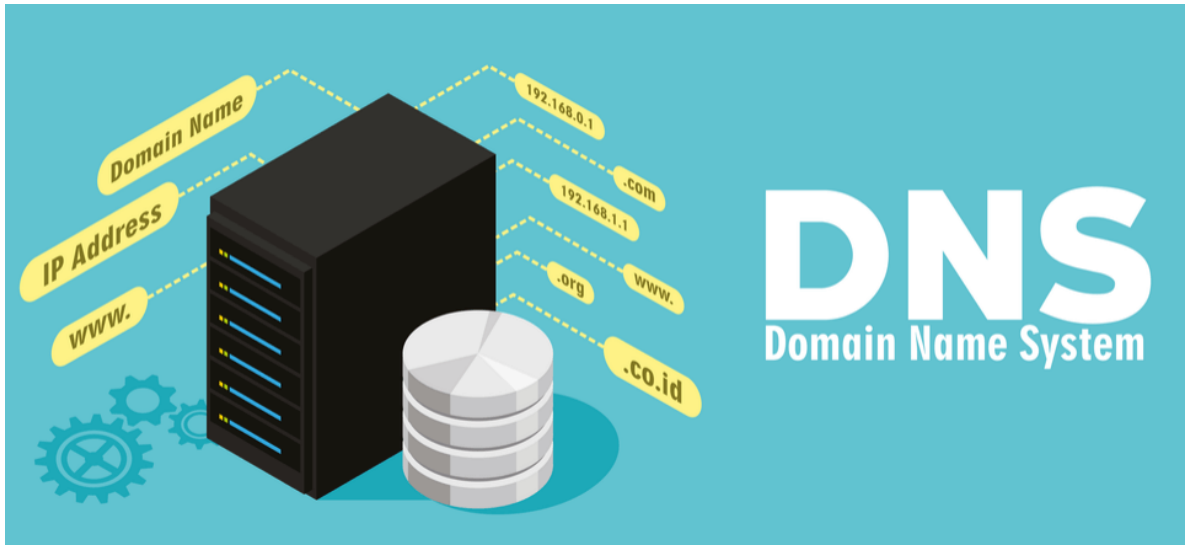
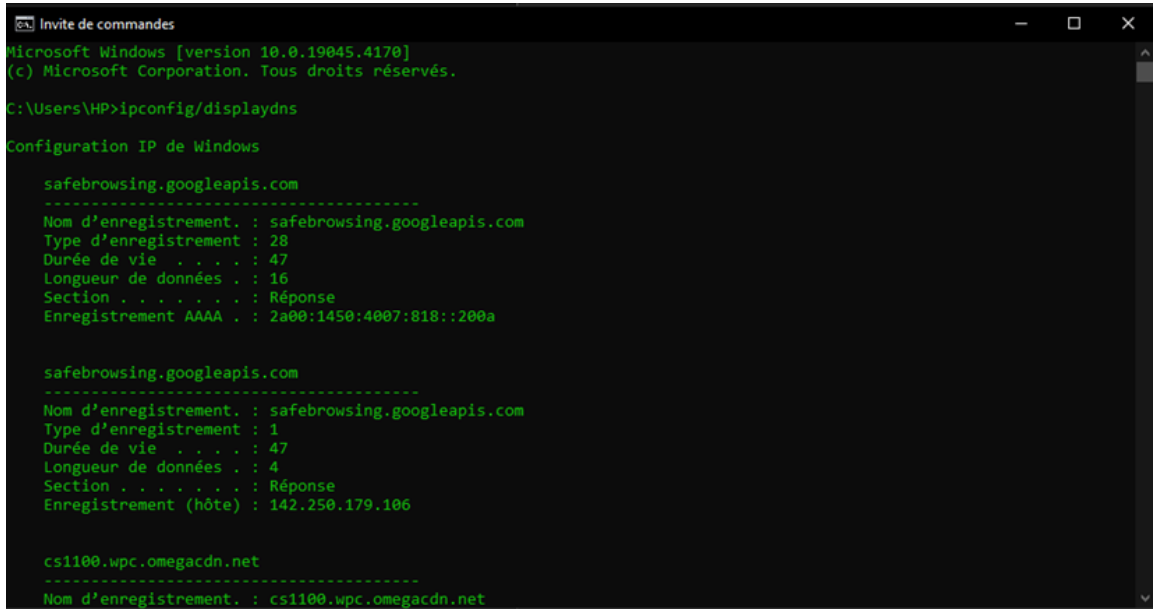
TP11 B1 DNS

Florentin Bracq- -Flabat, BTS SIO 1



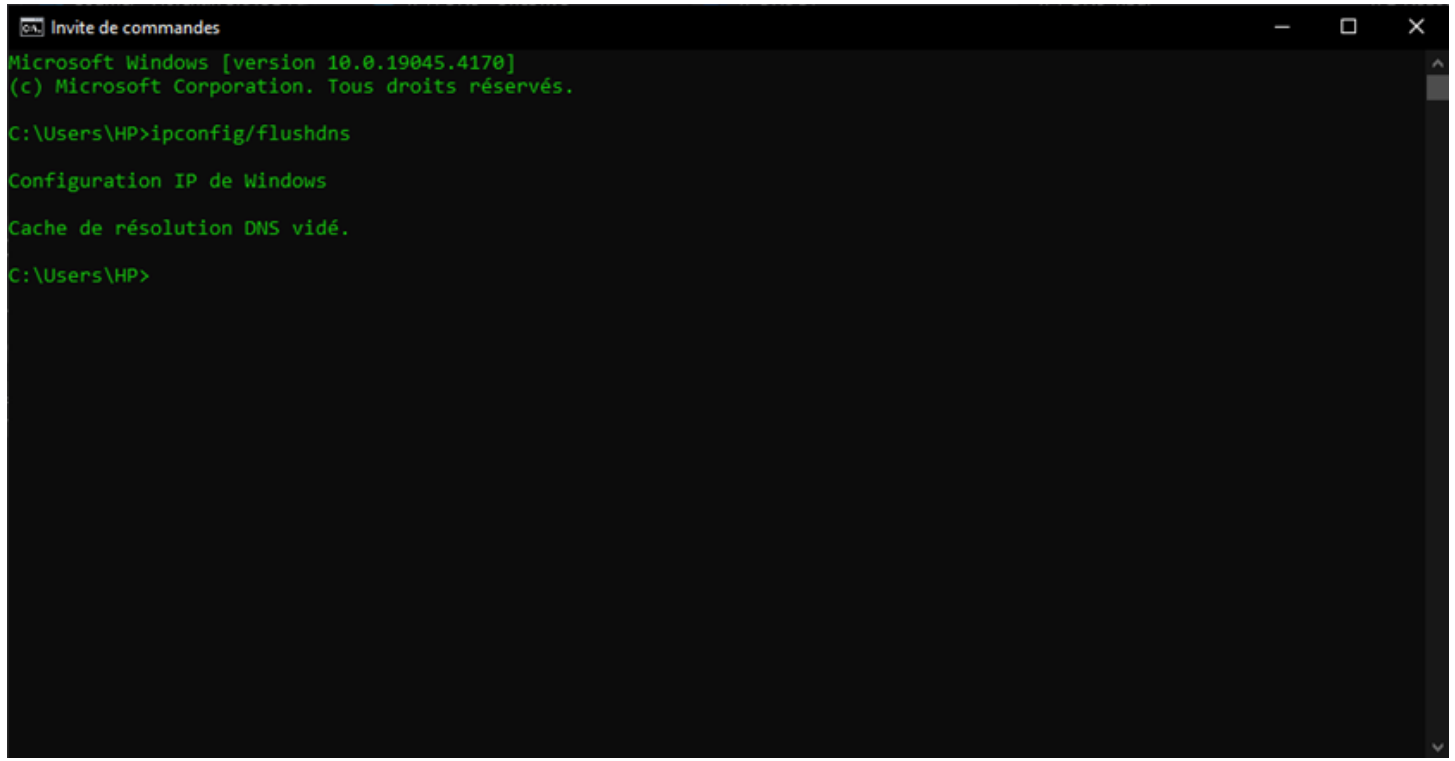
A quoi sert la commande **ipconfig/displaydns** ?

- Cette commande permet d'afficher le contenu du cache de résolution client DNS, qui comprend les entrées préchargées à partir du fichier hosts local et les enregistrements de ressource récemment obtenus pour les requêtes de nom résolues par l'ordinateur.
- Le service client DNS utilise ces informations pour résoudre rapidement les noms fréquemment interrogés, avant d'interroger ses serveurs DNS configurés.

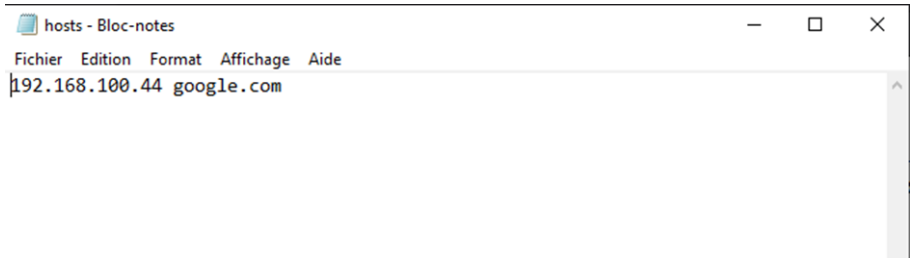


Vider les entrées du cache DNS

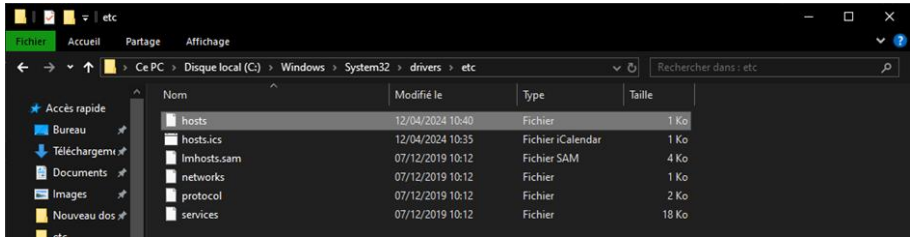
Pour vider le cache DNS taper la commande **ipconfig /flushdns**



Mise en place de la redirection DNS



- Pour mettre en place une redirection DNS, ouvrir le disque local Windows, puis suivre le chemin suivant : **C:\Windows\System32\drivers\etc**
- Dans le fichier host, indiquer en premier l'adresse IP, puis le nom de domaine, sur lequel on souhaite faire une redirection



Captures de trames avec Wireshark

- Pour filtrer les différentes requêtes, entrer dns dans la zone de texte Filter
- L'adresse IP associée à www.btssio.fr est 87.98.154.146

dns

No.	Time	Source	Destination	Protocol	Length	Info
50	2.745392	192.168.1.3	192.168.1.254	DNS	69	Standard query 0xecec HTTPS btssio.fr
51	2.745474	192.168.1.254	192.168.1.3	DNS	85	Standard query response 0x76b1 A btssio.fr A 87.98.154.146
52	2.745561	192.168.1.3	192.168.1.254	DNS	80	Standard query 0x13bb AAAA fonts.googleapis.com
53	2.745663	192.168.1.3	192.168.1.254	DNS	80	Standard query 0xeaef A fonts.googleapis.com
54	2.745793	192.168.1.3	192.168.1.254	DNS	80	Standard query 0x9713 HTTPS fonts.googleapis.com
55	2.745882	192.168.1.254	192.168.1.3	DNS	96	Standard query response 0xeaef A fonts.googleapis.com A 216.58.214.170
56	2.753102	192.168.1.254	192.168.1.3	DNS	108	Standard query response 0x13bb AAAA fonts.googleapis.com AAAA 2a00:1450:4007:81a::200a
57	2.753207	192.168.1.254	192.168.1.3	DNS	137	Standard query response 0x9713 HTTPS fonts.googleapis.com SOA ns1.google.com
58	2.758547	192.168.1.254	192.168.1.3	DNS	124	Standard query response 0x8bac AAAA btssio.fr SOA dns112.ovh.net
59	2.758547	192.168.1.254	192.168.1.3	DNS	124	Standard query response 0x6e83 AAAA btssio.fr SOA dns112.ovh.net
62	2.759698	192.168.1.3	192.168.1.254	DNS	77	Standard query 0xd15f AAAA fonts.gstatic.com
63	2.759809	192.168.1.3	192.168.1.254	DNS	77	Standard query 0x3cf1 A fonts.gstatic.com
64	2.759906	192.168.1.3	192.168.1.254	DNS	77	Standard query 0x79e9 HTTPS fonts.gstatic.com
66	2.766639	192.168.1.254	192.168.1.3	DNS	105	Standard query response 0xd15f AAAA fonts.gstatic.com AAAA 2a00:1450:4007:808::2003
69	2.767122	192.168.1.254	192.168.1.3	DNS	93	Standard query response 0x3cf1 A fonts.gstatic.com A 216.58.214.163
70	2.767195	192.168.1.254	192.168.1.3	DNS	134	Standard query response 0x79e9 HTTPS fonts.gstatic.com SOA ns1.google.com
73	2.771513	192.168.1.254	192.168.1.3	DNS	124	Standard query response 0x2e51 HTTPS btssio.fr SOA dns112.ovh.net
74	2.771513	192.168.1.254	192.168.1.3	DNS	124	Standard query response 0xecec HTTPS btssio.fr SOA dns112.ovh.net
128	5.207764	192.168.1.3	192.168.1.254	DNS	69	Standard query 0xde6b AAAA btssio.fr
129	5.208168	192.168.1.3	192.168.1.254	DNS	69	Standard query 0xd609 A btssio.fr
130	5.209750	192.168.1.254	192.168.1.3	DNS	85	Standard query response 0xd609 A btssio.fr A 87.98.154.146

Autres techniques pour récupérer l'adresse IP

- Utilisation de la commande nslookup
- Ping vers www.btssio.fr

```
Microsoft Windows [version 10.0.22631.3447]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Florentin>nslookup
Serveur par dÚfaut :   UnKnown
Address:  192.168.1.254

> btssio.fr
Serveur :   UnKnown
Address:  192.168.1.254

Réponse ne faisant pas autorité :
Nom :    btssio.fr
Address:  87.98.154.146

>
```

```
Microsoft Windows [version 10.0.22631.3447]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Florentin>ping btssio.fr

Envoi d'une requête 'ping' sur btssio.fr [87.98.154.146] avec 32 octets de données :
Réponse de 87.98.154.146 : octets=32 temps=11 ms TTL=56
Réponse de 87.98.154.146 : octets=32 temps=11 ms TTL=56
Réponse de 87.98.154.146 : octets=32 temps=12 ms TTL=56
Réponse de 87.98.154.146 : octets=32 temps=11 ms TTL=56

Statistiques Ping pour 87.98.154.146:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 11ms, Maximum = 12ms, Moyenne = 11ms

C:\Users\Florentin>
```