Oct. 31 2023

DNS protocol evolution - From plain text to secure and privacy preserving DNS

afnic
Internet
made in France

Sandoche BALAKRICHENAN

afnic | Labs

Agenda

- Follow a DNS Query/Response
- Adding Privacy to the DNS protocol
- Adding Security to the DNS protocol
- Tool to check your DNS health

afnic | Labs



- Sandoche BALAKRICHENAN
  - PhD (Univ. Pierre et Marie Curie), MSc in Comp. & Comm. Networks (Institut Nationales des Télécommunications), MSc in Innovation & Entrepreneurship (HEC)
  - Head of R&D Partnerships @ French Network Information Center
  - LoRa Alliance Academic WG Chair

afnic | Labs

DNS design idea

> "A name indicates what we seek. An address indicates where it is. A route indicates how we get there."
>
> —Jon Postel, RFC 791

Eco-system for the Domain Name Service

1. Naming Conventions

IETF is the SDO

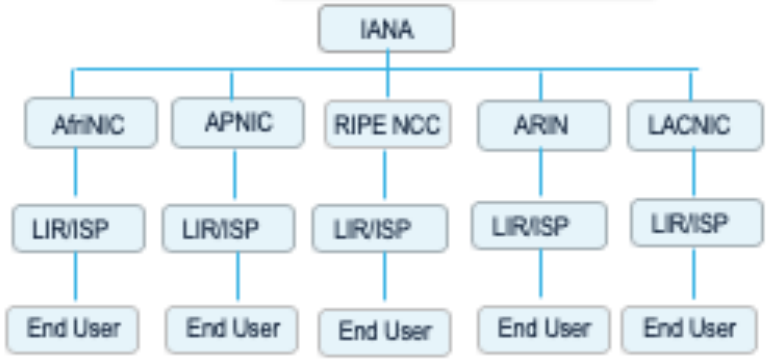
- Domain names, URI
- IP Addresses (IPv4/IPv6)

2. Provisioning

2.1. Domain registry



2.2 Internet number registry



3. Resolution



afnic | Labs

A classical Internet use-case



User accessing web

Internet

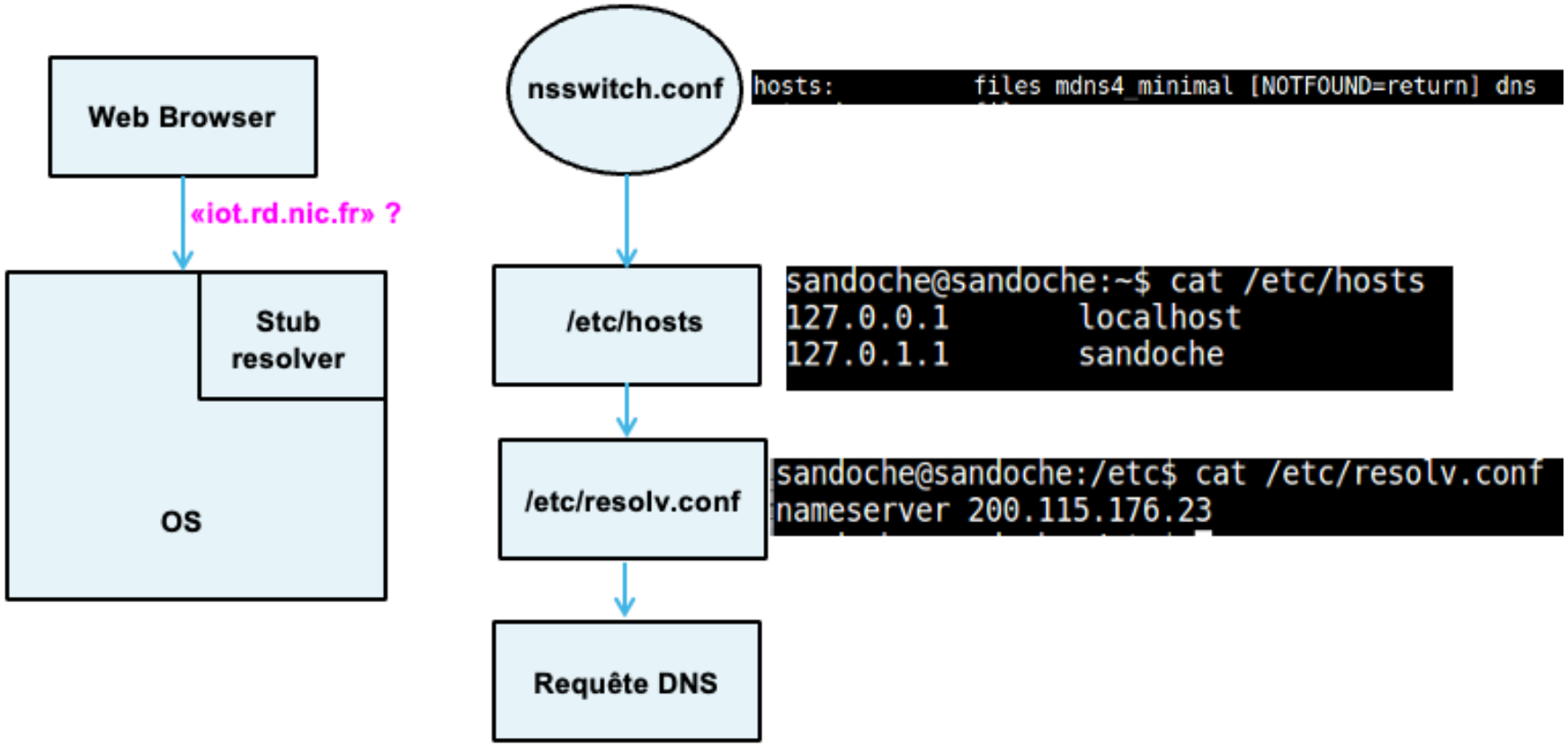
Web Server

afnic | Labs

User -> Web browser

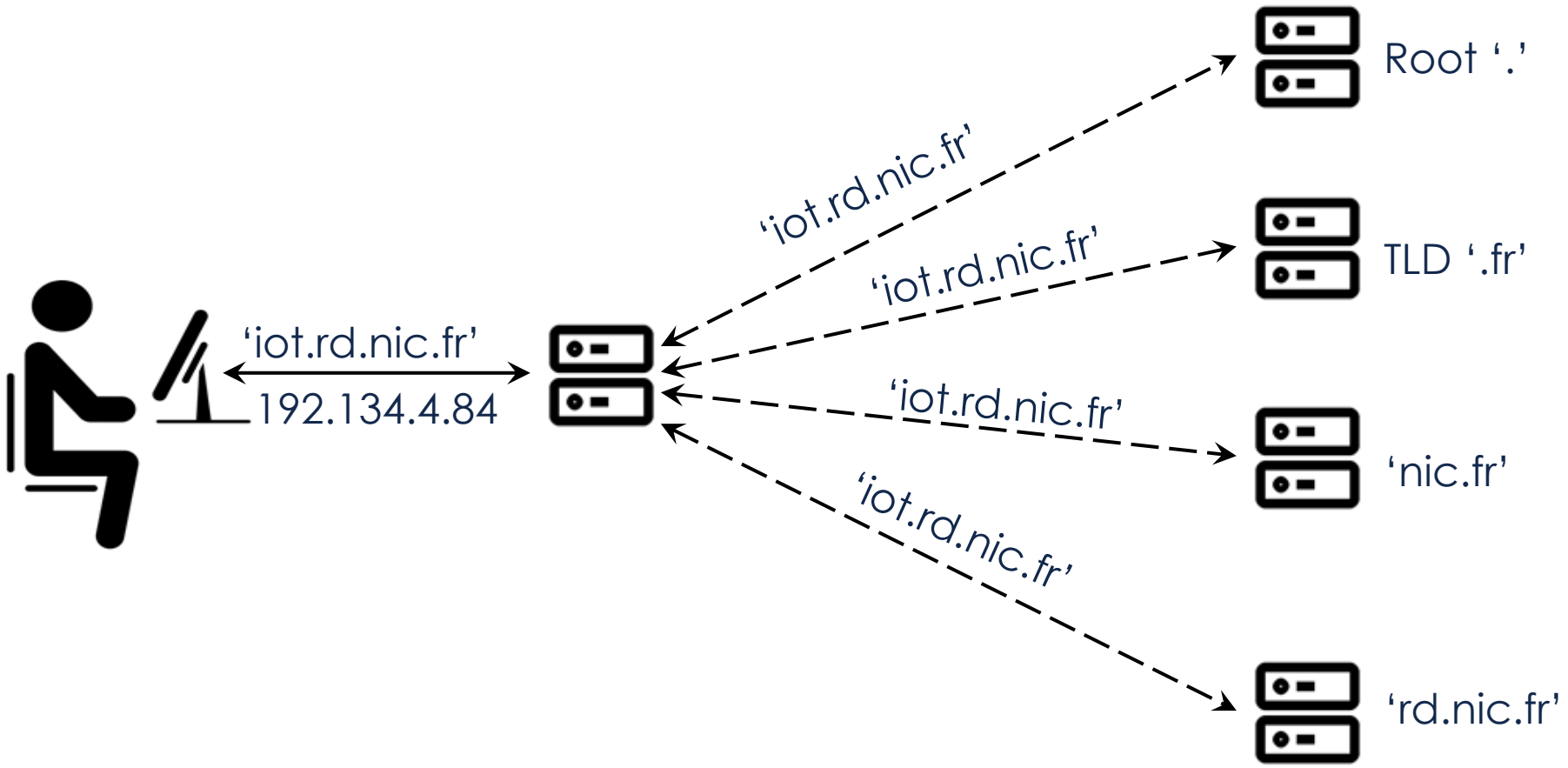
- User types the domain name ‘iot.rd.nic.fr’ in the browser tab
- The browser searches for the domain’s IP address in its cache
- If the IP address is not found, it asks the OS to resolve the domain’s IP address

Web browser -> Stub resolver



afnic | Labs

Recursive vs Iterative Query

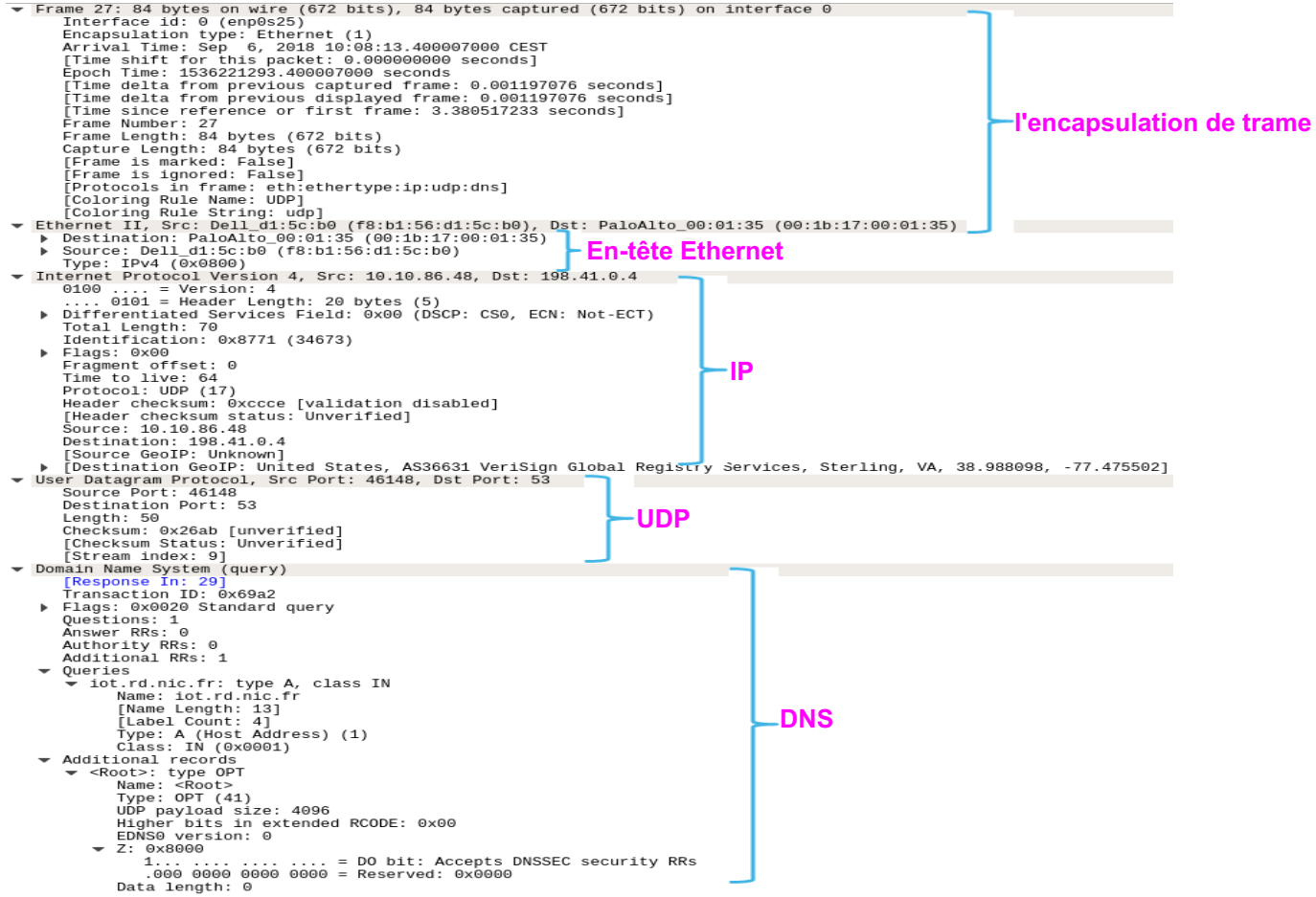


A view from Wireshark for 'iot.rd.nic.fr'

dns

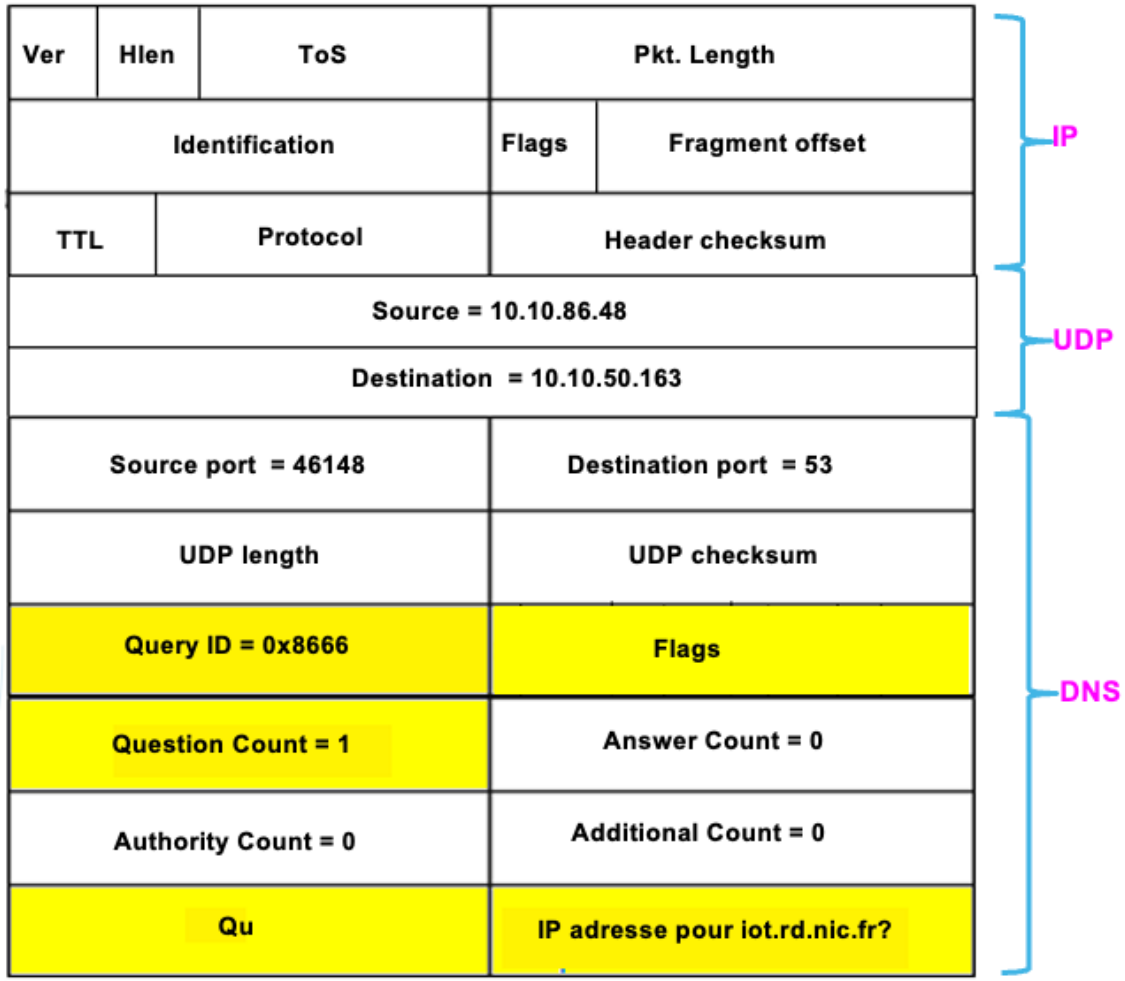
No.	Time	Source	Destination	Protocol	Length	Info
24	3.376011715	10.10.86.48	10.10.50.162	DNS	70	Standard query 0x8666 NS <Root> OPT
25	3.376021563	10.10.86.48	10.10.50.163	DNS	70	Standard query 0x8666 NS <Root> OPT
26	3.379320157	10.10.50.163	10.10.86.48	DNS	599	Standard query response 0x8666 NS <Root> NS m.root-servers.net NS b.root-servers.net NS k.root-servers.net NS
27	3.380517233	10.10.86.48	198.41.0.4	DNS	84	Standard query 0x69a2 A iot.rd.nic.fr OPT
28	3.381544874	10.10.50.162	10.10.86.48	DNS	1139	Standard query response 0x8666 NS <Root> NS a.root-servers.net NS b.root-servers.net NS c.root-servers.net NS
29	3.391674065	198.41.0.4	10.10.86.48	DNS	771	Standard query response 0x69a2 A iot.rd.nic.fr NS e.ext.nic.fr NS f.ext.nic.fr NS g.ext.nic.fr NS d.nic.fr NS
41	5.392571756	10.10.86.48	193.176.144.22	DNS	84	Standard query 0x724f A iot.rd.nic.fr OPT
42	5.411132162	193.176.144.22	10.10.86.48	DNS	580	Standard query response 0x724f A iot.rd.nic.fr NS ns3.nic.fr NS ns1.nic.fr NS ns6.ext.nic.fr NS ns2.nic.fr NS
43	5.411946369	10.10.86.48	10.10.50.163	DNS	70	Standard query 0x5cf6 A ns3.nic.fr
44	5.411980870	10.10.86.48	10.10.50.163	DNS	70	Standard query 0x7830 AAAA ns3.nic.fr
45	5.415349166	10.10.50.163	10.10.86.48	DNS	352	Standard query response 0x5cf6 A ns3.nic.fr A 192.134.0.49 NS ns1.ext.nic.fr NS ns1.nic.fr NS ns2.nic.fr NS r
46	5.416142770	10.10.50.163	10.10.86.48	DNS	352	Standard query response 0x7830 AAAA ns3.nic.fr AAAA 2001:660:3006:1::1:1 NS ns1.nic.fr NS ns6.ext.nic.fr NS r
47	5.416716514	10.10.86.48	10.10.50.163	DNS	70	Standard query 0xea33 A ns1.nic.fr
48	5.419495700	10.10.50.163	10.10.86.48	DNS	352	Standard query response 0xea33 A ns1.nic.fr A 192.134.4.1 NS ns3.nic.fr NS ns2.nic.fr NS ns6.ext.nic.fr NS ns
49	5.419711439	10.10.86.48	10.10.50.163	DNS	70	Standard query 0xbc5a AAAA ns1.nic.fr
50	5.422549781	10.10.50.163	10.10.86.48	DNS	352	Standard query response 0xbc5a AAAA ns1.nic.fr AAAA 2001:67c:2218:2::4:1 NS ns6.ext.nic.fr NS ns3.nic.fr NS r
51	5.422971970	10.10.86.48	10.10.50.163	DNS	74	Standard query 0x0842 A ns6.ext.nic.fr
52	5.422990827	10.10.86.48	10.10.50.163	DNS	74	Standard query 0x8704 AAAA ns6.ext.nic.fr
53	5.426147434	10.10.50.163	10.10.86.48	DNS	352	Standard query response 0x0842 A ns6.ext.nic.fr A 130.59.31.29 NS ns1.nic.fr NS ns6.ext.nic.fr NS ns1.ext.nic
54	5.426925883	10.10.50.163	10.10.86.48	DNS	352	Standard query response 0x8704 AAAA ns6.ext.nic.fr AAAA 2001:620:0:ff::2f NS ns1.ext.nic.fr NS ns3.nic.fr NS
55	5.427417215	10.10.86.48	10.10.50.163	DNS	70	Standard query 0x5353 A ns2.nic.fr
56	5.427448224	10.10.86.48	10.10.50.163	DNS	70	Standard query 0x7364 AAAA ns2.nic.fr
57	5.430539041	10.10.50.163	10.10.86.48	DNS	352	Standard query response 0x5353 A ns2.nic.fr A 192.93.0.4 NS ns2.nic.fr NS ns1.nic.fr NS ns6.ext.nic.fr NS ns3
58	5.431322099	10.10.50.163	10.10.86.48	DNS	352	Standard query response 0x7364 AAAA ns2.nic.fr AAAA 2001:660:3005:1::1:2 NS ns2.nic.fr NS ns1.ext.nic.fr NS r
59	5.431560886	10.10.86.48	10.10.50.163	DNS	74	Standard query 0xb684 A ns1.ext.nic.fr
60	5.431575483	10.10.86.48	10.10.50.163	DNS	74	Standard query 0x94f2 AAAA ns1.ext.nic.fr
61	5.434645906	10.10.50.163	10.10.86.48	DNS	352	Standard query response 0xb684 A ns1.ext.nic.fr A 193.51.208.13 NS ns6.ext.nic.fr NS ns1.nic.fr NS ns3.nic.fr
62	5.434653449	10.10.50.163	10.10.86.48	DNS	131	Standard query response 0x94f2 AAAA ns1.ext.nic.fr SOA dnsmaster.nic.fr
63	5.434917518	10.10.86.48	192.134.0.49	DNS	84	Standard query 0xb8d2 A iot.rd.nic.fr OPT
64	5.439661822	192.134.0.49	10.10.86.48	DNS	1412	Standard query response 0xb8d2 A iot.rd.nic.fr A 192.134.4.84 RRSIG NS ns2.rd.nic.fr NS ns3.nic.fr RRSIG A 19

Wireshark view - Layers

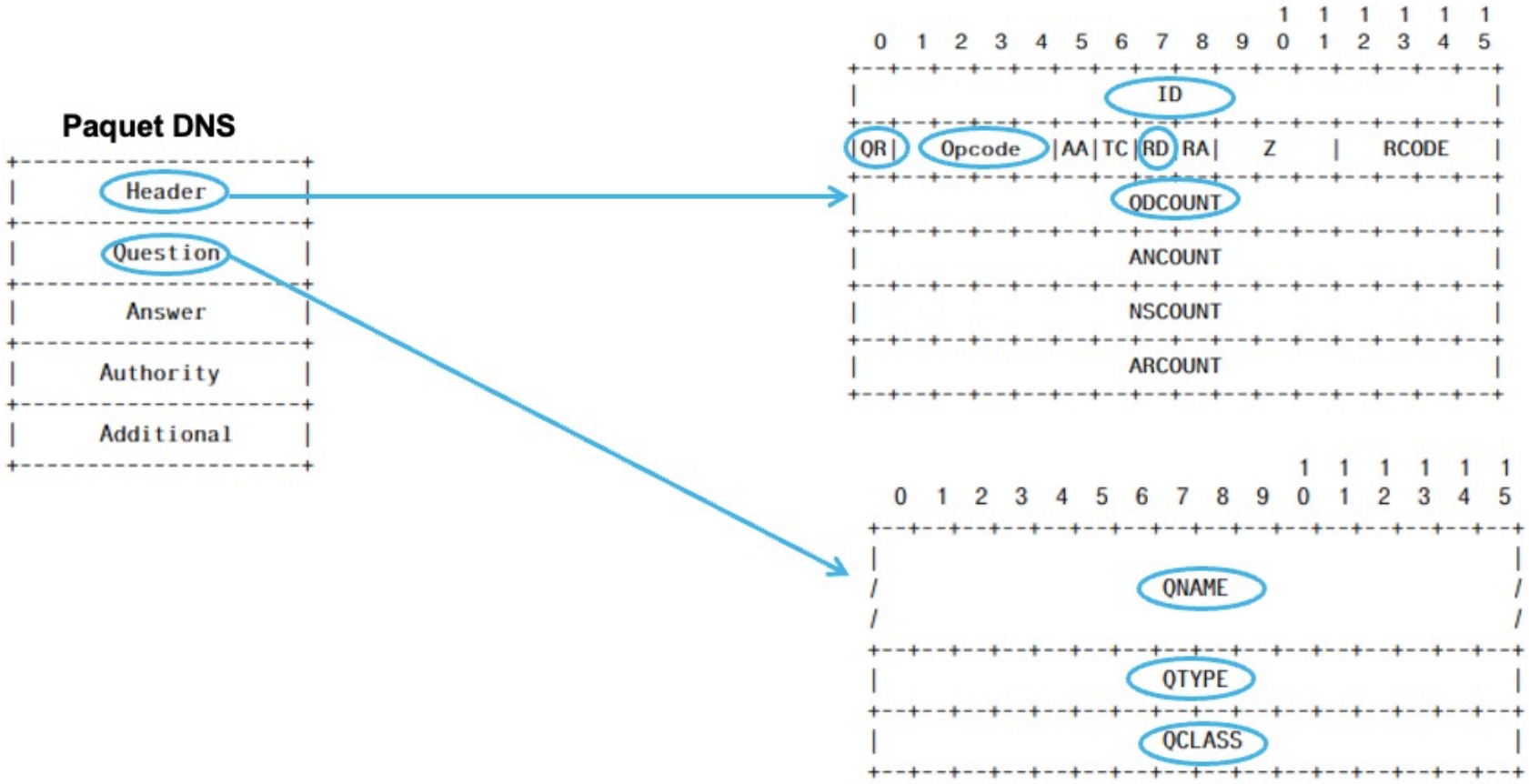


afnic | Labs

Wire format - DNS

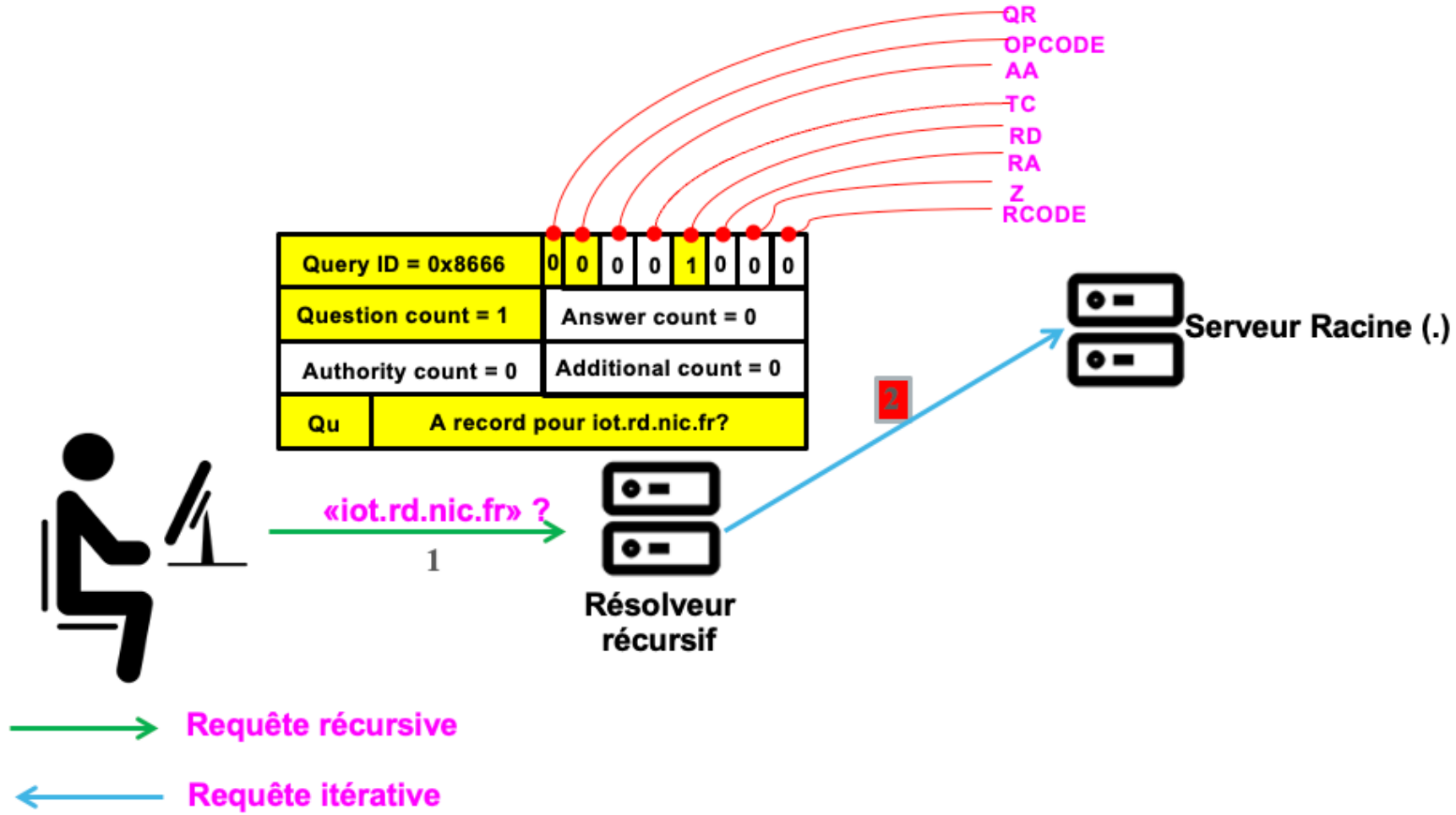


DNS Packet structure

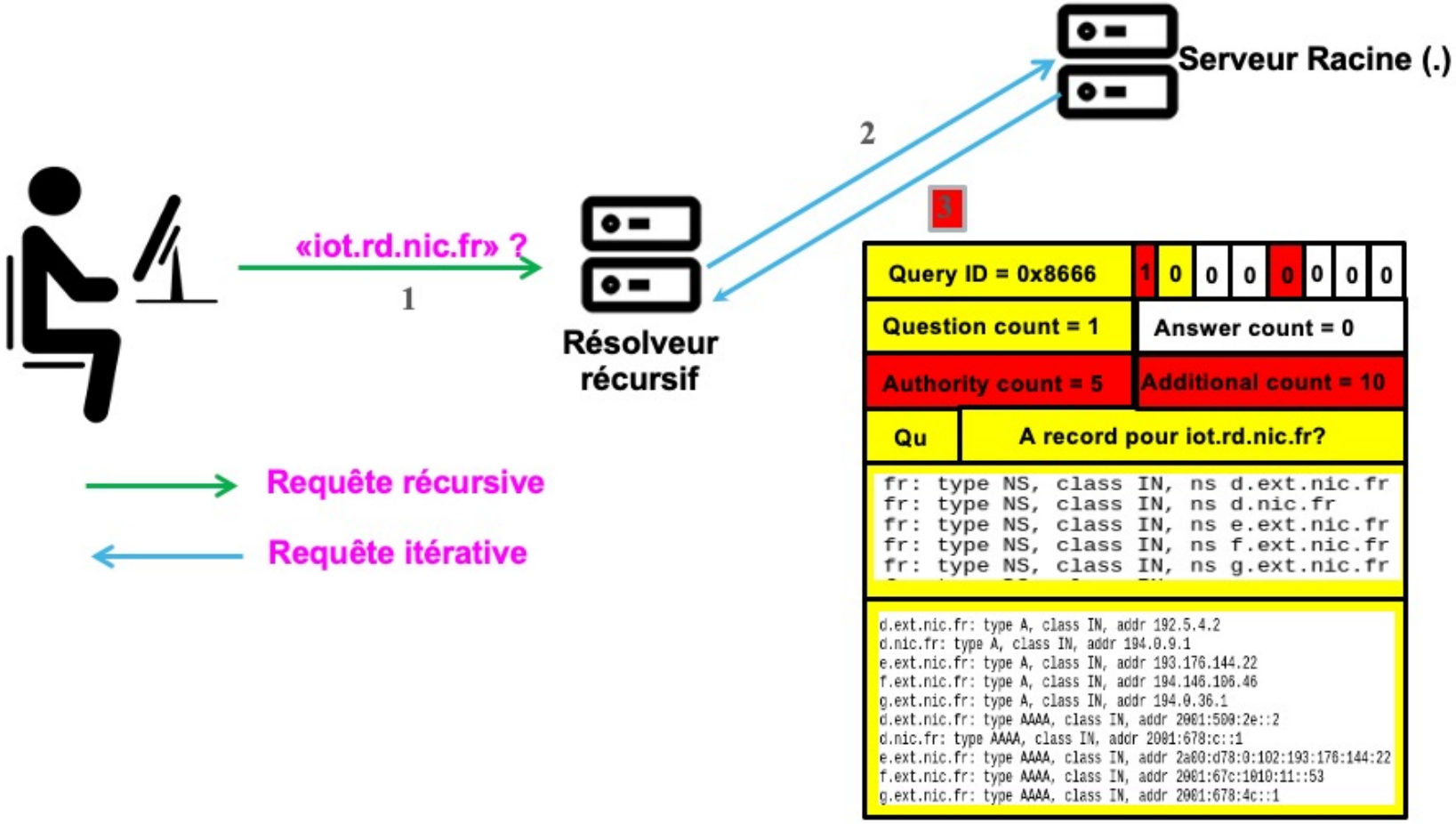


Fields required to resolve an IP address

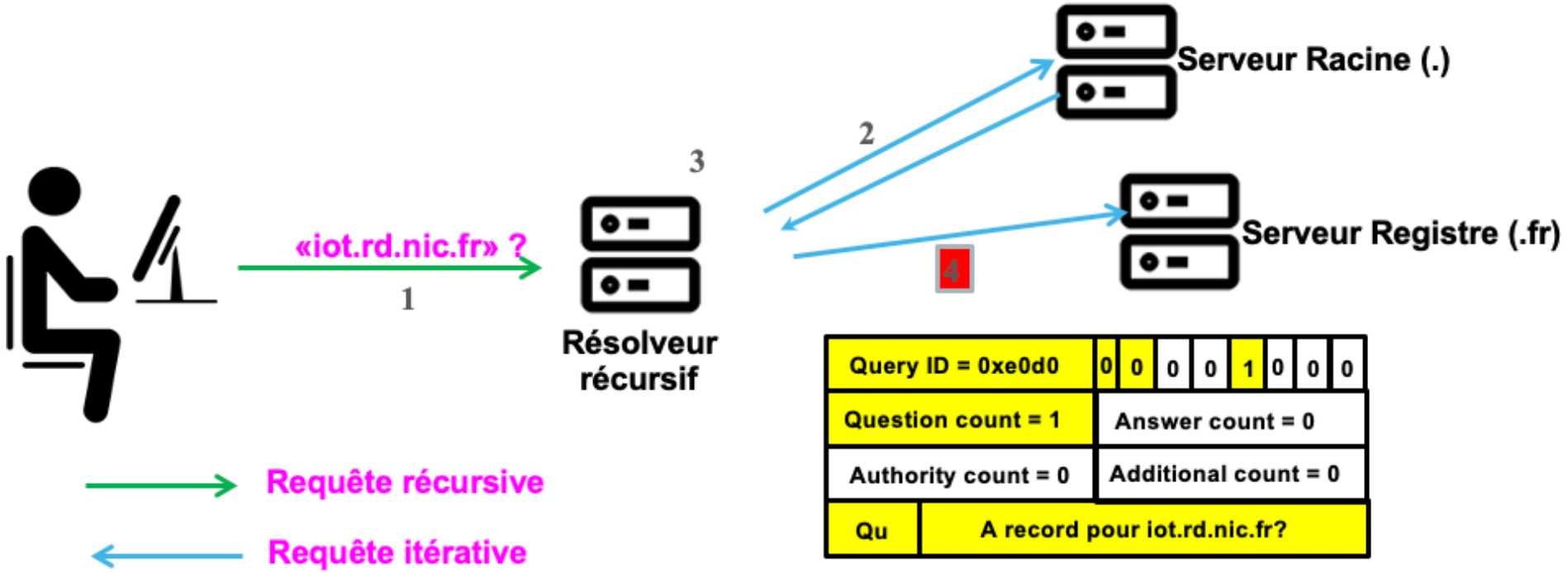
Resolver -> DNS root



Root -> Resolver

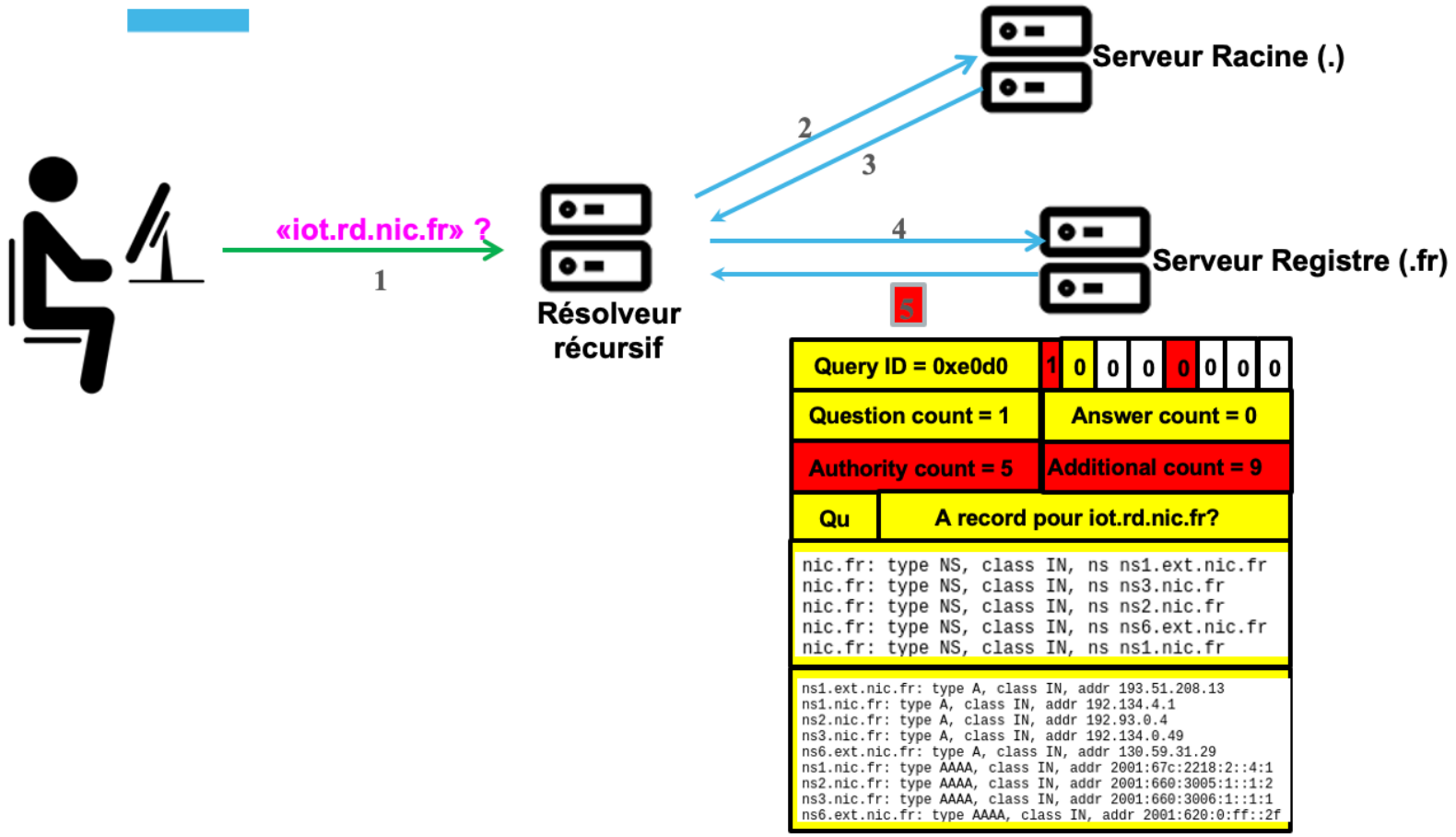


Resolver -> '.fr' Authoritative server

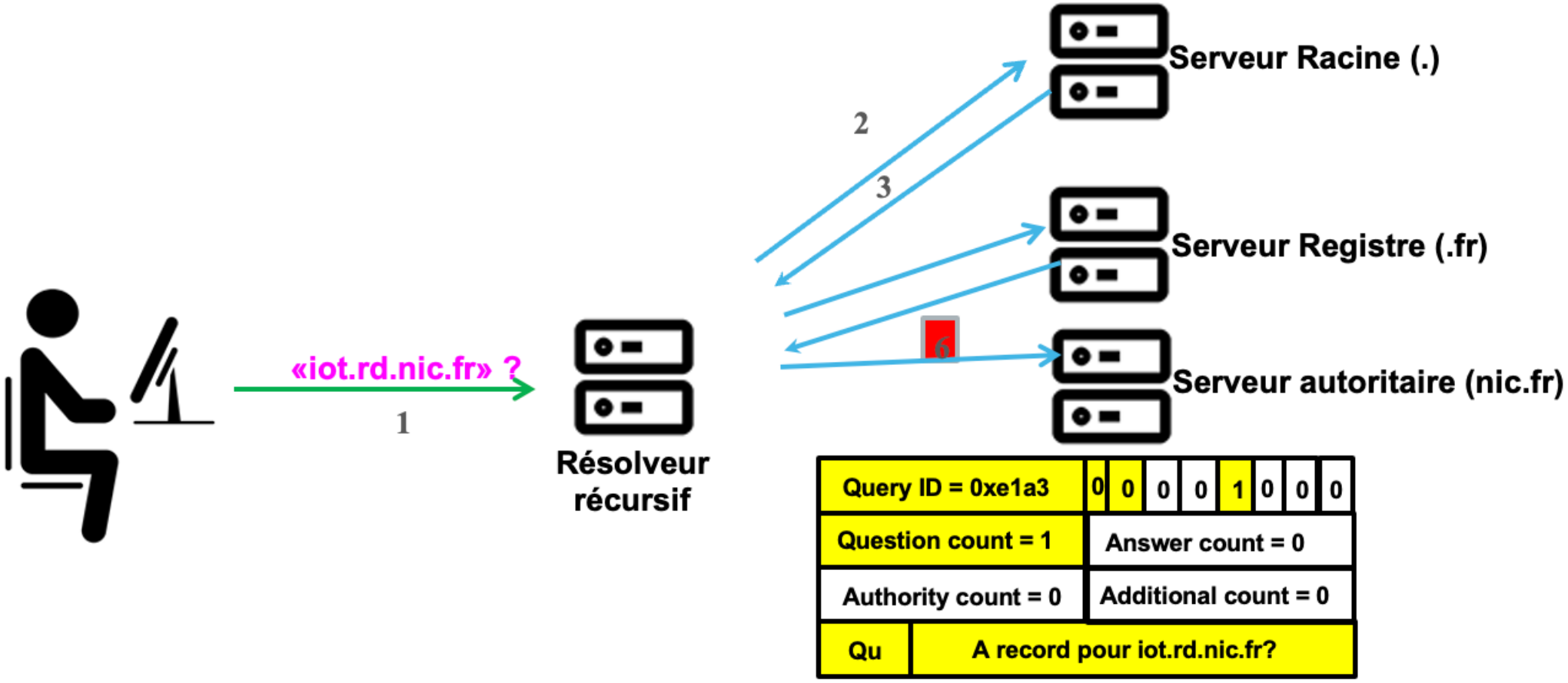


Query ID = 0xe0d0	0	0	0	0	1	0	0	0
Question count = 1	Answer count = 0							
Authority count = 0	Additional count = 0							
Qu	A record pour iot.rd.nic.fr?							

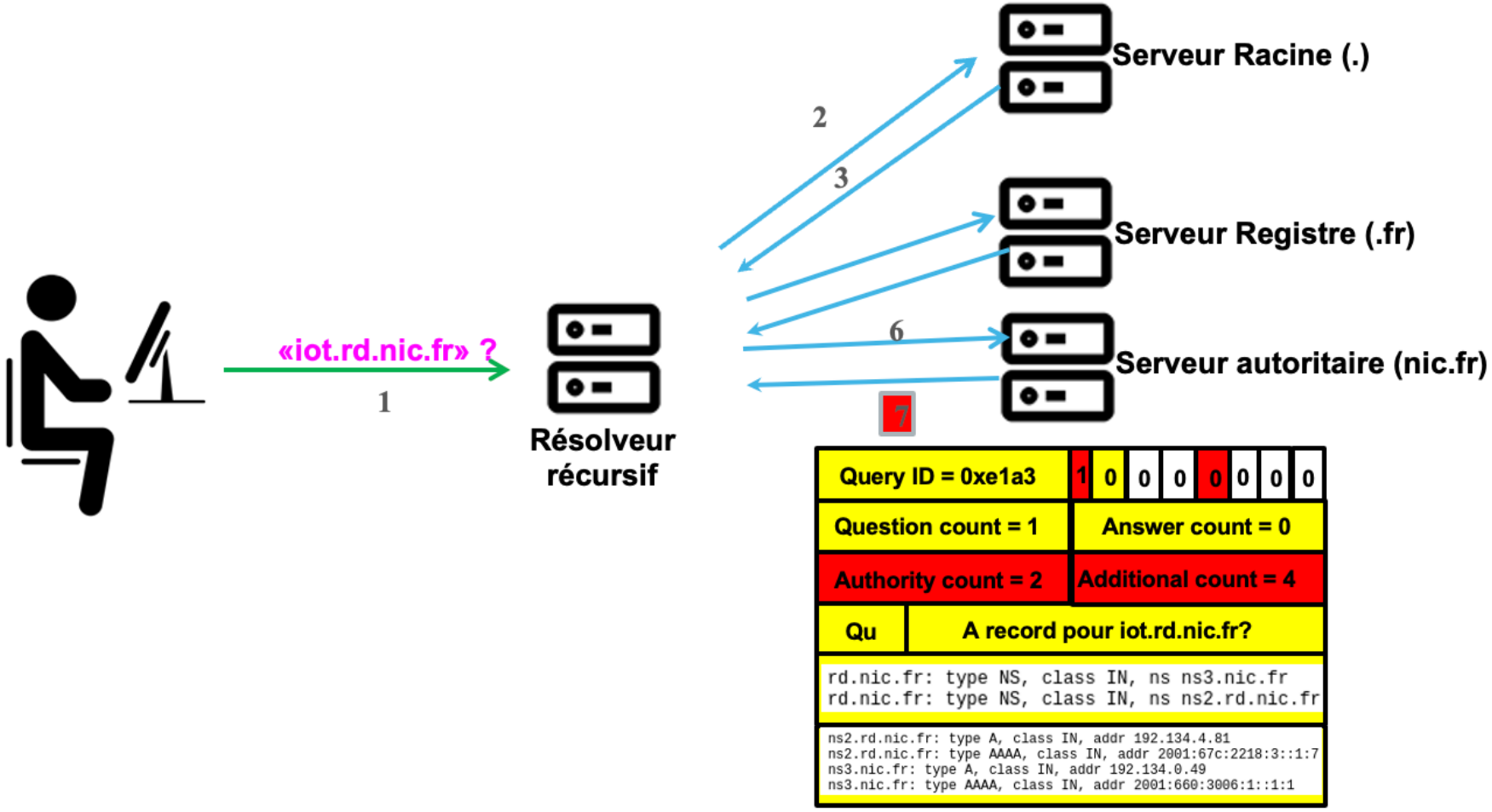
.fr Authoritative Server -> Resolver



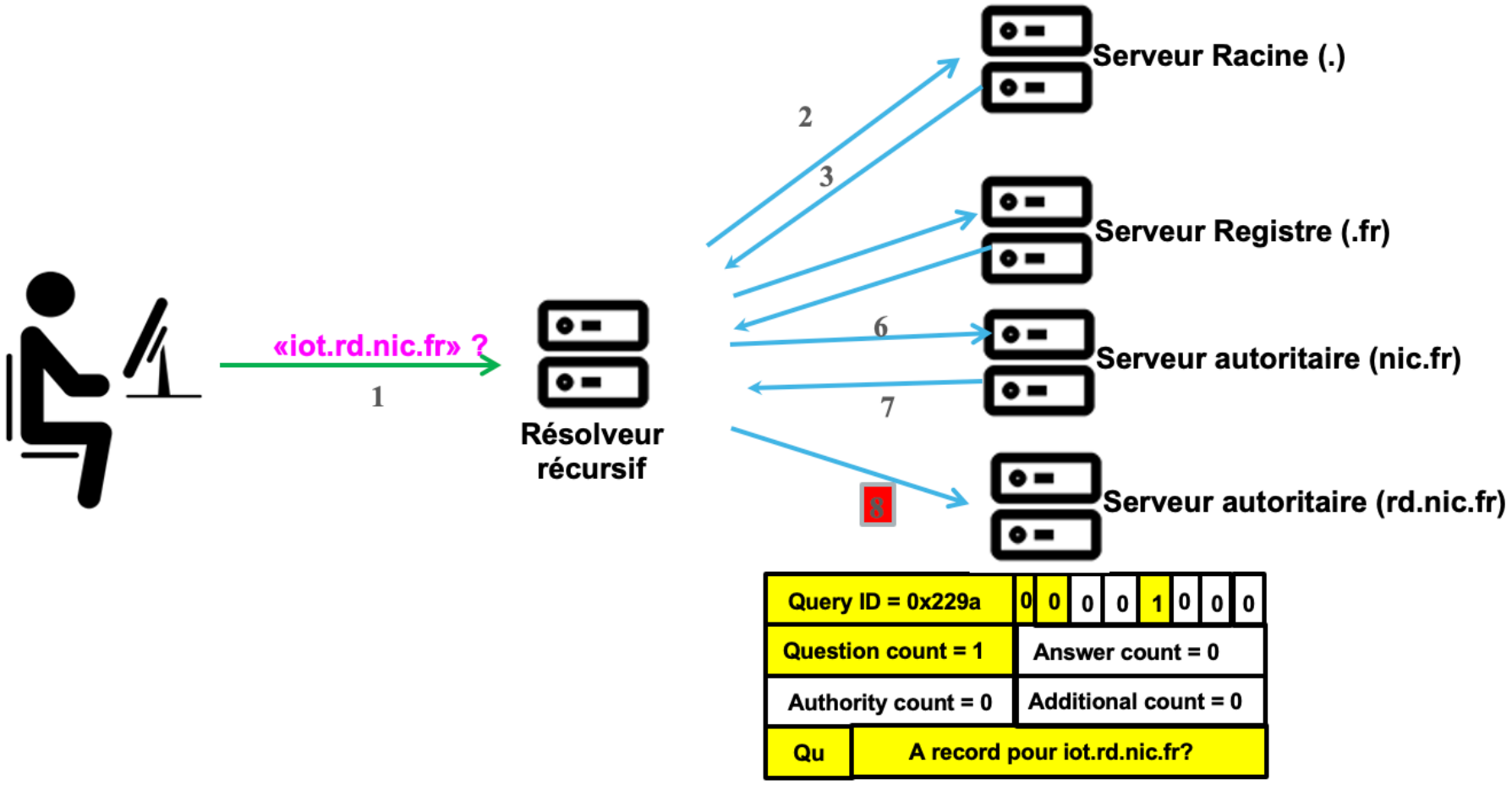
Resolver -> ‘nic.fr’ authoritative server



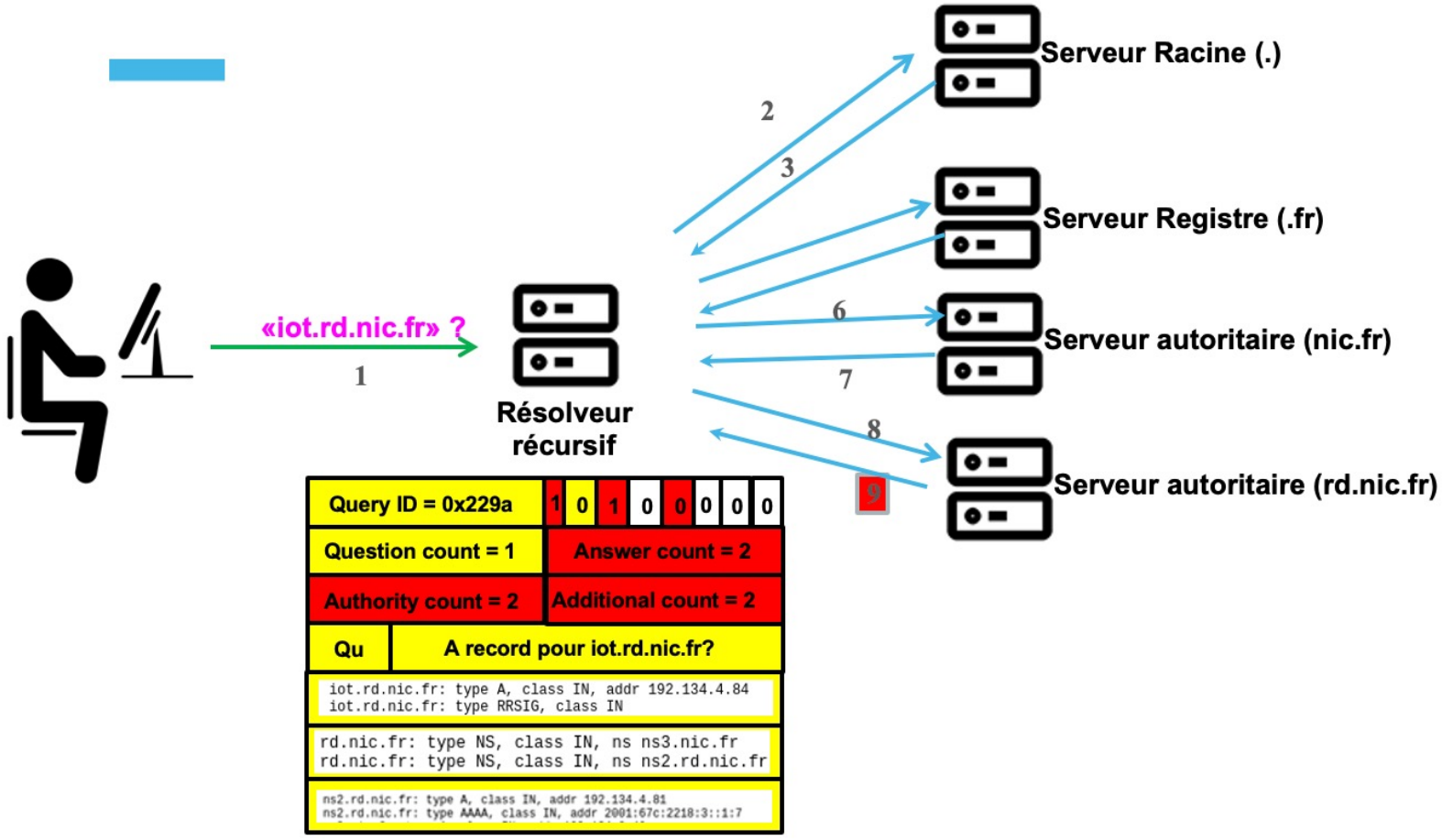
‘nic.fr’ authoritative server -> Resolver



Resolver -> ‘rd.nic.fr’ authoritative server



‘rd.nic.fr’ authoritative server -> resolver

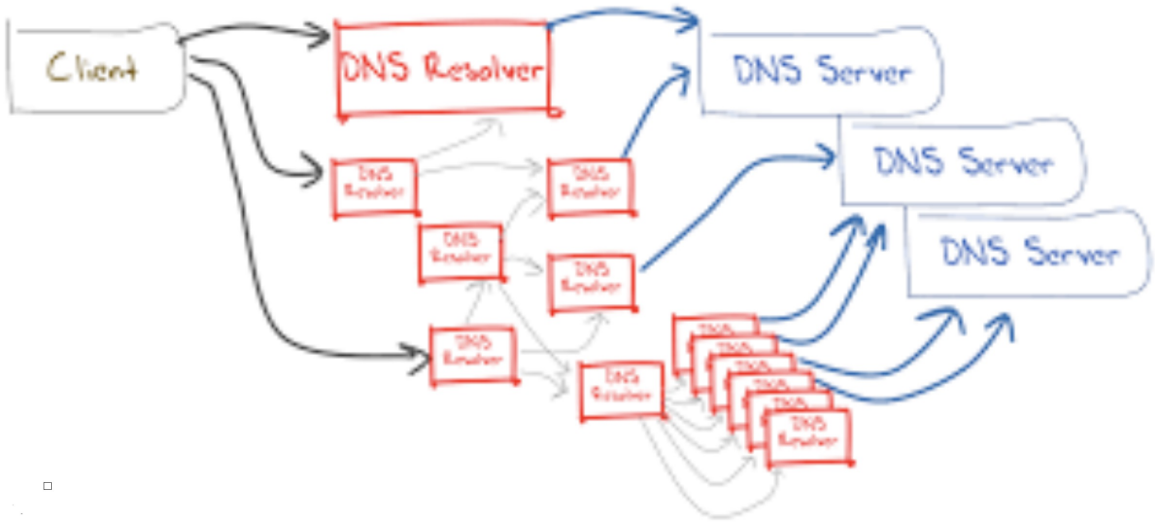


Privacy

Privacy (UK: /ˈprɪvəsiː/, US: /ˈpraɪ-/)[1][2] is the ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively.

Source: httpswikipedia.org

Privacy in DNS



Source: ISP Column September 2018

- Clear text
- DNS resolution is quite talkative
- DNS information could be used for Business intelligence as well as surveillance

```
15:29:24.409283 IP6 2001:67c:1348:8002::7:107.10127 > \
    2001:4b98:dc2:45:216:3eff:fe4b:8c5b.53: 32715+ [1au] \
    AAAA? www.armenpress.am. (46)
```

afnic | Labs

Inference from DNS queries

Device	DNS Queries
Sense Sleep Monitor	hello-audio.s3.amazonaws.com hello-firmware.s3.amazonaws.com messeji.hello.is ntp.hello.is sense-in.hello.is time.hello.is
Nest Security Camera	nexus.dropcam.com oculus519-vir.dropcam.com pool.ntp.org
WeMo Switch	prod1-fs-xbcs-net-1101221371. us-east-1.elb.amazonaws.com prod1-api-xbcs-net-889336557. us-east-1.elb.amazonaws.com
Amazon Echo	ash2-accesspoint-a92.ap.spotify.com audio-ec.spotify.com device-metrics-us.amazon.com ntp.amazon.com pindorama.amazon.com softwareupdates.amazon.com

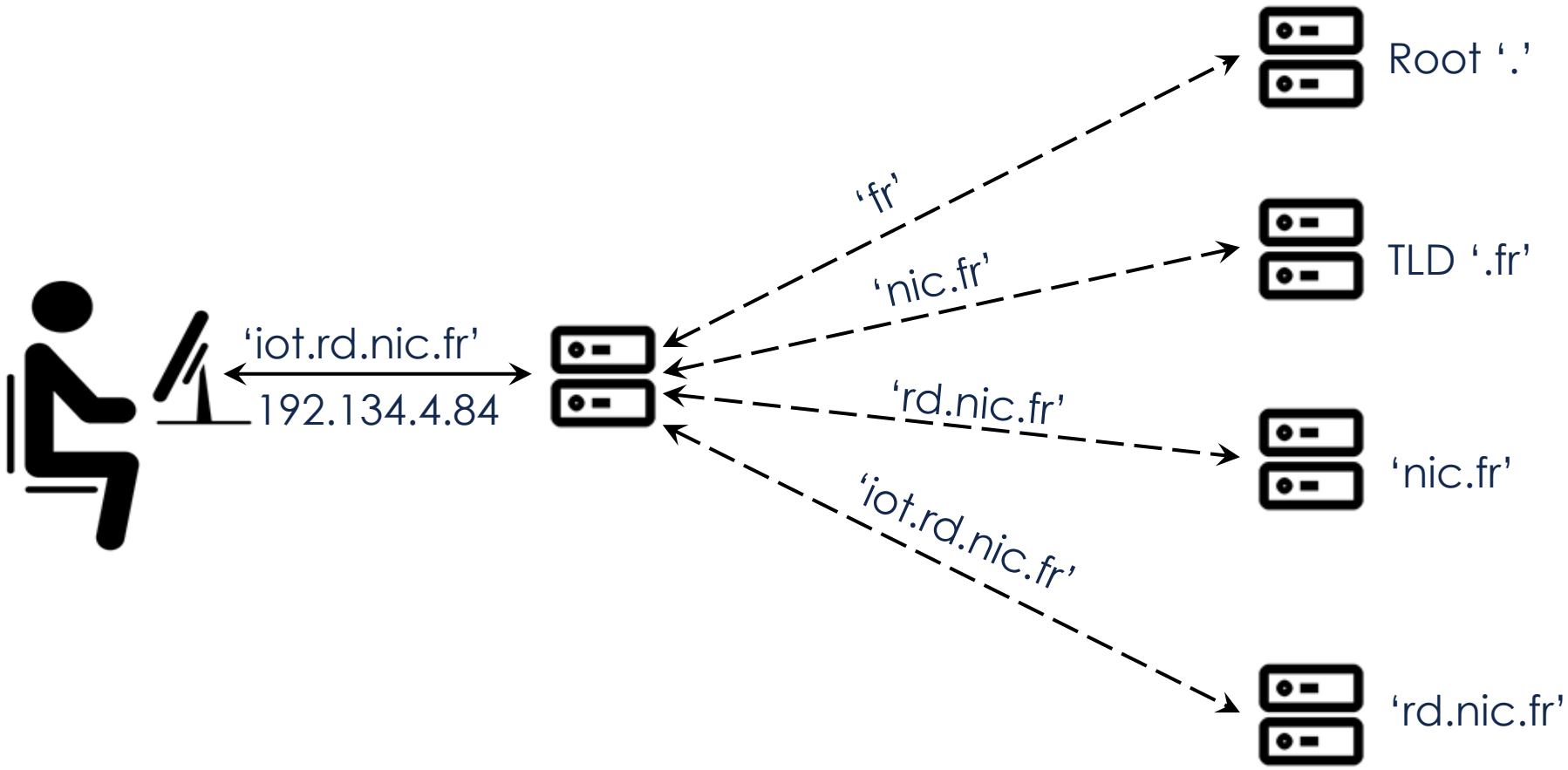
Source: A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic

afnic | Labs

Efforts to improve Privacy in DNS

- RFC 7626 – DNS privacy considerations
- RFC 7816 – DNS Query name minimisation to improve privacy
- RFC 9156 – Obsoletes RFC 7816

With QNAME minimisation



Configuring QNAME minimisation

- BIND - qname-minimization - (off, relaxed, strict)
- Unbound – qname-minimization – (yes,no)
- Knot – NO_MINIMIZE –(on,off)

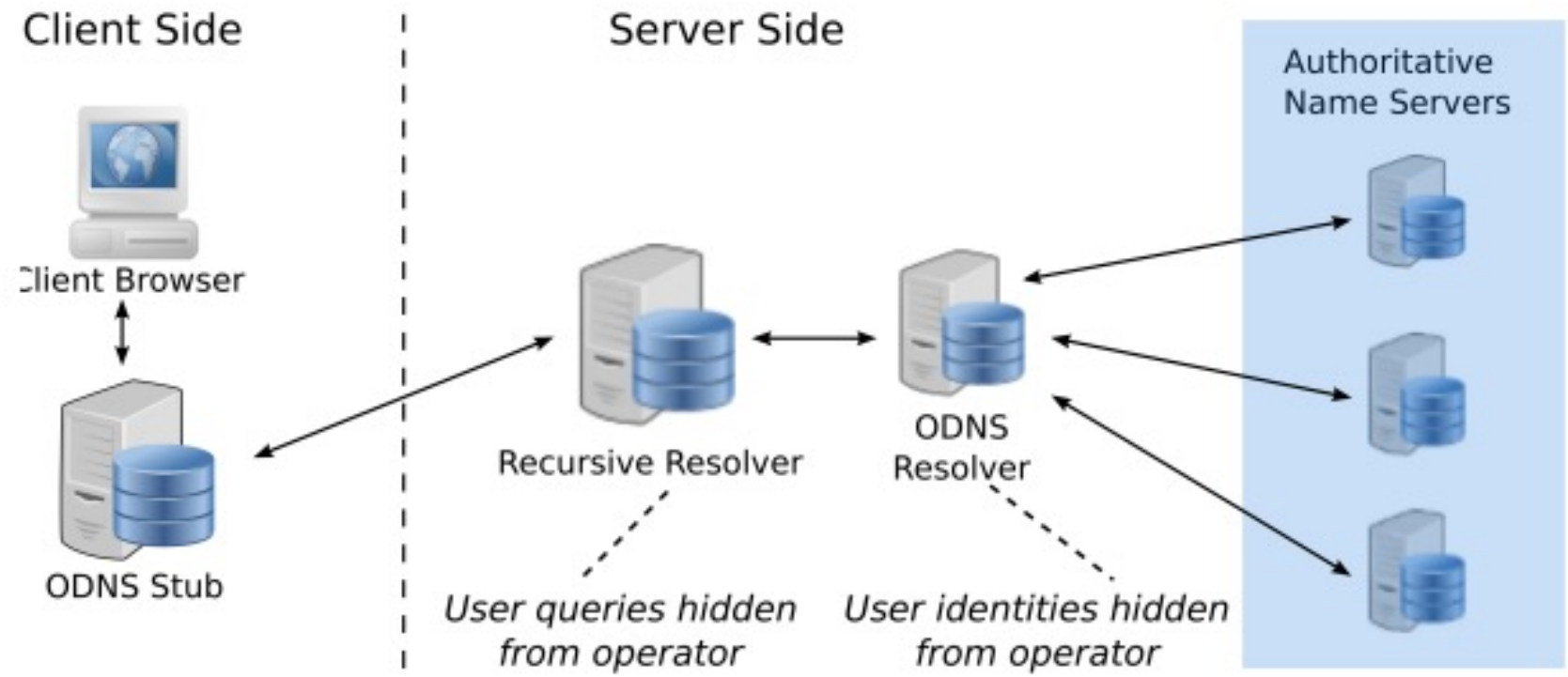
afnic | Labs

QNAME minimisation in action

```
/Users/sandoche $ dig @ns2.vainavi.net +nodnssec +short TXT qnamemintest.internet.nl
a.b.qnamemin-test.internet.nl.
"NO - QNAME minimisation is NOT enabled on your resolver :("
/Users/sandoche $ dig @ns8.maharashtra.gov.in +nodnssec +short TXT qnamemintest.internet.nl
a.b.qnamemin-test.internet.nl.
"HOORAY - QNAME minimisation is enabled on your resolver :)!"
```

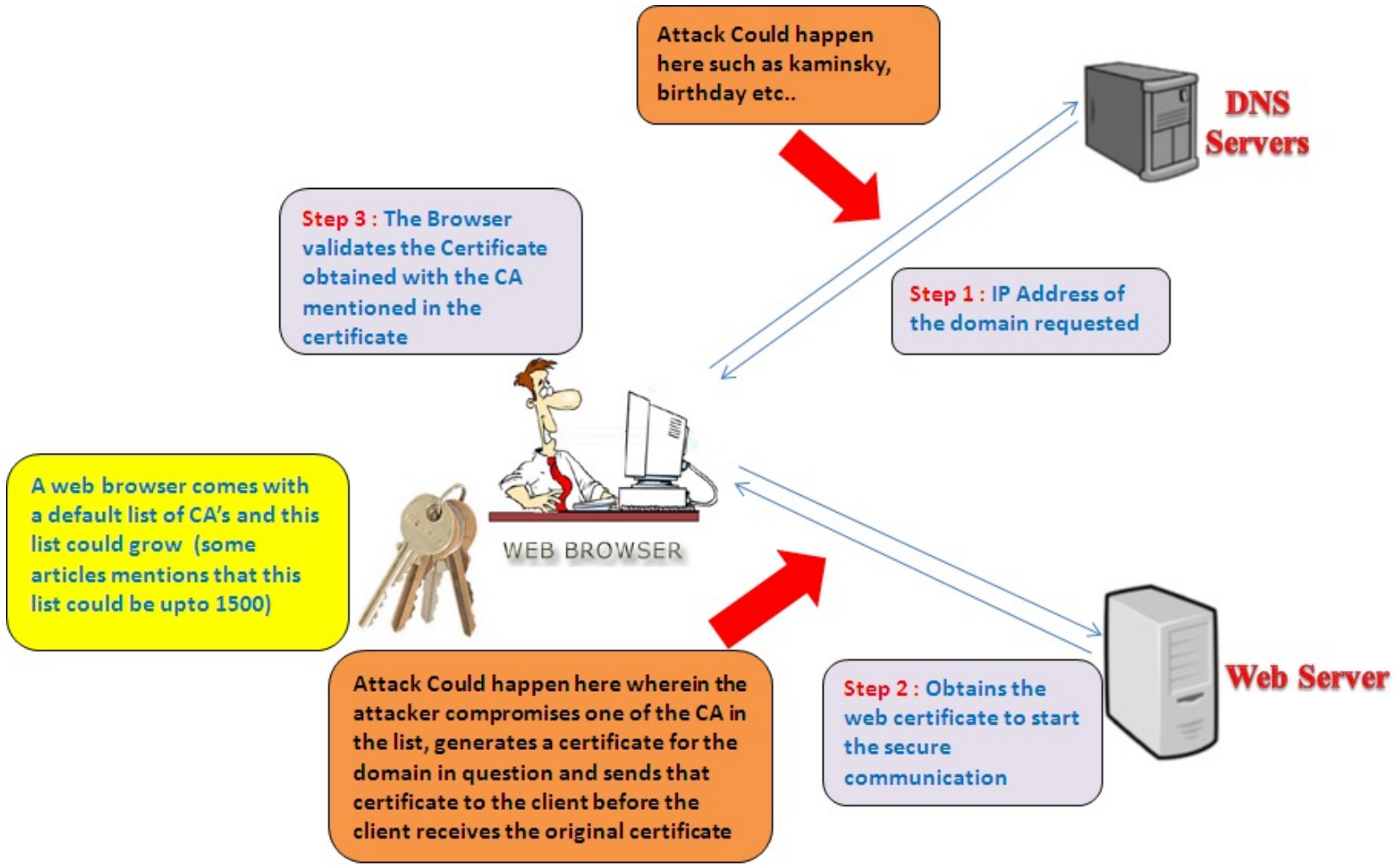
afnic | Labs

DNS

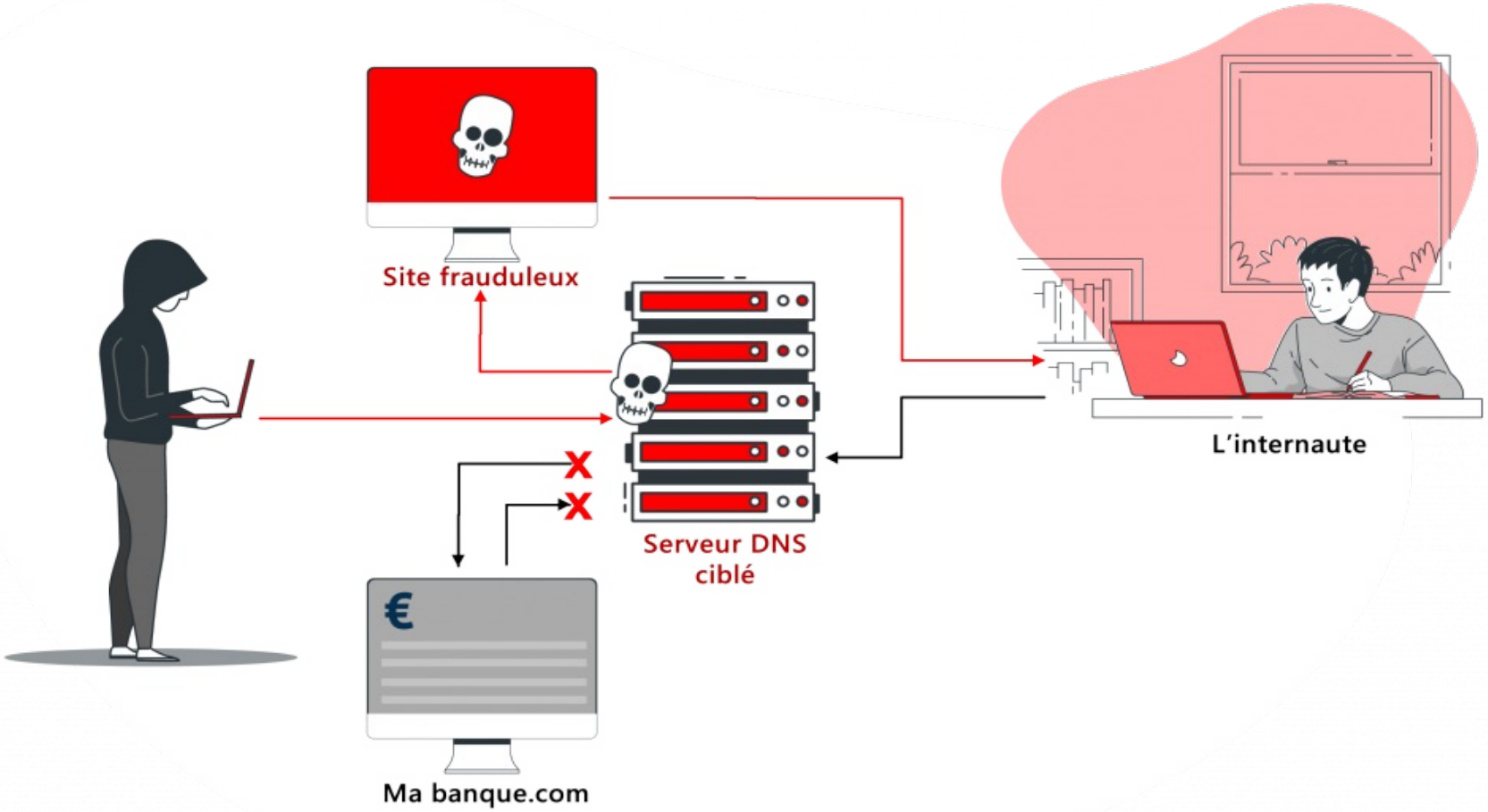


Source: Oblivious DNS: Practical Privacy for DNS Queries

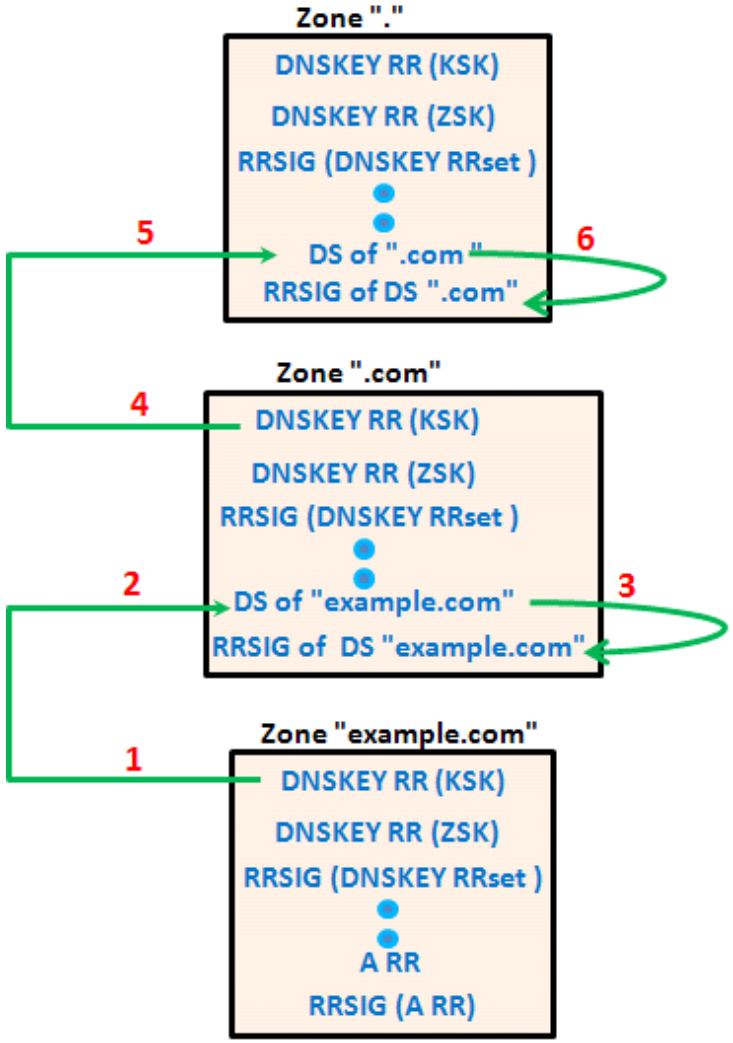
Attack scope in Web resolution



DNS Spoofing

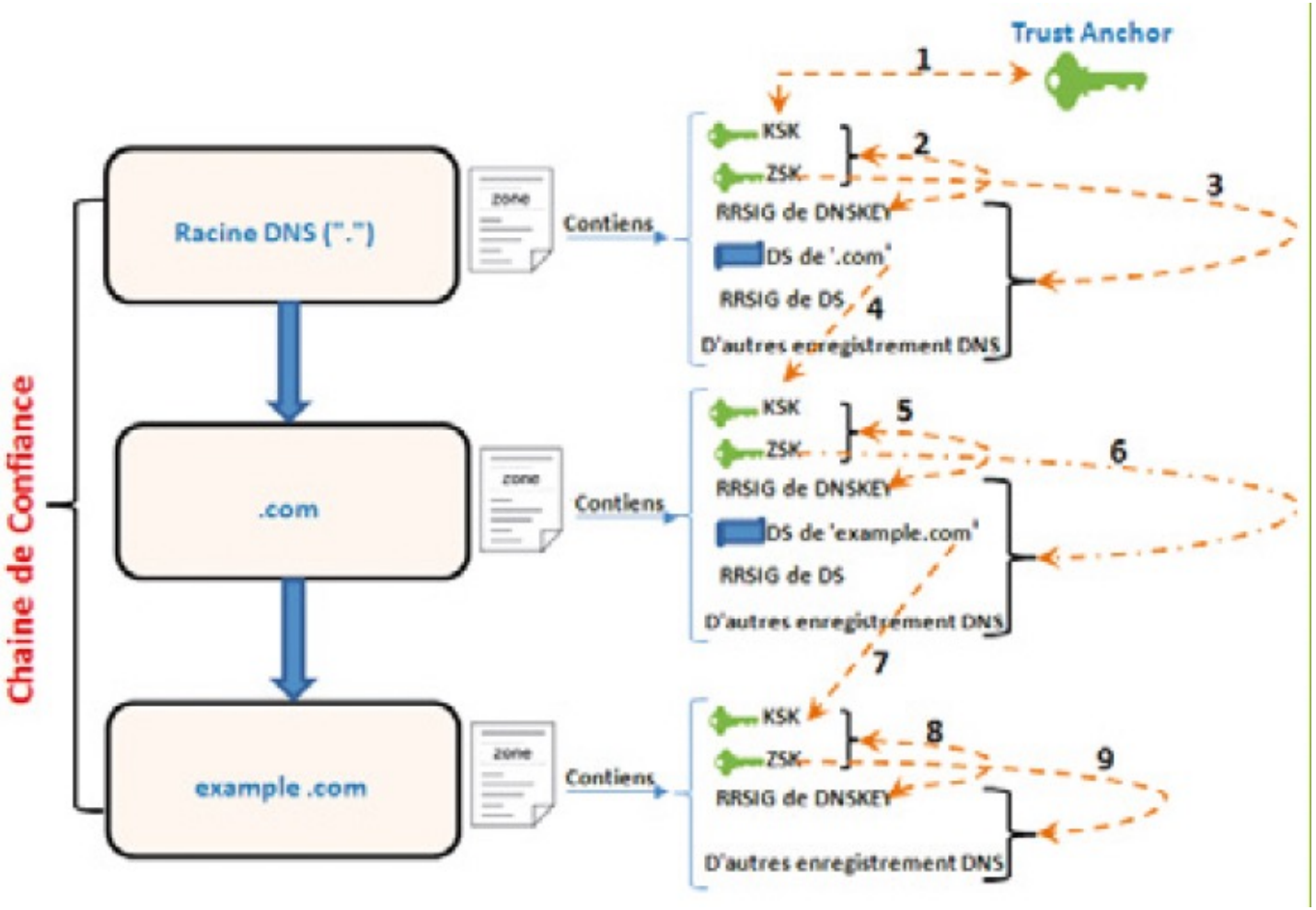


DNSSEC Trust chain - Creation



afnic | Labs

DNSSEC Trust chain - Verification



DNS

```
/Users/sandoche $ dig DS afnic.fr +trace

; <<>> DiG 9.10.6 <<>> DS afnic.fr +trace
;; global options: +cmd
.                       518372  IN      NS      m.root-servers.net.
.                       518372  IN      NS      g.root-servers.net.
.                       518372  IN      NS      l.root-servers.net.
.                       518372  IN      NS      i.root-servers.net.
.                       518372  IN      NS      j.root-servers.net.
.                       518372  IN      NS      b.root-servers.net.
.                       518372  IN      NS      e.root-servers.net.
.                       518372  IN      NS      a.root-servers.net.
.                       518372  IN      NS      d.root-servers.net.
.                       518372  IN      NS      k.root-servers.net.
.                       518372  IN      NS      h.root-servers.net.
.                       518372  IN      NS      f.root-servers.net.
.                       518372  IN      NS      c.root-servers.net.
.                       518376  IN      RRSIG   NS 8 0 518400 20231112050000 20231030040000 46780 . KOSvh8dmDkcY070FSYz+vAkH6BC+ZR4nGbEu0plshkZZX47oFXFpsHTJ /LiU7G7KXp6gE+g+QDcHk/HPEljGFNY5RwvzQaCjHGG063
ypr+Huj1vJ 0SR03fSwm1FALKZ0EFNI2aIfpxY/1S8xc2HzZmHuneQcp7mTY7i+KtOY z8ljk2jQbdCjHYPg/AgIPtF2+507LnFScSCTw+zOVFYFktoPHyy/wDIk 3G0VQQIQG5+1kjn7YZl1yuyxiSqJhq1+7tSkrL3AKhA4fJtynJcBbZsw dq3mVHPfARjUjby2WNt/M
2clERoo+W/zYsZpkKamUpvTNm6gYnnt2xUV 8F5/Ow==
;; Received 1109 bytes from 10.1.50.163#53(10.1.50.163) in 20 ms

fr.                     172800  IN      NS      f.ext.nic.fr.
fr.                     172800  IN      NS      d.nic.fr.
fr.                     172800  IN      NS      e.ext.nic.fr.
fr.                     172800  IN      NS      g.ext.nic.fr.
fr.                     86400   IN      DS      29133 13 2 1303E8DA8FB60DB500D5BEA1EE5DC9A2BCC93DFE2FC43D346576658F ECCF5749
fr.                     86400   IN      RRSIG   DS 8 1 86400 20231112050000 20231030040000 46780 . OLTR+EzZjrUdYBEhgO4gAq3cgupnnuR3rP83+t6xOJz4ppKMw+gdBIT3 V57PEljOLe+UeWp7L9UMvLqjhKBlDuY35h8g/yk8GZGA85S
1/YIiQaN9 Got4nvnMbqnfyXhHwpnk5BQFqhSirHybzGd26TBXcn/Q2eh2WQ916Kd/ EKaUn7fnmzTkp62K9H/rVxvt6H1Osl1WQEOFKh8qvuf3vgwaI/STVU+j VzsUxUjG6WBDW8PDEEkEsasE41iw3f9UNBqaNliM1tcnPHeQ7fa2+CU1 V8X7tL41V/rdFPpwIRJg0l
KgjeUp8ThlLGfPFPhlKVYNn73grNGp8t+8 zisv8Q==
;; Received 628 bytes from 202.12.27.33#53(m.root-servers.net) in 11 ms

afnic.fr.               3600    IN      DS      53080 13 2 EF2DC0C8CF1FDF2994E8C771E0F871949B83AF41A1BF594B484677F5 A85A657B
afnic.fr.               3600    IN      RRSIG   DS 13 2 3600 20231119153910 20230915134840 60747 fr. PuOWQnOQ5R+g16RCVHYvW0omQ5te4I/I7AW30OBVXNppiSNAlm47Gsde 9jdbUI6ao6KkAkzoQAbSrrn7VyoG/w==
;; Received 183 bytes from 194.146.106.46#53(f.ext.nic.fr) in 17 ms
```

afnic | Labs

DNS

```
/Users/sandoche $ dig afnic.fr +dnssec

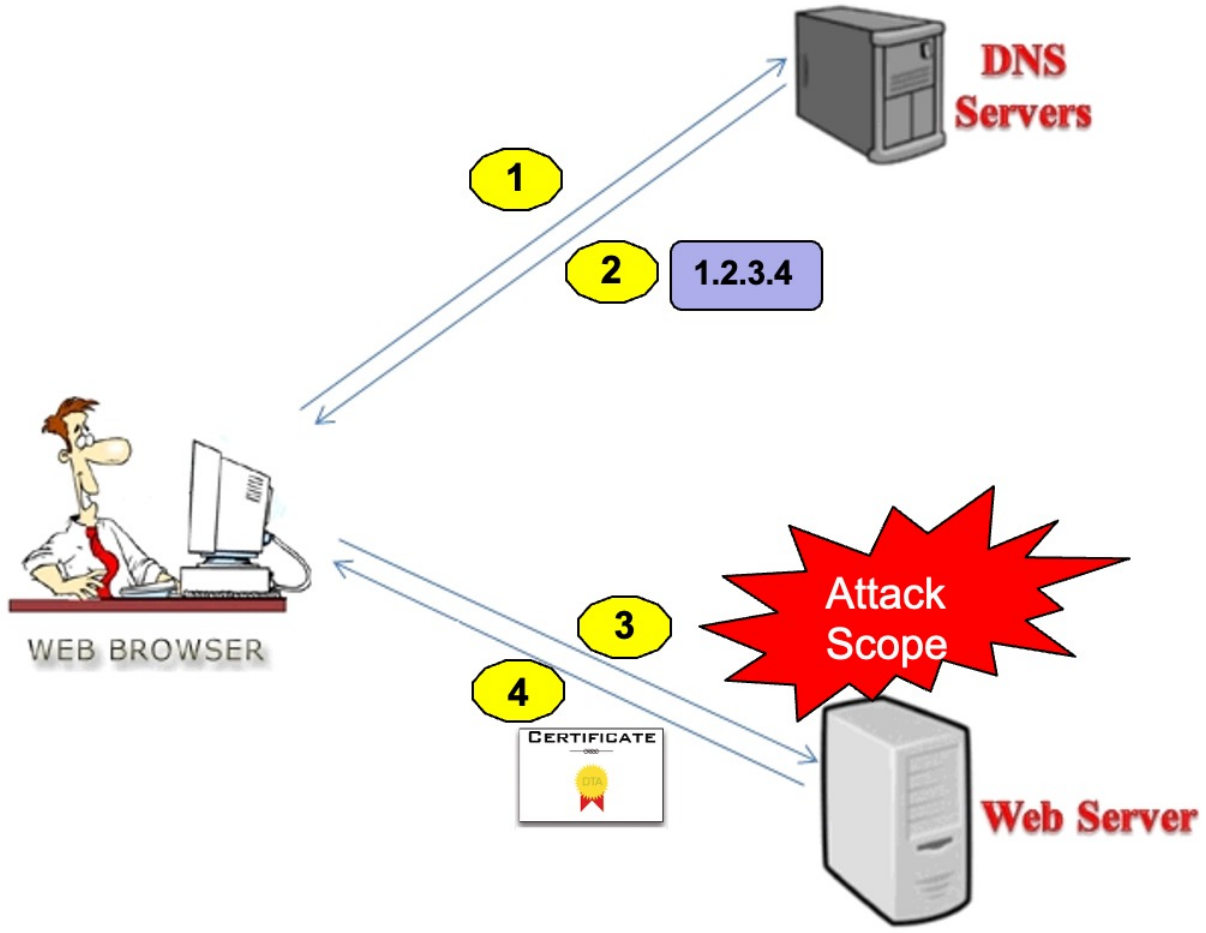
; <<>> DiG 9.10.6 <<>> afnic.fr +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15666
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
;; QUESTION SECTION:
;afnic.fr.                      IN      A

;; ANSWER SECTION:
afnic.fr.               600     IN      A       192.134.5.37
afnic.fr.               600     IN      RRSIG   A 13 2 600 20231127165743 20231028210743 50425 afnic.fr. ASrDVLjlkCNgUQ+IBZxxmm2mhHQeGgDUmHCR3L5/Pb+UBbhvMmSu8UcU xYJgfvTC4jiasCnsMcIU0JbDMPTk4w==

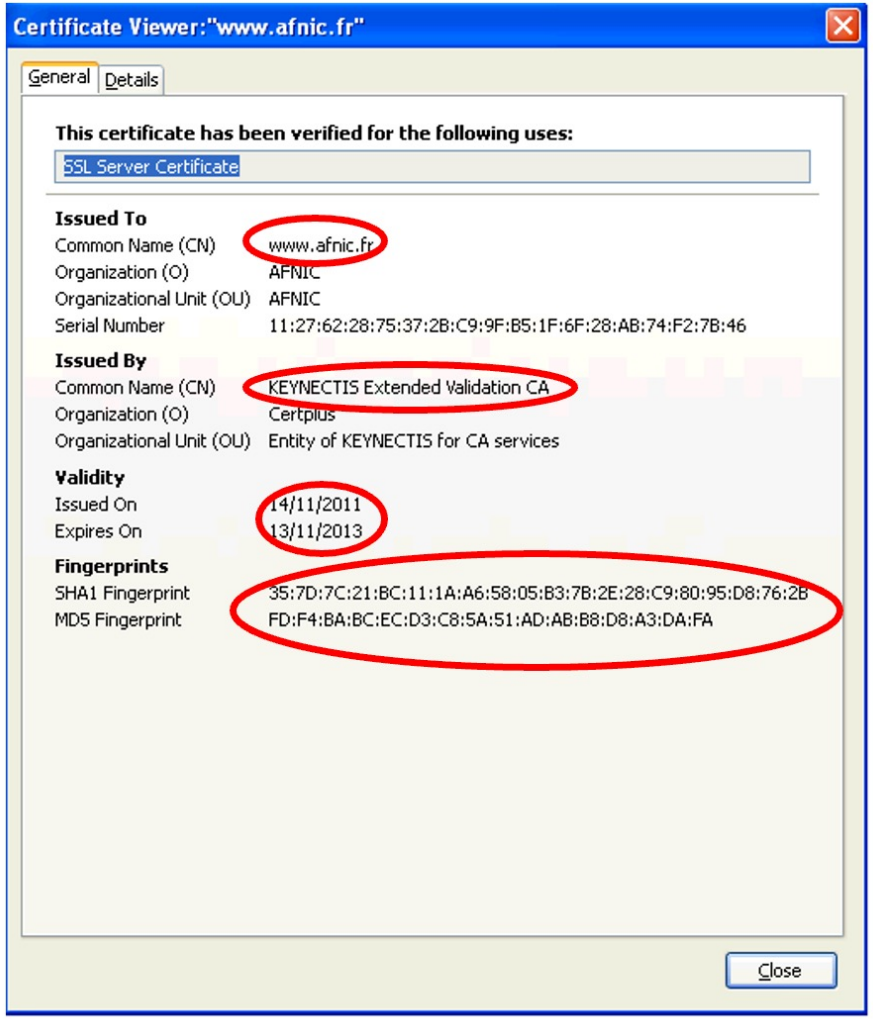
;; Query time: 55 msec
;; SERVER: 10.1.50.163#53(10.1.50.163)
;; WHEN: Mon Oct 30 09:20:58 CET 2023
;; MSG SIZE  rcvd: 157
```

X.509 Certificate validation – attack scope



afnic | Labs

CA Certificate

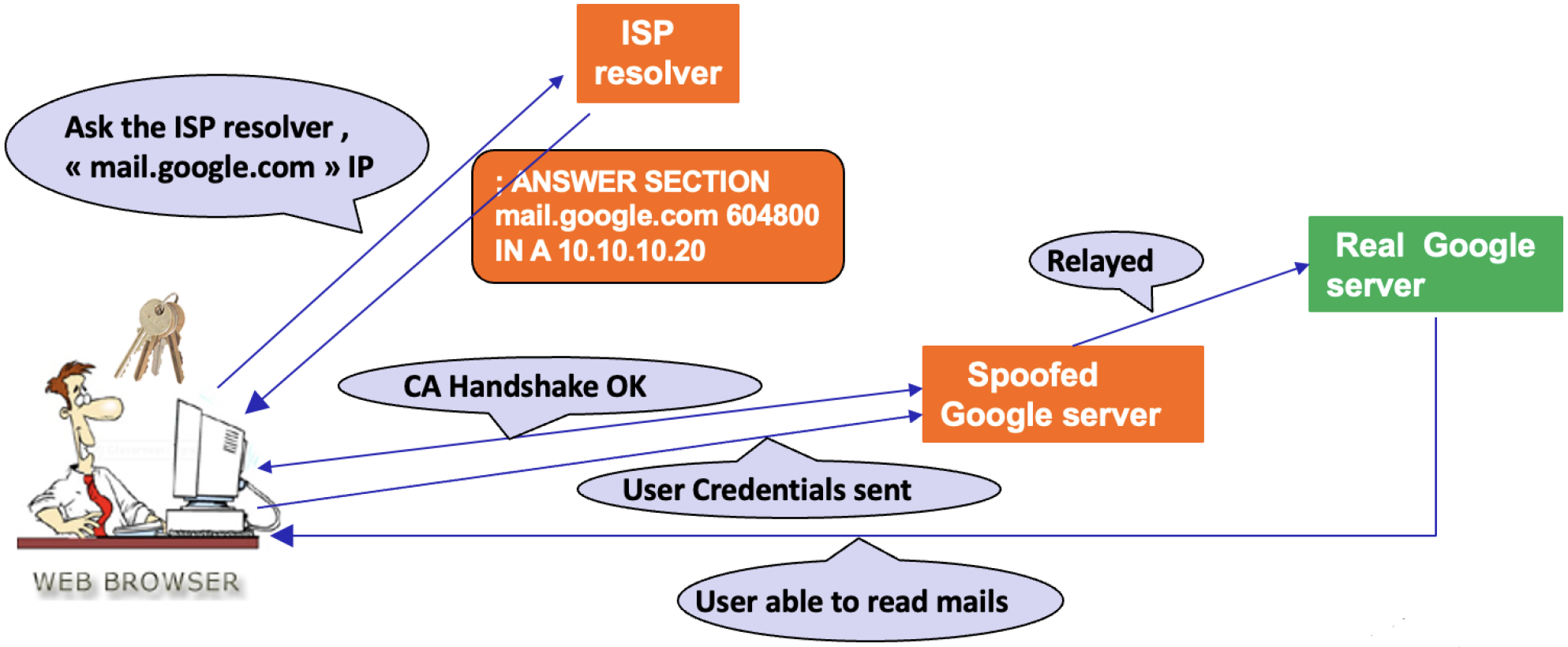


afnic | Labs

CA Root Certificates - The problem of many



Comodo attack

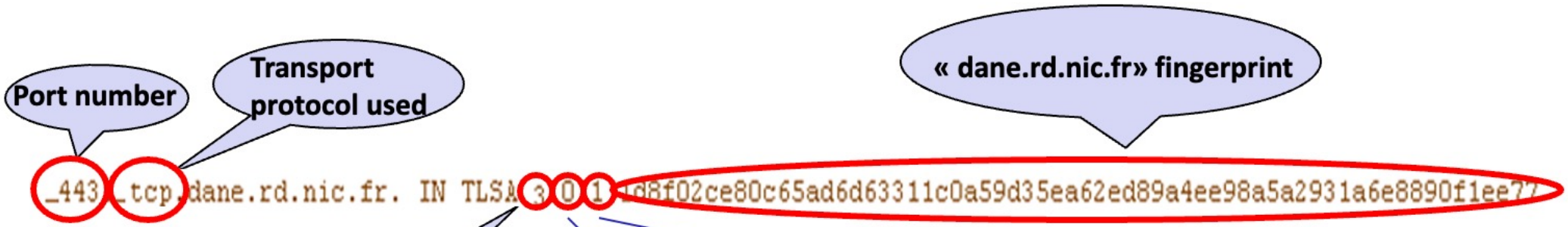


afnic | Labs

DNS Authentication of Named Entities

- At the IETF
  - DANE Use Case – RFC 6394
  - DANE Protocol – RFC 6698
  - RFC 7671 – Obsoletes 6698
  - Uses – s/MIME, POP3, IMAP and SMTP
  - Web use-case not successful
  - DANCE WG in progress

TLSA Resource record



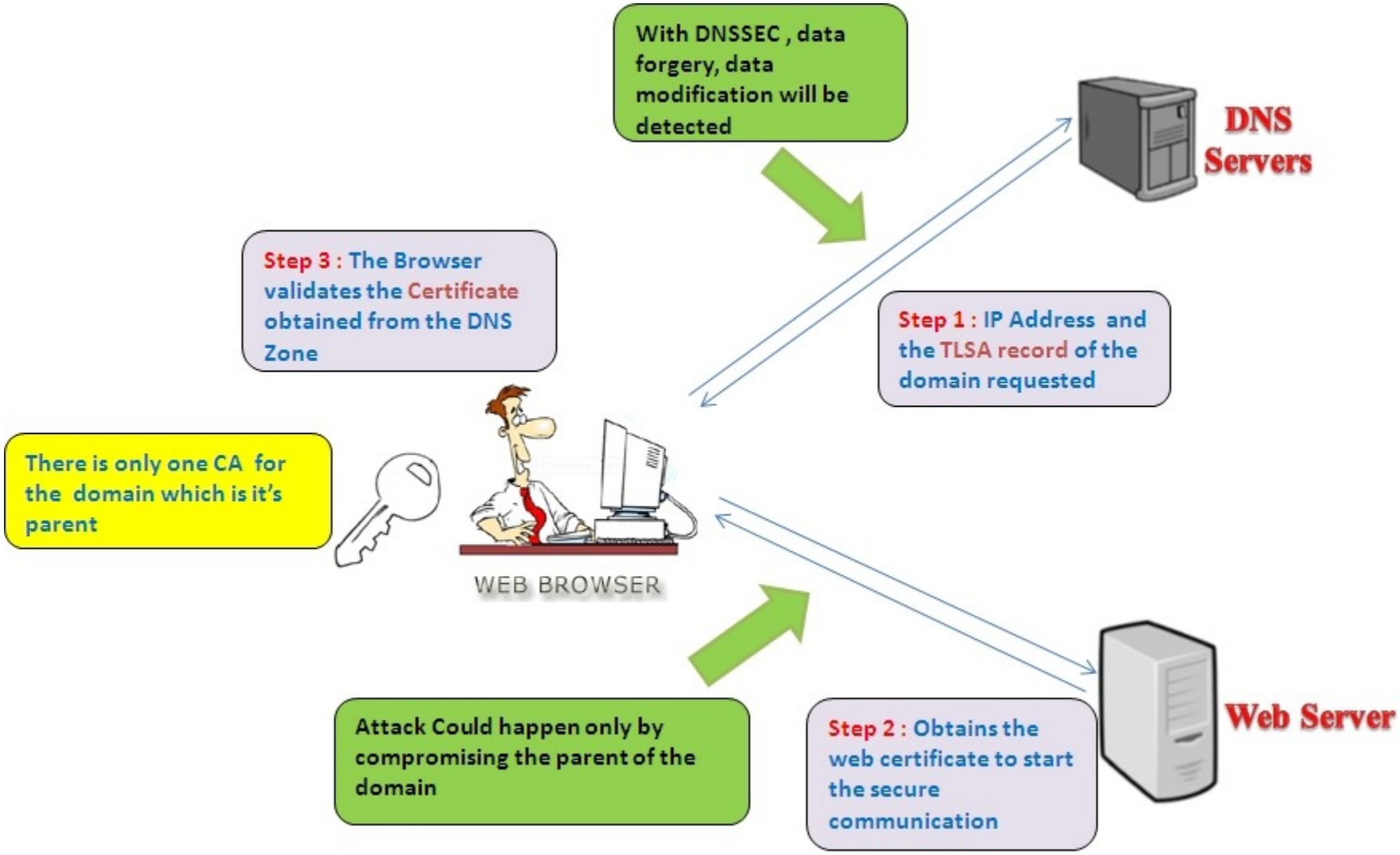
Value	Meaning
0	Exact match
1	SHA-256 hash of the selected content
2	SHA-512 hash of the selected content

Value	Meaning
0	Full certificate
1	Subject Public Key Info (Explained in RFC 5280)

Certificate Usage

- Must pass PKIX validation (Usage 0/1)
  - Usage 0 - Certificate Authority pinning (e.g. Validate only with « Keynectis » for www.afnic.fr)
  - Usage 1 – Certificate pinning (e.g. Validate only with the specific certificate (e.g. RSA with MD5) from « Keynectis » for www.afnic.fr)
- A new trust anchor is added (Usage 2/3)
  - Usage 2 – (e.g; AFNIC creates its own CA and wants it to be trusted)
  - Usage 3 – Self-signed certificates

How DANE could secure the last hop?



DANE Usage in IoT

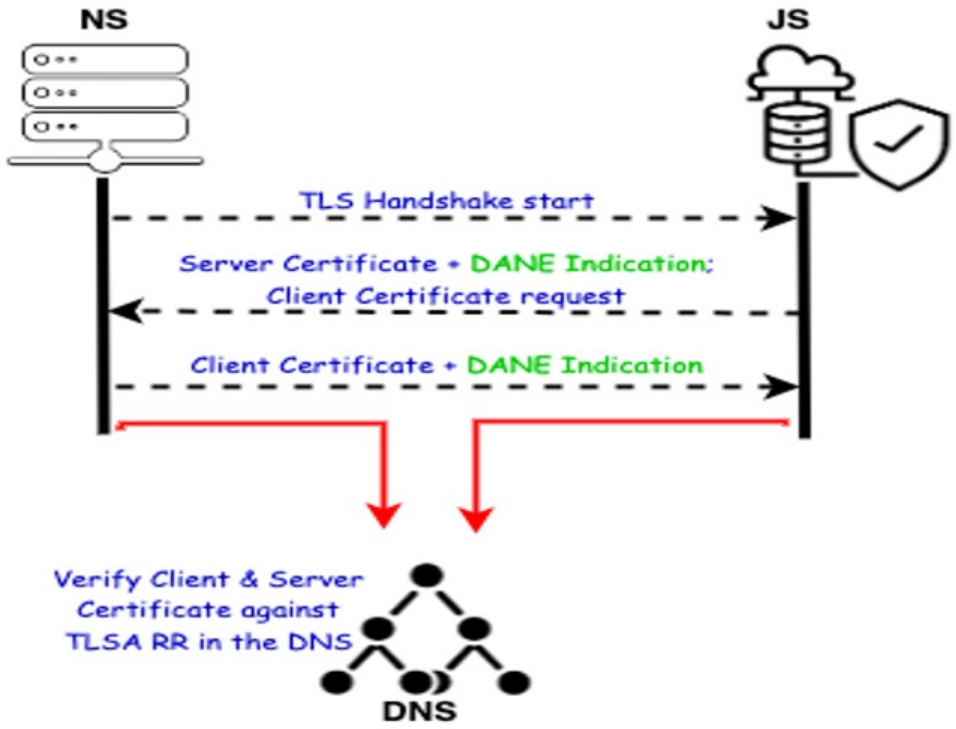
draft-ietf-dance-client-auth-00

TLS Client Authentication via DANE TLSA records

draft-ietf-dance-tls-clientid-00

TLS Extension for DANE Client Identity

Afnic –implemented and tested the two IETF drafts during IETF 113 Hackathon



Enables using self-signed certificate with multiple Root CA's

Need for Encryption

- RFC 7626 – DNS is too talkative
- Resolvers can lie

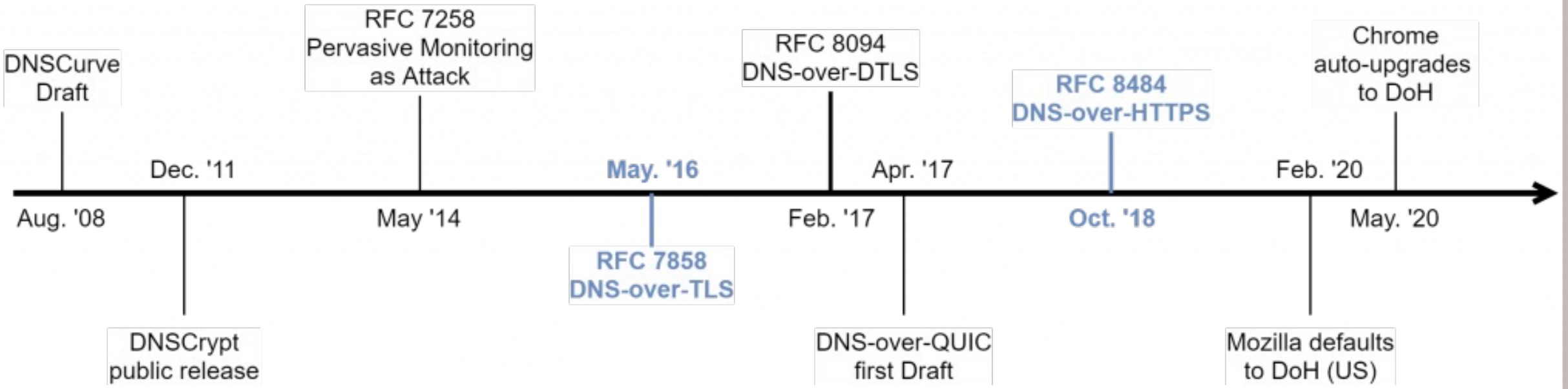
```
% python resolve-name.py -r 500 -c TR www.etha.com.tr
Measurement #2905528 for www.etha.com.tr/A uses 32 probes
[213.14.227.50] : 5 occurrences
[195.175.254.2] : 6 occurrences
[176.9.34.7] : 20 occurrences
```

```
% python resolve-name.py -r 500 -c DE www.etha.com.tr
Measurement #2905529 for www.etha.com.tr/A uses 498 probes
[ERROR: REFUSED] : 3 occurrences
[ERROR: SERVFAIL] : 3 occurrences
[176.9.34.7] : 463 occurrences
```

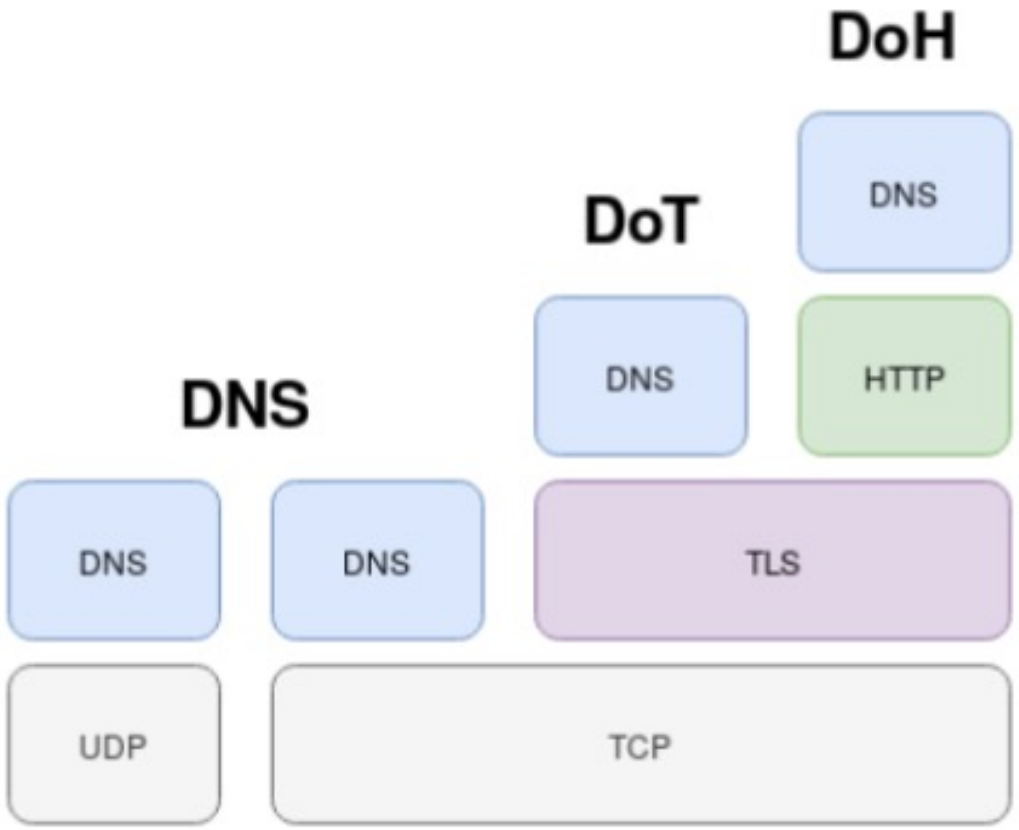
Source: https://gist.github.com/bortzmeyer/10fe2900c59068bb0c78

afnic | Labs

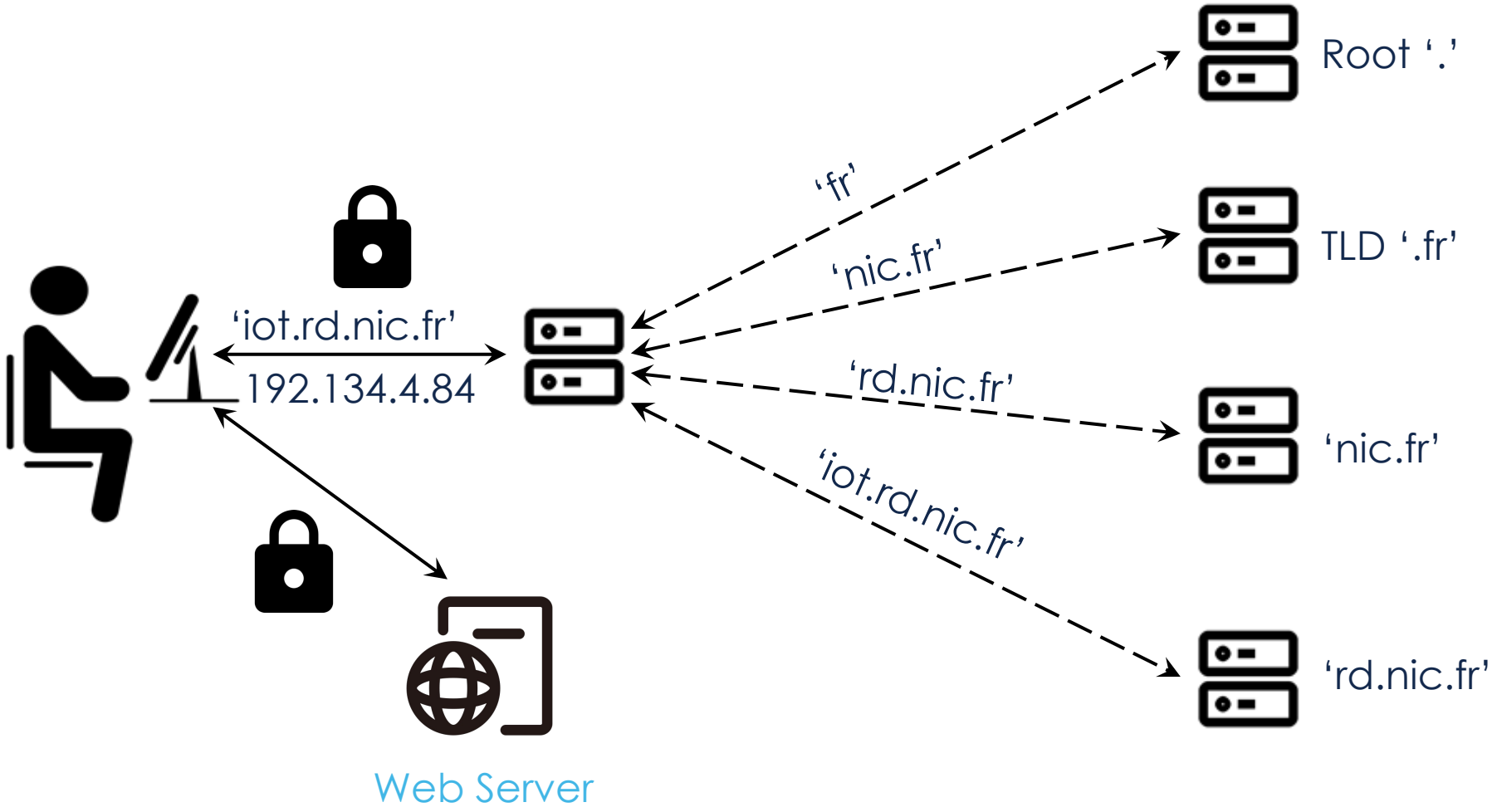
DNS Encryption timeline



Adding encryption to DNS resolution

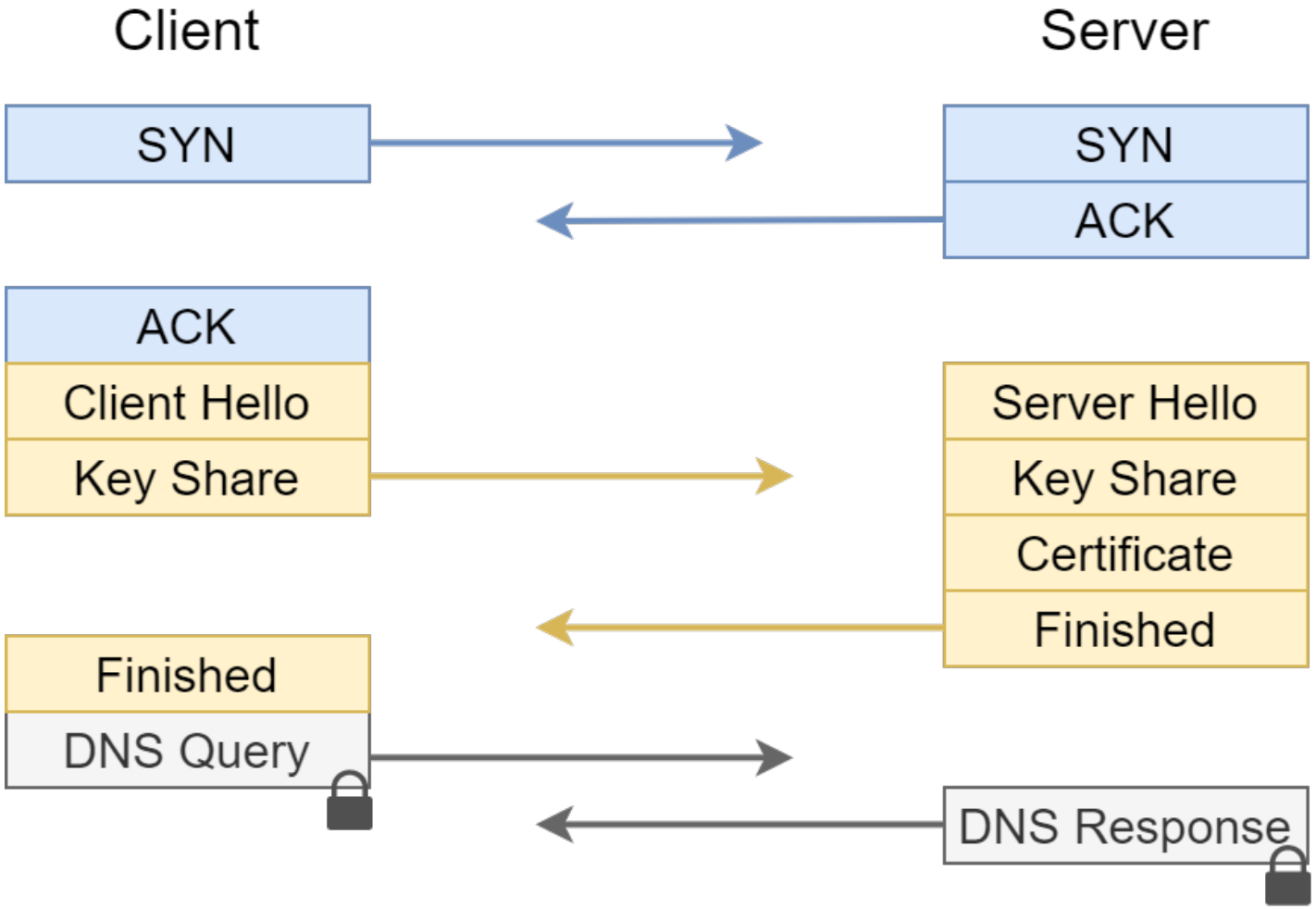


DoT – Encrypted communication



afnic | Labs

DoT in action



Configuring DoT

```
tls mytls {
  cert-file "/etc/bind9/fullchain.pem";
  key-file "/etc/bind9/privkey.pem";
};

options {
  directory "/var/cache/bind";
  querylog no;
  auth-nxdomain no;
  dnssec-validation auto;
  minimal-responses no-auth-recursive;
  listen-on port 53 { any; };
  listen-on-v6 { any; };
  listen-on port 853 tls mytls { any; };
  allow-transfer { none; };
  allow-recursion { 127.0.0.1; ::1; };
  recursion yes;
};
```

/var/unbound/etc/unbound.conf

```
        # CA Certificates used for forward-tls-upstream (RFC7858) hostname
        # verification.  Since it's outside the chroot it is only loaded at
        # startup and thus cannot be changed via a reload.
        tls-cert-bundle: "/etc/ssl/cert.pem"
```

```
# Use an upstream DNS-over-TLS forwarder and do not fall back to cleartext
# if that fails.
forward-zone:
        name: "."
        forward-tls-upstream: yes               # use DNS-over-TLS forwarder
        forward-first: no                       # do NOT send direct
#       # the hostname after "#" is not a comment, it is used for TLS checks:
        forward-addr: 2606:4700:4700::1111@853#cloudflare-dns.com
        forward-addr: 1.1.1.1@853#cloudflare-dns.com
        forward-addr: 2606:4700:4700::1001@853#cloudflare-dns.com
        forward-addr: 1.0.0.1@853#cloudflare-dns.com
```

afnic | Labs

DNS

Connected to 1.1.1.1	No
Using DNS over HTTPS (DoH)	No
Using DNS over TLS (DoT)	No
Using DNS over WARP	No
AS Name	Free SAS
AS Number	12322
Cloudflare Data Center	CDG

Connectivity to Resolver IP Addresses

1.1.1.1	Yes
1.0.0.1	Yes
2606:4700:4700::1111	No
2606:4700:4700::1001	No

afnic | Labs

DNS

Debug Information

Connected to 1.1.1.1	Yes
Using DNS over HTTPS (DoH)	Yes
Using DNS over TLS (DoT)	Yes
Using DNS over WARP	No
AS Name	Cloudflare
AS Number	13335
Cloudflare Data Center	CDG

afnic | Labs

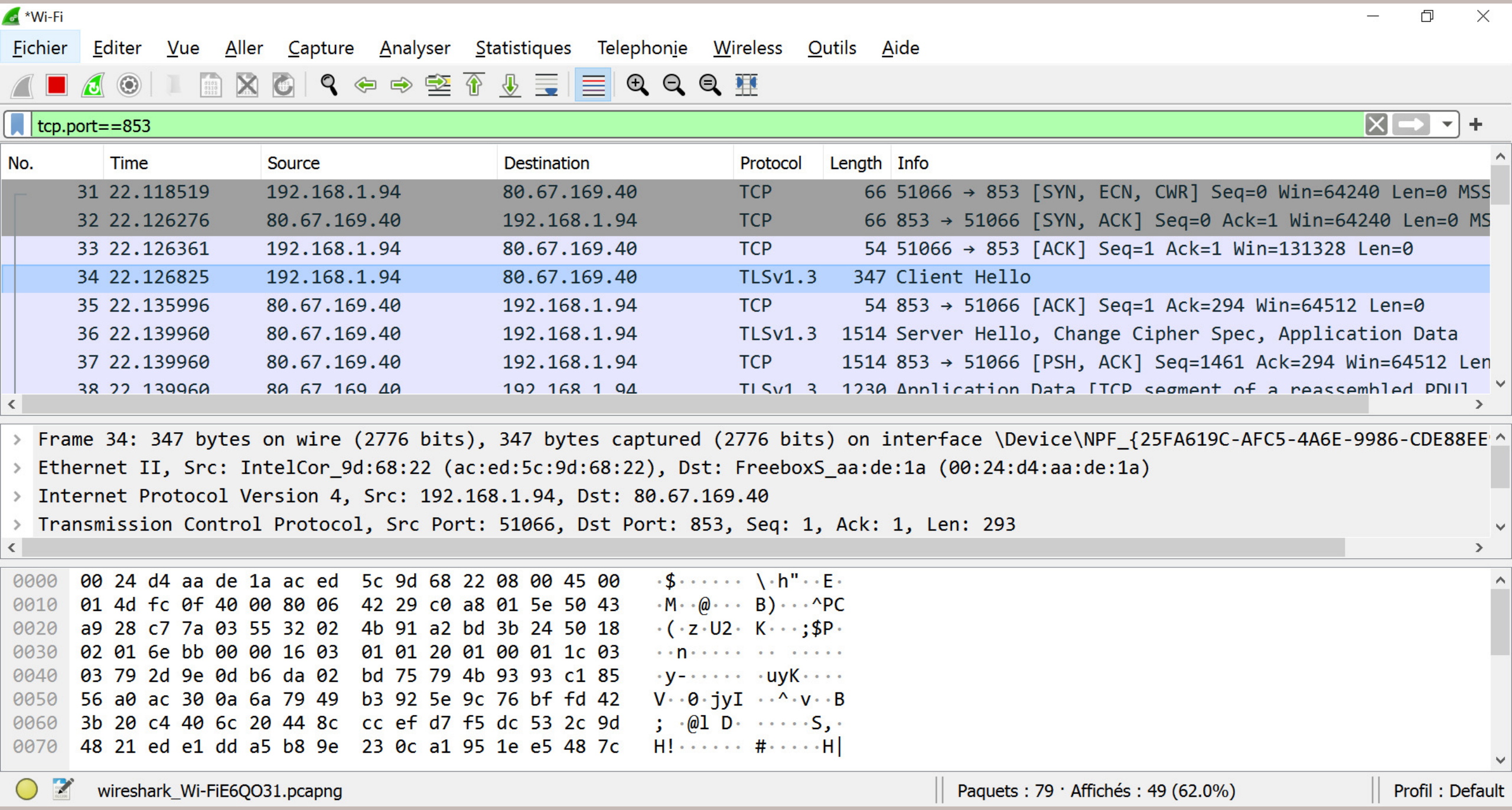
Testing DoT

```
/Users/sandoche $ kdig -d @1.1.1.1 +tls-ca +tls-host=one.one.one.one afnic.fr
;; DEBUG: Querying for owner(afnic.fr.), class(1), type(1), server(1.1.1.1), port(853), protocol(TCP)
;; DEBUG: TLS, imported 141 system certificates
;; DEBUG: TLS, received certificate hierarchy:
;; DEBUG:  #1, C=US,ST=California,L=San Francisco,O=Cloudflare\, Inc.,CN=cloudflare-dns.com
;; DEBUG:      SHA-256 PIN: GP8Knf7qBae+aIfythytMbYnL+yowaWVeD6MoLHkVRg=
;; DEBUG:  #2, C=US,O=DigiCert Inc,CN=DigiCert TLS Hybrid ECC SHA384 2020 CA1
;; DEBUG:      SHA-256 PIN: e0IRz5Tio3GA1Xs4fUVWmH1xHDiH2dMbVtCBSkOIdqM=
;; DEBUG: TLS, skipping certificate PIN check
;; DEBUG: TLS, The certificate is trusted.
;; TLS session (TLS1.3)-(ECDHE-X25519)-(ECDSA-SECP256R1-SHA256)-(AES-256-GCM)
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 14164
;; Flags: qr rd ra ad; QUERY: 1; ANSWER: 1; AUTHORITY: 0; ADDITIONAL: 1

;; EDNS PSEUDOSECTION:
;; Version: 0; flags: ; UDP size: 1232 B; ext-rcode: NOERROR
;; PADDING: 411 B

;; QUESTION SECTION:
;; afnic.fr.                    IN      A

;; ANSWER SECTION:
afnic.fr.               600     IN      A       192.134.5.37
```


*Wi-Fi
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide
tcp.port==853
No. Time Source Destination Protocol Length Info
31 22.118519 192.168.1.94 80.67.169.40 TCP 66 51066 → 853 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS
32 22.126276 80.67.169.40 192.168.1.94 TCP 66 853 → 51066 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MS
33 22.126361 192.168.1.94 80.67.169.40 TCP 54 51066 → 853 [ACK] Seq=1 Ack=1 Win=131328 Len=0
34 22.126825 192.168.1.94 80.67.169.40 TLSv1.3 347 Client Hello
35 22.135996 80.67.169.40 192.168.1.94 TCP 54 853 → 51066 [ACK] Seq=1 Ack=294 Win=64512 Len=0
36 22.139960 80.67.169.40 192.168.1.94 TLSv1.3 1514 Server Hello, Change Cipher Spec, Application Data
37 22.139960 80.67.169.40 192.168.1.94 TCP 1514 853 → 51066 [PSH, ACK] Seq=1461 Ack=294 Win=64512 Len
Frame 34: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits) on interface \Device\NPF_{25FA619C-AFC5-4A6E-9986-CDE88EE
Ethernet II, Src: IntelCor_9d:68:22 (ac:ed:5c:9d:68:22), Dst: FreeboxS_aa:de:1a (00:24:d4:aa:de:1a)
Internet Protocol Version 4, Src: 192.168.1.94, Dst: 80.67.169.40
Transmission Control Protocol, Src Port: 51066, Dst Port: 853, Seq: 1, Ack: 1, Len: 293
0000 00 24 d4 aa de 1a ac ed 5c 9d 68 22 08 00 45 00
0010 01 4d fc 0f 40 00 80 06 42 29 c0 a8 01 5e 50 43
0020 a9 28 c7 7a 03 55 32 02 4b 91 a2 bd 3b 24 50 18
0030 02 01 6e bb 00 00 16 03 01 01 20 01 00 01 1c 03
0040 03 79 2d 9e 0d b6 da 02 bd 75 79 4b 93 93 c1 85
0050 56 a0 ac 30 0a 6a 79 49 b3 92 5e 9c 76 bf fd 42
0060 3b 20 c4 40 6c 20 44 8c cc ef d7 f5 dc 53 2c 9d
0070 48 21 ed e1 dd a5 b8 9e 23 0c a1 95 1e e5 48 7c
wireshark_Wi-FiE6QO31.pcapng
Paquets : 79 · Affichés : 49 (62.0%)
Profil : Default

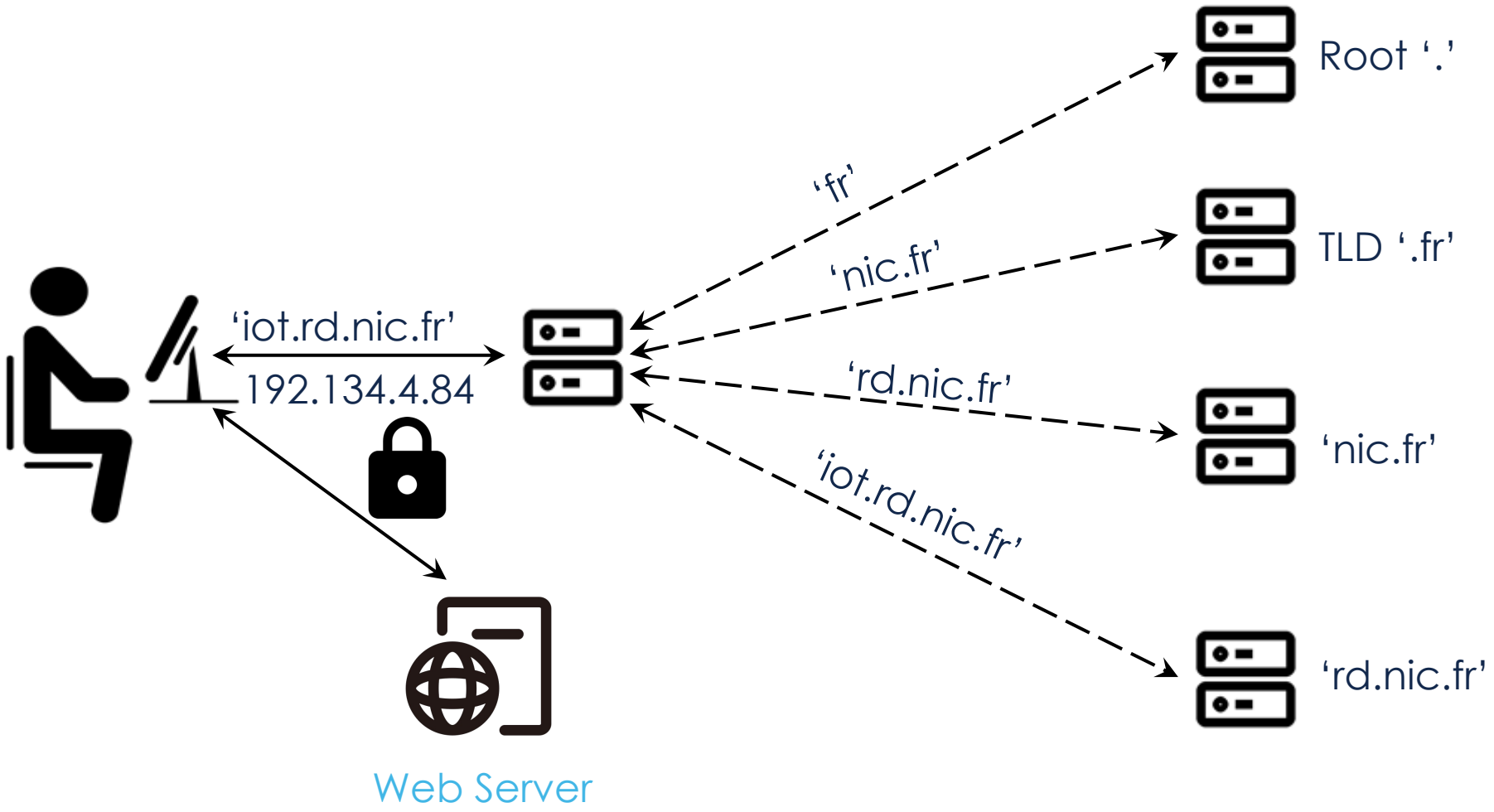
afnic | Labs

DoT Issues

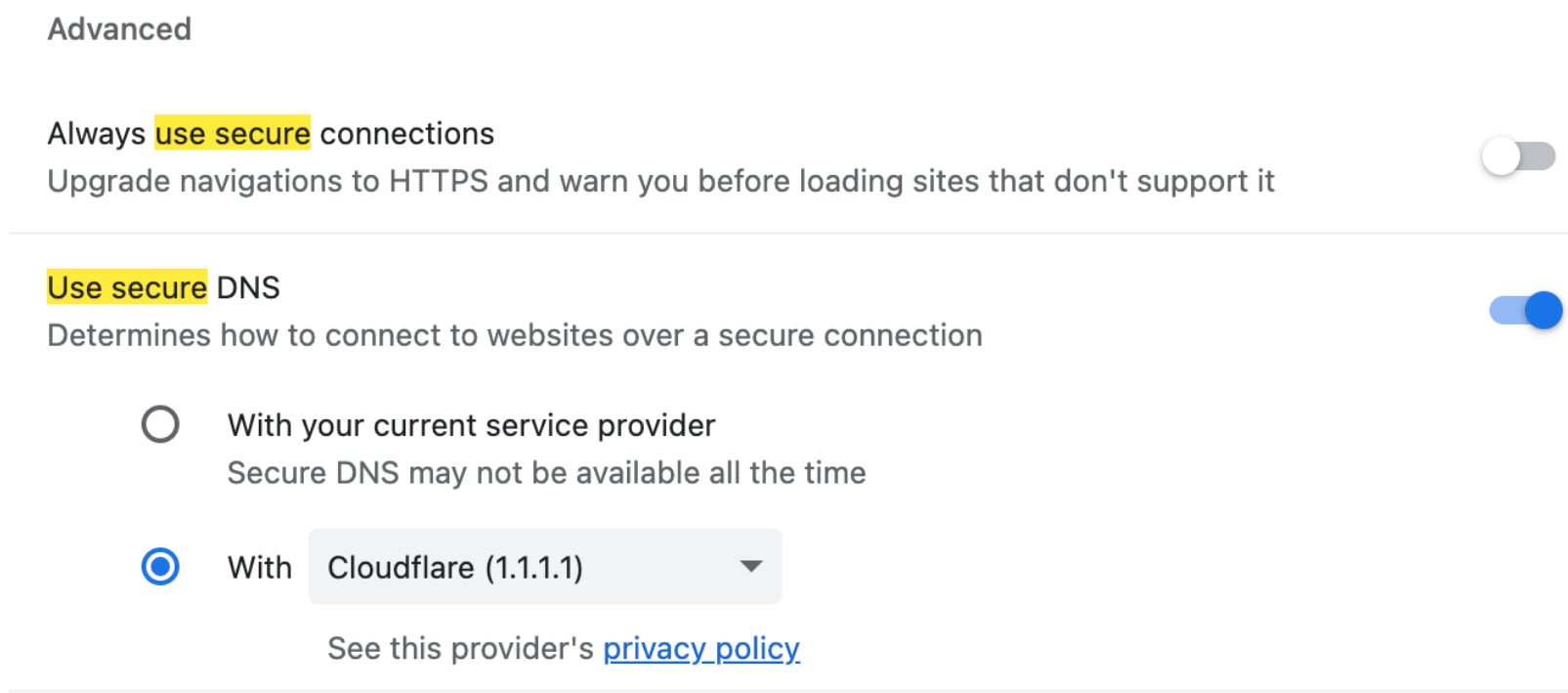
- Specific port 853

- Performance

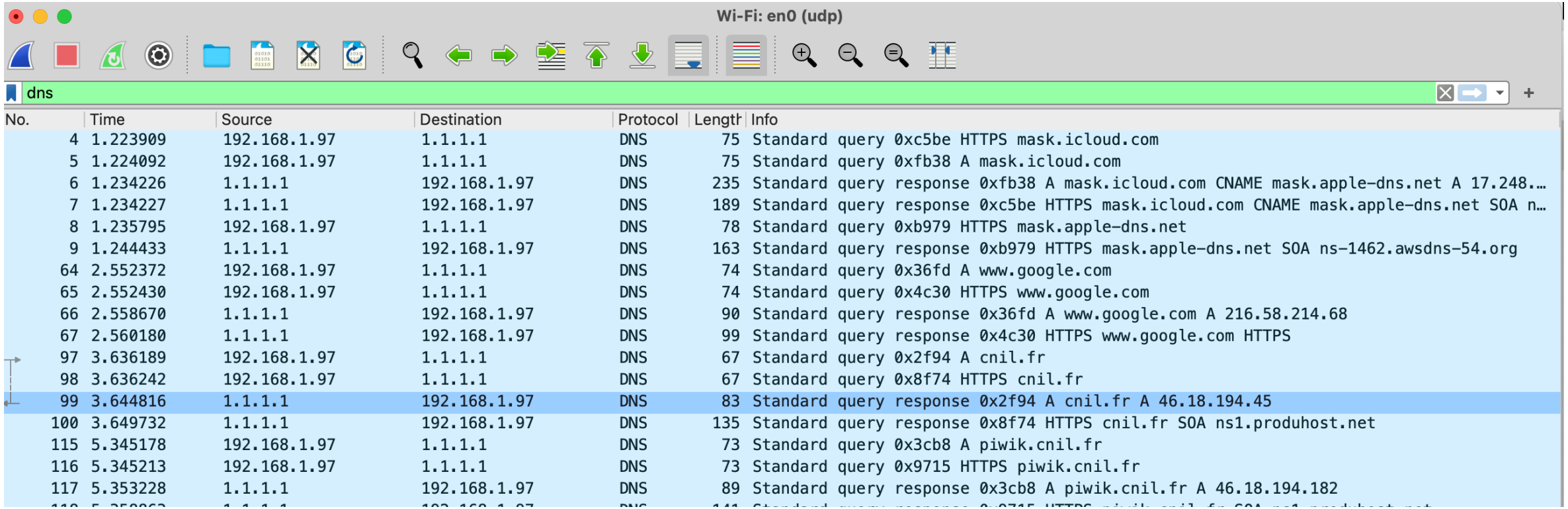
DoH – Encrypted communication



Configure DoH

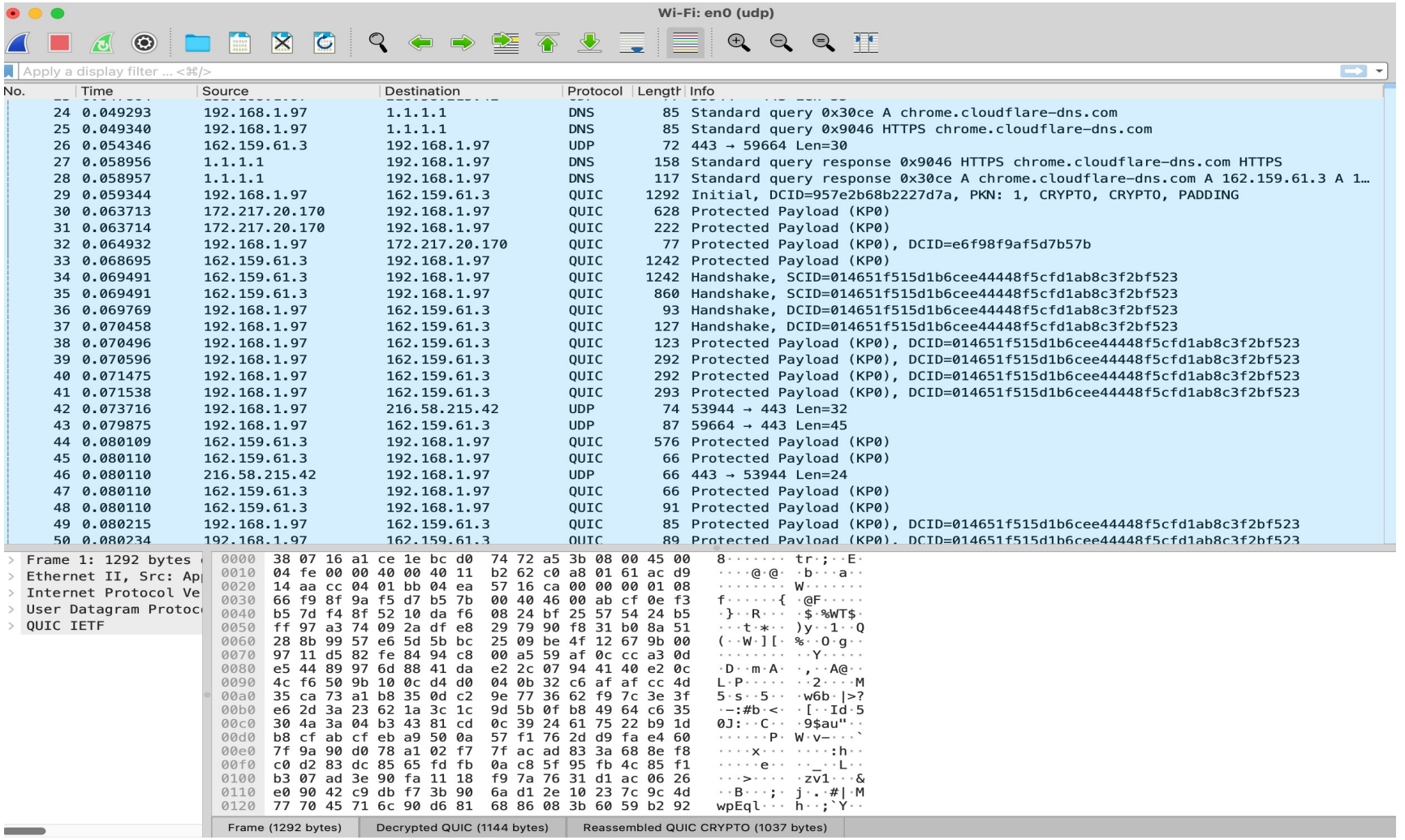


Without DoH



No.	Time	Source	Destination	Protocol	Length	Info
4	1.223909	192.168.1.97	1.1.1.1	DNS	75	Standard query 0xc5be HTTPS mask.icloud.com
5	1.224092	192.168.1.97	1.1.1.1	DNS	75	Standard query 0xfb38 A mask.icloud.com
6	1.234226	1.1.1.1	192.168.1.97	DNS	235	Standard query response 0xfb38 A mask.icloud.com CNAME mask.apple-dns.net A 17.248.…
7	1.234227	1.1.1.1	192.168.1.97	DNS	189	Standard query response 0xc5be HTTPS mask.icloud.com CNAME mask.apple-dns.net SOA n…
8	1.235795	192.168.1.97	1.1.1.1	DNS	78	Standard query 0xb979 HTTPS mask.apple-dns.net
9	1.244433	1.1.1.1	192.168.1.97	DNS	163	Standard query response 0xb979 HTTPS mask.apple-dns.net SOA ns-1462.awsdns-54.org
64	2.552372	192.168.1.97	1.1.1.1	DNS	74	Standard query 0x36fd A www.google.com
65	2.552430	192.168.1.97	1.1.1.1	DNS	74	Standard query 0x4c30 HTTPS www.google.com
66	2.558670	1.1.1.1	192.168.1.97	DNS	90	Standard query response 0x36fd A www.google.com A 216.58.214.68
67	2.560180	1.1.1.1	192.168.1.97	DNS	99	Standard query response 0x4c30 HTTPS www.google.com HTTPS
97	3.636189	192.168.1.97	1.1.1.1	DNS	67	Standard query 0x2f94 A cnil.fr
98	3.636242	192.168.1.97	1.1.1.1	DNS	67	Standard query 0x8f74 HTTPS cnil.fr
99	3.644816	1.1.1.1	192.168.1.97	DNS	83	Standard query response 0x2f94 A cnil.fr A 46.18.194.45
100	3.649732	1.1.1.1	192.168.1.97	DNS	135	Standard query response 0x8f74 HTTPS cnil.fr SOA ns1.produhost.net
115	5.345178	192.168.1.97	1.1.1.1	DNS	73	Standard query 0x3cb8 A piwik.cnil.fr
116	5.345213	192.168.1.97	1.1.1.1	DNS	73	Standard query 0x9715 HTTPS piwik.cnil.fr
117	5.353228	1.1.1.1	192.168.1.97	DNS	89	Standard query response 0x3cb8 A piwik.cnil.fr A 46.18.194.182

With DoH


Wi-Fi: en0 (udp)
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
24 0.049293 192.168.1.97 1.1.1.1 DNS 85 Standard query 0x30ce A chrome.cloudflare-dns.com
25 0.049340 192.168.1.97 1.1.1.1 DNS 85 Standard query 0x9046 HTTPS chrome.cloudflare-dns.com
26 0.054346 162.159.61.3 192.168.1.97 UDP 72 443 → 59664 Len=30
27 0.058956 1.1.1.1 192.168.1.97 DNS 158 Standard query response 0x9046 HTTPS chrome.cloudflare-dns.com HTTPS
28 0.058957 1.1.1.1 192.168.1.97 DNS 117 Standard query response 0x30ce A chrome.cloudflare-dns.com A 162.159.61.3 A 1…
29 0.059344 192.168.1.97 162.159.61.3 QUIC 1292 Initial, DCID=957e2b68b2227d7a, PKN: 1, CRYPTO, CRYPTO, PADDING
30 0.063713 172.217.20.170 192.168.1.97 QUIC 628 Protected Payload (KP0)
31 0.063714 172.217.20.170 192.168.1.97 QUIC 222 Protected Payload (KP0)
32 0.064932 192.168.1.97 172.217.20.170 QUIC 77 Protected Payload (KP0), DCID=e6f98f9af5d7b57b
33 0.068695 162.159.61.3 192.168.1.97 QUIC 1242 Protected Payload (KP0)
34 0.069491 162.159.61.3 192.168.1.97 QUIC 1242 Handshake, SCID=014651f515d1b6cee44448f5cfd1ab8c3f2bf523
35 0.069491 162.159.61.3 192.168.1.97 QUIC 860 Handshake, SCID=014651f515d1b6cee44448f5cfd1ab8c3f2bf523
36 0.069769 192.168.1.97 162.159.61.3 QUIC 93 Handshake, DCID=014651f515d1b6cee44448f5cfd1ab8c3f2bf523
37 0.070458 192.168.1.97 162.159.61.3 QUIC 127 Handshake, DCID=014651f515d1b6cee44448f5cfd1ab8c3f2bf523
38 0.070496 192.168.1.97 162.159.61.3 QUIC 123 Protected Payload (KP0), DCID=014651f515d1b6cee44448f5cfd1ab8c3f2bf523
39 0.070596 192.168.1.97 162.159.61.3 QUIC 292 Protected Payload (KP0), DCID=014651f515d1b6cee44448f5cfd1ab8c3f2bf523
40 0.071475 192.168.1.97 162.159.61.3 QUIC 292 Protected Payload (KP0), DCID=014651f515d1b6cee44448f5cfd1ab8c3f2bf523
41 0.071538 192.168.1.97 162.159.61.3 QUIC 293 Protected Payload (KP0), DCID=014651f515d1b6cee44448f5cfd1ab8c3f2bf523
42 0.073716 192.168.1.97 216.58.215.42 UDP 74 53944 → 443 Len=32
43 0.079875 192.168.1.97 162.159.61.3 UDP 87 59664 → 443 Len=45
44 0.080109 162.159.61.3 192.168.1.97 QUIC 576 Protected Payload (KP0)
45 0.080110 162.159.61.3 192.168.1.97 QUIC 66 Protected Payload (KP0)
46 0.080110 216.58.215.42 192.168.1.97 UDP 66 443 → 53944 Len=24
47 0.080110 162.159.61.3 192.168.1.97 QUIC 66 Protected Payload (KP0)
48 0.080110 162.159.61.3 192.168.1.97 QUIC 91 Protected Payload (KP0)
49 0.080215 192.168.1.97 162.159.61.3 QUIC 85 Protected Payload (KP0), DCID=014651f515d1b6cee44448f5cfd1ab8c3f2bf523
Frame 1: 1292 bytes
Ethernet II, Src: Ap
Internet Protocol Ve
User Datagram Protoc
QUIC IETF
0000 38 07 16 a1 ce 1e bc d0 74 72 a5 3b 08 00 45 00
0010 04 fe 00 00 40 00 40 11 b2 62 c0 a8 01 61 ac d9
0020 14 aa cc 04 01 bb 04 ea 57 16 ca 00 00 00 01 08
0030 66 f9 8f 9a f5 d7 b5 7b 00 40 46 00 ab cf 0e f3
0040 b5 7d f4 8f 52 10 da f6 08 24 bf 25 57 54 24 b5
0050 ff 97 a3 74 09 2a df e8 29 79 90 f8 31 b0 8a 51
0060 28 8b 99 57 e6 5d 5b bc 25 09 be 4f 12 67 9b 00
0070 97 11 d5 82 fe 84 94 c8 00 a5 59 af 0c cc a3 0d
0080 e5 44 89 97 6d 88 41 da e2 2c 07 94 41 40 e2 0c
0090 4c f6 50 9b 10 0c d4 d0 04 0b 32 c6 af af cc 4d
00a0 35 ca 73 a1 b8 35 0d c2 9e 77 36 62 f9 7c 3e 3f
00b0 e6 2d 3a 23 62 1a 3c 1c 9d 5b 0f b8 49 64 c6 35
00c0 30 4a 3a 04 b3 43 81 cd 0c 39 24 61 75 22 b9 1d
00d0 b8 cf ab cf eb a9 50 0a 57 f1 76 2d d9 fa e4 60
00e0 7f 9a 90 d0 78 a1 02 f7 7f ac ad 83 3a 68 8e f8
00f0 c0 d2 83 dc 85 65 fd fb 0a c8 5f 95 fb 4c 85 f1
0100 b3 07 ad 3e 90 fa 11 18 f9 7a 76 31 d1 ac 06 26
0110 e0 90 42 c9 db f7 3b 90 6a d1 2e 10 23 7c 9c 4d
0120 77 70 45 71 6c 90 d6 81 68 86 08 3b 60 59 b2 92
Frame (1292 bytes)
Decrypted QUIC (1144 bytes)
Reassembled QUIC CRYPTO (1037 bytes)

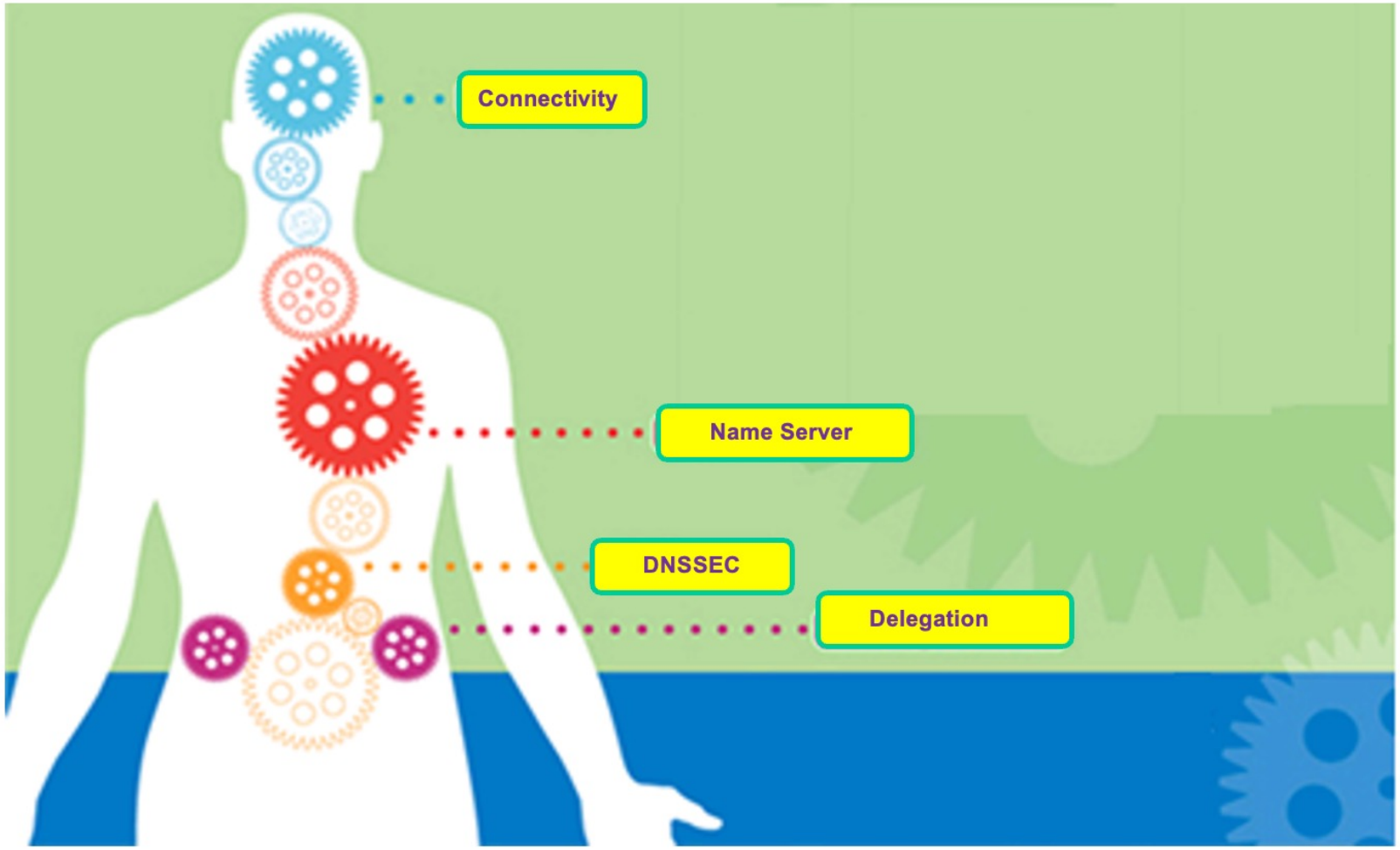
afnic | Labs

Health Check



afnic | Labs

DNS Health check



afnic | Labs

Basic tools – ‘dig’

```
afnic@zonemaster:~$ dig rmll.info

; <<>> DiG 9.9.5-9+deb8u8-Debian <<>> rmll.info
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2014
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;rmll.info.                     IN      A

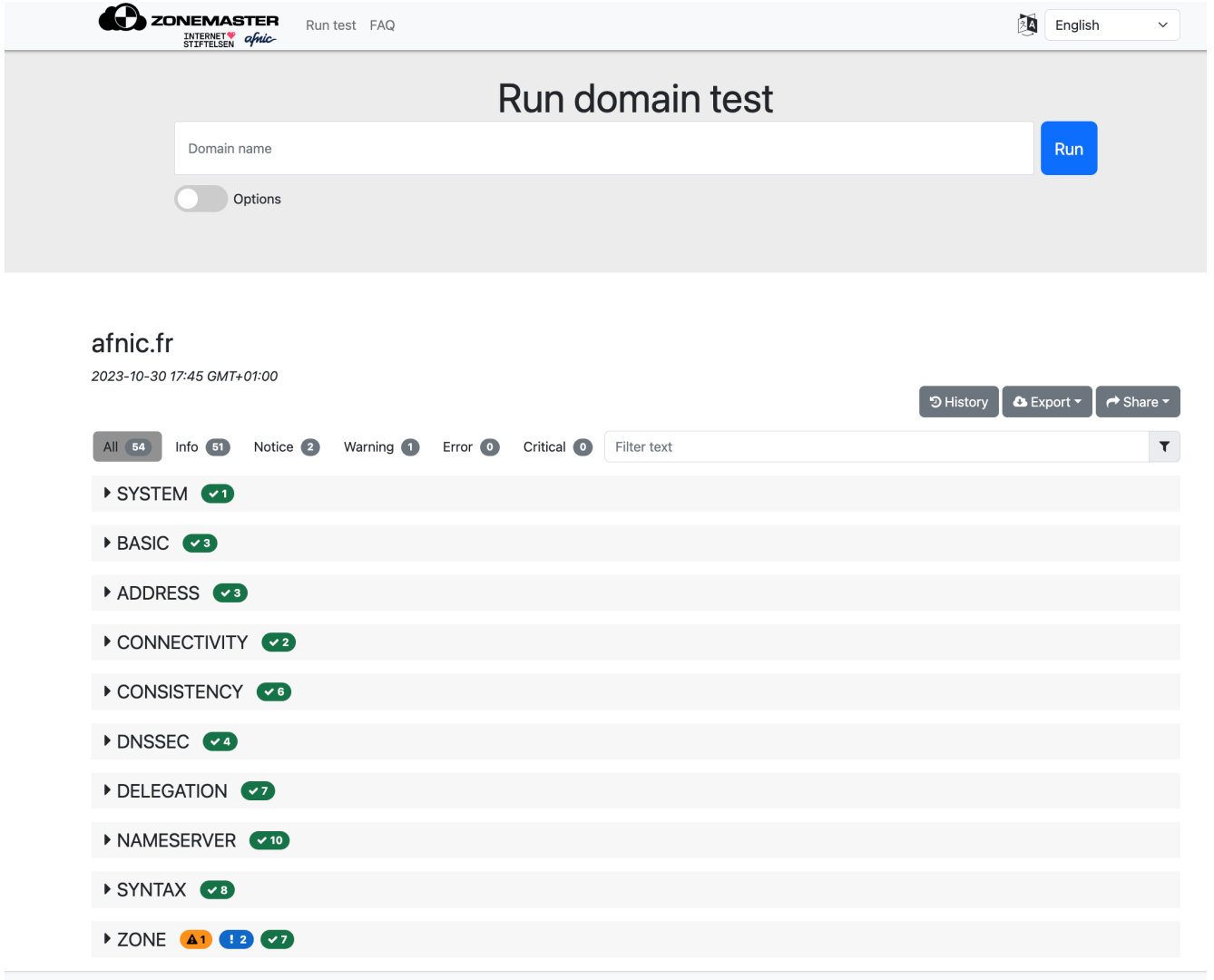
;; ANSWER SECTION:
rmll.info.              3600    IN      A       80.67.169.65

;; AUTHORITY SECTION:
rmll.info.              86399   IN      NS      ns0.abul.org.
rmll.info.              86399   IN      NS      rmll1.rmll.info.

;; ADDITIONAL SECTION:
ns0.abul.org.           86400   IN      A       195.214.228.104
rmll1.rmll.info.        86399   IN      A       80.67.169.65

;; Query time: 214 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Jun 22 09:26:10 CEST 2017
;; MSG SIZE  rcvd: 132
```

Zonemaster for comprehensive healthcheck



Functional breakdown

Usage method	Test engine	Output type
CLI method		CLI output
		Machine parsable output
Web GUI method		Web output
Batch method		Reports Statistics
		JSON Data

Some tests

▸ BASIC ✔3

▸ ADDRESS !1 ✔2

▾ CONNECTIVITY ⚠2 ✔1

⊟ ⚠ TCP connectivity ℹ CONNECTIVITY02

WARNING Nameserver nicnet.nic.in/164.100.105.105 does not respond to any queries over TCP.

WARNING Nameserver ns4.nic.in/164.100.11.2 does not respond to any queries over TCP.

⊞ ⚠ AS Diversity

⊞ ✔ IP Prefix Diversity

▸ CONSISTENCY ✔6

▾ DNSSEC ✖1 ⚠2 ✔3

⊞ ✖ Legal values for the DS hash digest algorithm

⊟ ⚠ Check for invalid DNSKEY algorithms ℹ DNSSEC05

WARNING The DNSKEY with tag 16320 uses an algorithm number 5 (RSA/SHA1) which is not recommended to be used.

WARNING The DNSKEY with tag 14983 uses an algorithm number 5 (RSA/SHA1) which is not recommended to be used.

WARNING The DNSKEY with tag 16320 uses an algorithm number 5 (RSA/SHA1) which is not recommended to be used.

WARNING The DNSKEY with tag 14983 uses an algorithm number 5 (RSA/SHA1) which is not recommended to be used.

⊟ ⚠ Check for valid RSA DNSKEY key size ℹ DNSSEC14

WARNING DNSKEY with tag 16320 and using algorithm 5 (RSA/SHA1) has a size (1024) smaller than the recommended one (2048).

WARNING DNSKEY with tag 14983 and using algorithm 5 (RSA/SHA1) has a size (1024) smaller than the recommended one (2048).

⊞ ✔ Check for too short or too long RRSIG lifetimes

⊞ ✔ Zone contains NSEC or NSEC3 records

⊞ ✔ Existence of CDS and CDNSKEY

▾ DELEGATION ✖1 ✔6

⊟ ✖ Minimum number of name servers ℹ DELEGATION01

ERROR Child does not list enough (1) nameservers (ns8.nic.in) that resolve to IPv6 addresses (2405:8a00:1000::2). Lower limit set to 2.

ERROR Delegation does not list enough (1) nameservers (ns8.nic.in) that resolve to IPv6 addresses (2405:8a00:1000::2). Lower limit set to 2.

INFO Parent lists enough (4) nameservers (nicnet.nic.in; ns4.nic.in; ns6.nic.in; ns8.nic.in). Lower limit set to 2.

INFO Child lists enough (4) nameservers (nicnet.nic.in; ns4.nic.in; ns6.nic.in; ns8.nic.in). Lower limit set to 2.

INFO Child lists enough (3) nameservers (nicnet.nic.in; ns4.nic.in; ns6.nic.in) that resolve to IPv4 addresses (164.100.105.105; 164.100.11.2; 164.100.4.2). Lower limit set to 2.

INFO Delegation lists enough (3) nameservers (nicnet.nic.in; ns4.nic.in; ns6.nic.in) that resolve to IPv4 addresses (164.100.105.105; 164.100.11.2; 164.100.4.2). Lower limit set to 2.

⊞ ✔ Name servers must have distinct IP addresses

afnic | Labs

DNS

All 54 | Info 44 | Notice 3 | Warning 5 | Error 2 | Critical 0 | Filter text

SYSTEM ✔1

BASIC ✔3

ADDRESS ✔3

CONNECTIVITY ⚠2

- ⚠ AS Diversity — CONNECTIVITY03
  - WARNING All authoritative nameservers have their IPv4 addresses in the same AS (7922).
  - WARNING All authoritative nameservers have their IPv6 addresses in the same AS (7922).
- ⚠ IP Prefix Diversity — CONNECTIVITY04
  - WARNING The following name server(s) are announced in the same IPv4 prefix (68.80.0.0/13): "dns102.comcast.net/68.87.85.132; dns103.comcast.net/68.87.76.228; dns104.comcast.net/68.87.68.244; dns105.comcast.net/68.87.72.244"
  - WARNING The following name server(s) are announced in the same IPv6 prefix (2001:558::/29): "dns101.comcast.net/2001:558:fe23:8:69:252:250:103; dns102.comcast.net/2001:558:1004:7:68:87:85:132; dns103.comcast.net/2001:558:1014:c:68:87:76:228; dns104.comcast.net/2001:558:100a:5:68:87:68:244; dns105.comcast.net/2001:558:100e:5:68:87:72:244"
  - INFO The following name server(s) are announced in unique IPv4 prefix(es): "dns101.comcast.net/69.252.250.103"

CONSISTENCY ✔6

DNSSEC ✖2 ⚠2 ✔3

- ✖ Legal values for the DS hash digest algorithm
- ✖ DS must match a valid DNSKEY in the child zone — DNSSEC02
  - ERROR There is no valid DNSKEY matched by any of the DS records. Fetched from the nameservers with IP addresses "2001:558:1004:7:68:87:85:132; 2001:558:100a:5:68:87:68:244; 2001:558:100e:5:68:87:72:244; 2001:558:1014:c:68:87:76:228; 2001:558:fe23:8:69:252:250:103; 68.87.68.244; 68.87.72.244; 68.87.76.228; 68.87.85.132; 69.252.250.103".
  - WARNING The DNSKEY record with tag 106 that the DS refers to does not exist in the DNSKEY RRset. Fetched from the nameservers with IP "2001:558:1004:7:68:87:85:132; 2001:558:100a:5:68:87:68:244; 2001:558:100e:5:68:87:72:244; 2001:558:1014:c:68:87:76:228; 2001:558:fe23:8:69:252:250:103; 68.87.68.244; 68.87.72.244; 68.87.76.228; 68.87.85.132; 69.252.250.103".
- ⚠ Check for invalid DNSKEY algorithms
- ⚠ Check for valid RSA DNSKEY key size