Description

Can you get the flag?Reverse engineer this binary.

Hints

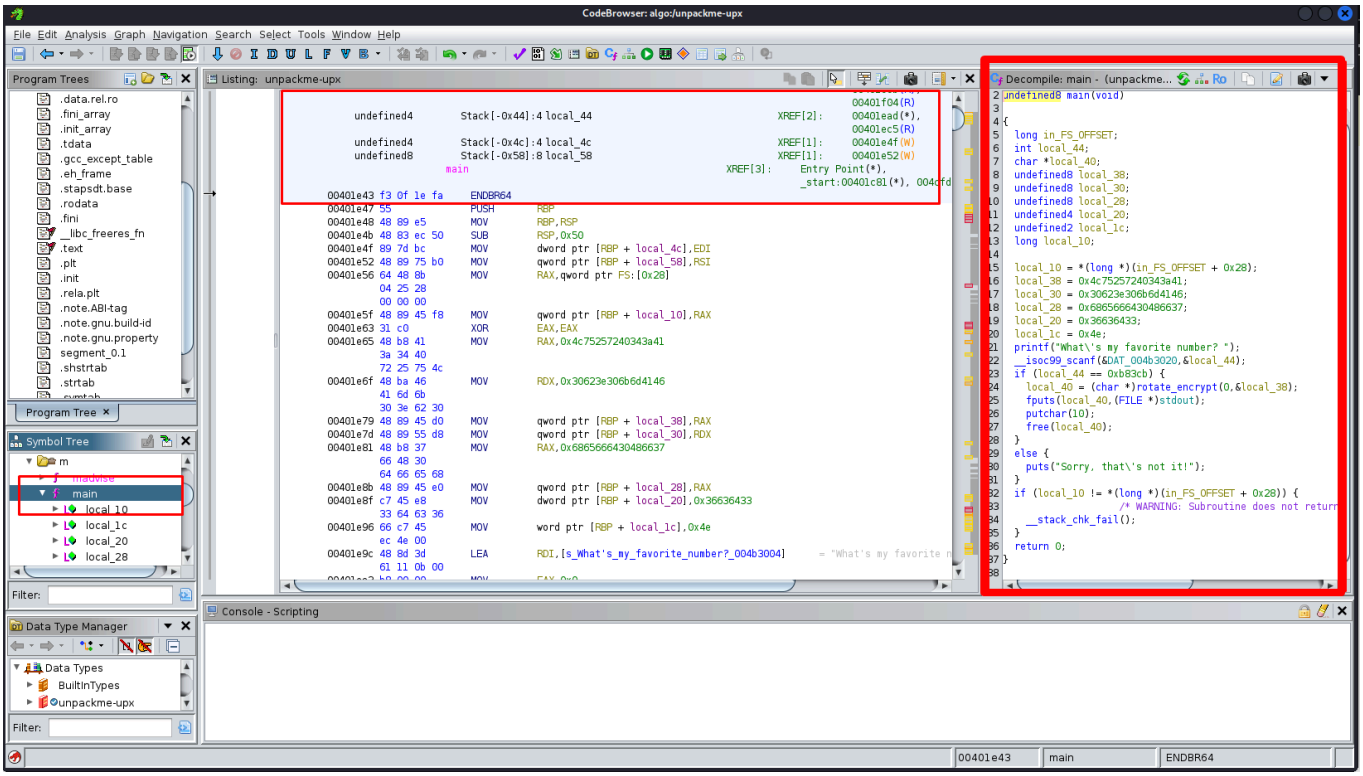
- What is UPX?

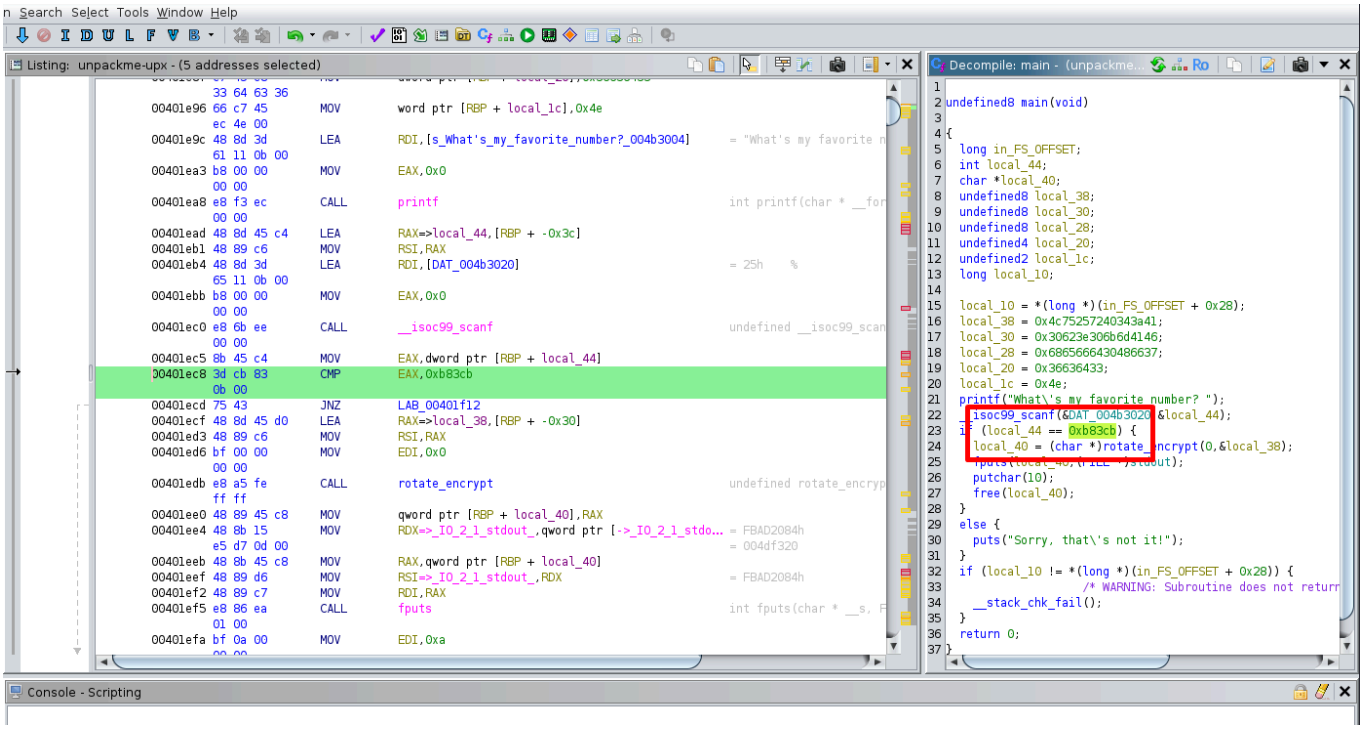
Solución

```
┌──(kali㉿kali)-[~/…/parciales/parcial_03/parte_04_reversing_02/unpackme]
└─$ file unpackme-upx
unpackme-upx: ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux),
statically linked, no section header

┌──(kali㉿kali)-[~/…/parciales/parcial_03/parte_04_reversing_02/unpackme]
└─$ ./unpackme-upx
What's my favorite number? 1
Sorry, that's not it!

┌──(kali㉿kali)-[~/…/parciales/parcial_03/parte_04_reversing_02/unpackme]
└─$ upx -dk unpackme-upx
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2024
UPX 4.2.4       Markus Oberhumer, Laszlo Molnar & John Reiser    May 9th
2024

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
   1006445 <-    379188   37.68%   linux/amd64   unpackme-upx

Unpacked 1 file.

┌──(kali㉿kali)-[~/…/parciales/parcial_03/parte_04_reversing_02/unpackme]
└─$ ls
unpackme.md  unpackme-upx  unpackme-upx.~

┌──(kali㉿kali)-[~/…/parciales/parcial_03/parte_04_reversing_02/unpackme]
└─$ ghidra unpackme-upx
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -
Dswing.aatext=true
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -
```

```
Dswing.aatext=true
```

Utilizando `Ghidra`:






```
┌──(kali㉿kali)-[~/…/parciales/parcial_03/parte_04_reversing_02/unpackme]
└─$ python3
Python 3.12.7 (main, Nov  8 2024, 17:55:36) [GCC 14.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
```

```
>>> 0xb83cb
754635
>>>
┌──(kali㉿kali)-[~/…/parciales/parcial_03/parte_04_reversing_02/unpackme]
└─$ ./unpackme-upx
What's my favorite number? 754635
picoCTF{up><_m3_f7w_5769b54e}
```

Bandera

```
flag: picoCTF{up><_m3_f7w_5769b54e}
```

Notas Adicionales

Referencias

-