

## Filtres de capture

### BPF

Berkeley Packets Filters

**Type** : Indique le nom ou le nombre

- host
- net
- port

**Dir** : permet de spécifier une direction

- src
- dst
- src or dst
- src and dst

**Proto** : permet de spécifier un protocole

- ether
- fddi
- ip
- arp
- rarp
- decnet
- tcp / udp

## Filtres d'affichage

### Les opérateurs de comparaison

- ' == ' : Egal à
- ' != ' : Différent de
- ' < ' : Plus petit / ' <=' : aussi égal
- ' > ' : Plus grand / ' >=' : aussi égal

### Les expressions logiques

- ' && ' : et
- ' || ' : ou
- ' ^ ' : ou exclusif
- ' ! ' : not
- snmp || dns : affiche trafic snmp ou dns

### Exemples de filtres

```
ip.src == @  
ip.dst != @  
ip == @  
tcp.port != #  
tcp.dstport == #
```

# ESD academy

Site : [esdacademy.eu](http://esdacademy.eu)

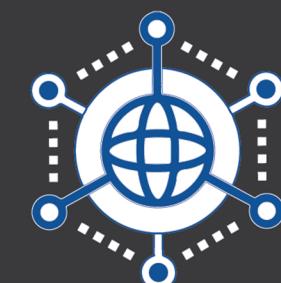
Twitter : [@esd\\_academy](https://twitter.com/esd_academy)

Instagram : [esd\\_academy](https://www.instagram.com/esd_academy/)

Github : [ESD-academy](https://github.com/ESD-academy)



## Aide mémoire



Investigation  
Réseau



[esdacademy.eu](http://esdacademy.eu)

## Redaction d'un rapport

Explication du contexte

Présentation du demandeur, horodatage, objectifs,

Contraintes, deadline ..

Typtologie réseau, données réseau

Collecte des preuves

Présentation des preuves + hash de conformité

Travail d'analyse

Etude des preuves, recherche d'éléments

Ligne du temps des événements notables à l'enquête

Conclusion

Mise en forme du résultat de l'analyse

Summary des recommandations

Proposer des solutions afin d'éviter la récidive

Acquisition passive

Les données sont collectées sans émission d'infos

Acquisition active

Aucune modification des paramètres, aucune émission

Envoyer de requêtes, connexion à un hôte

Interaction avec le système et réseau, analyse des ports

Utilisation des sondes réseau

Prises vampires, prises réseau ..

Capture difficile : grand nombre de protocoles

On parle de mode moniteur, promiscuïte

Acquisition sans fil

D'après les résultats par les NIDS

Caractéristiques d'un contenu numérique

## Methodologie Oscar

Obtention d'informations : Où ? Qui ? Quand ?

Enquête préliminaire : Où ? Qui ? Quand ?

Dejà réalisée ? Objectifs ? Deadline ?

Stratégie

Planification de l'enquête, allocation des ressources matérielles / humaines nécessaires

Collecter des preuves

Colléction à partir de différentes sources, 3 points :

Documentalisation / Capture de la preuve / Chain Of Custody

Recuperation des éléments de preuves.

Rapport

Redaction du résultat de l'enquête. Doit être

compréhensible, facile et défendable.

Volatile

Données perdues lors de l'extinction d'une machine

Données en mémoire morte

Disque dur externe, clé USB, Disque SSD ..

Complexe

Copie entière du réseau, sans filtre.

Session

Flux de données entre deux entités communicantes

Alerte

Données remotées par les NIDS

Metadata