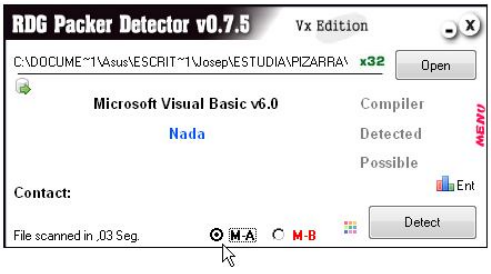
Crackme	Crackme DRm
Misión	-Remover Nag -Activar button -Registrarse
Compilado	Visual Basic 6.0
Herramientas	Olly 1.10 – RDG 0.7.5 – HxD V1.7.7.0
	(Plugin Olly Hide Debugger)
Sistema Operativo	Windows Xp SP3
Cracker	QwErTy
Dedicado a	RICNAR / CLS / SoftDat Newzombie / DavicoRm y a Ismael Pérez

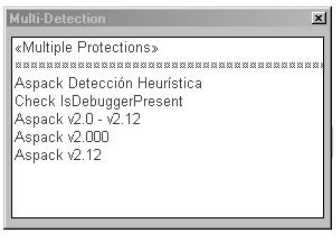
ESTUDIANDO A LA VÍCTIMA

Hacemos una copia del Crackme (Siempre es importante trabajar con una copia), lo abrimos y nos aparece una ventana en la que observamos; el nombre de la misma "Crackme!", un mensaje "Cracker??", y un button "Aceptar", le damos a "Aceptar" y nos saca fuera.

CONTINUAMOS ESTUDIANDO LA VÍCTIMA

Abrimos el Crackme con el RDG

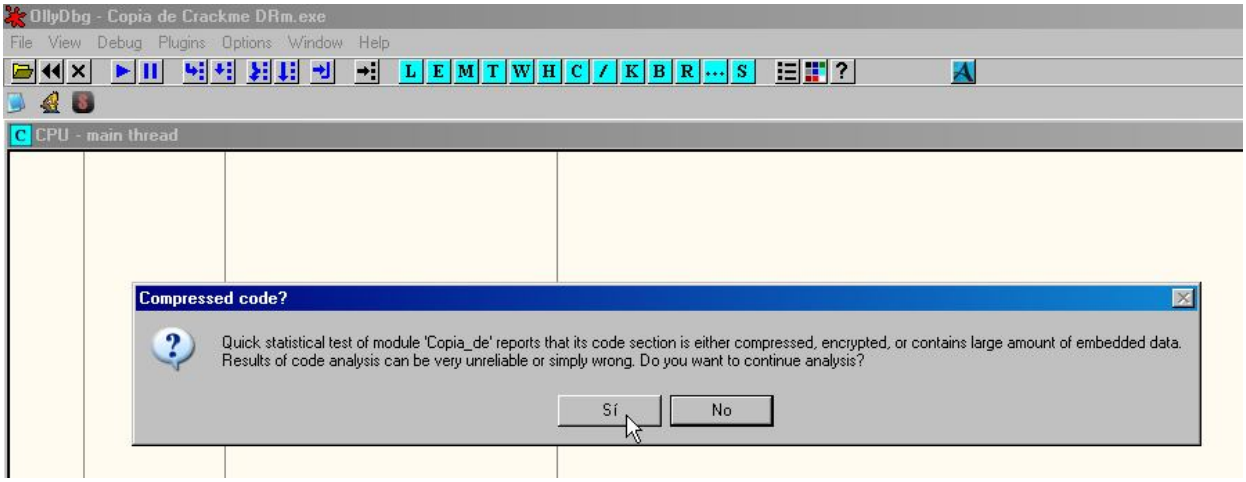




Ya sabemos algo más, el RDG Packer Detector nos informa en el escaneo rápido "M-A", que el crackme está compilado en Visual Basic V6.0, y en el escaneo profundo "M-B" de un compilado en Visual Basic 6.0 Código Nativo, de un Aspack v2.12 detectado y de un posible Check IsDebuggerPresent.
Bien…., pues lo tendremos en cuenta.

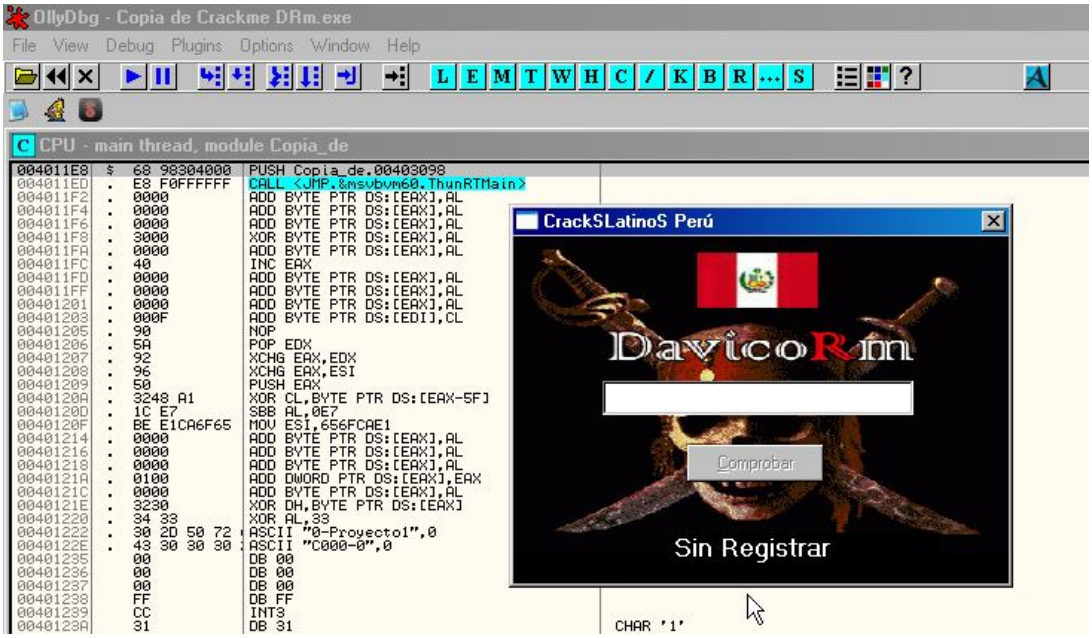
VAMOS A POR ELLA

Salimos del RDG y abrimos el crackme con Olly (importante: con los plugins antiloquetengamos desactivados), y nos sale el cartelito de "Compressed code?", avisándonos de que el crackme puede estar comprimido,encriptado, bla.bla.bla….. le decimos que "Sí" para que continúe con el análisis

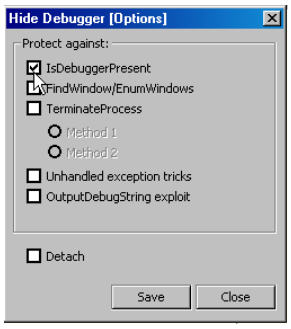


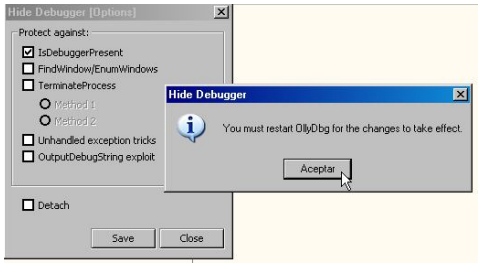
Olly lo analiza y abre correctamente. Además nos fijamos que empieza con un "PUSH seguido de una CALL" (detalle característico de los Visual Basic).

damos run (F9) para comprobar que el crackme corre y nos aparece la primera sorpresa

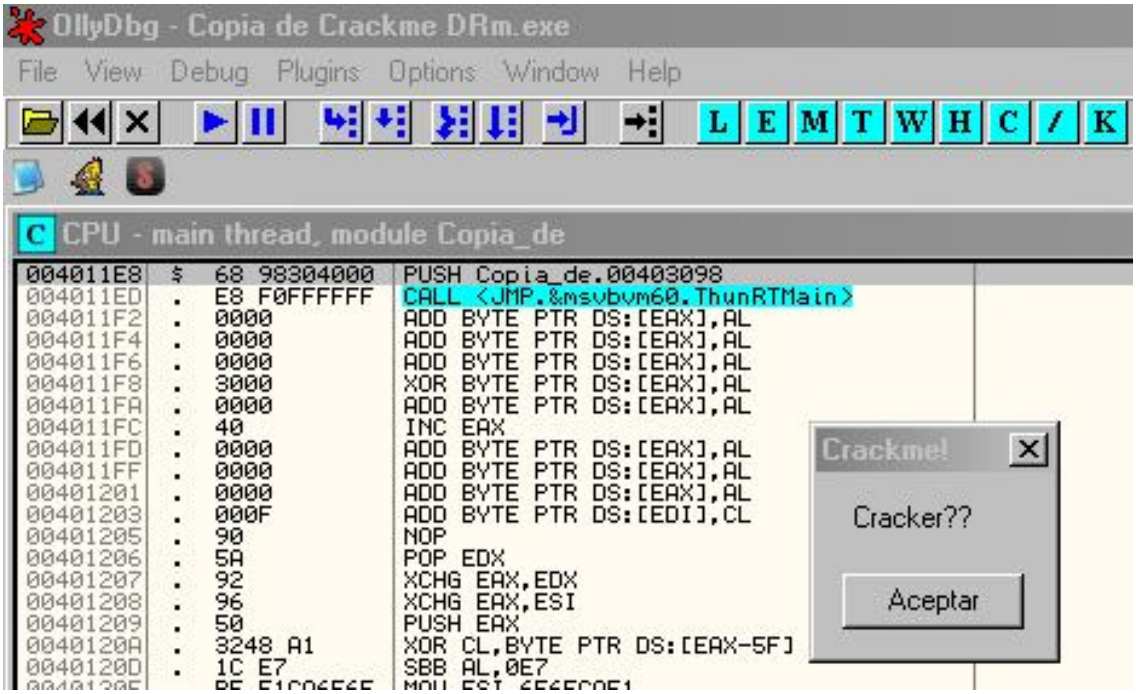


Que cosa más rara, cuando ejecutamos el crackme fuera de Olly nos mostró una ventana totalmente diferente a esta, aquí pasa algo……. mi instinto de cracker me dice que este crackme tiene algo metido dentro que detecta que lo estamos debuggeando.
Vamos a hacer una prueba, vamos a "Plugins – Hide Debugger" y activamos la casilla "IsDebuggerPresent" le doy a "Save" para guardar cambios, después a "Close" y a "Aceptar", Ahora salimos totalmente de Olly para que los cambios surtan efecto y volvemos a cargar de nuevo el crackme con Olly (ahora con el plugin IsDebuggerPresent activado).



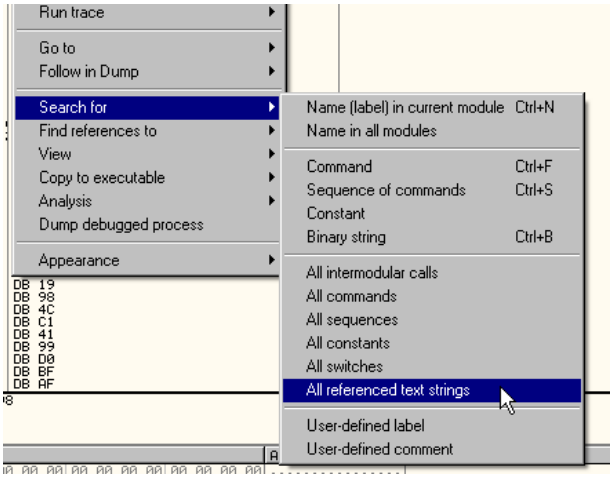


Damos "Run" para que corra y comprobamos que ahora Olly nos muestra el crakme de igual forma que cuando lo corremos fuera de el.



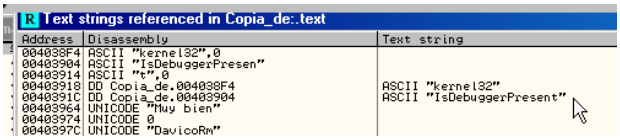
Osea que nuestra intuición queda demostrada, por tanto empecemos con nuestra PRIMERA MISIÓN: Conseguir que al ejecutar el crackme fuera de Olly no aparezca esta Nag y nos muestre la segunda ventana.

Continuamos, reiniciamos Olly, click derecho y "Search for – All referenced text strings"

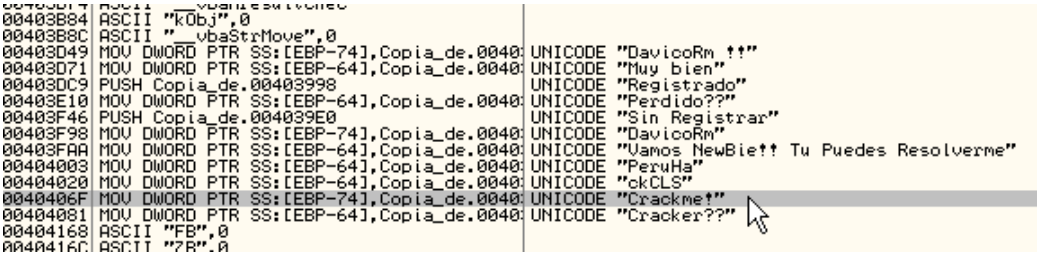


y encontramos de momento dos referencias que nos interesan: "Cracker??" y "Crackme!".

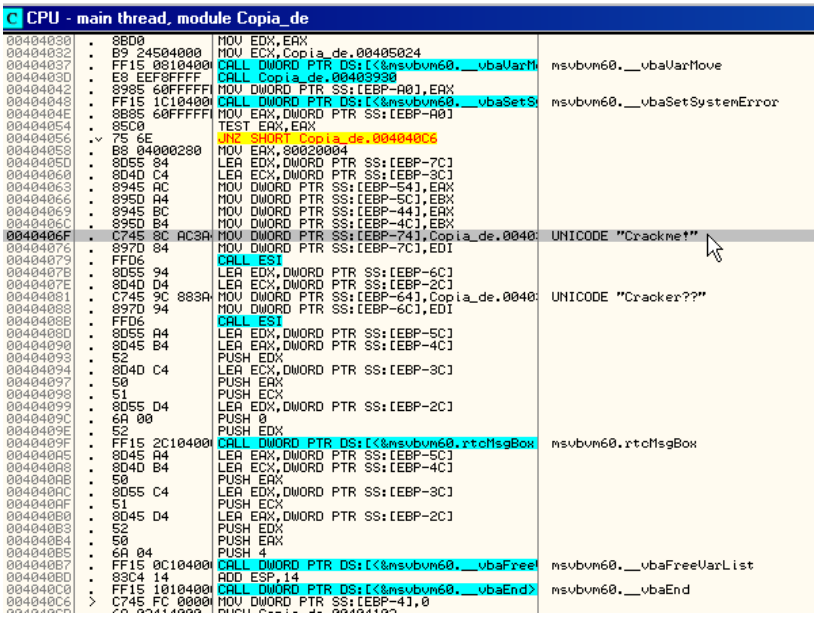
NOTA: Antes de llegar a ellas tambien vemos una referencia a "IsDebuggerPressent" pero este tema ya lo hemos detectado y solucionado al activar el Plugin.



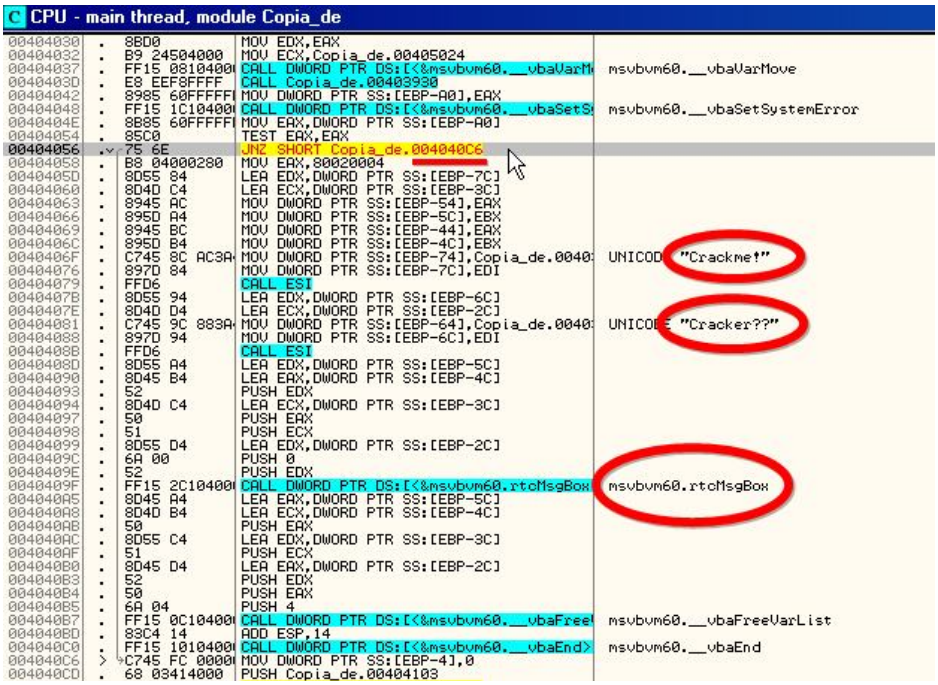
No nos entretengamos y sigamos,



"Cracker??" y "Crackme!" son las referencias que salen al abrir el Crackme.exe fuera de Olly. Pues, nos posicionamos con el cursor sobre una de ellas, yo lo hago sobre "Crackme!" que es el título de la ventana, dos clicks Izquierdos de ratón y aparecemos en la address "0040406F"



si observamos atentamente:

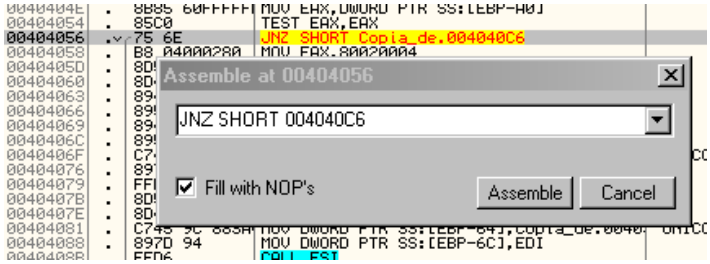


Vemos más abajo, en la address "00404081" la referencia "Cracker??", y todavía un poco más abajo en la address "0040409F" un "rtcMsgBox"
Y si miramos más arriba vemos en la address "00404056" el salto condicional JNZ (Salta si no es 0) donde se decide en este caso si el valor del registro EAX no es 0, saltará a la address "004040C6" para continuar hasta mostrarnos la ventana:

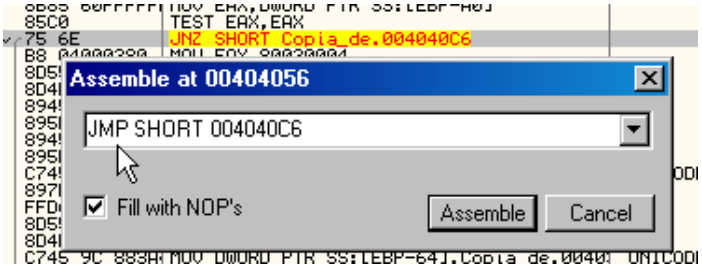
Si por el contrario el valor de EAX es 0 , continua hasta mostrarnos la ventana:

Pues voy a substituir el saldo condicional JNZ por un salto incondicional JMP para que siempre salte a la address "004040C6"

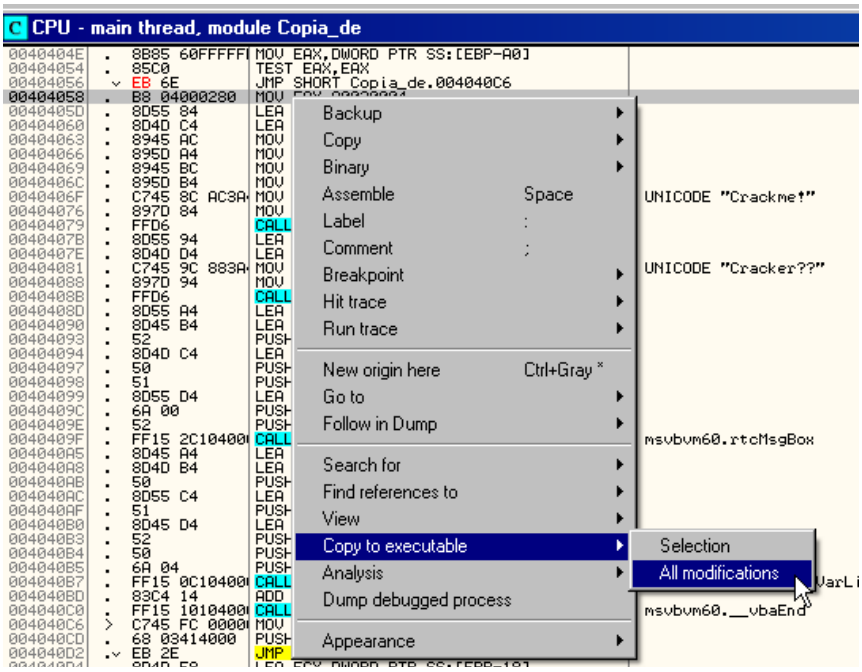
Osea esto



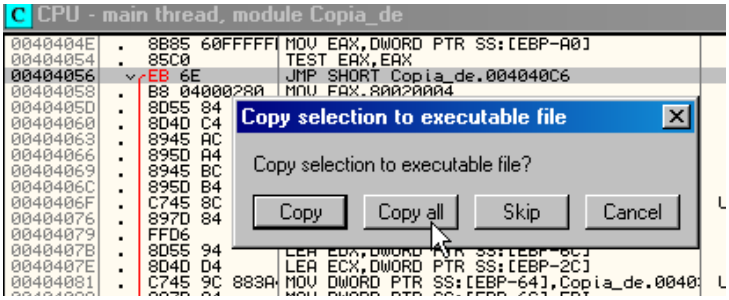
Por esto



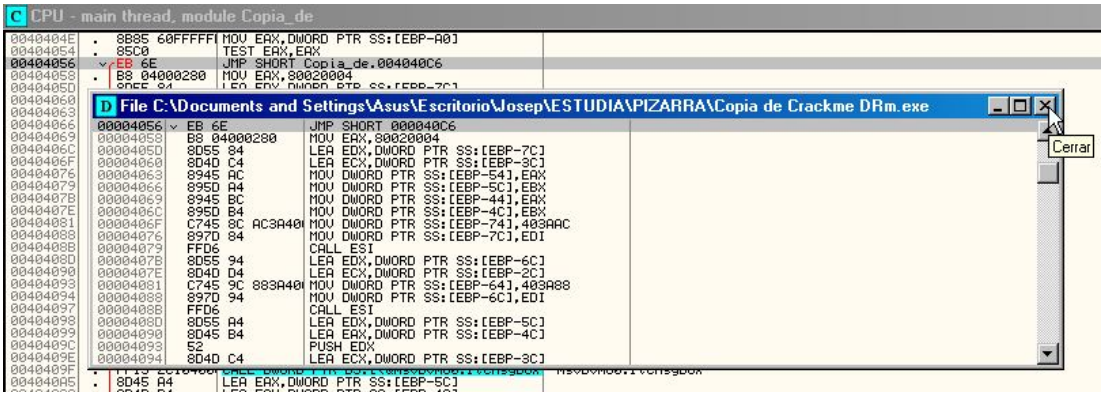
Le doy a “Assemble”, guardo cambios



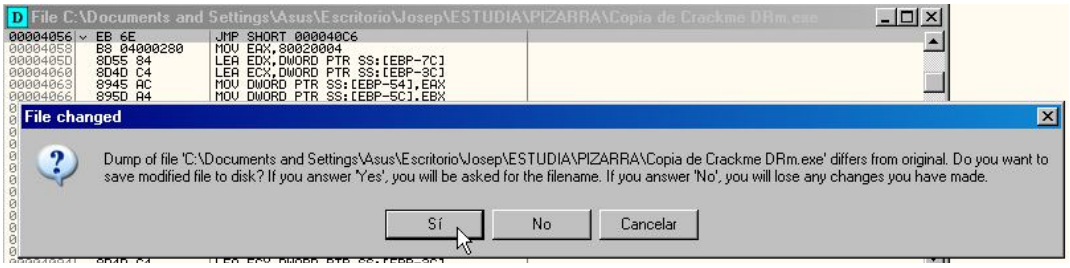
Le doy a “Copy all”



Después cierro la ventana donde me muestra los cambios



Olly me avisa de que los cambios difieren del .exe original, y que si quiero guardarlos, y le decimos que "Sí"



Por último lo guardamos con otro nombre, yo le pongo "Copia de Crackme DRm_1.exe"

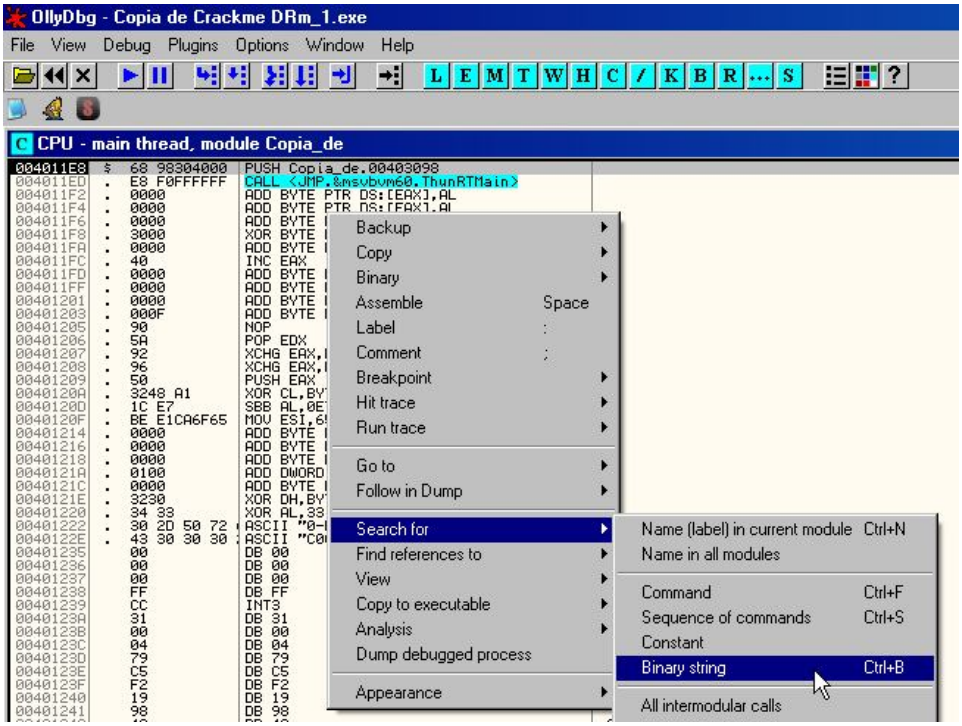
Salimos totalmente de Olly (Si queremos antes de salir ya podemos desactivar nuestro Plugin IsDebuggerPresent por que ya ha hecho su trabajo), comprobamos que el nuevo "Copia de Crackme DRm_1.exe" se ejecuta correctamente fuera de Olly sin la Nag del principio, y vemos que sí.

Ahora lo cargamos con Olly, lo hacemos correr y también nos sale lo mismo, o sea que con el salto incondicional hemos conseguido sortear el IsDebuggerPresent (que todavía está vivo dentro de las entrañas del crackme), ya que al pasar por el JMP siempre irá al mismo lugar de destino, y con ello solucionado nuestra primera misión de que la Nag no salte y de paso a la segunda ventana cuando corremos el crackme, tanto dentro como fuera de Olly.

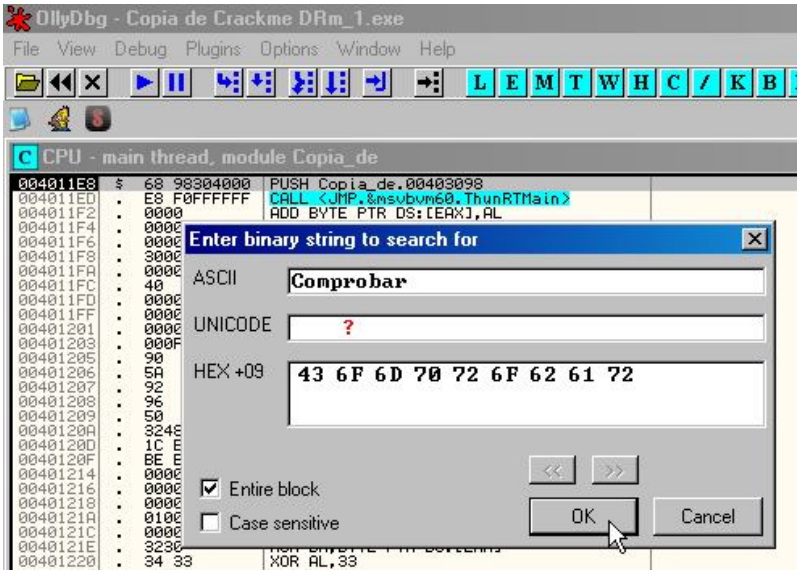
continuamos….

SEGUNDA MISIÓN: debemos activar el button "Comprobar"

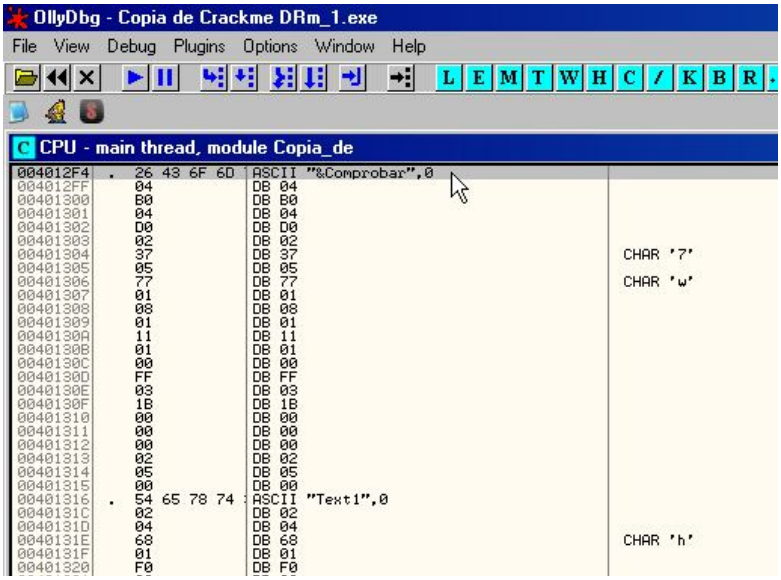
Cargamos de nuevo nuestro crackme modificado al que hemos llamado "Copia de Crackme DRm_1.exe" con Olly



Vamos ahora a *Activar el button "Comprobar", y sin ejecutar nada, en la ventana principal de Olly damos clic derecho "Search for - Binary string" y en la caja de texto "ASCII" tipeamos "Comprobar" (que es el Caption del Button que buscamos), damos "OK"*



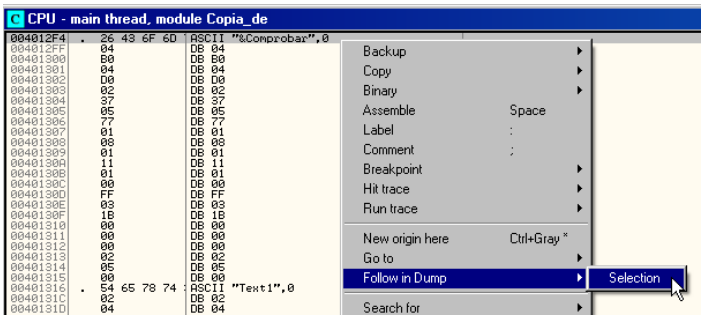
Y aparecemos en la address "004012F4"



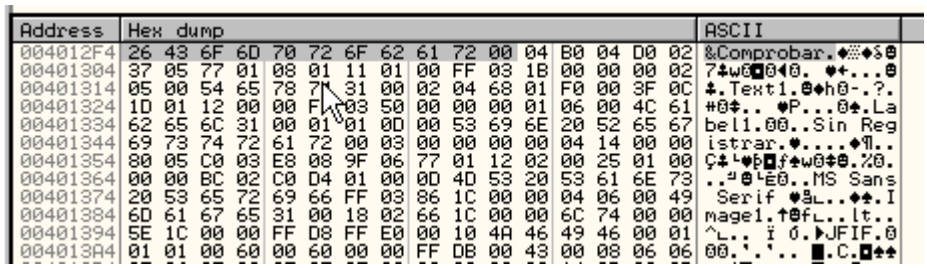
Si le damos a las teclas "Ctrl+L" para que Olly siga buscando, no encuentra nada más.

Aquí deberíamos observar los recursos que conforman el button "Comprobar", los bytes 00 significan desactivado = False i los bytes 01 activado = True, nuestro trabajo consiste en encontrar y modificar el 00 por 01 correcto para activar el button posicionándonos sobre el, y dando Clic derecho "Binary – Edit" guardado cambios cada vez, y probando uno a uno, (Normalmente suele ser el de la posición 11 contando hacia abajo) pero esta posición ya está en 01), también he probado con las demás y la cosa no funciona.

También si nos posicionamos sobre la address "004012F4 "&Comprobar" y le damos clic derecho "Follow in Dump – Selection"



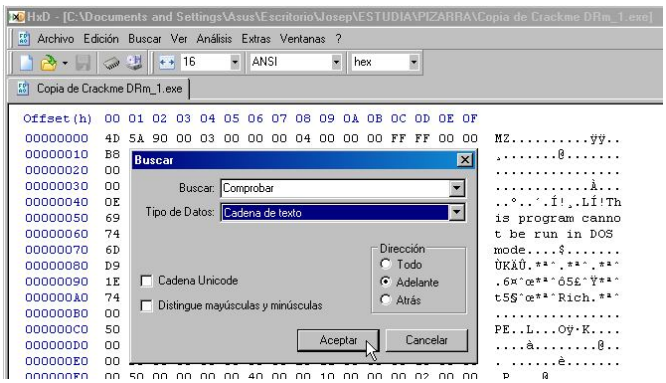
En la ventana "Hex dump" nos muestra la equivalencia de cada carácter de la palabra "Comprobar" en Hexadecimal seguido de los recursos que conforman este button



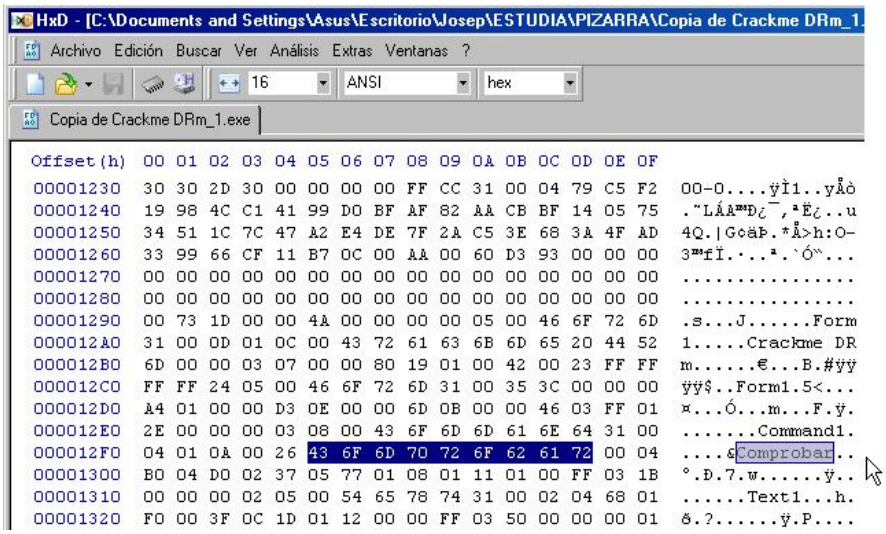
I si hacemos "scroll" con las flechas arriba y abajo tampoco vemos nada interesante.

Pues ahora que hacemos……

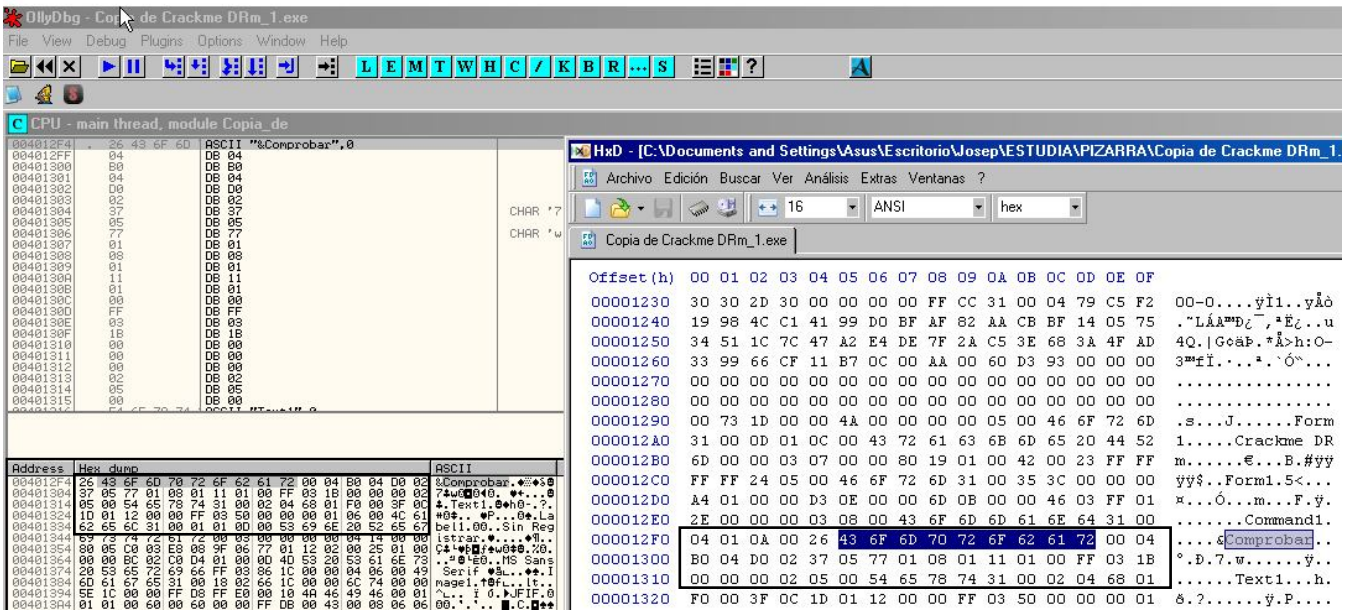
Salimos de Olly y vamos a abrir nuestro crackme modificado "Copia de Crackme DRm_1.exe" con la tool "HxD Editor Hexadecimal" y tipeamos dentro de la caja de texto "Buscar" la palabra "Comprobar", y desplegamos en la segunda caja de texto "Tipo de datos" para que busque como "Cadena de datos"



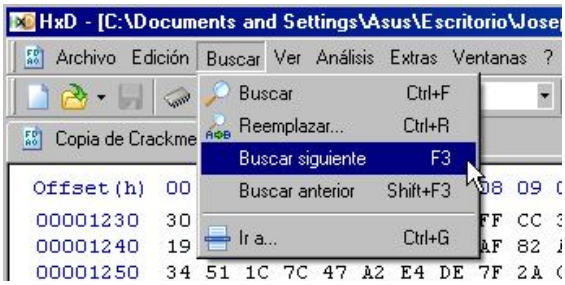
Le damos a "Aceptar" y aparecemos en



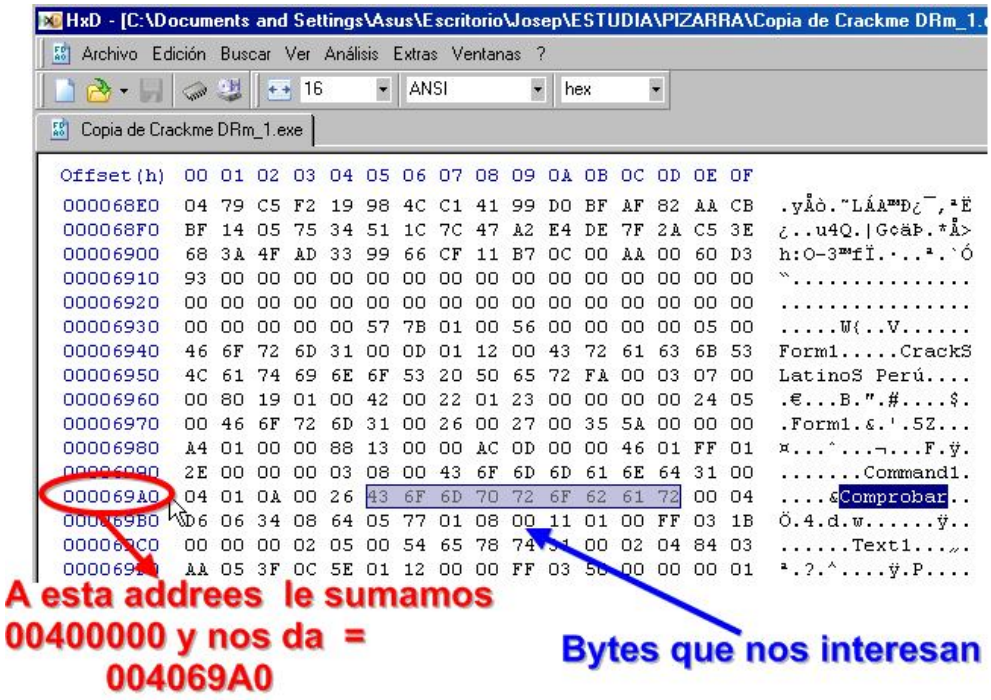
Que si recordamos (He sobrepuesto las dos imágenes para que se vea mejor) son exactamente los mismos valores hexadecimales que obtuvimos con Olly en la ventana "Dump"



Continuamos con la tool HxE, y vamos a ver si encuentra alguna otra cadena de texto con la misma referencia "Comprobar" dándole a la tecla "F3"



Y efectivamente encuentra otra. (que Olly no encontró). Ahora estamos parados aquí:



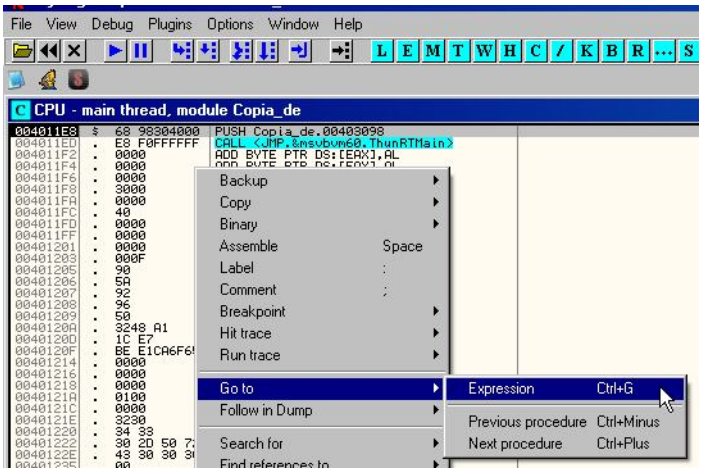
Creo que ahora si que estamos en el sitio adecuado para cambiar los recursos que conforman el button "Comprobar" y que Olly no nos mostraba. (Si continuamos buscando más referencias con la tecla "F3", el HxD nos dice que no hay más.

En este caso nuestra intuición de cracker nos dice que los Bytes que nos interesa cambiar están en la posición 12 después de la cadena de texto "Comprobar" de esta segunda parada, recordemos que OO=False=Desactivado y que 01=True=Activado, y yo había dicho que normalmente estaban en la posición 11 (pido disculpas, esta vez me he equivocado de una je.je.je.., pero normalmente están por estas posiciones).

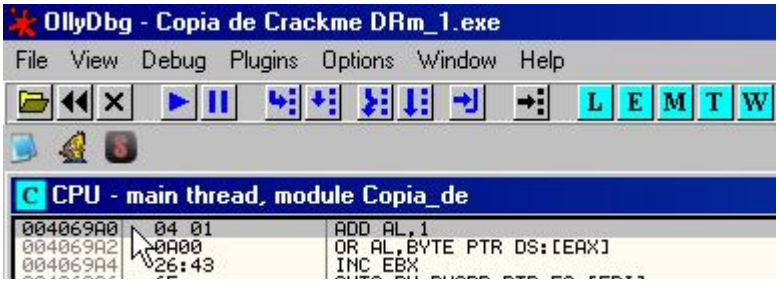
Bien, ahora podríamos cambiar directamente el valor hexadecimal 00 por 01 con este magnífico editor hexadecimal y guardar los cambios, pero vamos a intentarlo hacerlo con nuestro Olly.

Apuntamos la address "000069A0" que es la segunda parada obtenida con el HxD al buscar la cadena de texto "Comprobar", le sumamos el "ImageBase" del crackme que en este caso es "00400000" dándonos como resultado = "004069A0", lo anotamos y salimos del HxD (recordemos que no hemos hecho ningún cambio con esta tool).

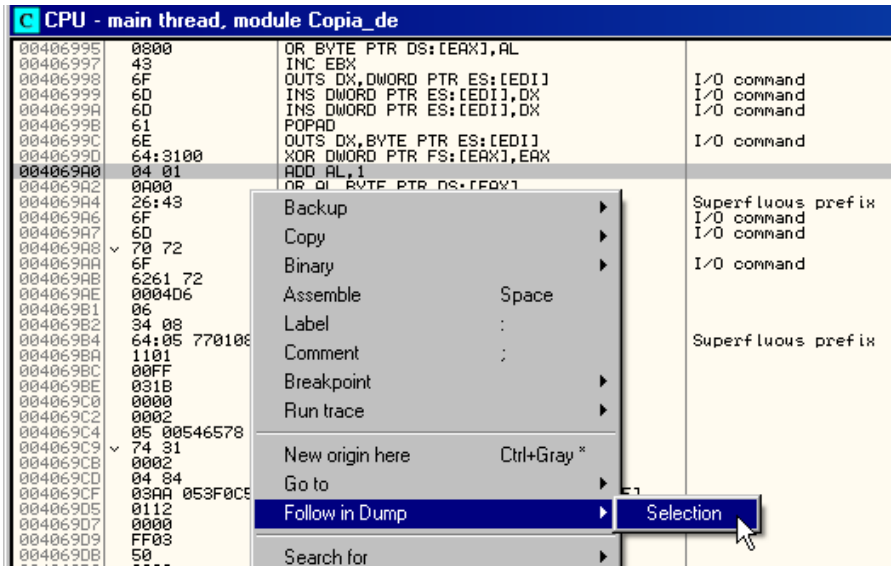
Cargamos nuestro "Copia de Crackme DRm_1.exe" de nuevo con Olly y sin ejecutar nada, parados en el punto de entrada, damos click derecho "Goto to" , "Expresión " e introducimos el resultado del cálculo de la address que realizamos anteriormente "004069A0" para que Olly la busque



Damos "OK", y aparecemos en

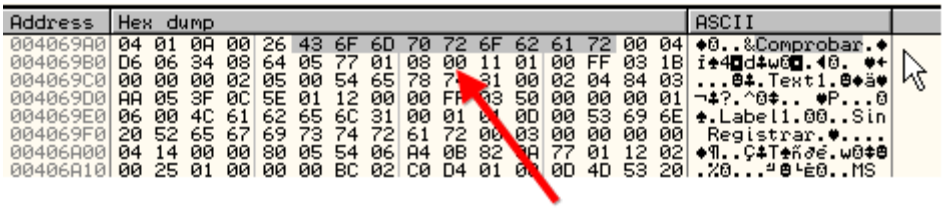


Nos posicionamos encima con el cursor, clic derecho y "Follow in Dump" – "Selecction" para que nos muestre en la ventana "Dump" lo que lleva dentro

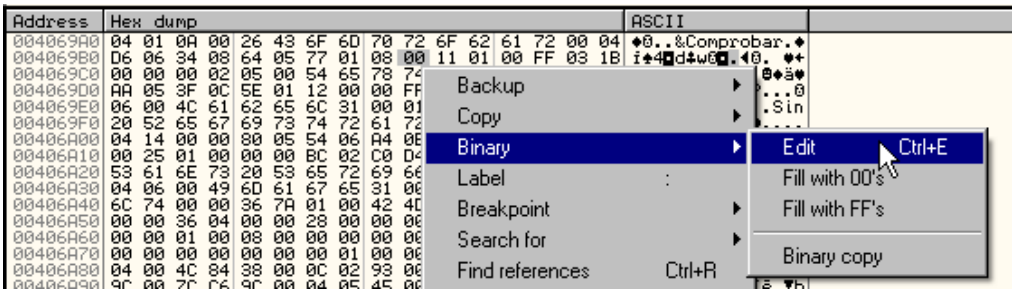


Ahora nos fijamos en la ventana "Dump", Olly nos muestra lo que estabamos buscando, que es exactamenete lo que nos mostró el Editor Hexadecimal HxE en su

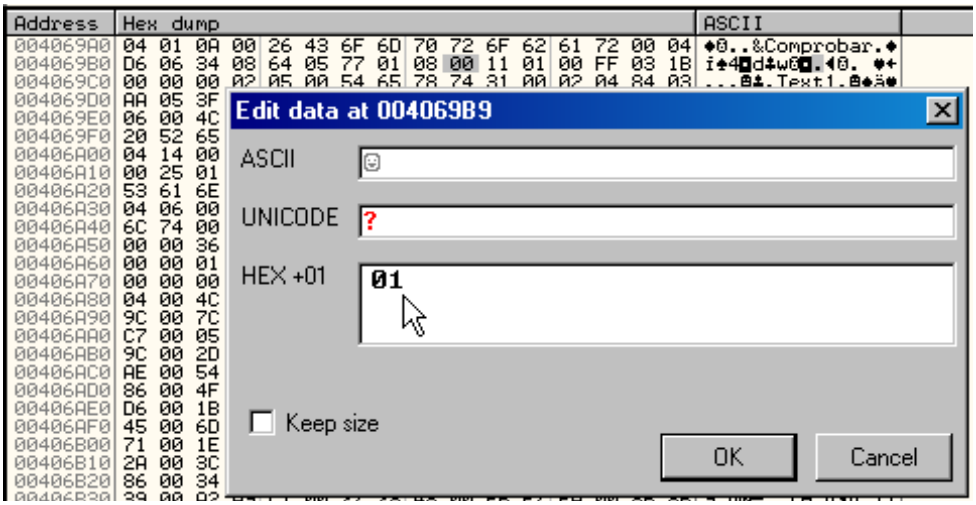
segunda parada de búsqueda, nos posicionamos marcando el texto entero "Comprobar" con el ratón, y en la posición número 12 tenemos los bytes que debemos cambiar.



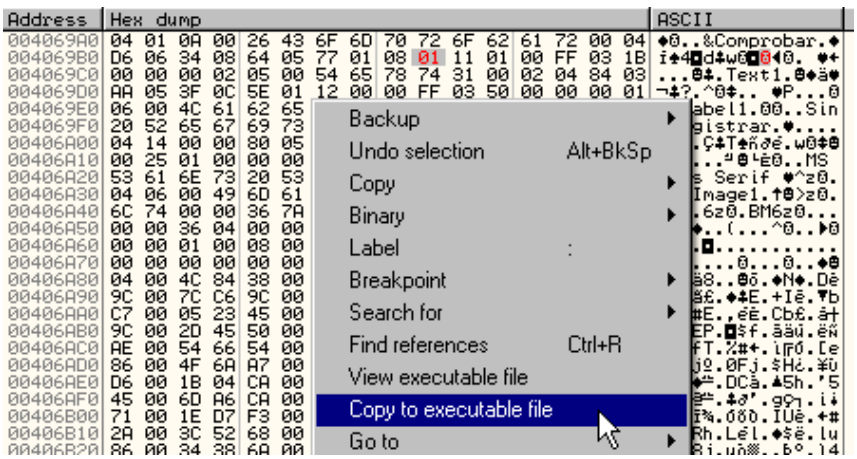
Nos posicionamos sobre este Byte "00", clic derecho de ratón y "Binary" – "Edit"



Y cambiamos su valor "00" por "01"

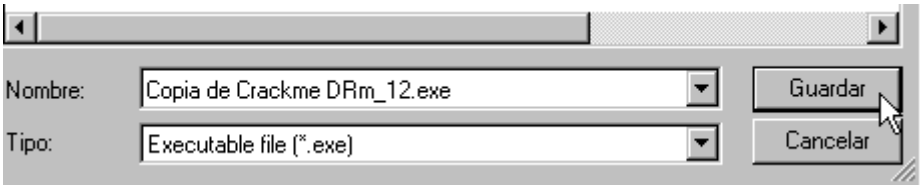


Le damos a "OK". Ahora solo queda guardar los cambios, que deberemos hacerlo posicionados dentro de la misma ventana "Dump", click derecho de ratón "Copy to executable file"



Olly nos mostrará el cambio y le decimos que "Sí"

Le ponemos otro nombre, yo lo he renombrado como "Copia de Crackme DRm_12.exe" y le damos a "Guardar"



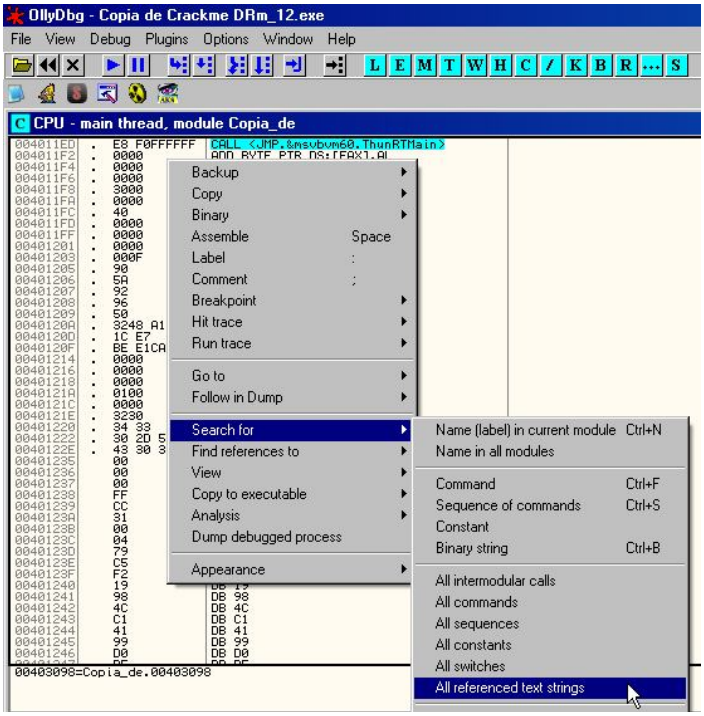
Salimos totalmente de Olly, vamos a buscar nuestro nuevo Crackme por segunda vez modificado, lo ejecutamos y vemos que el button "Comprobar" está activado con lo cual también hemos conseguido nuestra segunda misión.

Y continuamos….

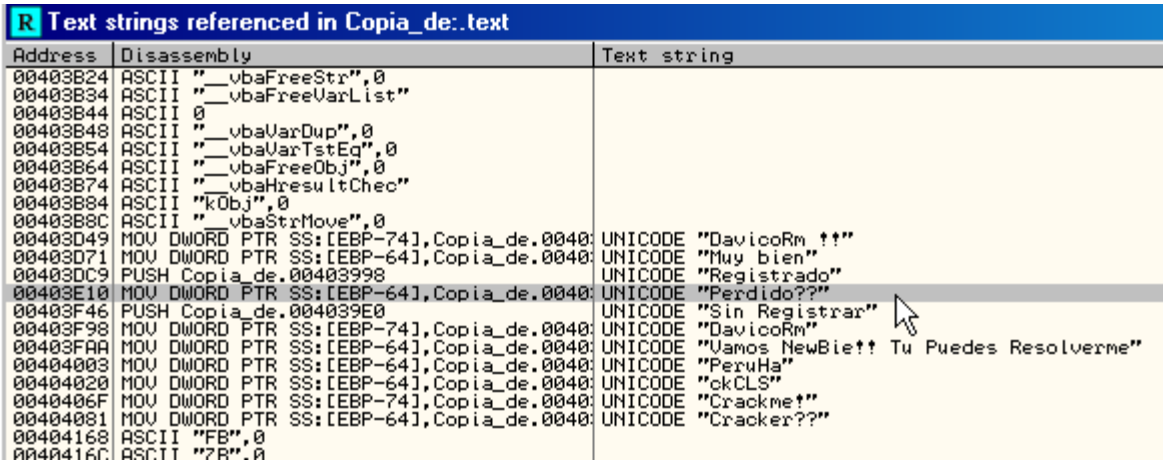
TERCERA MISIÓN: debemos registrarnos.

Abrimos nuestro Crackme ahora llamado "Copia de Crackme DRm_12.exe", le ponemos un pasword cualquiera para registranos, le damos a "Comprobar" y no cuela.
Pero tenemos un dato interesante, y es que nos muestra un espléndido mensaje que nos dice "Perdido??". Si no recuerdo mal, este mensaje de texto también nos lo mostrava Olly al buscar Referències de texto. Vamos a comprobarlo.

Aceptamos, salimos del Crackme, lo abrimos con Olly, buscamos todas las referencias



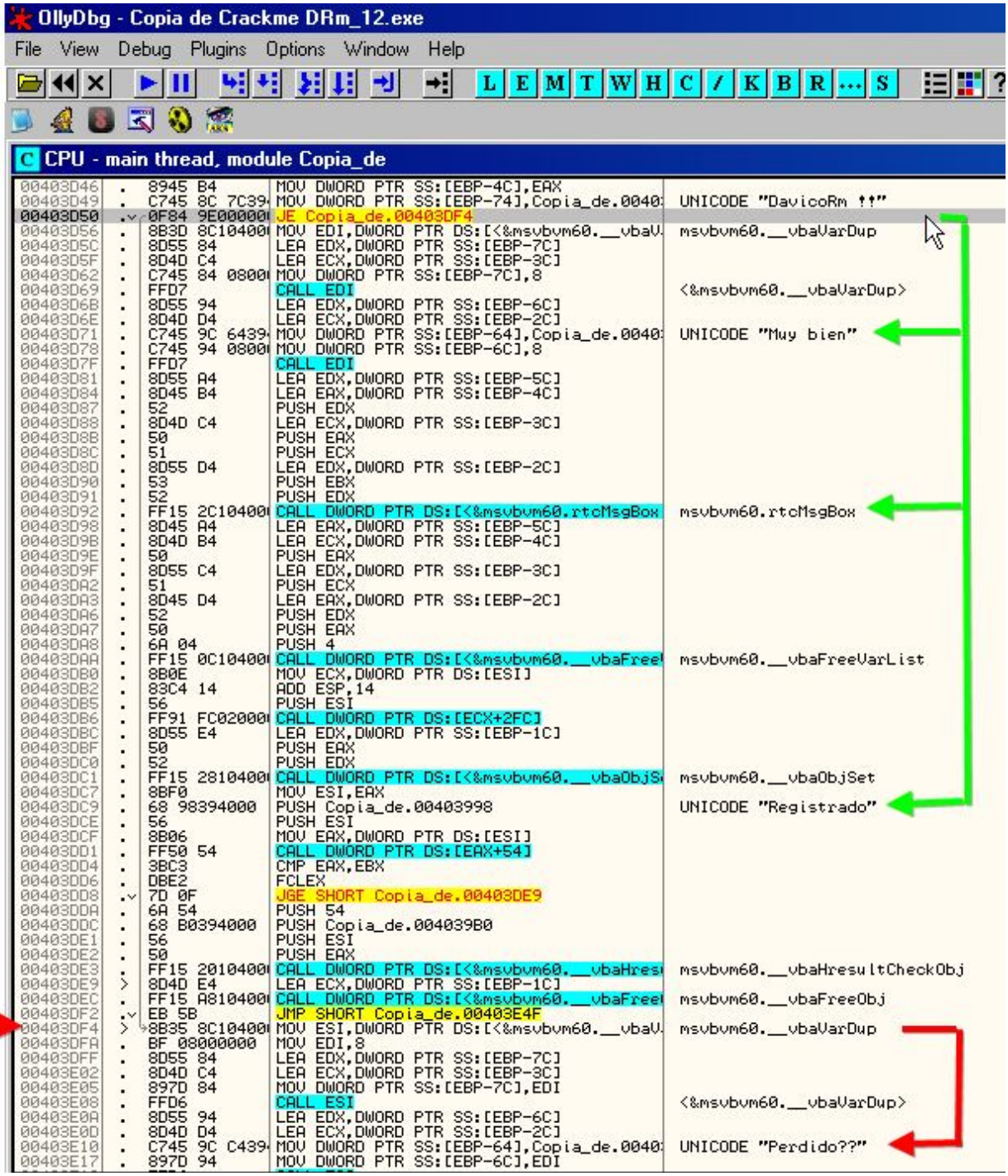
Hacemos "scroll" hacia abajo y efectivamente, aquí la tenemos. Se encuentra en la address "00403E10"



Nos posicionamos sobre ella, damos dos clics de ratón y aparecemos en la ventana principal, ahora si subimos haciendo scroll observamos que estamos en la zona caliente, y vemos el entramado de cómo funciona todo, je.je.je.

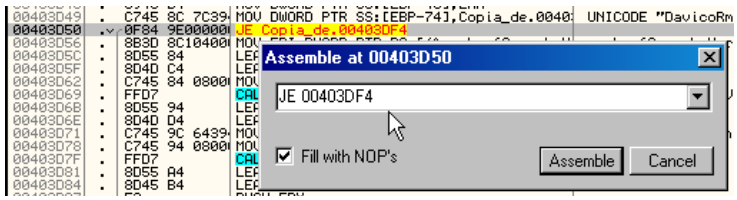
En la address "00403D50" esta el saldo condicional "JE" que decide, que si el password introducido es el correcto, seguirá el código y nos mostrará el mensaje de chico bueno "Muy Bien" y "Registrado".
Si el password introducido no es el correcto, saltará a la address "00403DF4" y mostrará el mensaje de chico malo "Perdido??"

La ruta de Chico malo la he pintado en rojo,
Y la de Chico bueno en verde

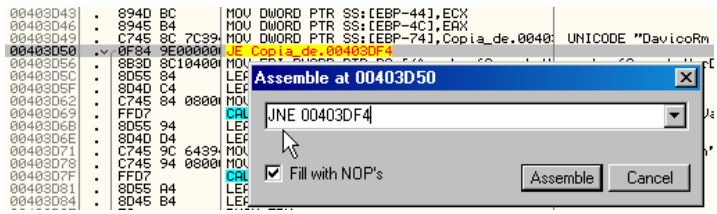


Pues a invertir el saldo condicional JE por un JNE consiguiendo que cualquier password que introduzcamos (menos el correcto), nos registrará y problema solucionado.

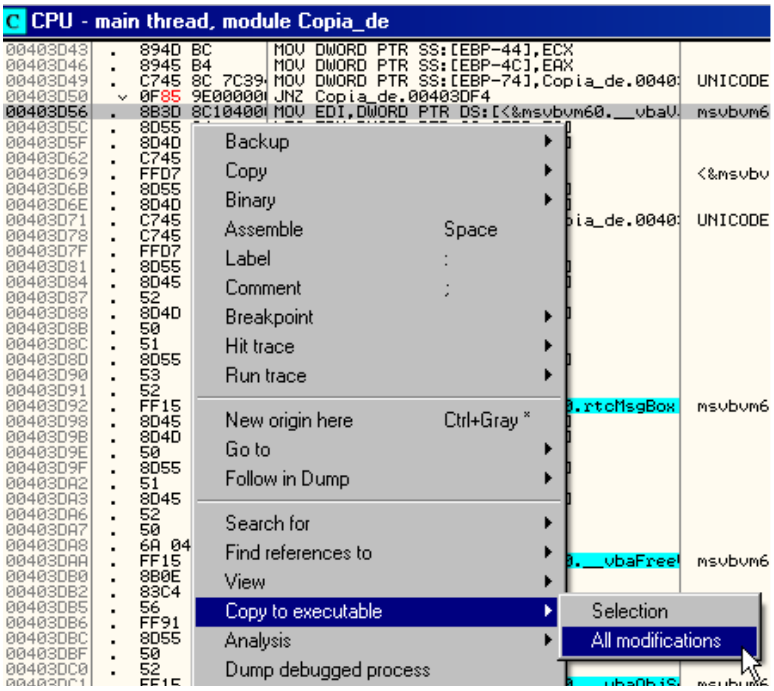
Nos posicionamos sobre el saldo condicional JE, damos dos clics izquierdo de ratón y cambiamos



Por



Le damos a "Assemble", Guardamos cambios "Clic izquierdo "Copy to executable - All modifications - Copy all" y lo guardamos con otro nombre "Copia de Crackme DRm_123"

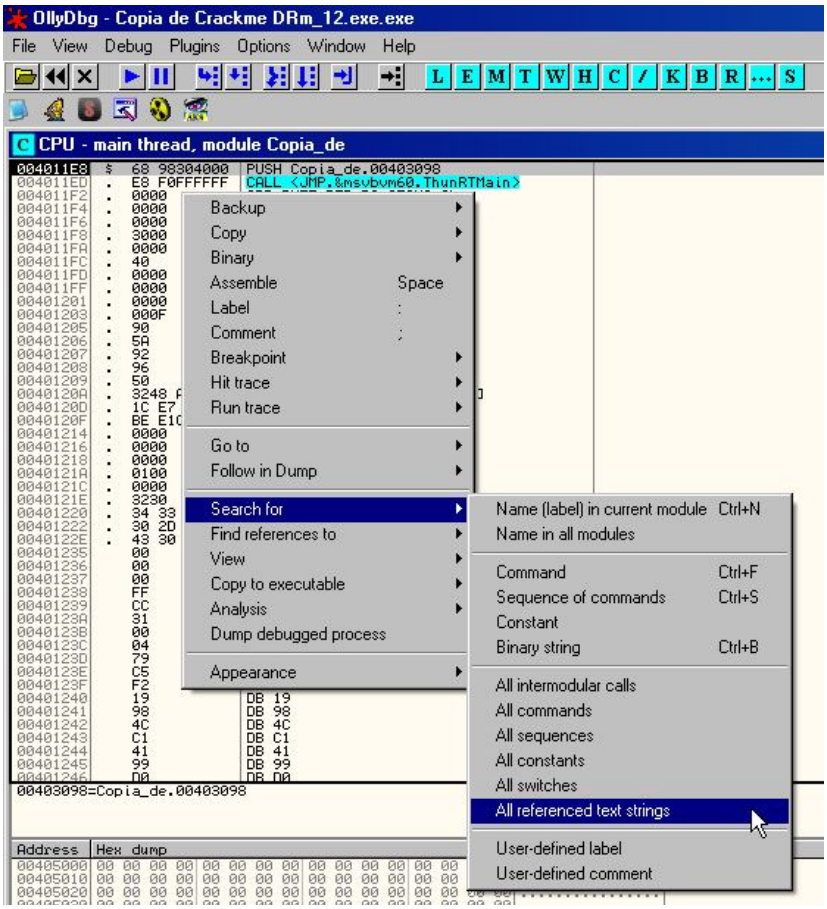


Salimos de Olly, abrimos el nuevo y final crackme modificado por tercera vez al que hemos llamado "Copia de Crackme DRm_123", lo ejecutamos, rellenamos la caja de texto con un password cualquiera, le damos a "Comprobar" y por fin estamos Registrados, con lo cual hemos conseguido nuestra tercera misión.

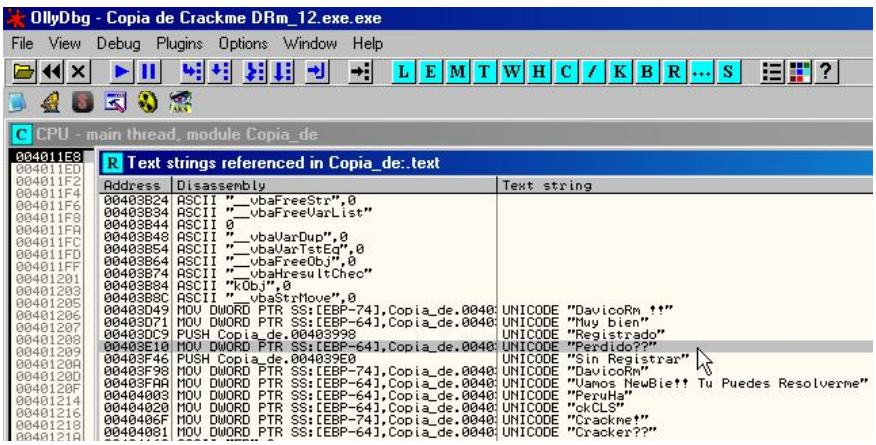
Pero eso, no es todo, ahora vamos a buscar el Pasword correcto. (y este se lo dedico a Ismael Pérez)

Para ello debemos retroceder y cargar en Olly el "Copia de Crackme DRm_12.exe" (Ojo, es el crackme que hemos modificado por segunda vez, al que únicamente hemos burlado la protección antidebbuger y activado el button "Comprobar"), que cuando ponemos un password cualquiera nos sale el mensage de chico malo "Perdido??"

parados en el punto de entrada, buscamos todas las referencias

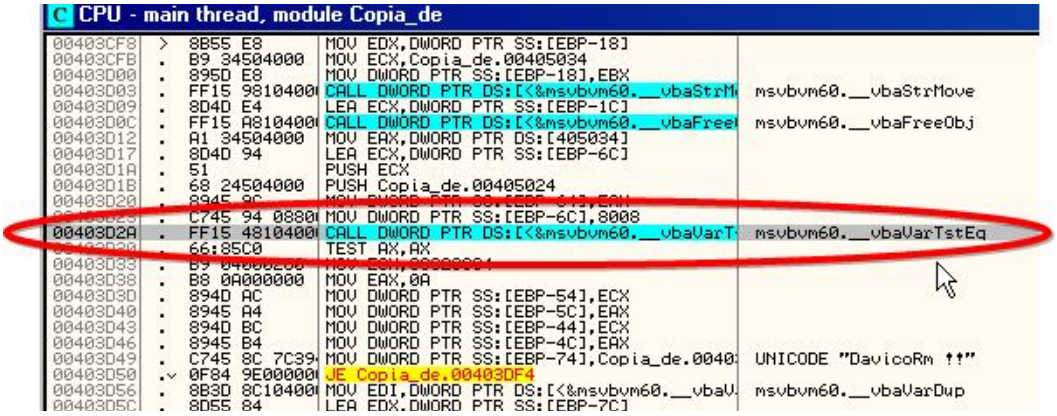


Hacemos "scroll" hacia abajo y aquí la tenemos. Se encuentra en la address "00403E10"

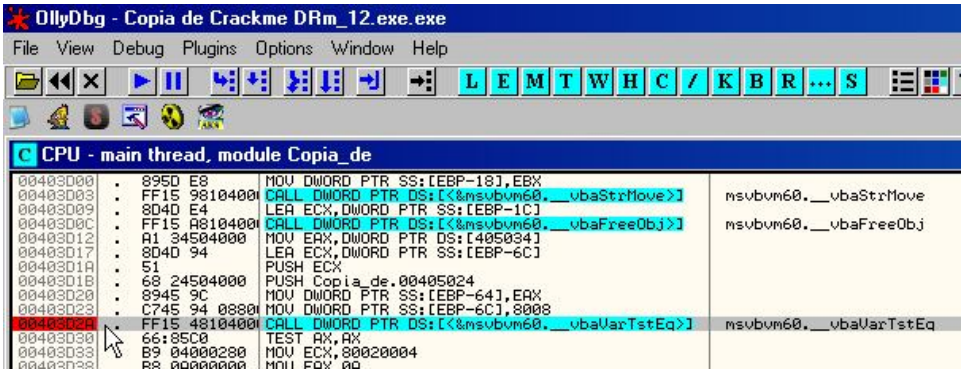


Nos posicionamos sobre ella, damos dos clics de ratón y aparecemos en la ventana principal, ahora si subimos haciendo scroll nos paramos en la address "00403D2A" que es la primera "CALL" que hay antes de llegar a la address "00403D50" donde se encuentra el saldo condicional "JE" que decide, si el password introducido es el correcto, seguirá el código y nos mostrará el mensaje de chico bueno "Muy Bien" y "Registrado" y si el password introducido no es el correcto, saltará a la address "00403DF4" y mostrará el mensaje de chico malo "Perdido??"

Además en la información de esta "CALL", Olly tambien nos muestra la APIs "__vbaVarTstEq" (que sirve para comparar cadenas), y esto es interesantísimo para nostros, je,je,je

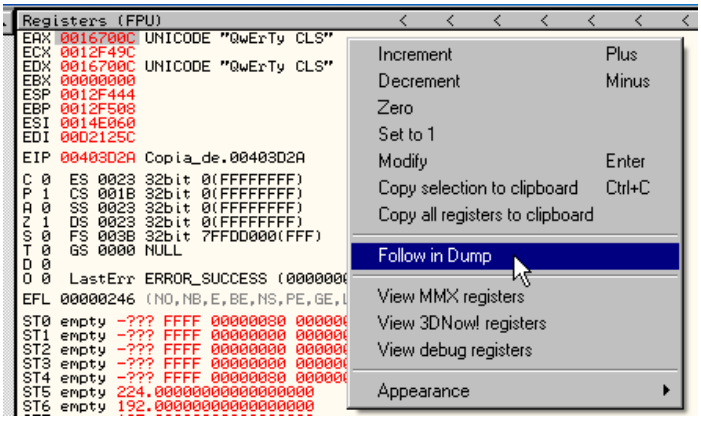


Bien, pues vamos a poner un "Breackpoint Toogle" a esta CALL para que Olly pare aquí cuando corramos el Crackme. Nos posicionamos sobre la "Call", le damos a la tecla "F2", y nos quedará así:

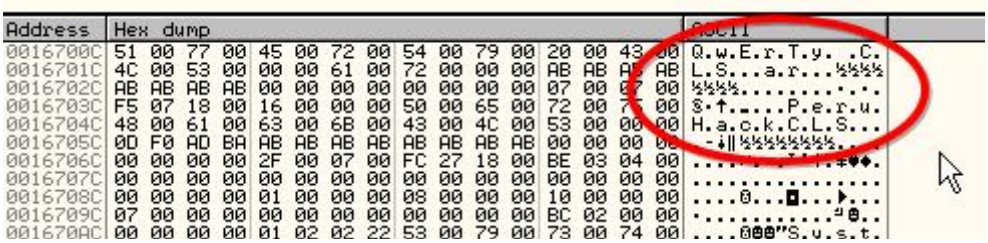


Ahora corremos el crackme, tipeamos en la caja de texto un serial cualquiera

Le damos a "Comprobar" y Olly para en el "Breackpoint", ahora nos vamos a la ventana "Registers" y vemos que en los registros "EAX" y "EDX" aparace nuestro pasword falso que hemos introducido, pues nos posionamos sobre cualquiera de estos dos registros, (yo lo hago sobre EAX", y con clic izquierdo del ratón le damos a "Follow in Dump" para que nos enseñe en el Dump lo que lleva dentro



Por último vamos a la ventana "Dump", y Olly nos muestra la comparación que buscamos Osea nuestro pasword falso introducido y el bueno.



Por lo que el pasword correcto es un magnífico hardcoded "PeruHackCLS"

Salimos de Olly, abrimos nuestro ""Copia de Crackme DRm_12.exe", insertamos el pasword obtenido, le damos a Comprobar y.....

Estamos Registrados.....Yuuuupiiiiii....

Me parece que me he enrollado demasiado y con una cuarta parte de la explicación y capturas de pantalla hubiera sido más que suficiente, pero es que hoy no tenia F1ACA y si muchas ganas de escribir.

A todo el que haya leído este tute quiero que sepa que si me he animado a escribirlo ha sido por la gran persona que hay dentro de "SoftDat Newzombie" por sus amenos e inteligentes videotutoriales que asiduamente comparte con todo el grupo de CLS y en la red compartiendo enseñanza y conocimientos, a "DavicoRm" creador del crackme, como no, al "MAESTRO RICNAR" culpable de que yo me metiera en esto je…je…je…, y a todo el gran grupo de "CLS". …..GRACIAS A TODOS…….AMIGOS

Otro para la colección…….

………MISIÓN CUMPLIDA………

Mis agradecimientos infinitos a
RICARDO NARVAJA, Ratón, Karpoff, _/_-=InDuLgEo=-_/_ ,Makkakko, Raziel , Guan de Dio , RDGMax, SoftDat Newzombie a todo el grupo de Cracks LatinoS
y a todos los crackers del mundo

Que la serenidad nos haga fuertes y tenaces, y no se convierta en somnolencia, plácida aceptación de realidades insatisfactorias pero cómodas, que la paciencia no nos haga cobardes, que el progreso no nos haga autocomplacientes, y que lo logrado hasta ahora no nos haga olvidar que estamos a mitad de camino.

"QwErTy"

11 de septiembre de 2016

-.