TP n° 02

Analyseur de protocoles - Wireshark

1. Objectif

Dans ce TP, nous allons observer quelques protocoles réseau "en action", en train d'interagir et d'échanger des messages dans une exécution réelle, et ceci en utilisant un logiciel appelé Renifleur ou Sniffer.
Le logiciel sniffer que nous allons utiliser dans nos TP est le Wireshark.
L'objectif de ce TP est :

- D'être capable à utiliser l'analyseur de protocoles Wireshark : capturer les paquets de données transitant dans le réseau, les observer et les analyser.
- De découvrir les caractéristiques générales et l'encapsulation des protocoles du modèle "TCP/IP".

2. Logiciels renifleurs (Sniffer)

Un logiciel renifleur ou sniffer est un logiciel capable d'intercepter, enregistrer et analyser les données transitant au sein d'un réseau. Ainsi, il permet de capturer les données du flux traversant le réseau, et afficher le contenu de chacun des champs constituant ces données conformément aux spécifications de chacun des protocoles utilisés. Noter qu'une donnée est structurée en un ensemble de champs, chacun contient une information bien précise.

3. Wireshark

Wireshark est un logiciel libre d'analyse de protocole, ou « packet sniffer », utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétroingénierie, mais aussi le piratage. Wireshark est multiplatesformes, il fonctionne sous Windows, Mac OS X, Linux, Solaris, ainsi que sous FreeBSD. Wireshark reconnait 759 protocoles.
L'installation se fait à partir d'une version adaptée à son système téléchargée à partir du site :
http://www.wireshark.org/download.html
La documentation est disponible sur : http://www.wireshark.org/docs/wsug_html_chunked/index.html

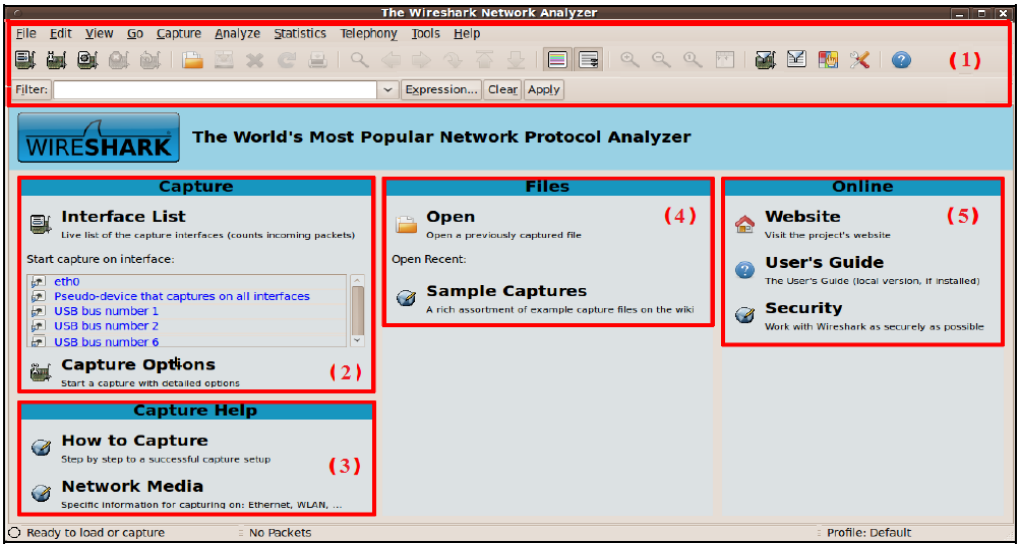
3.1. Principe de fonctionnement

Wireshark capture des trames de la couche liaison (Ethernet) d'un ordinateur, ce qui permettra de capturer tous les messages envoyés (ou reçus) par tous les protocoles exécutés sur cet ordinateur. Ceci car la communication se fait selon le principe d'encapsulation, et donc tous les protocoles des couches supérieures sont finalement encapsulés dans une trame Ethernet. Grâce à l'analyseur de paquets, qui comprend la structure des messages échangés par tous les protocoles, Wireshark peut afficher le contenu de chaque champ d'un message dépendant du protocole qu'il l'a échangé.

Exemple. Supposons qu'on a utilisé le navigateur pour consulter le site web du centre universitaire de Mila. Donc, au niveau « Application » on a utilisé le protocole HTTP. Le message HTTP est encapsulé dans des messages TCP ou UDP, qui sont à leurs tour encapsulés dans des paquets IP, encapsulés par la suite dans des trames Ethernet, et enfin transmis sur le support physique.
Wireshark capture une trame Ethernet. Comme il sait bien le format de cette trame, il peut identifier le datagramme IP encapsulé dedans. Aussi, il connait également le format du datagramme IP, et ainsi il peut extraire le segment TCP. Enfin, il connait la structure du segment TCP, et donc il peut extraire le message HTTP qu'il contient. Enfin, il analyse le message HTTP et l'affiche selon la structure de la donnée HTTP.

3.2. Interface principale

Wireshark permet d'analyser un trafic enregistré dans un fichier annexe, mais également et surtout le trafic en direct sur des interfaces réseau. Cette seconde fonction nécessite de posséder les droits administrateurs, ou d'appartenir à un groupe possédant ces droits.
Commencer par installer Wireshark.
On lançant Wireshark, il s'ouvre sur l'interface suivante composée de cinq zones :



(1) Le panneau de commande :
La partie haute de ce panneau contient les menus déroulants standards, les plus intéressants sont :

- Fichier : pour sauvegarder ou ouvrir un fichier contenant une capture de données.
- Capture : pour lancer et arrêter une capture de données.

En dessous des menus déroulant, il y a les icônes de lancement rapide des tâches présentées dans ces menus. Ensuite, il y a le champ Filtre, pour filtrer les paquets capturés à afficher. Aussi il y a le bouton «Expression» juste à côté pour définir une expression du filtre plus complexe.

(2) La liste des interfaces réseaux et lancement rapide d'une capture :
Ce panneau affiche toutes les cartes réseaux actives dans le PC y compris les cartes virtuelles (qui n'existent pas physiquement) installées par des logiciels comme Virtual Box.

(3) L'aide sur la capture de paquets :
Elle contient toute l'aide nécessaire pour apprendre à capturer et analyser les données.

(4) La liste des captures récentes (enregistrées) :
Cette zone affiche la liste des fichiers contenant des captures réalisées récemment. Elle offre un accès rapide pour ouvrir une capture récente enregistrée.

(5) L'aide en ligne et le manuel de l'utilisateur :
Cette zone affiche des liens utiles comme celui de la page principale et celui du guide de l'utilisateur.

3.3. Capture des trames avec Wireshark

La capture se fait en trois étapes :
(1) Le choix de l'interface réseau sur laquelle Wireshark va capturer les données (noter qu'un ordinateur peut avoir plusieurs interfaces réseau).
(2) Le lancement de la capture.
(3) L'arrêt de la capture.

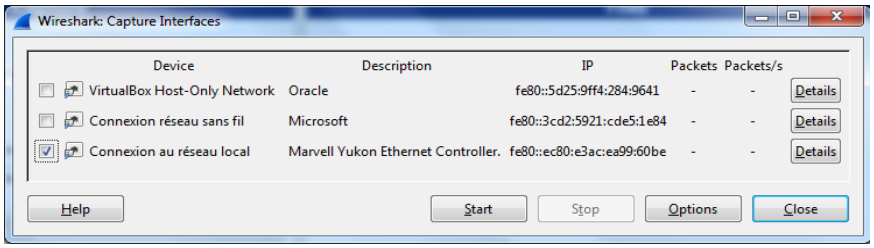
Pour le choix de l'interface et le lancement de la capture, différentes manières existent, les plus pratiques sont les deux suivantes :

- En utilisant la zone « Capture » :

Dans la zone (2) "Liste des interfaces réseau" sont affichées les interfaces réseaux de l'ordinateur. Cliquer directement sur l'interface désirée. Ensuite, cliquer sur le bouton « Start » qui se trouve au-dessus. 

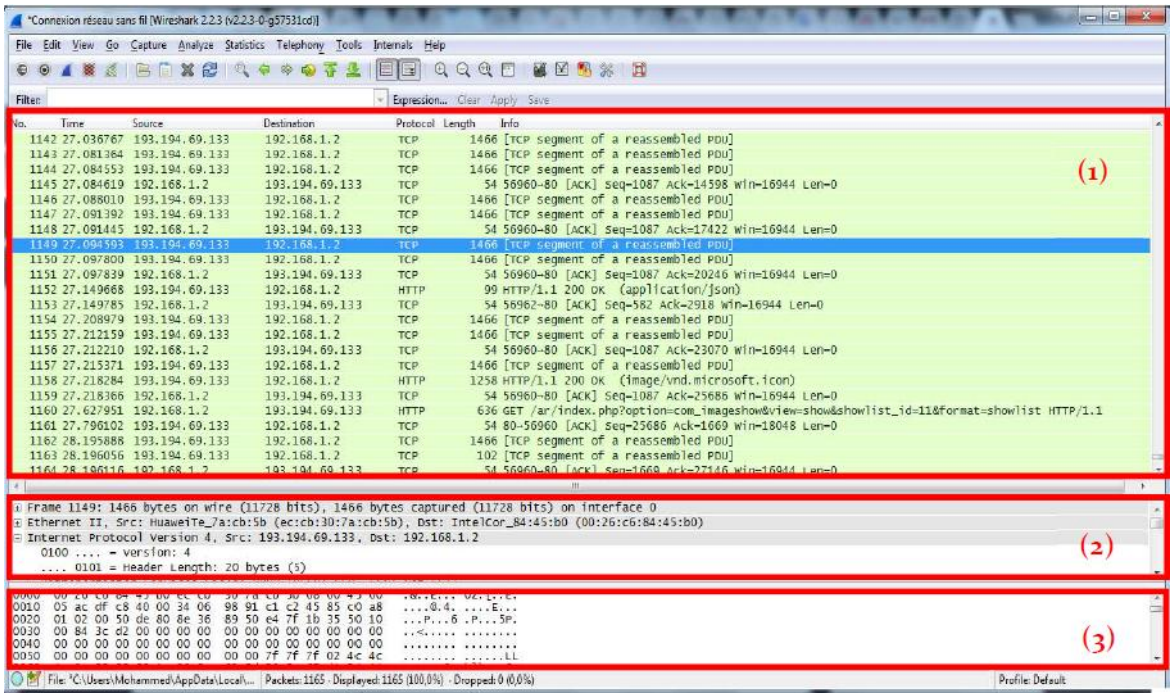
- En utilisant la zone (1) « Panneau de commande » : soit :
- En choisissant « Interfaces » dans le menu « Capture ».
- En cliquant sur le premier bouton de la liste des icônes de lancement rapide, intitulé «Interface List».
- En utilisant la combinaison clavier Ctrl + I.

La fenêtre suivante s'ouvre :



Il suffit de choisir l'interface désirée et puis cliquer sur le bouton « Start » pour lancer la capture.

Après le choix d'une interface et le lancement d'une capture, Wireshark commence la capture de tous les paquets envoyés à (ou reçu par) cette interface, et affiche une fenêtre comme celle-ci :



L'interface est constituée de trois zones :

(1) La zone (1) en haut : affiche la liste des paquets capturés.

(2) La zone (2) au milieu : affiche le détail d'un paquet sélectionné (mis en évidence) dans la zone (1).

(3) La zone (3) en bas : affiche le contenu du paquet sélectionné dans la zone (1) en ASCII et en hexadécimal.

La capture peut être stoppée en cliquant tout simplement sur le bouton « Stop the running live capture » de la barre des icônes de lancement rapide dans le « Panneau de commande ». 

3.4. Analyse des paquets capturés

Dans la fenêtre de capture, les informations affichées dans une zone inférieure correspondent à ce qui a été sélectionnée dans la zone supérieure. Ainsi, si on veut connaitre les détails sur un paquet capturé, il suffit de le sélectionner dans la zone (1), est ses informations d'encapsulation seront affichées dans la zone (2), ainsi que son contenu hexadécimal dans la zone (3).

3.4.1. Filtrer les paquets capturés

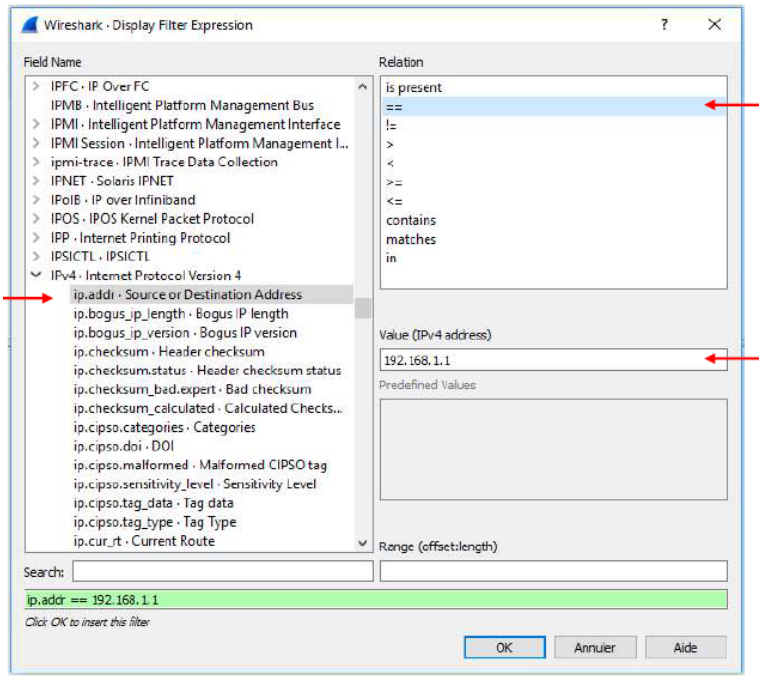
On peut remarquer qu'il y a beaucoup de types de paquets capturés et affichés par Wireshark, à cause du grand nombre de protocoles supportés par ce logiciel. Pour pouvoir chercher à l'intérieur des données capturées et n'afficher que le trafic qui nous intéresse, on utilise des filtres.

La syntaxe générale d'une expression simple d'un filtre est :

Protocole	•	Paramètre	Opérateur	Valeur

Exemple : ip . addr == 192.168.1.1

L'expression du filtre peut être définie visuellement en cliquant sur le bouton « Expression » à côté du champ « Filter » dans le panneau de commande.
Pour définir l'expression du filtre, suivre les étapes illustrées dans la figure suivante :



(1) Choisir le protocole, et pour le paramètre il suffit de dérouler la liste des paramètres en cliquant sur « > » devant le protocole et choisir un.
(2) Ensuite choisir l'opérateur de comparaison.
(3) Et enfin, mettre la valeur à considérer dans le champ valeur.
Tout au long des étapes, on voit construite l'expression tout en bas de la fenêtre. Une fois terminer, cliquer sur « OK ».
On peut définir des expressions de filtre plus complexes en utilisant des opérateurs logiques. Le format est :

Expression	Opérateur logique	Expression	.....

Exemple : TCP || UDP

Six opérateurs de comparaison sont disponibles :

Format anglais:	Format de type C:	Signification:
eq	==	Equal
ne	!=	Non équal (Not Equal)
gt	>	Plus grand que (Greater than)
lt	<	Plus petit que (Less than)
ge	>=	Plus grand ou égale à (Greater or equal)
le	<=	Plus petit ou égal à (Less or equal)

Quatre opérateurs logiques sont disponibles :

Format anglais:	Format de type C:	Signification:
and	&&	Logical AND (et)
or	||	Logical OR (ou)
xor	^^	Logical XOR (ou)
not	!	Logical NOT (non)

Exemples de filtres :

ip.addr == 192.168.1.1 → Affiche les paquets avec une adresse source ou destination de 192.168.1.1

tcp || ip || dns → Affiche les trafics TCP ou IP ou DNS.

ip.src == 192.168.1.1 && ip.dst ! = 172.16.10.2 → Affiche les paquets avec une adresse IP source égale à 192.168.1.1 et de destination différente de 172.16.10.2

eth.addr == 00:2F:4C:01:23:6C → affiche le trafic de la machine dont l'@ MAC est 00:2F:4C:01:23:6C

Remarque. Ces filtres sont des filtres d'affichage, et il y a aussi les filtres de capture qui déterminent quels types de paquets à capturer.

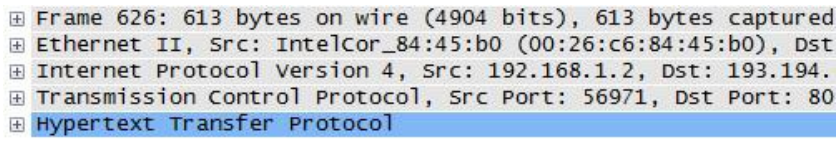
3.4.2. Le paquet capturé

Dans la liste des paquets capturés affichés dans la zone (1), chaque ligne correspond à un paquet capturé. Elle contient le numéro de paquet attribué par Wireshark, l'heure à laquelle le paquet a été capturé, les adresses de source et de destination du paquet, le type de protocole, et des informations spécifiques au protocole contenues dans le paquet. La liste des paquets capturés peut être triée selon l'une de ces catégories en cliquant sur le nom de la colonne correspondante.

3.4.3. Les détails sur le paquet sélectionné

Si un paquet est sélectionné dans la zone (1), la zone (2) fournit les détails sur ce paquet ainsi que ses différents niveaux d'encapsulation.

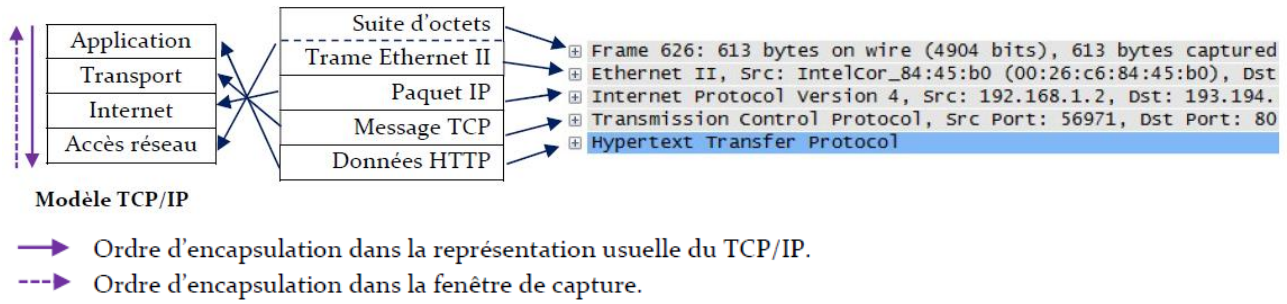
Exemple : si on sélectionne un paquet de type HTTP dans la zone (1), la zone (2) affiche quelque chose similaire à ceci :



Chacune des entrées correspond à un niveau d'encapsulation. L'ordre d'encapsulation se lit de bas en haut dans la zone (3). Noter que dans la zone (3), c'est en quelque sorte l'ordre de dé-encapsulation qui est affiché. En effet, Wireshark capture une suite d'octets. Il extrait la trame de cette suite. Ensuite, il extrait le paquet IP de la trame, puis il extrait le message TCP (ou UDP) du paquet IP, et enfin il extrait le message http.

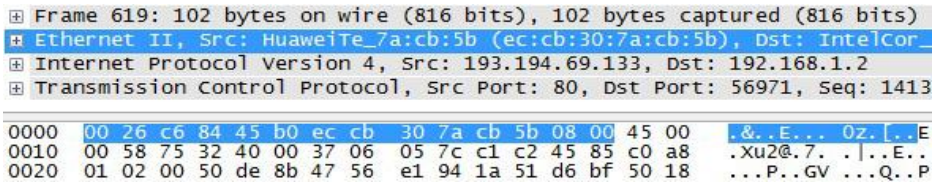
Noter que le clic sur le « + » devant chaque niveau d'encapsulation permet de visualiser l'ensemble des champs le composant. Aussi, certains champs à leur tour peuvent être déroulés.

Exemple : le déroulement de l'entrée Ethernet (couche liaison) permet de visualiser les champs « Destination », « Source » et « Type ». Les champs « Destination » et « Source » peuvent à leur tour être étendus.



3.4.4. Le contenu du paquet sélectionné

La zone (3) permet de visualiser le contenu de la trame capturée en hexadécimal. Un clic sur un niveau d'encapsulation de la zone (2) permet de visualiser la portion d'octets correspondante à ce niveau dans la zone (3). Inversement, un clic sur un octet quelconque de la zone (3) affiche le champ correspondant dans la zone (2).
Exemple : un clic sur le niveau Ethernet (couche liaison de données) mettra en évidence dans la zone (3) les octets correspondant. Ceci peut être fait pour chaque champ.



4. Travail demandé

1. Lancez une capture à l'aide de Wireshark en sélectionnant l'interface « Ethernet ».
2. Énumérez 5 différents protocoles exécutés par votre PC.
3. Appliquez les filtres d'affichage suivants à votre capture :
   a) Les paquets avec un port TCP de destination égal à 25.
   b) Tous les messages TCP sauf ceux dont le port de source ou de destination est 80.
   c) Seulement les paquets envoyés par votre machine.
   d) Tout sauf les paquets icmp.
4. Lancez une capture de paquets, et pendant que Wireshark est en cours d'exécution, lancez la commande « ping » vers une machine dans le réseau. Quel est le protocole utilisé suite à l'exécution du « ping »? A quelle couche appartient-il ?
5. Lancez une autre capture, et pendant que Wireshark est en cours d'exécution, entrez dans votre navigateur l'adresse du site du centre universitaire de Mila : www.centre-univ-mila.dz. Une fois que la page du site affichée par le navigateur, arrêtez la capture :
   a) Quels est le protocole utilisé par le navigateur pour communiquer avec le serveur du centre-univ-mila.dz ?
   b) Filtrez les paquets capturés et ne laissez affichés que les messages http.
   c) Sélectionnez un message HTTP dans la zone (1) :
      (i) Le protocole http est de quelle couche ?
      (ii) Quel protocole de transport utilisé par http ?
      (iii) Donnez les détails d'encapsulation du message HTTP.
   d) Quels sont les deux types de messages HTTP échangés entre votre PC et le serveur ?
   e) Combien de temps a-t-il fallu pour recevoir la réponse à la requête HTTP envoyée par votre PC ?
   f) Quelle-est l'adresse Internet du serveur du « centre-univ-mial.dz » ?
6. Enregistrez la dernière capture effectuée.
7. Ouvrir la capture depuis le fichier enregistré.