

UTILISATION DU LOGICIEL WIRESHARK



1 – PRESENTATION

Le logiciel **Wireshark** (anciennement Ethereal) est un logiciel libre **d'analyse de protocole**, ou « packet sniffer », utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie, mais aussi le piratage. Wireshark reconnaît **759 protocoles**.

Attention : l'installation ou l'utilisation d'une application Analyseur de paquets peut constituer une violation de la politique de sécurité d'une organisation, qui peut entraîner de graves conséquences légales et financières. Il est donc recommandé d'obtenir les autorisations requises avant de télécharger, d'installer ou d'exécuter une application Analyseur de paquets.

Site officiel : <http://www.wireshark.org/>

Documentation : http://www.wireshark.org/docs/wsug_html_chunked/index.html

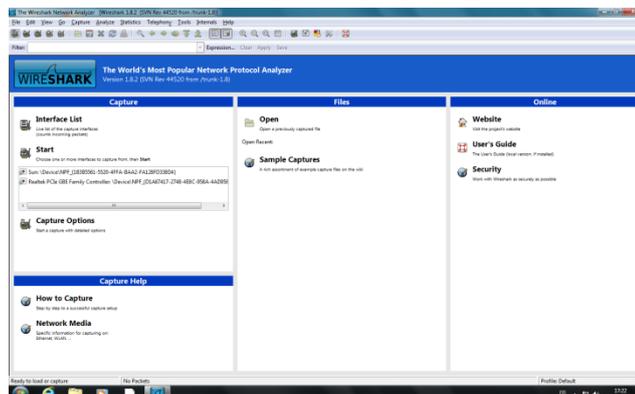
2 – PRISE EN MAIN

Étape 1 : lancement de Wireshark

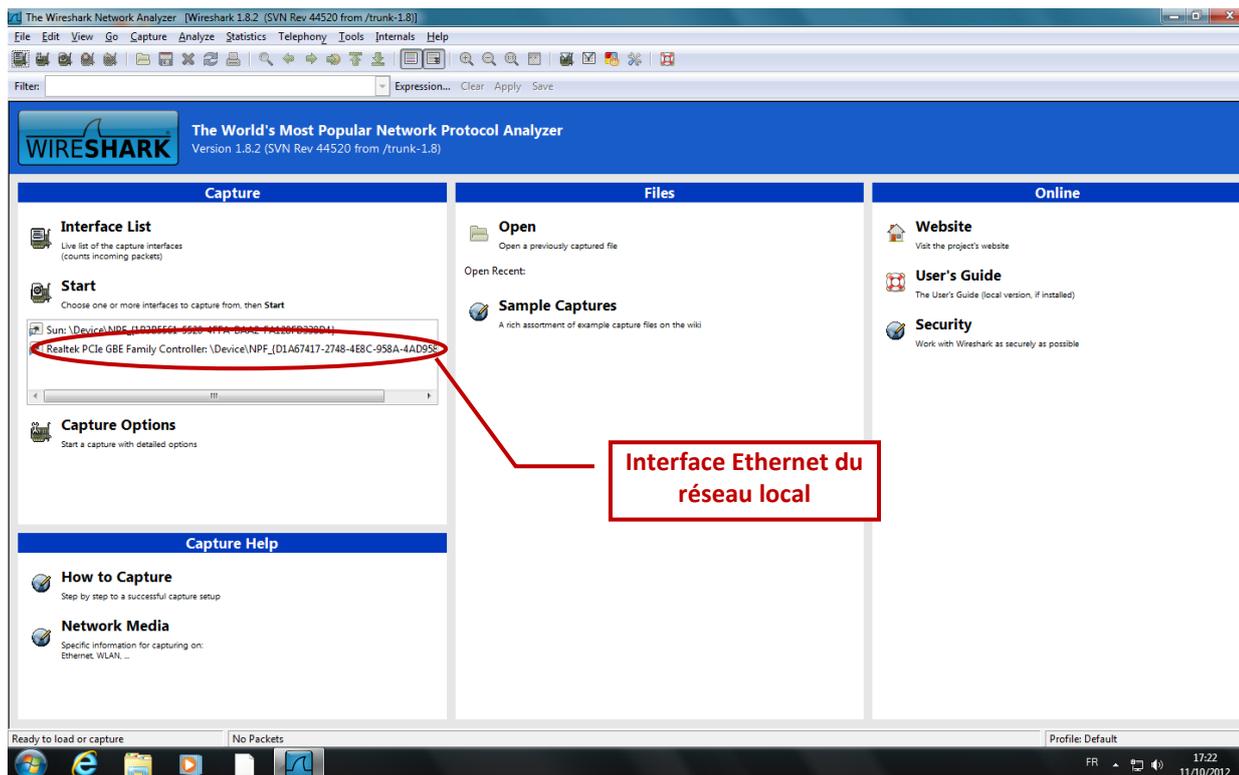
Double-cliquer sur l'icône Wireshark sur le Bureau.



Le logiciel s'ouvre sur cette page de menu :



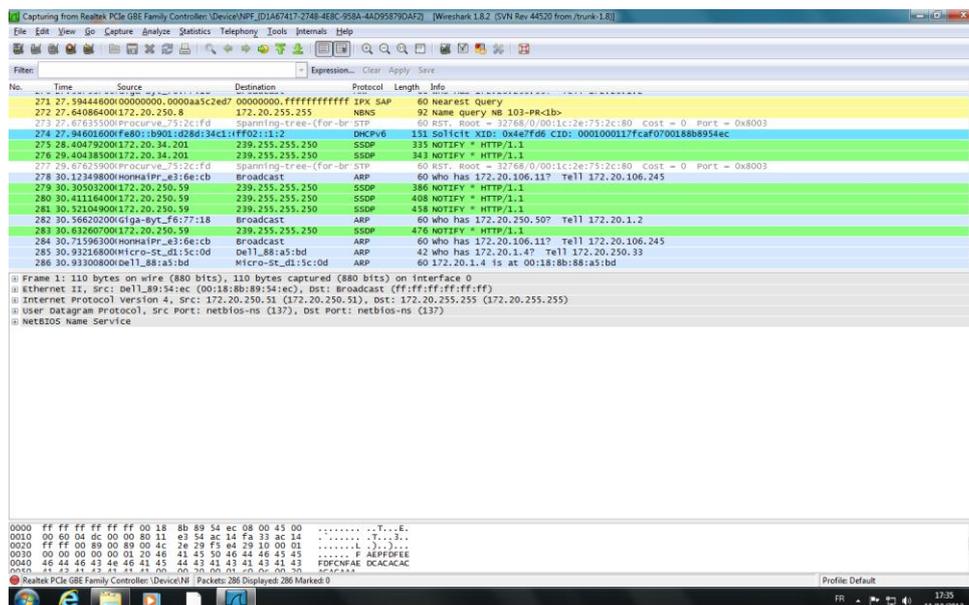
Étape 2 : capture réseau



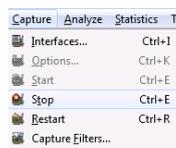
a. Choisir l'interface Ethernet du réseau local pour la capture du trafic.

b. Cliquer sur le bouton Start.  **Start**
Choose one or more interfaces to capture from, then Start

Les fenêtres de capture sont désormais actives. Dans la fenêtre Wireshark, on trouve des colonnes **Source**, **Destination** et **Protocol**.



- c. **Stopper** la capture en cliquant sur dans le menu *Capture*

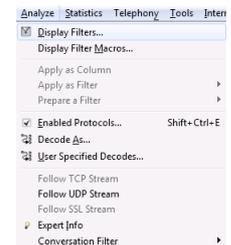


l'icône ou bien en cliquant sur *Stop*

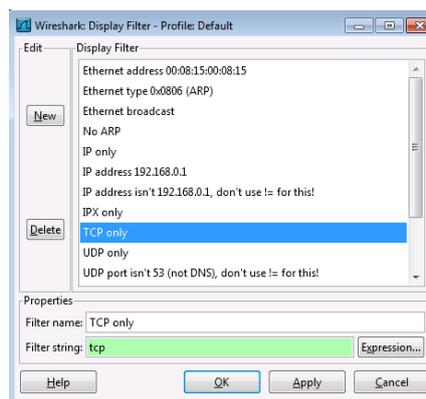
Étape 3 : filtrage de la capture pour afficher uniquement les paquets TCP

Il est possible d'utiliser la fonction de filtrage de Wireshark pour afficher uniquement les paquets TCP.

- a. Cliquer sur l'option **Analyze** dans le menu, puis cliquer sur **Display Filters**.



- b. Dans la fenêtre **Display Filter**, cliquer sur **TCP only**, puis sur **OK**.



Étape 4 : Analyse des paquets

L'affichage des résultats se décompose en trois parties :

- La **liste des trames** capturées disponibles en dessous de la barre de menu avec un affichage synthétique du contenu de chaque trame :

272	27.	64086400(172.20.250.8)	172.20.255.255	NBNS	92 Name query NB 103-PR<1b>
273	27.	67635500(Procurve_75:2c:fd)	Spanning-tree-(for-br>STP	60 RST. Root = 32768/0/00:1c:2e:75:2c:80 Cost = 0 Port = 0x8003	
274	27.	94601600(fe80::b901:d28d:34c1:fff02::1:2)	DHCPv6	151 Solicit XID: 0x4e7fd6 CID: 0001000117fcdf0700188b8954ec	
275	28.	40479200(172.20.34.201)	239.255.255.250	SSDP	335 NOTIFY * HTTP/1.1
276	29.	40438500(172.20.34.201)	239.255.255.250	SSDP	343 NOTIFY * HTTP/1.1
277	29.	67625900(Procurve_75:2c:fd)	Spanning-tree-(for-br>STP	60 RST. Root = 32768/0/00:1c:2e:75:2c:80 Cost = 0 Port = 0x8003	
278	30.	12349800(HonHa1Pr_e3:6e:cb)	Broadcast	ARP	60 who has 172.20.106.11? Tell 172.20.106.245
279	30.	30503200(172.20.250.59)	239.255.255.250	SSDP	386 NOTIFY * HTTP/1.1
280	30.	41116400(172.20.250.59)	239.255.255.250	SSDP	408 NOTIFY * HTTP/1.1
281	30.	52104900(172.20.250.59)	239.255.255.250	SSDP	458 NOTIFY * HTTP/1.1
282	30.	56620200(Giga-Byt_f6:77:18)	Broadcast	ARP	60 who has 172.20.250.50? Tell 172.20.1.2
283	30.	63260700(172.20.250.59)	239.255.255.250	SSDP	476 NOTIFY * HTTP/1.1
284	30.	71596300(HonHa1Pr_e3:6e:cb)	Broadcast	ARP	60 who has 172.20.106.11? Tell 172.20.106.245
285	30.	93216800(Micro-St_d1:5c:0d)	Del1_88:a5:bd	ARP	42 who has 172.20.1.4? Tell 172.20.250.33
286	30.	93300800(Del1_88:a5:bd)	Micro-st_d1:5c:0d	ARP	60 172.20.1.4 is at 00:18:8b:88:a5:bd



- La **décomposition exacte** de la trame sélectionnée dans la liste. Ce volet affiche les détails de la trame sélectionnée. Les **protocoles et les champs de protocole** de chacune des couches sont indiqués. Ils s'affichent sous la forme d'une arborescence qu'il possible de développer ou réduire.

```
Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
Ethernet II, Src: Dell_89:54:ec (00:18:8b:89:54:ec), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 172.20.250.51 (172.20.250.51), Dst: 172.20.255.255 (172.20.255.255)
User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
NetBIOS Name Service
```

- La troisième zone contient la **capture affichée en hexadécimal** et en ASCII.

```
0000 ff ff ff ff ff ff 00 18 8b 89 54 ec 08 00 45 00 .....T...E.
0010 00 60 04 dc 00 00 80 11 e3 54 ac 14 fa 33 ac 14 .....T...3..
0020 ff ff 00 89 00 89 00 4c 2e 29 f5 e4 29 10 00 01 .....L...)...
0030 00 00 00 00 00 01 20 46 41 45 50 46 44 46 45 45 .....F AEPDFEE
.....
```

Si une couche du volet précédent est sélectionnée, **l'entête correspondant à cette couche sera mis en surbrillance**.

Remarque : Le préambule et le CRC de la trame Ethernet ne sont pas visibles car ils sont traités uniquement de façon hardware au sein de la carte réseau.