Logiciel Wireshark

I Présentation

L'analyseur de trafic sur le réseau Ethernet est un outil essentiel pour comprendre les mécanismes de fonctionnement des protocoles. Celui-ci peut être également utile pour voir ce qui se passe réellement sur le réseau lorsqu'il y a, par exemple, un problème qu'on n'arrive pas à résoudre.

Pour cela, on utilise les outils qui sont capables de récupérer et analyser des trames qui circulent sur le réseau.

Il existe un outil sous licence GNU qui est capable d'effectuer toutes ces tâches et qui permet d'interpréter la structure des paquets. Cet outil s'appelle **Wireshark**.

Le logiciel Wireshark permet de capturer les trames qui arrivent sur votre PC. Il s'agit uniquement des trames émises ou reçues par le PC et les trames envoyées en multidiffusion si votre PC est connecté à un commutateur.

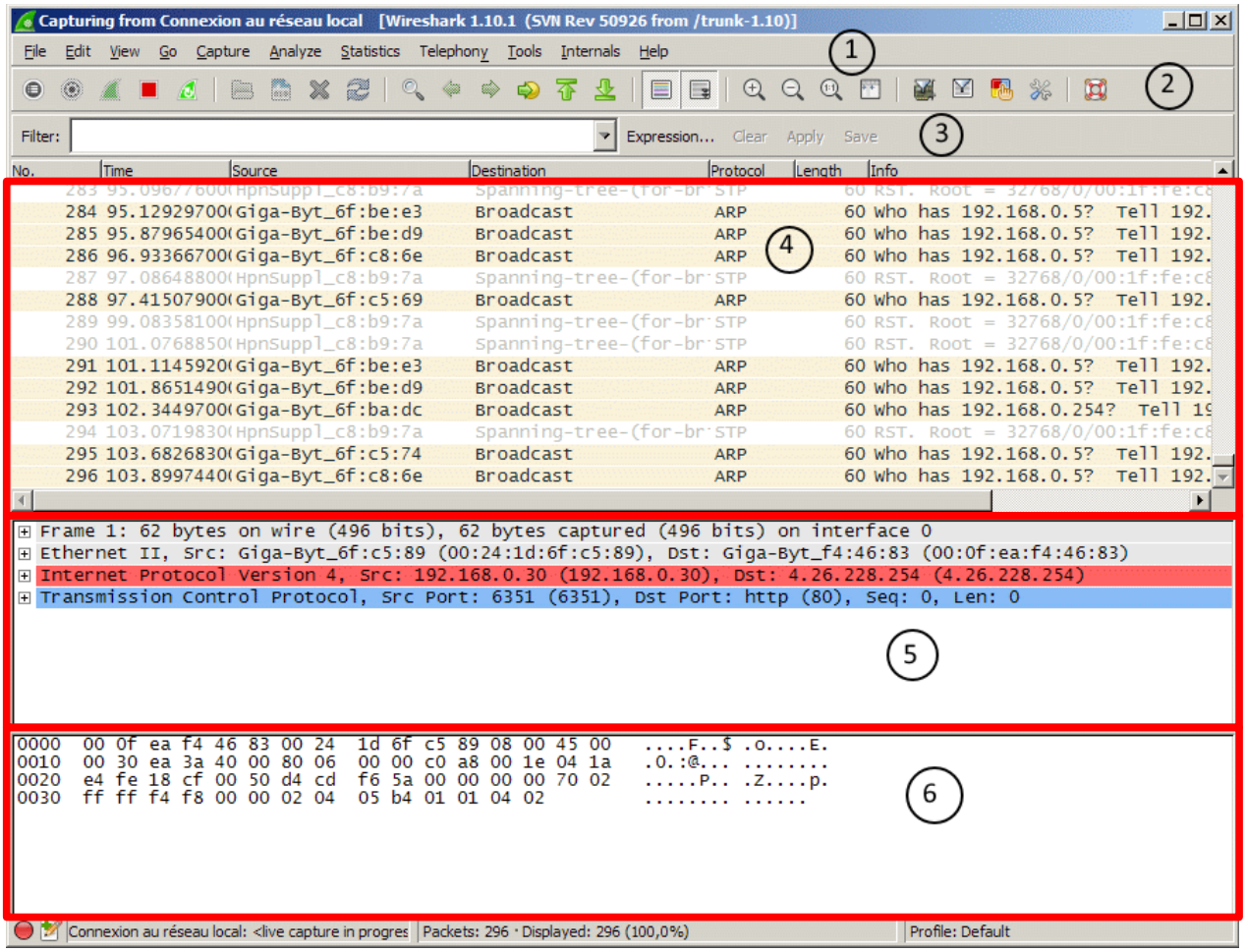
Il est extrêmement utile pour toute personne souhaitant travailler dans les communications réseau et permet aussi bien d'effectuer des opérations de maintenance des réseaux ou de logiciels, que de lutter contre le piratage ou de s'informer sur le contenu exact de certains protocoles.

Les trames peuvent être filtrées afin de n'obtenir que celles qui vous intéressent. Les filtrages possibles sont selon le sens de transmission, le protocole, l'adresse de la machine ou le port.

Les différentes trames capturées peuvent être sauvegardées dans un fichier de capture afin d'être visualisées après coup.

II Interface utilisateur

L'interface de l'analyseur se compose en plusieurs barres et fenêtres :

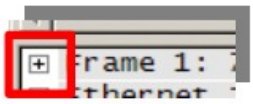


1. **Barre de menus** : on trouve la liste classique de menus. Voici une liste des fonctions accessibles à partir de ces menus :
   - ✗ Le menu « File » sert à sauvegarder ou charger un fichier de capture,
   - ✗ Le menu « Capture » sert à paramétrer une nouvelle capture réseau.
2. **Barre d'icônes** : cette barre regroupe tous les raccourcis sur la manipulation d'une capture.
3. **Barre de filtrage** : cette barre sert à saisir l'expression de filtrage à postériori d'une capture pour isoler tout ou une partie d'un échange de réseaux.
4. **Fenêtre contenant la liste des trames capturées** : sur chaque ligne on trouve :
   - ✗ le numéro de la trame capturée, par ordre croissant d'apparition ;
   - ✗ le temps relatif d'apparition de la trame par rapport à la première ;
   - ✗ la machine source de la trame (ici adresse IP, mais pourrait être un autre type d'adresse) ;
   - ✗ la machine destination de la trame ;
   - ✗ la taille de la trame ;
   - ✗ le protocole de couche le plus élevé trouvé dans la trame ;
   - ✗ un résumé des informations de la trame concernant la couche la plus élevée de celle-ci.
5. **Fenêtre d'affichage de la pile des protocoles décodés pour la trame sélectionnée** : avant tout développement des champs d'un ou de plusieurs protocoles, cette fenêtre donne la liste de la pile de protocoles décodés allant du niveau physique (en haut) jusqu'au niveau le plus haut reconnu (en bas). Le protocole de niveau le plus haut reconnu (du modèle OSI ou TCP/IP) qui apparaît est indiqué dans la colonne « protocole » de la fenêtre contenant la liste des trames capturées.

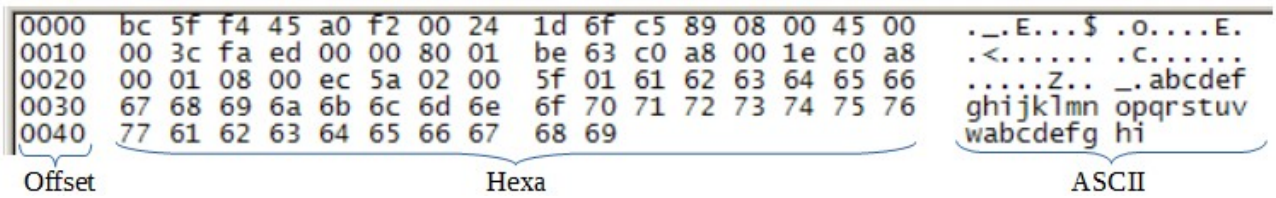
L'ordre des couches sera le suivant :

- ✗ Couche Physique
- ✗ Couche Liaison de Données
- ✗ Couche Réseau
- ✗ Couche Transport
- ✗ Couche Application
- ✗ Informations contenues dans la couche application

Pour développer chacun des champs de la trame, il faut cliquer sur le bouton « + » situé à gauche au niveau de chaque couche.



6. **Fenêtre « affichage » brut de la trame sélectionnée** : Cette fenêtre affiche tous les octets de la trame sélectionnée en hexadécimal et en ASCII avec le décalage par rapoort au début des données :

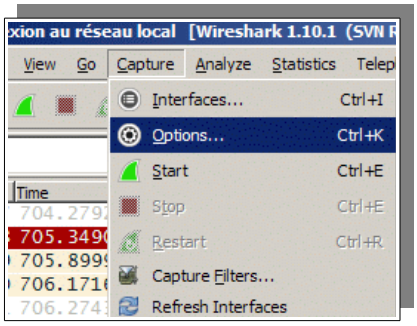


Pour retrouver des informations dans la trame brute, il suffit d'aller sélectionner une information dans la partie 5, celle-ci sera mise en surbrillance dans la partie 6.

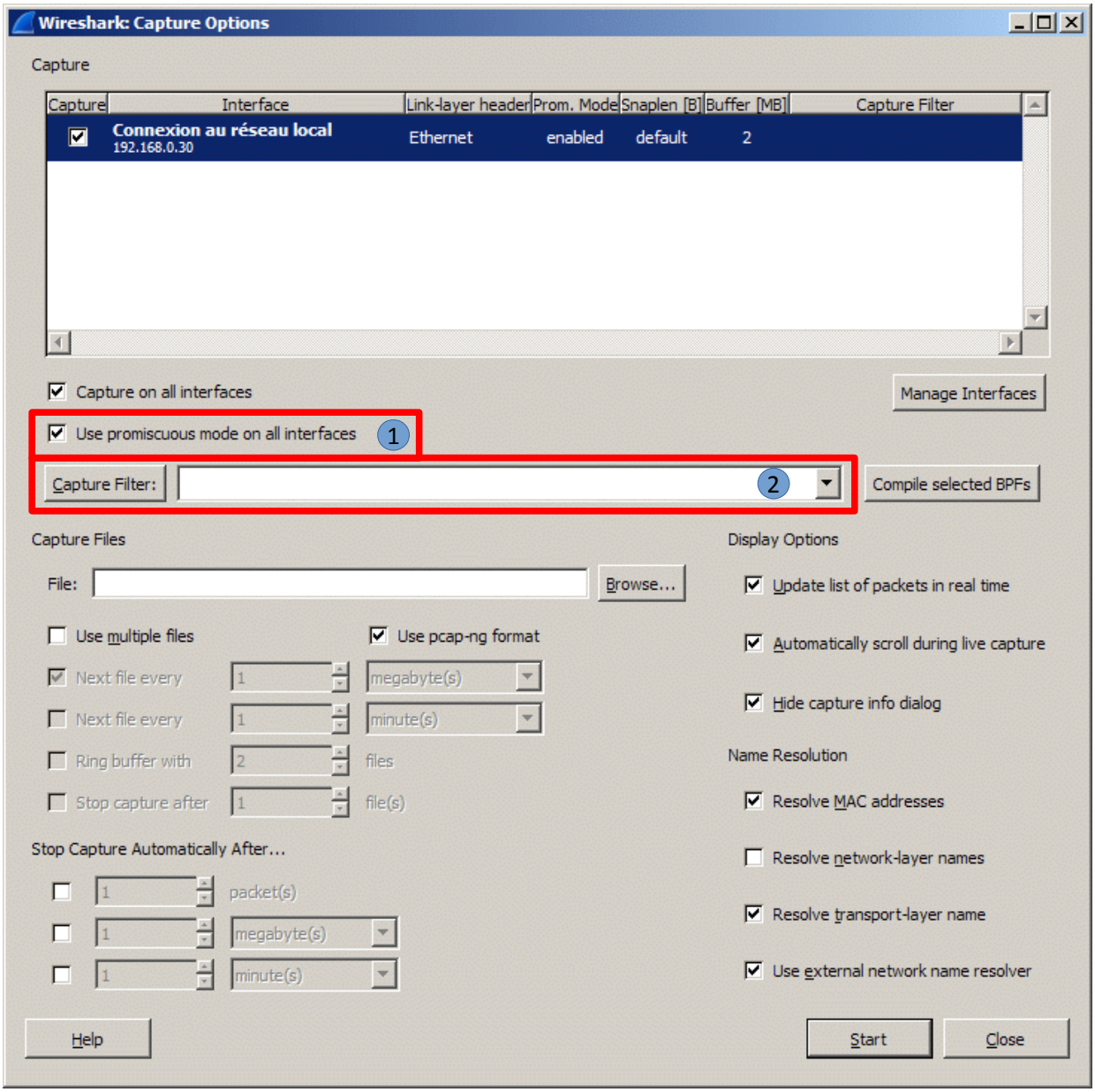
III Configuration de la capture de trames

Pour capturer des paquets de trames, vous devez démarrer une session de capture à l'aide du menu « Capture » Cette session peut être active ou pas. En d'autres termes, les paquets capturés peuvent être affichés au fur et à mesure ou à la fin de la capture.

Pour lancer une session de capture, il faut accéder au menu « Capture » puis cliquer sur « Options… »



Il apparaît la boîte de dialogue qui permet de spécifier ce qui doit être analysé :



La zone « Capture » comprend :

- Le champ « Interface » permet de choisir l'interface sur laquelle on va écouter. Sur l'ordinateur de la section, l'interface à sélectionner doit être « Realteck RTL8139… ». Si cette interface n'est pas disponible, il faut vérifier le compte utilisateur.

- Le champ « Capture Filter » (cadre2) est important car il permet de limiter les paquets qui seront capturés. Seuls les paquets pour lesquels cette expression est vraie seront conservés. Dans l'exemple donné, on s'intéresse aux paquets dont le protocole est « tcp » avec le port source ou destination 80 qui correspond au protocole « http » (Internet). Pour des détails sur les filtres, se référer au chapitre sur les filtres.
- L'option « Use promiscuous mode on all interfaces » (cadre 1) permet de capturer tous les paquets arrivant sur la carte réseau, même ceux qui ne sont pas destinés à l'ordinateur. Cette option peut être utile lorsque l'on souhaite intercepter des messages dont on n'est ni la source, ni la destination.

La zone « **Capture File** » permet de spécifier le nom du fichier dans lequel on va stocker la capture (ce n'est pas obligatoire).

La section « **Stop Capture** » permet de spécifier le nombre de paquets à capturer. Si ce champ n'est pas spécifié, Wireshark captera des paquets jusqu'à ce qu'on lui demande d'arrêter.

Dans la zone « **Display Options** » :

- « Update liste of packets in realtime » permet, s'il est coché, de voir les paquets s'afficher en temps réel, durant la capture, dans la fenêtre des paquets disponibles. Cette option n'est à utiliser que s'il n'y a pas beaucoup de paquets à conserver.
- « Automatic scrolling in live capture » permet, s'il est coché, de voir les derniers paquets affichés en temps réel (pendant la capture) dans la fenêtre des paquets disponibles en faisant défiler la liste des paquets disponibles. Cette option ne doit être utilisée que s'il y a peu de paquets à capturer.

Dans la zone « **Name Resolution** » :

- « enable mac name resolution » permet, s'il est coché, de demander une traduction des adresses MAC en nom de fabricant de la carte de réseau.
- « enable network name resolution » permet, s'il est coché, de demander une traduction des adresses IP en nom. Cette option doit être manipulée avec précaution car elle génère des requêtes DNS qui peuvent encombrer le réseau et prendre du temps.

IV Capture des trames

Pour lancer la capture des trames, cliquer sur le bouton « Start ». Durant la capture, une barre de tâches, se trouvant en bas et à gauche de la fenêtre, affiche le récapitulatif des paquets qui sont conservés.

En même temps, les paquets apparaissent dans la fenêtre principale si l'option « Update liste of packets in realtime » a été cochée.

L'appui du bouton « Stop » permet d'arrêter la capture.

L'affichage des résultats se décompose en trois parties :

- Zone 1 : c'est la fenêtre de capture de trames qui comprend les colonnes suivantes :
  - numéro de la trame ;
  - temps écoulé depuis le début de la capture et l'arrivée de la trame ;
  - adresse IP du poste source ;
  - adresse IP du poste destination ;
  - protocole utilisé ;
  - les informations sur la trame.
- Zone 2 : la décomposition de la trame sélectionnée dans la fenêtre de capture de trames. Cette décomposition permet de visualiser les champs des entêtes des protocoles ainsi que l'encapsulation des différentes couches de protocoles selon le modèle OSI.
- Zone 3 : la troisième zone contient le paquet affiché en hexadécimal et en ASCII.

Tout en haut de la fenêtre se trouve un champ « Filter » ; il permet de n'afficher que les trames qui correspondent aux critères spécifiés du filtre d'affichage. Ce filtre permet de cacher temporairement une partie des trames.

V Filtres

Il y a deux sortes de filtres : les filtres de capture et ceux d'affichage.

V.1 Filtres de capture

Ce filtre permet de capturer que des trames pour lesquelles le filtre est vrai. C'est un filtrage a priori.

D'une façon plus générale, ces filtres se décomposent en trois parties :

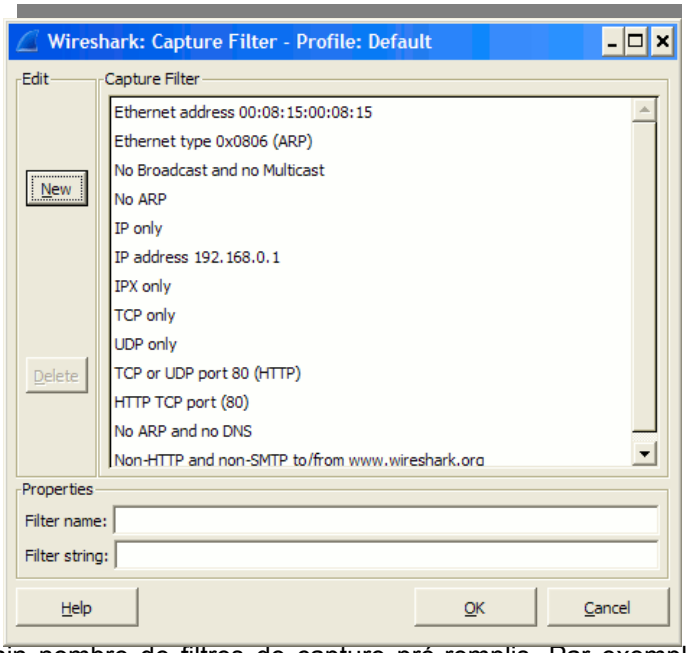
- Le type host, net ou port suivi d'une valeur,
- La direction qui peut être src ou dst,
- Les protocoles ether, fddi, ip, ip6, arp, rarp, decnet, lat, sca, tcp et udp.

Les opérateurs and, or et not peuvent être utilisés pour combiner les 3 parties précédentes.

En règle générale, il faut limiter au maximum le filtrage a priori de façon à disposer du maximum d'informations pour l'analyse.

Si on laisse le champ vide, vous capturez tout le trafic.

En ouvrant le menu de capture (Capture → Options) et en cliquant sur le bouton "Capture Filter", on obtient la fenêtre suivante :



On peut remarquer un certain nombre de filtres de capture pré-remplis. Par exemple, si on clique sur la première entrée "Ethernet address 00:08:15:00:08:15", on retrouve dans le cadre "Properties" cette entrée (sous la valeur "Filter Name", le nom que l'on donne au filtre). Y sera associé le Filter string "ether host 00:08:15:00:08:15", la chaîne de caractères qui permettra de programmer le filtre de capture. Dans notre cas ici, si l'on souhaite ne conserver que les trames dont une des deux adresses mac utilisée pour communiquer est 00:08:15:00:08:15, il faudra taper le filtre de capture "ether host 00:08:15:00:08:15".

Pour ajouter un filtre de capture, il faut lui donner un nom dans l'entrée "Filter name" et une expression dans l'entrée "Filter string". Nous avons un certain nombre d'exemples de filtres de capture. Les plus utiles sont les suivants :

Type de filtrage	Expression de filtrage de capture correspondante (filter string)
Par adresse MAC (physique)	ether host *xx:yy:zz:aa:bb:cc*
Par adresse IP (logique)	host *WWW.XXX.YYY.ZZZ*
Par protocole de couche 4	tcp udp
Par numéro de port	port *numport*

Il est de plus possible de cumuler les filtres avec les mots clef "and" ou "or" et de les inverser avec le mot clef "not".

Exemples de filtre de capture :

Filtre	Fonction
host 172.16.0.1 and tcp	Ne conserve que les paquets tcp à destination ou en provenance de la machine 172.16.0.1
tcp and port 80	Ne conserve que les paquets tcp en provenance ou à destination du port 80
tcp port 80 and dst host 172.16.0.1	Ne conserve que les paquets tcp en provenance ou à destination du port 80 à destination da la machine 172.16.0.1
tcp dst port 80 and dst host 172.16.0.1 and src net 172.16.0.0 mask 255.255.255.0	Ne conserve que les paquets tcp en destination de la machine 172.16.0.1 sur le port 80 et en provenance des machines du réseau 172.16.0.0/24

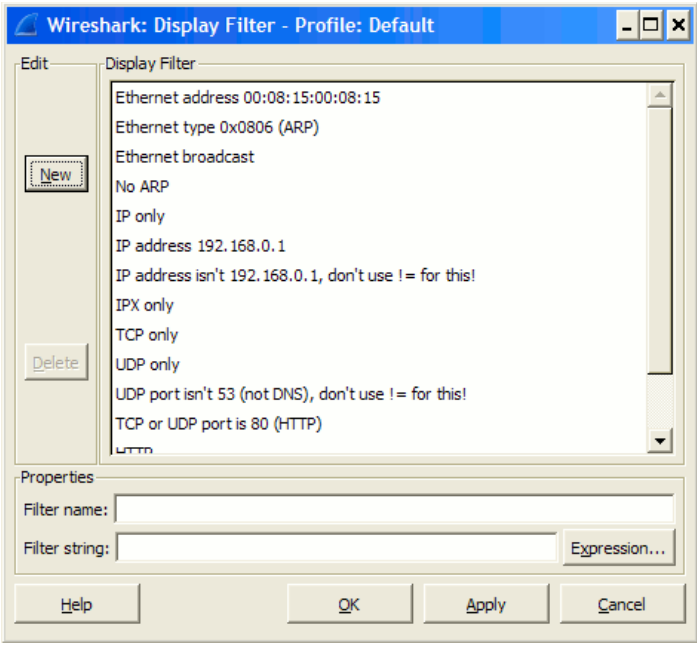
Le filtrage de capture ne peut pas réaliser une inspection en détail des informations contenues dans les trames, car il doit être réalisé en temps réel. Il permet cependant une première sélection des trames. Pour effectuer des filtrages sur des particularités très précises de certains protocoles, il ne faudra pas que cela soit fait lors de la capture, mais sur des trames déjà capturées. On pourrait alors les masquer grâce à un filtre d'affichage.

V.2 Filtres d'affichage

Les filtres d'affichage sont un peu plus fins que ceux de la capture. Ils vont permettre de filtrer les trames en fonction de critères plus évolués que l'adresse MAC, l'adresse IP ou le port. Seules les trames pour lesquelles l'expression du filtre est vraie, seront affichées dans la fenêtre de capture de trames.

Pour ajouter un filtre d'affichage, cliquons sur le bouton "Filter" en haut à gauche de la fenêtre wireshark :

La fenêtre qui apparaît ressemble à celle du filtrage de capture mais n'est pas tout à fait la même :



Par exemple, lorsque l'on clique sur le même filter name que dans le I) "Ethernet address 00:08:15:00:08:15", le filter string est différent et prend pour valeur "eth.addr == 00:08:15:00:08:15". C'est parce que la syntaxe pour le filtre d'affichage n'est pas la même que pour le filtre de capture. Ceci est dû au fait que la capture est réalisée par le programme WinPCap et que donc la syntaxe du filtre de capture est celle utilisée par ce logiciel, alors que l'affichage est réalisé par Wireshark en lui même (qui possède sa syntaxe propre).

On peut aussi utiliser les opérateurs ==, !=, >, <, >= et >= pour comparer les champs avec les valeurs.

Les expressions ainsi fabriquées peuvent être combinées avec les opérateurs && (un et logique), || (ou logique), ^^ (ou exclusif) et ! pour la négation.

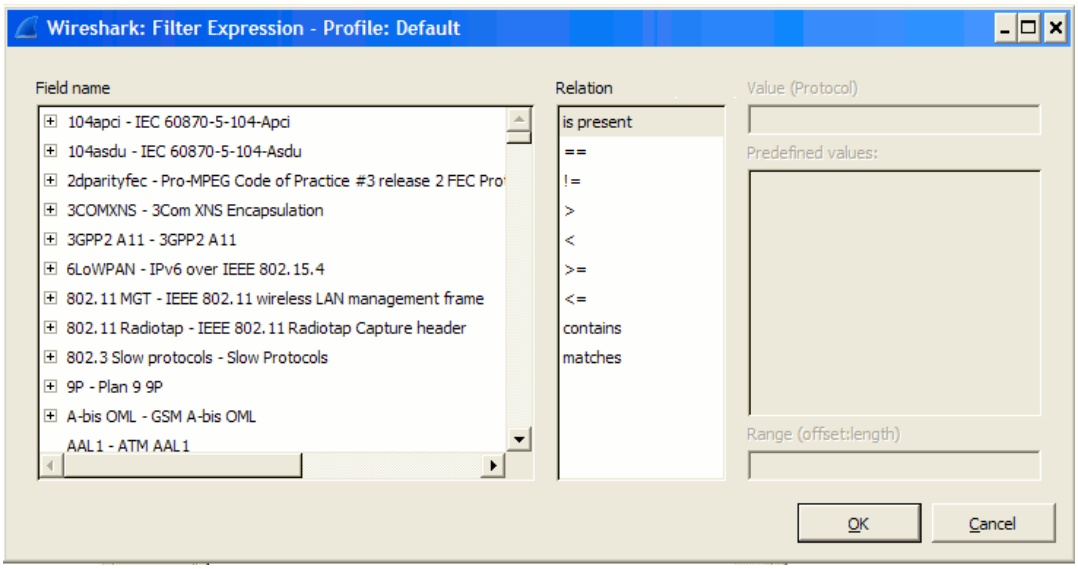
Champs du filtre :

Champ	Type	Signification
ip.addr	Adresse ip v4	Adresse ip 4 octets source ou destination
ip.dst	Adresse ip v4	Adresse ip destination
ip.flags.df	Booléen	Drapeau ip, ne pas fragmenter
ip.flags.mf	Booléen	Drapeau ip, fragments à venir
ip.ttl	Entier non signé sur 8 bits	Time to live
http.request	booléen	Requête http
http.response	Booléen	Réponse http
icmp.code	Entier non signé 8 bits	Numéro de code d'une commande icmp
ftp.request	Booléen	Requête ftp
ftp.request.command	Chaîne de caractères	Commande ftp
ftp.response.data	Chaîne de caractères	Données de transfert ftp

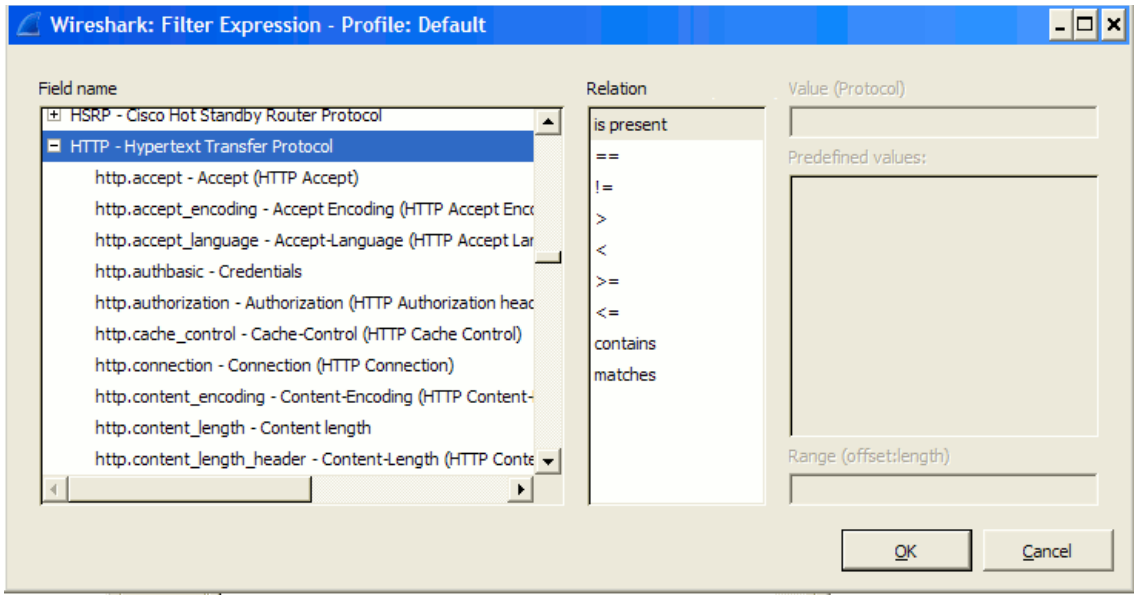
Exemple du champ de filtre d'affichage :

Filtre	Signification
ip.addr == 172.16.0.1	Tous les paquets IP en provenance ou à destination de la machine 172.16.0.1
(ip.addr == 172.16.0.1) && (dns.response)	Tous les paquets IP en provenance ou à destination de la machine 172.16.0.1 qui sont des réponses à des requêtes DNS
(ip.addr >= 172.16.0.1) && (ip.addr <= 172.16.0.123)	Tous les paquets ip en provenance ou à destination des machines comprises entre l'adresse ip 172.16.0.1 et l'adresse 172.16.0.123

Le filtrage d'affichage permet d'utiliser des spécificités de certains protocoles de couche application comme référence de filtrage. Par exemple avec HTTP, il faut cliquer sur le bouton "Expression..." dans la fenêtre des filtres d'affichage. La fenêtre suivante apparaît :



On observe sur la gauche une liste de protocoles (pas uniquement de couche application d'ailleurs!). Il faut trouver le protocole HTTP dans la liste (il suffit de cliquer dans la liste et de taper http pour tomber directement dessus). On obtient la liste suivante :



Pour appliquer un filtre, il suffit de le sélectionner, de sélectionner la relation (le type de condition) et puis éventuellement une valeur de comparaison.

Pour vérifier qu'un champ est présent, il suffit de l'ajouter comme filtre, par exemple, le filtre "http.request" et la relation "is present" permet de ne sélectionner que les requêtes HTTP (les trames envoyées par le client vers le serveur). Vous devriez obtenir une sélection des trames semblable à celle-ci (les adresses IP seront probablement différentes) :