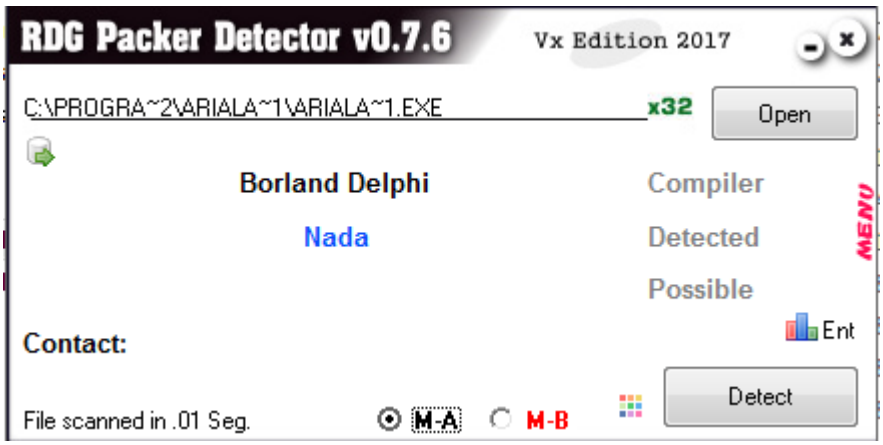
| | | | |
|---|---|---|---|
| **Programa** | Arial Audio Converter | | |
| **Protección** | Serial - Name | | |
| **Descripción** | Programa para convertir formatos a mp3 entre otros formatos | | |
| **Dificultad** | ninguna | | |
| **DownLoad** | http://www.xrlly.com/ | | |
| **Herramienta** | Ollydbg – Descompiler Delphi | | |
| **Cracker** | Abeln@v | | |
| **Lugar** | Lima – Peru | Fecha | 05/02/207 |

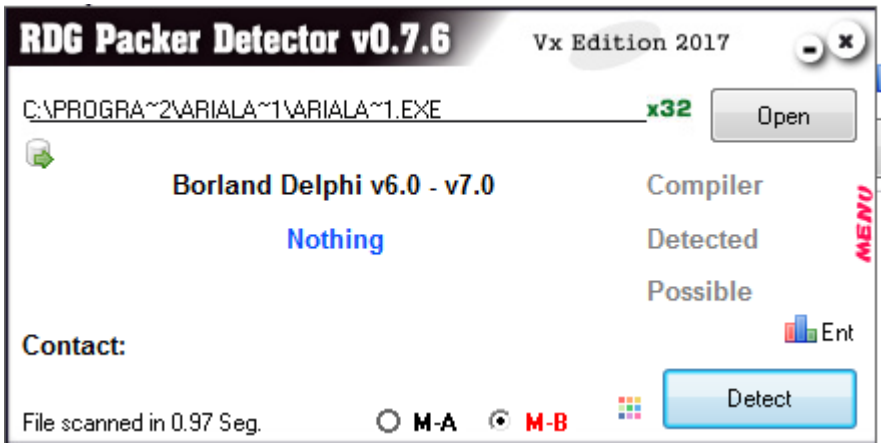
## INTRODUCCION

Bueno antes que nada quiero saludar al Maestro Ricardo narvaja ya que sin sus tutos y apoyo no estaría escribiendo hoy y Gracias a todos los de CLS, ya que en ellos encontré una familia que me apoya y siempre me impulsa a seguir adelante en este arte tan apasionante.
En esta ocasión escribiré sobre los avances que estado teniendo en el camino de aprendizaje con este software, ya que al ser la primera vez que me tope con un software hecho en Delphi , se me complico la cosa pero gracias a que tenemos tanta documentación en la web del maestro Ricardo . notaras que es mas sencillo de lo que piensas.

## AL ATAKE

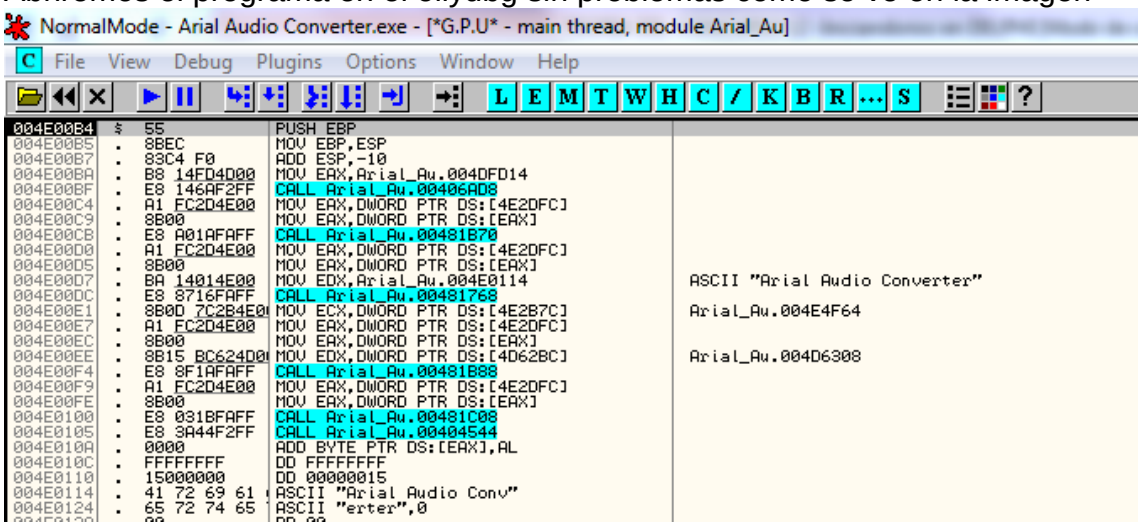
Bueno a comenzar. Primero ,instalado el programa revisamos con RDG packer si esta empacado o tiene un método antidebugging. y claro también para saber en qué lenguaje esta hecho XD





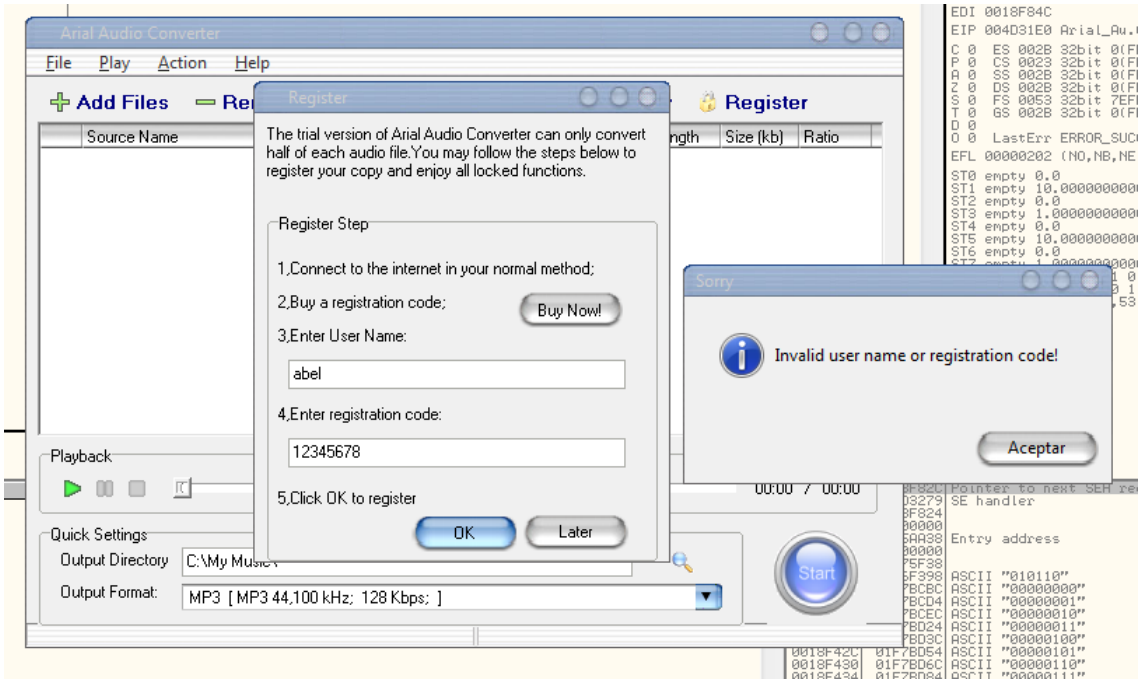

Como podemos ver no tiene ninguna protección ;) y apreciamos que está hecho en Borland Delphi .

Abriremos el programa en el ollydbg sin problemas como se ve en la imagen




Probaremos registrarnos, tal vez tengamos suerte y termine hasta aquí el tuto ;) XD . Damos run f9 . .tal vez a ustedes el software les arroje excepciones , eso es normal . con solo apretar f9 unas cuantas veces el programa correra .

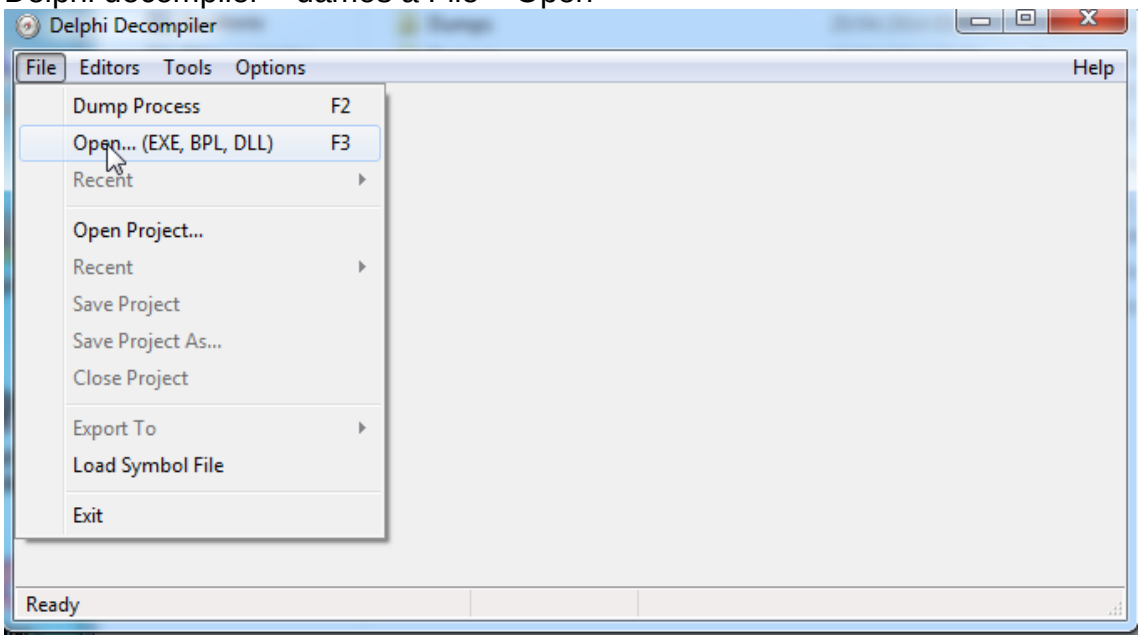
Abierto el programa nos vamos a help – register , probamos metiéndole mi nombre Abel y de serial 12345678



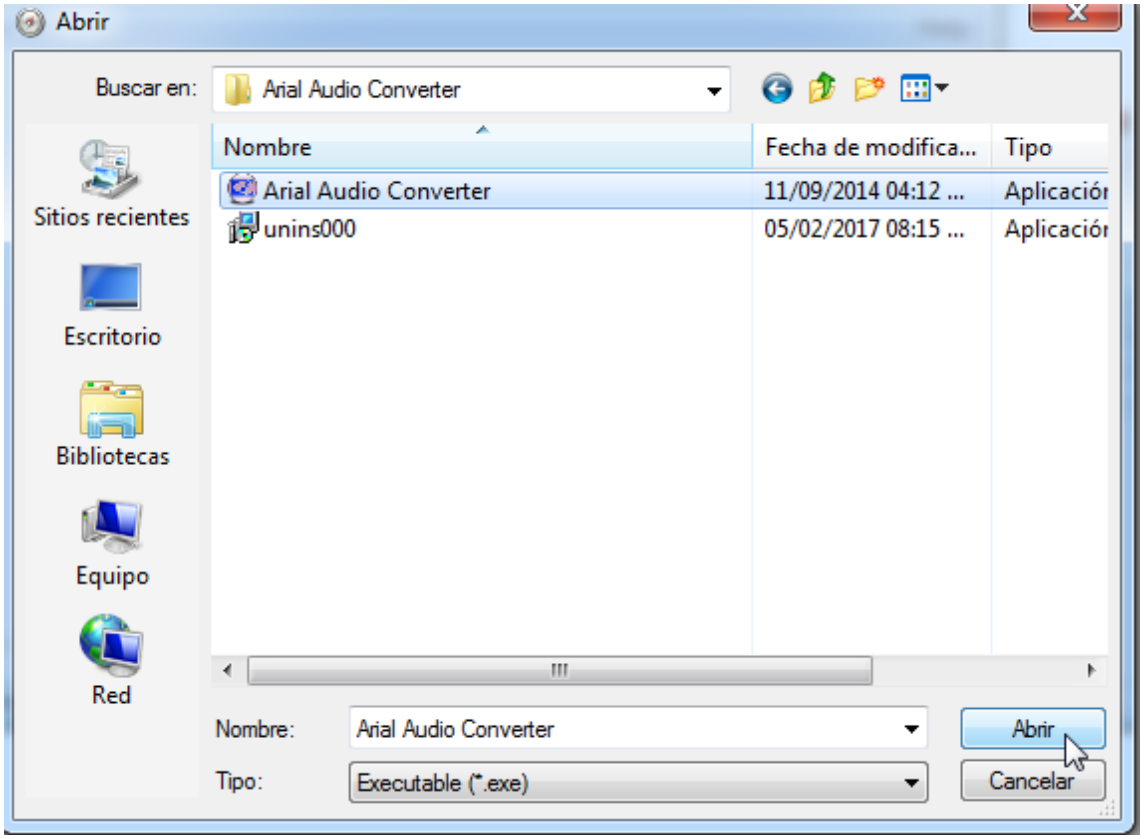

Como se aprecia en la imagen nos salió el chico malo con el título **sorry** y el mensaje **Invalid user name or registration code**. A partir de aquí aconsejo usar dede u otro descompilador de Delphi . Ya que según recomendaciones a veces será necesario usar esta herramientas. Cito unas palabras del maestro Ricardo en su tuto iniciándonos en Delphi

**“muchos dirán que esto puede ser hallado con Softice o con OLLY fácilmente, pero hay casos en que las STRINGS REFERENCES no aparecen, que no usa APIS conocidas y si no utilizas DEDE es muy difícil llegar hasta aquí.”**

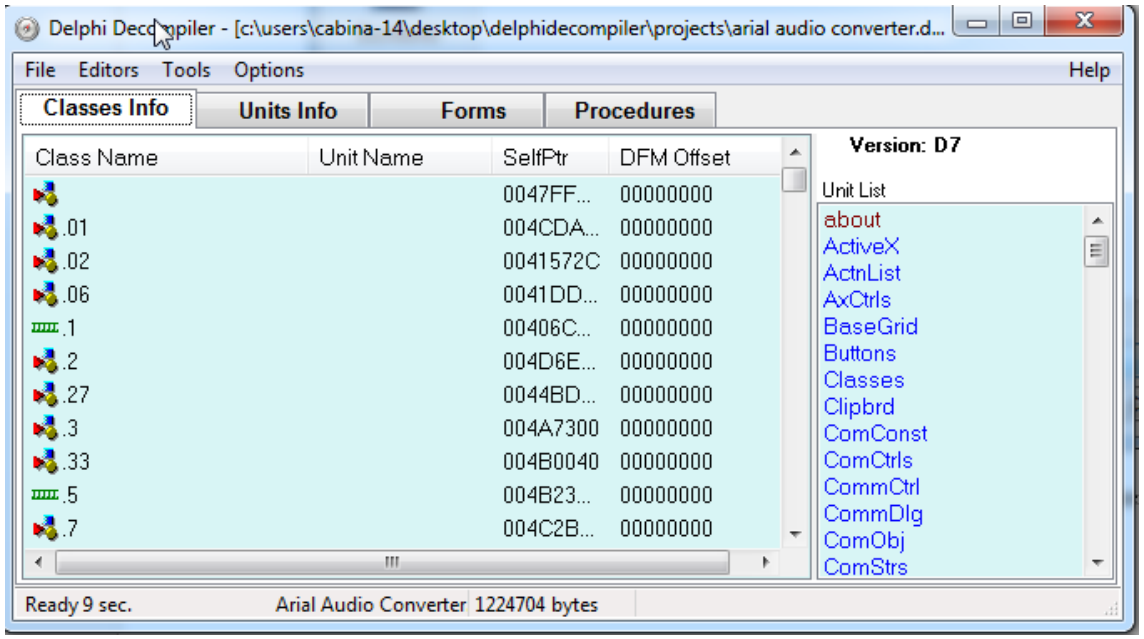
Seguimos .Al ver el mensaje del chico malo **sorry - Invalid user name or registration code** , quise comenzar haciendo un breakpoint en la api GetDlgItem,Getdlgimtemtexta o al messagebox pero no me salio .Asi que usaremos DEDE o en este caso DelphiDecompiler que el uso es el mismo,asi que pondré en el tuto las herramientas necesarias. Continuamos y abrimos Delphi decompiler – damos a File – Open




Y abrimos el programa

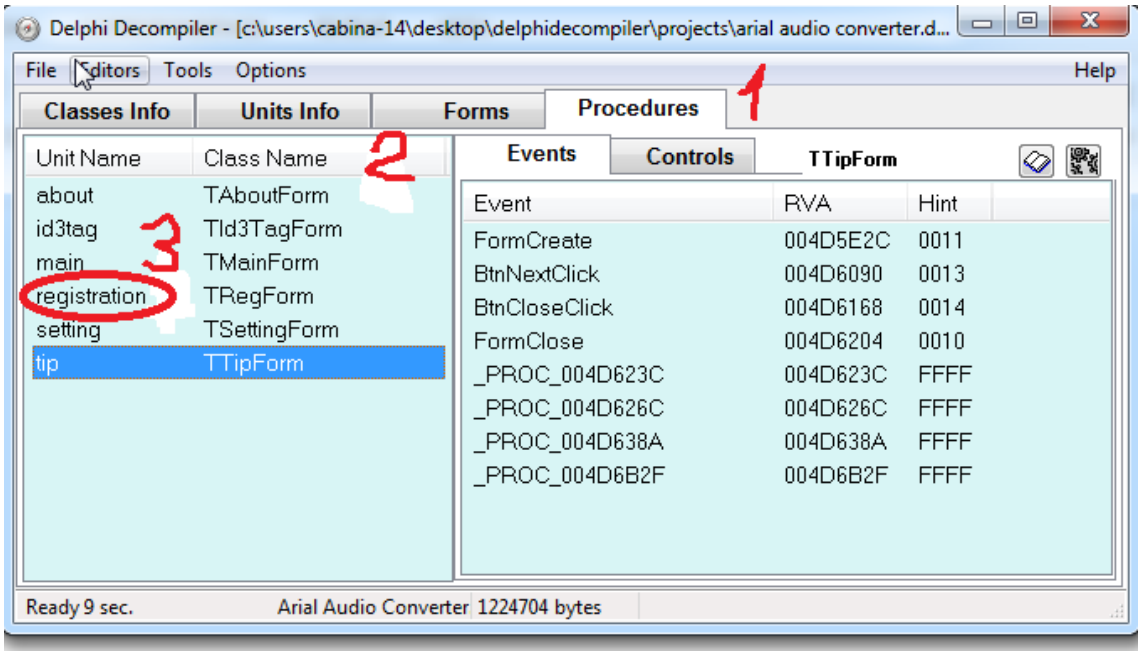



Se nos abrirá el software , yo lo di cerrar el software y apretó aceptar a los mensajes que aparecerán y no quedara asi

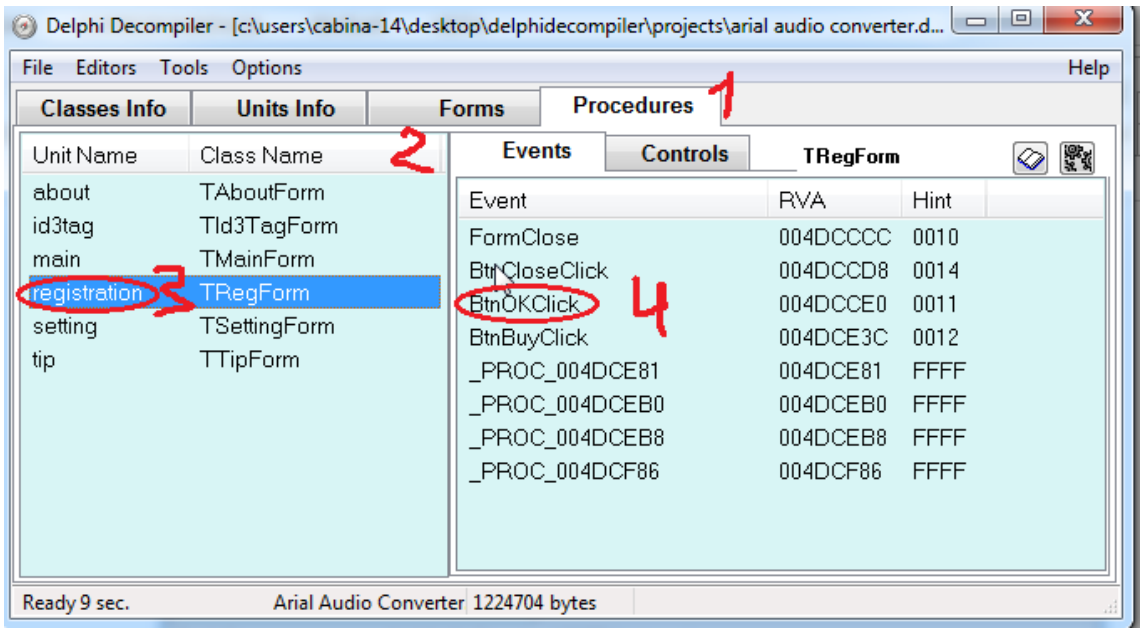



1. Elegiremos la pestaña Procedures
2. en la parte izquierda nos aparecerá dos columnas . la primera Unit name y columna izquierda class Name

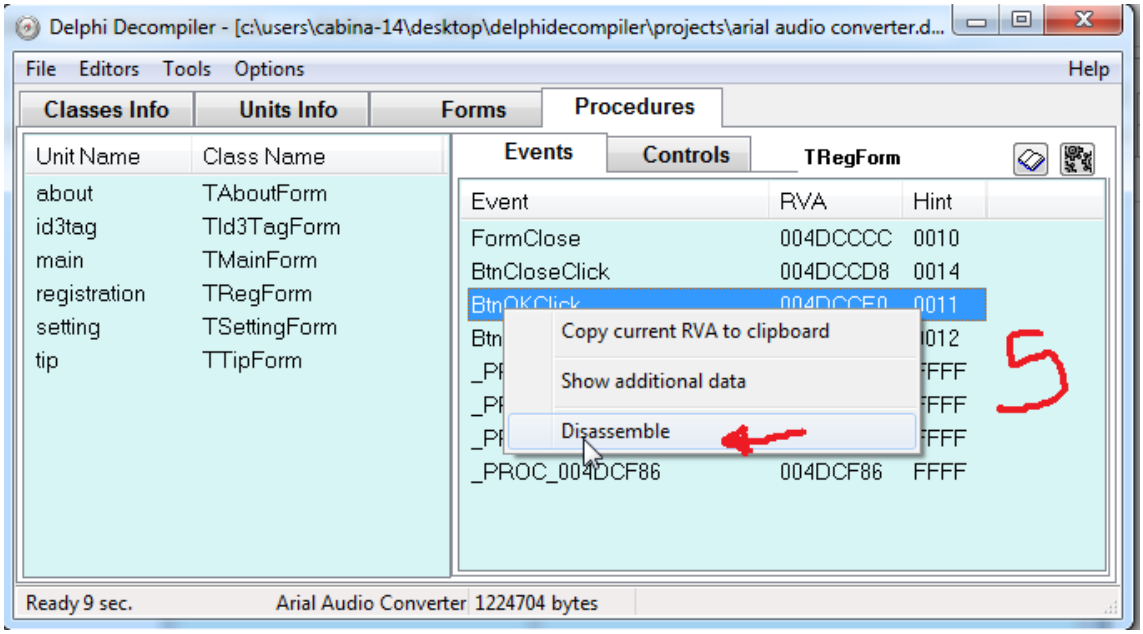
3. elegiremos Registration



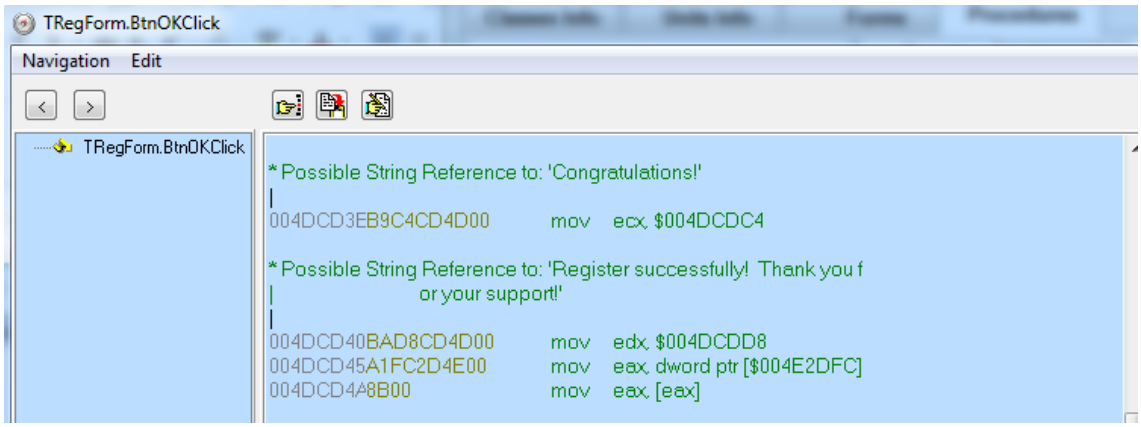

No se necesita ser un experto para notar que son las opciones de la pestañas del programa . en este caso nos interesa **Registration** . y nos aparece los botones de la ventana de registrar , el paso 4 seria elegir el btnOkClick para saber la dirección de las strings del chico malo y el chico bueno

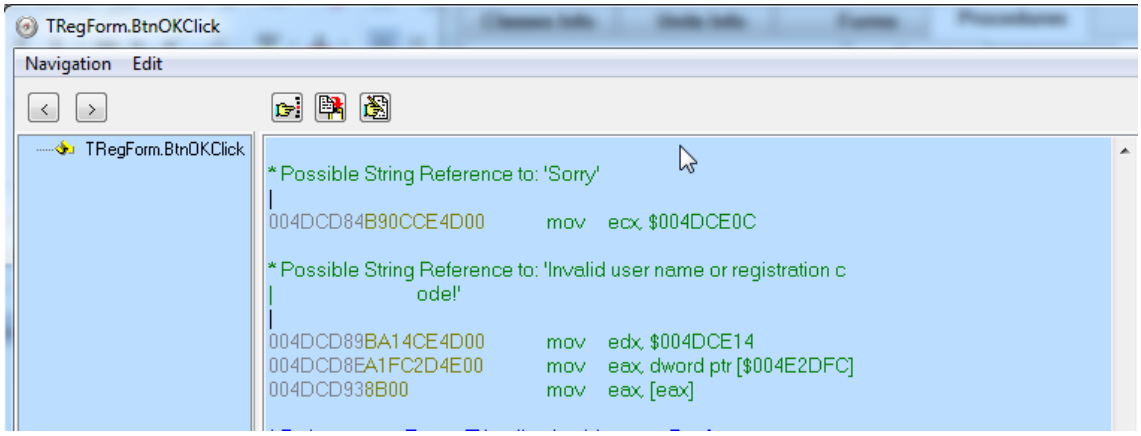



El paso 5 sería darle click derecho – y elegir la opción Disassemble

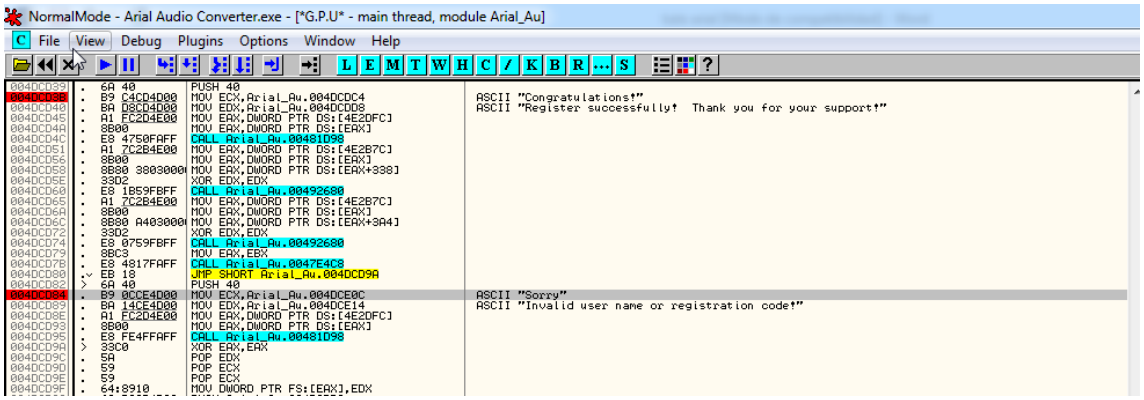



después de esto nos aparecerá un ventana y si bajamos un poco encontraremos el mensaje de chico bueno y si seguimos el mensaje de chico bueno





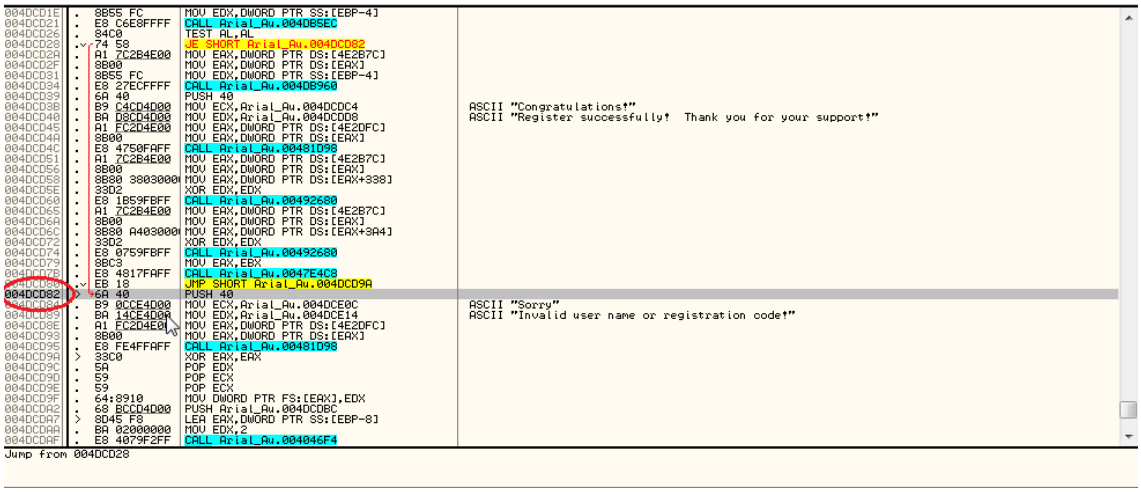

Solo nos queda ver en ollydbg aquella dirección , yo elegiré **4dcd3e** mensaje del chico bueno




Solo puse esos dos bp para que puedan apreciar que son las mismas direcciones que arroja Delphi Descompiler, ahora quito eso bp y me situo en el push 40 la dirección que esta arriba del ascii sorry .la dirección es :

004DCD82 |> \6A 40 PUSH 40

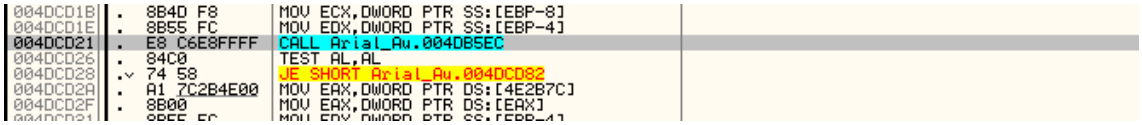
En la imagen se apreciara mejor



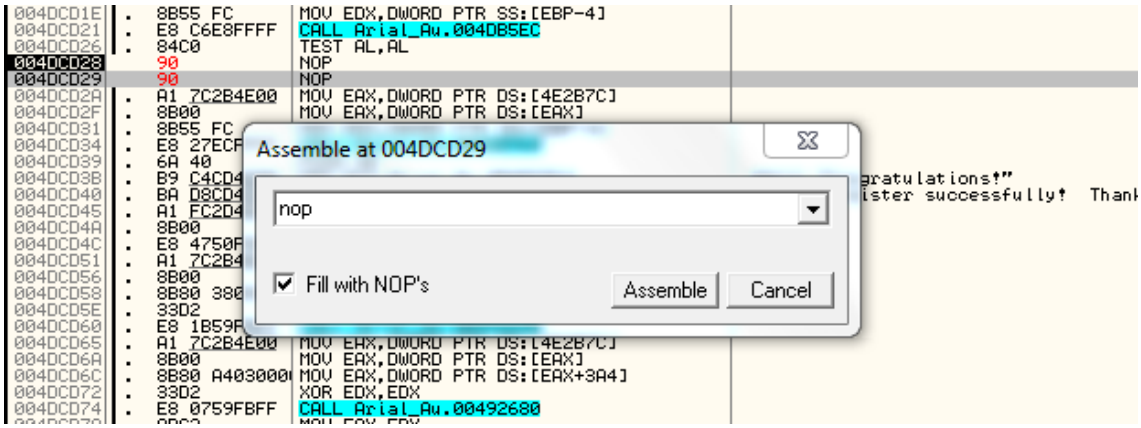

Vaya olly nos dice que viene de un salto

004DCD28 |. /74 58 JE SHORT Arial_Au.004DCD82

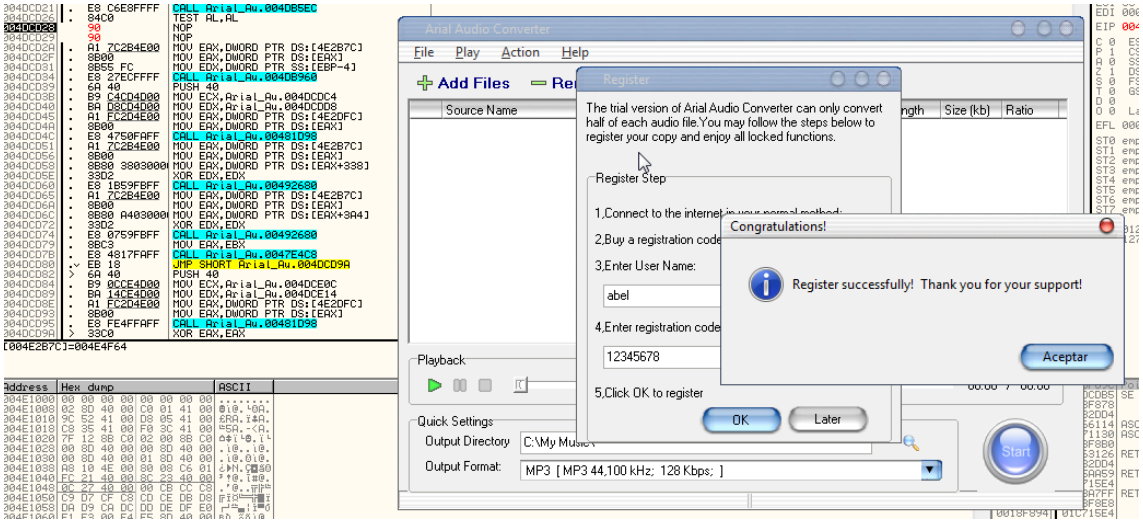
Este es la salto que decide el mensaje del chico malo y chico bueno . si somos mas curiosos arriba del salto hay un call , entonces sacamos conclusiones que esa call es la parte donde se genera el serial



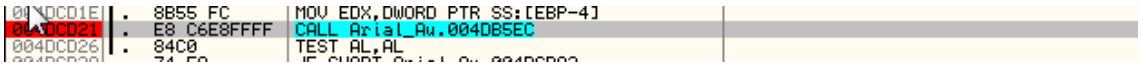

a ver probaremos nopeando el salto , nos situamos en
004DCD28 |. /74 58 JE SHORT Arial_Au.004DCD82
Y apretamos la tecla Space (espacio) y ponemos nop




Una vez hecho esto probamos ingresando nuestro user y cualquier serial

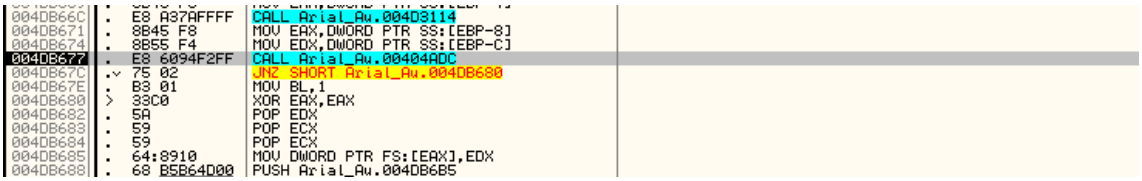



Genial pudimos registrarnos, ahora también veremos si podemos saber que serial genera con nuestro user . Normalmente pruebo si un programa es un serial fishing ya que guarda el serial en el dump para llevar al registro y hacer la comparación con el serial. Bueno volvamos a reiniciar el programa y esta vez pongamos un bp al call donde comente que hace el trabajo del serial

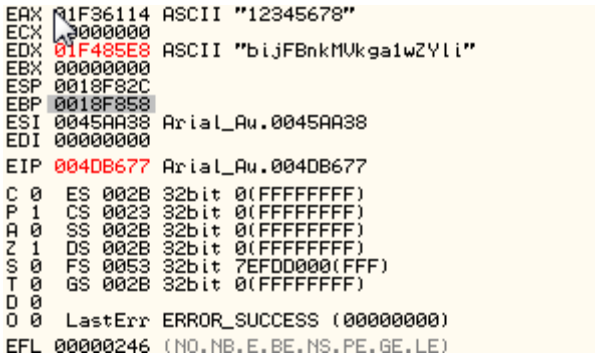



Volvamos a registrarnos, yo lo hare con los mismos datos que la vez anterior
user: abel
Pasword: 12345678

Una vez ponemos ok para en el bp que pusimos. Después entramos al call con F7 y traceamos con F8 hasta llegar hasta donde esta la dirección de la imagen




si pudiste ver mientras traceabas , te habras dado cuenta que iba apareciendo tu user y serial falso .pero al llegar al call 004DB677 ,veremos nuestro serial en los registros



Nuestro serial correcto seria el que esta en el registro edx , el serial “ bijFBnkMVkga1wZYli ”

Al principio me parecio muy complicado un programa hecho en Delphi , pero mientras mas practico se hace mas fácil. Gracias por tomarte el tiempo de leer este tuto ,espero que sirva a personas como yo , que estamos empezando en esto del reversing .
Queria aprovechar para Saludar y agradecer a DavicoRm por impulsarme a hacer un tutorial sobre mis avances. También agradecer por su apoyo a Apuromafo ,Ivinson,Softdat,Lior,Jaime,Nox a todos los CLS ,creo que si menciono a todos los que siempre me ayudan. seria interminable este tuto jeje . hasta la próxima ;)