

## UTILISATION DE L'OUTIL DE CAPTURE DE TRAMES WIRESHARK

## I- Présentation

Dans ce TD vous apprendrez à utiliser un logiciel de capture de trames et apprendrez à détecter et analyser quelques uns des protocoles les plus couramment utilisés dans les réseaux informatiques.

## II- Le logiciel de capture de trames Wireshark

Le logiciel de capture de trames Wireshark permet de configurer une interface réseau d'un ordinateur en mode Promiscuous. Dans ce mode, le filtre qui vérifie à partir de l'adresse mac de destination d'une trame du réseau si elle est destinée à votre ordinateur est désactivé (c'est-à-dire si elle est identique à celle de la carte réseau de votre ordinateur).

Ceci permet de capturer toutes les trames du réseau que l'interface de votre ordinateur voit passer (Figure 1). Autrement dit, toutes les trames du domaine de collision/diffusion de votre ordinateur. Quand un ordinateur dispose de plusieurs interface réseau Wireshark permet aussi de sélectionner l'interface sur laquelle on veut réaliser une capture de trames.

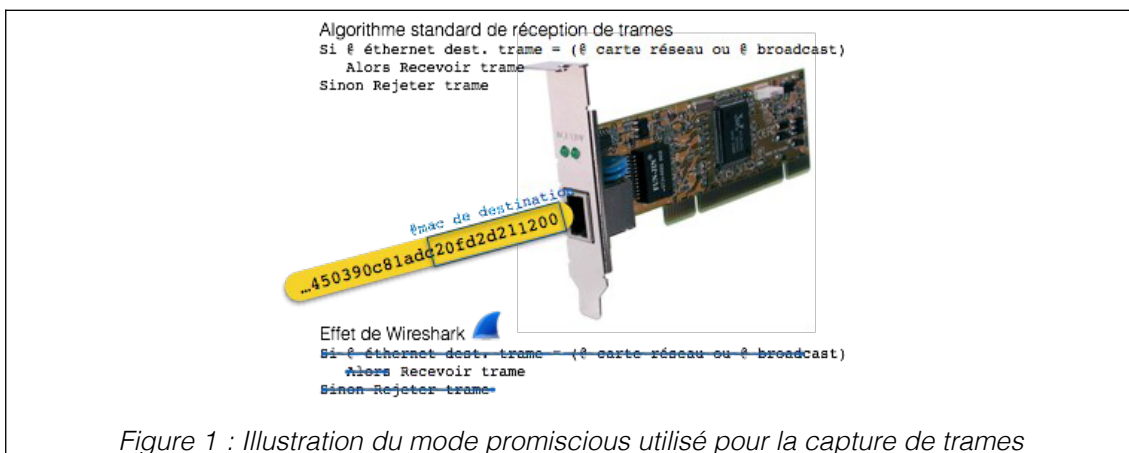


Figure 1 : Illustration du mode promiscuous utilisé pour la capture de trames

Avant de rentrer dans le détail des possibilités de capture de trames, réalisez une capture sur l'interface par laquelle votre ordinateur est connecté au réseau. La Figure 2 montre comment afficher les interfaces présentes sur votre machine. L'interface active pour votre connexion à Internet est l'interface qui indique **uha.fr**. Le chemin de cette fenêtre est **Panneau De Configuration → Réseau et Internet → Connexions réseau**. ( )

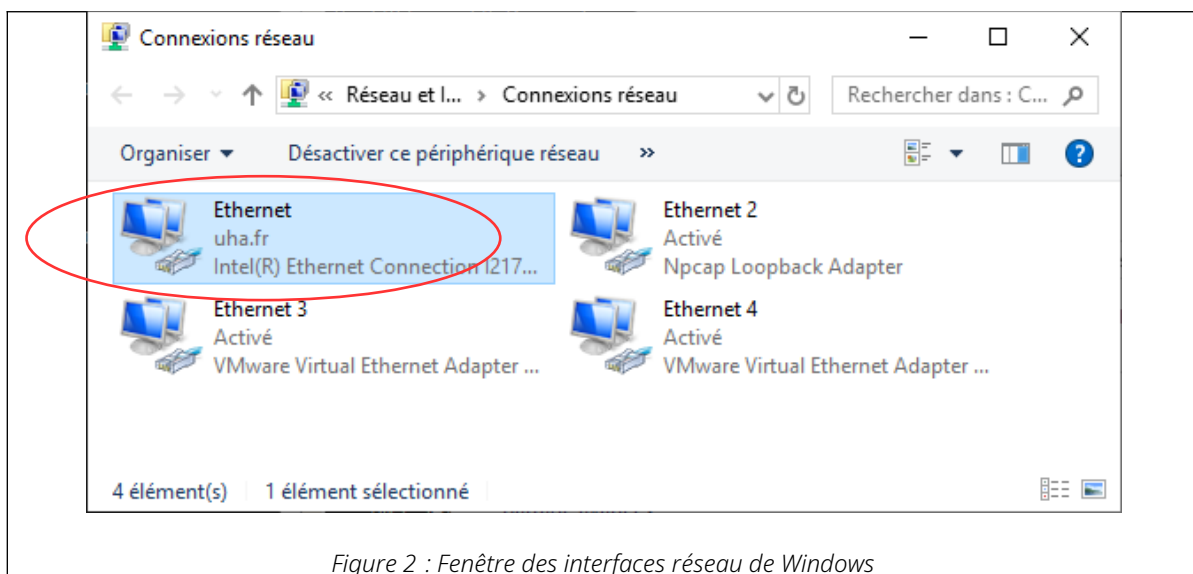


Figure 2 : Fenêtre des interfaces réseau de Windows

Après avoir lancé le programme Wireshark par Menu Démarrer → Tous les programmes → Spécifiques à R&T → Applications réseau, vous aboutissez à la page d'accueil ci-dessous (Figure 3).

Nb : Si vous observez qu'au lancement de Wireshark la capture de trame n'est pas possible, il peut être nécessaire d'exécuter le programme en tant qu'administrateur. Pour ce faire, lancez-le à l'aide d'un clic droit → Exécuter en tant qu'administrateur. L'enseignant devra faire une manipulation sur l'outil <http://webapps.iutcolmar.uha.fr> pour rendre cette manipulation possible.

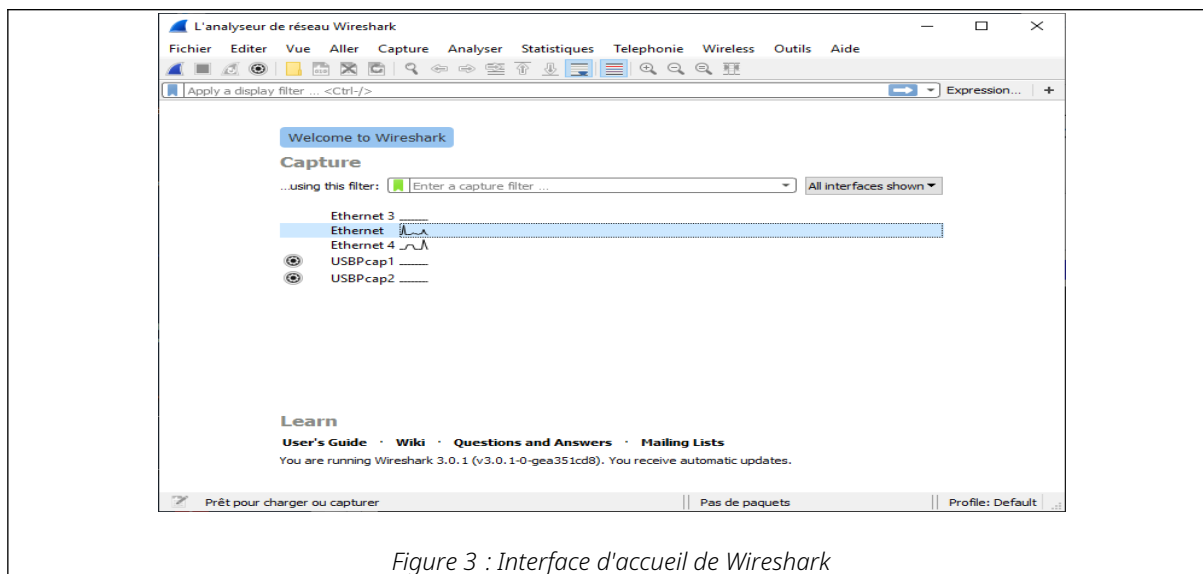




Figure 3 : Interface d'accueil de Wireshark

Le démarrage d'une capture de trames se fait en cliquant sur l'icône Start (aileron vert). L'interface sélectionnée est alors positionnée en mode promiscuous. Afin de sélectionner une interface qui "voit" du trafic, il suffit de sélectionner une interface active dans la liste des interfaces présentes.

Cliquer sur l'icône en forme de roue dentée vous donne accès à une fenêtre du type de celle de la Figure 3. Les interfaces dont les compteurs s'incrémentent sont des interfaces actives que vous pouvez sélectionner.

Le démarrage et l'arrêt d'une capture de trames se font à l'aide des boutons  (démarrer) et  (arrêter).

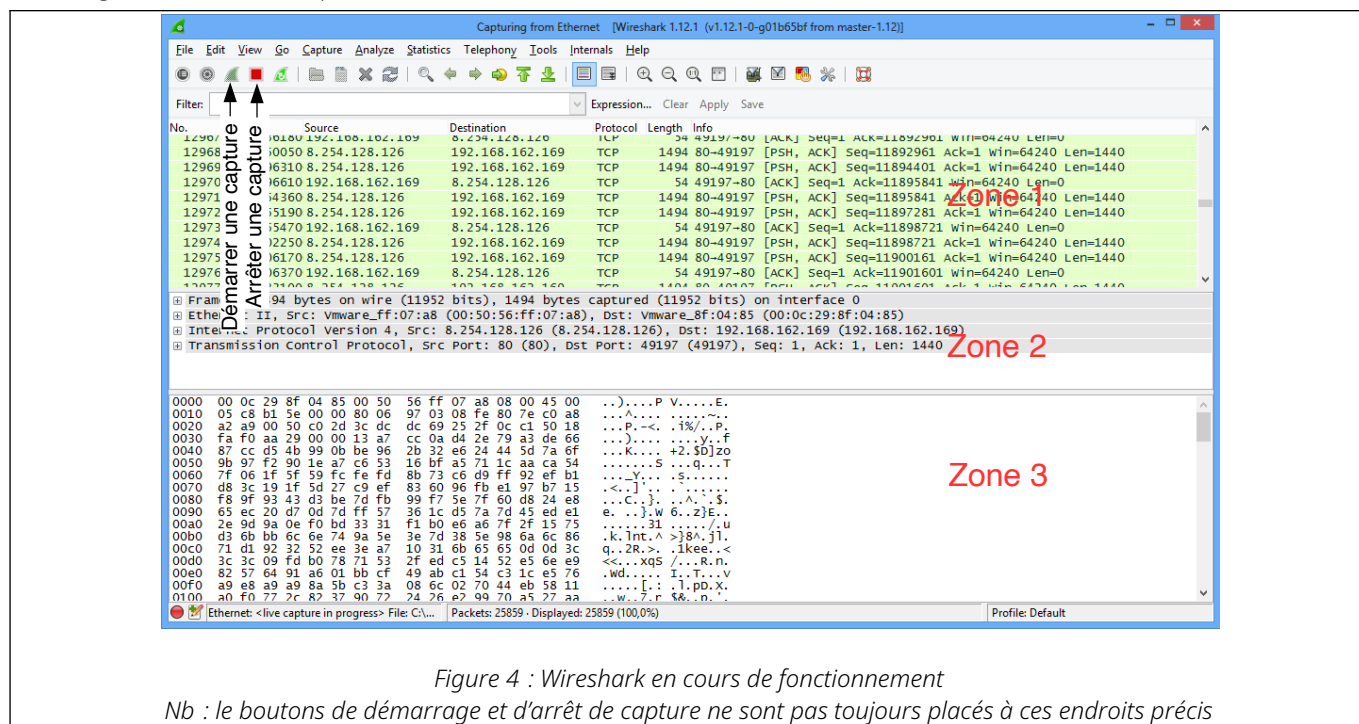
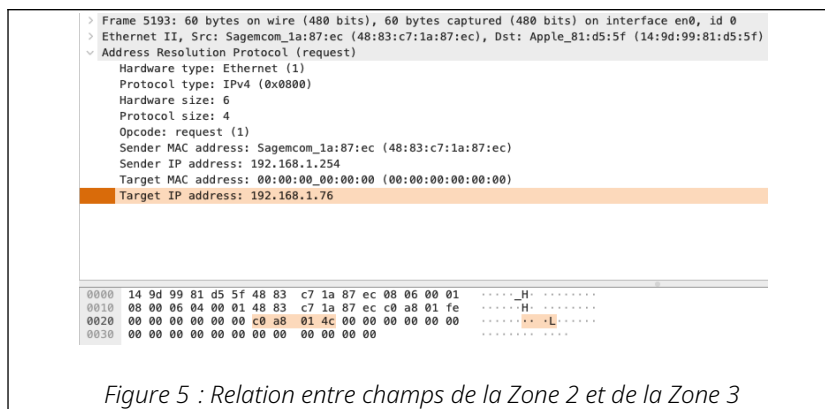


Figure 4 : Wireshark en cours de fonctionnement

Nb : le boutons de démarrage et d'arrêt de capture ne sont pas toujours placés à ces endroits précis

Lorsqu'une capture est en cours ou terminée, Wireshark présente une interface en trois zones :

- Zone 1** - Liste des paquets capturés avec un affichage synthétique de chaque paquet (Numéro dans la capture / Horodatage / @Source / @ Destination / Protocole principal / Longueur de la trame / Eléments principaux (*lié au protocole transporté*)).
- Zone 2** - Décomposition du paquet sélectionné dans la Zone 1 en protocoles de différents niveaux (cf. OSI ou TCP/IP). Cette décomposition permet de visualiser les champs des entêtes des protocoles ainsi que l'encapsulation des différentes couches des protocoles utilisés dans cette trame.
- Zone 3** - Affichage en hexadécimal (à gauche) et en ASCII (à droite) de la trame sélectionnée. Nb : quand on sélectionne un champ dans la Zone 2 il est mis en évidence dans la Zone 3 (cf. Figure 5).



Chaque ligne de la liste des paquets de la Zone 1 correspond à une trame capturée. Quand vous sélectionnez une ligne dans cette zone, les détails de cette trame s'affichent dans les Zone 2 et Zone 3.

Vous découvrirez et utiliserez les fonctionnalités plus avancées de Wireshark dans la suite des exercices de ce TD.

*Nb : Pour pouvoir exploiter le potentiel de cet outil et l'utiliser pour se former, il est indispensable d'avoir des connaissances minimales en ce qui concerne l'encapsulation de trames et le fonctionnement général des protocoles des réseaux informatiques.*

### III- Analyse des messages utilisés par le programme ping



Dans cette partie vous capturerez les trames d'un **ping**, qui est certainement l'un des outils les plus utilisés dans les réseaux. Ce logiciel permet de vérifier la connectivité IP d'un équipement. C'est à dire son existence, au sens réseau du terme. Pour ce faire il envoie des messages de sollicitation et attend des messages de réponse en retour. A l'aide d'une capture de trames vous allez découvrir le mode de fonctionnement de cet outil.

Nb : Lisez entièrement les parties **Préparation** et **Réalisation** ci-après avant de réaliser les opérations.

#### Préparation de la manipulation

Arrêtez la capture de trame en cours et sélectionnez une interface active pour enregistrer le trafic lié au programme **ping**. Ouvrez une fenêtre de l'interface de commande DOS (menu **Démarrer** → **Exécuter** → **Cmd**). Préparez la commande **ping www.google.fr**.

#### Réalisation de la capture

En cliquant sur  lancez la capture dans Wireshark  
Dans la fenêtre de l'interface de commande DOS validez la commande **ping www.google.fr**.  
Une fois le programme ping terminé arrêtez la capture en cliquant sur .

Dans les trames capturées vous chercherez les réponses aux questions ci-dessous.

#### Questions

Dans la liste des trames capturées trouvez-vous des trames qui correspondent à un échange DNS (Domain Name Service) ?  
Si oui, de quel type sont ces trames et quelle information permettent-elles de récupérer ?

Quel est le protocole utilisé par les messages générés par le programme **ping** ?

Nb : on pourra mettre en place un filtrage qui ne sélectionne que les messages de et vers l'adresse IP de la machine qui réalise le **ping** (**ip.host == xx.xx.xx.xx**).

#### III.1 Sélection de protocole(s)

##### III.1.1 Sélection de trames à l'affichage

Afin de sélectionner un type de trames qui correspond à un protocole en particulier, il suffit de saisir dans la zone **Filter** :, située en-dessous de la barre de menus de Wireshark, le nom d'un protocole (cf. Figure 5 ci-dessous). Quand la saisie correspond à un nom de protocole valide (par exemple arp, dns, tcp, udp, icmp, etc.) le fond de la zone **Filter** : devient vert. Il suffit alors d'appliquer le filtre, par une click sur **Apply** pour ne voir apparaître que les trames du type filtré.

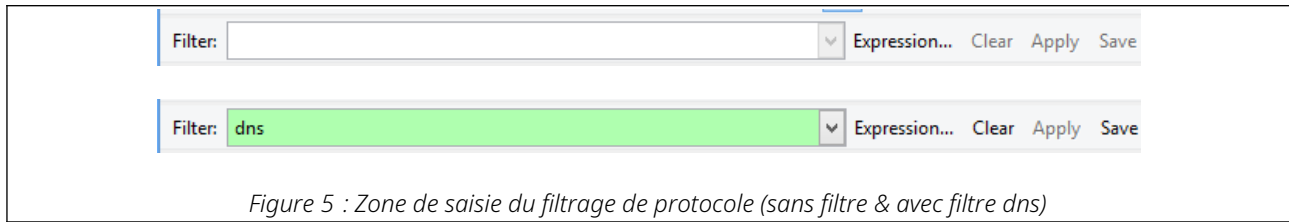


Figure 5 : Zone de saisie du filtrage de protocole (sans filtre & avec filtre dns)

Il est possible de combiner des filtres simples à l'aide des opérateurs logiques && (et) et || (ou).

Par exemple pour lister les trames ICMP d'un hôte IP xx.xx.xx.xx le filtre est : `ip.host == xx.xx.xx.xx && icmp`. Pour afficher les messages ICMP de ping et les échanges DNS : `dns || icmp`.

### III.1.1 Sélection de trames à la capture

En conditions réelles d'utilisation, sur un réseau opérationnel, Wireshark peut capturer une très grande quantité de trames. Afin de gagner de la place mémoire, il est possible de ne capturer que les trames pour lesquelles on a de l'intérêt. Le filtre d'affichage devient alors inutile. Mettre en place un filtre de capture nécessite d'indiquer avant de lancer la capture, dans la zone de Capture filter, le ou les filtres qui seront actifs pendant la capture des trames.

Pour ce type de filtres, DNS se dit `udp port 53` et pas `dns` comme dans le filtre d'affichage. Ce type de filtre est à indiquer dans la fenêtre accessible via la roue dentée du menu de Wireshark.

Enregistrez votre précédente capture dans un dossier de votre lecteur [U:](#) et relancez une capture avec un filtre de capture qui ne capture que les messages DNS et ICMP.

Attention, capturer deux type de trames différents, nécessite d'en assembler les définitions avec un || logique. Vous pouvez trouver llus d'informations sur les filtres de capture ici : <https://wiki.wireshark.org/CaptureFilters>.

### III.2 – Analyse du contenu d'une trame

Dans la Zone 2 une trame est affichée par niveau d'encapsulation. Pour chaque niveau le nom du protocole est indiqué (cf. Figure 6).

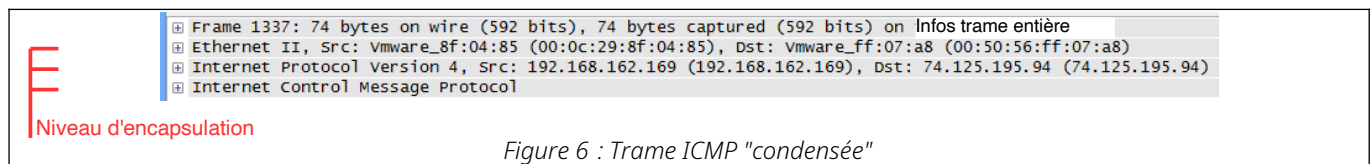


Figure 6 : Trame ICMP "condensée"

Il est possible à chaque niveau de "développer" le contenu. Cela permet d'afficher les informations d'entête du protocole concerné ainsi que les informations qui concernent les données situées dans le dernier niveau d'encapsulation (cf. figure 7).

Dans ce type d'affichage on peut se contenter de prendre en compte uniquement les informations "*qui nous intéressent*".

#### Questions concernant ICMP

Localisez deux types d'adresses **Source** et **Destination** différents. A quelles couches ces adresses appartiennent-elles ?

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

```
[message ICMP [datagramme IP[trame ethernet]]]
[datagramme IP [trame ethernet [message ICMP]]]
[trame ethernet [datagramme IP[message ICMP]]]
[message ICMP [trame ethernet [datagramme IP]]]
```

Dans quelle couche du modèle OSI se situent les protocoles ICMP, IP et Ethernet ?

Pour la prochaine série de questions vous sélectionnerez une trame de type DNS (filtre d'affichage `dns`).

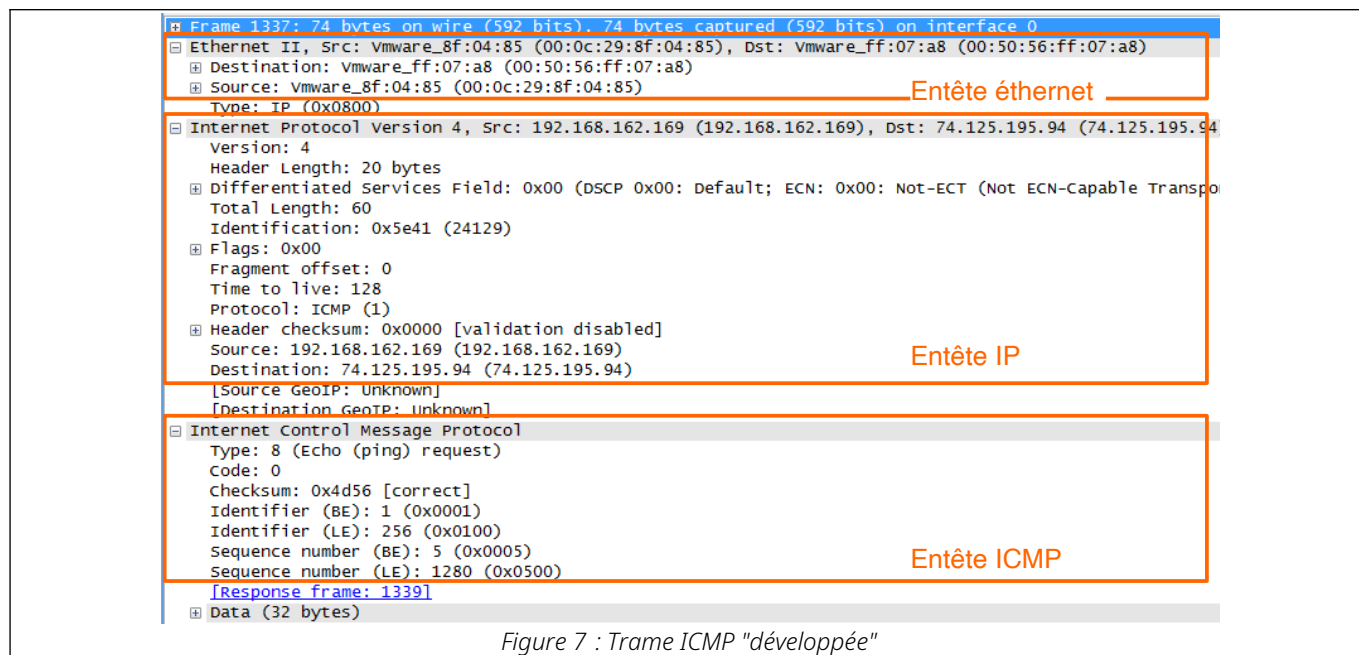
#### Questions concernant DNS

Quel est le nom complet du protocole DNS ?

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

Écrivez l'encapsulation utilisée pour transporter une requête DNS (sur le modèle des Questions concernant ICMP ci-dessus)

Dans la réponse du DNS, retrouvez l'adresse IP du site [www.google.fr](http://www.google.fr) ?



#### IV- Analyse d'un trafic d'échange de fichier ftp

Comme vous avez pu le constater dans la première partie de ce TD, analyser des trames à des fins pédagogiques, nécessite :

- d'avoir les connaissances/compétences requises pour arriver à chercher ce que l'on souhaite à l'aide de l'outil de capture de trames,
- d'être capable de générer le trafic qui utilise le protocole à étudier.

C'est pourquoi dans la suite de ce TD vous allez utiliser différents types de service réseau (web, transfert de fichier, ...) et créer du trafic qui met en œuvre les protocoles dédiés à ces services (http, ftp, ...).

Dans cet exercice vous allez utiliser le service de transfert de fichier (qui utilise le protocole **File Transfer Protocol**) à partir de ce qu'on appelle un "client en mode commande".

##### Manipulations

Depuis la Console, tapez la commande **ftp uha-ftp-01.uha.fr** (le username est anonymous ou ftp et le password est votre adresse mail uha).

Une fois connecté au serveur (les message **230 Login successful. apparaît**), tapez la commande **quit** ou **bye**. pour mettre fin à votre session ftp.

Une fois cette manipulation maîtrisée, refaites là en en capturant les trames.

Comme cela vous a été indiqué, le service ftp (File Transfer Protocol) utilise le protocole du même nom. Dans la capture de trame que vous venez de réaliser vous aller donc filtrer les trames qui concernent le protocole ftp.

##### Questions

Dans la couche réseau (entête IP ou Internet Protocol), quelle est la valeur du champ Time to Live ? Cherchez sur internet à quoi ce champ peut-il servir ?

Dans la couche réseau (entête IP ou Internet Protocol), quelle est la valeur du champ Protocol ? Cherchez sur internet à quoi ce champ peut-il servir ?

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

Examinez la totalité de la capture, en portant votre attention sur l'affichage en ASCII, et retrouvez le mot de passe saisi<sup>1</sup>.

Quel équipement d'infrastructure vous permettrait de capturer, à partir de votre machine, un mot de passe saisi par l'un de vos voisins ?

Cet équipement répèterait le trafic qui entre par un de ses ports sur tous ses autres ports.

#### V- Analyse d'un trafic Facebook

##### Manipulations

Lancez une capture de trames.

Ouvrez alors un navigateur web et connectez vous à votre compte Facebook (L'objectif est ici d'uniquement enregistrer la phase de connexion et pas d'échanger des messages avec vos contacts).

Une fois que vous êtes connecté, arrêtez la capture de trames.

<sup>1</sup> 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 !!!!

### Questions

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

En observant cette trame déterminez ?

- 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 ?

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

Donnez le développé des acronymes SSL et TLS ?

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

Pourquoi ?

### VI-Analyse d'un trafic DNS

#### Manipulations

Lancez une capture de trames.

Afin de récupérer une adresse IP, tapez la commande **ping www.google.fr**.

Depuis la Console, lancez la commande **nslookup <@IP récupérée>**.

Une fois la réponse obtenue, arrêtez la capture.

Dans la capture de trames que vous venez de réaliser tapez dans le champ **Filter** le protocole **dns** (n'oubliez pas de cliquer sur **Apply**).

#### Questions

Quelle est l'adresse IP du serveur DNS ?

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

Quels sont les deux types de trames utilisées par le protocole DNS ?

Sur la première trame déterminer la valeur des champs :

- @IP Src & @IP Dst
- Src Port & Dst Port

Sur la deuxième trame, déterminer la valeur des champs :

- @IP Src & @IP Dst
- Src Port & Dst Port

Que constatez-vous ?

Remerciement : Ces exercices sont issus d'une adaptation du sujet de TD qui porte sur le même thème et qui a été réalisé par JL Damoiseaux et Delphine Rousseau du département R&T de Marseille Luminy. Avec leur aimable autorisation.