TP1 R102 Wireshark

Exercice 1

1) IP.addr == 10.213.14.1
2) Ip.src == 10.213.14.1 ou ip.dst == …
3) Tcp/udp.port eq 25 or(et) icmp

2)
Voilà le resultat du site perdu.com :

Les couches avec protocole :
Application : HTTP
Transport : TCP
Internet : IPV4
Accès réseau : Ethernet

3)
Frame 17.
C'est un numéro attribuer à chaque '' capture ''. Dans l'ordre de capture du temps.

Exercice 2 :
1)
Les paquets ICMP :
-paquet reply
-paquet request

Il demande une confirmation à l'IP demandé et elle répond.

2)

La trame est encapsulée dans un IPV4 puis Ethernet.

Data > IPV4 > Ethernet

Exercice 3 :

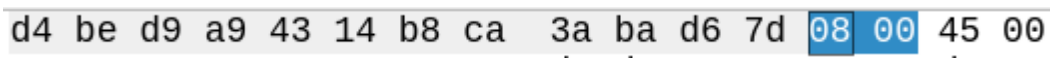
LE TCP stream suit les demande et question d'une demande http.
Il utilise les ip de source et destination pour faire un suivie des demande et réponse.

Exercice 4 :

1) Le tableau montre les IP qui ont été utiliser, le temps et les commentaires.

Exercice 5 :

1)



IPV4

0800 permet de dire ce que contient la trame

2) La valeur pour un paquet ARP sera 0806

Exercice 6

```
emis par la machine : ip.src == 10.213.14.1
TCP : tcp
Port 80 :tcp.port eq 80 ou == 80

Donc ip.src == 10.213.14.1 or tcp.port == 80
```

adresse mac de destination : d4:be:d9:a9:43:14
Adresse ip de destination : 172.42.20.254

Exercice 7 :
le logiciel capture tout les paquet, et affiche l'heure, l'ip source et destination.
Voila le filtre : | grep http

Exercice 8 :
arp -an
ou
ip neigh
10.213.5.1 dev eno1 lladdr 98:90:96:e0:7e:2b STALE
10.213.0.99 dev eno1 lladdr 3c:18:a0:02:b9:d5 STALE
10.213.15.1 dev eno1 lladdr 98:90:96:e0:80:c1 STALE
10.213.7.1 dev eno1 lladdr 98:90:96:e0:84:49 STALE
10.213.8.1 dev eno1 lladdr 98:90:96:e0:85:29 STALE
10.213.255.254 dev eno1 lladdr d0:7e:28:2d:84:8c STALE
10.213.11.1 dev eno1 lladdr 98:90:96:e0:80:bd STALE
10.213.10.1 dev eno1 lladdr 98:90:96:e0:83:b1 STALE
10.213.2.1 dev eno1 lladdr 98:90:96:e0:84:b2 STALE
10.213.12.1 dev eno1 lladdr 98:90:96:e0:81:37 STALE
fe80::9a90:96ff:fee0:7ece dev eno1 lladdr 98:90:96:e0:7e:ce STALE

Il affiche le cache ARP.

Et pour la vider:

ip neigh flush all dev (interface)

Exercice 9 :
J'émets une trame de demande ARP pour avoir l'adresse mac
je reçois une trame de réponse qui me dit que telle IP est à telle adresse mac

Ils enregistrent dans leur cache ARP les adresse MAC qui correspond à laquelle adresse IP

Exercice 10 :

Il contient bien l'adresse MAC précédente

Exercice 11 :

Il n’utilise pas le protocole ARP car il connaît déjà l’adresse mac affecter à l’IP demander.

Exercice 12 :

Il n’a pas mis à jour l’adresse car il l’a déjà en cache.

Exercice 13 :

Il ne se met pas à jour car on sort du réseau local.
Nan c’est le routeur qui va avoir le serveur google.

Exercice 14 :

Les statut des entre cache sont (failed, reachable, stable, delay, ect…)

Exercice 15 :

Oui, il y avait marqué delay, puis reachable

Exercice 16 :