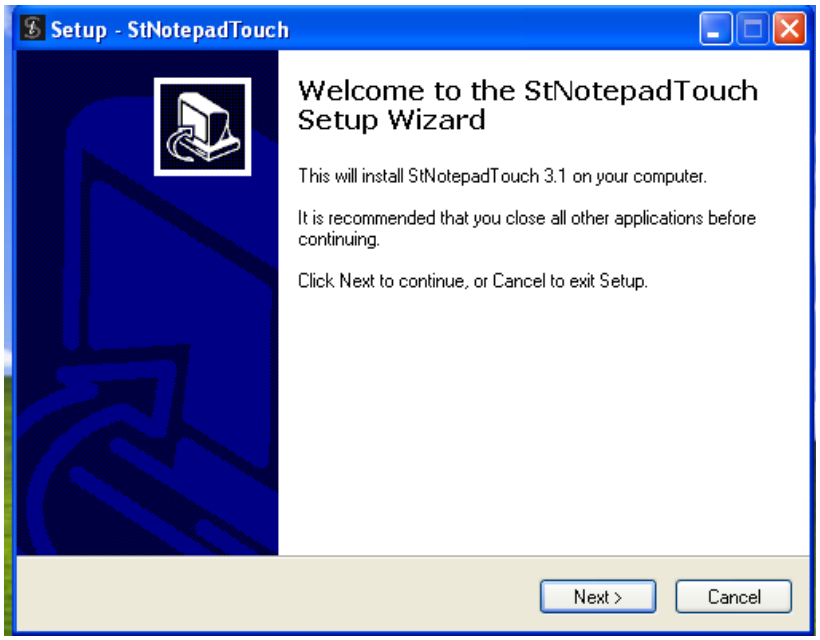
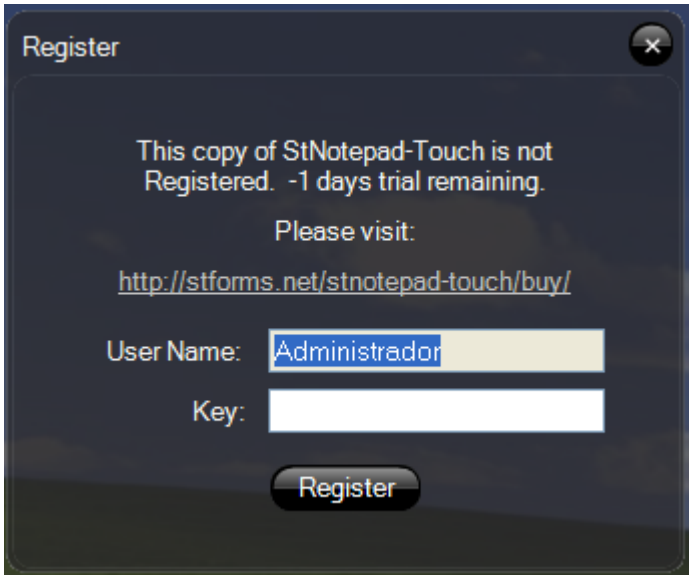
Hola.
El programa de hoy si se para que sirve..... :-)
se trata de StNotepadTouch que es un programa que encontré buscando un editor al cual le pudiera alterar su transparencia para poder leer y escribir sin necesidad de estarlo moviendo de un lado para otro.

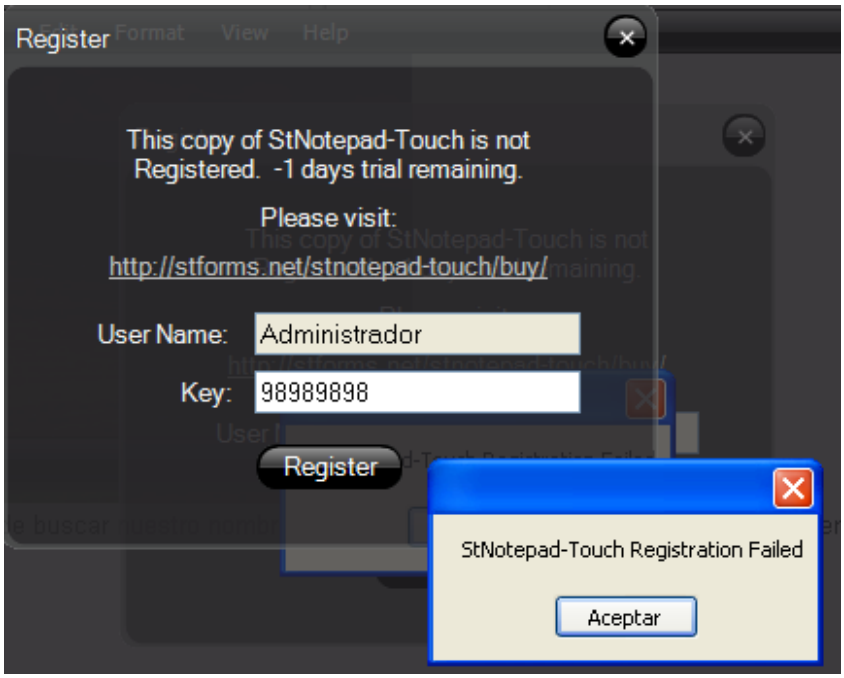


Después de su instalación, y arrancar el programa, tendremos nuestra interface recordándonos que no lo hemos pagado.

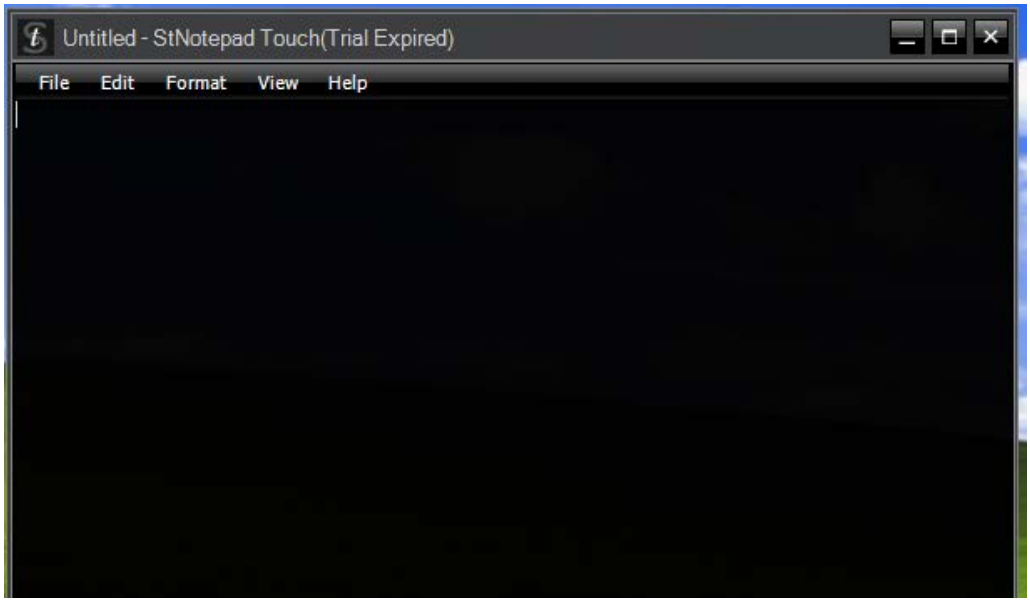
Y al buscar la opción de registrarlo, el mismo programa se encarga de buscar nuestro nombre en el equipo y colocarlo en la caja correspondiente.



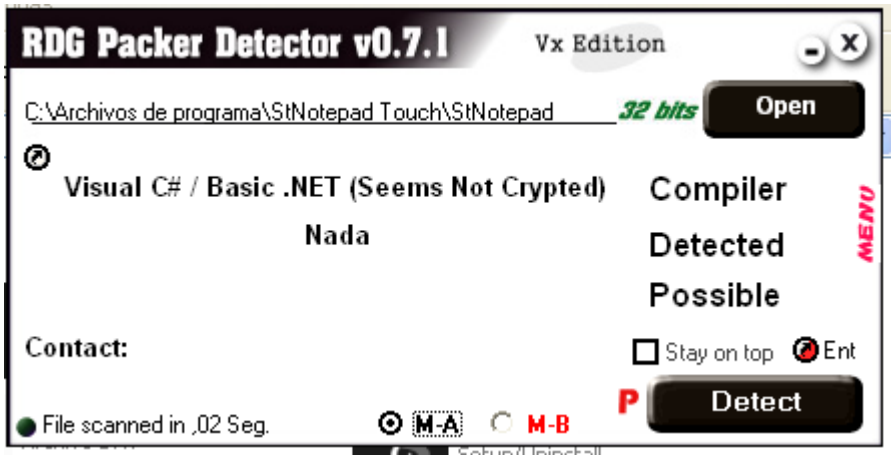
Al tratar de registrarlo:



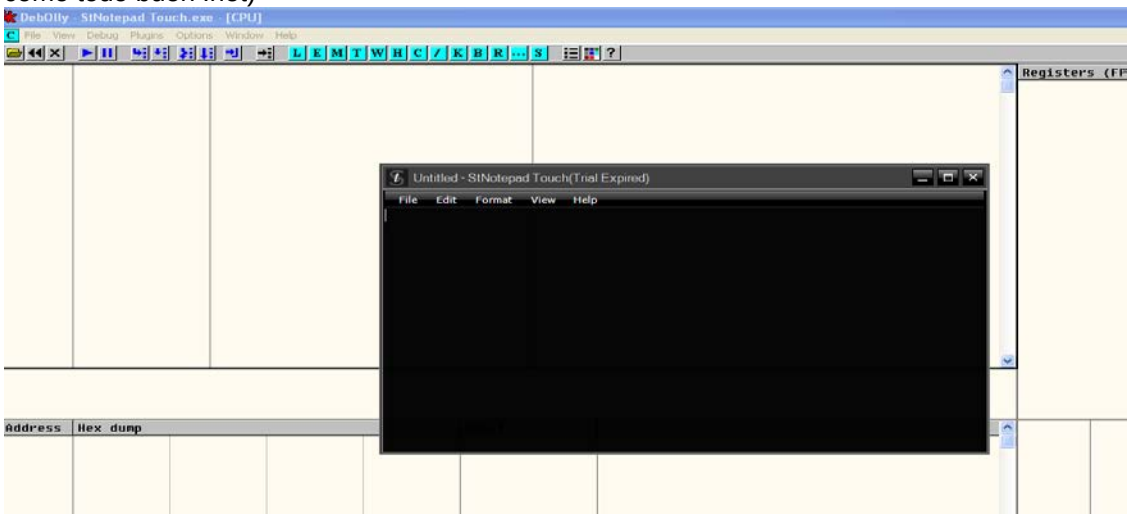
Y al adelantar la fecha para que se acabe el tiempo de prueba.



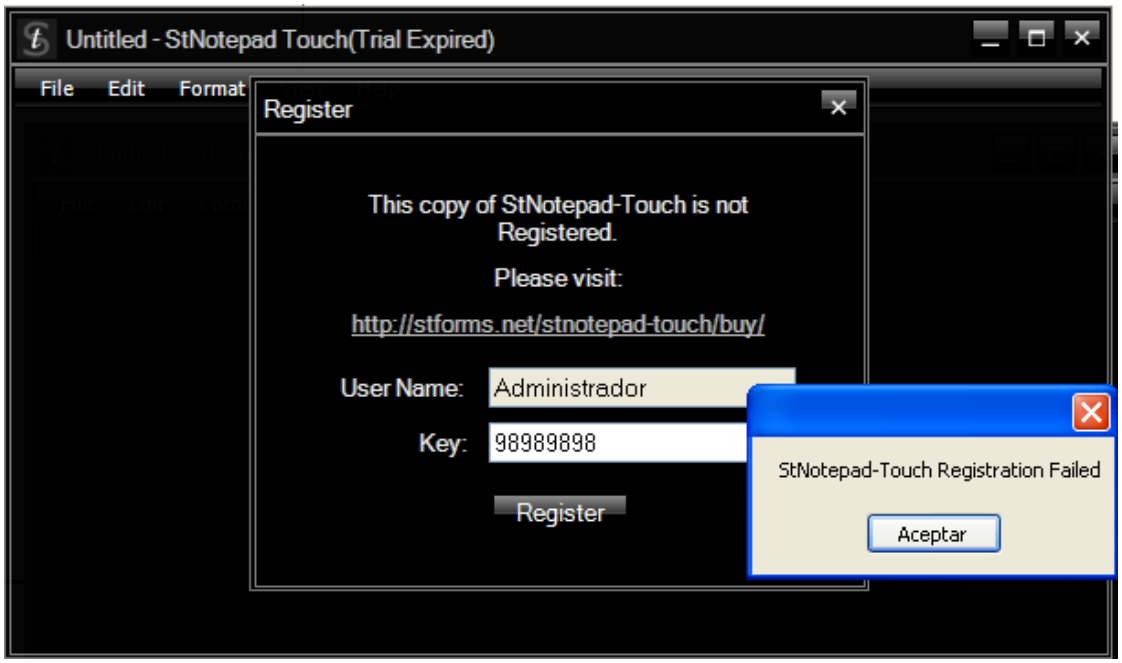
Ahora lo pasaremos por RDG.



Lo que haremos es abrirlo con olly y dejar que arranque normalmente. (Sin mostrar código ni nada como todo buen .net)

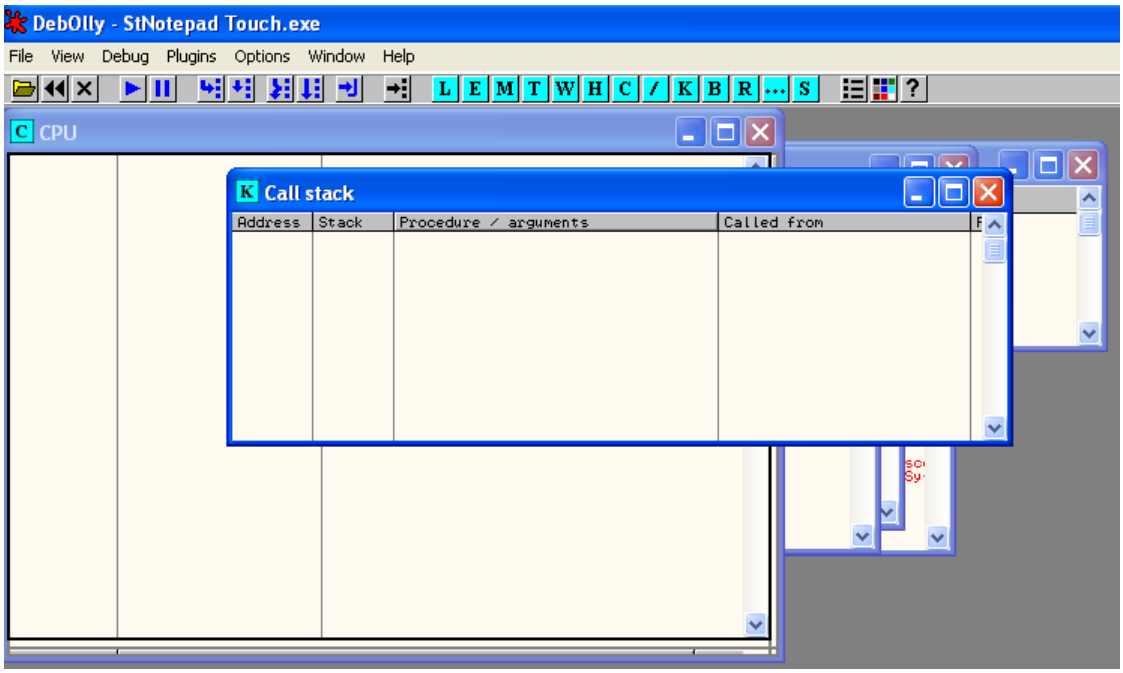


Nos iremos a la opción de registro e introduciremos los una clave pichi...
y daremos al boton de register.

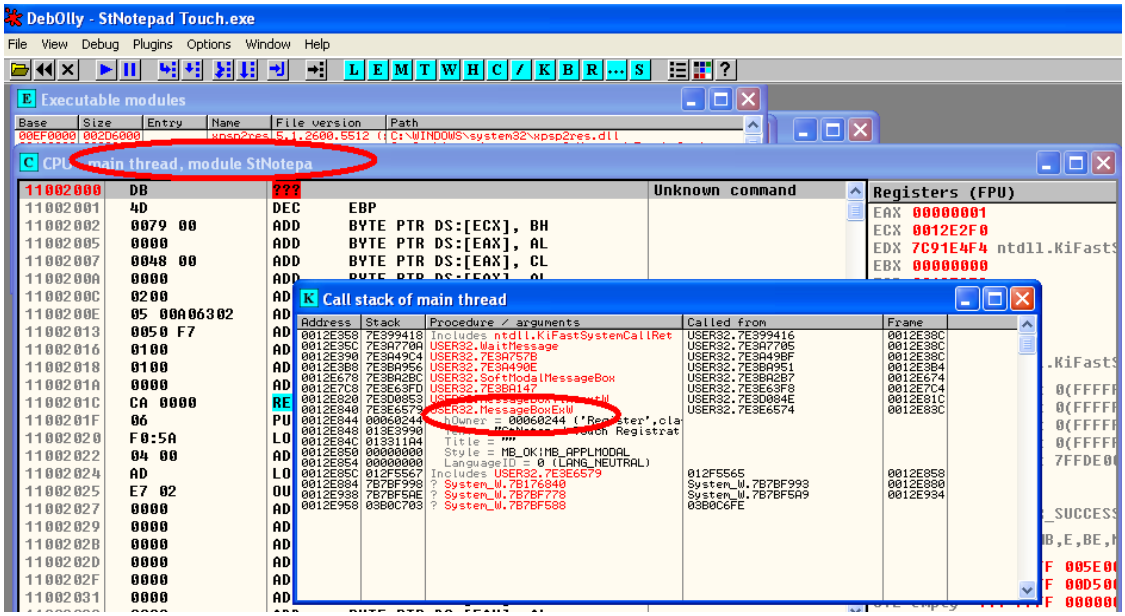


Ahora trataremos de saber qué tipo de mensaje es el que nos ha enviado el programa para poder colocar un bp.
Al colocar en pause el programa y oprimiremos "K" olly nos dirá que tipo de mensaje es.

Pero si lo hacemos en este momento en que no vemos el código del programa obtendremos esto:

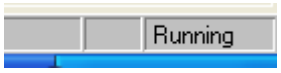


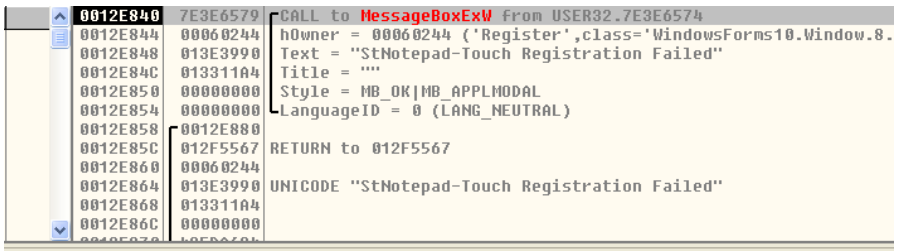
Si ahora nos vamos a "E" y seleccionamos el programa que estamos trabajando obtendremos esto:



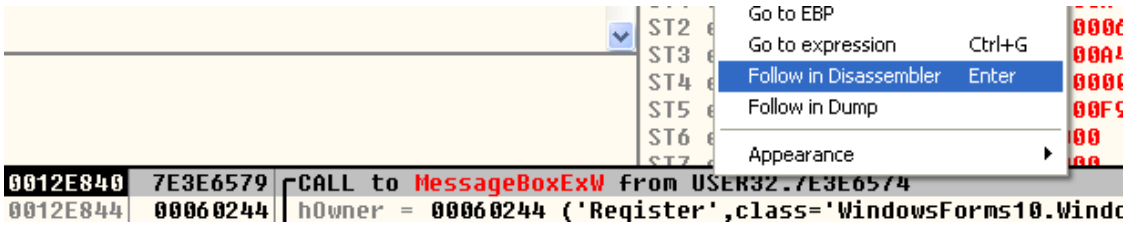
ya tenemos donde colocar nuestro bp.... :-)

Sola mente tenemos que reanudar el programa, oprimir el botón aceptar y colocar un "BP MessageBoxExW" y oprimir nuevamente register para que pique...





Tomaremos la dirección de retorno de user32 dándole click derecho y le prediremos que nos lo muestre en el desensamblado.

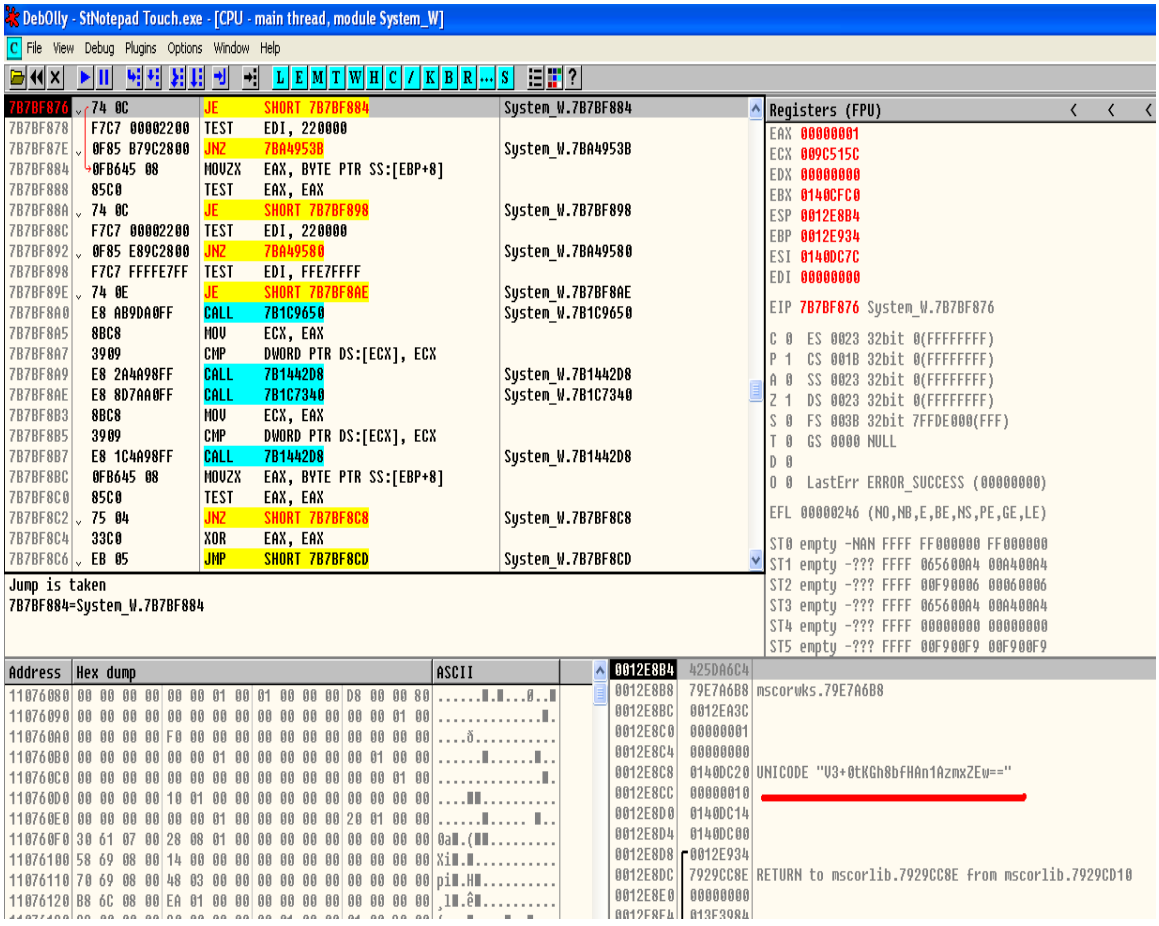


Donde colocaremos un bp con f2 para que pique cuando oprimamos el botón de aceptar,
le damos f9 para que arranque de nuevo , oprimimos el botón aceptar y caemos en el bp que acabamos de colocar.
y trocearemos hasta pasar 3 "RET" donde encontraremos USER32.GetActiveWindow (buscar

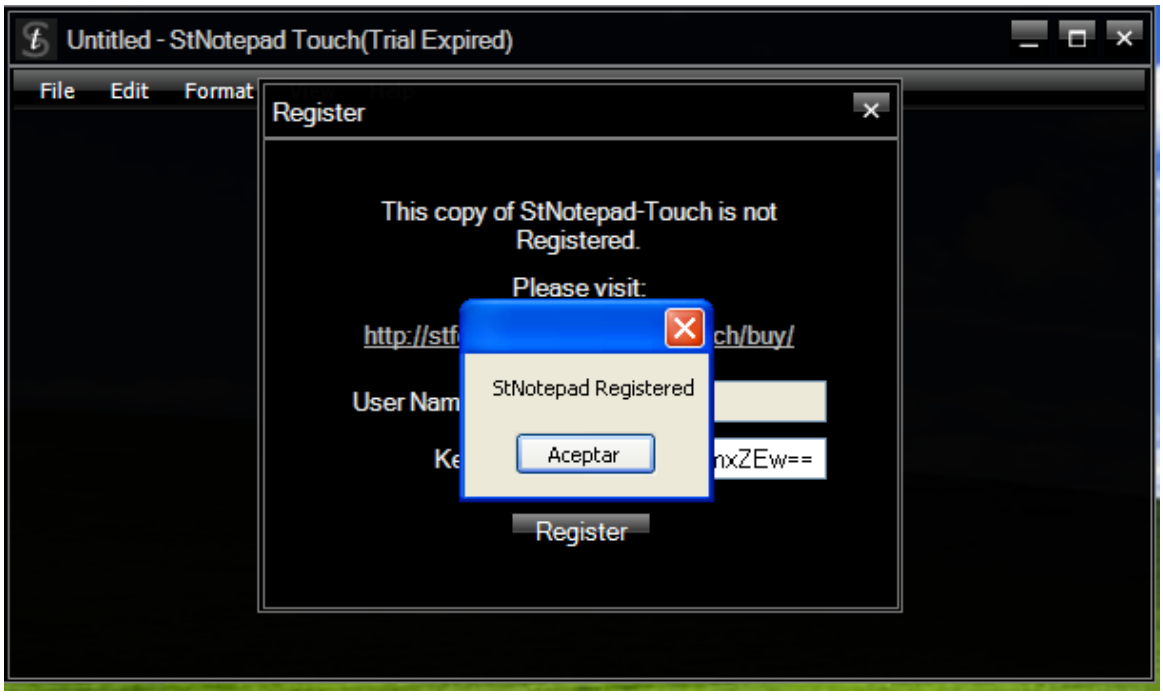
arriba en el código al pasar el tercer "RET")

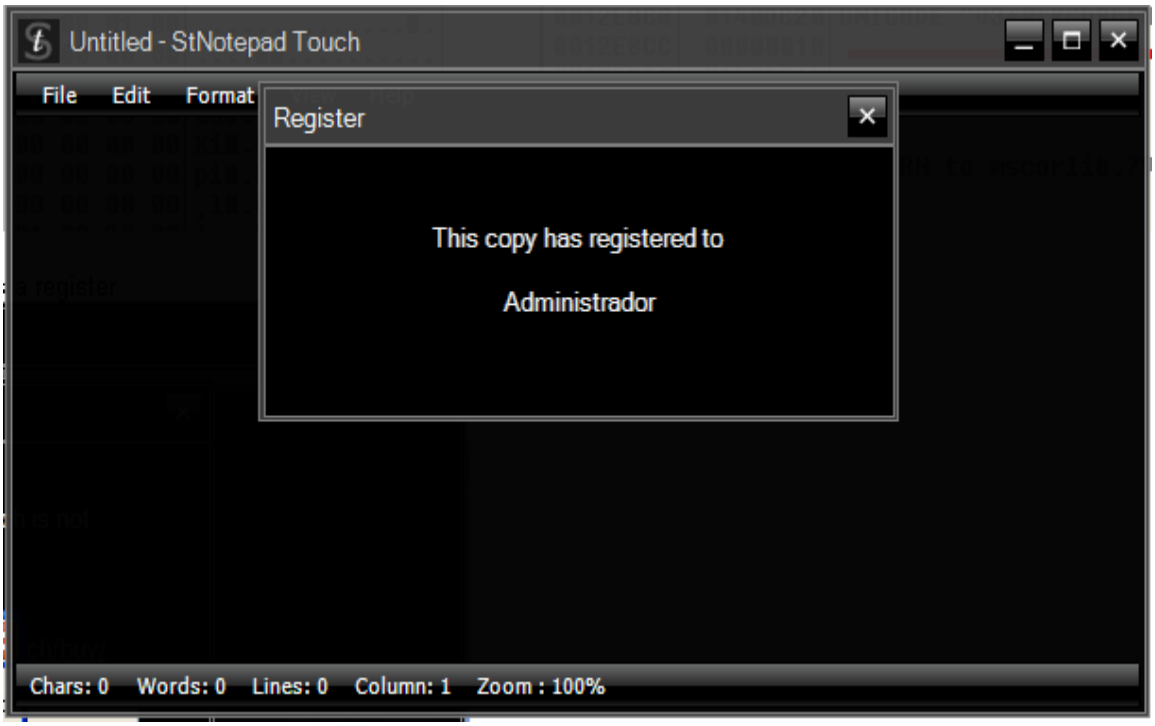
```
7B7BF8F4   85C0            TEST    EAX, EAX
7B7BF8F6   75 08           JNZ     SHORT 7B7BF900                  System_W.7B7BF900
7B7BF8F8   F7C7 00002200   TEST    EDI, 220000
7B7BF8FE   75 4E           JNZ     SHORT 7B7BF94E                  System_W.7B7BF94E
7B7BF900   837D AC 00       CMP     DWORD PTR SS:[EBP-54], 0
7B7BF904   75 3D           JNZ     SHORT 7B7BF943                  System_W.7B7BF943
7B7BF906   C745 8C E4A8087 MOV     DWORD PTR SS:[EBP-74], 7B08A8E4
7B7BF90D   8965 90         MOV     DWORD PTR SS:[EBP-70], ESP
7B7BF910   8B45 B8         MOV     EAX, DWORD PTR SS:[EBP-48]
7B7BF913   68 25F97B7B     PUSH    7B7BF925
7B7BF918   8F45 94         POP     DWORD PTR SS:[EBP-6C]
7B7BF91B   C640 08 00      MOV     BYTE PTR DS:[EAX+8], 0
7B7BF91F   FF15 10C00D7B   CALL    NEAR DWORD PTR DS:[7B0DC010]    USER32.GetActiveWindow
7B7BF925   8B4D B8         MOV     ECX, DWORD PTR SS:[EBP-48]
7B7BF928   C641 08 01      MOV     BYTE PTR DS:[ECX+8], 1
7B7BF92C   8B15 5413FD7A   MOV     EDX, DWORD PTR DS:[7AFD1354]    mscorwks.7A3B339C
7B7BF932   833A 00         CMP     DWORD PTR DS:[EDX], 0
7B7BF935   74 07           JE      SHORT 7B7BF93E                  System_W.7B7BF93E
7B7BF937   50              PUSH    EAX
7B7BF938   E8 9B8698FF     CALL    7B147FD8                        System_W.7B147FD8
7B7BF93D   58              POP     EAX
7B7BF93E   8945 D4         MOV     DWORD PTR SS:[EBP-2C], EAX
7B7BF941   EB 0B           JMP     SHORT 7B7BF94E                  System_W.7B7BF94E
DS:[7B0DC010]=7E3AC2E8 (USER32.GetActiveWindow)
```

Por encima de estor tres saltos condicionales encontramos más llamadas a system_w
Seleccionamos cualquiera por encima de estos, colocamos un bp con f2 , oprimimos f9, oprimimos aceptar y register.



Cuando nuestro bp pica tendremos el serial en el la pila.....
Lo copiamos y pegamos en la caja correspondiente y le damos a register





Nota:

Al realizarlo en window 7 cada vez que coloquemos un bp nos saldrá un cartel al cual le daremos que si para que el bp se marque.

Para ver la dirección de retorno del mensaje posiblemente sea necesario seleccionar el _CorExemain(mscore.dll**)(Evadiendo StrongNames de .NET con OllyDbg - por marciano)**

y no stnotepad ,pero sin la necesidad de parar en ella al arrancar. Solamente seleccionarla para que muestre la ventana después de tratar de registrarnos.

En xp no tenemos mucho problema para los bp, (al introducir la clave mala, introducir números y letras ,pj:"989898hola", en una prueba que hice con solo números me aceptó la clave y se registró, pero no se desbloqueó el programa, ni dejo de mostrar el mensaje trial, tampoco daba la opción de registrarlo nuevamente ya que la clave había sido almacenada como buena)