Cracking virtual dj 7

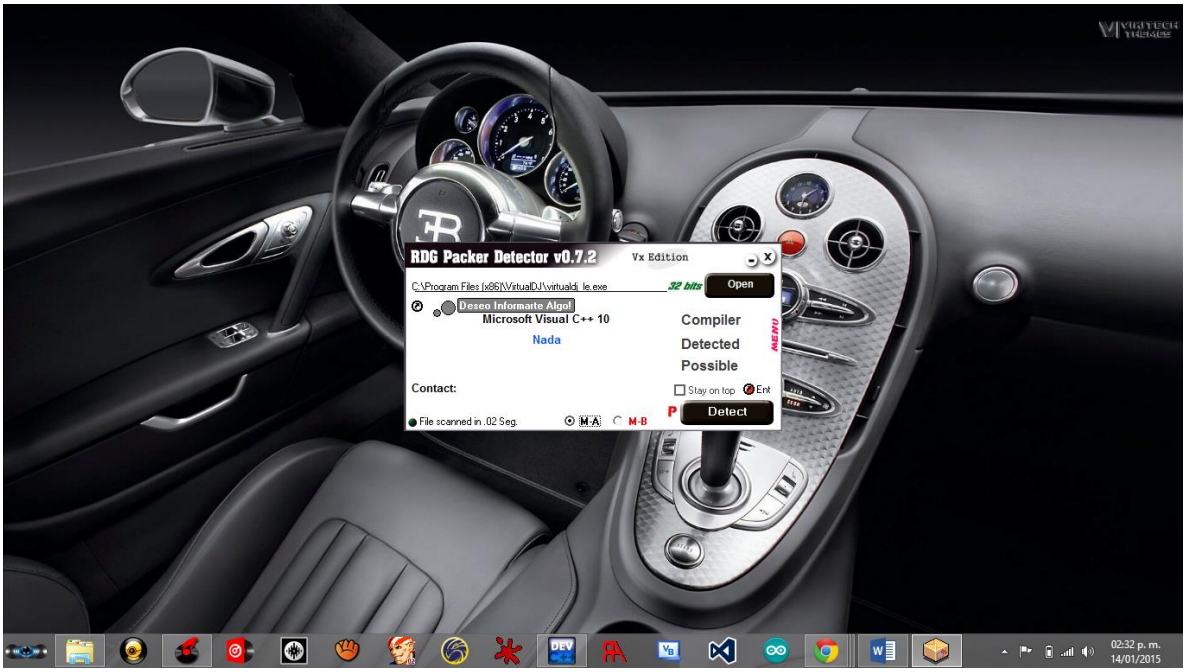
Nombre	Virtual dj
Proteccion	ExeCriptor
objetivo	Hacerlo full, ya que caduca a los 20 dias
Web	http://es.virtualdj.com/download/index.html
Dificultad	Muy facil
Plataforma	Windows 8
Lenguaje	Visual c++
Cracker	Carlos ismael
Fecha	20 de enero del 2015

Bueno mi nombre es Carlos Ismael Tun Tun me da mucho gusto participar difundiendo el conocimiento ademas me gusta, al parecer este es mi primer tutorial cracking, espero no sea el ultimo.

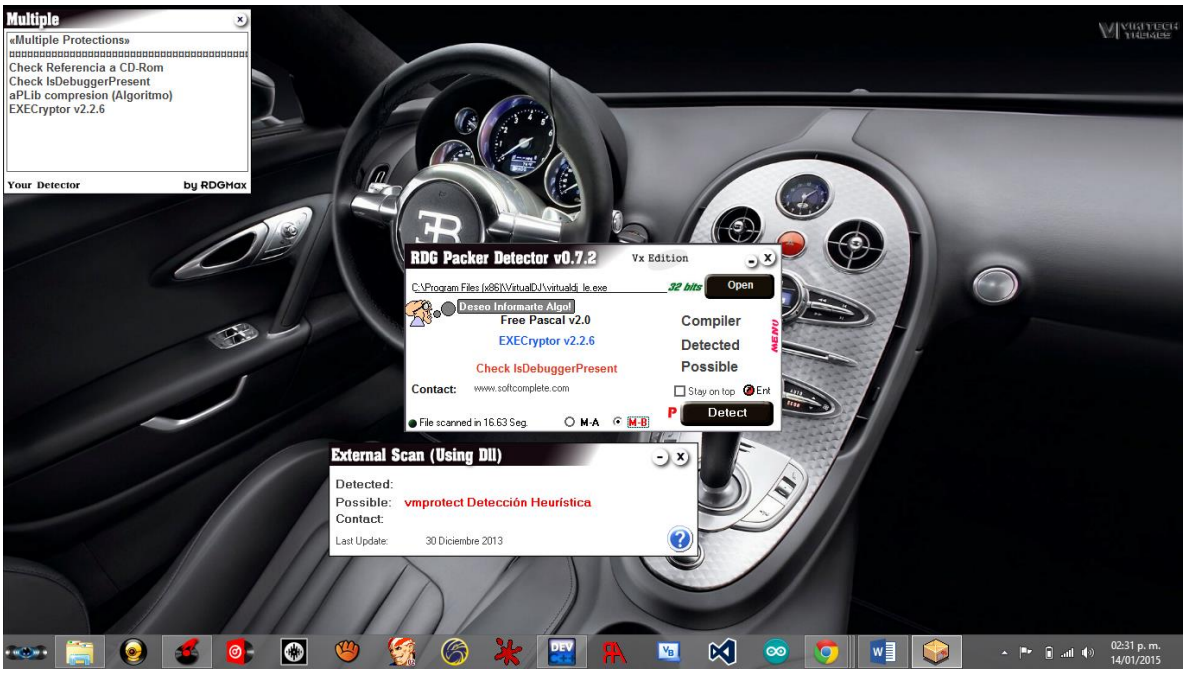
Disclaimer: como es un programa comercial aviso de una ves que este tutorial es con fines educativos y divulgacion de conocimientos, no me hago responsable por el mal uso que se le de a este tutorial.

Sin mas que decir comenzamos:

Lo analizamos con el RDG nos sale esto en modo M-A

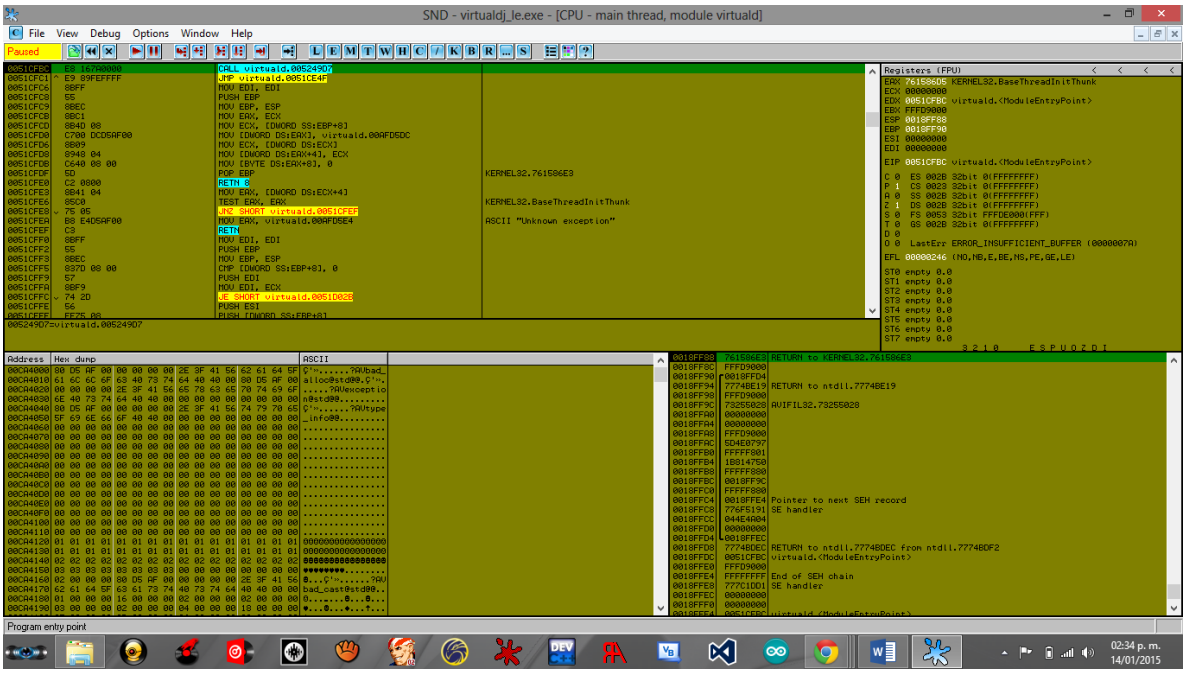


Y en modo M-B tenemos esto



Pero no importa ya que no causa ningun daño.

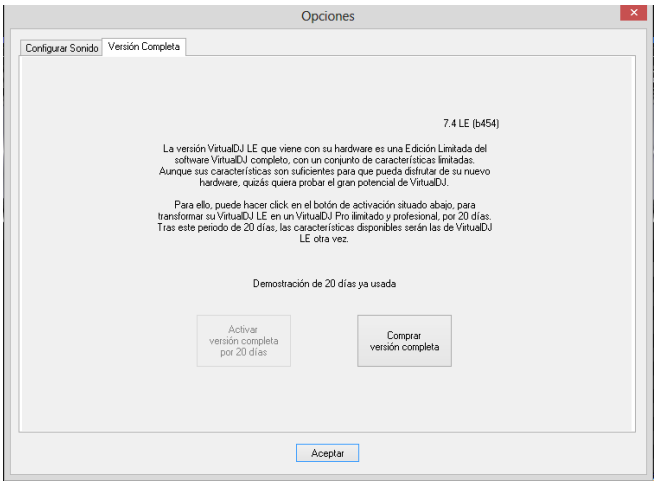
Luego lo abrimos con el olly dbg, y tenemos esto en su entry point.



Este es el programa original, todo parece funcionar como debe ser, pero no es asi, ya que al abrir el menu de config nos damos cuenta de que faltan pestañas en el menu. Eso es asi antes de activar la version de prueba o despues que se nos acaben los 20 dias.

Antes de que se acaben los 20 dias lo podemos usar como si fuese full, eso significa que el codigo del programa full esta ahí, solo hay que encontrarlo! Jejejeje

Así se ve el menú del programa antes de activar la versión de prueba de 20 días y después de que se nos acaben los 20 días



1.-luego pasamos a hacer el primer cambio en el código. Buscamos el CreateWindowExa y le ponemos un breakpoint on import, luego al botón de config y para, bajamos de a poco (7 call´s) hasta llegar a algo parecido a lo que se ve más abajo

Este salto evita que termine el conteo antes de tiempo así el conteo depende del cmp del segundo punto y no de este

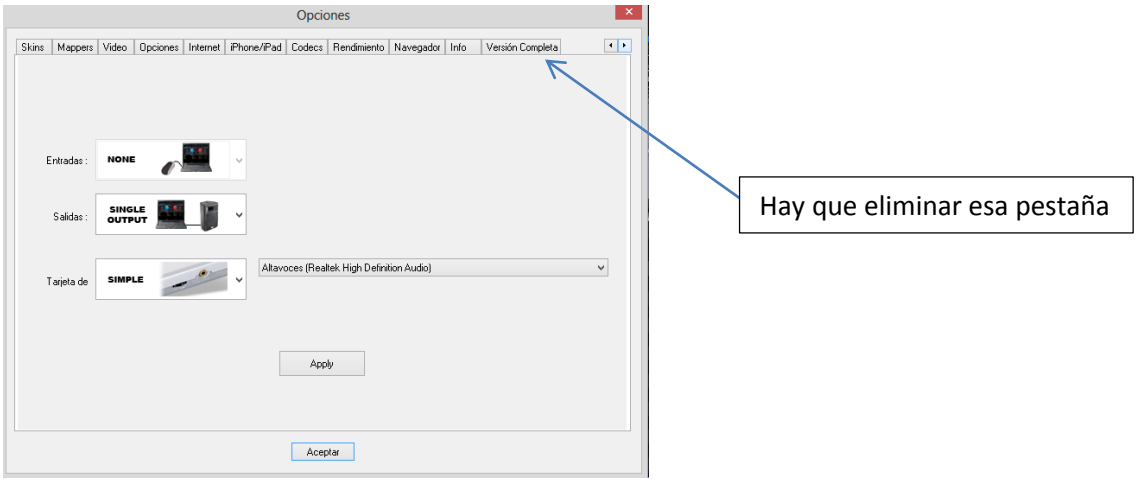
Antes:

```
00472415   897424 14          MOV [DWORD SS:ESP+14], ESI
00472419   85FF               TEST EDI, EDI
0047241B   74 0F              JE SHORT virtuald.0047242C
0047241D   83FE 0B            CMP ESI, 0B
00472420   74 0A              JE SHORT virtuald.0047242C
00472422   85F6               TEST ESI, ESI
00472424   0F85 AE010000      JNZ virtuald.004725D8
0047242A   EB 08              JMP SHORT virtuald.00472434
0047242C   85F6               TEST ESI, ESI
0047242E   0F85 30010000      JNZ virtuald.00472564
```

Este salto y el que le sigue(el segundo hasta el tercero) será cambiado por un nop a lo que queda así, ahora:

```
00472405   C74424 20 09000000  MOV [DWORD SS:ESP+20], 9
0047240D   C74424 18 FFFFFFFF  MOV [DWORD SS:ESP+18], -1
00472415   897424 14           MOV [DWORD SS:ESP+14], ESI
00472419   85FF                TEST EDI, EDI
0047241B   74 0F               JE SHORT virtuald.0047242C
0047241D   83FE 0B             CMP ESI, 0B
00472420   74 0A               JE SHORT virtuald.0047242C
00472422   85F6                TEST ESI, ESI
00472424   90                  NOP
00472425   90                  NOP
00472426   90                  NOP
00472427   90                  NOP
00472428   90                  NOP
00472429   90                  NOP
0047242A   EB 08               JMP SHORT virtuald.00472434
0047242C   85F6                TEST ESI, ESI
0047242E   0F85 30010000       JNZ virtuald.00472564
00472434   83FF 28             CMP EDI, 28
```

Hasta aquí ya queda crackeado el programa y se hace full después del nop:



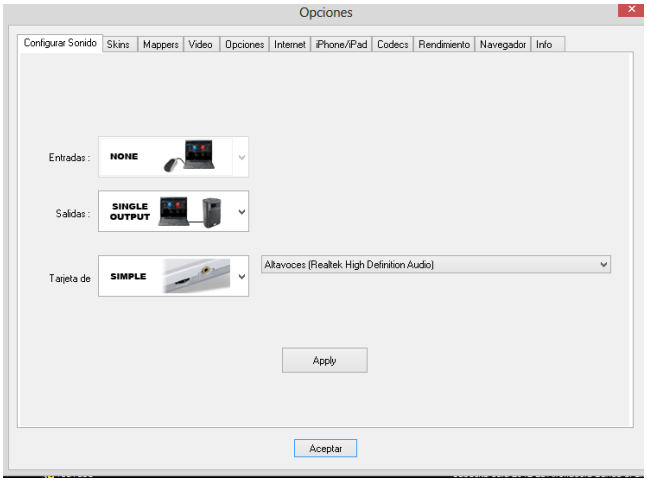
Ay que quitar la pestaña que dice versión completa.

2.-El cambio siguiente es para hacer el conteo de pestañas así en vez de ser 0C o 13decimal le quitamos el ultimo para que no llegue ahí, así se verá mejor, lo encontramos hasta más abajo.

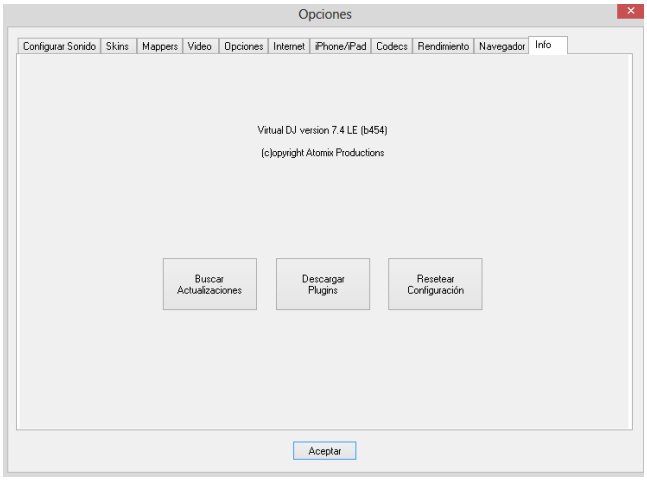
004725DD 83FE 0C CMP ESI, 0C ; cambiamos esto por 0b

```
004725BE   FF15 2887B000      CALL NEAR [DWORD DS:<&USER32.SendMessageA>]
004725C4   C64424 13 01       MOV [BYTE SS:ESP+13], 1
004725C9   8B7424 14          MOV ESI, [DWORD SS:ESP+14]
004725CD   A1 58BD3C01        MOV EAX, [DWORD DS:13CBD58]
004725D2   8B3D 24DFDB00      MOV EDI, [DWORD DS:DBDF24]
004725D8   46                 INC ESI
004725D9   897424 14          MOV [DWORD SS:ESP+14], ESI
004725DD   83FE 0C            CMP ESI, 0C
004725E0   0F8C 33FEFFFF      JL virtuald.00472419
004725E6   8B4424 18          MOV EAX, [DWORD SS:ESP+18]
004725EA   85C0               TEST EAX, EAX
004725EC   79 15              JNS SHORT virtuald.00472603
004725EE   6A 00              PUSH 0
```

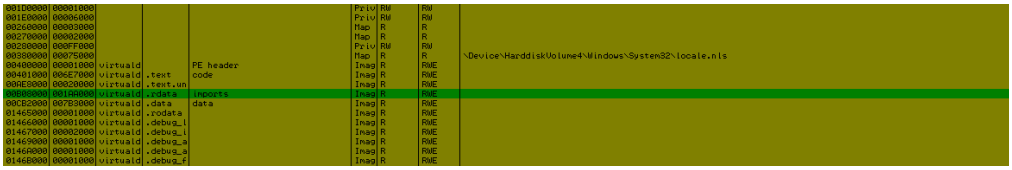
Ya asta aquí ya funciona y corre muy bien y se verá así:



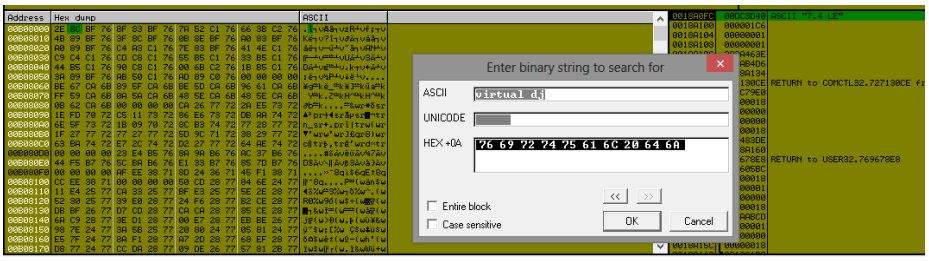
Nuestro siguiente objetivo es lo estético, los nombres o lo que queramos que muestre el programa durante su arranque y que muestro lo mismo u otra cosa en la pestaña de info



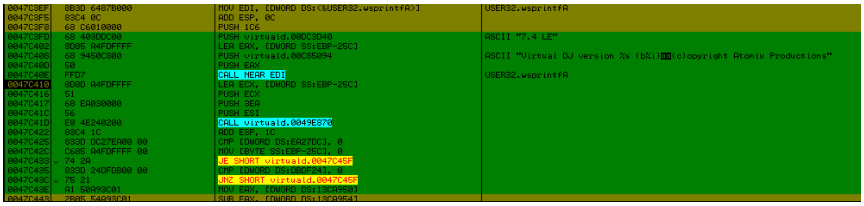
Bueno seguimos, a esa sección le hacemos dump in cpu



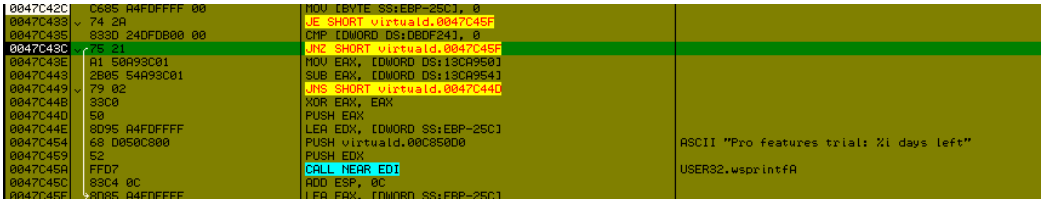
Luego hacemos un search for binary string a virtual dj, tal como lo vemos abajo



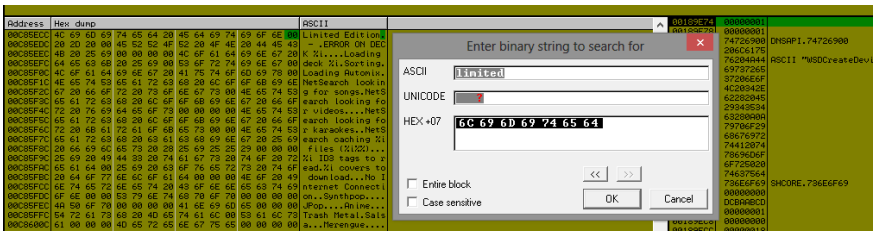
Pasamos dos retn´s hasta que llegamos a una zona parecida a esta:



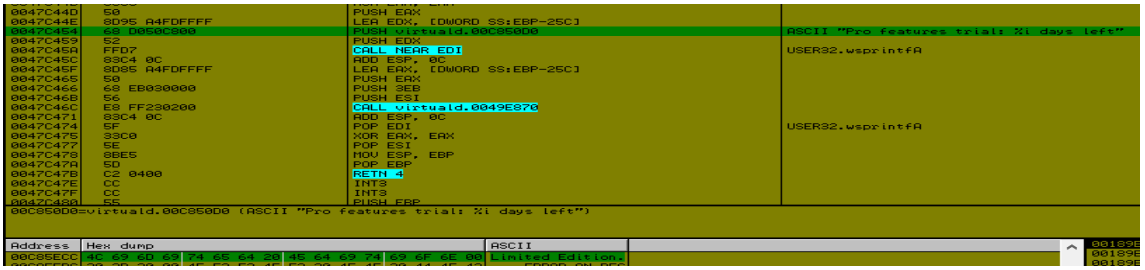
Aquí hay que hacerle nop a este salto para que puedan aparecer las letras, luego lo editamos y ponemos que pushee el mismo del principio



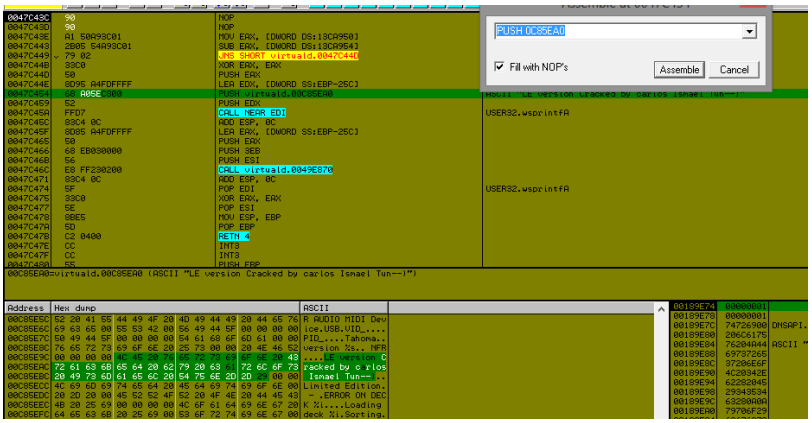
Nos vamos a buscar este texto:



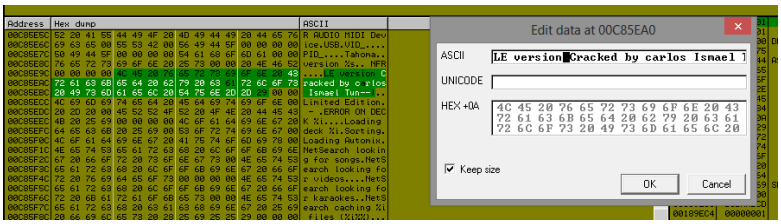
Luego este push



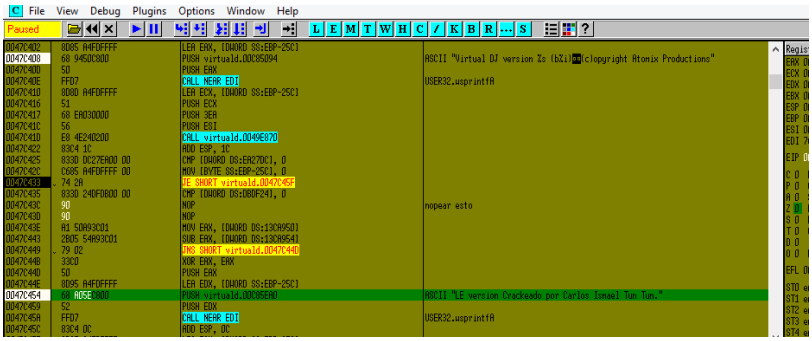
Lo cambiamos así



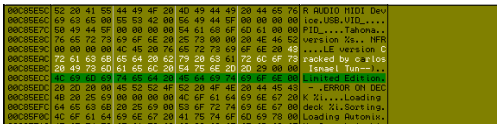
Luego en el dump, hacemos un binary >>edit y queda así



Lo cual queda así:

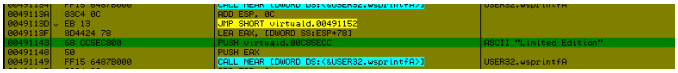


Para cambiar el texto de limited edition que aparece durante el arranque del programa hacemos lo siguiente

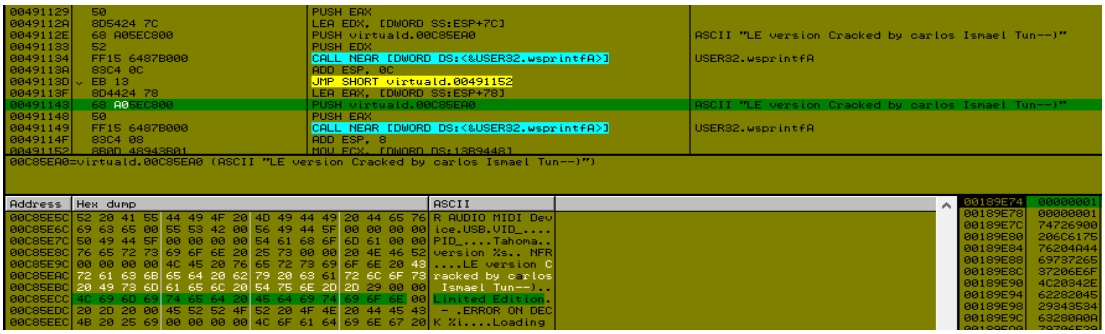


Ctr+R para buscar referencias

Doble click y nos lleva aquí:

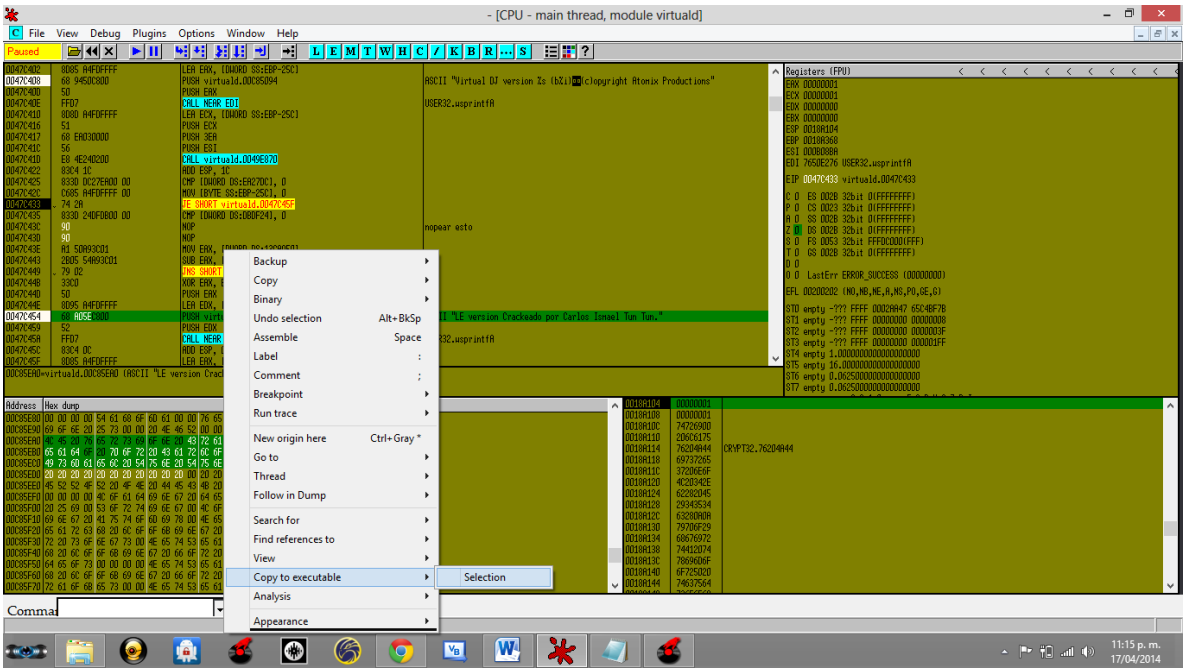


Lo editamos así

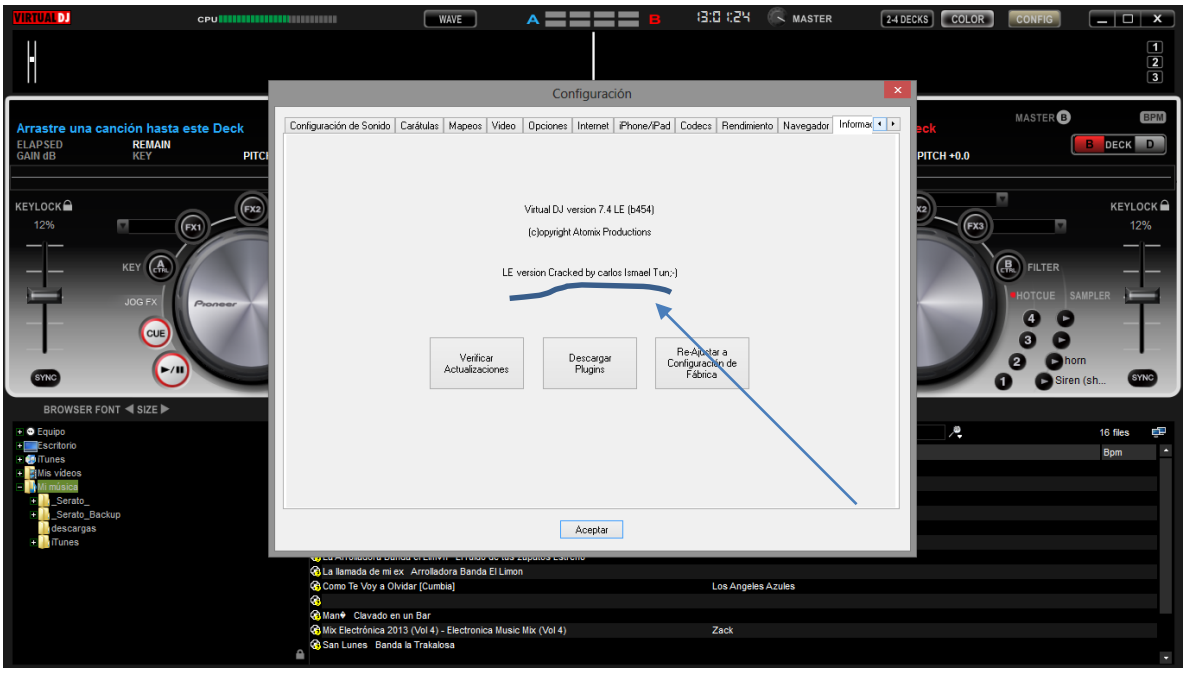


Y ya acabamos….

Guardamos todos los cambios ya sea uno por uno o todos al final y ya esta



Guardamos todos los cambios cerramos todo y verificamos que todo esté bien, en su lugar



Bueno ya podemos respirar tranquilamente, un programa muy facil de editar, no da complicaciones para nada, por cierto ya ha sido crackeado mucho tiempo atrás pero queria ver si lo puedo hacer yo mismo sin ningun tutorial(si es que hay uno jejeje).

Muchas gracias por haber leido este tutorial y un fuerte agradecimiento a los maestros de la lista cracklatinos, al gran maestro Ricardo Narvaja, invision, indulgeo, nox, por sus grandes tutoriales que sin ellos no hubiera podido hacer esto… bueno sin mas que decir me despido dando nuevamente las gracias por haber llegado a leer hasta aquí.