

## TP5:

### Exercise 1:

Execute: "dig A google.com"

- List what the different informations are:

```
root@ubuntu:~# dig A google.com

; <>> DiG 9.11.3-1ubuntu1.13-Ubuntu <>> A google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4520
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 65494
;; QUESTION SECTION:
;google.com.                IN      A

;; ANSWER SECTION:
google.com.                110     IN      A      172.217.22.142

;; Query time: 7 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Thu Jan 14 08:47:22 CET 2021
;; MSG SIZE  rcvd: 55
```

Les différentes informations que nous fournit cette commande sont :

- La version de Ubuntu
- Le flag , avec la question et la réponse
- La version de l' "Extension Domain Name System" et le protocole utilisateur
- La question
- La réponse avec le nombre de requêtes possibles sur l'adresse ip
- Le temps de réponse
- Le server
- La date
- La taille du message

What is the IP the resolver sent you :

L'adresse ip est 172.217.22.142

Is the IP address received the same for all your group members ? Can it be different ? Is this a normal behaviour ?

Ce n'est pas la même pour tout le groupe , il change en fonction de la zone géographique et d'un temps particulier. Oui c'est normal .

What happens if you go to the IP received on your browser ?

Les serveurs de Google répondent aux messages HTTP, on est donc redirigé vers la page d'accueil de Google.

What is the SERVER line at the bottom ? Is it the same for all your group members ?

C'est est l'adresse IP du résolveur DNS que j'utilise , elle est différente pour certains du groupe.

Execute "whois google.com", "whois 8.8.8.8", "whois 1.1.1.1", "whois inteltechniques.com", ... What similarities and differences can you spot ?

What does "dig AAAA google.com" do ?

Comme nous avons fait une requête AAAA, la réponse contient des adresses IPv6, au lieu d'adresses IPv4

What does "dig NS google.com" do ?

4 serveurs sont identifiés par leur nom, ns1.google.com, ns2.google.com, ns3.google.com et ns4.google.com.

What are the servers listed here ?

Ce sont les serveurs de noms faisant autorité de Google

How can you use dig to get the IP addresses of these servers ?

La commande suivante fonctionnera: dig A ns1.google.com. Le nom de domaine du serveur de noms n'est encore qu'un nom de domaine, nous pouvons donc l'interroger comme nous le ferions avec n'importe quel autre nom de domaine.

## Exercice 2:

Using the last command from the last exercise, get the IP address of the server ns1.google.com ; Use this IP to execute "dig @IP ns1.google.com" is the output the same ? Why ?

Cette commande renvoie l'adresse IP de l'un des serveurs de noms faisant autorité de Google.

Cela donne la même adresse ip.

Cela signifie que le serveur de noms faisant autorité de Google que l'on a interrogé cette fois a la même adresse IP que le résolveur.

Research the DNS Hierarchy: "Root > TLD > Authoritative"

Les serveurs racine connaissent les serveurs TLD, les serveurs TLD connaissent les serveurs faisant autorité et les serveurs faisant autorité connaissent des sites Web et des services Web spécifiques.

Execute: “dig A a.root-servers.net” and “dig A b.root-servers.net”. What did you get ?

On obtient les adresses ip des serveurs root a et b

dig A a.root-servers.net : 198.41.0.4

dig A b.root-servers.net : 199.9.14.201

What are the specificities of these IP addresses ?

Les spécificités de ces adresses ip sont qu’elles ne changent jamais

Use “traceroute -l” to find which of those two IP is closer to you

```
ynov@ubuntu:~$ traceroute 198.41.0.4
traceroute to 198.41.0.4 (198.41.0.4), 30 hops max, 60 byte packets
 1 _gateway (192.168.1.254) 1.079 ms 1.979 ms 2.092 ms
 2 lso-5.isdnet.net (194.149.164.46) 16.332 ms 16.297 ms 16.251 ms
 3 amsix-6k-1.routers.proxad.net (80.249.208.251) 29.913 ms 29.920 ms 29.903 ms
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 ^C
ynov@ubuntu:~$ traceroute 199.9.14.201
traceroute to 199.9.14.201 (199.9.14.201), 30 hops max, 60 byte packets
 1 _gateway (192.168.1.254) 1.188 ms 1.159 ms 1.190 ms
 2 jn.socabim.isdnet.net (194.149.169.45) 15.654 ms 15.607 ms 15.544 ms
 3 londres-asr9k-1-te-0-0-6.intf.routers.proxad.net (194.149.163.225) 22.457 ms 22.411 ms 22.354 ms
 4 newyork-6k-1-p01.intf.routers.proxad.net (212.27.58.206) 88.398 ms * *
 5 paloalto-6k-1-p01.intf.routers.proxad.net (212.27.58.222) 158.070 ms * 278.694 ms
 6 calren-cenic.paix.net (198.32.176.33) 279.675 ms 160.312 ms 159.325 ms
 7 dc-svl-agg10--oak-agg8-300g.cenic.net (137.164.11.94) 160.103 ms 160.455 ms 160.966 ms
 8 dc-svl-agg8--svl-agg10-300g.cenic.net (137.164.11.81) 159.891 ms 159.821 ms 160.177 ms
 9 dc-lax-agg8--svl-agg8-100ge-1.cenic.net (137.164.11.0) 168.334 ms 168.301 ms dc-lax-agg8--svl-agg8--100ge--2.cenic.net (137.164.11.20) 166.910 ms
10 130.152.185.8 (130.152.185.8) 166.795 ms 166.725 ms 166.678 ms
11 130.152.184.99 (130.152.184.99) 169.871 ms 169.814 ms 178.193 ms
12 206.117.5.21 (206.117.5.21) 180.260 ms 180.195 ms 180.145 ms
13 * * *
14 * * * ^C
ynov@ubuntu:~$ _
```

L’adresse ip la plus proche est celle du serveur a.

Use the IP of one of the root nameserver to query one IP for google.com. What command should you use ? Is the result similar to what you have seen before ?

dig @198.41.0.4 A google.com

Non, le résultat n’est pas le même qu’avant

What purpose do the servers in the additional section serve ?

On obtient les adresses ipv6 et ipv4 des serveurs TLD.

Elles nous permettent de nous rapprocher d’une adresse dig A google.com

afin d’affiner la recherche on peut effectuer un dig @ip-server-tld A google.com

qui nous donnera les serveurs d'autorité de google.

Did we get the IP for google.com like we asked ? Why ?

Non parce que le serveur root que nous avons interrogé n'avait pas d'enregistrement A pour google.com.

What is the relation between the Authority Section and the Additional Section ? How can we get the information required to get an IP address for google.com ?

Elles nous permettent de nous rapprocher d'une adresse dig A google.com afin d'affiner la recherche on peut effectuer un dig @ip-server-authorité A google.com qui nous donnera les serveurs A de google.com

Do and explain the necessary steps to get an IP address for google.com

1. dig A a.root-servers.net = 198.41.0.4
2. dig @198.41.0.4 A google.com = a.gtld-servers.net --- 192.5.6.30
3. dig @192.5.6.30 A google.com = ns1.google.com --- 216.239.32.10
4. dig @216.239.32.10 A google.com = dig A google.com --- 172.217.22.142

## Exercice 3:

Capture traffic including DNS

UDP	54915	54915	54915 → 54915	Len=263
DNS	37785	53	Standard query 0x3f1f A www.google.com OPT	
DNS	54952	53	Standard query 0xe4b3 AAAA www.google.com OPT	
DNS	53	37785	Standard query response 0x3f1f A www.google.com A 216.58.204.100 OPT	
DNS	53	54952	Standard query response 0xe4b3 AAAA www.google.com AAAA 2a00:1450:4007:815::2004 OPT	
ICMP			Echo (ping) request id=0x0283, seq=1/256, ttl=64 (reply in 10)	
ICMP			Echo (ping) reply id=0x0283, seq=1/256, ttl=128 (request in 9)	
DNS	43742	53	Standard query 0xdbaf PTR 100.204.58.216.in-addr.arpa OPT	
DNS	53	43742	Standard query response 0xdbaf PTR 100.204.58.216.in-addr.arpa PTR par10s28-in-f4.1e100.	
UDP	54915	54915	54915 → 54915	Len=263
ICMP			Echo (ping) request id=0x0283, seq=2/512, ttl=64 (reply in 15)	
ICMP			Echo (ping) reply id=0x0283, seq=2/512, ttl=128 (request in 14)	
UDP	54915	54915	54915 → 54915	Len=263
ARP			Who has 192.168.1.254? Tell 192.168.32.1	
ICMP			Echo (ping) request id=0x0283, seq=3/768, ttl=64 (reply in 19)	
ICMP			Echo (ping) reply id=0x0283, seq=3/768, ttl=128 (request in 18)	
UDP	54915	54915	54915 → 54915	Len=263
ARP			Who has 192.168.1.254? Tell 192.168.32.1	
ICMP			Echo (ping) request id=0x0283, seq=4/1024, ttl=64 (reply in 23)	
ICMP			Echo (ping) reply id=0x0283, seq=4/1024, ttl=128 (request in 22)	
UDP	54915	54915	54915 → 54915	Len=263
ARP			Who has 192.168.1.254? Tell 192.168.32.1	
UDP	54915	54915	54915 → 54915	Len=263
ARP			Who has 192.168.1.254? Tell 192.168.32.1	
UDP	54915	54915	54915 → 54915	Len=263
ARP			Who has 192.168.1.254? Tell 192.168.32.1	
UDP	54915	54915	54915 → 54915	Len=263

Is a DNS request made each time you go on a website ? Why ?

Oui il y a une requête DNS à chaque fois , car il a chaque fois il y a un nom de domaine à résoudre.

How can you make it so ?

DNS	54020	53	Standard query 0xcf5e A www.pornub.com OPT
DNS	53249	53	Standard query 0x239b AAAA www.pornub.com OPT
DNS	53	54020	Standard query response 0xcf5e A www.pornub.com A 216.18.168.79 OPT
DNS	53	53249	Standard query response 0x239b AAAA www.pornub.com SOA dns1.p02.nsone.net OPT
ICMP			Echo (ping) request id=0x0287, seq=1/256, ttl=64 (reply in 10)
ICMP			Echo (ping) reply id=0x0287, seq=1/256, ttl=128 (request in 9)
DNS	54868	53	Standard query 0x992f PTR 79.168.18.216.in-addr.arpa OPT
DNS	53	54868	Standard query response 0x992f No such name PTR 79.168.18.216.in-addr.arpa SOA ns0.reflect
DNS	54868	53	Standard query 0x992f PTR 79.168.18.216.in-addr.arpa
DNS	53	54868	Standard query response 0x992f No such name PTR 79.168.18.216.in-addr.arpa SOA ns0.reflect
UDP	54915	54915	54915 → 54915 Len=263
ICMP			Echo (ping) request id=0x0287, seq=2/512, ttl=64 (reply in 17)
ICMP			Echo (ping) reply id=0x0287, seq=2/512, ttl=128 (request in 16)
NTP	52387	123	NTP Version 4, client
UDP	54915	54915	54915 → 54915 Len=263
ICMP			Echo (ping) request id=0x0287, seq=3/768, ttl=64 (reply in 21)
ICMP			Echo (ping) reply id=0x0287, seq=3/768, ttl=128 (request in 20)
UDP	54915	54915	54915 → 54915 Len=263
UDP	54915	54915	54915 → 54915 Len=263
DNS	41996	53	Standard query 0x641e A www.google.com OPT
DNS	50129	53	Standard query 0xc3b4 AAAA www.google.com OPT
DNS	53	41996	Standard query response 0x641e A www.google.com A 216.58.198.196 OPT
DNS	53	50129	Standard query response 0xc3b4 AAAA www.google.com AAAA 2a00:1450:4007:80c::2004 OPT
ICMP			Echo (ping) request id=0x0288, seq=1/256, ttl=64 (reply in 29)
ICMP			Echo (ping) reply id=0x0288, seq=1/256, ttl=128 (request in 28)
DNS	56333	53	Standard query 0x6207 PTR 196.198.58.216.in-addr.arpa OPT
DNS	53	56333	Standard query response 0x6207 PTR 196.198.58.216.in-addr.arpa PTR par10s27-in-f196.1e100
UDP	54915	54915	54915 → 54915 Len=263