Programa	FairStars Audio Converter
Descripción	Programa para convertir distintos formatos de audio.
Download	http://www.fairstars.com/download/fsaconv_setup.exe
Herramientas	RDG – OllyDBG (+ plugin Ollydump) – ImpREC
Dificultad	Baja
Compilador	Microsoft Visual C++
Protección	AsPack v2.12 + Serial
Objetivos	Desempacar y parchear.
Cracker	Alone In The Shell
Tutorial nº	1

Bueno antes de nada quiero dar las gracias a toda la lista y en especial a Spandau, Stzwei y Ricardo que son los que en menos de 10 minutos desde que postee mi duda al desempacar el programa me respondieron dándome sendas soluciones, sin ellos y sin todos los miembros de la lista cuyos manuales me han enseñado y permitido desempacar este programa y crackearlo. Muchas gracias a todos y en honor a vosotros aquí va mi primer tuto que seguro que tiene fallos pero espero que sea el primero de una larga lista de aportaciones a esta maravillosa lista.

1. Analizando el objetivo.

El objetivo de este primer tuto es un programa de conversión de formato de ficheros de música, el software en cuestión se llama FairStars Audio Converter y se puede bajar gratis de este enlace **http://www.fairstars.com/download/fsaconv_setup.exe** la ultima versión a fecha de hoy 19/8/2009 es la 1.81 que es la que nos disponemos a analizar ;P .

La versión gratuita de este programa tiene la limitación de que solo combierte los primeros 180 segundos del archivo dado, nosotros vamos a analizar el programa para garantizar que combierte los archivos enteros y por su puesto si pagar ni un duro!!!!

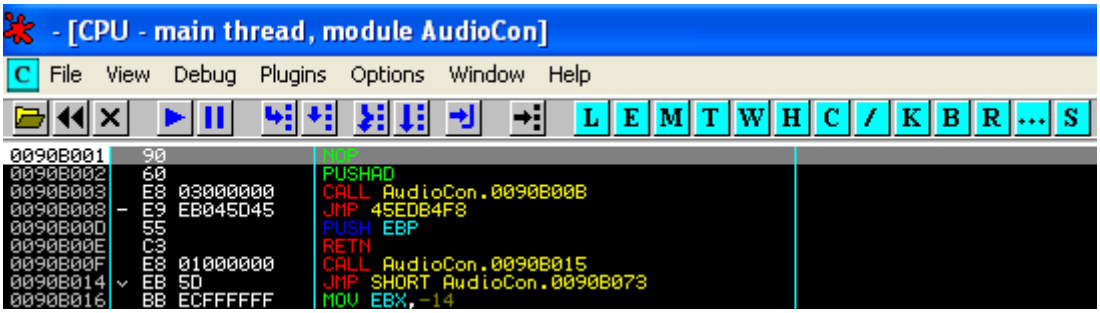
Lo primero como siempre pasarle el RDG Packer Detector el cual nos arroja lo siguiente:

La verdad es que para ser mi primer tuto me acojone un poco ;P pero despues de pasarle el RDG a varios programas que me baje de softonic y comprobar que todos estaban empacados me decidi por probar este ;P (proximamente intentare crackear los otros que vi pero todo a su tiempo).

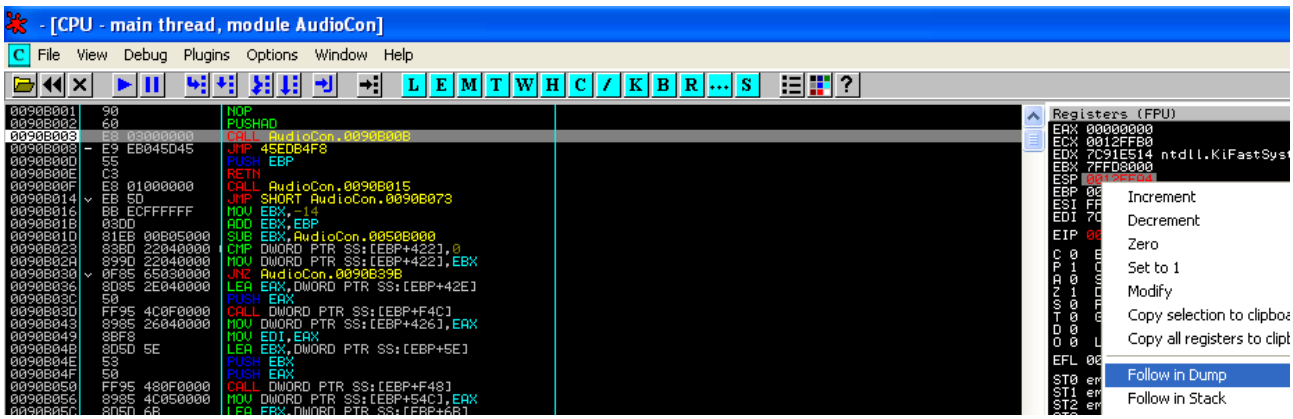
Vale pues perfecto AL ATAQUE!!!!!!!!!

2. Desempacado

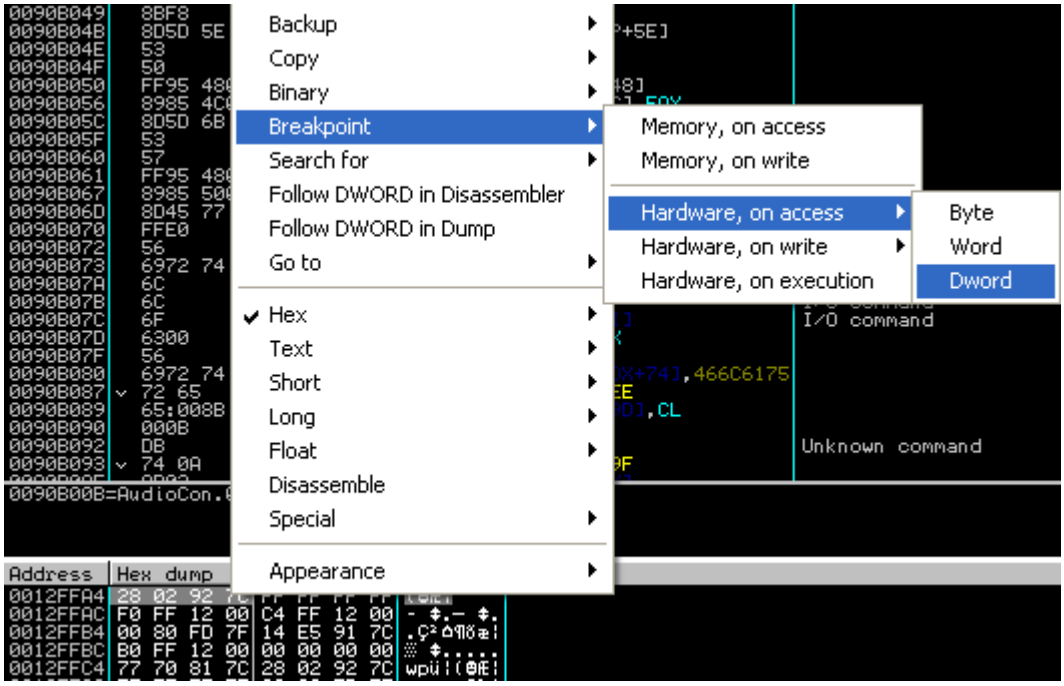
Bueno pues nada mas abrirlo con el OllyDbg este nos avisa de que el Entry Point esta fuera del las cabeceras del PE lo que es normal si esta empacado ;D



Y efectivamente empezamos muuuuyy lejos de donde deberíamos, pero que no cunda el pánico!!! enseguida vemos una instrucción **PUSHAD** (que guarda todos los registros en la pila) y tal y como dice Ricardo en su tutorial Cracking desde 0 si un packer guarda todos los registros en la pila lo normal es que cuando haya terminado de desempacar todo el programa los saque de la pila con **POPAD** ;D con lo que pasamos esa instrucción con "*f7*" y nos vamos al registro **ESP** y con el botón derecho del ratón damos a "*Follow in Dump*"

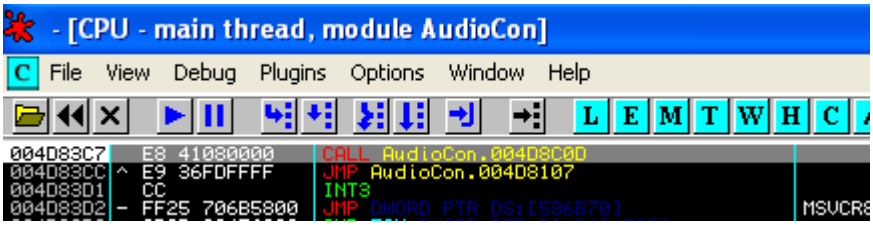


Y una vez que estamos en el Dump marcamos primeros 4 bytes y una vez mas con el botón secundario del ratón le ponemos un "*Breakpoint -> Hardware, on Access -> DWORD*"



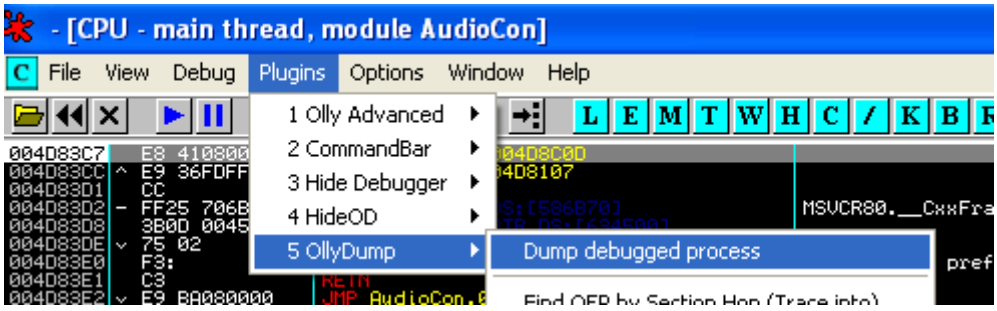
Perfecto ahora ya tenemos todo preparado le damos a "*f9*" para que el packer haga su trabajo y vemos que para justo después de la instrucción **POPAD**

Una de las cosas que mas me a costado coger (aunque parezca una tontería) es por que en todos los tutoriales después de llegar a este punto daban un par de veces a "f7" para llegar al *Original Entry Point*, hasta que me di cuenta que es lógico que si el packer utiliza una rutina para desempacar el código del programa una vez que desempaca todo y restaura todos los registros con la instrucción **POPAD** tiene que terminar esa rutina con un **RETN** (o similar) para poder "caer" en el *OEP*!!! pues lo dicho le damos a "*f7*" para saltar al **PUSH** que marca la captura y otra vez mas para llegar al la instrucción **RETN** que termina la rutina de desempacado del propio packer, y a donde nos lleva.... efectivamente al *OEP*!!!!!!!

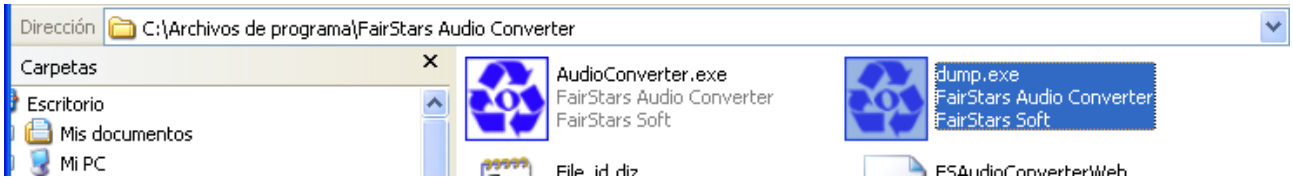


Perfecto la cosa va dando resultado ya tenemos el primer paso para desempacarlo, ahora queda dumpear y reconstruir la IAT!!!!

Para lo primero, dumpear, yo voy a utilizar el plugin Ollydump (aunque en su momento lo probé también con el LordPE) para ello y situados en el oep le damos a "*Plugins -> Ollydump -> Dump Debuged Process*"

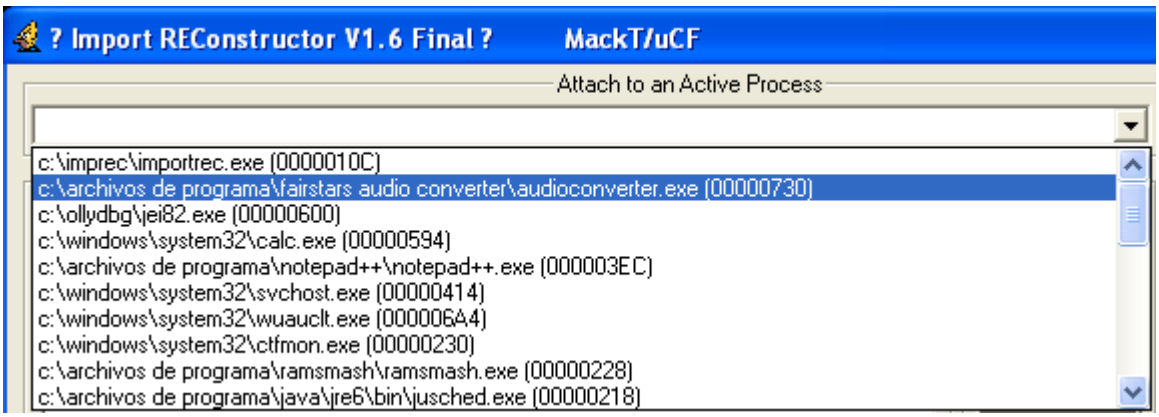


Y voilá!!! ya tenemos nuestro ejecutable volcado en el fichero dump.exe en el directorio del FairStars:

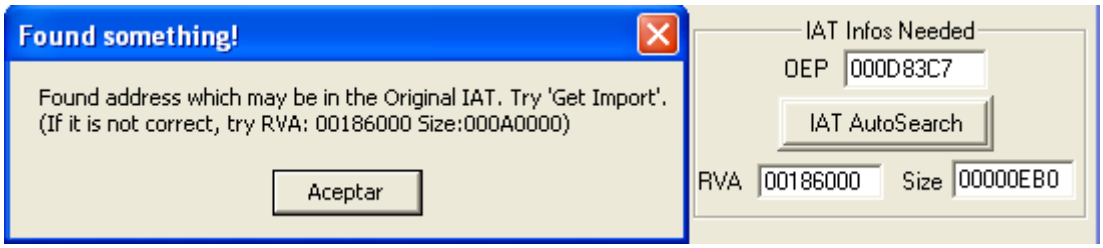


Si ahora intentáramos ejecutarlo nos daría un error por que no esta reparada la IAT, yo en su momento y siguiendo los tutos de Ricardo busque la IAT a mano y comprobé donde empezaba y terminaba a mano también (lo que en este programa es una pu**** porque antes y después de la IAT hay basura con lo cual tuve que mirar en el Memory map todas las librerías que cargaba y los rangos de direcciones de su sección de código para luego en la IAT comprobar donde terminaban las direcciones que hacían referencia a la sección de código de las dll's , vamos un jaleo) pero luego nuestro compañero **stzwei** me informo que el ImpREC la localizaba automáticamente :,(.... bueno da igual, aquí voy a mostrar como lo hace el ImpREC (...por cierto gracias stzwei ;D) .

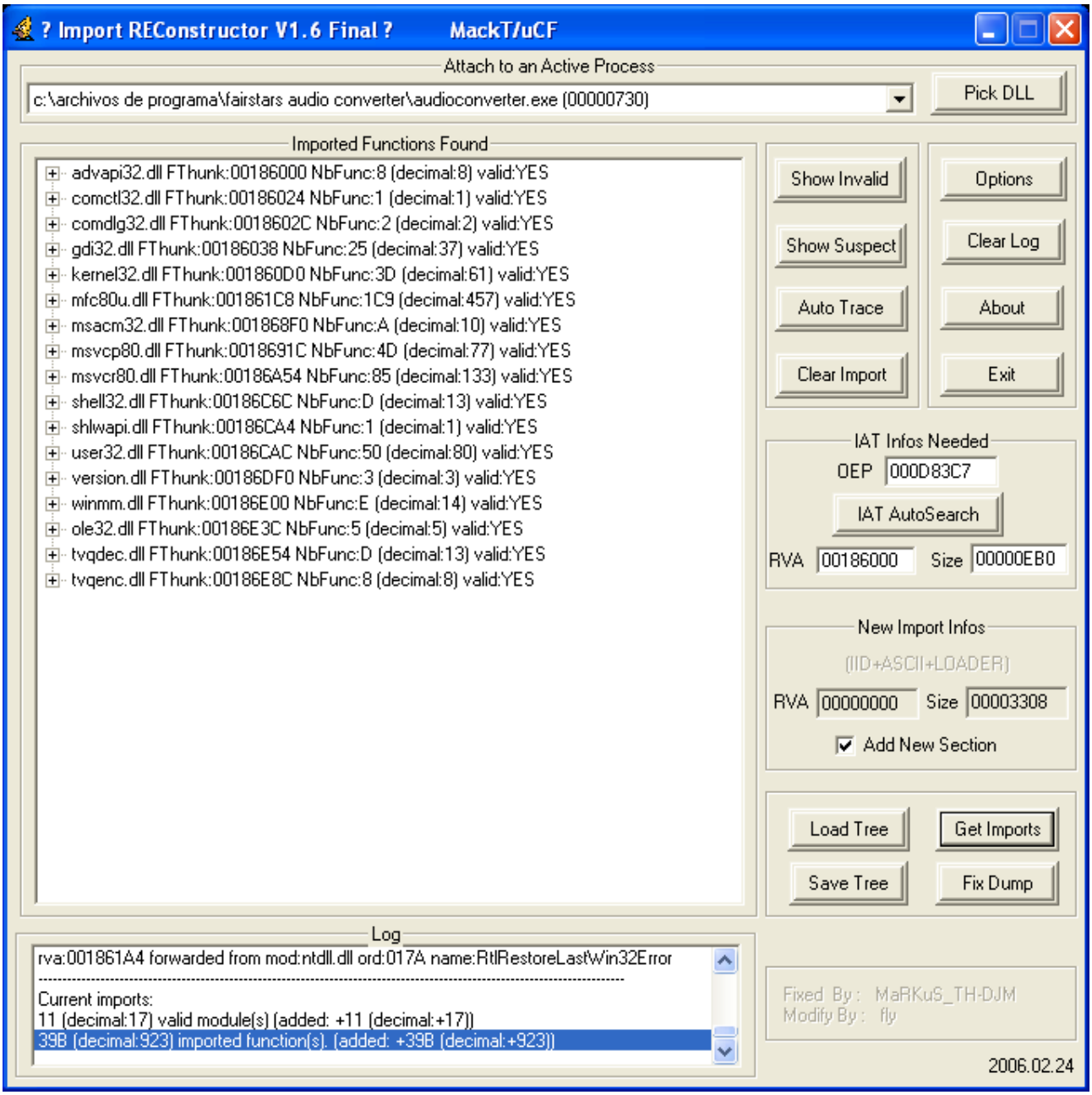
Pues lo dicho como nuestro oep es **004D83C7** y la imagen base es **00400000** al restarlo nos queda que el offset de nuestro oep es **000D83C7** y con esto al ImpREC, donde primero seleccionamos el proceso de FairStar Audio Converter :



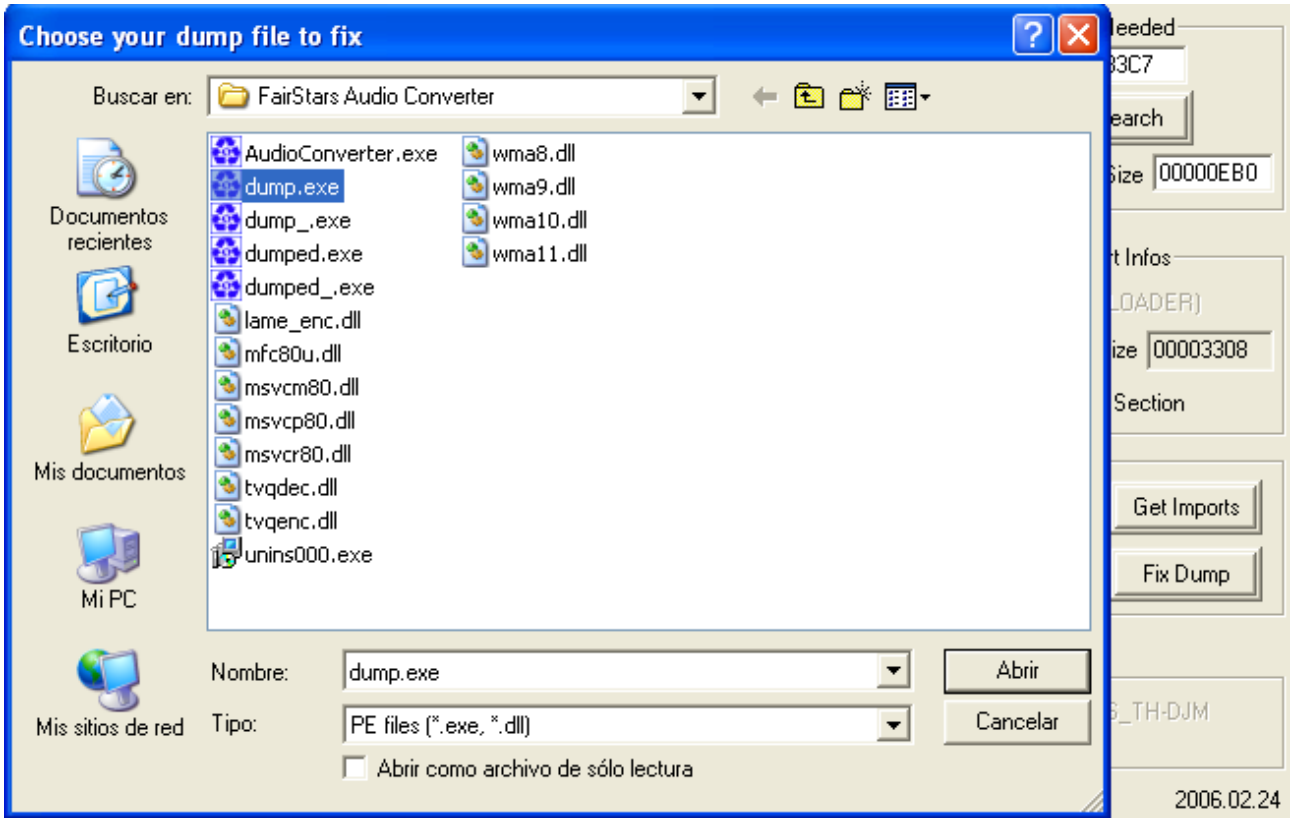
Y después rellenamos los datos y le damos al botón "*IAT AutoSearch*"



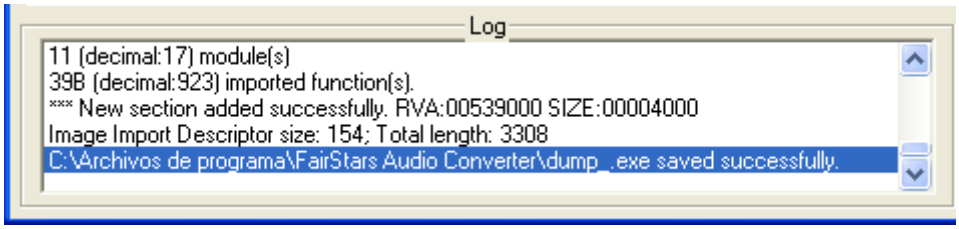
Como se puede observar el ImpRec nos reconoce la IAT , nos da el offset **00186000** donde empieza la IAT (para quien quiera comprobarlo en el dump solo hay que sumarle la imagen base y os dará la dirección de comienzo de la IAT ,es decir, **00586000**) y su tamaño **00000EB0** (con lo cual la IAT termina en la dirección **00586EB0**) y nos dice que ya podemos probar a importar las direcciones, pues vamos a hacerle caso no ;P , le damos al botón "*Get Import*"



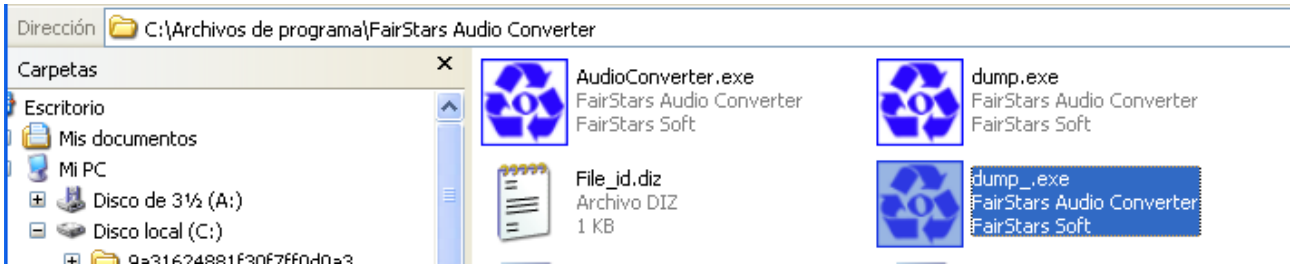
Y perfecto nos encuentra todas las librerías y sus offset así como todas las funciones de cada librería, nos fijamos que pone "*valid: YES"* en todas y toca darle al botón de "*Fix Dump*" para reparar el dumpeado que hicimos antes, llendonos al directorio del programa y seleccionando el fichero dump.exe (en la captura hay varios dump por que lo desempaque varias veces y con varias herramientas para practicar ;D):



Pues eso lo seleccionamos como aparece en la figura y al dar a "*Abrir*" el ImpREC en la parte de logs nos tiene que decir algo tal que así:

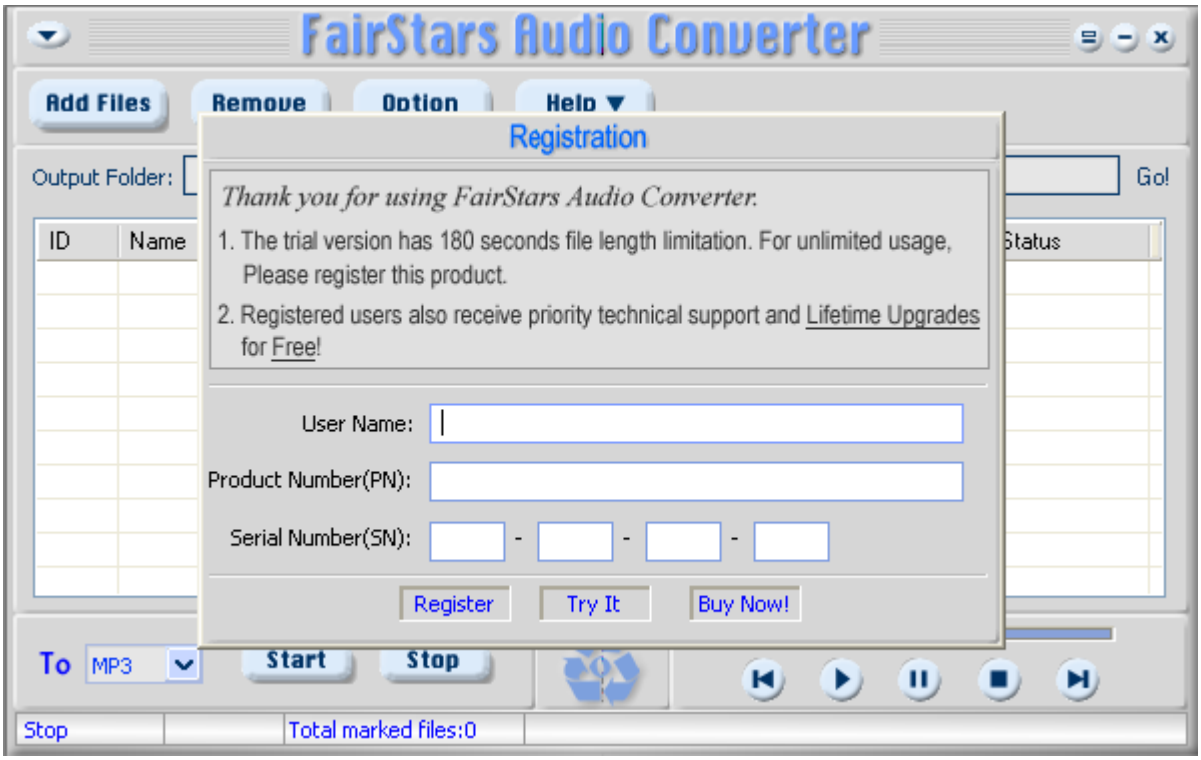


Perfecto ya esta reparado y nos ha generado el archivo "*dump_.exe*" que es el programa desempacado y con la IAT reparada ;D



3. Empezando el análisis y posterior crackeo ;D

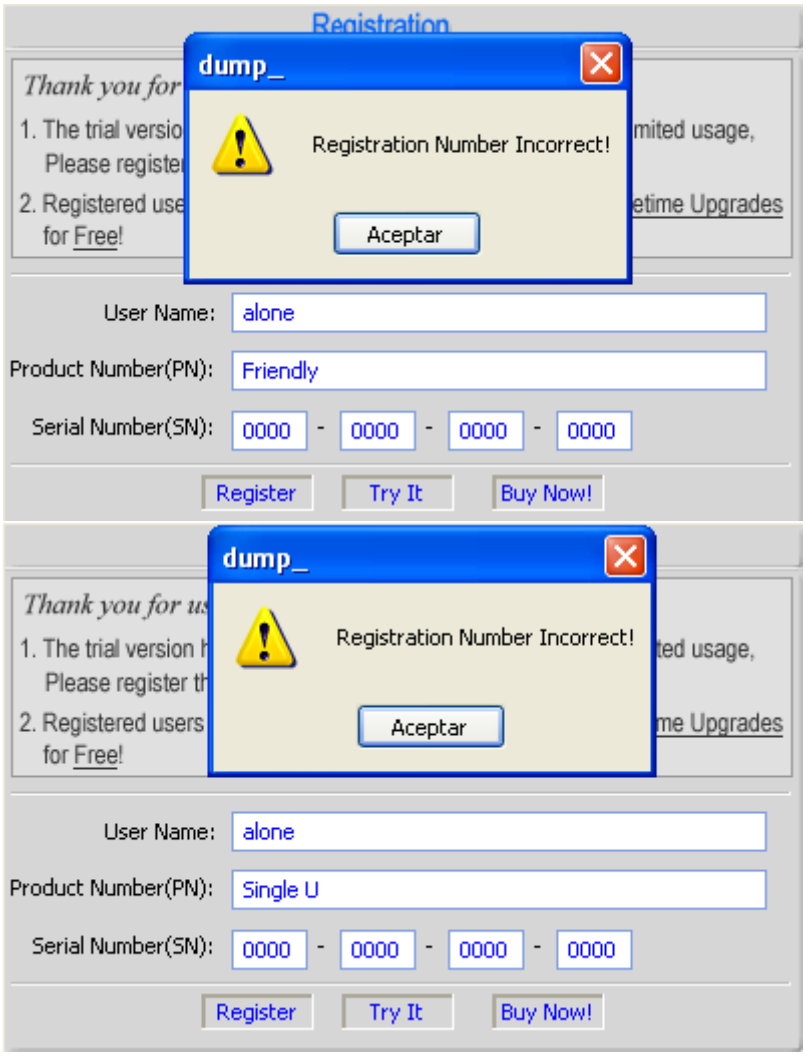
Uffff!!! que nervios después del arduo trabajo del desempacado toca la parte mas divertida :D, como ya tenemos a nuestra victima desempacada y lista para ejecutarse. Lo primero que vamos a hacer es ejecutarla tal cual para conocerla un poco mejor (si vamos a verle hasta las tripas con el olly lo suyo es conocerse primero no ;P jeje)



Vale perfecto la primera vez que se ejecuta la aplicación nos aparece esta ventanita de registro directamente, en realidad lo que hace es buscar un archivo que se llama fsreg.ini que esta en "C:\Documents and Settings\Administrador\Datos de Programa\FairStars Audio Converter\" si encuentra ese archivo lo abre y lee los registros que tiene (que son el User name, el PN y el SN) y comprueba si son validos, si lo son estas registrado ya y no te muestra nada, si no lo son te muestra esta pantallita al igual que si ese fichero no existe (lo que ocurre la primera vez que ejecutas el programa), en tal caso te muestra esta pantalla y cuando termines de escribir los datos te generará el archivo con los datos introducidos.

Pues vamos alla, rellenamos los datos haber si por casualidad acertamos ;D

Gups!!! Nos da error en el PN, que simpático el programa que te da tanta info ;D, bueno esto no tiene misterio, nos vamos al olly y le damos a “Search for -> All reference strings” y con rápido vistazo veremos que los tipos de Product Number válidos son o “Single-user License” o “Friendly License” o “Site nose que...” bueno el caso es que en el código solo comprueba que ponga o “Single U” o “Friendly” así que nos decantamos por “Friendly” (aunque pruebas sucesivas me demostraron que no hay diferencia...)



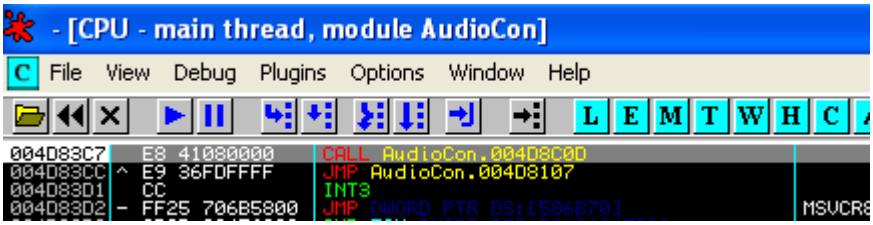
Efectivamente ya no nos da el error en PN pero el muy cab*** nos dice que nuestro Serial es incorrecto!!!! pero como se atreve!!!!grrrrrrr.... bueno da igual eso ya lo veremos después, vamos a seguir intimando con nuestra aplicación ;D.

Pues nada visto que no hemos acertado con nuestro serial le damos a "Try It" para probar el programa (con la limitación que solo convierte 180 segundos de archivo) y nos aparece lo siguiente:

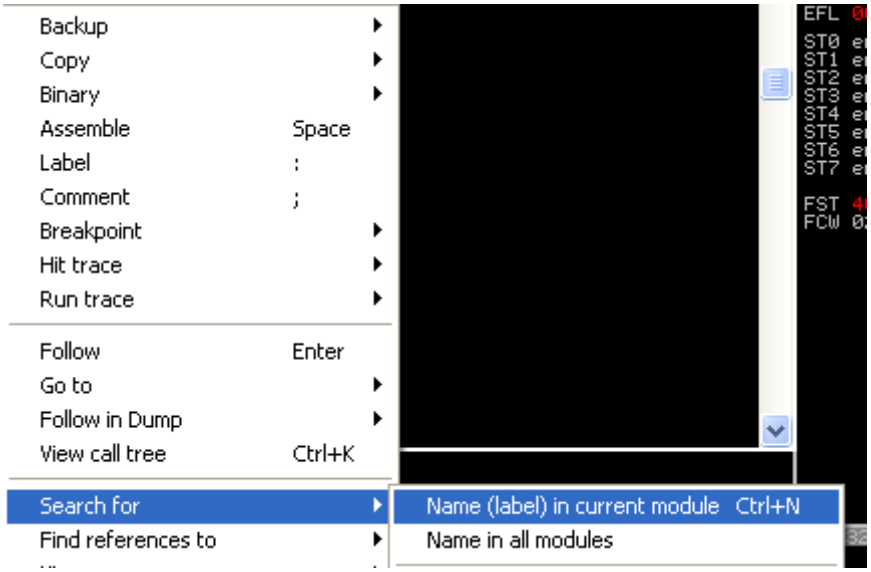
Como vemos el programa es muy sencillito, en la parte de "*Help*" nos aparece la opción de "*Registration*" grrrrr!!! que nos mostrara la misma ventana de antes y en el "*About...*" nos muestra esto:

Bueno pues ya esta ya nos conocemos :D jeje ahora a meternos hasta la cocina!!!!!

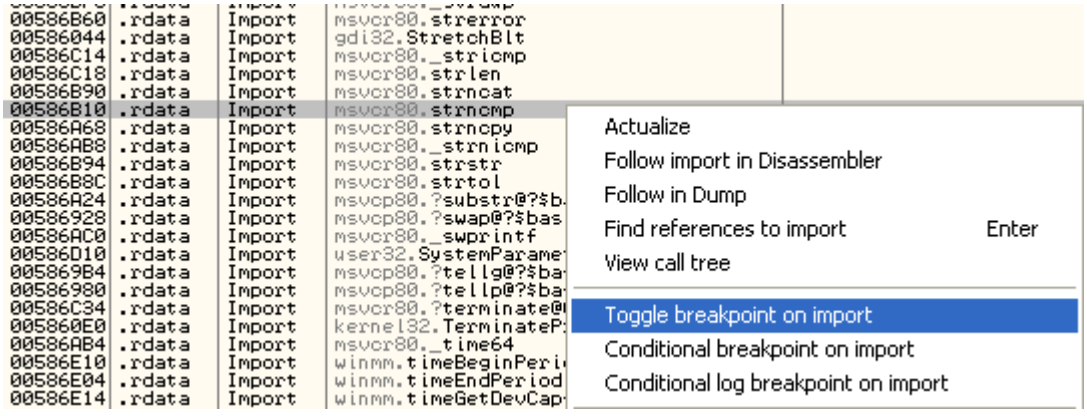
Pues ya esta bien lo abrimos con nuestro queridísimo OllyDbg (recomendaría poner la protección de IsDebugerPresent ;D) y nos encontramos en el Entry Point



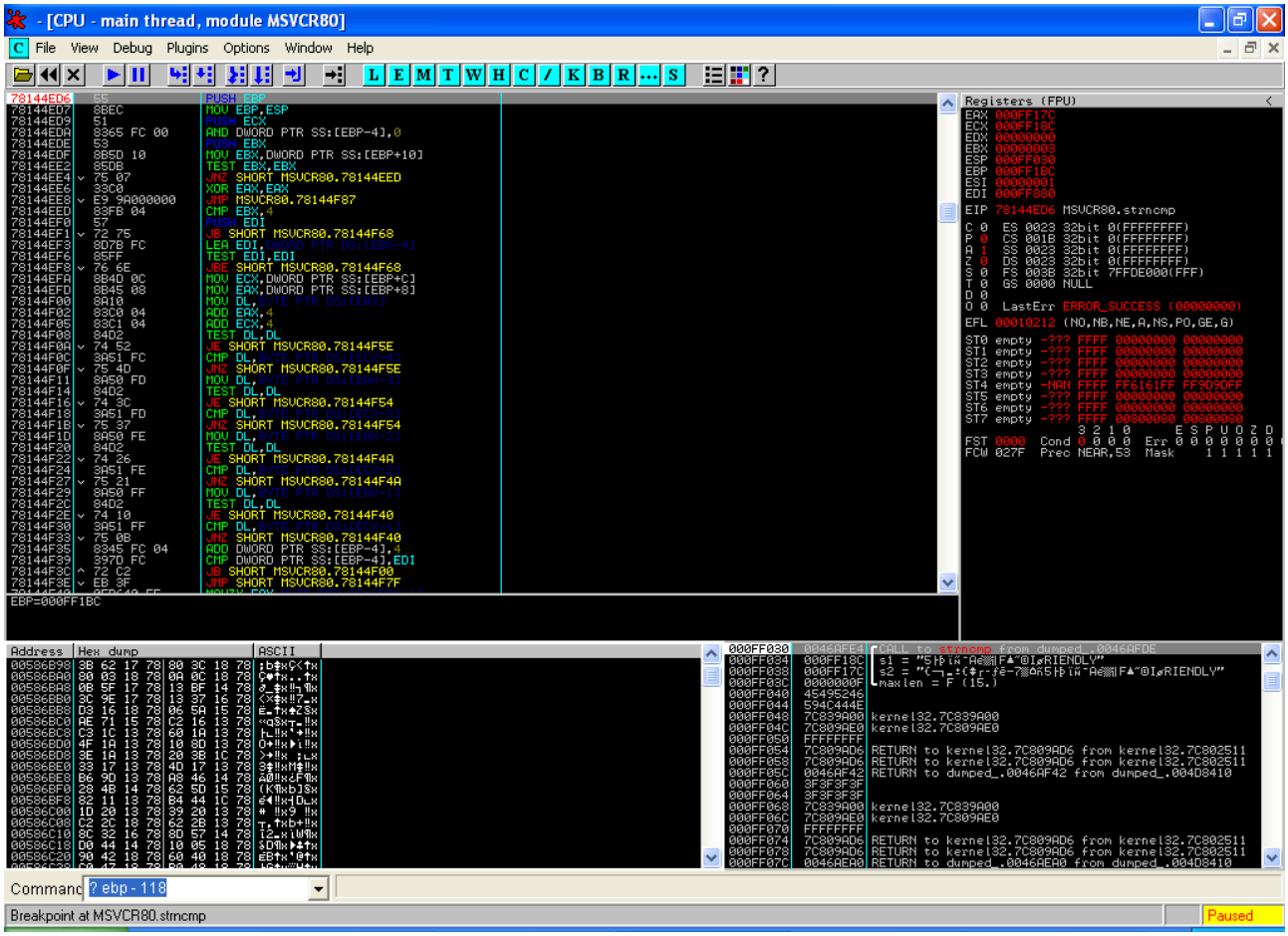
Pues nada si echamos un vistazo a las strings del programa veremos que hay un montón de basura pero realmente nada interesante así que nos vamos a mirar todas las funciones que utiliza. Así que hacemos "*Search for -> Name (label) in current module*":



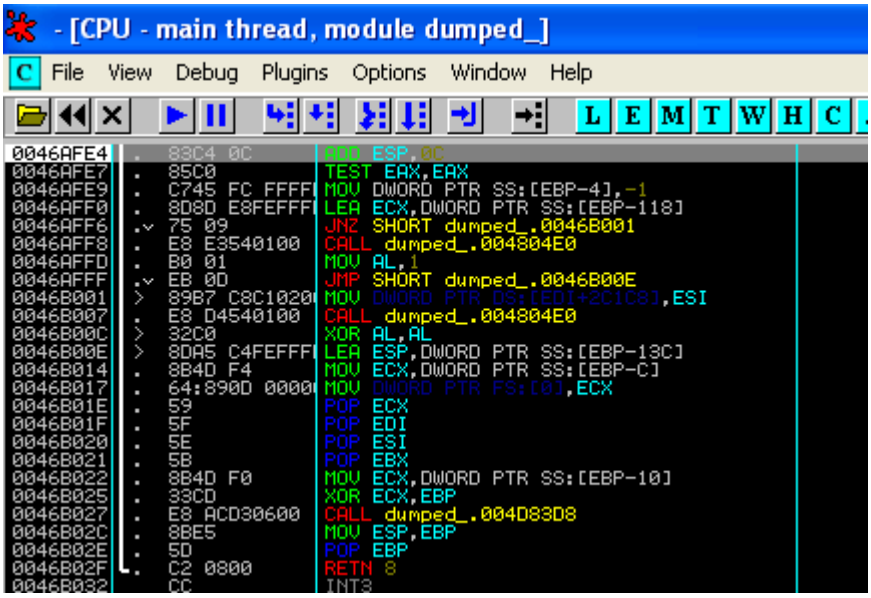
Si le echamos un pequeño vistazo veremos una serie de funciones de C interesantes como por ejemplo "**fopen**", "**fseek**" y "**fread**" que son funciones que sirven para abrir, posicionarse y leer de un fichero respectivamente, pero las funciones que realmente llaman nuestro interés son todas las funciones de comprobación de strings como por ejemplo la archiconocida "**strncmp**", esta función recibe dos cadenas de caracteres y un tercer parámetro con el tamaño máximo de la cadena a comparar. Pues lo dicho le ponemos un breakpoint dando a botón secundario "*Toggle breakpoint on import*":



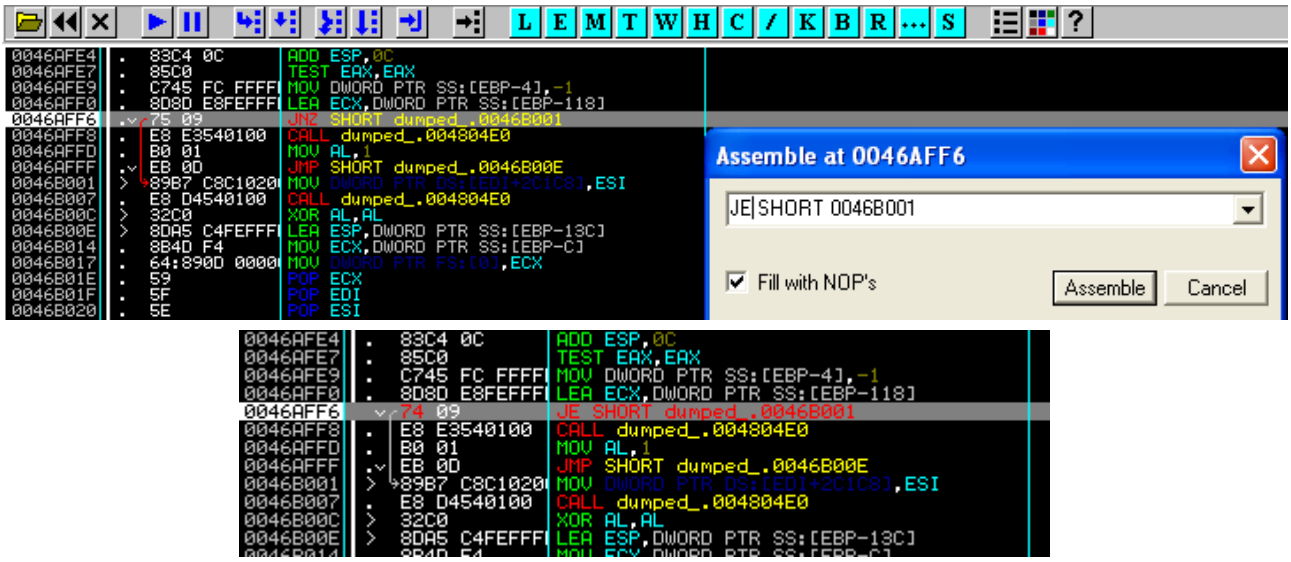
Y en el desensamblado le damos a "*f9*" para que se ejecute hasta el breakpoint. Como ya es la segunda vez que ejecutamos el programa, el fichero fsreg.ini del que hablamos antes existe, con lo cual ahora el programa se para directamente en la función "**strncmp**" sin mostrar nada, si fuera la primera vez que ejecutamos el programa o si borramos ese fichero, primero nos saldría la ventana de registro y posteriormente nos pararía en el breakpoint. De cual quier forma aparecemos aquí:



Estamos en el principio de la función "strncmp" en la dll MSVCR80,como no nos interesa pues apretamos "*Ctrl+f9*" o vamos al menú "*Debug -> Execute till return*" para que se ejecute el código de la librería hasta el **RETN** y una vez ahi le damos a "*f7*" para volver al código de nuestro programa:



La función nos devuelve a esta instrucción **ADD ESP, 0C** en la dirección "**0046AFE4**" y si miramos un poquito mas abajo veremos que en la dirección **0046AFF6** hay un salto condicional que tiene toda la pinta de ser el quiz de la cuestión, si nos fijamos si ese salto se cumple nos saltamos el **CALL dumped_.004804E0** y el **JMP SHORT dumped_.0046B00E** así que damos "*f7*" hasta llegar a esa instrucción **JNZ SHORT dumped_.0046B001** y damos al espacio para modificar lo por su antónimo **JE**



Una vez modificado ese salto presionamos "*f9*" y que obtenemos ¿¿??

Siiiiiiiiiiiiiiiiiiiiiiiiiiiii!!!! en la parte de "*Help*" del programa aparece inactivo el botón de registro y si presionamos en "*About...*" nos aparece lo siguiente

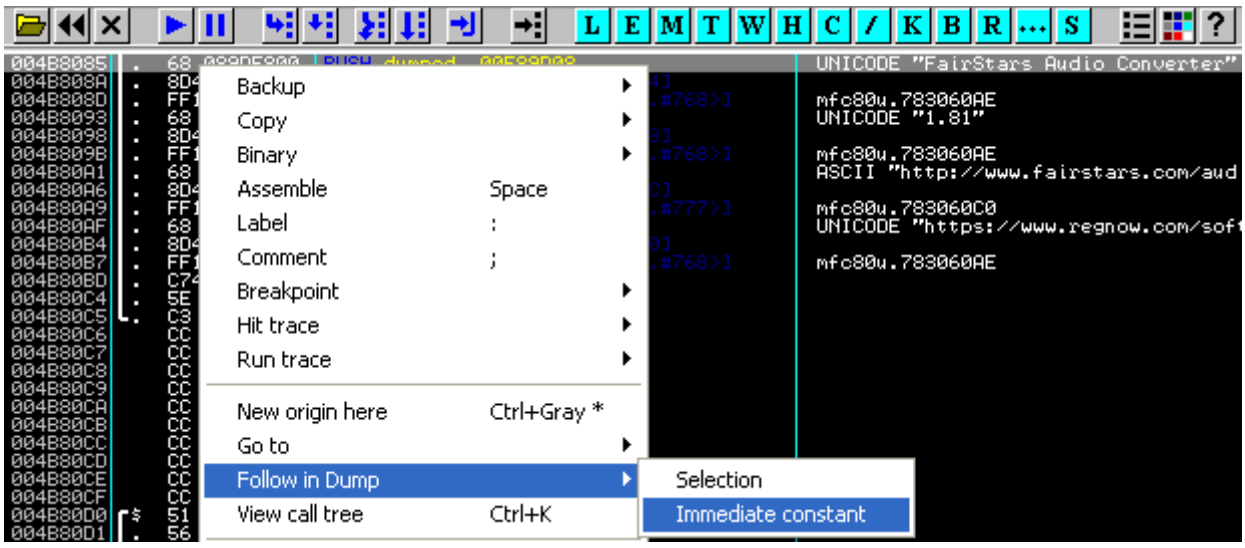
Jajajaja esta licenciado y gratis ;D podemos comprobarlo cargando un archivo de mas de 3 minutos (o lo que es lo mismo 180 segundos) y comprobando que lo convierte perfectamente ;D

Ya solo quedaría volcar lo a un fichero guardando los cambios y listo pero no lo voy a hacer por que es muy sencillo y por que a parte yo solo uso güindous para el cracking ;D

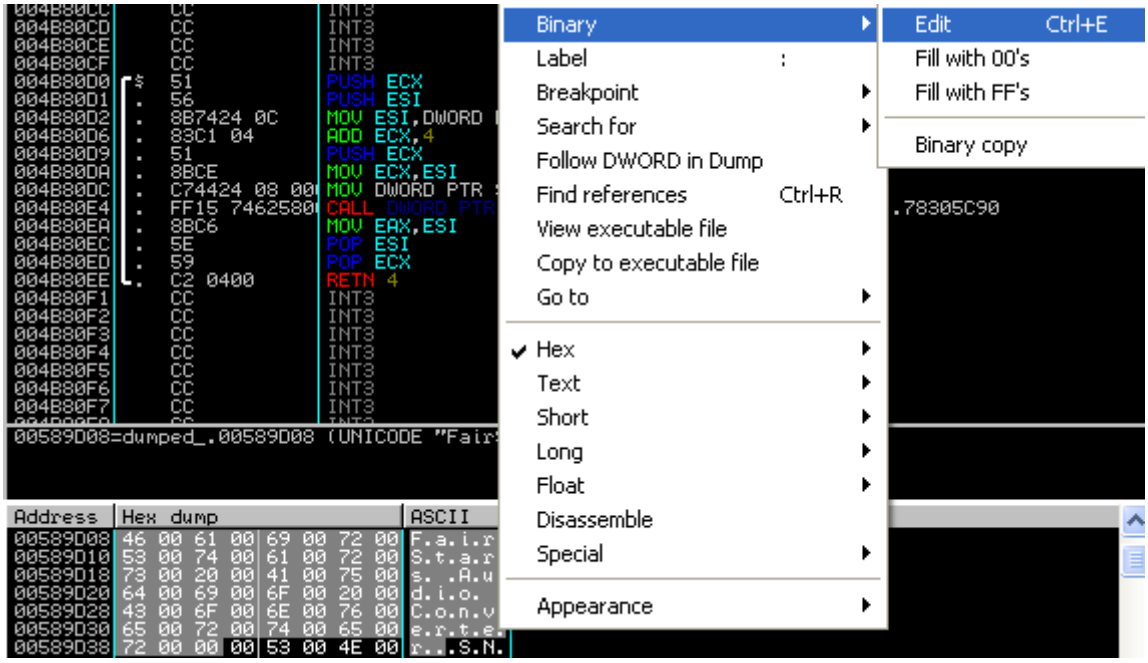
4. Firmar la obra.

Para los curiosos que se hayan fijado en la firma de "Cracked By Alone Shell" solo decir que es tan facil como buscar en las strings del programa la que pone "FairStars Audio Converter"

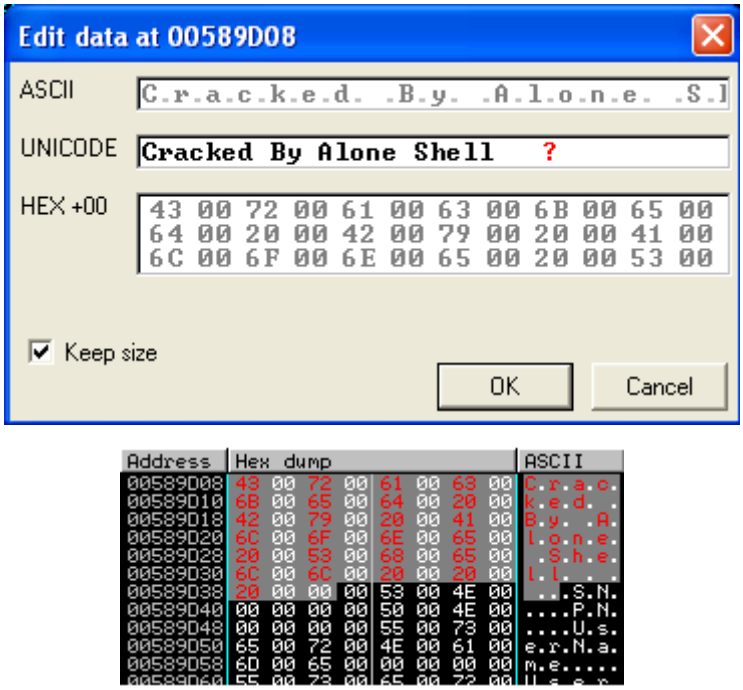
Dándole doble click te lleva a la parte del código donde carga esa string y ahí "*Follow in Dump -> Inmediate constant*"



Y te lleva a la parte de la memoria donde esta esa cadena, así que solo hay que seleccionarla y con el botón secundario del ratón "*Binary -> Edit*"



Y poner lo que se quiera ;D siempre teniendo cuidado de no pasarnos de caracteres!!!!



5. Agradecimientos.

Pues eso que solo me queda agradecer esto a toda la lista de CracksLatinoS y en especial al maestro Ricardo Narvaja y como no a los compañeros Spandau y stzwei que me ayudaron con el desempacado del programa. Muchas gracias a todos y por favor sigan siendo como son que son ustedes maravillosos!!!!!

Un saludo y un fuerte abrazo.
Alone In The Shell