Wireshark - Installation et utilisation

Difficulté : Confirmé

Notions : Réseaux, protocoles, analyse de trame.

I.Introduction

Ce document a pour but de vous apprendre à utiliser les fonctions basiques de wireshark. Ce qui peut être utile pour annalyser la cause d'un problème réseau ou tester le bon fonctionnement d'un protocole.

> Wireshark peut être téléchargé ici : Download Wireshark

> Prérequis : Un poste sous Windows 7 minimum, Une carte réseau RJ45 ou une carte wifi.

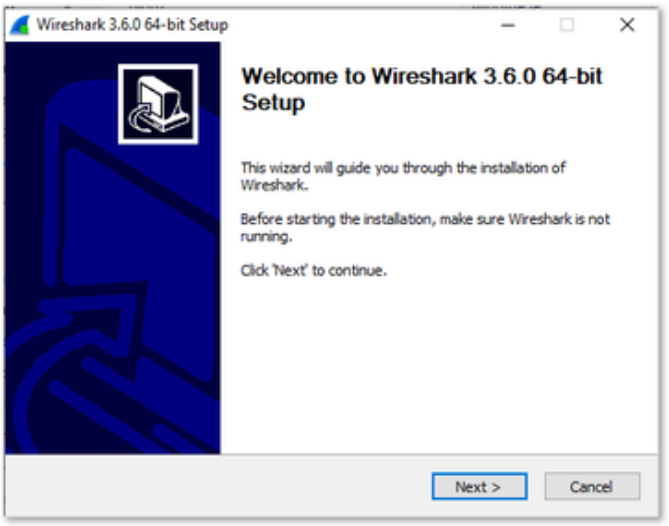
II. Installation

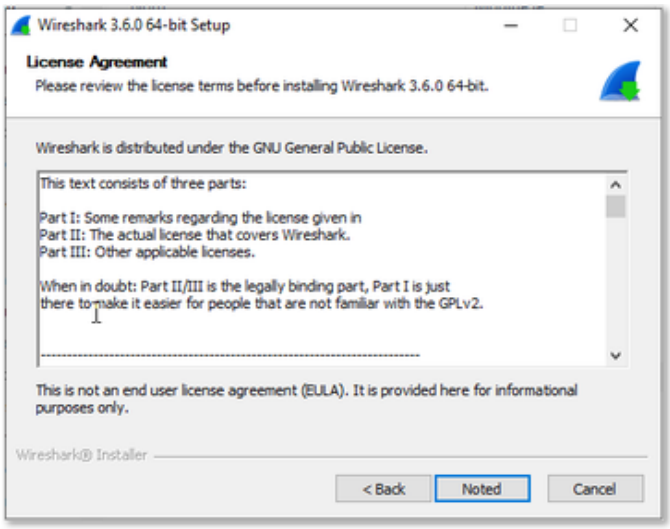
2.1 Lancement de l'installation

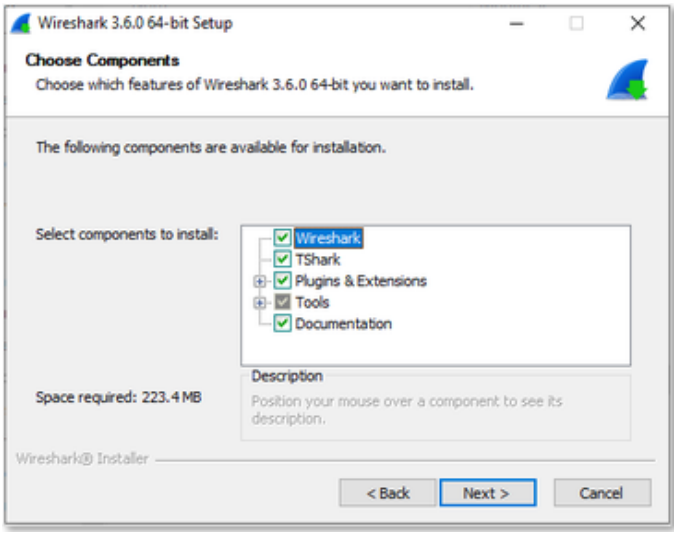
Lancer l'installer.

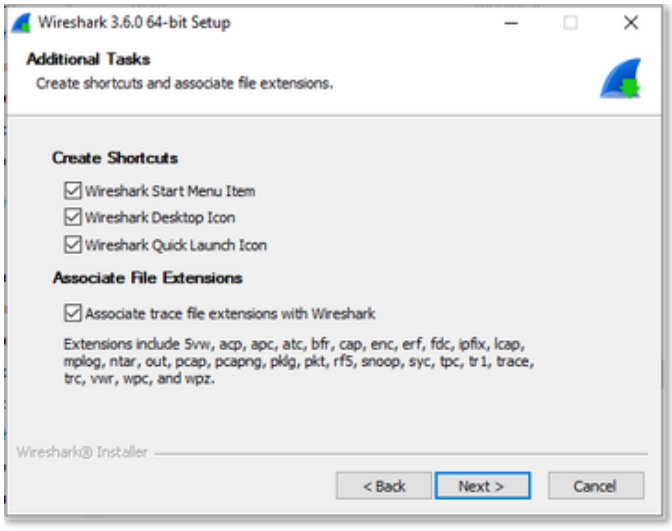
Wireshark-win64-3.6.0

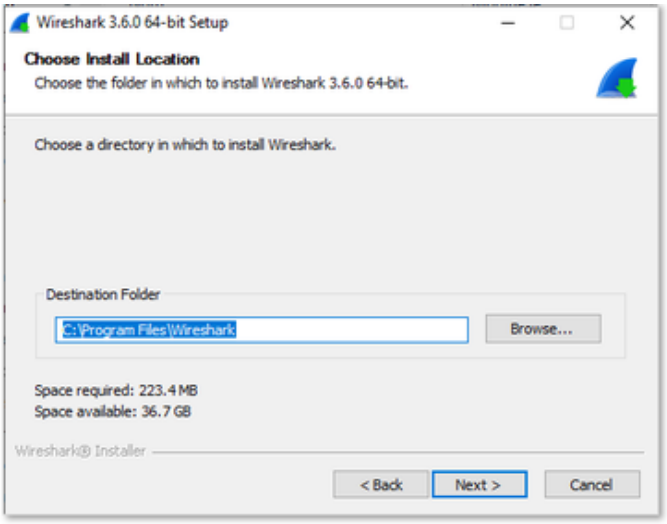
L'installation est basique. Il suffit de suivre l'assistant d'installation.

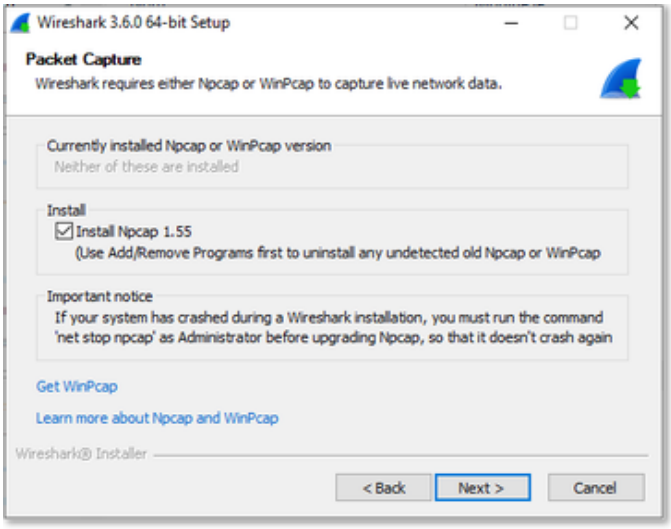


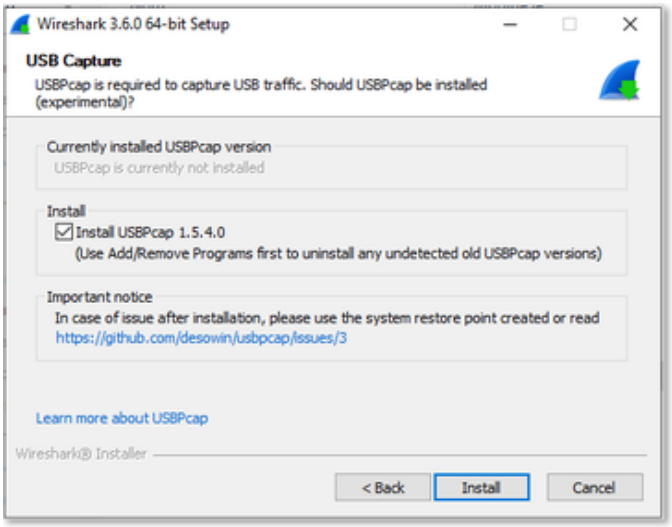


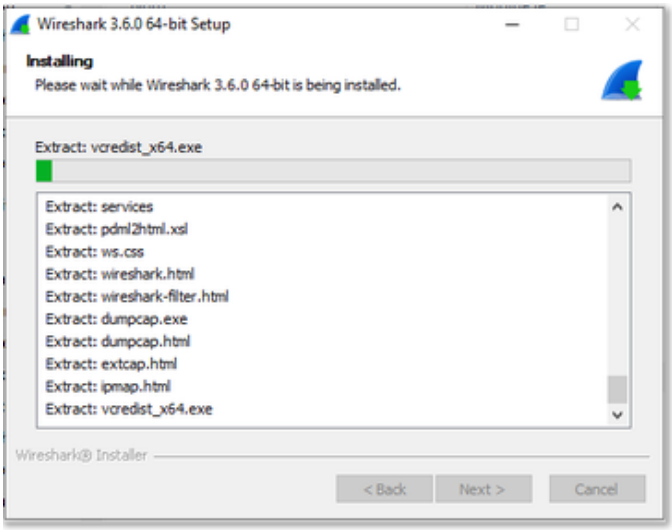






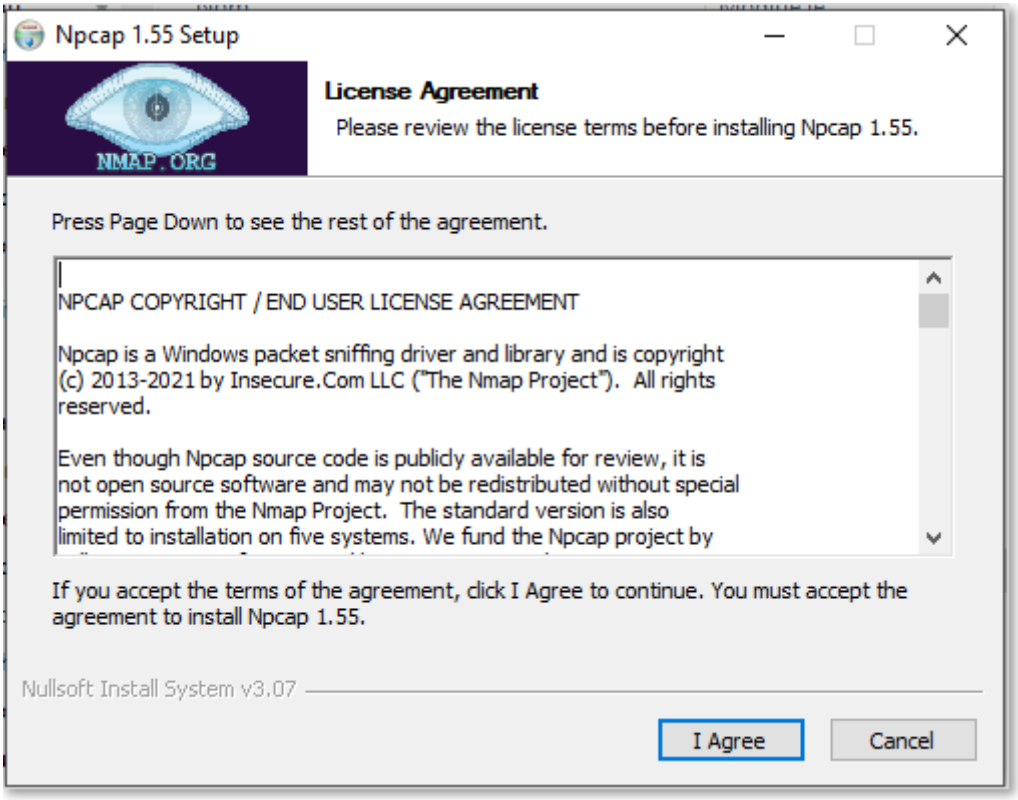




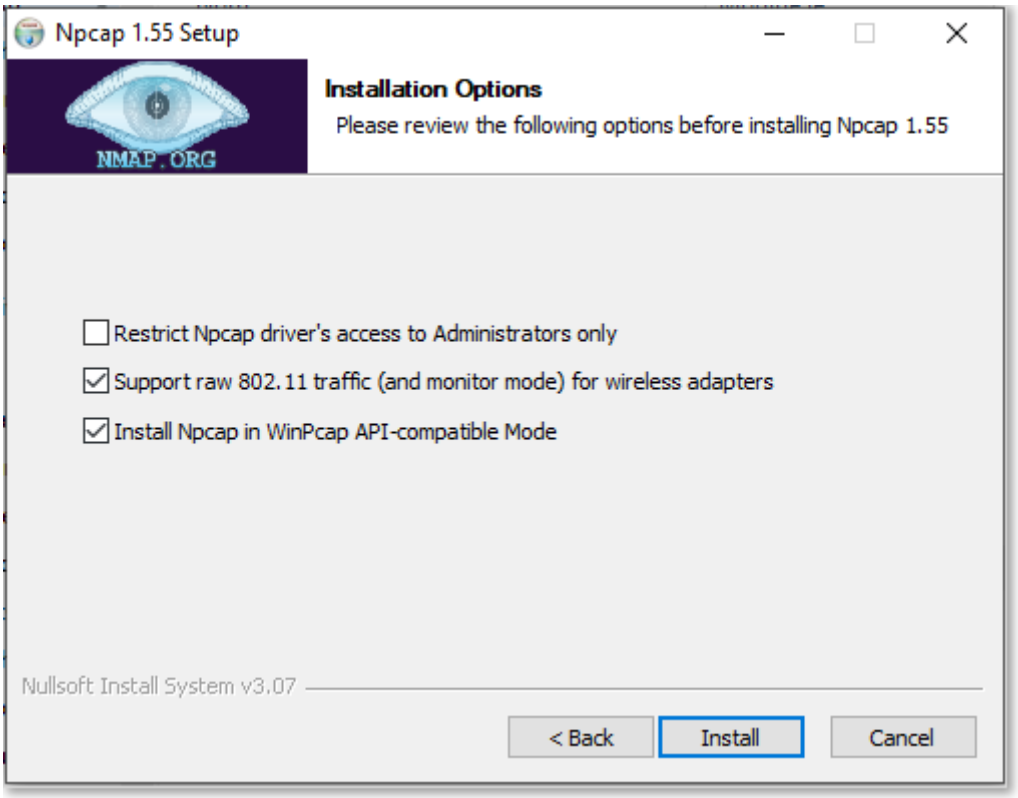


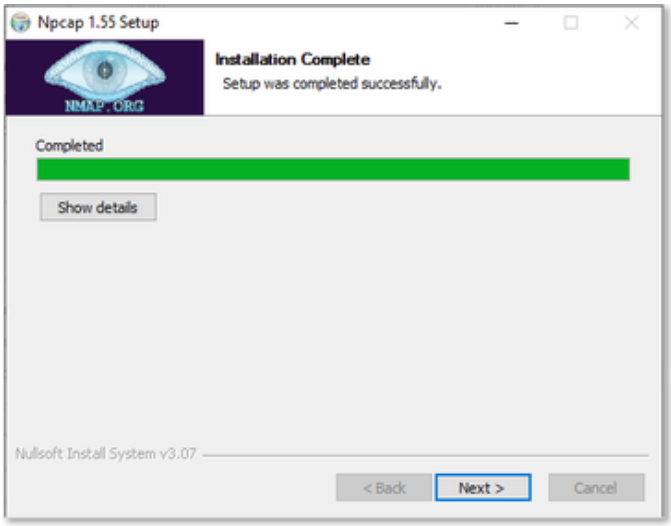
2.2 Installation de Npcap

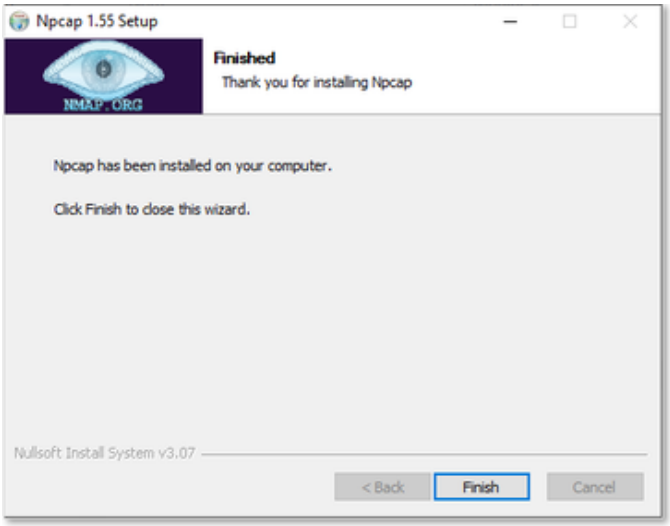
Lors de l’installation de Npcap, Valider en Cliquant sur ‘***I Agree***’



Cocher les cases suivantes :

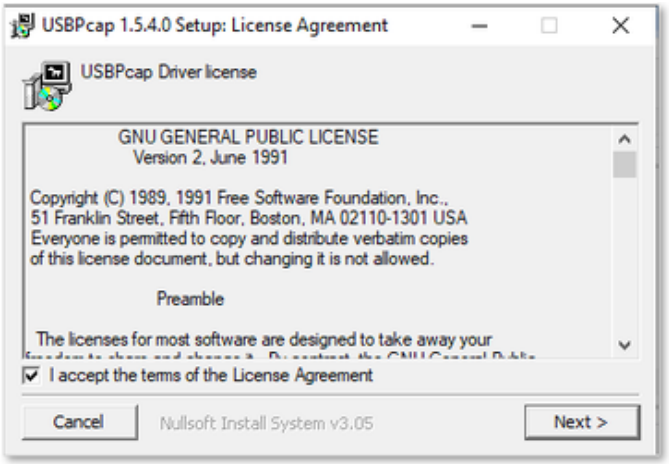


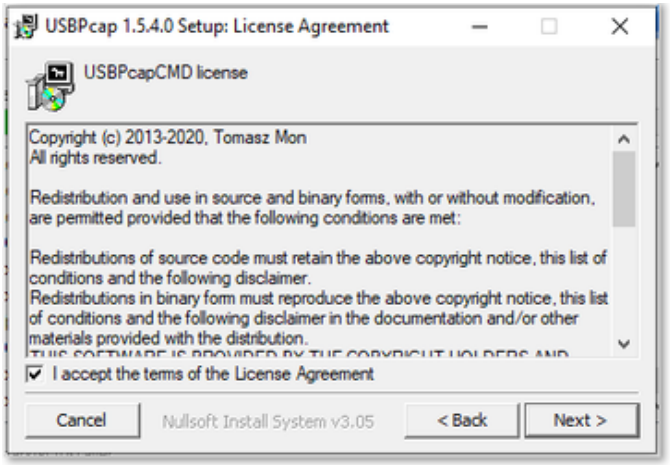




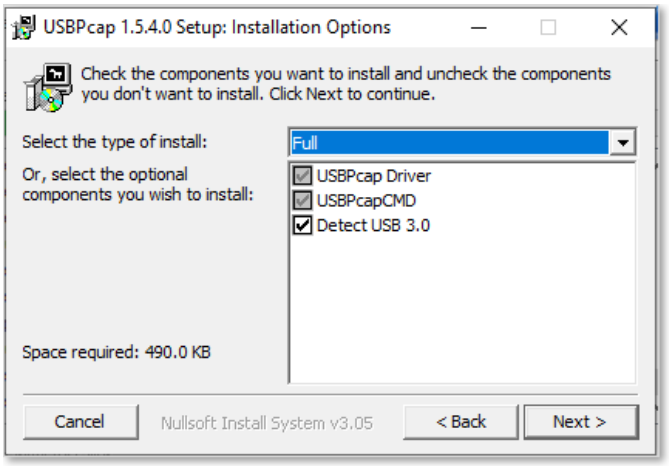
2.3 Installation de USBpcap

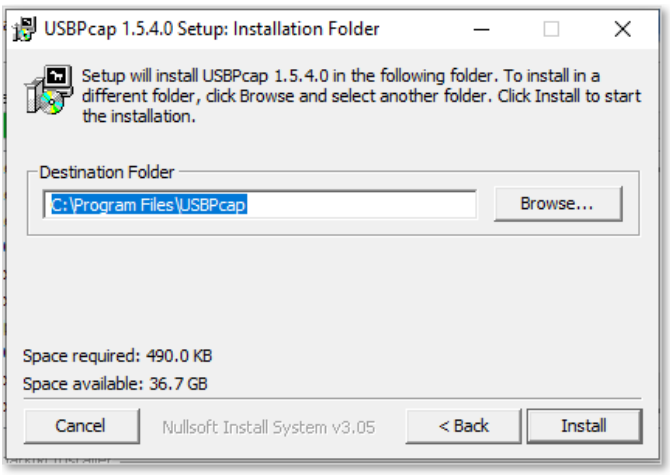
Puis, Installer USB Pcap. Cocher les deux cases et cliquer sur suivant.

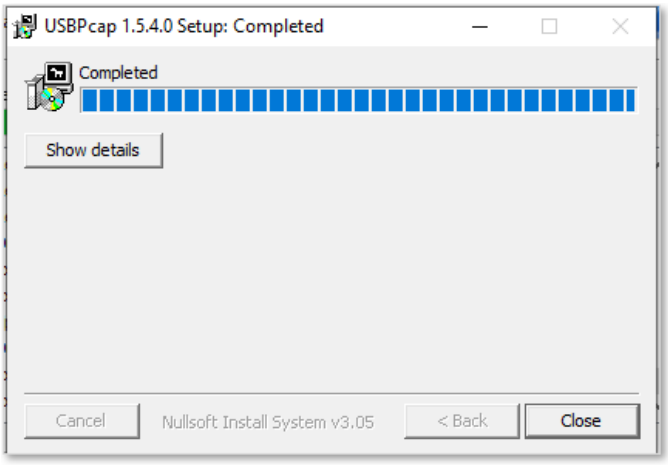




Laisser les cases cochées et terminer l’installation.

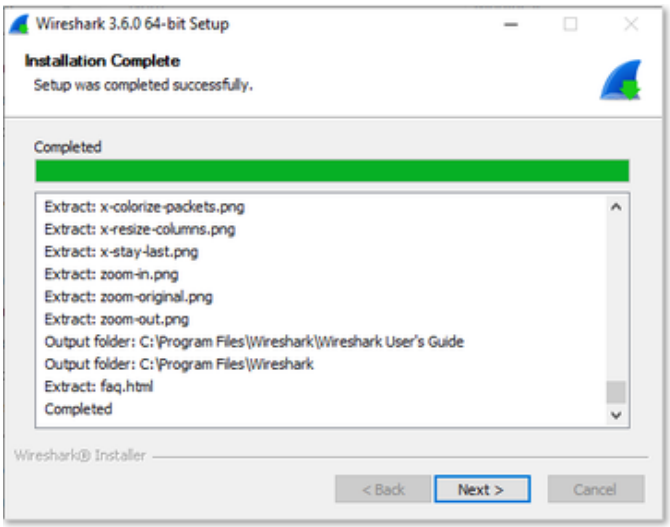


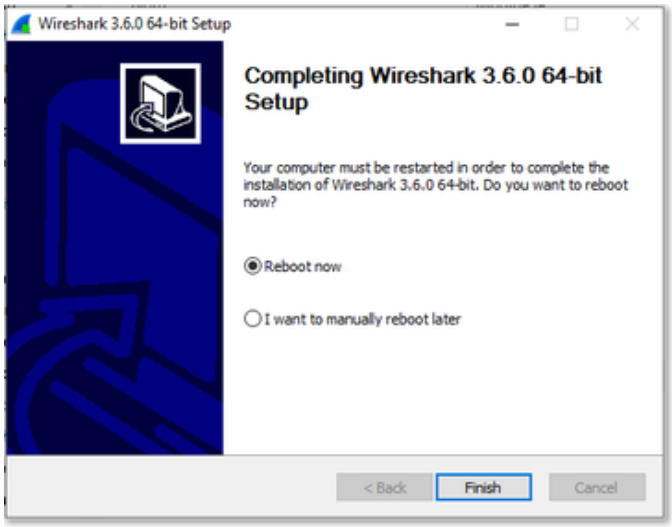




2.4 Fin de l'installation

Terminer l’installation.



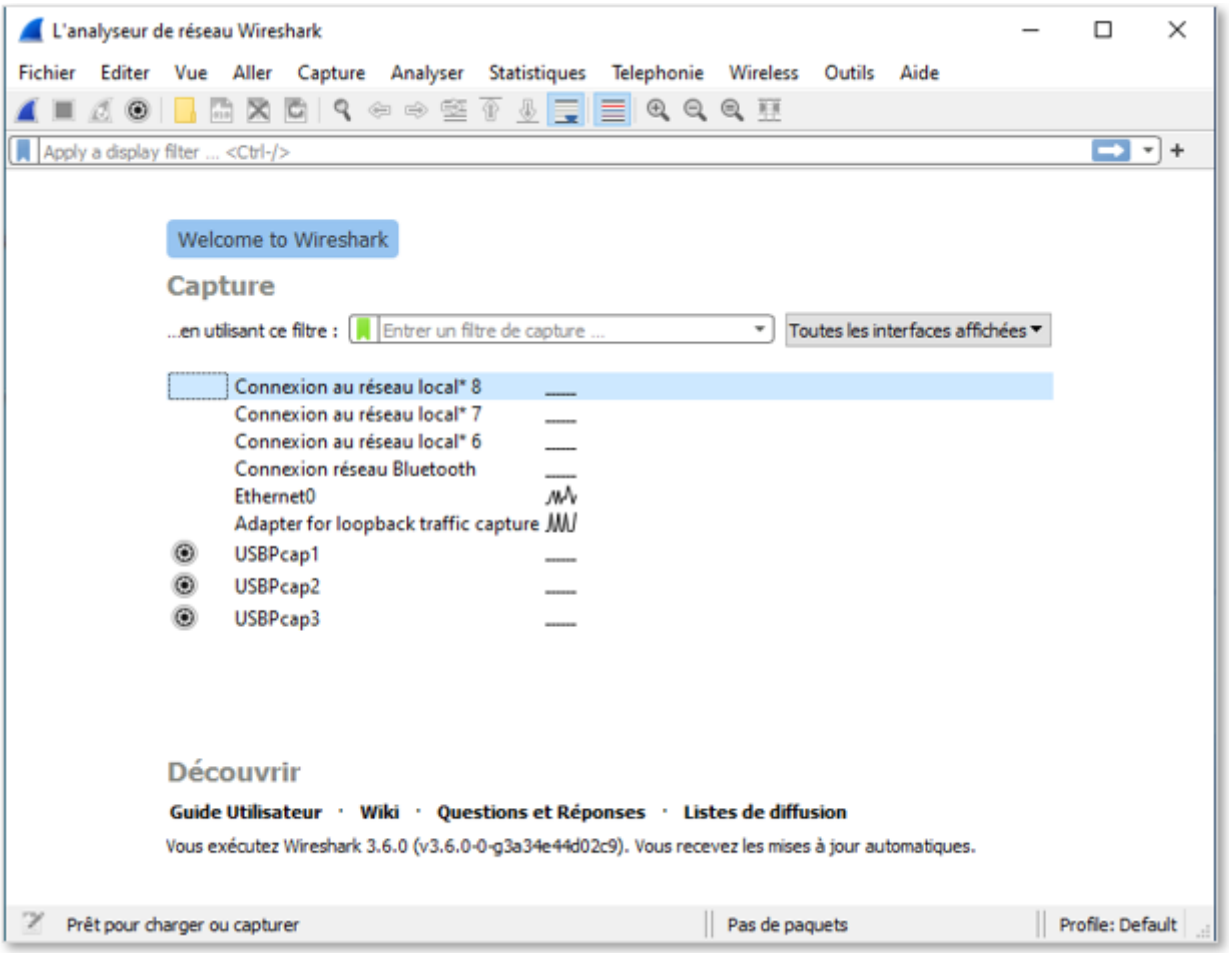


III. Démarrer une capture

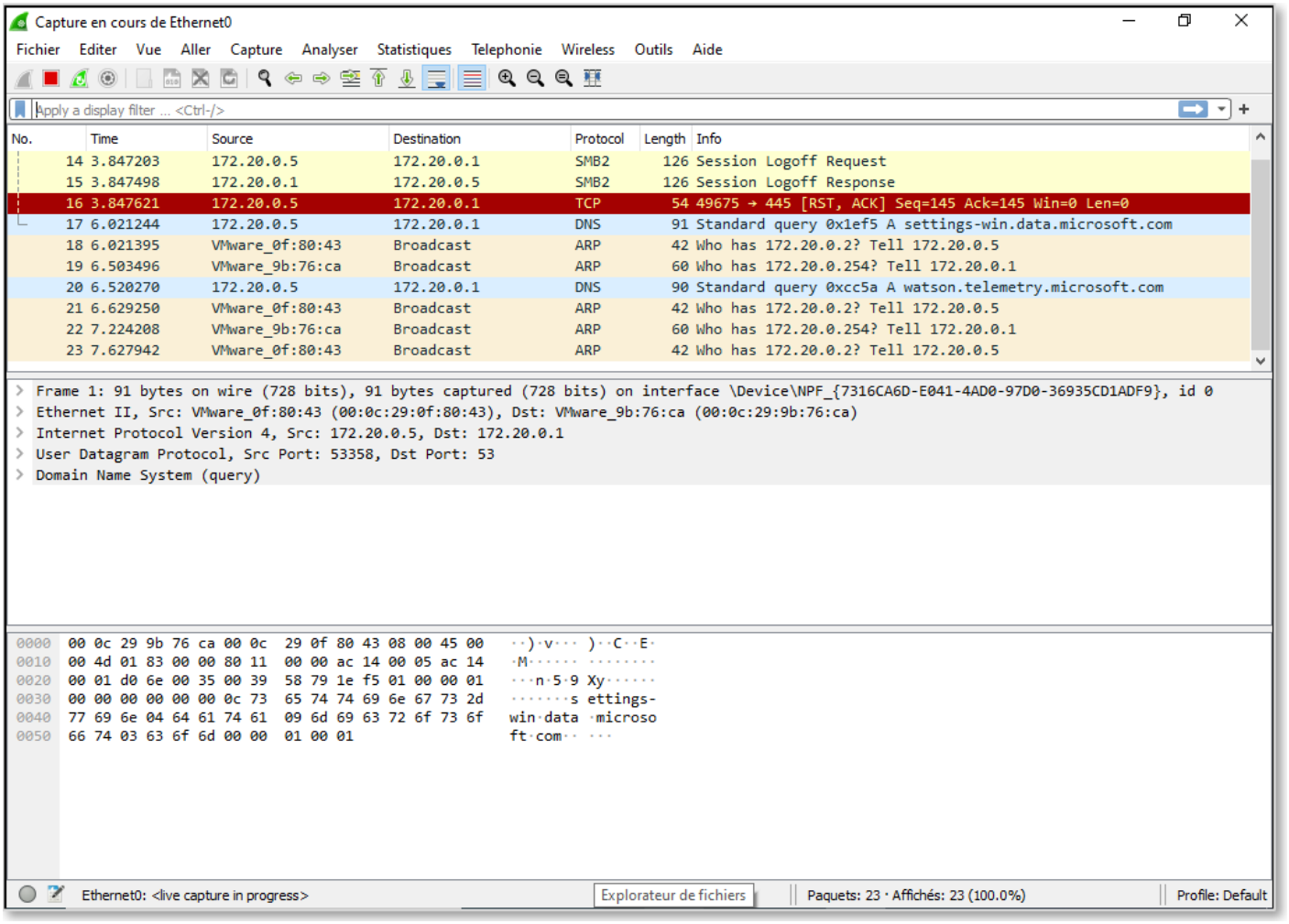
Lancer le programme.

Sélectionner l’interface réseau à utiliser.

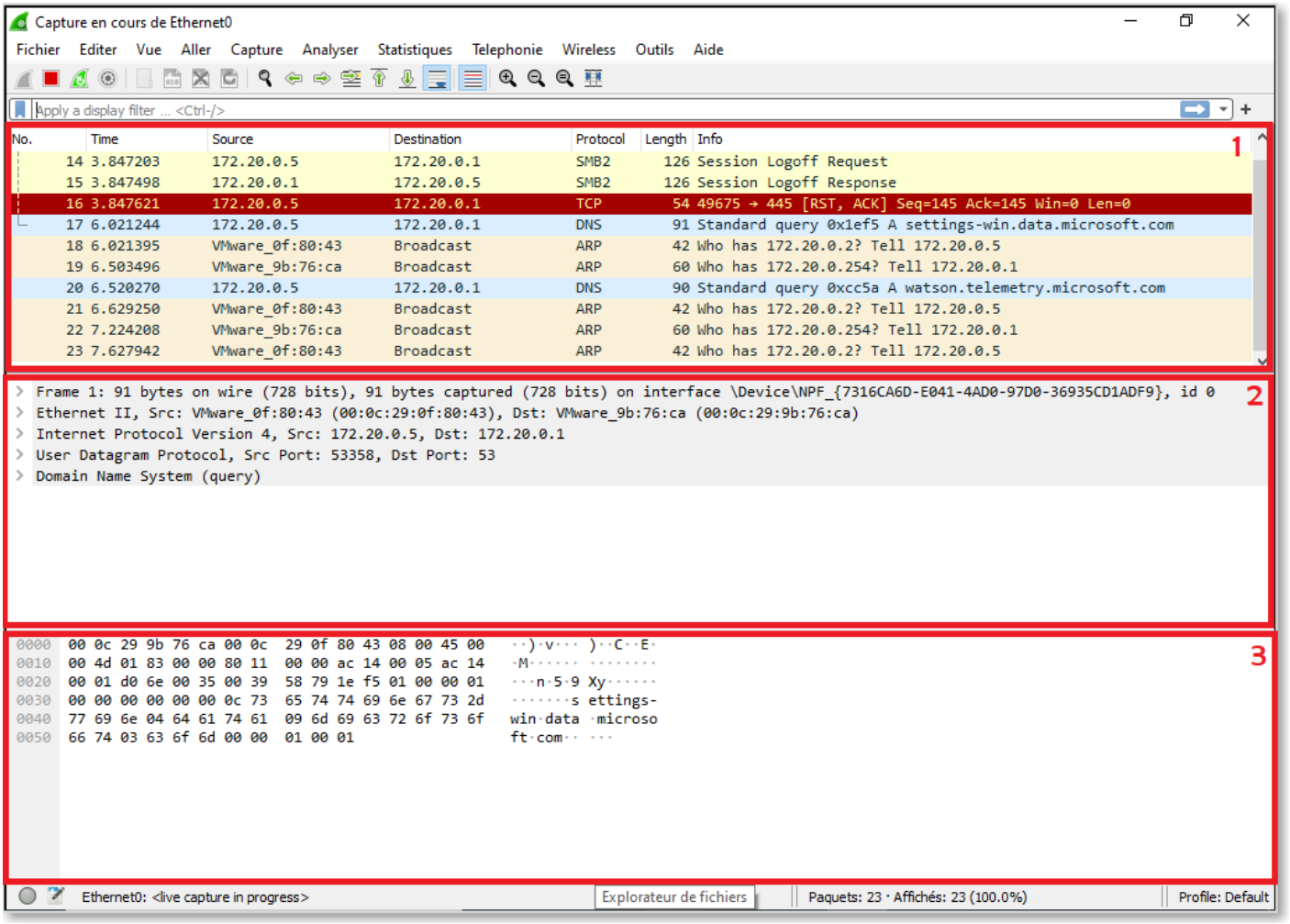
(ici : Ethernet0)



La capture se lance et les paquet capturés apparaissent.



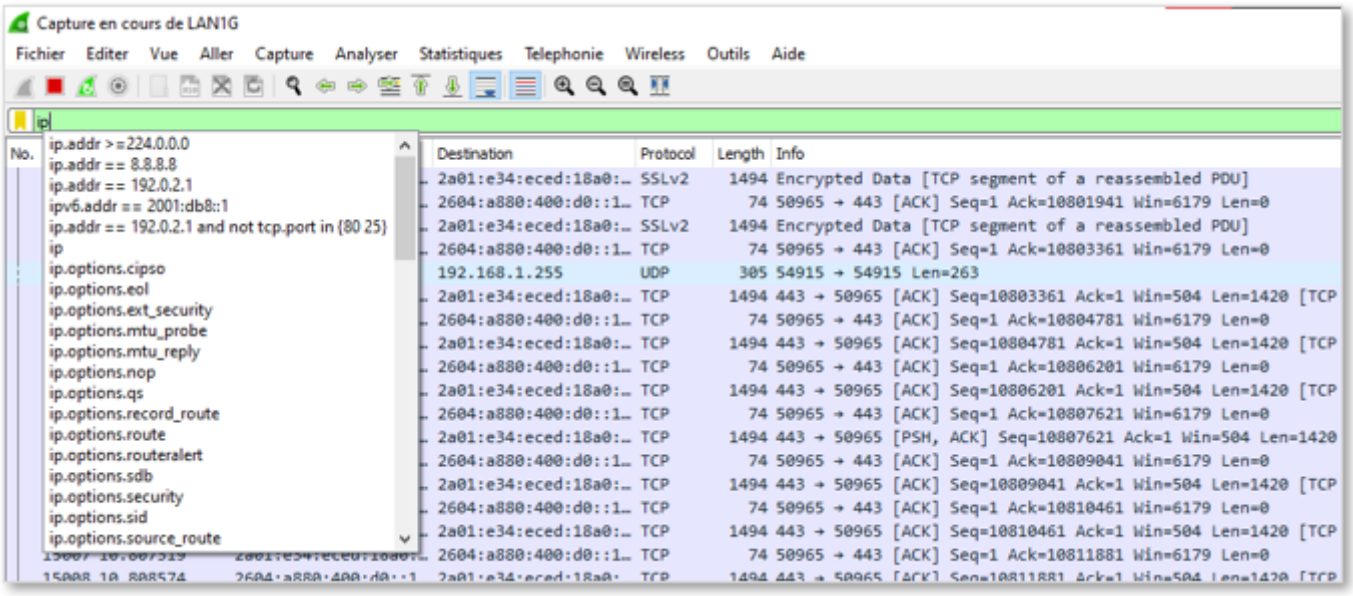
La fenêtre est composée de Trois espaces :



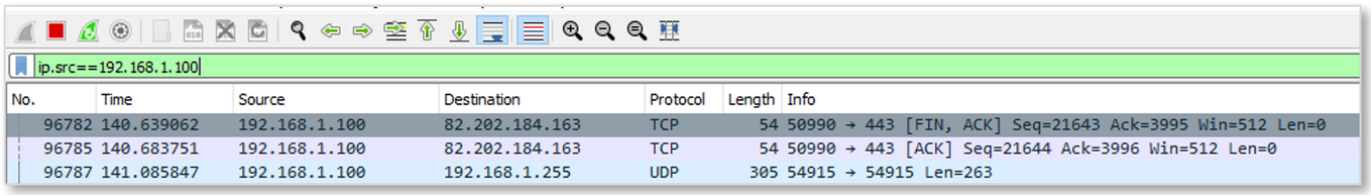
1. Liste des paquets capturés. Par défaut, cela défile en temps réel et ne trie pas les paquets.
2. Contenu de la trame découpée par blocs.
3. Contenu du paquet affiché en hexadécimal et texte.

IV. Utiliser les filtres

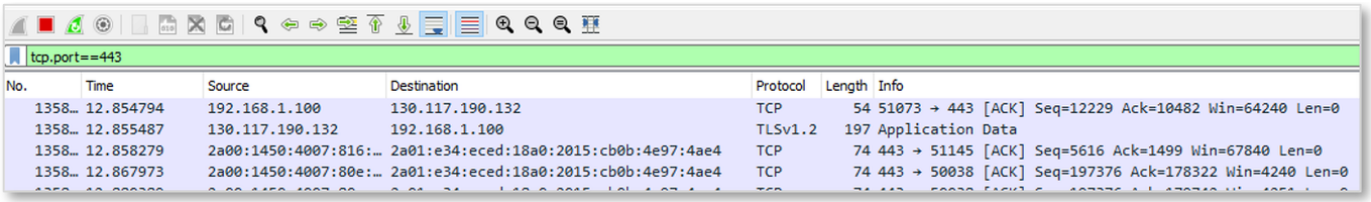
Afin de rendre la capture plus facile et lisible, il est possible de filtrer sur une IP ou un protocole particulier.



Par exemple :



ip.src==192.168.1.100 permet d'afficher tous les paquets provenant de l'hôte avec l'ip 192.168.1.100

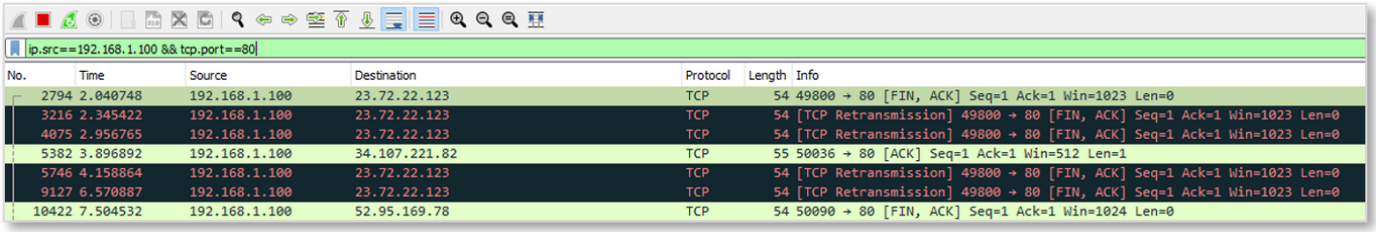


tcp.port==443 Permet d'afficher tout les paquets utilisant le port HTTPS.

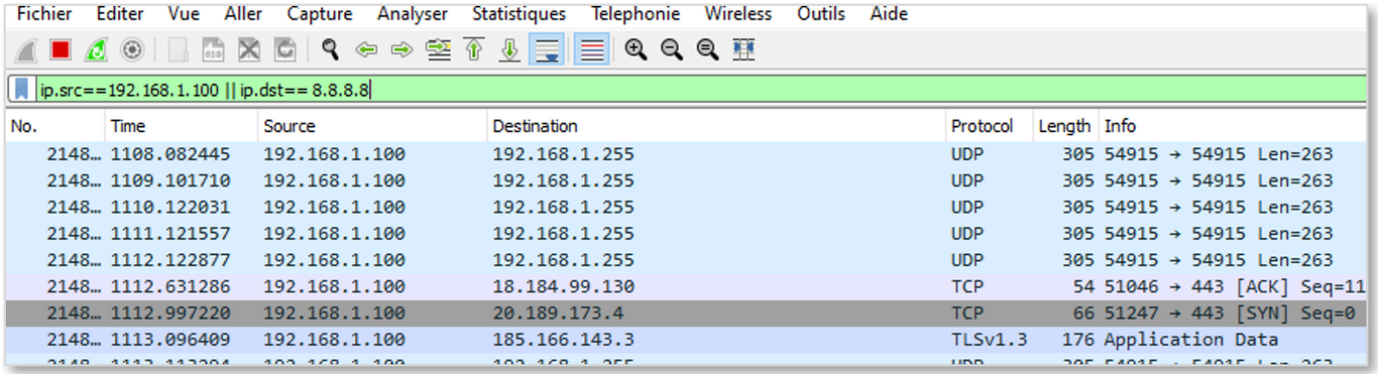
Il est également possible de combiner des filtres avec des opérateurs.

- && : et
- || : ou
- != : non égal à

Par exemple :



ip.src==192.168.1.100 && tcp.port==80 Permet d'afficher tout les paquets provenant de 192.168.1.100 sur le port 80.



ip.src==192.168.1.100 || ip.dst== 8.8.8.8 Permet d'afficher tout le trafic en provenance de 102.168.1.100 OU à destination de 8.8.8.8

> Pour plus de filtres : DisplayFilters

Revision #2
Created 2026-07-29 14:04:53 UTC by Olivier
Updated 2026-07-29 14:14:01 UTC by Olivier