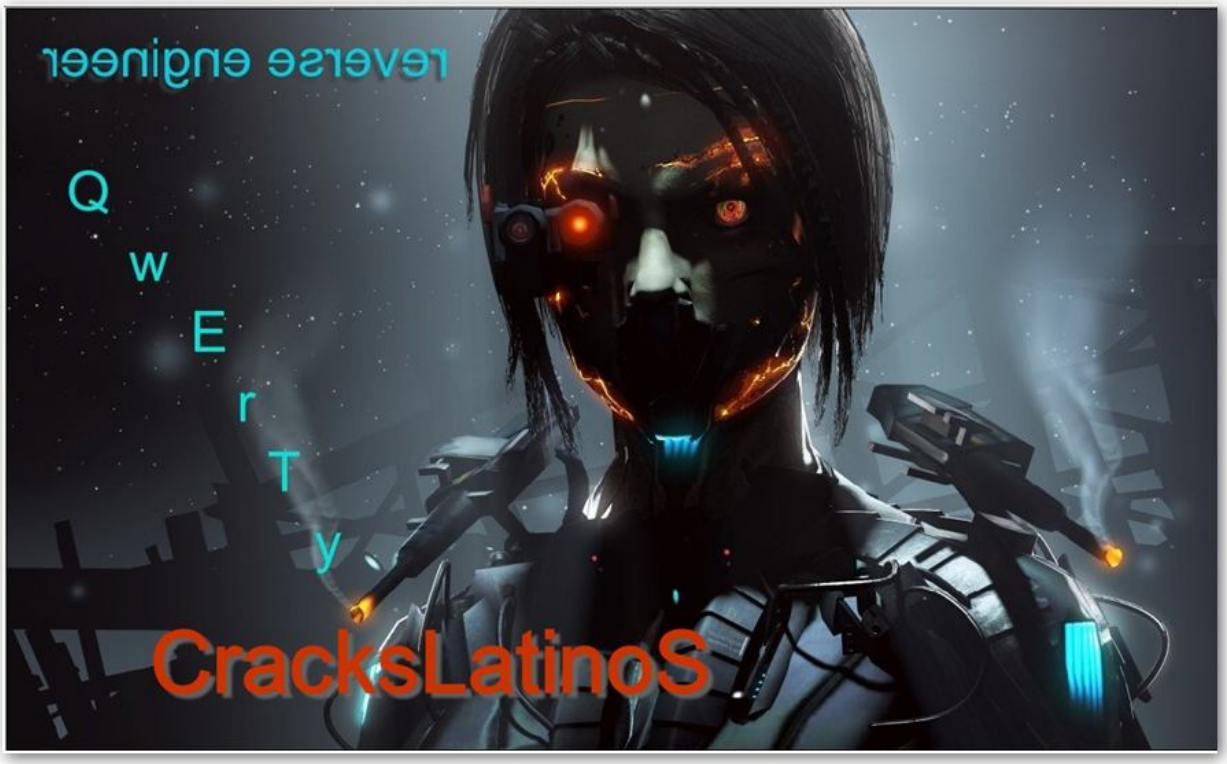
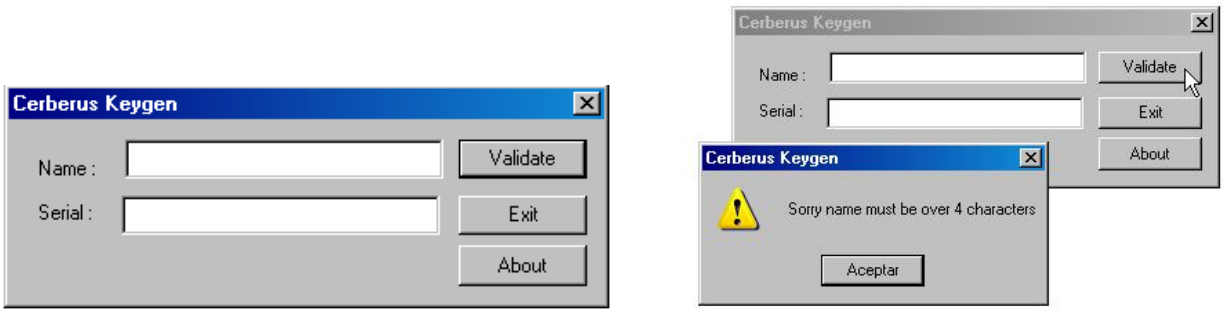


Crackme	Cerberus Keygen
Misión	Buscar Name y Serial Hacer un Selft-Keygen
Compilado	Microsoft Visual C++ ver 5.0/6.0
Protección	Not packed
Herramientas	OllyDbg 1.10 – RDG v0.7.5 - Resource Hacker v4.2.5
Sistema Operativo	Windows Xp SP3
Cracker	QwErTy
Dedicado a	RICNAR - Cerberus - CLS
Link (hay que registrarse)	http://crackmes.de/users/cerberus/keygen/

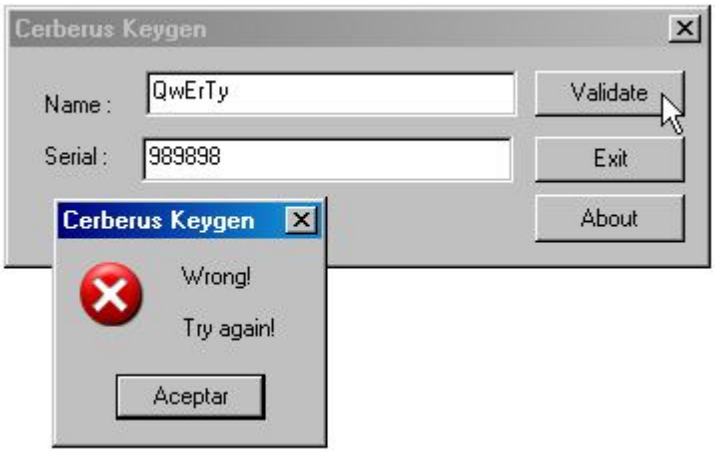
Vaya por delante que para este Crackme es extremadamente facilón encontrar un serial válido, y sabedor que un buen Cracker no es amante de los Selft-Keygen, (a mí me divierten), creo que también es bueno saber que existe esta técnica, por llamarla de alguna manera. He visto otras soluciones en la Web pero no me convencían del todo. Espero que ésta sea del agrado del lector….

ESTUDIANDO LA VÍCTIMA

Hacemos una copia del Crackme, lo ejecutamos y nos pide un Name y un Code para registrarnos. Si le damos directamente a "Validate" nos salta un mensaje que nos dice que el "Name" debe tener más de 4 caracteres.



Aceptamos, rellenamos datos



Le damos a "Validate" y nos salta el mensaje de chico malo.

CONTINUAMOS ESTUDIANDO LA VÍCTIMA

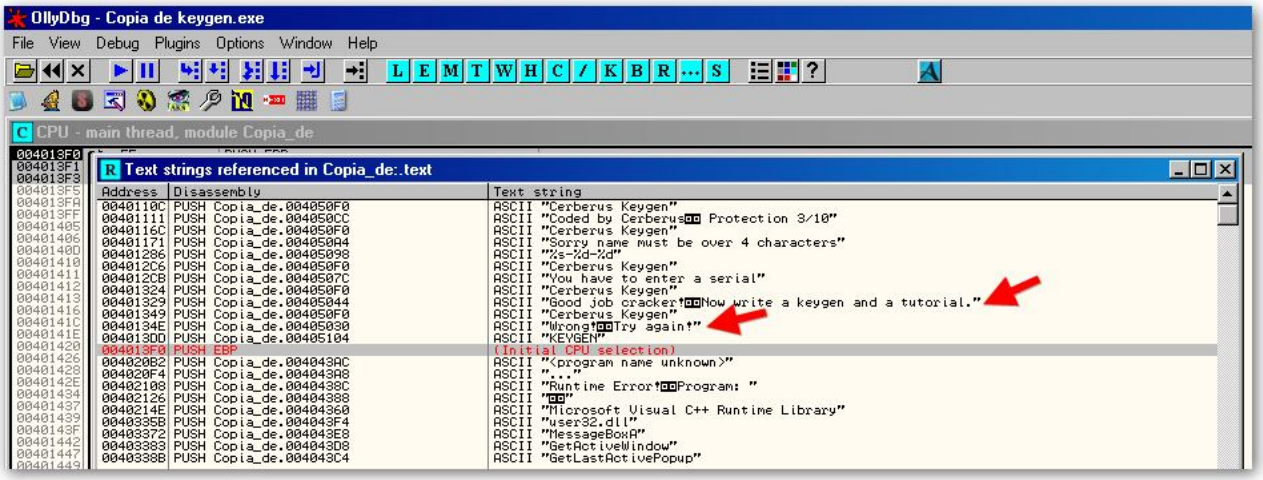
Abrimos el Crackme con el detector "RDG"

y nos dice que está compilado en "Microsoft Visual C++ 6.0" y que no está empacado. Bien

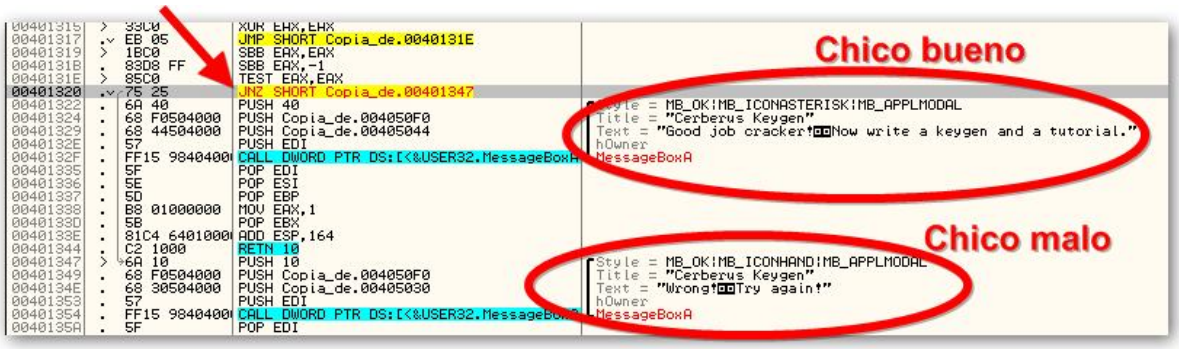
VAMOS A POR ELLA

PRIMERA MISIÓN: Buscar un Name y un Serial

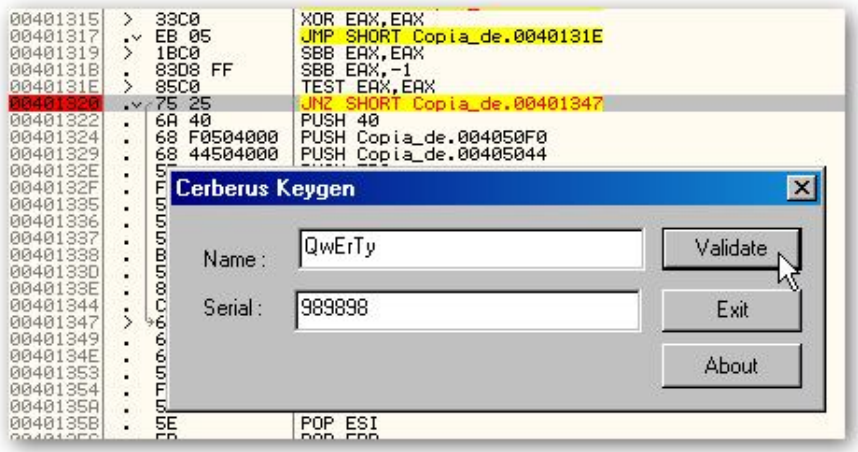
Salimos del "RDG" cargamos el Crackme con Olly, buscamos alguna referencia que nos pueda interesar, y encontramos, entre otras, la de chico bueno, y la de chico malo.



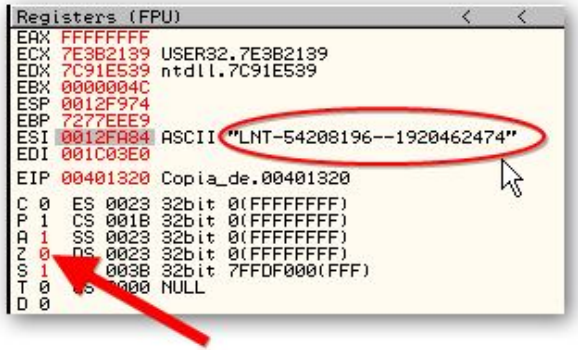
Le damos a cualquiera de las dos y en la ventana del desensamblado aparecemos en la zona caliente, donde vemos los dos "MessageBoxA", un "TEST" y el salto condicional "JNZ" decisivo.



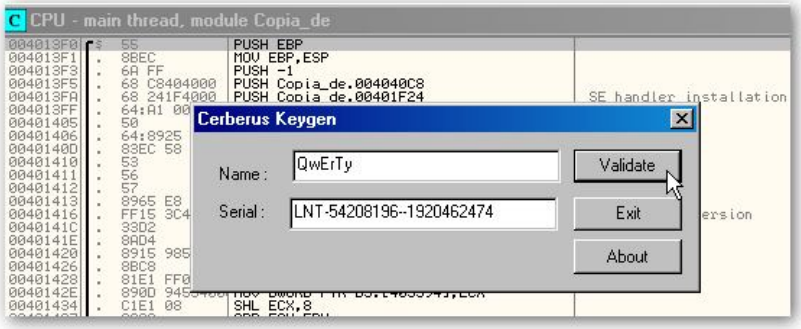
Pues probemos a poner directamente un "Breakpoint" con "F2" a este salto condicional a ver que pasa, je,je,je. Una vez puesto, le damos a "F9" para que corra el Crackme, rellenamos datos



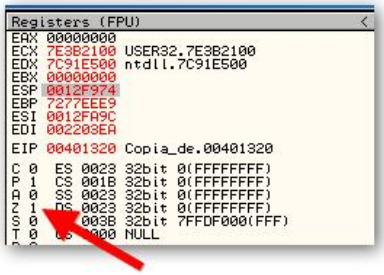
Le damos a "Validate" y en el registro "ESI" aparece un posible "Serial" para nuestro "Name" "LNT-54208196--1920462474". También nos fijamos que al estar el flag "Z" en "0", no se cumplirá la condición del salto y nos mandará a chico malo.



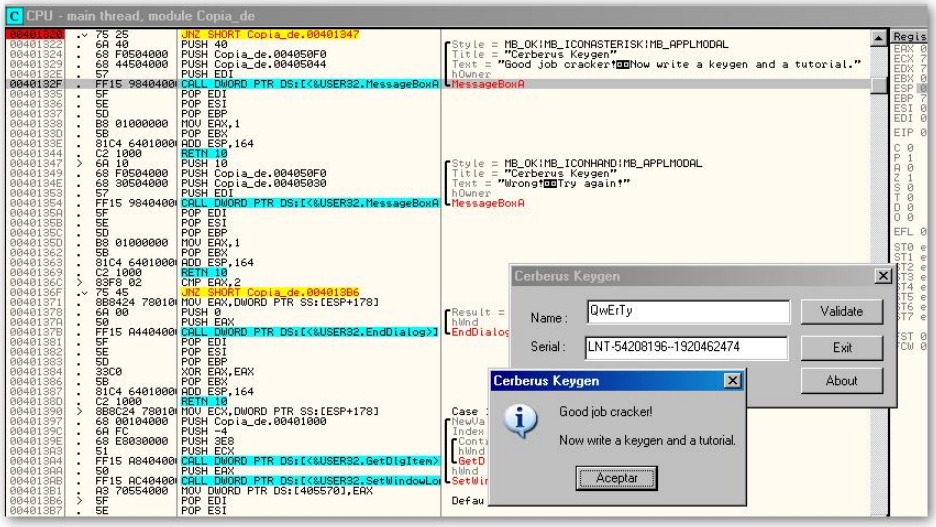
Reiniciamos el Crackme con Olly (tenemos el "BP" puesto en el salto condicional), lo corremos, rellenamos datos, esta vez con el posible serial que obtuvimos anteriormente para nuestro "Name"



Le damos a "Validate" y parados en el "BP", observamos en la ventana "Registers" que ahora el flag "Z" está en "1", y se cumplirá la condición del salto que nos mandará a chico bueno.



Seguimos traceando, y efectivamente nos salta el mensaje de felicitación



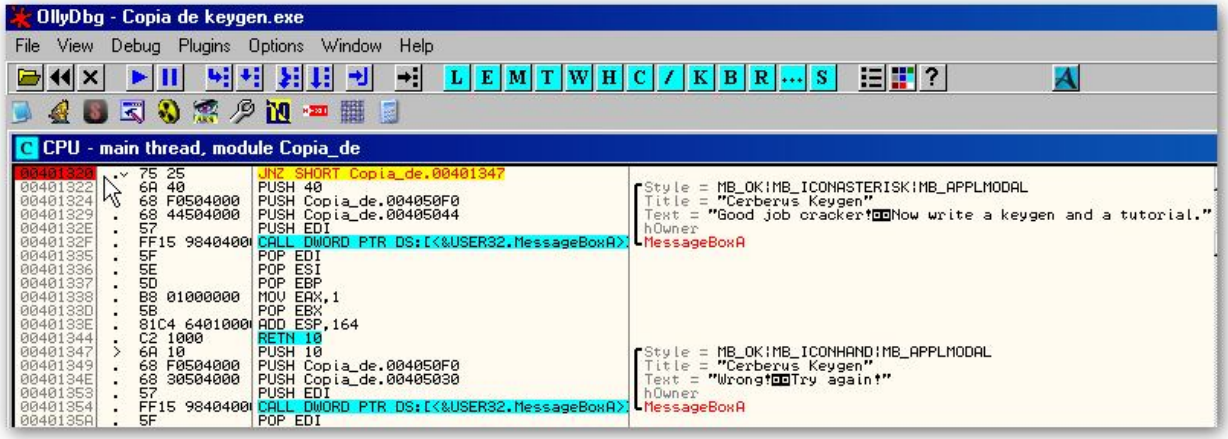
Dando con ello nuestra primera misión por finaliza.

SEGUNDA MISIÓN: Vamos a hacer un Selft-Keygen (generador de llaves con la misma víctima)

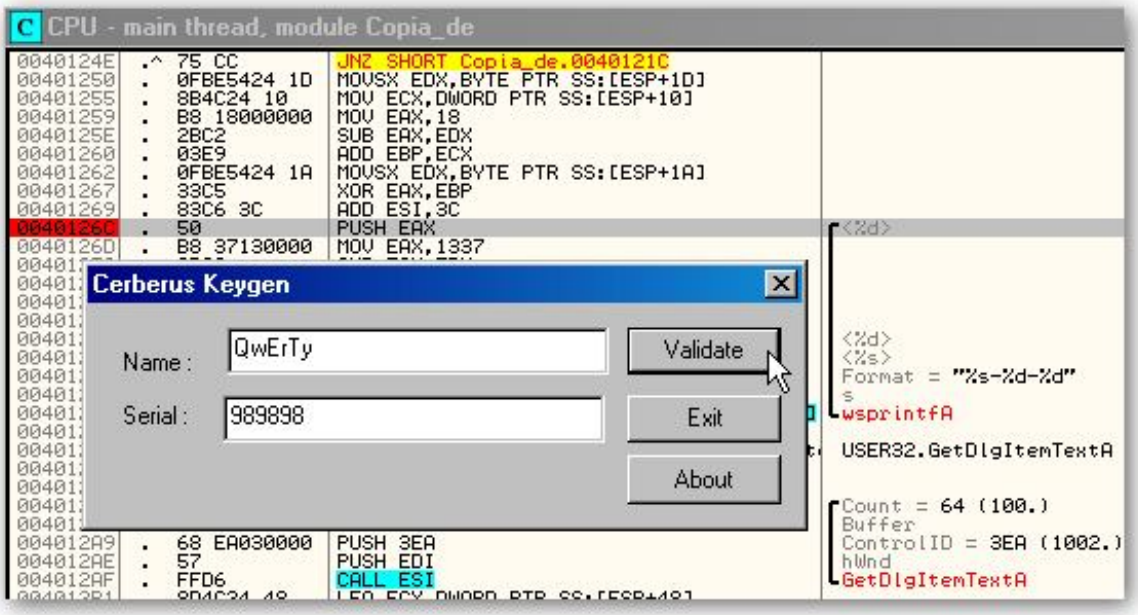
Para ello utilizaremos la APIs "User32.SetDlgItemTextA". Esta función envía un mensaje "WM_SETTEXT" al control especificado, y también establece el título o texto de un control en un cuadro de diálogo.
Debemos saber que para que esta APIs funcione, necesitamos el "handle de la ventana", el "ID de la caja de texto" y la "String a mostrar".

Pues vamos a buscar todos estos datos.

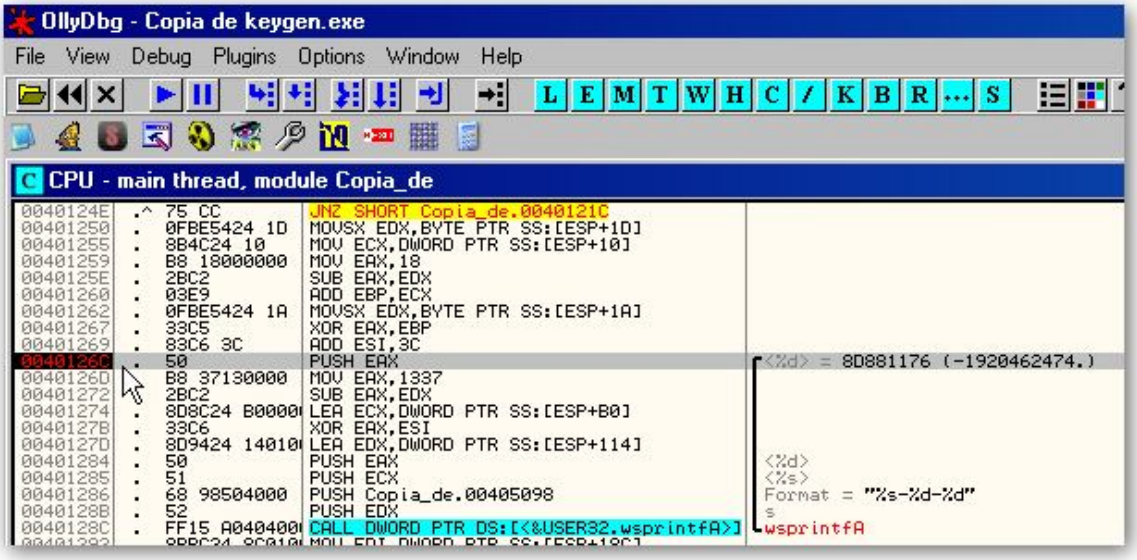
Reiniciamos el Crackme con Olly, y nos vamos directamente a la address "00401320" donde tenenos el "Breakpoint"



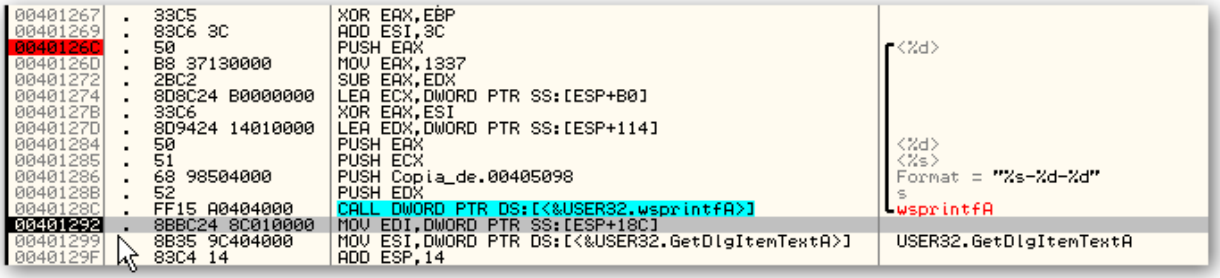
Subimos haciendo "scroll" hasta "0040126C", y le ponemos otro Breakpoint con "F2", corremos el Crackme, rellenamos datos



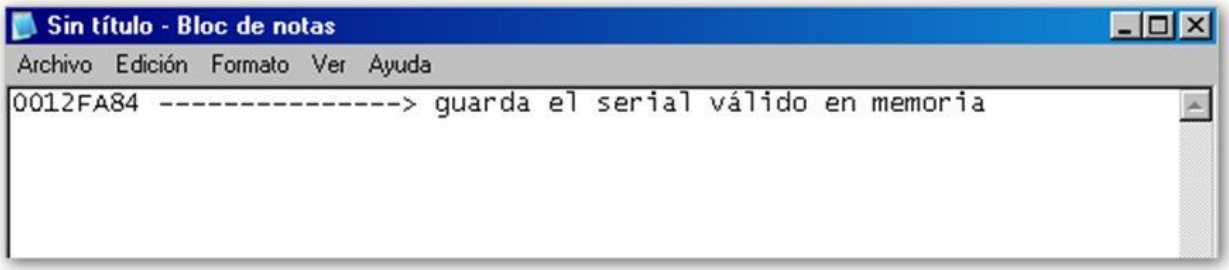
Le damos a "Validate" y Olly para en nuestro "BP".



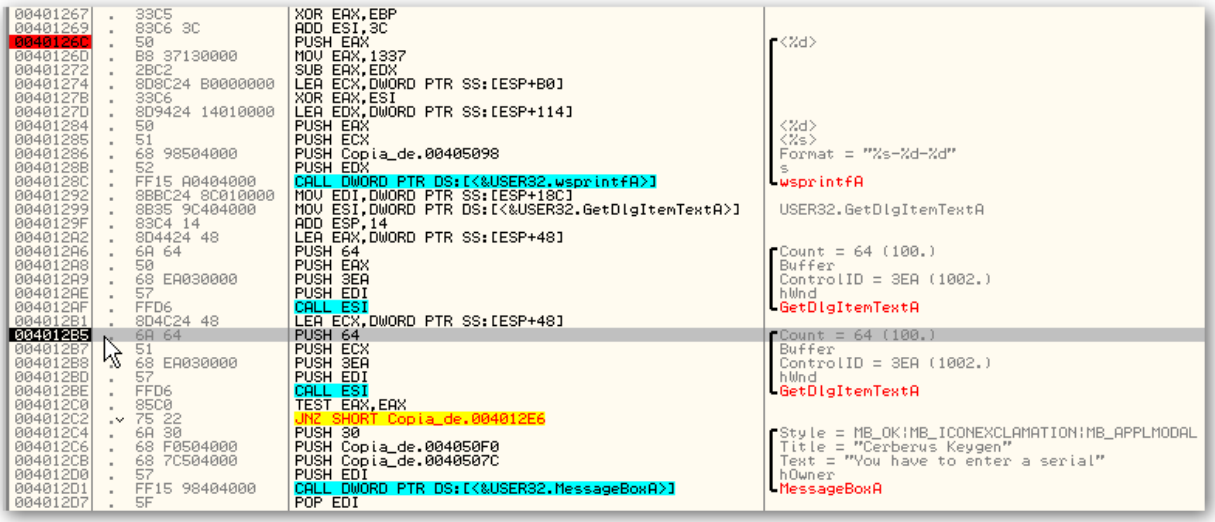
Ahora vamos traceando con "F8" hasta llegar a la address "00401292", y aquí parados, en la ventana "Stack" vemos el Serial válido

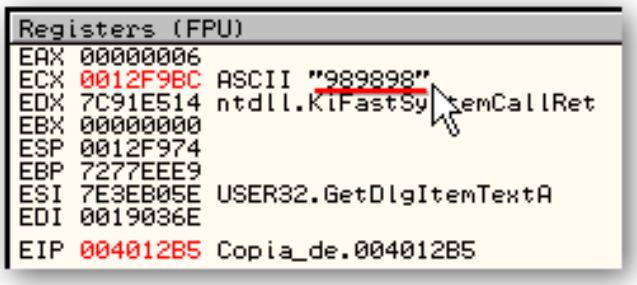


Bien, ya tenemos nuestro primer dato que buscamos, nos quedamos con "0012FA84" que es uno de los lugares donde guarda el serial válido en memoria, y lo apuntamos en un "Notepad"



Continuamos traceando hasta la address "004012B5", y en la ventana "Registers" aparece nuestro Serial falso

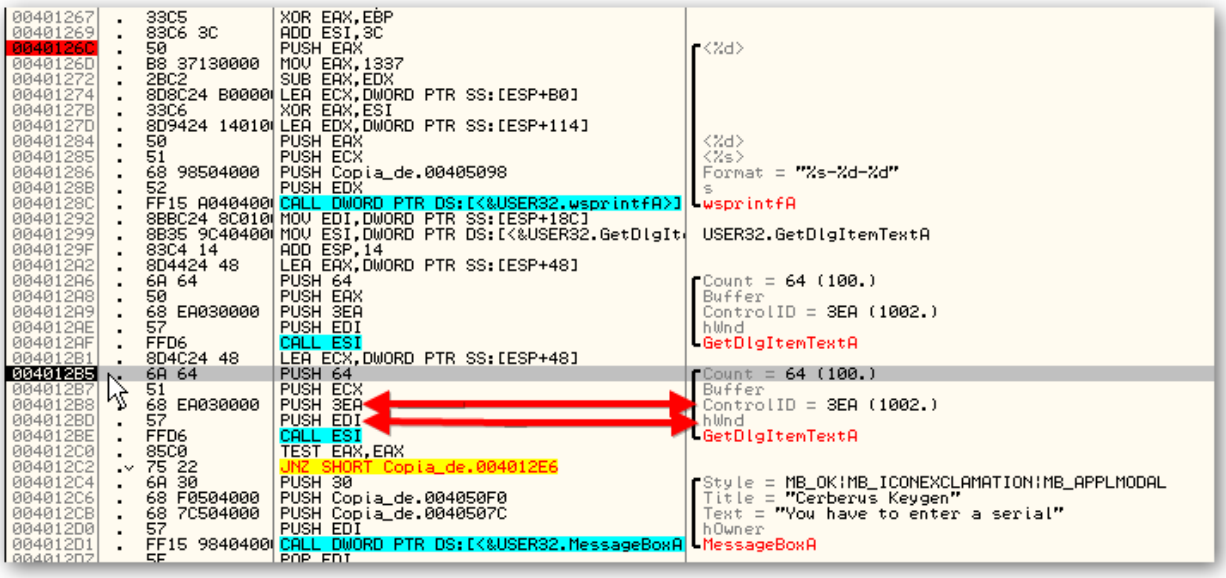




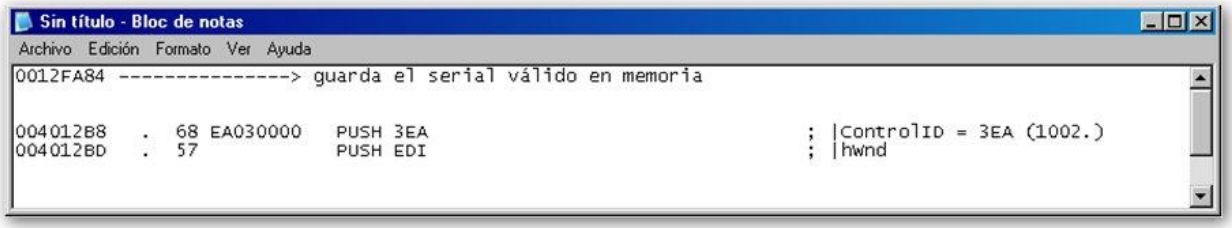
Con este detalle, intuimos que estamos en la parte de código correcto, y de que también estamos dentro del evento que nos interesa para nuestro propósito, donde deberemos modificar la instrucción para que en la caja de texto nos muestre el serial válido en lugar de leer el falso.

También hemos encontrado dentro del evento los demás datos que nos faltaban, o sea el Control "ID" y el "handle", que también los apuntaremos en el "Notepad":

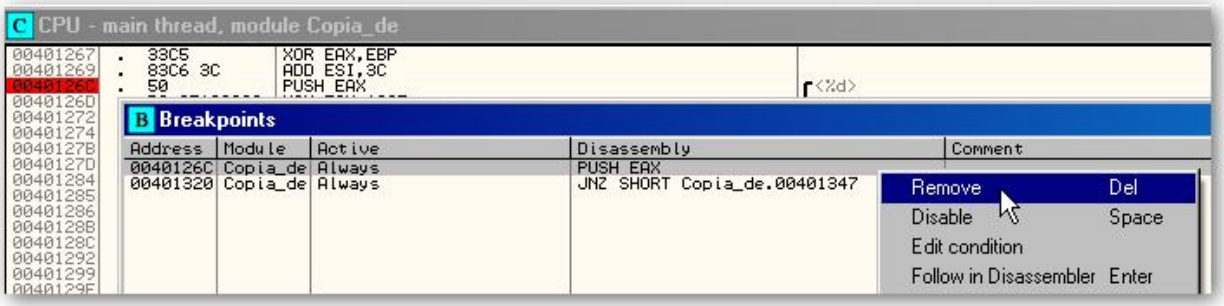
El Control "ID" de la caja de texto, es "PUSH 3EA" y el "handle" de la ventana, es "PUSH EDI".



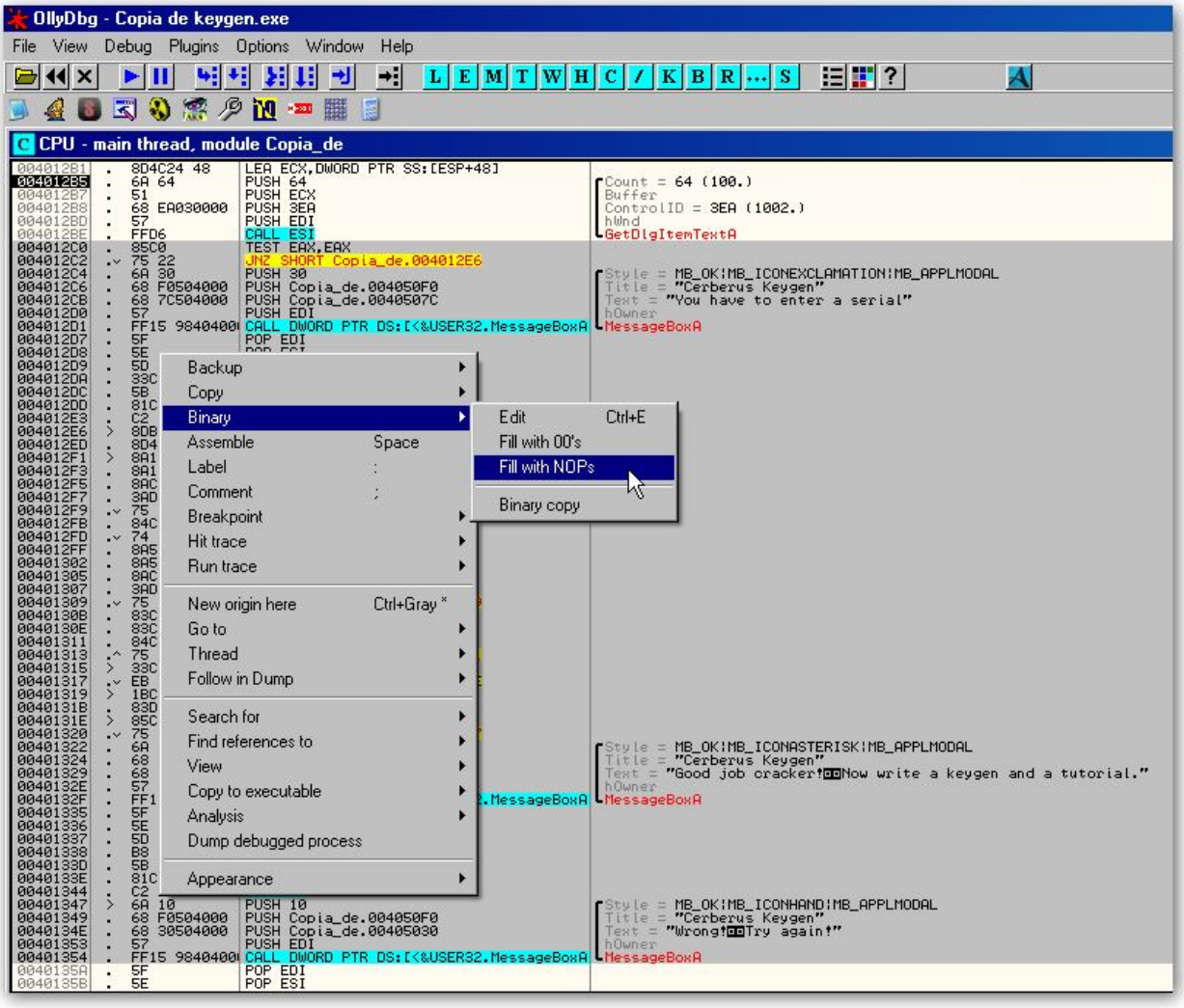
Nuestro "Notepad" queda ahora de la siguiente manera



Acto seguido ya podemos borrar los dos "BP"

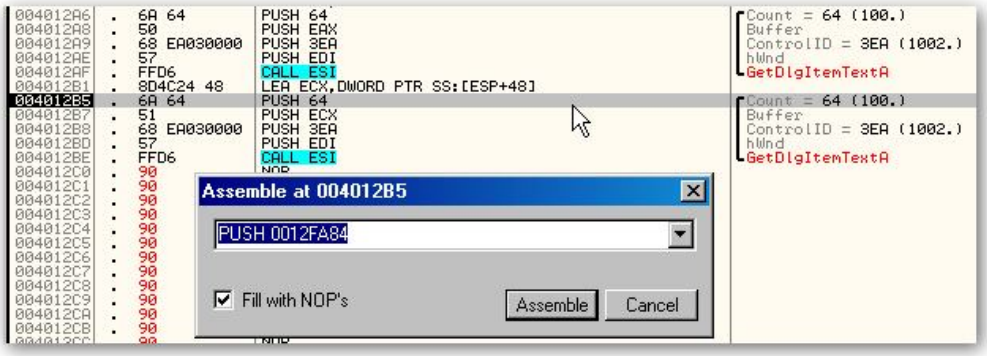


Y NOPeamos la parte de código que no nos interesa para nada, y que va desde la address "004012C0" hasta la "00401354"

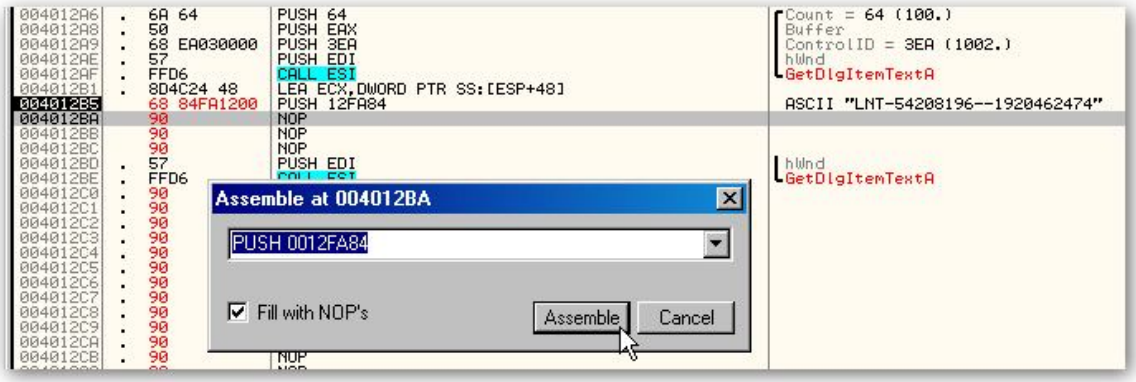


Analizamos código para que se vea todo mejor, y haciendo "scroll" volvemos a la posición donde estábamos parados, y que era la address "004012B5"

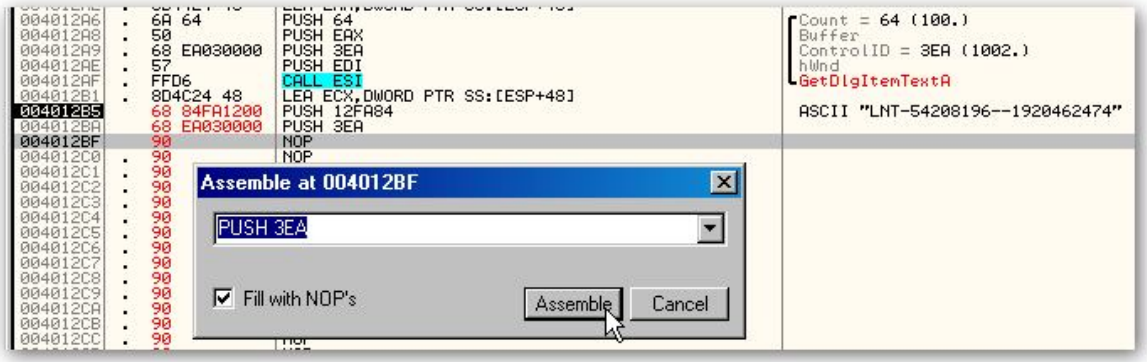
Una vez aquí, primero cambiamos la instrucción "PUSH 64" por "PUSH 0012FA84" que es como vimos antes, donde guarda el serial válido en memoria para nuestro "Name"



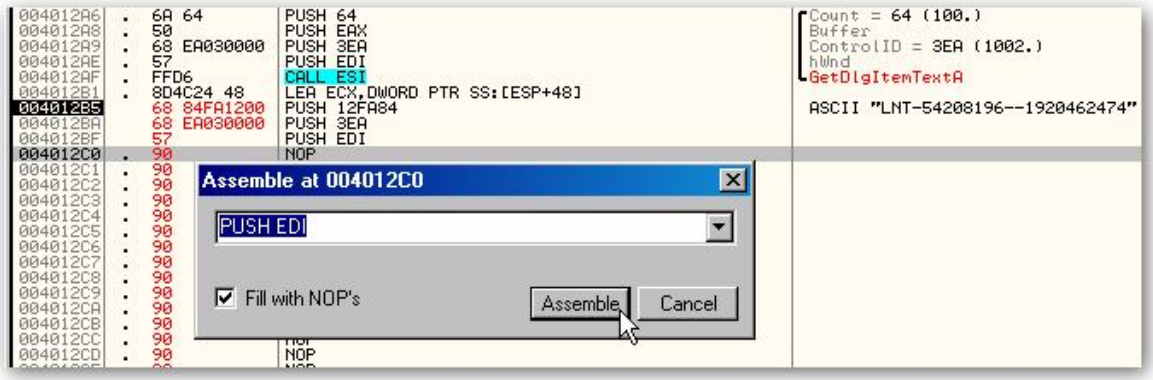
Quedando así



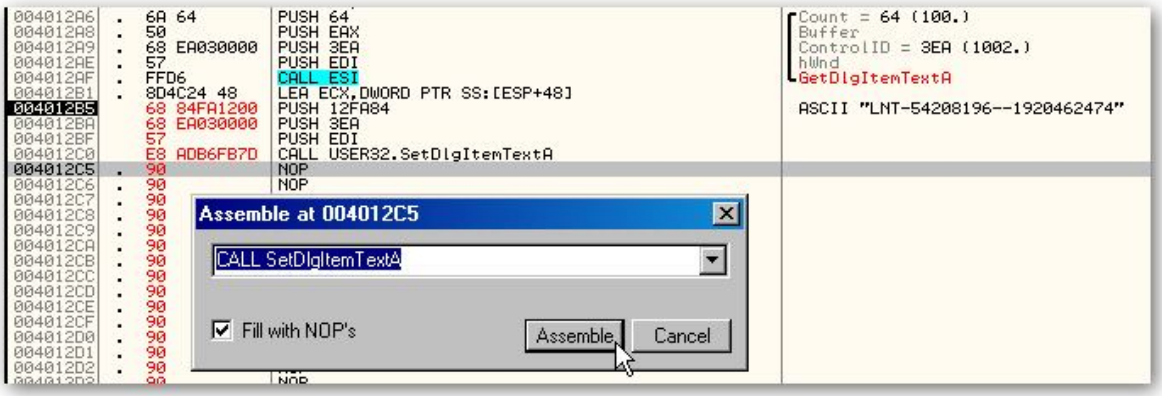
Segundo, insertamos "PUSH 3EA" que es el Control "ID" de la caja de texto



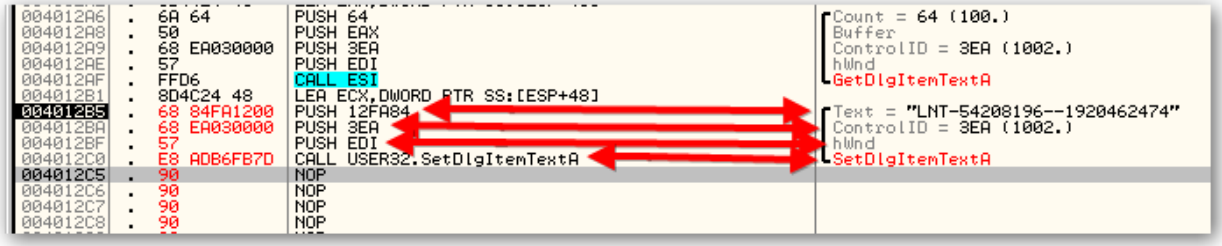
Tercero, insertamos "PUSH EDI" que es el "handle" de la ventana



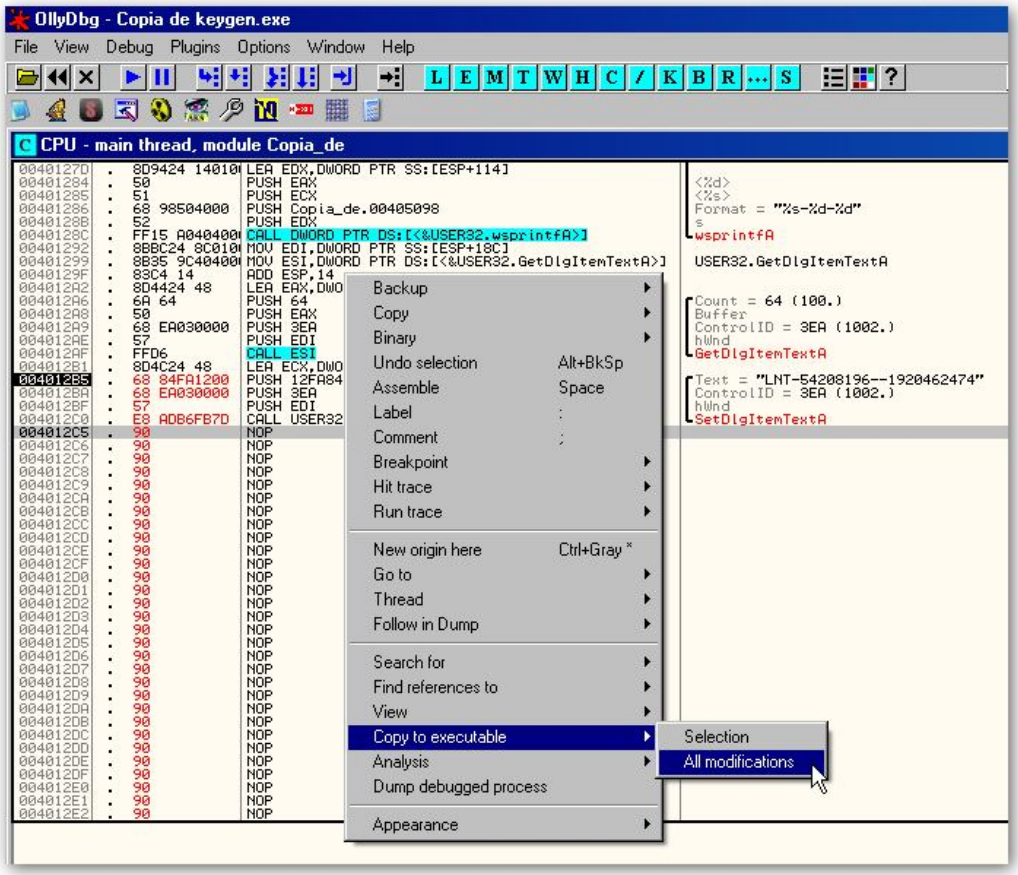
Y, cuarto, insertamos la función APIs "CALL SetDlgItemTextA" que se encargará de mostrarnos el Serial válido para nuestro Name en la caja de texto.



Analizamos código para que se reorganice todo, y nos queda así de guapo…



Por último, guardamos todas las modificaciones

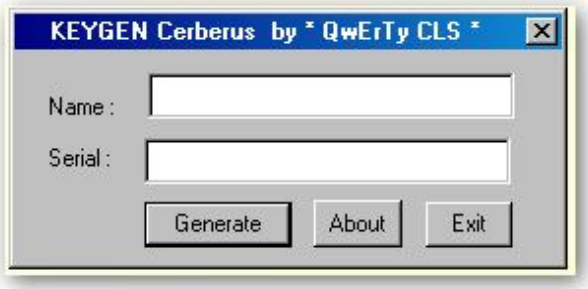


Renombramos , yo le he llamado, Selft-Keygen.exe y le damos a "Guardar"

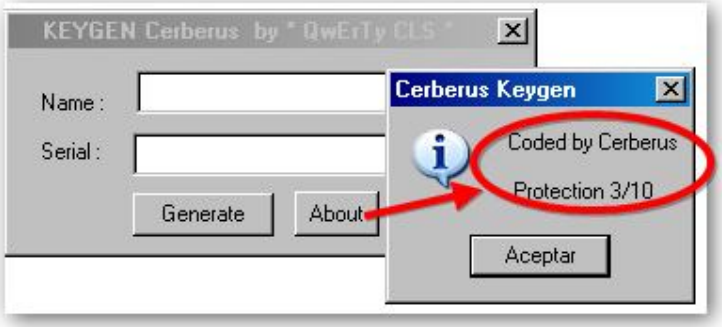
Ahora ya podemos salir de Olly, nos vamos a la ruta donde lo hemos guardado, y comprobamos que funcione.

Y ……..funciona de maravilla

Ahora, su aspecto exterior no queda muy serio que digamos para un auténtico generador de llaves. Salimos de nuestro "Selft-Keygen.exe" lo maqueamos con la Tool "Resource Hacker" y lo dejamos así:

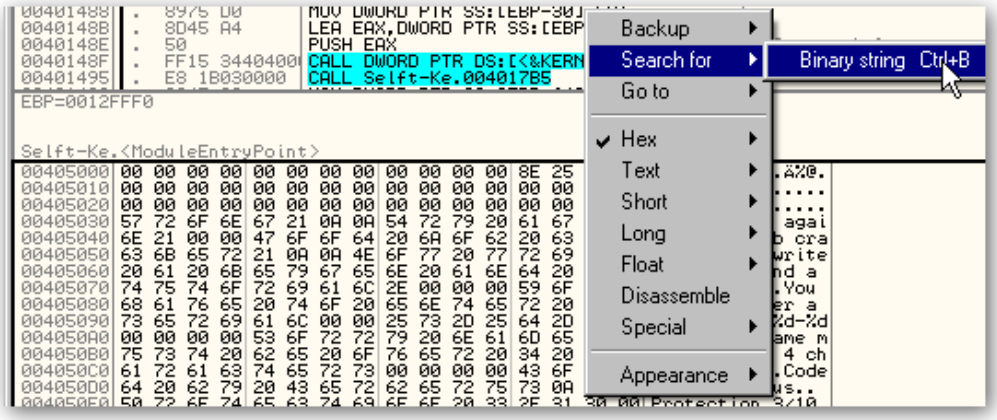


Pero aún nos queda un último detalle…… si le damos a la tecla "About" nos muestra el cartelito de

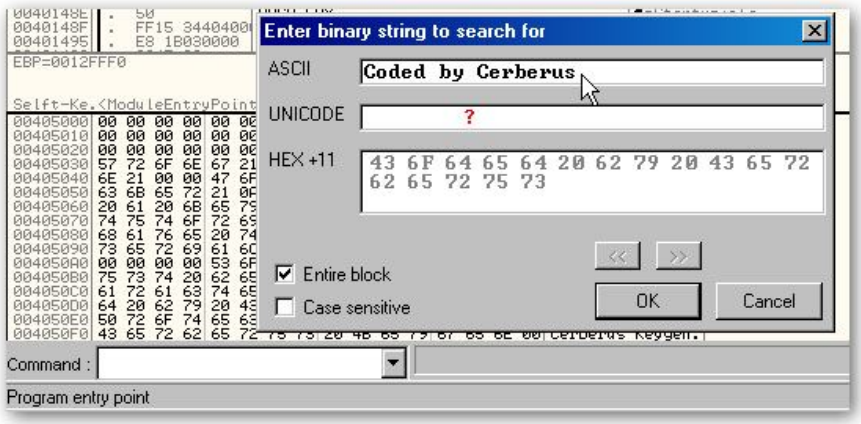


Pues vamos a cambiar ese texto con Olly (aunque también podríamos hacerlo con un Editor Hexadecimal).

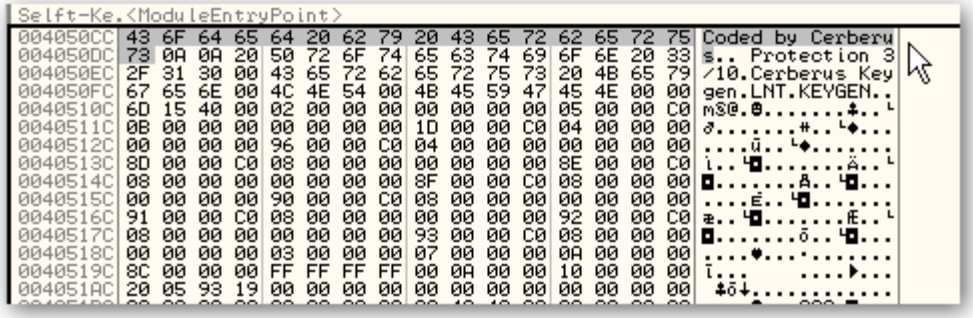
Salimos de nuestro "Selft-Keygen.exe". Lo cargamos con Olly, nos posicionamos sobre la ventana "Dump" hacemos "Search for – Binary string "



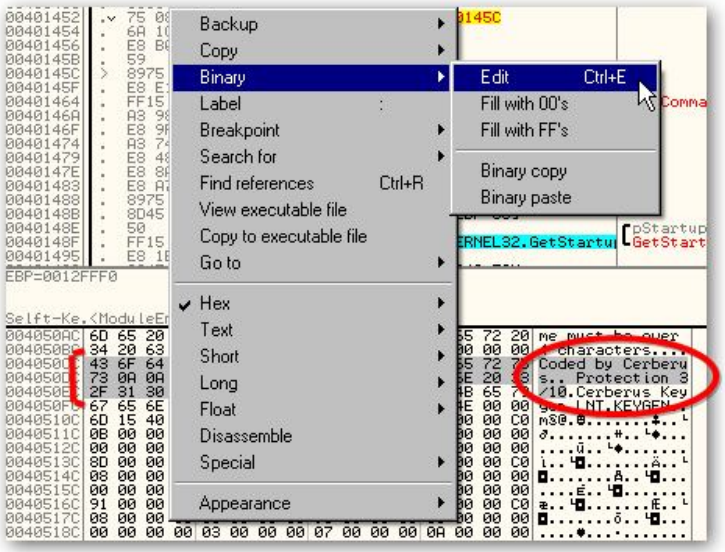
Ahora en la caja de texto "ASCII" tipeamos el mensaje a buscar o parte del mismo



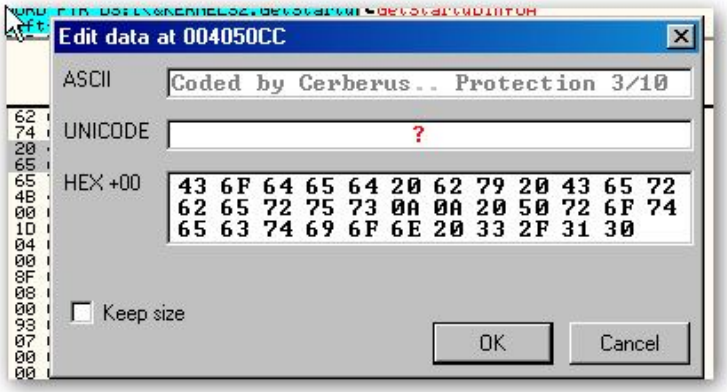
Le damos a "OK" y aparecemos aquí, justo lo que andamos buscando



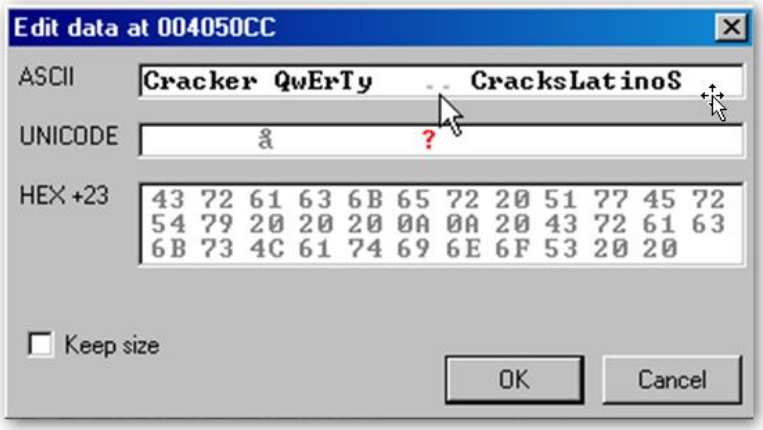
Sombreamos lo que queremos cambiar, editamos el Binario "Binary – Edit"



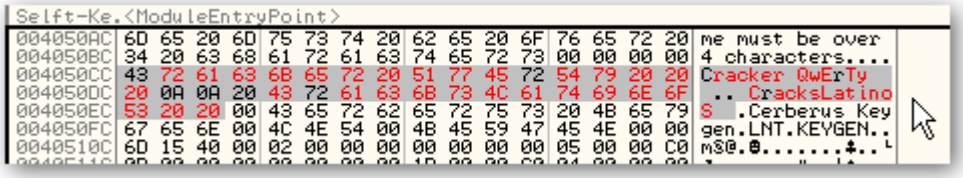
Cambiamos el texto por el que queramos (Respetando el largo)



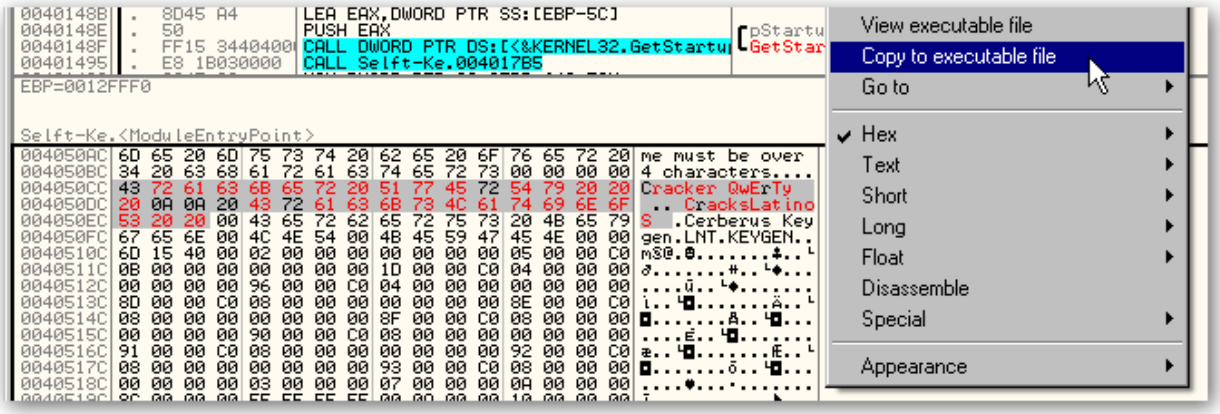
Yo tipeo



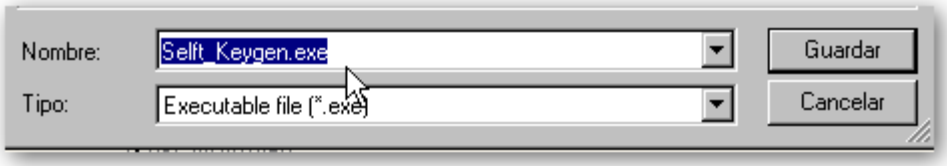
Le damos a "OK" y en la ventana "Dump" nos quedará así:



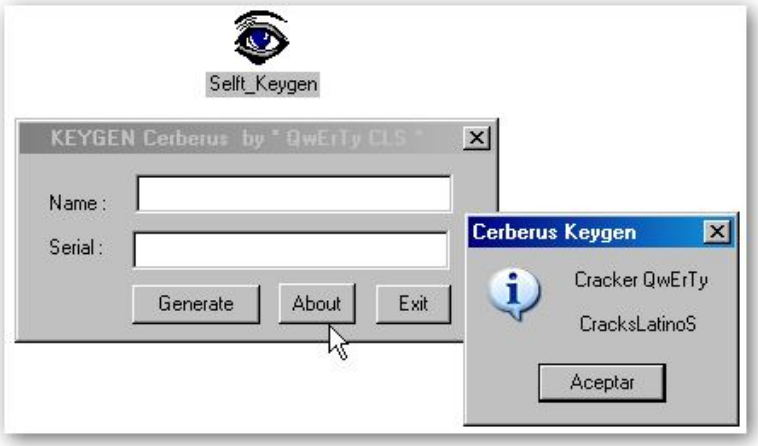
Ahora para guardar los cambios <u>sobre la misma ventana del "Dump" y con el texto marcado</u>, damos clic derecho de ratón y "Copy to executable file"



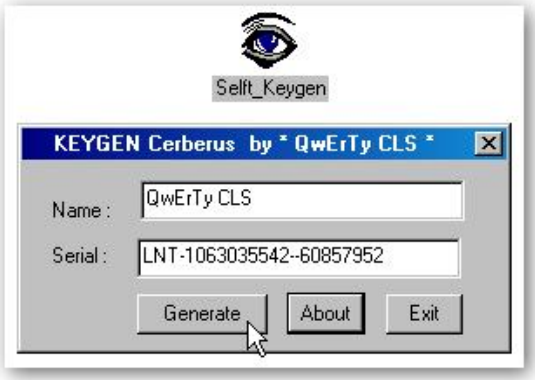
Renombramos el nombre del ".exe" con el que estamos trabajando por si las moscas, (si algo va mal siempre tendremos el ".exe" antes de la modificación), yo he cambiado el guión medio por guión bajo, y le damos a"Guardar".

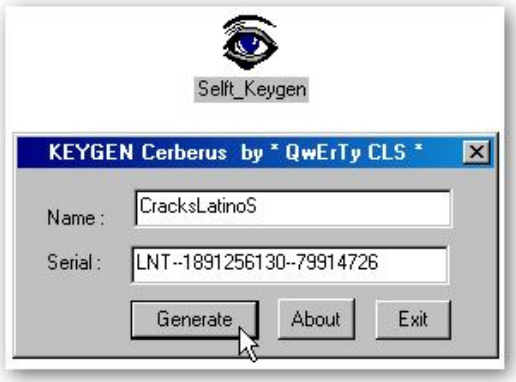


Ya podemos salir de Olly, vamos a la ruta donde tenemos nuestro flamante "Selft_Keygen.exe" final, lo ejecutamos, le damos a "About" y comprobamos que el cambio que hemos hecho haya surtido efecto……. y aquí lo tenemos……

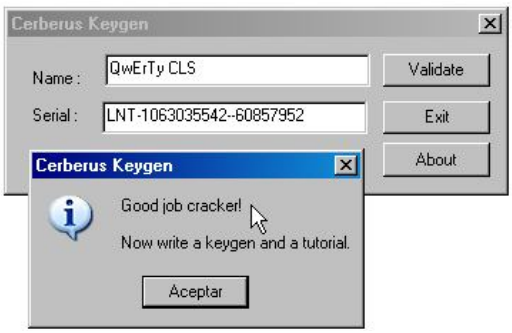


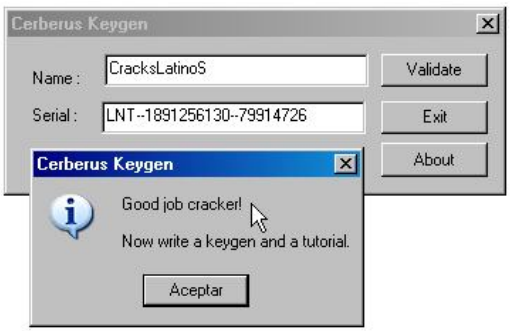
Y generando seriales a la perfección:





Comprobamos los Serials generados y…….





Se nos cae la baba sobre el teclado de lo orgullosos que estamos de nosotros mismos al ver finalizada y con éxito nuestra esplendida obra, decimos en voz alta QUE BIEN VA, los labios se nos ensanchan de oreja a oreja, y nuestra felicidad no tiene precio al ver también nuestra segunda misión finalizada y descaradamente recompensada.

A, se me olvidaba, ya podemos cerrar el Notepad….

……MISIÓN CUMPLIDA……

Mis agradecimientos infinitos a

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

La lectura solo proporciona a la mente material de conocimiento;
es el pensamiento lo que hace lo que leemos nuestro.
John Locke

5 de Noviembre de 2016