

Fausse Piste

<http://fausse-piste.net/piste1>

# Ethereal, un outil pour mieux surveiller son réseau informatique

Paranoïaque de la sécurité ? Cet outil est pour vous ! -

**Partie 1**

- LA FAUSSE PISTE DES MANCHOTS - Les Manchots de Big Brother -

Red Herring

Publication le jeudi 1er janvier 2004

Modification le lundi 30 juillet 2007

Fichier PDF créé le vendredi 24 juillet 2009

**Cet article s'adresse plutôt à ceux qui aiment bien mettre les mains dans le cambouis informatique pour mieux comprendre ce qui se passe dans les "tuyaux", mais les novices et les curieux peuvent y trouver leur compte...**



Avoir un réseau local avec des machines connectées vers l'extérieur (Internet par exemple) peut ne pas être de tout repos.

La mise en place d'antivirus, de pare-feux est en général assez efficace... si tout est correctement configuré :-D.

Il existe de nombreux outils de surveillance de réseau qui permettent de vérifier tout ce qui se passe dans les câbles ;-). Et donc après analyse attentive des résultats prendre des mesures si nécessaire pour assurer une meilleure sécurité sur le réseau. Nous allons aborder dans cet article, l'un des meilleurs dans la catégorie *surveillance* du trafic : [Ethereal](#) .

Ce logiciel peut s'installer sur une machine d'un réseau sous Linux ou Windows

## Installation

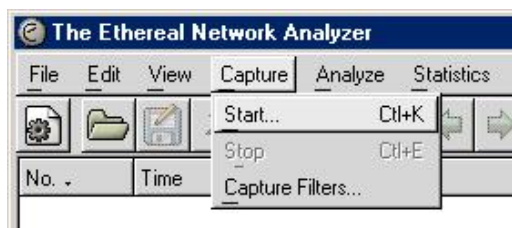
La première chose à faire est de [télécharger Ethereal](#) :

- Linux : si on dispose d'une Mandrake, l'installation du rpm de Ethereal ne devrait pas vous poser de problème (voir sur les CD de la distribution). Vous pouvez opter pour la version tar.gz, si vous aimez compiler :-)
- Windows : télécharger Ethereal [ICI](#) en prenant la dernière version (on n'oubliera pas non plus de télécharger également la dernière version stable de [WinPcap](#) pour une utilisation optimale d'Ethereal). Il suffit de cliquer sur les 2 fichiers d'installation, de suivre les instructions (pas de difficultés particulières) et tout s'installe quasiment automatiquement. Une icône viendra se rajouter sur le bureau.

## Utilisation

L'utilisation sous Linux et Windows est assez similaire, mis à part que sous Linux il faut être *root* (ouvrir une console, utiliser la commande *su*) :

- lancer Ethereal
- cliquer sur capture

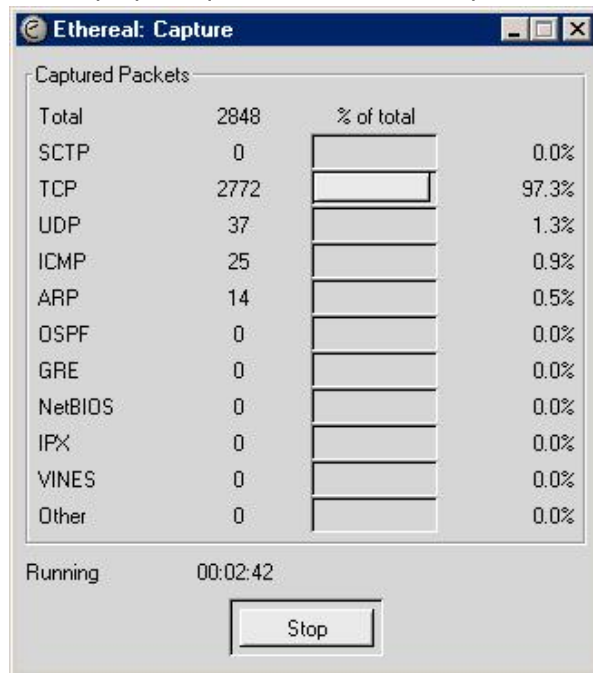


**menu capture**

- indiquer l'interface (eth0 par ex sur Linux, ou le nom de la carte réseau sous Windows - par ex : RTL8139

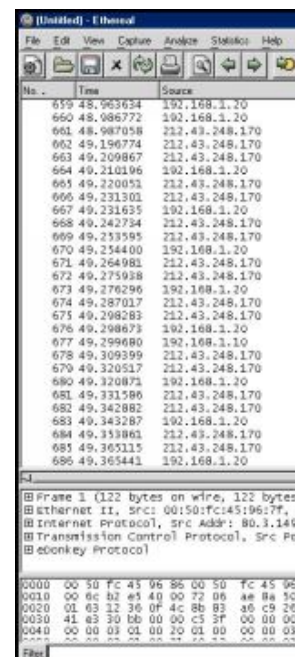
### choix interface

- cliquer sur Ok
- une fenêtre de capture s'affiche en indiquant le nombre de paquets qui transitent selon les protocoles (TCP, UDP, ARP, NetBios, etc.)



### pendant la capture...

- cliquer sur **Stop** lorsque vous estimez avoir assez surveillé le trafic (attention le fichier de surveillance peut dépasser plusieurs Mégaoctets)
- la fenêtre principale se remplit alors... et le boulot d'interprétation commence ;-)



### données capturées...

## Quelques explications

Le fenêtre principale se compose de trois parties :

- La première contient le flux des paquets classés par défaut par ordre chronologique ; pour chacun d'eux :
  - le numéro d'ordre
  - le temps depuis le début de capture
  - la source : en générale une adresse IP ou l'adresse MAC de la carte réseau
  - la destination : idem que ci-dessus
  - le protocole utilisé : ARP, DNS, TCP, HTTP, BROWSE, etc.
  - des informations complémentaires sur le paquet
  
- La deuxième partie contient des détails sur un paquet sélectionné dans la fenêtre de dessus. les différentes parties de cette information peuvent être différentes selon les protocoles utilisés. Par exemple pour un paquet TCP, on aura :
  - le numéro du paquet avec le nombre d'octets et sa date
  - L'Ethernet II avec l'adresse MAC de l'interface source et de celle destinataire
  - L'Internet protocol avec les adresses IP de la source et de la destination
  - La Transmission Control Protocol qui contient principalement les ports utilisés par la source et le destinataire
  
- Dans la dernière fenêtre apparaît en hexadécimal et ASCII le contenu (ou une partie) du paquet.

Une fonction intéressante : **Follow TCP Stream**, que l'on obtient à partir de la barre de menu *Analyse - Follow TCP Stream* permet à partir d'une IP sélectionnée (source ou destination) de suivre le dialogue "en clair" dans une fenêtre. Attention : cette fonction devient d'un usage illégale si les personnes ne vous donnent pas l'autorisation ; c'est assimilable à de la violation de correspondance privée !

***dans un prochain article, nous rentrerons plus en détails sur l'analyse que l'on peut faire avec Ethereal pour mieux sécuriser son réseau***

Note du 30 juillet 2007 : attention depuis la parution de cet article Ethereal est devenu WireShark