Manual Program

Source code tersedia pada GitHub melalui link berikut:

https://github.com/felixfren/Ransomwatch

Program sudah tersedia dalam bentuk exe, sehingga tidak perlu melakukan instalasi. Kompabilitas antar sistem operasi windows dan linux terdukung, sehingga manual program ini akan menujukkan cara menggunakan program pada dua sistem operasi yang berbeda. Dibawah merupakan file yang perlu diunduh untuk menjalankan program. Perlu diperingatkan bahwa pengujian dengan *ransomware* asli sebaiknya dilakukan pada sistem terisolasi seperti *virtual machine* agar sistem anda tidak terinfeksi *ransomware* karena program ini hanya dapat mendeteksi.

File Program (EXE) untuk Sistem Operasi Windows :

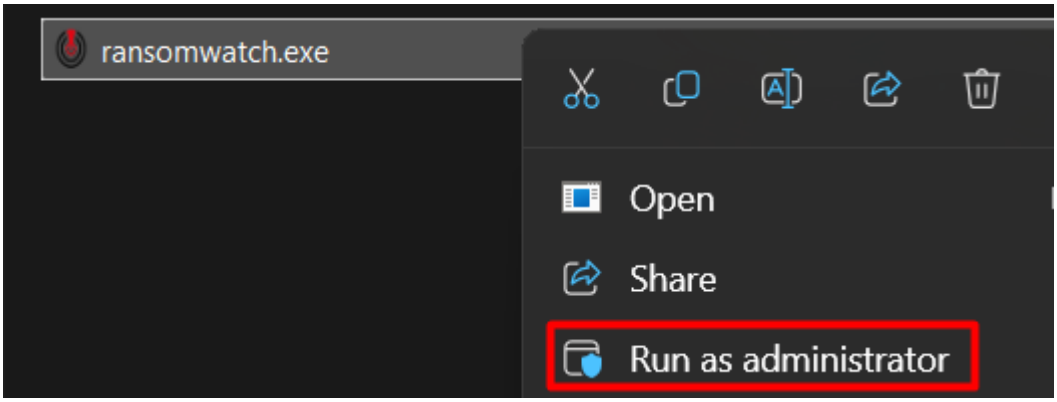
https://drive.google.com/file/d/13FNgLHytSPWZoGFovyp0WI7h0CFwhKp9/view?usp=sharing

File Program untuk Sistem Operasi Linux :

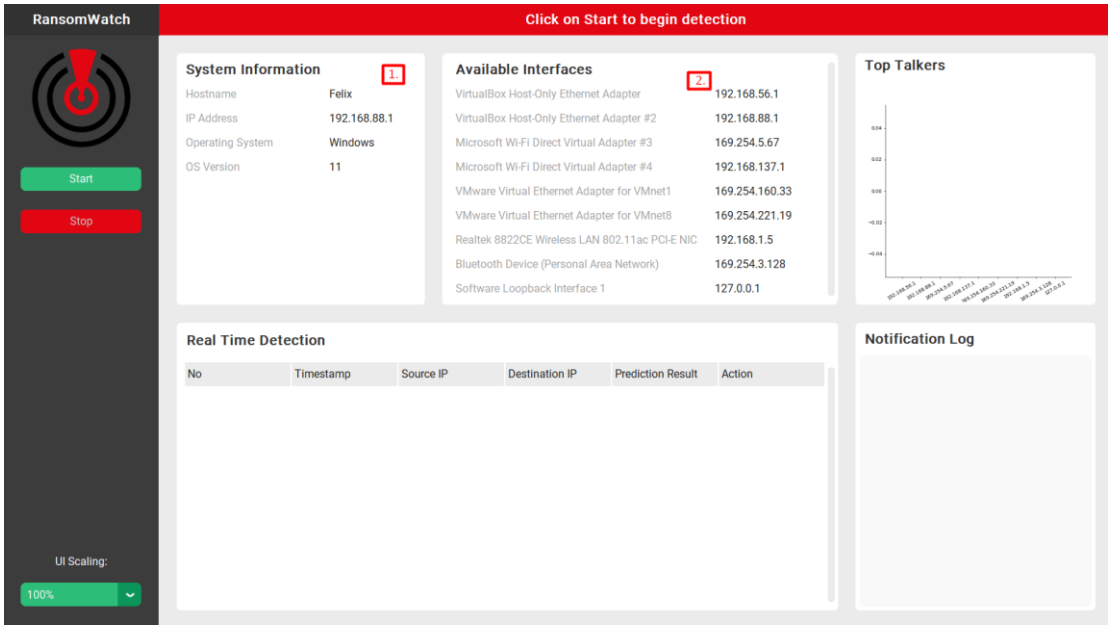
https://drive.google.com/file/d/1nKoGslxtelWkhey7_lUOFbbhecZhu1xZ/view?usp=sharing

A. Windows

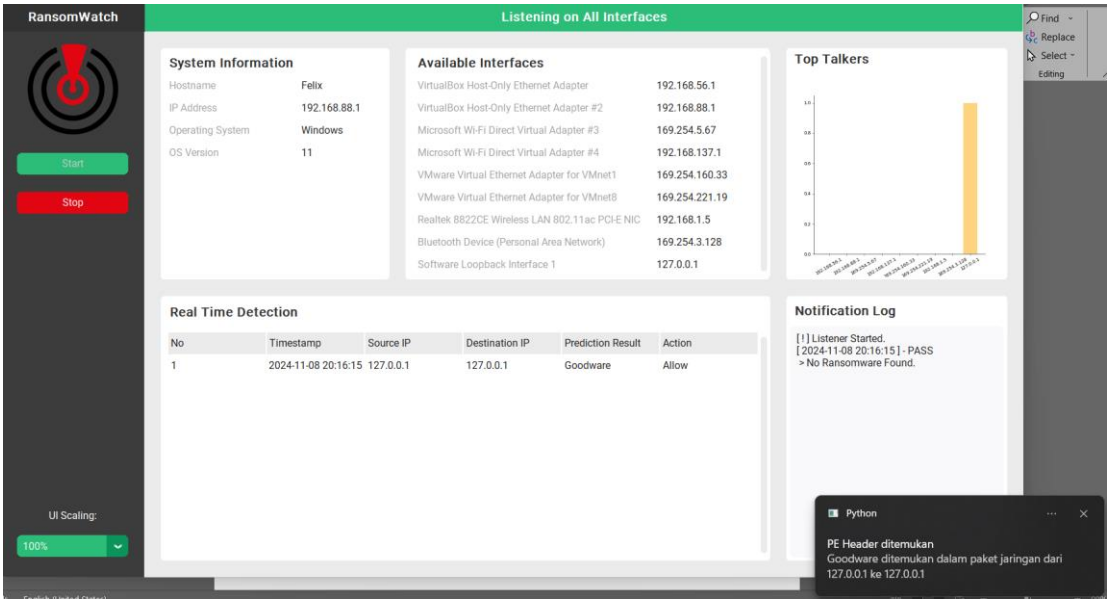
1. Pada sistem operasi windows, jalankan program dengan run as administrator.



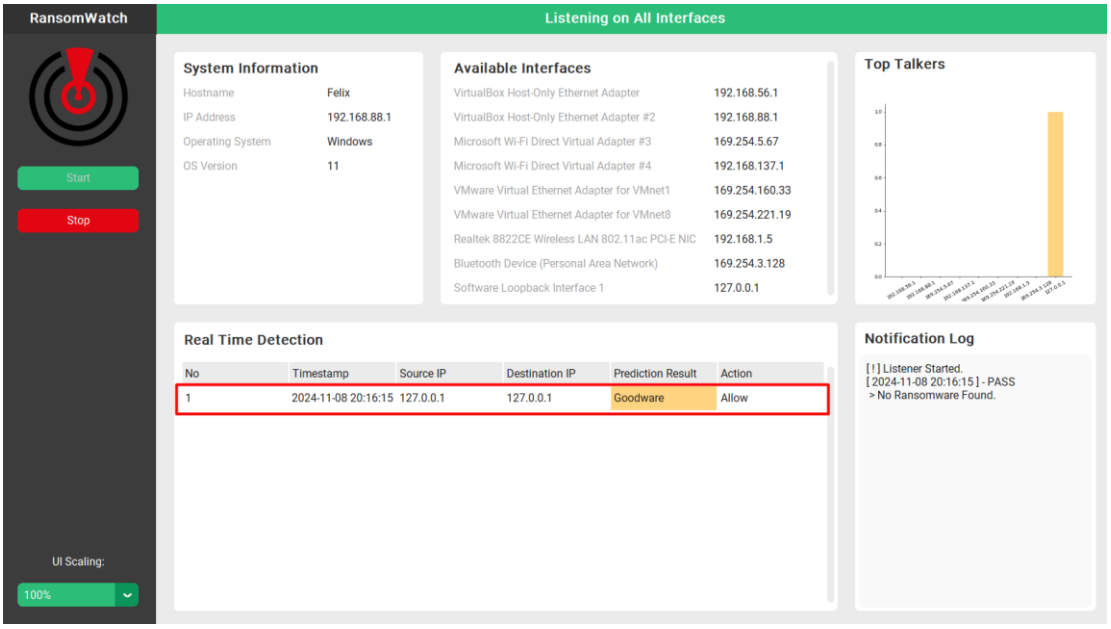
2. *Widget* 1 dan 2 yaitu system information dan available interfaces akan menampilkan informasi lokal milik sistem berjalannya program ini, pada tampilan dibawah informasi sistem dan antarmuka jaringan perangkat windows dapat dilihat.



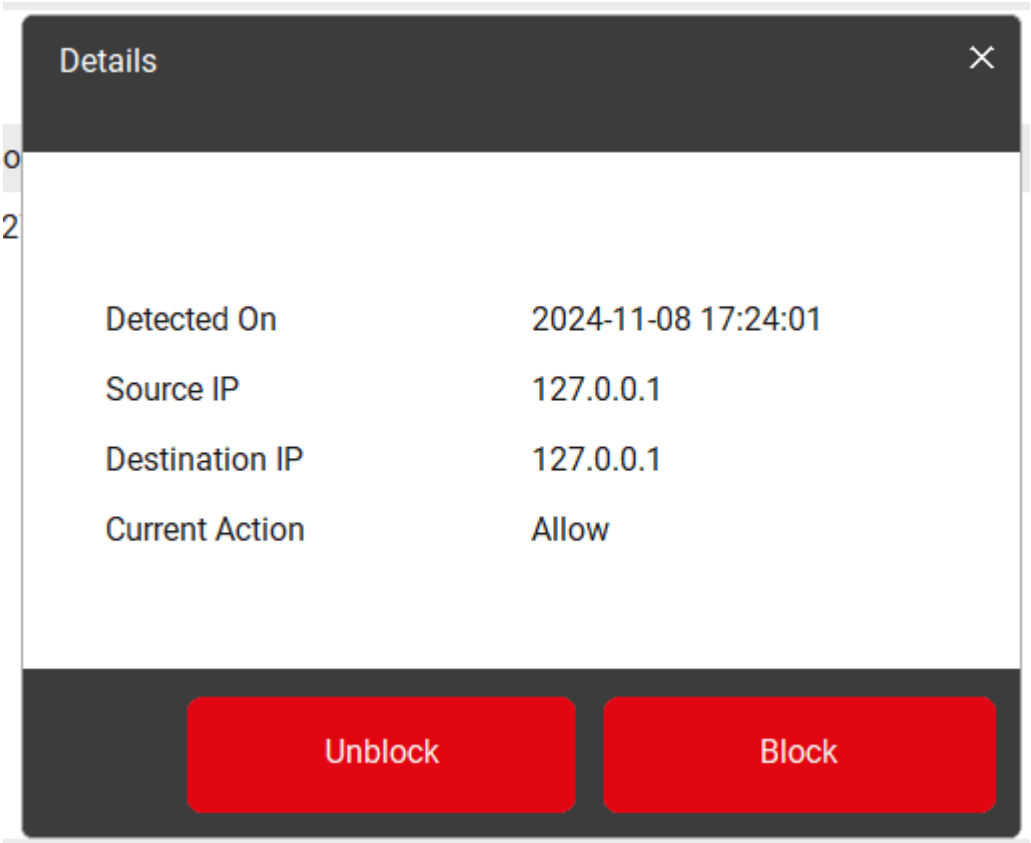
3. Klik tombol “Start” pada sisi kiri program untuk memulai pendeteksian. Program akan memulai mode pendeteksian dengan mendengar pada seluruh antarmuka jaringan untuk mencari *executable*. Ketika pengunduhan atau pengiriman dilakukan dengan protokol tanpa enkripsi seperti HTTP dan FTP, atau dengan *script* pengujian maka hasil pendeteksian akan diberikan beserta sebuah notifikasi.



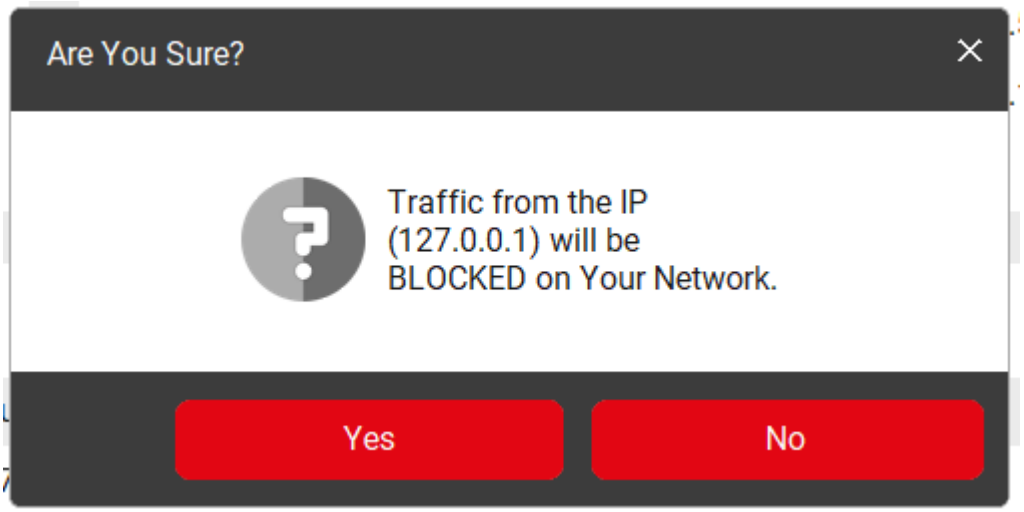
4. Hasil pendeteksian pada *widget Real Time Detection* dapat diklik untuk melakukan tindakan terhadap sumber alamat *IP* yang terdeteksi.

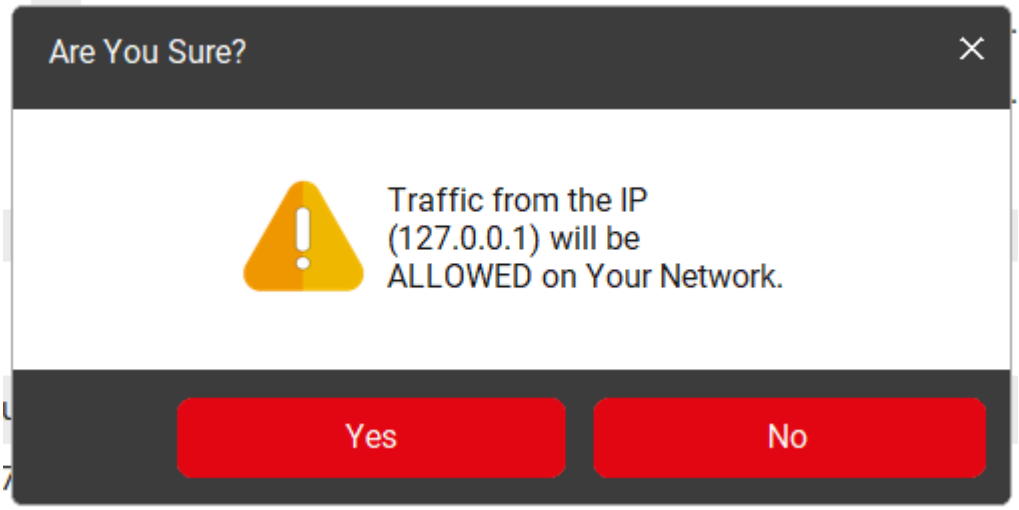


5. Sumber Alamat *IP* dapat diblokir atau dibuka blokir dengan *Block dan Unblock*.



6. Setelah unblock atau block diklik, akan ada window konfirmasi terakhir. Jika block dan yes dipilih maka ip sumber akan ditambahkan rule deny pada firewall perangkat sehingga tidak dapat diakses, jika unblock dan yes maka rule deny pada firewall perangkat akan dihapus sehingga dapat diakses kembali.



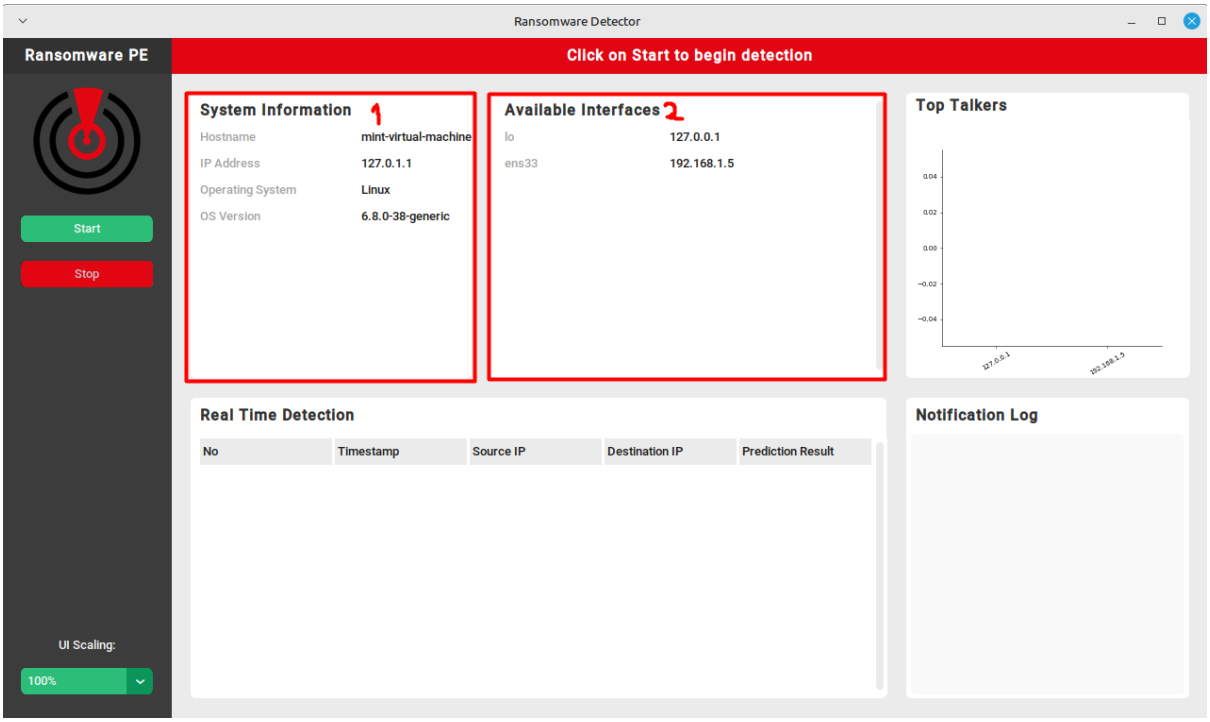

Are You Sure?
Traffic from the IP
(127.0.0.1) will be
ALLOWED on Your Network.
Yes
No

B. Linux

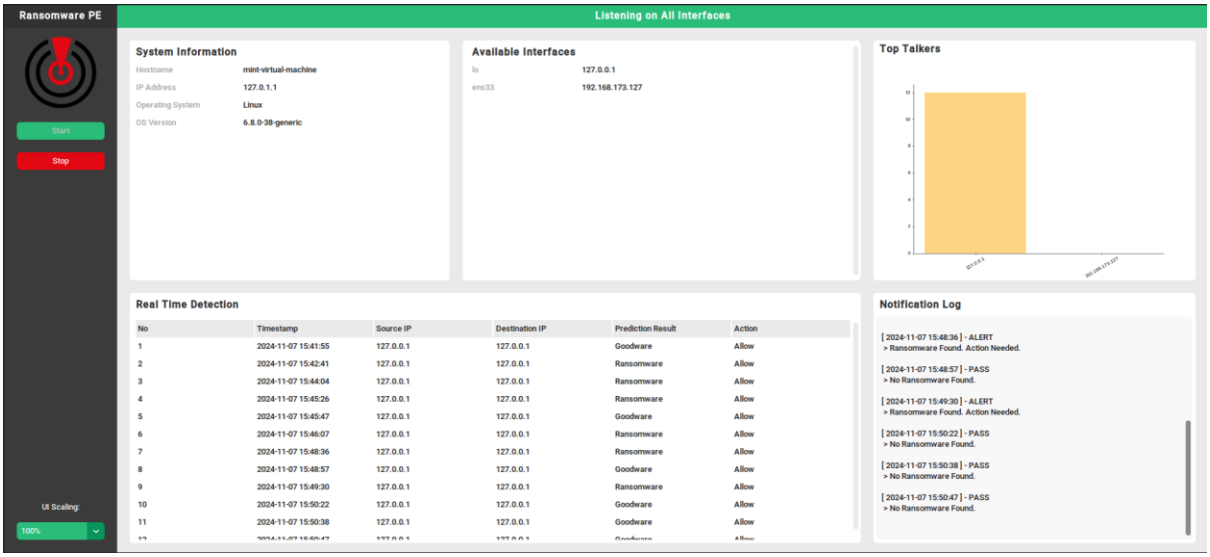
1. Pada sistem operasi Linux, jalankan program sebagai root dengan command sudo.

```
:/home/mint/Downloads# sudo ransomwatch
```

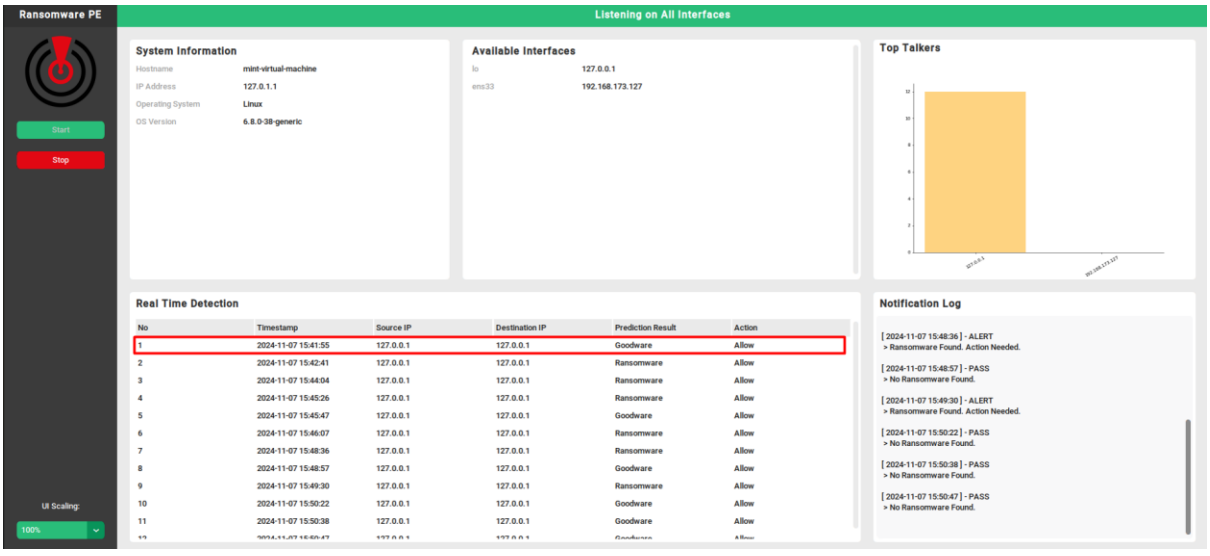
2. *Widget* 1 dan 2 yaitu system information dan available interfaces akan menampilkan informasi lokal milik sistem berjalannya program ini, pada tampilan dibawah informasi sistem dan antarmuka jaringan perangkat Linux dapat dilihat.



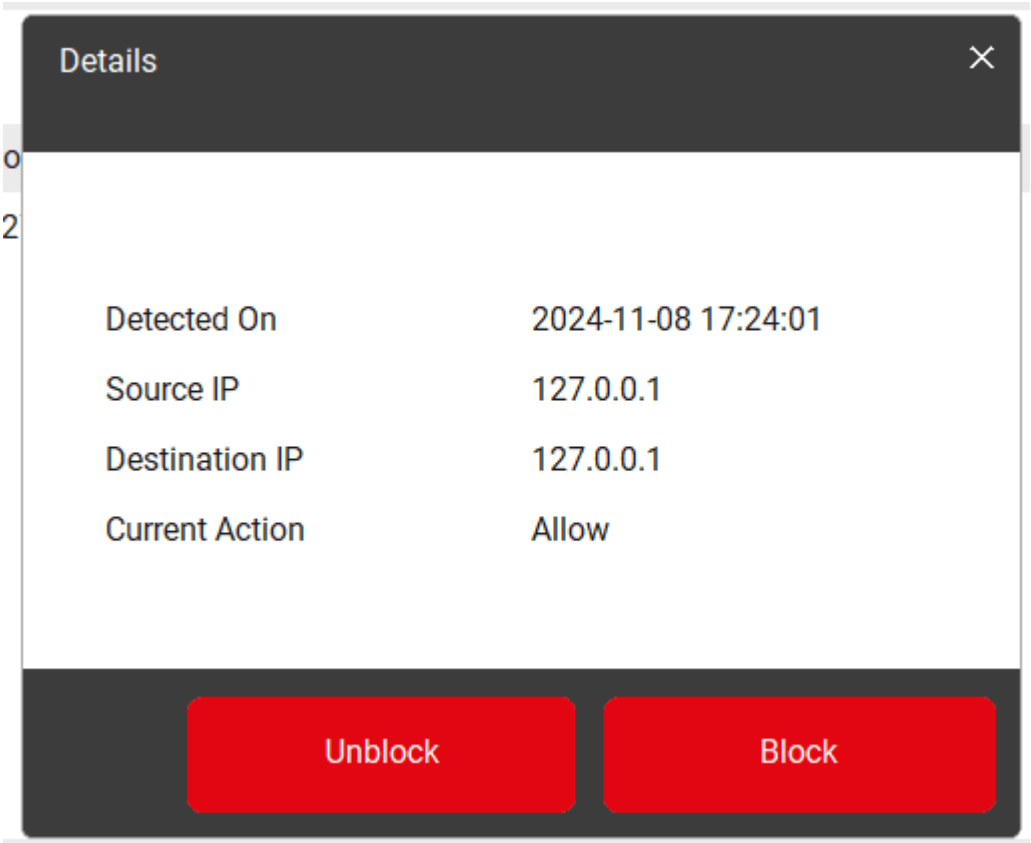
3. Klik tombol “Start” pada sisi kiri program untuk memulai pendeteksian. Program akan memulai mode pendeteksian dengan mendengar pada seluruh antarmuka jaringan untuk mencari *executable*. Ketika pengunduhan atau pengiriman dilakukan dengan protokol tanpa enkripsi seperti HTTP dan FTP, atau dengan *script* pengujian maka hasil pendeteksian akan diberikan beserta sebuah notifikasi seperti berikut.



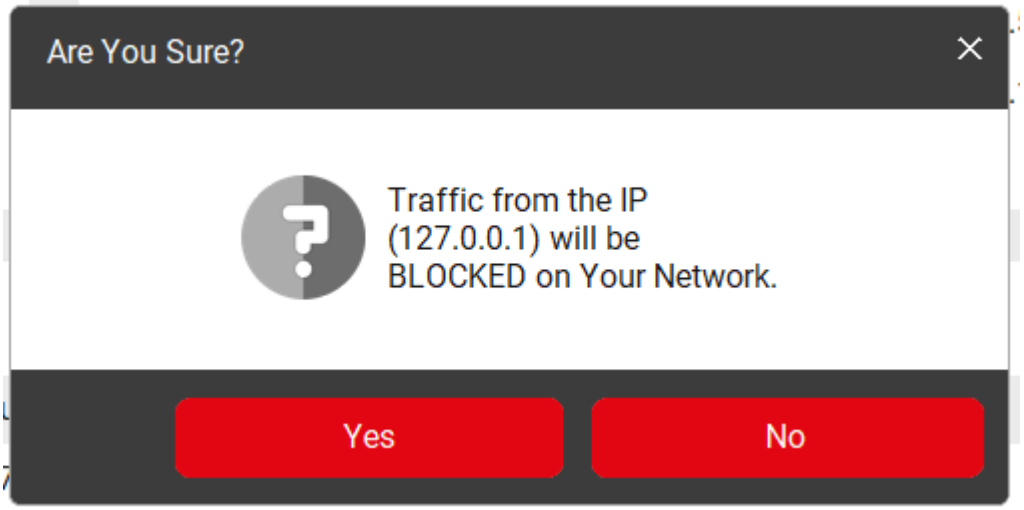
4. Hasil pendeteksian pada *widget Real Time Detection* dapat diklik untuk melakukan tindakan terhadap sumber alamat *IP* yang terdeteksi.

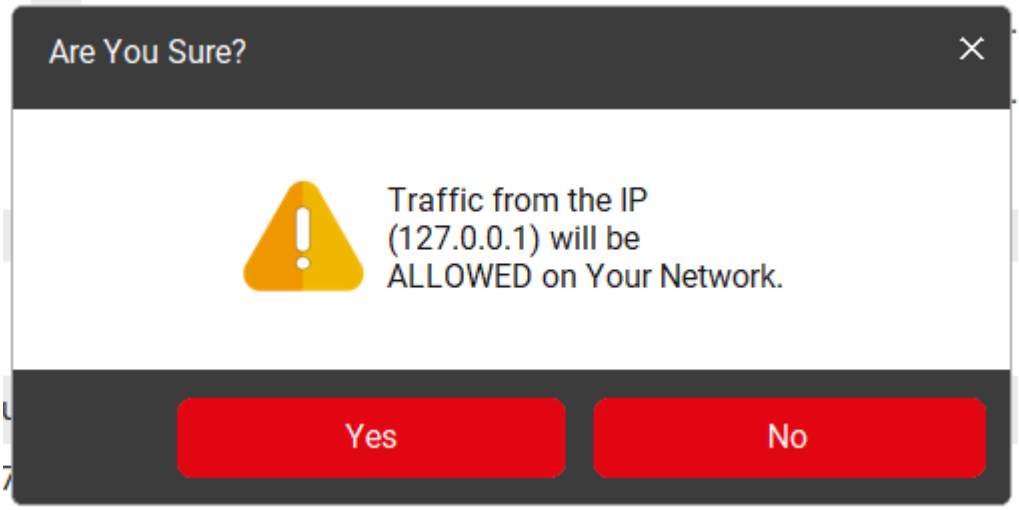


5. Sumber Alamat *IP* dapat diblokir atau dibuka blokir dengan *Block dan Unblock*.



6. Setelah unblock atau block diklik, akan ada window konfirmasi terakhir. Jika block dan yes dipilih maka ip sumber akan ditambahkan rule deny pada firewall perangkat sehingga tidak dapat diakses, jika unblock dan yes maka rule deny pada firewall perangkat akan dihapus sehingga dapat diakses kembali.




Are You Sure?
Traffic from the IP
(127.0.0.1) will be
ALLOWED on Your Network.
Yes
No