TP N°9 : Mise en évidence de l'encapsulation

Objectifs

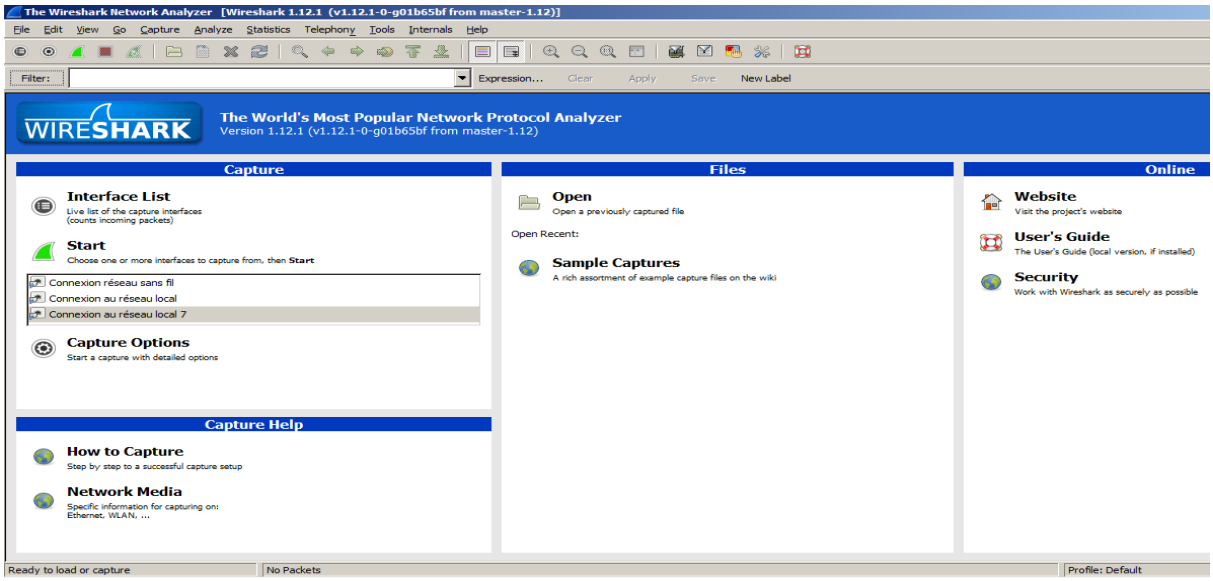
- Comprendre l'encapsulation : capture des trames avec Wireshark
- Reconnaitre les champs des protocoles IPv4, Ethernet II, Ethernet 802.3, LLC, ARP, ICMP, TCP, UDP, DNS, DHCP, http, POP3, SMTP, ftp, telnet/ssh en effectuant capture du trafic

Contexte

Wireshark est un analyseur de protocole gratuit pour Windows, Unix et ses dérivés. Il permet d'examiner des trames à partir d'un fichier ou directement en les capturant sur le réseau.

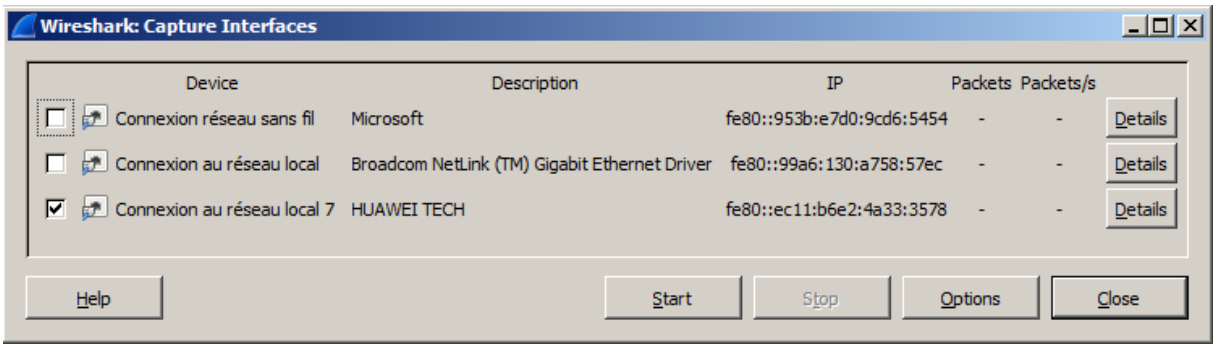
Configuration de Wireshark

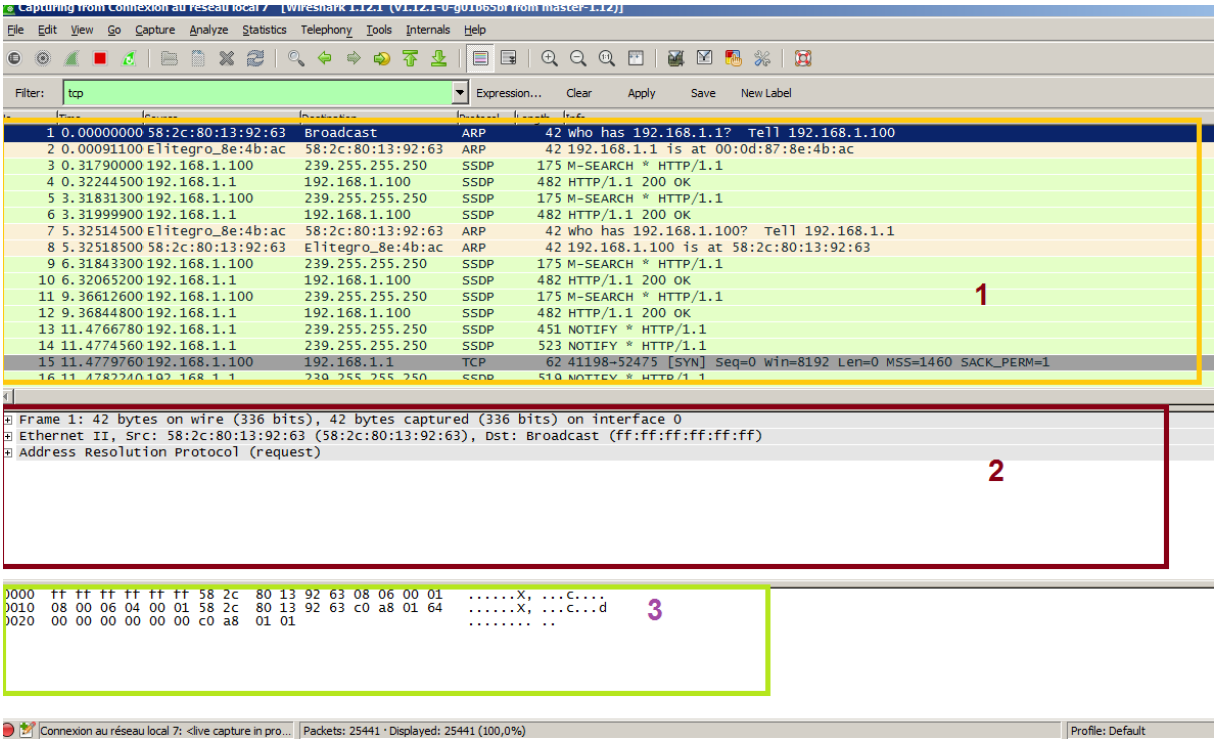
Une fois Wireshark installé, l'interface d'accueil est la suivante



Il faut spécifier en premier lieu l'interface pour lancer la capture sur cette interface.

Capture -> interface : On choisit l'interface qu'on veut utiliser et on commence





L'affichage des résultats se décompose en trois parties :

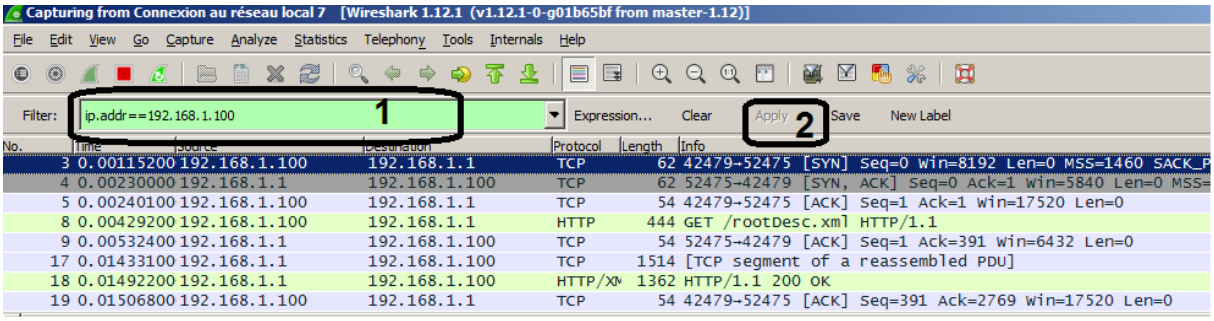
a. La liste des paquets capturés ainsi que leurs caractéristiques principales
b. Le détail de la trame sélectionnée dans le panneau 1.
c. La troisième zone contient la capture affichée en hexadécimal et en ASCII.

Filtrage de paquets

Il est souvent utile de filtrer les paquets à capturer, afin de pouvoir visualiser correctement un certain type de paquets seulement.

En plus des filtres existants par défaut, on peut créer de nouveaux filtres en utilisant la fenêtre capture-> capture filters.

Pour appliquer des filtres on peut préciser dans capture-> options Et on rempli le champ capture filters. Ou bien on spécifie le filtre dans la barre comme suit



Travail demandé :

Lancer l'outil Wireshark et observer les paquets capturés.

1. Quels sont les protocoles utilisés et que vous connaissez.
2. Dans la capture d'écran, le processus commence par la trame 1, qui est une diffusion ARP provenant de l'ordinateur source et qui permet de déterminer l'adresse MAC de la passerelle par défaut du routeur et ensuite ce dernier répond.
    i. Quelle est l'adresse IP de la passerelle par défaut du routeur et son adresse MAC
    ii. Quelle est l'adresse IP de l'ordinateur source et son adresse MAC, vérifiez s'il s'agit des mêmes informations de votre ordinateur
3. Ouvrez dans le navigateur www.google.tn. Une fois la page ouverte arrêter la capture

La trame est une requête DNS transmise de l'ordinateur vers le serveur DNS configuré, qui tente de convertir le nom de domaine www.google.com en adresse IP du serveur Web. L'ordinateur doit disposer de l'adresse IP pour pouvoir envoyer la première trame au serveur Web.

    i. Quel est le port utilisé
    ii. Quelle est l'adresse IP du serveur DNS requise par l'ordinateur ?
    iii. Quelle est l'adresse IP du serveur Web de Google ?

4. Ouvrez une fenêtre de commande DOS (menu Démarrer - > Exécuter -> cmd), et lancer un Ping sur www.google.fr. Quand le Ping s'arrête, arrêter la capture sous Wireshark en cliquant sur l'icône adéquate.
    i. Quel est le protocole utilisé pour le Ping ? quel est le port utilisé ?