2ème année *Génie Informatique* 31/10/2013
Génie Réseaux & Télécom *Pr. KHAMLICHI*

TP 3 : Réseaux – WireShark

Objectifs pédagogiques

Expliquer l'objectif d'un analyseur de protocoles (Wireshark)
Exécuter une capture de base des unités de données de protocole (PDU) à l'aide de Wireshark
Exécuter une analyse de base des PDU sur un trafic de données réseau simple
Se familiariser aux fonctionnalités et options de Wireshark telles que la capture des PDU et le filtrage de l'affichage

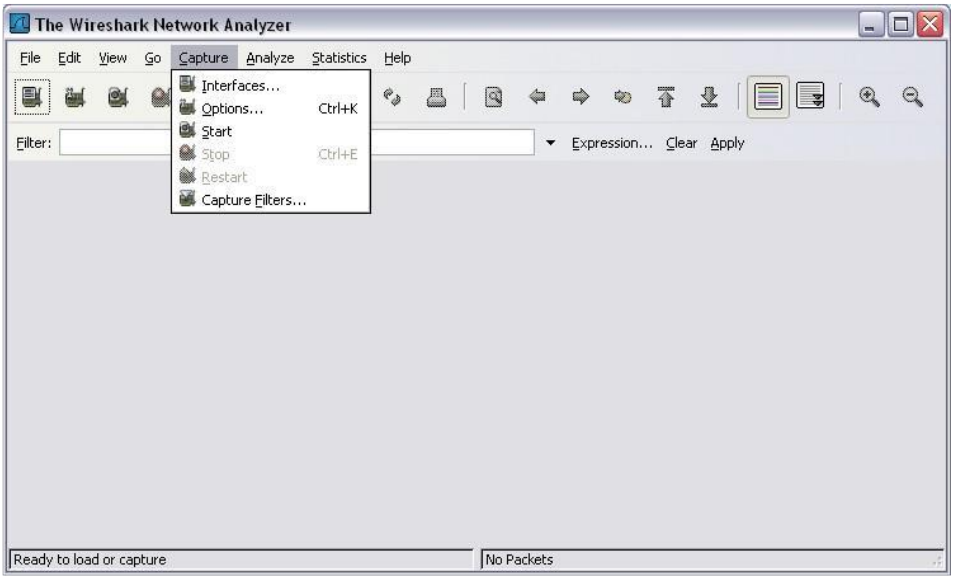
Contexte

Wireshark est un analyseur de protocoles (analyseur de paquets) utilisé pour dépanner les réseaux, effectuer des analyses, développer des logiciels et des protocoles et s'informer. Avant juin 2006, Wireshark répondait au nom d'Ethereal. Un analyseur de paquets (ou analyseur de réseaux ou de protocoles) est un logiciel permettant d'intercepter et de consigner le trafic des données transférées sur un réseau de données. L'analyseur « capture » chaque PDU des flux de données circulant sur le réseau. Il permet de décoder et d'analyser leur contenu conformément aux spécifications RFC ou autres appropriées. Wireshark est programmé pour reconnaître la structure de différents protocoles réseau. Vous pouvez l'utiliser pour afficher l'encapsulation et les champs spécifiques aux PDU, puis interpréter leur signification.

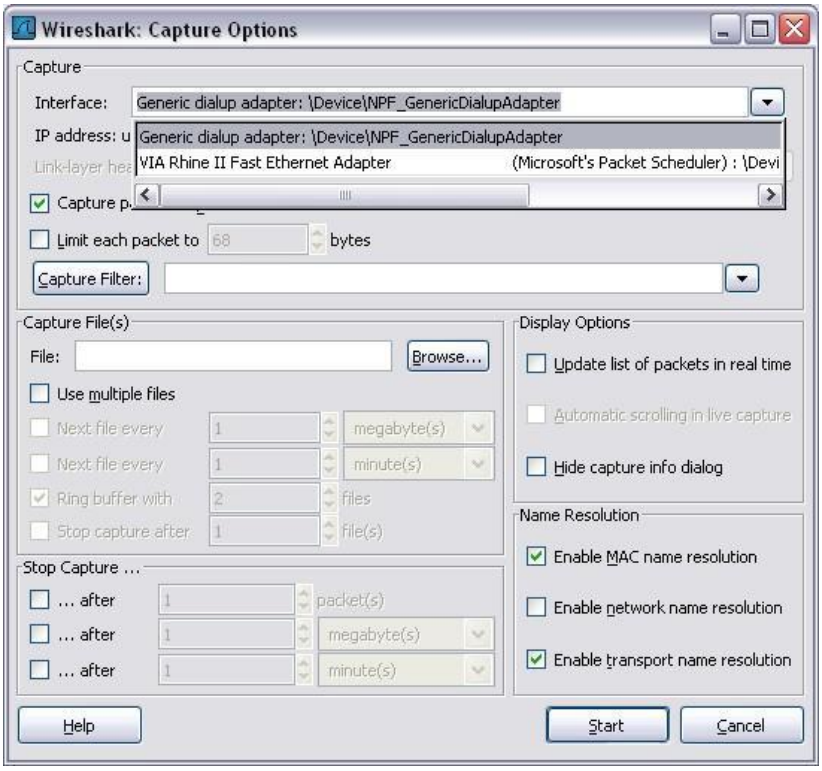
Pour en savoir plus sur cet analyseur et télécharger le programme correspondant, accédez au site http://www.Wireshark.org

Scénario

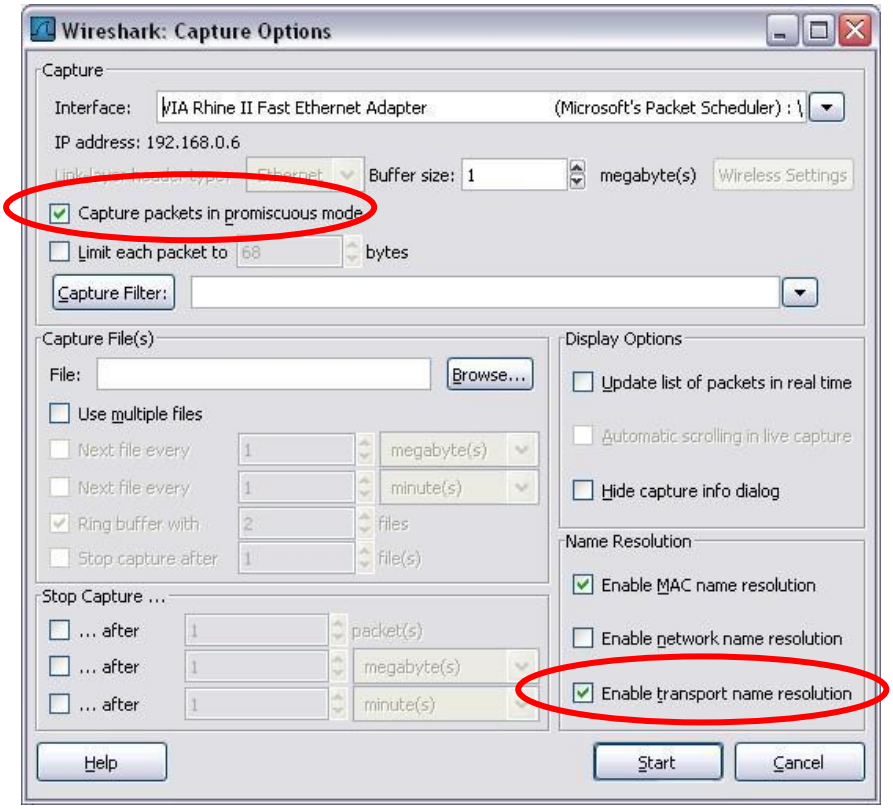
Pour pouvoir capturer des données, vous devez d'abord vous connecter au réseau depuis l'ordinateur sur lequel Wireshark est installé et exécuter Wireshark.



Pour lancer la capture des données, sélectionnez d'abord l'élément Options dans le menu Capture. La boîte de dialogue Options comprend tout un ensemble de paramètres et de filtres déterminant le trafic de données capturé et le mode de capture utilisé.



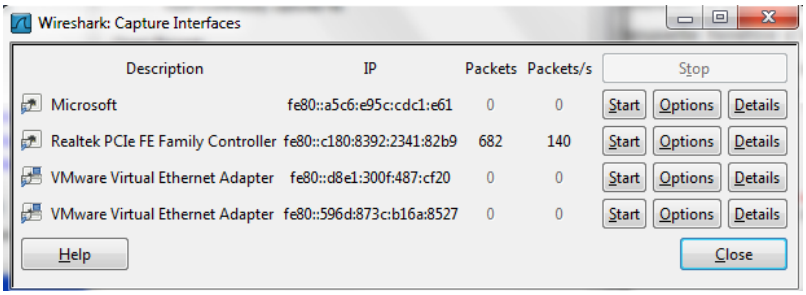
Vous devez commencer par vous assurer que Wireshark est configuré pour l'interface appropriée. Dans la liste déroulante Interface, sélectionnez la carte réseau utilisée. Pour un ordinateur, il s'agit généralement de la carte Ethernet connectée. Vous pouvez ensuite définir les Capture options. Examinez les deux options mises en relief ci-dessous.



Configuration de Wireshark permettant de capturer des paquets en mode de proximité

Si vous ne sélectionnez pas l'option Capture packets in promiscious mode, seules les PDU destinées à l'ordinateur sont capturées. Si vous la sélectionnez, toutes les PDU destinées à l'ordinateur et toutes celles détectées par la carte réseau de l'ordinateur sur le même segment de réseau (c'est-à-dire les PDU transitant par la carte réseau non destinées à l'ordinateur) sont capturées. Remarque : la capture de ces PDU supplémentaires dépend du périphérique utilisé pour connecter les ordinateurs finaux sur le réseau. Les résultats d'analyse Wireshark varient en fonction des différents périphériques (concentrateurs, commutateurs, routeurs) utilisés au cours de la formation. Configuration de Wireshark permettant de résoudre les noms réseau Utilisez l'option Enable... name resolution pour indiquer si Wireshark doit convertir les adresses réseau détectées dans les PDU en noms. Bien que cette fonction soit utile, notez que le processus de résolution des noms risque d'ajouter des PDU aux données capturées et ainsi peut-être de fausser l'analyse. Un certain nombre d'autres paramètres de filtrage et processus de capture sont également disponibles.

Pour réaliser une capture, il est nécessaire de sélectionner d'abord une interface réseau. Allez dans le menu "Capture" et choisissez "Interfaces". Une nouvelle fenêtre s'ouvre et vous présente l'ensemble des interfaces réseau de l'ordinateur. Choisissez celle qui est active (celle qui possède l'adresse IP que vous avez spécifiée) en cliquant sur le bouton "start".



Exercice 1 : Capture de paquets TCP avec Wireshark

Exécutez WireShark sur chaque machine et démarrez une capture sur l'interface réseau active.

1- Que se passe-t-il lorsque si on exécute une commande ping sur une autre machine ? Et si une machine distante exécute la commande ping sur une autre machine ?
   a. Quel protocole est utilisé avec la commande ping ?
   b. Quel est le nom complet du protocole ?
   c. Quels sont les noms des deux messages ping ?
2- Ouvrez un navigateur Web et accéder à l'adresse suivante : "http://localhost"
3- Observez les paquets capturés
   a. Identifier l'ouverture d'une connexion TCP avec le serveur Apache
      i. Quels sont les numéros de séquences initiaux utilisés ?
      ii. quels sont les ports utilises du côté serveur et du côté client ?
   b. Combien de segments TCP sont envoyés ? Quelles sont leurs tailles ?
   c. Identifier les valeurs de taille de fenêtre TCP utilisées.

Exercice 2 : Capture de paquets UDP/ICMP

1- Redémarrer la capture de paquets avec WireShark
2- Utiliser l'outil en ligne de commande « traceroute » avec « localhost » comme destination
3- Observer les paquets capturés
   a. Identifier les paquets UDP et/ou ICMP utilisés par Traceroute

b. quel est le port de destination des sondes UDP ?
c. quel est le type des messages ICMP échangés ?

4- Utiliser l'outil en ligne de commande « ping » avec « localhost » comme destination
5- Observer les paquets capturés
   a. Identifier les paquets utilisés par Ping.
   b. Quels sont les types de message ICMP échangés ?

Exercice 3 : Etude de DHCP

L'objectif de cette partie est d'étudier Arp et DHCP dans WireShark

- Effacer toutes les entrées de la table arp (arp -d x.x.x.x), sur un PC voisin, après avoir lancé une capture WireShark chez vous, demandez à vos collègues d'arrêter et de redémarrer les fonctions réseau (ifdown eth0 ; ifup eth0).
- En fonction de la trace WireShark, décrire en détails le protocole DHCP. Sur quel protocole s'appuie-t-il ? Quelles informations sont-elles transmises, par qui, dans quel ordre ?

Exercice 4 : utilisation des outils « satistics »

Analyse en utilisant « fow graphs »

- Effacez la table ARP, lancez une capture et lancez une session http (web). Après capture, donnez le détail de tous les protocoles utilisés au cours de l'échange via l'outil «flow graphs»

Analyse du trafic

- Faites une capture sur 5 minutes, en générant le plus de trafic différencié possible. Utilisez l'outil IO Graphs avec différents filtrages et indiquez les trafics captés.
- Sur la même capture, utilisez les outils Conversation, Endpoints, et protocol hierarchy. En fonction des résultats, faites un bilan complet avec, d'une part, l'analyse du trafic, et d'autre part, les indications sur les niveaux de protocoles utilisés.