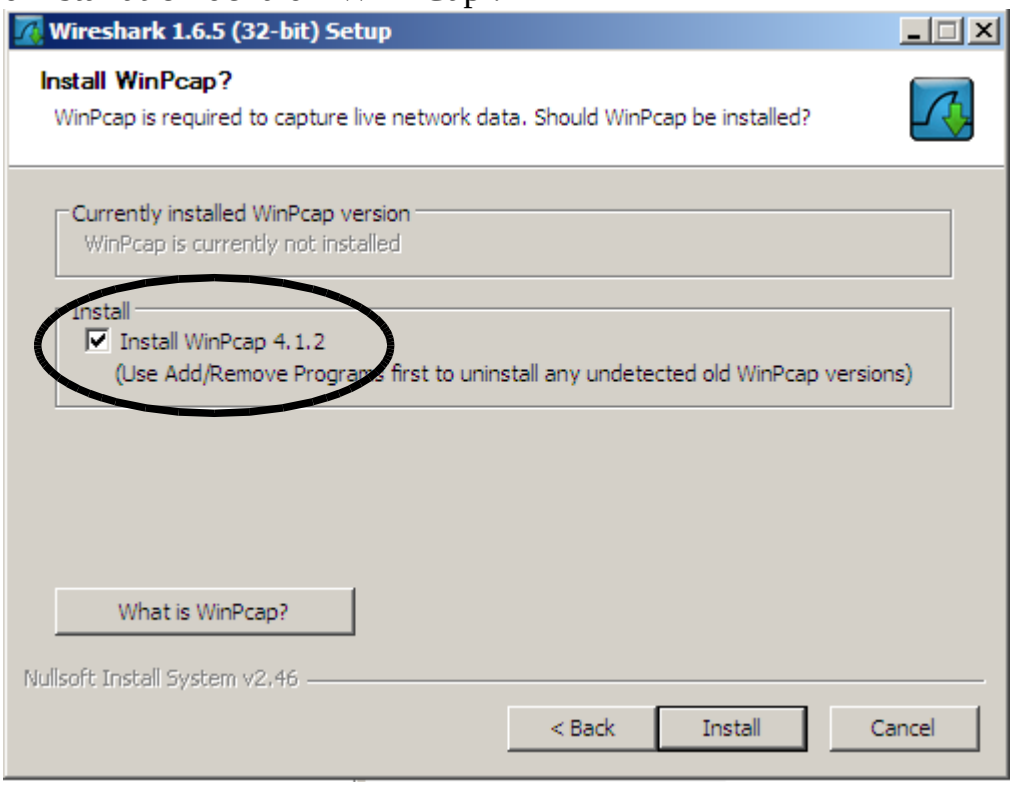
TP Wireshark

Wireshark est un analyseur de protocole réseau. Il permet de visualiser et de capturer les trames, les paquets de différents protocoles réseau, filaire ou pas.
Le site originel est à `http://www.wireshark.org/`. A partir de ce site, on peut lire un tutoriel à `http://www.wireshark.org/docs/wsug_html_chunked/`.
On peut télécharger pour l'installer sur diverses plate-formes (Windows, Linux, Unix et donc Mac OS) à partir de `http://www.wireshark.org/download.html`.
Une FAQ est disponible à `http://www.wireshark.org/faq.html`.

Au 18 février 2013, la dernière version stable est Wireshark 1.8.5. C'est un produit open source et gratuit.
Il a été écrit par Gerald Combs à partir de 1997. C'est la suite du produit Ethereal (son ancien nom).

Pour ce TP, Wirehark est installé sur les machines. Si vous voulez l'installer sur votre propre machine c'est possible. Au moment de l'installation, bien cocher la case d'installation de la dll WinPCap :



"The experience capturing your first packets can range from "it simply works" to "very strange problems"." Si problème voir à `http://wiki.wireshark.org/CaptureSetup`.

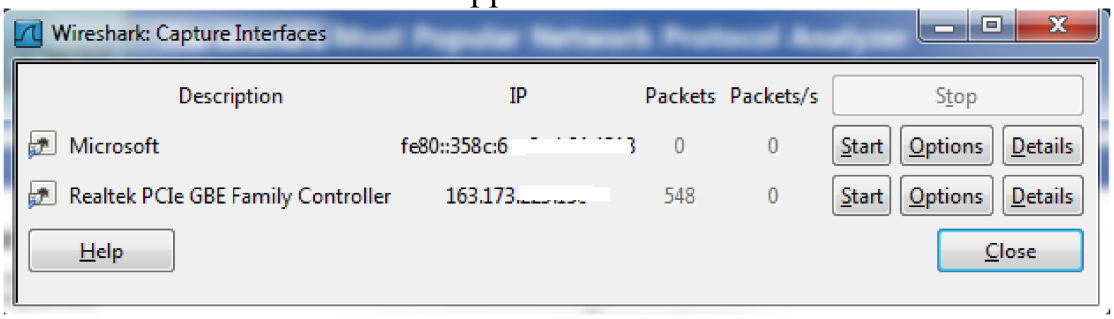
Première approche de Wireshark

1°) Lancer Wireshark (double clic sur l'icône 

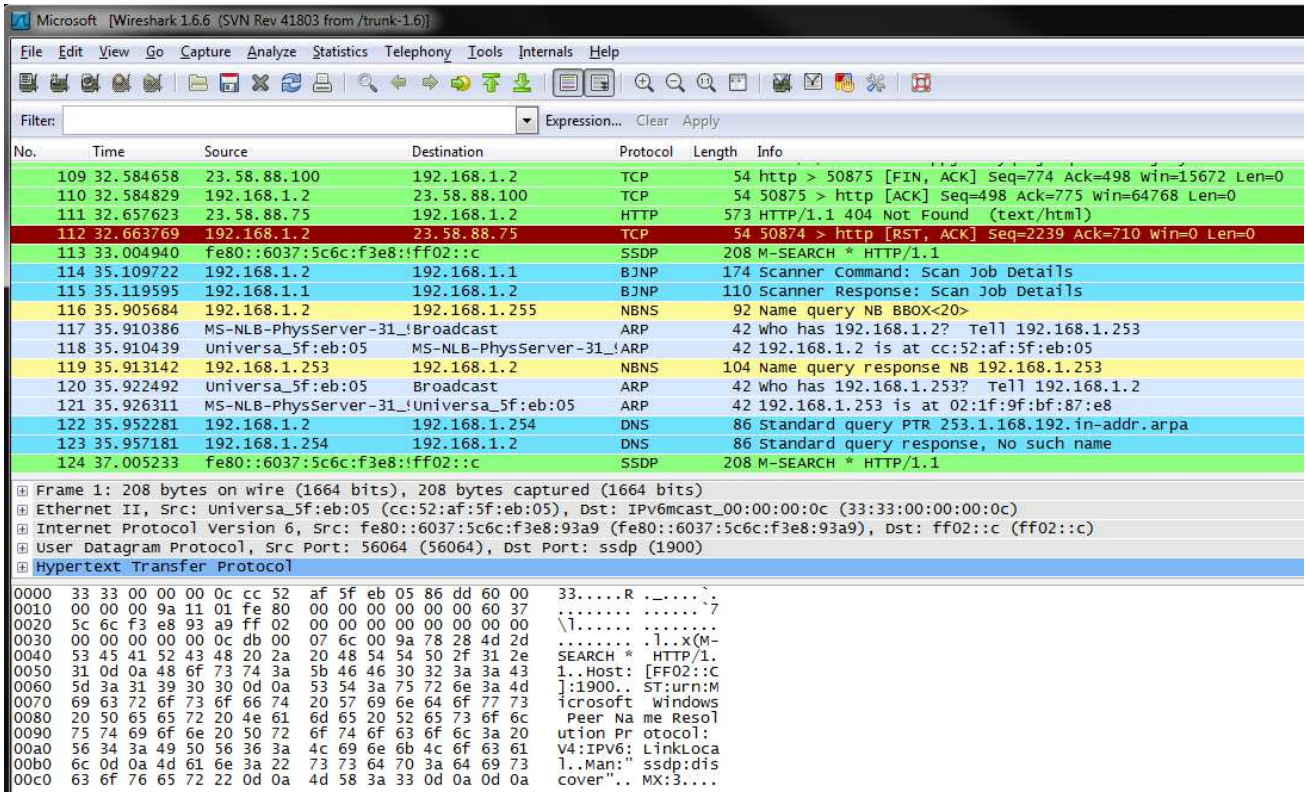
sur le bureau).
La fenêtre

apparaît.

2°) Sélectionner Capture | Interfaces... (ou cliquer sur Interface List ci dessus). Une fenêtre comme celle ci dessous apparaît :



3°) Repérez une entrée ayant du trafic réseau. Cliquer sur son bouton Start. Vous devriez voir une fenêtre similaire à :



4°) Indiquer ce qu'on appelle une "pile" réseau. Donner les composants essentiels de la pile OSI/ISO. Indiquer pour chacune des couches leur s fonctionnalités. Donner les composants essentiels de la pile internet. Pourquoi appelle t -on cela une pile ?

5°) Donner des exemples de protocoles réseau que vous connaissez qui apparaissent dans votre (cette) fenêtre.

6°) La "pile" réseau est illustrée dans une partie de la fenêtre. Indiquer les couches empilées qui ont été utilisées pour la transmission d'un paquet donné. Pour un paquet donné en étudiant chacune de ces couches, indiquer des informations techniques comme :
- la date d'arrivée
- la valeur MAC de la machine émettrice
- l'adresse IP de la machine émettrice
- son type MIME

7°) Sélectionner certains messages et visualiser leur contenu y compris en hexadécimal !

Les protocoles Ethernet et ARP

Pour communiquer sur internet, on utilise les adresses IP. Un des intérêts et de pouvoir hiérarchiser les adresses (une grande entreprise aura une plage d'adresse de type A, une plus petite, une plage beaucoup plus petite d'adresse de type C). Ce sont ces adresses IP qui sont utiliser par les routeurs et pour envoyer un message de France en Australie.

Lorsque le message arrive dans le sous réseau (= petit réseau d'entreprise) contenant votre ordinateur, on utilise les adresses MAC (Media Access Control). Par exemple le protocole Ethernet utilise les adresses MAC.

8°) Expliquer comment fonctionne le protocole Ethernet.
Indication : C'est un protocole de la forme CSMA/CD c'est à dire Carrier Sense Multiple Access with Collision Detection (écoute de porteuse avec accès multiples et détection de collision).

9°) Indiquer le rôle joué par une adresse MAC. Peut il y avoir des ordinateurs sur la planête qui ont la même adresse MAC ? Donner un équivalent de la notion d'adresse MAC pour les personnes françaises.

10°) Il va donc falloir traduire les adresses IP en adresse MAC. Le protocole qui le fait est le protocole ARP (Address Resolution Protocol) (pour la version IPv4). Indiquer dans quelle couche réseau est situé le protocole ARP (bon sens).

11°) Indiquer comment fonctionne le protocole ARP c'est à dire indiquer comment dans un sous réseau, ce protocole s'y prend pour trouver l'adresse MAC d'un ordinateur (ou périphérique) ayant une adresse IP de la forme XXX.YYY.ZZZ.TTT. En déduire qu'on ne pourrait pas utiliser ce protocole pour transmettre des messages sur la planête.

12°) Vous pouvez voir dans une fenêtre Windows les correspondances (= la table) IP / MAC en tappant `arp -a`.

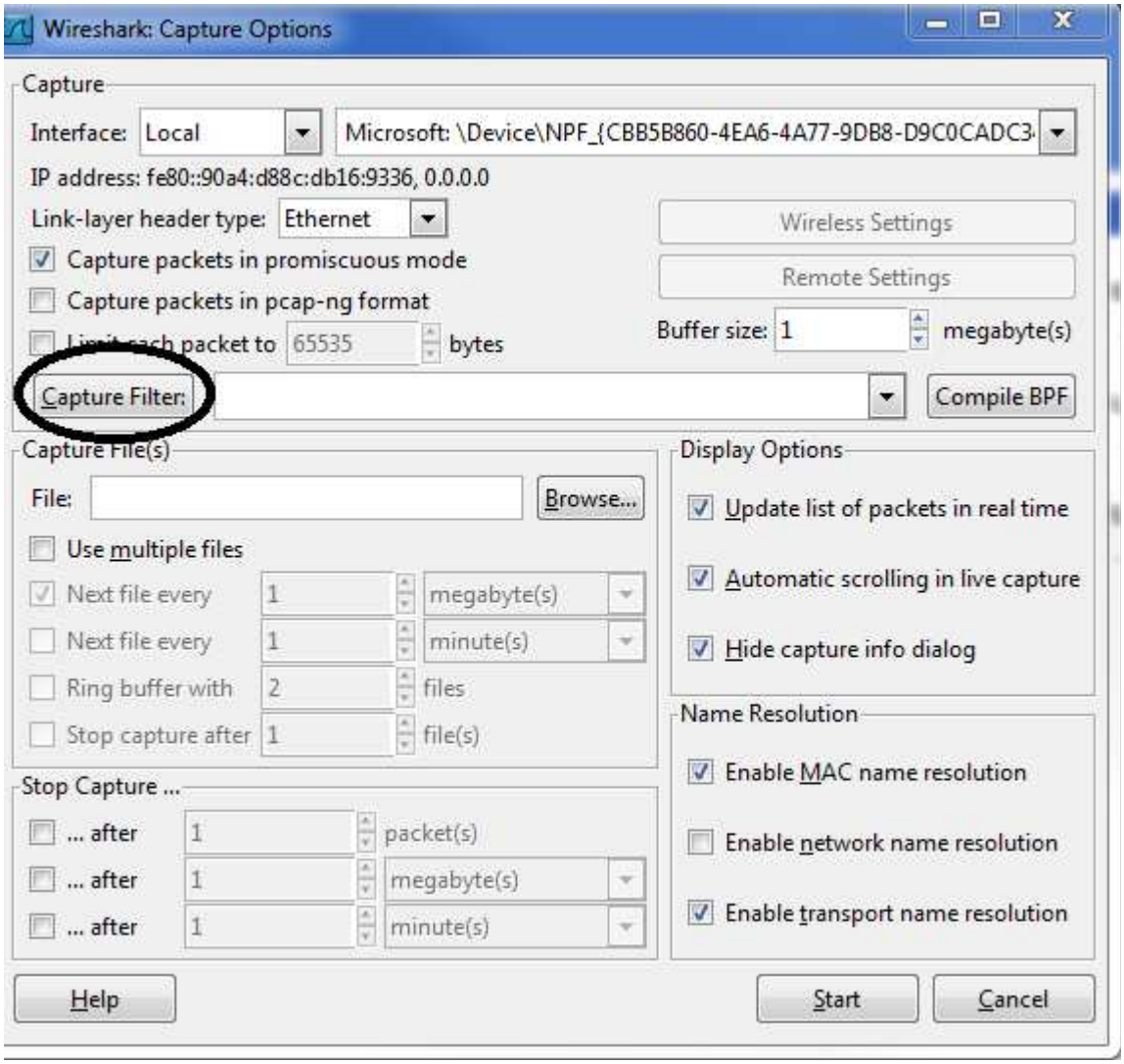
Les filtres sous Wireshark

Comme la première étape fait apparaître toutes sortes de paquets et comme "trop d'information tue l'information", on veut ne faire apparaître qu'un certain type de paquet. Wireshark propose 2 types de filtres l'un au moment de la capture, l'autre au moment de l'affichage.
Plus précisément :
- les filtres de capture sont les filtres qui sélectionnent les données à enregistrer dans les journaux. Ils sont définis au démarrage de la capture,
- les filtres d'affichage sont utilisés pour rechercher à l'intérieur des données capturées. Ils peuvent être modifiés pendant que des données sont capturées.
Ainsi un filtre d'affichage est utilisé pour rechercher à l'intérieur des données récoltées avec un filtre de capture.

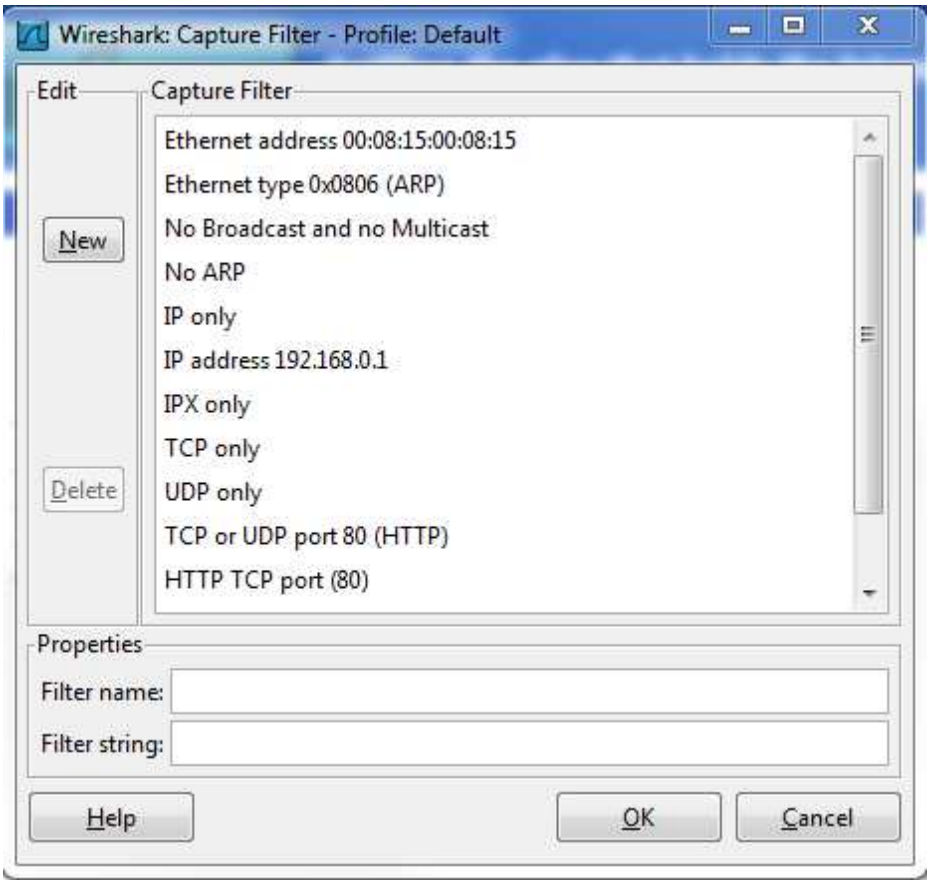
Mise en place de filtre

source : les tutoriaux à
`http://www.wireshark.org/docs/wsug_html_chunked/ChCapCaptureFilterSection.html`
et à
`http://www.wireshark.org/docs/wsug_html_chunked/ChWorkDisplayFilterSection.html`

Il faut construire le filtre avant de lancer la capture.
Lorsque vous lancez la demande de capture (cf. début du TP), sélectionner le bouton options, puis dans la fenêtre "Wireshark: Capture Options", le bouton "Capture Filter:"



La fenêtre "Wireshark: Capture Filter - Profile: Default" propose des protocoles.
Comme Wireshark est plutôt orienté "couches hautes", choisissez celui qui convient pour n'obtenir que les paquets HTTP.



Cliquer OK, puis dans la fenêtre "Wireshark: Capture Options" cliquer start.

Remarque

Ces filtres peuvent être très puissants. On peut filtrer suivant la consition :

```
src host 10.7.2.12 and not dst net 10.200.0.0/16
```

Voir un bon tutoriel sur les filtres à

`http://openmaniak.com/fr/wireshark_filters.php`.

Retour sur ARP

Retrouver un message ARP. On pourra éviter les filtres. Indiquer la correspondance entre des adresses IP et des adresses MAC pour deux machines.

Sauvegarde et Relecture

Vous pouvez sauvegarder un travail dans Wireshark. Pour cela il faut arrêter la capture par Capture | Stop. Le bouton Save du menu File est alors actif. Sauvegarder le travail dans un fichier dans votre répertoire de travail (pas sur le bureau !).

Vous pouvez relire un travail dans Wireshark. Pour cela il faut arrêter la capture par Capture | Stop. Le bouton Open du menu File est alors actif. Charger le fichier que vous voulez relire. Il s'affiche dans Wireshark.

Bibliographie

En plus des éléments donnés en début de cet énoncé, on peut trouver :
Un tutorial à :
`http://blog.nicolargo.com/2007/07/tutoriel-wireshark-ex-ethereal.html`
Les filtres à `http://openmaniak.com/fr/wireshark_filters.php`

Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems, C. Sanders; ed. no starch press.

Wireshark Network Analysis (Second Edition): The Official Wireshark Certified Network Analyst Study Guide, Laura Chappell; ed Chappell University.

Wireshark Certified Network Analyst Exam Prep Guide (Second Edition), Laura Chappell; ed Chappell University.