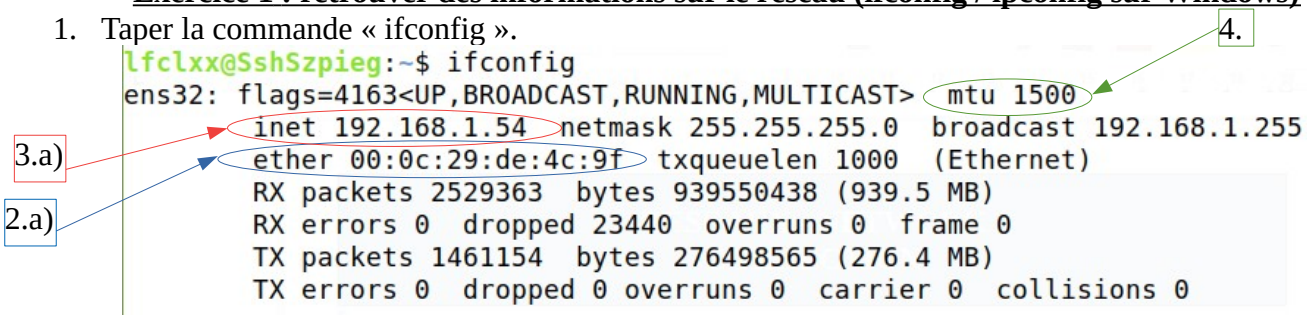
RÉSEAUX – NETWORK I
CORRECTION

Exercice 0

1. Connectez-vous au serveur « ssh » « marion.szpieg.fr » avec votre compte.
2. Taper la commande « history -c », afin d'effacer votre historique du TP précédent.
3. Avec la commande « mkdir », créer un répertoire « tpSE2 » dans votre home directory.
4. Vérifier avec la commande « ls » que le répertoire a bien été créé.
5. Avec la commande « cd », se placer dans le répertoire tpSE2.

Exercice 1 : retrouver des informations sur le réseau (ifconfig / ipconfig sur Windows)

1. Taper la commande « ifconfig ».



2. a) A la 3e ligne, on lit : « ether 00:0c:29:de:4c:9f »
   b) On reconnaît que c'est une adresse MAC car elle est composée 6 octets séparés par des « : » et codés en hexadécimale.
   c) Elle représente l'adresse MAC de la carte réseau du serveur szpieg.fr

3. a) A la 2e ligne, on lit : « inet 192.168.1.54 »
   b) On reconnaît que c'est une adresse IP car elle est composée 4 octets séparés par des « . » et codés en décimal.
   c) C'est l'adresse IP dans mon réseau local de mon serveur.
4. Le MTU est la taille maximale en octets d'une trame (ou d'un fragment).
   Plus précisément, lorsqu'une machine veut envoyer un message (gros!) sur un réseau, ce dernier est découpé en plus petits paquets, appelés « tramefragment ». Le MTU (Maximum Transmission Unit) étant à 1500, les trames seront de taille maximale de 1500 octets.

Exercice 2 (arp)

1.
```
lfclxx@SshSzpieg:~$ arp -n
Adresse                  TypeMap AdresseMat          Indicateurs          Iface
192.168.1.1              ether   44:a6:1e:8e:81:f6   C                    ens32
```

2. On voit une adresse IP et une adresse MAC, mais elles ne correspondent pas à la carte réseau de l'exercice précédent. On en conclut donc que notre machine connaît les adresses IP et MAC d'une autre autre machine sur le réseau.
   Remarque : ens32 signifie que pour échanger avec cette autre machine, votre machine virtuelle passe par la carte réseau ens32 vue précédemment.

Exercice 3 : interpeller une machine (ping)

Temps de l'aller et retour

Il y a 2 lignes, donc ça signifie qu'on a envoyé 2 paquets

Taille dans la couche 2 des paquets envoyés

Sur les 2 paquets envoyés, les 2 ont bien été reçus, on a donc 0 % de perte

```
lfclxx@SshSzpieg:~$ ping -c2 192.168.1.43
PING 192.168.1.43 (192.168.1.43) 56(84) bytes of data.
64 bytes from 192.168.1.43: icmp_seq=1 ttl=64 time=1.36 ms
64 bytes from 192.168.1.43: icmp_seq=2 ttl=64 time=0.622 ms

--- 192.168.1.43 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.622/0.990/1.359/0.368 ms
```

Exercice 4 (arp)

1.
```
lfclxx@SshSzpieg:~$ arp -n
Adresse                  TypeMap AdresseMat          Indicateurs           Iface
192.168.1.43             ether   00:0c:29:f7:b2:93   C                     ens32
192.168.1.1              ether   44:a6:1e:8e:81:f6   C                     ens32
```

2. On remarque qu'il y a une nouvelle ligne avec l'adresse IP de la machine avec laquelle on vient de faire le ping. En plus de son adresse IP, on voit qu'on a l'adresse MAC.

   Pourquoi ? En théorie : on rappelle que lorsqu'un paquet de données part d'une machine, il traverse les différentes couches du protocole TCP/IP. L'adresse IP se trouvant dans la couche n°2, le message ne peut pas sauter la couche 1 (adresse MAC!) avant d'aller sur le réseau local.

   En pratique : ma machine a envoyé au serveur (dont l'adresse IP est 192.168.1.54 d'après l'exercice 1) un message pour retrouver la machine dont l'adresse IP est 192.168.1.43. Le serveur a envoyé un message à toutes les machines du réseau local en demandant « est-ce que l'un d'entre vous a pour adresse IP 192.168.1.43? ». La machine qui s'est reconnue a envoyé un message de réponse avec son adresse MAC.

Exercice 5 : capturer les paquets (sera utile pour plus tard!)

```
lfclxx@SshSzpieg:~$ arp -n
Adresse                  TypeMap AdresseMat          Indicateurs           Iface
192.168.1.1              ether   44:a6:1e:8e:81:f6   C                     ens32
lfclxx@SshSzpieg:~$ tcpdump arp or icmp -w ping.cap&
[1] 2970
lfclxx@SshSzpieg:~$ tcpdump: listening on ens32, link-type EN10MB (Ethernet), capture
 size 262144 bytes

lfclxx@SshSzpieg:~$ ping -c2 192.168.1.43
PING 192.168.1.43 (192.168.1.43) 56(84) bytes of data.
64 bytes from 192.168.1.43: icmp_seq=1 ttl=64 time=1.05 ms
64 bytes from 192.168.1.43: icmp_seq=2 ttl=64 time=0.639 ms

--- 192.168.1.43 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.639/0.846/1.053/0.207 ms
lfclxx@SshSzpieg:~$ fg
tcpdump arp or icmp -w ping.cap
^C16 packets captured
19 packets received by filter
0 packets dropped by kernel
lfclxx@SshSzpieg:~$ ls -l ping*
-rw-r--r-- 1 lfclxx lfcl 1356 févr.  4 19:48 ping.cap
```

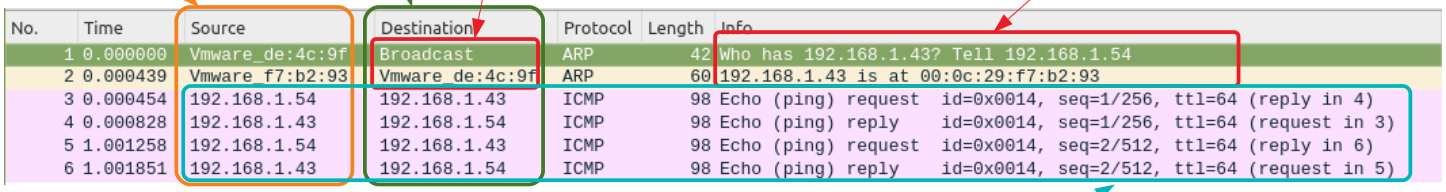
Exercice 7 : analyser un paquet capturé (avec Wireshark)

Adresse IP de la machine destinataire du paquet

Adresse IP de la machine qui a envoyé le paquet

Ce message est un envoi broadcast (c'est-à-dire un message envoyé à toutes les machines du réseau local)

Description de la demande.
On lit ici que c'est la requête de l'ordinateur 192.168.1.54 qui veut récupérer l'adresse MAC de la machine ayant pour adresse IP 192.168.1.43.
A la 2e ligne, ont voit la réponse.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Vmware_de:4c:9f	Broadcast	ARP	42	Who has 192.168.1.43? Tell 192.168.1.54
2	0.000439	Vmware_f7:b2:93	Vmware_de:4c:9f	ARP	60	192.168.1.43 is at 00:0c:29:f7:b2:93
3	0.000454	192.168.1.54	192.168.1.43	ICMP	98	Echo (ping) request id=0x0014, seq=1/256, ttl=64 (reply in 4)
4	0.000828	192.168.1.43	192.168.1.54	ICMP	98	Echo (ping) reply id=0x0014, seq=1/256, ttl=64 (request in 3)
5	1.001258	192.168.1.54	192.168.1.43	ICMP	98	Echo (ping) request id=0x0014, seq=2/512, ttl=64 (reply in 6)
6	1.001851	192.168.1.43	192.168.1.54	ICMP	98	Echo (ping) reply id=0x0014, seq=2/512, ttl=64 (request in 5)

On voit dans ces 4 lignes que la machine à l'adresse IP 192.168.1.54 qui envoie le 1er ping à l'ordinateur 192.168.1.43.
Dans la ligne suivante il y a la réponse de 192.168.1.43.
Dans les 2 dernières lignes, il y a le 2e ping.