3iL ALLIANCE
</sciences et techniques informatiques>

Prog Avancée & Cybersécurité

Algo & Python

TP n°3

Programmation Python et Analyse trafic réseau

Analyse de trafic réseau

1 – Vous téléchargerez 60Mo de capture réseau à :
`http://downloads.digitalcorpora.org/corpora/scenarios/2008-nitroba/nitroba.pcap`

Questions :

a. Faites la liste des adresses MAC présentes dans la capture réseau.
Pouvez vous déterminer quelle est l'adresse MAC du routeur ?
En téléchargeant le fichier `ieee-oui.txt` à :
`https://p-fb.net/3IL/fiches/ieee-oui.txt`
Pouvez vous donner la liste des constructeurs de ces matériels ?

b. Est-ce que le réseau propose du DHCP ?

Si oui quelle configuration donne-t-il ?

c. Y-a-t-il des échanges ICMP ?

Entre quelles machines ?

d. Faites la liste des requêtes DNS réalisées.

e. Faites la liste des services TCP utilisés dans le réseau.

Identifiez ces services avec l'annuaire inversé, fourni par :

```
MY_TCP_SERVICES={}
for proto in TCP_SERVICES.keys():
   MY_TCP_SERVICES[TCP_SERVICES[proto]] = proto
```

Pour le service http, indiquez quels sont les serveurs contactés.

Pouvez vous trouver les requêtes émises par les clients ?