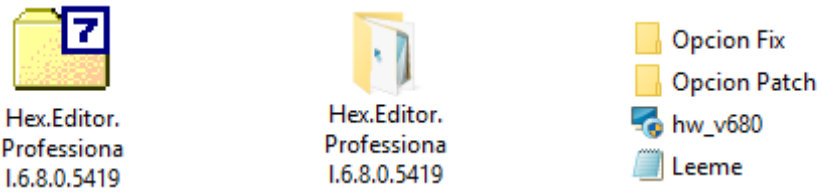
Aplicación	*Hex Workshop Hex Editor Pro v6.8.0.5419 (Editor Hexadecimal)*
Misión	*Hacer un Patch para reparar un pequeño detalle que me encontré al registrar la aplicación usando el "Fix" de Embrace en un SO Windows 10 (64bits)*
Compilado	*Microsoft Visual C++*
Protección	*Ninguna*
Herramientas	*RDG Packer Detector v0.7.6 - X64dbg*
Sistema Operativo	*Windows 10 Home (64bits)*
Cracker	*QwErTy*
Dedicado a	*Embrace - CrackSLatinoS*
Descargar Aplicación (Incluye Fix Embrace)	*https://mega.nz/#!7l8ljK4ZlJ5EoFuO7FBov33QutR3sEZlClMtG_KYaWQp1miigrUY*

Todo empezó cuando al instalar la Tool "Hex Workshop Hex Editor Pro v6.8.0.5419" en un SO Windows 10 Home (64bits), al registrar la aplicación utilizando la opción "Fix" de Embrace (para no pasar por caja), me encontré que una vez aplicado, al ejecutar el editor Hexadecimal vi que era totalmente funcional pero cada vez que lo iniciaba aparecía una molesta "Nag" que finalmente he conseguido que no aparezca. He decidido compartir este pequeño trabajo, por si puede servir de ayuda a quien pueda encontrarse en la misma situación.

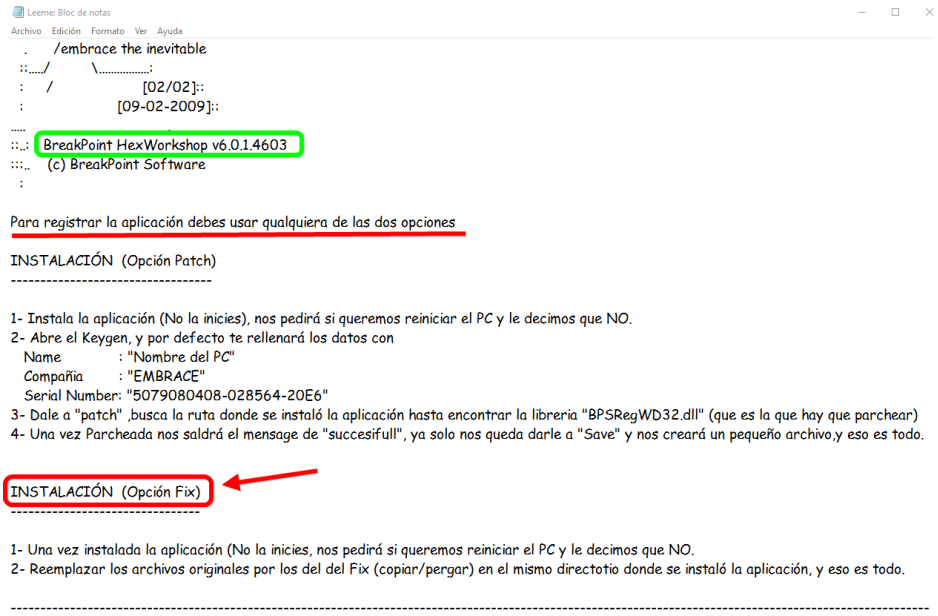
Desconozco si en otros Sistemas Operativos aparece el mismo problema una vez aplicado el Fix, pero les aseguro que con Windows 10 Home (64bits) sí que aparece la "Nag", y vamos a solucionarlo.

EMPECEMOS POR EL PRINCIPIO

Bajamos la aplicación del link arriba indicado, descomprimimos (no tiene contraseña), y obtenemos los siguientes archivos;



Abrimos el "Leeme",


Leeme: Bloc de notas

Archivo Edición Formato Ver Ayuda

. /embrace the inevitable
::...../ \.....:
: / [02/02]::
: [09-02-2009]::
.....
::..: BreakPoint HexWorkshop v6.0.1.4603
:::.. (c) BreakPoint Software
:

Para registrar la aplicación debes usar qualquiera de las dos opciones

INSTALACIÓN (Opción Patch)

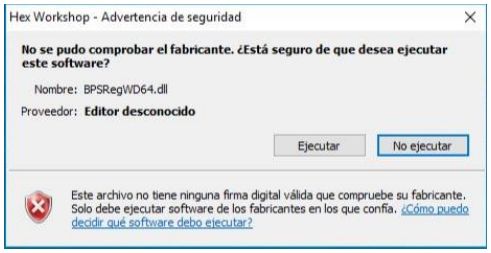
1- Instala la aplicación (No la inicies), nos pedirá si queremos reiniciar el PC y le decimos que NO.
2- Abre el Keygen, y por defecto te rellenará los datos con
Name : "Nombre del PC"
Compañia : "EMBRACE"
Serial Number: "5079080408-028564-20E6"
3- Dale a "patch" ,busca la ruta donde se instaló la aplicación hasta encontrar la libreria "BPSRegWD32.dll" (que es la que hay que parchear)
4- Una vez Parcheada nos saldrá el mensage de "succesifull", ya solo nos queda darle a "Save" y nos creará un pequeño archivo,y eso es todo.

INSTALACIÓN (Opción Fix)

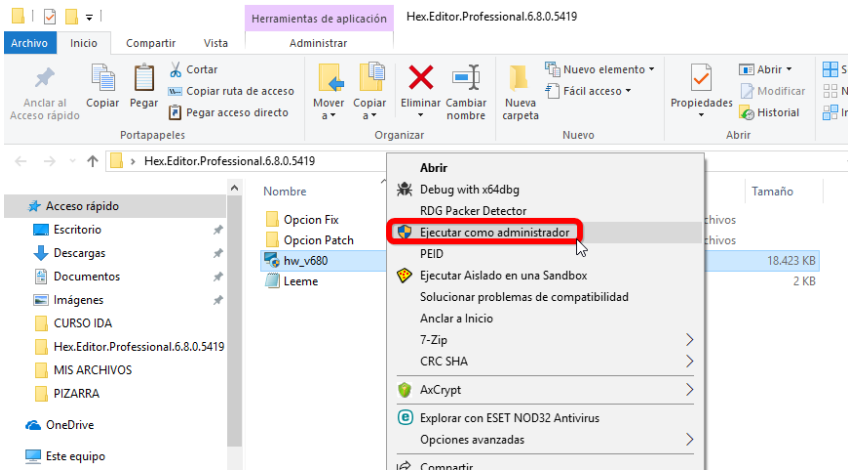
1- Una vez instalada la aplicación (No la inicies, nos pedirá si queremos reiniciar el PC y le decimos que NO.
2- Reemplazar los archivos originales por los del del Fix (copiar/pergar) en el mismo directotio donde se instaló la aplicación, y eso es todo.

Vemos que la versión de la tool descrita en el léeme v6.0.1.4603 es inferior a la que vamos a instalar v6.8.0.5419, y los que piensen que ese podría ser la causa del problema, están equivocados. <u>En este caso</u> el "Fix" no afecta a la versión.

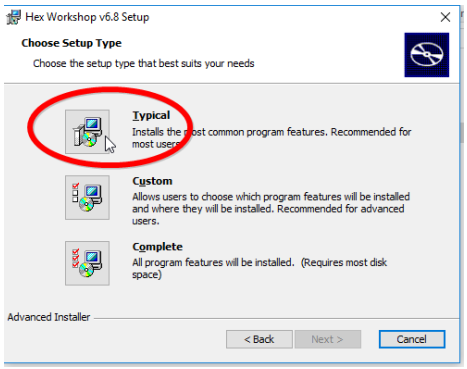
Sigamos…, yo me decanto por utilizar la (Opción Fix). *Si eligen la (Opción Patch) la aplicación estará Full, no aparecerá la "Nag" de la que les hablo, pero cada vez que inicien el editor les aparecerá esta otra ventanita que también molesta.*



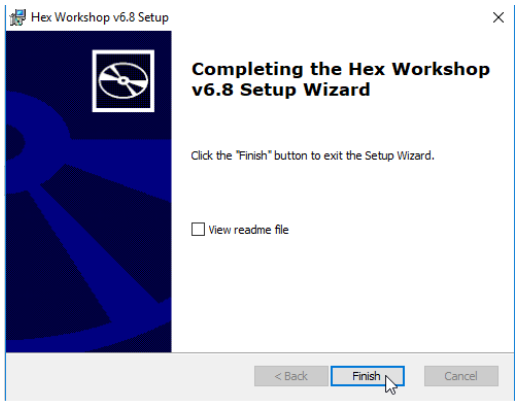
Cierro el bloc de notas, y procedo a la instalación como administrador



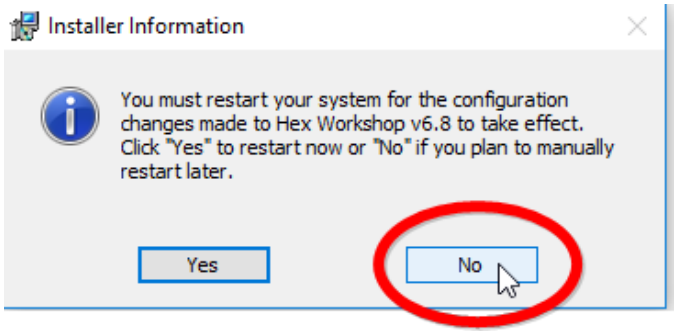
Elegimos "Typical"



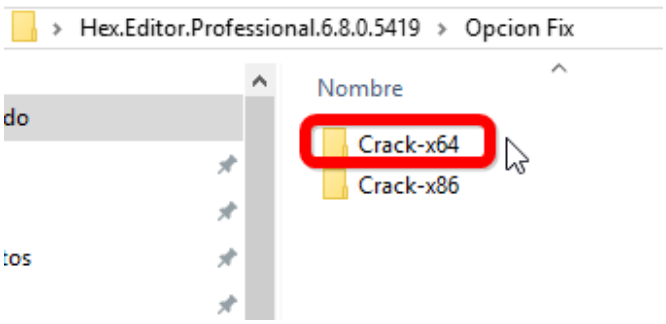
Le damos a "Finish"



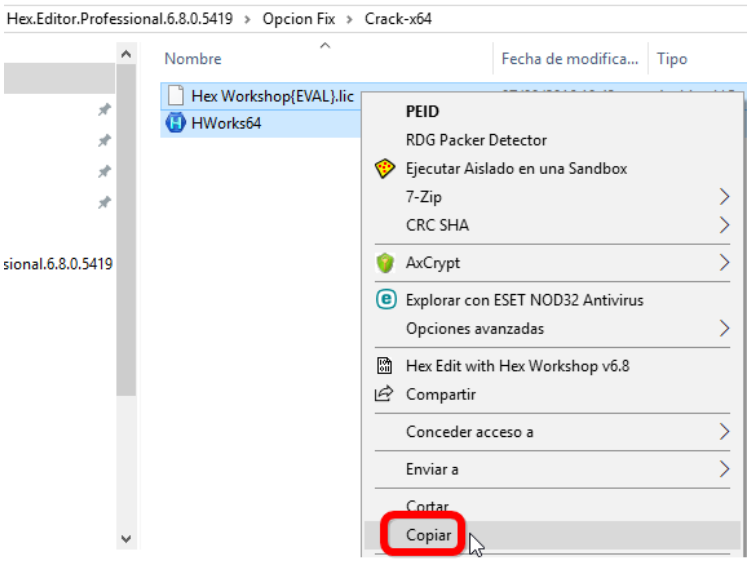
Una vez finalizada nos va a pedir si queremos reiniciar el PC para que los cambios que hemos hecho surtan efecto y le decimos que "No" , que ya lo reiniciaremos manualmente más tarde.



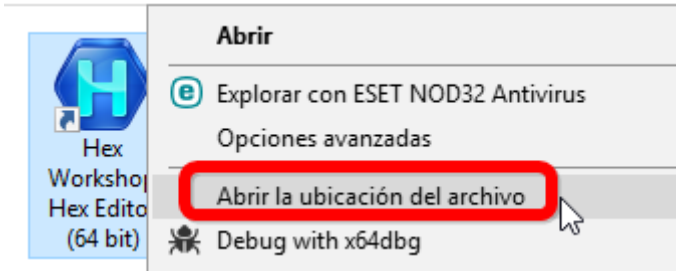
Nos vamos a la carpeta "Fix", entramos dentro de "Crack-x64"



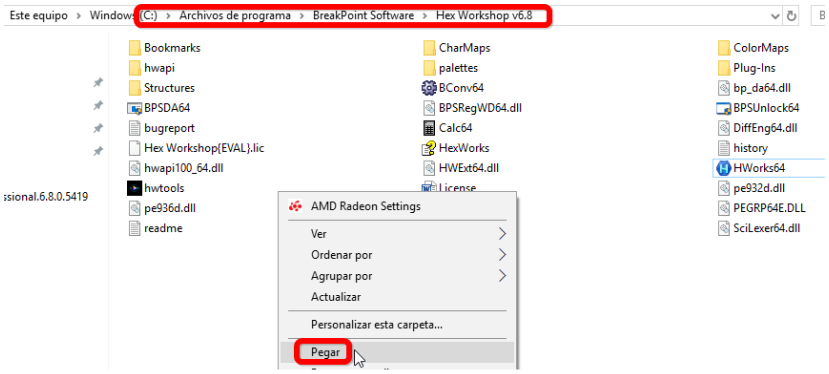
Copiamos los dos archivos que contiene



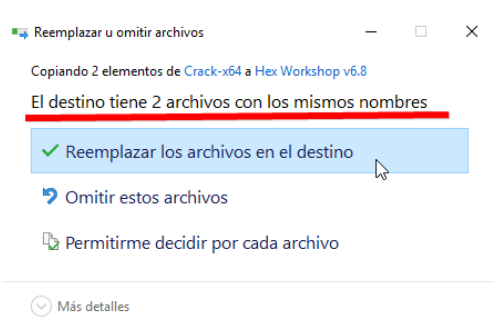
Ahora en el escritorio, nos posicionamos sobre el icono de acceso directo que automáticamente nos ha creado el instalador, "Click" derecho de ratón y nos vamos a la ruta donde se ubica la aplicación.



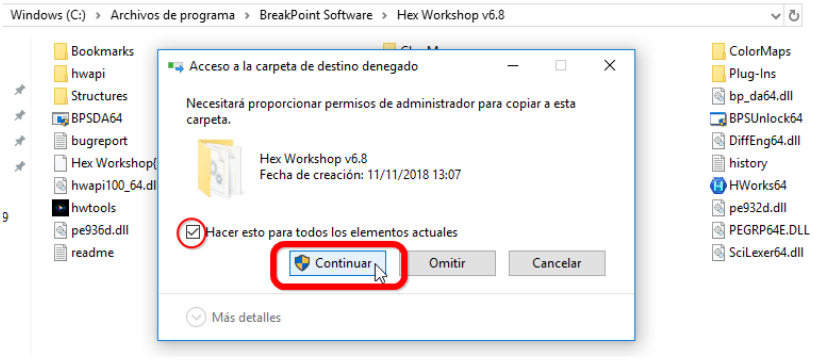
Aquí, substituimos los dos archivos originales



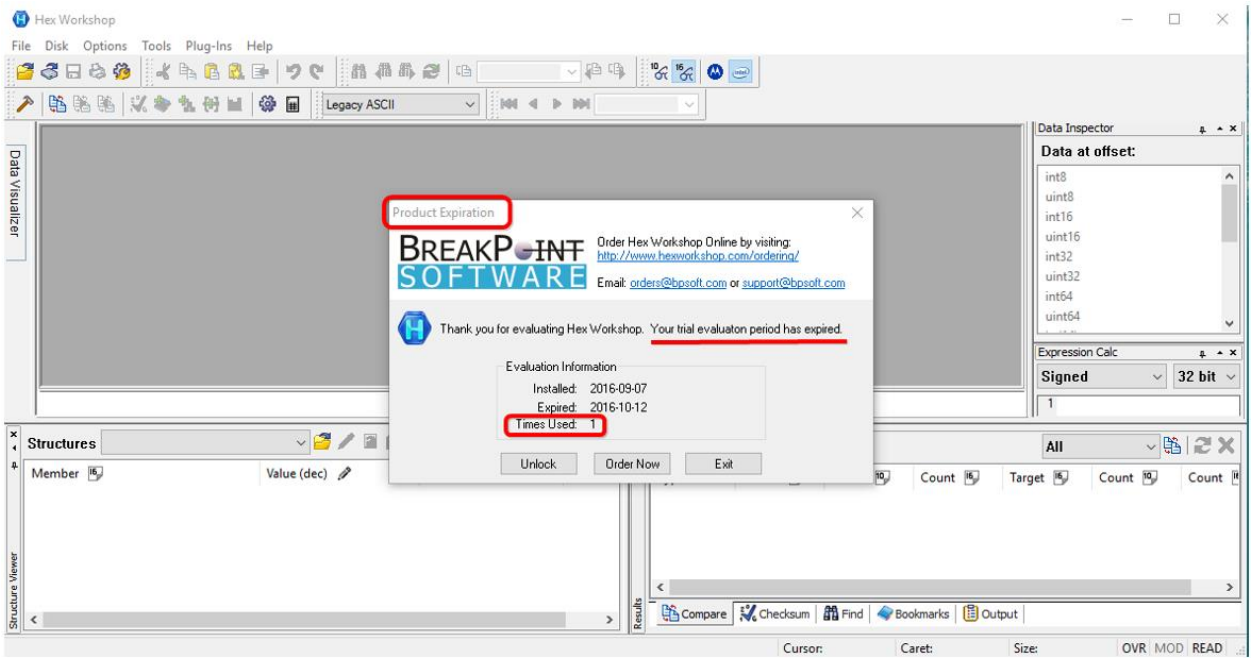
Nos dice que ya existen 2 archivos con los mismos nombres y los Reemplazamos



Le damos permisos de administrador, y clicamos en "Continuar"

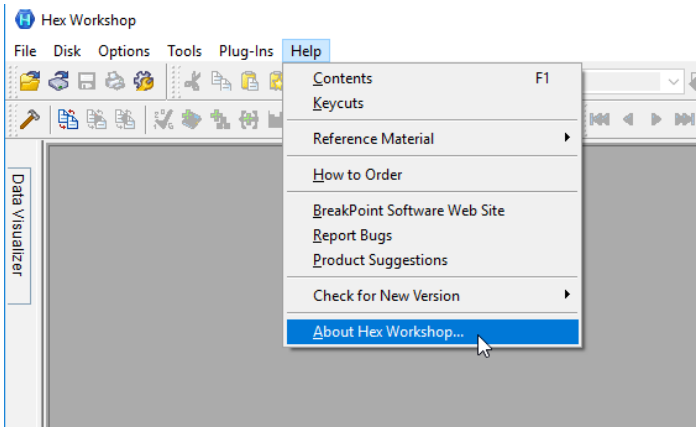


Una vez substituidos, reinicio el PC, abro la aplicación y me aparece esto:

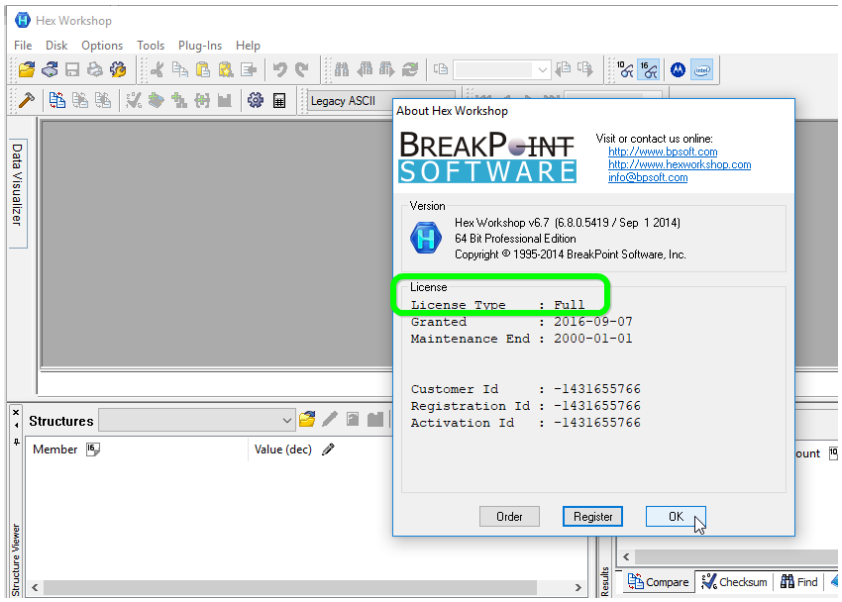


Una malvada "Nag" de aviso de "Product Expiración", aviso de "Your Trial evaluación period has expired" y con indicación de veces de uso de la aplicación. "Times Used: 1"

Bien, ahora salimos de la "Nag" dándole a "Exit", y me dirijo a "Help" > "About Hex Workshop…"

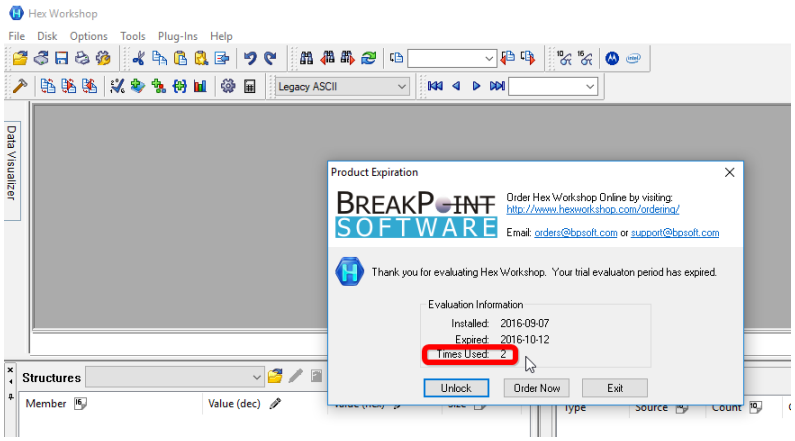


Y observo que la aplicación está registrada

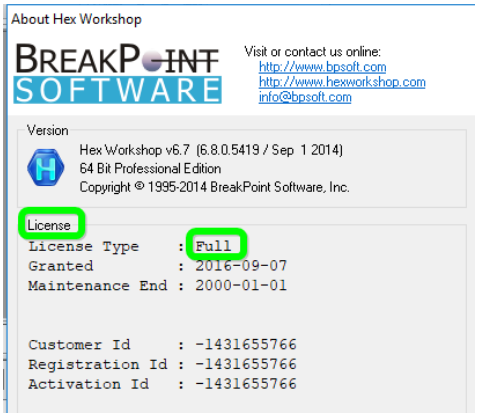


Se me encojen las cejas, le pego un trago a mí "Woll-Damm" (Si no disponen de una cerveza a mano pueden saltarse lo de pegarle un trago….), y me digo a mí mismo, ¿Me habré equivocado en algún paso al instalar el "Fix" de Embrace? , o realmente y con todos mis respetos por el autor, el "Fix" no está del todo pensado para el "Sistema Operativo Windows 10 Home" y solamente ha realizado su trabajo a medias.

Cierro la aplicación y la vuelvo a abrir, y….la maldita "Nag" aparece de nuevo, esta vez con indicación número 2 de uso ,"Times Used: 2"



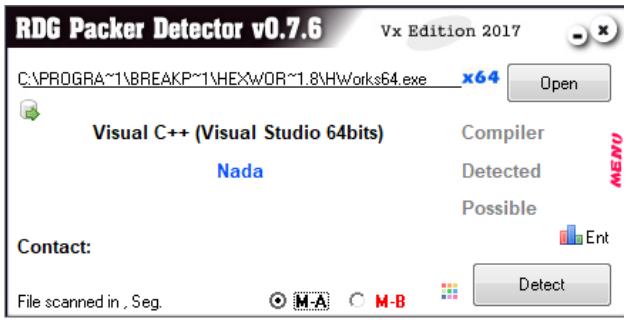
Nuevamente salgo de la "Nag", miro el "About.." y la aplicación continúa registrada



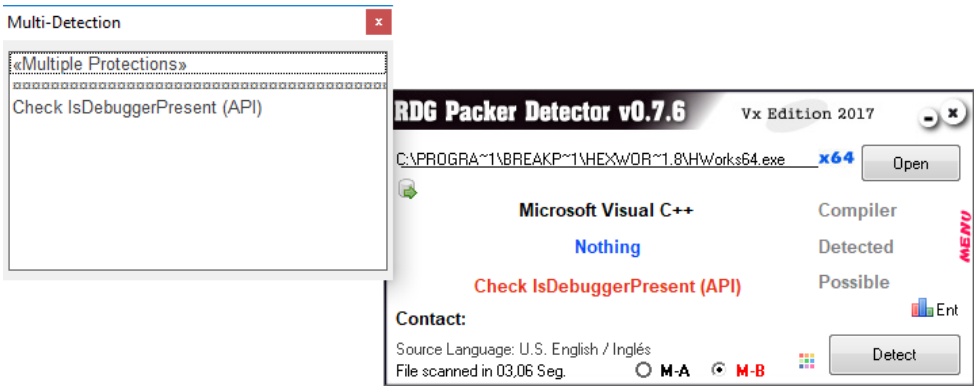
Bien, todo parece indicar que el "Fix" ha dejado la aplicación registrada pero en cambio no evita que salga la pesada "Nag". Vamos a solucionar esto de una vez.

ESTUDIANDO LA VÍCTIMA

Salimos totalmente de la aplicación, le pasamos el detector de ejecutables "RDG Packer Detector v0.7.6" y en el modo escaneo normal "M-A" nos dice que está compilado en Visual C++ (Visual Studio 64bits), y que no está empacado.

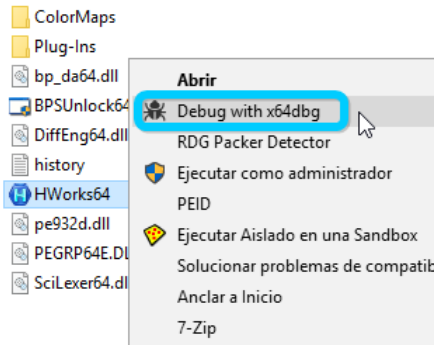


y el modo escaneo profundo "M-B" nos avisa además de un posible "Check IsDebuggerPressent (API)" como protección.

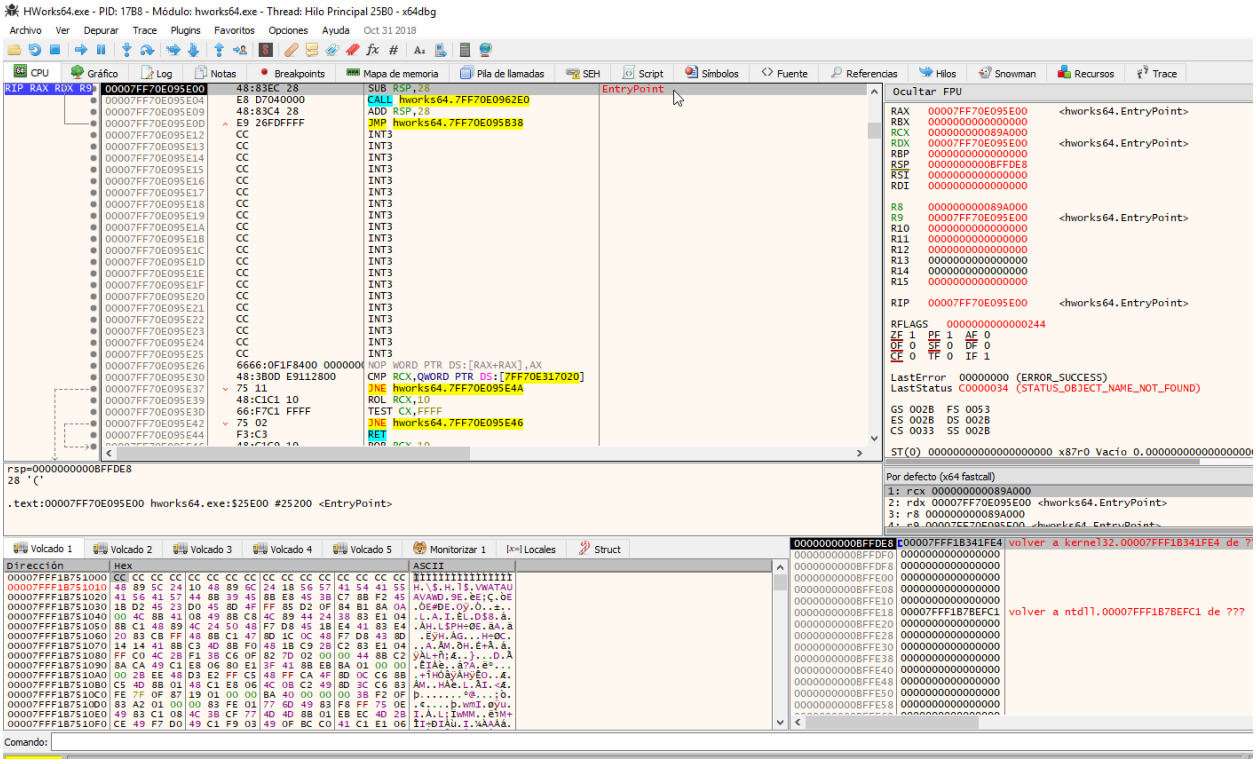


VAMOS A POR ELLA

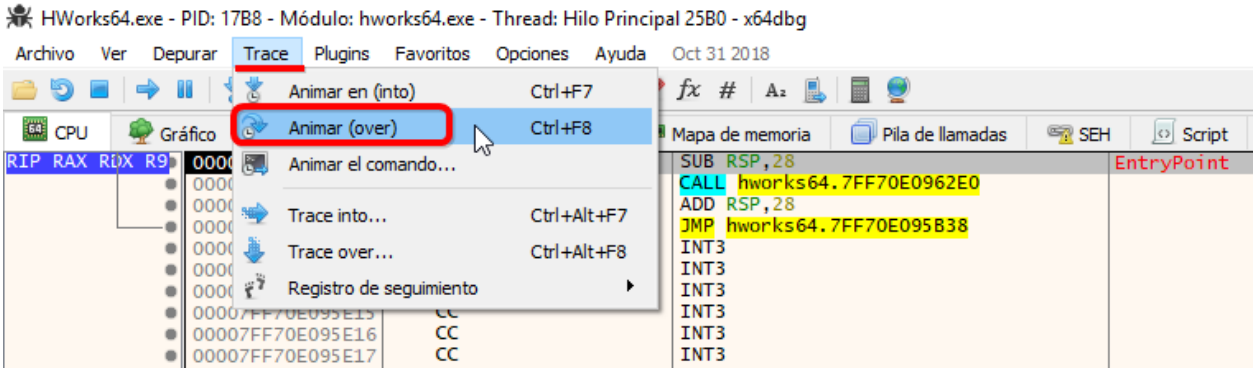
Salimos del detector de ejecutable, y desde la ubicación del archivo, nos posicionamos directamente sobre el "HWorks64.exe", "Click" derecho de ratón, seleccionamos la tool "x64dbg" de nuestro menú



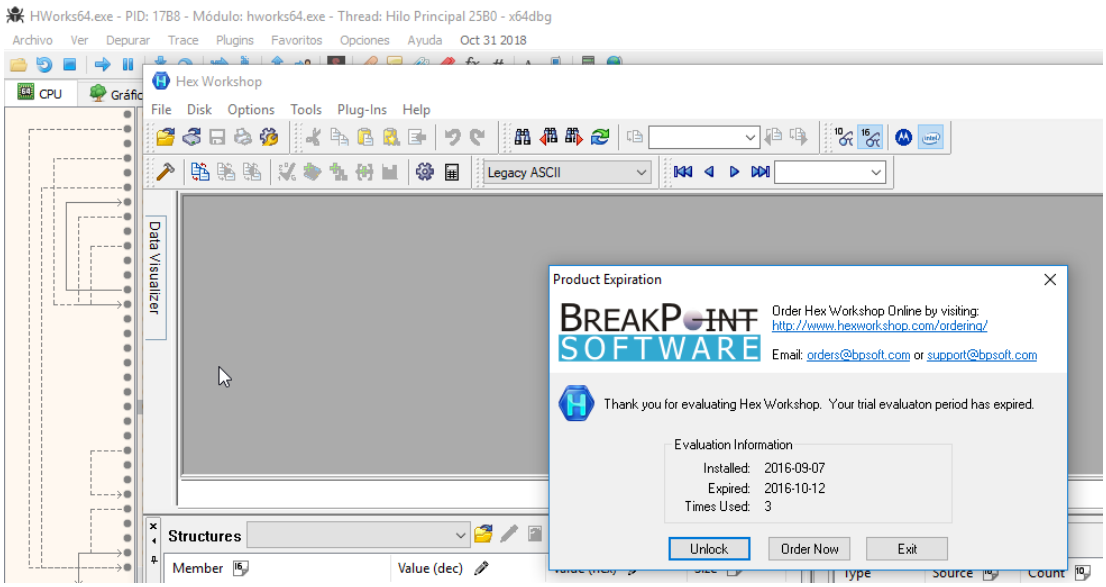
y aparecemos en el "EntryPoint", address "00007FF70E095E00"



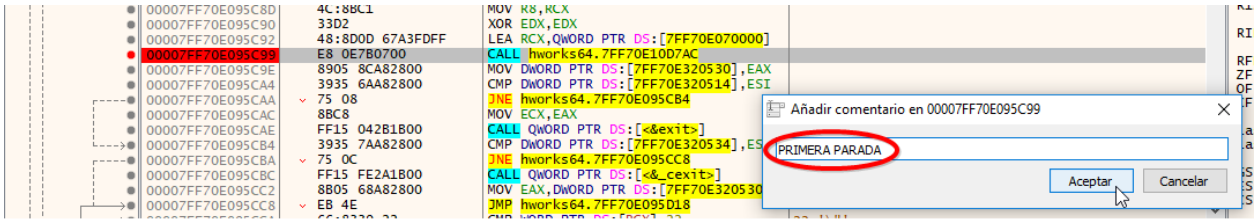
Nos vamos al menú "Trace -> Animar (over)",



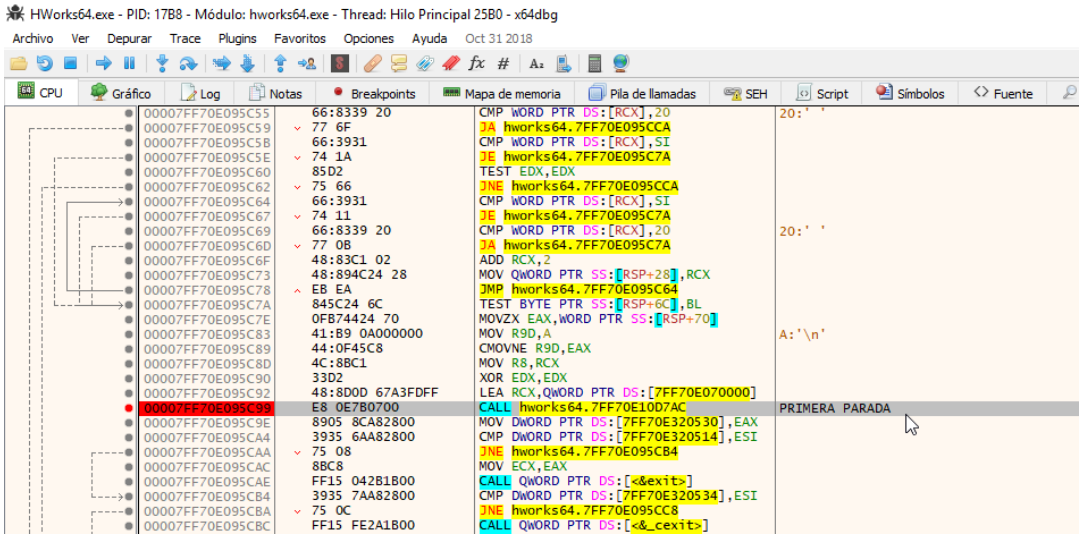
y vamos observando cómo automáticamente va trabajando el debugger sin entrar en las "CALL" hasta que salta la aplicación (La posible protección "IsDebuggerPressent" no está presente ya que corre perfectamente)



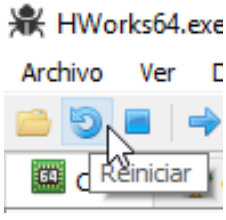
Y esto lo hace en la "CALL" address "00007FF70E095C99" , donde le ponemos un "BP" (Breakpoint), y como comentario tipeamos "PRIMERA PARADA"



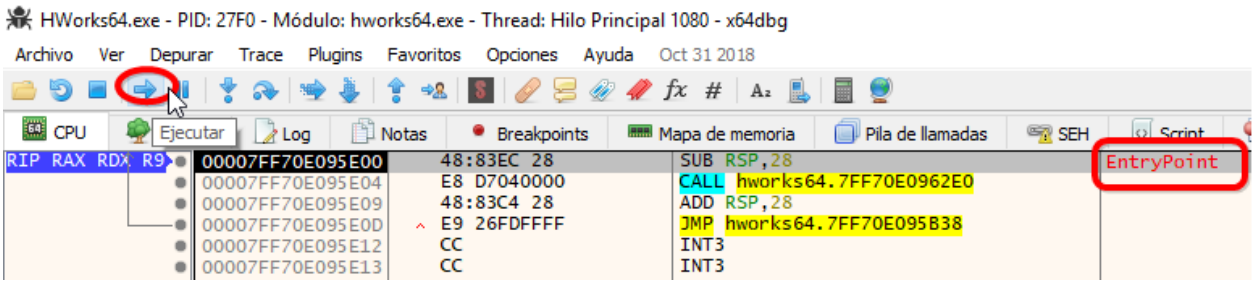
Y nos queda así:



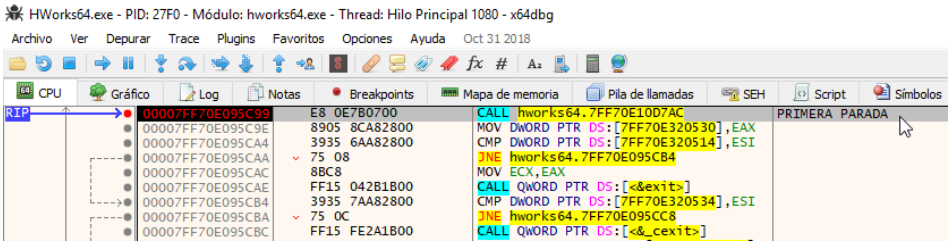
Bien, ahora reiniciamos



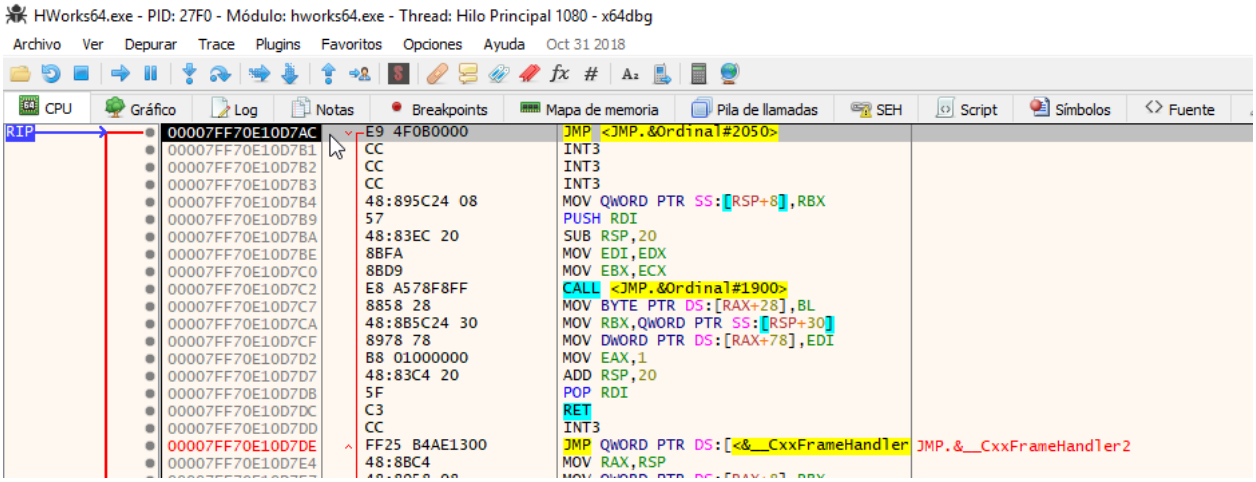
Y nos encontramos parados de nuevo en el "Entry Point"



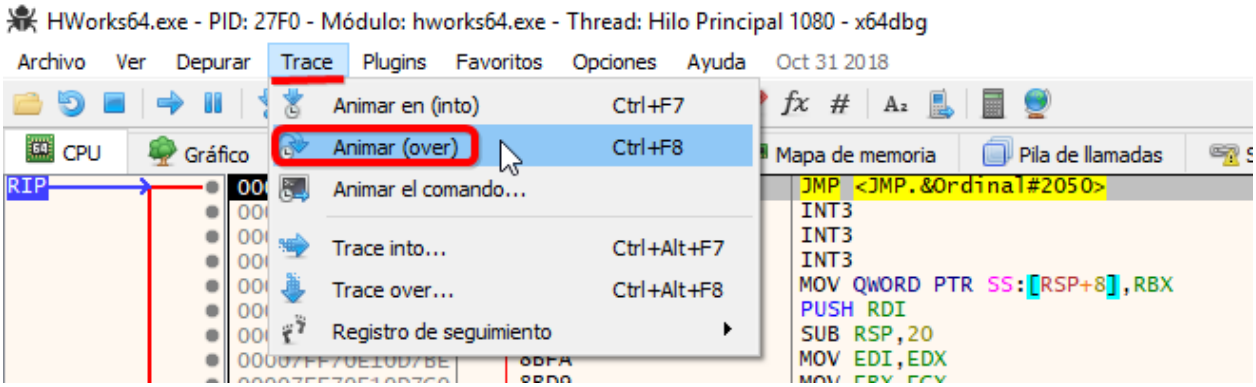
Le damos a "Ejecutar" para que corra el debugger y como era de esperar parará en nuestro primer "Breakpoint" tal como le indicamos.



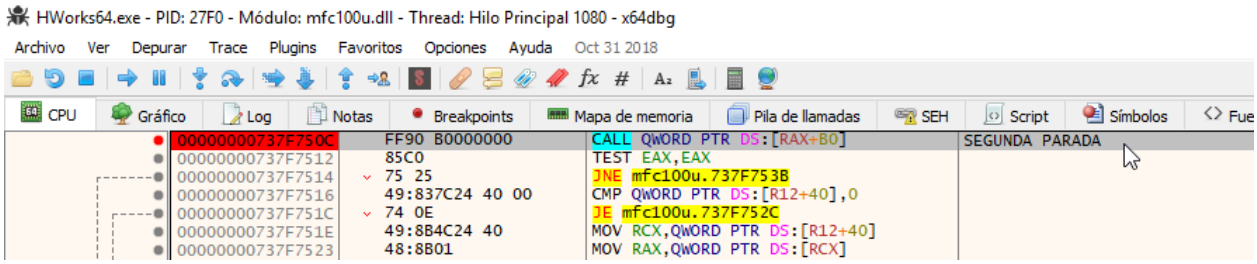
Entramos en esa "CALL" y una vez dentro aparecemos en un salto incondicional "JMP" muy largo, que está en la address "00007FF70E10D7AC".



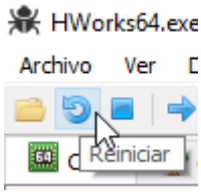
Volvemos a darle a "Animar (over)"

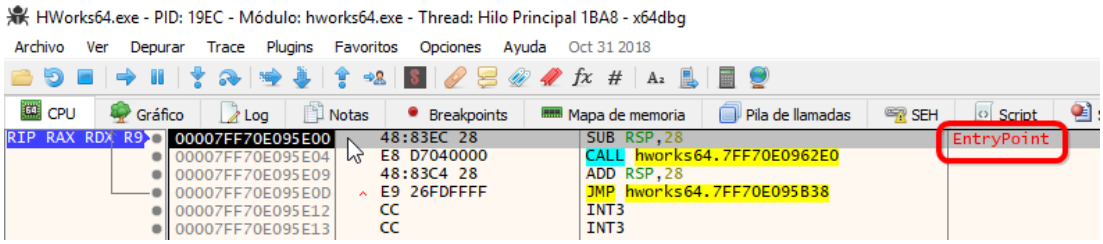


Y ahora nuestro "x64dbg" para en la "CALL" ubicada en la address "00000000737F750C" donde escribimos como comentario "SEGUNDA PARADA" y nos debe quedar así:

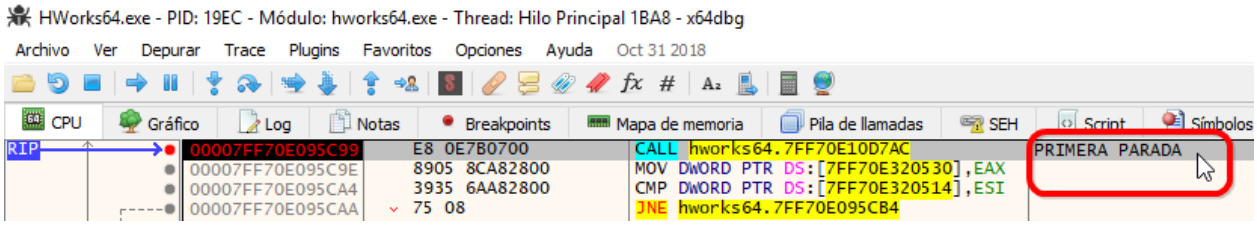


Reiniciamos de nuevo para volver al punto de entrada

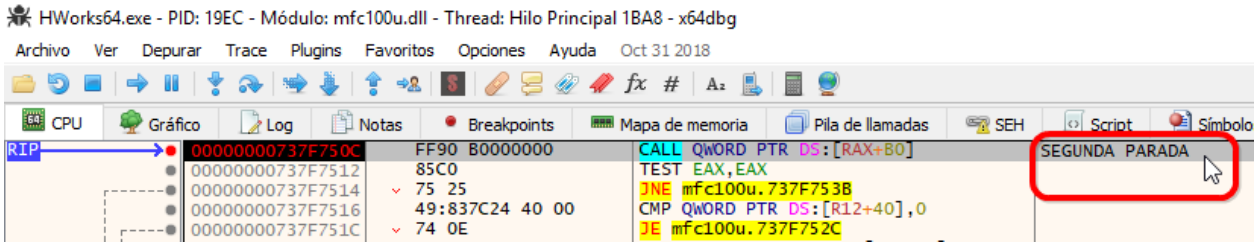




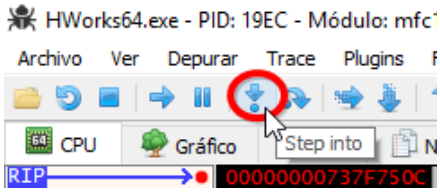
Damos a "Ejecutar" para que corra el debugger y paramos en el primer "BP",



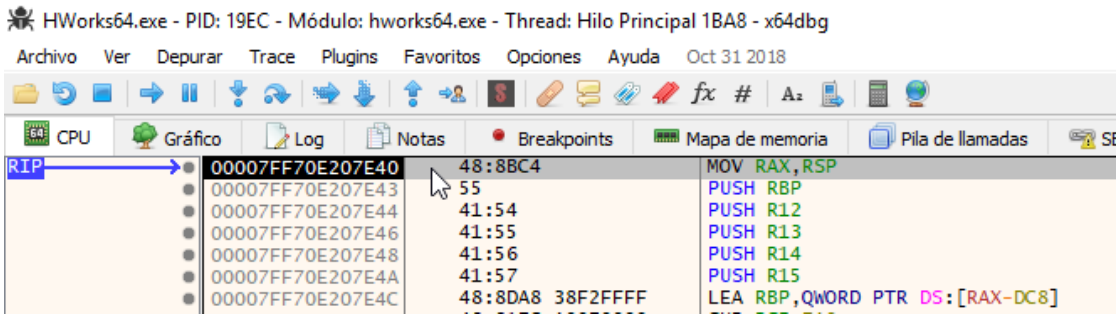
Damos otra vez a "Ejecutar" y paramos en el segundo "BP"



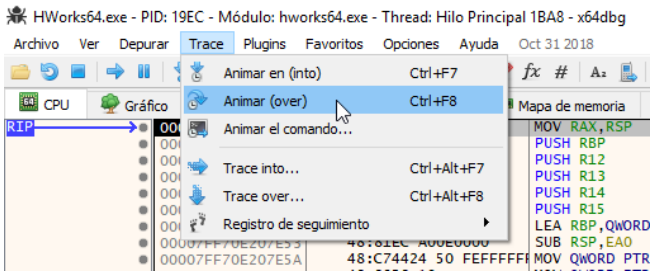
Entramos en esta segunda "CALL" dándole a "Step into"



Y ahora estamos aquí, en la address "00007FF70E207E40"

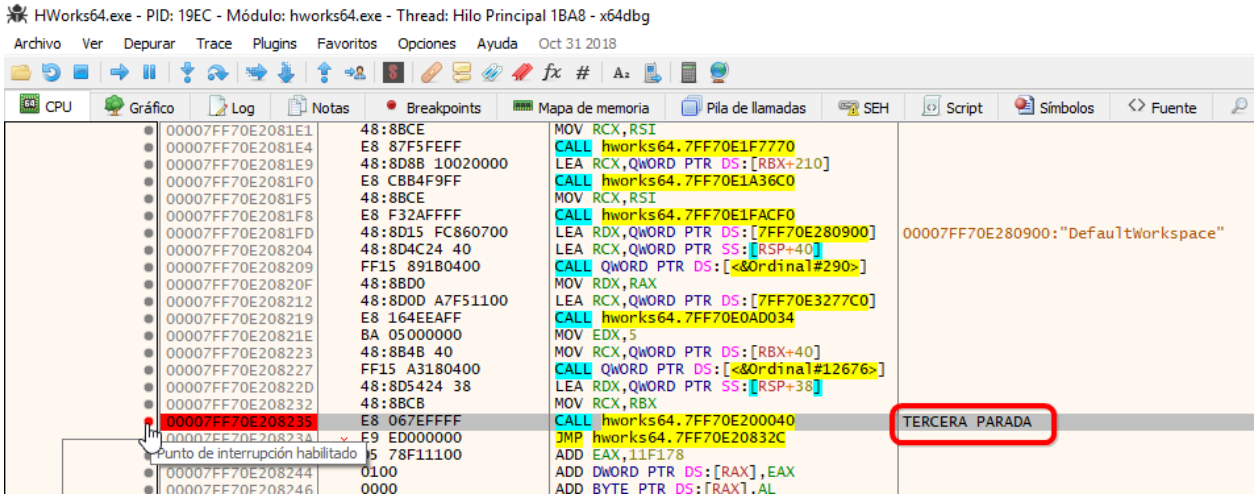


Volvemos a darle a "Animar (over)"

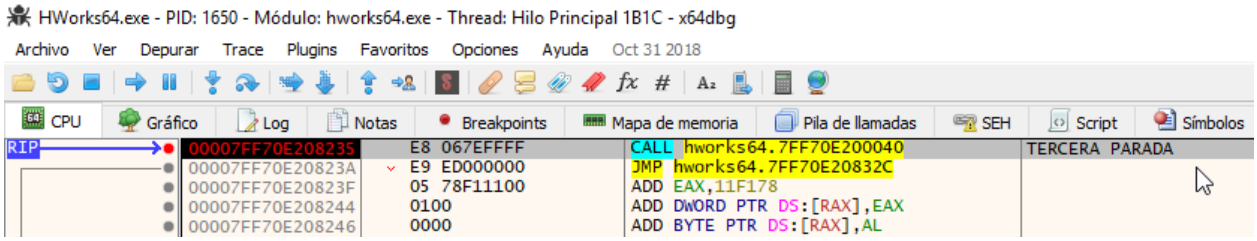


Y aparecemos en otra "CALL" que a nuestros efectos es la TERCERA PARADA, (tranquilos que aunque sea muy repetitivo ya queda poco…)"

Volvemos a ponerle un "Breakpoint" y agregamos el comentario de "TERCERA PARADA", quedándonos así:

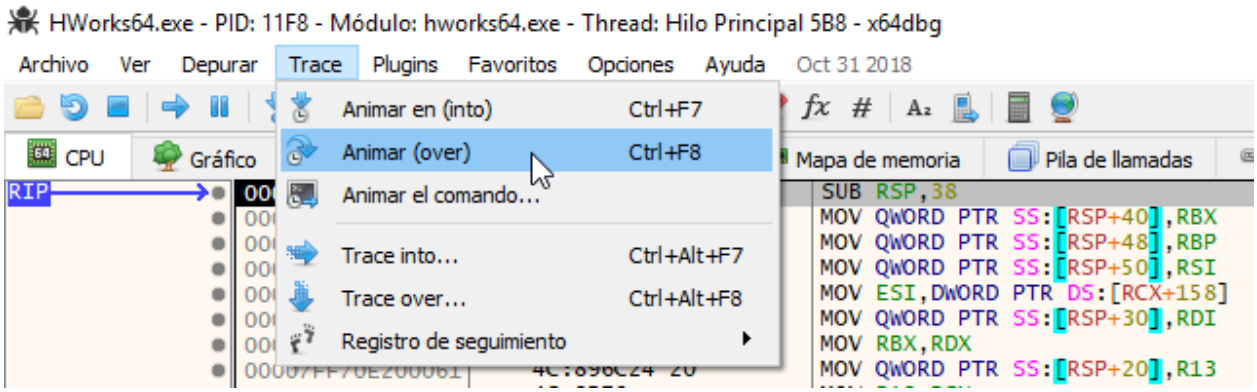


Reiniciamos por tercera vez el debugger y le vamos dando a ejecutar hasta que nos encontremos parados en la "TERCERA PARADA"



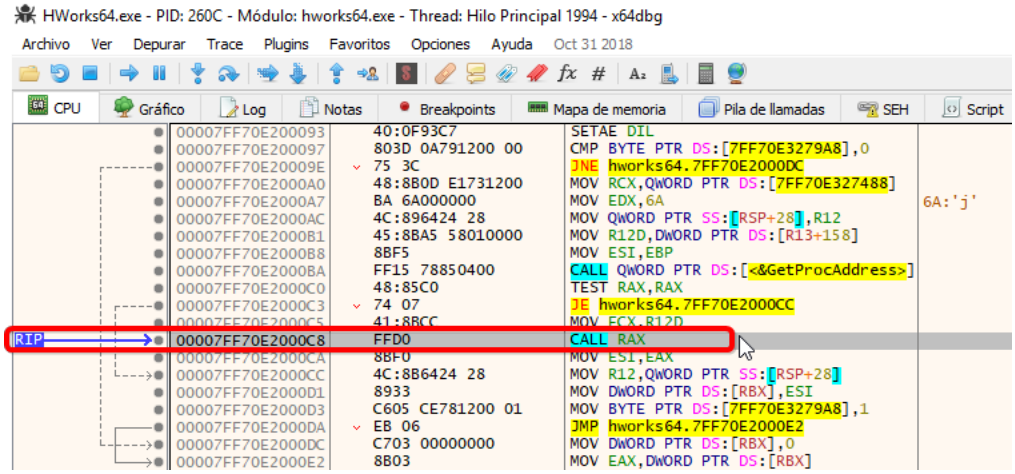
De nuevo <u>entramos</u> en esta tercera "CALL" , y aparecemos aquí

Y una vez más volvemos a darle a "Animar (over)"

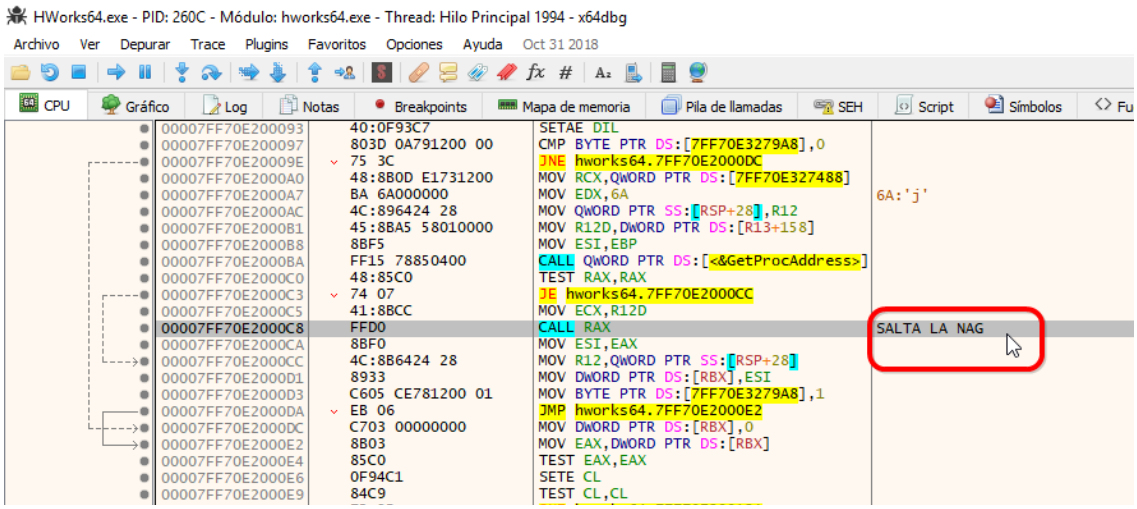


Y esta vez.. nos aparece la dichosa "Nag" que andábamos buscando..je,je,je..

Ha saltado justamente cuando hemos llegado a la "CALL" que en mi máquina se encuentra en la address "00007FF70E2000C8"



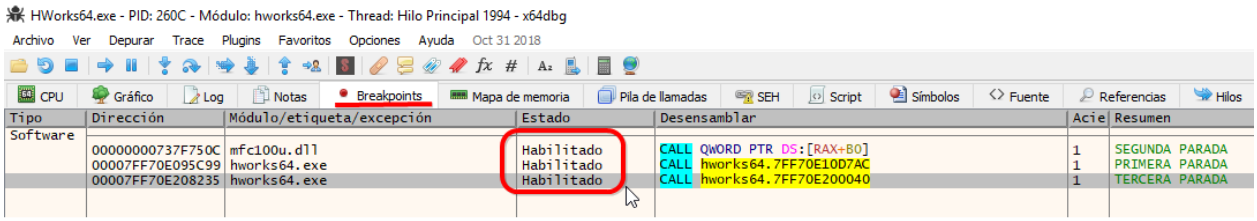
Ahora sencillamente le ponemos la anotación de "SALTA LA NAG" y nos queda así:



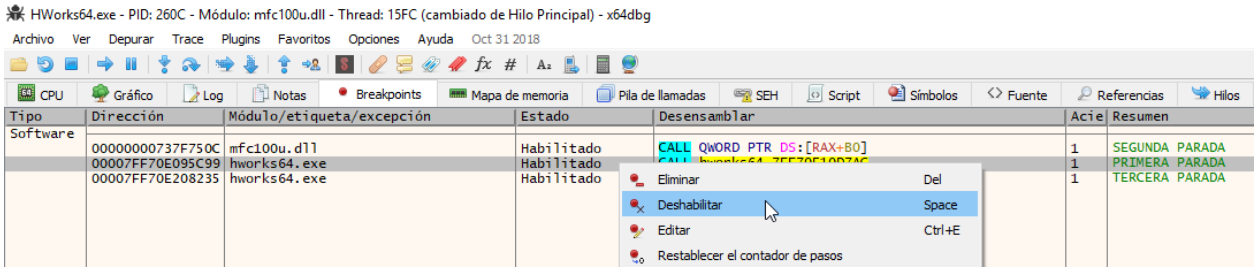
Con un simple vistazo, mi instinto de cracker ya me está indicando que esa "CALL" donde salta la "Nag" está precedida de una instrucción "TEST" (testeo) y un lindo salto condicional "JE", que sin duda decidirá si nos muestra o no la "Nag". Vamos a comprobarlo.

Esta vez para ir directos a la Zona Caliente vamos a deshabilitar los dos "BP" que no nos interesa parar en ellos, y solamente dejaremos habilitado el de la "TERCERA PARADA"

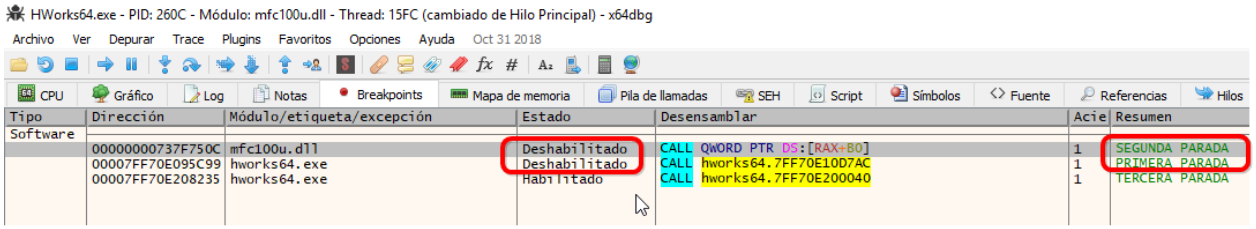
Para ello nos vamos a la pestaña de los "Breakpoints"



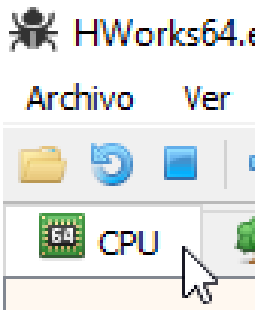
Nos posicionamos con el cursor sobre el que elijamos, "Click" derecho y Deshabilitar.



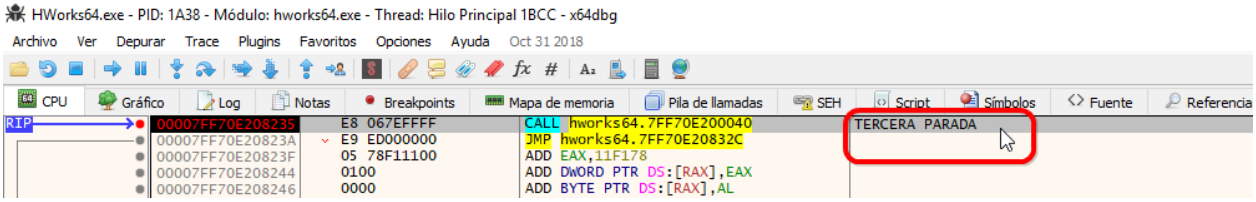
Y nos debe quedar así:



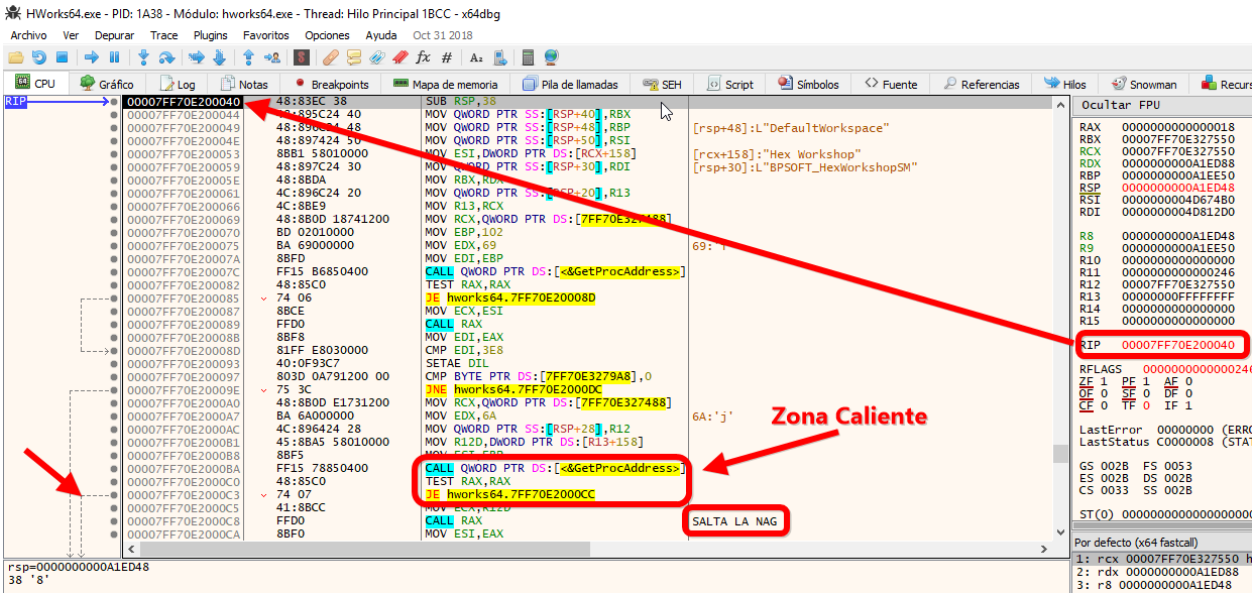
Volvamos a la ventana principal dándole a la pestaña "CPU"



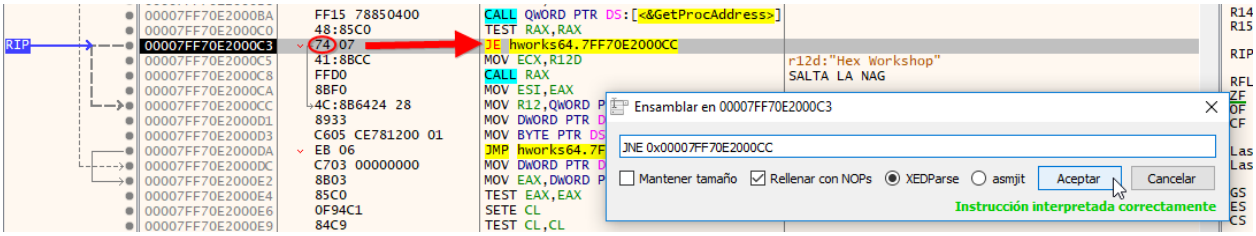
Reiniciamos, ejecutamos y ahora nos encontramos parados en el único "BP" que dejamos habilitado



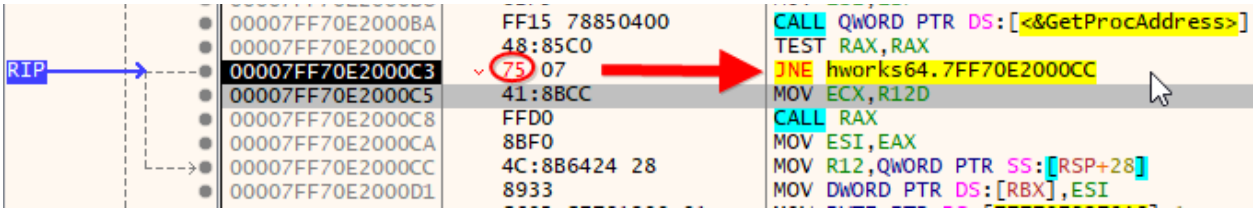
Entramos en esa "CALL" con "F7", y aparecemos aquí



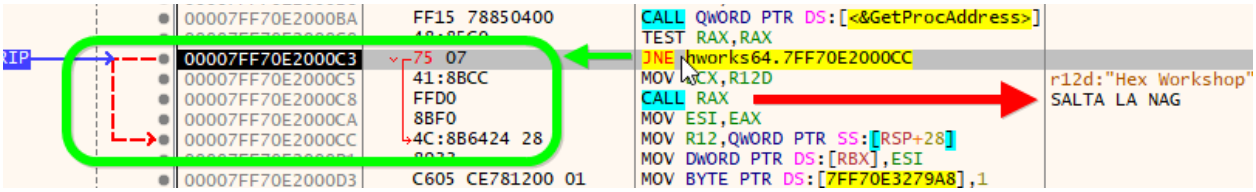
Vamos traceando con "F8", hasta llegar al salto condicional "JE" y lo invertimos por un "JNE"



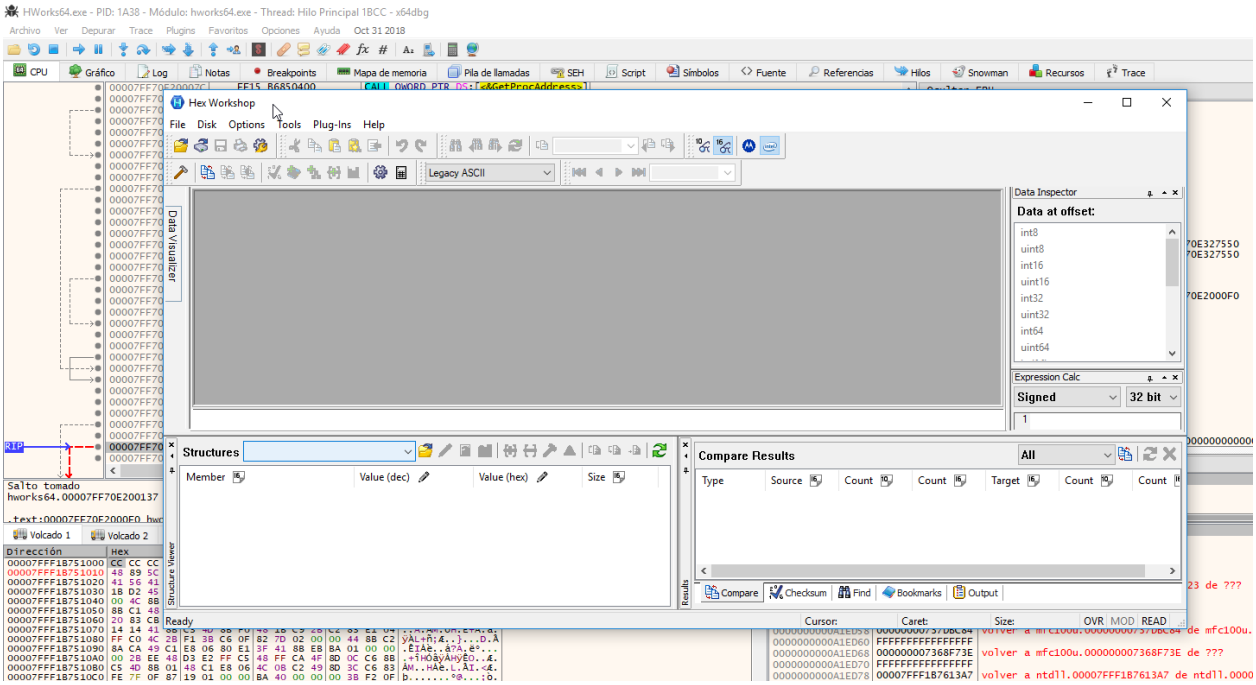
así:



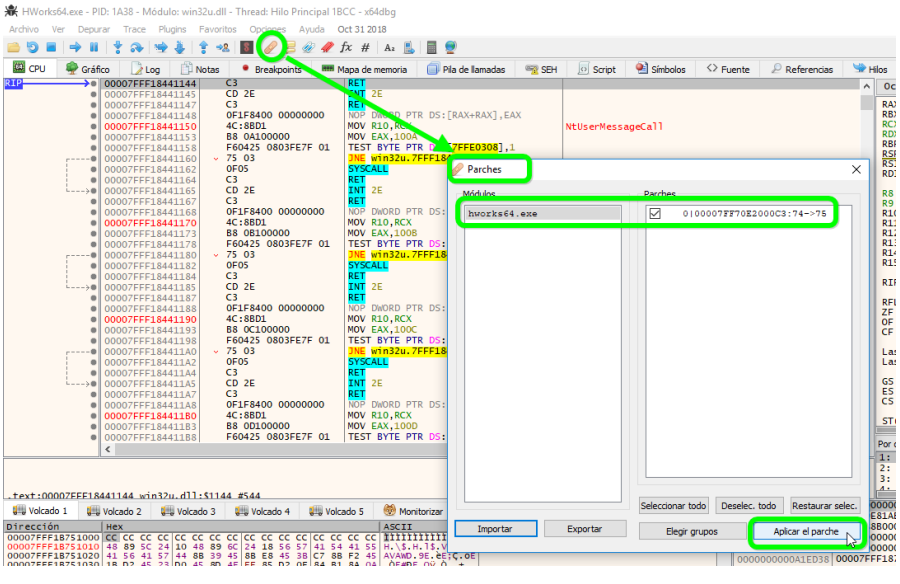
Si nos posicionamos con el cursor sobre la instrucción "JNE" que acabamos de substituir, nos daremos cuenta que cuando se ejecute ya no entrará en la "CALL" donde saltaría la "Nag" y por lo tanto la habremos burlado.



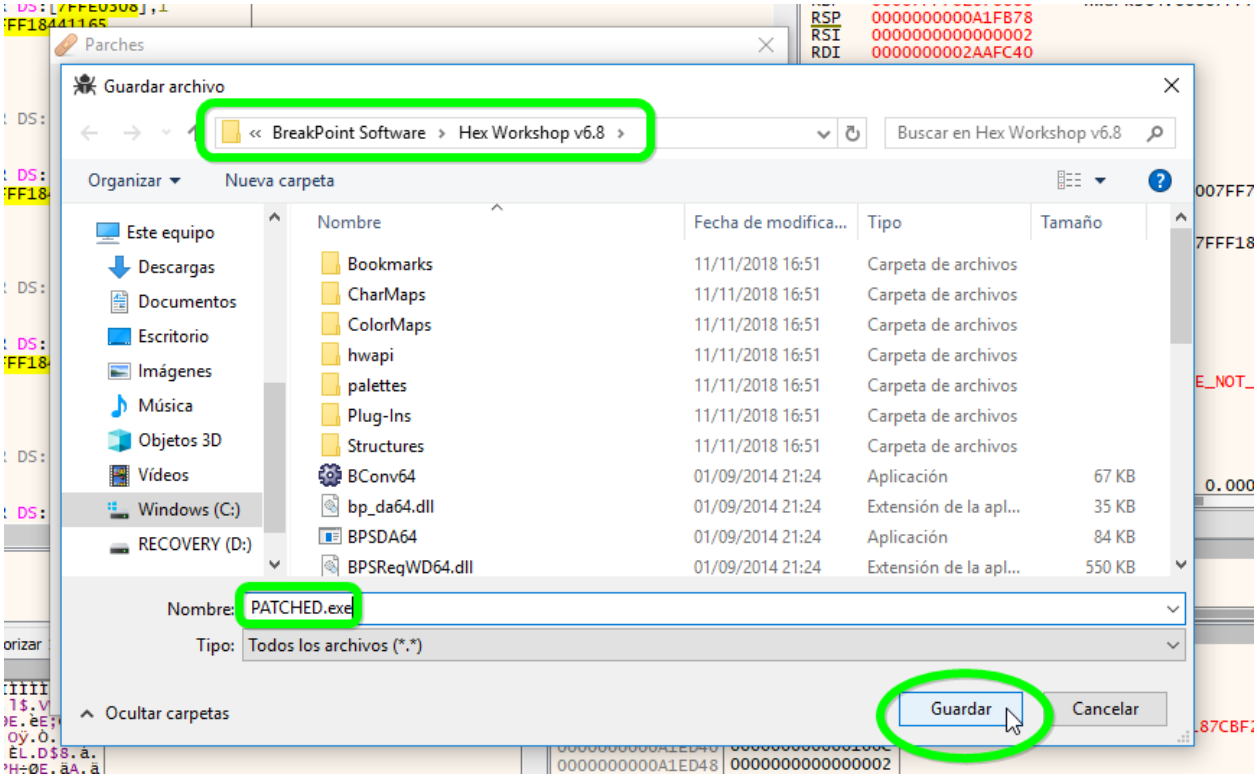
Le damos directamente a "Ejecutar" y por fin……. problema solucionado, je,je,je…. se abre la aplicación perfectamente sin que haya aparecido la "Nag"



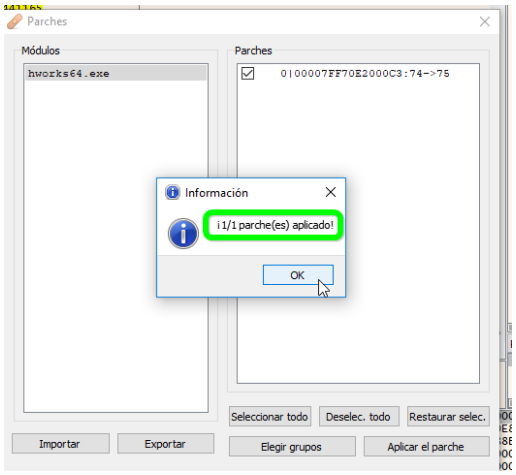
Solo nos queda guardar los cambios. Nos dirigimos a "Parches"



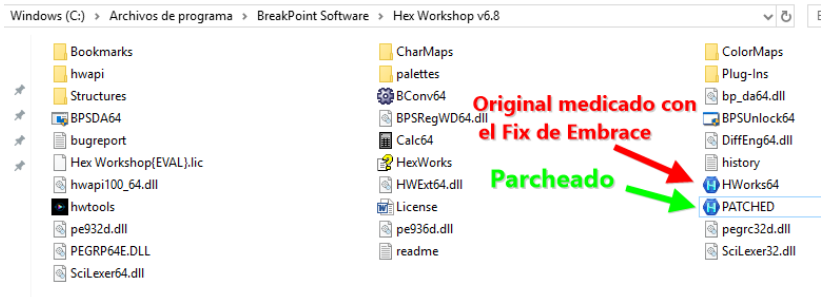
Aplicamos el parche, yo le llamo "PATCHED.exe" y como vemos, por defecto nos lo guardará directamente en el mismo directorio donde tenemos instalada la aplicación.



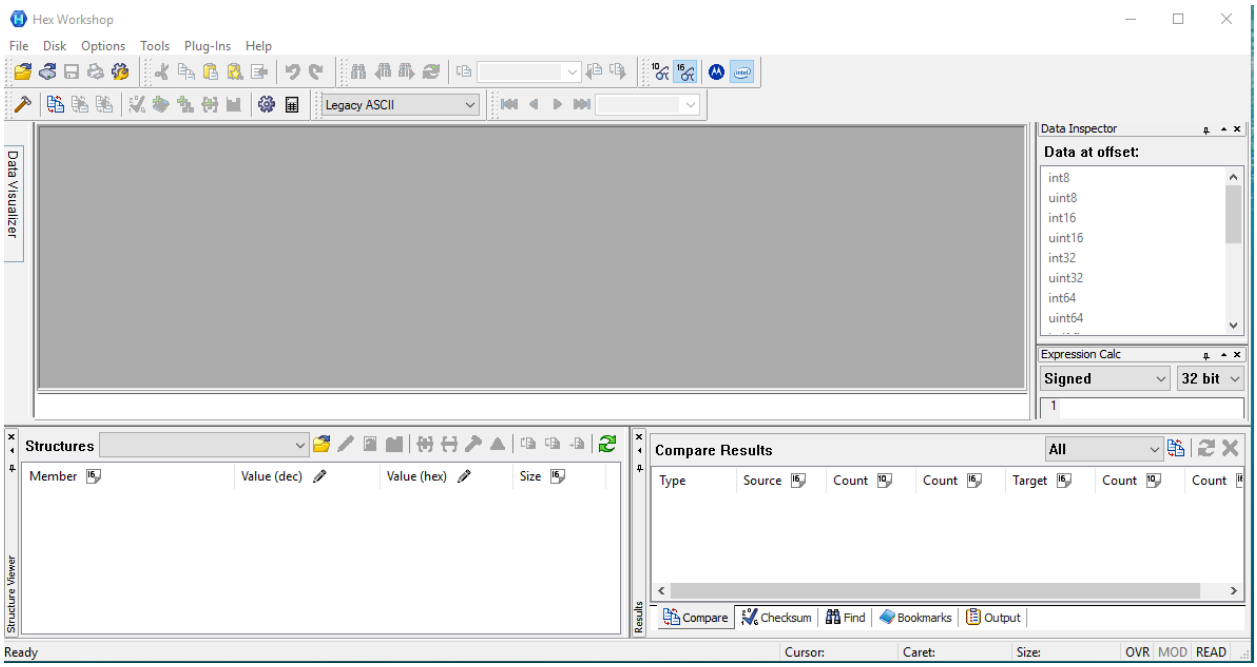
Le damos a "Guardar" y nos dice que ha sido aplicado.



Le damos a "OK", salimos de nuestro magnífico "X64dbg", nos dirigimos a la ruta de nuestro PC donde tenemos la aplicación instalada

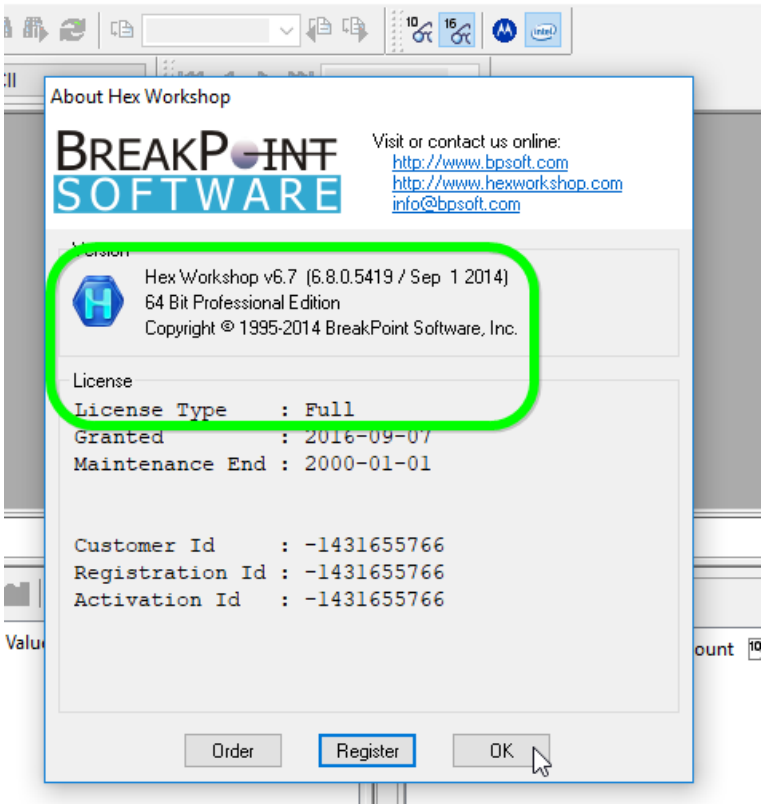


Le damos a nuestra flamante creación a la que hemos llamado "PATCHED.exe" y……..

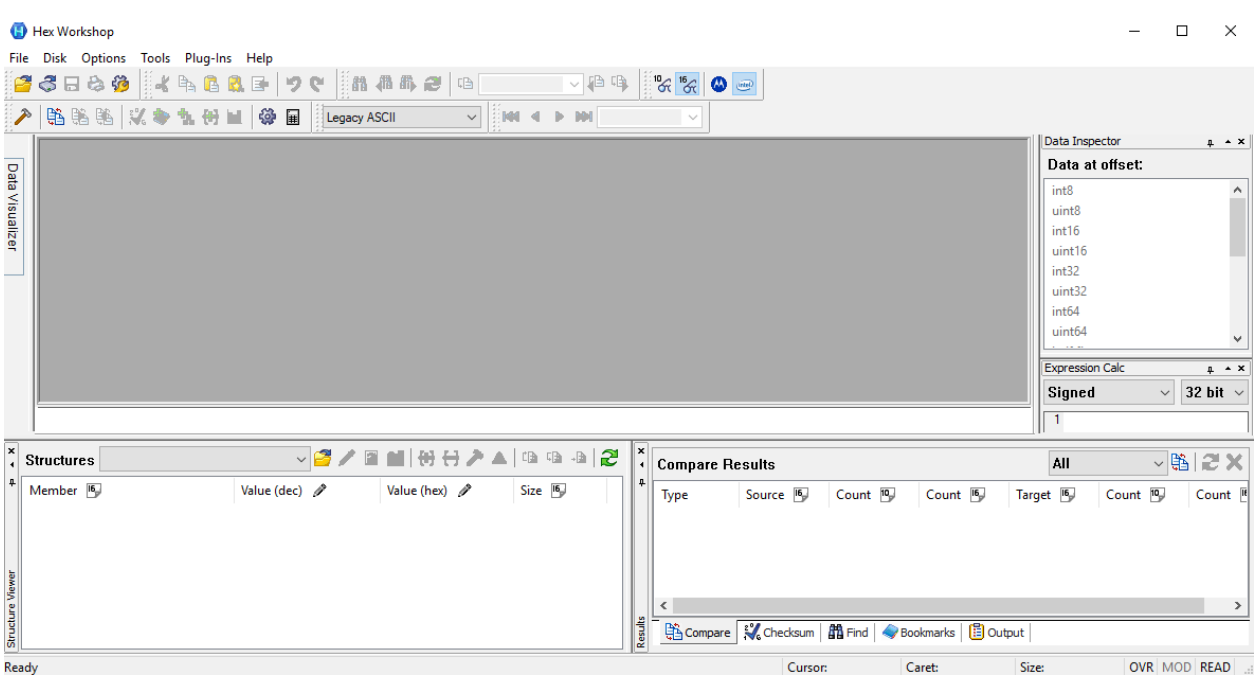


PROBLEMA FELIZMENTE SOLUCIONADO, LA APLICACIÓN SE ABRE CORRECTAMENTE SIN QUE NOS MUESTRE LA DICHOSA "NAG"

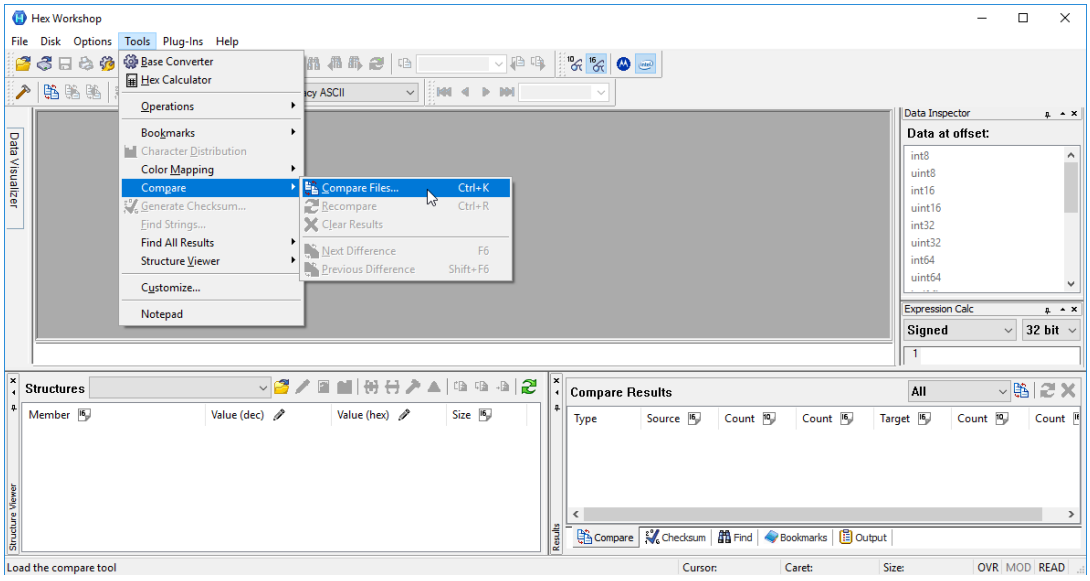
Y si nos vamos a "About" seguimos viendo que está "Full" y completamente funcional.



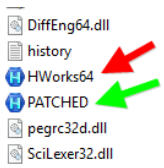
Ahora, ya que estamos, vamos a probar una de las <u>muchas utilidades de este Editor Hexadecimal.</u>

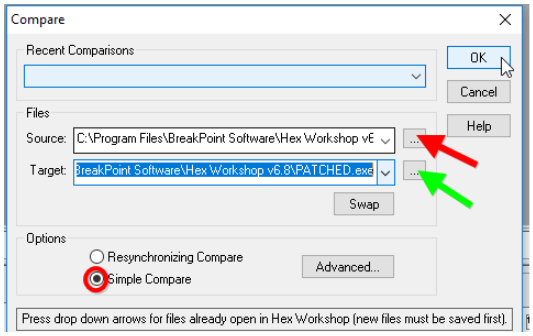


Nos dirigimos a "Tools > Compare > Compare Files…"

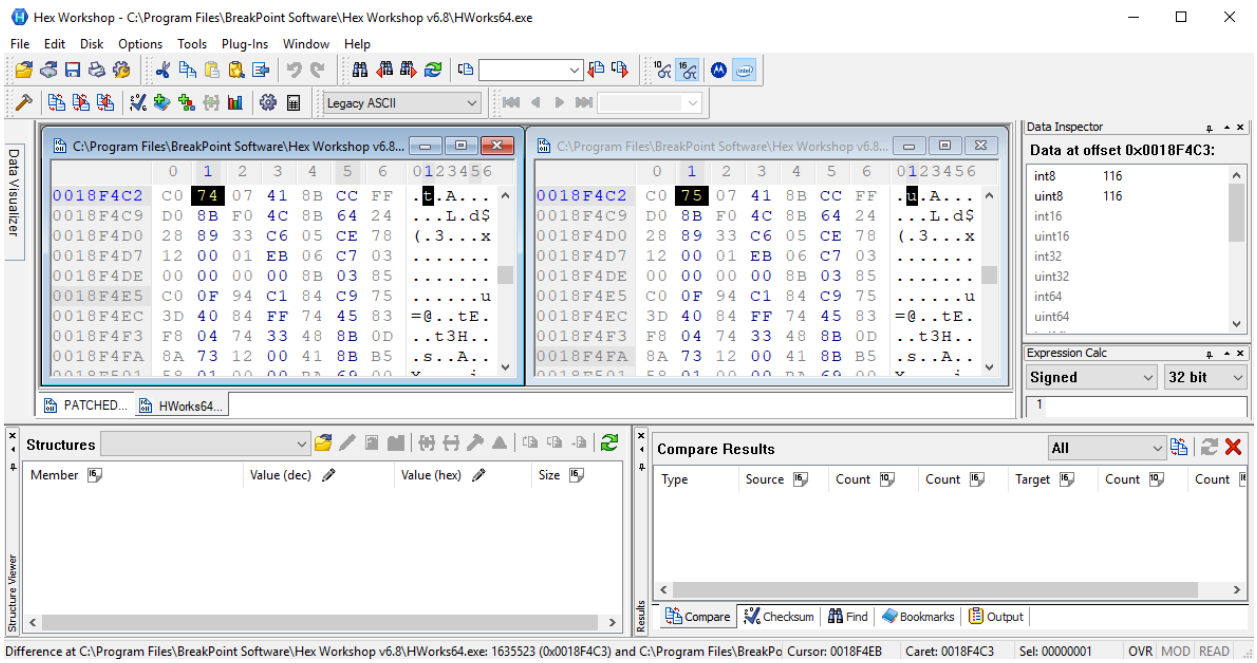


Cargamos los dos archivos buscando sus respectivas rutas (El original al que el hemos aplicado el Fix "HWorks64" y nuestro "PATCHED")





Tildamos "Simple Compare" , le damos a "OK" y……



Funciona a la perfección, nos enseña el resultado de lo que le hemos pedido mostrándonos el "byte" que hemos modificado, y que en este caso es la única diferencia entre ambos archivos.

Que lo disfruten……..

Antes de despedirme, solo decirles que el que disponga de SO Windows 10 (64bits), quiera instalar el Editor Hexadecimal "Hex Workshop Hex Editor Pro v6.8.0.5419" validándolo de la forma explicada en este pequeño tutorial, y sea un vago de campeonato con muuucha F1ACA como diría Ricnar…… también pongo a su disposición mi "Patch" personal que pueden bajarse del siguiente enlace:

https://mega.nz/#!zsNXyQwJ!i0zjfXrVZm8YDEzuLvZt-XWax9vShgp7Kmp5UvTYV9g

Pero recuerden, que antes de ejecutarlo, deben primero aplicar la opción "Fix del maestro Ebrace" para no pasar por caja una vez instalada la aplicación.

Hasta el próximo tute.

……MISIÓN CUMPLIDA……

Mis agradecimientos infinitos a

CracksLatinoS

El esfuerzo sin talento es una situación deprimente, pero talento sin esfuerzo es una tragedia.

Mike Ditka

Salu2

QwErTy CLS

19 de Noviembre de 2018