Institut Universitaire de Technologie
Aix*Marseille Université

Réseaux & Télécoms

TP – INITIATION AUX RESEAUX D'ENTREPRISE

DECOUVERTE ET UTILISATION DE WIRESHARK

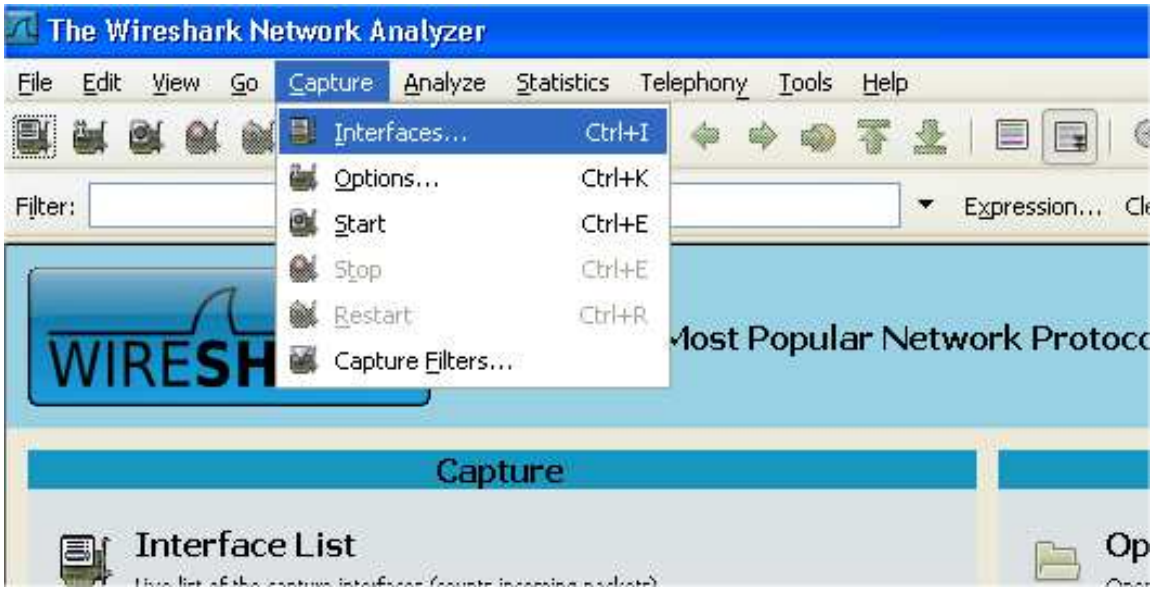
I) Bon à savoir

L'adresse MAC de votre passerelle est : 00:23:89:40:27:82

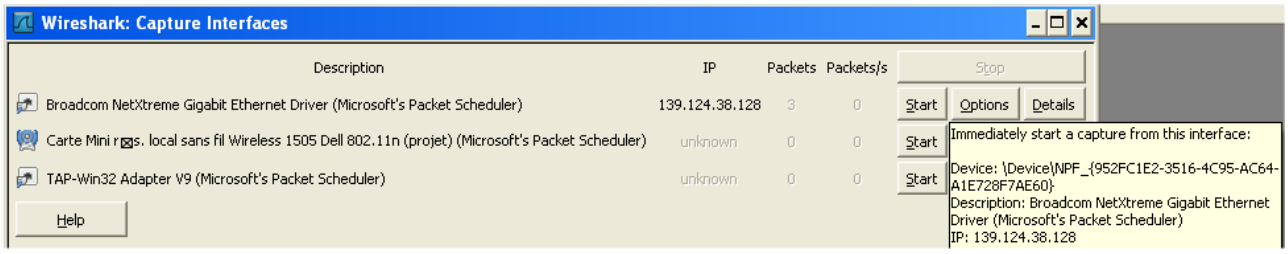
L'adresse IP de votre passerelle est : 139.124.87.1

II) Wireshark

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

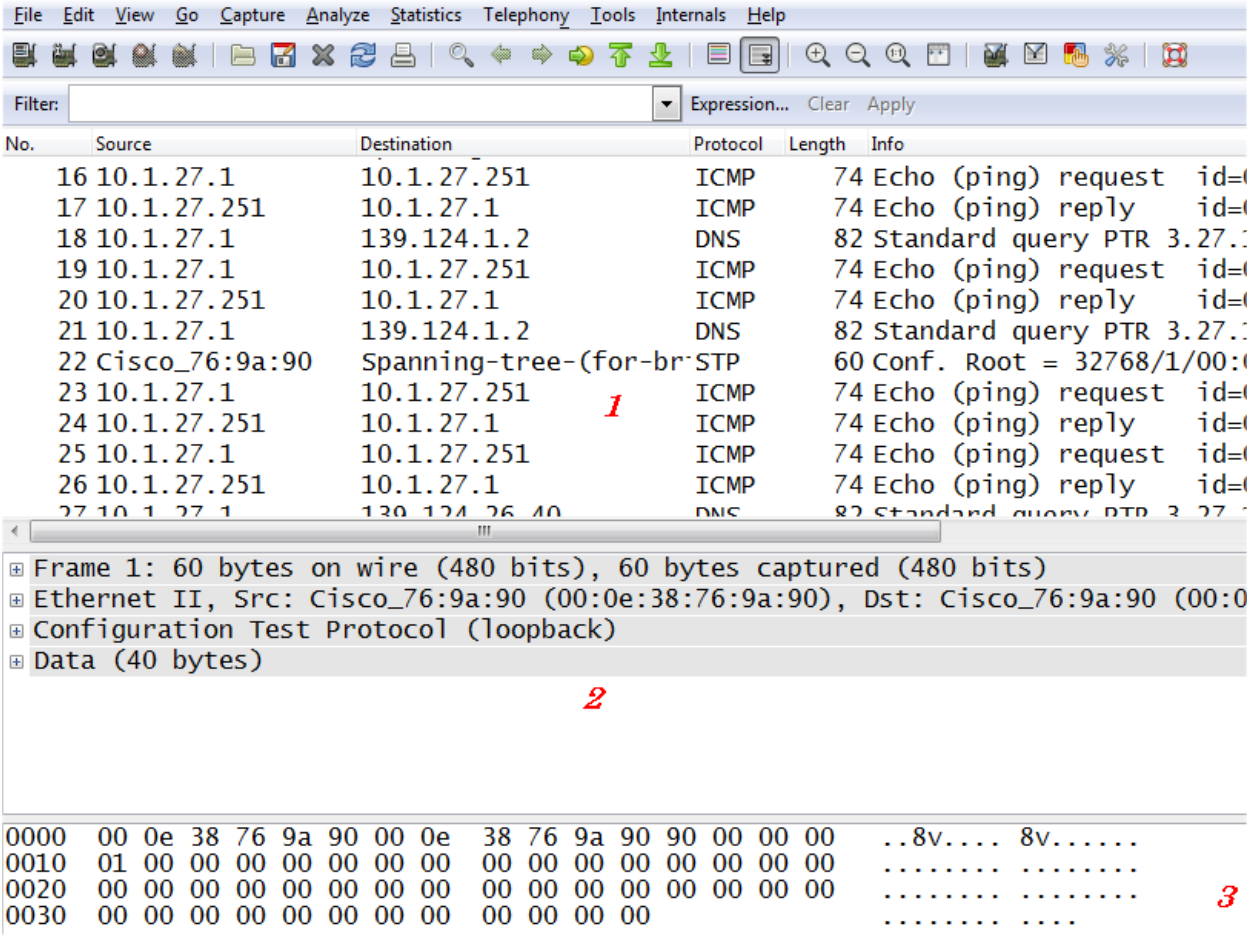


Dans le menu `capture`, sélectionner le sous-menu `Interfaces` puis lancer une capture sur la carte réseau portant votre adresse IP en appuyant sur `Start`



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

Résultat d'une capture
Votre capture est effectuée et vous obtenez la fenêtre suivante :



L'affichage des résultats se décompose en trois parties :

- ⇨ ① la liste des message capturés avec un affichage synthétique du contenu de chaque message ;
- ⇨ ② zone contenant la décomposition exacte du message actuellement sélectionné dans la liste précédente. Cette décomposition permet de visualiser les PDU de chaque couche qui s'affichent sous la forme d'une arborescence que vous pouvez développer ou réduire.
- ⇨ ③ zone contenant la capture affichée en hexadécimal et en ASCII.

Que signifie mot PDU ? [1]

III) Analyse de la capture du ping

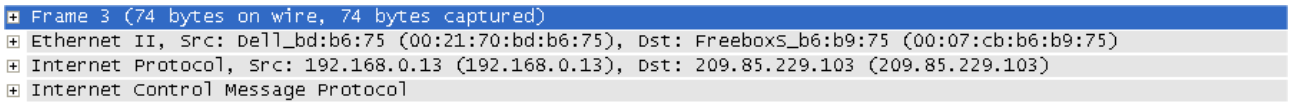
Observez la liste des message capturés et répondre aux questions suivantes :

a) Avez-vous capturé un échange avec le DNS dont l'adresse IP source est celle de votre machine ? Pourquoi votre ordinateur a t-il interrogé le DNS ?

[1] Lors de votre recherche sur internet, associez les mots PDU et réseau.

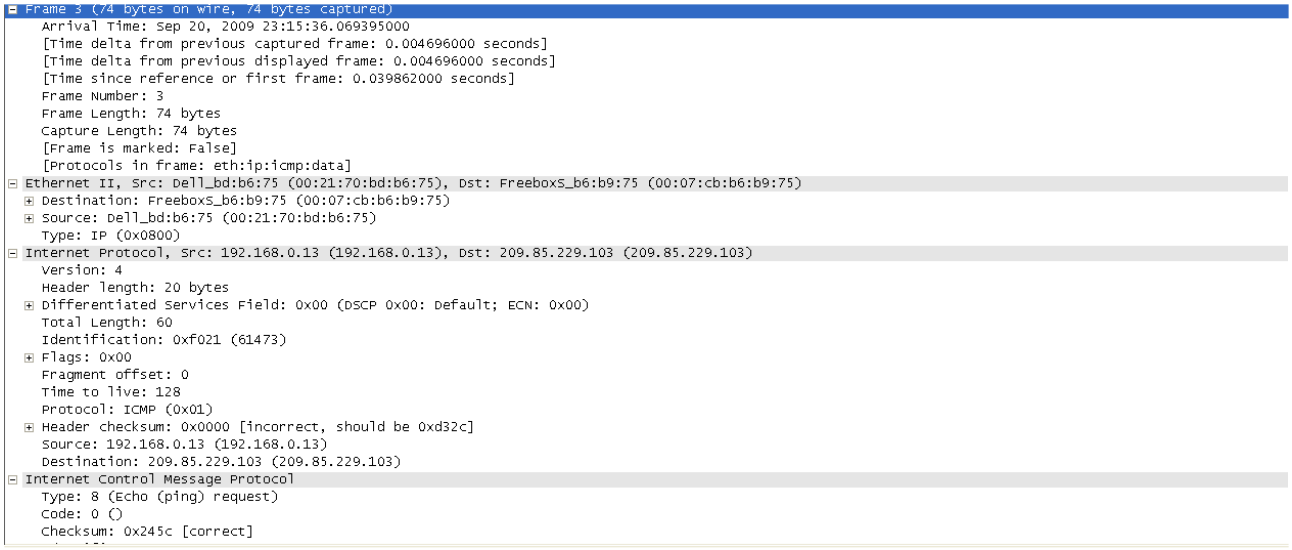
b) En observant la colonne `Info`, donnez les deux types de messages ICMP que vous avez capturés ?

Sélectionnez dans la première fenêtre un message contenant une requête `Echo ping request`. Le volet du milieu affiche des informations détaillées sur le message semblables à celles-ci :



Ce que vous voyez correspond à l'encapsulation des protocoles utilisés. Ici dans une trame Ethernet, il y a un paquet IP, qui lui même contient un message ICMP. Nous pouvons schématiser cela par écrit de la sorte`[Ethernet[IP[ICMP]]]`

Comme vous pourrez le constater, il est possible de développer encore chaque section et protocole en cliquant sur les quatre signes « + ».



Nous allons consacrez un peu de temps à l'étude de ces informations même si vous ne les comprenez pas encore toutes.

Dans le PDU Ethernet :

a) Retrouvez les adresses MAC « Source » et « Destination » qui ont été utilisées.
@MAC src @MAC dst

b) L'adresse MAC de destination correspond-t-elle à l'adresse MAC de la passerelle ?

c) Rechercher sur internet le rôle du champ `Type`

d) Quelle est la valeur du champ `Type` ?

Dans le PDU Internet Protocol :

a) Retrouvez les adresses IP « Source » et « Destination » qui ont été utilisées.
@IP src @IP dst

b) L'adresse IP de destination correspond-t-elle à l'adresse IP de la passerelle ?

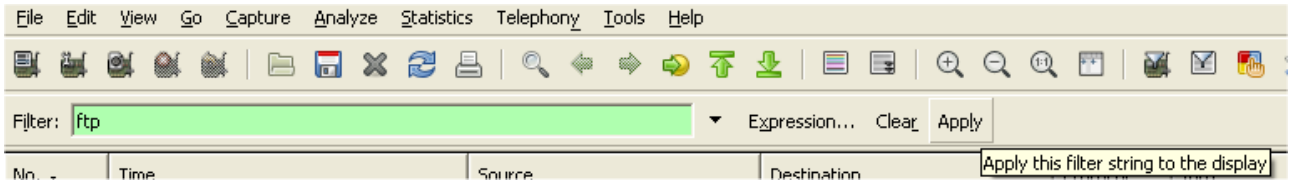
c) Rechercher sur internet le rôle du champ `Protocol`

d) Quelle est la valeur du champ `Protocol` ?

IV) Analyse d'un trafic `ftp`

Lancez une capture et depuis la Console tapez la commande `ftp dl.free.fr` (le `username` est une adresse mail valide de votre choix, et le `password` est celui que vous voulez). Une fois connecté sur le serveur de free, tapez un `?` pour afficher les commandes disponibles utilisez la commande `quit`) pour mettre fin à la session. Arrêtez 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 les messages sélectionnés par le filtre et/ou en détaillant les PDUs dans la deuxième fenêtre, répondez aux questions suivantes :

a) Retrouver le login et le mot de passe saisi[2].

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

c) Quelle est l'encapsulation des protocoles utilisés ?

V) 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 :

[2] 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 !!!!

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 ?

c) Donnez le sens des acronymes SSL et TLS ?

SSL :
TLS :

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

e) Quelle est l'encapsulation des protocoles utilisés ?

VI) Analyse d'un trafic DNS

Lancez une capture de trames et depuis la Console, lancez la commande `nslookup www.jldamoiseaux.fr` . 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) A quoi correspond l'acronyme DNS ?

b) Quelle est l'adresse IP du serveur DNS ?

c) Dans la réponse du DNS, retrouvez (en cliquant sur les +) le nom du site dont l'adresse IP est `131.253.33.200`

En ouvrant un navigateur, et en tapant dans la barre de navigation cette adresse IP, vérifiez que l'on arrive bien sur ce site

d) Quels sont les deux types de trames possibles pour le protocole DNS ?

e) Sur la première trame déterminer la valeur des champs :

@IP Src	@IP Dst
Src Port	Dst Port

f) Sur la deuxième trame, déterminer la valeur des champs :

@IP Src	@IP D
Src Port	Dst Port

Que constatez vous ?

g) Quelle est l'encapsulation des protocoles utilisés ?