TP - MODELISATION DES RESEAUX

Objectifs :

- Connaitre la classification des protocoles présents dans les réseaux ;
- Comprendre le rôle d'un protocole réseau suivant son niveau ;
- Comprendre le principe de l'encapsulation par rajout successif des en-têtes de protocole.

1. Présentation de l'analyseur de protocoles « Wireshark »

Wireshark est un analyseur de protocole (*sniffer*) gratuit et *open-source*, utilisable sur les systèmes Windows et Linux et MAC OS. Il est actuellement téléchargeable à l'adresse http://www.wireshark.org/download.html

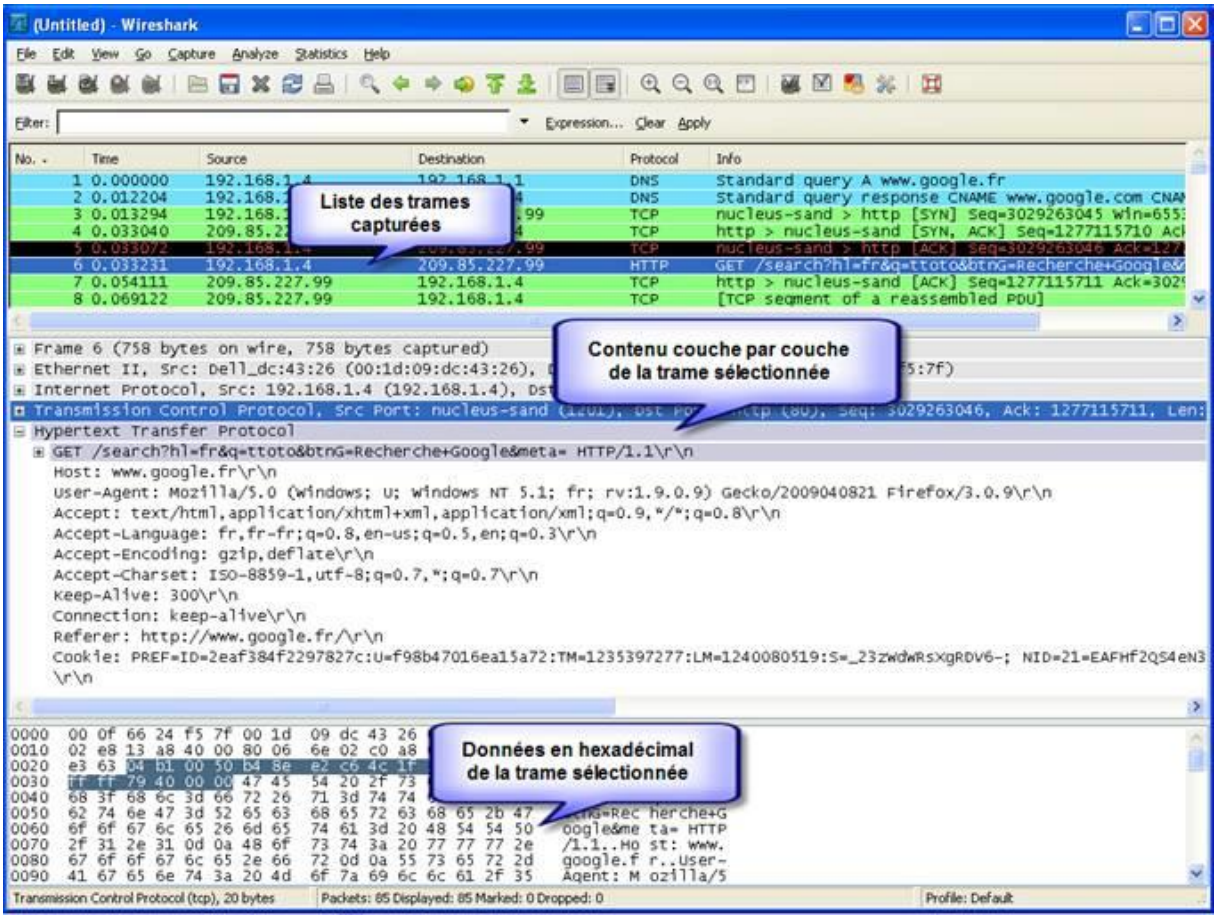
L'interface de *Wireshark* est constituée de trois fenêtres principales (voir figure) :

- La fenêtre la plus haute liste les trames capturées dont elle résume les caractéristiques (une couleur par protocole). En cliquant sur une trame de cette fenêtre, vous modifiez le contenu des deux autres.
- La fenêtre du milieu décrit précisément le contenu de la trame sélectionnée dans la fenêtre précédente. Les champs constituant la trame et les protocoles associés à chaque couche, ainsi que diverses informations fournies par le logiciel, y sont présentés dans une structure arborescente reprenant le modèle en couches OSI (ou le modèle TCP-IP suivant le nombre de couches présentes).
- La fenêtre du bas contient les données (exprimées en hexadécimal) portées par la trame sélectionnée. Les champs sélectionnés dans l'arbre de la fenêtre du milieu y sont affichés en surligné.

Pour éviter d'afficher toutes les trames qui circulent sur le réseau, vous pouvez utiliser un **filtre à la capture** (l'analyseur ne capture que les trames issues de l'adresse IP 192.168.1.3 avec un protocole de messagerie SMTP par exemple) ou un **filtre à l'affichage** (toutes les trames sont capturées mais seules les trames SMTP sont affichées).
Le filtre d'affichage est plus simple d'emploi, il est activé à l'aide du bouton « Filter » sous la barre des icônes. Vous accédez alors à la boîte de dialogue dédiée à la construction de filtres d'affichage. La fenêtre à sa droite vous permet de composer un filtre directement ou d'en choisir un prédéfini ; il est activé en cliquant sur le bouton « Apply ». Un clic sur le bouton « Clear » désactive le filtre d'affichage en cours d'utilisation. L'aide intégrée (F1) explique la syntaxe des filtres d'affichage (section 6.3).

Pour lancer une capture, sélectionnez «Options » dans le menu « Capture ». La fenêtre « Capture options » s'affiche. Elle vous permet de définir les options à utiliser lors de la capture : interface sur laquelle est réalisée la capture, utilisation d'un filtre de capture, limitation du nombre de trames capturées, durée de la capture, résolution de nom à l'affichage. **Attention** : vous devez sélection une interface qui correspond à une carte réseau active sur vote PC. Par ailleurs, la case « Capture packets in promiscuous mode » qui permet de capturer toutes les trames (y compris celles qui n'ont ne provienne pas ou ne sont pas destinées à votre PC) doit être décochée si vous utilisez une interface WiFi.

Un manuel utilisateur est disponible à l'adresse http://www.wireshark.org/docs/wsug_html_chunked/



2.Etude des couches OSI.

a) Lancez une capture (gardez toutes les options par défaut).

b) Utilisez votre navigateur ou votre messagerie pour faire du trafic. Vous devez voir apparaitre les trames capturées, dans le cas contraire sélectionnez une autre interface.

c) Quels protocoles voyez-vous apparaitre dans la fenêtre du haut ?

d) Sélectionnez les successivement les différentes trames capturées, toutes les couches du modèle OSI sont-elles représentées dans la fenêtre du milieu ? Expliquez.

e) Quelle est la taille des trames capturées ?

f) Choisissez une trame dans laquelle le protocole HTTP est présent (il faut pour cela que vous généries du trafic avec votre navigateur). Sélectionnez ensuite dans la fenêtre du milieu les différents protocoles présent dans cette trame (Ethernet, IP, TCP, HTTP). Les octets correspondant à chacun des en-têtes de protocole doivent apparaitre en surligné dans la fenêtre du bas. Combien d'octets obtenez-vous pour chaque protocole ? Retrouvez en additionnant le total indiqué sur la première ligne de la fenêtre du milieu.

g) Dans quel ordre les octets sont-ils capturés par l'analyseur ? En d'autres termes, à quelle couche correspondent les premiers octets de la trame ? Comment sont encapsulées les données HTTP pour au final constituer une trame circulant sur le réseau ?

3. Analyse du protocole HTTP

a) Lancez une capture. Connectez-vous à un site web quelconque à l'aide de votre navigateur. Arrêtez la capture.
Utilisez un filtre à l'affichage pour ne visualiser que les trames contenant le protocole http.

b) Développez dans la fenêtre du milieu le protocole http. Quelle est la première commande HTTP relevée ? A quoi correspond-t-elle ? Retrouvez dans l'en-tête http les différentes informations : nom du site demandé (URL), version du navigateur utilisé, langage accepté.

c) Analysez la première réponse du serveur web interrogé. Quel est le type du serveur web ? Combien reste-t-il d'octets après l'en-tête http ? A quoi correspondent-t-il ?

d) Quel est l'intérêt d'indiquer dans l'en-tête http la date et l'heure et une information de type « Last-Modified » ?