1- Utiliser Wireshark pour caractériser le trafic réseau dans les 2 fichiers pcaps

Nombre de paquets, taille moyennes de paquets, nombre de sessions, protocoles utilisés etc.

2- Extraire avec un programme Python

2.a des informations pour chaque paquet : adresse IP source, adresse IP destination, port source, port destination, protocole de la couche transport, taille d’un paquet, temps inter paquets

(tout autre feature est également accepté)

2.b des informations pour chaque session/flux : nombre de paquets par flux, moyenne des tailles des paquets par flux, moyenne du temps inter paquets

(tout autre feature est également accepté)

3- Utiliser du clustering pour diviser le trafic en différentes catégories

4- Utiliser des algorithmes de AI/ML pour détecter des anomalies dans le trafic (un fichier pourra être utilisé pour l’apprentissage et l’autre pour le test)