



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

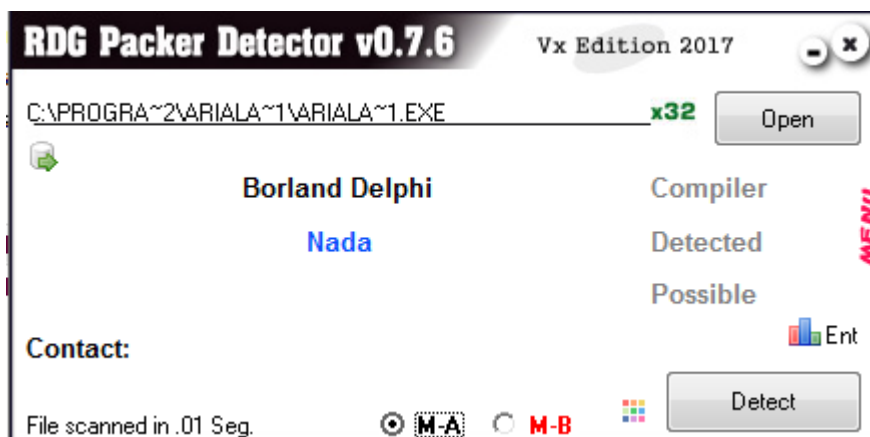
INTRODUCCION

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 . notarás que es mas sencillo de lo que piensas.

AL ATAQUE

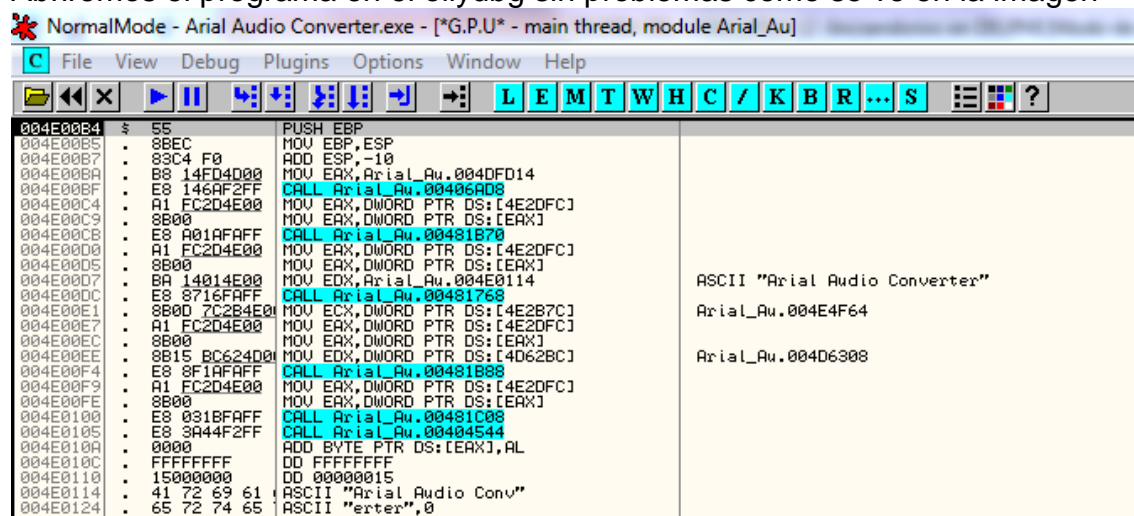
Bueno a comenzar. Primero ,instalado el programa revisamos con RDG packer si esta empacado o tiene un método antidebugging. y claro también para saber en qué lenguaje esta hecho XD





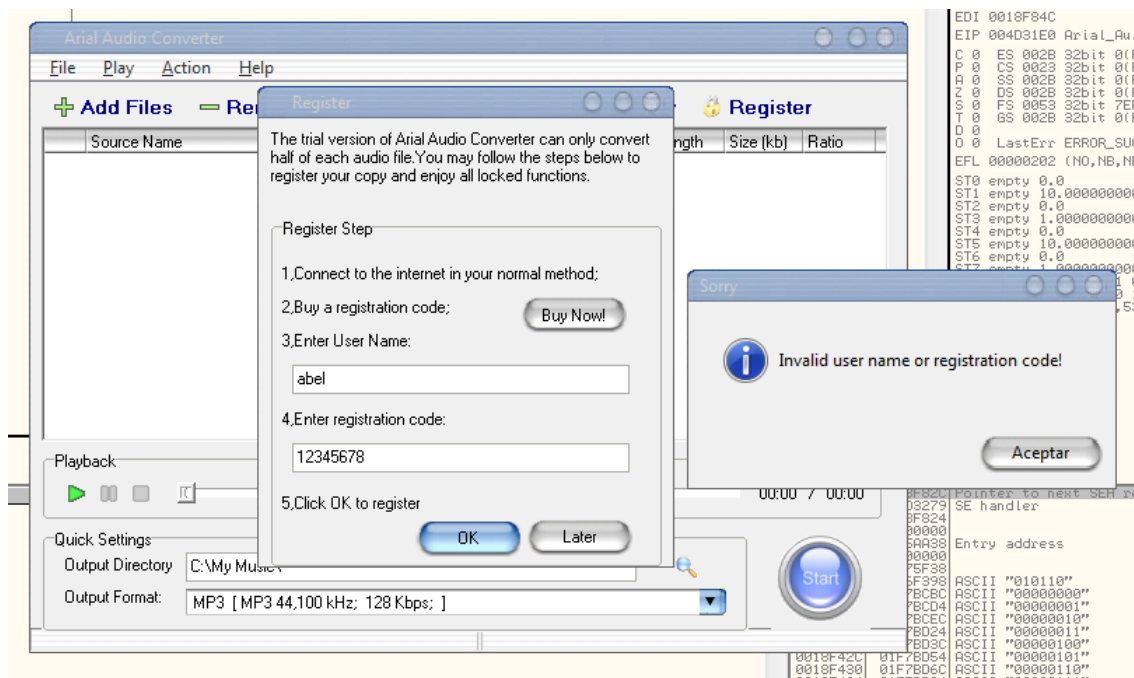
Como podemos ver no tiene ninguna protección ;) y apreciamos que está hecho en Borland Delphi .

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 .

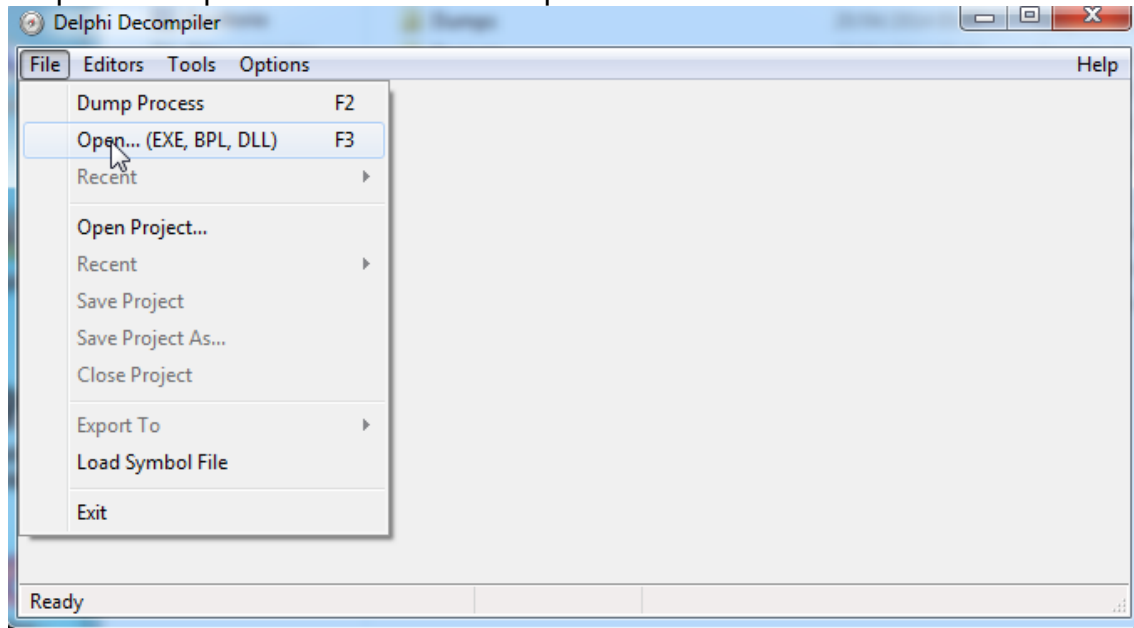
Abierto el programa nos vamos a help – register , probamos metiéndole mi nombre Abel y de serial 12345678



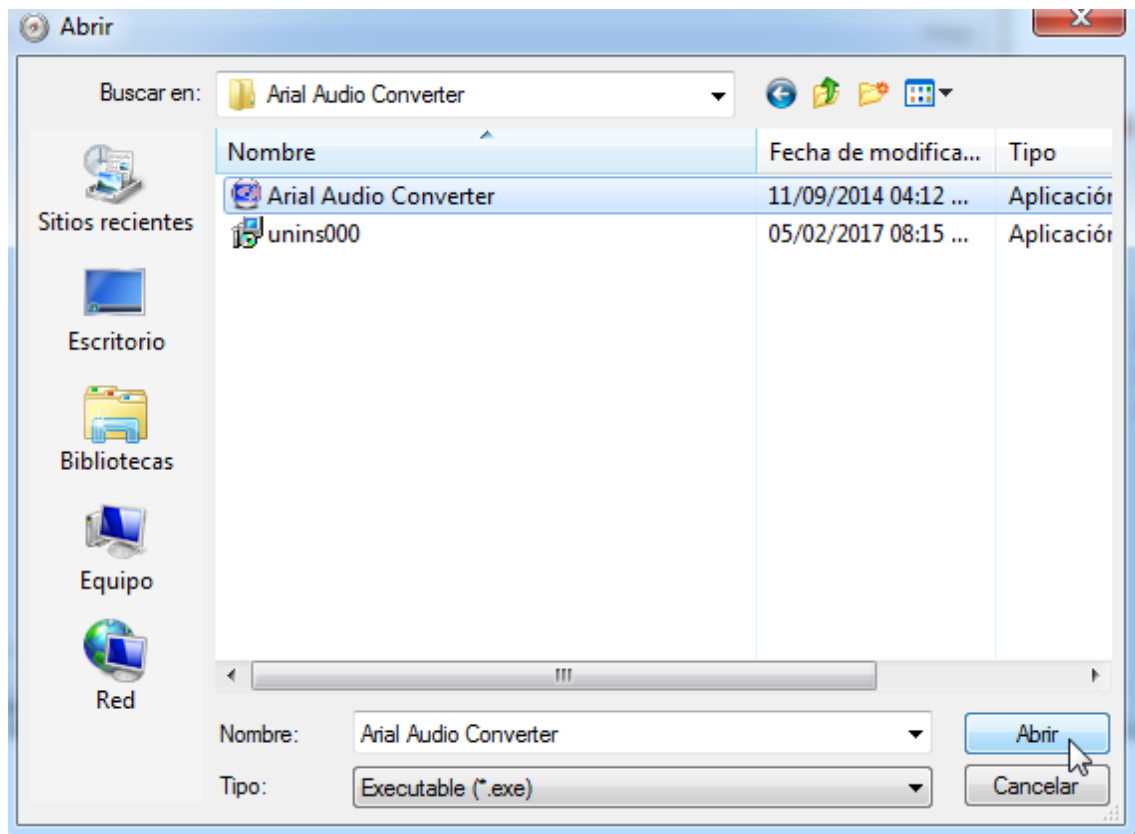
Como se aprecia en la imagen nos salió el chico malo con el título **sorry** y el mensaje **Invalid user name or registration code**. A partir de aquí aconsejo usar dede u otro descompilador de Delphi . Ya que según recomendaciones a veces será necesario usar esta herramientas. Cito unas palabras del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

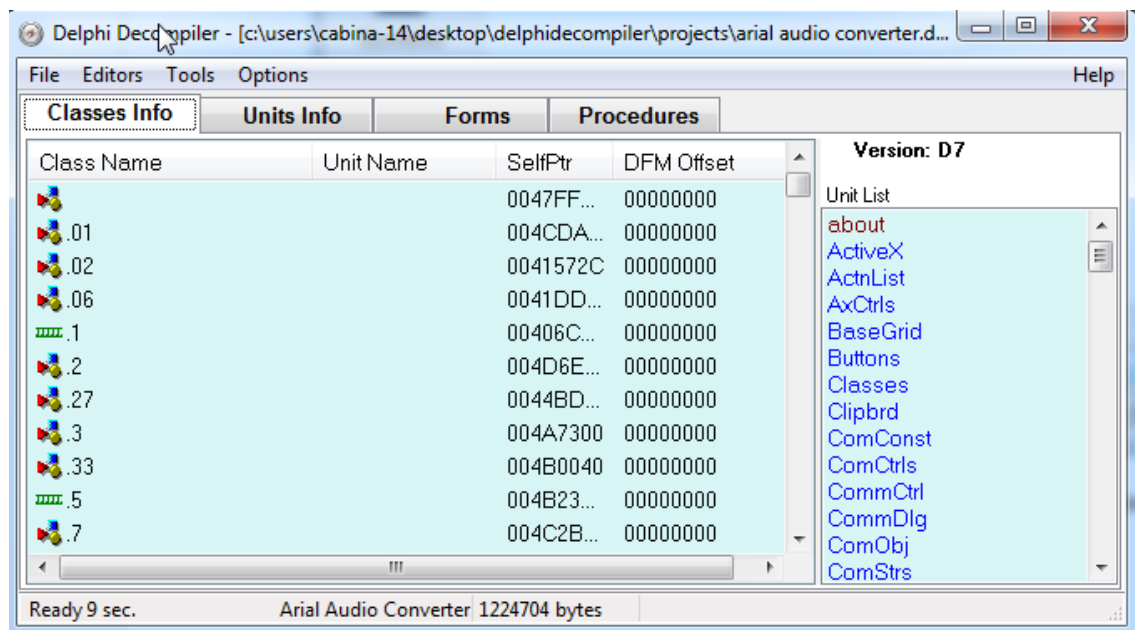
Seguimos .Al ver el mensaje del chico malo **sorry - Invalid user name or registration code** , quise comenzar haciendo un breakpoint en la api GetDlgItem,GetDlgItemtext o al messagebox pero no me salio .Asi que usaremos DEDE o en este caso DelphiDecompiler que el uso es el mismo,asi que pondré en el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



Y abrimos el programa

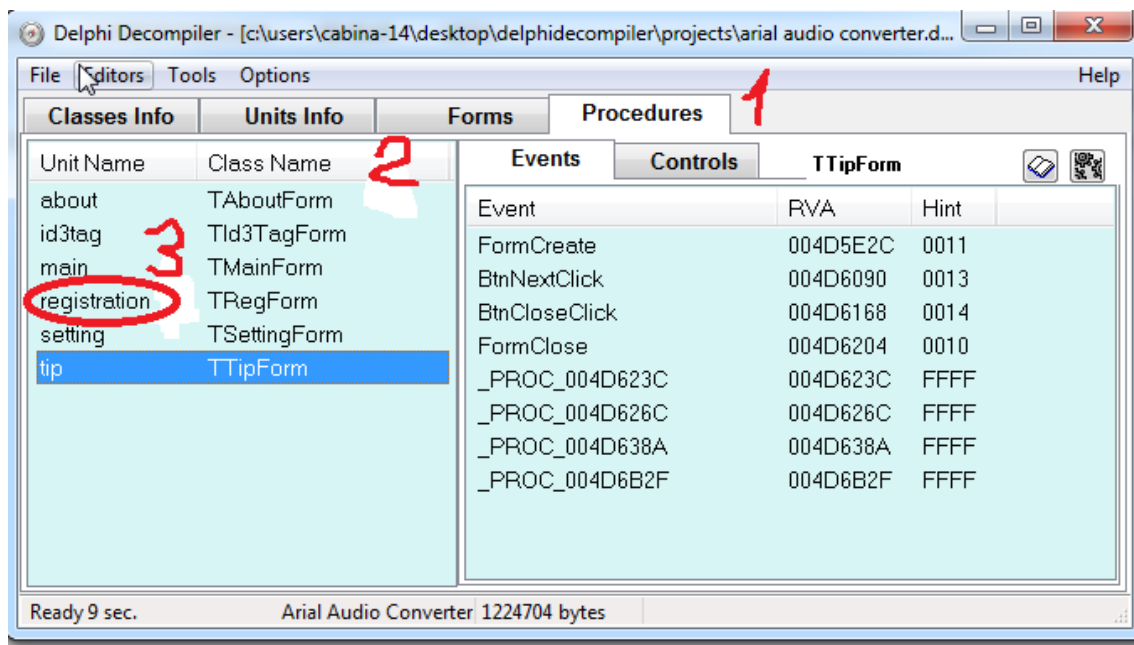


Se nos abrirá el software , yo lo di cerrar el software y apretó aceptar a los mensajes que aparecerán y no quedara asi

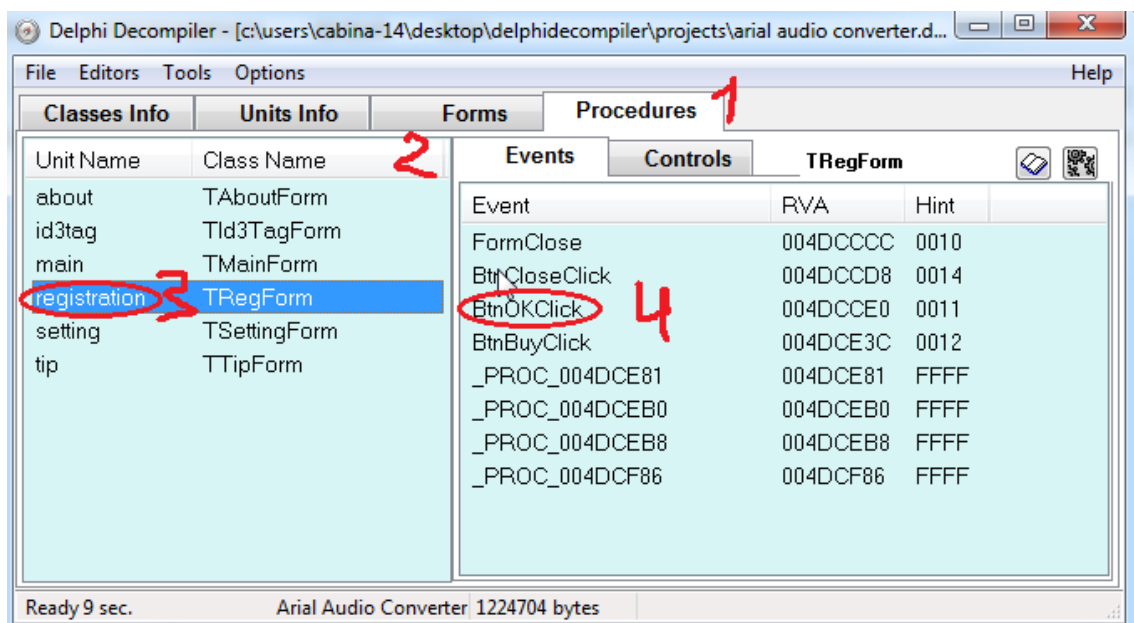


1. Elegiremos la pestaña Procedures
2. en la parte izquierda nos aparecerá dos columnas . la primera Unit name y columna izquierda class Name

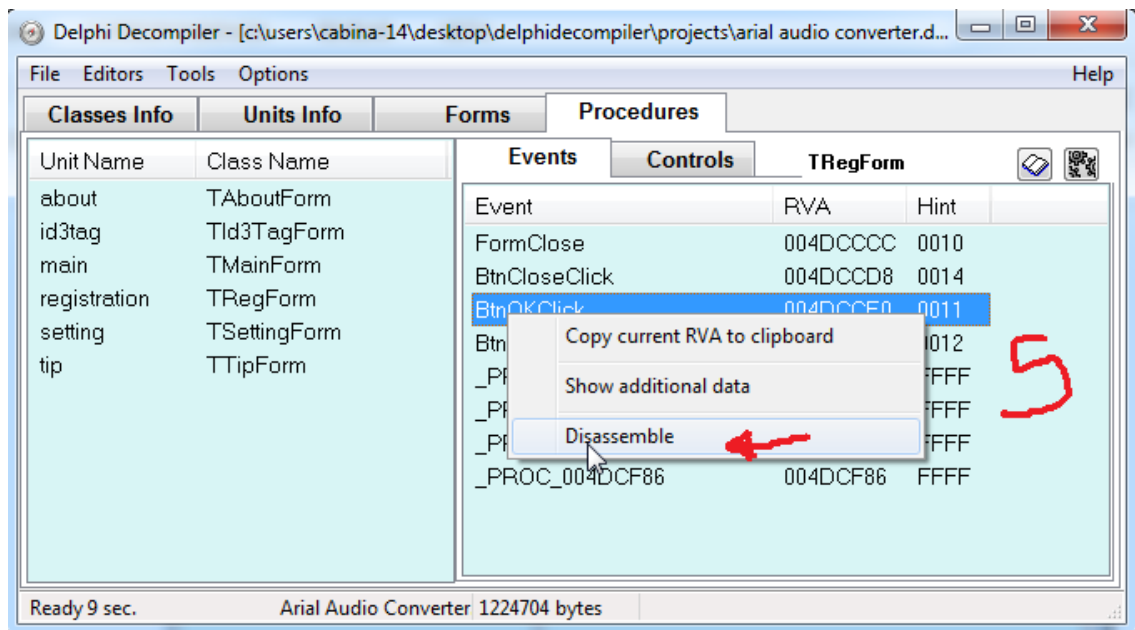
3. elegiremos Registration



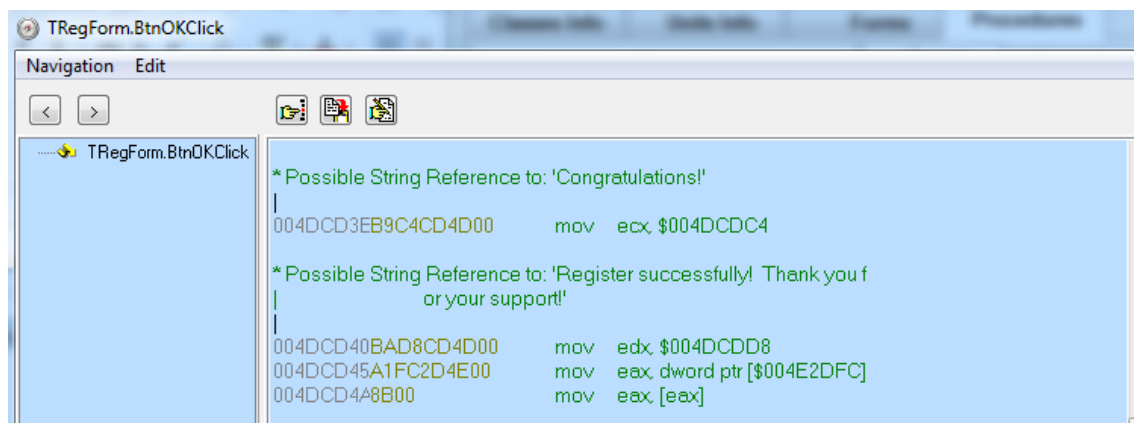
No se necesita ser un experto para notar que son las opciones de la pestañas del programa . en este caso nos interesa **Registration** . y nos aparece los botones de la ventana de registrar , el paso 4 seria elegir el btnOkClick para saber la dirección de las strings del chico malo y el chico bueno

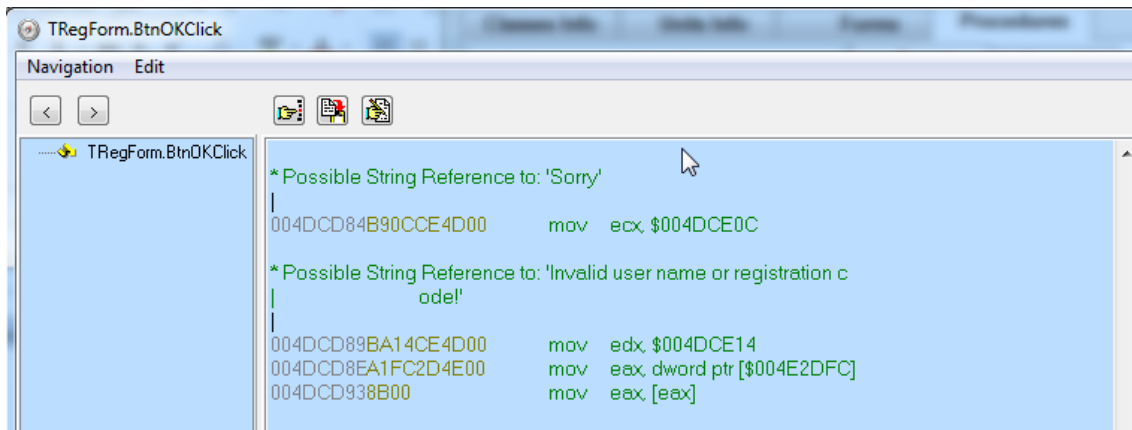


El paso 5 sería darle click derecho – y elegir la opción Disassemble

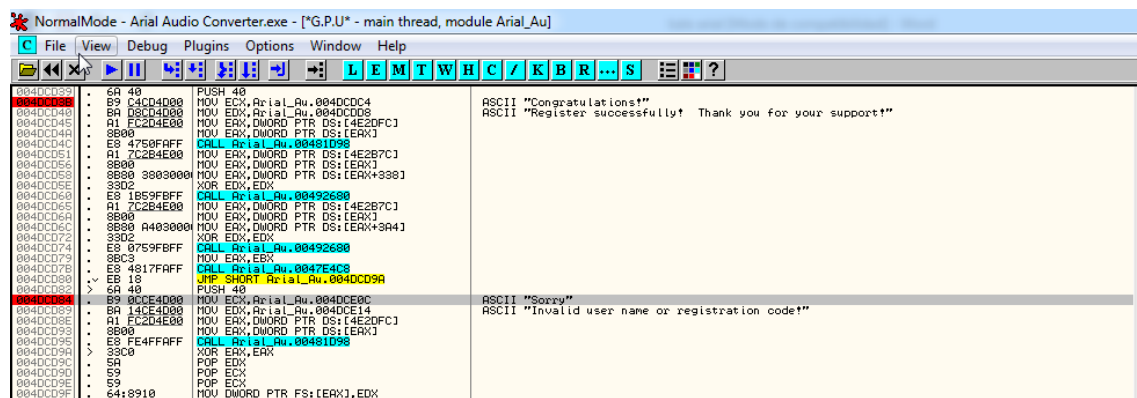


después de esto nos aparecerá un ventana y si bajamos un poco encontraremos el mensaje de chico bueno y si seguimos el mensaje de chico bueno





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

004DCD1E	8B55 FC	MOV EDX,DWORD PTR SS:[EBP-4]	
004DCD21	E8 C6E8FFFF	CALL Arial_Au.004DB5EC	
004DCD26	84C0	TEST AL,AL	
004DCD28	74 58	JE SHORT Arial_Au.004DCD82	
004DCD2A	A1 7C2B4E00	MOV EAX,DWORD PTR DS:[4E2B7C]	
004DCD2F	8B00	MOV EAX,DWORD PTR DS:[EAX]	
004DCD31	8B55 FC	MOV EDX,DWORD PTR SS:[EBP-4]	
004DCD34	E8 27ECFFFF	CALL Arial_Au.004DB5E0	
004DCD39	6A 40	PUSH 40	
004DCD3B	B9 C4CD4000	MOV ECX,Arial_Au.004DCD04	
004DCD3E	BA D8CD4000	MOV EDI,Arial_Au.004DCD08	
004DCD45	A1 FC2D4E00	MOV EAX,DWORD PTR DS:[4E2DFC]	
004DCD4A	8B00	MOV EAX,DWORD PTR DS:[EAX]	
004DCD4C	E8 4759FAFF	CALL Arial_Au.00492680	
004DCD51	A1 7C2B4E00	MOV EAX,DWORD PTR DS:[4E2B7C]	
004DCD56	8B00	MOV EAX,DWORD PTR DS:[EAX]	
004DCD58	8B80 38030000	MOV EAX,DWORD PTR DS:[EAX+3803]	
004DCD5E	33D2	XOR EDX,EDX	
004DCD59	E8 1B59FAFF	CALL Arial_Au.00492680	
004DCD65	A1 7C2B4E00	MOV EAX,DWORD PTR DS:[4E2B7C]	
004DCD6A	8B00	MOV EAX,DWORD PTR DS:[EAX]	
004DCD6C	8B80 A4030000	MOV EAX,DWORD PTR DS:[EAX+3A4]	
004DCD72	33D2	XOR EDX,EDX	
004DCD74	E8 0759FAFF	CALL Arial_Au.00492680	
004DCD79	8B83	MOV EAX,EBX	
004DCD7B	E8 4817FAFF	CALL Arial_Au.0047E4C0	
004DCD7E	EB 18	JMP SHORT Arial_Au.004DCD9A	
004DCD82	90 40	PUSH 40	
004DCD84	B9 0CE4D000	MOV ECX,Arial_Au.004DCE0C	
004DCD89	BA 1AC4D000	MOV EDI,Arial_Au.004DCE14	
004DCD8E	A1 FC2D4E00	MOV EAX,DWORD PTR DS:[4E2DFC]	
004DCD93	8B00	MOV EAX,DWORD PTR DS:[EAX]	
004DCD95	E8 FE4FAFF	CALL Arial_Au.00481090	
004DCD9A	33C0	XOR EAX,EAX	
004DCD9C	5A	POP EDI	
004DCD9D	59	POP ECX	
004DCD9E	59	POP ECX	
004DCD9F	64:8910	MOV DWORD PTR FS:[EAX],EDX	
004DCDA2	F5	REP	
004DCDA7	8D45 F8	LEA EAX,DWORD PTR DS:[EBP-8]	
004DCDA9	BA 02000000	MOV EDI,2	
004DCDAF	E8 4879FAFF	CALL Arial_Au.004046F4	

Vaya olly nos dice que viene de un salto

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

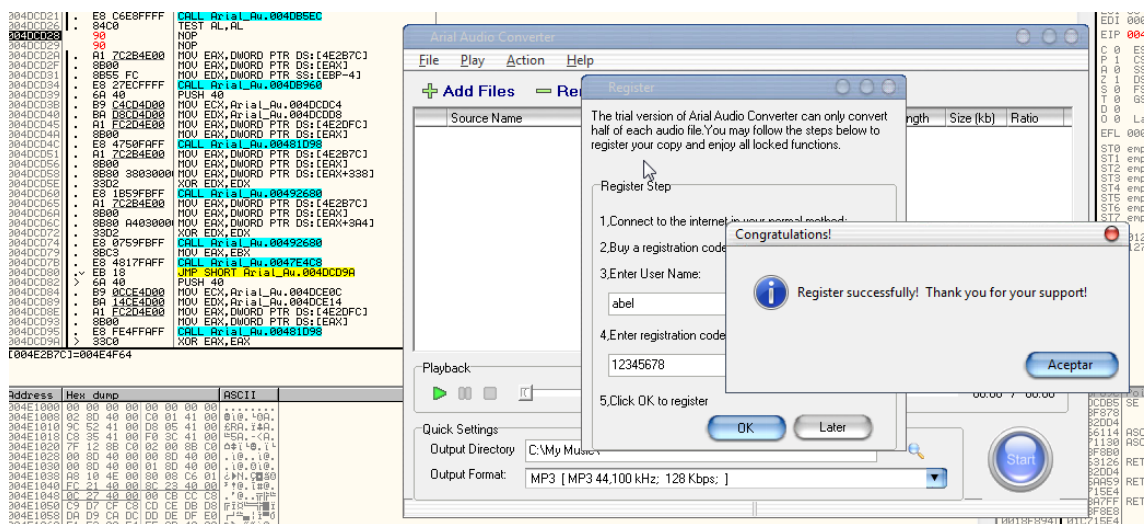
Este es la salto que decide el mensaje del chico malo y chico bueno . si somos mas curiosos arriba del salto hay un call , entonces sacamos conclusiones que esa call es la parte donde se genera el serial

004DCD1B	8B4D F8	MOV ECX,DWORD PTR SS:[EBP-8]	
004DCD1E	8B55 FC	MOV EDX,DWORD PTR SS:[EBP-4]	
004DCD21	E8 C6E8FFFF	CALL Arial_Au.004DB5EC	
004DCD26	84C0	TEST AL,AL	
004DCD28	74 58	JE SHORT Arial_Au.004DCD82	
004DCD2A	A1 7C2B4E00	MOV EAX,DWORD PTR DS:[4E2B7C]	
004DCD2F	8B00	MOV EAX,DWORD PTR DS:[EAX]	
004DCD31	8B55 FC	MOV EDX,DWORD PTR SS:[EBP-4]	

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

004DCD1E	8B55 FC	MOV EDX,DWORD PTR SS:[EBP-4]	
004DCD21	E8 C6E8FFFF	CALL Arial_Au.004DB5EC	
004DCD26	84C0	TEST AL,AL	
004DCD28	90	NOP	
004DCD29	90	NOP	
004DCD2A	A1 7C2B4E00	MOV EAX,DWORD PTR DS:[4E2B7C]	
004DCD2F	8B00	MOV EAX,DWORD PTR DS:[EAX]	
004DCD31	8B55 FC	MOV EDX,DWORD PTR SS:[EBP-4]	
004DCD34	E8 27ECFFFF	CALL Arial_Au.004DB5E0	
004DCD39	6A 40	PUSH 40	
004DCD3B	B9 C4CD4000	MOV ECX,Arial_Au.004DCD04	
004DCD3E	BA D8CD4000	MOV EDI,Arial_Au.004DCD08	
004DCD45	A1 FC2D4E00	MOV EAX,DWORD PTR DS:[4E2DFC]	
004DCD4A	8B00	MOV EAX,DWORD PTR DS:[EAX]	
004DCD4C	E8 4759FAFF	CALL Arial_Au.00492680	
004DCD51	A1 7C2B4E00	MOV EAX,DWORD PTR DS:[4E2B7C]	
004DCD56	8B00	MOV EAX,DWORD PTR DS:[EAX]	
004DCD58	8B80 38030000	MOV EAX,DWORD PTR DS:[EAX+3803]	
004DCD5E	33D2	XOR EDX,EDX	
004DCD60	E8 1B59FAFF	CALL Arial_Au.00492680	
004DCD65	A1 7C2B4E00	MOV EAX,DWORD PTR DS:[4E2B7C]	
004DCD6A	8B00	MOV EAX,DWORD PTR DS:[EAX]	
004DCD6C	8B80 A4030000	MOV EAX,DWORD PTR DS:[EAX+3A4]	
004DCD72	33D2	XOR EDX,EDX	
004DCD74	E8 0759FAFF	CALL Arial_Au.00492680	

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

```

0040C021 | . 8B55 FC      MOV EDX,DWORD PTR SS:[EBP-4]
0040C022 | . E8 C6E8FFFF  CALL Aria_Au.0040B5EC
0040C026 | . 84C0         TEST AL,AL
0040C028 | . 74 F0        IF SHORT Aria_Au.0040B5EC

```

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

```

0040B676 | . E8 A379FFFF  CALL Aria_Au.0040B114
0040B677 | . 8B45 F8      MOV EAX,DWORD PTR SS:[EBP-8]
0040B678 | . 8B55 F4      MOV EDX,DWORD PTR SS:[EBP-C]
0040B679 | . E8 6094F2FF  CALL Aria_Au.0040B40C
0040B67A | . 75 02        JNZ SHORT Aria_Au.0040B680
0040B67B | . B3 01        MOV BL,1
0040B67C | . 33C0         XOR EAX,EAX
0040B67D | . 5A          POP EDX
0040B67E | . 59          POP ECX
0040B67F | . 59          POP ECX
0040B680 | . 64:8910     MOV DWORD PTR FS:[EAX],EDX
0040B681 | . 68 B5B64D00 PUSH Aria_Au.0040B685

```

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

```

EAX 01F36114 ASCII "12345678"
ECX 00000000
EDX 01F485E8 ASCII "bijFBnkMUKga1wZYli"
EBX 00000000
ESP 0018F82C
EBP 0018F858
ESI 0045AA38 Aria_Au.0045AA38
EDI 00000000
EIP 004DB677 Aria_Au.004DB677

C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 1 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 7EFD0000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
O 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO.NB.E.BE.NS.PE.GE.LE)

```

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

Al principio me parecia 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 ;)