ESTUDIO DE PROTECCIONES BASICO PARA PRINCIPIANTES (También llamado cracking)

Impartido por Ratón (Nivel principiante)

Nota

Cada capitulo ira acompañado de su crackme correspondiente.No facilitare paginas de donde bajarse herramientas ni enlaces a paginas de crackers, la intención es que busquéis en Internet todo lo necesario. Seguro que encontráis mas paginas de herramientas, tutoriales y utilidades relacionadas con este tema que las que yo pueda deciros.
Con esto solo quiero fomentar vuestro interés, además se que la búsqueda os proporcionara gratas sorpresas.
A todos un saludo.

Capitulo 3

Victima

Karpoff crackme 1 de el maestro Karpoff

Herramientas

Olly Debugger.
Peid – Detector de protecciones.
DeDe – Delphi Decompiler.
Instinto

Objetivo

Aprender el manejo básico de herramientas nuevas: Peid - DeDe
Crearnos una rutina la cual adoptaremos de aquí en adelante a la hora de trabajar con los siguientes crackmes.

Al ataque

Lo primero será sentar unas bases que utilizaremos con todos los crackmes o programas que analicemos de aquí en adelante.

0 – Hacer una copia del ejecutable con el que vamos a trabajar.
1 – Analizar el ejecutable con un detector de protecciones para ver si esta protegido/comprimido.
2 – Fijarnos en que lenguaje esta escrito el programa.
3 – Si estuviera protegido desprotegerlo con el descompresor adecuado para poder analizar el código.
4 – Ejecutar el programa una vez desprotegido.
5 – Acostumbrarnos a introducir el mismo serial de prueba en todos los programas que nos pidan serial para registrarnos.

Comenzamos con el crackme de hoy.

0 – Hacemos copia del crackme.

No creo que tenga que explicar esto, verdad ¿?

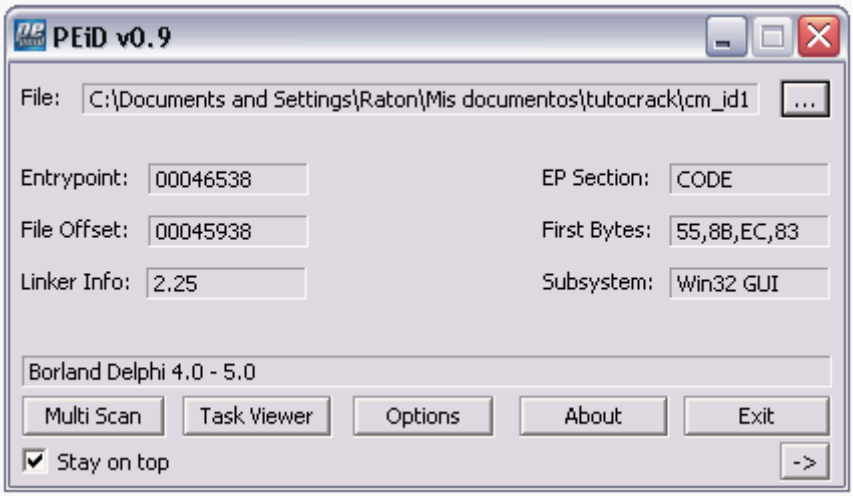
1 – Analizamos con un detector de protecciones.

Utilizaremos una nueva herramienta Peid (PE identifier).

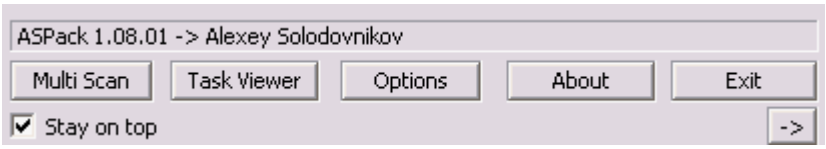
Peid

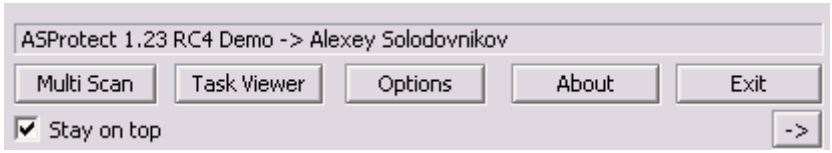
Abrimos el Peid y en la ventana del programa pulsamos el botón con los tres puntos (…) para buscar y cargar nuestro crackme como haríamos con cualquier otro programa.

Tenemos el crackme cargado en el Peid y nos fijamos en la parte inferior justo encima de la línea de botones y vemos que nos dice
Borland Delphi 4.0 – 5.0
Eso significa que esta escrito en Delphi y que no tiene ninguna protección.



Como sabemos si tiene o no protección un programa ¿?
Mirad los siguientes ejemplos





Se ve el nombre de la protección y el del creador de la misma, nada que ver con los nombres de los lenguajes de programación (Delphi, C, C++, Visual Basic, Visual C, etc).

Antes de cerrar el Peid pulsamos el botón Options y lo dejamos como en la imagen siguiente y pulsamos save para guardar los cambios.

Lo que suelen hacer estos programas es comprimir o empacar el programa empleando rutinas de protección.
Realmente cuando se ejecuta el programa lo primero que se ejecuta es la rutina de descompresión pero es más sencillo de entender si lo imaginamos como dije en la línea anterior.

No tiene que ver nada con la compresión Zip o Rar que hacen Winzip o Winrar.
Estas protecciones se verán en capítulos posteriores, quedaros de momento con el manejo del Peid y la costumbre de analizar los crackmes antes de abrirlos con el Olly.

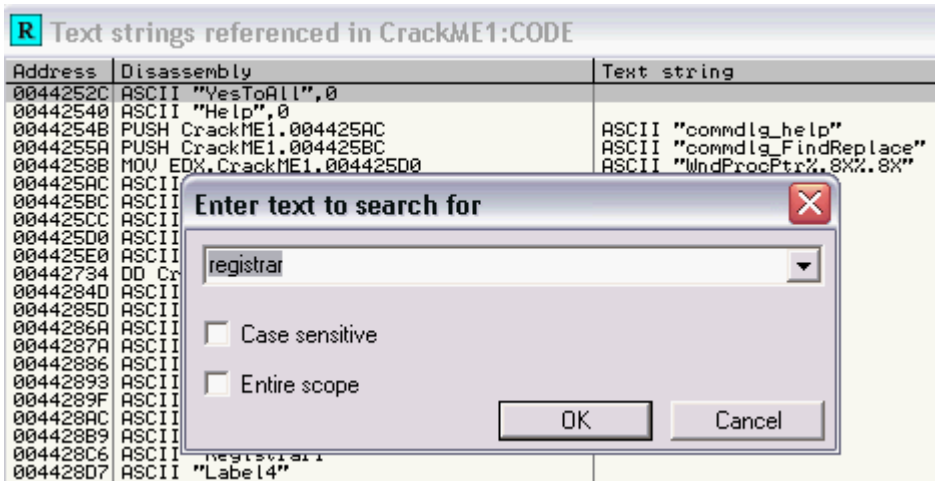
2 – Nos quedamos con el lenguaje en que esta escrito el programa: Delphi (en este caso).
3 – No esta protegido pues seguimos con el siguiente paso.
4 – Ejecutamos el programa.

Vemos que debemos introducir un serial y pulsar Registrar para registrarnos.
Pero escribir nuestro serial falso y pulsar Registrar no pasa nada, no sale ninguna ventana con aviso de registrado o no registrado.

Este programa esta defectuoso, me han engañado...

Por que pasa esto ¿?
Pues amigos porque no todas las protecciones te dan pistas tan claras para encontrar el serial correcto como los crackmes facilones de los capítulos anteriores.

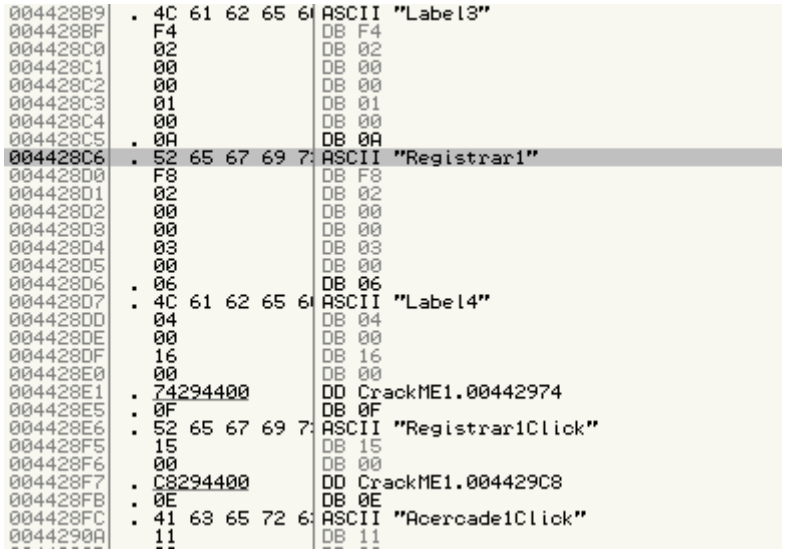
Abrámoslo con Olly para investigar que esta pasando.
Buscaremos la única pista que tenemos: la cadena Registrar.
Buscamos las Strings en el Olly, pero esta vez como profesionales: nos colocamos encima de la primera cadena y con el botón derecho del ratón Search for text



Con click derecho – Search text

Aparece otra ventana desmarcamos Case sensitive (esto es para que busque indistintamente escribamos en mayúsculas o minúsculas) y escribimos la palabra (cadena) a buscar.
Pulsamos OK.
Llegamos a un sitio que puede interesarnos vemos en dos líneas la palabra Registrar.

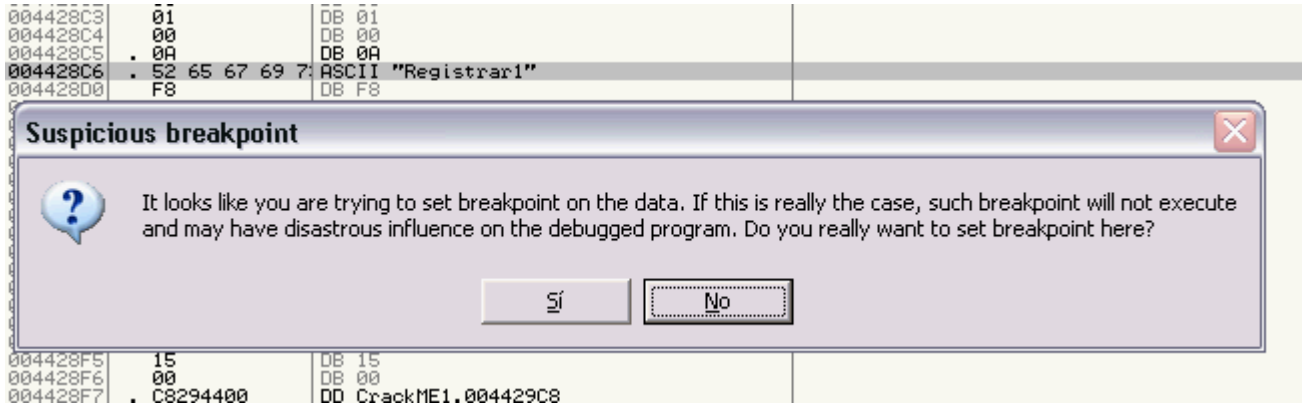
Doble click sobre el primero Olly nos lleva a 00446132 pero no vemos ningún CALL ni CMP ni salto ni nada de lo que nos había servido para crackmes anteriores.



Aquí no hay pistas

Reflexionemos:
No vemos nada conocido, ni cadena diciendo registrado o crackme resuelto o algo por el estilo.
No podemos rendirnos al principio del curso, usemos la intuición.
Intentaremos poner un Breakpoint en Registrar1 a ver que pasa, pues se supone que el programa al llegar aquí debe parar.

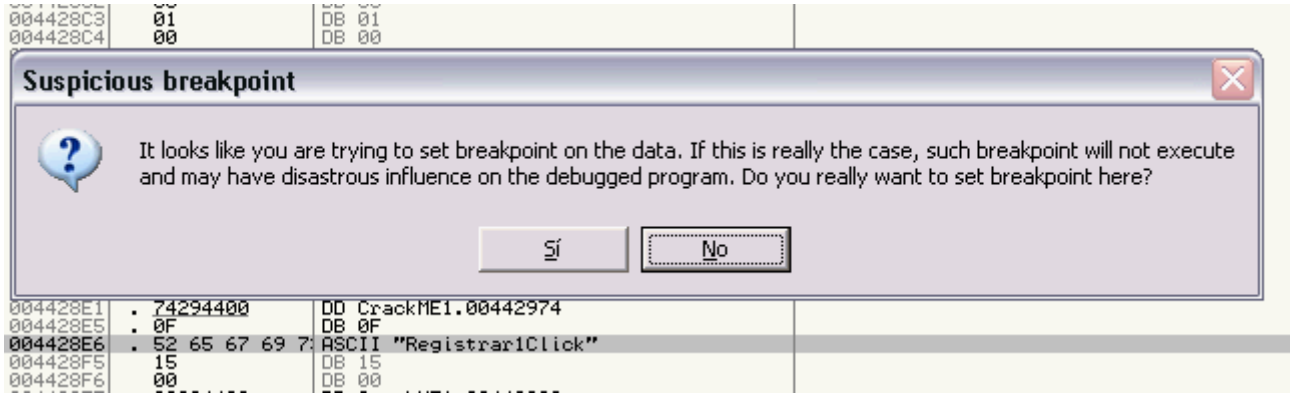
Al pulsar F2 para poner el Breakpoint aparece este aviso que nos asusta.



Lagarto i! Lagarto!!

Traducción ratonil del mensaje de advertencia = como pongas el Breakpoint aquí la puedes cagar.

Lo mismo nos pasa con la otra String



Otra vez la misma advertencia

Como aun nos asusta un poco este tema del crackeo no ponemos Breakpoint en ninguna de estas dos direcciones (aparte de que no conseguiremos nada).

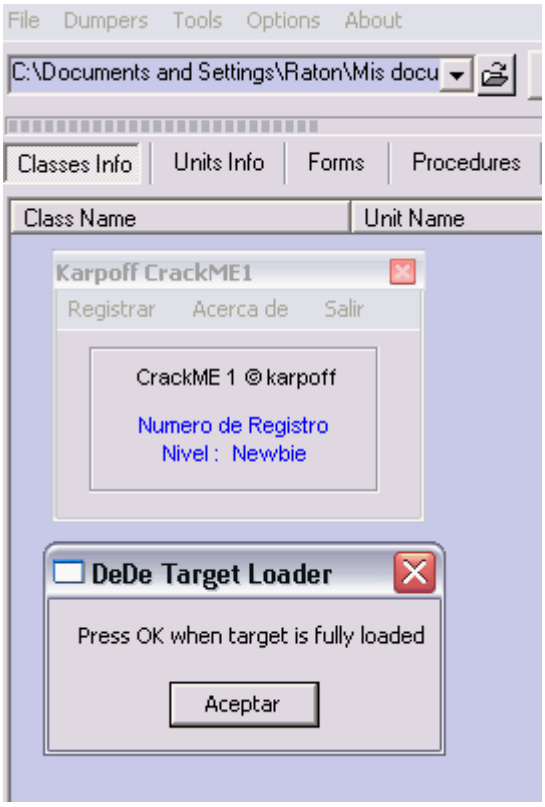
Reflexión 2:

Que c#ñ# hacemos ahora ¿?
Recordamos una de las normas en las que hizo hincapié el ratón: 2 – Fijarnos en que lenguaje esta escrito el programa.
Miramos la lista de herramientas y vemos un programa nuevo: DeDe Delphi decompiler.
Nuestro crackme esta escrito en Delphi.
Conclusión: parece que deberíamos abrirlo con un programa especial para Delphi.

DeDe

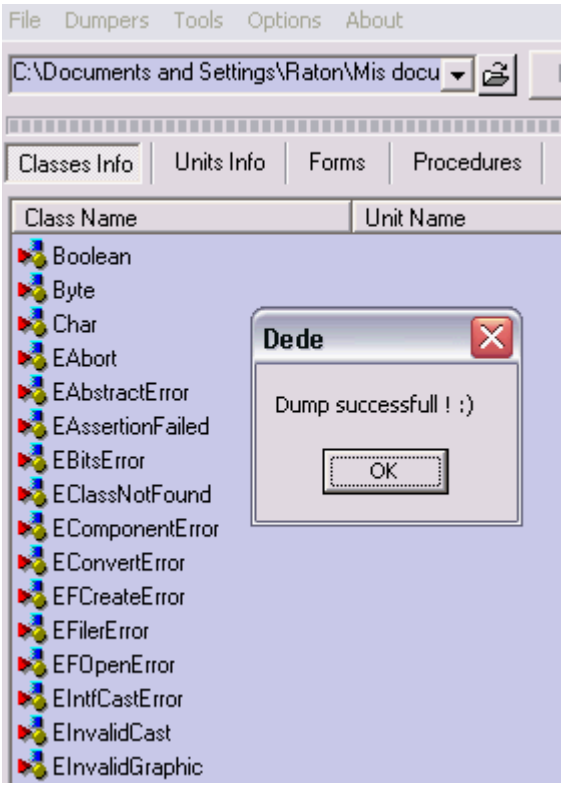
Abrimos DeDe.
Cargamos el crackme en DeDe pulsando en el botón que tiene dibujada la carpeta

Una vez cargado pulsamos el botón Process y nos aparece la ventana del crackme y otra ventanita que nos dice que presionemos aceptar cuando el objetivo este cargado.
Como sabemos que el crackme esta cargado ¿? Pues cuando nos aparece la primera ventana del crackme (como ahora) esperamos un par de segundos y pulsamos Aceptar.



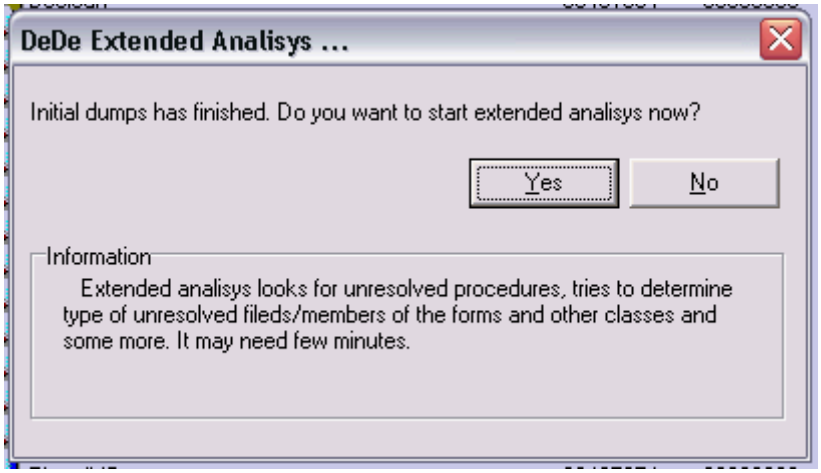
Cargando el programa en DeDe

Empieza el DeDe a trabajar con nuestro crackme y cuando termina aparece este aviso

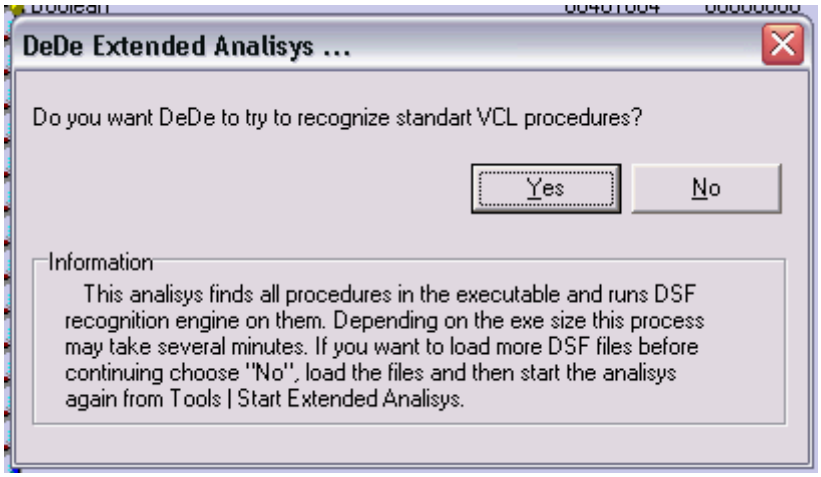


DeDe ha terminado de cargar el programa

Pulsamos OK y en las dos siguientes ventanas que aparecen pulsamos NO.

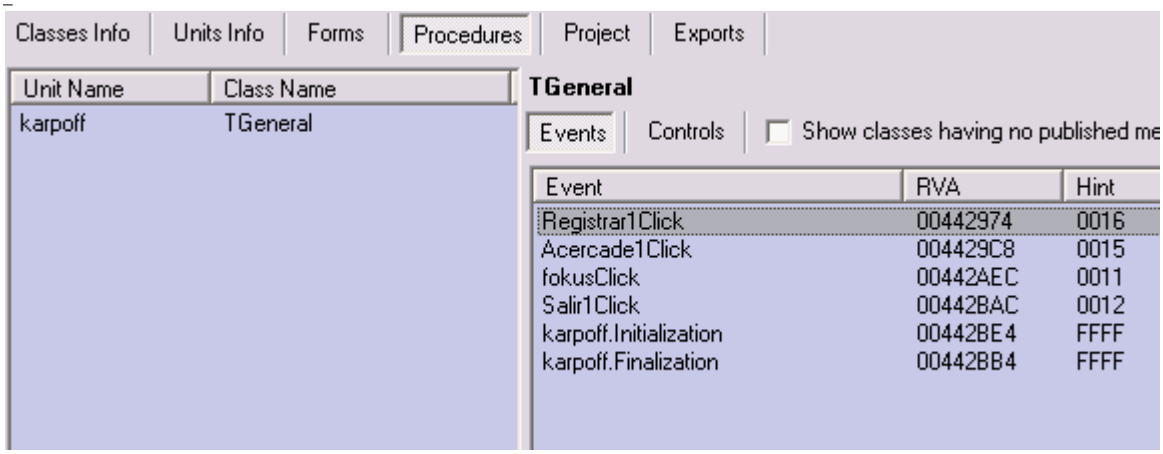


Pulsamos no



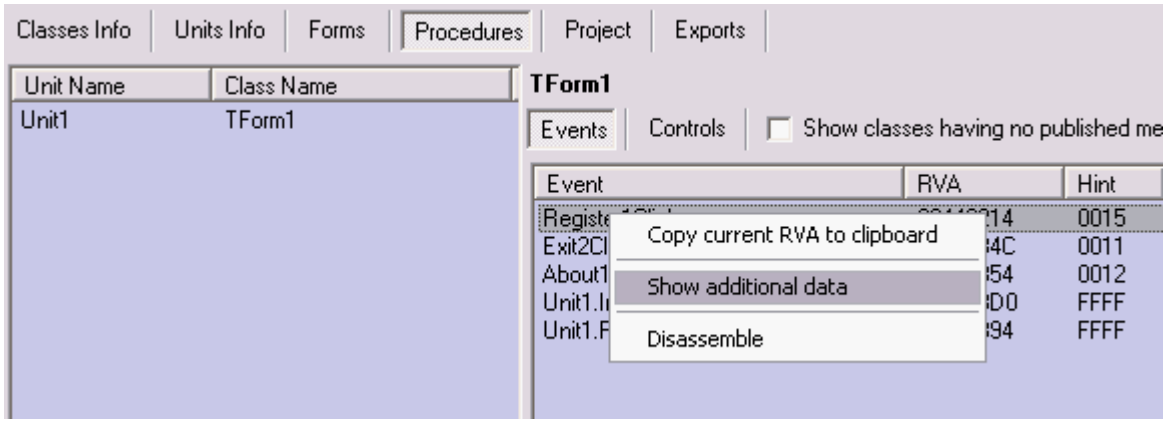
Pulsamos no

Una vez que cerramos las dos ventanas vemos la pantalla principal del DeDe con el crackme destripado.
Pulsamos en Procedures y vemos esto

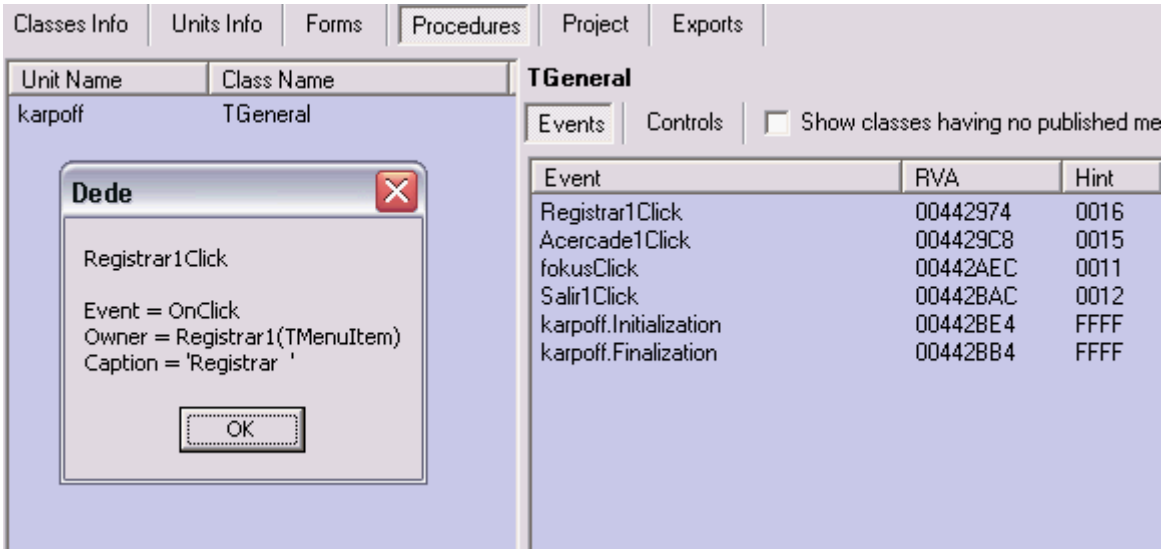


Ventana Procedures

Registrar1Click es una de las Strings que encontramos en el Olly, nos colocamos encima y click derecho - Show additional data

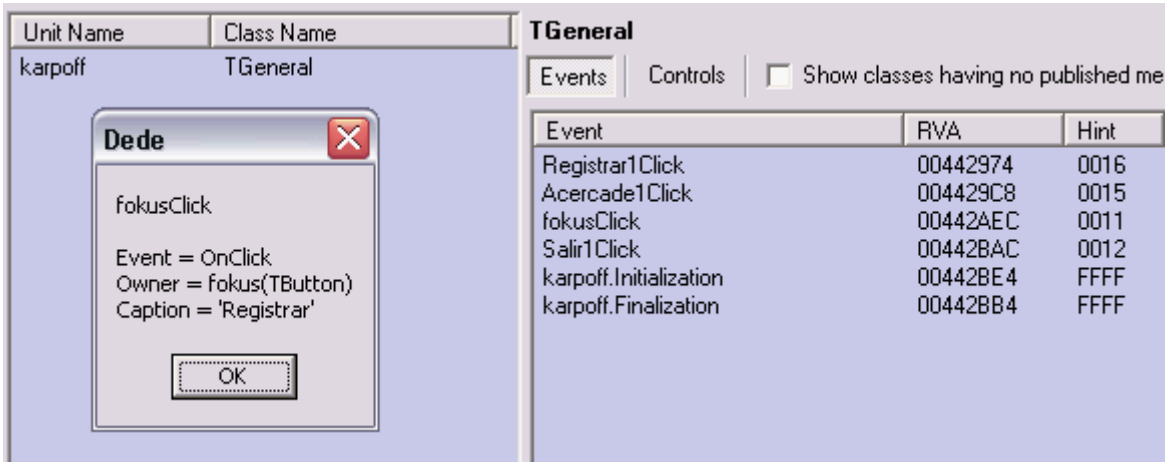


Y vemos una ventana con información interesante



En esta imagen vemos información adicional de Registrar1Click

Caption = Registrar Caption es el nombre que vemos de algún componente del programa (en este caso del crackme) esto nos indica que el Caption de este componente es Registrar.
En nuestro crackme el componente que tiene el Caption Registrar es el botón donde debemos pulsar para registrarnos.
Por tanto hemos encontrado el botón Registrar, el que pulsamos para hacer aparecer la casilla donde introducir nuestro numero de serie.
Pero este no es el botón que nos interesa, tiene que haber otro cuyo Caption sea Registrar, tenemos que buscarlo en el DeDe.
Fijaros en que no es igual el nombre del componente que el Caption del componente.
Fokus parece un nombre sospechoso le diremos que nos muestre datos adicionales



Te pille i!

Efectivamente el caption de focusClick es Registrar

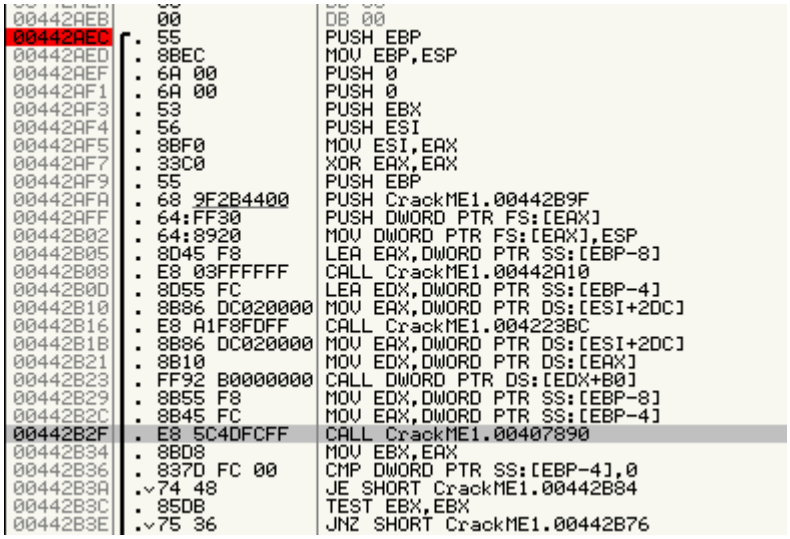
Nombre del componente = Fokus (TButton tipo botón)
Caption del componente Fokus = Registrar

Event = OnClick Algo (un evento) ocurre cuando se "clickea" este botón (el botón Fokus cuyo Caption es Registrar)

Vemos al lado de FokusClick en el apartado RVA una dirección (00442AEC) la apuntamos.
Esa dirección es donde se produce el evento OnClick, para entendernos donde se "clickea" el botón Register.
Si vamos a esa dirección en el Olly y ponemos un Breakpoint el programa parara cuando hagamos click sobre el botón Registrar.
Para aclarar un poco las cosas el botón Registrar1Click (tipo menú item) corresponde a la palabra Registrar del menú superior del crackme.
El botón focusClick (tipo botón) corresponde a la palabra Registrar que aparece debajo de la casilla donde debemos introducir el serial y su dirección es 00442AEC.

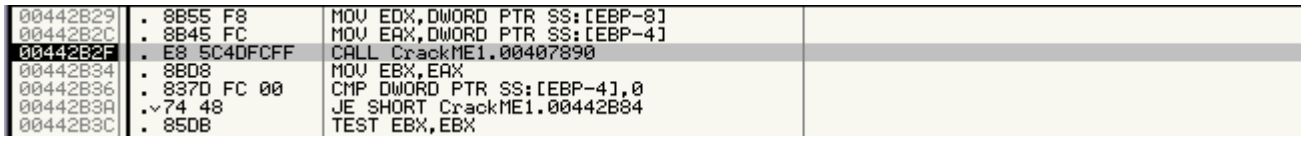
Cerramos DeDe, abrimos Olly y cargamos el ejecutable
Lo siguiente será ir a la dirección 00442AEC con Control + G con el fin de colocar un Breakpoint (BP) en esa dirección.
Con esto conseguiremos que Olly pare cuando pulsemos el botón registrar.
Arrancamos el programa con F9 introducimos nuestro numero y pulsamos registrar, el

Olly para hache



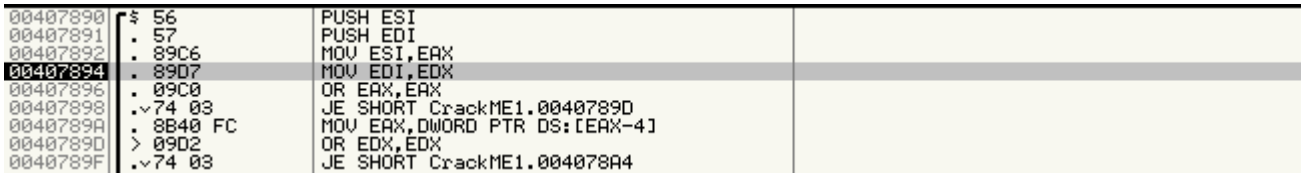
00442AEC aquí para Olly cuando pulsamos el botón Registrar, mas abajo una zona con instrucciones conocidas

Olly paro cuando pulsamos el botón Registrar, antes de pulsarlo habíamos introducido nuestro numero (yo sigo con mi 15151515), por tanto nuestro numero debe de andar por algún sito para que el programa lo compare.
Vemos unas líneas más debajo de donde paro Olly unas instrucciones conocidas Call Cmp Je.
Bajemos con F8 hasta la dirección 00442B2F y una vez encima de ella pulsemos F7 para entrar a examinar el Call (aunque vemos ya algo que nos gusta en la ventana registers del Olly).



Je je

Dentro del Call confirmamos la sospecha



Dentro del Call nos movemos con F8 hasta ver esto

Probamos y...

Lo de siempre: intentadlo sin mirar tutorial

Gracias

A todos los crackers y programadores de los cuales he aprendido y sigo aprendiendo.
A los creadores de crackmes
En especial y sin menospreciar a nadie a Ricardo Narvaja por su aportación y su trabajo sobre el estudio de las protecciones y sus tutoriales en castellano y a Makkakko por sus tutoriales con Olly Debugger (Recomendados 100%).
A ti que me lees.

Ratón Enero 2004