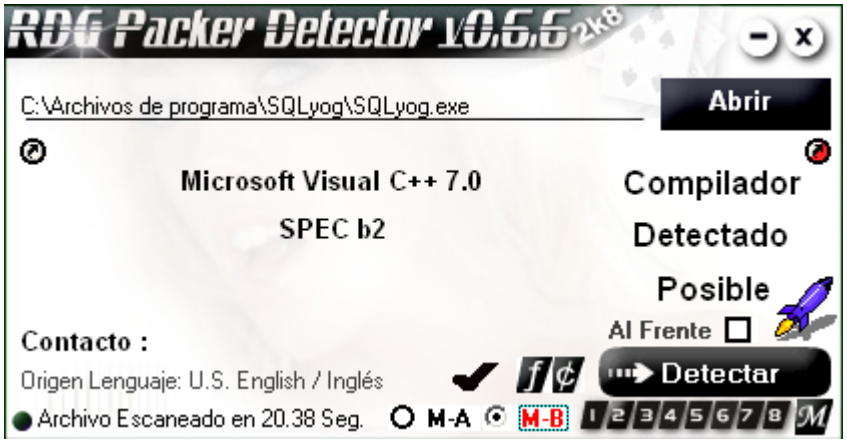
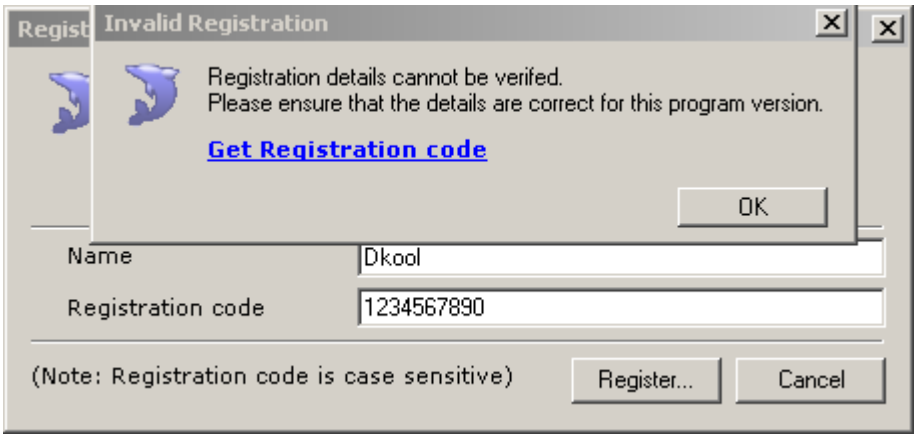
Victima:	Sqlyog
Version:	8.32
Descripción:	Frontd para administrar Mysql
Url:	http://www.webyog.com
Protección:	Serial
Objetivo:	Encontrar serial para activarlo
Dificultad:	Newbie
Herramientas:	RDG, Ollydbg
Cracker:	Dkool
Fecha:	22/04/10

Este es mis segundo tute, por la escuela y el trabajo pues estaba muy ocupado, pero bueno vamos al grano haber que sale jeje.

Como primer paso seria checar el programa si no esta empacado, como siempre lo hago lo abrimos con el RDG.

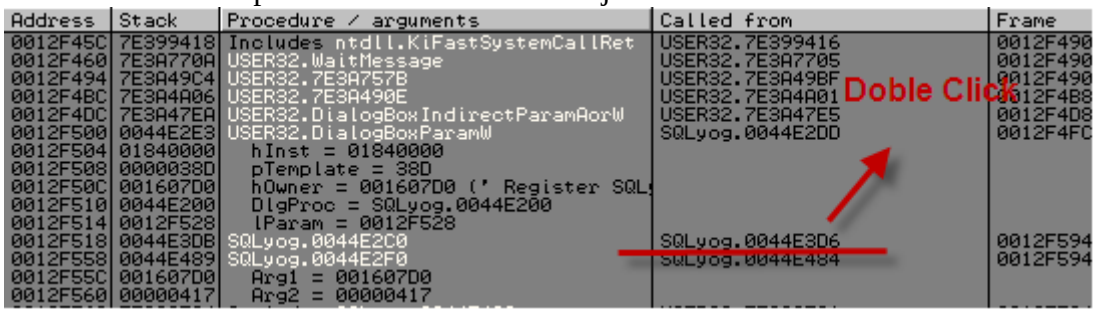


Y vemos que esta en Visual C++ y el RDG detecta SPEC b2. mmm pues no habia visto ese SPEC b2, pero sigamos a ver que pasa abrimos el programa y nos pide la ventana de registro, para ello ingresamos datos y haber que pasa pero pues como era esperarse nos manda error como se muestra.



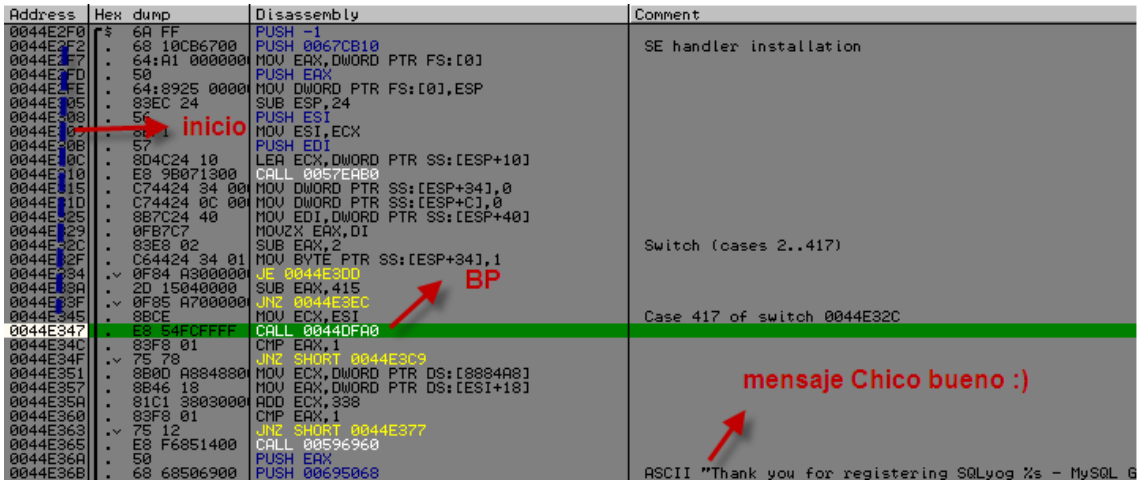
Bien ahora le toca a ollydbg, lo abrimos y nos vamos alas referenced Strings no encontramos el mensaje de chico malo, mmmmm entonces vamos por otro metodo, bien damos F9 para correr el programa y cuando nos pida los datos de registro los llenamos y damos click en el boton de register nos sale el mensaje de error y antes de dar click en ok del chico malo nos vamos a ollydbg y presionamos pause y enseguida damos click en la letra k como se muestra.

Terminando esos 2 pasos caemos en los mensajes de error como se muestra.



Y en la dirección 0012F518 damos doble click como muestra la imagen, dando dbl clic caemos en esa dirección como se muestra.

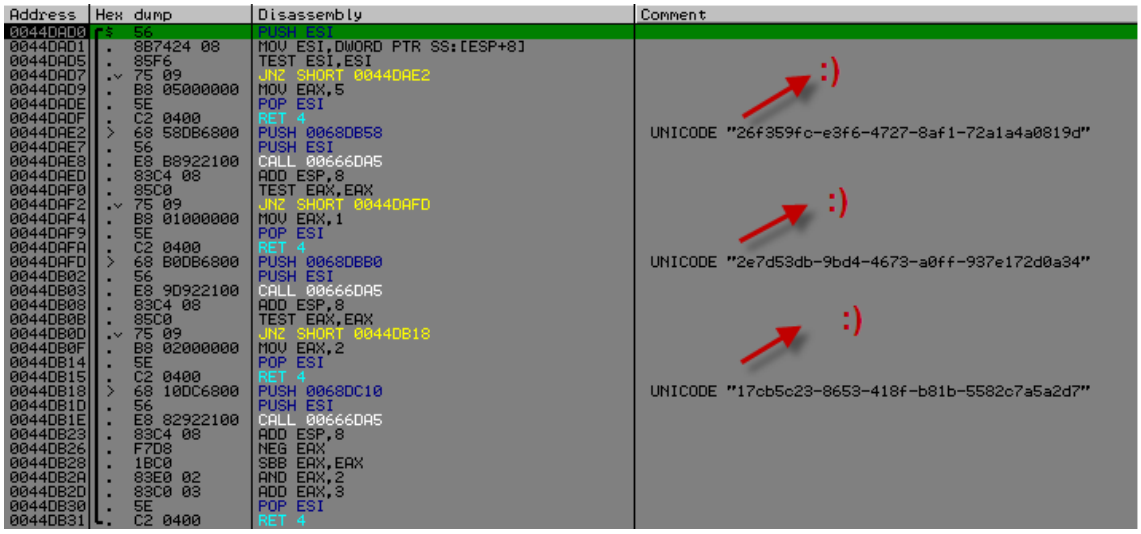
Y bien ya estando ahí vamos subiendo hasta donde inicia la función o en esta dirección 0044E2F0, y mas abajo esta una CALL 0044DFA0 y abajo de esta call esta una comparación CMP AX,1 como que suena bien esta call y le damos un bp con F2. Como se muestra.



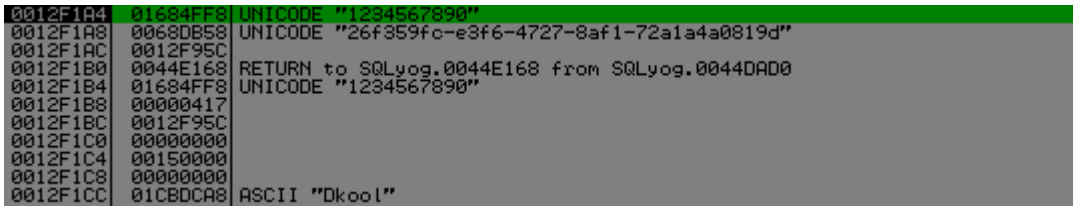
Bien ya que le dimos un bp a la call reiniciamos el olly CTRL + F2, y nuevamente damos F9 para correr el programa e ingresamos los datos de registro y le damos ok al

chico malo y caemos en la call que ingresamos el bp, enseguida de esto entramos a ella con F7, ya estando ahí vamos traceando con F8 hasta llegar a una call 00665C66 ya abajo un JNZ esa call significa junto con el salto si no ingresamos el numero de registro se habilita el salto y nos manda al call de error. Pero eso no pasara ya que nosotros ingresamos jeje, y bien pasemos ese JNZ y sigamos traceando hasta llegar esta CALL 0044DAD0. como se muestra.

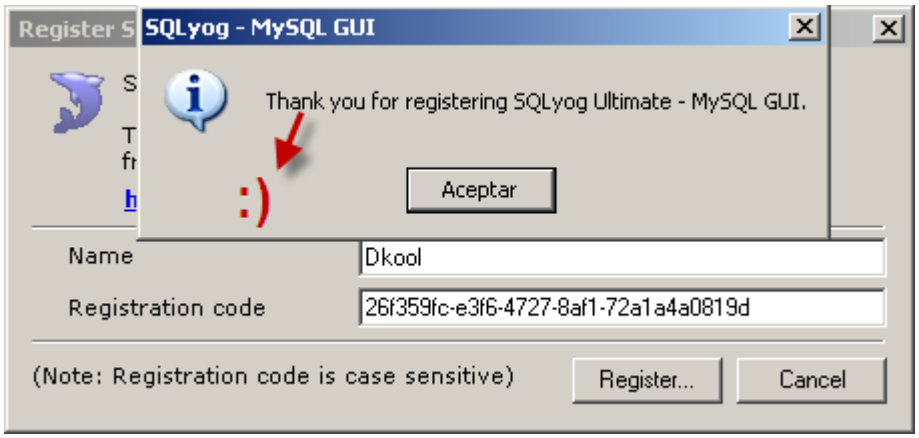
Entramos a es call con F7 y Woowww creo q encontramos el tesoro jejeje nos aparecen 3 seriales distintos como se muestra.



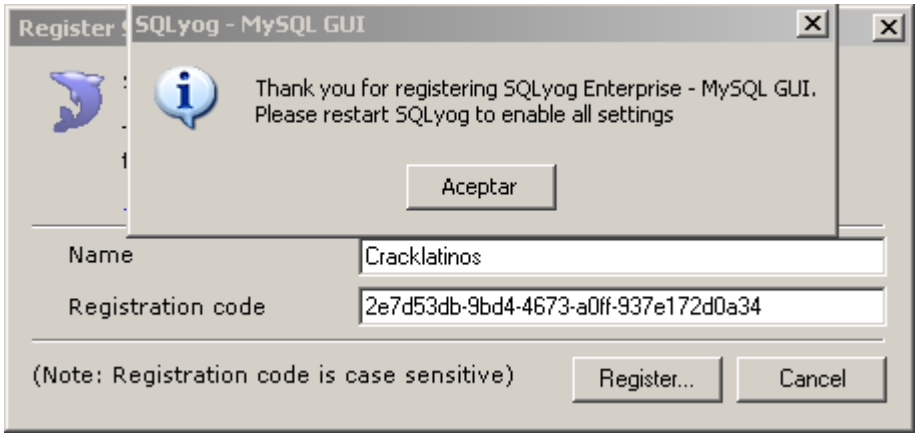
Bien si queremos podemos ir traceando para ver como se compara el serial que ingresamos por ejemplo.. 1234567890 con los 3 de ahí. Lo podemos ver en el stack como se muestra.



Ahora viene probar esos seriales sin son los correctos para ello copiare el primero, bien vamos haber, abrimos ejecutamos el programa y probemos.



Bien si funciono jeje muy bien. Pues como observamos el name no importa para los seriales, mmm ingresemos con otro name y ahora probemos el segundo serial jeje vamos haber si funciona.



Perfecto si funciona con cualquier name y con el segundo serial jejee era de esperarse jeje. Ahora mi programa queda registrado a **CRACKLATINOS.** Me parece excelente que quede con ese nombre registrado por que sin ellos no estaría haciendo estos tutoriales, sencillos pero efectivos jeje. Bueno un saludo a todos los Cracklatinos a ZELT@ y al buen master ricardo narvaja.. Bien me despido y prometo hacer otro tutorial mientras sigo tomando unas cervezas jeje por que esta duro la calor jeje.