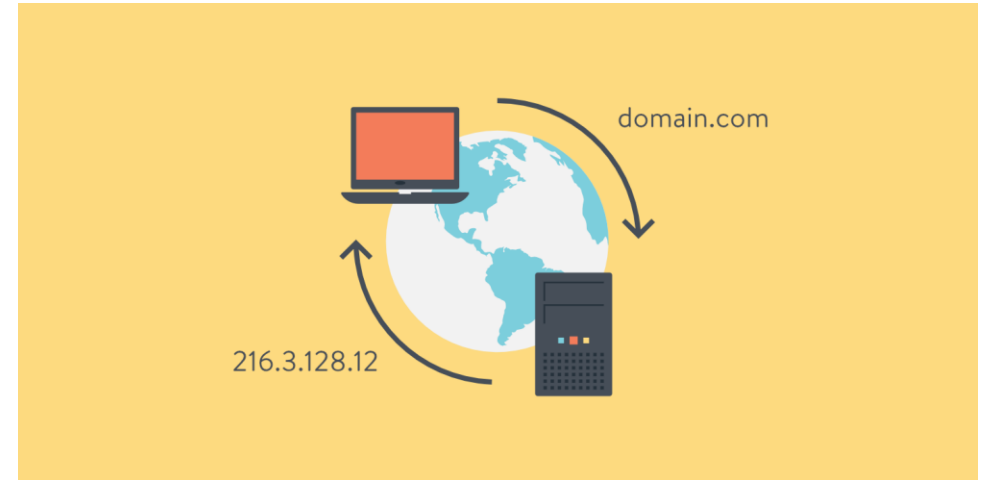


TP – DNS



Sommaire

01

Qu'est-ce
qu'un DNS ?

02

L'intérêt des
commandes en
mode terminal
sur Windows

03

Que peut
interroger le
poste client
serveur DNS ?

04

L'utilité des
commandes
"set type" avec
nslookup

Qu'est-ce qu'un DNS ?

Le DNS, ou bien « **Domain Name System** », est un système essentiel d'Internet qui agit comme un « annuaire » en traduisant les noms de domaine (comme google.fr) en adresses IP (142.250.201.163 parmi l'une des adresses de google en France) comprises par les machines.

Sans le DNS, il faudrait mémoriser chaque adresse IP pour chaque site, ce qui n'est pas pratique contrairement à un nom de domaine.

De plus, il permet de structurer l'organisation hiérarchique des domaines, tels que le **.com** ou le **.org**, qui facilite la navigation et permet de répartir la charge des serveurs.

Pour résumer, le DNS simplifie l'accès aux ressources en ligne et assure le bon fonctionnement d'Internet.

**L'intérêt des
commandes
en mode
terminal sur
Windows**



À quoi correspond la commande « ipconfig /displaydns »

```
Invite de commandes
Microsoft Windows [version 10.0.26100.3476]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\moon>ipconfig /displaydns

Configuration IP de Windows

fe3cr.delivery.mp.microsoft.com
-----
Nom d'enregistrement. : fe3cr.delivery.mp.microsoft.com
Type d'enregistrement : 5
Durée de vie . . . . : 64
Longueur de données : 8
Section . . . . . : Réponse
Enregistrement CNAME : fe3.delivery.mp.microsoft.com

Nom d'enregistrement. : fe3.delivery.mp.microsoft.com
Type d'enregistrement : 5
Durée de vie . . . . : 64
Longueur de données : 8
Section . . . . . : Réponse
Enregistrement CNAME : glb.cws.prod.dcat.dsp.trafficmanager.net

Nom d'enregistrement. : glb.cws.prod.dcat.dsp.trafficmanager.net
Type d'enregistrement : 1
Durée de vie . . . . : 64
Longueur de données : 4
Section . . . . . : Réponse
```

```
Invite de commandes

Aucun enregistrement de type AAAA

www.btssio.fr
-----
Aucun enregistrement de type AAAA

Nom d'enregistrement. : www.btssio.fr
Type d'enregistrement : 1
Durée de vie . . . . : 604800
Longueur de données : 4
Section . . . . . : Réponse
Enregistrement (hôte) : 87.98.154.146

fd.api.iris.microsoft.com
-----
Nom d'enregistrement. : fd.api.iris.microsoft.com
Type d'enregistrement : 5
Durée de vie . . . . : 172
Longueur de données : 8
Section . . . . . : Réponse
Enregistrement CNAME : fd-api-iris.trafficmanager.net

Nom d'enregistrement. : fd-api-iris.trafficmanager.net
Type d'enregistrement : 5
Durée de vie . . . . : 172
Longueur de données : 8
```

La commande « **ipconfig /displaydns** » permet d'afficher tout le contenu du cache DNS local de son ordinateur.

Elle montre également toutes les entrées DNS en mémoire avec des informations comme :

- Le nom de domaine
- Le type d'enregistrement
- Le Time-To-Live (TTL)
- L'adresse IP associée

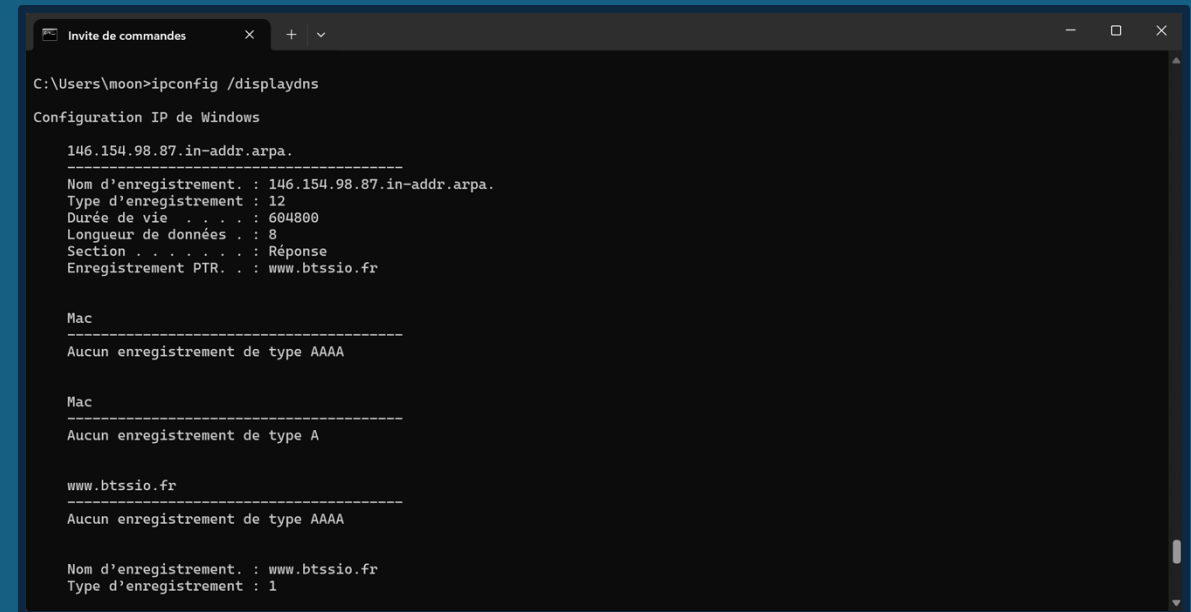
Cette commande se révèle utile lorsque l'on souhaite vérifier que le PC a bien résolu le nom de domaine, de détecter des comportements suspects comme un nom de domaine étranger qui est résolu dans le cache.

À quoi correspond la commande « ipconfig /flushdns »

```
C:\Users\moon>ipconfig /flushdns
```

Configuration IP de Windows

Cache de résolution DNS vidé.



```
Invite de commandes
C:\Users\moon>ipconfig /displaydns

Configuration IP de Windows

146.154.98.87.in-addr.arpa.
-----
Nom d'enregistrement. : 146.154.98.87.in-addr.arpa.
Type d'enregistrement : 12
Durée de vie          : 604800
Longueur de données   : 8
Section               : Réponse
Enregistrement PTR.   : www.btssio.fr

Mac
-----
Aucun enregistrement de type AAAA

Mac
-----
Aucun enregistrement de type A

www.btssio.fr
-----
Aucun enregistrement de type AAAA

Nom d'enregistrement. : www.btssio.fr
Type d'enregistrement : 1
```

La commande « **ipconfig /flushdns** » permet de **vider le cache DNS de son ordinateur**.

Cette commande sert à :

- Supprimer les entrées DNS obsolètes ;
- De résoudre des problèmes de navigation ;
- Forcer Windows à rechercher à nouveau les adresses IP auprès d'un serveur DNS.

Ainsi, la prochaine fois que l'utilisateur tapera une URL, son PC devra interroger un serveur DNS afin d'obtenir l'adresse IP.

Que peut interroger le poste client comme serveur DNS ?



1. L'utilisateur saisie un nom de domaine.
(ex: google.com)



2. Le fichier **hosts** est vérifié.
Si une ligne correspond alors il est utilisé directement.
Sinon, voir étape suivante.



3. Vérifie si il y a une entrée encore valide et l'utilise.
Autrement, voir étape suivante.



4. Interroge le serveur DNS configuré jusqu'à l'obtention de l'IP qui est retourné au client.



5. L'IP est enregistrée dans le cache DNS local.



6. Le client utilise l'IP pour contacter le site ou le serveur souhaité.

À quoi correspond la commande « ipconfig /all »

```
Microsoft Windows [version 10.0.26100.3476]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\moon>ipconfig /all

Configuration IP de Windows

    Nom de l'hôte . . . . . : MOONC609
    Suffixe DNS principal . . . . . :
    Type de noeud . . . . . : Hybride
    Routage IP activé . . . . . : Non
    Proxy WINS activé . . . . . : Non
    Liste de recherche du suffixe DNS.: lan

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . : localdomain
    Description. . . . . : Parallels VirtIO Ethernet Adapter
    Adresse physique . . . . . : 00-1C-42-81-66-39
    DHCP activé. . . . . : Oui
    Configuration automatique activée. . . : Oui
    Adresse IPv6. . . . . : fdb2:2c26:f4e4:0:57cc:2eb9:c4f2:c189(préféré)
    Adresse IPv6 temporaire . . . . . : fdb2:2c26:f4e4:0:99d:e7a3:c7ae:d225(préféré)
    Adresse IPv6 de liaison locale. . . . : fe80::d09b:c7c8:84a5:a04c%9(préféré)
    Adresse IPv4. . . . . : 10.211.55.4(préféré)
    Masque de sous-réseau. . . . . : 255.255.255.0
    Bail obtenu. . . . . : jeudi 1 mai 2025 22:15:07
    Bail expirant. . . . . : jeudi 1 mai 2025 22:45:06
    Passerelle par défaut. . . . . : fe80::21c:42ff:fe00:18%9
                                   10.211.55.1
    Serveur DHCP . . . . . : 10.211.55.1
    IAID DHCPv6 . . . . . : 83893314
    DUID de client DHCPv6. . . . . : 00-01-00-01-2F-78-07-25-00-1C-42-81-66-39
    Serveurs DNS. . . . . : fe80::21c:42ff:fe00:18%9
                                   10.211.55.1
                                   fe80::21c:42ff:fe00:18%9

    NetBIOS sur Tcpip. . . . . : Activé
    Liste de recherche de suffixes DNS propres à la connexion :
                                   lan

C:\Users\moon>
```

La commande « **ipconfig /all** » renseigne sur les informations réseau du poste informatique tel que :

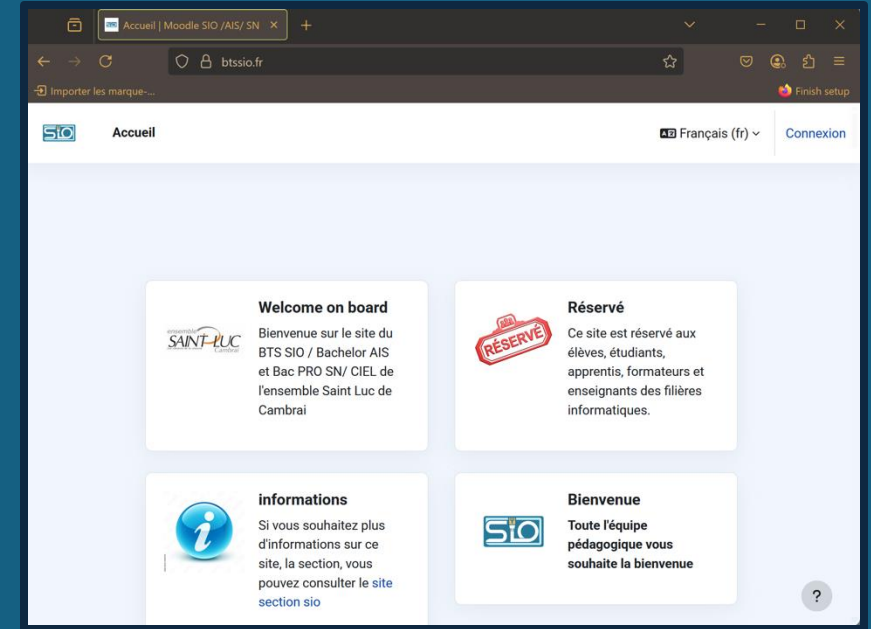
- L'adresse IP locale
- Le masque de sous-réseau/passerelle par défaut
- Le serveur DNS utilisé par le poste
- L'adresse MAC
- Le bail DHCP
- Etc.

Cette commande est principalement utilisée pour vérifier la connexion, d'identifier des conflits DHCP ou des problèmes de résolution de DNS.

Améliorer la fluidité du trafic

```
moon@Moon ~ %  
moon@Moon ~ % nslookup btssio.fr  
Server:      8.8.8.8  
Address:     8.8.8.8#53  
  
Non-authoritative answer:  
Name:   btssio.fr  
Address: 87.98.154.146  
  
moon@Moon ~ %
```

```
C:\Windows\System32\drivers\etc\hosts - Notepad++ [Administrator]  
Fichier  Édition  Recherche  Affichage  Encodage  Langage  Paramètres  Outils  Macro  Exécution  Modules d'  
change.log  hosts  
4 #  
5 # This file contains the mappings of IP addresses to host names. Each  
6 # entry should be kept on an individual line. The IP address should  
7 # be placed in the first column followed by the corresponding host name.  
8 # The IP address and the host name should be separated by at least one  
9 # space.  
10  
11 # Additionally, comments (such as these) may be inserted on individual  
12 # lines or following the machine name denoted by a '#' symbol.  
13  
14 # For example:  
15 #  
16 #      102.54.94.97      rhino.acme.com      # source server  
17 #      38.25.63.10      x.acme.com         # x client host  
18  
19 # localhost name resolution is handled within DNS itself.  
20 #      127.0.0.1        localhost  
21 #      ::1             localhost  
22 0.0.0.0                .psf  
23 0.0.0.0                Mac  
24 0.0.0.0                psf  
25 87.98.154.146 www.btssio.fr
```

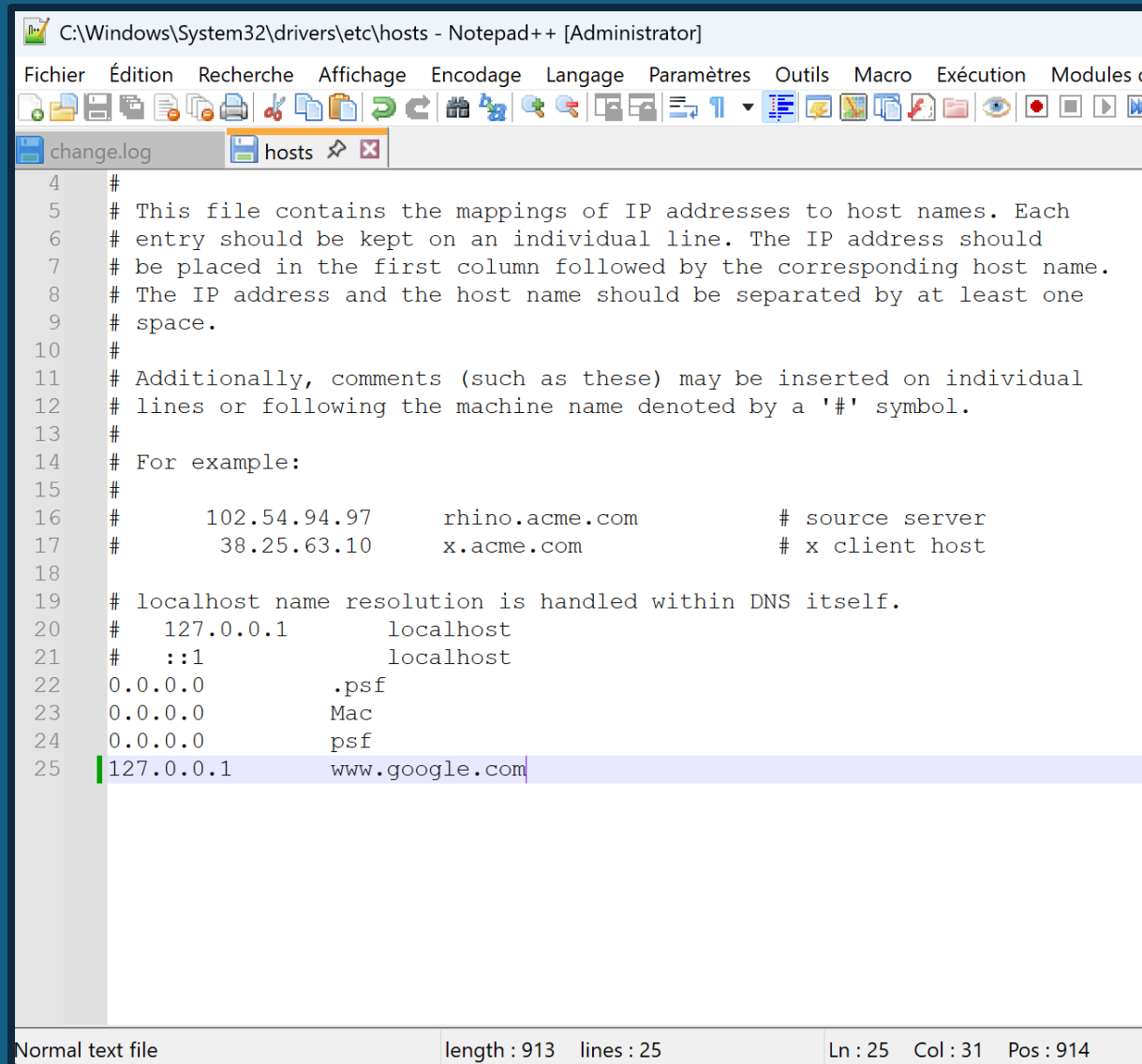


Il est également possible d'améliorer la rapidité d'accès aux sites en insérant l'IP publique ainsi que le domaine du site toujours dans le fichier **hosts**.

Afin de récupérer l'adresse IP publique, nous utiliserons la commande « **nslookup [site_web]** », celui-ci nous renvoie l'adresse que nous rentrerons dans le fichier **hosts** suivi du nom de domaine du site.

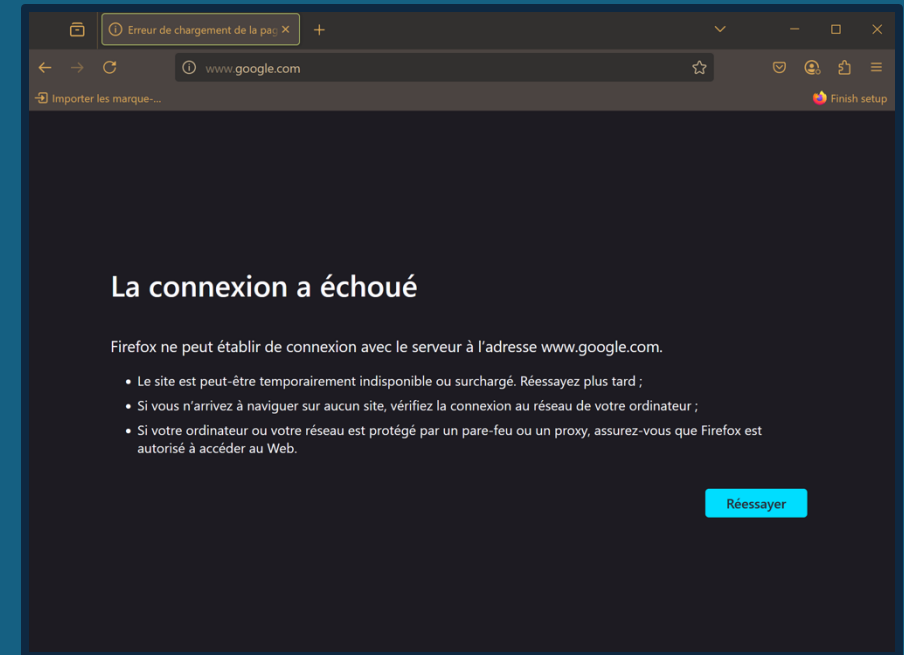
En effet, la prochaine fois que vous vous connecterez, le chargement de la page sera plus rapide.

Bloquer localement un site sur une machine Windows



```
C:\Windows\System32\drivers\etc\hosts - Notepad++ [Administrator]
Fichier Édition Recherche Affichage Encodage Langage Paramètres Outils Macro Exécution Modules d'extension
change.log hosts
4 #
5 # This file contains the mappings of IP addresses to host names. Each
6 # entry should be kept on an individual line. The IP address should
7 # be placed in the first column followed by the corresponding host name.
8 # The IP address and the host name should be separated by at least one
9 # space.
10 #
11 # Additionally, comments (such as these) may be inserted on individual
12 # lines or following the machine name denoted by a '#' symbol.
13 #
14 # For example:
15 #
16 #      102.54.94.97      rhino.acme.com      # source server
17 #      38.25.63.10      x.acme.com          # x client host
18
19 # localhost name resolution is handled within DNS itself.
20 # 127.0.0.1      localhost
21 # ::1           localhost
22 0.0.0.0         .psf
23 0.0.0.0         Mac
24 0.0.0.0         psf
25 127.0.0.1       www.google.com
```

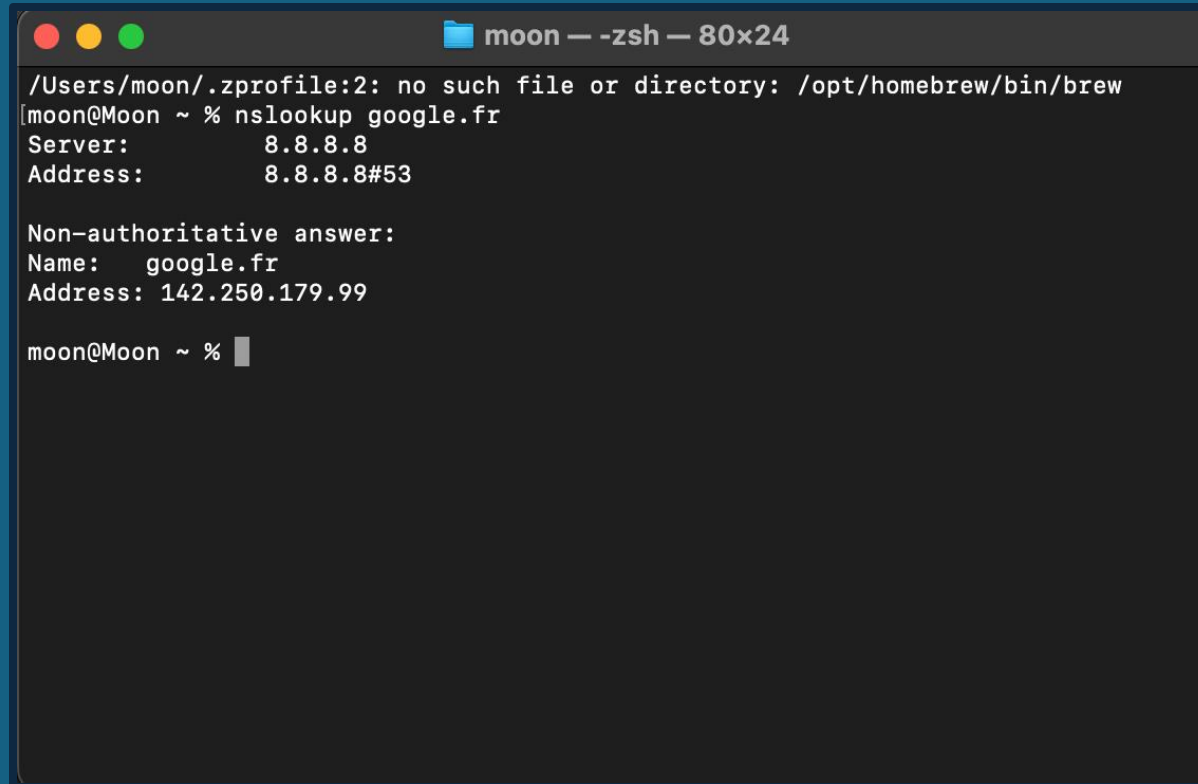
Normal text file length : 913 lines : 25 Ln : 25 Col : 31 Pos : 914



Pour bloquer localement sur une machine un site spécifique, il suffit de se rendre dans le répertoire : **c:\WINDOWS\system32\drivers\etc** et d'ouvrir le fichier **hosts**.

En rattachant l'IP localhost à un nom de domaine public permet de bloquer l'accessibilité au site comme nous pouvons le constater sur le second screen avec l'exemple de **google.com**.

Exécuter une nouvelle demande de résolution DNS



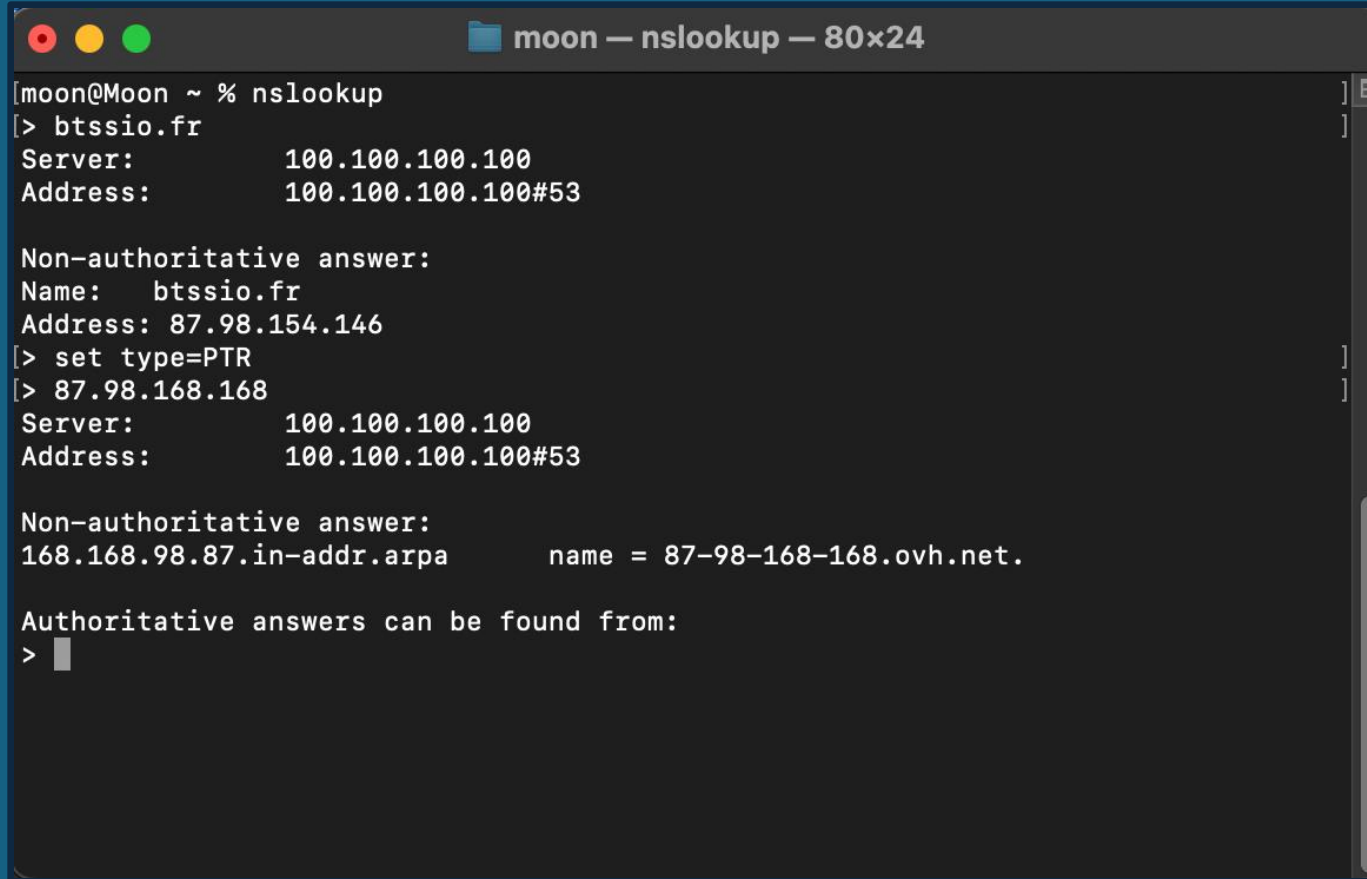
```
moon — -zsh — 80x24
/Users/moon/.zprofile:2: no such file or directory: /opt/homebrew/bin/brew
moon@Moon ~ % nslookup google.fr
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   google.fr
Address: 142.250.179.99

moon@Moon ~ %
```

La commande **nslookup** permet également de faire une nouvelle demande lorsque la résolution du DNS ne fonctionne pas.

Reverse DNS



```
moon@Moon ~ % nslookup
> btssio.fr
Server:      100.100.100.100
Address:     100.100.100.100#53

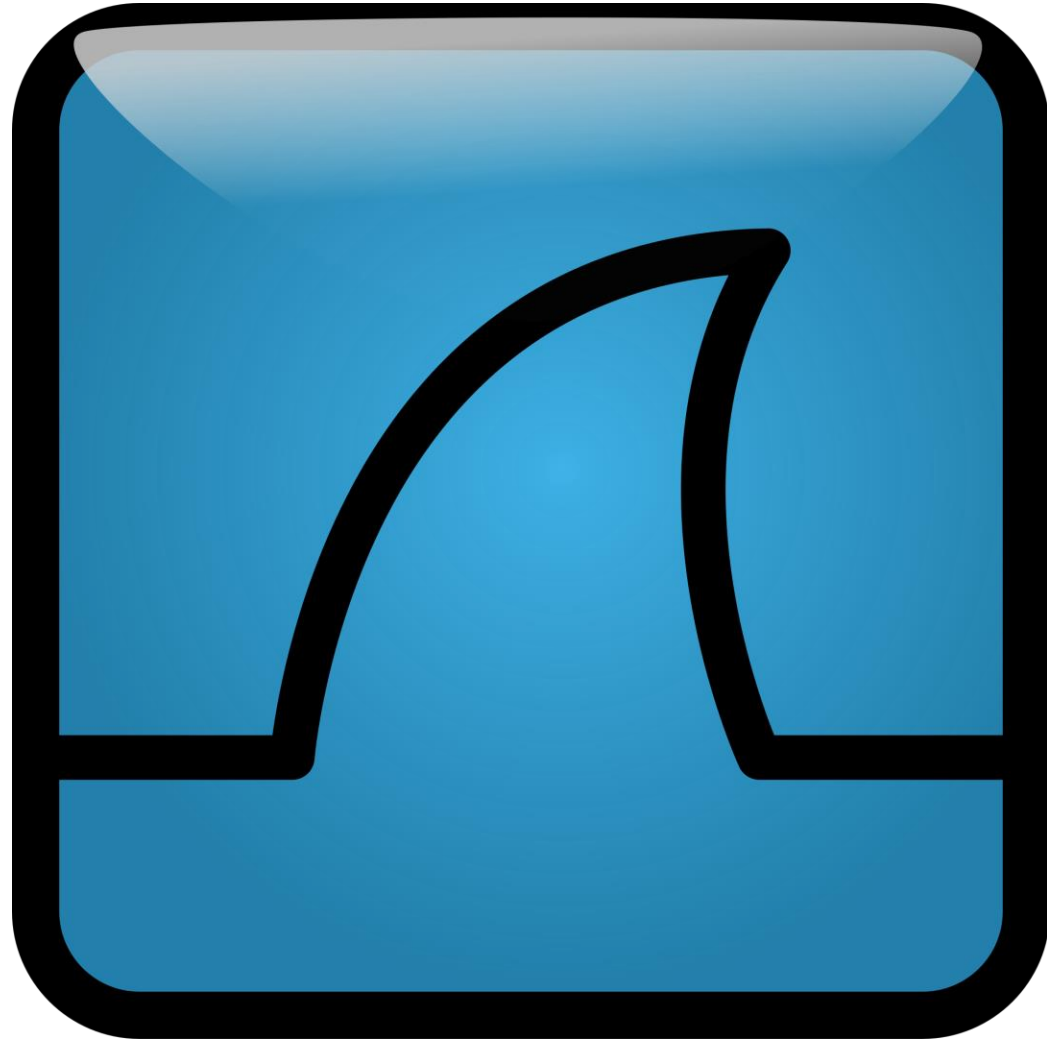
Non-authoritative answer:
Name:   btssio.fr
Address: 87.98.154.146
> set type=PTR
> 87.98.168.168
Server:      100.100.100.100
Address:     100.100.100.100#53

Non-authoritative answer:
168.168.98.87.in-addr.arpa      name = 87-98-168-168.ovh.net.

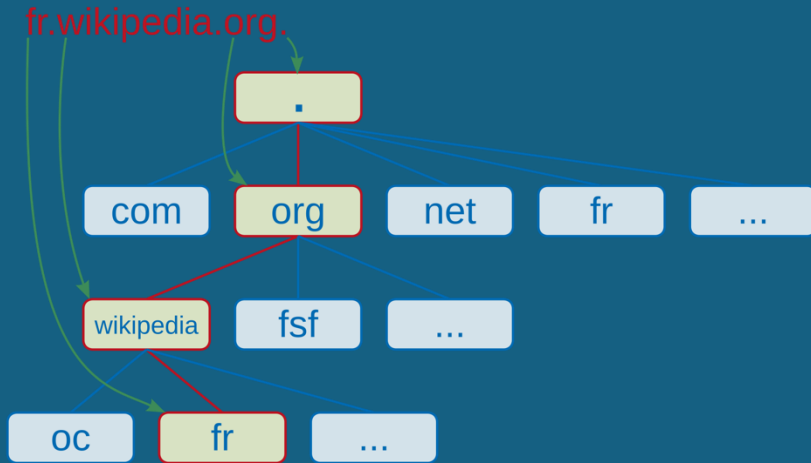
Authoritative answers can be found from:
>
```

Le reverse DNS permet de retrouver un nom de domaine associé à une adresse IP. Contrairement au DNS classique (A/AAAA), il fonctionne en inversant l'IP et en utilisant le domaine spécial « **.in-addr.arpa** » en **IPv4** ou « **.ip6.arpa** » en **IPv6**.

**Analyse
d'une trame
DNS sur
Wireshark**



À quoi est associé le FQDN de btssio.fr ?



Le **FQDN**, ou **Fully Qualified Domain Name**, est un nom de domaine qui donne la position exacte de son nœud dans l'arborescence DNS en indiquant tous les domaines de niveau supérieur.

The image shows a Wireshark capture of a DNS query and response. The top pane shows a list of packets, with packet 89 selected. The middle pane shows the details of the selected packet, which is a DNS Standard query response. The bottom pane shows the packet bytes in hexadecimal and ASCII. A blue arrow points to the answer section of the DNS response, which contains the IP address 87.98.154.146 for the domain www.btssio.fr.

No.	Time	Source	Destination	Protocol	Length	Info
77	5.543654	192.168.60.126	185.156.80.7	DNS	73	Standard query 0xalc7 A www.btssio.fr
89	6.544267	192.168.60.126	8.8.8.8	DNS	73	Standard query 0xalc7 A www.btssio.fr
90	6.566954	8.8.8.8	192.168.60.126	DNS	89	Standard query response 0xalc7 A www.btssio.fr A 87.98.154.146

Transaction ID: 0xalc7
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
Answers
www.btssio.fr: type A, class IN
www.btssio.fr: type A, class IN, addr 87.98.154.146
[Request In: 89]
[Time: 0.022687000 seconds]

```
moon — zsh — 80x24
root@Moon ~ # nslookup www.btssio.fr
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   www.btssio.fr
Address: 87.98.154.146
```

Videz le cache de la résolution DNS.

En lançant Wireshark, puis en tapant « **dns** » dans les filtres de recherche, capturons une trame lorsque l'on se connecte sur le site **btssio.fr** ou en faisant une requête **nslookup**.

Sans surprise, le FQDN de btssio.fr est l'IP **87.98.154.146**.

**L'utilité des
commandes
"set type"
avec nslookup**



Tableau des commandes « set type » dans nslookup

Commande	Type d'enregistrement	Définition
set type=A	Address	Résout un nom de domaine en adresse IPv4. (Par défaut)
set type=AAAA	AAAA	Résout un nom de domaine en adresse IPv6.
set type=MX	Mail Exchange	Liste les serveurs de messagerie (emails) d'un domaine.
set type=NS	Name Server	Affiche les serveurs DNS faisant autorité pour le domaine.
set type=PTR	Pointer	Effectue une résolution inverse (IP → nom de domaine).
set type=CNAME	Canonical Name	Trouve les alias DNS (redirections de noms).
set type=SOA	Start of Authority	Affiche les infos techniques de la zone DNS (serveur principal, TTL, etc.).
set type=TXT	Text	Récupère les enregistrements textes (utilisés pour SPF, DKIM, etc.).
set type=hinfo	Hardware Information	Permet d'afficher les informations concernant le système d'exploitation de l'hôte et de son matériel.