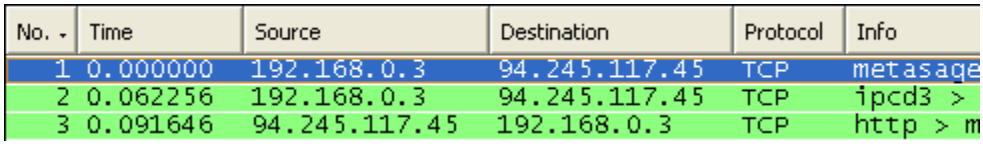
1. Introduction

Une information va circuler entre deux ordinateurs : un fichier par exemple.
Ce fichier va circuler sous forme d'un "train d'informations". On trouvera différents wagons, chacun ayant un rôle bien particulier. Un de ces wagons transportera le fichier, mais on trouvera d'autres wagons nécessaires au bon transport de l'information.
Une trame est tout simplement le nom technique de ce "train" d'informations.
"**Wireshark**" est un logiciel qui va nous permettre de visualiser ces trames, ces trains d'informations. C'est un analyseur de trames open-source.

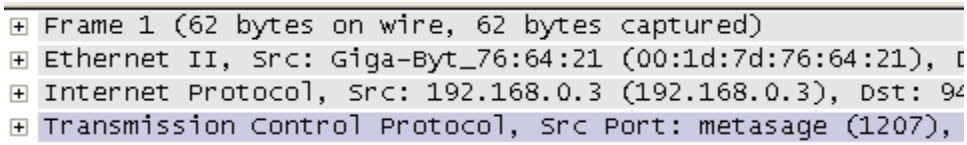
2. Capturer des trames

Dans "Wireshark", aller dans Menu \ Captures \ Interfaces. On voit alors les différentes cartes réseaux de votre machine.
Les ordinateurs ont souvent plusieurs cartes réseaux. Il faut commencer par trouver celle qui est active, qui est réellement utilisée.
Il suffit, pour cela, de prendre la carte qui reçoit et / ou envoie des "paquets" (nous dirons, pour l'instant, que "paquet" est très voisin de "trame").
Pour gagner un peu de temps, forcer le poste à émettre ou recevoir: surfer simplement sur Internet.
Une fois la carte choisie, il suffit, pour capturer, de cliquer sur "Start".
On trouve alors trois zones:
- zone 1: les trames capturées.
On a ici trois trames. La première est en bleu, c'est celle qui est sélectionnée.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.3	94.245.117.45	TCP	metasage
2	0.062256	192.168.0.3	94.245.117.45	TCP	ipcd3 >
3	0.091646	94.245.117.45	192.168.0.3	TCP	http > m

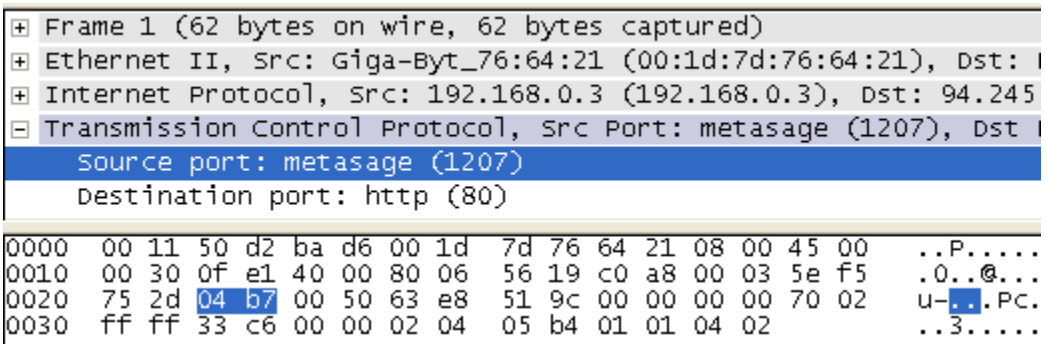
- zone 2: on voit ici les détails de la trame capturée.



```
⊞ Frame 1 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: Giga-Byt_76:64:21 (00:1d:7d:76:64:21), D
⊞ Internet Protocol, Src: 192.168.0.3 (192.168.0.3), Dst: 94
⊞ Transmission Control Protocol, Src Port: metasage (1207),
```

- zone 3: on voit ici encore plus de détails de la trame capturée.

Par exemple, ici: dans la zone 2, j'ai cliqué sur la valeur "Source port", qui vaut, en zone 2, "1207(10)". C'est une valeur décimale.
Si on regarde en zone 3, on voit que ce "1207(10)", est, en réalité, codé par "04 b7(hex)", et que les caractères qui correspondent sont deux points ("04(hex)" ne correspond à aucun caractère comme "A", "B", etc.).



Rassurez-vous, vous utiliserez principalement les zones 1 et 2.

3. Capturer une requête de ping

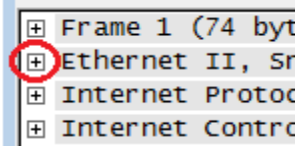
Sur votre poste Windows, passer en mode commande : Démarrer \ Rechercher les programmes et fichiers \ Saisir "cmd" (sans les ") \ "Entrée".
Dans la fenêtre obtenue consulter la configuration IP de la machine: "ipconfig".
L'adresse IP de ma machine est ……..
Noter l'adresse IP du poste voisin ("192.168.27.42" par exemple).
Vérifier, sur votre machine et celle du voisin, que le firewall est désactivé: Panneau de configuration \ Pare-feu Windows \ Activer ou désactiver le pare-feu Windows.
En mode commande, préparer un ping du poste voisin: "ping 192.168.20.42" par exemple (sans les "). Ne pas faire "Entrée" pour l'instant.
Lancer une capture de trames.
Dans la console où le ping a été préparé, lancer le ping. Une fois le ping terminé, arrêter la capture.

Exercice 1 : Analyse de la requête de ping

Avant d'analyser la capture, il nous manque une dernière information. En mode console, récupérer l'adresse MAC physique de votre machine: "ipconfig /all".
L'adresse MAC de ma machine est : ……..
Sélectionner la première trame de type "Info = Echo (ping) request" (et non pas "reply"):

Source	Destination	Protocol	Info
192.168.56.1	192.168.56.2	ICMP	Echo (ping) request
192.168.56.2	192.168.56.1	ICMP	Echo (ping) reply
192.168.56.1	192.168.56.2	ICMP	Echo (ping) request
192.168.56.2	192.168.56.1	ICMP	Echo (ping) reply

En zone 2, cliquer sur la croix pour voir le détail de la ligne "Ethernet":



Vérifier alors que :
- "Source" correspond à votre adresse MAC physique,
-"Destination" correspond à l'adresse MAC physique du poste cible du ping.

Réaliser la même opération afin de consulter le détail de la ligne "Internet Protocol":
Vérifier alors que :

- "Source" correspond à votre adresse IP,
- "Destination" correspond à l'adresse IP du poste cible du ping.

Consulter maintenant le détail de la ligne "Internet Control Message Protocol"(ICMP).
Vous êtes en train de consulter en détail une trame "Info = Echo (ping) request".
Vérifier que vous avez bien ici "Type: 8 (Echo (ping) request)".

	Adresse MAC physique		**Adresse IP**		**ICMP (Request/ Reply)**
	Source	Destination	Source	Destination	
Trame "Echo request" Ping aller					

Sur quel type de codage (du système de numération) est codée l'adresse MAC physique ?
Sur combien d'octets est codée l'adresse MAC physique ?
À quoi correspondent les trois premiers octets ?
Et les autres octets ?
Sur le site http://standards.ieee.org/develop/regauth/oui/public.html, saisir les trois premiers octets dans la zone de recherche comme indiqué ci-dessous

Quelles informations supplémentaires avez-vous reçues ?

Étudier maintenant une trame "Info = Echo (ping) reply", puis finir de compléter le tableau ci-dessus.

	Adresse MAC physique		**Adresse IP**		**ICMP (Request/ Reply)**
	Source	Destination	Source	Destination	
Trame "Echo reply" Ping retour					

Réaliser la même opération avec un autre poste :
- ping du poste avec capture de trames,

- étude des trames et remplissage du tableau.
Quelles sont les différences entre les deux tableaux ?

Exercice 2 :Analyse ARP et ICMP

En vous aidant des commandes ***arp*** et ***ping*** :

1. . Consultez et videz la table (cache) ARP de votre machine.
2. Mettez en route une capture de trame avec Wireshark et lancez un ***ping*** vers la Machine voisine en ne générant qu'un seul paquet de demande d'écho. Pour avoir une vision plus claire des résultats de la capture, il est préférable de créer un filtre sur les protocoles ARP et ICMP.
3. Analysez le format d'un message ARP et retrouvez les différents champs en précisant Leur rôle.
4. Retracez un échange ARP en précisant les adresses Ethernet et IP utilisées à chaque étape.
5. Analysez le format d'un message ICMP et retrouvez les différents champs en précisant leur rôle.
6. Comparez les données des messages *ICMP Echo Request* et *ICMP Echo Reply ;* que constatez-vous ? Quel est le contenu de ces champs de données ?
7. Les protocoles ARP et ICMP sont chacun des protocoles indispensables à la couche 3, cependant ils utilisent un empilement protocolaire différent : expliquez cette différence.

Exercice 3 : Analyse du DHCP

Lancez Wireshark, et redemandez une adresse IP pour votre carte NIC.
Arrêtez la capture.

1. Est ce que les messages DHCP utilisent UDP ou TCP ?
2. Dessinez un diagramme temporel pour les quatre premiers messages ((Discover/Offer/Request/ACK) échangés entre le client et serveur DHCP ? Pour chaque paquet indiquez le port source et destination ?
3. Quelles sont les adresses IP source et destination utilisées dans le DHCP Discover et Request ?
4. Quelles valeurs dans le DHCP Discover permettent de le différentier du message DHCP Request ?
5. Quelle est l'adresse du serveur DHCP ?
6. Quelle est l'adresse IP que le serveur DHCP offre à votre machine ? Indiquez quel Message DHCP contient l'adresse offerte ?