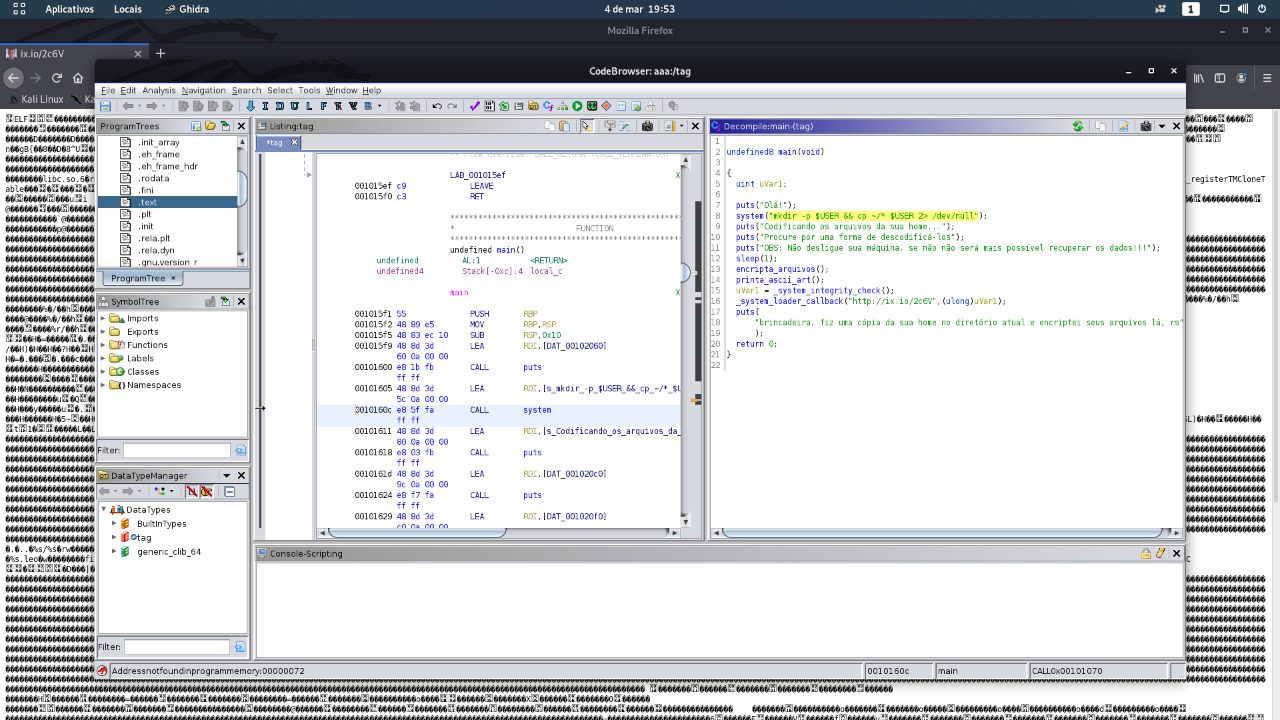
TAG DE ENGENHARIA REVERSA

Analisando o programa no qual o objetivo era descobrir o que ele fazia

Programa utilizado:  
-GHIDRA

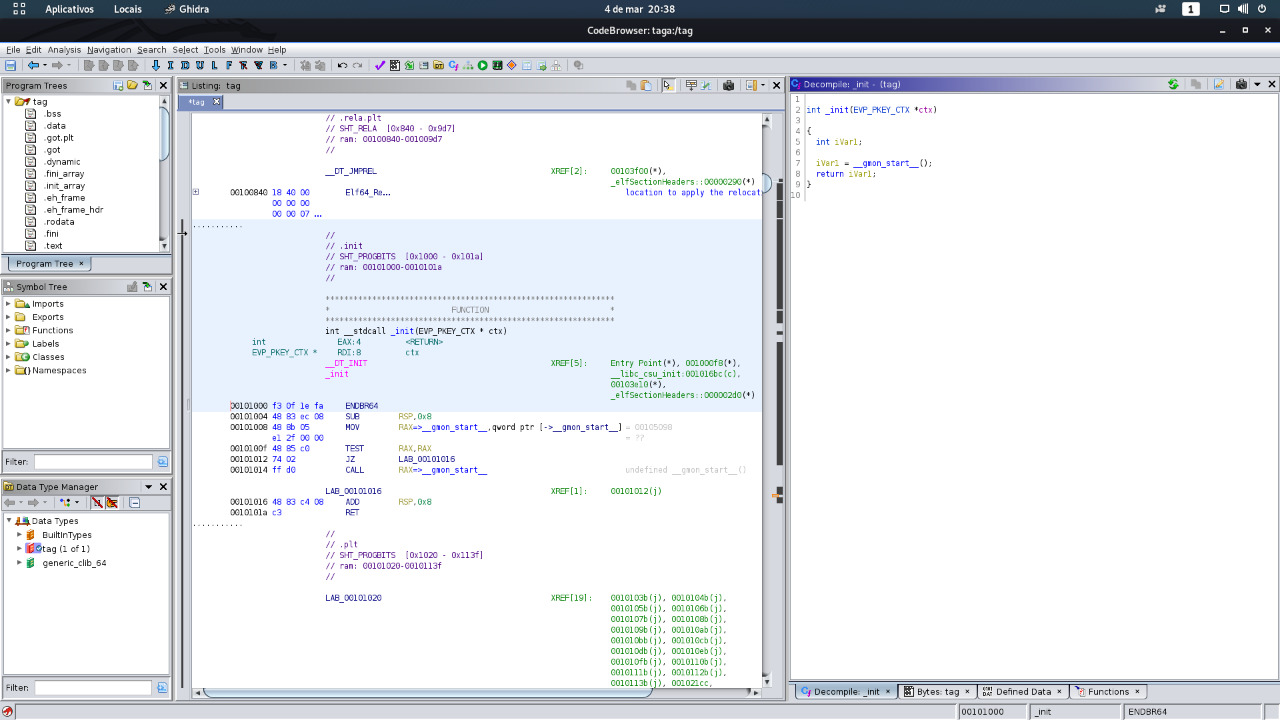
Para que o programa servia:  
-Ele pegava a sua Home e a codificada deixando assim tudo o que tinha nela inacessivel, porem ele fazia uma copia para não ser tudo perdido com a descodificação.

Como era feito

O programa primeiramente escreve um “OLA” na tela e logo em seguida faz uma copia da sua home

Apos isso ele coloca na sua tela que os arquivos estavam sendo criptografados

Em relação a criptografia..



## Ele usou uma função ‘’EVP\_PKEY\_CTX\_new’’ na qual ele pegava umafunção que alocava uma chave de algoritimo publico e a alocava com uma chave privada.

## 

## Logo em seguida isso era printado na tela enquanto a mensagem que ainda tinha uma copia dos seus arquivos da home era lançada.