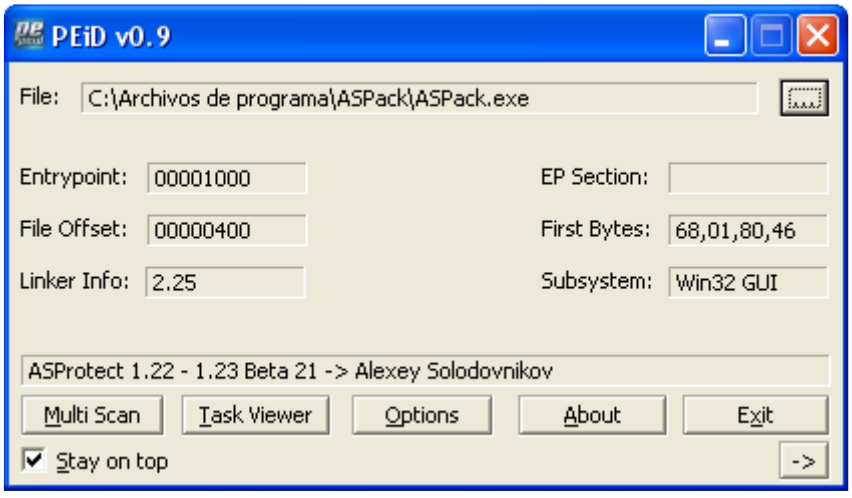
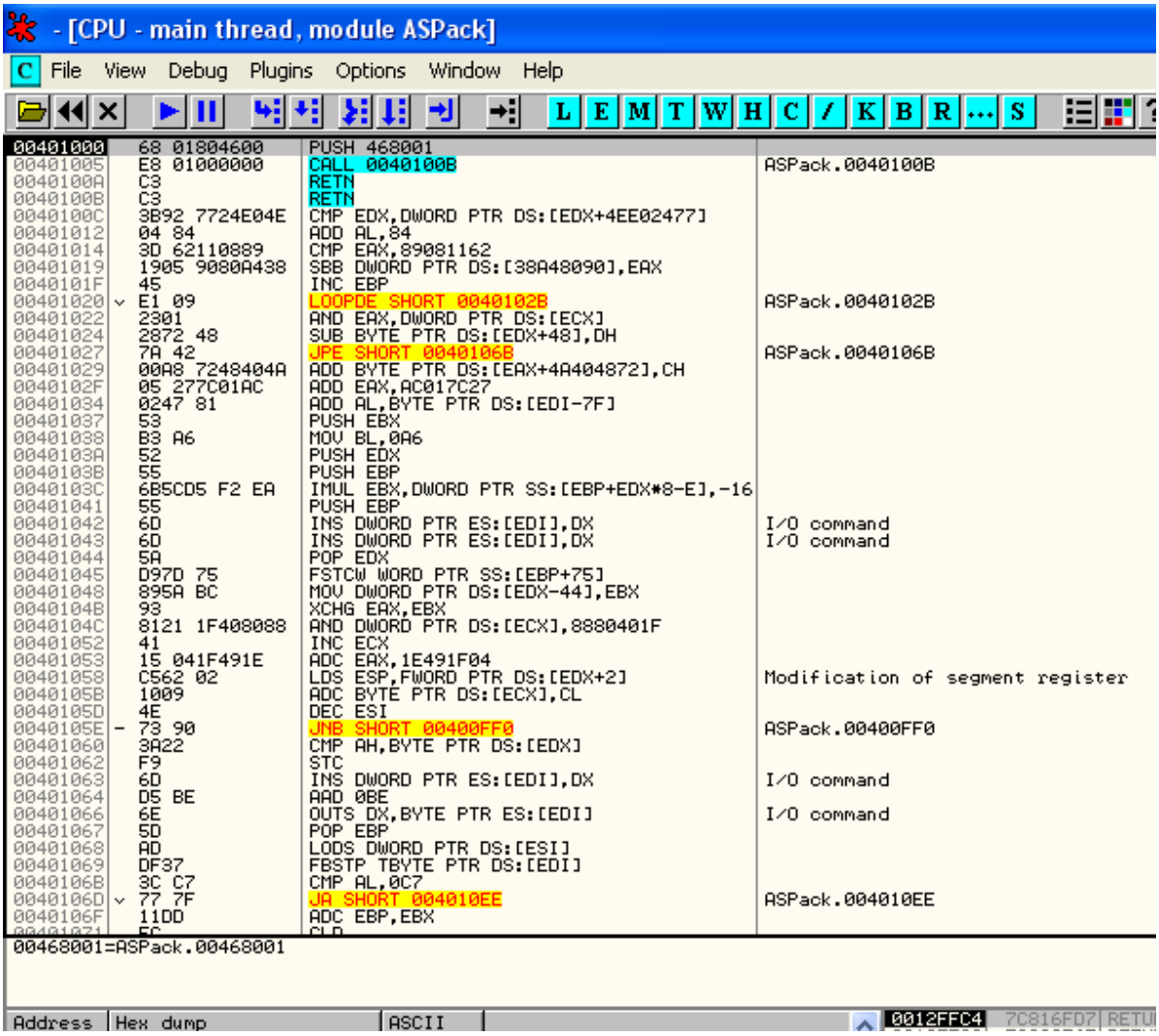
Programa	ASPACK
Versión	2.12
Herramientas	OLLYDBG 1.10, IMPORT REC, PEID
Compilador	Borland Delphi Heuristic Mode
Objetivos	DESEMPACAR EL EJECUTABLE
Cracker	AGUML

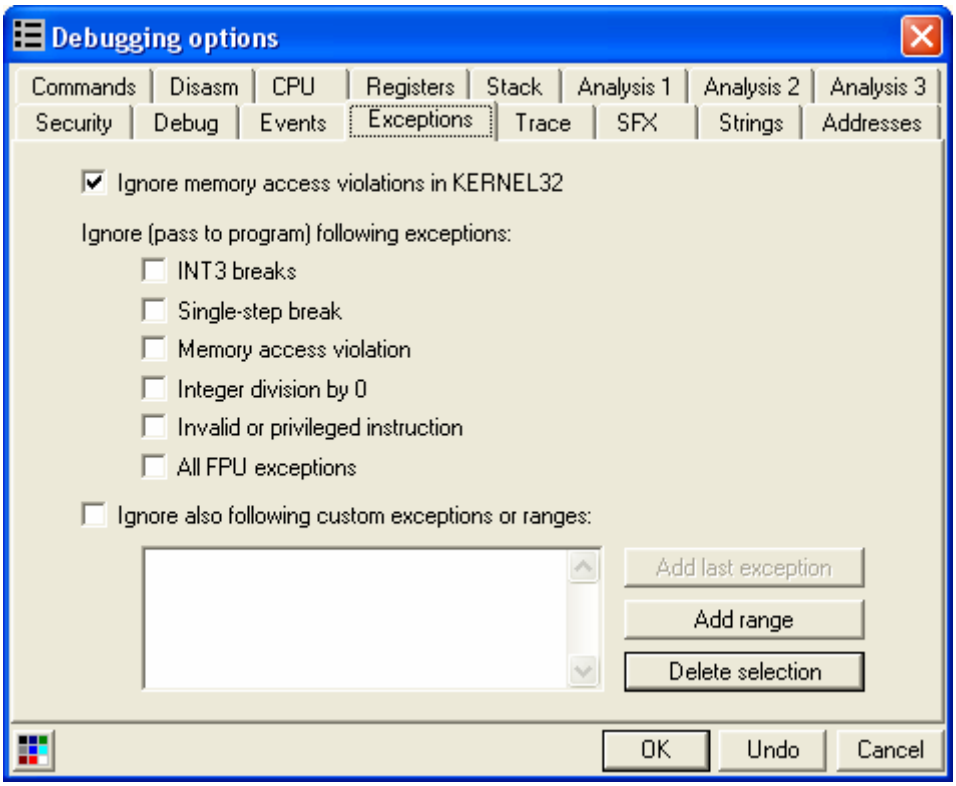
Antes de nada conozcamos a nuestro enemigo. Abrimos PEID y miramos a ver con que esta empacado y:



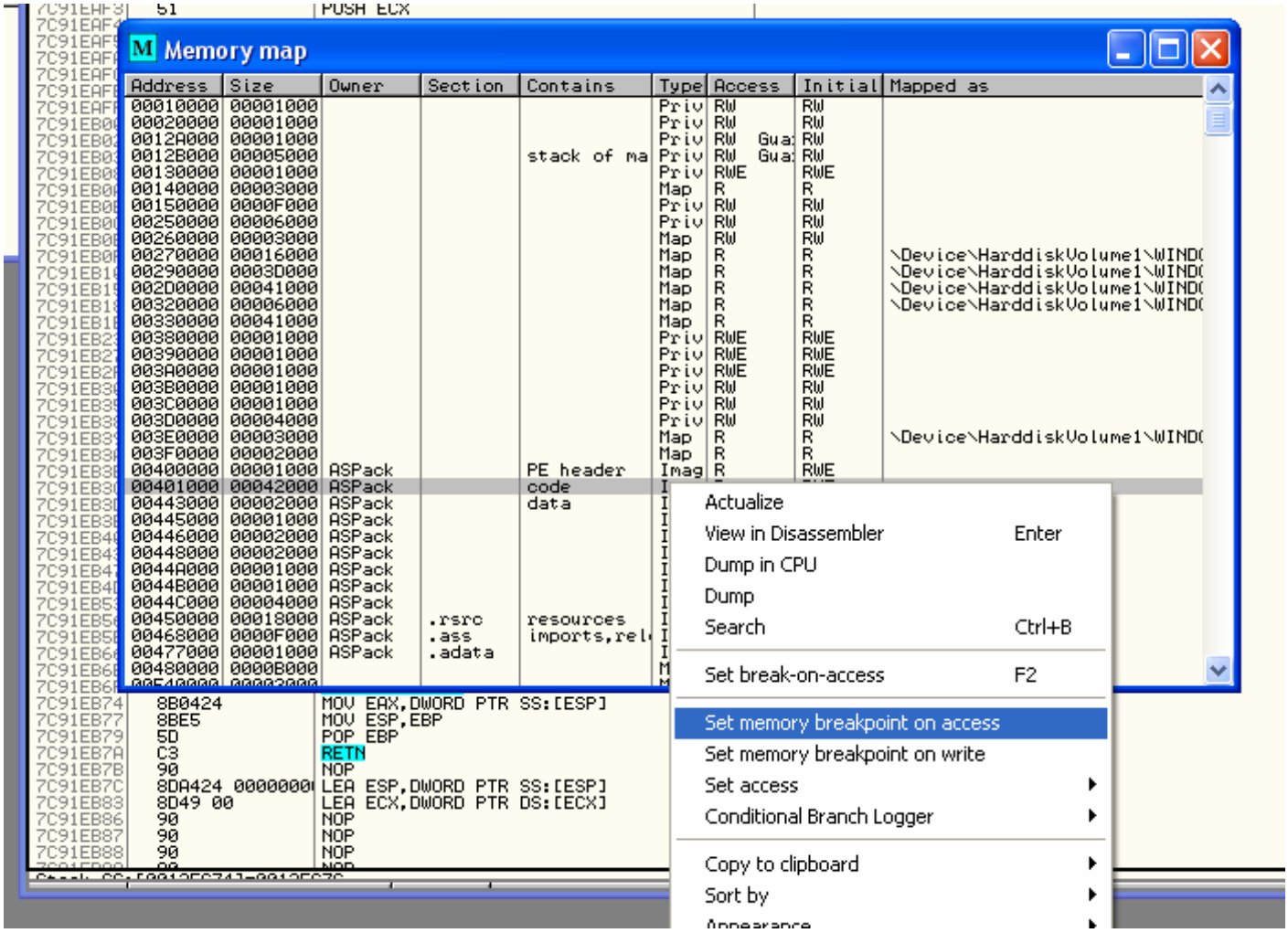
Ufff, con lo poco que me gusta ese packer, jejeje.
Bueno pues carguémoslo en Olly a ver que pasa:



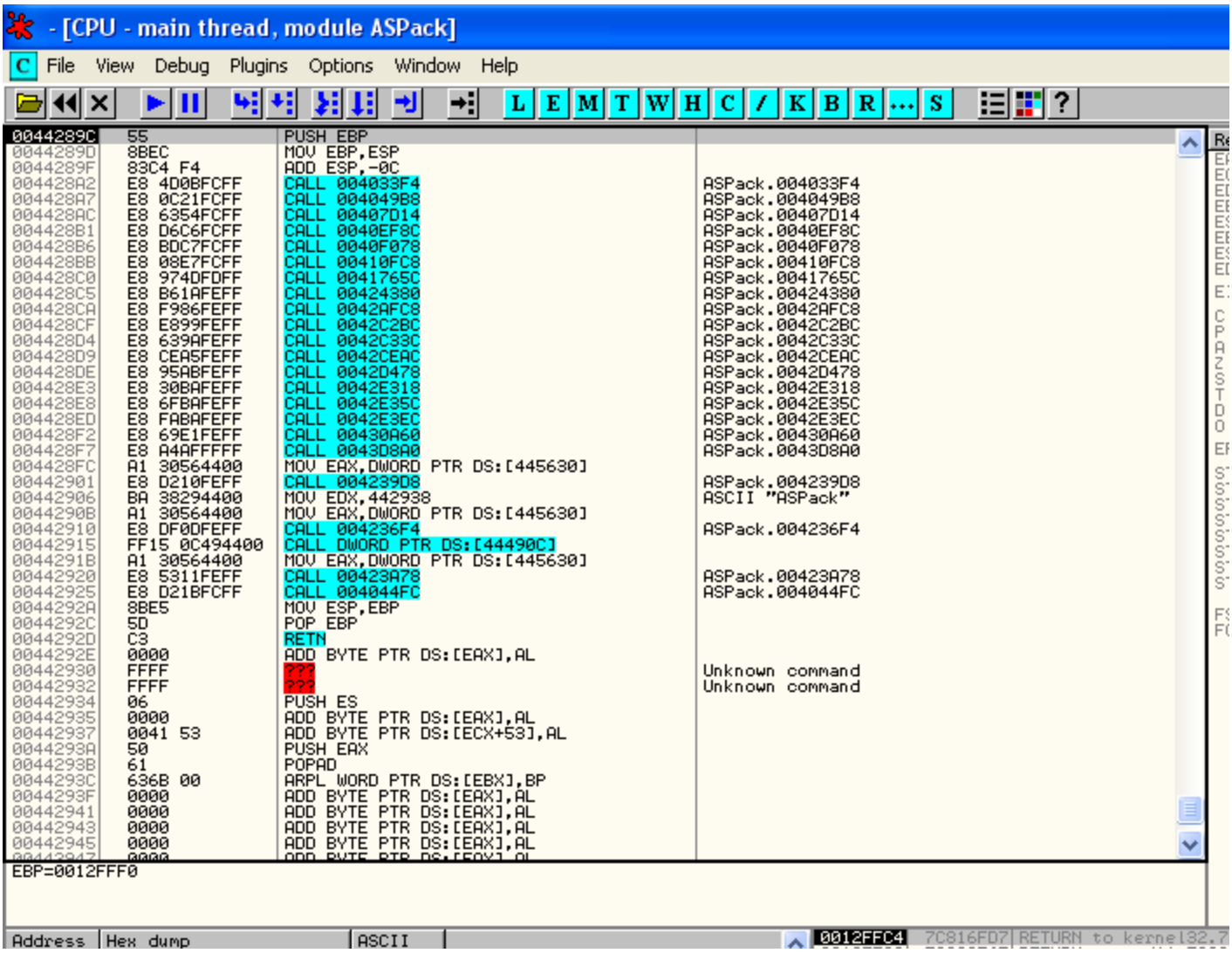
Ahora usaremos el método que mas he visto y que a mi me ha dado resultado para llegar al OEP. Simplemente nos vamos a Options->Debugging Options o si lo prefieren Alt + O y dan en la pestaña Exceptions y dejan marcada solo la primera opción que hay:



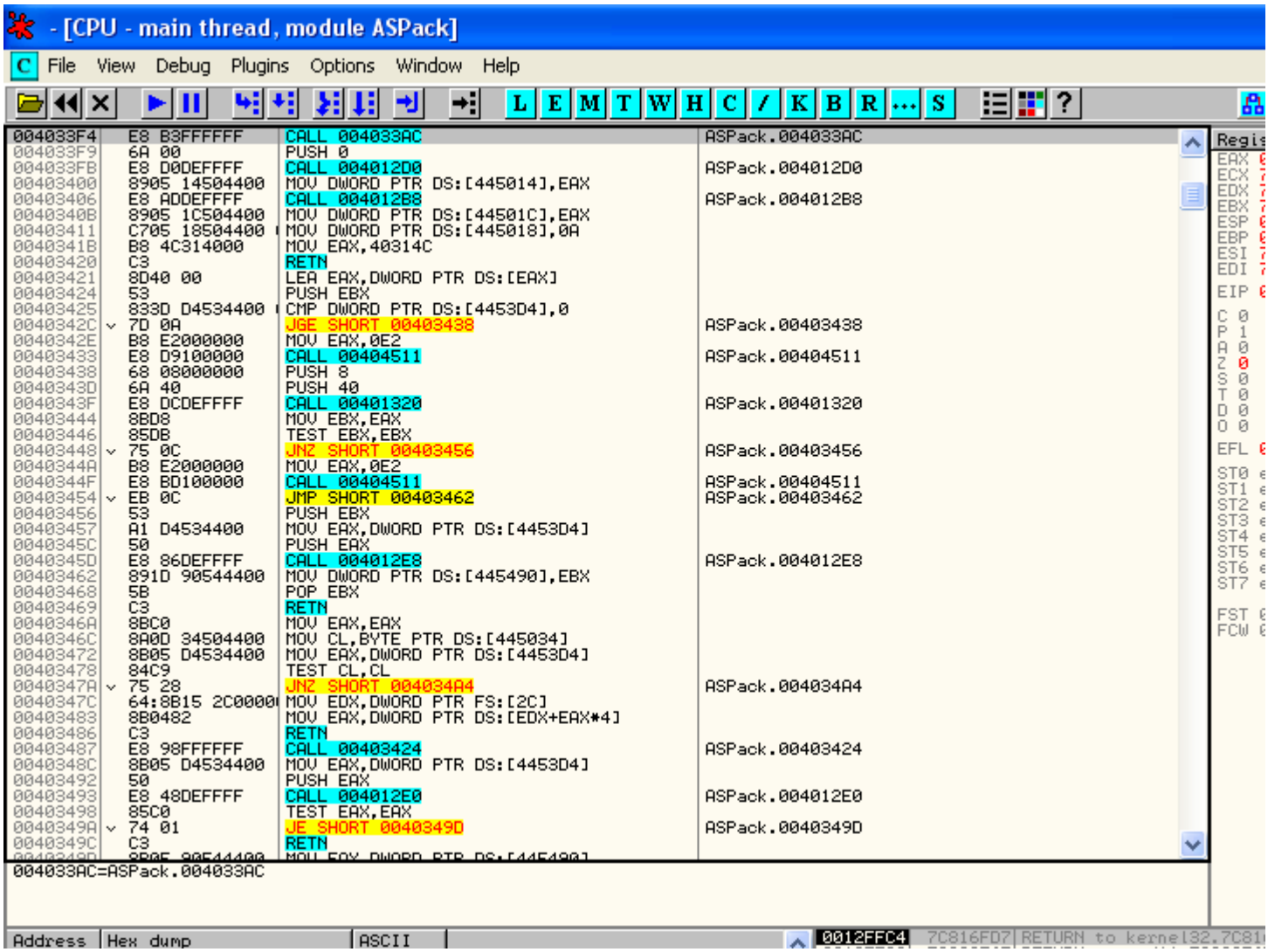
Le dan a OK y ahora simplemente le dan a F9 y empiezan a pasar las excepciones con Shift +F7 y F9 y teniendo mucho cuidado al contar las excepciones hasta que el programa arranque (en mi caso fueron 26 excepciones). Ahora reiniciamos Olly con Ctrl. + F2 y hacemos lo mismo pero esta vez nos pararemos en la ultima excepción y le damos a Shift + F7 solo para pasarla.
Ahora pulsamos Alt + M para sacar la ventana Memory Map y marcamos la sección .code del ejecutable y le ponemos un BP Memory on Access haciendo clic derecho sobre ella como se muestra en la imagen:



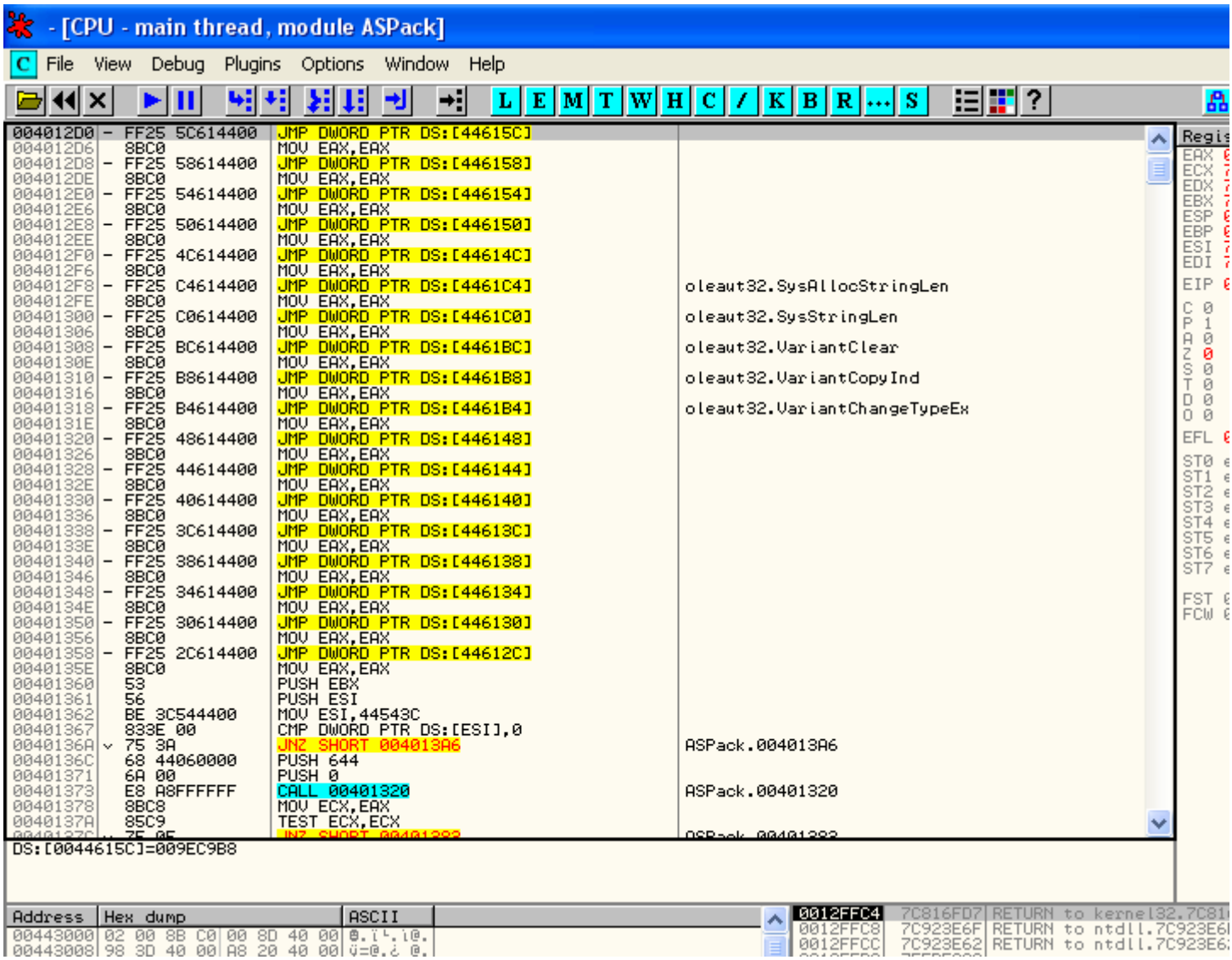
Y ahora demos a F9 y…



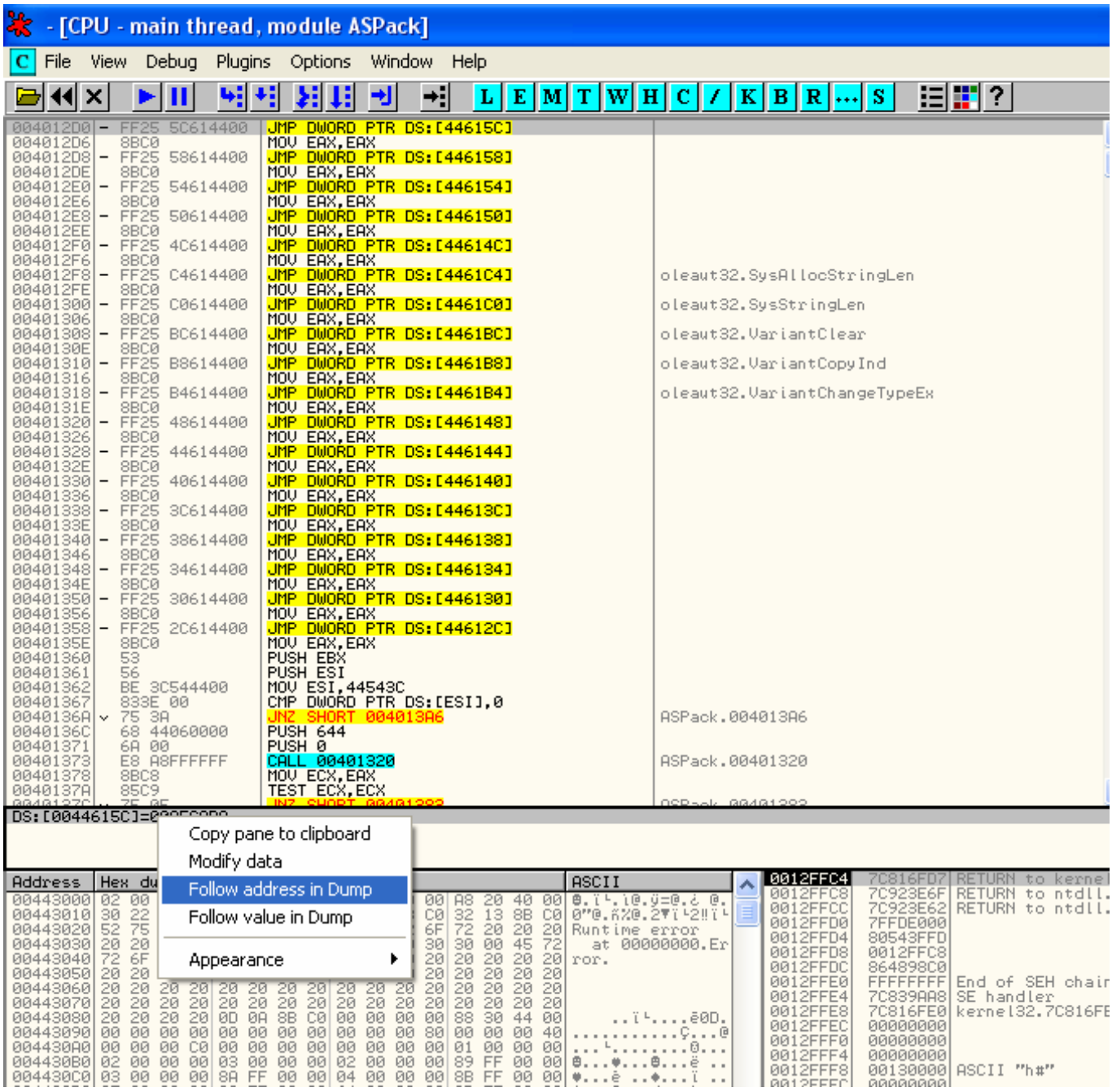
Ya estamos en el OEP y tiene buena pinta porque parece ser que no hay Stolen Bytes así que sigamos.
Para encontrar la IAT simplemente ponte encima de la primera CALL y das Intro a ver a donde nos lleva:



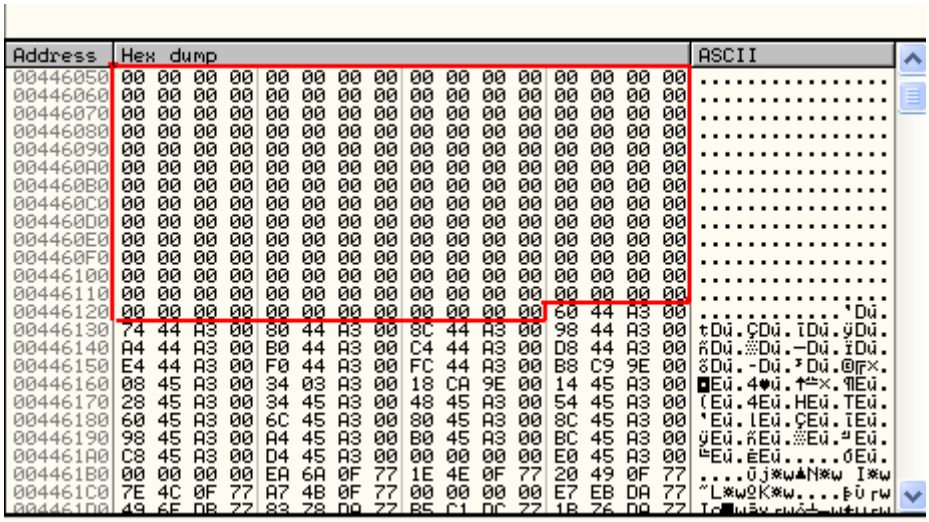
No se ve nada interesante pero como siempre se llama a alguna API muy cerca del OEP, pues probare a ver que hay dentro de esas CALLs.
En la primera no hay tampoco nada interesante pero en la segunda salimos aquí:



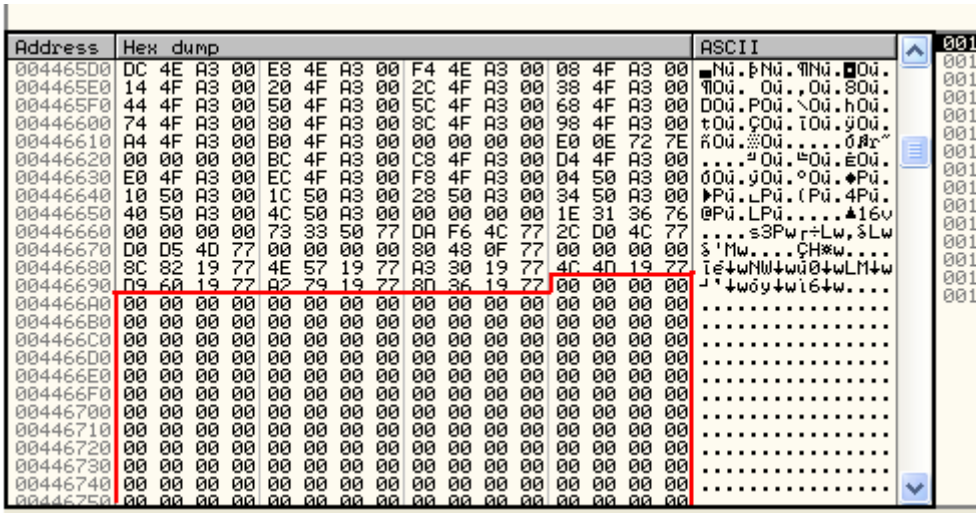
Bueno pues ya dimos con la zona caliente para dar con la IAT. Ahora nos ponemos encima de cualquiera de esos saltos incondicionales que empiezan con FF25 y nos vamos al panel que es la parte de debajo de la ventana Disassembler y hacemos clic derecho sobre el valor que se ve y elegimos Follow Address in Dump:



Y ya estamos en la IAT aunque tiene muy mala pinta y esta redireccionado casi todo hacia el Asprotect pero vamos a repararla. Lo primero es ver donde empieza y donde termina y para ello subamos buscando a ver si vemos una zona de 00000000 o vemos direcciones seguidas que no tengan referencias (para saber si un dword tiene referencias lo marcamos y hacemos Ctrl. + R y si sale la lista vacía es porque no es un dato valido de nuestra IAT y sobra así que si no se ve la zona de 00000000 tendríamos que buscar el inicio de nuestra IAT mirando si los dwords tienen referencias o no. En este caso tenemos suerte y Podemos ver el comienzo de la IAT en 446128 :



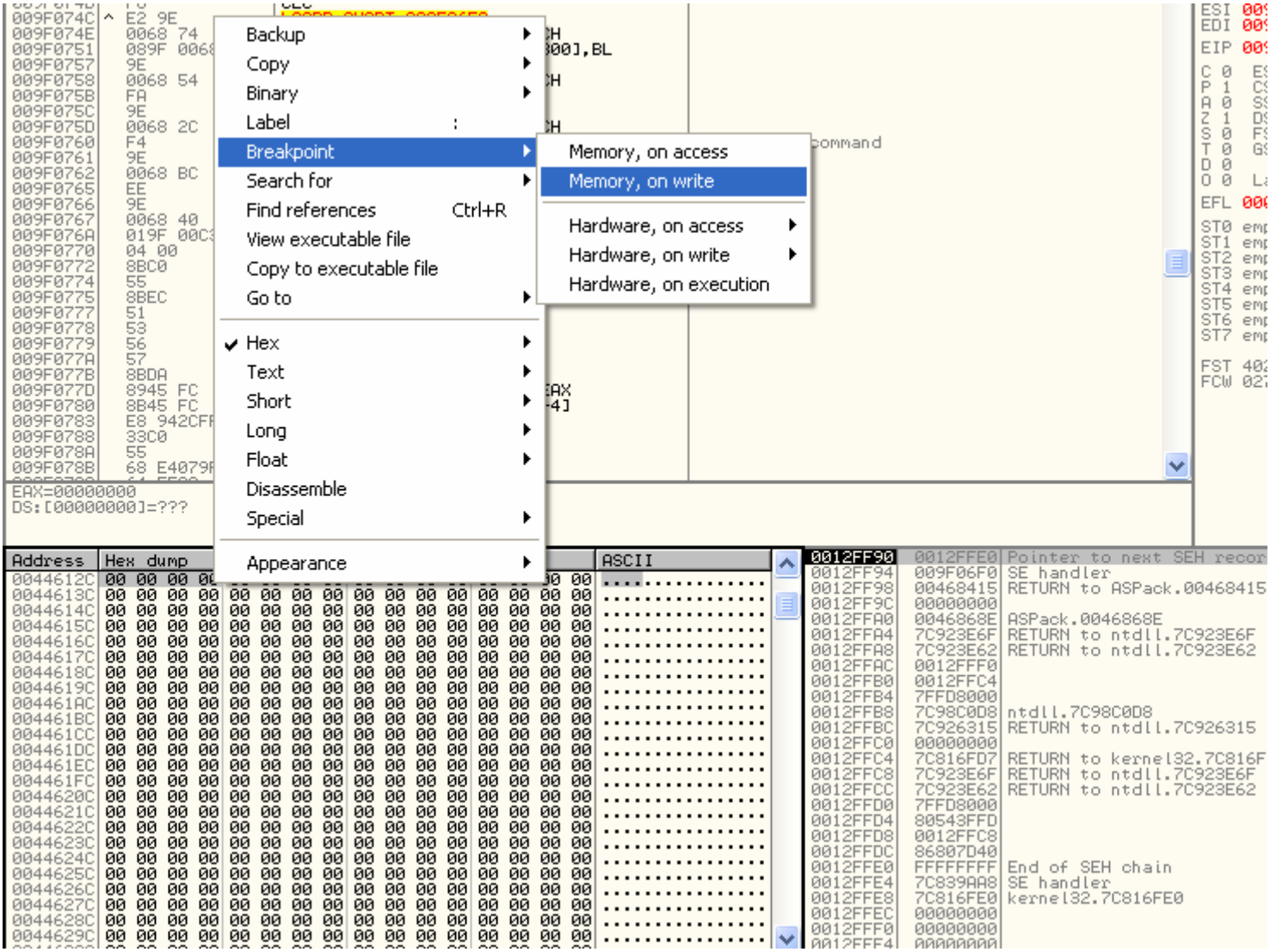
Y en 4466A0 podemos ver también claramente el final:



Entonces tenemos que:
El OEP es 44289C
El inicio de la IAT esta en 446128
El fin de la IAT esta en 4466A0
Y su tamaño es el resultado de restarle al fin de la IAT el inicio de la IAT así que:
Tamaño de la IAT = 4466A0 – 446128= 578

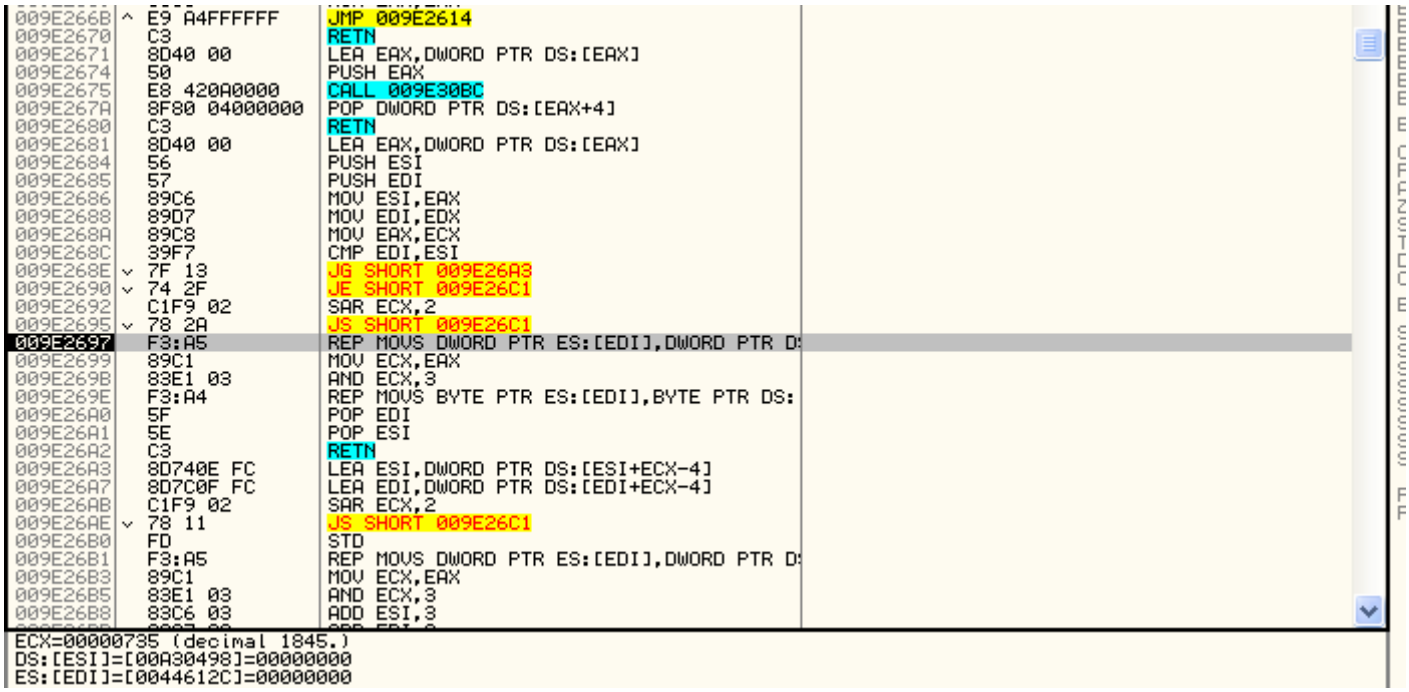
A LA CAZA DEL CALL SEMI-MAGICO

Ahora reiniciemos y vayamos a 44612C que es el principio de las direcciones que debe escribir en nuestra IAT y pongamos un Memory Breakpoint on Write:

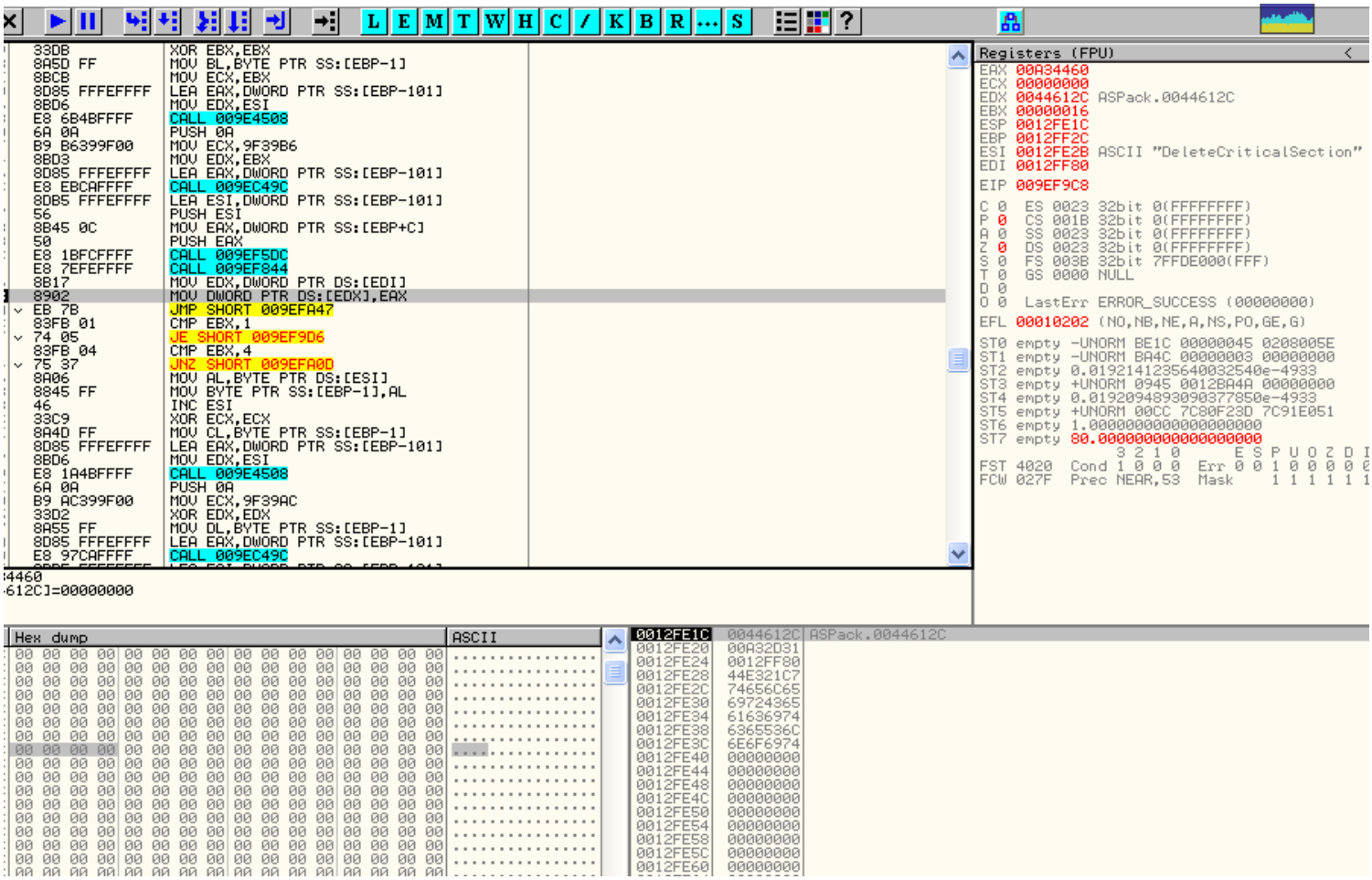


Y le damos a F9 y empezamos a pasar las excepciones otra vez igual que antes pero esta vez hay que tener mucho cuidado porque hay que contar muy bien las excepciones ya que te puedes equivocar y contar la parada en el BPM como si fuera una excepción.

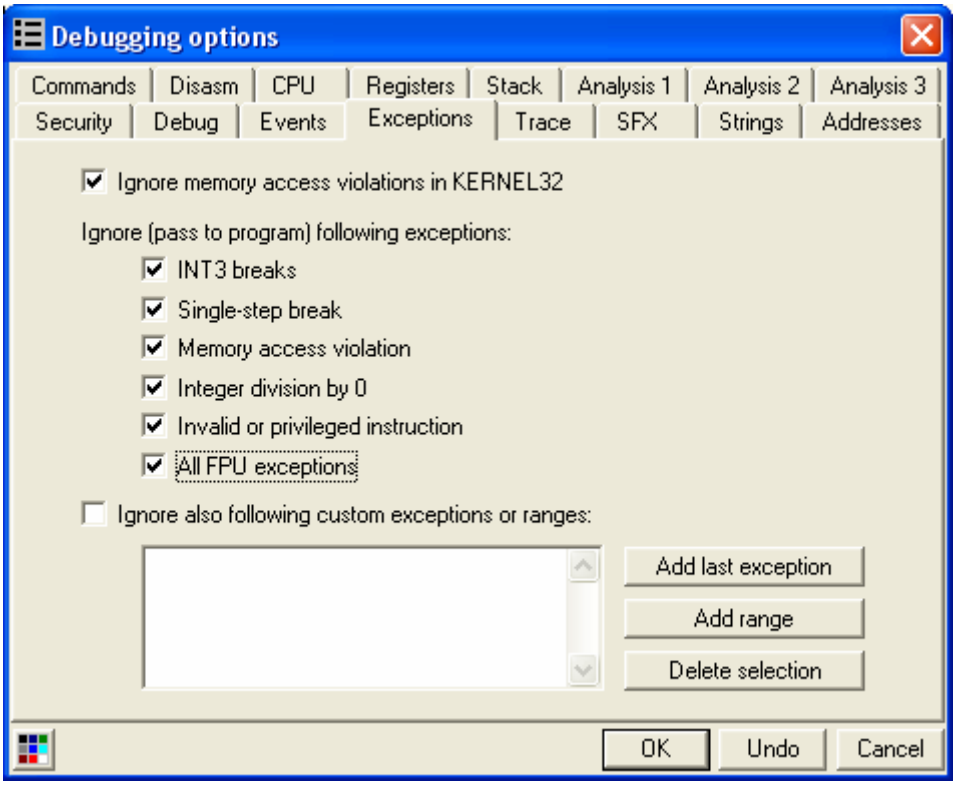
La primera vez que para por nuestro BPM es en :



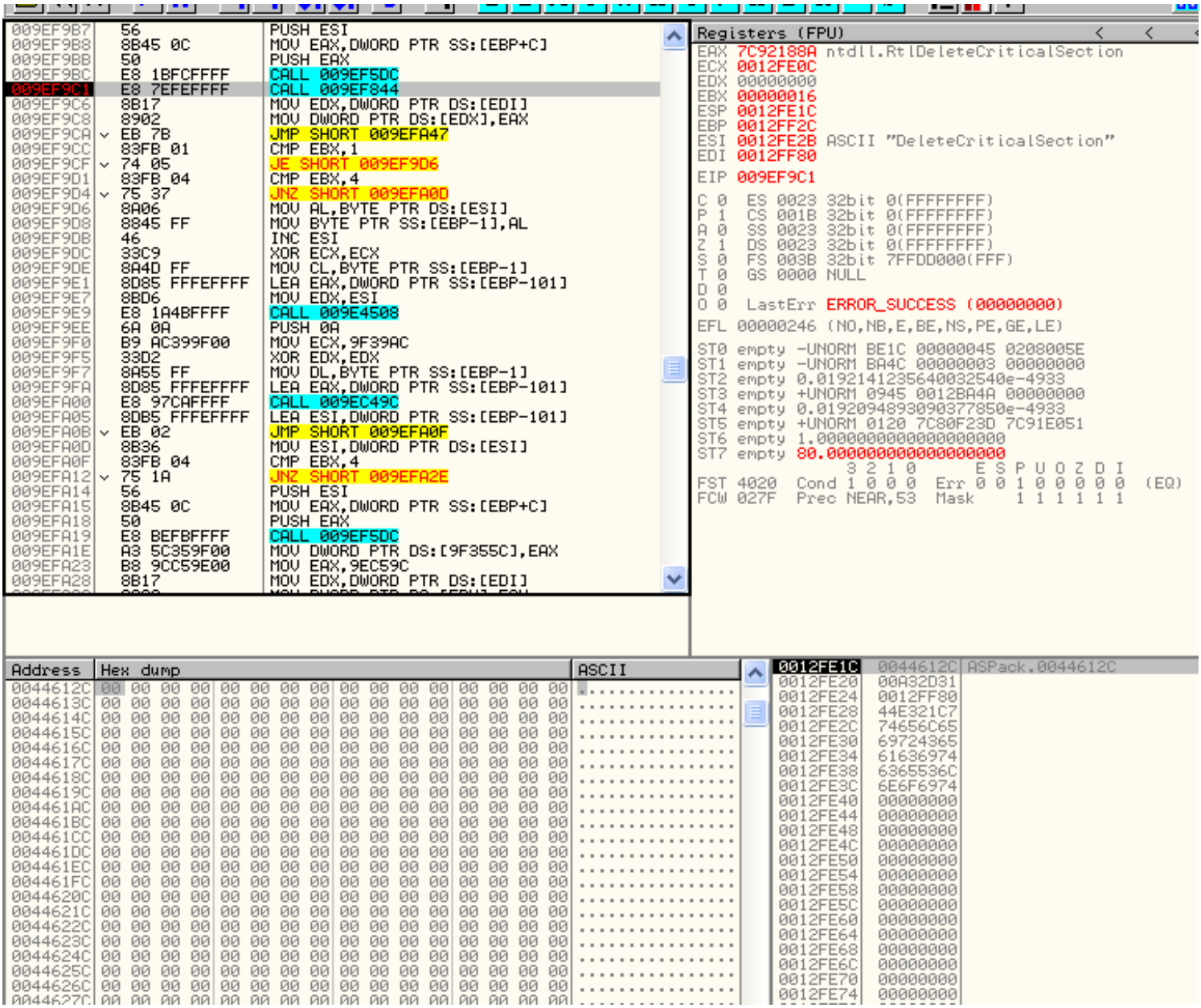
Esta no nos interesa así que sigamos y recordad que esta vez que paro no la debéis contar ya que no fue una excepciona si que sigamos:



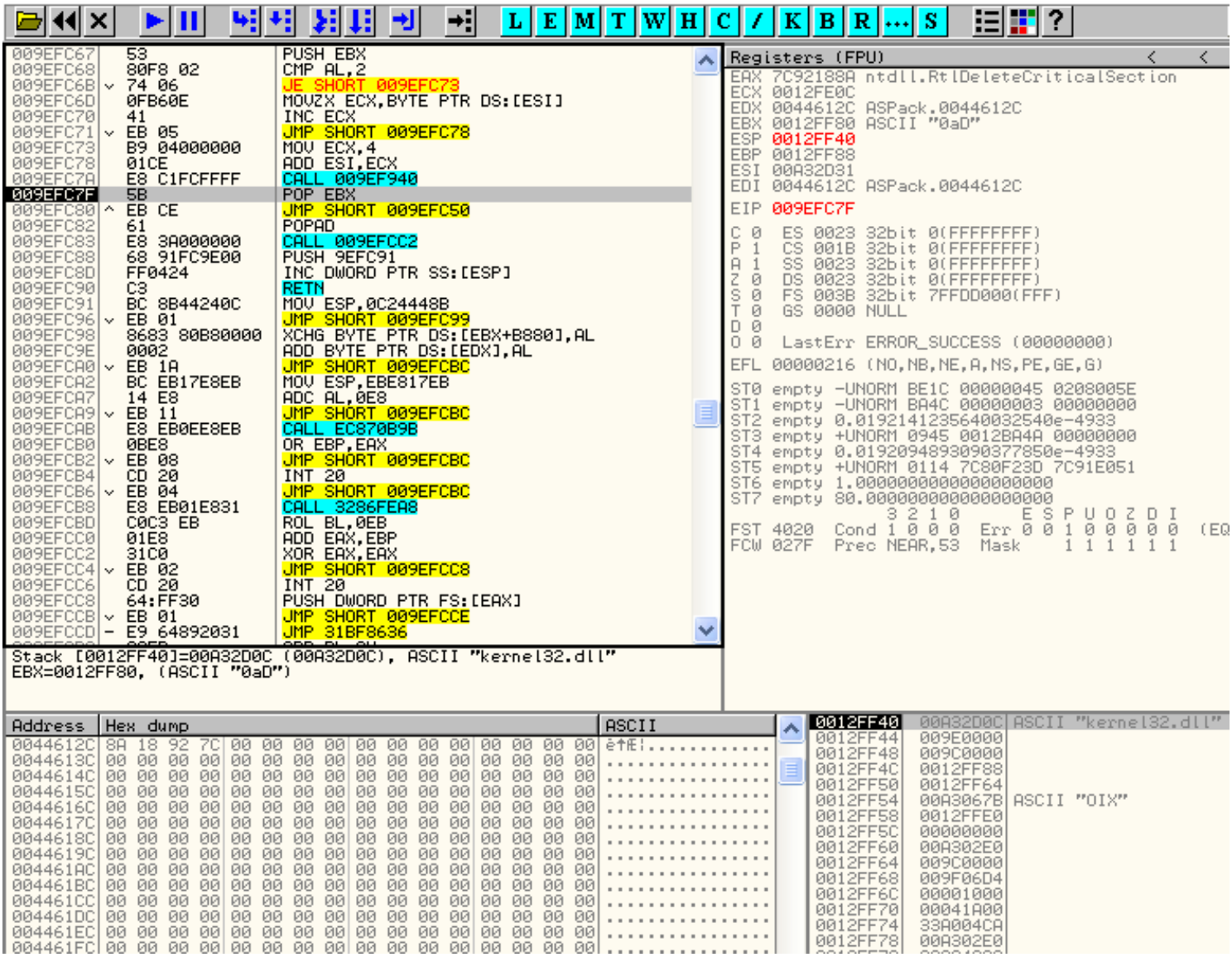
Esta si es importante ya que esta justo después del salto semi-mágico que nos arreglara casi toda la IAT.
El salto que tendremos que nopear será el que esta encima de donde nos detuvimos así que apuntemos la dirección donde esta ese CALL y volvamos a reiniciar con Ctrl. + F2. Le damos a F9, le damos a Ctrl. + G y metemos la dirección de donde estaba la CALL que en mi caso esta en 009EF9C1 y le damos a OK y nos llevara a donde esta la CALL. Le ponemos un BP y pulsamos Alt + O y marcamos todas opciones de la pestaña Exceptions excepto la última:



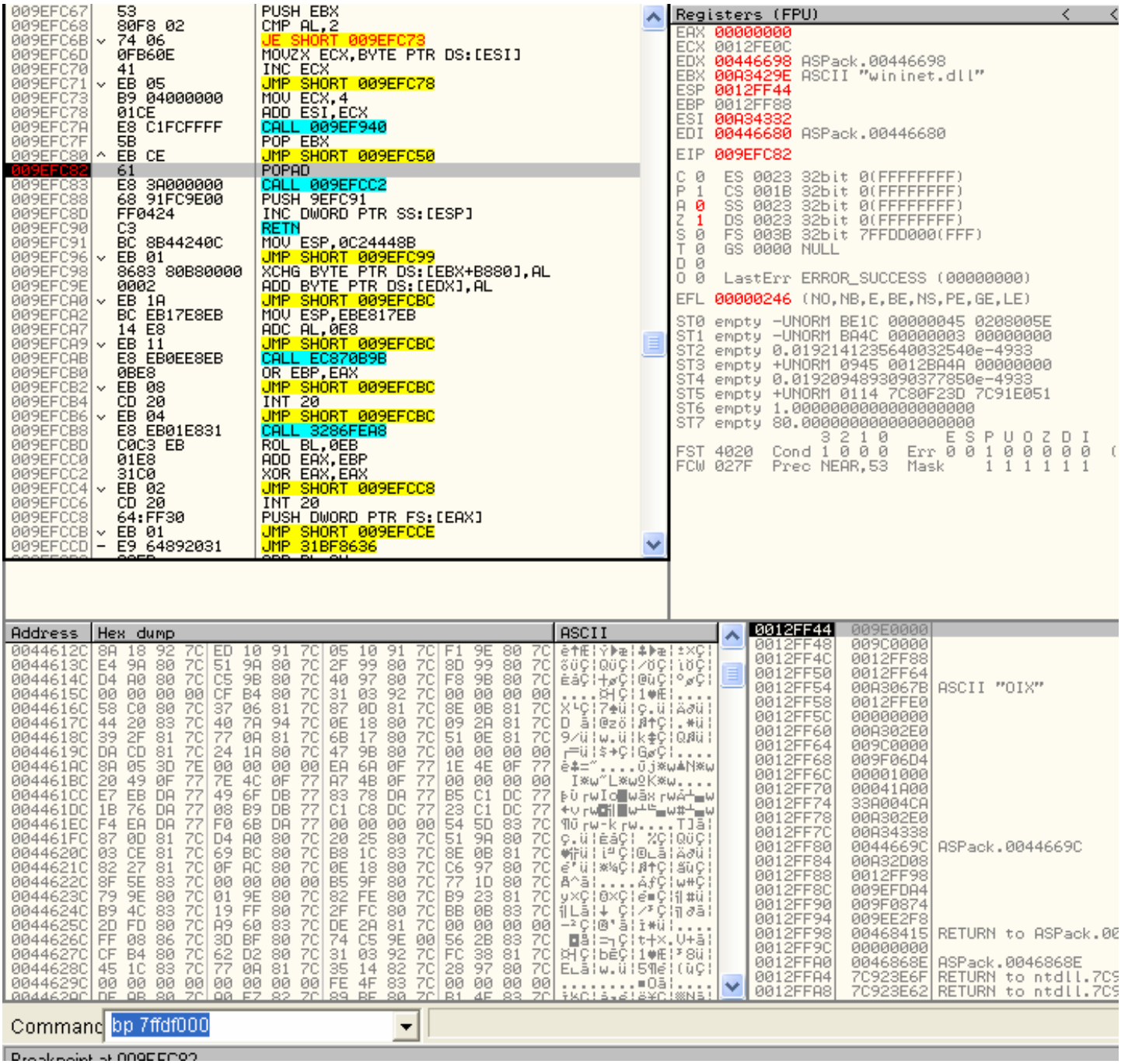
Damos a OK y ahora Shift + F7 y F9 y llegamos al BP.



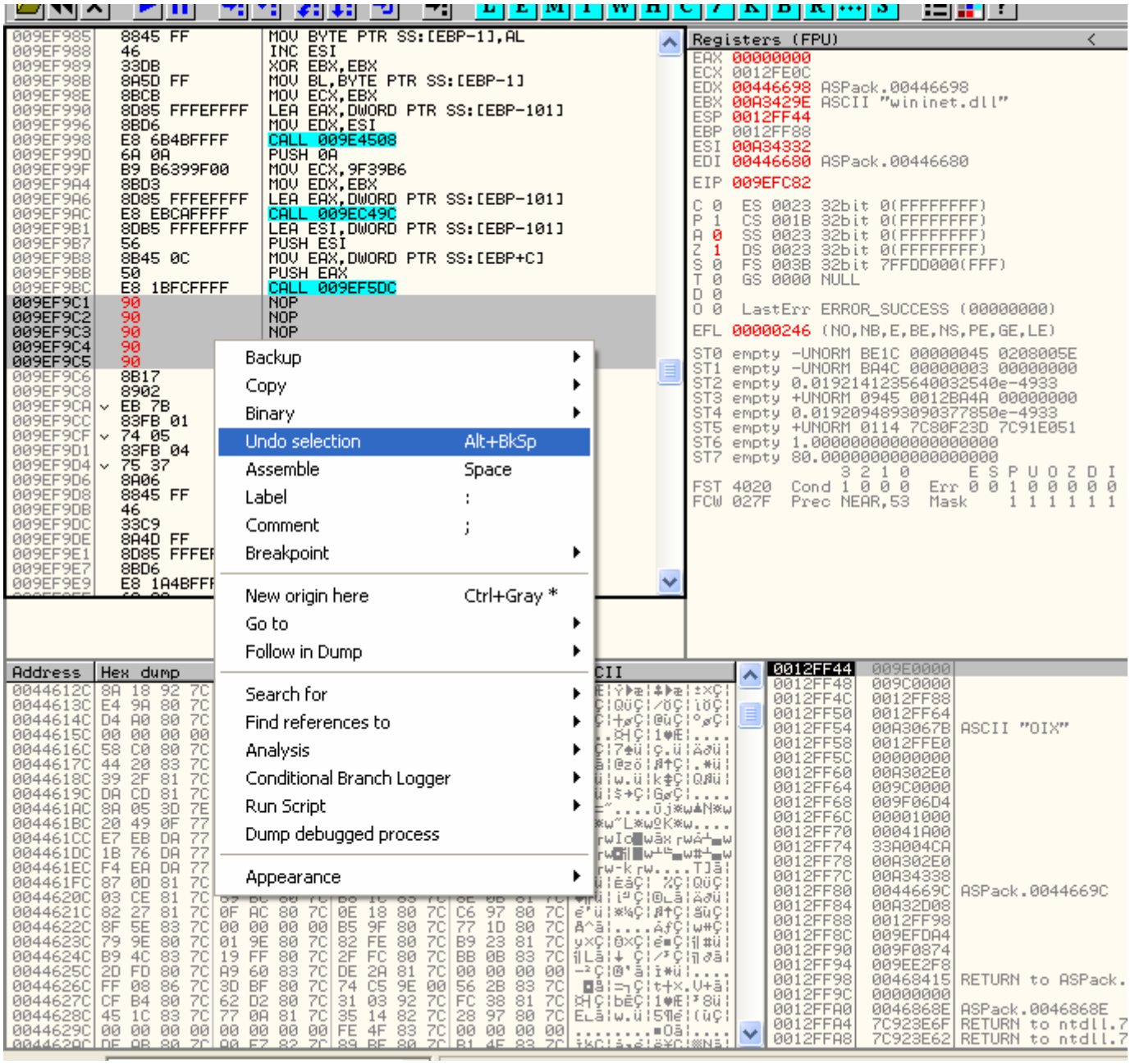
Parece que vamos bien, jeje, miren el valor que se encuentra en EAX. Es una entrada buena a la IAT. Pues quitemos el BP y nopeemos el CALL y vamos trazando con F8 hasta que vemos un POPAD (hay que tracear muy poco, en mi caso con pulsar 15 veces F8 llegue a el).



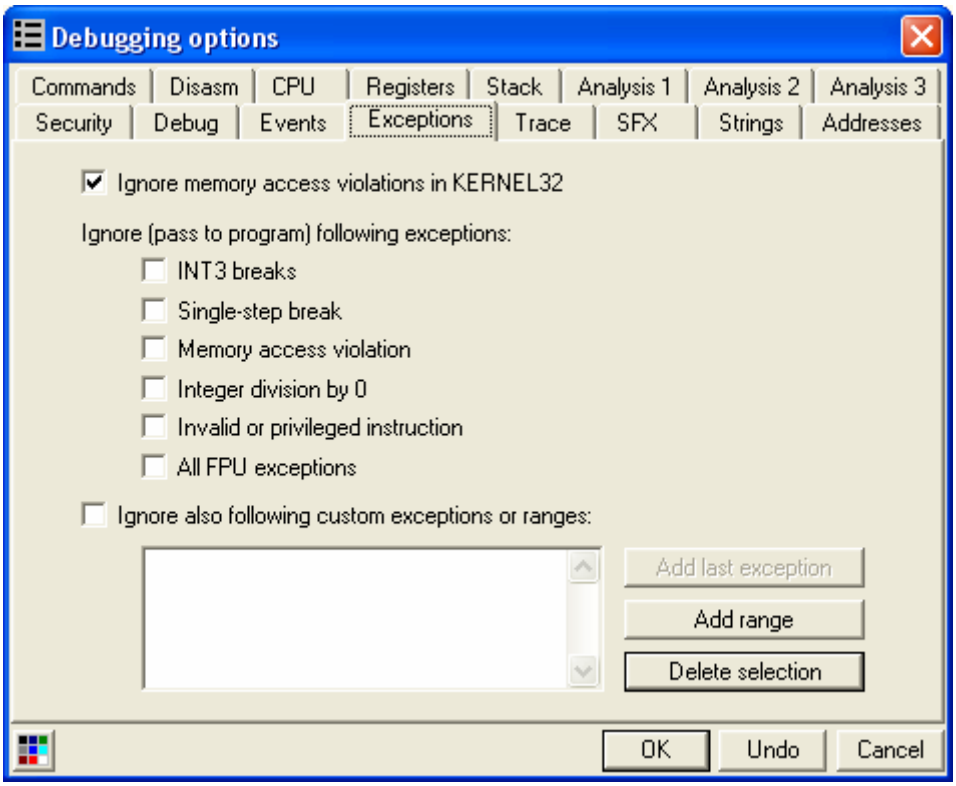
Bueno, en la anterior imagen podemos ver el POPAD, pero no solo eso, también podemos ver que nuestro primer valor de la IAT ya si que parece una entrada de la IAT buena. Para que nos la repare toda sin tener que tracear para reparar toda la IAT, pongamos un BP en el POPAD y demos a F9.



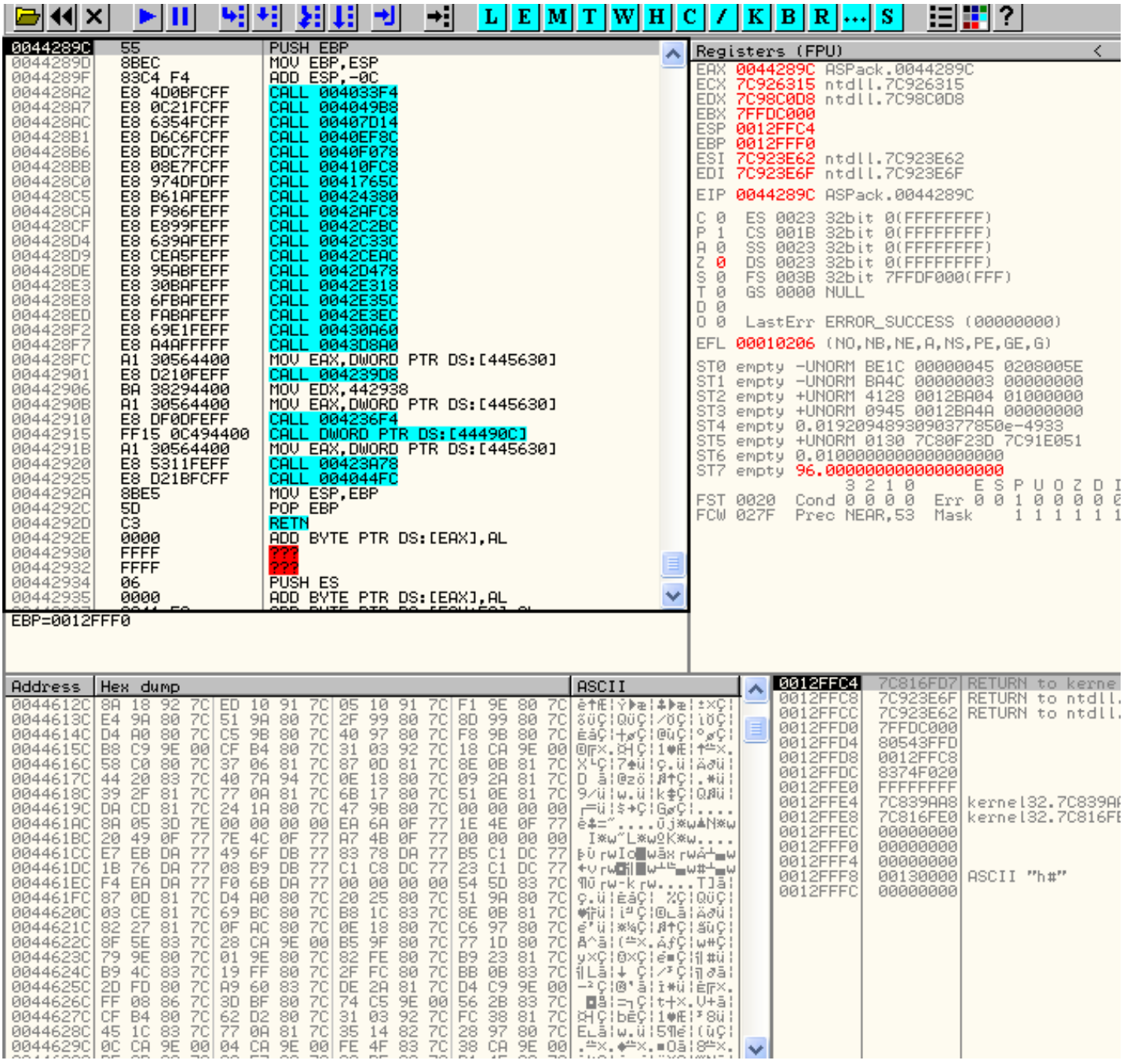
Mirad que bien quedo la IAT, jeje, ahora quitemos el BP y con el – del teclado vamos volviendo hacia atrás hasta llegar a los nops de la CALL que nopeamos y una vez allí seleccionamos todos los nops que forman parte del lugar donde estaba el CALL, hacemos clic derecho y le damos a Undo Selection para dejarlo como antes y que no nos detecte Asprotect:



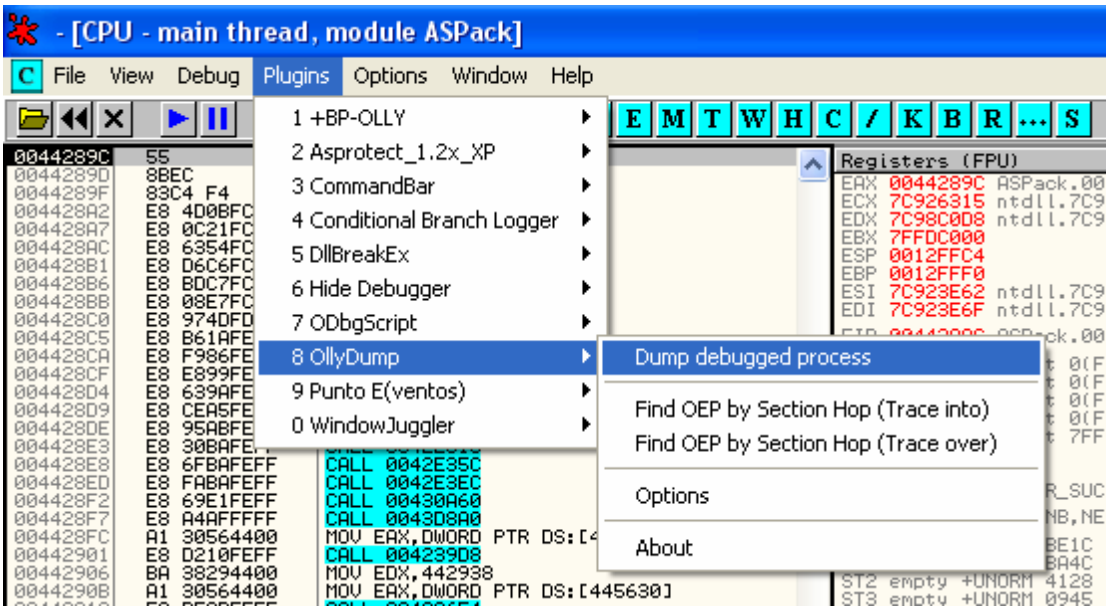
Ahora volvemos a pulsar Ctrl. + O y volvemos a dejar desmarcadas todas las opciones menos la primera:

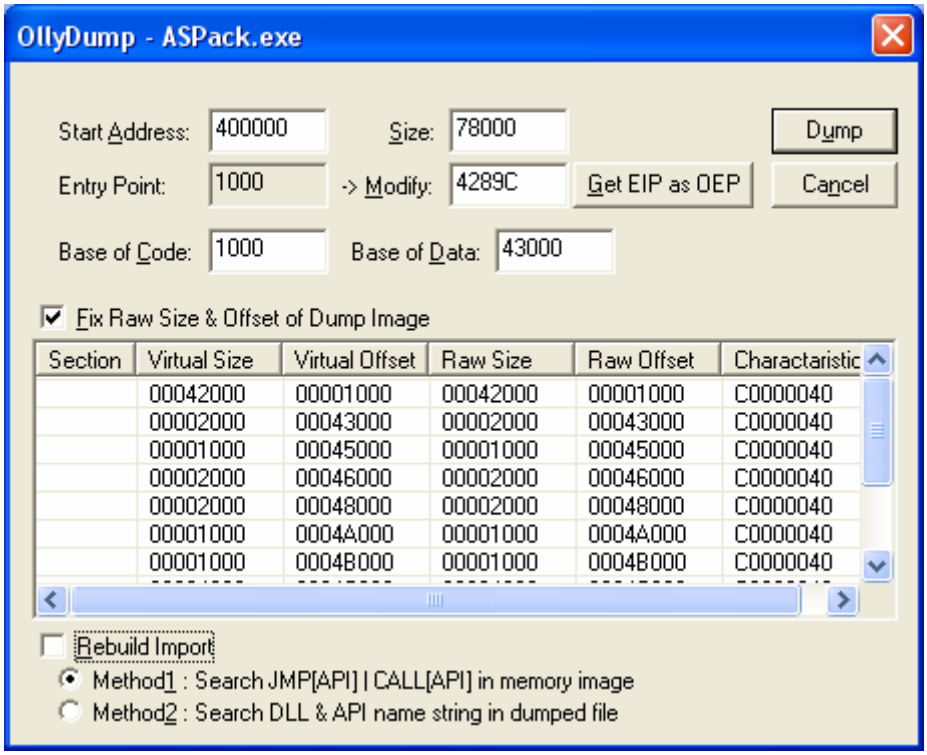


Aceptamos y le damos a F9 y empezamos a contar las excepciones incluida la primera que te da a al darle a F9. En mi caso, a la 10 ya arranca el programa así que vuelvo a reiniciar el Olly y vuelvo a hacer todo igual para reparar la IAT hasta volver a llegar a este punto donde ya se que tengo que parar en la excepción 9ª en mi caso. Una vez parado en la ultima excepción antes de que arranque el programa, voy al Memory Map con Alt + M y pongo un Breakpoint on Memory Access en la sección .code del ejecutable y le doy a F7 y F9 y nos parara en el OEP y esta vez con la IAT prácticamente reparada.

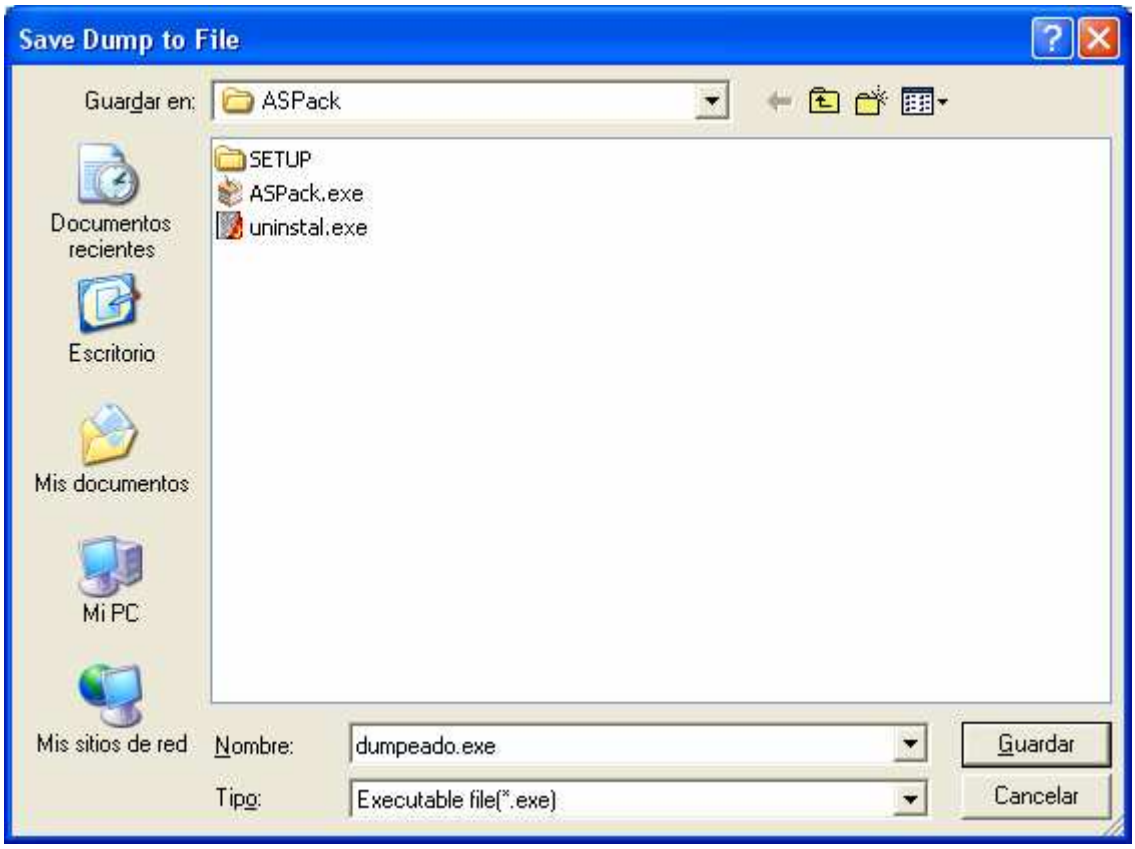


Este es el momento de dumpear y yo lo haré con el plugin para Olly OllyDump así que adelante:

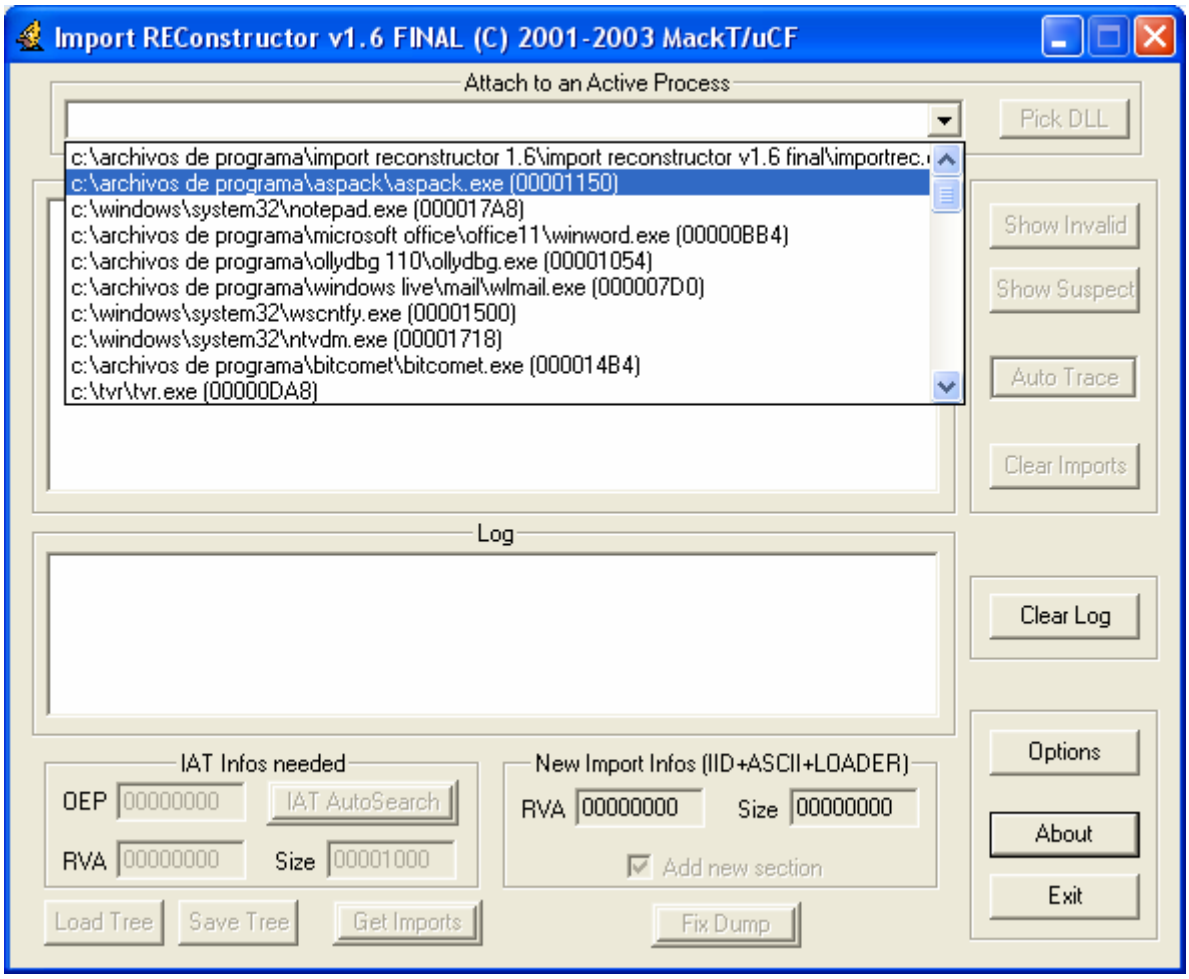




Nos aparece una ventana como la de arriba a la cual le desmarcamos la opción Rebuild Import y le damos a Dump y en la siguiente ventana elegimos un nombre y una ubicación y le damos a Guardar y ya tenemos nuestro dumpeado.



Ahora le vamos a reparar la IAT y para ello usaremos Import Rec.
Lo ejecutamos y como se muestra en la siguiente imagen, buscamos en la lista nuestro proceso para atachearlo y hacemos clic encima.



Ahora llega el momento de meter el OEP, RVA y Size y para eso lo apuntamos todo antes.
El Oep es el que tenemos apuntado menos la Image Base que es 400000.

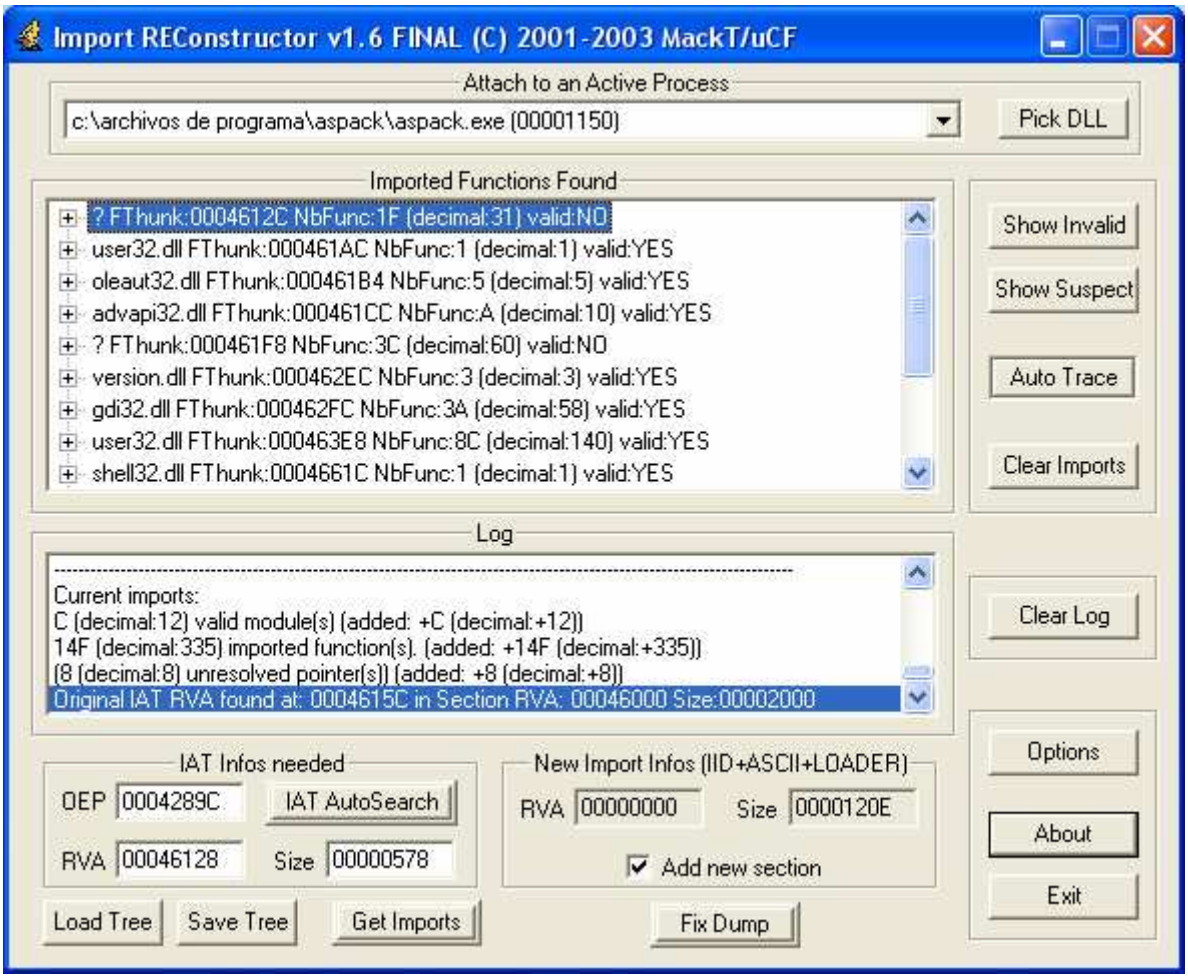
44289C – 400000 = 4289C Axial que ya tenemos el dato para meter en el OEP.

El RVA es el inicio de nuestra IAT menos la Image Base así que:

446128 – 400000 = 46128

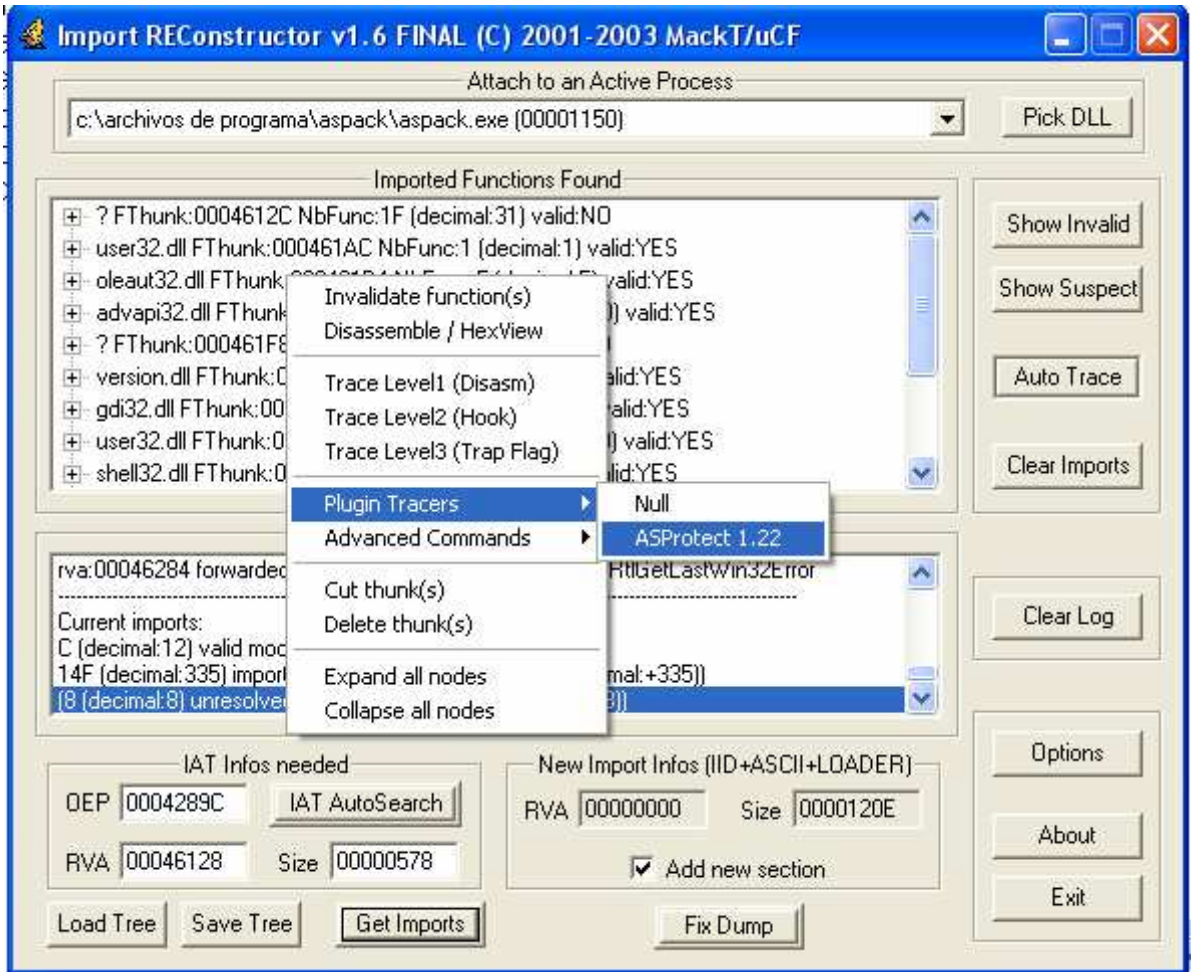
Y el Size es el tamaño de nuestra IAT.

Metamos solo el OEP y demos al botón IAT AutoSearch a ver que pasa.

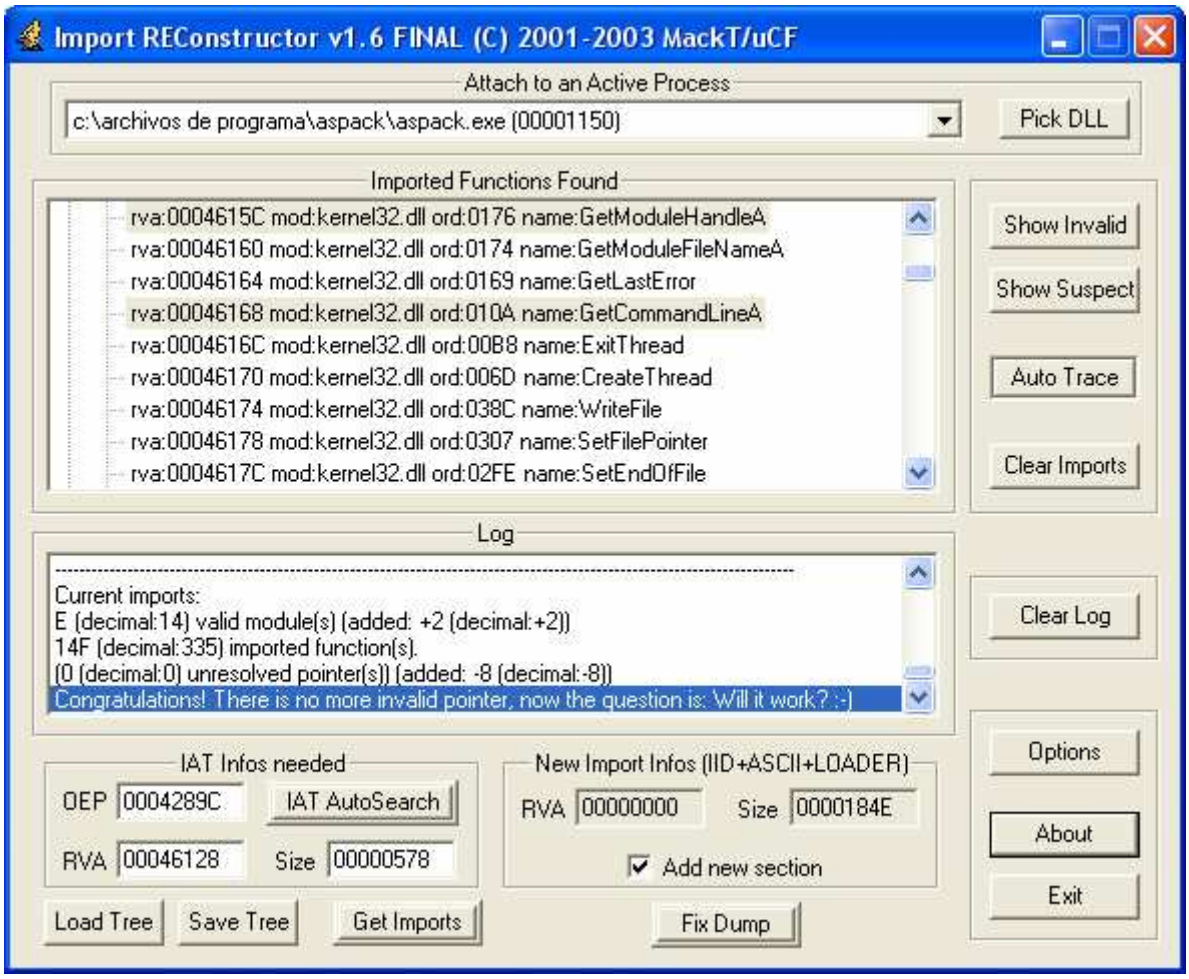


Como vemos, todos los datos coinciden así que vamos bien. Ahora demos al botón Get Imports y nos deben de aparecer todas las llamadas a las apis que realiza nuestra IAT.

Pero hay un problema, como pueden ver arriba, hay entradas malas que tendremos que resolver nosotros pero antes me queda un ultimo cartucho, usaremos el plugin para Asprotect 1.22 que se le puede meter al ImportRec y que en mi caso ya lo trae así que hago clic en el botón Show Invalid y acto seguido clic derecho encima de la lista que aparece y ejecuto el plugin.

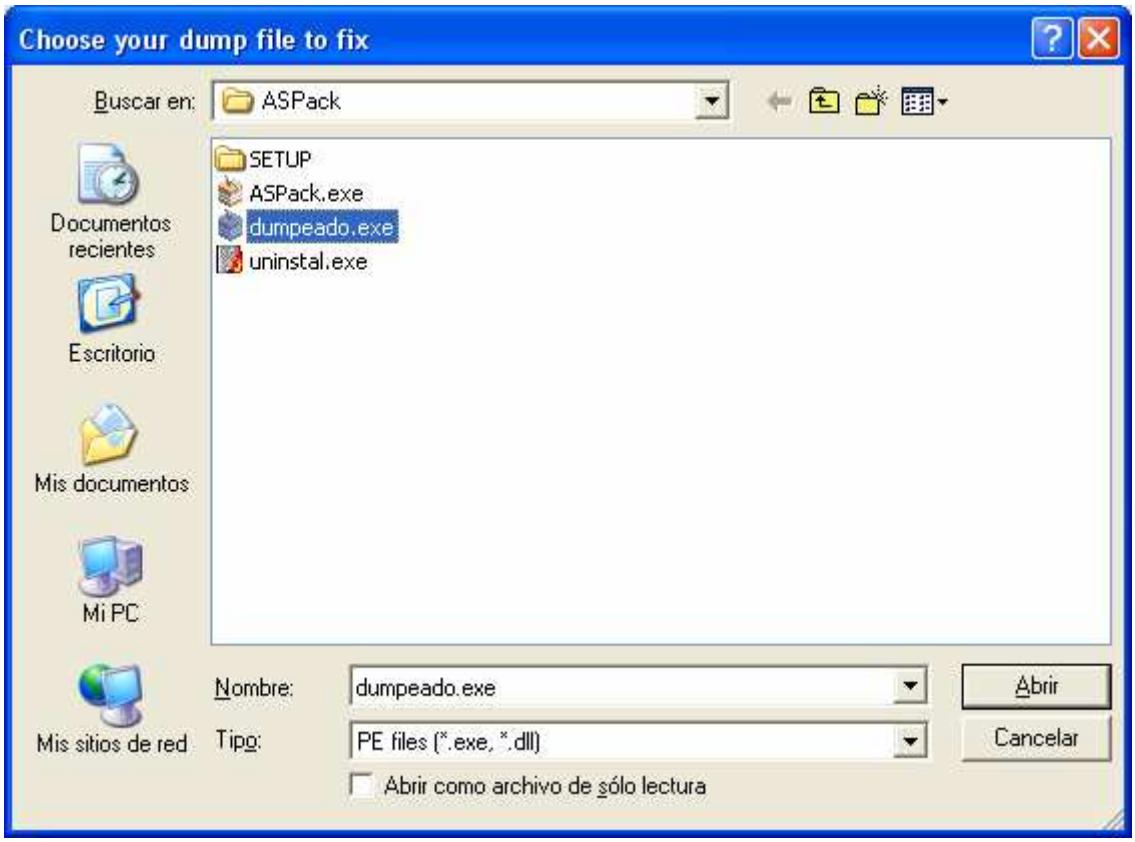


Y el resultado es…



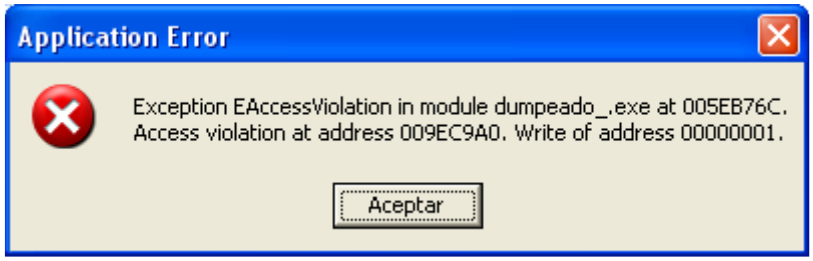
Como se puede apreciar, en el Log nos dice que ya no quedan mas entradas malas por resolver y nos felicita.
¡ Ya la tenemos reparada!

Ahora demos al botón Fix Dump y elijamos el dumpeado que hicimos antes:



Le damos a Abrir y…

En el Log nos dice que el archivo se guardo sin problemas así que intentemos ejecutar nuestro dumpeado a ver que pasa. Ojo, el dumpeado con la IAT correcta se guardara como dumpeado_.exe.



Bueno, este Asprotect tiene algunos ases en la manga pero intentaremos derrotarlo. Carguémoslo en otro Olly .

Bueno, aparecemos en el OEP bueno y el método que voy a usar para sacar el error es el siguiente.
En el Olly con el dumpeado, dejo pulsada F8 hasta que me da la siguiente excepción:

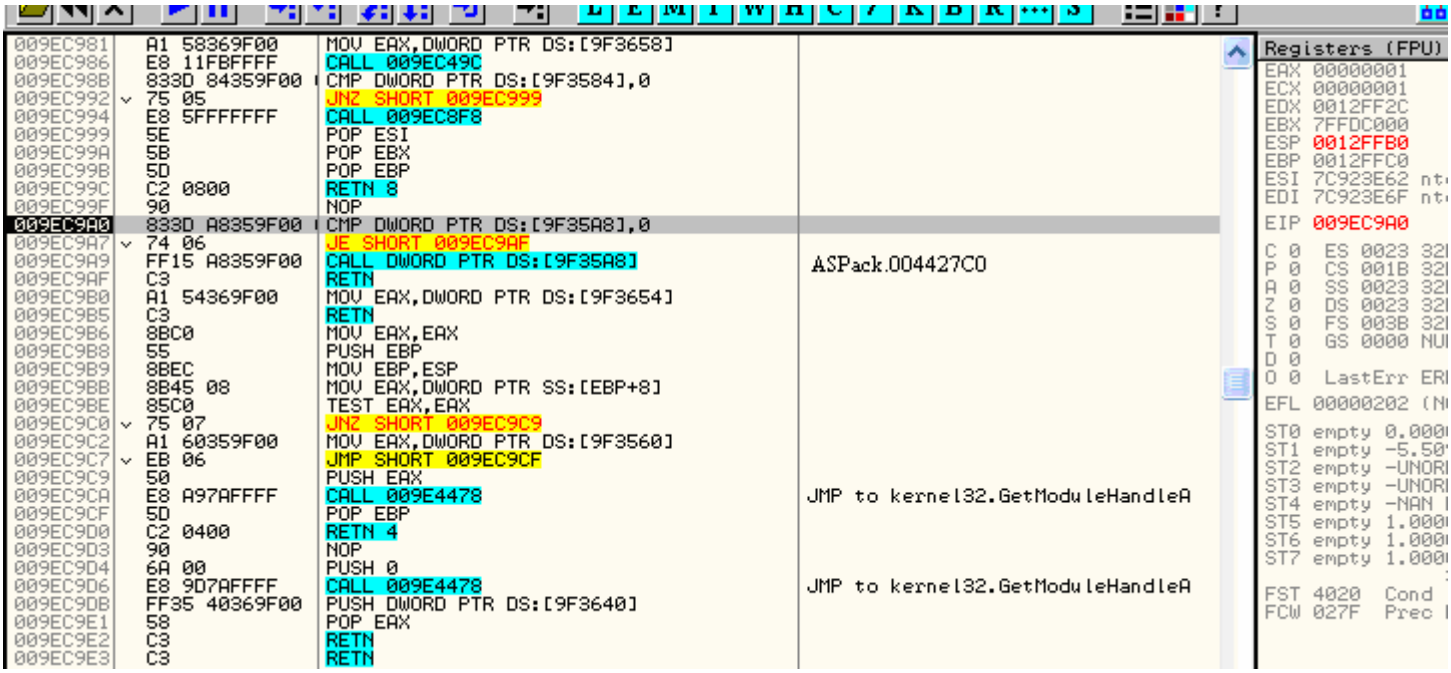
Access violation when writing to [00000001]

Si miramos la pila vemos justo arriba del todo:

0012FFB0 0044291B RETURN to dumpeado.0044291B from 009EC9A0

O sea, que donde estamos hemos llegado desde un CALL y si todo hubiera ido bien nos habría retornado a 0044291B así que vayamos allí a ver que vemos. Para ello hacemos clic derecho sobre esa entrada de la pila y elegimos Follow in Disassembler o pulsamos Intro y apareceremos en el retorno de esa CALL.

Es curioso pero estamos unas líneas mas abajo del OEP y el CALL que nos mando allí es el que esta justo encima y es el único de todos los que vemos ahí que usa una dirección indirecta.
Pues bien, vayamos al Olly que tiene el programa original parado en el OEP y vayamos con F8 hasta llegar a ese CALL sin ejecutarlo y cuando estemos encima de el pulsamos F7y vemos:



Pues vale, guardemos esta dirección por si nos volviera a hacer falta y ahora con F7 vamos traceando a ver que pasa y veremos que no se cumple la condición y el salto no se realiza y nos quedamos parados un momento en el CALL que esta justo después del

salto para ver a donde va ya que justo después tenemos un RETN y ese CALL es lo ultimo que se ejecutara en ese trozo de código y veremos esto:

009EC9A9 FF15 A8359F00 CALL DWORD PTR DS:[9F35A8] ; ASPack.004427A8

O sea, que eso es lo mismo que un CALL 004427A8, pues apuntemos eso también que va ha ser vital.
Ahora vamos a comprobar algo; estando parado en el CALL, pon un BP en el salto que tienes justo encima y que no se realizo antes porque la condición no se cumplía. Ahora quitemos el BPM y demos a F9 a ver si vuelve a parar ahí.
Bueno pues ya os digo que no para y como 004427C0 esta dentro del código del ejecutable pues vamos a hacer algo.
Sabemos que:

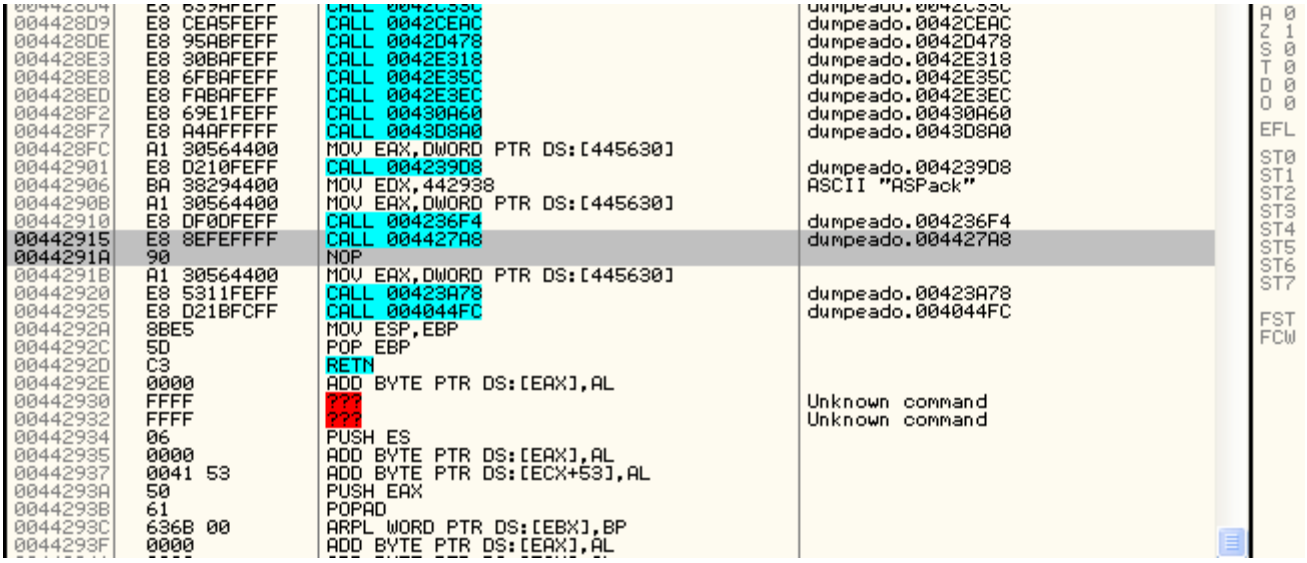
00442915 FF15 0C494400 CALL DWORD PTR DS:[44490C]

Nos manda de cabeza a …

009EC9A9 FF15 A8359F00 CALL DWORD PTR DS:[9F35A8] ; ASPack.004427A8

Y que este ultimo CALL es igual que hacer CALL 004427C0

Pues me la juego, voy a hacer algo interesante porque no tendré ni que crear ningún tipo de injerto especial ni nada, simplemente cambiare al primer CALL para que vaya al lugar que va el otro CALL ya que el error que me da en el dumpeado es porque el salto indirecto del primer CALL no esta bien y con esto podríamos solucionarlo.
Quedaría así:

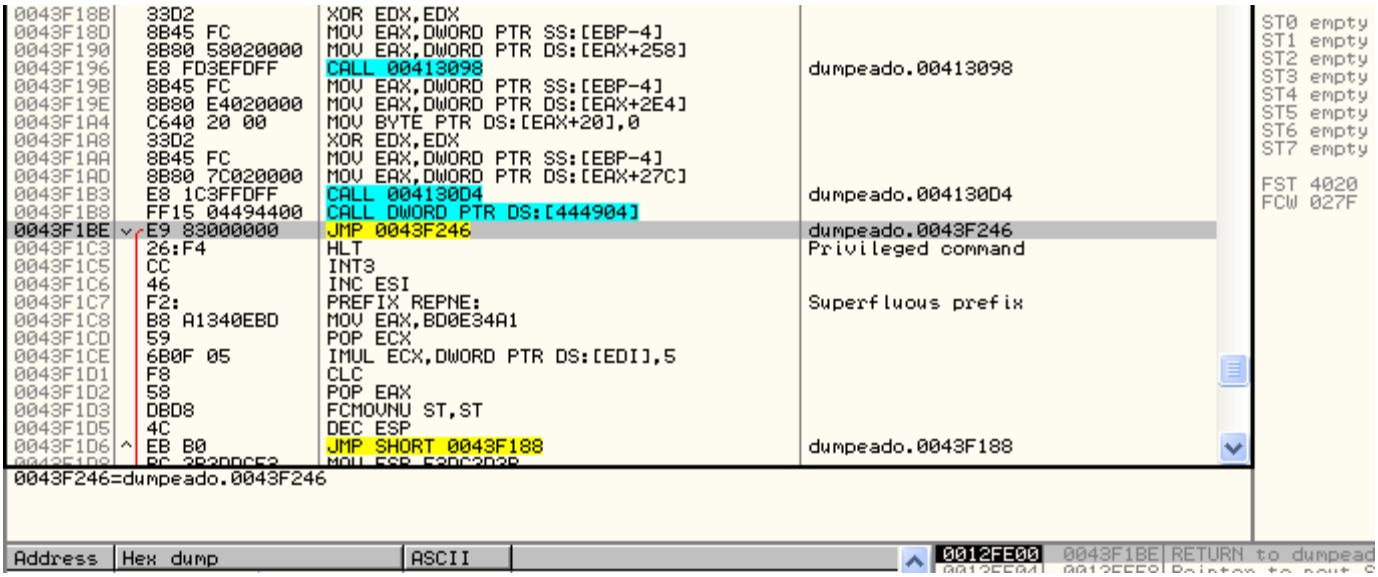


Ahora guardemos los cambios seleccionando las líneas que hemos modificado y haciendo clic derecho y dándole a Copy to Executable->Selecction y acto seguido reiniciemos el Olly que tiene el dumpeado y ejecutémoslo a ver que pasa ahora.

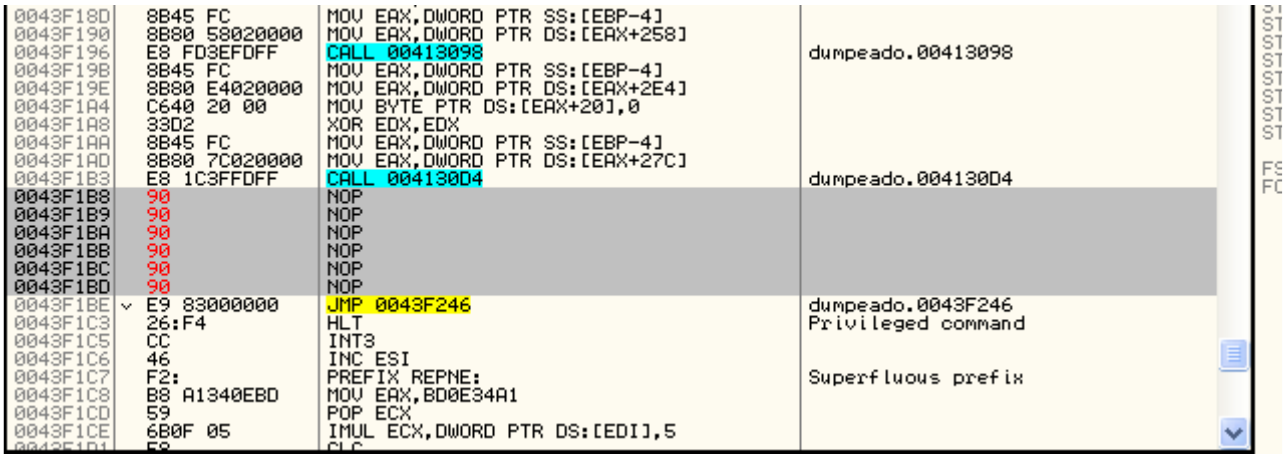
Y nos vuelve a dar otro error igual que el de antes. Axial que lo mismo, miremos en el Stack a ver si hay suerte y…

0012FE00 0043F1BE RETURN to dumpeado.0043F1BE from 009EC8F4

Pues vallamos a 0043F1BE colocándonos encima de esa entrada del Stack y dándole a Intro a ver que se cuece por allí.



Pues miremos en el original a ver que hace el CALL que tenemos justo arriba que es el culpable del error. Simplemente vamos a la dirección donde esta la CALL y damos a Intro y, sorpresa sorpresa, jeje, lo único que hace es ir a esa zona que se crea en ejecución y donde solo se encuentra un RETN con lo cual ese CALL es simplemente una trampa para que no lo podamos dumpear limpiamente así que nopeemos ese CALL en el dumpeado y quedara así:

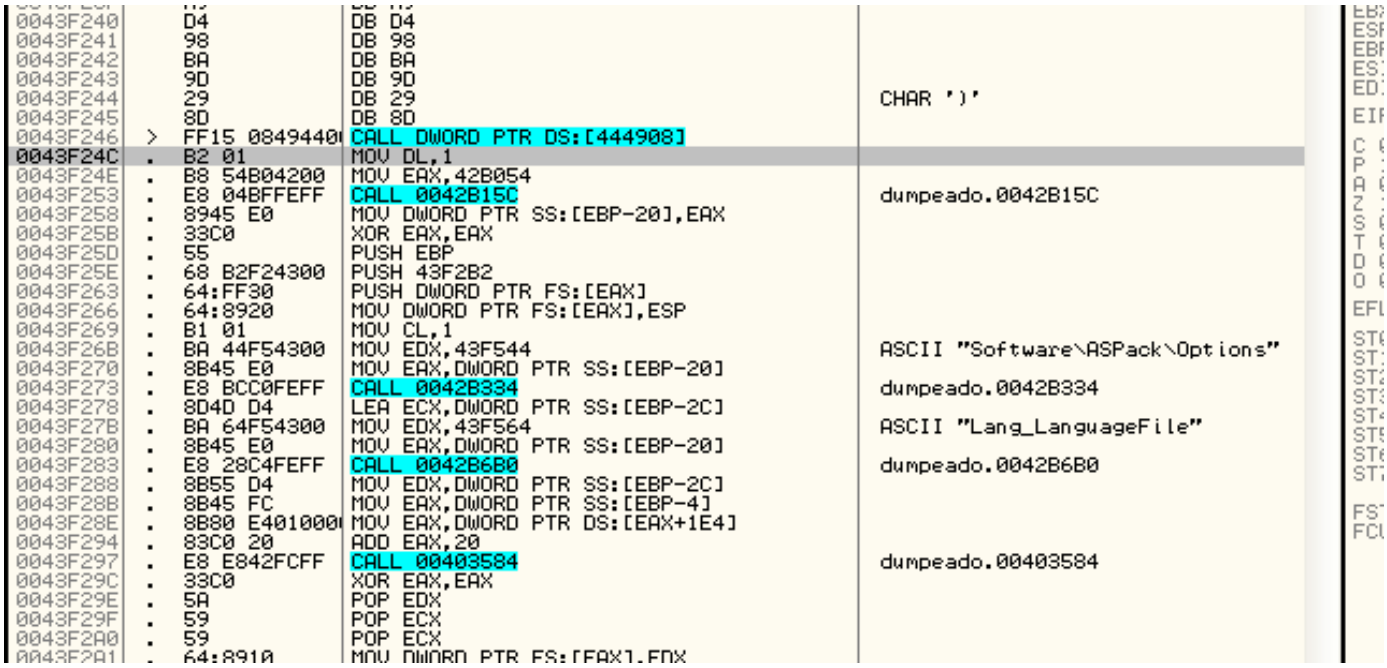


Volvamos a guardar los cambios realizados y volvamos a reiniciar el Olly que tiene el dumpeado y volvamos a ejecutarlo a ver que pasa ahora y…

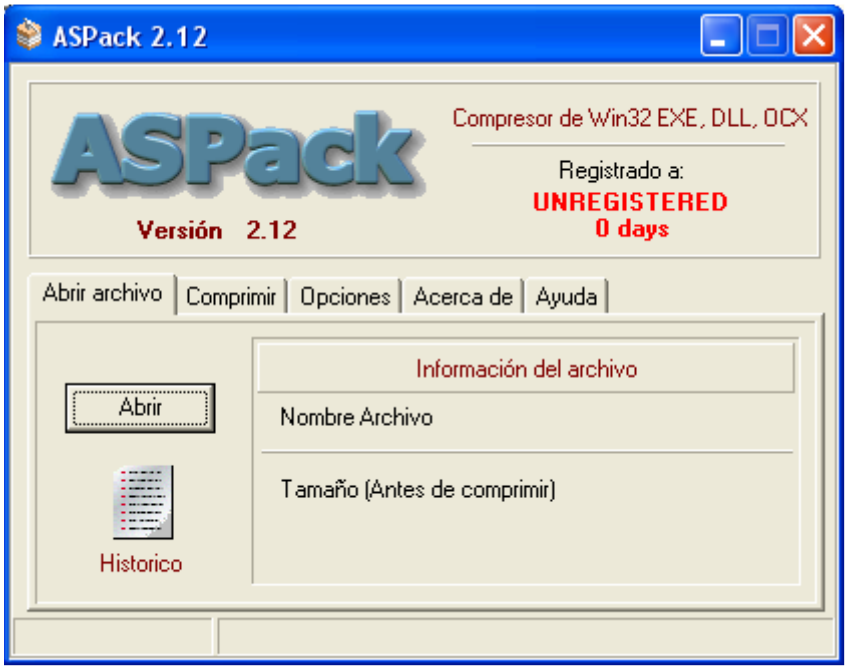
Otra vez igual, y esto empieza a desesperar. Ahora en el Stack tengo esto:

0012FE00 0043F24C RETURN to dumpeado.0043F24C from 009EC8F4

Axial que, como en las otras ocasiones, me planto encima de esa entrada y le doy a Intro y llego a:



Vuelvo a ir al Olly que tiene el original y voy a la dirección donde esta esa CALL que vemos encima de donde retornamos y vemos que otra vez es lo mismo, un CALL que nos manda a un lugar de la memoria creado en ejecución y que lo único que ejecuta allí es un RETN. Pero claro, en el dumpeado tampoco existe ese lugar y, por tanto, no existe ese RETN pero como ya dije, un CALL con un RETN detrás no sirve absolutamente para nada así que nopeamos esa CALL en el dumpeado y volvemos a guardar de nuevo los cambios.
Volvemos a reiniciar el Olly con el dumpeado y volvemos a ejecutarlo y…



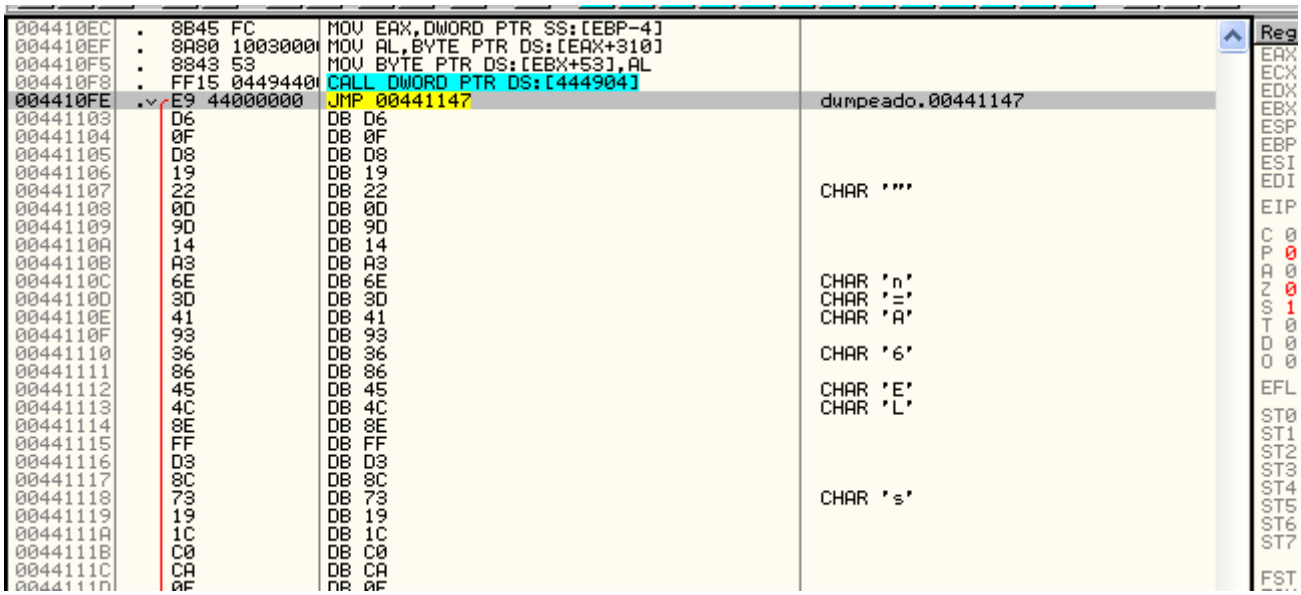
Por fin, jeje. Pero eso de los 0 días es porque modifique la fecha haciendo pruebas pero te saldrá la cantidad de días que te quedan. Eso si, para que mi método funcione y no caduque, tienes que descomprimirlo antes de que caduque ya que la comprobación se encuentra en la primera CALL que modificamos y, no se como, pero, cuando caduca, en el original esa CALL coge otro valor que esta justo debajo del destino que tiene ahora y si vais veréis algo muy curioso allí jeje.

Bueno, yo suponía que se había acabado el trabajo pero me dio por probar a comprimir algún exe y cuando acepto la ventanita que me dice que va a comprimir el archivo y le digo que si, vuelve a saltar otro error como los anteriores así que veamos a ver donde esta el fallo.

Esta vez en el Stack tenemos esto:

0012F8DC 004410FE RETURN to dumpeado.004410FE from 009EC8F4

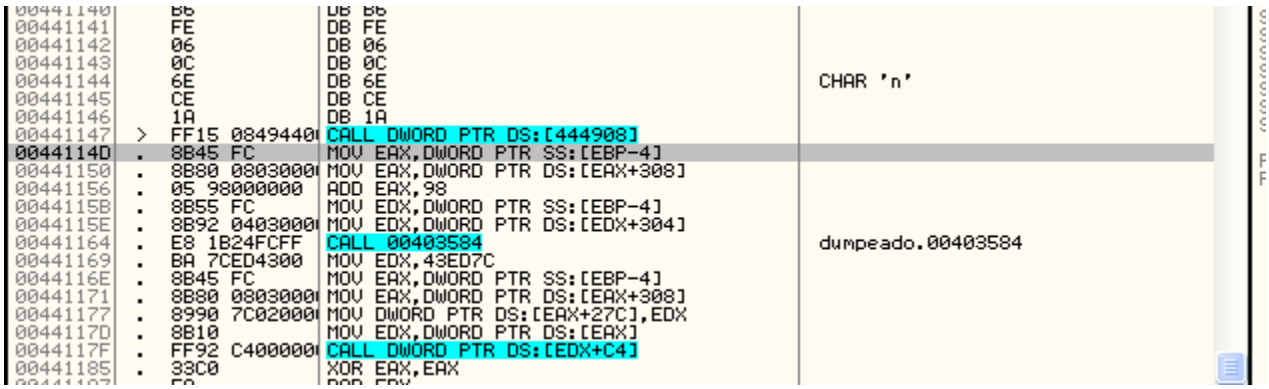
Usando el mismo método que en todas las otras fallas, llego a:



Me vuelvo a ir a la dirección de este CALL en el original y una vez encima pulso Intro y otra vez la misma historia, otro RETN así que a nopear ese CALL en el dumpeado y a guardar los cambios.
Otra vez vuelvo a intentarlo y esta vez al volver a aceptar la ventanita que sale para comprimir me vuelve a dar otro error y esta vez en el Stack tenemos:

0012F8DC 0044114D RETURN to dumpeado.0044114D from 009EC8F4

Y en la dirección de retorno:

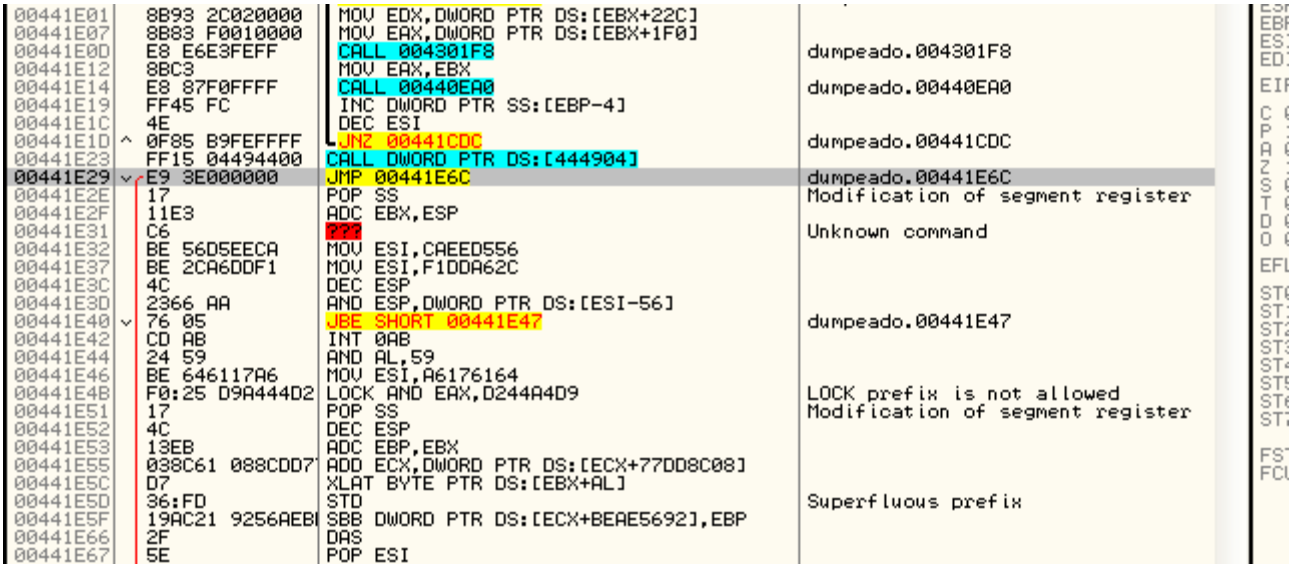


Pues hago ooootra vez lo mismo y ooootra vez igual, otro RETN así que a nopear la CALL y a volver a guardar los cambios.

Vuelvo a reiniciar Olly un poco cansado ya de esto y vuelvo a intentarlo y esta vez casi termina pero al final de la compresión salta otro error y siguiendo otra vez el método pues tengo en el Stack:

0012F92C 00441E29 RETURN to dumpeado.00441E29 from 009EC8F4

Y en el retorno:



Bueno, pues miremos esa CALL en el original a ver que es.
Y otra vez la misma historia así que a nopear también esa CALL en el dumpeado y a guardar los cambios.
Lo volvemos a intentar y otra vez mas el mismo error así que miremos otra vez a ver si esto se acaba ya.

En el Stack tenemos:

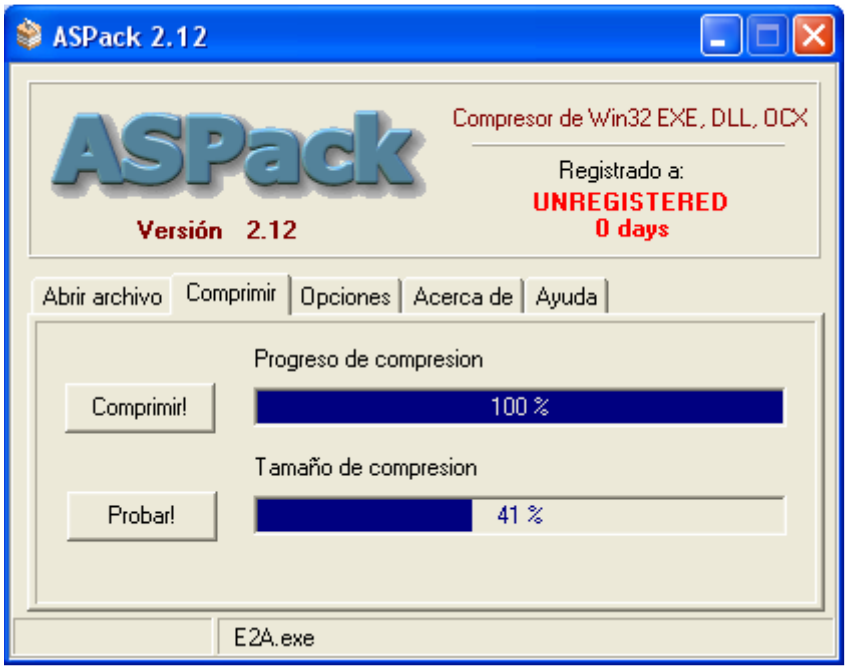
0012F92C 00441E72 RETURN to dumpeado.00441E72 from 009EC8F4

Y en el retorno:

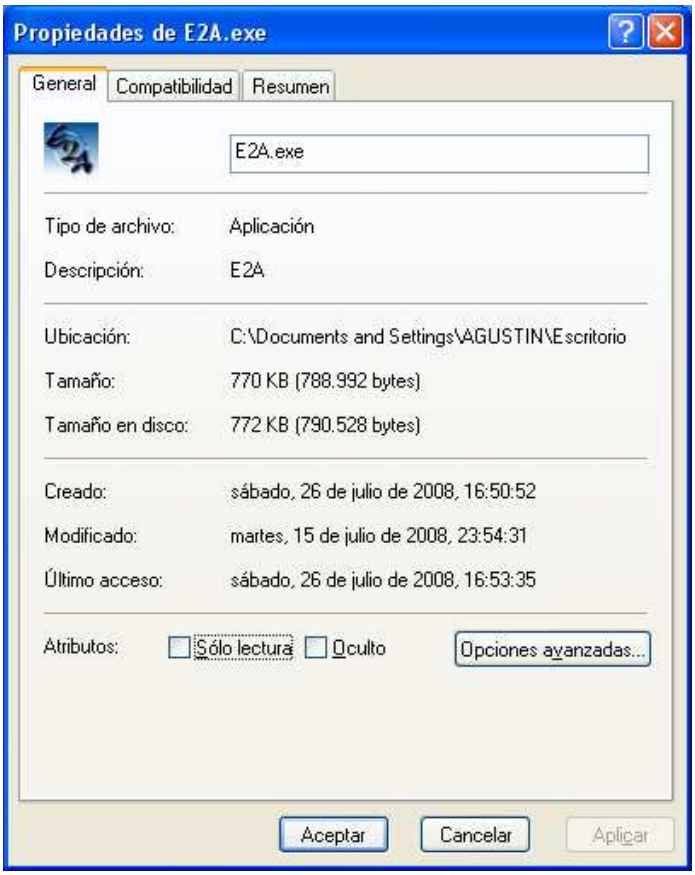
```
00441E65    BE          DB BE
00441E66    2F          DB 2F                    CHAR '/'
00441E67    5E          DB 5E                    CHAR '^'
00441E68    95          DB 95
00441E69    0D          DB 0D
00441E6A    66          DB 66                    CHAR 'f'
00441E6B    11          DB 11
00441E6C  > FF15 0849440( CALL DWORD PTR DS:[444908]
00441E72  > 33C0        XOR EAX,EAX
00441E74  . 5A          POP EDX
00441E75  . 59          POP ECX
00441E76  . 59          POP ECX
00441E77  . 64:8910     MOV DWORD PTR FS:[EAX],EDX
00441E7A  . 68 941E4400 PUSH 441E94
00441E7F  > 8D45 F4     LEA EAX,DWORD PTR SS:[EBP-C]
00441E82  . BA 02000000 MOV EDX,2
00441E87  . E8 C816FCFF CALL 00403554            dumpeado.00403554
00441E8C  . C3          RETN
00441E8D  .^ E9 8212FCFF JMP 00403114            dumpeado.00403114
00441E92  .^ EB EB      JMP SHORT 00441E7F       dumpeado.00441E7F
00441E94  . 5F          POP EDI
00441E95  . 5E          POP ESI
00441E96  . 5B          POP EBX
00441E97  . 8BE5        MOV ESP,EBP
00441E99  . 5D          POP EBP
00441E9A  . C3          RETN
00441E9B    00          DB 00
00441E9C  . FFFFFFFF    DD FFFFFFFF
Jump from 00441CB5
```

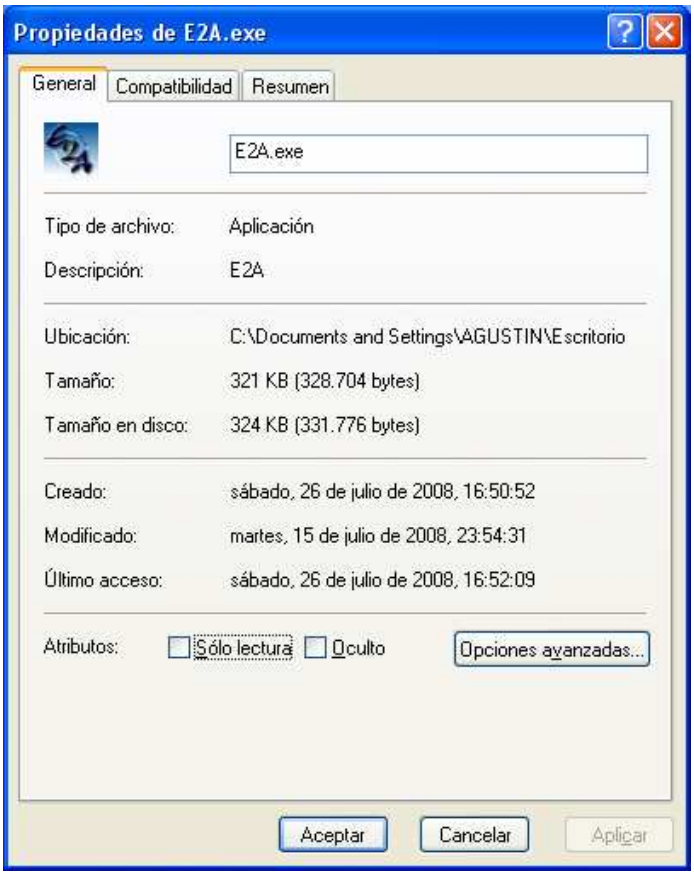
Y al mirar esa CALL en el original veo que es más de lo mismo así que a nopearla y a guardar el dumpeado.

Y vuelvo a intentarlo y…



Y a continuación veréis que si lo comprimió y funciona perfectamente.





Bueno, el objetivo de este tuto esta cumplido pero queda muy feo eso de UNREGISTERED así que lo cambiaremos usando un editor hexadecimal buscando las palabras esas ya que no aparecen en el Olly y con el editor hexa funciona.

Lo abrimos con cualquier editor hexa y buscamos y a mí con el Pspad me aparece así:

```
72 0709 6276 4C6F 7765 7265 6408  uter..bvLowered.
4F 7264 6572 0200 0006 5450 616E  TabOrder....TPan
50 616E 656C 3204 4C65 6674 0201  el.Panel2.Left..
70 0201 0557 6964 7468 039C 0106  .Top...Width.œ..
67 6874 0328 0105 416C 6967 6E07  Height.(..Align.
54 6F70 0854 6162 4F72 6465 7202  .alTop.TabOrder.
54 4265 7665 6C06 4265 7665 6C31  ...TBevel.Bevel1
66 7402 0803 546F 7002 0805 5769  .Left...Top...Wi
03 8C01 0648 6569 6768 7402 5905  dth.Œ..Height.Y.
70 6507 0762 7346 7261 6D65 0553  Shape..bsFrame.S
65 0708 6273 5261 6973 6564 0000  tyle..bsRaised..
61 6265 6C0A 4C61 6265 6C54 7269  .TLabel.LabelTri
4C 6566 7403 E000 0354 6F70 023E  al.Left.à..Top.>
64 7468 03AC 0006 4865 6967 6874  .Width.¬..Height
41 6C69 676E 6D65 6E74 0708 7461  . .Alignment..ta
74 6572 0841 7574 6F53 697A 6508  Center.AutoSize.
70 7469 6F6E 060C 554E 5245 4749  .Caption..UNREGI
52 4544 0A46 6F6E 742E 436F 6C6F  STERED.Font.Colo
63 6C52 6564 0B46 6F6E 742E 4865  r..clRed.Font.He
74 02F5 0946 6F6E 742E 4E61 6D65  ight.õ.Font.Name
53 2053 616E 7320 5365 7269 660A  ..MS Sans Serif.
74 2E53 7479 6C65 0B06 6673 426F  Font.Style..fsBo
0A 5061 7265 6E74 466F 6E74 0808  ld..ParentFont..
```

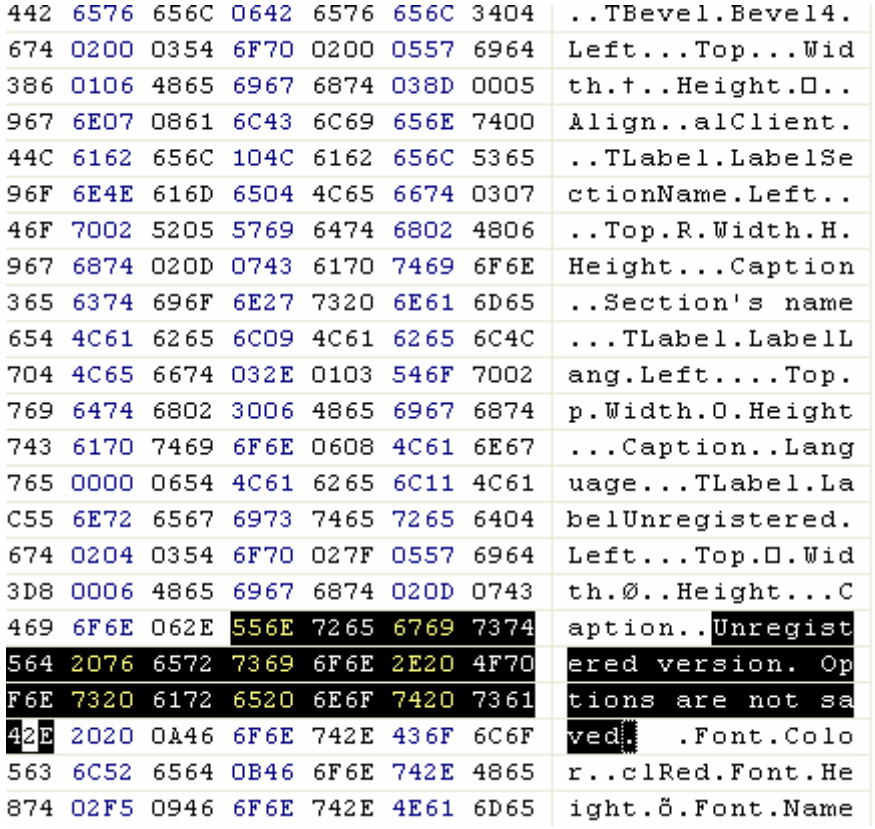
Y lo cambio por:

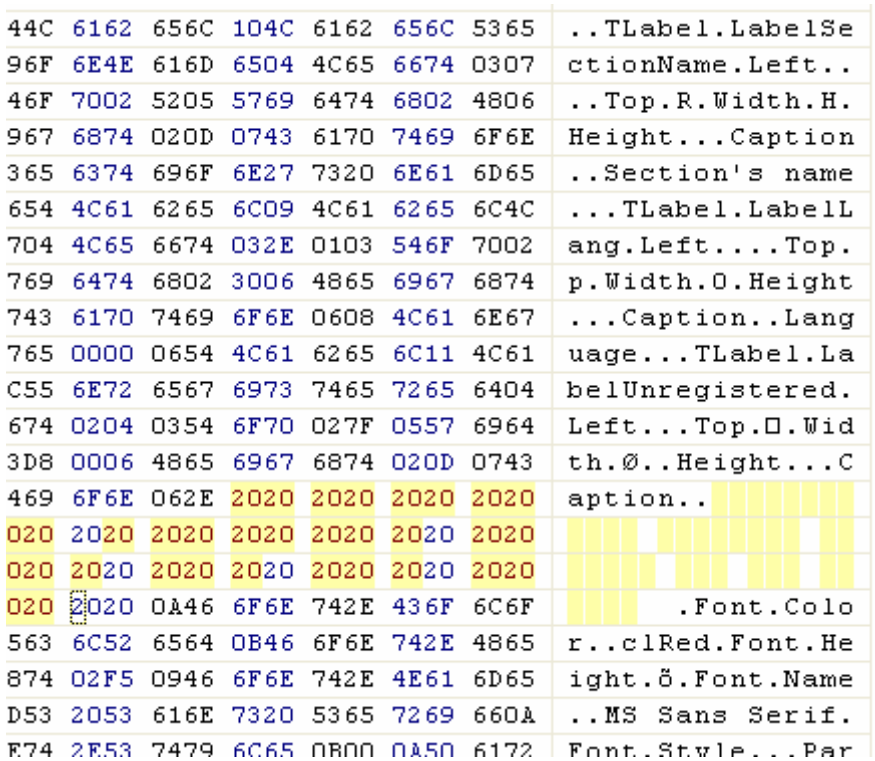
```
72 0709 6276 4C6F 7765 7265 6408  uter..bvLowered.
4F 7264 6572 0200 0006 5450 616E  TabOrder....TPan
50 616E 656C 3204 4C65 6674 0201  el.Panel2.Left..
70 0201 0557 6964 7468 039C 0106  .Top...Width.œ..
67 6874 0328 0105 416C 6967 6E07  Height.(..Align.
54 6F70 0854 6162 4F72 6465 7202  .alTop.TabOrder.
54 4265 7665 6C06 4265 7665 6C31  ...TBevel.Bevel1
66 7402 0803 546F 7002 0805 5769  .Left...Top...Wi
03 8C01 0648 6569 6768 7402 5905  dth.Œ..Height.Y.
70 6507 0762 7346 7261 6D65 0553  Shape..bsFrame.S
65 0708 6273 5261 6973 6564 0000  tyle..bsRaised..
61 6265 6C0A 4C61 6265 6C54 7269  .TLabel.LabelTri
4C 6566 7403 E000 0354 6F70 023E  al.Left.à..Top.>
64 7468 03AC 0006 4865 6967 6874  .Width.¬..Height
41 6C69 676E 6D65 6E74 0708 7461  . .Alignment..ta
74 6572 0841 7574 6F53 697A 6508  Center.AutoSize.
70 7469 6F6E 060C 2020 2020 4147  .Caption..    AG
20 2020 0A46 6F6E 742E 436F 6C6F  UML  .Font.Colo
63 6C52 6564 0B46 6F6E 742E 4865  r..clRed.Font.He
74 02F5 0946 6F6E 742E 4E61 6D65  ight.õ.Font.Name
53 2053 616E 7320 5365 7269 660A  ..MS Sans Serif.
74 2E53 7479 6C65 0B06 6673 426F  Font.Style..fsBo
```

Y guardo los cambios y voy a ver:

Fue bien pero hay mas cosillas que quitar de en medio como el rotulo que sale abajo cuando vas a la pestaña opciones.

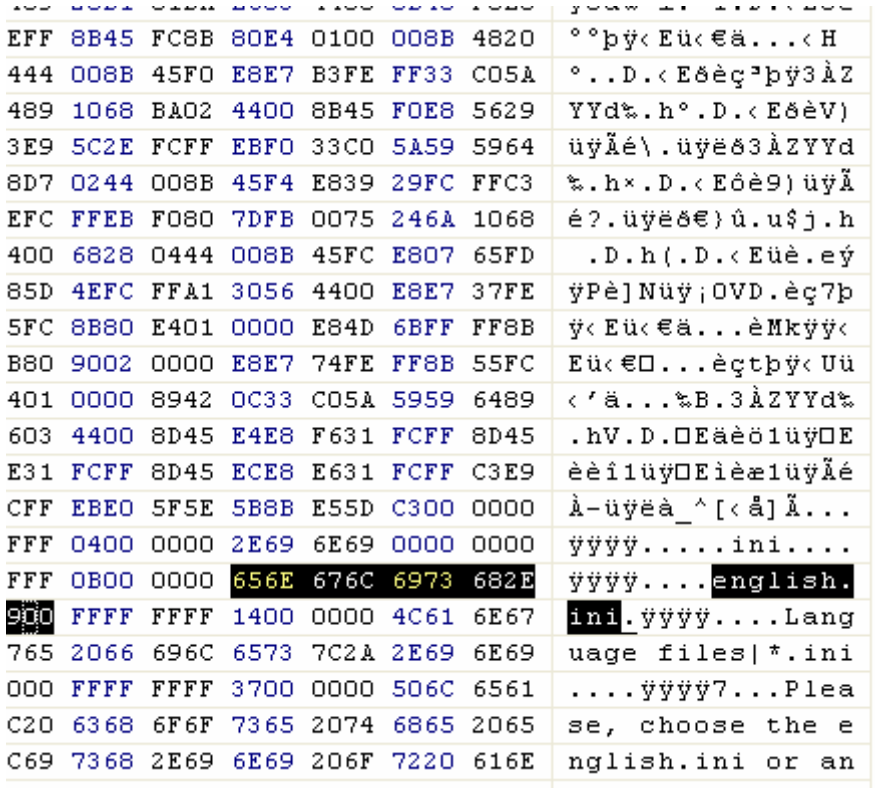
Volvemos a abrirlo en el editor hexa y buscamos y llenamos esa frase con espacios y el resultado es:



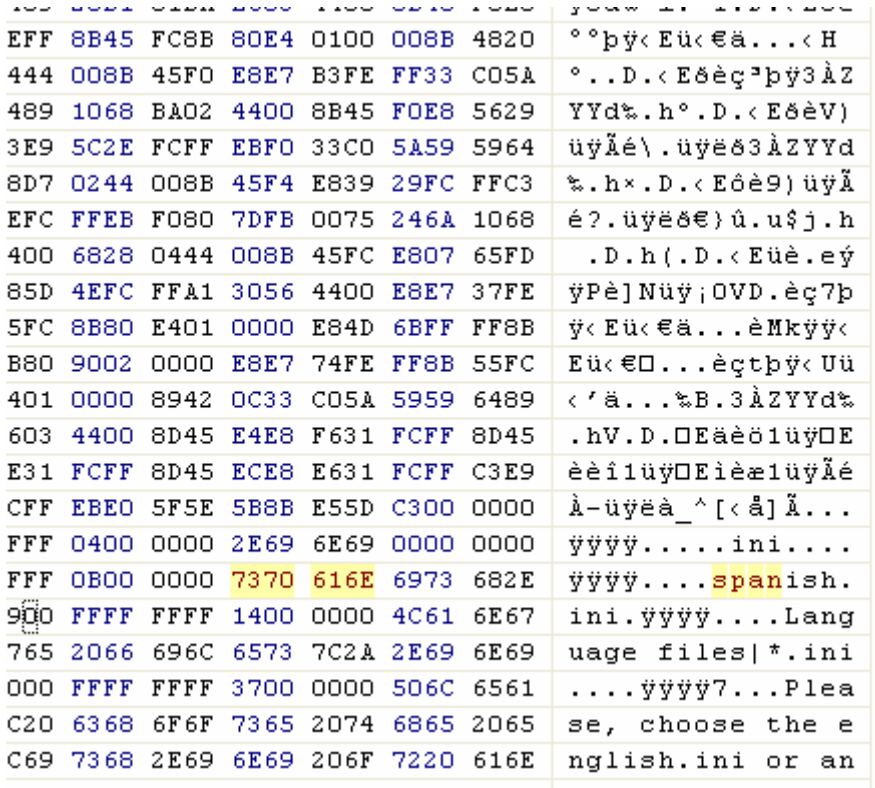


Otra cosilla que le voy a hacer es poner por defecto el lenguaje español ya que este exe no guarda la configuración, pues por lo menos que salga de entrada en español y lo

voy a hacer con el editor hexa también. Simplemente busco "english.ini" que es el que esta por defecto y solo aparece una entrada así que nos lo pone fácil.



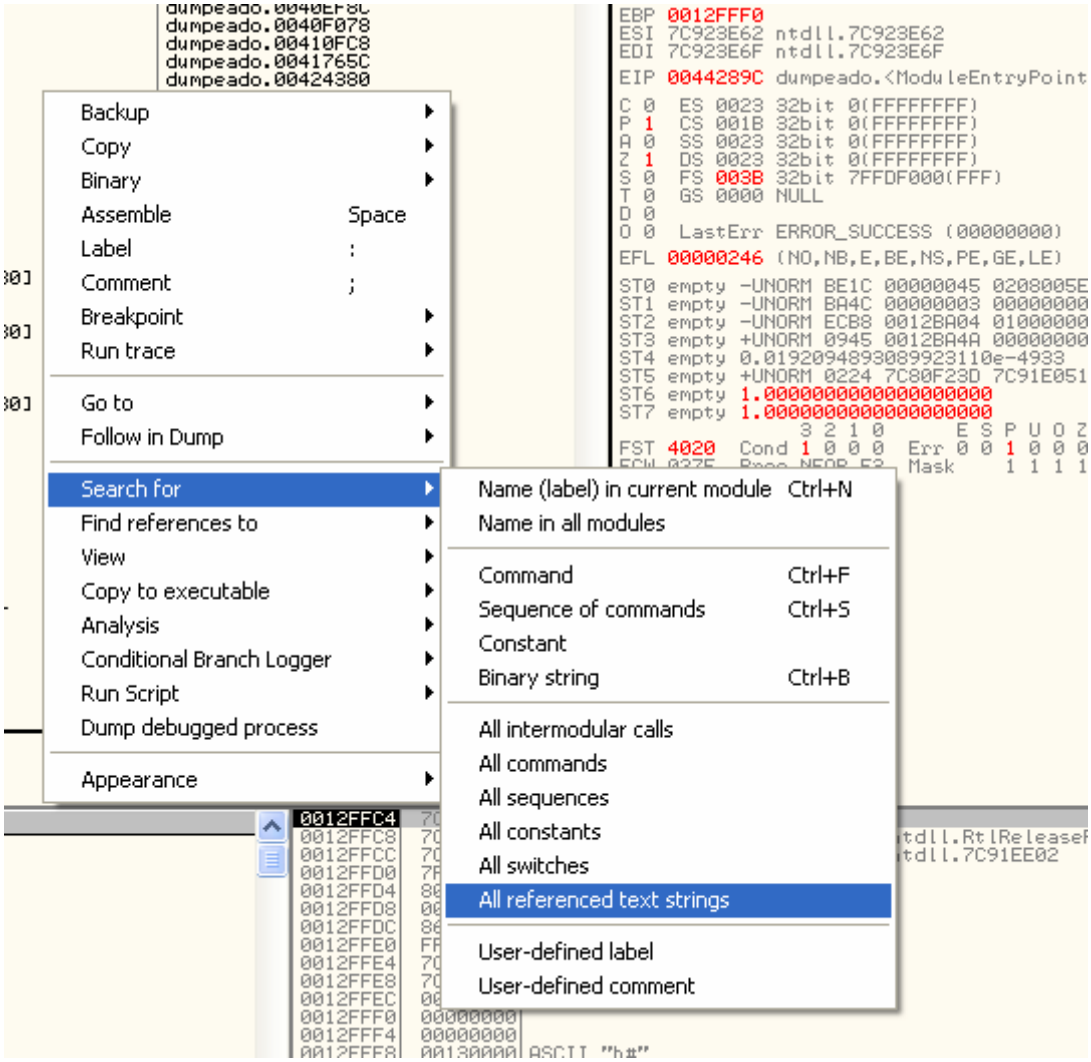
EFF	8B45	FC8B	80E4	0100	008B	4820	°°þÿ‹Eü‹€ä...‹H
444	008B	45F0	E8E7	B3FE	FF33	C05A	°..D.‹Eðèç³þÿ3ÀZ
489	1068	BA02	4400	8B45	F0E8	5629	YYd%.h°.D.‹EðèV)
3E9	5C2E	FCFF	EBF0	33C0	5A59	5964	üÿÃé\.üÿëð3ÀZYYd
8D7	0244	008B	45F4	E839	29FC	FFC3	%.h×.D.‹Eôè9)üÿÃ
EFC	FFEB	F080	7DFB	0075	246A	1068	é?.üÿëð€)û.u$j.h
400	6828	0444	008B	45FC	E807	65FD	.D.h(.D.‹Eüè.eý
85D	4EFC	FFA1	3056	4400	E8E7	37FE	ÿPè]Nüÿ¡0VD.èç7þ
5FC	8B80	E401	0000	E84D	6BFF	FF8B	ÿ‹Eü‹€ä...èMkÿÿ‹
B80	9002	0000	E8E7	74FE	FF8B	55FC	Eü‹€□...èçtþÿ‹Uü
401	0000	8942	0C33	C05A	5959	6489	‹'ä...‰B.3ÀZYYd‰
603	4400	8D45	E4E8	F631	FCFF	8D45	.hV.D.□Eäèö1üÿ□E
E31	FCFF	8D45	ECE8	E631	FCFF	C3E9	èèî1üÿ□Eìèæ1üÿÃé
CFF	EBE0	5F5E	5B8B	E55D	C300	0000	À-üÿëà_^[‹å]Ã...
FFF	0400	0000	2E69	6E69	0000	0000	ÿÿÿÿ.....ini....
FFF	0B00	0000	656E	676C	6973	682E	ÿÿÿÿ....english.
900	FFFF	FFFF	1400	0000	4C61	6E67	ini.ÿÿÿÿ....Lang
765	2066	696C	6573	7C2A	2E69	6E69	uage files|*.ini
000	FFFF	FFFF	3700	0000	506C	6561	....ÿÿÿÿ7...Plea
C20	6368	6F6F	7365	2074	6865	2065	se, choose the e
C69	7368	2E69	6E69	206F	7220	616E	nglish.ini or an



EFF	8B45	FC8B	80E4	0100	008B	4820	°°þÿ‹Eü‹€ä...‹H
444	008B	45F0	E8E7	B3FE	FF33	C05A	°..D.‹Eðèç³þÿ3ÀZ
489	1068	BA02	4400	8B45	F0E8	5629	YYd%.h°.D.‹EðèV)
3E9	5C2E	FCFF	EBF0	33C0	5A59	5964	üÿÃé\.üÿëð3ÀZYYd
8D7	0244	008B	45F4	E839	29FC	FFC3	%.h×.D.‹Eôè9)üÿÃ
EFC	FFEB	F080	7DFB	0075	246A	1068	é?.üÿëð€)û.u$j.h
400	6828	0444	008B	45FC	E807	65FD	.D.h(.D.‹Eüè.eý
85D	4EFC	FFA1	3056	4400	E8E7	37FE	ÿPè]Nüÿ¡0VD.èç7þ
5FC	8B80	E401	0000	E84D	6BFF	FF8B	ÿ‹Eü‹€ä...èMkÿÿ‹
B80	9002	0000	E8E7	74FE	FF8B	55FC	Eü‹€□...èçtþÿ‹Uü
401	0000	8942	0C33	C05A	5959	6489	‹'ä...‰B.3ÀZYYd‰
603	4400	8D45	E4E8	F631	FCFF	8D45	.hV.D.□Eäèö1üÿ□E
E31	FCFF	8D45	ECE8	E631	FCFF	C3E9	èèî1üÿ□Eìèæ1üÿÃé
CFF	EBE0	5F5E	5B8B	E55D	C300	0000	À-üÿëà_^[‹å]Ã...
FFF	0400	0000	2E69	6E69	0000	0000	ÿÿÿÿ.....ini....
FFF	0B00	0000	7370	616E	6973	682E	ÿÿÿÿ....spanish.
900	FFFF	FFFF	1400	0000	4C61	6E67	ini.ÿÿÿÿ....Lang
765	2066	696C	6573	7C2A	2E69	6E69	uage files|*.ini
000	FFFF	FFFF	3700	0000	506C	6561	....ÿÿÿÿ7...Plea
C20	6368	6F6F	7365	2074	6865	2065	se, choose the e
C69	7368	2E69	6E69	206F	7220	616E	nglish.ini or an

Y como tenemos la suerte de que las dos palabras tienen el mismo largo pues mejor aun.
Ya hay una cosa menos. Ahora a por lo de days, pero eso lo haré en el Olly para que me sirva de ayuda para encontrar la cifra que aparece también ya que days si aparece en las strings.

Hacemos una búsqueda de las strings en el exe:



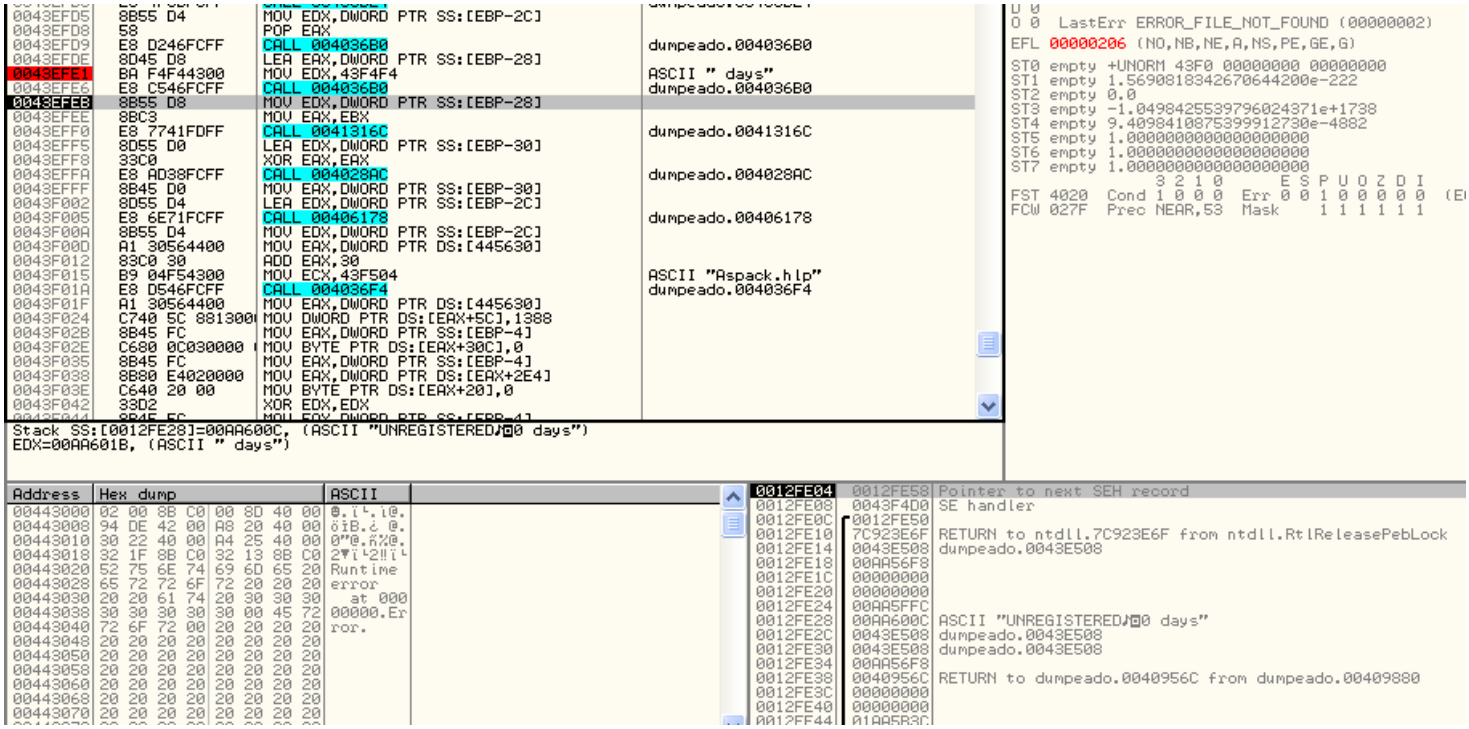
Y buscamos la string "days" y le ponemos un BP con F2:

```
0043B741 MOV EAX,43809C                          ASCII 04,"TLZB"
0043B786 MOV EAX,43CDB8                          ASCII "12"
0043B8CF MOV EAX,43CDC4                          ASCII "04"
0043B961 MOV EAX,43CDB8                          ASCII "12"
0043B99D MOV EAX,43CDD0                          ASCII "05"
0043BA62 MOV EDX,43CDDC                          ASCII ".reloc"
0043BA80 CMP DWORD PTR DS:[EAX+34],400000        ASCII "MZP"
0043C1FE MOV EAX,43CDEC                          ASCII "06"
0043CB69 MOV EDX,43CE00                          ASCII ".bak"
0043CFF0 MOV EAX,44390C                          UNICODE "REGVSTRYTYPELIB"
0043D23F MOV EDX,43D61C                          ASCII "kernel32.dll"
0043D291 MOV EDX,43D634                          ASCII " $"
0043DE2D MOV EAX,43DE80                          ASCII "HTTP://"
0043DEC8 PUSH 43E090                             ASCII "InternetReader"
0043DF01 PUSH 43E0A0                             ASCII "HTTP/1.0"
0043DF0F PUSH 43E0AC                             ASCII "GET"
0043E233 PUSH 43E250                             ASCII "\VarFileInfo\Translation"
0043E33B MOV EDX,43E3F4                          ASCII "\StringFileInfo\"
0043E41F MOV EDX,43E458                          ASCII "ProductVersion"
0043E4AE MOV EAX,43E4C8                          ASCII "%d.%d.%d.%d"
0043EE03 MOV EDX,43EED4                          ASCII "ASPack - "
0043EFBA MOV EDX,43F4E8                          ASCII "♪◘"
0043EFE1 MOV EDX,43F4F4                          ASCII " days"
0043F015 MOV ECX,43F504                          ASCII "Aspack.hlp"
0043F064 MOV EAX,43E0E4                          ASCII 0C,"TVersionInfo"
0043F0DE MOV EDX,43F518                          ASCII "SOFTWARE\ASPack"
0043F0EE MOV EDX,43F530                          ASCII "VersionNum"
0043F12F MOV EDX,43F530                          ASCII "VersionNum"
0043F26B MOV EDX,43F544                          ASCII "Software\ASPack\Options"
0043F27B MOV EDX,43F564                          ASCII "Lang_LanguageFile"
0043F2FB MOV EDX,43F580                          ASCII "*.ini"
0043F38E MOV EAX,43F590                          ASCII ".ini"
0043F534 IMUL EBP,DWORD PTR DS:[EDI+6E],6D754E   UNICODE "va"
0043F60A MOV EDX,43F6A0                          ASCII "08"
0043F61E MOV ECX,43F6A4                          ASCII "Error"
0043F6F0 MOV ECX,43F7C8                          ASCII "aspack.ini"
0043F722 MOV EDX,43F7DC                          ASCII "Item"
0043F747 MOV EDX,43F7EC                          ASCII "PopMenuHistory"
0043F818 MOV ECX,43F8F0                          ASCII "aspack.ini"
0043F866 MOV EDX,43F904                          ASCII "Item"
0043F88B MOV EDX,43F914                          ASCII "PopMenuHistory"
0043F967 MOV EDX,43FA60                          ASCII "10"
0043F981 MOV ECX,43FA64                          ASCII "Error"
0043F998 MOV ECX,43FA74                          ASCII ".bak"
0043FB49 MOV EDX,43FEAC                          ASCII "exefile\shell\"
0043FB80 MOV EDX,43FEC4                          ASCII "\Command"
0043FBD4 MOV EDX,43FED8                          ASCII " "%1""
0043FC16 MOV EDX,43FEF4                          ASCII "dllfile\shell\"
```

Damos a F9 y vemos que para aquí:

```
0043EFB0   8BC3            MOV EAX,EBX
0043EFB2   E8 8541FDFF     CALL 0041313C                    dumpeado.0041313C
0043EFB7   8D45 D8         LEA EAX,DWORD PTR SS:[EBP-28]
0043EFBA   BA E8F44300     MOV EDX,43F4E8                   ASCII "♪◘"
0043EFBF   E8 EC46FCFF     CALL 004036B0                    dumpeado.004036B0
0043EFC4   8D45 D8         LEA EAX,DWORD PTR SS:[EBP-28]
0043EFC7   50              PUSH EAX
0043EFC8   8D55 D4         LEA EDX,DWORD PTR SS:[EBP-2C]
0043EFCB   A1 00494400     MOV EAX,DWORD PTR DS:[444900]
0043EFD0   E8 4F6DFCFF     CALL 00405D24                    dumpeado.00405D24
0043EFD5   8B55 D4         MOV EDX,DWORD PTR SS:[EBP-2C]
0043EFD8   58              POP EAX
0043EFD9   E8 D246FCFF     CALL 004036B0                    dumpeado.004036B0
0043EFDE   8D45 D8         LEA EAX,DWORD PTR SS:[EBP-28]
0043EFE1   BA F4F44300     MOV EDX,43F4F4                   ASCII " days"
0043EFE6   E8 C546FCFF     CALL 004036B0                    dumpeado.004036B0
0043EFEB   8B55 D8         MOV EDX,DWORD PTR SS:[EBP-28]
0043EFEE   8BC3            MOV EAX,EBX
0043EFF0   E8 7741FDFF     CALL 0041316C                    dumpeado.0041316C
0043EFF5   8D55 D0         LEA EDX,DWORD PTR SS:[EBP-30]
0043EFF8   33C0            XOR EAX,EAX
0043EFFA   E8 AD38FCFF     CALL 004028AC                    dumpeado.004028AC
0043EFFF   8B45 D0         MOV EAX,DWORD PTR SS:[EBP-30]
0043F002   8D55 D4         LEA EDX,DWORD PTR SS:[EBP-2C]
0043F005   E8 6E71FCFF     CALL 00406178                    dumpeado.00406178
0043F00A   8B55 D4         MOV EDX,DWORD PTR SS:[EBP-2C]
0043F00D   A1 30564400     MOV EAX,DWORD PTR DS:[445630]
0043F012   83C0 30         ADD EAX,30
0043F015   B9 04F54300     MOV ECX,43F504                   ASCII "Aspack.hlp"
0043F01A   E8 D546FCFF     CALL 004036F4                    dumpeado.004036F4
0043F01F   A1 30564400     MOV EAX,DWORD PTR DS:[445630]
0043F024   C740 5C 881300( MOV DWORD PTR DS:[EAX+5C],1388
0043F02B   8B45 FC         MOV EAX,DWORD PTR SS:[EBP-4]
0043F02E   C680 0C030000 ( MOV BYTE PTR DS:[EAX+30C],0
0043F035   8B45 FC         MOV EAX,DWORD PTR SS:[EBP-4]
0043F038   8B80 E4020000   MOV EAX,DWORD PTR DS:[EAX+2E4]
0043F03E   C640 20 00      MOV BYTE PTR DS:[EAX+20],0
0043F042   33D2            XOR EDX,EDX
0043F044   8B45 FC         MOV EAX,DWORD PTR SS:[EBP-4]
0043F047   8B80 7C020000   MOV EAX,DWORD PTR DS:[EAX+27C]
0043F04D   E8 8240FDFF     CALL 004130D4                    dumpeado.004130D4
0043F052   8D55 D4         LEA EDX,DWORD PTR SS:[EBP-2C]
0043F055   A1 30564400     MOV EAX,DWORD PTR DS:[445630]
0043F05A   E8 D14CFFFF     CALL 00423D30                    dumpeado.00423D30
```

Vamos traceando a ver si aparecen los días que muestra y:



Bueno pues estuve haciendo pruebas y la forma que me funciono fue nopear los dos CALLs que están justo debajo del BP y con eso ya no salen los días.

```
0043EFC4  8D45 D8       LEA EAX,DWORD PTR SS:[EBP-28]
0043EFC7  50            PUSH EAX
0043EFC8  8D55 D4       LEA EDX,DWORD PTR SS:[EBP-2C]
0043EFCB  A1 00494400   MOV EAX,DWORD PTR DS:[444900]
0043EFD0  E8 4F6DFCFF   CALL 00405D24                    dumpeado.00405D24
0043EFD5  8B55 D4       MOV EDX,DWORD PTR SS:[EBP-2C]
0043EFD8  58            POP EAX
0043EFD9  E8 D246FCFF   CALL 004036B0                    dumpeado.004036B0
0043EFDE  8D45 D8       LEA EAX,DWORD PTR SS:[EBP-28]
0043EFE1  BA F4F44300   MOV EDX,43F4F4                   ASCII " days"
0043EFE6  90            NOP
0043EFE7  90            NOP
0043EFE8  90            NOP
0043EFE9  90            NOP
0043EFEA  90            NOP
0043EFEB  8B55 D8       MOV EDX,DWORD PTR SS:[EBP-28]
0043EFEE  8BC3          MOV EAX,EBX
0043EFF0  90            NOP
0043EFF1  90            NOP
0043EFF2  90            NOP
0043EFF3  90            NOP
0043EFF4  90            NOP
0043EFF5  8D55 D0       LEA EDX,DWORD PTR SS:[EBP-30]
0043EFF8  33C0          XOR EAX,EAX
0043EFFA  E8 AD38FCFF   CALL 004028AC                    dumpeado.004028AC
0043EFFF  8B45 D0       MOV EAX,DWORD PTR SS:[EBP-30]
0043F002  8D55 D4       LEA EDX,DWORD PTR SS:[EBP-2C]
0043F005  E8 6E71FCFF   CALL 00406178                    dumpeado.00406178
0043F00A  8B55 D4       MOV EDX,DWORD PTR SS:[EBP-2C]
0043F00D  A1 30564400   MOV EAX,DWORD PTR DS:[445630]
0043F012  83C0 30       ADD EAX,30
0043F015  B9 04F54300   MOV ECX,43F504                   ASCII "Aspack.hlp"
0043F01A  E8 D546FCFF   CALL 004036F4                    dumpeado.004036F4
0043F01F  A1 30564400   MOV EAX,DWORD PTR DS:[445630]
0043F024  C740 5C 881300 MOV DWORD PTR DS:[EAX+5C],1388
0043F02B  8B45 FC       MOV EAX,DWORD PTR SS:[EBP-4]
0043F02E  C680 0C030000 MOV BYTE PTR DS:[EAX+30C],0
0043F035  8B45 FC       MOV EAX,DWORD PTR SS:[EBP-4]
0043F038  8B80 E4020000 MOV EAX,DWORD PTR DS:[EAX+2E4]
0043F03E  C640 20 00    MOV BYTE PTR DS:[EAX+20],0
0043F042  33D2          XOR EDX,EDX
0043F044  8B45 FC       MOV EAX,DWORD PTR SS:[EBP-4]
0043F047  8B80 7C020000 MOV EAX,DWORD PTR DS:[EAX+27C]
0043F04D  E8 8240FDFF   CALL 004130D4                    dumpeado.004130D4
```

Bueno, yo le hice algún que otro cambio más jejeje

Si se pulsa en donde pone **** Crackeado por Aguml **** te lleva a google

Bueno, lo hice para que lo entienda gente tan torpe como yo que empiecen desde 0 ya que la gran mayoría de la comunidad sabe manejarse en esto y no necesitan tantas imágenes.
Pos eso, espero que disfrutéis los Newbies tanto como yo cuando lo destripe.