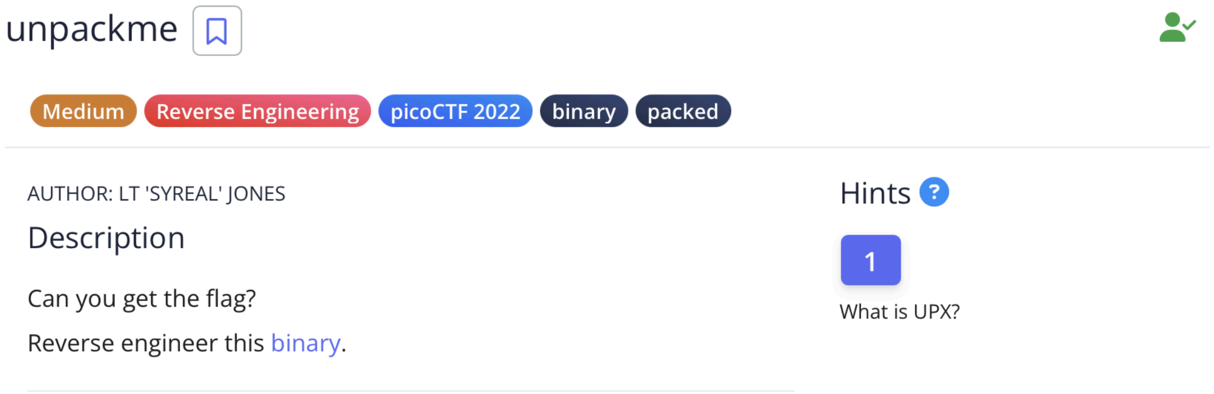


unpackme

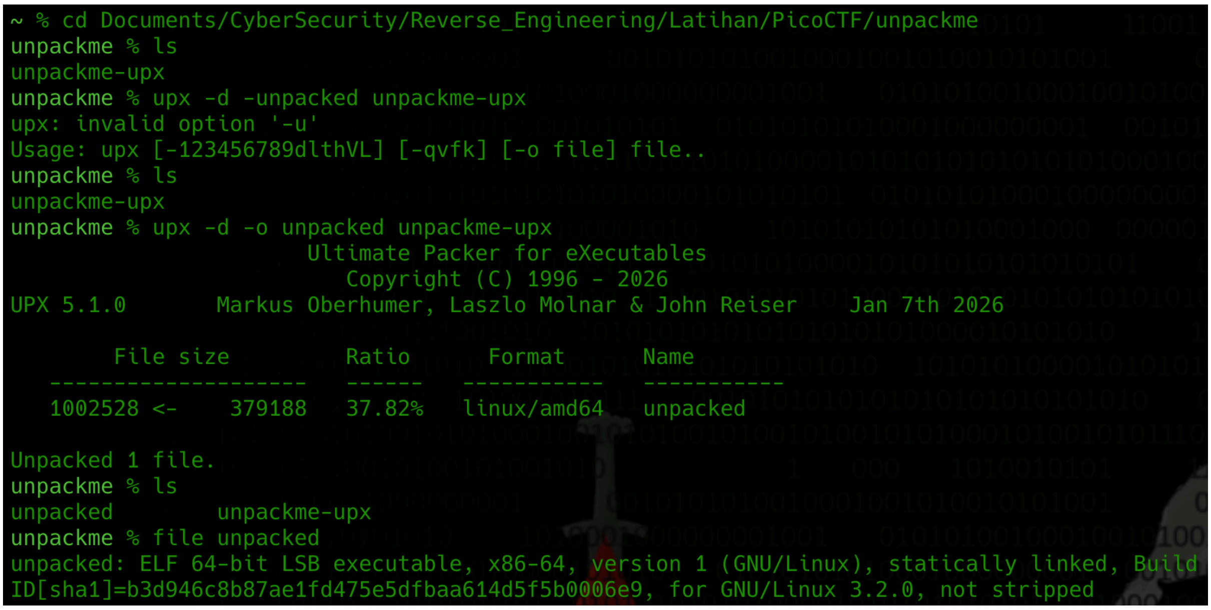
AUTHOR: LT 'SYREAL' JONES

Description

Can you get the flag?

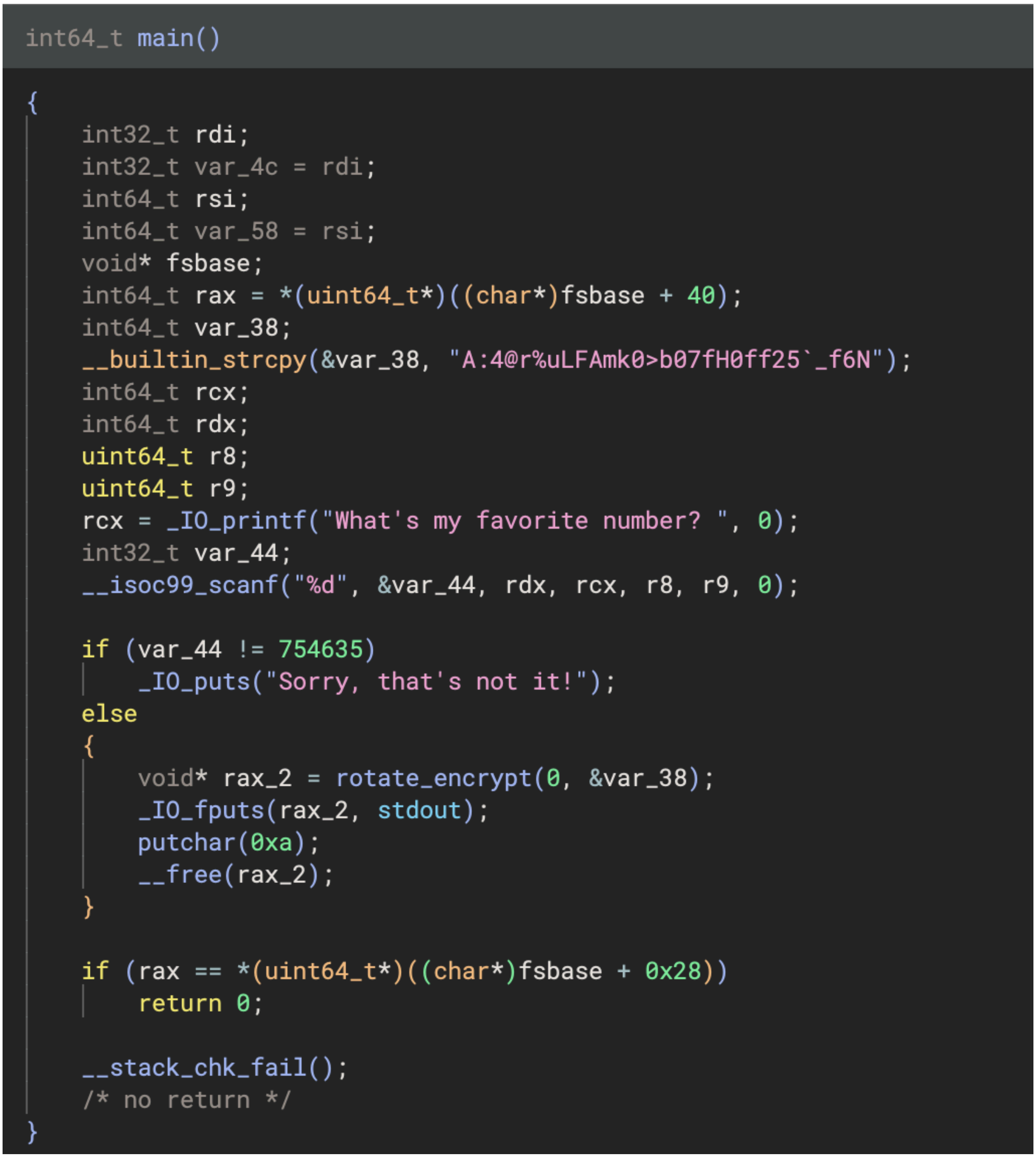
Reverse engineer this binary.

Solusi :



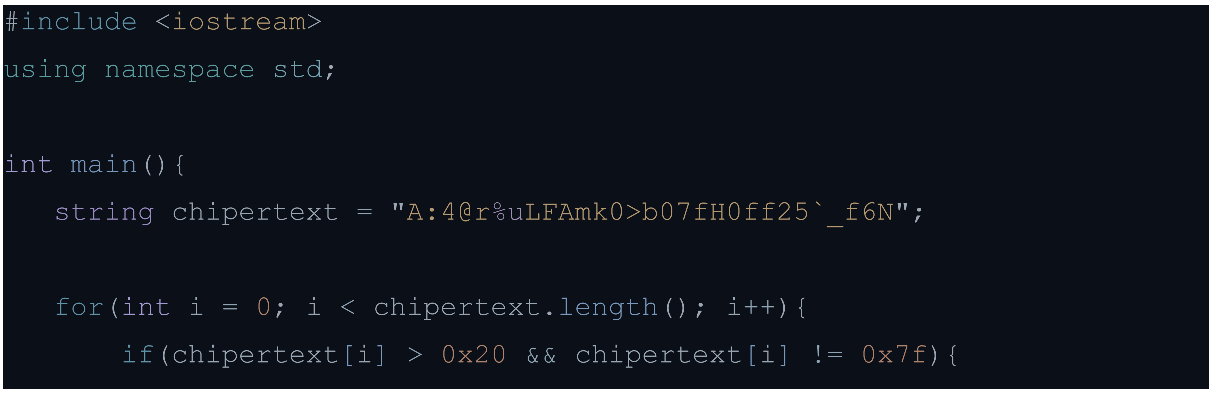
```
~ % cd Documents/CyberSecurity/Reverse_Engineering/Latihan/PicoCTF/unpackme
unpackme % ls
unpackme-upx
unpackme % upx -d -unpacked unpackme-upx
upx: invalid option '-u'
Usage: upx [-123456789dlthVL] [-qvfk] [-o file] file..
unpackme % ls
unpackme-upx
unpackme % upx -d -o unpacked unpackme-upx
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2026
UPX 5.1.0       Markus Oberhumer, Laszlo Molnar & John Reiser    Jan 7th 2026

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
   1002528 <-    379188   37.82%   linux/amd64   unpacked

Unpacked 1 file.
unpackme % ls
unpacked        unpackme-upx
unpackme % file unpacked
unpacked: ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux), statically linked, Build
ID[sha1]=b3d946c8b87ae1fd475e5dfbaa614d5f5b0006e9, for GNU/Linux 3.2.0, not stripped
```

Langsung ke binary ninja dan menuju ke fungsi main.

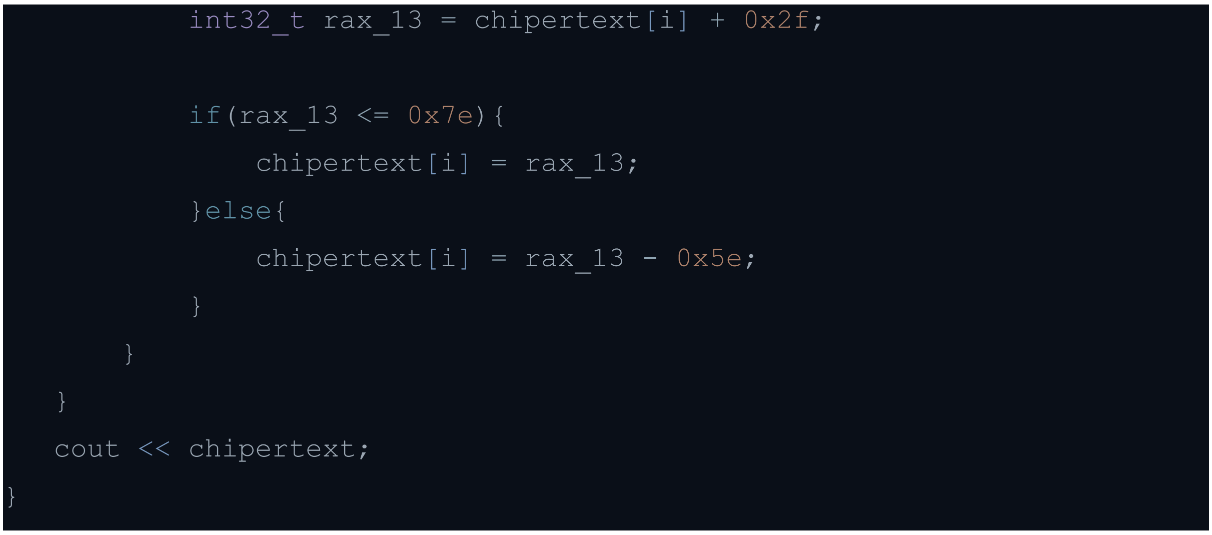


```
int64_t main()

{
    int32_t rdi;
    int32_t var_4c = rdi;
    int64_t rsi;
    int64_t var_58 = rsi;
    void* fsbase;
    int64_t rax = *(uint64_t*)((char*)fsbase + 40);
    int64_t var_38;
    __builtin_strcpy(&var_38, "A:4@r%uLFAmk0>b07fH0ff25`_f6N");
    int64_t rcx;
    int64_t rdx;
    uint64_t r8;
    uint64_t r9;
    rcx = _IO_printf("What's my favorite number? ", 0);
    int32_t var_44;
    __isoc99_scanf("%d", &var_44, rdx, rcx, r8, r9, 0);

    if (var_44 != 754635)
        _IO_puts("Sorry, that's not it!");
    else
    {
        void* rax_2 = rotate_encrypt(0, &var_38);
        _IO_fputs(rax_2, stdout);
        putchar(0xa);
        __free(rax_2);
    }

    if (rax == *(uint64_t*)((char*)fsbase + 0x28))
        return 0;

    __stack_chk_fail();
    /* no return */
}
```

terdapat fungsi rotate_encrypt langsung saja kita solve dengan C++.



```
#include <iostream>
using namespace std;

int main(){
   string chipertext = "A:4@r%uLFAmk0>b07fH0ff25`_f6N";

   for(int i = 0; i < chipertext.length(); i++){
       if(chipertext[i] > 0x20 && chipertext[i] != 0x7f){
```



```
            int32_t rax_13 = chipertext[i] + 0x2f;

            if(rax_13 <= 0x7e){
                chipertext[i] = rax_13;
            }else{
                chipertext[i] = rax_13 - 0x5e;
            }
        }
    }
    cout << chipertext;
}
```

output : picoCTF{up><_m3_f7w_77ad107e}