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

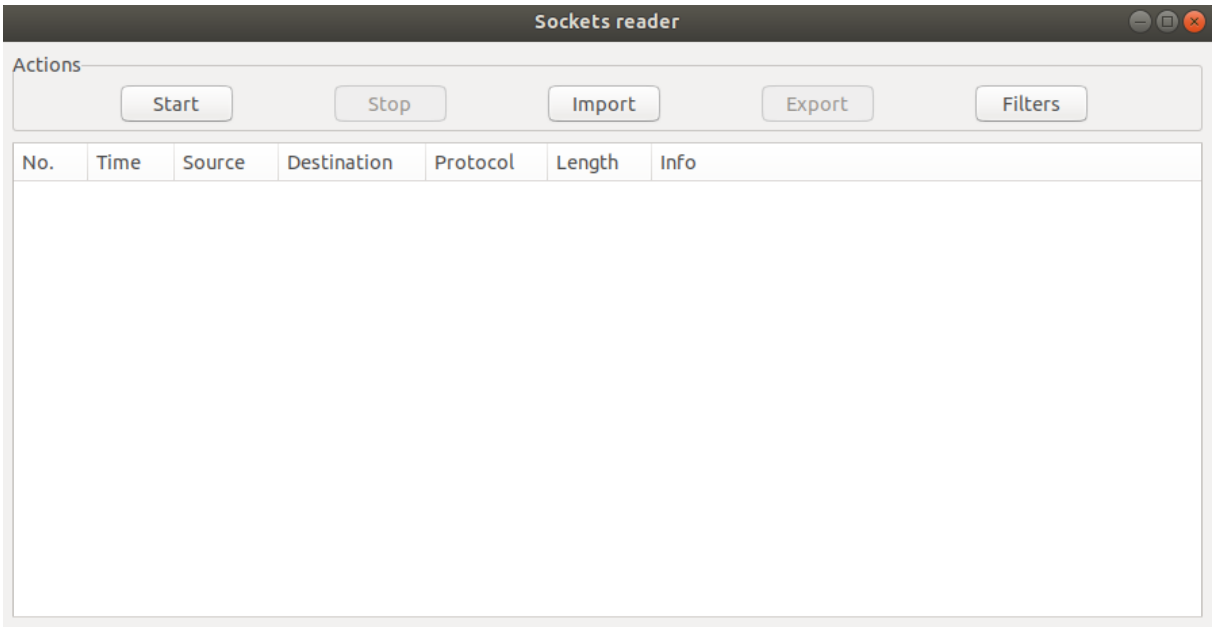
Pour démarrer le programme vous devez lancer le binaire.

```
network-analysis
```

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

Vue principale

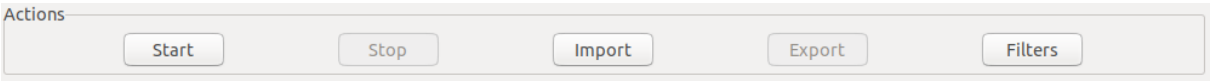
La vue principale de l'application liste les paquets capturés et vous permet d'accéder aux différentes fonctionnalités du programme.



Actions possibles

Start	**Démarre** la capture
Stop	**Stop** la capture
Import	**Ouvre** et charger un fichier de format pcap
Export	**Sauvegarde** la capture dans un fichier au format pcap
Filtres	Définie les **filtres** pour la capture

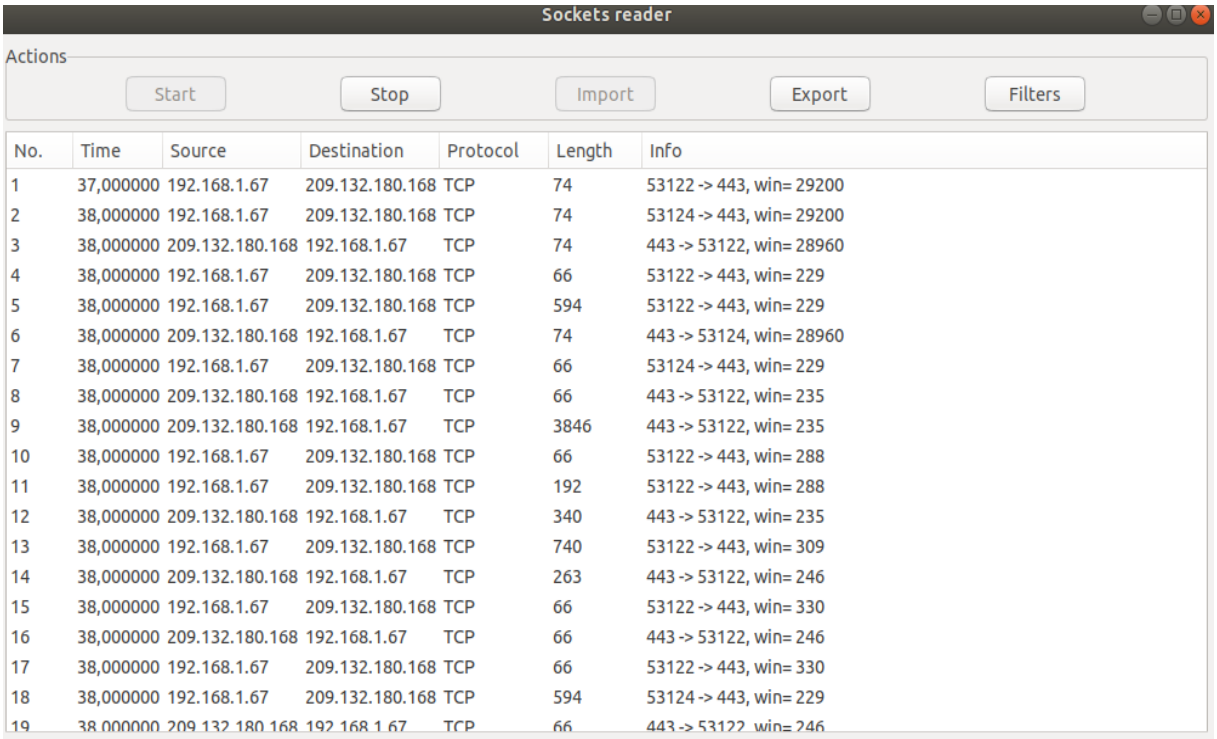
Représentation des boutons



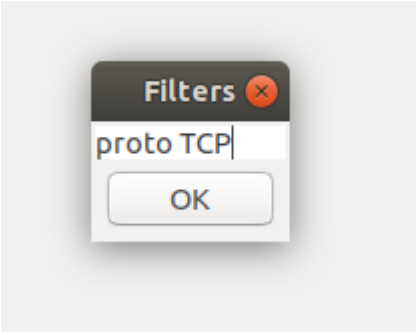
Capture

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. ».



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.

1er colonne : Information générale

2eme colonne : Contenu en hexadécimale

3eme colonne : Contenu en ascii