



Documentation D'Exploitation



Table des matières

- 1. Définitions**
- 2. Prérequis**
- 3. Installation**
- 4. Fonctionnement**
- 5. Fonctionnalités**

1. Définition

Wireshark est un analyseur de protocole réseau gratuit et open source qui permet aux utilisateurs de parcourir de manière interactive le trafic de données sur un réseau informatique. Le projet de développement a été lancé sous le nom d'Ethereal, mais a été renommé Wireshark en 2006.

De nombreux développeurs de réseaux du monde entier ont contribué à ce projet avec l'analyse de réseau, le dépannage, le développement de logiciels et les protocoles de communication. Wireshark est utilisé dans de nombreux établissements d'enseignement et autres secteurs industriels.

2. Prérequis

La quantité de ressources requise par Wireshark dépend de votre environnement et de la taille du fichier de capture que vous analysez. Les valeurs ci-dessous devraient être adaptées pour les fichiers de capture de petite à moyenne taille de quelques centaines de Mo. Les fichiers de capture plus importants nécessiteront plus de mémoire et d'espace disque.

Les réseaux occupés signifient de grandes captures

Travailler avec un réseau occupé peut facilement produire d'énormes fichiers de capture. La capture sur un réseau gigabit ou même 100 mégabits peut produire des centaines de mégaoctets de données de

capture en peu de temps. Un processeur rapide, beaucoup de mémoire et d'espace disque est toujours une bonne idée.

Bien que Wireshark capture des paquets en utilisant un processus distinct, l'interface principale est simple et ne bénéficiera pas beaucoup des systèmes multi-core.

Microsoft Windows

- Les versions de Wireshark supportent les versions de Windows avec **extended support lifetime** : Windows 10, 8, 7, Vista, Server 2016, Server 2012 R2, Server 2012, Server 2008 R2, and Server 2008.
- Processeur 64-bit AMD64/x86-64 or 32-bit x86 processor.
- 400 MB RAM disponible. Des fichiers de captures important nécessitent plus de RAM.
- 300 MB d'espace disque pour l'installation.
- Graphique 1024×768 (1280×1024 or ou plus recommandé) resolution en couleur 16 bits.
- Une carte réseau (NIC) supportée.
 - Ethernet. N'importe quelle carte devrait être fonctionnelle. Voir **Ethernet et Offloading** en cas problèmes.
 - 802.11. Capturer du trafic réseau Wi-Fi sans matériel adapté peut être difficile sous Windows : [Wireshark wiki page](#). Capturing raw 802.11 information may be difficult without special equipment.
 - Autres supports. Voir **NetworkMedia**.

UNIX / Linux

Wireshark fonctionne sur la plupart des systèmes UNIX, UNIX-like comme par exemple macOS ou Linux. Les pré-requis systèmes sont identiques à ceux d'une installation Windows.

Les binaires d'installation sont mis à disposition pour les systèmes suivants :

Apple macOS

Debian GNU/Linux

FreeBSD

Gentoo Linux

HP-UX

Mandriva Linux

NetBSD

OpenPKG

Red Hat Enterprise/Fedora Linux

Sun Solaris/i386

Sun Solaris/SPARC

Canonical Ubuntu

3. Installation

Installation de Wireshark sous Windows


L'installateur Wireshark contient le type de système et sa version : Wireshark-win64-2.3.0.exe installe Wireshark 2.3.0 pour Windows 64-bit. L'installateur Wireshark installe le pilote Win cap indispensable aux captures.

Il faut se rendre sur le site de Wire Shark, puis cliquer sur sa version.

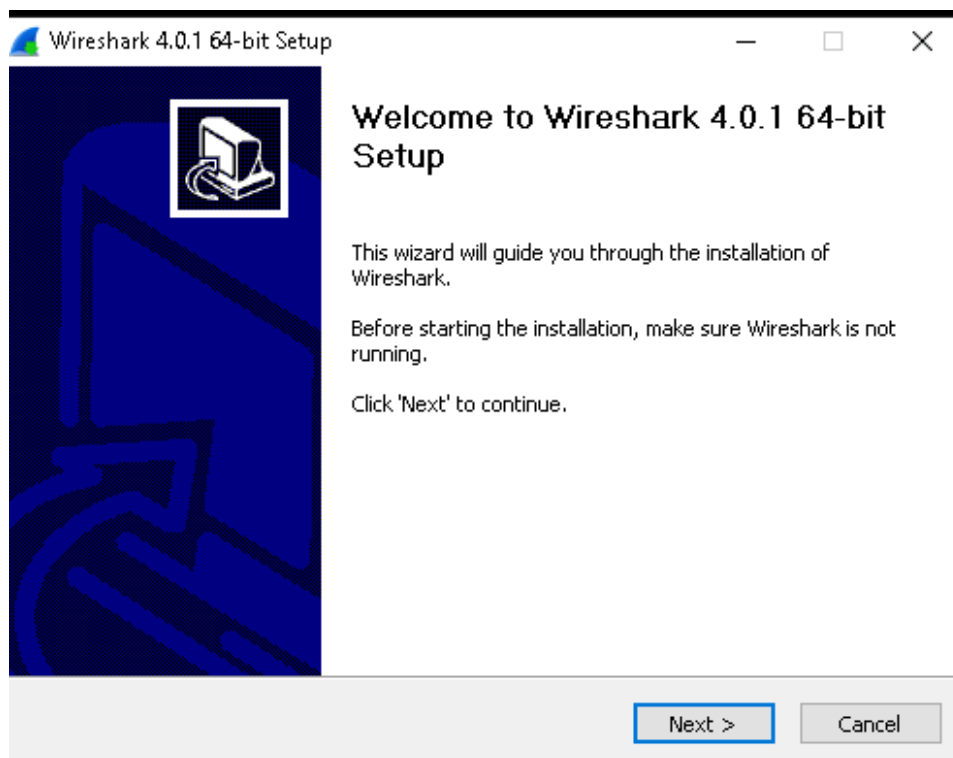
<https://www.wireshark.org/download.html>

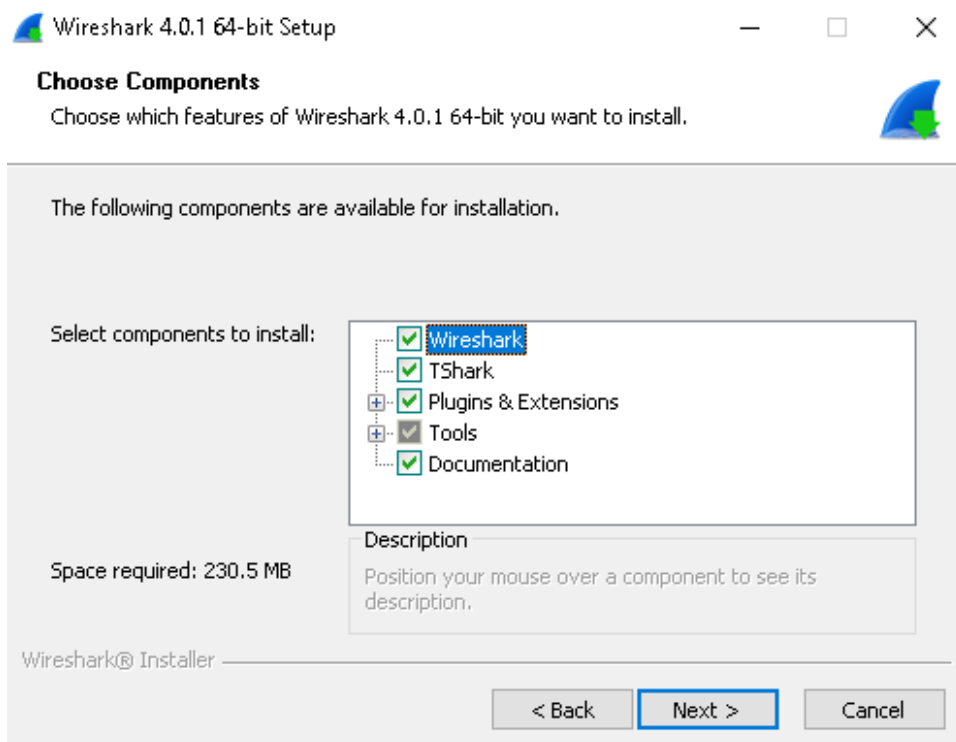
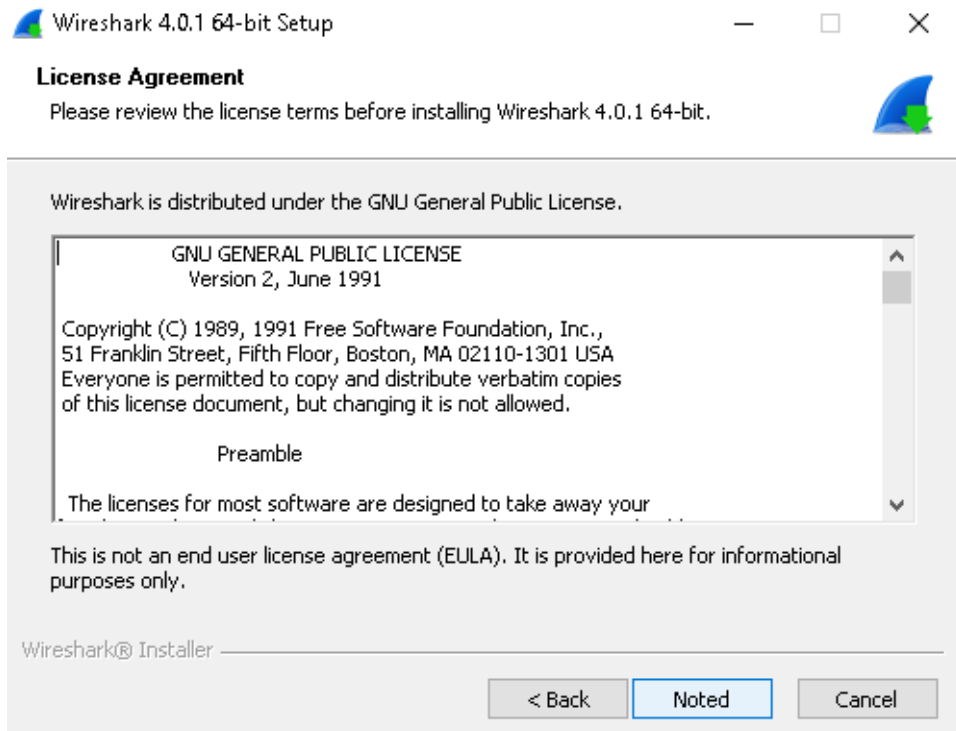
Download Wireshark

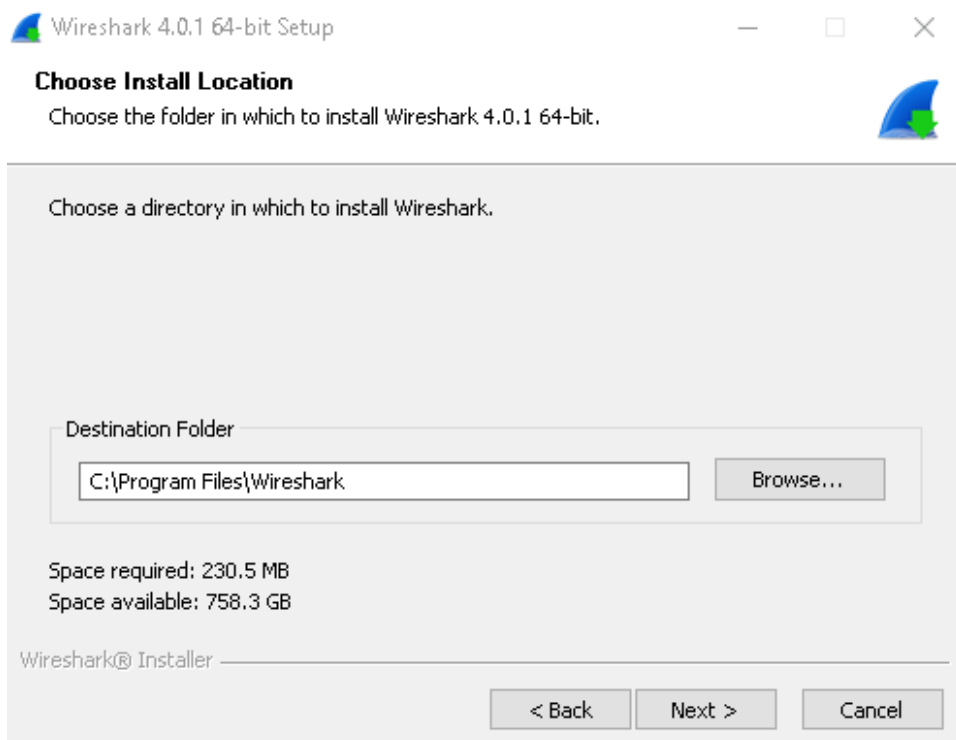
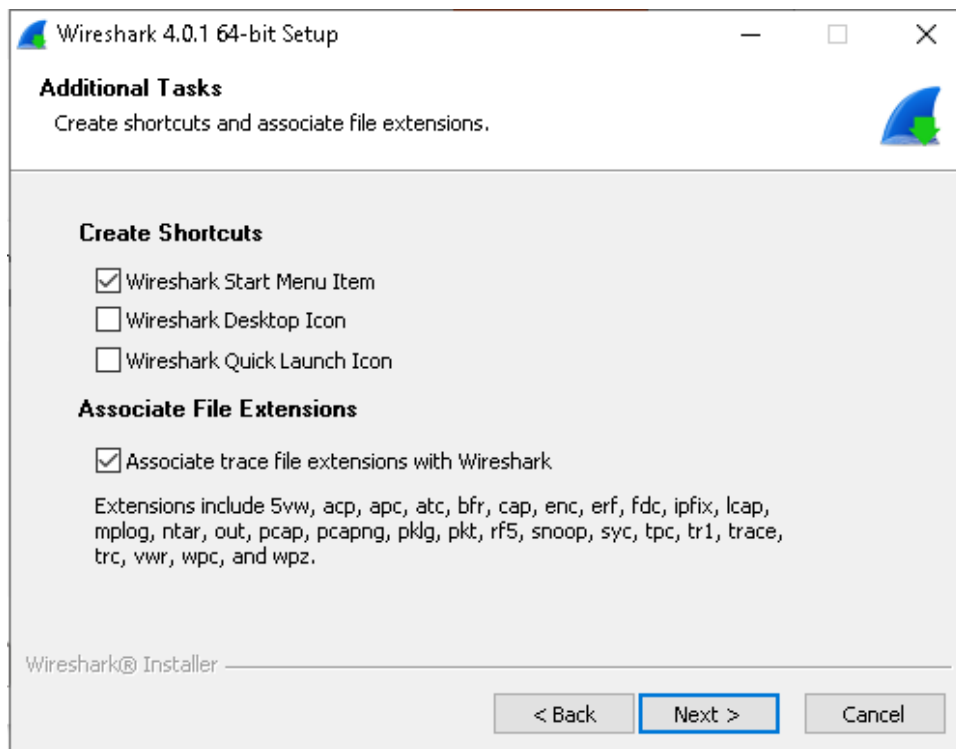
The current stable release of Wireshark is 4.0.1. It supersedes all previous releases.

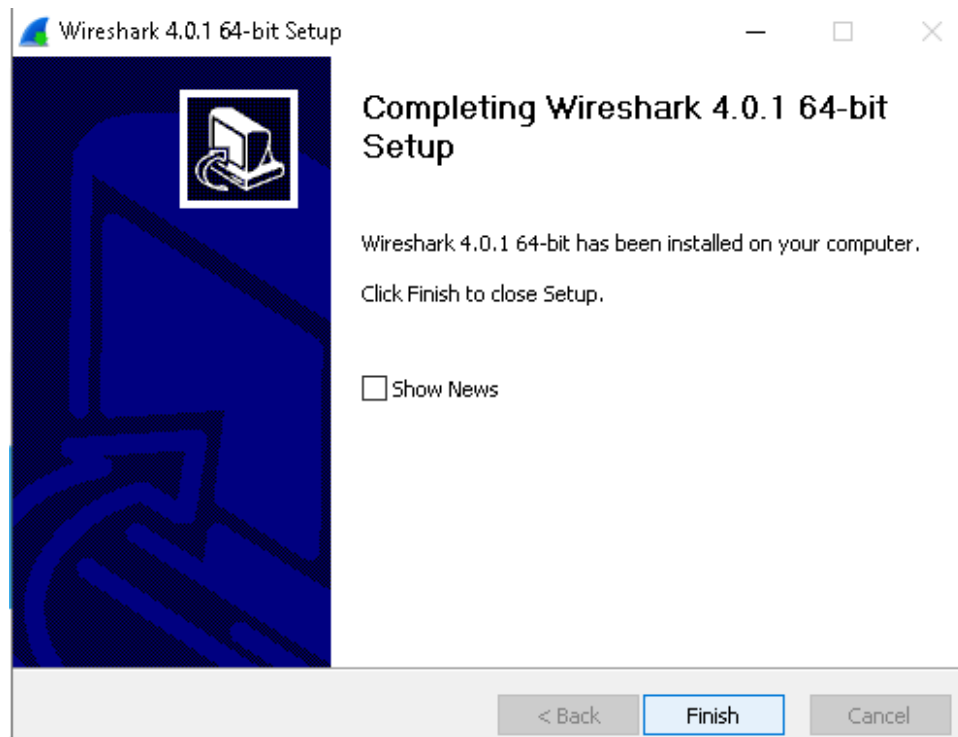
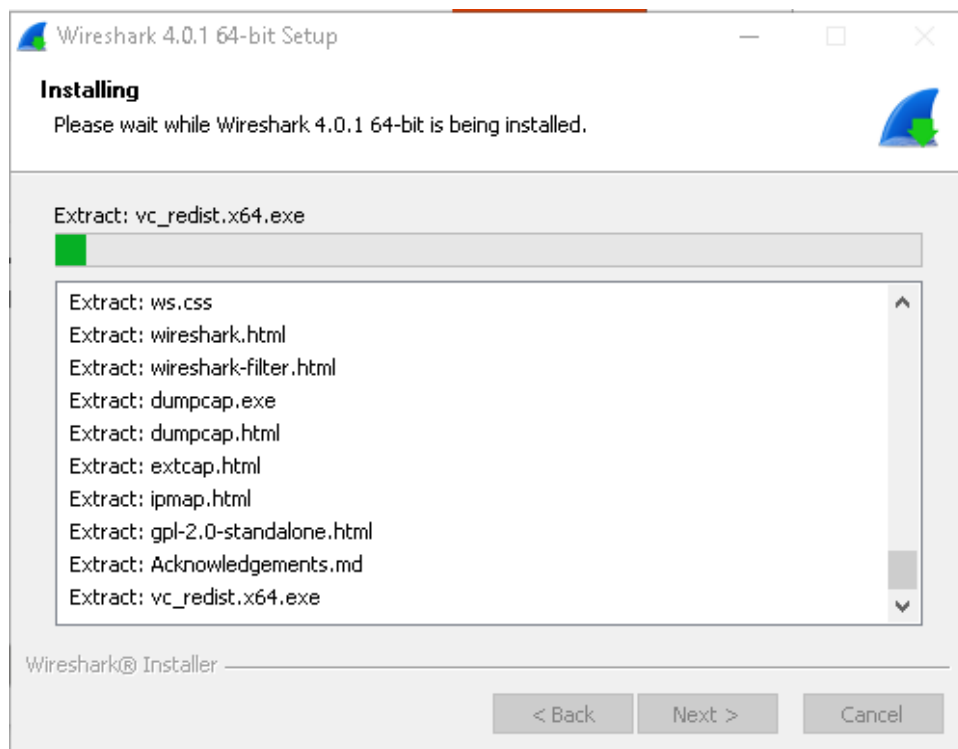
Stable Release (4.0.1)	^
 Windows Installer (64-bit) Windows PortableApps® (64-bit) macOS Arm 64-bit .dmg macOS Intel 64-bit .dmg Source Code	
Old Stable Release (3.6.9)	^
Documentation	^

Dans notre cas ça sera Windows installer. Puis il n'y aura qu'à suivre les étapes.





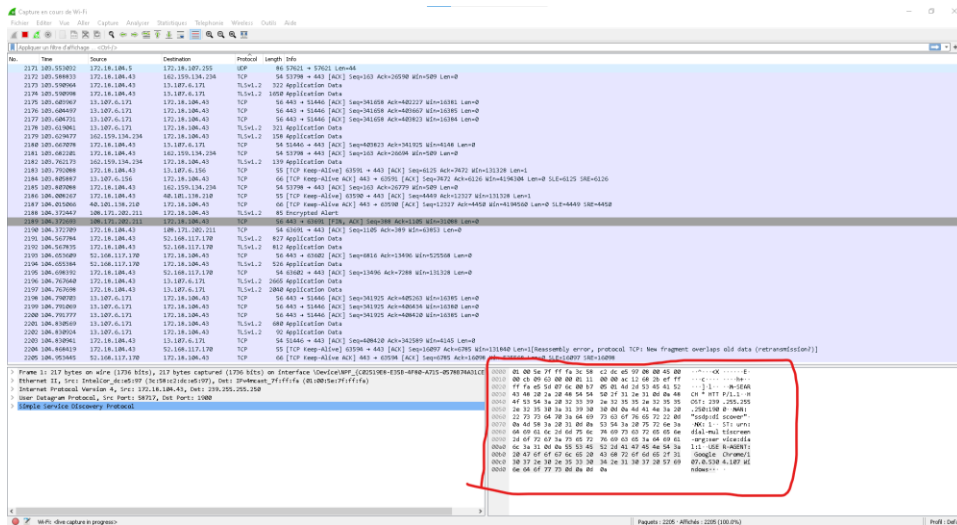
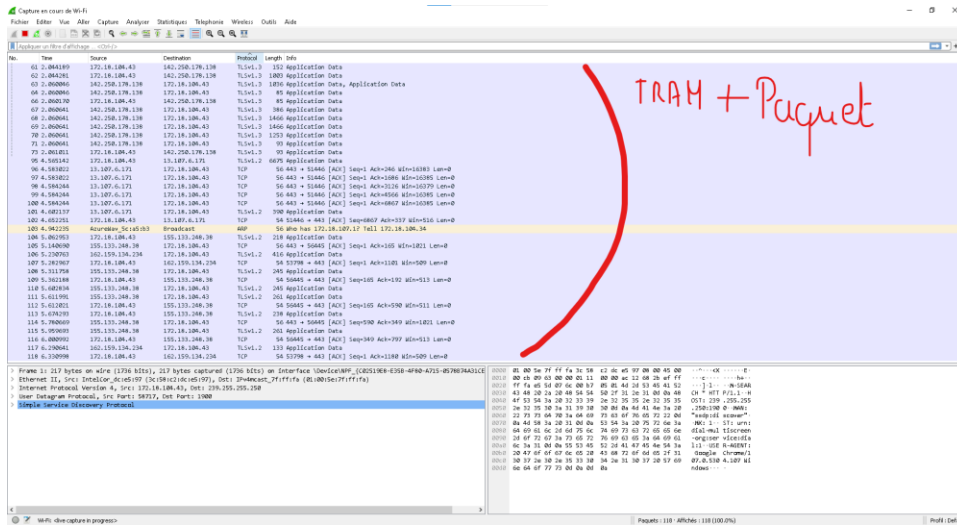




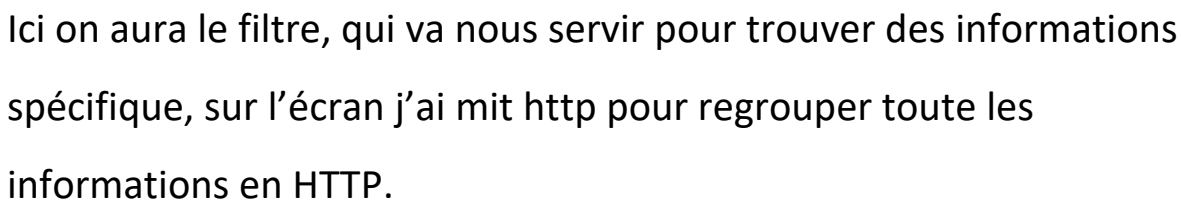
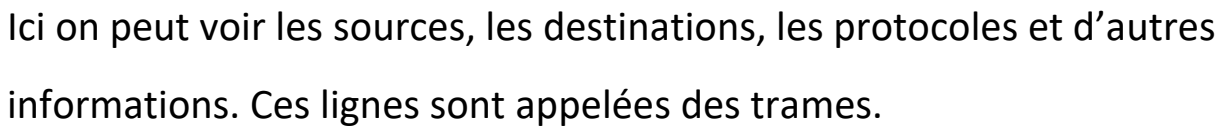
Et donc voila, wireshark est installé.

4. Fonctionnement

Wireshark est un outil de capture et d'analyse de paquets. Il capture le trafic du réseau local et stocke les données ainsi obtenues pour permettre leur analyse hors ligne. Wireshark est capable de capturer le trafic Ethernet, Bluetooth, sans fil (IEEE.802.11), Token Ring, Frame Relay et plus encore. *Remarque : un « paquet » est un message d'un protocole réseau (par ex., TCP, DNS, etc.). Le trafic du réseau local est basé sur le concept de diffusion, cela signifie qu'un seul ordinateur disposant de Wireshark peut visualiser le trafic reliant deux autres ordinateurs. Pour visualiser le trafic émis vers un site externe, vous devez capturer les paquets sur l'ordinateur local.* Wireshark vous permet de filtrer le journal avant le début de la capture ou pendant l'analyse. Il vous est ainsi possible d'éliminer le bruit pour trouver exactement ce que vous recherchez dans la trace réseau. Par exemple, vous pouvez définir un filtre qui n'affiche que le trafic TCP entre deux adresses IP. Vous pouvez également choisir de n'afficher que les paquets envoyés depuis un ordinateur précis. Si Wireshark est devenu une référence de l'analyse de paquets, c'est en grande partie grâce à ses filtres.



Ce qu'on voit ici c'est les paquets bruts, à l'intérieur il y aura les informations en hexadécimale de ce que nous pouvons voir à gauche, avec les destinations.



5. Fonctionnalités

Les fonctionnalités principales de Wireshark sont :

- Disponibles pour les systèmes *UNIX* et *Windows*.
- *Capturer* les packets de données en “live” qui passent en live sur les interfaces à partir de n’importe quel type de supports : Ethernet, Wi-Fi, Bluetooth, Frame-Relay, ATM, HDLC, USB, ...
Voir Network Media.
- *Ouvrir* des fichiers de captures de paquets réalisés avec Tc dump/Win Dump, Wireshark et bien d’autres programmes.
- *Importer* des paquets venant de fichiers texte contenant les charges en hexa de paquets de données.
- Display packets with *Very detailed Protocol information*.
- *Enregistrer* des paquets de données capturés.
- *Exporter* certains ou tous les paquets capturés dans différents formats.
- *Filtrer les paquets* sur base de différents critères.
- *Rechercher* des paquets sur base de différents critères.
- *Coloriser* des paquets sur base de différents critères.
- Créer différentes *statistiques*