

TP Wireshark

Wireshark est un analyseur de protocole réseau. Il permet de visualiser et de capturer les trames, les paquets de différents protocoles réseau, filaire ou pas.

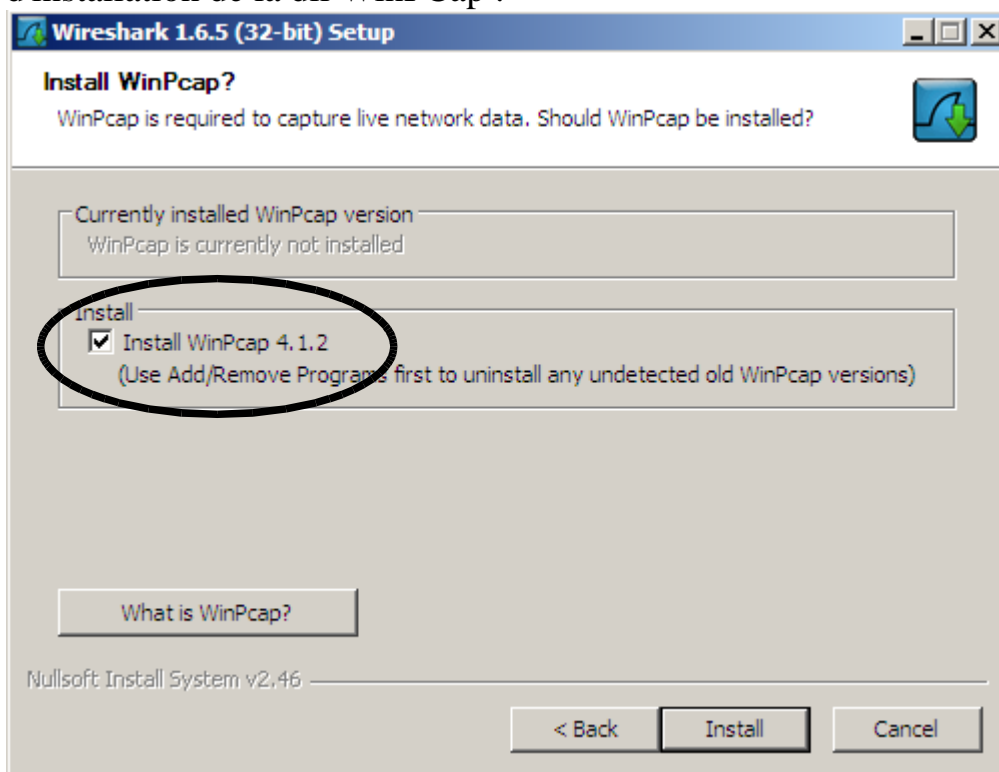
Le site originel est à <http://www.wireshark.org/>. A partir de ce site, on peut lire un tutoriel à http://www.wireshark.org/docs/wsug_html_chunked/.

On peut télécharger pour l'installer sur diverses plate-formes (Windows, Linux, Unix et donc Mac OS) à partir de <http://www.wireshark.org/download.html>. Une FAQ est disponible à <http://www.wireshark.org/faq.html>.

Au 18 février 2013, la dernière version stable est Wireshark 1.8.5. C'est un produit open source et gratuit.

Il a été écrit par Gerald Combs à partir de 1997. C'est la suite du produit Ethereal (son ancien nom).

Pour ce TP, Wirehark est installé sur les machines. Si vous voulez l'installer sur votre propre machine c'est possible. Au moment de l'installation, bien cocher la case d'installation de la dll WinPCap :

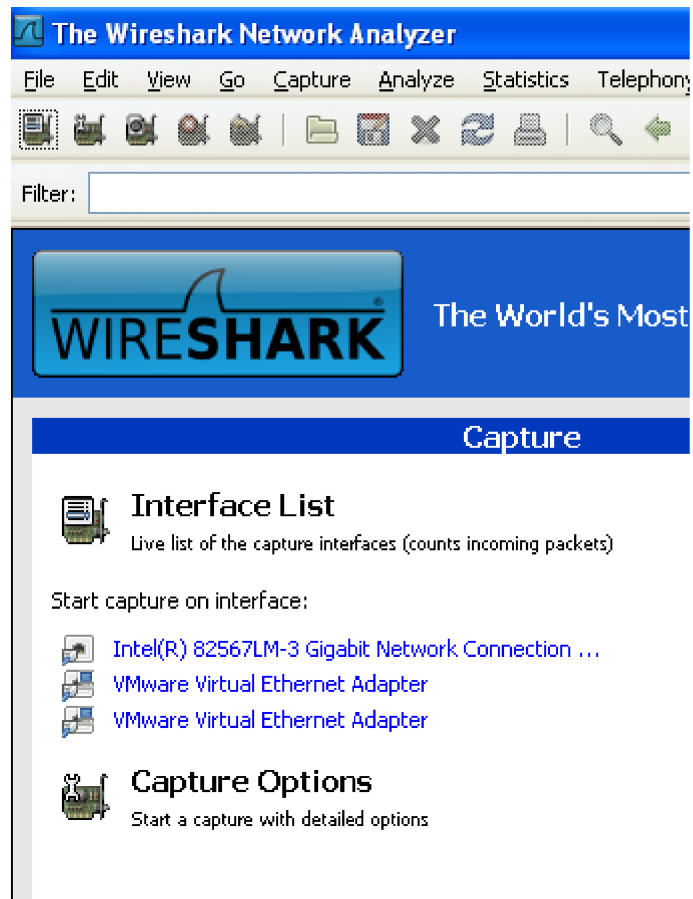


"The experience capturing your first packets can range from "it simply works" to "very strange problems". Si problème voir à <http://wiki.wireshark.org/CaptureSetup>.

Première approche de Wireshark

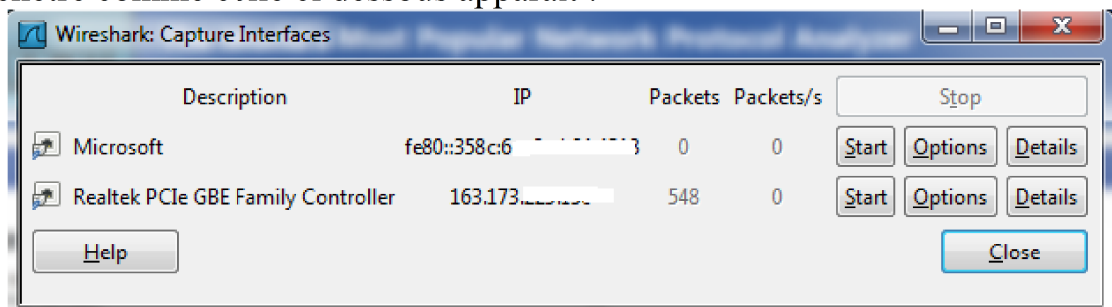


1°) Lancer Wireshark (double clic sur l'icône sur le bureau).
La fenêtre



apparaît.

2°) Sélectionner Capture | Interfaces... (ou cliquer sur Interface List ci dessus). Une fenêtre comme celle ci dessous apparaît :



3°) Repérez une entrée ayant du trafic réseau. Cliquer sur son bouton Start. Vous devriez voir une fenêtre similaire à :

Microsoft [Wireshark 1.6.6 (SVN Rev 41803 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
109	32.584658	23.58.88.100	192.168.1.2	TCP	54	http > 50875 [FIN, ACK] Seq=774 Ack=498 win=15672 Len=0
110	32.584829	192.168.1.2	23.58.88.100	TCP	54	50875 > http [ACK] Seq=498 Ack=775 win=64768 Len=0
111	32.657623	23.58.88.75	192.168.1.2	HTTP	573	HTTP/1.1 404 Not Found (text/html)
112	32.663769	192.168.1.2	23.58.88.75	TCP	54	50874 > http [RST, ACK] Seq=2239 Ack=710 win=0 Len=0
113	33.004940	fe80::6037:5c6c:f3e8::ff02::c	192.168.1.1	SSDP	208	M-SEARCH * HTTP/1.1
114	35.109722	192.168.1.2	192.168.1.1	BJNP	174	Scanner Command: Scan Job Details
115	35.119595	192.168.1.1	192.168.1.2	BJNP	110	Scanner Response: Scan Job Details
116	35.905684	192.168.1.2	192.168.1.255	NBNS	92	Name query NB BBOX<20>
117	35.910386	MS-NLB-PhysServer-31	Broadcast	ARP	42	who has 192.168.1.2? Tell 192.168.1.253
118	35.910439	Universa_5f:eb:05	MS-NLB-PhysServer-31	ARP	42	192.168.1.2 is at cc:52:af:5f:eb:05
119	35.913142	192.168.1.253	192.168.1.2	NBNS	104	Name query response NB 192.168.1.253
120	35.922492	Universa_5f:eb:05	Broadcast	ARP	42	who has 192.168.1.253? Tell 192.168.1.2
121	35.926311	MS-NLB-PhysServer-31	Universa_5f:eb:05	ARP	42	192.168.1.253 is at 02:1f:9f:bf:87:e8
122	35.952281	192.168.1.2	192.168.1.254	DNS	86	Standard query PTR 253.1.168.192.in-addr.arpa
123	35.957181	192.168.1.254	192.168.1.2	DNS	86	Standard query response, No such name
124	37.005233	fe80::6037:5c6c:f3e8::ff02::c	192.168.1.1	SSDP	208	M-SEARCH * HTTP/1.1

Frame 1: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits)

Ethernet II, Src: Universa_5f:eb:05 (cc:52:af:5f:eb:05), Dst: IPv6mcast_00:00:00:0c (33:33:00:00:00:0c)

Internet Protocol Version 6, Src: fe80::6037:5c6c:f3e8:93a9 (fe80::6037:5c6c:f3e8:93a9), Dst: ff02::c (ff02::c)

User Datagram Protocol, Src Port: 56064 (56064), Dst Port: ssdp (1900)

Hypertext Transfer Protocol

```

0000 33 33 00 00 00 0c cc 52 af 5f eb 05 86 dd 60 00 33.....R .....
0010 00 00 00 9a 11 01 fe 80 00 00 00 00 00 00 60 37 .....7
0020 5c 6c f3 e8 93 a9 ff 02 00 00 00 00 00 00 00 00 \l.....
0030 00 00 00 00 00 0c db 00 07 6c 00 9a 78 28 4d 2d .....l..x(M-
0040 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f 31 2e SEARCH * HTTP/1.
0050 31 0d 0a 48 6f 73 74 3a 5b 46 46 30 32 3a 3a 43 1..Host: [FF02::C
0060 5d 3a 31 39 30 30 0d 0a 53 54 3a 75 72 6e 3a 4d ]:1900.. ST:urn:M
0070 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 icrosoft windows
0080 20 50 65 65 72 20 4e 61 6d 65 20 52 65 73 6f 6c Peer Na me Resol
0090 75 74 69 6f 6e 20 50 72 6f 74 6f 63 6f 6c 3a 20 ution Pr otocol:
00a0 56 34 3a 49 50 56 36 3a 4c 69 6e 6b 4c 6f 63 61 v4:IPv6: LinkLoca
00b0 6c 0d 0a 4d 61 6e 3a 22 73 73 64 70 3a 64 69 73 l..Man: " ssdp:dis
00c0 63 6f 76 65 72 22 0d 0a 4d 58 3a 33 0d 0a 0d 0a cover"... MX:3....

```

4°) Indiquer ce qu'on appelle une "pile" réseau. Donner les composants essentiels de la pile OSI/ISO. Indiquer pour chacune des couches leurs fonctionnalités. Donner les composants essentiels de la pile internet. Pourquoi appelle-t-on cela une pile ?

5°) Donner des exemples de protocoles réseau que vous connaissez qui apparaissent dans votre (cette) fenêtre.

6°) La "pile" réseau est illustrée dans une partie de la fenêtre. Indiquer les couches empilées qui ont été utilisées pour la transmission d'un paquet donné. Pour un paquet donné en étudiant chacune de ces couches, indiquer des informations techniques comme :

- la date d'arrivée
- la valeur MAC de la machine émettrice
- l'adresse IP de la machine émettrice
- son type MIME

7°) Sélectionner certains messages et visualiser leur contenu y compris en hexadécimal !

Les protocoles Ethernet et ARP

Pour communiquer sur internet, on utilise les adresses IP. Un des intérêts et de pouvoir hiérarchiser les adresses (une grande entreprise aura une plage d'adresse de type A, une plus petite, une plage beaucoup plus petite d'adresse de type C). Ce sont ces adresses IP qui sont utilisées par les routeurs et pour envoyer un message de France en Australie.

Lorsque le message arrive dans le sous réseau (= petit réseau d'entreprise) contenant votre ordinateur, on utilise les adresses MAC (Media Access Control). Par exemple le protocole Ethernet utilise les adresses MAC.

8°) Expliquer comment fonctionne le protocole Ethernet.

Indication : C'est un protocole de la forme CSMA/CD c'est à dire Carrier Sense Multiple Access with Collision Detection (écoute de porteuse avec accès multiples et détection de collision).

9°) Indiquer le rôle joué par une adresse MAC. Peut il y avoir des ordinateurs sur la planète qui ont la même adresse MAC ? Donner un équivalent de la notion d'adresse MAC pour les personnes françaises.

10°) Il va donc falloir traduire les adresses IP en adresse MAC. Le protocole qui le fait est le protocole ARP (Address Resolution Protocol) (pour la version IPv4). Indiquer dans quelle couche réseau est situé le protocole ARP (bon sens).

11°) Indiquer comment fonctionne le protocole ARP c'est à dire indiquer comment dans un sous réseau, ce protocole s'y prend pour trouver l'adresse MAC d'un ordinateur (ou périphérique) ayant une adresse IP de la forme XXX.YYY.ZZZ.TTT. En déduire qu'on ne pourrait pas utiliser ce protocole pour transmettre des messages sur la planète.

12°) Vous pouvez voir dans une fenêtre Windows les correspondances (= la table) IP / MAC en tapant `arp -a`.

Les filtres sous Wireshark

Comme la première étape fait apparaître toutes sortes de paquets et comme "trop d'information tue l'information", on veut ne faire apparaître qu'un certain type de paquet. Wireshark propose 2 types de filtres l'un au moment de la capture, l'autre au moment de l'affichage.

Plus précisément :

- les filtres de capture sont les filtres qui sélectionnent les données à enregistrer dans les journaux. Ils sont définis au démarrage de la capture,
- les filtres d'affichage sont utilisés pour rechercher à l'intérieur des données capturées. Ils peuvent être modifiés pendant que des données sont capturées.

Ainsi un filtre d'affichage est utilisé pour rechercher à l'intérieur des données récoltées avec un filtre de capture.

Mise en place de filtre

source : les tutoriaux à

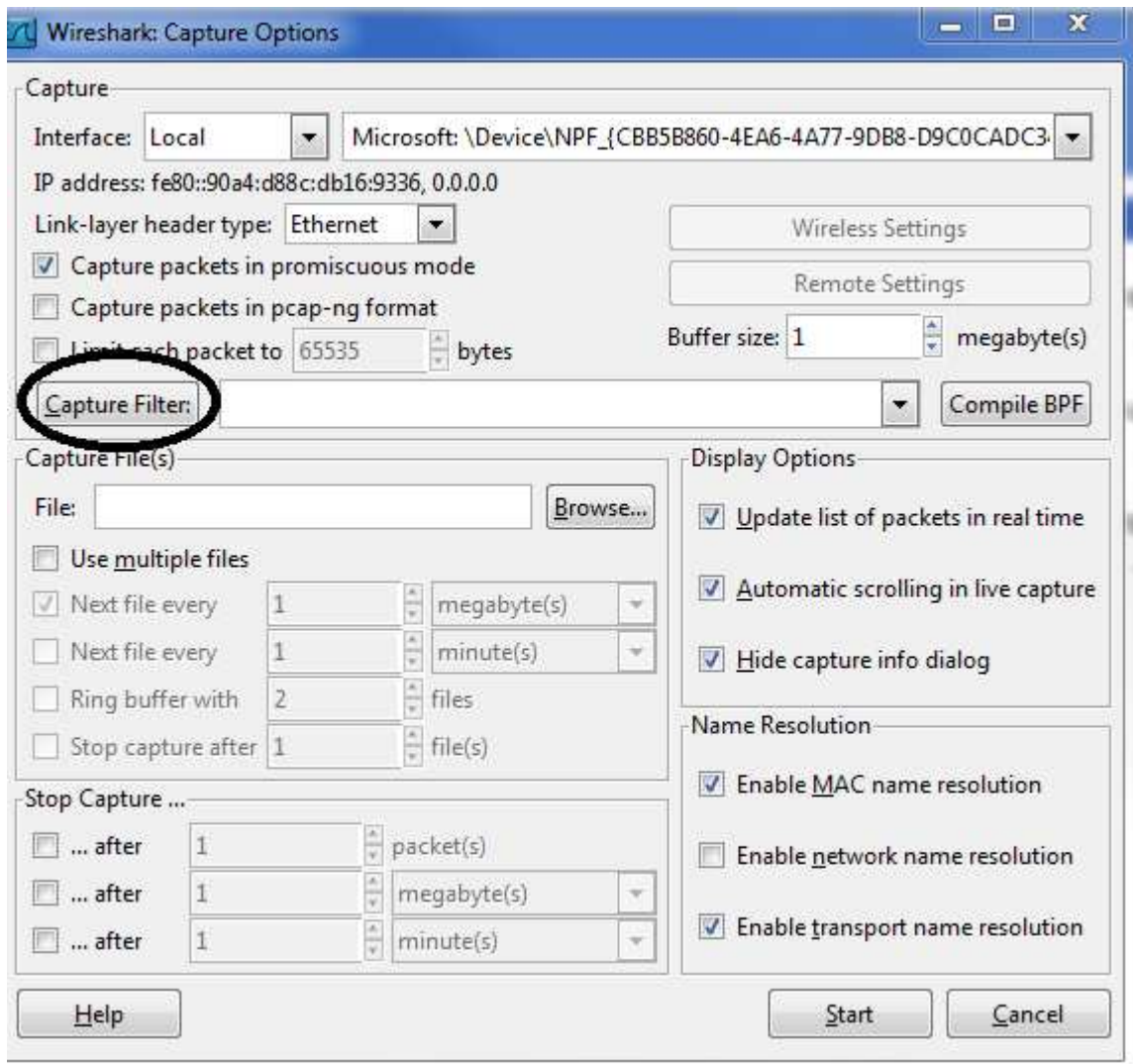
http://www.wireshark.org/docs/wsug_html_chunked/ChCapCaptureFilterSection.html

et à

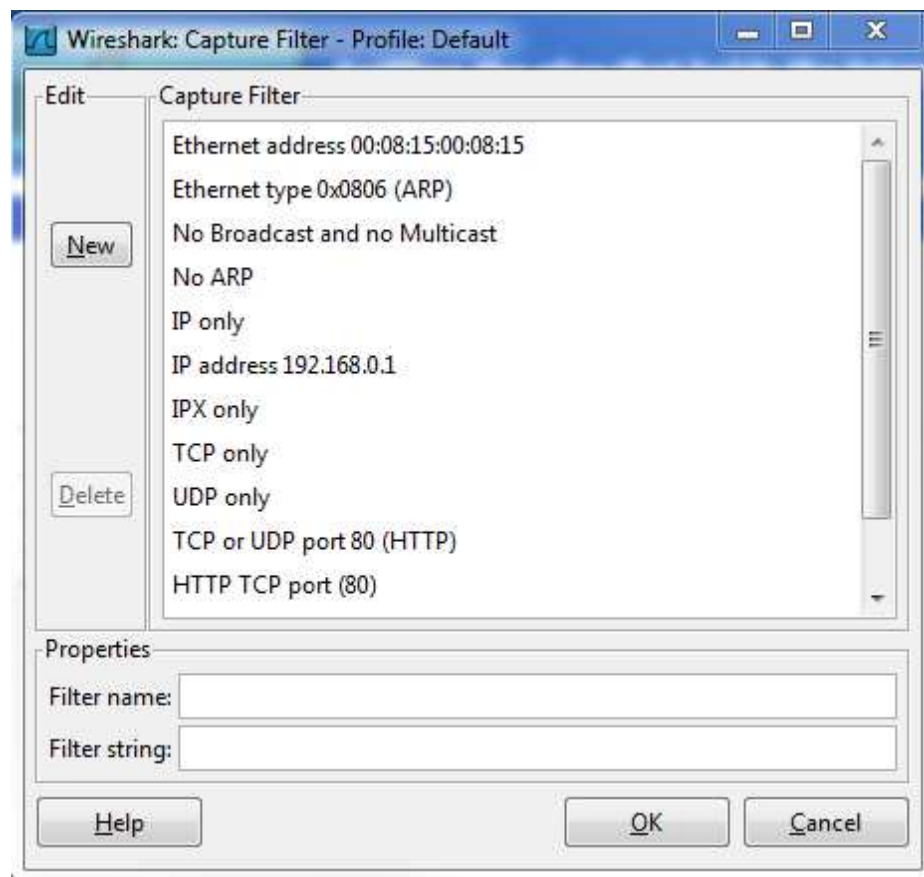
http://www.wireshark.org/docs/wsug_html_chunked/ChWorkDisplayFilterSection.html

Il faut construire le filtre avant de lancer la capture.

Lorsque vous lancez la demande de capture (cf. début du TP), sélectionner le bouton options, puis dans la fenêtre "Wireshark: Capture Options", le bouton "Capture Filter:"



La fenêtre "Wireshark: Capture Filter - Profile: Default" propose des protocoles. Comme Wireshark est plutôt orienté "couches hautes", choisissez celui qui convient pour n'obtenir que les paquets HTTP.



Cliquer OK, puis dans la fenêtre "Wireshark: Capture Options" cliquer start.

Remarque

Ces filtres peuvent être très puissants. On peut filtrer suivant la consition :

`src host 10.7.2.12 and not dst net 10.200.0.0/16`

Voir un bon tutoriel sur les filtres à

http://openmaniak.com/fr/wireshark_filters.php.

Retour sur ARP

Retrouver un message ARP. On pourra éviter les filtres. Indiquer la correspondance entre des adresses IP et des adresses MAC pour deux machines.

Sauvegarde et Relecture

Vous pouvez sauvegarder un travail dans Wireshark. Pour cela il faut arrêter la capture par Capture | Stop. Le bouton Save du menu File est alors actif. Sauvegarder le travail dans un fichier dans votre répertoire de travail (pas sur le bureau !).

Vous pouvez relire un travail dans Wireshark. Pour cela il faut arrêter la capture par Capture | Stop. Le bouton Open du menu File est alors actif. Charger le fichier que vous voulez relire. Il s'affiche dans Wireshark.

Bibliographie

En plus des éléments donnés en début de cet énoncé, on peut trouver :

Un tutorial à :

<http://blog.nicolargo.com/2007/07/tutoriel-wireshark-ex-ethereal.html>

Les filtres à http://openmaniak.com/fr/wireshark_filters.php

Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems, C. Sanders; ed. no starch press.

Wireshark Network Analysis (Second Edition): The Official Wireshark Certified Network Analyst Study Guide, Laura Chappell; ed Chappell University.

Wireshark Certified Network Analyst Exam Prep Guide (Second Edition), Laura Chappell; ed Chappell University.