

# Cracks Latinos Team

## Iv!N\$0n

Programas	Easy Mp3 Ogg Wma Wav Cutter 1.91 y 1.95
Descarga	<a href="http://www.mediafire.com/?2ce03czf2cebours">http://www.mediafire.com/?2ce03czf2cebours</a>
Dificultad	Depende
Herramientas	Olly, RDG.
Objetivo	Encontrar serial válido y/o parchear.
Protección	Packer
Cracker	Iv!N\$0n
Tutorial Nº	1

### Introducción

Hola, listeros y lectores en general, quiero darles un saludo cordial. En este primer, tutorial intentaré conseguir un serial válido y/o parchear poniendo en práctica lo aprendido en los materiales realizados por varios integrantes de CLS, especialmente, a Ricardo Narvaja por su paciencia enorme. Sobre todo cuando trazó casi todo un programa en P-Code en el tutorial Nº 31 de introducción al cracking desde cero para que entendamos su funcionamiento. Eso digno de admirar.

Empecemos.

### Conociendo a nuestra víctima:

Instalemos Mp3 Cutter 1.91 el de la imagen de abajo.



Busquemos Easy Mp3 Ogg Wma Wav Cutter 1.91 que se encuentra en "C:\Archivos de programa\Free Audio Pack\Easy Audio Cutter\AudioCutter.exe"

Le haré los chequeos necesarios para determinar si está empacado o no.



Como podemos ver está empacado con ASPack v2.12.

Antes de desempacar, miremos como es el proceso de registro. Al ejecutarlo, nos sale el mensaje de "Versión expirada". En mi caso, porque adelanté el reloj. Pero, no importa si ha expirado o no. (Es un trial de 30 días)



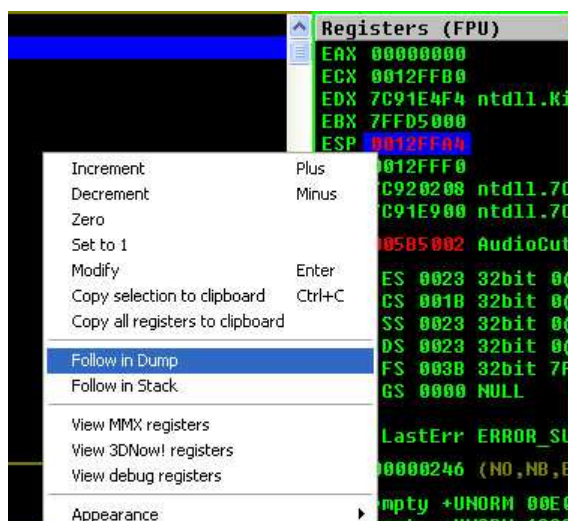
Demos a registrar e introduzcamos un Nombre o Serial cualquiera.



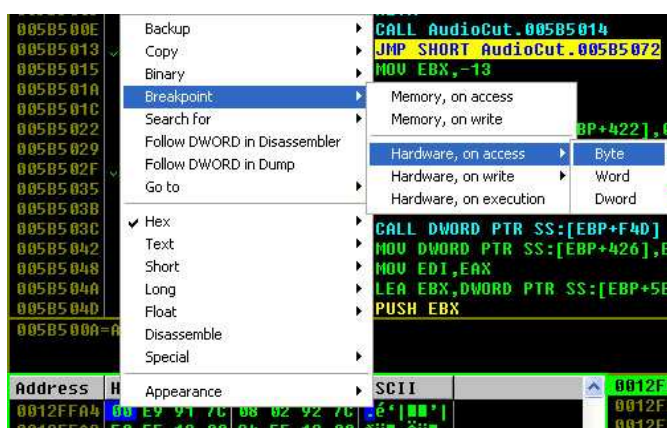
Típico cartel que muestra Olly para indicar que el programa a desensamblar está empacado. Demos click en “No”.



Lo primero que vemos es el **EntryPoint** del packer que comienza con un **PUSHAD**. Aplicaremos el método **PUSHAD/POPAD**. Presionamos **F7** una sola vez. Luego, vamos al registro **ESP** y le damos click derecho/**Follow in Dump**.



En el Dump, pondremos un BPMB en el primer Byte.



Demos Run.





Tracemos con F7 hasta el segundo RETN. Al pasar ese RETN, ya llegamos directamente al OEP.

```

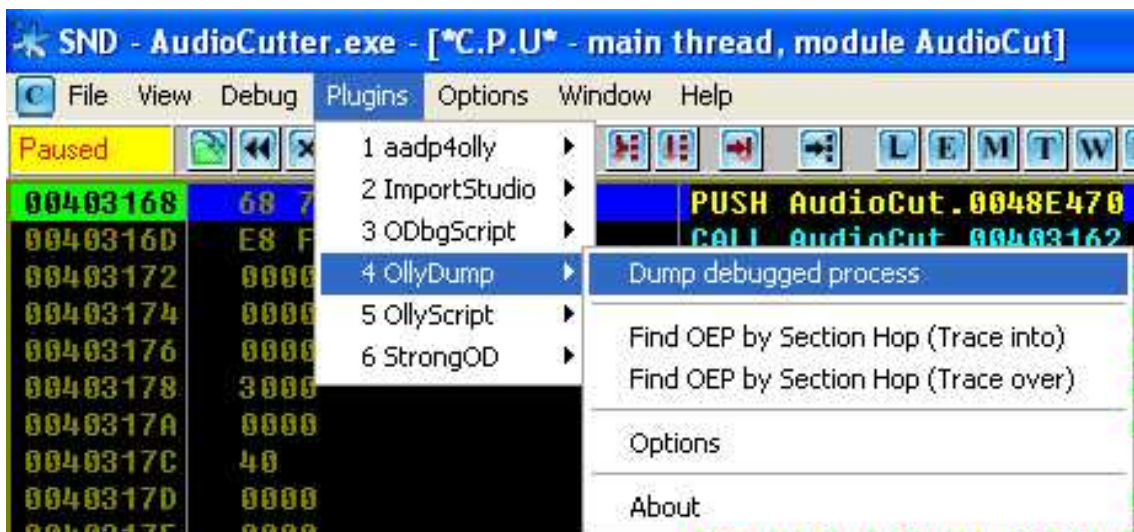
005B53B8 75 08 JNZ SHORT AudioCut.005B53BA
005B53B2 B8 01000000 MOV EAX,1
005B53B7 C2 0C00 RETN 0C
005B53BA 68 68314000 PUSH AudioCut.00403168
005B53BF C3 RETN
  
```

OEP: 00403168

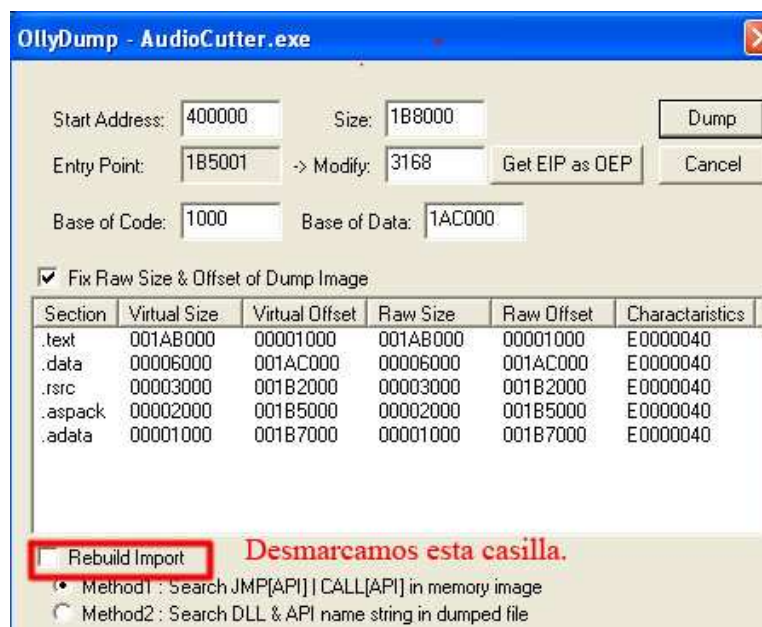
```

00403168 68 70E44800 PUSH AudioCut.0048E470
0040316D E8 F0FFFFFF CALL AudioCut.00403162
  
```

Dumpearemos con el plugin de Olly.

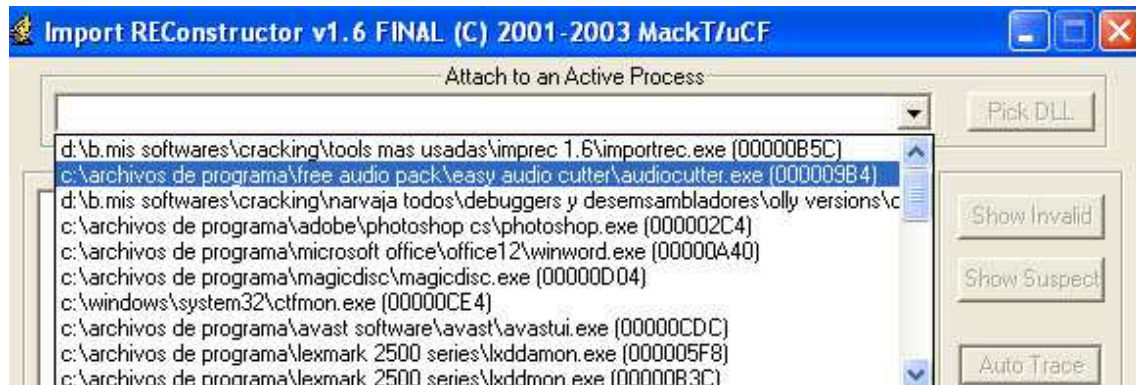


Desmarcamos la casilla Rebuild Import.



Le damos click a “Dump” y lo guardaremos con el nombre de AudioDumped.

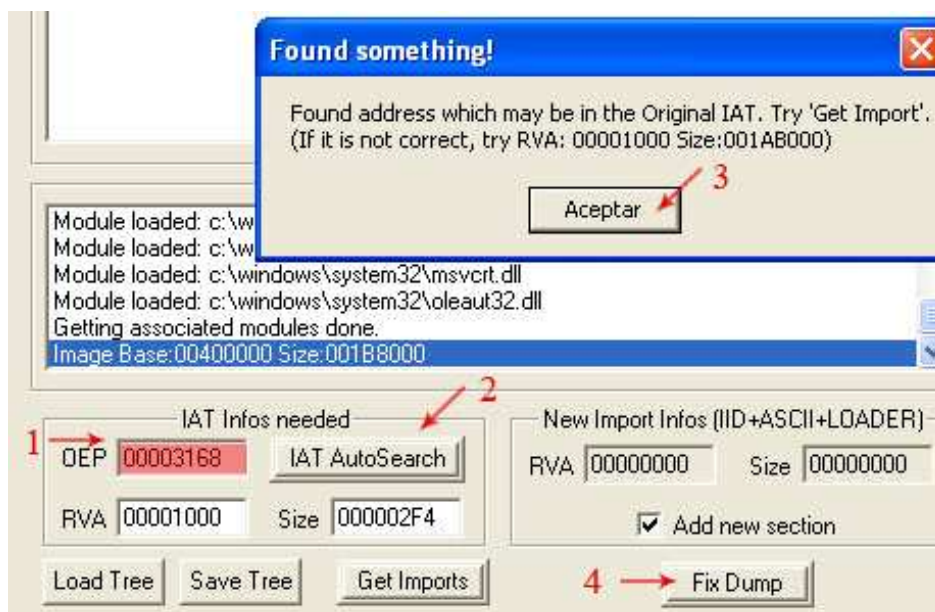
Parados en el “OEP”, abrimos ImportRec y seleccionamos el proceso AudioCutter.exe.



Modificaremos **001B5001** colocando el “OEP” correcto restándole la ImageBase.  
**00403168-400000= 3168.**



Debe quedar como la imagen siguiente siguiendo los pasos del 1-4.

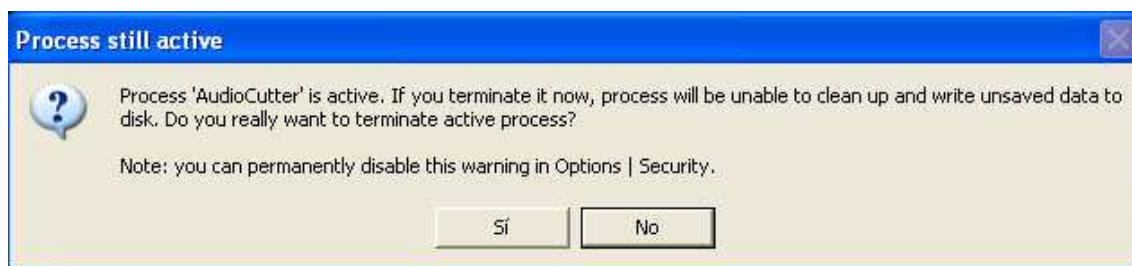


Al darle “Fix Dump”, buscamos el archivo AudioDumped.exe y lo arreglamos. Ya tenemos el archivo desempaado. (Si todos los packers fueran tan fáciles como este, el cracking sería muy mecánico y aburrido. Por eso, practicaré desempaando Armadillos, ExeCriptor, Enigma, etc. Que requieren más atención. Uff, lo que me tocará.)

Chequeamos nuevamente AudioDumped\_.exe con el detector RDG.



Abramos el desempaado AudioDumped\_.exe, que arreglamos en ImportRec, en Olly.

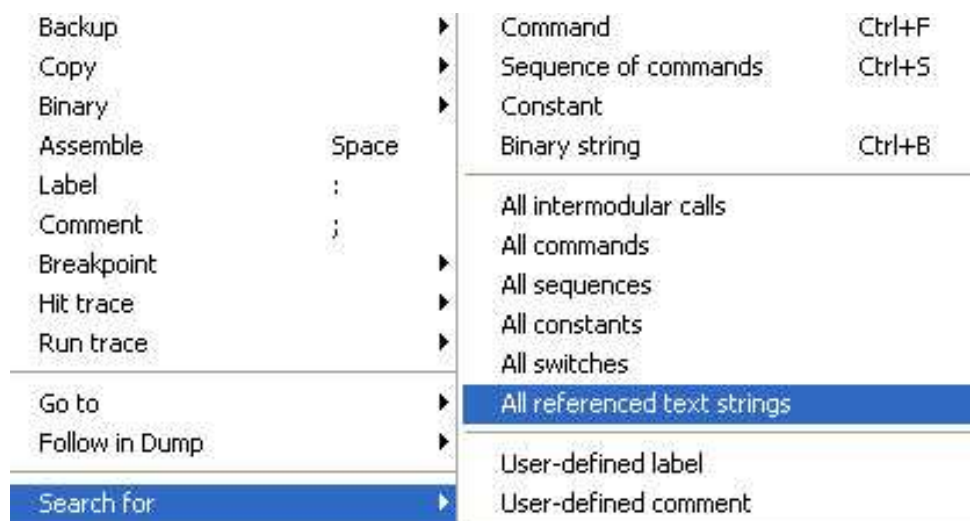


Nos pregunta si deseamos terminar el proceso de AudioCutter.exe. Click en “Sí”.



Veamos las “Strings” o cadenas de texto para ver si encontramos algo interesante.





Veo algo que me llama mucho la atención: “EAC-” varias veces.



Aquí, en mi lógica de novato, me imagino que la más importante de todas esas instancias de “EAC-” debería ser la última la que cocine el serial definitivo. Pongamos un BP justo allí en 0058026B (en mi máquina) de todas maneras, es en el último “EAC-”.

Demos “Run”. Vayamos a “Registrar” y escribamos de nuevo los datos.





Para aquí:

Address	Disassembly	Comment
00580268	PUSH EAX	
00580270	PUSH EAX	
00580271	CALL ESI	
00580273	MOV EDI,DWORD PTR DS:[<msubvm60. __vbaStr	
00580279	MOV EDX,EAX	
0058027B	LEA ECX,DWORD PTR SS:[EBP-4C]	
0058027E	CALL EDI	
00580280	MOV ECX,DWORD PTR SS:[EBP-3C]	
00580283	PUSH EAX	
00580284	PUSH ECX	
00580285	CALL DWORD PTR DS:[<msubvm60. __vbaStr14	
00580288	MOV EDX,EAX	
0058028D	LEA ECX,DWORD PTR SS:[EBP-50]	
00580290	CALL EDI	
00580292	PUSH EAX	
00580293	CALL ESI	
00580295	MOV EDX,EAX	
00580297	LEA ECX,DWORD PTR SS:[EBP-44]	
0058029A	CALL EDI	
0058029C	LEA EDX,DWORD PTR SS:[EBP-50]	
0058029F	LEA EAX,DWORD PTR SS:[EBP-4C]	
005802A2	PUSH EDX	
005802A3	PUSH EAX	

Register	Value
EAX	001717C4
ECX	00120000
EDX	0015F650
EBX	73484C74
ESP	0012E258
EBP	0012E300
ESI	734868BA
EDI	734A77C1
EIP	00580268

En EAX, vemos que se está creando un posible serial para mi nombre:

EAC-11446150941364313178

Tracemos con F8. Al llegar al segundo Call ESI, vemos que es una llamada a la API `vbaStrCat` que concatena/une "Strings" o cadenas de texto. Y Luego, en `00580295`, vemos el posible producto final. Recién salido del horno.

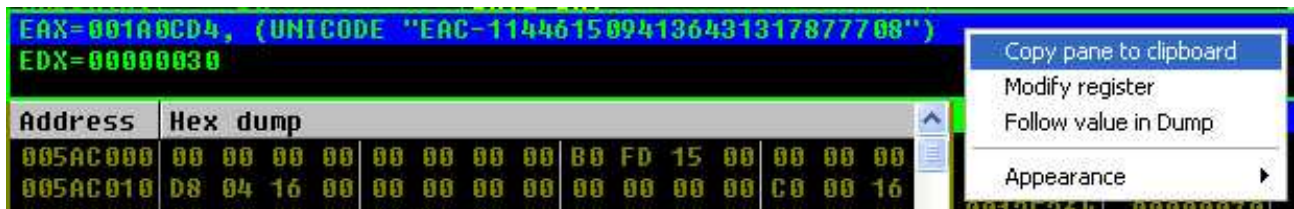
ESI 734868BA msubvm60. \_\_vbaStrCat

Address	Disassembly	Comment
00580293	CALL ESI	
00580295	MOV EDX,EAX	
00580297	LEA ECX,DWORD PTR SS:[EBP-4C]	
0058029A	CALL EDI	
0058029C	LEA EDX,DWORD PTR SS:[EBP-50]	
0058029F	LEA EAX,DWORD PTR SS:[EBP-4C]	
005802A2	PUSH EDX	
005802A3	PUSH EAX	

EAX=001A0CD4, (UNICODE 'EAC-1144615094136431317877708')

Resultado

Demos click derecho **Copy Pane to Clipboard** (Copiar al portapapeles).



Pegamos en el Block de notas, por ejemplo.

EAX=001A0CD4, (UNICODE "EAC-1144615094136431317877708")

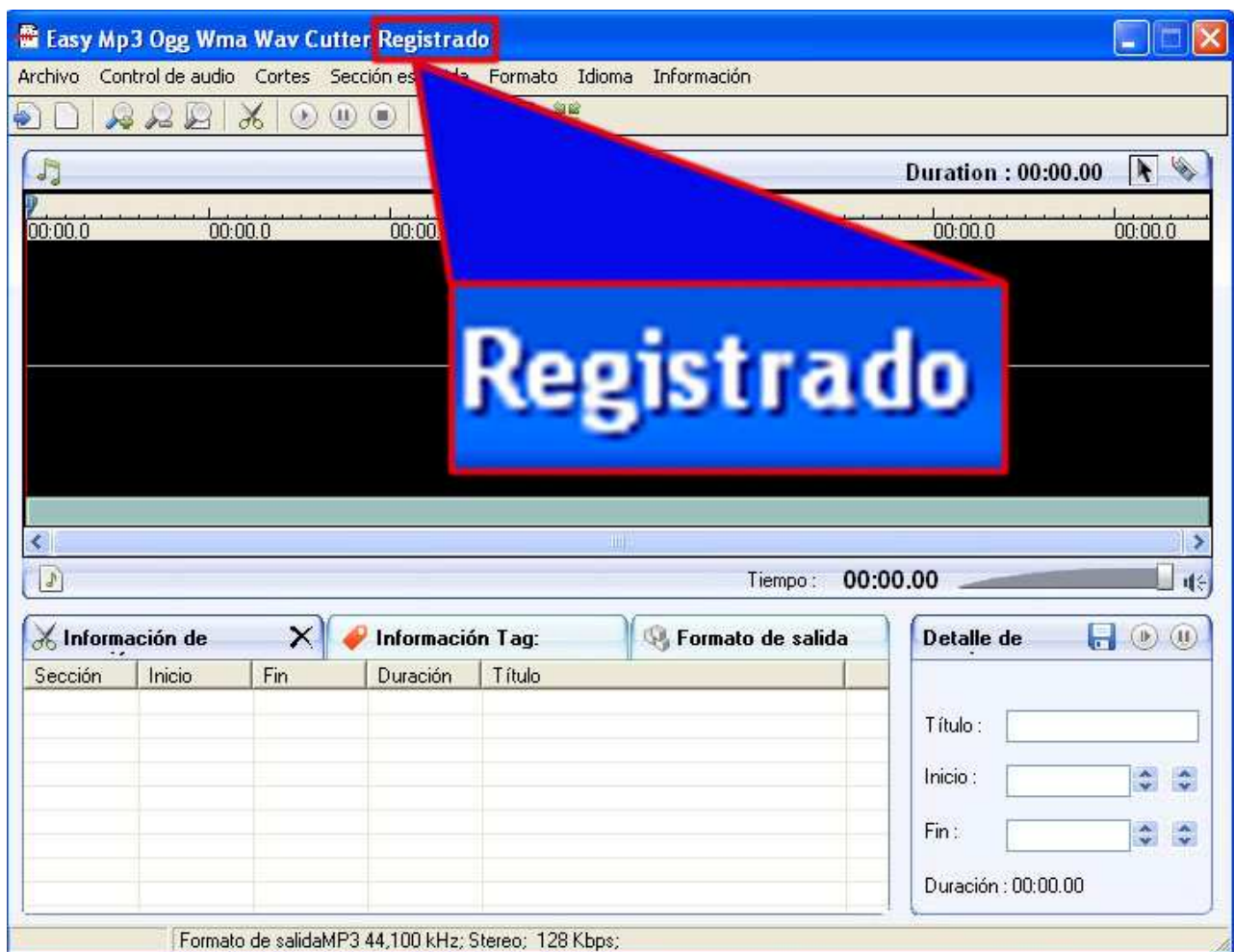
EDX=00000030

Probemos este serial: **EAC-1144615094136431317877708**

Nombre: Ivinson



Y voila....



Aprovechemos para ver la lista negra que tiene este programita.

```

0059BC2F PUS UNICODE "EMBRACE"
0059BC4E PUS UNICODE "TEAM CAT 2005"
0059BC60 PUS UNICODE "freserials.com"
0059BC8C PUS UNICODE "www.serials.ws"
0059BCAB PUS UNICODE "[8C^~^}8]"
0059BCCA PUS UNICODE "Evaluation Version"
0059BCE9 PUS UNICODE "www.serialsdb.com"
0059BD08 PUS UNICODE "www.funmania.net.ru"
0059BD27 PUS UNICODE "www.bg-warez.org"
0059BD46 PUS UNICODE "GaBoR"
0059BD65 PUS UNICODE "Kamtna / AC"
0059BD84 PUS UNICODE "Kamtna / AC"
0059BDA3 PUS UNICODE "Kamtna / AC"
0059BDC2 PUS UNICODE "Kamtna / AC"
0059BDE1 PUS UNICODE "Kamtna"
0059BE33 MO\ UNICODE "TEAM"

```

Que bueno que no aparece CracksLatinos porque somos muy buenos.

Ahora, intentemos parchearlo para que agarre cualquier serial y cualquier nombre.

Abramos nuevamente el programa desempacado en Olly.

Aplicaremos mi **Técnica del Final**. Busquemos en las Strings.



```

0059F10C MOV DWORD PTR SS:[EBP-001],AudiDump.0049E7EC UNICOD "Your licence key is no more Valid. Please go to http://www.koyotesoft.com/en/contact.html and click "
0059F10E MOV DWORD PTR SS:[EBP-001],AudiDump.0049E7EC UNICOD "Easy Audio Cutter"
0059F110 MOV DWORD PTR SS:[EBP-001],AudiDump.0049E7EC UNICOD "Your licence key is no more Valid. Please go to http://www.koyotesoft.com/en/contact.html and click "
0059F112 MOV DWORD PTR SS:[EBP-001],AudiDump.0049E7EC UNICOD "Easy Audio Cutter"
0059F114 MOV DWORD PTR SS:[EBP-001],AudiDump.0049E7EC UNICOD "Your licence key is no more Valid. Please go to http://www.koyotesoft.com/en/contact.html and click "
0059F116 MOV EDX,AudiDump.0049E7EC UNICOD "Nom"
0059F118 MOV EDX,AudiDump.0049EB6C UNICOD "LICENCE"
0059F11A MOV EDX,AudiDump.0049EB80 UNICOD "Code"

```

Le pondré un poco de “zoom” a la últimas 4 líneas.

```

0059F538 MOV DWORD PTR SS:[EBP-001],AudiDump.0049E7EC UNICOD "Your lice
0059F6B0 MOV EDX,AudiDump.0049E7EC UNICOD "Nom"
0059F6BE MOV EDX,AudiDump.0049EB6C UNICOD "LICENCE"
0059F70B MOV EDX,AudiDump.0049EB80 UNICOD "Code"

```

Your Licence key is no more valid. Please go to <http://www.coyotesoft.com/en/contact.html> and click. Aparece 17 veces.

Y al final, dice:

Nom:

LICENCE:

Code:

La lógica me dice que, por lo menos, debería haber un salto condicional que decida si registrarnos completando los datos arriba mencionados o mandarnos a “ver si el gallo puso”. (Modismo Venezolano para decir “Go to hell”)

Demos doble click a “0057F70B Nom”.

```

0059F698 . FF15 3C114000 CALL DWORD PTR DS:[<&msubum60.__vbaStrCopy
0059F69E . 0FBFC8 MOVSX ECX,AX
0059F6A1 . 85C9 TEST ECX,ECX
0059F6A3 . 0F84 16050000 JE AudiDump.0059F8BF
0059F6A9 . C745 FC CA0001 MOV DWORD PTR SS:[EBP-4],0CA0001
0059F6B0 . BA ECE74900 MOV EDX,AudiDump.0049E7EC UNICOD "Nom"
0059F6B5 . 8D4D A0 LEA ECX,DWORD PTR SS:[EBP-6]
0059F6B8 . FF15 30124000 CALL DWORD PTR DS:[<&msubum60.__vbaStrCopy
0059F6BE . BA 6CEB4900 MOV EDX,AudiDump.0049EB6C UNICOD "LICENCE"
0059F6C3 . 8D4D A4 LEA ECX,DWORD PTR SS:[EBP-5]
0059F6C6 . FF15 30124000 CALL DWORD PTR DS:[<&msubum60.__vbaStrCopy
0059F6CC . 8D55 BC LEA EDX,DWORD PTR SS:[EBP-4]
0059F6CF . 52 PUSH EDX
0059F6D0 . 8D45 A0 LEA EAX,DWORD PTR SS:[EBP-6]
0059F6D3 . 50 PUSH EAX
0059F6D4 . 8D4D A4 LEA ECX,DWORD PTR SS:[EBP-5]
0059F6D7 . 51 PUSH ECX
0059F6D8 . 68 50C55A00 PUSH AudiDump.005AC55A
0059F6DD . E8 3EEAFCFF CALL AudiDump.0056E120
0059F6E2 . 8BD0 MOV EDX,EAX
0059F6E4 . 8D4D A0 LEA ECX,DWORD PTR SS:[EBP-6]
0049E7EC=AudiDump.0049E7EC (UNICOD "Nom")

```

Se ve muy jugosa esta parte. En 0059F698, vemos un CALL a "vbaVarTstEq".

Según el tuto Nº 26, Cracking desde cero de Ricardo, dice lo siguiente:

"iii) \_\_vbavartsteq - Compara dos variables si son iguales."

Tsteq =Test Equal-Probar igualdad.

Ese salto "JE" en 0059F6A3 Cambiémoslo por "JNZ" que es todo lo contrario. Compare todo lo que quiera. Así haga 50.000.000.000 de operaciones matemáticas. Va a depender de un "JE". (2 miserables letras que al cambiarlas por "JNZ" le tirarán a la basura todo el esfuerzo que hizo el programador para proteger a su creación a través de un serial) "JE" es el encargado de dar el visto bueno. Pero, nuestro amigo "JNZ" lo va a sustituir y a dejarnos entrar cada vez que queramos.

Quedaría así:

0059F6A1	. 85C9	TEST ECX,ECX	
0059F6A3	. 0F85 16050000	JNZ AudIDump.0059F8BF	
0059F6A9	. C745 FC CA0000	MOV DWORD PTR SS:[EBP-4],0C	
0059F6B0	. BA ECE74900	MOV EDX,AudIDump.0049E7EC	UNICODE "Nom"
0059F6B5	. 8D4D A0	LEA ECX,DWORD PTR SS:[EBP-6	
0059F6B8	. FF15 30124000	CALL DWORD PTR DS:[<&msubvum	msubvum60.__vbaStrCopy
0059F6BE	. BA 6CEB4900	MOV EDX,AudIDump.0049EB6C	UNICODE "LICENCE"
0059F6C3	. 8D4D A4	LEA ECX,DWORD PTR SS:[EBP-5	
0059F6C6	. FF15 30124000	CALL DWORD PTR DS:[<&msubvum	msubvum60.__vbaStrCopy
0059F6CC	. 8D55 BC	LEA EDX,DWORD PTR SS:[EBP-4	
0059F6CF	. 52	PUSH EDX	
0059F6D0	. 8D45 A0	LEA EAX,DWORD PTR SS:[EBP-6	
0059F6D3	. 50	PUSH EAX	
0059F6D4	. 8D4D A4	LEA ECX,DWORD PTR SS:[EBP-5	
0059F6D7	. 51	PUSH ECX	
0059F6D8	. 68 50C55A00	PUSH AudIDump.005AC550	
0059F6DD	. E8 3EEAFCFF	CALL AudIDump.0056E120	
0059F6E2	. 8BD0	MOV EDX,EAX	
0059F6E4	. 8D4D AC	LEA ECX,DWORD PTR SS:[EBP-6	
0059FBBF=AudIDump.0059F8BF			

Quitemos todos los "breakpoints". Vayamos a "C:\Documents and Settings\Ivinson\Datos de programa\FreeAudioPack\EasyCutter.ini"

Obviamente, va a ser la dirección de ustedes. La única diferencia es el nombre de usuario de Windows.

Este programa crea un archivo: EasyCutter.ini. Borremos lo que puse en rojo.

[WMA]

WMASUPPORT=False

[Lang]

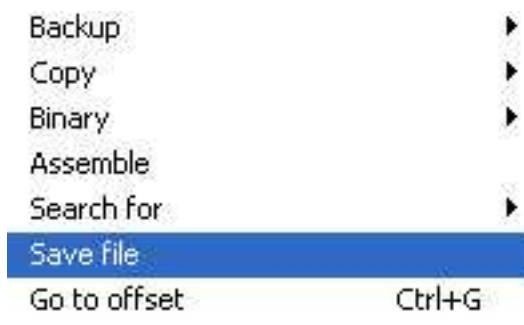
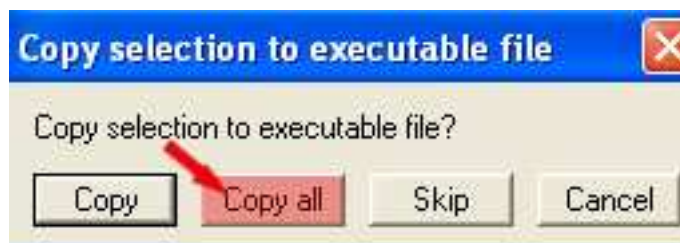
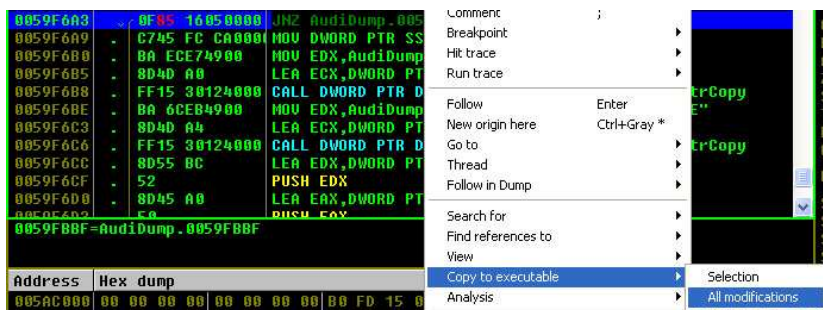
Val=Español

[LICENCE]

Nom=Ivinson

Code=EAC-1144615094136431317877708

Para volver a quedar: No registrado o “Unregistered”. Volvamos a Olly. Guardemos los cambios.



Guardémoslo con el nombre “parcheado.exe” o como ustedes quieran. Pero, deben guardarlo en la carpeta de instalación donde está el original. Cerremos Olly. Ejecutemos el “parcheado.exe” y coloquemos, por ejemplo:

Nombre: CracksLatinos

Serial: 9898989898989898

OK. Y al meternos en Información/Acerca de, vemos en “User”/Usuario:





Le eché un vistazo a la versión 1.95 y el proceso para obtener el serial es idéntico al que acabamos de hacer. La única diferencia es que el **OEP** es **403208**.

Por lo que, ya tenemos el **OEP** menos la “**Imagebase**”= **3208** para el ImportRec.

Espero hayan disfrutado este tutorial Nº 1. Mientras vaya aprendiendo, me gustaría ir aportando mis conocimientos aunque no sean avanzados, pero, para allá vamos.

Críticas constructivas, sugerencias u otras acotaciones, por favor, enviarlas a mi correo: [ipadilla63@gmail.com](mailto:ipadilla63@gmail.com)

“Si lo puedes imaginar, lo puedes lograr” Albert Einsten.

PD: Gracias a este programa conocí la excelente lista CracksLatinos.

Érase una vez, yo descargué un programa por cortar archivos Mp3, el cual, después de usarlo por un mes (30 días). Me mostró un cartel muy simpático diciéndome con un amable sarcasmo que ya se me había acabado el tiempo de uso y que debería comprarlo. Al leer esa mala noticia, me dispuse a buscar un serial por la web. De tanto buscar quedé agotado. Hasta que, de repente, vi una puerta hacia el éxito, decía CracksLatinos. El nombre me pareció muy original. El sitio parecía una biblioteca en donde estaban casi todas las herramientas esperando por mi para darles uso y poder comprender lo que me había pasado y como solventarlo.

He aquí el resultado. Mi primer logro. Ahora, soy yo quien me río de el. Y puedo usarlo cuantas veces quiera y por el tiempo que me de la gana.

Gracias a todos los listeros nuevamente. Bye.

