

INSTALLATION DE WIRESHARK



Sniffing Problems a Mile Away

Document d'exploitation

Table des matières

- 1. Définition**
- 2. Prérequis**
- 3. Installation**
- 4. Fonctionnement**
- 5. Fonctionnalités**

1.Définition

Wireshark est un analyseur de paquets libre et gratuit. Il est utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie.

Wireshark utilise la bibliothèque logicielle Qt pour l'implémentation de son interface utilisateur et pcap pour la capture des paquets ; il fonctionne sur de nombreux environnements compatibles UNIX comme GNU/Linux, FreeBSD, NetBSD, OpenBSD ou Mac OSX, mais également sur Microsoft Windows. Il existe aussi entre autres une version en ligne de commande nommé TShark. Ces programmes sont distribués gratuitement sous la licence GNU General Public License.

Wireshark reconnaît 1 515 protocoles.

2. Prérequis

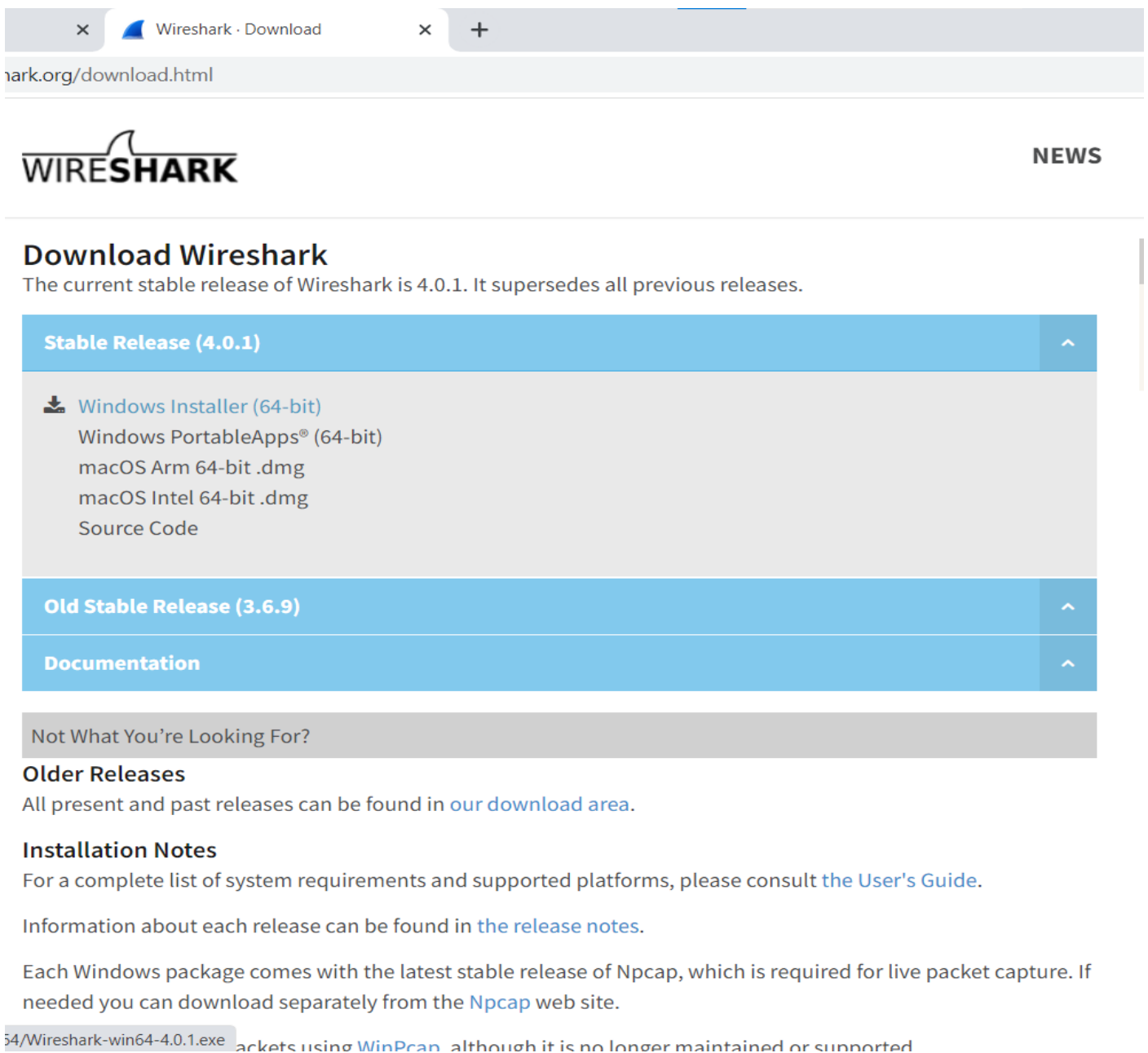
Pour utiliser Wireshark, il vous faut :

- Un ordinateur.
- Une connexion a internet (Ethernet/Wifi).

3. Installation

Allez sur le site

<https://www.wireshark.org/download.html> et télécharger la version adapté à votre système d'exploitation.



The screenshot shows a web browser window with the address bar displaying 'Wireshark · Download' and the URL 'https://www.wireshark.org/download.html'. The page features the Wireshark logo and a 'NEWS' link. The main heading is 'Download Wireshark', followed by the text 'The current stable release of Wireshark is 4.0.1. It supersedes all previous releases.' Below this, there are three expandable sections: 'Stable Release (4.0.1)', 'Old Stable Release (3.6.9)', and 'Documentation'. The 'Stable Release (4.0.1)' section is expanded, showing a list of download links: 'Windows Installer (64-bit)', 'Windows PortableApps® (64-bit)', 'macOS Arm 64-bit .dmg', 'macOS Intel 64-bit .dmg', and 'Source Code'. Below these sections is a 'Not What You're Looking For?' section with links to 'Older Releases', 'Installation Notes', and 'the release notes'. At the bottom, there is a note about Windows packages including Npcap and a link to 'WinPcap'.

Wireshark · Download

ark.org/download.html

WIRESHARK

NEWS

Download Wireshark

The current stable release of Wireshark is 4.0.1. It supersedes all previous releases.

Stable Release (4.0.1)

- Windows Installer (64-bit)
- Windows PortableApps® (64-bit)
- macOS Arm 64-bit .dmg
- macOS Intel 64-bit .dmg
- Source Code

Old Stable Release (3.6.9)

Documentation

Not What You're Looking For?

Older Releases

All present and past releases can be found in [our download area](#).

Installation Notes

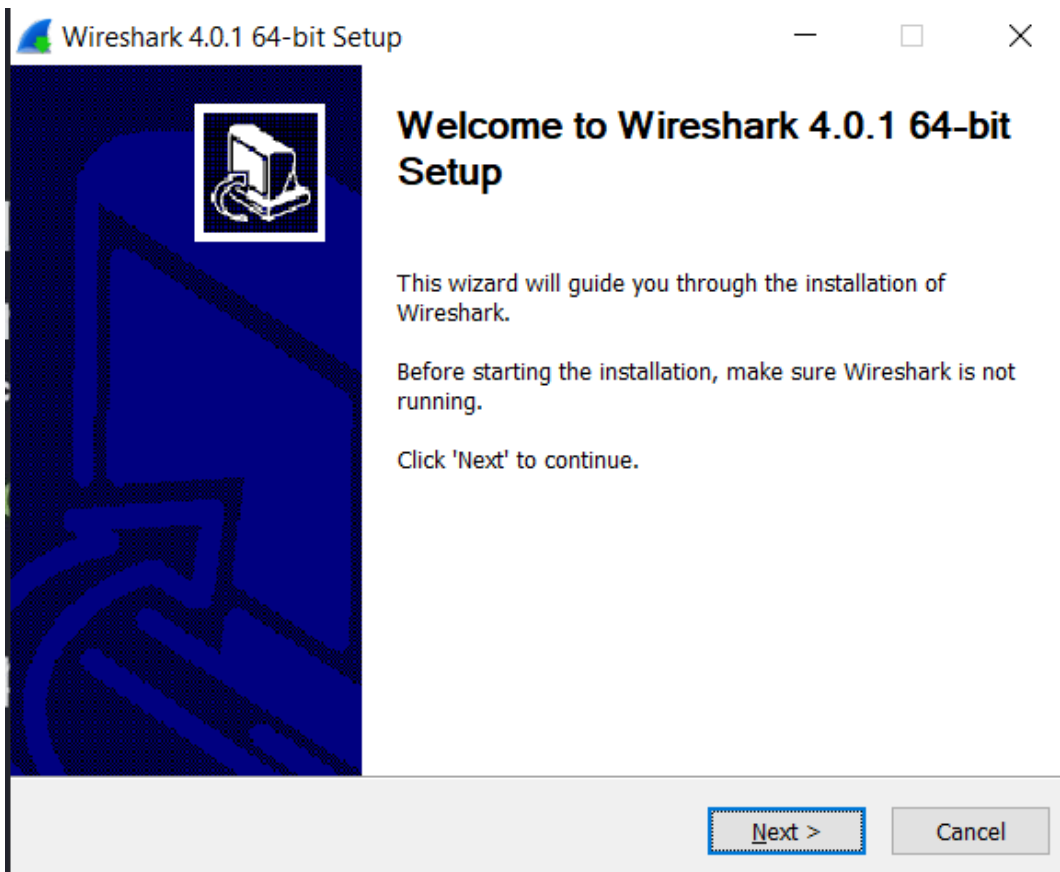
For a complete list of system requirements and supported platforms, please consult [the User's Guide](#).

Information about each release can be found in [the release notes](#).

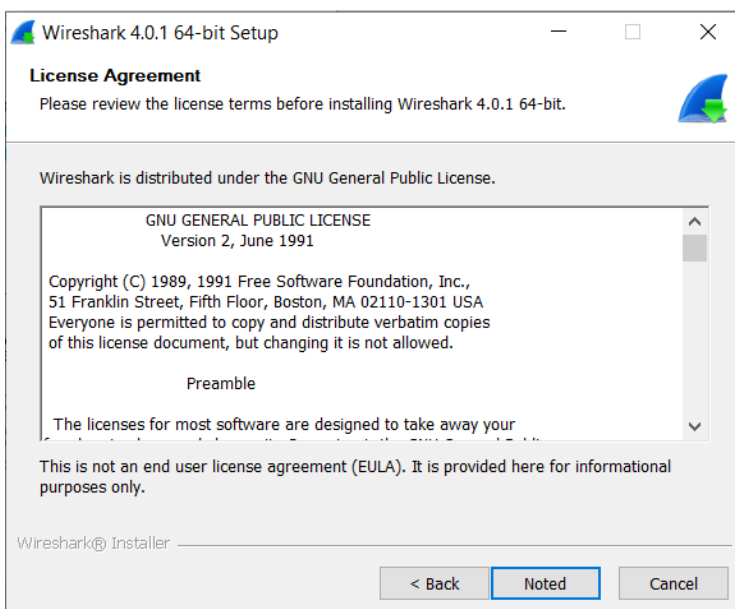
Each Windows package comes with the latest stable release of Npcap, which is required for live packet capture. If needed you can download separately from the [Npcap](#) web site.

54/Wireshark-win64-4.0.1.exe [packets using WinPcap](#) although it is no longer maintained or supported

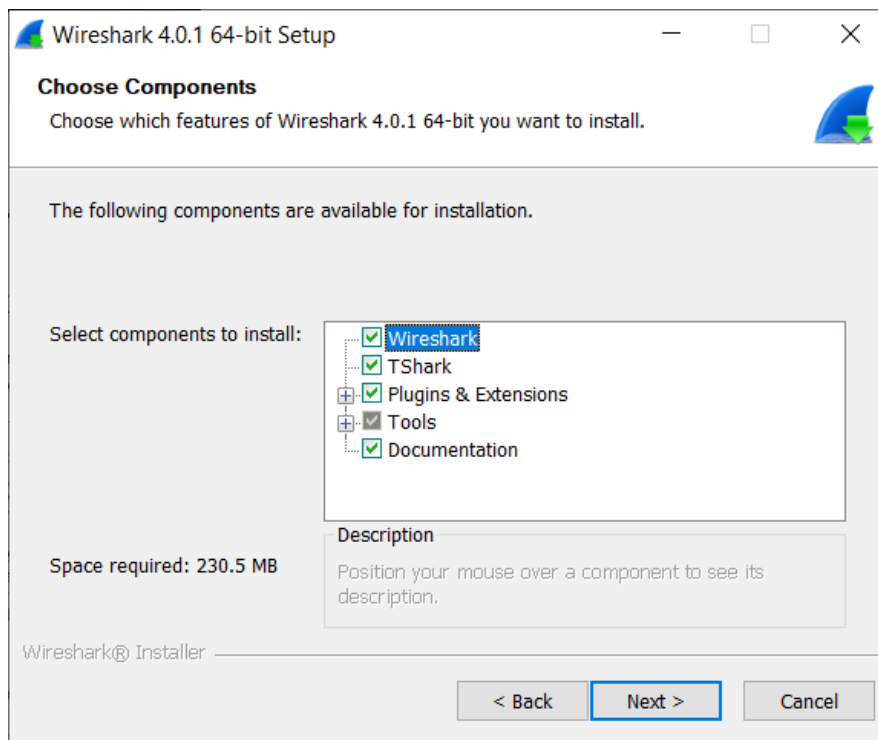
Cliquer sur Next



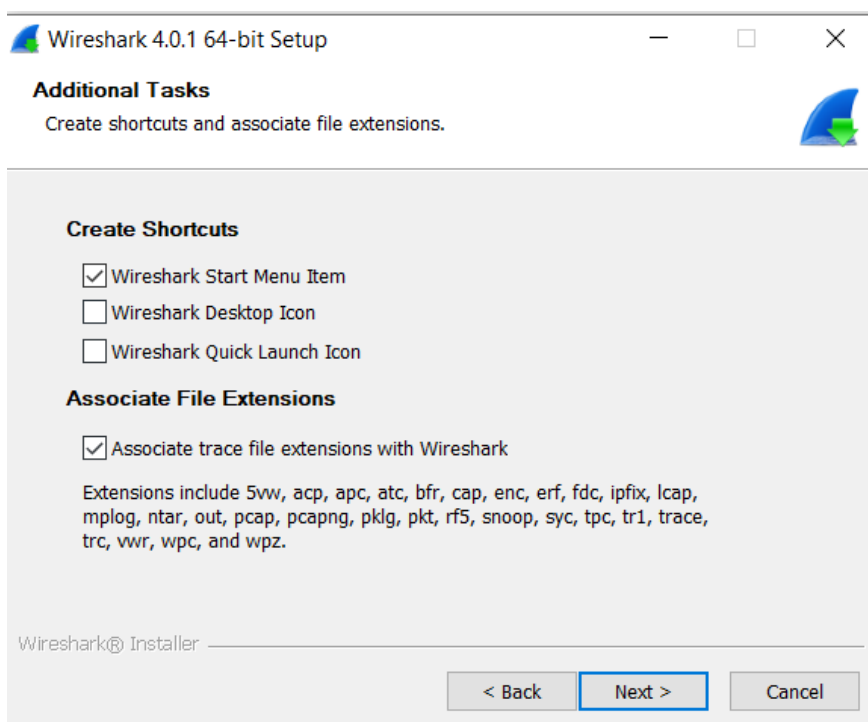
Puis noted .



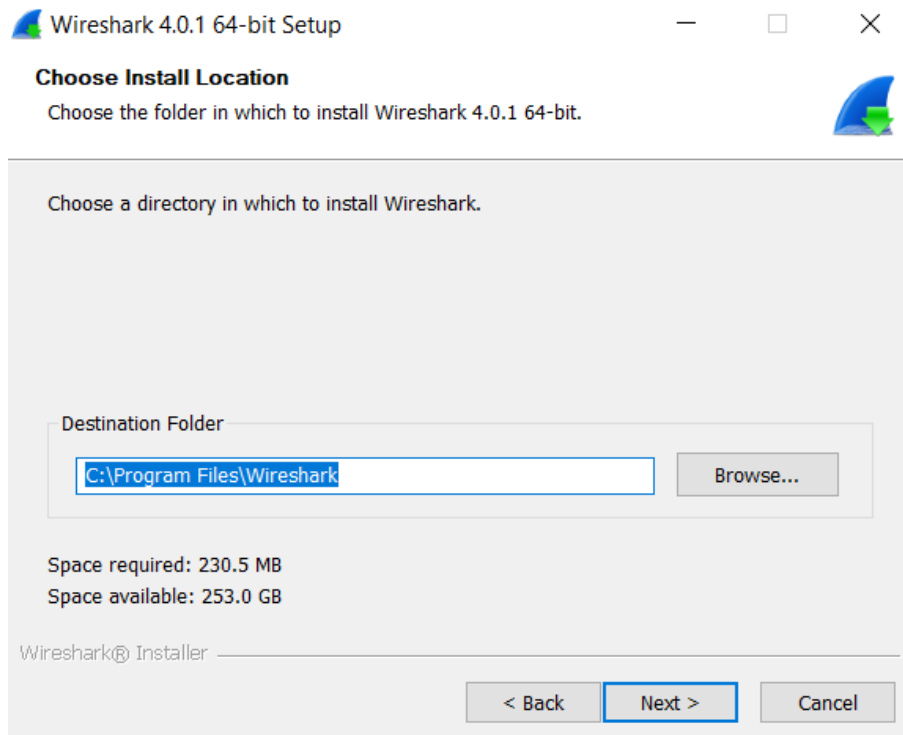
Next.



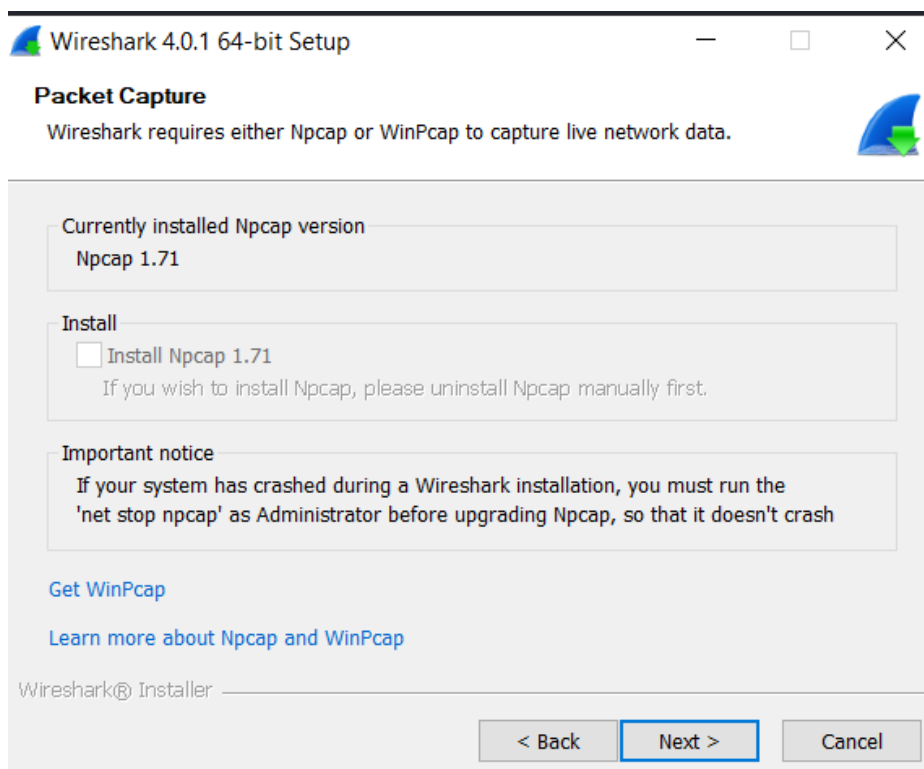
Encore Next.



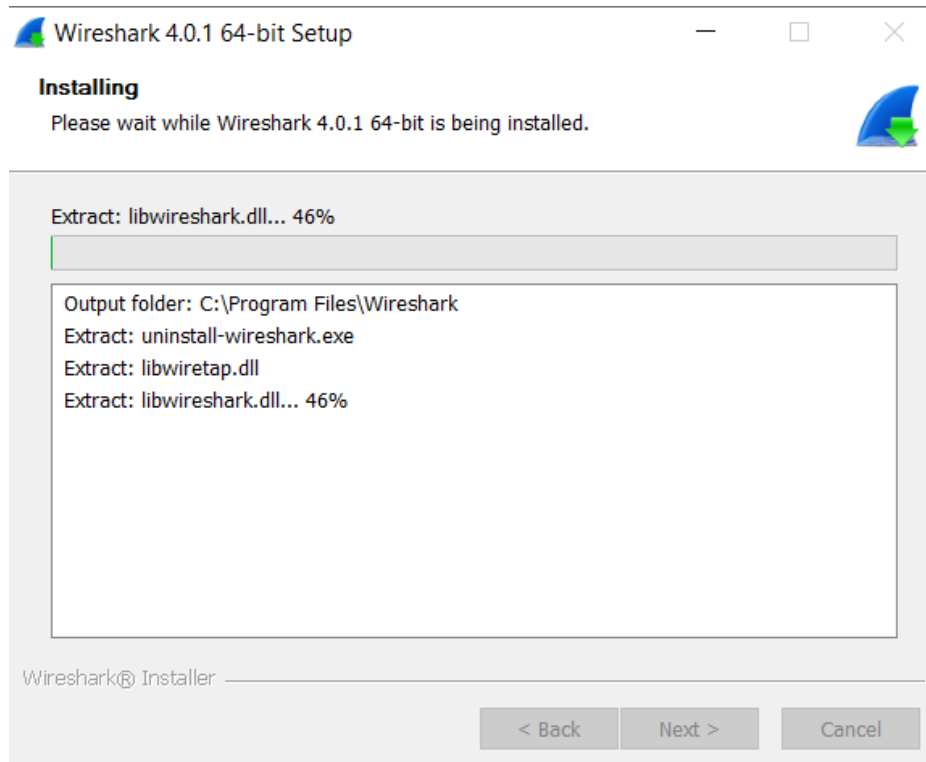
Next.



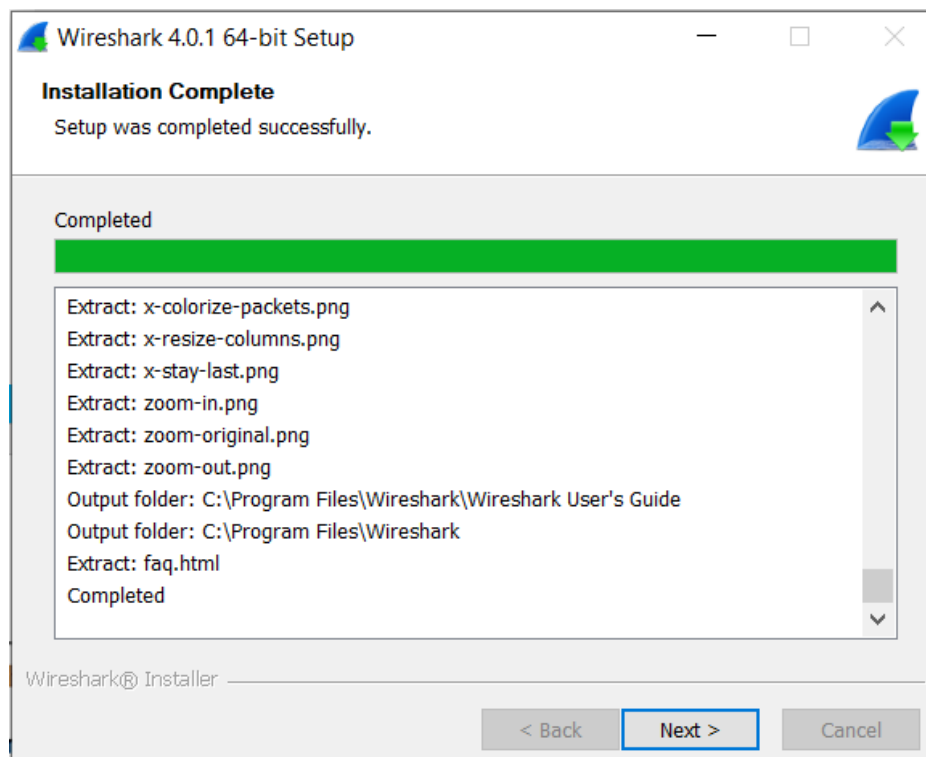
Next.



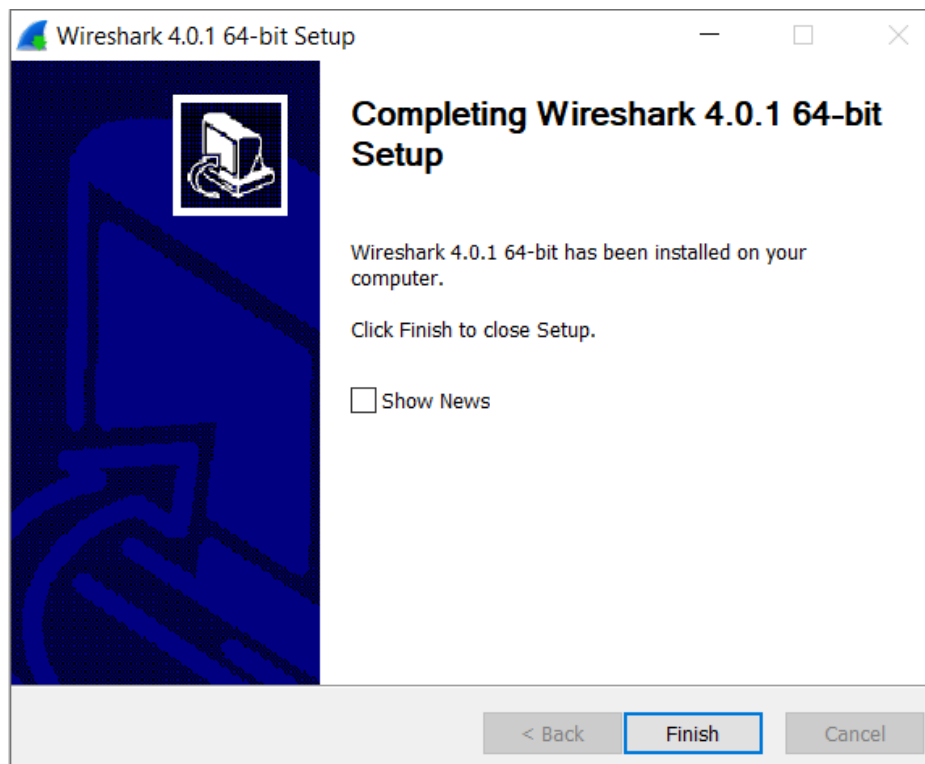
Attendez la fin du chargement.



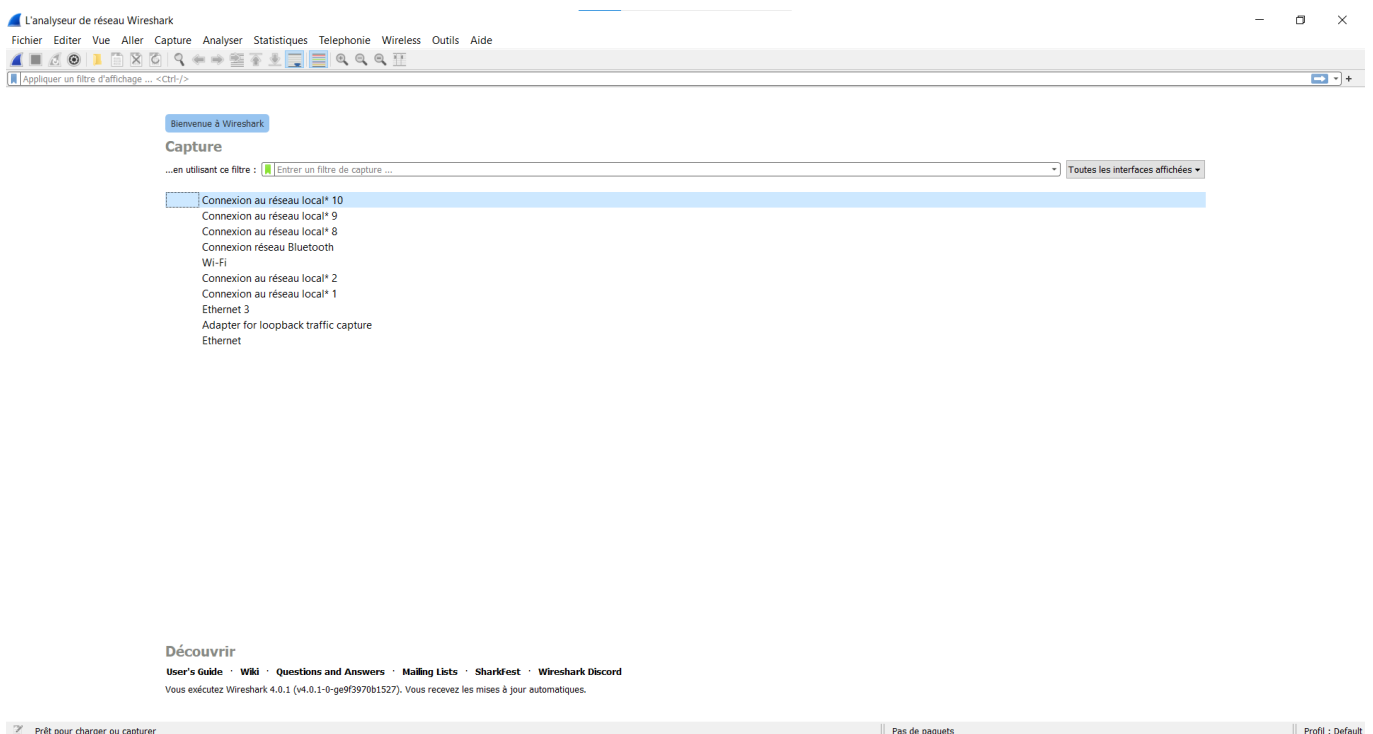
Next.

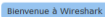


Et enfin Finish.



Vous pouvez maintenant utiliser Wireshark





Adresses: 169.254.59.233,
fe80::22cc:56e1:b0cf:d413
Pas de filtre de capture



0000	00 e0 ed f0 5a 49 80 b2	f9 5d 63 37 08 00 45 0421+[]c7-E-
0010	00 62 c5 2f 40 00 80 06	a9 0c 0a 04 21 34 72	..b/@-[]-[]-
0020	4c ed ca 33 01 bb 66 0a	35 05 be dd 52 83 50 18	L-3--f-5--R-P-
0030	02 05 f2 af 00 00 17 03	03 00 35 00 00 00 005--
0040	00 00 94 ca 46 6d b4 c8	b8 03 86 ea 94 be 42 0bFm-[]-Bk
0050	07 a3 ac 80 83 89 fe d0	05 0d 19 3d 46 b9 42 824F-B-
0060	6a e2 9d a0 90 39 5f 55	5b 94 9d 42 88 ad 71 51	j--9_U[]--Q-

0000	01 00 5e 7f ff fa 04 ea	56 33 2d db 08 00 45 00	...^..... V3---E.
0010	00 ff ba 88 b5 00 00 01 11	36 0c 0a 0a 00 1d ef ff 6-].....
0020	00 cb fa c5 bd 07 6c 00 b7	b7 35 4d 2d 53 45 41 521.....5M-SEAR
0030	43 48 20 2a 20 48 54 54	50 2f 31 2e 31 0d 0a 48	CH * HTTP/1.1- H
0040	4f 53 54 3a 20 32 33 39	2e 32 35 35 2e 32 35 35	OST: 239.255.255
0050	2e 32 35 30 3a 31 39 30	30 0d 0a 4d 41 4e 3a 20	250:190 0- MAN:
0060	22 73 73 64 70 3a 64 69	73 63 6f 76 65 72 22 0d	"ssdp:discover"
0070	0a 4d 58 3a 20 31 0d 0a	53 54 3a 20 75 72 6e 3a	-MX: 1- ST: urn:
0080	64 69 61 6c 2d 6d 75 6c	74 69 73 62 72 65 65 6e	dial-multiscreen
0090	2d 6f 72 67 3a 73 65 72	76 69 63 63 3a 64 69 61	org:service:dia
00a0	6c 3a 31 0d 0a 55 53 45	52 2d 41 47 45 4e 54 3a	1:-USE R-AGENT:
00b0	20 4d 69 62 72 6f 73 6f	66 74 20 45 64 67 65 2f	Microsoft Edge/
00c0	31 31 30 2e 30 2e 31 35	38 37 2e 34 36 20 57 69	110.0.15 87.46 Wi
00d0	6e 64 6f 77 73 0d 0a 0d	0a	ndows...