Hackathon AIS’19

Measurement group

DNS over HTTPS/TLS team

Team name: Just DoH it!

Kampala, 19-20 June 2019

Group’s members

❑Philippe Muziko	Congo DRC	Citadella corporation
❑Yazid AKANHO	Benin	ISOC Benin
❑Angela Natlapeng	Botswana	Bocra
❑Japser den Hertog	Netherlands	RIPE NCC
❑Jasper Mangwana	Zimbabwe	SCA
❑Samuel Ochola	Uganda	Busitema University

Problem statement

- Traditional DNS queries and responses are sent over UDP or TCP without encryption.
- Vulnerable to eavesdropping and spoofing. Responses from recursive resolvers to clients are the most vulnerable to undesired/malicious changes, while communications between recursive resolvers and authoritative NS often incorporate additional protection such as DNSSEC.
- **How to protect/secure clients to resolvers communication???**

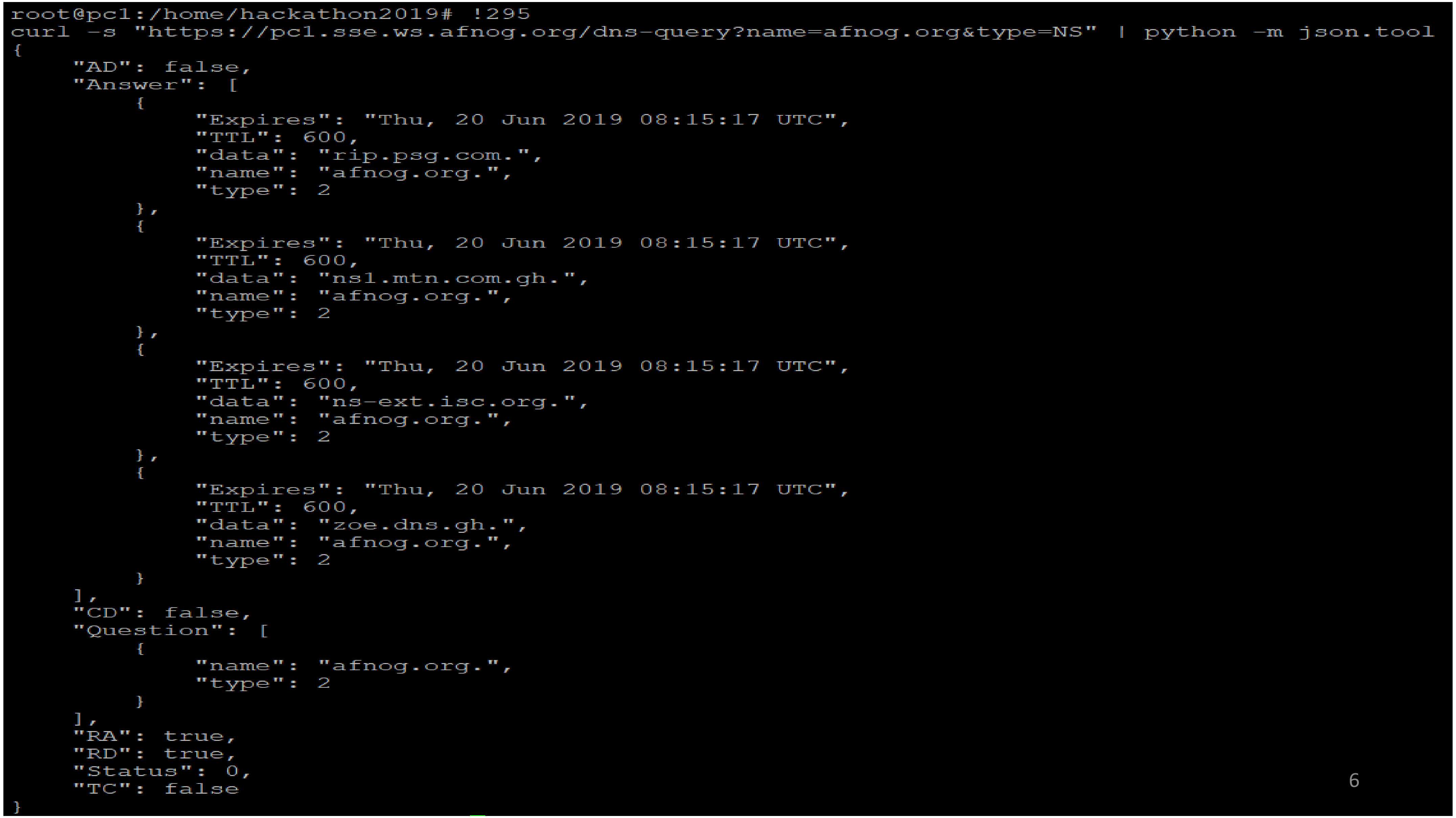
Motivation

- Run your own DoH and/or DoT server
- Increase user privacy and security by preventing eavesdropping and manipulation of DNS data.

REQUIREMENTS

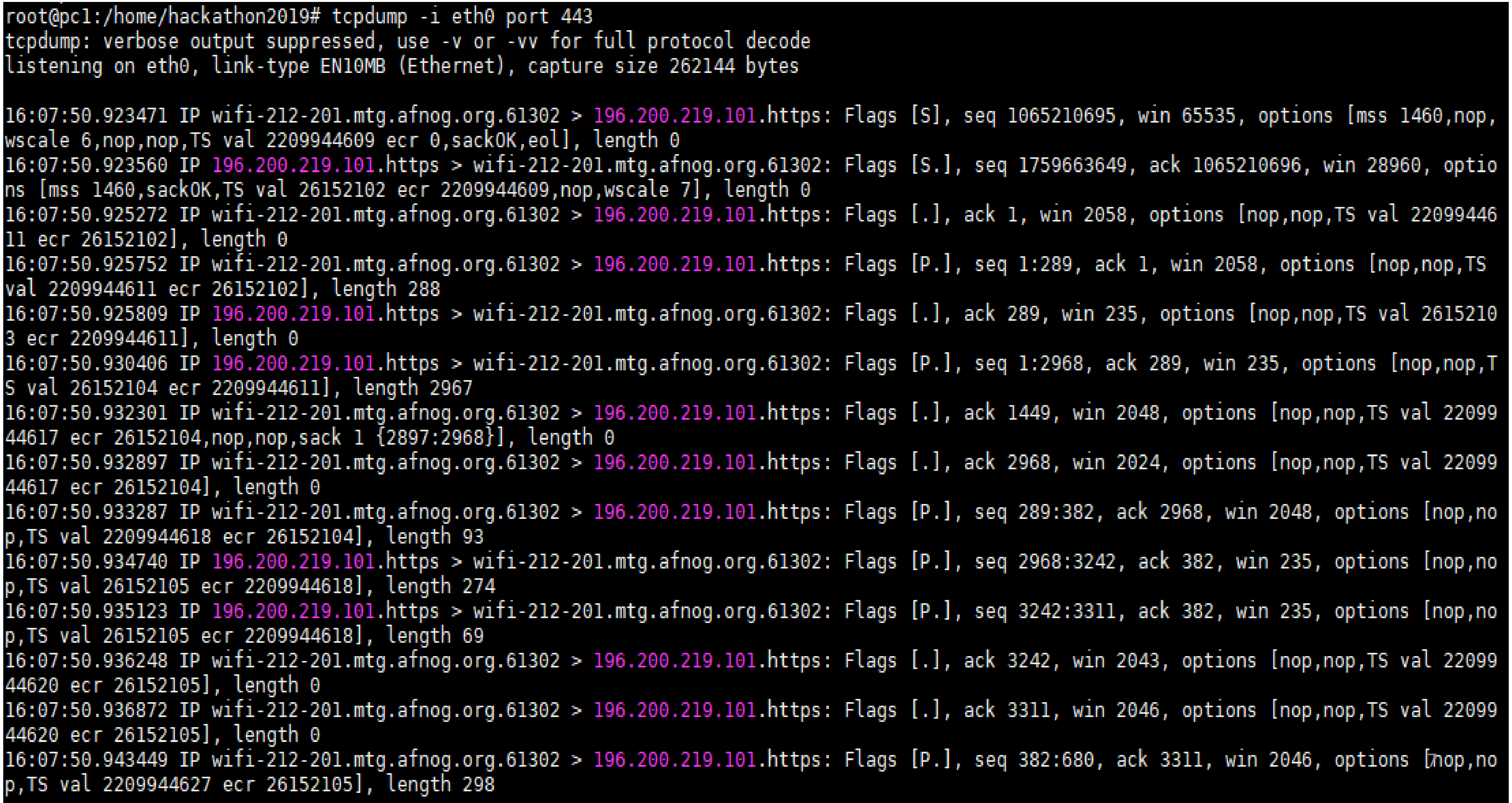
- HTTP Server: Nginx for example
- Certbot/Let’s Encrypt to generate SSL certificates and integrate to the HTTP server.
- A resolver: Unbound is simple and perfect!
- Firewall rules for security: iptables/firewalld
- a browser: Firefox is fine!
- Wireshark or tcpdump to analyse the traffic
- Be patient and open your eyes!

Test your DoH server locally



```
root@pc1:/home/hackathon2019# !295
curl -s "https://pc1.sse.ws.afnog.org/dns-query?name=afnog.org&type=NS" | python -m json.tool
{
    "AD": false,
    "Answer": [
        {
            "Expires": "Thu, 20 Jun 2019 08:15:17 UTC",
            "TTL": 600,
            "data": "rip.psg.com.",
            "name": "afnog.org.",
            "type": 2
        },
        {
            "Expires": "Thu, 20 Jun 2019 08:15:17 UTC",
            "TTL": 600,
            "data": "ns1.mtn.com.gh.",
            "name": "afnog.org.",
            "type": 2
        },
        {
            "Expires": "Thu, 20 Jun 2019 08:15:17 UTC",
            "TTL": 600,
            "data": "ns-ext.isc.org.",
            "name": "afnog.org.",
            "type": 2
        },
        {
            "Expires": "Thu, 20 Jun 2019 08:15:17 UTC",
            "TTL": 600,
            "data": "zoe.dns.gh.",
            "name": "afnog.org.",
            "type": 2
        }
    ],
    "CD": false,
    "Question": [
        {
            "name": "afnog.org.",
            "type": 2
        }
    ],
    "RA": true,
    "RD": true,
    "Status": 0,
    "TC": false
}
```

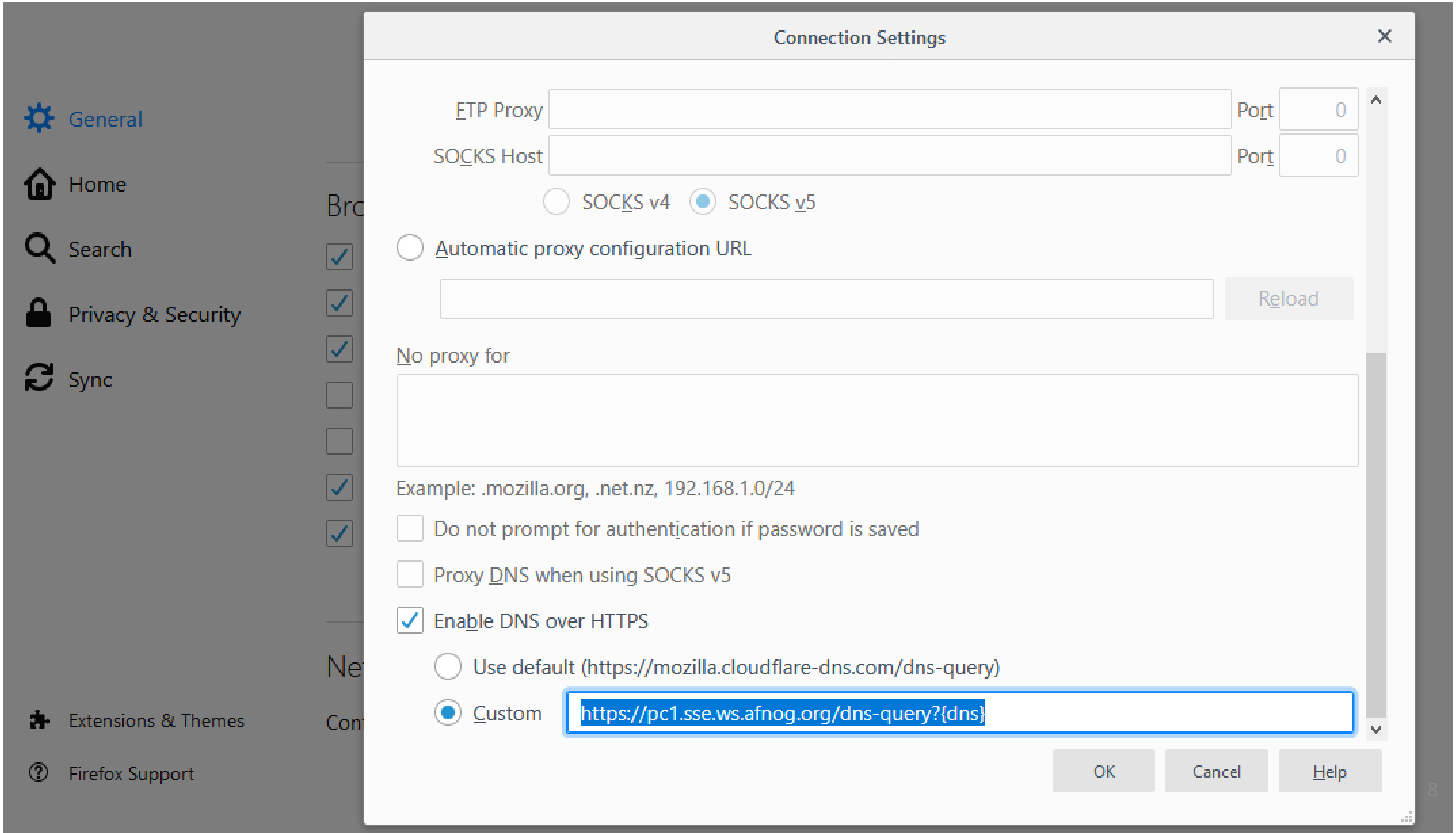
Tcpdump on SSL port



```
root@pc1:/home/hackathon2019# tcpdump -i eth0 port 443
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes

16:07:50.923471 IP wifi-212-201.mtg.afnog.org.61302 > 196.200.219.101.https: Flags [S], seq 1065210695, win 65535, options [mss 1460,nop,
wscale 6,nop,nop,TS val 2209944609 ecr 0,sackOK,eol], length 0
16:07:50.923560 IP 196.200.219.101.https > wifi-212-201.mtg.afnog.org.61302: Flags [S.], seq 1759663649, ack 1065210696, win 28960, optio
ns [mss 1460,sackOK,TS val 26152102 ecr 2209944609,nop,wscale 7], length 0
16:07:50.925272 IP wifi-212-201.mtg.afnog.org.61302 > 196.200.219.101.https: Flags [.], ack 1, win 2058, options [nop,nop,TS val 22099446
11 ecr 26152102], length 0
16:07:50.925752 IP wifi-212-201.mtg.afnog.org.61302 > 196.200.219.101.https: Flags [P.], seq 1:289, ack 1, win 2058, options [nop,nop,TS
val 2209944611 ecr 26152102], length 288
16:07:50.925809 IP 196.200.219.101.https > wifi-212-201.mtg.afnog.org.61302: Flags [.], ack 289, win 235, options [nop,nop,TS val 2615210
3 ecr 2209944611], length 0
16:07:50.930406 IP 196.200.219.101.https > wifi-212-201.mtg.afnog.org.61302: Flags [P.], seq 1:2968, ack 289, win 235, options [nop,nop,T
S val 26152104 ecr 2209944611], length 2967
16:07:50.932301 IP wifi-212-201.mtg.afnog.org.61302 > 196.200.219.101.https: Flags [.], ack 1449, win 2048, options [nop,nop,TS val 22099
44617 ecr 26152104,nop,nop,sack 1 {2897:2968}], length 0
16:07:50.932897 IP wifi-212-201.mtg.afnog.org.61302 > 196.200.219.101.https: Flags [.], ack 2968, win 2024, options [nop,nop,TS val 22099
44617 ecr 26152104], length 0
16:07:50.933287 IP wifi-212-201.mtg.afnog.org.61302 > 196.200.219.101.https: Flags [P.], seq 289:382, ack 2968, win 2048, options [nop,no
p,TS val 2209944618 ecr 26152104], length 93
16:07:50.934740 IP 196.200.219.101.https > wifi-212-201.mtg.afnog.org.61302: Flags [P.], seq 2968:3242, ack 382, win 235, options [nop,no
p,TS val 26152105 ecr 2209944618], length 274
16:07:50.935123 IP 196.200.219.101.https > wifi-212-201.mtg.afnog.org.61302: Flags [P.], seq 3242:3311, ack 382, win 235, options [nop,no
p,TS val 26152105 ecr 2209944618], length 69
16:07:50.936248 IP wifi-212-201.mtg.afnog.org.61302 > 196.200.219.101.https: Flags [.], ack 3242, win 2043, options [nop,nop,TS val 22099
44620 ecr 26152105], length 0
16:07:50.936872 IP wifi-212-201.mtg.afnog.org.61302 > 196.200.219.101.https: Flags [.], ack 3311, win 2046, options [nop,nop,TS val 22099
44620 ecr 26152105], length 0
16:07:50.943449 IP wifi-212-201.mtg.afnog.org.61302 > 196.200.219.101.https: Flags [P.], seq 382:680, ack 3311, win 2046, options [nop,no
p,TS val 2209944627 ecr 26152105], length 298
```

Use your DoH using your client browser



Connection Settings

FTP Proxy Port 0

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

□ Do not prompt for authentication if password is saved

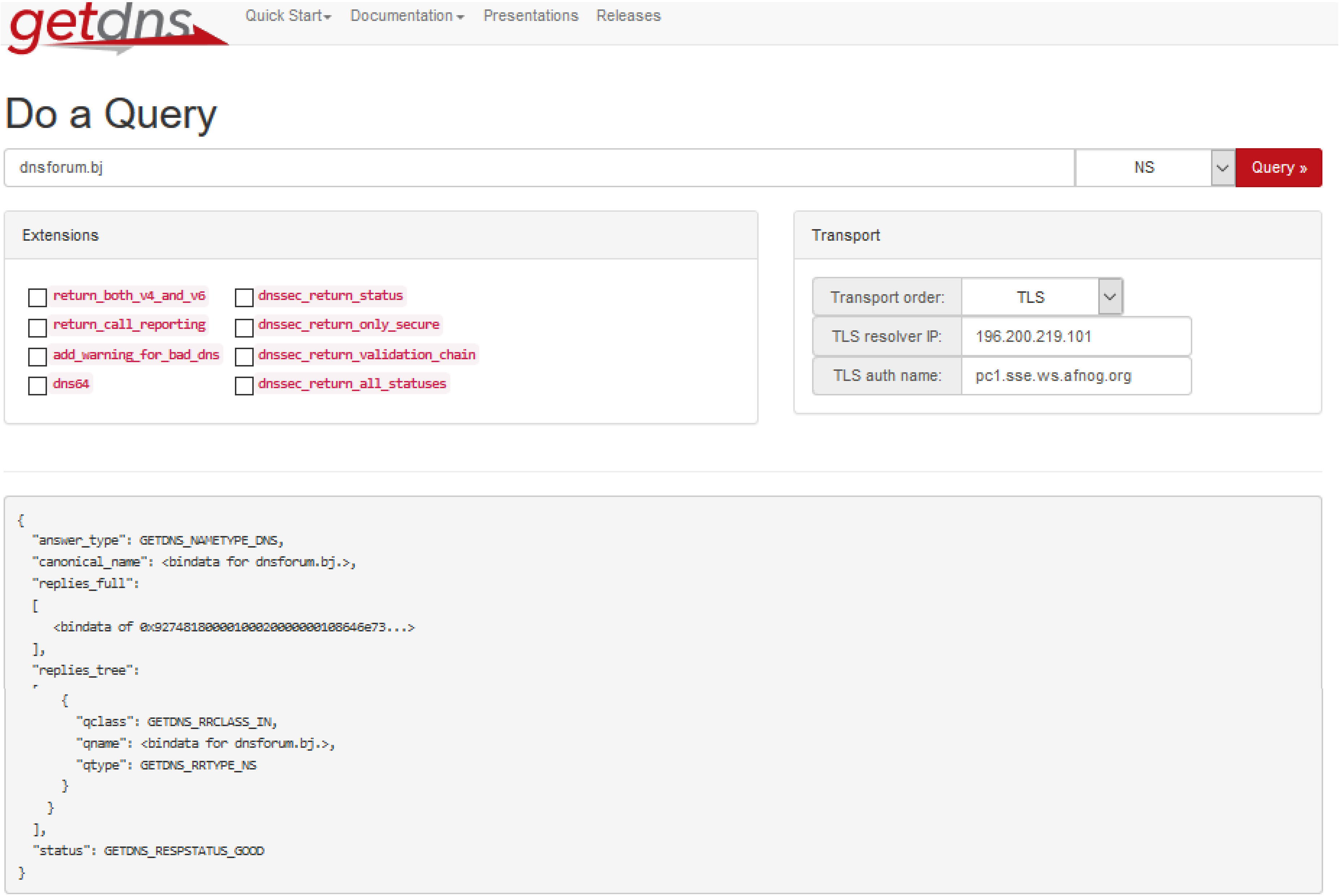
□ Proxy DNS when using SOCKS v5

☑ Enable DNS over HTTPS

○ Use default (https://mozilla.cloudflare-dns.com/dns-query)

● Custom https://pc1.sse.ws.afnog.org/dns-query?{dns}

Test your DoT server using getdnsapi
Answer should be "status": GETDNS_RESPSTATUS_GOOD



Do a Query

dnsforum.bj

NS

Extensions

□ return_both_v4_and_v6
□ return_call_reporting
□ add_warning_for_bad_dns
□ dns64
□ dnssec_return_status
□ dnssec_return_only_secure
□ dnssec_return_validation_chain
□ dnssec_return_all_statuses

Transport

Transport order:	TLS
TLS resolver IP:	196.200.219.101
TLS auth name:	pc1.sse.ws.afnog.org

```
{
  "answer_type": GETDNS_NAMETYPE_DNS,
  "canonical_name": <bindata for dnsforum.bj.>,
  "replies_full":
  [
     <bindata of 0x92748180000100020000000108646e73...>
  ],
  "replies_tree":
  [
      {
        "qclass": GETDNS_RRCLASS_IN,
        "qname": <bindata for dnsforum.bj.>,
        "qtype": GETDNS_RRTYPE_NS
      }
    }
  ],
  "status": GETDNS_RESPSTATUS_GOOD
}
```

Future improvements

- Implement a Windows client like Stubby so that the entire client OS DNS requests will be secured, not only the browser requests.
- Test on Android clients.
- …

Documentation

- Tutorial 1 to setup DoH: https://www.bentasker.co.uk/documentation/linux/407-building-and-running-your-own-dns-over-https-server
- Tutorial 2 to setup DoH: https://www.aaflalo.me/2018/10/tutorial-setup-dns-over-https-server/
- Tutorial to setup DoT: https://www.aaflalo.me/2019/03/dns-over-tls/
- Test DNS over TLS: https://getdnsapi.net/query/

Typos in documentation

- In Tutorial 1 to setup DoH, installing Nginx, /etc/nginx/conf.d/doh.conf: “listen 80;” instead of “listen 80”

- In DoT configuration, /etc/nginx/nginx.conf :

  Append “include /etc/nginx/streams/*;” instead of

  ```
  stream {
          include /etc/nginx/streams/*;
  }
  ```