Pre-Deployment DNS Testing: Or How to Avoid a Train Wreck

Casey Deccio, Verisign Labs

DNS-OARC 25

Oct. 15, 2016, Dallas, TX

DNS Diagnostics and Measurement

powered by **VERISIGN**

DNS Measurement: Quantitative and Qualitative

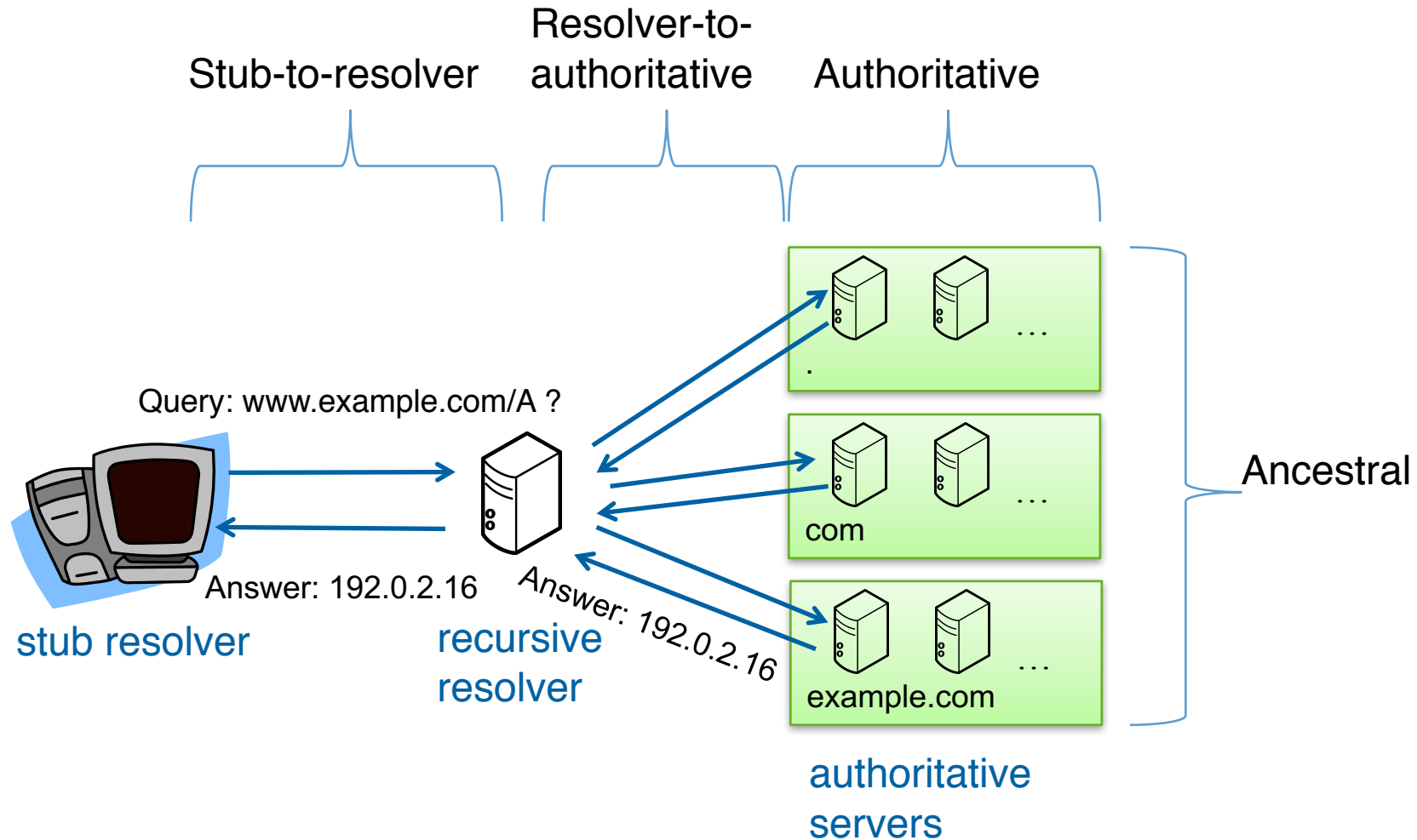- **Quant**itative
  - Availability
    - TCP/UDP
    - IPv4/IPv6
  - Responsiveness (function of loss rate)
  - Response time
  - Response size

- **Qual**itative
  - DNS server/path capabilities
    - EDNS capable
    - DNSSEC aware/validating
  - Response consistency
  - Delegation consistency and correctness
    - NS
    - DS/DNSKEY
  - DNSKEY/RRSIG/NSEC consistency and correctness

2

powered by **VERISIGN**

Measurement Areas Across a DNS Deployment

Stub-to-resolver

Resolver-to-authoritative

Authoritative

Query: www.example.com/A ?

Answer: 192.0.2.16

Answer: 192.0.2.16

stub resolver

recursive resolver

.

com

example.com

Ancestral

authoritative servers

Temporal DNS Measurement

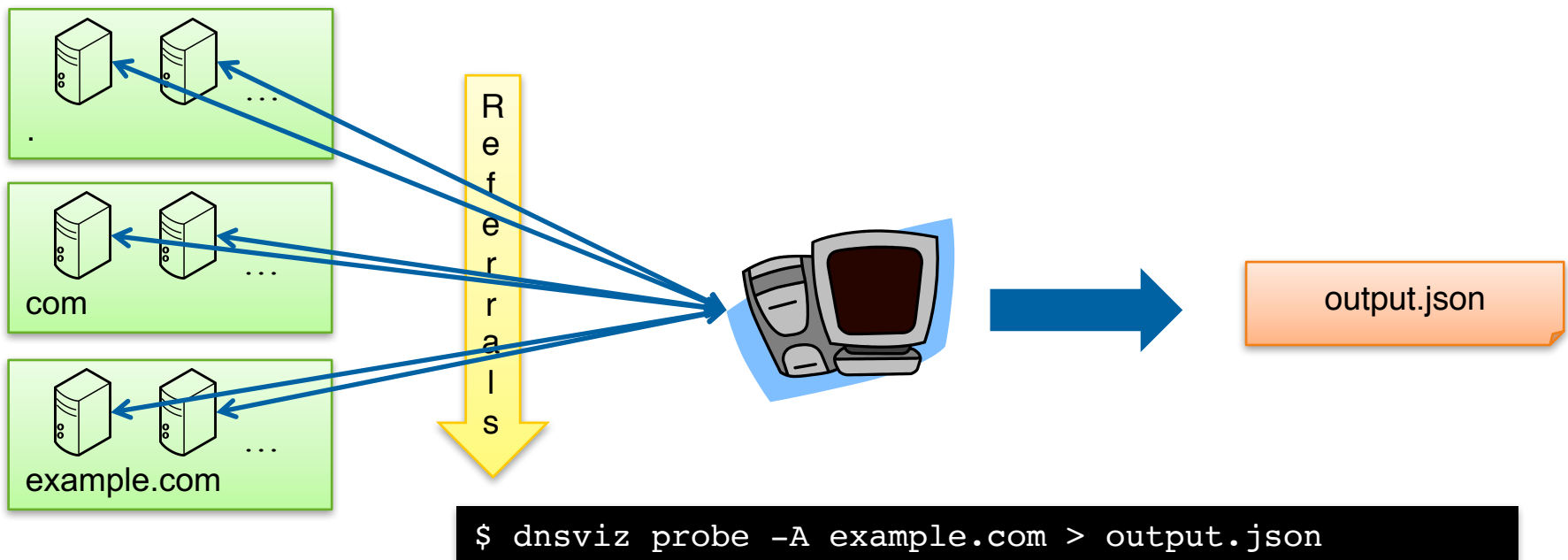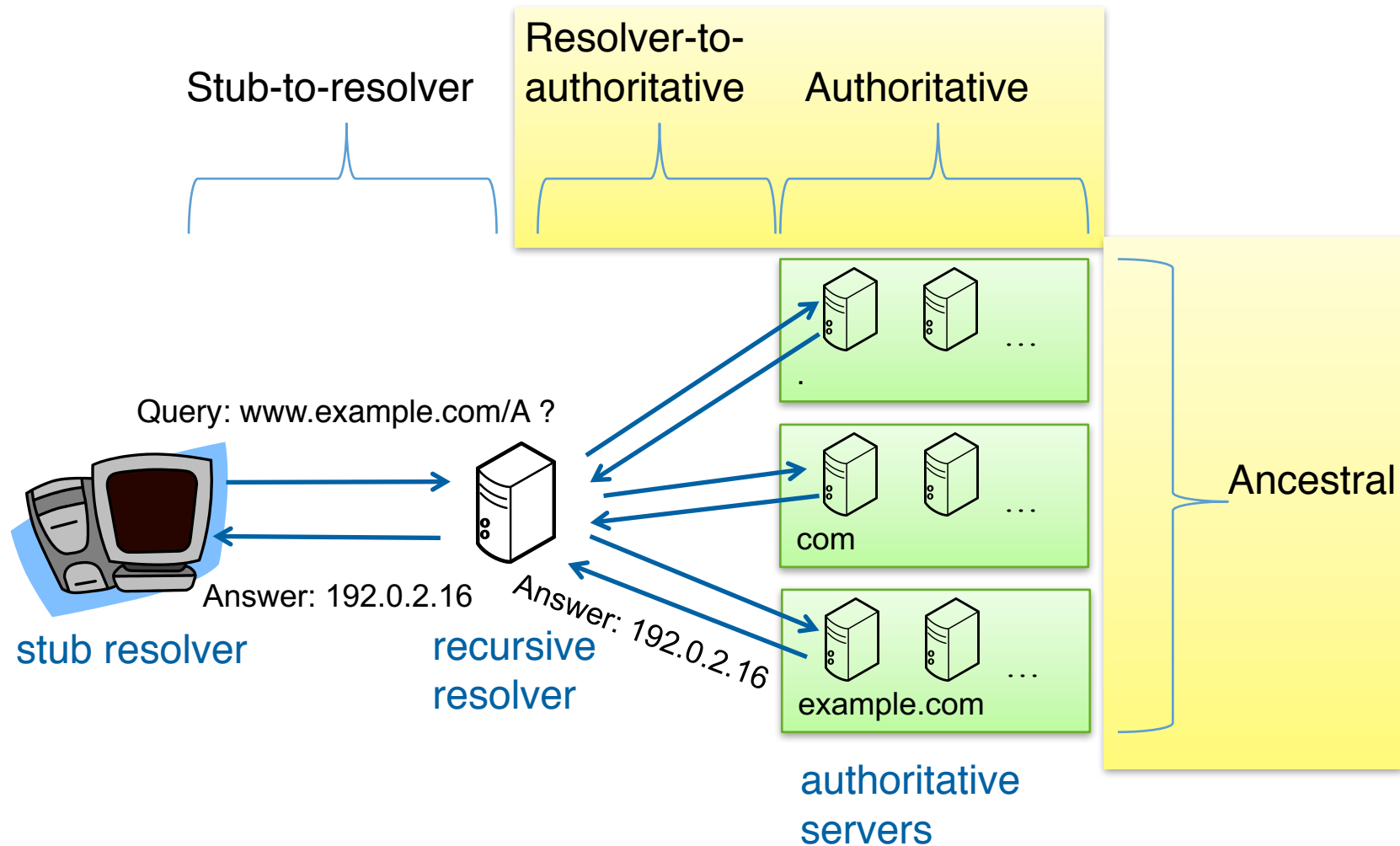| Pre-deployment	Post-deployment
Stealth authoritative servers	No cache presence
Pre-delegation	Some cache presence
Delegation change – NS/DS/glue	
Authoritative change – NS/DNSKEY/A/AAAA	

Post-Delegation DNS Diagnostics and Measurement

DNS Authoritative Diagnostics with DNSViz

- Diagnostic queries issued towards authoritative servers and ancestor authoritative servers.

- All IPv4/IPv6 server addresses queried over UDP and TCP.

- Diagnostic response information is encoded in JSON format to a file.


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

Measurement Areas Across a DNS Deployment

Stub-to-resolver

Resolver-to-authoritative

Authoritative

Query: www.example.com/A ?

Answer: 192.0.2.16

stub resolver

Answer: 192.0.2.16

recursive resolver

.

com

example.com

Ancestral

authoritative servers

Temporal DNS Measurement

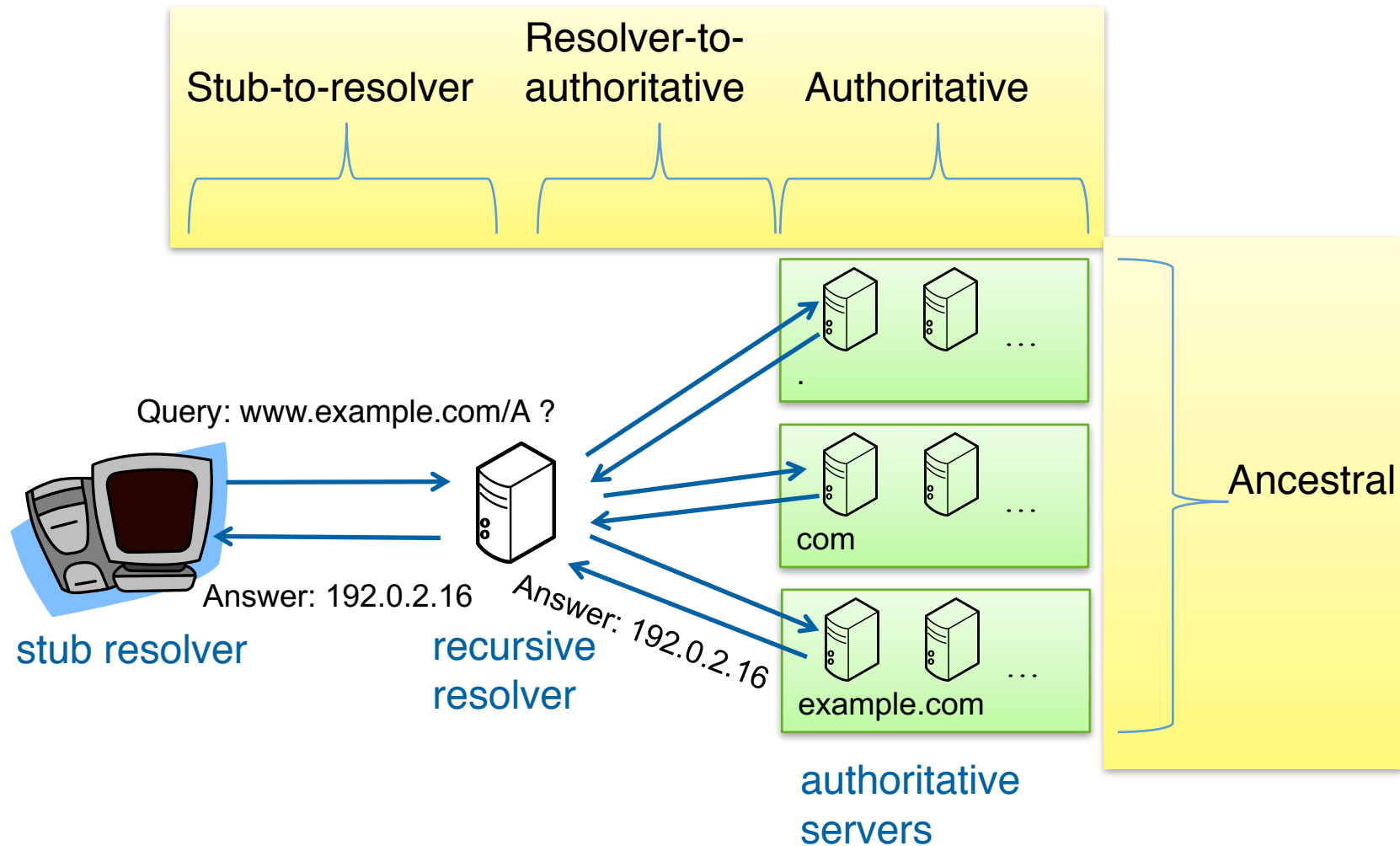|	
Pre-deployment	**Post-deployment**
Stealth authoritative servers	No cache presence
Pre-delegation	Some cache presence
Authoritative change – NS/DNSKEY/A/AAAA	
Delegation change – NS/DS/glue	

DNS Recursive Diagnostics with DNSViz

- Queries issued towards recursive servers.

- Default recursive servers used if none specified.

- Diagnostic response information is encoded in JSON format to a file.

- Looking glass can also be used.

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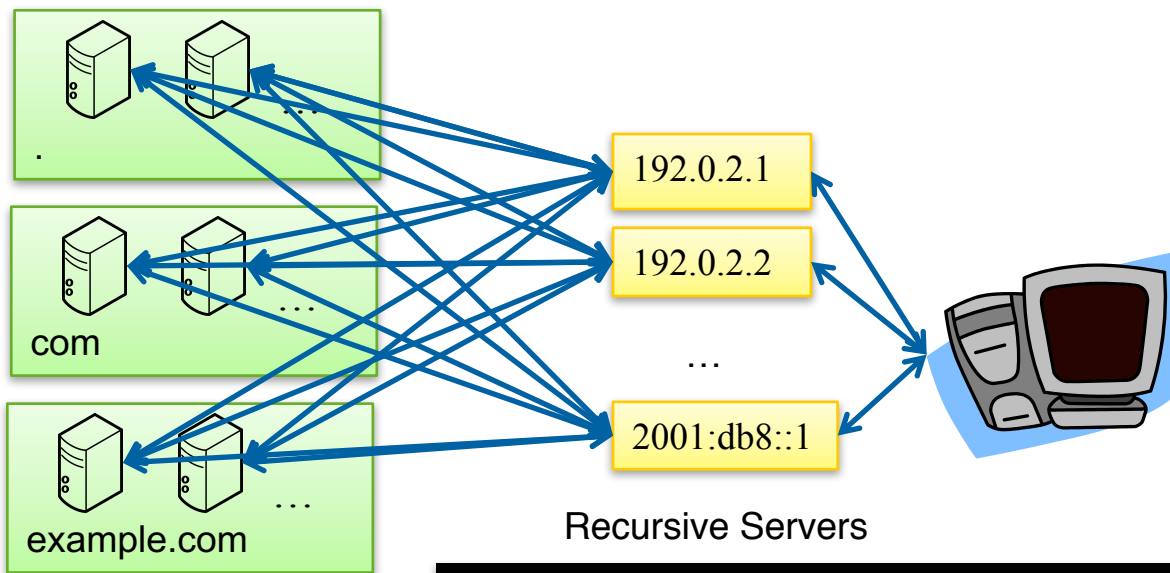
```
$ dnsviz probe -s 192.0.2.1,192.0.2.2,2001:db8::1 \
        example.com > output.json
```

Measurement Areas Across a DNS Deployment

powered by **VERISIGN**

Temporal DNS Measurement

Pre-deployment	**Post-deployment**

Pre-deployment

Stealth authoritative servers

Pre-delegation

Authoritative change –
NS/DNSKEY/A/AAAA

Delegation change –
NS/DS/glue

Post-deployment
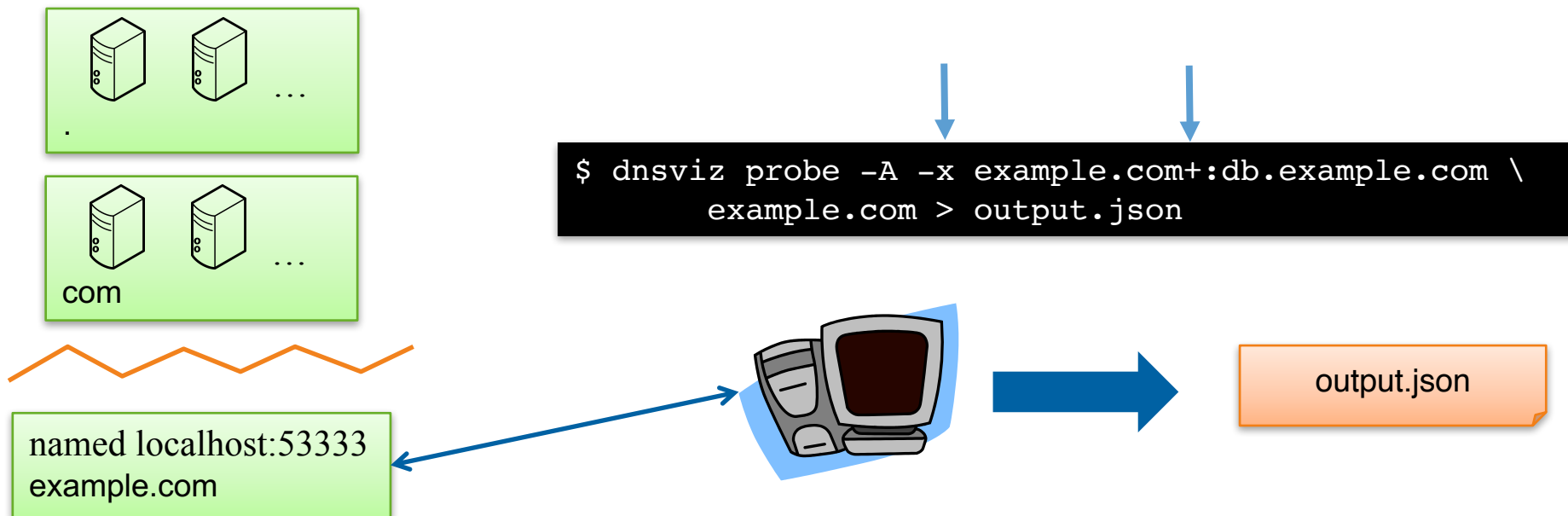
No cache presence

Some cache presence

Pre-Delegation DNS Checking
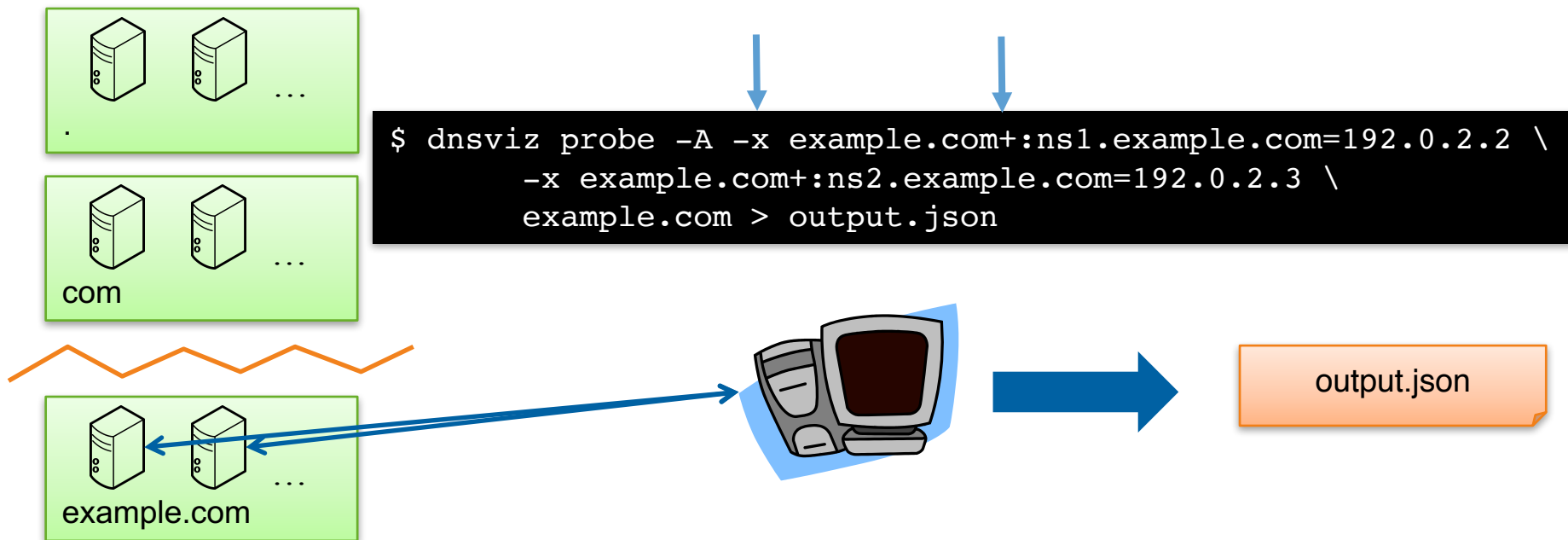
powered by **VERISIGN**

Pre-Delegation DNS Testing with DNSViz

- Issue diagnostic queries against a zone file using "-x" and "+".

- Specify name of zone file as argument.

- Ancestors **not** queried; delegation NS/DS records **not** evaluated.


```
$ dnsviz probe -A -x example.com+:db.example.com \
        example.com > output.json
```

.

com

…

…

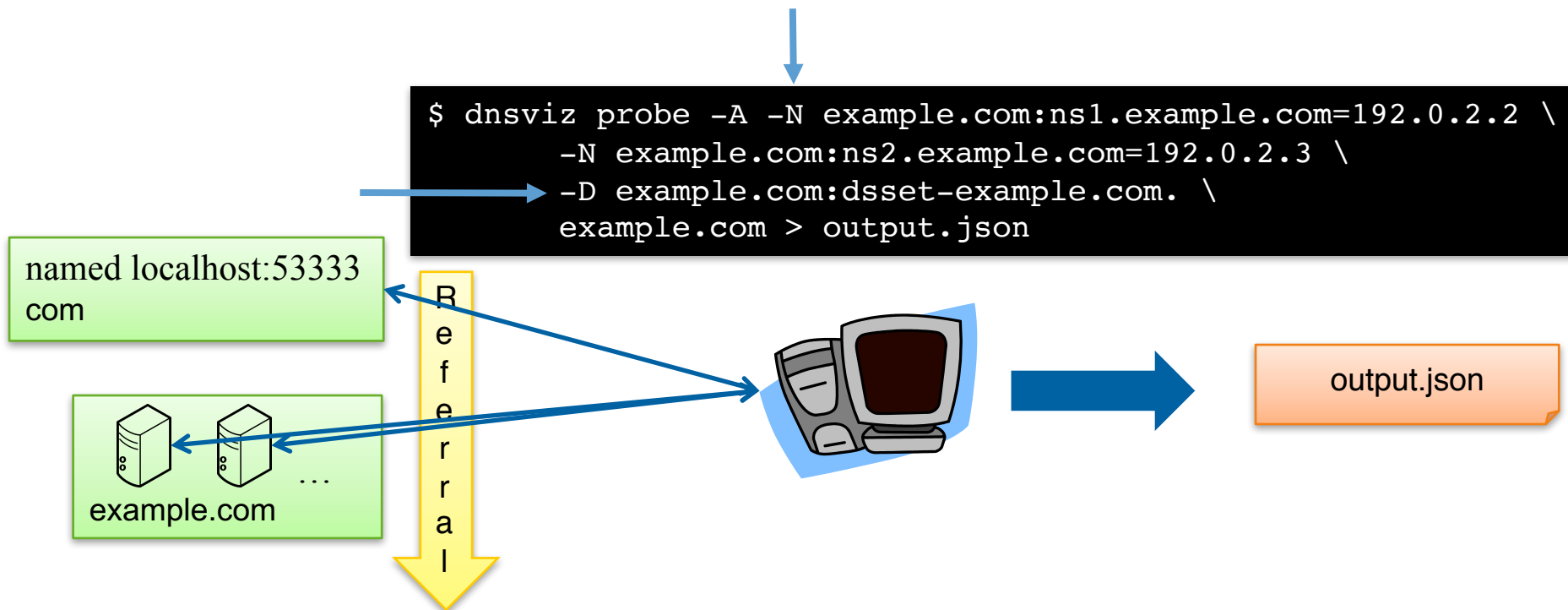named localhost:53333
example.com

output.json

Pre-Delegation DNS Testing with DNSViz

- Issue diagnostic queries against a stealth authoritative using "-x" and "+".

- Specify servers by names, addresses, or both – might or might not correspond to names in NS RRset.

- Ancestors **not** queried; delegation NS/DS records **not** evaluated.


```
$ dnsviz probe –A –x example.com+:ns1.example.com=192.0.2.2 \
        –x example.com+:ns2.example.com=192.0.2.3 \
        example.com > output.json
```

output.json

Pre-Delegation DNS Testing with DNSViz

- Set up an artificial parent zone to test delegation using "-N" and "-D".

- Specify delegation NS names and glue as arguments to "-N".

- Specify DS records or dsset file as arguments to "-D".

- Parent zone queried; delegation NS/DS records **are** evaluated.

```
$ dnsviz probe –A –N example.com:ns1.example.com=192.0.2.2 \
      –N example.com:ns2.example.com=192.0.2.3 \
      –D example.com:dsset–example.com. \
      example.com > output.json
```

named localhost:53333
com

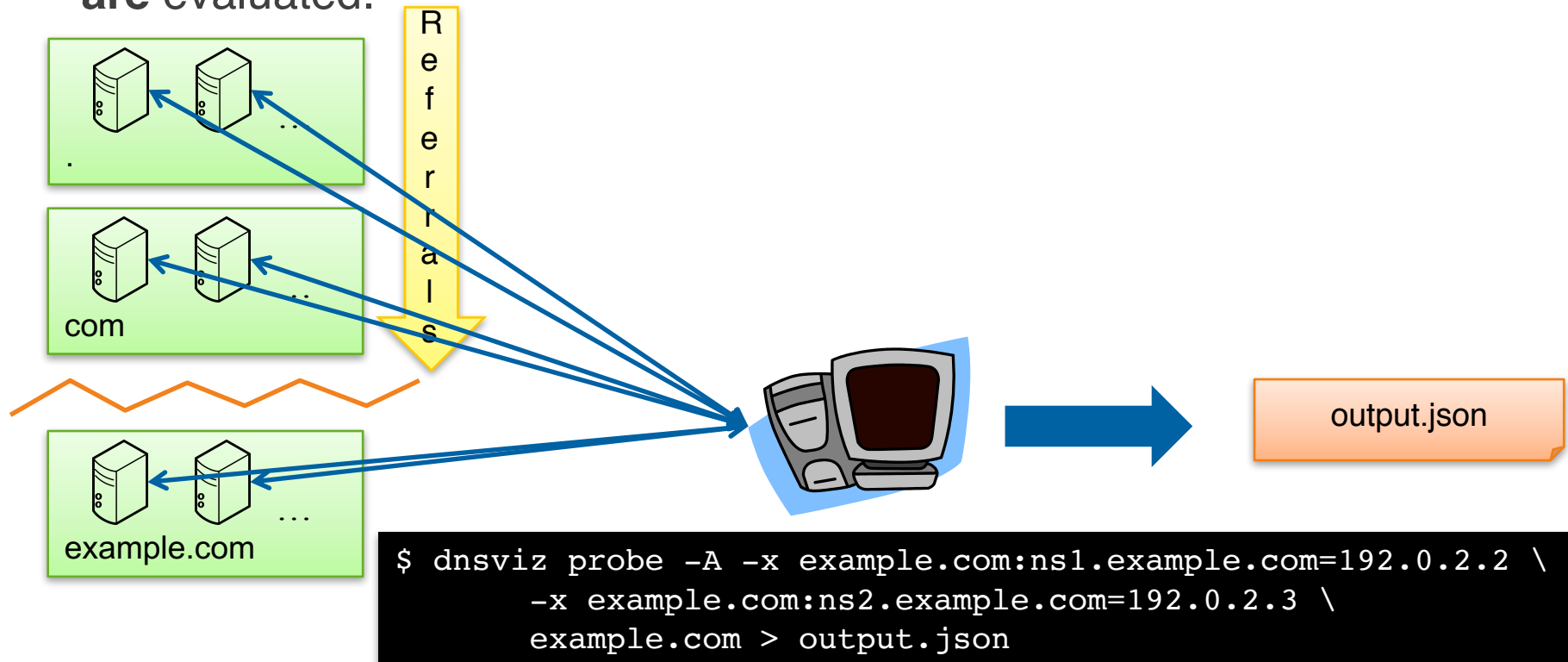Referral

example.com

…

output.json

Pre-Authoritative Change DNS Testing with DNSViz

- Issue diagnostic queries against a zone file using "-x".

- Specify name of zone file as argument.

- Ancestors **are** queried; delegation NS records **not** evaluated; DS records **are** evaluated.
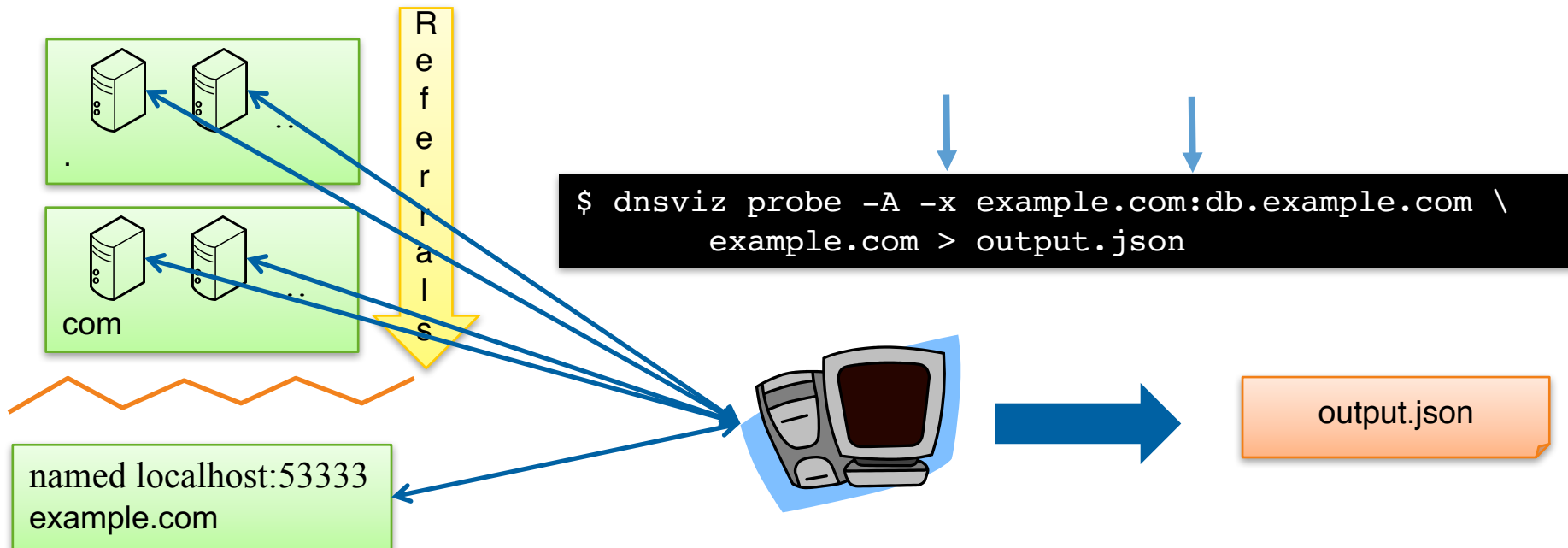

```
$ dnsviz probe –A –x example.com:db.example.com \
        example.com > output.json
```
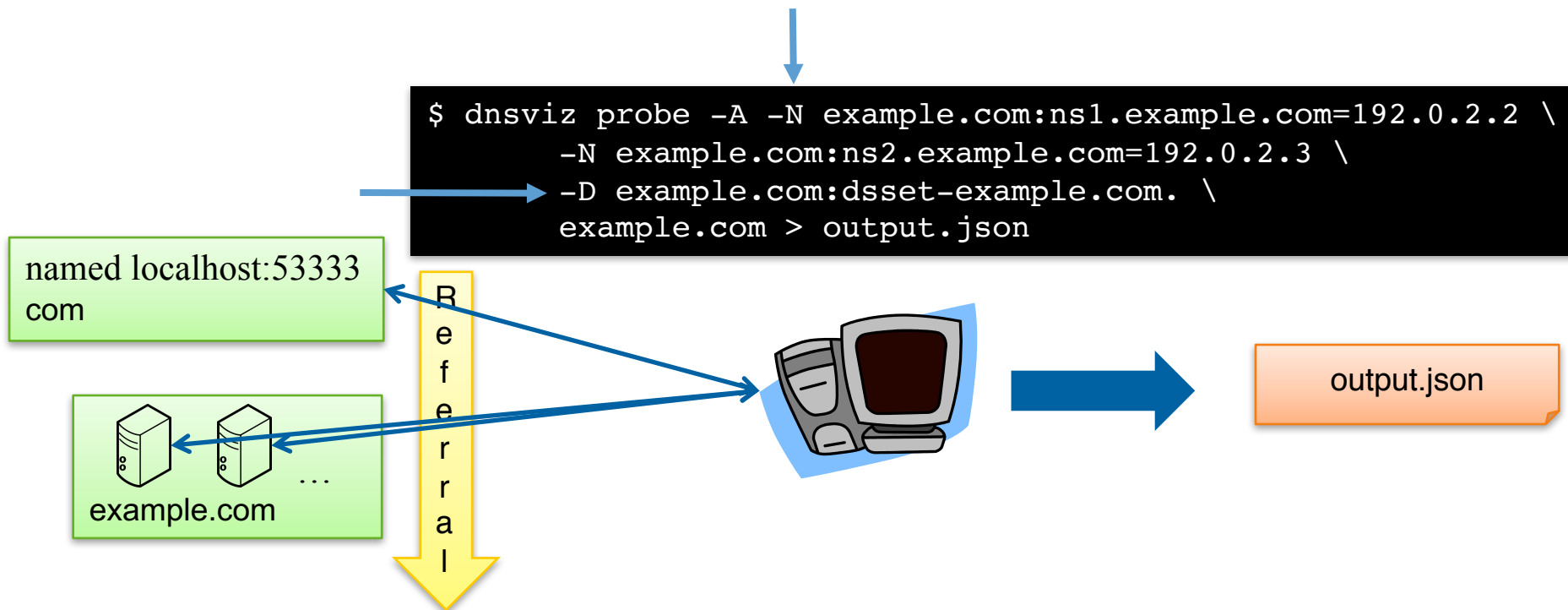
Pre-Authoritative Change DNS Testing with DNSViz

- Issue diagnostic queries against a stealth authoritative using "-x".

- Specify servers by names, addresses, or both – might or might not correspond to names in NS RRset.

- Ancestors **are** queried; delegation NS records **not** evaluated; DS records **are** evaluated.
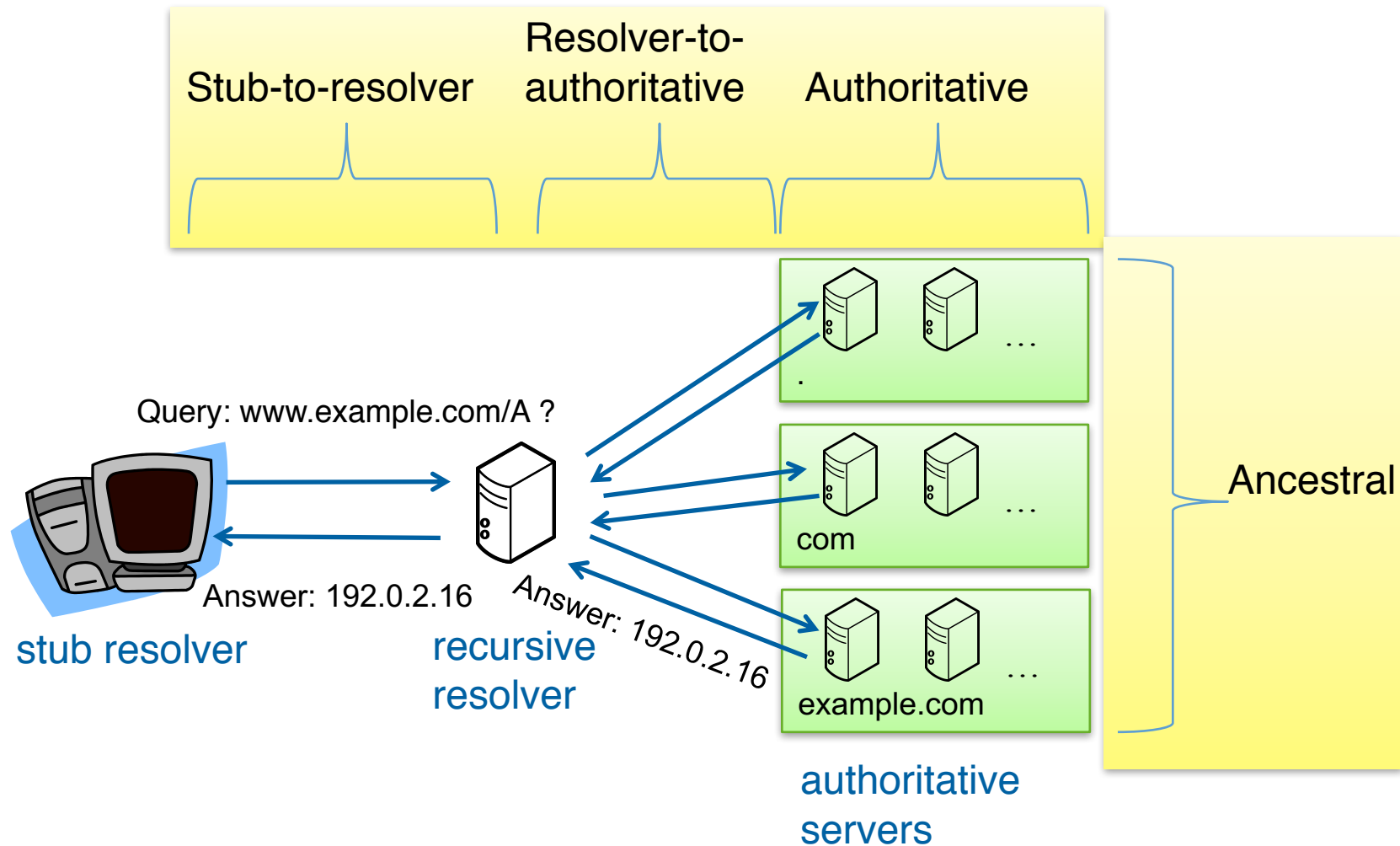


```
$ dnsviz probe –A –x example.com:ns1.example.com=192.0.2.2 \
       –x example.com:ns2.example.com=192.0.2.3 \
       example.com > output.json
```

Pre-Delegation Change DNS Testing with DNSViz

- Set up an artificial parent zone to test delegation using "-N" and "-D".

- Specify delegation NS names and glue as arguments to "-N".

- Specify DS records or dsset file as arguments to "-D".

- Parent zone queried; delegation NS/DS records **are** evaluated.

```
$ dnsviz probe –A –N example.com:ns1.example.com=192.0.2.2 \
      –N example.com:ns2.example.com=192.0.2.3 \
      –D example.com:dsset–example.com. \
      example.com > output.json
```

named localhost:53333
com

example.com

Referral

output.json

Measurement Areas Across a DNS Deployment

Temporal DNS Measurement

Pre-deployment	Post-deployment
Stealth authoritative servers Pre-delegation Authoritative change – NS/DNSKEY/A/AAAA Delegation change – NS/DS/glue	No cache presence Some cache presence

Summary

- The following provide improved perspectives for DNS health measurement:

    - A multi-vantage point perspective view, including recursive and authoritative.

    - Pre- and post-deployment checks.

- DNSViz provides functionality for quantitative and qualitative measurement via:

    - Authoritative checks, pre- and post-deployment.

    - Recursive checks.

    - DNS looking glass.

- Resources:

    - https://github.com/dnsviz/dnsviz

    - http://dnsviz.net/

powered by