Semaine 1 – Outil d'analyse de paquets

1 Prérequis

Pour effectuer ce TP, vous devez installer sur votre ordinateur le logiciel Wireshark (disponible sur Windows, Linux, MacOS, via http://wireshark.org).

2 Interfaces

Quelles sont les interfaces réseaux disponibles sur votre ordinateur ? À quoi correspondent-elles ?

3 Capture de trafic

Ouvrez une fenêtre avec un navigateur Web.

Avec Wireshark, démarrez une capture de trafic en sélectionnant l'interface utilisée par votre ordinateur pour accéder à l'Internet. Si vous ne savez pas de laquelle il s'agit, démarrez une capture avec la première interface : s'il ne se passe rien, arrêtez la capture sans sauvegarder, puis passez à la deuxième interface, et ainsi de suite.

Lorsque vous voyez des paquets affichés par Wireshark, ouvrez une page Web dans votre navigateur. Pour avoir des données utiles, il faut utiliser le protocole HTTP (et non HTTPS) qui ne chiffre pas les données. Par exemple, accédez à la page Web http://www.netmagis.org.

Lorsque la page Web est affichée, arrêtez la capture (via le menu ou via le bouton avec un gros carré rouge) pour ne pas surcharger votre ordinateur.

4 Sélection d'une partie du trafic

Vous avez sans doute beaucoup de paquets affichés à l'écran, dont un certain nombre sans rapport avec la page Web affichée. Sélectionnez la partie du trafic qui nous intéresse avec un filtre (barre de filtre juste en dessous des boutons). Par exemple, comme l'adresse IP de `www.netmagis.org` est 130.79.201.63, le filtre « `ip.addr == 130.79.201.63` » n'affichera que les paquets dont l'adresse IP source ou destination correspond à la valeur indiquée.

Vous pourriez aussi utiliser le filtre « `tcp.port == 80` », mais vous afficheriez alors tous les paquets Web et pas seulement ceux échangés avec notre serveur Web.

5 Analyse d'un paquet

Localisez maintenant le paquet commençant par « `GET /...` ».

Par qui ce paquet est-il émis ? Que signifient les différentes colonnes (No, Time, etc.) de la partie supérieure de la fenêtre ?

Sélectionnez le paquet si ce n'est déjà fait. À quoi correspondent les 5 lignes (5 lorsqu'elles sont toutes repliées) de la fenêtre du milieu ?

5.1 Partie « Ethernet »

Quelle est le fabricant de votre carte réseau ? Vérifiez les 24 premiers bits de l'adresse Ethernet par rapport à la liste disponible sur http://standards-oui.ieee.org/oui/oui.txt (attention, gros fichier).

5.2 Partie « Internet Protocol »

Quelles sont les adresses source et destination ? Quelle est la longueur du paquet ?

5.3 Partie « Transmission Control Protocol »

Quelle est la valeur et que représentent les ports source et destination ?

5.4 Partie « Hypertext Transfer Protocol »

Quelle commande HTTP est envoyée au serveur ? Quels sont les langues acceptées par votre navigateur ?

6 Encodage du paquet

Dans la partie inférieure de la fenêtre sont indiqués tous les octets formant le paquet (16 octets en hexadécimal à gauche, et signification en ASCII si c'est possible à droite). En sélectionnant une partie du paquet dans la partie du milieu de la fenêtre, on peut déterminer les octets correspondants dans le paquet dans la partie inférieure.

1. Combien d'octets sont pris par l'en-tête Ethernet. Que contient cet en-tête et dans quel format ?
2. Comment est encodée une adresse IP ?
3. Combien d'octets compte l'en-tête d'un paquet (datagramme) IP ?
4. Combien d'octets compte l'en-tête d'un paquet (segment) TCP ?
5. Comment sont encodées les informations dans un paquet HTTP ?

7 Protocole HTTP

Toujours sur le même paquet (commençant par « `GET /...` »), faites un clic droit sur le paquet, puis sélectionnez « Suivre le flux TCP ».

Déterminez ce qui est envoyé par votre navigateur et ce qui est envoyé par le serveur.