Capture, Filtrage et Analyse de trames ETHERNET avec le logiciel Wireshark

Wireshark est un programme informatique libre de droit, qui permet de capturer et d'analyser les trames d'information qui transitent par les interfaces de communication du terminal sur lequel il s'exécute. *Wireshark* est ainsi apparenté aux logiciels appelés « Sniffer » ou « analyseur de trafic ». Il est multi-OS et téléchargeable sur le site www.wireshark.com.

Avec *Wireshark ,* il est possible de capturer des trames Ethernet en temps réel directement sur les Cartes de communication du terminal, de sauvegarder les résultats de cette capture dans des fichiers qui peuvent être analysés ultérieurement hors ligne. *Wireshark* supporte un très grand nombre de protocoles de communication et de formats de fichiers de capture : Ethernet, ARP, IP, TCP/UDP, HDLC, etc … libpcap/tcpdump, Sun's snoop/atmsnoop, LanAlyzer, MS Network Monitor, HPUX nettl, AIX iptrace, Cisco Secure IDS, etc….

Durant ce TP, nous allons :

1. lancer le programme Wireshark,
2. capturer et analyser une trame Ethernet
3. définir des filtres pour la capture et la visualisation des trames
4. Enregistrer le résultat de cette capture dans un fichier

Etape 1 : Lancement des machines virtuelles VMWARE et de Wireshark

1.1 – Démarrer la machine virtuelle vmware sur votre poste au moyen de la commande suivante :

[user1@machine] $ vmware&

si nécessaire ajouter le chemin aux répertoires etc/sbin et /bin à la variable d'environnement PATH, en tapant la commande suivante :

[user1@machine] $ export PATH= "$PATH":/etc/sbin :/sbin

Lancer la machine virtuelle Serveur (FC5-ServerG) en sélectionnant la machine dans la liste (menu de gauche)

Connectez vous en tant qu'administrateur sur le serveur avec :

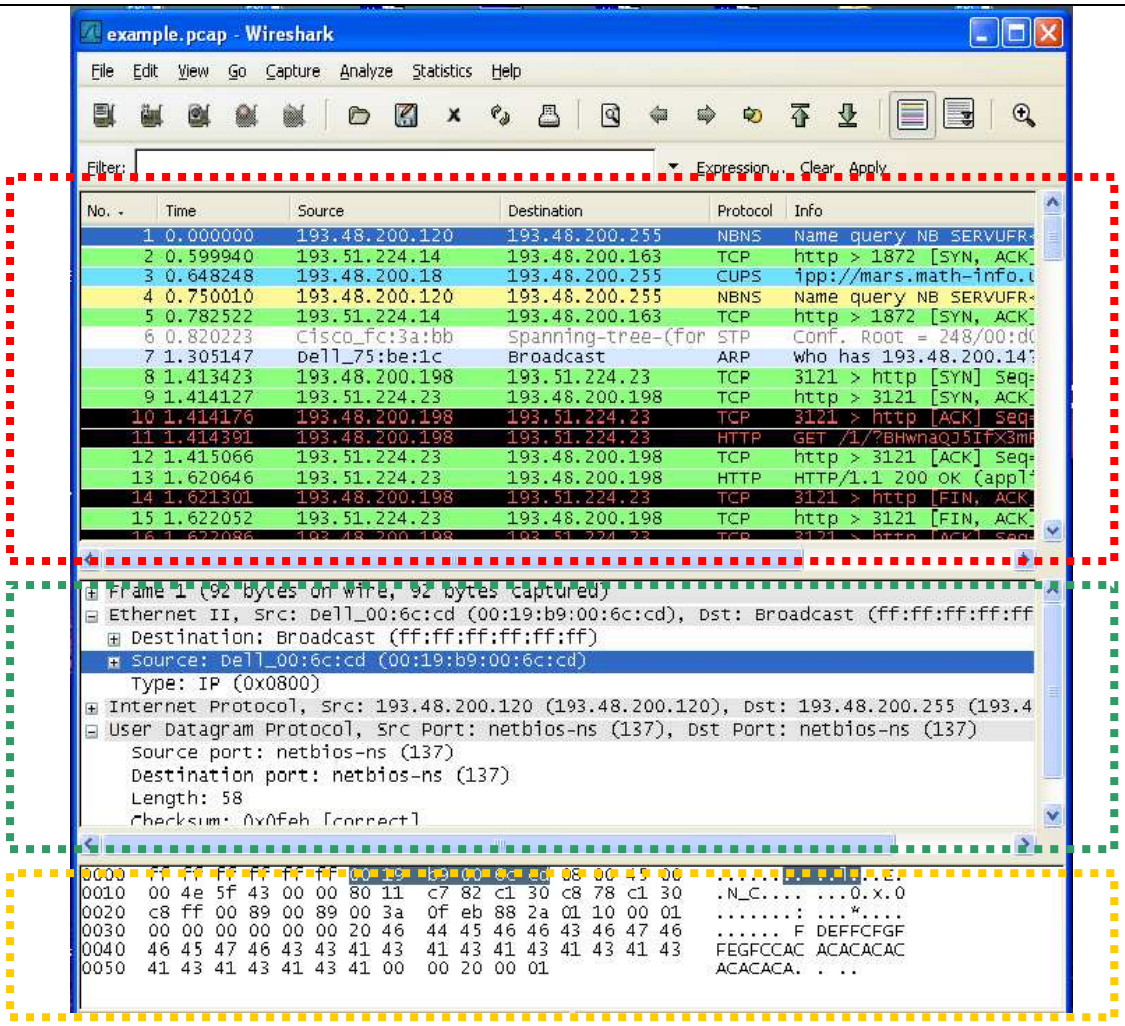
login = root
mot de passe = etu&reseaux

Lancer la machine virtuelle Cliente (FC5-client) en sélectionnant la machine dans la liste (menu de gauche)

Connectez vous en tant qu'administrateur sur le client avec :

login = root
mot de passe = etu&reseaux

1.2 Démarrez ensuite l'application *Wireshark*. Créez un raccourci sur votre bureau il vous sera bien utile. Voila comment le sniffer se présente.



Partie 1

Partie 2

Partie 3

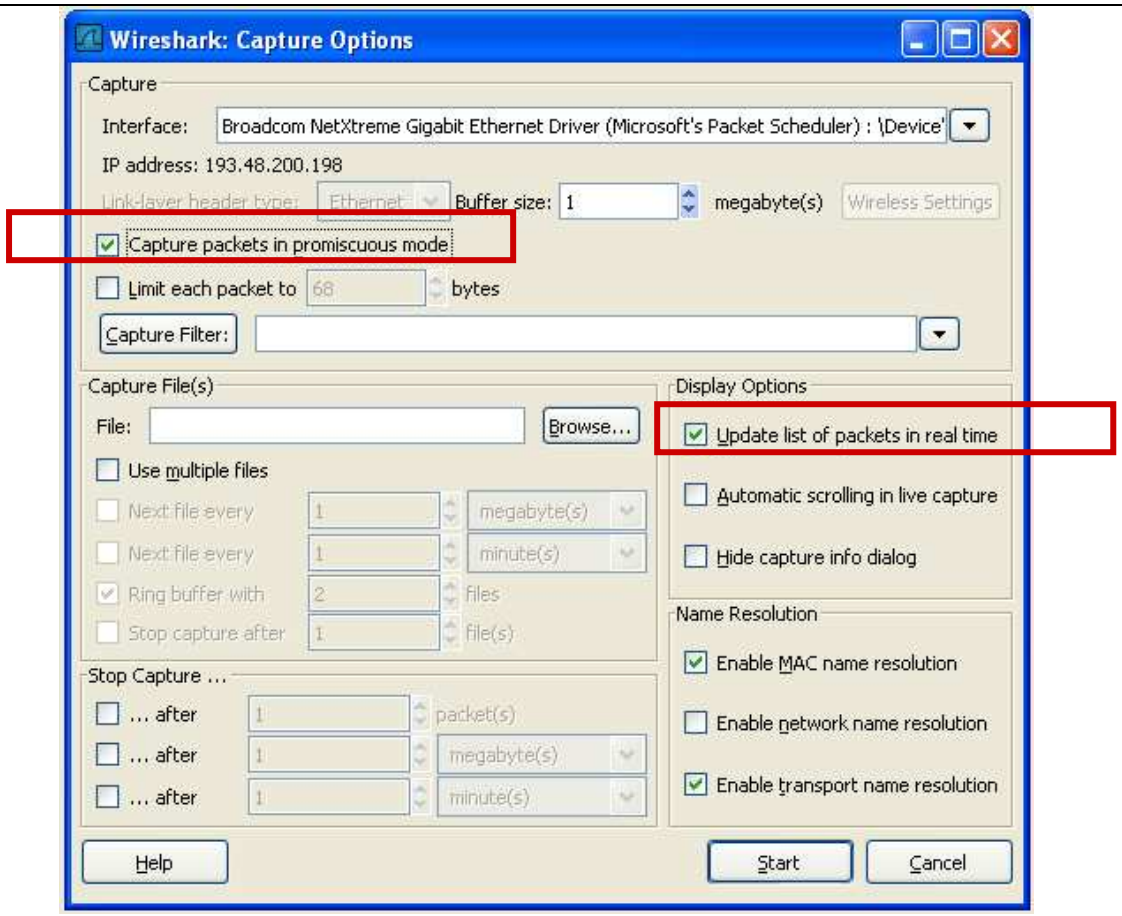
La fenêtre est divisée en trois parties.

1. La **première partie** est de type général, on y trouve des informations de type adresse IP des machines ou encore protocole utilisé lors de l'échange des données.
2. La **deuxième partie** de la fenêtre reprend ici la trame sélectionnée et la détaille soit dans les sept couches du modèles OSI ou dans les quatre couches du modèle IP. Pour plus d'informations à ce sujet des tutoriaux sont disponibles sur le net.
3. La **troisième et dernière partie** est une vision de la trame en codage hexadécimal et ASCII

Nous allons voir maintenant comment capturer les trames sur le réseau sur lequel le sniffer est connecté.

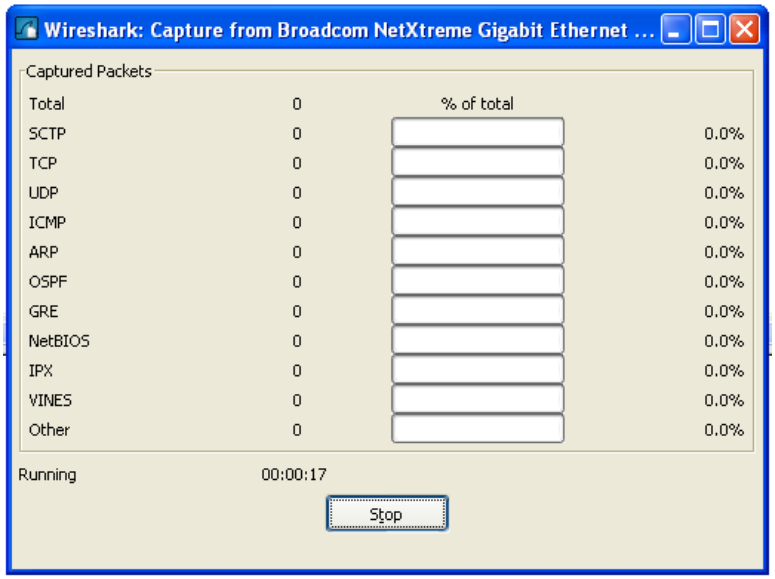
Etape 2 : Capture de trames sur le réseau

Pour capturer les trames sur le réseau, vous devez allez dans le menu *"Capture"* et cliquez sur "Start".
La fenêtre suivante s'ouvre.

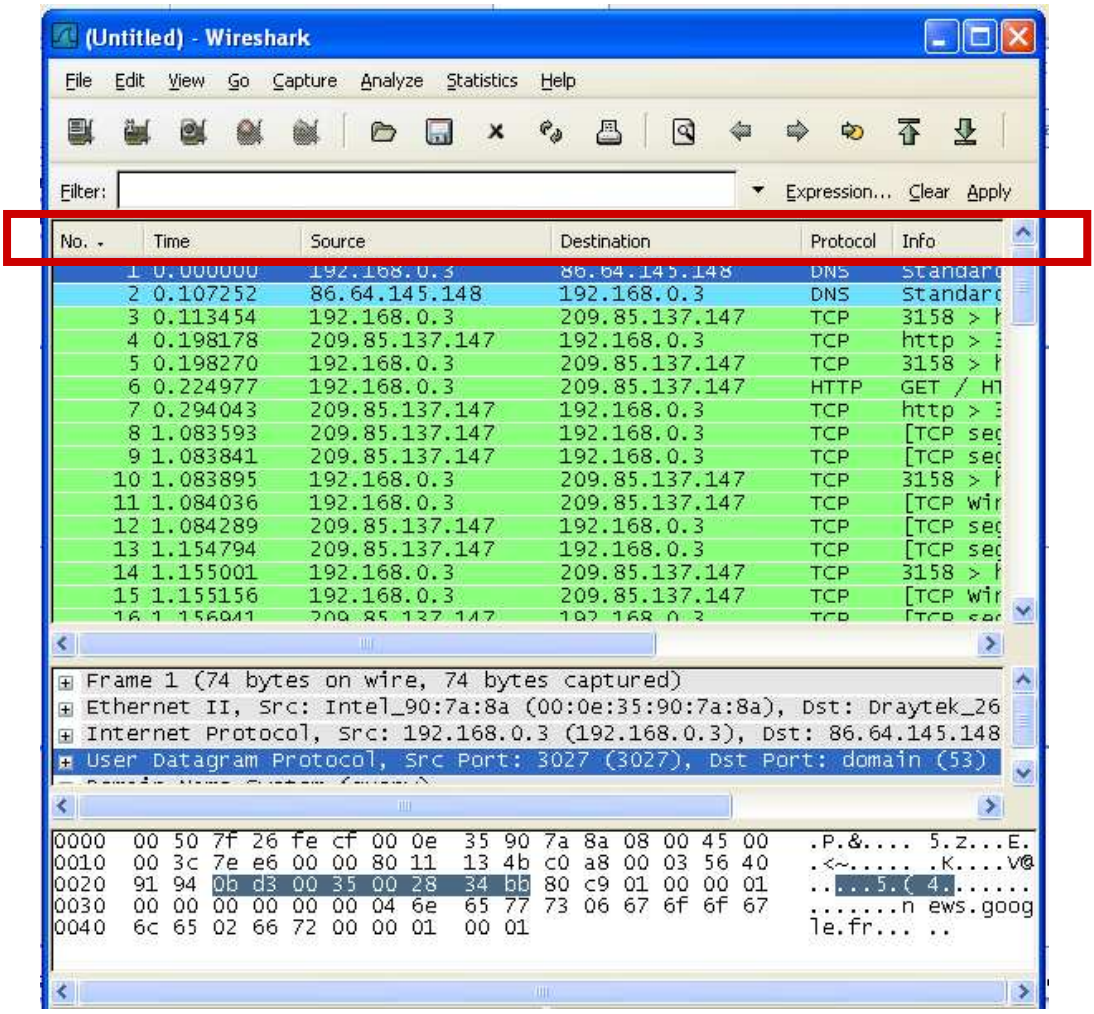


Choisissez l'interface sur laquelle vous voulez "écouter" le trafic. Si vous en avez qu'une le choix ne sera pas très difficile.
Par défaut l'espace réservé à la collecte des données est défini à 1MB. Cela devrait être suffisant. Dans le cas contraire augmentez-le.

Activer l'option **"Capture packets in promiscuous mode"**. Cette option permet à la carte réseau de lire et d'intercepter tout le trafic sur le réseau. Dans le cas contraire celle-ci n'interceptera que les trames qui lui sont destinées et ainsi vous ne verrez pas toutes les trames Multicast et Broadcast.
Laissez le champ "**Capture Filter**" vide dans un premier temps. Nous verrons par la suite comment le remplir. Nous ne toucherons pas non plus aux autres options.
Il ne vous reste plus qu'à démarrer la capture en cliquant sur "OK". La fenêtre suivante s'ouvre.



Capturez environ 30 secondes de trafic entre le poste client et serveur. Puis cliquez sur “Stop”. *Wireshark* va alors afficher les trames capturées par votre carte réseau dans un format lisible ci -dessous.



Sur la première partie de cette fenêtre les différentes trames capturées s’affichent et suivant les colonnes nous avons les informations suivantes:

Première colonne : numéro de la trame.
Deuxième colonne : temps écoulé depuis le départ de la capture et l’arrivée de la trame.
Troisième colonne : adresse IP ou nom de la machine émettrice
Quatrième colonne : adresse IP ou nom de la machine réceptrice
Cinquième colonne : protocole utilisé entre les deux machines
Sixième colonne : informations complémentaires

La quantité de données capturées peut vite devenir considérable, d’autant plus que plusieurs communications peuvent êtres établies en parallèle comme par exemple une connexion à www.google.fr et une autre à www.tplpc.com.
C’est pourquoi nous allons voir comment définir un filtre pour capturer une partie de tout ce que voit la carte réseau.

Etape 3 : Les filtres

Il y a deux sortes de filtres. **Les filtres à la capture** et **les filtres à l'affichage**. Ces filtres n'ont pas la même syntaxe. Pour Unix la syntaxe des filtres à la capture est la même que les filtres utilisés pour la commande tcpdump. Pour en connaitre le format, il faut donc utiliser man tcpdump. Quand aux filtres à l'affichage, la

syntaxe est une syntaxe propriétaire à Wireshark. Pour en connaître la syntaxe, il faut utiliser la commande man wireshark. La section présente donne des exemples pour ces deux types de filtres.

1. Filtres de capture

Ne seront conservés que les paquets pour lesquels le filtre est vrai. Les filtres se décomposent en 3 parties :

- le ***protocole*** à capturer : exemples : ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp ou udp,
- l'identifiant qui peut être src ou dst,
- un champ qui peut être host, net ou port suivi d'une valeur.

Les opérateurs and, or et not peuvent être utilisés pour combiner des filtres.

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
udp port 53	ne conserve que les paquets UDP en provenance ou à destination du port 53
udp port 53 and dst host 172.16.0.1	ne conserve que les paquets UDP en provenance ou à destination du port 53 et à destination de 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 à destination de la machine 172.16.0.1 sur le port 80 et en provenance des machines du sous-réseau 172.16.0/24

2. Filtres d'affichage

Les filtres d'affichage sont un peu plus fins que ceux de la capture. Seuls les paquets pour lesquels l'expression du filtre est vraie seront gardés. Les expressions sont basées sur les champs disponibles dans un paquet. Le simple ajout d'un champ veut dire que l'on garde le paquet si ce champ est disponible. Maintenant, on peut aussi utiliser les opérateurs ==, !=, >, <, >= et <= pour comparer les champs avec des valeurs. Les expressions ainsi fabriquées peuvent être combinées avec les opérateurs && (pour un et logique), || (pour un ou logique), ^^ (pour le ou exclusif) et ! Pour la négation. L'usage des parenthèses est possible.

Voici quelques exemples de champs disponibles

Champ	Type	Signification
ip.addr	adresse IPv4	adresse IP source ou destination
ip.dst	adresse IPv4	adresse IP destination
ip.flags.df	booléen	Drapeau IP, ne pas fragmenter
ip.flags.mf	booléen	Drapeau IP, fragments Ã venir
ip.ttl	entier non signé sur 8 bits	Time to live
nbdgm.src.ip	adresse IPv4	adresse IP source d'un paquet Netbios Datagram
nbdgm.src.port	entier non signé sur 16 bits	port IP source d'un paquet Netbios Datagram
http.request	booléen	requête HTTP
http.response	booléen	réponse HTTP
icmp.code	entier non signé sur 8 bits	numéro du code d'une commande ICMP
icmp.type	entier non signé sur 8 bits	numéro du type d'une commande ICMP
ftp.request	booléen	requête FTP
ftp.request.command	chaine de caractères	commande FTP
ftp.reponse.data	chaine de caractères	donnée de transfer FTP
dns.query	booléen	requête DNS
dns.response	booléen	réponse d'une requête DNS

Voici quelques exemples de filtres

Filtre	Signification
ip.addr == 172.16.0.100	tous les paquets IP en provenance ou Ã destination de la machine

	172.16.0.100
(ip.addr == 172.16.0.100) && (dns.response)	tous les paquets IP en provenance ou Ã destination de la machine 172.16.0.100 qui sont des réponses Ã des requêtes DNS
(ip.addr >= 172.16.0.100) && (ip.addr <= 172.16.0.123)	tous les paquets IP en provenance ou Ã destination des machines comprises entre l'adresse IP 172.16.0.100 et l'adresse IP 172.16.0.123 (comprises)

3. Comment définir un filtre pour la capture des trames (Capture Filter)

Allez dans le menu "Capture". Puis cliquez sur "Capture Filters".La fenêtre suivante s'ouvre.

Considérons que notre machine a l'adresse IP 192.168.1.33.

Nous voulons capturer uniquement les trames échangées entre celle-ci et la machine avec l'adresse IP 145.200.80.45.

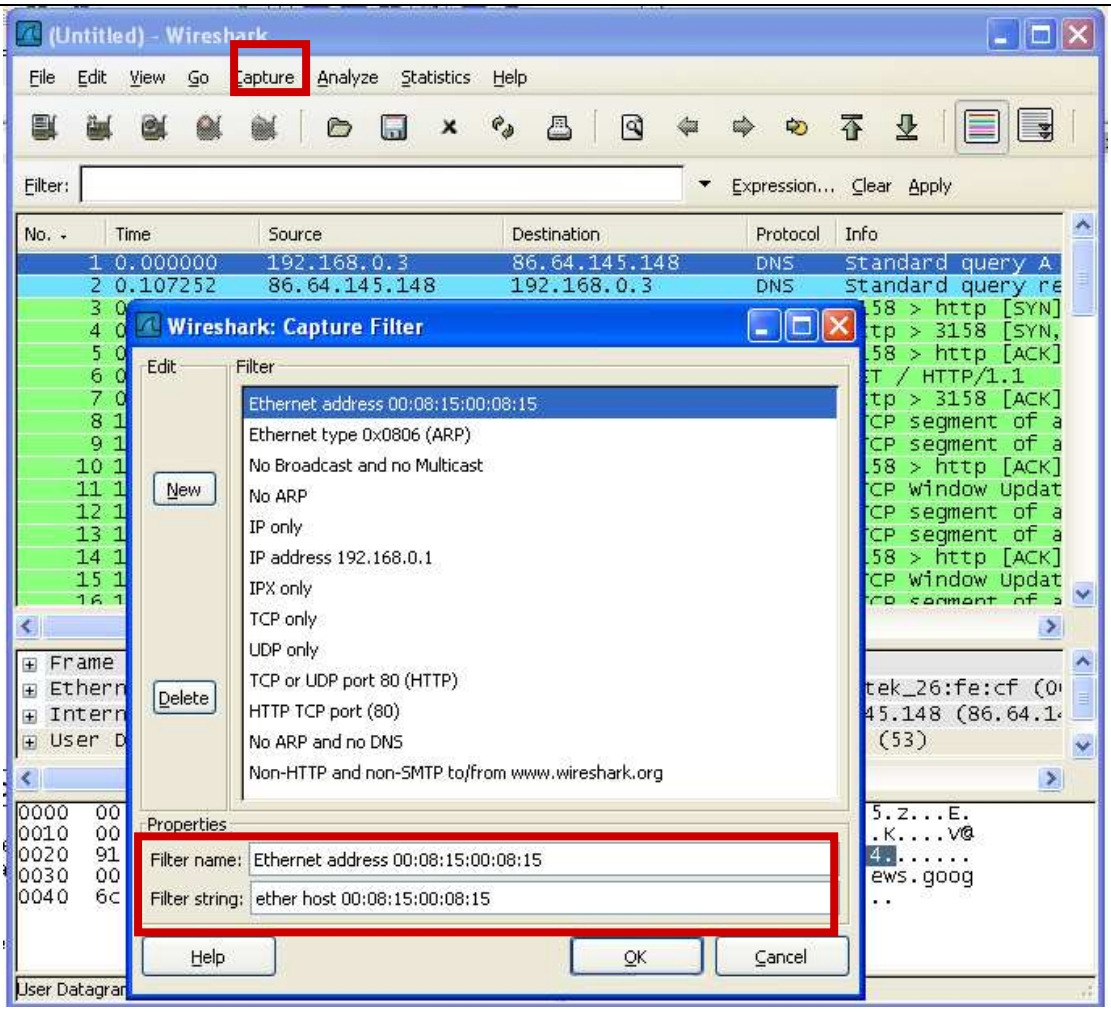
Pour cela cliquez sur "New".

Dans le champ "Filter Name" entrez le nom de votre filtre : mon filtre (par exemple).

Dans le champ "Filter string" entrez la chaîne suivante : host 145.200.80.45. Cliquez maintenant sur "save" et voilà votre filtre est défini vous pouvez cliquez sur "close" pour fermer la fenêtre.

Retournez dans le menu "Capture" et cliquez sur "Start". Reprenez les mêmes options que précédemment. Cliquez sur le bouton "Capture Filter" et sélectionnez votre filtre. Voilà cliquez sur "OK" pour démarrer la capture avec le filtre en question.

Pour plus de détail sur la structure des filtres vous pouvez consulter l'aide en appuyant sur la touche F1 et en allant sur l'onglet "Capture Filter"

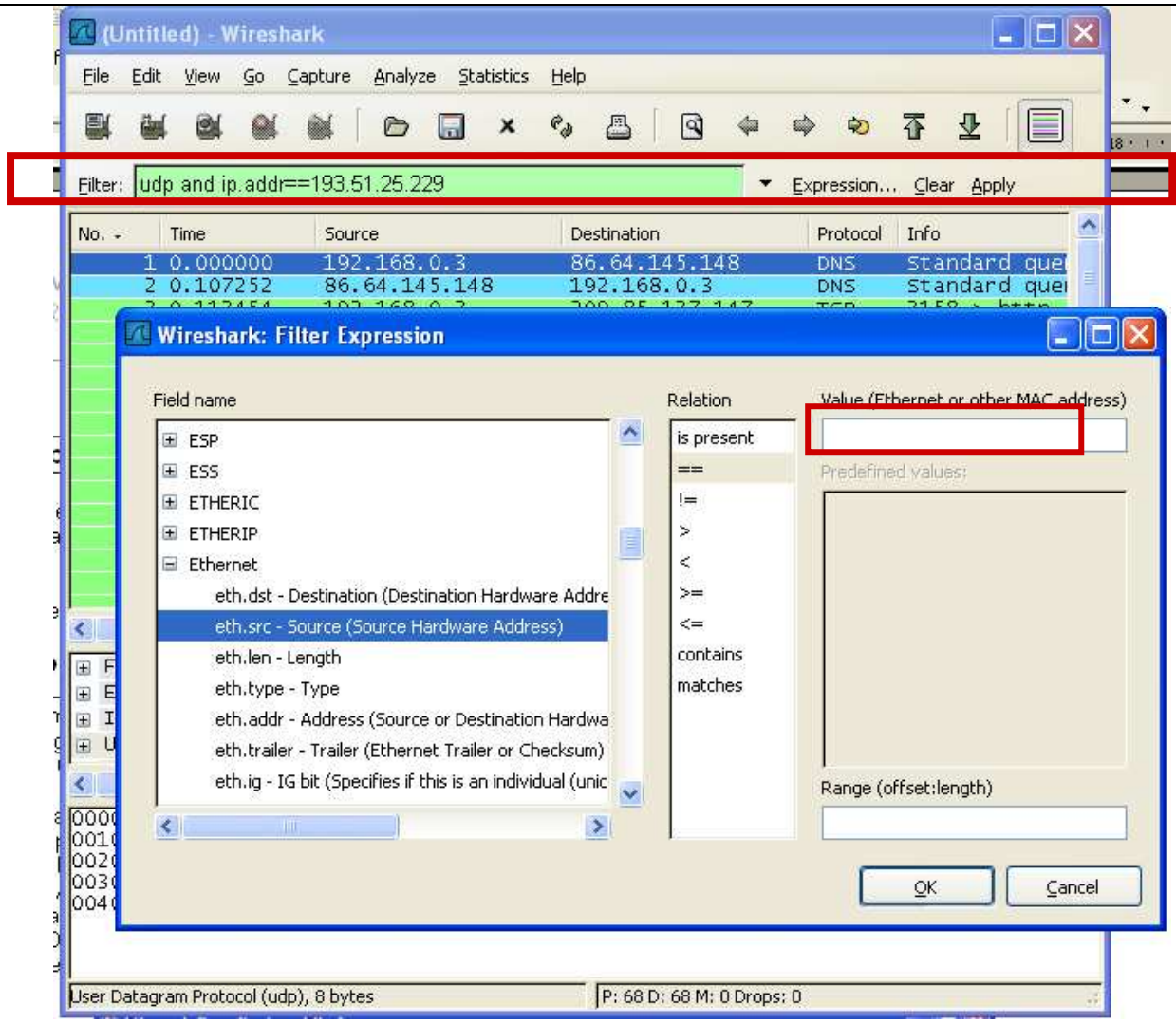


Une autre méthode consiste à capturer toutes les trames dans un premier temps et de filtrer par la suite. L'avantage de cette solution est d'avoir toujours la capture de départ et d'y appliquer par la suite autant de filtres que l'on souhaite. C'est ce que nous allons voir dans le prochain chapitre.

4. Comment définir un filtre pour la visualisation des trames (Display Filter)

Essayons d'appliquer le même filtre que précédemment. Dans un premier temps faites une capture sans appliquer de filtre (reportez vous au premier paragraphe). Stoppez la capture. Allez sur la barre FILTER et sélectionner « EXRESSION ». une fenêtre s'ouvre vous permettant de rédiger des flitres d'affichage
Par exemple on sélectionne le protocole Ethernet et l'adresse source. On tape la chaîne suivante : eth.src==12:23:45:67:34 5A et on valide. Voilà le filtre d'affichage est appliquez. Si vous voulez le sauvegarder cliquez sur "Save".

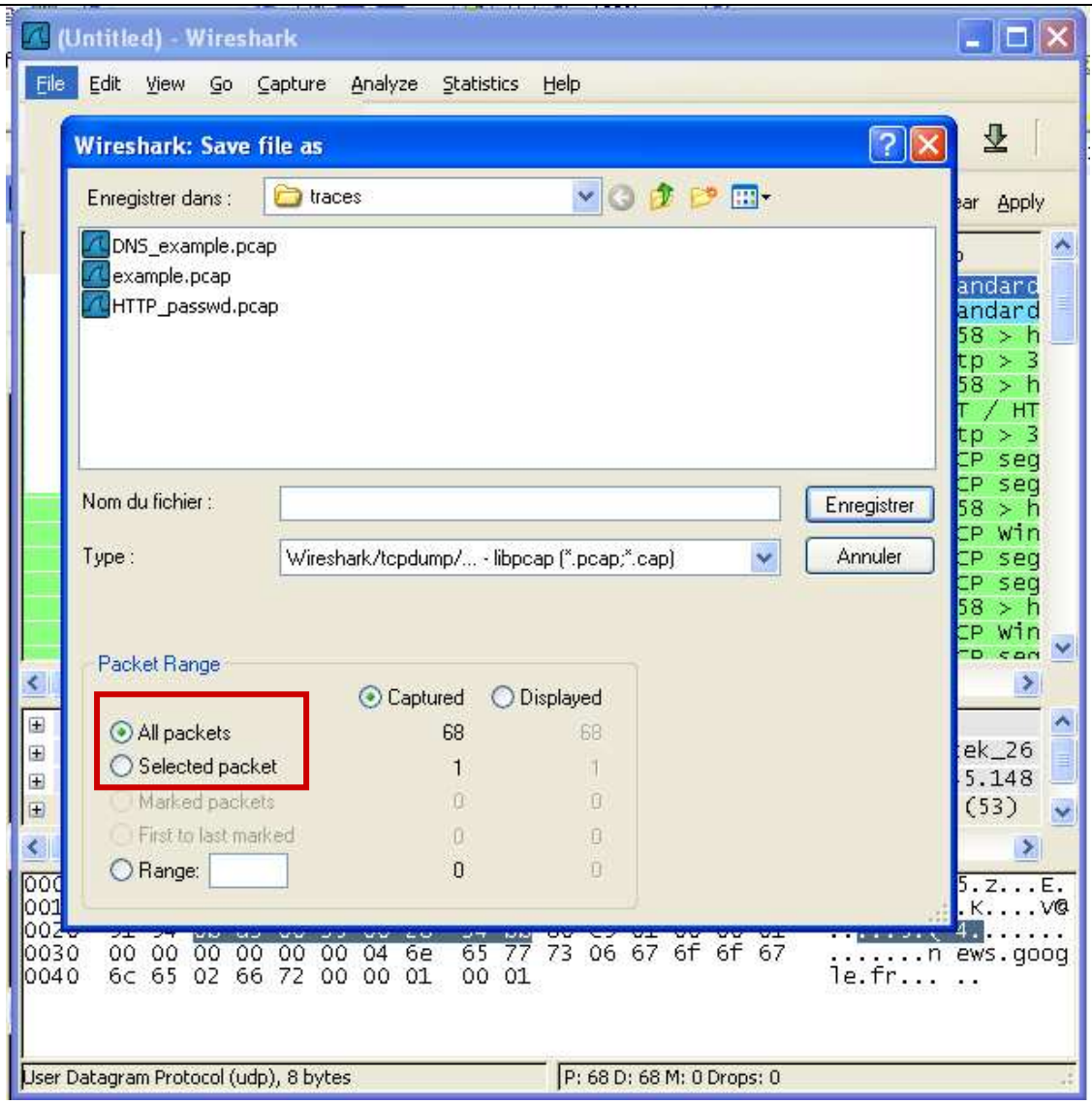
Si maintenant vous voulez l'annuler, effacez la chaîne dans le champ "Filter string" ou cliquer sur « CLEAR ».



Etape 4 : sauvegarde d'un résultat de capture

Pour sauvegarder le résultat d'une capture dans un fichier, il faut sélectionner la commande « Save as » dans le menu « File ». Une fenêtre nous proposer de choisir le répertoire et le nom du fichier, ainsi que le format/type de fichier de sauvegarde (conserver le format par défaut libpcap).

Pour n'enregistrer qu'une trame ou un une sélection de trames, vous avez a votre disposition ces options dans le menu « Packet Range ».



Etape 5 : Répondre aux questions suivantes :

5.1 Lancer les machines virtuelles client et Serveur
5.2 taper sur la console du serveur la commande « ifconfig » (voir le manuel man pour la syntaxe de la commande ifconfig). Identifier les adresses Ethernet du serveur. Identifier les adresses IP du serveur. Réitérer la même opération avec le poste client.
5.3 sur le poste Serveur, lancer le logiciel Wireshark sur votre interface Ethernet (eth0),
5.4 sur le poste client, taper une commande de type « ping » à destination du serveur et capturer environ 30 secondes de trafic sur le poste serveur (voir le manuel man pour la syntaxe de la commande ping). Enregistrer le résultat dans un fichier « test ».
5.5 Combien de trames avez-vous capturé ?
5.6 Analyser la première trame Ethernet et reporter les valeurs des champs de contrôle de cette trame dans un tableau. Quelle information cette trame transporte t elle ?
5.7 Recherchez sur Internet le document RFC 1700. Quelle information mentionne t il en relation avec la trame Ethernet ?
5.8 Au moyen des filtres d'affichage sélectionner uniquement les trames dont l'émetteur est le poste client (sur la base de son adresse Ethernet).
5.9 Décrivez la procédure (commandes systèmes, filtres wireshark) permettant de capturer et de filtrer les trames Ethernet transportant uniquement un paquet ARP ayant pour origine (émission) le poste serveur.