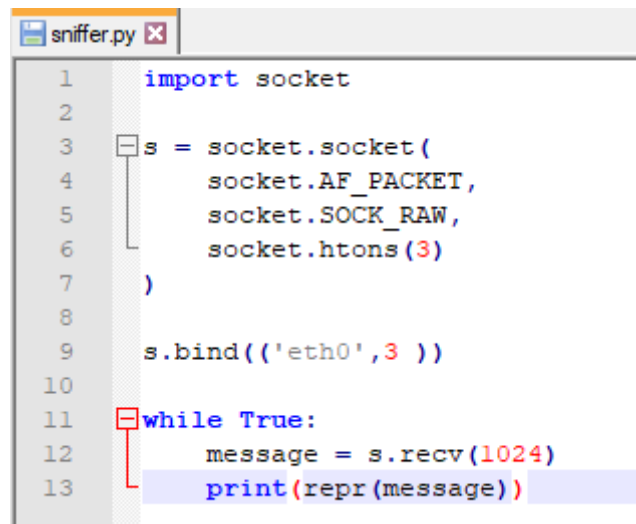


Exercice

Le code suivant vous donne la base d'un outil d'écoute du trafic réseau sur une interface nommée eth0.



```
1  import socket
2
3  s = socket.socket(
4      socket.AF_PACKET,
5      socket.SOCK_RAW,
6      socket.htons(3)
7  )
8
9  s.bind(('eth0', 3))
10
11 while True:
12     message = s.recv(1024)
13     print(repr(message))
```

A l'aide de cette base de script Python, vous construirez un scanner de trafic réseau qui enregistrera dans une base de données de votre choix (SQL ite par exemple) toutes les informations nécessaires vous permettant de créer les requêtes SQL suivantes :

- Liste des trames Ethernet capturées
- Liste des paquets IPv4 ou IPv6 capturés
- Liste des messages ARP (requêtes et réponses) capturés
- Liste des associations entre adresses MAC vues et adresses IP correspondantes
- Liste des segments TCP ou UDP capturés
- Liste des adresses IP sources et destinations du trafic capturé
- Nombre de demandes de connexions TCP capturées
- Volume de trafic généré pour chacun des protocoles précédents

Remarques importantes :

Cette base de script est fonctionnelle en environnement Linux.

Pour l'analyse des paquets reçus, vous pourrez vous appuyer sur des bibliothèques existantes de Python. Par exemple **struct** vous permettra de décoder des structures binaires.

Votre script sera documenté, notamment en ce qui concerne le format des différents types de messages reçus et la manière dont vous les aurez décodés.