SharkFest'25 EUROPE

DNS-Security

Johannes Weber
SVA System Vertrieb Alexander GmbH

#sf25eu

Who Am I?

- Johannes Weber
- SVA System Vertrieb Alexander GmbH

- Master IT-Security
- Network Security Consultant
- IPv6 & DNS

- LinkedIn: https://www.linkedin.com/in/johannes-webernetz/
- Blog: https://weberblog.net/

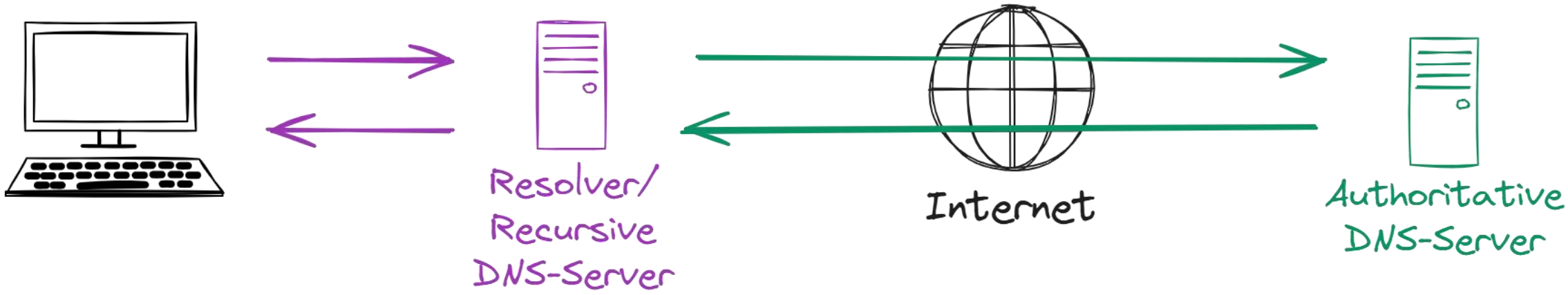
DNS-Security – Agenda

- Malicious DNS
  - Malware & DNS
  - Look-Alike Domains
  - DGAs
  - DNS-Exfiltration
  - DNS-Tunneling
- DNS Spoofing
- DNSSEC
- DoT & DoH

- Attacks & Defenses
- Tools

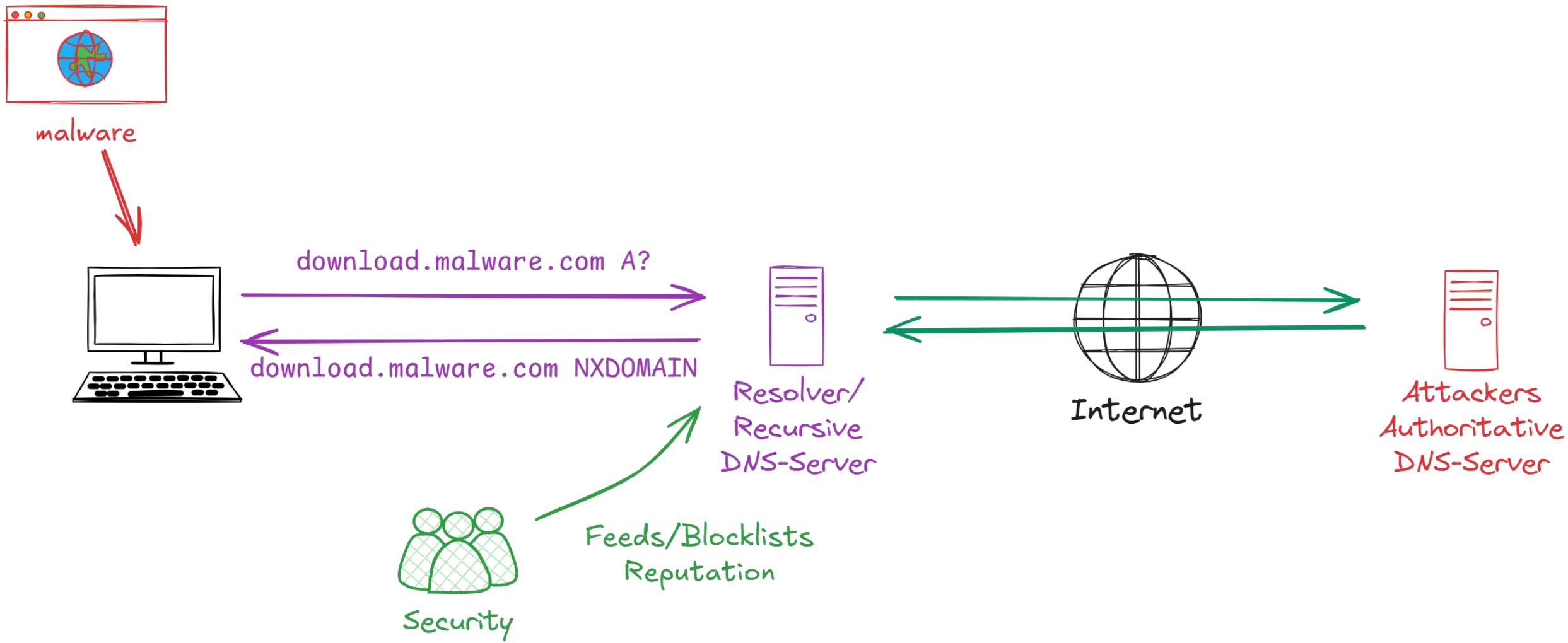
- Normally a 1-day course 😂

DNS Basics



- Privacy: use own recursive resolvers
- Don‘t use 8.8.8.8 at all

Malware & DNS


malware
download.malware.com A?
download.malware.com NXDOMAIN
Resolver/
Recursive
DNS-Server
Internet
Attackers
Authoritative
DNS-Server
Security
Feeds/Blocklists
Reputation

Malware & DNS

- 90 % of malware use DNS
- to find HTTPS servers to download executables
- C2 traffic, command-and-control
- „kill switch“

- Defense: known-malicious feeds, DNS blocklist, RPZ
- → clients get an `NXDOMAIN` or sinkhole address

Look-Alike Domains

- phising mails
- paypal.com paypal.com
- `paypal.com paypaI.com`

- gmial.com

- Defense: known-malicious feeds, DNS blocklist, RPZ
- → clients get an `NXDOMAIN` or sinkhole address

Domain Generation Algorithms (DGAs)

- millions of pseudo-random names
- `exxkosgrtkidfhlibffoi.com`
- `kbucdfkqpeksffoikkgb.com`

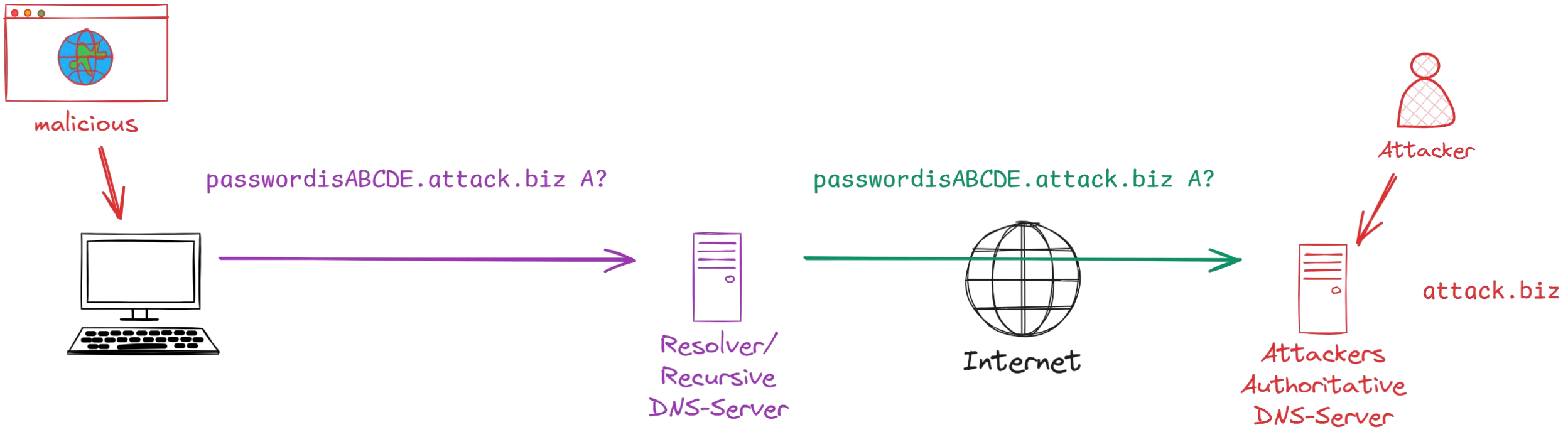
- or even better: dictionary-based names
- `legoutlineactually.net`
- `packageflyexcept.com`

Domain Generation Algorithms (DGAs)

- DNS blocklists are not working (too many entries)
- Millions of domains are registered per day → most of them are malicious!
- → We assume that all new domains are malicious until we verified they‘re not

- Defense: „newly registered | observed domains“ feeds

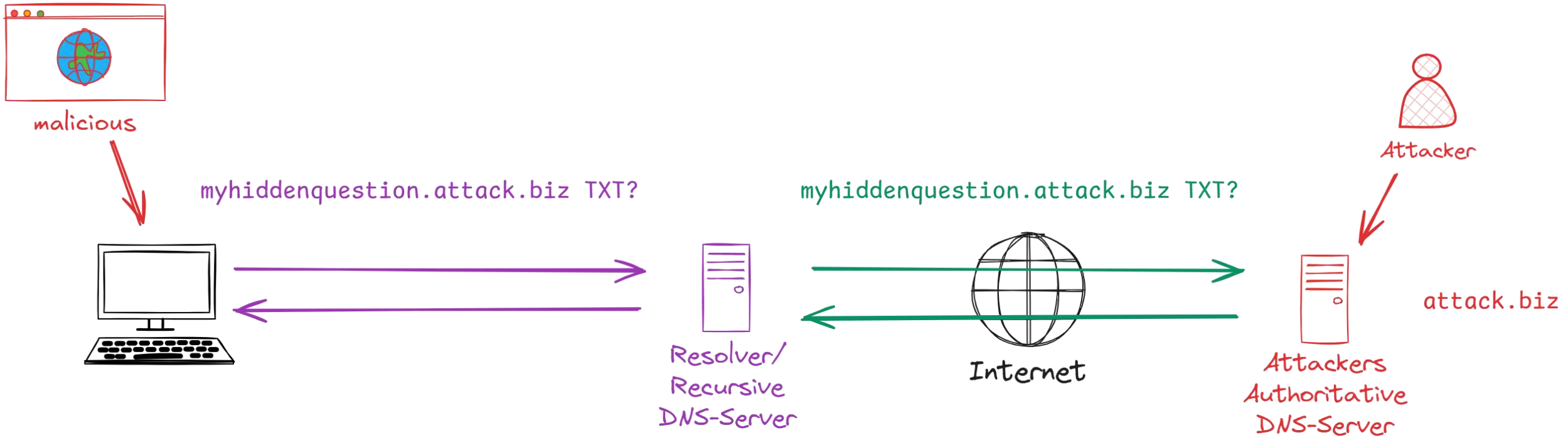
DNS-Exfiltration



DNS-Exfiltration

- Live-Demo:
  `tcpdump -i ens6 port 53 | grep .weberlab.de`

DNS-Tunneling



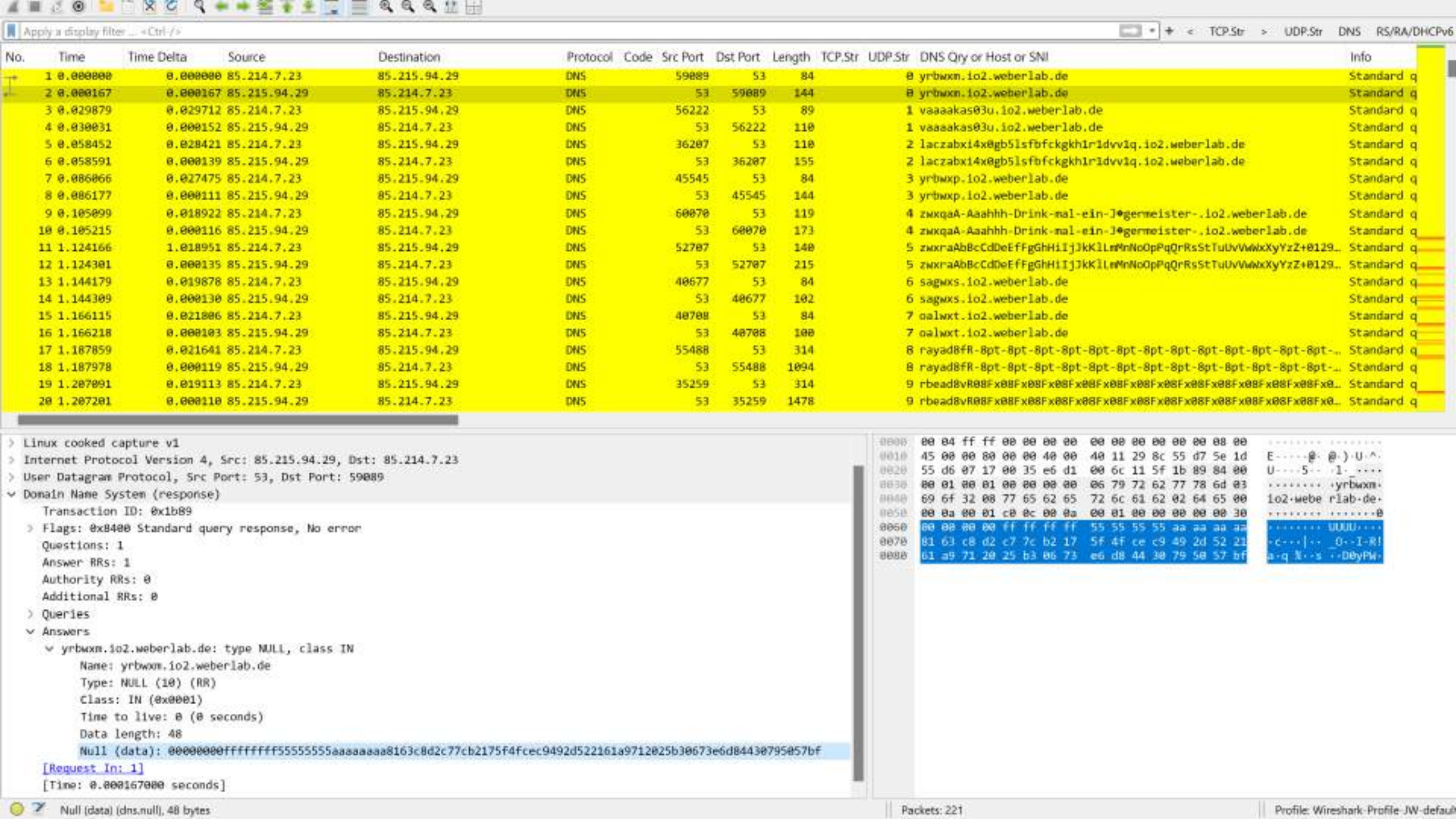
DNS-Exfiltration/-Tunneling

- DNS-Exfiltration:
  - **DNSteal**: https://github.com/m57/dnsteal
  - **dns-exfil**: https://github.com/rybolov/dns-exfil

- DNS-Tunneling:
  - **iodine**: https://github.com/yarrick/iodine
  - **dnscat2**: https://github.com/iagox86/dnscat2

DNS-Tunneling: iodine

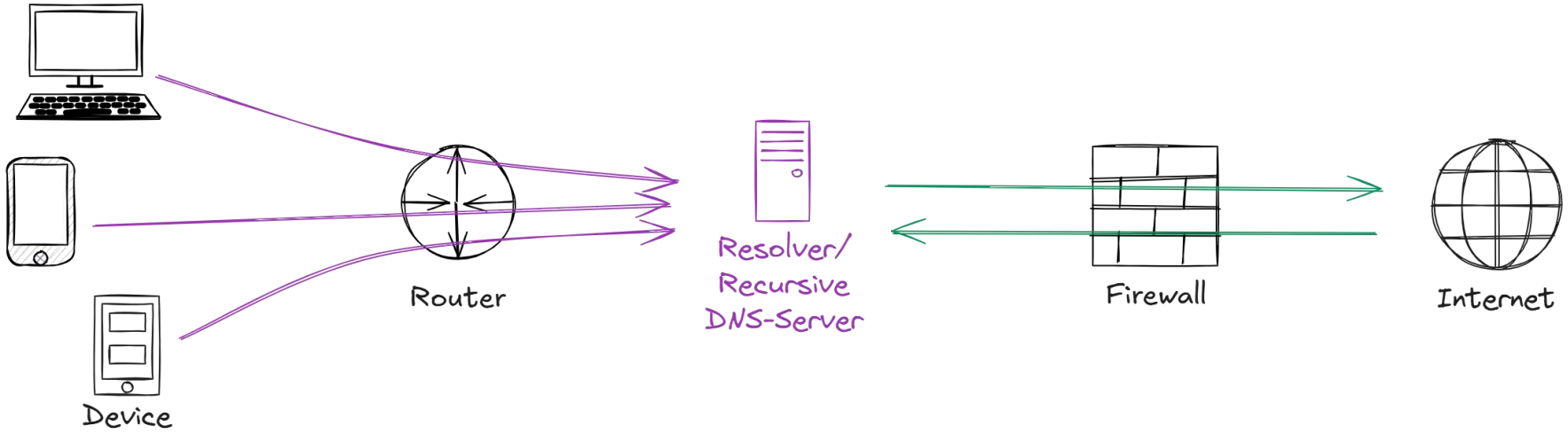
```
weberjoh@nb15-lx:~$ sudo iodine -f -P passphrase -r 85.22.58.63 io.weberlab.de
Opened dns0
Opened IPv4 UDP socket
Sending DNS queries for io.weberlab.de to 85.22.58.63
Autodetecting DNS query type (use -T to override).
Using DNS type NULL queries
Version ok, both using protocol v 0x00000502. You are user #0
Setting IP of dns0 to 192.168.99.2
Setting MTU of dns0 to 1130
Server tunnel IP is 192.168.99.1
Skipping raw mode
Using EDNS0 extension
Switching upstream to codec Base128
Server switched upstream to codec Base128
No alternative downstream codec available, using default (Raw)
Switching to lazy mode for low-latency
Server switched to lazy mode
Autoprobing max downstream fragment size... (skip with -m fragsize)
768 ok.. ...1152 not ok.. ...960 not ok.. 864 ok.. 912 ok.. 936 ok.. ...948 not
ok.. will use 936-2=934
Setting downstream fragment size to max 934...
Connection setup complete, transmitting data.
```


Apply a display filter ... <Ctrl-/>
TCP.Str
UDP.Str
DNS
RS/RA/DHCPv6
No. Time Time Delta Source Destination Protocol Code Src Port Dst Port Length TCP.Str UDP.Str DNS Qry or Host or SNI Info
1 0.000000 0.000000 85.214.7.23 85.215.94.29 DNS 59089 53 84 0 yrbwxm.io2.weberlab.de Standard q
2 0.000167 0.000167 85.215.94.29 85.214.7.23 DNS 53 59089 144 0 yrbwxm.io2.weberlab.de Standard q
3 0.029879 0.029712 85.214.7.23 85.215.94.29 DNS 56222 53 89 1 vaaaakas03u.io2.weberlab.de Standard q
4 0.030031 0.000152 85.215.94.29 85.214.7.23 DNS 53 56222 110 1 vaaaakas03u.io2.weberlab.de Standard q
5 0.058452 0.028421 85.214.7.23 85.215.94.29 DNS 36207 53 110 2 laczabxi4x0gb5lsfbfckgkh1r1dvv1q.io2.weberlab.de Standard q
6 0.058591 0.000139 85.215.94.29 85.214.7.23 DNS 53 36207 155 2 laczabxi4x0gb5lsfbfckgkh1r1dvv1q.io2.weberlab.de Standard q
7 0.086066 0.027475 85.214.7.23 85.215.94.29 DNS 45545 53 84 3 yrbwxp.io2.weberlab.de Standard q
8 0.086177 0.000111 85.215.94.29 85.214.7.23 DNS 53 45545 144 3 yrbwxp.io2.weberlab.de Standard q
9 0.105099 0.018922 85.214.7.23 85.215.94.29 DNS 60070 53 119 4 zwxqaA-Aaahhh-Drink-mal-ein-J@germeister-.io2.weberlab.de Standard q
10 0.105215 0.000116 85.215.94.29 85.214.7.23 DNS 53 60070 173 4 zwxqaA-Aaahhh-Drink-mal-ein-J@germeister-.io2.weberlab.de Standard q
11 1.124166 1.018951 85.214.7.23 85.215.94.29 DNS 52707 53 140 5 zwxraAbBcCdDeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZ+0129… Standard q
12 1.124301 0.000135 85.215.94.29 85.214.7.23 DNS 53 52707 215 5 zwxraAbBcCdDeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZ+0129… Standard q
13 1.144179 0.019878 85.214.7.23 85.215.94.29 DNS 40677 53 84 6 sagwxs.io2.weberlab.de Standard q
14 1.144309 0.000130 85.215.94.29 85.214.7.23 DNS 53 40677 102 6 sagwxs.io2.weberlab.de Standard q
15 1.166115 0.021806 85.214.7.23 85.215.94.29 DNS 40708 53 84 7 oalwxt.io2.weberlab.de Standard q
16 1.166218 0.000103 85.215.94.29 85.214.7.23 DNS 53 40708 100 7 oalwxt.io2.weberlab.de Standard q
17 1.187859 0.021641 85.214.7.23 85.215.94.29 DNS 55488 53 314 8 rayad8fR-8pt-8pt-8pt-8pt-8pt-8pt-8pt-8pt-8pt-8pt-8pt-8pt-8pt-… Standard q
18 1.187978 0.000119 85.215.94.29 85.214.7.23 DNS 53 55488 1094 8 rayad8fR-8pt-8pt-8pt-8pt-8pt-8pt-8pt-8pt-8pt-8pt-8pt-8pt-8pt-… Standard q
19 1.207091 0.019113 85.214.7.23 85.215.94.29 DNS 35259 53 314 9 rbead8vR08Fx08Fx08Fx08Fx08Fx08Fx08Fx08Fx08Fx08Fx08Fx08Fx08Fx08… Standard q
20 1.207201 0.000110 85.215.94.29 85.214.7.23 DNS 53 35259 1478 9 rbead8vR08Fx08Fx08Fx08Fx08Fx08Fx08Fx08Fx08Fx08Fx08Fx08Fx08Fx08… Standard q
Linux cooked capture v1
Internet Protocol Version 4, Src: 85.215.94.29, Dst: 85.214.7.23
User Datagram Protocol, Src Port: 53, Dst Port: 59089
Domain Name System (response)
Transaction ID: 0x1b89
Flags: 0x8400 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
Answers
yrbwxm.io2.weberlab.de: type NULL, class IN
Name: yrbwxm.io2.weberlab.de
Type: NULL (10) (RR)
Class: IN (0x0001)
Time to live: 0 (0 seconds)
Data length: 48
Null (data): 00000000ffffffff55555555aaaaaaaa8163c8d2c77cb2175f4fcec9492d522161a9712025b30673e6d84430795057bf
[Request In: 1]
[Time: 0.000167000 seconds]
0000 00 04 ff ff 00 00 00 00 00 00 00 00 00 00 08 00
0010 45 00 00 80 00 00 40 00 40 11 29 8c 55 d7 5e 1d
0020 55 d6 07 17 00 35 e6 d1 00 6c 11 5f 1b 89 84 00
0030 00 01 00 01 00 00 00 00 06 79 72 62 77 78 6d 03
0040 69 6f 32 08 77 65 62 65 72 6c 61 62 02 64 65 00
0050 00 0a 00 01 c0 0c 00 0a 00 01 00 00 00 00 00 30
0060 00 00 00 00 ff ff ff ff 55 55 55 55 aa aa aa aa
0070 81 63 c8 d2 c7 7c b2 17 5f 4f ce c9 49 2d 52 21
0080 61 a9 71 20 25 b3 06 73 e6 d8 44 30 79 50 57 bf
Null (data) (dns.null), 48 bytes
Packets: 221
Profile: Wireshark-Profile-JW-default

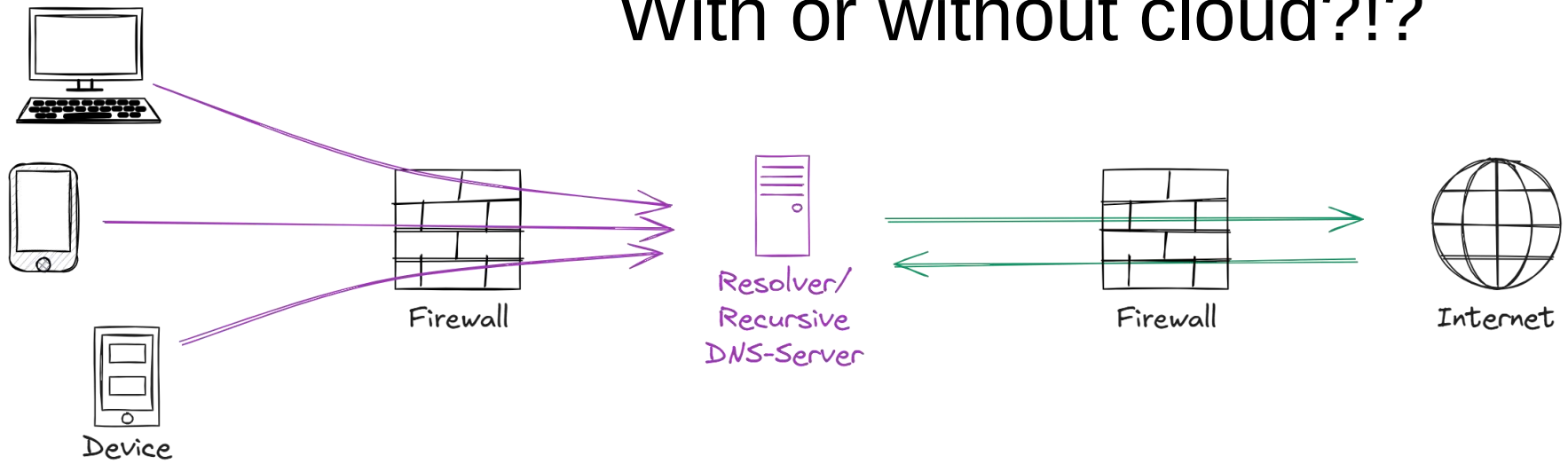
DNS-Exfiltration/-Tunneling

- Defense: Deep Query Inspection
  - Length of labels
  - Lexical analysis
  - Entropy of labels
  - Frequency
  - Total number of queries
  - Size of queries/responses

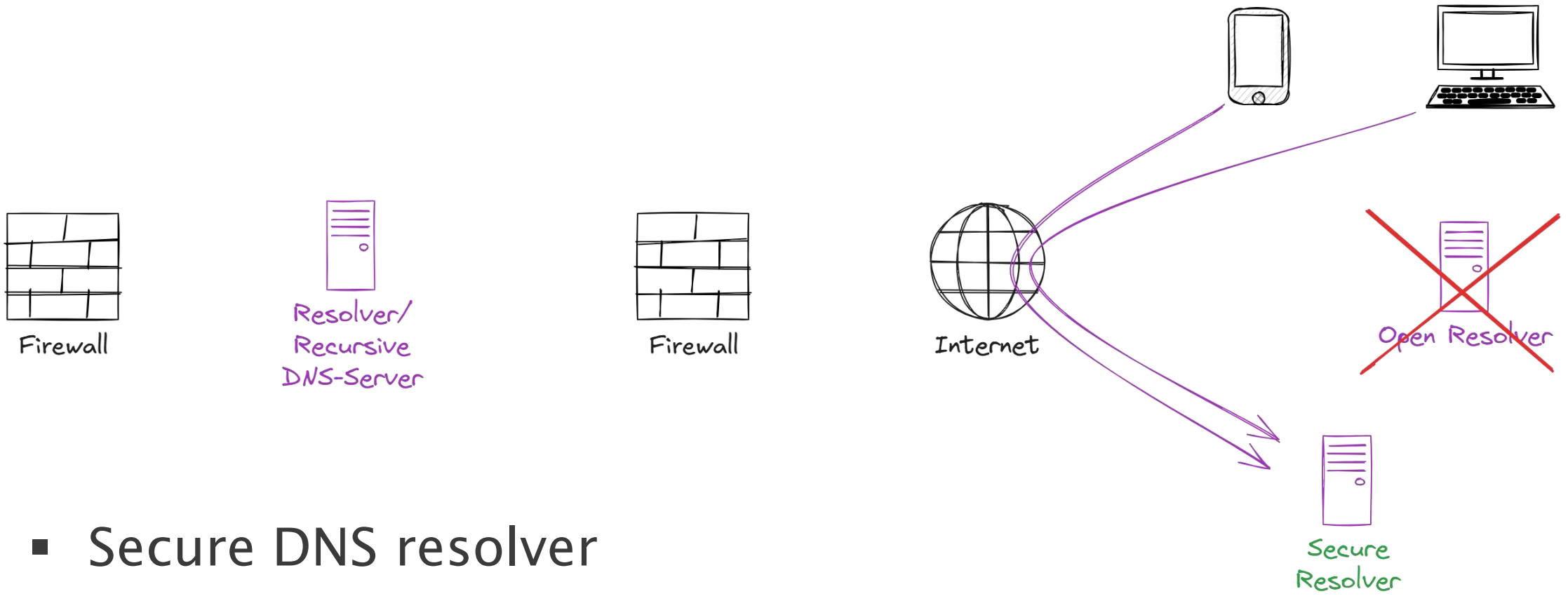
Where to leverage DNS-Security? On-Prem



License on segmentation firewall?
With or without cloud?!?



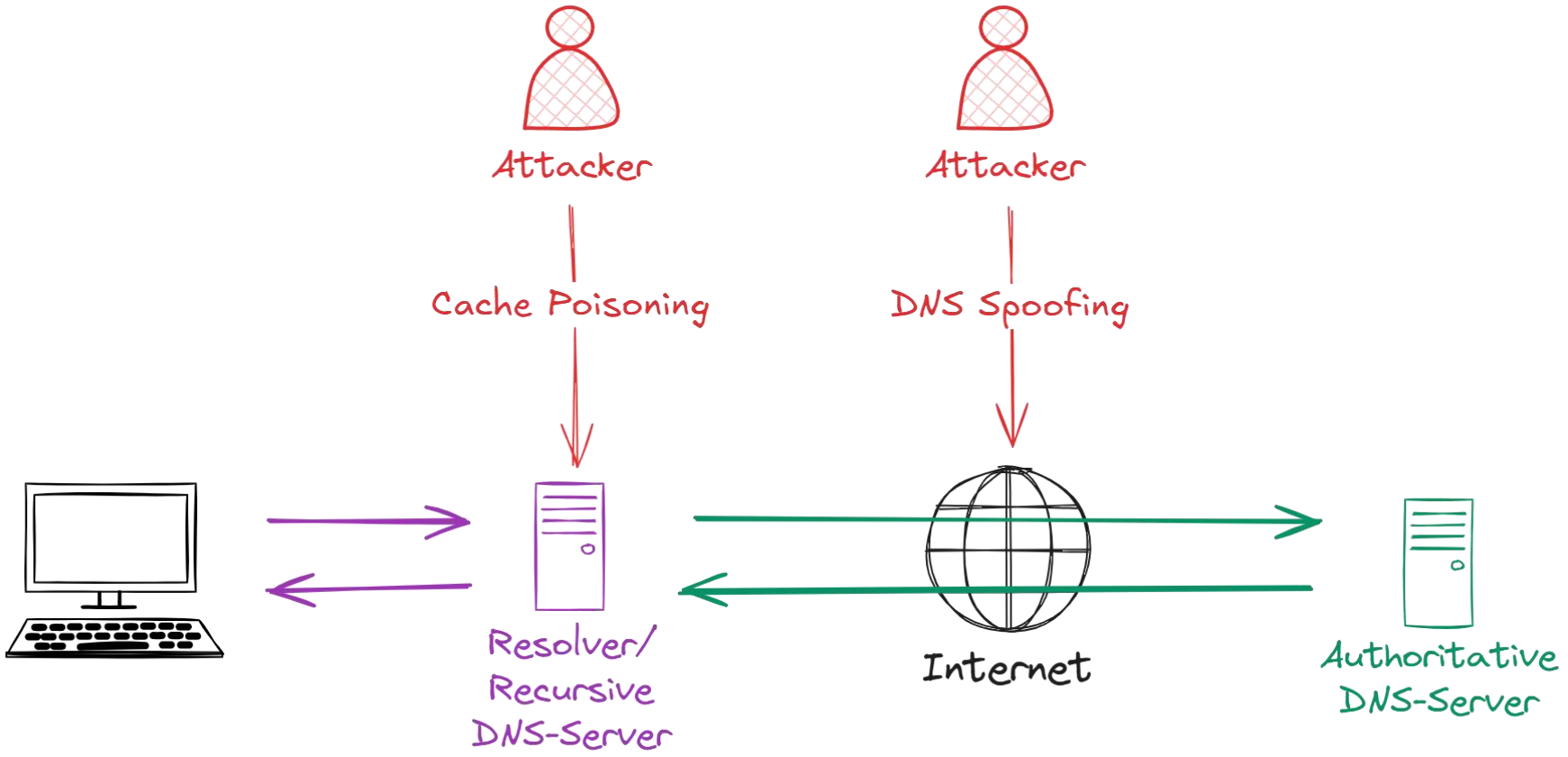
Where to leverage DNS-Security? Road Warrior



- Secure DNS resolver
- Via agent, full-tunnel VPN, proxy, #SASE #SSE

DNS Spoofing

DNS Spoofing / Cache Poisoning



DNS Spoofing

- UDP 53 <- easy to spoof
- MITM at layer 3
  - ARP-/NDP-spoofing
  - BGP hijacking
  - (root) access on a router
- (root) access on a resolver
- middleware like firewalls
- censoring states (packet drop is possible anyway)

- Defense: DNSSEC

DNS Cache Poisoning

- Fooling recursive resolver
  to store falsified RRs in its cache

- Attacker asks `something01.mybank.com A?`

- Attacker guesses source port & query ID

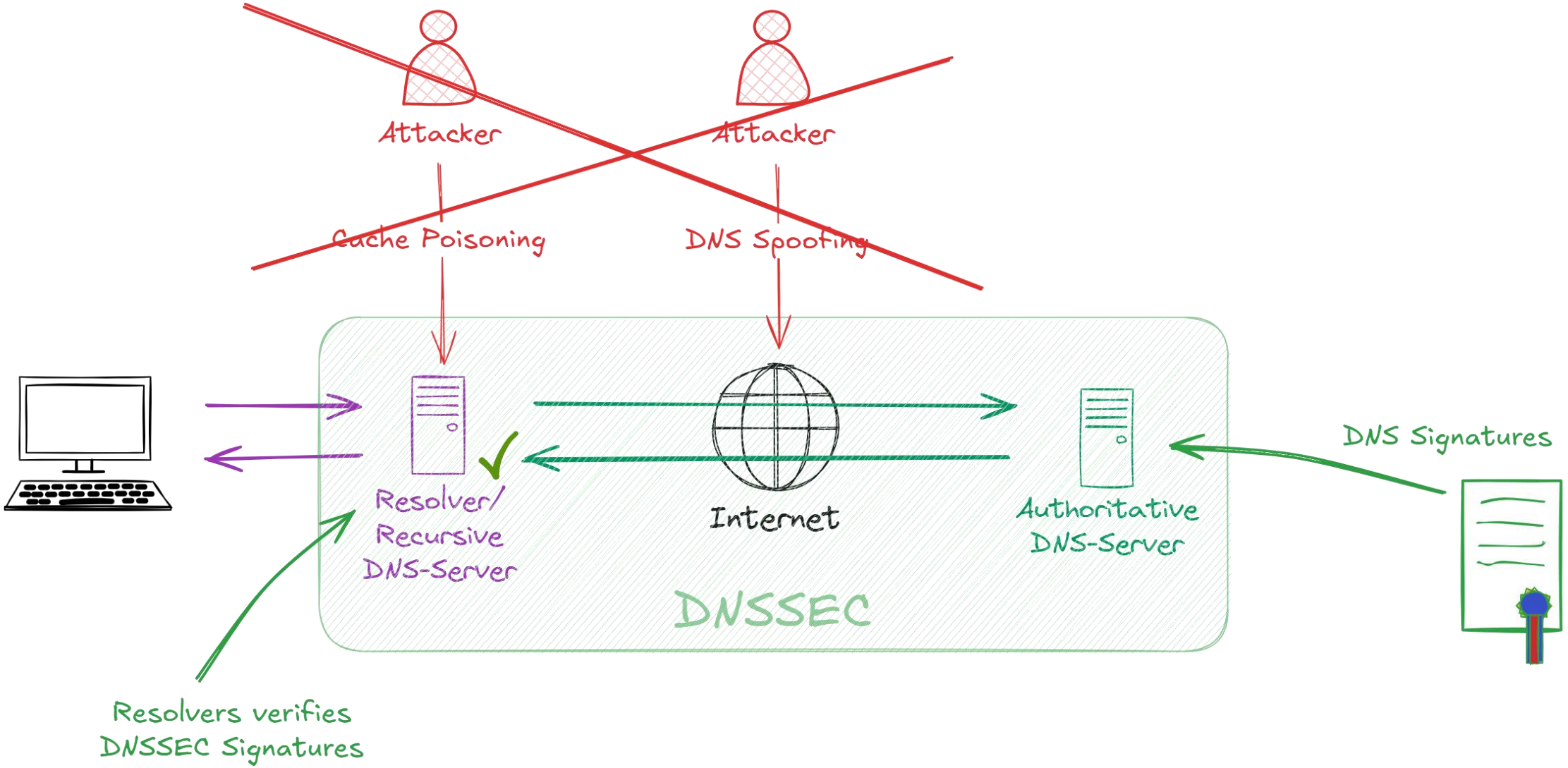
```
something01.mybank.com NS www.mybank.com

;;; ADDITIONAL SECTION
www.mybank.com 86400 IN A 192.0.2.66
```

- Defense: DNSSEC

DNSSEC

DNSSEC


Attacker
Attacker
Cache Poisoning
DNS Spoofing
Resolver/
Recursive
DNS-Server
Internet
Authoritative
DNS-Server
DNS Signatures
DNSSEC
Resolvers verifies
DNSSEC Signatures

DNSSEC

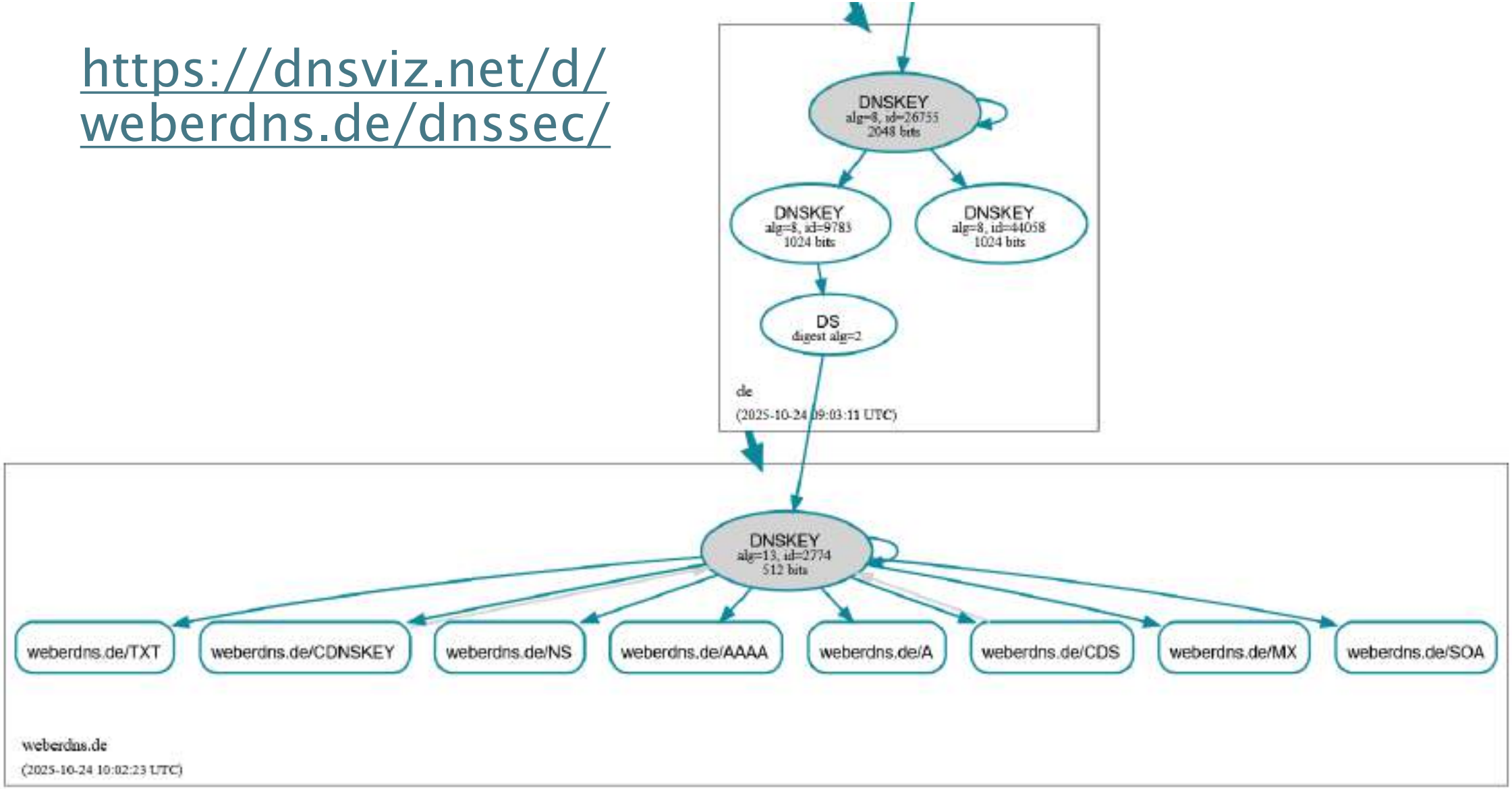
- Authenticity & integrity
- NOT: confidentiality!

- DNSKEY: KSK, ZSK
- DS signed in parent zone
- RRSIG

```
weberdns.de.     3600 IN A 87.106.163.167
weberdns.de.     3600 IN RRSIG A 13 2 3600 (
                         20251105201251 20251022193302 2774 weberdns.de.
                         Ud5Fi3p+X+sG6jz/2PcCR8F1OEZzoYxuPGMb4bWjCsZ+
                         HkCPjUR1t5LI5kmcfi7VQPfJnDAK6x2x2WXzVAGdIA== )
```

DNSViz

https://dnsviz.net/d/weberdns.de/dnssec/



dig

```
weberjoh@nuc:~$ dig weberdns.de

; <<>> DiG 9.18.39-0ubuntu0.22.04.2-Ubuntu <<>> weberdns.de
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40761
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;weberdns.de.                   IN      A

;; ANSWER SECTION:
weberdns.de.            3600    IN      A       87.106.163.167

;; Query time: 3 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Fri Oct 24 10:52:55 CEST 2025
;; MSG SIZE  rcvd: 56
```

dig

```
weberjoh@nuc:~$ dig weberdns.de +dnssec

; <<>> DiG 9.18.39-0ubuntu0.22.04.2-Ubuntu <<>> weberdns.de +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34320
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
weberdns.de.            3592    IN      A       87.106.163.167
weberdns.de.            3592    IN      RRSIG   A 13 2 3600 20251105201251
20251022193302 2774 weberdns.de.
Ud5Fi3p+X+sG6jz/2PcCR8F1OEZzoYxuPGMb4bWjCsZ+HkCPjUR1t5LI
5kmcfi7VQPfJnDAK6x2x2WXzVAGdIA==

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Fri Oct 24 10:53:03 CEST 2025
;; MSG SIZE  rcvd: 163
```

DNSSEC

- DNSSEC validation normally on resolvers, not clients

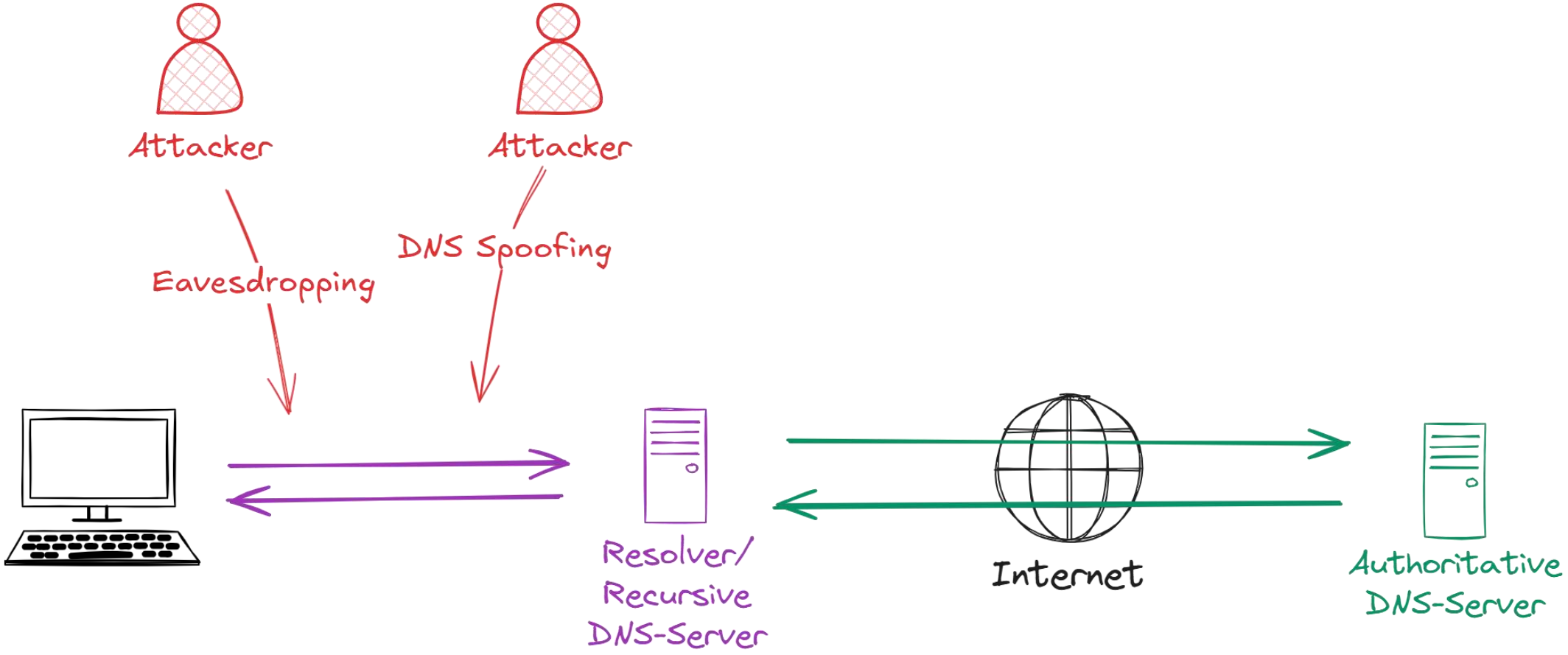
- DNSSEC-Validation: Client-Side
- http://www.dnssec-or-not.com/
- https://wander.science/projects/dns/dnssec-resolver-test/

- Caution: Attackers will sign their zones as well ☹

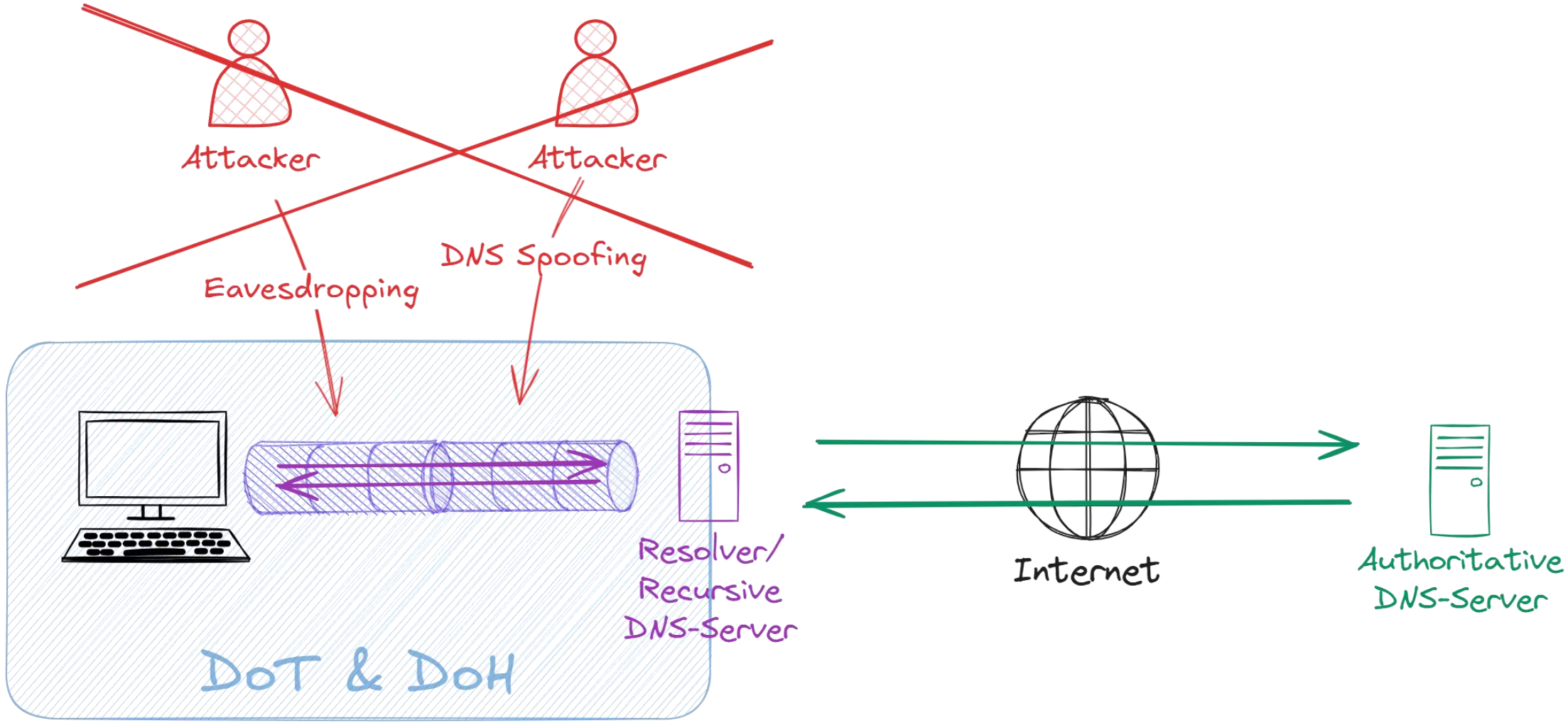
- https://weberblog.net/dns/

DoT & DoH

DoT & DoH


Attacker
Attacker
Eavesdropping
DNS Spoofing
Resolver/
Recursive
DNS-Server
Internet
Authoritative
DNS-Server

DoT & DoH


Attacker
Attacker
Eavesdropping
DNS Spoofing
Resolver/
Recursive
DNS-Server
DoT & DoH
Internet
Authoritative
DNS-Server

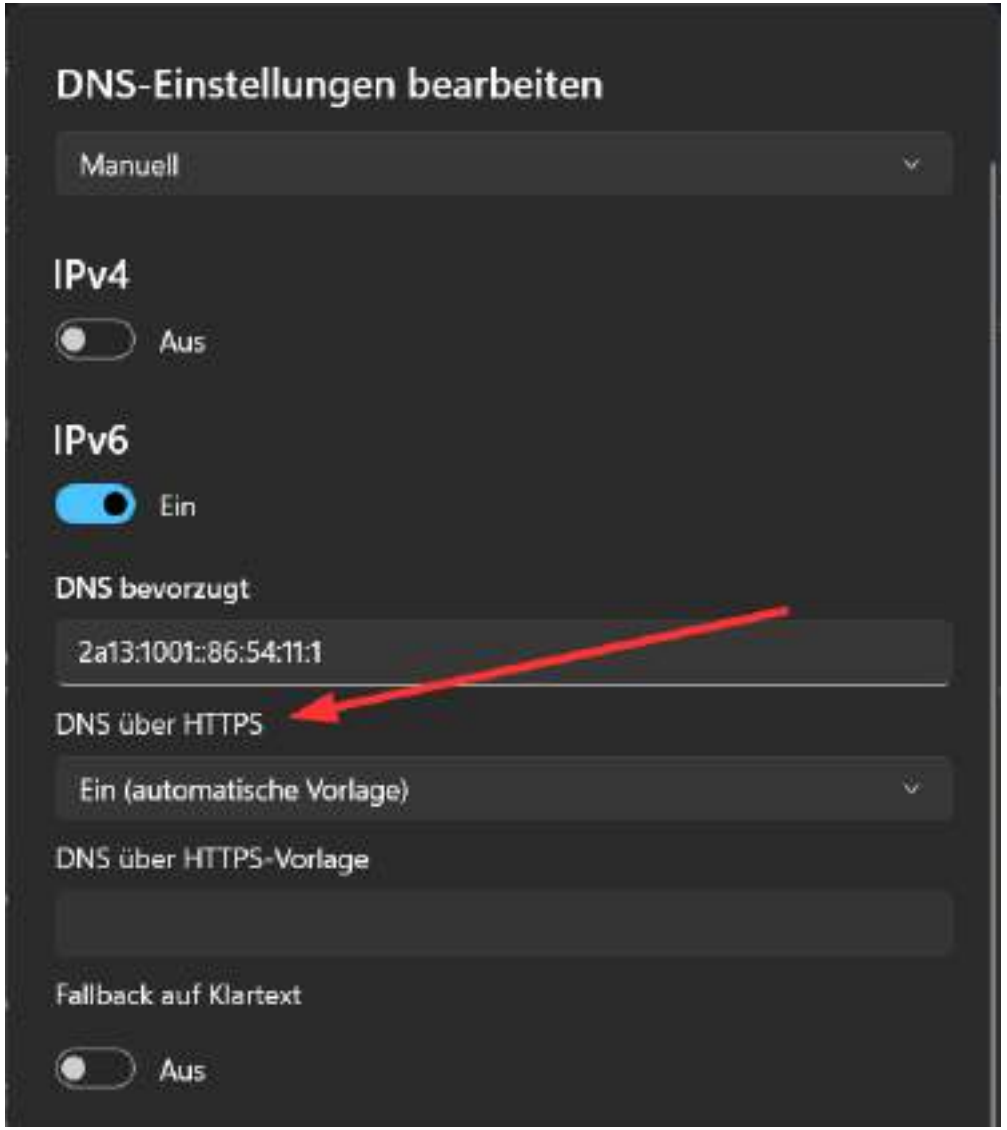
DoT & DoH

- Confidentiality!
- DoT, DNS-over-TLS: `tcp.port eq 853`
  - Encryption between **OS** <-> **Resolver**
- DoH, DNS-over-HTTPS: `tcp.port eq 443`
  - Encryption between **App (Browser)** <-> **Resolver**
  - Encryption between **OS** <-> **Resolver**

```
curl -H 'accept: application/dns-json' 'https://cloudflare-
dns.com/dns-query?name=example.com&type=A' | jq .
```

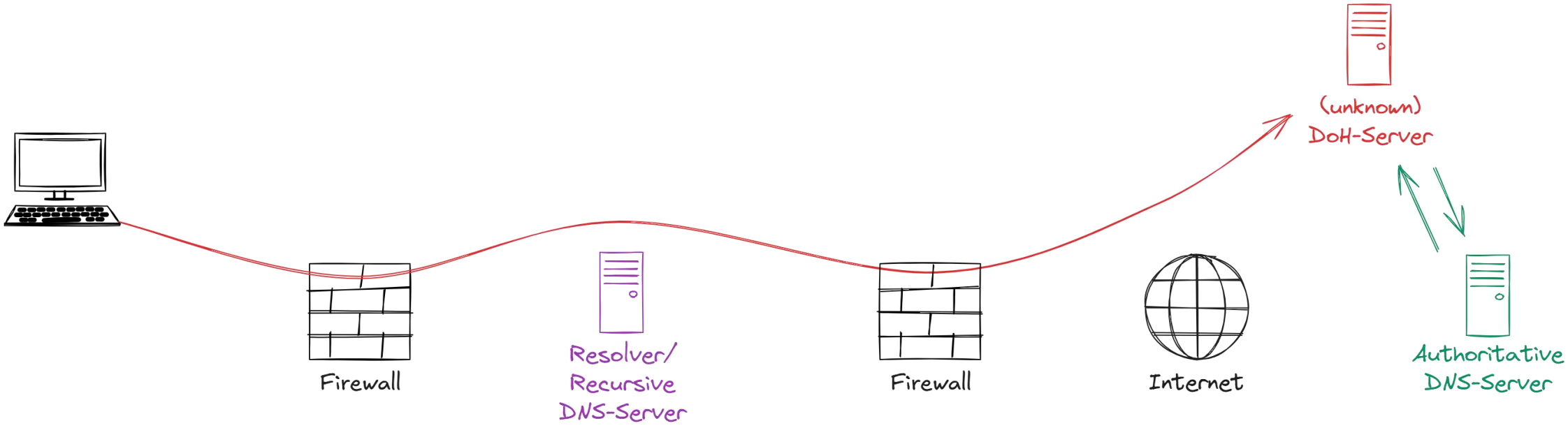
```
curl -H 'accept: application/dns-message' 'https://dns.google/dns-
query?dns=q80BAAABAAAAAAAAA3d3dwdleGFtcGxlA2NvbQAAAQAB'  | hexdump -c
```

DoH in Windows 11



DoT & DoH

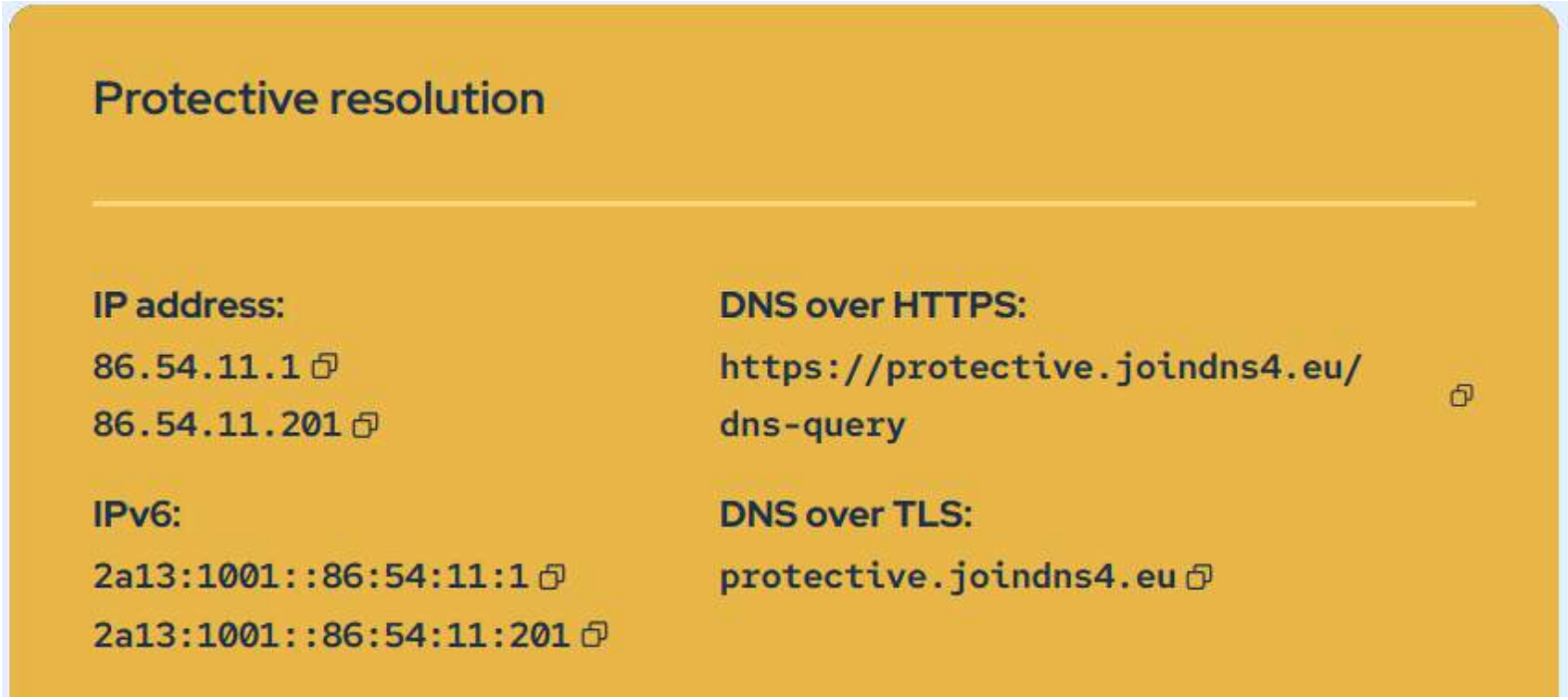
- DoH might circumvent internal DNS security!



- Best Practise: Blocking of DoH on firewalls / Disabling DoH through group policies
- Offer DoH on your resolver

DNS4EU

- https://www.joindns4.eu/
- Protect yourself -> Protective resolution



Testing DoT & DoH

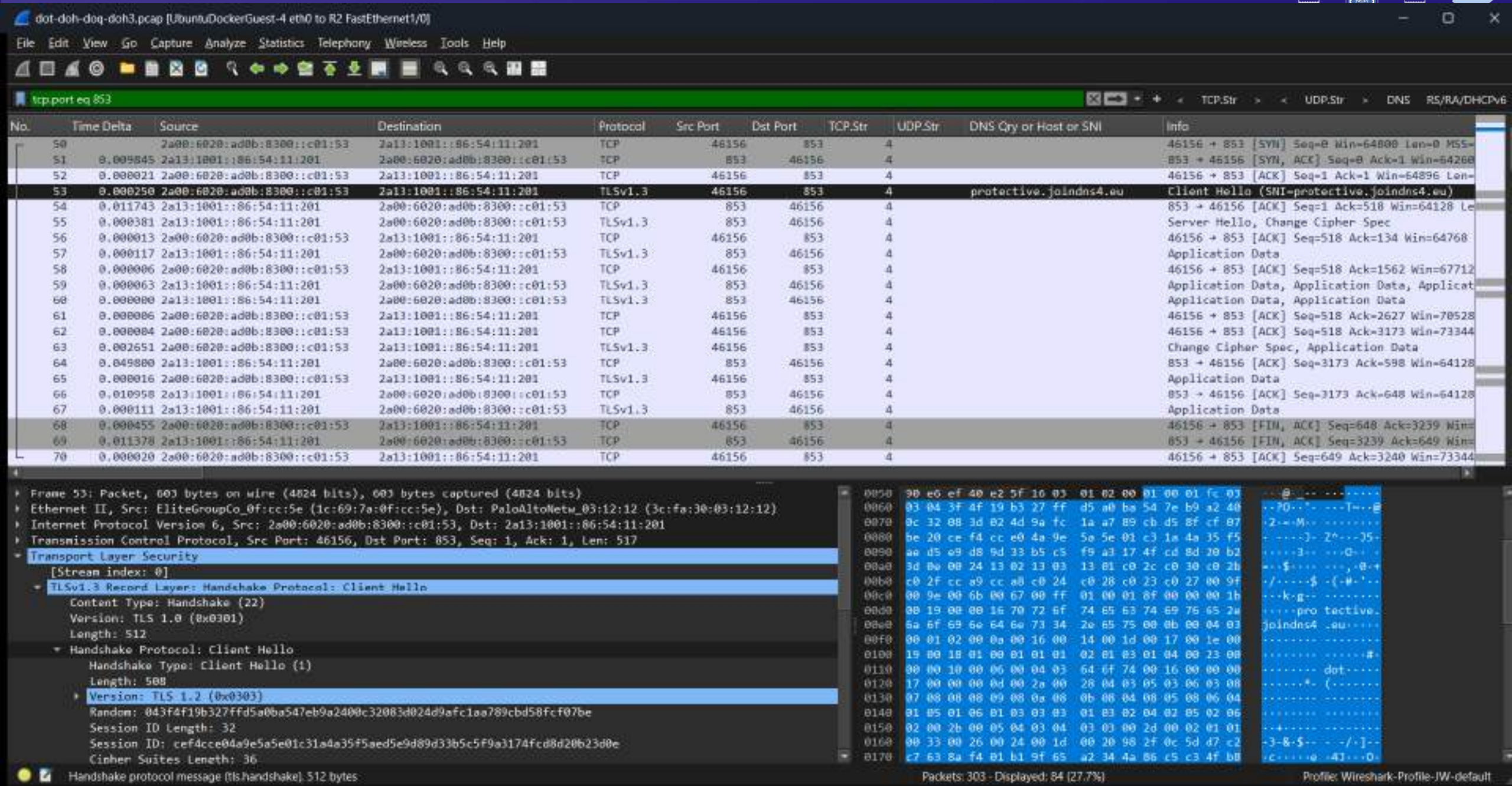
```
dig @protective.joindns4.eu +tls heise.de
dig @protective.joindns4.eu +https heise.de
```

- DNSDiag: https://dnsdiag.org/

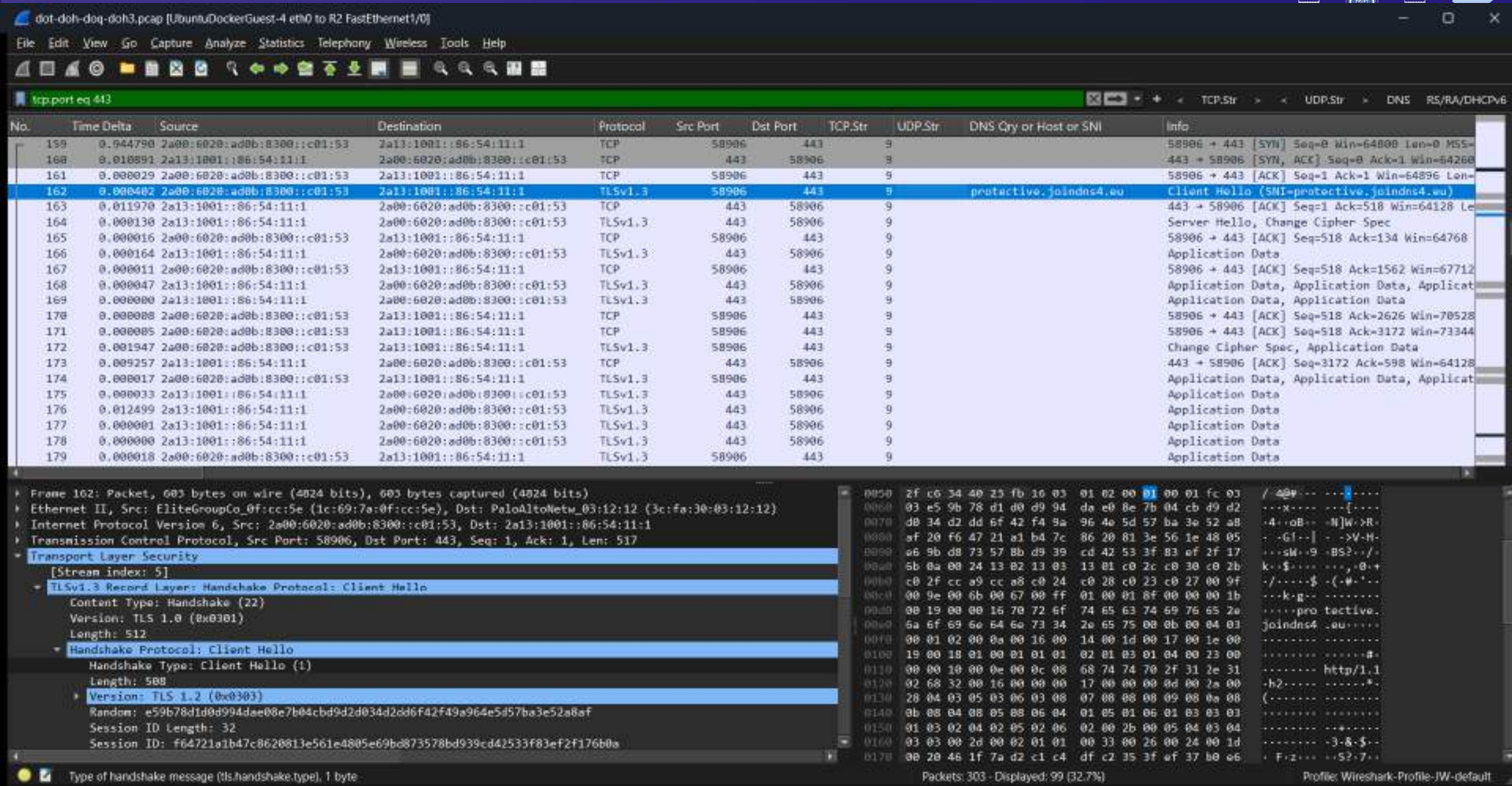
```
./dnsping.py --server 2a13:1001::86:54:11:1 heise.de
./dnsping.py --server protective.joindns4.eu --tls heise.de
./dnsping.py --server protective.joindns4.eu --doh heise.de
```

- Ultimate PCAP: https://weberblog.net/the-ultimate-pcap/

DoT


dot-doh-doq-doh3.pcap [Ubuntu\DockerGuest-4 eth0 to R2 FastEthernet1/0]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port eq 853
TCP.Str UDP.Str DNS RS/RA/DHCPv6
No. Time Delta Source Destination Protocol Src Port Dst Port TCP.Str UDP.Str DNS Qry or Host or SNI Info
50 2a00:6020:ad0b:8300::c01:53 2a13:1001::86:54:11:201 TCP 46156 853 4 46156 → 853 [SYN] Seq=0 Win=64800 Len=0 MSS=
51 0.005845 2a13:1001::86:54:11:201 2a00:6020:ad0b:8300::c01:53 TCP 853 46156 4 853 → 46156 [SYN, ACK] Seq=0 Ack=1 Win=64260
52 0.000021 2a00:6020:ad0b:8300::c01:53 2a13:1001::86:54:11:201 TCP 46156 853 4 46156 → 853 [ACK] Seq=1 Ack=1 Win=64896 Len=
53 0.000250 2a00:6020:ad0b:8300::c01:53 2a13:1001::86:54:11:201 TLSv1.3 46156 853 4 protective.joindns4.eu Client Hello (SNI=protective.joindns4.eu)
54 0.011743 2a13:1001::86:54:11:201 2a00:6020:ad0b:8300::c01:53 TCP 853 46156 4 853 → 46156 [ACK] Seq=1 Ack=518 Win=64128 Le
55 0.000381 2a13:1001::86:54:11:201 2a00:6020:ad0b:8300::c01:53 TLSv1.3 853 46156 4 Server Hello, Change Cipher Spec
56 0.000013 2a00:6020:ad0b:8300::c01:53 2a13:1001::86:54:11:201 TCP 46156 853 4 46156 → 853 [ACK] Seq=518 Ack=134 Win=64768
57 0.000117 2a13:1001::86:54:11:201 2a00:6020:ad0b:8300::c01:53 TLSv1.3 853 46156 4 Application Data
58 0.000006 2a00:6020:ad0b:8300::c01:53 2a13:1001::86:54:11:201 TCP 46156 853 4 46156 → 853 [ACK] Seq=518 Ack=1562 Win=67712
59 0.000063 2a13:1001::86:54:11:201 2a00:6020:ad0b:8300::c01:53 TLSv1.3 853 46156 4 Application Data, Application Data, Applicat
60 0.000000 2a13:1001::86:54:11:201 2a00:6020:ad0b:8300::c01:53 TLSv1.3 853 46156 4 Application Data, Application Data
61 0.000006 2a00:6020:ad0b:8300::c01:53 2a13:1001::86:54:11:201 TCP 46156 853 4 46156 → 853 [ACK] Seq=518 Ack=2627 Win=70528
62 0.000004 2a00:6020:ad0b:8300::c01:53 2a13:1001::86:54:11:201 TCP 46156 853 4 46156 → 853 [ACK] Seq=518 Ack=3173 Win=73344
63 0.002651 2a00:6020:ad0b:8300::c01:53 2a13:1001::86:54:11:201 TLSv1.3 46156 853 4 Change Cipher Spec, Application Data
64 0.045880 2a13:1001::86:54:11:201 2a00:6020:ad0b:8300::c01:53 TCP 853 46156 4 853 → 46156 [ACK] Seq=3173 Ack=598 Win=64128
65 0.000016 2a00:6020:ad0b:8300::c01:53 2a13:1001::86:54:11:201 TLSv1.3 46156 853 4 Application Data
66 0.010958 2a13:1001::86:54:11:201 2a00:6020:ad0b:8300::c01:53 TCP 853 46156 4 853 → 46156 [ACK] Seq=3173 Ack=648 Win=64128
67 0.000111 2a13:1001::86:54:11:201 2a00:6020:ad0b:8300::c01:53 TLSv1.3 853 46156 4 Application Data
68 0.000455 2a00:6020:ad0b:8300::c01:53 2a13:1001::86:54:11:201 TCP 46156 853 4 46156 → 853 [FIN, ACK] Seq=648 Ack=3239 Win=
69 0.011378 2a13:1001::86:54:11:201 2a00:6020:ad0b:8300::c01:53 TCP 853 46156 4 853 → 46156 [FIN, ACK] Seq=3239 Ack=649 Win=
70 0.000020 2a00:6020:ad0b:8300::c01:53 2a13:1001::86:54:11:201 TCP 46156 853 4 46156 → 853 [ACK] Seq=649 Ack=3240 Win=73344
Frame 53: Packet, 603 bytes on wire (4824 bits), 603 bytes captured (4824 bits)
Ethernet II, Src: EliteGroupCo_0f:cc:5e (1c:69:7a:0f:cc:5e), Dst: PaloAltoNetw_03:12:12 (3c:fa:30:03:12:12)
Internet Protocol Version 6, Src: 2a00:6020:ad0b:8300::c01:53, Dst: 2a13:1001::86:54:11:201
Transmission Control Protocol, Src Port: 46156, Dst Port: 853, Seq: 1, Ack: 1, Len: 517
Transport Layer Security
[Stream index: 0]
TLSv1.3 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 512
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 508
Version: TLS 1.2 (0x0303)
Random: 043f4f19b327ffd5a0ba547eb9a2400c32083d024d9afc1aa789cbd58fcf07be
Session ID Length: 32
Session ID: cef4cce04a9e5a5e01c31a4a35f5aed5e9d89d33b5c5f9a3174fcd8d20b23d0e
Cipher Suites Length: 36
0050 00 e6 ef 40 e2 5f 16 03 01 02 00 01 00 01 fc 03
0060 03 04 3f 4f 19 b3 27 ff d5 a0 ba 54 7e b9 a2 40
0070 0c 32 08 3d 02 4d 9a fc 1a a7 89 cb d5 8f cf 07
0080 be 20 ce f4 cc e0 4a 9e 5e 5e 01 c3 1a 4a 35 f5
0090 aa d5 e9 d8 9d 33 b5 c5 f9 a3 17 4f cd 8d 20 b2
00a0 3d 0e 00 24 13 02 13 03 13 01 c0 2c c0 30 c0 2b
00b0 c0 2f cc a9 cc a8 c0 24 c0 28 c0 23 c0 27 00 9f
00c0 00 9e 00 6b 00 67 00 ff 01 00 01 8f 00 00 00 1b
00d0 00 19 00 00 16 70 72 6f 74 65 63 74 69 76 65 2e
00e0 6a 6f 69 6e 64 6e 73 34 2e 65 75 00 0b 00 04 03
00f0 00 01 02 00 0a 00 16 00 14 00 1d 00 17 00 1e 00
0100 19 00 18 01 00 01 01 01 02 01 03 01 04 00 23 00
0110 00 00 10 00 06 00 04 03 64 6f 74 00 16 00 00 00
0120 17 00 00 00 0d 00 2a 00 28 04 03 05 03 06 03 08
0130 07 08 08 08 09 08 0a 08 0b 08 04 08 05 08 06 04
0140 01 05 01 06 01 03 03 03 01 03 02 04 02 05 02 06
0150 02 00 2b 00 05 04 03 04 03 03 00 2d 00 02 01 01
0160 00 33 00 26 00 24 00 1d 00 20 98 2f 0c 5d d7 c2
0170 c7 63 8a f4 01 b1 9f 65 a2 34 4a 86 c5 c3 4f b8
Handshake protocol message (tls.handshake), 512 bytes
Packets: 303 - Displayed: 84 (27.7%)
Profile: Wireshark-Profile-JW-default

DoH


dot-doh-doq-doh3.pcap [UbuntuDockerGuest-4 eth0 to R2 FastEthernet1/0]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port eq 443
TCP.Str UDP.Str DNS RS/RA/DHCPv6
No. Time Delta Source Destination Protocol Src Port Dst Port TCP.Str UDP.Str DNS Qry or Host or SNI Info
159 0.944790 2a00:6020:ad0b:8300::c01:53 2a13:1001::86:54:11:1 TCP 58906 443 9 58906 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=
160 0.010891 2a13:1001::86:54:11:1 2a00:6020:ad0b:8300::c01:53 TCP 443 58906 9 443 → 58906 [SYN, ACK] Seq=0 Ack=1 Win=64260
161 0.000029 2a00:6020:ad0b:8300::c01:53 2a13:1001::86:54:11:1 TCP 58906 443 9 58906 → 443 [ACK] Seq=1 Ack=1 Win=64896 Len=
162 0.000402 2a00:6020:ad0b:8300::c01:53 2a13:1001::86:54:11:1 TLSv1.3 58906 443 9 protective.joindns4.eu Client Hello (SNI=protective.joindns4.eu)
163 0.011970 2a13:1001::86:54:11:1 2a00:6020:ad0b:8300::c01:53 TCP 443 58906 9 443 → 58906 [ACK] Seq=1 Ack=518 Win=64128 Le
164 0.000130 2a13:1001::86:54:11:1 2a00:6020:ad0b:8300::c01:53 TLSv1.3 443 58906 9 Server Hello, Change Cipher Spec
165 0.000016 2a00:6020:ad0b:8300::c01:53 2a13:1001::86:54:11:1 TCP 58906 443 9 58906 → 443 [ACK] Seq=518 Ack=134 Win=64768
166 0.000164 2a13:1001::86:54:11:1 2a00:6020:ad0b:8300::c01:53 TLSv1.3 443 58906 9 Application Data
167 0.000011 2a00:6020:ad0b:8300::c01:53 2a13:1001::86:54:11:1 TCP 58906 443 9 58906 → 443 [ACK] Seq=518 Ack=1562 Win=67712
168 0.000047 2a13:1001::86:54:11:1 2a00:6020:ad0b:8300::c01:53 TLSv1.3 443 58906 9 Application Data, Application Data, Applicat
169 0.000000 2a13:1001::86:54:11:1 2a00:6020:ad0b:8300::c01:53 TLSv1.3 443 58906 9 Application Data, Application Data
170 0.000008 2a00:6020:ad0b:8300::c01:53 2a13:1001::86:54:11:1 TCP 58906 443 9 58906 → 443 [ACK] Seq=518 Ack=2626 Win=70528
171 0.000005 2a00:6020:ad0b:8300::c01:53 2a13:1001::86:54:11:1 TCP 58906 443 9 58906 → 443 [ACK] Seq=518 Ack=3172 Win=73344
172 0.001947 2a00:6020:ad0b:8300::c01:53 2a13:1001::86:54:11:1 TLSv1.3 58906 443 9 Change Cipher Spec, Application Data
173 0.009257 2a13:1001::86:54:11:1 2a00:6020:ad0b:8300::c01:53 TCP 443 58906 9 443 → 58906 [ACK] Seq=3172 Ack=598 Win=64128
174 0.000017 2a00:6020:ad0b:8300::c01:53 2a13:1001::86:54:11:1 TLSv1.3 58906 443 9 Application Data, Application Data, Applicat
175 0.000033 2a13:1001::86:54:11:1 2a00:6020:ad0b:8300::c01:53 TLSv1.3 443 58906 9 Application Data
176 0.012499 2a13:1001::86:54:11:1 2a00:6020:ad0b:8300::c01:53 TLSv1.3 443 58906 9 Application Data
177 0.000001 2a13:1001::86:54:11:1 2a00:6020:ad0b:8300::c01:53 TLSv1.3 443 58906 9 Application Data
178 0.000000 2a13:1001::86:54:11:1 2a00:6020:ad0b:8300::c01:53 TLSv1.3 443 58906 9 Application Data
179 0.000018 2a00:6020:ad0b:8300::c01:53 2a13:1001::86:54:11:1 TLSv1.3 58906 443 9 Application Data
Frame 162: Packet, 603 bytes on wire (4824 bits), 603 bytes captured (4824 bits)
Ethernet II, Src: EliteGroupCo_0f:cc:5e (1c:69:7a:0f:cc:5e), Dst: PaloAltoNetw_03:12:12 (3c:fa:30:03:12:12)
Internet Protocol Version 6, Src: 2a00:6020:ad0b:8300::c01:53, Dst: 2a13:1001::86:54:11:1
Transmission Control Protocol, Src Port: 58906, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
Transport Layer Security
[Stream index: 5]
TLSv1.3 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 512
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 508
Version: TLS 1.2 (0x0303)
Random: e59b78d1d0d994dae08e7b04cbd9d2d034d2dd6f42f49a964e5d57ba3e52a8af
Session ID Length: 32
Session ID: f64721a1b47c8620813e561e4805e69bd873578bd939cd42533f83ef2f176b0a
0050 2f c6 34 40 25 fb 16 03 01 02 00 01 00 01 fc 03
0060 03 e5 9b 78 d1 d0 d9 94 da e0 8e 7b 04 cb d9 d2
0070 d0 34 d2 dd 6f 42 f4 9a 96 4e 5d 57 ba 3e 52 a8
0080 af 20 f6 47 21 a1 b4 7c 86 20 81 3e 56 1e 48 05
0090 e6 9b d8 73 57 8b d9 39 cd 42 53 3f 83 ef 2f 17
00a0 5b 0a 00 24 13 02 13 03 13 01 c0 2c c0 30 c0 2b
00b0 c0 2f cc a9 cc a8 c0 24 c0 28 c0 23 c0 27 00 9f
00c0 00 9e 00 6b 00 67 00 ff 01 00 01 8f 00 00 00 1b
00d0 00 19 00 00 16 70 72 6f 74 65 63 74 69 76 65 2e
00e0 6a 6f 69 6e 64 6e 73 34 2e 65 75 00 0b 00 04 03
00f0 00 01 02 00 0a 00 16 00 14 00 1d 00 17 00 1e 00
0100 19 00 18 01 00 01 01 01 02 01 03 01 04 00 23 00
0110 00 00 10 00 0e 00 0c 08 68 74 74 70 2f 31 2e 31
0120 02 68 32 00 16 00 00 00 17 00 00 00 0d 00 2a 00
0130 28 04 03 05 03 06 03 08 07 08 08 08 09 08 0a 08
0140 0b 08 04 08 05 08 06 04 01 05 01 06 01 03 03 03
0150 01 03 02 04 02 05 02 06 02 00 2b 00 05 04 03 04
0160 03 03 00 2d 00 02 01 01 00 33 00 26 00 24 00 1d
0170 00 20 46 1f 7a d2 c1 c4 df c2 35 3f af 37 b0 e6
Type of handshake message (tls.handshake.type), 1 byte
Packets: 303 · Displayed: 99 (32.7%)
Profile: Wireshark-Profile-JW-default

Palo Alto Traffic Log

01::86:54:11:201') or (addr.dst in '2a10:50c0::ad1:ff') or (addr.dst in '2a10:50c0::ad2:ff')

FROM ZONE	TO ZONE	SOURCE	DESTINATION	IP PROTO...	FROM PORT	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON	BYTES SENT	BYTES R
DMZ	Internet	2a00:6020:ad0b:8300::c01:53	2a10:50c0::ad1:ff	udp	52874	443	quic-base			aged-out	2.9k	3.7k
DMZ	Internet	2a00:6020:ad0b:8300::c01:53	2a10:50c0::ad2:ff	udp	33713	443	quic-base			aged-out	4.2k	3.9k
DMZ	Internet	2a00:6020:ad0b:8300::c01:53	2a10:50c0::ad1:ff	udp	35898	853	unknown-udp	allow	NUC raus mit Logging	aged-out	4.1k	3.8k
DMZ	Internet	2a00:6020:ad0b:8300::c01:53	2a10:50c0::ad1:ff	udp	52879	853	unknown-udp			aged-out	2.9k	3.5k
DMZ	Internet	2a00:6020:ad0b:8300::c01:53	2a10:50c0::ad1:ff	udp	58092	853	unknown-udp			aged-out	4.1k	3.7k
DMZ	Internet	2a00:6020:ad0b:8300::c01:53	2a10:50c0::ad1:ff	udp	44640	853	unknown-udp	allow	NUC raus mit Logging	aged-out	4.1k	3.7k
DMZ	Internet	2a00:6020:ad0b:8300::c01:53	2a13:1001::86:54:11:201	tcp	46110	443	ssl			tcp-fin	2.1k	4.3k
DMZ	Internet	2a00:6020:ad0b:8300::c01:53	2a13:1001::86:54:11:201	tcp	46100	443	ssl			tcp-fin	2.1k	4.4k
DMZ	Internet	2a00:6020:ad0b:8300::c01:53	2a13:1001::86:54:11:201	tcp	46172	853	ssl	allow	NUC raus mit Logging	tcp-fin	1.6k	4.1k
DMZ	Internet	2a00:6020:ad0b:8300::c01:53	2a13:1001::86:54:11:201	tcp	46162	853	ssl			tcp-fin	1.6k	4.1k
DMZ	Internet	2a00:6020:ad0b:8300::c01:53	2a13:1001::86:54:11:201	tcp	46160	853	ssl			tcp-fin	1.6k	4.1k
DMZ	Internet	2a00:6020:ad0b:8300::c01:53	2a13:1001::86:54:11:201	tcp	46156	853	ssl	allow	NUC raus mit Logging	tcp-fin	1.6k	4.1k

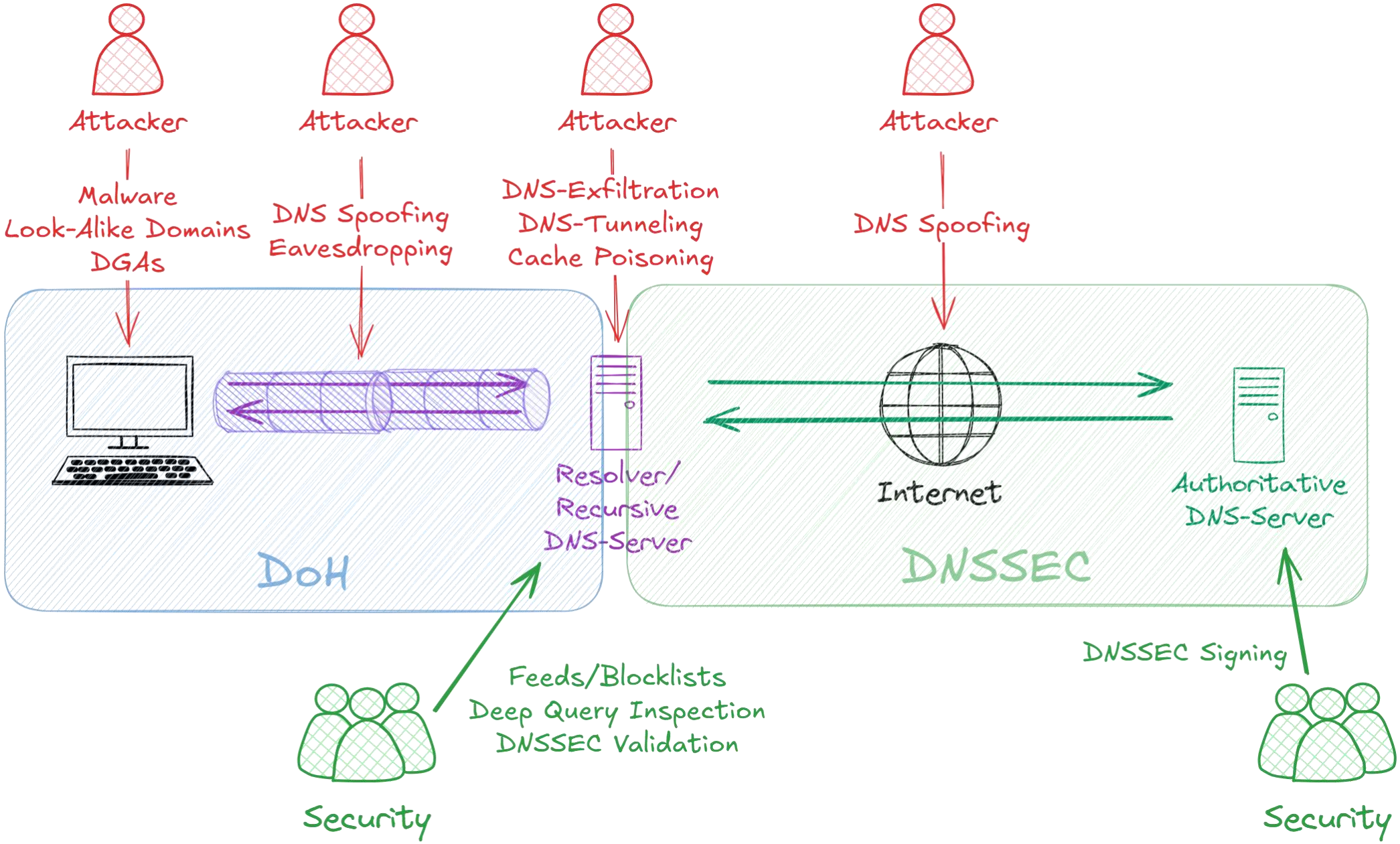
DoH3 = UDP/443

DoQ = UDP/853

DoH = TCP/443

DoT = TCP/853

Secure DNS - Summary



Secure DNS @Home

- Pi-hole: https://pi-hole.net/

✅ Blocking ads, tracking, malware (known malicious)
✅ DNSSEC validation
✅ [optional] own recursive resolver
🟡 DGAs
❌ DNS-Exfiltration/-Tunneling

- https://weberblog.net/pi-hole-installation-guide/
- https://github.com/hagezi/dns-blocklists
- DNS4EU: https://www.joindns4.eu/

Pi-hole

hostname: nuc

Status
- Active
- 3.8 q/s
- Load: 0.70 / 0.70 / 0.71
- Memory usage: 35.8 %

MAIN
- Dashboard
- Query Log

GROUP MANAGEMENT
- Groups 1
- Clients 0
- Domains 6 14
- Lists 808.936 30

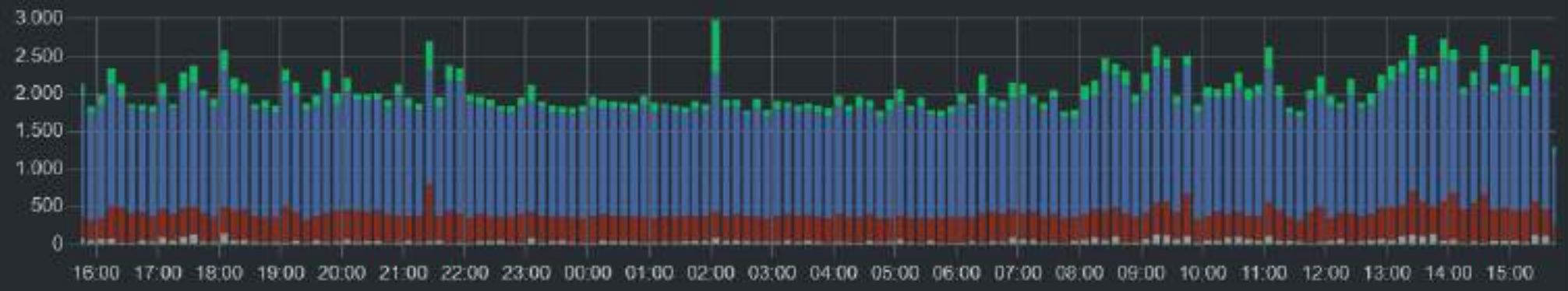
DNS CONTROL
- Disable Blocking

SYSTEM
- Settings
- Tools

DONATE

Total Queries	Queries Blocked	Percentage Blocked	Domains on Lists
299.073	53.251	17.8%	808.936
57 active clients	List blocked queries	List all queries	Manage lists

Total queries



Client activity

Challenges for DNS

- Query and response logging is a MUCH DATA!
- Logging to a SIEM only does not block anything
- UDP size (→ IP fragmentation) vs. TCP
- Legitimate DNS tunnelings do exist 🤦
  - McAfee, Spotify, Apple

What we've not talked about

- DoQ, DoH3
- Oblivious DNS over HTTPS (ODoH)
- DNS cookies
- TSIG, EDNS(0)
- DANE: TLSA, SSHFP, CAA
- SPF/DKIM/DMARC
- …

Thanks for watching ;)