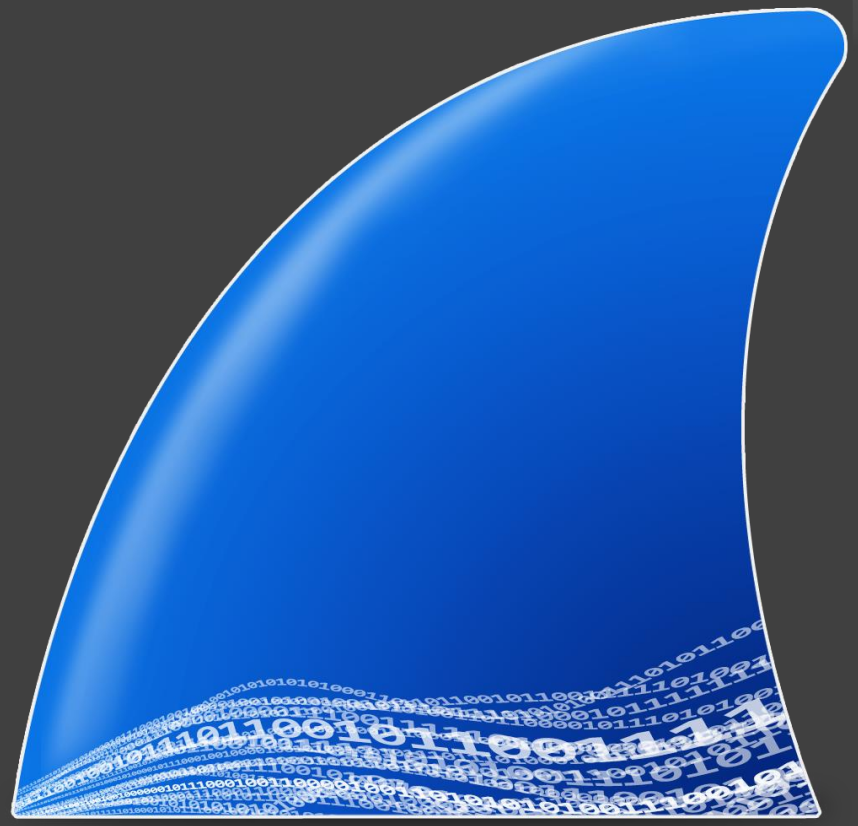
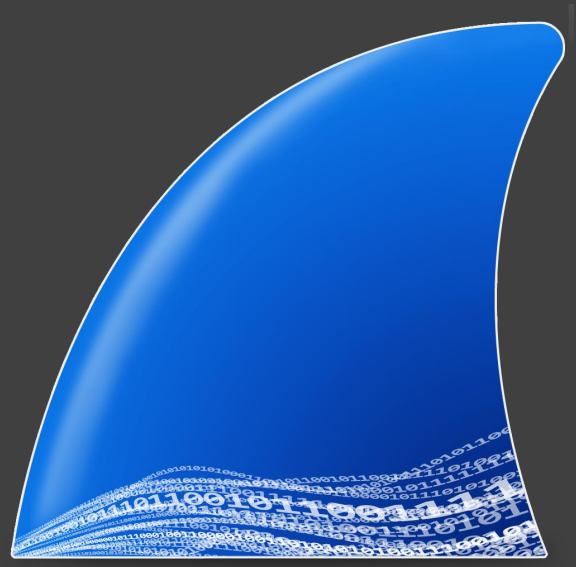


TP WIRESHARK

Téléchargement de Wireshark

1-Télécharger Wireshark sur le site: http://www.wireshark.org/download.html

2-Puis installez le



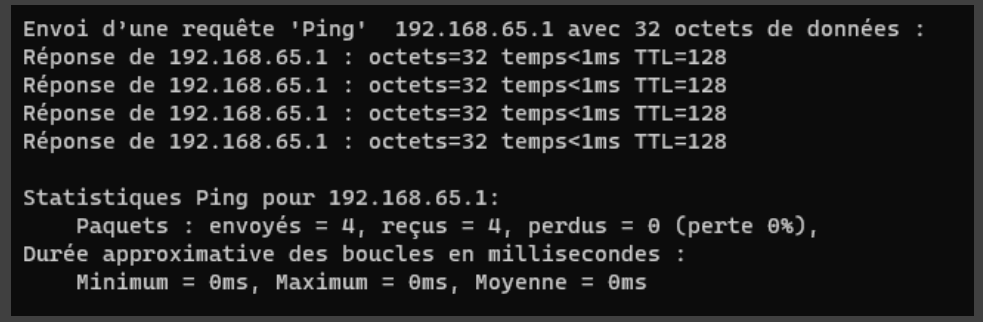
Vérification de la bonne connectivité du réseau

3-Pour que une machine physique et virtuelle communique bien entre-elle il faut que vous paramétrez votre ip sur les deux machines et que vous enleviez le pare-feu sur les deux machine.

Ensuite

4- Ouvrez l'invite de commande :

5- Et tapez la commande « ipconfig » suivi du numéro de l'adresse IP cible. Si les machines sont bien en communication ceci devrait s'afficher :

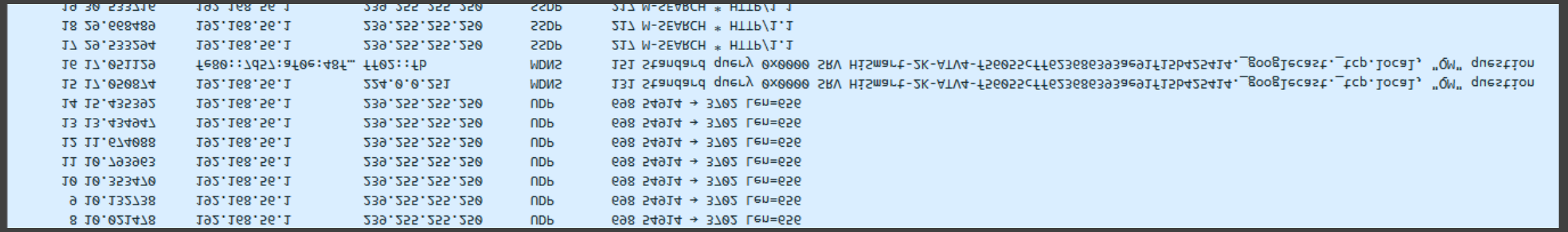


Utilisation de Wireshark:

6-Lancez l’application et cliquez sur « Capture » et puis sélectionnez votre VM

7-Démarrer

8- Si tout fonctionne correctement ceci devrait s’afficher:



Détermination:

-Adresse MAC source et destinataire:

Source:00-E0-4C-C8-6D-42

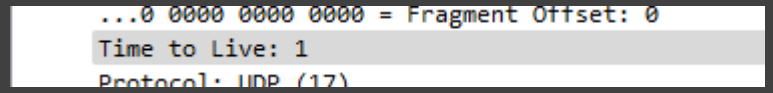
Destinataire:

-Adresse IP source et destinataire

Source:192,168,56,2

Destinataire:192.168.56.1

-Le time to live: 1



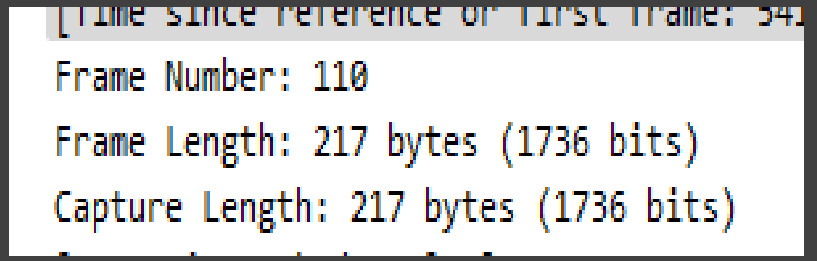
Détermination

-Numéro de la trame:110

-La taille de la trame : 217 bytes(1736 bits)

-Taille des données :217 bytes (1736bits)

-Le code type ICMP : 0



Modification des paramètres IP

-Pour effectuer une modification d’une adresse IP il vous suffit d ’allez dans le panneau de configuration (voir TP1)

- Adresse IP source :192.168.56.2

-Adresse IP Destinataire: 172.16.56.1

-Retournez dans le terminal de commande de votre machine physique est entrer la commande « ping 172.16.56.1 »

-La machine vous répondra ceci

c’est à dire que les machines ne

peuvent pas entrer en communication

```
C:\Users\thoma>ping 172.16.56.1

Envoi d’une requête 'Ping'  172.16.56.1 avec 32 octets de données :
Réponse de 192.168.0.40 : Impossible de joindre l’hôte de destination.
Réponse de 192.168.0.40 : Impossible de joindre l’hôte de destination.
Réponse de 192.168.0.40 : Impossible de joindre l’hôte de destination.
Réponse de 192.168.0.40 : Impossible de joindre l’hôte de destination.

Statistiques Ping pour 172.16.56.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
```

Modification des paramètres IP

-Si vous décidez de changer le masque de la machine destinataire avec par exemple « 255.255.0. » et que vous pingez ensuite votre machine répondra aussi ceci

car c'est l'adresse Ip qui permet

la communication entre deux machines

```
C:\Users\thoma>ping 172.16.56.1

Envoi d'une requête 'Ping'  172.16.56.1 avec 32 octets de données :
Réponse de 192.168.0.40 : Impossible de joindre l'hôte de destination.
Réponse de 192.168.0.40 : Impossible de joindre l'hôte de destination.
Réponse de 192.168.0.40 : Impossible de joindre l'hôte de destination.
Réponse de 192.168.0.40 : Impossible de joindre l'hôte de destination.

Statistiques Ping pour 172.16.56.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
```

Analyse du protocole http et https

Pour trouver les paquets http entre http dans filtrer

-pour le site du bts il suffit de rentrer la commande tls

Analyse du protocole Ftp

- Démarrer le serveur FTP

-Capturez la trame de connexion d’un client sur votre serveur

- Soucis de config donc a finir ce weekend