URL	http://www.InertiaSoftware.com
Victima	Jigsaw Mania
Herramientas	Olly
Cracker	ZiKaTRiZ
Dificultad	Facil
Fecha	4 – agosto - 2011

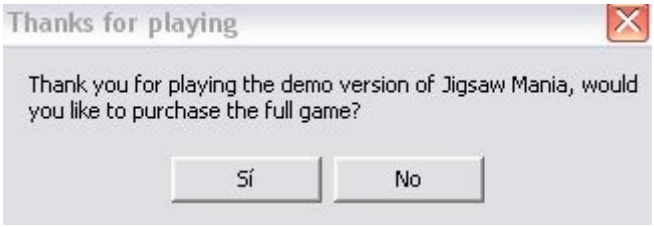
Hola, hoy nos encontramos con este paciente, que tiene la enfermedad del trial versión, una enfermedad muy habitual.

Al ejecutar el software, comprobamos los tres puntos importantes que debemos corregir :

1. 

2. Trial version expired 

3. Y el aviso final , que te da las gracias por jugar, pero que si no lo compras, caduca.



Carguemoslo en Olly
Primer punto:
Miramos en las String references y nos encontramos

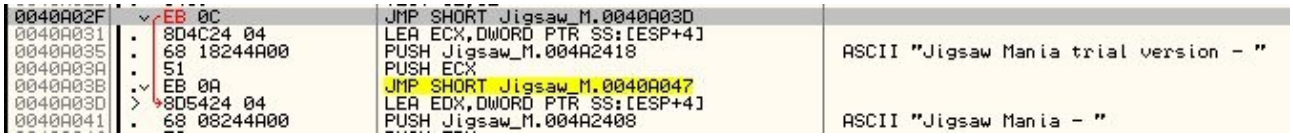
```
0040A035 PUSH Jigsaw_M.004A2418    ASCII "Jigsaw Mania trial version - "
0040A041 PUSH Jigsaw_M.004A2408    ASCII "Jigsaw Mania - "
```

pulsamos con el ratón en cualquiera de las dos referencias y nos manda a

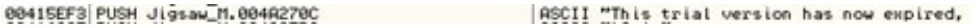
```
0040A02F  74 0C          JE SHORT Jigsaw_M.0040A03D
0040A031  8D4C24 04      LEA ECX,DWORD PTR SS:[ESP+4]
0040A035  68 18244A00    PUSH Jigsaw_M.004A2418     ASCII "Jigsaw Mania trial version - "
0040A03A  51             PUSH ECX
0040A03B  EB 0A          JMP SHORT Jigsaw_M.0040A047
0040A03D  8D5424 04      LEA EDX,DWORD PTR SS:[ESP+4]
0040A041  68 08244A00    PUSH Jigsaw_M.004A2408     ASCII "Jigsaw Mania - "
0040A046  52             PUSH EDX
```

```
00415EF3 PUSH Jigsaw_M.004A270C    ASCII "This trial version has now expired, thar
004160AF PUSH Jigsaw_M.004A27D0    ASCII "&Quit"
```

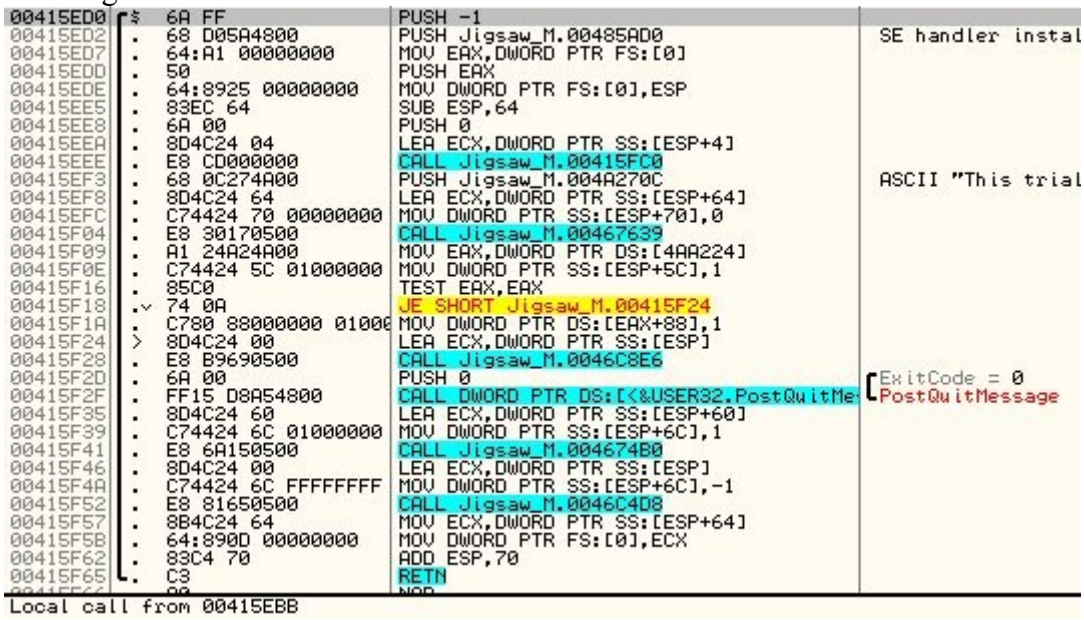
aquí nos encontramos con un salto condicional, bueno pues le diremos que cuando llegue a la dirección 0040A02F realice el salto sin pensar. Colocándonos en ese dirección pulsaremos las teclas CTRL+E o botón derecho del ratón Binary – Edit. Cambiaremos el 74 0C por EB 0C , como muestra la siguiente imagen.



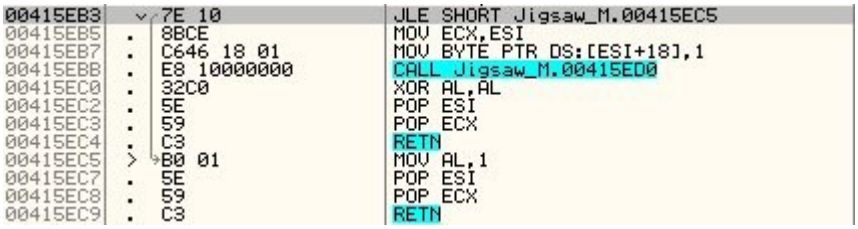
Segundo punto:



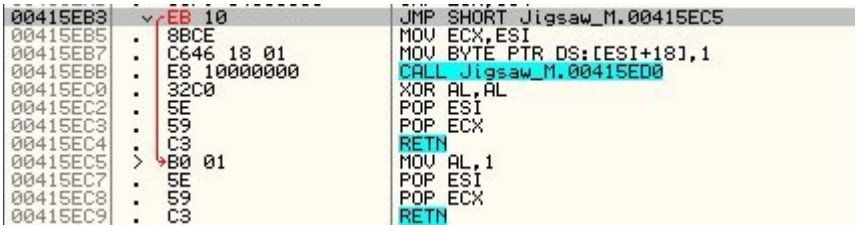
podemos ver que hace referencia a la llamada de una call con la dirección 00415EBB como muestra la siguiente imagen



colocándonos en el inicio de la rutina, botón derecho del ratón Goto Call from 00415EBB



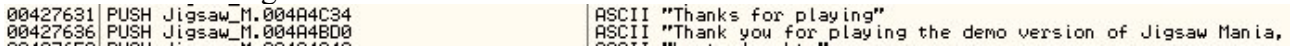
otro salto condicional, bueno pues le diremos que cuando llegue a la dirección 00415EB3 realice el salto sin pensar. Colocándonos en ese dirección pulsaremos las teclas CTRL+E o botón derecho del ratón Binary – Edit. Cambiaremos el 7E 10 por EB 10 , como muestra la siguiente imagen.



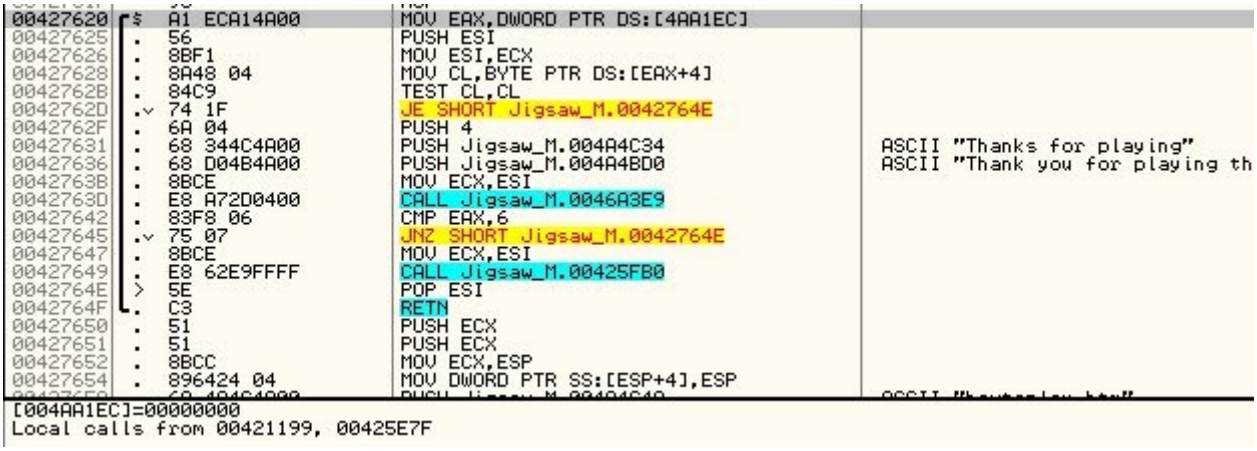
Con esto, no caduca y eliminamos el purchase automáticamente

Tercer punto:

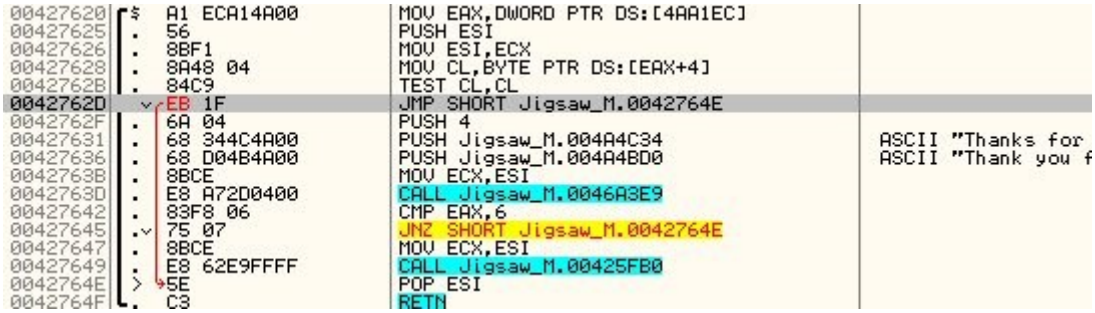
Mirando en las string references vemos



Vallamos a la dirección 00427631, como podemos comprobar el salto JE que tenemosjusto encima de las referencias, es el que decide si nos muestra el aviso de que estamos en una demo o no.



bueno pues le diremos que cuando llegue a la dirección 0042762D realice el salto sin pensar. Colocándonos en ese dirección pulsaremos las teclas CTRL+E o botón derecho del ratón Binary – Edit. Cambiaremos el 74 1F por EB 1F , y de esta manera cuando cerremos el programa lo cerrará sin necesidad de darnos las gracias por jugar en su versión demo



Listo.

ZiKaTRiZ