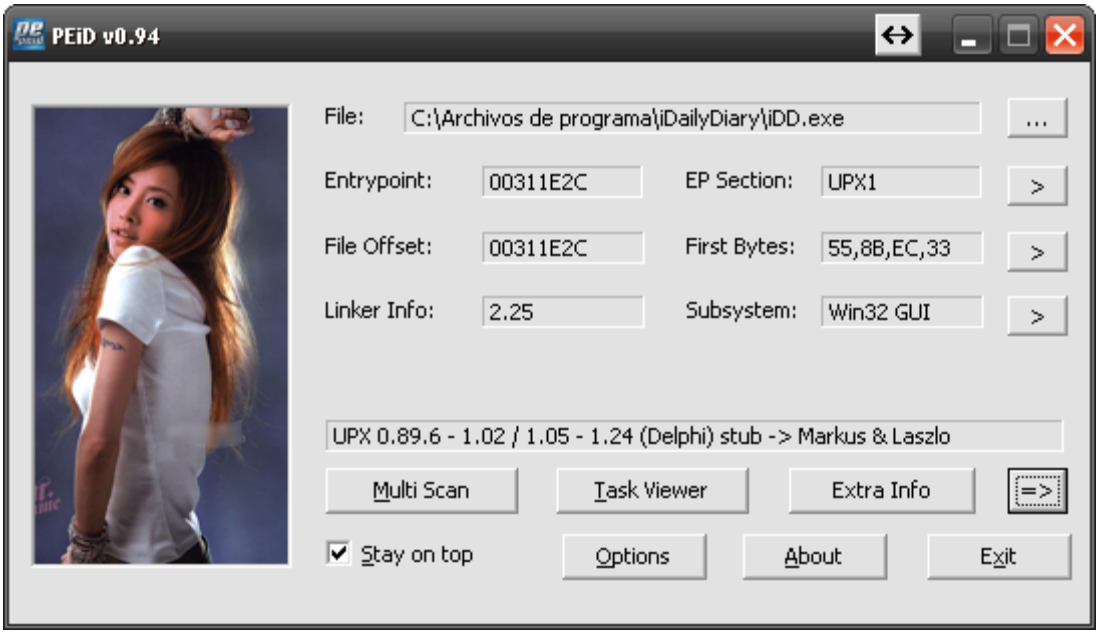
iDailyDiary Professional v.3.41	
Fecha	**24 de enero de 2011**
Victima	**iDailyDiary Professional Versión 3.41**
MD5 del instalador	**447AED8E503A40BF8FBA5C430E5CB0CE**
Protección	**Creo que ninguna**
Herramientas	**Ollydbg portable v.1 de Neutrino**
Objetivo	**Recuperar la clave de mi diario**
Dificultad	**Sencilla**
Cracker	**Aguml**

Introducción

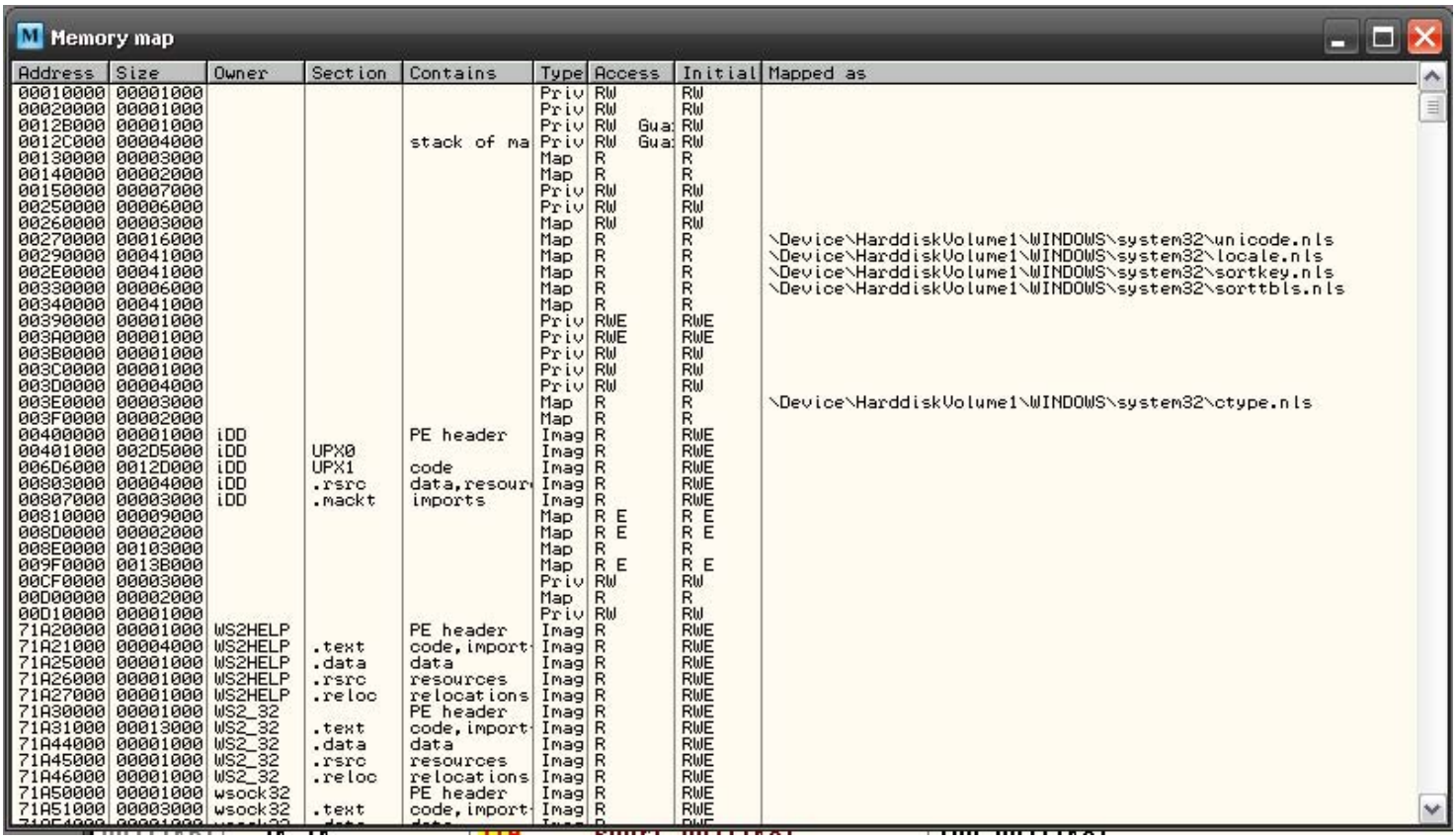
Antes de nada aclarar que aquí no pretendo registrar la aplicación ya que ésta ya la tengo registrada, más bien intento romper su seguridad para poder abrir un archivo sin contraseña valida y de paso poder averiguar su contraseña.
Bueno, os cuento como empezó esta historia; Hace algo más de un año instalé este programa y me agradó, así que creé mi diario personal y empecé a darle forma día a día. Como suele pasarme siempre, con el tiempo lo dejé de lado y hoy fui a abrir el diario y, sorpresa, no recordaba la contraseña para abrir mi diario. Lo que hay escrito es muy valioso para mí porque en él está la historia de cómo conocí a mi prometida y como fue nuestra historia durante casi un año.
Probé todas las contraseñas que se me ocurrieron pude haber puesto pero nada, no tuve éxito así que me dije, “antes de empezar a lamentarme probaré con Olly a ver qué pasa” y aquí continua esa historia.

Conociendo mejor a la víctima

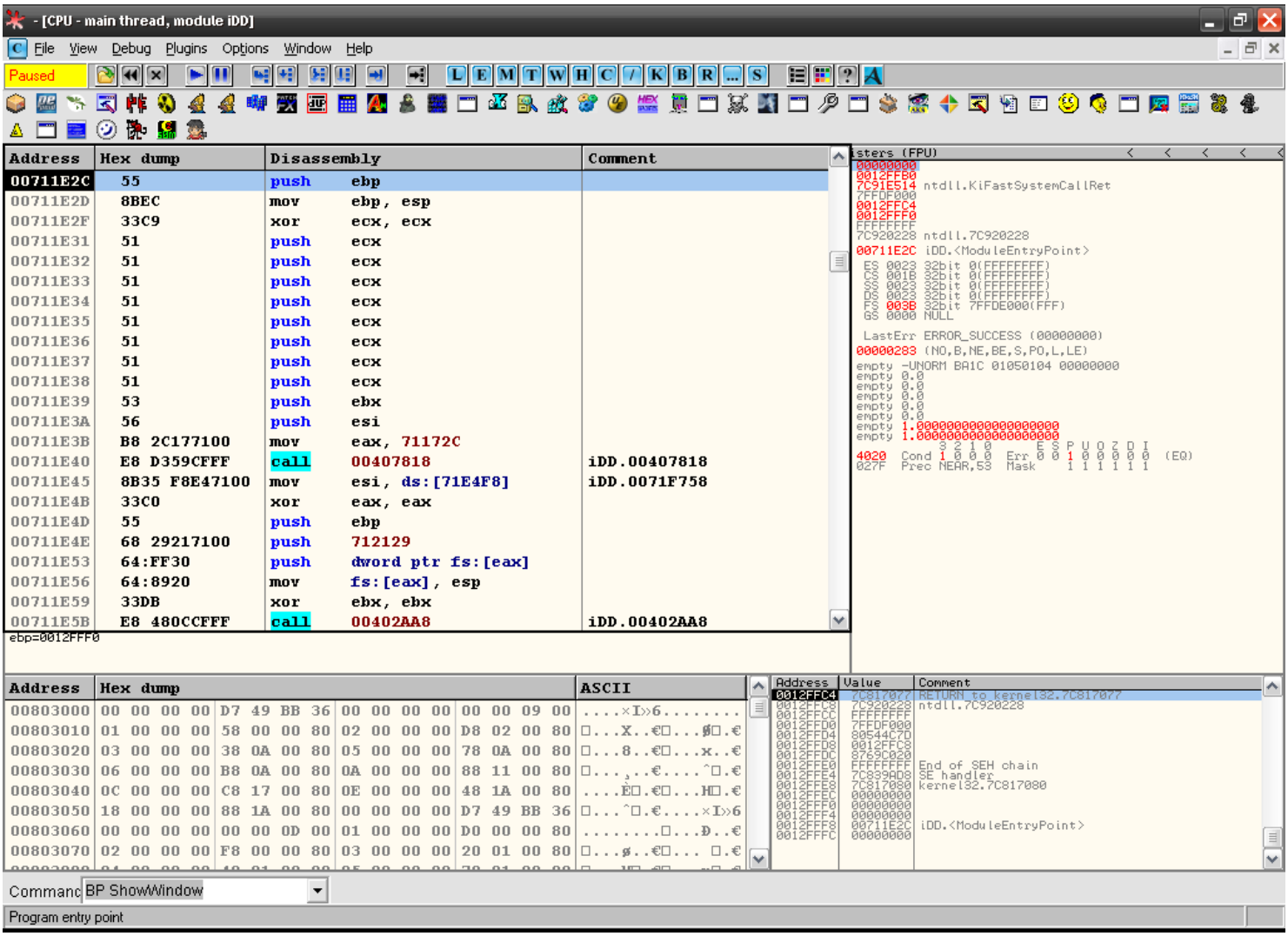
Lo primero que hago es examinarla con Peid:



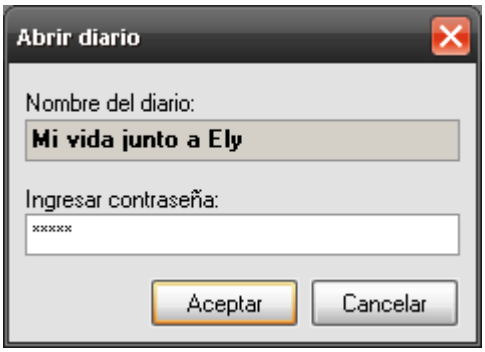
Bueno, no creo que sea ningún problema así que lo abro en Olly y miro donde se encuentra el EP y el Memory Map para tener más información:



Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
00010000	00001000				Priv	RW	RW	
00020000	00001000				Priv	RW	RW	
0012B000	00001000				Priv	RW Gua	RW	
0012C000	00004000			stack of ma	Priv	RW Gua	RW	
00130000	00003000				Map	R	R	
00140000	00002000				Map	R	R	
00150000	00007000				Priv	RW	RW	
00250000	00006000				Priv	RW	RW	
00260000	00003000				Map	RW	RW	
00270000	00016000				Map	R	R	\Device\HarddiskVolume1\WINDOWS\system32\unicode.nls
00290000	00041000				Map	R	R	\Device\HarddiskVolume1\WINDOWS\system32\locale.nls
002E0000	00041000				Map	R	R	\Device\HarddiskVolume1\WINDOWS\system32\sortkey.nls
00330000	00006000				Map	R	R	\Device\HarddiskVolume1\WINDOWS\system32\sorttbls.nls
00340000	00041000				Map	R	R	
00390000	00001000				Priv	RWE	RWE	
003A0000	00001000				Priv	RWE	RWE	
003B0000	00001000				Priv	RW	RW	
003C0000	00001000				Priv	RW	RW	
003D0000	00004000				Priv	RW	RW	
003E0000	00003000				Map	R	R	\Device\HarddiskVolume1\WINDOWS\system32\ctype.nls
003F0000	00002000				Map	R	R	
00400000	00001000	iDD		PE header	Imag	R	RWE	
00401000	002D5000	iDD	UPX0		Imag	R	RWE	
006D6000	0012D000	iDD	UPX1	code	Imag	R	RWE	
00803000	00004000	iDD	.rsrc	data,resour	Imag	R	RWE	
00807000	00003000	iDD	.mackt	imports	Imag	R	RWE	
00810000	00009000				Map	R E	R E	
008D0000	00002000				Map	R E	R E	
008E0000	00103000				Map	R	R	
009F0000	0013B000				Map	R E	R E	
00CF0000	00003000				Priv	RW	RW	
00D00000	00002000				Map	R	R	
00D10000	00001000				Priv	RW	RW	
71A20000	00001000	WS2HELP		PE header	Imag	R	RWE	
71A21000	00004000	WS2HELP	.text	code,import	Imag	R	RWE	
71A25000	00001000	WS2HELP	.data	data	Imag	R	RWE	
71A26000	00001000	WS2HELP	.rsrc	resources	Imag	R	RWE	
71A27000	00001000	WS2HELP	.reloc	relocations	Imag	R	RWE	
71A30000	00001000	WS2_32		PE header	Imag	R	RWE	
71A31000	00013000	WS2_32	.text	code,import	Imag	R	RWE	
71A44000	00001000	WS2_32	.data	data	Imag	R	RWE	
71A45000	00001000	WS2_32	.rsrc	resources	Imag	R	RWE	
71A46000	00001000	WS2_32	.reloc	relocations	Imag	R	RWE	
71A50000	00001000	wsock32		PE header	Imag	R	RWE	
71A51000	00003000	wsock32	.text	code,import	Imag	R	RWE	

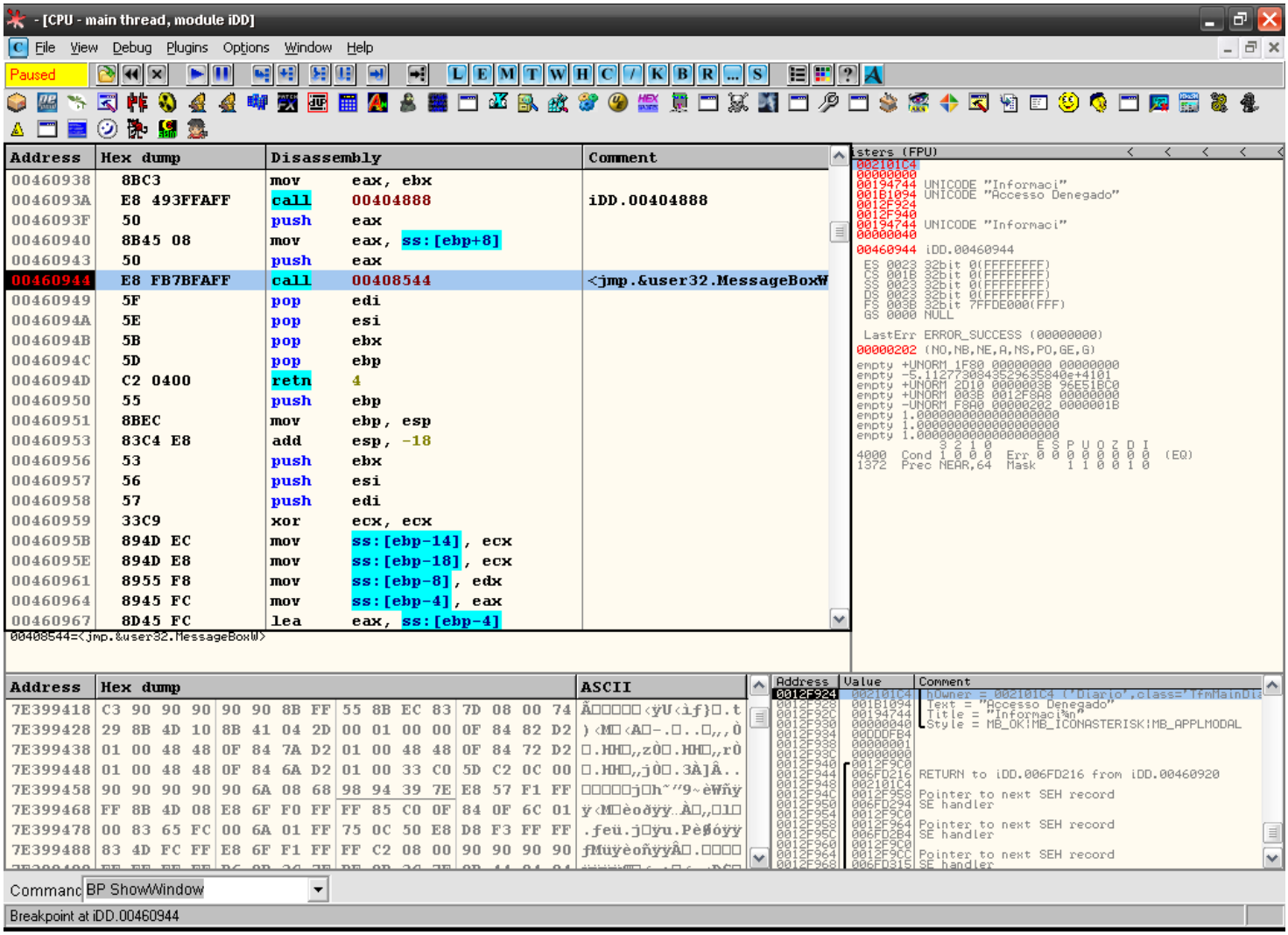


Puedo ver dos cosas, la primera es que hay secciones nombradas como UPX y la segunda es que no empieza con un PUSHAD.
Le doy a F9 para que arranque el programa y este arranca sin problema así que me voy a abrir mi diario para empezar a investigar y me pide la clave para abrirlo:

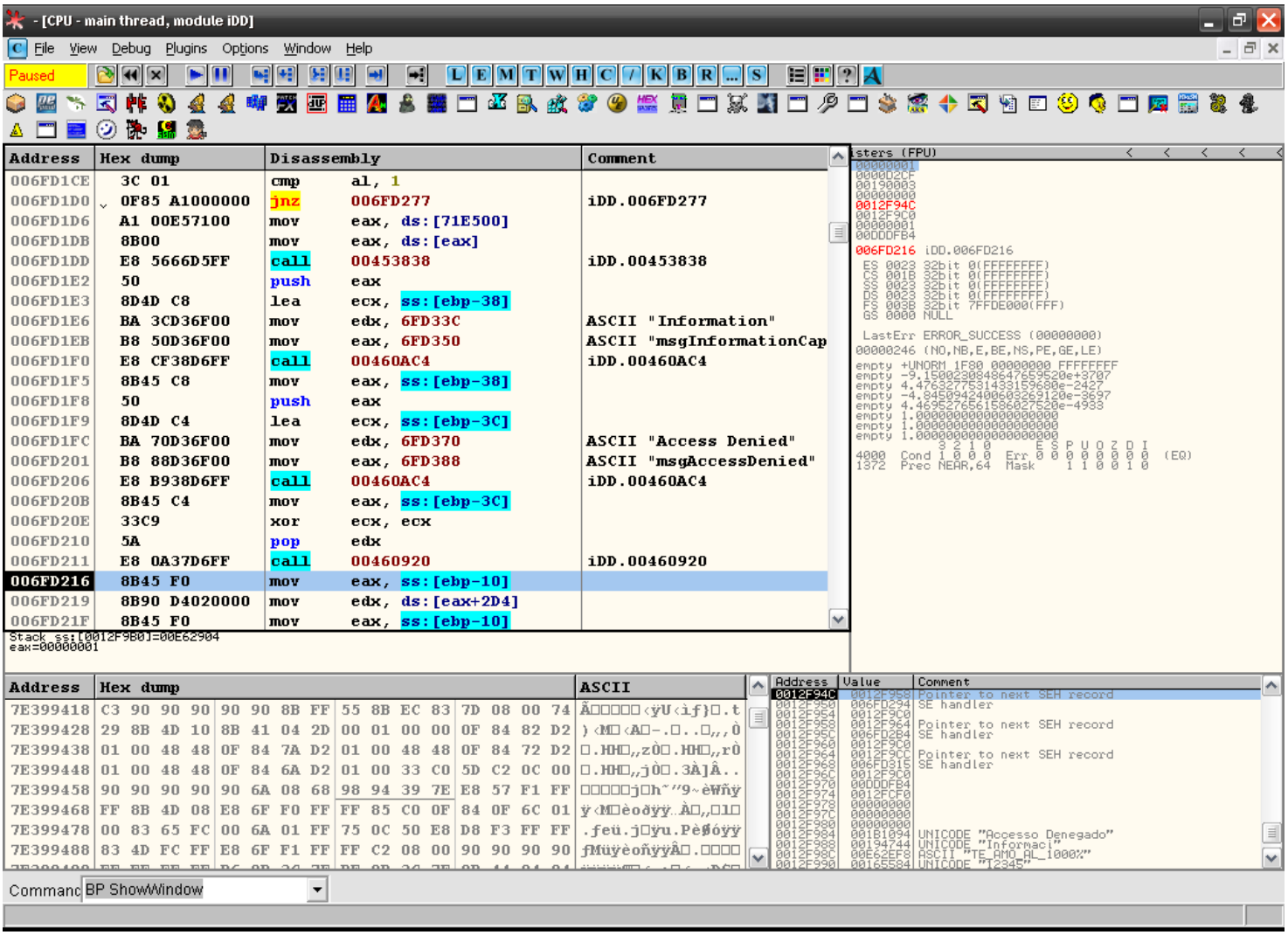


Introduzco la clave de pruebas 12345 y veamos que pasa:

No me deja abrirlo sin la clave pero vamos a intentar ver quién es el responsable de mostrar al chico malo. De momento pruebo con MessageBoxA y MessageBoxW poniendo un BP en ambos y pruebo de nuevo y…



Parece que tenemos suerte y damos pronto con el responsable. Traceamos un poco con F8 para llegar al RETN y ver de dónde venimos y al salir caemos aquí:



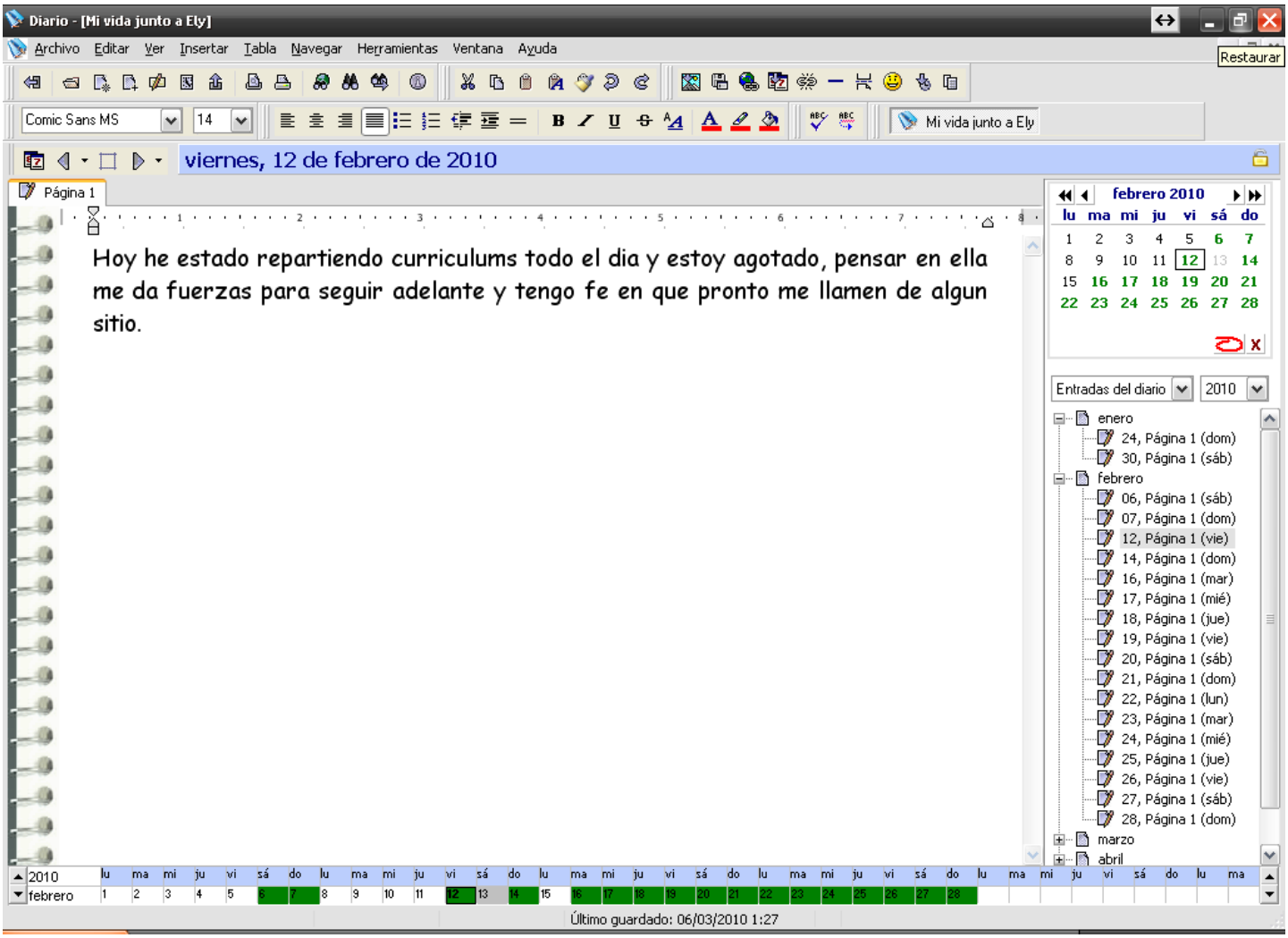
Si miramos el Stack vemos lo que podría ser la clave buena junto con la clave mala y justo encima de donde caímos tenemos algo sospechoso y si miramos más arriba vemos un JNZ que saltaría todo esto así que voy a probar a poner un BP en ese salto condicional y cambiar el FLAG Z cuando pare para ver qué resultado obtengo. Pues no pasa nada, simplemente no muestra mensaje de chico malo pero tampoco consigo que abra el diario así que subo un poco más a ver que veo y un poco más arriba veo esto:

Address	Hex dump	Disassembly	Comment
006FD1C6	75 02	jnz short 006FD1CA	iDD.006FD1CA
006FD1C8	B3 01	mov bl, 1	
006FD1CA	8BC3	mov eax, ebx	
006FD1CC	34 01	xor al, 1	
006FD1CE	3C 01	cmp al, 1	
006FD1D0	0F85 A1000000	jnz 006FD277	iDD.006FD277
006FD1D6	A1 00E57100	mov eax, ds:[71E500]	
006FD1DB	8B00	mov eax, ds:[eax]	

Al salir de un CALL me encuentro con ese JNZ y justo debajo, si no salta, pone BL a 1. Si miro donde me lleva el siguiente salto veo esto:

```
006FD272    E8 A936D6FF     call    00460920        iDD.00460920
006FD277    80FB 01         cmp     bl, 1
006FD27A    74 0E           je      short 006FD28A  iDD.006FD28A
006FD27C    83FE 02         cmp     esi, 2
006FD27F    74 09           je      short 006FD28A  iDD.006FD28A
006FD281    83FE 07         cmp     esi, 7
006FD284    0F85 75FEFFFF   jnz     006FD0FF        iDD.006FD0FF
006FD28A    33C0            xor     eax, eax
```

Puede ser que después de forzar ese segundo salto haga una segunda comprobación y por eso no haga lo que queremos conseguir así que voy a poner un BP en el primer salto y cuando pare voy a cambiar el FLAG Z para que no salte y a ver qué pasa al hacer eso así que pongo el BP, doy a F9 y vuelvo a intentarlo y para en el nuevo BP y cambio el FLAG Z para que no salte y voy traceando con F8 para ver que va haciendo y ya salta solo en el segundo salto ya que primero pasa 1 a EBX y luego copia EBX en EAX y luego xorea AL con 1 y como vale 1 pues se pone EAX a 0. Por último compara EAX con 1 y como no son iguales pues salta en el segundo salto. Luego llega a la comprobación de la imagen de arriba y como BL ahora si vale 1 pues salta y evitamos todos esos saltos y ahí di a F9 y…



Vaya seguridad que tiene el programa jajaja, con un simple salto abro todos los diarios sin saber la clave. Bueno, algo es algo pero yo quiero recuperar mi clave y por aquí no sé como hincarle el diente así que cierro nuevamente el diario y cuando pare en el primer BP cambio el FLAG Z y voy con F8 para ver quién es el

responsable de llamar a esta función ya que no me muestra nada el Olly. Voy saliendo de algunos RETNs y llego aquí:

```
007092CA  >  8B45 E4      mov     eax, ss:[ebp-1C]
007092CD  .  50           push    eax
007092CE  .  A1 0CE37100  mov     eax, ds:[71E30C]
007092D3  .  8B00         mov     eax, ds:[eax]
007092D5  .  8B4D EC      mov     ecx, ss:[ebp-14]
007092D8  .  8B55 F0      mov     edx, ss:[ebp-10]
007092DB  .  E8 6C3DFFFF  call    006FD04C          iDD.006FD04C
007092E0  .  48           dec     eax
007092E1  .v 74 0A        je      short 007092ED    iDD.007092ED
007092E3  .  E8 CCA7CFFF  call    00403AB4          iDD.00403AB4
007092E8  .v E9 F5030000  jmp     007096E2          iDD.007096E2
007092ED  >  A1 C0E77100  mov     eax, ds:[71E7C0]
007092F2  .  8038 00      cmp     byte ptr ds:[eax], 0
007092F5  .v 74 28        je      short 0070931F    iDD.0070931F
```

Pongo un BP en el comienzo de la función, doy a F9 y vuelvo a cerrar el diario y lo vuelvo a abrir para que me vuelva a pedir la pass y esta vez para al comprobar la pass y si traceamos un poquito vemos esto:

```
Address   Hex dump     Disassembly                      Comment
007092B1  .  A1 BCE27100  mov     eax, ds:[71E2BC]
007092B6  .  8B00         mov     eax, ds:[eax]
007092B8  .  8078 47 00   cmp     byte ptr ds:[eax+47], 0
007092BC  .v 74 0C        je      short 007092CA    iDD.007092CA
007092BE  .  A1 BCE27100  mov     eax, ds:[71E2BC]
007092C3  .  8B00         mov     eax, ds:[eax]
007092C5  .  E8 F62AD3FF  call    0043BDC0          iDD.0043BDC0
007092CA  >  8B45 E4      mov     eax, ss:[ebp-1C]
007092CD  .  50           push    eax
007092CE  .  A1 0CE37100  mov     eax, ds:[71E30C]
007092D3  .  8B00         mov     eax, ds:[eax]
007092D5  .  8B4D EC      mov     ecx, ss:[ebp-14]
007092D8  .  8B55 F0      mov     edx, ss:[ebp-10]
007092DB  .  E8 6C3DFFFF  call    006FD04C          iDD.006FD04C
007092E0  .  48           dec     eax
007092E1  .v 74 0A        je      short 007092ED    iDD.007092ED
007092E3  .  E8 CCA7CFFF  call    00403AB4          iDD.00403AB4

Registers (FPU)
ECX 0195400C ASCII "Te_amo_al_1000%"
EDX 026C400C ASCII "Mi vida junto a Ely"
EBX 00000000
EBP 0012FA74
ESI 0012FCF0
EDI 00DDDFB4
EIP 007092DB iDD.007092DB
C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty 5.542637659842661376 0e-4932
ST1 empty 0.266769655095181792 0e-4933
ST2 empty -4.044950770970718208 0e+3080
ST3 empty +UNORM 03AC 00000002 00000395
ST4 empty 5.005777026236472320 0e-4918
ST5 empty 1.000000000000000000 0
ST6 empty 1.000000000000000000 0
ST7 empty 3.472416000000000000 0e+11
               3 2 1 0      E S P U O Z D I
FST 4000  Cond 1 0 0 0  Err 0 0 0 0 0 0 0 0
FCW 1272  Prec NEAR,53  Mask    1 1 0 0 1 0
```

En ECX vemos mi clave original y en EDX el nombre del archivo de diario. Con eso ya me puedo dar por satisfecho aunque no veo la comparación directa pero sabiendo esto ya no volveré a tener el mismo problema con las pass de mis diarios en este programa. Se podría conseguir con un loader sin necesidad de desempacar el ejecutable o desempacando el ejecutable, renombrándolo y haciendo las modificaciones oportunas como por ejemplo un injerto con un MessageBoxW para que nos muestre la pass correcta y listo.
Espero que os haya gustado, hace mucho que no toco la ingeniería inversa así que estoy muy oxidado jejeje.