Gastcollege DNS en DNS Security

Jelte Jansen

Saxion Hogeschool

2020-10-19

SIDN LABS

Agenda

- Introductie
- DNS
- Aanvallen op, en met, DNS
- Misbruik van domeinnamen
- Fake webshops

Stichting Internet Domeinregistratie Nederland (SIDN)

- Beheert '.nl'
  - > 6 miljoen .nl-domeinnamen
  - > 2 miljard bevragingen per dag

https://sidn.nl

Activiteiten naast .nl

- SIDN Fonds
- Cybersterk
- IRMA
- .aw, .amsterdam, .politie

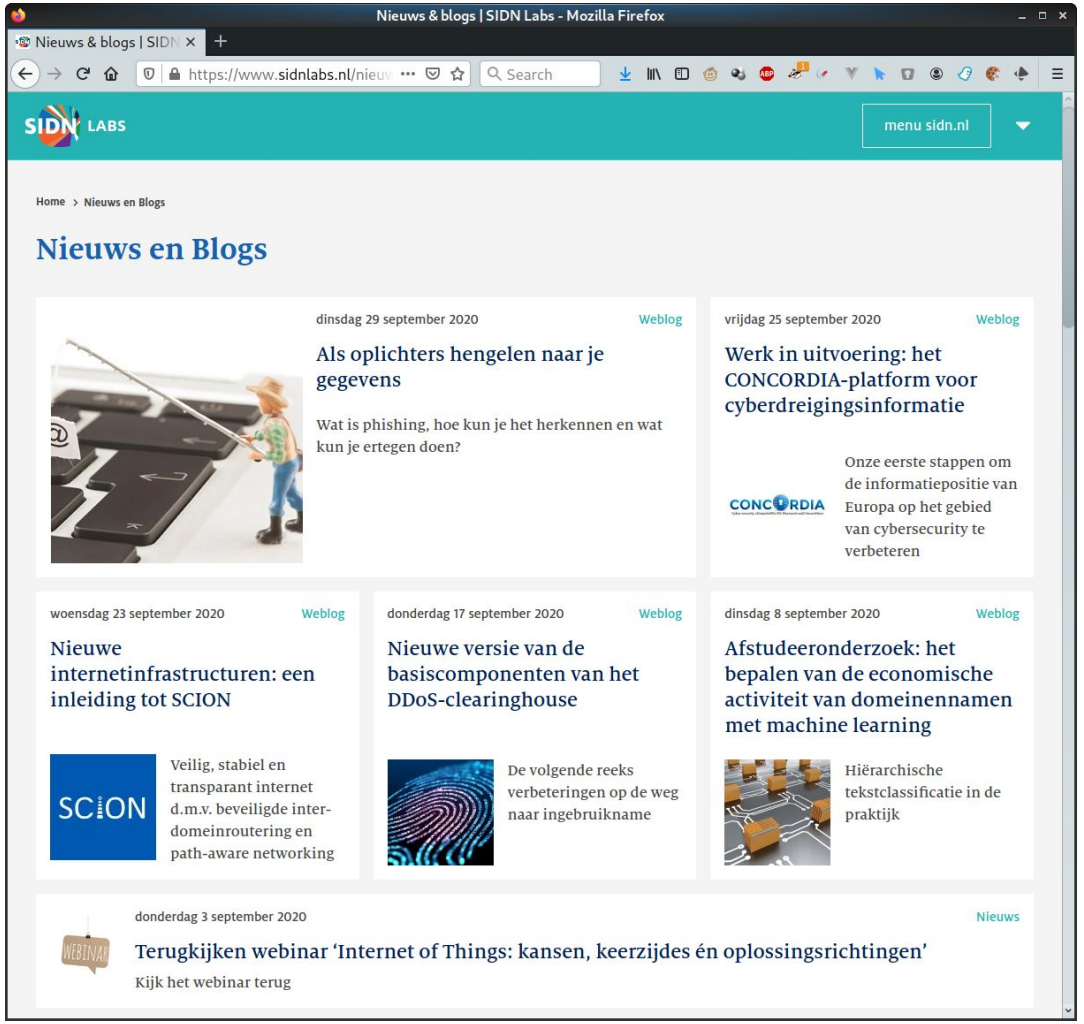
SIDN Labs

Onderzoek, Prototyping, Security

Bijvoorbeeld:

- Fake webshop-detectie
- SPIN (IoT-bescherming)
- Ondersteuning operations en support

https://www.sidnlabs.nl

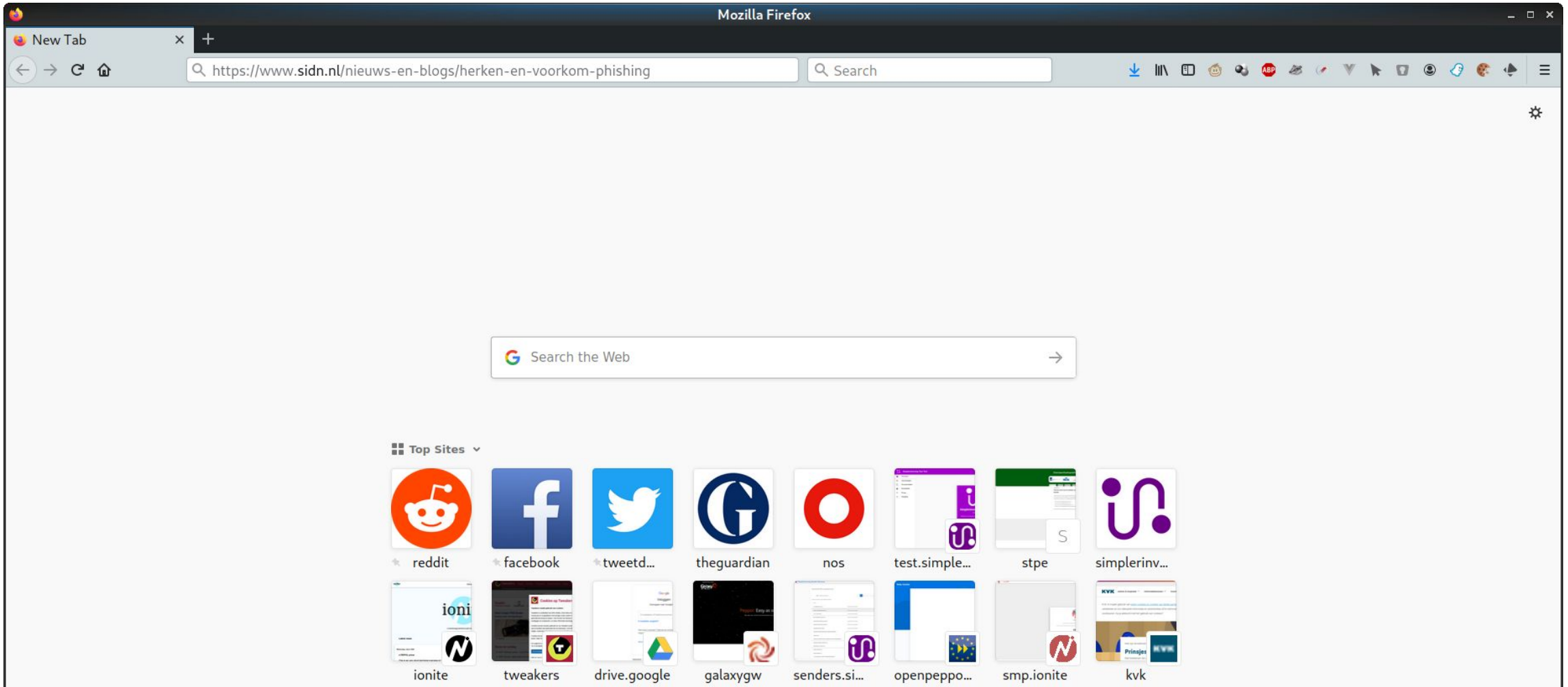


Maar wat **doet** SIDN dan eigenlijk?

Daarvoor eerst wat over de geschiedenis en werking van DNS

SIDN LABS

DNS


Mozilla Firefox
New Tab
https://www.sidn.nl/nieuws-en-blogs/herken-en-voorkom-phishing
Search
Search the Web
Top Sites
reddit
facebook
tweetd...
theguardian
nos
test.simple...
stpe
simplerinv...
ionite
tweakers
drive.google
galaxygw
senders.si...
openpeppo...
smp.ionite
kvk

Domeinnamen

https://www.sidn.nl/nieuws-en-blogs/herken-en-voorkom-phishing

Domeinnamen

https://www.sidn.nl/nieuws-en-blogs/herken-en-voorkom-phishing

Wat is hier de domeinnaam?

Domeinnamen

https://www.sidn.nl/nieuws-en-blogs/herken-en-voorkom-phishing

Wat is hier de domeinnaam?

Domeinnamen

Een domeinnaam bestaat uit **labels**

www sidn nl

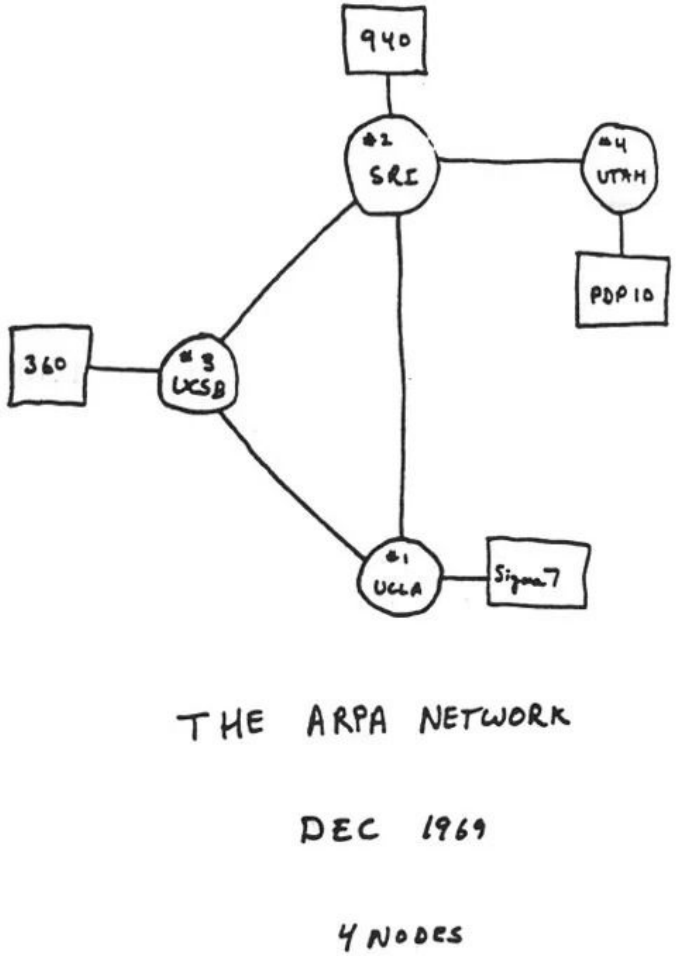
Van rechts naar links:

1) Top-level domain: nl (of .com, .org, .amsterdam, etc.)
2) Second-level domain: sidn (of saxion, nos, telegraaf, etc.)
3) Third-level domain: www
4) enzovoorts

Een kleine geschiedenis van DNS

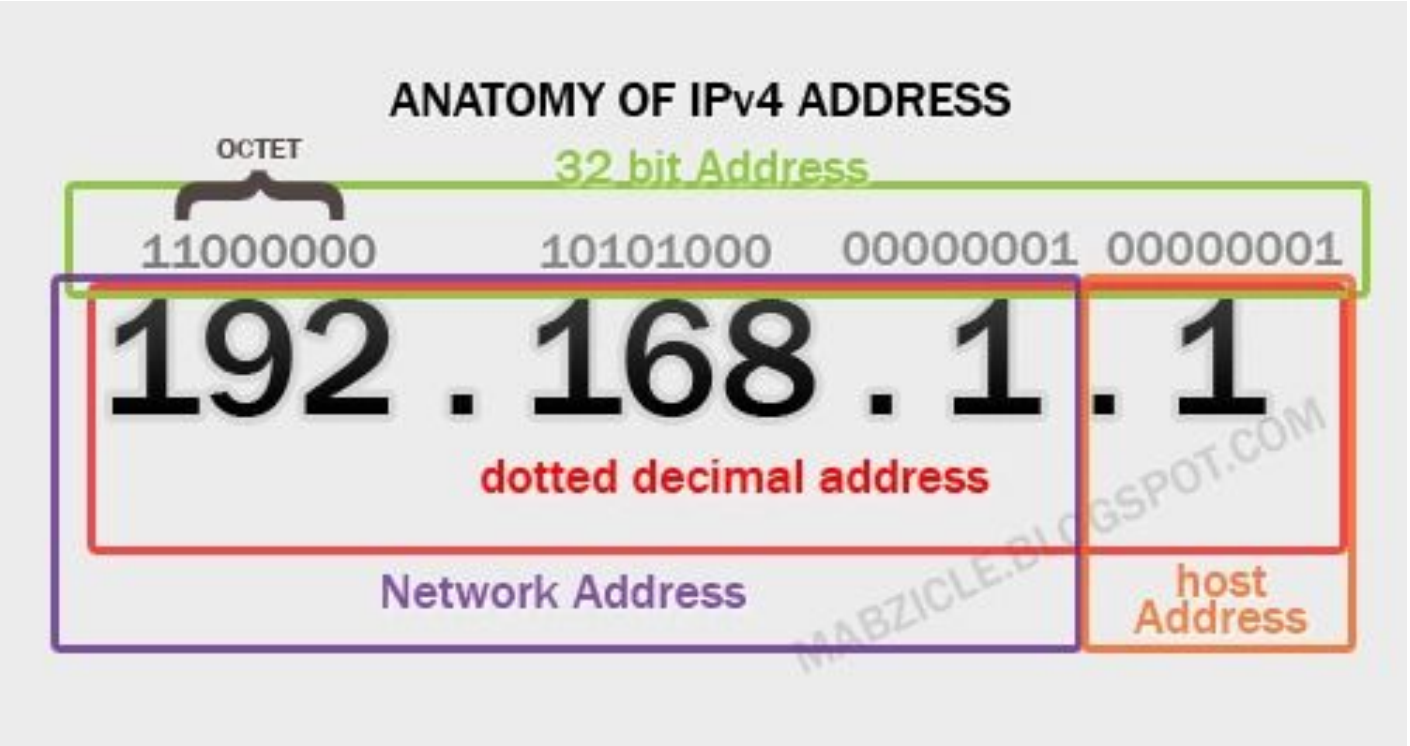
De tijd voor DNS

- In het begin waren er maar een paar computers op het Internet
- Deze hadden zogenaamde IP-adressen, zoals 35.190.27.69
- Iedereen op het netwerk kende de adressen uit hun hoofd
- Maar het netwerk groeide…



De tijd voor DNS

- Het internet werd een hierarchisch netwerk van netwerken
- Netwerken, en computers daarop kregen IP-adressen



De tijd voor DNS

- Mensen gebruiken liever namen, zoals www.internet.nl
- Dus bedacht men dat het handig was om op elke computer een 'adresboek' neer te zetten
- Dit werd een vast bestand hosts.txt
- Hierin stonden **alle** computers op het Internet
- Als er een bijkwam, updatete iedereen hun hosts.txt

De tijd voor DNS

- Dit werd -uiteraard- geautomatiseerd
- Er werd 1 centrale computer uitgekozen, waar hosts.txt werd bijgehouden
- Elke computer op het Internet downloadde updates hiervan automatisch
- Maar het netwerk groeide…

De eerste versie van DNS

- Toen kwam het concept van domeinnamen
- In plaats van dat iedere machine alle adressen kent, kon je adressen individueel opvragen
- 'Wat is het adres van www.sidn.nl?'
  - **Authoritative servers** kennen deze informatie
  - **DNS Resolvers** weten hoe je deze informatie kunt opzoeken

Dit is in 1986 de standaard geworden,

en deze gebruiken we nog steeds

SIDN LABS

Top-level domains

- Domeinnamen zijn verdeeld over 'top-level' domains

- Country code top-level domains
  - .nl, .be, .au, etc.
- Generic top-level domains
  - .com, .org, .net, .amsterdam, etc.
- Deze worden beheerd door organisaties zoals SIDN
  - SIDN doet .nl
  - Verisign doet .com
  - Afilias doet .org

Second-level domains

- Dit is meestal waar je aan denkt als je zegt 'een domeinnaam'
  - nu.nl
  - sidn.nl
  - cnn.com
  - instagram.com
  - Etc.

DNS in Nederland

- In 1986 heeft Piet Beertema (CWI) '.nl' aangevraagd
- Het eerste country-code top-level domain!
- De eerste nederlandse domeinnaam was cwi.nl
- In 1996 is SIDN opgericht om het beheer over te nemen

Website van Piet met deze geschiedenis:

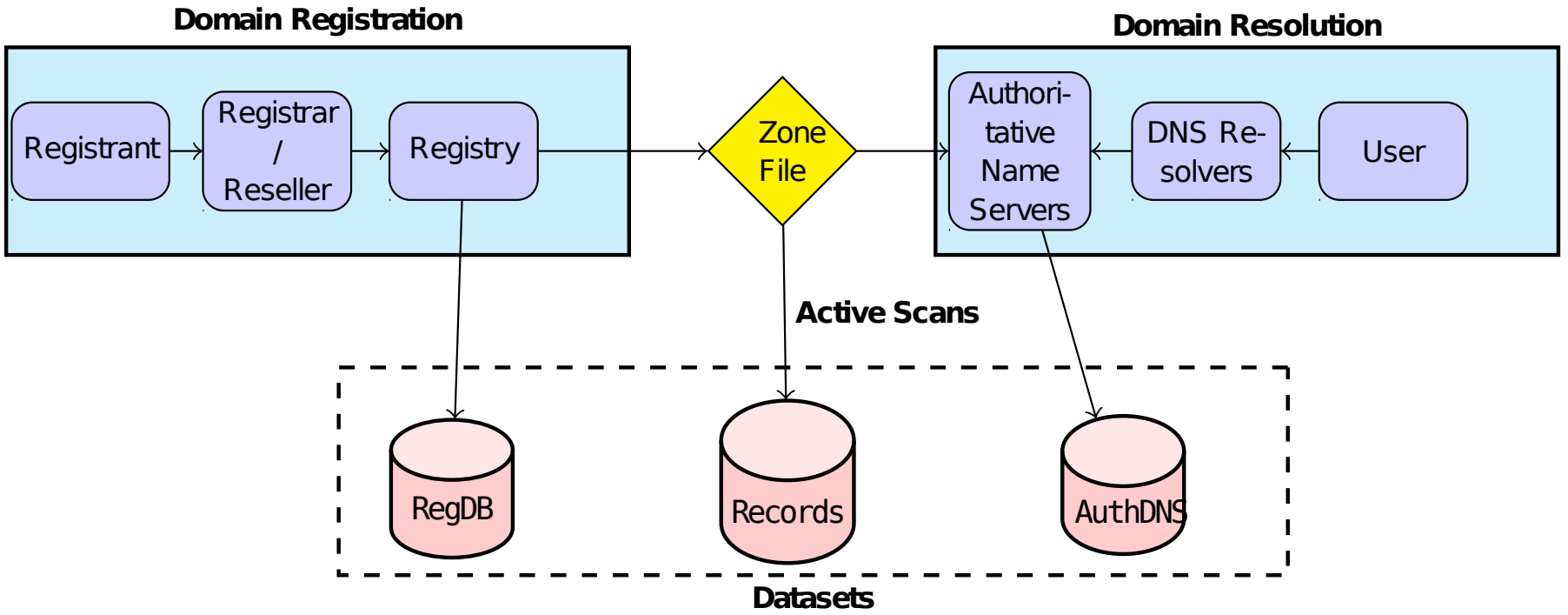
https://godfatherof.nl/

DNS vandaag de dag

- Inmiddels meer dan 300 miljoen 'domeinnamen'
- Met adressen van meer dan een miljard computers
- Verdeeld over meer dan 250 'top-level domains'

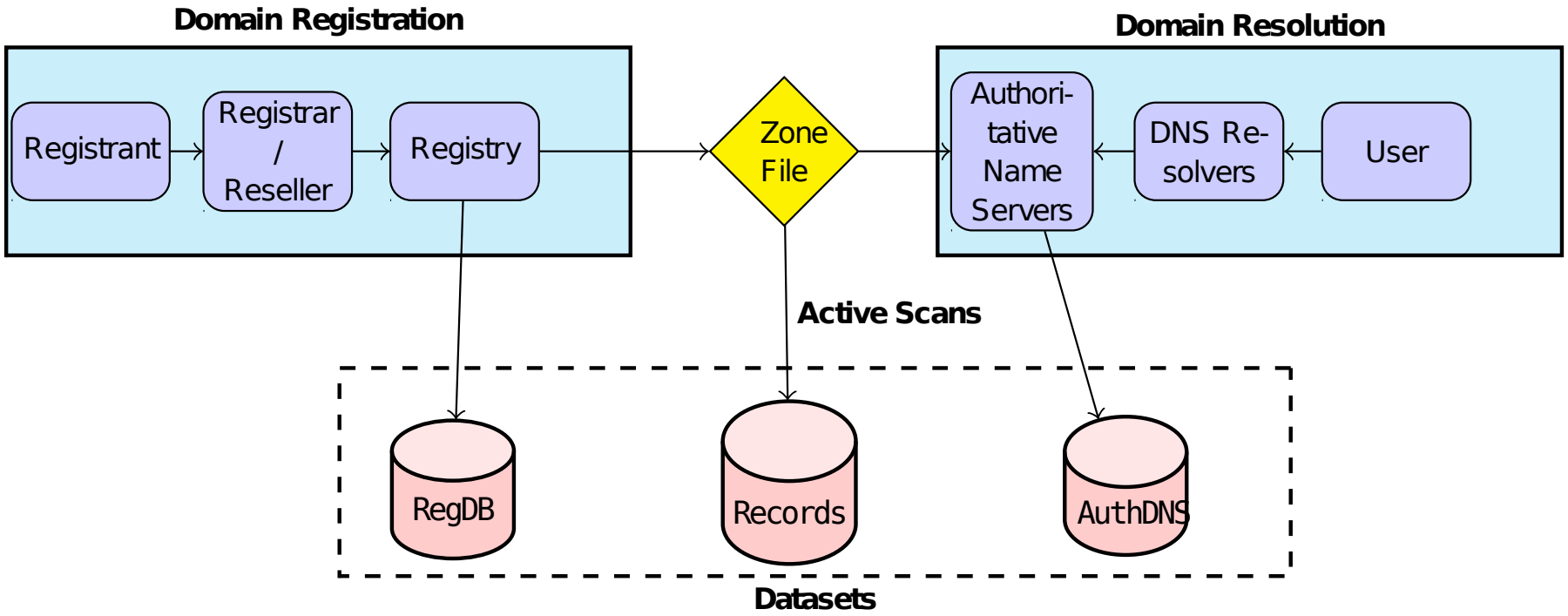
Domeinnamen registreren

- Om monopolies te voorkomen bieden de meeste TLD's domeinnamen niet rechststreeks aan
- Registratie gaat via registrars: bedrijven die met alle TLD's contracten hebben



Domeinnamen registreren

- **Registrant**: de bezitter van een domeinnaam
- **Registrar**: bedrijf dat domeinnamen registreert
- **Registry**: organisatie die registraties bijhoudt



DNS: Het opzoeken van een domeinnaam

Domeinnamen

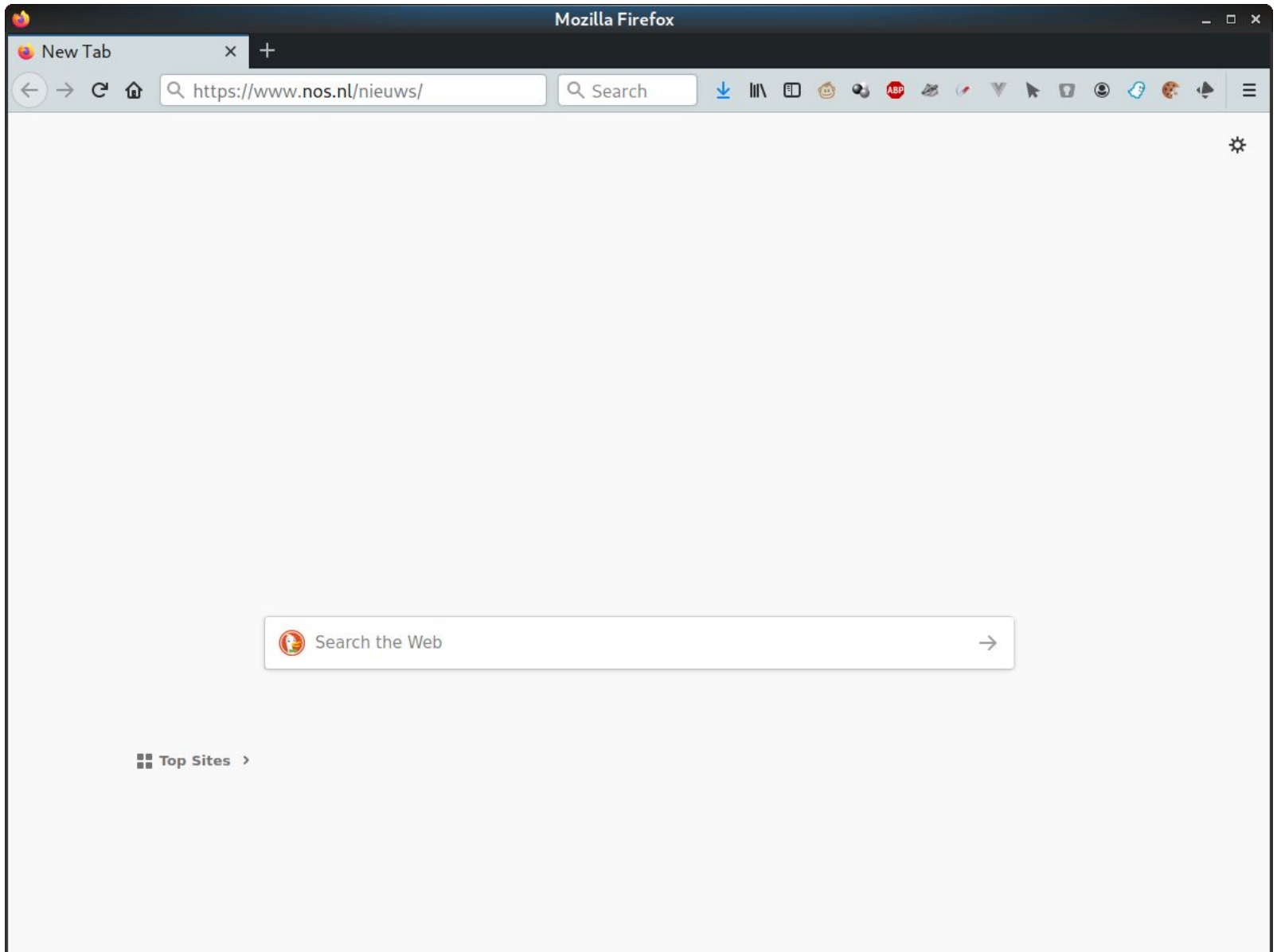
Mensen denken in domeinnamen

Computers denken in IP-adressen

Het proces om adhv een domeinnaam een ip-adres op te zoeken heet 'DNS resolution'

(je 'resolvet' een domeinnaam)

DNS Resolution in 1 minuut

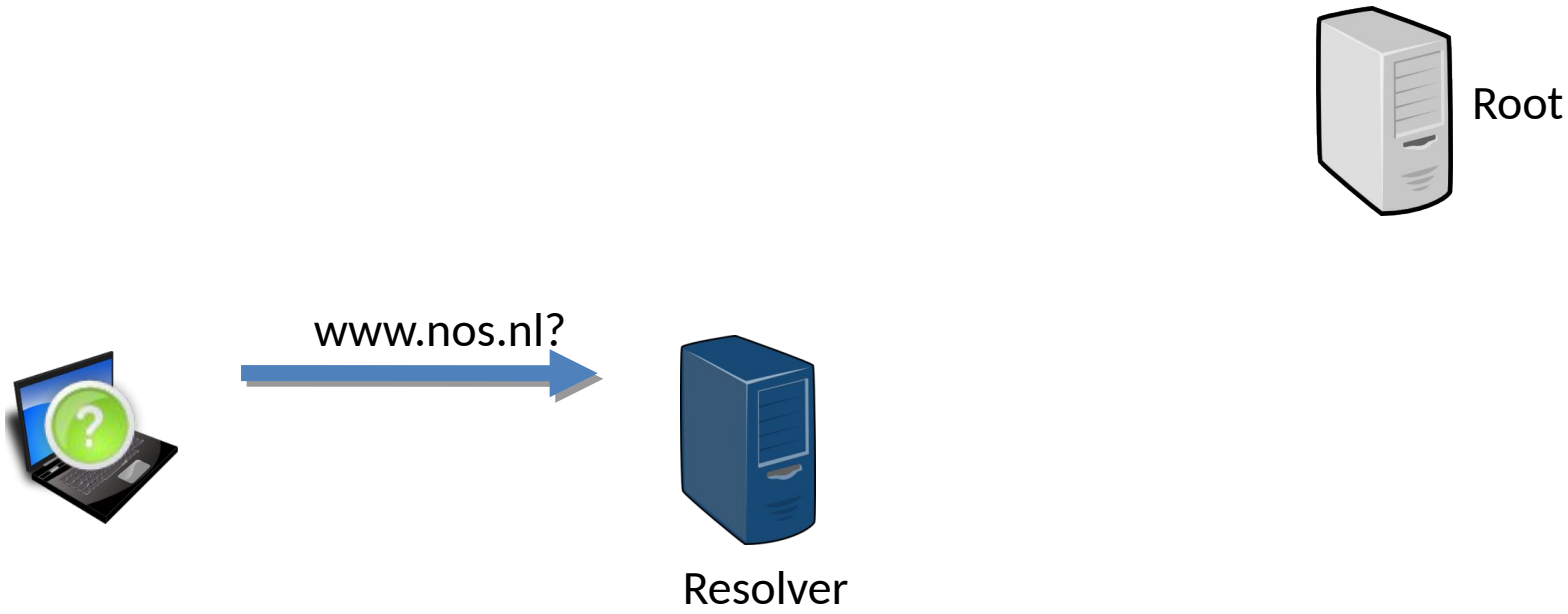

Mozilla Firefox
New Tab
https://www.nos.nl/nieuws/
Search
Search the Web
Top Sites

DNS Resolution in 1 minuut

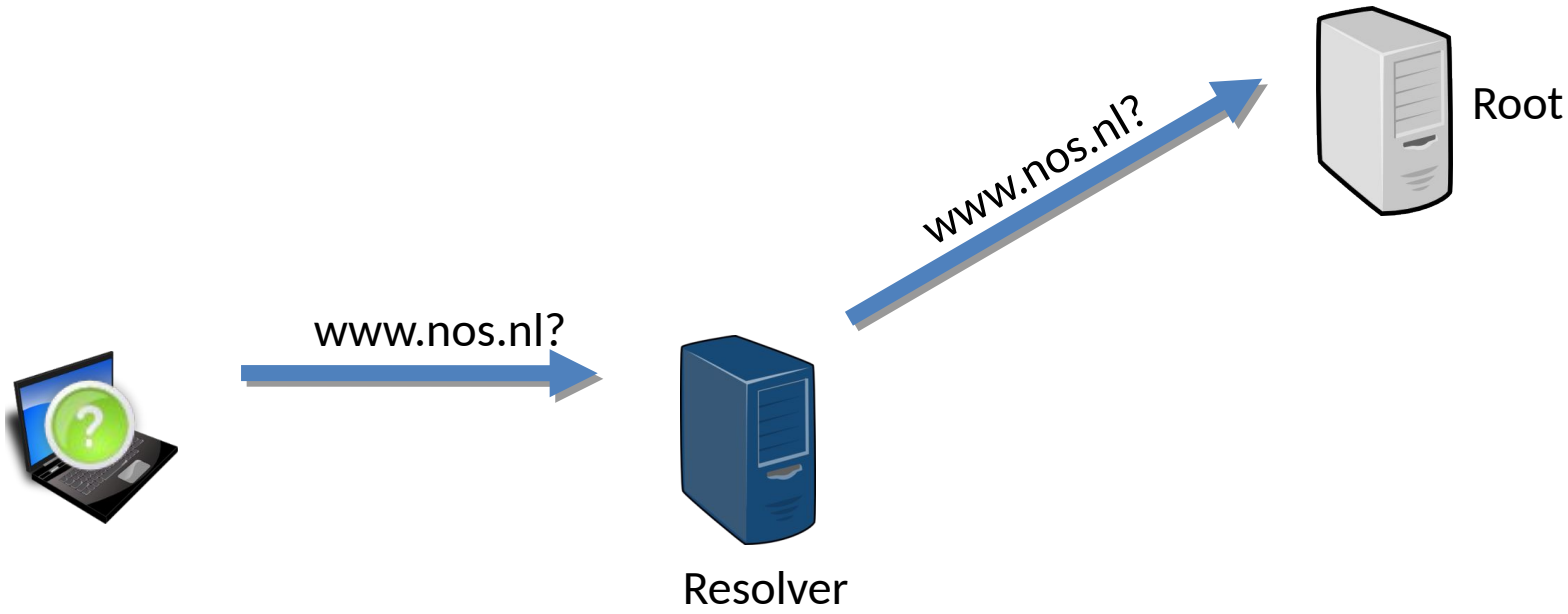
Resolver

DNS Resolution in 1 minuut

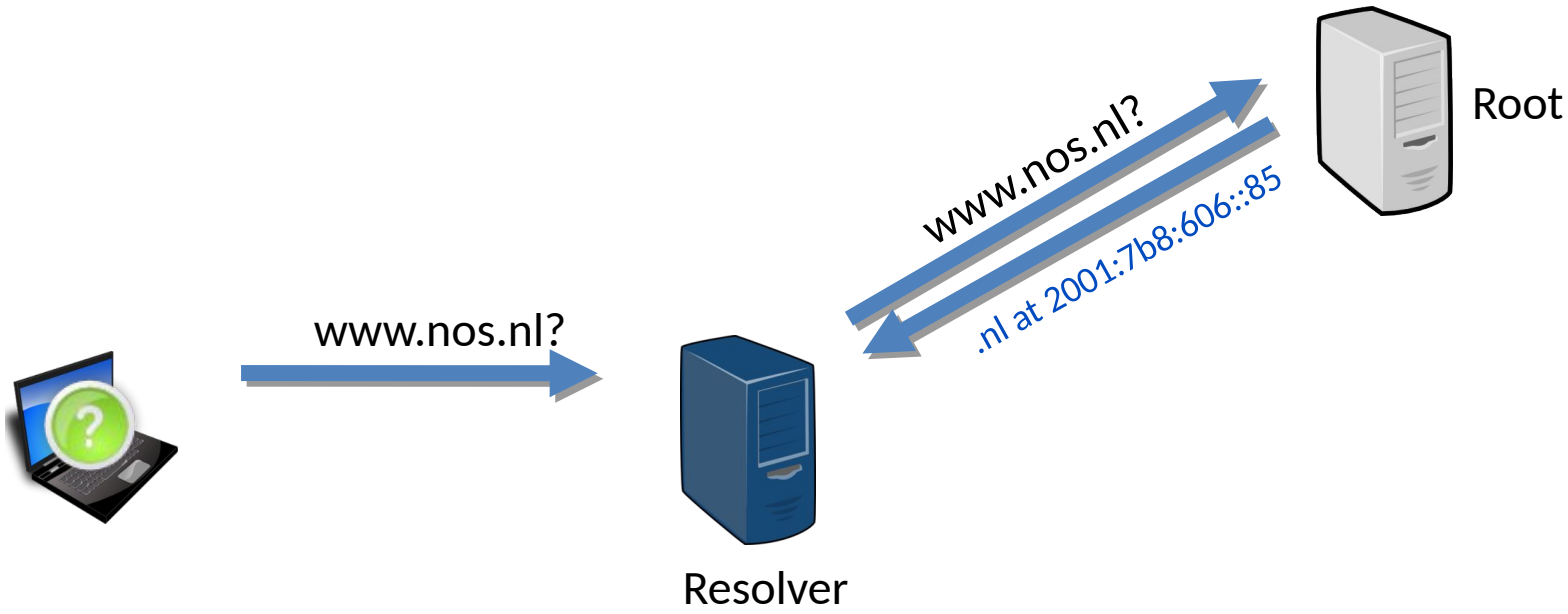
DNS Resolution in 1 minuut



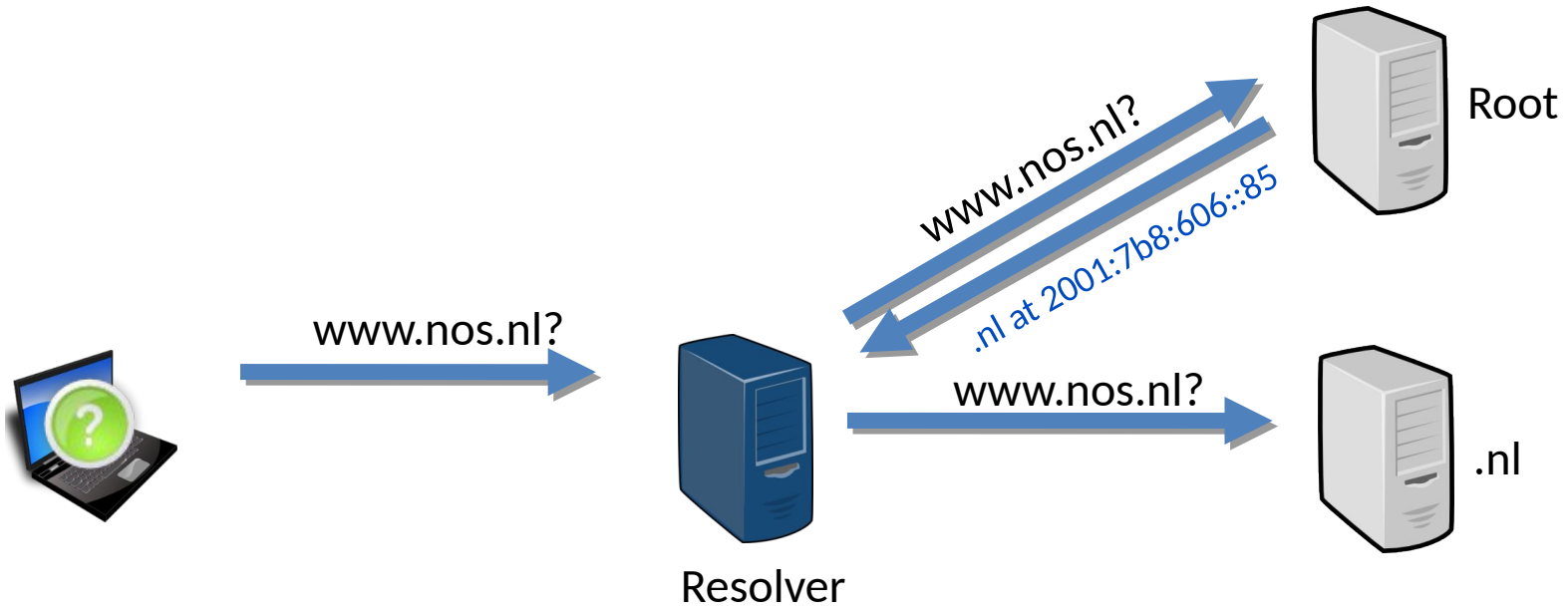
DNS Resolution in 1 minuut



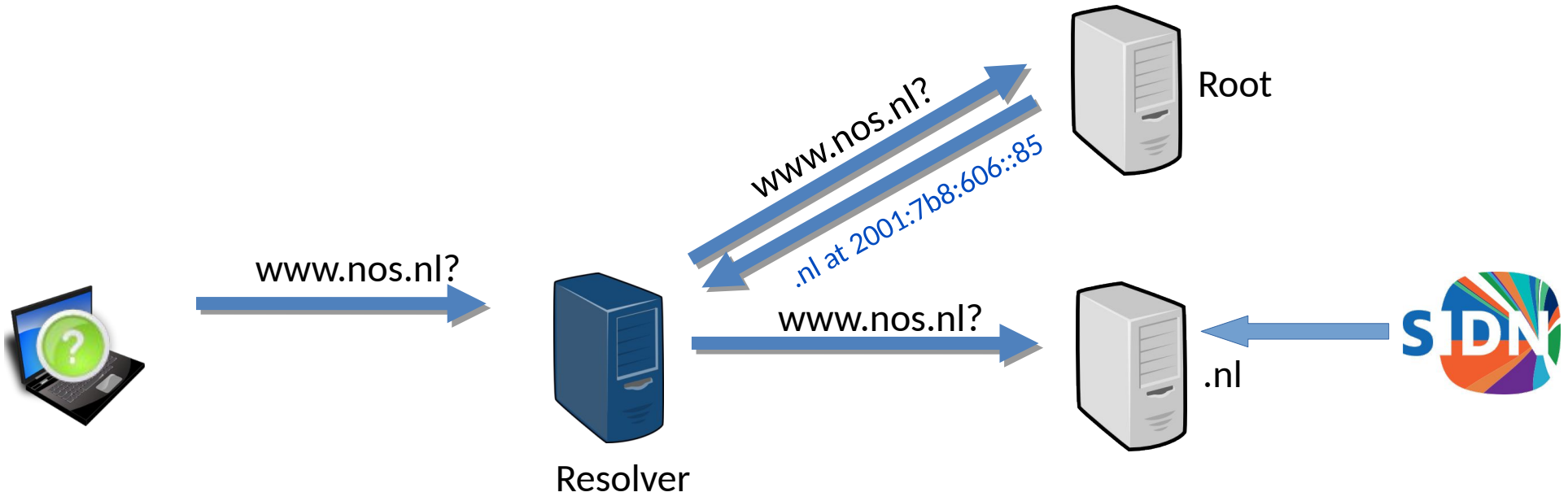
DNS Resolution in 1 minuut



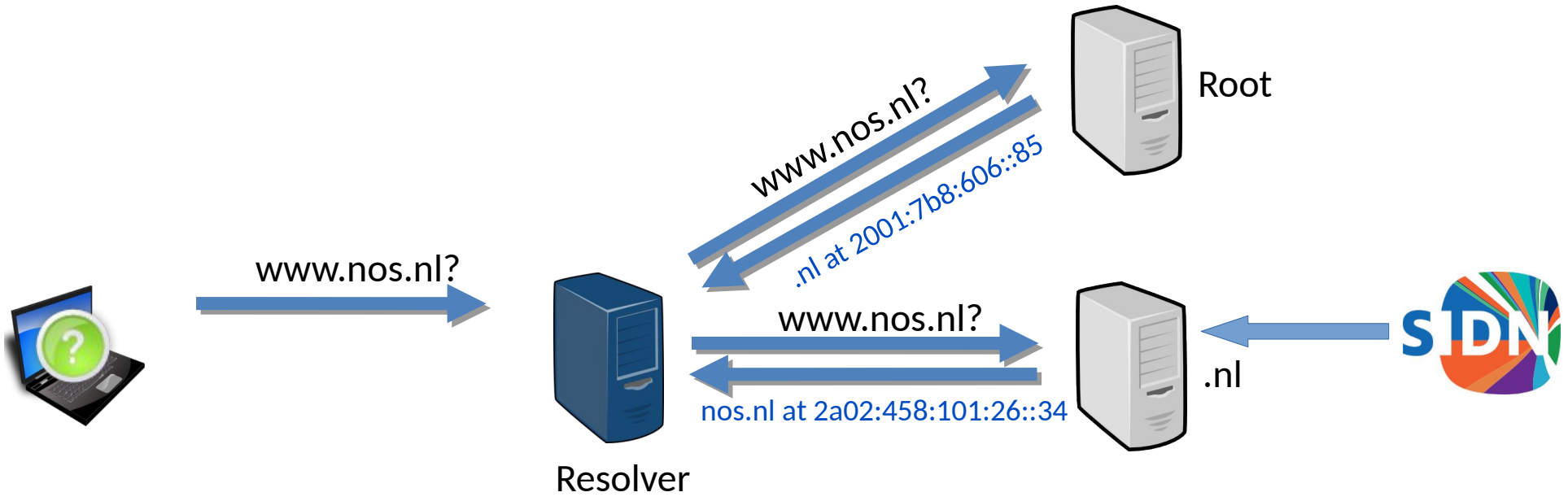
DNS Resolution in 1 minuut



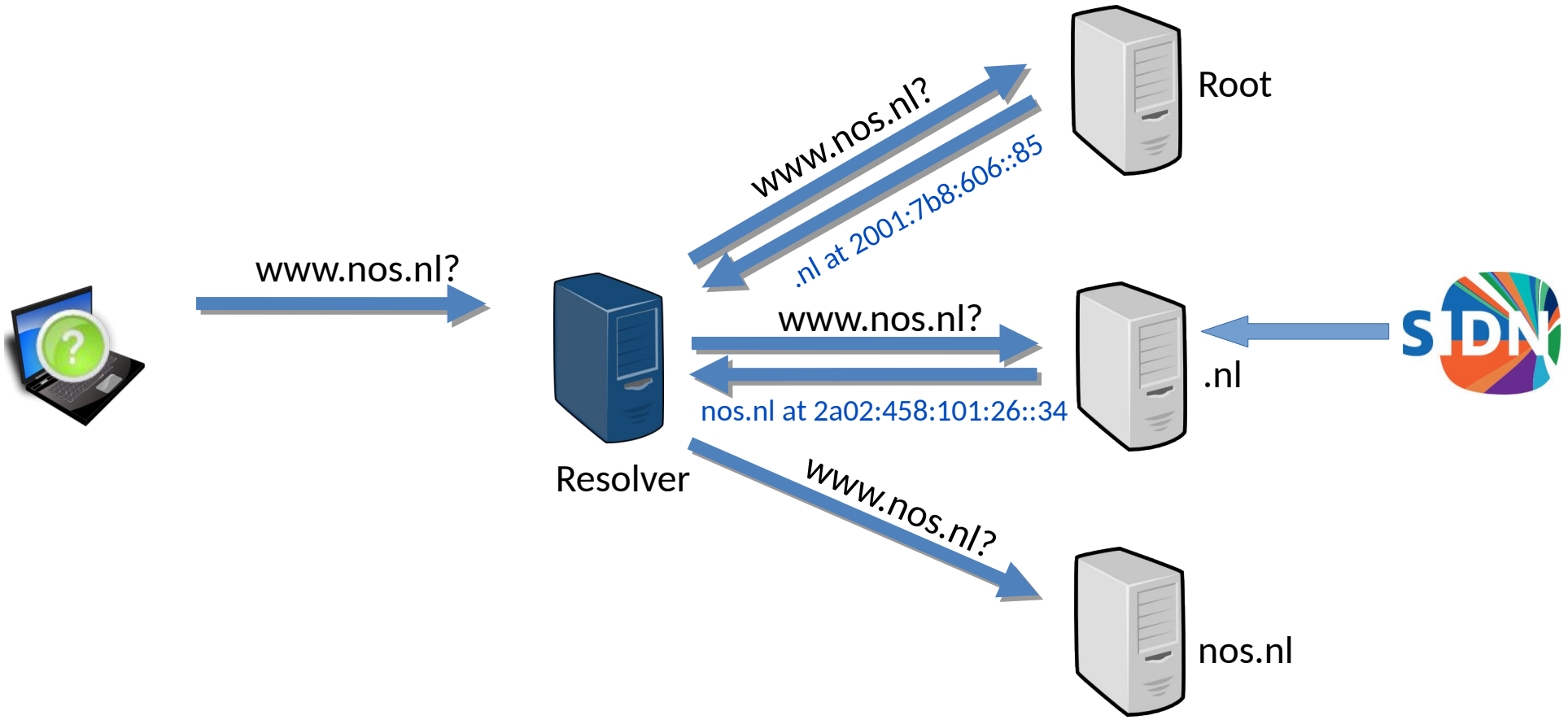
DNS Resolution in 1 minuut



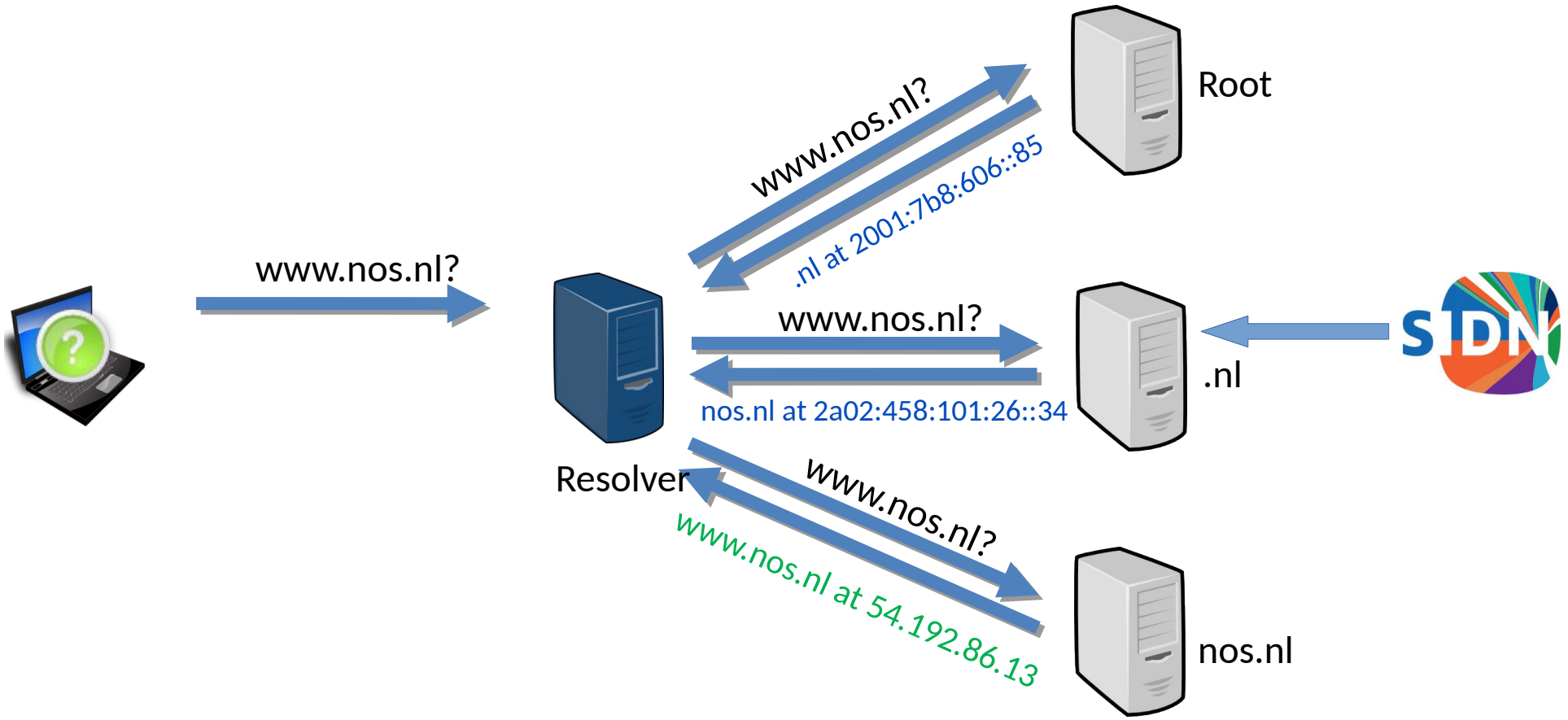
DNS Resolution in 1 minuut



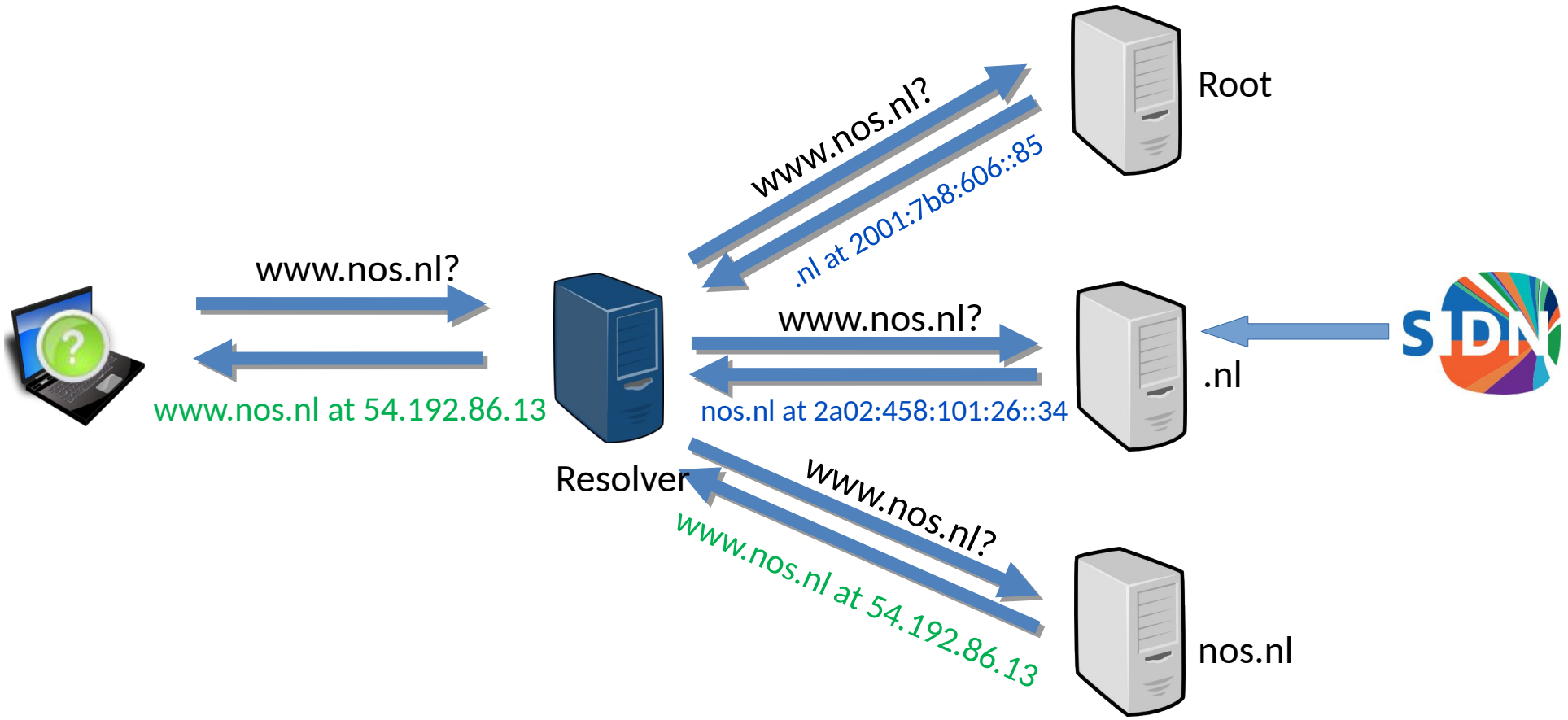
DNS Resolution in 1 minuut

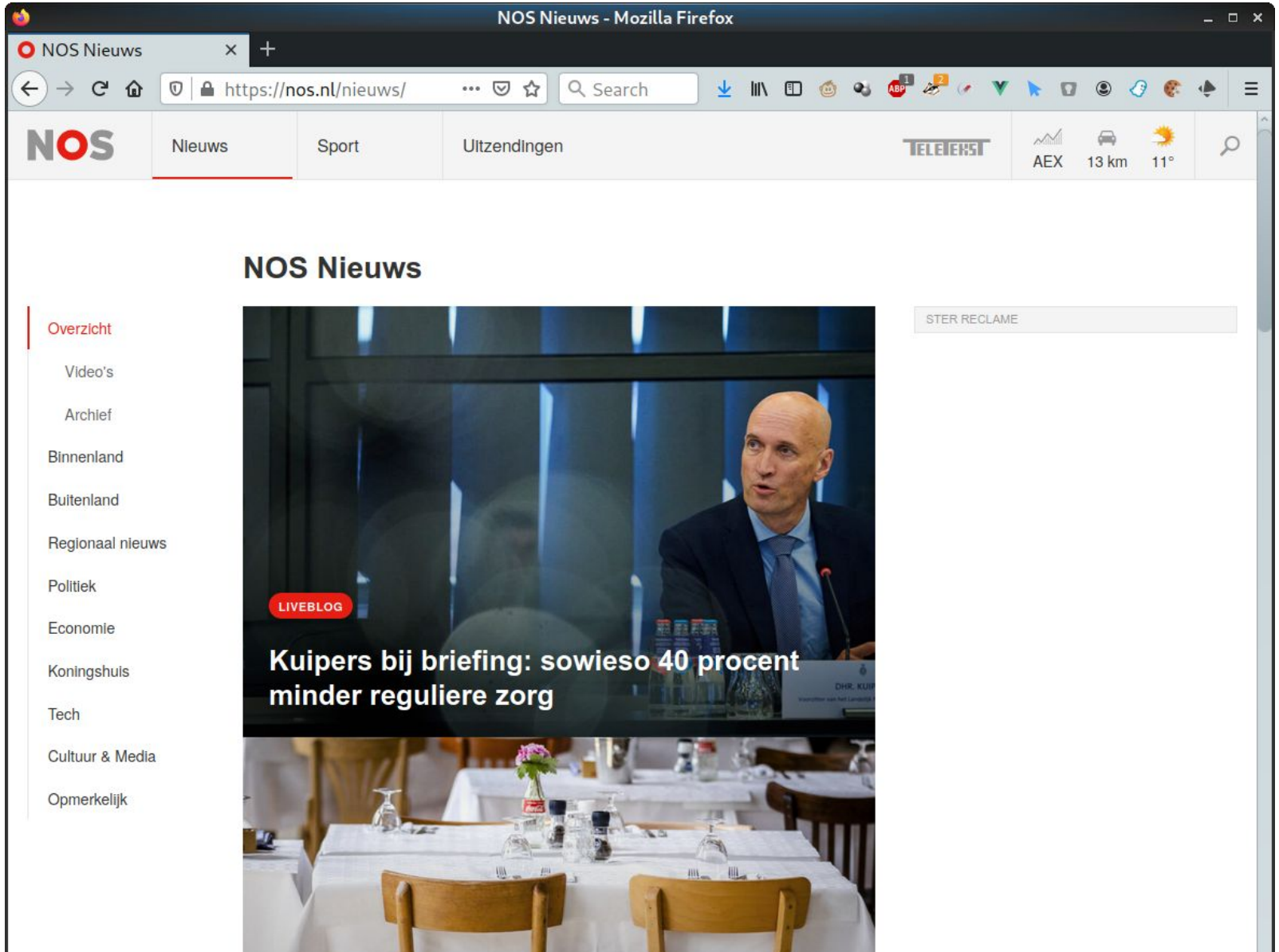


DNS Resolution in 1 minuut

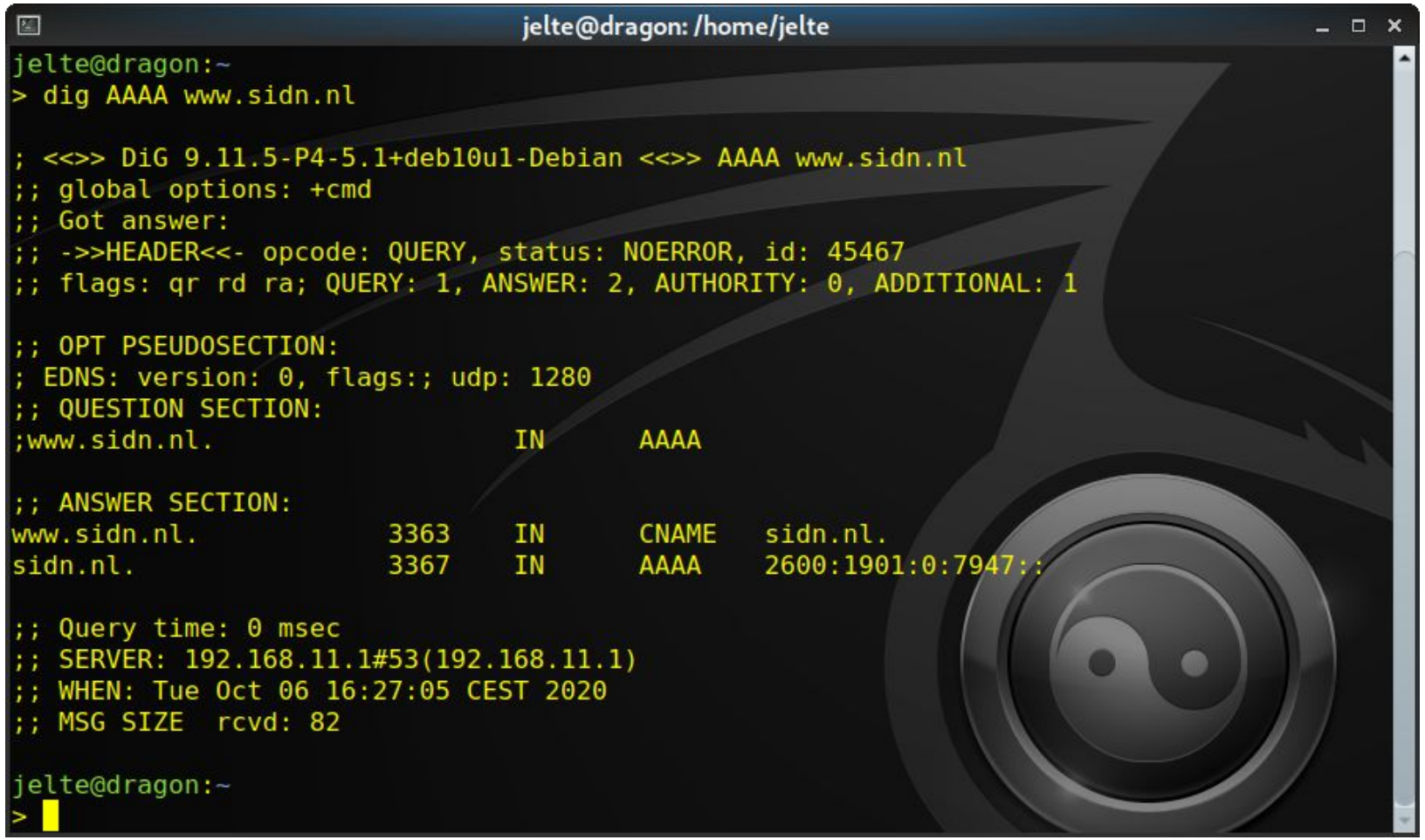


DNS Resolution in 1 minuut

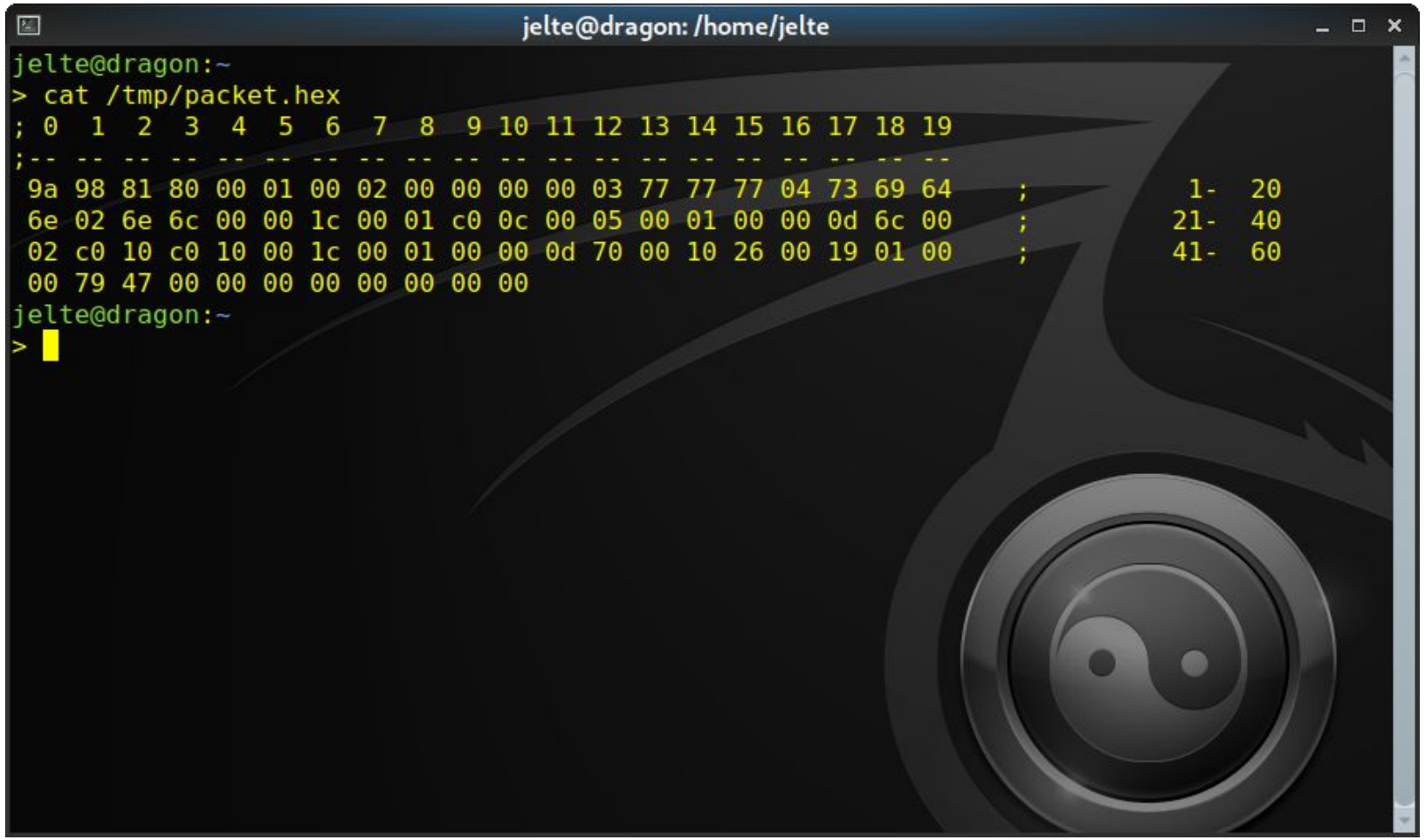



NOS Nieuws - Mozilla Firefox
NOS Nieuws
https://nos.nl/nieuws/
Search
NOS
Nieuws
Sport
Uitzendingen
TELETEKST
AEX
13 km
11°
NOS Nieuws
Overzicht
Video's
Archief
Binnenland
Buitenland
Regionaal nieuws
Politiek
Economie
Koningshuis
Tech
Cultuur & Media
Opmerkelijk
LIVEBLOG
Kuipers bij briefing: sowieso 40 procent minder reguliere zorg
STER RECLAME

Een DNS pakketje (tekst)



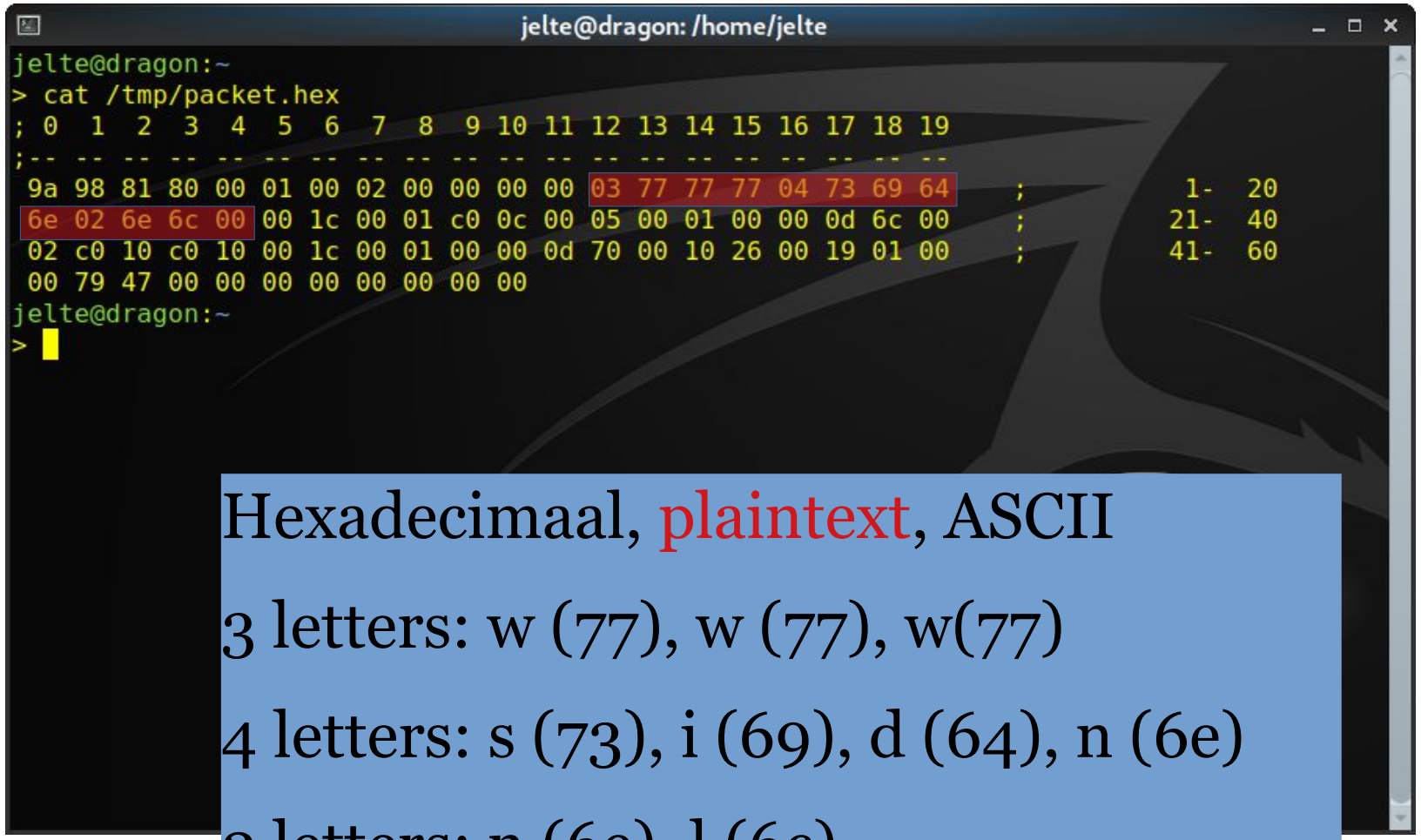
Een DNS pakketje (hexadecimaal)



Een DNS pakketje (hexadecimaal)

Een DNS pakketje (hexadecimaal)

Een DNS pakketje (hexadecimaal)



Hexadecimaal, plaintext, ASCII

3 letters: w (77), w (77), w(77)

4 letters: s (73), i (69), d (64), n (6e)

2 letters: n (6e), l (6c)

0 letters (einde van de domeinnaam)

DNS is meer!

Adressen zijn maar 1 soort informatie

In DNS staan ook dingen voor:

- E-mail en e-mailbeveiliging
- Websitebeveiliging
- Informatie over services zoals internetbellen
- Geografische informatie
- enzovoorts

DNS is overal

- Web
- E-mail
- Games
- On-demand televisie
- On-demand muziek
- Internetbellen
- Netwerkconfiguratie, firewalls

En veel, veel meer. Als het via Internet werkt, kun je ervan uit gaan dat het DNS gebruikt.

DNS is overal

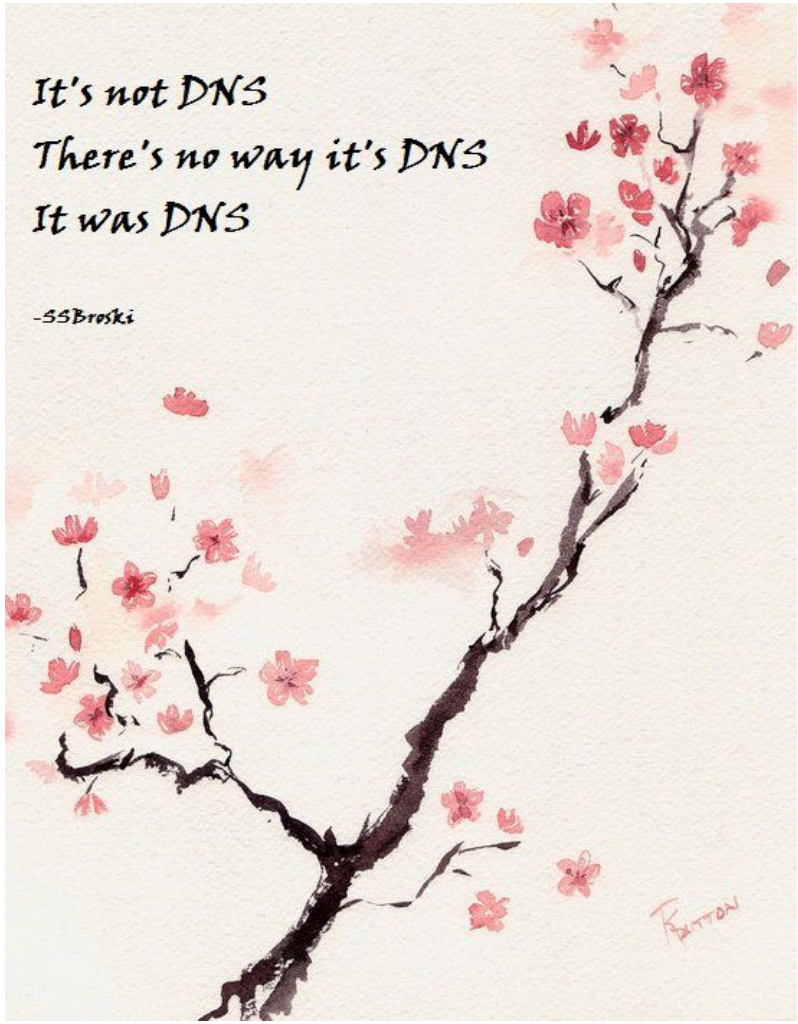
- Web
- E-mail
- Games
- On-demand televis
- On-demand muzie
- Internetbellen
- Netwerkconfigurat

En veel, veel meer. A
DNS gebruikt.

DNS is overal

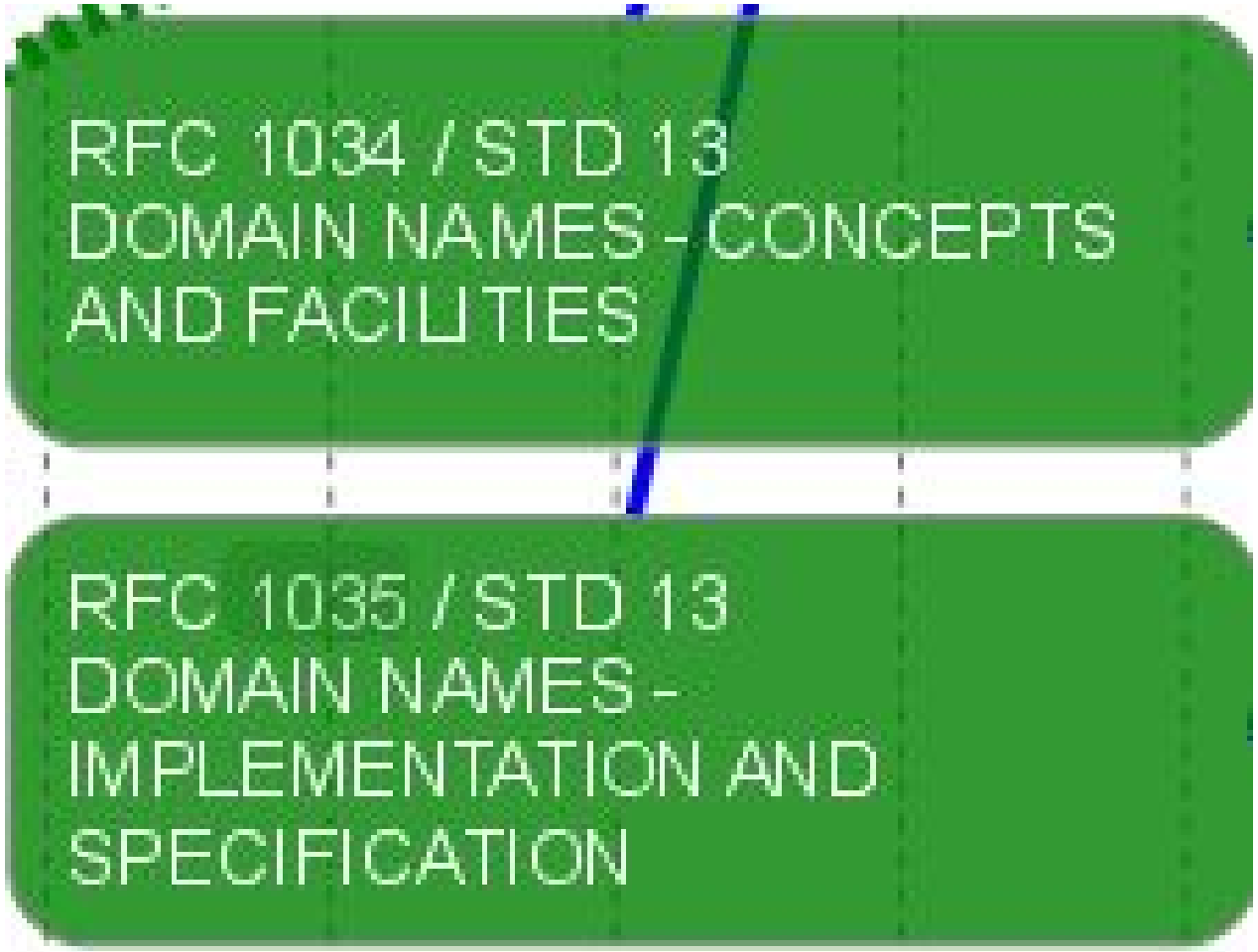
- Als het stuk gaat…
- Dan is 'alles' stuk.

'Internet doet het niet'

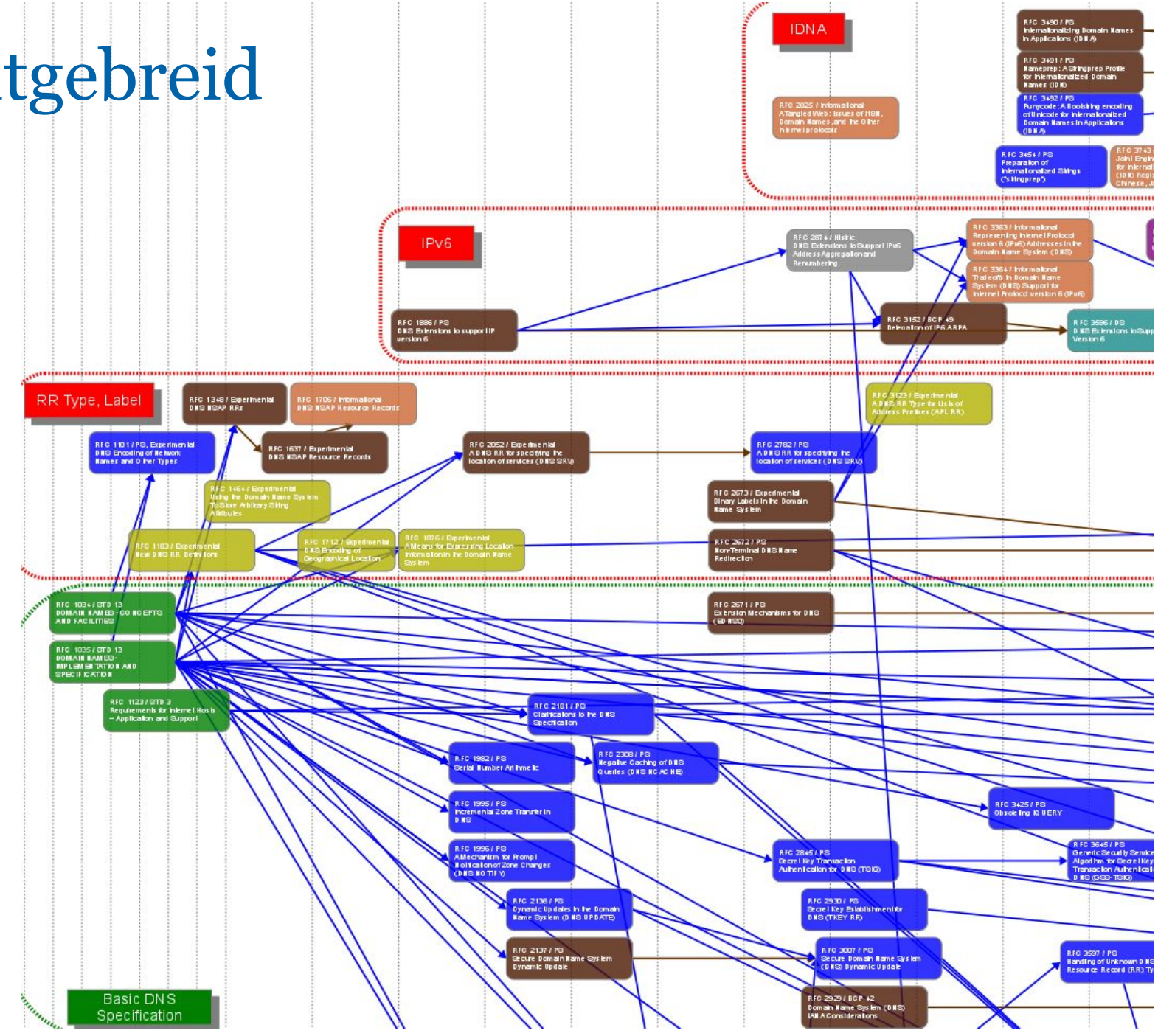


DNS is oud

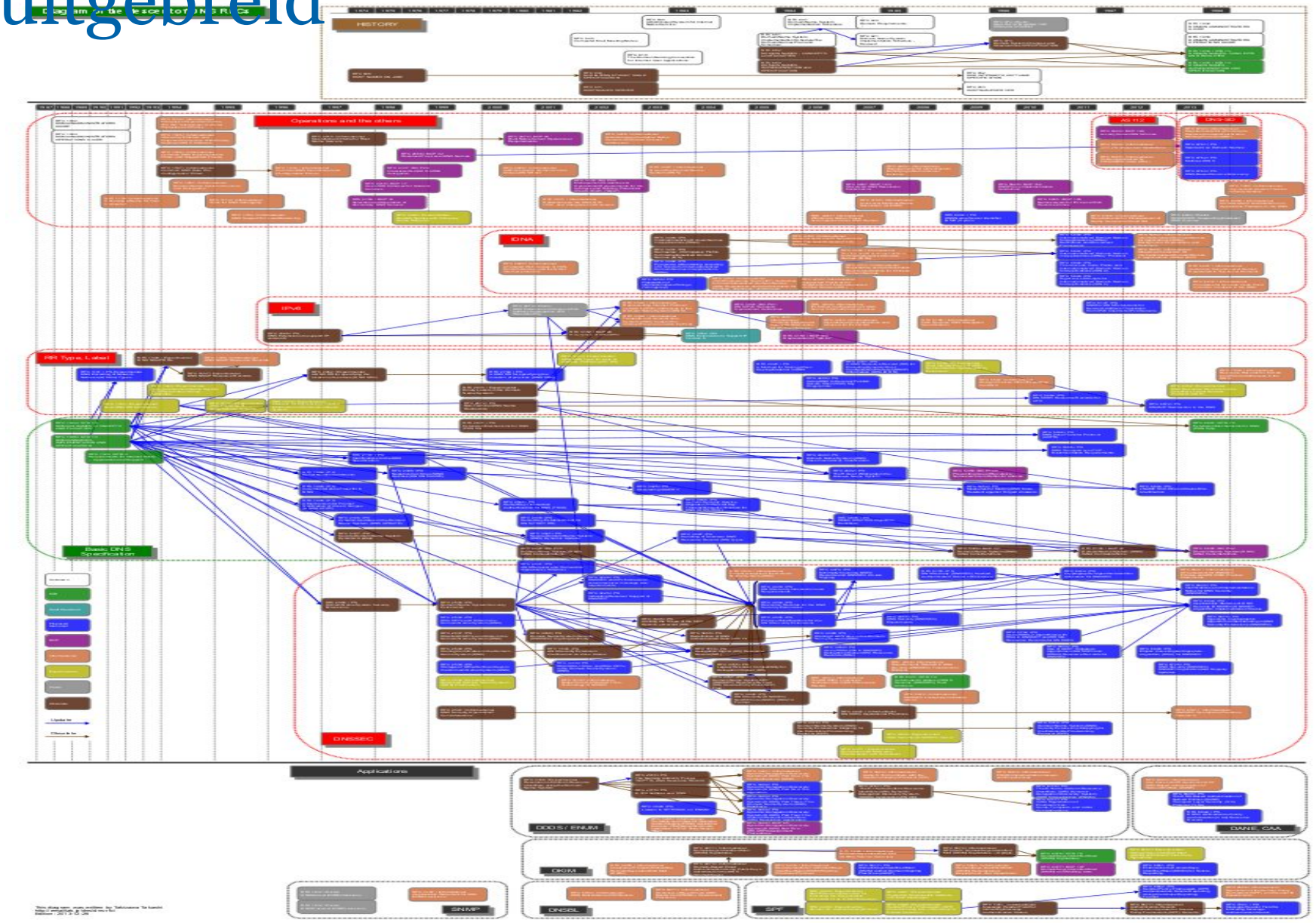
- Gedefinieerd in RFC1034 / RFC 1035 (1987)
- Samen 108 pagina's



DNS is uitgebreid



DNS is uitgebreid



DNS is schaalbaar

- Meer dan 300 miljoen second-level domains
- Verdeeld over 'delegation points' (root, top-level, second-level, etc)
- Iedereen met een eigen domeinnaam kan in principe zijn of haar eigen server gebruiken
- Antwoorden kunnen tijdelijk onthouden worden, zodat ze niet voor iedereen telkens opnieuw opgevraagd hoeven worden

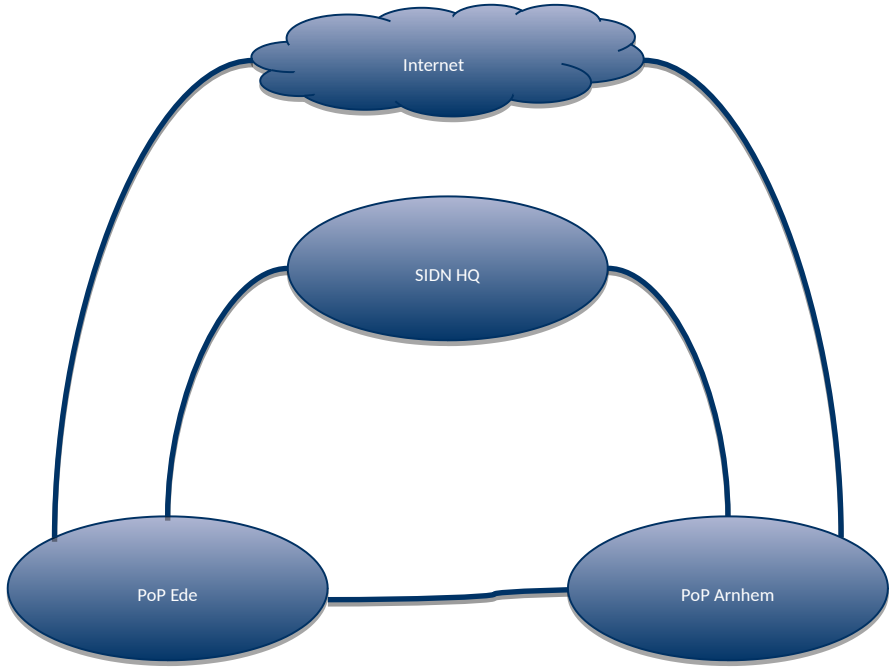
SIDN LABS

DNS bij SIDN

- 6 miljoen domeinnamen
- >2 miljard query's per dag

Onze servers:

- Database op twee datacenters
- Automatische failover



- DNS servers verdeeld over 3 groepen
- Een in eigen beheer, twee door andere organisaties
- In totaal tientallen servers overal op aarde

Aanvallen op DNS

En wat we ertegen (kunnen) doen

SIDN LABS

Aanvallen op DNS: Spoofing

- Spoofing: Het vervalsen van het afzenderadres
  - In plaats van je eigen adres te gebruiken, gebruik je dat van een ander
  - Dit is (bij aankomst) niet te herkennen!

Aanval op DNS: Cache poisoning

Met zo'n 'nep-antwoord' kun je een ander adres laten gebruiken

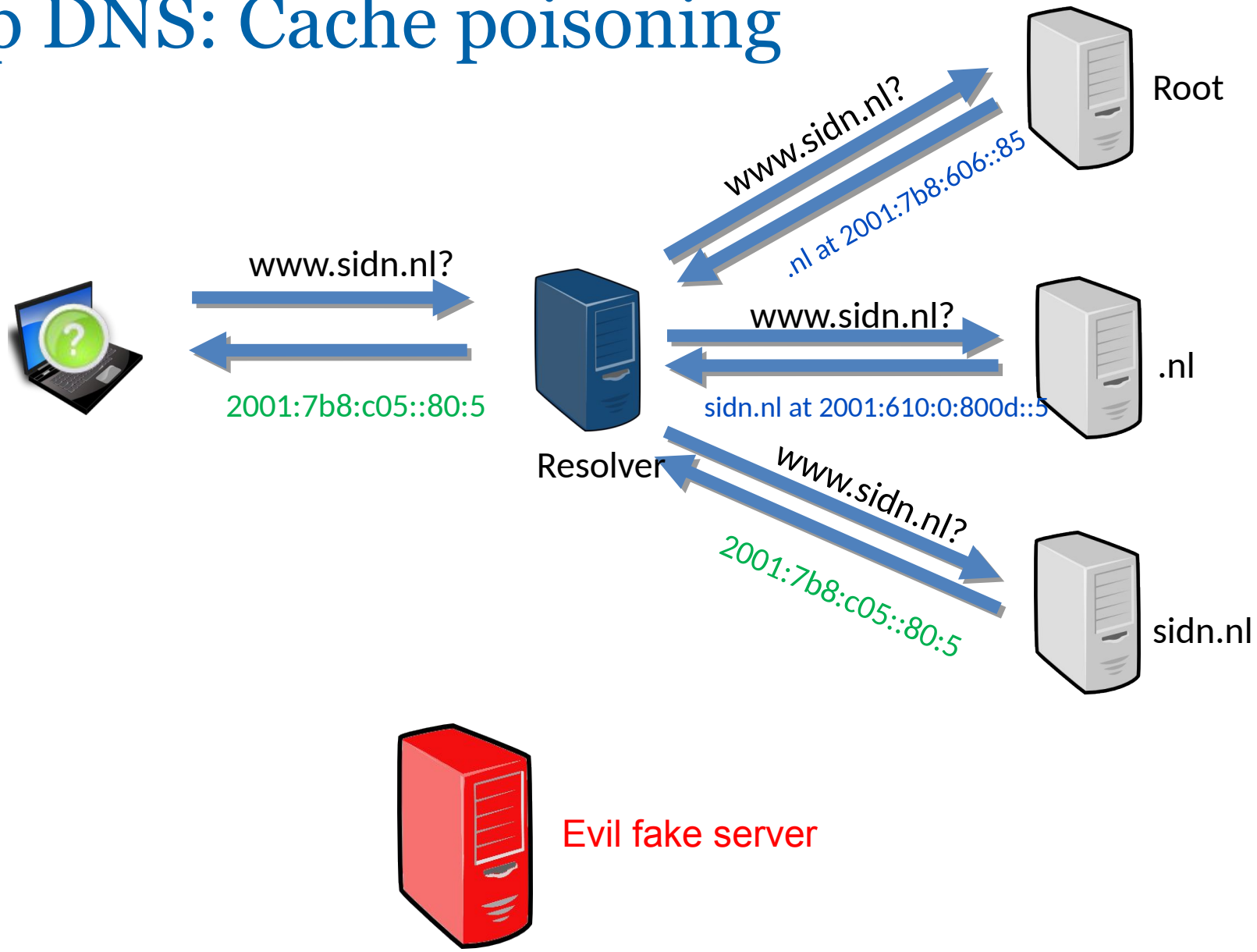
Bijvoorbeeld:

In plaats van de server van www.sidn.nl, laat je *iedereen* achter een resolver naar je eigen (kwaadaardige) server gaan.

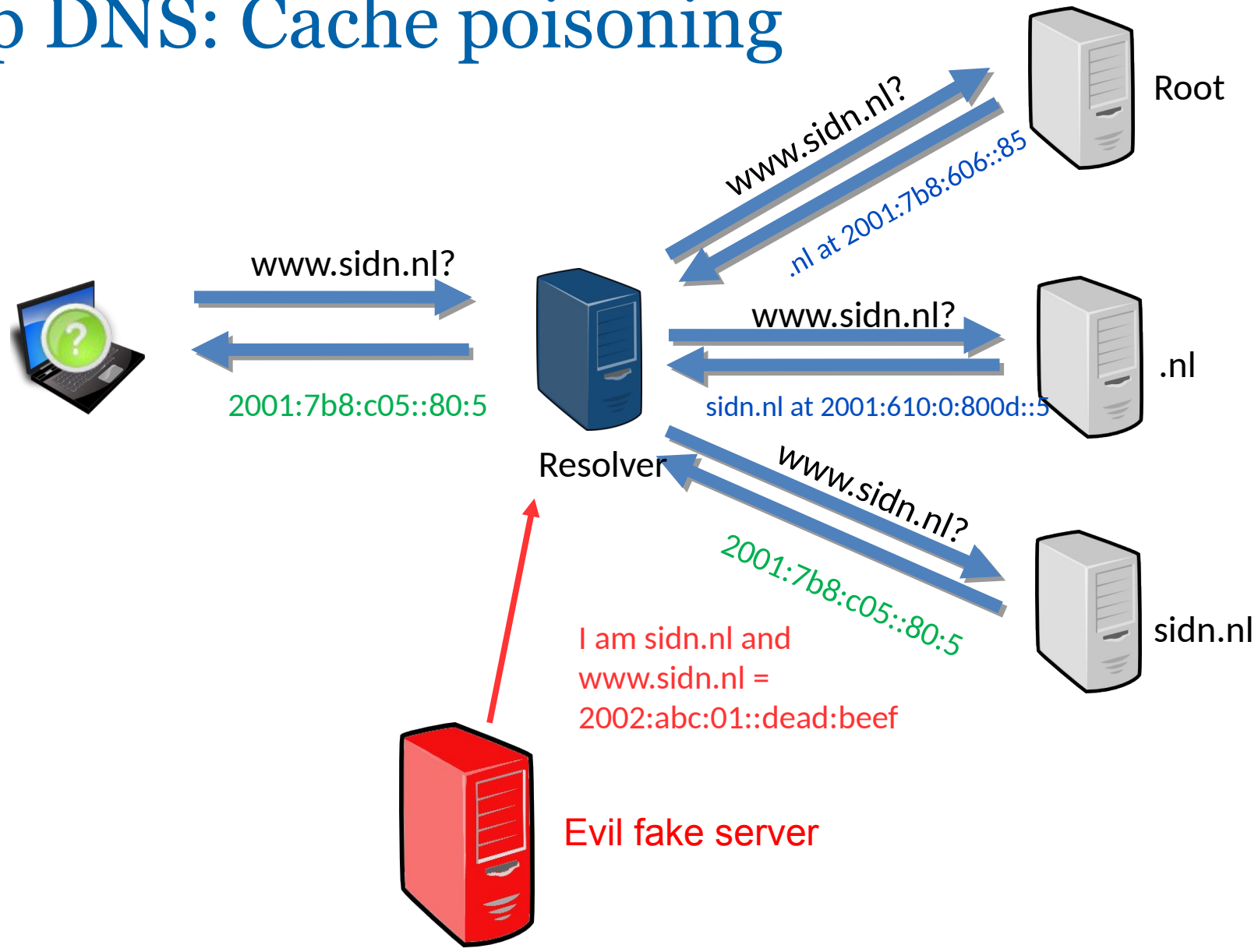
Doel: wachtwoorden stelen, valse informatie uitgeven, mensen afluisteren

SIDN LABS

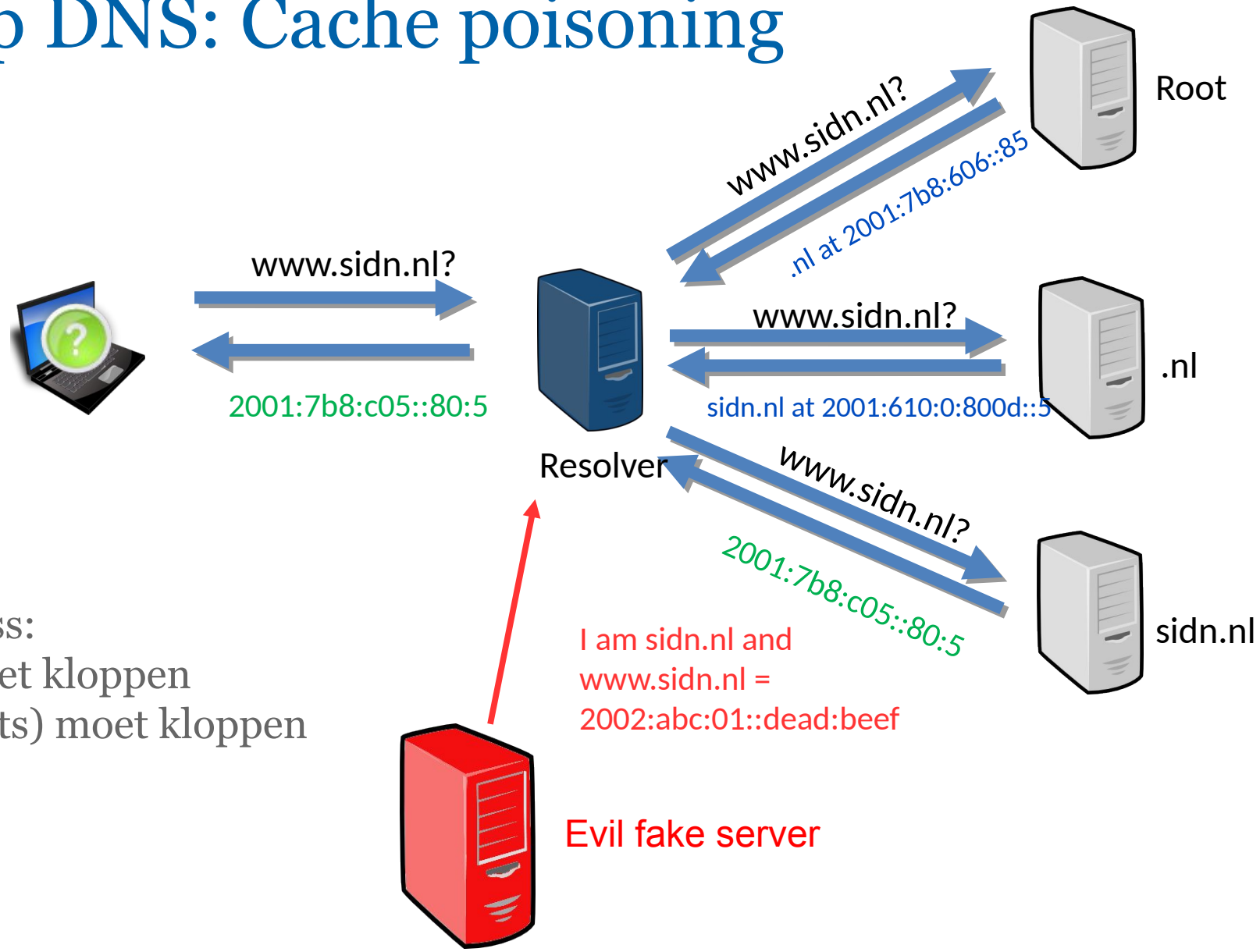
Aanval op DNS: Cache poisoning



Aanval op DNS: Cache poisoning

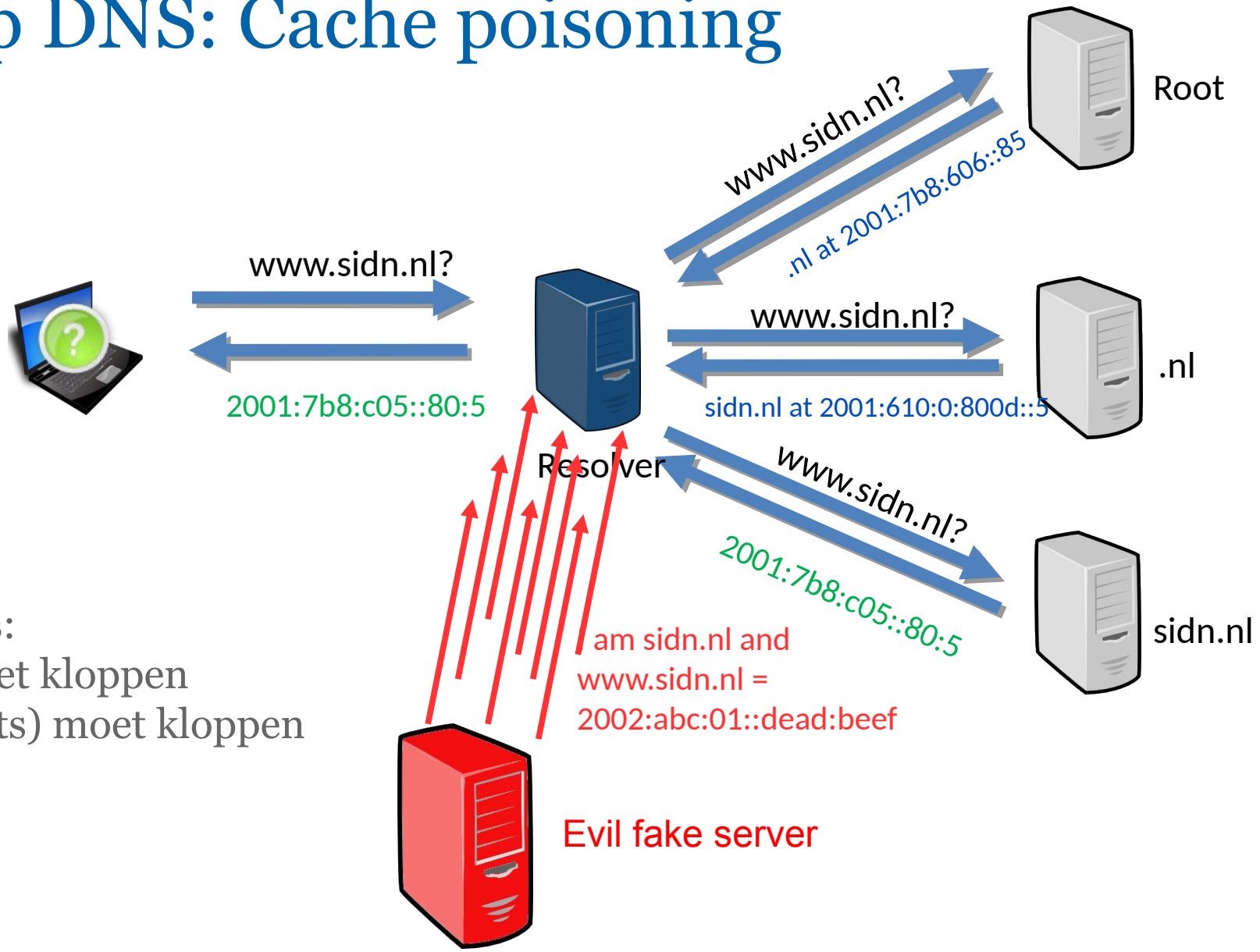


Aanval op DNS: Cache poisoning



Eisen voor success:
- qid (16 bits) moet kloppen
- UDP port (16 bits) moet kloppen

Aanval op DNS: Cache poisoning



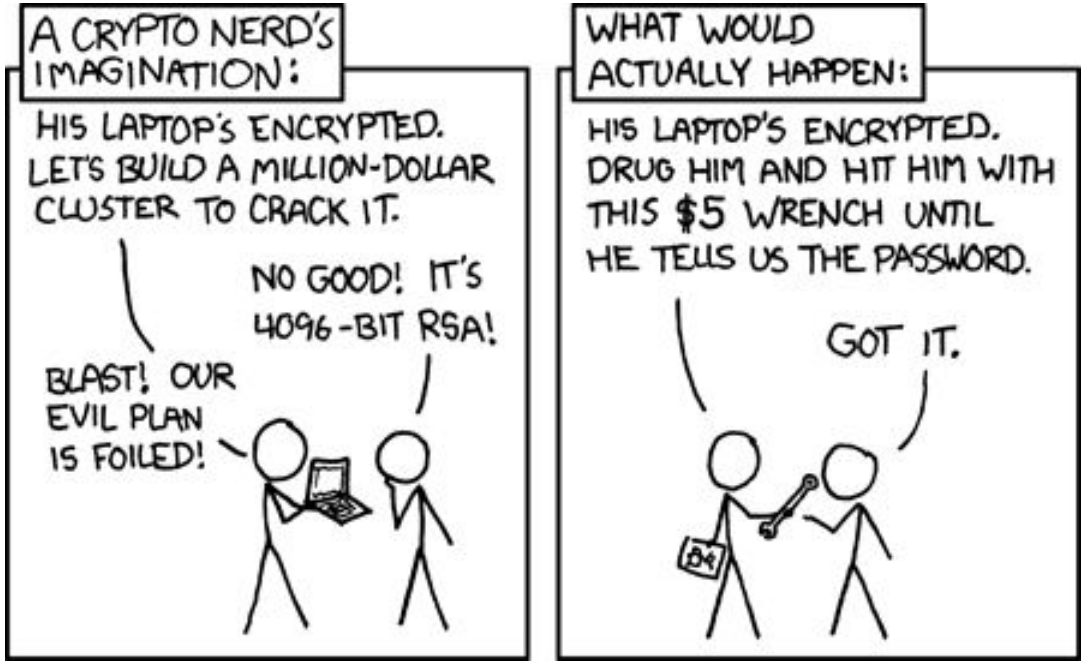
Eisen voor succes:
- qid (16 bits) moet kloppen
- UDP port (16 bits) moet kloppen

Aanval op DNS: Cache poisoning

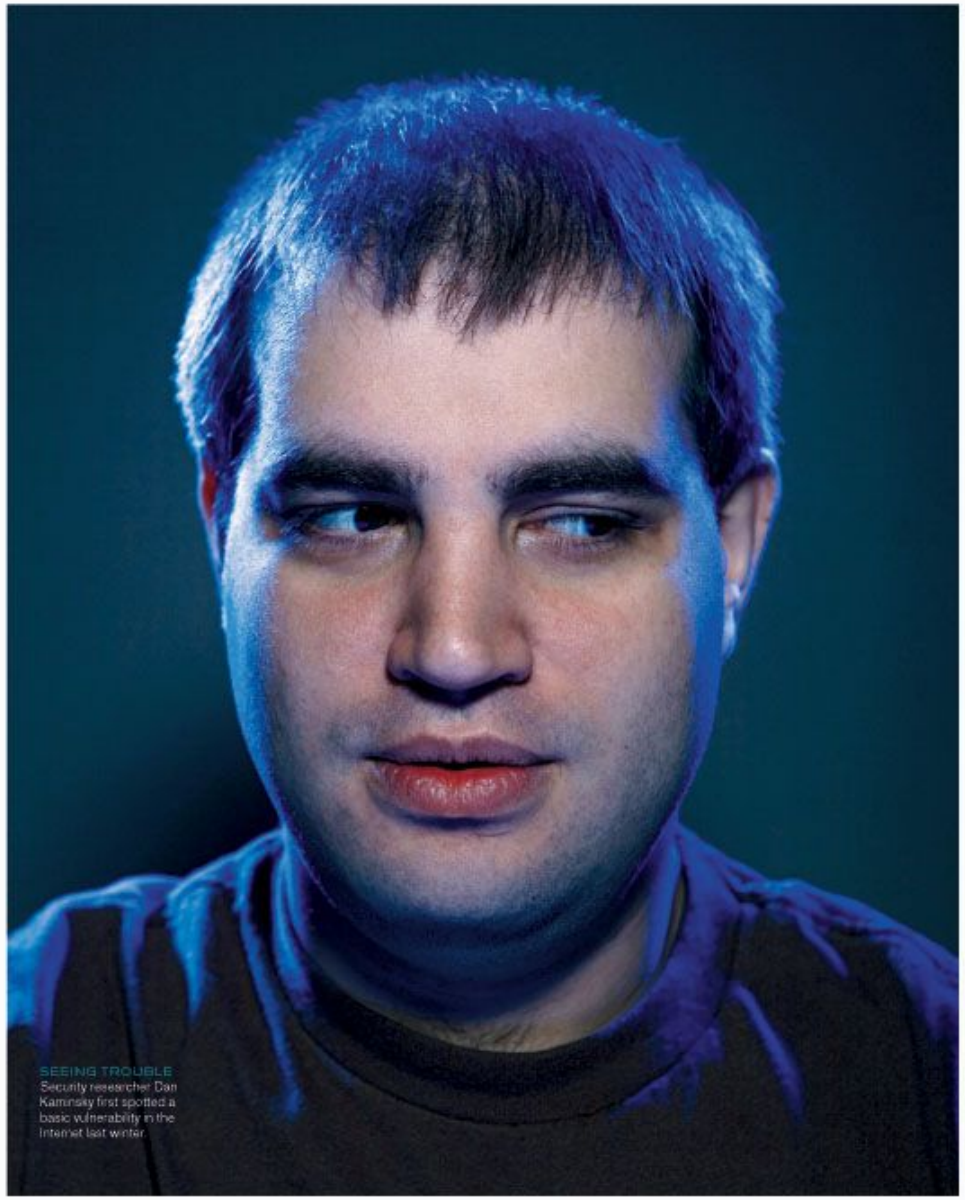
32 bits die je moet gokken! (4294967296 mogelijkheden)

“Dat gebeurt niet in de praktijk”

Want je hebt maar een paar seconden, in het meest positieve geval.



Of toch wel...



SEEING TROUBLE
Security researcher Dan Kaminsky first spotted a basic vulnerability in the Internet last winter.

The Flaw at the Heart of the Internet

DAN KAMINSKY DISCOVERED A FUNDAMENTAL SECURITY PROBLEM IN THE INTERNET AND GOT PEOPLE TO CARE IN TIME TO FIX IT. IT'S A DRAMATIC STORY WITH A HAPPY ENDING ... BUT WE WERE LUCKY THIS TIME.

By ERICA NAONE

Dan Kaminsky, uncharacteristically, was not looking for bugs earlier this year when he happened upon a flaw at the core of the Internet. The security researcher was using his knowledge of Internet infrastructure to come up with a better way to stream videos to users. Kaminsky's expertise is in the Internet's domain name system (DNS), the protocol responsible for matching websites' URLs with the numeric addresses of the servers that host them. The same content can be hosted by multiple servers with several addresses, and Kaminsky thought he had a great trick for directing users to the servers best able to handle their requests at any given moment.

Normally, DNS is reliable but not nimble. When a computer—say, a server that helps direct traffic across Comcast's network—requests the numerical address associated with a given URL, it stores the answer for a period of time known as "time to live," which can be anywhere from seconds to days. This helps to reduce the number of requests the server makes. Kaminsky's idea was to bypass the time to live, allowing the server to get a fresh answer every time it wanted to know a site's address. Consequently, traffic on Comcast's network would be sent to the optimal address at every moment, rather than to whatever address had already been stored. Kaminsky was sure that the strategy could significantly speed up content distribution.

It was only later, after talking casually about the idea with a friend, that Kaminsky realized his "trick" could completely break the security of the domain name system and, therefore, of the Internet itself. The time to live, it turns out, was at the core of DNS security; being able to bypass it allowed for a wide variety of attacks. Kaminsky wrote a little code to make sure the situation was as bad as he thought it was. "Once I saw it work, my stomach dropped," he says. "I thought, 'What the heck am I going to do about this? This affects everything.'"

Kaminsky's technique could be used to direct Web surfers to any Web page an attacker chose. The most obvious use is to send people to phishing sites (websites designed to trick people into entering banking passwords and other personal information, allowing an attacker to steal their identities) or other fake versions of Web pages. But the danger is even worse: protocols such as those used to deliver e-mail or for secure communications over the Internet ultimately rely on DNS. A creative attacker could use Kaminsky's technique to intercept sensitive e-mail, or to create forged versions of the certificates that ensure secure transactions between users and banking websites. "Every day I find another domino," Kaminsky says. "Another thing falls over if DNS is bad. ... I mean, literally, you look around and see anything that's using a network—*anything* that's using a network—and it's probably using DNS."

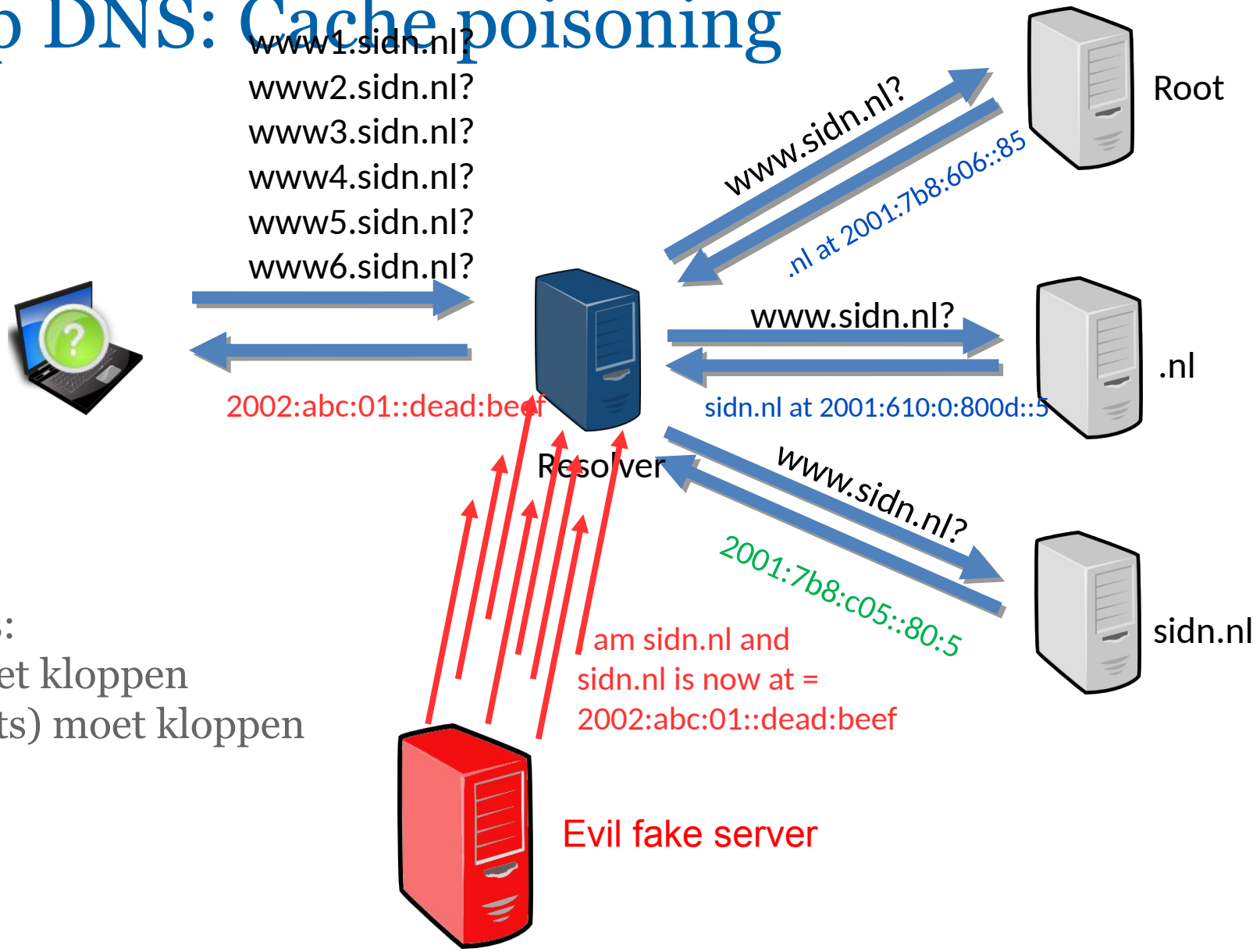
Kaminsky called Paul Vixie, president of the Internet Systems Consortium, a nonprofit corporation that supports several aspects of Internet infrastructure, including the software most commonly used in the domain name system. "Usually, if somebody wants to report a problem, you expect that it's going to take a fair amount of time for them to explain it—maybe a whiteboard, maybe a Word document or two," Vixie says. "In this case, it took 20 seconds for him to explain the problem, and another 20 seconds for him to answer my objections. After that, I said, 'Dan, I am speaking to you over an unsecure cell phone. Please do not ever say to anyone what you just said to me over an unsecure cell phone again.'"

Perhaps most frightening was that because the vulnerability was not located in any particular hardware or software but in the design of the DNS protocol itself, it wasn't clear how to fix it. In secret, Kaminsky and Vixie gathered together some of the top DNS experts in the world: people from the U.S. government and

Photograph by JOHN KEATLEY

DNS LABS

Aanval op DNS: Cache poisoning



Eisen voor succes:
- qid (16 bits) moet kloppen
- UDP port (16 bits) moet kloppen

Toch wel ja...

Security / Report Claims DNS Cache Poisoning Attack Against Brazilian Bank and ISP

Report Claims DNS Cache Poisoning Attack Against Brazilian Bank and ISP

By Larry Seltzer | Posted 2009-04-22 Email Print

OPINION: Attack shows the potential for serious spoofing attacks that could leave end
only real solution is DNSSEC, which will take years to implement under the best of circu

art
ernet
A FUNDAMEN-
HE INTERNET

Topic: Security *Follow via:*

DNS cache poisoning attacks exploited in the wild

Summary: *UPDATE: Arbor Networks have provided more details in their "30 Days of DNS*
HD Moore's statement on DNS cache poisoned AT&T
ces are starting to see evidence of DNS cache poisoning
ppears to be an attempt to take advantage of the
y :" client 143.

y | July 29, 2008 -- 03:24 GMT (04:24 BST)

HOME « NEWS « TOP SECURITY STORIES « GOOGLE'S MALAYSIAN DOMAINS HIT WITH DNS CACHE POISONING...

GOOGLE'S MALAYSIAN DOMAINS HIT WITH DNS CACHE POISONING ATTACK

DNS poisoning slams web traffic from millions in China into the wrong hole

ISP blames unspecified attack for morning outage

ys of DNS Attack Activity"
ned AT&T DNS servers. Numerous
ning attempts on their local
e "recent" DNS cache poisoning
vulnerable" if any of the results below are

Scatterplot

BS

Beveiliging: DNSSEC

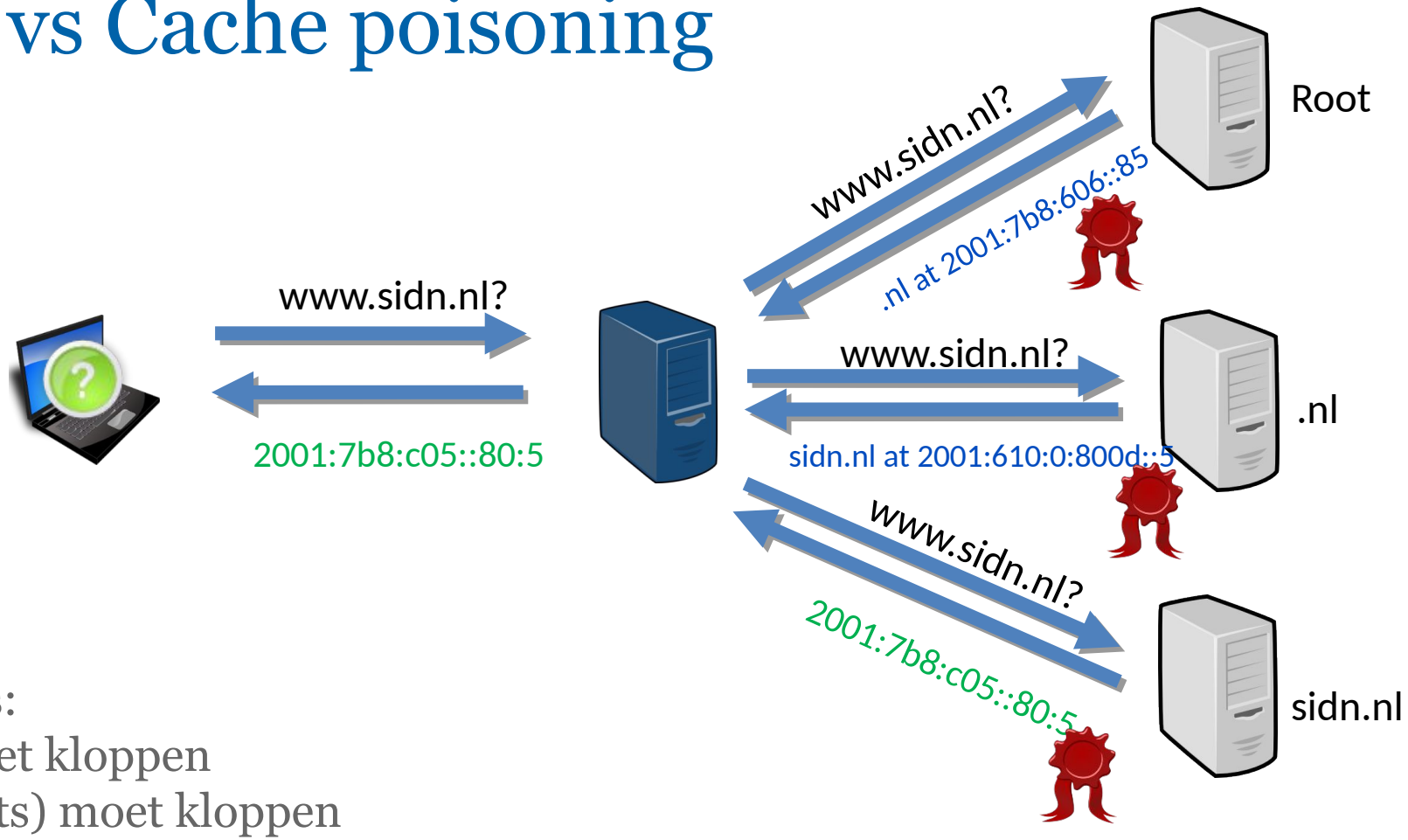
- RFC4033, 4034, 4035 (voor de kern, daarna nog een aantal met verhelderingen en uitbreidingen)
- Beschermt de data zelf; je weet zeker dat wat je terug krijgt van de beheerder van het domein komt

- Digitale handtekeningen onder alle data in een DNS antwoord
- (inclusief het antwoord “er is geen antwoord”!)

- Voordeel, beveiliging van het kanaal is niet belangrijk, je kunt zelf controleren of de data gewijzigd is.
- Kan als basis dienen voor andere beviligingsprotocollen (zoals bijv email)
- Nadelen: ingewikkeld, en DNS pakketten worden heel groot

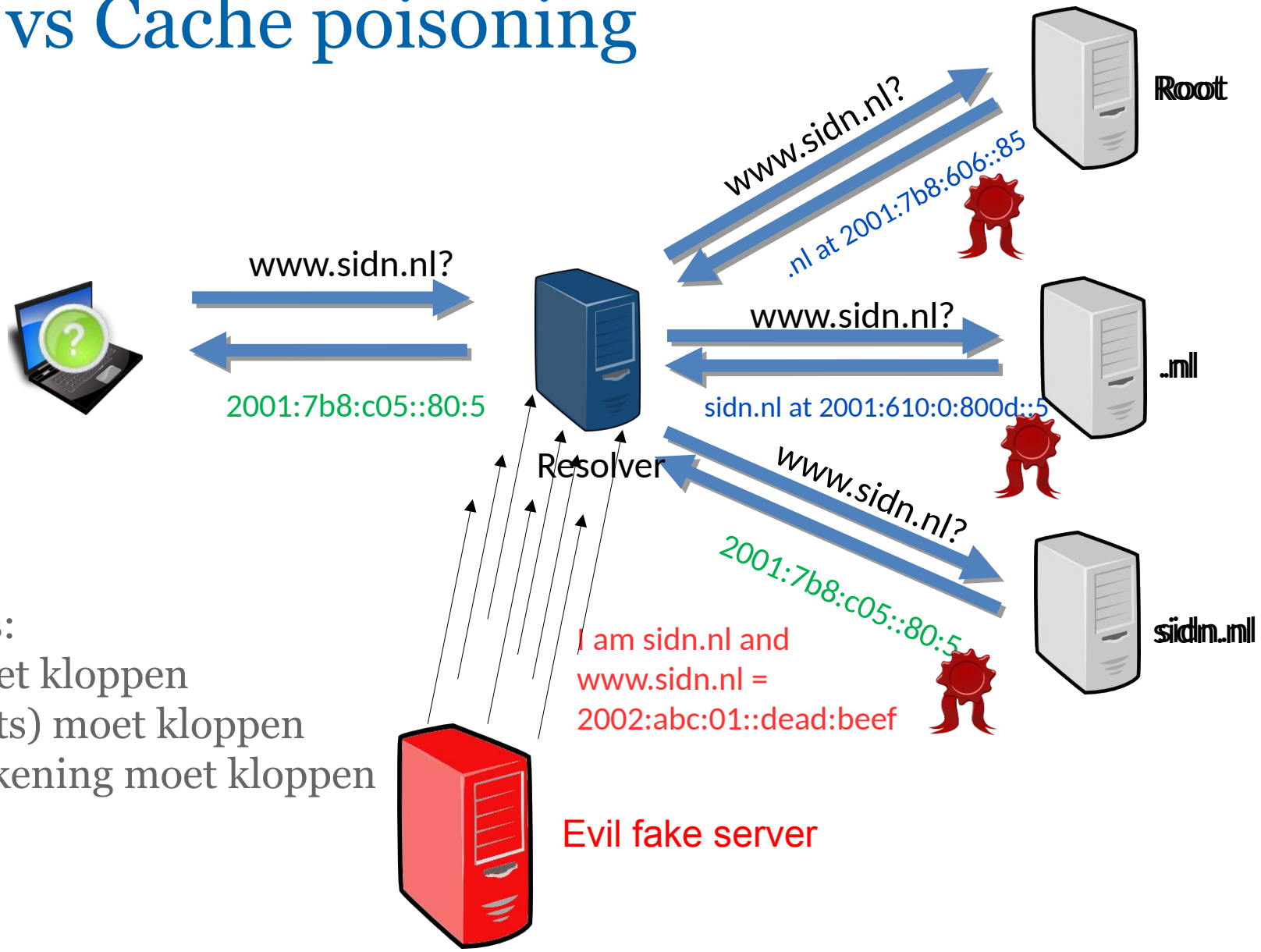
SIDN LABS

DNSSEC vs Cache poisoning



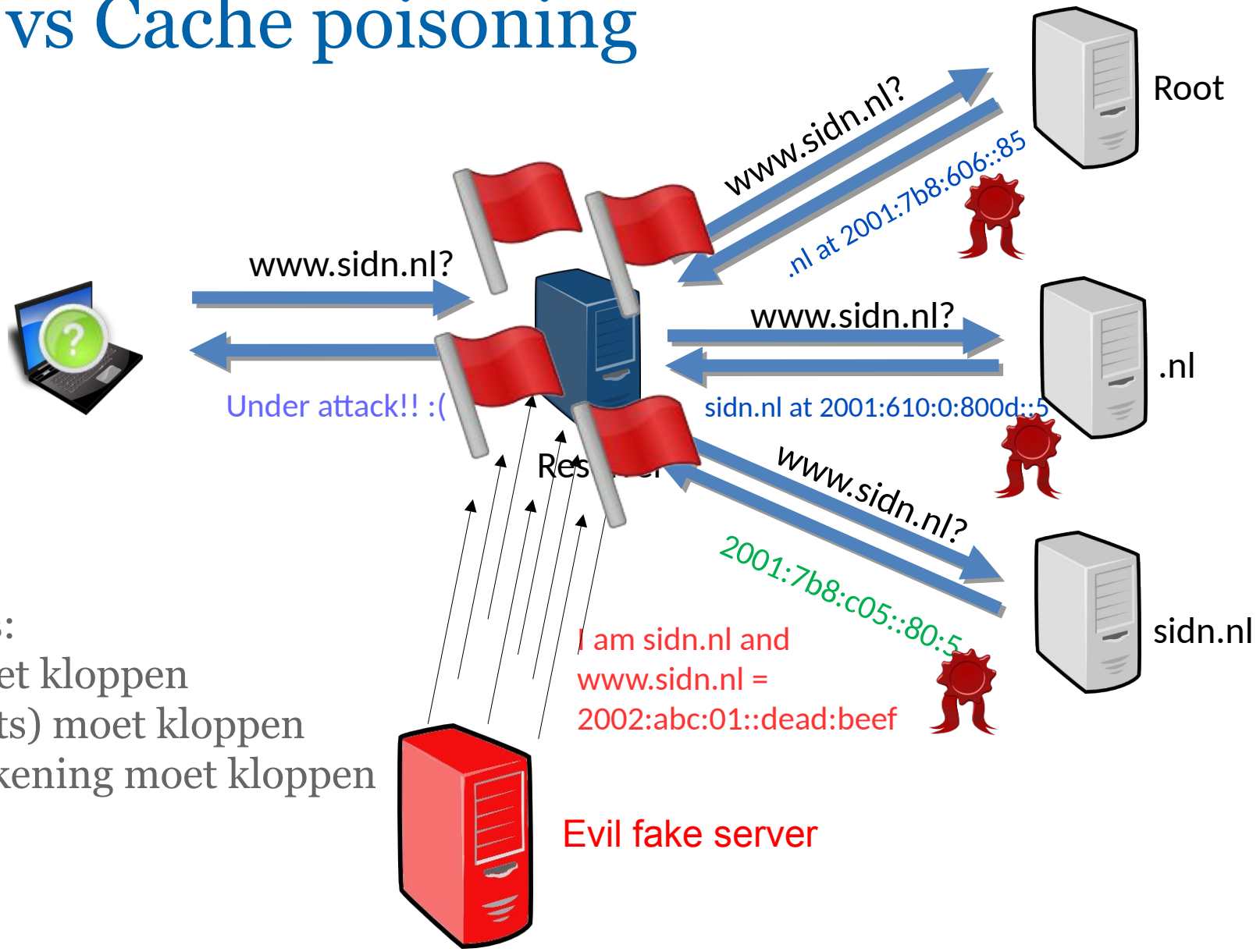
Eisen voor succes:
- qid (16 bits) moet kloppen
- UDP port (16 bits) moet kloppen
- Digitale handtekening moet kloppen

DNSSEC vs Cache poisoning



Eisen voor succes:
- qid (16 bits) moet kloppen
- UDP port (16 bits) moet kloppen
- Digitale handtekening moet kloppen

DNSSEC vs Cache poisoning



Eisen voor succes:
- qid (16 bits) moet kloppen
- UDP port (16 bits) moet kloppen
- Digitale handtekening moet kloppen

Bescherming: DNS-over-TLS

- RFC7858
- Beschermt het **kanaal** (niet de data zelf)
- Denk aan HTTPS, en het slotje in je browser

- Beschermt het kanaal tussen jouw computer en de resolver
- **Niet** tussen de resolver en de authoritative servers (zoals die van .nl)

- Voordeel: beschermt (lokaal) tegen afluisteren, en (lokaal) tegen spoofing
- Nadeel: de resolver zelf is niet beschermd

SIDN LABS

Bescherming: DNS-over-HTTPS

- RFC8484
- Beschermt het **kanaal** (niet de data zelf)
- **Is** HTTPS; je vraagt een domeinnaam op op dezelfde manier als dat je een website opvraagt.

- Ook hier alleen tussen jouw computer en de resolver

- Voordeel: beschermt (lokaal) tegen afluisteren, en (lokaal) tegen spoofing
- Nadeel: centralisatie (niet inherent, maar wel hoe het nu uitgerold wordt)

Samenvatting aanvallen op DNS

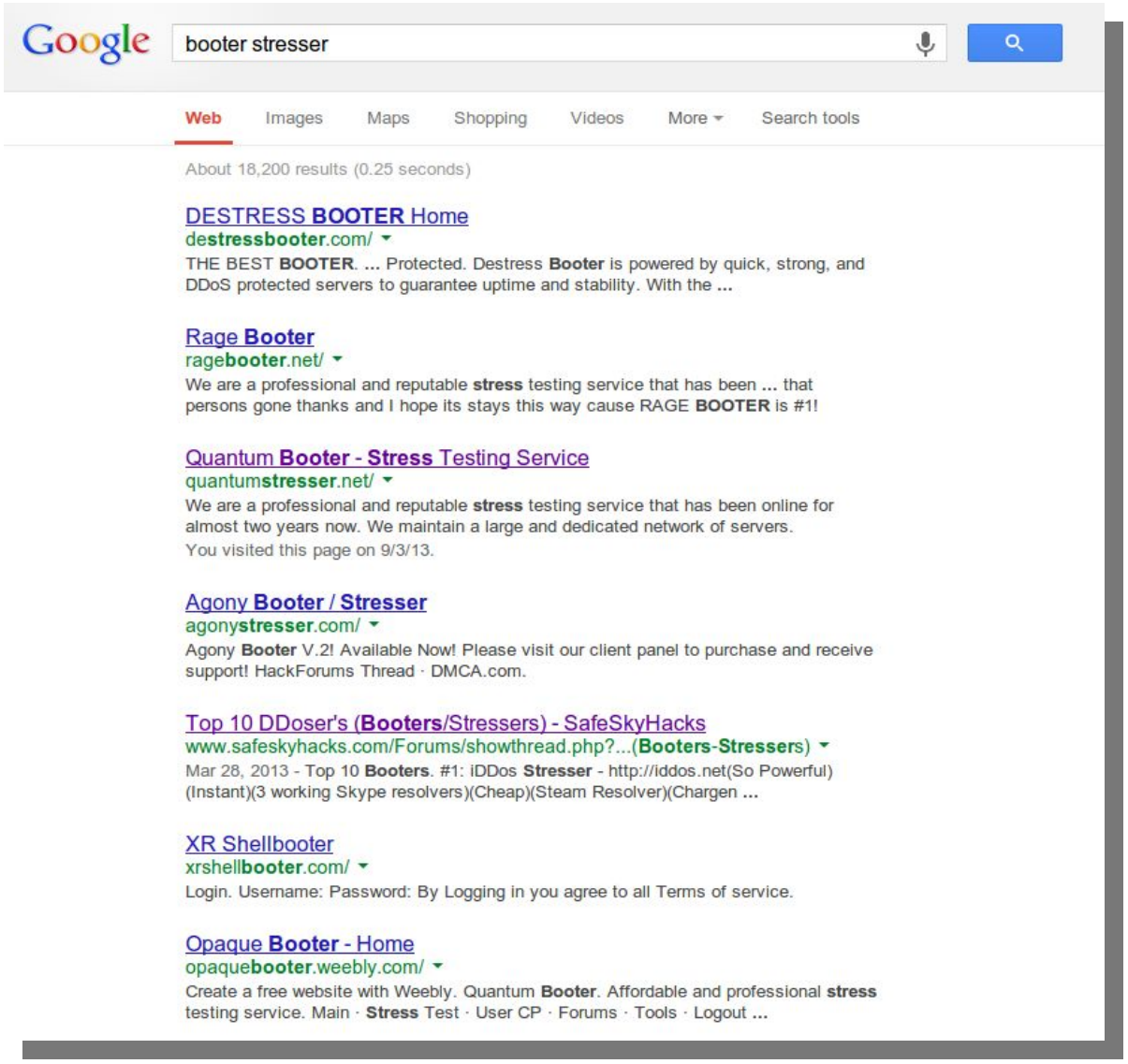
- DNS is oud, en onveilig
- Verschillende manieren om dat te verbeteren
- “Het hoeft alleen maar uitgerold te worden”
- Maar ze hebben allemaal nadelen.

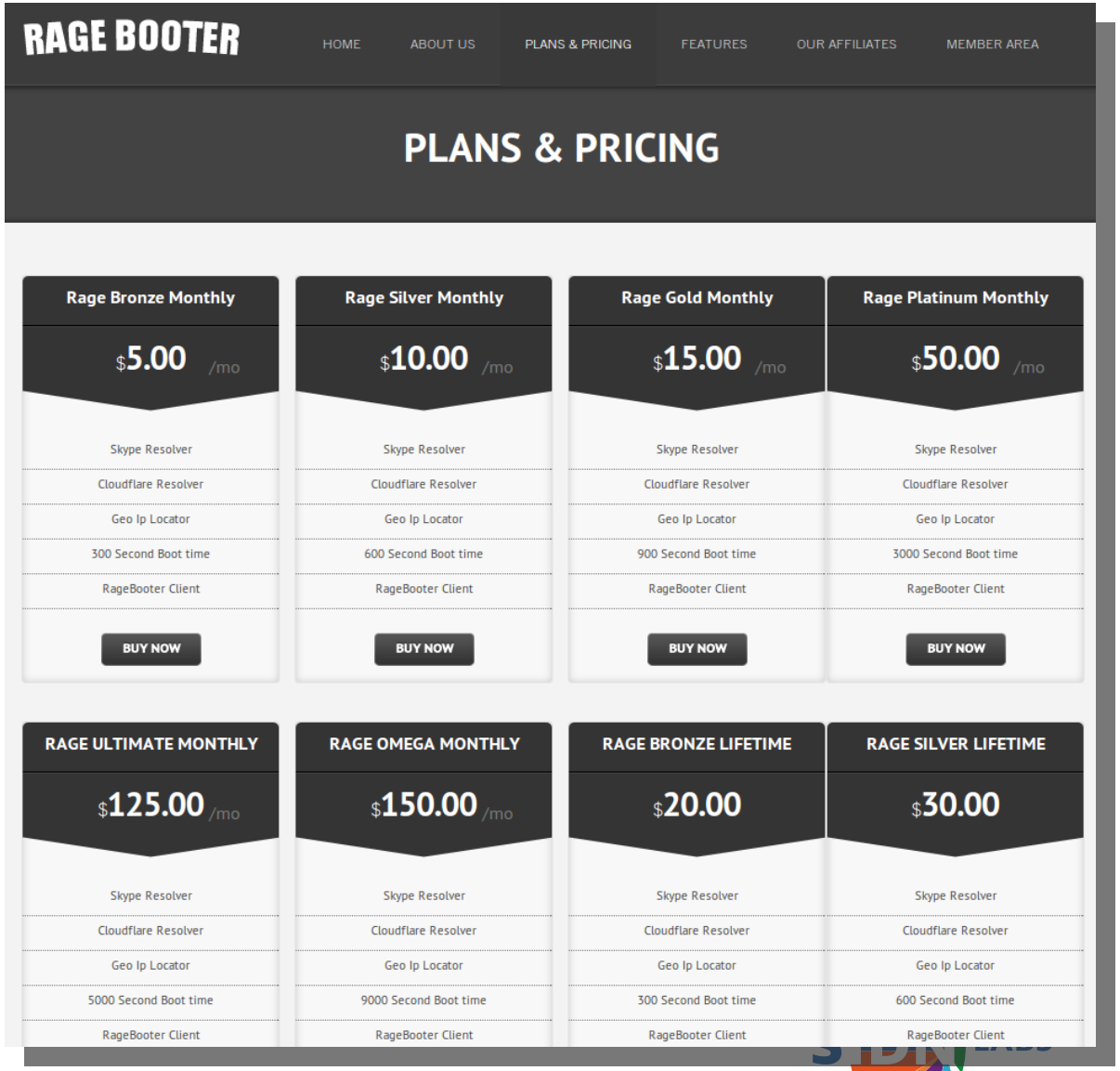
Aanvallen **met** DNS

DDoS-aanvallen

Vraag: wat denk je dat een DDoS-aanval kost?

DDoS == big business





Aanval met DNS: DDoS

- Net zoals DNS zijn botnets ook overal
- Die kunnen samen rechtstreeks een doelwit aanvallen
- Maar ze kunnen ook slimmer zijn…

Eigenschappen van DNS

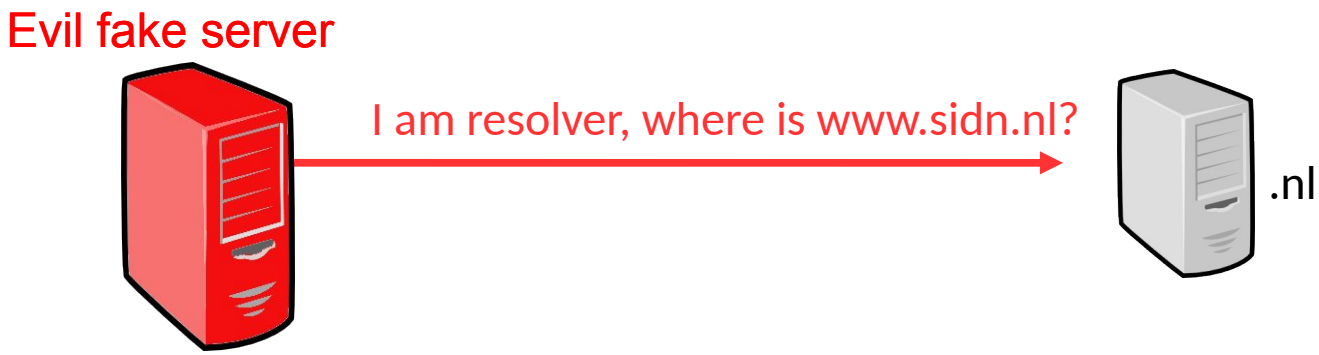
Je kunt de 'afzender' vervalsen (spoofing)

Dus gaat het antwoord niet naar jou maar naar je doelwit

DNS is assymetrisch

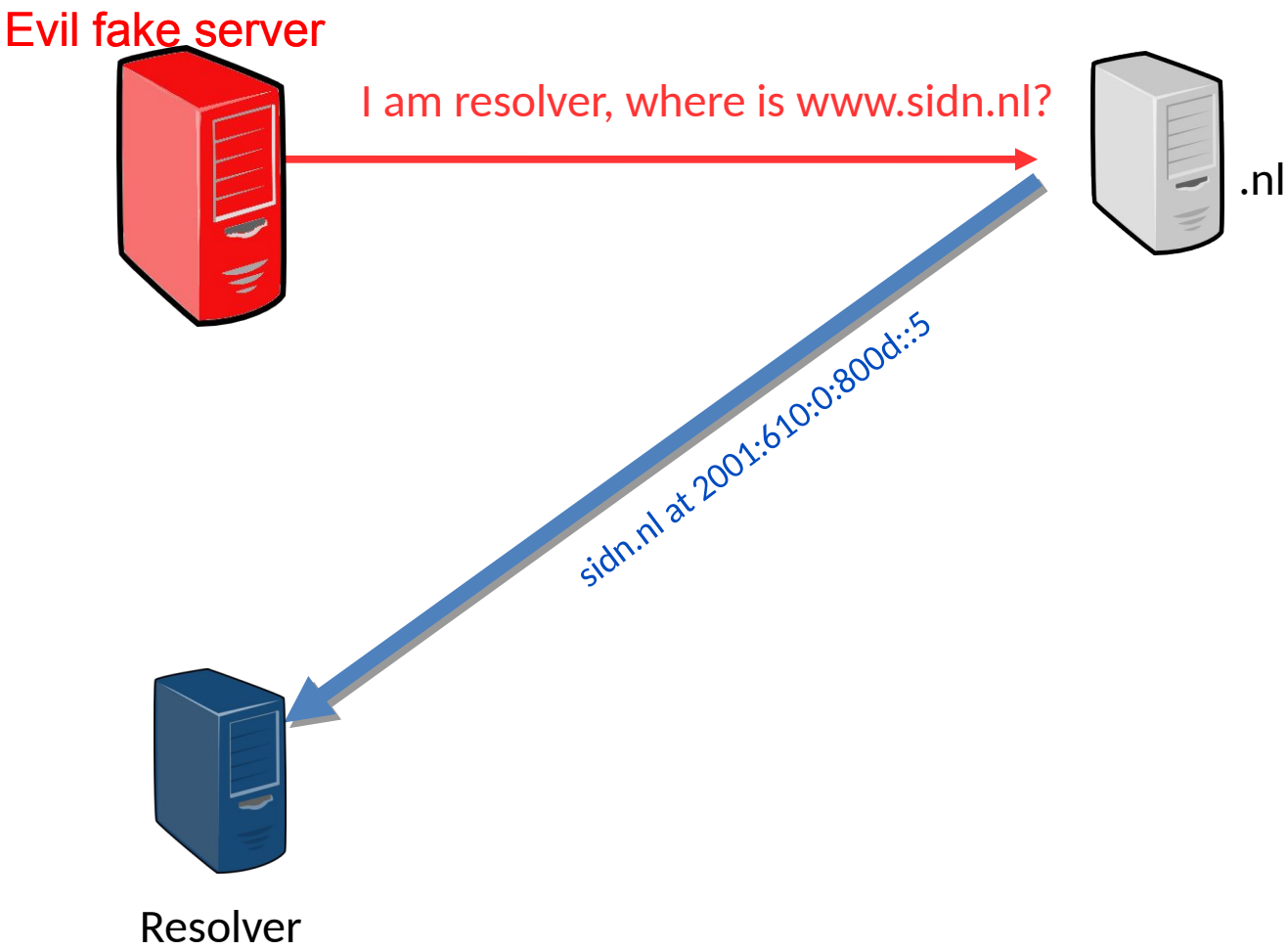
Dus is het antwoord groter dan de vraag

Reflection / amplification attack

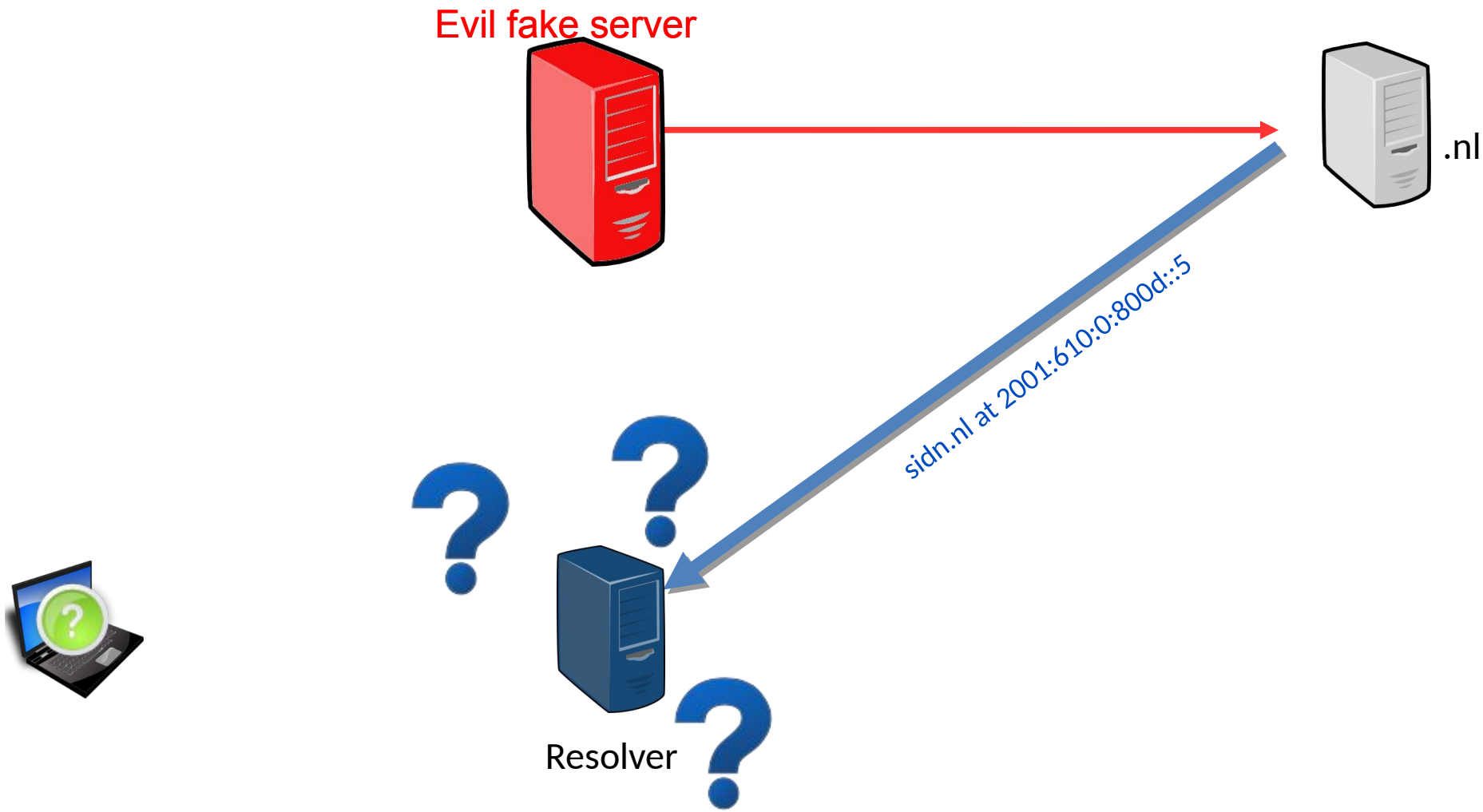


Resolver

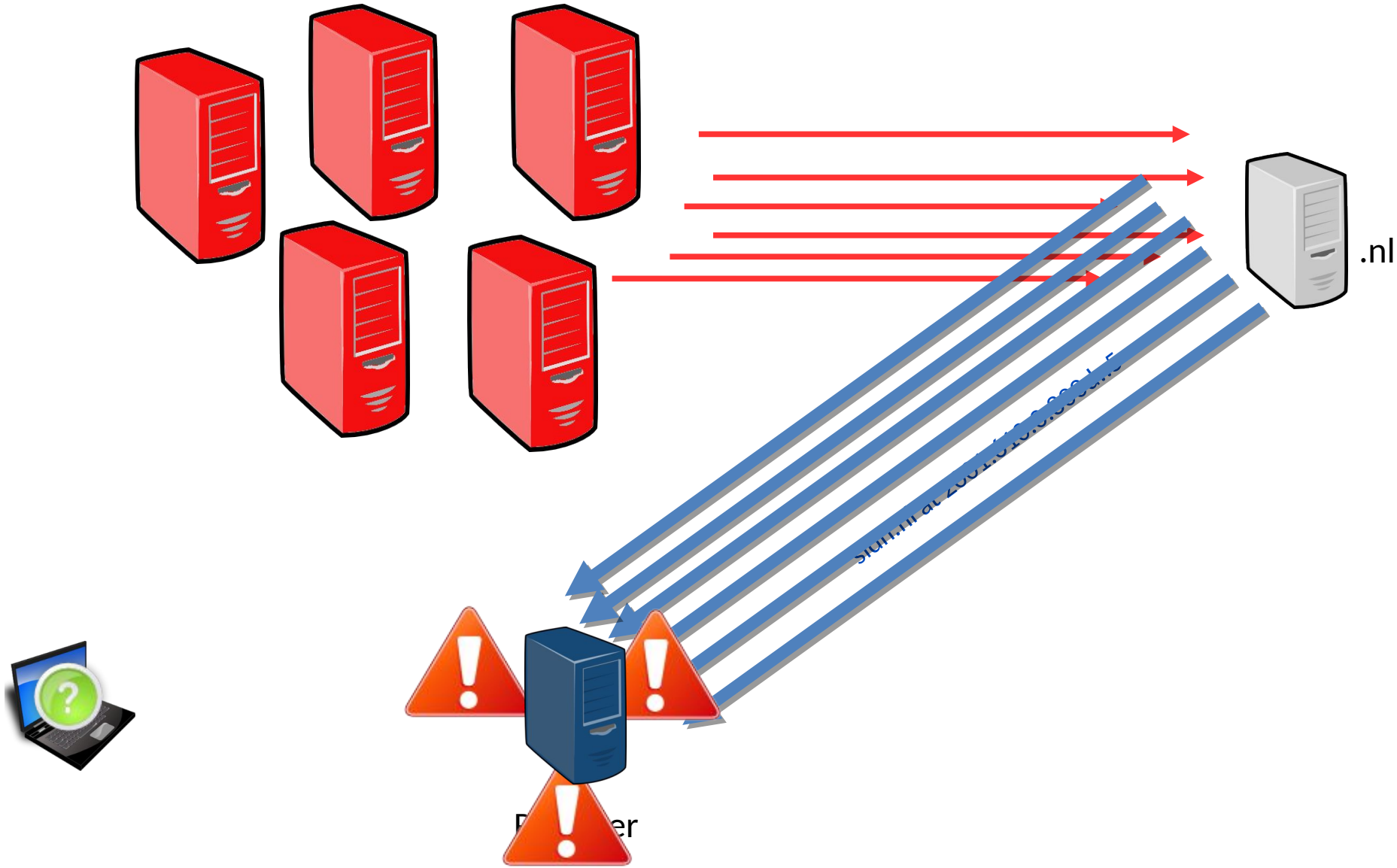
Reflection / amplification attack



Reflection / amplification attack



Reflection / amplification attack



Reflectie-aanval

```
; <<>> DiG 9.11.5-P4-5.1+deb10u1-Debian <<>> +qr ANY sidn.nl
;; global options: +cmd
;; Sending:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8201
;; flags: rd ad; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 2a6c62cbf5eab93d
;; QUESTION SECTION:
;sidn.nl.      IN  ANY

;; QUERY SIZE: 48
```

Reflectie-aanval

```
; <<>> DiG 9.11.5-P4-5.1+deb10u1-Debian <<>> +qr ANY sidn.nl
;; global options: +cmd
;; Sending:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8201
;; flags: rd ad; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 2a6c62cbf5eab93d
;; QUESTION SECTION:
;sidn.nl.      IN  ANY

;; QUERY SIZE: 48
```

Reflectie-aanval

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4856

;; flags: qr aa rd; QUERY: 1, ANSWER: 26, AUTHORITY: 0, ADDITIONAL: 1

;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 1232

; COOKIE: 1e56533a82a230a2edeac56d5f7f1d1f320f40c5d28c6594 (good)

;; QUESTION SECTION:

;sidn.nl. IN ANY

;; ANSWER SECTION:

sidn.nl. 3600 IN SOA ns1.sidn.nl. hostmaster.sidn.nl. 1602144661 14400 3600 3456000 300

Reflectie-aanval

sidn.nl. 3600 IN RRSIG SOA 8 2 3600 20201107071101 20201008071101 42033 sidn.nl.
KoAsT9lbpqLi3/cbDK7/wtkB34fiBXYiSlPqtWFrCDf119RL9ib17HJ1
CcEBzffl/g24jMRTZjMce1zxjGZhSsuS7ZHrKIcFIKgrLtYsYxZ3+Qjy
C2YmNRP61gA90B2uRgYHMQEH/QDL25DsLxGDeCcbIJmGeH3R8JFw7m2x DBw=

sidn.nl. 3600 IN NS ns3.sidn.nl.

sidn.nl. 3600 IN NS ns2.sidn.nl.

sidn.nl. 3600 IN NS ns1.sidn.nl.

sidn.nl. 3600 IN RRSIG NS 8 2 3600 20201107071101 20201008071101 42033 sidn.nl.
Ix5pG7GONQl0RN7N8eVMKWGIxlH9Bxd01g4wDOrztgSAVfD3I5/8fd/Z
SHRASnCTVdyJdJCScgZKDnRMyFCwW4ZHpxhE/5vvWBeuaCKaROth1B70
GtTiNPOwy+nye47DCarE9ZkYMrGImVoZlEwqgbsUDpDENA34QddiCTFz YDo=

sidn.nl. 3600 IN A 35.190.27.69

sidn.nl. 3600 IN RRSIG A 8 2 3600 20201107071101 20201008071101 42033 sidn.nl.
mIZzs7zZPjyX/Excj6yt7Cw8CuZhI7t7/DLIVQjRP4NevLK4JlqETS2q
VP8Vaxz1OOeN6ISRTEEUhZ9DZFv6Jtv7H7wqimCox42ptq2J5bFSPiIM
Fi+shjpNN09MMhBkJoucGTvBwIsE8k1rHseUevNG+Yf30ZvFG1gekLRK Bs4=

Reflectie-aanval

sidn.nl. 300 IN MX 5 esa.sidn.nl.

sidn.nl. 300 IN RRSIG MX 8 2 300 20201107071101 20201008071101 42033 sidn.nl.
l9CVNZnocTOdt+eUFoFNpOWj2/EilBzxIVg2pLH03Mysof/ytWOwuEvd
nJArp+sUFc7ubWv4xqiCNJapdbpCiG3bgXXyKgUXPeMLYG8UUEZnwJWb
t+HH/jJ+aZdcMKdibmVmyvCWwUghfNT5d0It7KsG6dCvxyY45cfd995u A70=

sidn.nl. 3600 IN TXT "b49e83a3cf3f49b49be0ceea668e8457"

sidn.nl. 3600 IN TXT "google-site-verification=nGdTpBOjSS2sHxxqhEE9Tj3xcK5X4-lF9YLqtYmXbwI"

sidn.nl. 3600 IN TXT "google-site-verification=UgJBr_GdHnW8WlMHFlo59LLMiNz0g-T3g6ijOs7KBWE"

sidn.nl. 3600 IN TXT "v=spf1 ip4:193.176.144.0/24 ip4:94.198.152.0/21 ip6:2001:610:118::/48
ip6:2a00:d78::/32 include:spf.protection.outlook.com mx exp=explain._spf.%{d} ~all"

sidn.nl. 3600 IN RRSIG TXT 8 2 3600 20201107071101 20201008071101 42033 sidn.nl.
Q0v/MOrLVkF1dM2Swx2pm5m33fhr6dt/RSJTSFOAAi9FiHsAaq0CjTeE
gtho9G/oVS9rhVpx52fSCItUVUPM7LeKn3BbzMVe/NzWc54WOkQzIqS5
ygpIN5PkGexbDzf7V0QXwfuQ6haZhKrHzcYG0G9xtowoE2scAxflZ6QA wVI=

sidn.nl. 3600 IN AAAA 2600:1901:0:7947::

Reflectie-aanval

sidn.nl. 3600 IN RRSIG AAAA 8 2 3600 20201107071101 20201008071101 42033 sidn.nl.
a6cPMcoiWi7PRs47PrQZ9iHlxxrBOEKlwWjkPCLd8vCBk8rNGuAP31rY
EvnfvdXo/B5WjWGJcpatcMrd+8XwM5Fv7pl+7K1uMlKQr65psTxOYhsB
hBB0EDn9YuWMcoROLeNDWJou/VVxnPf6kqY0i4jtrFdZpvBuxG6MK8+h Rm4=

sidn.nl. 300 IN NSEC _ac8039507f4e87cce543dde15f92938c.sidn.nl. A NS SOA MX TXT AAAA RRSIG NSEC DNSKEY CAA

sidn.nl. 300 IN RRSIG NSEC 8 2 300 20201107071101 20201008071101 42033 sidn.nl.
bx6A/5JmWIjIxzu/Cq4AKI3MqfHnu8vOf51Eke+9XO+MTpDUNwdwzjH/
OD/d1biYiOB4jJfCnXo7l00Ji0qMUKq4x9pRcxLGidlvAtprBG1vxx6A
rXdHWjkhIX/1ADpfsLPfveyucX8hXmTyshrVZvU9Xexm1bBD1rbroo0P gVg=

sidn.nl. 3600 IN DNSKEY 257 3 8 AwEAAc31XDE3QWphFz6CR77Hp3ZjDRx7zqe1AXx1QMvqFKzrEKrX4oj2
nv8zDquCotbQ1ObHI4KGLRf3ycaq0fYslXFJ1JxLxJUl/lpGvE8Okqdh GW3vj3YS9MlbfoyYC2bNUY875UgDNRLqWtVSEXO/
PCcqr3RIzpngu+6J F/1bfQB7ituFHxoanhAiWOpc24ZAnrhmyIsDwyy1k0iyvVTSyPugnYD/
bF7CR7ObQCiuucjwCkK2KS52bcihHvyPDU/DlsSJeEO/G31zFxzXwHjr
3h3mdJE4mQuceS11e5/c9hht6rUL0PEGve1Ygknz+0ruAinlhFYnny2u xES5M9r0FIM=

sidn.nl. 3600 IN DNSKEY 256 3 8 AwEAAbjldpe4GB8sn+MWifCAup9RB34jjUimwi4DD59ZUSS1fO8QfpXT
YWyF9QVFlpiVHxTZ0jKO2CAOiS3pz9GCn3ICjEjzjg6OSLFFMjT/X3gn
3kRK9IXhjT+tNsBC5pfS5di4SIf6dq0ms5iI3YLzV2n6CsZsQziAUdM8 mpSOFWqx

Reflectie-aanval

sidn.nl. 3600 IN RRSIG DNSKEY 8 2 3600 20201107071101 20201008071101 39274 sidn.nl.
vyL5gmyzyOVZl6nZHP4oI2qSar+wgGzPAxCqbtwTmUv0hi0b+WMBYwL2
Qkz6jRqJmby5kJakIx/iIURWOCAWSylQuYPqi7t7XswphKIMnACKVCSQ
RocOvJkUtZUxx3bypTzloXQy67Zr1YqNBM+Y6HBsRhdnF96uQOUiPvd5
Ry2Gq9vH1RKws4WGtAuQuxNrV7u1C+afSHoVVI2AaO2z2JyM92GanIYK
Bk9wD7hqGWQnJEmHfysatxmhVYjM5SpKpiUP72eQM98U53stRfO8+p0h
RkzOUHTBc/tWZ2QcyQCRzJykMRXCPkF+q+LWCo9QaaiG6Dp81xcWhm6m /5xApg==

sidn.nl. 3600 IN RRSIG CAA 8 2 3600 20201107071101 20201008071101 42033 sidn.nl.
JVTKVv5DcsZkBHnrRVtIpxnTUL/GQWssk4Q+7rX88uHelE0BPOCb3O2B
mw8i/kXoYo3/u//FGL58mO0KYWVtyaVo8DgJdlGOO15fWciANCY/3/MX
hUD5QO6f0uCKuucWDnDepCcooDAd355YAwg4fj00BRq+HumttRufZEYi KJY=

sidn.nl. 3600 IN CAA 0 iodef "mailto:abuse@sidn.nl"

sidn.nl. 3600 IN CAA 0 issue "digicert.com"

sidn.nl. 3600 IN CAA 0 issue "sectigo.com"

;; Query time: 91 msec

;; SERVER: 2001:7b8:606::88#53(2001:7b8:606::88)

;; WHEN: Thu Oct 08 16:07:27 CEST 2020

;; MSG SIZE rcvd: 2823

SIDN LABS

Reflectie-aanval

sidn.nl. 3600 IN RRSIG DNSKEY 8 2 3600 20201107071101 20201008071101 39274 sidn.nl.
vyL5gmyzyOVZl6nZHP4oI2qSar+wgGzPAxCqbtwTmUv0hi0b+WMBYwL2
Qkz6jRqJmby5kJakIx/iIURWOCAWSylQuYPqi7t7XswphKIMnACKVCSQ
RocOvJkUtZUxx3bypTzloXQy67Zr1YqNBM+Y6HBsRhdnF96uQOUiPvd5
Ry2Gq9vH1RKws4WGtAuQuxNrV7u1C+afSHoVVI2AaO2z2JyM92GanIYK
Bk9wD7hqGWQnJEmHfysatxmhVYjM5SpKpiUP72eQM98U53stRfO8+p0h
RkzOUHTBc/tWZ2QcyQCRzJykMRXCPkF+q+LWCo9QaaiG6Dp81xcWhm6m /5xApg==

sidn.nl. 3600 IN RRSIG CAA 8 2 3600 20201107071101 20201008071101 42033 sidn.nl.
JVTKVv5DcsZkBHnrRVtIpxnTUL/GQWssk4Q+7rX88uHelE0BPOCb3O2B
mw8i/kXoYo3/u//FGL58mO0KYWVtyaVo8DgJdlGOO15fWciANCY/3/MX
hUD5QO6f0uCKuucWDnDepCcooDAd355YAwg4fj00BRq+HumttRufZEYi KJY=

sidn.nl. 3600 IN CAA 0 iodef "mailto:abuse@sidn.nl"

sidn.nl. 3600 IN CAA 0 issue "digicert.com"

sidn.nl. 3600 IN CAA 0 issue "sectigo.com"

;; Query time: 91 msec

;; SERVER: 2001:7b8:606::88#53(2001:7b8:606::88)

;; WHEN: Thu Oct 08 16:07:27 CEST 2020

;; MSG SIZE rcvd: 2823

Reflectie-aanval

- De vraag was 48 bytes
- Het antwoord 2823

Dat geeft je meer dan 50 keer je beschikbare bandbreedte als aanval.
(theoretisch zelfs 100 keer)

En je bots zijn moeilijker te traceren.

Reflectie-aanvallen

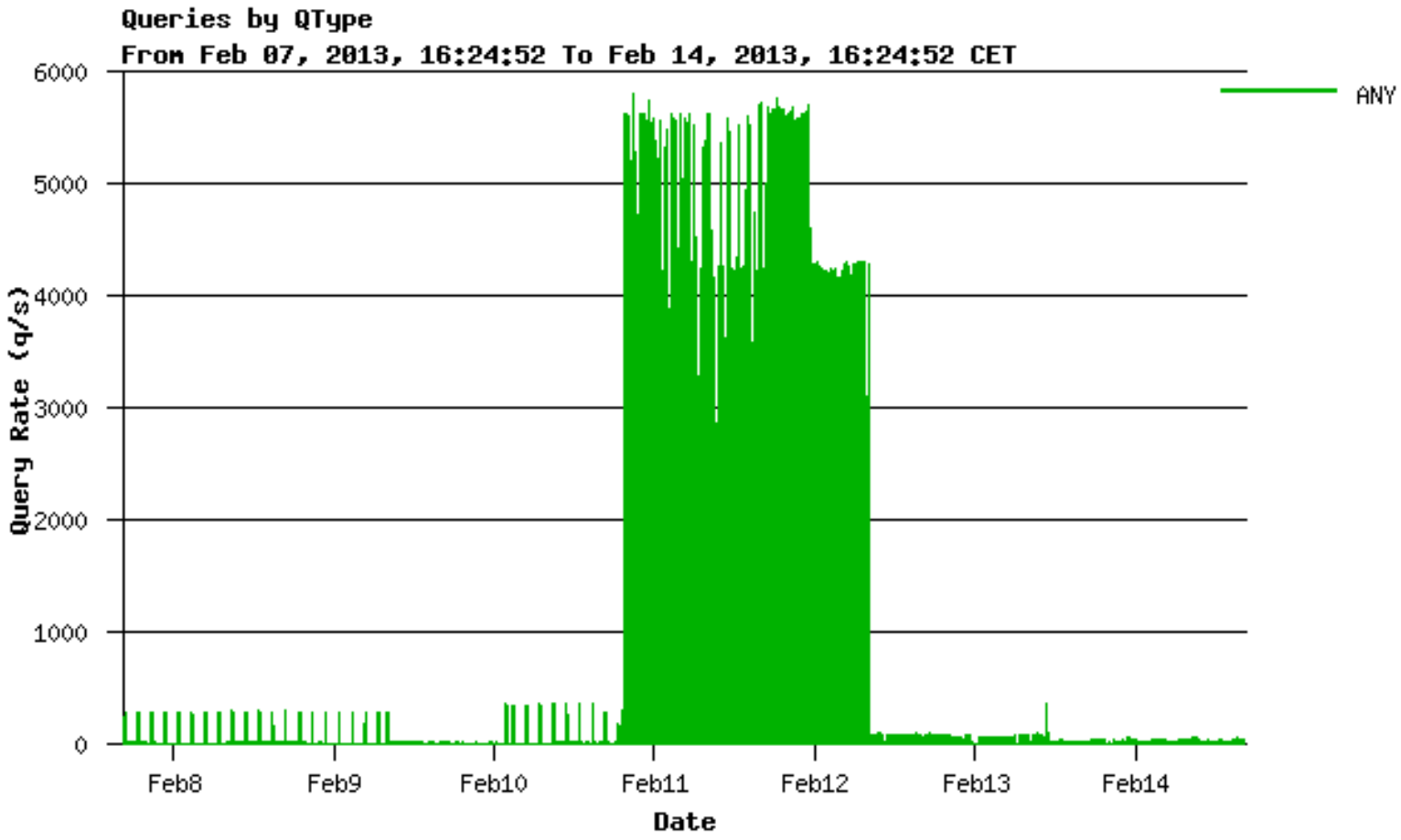
- Grootste winst via 'open resolvers'
- Dat zijn resolvers die per ongeluk voor de hele wereld dns resolution doen.

Reflectie-aanvallen

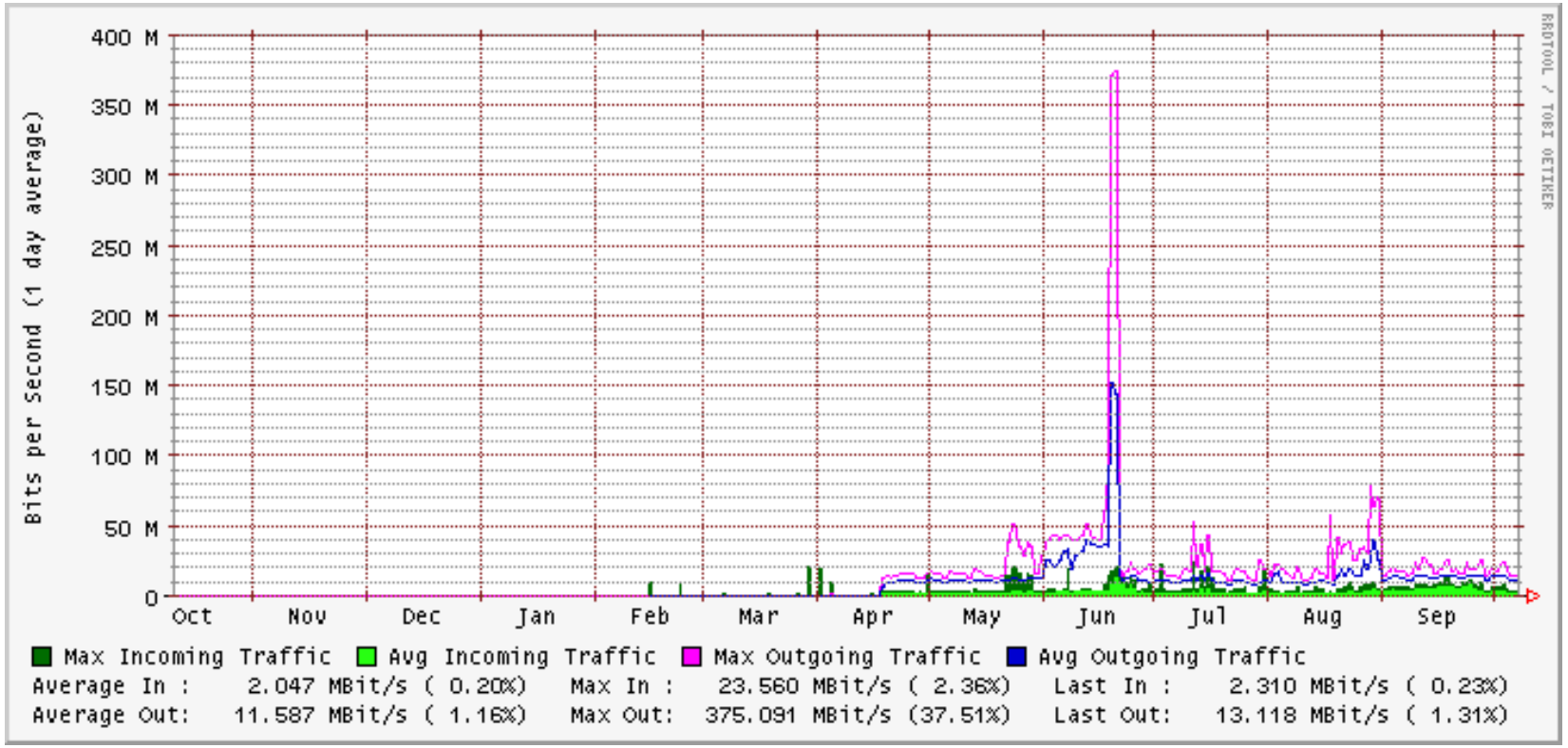
Maar ook beheerders van 'normale' zones kunnen misbruikt worden

Zoals SIDN...

ANY-aanval op SIDN



ANY-aanval op SIDN



ANY-aanval op SIDN

Dus maar een firewall rule

```
rule=$(python generate-netfilter-u32-dns-rule.py --qname nl --qtype ANY)

iptables -A INPUT -p udp --dport 53 --match u32 --u32 "$rule" -j RATELIMITER

iptables -A RATELIMITER -m hashlimit \
--hashlimit-name DNS --hashlimit-above 20/second --hashlimit-mode srcip \

--hashlimit-burst 100 --hashlimit-srcmask 28 -j DROP
```

SIDN LABS

ANY-aanval op SIDN

Dus maar een firewall rule

```
rule=$(python generate-netfilter-u32-dns-rule.py --qname nl --qtype ANY)
```

ANY-aanval op SIDN

Maar wacht. DNS is 'case-insensitive'. Firewalls zijn dat niet...

```
rule=$(python generate-netfilter-u32-dns-rule.py --qname nl --qtype ANY)
rule=$(python generate-netfilter-u32-dns-rule.py --qname NL --qtype ANY)
```

ANY-aanval op SIDN

Maar wacht. DNS is 'case-insensitive'. Firewalls zijn dat niet...

```
rule=$(python generate-netfilter-u32-dns-rule.py --qname nl --qtype ANY)
rule=$(python generate-netfilter-u32-dns-rule.py --qname NL --qtype ANY)
rule=$(python generate-netfilter-u32-dns-rule.py --qname Nl --qtype ANY)
```

ANY-aanval op SIDN

Maar wacht. DNS is 'case-insensitive'. Firewalls zijn dat niet...

```
rule=$(python generate-netfilter-u32-dns-rule.py --qname nl --qtype ANY)
rule=$(python generate-netfilter-u32-dns-rule.py --qname NL --qtype ANY)
rule=$(python generate-netfilter-u32-dns-rule.py --qname Nl --qtype ANY)
rule=$(python generate-netfilter-u32-dns-rule.py --qname nL --qtype ANY)
```

ANY-aanval op SIDN

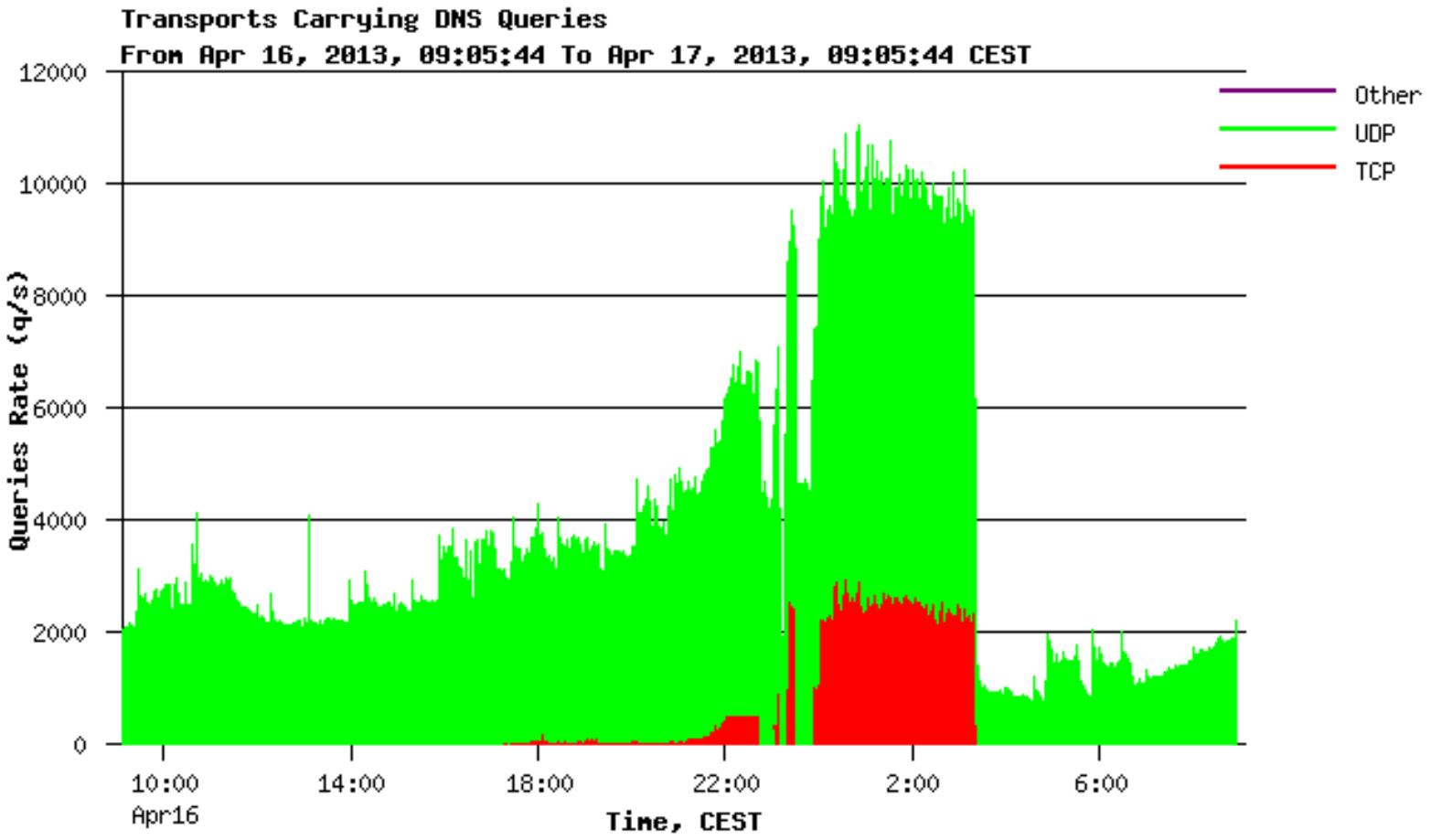
Maar wacht. DNS is 'case-insensitive'. Firewalls zijn dat niet...

```
rule=$(python generate-netfilter-u32-dns-rule.py --qname nl --qtype ANY)
rule=$(python generate-netfilter-u32-dns-rule.py --qname NL --qtype ANY)
rule=$(python generate-netfilter-u32-dns-rule.py --qname Nl --qtype ANY)
rule=$(python generate-netfilter-u32-dns-rule.py --qname nL --qtype ANY)
```

Bescherming: Response Rate Limiting

- Ingebouwd in DNS servers
- Als je steeds opnieuw dezelfde vraag krijgt, geef minder (of geen) antwoorden
- Of forceer TCP (beschermt tegen spoofen)

Bescherming: Response Rate Limiting



En de aanvallen bleven daarna weg!

En dan is er nog privacy…

SIDN LABS

DNS en Privacy

- DNS is een plain-text protocol
- Als iemand je netwerkverkeer kan zien (publieke wifi bijvoorbeeld) kunnen ze zien wat je kan doen

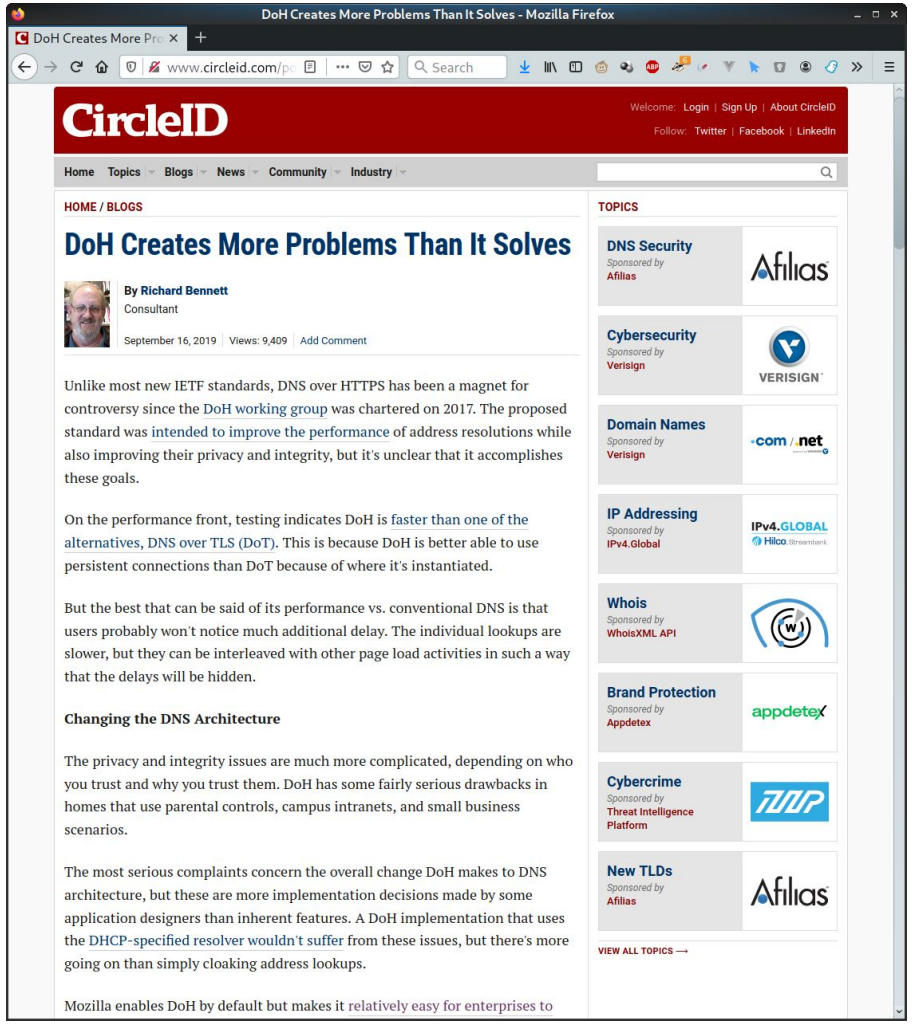
- Al je domeinnamen, of dat nu van je bank is of van, zeg, websites voor 'volwassenen'.

- Degene die je DNS-resolver beheert kan dat ook!

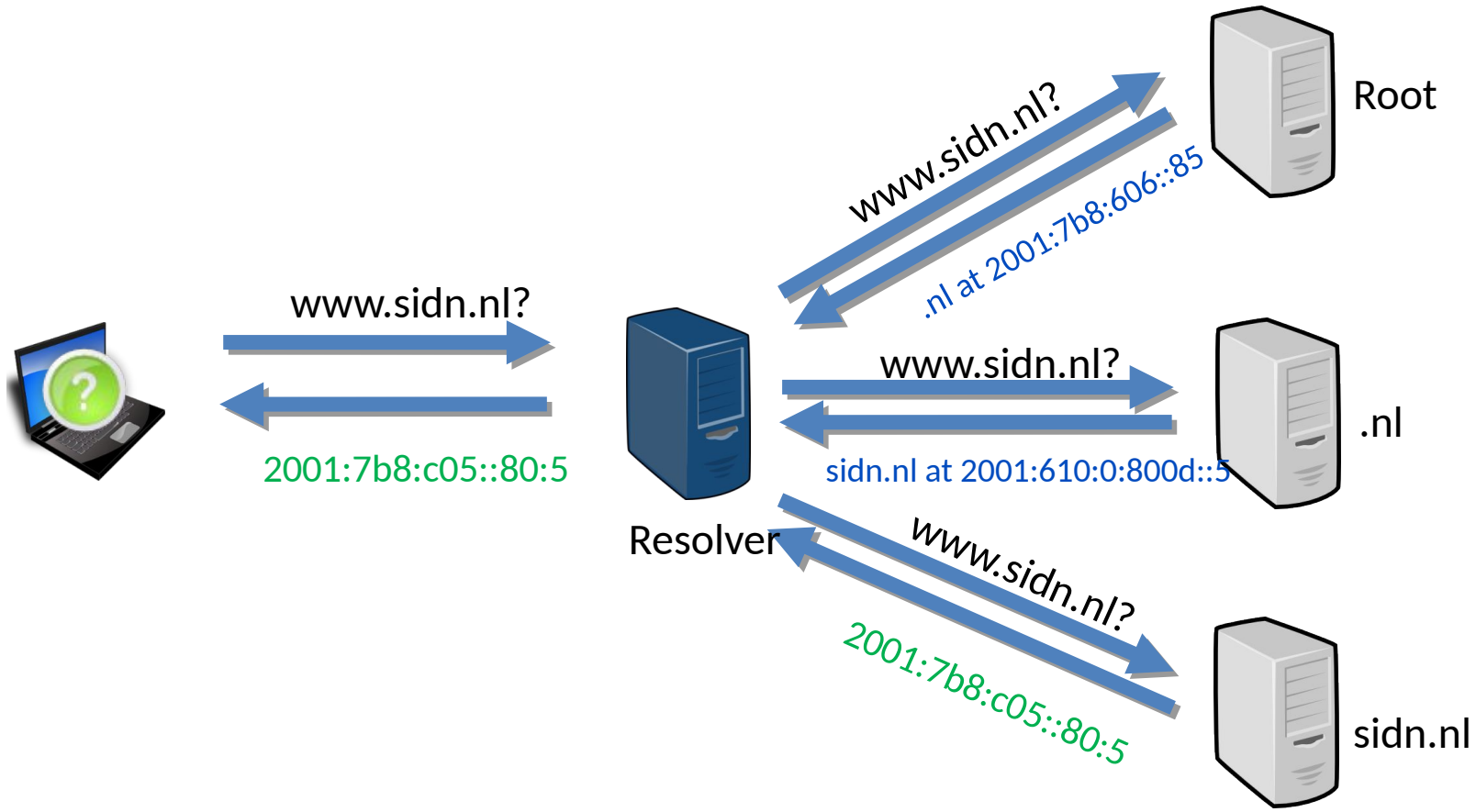
SIDN LABS

Bescherming tegen afluisteren

- DNS-over-https
- Je 'kiest' wie je resolver is
- Duivelse keuze:
  - Mag je ISP het zien, of Cloudflare?
- Moet het standaard ingebouwd worden?

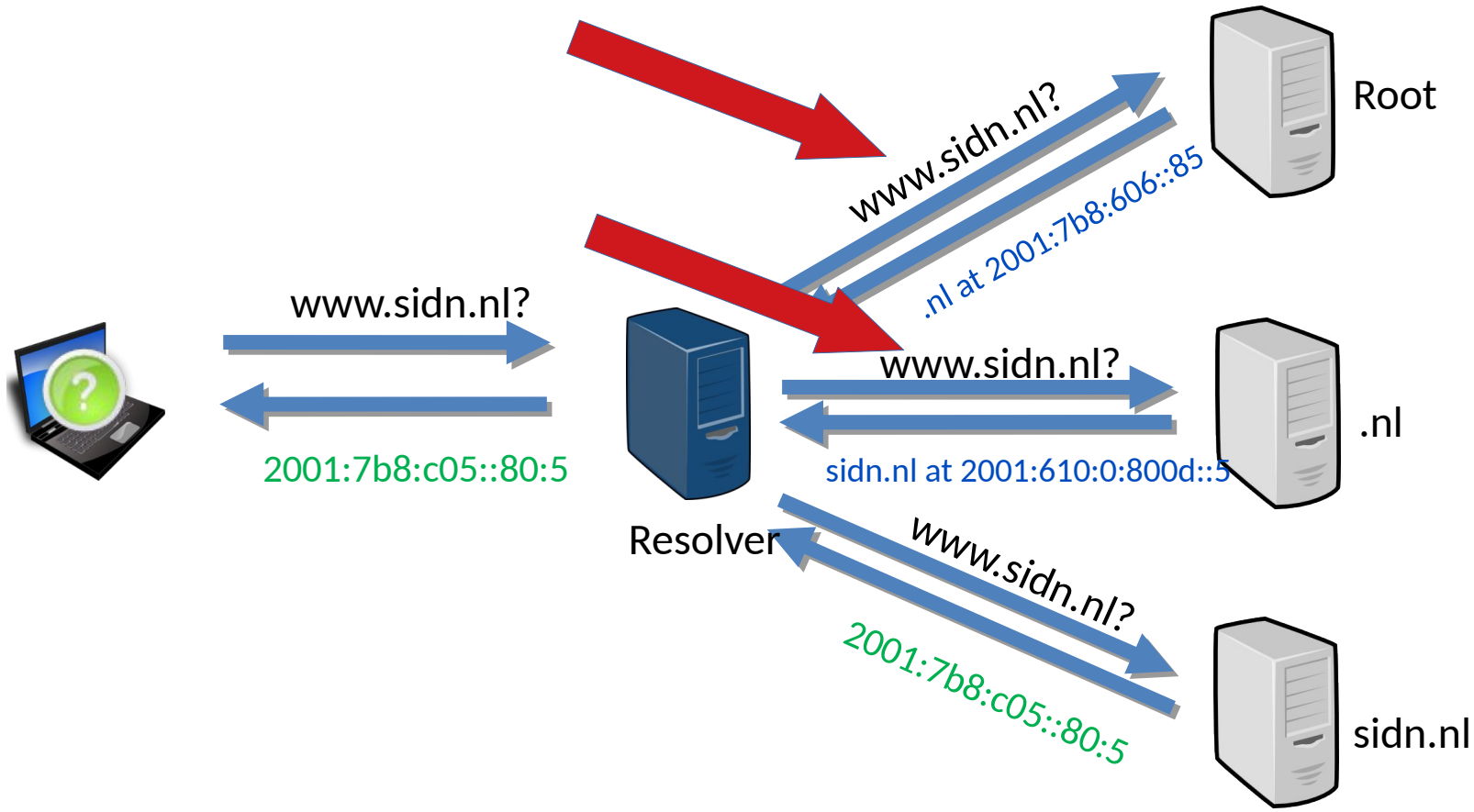


Nog een leuke over privacy: terug naar resolution



Vraag: valt hier iets op?

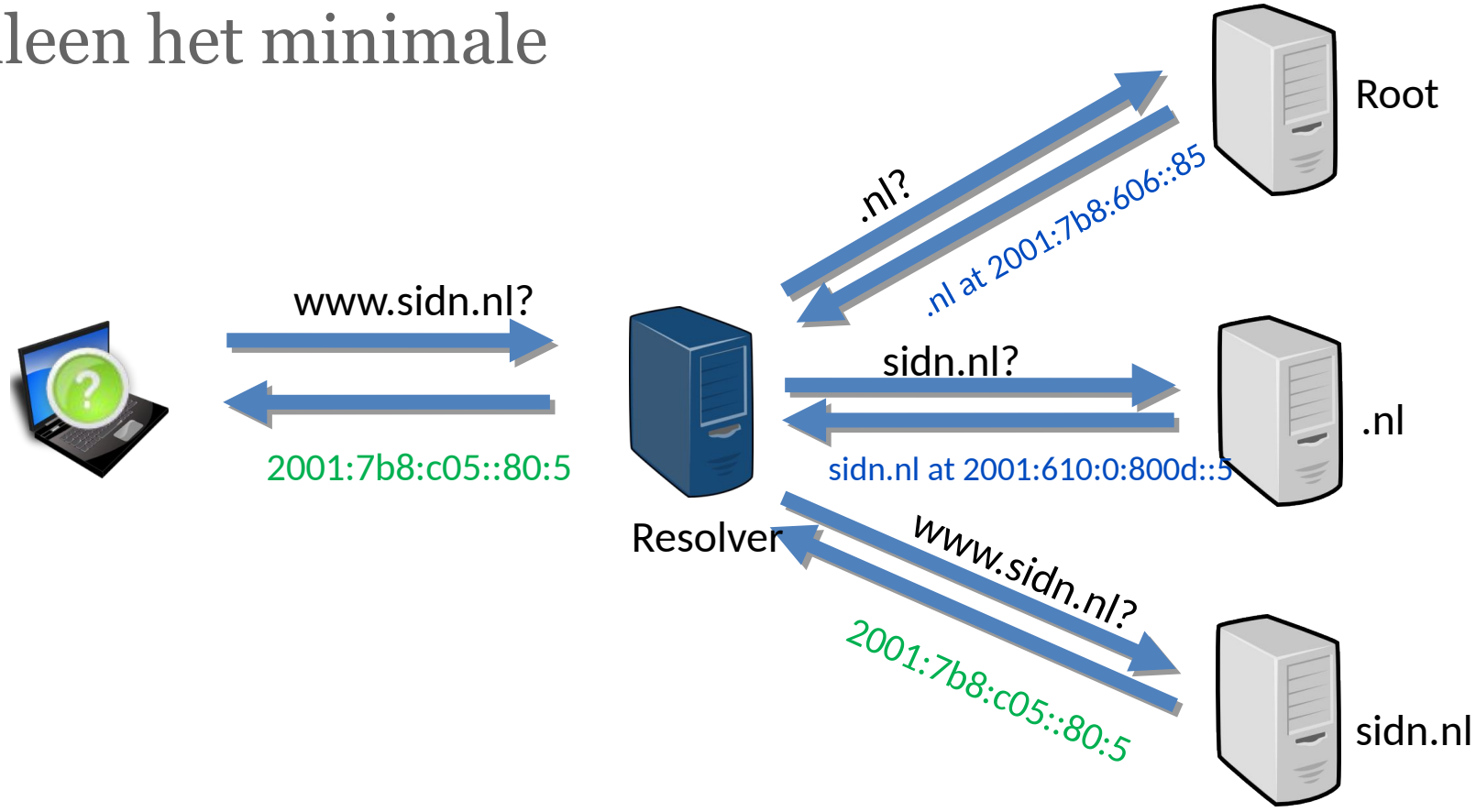
Nog een leuke: terug naar resolution



Vraag: valt hier iets op?

Relatief nieuw: QNAME Minimization

- Iets slimmer
- Resolver splitst zelf de domeinnaam op in labels
- Vraagt alleen het minimale



Voorzichtige conclusie

- DNS is meer, veel meer, dan de meeste mensen denken
- Met vele veiligheidsproblemen, maar ook vele oplossingen
- Ondanks de leeftijd wordt er nog steeds volop aan gesleuteld

Zijn er nog vragen?

Volg ons


SIDN.nl


@SIDN


SIDN

Dank jullie wel voor de aandacht!