Wireshark - TP de découverte

Ce logiciel est un analyseur de trafic réseau (sniffer). Ce TP se déroule en 3 parties :

1. Découverte de l'interface
2. Capture et analyse de trafic généré par la commande ***ping***
3. Analyse d'un fichier de capture fourni.

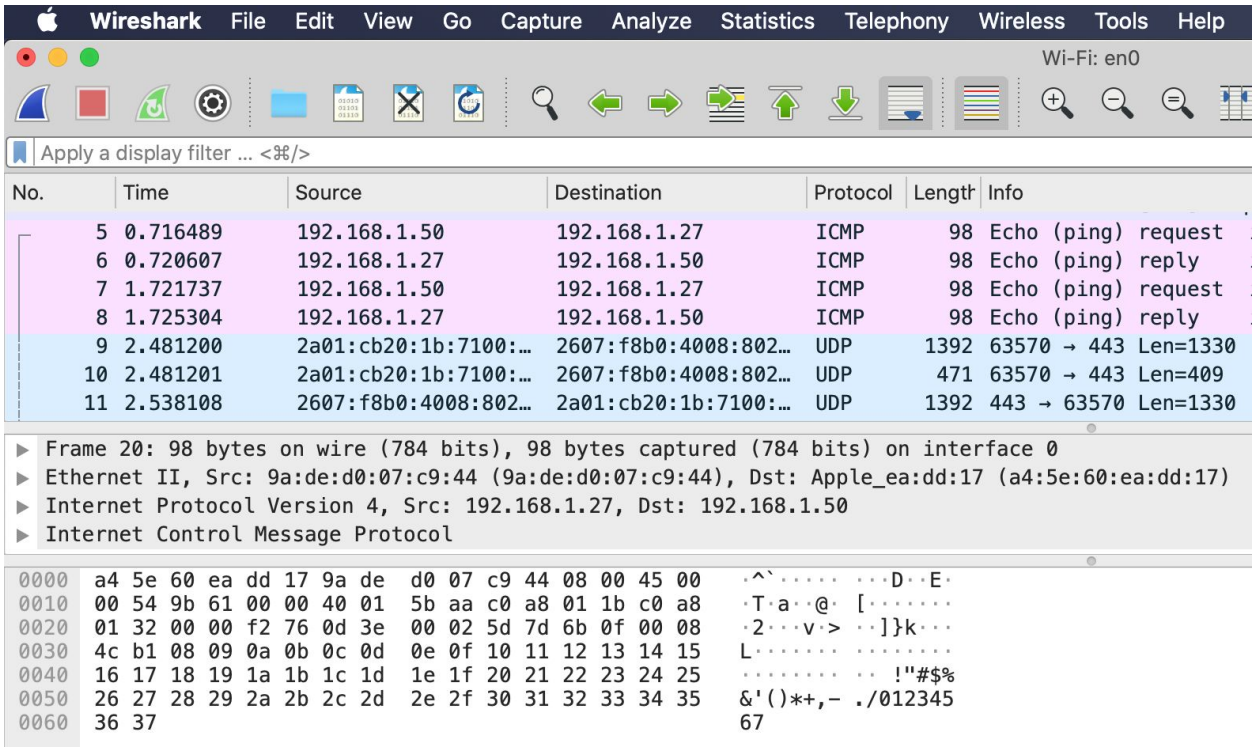
Wireshark est un logiciel gratuit, on peut le télécharger ici :
https://www.wireshark.org/download.html

Pour une utilisation avancée la documentation est disponible ici :
https://www.wireshark.org/docs/

1. Découverte de l'interface de wireshark

Wireshark fonctionne à la manière d'un enregistreur numérique : on lance un enregistrement, on l'arrête, et on analyse ensuite le trafic capturé.

- Télécharger, installer, et exécuter Wireshark,
- Lancer ensuite une capture (bouton bleu),
- Accepter les propositions par défaut de la capture (généralement c'est la carte réseau installée),
- Stopper la capture au bout de quelques secondes (bouton rouge).



De haut en bas, on va trouver :

- La barre des menus
- La barre des icônes (raccourcis permettant d'éviter de passer par les menus)
- La zone de filtrage (un filtre permet de choisir le trafic que l'on veut observer)
- La liste des trames numérotées et chronométrées dans l'ordre chronologique de la capture. Les adresses IPv4 ou IPv6 de l'émetteur et du destinataire sont indiquées, ainsi que le protocole utilisé.
- La fenêtre d'affichage de la pile des protocoles pour la trame sélectionnée. On peut dérouler chaque protocole pour obtenir le détail des informations contenues.
- Fenêtre d'affichage brut de la trame sélectionnée (tous les octets de la trame en hexadécimal).

2. Capture et analyse de trafic généré par la commande ping

Pour cet exercice, il est demandé de noter son adresse IPv4 ainsi que celle de sa passerelle. On va pour cela utiliser la commande ***ipconfig*** dans la console de commande de Windows (voir https://fr.wikipedia.org/wiki/Ipconfig) :

```
C:>ipconfig

Configuration IP de Windows

Carte réseau sans fil Connexion réseau sans fil :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte Ethernet Connexion au réseau local :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::89c9:7d53:f73:c8c4%11
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.1.2
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle [[par défaut]]. . . . . . . . . : 192.168.1.1
```

- Adresse IP de votre ordinateur : _____
- Adresse IP de votre passerelle : _____

La commande ***ping*** utilise le protocole ***ICMP*** (https://fr.wikipedia.org/wiki/Internet_Control_Message_Protocol)

On va maintenant observer le trafic réseau généré par la commande ping :

- Lancer une nouvelle capture avec Wireshark (on acceptera de ne pas sauvegarder la précédente)
- Dans la console de commande de Windows, exécuter la commande ***ping x.x.x.x*** (remplacer x.x.x.x par l'@IPv4 de la passerelle)
- Une fois les 4 réponses obtenues, stopper la capture.
- Appliquer le filtre ***icmp*** pour n'afficher que les trames générées par la commande ***ping***.

On peut maintenant analyser le trafic capturé :

- Nombre de trames générées : _____
- @IP source d'une trame request : _____
- @IP destination d'une trame request : _____
- @IP source d'une trame reply : _____
- @IP destination d'une trame reply : _____
- Durée écoulée entre la trame request et la trame reply du premier échange : _____
- Nombre d'octets de données de la trame request : _____
- Nombre d'octets de données de la trame reply : _____

3. Analyse d'un fichier de capture fourni

Avec Wireshark, ouvrir le fichier ***http-wget-iana-ipv4.pcap*** disponible sur le site de ressources. Ce fichier contient les trames capturées lors du chargement d'une page web.

- @IPv4 du client HTTP : _____
- @IPv4 du serveur HTTP : _____
- @IPv4 du serveur DNS : _____
- Rôle des trames 1 & 2 : _____
- Rôle des trames 3 à 5 : _____
- Rôle de la trame 6 : _____
- Rôle de la trame 12 : _____
- Rôle des trames 13 à 15 : _____

On peut récupérer l'adresse IP publique d'un serveur avec son nom de domaine, en utilisant https://mxtoolbox.com/DNSLookup.aspx

- Pourquoi une requête DNS est-elle nécessaire ?
  _____
- Adresse IPv4 de google.fr : _____