Document d'exploitation

BUON Jérémy
BTS SIO SISR

Table des matières

○ Définition

Wireshark est un logiciel open-source de capture et d'analyse de paquets réseau. Il est largement utilisé par les professionnels des réseaux et les chercheurs en sécurité pour examiner le trafic réseau et comprendre le fonctionnement des protocoles.

Avec Wireshark, vous pouvez capturer et examiner le trafic réseau en temps réel ou à partir de fichiers de capture préalablement enregistrés. Il prend en charge une large gamme de protocoles réseau, tels que TCP/IP, DNS, HTTP, FTP, SSH, et bien d'autres. Wireshark peut être utilisé pour diagnostiquer les problèmes de réseau, analyser les performances, déceler les problèmes de sécurité, et effectuer des tests de conformité des protocoles.

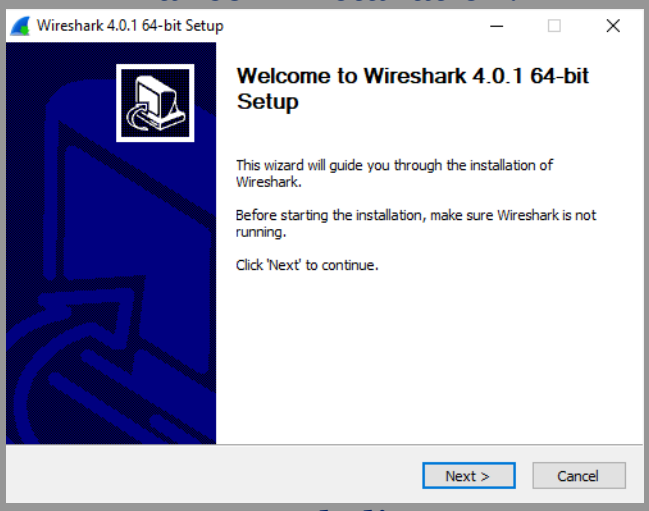
Wireshark dispose d'un riche ensemble de fonctionnalités :

- Inspection approfondie de centaines protocoles, avec d'autres ajoutés en permanence ;
- Capture en direct et analyse hors-ligne ;
- Navigateur de paquets standard à trois volets ;
- Fonctionne sous Windows, Linux, macOS, Solaris, FreeBSD, NetBSD…
- Les données réseau capturées peuvent être consultées via une interface graphique ou via l'utilitaire TShark en mode TTY.
- Les filtres d'affichage les plus puissants de l'industrie
- Analyse riche de la VoIP.

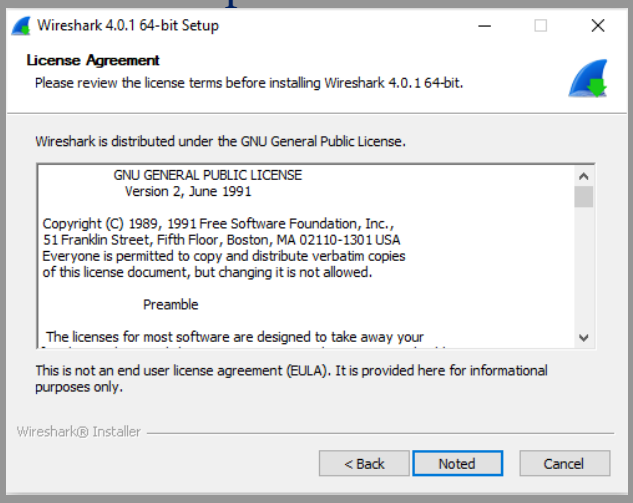
Installation

Pour télécharger Wireshark, il faut suivre le lien : Wireshark · Go Deep.. Aller sur la rubrique Download, puis sélectionner la version correspondante selon l'OS et la capacité du processeur.

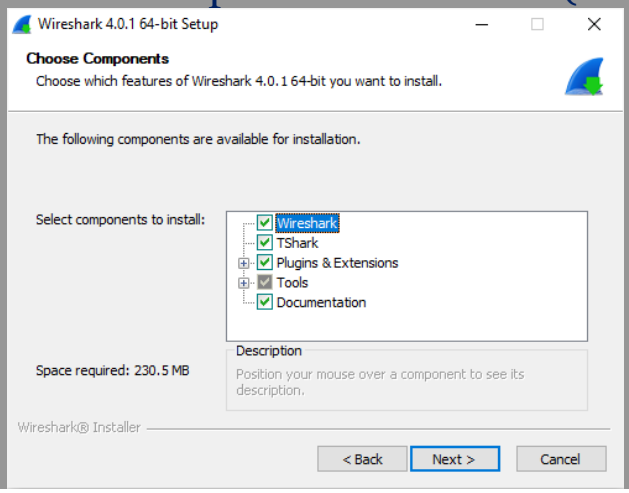
Lancer l'installation.



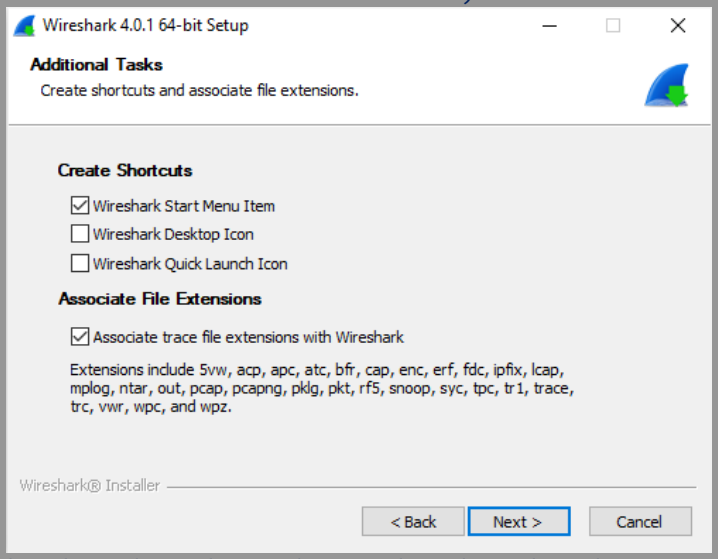
Accepter la licence.



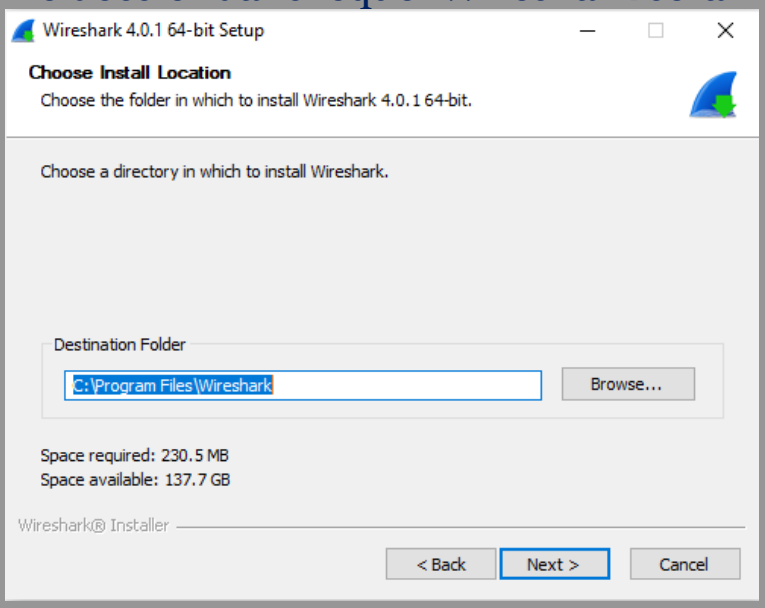
Il faut sélectionner les composants à installer (laisser par défaut).



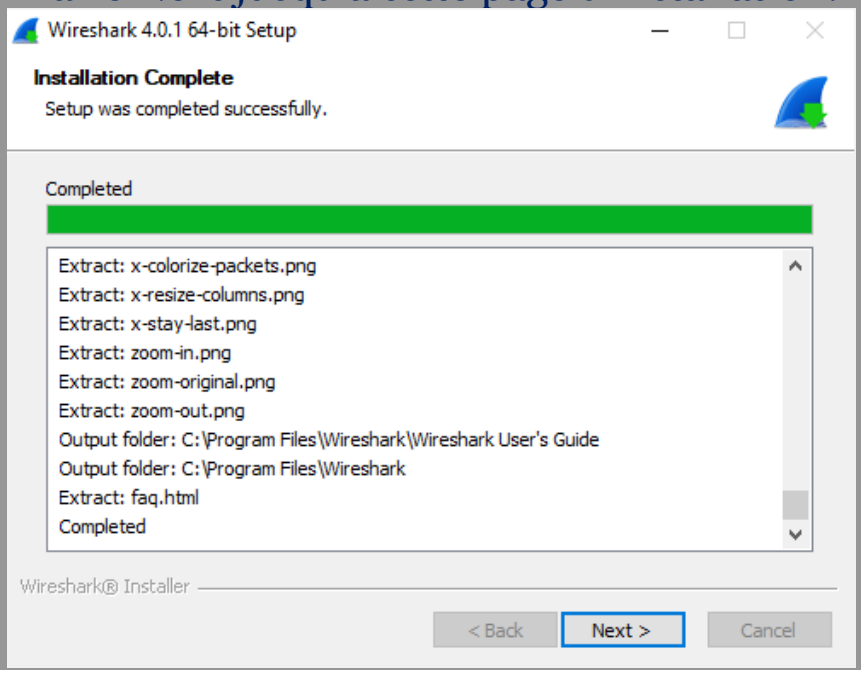
Préciser s'il faut que des tâches supplémentaires soient réalisées (créer une icône sur le menu, sur le bureau…).



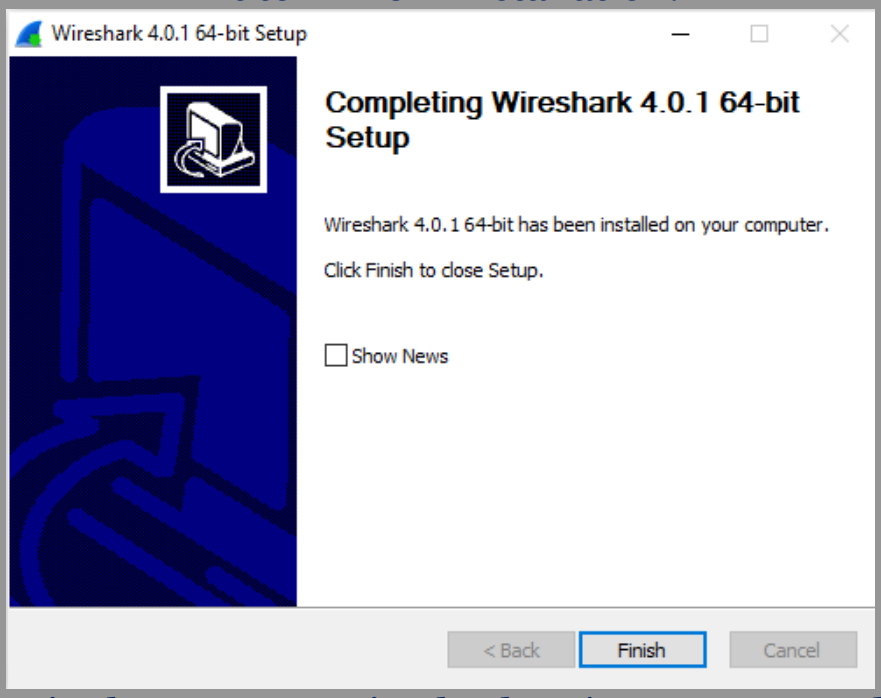
Choisir le dossier dans lequel Wireshark sera installé.



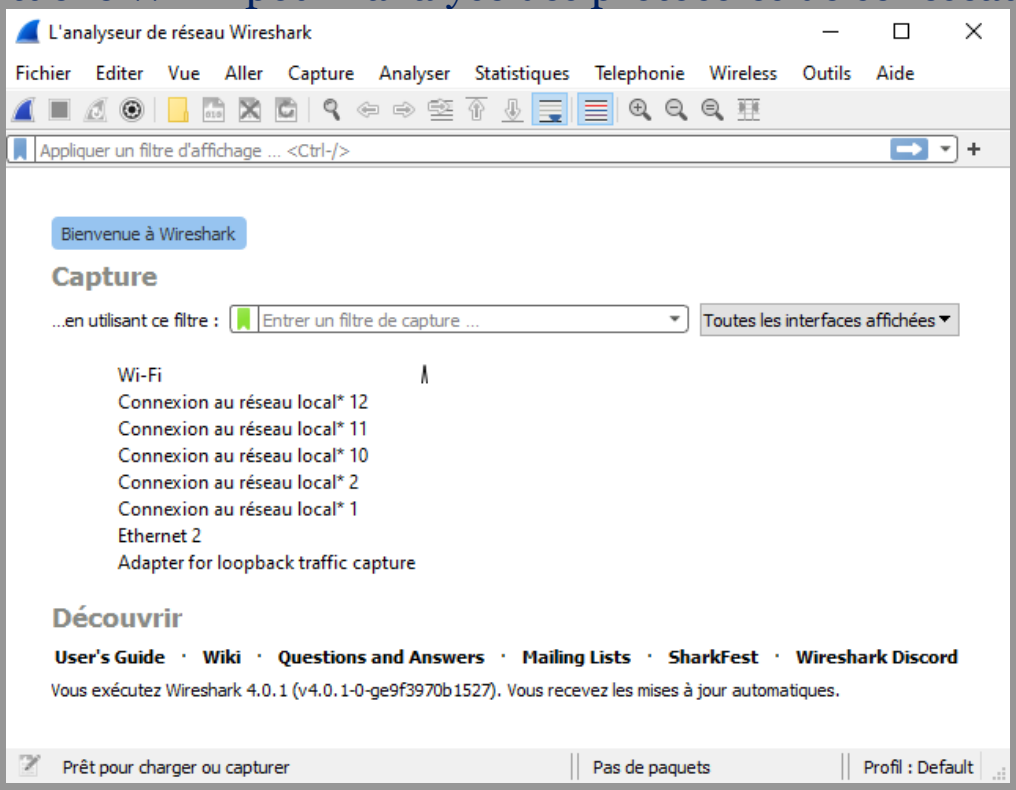
Faire Next jusqu'à cette page d'installation.



Et terminer l'installation.



Pour le premier lancement, Wireshark présente un scan des réseaux disponible pour une analyse. Il faudra sélectionner l'interface virtuelle Wi-Fi pour l'analyse des protocoles de ce réseaux.



Fonctionnalités