UTILISATION DU LOGICIEL WIRESHARK

1 – PRESENTATION

Le logiciel **Wireshark** (anciennement Ethereal) est un logiciel libre **d'analyse de protocole**, ou « packet sniffer », utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie, mais aussi le piratage. Wireshark reconnait **759 protocoles**.

Attention : l'installation ou l'utilisation d'une application Analyseur de paquets peut constituer une violation de la politique de sécurité d'une organisation, qui peut entrainer de graves conséquences légales et financières. Il est donc recommandé d'obtenir les autorisations requises avant de télécharger, d'installer ou d'exécuter une application Analyseur de paquets.

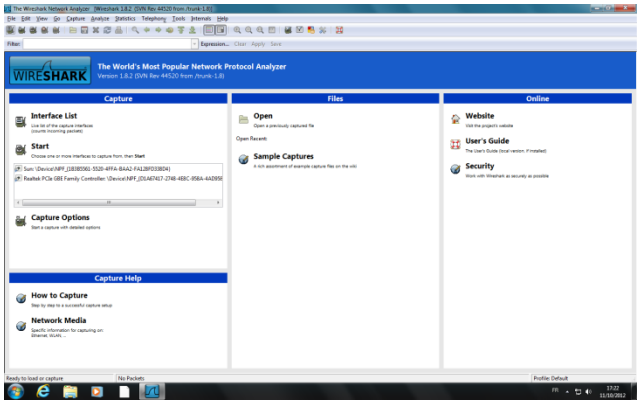
Site officiel : http://www.wireshark.org/
Documentation : http://www.wireshark.org/docs/wsug_html_chunked/index.html

2 – PRISE EN MAIN

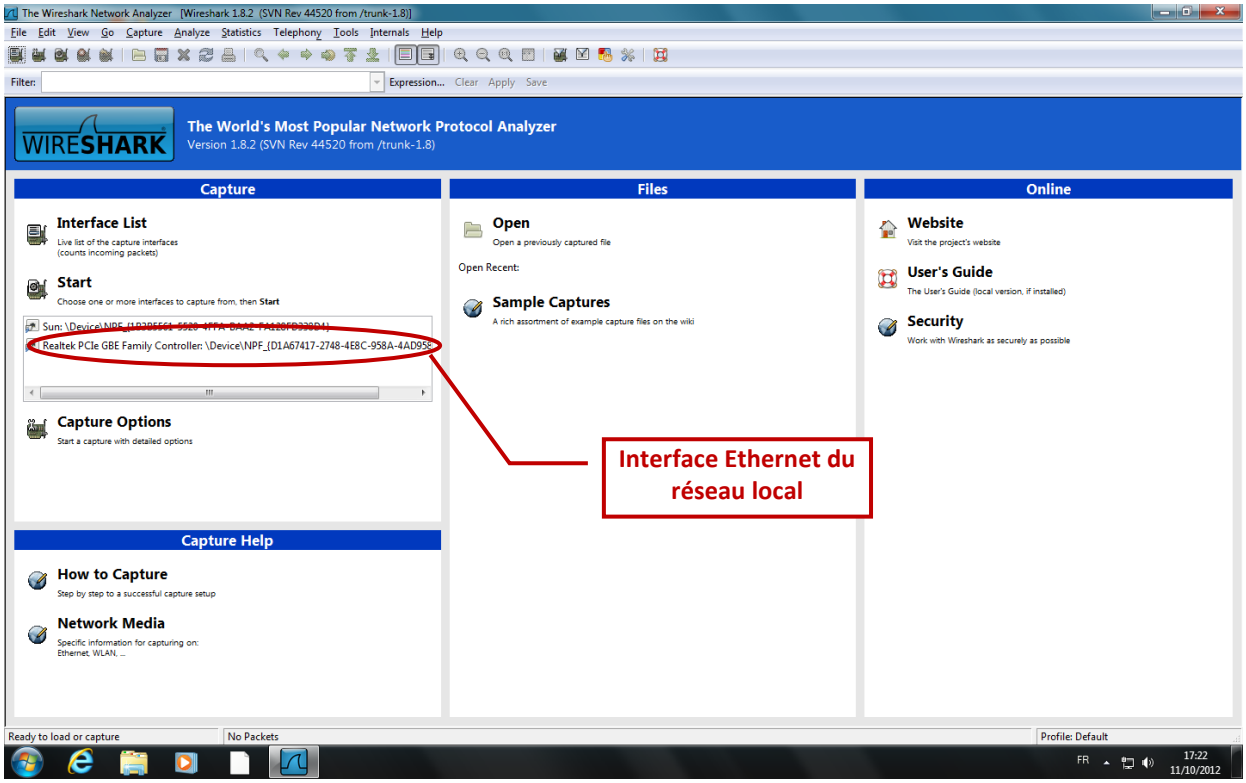
Étape 1 : lancement de Wireshark

Double-cliquer sur l'icône Wireshark sur le Bureau. 

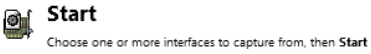
Le logiciel s'ouvre sur cette page de menu :



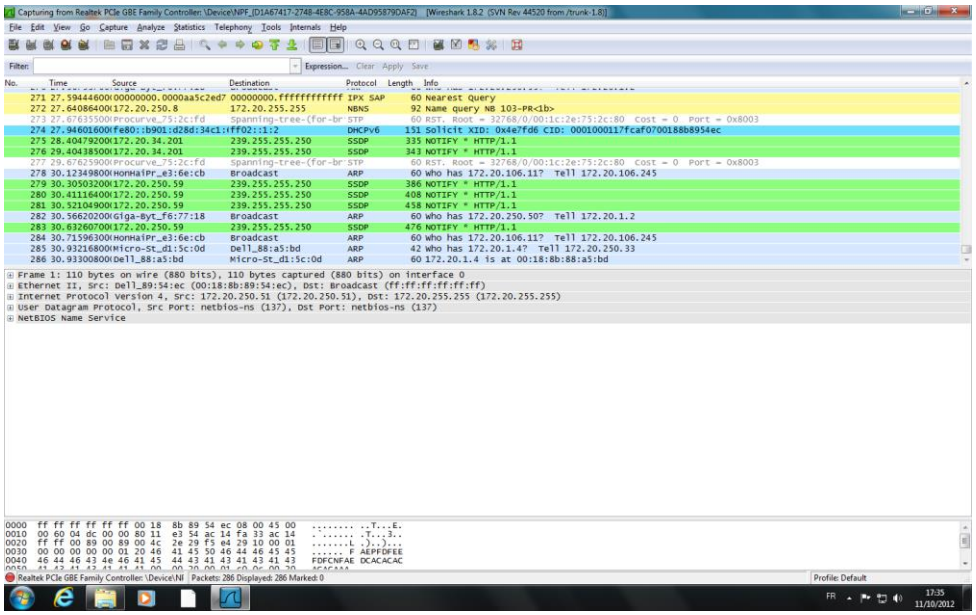
Étape 2 : capture réseau



a. **Choisir** l'interface Ethernet du réseau local pour la capture du trafic.

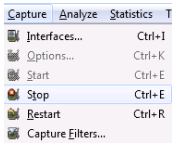
b. **Cliquer** sur le bouton Start. 

Les fenêtres de capture sont désormais actives. Dans la fenêtre Wireshark, on trouve des colonnes **Source, Destination** et **Protocol.**



c. **Stopper** la capture en cliquant sur 

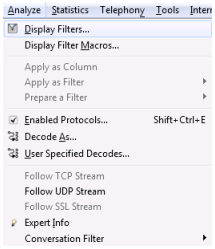
l'icône ou bien en cliquant sur *Stop* dans le menu *Capture*



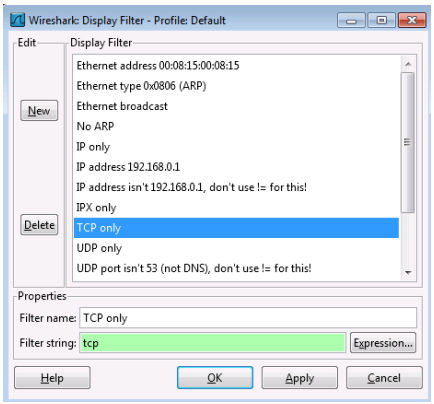
Étape 3 : filtrage de la capture pour afficher uniquement les paquets TCP

Il est possible d'utiliser la fonction de filtrage de Wireshark pour afficher uniquement les paquets TCP.

a. **Cliquer** sur l'option ***Analyze*** dans le menu, puis **cliquer** sur ***Display Filters***.



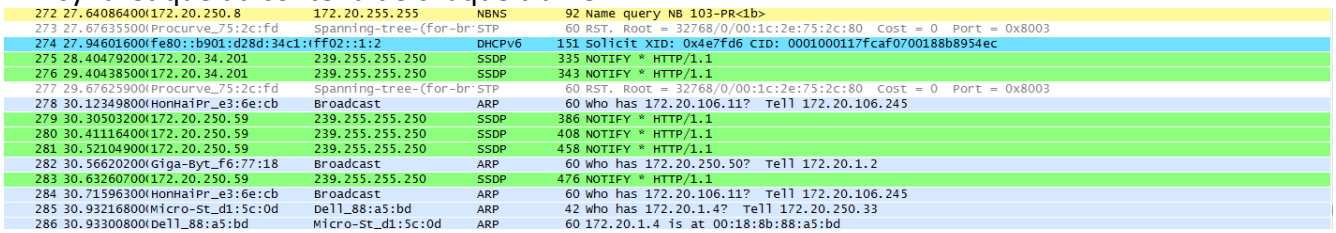
b. Dans la fenêtre ***Display Filter***, **cliquer** sur **TCP only**, puis sur **OK**.



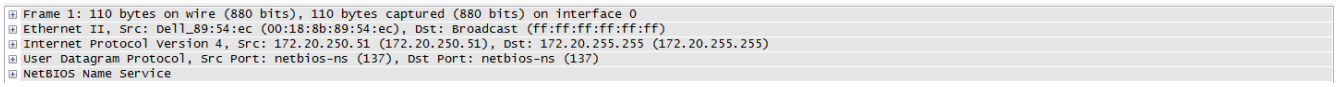
Étape 4 : Analyse des paquets

L'affichage des résultats se décompose en trois parties :

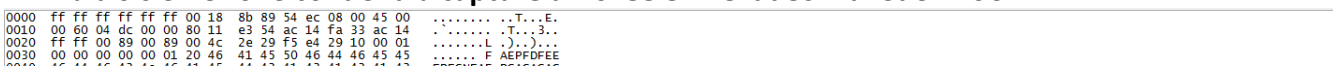
❒ La **liste des trames** capturées disponibles en dessous de la barre de menu avec un affichage synthétique du contenu de chaque trame :



- La **décomposition exacte** de la trame sélectionnée dans la liste. Ce volet affiche les détails de la trame sélectionnée. Les **protocoles et les champs de protocole** de chacune des couches sont indiqués. Ils s'affichent sous la forme d'une arborescence qu'il possible de développer ou réduire.



- La troisième zone contient la **capture affichée en hexadécimal** et en ASCII.



Si une couche du volet précédent est sélectionnée, **l'entête correspondant à cette couche sera mis en surbrillance**.

Remarque : Le préambule et le CRC de la trame Ethernet ne sont pas visibles car ils sont traités uniquement de façon hardware au sein de la carte réseau.