
TP - MODELISATION DES RESEAUX

Objectifs :

- Connaître 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 sélectionner une interface qui correspond à une carte réseau active sur votre PC. Par ailleurs, la case « Capture packets in promiscuous mode » qui permet de capturer toutes les trames (y compris celles qui n'ont 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/

The screenshot shows the Wireshark interface with the following components:

- Filter:** Empty.
- Packet List:**

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.4	192.168.1.1	DNS	Standard query A www.google.fr
2	0.012204	192.168.1.1	192.168.1.4	DNS	Standard query response CNAME www.google.com CNAME
3	0.013294	192.168.1.1	192.168.1.4	TCP	nucleus-sand > http [SYN] Seq=3029263045 win=65535
4	0.033040	209.85.227.99	192.168.1.4	TCP	http > nucleus-sand [SYN, ACK] Seq=1277115710 Ack=1277115711
5	0.033072	192.168.1.4	209.85.227.99	TCP	nucleus-sand > http [ACK] Seq=3029263046 Ack=1277115711
6	0.033231	192.168.1.4	209.85.227.99	HTTP	GET /search?hl=fr&q=ttoto&btnG=Recherche+Google&meta= HTTP/1.1
7	0.054111	209.85.227.99	192.168.1.4	TCP	http > nucleus-sand [ACK] Seq=1277115711 Ack=3029263046
8	0.069122	209.85.227.99	192.168.1.4	TCP	[TCP segment of a reassembled PDU]
- Packet Details:**
 - Frame 6 (758 bytes on wire (758 bytes captured) on interface 0:00:00:00:00:00)
 - Ethernet II, Src: Dell_dc:43:26 (00:1d:09:dc:43:26), Dst: 192.168.1.4 (02:00:00:00:00:00)
 - Internet Protocol, Src: 192.168.1.4 (192.168.1.4), Dst: 209.85.227.99 (01:00:00:00:00:00)
 - Transmission Control Protocol, Src Port: nucleus-sand (4242), Dst Port: http (80), Seq: 3029263046, Ack: 1277115711, Len: 758
 - Hypertext Transfer Protocol
 - GET /search?hl=fr&q=ttoto&btnG=Recherche+Google&meta= HTTP/1.1
 - Host: www.google.fr
 - User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; fr; rv:1.9.0.9) Gecko/2009040821 Firefox/3.0.9
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
 - Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
 - Accept-Encoding: gzip,deflate
 - Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
 - Keep-Alive: 300
 - Connection: keep-alive
 - Referer: http://www.google.fr
 - Cookie: PREF=ID=2eaf384f2297827c:U=f98b47016ea15a72:TM=1235397277:LM=1240080519:S=_23zwdwRsxgRDV6-; NID=21=EAFHF2Q54eN3
- Packet Bytes:**

```

0000  00 0f 66 24 f5 7f 00 1d 09 dc 43 26
0010  02 e8 13 a8 40 00 80 06 6e 02 c0 a8
0020  e3 63 04 31 00 50 05 86 22 55 10 1f
0030  ff 79 40 00 00 47 45 54 20 2f 73
0040  68 3f 68 6c 3d 65 72 26 71 3d 74 74
0050  62 74 6e 47 3d 52 65 63 68 65 72 63 68 65 2b 47
0060  6f 6f 67 6c 65 26 6d 65 74 61 3d 20 48 54 54 50
0070  2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e
0080  6f 6f 6f 67 6c 65 2e 66 72 0d 0a 55 73 65 72 2d
0090  41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35
  
```

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 apparaître les trames capturées, dans le cas contraire sélectionnez une autre interface.

c) Quels protocoles voyez-vous apparaître 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 génériez 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 apparaître 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 » ?