



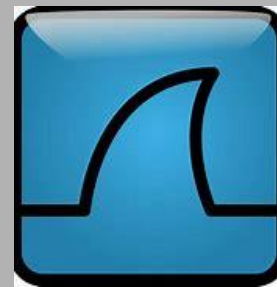
Document d'exploitation

*BUON Jérémy
BTS SIO SISR*

Table des matières

- **Définition**
- **Installation**
- **Fonctionnement**
- **Fonctionnalités**

○ 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.

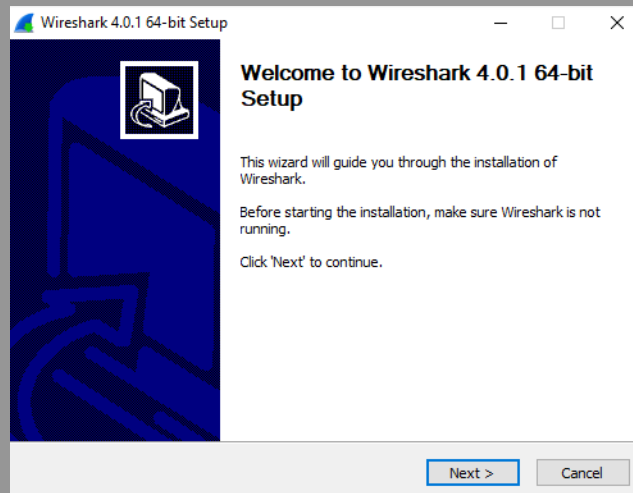
Wireshark dispose d'un riche ensemble de fonctionnalités :

- 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.

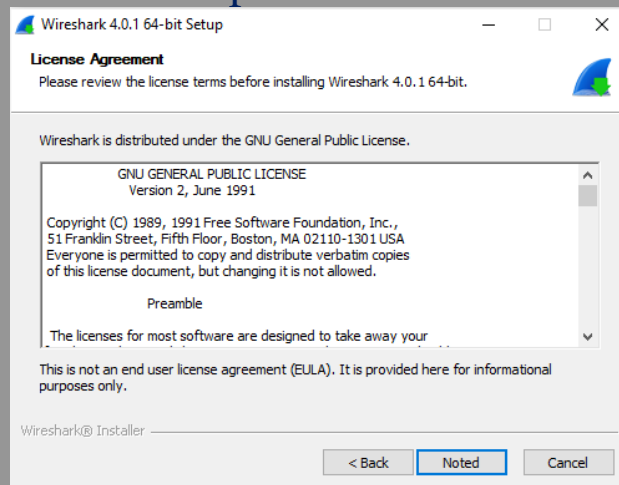
○ Installation

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.

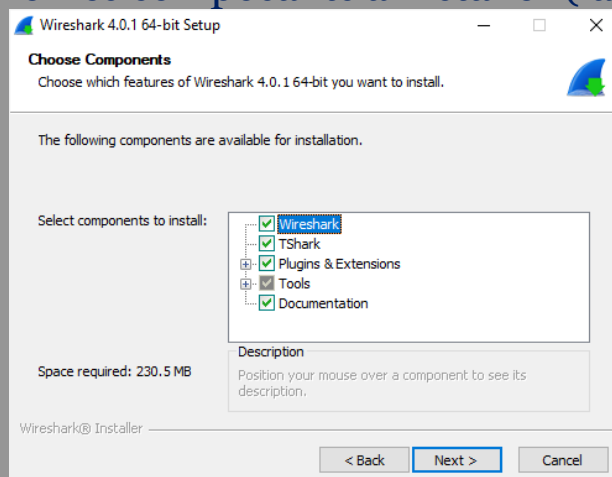
Lancer l'installation.



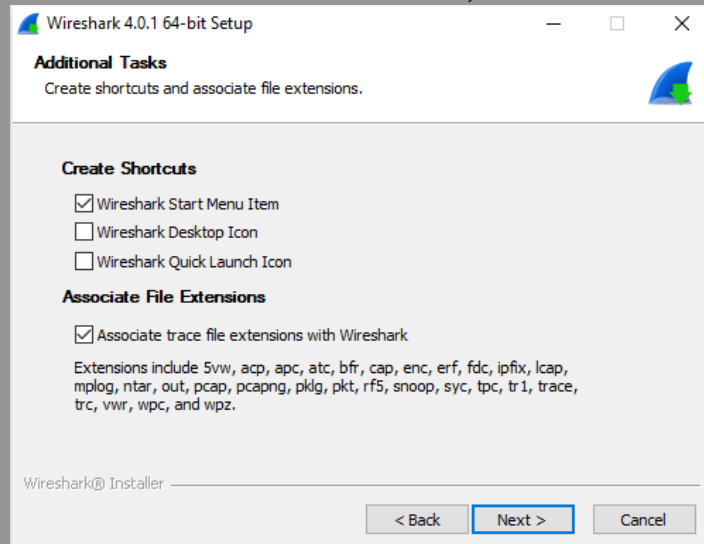
Accepter la licence.



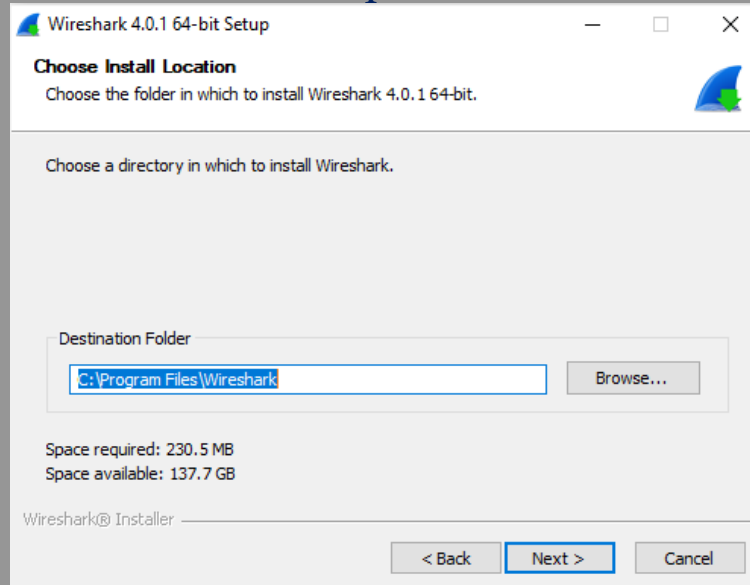
Il faut sélectionner les composants à installer (laisser par défaut).



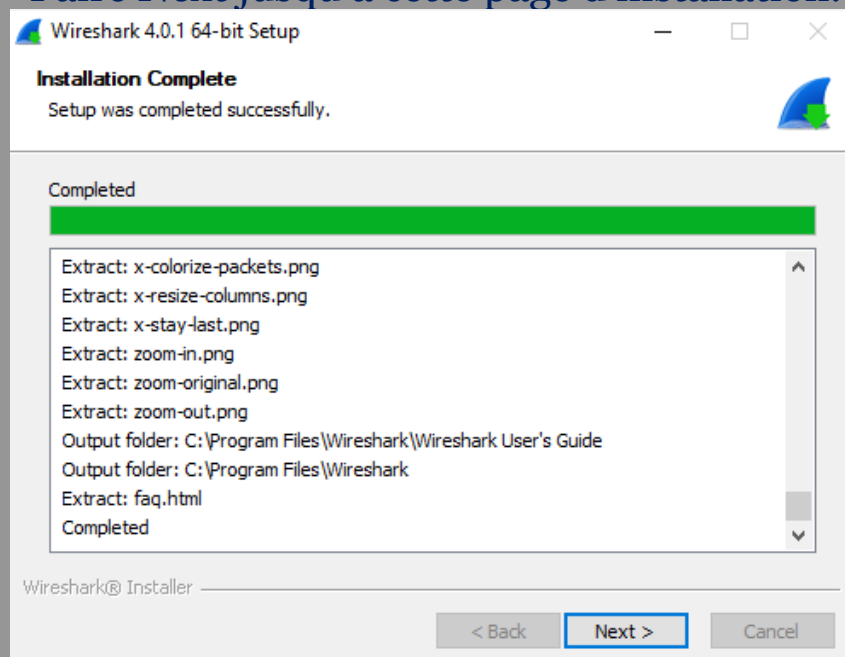
Préciser s'il faut que des tâches supplémentaires soient réalisées (créer une icône sur le menu, sur le bureau...).



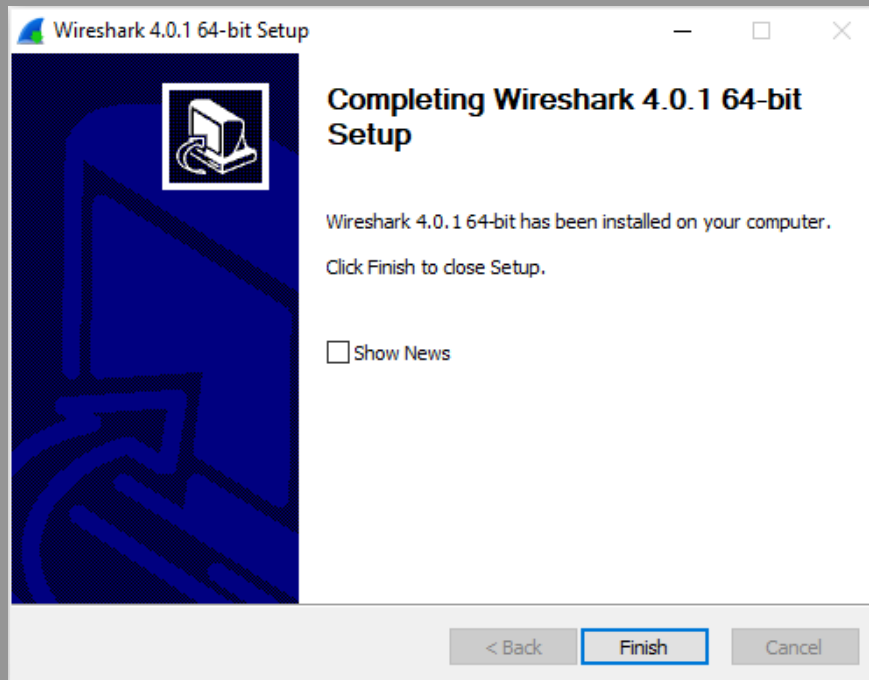
Choisir le dossier dans lequel Wireshark sera installé.



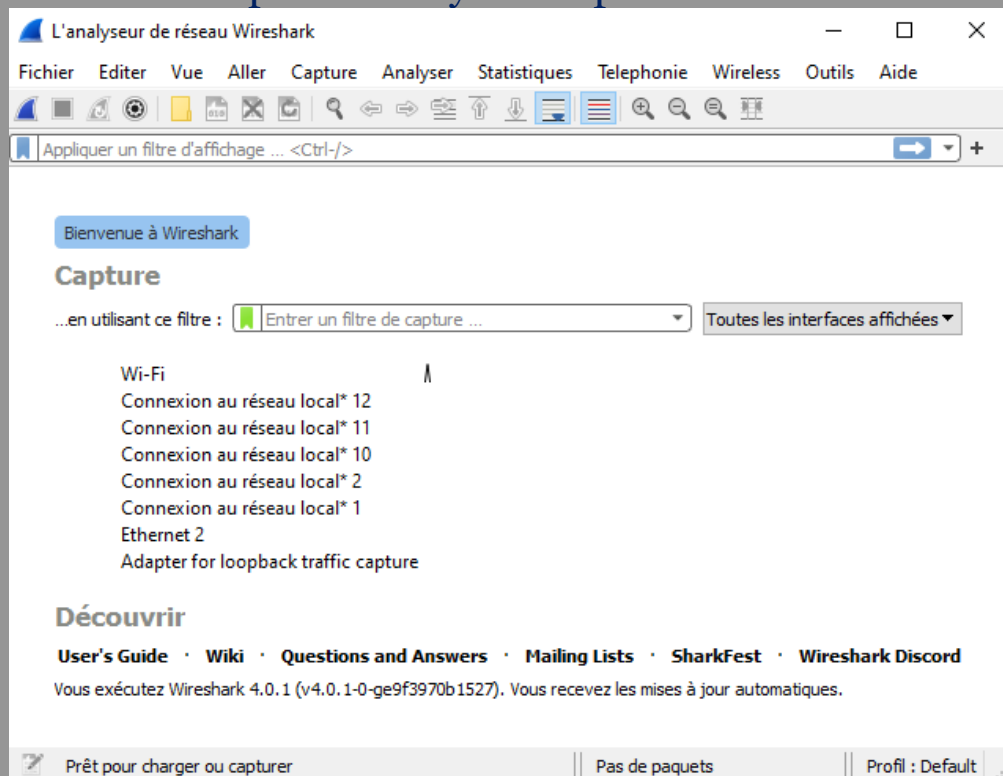
Faire Next jusqu'à cette page d'installation.



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

Capture en cours de Wi-Fi

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

Appliquer un filtre d'affichage ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
779	19.447497	95.101.143.137	172.18.104.44	TCP	56	443 → 520
780	19.447574	172.18.104.44	95.101.143.137	TCP	54	52002 → 4
781	19.449069	20.234.93.27	172.18.104.44	TCP	56	443 → 520
782	19.449262	95.101.143.137	172.18.104.44	TLSv1.3	78	Applicati
783	19.449324	172.18.104.44	95.101.143.137	TCP	54	52003 → 4
784	19.449511	95.101.143.137	172.18.104.44	TCP	56	443 → 520
785	19.492598	fe80::769d:4c9f:451...	ff02::c	UDP	718	63834 → 3
786	20.780856	172.18.104.44	20.199.120.182	TLSv1.2	98	Applicati
787	20.792104	20.199.120.182	172.18.104.44	TLSv1.2	229	Applicati
788	20.844136	172.18.104.44	20.199.120.182	TCP	54	65328 → 4

< >

> Frame 1: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface 0
 > Ethernet II, Src: LiteonTe_0e:12:a5 (3c:91:80:0e:12:a5), Dst: 3c:91:80:0e:12:a5
 > Internet Protocol Version 4, Src: 172.18.104.44, Dst: 239.255.255.255
 > User Datagram Protocol, Src Port: 52365, Dst Port: 1900
 > Simple Service Discovery Protocol

0000 01 00 5e 7f ff ff 3c 91 80 0e 12 a5 3c 91 80 0e 12 a5
 0010 00 cb dd 6a 00 00 00 00 00 00 00 00 00 00 00 00
 0020 ff fa cc 8d 07 60 00 00 00 00 00 00 00 00 00 00
 0030 43 48 20 2a 20 48 00 00 00 00 00 00 00 00 00
 0040 4f 53 54 3a 20 3e 00 00 00 00 00 00 00 00 00
 0050 2e 32 35 30 3a 30 00 00 00 00 00 00 00 00 00
 0060 22 73 73 64 70 3a 00 00 00 00 00 00 00 00 00
 0070 0a 4d 58 3a 20 3e 00 00 00 00 00 00 00 00 00

< >

Wi-Fi: <live capture in progress> | Paquets : 788 · Affichés : 788 (100.0%) | Profil : Default