TP Réseau N°2 - MMI 1

Ce TP permet de visualiser très précisément le contenu des trames circulant sur un réseau de type ethernet. Grâce à l'outil de capture wireshark. Avant de d'utiliser cet outil, une rapide introduction au branchement physique des machines.

Quel matériel utiliser ?

Les PC sont reliés au niveau 2 de la couche OSI, c'est à dire la couche liaison grâce à un équipement spécifique. Quel matériel peut on utiliser dans ce cas ? (cochez la bonne réponse):

☐ Switch

☐ Hub

☐ Gateway

☐ Routeur

Raccordement matériel

Regardez derrière la tour de votre PC. Identifiez le connecteur réseau. Tous les PC sont reliés à un matériel spécifique (voir ci-dessus) grâce à un câble de type…

☐ RJ11

☐ RJ45

☐ Coaxial

Est-ce un câble :

☐ droit

☐ croisé

Comment les distinguer ?

-

Grâce à la commande `dmesg | grep eth0`, quelles informations obtenez vous à propos de la liaison avec le matériel spécifique ? Vitesse, négociation .. etc.

-

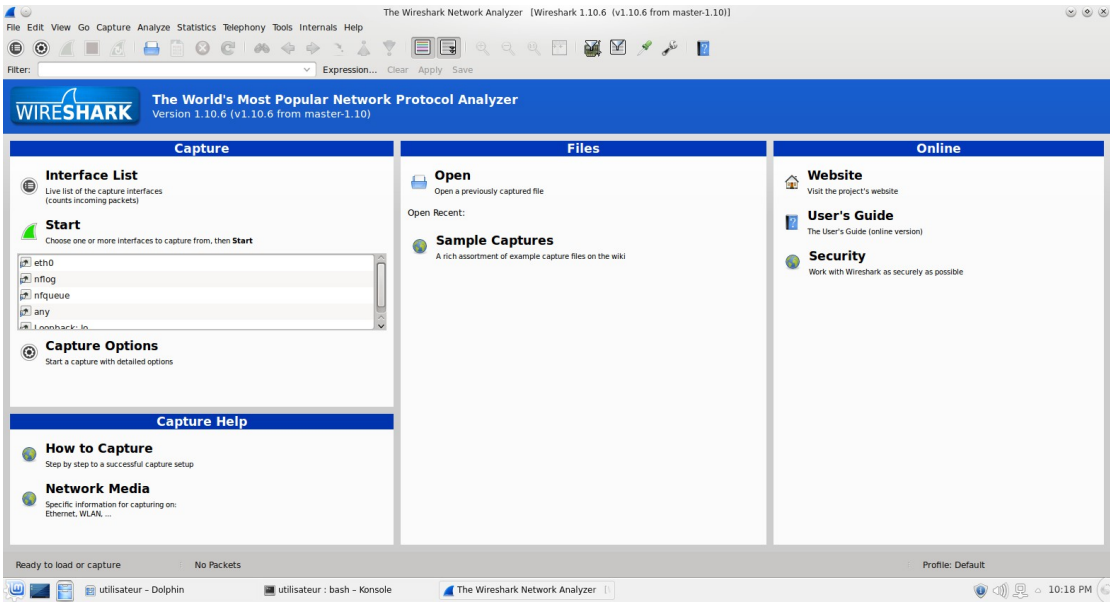
Présentation de wireshark

Wireshark est un outil qui permet de 'sniffer' les trames circulant sur le réseau. Avant de commencer, tapez les deux commandes suivantes :

sudo groupadd wireshark

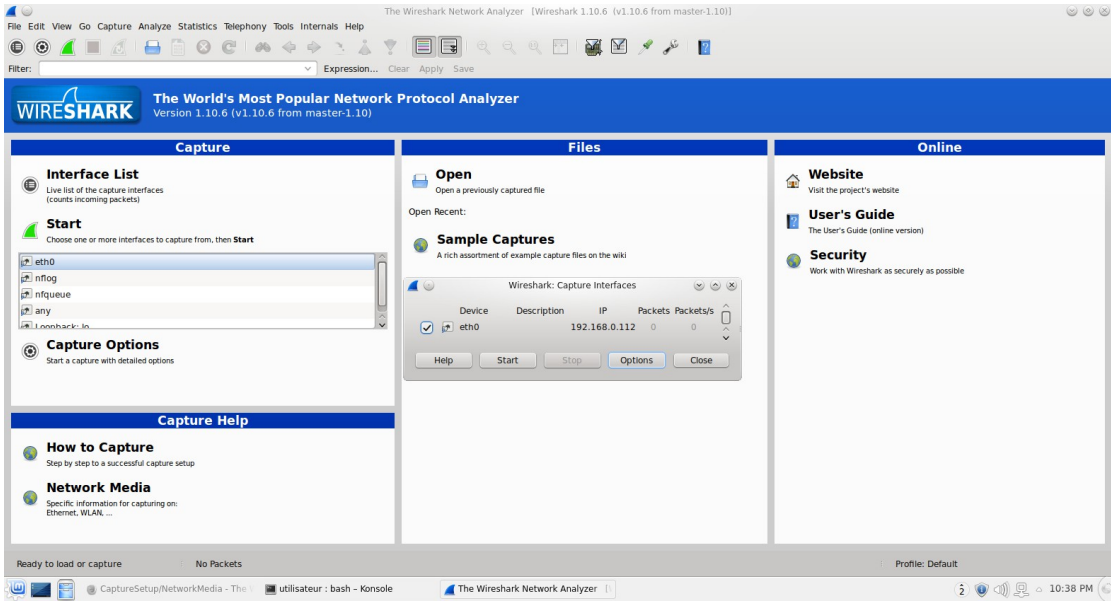
sudo adduser $USER wireshark

Fermez la session, puis ouvrez-la de nouveau. Dans le menu, ouvrez la catégorie 'Internet' et lancez wireshark. La fenêtre principale apparaît :

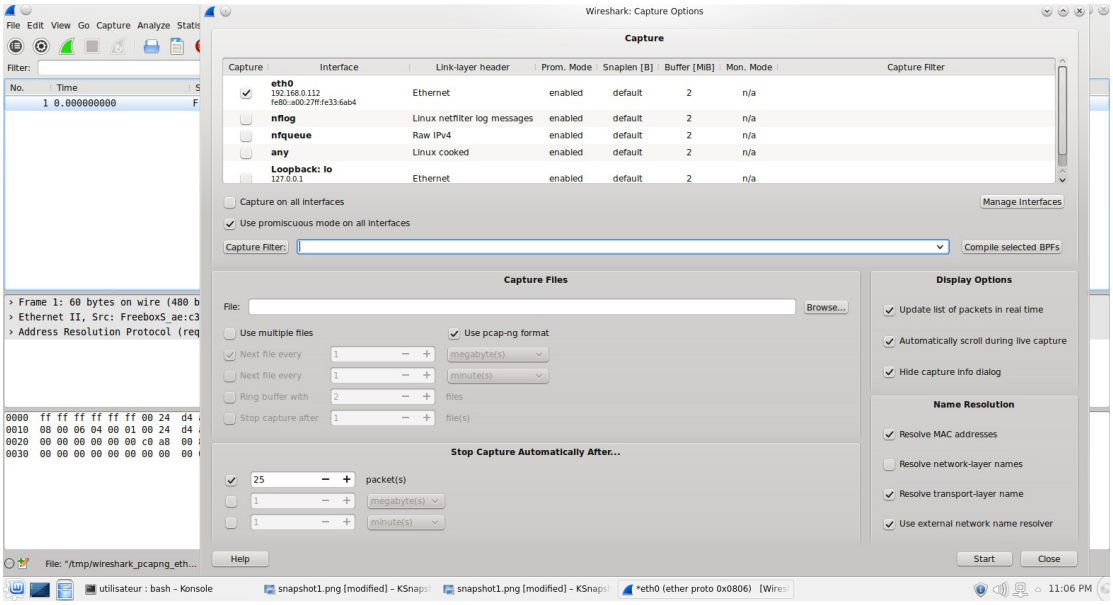


Pour effectuer une capture, suivez ces 5 étapes :

1) Cliquez sur 'Interface List', vous allez choisir de capturer le trafic sur une ou plusieurs interfaces : cochez la case correspondante.



2) …. et cliquez sur 'option'.



3) La ligne Capture Filter, permet de préciser un filtrage 'à priori'. Voici 4 exemples :

a) `ip` : en spécifiant le protocole réseau à analyser, on évite la capture des trames des autres protocoles de niveau réseau (IPX) et des protocoles de niveau liaison (STP, CDP, etc.).

b) `host 192.168.0.1` : en spécifiant l'adresse IP d'un hôte, on ne retient que le trafic émis et reçu par cette adresse.

c) `host 192.168.0.1` and `host 10.0.0.1` : en spécifiant les adresses IP de 2 hôtes, on ne retient que le trafic entre ces 2 adresses.

d) `ip and dst host 192.168.0.2` : capture le trafic ip à destination de la machine d'adresse IP `192.168.0.2`

D'une façon plus générale, on peut combiner plusieurs critères avec les opérateurs logiques `and` et/ou `or`.

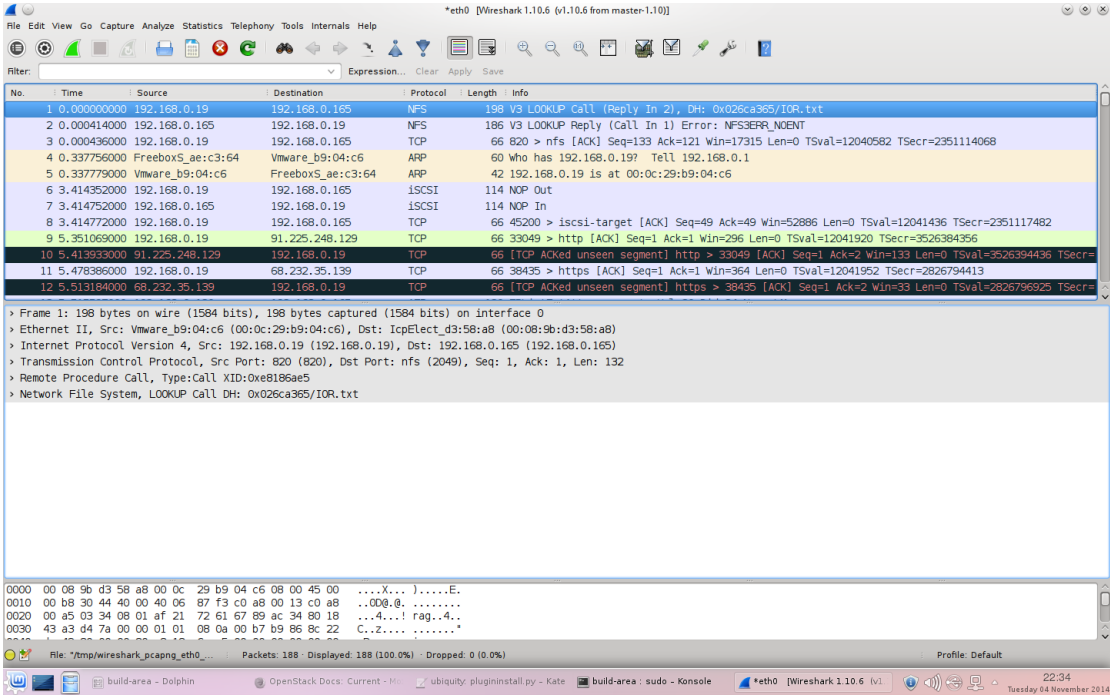
le type : `host, net` et `port`.

la direction : `src` et `dst`.

le protocole : `ether, fddi, tr, ip, ip6, arp, rarp, decnet, tcp` et `udp`.

4) La rubrique 'Stop Capture' permet comme son nom l'indique d'établir des conditions d'arrêt (nombre de paquets et/ou durée...)

5) Cliquez sur le bouton 'Start'



Un écran détaillant la capture apparaît. La barre filter, permet le filtrage 'à postériori'.

En dessous, on trouve la fenêtre contenant la liste des trames capturées, sur chaque ligne on retrouve :

- le numéro du paquet

- le timing de capture

- la source

- la destination

- le protocole de plus haut niveau identifié

- la taille du paquet en octets

- une traduction à peu près humainement compréhensible du paquet considéré

Plus bas, une zone de détail du paquet sélectionné, et enfin la dernière zone affiche le paquet en hexadécimal.

Exercices

1) Lancez une capture des échanges ARP, de 20 paquets. Indiquez le filtre utilisé :

-

2) Lancer une capture en ne capturant que les paquets en provenance et à destination de votre machine. Indiquez le filtre utilisé :

-

3) Lancez un ping continu de la machine de votre voisin de droite. Trouvez grâce au manuel le type de protocole à capturer, et établissez le filtre correspondant.

-

4) Ouvrez firefox et identifiez vous afin de pouvoir surfer sur le net. Etablissez un filtre afin de capturer uniquement le trafic HTTP émis et reçu depuis www.akatone.com (208.92.233.240)

Tapez l'adresse suivante dans firefox :

http://www.akatone.com/MMI

Stoppez la capture.

Chaque couche dans cet exemple utilise des numéros identifiant les protocoles de niveau supérieur qu'il transporte.

Sélectionnez une trame transportant des données HTTP.

Le champ de l'entête Ethernet identifiant le protocole de niveau réseau est *Type*.

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

-

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

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

-

Note	Vérifiez le numéro de protocole assigné à TCP en consultant le fichier /etc/protocols

Dans l'entête 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 de manière aléatoire, tandis que le numéro de port des applications exécutées sur le serveur est normalisé.

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

-

Note	Vérifiez le numéro de protocole assigné à HTTP en consultant le fichier /etc/services

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

-

9) Sur combien d'octets sont codés les numéros de ports en TCP ?

-

10) Combien de processus simultanés peuvent théoriquement communiquer via TCP sur une machine ?

-

11) Par quelle primitive commence la requête HTTP ?

-

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

-

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

-

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

-

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

-

Dans le menu Analyze, sélectionnez 'Follow TCP stream'. Une nouvelle fenêtre s'ouvre.

16) Que contient-elle ?

-

Sélectionnez le menu Summary.

17) Quel est le débit moyen mesuré par Wireshark ?

-

Note	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.

Le code de retour envoyé par le serveur est 200 : OK.

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

-

Arrêtez et fermez la capture actuelle. Démarrez une nouvelle capture en établissant un filtre afin de capturer le trafic DNS. (Indice : cherchez le numéro de port à capturer dans /etc/services...)

-

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

-

20) Sur combien d'octets sont codés les numéros de ports en UDP ?

-

21) Combien de processus simultanés peuvent théoriquement communiquer via UDP sur une machine ?

-

Sélectionnez le menu Summary.

22) Quel est le débit moyen mesuré par Wireshark ?

-

23) Des deux protocoles de niveau transport utilisés, lequel est le plus rapide ? Le plus fiable ?Argumentez votre réponse.

-