TP ANALYSEUR RESEAU

Utilisation du logiciel libre « WIRESHARK »

A – Description de Wireshark

1- C'est quoi « Wireshark » ?

« **Wireshark** » est un logiciel d'analyse réseau (**sniffer**) qui permet de visualiser l'ensemble des données qui arrivent sur les interfaces réseau de la machine qui l'exécute. Il permet donc d'obtenir des informations sur les protocoles applicatifs utilisés. Les octets sont capturés en utilisant la librairie réseau libre « **PCAP** », puis regroupés en blocs d'informations et analysés par le logiciel.

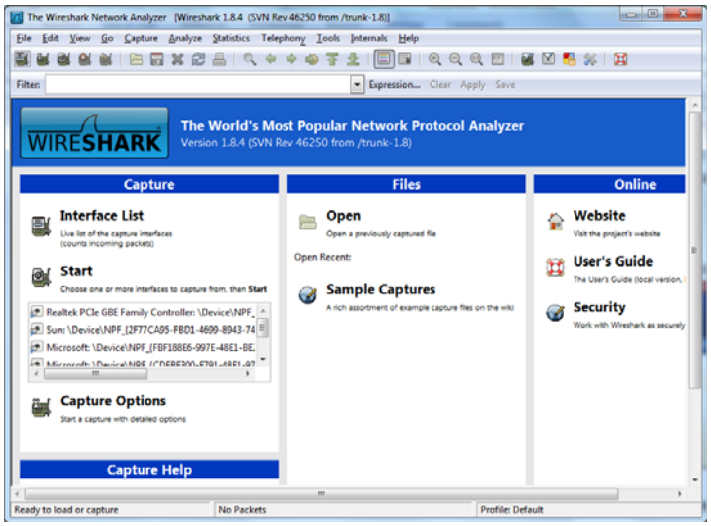
2- Téléchargement et installation.

Allez au site http://www.wireshark.org et télécharger la dernière version stable.

Exécutez le programme d'installation et laissez-le utiliser les paramètres par défaut.

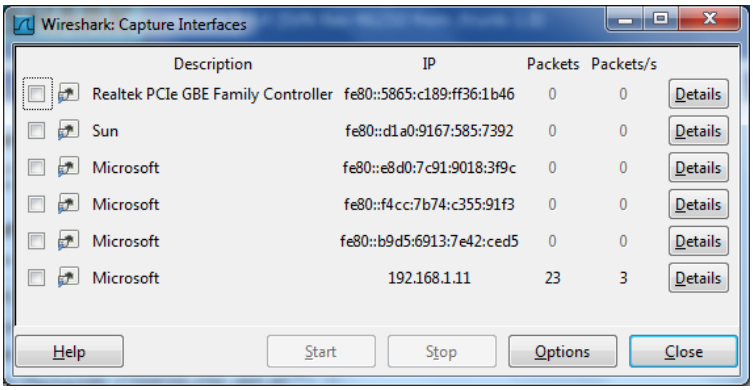
3- Lancez le programme dans le menu : « Démarrer>programme>wireshark »

Cela donne :



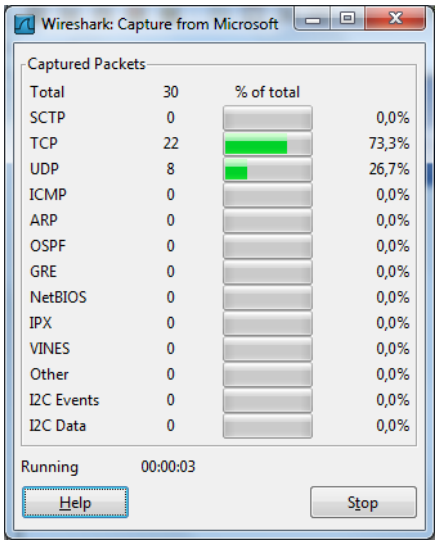
4- Choix de l'interface à écouter :

Dans le menu « **Capture** » choisissez « **Interfaces** » cela affiche :



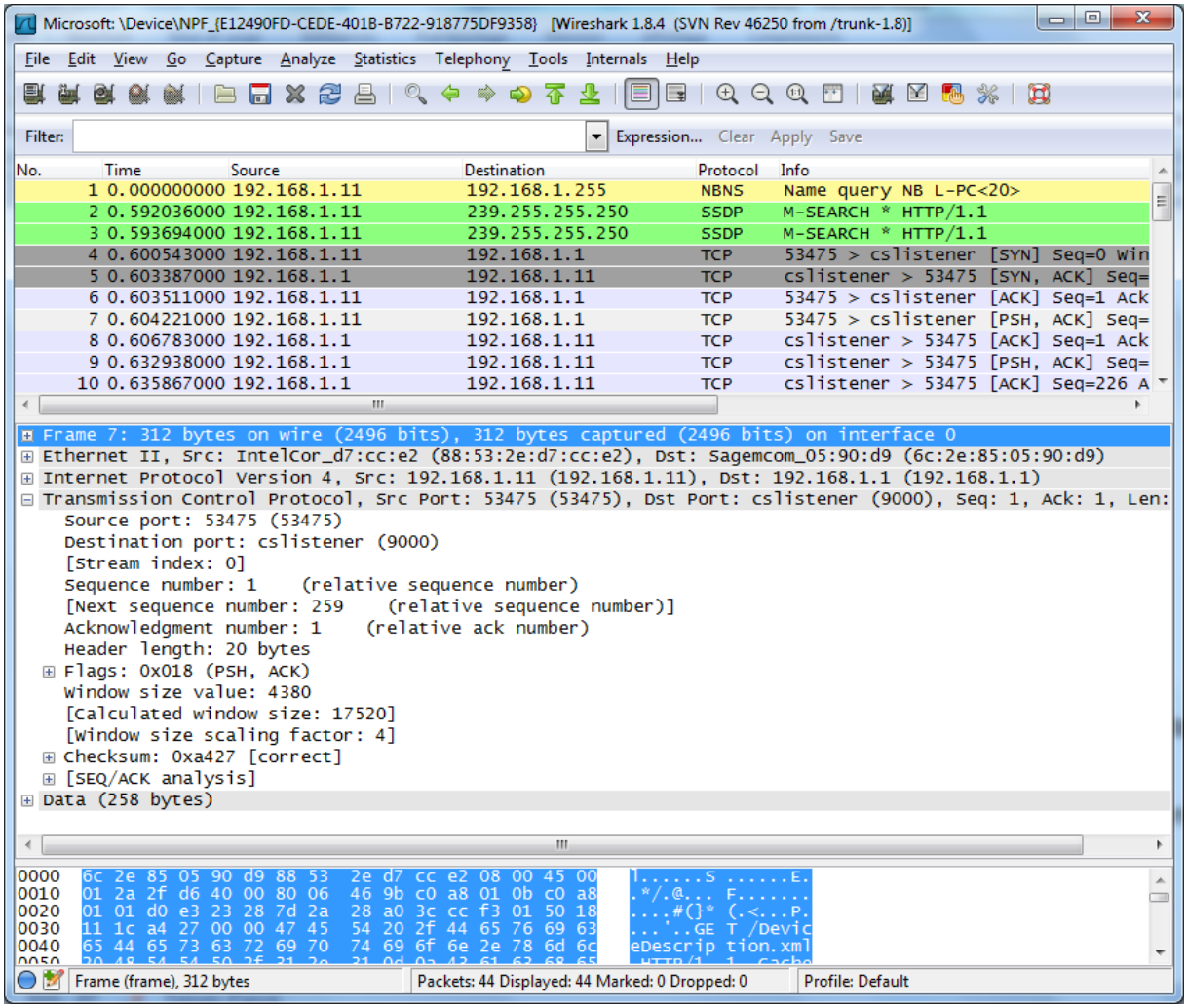
Cette boite de dialogue permet de choisir l'interface réseau qu'on veut écouter.

On remarque les interfaces actives et qui reçoivent les paquets dans la colonne « **packets** ».
Il suffit alors de cocher cette interface puis d'appuyer sur « **start** » :



Attendre un petit moment puis arrêter la capture en appuyant sur « **stop** ».

Le programme présente alors les paquets capturés dans une liste colorée en fonction des protocoles.



Fenêtre principale de « **wireshark** »

La fenêtre présente trois parties :

- La liste des paquets capturés, numérotés et datés.
- Détail d'un paquet (ici le paquet numéro 7)
- Contenu de la trame en hexadécimal.
-

5- Analyse de paquets.

Lorsqu'un paquet est sélectionné, la zone centrale permet de visualiser clairement lesdifférentes couches d'encapsulation du paquet. Par exemple si l'on sélectionne un paquet de type TCP, la zone centrale pourrait afficher quelque chose de similaire à ce qui est présenté la capture d'écran précédente.

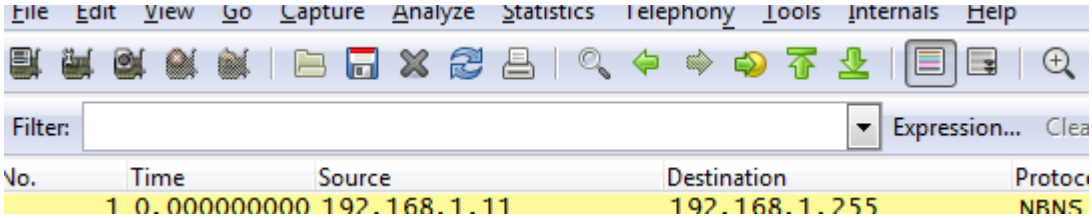
Les 5 entrées présentées correspondent à différentes encapsulations, ordonnées de la couche laplus basse à la couche la plus haute :

1. Données sur le média de capture
2. Trame relative à la couche liaison de donnée
3. Paquet relatif à la couche réseau
4. Segment relatif à la couche
5. Données de l'application

6- Filtrage de paquets

Lorsqu'on fait une capture, on obtient un nombre très grand de paquets. En général on s'intéresse uniquement à certains paquets que l'on veut étudier. Pour pouvoir sélectionner

les paquets, on utilise un filtre. Dans la fenêtre de « wireshark », on peut configurer un « filtre » :



La mise en place d'un filtre s'effectue par le biais d'une règle de filtre à définir dans la zone« **filter** » de l'analyseur. Une règle de filtre est constituée d'un ensemble de tests d'expressionsimpliquant des noms de champs et des valeurs. Un paquet n'est alors listé que s'il satisfait les conditions du filtre. L'ensemble des champs utilisables dans l'établissement desrègles est listé dans la fenêtre pop-up accessible en cliquant sur le bouton « **expression** ». Lesrègles peuvent être élaborées en sélectionnant les champs a partir de cette fenêtre, ou en lesécrivant directement dans la zone de filtre. Un ensemble de filtres prédéfinis est accessible encliquant sur le bouton « **filter** ».
Une fois le filtre défini, il ne faut pas oublier de l'appliquer avec le bouton « **Apply** ».

Voici quelques filtres :

Segments TCP uniquement	: tcp
Paquets relatifs à TCP uniquement	: ip.proto == 0x06
Adresse ip 192.168.0.1 ou 192.168.1.5	: ip.addr == 192.168.0.1 || ip.addr == 192.168.1.5
Trafic HTTP uniquement	: http
Segment TCP sauf sur port 80	: tcp&&!(tcp.port == 80)
Adresse Ethernet 00:FF:12:34:AE:FF	: eth.addr == 00:FF:12:34:AE:FF
Trafic 192.168.0.1 vers 197.168.10.5	: ip.src == 192.168.0.1 && ip.dst == 197.168.10.5
Trafic UDP entre ports 40 et 67	: udp&&udp.port>= 40 &&udp.port<=67
Trafic MSN	: tcp&&tcp.port ==1863

B – Travail demandé

1- Lancez l'analyseur réseau et démarrez la capture. Aller au navigateur web et saisissez le l'url suivante : http://www.casaubon.tv. Après le chargement de la page, stoppez la capture et notez :
   a. Les différentes requêtes « http » effectuées.
   b. Les différentes requêtes « DNS » effectués.
   c. Les connexions et les déconnexions « TCP ».

2- Capture d'un mot de passe « **telnet** » dans le réseau.
   a. Lancez l'analyseur réseau et démarrez la capture.
   b. Connectez-vous en « telnet » à l'adresse « 192.168.10.3 » et loggez vous en tant que « admin » avec le mot de passe « admin ». « telnet 192.168.10.3 »
   c. Arrêtez la capture
   d. Trouver le paquet contenant le mot de passe.