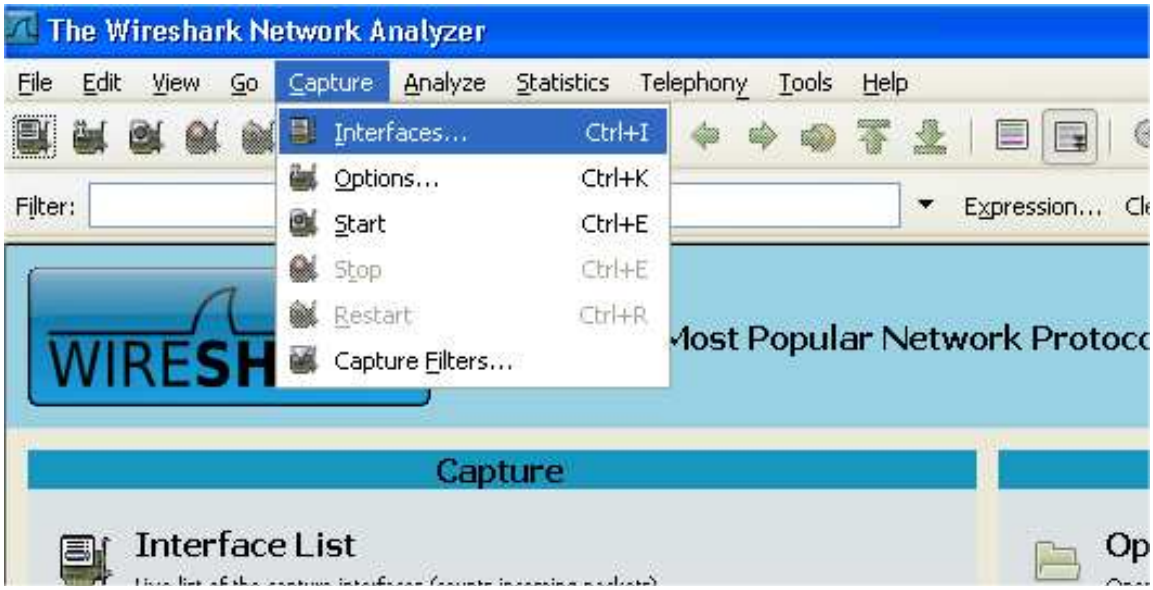
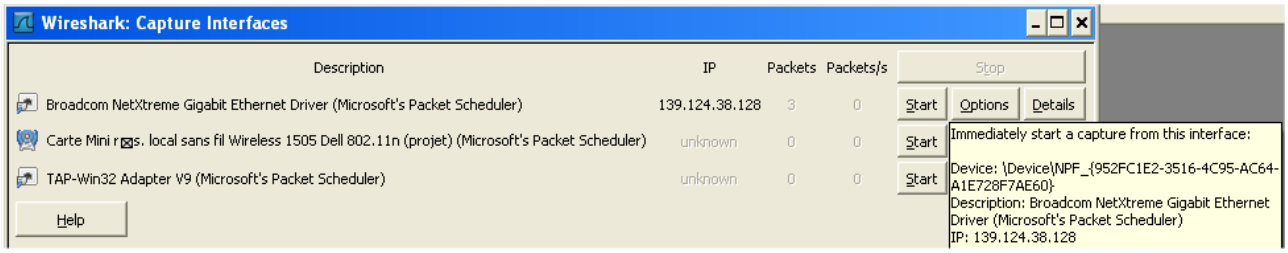
DECOUVERTE ET UTILISATION DE WIRESHARK

I) Wireshark

Depuis le menu Demarrer, lancer l'appliaction Wireshark. Vous devriez voir apparaître une fenêtre similaire à celle-ci :

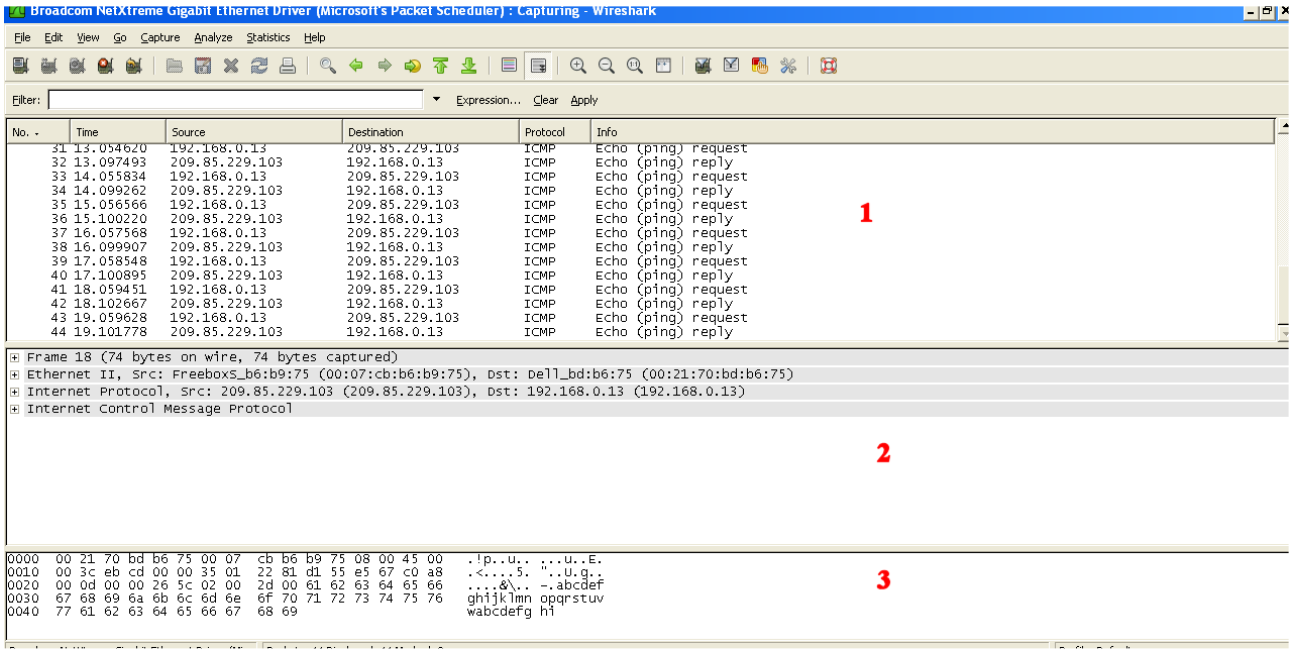


Dans le menu `capture`, sélectionner le sous-menu `Interfaces` et lancer une capture de trame. sur la carte réseau portant votre adresse IP et appuyer sur `Start`



Une fois la capture lancée, ouvrez une fenetre de commande DOS (menu Demarrer - > Exécuter -> cmd), et lancer un ping sur `www.google.fr`. Quand le ping s'arrête, arrêter la capture en cliquant sur l'icône adéquate (voir image ci-dessous).

Résultat d'une capture
Une fois la capture effectuée, vous obtiendrez la fenêtre suivante :



L'affichage des résultats se décompose en trois parties :

1) la liste des paquets capturés disponibles en dessous de la barre de menu avec un affichage synthétique du contenu de chaque paquet.
2) la décomposition exacte du paquet actuellement sélectionné dans la liste. Cette décomposition permet de visualiser les champs des entêtes des protocoles ainsi que l'imbrication des différentes couches de protocoles connus.
3) La troisième zone contient la capture affichée en hexadécimal et en ASCII.

Chaque ligne de la liste des paquets (premier volet) correspond à une PDU de données capturées. Si vous sélectionnez une ligne dans ce volet, ses détails s'affichent dans les volets du milieu et inférieur.

Le volet du milieu affiche les détails de ce paquet. Les protocoles et les champs de protocole du paquet sélectionné sont indiqués. Ils s'affichent sous la forme d'une arborescence que vous pouvez développer ou réduire.

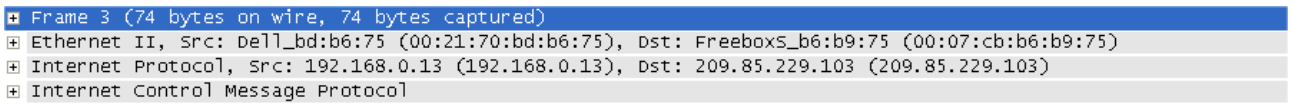
II) Analyse de la capture du ping

Observez la liste des paquets capturés et réponder aux questions suivantes :

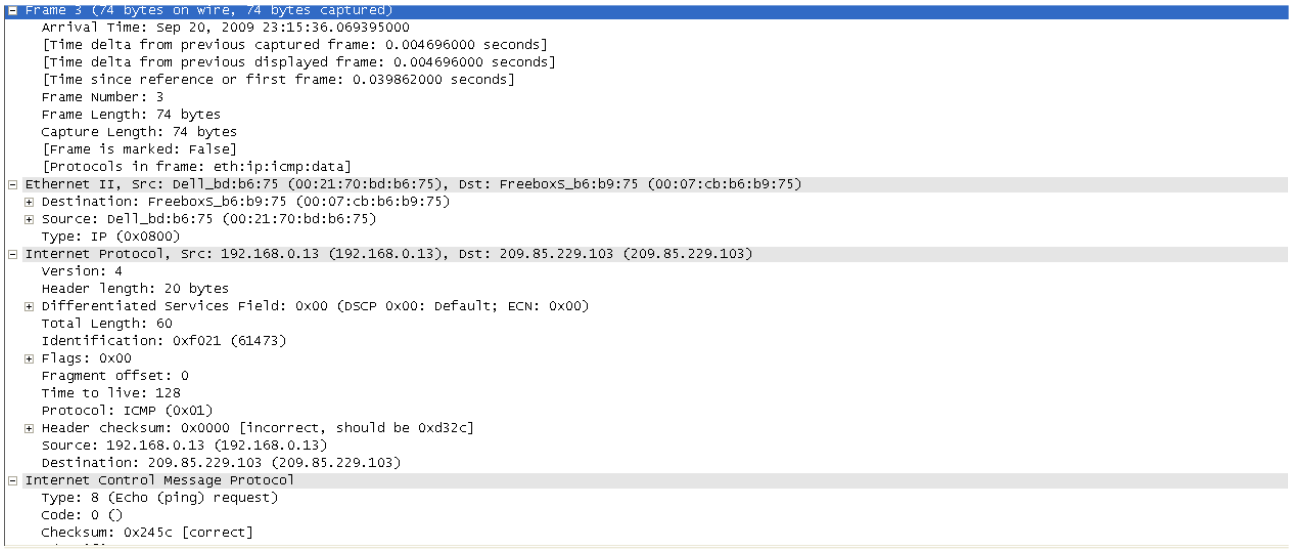
a) Avez-vous capturé un échange avec le DNS ?
Pourquoi votre ordinateur a t-il interrogé le DNS ?

b) Quels sont les deux types de messages "ping" que vous avez capturés ?

Dans la première fenêtre, sélectionner une trame contenant une requête écho (`echo ping request`). Le volet du milieu affiche des informations détaillées sur le paquet semblables à celles-ci :



Cliquez sur les quatre signes « + » pour développer les arborescences correspondantes.



Comme vous pourrez le constater, il est possible de développer encore chaque section et protocole. Consacrez un peu de temps à l'étude de ces informations même si vous ne comprenez pas encore toutes les informations affichées.

a) Localisez deux types d'adresses « Source » et « Destination » différents.

   A quelles couches ces adresses appartiennent-elles ?

b) Parmi les encapsulations suivantes, laquelle correspond à ce que vous voyez dans la capture ?

   [message ICMP [paquet IP[trame ethernet]]]

   [paquet IP [trame ethernet [message ICMP]]]

   [trame ethernet [paquet IP[message ICMP]]]

   [message ICMP [trame ethernet [paquet IP]]]

c) A quelle couche du modèle OSI se situent les protocoles ICMP, IP et Ethernet ?

Sélectionnez maintenant une trame contenant la réponse à votre requête DNS.

a) Quel est le nom complet du protocole DNS ?

b) Quel protocole de la couche transport est utilisé par le DNS ?

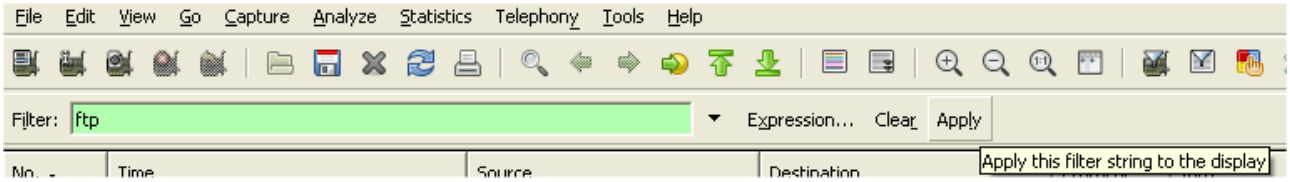
c) Ecrire l'encapsulation utilisée pour transporter une requête DNS

d) Dans la réponse du DNS, retrouvez l'adresse IP du site www.google.fr ?

III) Analyse d'un trafic `ftp`

Lancez une capture de trames. Depuis la Console, lancez la commande `ftp dl.free.fr` (le username est `essai@free.fr`, et le password est celui que vous voulez). Une fois connecté sur le serveur, tapez la commande `quit` et arrêtez alors la capture.

Nous allons maintenant utilisez un filtre d'affichage pour n'afficher que les trames relatives au protocole `ftp`. Pour cela, dans le champ `Filter`, vous allez saisir `ftp` puis cliquez sur `Apply`.



En observant la première trame du protocole `ftp`, et en détaillant les PDU dans la deuxième fenêtre, répondez aux questions suivantes :

a) Dans le PDU de la couche réseau, quelle est la valeur du champ `Time to Live` ? Chercher sur internet à quoi ce champ peut-il servir ?

b) Dans le PDU de la couche réseau, quelle est la valeur du champ `Protocol`? Chercher sur internet à quoi ce champ peut-il servir ?

c) Quel est le protocole de la couche transport utilisé par `ftp` ?

d) Existe-t-il dans le PDU de la couche transport, un champ contenant le numéro du segment ?

e) Existe-t-il dans le PDU de la couche transport, un champ nommé `Flag` ?
Quelles sont les valeurs possibles de ce champ ?

f) Examinez la totalité de la capture, en portant votre attention sur l'affichage en ASCII, et retrouver le mot de passe saisi[1].

g) Quel équipement d'infrastructure vous permettrez de capturer, à partir de votre machine, un mot de passe saisi par l'un de vos voisins ? Justifiez.

[1] Si jamais vous n'y arrivez pas, sélectionnez n'importe quelle trame `ftp`, puis dans le menu `Analyse`, lancez la commande `Follow TCP Stream`. Magique non !!!!

IV) Analyse d'un trafic facebook

Lancez une capture de trames. Ouvrez alors un navigateur et connectez vous à votre compte facebook (Attention, il ne s'agit pas d'y passer des heures !!!). Une fois que vous êtes connecté, arrêtez la capture de trame et répondez aux questions suivantes :

a) Existe t-il dans la capture une trame dont le protocole est TLSv1 ?

b) En observant cette trame déterminer ?
- l'adresse IP du serveur hébergeant facebook ?
- le protocole de couche réseau utilisé ?
- le protocole de couche transport utilisé ?
- le protocole de la couche application utilisé ?

c) En interrogeant le DNS, vérifiez que l'adresse IP trouvée à la question précédente correspond bien au serveur de facebook ?

d) Donnez le développé des acronymes SSL et TLS ?

e) Retrouve t-on, comme dans l'exercice précédent, le mot de passe en clair dans l'échange ? Pourquoi ?

V) Analyse d'un trafic DNS

Lancez une capture de trames. Depuis la Console, lancez la commande `nslookup 66.220.153.11`. Une fois la réponse obtenue, arrêtez la capture, tapez dans le champ `Filter` le protocole `dns` (n'oubliez pas de faire `Apply`) et répondez aux questions suivantes :

a) Quelle est l'adresse IP du DNS ?

b) Quel est le protocole de la couche transport utilisé par le `DNS` ?

c) Quels sont les deux types de trames possible pour le protocole DNS ?

d) Sur la première trame déterminer la valeur des champs :
- @IP Src @IP Dst
- Src Port Dst Port

e) Sur la deuxième trame, déterminer la valeur des champs :
- @IP Src @IP Dst
- Src Port Dst Port

Que constatez vous ?