



LE SERVICE DNS

- L'adresse IP indiquée est celle du wordpress du TP précédent.
- Dans cet annuaire, nous pouvons faire correspondre des noms de postes avec des adresses IP.
- Mettre l'adress 127.0.0.1 et l'attribuer à <https://google.fr> ne fonctionne pas car ce n'est pas l'adresse de google

hosts - Bloc-notes

Fichier Edition Format Affichage Aide

```
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97      rhino.acme.com      # source server
#      38.25.63.10      x.acme.com          # x client host


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


# nas local
      192.168.100.64| www.nas.local
      127.0.0.1        https://google.fr/
```

LE SERVICE DNS

Ipconfig /displaydns, affiche le contenu du cache de notre DNS. Plusieurs informations sont visibles comme le nom et le type d'enregistrement, la durée de vie, la longueur de données...

```
C:\Users\windob>ipconfig /all

Configuration IP de Windows

    Nom de l'hôte . . . . . : DESKTOP-A69G50B
    Suffixe DNS principal . . . . . :
    Type de noeud . . . . . : Hybride
    Routage IP activé . . . . . : Non
    Proxy WINS activé . . . . . : Non
    Liste de recherche du suffixe DNS.: sio.local

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . : sio.local
    Description. . . . . : Intel(R) PRO/1000 MT Desktop Adapter
    Adresse physique . . . . . : 08-00-27-6E-6C-A7
    DHCP activé. . . . . : Oui
    Configuration automatique activée. . . : Oui
    Adresse IPv6 de liaison locale. . . . : fe80::f451:c235:1a19:dd5d%6(préfééré)
    Adresse IPv4. . . . . : 192.168.60.179(préfééré)
    Masque de sous-réseau. . . . . : 255.255.255.0
    Bail obtenu. . . . . : vendredi 5 avril 2024 11:51:58
    Bail expirant. . . . . : vendredi 5 avril 2024 13:51:58
    Passerelle par défaut. . . . . : 192.168.60.254
    Serveur DHCP . . . . . : 192.168.60.254
    IAID DHCPv6 . . . . . : 101187623
    DUID de client DHCPv6. . . . . : 00-01-00-01-2D-A1-7C-B5-08-00-27-6E-6C-A7
    Serveurs DNS. . . . . : 185.156.80.7
                           8.8.8.8
    NetBIOS sur Tcpip. . . . . : Activé

C:\Users\windob>
```

```
C:\Users\windob>ipconfig /displaydns

Configuration IP de Windows

    client.wns.windows.com
    -----
    Nom d'enregistrement. : client.wns.windows.com
    Type d'enregistrement : 5
    Durée de vie . . . . : 208
    Longueur de données . : 8
    Section . . . . . : Réponse
    Enregistrement CNAME : wns.notify.trafficmanager.net

    Nom d'enregistrement. : wns.notify.trafficmanager.net
    Type d'enregistrement : 1
    Durée de vie . . . . : 208
    Longueur de données . : 4
    Section . . . . . : Réponse
    Enregistrement (hôte) : 20.199.120.182

    wpad
    -----
    Le nom n'existe pas.

    wpad
    -----
    Le nom n'existe pas.

C:\Users\windob>
```

LE SERVICE DNS

```
Microsoft Windows [version 10.0.1904
Microsoft Corporation. Tous droit
ers\windob>nslookup
request timed out.
timeout was 2 seconds.
eur par d'faut : UnKnown
ess: 185.156.80.7

C:\Users\windob>ipconfig /flush
Configuration IP de Windows
Cache de r solution DNS vid .

C:\Users\windob>_
```

- La commande `ipconfig /flushdns`, permet de vider le cache du DNS
- La commande `NSLOOKUP`, pour faire une nouvelle requ te de DNS.

UTILISATION DE WIRESHARK

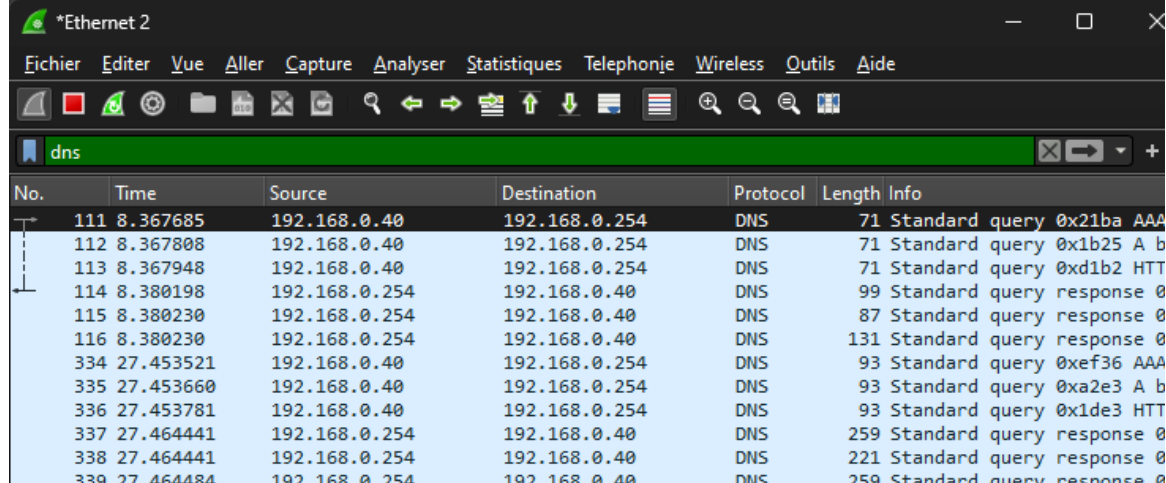
- Après avoir vider mon cache DNS (`ipconfig /flushdns`) et fais un `nslookup`, je me rend dans Wireshark.
- On voit donc les requêtes DNS, de mon adresse IP afin d'obtenir un nouveau DNS.

```
PS C:\Users\Bapt> ipconfig /flushdns

Configuration IP de Windows

Cache de résolution DNS vidé.
PS C:\Users\Bapt> nslookup
Serveur par défaut : UnKnown
Address: 192.168.0.254

>
```



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|---------------|---------------|----------|--------|---------------------------|
| 111 | 8.367685 | 192.168.0.40 | 192.168.0.254 | DNS | 71 | Standard query 0x21ba AAA |
| 112 | 8.367808 | 192.168.0.40 | 192.168.0.254 | DNS | 71 | Standard query 0x1b25 A b |
| 113 | 8.367948 | 192.168.0.40 | 192.168.0.254 | DNS | 71 | Standard query 0xd1b2 HTT |
| 114 | 8.380198 | 192.168.0.254 | 192.168.0.40 | DNS | 99 | Standard query response 0 |
| 115 | 8.380230 | 192.168.0.254 | 192.168.0.40 | DNS | 87 | Standard query response 0 |
| 116 | 8.380230 | 192.168.0.254 | 192.168.0.40 | DNS | 131 | Standard query response 0 |
| 334 | 27.453521 | 192.168.0.40 | 192.168.0.254 | DNS | 93 | Standard query 0xef36 AAA |
| 335 | 27.453660 | 192.168.0.40 | 192.168.0.254 | DNS | 93 | Standard query 0xa2e3 A b |
| 336 | 27.453781 | 192.168.0.40 | 192.168.0.254 | DNS | 93 | Standard query 0x1de3 HTT |
| 337 | 27.464441 | 192.168.0.254 | 192.168.0.40 | DNS | 259 | Standard query response 0 |
| 338 | 27.464441 | 192.168.0.254 | 192.168.0.40 | DNS | 221 | Standard query response 0 |
| 339 | 27.464484 | 192.168.0.254 | 192.168.0.40 | DNS | 259 | Standard query response 0 |