# Logiciel d’analyse de capture de trames avec Wireshark

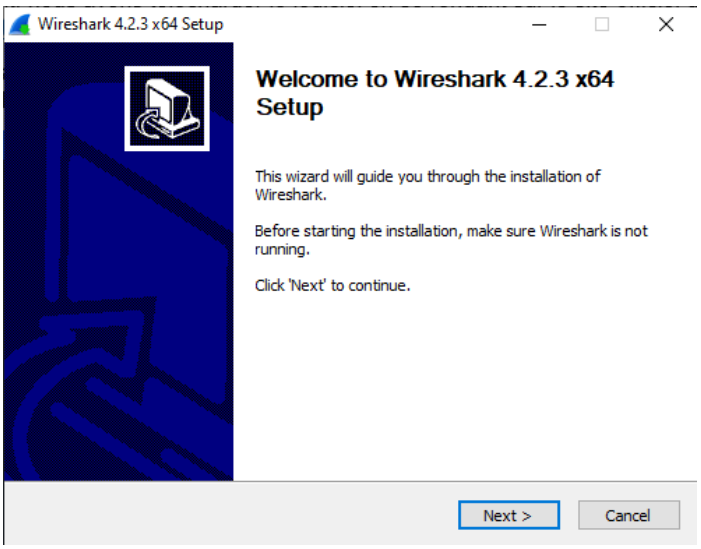
Wireshark est un logiciel utilisé pour l'analyse des réseaux informatiques. Il permet de capturer et d'examiner le trafic réseau en temps réel sur une interface réseau spécifiée. Wireshark est capable d'intercepter et d'afficher le contenu des paquets de données qui transitent sur le réseau, ce qui permet aux administrateurs système, aux professionnels de la sécurité informatique et aux développeurs de comprendre le fonctionnement du réseau, de diagnostiquer les problèmes de performance ou de sécurité, et d'analyser le comportement des applications.

## Télécharger Wireshark :

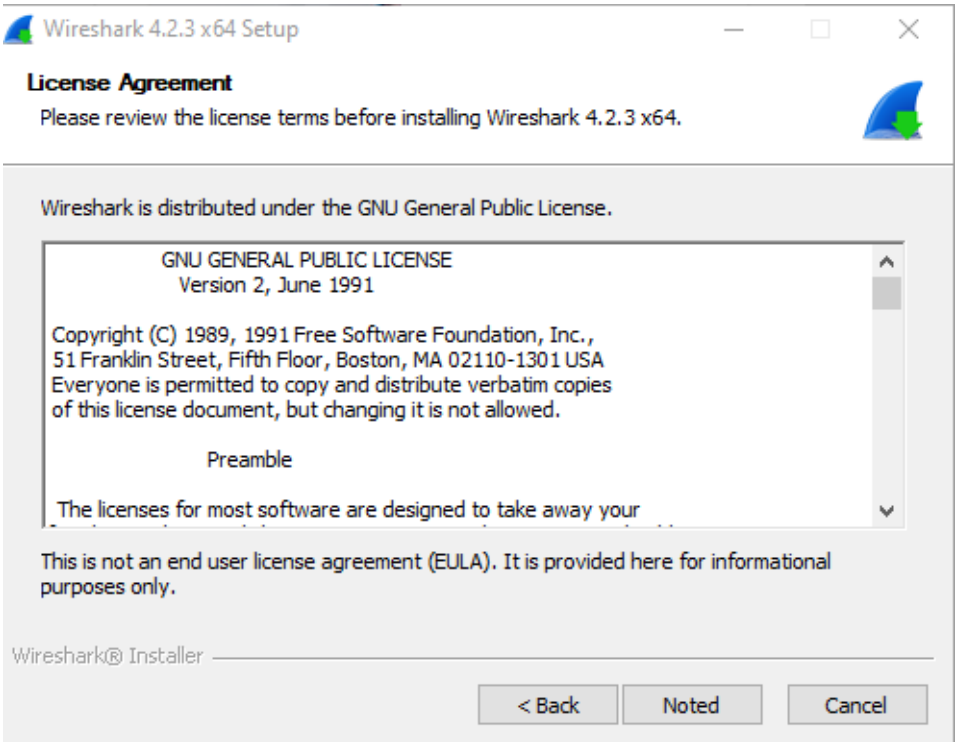
Premièrement, nous avons télécharger le logiciel en se rendant sur le site officiel de Wireshark (https://www.wireshark.org/download.html).

Sur la page suivante on choisit la meilleure version pour notre machine. Dans notre cas **"Windows x64 installer"**.

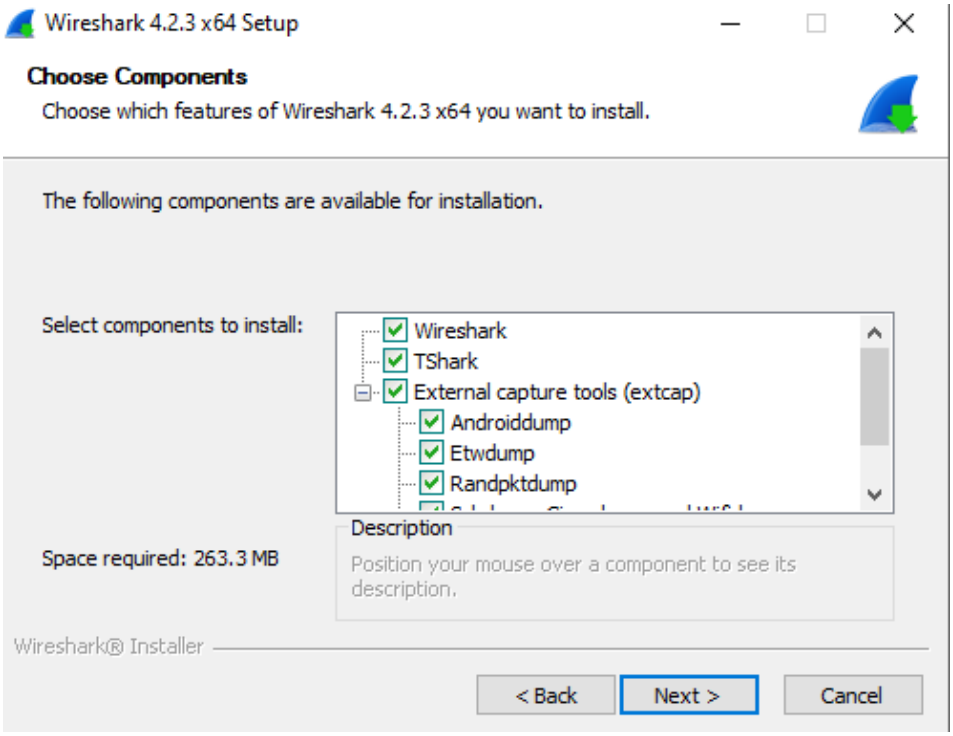

Ensuite on l’exécute sur notre machine. Dans notre cas nous l’avons installé sur notre Windows server 2019 qui contient l’Active Directory Primaire (**LPRS-ADP**). Nous arrivons sur le setup d’installation, il suffit de cliquer sur **"Next"**.



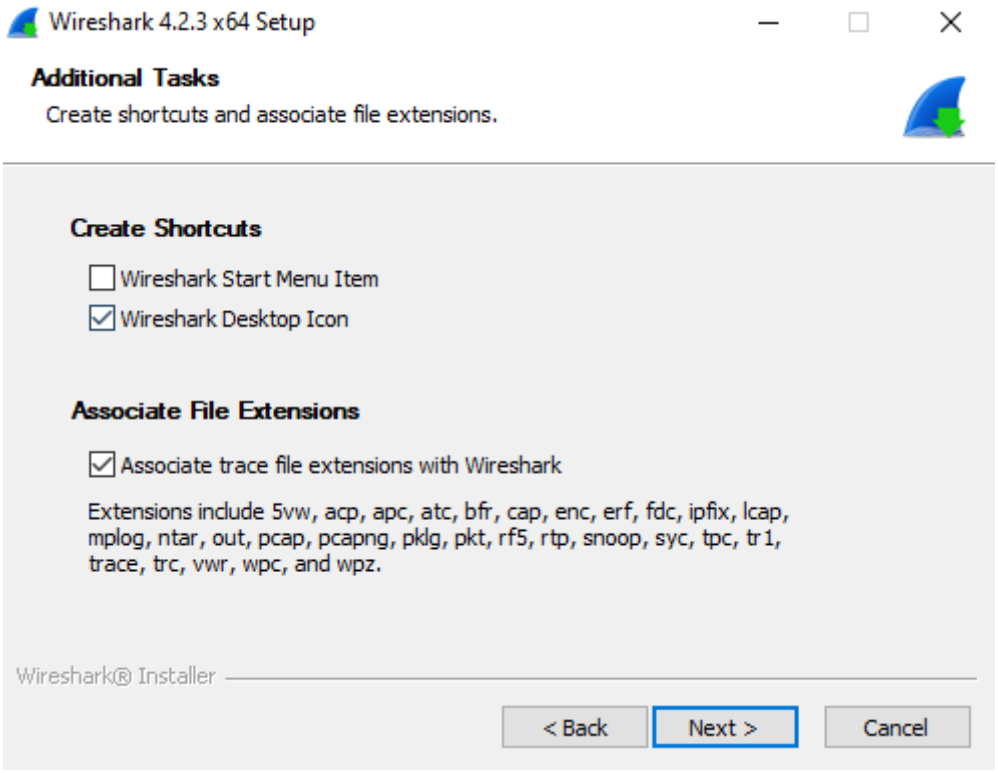
Il faut accepter la licence d'utilisation pour continuer l'installation, il faut cliquer sur "**Noted**".



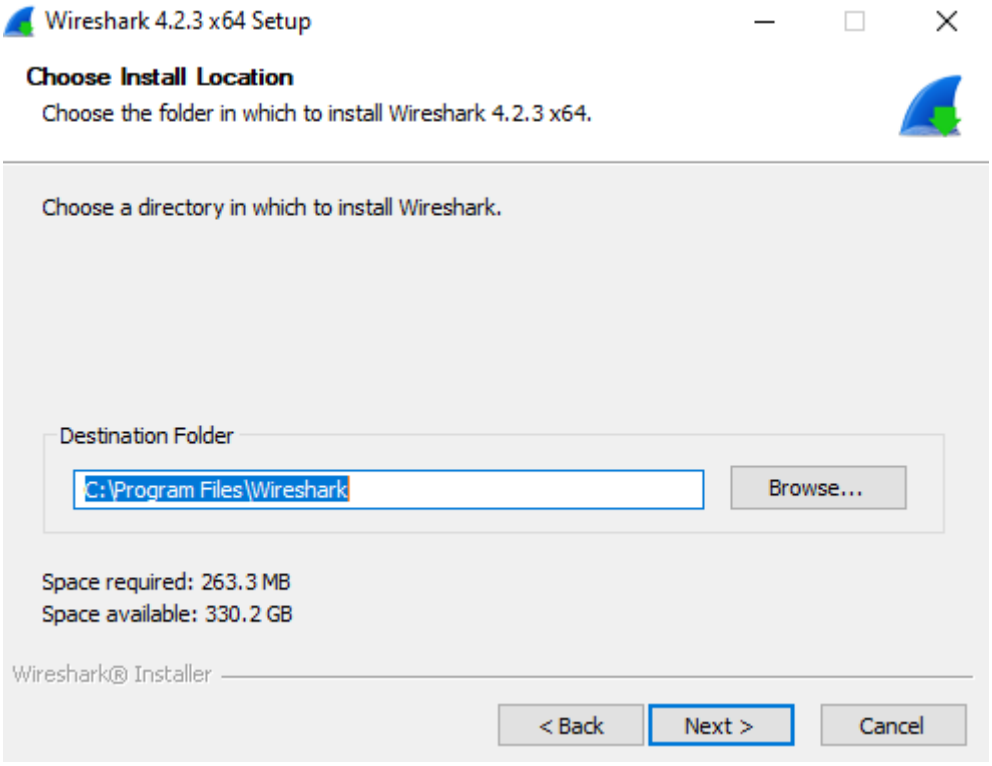

Ici, on va choisir l'ensemble des composants que nous souhaitons installer, comme les outils en ligne de commandes dont fait partie **Tshark**, ou bien les utilitaires comme **Editcap** qui permet d'éditer des traces réseau. On coche tout et on peut cliquer sur "**Next**".



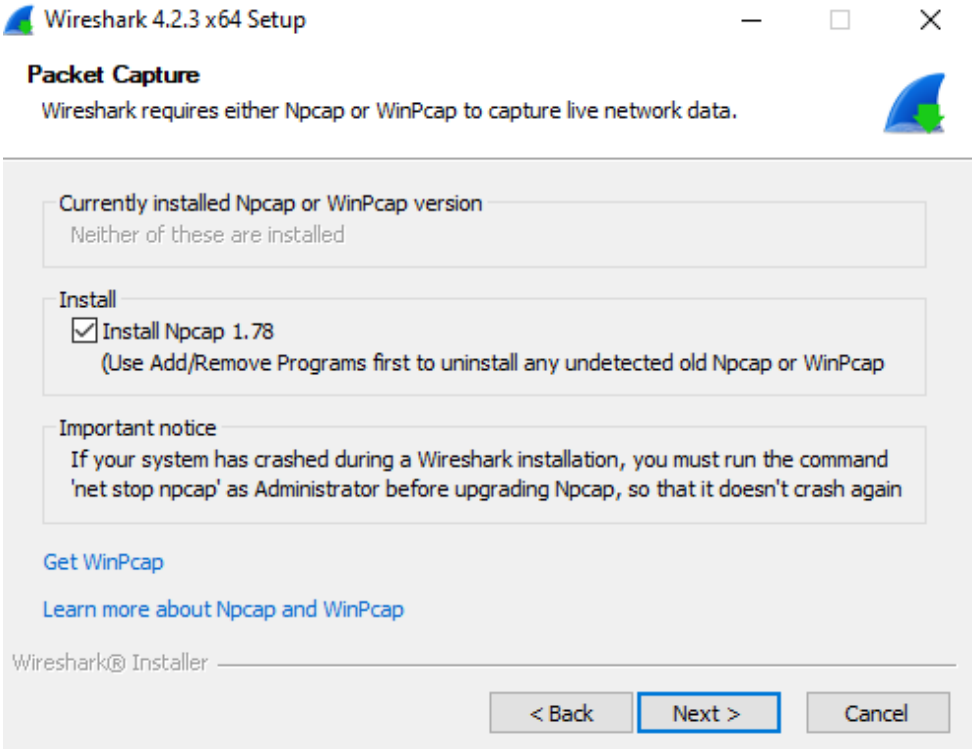
Ici on sélectionne l'option **"icône sur le bureau"**. L'autre option que propose Wireshark, c'est de pouvoir associer l'ouverture d'extension de fichier de capture appartenant à d'autres outils de capture, comme cap, qui est l'extension de fichier par défaut d'une capture venant d'un load-balancer Citrix. Donc, ici, on coche la case et ensuite on clique sur "**Next**".



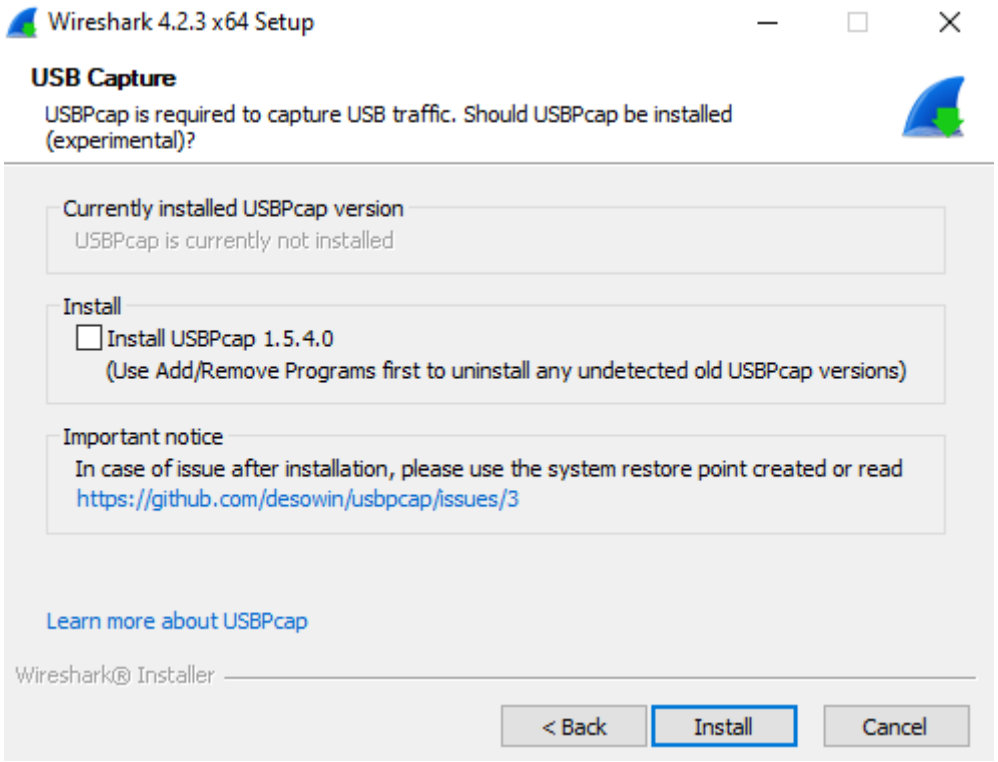

Par la suite, on sélectionne le répertoire d'installation de Wireshark et on clique sur "**Next**". Dans notre cas nous l'avons laissé par défaut.



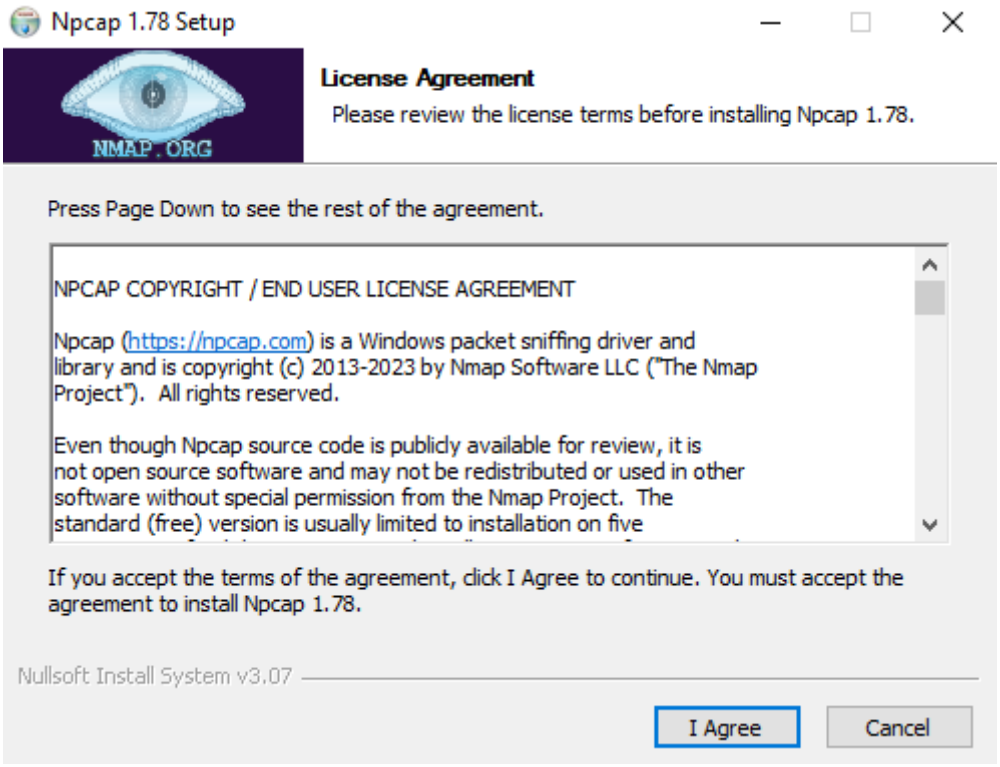
Afin que Wireshark puisse capturer des paquets, il faut installer l'outil **Npcap.** Si on ne l'installe pas, on pourra uniquement lire des fichiers de capture. Ici, on coche donc "**install Npcap 1.78**" et on clique sur "**Next**".



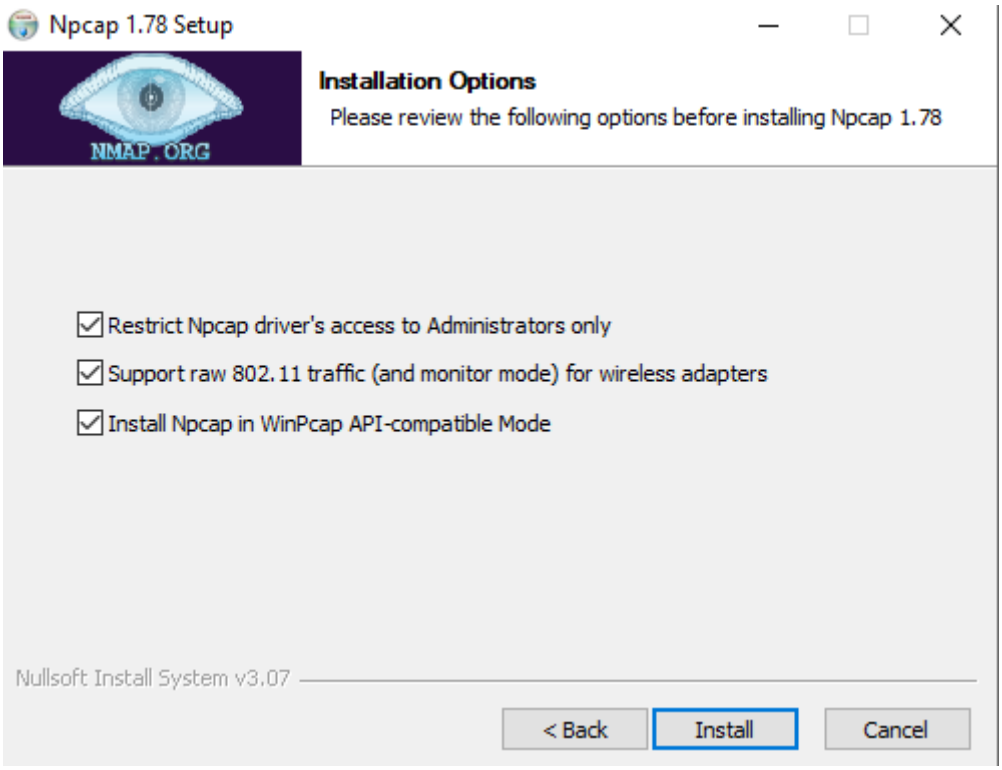

Wireshark est capable de capturer les échanges USB via l'utilitaire USBPcap, on peut l'installer si on souhaite analyser des échanges USB. Dans notre cas nous n'en avons pas besoin, on laisse et on clique sur **"Install"**



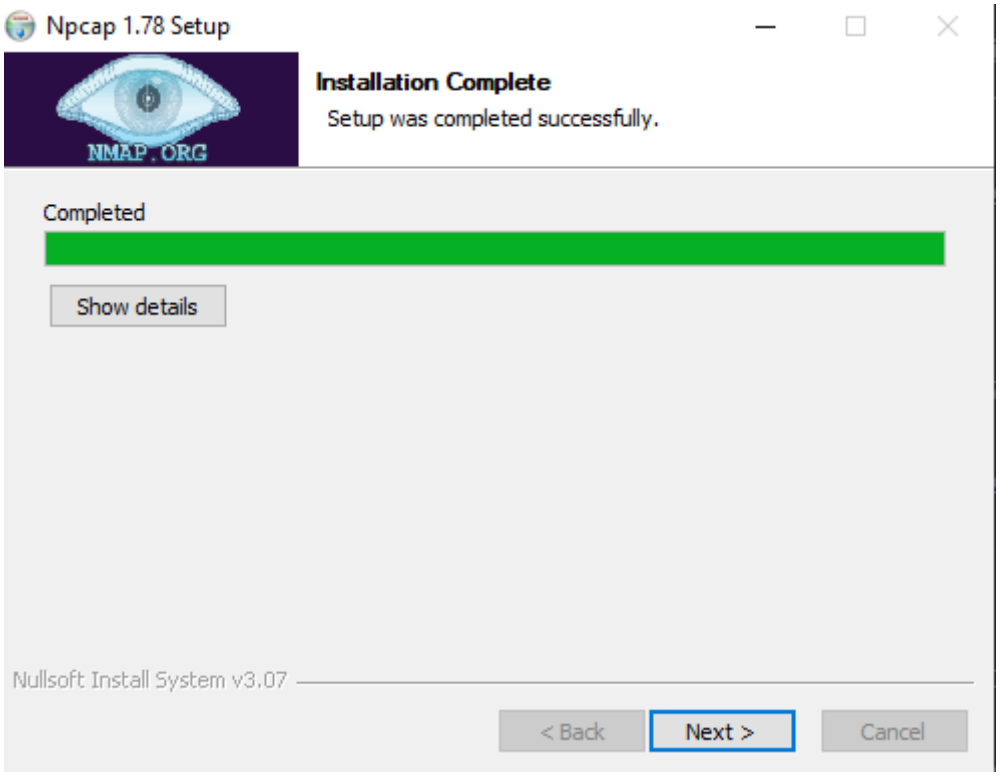
Nous devons maintenant installer **npcap**. C'est indispensable pour réaliser des captures. Ici, on valide la licence d'utilisation **npcap** pour continuer l'installation et on clique sur **"I Agree"**.



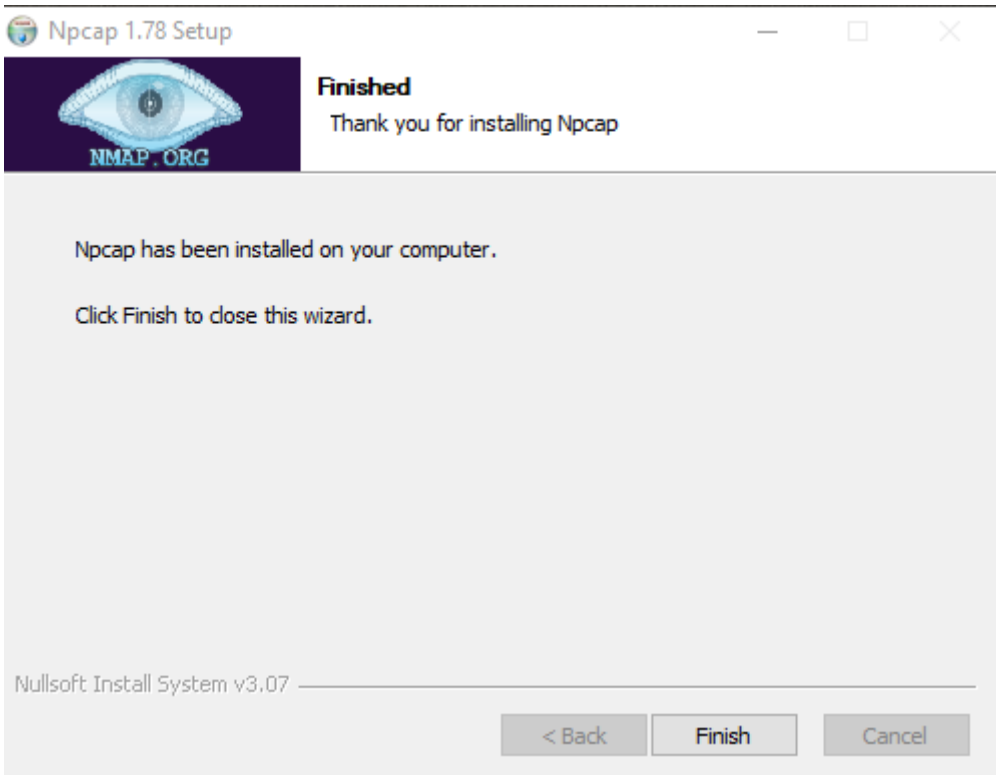

Ensuite, nous allons choisir les options d'installation. Ici on coche les 3 option et on clique sur **"Install"** pour lancer l'installation de **npcap**.



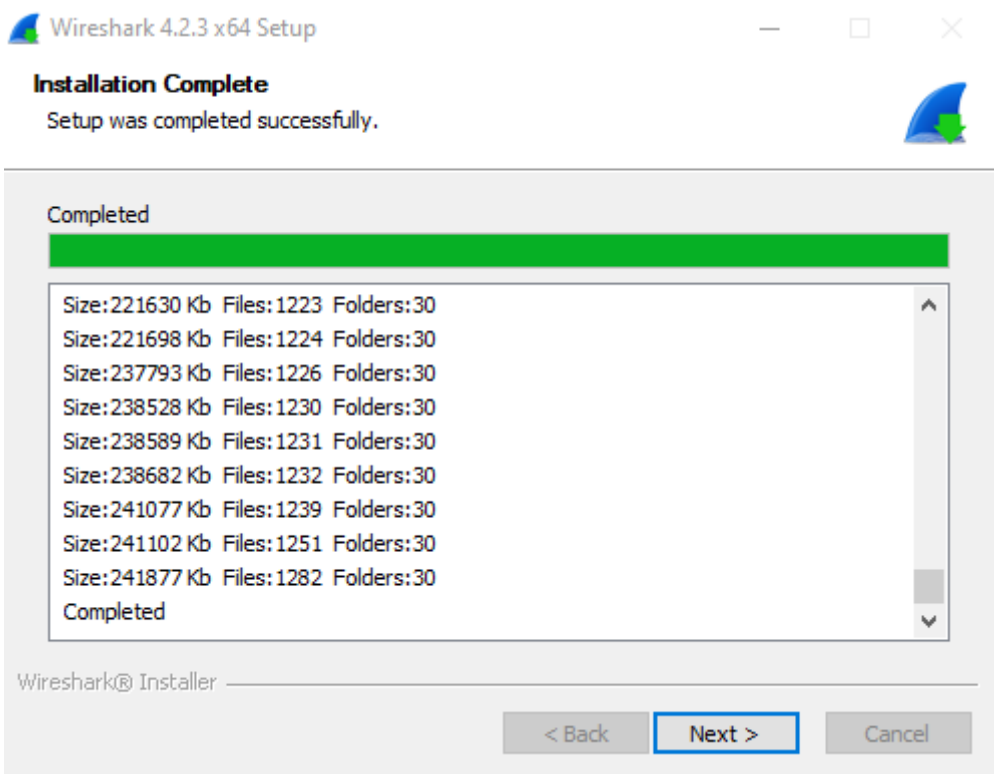
Enfin, pour terminer l'installation de **npcap**, il suffit de cliquer sur **"Next"**.



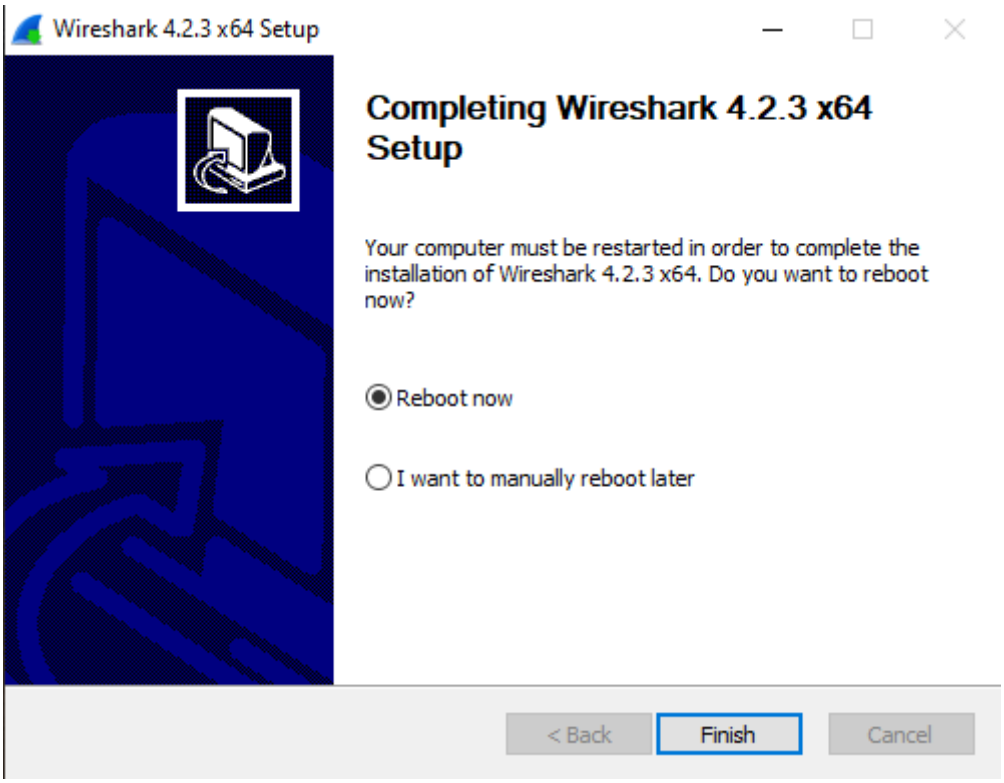

L'installation de **npcap** est terminée, maintenant il faut cliquer sur **"Finish"** pour filer vers la fin de l'installation de Wireshark.



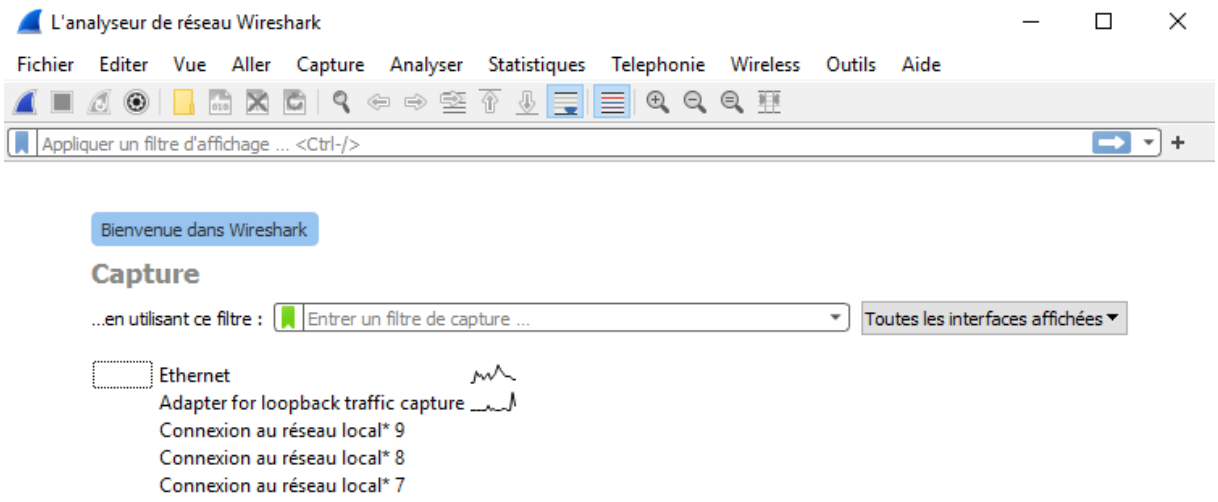
Dès que **npcap** est finie d'être installé, Wireshark termine son installation à son tour. Dès que c'est fait, il faut cliquer sur **"Next"** pour finaliser l'installation.




L'installation de Wireshark est terminée ! il ne reste plus qu'à cliquer sur **"Finish"**.



Maintenant on ouvre Wireshark sur notre machine. L'ensemble de nos interfaces réseau apparaissent.




On est maintenant prêt à lancer la capture d'une trace réseau. Il suffit de **double cliquer sur une interface réseau** et la **capture se lance**.