Programa : Glary Utilities v 2.35 Trial Version (algunas funciones estan desabilitadas)

Tipo : Utilidades --- Glary Utilities offers numerous powerful and easy-to-use system tools and utilities to fix, speed up, maintain and protect your PC (winXP,Vista,Seven)

Proteccion :RDG nada , Delphi DLL

Lenguaje : Delphi v6 – v7

Link : <http://download.cnet.com/Glary-Utilities/3000-2094_4-10508531.html>

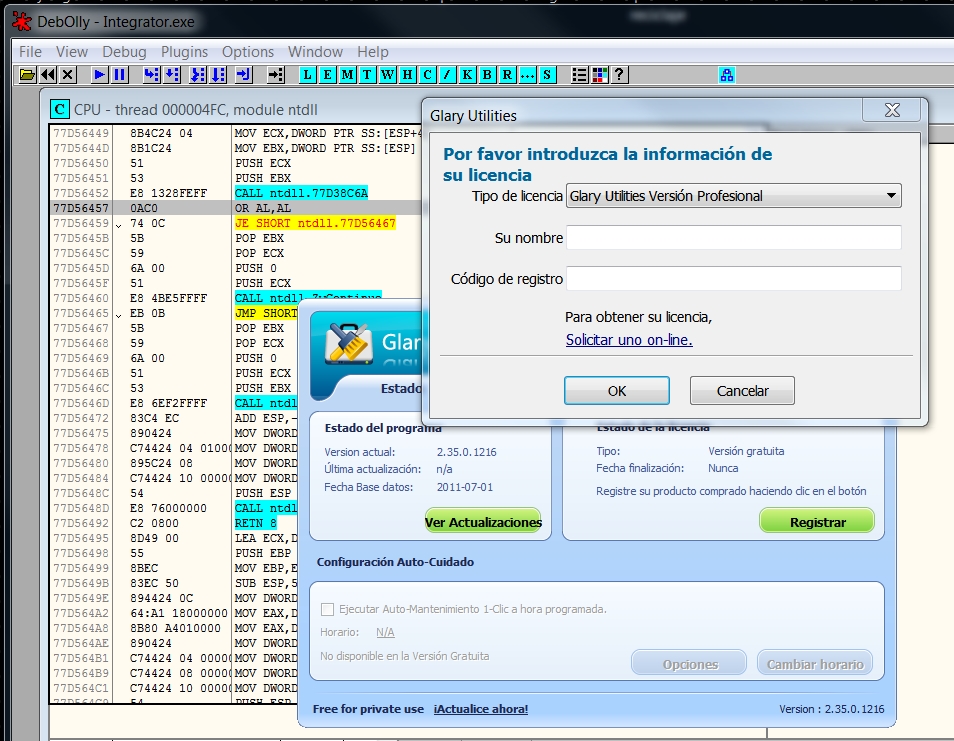
Cracker : EmO

Instrumentos de análisis : RDG y Ollydbg

Objetivo : Registrar el programa en su versión profesional.

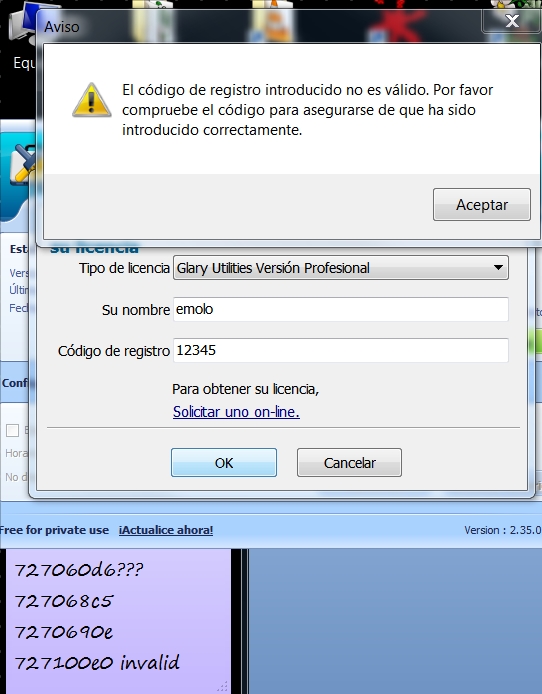
Tipo de Registro : Codigo de registro fijo,no depende del nombre

Hola!



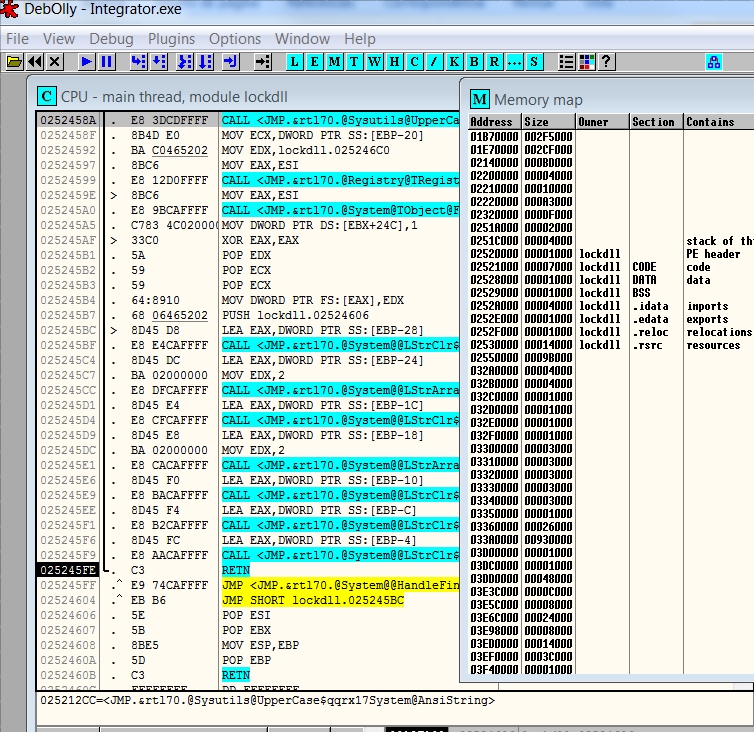
Empezamos abriendo en olly el programa (Integrator.exe) ,y aquí podemos ver el formulario de registro .

Introducimos un nombre y un código y click en OK,sale esta nag …



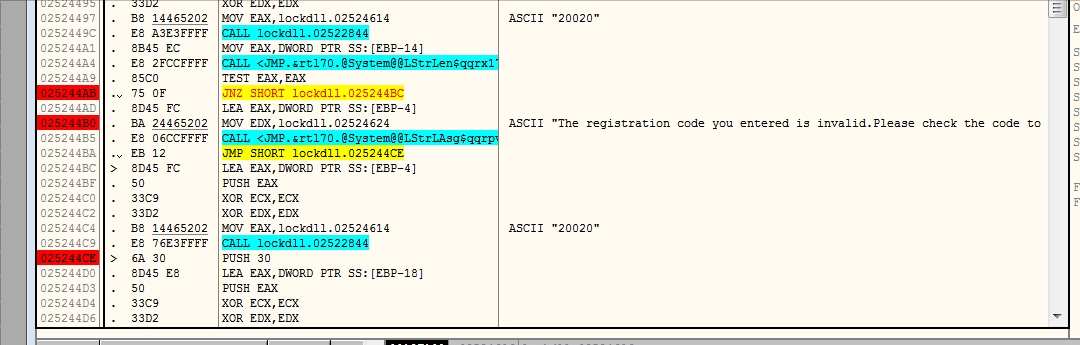
La idea es de cazar esta nag para ver desde donde ha sido llamada ,a ver si estamos en una zona de comprobación del serial ..

En este caso ,antes de cerrar esta nag ,doy f12(pausa) ,click en Aceptar y traceo con ctrl-f9 hasta regresar al primer modulo que encuentro del programa (podemos verlos desde el Memory Map),en este caso,después de varios ctrl-f9, regreso a lockdll,perteneciente al programa..

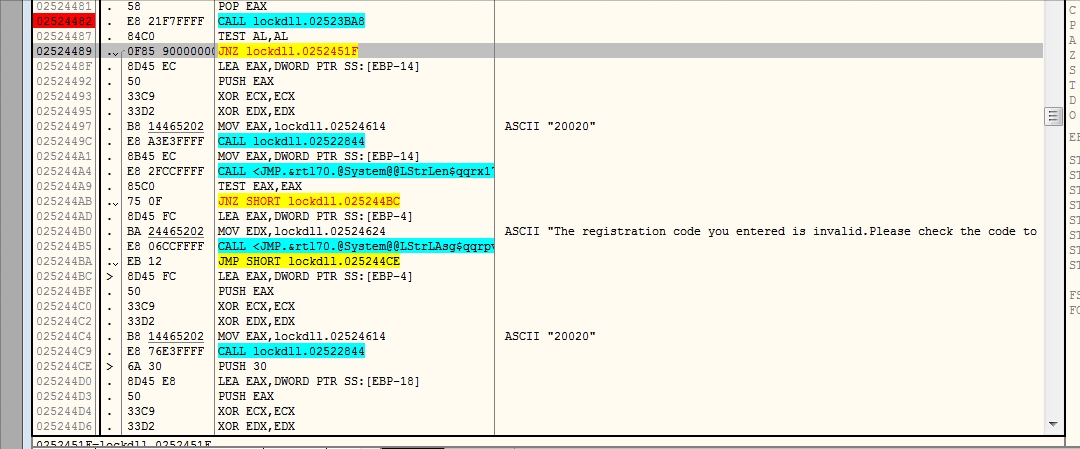


Aquí es donde retorna el ejecutable después de haber visualizado la nag de error,en 25245fe.

Si echamos un ojo hacia arriba,con el código analizado (ctrl-A),encontramos esto

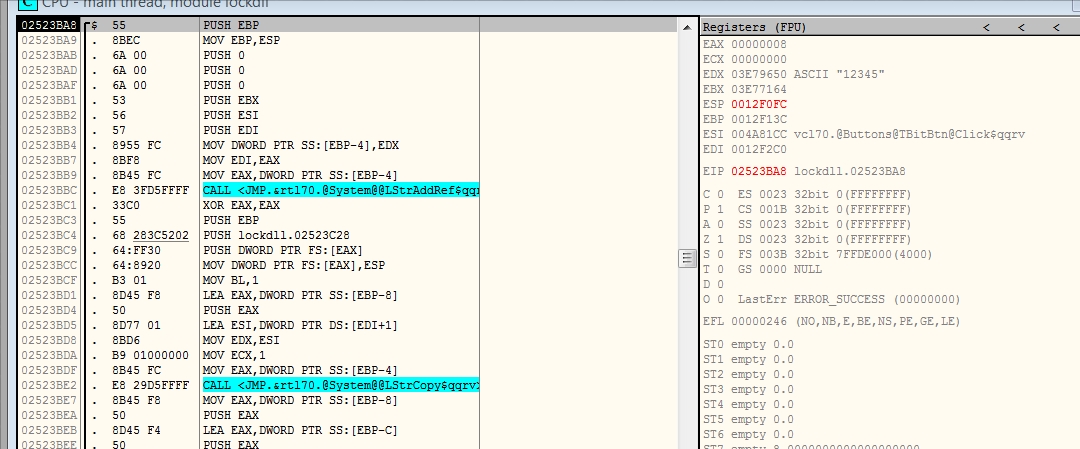


Podemos ver un salto decisivo unas líneas mas arriba en 2524489..

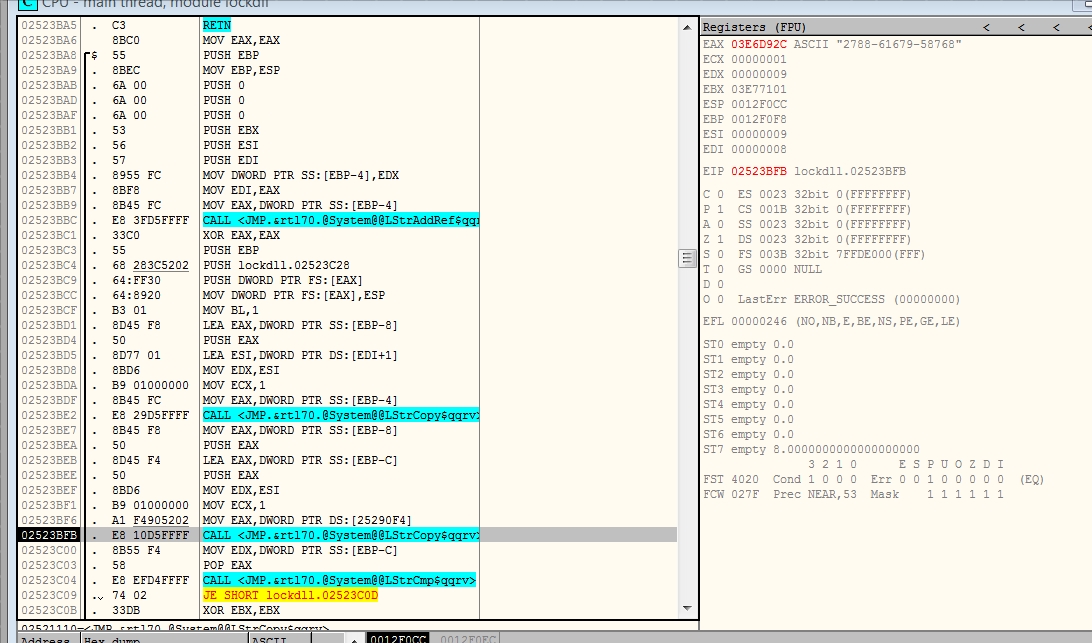


Seguramente en la call anterior se evalúan los datos introducidos ,ponemos un bp y damos f9,olly para en la call y entramos con f7..

Nada mas tener ojo a los registros y podemos ver nuestro código (12345)



Seguimos traceando con f8 y aquí podemos ver el código correcto ..



Si prueban a registrar con el código ascii que se encuentra en EAX,el programa quedara full .

A modo de estudio teorico,podemos ver como maneja la comparación del código en la call en 2523c04 (LStrgCmp),entonces entremos en ella con F7..

Podemos ver como aquí pasa el valor de eax a esi,pero notamos que es 0 y en los saltos que siguen vemos un TEST ESI,ESI para poder continuar ,si no salta.

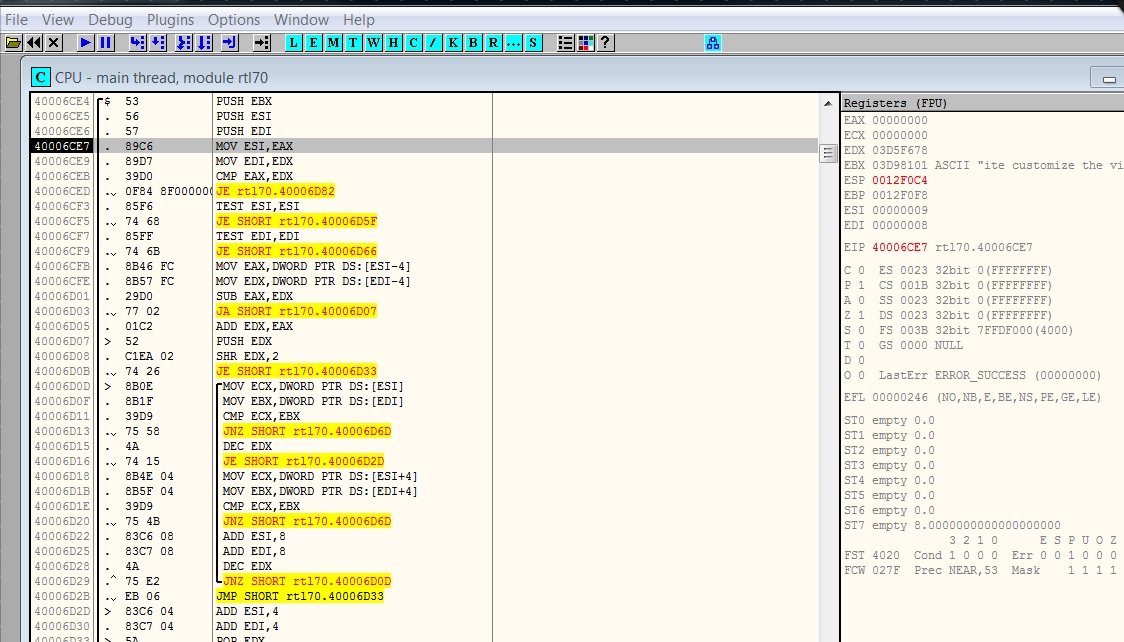
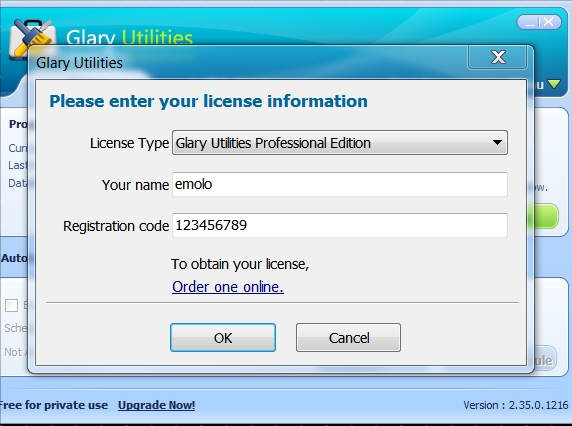


FIGURA 2

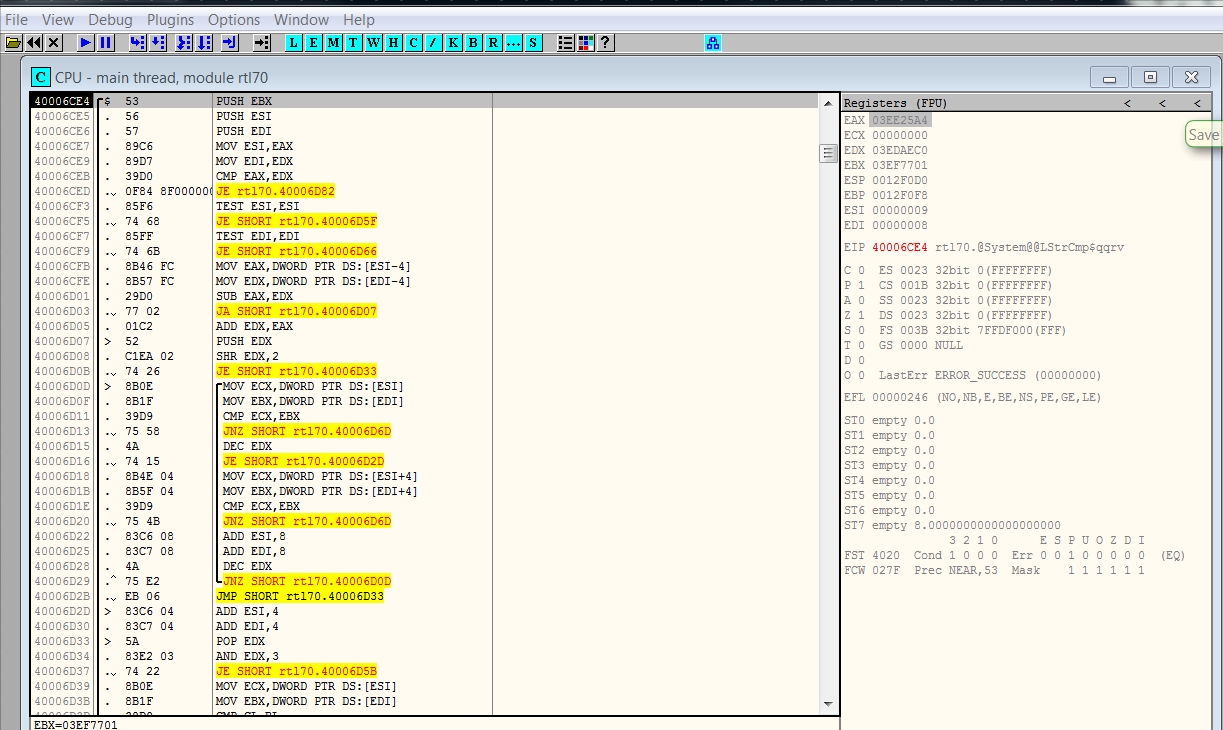
Con buen ojo ,nos damos cuenta que antes de entrar a esta call ,en el modulo lockdll,donde empieza toda esta rutina del serial,EAX valia 8 …



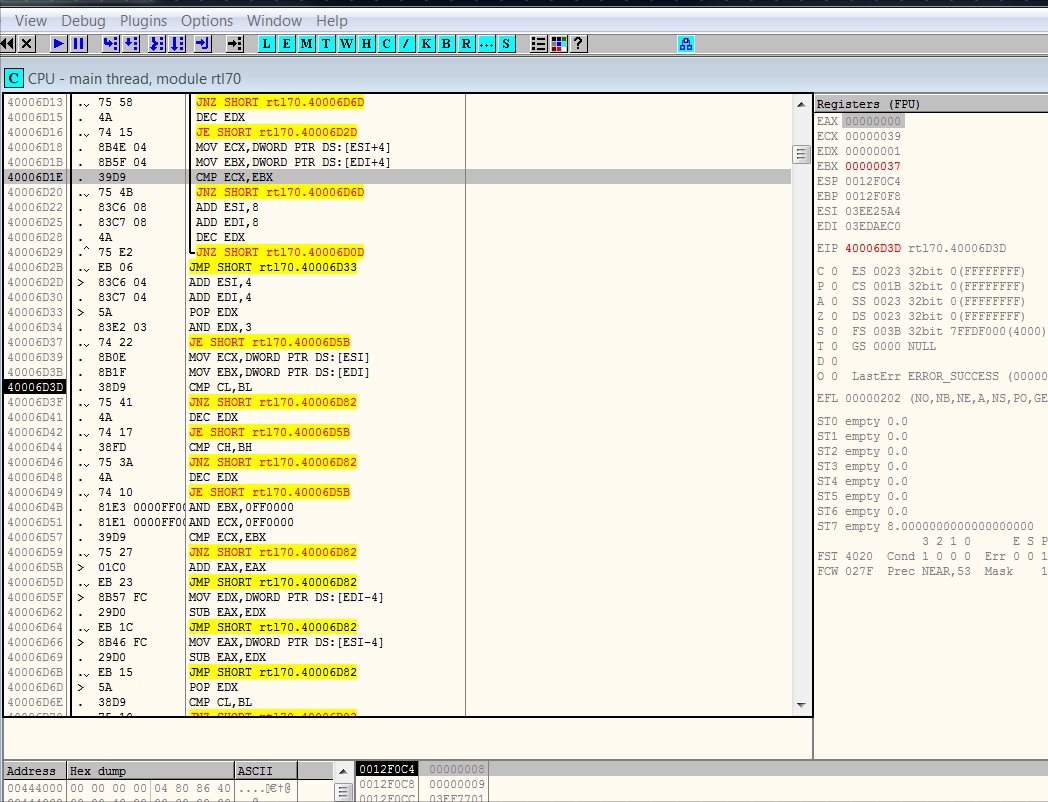
Me imagino sea un valor importante,seguramente el largo minimo para el código introducido..

Volvamos a la form del License y metemos un código de 9 digitos minimo 

Con nuestro BP en LStrgCmp ,olly para y volvamos a entrar en ella con f7…



Y podemos ver que EAX no es 0,traceamos con f8 y el programa sigue ,



Aquí compara bl con cl ,cl=39 (9) y bl=37 (7) , entonces el noveno digito de nuestro código debería ser un 7….

Si seguimos traceando,vemos como esta comprobación es bastante para el programa para licenciarnos ¡!!!

Concluimos que podemos meter en la form de licencia cualquier código que tenga un 7 en la novena posición …Probar para creer!!!

Para deregistrar el programa podemos borrar desde regedit las claves en HKEY\_LOCAL\_MACHINE\SOFTWARE\GlarySoft\Glary Utilities , regname y regcode

Gracias a CrackSlatinoS