Exercice Pratiques de DNS

Ilyas Bambrik

Table des matières

DNS

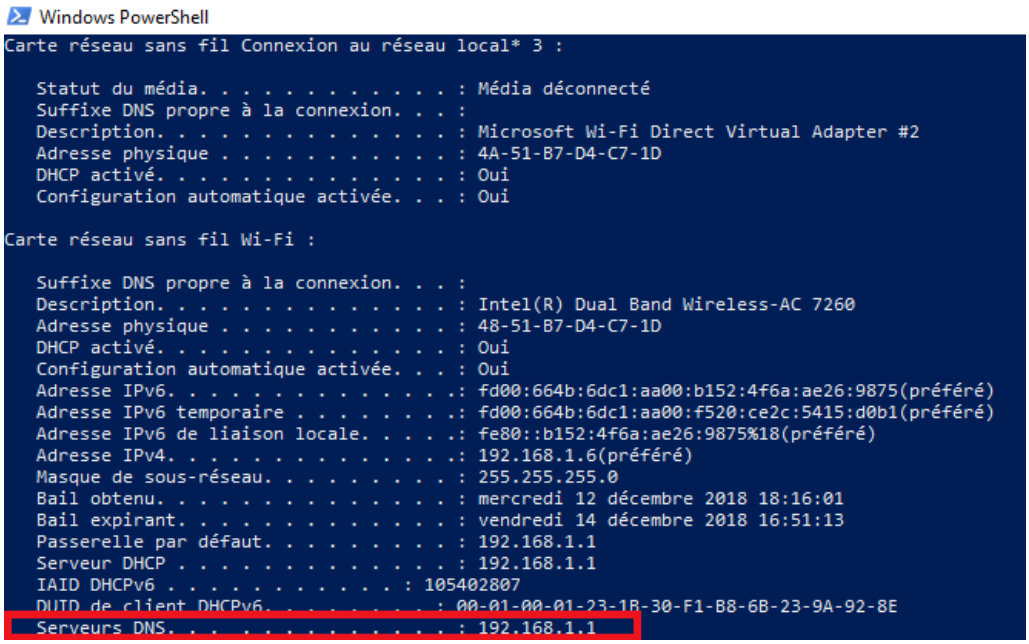
I

1. Travail demandé

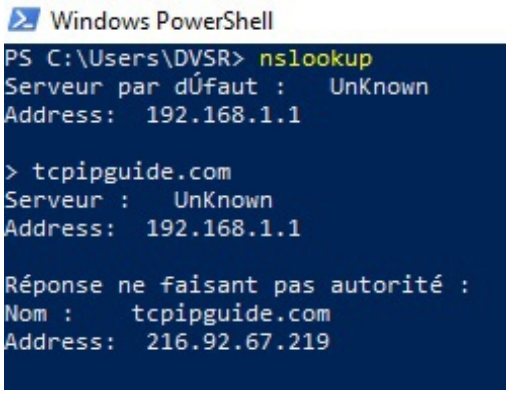
Pour chaque capture d'écran existante dans cette fiche TP, vous devez avoir la même capture afin de répondre aux questions lors de la consultation.

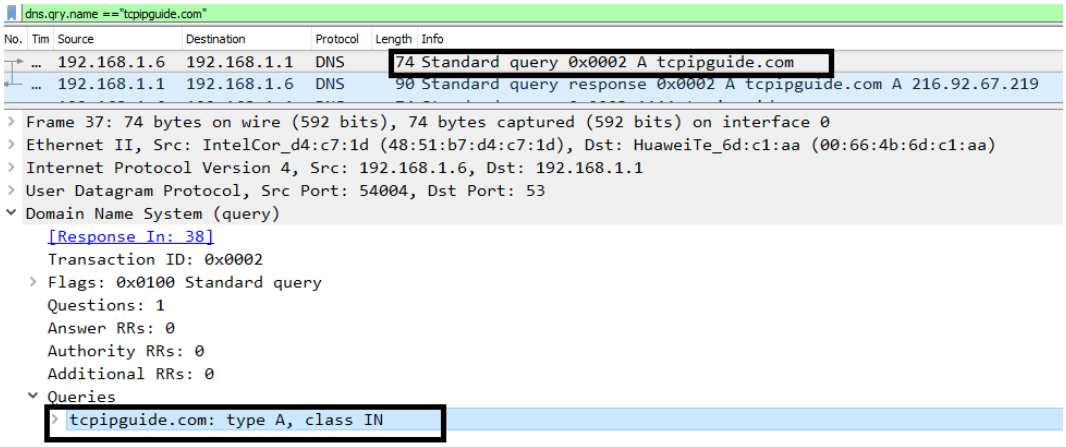
2. Exercice : Commandes DNS

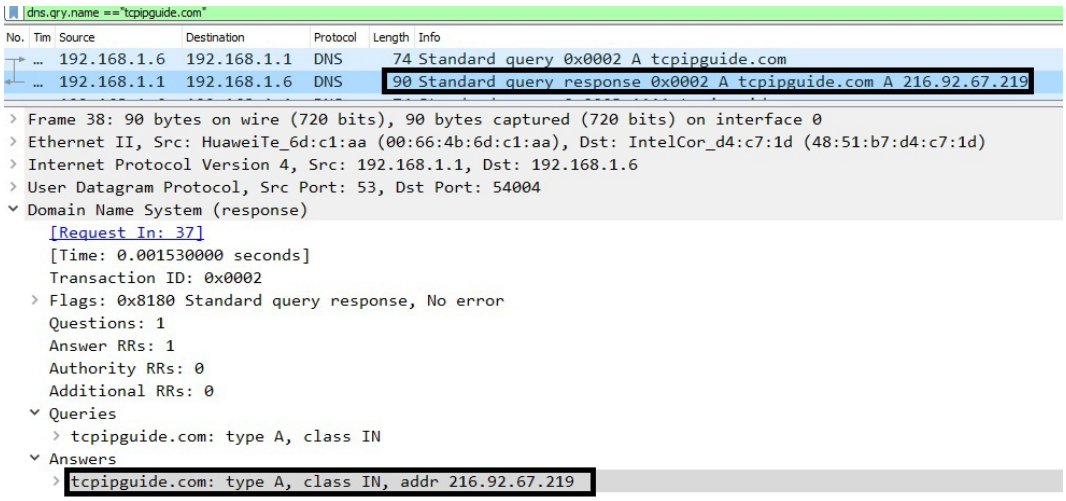
Ouvrez votre invité de commande et tapez *ipconfig /all* (ifconfig pour linux) et ensuite repérez votre configuration DNS pour l'interface avec la quelle vous êtes connecté sur Internet. Vous pouvez voir l'adresse IP de votre serveur DNS (voir la figure en bas)



- Tapez *nslookup* (outil de résolution de nom de domaine) et ouvrez *wireshark (ainsi que votre interface correspondante)* .
- Écrivez le nom de domaine suivant *tcpipguide.com* dans l'invité de commande nslookup ;
- Appliquez le filtre suivant dans Wireshark : *dns.qry.name =="tcpipguide.com"*
- L'envoie de la requête DNS retourne l'adresse IP du nom de domaine *"tcpipguide.com"*. La requête transmise par le Resolver (client nslookup) est une demande d'enregistrement A (*A == Adresse record*) [*voir la capture d'écran Wireshark*]. Ce type d'enregistrement fait la correspondance entre un nom de domaine et l'adresse IP correspondante (voir le cours).
- Par la suite la réponse correspondante à la requête est l'enregistrement de type A contenant l'adresse IP de *"tcpipguide.com"*.







- Pour récupérer l'adresse IPv6 d'un nom de domaine (si ce domaine possède une adresse IPv6 public), tapez dans l'invité de nslookup les commandes suivantes :

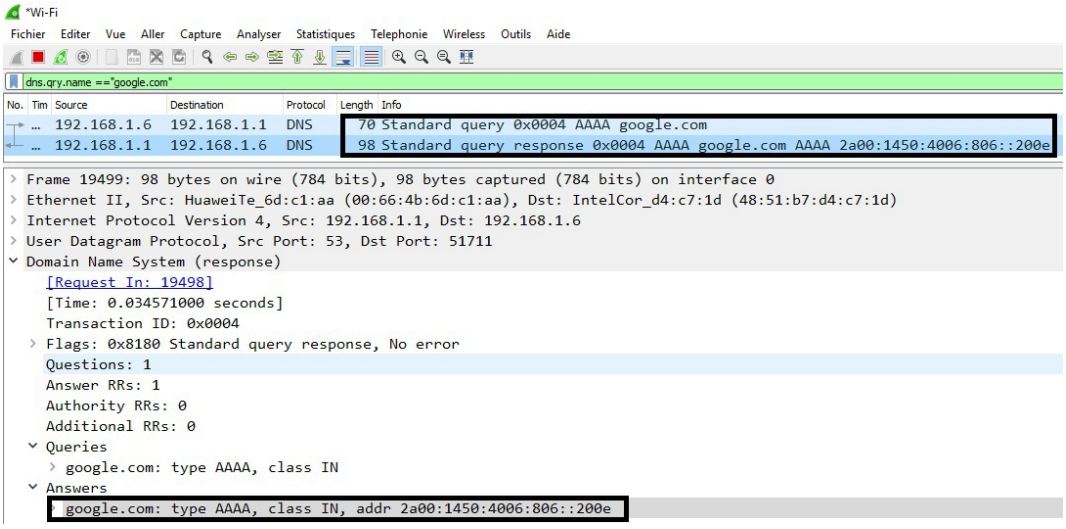
```
set type=AAAA
google.com
```

- Les deux commandes prétendantes permettent d'avoir l'adresse IPv6 public de google.com. *set type=AAAA* change le type d'enregistrement demandé par la requête DNS.

```
> set type=AAAA
> google.com
Serveur :   UnKnown
Address:  192.168.1.1

Réponse ne faisant pas autorité :
Nom :    google.com
Address:  2a00:1450:4006:806::200e

>
```



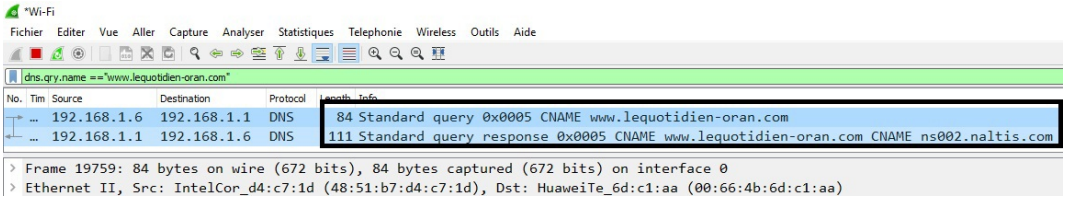
- Pour récupérer l'enregistrement CNAME (alias d'un nom de domaine) d'un nom de domaine (si ce domaine possède un alias), tapez dans l'invité de nslookup les commandes suivantes :

```
set type=CNAME
www.lequotidien-oran.com
```

- Les deux commandes prétendantes permettent d'avoir l'alias de *www.lequotidien-oran.com*. Dans cette exemple *www.lequotidien-oran.com* pointe sur *ns002.naltis.com* (voir la capture d'écran de).
- *ns002.naltis.com* possède l'adresse IP 91.121.146.205
- CNAME == *Canonical Name* ou bien nom canonique.
- Si vous procédez à exécuter un *ping* vers *www.lequotidien-oran.com* et *ns002.naltis.com*, vous remarquerais que les deux machines auront la même adresse IP (*voir le déroulement du ping, l'adresse IP des deux domaines est identique*).

```
> set type=CNAME
> www.lequotidien-oran.com
Serveur :   UnKnown
Address:  192.168.1.1

Réponse ne faisant pas autorité :
www.lequotidien-oran.com        canonical name = ns002.naltis.com
>
```



Invite de commandes

```
C:\Users\DVSR>ping www.lequotidien-oran.com

Envoi d'une requête 'ping' sur ns002.naltis.com [91.121.146.205] avec 32 octets de données :
Réponse de 91.121.146.205 : octets=32 temps=133 ms TTL=48
Réponse de 91.121.146.205 : octets=32 temps=75 ms TTL=48
Réponse de 91.121.146.205 : octets=32 temps=73 ms TTL=48
Réponse de 91.121.146.205 : octets=32 temps=83 ms TTL=48

Statistiques Ping pour 91.121.146.205:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 73ms, Maximum = 133ms, Moyenne = 91ms

C:\Users\DVSR>ping ns002.naltis.com

Envoi d'une requête 'ping' sur ns002.naltis.com [91.121.146.205] avec 32 octets de données :
Réponse de 91.121.146.205 : octets=32 temps=74 ms TTL=48
Réponse de 91.121.146.205 : octets=32 temps=74 ms TTL=48
Réponse de 91.121.146.205 : octets=32 temps=74 ms TTL=48
Réponse de 91.121.146.205 : octets=32 temps=74 ms TTL=48

Statistiques Ping pour 91.121.146.205:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 74ms, Maximum = 74ms, Moyenne = 74ms

C:\Users\DVSR>
```

- Pour récupérer les noms des serveurs mail dans un domaine, il suffit de changer le type de l'enregistrement demandé (set type=MX) :

```
set type=MX
google.com
```

- Les noms des serveurs retournés sont des noms de serveurs mail. La valeur de préférence permet de choisir entre plusieurs serveurs mail (une valeur de préférence plus petite indique une préférence supérieur par rapport aux autres serveurs mail disponibles) ; Dans cet exemple : Le serveur mail préféré de google est == *asmpx.l.google.com* (la valeur de préférence minimale);
- Plusieurs serveurs mail peuvent coexister dans un domaine pour que le système soit tolérant au pannes (s un serveur ne peut pas recevoir le mail entrant, le prochain mail selon la valeur de préférence est choisi pour l'échange du mail en question) ;
- *MX= Mail eXchanger* ;

Windows PowerShell

```
PS C:\Users\DVSR> nslookup
Serveur par dÚfaut :   UnKnown
Address:  192.168.1.1

> set type=mx
> google.com
Serveur :   UnKnown
Address:  192.168.1.1

Réponse ne faisant pas autorité :
google.com      MX preference = 40, mail exchanger = alt3.aspmx.l.google.com
google.com      MX preference = 50, mail exchanger = alt4.aspmx.l.google.com
google.com      MX preference = 20, mail exchanger = alt1.aspmx.l.google.com
google.com      MX preference = 30, mail exchanger = alt2.aspmx.l.google.com
google.com      MX preference = 10, mail exchanger = aspmx.l.google.com
>
```