



Tute - crackme_solid_04.exe – KarasuRØØT – Fecha: 13/08/2024

Buenas! Aquí de nuevo siguiendo aprendiendo esto del reversing – Bueno el tema es así, tengo un crackme con nombre: crackme_solid_04.exe

En primera instancia, me encontré que el archivo estaría hecho en C++ y compilado en 64bits

Ahora bien, al ejecutarlo aparece esto:

```
C:\> Administrador: C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\SQL-PC>cd c:\revv

c:\revv>crackme_solid_04.exe
Bienvenidos al curso de Reversing 2024
Para empezar, decime tu nombre: pepe
Hola pepe vamos a aprender reversing !
falta algo para seguir avanzando...

c:\revv>
```

Bueno eso quiere decir, según mi entender es que “falta” algo, entonces decidí abrirlo con el IDA

```

; int __fastcall main(int argc, const char **argv, const char **envp)
main proc near

    dwCreationDisposition= dword ptr -58h
    dwFlagsAndAttributes= dword ptr -50h
    hTemplateFile= qword ptr -48h
    var_38= dword ptr -38h
    FileName= byte ptr -30h
    var_20= qword ptr -20h

; __unwind { // __GSHandlerCheck
push    rsi
push    rdi
sub     rsp, 68h
mov     rax, cs:__security_cookie
xor     rax, rsp
mov     [rsp+78h+var_20], rax
lea     rcx, aBienvenidosAlC ; "Bienvenidos al curso de Reversing 2024"...
call    sub_13F9812B0
mov     ecx, 3E8h ;
call    cs:Sleep
call    sub_13F981070
lea     rax, [rsp+78h+FileName]
lea     rcx, aTestTxt ;
mov     rdi, rax
mov     rsi, rcx

```

```

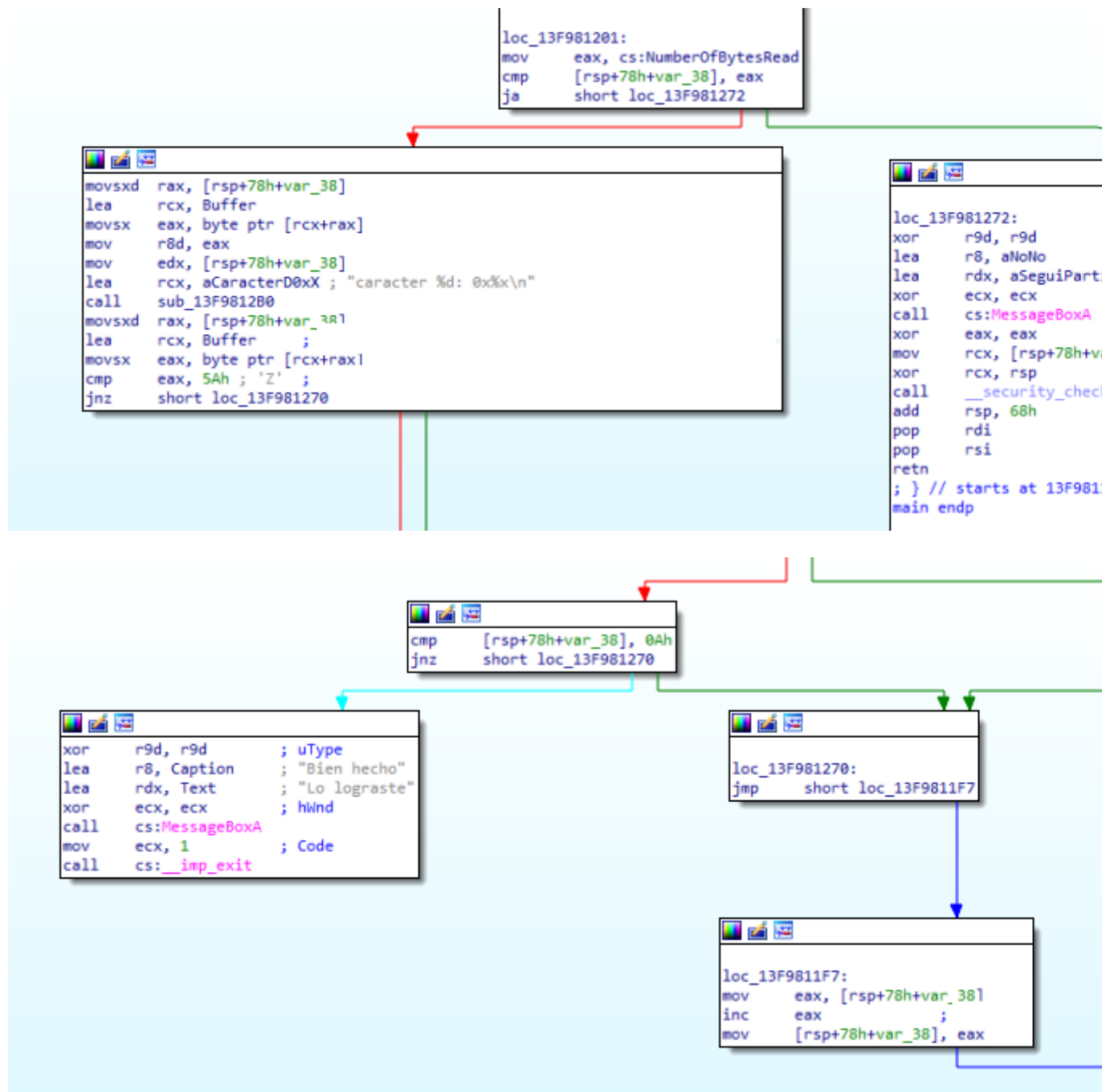
mov     ecx, 9 ;
rep movsb
mov     [rsp+78h+hTemplateFile], 0 ; hTemplateFile
mov     [rsp+78h+dwFlagsAndAttributes], 80h ; dwFlagsAndAttributes
mov     [rsp+78h+dwCreationDisposition], 3 ; dwCreationDisposition
xor     r9d, r9d ; lpSecurityAttributes
xor     r8d, r8d ; dwShareMode
mov     edx, 0C0000000h ; dwDesiredAccess
lea     rcx, [rsp+78h+FileName] ; lpFileName
call    cs:CreateFileA ;
mov     cs:qword_13F985040, rax ;
cmp     dword ptr cs:qword_13F985040, 0FFFFFFFFh ;
jnz     short loc_13F9811E1

```

```

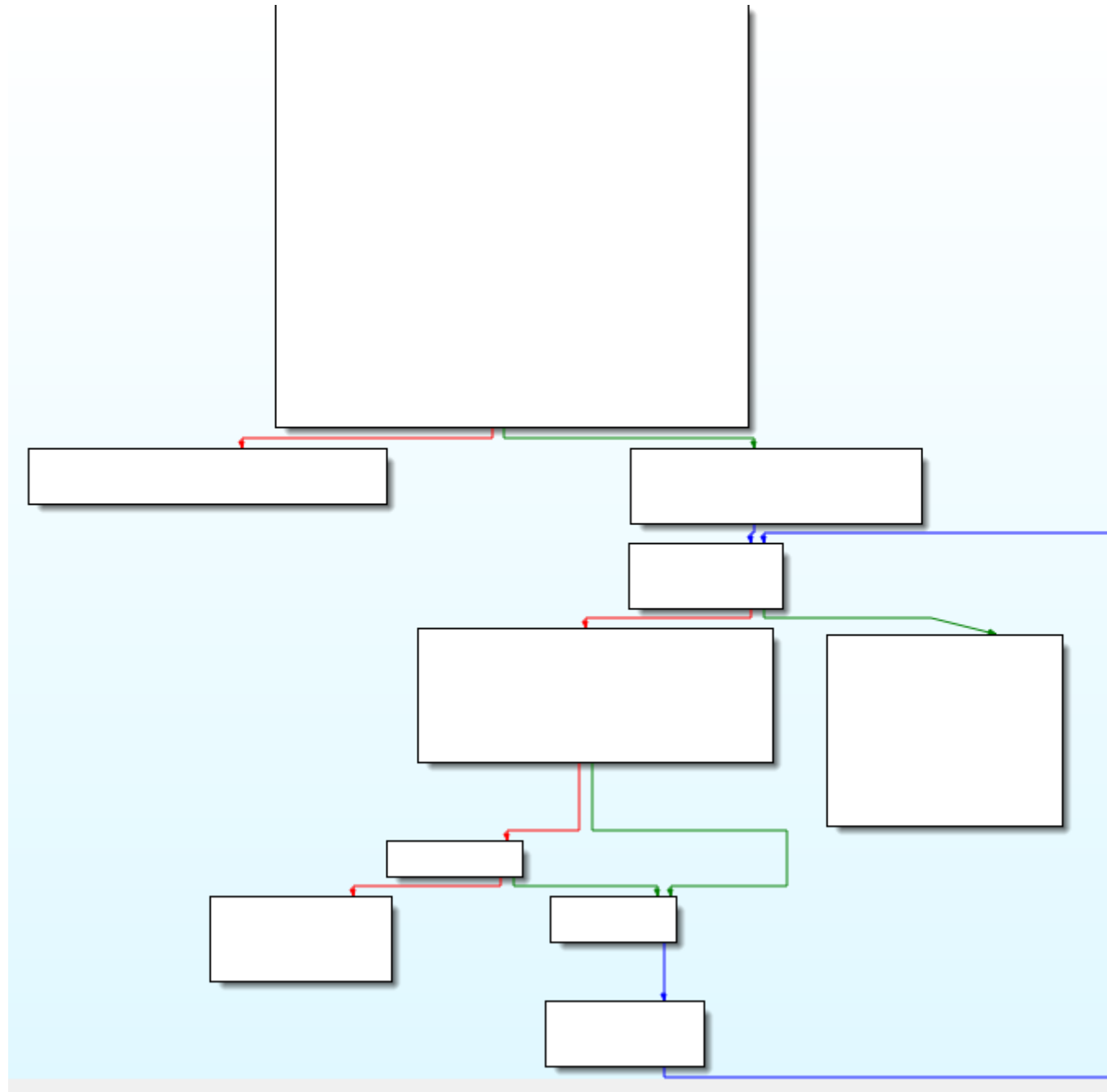
lea     rcx, aFaltaAlgoParaS ; "falta algo para seguir avanzando...\n"
call    sub_13F9812B0
mov     ecx, 1 ;
call    cs:__imp_exit

```



Pido disculpas pero no tenía otra forma más que sacar varias capturas.

Para una idea más “global” dejo lo que es el diagrama de flujo completo:



Bueno algunos detalles que a primera vista observo:

```

; __unwind { // __GSHandlerCheck
push    rsi
push    rdi
sub     rsp, 68h
mov     rax, cs:__security_cookie
xor     rax, rsp
mov     [rsp+78h+var_20], rax
lea     rcx, aBienvenidosAlC ; "Bienvenidos al curso de Reversing 2024"...
call    sub_13F8A12B0
mov     ecx, 3E8h             ; imprime bienvenida y espera 1 seg
call    cs:Sleep

```

El call que dice sub_13F8A12B0 parecería ser un printf

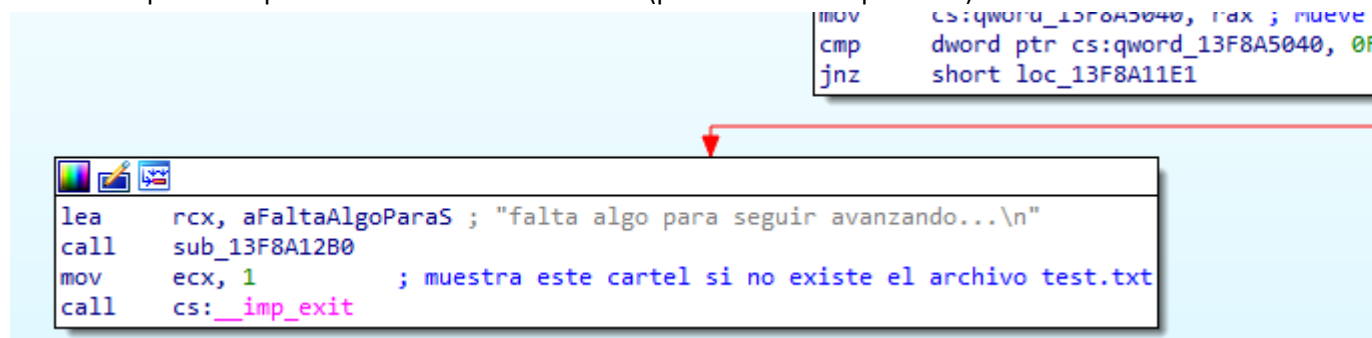
```
var_10= qword ptr -10h
; __unwind { // __GSHandlerCheck
push    rdi
sub     rsp, 40h
mov     rax, cs:__security_cookie
xor     rax, rsp
mov     [rsp+48h+var_10], rax
lea     rax, [rsp+48h+Buffer]
mov     rdi, rax
xor     eax, eax
mov     ecx, 14h
rep stosb
lea     rcx, aParaEmpezarDec ; "Para empezar, decime tu nombre: "
call    sub_13F8A12B0
mov     edx, 14h           ; Size
lea     rcx, [rsp+48h+Buffer] ; Buffer
call    cs:gets_s
lea     rdx, [rsp+48h+Buffer]
lea     rcx, aHolaSVamosAApr ; "Hola %s vamos a aprender reversing !\n"
call    sub_13F8A12B0
mov     rcx, [rsp+48h+var_10]
```

Esta es la imagen de dicho call -> al poner un BP y ejecutarlo coincide con que imprime dicho cartel de bienvenida

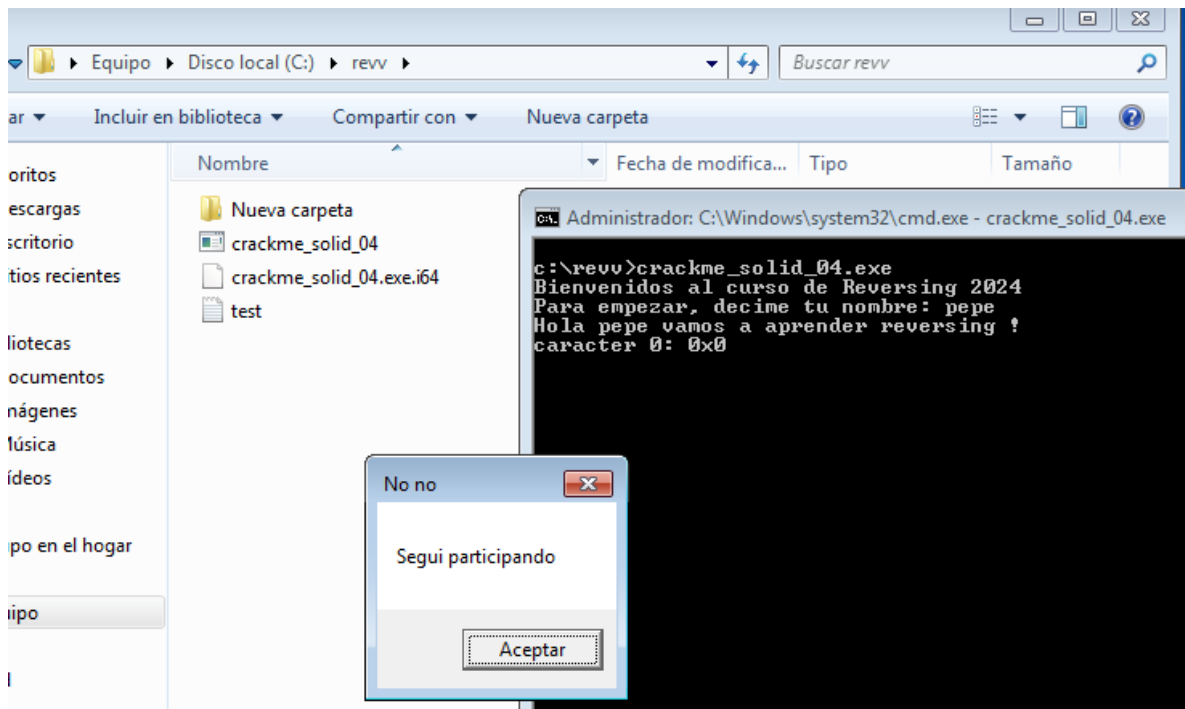
Siguiendo con el traceo me doy cuenta que indica lo siguiente:

```
call    sub_1400012B0
mov     ecx, 3E8h          ; dwMilliseconds
call    cs:Sleep
call    sub_140001070
lea     rax, [rsp+78h+FileName]
lea     rcx, aTestTxt      ; "test.txt"
mov     rdi, rax
mov     rsi, rcx
```

Otra de las pistas es que en el IDA muestra este salto (previa a una comparación)



Yo creo que ahí está buscando un archivo "test.txt" – entonces yo creo que la mejor opción sería crear ese archivo en la misma ubicación donde está el crackme y luego probar que ocurre:



Bien, logramos esquivar el anterior cartel, pero aun así no logramos dar con el CHICO BUENO

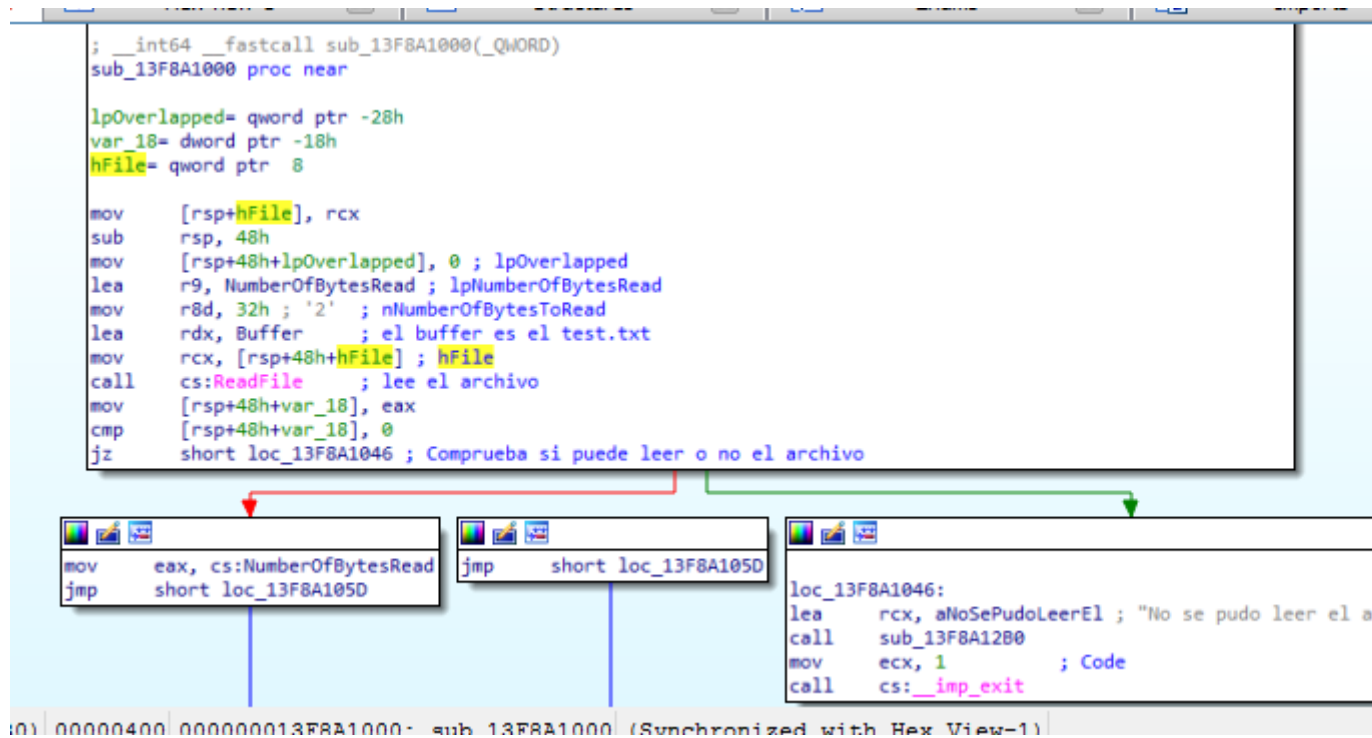
Entonces hasta ahora es: un crackme que te da la bienvenida amablemente a un curso ¿? Y te pide un nombre, imprime un saludo y luego busca si existe o no el archivo test.txt -> Si existe, entonces devuelve “carácter 0: 0x0” y un simpático cartel.

Algunos detalles que me saltee:

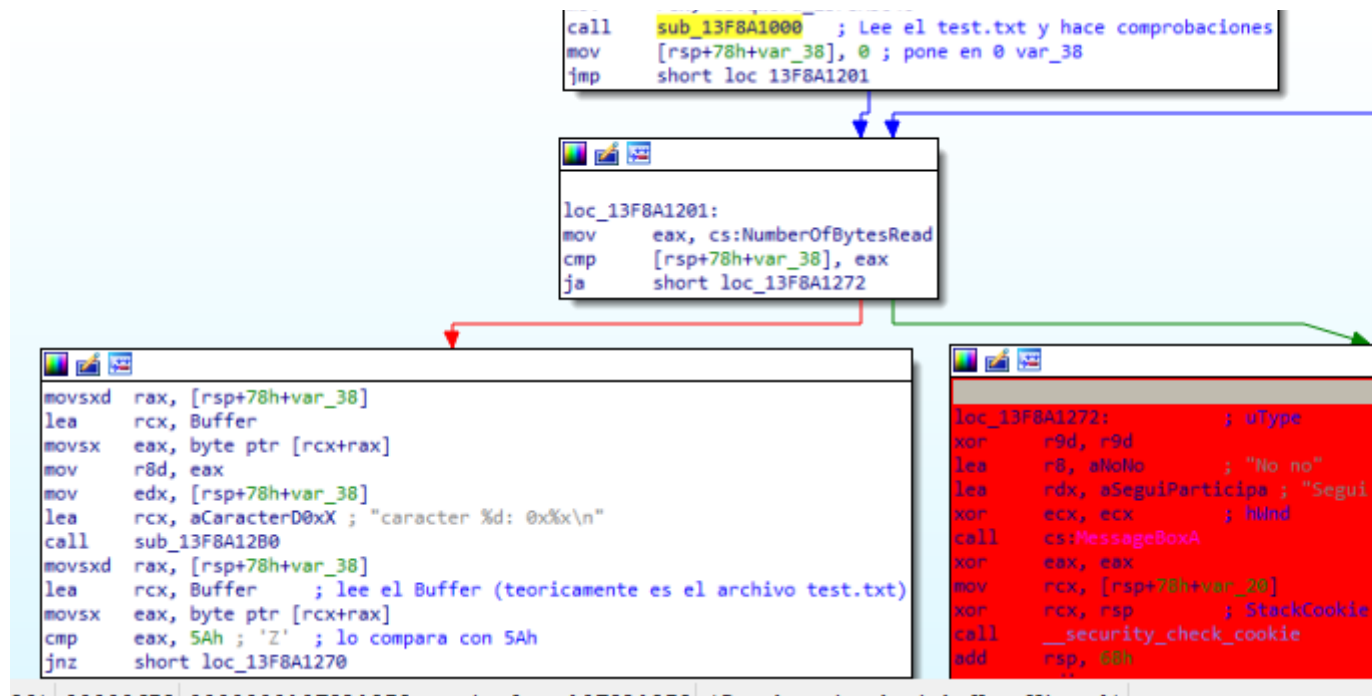
```
call cs:CreateFileA ; Crea o abre un archivo o dispositivo de E/S - en este caso lo abre
```

Según en MSDN la función CreateFileA – crea o abre un archivo o disp. De e/s – por lo que venimos viendo, en esta oportunidad, no crea nada sino que abre dicho archivo

Otra cosa que note es que el call sub_13F8A1000 hace ciertas verificaciones:



Bien entonces sigo mirando el ida – antes que nada marco el cartel de chico malo ->



Bueno mirándolo así, hay un detalle que me llama la atención:

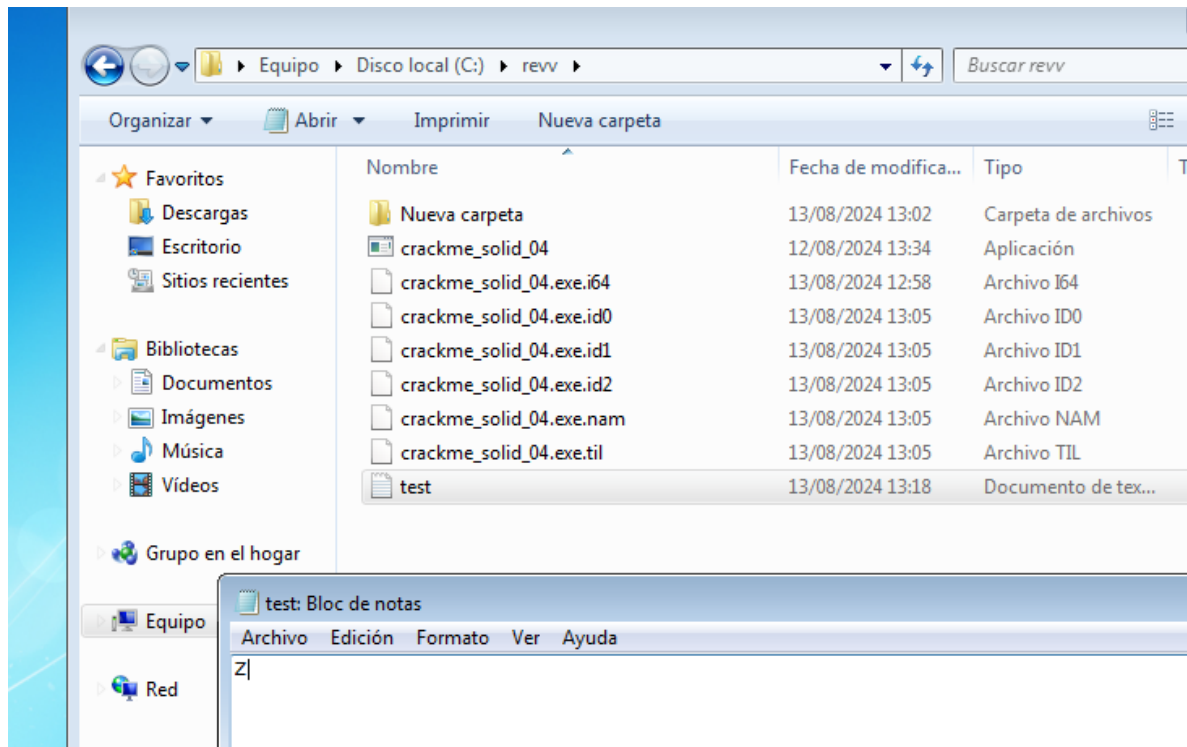
```

cmp     eax, 5Ah ; 'Z' ; lo compara con 5Ah
jnz     short loc_13F8A1270

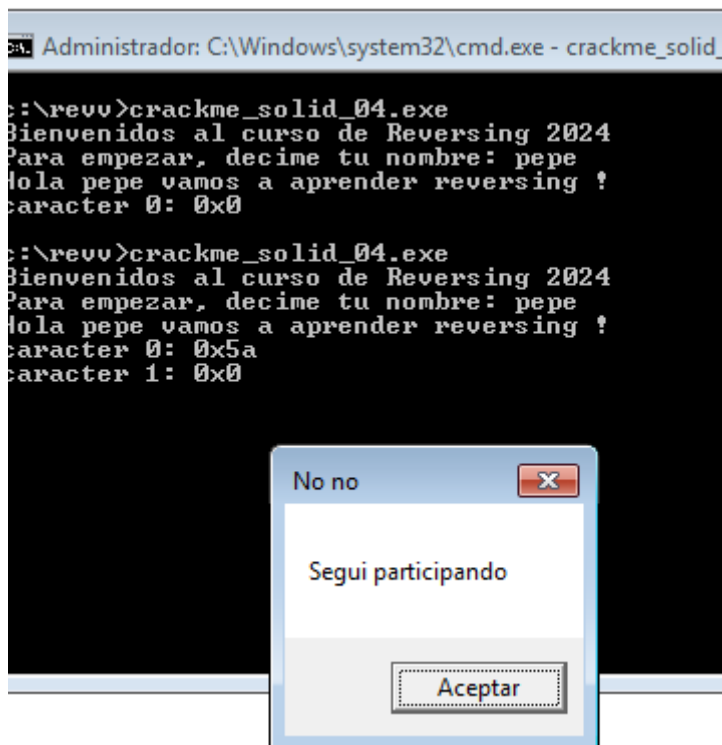
```

Eso! Ahí?! Que es?! Ósea compara el contenido de EAX con 5A (ósea Z en hexa)

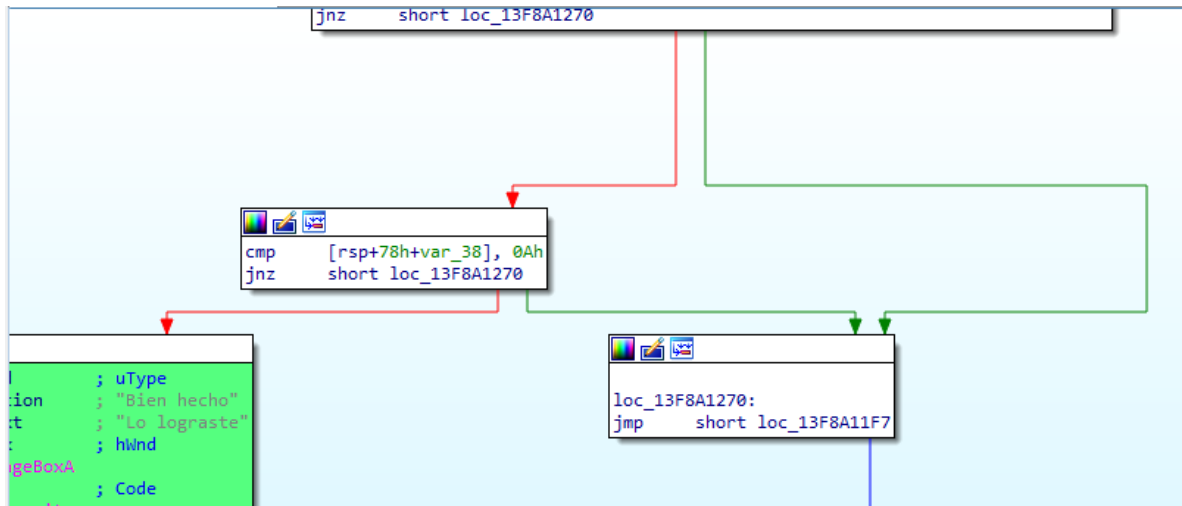
Bueno acá tenemos una pista, voy a poner Z (tener en cuenta que es Z mayúscula – no minúscula) en el archivo txt y ver que me hace



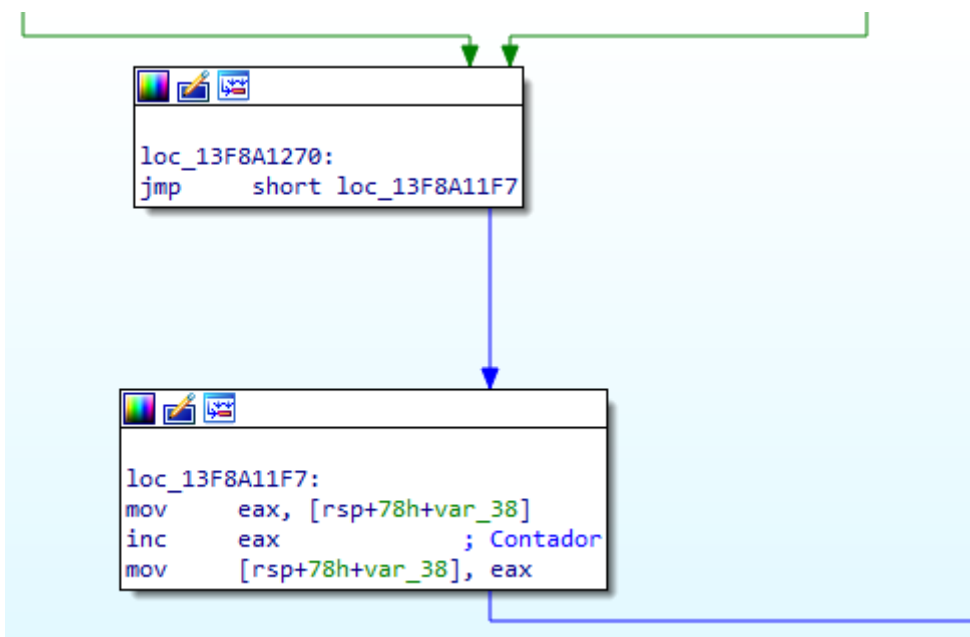
Epa!



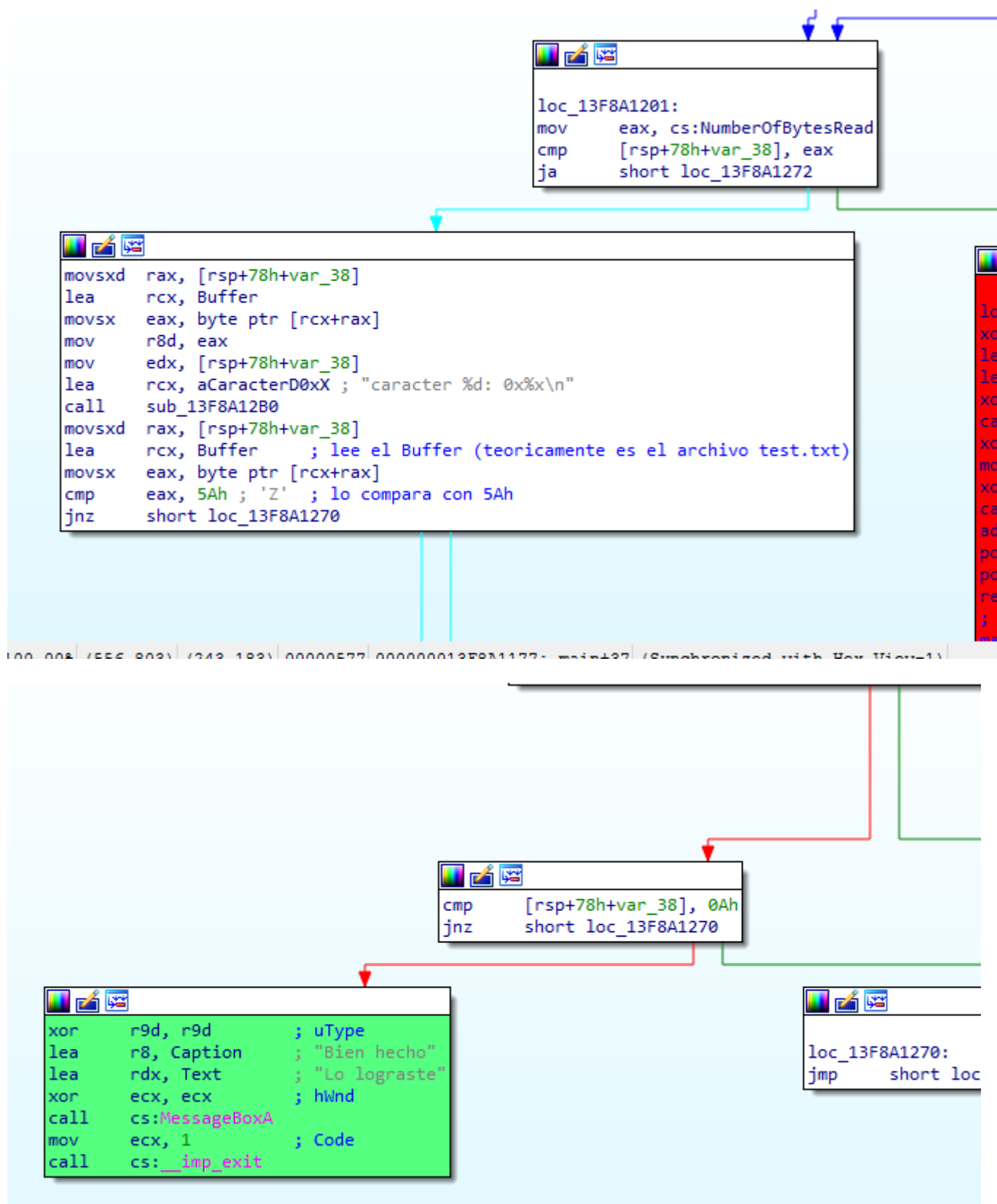
¿Qué paso ahí? Si bien tenemos el cartel de “Segui participando” -> indica carácter 0x5a (ósea que tenía algo de razón)- pero también dice carácter 1: 0x0 – y estoy seguro que solo puse Z en el archivo – ok vuelvo a IDA



Aquí veo que esta el salto jnz -> y después lo vuelve a comparar contra 0A (osea 10) y tiene dos caminos -> o sale por el cartel de Chico bueno que hasta ahora no hemos llegado o va por el otro jmp ->



Ok encuentro que esos saltos van a parar a un contador (es decir que var_38 es muy probable que sea un contador) – y ese salto luego vuelve acá:



Entonces, hasta ahora tenemos lo siguiente:

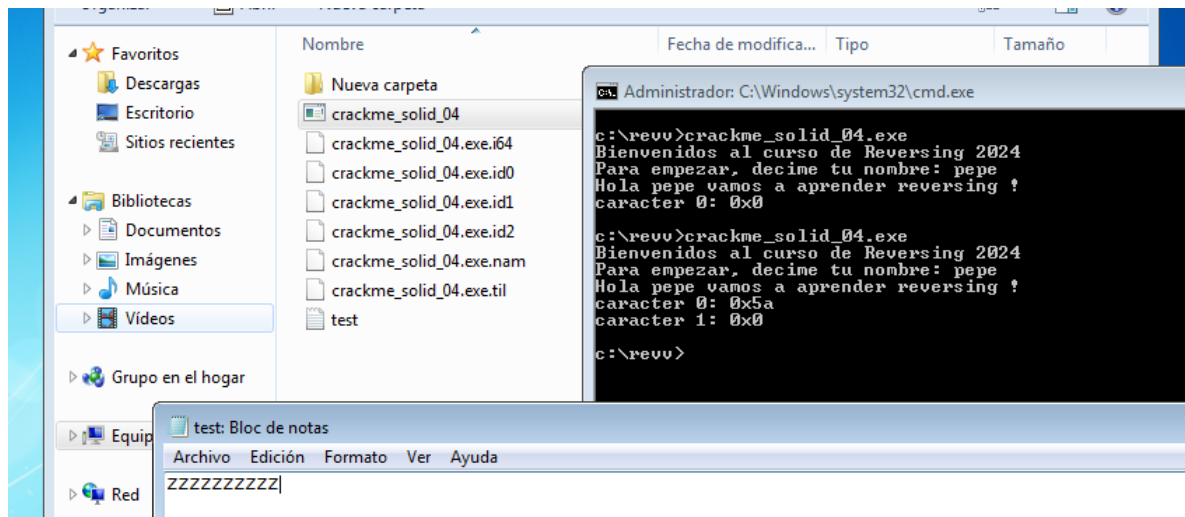
1 - te pide un usuario – el cual hasta ahora no encontré nada sobre alguna operación que haga con el mismo.

2 – Espera encontrar un archivo test.txt con contenido (en principio puedo estimar que tenga escrito Z)

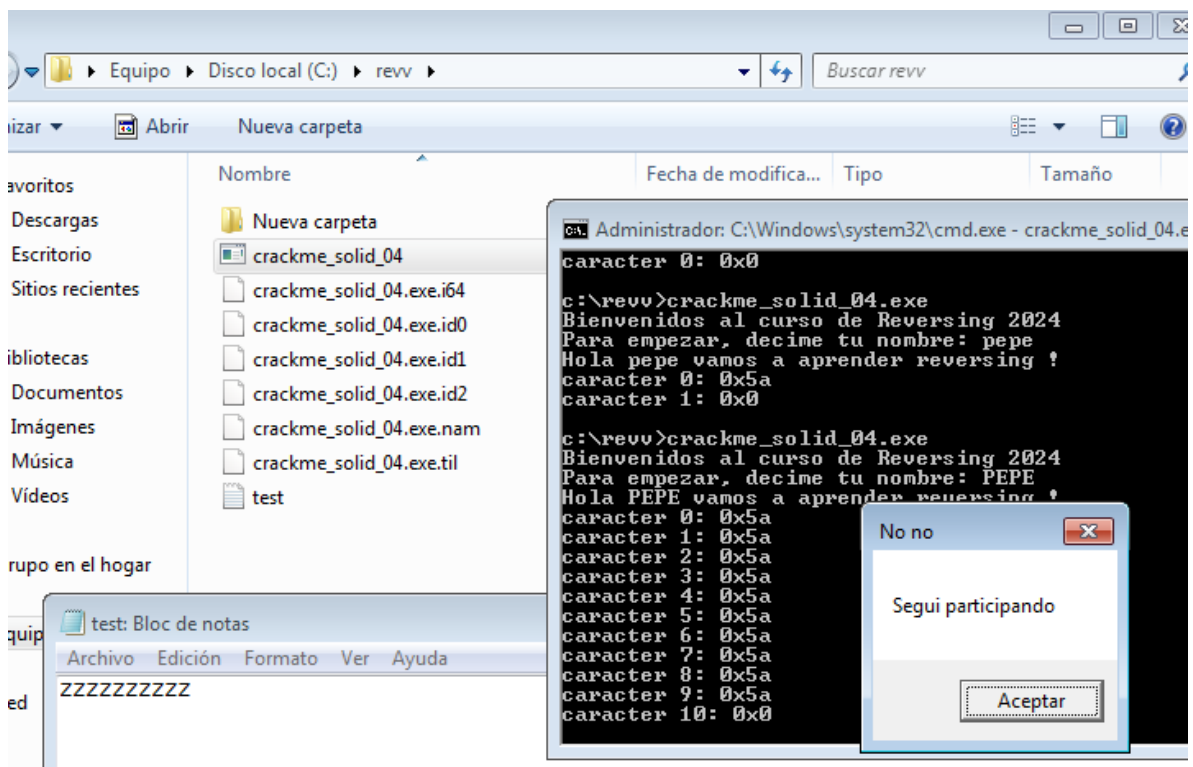
3 – y creo que acá es lo más importante, entra en un bucle, pero que el mismo lo compara con 0A (osea 10)

Creo que no es muy loco pensar que, lo que hace es que lee el archivo y lo recorre 10 veces – viendo que cada carácter sea o no Z – entonces porque no poner “ZZZZZZZZZZ”?

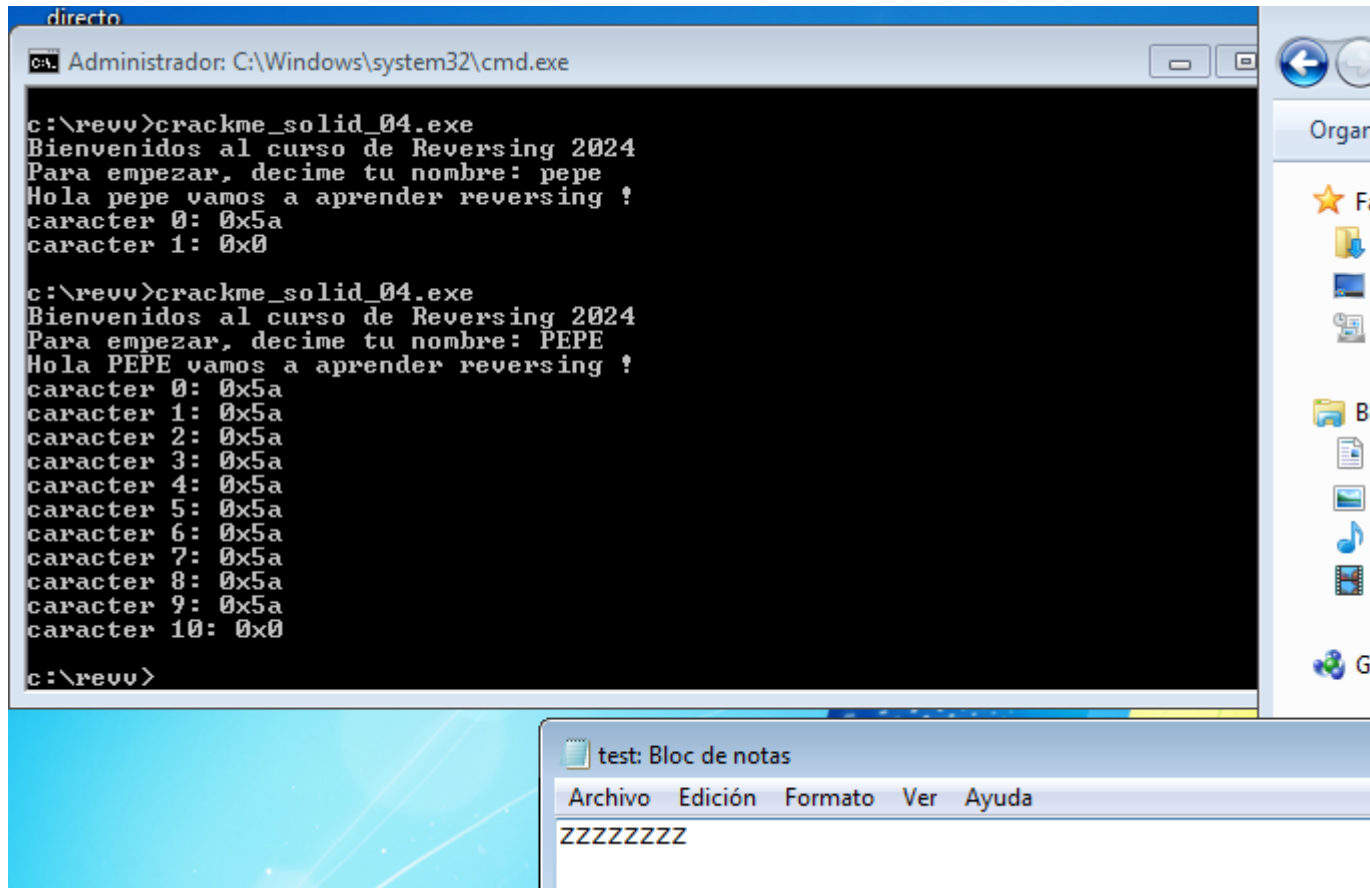
Voy a probarlo:



Y lo ejecuto de nuevo



Si bien tiene 10 caracteres Z -> me sigue diciendo "Segui participando" – pero aquí hay algo raro pareciera, es decir dice carácter 0: 0x5a – pero llega al carácter 9 – es decir que es uno más – como sucede cuando se recorre una lista en Python u otro lenguaje – es decir comienza en el índice 0 y siempre es el string por ejemplo -1 – entonces en vez de poner 10 veces Z – voy a poner 11 veces



The screenshot shows a Windows desktop environment. In the foreground, there is a command prompt window titled "directo" with the command prompt "Administrador: C:\Windows\system32\cmd.exe". The command prompt shows the execution of "c:\revu>crackme_solid_04.exe". The program outputs a welcome message and asks for a name. In the first run, the name "pepe" is entered, and it shows "caracter 0: 0x5a" and "caracter 1: 0x0". In the second run, the name "PEPE" is entered, and it shows "caracter 0: 0x5a" through "caracter 10: 0x0". Below the command prompt, there is a Notepad window titled "test: Bloc de notas" with a menu bar (Archivo, Edición, Formato, Ver, Ayuda) and the text "ZZZZZZZZ".

```
directo
Administrador: C:\Windows\system32\cmd.exe

c:\revu>crackme_solid_04.exe
Bienvenidos al curso de Reversing 2024
Para empezar, decime tu nombre: pepe
Hola pepe vamos a aprender reversing !
caracter 0: 0x5a
caracter 1: 0x0

c:\revu>crackme_solid_04.exe
Bienvenidos al curso de Reversing 2024
Para empezar, decime tu nombre: PEPE
Hola PEPE vamos a aprender reversing !
caracter 0: 0x5a
caracter 1: 0x5a
caracter 2: 0x5a
caracter 3: 0x5a
caracter 4: 0x5a
caracter 5: 0x5a
caracter 6: 0x5a
caracter 7: 0x5a
caracter 8: 0x5a
caracter 9: 0x5a
caracter 10: 0x0

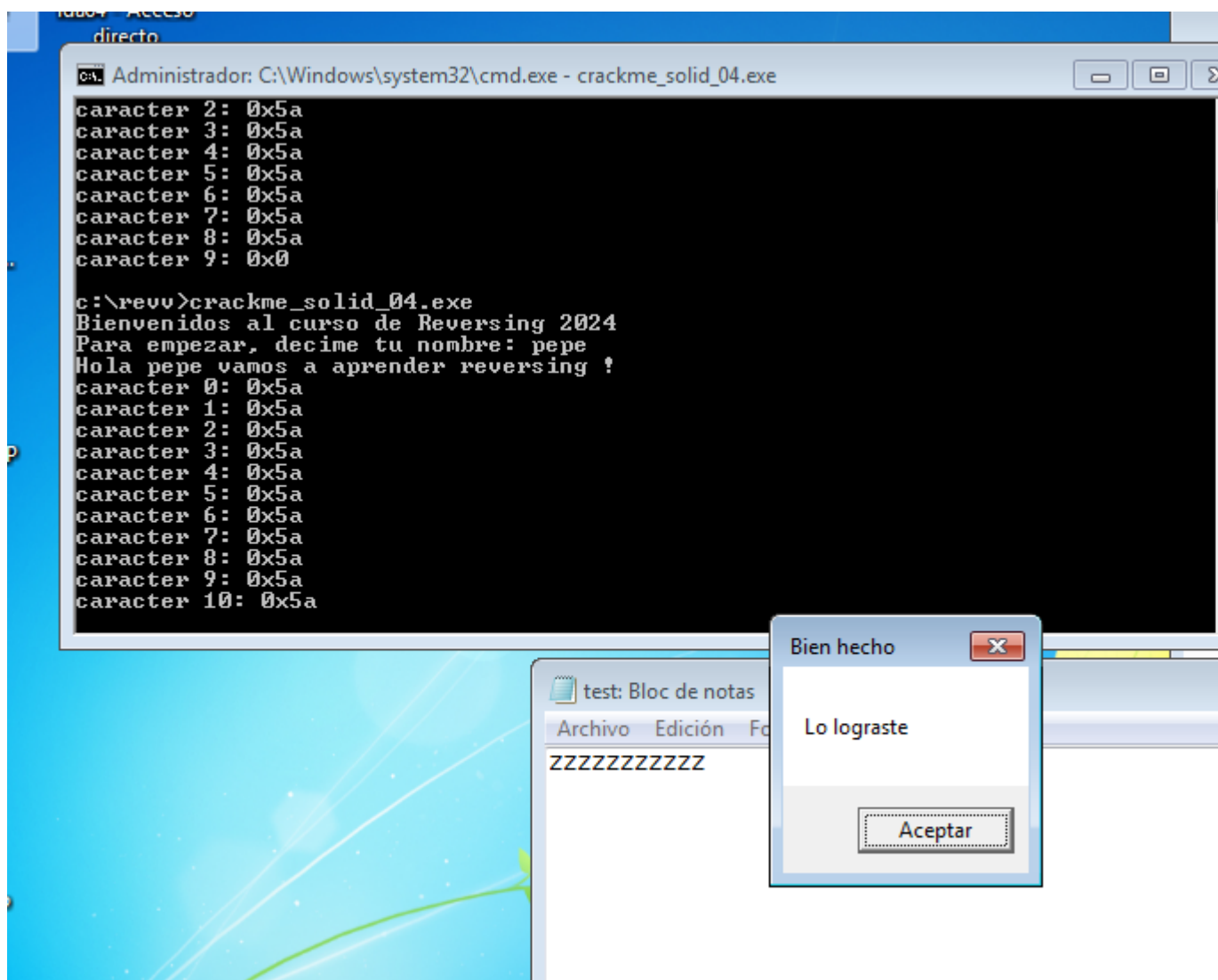
c:\revu>
```

test: Bloc de notas

Archivo Edición Formato Ver Ayuda

ZZZZZZZZ

Y lo voy a ejecutar:



TATA! Lo logre –

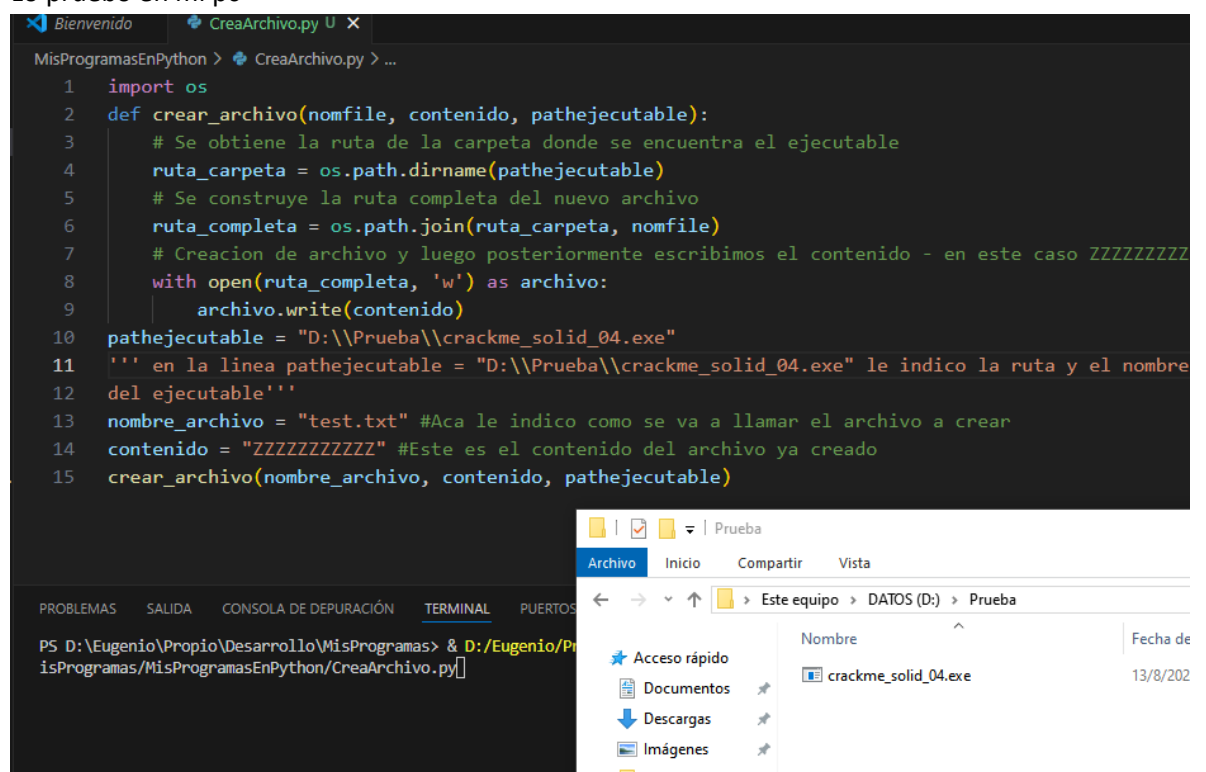
Pero como tampoco tengo ni idea de programación (bueno si algo tengo pero no como quisiera, y estoy tratando de aprender Python) voy a generar un script con la idea de que si encuentra en el directorio especificado un ejecutable con un nombre determinado – cree un archivo test.txt con el contenido de “ZZZZZZZZZZ” –

```

MisProgramasEnPython > CreaArchivo.py > ...
1  import os
2  def crear_archivo(nomfile, contenido, pathejecutable):
3      # Se obtiene la ruta de la carpeta donde se encuentra el ejecutable
4      ruta_carpeta = os.path.dirname(pathejecutable)
5      # Se construye la ruta completa del nuevo archivo
6      ruta_completa = os.path.join(ruta_carpeta, nomfile)
7      # Creacion de archivo y luego posteriormente escribimos el contenido
8      with open(ruta_completa, 'w') as archivo:
9          archivo.write(contenido)
10 pathejecutable = "D:\\Prueba\\crackme_solid_04.exe"
11 ''' en la linea pathejecutable = "D:\\Prueba\\crackme_solid_04.exe" le
12 del ejecutable'''
13 nombre_archivo = "test.txt" #Aca le indico como se va a llamar el arch
14 contenido = "ZZZZZZZZZZ" #Este es el contenido del archivo ya creado
15 crear_archivo(nombre_archivo, contenido, pathejecutable)

```

➔ Lo pruebo en mi pc

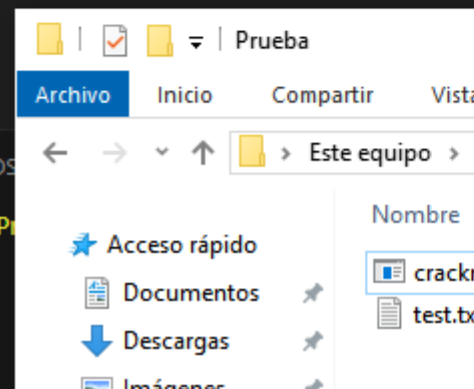


Ahí lo creo con el contenido correspondiente:

```
Bienvenido CreaArchivo.py U X
MisProgramasEnPython > CreaArchivo.py > ...
1 import os
2 def crear_archivo(nomfile, contenido, pathejecutable):
3     # Se obtiene la ruta de la carpeta donde se encuentra el ejecutable
4     ruta_carpeta = os.path.dirname(pathejecutable)
5     # Se construye la ruta completa del nuevo archivo
6     ruta_completa = os.path.join(ruta_carpeta, nomfile)
7     # Creacion de archivo y luego posteriormente escribimos el contenido
8     with open(ruta_completa, 'w') as archivo:
9         archivo.write(contenido)
10 pathejecutable = "D:\\Prueba\\crackme_solid_04.exe"
11 ''' en la linea pathejecutable = "D:\\Prueba\\crackme_solid_04.exe"
12 del ejecutable'''
13 nombre_archivo = "test.txt" #Aca le indico como se va a llamar el archivo
14 contenido = "ZZZZZZZZZZ" #Este es el contenido del archivo ya creado
15 crear_archivo(nombre_archivo, contenido, pathejecutable)
```

PROBLEMAS SALIDA CONSOLA DE DEPURACIÓN **TERMINAL** PUERTOS

```
PS D:\Eugenio\Propio\Desarrollo\MisProgramas> & D:/Eugenio/Propio/Desarrollo/MisProgramas/MisProgramasEnPython/CreaArchivo.py
PS D:\Eugenio\Propio\Desarrollo\MisProgramas>
```



Nombre	Fecha de modificación	Tipo	Tamaño
crackme_solid_04.exe	13/8/2024 14:03	Aplicación	12 KB
test.txt	13/8/2024 14:20	Documento de texto	1 KB

test.txt: Bloc de notas







Archivo Edición Formato Ver Ayuda

ZZZZZZZZZZ

Y funciona:

Compartir Vista

Este equipo > DATOS (D:) > Prueba

Nombre	Fecha de modificación	Tipo	Tamaño
 crackme_solid_04.exe	13/8/2024 14:03	Aplicación	12 KB
 test.txt	13/8/2024 14:20	Documento de te...	1 KB
			
			
			
			

Símbolo del sistema - crackme_solid_04.exe

```
D:\Prueba>crackme_solid_04.exe
Bienvenidos al curso de Reversing 2024
Para empezar, decime tu nombre: KarasuRoot
Hola KarasuRoot vamos a aprender reversing !
caracter 0: 0x5a
caracter 1: 0x5a
caracter 2: 0x5a
caracter 3: 0x5a
caracter 4: 0x5a
caracter 5: 0x5a
caracter 6: 0x5a
caracter 7: 0x5a
caracter 8: 0x5a
caracter 9: 0x5a
caracter 10: 0x5a
```

Bien hecho

Lo logras

Ac

Espero que aquellos que se inician les sirva de algo – Saludos!