Guide d'utilisation de l'analyseur de réseau Wireshark

Anthony Juton – décembre 2019

Wireshark est l'outil d'analyse réseau le plus répandu pour comprendre et diagnostiquer les réseaux IP. Il fonctionne sur tous les systèmes d'exploitation PC. Il est open source.

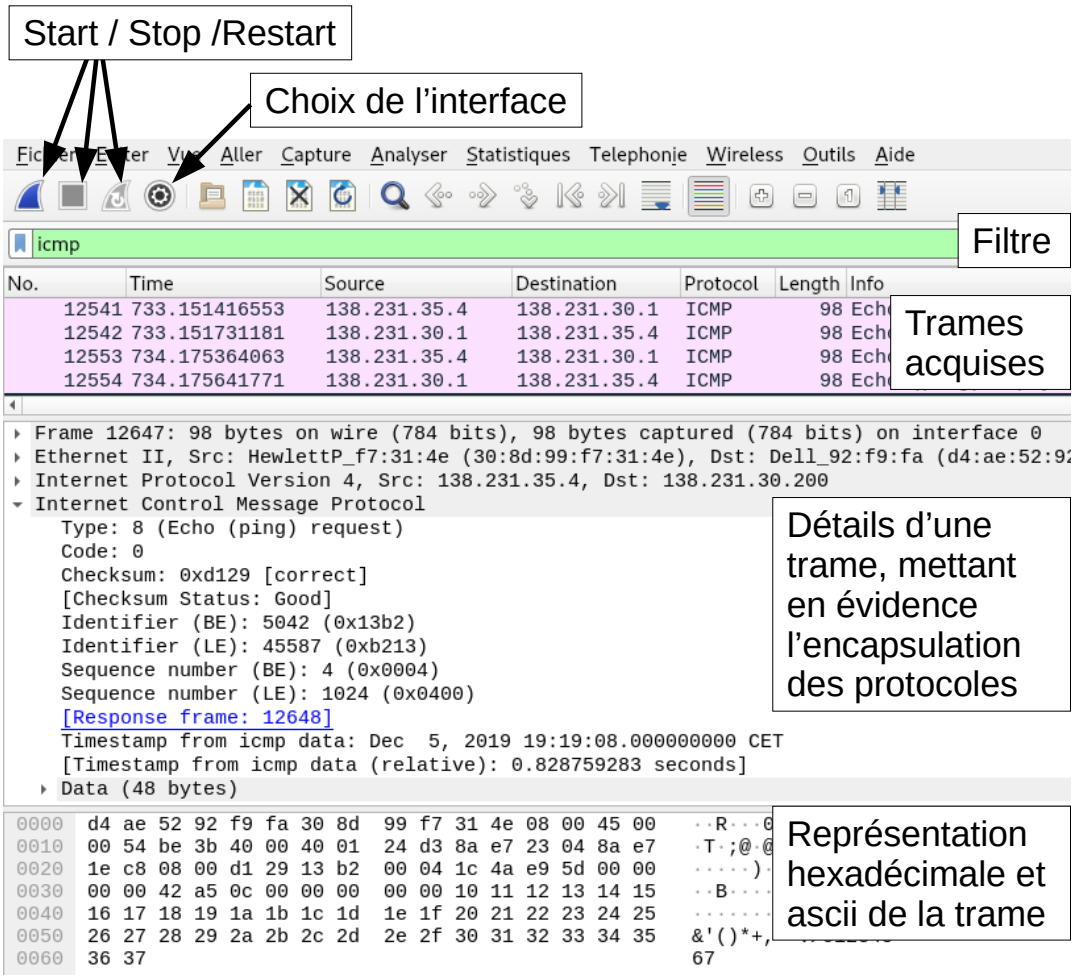
Wireshark lit les trames arrivant sur les cartes réseau (Ethernet ou Wifi mais aussi bluetooth et USB) et les formate de manière lisible pour l'utilisateur. Des connaissances de base en réseaux permettent alors de lire le contenu des trames.

La grande quantité de données demande d'utiliser des filtres (de capture ou d'affichage) adéquat pour les exploiter.

Enfin Wireshark propose des outils d'analyse de données.

L'essentiel des informations suivantes sont issues du user guide de wireshark, disponible sur le site web de l'organisation, tout comme le téléchargement du logiciel : https://www.wireshark.org/

1. L'interface utilisateur



1.1. Le menu

- Dans le menu *Fichier*, on trouve notamment de quoi enregistrer ou ouvrir la sauvegarde d'une capture. Il est possible d'exporter au format csv.
- Dans le menu *Edition*, on trouve notamment *Trouver un paquet*, fonction très pratique pour recherche un paquet avec juste un élément de texte du paquet par exemple,
- Dans le menu *Vue*, on trouve *Format d'Affichage et de l'Heure* qui permet d'afficher l'heure et le date de réception d'un paquet et *Colorize conversation*, bien utile quand on veut suivre des échanges, parmi d'autres,
- Dans le menu *Analyser*, on trouve la fonction *Follow TCP Stream*, pour suivre le flux TCP lors d'un échange (idem en UDP et même HTTP),
- Les fonctions du menu *Statistiques* permettent d'utiliser d'autres formats d'affichage pour mettre en relief tel ou tel protocole.

1.2. La barre d'outils

Les 4 premières icônes permettent

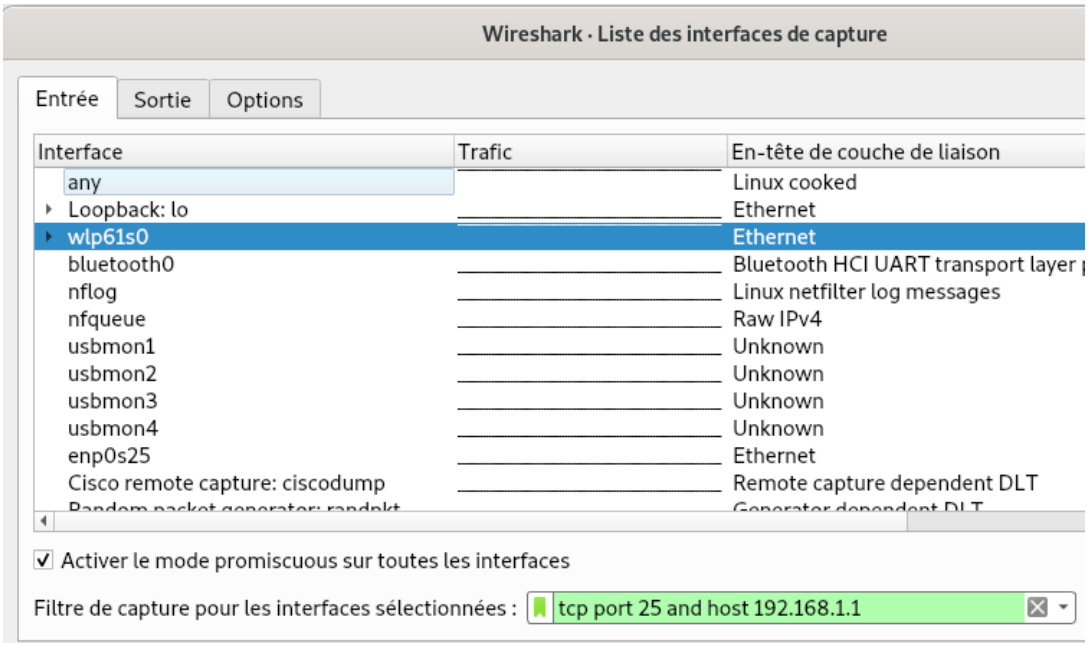
-  le démarrage,
-  l'arrêt,
-  le redémarrage,
-  le choix de l'interface réseau (Options de capture)

1.3. La liste des paquets

La liste des trames acquises utilise un jeu de symbole dans la marge :

2. La capture

L'icône Options de capture  permet de choisir l'interface réseau utilisée pour l'acquisition. Sous linux les cartes ethernet physiques se nomment ethx ou, plus moderne, enspxxx. Les cartes wifi se nomment wlpxxx.



On notera qu'il est possible d'analyser le trafic du port usb.

Il est également possible dans cette fenêtre d'ajouter des filtres de capture, qui vont sélectionner ou non les paquets acquis. Ces filtres sont écrit dans le format libpcap du module d'acquisition. Voici quelques exemples :

- host 172.18.5.4 (sélection d'une machine)
- net 192.168.0.0/24 (sélection d'un réseau)
- `port 53` `(sélection d'un port)`
- `host www.example.com and not (port 80 or port 25)`
- `vlan and (host 192.168.0.0 and port 80)`
- `tcp port 23 and not src host 10.0.0.5`

3. Les filtres d'affichage

Une fois les paquets acquis, des outils permettent de les analyser.

3.1. Affichage dans une nouvelle fenêtre

Un clic droit sur un paquet permet de demander *Affiche paquet dans une nouvelle fenêtre*.

3.2. Création rapide d'un filtre adresse IP

Il est possible de cliquer droit sur une adresse IP pour l'ajouter en filtrage : Clic droit sur une IP dans la liste des paquets ou dans le détail d'un paquet puis *Appliquer comme un filtre*.

Dans ce menu contextuel, il est aussi possible d'appeler la fonction *Colorier la conversation*.

3.3. Filtres d'affichage communs

Voici quelques exemples de filtres utiles :

- tcp
- udp
- dns
- bootp (bootp étant l'ancêtre de dhcp, ce filtre permet d'afficher les paquets DHCP)
- `tcp.port eq 25 or icmp`
- `ip.src==192.168.0.0/16 and ip.dst==192.168.0.0/16`
- eth.addr[0:3]==00:06:5B (permet de sélectonner les machines DELL)
- `udp contains 81:60:03`

3.4. L'aide à la génération de filtres d'affichage

Il est possible d'utiliser l'outil *Expression de Filtre* pour générer le filtre souhaité.