DNS

THOMAS-GRZESINSKI

A quoi sert le DNS ?

Définition: Le Domain Name Système est un service informatique distribué qui associe les noms de domaine internet avec leurs adresses IP ou d'autres types d'enregistres. En effet il est beaucoup plus facile de retenir un nom de domaine qu'une adresse IP, quand vous tapez un nom de domaine sur internet votre navigateur se charge de le convertir en adresse IP car seul les adresses IP circulent sur Internet.

Par exemple: Le nom de domaine de www.btssio.fr est raccordé l'adresse IP 87.98.154.146 si vous décidez de rentrer le nom de domaine ou l'adresse IP dans l'url de votre navigateur web vous arriverez dans tous les cas sur le site que vous souhaitiez visitez.

Le fichier hosts

Chaque ordinateur qui est sous Windows possède un fichier texte en clair qui se nomme «hosts », il agit comme un résolveur DNS local (type de serveur qui gère la traduction du « nom en adresse » dans laquelle une adresse IP est mise en correspondance avec un nom domaine, puis renvoyée à l'ordinateur qui l'a demandé) c'est dire que on peut utiliser ce fichier pour remplacer ou personnaliser la résolution DNS pour un nom de domaine uniquement sur la machine locale.

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# 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
```

Pour accéder à ce fichier :

c:\WINDOWS\system32\drivers\etc\hosts

ATTENTION il n'est modifiable qu'avec les droits d'administrateur

Les dangers

Avec le DNS il existe un piratage de nom de domaine qui est le DNS hijacking. Avec cette méthode un cybercriminel peut décider de rediriger les visiteurs d'un site web d'une entreprise vers un site contrefaits pour qu'ils puissent récupérer: de l'agent, données(personnels/sensibles).

Les cybercriminels peuvent aussi avoir des informations a partir de la messagerie entrante de l'entreprise afin de lancer des attaques de phishing sur les clients et personnels en utilisant les noms de domaine de l'entreprise pour mieux dissimuler la supercherie.

Trois vecteurs d'attaque du DNS HIJACKIN:

- Système de gestion de noms de domaine du registrar
- Registre de serveur de noms de domaine
- Les systèmes des prestataires de services DNS

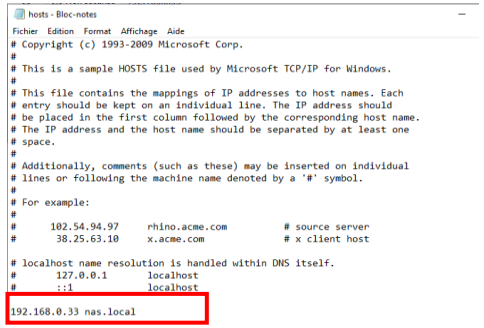
Attaque la plus utilisé: DOMAIN-SHADOWING les cybercriminels modifie les fichiers de zone d'un nom de domaine au lieu d'agir sur les serveurs de noms. Ce faisant, ils laissent le site Web ciblé intact, mais ajoutent un sous-domaine au fichier de zone, qui pourra être utilisé pour une attaque de phishing.

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# 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
```

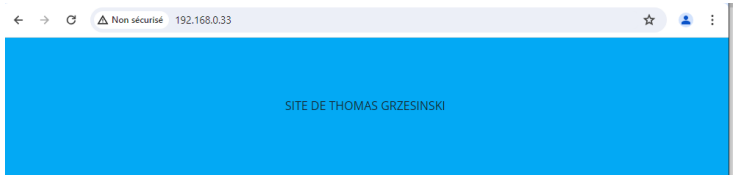
LES POSSIBILITÉS AVEC LE FICHIER HOSTS

Possibilité: Redirection

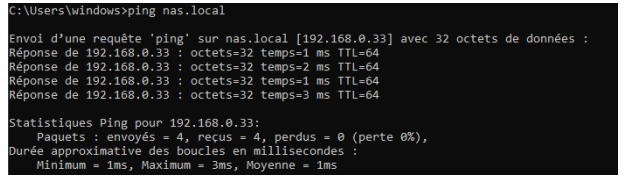
Mon site internet se trouve actuellement sur l'adresse IP 192.168.0.33 et son nom de domaine est nas.local



Quand sur internet je décide donc d'écrire dans la barre d'url mon nom de domaine je me retrouve sur mon site internet



Et on peut voir que lorsque je décide de ping mon nom de domaine il ping bien l'adresse IP de mon site



Possibilité: Redirection

Si vous souhaitez faire un sorte qu'un nom de domaine vous redirige vers un nom de domaine différents vous n'avez qu'a simplement modifier l'adresse IP de votre nom de domaine précédent.

Exemple: J'ai décidé de rediriger le nom de domaine vers le site du gouvernement vers les services publics. Si on tape donc le nom de domaine dans la barre d'URL je vais donc bien me retrouver sur le site des services public

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

160.92.168.33 www.nas.local
```

Même chose si je ping mon nom de domaine se sera maintenant l'adresse des services publics qui apparaîtra

```
C:\Users\windows>ping www.nas.local

Envoi d'une requête 'ping' sur www.nas.local [160.92.168.33] avec 32 octets de données :
Réponse de 160.92.168.33 : octets=32 temps=13 ms TTL=247
Réponse de 160.92.168.33 : octets=32 temps=13 ms TTL=247
Réponse de 160.92.168.33 : octets=32 temps=13 ms TTL=247
Réponse de 160.92.168.33 : octets=32 temps=13 ms TTL=247

Statistiques Ping pour 160.92.168.33:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 13ms, Maximum = 13ms, Moyenne = 13ms
```

Possibilité:Bannissement

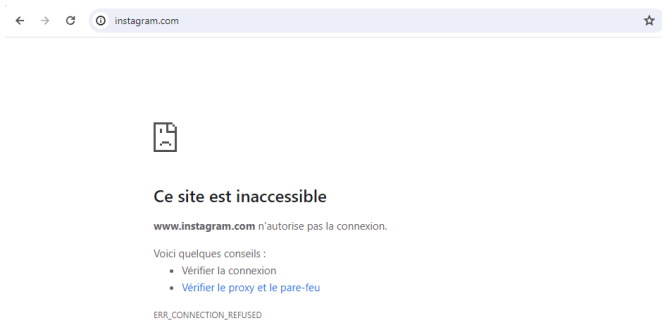
Si par exemple vous êtes une entreprise et que vous ne souhaitiez pas que vos salariés aillent sur les réseaux-sociaux ou autres sites.

Dans le fichier host vous n'avez qu'à rediriger le nom de domaine du site sur l'adresse 127.0.0.1.

Cet adresse réseau n'est disponible que dans votre ordinateur car elle signifie vous-mêmes d'où le nom « localhost ».

Donc pour bannir une IP on va donc rediriger les url des sites vers nous-mêmes et on verra que l'accès sera donc impossible.

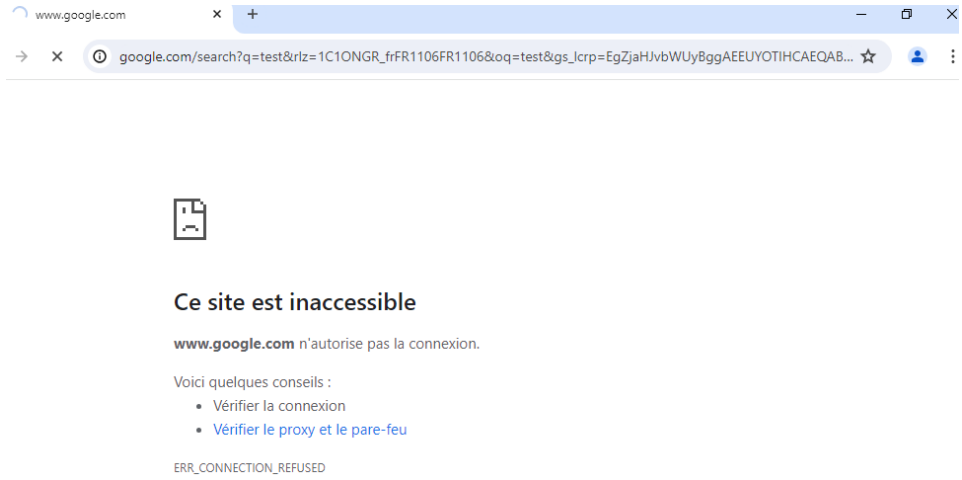
```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

127.0.0.1 www.instagram.com
```



Possibilité: Bannissement

Si vous décider de bannir www.google.com alors lorsque vous souhaiterez effectuer une recherche google vous aurez un message d'erreur indiquant que google n'autorise pas les connexions c'est-à-dire qu'aucune recherche ne sera disponible

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

127.0.0.1 www.google.com
```



Possibilité: Rapidité

Lorsque vous souhaitiez allez sur une page web plus rapidement il vous suffit donc de rentrer son adresse IP et son nom de domaine dans le fichier host et votre Ordinateur mettra donc moins de temps à retrouver une IP et son nom de domaine

Exemple:

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

160.92.168.33 www.service-public.fr
```

Que peut interroger le serveur DNS ?

Le serveur DNS peut interroger:

- La résolution des noms de domaine : Le client peut demander l'adresse IP associée à un nom de domaine (exemple www.btssio.fr vers son adresse IP)

- La résolution inverse : Demander le nom de domaine associée à une adresse IP

- Rechercher le serveur de messagerie : Le client peut interroger le serveur DNS pour obtenir les serveurs d'échange de courrier responsables de la réception des e-mails pour un domaine particulier

- Information sur les serveurs de noms : Il peut obtenir des informations sur les serveurs de noms autoritaires responsables d'un domaine

Que peut interroger le serveur DNS ?

- Informations textuelles : Les clients peuvent demander des informations textuelles arbitraires associées à un domaine, souvent utilisées à des fins de configuration ou pour fournir des détails supplémentaires.

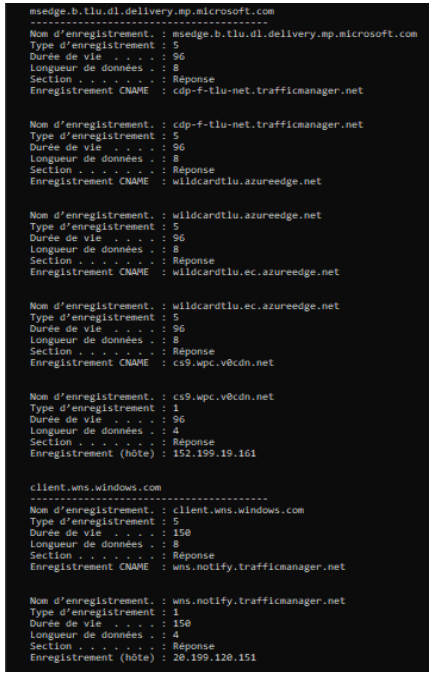
- Résolution des adresses IPV6 : Les clients peuvent demander des adresses IPV6 associées à un domaine

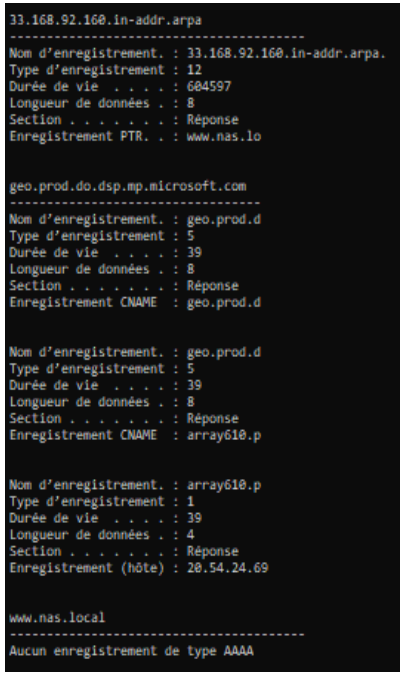
-Extensions de sécurité DNS (DNSSEC) : Si DNSSEC est implémenté, les clients peuvent demander des informations relatives à DNSSEC pour des transactions DNS sécurisées

LES COMMANDES UTILES/NSLOOKUP

Commande ipconfig/displaydns

La commande ipconfig/displaydns affiche le contenu DNS du cache de l'hôte.
Lorsque une requête pour un nom d'hôte est exécuté le résultat est mis en cache pour éviter les requêtes inutiles





Commande IPCONFIG/FLUSHDNS

La commande ipconfig/flushdns permet de supprimer le cache DNS de l'hôte

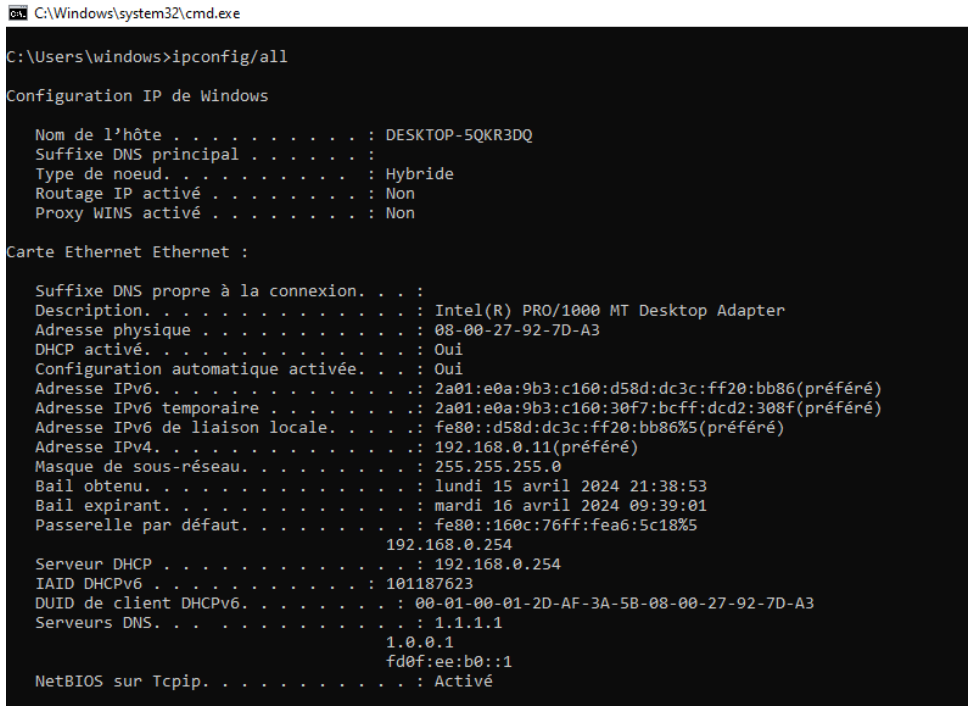
```
Microsoft Windows [version 10.0.19043.928]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\windows>ipconfig/flushdns

Configuration IP de Windows

Cache de résolution DNS vidé.
```

En effet quand on décide de réutiliser la commande ipconfig/displaydns tous les autres DNS ont disparu et seul celui que nous avions rajouté dans le fichier hosts apparait

```
Configuration IP de Windows

    33.168.92.160.in-addr.arpa
    ----------------------------------------
    Nom d'enregistrement. : 33.168.92.160.in-addr.arpa.
    Type d'enregistrement : 12
    Durée de vie  . . . . : 603833
    Longueur de données . : 8
    Section . . . . . . . : Réponse
    Enregistrement PTR. . : www.nas.local


    www.nas.local
    ----------------------------------------
    Aucun enregistrement de type AAAA


    www.nas.local
    ----------------------------------------
    Nom d'enregistrement. : www.nas.local
    Type d'enregistrement : 1
    Durée de vie  . . . . : 603833
    Longueur de données . : 4
    Section . . . . . . . : Réponse
    Enregistrement (hôte) : 160.92.168.33
```

Commande ipconfig/all

La commande ipconfig/all permet d'afficher la configuration TCPIP complète de toute les cartes réseau ainsi que la configuration DHCPet DNS



nslookup

La commande nslookup permet souvent de résoudre les problèmes liés à de la résolution DNS ou pour vérifier rapidement l'état d'un enregistrement DNS.

Qu'il y est un problème avec un serveur DNS local ou une zone DNS publique on peut utiliser nslookup pour obtenir des informations sur les enregistrements s DNS et tester la résolution de noms au niveau de la machine locale

nslookup

Exemple: Si vous voulez vérifier l'adresse IP associée au nom de domaine « service-public.fr » vous allez devoir entrer dans votre terminal windows la commande nslookup et ensuite entrer le nom de domaine.
On peut y constater que on peut y retrouver donc le nom de domaine et l'adresse IPV4 du nom de domaine.

Mais on peut voir qu'on y observe également un serveur et une adresse en 1.1.1.1 ce serveur et cette adresse correspond au serveur DNS sollicité par nslookup pour résoudre le nom de domaine. L'outil utilise ce serveur DNS car c'est le serveur DNS préféré sur notre interface réseau utilisé pour accéder à internet

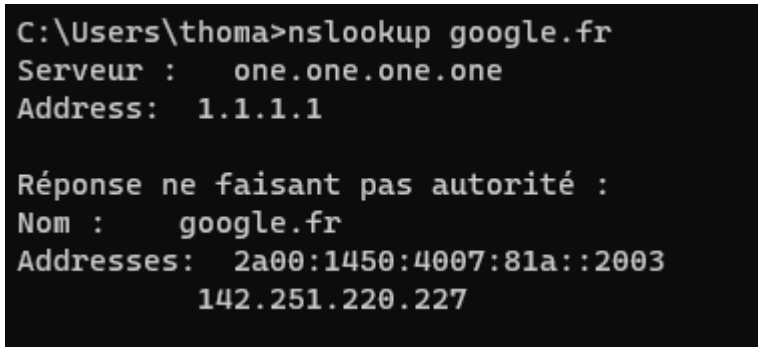
```
C:\Users\thoma>nslookup service-public.fr
Serveur :   one.one.one.one
Address:  1.1.1.1

Réponse ne faisant pas autorité :
Nom :    service-public.fr
Address:  160.92.168.33
```

```
Serveurs DNS. . .  . . . . . . . . . . . : 1.1.1.1
                                           1.0.0.1
```

Ipconfig/all pour voir le serveur DNS

nslookup

Si on souhaite le faire avec google on peut constater que le nom de domaine et une adresse IPV4 et IPV6 apparait, mais google possède différentes adresse IP et le résultat peut-être différents selon les machines



nslookup

On peut aussi faire une zone de recherche inversé c'est-à-dire que si on utilise l'adresse IP d'un nom de domaine on peut retrouver à quel nom de domaine elle est associée ici c'est donc cluster026.hosting.ovh.net

Vous pouvez le faire de deux façons différentes la première est de faire un nslookup + adresse IP ou bien alors utiliser la commande set type=PTR qui contient aussi l'information

```
C:\Users\thoma>nslookup 87.98.154.146
DNS request timed out.
    timeout was 2 seconds.
Serveur :   UnKnown
Address:  1.1.1.1

Nom :    cluster026.hosting.ovh.net
Address:  87.98.154.146
```

```
> set type=PTR
> 87.98.154.146
Serveur :   one.one.one.one
Address:  1.1.1.1

Réponse ne faisant pas autorité :
146.154.98.87.in-addr.arpa      name = cluster026.hosting.ovh.net
```

nslookup (interroger une messagerie d'un serveur)

Il existe aussi plusieurs commandes qui permettent d'interroger les serveurs de messagerie:

Set type=mx permet de recueillir les informations concernant le ou les serveurs de messagerie d'un domaine.

```
> set type=mx
> btssio.fr
Serveur :   one.one.one.one
Address:  1.1.1.1

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
```

set type=ns permet de recueillir les informations concernant le serveur de noms associé au domaine

```
> btssio.fr
Serveur :   one.one.one.one
Address:  1.1.1.1

Réponse ne faisant pas autorité :
btssio.fr       nameserver = dns112.ovh.net
btssio.fr       nameserver = ns112.ovh.net
```

nslookup (interroger une messagerie d'un serveur)

set type=a permet de recueillir les informations concernant un hôte du réseau. Il s'agit du mode d'interrogation par défaut.

```
> set type=a
> btssio.fr
Serveur :   one.one.one.one
Address:  1.1.1.1

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

set type=soa permet d'afficher les informations du champ SOA (Start Of Authority).

```
> set type=soa
> btssio.fr
Serveur :   one.one.one.one
Address:  1.1.1.1

Réponse ne faisant pas autorité :
btssio.fr
        primary name server = dns112.ovh.net
        responsible mail addr = tech.ovh.net
        serial  = 2023011007
        refresh = 86400 (1 day)
        retry   = 3600 (1 hour)
        expire  = 3600000 (41 days 16 hours)
        default TTL = 300 (5 mins)
```

set type=cname permet d'afficher les informations concernant les alias.

```
> set type=cname
> btssio.fr
Serveur :   one.one.one.one
Address:  1.1.1.1

btssio.fr
        primary name server = dns112.ovh.net
        responsible mail addr = tech.ovh.net
        serial  = 2023011007
        refresh = 86400 (1 day)
        retry   = 3600 (1 hour)
        expire  = 3600000 (41 days 16 hours)
        default TTL = 300 (5 mins)
```

nslookup (interroger une messagerie d'un serveur)

set type=hinfo permet, lorsque ces données sont renseignées, d'afficher les informations concernant le matériel et le système d'exploitation de l'hôte.

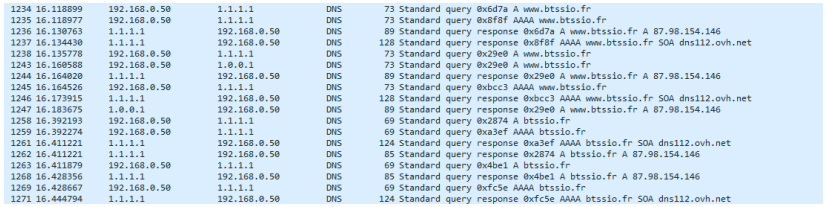
```
> set type=hinfo
> btssio.fr
Serveur :   one.one.one.one
Address:  1.1.1.1

btssio.fr
        primary name server = dns112.ovh.net
        responsible mail addr = tech.ovh.net
        serial  = 2023011007
        refresh = 86400 (1 day)
        retry   = 3600 (1 hour)
        expire  = 3600000 (41 days 16 hours)
        default TTL = 300 (5 mins)
```

RÉCUPÉRER UNE TRAME DNS AVEC WIRESHARK

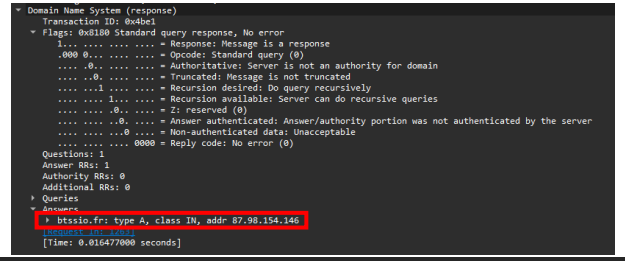
Récupérer une trame DNS

Pour récupérer une trame DNS avec Wireshark il vous suffit de rentrer le filtre DNS lors de votre récupération de trames.

Ensuite, vous allez sur le nom de domaine que vous souhaitiez allez et votre Wireshark vous récupéra la trame



Il est préférable de copier votre trame dans un fichier texte mais pour ma part je n'ai jamais pu le faire donc pour trouver le FQDN d'un nom de domaine cliquer sur la trame et dans DNS et vous pouvez observer le FQDN du nom de domaine pour le www.btssio.fr se sera donc 87.98.154.146



Le FQDN c’est quoi ?

Définition: Le FQDN (Fully qualified domain name) st un nom de domaine qui donne la position exacte de son nœud dans l'arborescence DNS en indiquant tous les domaines de niveau supérieur. On parle également d'un domaine absolu, par opposition à un domaine relatif.