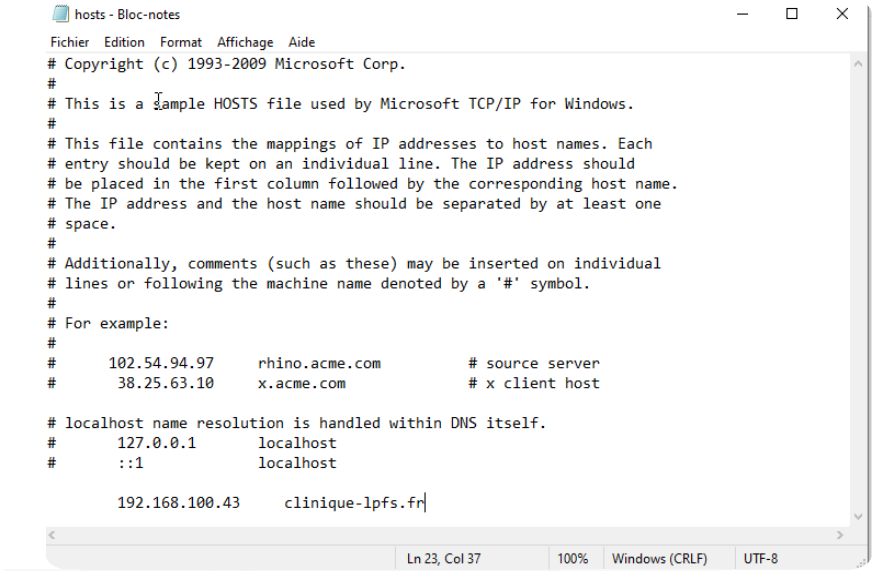
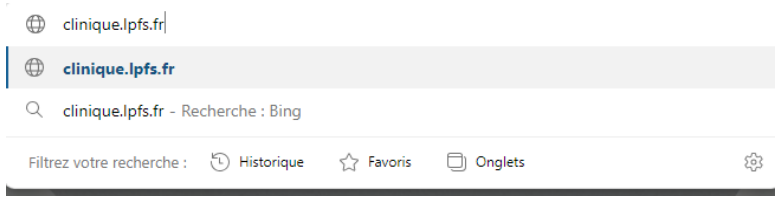
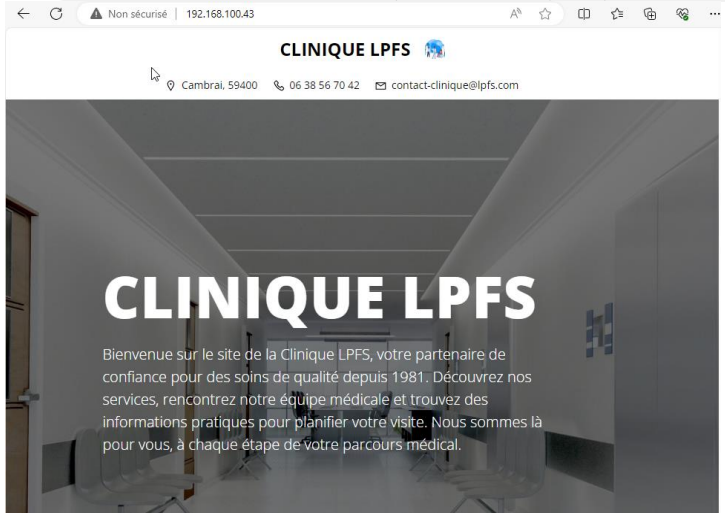
TP DNS

- Sous Windows, le fichier interrogé pour la résolution des noms de domaine est : C:\WINDOWS\system32\drivers\etc\hosts
- Lorsque l'on ajoute un nom de domaine à l'adresse IP d'un site dans ce fichier, celle-ci sera accessible en tapant le nom de domaine dans le navigateur : exemple avec le site 192.168.100.43 du TP Wordpress que j'ai associé au nom de domaine clinique-lpfs.fr

Modification du fichier e résolution des noms de domaine

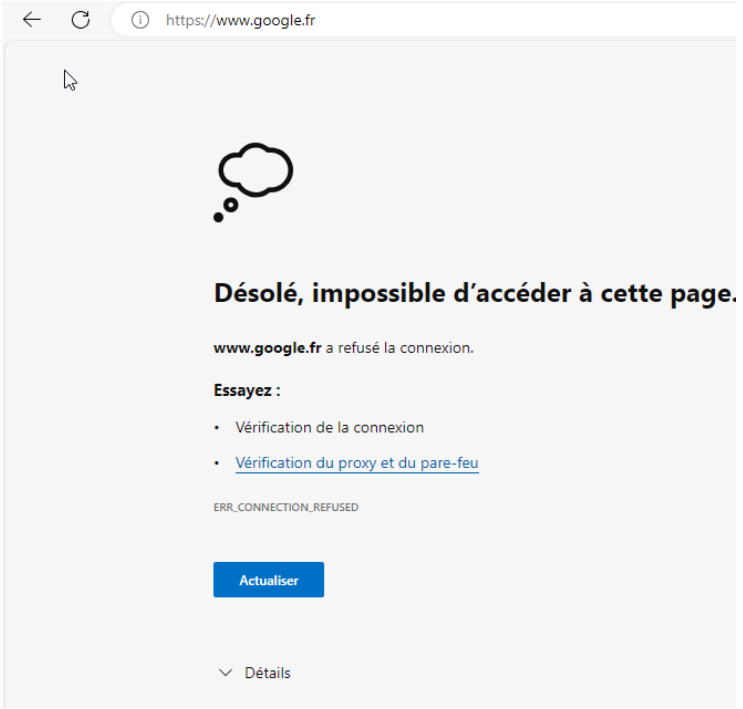






Modification du fichier

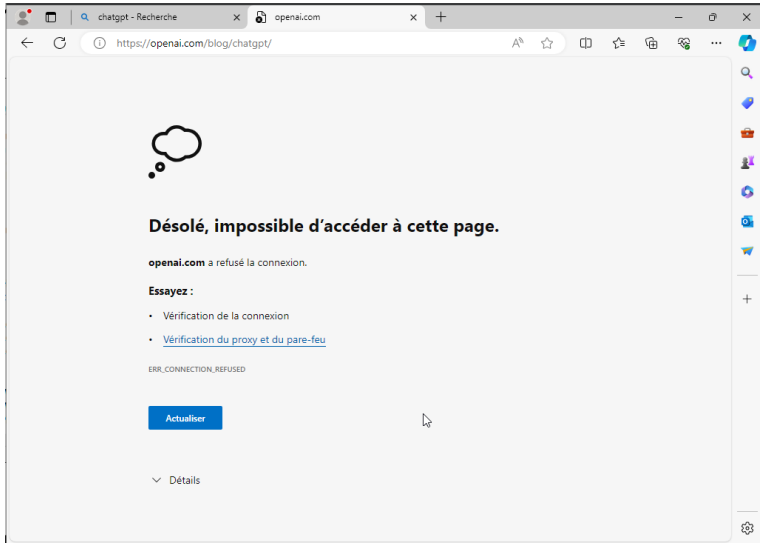
- Lorsque l'on ajoute 127.0.0.1 (le localhost) devant un nom de domaine le site n'est plus accessible, exemple avec google.fr

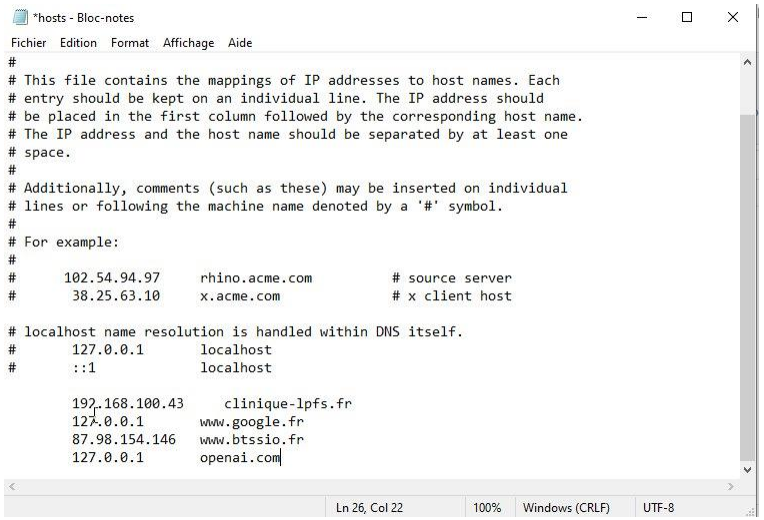



```
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Wind
#
# This file contains the mappings of IP addresses to host names
# entry should be kept on an individual line. The IP address sh
# be placed in the first column followed by the corresponding h
# The IP address and the host name should be separated by at le
# space.
#
# Additionally, comments (such as these) may be inserted on ind
# 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

        192.168.100.43     clinique-lpfs.fr
        127.0.0.1       www.google.fr
```

Bloquer ChatGPT

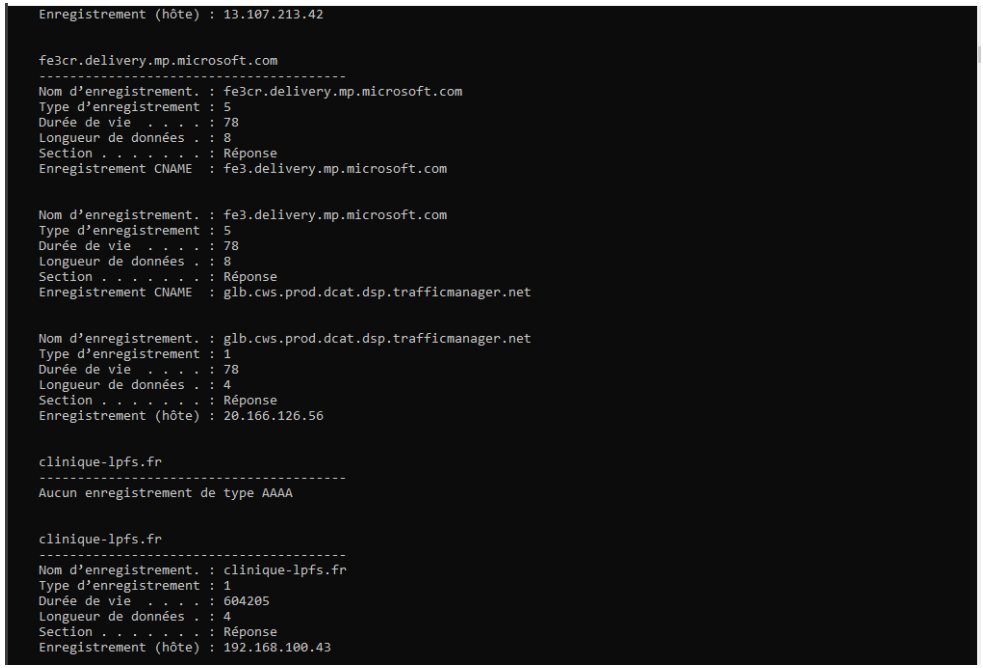
- Pour bloquer ChatGPT, la démarche a suivre est la meme que pour google et le site sera inaccessible.

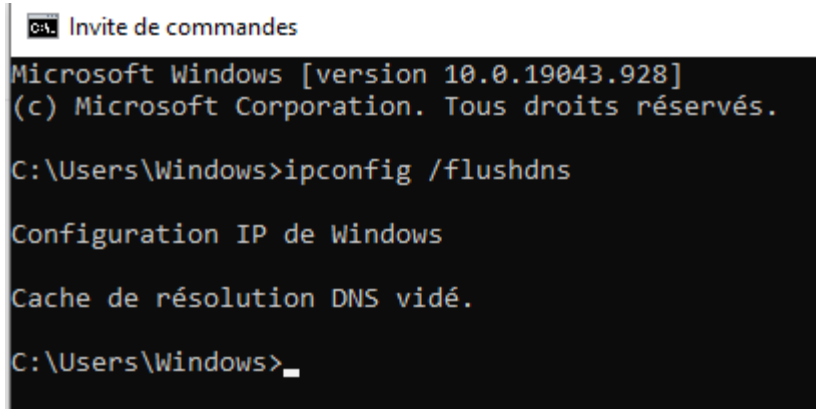




Cache DNS

- La commande ipconfig /displaydns sert à afficher le contenu du cache de la resolution DNS
- La commande ipconfig /flushdns sert a vider le cache de resolution DNS. Cela peut permettre de faciliter le dépannage des erreurs DNS.





Nslookup

- Le poste client peut interroger un servuer DNS pour obtenir des informations de resolutions de noms. C’est-à-dire qu'il envoie une requête DNS au serveur pour obtenir l'IP associée au nom de domaine.
- Pour se faire il faut utiliser la commande nslookup, puis le nom de domaine, exemple avec google.fr :

```
user@debian:~$ nslookup
> www.google.fr
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   www.google.fr
Address: 142.250.74.227
Name:   www.google.fr
Address: 2a00:1450:4007:80b::2003
>
```

Nslookup

- La commande Nslookup permet d'interroger le serveur DNS pour avoir d'autres informations sur le domaine comme par exemple le serveur de messageries, de nom, le mode d'interrogation etc…
- Sur linux la commande est : **dig *domaine* aaa**

```
user@debian:~$ nslookup
> www.google.fr
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   www.google.fr
Address: 142.250.74.227
Name:   www.google.fr
Address: 2a00:1450:4007:80b::2003
>
```

Par exemple pour obtenir le service de messagerie d'un domaine sur Windows on utilise la commande **set type=mx** ce qui donne :

```
> set type=mx
> btssio.fr
Serveur :   UnKnown
Address:  192.168.1.254

Réponse ne faisant pas autorité :
btssio.fr       MX preference = 1, mail exchanger = mx1.mail.ovh.net
btssio.fr       MX preference = 100, mail exchanger = mx3.mail.ovh.net
btssio.fr       MX preference = 5, mail exchanger = mx2.mail.ovh.net
```

```
user@debian:~$ dig www.google.fr aaaa

; <<>> DiG 9.16.44-Debian <<>> www.google.fr aaaa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51069
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.google.fr.                 IN      AAAA

;; ANSWER SECTION:
www.google.fr.          300     IN      AAAA    2a00:1450:4007:80b::2003

;; Query time: 24 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Apr 17 15:03:41 CEST 2024
;; MSG SIZE  rcvd: 70
```

Capture de Trame DNS

- Lorsque nous lançons une résolution du FQDN, avec la commande **Nslookup** après avoir vidé le cache local DNS avec la commande **ipconfig /flushdns**, nous pouvons constater que nous trouvons des trames DNS sur wireshark, l'adresse IP à laquelle est associée le FQDN pour www.btssio.fr est **185.156.80.7**