TP5:

Exercice 1:

Execute: “dig A google.com”
• List what the different informations are:

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 ?

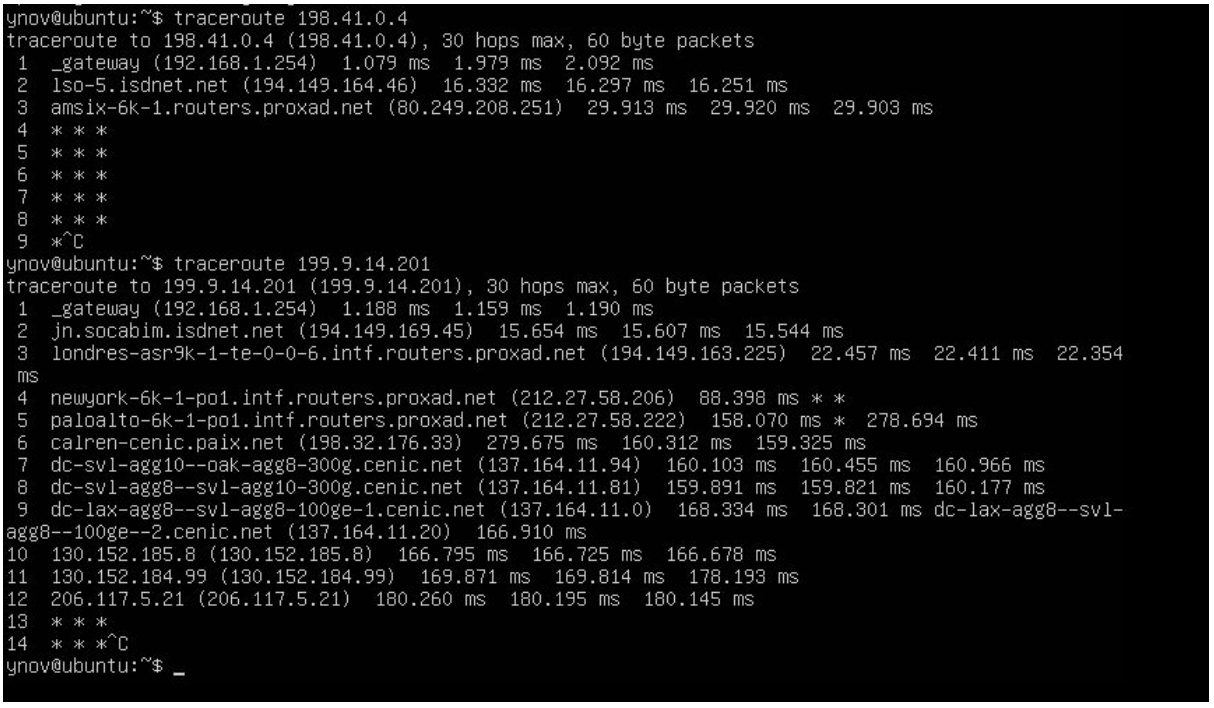
On obtient les adresses ip des serveurs root a et b

dig A a.root-servers.net : 198.41.0.4
dig A b.root-servers.net : 199.9.14.201

What are the specificites of these IP addresses ?

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

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



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
```