

# DNSProxy

Local DNS-over-HTTP private resolver

Massimiliano Fantuzzi

# WHO

IBM, CERN

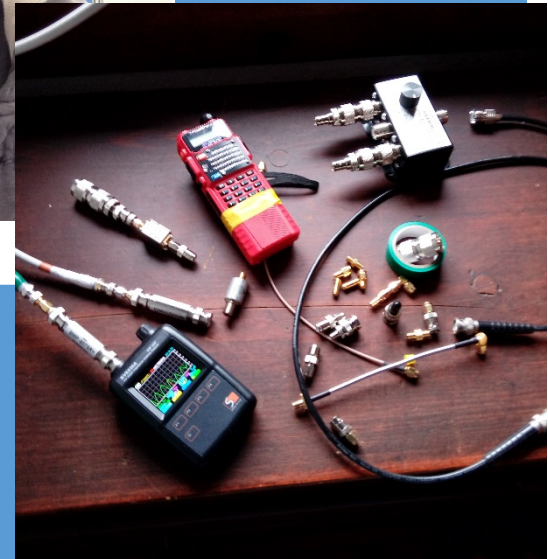
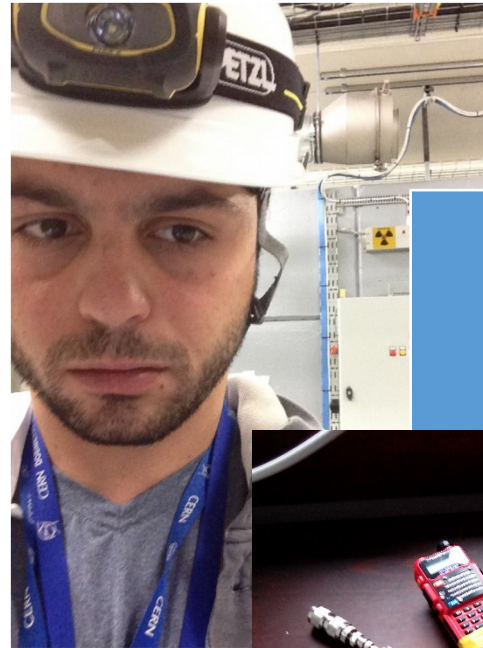
Landline mobile and sat Telcos

Hosting on ARM since 2005

Radioamateur

Interested in HTTP since

Have seen DNS mistreated /  
misunderstood



# WHY

## Wished to:

- TOR like a boss (hushmail, 2011)
- Reliable transport on high delay networks (2013-2015)
- Using polipo proxy (IRIF). Pipelining, HTTP version 1.

## Must be:

- Reliable. A, MX...
- Idempotent/idiosyncratic (not the case with ISP/caches)
- Sometimes, no auth/add needed (compression, chances of no-change, Skype 5sec..)

## BIND is amazing, Coredns.io too

- DNSP: no zone files (yet), 1 contributor
- Poor's man total-system wrapper, slow (from <1msec to more than 400msec)
- K8S, Docker, GCP ?

## Adhere to doh-draft (2018)

# HOW

Many options, I choosen C+PHP but Golang is sexy.

Works on a single workstation, little LAN, small sat ISP.

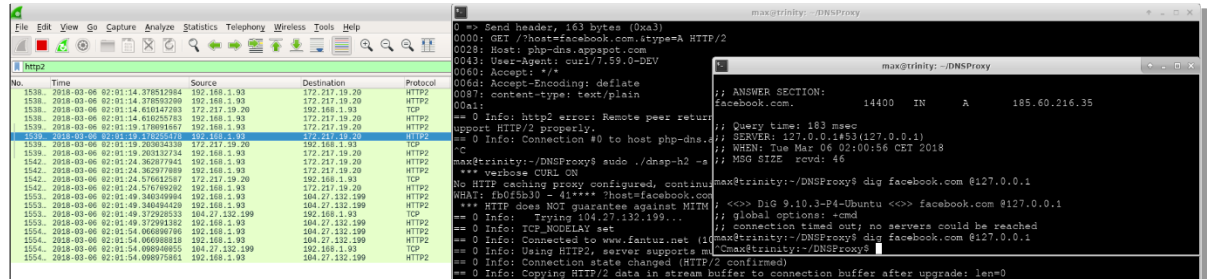
Forging packets is fun, spawning threads too. Learning.

In a sense, back to /etc/hosts (or CURL\_RESOLVE)

Added H2 with a simple update of CURL. Bye bye polipo.

Would test with GHTTP2 but my boost is worse than my C.

# HOW



```
max@trinity:~/DNSProxy$ sudo ./dnsp-h2 -s https://www.fantuz.net/nslookup-doh.php -T 86400
```

```
*** TTL SET TO 86400
```

```
No HTTP caching proxy configured, continuing
```

```
WHAT: 8fc6b60 - 39
```

```
HTTP/2 200
```

```
x-powered-by: PHP/7.1.12
```

```
x-powered-by: PleskLin
```

```
content-type: text/plain;charset=UTF-8
```

```
last-modified: Thu, 15 Mar 2018 16:56:48 GMT
```

```
etag: c99cc4d4646f4e9ee2b3e87f21cbc8df
```

```
cache-control: public, max-age=127, s-maxage=127
```

```
content-length: 35
```

```
content-encoding: gzip
```

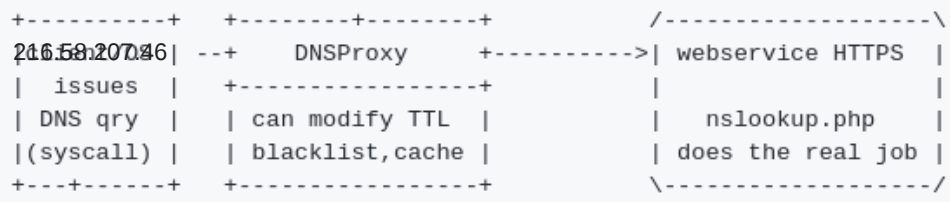
```
vary: Accept-Encoding
```

```
date: Thu, 15 Mar 2018 16:56:48 GMT
```

```
accept-ranges: bytes
```

```
server: LiteSpeed
```

```
alt-svc: quic=":443"; ma=2592000; v="35,37,38,39"
```



```
: ^
| UDP query goes to DNSP daemon on 127.0.0.1:53 |
+-----+
```

and is being transported on HTTP, with  
no use of DNS or UDP whatsoever

TP(S)  
which  
P/DNS  
dance  
1.

# INSPIRATION

- Torsocks
- pdns / Power DNS
- http\_dns\_proxy
- google\_https\_dns
- Unbound
- PCAP\_Dnsproxy

## Reports from users:

- dnspod et Ali <https://www.v2ex.com/t/250611>
- Netflix bypass
- Webex prep call Hackathon 101
- Arduino version

# HOW REALLY

HTTP headers

PHP `dns_get_record`

libcurl

Does:

- «comply»
- memcache
- expire
- cluster

Solves .. problems

- Poisoning ?
- Censorship ?
- Redundancy

Offers .. solutions

- democratisation
- CDN-friendly, Etag
- Anti DDOS
- Proxify HTTP(S) (i.e. charles)

# GOALS

- GET --> POST
- Load balancing (or multipath). How verbose is verbose ?
- Authority, Additional back in at no cost
- DNSSEC
- Keep supporting googleDNS / D-o-H / Max's D-o-H / others
- redis WIP, arduino radio blockchain, fun



# FUTURE EVOLUTIONS (!)

- HTTP/2 on
  - 8.8.8.8
  - 9.9.9.9, 9.9.9.10
  - 16.16.16.16 ?
- DNS ≠ DN\$ (Tuvalu island --> .tv)
- ....

Something else to add to draft proposals ?

Being verbal adds no trust over domaine naming (service, discovery) ?

Create more official test bed (see Yeti) !?

