

# CEI - NETSEC #1

## *UI/UX documentation*

L'interface du projet est gérée avec **GTK+** aussi appelé *GTK3*.  
Nous avons choisi d'utiliser cette librairie pour sa simplicité et son efficacité.

### Installation de la librairie

Pour installer GTK+ il vous suffit d'utiliser apt :

```
sudo apt install libgtk-3-dev
```

### Utilisation du programme

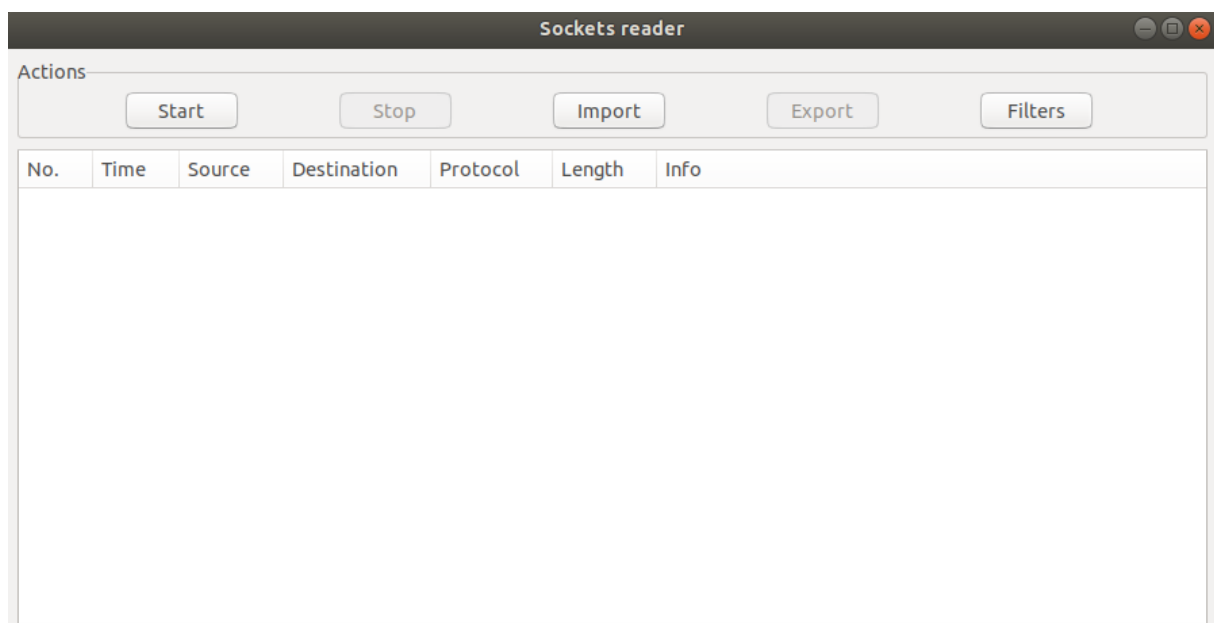
Pour démarrer le programme vous devez lancer le binaire.

network-analysis

**Il se peut que vous ayez besoin de lancer le programme en administrateur**

### Vue principale

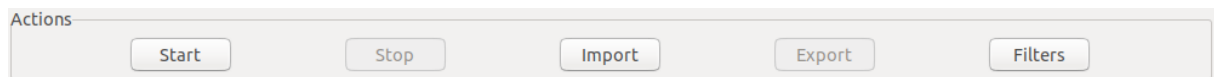
La vue principale de l'application liste les paquets capturés et vous permet d'accéder aux différentes fonctionnalités du programme.



## Actions possibles

Start	<b>Démarre</b> la capture
Stop	<b>Stop</b> la capture
Import	<b>Ouvre</b> et charge un fichier de format pcap
Export	<b>Sauvegarde</b> la capture dans un fichier au format pcap
Filtres	Définie les <b>filtres</b> pour la capture

## Représentation des boutons



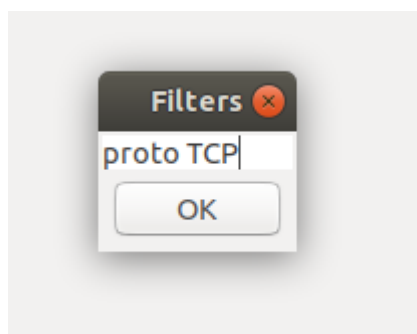
## Capture

Les paquets se remplissent au fur et à mesure de leur capture dans la **liste**.

Il est possible de cliquer sur les colonnes pour **filtrer** l'affichage.

Pour revenir à l'affichage initial, filtrez sur la colonne numéro « No. ».

Sockets reader						
Actions						
<div>Start Stop Import Export Filters</div>						
No.	Time	Source	Destination	Protocol	Length	Info
1	37,000000	192.168.1.67	209.132.180.168	TCP	74	53122 -> 443, win= 29200
2	38,000000	192.168.1.67	209.132.180.168	TCP	74	53124 -> 443, win= 29200
3	38,000000	209.132.180.168	192.168.1.67	TCP	74	443 -> 53122, win= 28960
4	38,000000	192.168.1.67	209.132.180.168	TCP	66	53122 -> 443, win= 229
5	38,000000	192.168.1.67	209.132.180.168	TCP	594	53122 -> 443, win= 229
6	38,000000	209.132.180.168	192.168.1.67	TCP	74	443 -> 53124, win= 28960
7	38,000000	192.168.1.67	209.132.180.168	TCP	66	53124 -> 443, win= 229
8	38,000000	209.132.180.168	192.168.1.67	TCP	66	443 -> 53122, win= 235
9	38,000000	209.132.180.168	192.168.1.67	TCP	3846	443 -> 53122, win= 235
10	38,000000	192.168.1.67	209.132.180.168	TCP	66	53122 -> 443, win= 288
11	38,000000	192.168.1.67	209.132.180.168	TCP	192	53122 -> 443, win= 288
12	38,000000	209.132.180.168	192.168.1.67	TCP	340	443 -> 53122, win= 235
13	38,000000	192.168.1.67	209.132.180.168	TCP	740	53122 -> 443, win= 309
14	38,000000	209.132.180.168	192.168.1.67	TCP	263	443 -> 53122, win= 246
15	38,000000	192.168.1.67	209.132.180.168	TCP	66	53122 -> 443, win= 330
16	38,000000	209.132.180.168	192.168.1.67	TCP	66	443 -> 53122, win= 246
17	38,000000	192.168.1.67	209.132.180.168	TCP	66	53122 -> 443, win= 330
18	38,000000	192.168.1.67	209.132.180.168	TCP	594	53124 -> 443, win= 229
19	38,000000	209.132.180.168	192.168.1.67	TCP	66	443 -> 53122, win= 246



Il est possible de filtrer la capture à l'aide des options de filtres

## Filtres

- **Proto** exemple « proto TCP »
- **Host** exemple « host 192.168.2.1 »
- **Port** exemple « port 53 »

Pour ouvrir les informations d'un paquet, il faut double cliquer dessus dans la liste.

1<sup>er</sup> colonne : Information générale

2eme colonne : Contenu en hexadécimale

3eme colonne : Contenu en ascii

network-analysis		
ETHERNET HEADER	38BAF8771096B8D94DB	8..w....M.....E..<..@.,.....C.....h..y1....q .....P....R.j.z..r....
Source: (B8-D9-4D-B9-9A-8C)	99A8C08004500003C00	
Destination: (38-BA-F8-77-10-96)	0040002C0606A4D184B	
Type: IPv4 (0x0800)	4A8C0A8014301BB CF84	
	EA68CA187931F50DA01	
IP HEADER	27120DAAD0000020405	
Version: 4	500402080A52ED6A1D7	
Header Length: 20 bytes	AEF887201030307	
Services Field: 0x0		
Total Length: 60		
Identification: 0x0		
Time to live: 44		
Protocol: TCP		
Header checksum: 0x6A4		
Source: 209.132.180.168		
Destination: 192.168.1.67		
TCP HEADER		
Source Port: 443		
Destination Port: 53124		
Sequence number: 3932736024		
Window size value: 28960		
Checksum: 0xDAAD		
Urgent pointer: 0		