

Cracking virtual dj 7

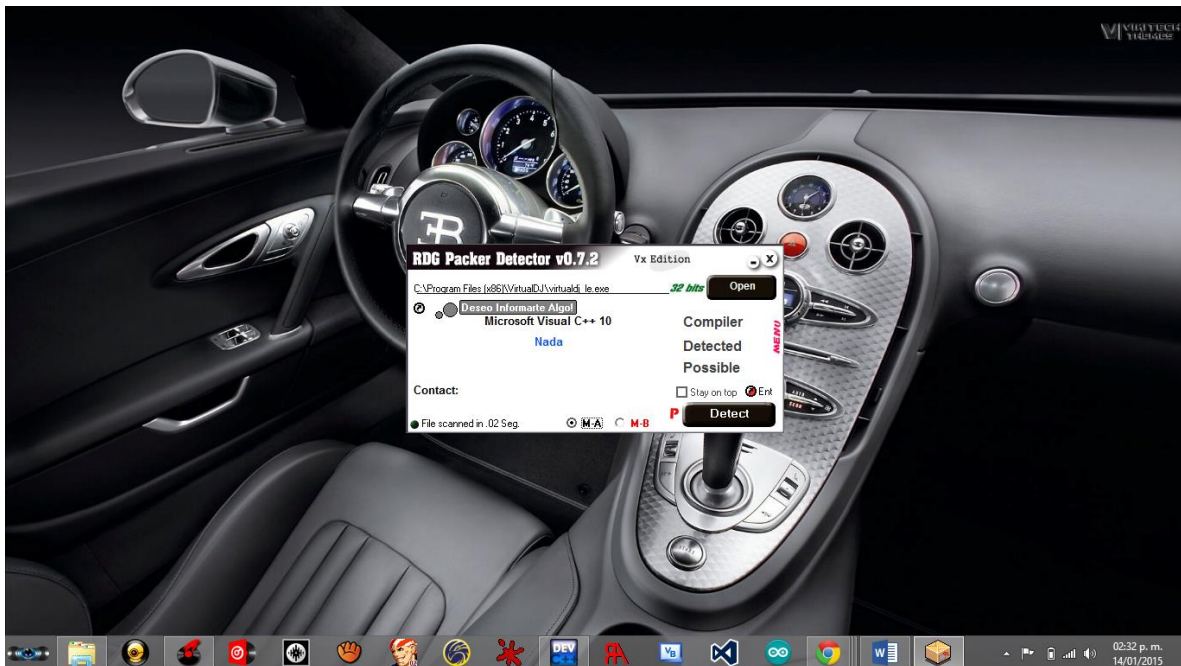
Nombre	Virtual dj
Proteccion	ExeCriptor
objetivo	Hacerlo full, ya que caduca a los 20 dias
Web	http://es.virtualdj.com/download/index.html
Dificultad	Muy facil
Plataforma	Windows 8
Lenguaje	Visual c++
Cracker	Carlos ismael
Fecha	20 de enero del 2015

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.

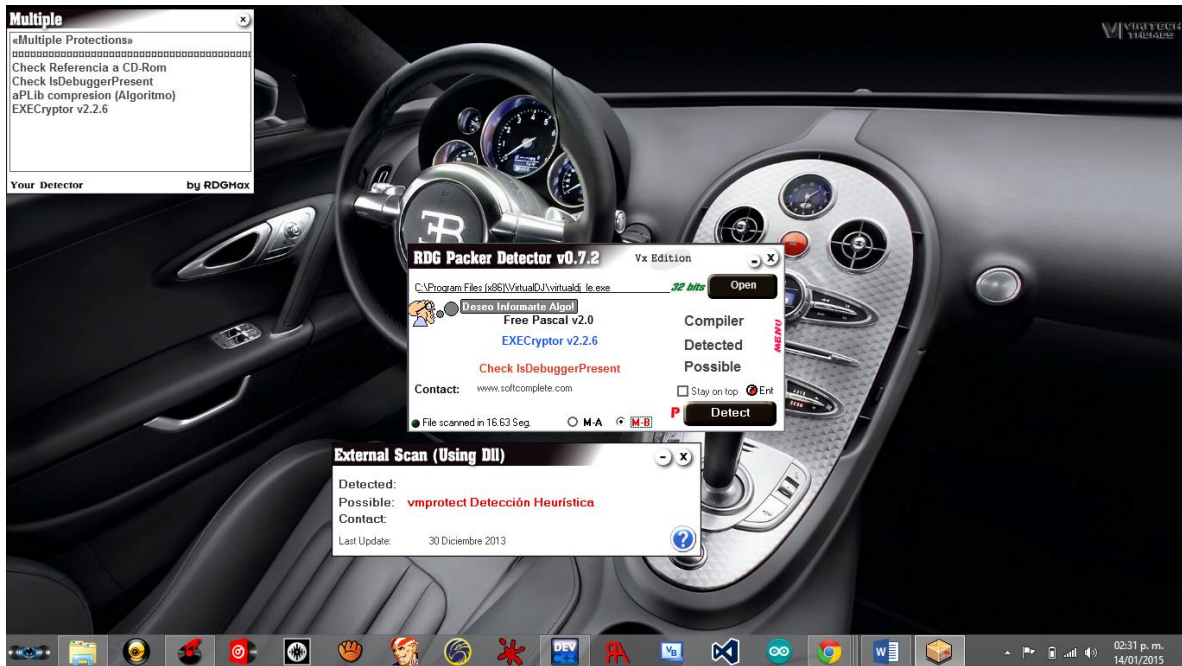
Disclaimer: como es un programa comercial aviso de una vez que este tutorial es con fines educativos y divulgacion de conocimientos, no me hago responsable por el mal uso que se le de a este tutorial.

Sin mas que decir comenzamos:

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

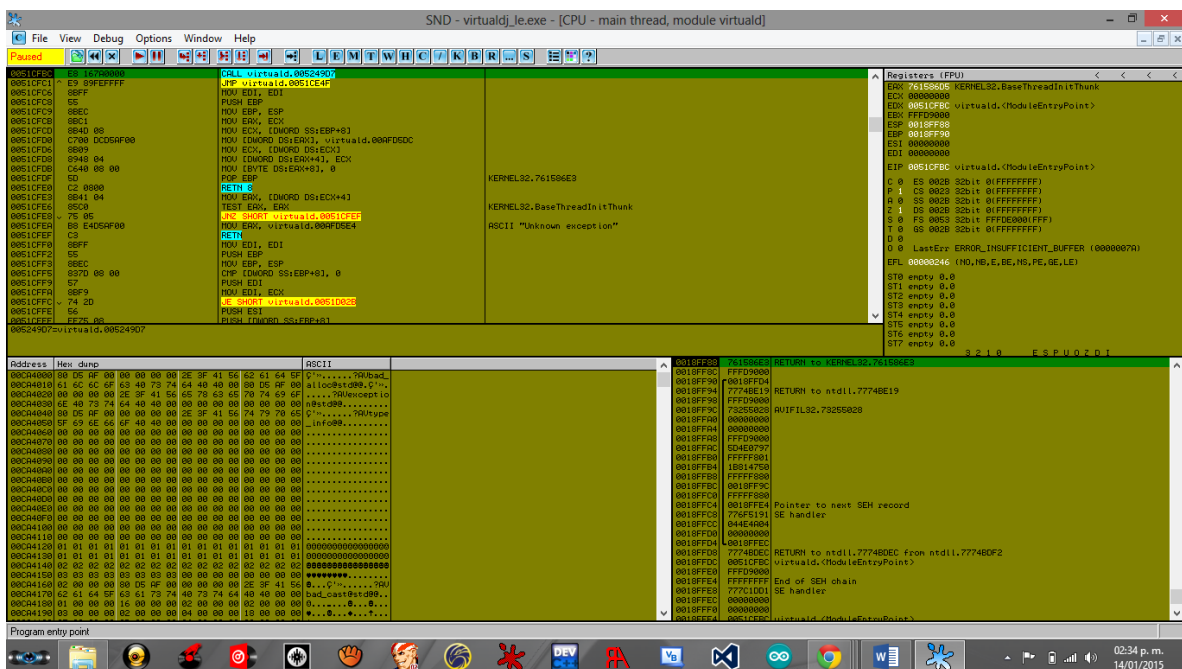


Y en modo M-B tenemos esto



Pero no importa ya que no causa ningun daño.

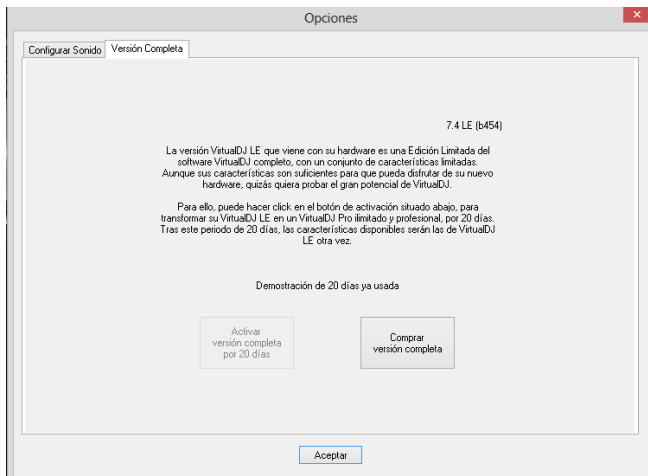
Luego lo abrimos con el olly dbg, y tenemos esto en su entry point.



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 días lo podemos usar como si fuese full, eso significa que el código del programa full está 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

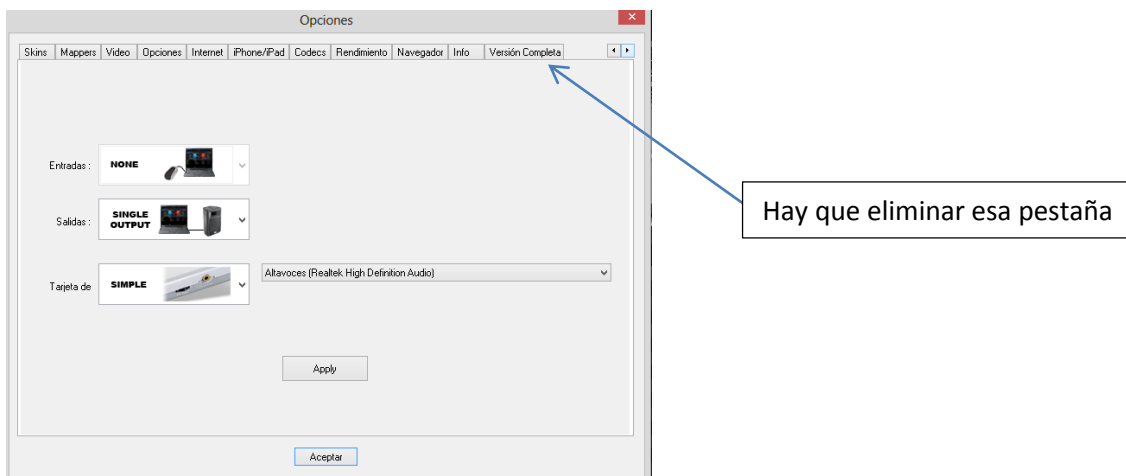
Antes:

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:



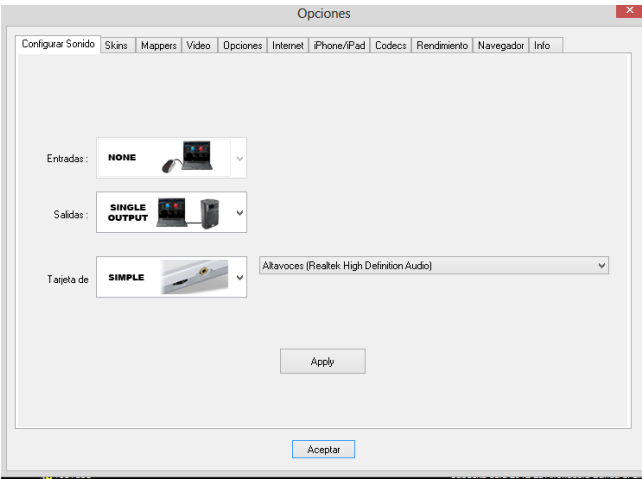
Ay que quitar la pestaña que dice versión completa.

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.

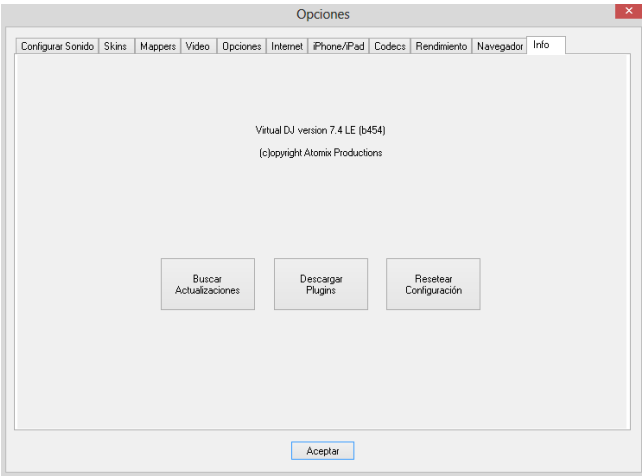
004725DD 83FE 0C CMP ESI, 0C ; cambiamos esto por 0b

004725BE	FF15 28878000	CALL NEAR [DWORD DS:<USER32.SendMessage>]
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:13CB058]
004725D2	8B3D 24DFDB00	MOV EDI, [DWORD DS:DBDF24]
004725D8	46	INC ESI
004725D9	897424 14	MOV [DWORD SS:ESP+14], ESI
004725DB	83FE 0C	CMP ESI, 0C
004725E0	0F8C 33FEFFFF	JL virtuald.00472419
004725E6	8B4424 18	MOV EAX, [DWORD SS:ESP+18]
004725EA	85CD	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:



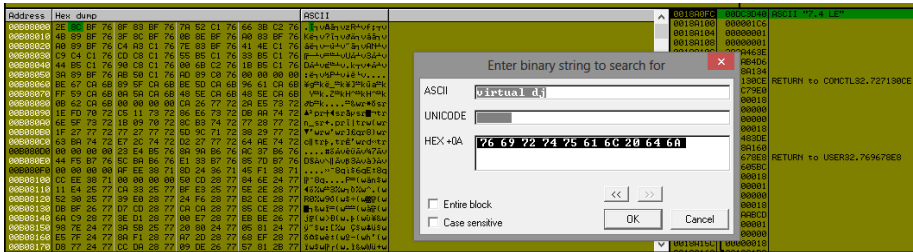
Nuestro siguiente objetivo es lo estético, los nombres o lo que queramos que muestre el programa durante su arranque y que muestro lo mismo u otra cosa en la pestaña de info



Bueno seguimos, a esa sección le hacemos dump in cpu

00100000	00001000				Priv	RM	
00100000	00000000				Priv	RM	
00200000	00000000				Priv	R	
00270000	00000000				Priv	R	
00280000	0000FF00				Priv	RM	
00300000	00007000				Priv	R	
00400000	00001000	virtuald		PE header	Priv	R	~Device-Harddisk\Volume4\Windows\System32\locale.nls
00401000	000E7000	virtuald	.text	code	Priv	R	
00402000	00000000	virtuald	.text.un		Priv	R	
00600000	00100000	virtuald	.xdata	imports	Priv	R	
00602000	00700000	virtuald	.data	data	Priv	R	
01465000	00001000	virtuald	.xdata		Priv	R	
01466000	00001000	virtuald	.debug_l		Priv	R	
01467000	00000000	virtuald	.debug_l		Priv	R	
01468000	00001000	virtuald	.debug_a		Priv	R	
01469000	00001000	virtuald	.debug_a		Priv	R	
0146B000	00001000	virtuald	.debug_l		Priv	R	

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:

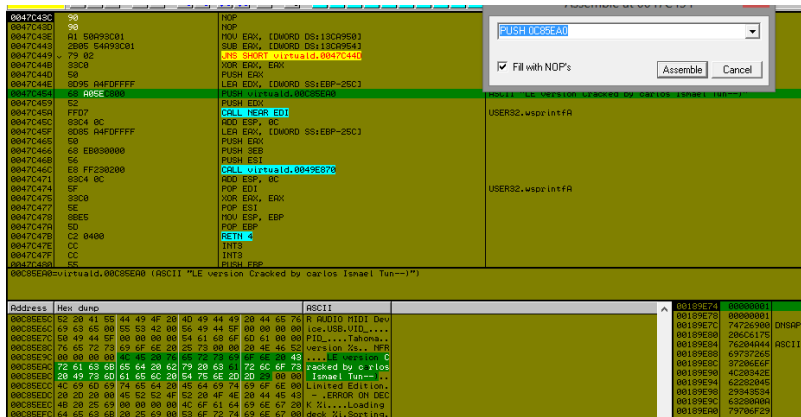
0047C3E7	8B30 84F00000	MOV EDI, [DWORD DS:USER32.wsprintfA]	USER32.wsprintfA
0047C3F5	83C4 0C	ADD ESP, 0C	
0047C3F8	68 C6D10000	PUSH 10E	
0047C3FE	68 44D00000	PUSH virtuald.0047C394	ASCII "7.4 LE"
0047C402	8085 84F0FFFF	LEA EAX, [DWORD DS:EBP-25C]	
0047C406	68 74D00000	PUSH virtuald.00C85800	ASCII "Virtual D3 version 3.0 (c) 1999 Microsoft. All Rights Reserved"
0047C40A	58	PUSH EDX	
0047C410	FFD0	CALL NEAR EDI	USER32.wsprintfA
0047C416	8085 84F0FFFF	LEA EAX, [DWORD DS:EBP-25C]	
0047C41A	51	PUSH ECX	
0047C41F	68 D2D00000	PUSH 32	
0047C425	58	PUSH EDI	
0047C428	68 4E240000	CALL virtuald.0049E876	
0047C432	58C4 1C	ADD ESP, 1C	
0047C435	8330 DC2E0000	CMPL [DWORD DS:EBP+70C], 0	
0047C438	2505 84F0FFFF	JNZ SHORT virtuald.0047C45F	
0047C43B	74 50	JZ SHORT virtuald.0047C45F	
0047C43E	8085 84F0FFFF	LEA EAX, [DWORD DS:EBP-25C]	
0047C442	75 21	JNC SHORT virtuald.0047C45E	
0047C445	A1 50A93C01	MOV EAX, [DWORD DS:13CR950]	
0047C448	2B05 54A93C01	SUB EAX, [DWORD DS:13CR954]	
0047C44B	79 82	JNS SHORT virtuald.0047C44E	
0047C44D	33C0	XOR EAX, EAX	
0047C44E	50	PUSH EAX	
0047C44F	8D95 84F0FFFF	LEA EDI, [DWORD SS:EBP-25C]	
0047C454	68 D05C8000	PUSH virtuald.00C85800	ASCII "Pro features trial: %i days left"
0047C459	52	PUSH EDX	
0047C45A	FFD0	CALL NEAR EDI	USER32.wsprintfA
0047C45C	83C4 0C	ADD ESP, 0C	
0047C45F	8085 84F0FFFF	LEA EAX, [DWORD SS:EBP-25C]	

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

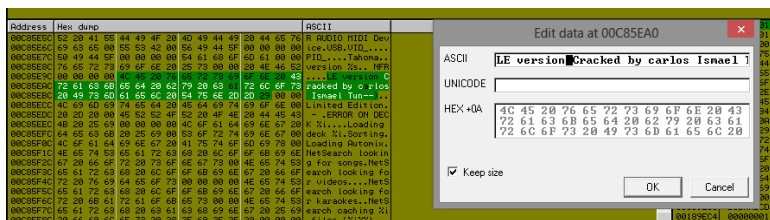
0047C42C	C685 84F0FFFF	00	MOV LEAVE SS:EBP-25C], 0	
0047C43F	74 20		JZ SHORT virtuald.0047C45F	
0047C43E	8330 24D00000	00	CMPL [DWORD DS:EBP+24], 0	
0047C43C	75 21		JNC SHORT virtuald.0047C45E	
0047C43E	A1 50A93C01		MOV EAX, [DWORD DS:13CR950]	
0047C443	2B05 54A93C01		SUB EAX, [DWORD DS:13CR954]	
0047C449	79 82		JNS SHORT virtuald.0047C44E	
0047C44B	33C0		XOR EAX, EAX	
0047C44D	50		PUSH EAX	
0047C44F	8D95 84F0FFFF		LEA EDI, [DWORD SS:EBP-25C]	
0047C454	68 D05C8000		PUSH virtuald.00C85800	ASCII "Pro features trial: %i days left"
0047C459	52		PUSH EDX	
0047C45A	FFD0		CALL NEAR EDI	USER32.wsprintfA
0047C45C	83C4 0C		ADD ESP, 0C	
0047C45F	8085 84F0FFFF		LEA EAX, [DWORD SS:EBP-25C]	

Nos vamos a buscar este texto:

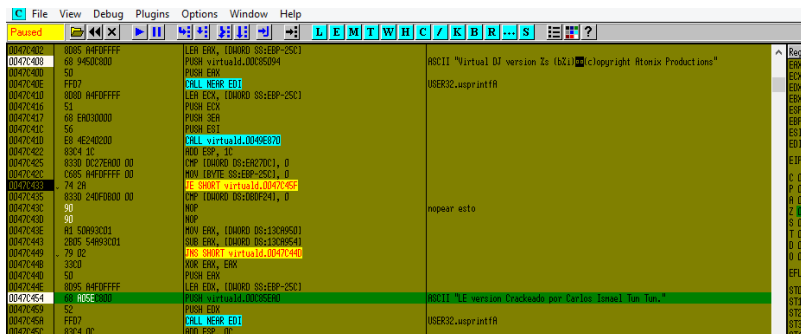
Address	Hex dump	ASCII
00C85ECC	4C 69 60 69 74 65 64 20 46 64 69 74 69 6F 6E	00000001
00C85ED0	20 20 80 45 52 62 52 4F 4E 59 44 45 43	00000001
00C85ED4	4B 20 25 69 00 00 00 00 4C 6F 61 64 69 6E	74726900
00C85ED8	64 65 69 20 25 69 00 00 53 62 72 74 69 6E	20616176
00C85EDC	4C 6F 61 64 69 6E 67 20 41 75 74 6F 60	76204044
00C85EE0	4E 65 74 65 6E 72 69 69 20 6F 6F 68 69 6E	69737265
00C85EE4	67 20 66 6F 72 20 73 6F 6E 6F 67 73 00	3720656F
00C85EE8	65 61 72 63 68 20 6C 6F 6F 68 69 6E 67	4C20432E
00C85EEC	72 20 76 69 64 65 6F 73 00 00 00 4E 65	62203045
00C85EF0	65 61 72 63 68 20 6C 6F 6F 68 69 6E 67	23452034
00C85EF4	20 66 69 6C 65 73 20 25 69 25 25 29 00	63200000
00C85EF8	61 64 00 25 69 20 63 6F 76 65 72 73 20	67720020
00C85EFC	65 61 64 00 25 69 20 63 6F 76 65 72 73	73706F20
00C85F00	25 69 20 44 33 20 74 61 67 73 20 74 6F	68676972
00C85F04	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F08	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F0C	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F0E	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F10	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F12	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F14	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F16	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F18	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F1A	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F1C	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F1E	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F20	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F22	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F24	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F26	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F28	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F2A	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F2C	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F2E	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F30	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F32	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F34	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F36	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F38	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F3A	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F3C	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F3E	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F40	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F42	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F44	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F46	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F48	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F4A	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F4C	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F4E	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F50	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F52	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F54	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F56	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F58	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F5A	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F5C	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F5E	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F60	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F62	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F64	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F66	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F68	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F6A	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F6C	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F6E	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F70	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F72	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F74	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F76	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F78	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F7A	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F7C	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F7E	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F80	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F82	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F84	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F86	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F88	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F8A	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F8C	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F8E	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F90	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F92	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F94	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F96	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F98	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85F9A	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85F9C	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85F9E	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85FA0	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85FA2	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85FA4	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85FA6	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85FA8	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85FAA	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85FAC	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85FAE	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85FB0	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85FB2	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85FB4	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85FB6	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85FB8	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85FBA	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85FBC	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85FBE	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85FBF	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85FC0	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85FC2	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85FC4	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85FC6	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85FC8	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85FCA	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85FCC	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85FCE	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85FCF	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85FD0	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85FD2	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85FD4	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85FD6	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85FD8	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85FDA	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85FDE	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85FDF	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85FE0	65 61 64 00 25 69 20 63 6F 76 65 72 73	74412074
00C85FE2	65 61 64 00 25 69 20 63 6F 76 65 72 73	7869606F
00C85FE4	65 61 64 00 25 69 20 63 6F 76 65 72 73	67720020
00C85FE6	65 61 64 00 25 69 20 63 6F 76 65 72 73	7441



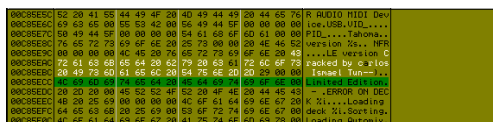
Luego en el dump, hacemos un binary >>edit y queda así



Lo cual queda así:

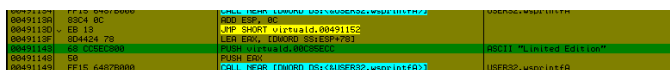


Para cambiar el texto de limited edition que aparece durante el arranque del programa hacemos lo siguiente



Ctrl+R para buscar referencias

Doble click y nos lleva aquí:

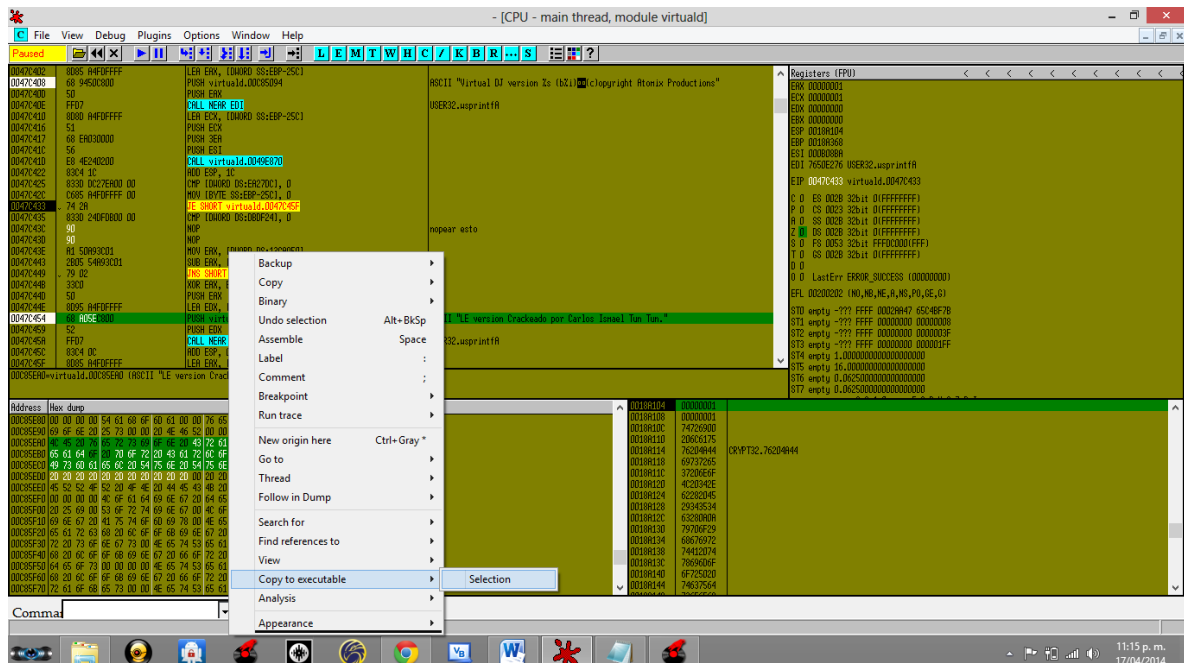


Lo editamos así

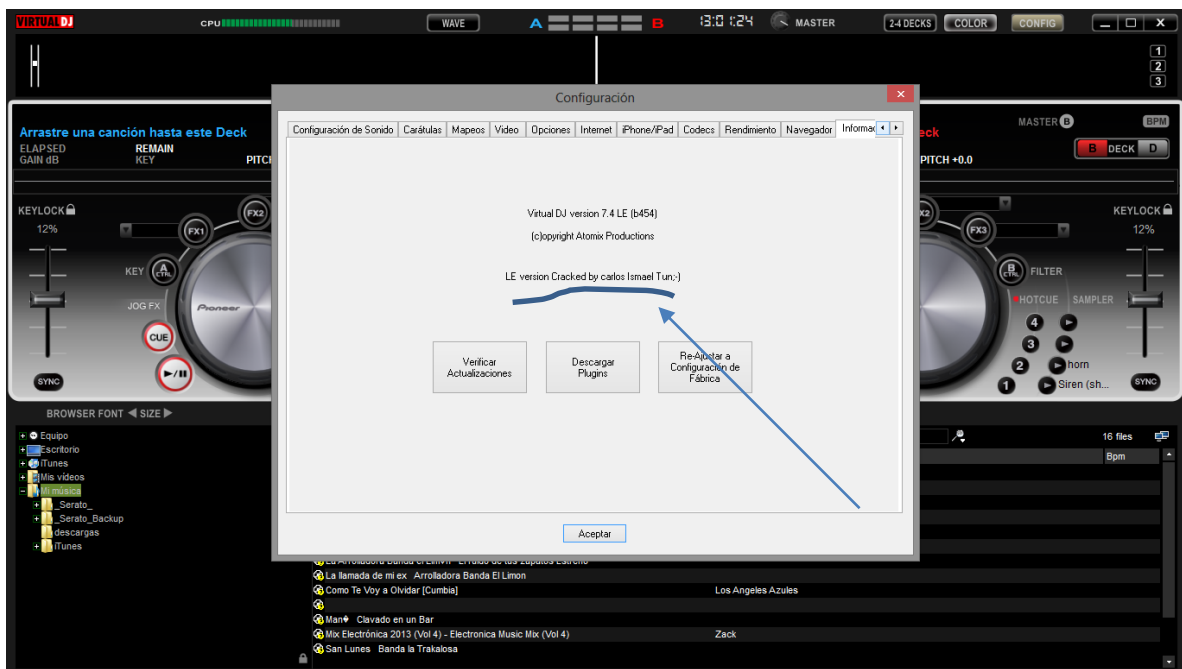
00491129	50		PUSH EAX		
0049112A	805424 7C		LEA EAX, [DWORD SS:ESP+7C]		
0049112E	60 805EC800		PUSH virtuald.00C85E80		ASCII "LE version Cracked by carlos Ismael Tun--")"
00491133	52		PUSH EDI		
00491134	FF15 6487B000		CALL NEAR [DWORD DS:<USER32.usprintfA>]		USER32.usprintfA
0049113A	89C4 0C		ADD ESP, 10		
0049113D	EB 13		JMP SHORT virtuald.00491152		
0049113F	8D424 78		LEA EAX, [DWORD SS:ESP+78]		
00491143	60 805EC800		PUSH virtuald.00C85E80		ASCII "LE version Cracked by carlos Ismael Tun--")"
00491148	50		PUSH EDI		
00491149	FF15 6487B000		CALL NEAR [DWORD DS:<USER32.usprintfA>]		USER32.usprintfA
0049114F	89C4 08		ADD ESP, 8		
00491152	ADDI 48343601		ADD EAX, [DWORD DS:13634481]		
00C85E80=virtuald.00C85E80 (ASCII "LE version Cracked by carlos Ismael Tun--")"					
Address	Hex dump		ASCII		
00C85E50	52 20 41 55	44 49 4F 20	40 49 44 49	20 44 65 76	R AUDIO MIDI Dev
00C85E60	69 63 65 00	55 53 42 00	56 49 44 5F	00 00 00 00	ice,USB,VIL,....
00C85E70	50 49 44 5F	00 00 00 00	54 61 68 6F	60 61 00 00	PID,....Tahona..
00C85E80	76 65 72 73	69 6F 6E 20	25 73 00 00	20 4E 46 52	version %s. NFR
00C85E90	00 00 00 00	40 45 20 76	65 73 73 69	5F 6E 20 48LE version C
00C85EA0	72 31 65 68	65 64 20 62	79 20 65 61	72 60 6F 73	Cracked by Carlos
00C85EB0	20 49 73 60	61 65 6C 20	54 75 6E 20	2D 29 00 00	Ismael Tun--)...
00C85EC0	4C 69 60 69	74 65 64 20	45 64 69 74	69 6F 6E 00	Limited Edition.
00C85ED0	20 2D 20 00	45 52 52 4F	52 2D 4F 4E	20 44 45 48	- .ERROR ON DEC
00C85EE0	4B 20 25 69	00 00 00 00	4C 6F 61 64	69 6E 67 20	K X!....Loading

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 leído 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.