DNSProxy

Local DNS-over-HTTP private resolver

Massimilano Fantuzzi

WHO

IBM, CERN

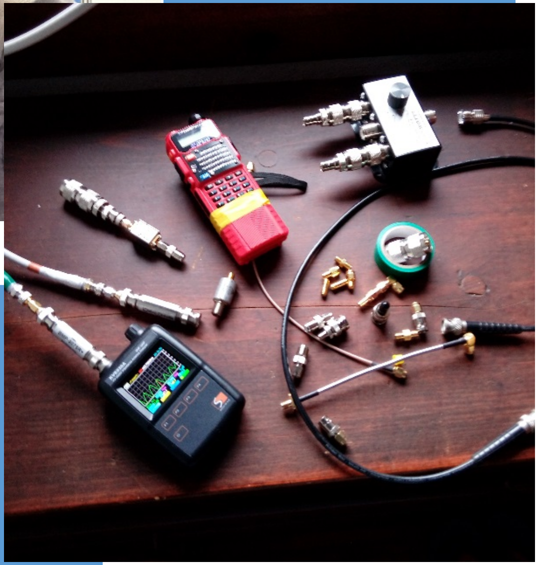
Landline mobile and sat Telcos

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.

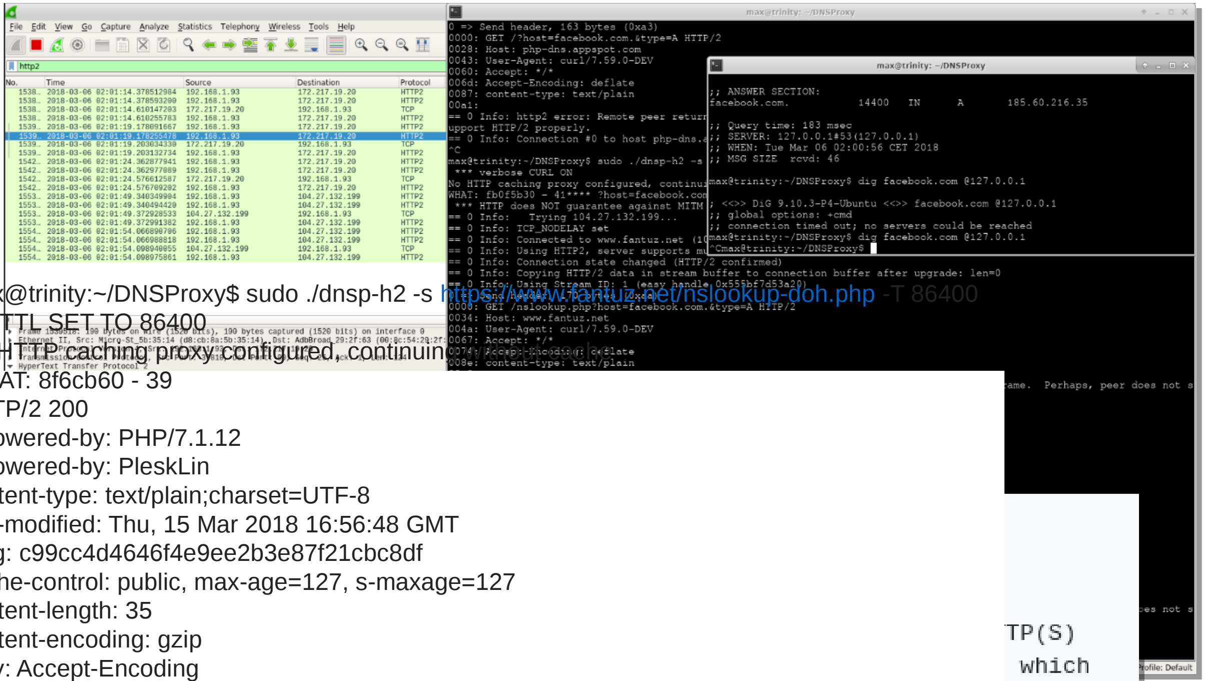
Forging packets is fun, spawning threads too. Learning.

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



```
No.      Time                           Source           Destination      Protocol
 1538…   2018-03-06 02:01:14.378512984  192.168.1.93     172.217.19.20    HTTP2
 1538…   2018-03-06 02:01:14.378593200  192.168.1.93     172.217.19.20    HTTP2
 1538…   2018-03-06 02:01:14.610147203  172.217.19.20    192.168.1.93     TCP
 1538…   2018-03-06 02:01:14.610255783  192.168.1.93     172.217.19.20    HTTP2
 1539…   2018-03-06 02:01:19.178091667  192.168.1.93     172.217.19.20    HTTP2
 1539…   2018-03-06 02:01:19.178255478  192.168.1.93     172.217.19.20    HTTP2
 1539…   2018-03-06 02:01:19.203034330  172.217.19.20    192.168.1.93     TCP
 1539…   2018-03-06 02:01:19.203132734  192.168.1.93     172.217.19.20    HTTP2
 1542…   2018-03-06 02:01:24.362877941  192.168.1.93     172.217.19.20    HTTP2
 1542…   2018-03-06 02:01:24.362977089  192.168.1.93     172.217.19.20    HTTP2
 1542…   2018-03-06 02:01:24.576612587  172.217.19.20    192.168.1.93     TCP
 1542…   2018-03-06 02:01:24.576709202  192.168.1.93     172.217.19.20    HTTP2
 1553…   2018-03-06 02:01:49.340349904  192.168.1.93     104.27.132.199   HTTP2
 1553…   2018-03-06 02:01:49.340494420  192.168.1.93     104.27.132.199   HTTP2
 1553…   2018-03-06 02:01:49.372928533  104.27.132.199   192.168.1.93     TCP
 1553…   2018-03-06 02:01:49.372991382  192.168.1.93     104.27.132.199   HTTP2
 1554…   2018-03-06 02:01:54.066890706  192.168.1.93     104.27.132.199   HTTP2
 1554…   2018-03-06 02:01:54.066988818  192.168.1.93     104.27.132.199   HTTP2
 1554…   2018-03-06 02:01:54.098940055  104.27.132.199   192.168.1.93     TCP
 1554…   2018-03-06 02:01:54.098975861  192.168.1.93     104.27.132.199   HTTP2

▸ Frame 1539518: 190 bytes on wire (1520 bits), 190 bytes captured (1520 bits) on interface 0
▸ Ethernet II, Src: Micro-St_5b:35:14 (d8:cb:8a:5b:35:14), Dst: AdbBroad_29:2f:63 (00:8c:54:29:2f:
▸ Internet Protocol Version 4, Src: 192.168.1.93, Dst: 172.217.19.20
▸ Transmission Control Protocol, Src Port: 3?810, Dst Port: 443, Seq: 2?, Ack: 1, Len: 124
▾ HyperText Transfer Protocol 2
```

```
0 => Send header, 163 bytes (0xa3)
0000: GET /?host=facebook.com.&type=A HTTP/2
0028: Host: php-dns.appspot.com
0043: User-Agent: curl/7.59.0-DEV
0060: Accept: */*
006d: Accept-Encoding: deflate
0087: content-type: text/plain
00a1:
== 0 Info: http2 error: Remote peer returr
upport HTTP/2 properly.
== 0 Info: Connection #0 to host php-dns.a
^C
max@trinity:~/DNSProxy$ sudo ./dnsp-h2 -s
 *** verbose CURL ON
No HTTP caching proxy configured, continui
WHAT: fb0f5b30 - 41**** ?host=facebook.com
 *** HTTP does NOT guarantee against MITM
== 0 Info:   Trying 104.27.132.199...
== 0 Info: TCP_NODELAY set
== 0 Info: Connected to www.fantuz.net (10
== 0 Info: Using HTTP2, server supports mu
== 0 Info: Connection state changed (HTTP/2 confirmed)
== 0 Info: Copying HTTP/2 data in stream buffer to connection buffer after upgrade: len=0
== 0 Info: Using Stream ID: 1 (easy handle 0x555bf7d53a20)
0 => Send header, 170 bytes (0xaa)
0000: GET /nslookup.php?host=facebook.com.&type=A HTTP/2
0034: Host: www.fantuz.net
004a: User-Agent: curl/7.59.0-DEV
0067: Accept: */*
0074: Accept-Encoding: deflate
008e: content-type: text/plain
ame.  Perhaps, peer does not s
es not s
```

```
;; ANSWER SECTION:
facebook.com.           14400   IN      A       185.60.216.35

;; Query time: 183 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Mar 06 02:00:56 CET 2018
;; MSG SIZE  rcvd: 46

max@trinity:~/DNSProxy$ dig facebook.com @127.0.0.1

; <<>> DiG 9.10.3-P4-Ubuntu <<>> facebook.com @127.0.0.1
;; global options: +cmd
;; connection timed out; no servers could be reached
max@trinity:~/DNSProxy$ dig facebook.com @127.0.0.1
^Cmax@trinity:~/DNSProxy$
```

```
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 without cache
WHAT: 8f6cb60 - 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"
216.58.207.46
```

```
TP(S)
 which
P/DNS
dance
l.
```

```
  v                    |                           :
+----------+   +--------+--------+          /------------------\
|          | --+    DNSProxy     +---------->| webservice HTTPS |
|  issues  |   +-----------------+          |                  |
| DNS qry  |   | can modify TTL  |          |   nslookup.php   |
|(syscall) |   | blacklist,cache |          | does the real job|
+---+------+   +-----------------+          \------------------/
    :                                                  ^
    |  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
```

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) !?

?