# Fonctionnement d’un fichier PCAP :

L’objectif de cette section est de comprendre en détail le principe des fichiers **PCAP**. Nous allons examiner leur structure, leur mode de fonctionnement ainsi que leurs rôles dans l’analyse et la surveillance des réseaux. Cette étude nous permettra de mieux comprendre leur utilité dans la capture et l’interprétation du trafic réseau, notamment pour le diagnostic des performances, la détection d’anomalies.

## Qu’es que le PCAP ?

Un fichier **PCAP (Packet Capture**) est un fichier contenant des données capturées sur un réseau informatique. Ces données capturées et permettent ensuite d’examiner chaque paquet individuellement ou globalement, facilitant ainsi une vue claire du trafic sur un réseau.

Pour chaque paquet enregistré dans le fichier on retrouve les informations :

* **Couche Lien** (adresse MAC source/destination).
* **Couche Réseau** (adresse IP source/destination).
* **Couche Transport** **TCP/UDP** (port source/destination).
* **Couche Application/Les données utiles du paquet** (requêtes HTTP, emails SMTP, fichiers transférés, etc).

## Quel est l’objectif du PCAP ?

La capture du trafic réseau offre des informations sur les performances, les schémas d'utilisation et les vulnérabilités potentielles. Comme vu précédemment les fichiers PCAP permettent de stocker ces captures et rendent donc les informations du réseau exploitable pour une analyse. Cette analyse permet alors effectuer les actions suivantes :

* **Diagnostiquer et résoudre les problèmes réseau** : L'analyse des paquets permet d'identifier des erreurs de configuration, différents problèmes liés à la bande passante et des problèmes de latence.
* **Renforcer la sécurité** : En surveillant le trafic on peut détecter différents types d’attaques sur le réseau tel que des scannes de ports, des attaques http, …
* **Assurer la conformité réglementaire** : Certaines normes imposent la conservation des enregistrements de trafic afin de garantir transparence et responsabilité.
* **Optimiser les performances réseau** : L’analyse des flux de données permet d’adapter l’infrastructure et d’améliorer la gestion des ressources pour optimiser le réseau.

De notre côté nous allons surtouts nous concentré sur la création de courbe et de graphique afin d’établir des statistiques du trafic réseau, ainsi que sur la détection de malwares et de divers attaques.

## Protocole PCAP :

Le processus PCAP commence par la surveillance des interfaces réseau. Lorsqu'un paquet passe par une interface, une copie est effectuée et stockée dans un [fichier PCAP](https://www.endace.com/learn/what-is-a-pcap-file) , dont le contenu peut être analysé. Les outils PCAP transforment essentiellement les données brutes en informations sur lesquelles on peut agir comme expliquer précédemment.

Il existe différent type d’interface réseau à analyser. Il est donc important de choisir l'interface appropriée en fonction des donné que l’on souhaite analyser. On retrouve essentiellement :

* **Les réseaux locaux (**[**LAN**](https://www.ipxo.com/blog/wan-vs-lan/)**) :** les interfaces Ethernet sont les plus couramment utilisées.
* **Les réseaux sans fil :** les interfaces Wi-Fi nécessitent des outils spécialisés pour capturer les paquets sans interférence.
* **Les réseaux virtuels :** communications internes entre les machines virtuelles.

Dans les analyses que nous mènerons dans la suite de ce projet nous utiliserons des paquets provenant de réseaux locaux et sans fil.