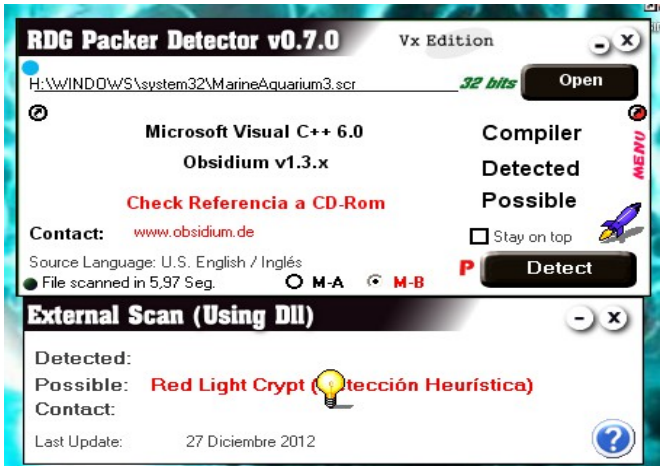
CRACKS LATINOS

Programa	Marine Aquarium 3		
Protección	Serial y limite		
Descripción	Un screensaver		
Dificultad	Pues.....		
DownLoad	softonic		
Herramienta	olly		
Cracker	La Calavera	**Fecha**	

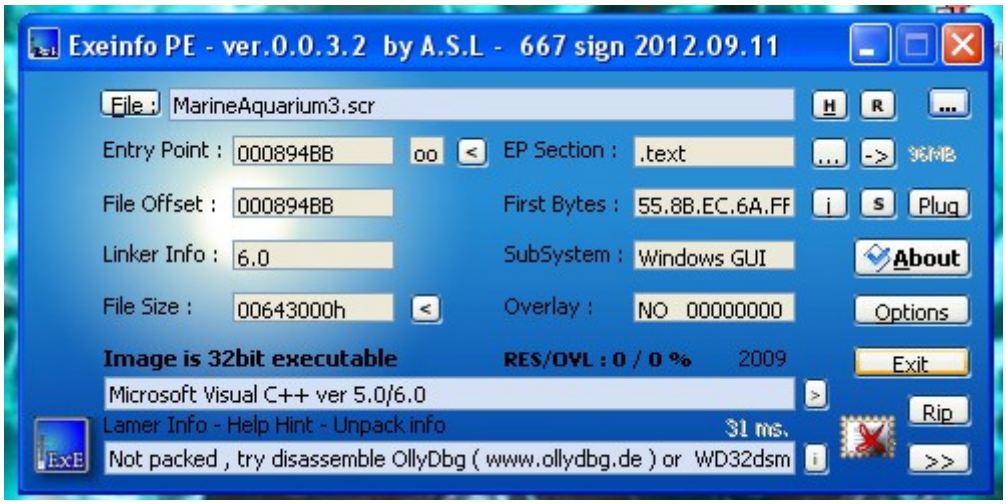
INTRODUCCION
Bueno esto sigue siendo como desde un principio solo para el aprendizaje y nada de piratería ;-)

AL ATAKE

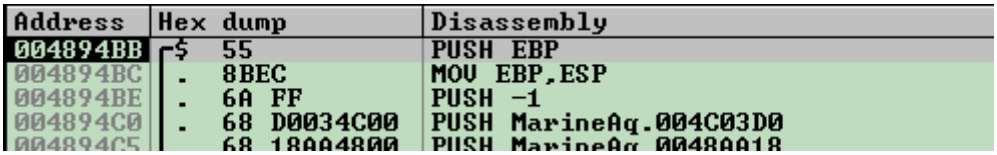
Bueno comencemos lo primero analizarlo a ver si esta comprimido y con que esta compilado



bueno ahí tenemos los que nos dice el RDG veamos el exeinfo PE

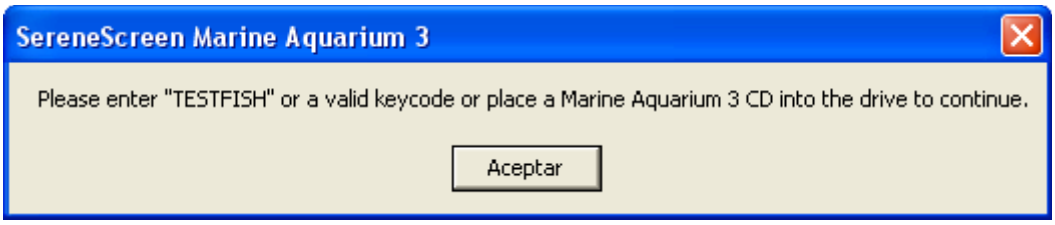


bueno como ven ambos dicen que es un VC++ así que manos a la obra lo cargamos con el olly y nos muestra el EP

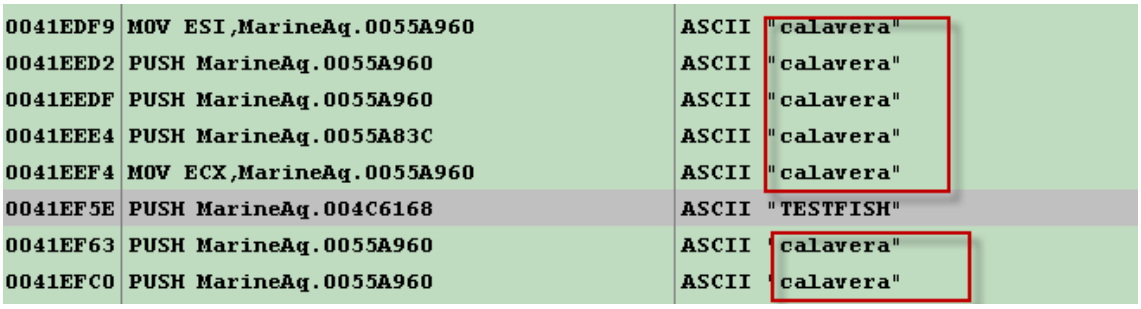


le damos a F9 y nos sale

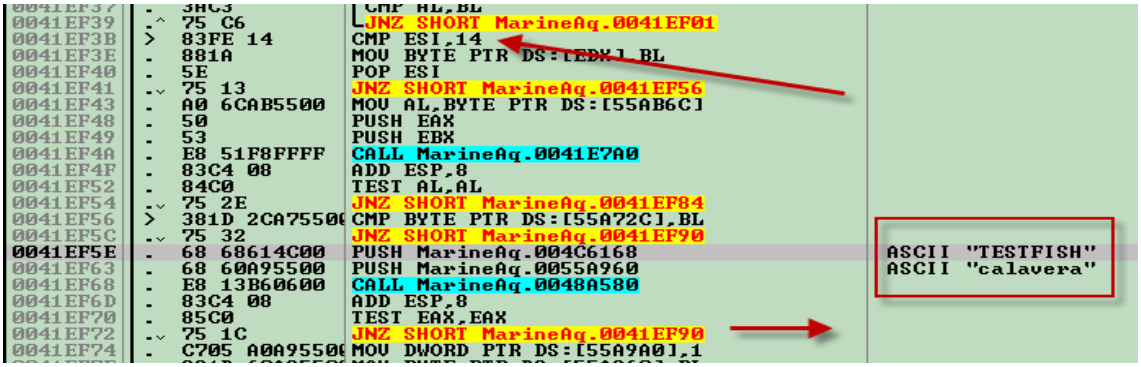
bueno como ven nos pide que ingresemos el serial que hemos adquirido para registrar o TESTFISH para entrar en modo de prueba bien ingresamos un serial “calavera” que tiene un largo de 8 caracteres y le damos a OK y nos muestra



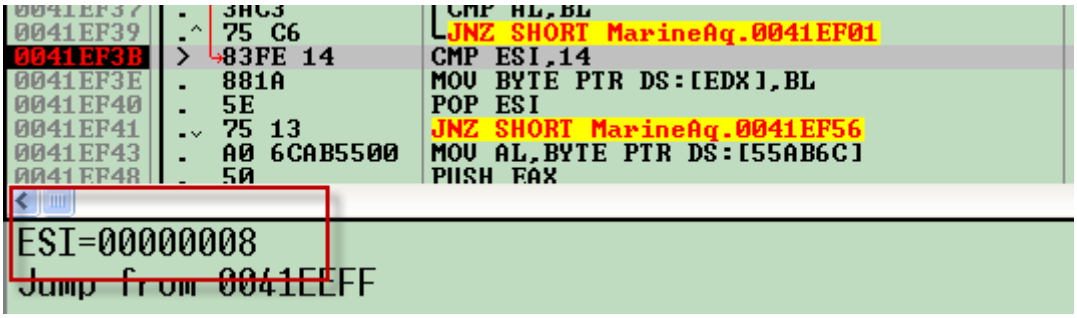
Bien vamos a ver entre las string si sale el dicho cartelito buscamos keycode y no sale nada, probemos con el TESTFISH a que si encontramos algo



pues no hay muchos que decir si estamos cerca no?? jejeje hacemos doble clic y caemos aquí



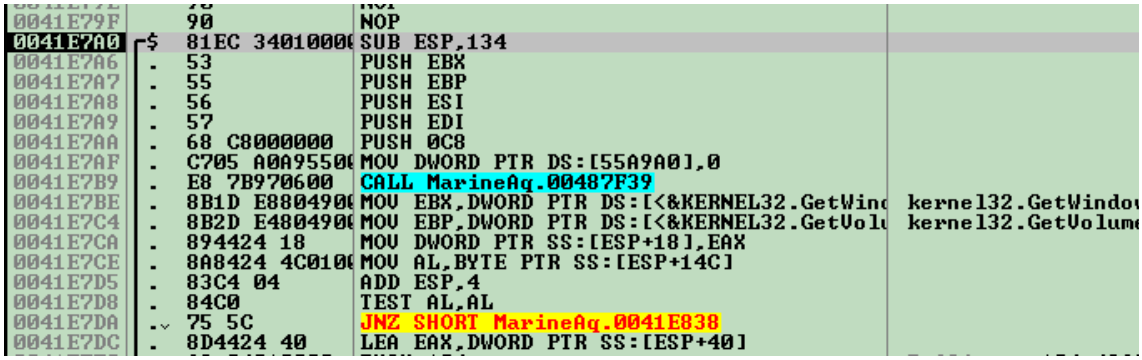
como ven en el recuadro lo compara con el serial de prueba si es igual entra en modo de demostración y un poco mas arriba vemos algo muy interesante 41EF3B un comparación con 14h osea 20 en decimal ponemos un BP en la comparación, aceptamos el mensaje y apretamos nuevamente en OK y cuando para en la comparación vemos



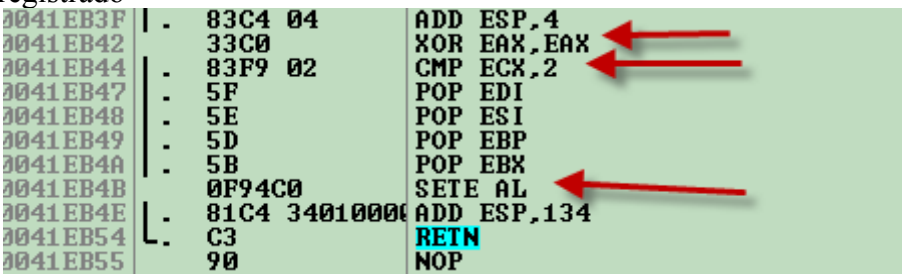
como ven compara el largo de mi serial con 14h así que le damos a OK y pongo "calaveracalaveracala" :-) que es un largo de 20 decimal y le doy a OK, cuando para vemos que tenemos el largo correcto pero el serial ni ahí jajajaja, así que sigamos a ver donde nos lleva comenzamos a tracear

0041EF41 |. /75 13 JNZ SHORT MarineAq.0041EF56
0041EF43 |. |A0 6CAB5500 MOV AL,BYTE PTR DS:[55AB6C]
0041EF48 |. |50 PUSH EAX
0041EF49 |. |53 PUSH EBX
0041EF4A |. |E8 51F8FFFF CALL MarineAq.0041E7A0
0041EF4F |. |83C4 08 ADD ESP,8
0041EF52 |. |84C0 TEST AL,AL
0041EF54 |. |75 2E JNZ SHORT MarineAq.0041EF84

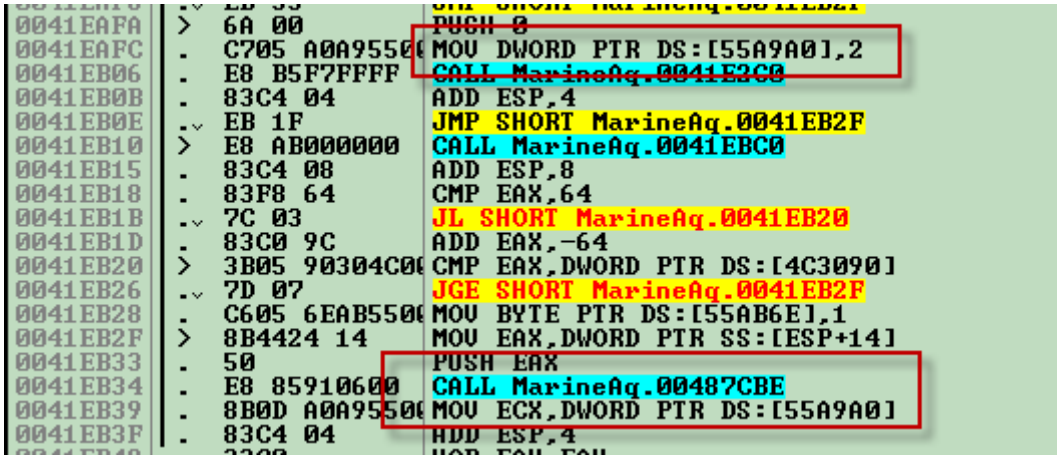
hasta el call traceamos y entramos en el y vemos



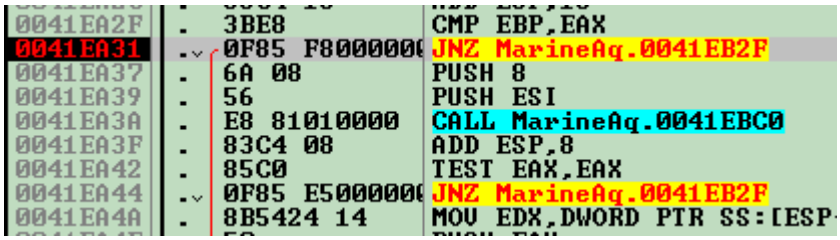
bien analizamos un poco y veamos el final del call que valores sale EAX o AL para que estemos registrado



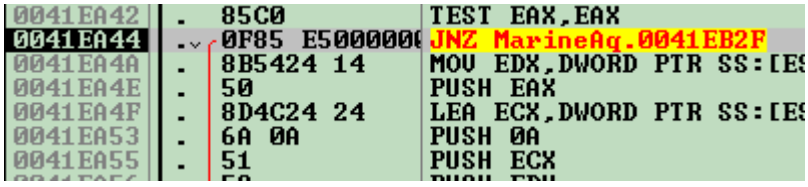
como vemos primero pone a EAX en cero luego compara a ECX con 2 y luego setea si la comparación dio OK pone a EAX o AL en 1 si no lo deja en cero así que debemos buscar donde mete el 2 en ECX mirando un poco mas arriba vemos



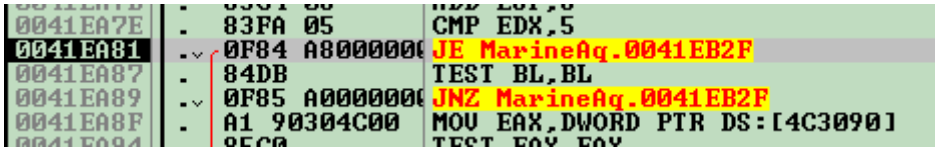
como ven en 41EAFC mueve un 2 a 55A9A0 y luego en 41EB39 lo mueve a ECX bien ahí tenemos la dirección a la cual debemos llegar así que como estamos parados en el inicio del call comenzamos a tracear y ver que salto evita caer en esta zona, vamos traceando y si miran un poco verán que el serial lo pasa a binarios así que yo me olvide de hallarlo así que seguimos traceando hasta esta dirección



como ven el salto se va a efectuar y nos manda lejos de donde queremos llegar así que lo nopeamos y seguimos



el próximo es es y efectivamente también va a saltar así que lo nopeamos y seguimos



lo mismo nopeamos los 2 ya que van a la misma dirección y seguimos

```
0041EA96  .  8BF8          MOV EDI,EAX
0041EA98  .v 75 05         JNZ SHORT MarineAq.0041EA9F
0041EA9A  .  BF 01000000   MOV EDI,1
0041EA9F  >  8B5424 14     MOV EDX,DWORD PTR SS:[ESP+14]
0041EAA3  .  6A 07         PUSH 7
```

ese como es un salto corto lo dejamos ya que no influye seguimos

```
0041EABD  .  56            PUSH ESI
0041EABE  .v 75 50         JNZ SHORT MarineAq.0041EB10
0041EAC0  .  E8 FB000000   CALL MarineAq.0041EBC0
0041EAC5  .  83C4 08       ADD ESP,8
0041EAC8  .  83F8 64       CMP EAX,64
0041EACB  .v 7C 2D         JL SHORT MarineAq.0041EAFA
0041EACD  .  6A 07         PUSH 7
```

como vemos este salto se va a efectuar y evita nuestra zona así que lo mismo NOP y seguimos traceando

```
0041EAED  .  84C0          TEST AL,AL
0041EAEF  .v 75 09         JNZ SHORT MarineAq.0041EAFA
0041EAF1  >  C605 6DAB550  MOV BYTE PTR DS:[55AB6D],1
0041EAF8  .v EB 35         JMP SHORT MarineAq.0041EB2F
0041EAFA  >  6A 00         PUSH 0
0041EAFC  .  C705 A0A9550  MOV DWORD PTR DS:[55A9A0],2
0041EB06  .  E8 B5F7FFFF   CALL MarineAq.0041E2C0
0041EB0B  .  83C4 04       ADD ESP,4
```

bueno llegamos y como vemos el salto no se va a efectuar y llegamos al JMP que evita nuestra zona y si el sato se efectúa mete el dichoso 2 a nuestra dirección así que lo cambiamos por un JMP 41EAFA y le damos a F9 y arranca el panel de control del screensaver

vamos a Settings y vemos

como ven salen todos los peces que trae el programa

y esa es una captura del programa sin registrar de la misma ventana como ven el screensaver quedo registrado.

Bueno esto es para toda la maravillosa lista CracksLatinos y este es un regalito de cumple AÑOS

Saludos y vamos por muchos años masssssss!!!!!!!!!!!!!!!!!!!

Daniel