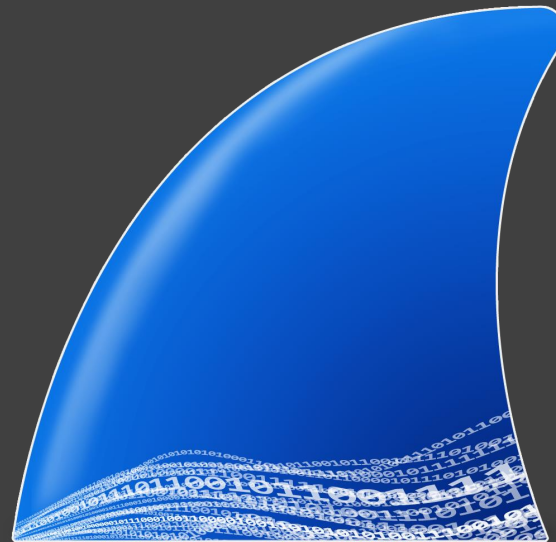


TP WIRESHARK

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 paramétrerez 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 :

```
Envoi d'une requête 'Ping' 192.168.65.1 avec 32 octets de données :  
Réponse de 192.168.65.1 : octets=32 temps<1ms TTL=128  
Réponse de 192.168.65.1 : octets=32 temps<1ms TTL=128  
Réponse de 192.168.65.1 : octets=32 temps<1ms TTL=128  
Réponse de 192.168.65.1 : octets=32 temps<1ms TTL=128  
  
Statistiques Ping pour 192.168.65.1:  
  Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),  
Durée approximative des boucles en millisecondes :  
  Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

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:

```
18 30 23331e 1a5.1e8.2e.1 530.522.522.520 220b 513 W-2EVBCH * H11b\T.T
18 50'0e8480 1a5.1e8.2e.1 530.522.522.520 220b 513 W-2EVBCH * H11b\T.T
11 50'233504 1a5.1e8.2e.1 530.522.522.520 220b 513 W-2EVBCH * H11b\T.T
1e 11'021150 4680::1921:9406:484 4405::4p WDM2 121 2f9uq9rlq dn6Lλ 0x0000 28λ H12m9L4-5K-V1A4-42e022c44e53e8e3039e01412p452414.~8008Jec92f.~fcb.1oc9J' „0W„ dne2frou
12 11'020814 1a5.1e8.2e.1 554'0'0'521 WDM2 131 2f9uq9rlq dn6Lλ 0x0000 28λ H12m9L4-5K-V1A4-42e022c44e53e8e3039e01412p452414.~8008Jec92f.~fcb.1oc9J' „0W„ dne2frou
14 12'432305 1a5.1e8.2e.1 530.522.522.520 NDb e08 24014 → 3105 ΓεU=e2e
13 13'434041 1a5.1e8.2e.1 530.522.522.520 NDb e08 24014 → 3105 ΓεU=e2e
15 11'014088 1a5.1e8.2e.1 530.522.522.520 NDb e08 24014 → 3105 ΓεU=e2e
11 10'1030e3 1a5.1e8.2e.1 530.522.522.520 NDb e08 24014 → 3105 ΓεU=e2e
10 10'323410 1a5.1e8.2e.1 530.522.522.520 NDb e08 24014 → 3105 ΓεU=e2e
0 10'135138 1a5.1e8.2e.1 530.522.522.520 NDb e08 24014 → 3105 ΓεU=e2e
8 10'051418 1a5.1e8.2e.1 530.522.522.520 NDb e08 24014 → 3105 ΓεU=e2e
```

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

```
...0 0000 0000 0000 = Fragment Offset: 0
```

```
Time to Live: 1
```

```
Protocol: UDP (17)
```

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

```
[Time since reference or first frame: 341]
Frame Number: 110
Frame Length: 217 bytes (1736 bits)
Capture Length: 217 bytes (1736 bits)
```

Modification des paramètres IP

-Pour effectuer une modification d'une adresse IP il vous suffit d'aller 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