Post-Quantum

Cryptography Conference

A testbed for evaluating Post-Quantum Algorithms for the DNS

Elmer Lastdrager

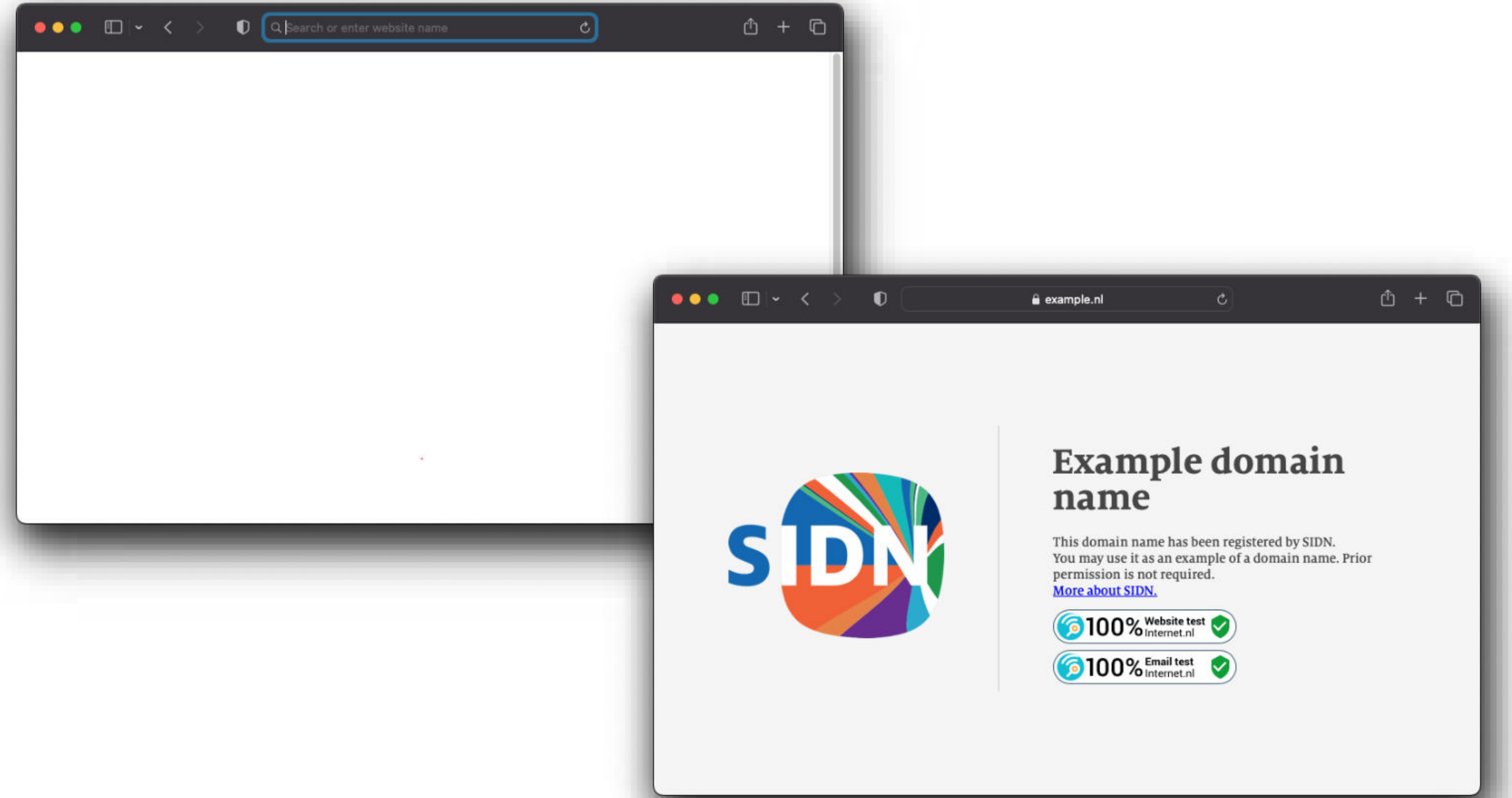
Research Engineer at SIDN Labs

A testbed for evaluating post-quantum algorithms for the DNS

Elmer Lastdrager| PQC Conference

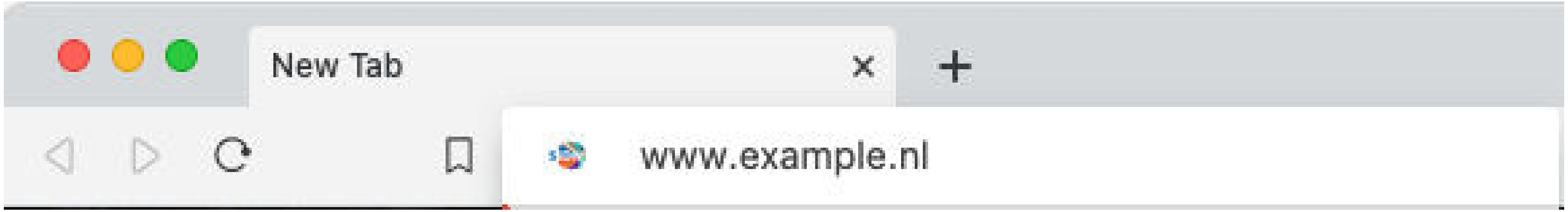
8 November 2023

A testbed for evaluating post-quantum algorithms for the DNS


Search or enter website name
example.nl
SIDN
100% Website test Internet.nl
100% Email test Internet.nl

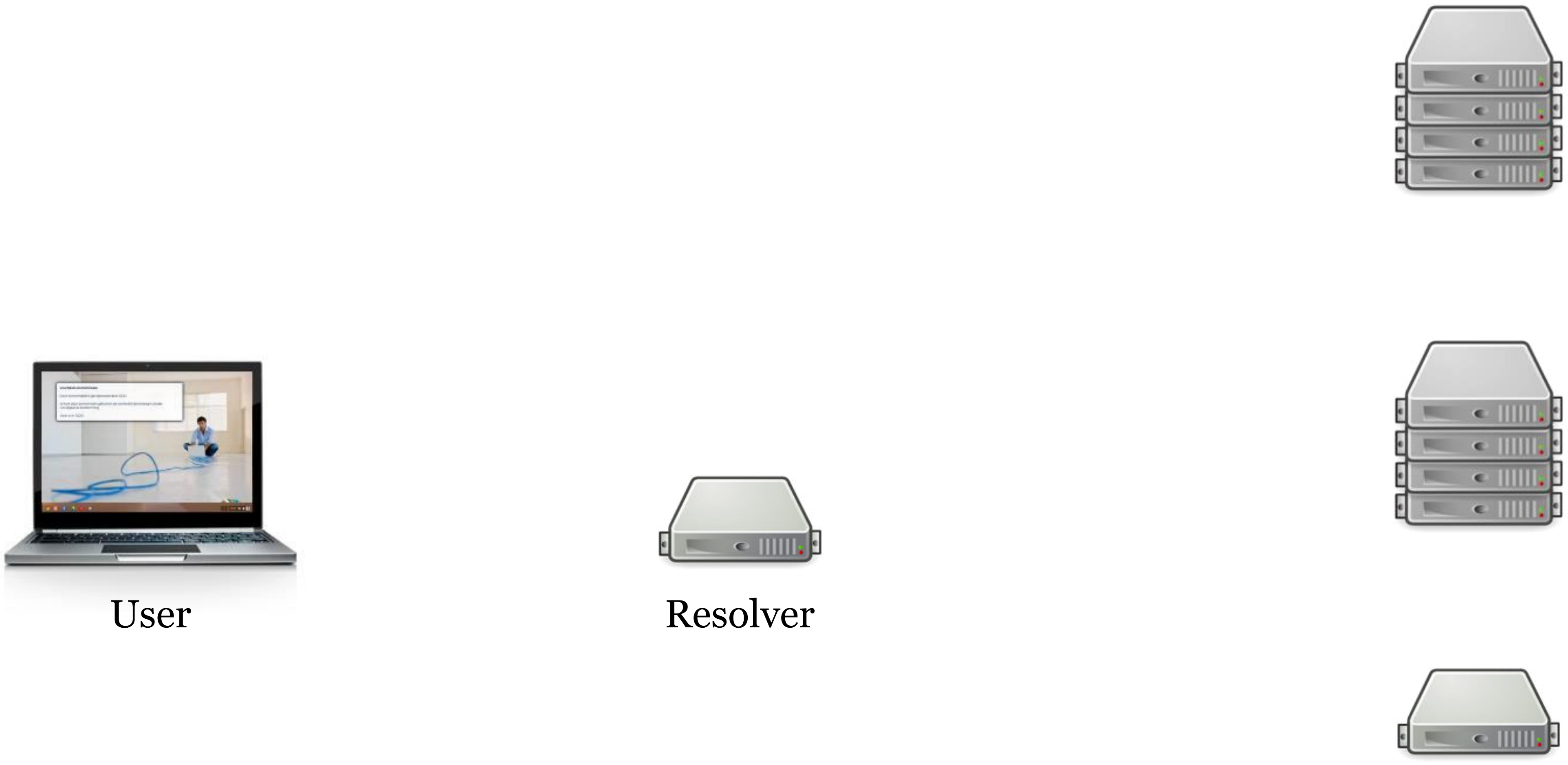
Example domain name

This domain name has been registered by SIDN.
You may use it as an example of a domain name. Prior permission is not required.
More about SIDN.



www.example.nl

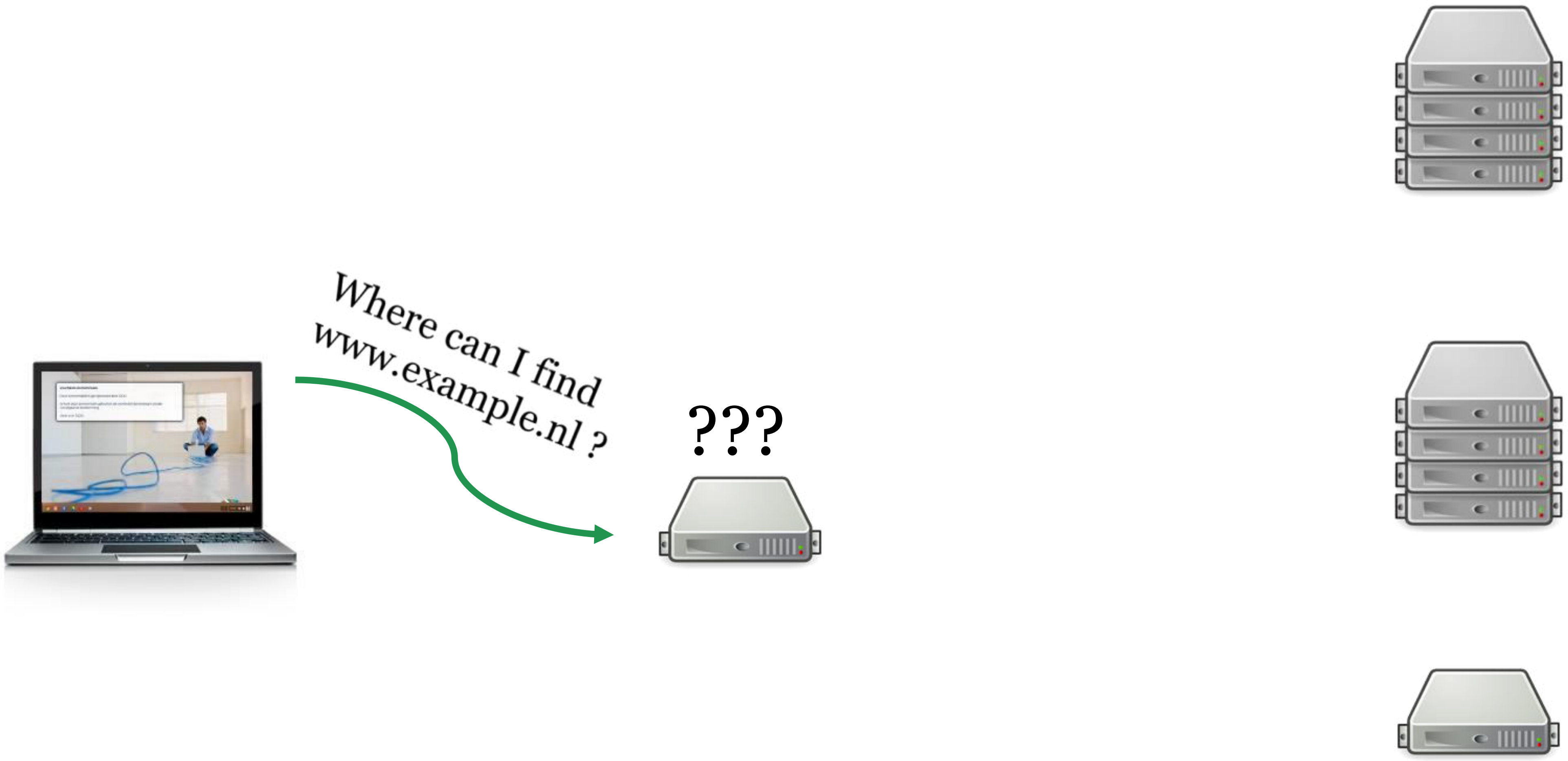
2a00:d78:0:712:94:198:159:35



User

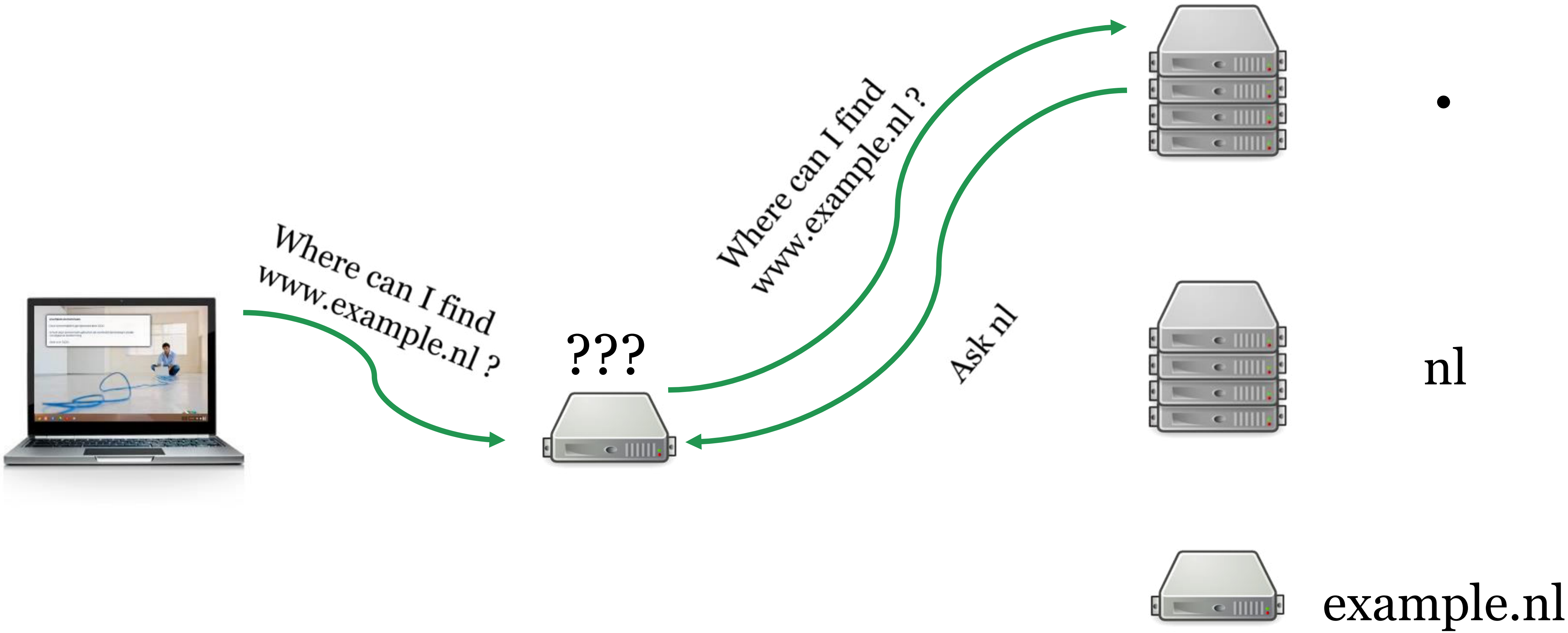
Resolver

Authoritative name servers



Where can I find www.example.nl ?

???



Where can I find www.example.nl ?

???

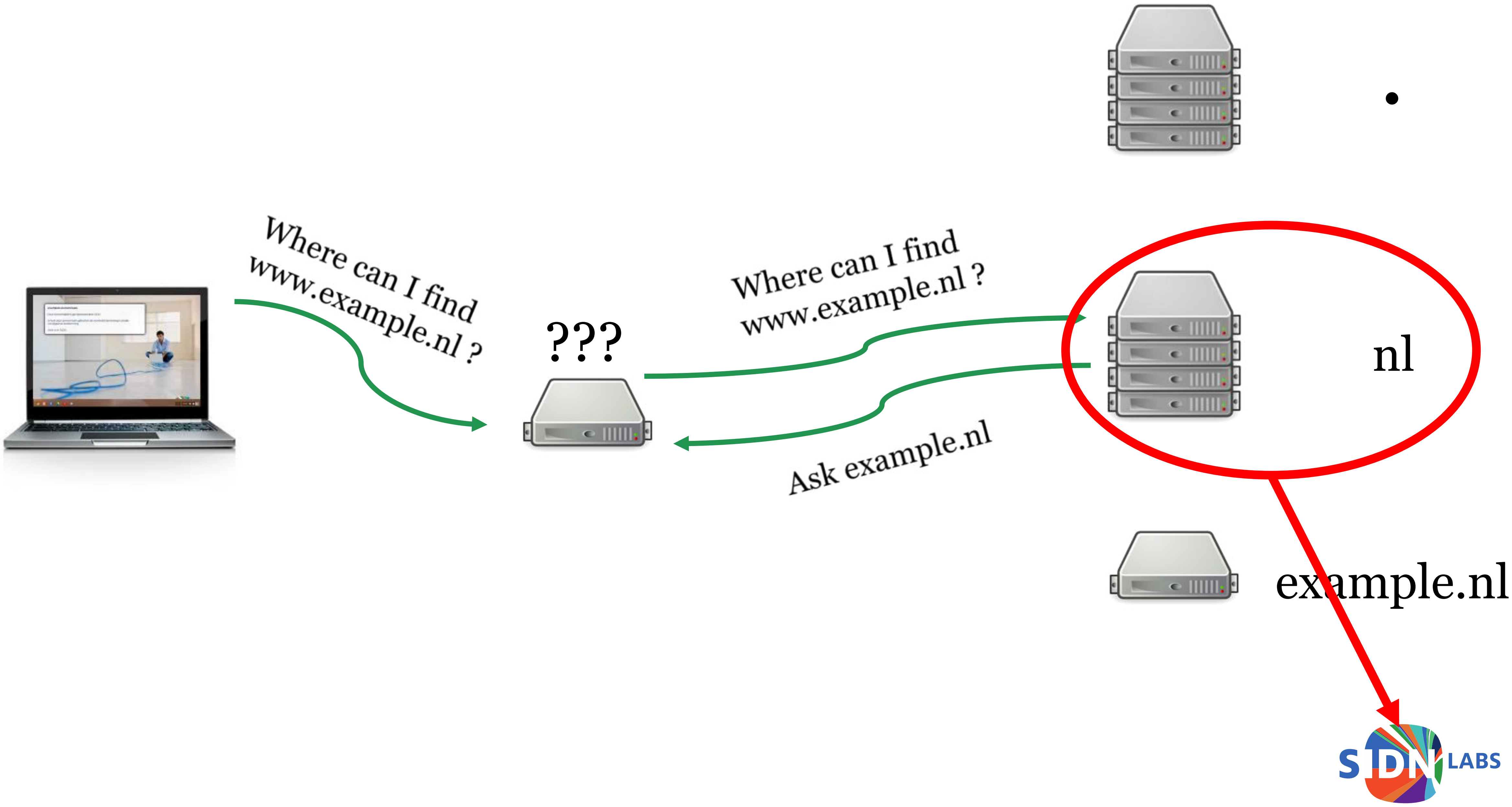
Where can I find www.example.nl ?

Ask nl

.

nl

example.nl



Where can I find www.example.nl ?

???

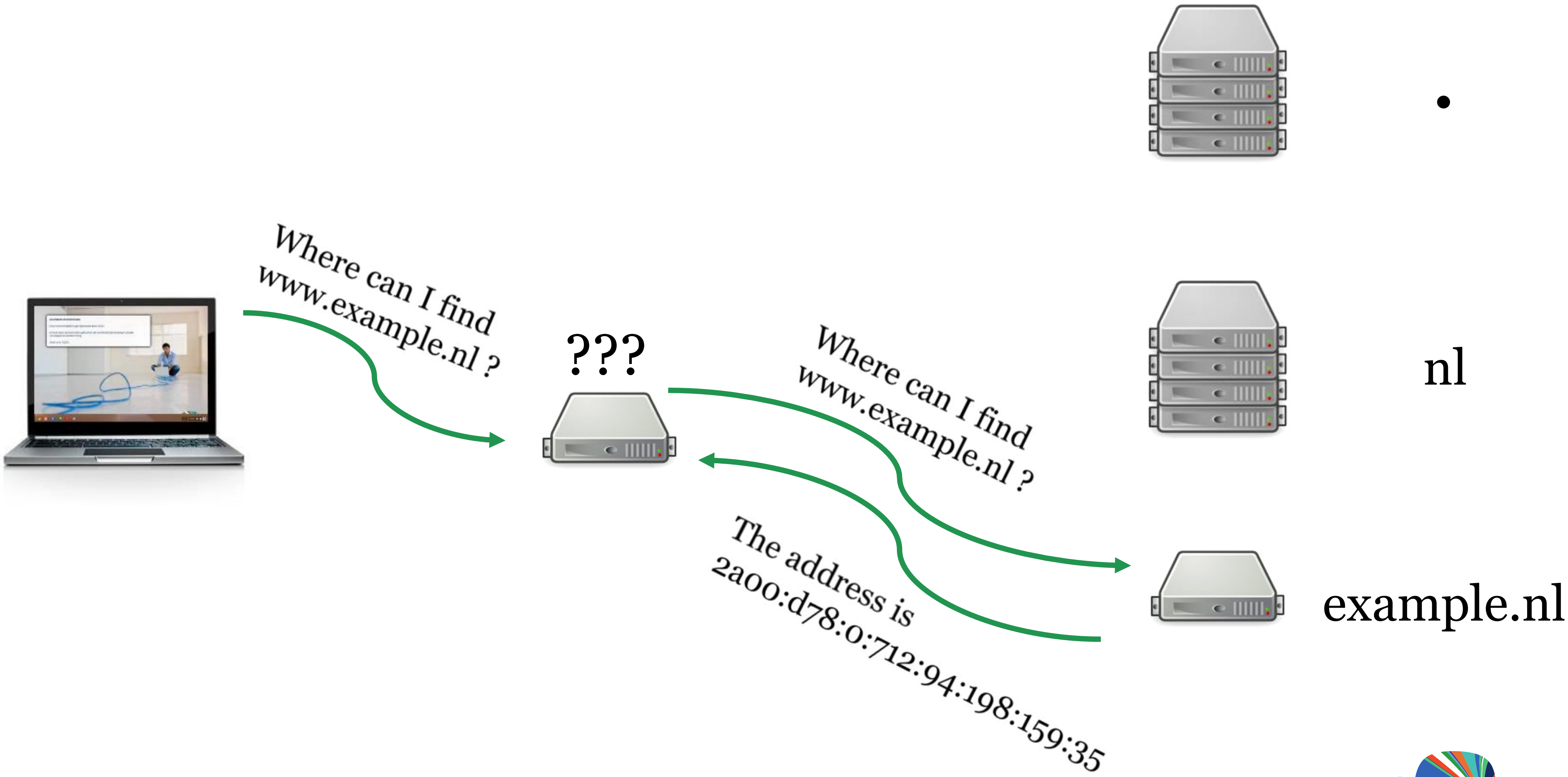
Where can I find www.example.nl ?

Ask example.nl

.

nl

example.nl



Where can I find www.example.nl ?

???

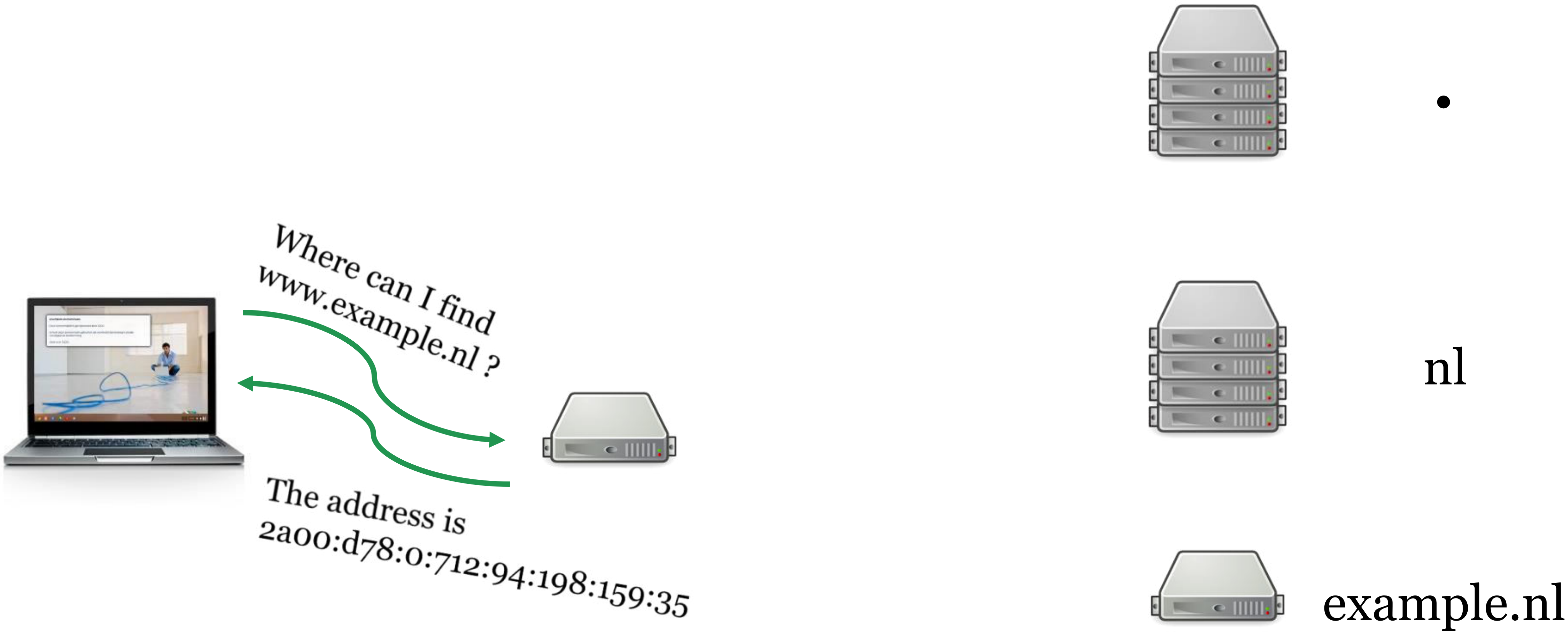
Where can I find www.example.nl ?

The address is 2a00:d78:0:712:94:198:159:35

.

nl

example.nl



Where can I find www.example.nl ?

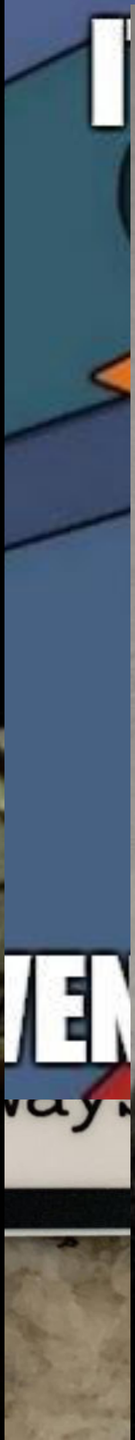
The address is 2a00:d78:0:712:94:198:159:35

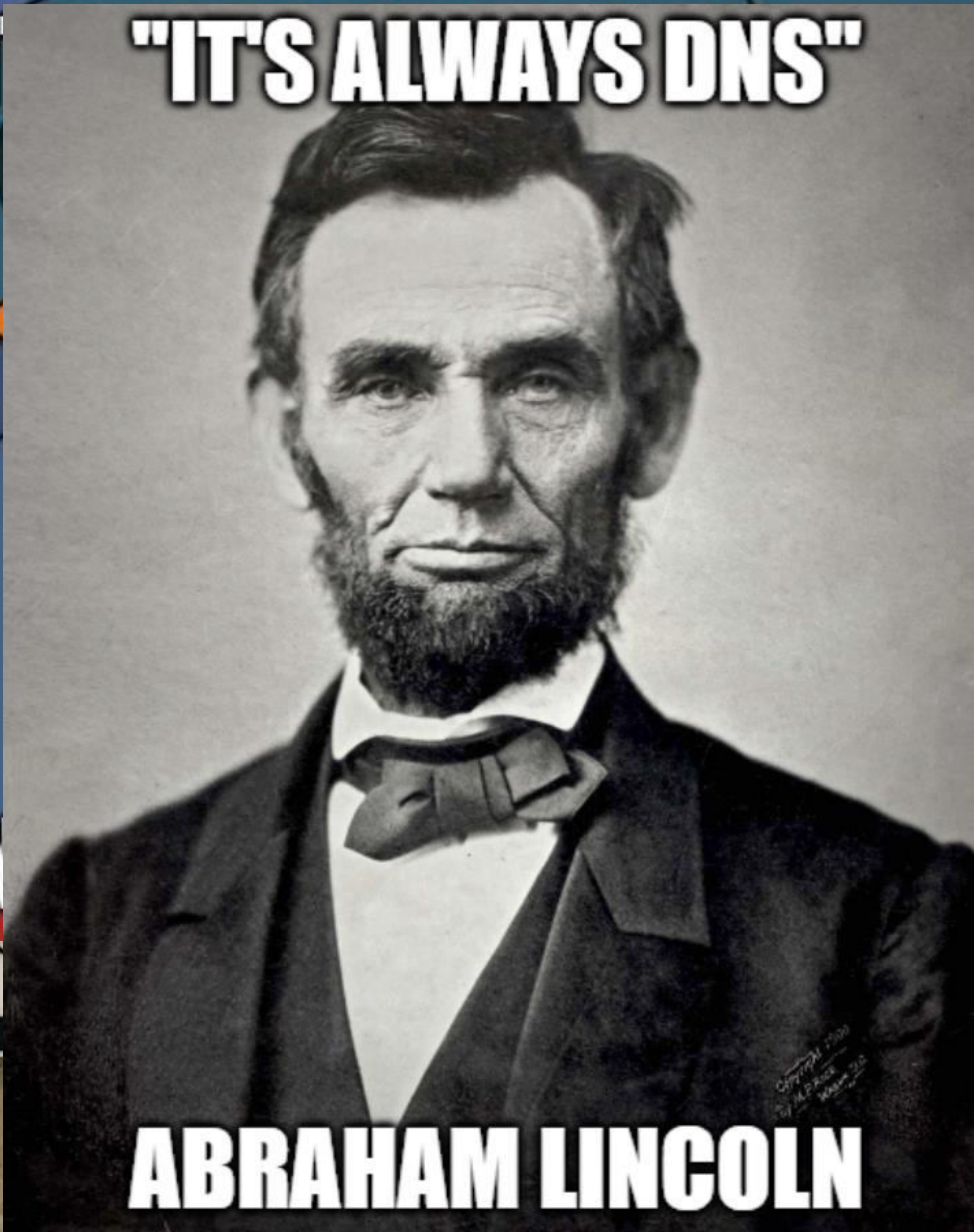
.

nl

example.nl

Why is it when something happens, it's always you three?
DNS
BGP
DHCP


I
VEN
way


"IT'S ALWAYS DNS"
ABRAHAM LINCOLN

.nl = the Netherlands

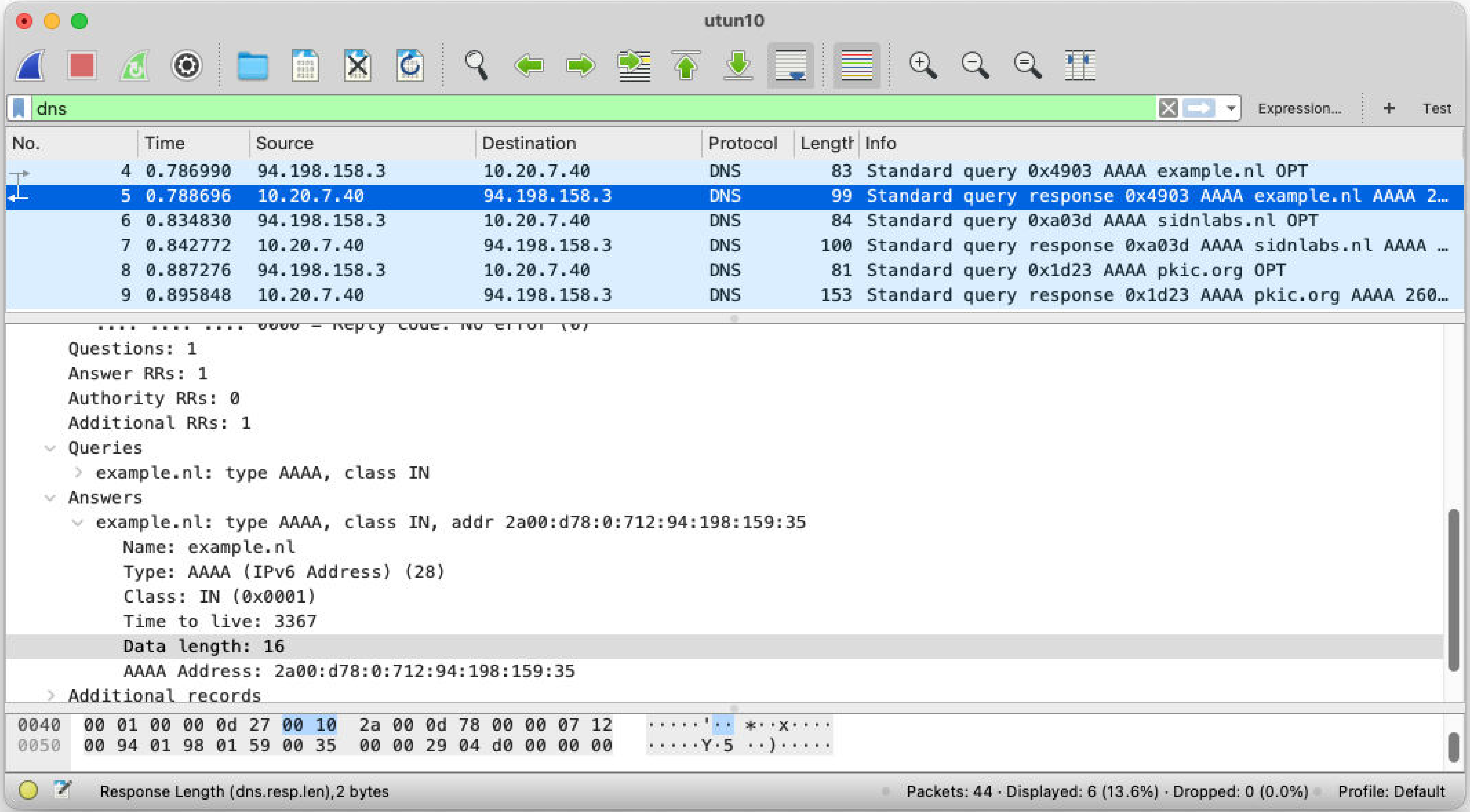
17M inhabitants

6.3M domain names

3.8M DNSSEC-signed

4.0B DNS queries/day

8.6B NTP queries/day



```
No.   Time       Source         Destination    Protocol  Length  Info
  4  0.786990   94.198.158.3   10.20.7.40     DNS        83  Standard query 0x4903 AAAA example.nl OPT
  5  0.788696   10.20.7.40     94.198.158.3   DNS        99  Standard query response 0x4903 AAAA example.nl AAAA 2…
  6  0.834830   94.198.158.3   10.20.7.40     DNS        84  Standard query 0xa03d AAAA sidnlabs.nl OPT
  7  0.842772   10.20.7.40     94.198.158.3   DNS       100  Standard query response 0xa03d AAAA sidnlabs.nl AAAA …
  8  0.887276   94.198.158.3   10.20.7.40     DNS        81  Standard query 0x1d23 AAAA pkic.org OPT
  9  0.895848   10.20.7.40     94.198.158.3   DNS       153  Standard query response 0x1d23 AAAA pkic.org AAAA 260…
```

```
    .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 1
  ⌄ Queries
    › example.nl: type AAAA, class IN
  ⌄ Answers
    ⌄ example.nl: type AAAA, class IN, addr 2a00:d78:0:712:94:198:159:35
        Name: example.nl
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
        Time to live: 3367
        Data length: 16
        AAAA Address: 2a00:d78:0:712:94:198:159:35
  › Additional records
```

```
0040  00 01 00 00 0d 27 00 10  2a 00 0d 78 00 00 07 12   .....'.. *..x....
0050  00 94 01 98 01 59 00 35  00 00 29 04 d0 00 00 00   .....Y.5 ..).....
```

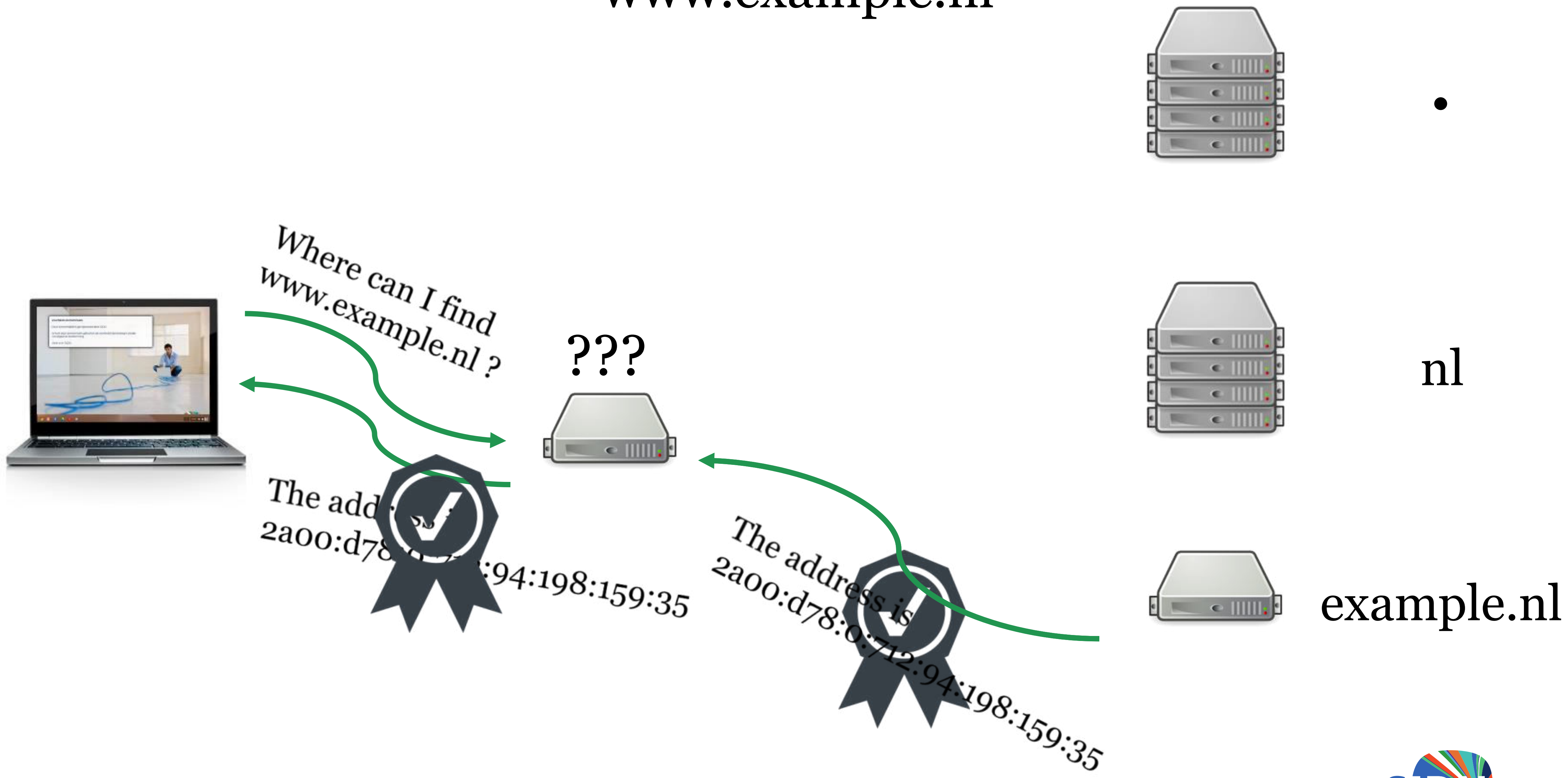
```
Response Length (dns.resp.len),2 bytes          Packets: 44 · Displayed: 6 (13.6%) · Dropped: 0 (0.0%)    Profile: Default
```

DoH, DoT, DNScrypt
https://dns4all.eu/

X25519Kyber768

DNSSEC

www.example.nl



.

nl

example.nl

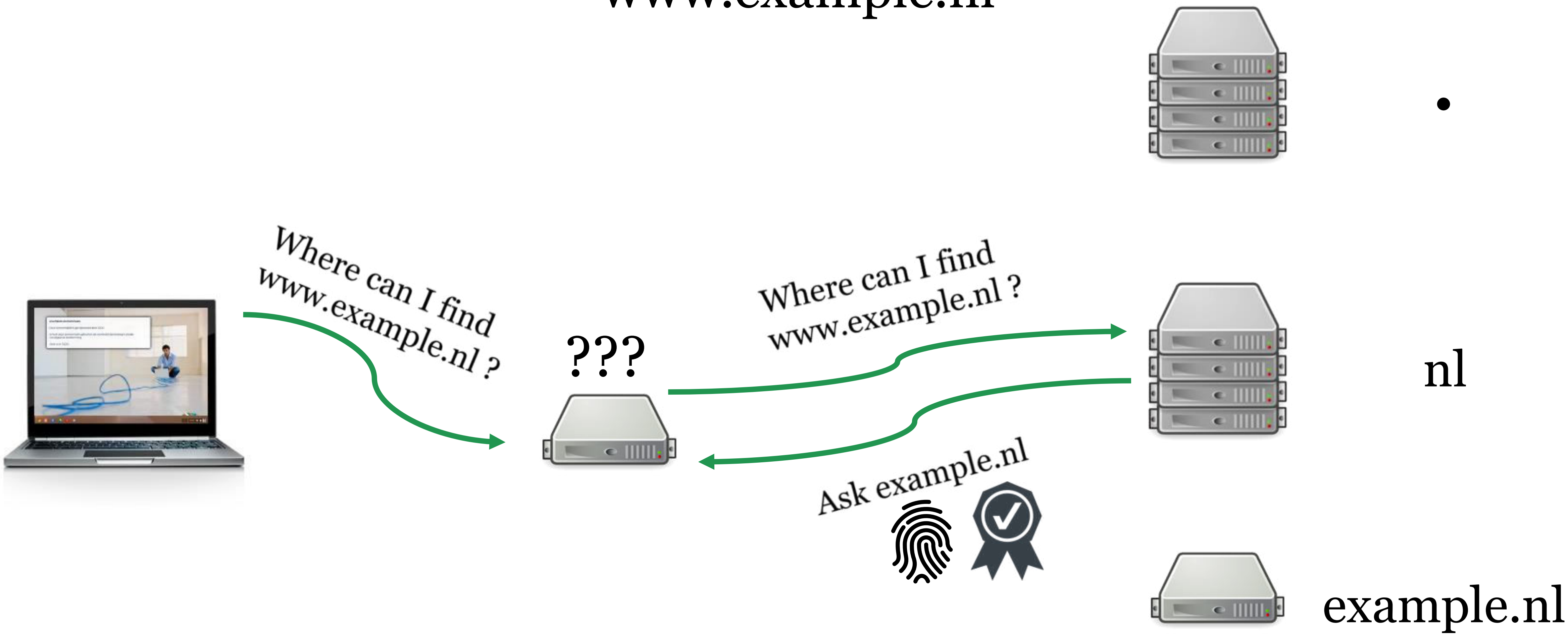
Where can I find www.example.nl ?

???

The address is 2a00:d78:0:712:94:198:159:35

The add 2a00:d78 :94:198:159:35

www.example.nl



.

Where can I find www.example.nl ?

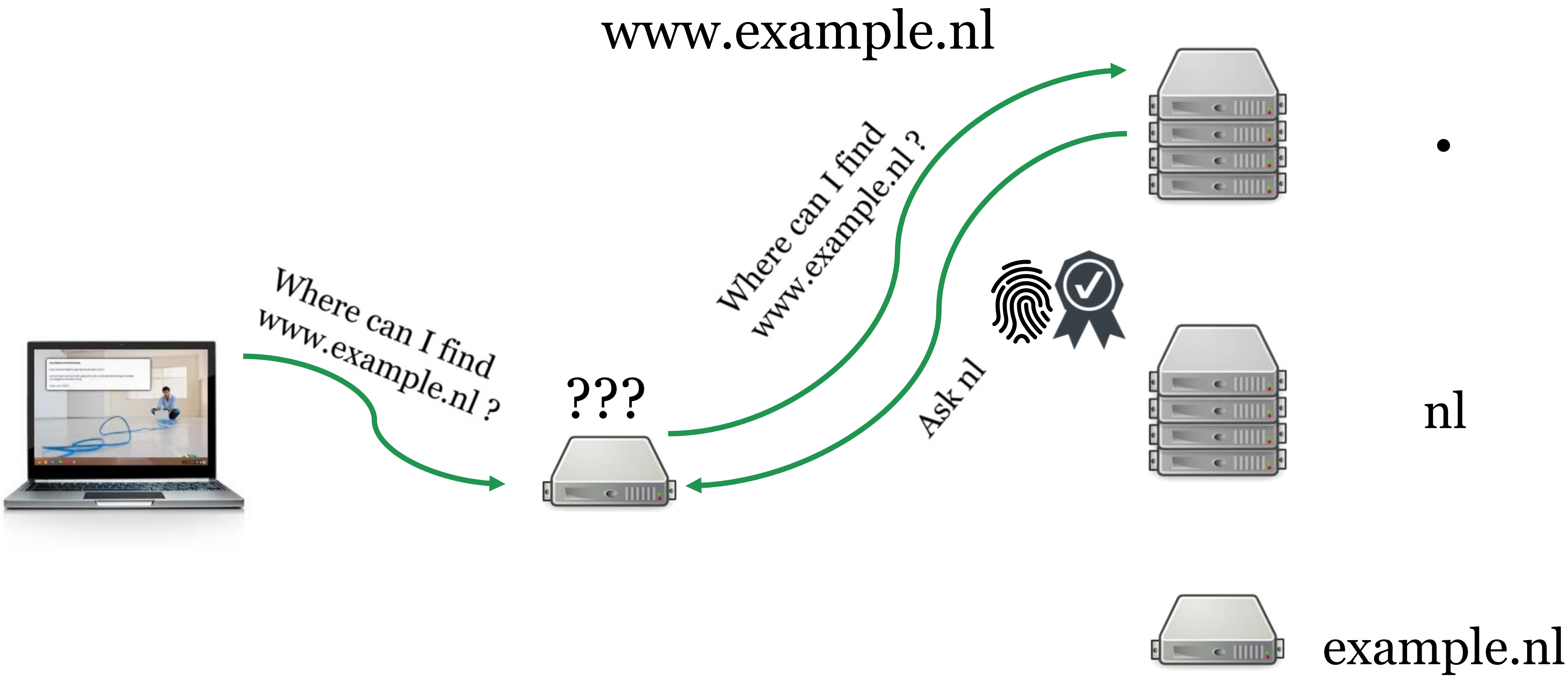
???

Where can I find www.example.nl ?

nl

Ask example.nl

example.nl



www.example.nl

Where can I find www.example.nl ?

???

Where can I find www.example.nl ?

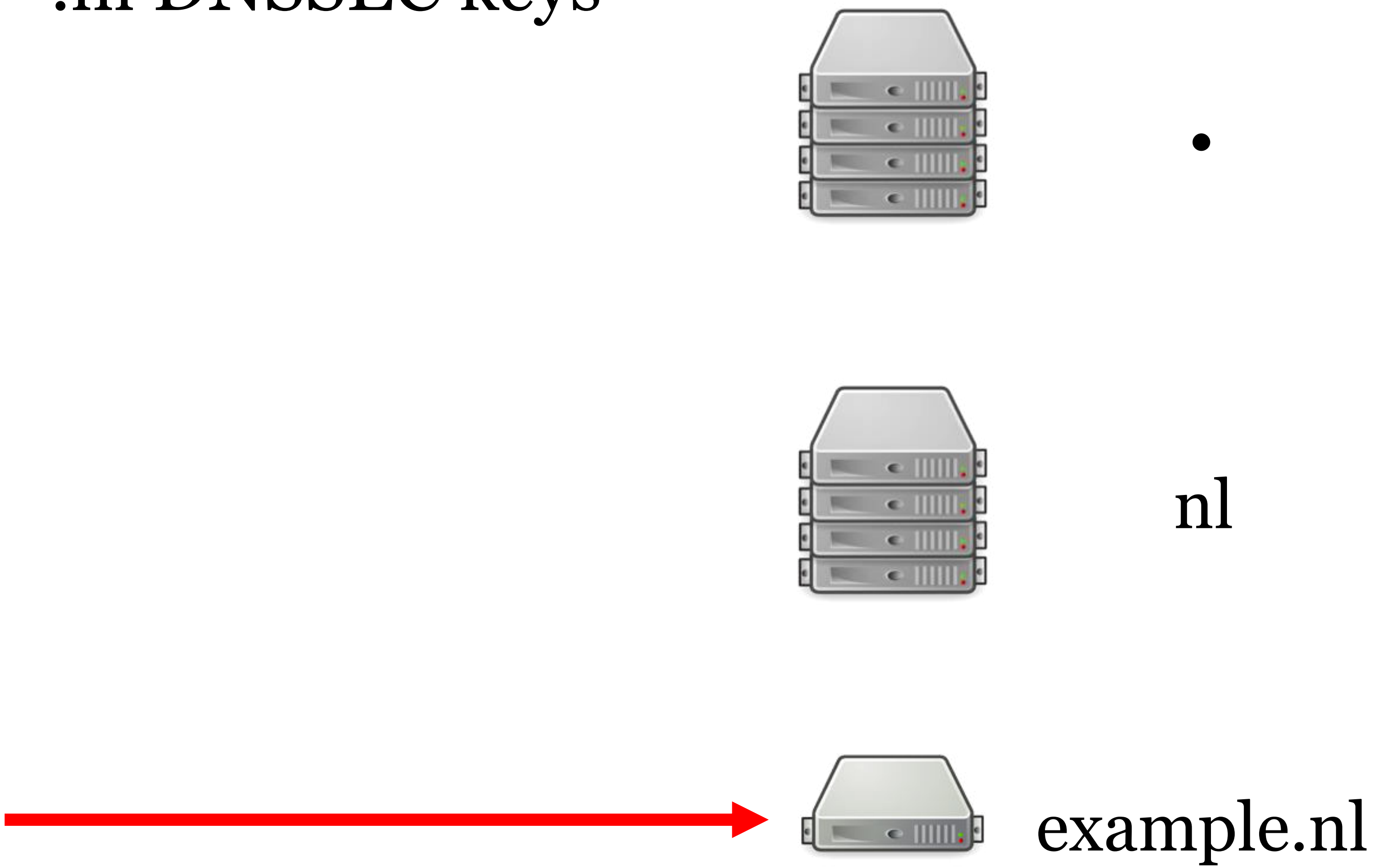
Ask nl

.

nl

example.nl

.nl DNSSEC keys

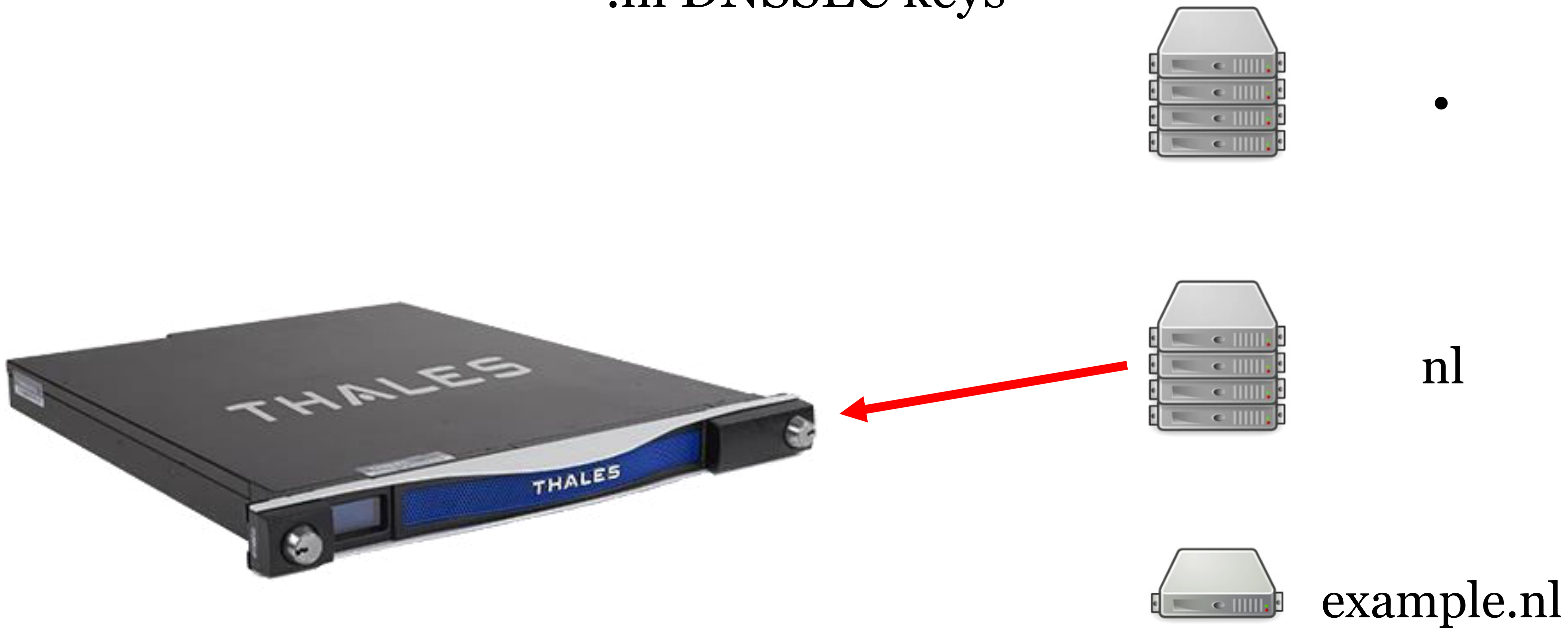


.

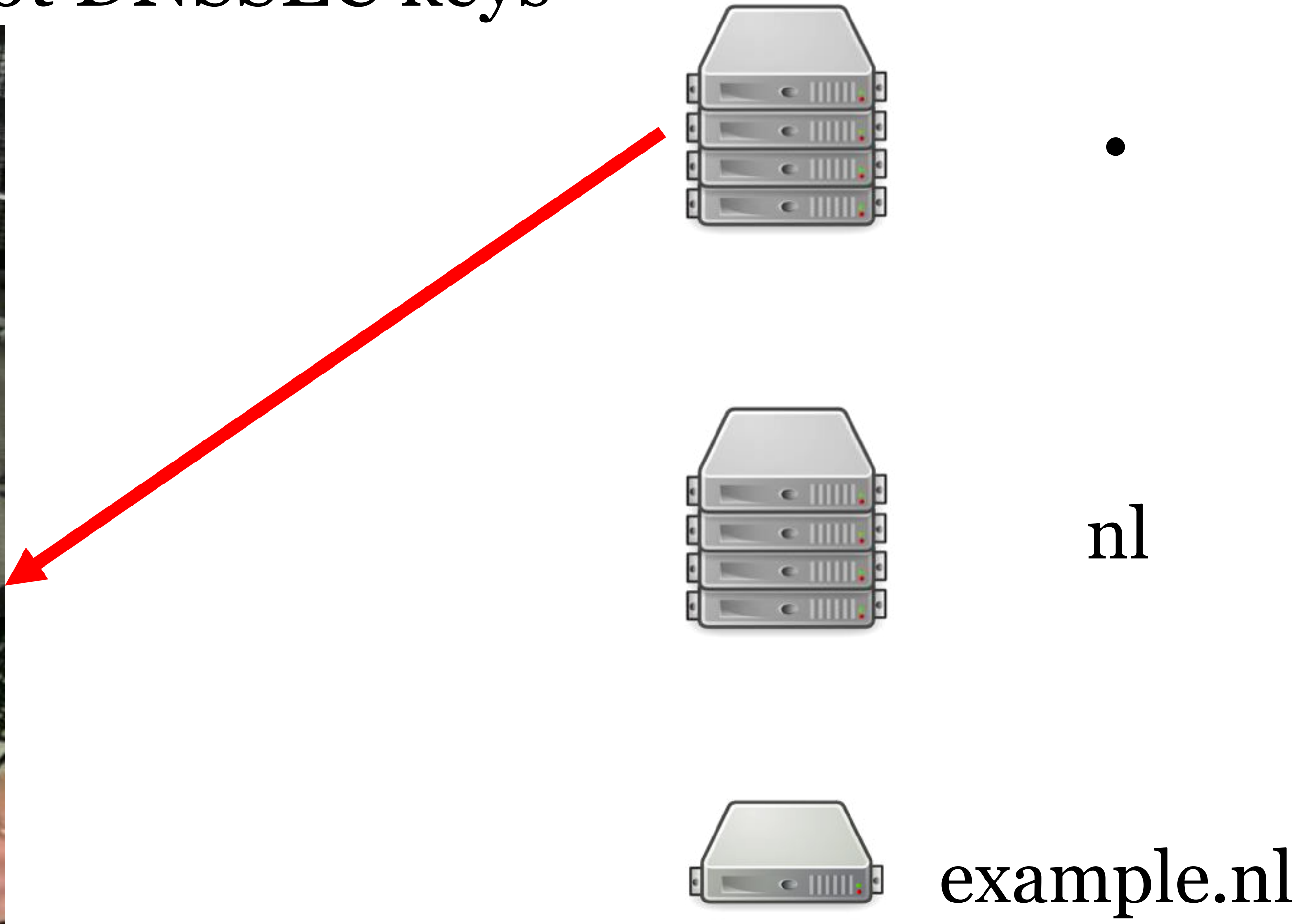
nl

example.nl

.nl DNSSEC keys

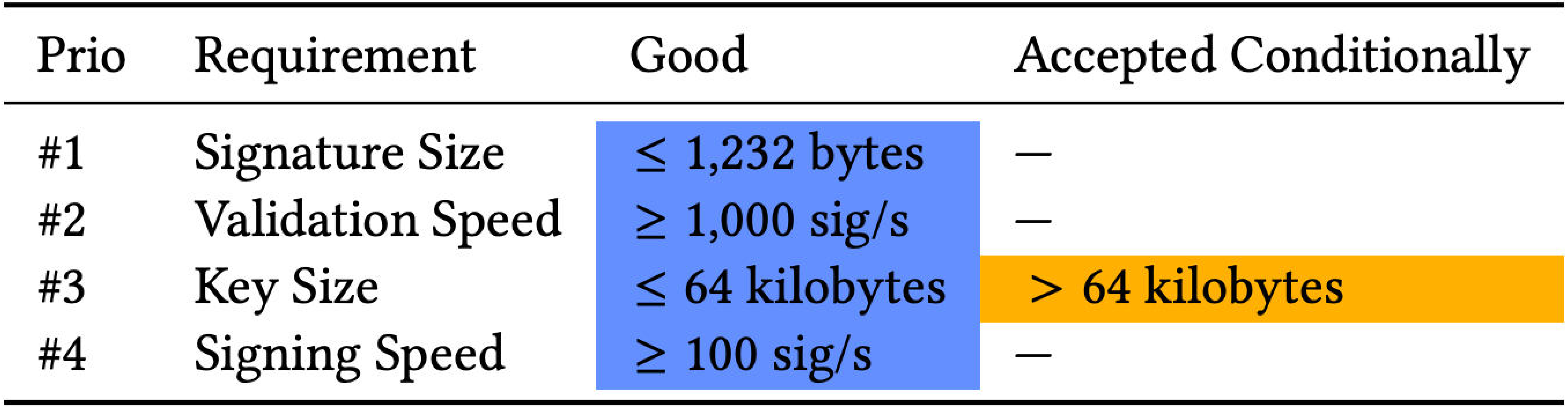


Root DNSSEC keys



A testbed for evaluating post-quantum algorithms for the DNS

Requirements



Prio	Requirement	Good	Accepted Conditionally
#1	Signature Size	≤ 1,232 bytes	—
#2	Validation Speed	≥ 1,000 sig/s	—
#3	Key Size	≤ 64 kilobytes	> 64 kilobytes
#4	Signing Speed	≥ 100 sig/s	—

Table 2: Requirements for quantum-safe algorithms.

M. Müller et al, "Retrofitting Post-Quantum Cryptography in Internet Protocols: A Case Study of DNSSEC", ACM SIGCOMM Computer Communication Review, vol. 50, no. 4, 2020.

Jürgen Henn – 11foot8.com

CONSOLE
DISK 1
EJECT

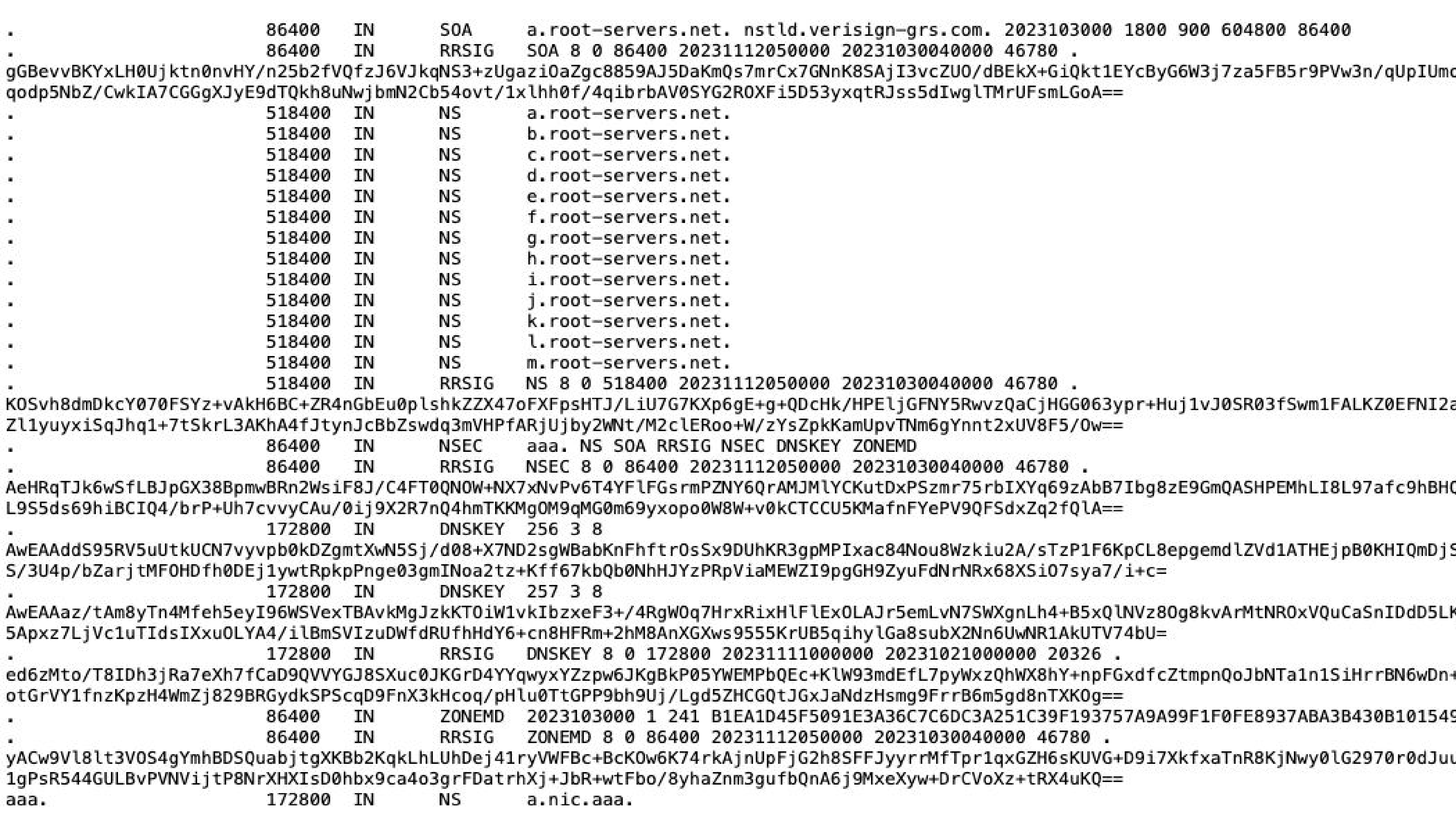
gifbin.com

THALES
THALES

NCIPHER
29 40 49 60 71 82 °C
NCIPHER
N-022000-L

utimaco

A testbed for evaluating post-quantum algorithms for the DNS



```
.                       86400   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2023103000 1800 900 604800 86400
.                       86400   IN      RRSIG   SOA 8 0 86400 20231112050000 20231030040000 46780 .
gGBevvBKYxLH0Ujktn0nvHY/n25b2fVQfzJ6VJkqNS3+zUgaziOaZgc8859AJ5DaKmQs7mrCx7GNnK8SAjI3vcZUO/dBEkX+GiQkt1EYcByG6W3j7za5FB5r9PVw3n/qUpIUmc
qodp5NbZ/CwkIA7CGGgXJyE9dTQkh8uNwjbmN2Cb54ovt/1xlhh0f/4qibrbAV0SYG2ROXFi5D53yxqtRJss5dIwglTMrUFsmLGoA==
.                       518400  IN      NS      a.root-servers.net.
.                       518400  IN      NS      b.root-servers.net.
.                       518400  IN      NS      c.root-servers.net.
.                       518400  IN      NS      d.root-servers.net.
.                       518400  IN      NS      e.root-servers.net.
.                       518400  IN      NS      f.root-servers.net.
.                       518400  IN      NS      g.root-servers.net.
.                       518400  IN      NS      h.root-servers.net.
.                       518400  IN      NS      i.root-servers.net.
.                       518400  IN      NS      j.root-servers.net.
.                       518400  IN      NS      k.root-servers.net.
.                       518400  IN      NS      l.root-servers.net.
.                       518400  IN      NS      m.root-servers.net.
.                       518400  IN      RRSIG   NS 8 0 518400 20231112050000 20231030040000 46780 .
KOSvh8dmDkcY070FSYz+vAkH6BC+ZR4nGbEu0plshkZZX47oFXFpsHTJ/LiU7G7KXp6gE+g+QDcHk/HPEljGFNY5RwvzQaCjHGG063ypr+Huj1vJ0SR03fSwm1FALKZ0EFNI2a
Zl1yuyxiSqJhq1+7tSkrL3AKhA4fJtynJcBbZswdq3mVHPfARjUjby2WNt/M2clERoo+W/zYsZpkKamUpvTNm6gYnnt2xUV8F5/Ow==
.                       86400   IN      NSEC    aaa. NS SOA RRSIG NSEC DNSKEY ZONEMD
.                       86400   IN      RRSIG   NSEC 8 0 86400 20231112050000 20231030040000 46780 .
AeHRqTJk6wSfLBJpGX38BpmwBRn2WsiF8J/C4FT0QNOW+NX7xNvPv6T4YFlFGsrmPZNY6QrAMJMlYCKutDxPSzmr75rbIXYq69zAbB7Ibg8zE9GmQASHPEMhLI8L97afc9hBHQ
L9S5ds69hiBCIQ4/brP+Uh7cvvyCAu/0ij9X2R7nQ4hmTKKMgOM9qMG0m69yxopo0W8W+v0kCTCCU5KMafnFYePV9QFSdxZq2fQlA==
.                       172800  IN      DNSKEY  256 3 8
AwEAAddS95RV5uUtkUCN7vyvpb0kDZgmtXwN5Sj/d08+X7ND2sgWBabKnFhftrOsSx9DUhKR3gpMPIxac84Nou8Wzkiu2A/sTzP1F6KpCL8epgemdlZVd1ATHEjpB0KHIQmDjS
S/3U4p/bZarjtMFOHDfh0DEj1ywtRpkpPnge03gmINoa2tz+Kff67kbQb0NhHJYzPRpViaMEWZI9pgGH9ZyuFdNrNRx68XSiO7sya7/i+c=
.                       172800  IN      DNSKEY  257 3 8
AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LK
5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU=
.                       172800  IN      RRSIG   DNSKEY 8 0 172800 20231111000000 20231021000000 20326 .
ed6zMto/T8IDh3jRa7eXh7fCaD9QVVYGJ8SXuc0JKGrD4YYqwyxYZzpw6JKgBkP05YWEMPbQEc+KlW93mdEfL7pyWxzQhWX8hY+npFGxdfcZtmpnQoJbNTa1n1SiHrrBN6wDn+
otGrVY1fnzKpzH4WmZj829BRGydkSPScqD9FnX3kHcoq/pHlu0TtGPP9bh9Uj/Lgd5ZHCGQtJGxJaNdzHsmg9FrrB6m5gd8nTXKOg==
.                       86400   IN      ZONEMD  2023103000 1 241 B1EA1D45F5091E3A36C7C6DC3A251C39F193757A9A99F1F0FE8937ABA3B430B101549
.                       86400   IN      RRSIG   ZONEMD 8 0 86400 20231112050000 20231030040000 46780 .
yACw9Vl8lt3VOS4gYmhBDSQuabjtgXKBb2KqkLhLUhDej41ryVWFBc+BcKOw6K74rkAjnUpFjG2h8SFFJyyrrMfTpr1qxGZH6sKUVG+D9i7XkfxaTnR8KjNwy0lG2970r0dJuu
1gPsR544GULBvPVNVijtP8NrXHXIsD0hbx9ca4o3grFDatrhXj+JbR+wtFbo/8yhaZnm3gufbQnA6j9MxeXyw+DrCVoXz+tRX4uKQ==
aaa.                    172800  IN      NS      a.nic.aaa.
```

TAKE
AWAY
1
ZURICH

Thank you for your attention!

Elmer Lastdrager
elmer.lastdrager@sidn.nl

@elmerlastdrager
@elmer@c.im

https://www.sidnlabs.nl/en

SIDN LABS

Post-Quantum

Cryptography Conference

A testbed for evaluating Post-Quantum Algorithms for the DNS

Elmer Lastdrager

Research Engineer at SIDN Labs