# TP DNS

# Qu’est ce que le dns ?

Lorsque nous souhaitons se connecter à un site, nous utilisons donc le nom de domaine dans la barre de recherche, par exemple btssio.fr, à moins que le nom de domaine pour notre navigateur soit techniquement inutile.

Il lui faut donc savoir à quel serveur il se connecte, ainsi qu'à l'adresse IP du serveur sur lequel il trouvera les pages web.

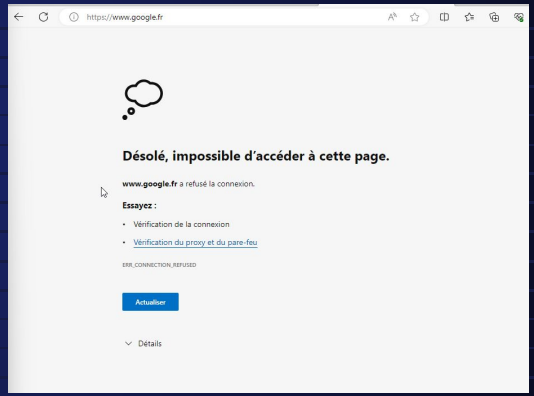
Le DNS ( Domainname system ) est un outil qui permet de traduire les nom de domaines en adresses IP.

La résolution des noms de domaine est la corrélation entre ces nom de domaines et les adresses IP, et les serveurs dns sont chargés de faire la correspondance entre ces nom de domaines et les adresses ip.

Sous Windows, le premier fichier interrogé pour la résolution des noms de domaine est : c:\WINDOWS\system32\drivers\etc\hosts

Nous allons donc nous rendre dans le bloc note, l'ouvrir en administrateur et aller dans les fichiers, sélectionner tous les fichiers pour voir le fichier host, et ainsi pouvoir ajouter l'ip 127.0.0.1 devant le nom de domaine du site qu'on veut interdire car cela va faire en sorte qu'on ne puisse plus y accéder que ce soit pour Google ou n'importe quel site et navigateur.

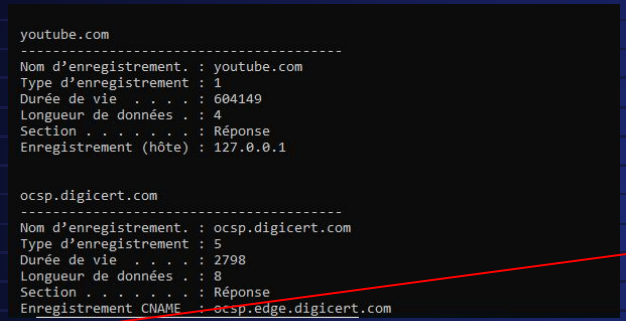
```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

127.0.0.1 google.fr
```




L'IP 127.0.0.1 est l'adresse de boucle locale de notre propre ordinateur, souvent appelée localhost. En redirigeant un nom de domaine vers cette adresse, toute requête destinée à ce domaine sera renvoyée vers votre propre machine plutôt que vers l'adresse IP réelle du site web.

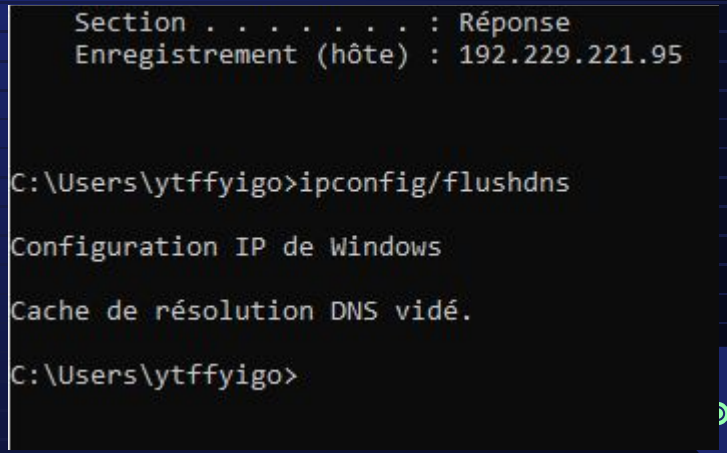
# A quoi sert la commande ipconfig/displaydns ?

La commande ipconfig /displaydns sous Windows est utilisée pour afficher le cache DNS du système. Ce cache contient les réponses récentes des requêtes DNS émises par notre ordinateur.il affiche les adresses des sites Web et autres services Web visités récemment, ce qui peut accélérer la résolution DNS de ces sites Web lorsqu'on les visite à nouveau.




Don cette commande vide le cache de résolution dns.

Le cache DNS est une forme de répertoire temporaire utilisée par notre système pour enregistrer les réponses aux requêtes DNS récentes. Ces réponses consistent en les adresses IP des sites web auxquels vous vous êtes connecté. Enregistrer ces informations permet à votre système d'accéder plus rapidement à ces sites lors de visites futures, car il n'a pas besoin de demander l'adresse IP à un serveur DNS distant.



L'accès au site internet est parfois plus long. Si vous désirez arriver plus rapidement sur la page d'un site préféré alors vous pouvez faire une entrée dans le fichier host

```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
127.0.0.1 www.youtube.com
87.98.154.146 www.btssio.fr
```

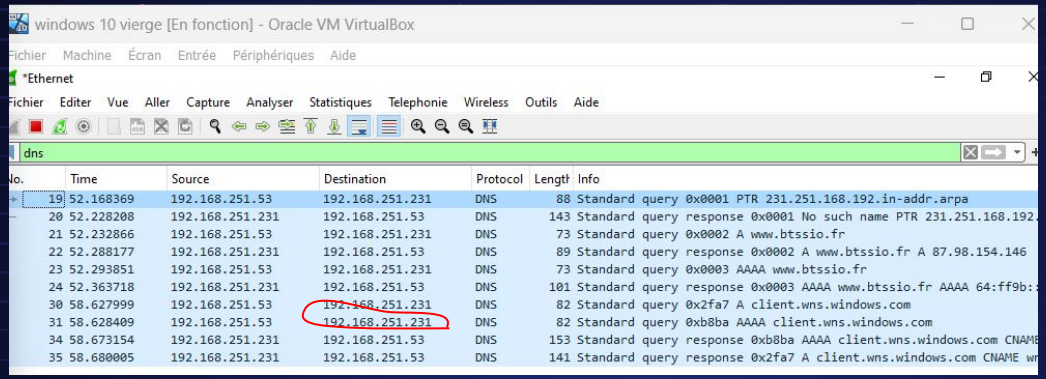
Que peut interroger le poste client comme serveur DNS ?

Il peut interroger tous les serveurs dns

Ma résolution DNS ne fonctionne pas et  je veux relancer une demande. La commande NSLOOKUP permet de faire une nouvelle demande

```
C:\Users\marel>nslookup btssio.fr
Serveur :   UnKnown
Address:  192.168.251.231

Réponse ne faisant pas autorité :
Nom :    btssio.fr
Addresses:  64:ff9b::5762:9a92
          87.98.154.146
```

Pour capturer une trame dns , on peut aller dans wireshark et marquer dns dans le filtre pour obtenir que les requêtes dns . Le nom de domaine est reliée à l'ip 192.168.251.231




L'opération inverse DNS consiste à trouver un nom de domaine associé à une adresse e-mail. Dans les serveurs DNS, cette information est enregistrée sous forme de PTR.

Par exemple, si je souhaiterais connaître le nom de domaine associé à l'adresse IP 87.98.168.168 :

```
\Users\Nico>nslookup 87.98.154.146
rveur :   UnKnown
dress:  192.168.251.231

m :    cluster026.hosting.ovh.net
dress:  87.98.154.146
```