

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 analyser 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.

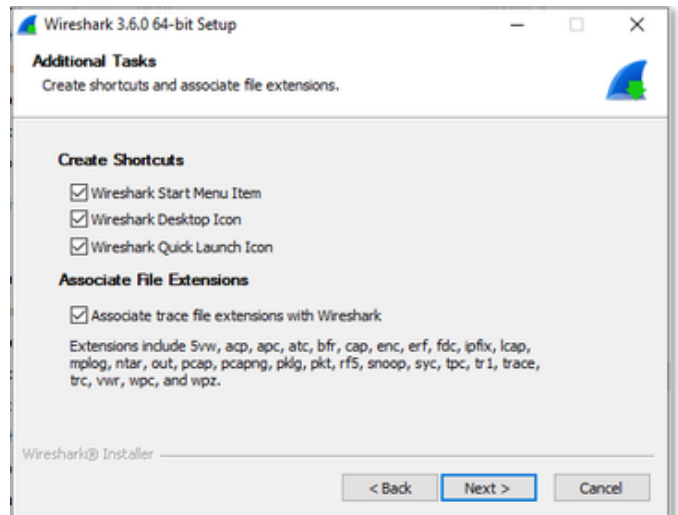
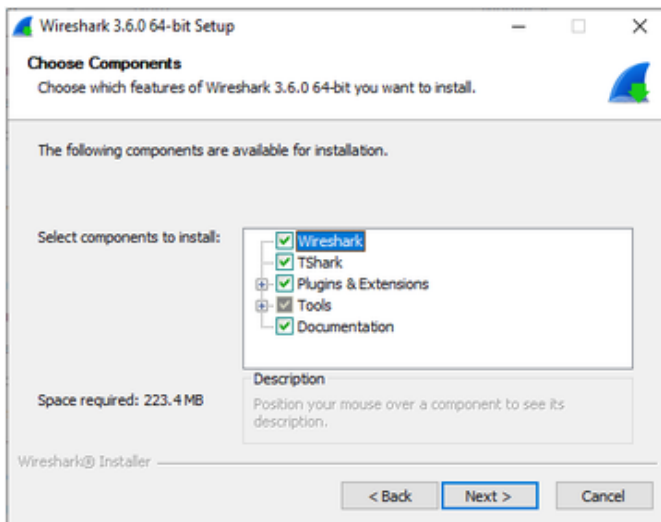
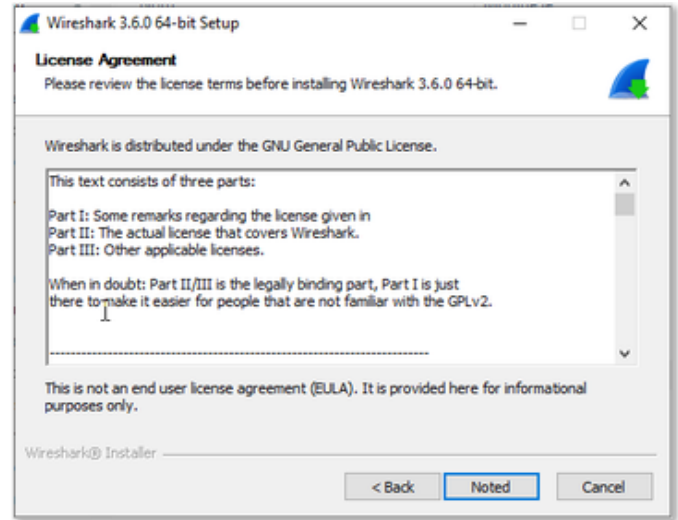
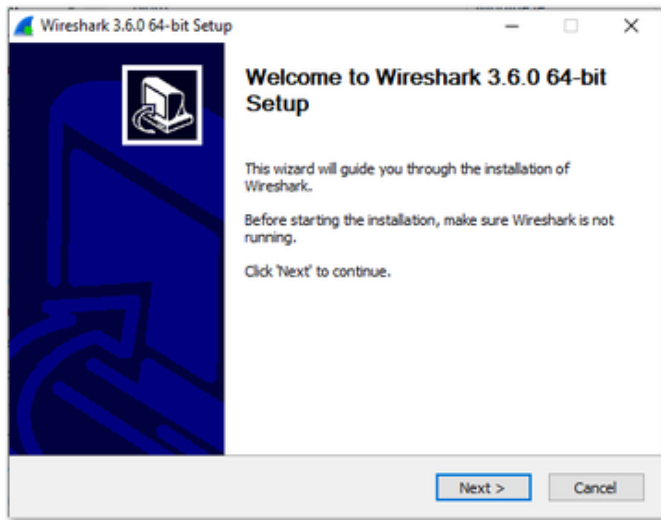
II. Installation

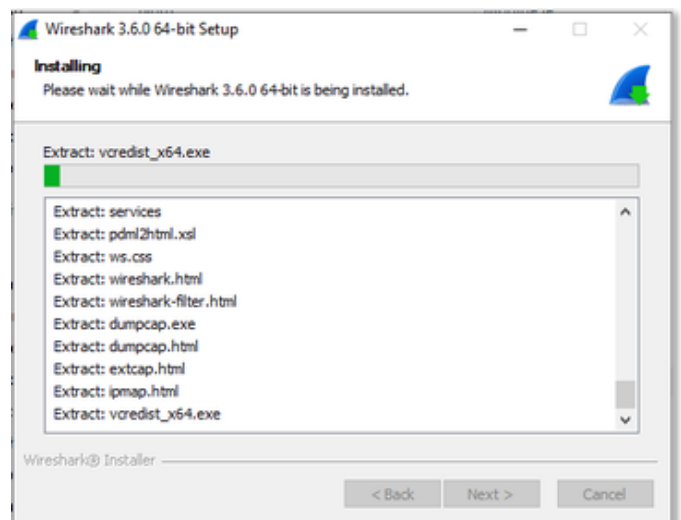
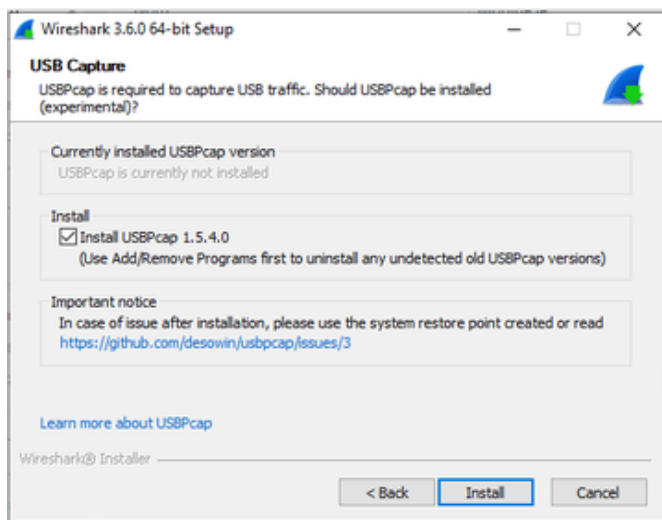
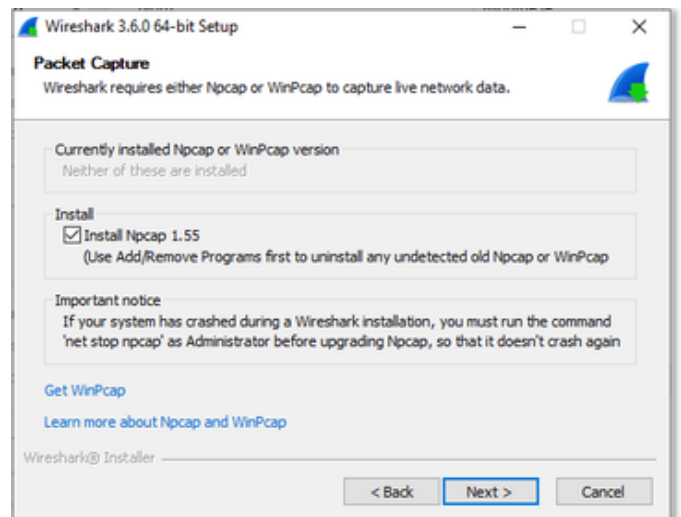
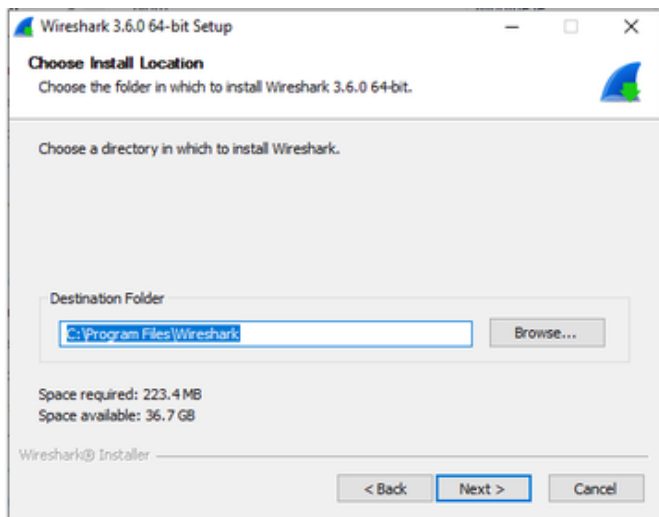
2.1 Lancement de l'installation

Lancer l'installateur.

 Wireshark-win64-3.6.0

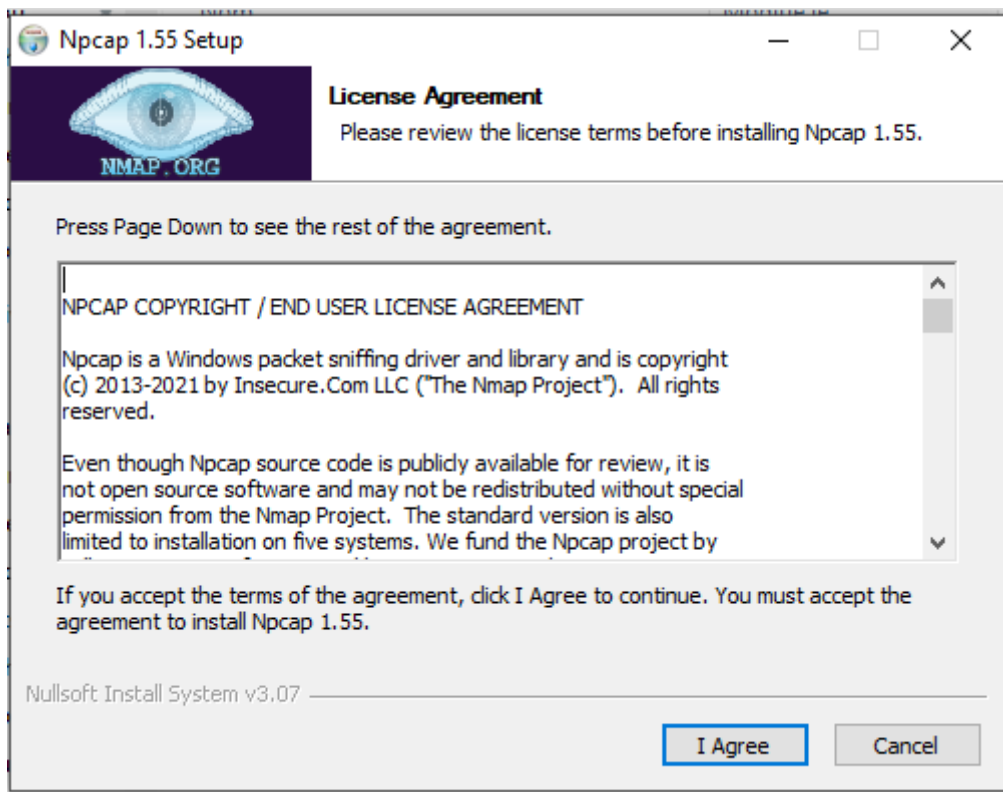
L'installation est basique. Il suffit de suivre l'assistant d'installation.



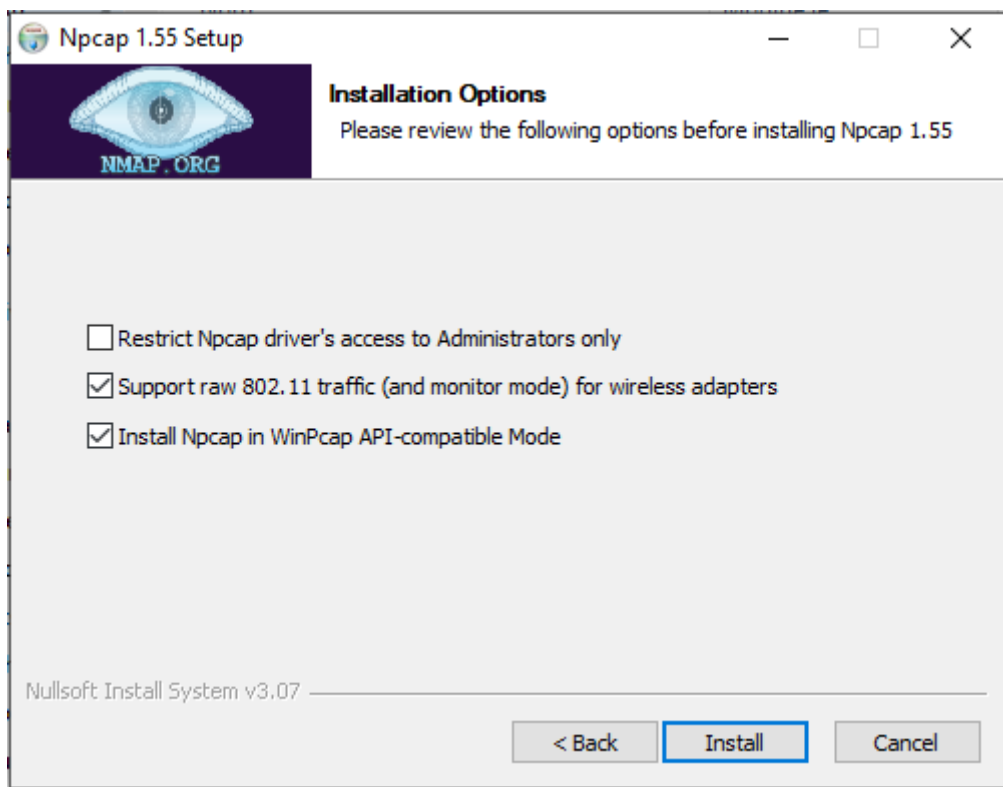


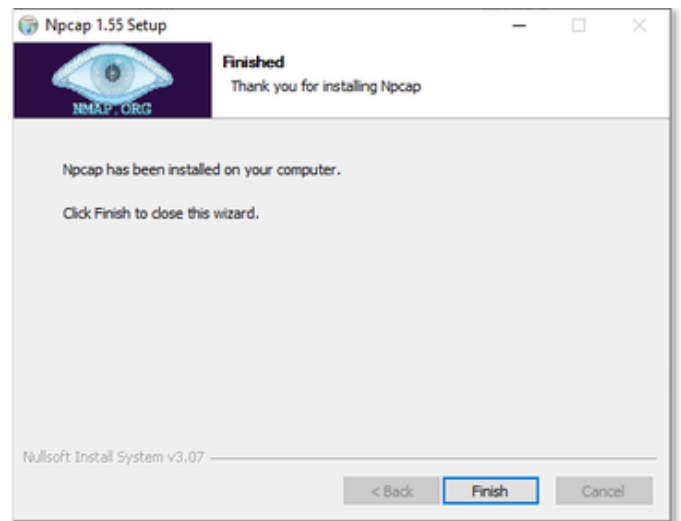
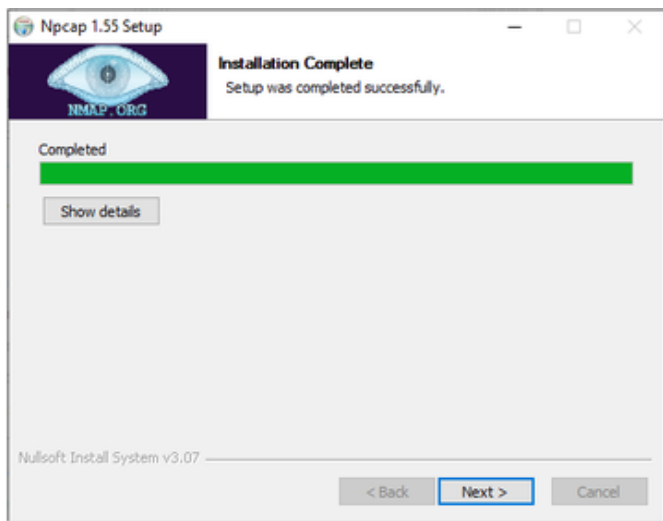
2.2 Installation de Npcap

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



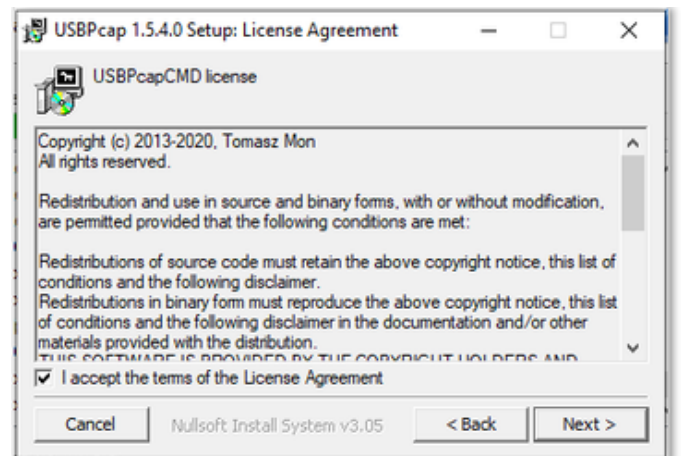
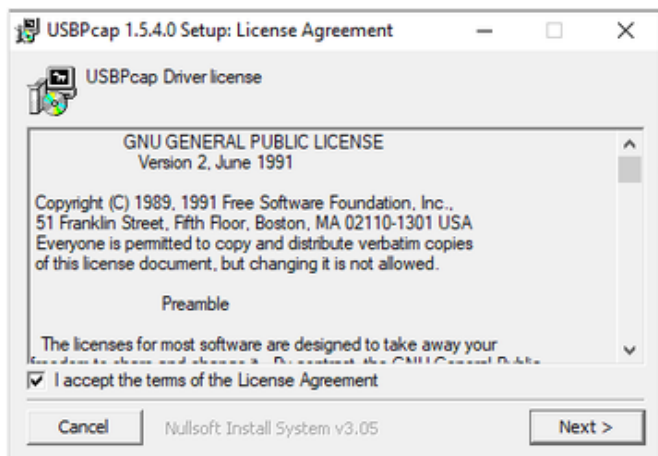
Cocher les cases suivantes :



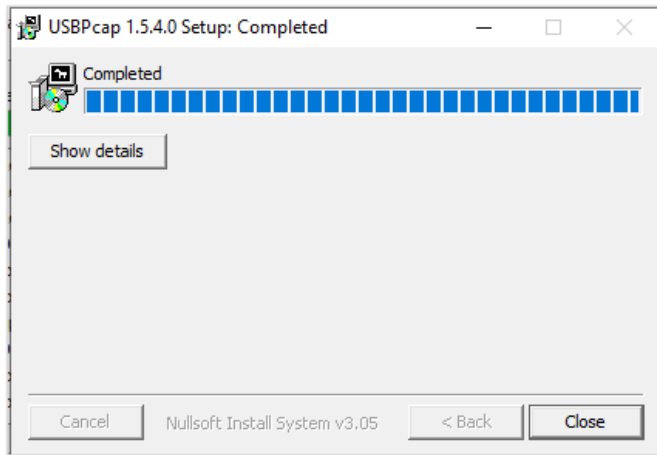
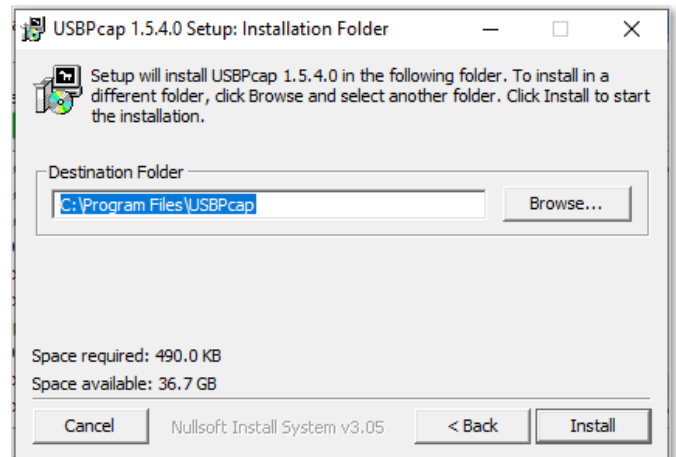
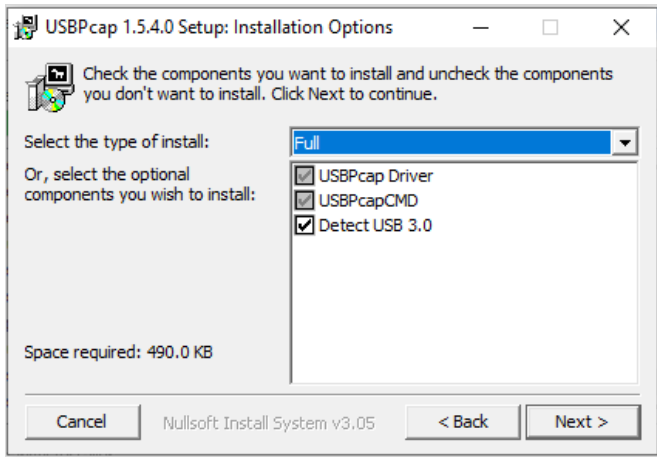


2.3 Installation de USBpcap

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

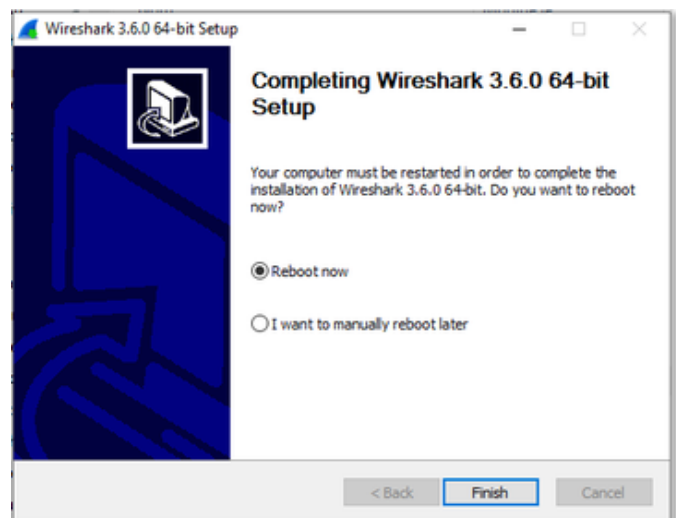
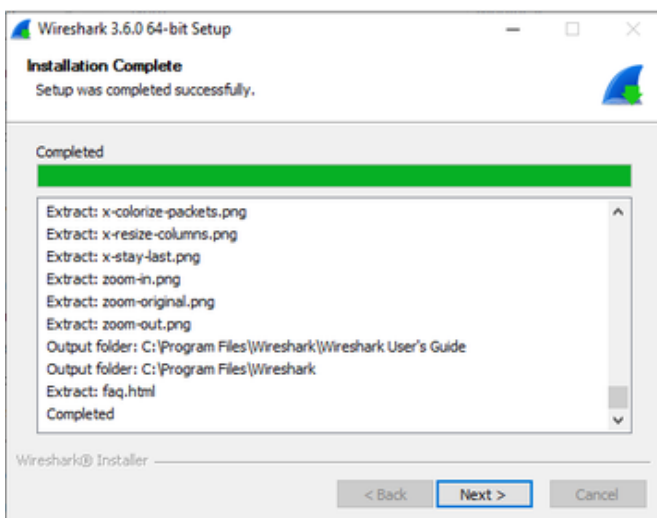


Laisser les cases cochées et terminer l'installation.



2.4 Fin de l'installation

Terminer l'installation.



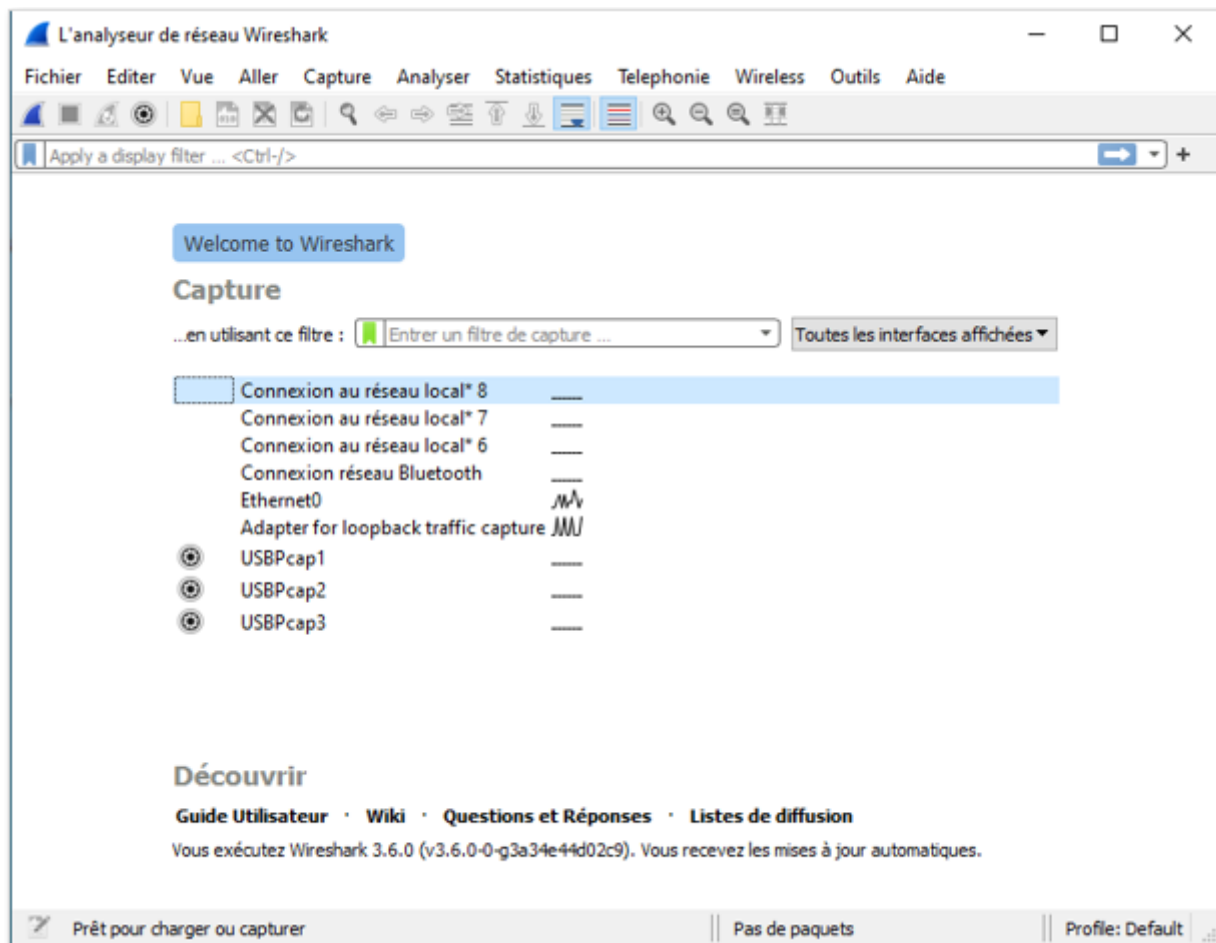
III. Démarrer une capture

Lancer le programme.



Sélectionner l'interface réseau à utiliser.

(ici : Ethernet0)



La capture se lance et les paquet capturés apparaissent.

Capture en cours de Ethernet0

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
14	3.847203	172.20.0.5	172.20.0.1	SMB2	126	Session Logoff Request
15	3.847498	172.20.0.1	172.20.0.5	SMB2	126	Session Logoff Response
16	3.847621	172.20.0.5	172.20.0.1	TCP	54	49675 → 445 [RST, ACK] Seq=145 Ack=145 Win=0 Len=0
17	6.021244	172.20.0.5	172.20.0.1	DNS	91	Standard query 0x1ef5 A settings-win.data.microsoft.com
18	6.021395	VMware_0f:80:43	Broadcast	ARP	42	Who has 172.20.0.2? Tell 172.20.0.5
19	6.503496	VMware_9b:76:ca	Broadcast	ARP	60	Who has 172.20.0.254? Tell 172.20.0.1
20	6.520270	172.20.0.5	172.20.0.1	DNS	90	Standard query 0xcc5a A watson.telemetry.microsoft.com
21	6.629250	VMware_0f:80:43	Broadcast	ARP	42	Who has 172.20.0.2? Tell 172.20.0.5
22	7.224208	VMware_9b:76:ca	Broadcast	ARP	60	Who has 172.20.0.254? Tell 172.20.0.1
23	7.627942	VMware_0f:80:43	Broadcast	ARP	42	Who has 172.20.0.2? Tell 172.20.0.5

> Frame 1: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{7316CA6D-E041-4AD0-97D0-36935CD1ADF9}, id 0
 > Ethernet II, Src: VMware_0f:80:43 (00:0c:29:0f:80:43), Dst: VMware_9b:76:ca (00:0c:29:9b:76:ca)
 > Internet Protocol Version 4, Src: 172.20.0.5, Dst: 172.20.0.1
 > User Datagram Protocol, Src Port: 53358, Dst Port: 53
 > Domain Name System (query)

```

0000  00 0c 29 9b 76 ca 00 0c 29 0f 80 43 08 00 45 00  ..).v... )..C..E.
0010  00 4d 01 83 00 00 80 11 00 00 ac 14 00 05 ac 14  .M.....
0020  00 01 d0 0e 00 35 00 39 58 79 1e f5 01 00 00 01  .n.5.9 Xy.....
0030  00 00 00 00 00 00 0c 73 65 74 74 69 6e 67 73 2d  .....s ettings-
0040  77 69 6e 04 64 61 74 61 09 6d 69 63 72 6f 73 6f  win data microso
0050  66 74 03 63 6f 6d 00 00 01 00 01                ft.com...
  
```

Ethernet0: <live capture in progress> | Explorateur de fichiers | Paquets: 23 · Affichés: 23 (100.0%) | Profile: Default

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.

No.	Time	Source	Destination	Protocol	Length	Info
14	3.847203	172.20.0.5	172.20.0.1	SMB2	126	Session Logoff Request
15	3.847498	172.20.0.1	172.20.0.5	SMB2	126	Session Logoff Response
16	3.847621	172.20.0.5	172.20.0.1	TCP	54	49675 → 445 [RST, ACK] Seq=145 Ack=145 Win=0 Len=0
17	6.021244	172.20.0.5	172.20.0.1	DNS	91	Standard query 0x1ef5 A settings-win.data.microsoft.com
18	6.021395	VMware_0f:80:43	Broadcast	ARP	42	Who has 172.20.0.2? Tell 172.20.0.5
19	6.503496	VMware_9b:76:ca	Broadcast	ARP	60	Who has 172.20.0.254? Tell 172.20.0.1
20	6.520270	172.20.0.5	172.20.0.1	DNS	90	Standard query 0xcc5a A watson.telemetry.microsoft.com
21	6.629250	VMware_0f:80:43	Broadcast	ARP	42	Who has 172.20.0.2? Tell 172.20.0.5
22	7.224208	VMware_9b:76:ca	Broadcast	ARP	60	Who has 172.20.0.254? Tell 172.20.0.1
23	7.627942	VMware_0f:80:43	Broadcast	ARP	42	Who has 172.20.0.2? Tell 172.20.0.5

2. Contenu de la trame découpée par blocs.

```
> Frame 1: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{7316CA6D-E041-4AD0-97D0-36935CD1ADF9}, id 0
> Ethernet II, Src: VMware_0f:80:43 (00:0c:29:0f:80:43), Dst: VMware_9b:76:ca (00:0c:29:9b:76:ca)
> Internet Protocol Version 4, Src: 172.20.0.5, Dst: 172.20.0.1
> User Datagram Protocol, Src Port: 53358, Dst Port: 53
> Domain Name System (query)
```

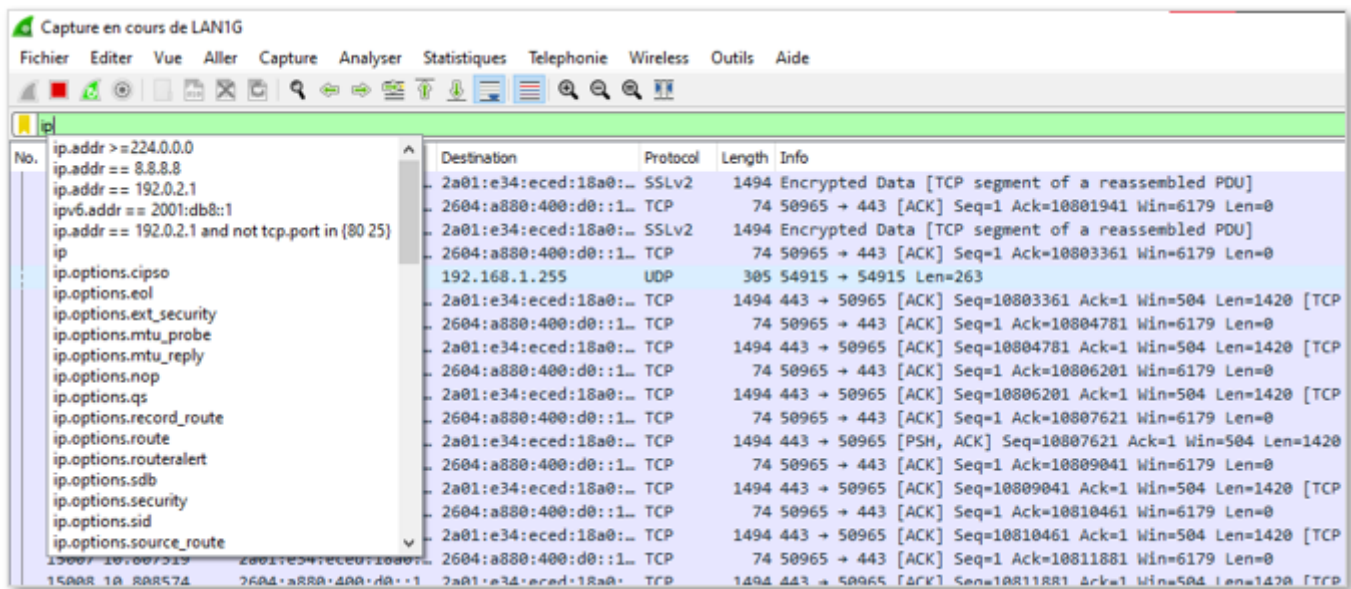
3. Contenu du paquet affiché en hexadécimal et texte.

```
0000  00 0c 29 9b 76 ca 00 0c 29 0f 80 43 08 00 45 00  ..).v....).C.E.
0010  00 4d 01 83 00 00 80 11 00 00 ac 14 00 05 ac 14  .M.....
0020  00 01 d0 0e 00 35 00 39 58 79 1e f5 01 00 00 01  ...n.5.9.Xy.....
0030  00 00 00 00 00 00 0c 73 65 74 74 69 6e 67 73 2d  .....settings-
0040  77 69 6e 04 64 61 74 61 09 6d 69 63 72 6f 73 6f  win.data.microso
0050  66 74 03 63 6f 6d 00 00 01 00 01                ft.com...

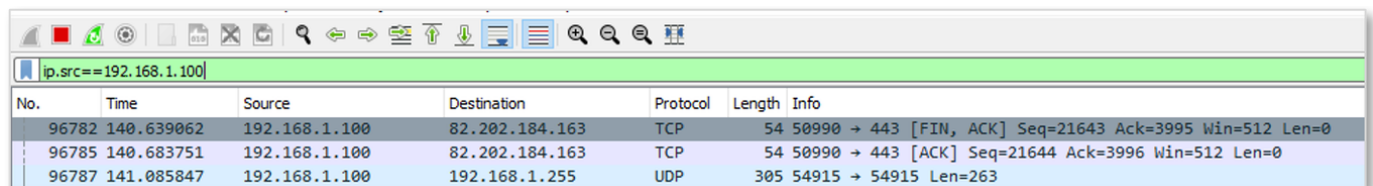
```

IV. Utiliser les filtres

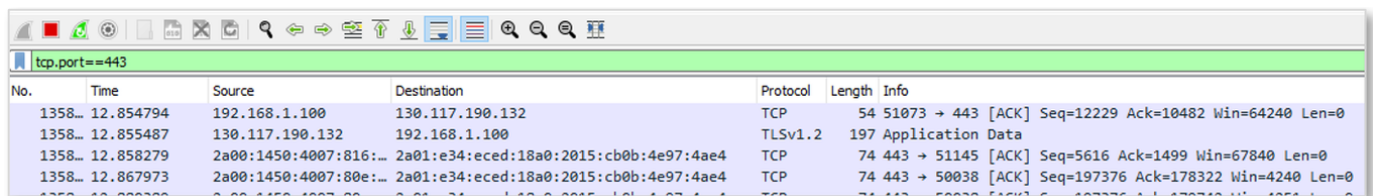
Afin de rendre la capture plus facile et lisible, il est possible de filtrer sur une IP ou un protocole particulier.



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						
No.	Time	Source	Destination	Protocol	Length	Info
2794	2.040748	192.168.1.100	23.72.22.123	TCP	54	49800 → 80 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
3216	2.345422	192.168.1.100	23.72.22.123	TCP	54	[TCP Retransmission] 49800 → 80 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
4075	2.956765	192.168.1.100	23.72.22.123	TCP	54	[TCP Retransmission] 49800 → 80 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
5382	3.896892	192.168.1.100	34.107.221.82	TCP	55	50036 → 80 [ACK] Seq=1 Ack=1 Win=512 Len=1
5746	4.158864	192.168.1.100	23.72.22.123	TCP	54	[TCP Retransmission] 49800 → 80 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
9127	6.570887	192.168.1.100	23.72.22.123	TCP	54	[TCP Retransmission] 49800 → 80 [FIN, ACK] Seq=1 Ack=1 Win=1023 Len=0
10422	7.504532	192.168.1.100	52.95.169.78	TCP	54	50090 → 80 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0

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.

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide						
ip.src==192.168.1.100 ip.dst== 8.8.8.8						
No.	Time	Source	Destination	Protocol	Length	Info
2148...	1108.082445	192.168.1.100	192.168.1.255	UDP	305	54915 → 54915 Len=263
2148...	1109.101710	192.168.1.100	192.168.1.255	UDP	305	54915 → 54915 Len=263
2148...	1110.122031	192.168.1.100	192.168.1.255	UDP	305	54915 → 54915 Len=263
2148...	1111.121557	192.168.1.100	192.168.1.255	UDP	305	54915 → 54915 Len=263
2148...	1112.122877	192.168.1.100	192.168.1.255	UDP	305	54915 → 54915 Len=263
2148...	1112.631286	192.168.1.100	18.184.99.130	TCP	54	51046 → 443 [ACK] Seq=11
2148...	1112.997220	192.168.1.100	20.189.173.4	TCP	66	51247 → 443 [SYN] Seq=0
2148...	1113.096409	192.168.1.100	185.166.143.3	TLSv1.3	176	Application Data
2148...	1113.113304	192.168.1.100	192.168.1.255	UDP	305	54915 → 54915 Len=263

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