued from Java app(let).



Summary

- DNS name resolution paths can be diverse.
- A multi-perspective analysis can help understand general resolver experience.
- DNSViz allows a flexible platform for multi-vantage point DNS diagnostics and measurement:
 - Recursive and authoritative diagnostic analysis
 - Command-line diagnostic tools
 - Web-based diagnostic tools
 - Looking glass software
- Resources:
 - <https://github.com/dnsviz/dnsviz>
 - <http://dnsviz.net/>

powered by



VERISIGN™