heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

Laboratoire de téléinformatique
Introduction à l'analyseur de réseau Wireshark (Ethereal)

Description

Wireshark est un analyseur de protocole gratuit pour Windows, Unix et ses dérivés. Il permet d'examiner des trames à partir d'un fichier ou directement en les capturant sur le réseau. Pour chaque paquet, il est possible d'obtenir un résumé ainsi qu'un décodage détaillé. Wireshark peut être téléchargée à l'adresse suivante : http://www.wireshark.org/.

En outre, le logiciel possède des fonctionnalités très utiles comme les filtres de capture et d'affichage et la reconstitution du flux d'une session TCP. De plus, le nombre de protocoles reconnus par l'analyseur est très élevé.

Wireshark est un projet *open source* réalisé sous la licence public GNU (GPL). Il est donc possible d'obtenir les programmes sources afin de les modifier.

Ce document, basé sur la version 0.99.0 (windows) du logiciel, est inspiré du User's Guide disponible sous www.ethereal.com (ancien nom de Wireshark : http://www.wireshark.org/docs/).

Pour la manipulation au laboratoire (nous en aurons besoin pour les autres manipulations), il faut suivre la procédure ci-dessous.

Comment commencer ?

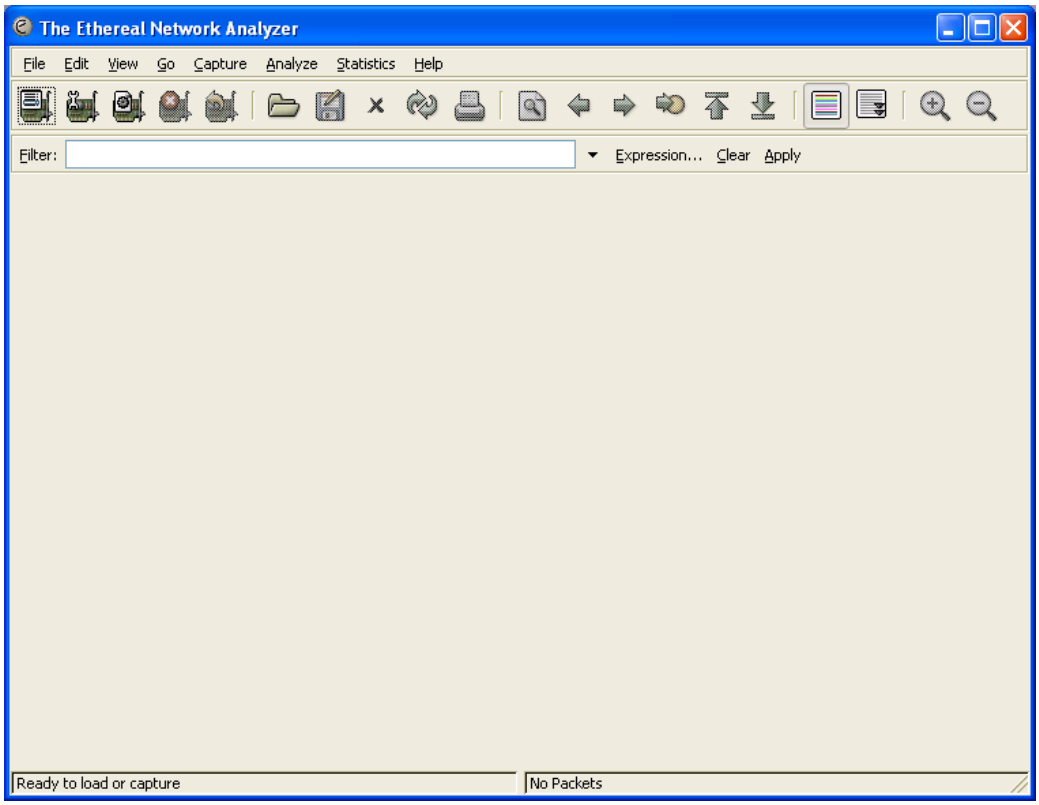
Si vous travaillez sur les machines de l'école il faut premièrement vous mettre sur une station de travail (PC) et démarrer sous Linux[1]:

Login : labo
Password : labo

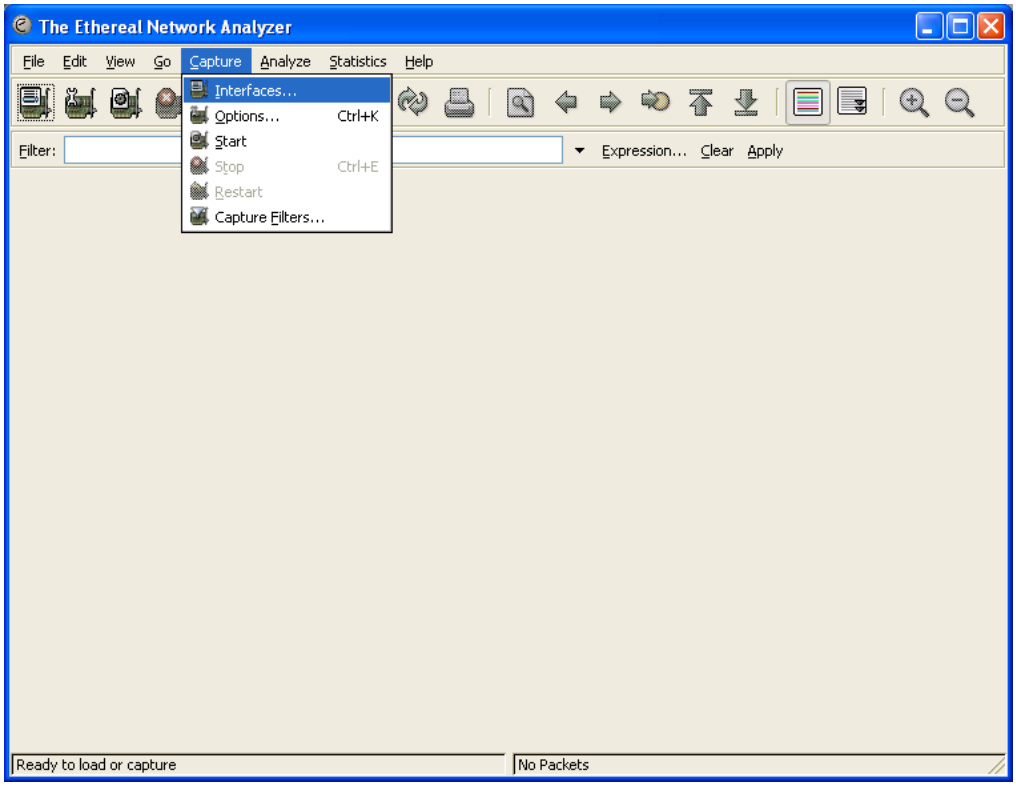
Ensuite il faut démarrer le programme en cliquant sur l'icône « Wireshark » (bureau du Desktop).

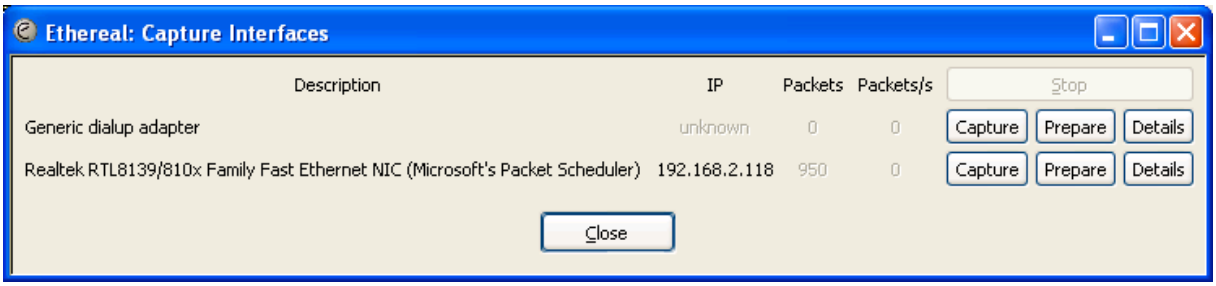
Vous obtiendrez une fenêtre de ce type :

[1] Il faut être administrateur pour utiliser Ethereal, c'est pourquoi vous ne pouvez pas utilier Windows 2k/XP!

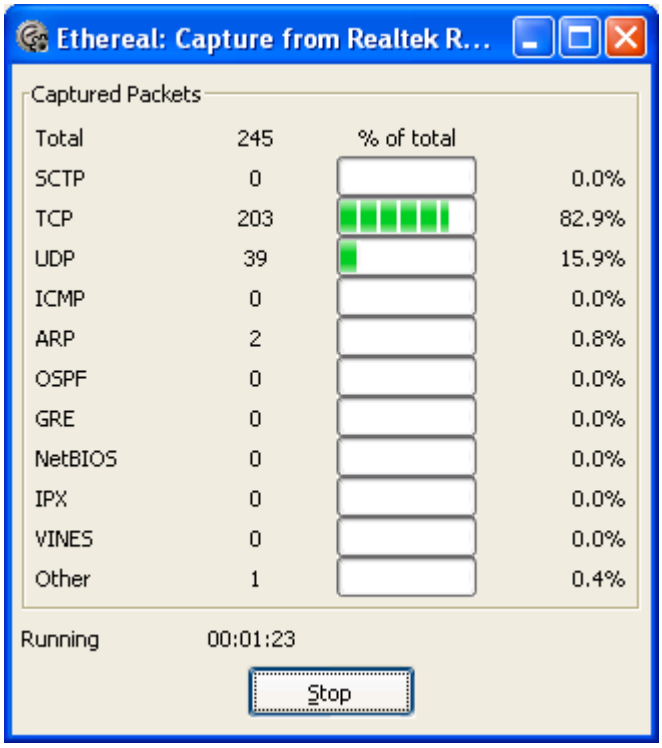


Ensuite faites une analyse sur le réseau en cliquant « Capture » et « Interfaces » et vous obtenez ceci:
(il faut choisir une carte réseau comme interface et eth0 si vous êtes sur un PC école).

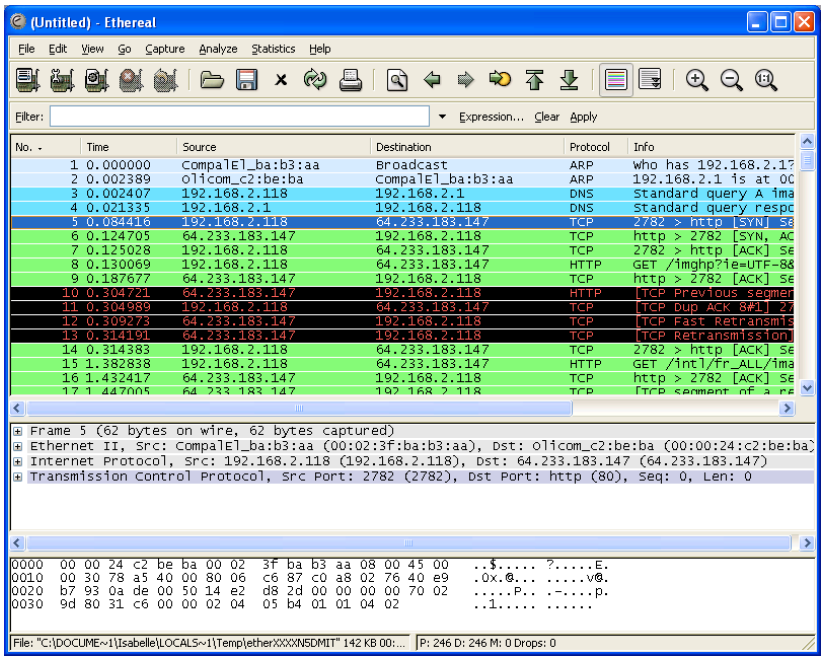




Faites « capture » et l'analyse commence. Vous obtenez ceci :



Quand vous voulez arrêter l'analyse, faites « STOP ». Vous obtenez une fenêtre qui ressemble à ceci :



1

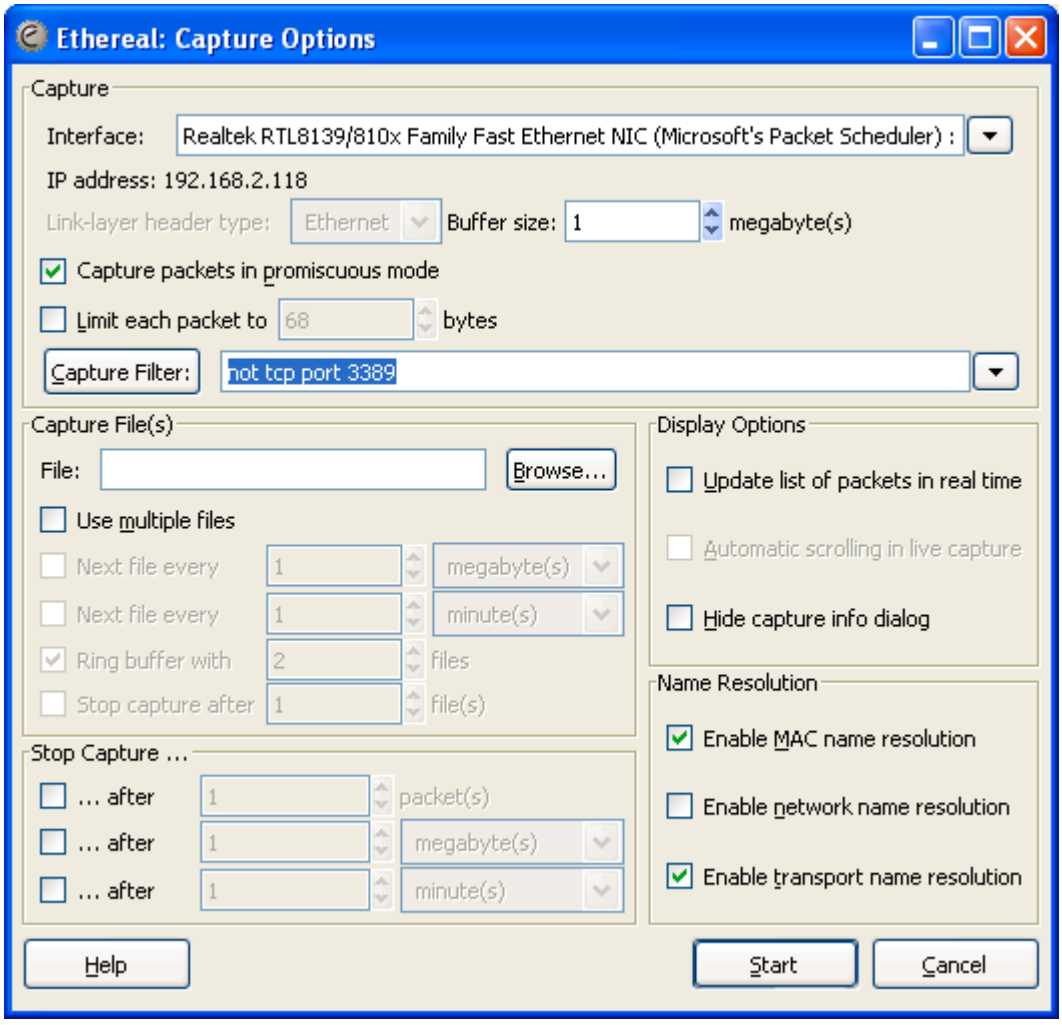
2

3

Nous remarquons que Wireshark est composé de trois panneaux principaux :

1. Ce panneau affiche la liste des paquets ainsi que leurs caractéristiques principales. En cliquant dans ce panneau, on contrôle l'affichage des deux autres.
2. Le panneau du milieu montre le détail de la trame sélectionnée dans le panneau 1.
3. Le dernier panneau permet de visualiser le contenu brut des trames. Il représente le paquet sélectionné dans le panneau 1 et met en évidence le champ sélectionné dans le panneau 2.

Maintenant revenons un peu plus en détail sur la façon dont on peut capturer les paquets. Après avoir cliqué « Options » (faisons-le, au lieu de cliquer sur Interfaces), nous obtenons cette fenêtre :



La capture peut être personnalisée avec les paramètres suivants :

Interface : L'interface réseau sur laquelle la capture est effectuée. Laissez l'interface par défaut proposée, sous Windows. Pour Linux, utilisée ethX, où X est le numéro de l'interface (en général eth0).

Limit each packet to : Spécifie le nombre maximum de données à capturer pour chaque paquet. La valeur par défaut est généralement suffisante pour les protocoles usuels. Il faut cependant que le nombre corresponde au MTU (*Maximum Transfer Unit*) de l'interface de capture.

Capture packets in promiscuous mode : L'option *promiscious* permet de capturer des paquets qui ne nous sont pas destinés. Ceci est évidemment dépendant de la structure du réseau.

Capture Filter : La zone de texte permet d'entrer ou de modifier le filtre de capture. Le bouton ouvre la boîte de dialogue contenant les filtres enregistrés. La conception d'un filtre de capture est présentée au point « Filtres de capture».

File : Ce champ vous permet de spécifier le nom du fichier qui sera utilisé pour la capture quand vous choisirez plus tard « Save » ou « Save as… » dans le menu « File » d'Ethereal.

Update list of packets in real time : Affichage des paquets en cours de capture. Il est préférable de ne pas activer cette option.

Capture limits : Il est possible d'arrêter la capture suivant différents critères : nombre de paquets, de kB, de secondes.

Enable MAC name resolution : Permet de traduire les trois premiers octets des adresses MAC avec le nom du constructeur.

Enable network name resolution : Permet de traduire les adresses IP avec le nom de machine équivalent.

Enable transport name resolution : Permet d'indiquer le nom du protocole, ceci pour les numéros de ports connus.

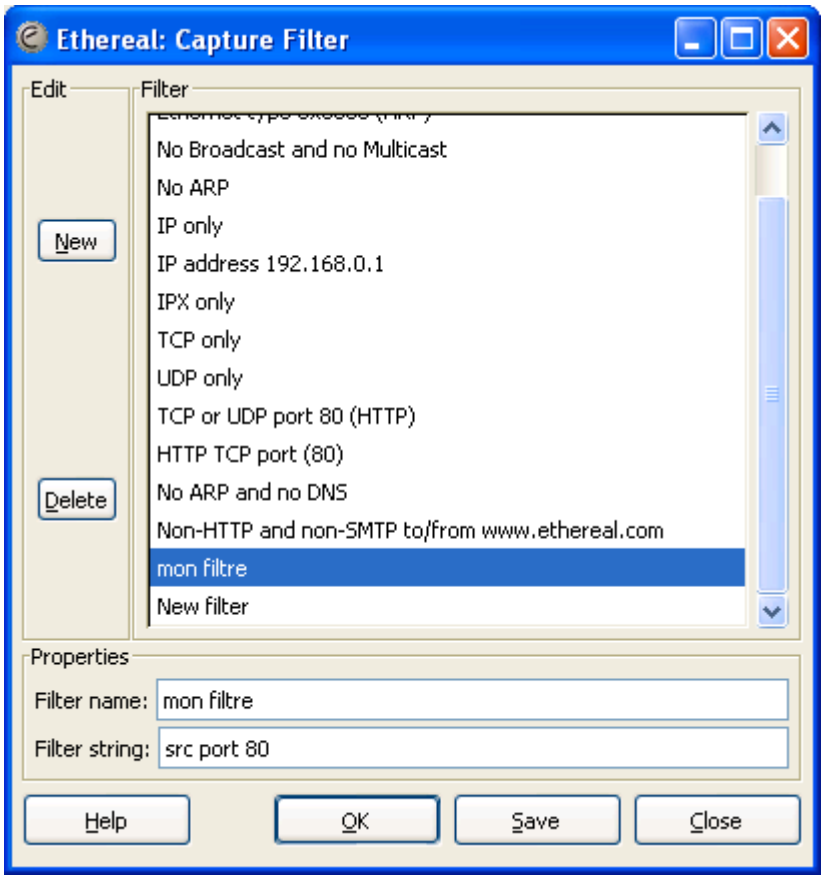
Lorsque toutes les options sont choisies, cliquer sur "Start" pour démarrer une nouvelle capture. Une nouvelle boîte de dialogue s'ouvre alors et indique l'évolution de la capture. Cliquer sur le bouton "Stop" pour terminer la session de capture.

L'affichage peut être modifié à souhait à l'aide des filtres d'affichage dont nous allons parler plus loin.

Filtres de capture

Ethereal utilise les filtres de capture basés sur le langage libpcap. Le détail complet de la syntaxe est expliqué dans le manuel tcpdump (man tcpdump sous Unix/Linux).

Les filtres de capture sont indiqués dans le zone de texte prévue à cet effet dans la boîte de dialogue des options de capture. Il est possible de stocker différents filtres. Pour cela, il faut ouvrir la boîte de dialogue d'édition de filtres de capture en cliquant sur le menu "Capture" / "Capture Filters...". Cette boîte peut également être affichée depuis les options de capture à l'aide du bouton "Filter".



La conception d'un nouveau filtre est la suivante :

- Donner un nom au filtre dans la zone de texte "Filter name" (mon filtre ici).
- Ecrire le filtre dans la zone de texte "Filter string", en respectant la syntaxe ci-dessous.
- Ajouter le filtre en cliquant sur le bouton "New".
- Sauvegarder la liste de filtres à l'aide du bouton "Save".

Syntaxe des filtres de capture

Un filtre de capture est composé d'une suite d'instructions reliées entre elles par des opérateurs `and` ou `or`. On peut inverser le sens des instructions en ajoutant un `not`. Il est possible de grouper les expressions avec des parenthèses.

- `[not] primitive [and|or [not] primitive ...]`

Ceci est la forme générale d'un filtre. Une primitive est l'une de celles présentées ci-dessous.

- `[src|dst] host <host> (exemple: src host 192.169.1.37)`

Filtre sur une adresse IP ou un nom d'hôte. Les mots clés src, dst permettent de se concentrer sur l'adresse IP source, respectivement destination. Sans ces mots clés, tous les paquets liés à l'adresse IP spécifiée sont pris en compte.

- `ether [src|dst] host <ehost>`

Ce filtre suit exactement les principes cités ci-dessus mais s'applique cette fois sur les adresses MAC.

- `[tcp|udp] [src|dst] port <port>`

Filtre sur un port et, par corollaire, un service précis. Délimite la capture aux trames correspondants à un certain numéro de port. De plus, l'on peut spécifier le type de protocole ou encore s'il s'agit d'un port source ou destination.

- `[src|dst] net <net> [{mask <mask>}|{len <len>}]`

Filtre sur un réseau ou un sous-réseau. La capture peut être limitée avec les paramètres src et dst de la même manière que pour les primitives précédentes. Le masque de sous-réseau ou le préfixe CIDR[2] peut être indiqué s'il est différent de la machine sur laquelle se trouve l'analyseur.

- `less|greater <length>`

Filtre sur le paquets dont la longueur est plus petite ou égale, ou respectivement, plus grande ou égale à la longueur spécifiée.

- `[ip|ether] proto <protocol>`

Filtre sur un protocole spécifique au niveau IP respectivement au niveau MAC. Le paramètre protocol correspond au numéro du protocole ou un nom reconnu. Quelques exemples : Un datagramme IP encapsulant un message ICMP à la valeur du champ protocol ID à 1. De même, on reconaît une requête ARP à la valeur 0x0806 du champ type de la trame ethernet.

- `[ether|ip] broadcast|multicast`

Filtre sur du *broadcast* ou du *multicast* IP ou au niveau MAC.

- `<expr> relop <expr>`

Permet de créer des expressions complexes. Les détails sont donnés dans les pages du manuel tcpdump.

Exemples

Les deux filtres ci-dessous sont équivalents : capture du trafic FTP.

- `(src port 21) or (dst port 21)` *ou* `port 21`

Un filtre pour capturer tout le trafic telnet concernant un hôte IP particulier.

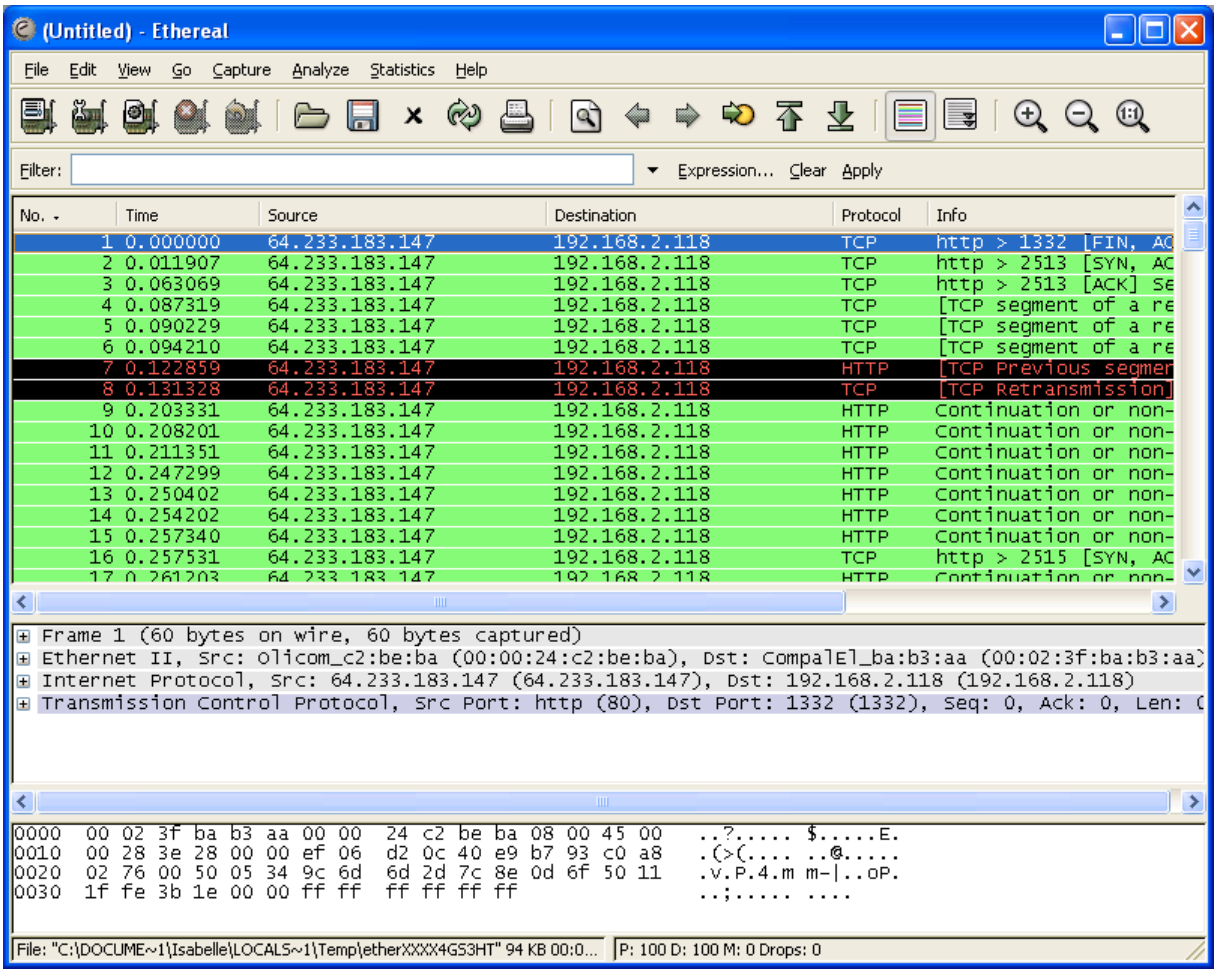
- `tcp port 23 and host 10.192.73.1`

Un filtre de capture concernant le trafic telnet visible sans inclure celui générer vers et à partir un hôte IP particulier.

- `tcp port 23 and not host 10.192.73.1`

Maintenant que nous savons comment faire un filtre, il suffit de relancer l'analyseur et maintenant nous n'obtenons que les paquets http:

2 CIDR, Classless Inter-Domain Routing



Fantastique, non ? A vous de jouer maintenant…

Nous vous encourageons néanmoins à consulter l'aide d'Ethereal.

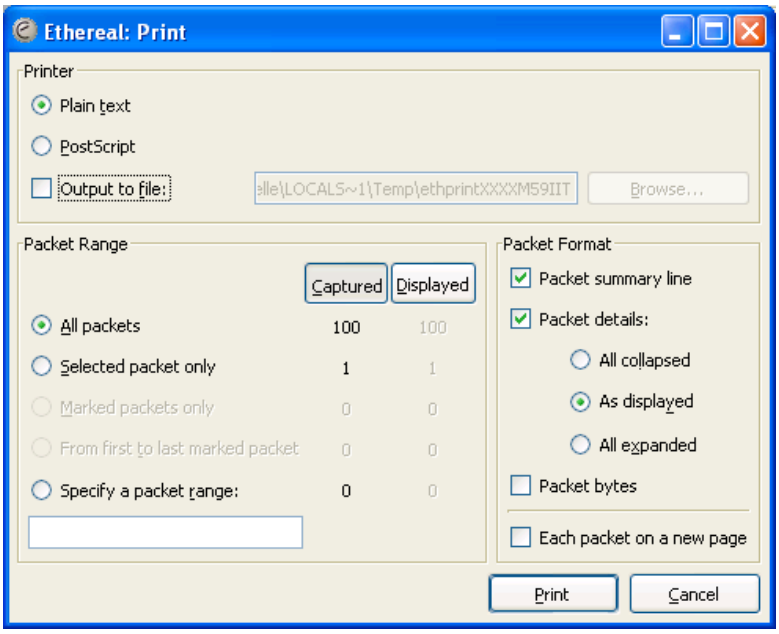
Enregistrer les captures

Il est possible de sauvegarder les captures pour les importer dans un certain nombre d'analyseurs de protocoles. Cependant, il ne s'agit pas de fichiers textes lisibles. De plus le passage du logiciel de Unix à Windows n'a pas permis de gérer l'impression correctement.

Le meilleur moyen pour sauvegarder et imprimer une capture est l'impression dans un fichier à l'aide du menu "File" / "Print...".

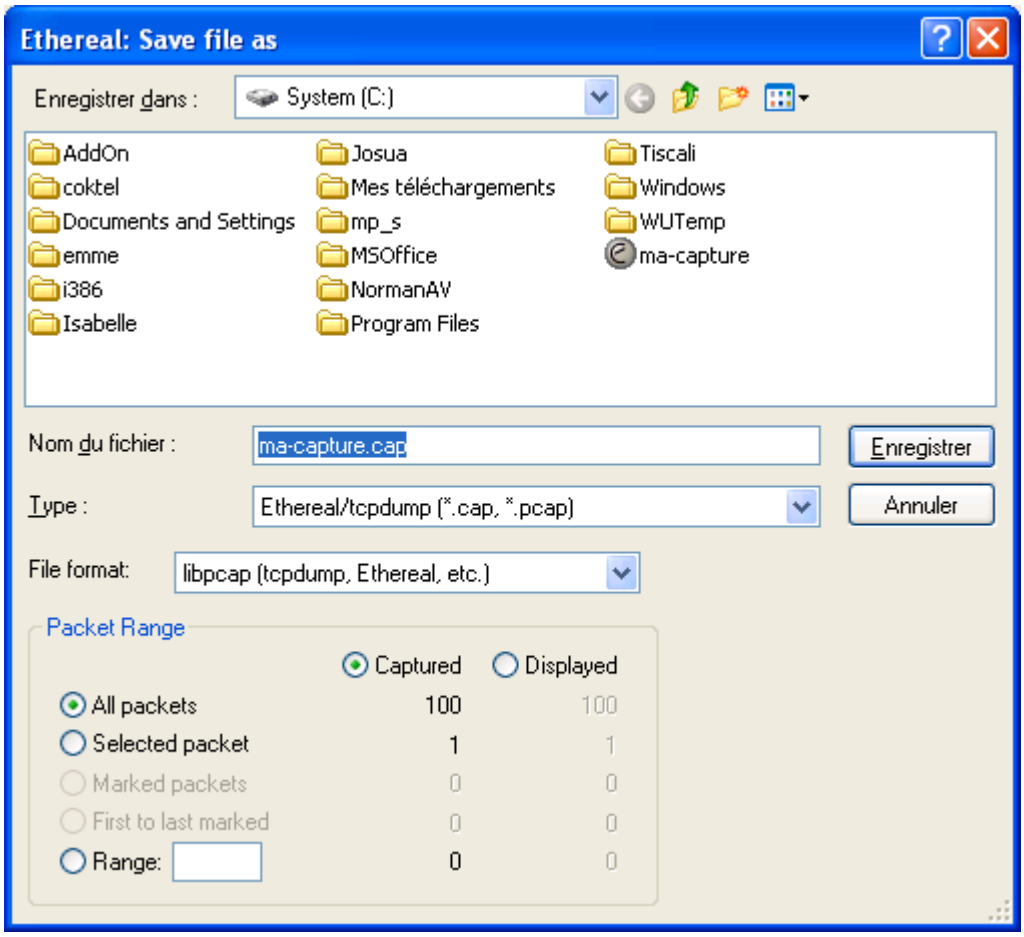
Une boîte de dialogue s'ouvre

Choisir l'option "Plain Text" (par exemple)



L'impression sous Linux ne pose pas de problème praticulier. En utilisant la commande lpr, l'impression est envoyé vers l'imprimante par défaut.

Le bouton "File" permet de choisir le fichier destination (par défault il se place dans le répertoire d'Ethereal chez moi). Vous pouvez aussi sauver un fichier en format .cap :



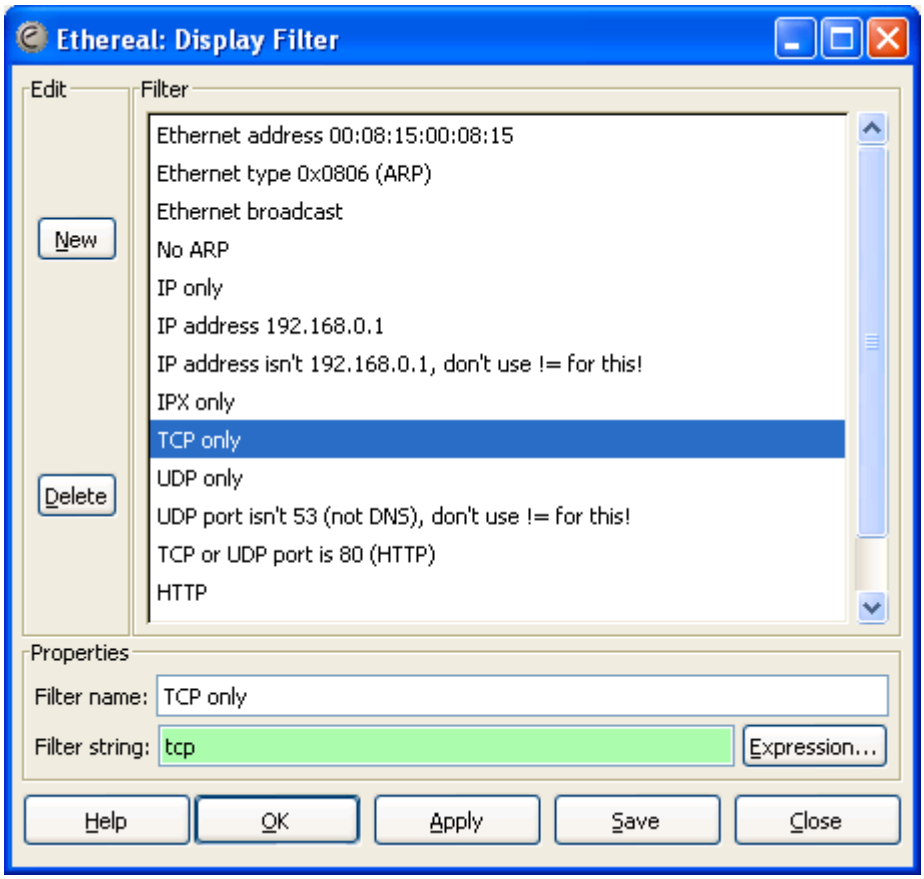
Il est aussi utile de savoir que nous pouvons exporter les données en fichier .txt, .ps,…

Filtres d'affichage

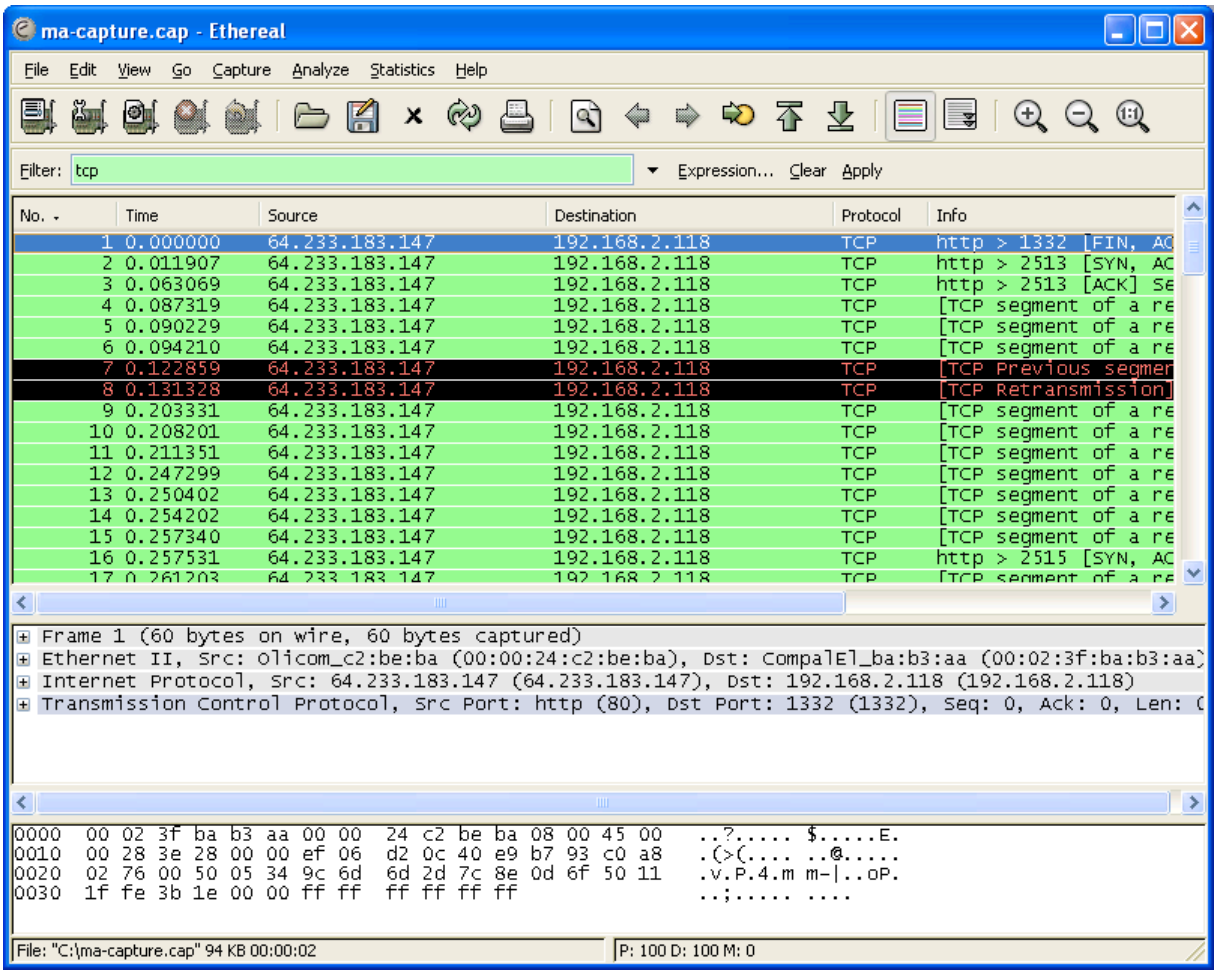
Après avoir effectué une capture, il est toujours possible de modifier l'affichage des paquets en spécifiant un filtre d'affichage (ou filtre de post-capture).

Les filtres d'affichage offrent un nombre d'options et de protocoles reconnus nettement plus grand que celui des filtres de capture. La sélection peut se faire sur :

- un protocole ;
- la présence d'un champ ;
- les valeurs des champs ;
- la comparaison de champs.



Les filtres d'affichage s'écrivent dans la zone de texte située au bas de la fenêtre d'Ethereal (zone B du panneau d'Ethereal). Le bouton "Filter" permet de charger un filtre enregistré préalablement. La création d'un nouveau filtre d'affichage est identique à celle des filtres de capture. Pour sélectionner un protocole particulier, vous pouvez simplement taper le nom du protocole dans la zone B (page 3) et ensuite « Apply » ou « return » pour obtenir ce que vous voulez :

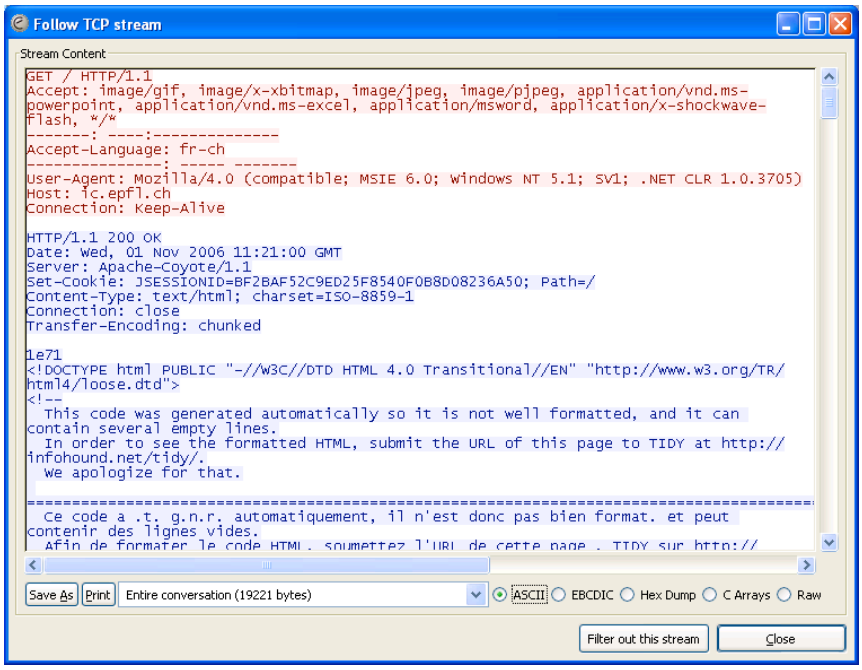


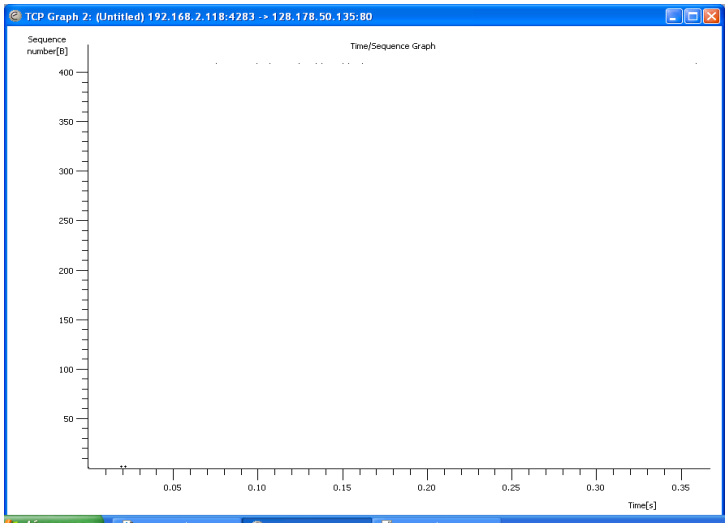
Essayez de faire un ping (ping www.epfl.ch) et de filtrer que ces paquets avec un filtre de d'affichage (en bas à gauche dans cette version d'Ethereal). Le protocole utilisé pour les pings est ICMP.

Flux TCP

La recomposition d'un flux de données n'est disponible que pour le TCP. En effet, les protocoles comme UDP, ICMP, etc. n'établissent pas de connexion et n'ont donc pas de session. Ethereal permet donc de rassembler un flux TCP et d'y appliquer un décodage.

Pour suivre un flux TCP, il faut premièrement sélectionner un paquet faisant parti du flux puis cliquer sur le menu "Statistics" / "Follow TCP Stream". Il est possible d'analyser le comportement de la liaison avec cette option : Timesequence, débit, RTT,…. Essayez… Ne pas oublier que l'utilisation de cette option applique un filtre d'affichage afin de ne prendre en compte que les paquets en relation à la session sélectionnée. Pour supprimer le filtre d'affichage, il suffit d'appuyer sur le bouton "clear" dans la fenêtre.





Référence

- Manuel de l'utilisateur : www.wireshark.com (ou www.ethereal.com). Si vous avez besoin de plus de connaissances sur l'analyseur il est vivement recommandé de consulter ce manuel qui est bien fait.