Annexe - Wireshark

1 Introduction

Wireshark est un analyseur de protocoles *open source*, disponible pour les plateformes Windows, Mac OS, Linux et autres. Il permet d'examiner des paquets à partir d'un fichier ou directement en les capturant sur le réseau. Pour chaque paquet, il est possible d'obtenir un résumé ainsi qu'un décodage détaillé.

En outre, le logiciel possède des fonctionnalités très utiles comme les filtres de capture et d'affichage et la reconstitution du flux d'une session TCP. De plus, le nombre de protocoles reconnus est très élevé.

2 Tutoriel vidéo

En guise d'introduction rapide à Wireshark vous pouvez regarder le tutoriel vidéo sur le site Wireshark : http://wiresharkdownloads.riverbed.com/video/wireshark/introduction-to-wireshark/.

La vidéo est en anglais.

3 Interface

Après avoir démarré le programme et effectué une capture, on obtient une fenêtre similaire à la Figure 1.

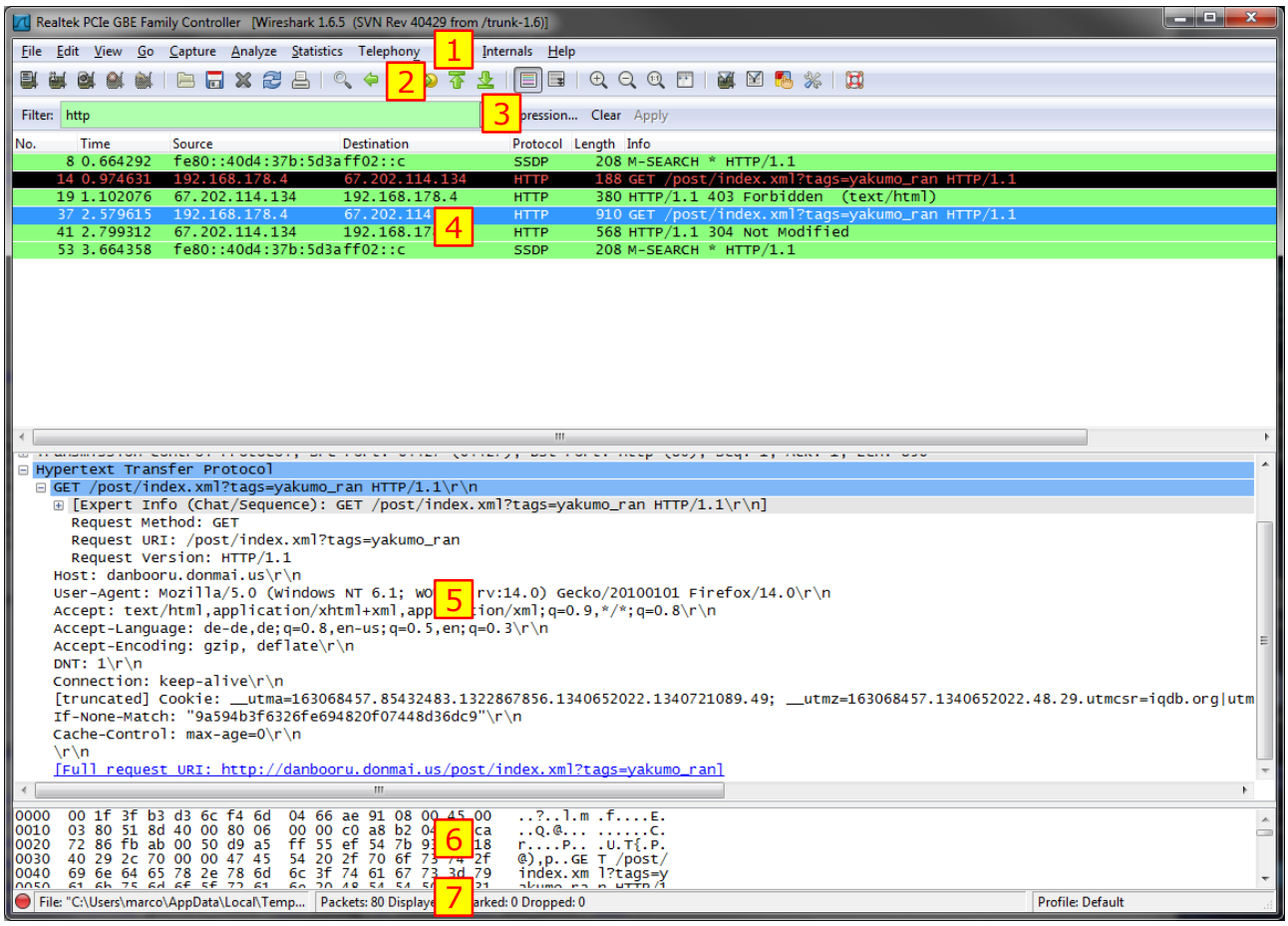

Figure 1: Fenêtre principale de Wireshark

La fenêtre principale est divisée en différentes zones :

1. **La barre de menus**. Utilisée pour démarrer les différentes actions, comme dans n'importe quelle application graphique.
2. **La barre d'outils**. Offre des raccourcis vers les actions les plus utilisées.
3. **La barre d'outils des filtres**. Permet de manipuler des filtres d'affichage.
4. **Le panneau liste de paquets**. Affiche la liste des paquets ainsi que leurs caractéristiques principales. En cliquant dans ce panneau, on contrôle l'affichage des deux autres.
5. **Le panneau détail de paquet**. Montre le détail du paquet sélec- tionné dans le panneau liste. Chaque niveau peut être développé indépendamment des autres.
6. **Le panneau bytes**. Visualise le contenu brut des trames. Il repré- sente le paquet sélectionné dans le panneau 1 et met en évidence le champ sélectionné dans le panneau 2.
7. **La barre d'état**. Montre des informations détaillées dur l'état du programme et les données capturées.

4 Capturer des paquets

Pour démarrer une capture, sélectionner le menu "Capture" / "Start..."

(ou CTRL+K ou ) afin de faire apparaître la boîte de dialogue des options de capture (Figure 2).

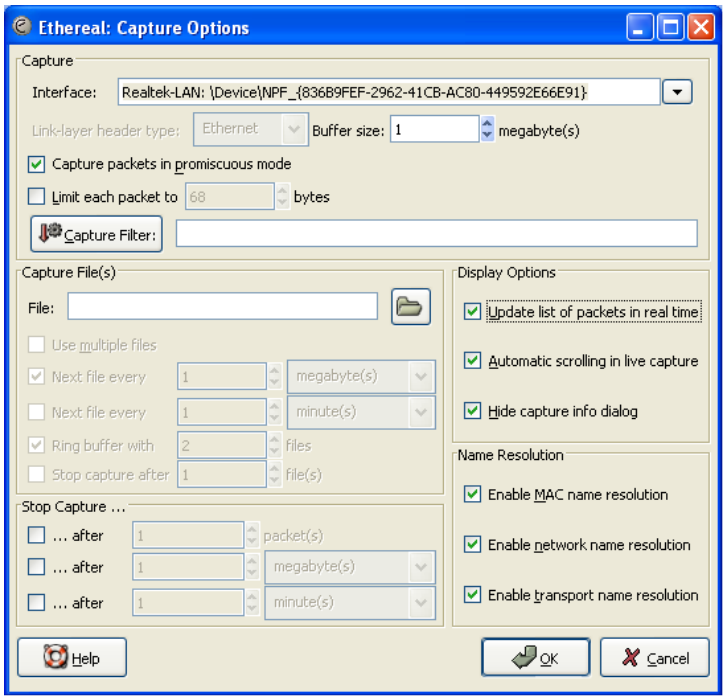

Figure 2: Dialogue des options de capture

La capture peut être personnalisée avec les paramètres suivants :

- **Interface** : L'interface réseau sur laquelle la capture est effectuée. Sous Windows, le nom de l'interface est fonction de l'identification du matériel dans la base de registres. Attention à ne pas choisir l'interface NDIS WAN. Pour Linux, utilisée ethX, où X est le numéro de l'interface, en général eth0. Indiquer any si l'interface à l'adresse IP 0.0.0.0. Ceci est utile en cas d'analyse passive du réseau. L'analyseur ne "pollue" pas avec ses propres messages.
- **Capture packets in promiscuous mode** : L'option *promiscious* permet de capturer des paquets qui ne nous sont pas destinés.
- **Filter** : La zone de texte permet d'indiquer ou de modifier le *filtre de capture*. Le bouton ouvre la boîte de dialogue contenant les filtres enregistrés. La conception d'un filtre de capture est présentée plus bas.
- **Enable network name resolution** : Permet de traduire les adresses IP avec le nom de machine équivalent. **Attention, le serveur DNS doit être accessible.**

- **Enable transport name resolution** : Permet d'indiquer le nom du protocole, ceci pour les numéros de ports connus.

Lorsque toutes les options désirées sont choisies, cliquer sur "OK" pour démarrer la capture. Une nouvelle boîte de dialogue s'ouvre alors et indique l'évolution de la capture. Cliquer sur le bouton "Stop" ou l'icône pour terminer la session de capture. ☐L'affichage peut être modifié à souhait à l'aide des filtres d'affichage. Des informations sont données à la Section "Filtres d'affichages".

5 Filtres d'affichage

Après avoir effectué une capture, il est toujours possible de modifier l'affichage des paquets en spécifiant un filtre d'affichage (ou filtre de post-capture).

La sélection peut se faire sur :

- un protocole : par exemple *http*
- la présence d'un champ : par exemple *http.cookie* ou *not http.cookie*
- les valeurs des champs : par exemple *ip.src == 192.168.0.155*

Les filtres d'affichage sont manipulés à l'aide de la barre d'outils des filtres (voir Figure 1). Le bouton "Filter" permet de charger un filtre enregistré préalablement.

La boîte de dialogue d'enregistrement des filtres est atteignable par le menu "Analyse" -> "Display Filters..." ou  l'icône.

Vous pouvez aussi sélectionner un champ dans les détails d'un paquet, puis avec clic droit : Apply as filter…

6 Filtres de capture

Les filtres de captures permettent de réduire le nombre de paquets capturés, ce qui peut être utile lors de capture de grands volumes de trafic.

La syntaxe est différente des filtres d'affichage. Par exemple, le filtre

host 192.168.0.1 and port 80

capture uniquement du trafic http (port 80) de l'adresse IP donnée.

Vous pouvez enregistrer des filtres de capture et les charger au besoin.

Pour utiliser un filtre de capture, utiliser le menu « Capture » -> « Capture Filters » ou l'icône  .

7 Flux TCP et UDP

Wireshark possède une méthode utile qui permet d'afficher le texte de tous les paquets d'un flux, comme par exemple d'une connexion http. Wireshark affiche alors le contenu des requêtes http ainsi que des réponses. Ceci est très utile pour suivre une conversation entre deux machines.

Pour suivre un flux, il faut sélectionner un paquet faisant parti du flux puis cliquer sur le menu « Analyze » / « Follow TCP Stream » ou « Follow UDP Stream ». Ne pas oublier que l'utilisation de cette option applique un filtre d'affichage afin de ne prendre en compte que les paquets en relation à la session sélectionnée. Pour supprimer le filtre d'affichage, il suffit d'appuyer sur le bouton « Clear » en bas de la fenêtre.

8 Plus d'informations

Vous pouvez trouver plus d'informations sur le site Web http://www.wireshark.org/.