Crackme	Ice9
Misión	1- Saltar la protección de la API "IsDebuggerPresent" de forma manual usando la Tool x32dbg 2- Registrarnos
Compilado	ASM
Empacado	No
Tools	x32dbg - RDG Packer Detector v0.7.6.
Sistema Operativo	Windows XP SP3
Reverser	QwErTy CLS
Dedicado	Solid,@riel,Tena,kienmanowar,CLS y a todos los Crackers del mundo
Descargar Crackme	https://mega.nz/#!W5FUhYJS!iNqwf5Voq6VjhVQhtrflkoZOPF8jfXZqcL16pQefBw4

Este pequeño Crackme seguro que es súper conocido por todos ustedes, y ya lo solucionó de forma magistral con keygen incluido, el grandísimo maestro _/_-=InDuLgEo=-_/_ . (Por cierto, sus tutoriales y keygens son realmente espectaculares).

Mí única intención con este pequeño tute es dar a conocer como saltar la protección "IsDebuggerPresent" de forma manual con la Tool "x32dbg" tal como me apuntó el maestro Solid, ya que hasta el día de hoy, no he encontrado ningún plugin efectivo para conseguirlo de forma automática.

Una vez descargado el Crackme, lo descomprimimos y aquí lo tenemos

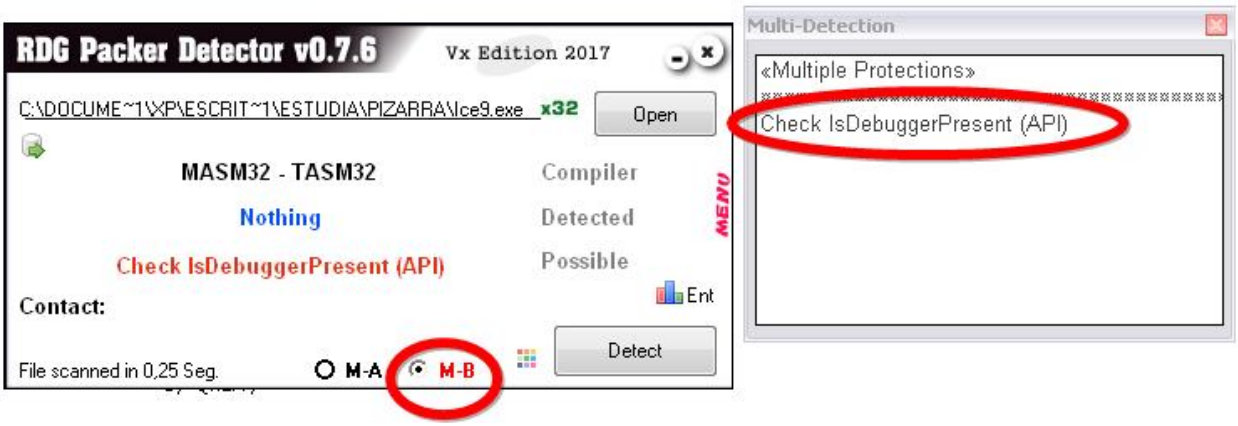
Ice9

ESTUDIANDO LA VÍCTIMA

Lo ejecutamos, rellenamos datos, le damos a "Check" y nos salta el mensaje de "Chico malo"

CONTINUEMOS ESTUDIANDO LA VÍCTIMA

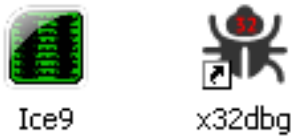
Le pasamos el detector de ejecutables "RDG" y nos informa que es de 32 bits, que está compilado en MASM/TASM, y de un posible "IsDebuggerPresent"



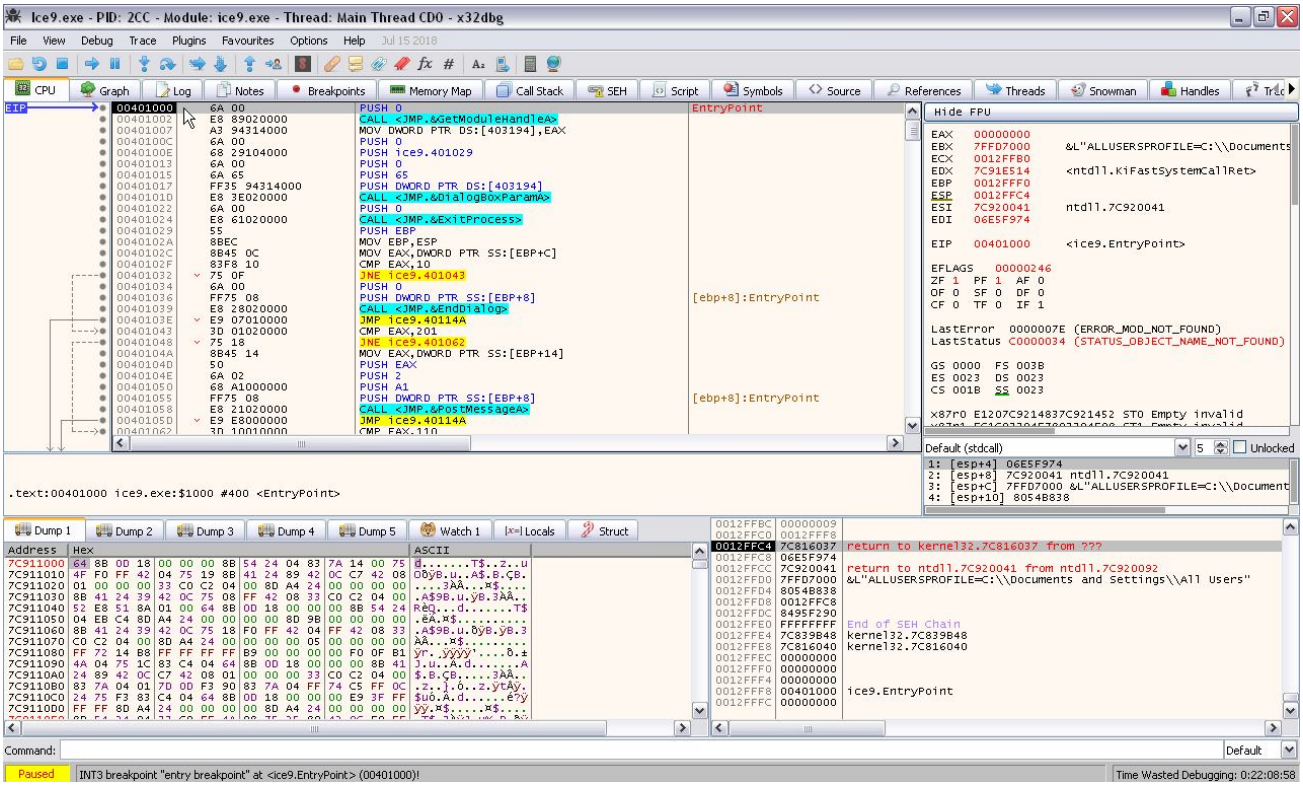
AL ATAQUE

PRIMERA MISIÓN

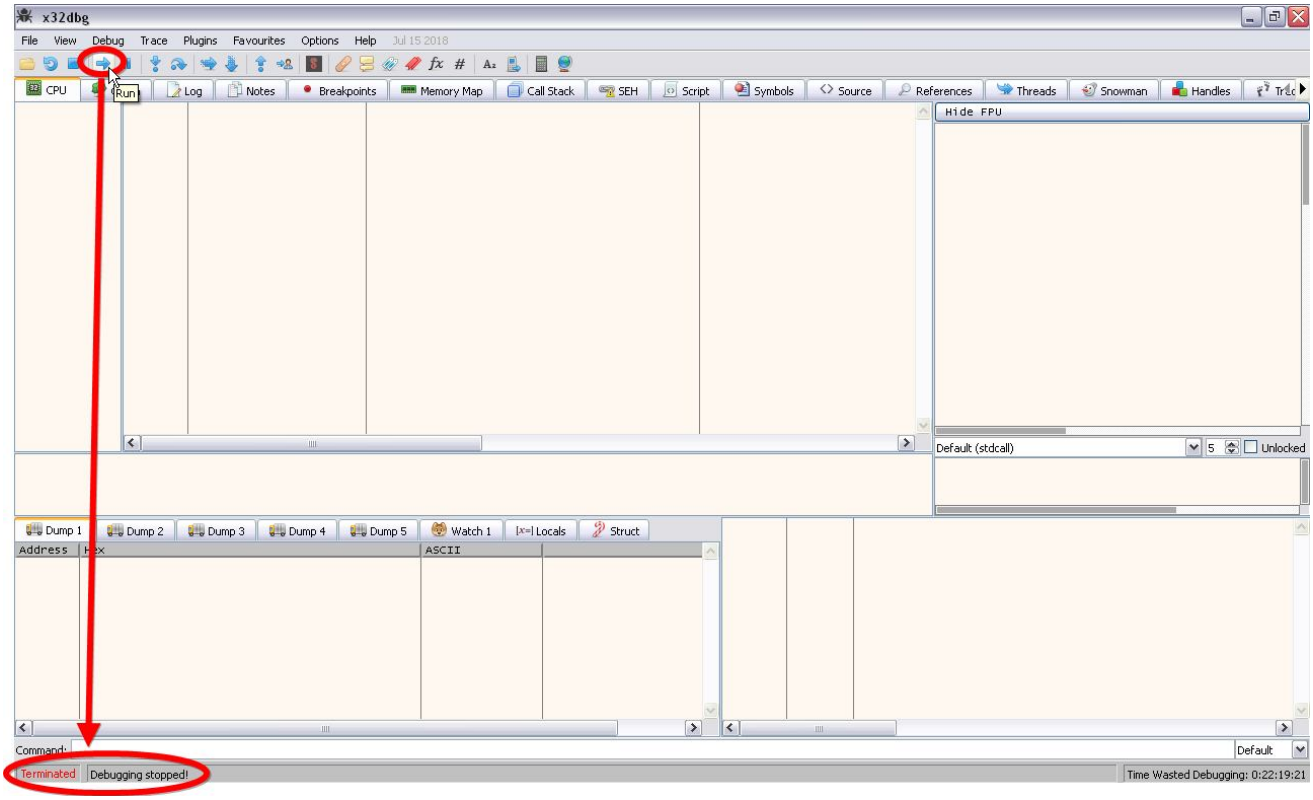
Sortear el chequeo/protección de la APIs "IsDebuggerPresent" usando la Tool "x32dbg"



Cargamos el Crackme arrastrándolo y soltándolo directamente sobre "x32dbg" y aparecemos aquí

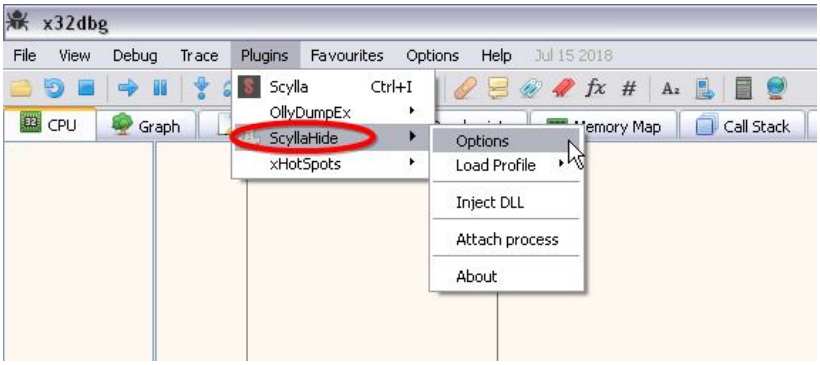


Damos "run", y efectivamente nos saca fuera. Esto quiere decir que el detector "RDG" tenía razón, este bicho tiene algo metido dentro que cuando detecta que lo estamos debuggeando nos echa, sin más…

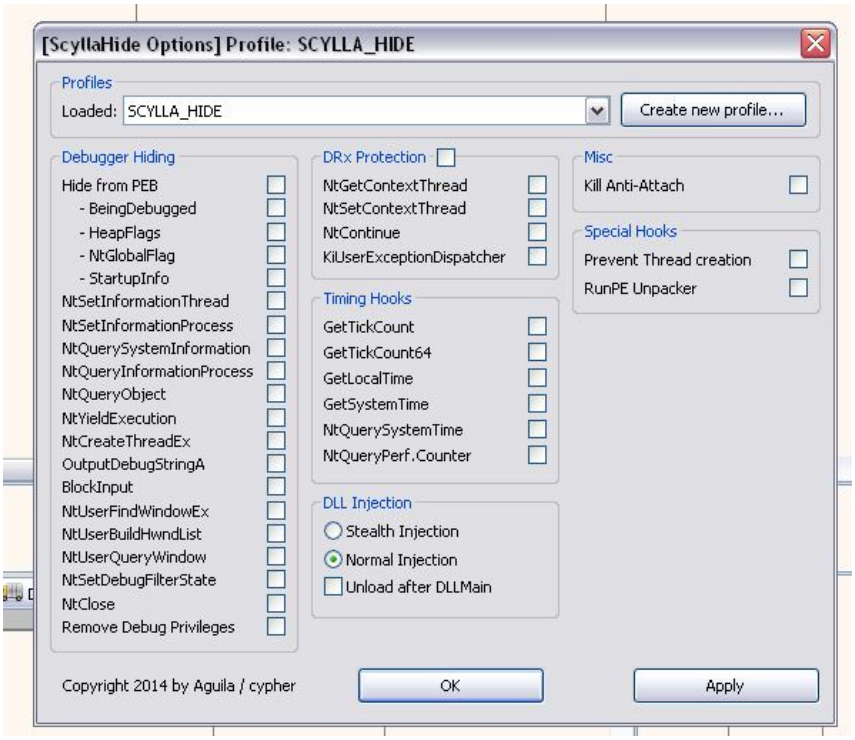


Ahora vamos a comprobar si el plugin "ScyllaHide" realmente sirve para nuestra pretensión tal y como me indicó un miembro del grupo.

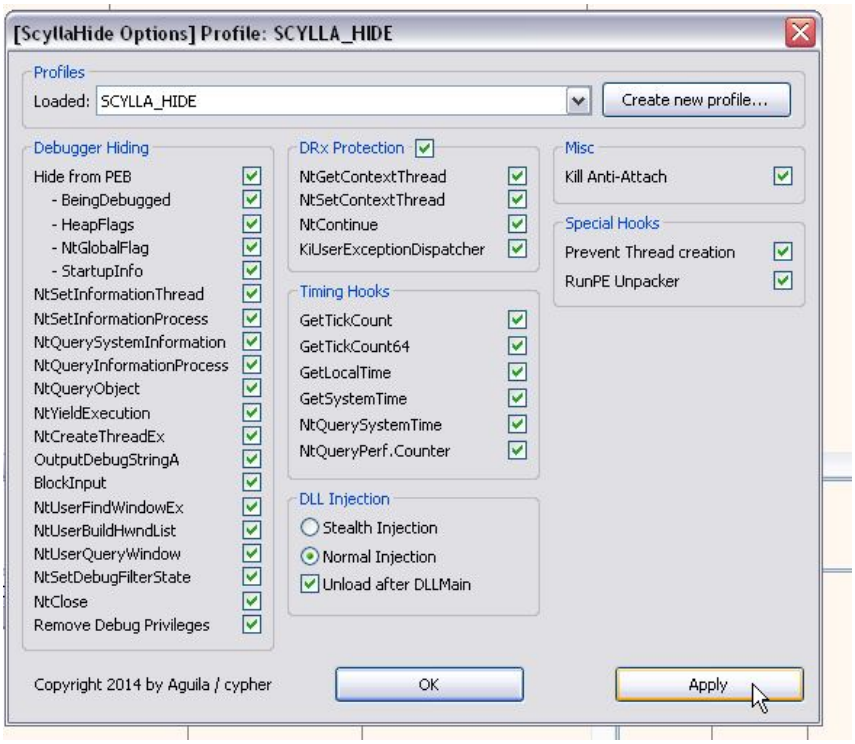
En sus "Options"



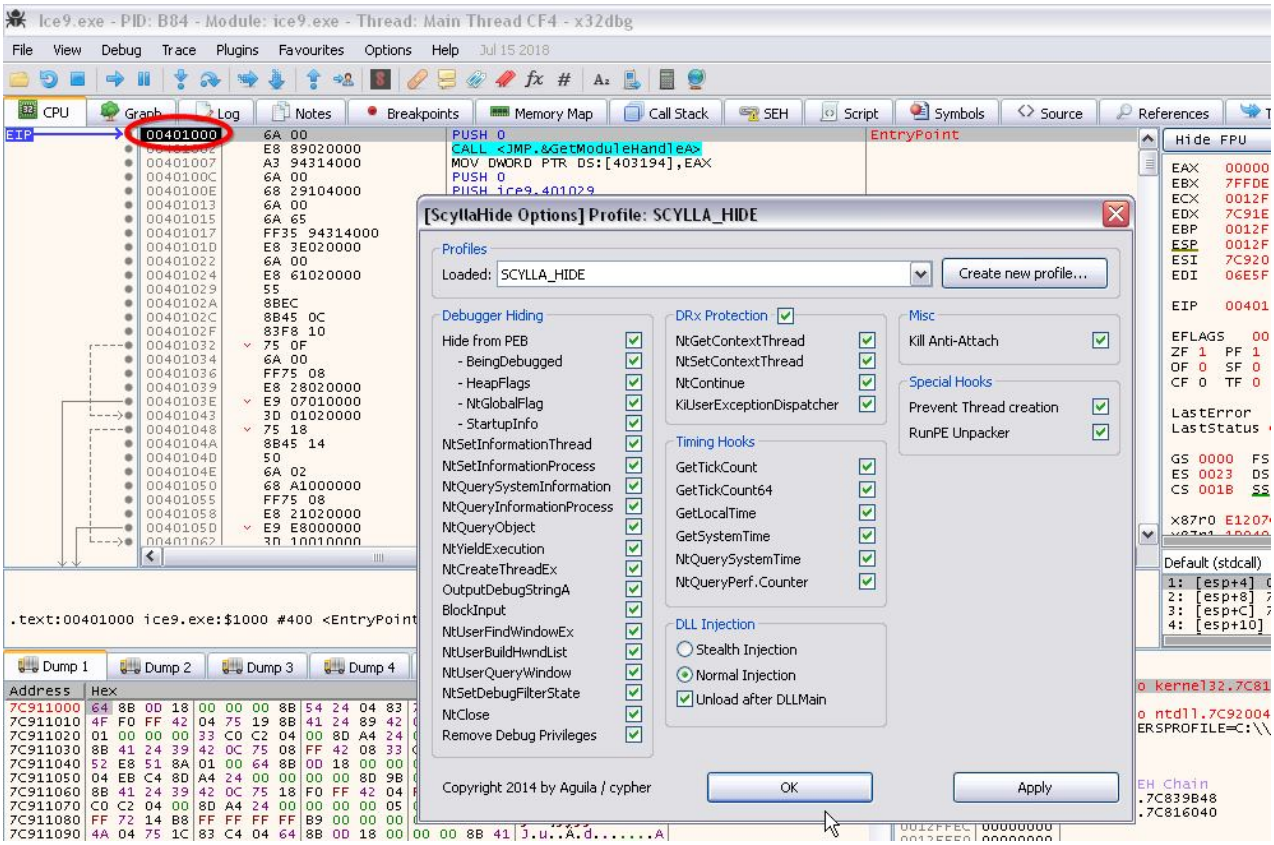
NO encuentro ninguna referencia a "IsDebuggerPresent",



Pues…… lo que se me ocurre es ir a lo bruto…..., y las tildo todas

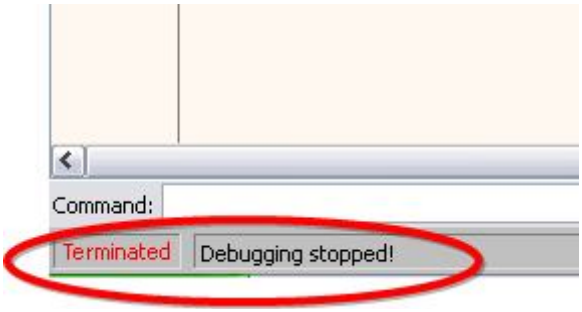


Aplicamos los cambios, cargo de nuevo el "Crackme", verifico también que todas las opciones del plugin " ScyllaHide" siguen tildadas

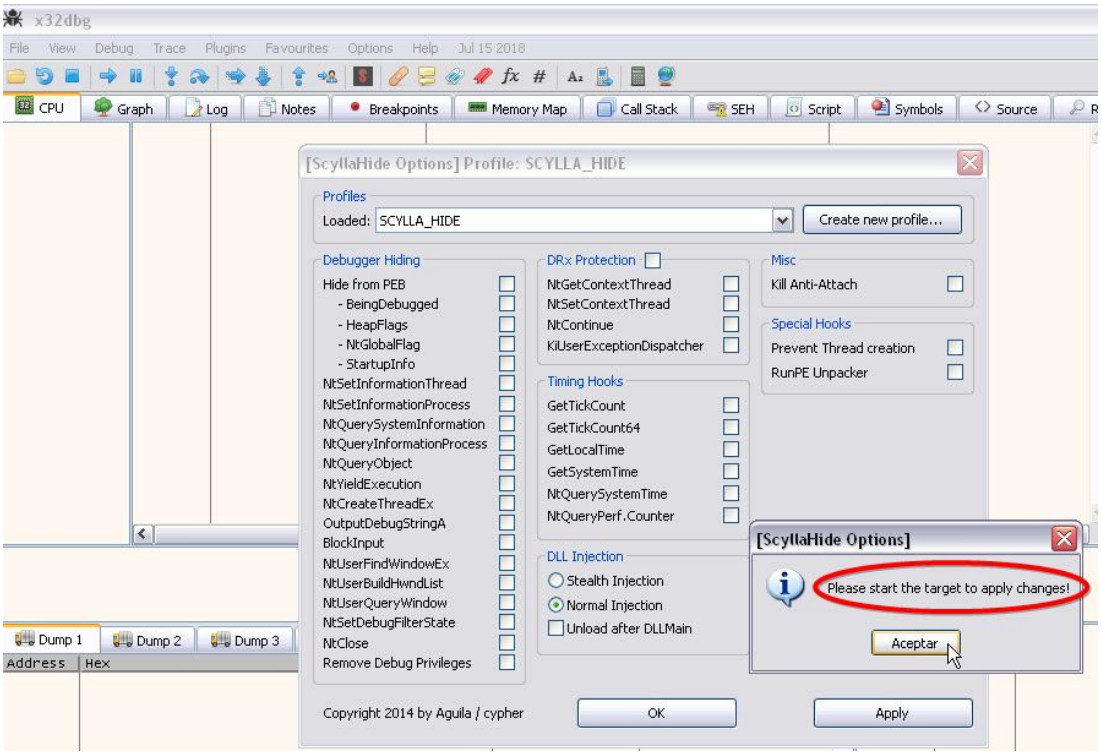


Le damos a "run" y……

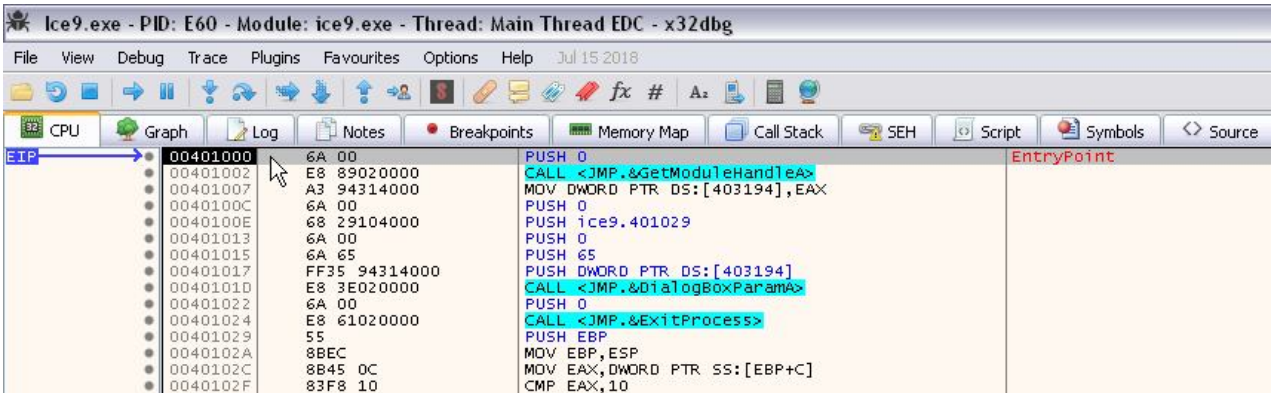
Una vez más nos vuelve a echar fuera….GGGGrrrrrrr……. de lo que deduzco que este plugin quizá su cometido es ocultar únicamente la tool Scylla, ya que el chequeo de la APIs "IsDebuggerPresent" del Crackme en cuestión no lo ha nopeado para nada y sigue presente en las entrañas del Crackme.



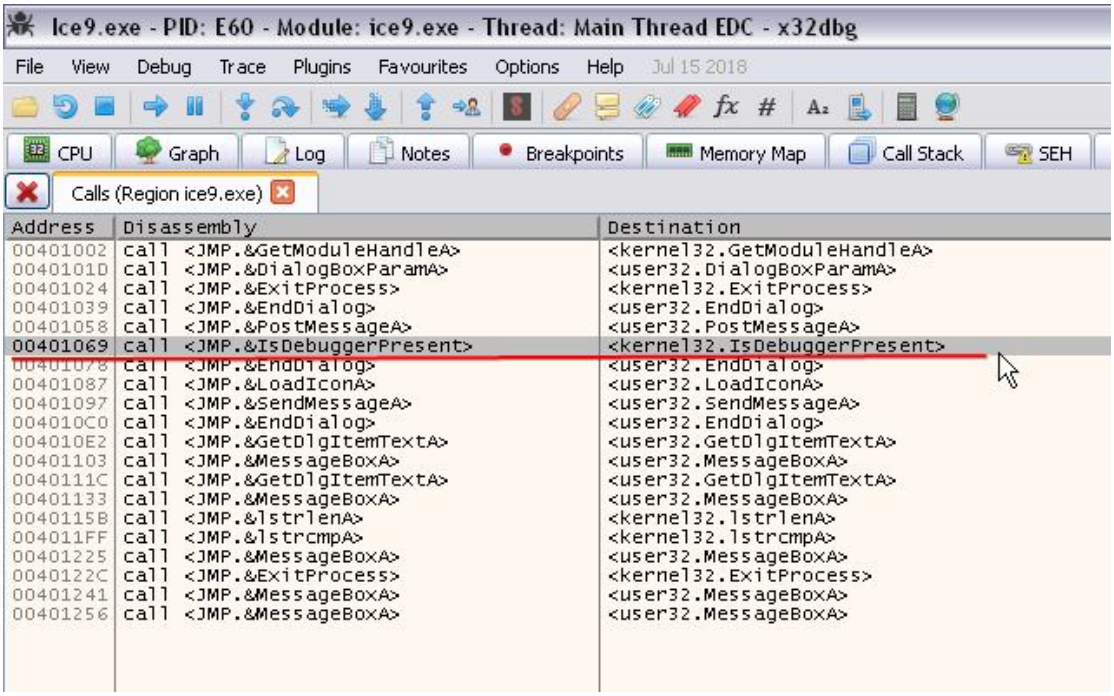
Ahora que hacemos……, pues lo primero vamos a dejar sin efecto el plugin "ScyllaHide" ya que no nos ha servido para el fin que buscamos, y procedemos a destildar todas sus opciones



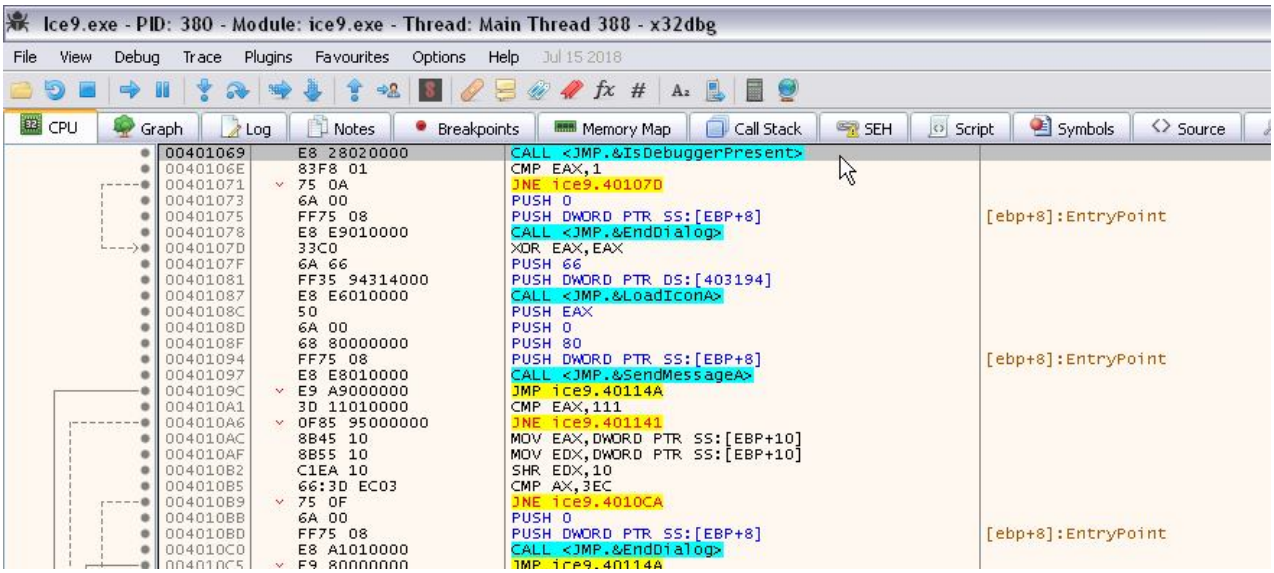
Aceptamos, y salimos totalmente de "x32dbg" para que se apliquen bien los cambios. Arrancamos de nuevo con nuestro "Crackme", y aquí estamos de nuevo:



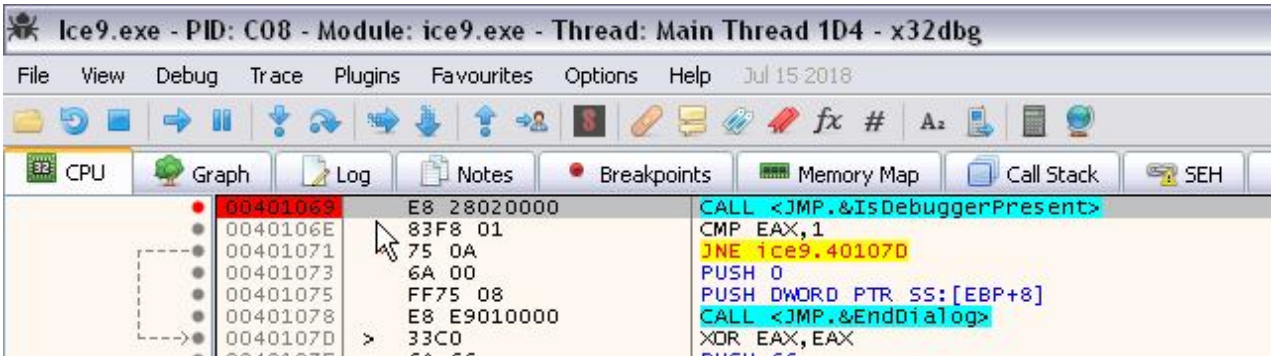
Miramos las APIs, y vemos la que nos interesa



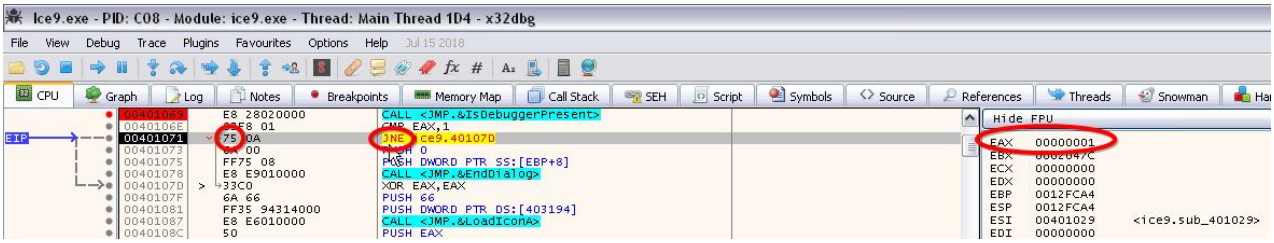
Nos posicionamos sobre ella, dos clics Izquierdo de ratón y aparecemos en la address "00401069" "CALL <JMP.&IsDebuggerPresent>" precedida de un "CMP EAX,1" y de un salto condicional "JNE" "…… muy sospechoso….



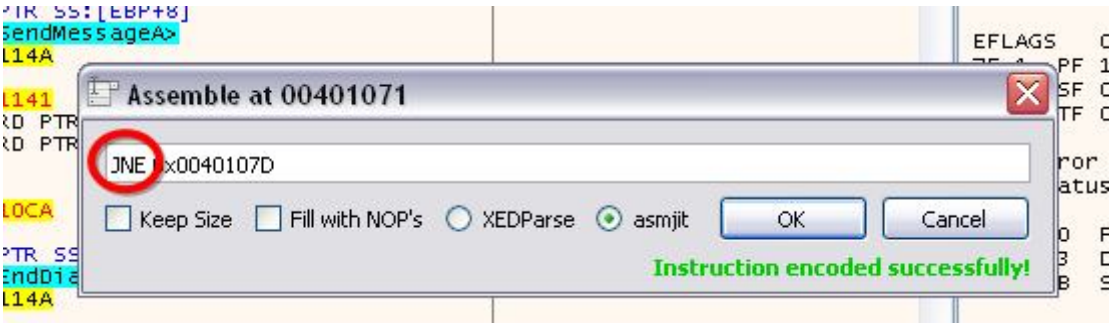
Vamos a ponerle un "BP" a esa "Call"



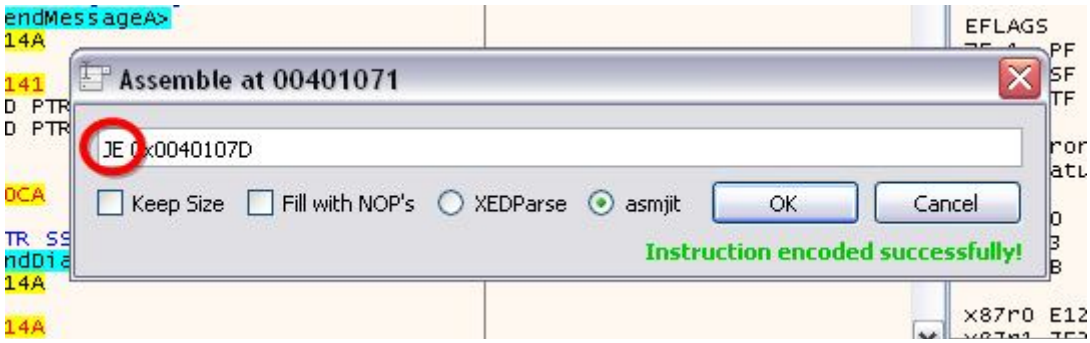
Damos "run" y parados en el "BP", traceamos hasta el salto condicional y vemos que el valor del registro "EAX" es "1"



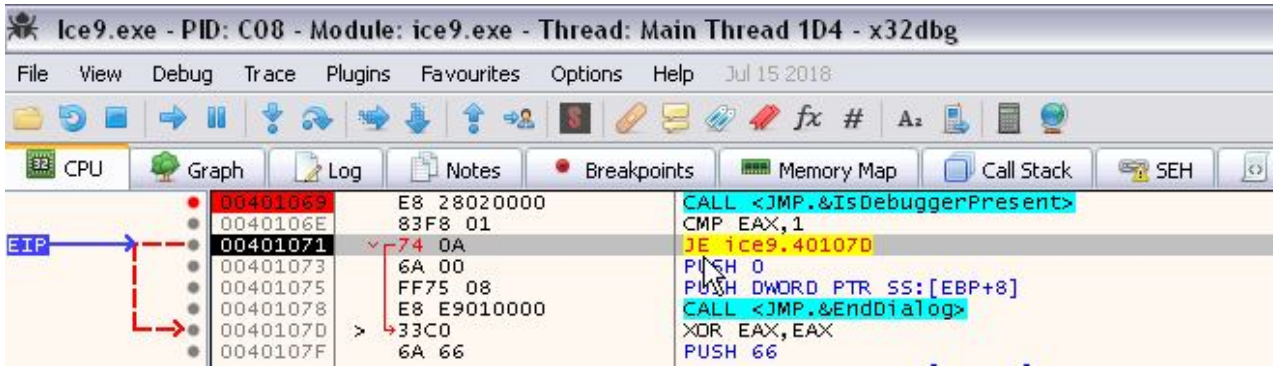
Cambiamos la condición :



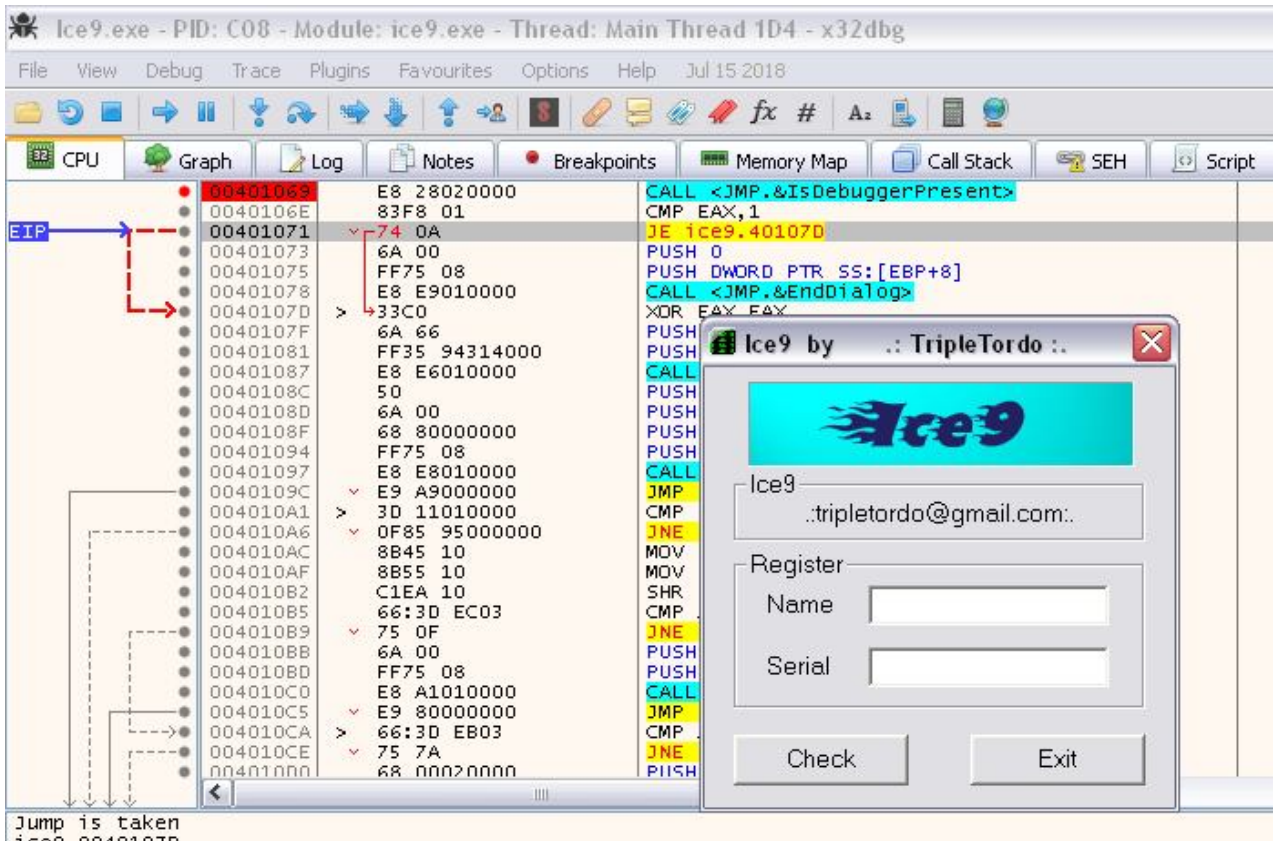
Por



Y nos queda así



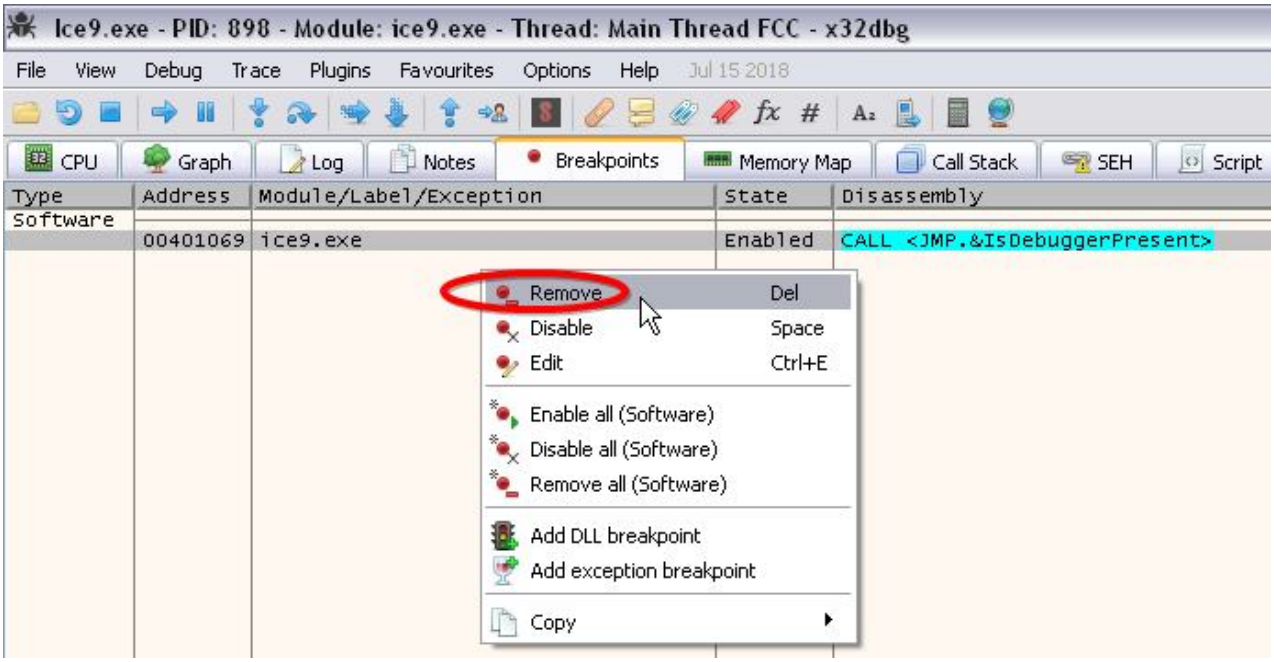
Damos "run" y observamos que hemos sorteado el Chequeo de la APIs "IsDebuggerPresent".



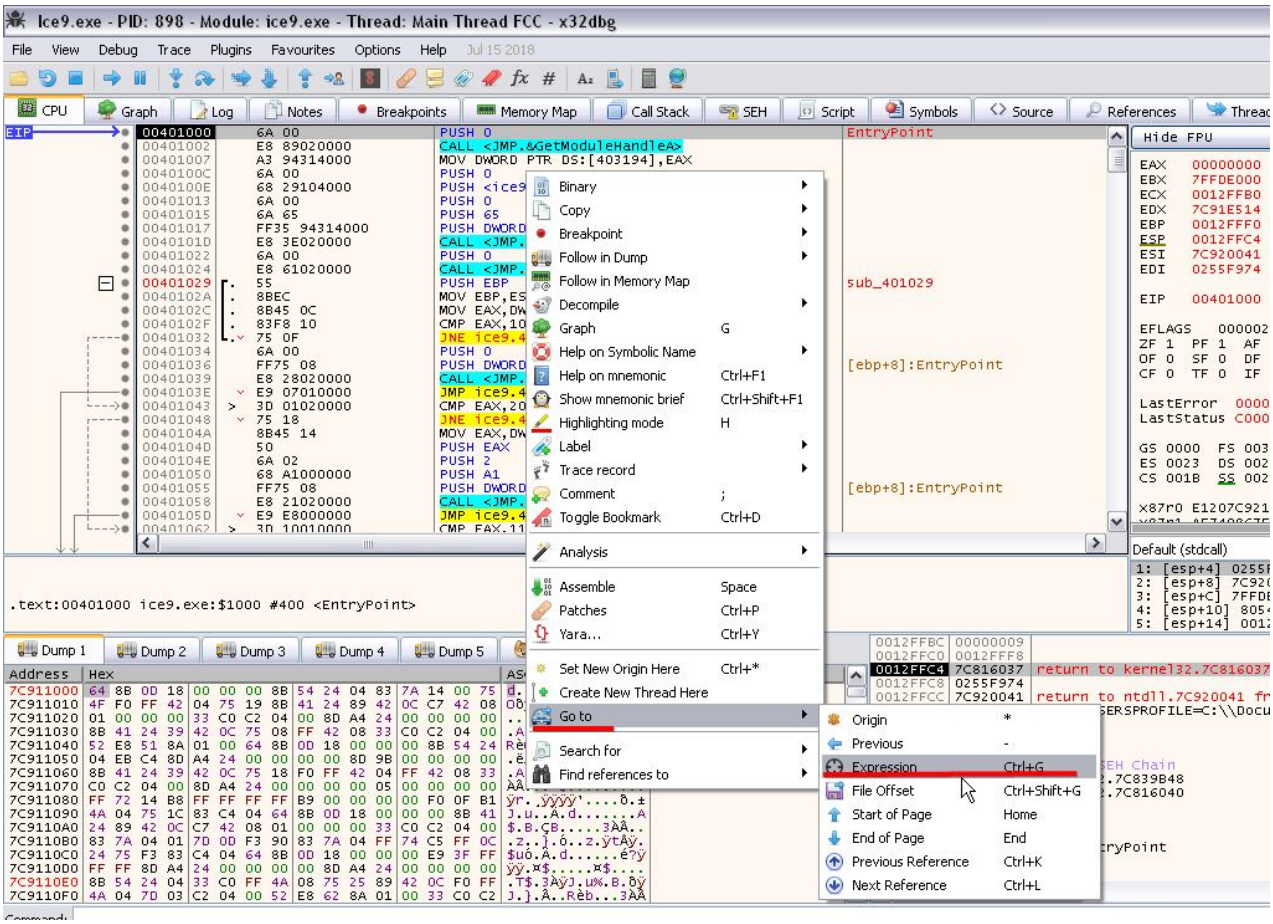
Bien, ahora, sin guardar ningún cambio vamos a aprender a sortearla con el método que me indicó el maestro Solid, tal como les avancé al principio; el cual me dijo textualmente:

Solo dirígite con "ctrl+g" al registro "fs:[30]" o "gs:[60]" (según sea 32 o 64 bits) y cambia el 01 a mano desde el "EP" del programa y listo !

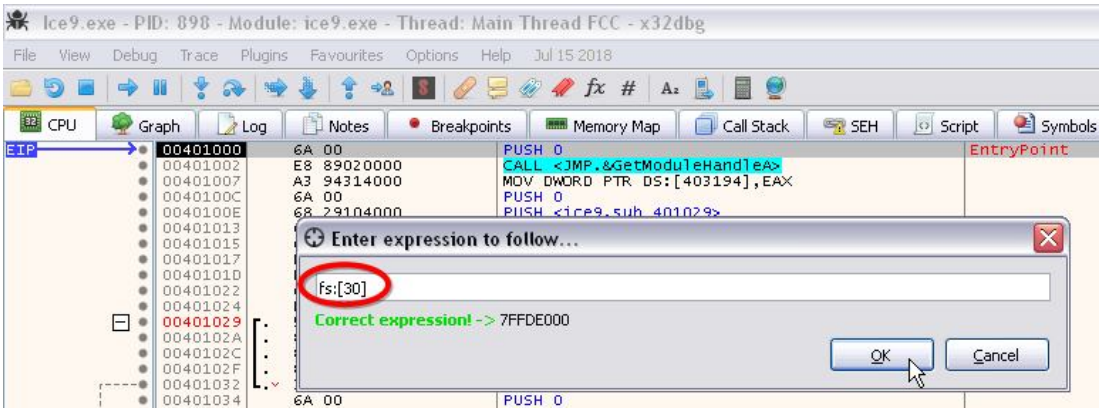
Pues manos a la obra, reiniciamos el Cracmke, y nos encontramos de nuevo parados en el "Entry Point", nos vamos a la lista de "BP" y borramos el único que tenemos puesto



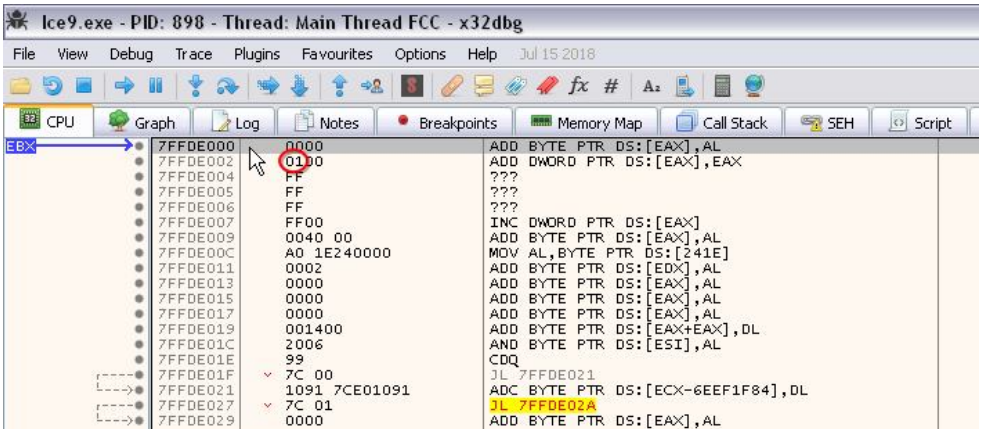
Volvemos a la ventana principal del desensamblado, clic derecho de ratón y nos vamos a la ruta "Goto to" -> "Expresion"



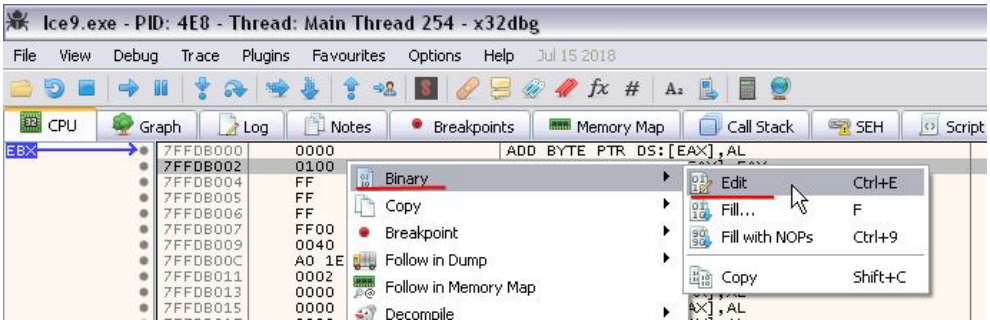
tipeamos "fs:[30]" (por tratarse de un ".exe" de 32 bits)



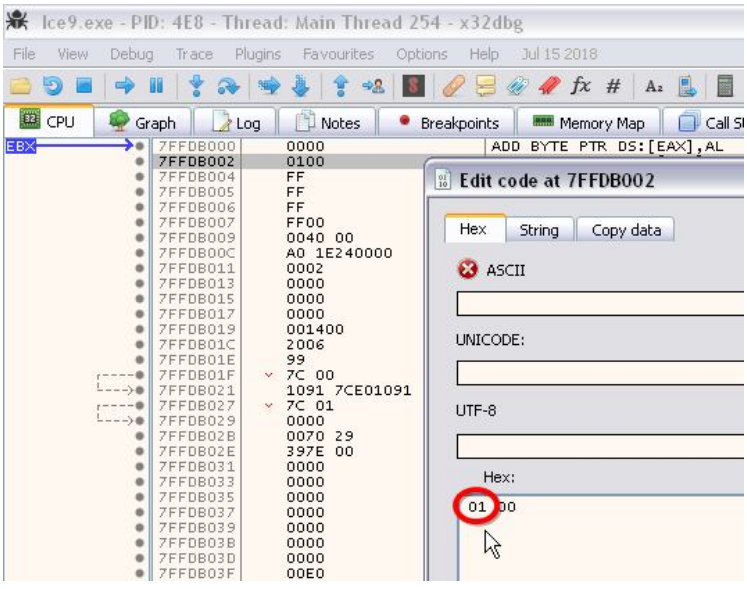
Le damos a "OK" y aparecemos aquí:



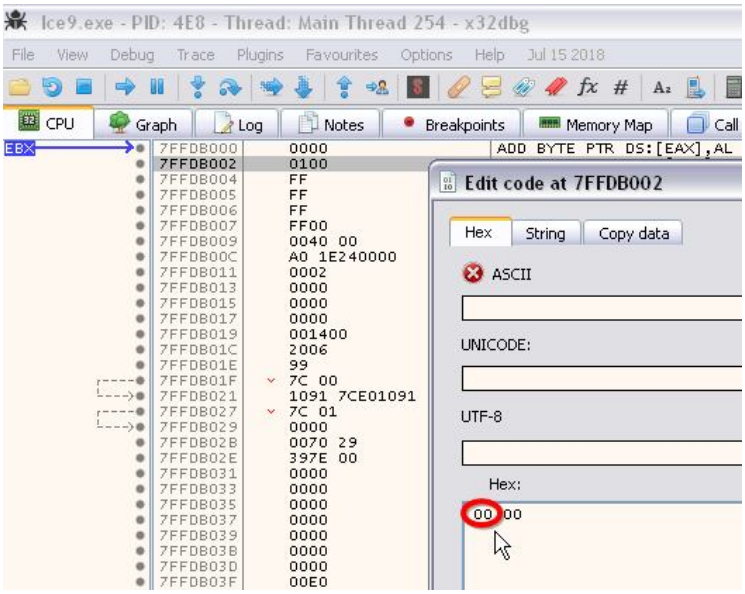
Ahora nos posicionamos sobre el valor "01" y lo cambiamos por "00"



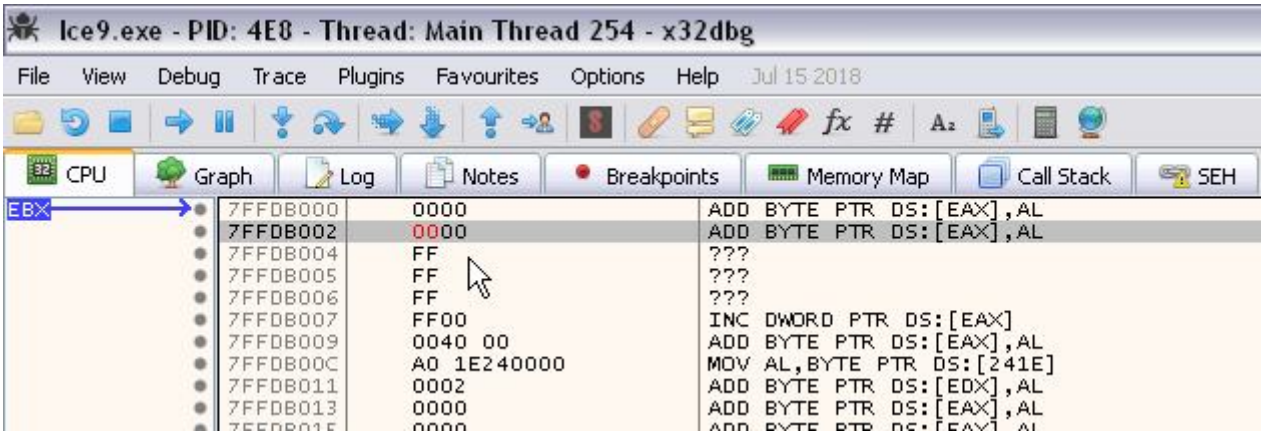
De esta forma



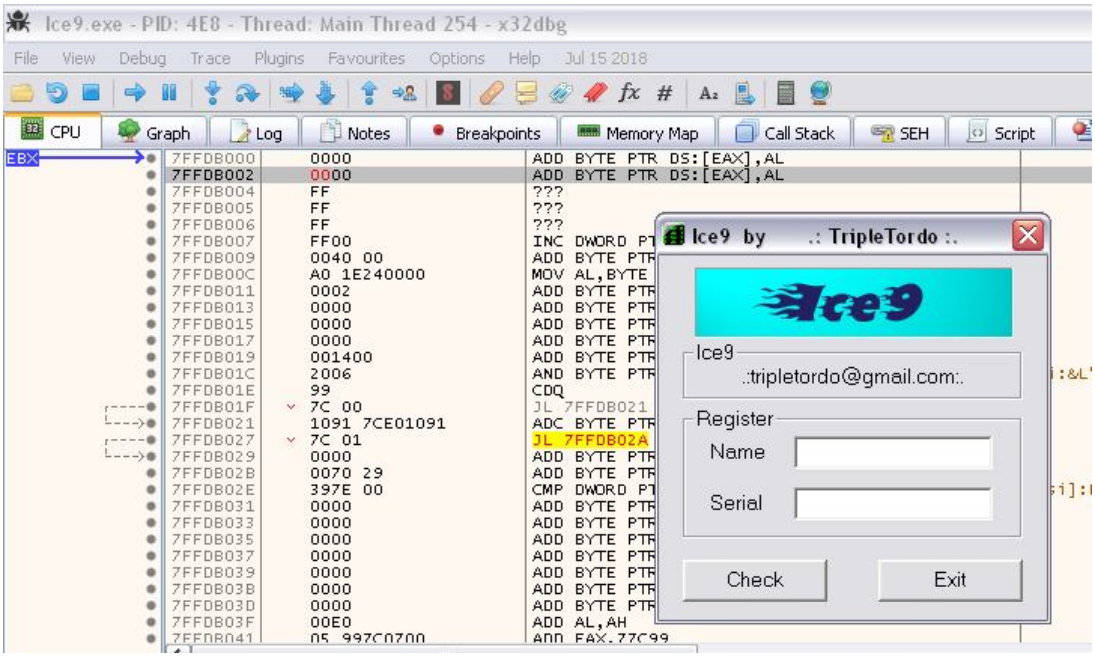
Por



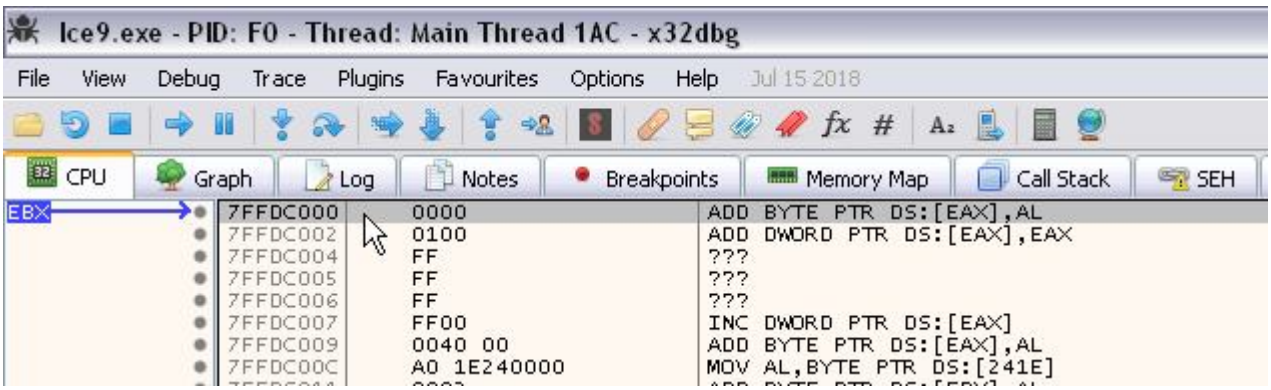
Y nos queda así:



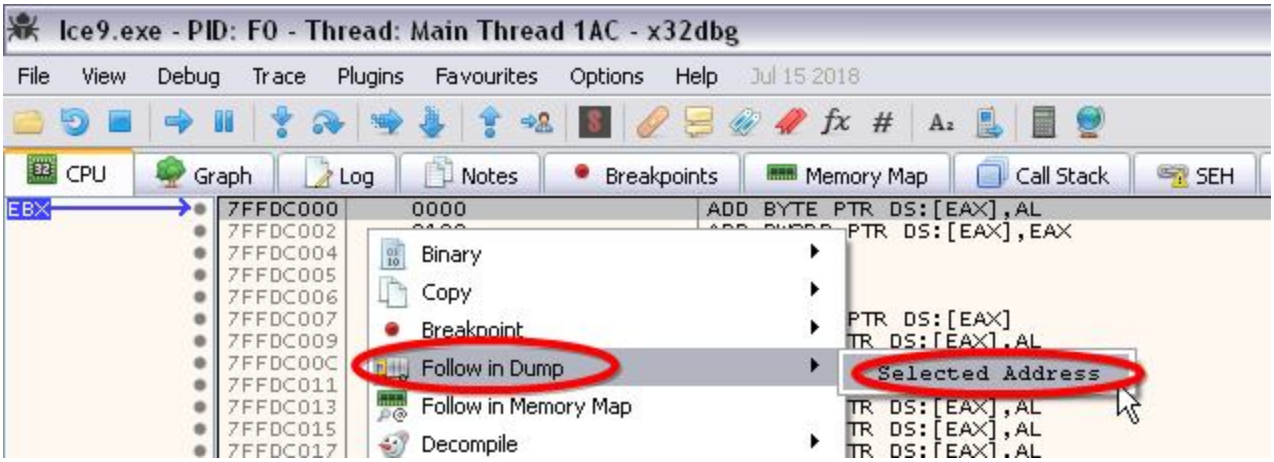
Damos "run" y con cara de satisfacción observamos que hemos sorteado el Chequeo del "IsDebuggerPresent" , y por tanto este método también ha funcionado a la perfección.



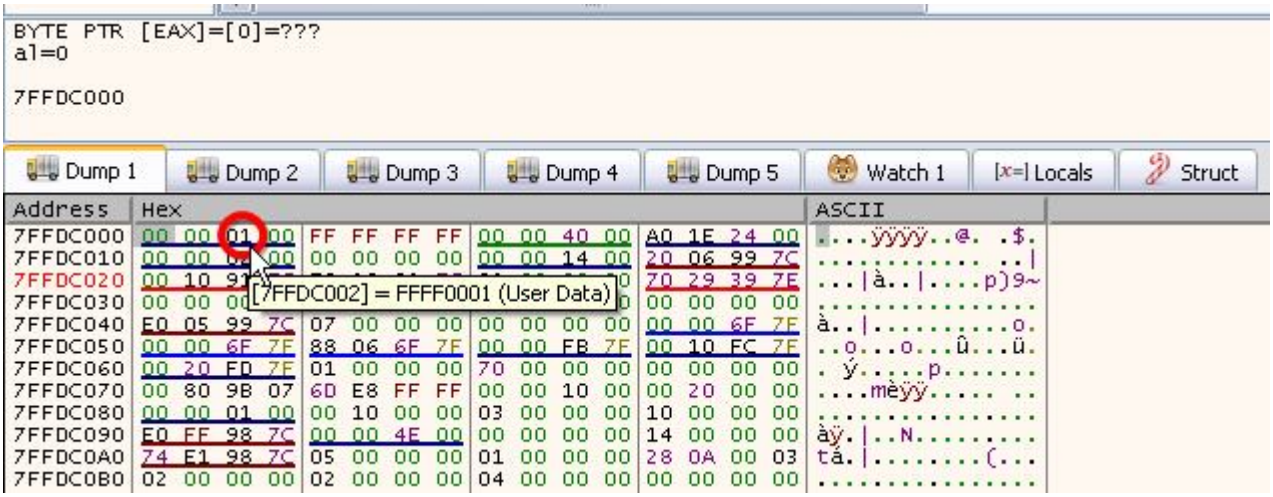
Otra manera es, siguiendo el mismo método de Solid, y cuando estamos parados en la address "7FFDC000"



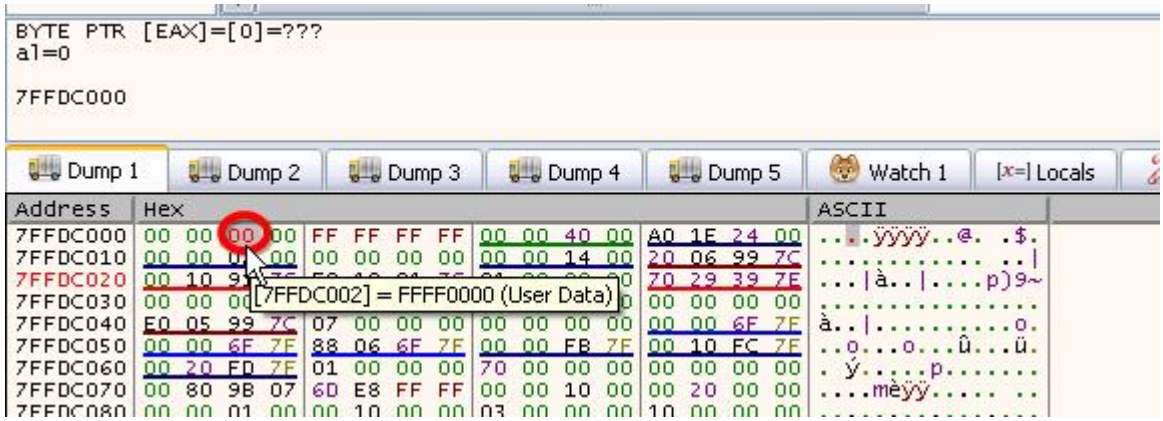
Click derecho de ratón y "Follow in Dump" -> "Selected Address"



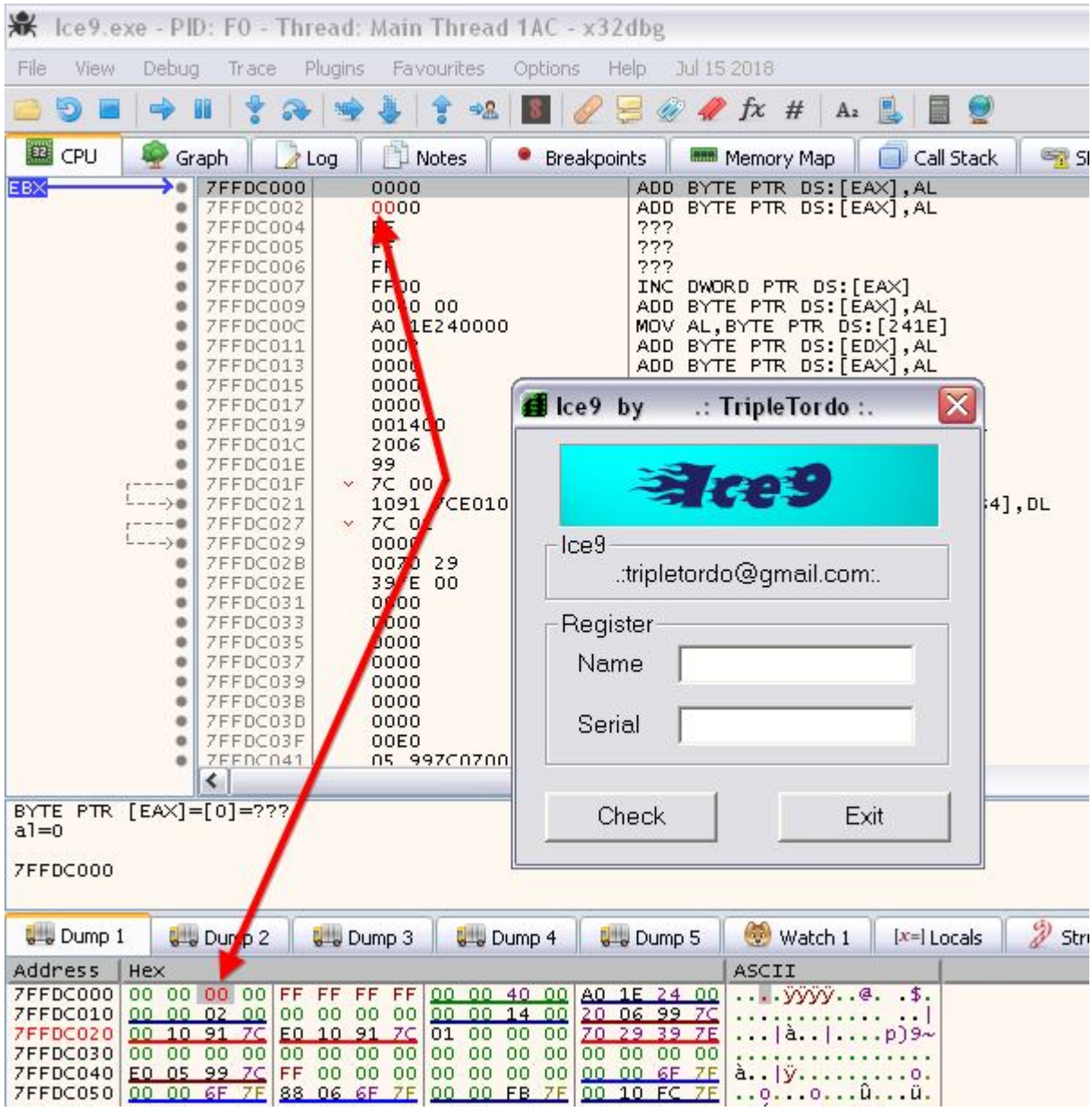
Y en la ventana "Dump 1"



Cambiamos el valor "01" por "00"



Damos "run" y oleeeee.



Bien, ahora ya podemos buscar un "Serial" para nuestro "Name".

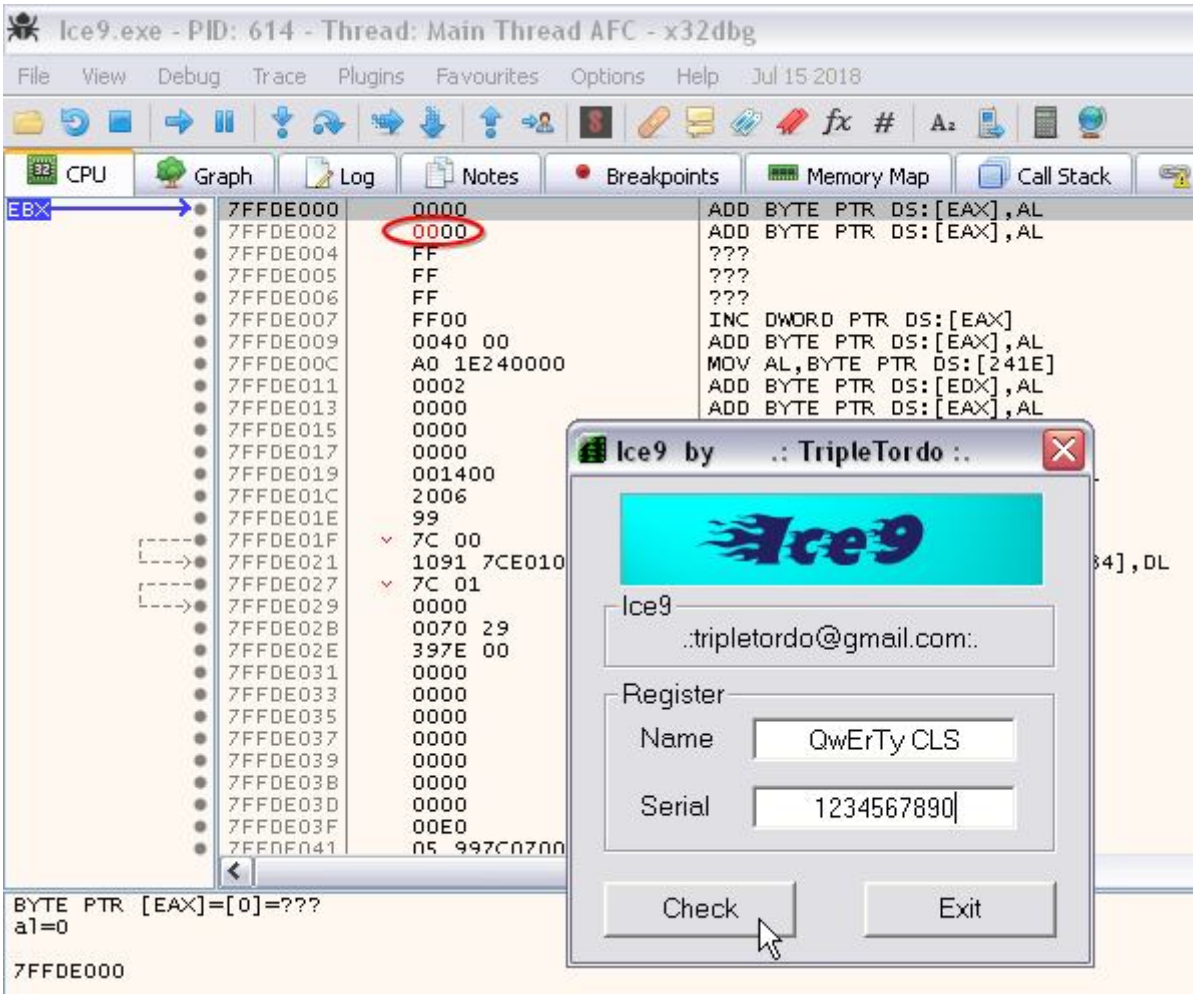
SEGUNDA MISIÓN

Registrarnos

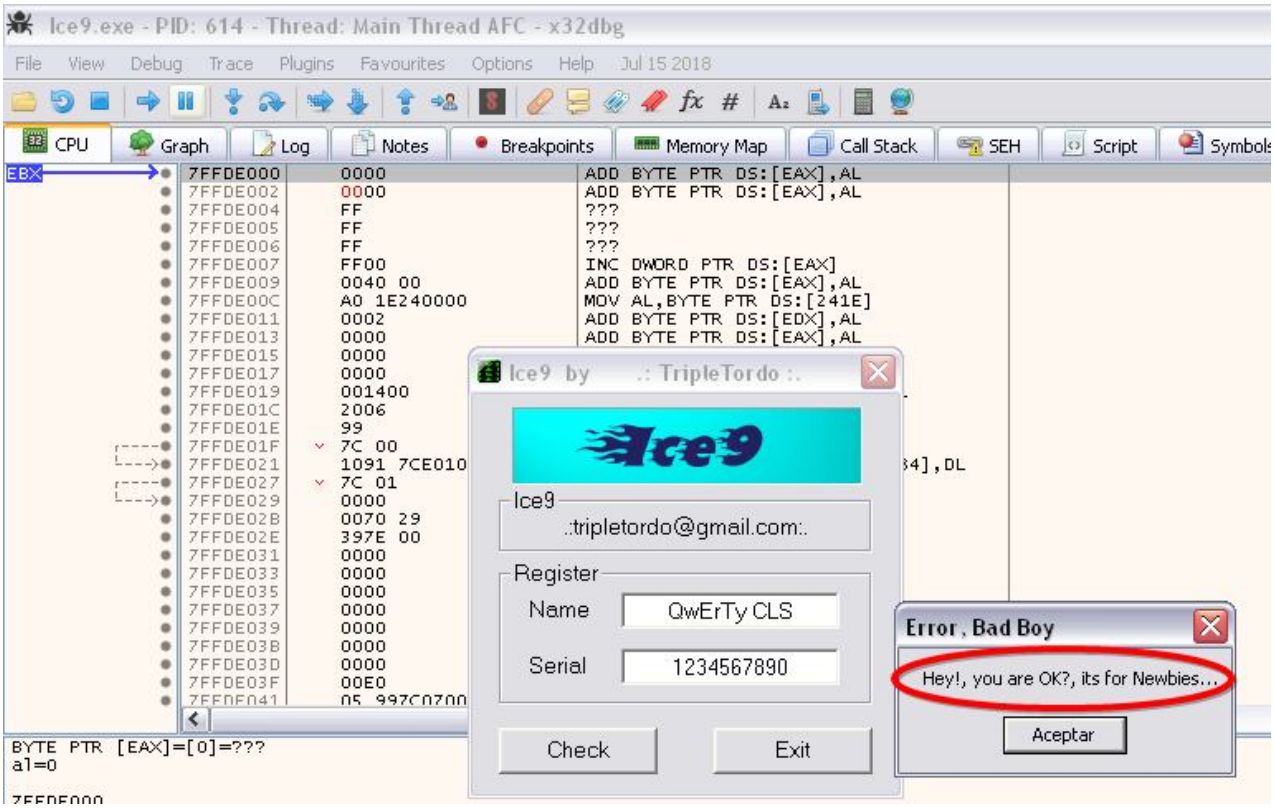
Este Crackme es para principiantes y es sumamente fácil encontrar un Serial válido.

Como siempre hay muchas maneras pero esta vez voy a mostrarles como hacerlo poniendo en práctica el método del maestro TENA, y que Ariel también utilizó en su último tute al solucionar los crackmes de AbelJM

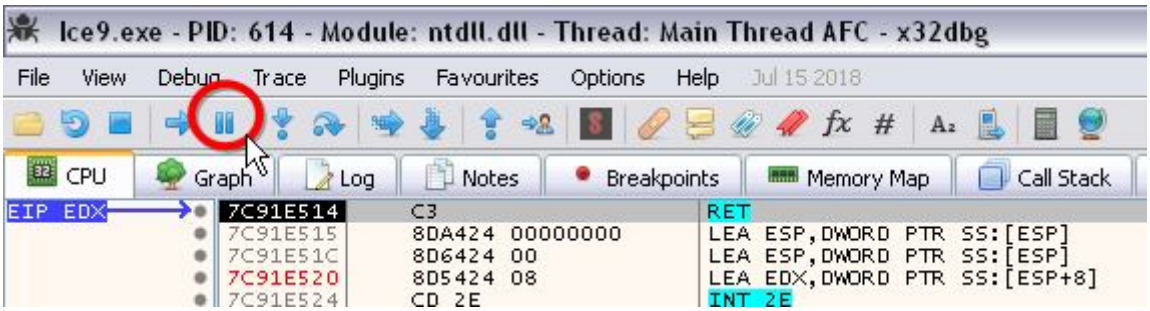
Rellenamos datos



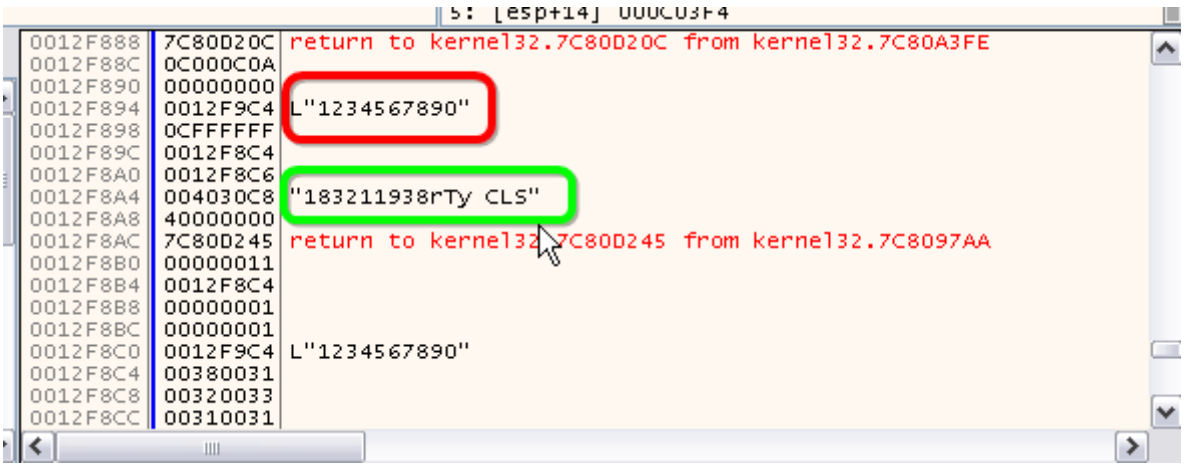
Le damos a "Check", y nos salta el mensaje de "Chico malo",



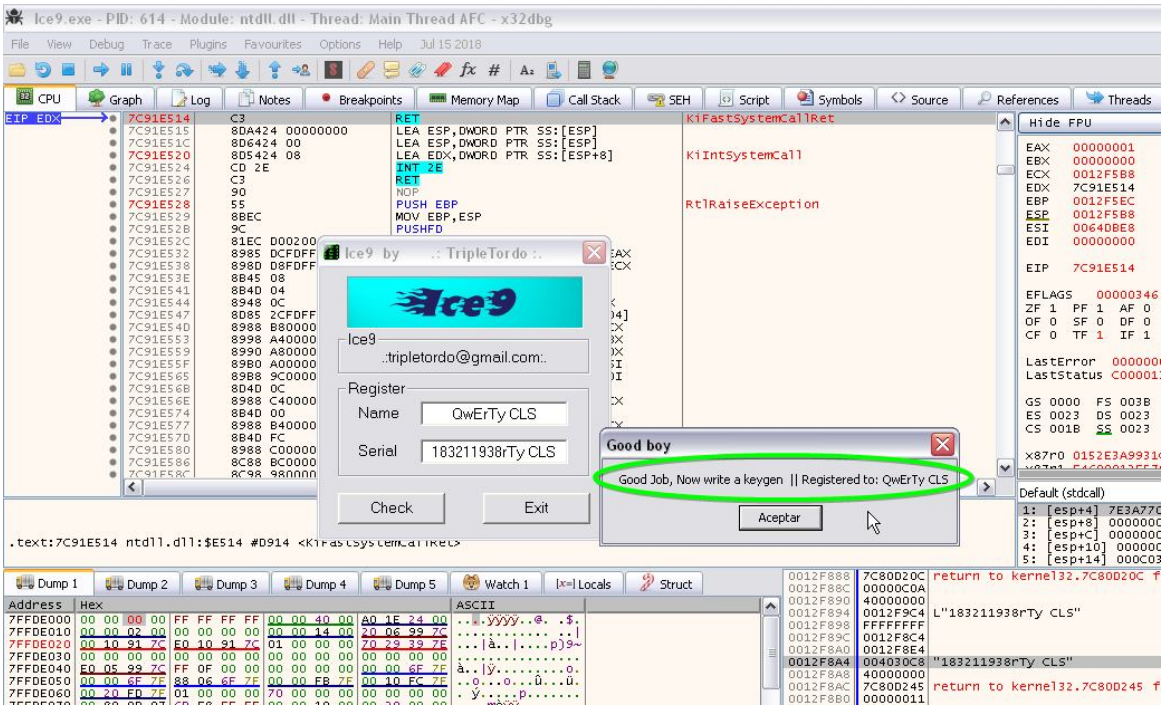
Ahora, sin más, le damos a "Pause" para parar el proceso,



Nos dirigimos a la ventana "Stack" y simplemente haciendo "scroll" hacia abajo encontramos lo que parece la solución



Probamos…… y ……



Crackme felizmente Solucionado.

Pero sigo sin encontrar un plugin para la tool "x32dbg", que desactive de forma automática el chequeo de la APIs "IsDebuggerPresent" cuando un .exe es debugeado.

en fin…., seguiré buscando…

……MISIÓN CUMPLIDA……

Mis agradecimientos infinitos

Al grandísimo RICARDO NARVAJA, y a todo el grupo CracksLatinoS

> ***No hay viento favorable para el que no sabe a qué puerto se dirige***
>
> ***Séneca***

Salu2

<< QwErTy CLS>>

26 de Julio de 2018