

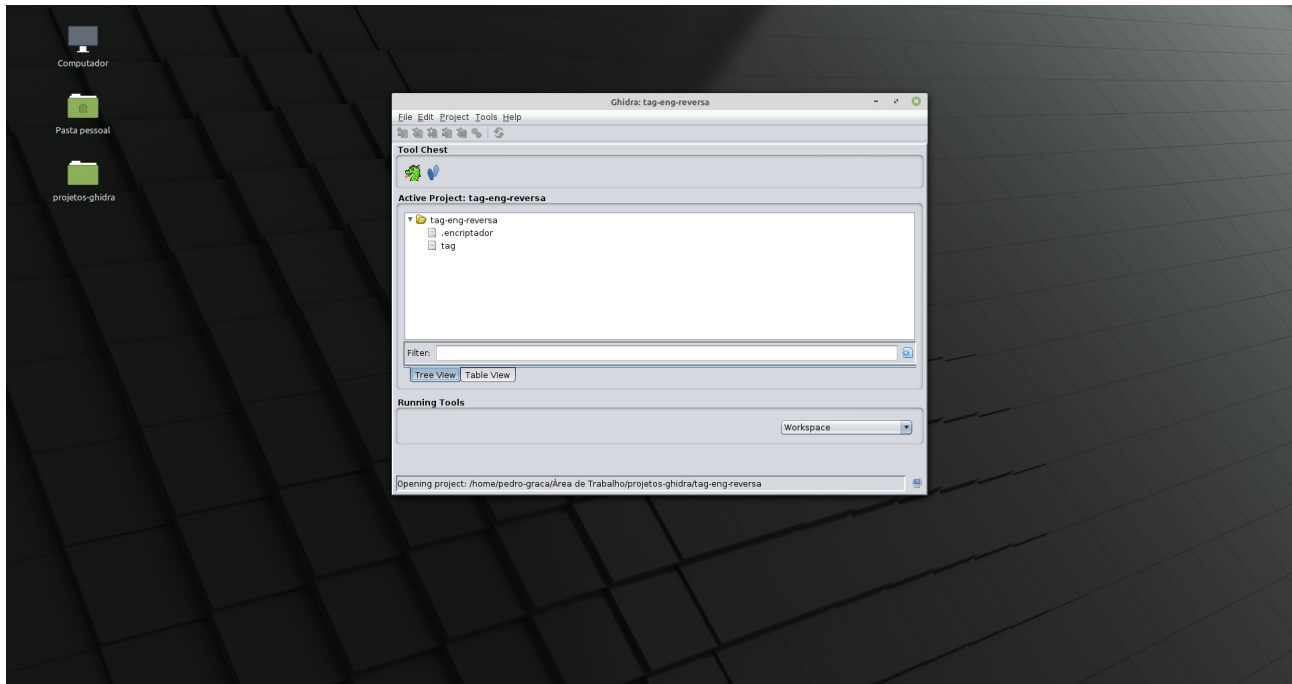
UFRJ

[tag-parte1-engenharia reversa]

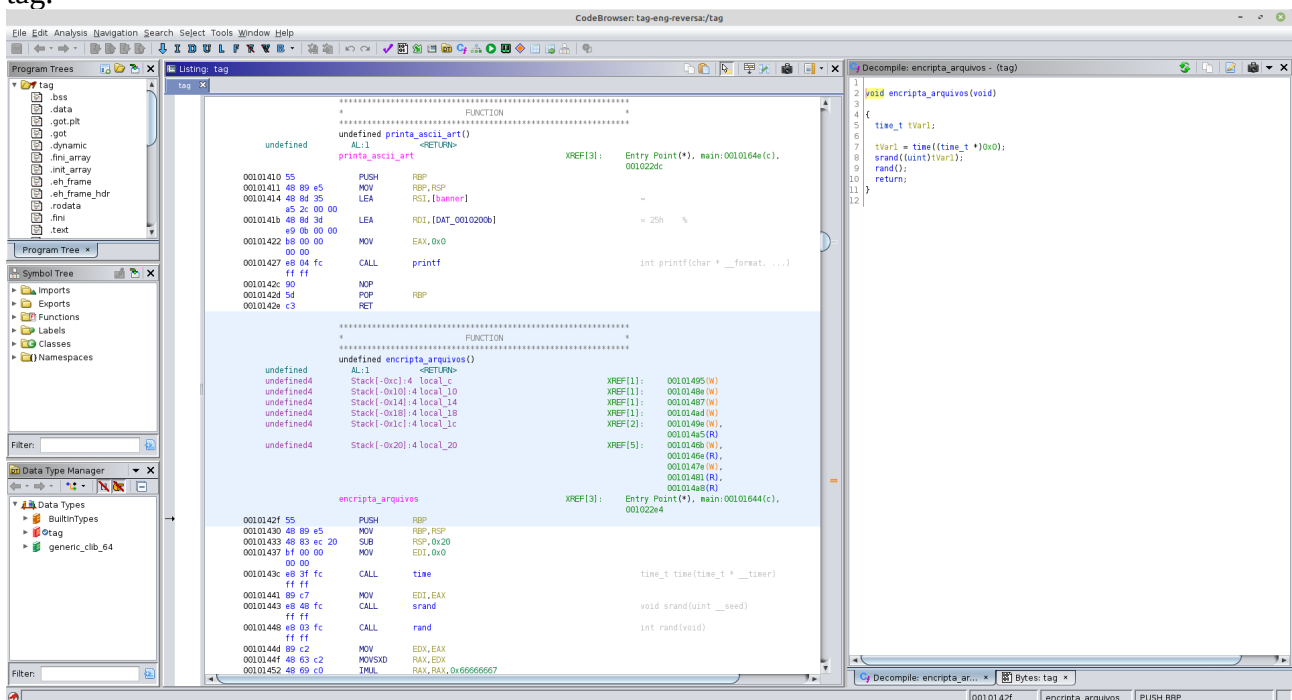
Autor: Pedro Jullian Medina Torres Graça

Processo Seletivo GRIS

Aplicador: Leonardo Ventura



Aqui mostra onde comecei. Usei o Ghidra por ser mais simples. Apenas cliquei duas vezes sobre tag.



Desci a “listing” seguindo o código até encontrar a função “encrypta_arquivos”

Ela não pareceu nada demais, basicamente está colocando um valor pseudoaleatório em tvar1.

```

1 void _system_integrity_check(void)
2 {
3     uint iVar1;
4     int iVar2;
5     FILE * __stream;
6
7     iVar2 = rand();
8     iVar1 = iVar2 % 5 + 1;
9     __stream = fopen("/tmp/key", "w+");
10    fprintf(__stream, "%d\n", (ulong) iVar1);
11    fclose(__stream);
12    return (ulong) iVar1;
13 }

```

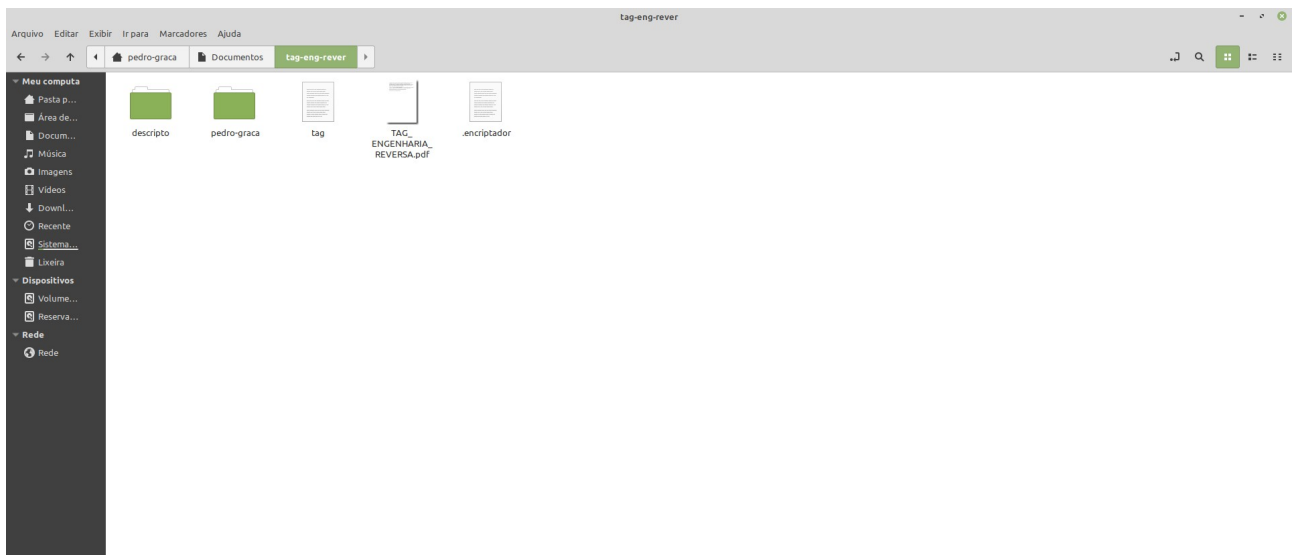
Descendo mais encontrei esse outra função que parece fazer parte da anterior. Pelo o que entendi ela faz com que o valor aleatorio gerado anteriormente fique restrito de 1 a 5 e é colocado dentro de um arquivo key na pasta temporaria.

```

1 void _system_loader_callback(undefined8 param_1, uint param_2)
2 {
3     long in_FS_OFFSET;
4     char local_98[136];
5     long local_10;
6
7     local_10 = *(long *) (in_FS_OFFSET + 0x28);
8     download_file_from_url(param_1, "encryptador", "encryptador");
9     system(local_98);
10    sleep(2);
11    if (local_10 != *(long *) (in_FS_OFFSET + 0x28)) {
12        /* WARNING: Subroutine does not return */
13        __stack_chk_fail();
14    }
15    return;
16 }

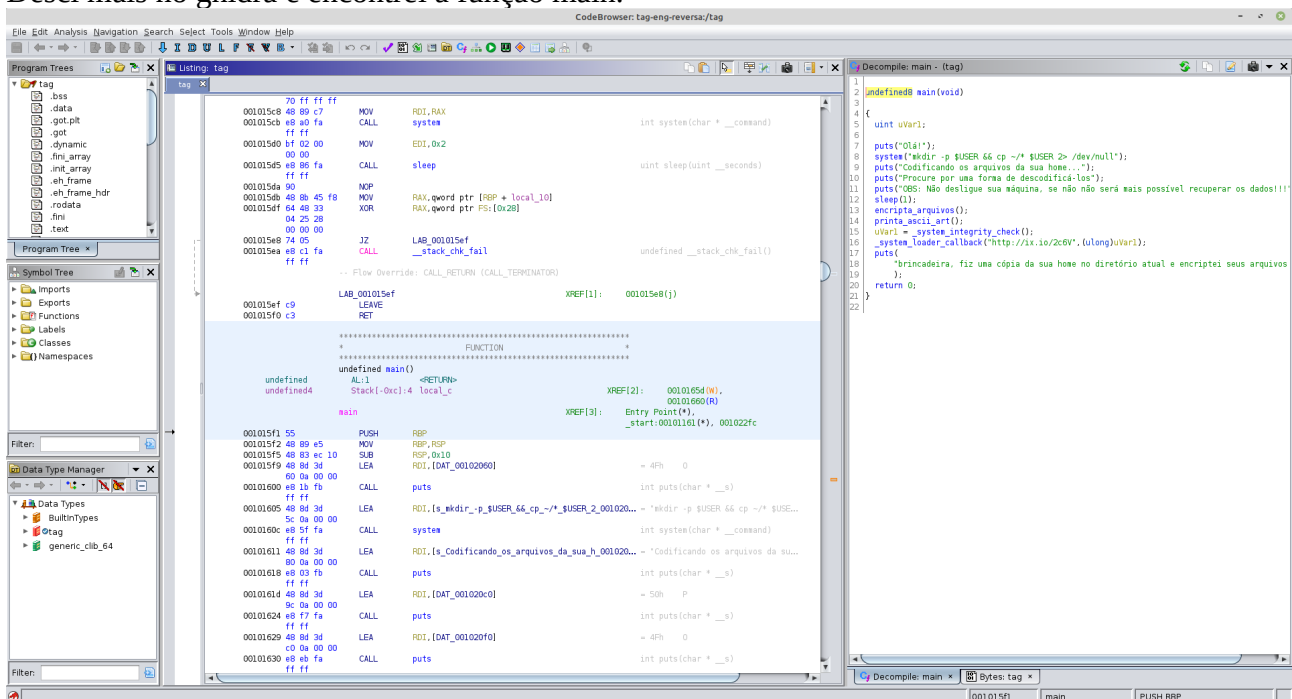
```

Mais uma vez descendo encontrei essa função. Pelo nome “donwload_file_from_url” e por leituras de curl supus que essa parte era resposavel por baixar um arquivo chamado de .encryptador.



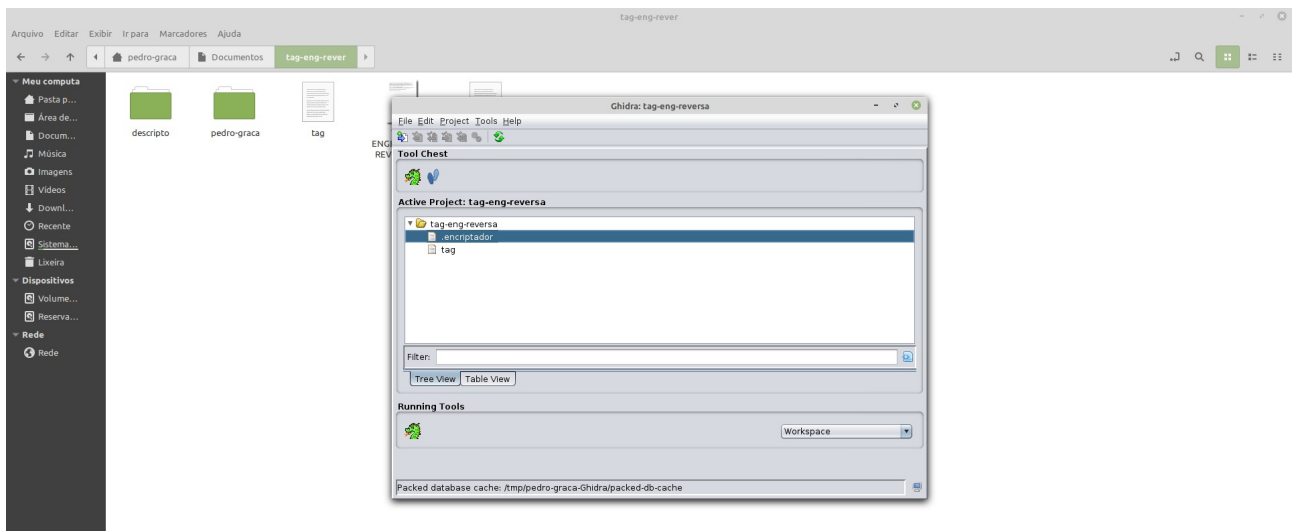
Pomos ver ai o arquivo baixado.

Desci mais no ghidra e encontrei a função main.

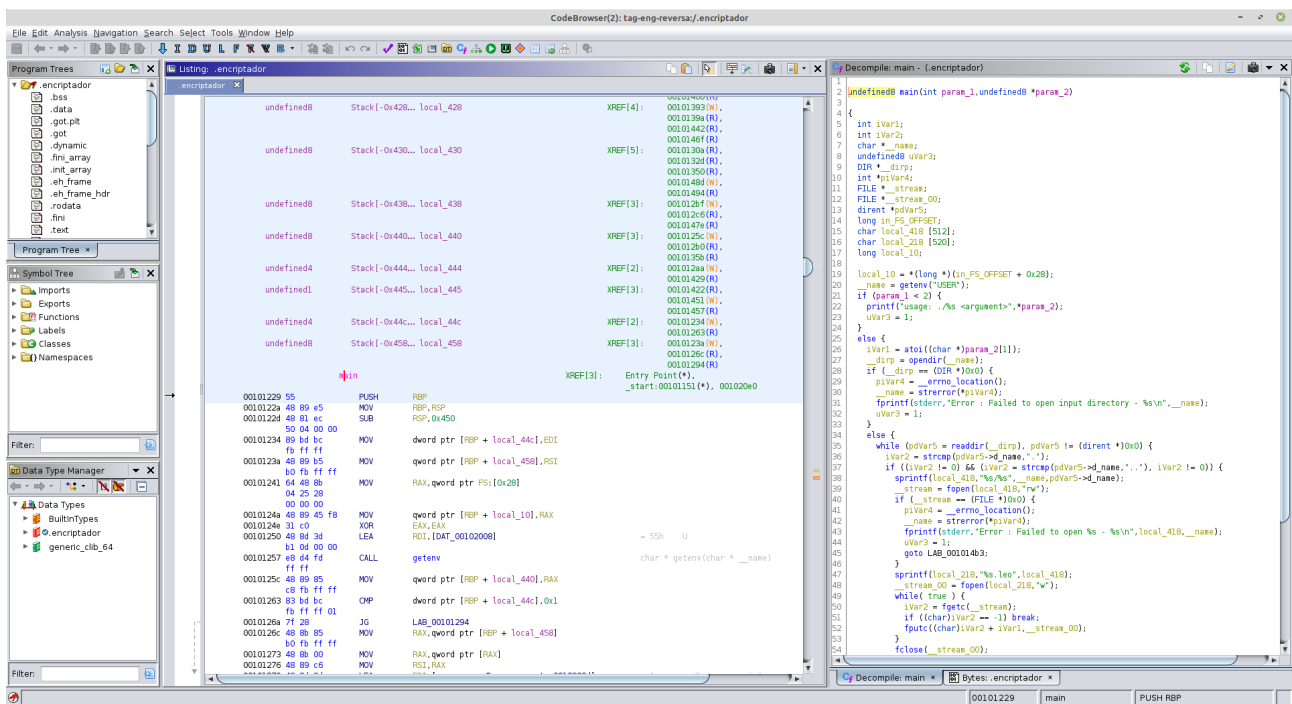


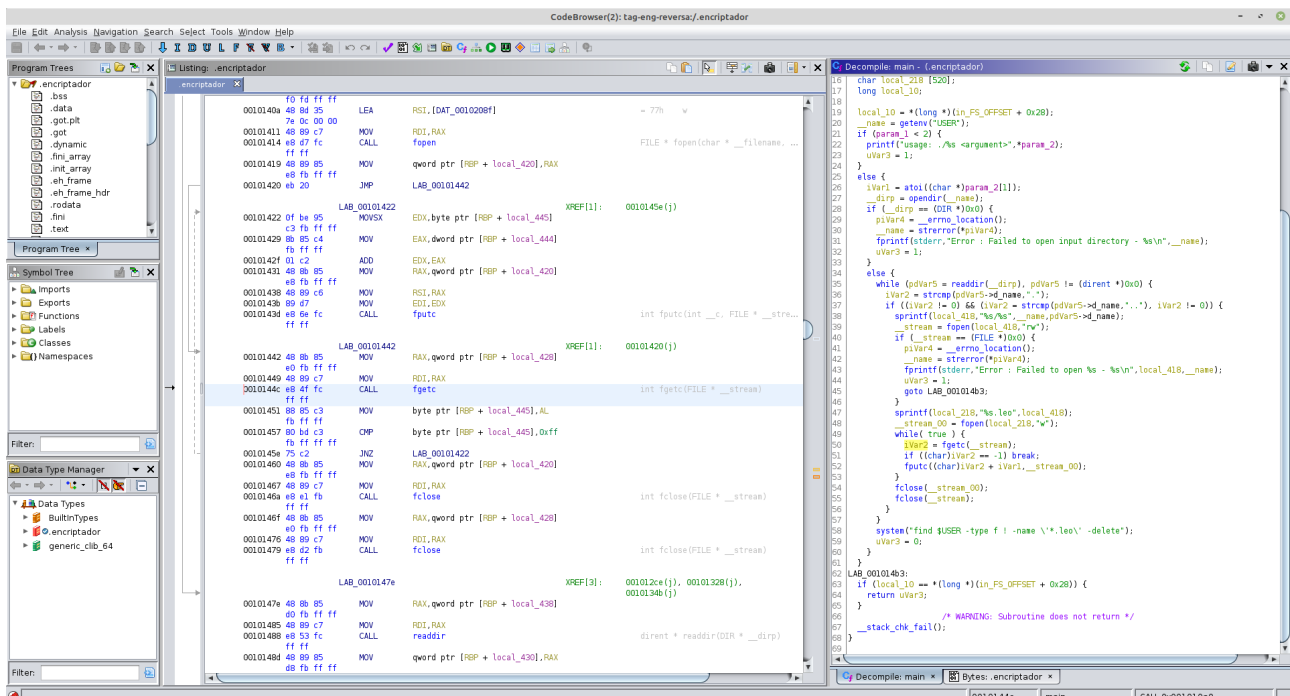
Nela deu pra entender como o programa funcionava. Faltava entender como o arquivo .encriptador funcionava, uma vez que dá para ver que ele era executado (duas imagens pra cima.)

Usei o ghidra em cima do arquivo também.



Nele, pelo mesmo método de antes, onde vi a sua main





na linha 39 podemos “ver” que é ele pegado o conteúdo pseudoaleatório em key e na linha 49 a 53 podemos ver a essência do encriptador

```

while( true ) {
    iVar2 = fgetc(__stream);
    if ((char)iVar2 == -1) break;
    fputc((char)iVar2 + iVar1, __stream_00);
}

```

Ele basicamente soma o valor aleatório (mas constante) a todos os valores. Assim, para descriptografar, basta subtrair desse valor no arquivo key.