

Bien utiliser le logiciel SNIFFER

Par D. Delabre

Introduction

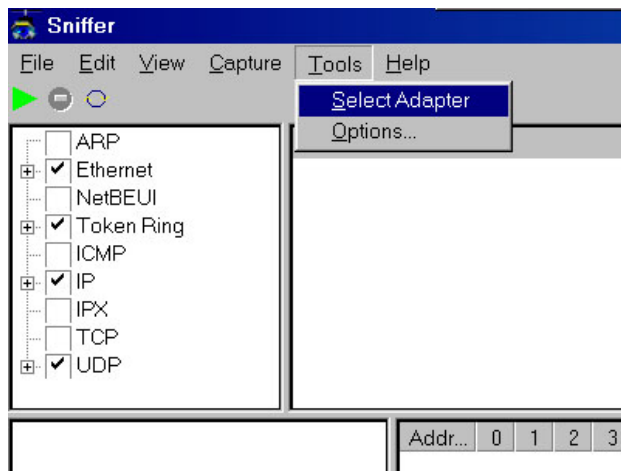
Le logiciel SNIFFER de Ufasoft permet d'analyser les données circulant sur un réseau selon les protocoles suivants : ARP, Ethernet, NetBEUI, Token Ring, ICMP, IP, IPX, TCP et UDP.

Installation

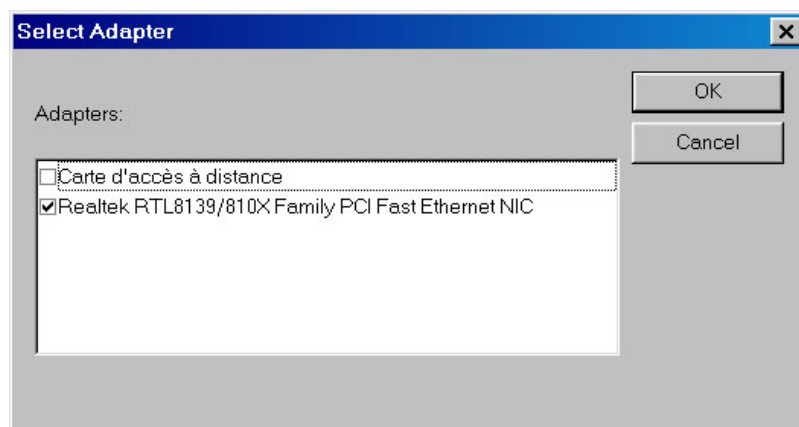
SNIFFER est disponible sur le Web à l'adresse suivante : <http://www.ufasoft.com> .
C'est un shareware utilisable 30 jours. Pour l'utiliser au delà, il faut déboursier 39\$.
Son installation est très simple. Il suffit d'un double-clic sur le fichier sniffer_setup.

Remarque : Sa désinstallation en vue d'une réinstallation après 30 jours doit être effectuée avec un logiciel comme CleanSweep, sinon le logiciel est verrouillé dès la première utilisation.

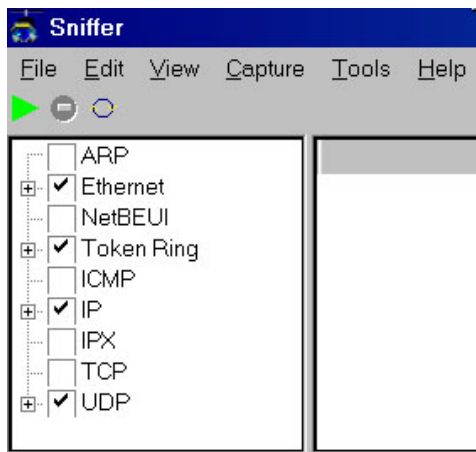
Choix de l'adaptateur réseau



A la première utilisation sur un réseau local, il faut choisir l'adaptateur réseau au moyen du menu Tools.



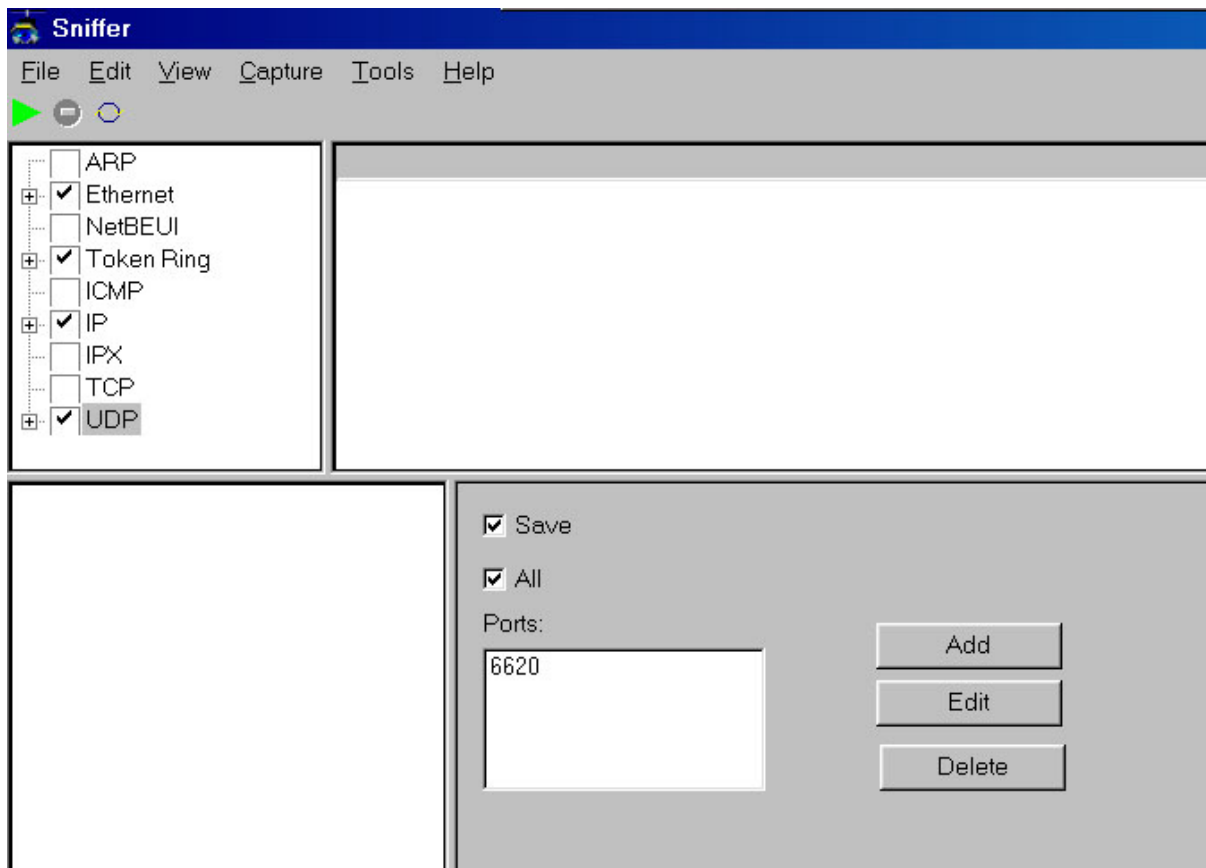
Choix du protocole réseau



Si le protocole qui nous intéresse est UDP, le fait de cocher la case UDP coche aussi les cases IP, Token Ring et Ethernet.

Essayez d'autres protocoles comme TCP ou ICMP.

Ajout du port UDP de l'application analysée



La rubrique UDP étant sélectionnée, ajouter le numéro de port UDP de l'application fonctionnant selon ce protocole. Cliquer sur le bouton Add et entrer le nombre 6620 pour l'exemple. Cocher aussi Save et All dont les fonctions sont expliquées dans l'aide de SNIFFER.

Lancer la capture des trames Ethernet



Le logiciel SNIFFER et l'application réseau à analyser étant tous les deux ouverts, on déclenche la capture des trames avec le bouton supportant une *flèche verte* juste avant d'envoyer les données sur le réseau.

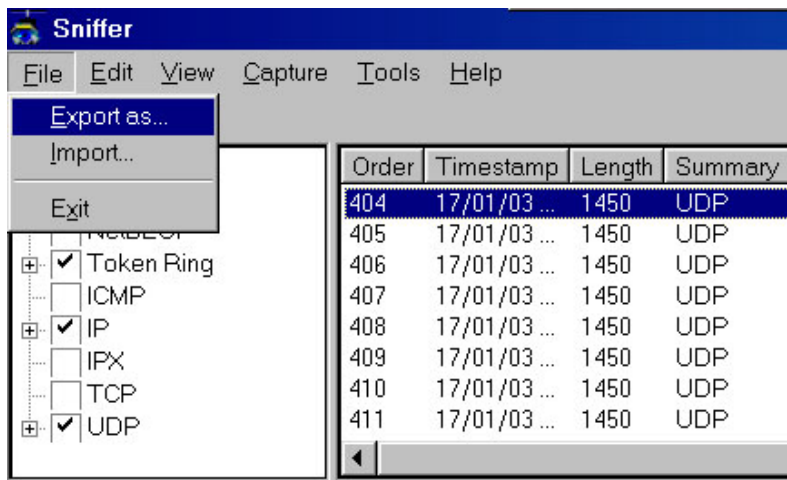


Pour ne pas capturer des trames ne correspondant pas aux données envoyées, arrêter la capture au moyen du bouton *sens interdit* dès que l'application étudiée a reçu ou envoyé les données. En effet les PC du réseau continuent de dialoguer et l'on peut accumuler les trames correspondantes dans la capture. Ce qui est inutile. En outre le nombre maximal de trames est limité à 20000 par défaut (modifiable).

Sauvegarder une capture

SNIFFER ne permet pas d'imprimer les analyses, mais il permet de sauvegarder chaque capture avec la commande *Export as* du menu *File*.

Cette sauvegarde peut se faire sous forme de fichier .txt, mais, par défaut elle est réalisée en fichier .xml que l'on peut relire avec Internet Explorer.



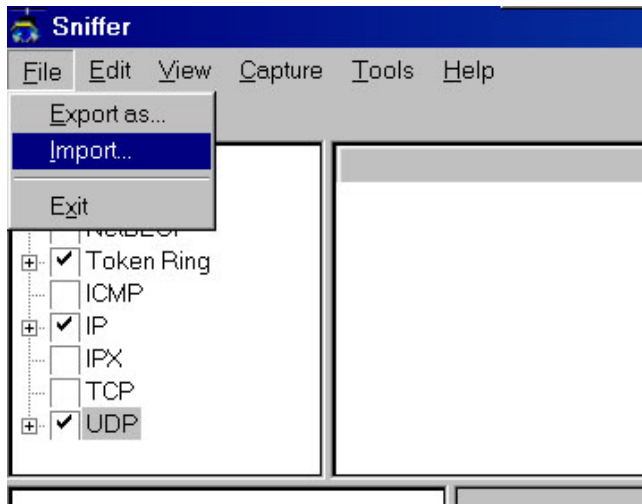
L'exemple de capture représentée ci-contre comporte 77 trames numérotées de 404 à 480. L'ensemble de ces 77 trames sera sauvegardé dans le même fichier .xml d'où l'intérêt d'arrêter la capture comme il est indiqué ci-dessus.

La numérotation des trames tient compte des captures précédentes effectuées pendant la même session.

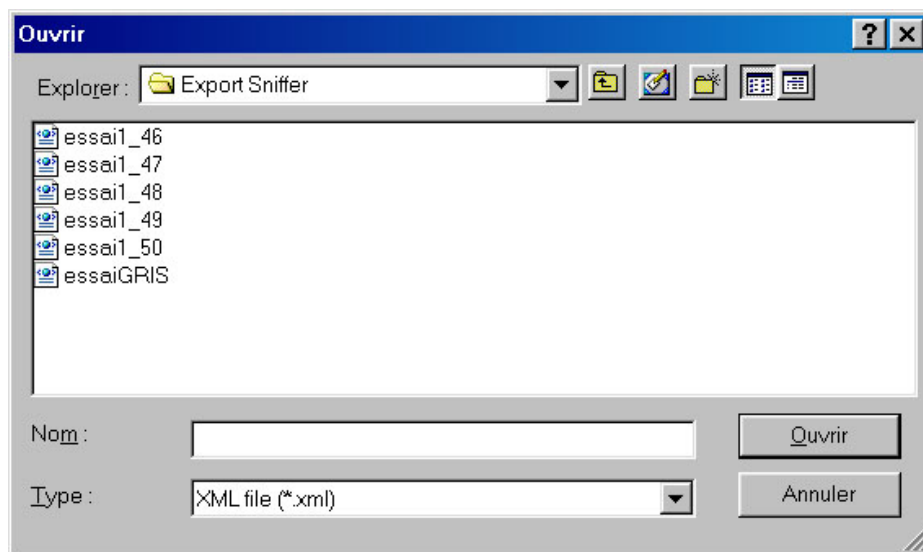
Remarque : Pour tout savoir sur XML, visiter le site <http://www.developpez.com> et cliquer sur l'onglet **XML**.

Ouvrir une capture sauvegardée

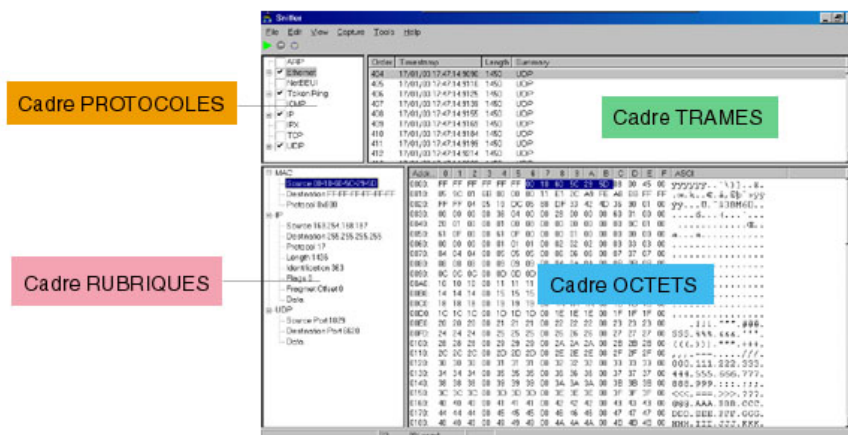
Pour ouvrir une capture de trames sauvegardées afin par exemple de réaliser et d'imprimer quelques captures d'écran comme celles qui sont dans ce document, il faut utiliser la commande *Import* du menu *File*.



L'exemple qui apparaît dans le paragraphe suivant provient de l'importation du fichier `essaiGRIS.xml`. Ce fichier résulte de la capture des trames représentant une image FOND GRIS de 352 pixels sur 288 pixels et émises selon un protocole UDP.

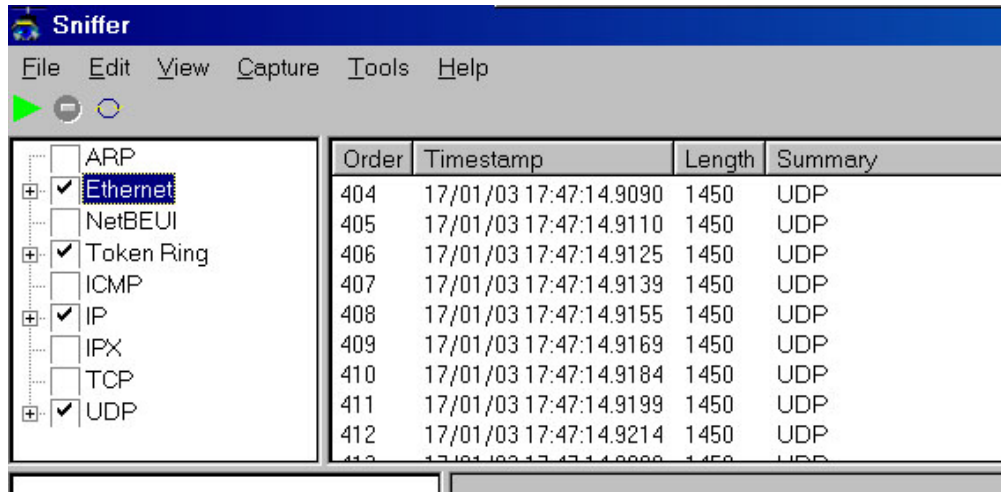


Visualiser les différents éléments d'une trame Ethernet



Cas n°1 : On vient d'effacer une capture avec la commande *delete All* du menu *Edit* et on a importé une capture déjà sauvegardée.

S'il s'agit d'une capture de trame UDP par exemple, il faut sélectionner Ethernet ou UDP dans **le cadre PROTOCOLES** pour afficher les trames dans **le cadre TRAMES**. Ensuite on procède comme dans le cas n°2.



Cas n°2 : On vient de réaliser une capture UDP.

On sélectionne une trame dans **le cadre TRAMES** de Sniffer. Puis, on clique sur les cases + de MAC, IP et UDP pour ouvrir l'arborescence du **cadre RUBRIQUES** de Sniffer si elle n'est pas déjà ouverte. Ensuite il suffit de sélectionner une rubrique de l'arborescence pour visualiser en inversion vidéo les octets concernés dans **le cadre OCTETS**.

