Fábrica de Noobs

Criptografia – Utilizando MultiObfuscator

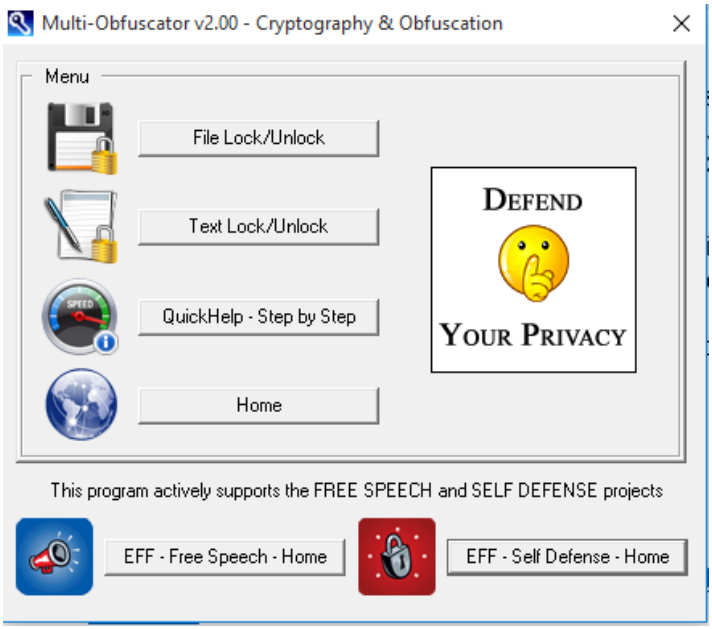
O MultiObfuscator é uma ferramenta criada pelos mesmos desenvolvedores do OpenPuff, destinada a criptografar arquivos, tornando-os inelegíveis a menos que sejam decodificados com o uso de uma senha.

Ao criptografar um arquivo, o programa insere uma série de dados e caracteres aleatórios (denominado ruído), que impedem a leitura do arquivo em questão e só podem ser removidos com uma (ou até 4) senhas, as quais são criptografas utilizando vários métodos open-source de criptografia com hash. Os interessados em mais detalhes do processo, podem consultar o manual oficial aqui: http://embeddedsw.net/doc/MultiObfuscator_Help_EN.pdf.

O programa dispensa instalação:

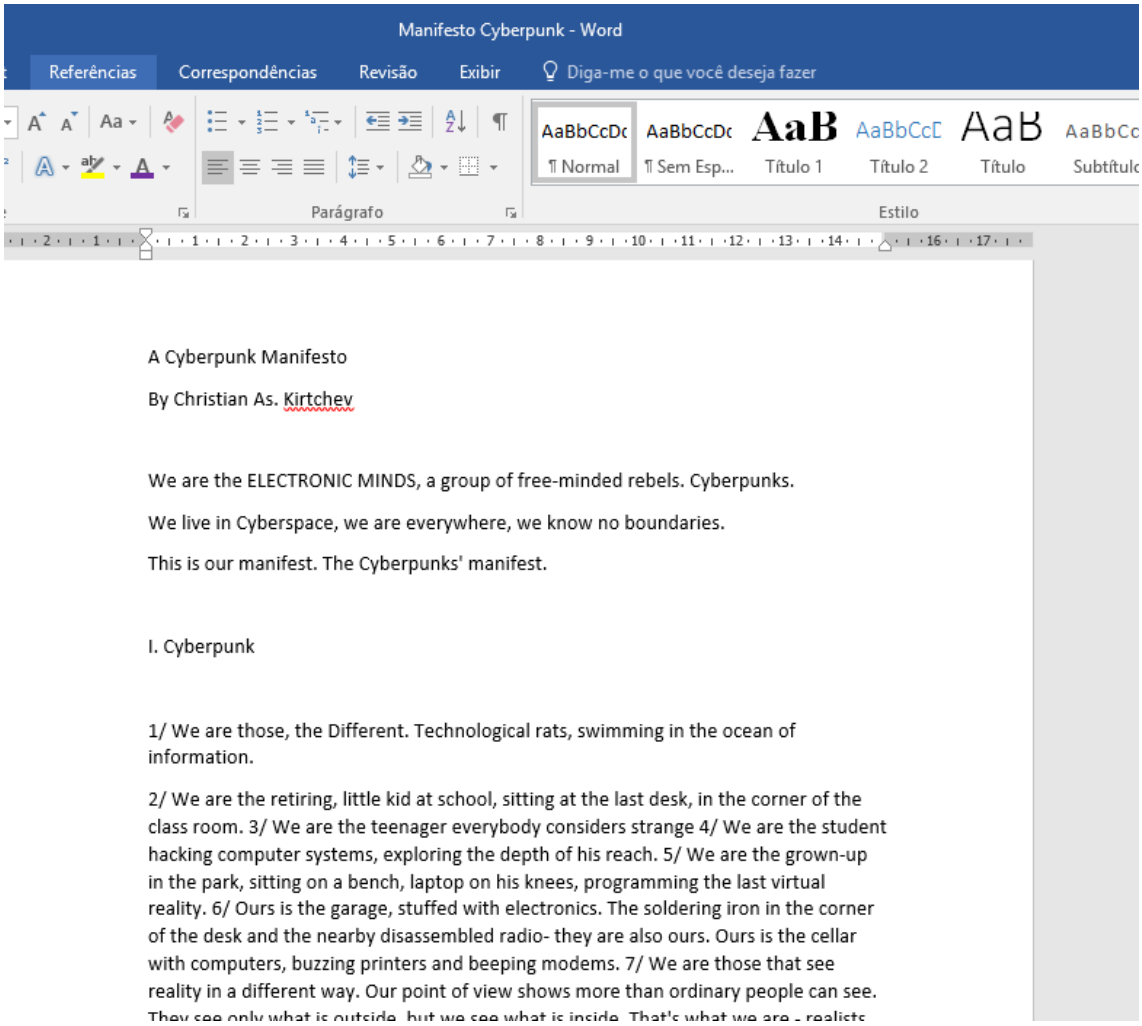
1. Baixe o programa em http://embeddedsw.net/MultiObfuscator_Cryptography_Home.html.
2. Extraia o conteúdo do arquivo Zip.
3. Mova a pasta para o local desado.
4. Inicie o programa executando o arquivo MultiObfuscator.

Essa é a interface do programa:

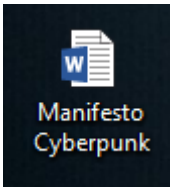


A primeira opção permite trabalhar com qualquer tipo de arquivo. A segunda funciona dentro dos mesmos padrões, mas é voltada para texto.

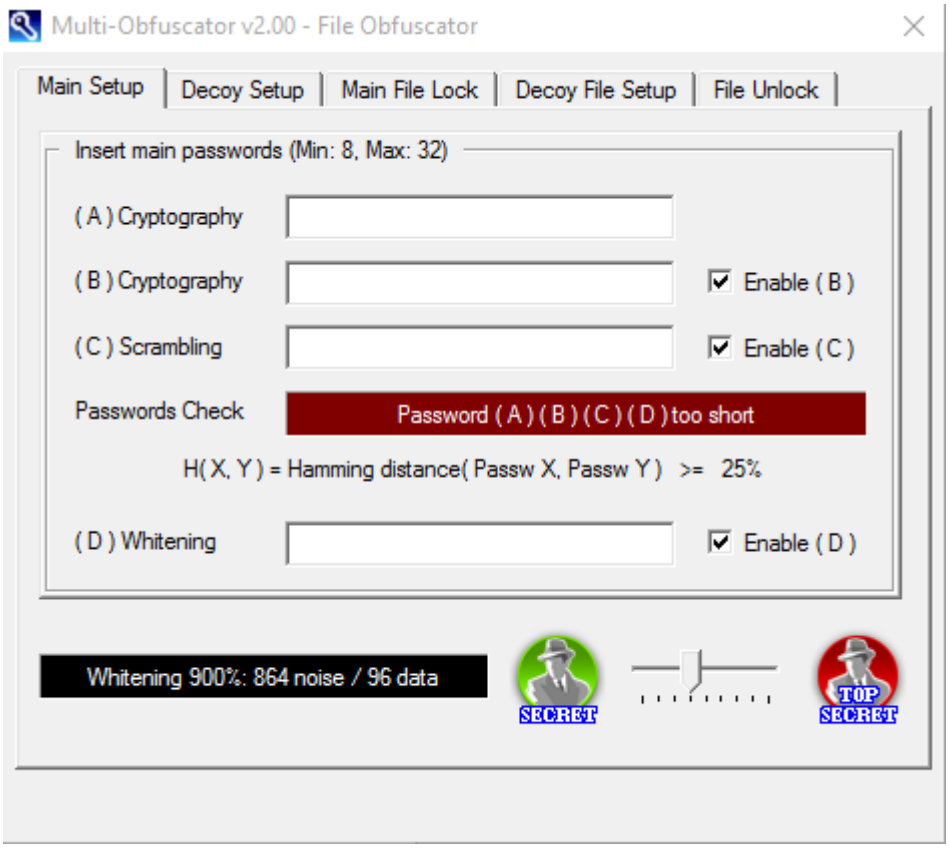
Vamos tomar como exemplo o seguinte documento do Word:



Ele está localizado na área de trabalho, e pode ser aberto normalmente, como qualquer arquivo:



Para codificarmos o mesmo, clicamos em File Lock/Unlock. Essa é a janela que encontramos:

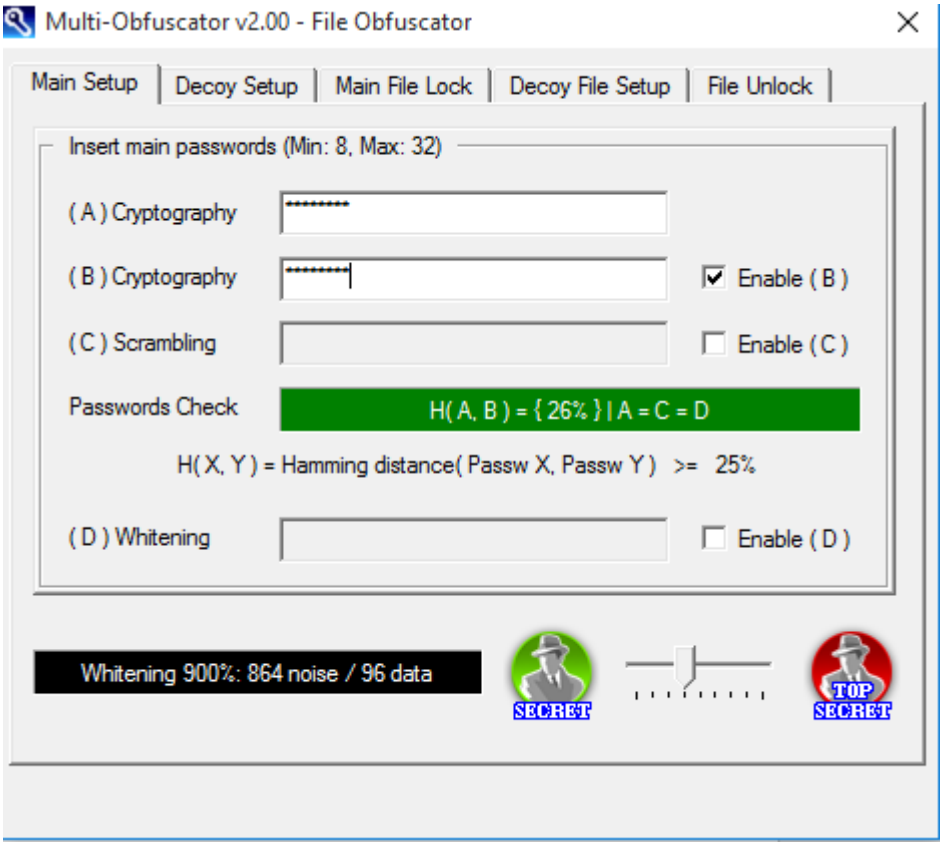


As janelas Main Setup e Main File Lock são usadas para criptografar o arquivo em questão.

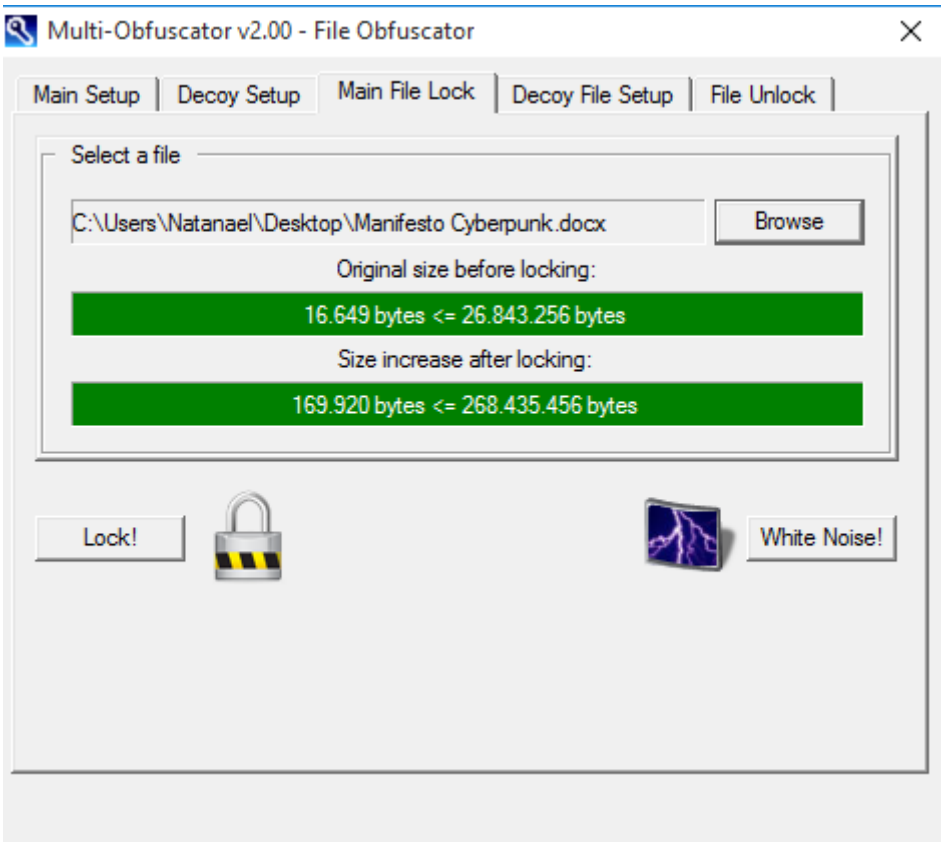
Na primeira janela, insira todas as senhas que deseja usar para proteger o arquivo. São permitidas até 4 senhas, sendo elas de 8 a 32 caracteres.

Logo abaixo, podemos escolher o nível de segurança. Quanto maior o nível, maior será a porcentagem de ruído (noise) inserido no arquivo em questão. Recomendo deixar como está, uma vez será necessário informar o nível de criptografia para revelar o arquivo.

No nosso exemplo, usaremos “12345678” como senha A e “abcdefgh” como senha B. Mantermos o nível de segurança em 900%, que é o padrão do programa. ~~Não use essas senhas numa situação real.~~



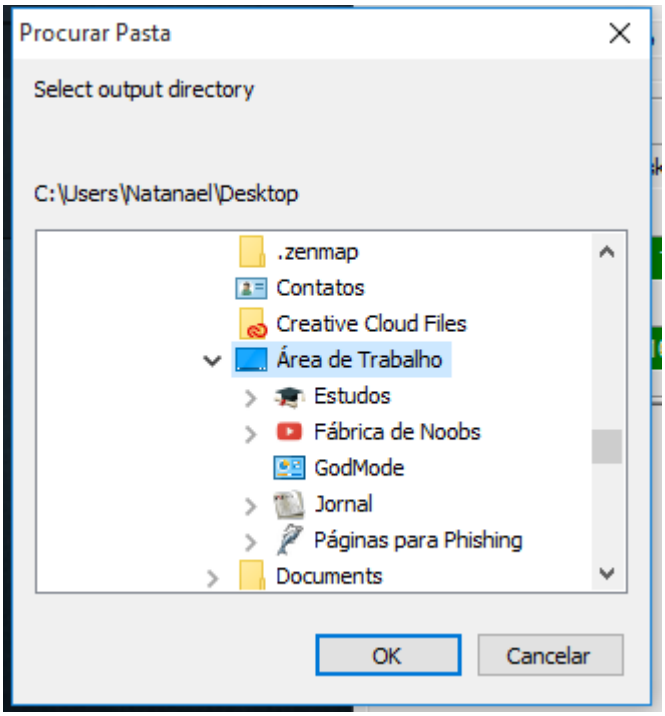
Feito isso, memorizamos as senhas e o nível de segurança. Em seguida, vamos para Main File Lock:



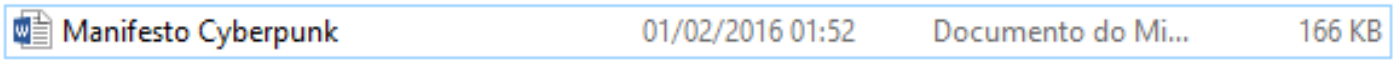
Clicando em Browse podemos escolher o arquivo que desejamos criptografar.

Se as duas barras ficarem em verde significa que tudo está pronto para ser criptografado. Clique em Lock!.

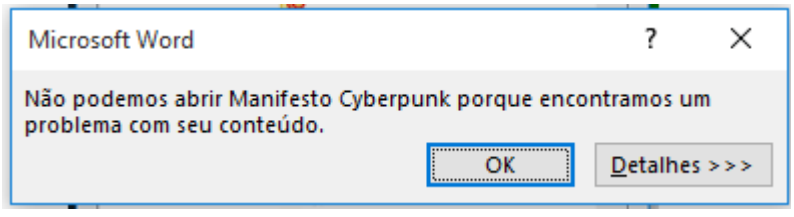
Uma janela irá se abrir, na qual deve-se escolher o diretório no qual o arquivo criptografado será salvo. Ele não pode ser o mesmo diretório do arquivo atual.



Clicamos em OK, e nosso arquivo criptografado é salvo no diretório escolhido:



Isso é o que acontece quando tentamos abrir um arquivo protegido com o MultiObfuscator:

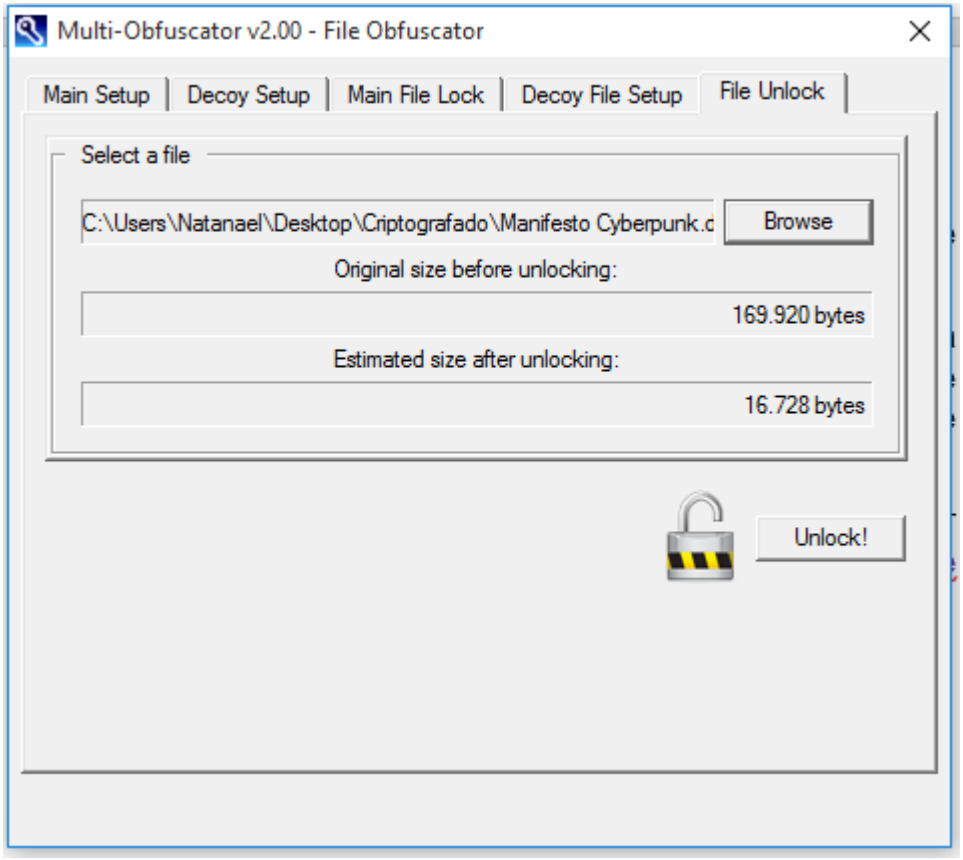


Qualquer arquivo que seja sempre apresentará uma mensagem de erro equivalente ao programa que tentar abri-lo. Métodos para recuperá-lo serão sempre inviáveis. A única forma

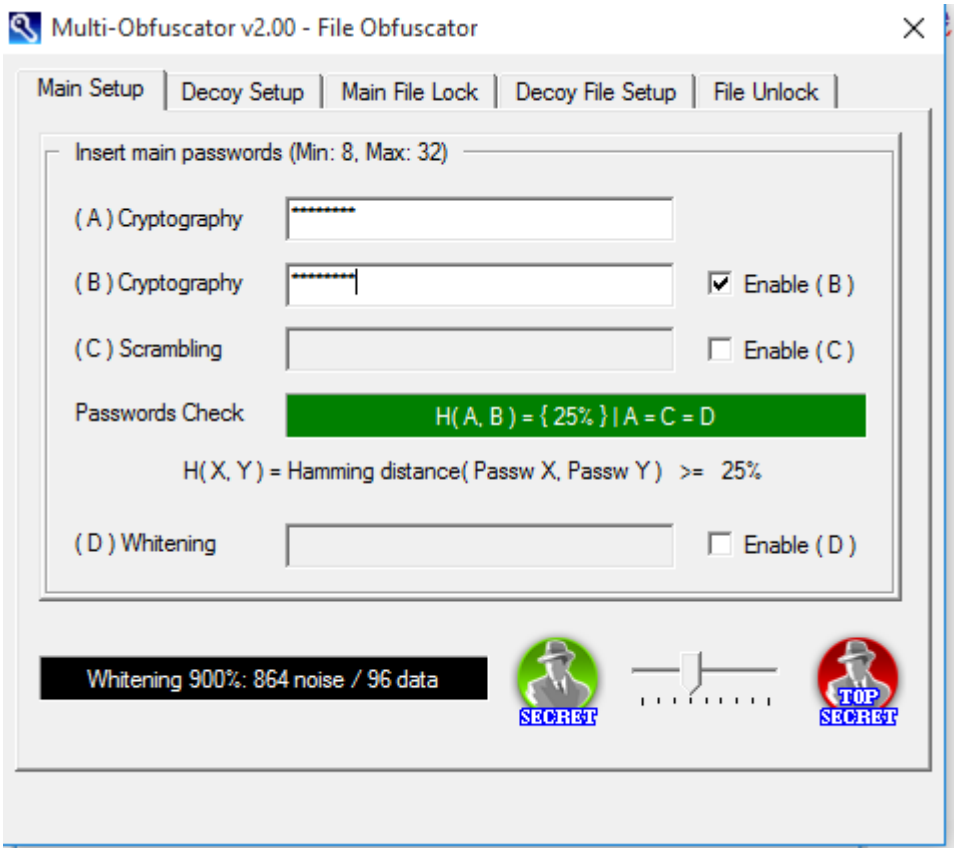
de acessá-lo novamente é utilizando o próprio MultiObfuscator e inserindo as informações de segurança.

Se tivéssemos clicado em White Noise!, o programa iria gerar um arquivo de mesmo tamanho e formato, mas cheio de ruído, sem nenhum traço do arquivo original. Um atacante que tentasse recuperá-lo não iria encontrar nada.

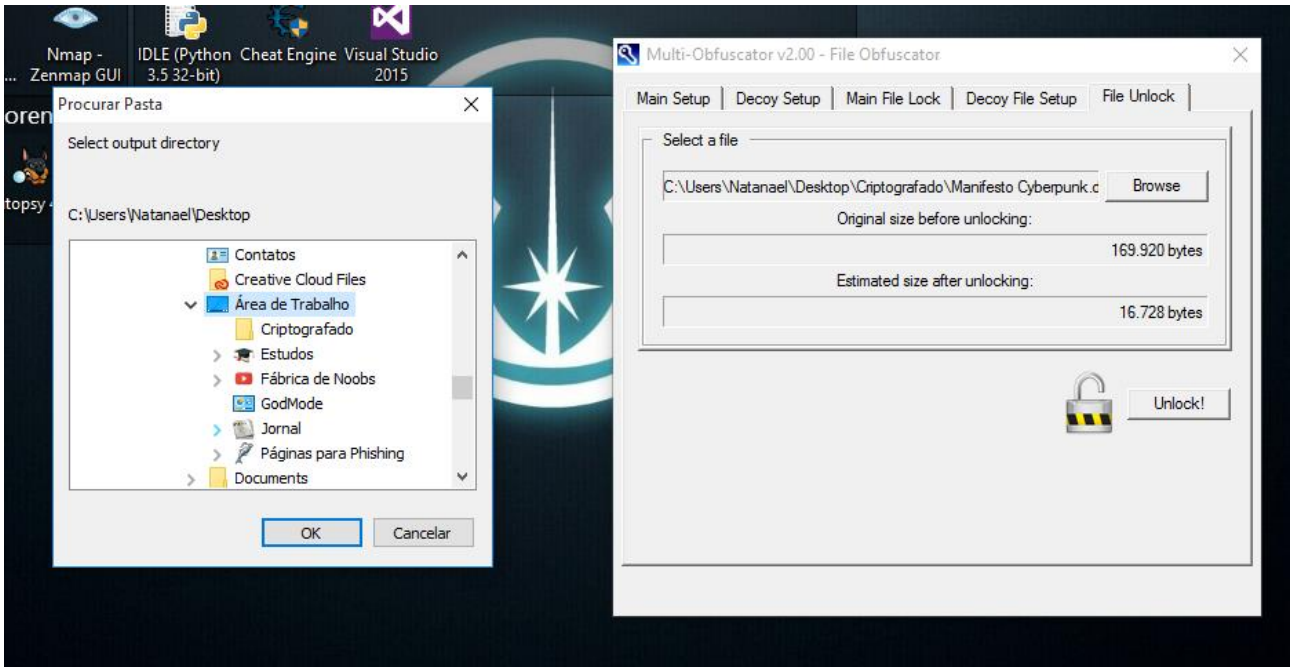
Para recuperar um arquivo criptografado, devemos abrir o MultiObfuscator e ir na aba File Unlock. Clicamos em Browse e escolhemos o arquivo.



Em seguida, voltamos na aba Main Setup e lá inserimos todas as senhas e o nível de criptografia do arquivo em questão, exatamente da forma como fizemos para criptografá-lo.

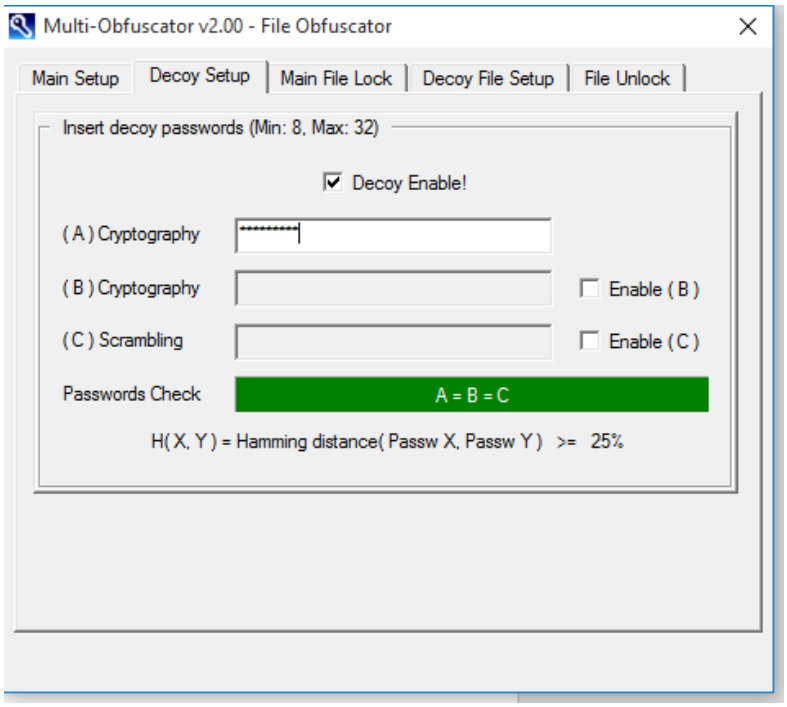


Depois, vamos novamente em File Unlock e clicamos em Unlock. Selecionamos o diretório, clicamos em OK e o arquivo original será recuperado.

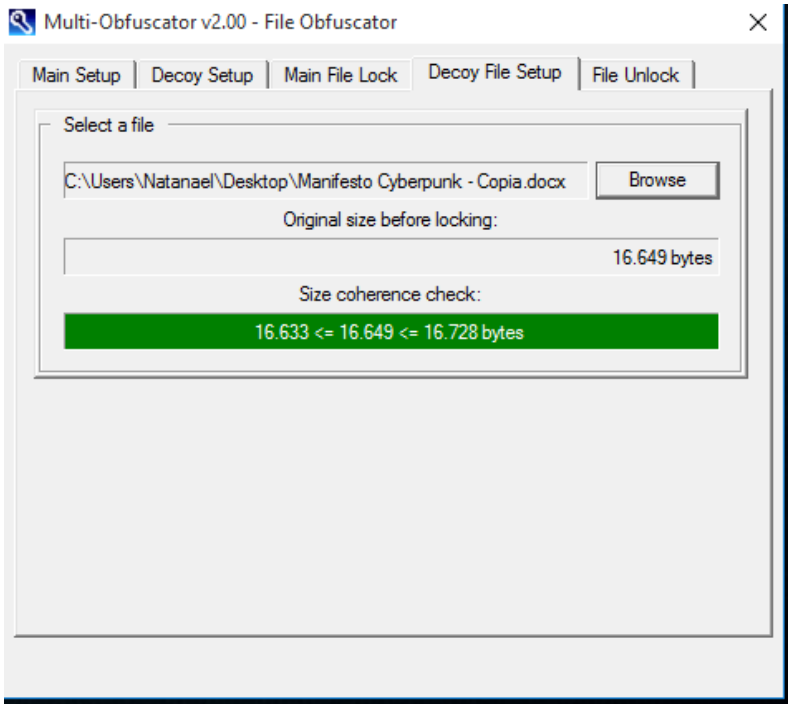


O programa oferece ainda a possibilidade de inserirmos uma Decoy, que é um “arquivo falso”, o qual será extraído caso colocarmos outra senha especificada. Para isso, vamos no

menu Decoy Setup e definimos um conjunto de até 3 senhas para extrair.



Depois, vamos no menu Decoy File Setup e escolhemos o arquivo falso. Esse arquivo precisa ter exatamente o mesmo tamanho do arquivo original. Talvez seja uma boa ideia inserir, no lugar da Decoy, um arquivo de WhiteNoise.



Feito isso, basta seguir o procedimento já feito anteriormente para criar o arquivo criptografado.