UTILISATION DE WIRESHARK

PC - Windows / LINUX
Configuration de base
Tutoriel **WIRESHARK** - WINDOWS / LINUX
31 mars 2025

David GOÏTRÉ

Table des matières

Introduction

Wireshark est un outil pédagogique. Il analyse le trafic réseau. Cela est essentiel pour comprendre les mécanismes de fonctionnement des protocoles de communication sur les réseaux contemporains. Il capture des paquets **directement sur les interfaces** du système utilisé ou de lire des fichiers de captures sauvegardées. Il supporte les formats de fichiers de capture les plus courants. Bien sûr, seules les **connexions non chiffrées** pourront être analysées.

1. Prérequis

On a besoin de différents matériels et logiciels pour la capture d'un trafic réseau

- Un PC client sous Windows ou Linux
- Le logiciel Wireshark installé
- La ligne de commande et la commande nslookup
- Les droits Administrateur
- Connaître le modèle O.S.I
- Connaître les différents protocoles réseau

2. Les protocoles supportés

La liste des protocoles supportés par Wireshark évolue de façon continue depuis de nombreuses années. On peut accéder au catalogue soit en consultant la page **Protocol Reference** qui fournit un classement par famille de tous les protocoles.

3. Droits d'accès aux interfaces via Wireshark

Lorsque l'on exécute W**ireshark** en tant q**u'utilisateur normal**, on **ne peut accéder** à la liste des **interfaces** en lançant l'opération **Capture**. Sur un système d'exploitation correctement administré, un utilisateur normal ne doit pas avoir accès aux interfaces sans conditions.
Pour exécuter Wireshark en mode Administrateur, suivre les étapes ci-dessous :

a) Donner les droits Administrateur sous **Windows**

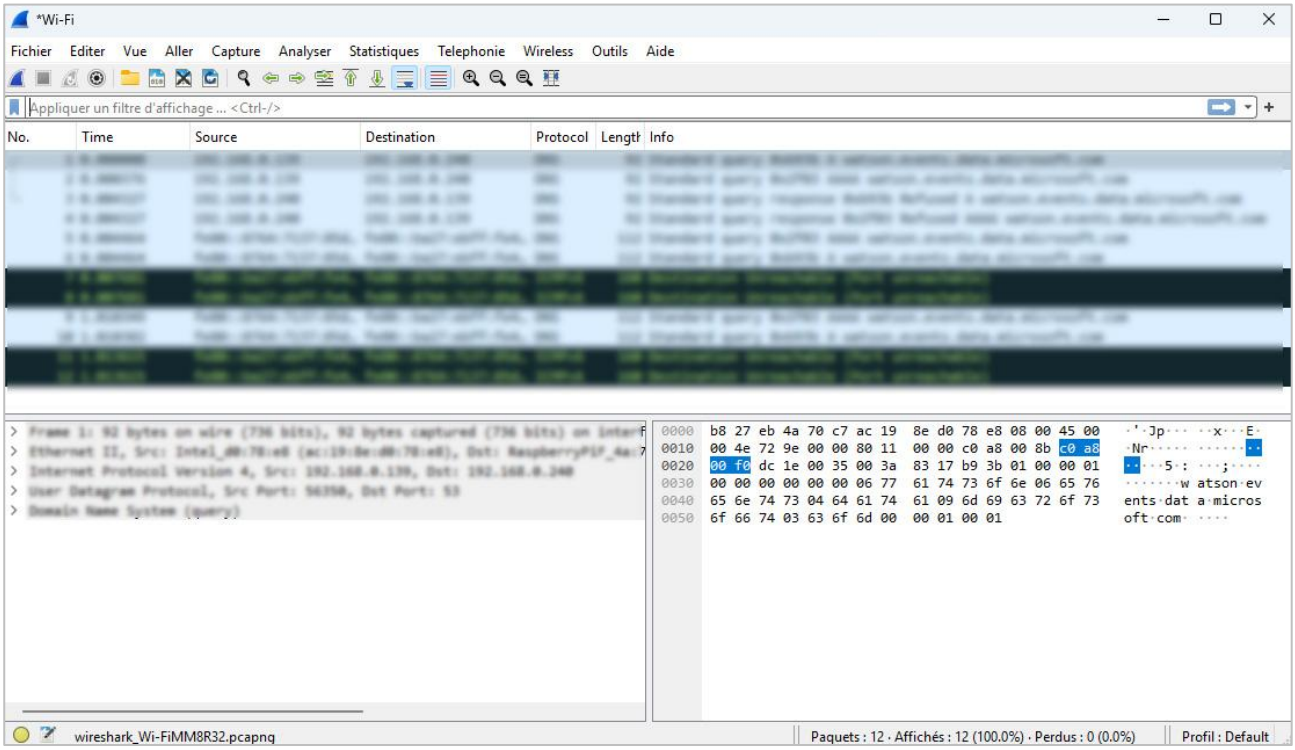
- Exécuter Wireshark en mode administrateur
- Saisir les identifiants Administrateur

b) Donner les droits Administrateur sous **Linux**

```
# sudo dpkg-reconfigure wireshark-common
# sudo adduser $USER wireshark
# sudo groupadd wireshark
# sudo usermod -a -G wireshark $USER
# sudo chgrp wireshark /usr/bin/dumpcap
# sudo chmod o-rx /usr/bin/dumpcap
# sudo setcap cap_net_raw,cap_net_admin=eip /usr/bin/dumpcap
# sudo getcap /usr/bin/dumpcap
```

4. L'interface de Wireshark

Wireshark se décompose en plusieurs parties distinctes permettant une capture précise. Voici une capture d'écran, ainsi qu'une brève description des outils.



a) Le menu

Il permet d'accéder aux différentes fonctionnalités de **Wireshark**

b) Les icônes

Les icônes sont des raccourcis se trouvant sur la barre, pour manipuler une capture

c) Les filtres de capture

Ils permettent le filtrage de la capture via une liste prédéfinie ou la saisie d'une l'expression de filtrage à posteriori d'une capture pour isoler tout ou partie d'un échange réseau.

d) La fenêtre des trames capturées

- Le numéro du paquet
- Le temps de capture
- La source
- La destination
- Le protocole de plus haut niveau décodé
- Le résumé des champs caractéristiques du protocole

e) La fenêtre de la pile des protocoles décodés pour la trame sélectionnée

Ligne	Niveau	Description
1	Frame	Quantité de bits capturés et la date de la capture
2	Liaison	Type et champs de la trame et les adresses physiques
3	Réseau	Détails des champs du protocole réseau reconnu
4	Transport	Détails les champs du protocole transport reconnu
5	Application	Détails des données utilisateurs

Pour le développement de chacun des champs de la trame, il faut cliquer sur le triangle situé à gauche au niveau de chaque couche.

5. Réaliser une capture de série de trame

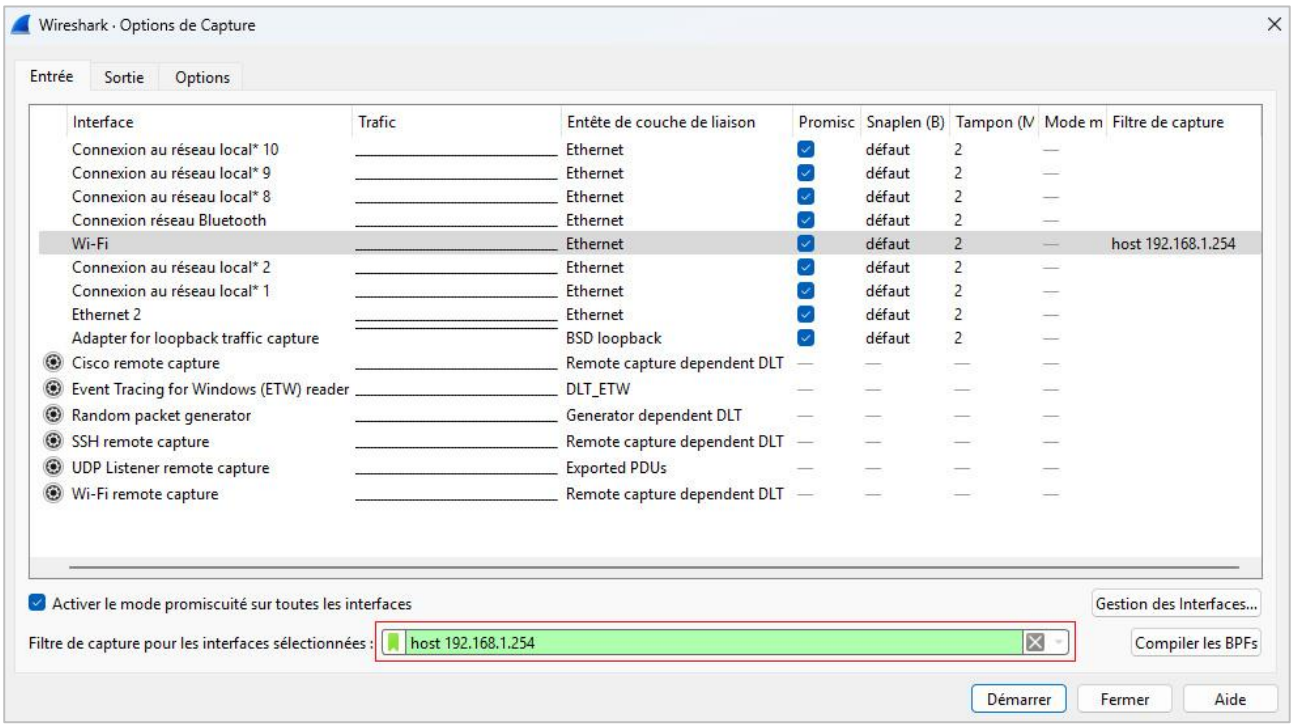
Après avoir lancer Wireshark en mode Administrateur, il faut :

a) Sélectionner le menu **Capture/Options**
b) Sélectionner l'interface réseau souhaité (Wi-Fi, Ethernet, eno1, eth0…)
c) Cliquer sur le bouton **Démarrer**

6a. Les filtres de capture

Les filtres de capture permettent comme le nom l'indique de filtrer les flux de capture en entrée afin de voir seulement le trafic qui nous intéressent, pour ensuite l'analyser plus facilement, car la capture sera épurée.

a) Sélectionner le menu **Capture/Options**
b) Sélectionner l'interface réseau souhaité (Wi-Fi, Ethernet, eno1, eth0…)
c) Saisir un filtre dans le champ **Filtre de capture pour les interfaces sélectionnées**
d) Cliquer sur le bouton **Démarrer**



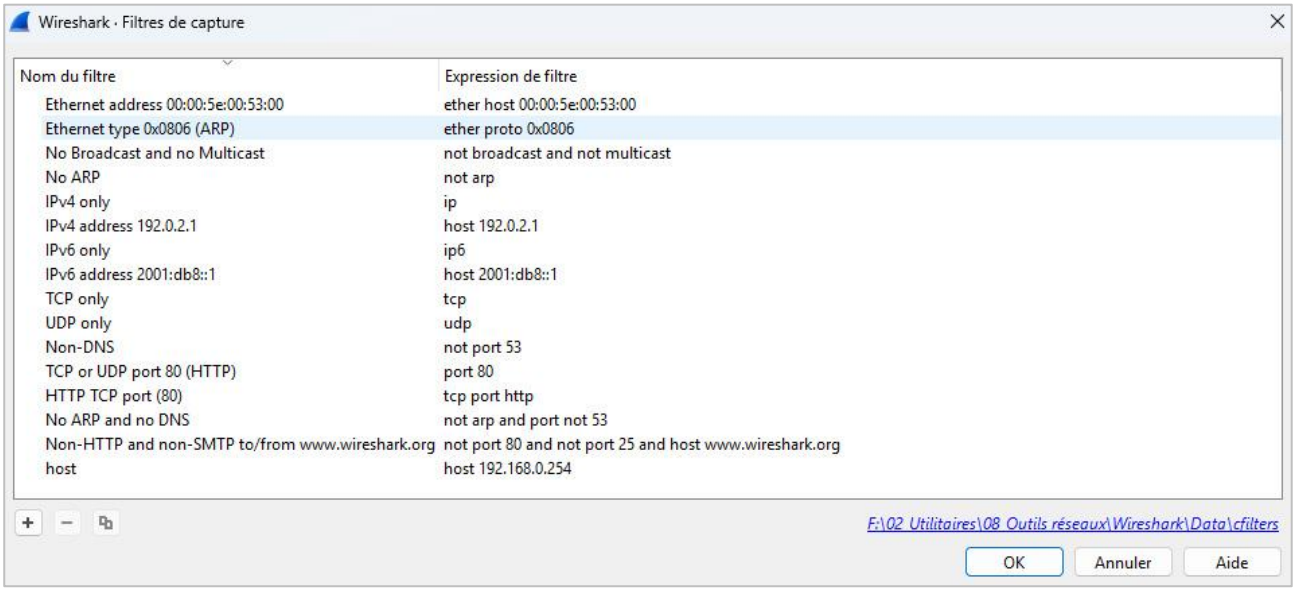
6b. Liste de quelques filtres de capture

Filtres de captures	**Exemples**
Sur une adresse IP	host == 192.168.0.254
Sur un réseau	net == 192.168.0.0/24
Sur un vlan	vlan 55
Sur une adresse MAC	ether host 00:00:5e:00:53:00
Sur le trafic HTTPS	tcp port 443
Sur le protocole QUIC	udp port 443
Le protocole OSPF	ip proto ospf
Exclure le trafic Broadcast	not broadcast

6c. Sauvegarder les filtres de capture

Wireshark donne la possibilité de sauvegarder les filtres, en vue d'une restauration. Pour sauvegarder les filtres, il faut :

a) Sélectionner le menu **Capture/Options**
b) Saisir un filtre dans le champ **Filtre de capture pour les interfaces sélectionnées**
c) Cliquer sur le **signet** pour afficher le menu contextuel
d) Cliquer sur le menu **Sauvegarder ce filtre**
e) Cliquer sur le chemin en bas de la fenêtre pour ouvrir le fichier



f) Enregistrer le fichier dans un dossier de sauvegarde

6d. Restaurer les filtres de capture

Pour restaurer les filtres, il suffit simplement de copier le fichier sauvegardé dans notre le dossier **CFILTERS** de Wireshark :

a) Windows : **c:\User\nomutilisateur\appData\Romaing\wireshark\cfilters**
b) Linux : **/root/config/wireshark/cfilters**

6e. Vérifier la syntaxe d'un filtre de capture

La syntaxe correcte d'un filtre de capture s'affiche en vert. Si cette syntaxe s'affiche en rouge, il y a une erreur dans la saisie.

7a. Les filtres d'affichage

Les filtres d'affichage s'utilisent sur une capture existante. On peut sélectionner un filtre existant ou en créer un en le saisissant. Ces filtres permettent plusieurs choses :

- Vérifier la présence d'un protocole
- Vérifier un champ ou une valeur
- Utiliser pour les règles de coloriage
- Utiliser pour construire un graphique via "I/O graph"

Il faut savoir que l'ensemble des protocoles et des champs inclus à Wireshark peuvent être utilisés en tant que filtre d'affichage. Par ailleurs, la **syntaxe** entre les filtres de capture et les filtres d'affichage **n'est pas identique**, et on peut **modifier à la volée** les filtres d'affichage contrairement aux filtres de capture qui sont lancés avant de prendre une capture réseau.

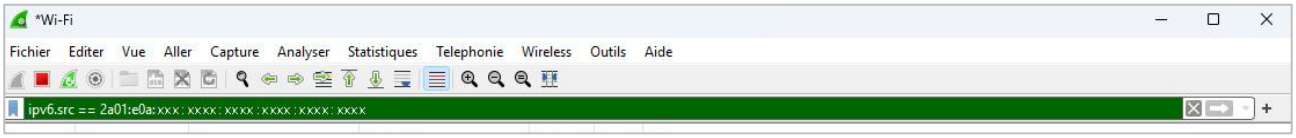
a) Cliquer sur l'icône des filtres
b) Sélectionner un protocole **(ex : http)** dans la liste
c) Cliquer sur le bouton **Démarrer**
d) Ouvrir une page Web
e) Cliquer sur le bouton **Stop** et analyser les trames

7b. Liste de quelques filtres d'affichage

Filtres de captures	**Exemples**
Sur une adresse MAC	eth.addr == 00:00:5e:00:53:00
Sur une adresse IP	ip == 192.168.1.254
Sur une URL	http.request.uri == gdidees.eu
Le protocole ICMP	icmp
Sur le DNS	dns (travaille le **port 53** sur tous les réseaux)
Sur le mDNS	mdns (travaille le **port 5353** sur le réseau local)

7c. Enregistrer un filtre d'affichage provenant d'une trame

a) Cliquer avec le bouton droit sur **le champ** dans les détails du paquet
b) Sélectionner le menu **Appliquer comme un filtre/Sélectionné**
c) Le filtre doit apparaitre en vert dans le champ des filtres d'affichage
d) Cliquer sur le signet en couleur



e) Dans le menu contextuel, cliquer sur le menu **Sauvegarder ce filtre**

7d. Restaurer les filtres d'affichage

Les filtres d'affichage s'enregistrent automatiquement dans un fichier. Pour les restaurer, il suffit simplement de copier le fichier sauvegardé dans notre le dossier **DFILTERS** de Wireshark :

a) Windows : **c:\User\nomutilisateur\appData\Roaming\wireshark\dfilters**
b) Linux : **/root/config/wireshark/dfilters**

7e. Vérifier la syntaxe d'un filtre d'affichage

La syntaxe correcte d'un filtre d'affichage s'affiche en vert. Si cette syntaxe s'affiche en rouge, il y a une erreur dans la saisie.

8. Nslookup et le protocole DNS

Liste des requêtes DNS à utiliser en ligne de commandes avec l'outil **nslookup**. Elles permettent de trouver les informations nécessaires au filtrage via Wireshark, tel que l'@IP d'un domaine…

Requête	**Description**
A	Associe un nom d'hôte à une adresse IPv4 32 bits
AAAA	Association un nom d'hôte à une adresse IPv6 128 bits
CNAME	Nom canonique : associe un nom d'alias au nom de domaine réel ou canonique
MX	Échange de courrier : associe un nom de domaine à une liste d'agents de transfert de messages pour ce domaine
NS	Serveur de noms : spécifie un serveur DNS faisant autorité pour le domaine
PTR	Pointeur : associe une adresse IPv4 au CNAME de l'hôte
SOA	Début d'autorité : spécifie les informations faisant autorité sur une zone DNS
SRV	Localisateur de services : spécifie l'emplacement des services (tels que VoIP ou IMAP) pour le domaine
TXT	Texte : permet aux administrateurs d'insérer du texte arbitraire dans un enregistrement DNS
DNSKEY	Clé DNS : utilisée par DNSSEC pour signer les enregistrements DNS

a) Chercher l'**@IP** utilisée par le site web (**gdidees**)

```
nslookup
> set type=A
> gdidees.eu
```

Résultat

```
Serveur :   UnKnown
Address:  192.168.1.254
Réponse ne faisant pas autorité :
Nom :    gdidees.eu
Address:  213.186.33.87
```

b) Chercher le **nom du Serveur DNS** utilisé par le site web (**gdidees**)

```
nslookup
> set type=NS
> gdidees.eu
```

Résultat

```
Serveur :   UnKnown
Address:  192.168.1.254
Réponse ne faisant pas autorité :
gdidees.eu      nameserver = dns103.ovh.net
gdidees.eu      nameserver = ns103.ovh.net
```

c) Chercher L'**@IP du Serveur DNS utilisé** par le site web (**gdidees**)

```
nslookup
> set type=A
> dns103.ovh.net
```

Résultat

```
Serveur :   UnKnown
Address:  192.168.1.254
Réponse ne faisant pas autorité :
Nom : dns103.ovh.net
Address : 213.251.188.147
```

d) Connaître les **serveurs racines**

Les serveurs racines suivent une hiérarchie. Ils sont au sommet de cette hiérarchie. Ils gèrent les serveurs DNS de premier niveau tel que (com, fr, eu, edu, gov, us...). Pour connaitre le domaine DNS d'un site fr, ils interrogent les serveurs de premier niveau. Cliquer sur Root Servers Zone Dns pour afficher la page web du site.

e) Chercher l'**@IP d'un hébergeur** (@Ip relevé sur le site des serveurs racines)

```
nslookup
> server 198.41.0.4 (définit le serveur racine a utilisé par défaut)
> gdidees.eu
```

Résultat

```
Nom :    gdidees.eu
Served by:
 - be.dns.eu
      149.38.1.26
      eu
 - x.dns.eu
      185.151.141.1
      2a02:568:fe00::6575
      eu
 - y.dns.eu
      194.146.106.90
      2001:67c:1010:23::53
      Eu
```

f) Chercher l'**@IP du dns103.ovh.net**

```
nslookup
> server 149.38.1.26 (définit le serveur de premier niveau a utilisé par défaut)
> dns103.ovh.net
```

Résultat

```
in-addr.arpa    nameserver = f.in-addr-servers.arpa
in-addr.arpa    nameserver = b.in-addr-servers.arpa
in-addr.arpa    nameserver = d.in-addr-servers.arpa
in-addr.arpa    nameserver = a.in-addr-servers.arpa
f.in-addr-servers.arpa  internet address = 193.0.9.1
f.in-addr-servers.arpa  AAAA IPv6 address = 2001:67c:e0::1
d.in-addr-servers.arpa  internet address = 200.10.60.53
d.in-addr-servers.arpa  AAAA IPv6 address = 2001:13c7:7010::53
a.in-addr-servers.arpa  internet address = 199.180.182.53
a.in-addr-servers.arpa  AAAA IPv6 address = 2620:37:e000::53
Serveur par défaut :        [149.38.1.26]
Address :           149.38.1.26
```

g) Chercher le **nom du serveur dns** utilisé par le site web (**gdidees**)

```
nslookup
> server 149.38.1.26 (définit le serveur de premier niveau a utilisé par défaut)
> gdidees
```

Résultat

```
Nom :    gdidees.eu
Served by:
  - ns103.ovh.net
      gdidees.eu
  - dns103.ovh.bet
      gdidees.eu
```

9. Capture de trame avec les valeurs trouver avec nslookup

On peut maintenant faire une capture de Trame avec l'adresse IP du dns de l'hébergeur site dns103.ovh.net avec le filtre suivant :

```
Ip==149.38.1.26
```

10. Liens annexes

Liste de contenu à consulter

- Serveurs racines : https://www.iana.org/domains/root/servers
- Liste de filtres d'affichage : https://www.tutos.eu/5645
- Protocole de référence : https://wiki.wireshark.org/ProtocolReference
- Wireshark découverte : https://blog.alphorm.com/decouverte-wireshark
- Aide-mémoire : https://3donline.be/wireshark-cheat-sheet-commands-captures-filters-shortcuts

11. Conclusion

Wireshark est un outil incontournable pour l'analyse de réseaux, offrant une multitude de fonctionnalités pour explorer et dépanner efficacement.

Pour télécharger Wireshark cliquer sur le lien : https://www.wireshark.org/download.html