



Région académique
AUVERGNE-RHÔNE-ALPES



Technologie, Sciences de l'Ingénieur et Techniques Industrielles

Wireshark

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

Gratuit

OS : Windows / Mac OS

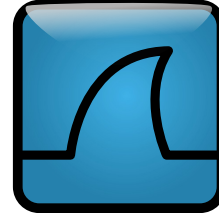
Niveau : Lycée

Point(s) positif(s) :

- Open-source
- Portable

Point(s) négatif(s) :

- En anglais



Présentation :

Wireshark est un analyseur de paquets libre et gratuit. Il est utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie.

Source [Wikipedia](#)

Utilisation :

Un exemple d'utilisation de Wireshark est la lecture et l'analyse de trame issu du protocole TCP/IP. Pour lire ("sniffer") les information échanger entre le pc et un autre hôte du réseau il faut :

- Lancer la lecture de trames (menu *Capture / Start*)
- Appliquer le filtre permettant de ne voir que les trames souhaitées :

IP.addr == adresse IP de l'autre hôte (valider avec Apply)

Les trames échangées apparaissent alors dans la fenêtre du logiciel, elles sont découpées en octets, eux même convertis en hexadécimal. Un affichage graphique permet aussi de repérer les différentes couches du protocole.

The screenshot shows the Wireshark interface with a packet capture from Intel(R) Gigabit Network Connection. The main pane displays a list of captured packets. A filter is applied: `Expression... Clear Apply Save`. A red arrow points to the filter bar with the annotation: "Filtre : permet de sélectionner les trames que l'on veut observer".

The packet list shows several packets, including ARP, DHCPv6, and TCP. A red arrow points to the selected packet (No. 11) with the annotation: "Liste des trames capturées".

The packet details pane shows the structure of the selected packet. A red arrow points to the "Ethernet II" section with the annotation: "Détails du protocole de la trame : permet de sélectionner la partie de la trame qui nous intéresse".

The packet bytes pane shows the raw data in hexadecimal and ASCII. A red arrow points to the hex data with the annotation: "Contenu de la trame : affiche les octets de la trames en hexadécimal(16 par lignes) et affiche à droite la conversion en ASCII".