Sommaire

INTRODUCTION

Objectifs

Être capable d'utiliser un analyseur de protocoles.

Découvrir les caractéristiques générales et l'encapsulation des protocoles du modèle "TCP/IP"

Contexte

Un ordinateur équipé d'une carte de communication Ethernet fonctionnant sous Windows ou Linux sur lequel est installé un logiciel d'analyse de trames.

On utilisera dans les manipulations **tcpdump** (sous Linux) et **Wireshark** (sous Windows ou Linux).

tcpdump

tcpdump est un « *packet sniffer* » en ligne de commande. Il permet d'obtenir le détail du trafic visible depuis une interface réseau. C'est un outil de mise au point apprécié pour sa puissance.

Site officiel : http://www.tcpdump.org/

[Source : http://fr.wikipedia.org/wiki/Tcpdump]

Wireshark

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 est multi-plates-formes, il fonctionne sous Windows, Mac OS X, Linux, Solaris, ainsi que sous FreeBSD. Wireshark reconnait 759 protocoles.

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

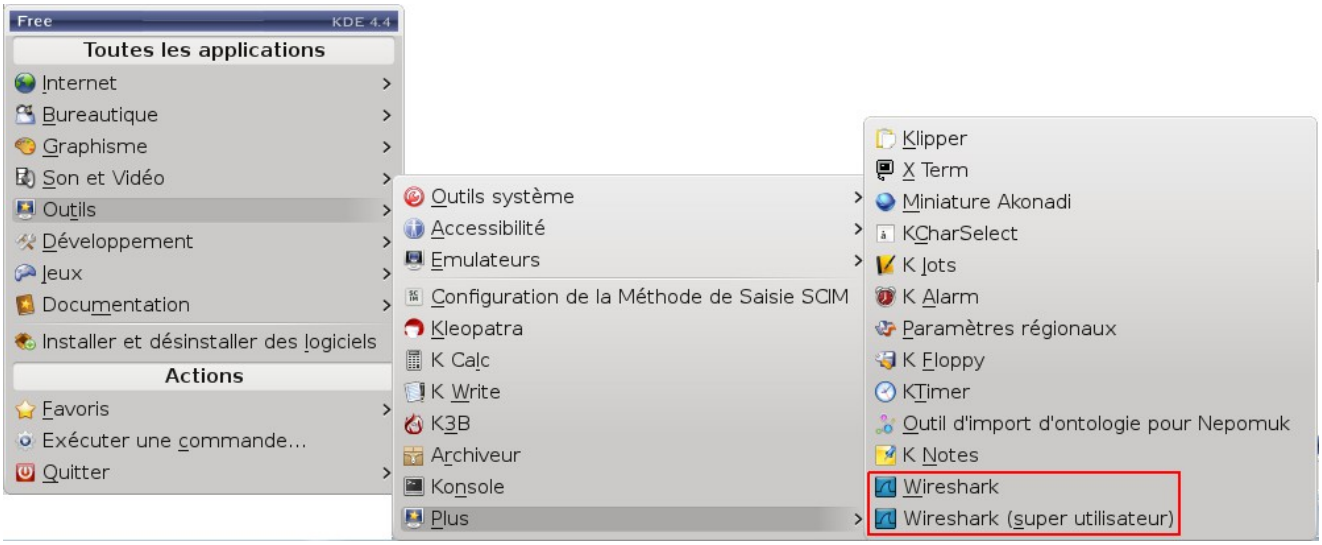
Documentation : http://www.wireshark.org/docs/wsug_html_chunked/index.html

[Source : http://fr.wikipedia.org/wiki/Wireshark]

INSTALLATION

Vérifier si le logiciel Wireshark est installé sur votre poste.

- Sous Linux (Mandriva 2010) :



Ou en mode console :

```
$ wireshark -help
Wireshark 1.2.10
Interactively dump and analyze network traffic.
See http://www.wireshark.org for more information.
...
```

Sinon installation (sous le compte root) à partir de la console :

```
# urpmi wireshark
```

Remarque : sous Linux, wireshark propose deux modes d'exploitation : le mode simple utilisateur et le mode super utilisateur (root). La différence essentielle entre les deux modes se situe au niveau de la capture de trames à partir des interfaces réseaux permises seulement en mode super utilisateur. Le mode simple utilisateur servira surtout pour l'analyse de trames déjà capturées.

- Sous Ubuntu :

Installation (sous le compte root) à partir de la console :

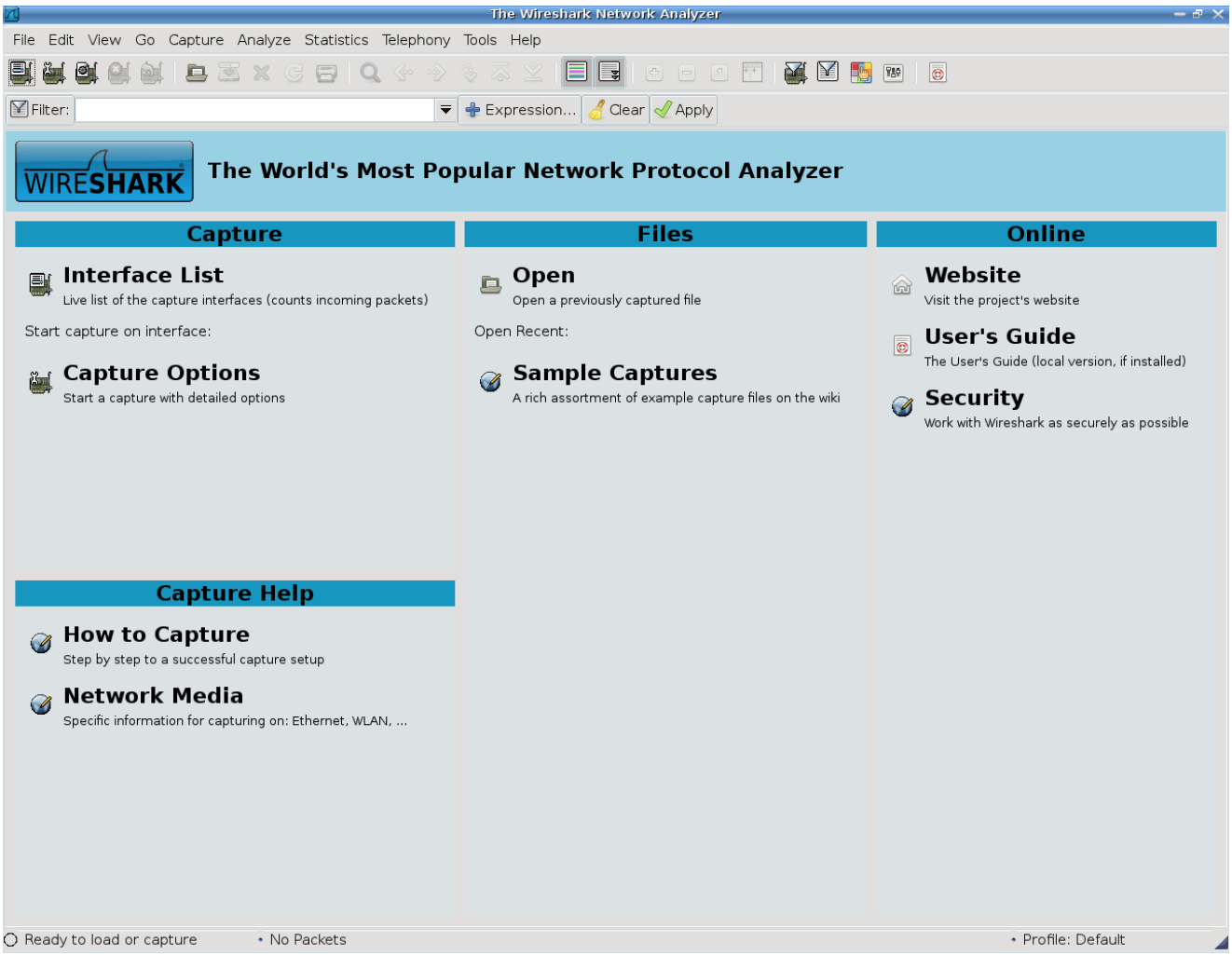
```
# apt-get install wireshark
```

- Sous Windows : l'installation se fait à partir d'une version adaptée à son système téléchargée à partir du site http://www.wireshark.org/download.html

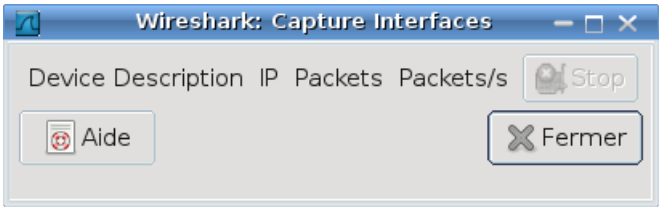
PRISE EN MAIN

Mode simple utilisateur

Le logiciel s'ouvre sur cette page de menu :



On peut vérifier qu'en cliquant sur « **Interface List** » que l'on possède aucun droit d'accès sur les interfaces réseaux disponibles pour une capture :

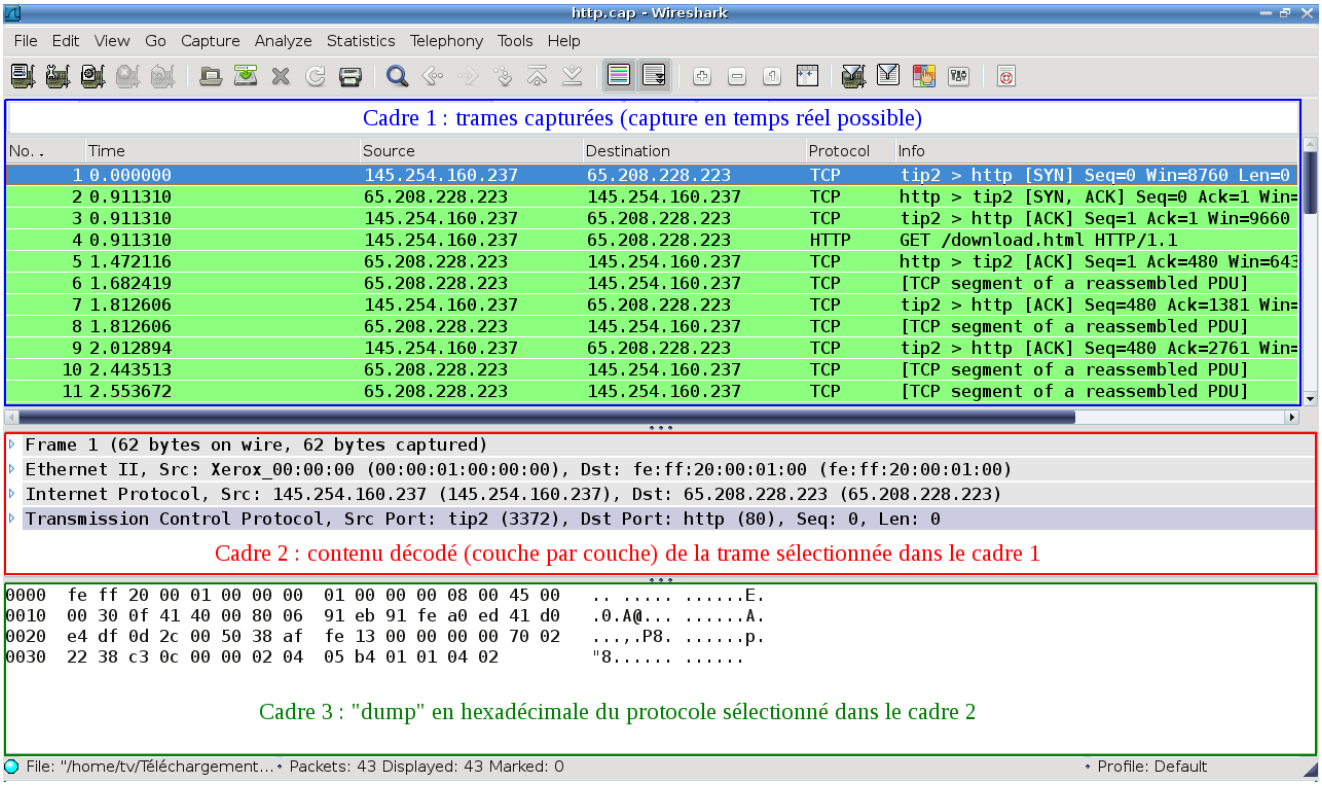


Remarque : il faudra donc passer en mode super utilisateur (root) pour réaliser des captures sur ses interfaces réseaux.

Donc, on utilisera essentiellement le menu « **Open** » qui permettra de charger un fichier de capture pour analyse.

Ouvrir le fichier `http.cap` disponible sur le serveur ou sur le site http://wiki.wireshark.org/SampleCaptures (HTTP).

L'affichage se décompose en trois cadres :

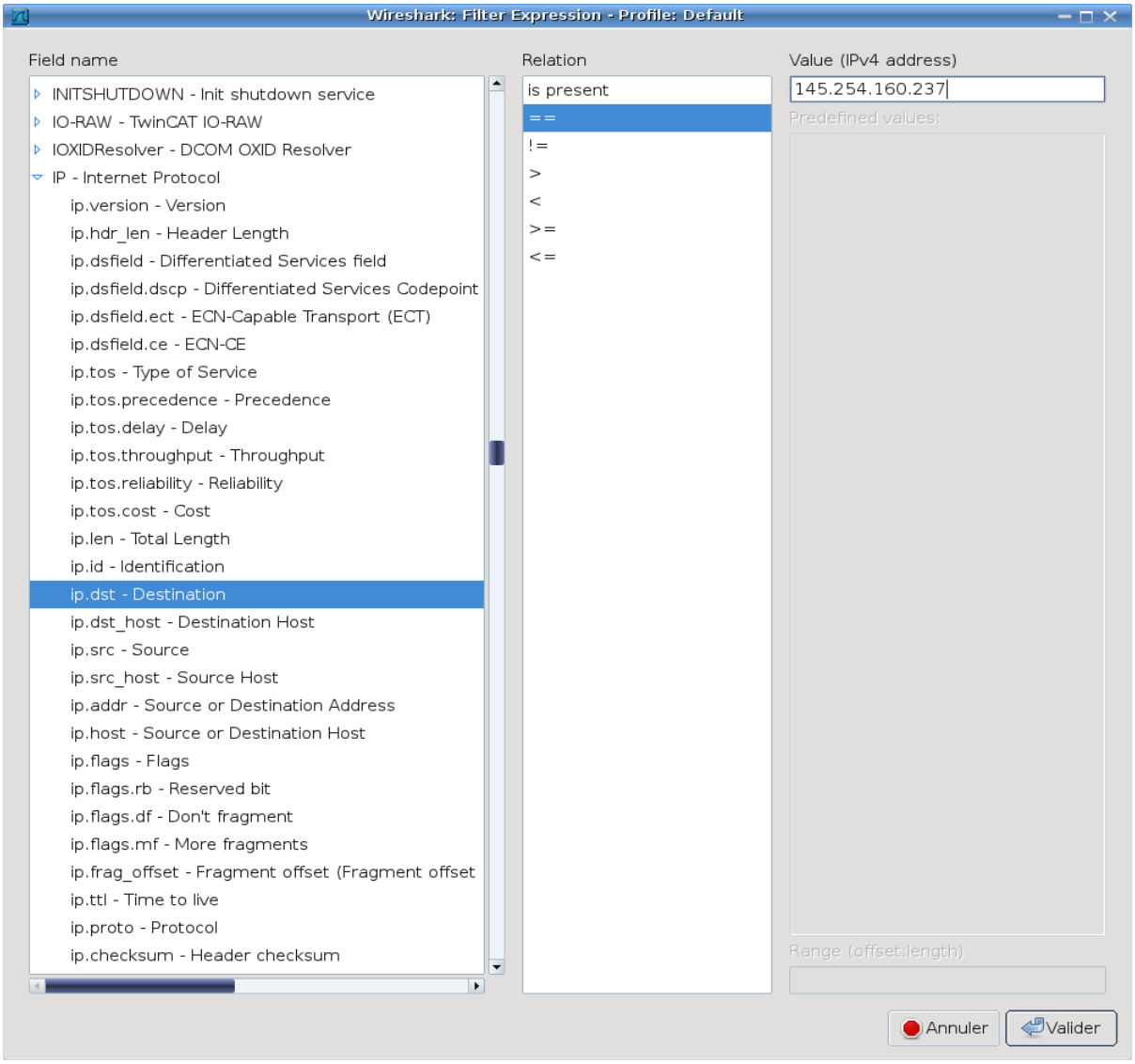


Filtrage

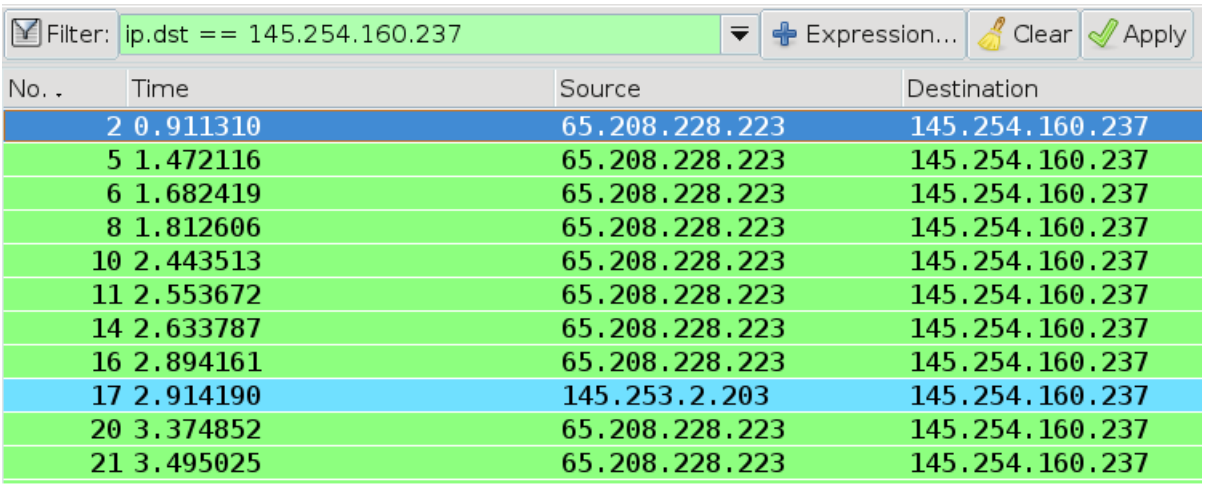
Il est possible (indispensable !) de créer des filtres d'affichage qui ne montrent que les trames conformes à la règle de filtrage. Cela permettra d'isoler un échange en particulier ou l'analyse d'un protocole spécifique.

On renseignera alors le cadre **Filter** dans la barre du haut du cadre 1 :

Le bouton « **Expression** » permet d'accéder à un assistant pour créer une règle de filtrage. Une règle de filtrage s'appuie sur les champs des en-têtes (*header*) des protocoles connus du logiciel Wireshark :



En cliquant sur « **Valider** » puis sur « **Apply** », on obtient alors :



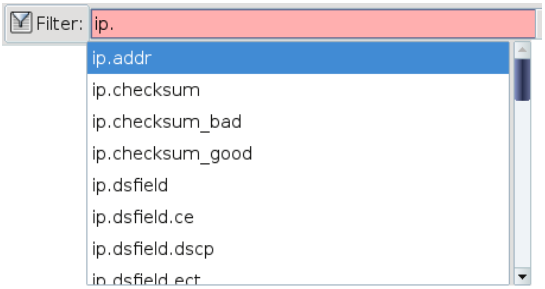
No.	Time	Source	Destination
2	0.911310	65.208.228.223	145.254.160.237
5	1.472116	65.208.228.223	145.254.160.237
6	1.682419	65.208.228.223	145.254.160.237
8	1.812606	65.208.228.223	145.254.160.237
10	2.443513	65.208.228.223	145.254.160.237
11	2.553672	65.208.228.223	145.254.160.237
14	2.633787	65.208.228.223	145.254.160.237
16	2.894161	65.208.228.223	145.254.160.237
17	2.914190	145.253.2.203	145.254.160.237
20	3.374852	65.208.228.223	145.254.160.237
21	3.495025	65.208.228.223	145.254.160.237

On peut créer des règles de filtrage en combinant plusieurs expressions avec des opérateurs && (ET), || (OU) et ! (INVERSEUR), par exemple :

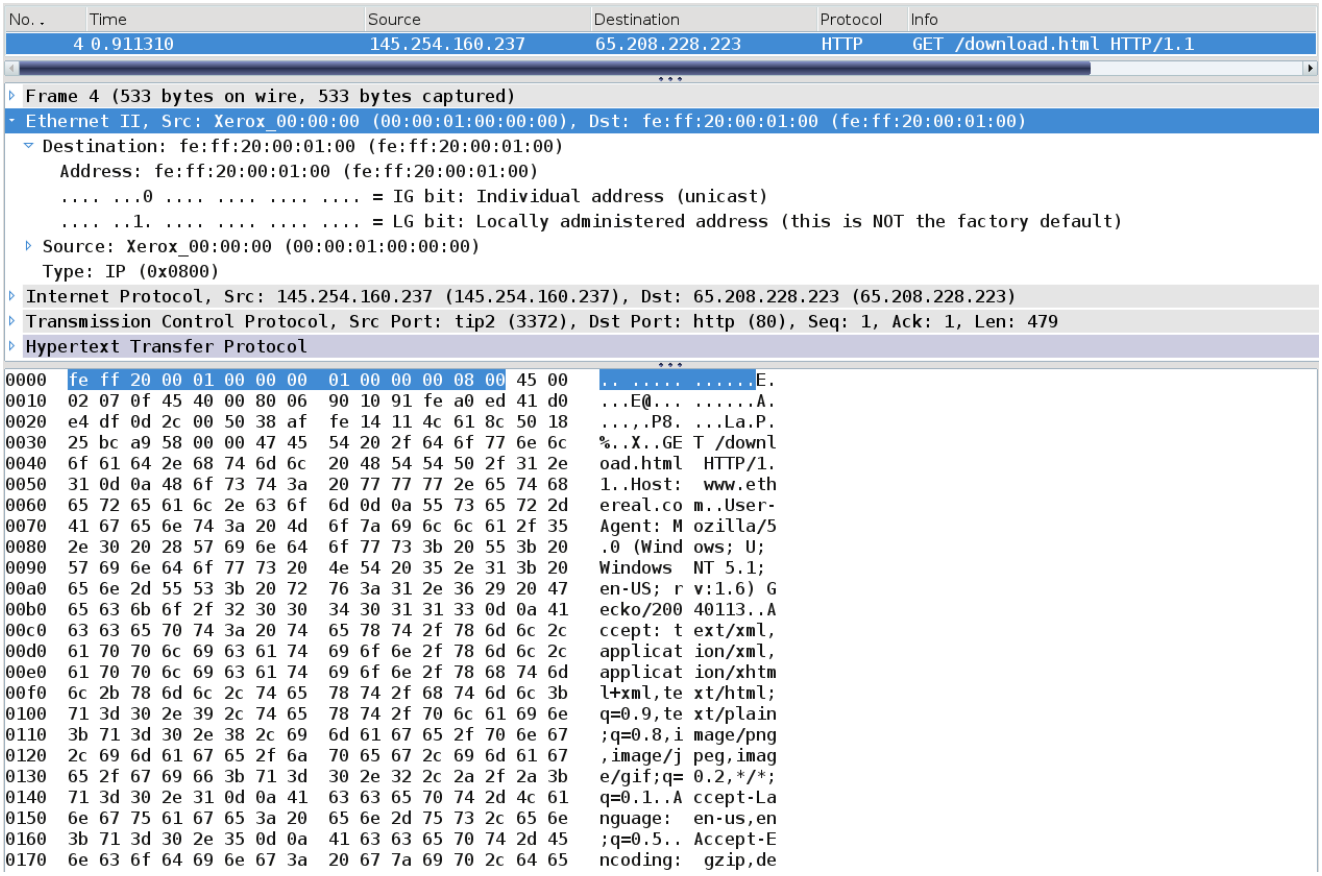
Toutes les trames dont l'adresse ip destination est égale à 145.254.160.237 et dont le port source ou destination n'est pas 80 :

```
ip.dst == 145.254.160.237 && !tcp.port == 80
```

*Remarque : en tapant directement dans la zone de saisie « **Filter** », Wireshark propose une complétion bien pratique.*



On sélectionne la trame n°4 dans le cadre 1. Cette trame encapsule les protocoles visibles dans le cadre 2 :

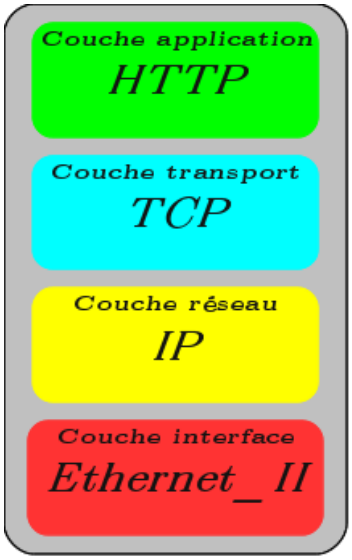


Wireshark est capable de décoder les champs des différents en-tête de protocoles présents dans la trame capturée.

Remarque : mais sans connaissances théoriques, l'utilisation de wireshark s'avère très vite limitée ! C'est un outil de spécialiste. En effet, qu'est-ce qu'une « address unicast » ? « Seq » ? etc . . .

Encapsulation

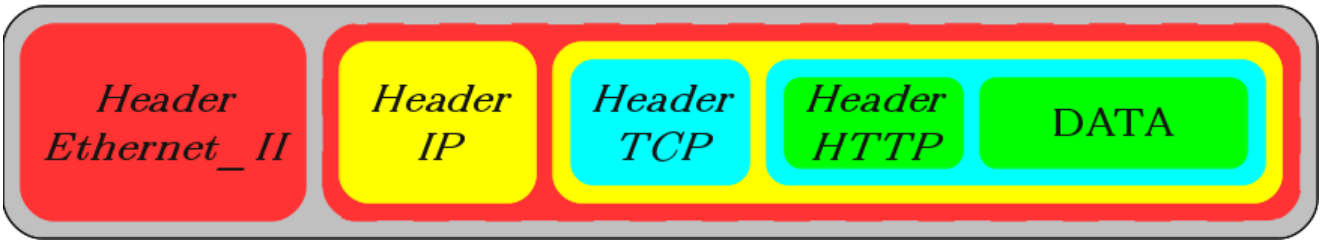
Le cadre 2 illustre le principe de l'encapsulation des protocoles utilisées dans l'échange d'une trame. On fait souvent référence à un modèle pour représenter cette communication. Ici, le modèle est celui qui implémente les protocoles de la famille « TCP/IP » appelée aussi DoD (*Department of Defense*) :



Modèle DoD

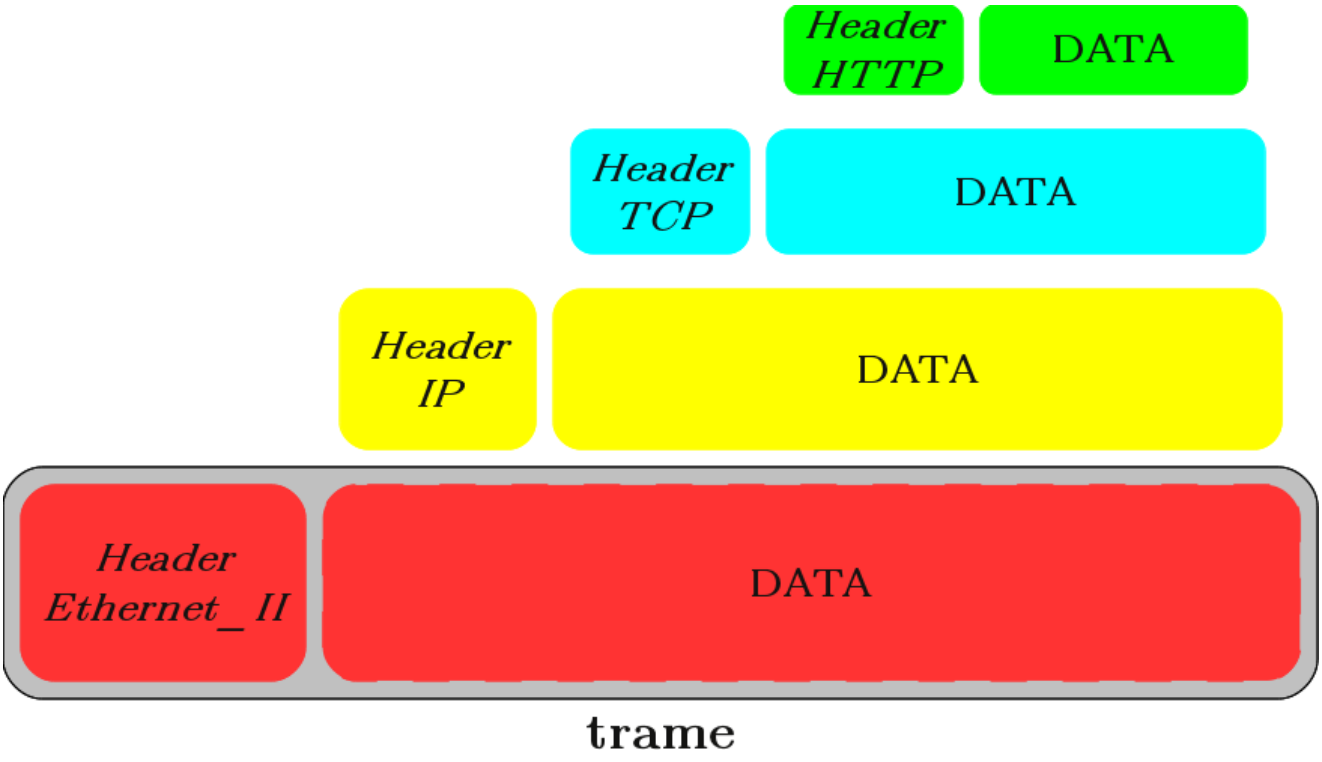
En sachant qu'une couche se décomposera en deux parties comprenant un en-tête (*header*) appelé aussi PCI (*Protocol Control Information*) et un champ DATA (au sens « *network data* »). En fait, cela représente les protocoles présents dans la trame de la manière suivante :

trame



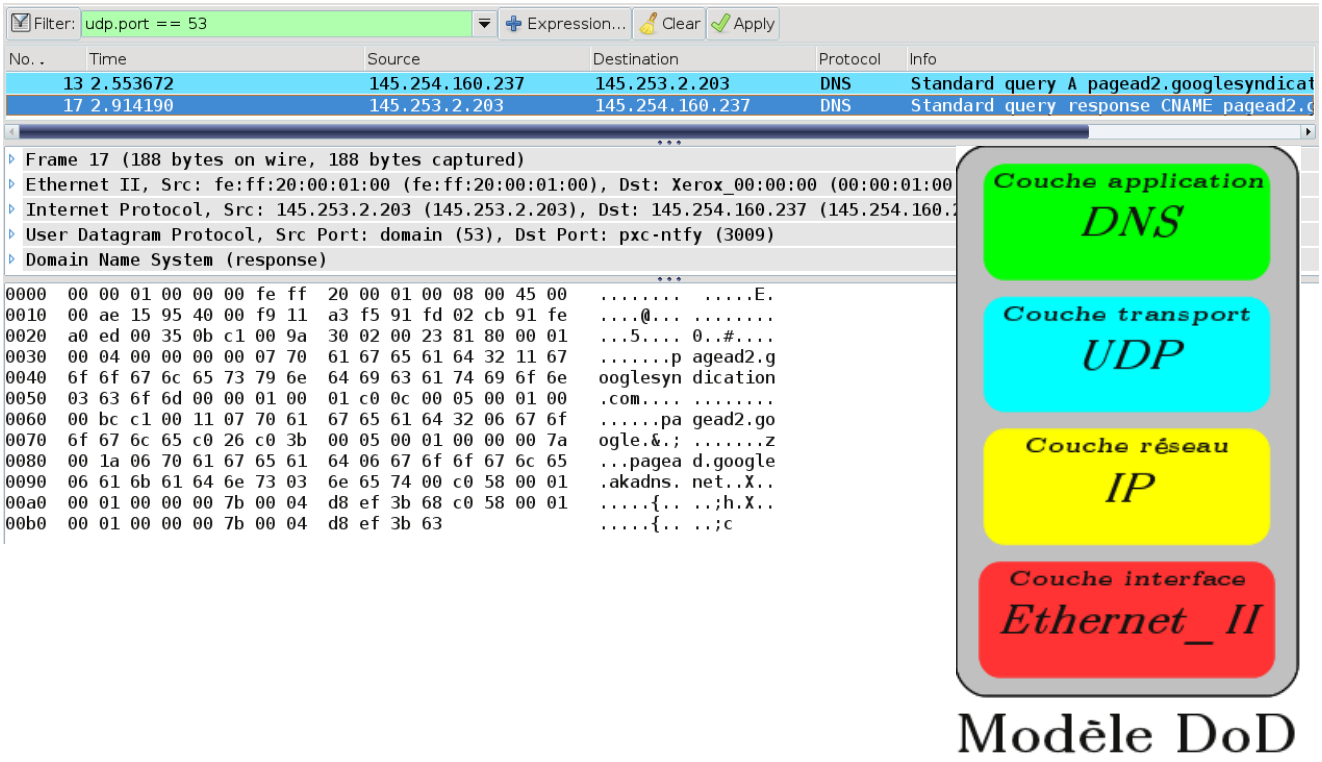
On comprend alors que le champ DATA d'une couche contient le bloc de la couche supérieure (*Header* + DATA). C'est le principe de l'encapsulation.

Une fois le rapprochement fait avec le modèle « TCP/IP », on obtient la « vision suivante » :



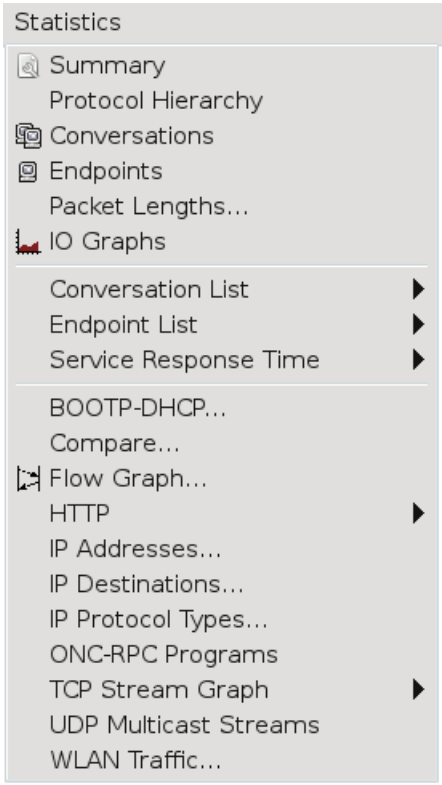
Remarques : certaines couches ou certains champs DATA peuvent être vides. Par exemple, la trame n°1 n'encapsule que les protocoles Ethernet_ II, IP et TCP. La couche application est donc vide.

D'autre part les couches du modèle DoD offre l'utilisation d'autres protocoles. Par exemple, les trames n°13 et 17 encapsulent les protocoles Ethernet_ II, IP, UDP et DNS :



Outils statistiques

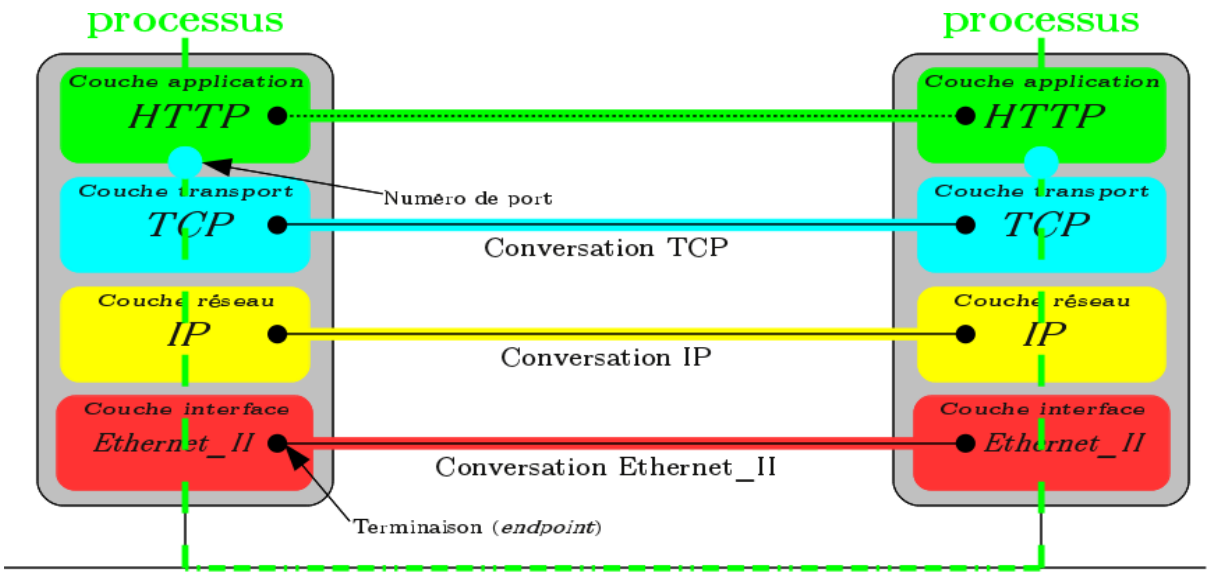
Wireshark fournit des outils pour l'analyse et les statistiques du trafic capturé.



- Summary : statistiques générales sur la capture actuelle
- Protocol Hierarchy : statistiques sur la pile de protocoles utilisé dans l'échange
- Conversations : statistiques des conversations saisies. Une conversation est le trafic entre deux points de terminaison spécifique. Par exemple, une conversation IP est tout le trafic entre deux adresses IP.
- Endpoints : statistiques des points de terminaison. Un point de terminaison réseau est la terminaison logique d'un protocole d'une couche spécifique.

Il y a deux aspects à prendre en compte dans un échange :

- le transfert physique de trames contenant des protocoles encapsulés (fabrication à l'émission et décodage à la réception : parcours vertical du modèle)
- un dialogue logique entre protocole de couche spécifique (dialogue virtuel horizontal entre deux modèles)



ANALYSE DE TRAMES

Ouvrir le fichier `http.cap` disponible sur le serveur ou sur le site http://wiki.wireshark.org/SampleCaptures (HTTP).

Adressage des protocoles dans le modèle Dod

Un protocole utilise des numéros (les *assigned numbers*) identifiant les protocoles de niveau supérieur qu'il transporte.

Sélectionnez une trame transportant des données http.

Le champ de l'en-tête Ethernet identifiant le protocole de niveau réseau est **Type**.

1) Quelle est la valeur de ce champ pour le protocole IP ?

Dans l'en-tête IP, le protocole de niveau transport est identifié par le champ **Protocol**.

2) Quelle est la valeur du champ Protocol pour le protocole TCP ?

Sous Linux seulement, vérifier le numéro de protocole assigné à TCP en consultant le fichier /etc/protocols

```
$ grep 'tcp' /etc/protocols
```

Dans l'en-tête de niveau transport, le nombre identifiant le processus applicatif est appelé **port**. Les processus client et serveur utilisent un numéro de port chacun : le numéro de port du client est généralement choisi par la machine, tandis que le numéro de port des applications exécutées sur le serveur est normalisé.

3) Quel est le numéro de port utilisé par le service HTTP ?

4) Quel est le numéro de port choisi par votre client ?

5) Sur combien d'octets sont codés les numéros de ports en TCP ? Combien de processus simultanés peuvent théoriquement communiqués via TCP sur une machine ?

Sous Linux seulement, vérifier le numéro de port utilisé par le service HTTP en consultant le fichier /etc/services

```
$ grep 'http' /etc/services
```

6) Les en-têtes des protocoles Ethernet_II, IP et TCP sont-ils encodées en ASCII ?

7) L'en-tête du HTTP est-il encodé en ASCII ?

Sélectionnez une trame transportant des données dns.

8) Quelle est la valeur du champ Protocol pour le protocole UDP ?

Sous Linux seulement, vérifier le numéro de protocole assigné à UDP en consultant le fichier /etc/protocols

```
$ grep 'udp' /etc/protocols
```

9) Quel est le numéro de port utilisé par le service DNS ?

Sous Linux seulement, vérifier le service associé par défaut au numéro de port 53 en consultant le fichier /etc/services

```
$ grep '53' /etc/services
```

10) Sur combien d'octets sont codés les numéros de ports en UDP ? Combien de processus simultanés peuvent théoriquement communiqués via UDP sur une machine ?

Étude des statistiques

Sélectionner le menu Summary.

11) Quel est le débit moyen mesuré par Wireshark ?

Sélectionner l'outil Protocol Hierarchy qui permet de visualiser la pile de protocoles, le pourcentage de bande passante consommé par chaque protocole, le débit, à chaque niveau etc.

12) Des deux protocoles de niveau transport utilisés, lequel est prépondérant ?

13) Pour le protocole TCP les valeurs indiquées dans colonnes Packets et End packets diffèrent. Pourquoi la colonne End packets contient-elle moins de paquets ? Est-ce aussi le cas pour le protocole UDP ?

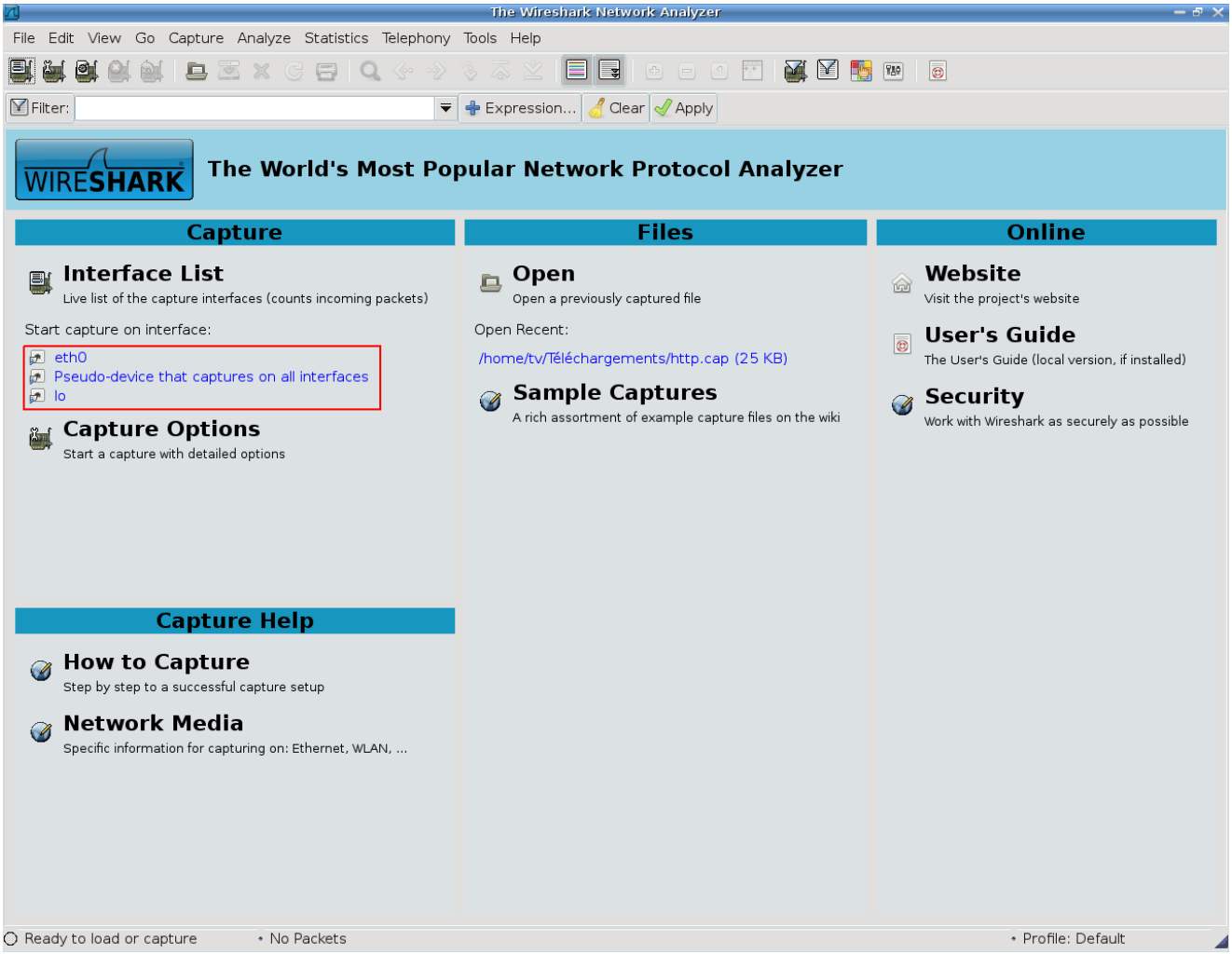
14) À quoi servent les paquets qui ne sont pas comptabilisés dans la colonne End packets ?

15) Pourquoi le débit affiché pour les couches hautes est-il inférieur à celui des couches basses ?

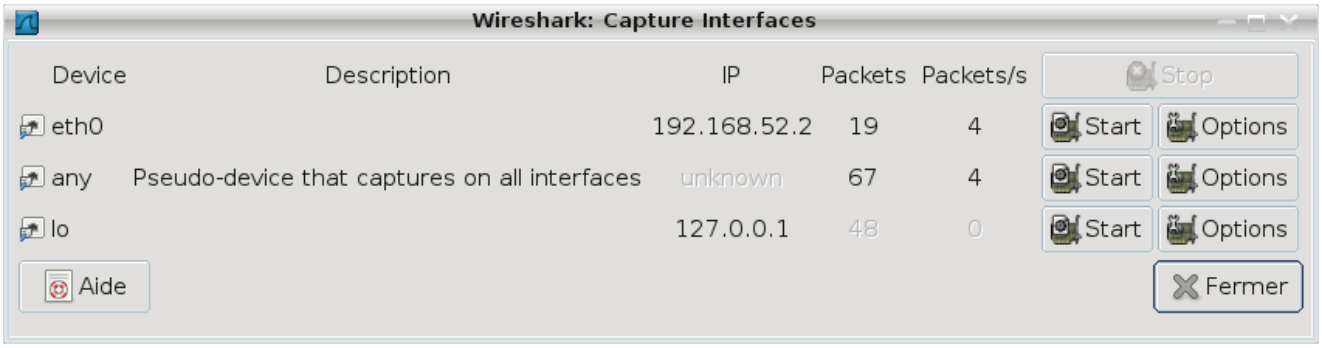
CAPTURE DE TRAMES

Mode super utilisateur

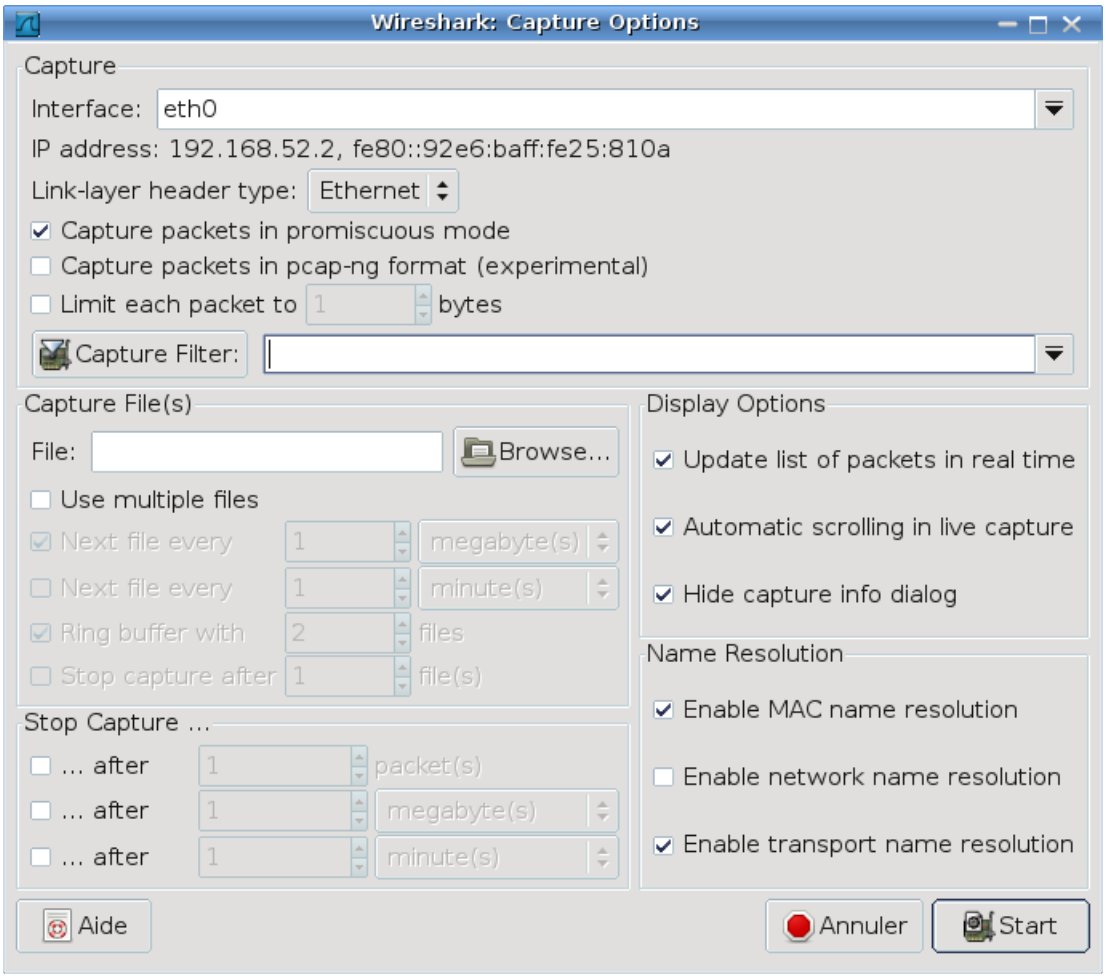
Le logiciel s'ouvre alors sur cette page de menu :



On peut vérifier qu'en cliquant sur « **Interface List** » que l'on possède les droits d'accès sur les interfaces réseaux disponibles pour une capture :



Il existe des options intéressantes avant de démarrer une capture :



- *Update list of packets in real time* : affiche en temps réel à l'écran les trames capturées.
- *Enable MAC name resolution* : affiche le nom de la machine ou son adresse IP à la place de l'adresse MAC.
- *Enable network name resolution* : affiche le nom d'hôte de la machine à la place de l'adresse IP.
- *Enable transport name resolution* : remplace les numéros de port TCP et UDP par le nom du protocole applicatif associé.

Il est évidemment possible de créer des filtres de capture (qui n'enregistrent que les trames conformes à la règle) et d'enregistrer une capture dans un fichier. Il y a aussi des options pour afficher une capture en temps réel.

Remarque : on laissera généralement l'activation du mode promiscuous qui permet à une carte réseau d'accepter tous les paquets qu'elle reçoit, même si ceux-ci ne lui sont pas adressés. Ce mode est une fonctionnalité utilisée pour écouter tout le trafic réseau.

Manipulations

Capturer le trafic d'une communication vers un site Internet que vous n'avez pas consulté depuis le démarrage de votre machine.

Proposer une règle de filtrage pour isoler dans la capture la communication avec ce site Internet.

Vous devez visualiser des paquets DNS de type query et response. Observez le contenu de ces paquets DNS.

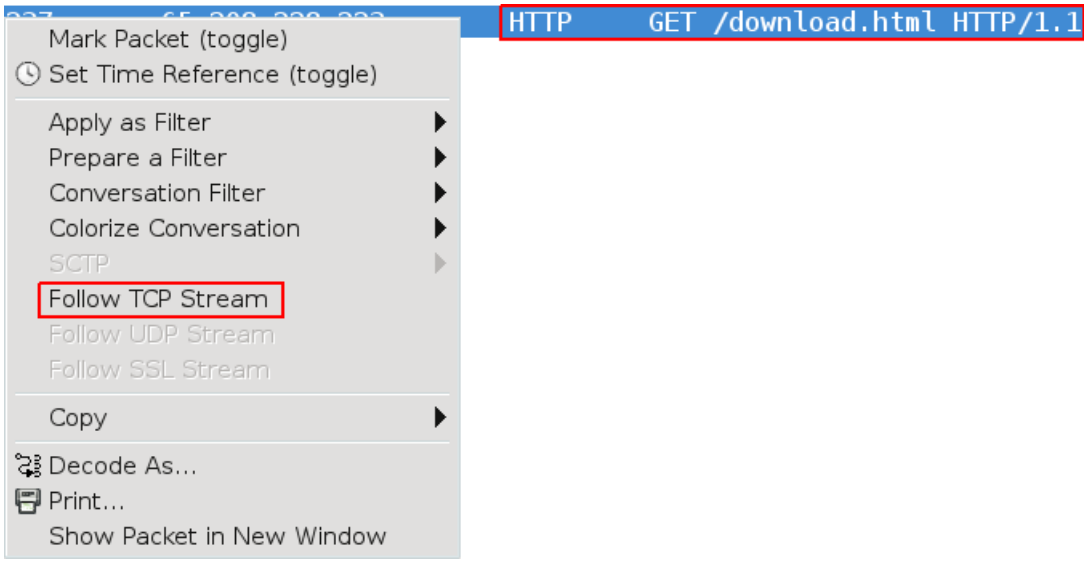
16) Déduisez-en leur rôle.

17) Quelle est l'adresse IP du serveur auquel votre machine a envoyé la requête DNS ?

18) À votre avis, à qui appartient ce serveur ?

19) À votre avis, l'adresse physique destination de la trame Ethernet_II contenant la requête DNS est-elle celle du serveur DNS ? Si non, à qui appartient-elle ?

Sélectionnez une trame contenant l'indication HTTP dans la colonne Info. Avec le bouton droit de la souris, choisissez l'option Follow TCP stream. Le dialogue entre votre navigateur et le serveur web apparaît.



20) Par quelle primitive commence la requête HTTP ?

21) Quelle version du protocole HTTP est utilisée par votre navigateur ?

22) La requête HTTP émise par le navigateur contient-elle des données ?

23) Quelle est la version du protocole HTTP utilisée par le serveur dans sa réponse ?

24) Quelle est le type de données renvoyées par le serveur ?

25) A votre avis, quel code réponse aurait renvoyé le serveur si le document demandé dans la requête était introuvable ? Tester avec un document inexistant.

Remarque : lorsque vous fermez la fenêtre ouverte par cette option, il reste un filtre d'affichage : il faut l'effacer en cliquant sur clear.

26) Enregistrer la capture réalisée dans un fichier `capture_votreNom` **au format Wireshark/tcpdump.**

Vous m'enverrait votre compte-rendu (réponses aux questions en précisant leur numéro) au **format txt ou rtf** (aucun autre format accepté) ainsi que le fichier de capture à cette adresse : tvaira@free.fr.