DNS

NETMET Lab Exercises 11 -- **GRADED**

Introduction

DNS protocol is one of the most fundamental protocols on the Internet and it's used to get information about domain translations.
But in terms of geolocation, it can be used to find information about a host of a router location, mainly thanks to reverse domains. Unfortunately, these location hints are not standardized at all, and so it's not guaranteed that it exists or it could be inferred easily.

Grading information

You must give a report following the structure of this lab and answering the questions.
This is individual work.
Any piece of code must be either pasted on the report or transmitted via a Github Gist (https://gist.github.com/) link.

Prelude

- Cite three different types of programs that use DNS.
- Explain the principles of DNS. What is the difference between a *local server* and an *authoritative server* ?
- Explain the role of these different DNS types : A, AAAA, CNAME NS, MX, PTR

First step with nslookup

Nslookup is a tool to perform DNS requests. It's very handy to troubleshoot DNS problems in an infrastructure. Other tools have the same purpose such as *dig* (you can use it instead of *nslookup* during this lab if you prefer).

- Get the ip address of the web server associated with the domain name github.com.
- Get all the name servers of the domain github.com.
- Get the IP address of the web server associated with domain github.com from one of the authoritative servers of that domain. Make this command multiple times, what do you notice ?
- Make a reverse lookup from the precedent output.
- Get all the mail servers ip addresses associated with the domain github.com.

Deep dive in without Wireshark

- Decode this frame (by hand)

```
0000   00 11 32 65 fb 1f a4 83 e7 4a 77 be 08 00 45 00     ..2e.....Jw...E.
0010   00 38 88 e2 00 00 40 11 6e 63 c0 a8 01 1d c0 a8   .8....@.nc......
0020   01 02 fd 2d 00 35 00 24 02 df 70 2d 01 00 00 01     ...-.5.$..p-....
0030   00 00 00 00 00 00 06 67 69 74 68 75 62 03 63 6f     .......github.co
0040   6d 00 00 01 00 01                                   m.....
```

What type of information is in the application layer exactly ?

- Decode this frame (by hand)

```
0000   a4 83 e7 4a 77 be 00 11 32 65 fb 1f 08 00 45 00      ...Jw...2e....E.
0010   00 48 0f 85 00 00 40 11 e7 b0 c0 a8 01 02 c0 a8     .H....@.........
0020   01 1d 00 35 fd 2d 00 34 bf b7 70 2d 81 80 00 01     ...5.-.4..p-....
0030   00 01 00 00 00 00 06 67 69 74 68 75 62 03 63 6f     .......github.co
0040   6d 00 00 01 00 01 c0 0c 00 01 00 01 00 00 00 1d   m...............
0050   00 04 8c 52 76 03                                   ...Rv........'
```

What type of information is in the application layer exactly ?

Deep dive in with Wireshark (from nslookup)

- Make a simple DNS request with nslookup and check the frames from wireshark. What is the destination port for the DNS query message ? What is the source port of the DNS response message ?
- Make a request to get the name servers. What changed in the request ? What changed in the answer ?
- Make a request towards a name server. What changed in the request ? What changed in the answer ?
- Make a request to get a mail server ip address. What changed in the request ? What changed in the answer ?
- Make a reverse lookup. What changed in the request ? What changed in the answer ?

Geolocation

When doing the previous exercises, you may have noticed some geolocation hints in the DNS names, especially in reverse DNS records.

Here are some IP addresses. Get the reverse DNS names with nslookup and try to find manually the geolocation hints :

```
146.97.128.18
4.69.142.245
193.51.181.93
212.162.31.82
194.149.163.214
212.74.72.189
86.43.244.45
193.191.3.250
```

Then, imagine a programming procedure to infer the most possible hints based on what you saw in these examples. This procedure must be general enough to work on other IP addresses not cited here.