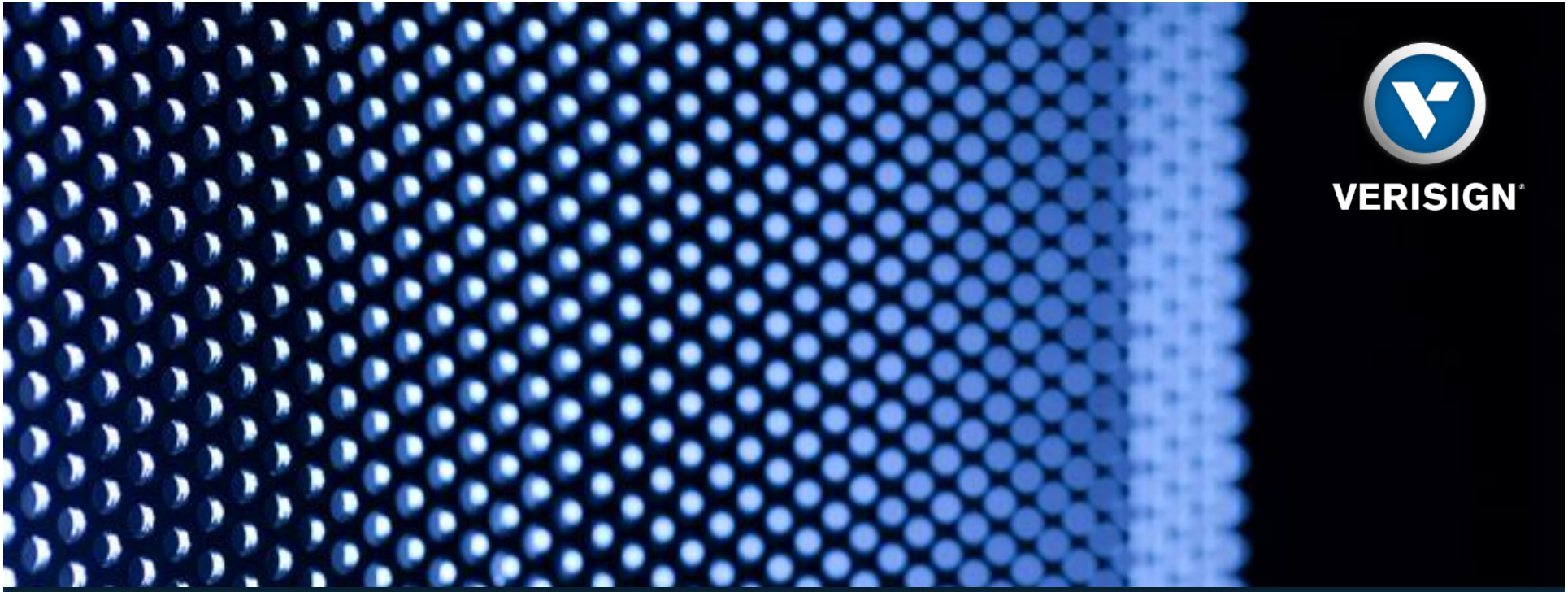


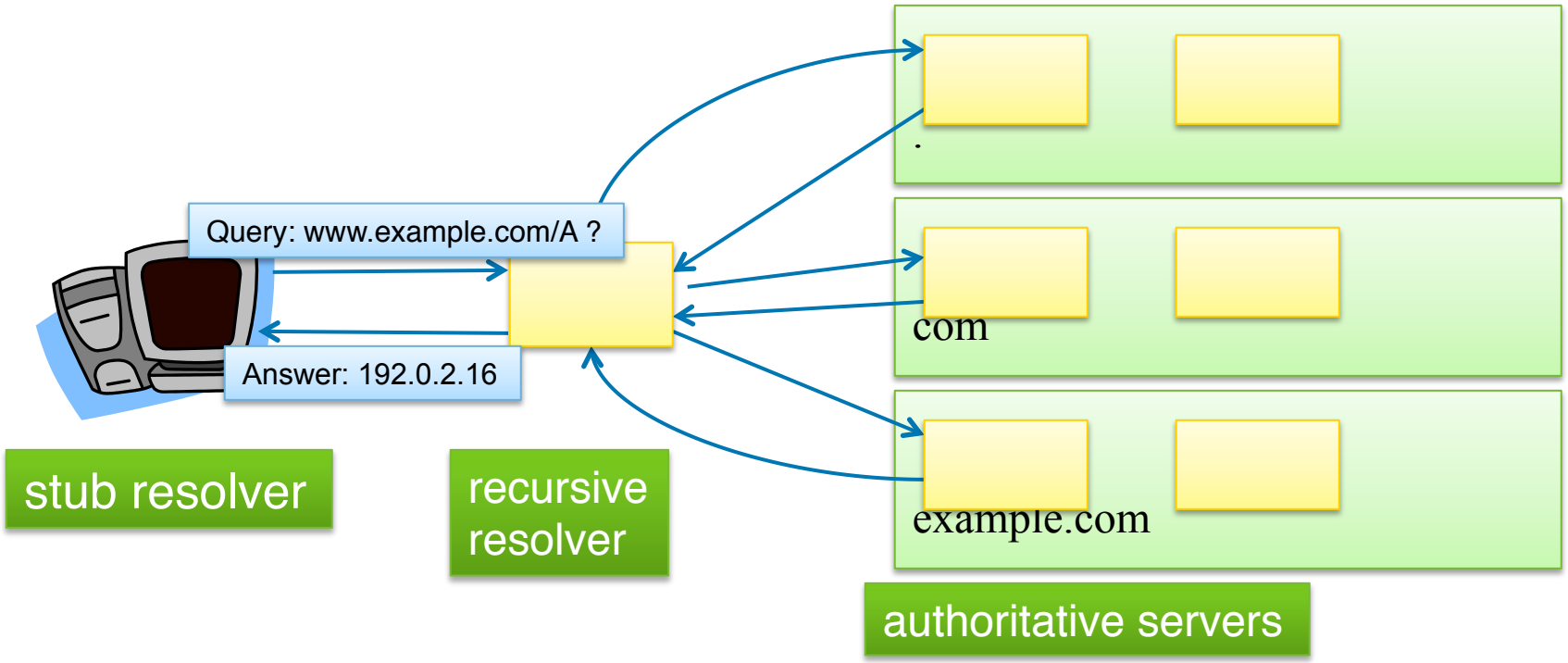
Multi-vantage Point DNS Diagnostics and Measurement

Casey Deccio, Verisign Labs

OARC 24, Buenos Aires

Apr 1, 2016

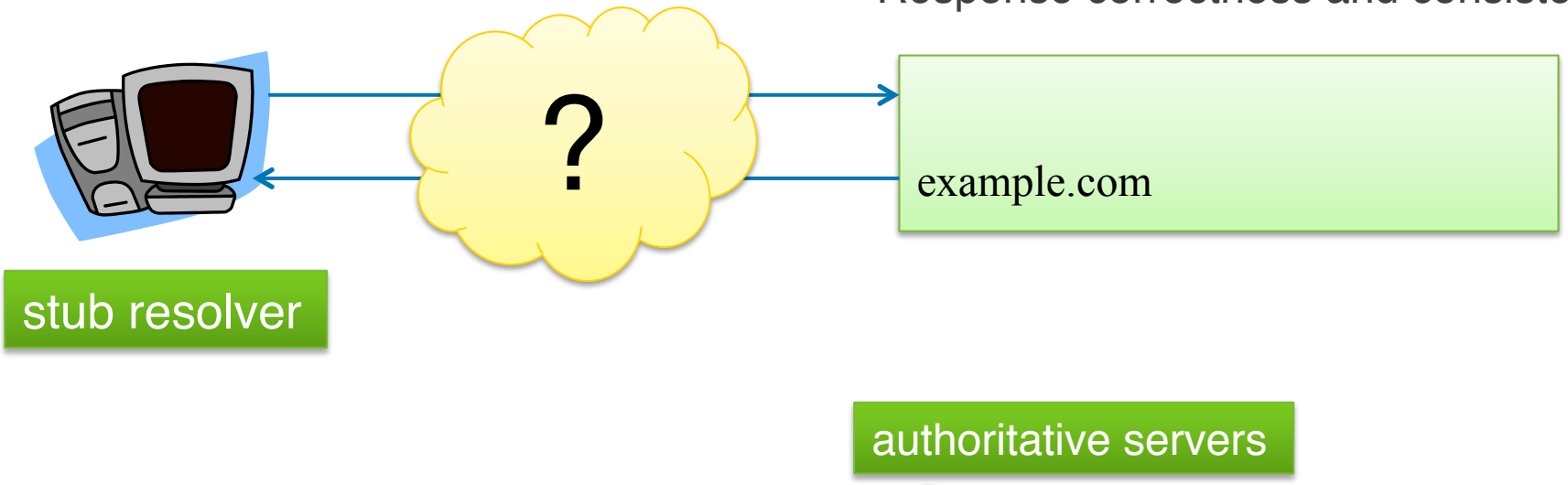
DNS Name Resolution



The Path Between Stub and Authoritative

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

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

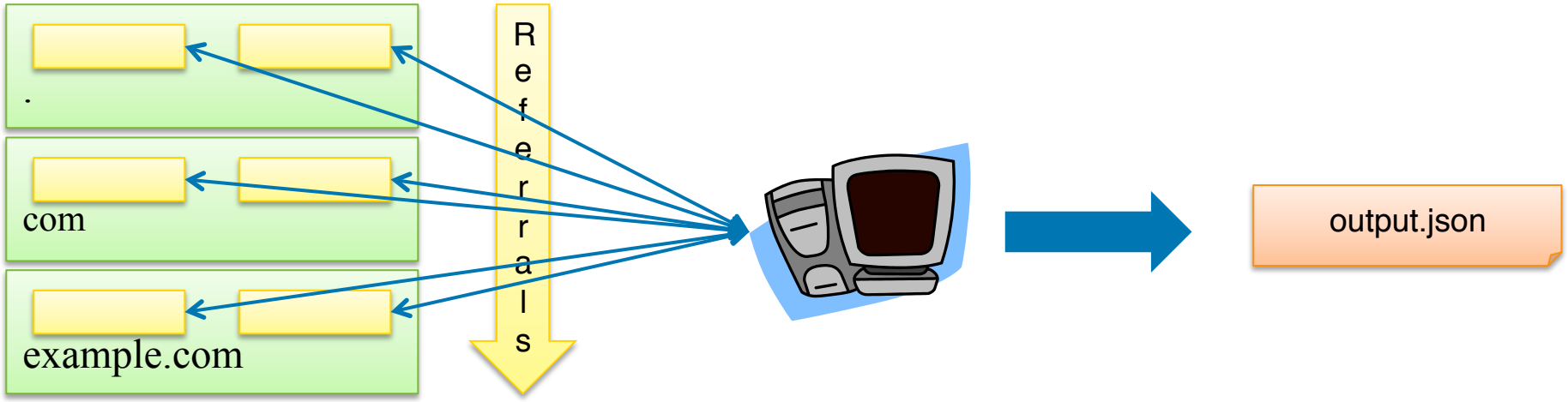


Vantage Point Utility

- Measure and monitor **authoritative** or **recursive** DNS services from different vantage points.
- Understand client perspectives/problems.
- Diagnose problems from specific network locations.
- Diagnose problems at DNS caches.

Authoritative DNS Queries with DNSViz: `dnsviz probe -A`

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

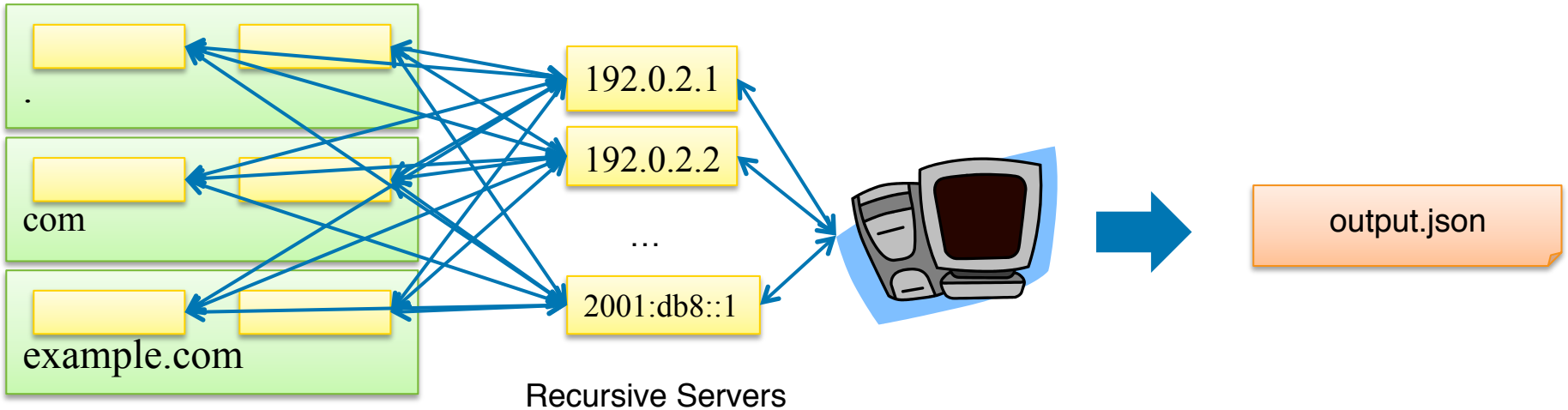


Authoritative Servers

```
$ dnsviz probe -A example.com > output.json
```

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

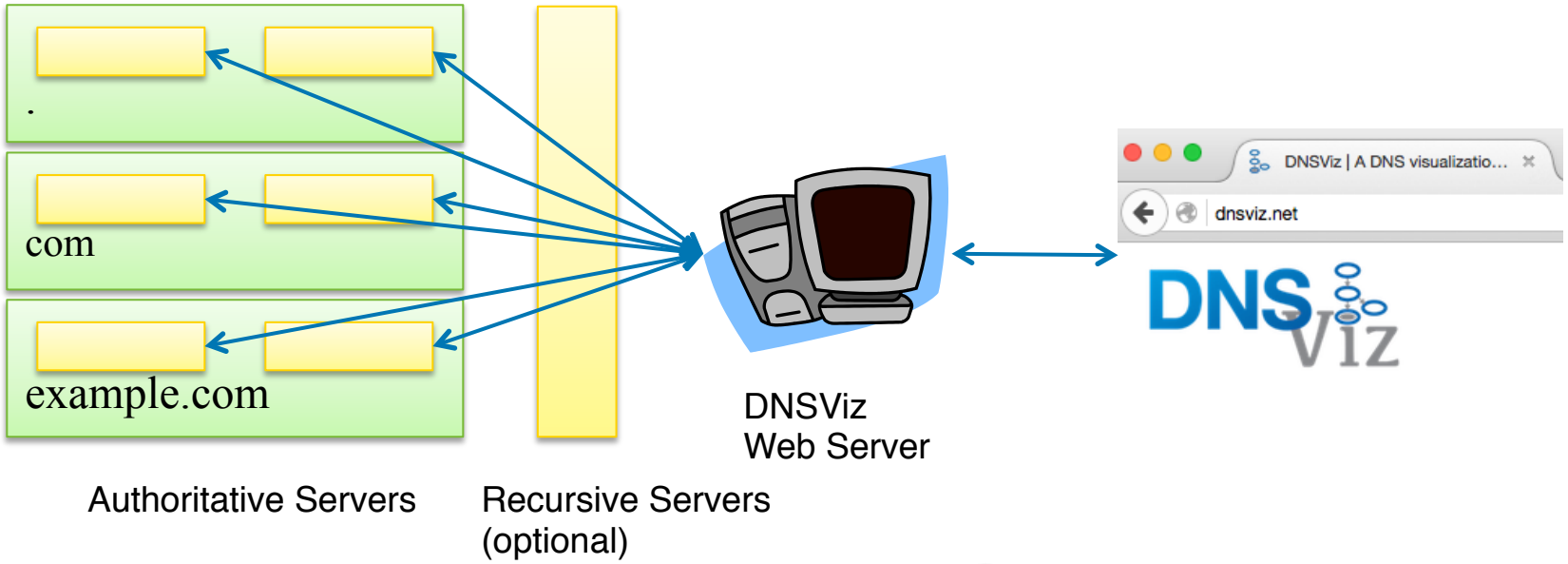
- Queries issued towards recursive servers (all the way to the root, by default)
- Default recursive servers used if none specified.



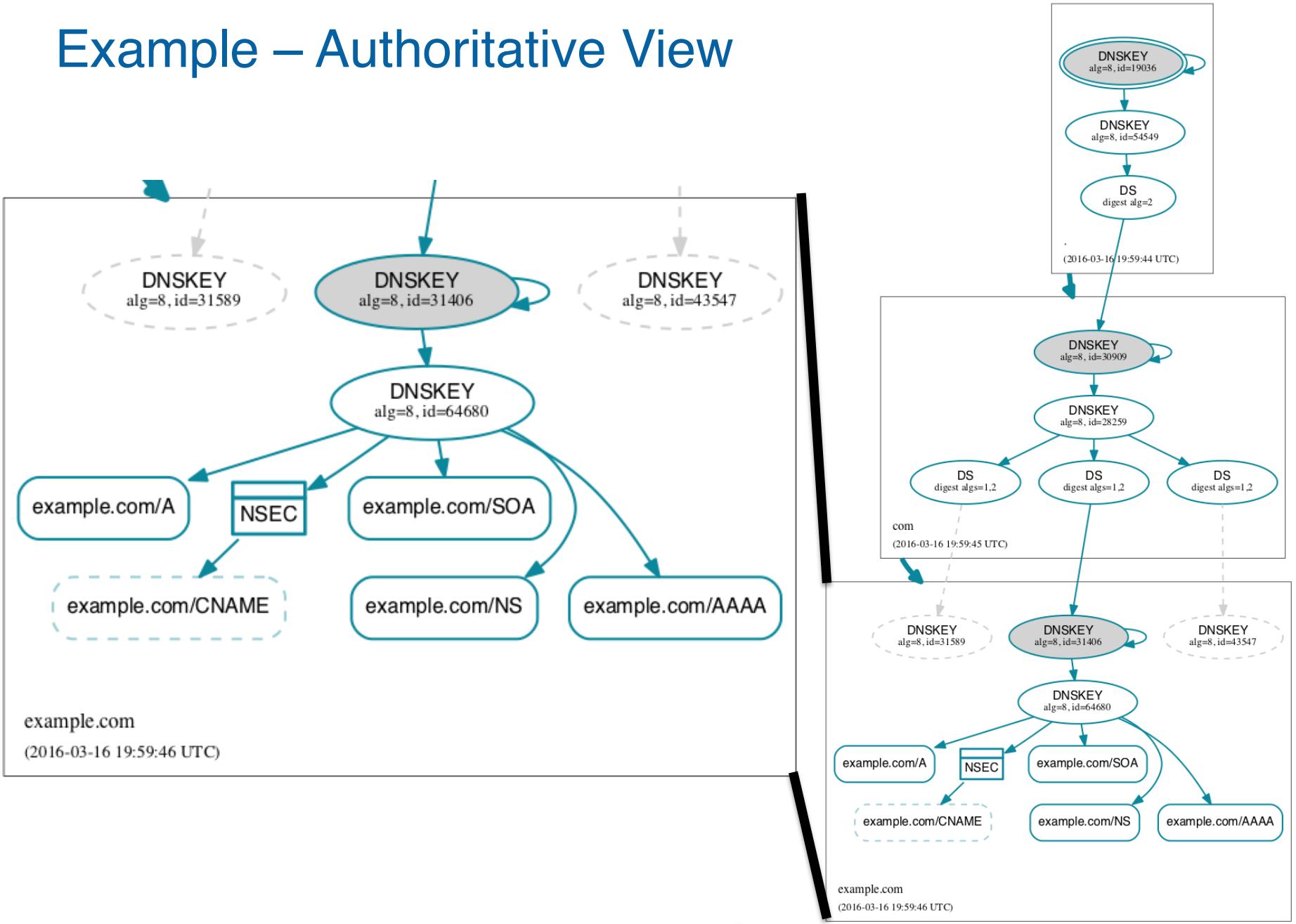

```
$ dnsviz probe -s 192.0.2.1,192.0.2.2,2001:db8::1 \
      example.com > output.json
```

DNSViz Web Interface – Authoritative or Recursive Analysis

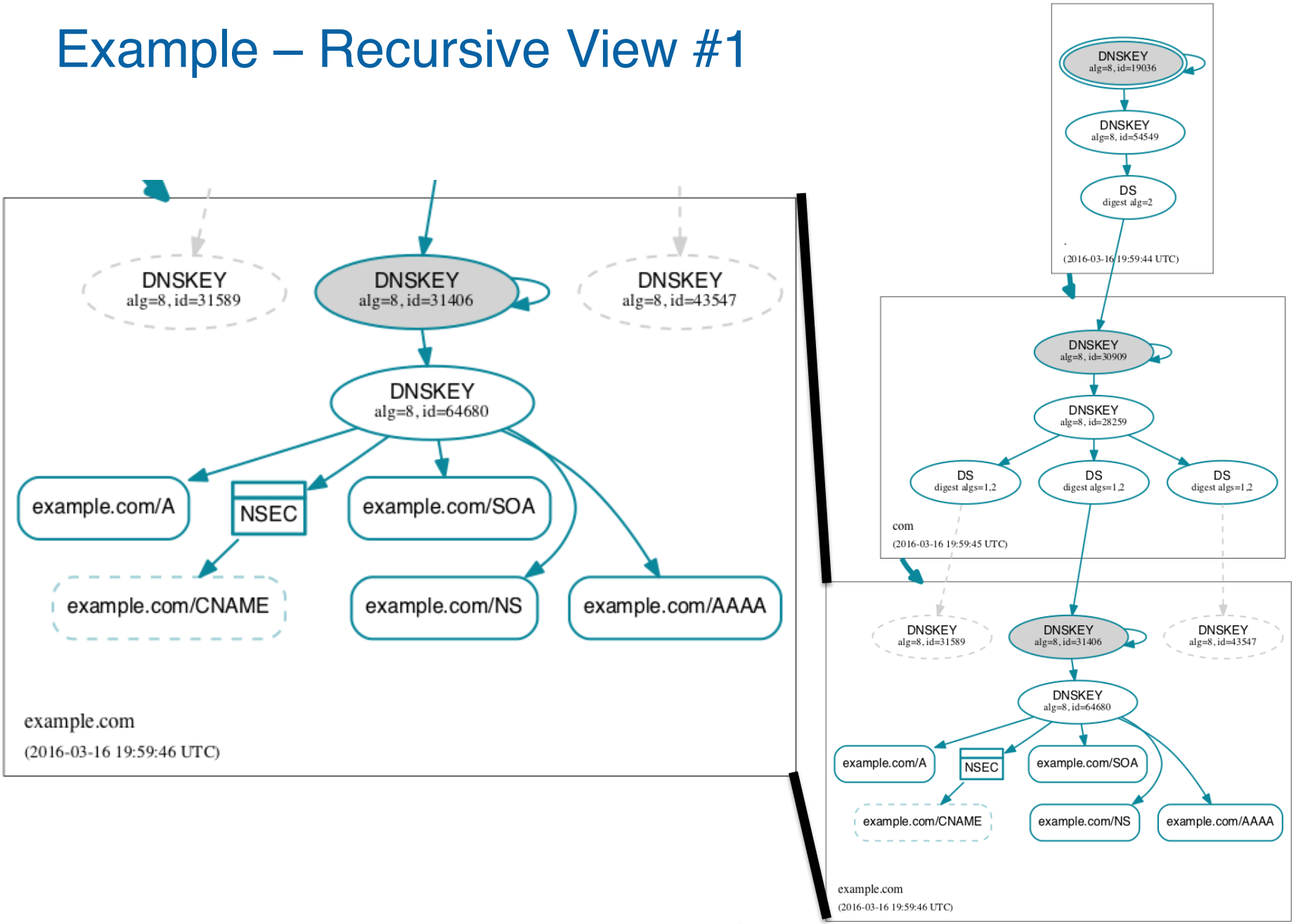
- Select “authoritative” or “recursive” analysis from analysis form.



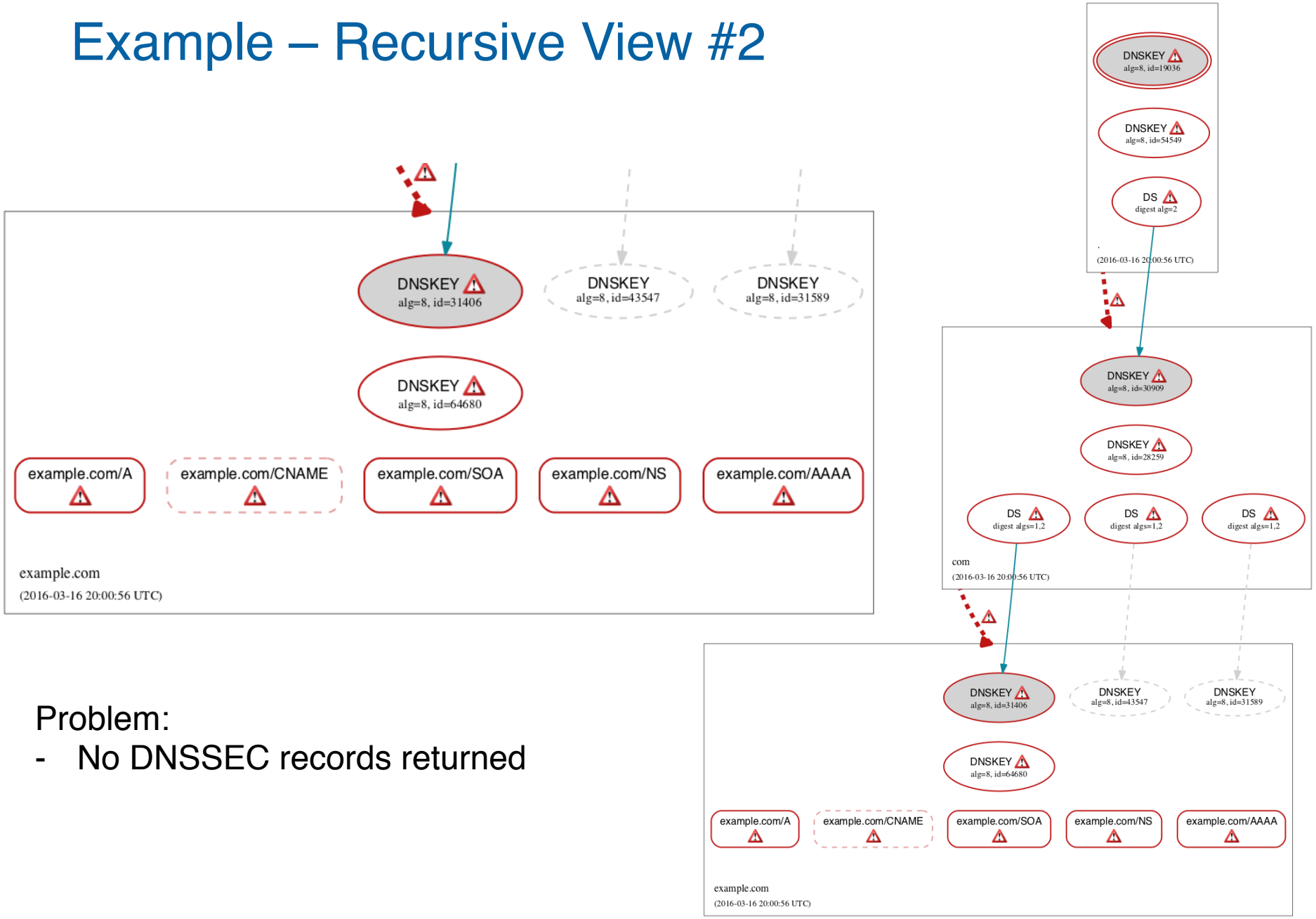
Example – Authoritative View



Example – Recursive View #1



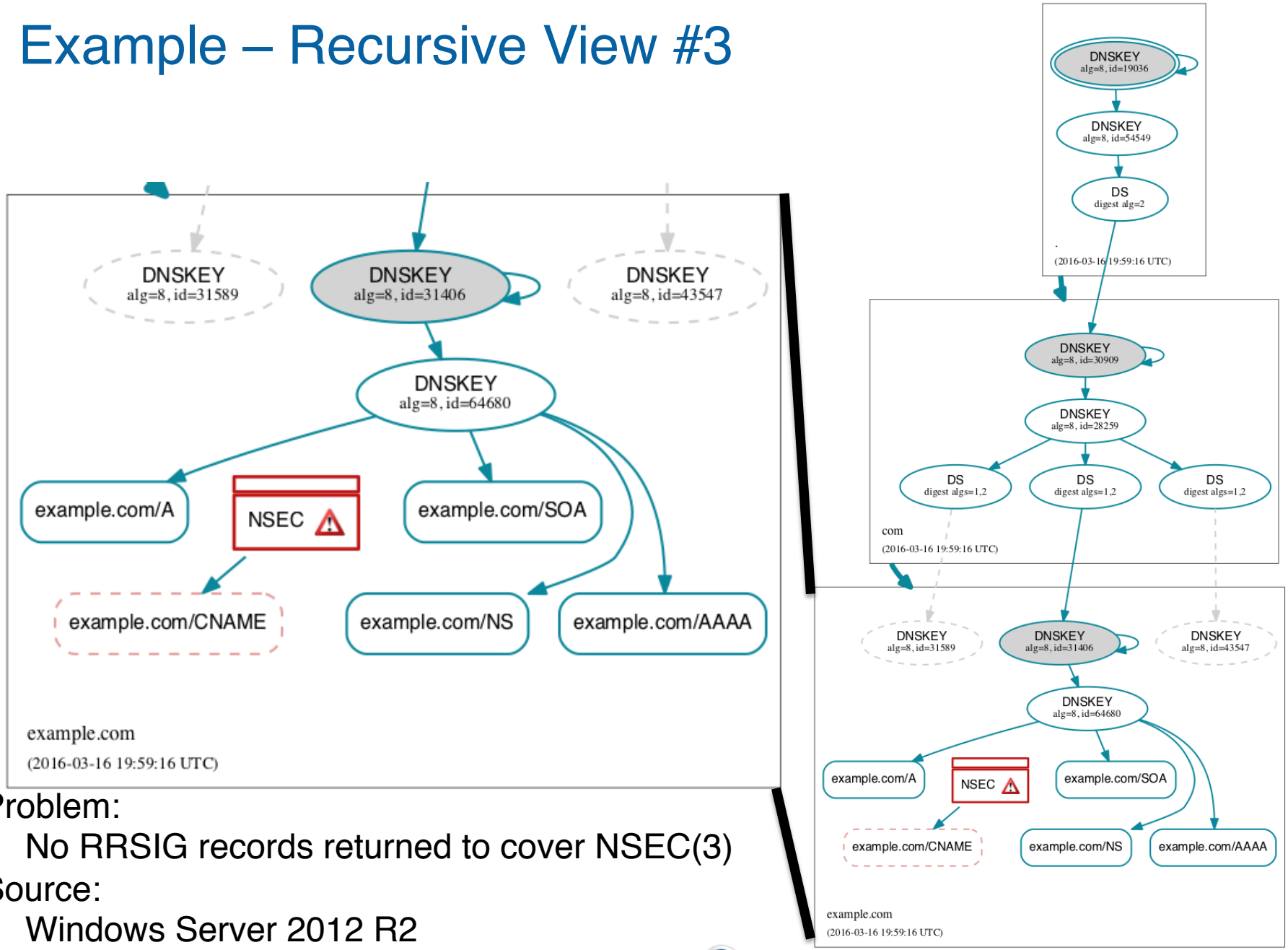
Example – Recursive View #2



Problem:

- No DNSSEC records returned

Example – Recursive View #3



Problem:

- No RRSIG records returned to cover NSEC(3)

Source:

- Windows Server 2012 R2

The Case of Windows Server 2012 R12

- Testing DNSSEC validation on Windows 2012 R12.
- After validation enabled, all unsigned domains became unavailable.
- Cause: authenticated denial-of-existence proofs failed due to lack of RRSIG covering NSEC.
- Problem only occurred when server was configured to forward queries.
- Problem only occurred when upstream forwarder was BIND.

Negative DNS Responses – A Closer Look

- BIND negative response

```
example.com.        3600    IN      SOA     sns.dns.icann.org. …
example.com.        3600    IN      RRSIG   SOA 8 2 3600 …
example.com.        3600    IN      RRSIG   NSEC 8 2 3600 …
example.com.        3600    IN      NSEC    www.example.com. …
```

- unbound negative response

```
example.com.        3600    IN      SOA     sns.dns.icann.org. …
example.com.        3600    IN      RRSIG   SOA 8 2 3600 …
example.com.        3600    IN      NSEC    www.example.com. …
example.com.        3600    IN      RRSIG   NSEC 8 2 3600 …
```

Windows Server 2012 R12 – the Fix

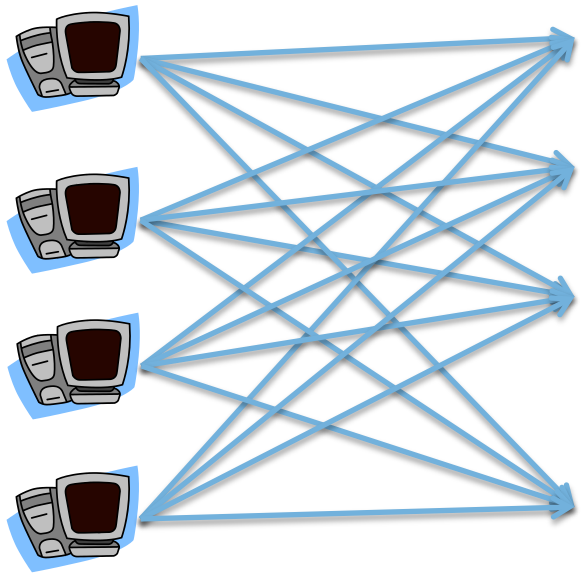
Knowledge base article: 3133717

“Windows Server 2012 R2-based DNS server doesn't return all the Resource record signature (RRSIG) records that should be returned with the Next Secure (NSEC) records if the query passes through a BIND forwarder during resolution. This causes DNSSEC validation to fail for any servers that are using Windows Server 2012 R2-based server as a forwarder.”

https://support.microsoft.com/en-us/kb/3133717

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 – Desired Capabilities

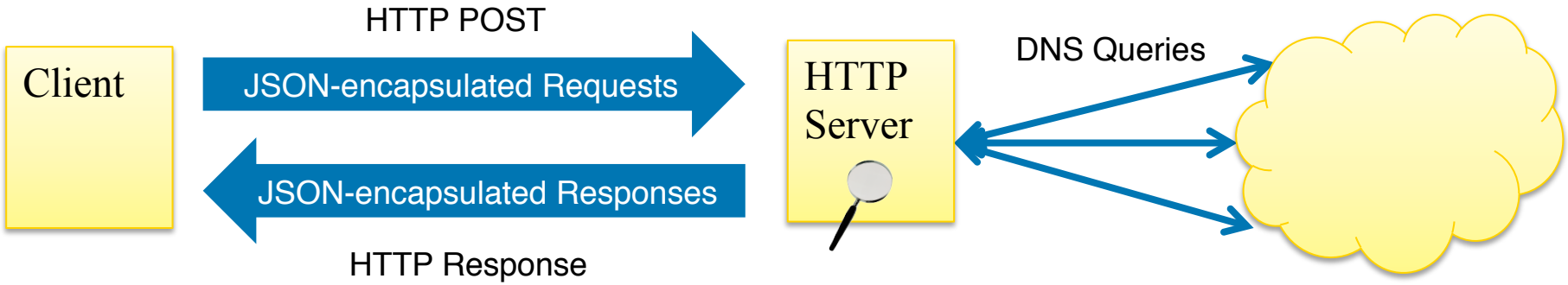
- Request components
  - Message (or optionally, parameters)
  - Destination IP
  - Destination port
  - Source IP (optional)
  - Source port (optional)
  - Transport protocol (TCP/UDP)
  - Timeout value
- Response components
  - Message (if no error)
  - Error (timeout or network error)
  - Error description (e.g., errno)
  - Source IP
  - Source port
  - Time elapsed
  - Traceroute (optional)

DNS Looking Glass – Desired Capabilities (2)

- Security
  - Restriction of local and loopback queries
  - Resource usage limits
  - Simultaneous queries
  - Authentication
  - Privileges/access control
  - Privacy/encryption
- Other
  - Ease of deployment
  - Accessibility (IPs, ports, protocol)
  - Synchronous execution, for diagnostics
  - Support for multiple queries per request
  - Parallel execution

DNS Looking Glass – Over HTTP

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

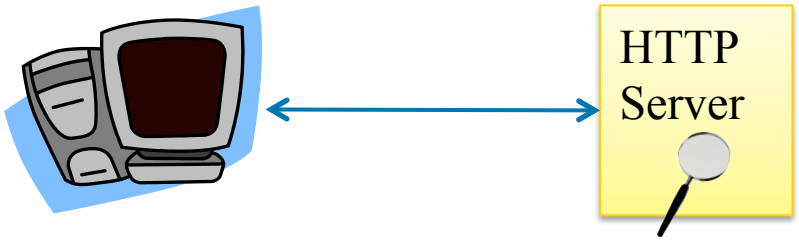


DNSViz Proof-of-concept Looking Glass

- Client/server components included with DNSViz source:
  - https://github.com/dnsviz/dnsviz
- Server:
  - `contrib/dnsviz-lg.cgi`

  (requires DNSViz installation)
- Client:
  - `contrib/digviz`

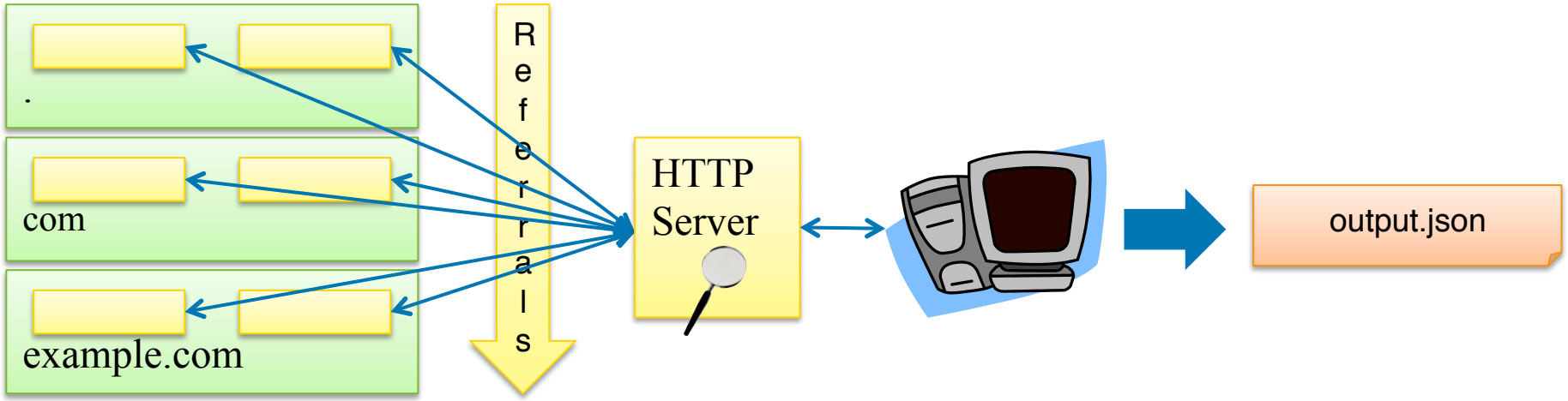
  (behaves similar to ISC `dig`)




```
$ 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>`

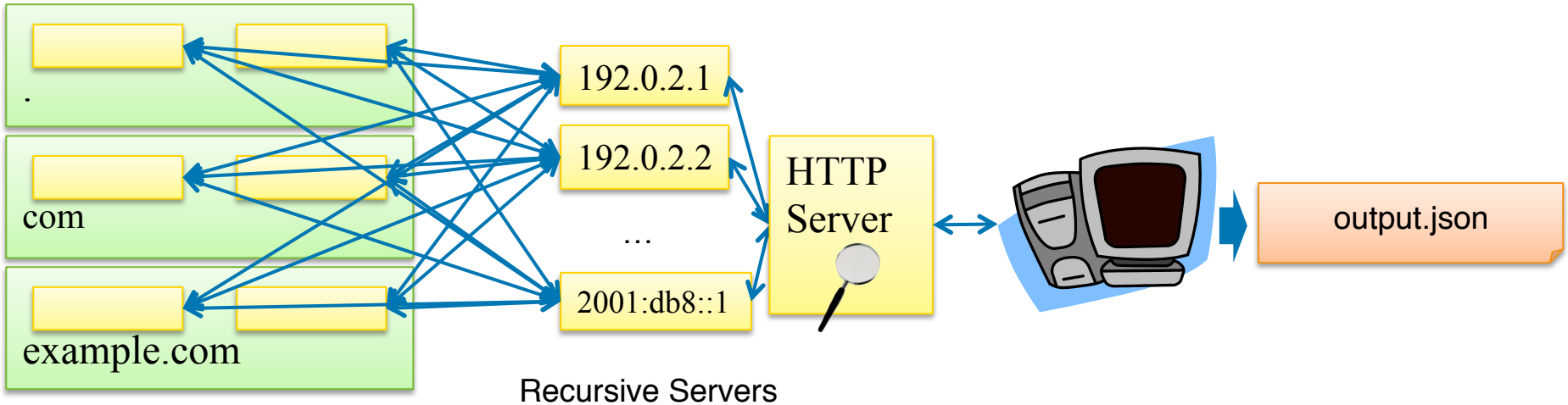
- Queries issued towards authoritative servers (optionally, all the way from root)
- All servers addresses queried
  - IPv4/IPv6
  - UDP/TCP




```
$ dnsprobe -A -u http://dns-lg-example.com/ \
        example.com > output.json
```

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

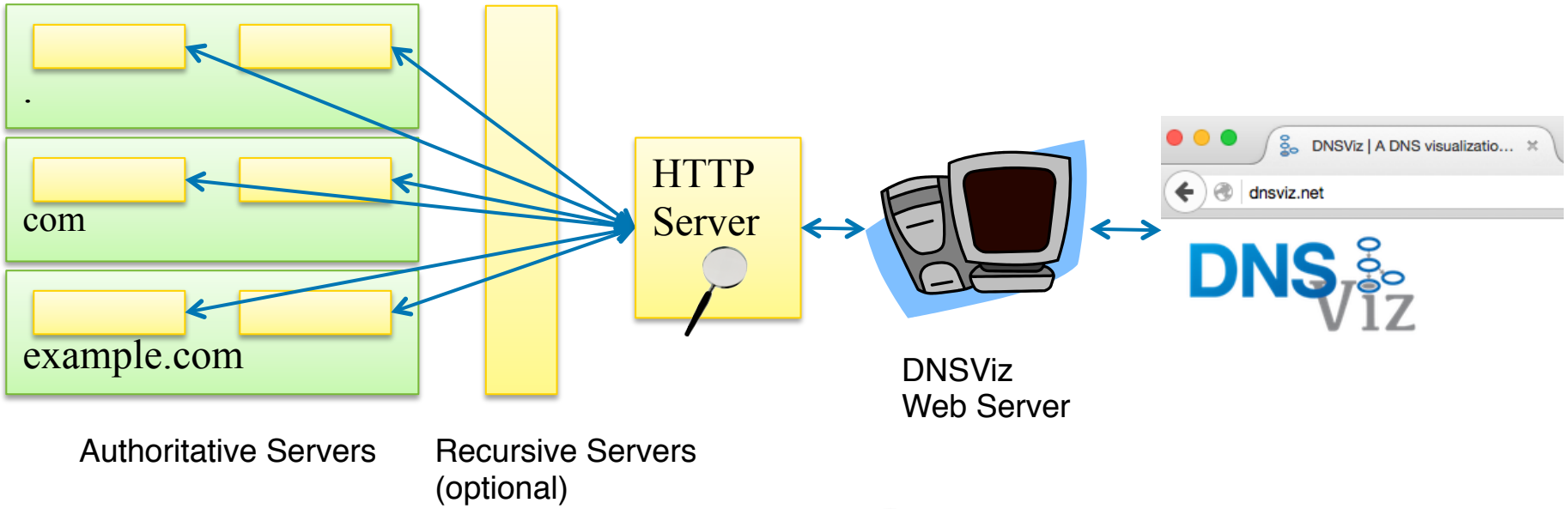
- Queries issued towards recursive servers (all the way to the root, by default)




```
$ dnsprobe -A -u http://dns-lg-example.com/lg.cgi \
      -s 192.0.2.1,192.0.2.2,2001:db8::1 \
      example.com > output.json
```

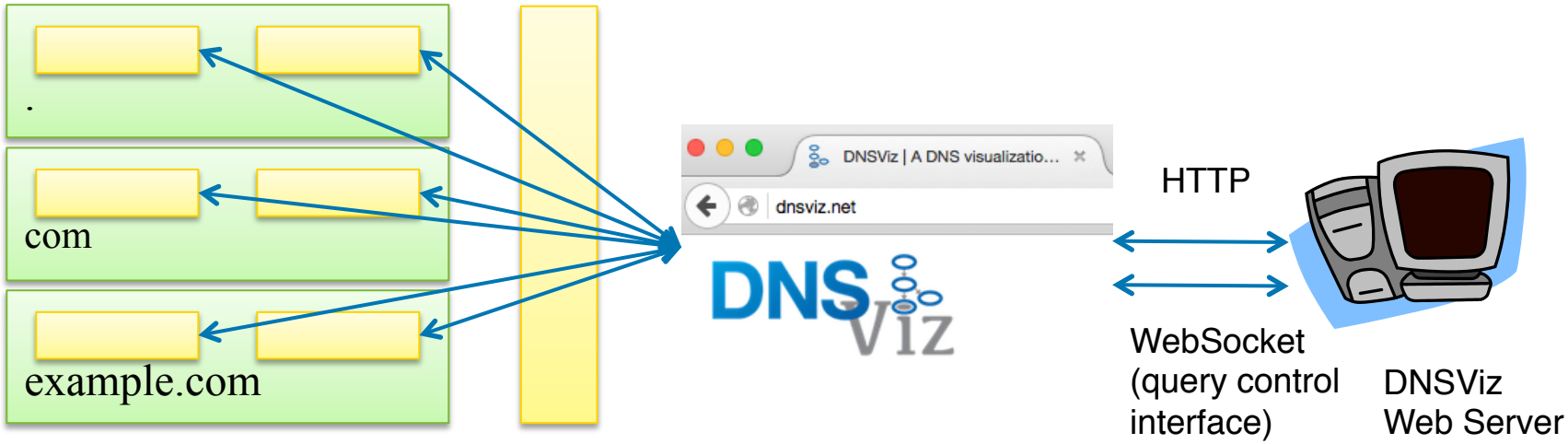
DNSViz Web Interface – Third-party Looking Glass

- 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™