Sylvain THIROINE

Fiche n ° 7 : Wireshark

1. Lancement de Wireshark

a) Cliquer sur Capture
b) Choisir la carte réseau que l'on veut surveiller
c) Cliquer sur Démarrer

2. Description de l'écran d'affichage

a) **Fenêtre du haut** : Analyse de paquets de données
- **No.** : numéro du paquet capturé. Le trait vertical indique que ce paquet fait partie d'une conversation.
- **Time** : cette colonne indique combien de temps après le lancement de la capture le paquet a été capturé. Vous pouvez changer la nature de cette valeur dans les paramètres.
- **Source** : adresse du système qui a émis le paquet.
- **Destination** : adresse de la destination du paquet.
- **Protocole** : type du paquet. Par exemple : TCP, DNS, DHCPv6 ou ARP.
- **Length** : cette colonne indique la longueur du paquet, en octets.
- **Info** : cette colonne présente plus d'informations sur le contenu du paquet et varie selon le type du paquet.

b) Fenêtre de gauche
Le panneau central, intitulé Packet Details, présente autant d'informations lisibles sur le paquet que possible, en fonction du type de paquet. Vous pouvez effectuer un clic droit et créer des filtres basés sur le texte en surbrillance dans ce champ

c) Fenêtre de droite
Le panneau inférieur, Packet Bytes, présente le paquet exactement tel qu'il a été capturé, sous sa forme hexadécimale. Lorsque vous observez un paquet qui fait partie d'une conversation, vous pouvez effectuer un clic droit dessus et sélectionner Follow pour afficher uniquement les paquets qui font partie de la conversation.

3. Analyse des protocoles

- ⇒ **ARP - Address Resolution Protocol** : C'est un protocole qui associe l'adresse IPv4 à son adresse MAC
- ⇒ **DNS – Domain Name System** : C'est un protocole qui associe un nom de domaine internet avec une adresse IPv4
- ⇒ **ICMPv6 – Internet Control Message Protocol v6** : Il est utilisé pour rapporter des erreurs trouvées dans le traitement de paquets, effectuer des diagnostics, effectuer une découverte de voisinage et rapporter l'appartenance à un multicast
- ⇒ **IGMPv2 – Internet Group Management Protocl v2** : C'est un protocole qui permet d'envoyer des messages aux hôtes d'un groupe de multidiffusion
- ⇒ **MDNS – Multicast Domain Name System** : C'est un protocole qui permet de bénéficier des fonctionnalités de DNS sans avoir un serveur DNS sur le réseau. Utilisé surtout par APPLE
- ⇒ **NBNS – NetBios Name Server** : Cela permet d'établir de des sessions entre différents ordinateurs d'un réseau
- ⇒ **NTP – Network Time Protocole** : C'est un protocole qui permet de synchroniser l'horloge local d'ordinateur via un réseau informatique
- ⇒ **SSDP – Simple Service Discovery Protocol** : C'est un protocole réseau basé sur la suite de protocole internet (DNS, TCP, DHCP..), pour la diffusion et la découverte de services de réseau et d'information de présente (Plug and Play)
- ⇒ **TCP – Transmission Control Protocol** : Il permet aux appareils connectés à internet de communiquer entre eux via les réseaux
- ⇒ **TLSv1.2 – Transport Layer Security** : C'est un protocole de sécurisation des échanges par réseau
- ⇒ **UDP – User Datagram Protocol** : C'est un protocole de communication de substitution à TCP, il est surtout utilisé pour établir des connexions à faible latence et à tolérance de perte entre application sur internet.