

Utilisation de la bibliothèque pandas

■ ■ ■ **Analyse de log**

- 1 – Vous referez l’analyse de fichier log d’Apache à l’aide de pandas.

■ ■ ■ **Analyse de trafic réseaux**

- 2 – Vous récupérez les adresses IPs d’une capture réseau et pour chacune des adresses récupérez l’entrée DNS.
Vous utiliserez la commande « `dig -x xx.xx.xx.xx` » pour obtenir le FQDN à partir de l’adresse IP.
- 3 – Vous construirez une table pandas à partir des résultats de la commande « `traceroute -n` ».
Pour chaque adresse IP non privée de routeur, vous récupérez les coordonnées GPS et l’organisme d’appartenance avec le service `ipinfo.io`.
- 4 – Vous utiliserez pandas avec Scapy pour obtenir une table des paquets contenant :
 - ▷ adresse IP source ;
 - ▷ adresse IP destination ;
 - ▷ port source dans le cas d’UDP et de TCP ;
 - ▷ port destination dans le cas d’UDP et de TCP ;
 - ▷ le protocole utilisé ;
 - ▷ la taille du paquet ;
 - ▷ l’heure de transmission du paquet.Vous effectuerez des statistiques sur cette table.

■ ■ ■ **Utilisation de tshark**

- 5 – Vous utiliserez pandas avec tshark pour analyser les requêtes HTTP au format GET et POST dans la capture de fichiers pcap.
Pouvez vous trouver des secrets ?

■ ■ ■ **Représentation graphique de l’information**

- 6 – Vous utiliserez Geopandas pour afficher sur une carte du monde les emplacements des routeurs obtenu dans l’exercice 3.
Vous trouverez la procédure dans le support de cours.