PROGRAMA~ DESCRIPCION	CALCULO HABER JUBILATORIO
HERRAMIENTAS	RDG PACKER DETECTOR ~ IL SPY
DIFICULTAD	POCA
COMPRESOR/ COMPILADOR	.NET
PROTECCION	ANTI DEBUGGER (IS DEBUGGER PRESENT)
OBJETIVOS	REGISTRARSE
MÉDICO:	GUILLE3000
TUTORIAL N°:	1

PRIMERO QUE NADA QUIERO AGRADECER A TODA LA COMUNIDAD DE CRACKSLATINOS POR SU COLABORACIÓN Y MUY ESPECIALMENTE A "TROMPETIN17EVONY" QUIEN ME HA AYUDADO MUCHO PARA LLEGAR AL RESULTADO AQUÍ MOSTRADO, QUIEN CONSIDERO COMO UN GRAN MAESTRO, Y APROVECHO PARA MANDARLE UN GRAN ABRAZO!.

ADEMAS HAGO PROPICIA ESTA OCASIÓN PARA MANDARLES UN GRAN SALUDO A TODA LA LISTA DE CRACKS LATINOS!

El obra es solo a los fines científico - didáctica y como conocimiento de la programación en general. El autor de la misma no se hace responsable del uso ilícito de los contenidos de la presente obra.

Además no quiero dejar de mencionar que soy nuevo en esto, soy solo un aprendiz de aprendiz.. así que desde ya pido disculpa a los Maestros del crack, por los errores que seguramente cometí en este tutorial, sepan disculpar ya que estoy aprendiendo y sus críticas y consejos serán muy bien recibidos en todo momento.

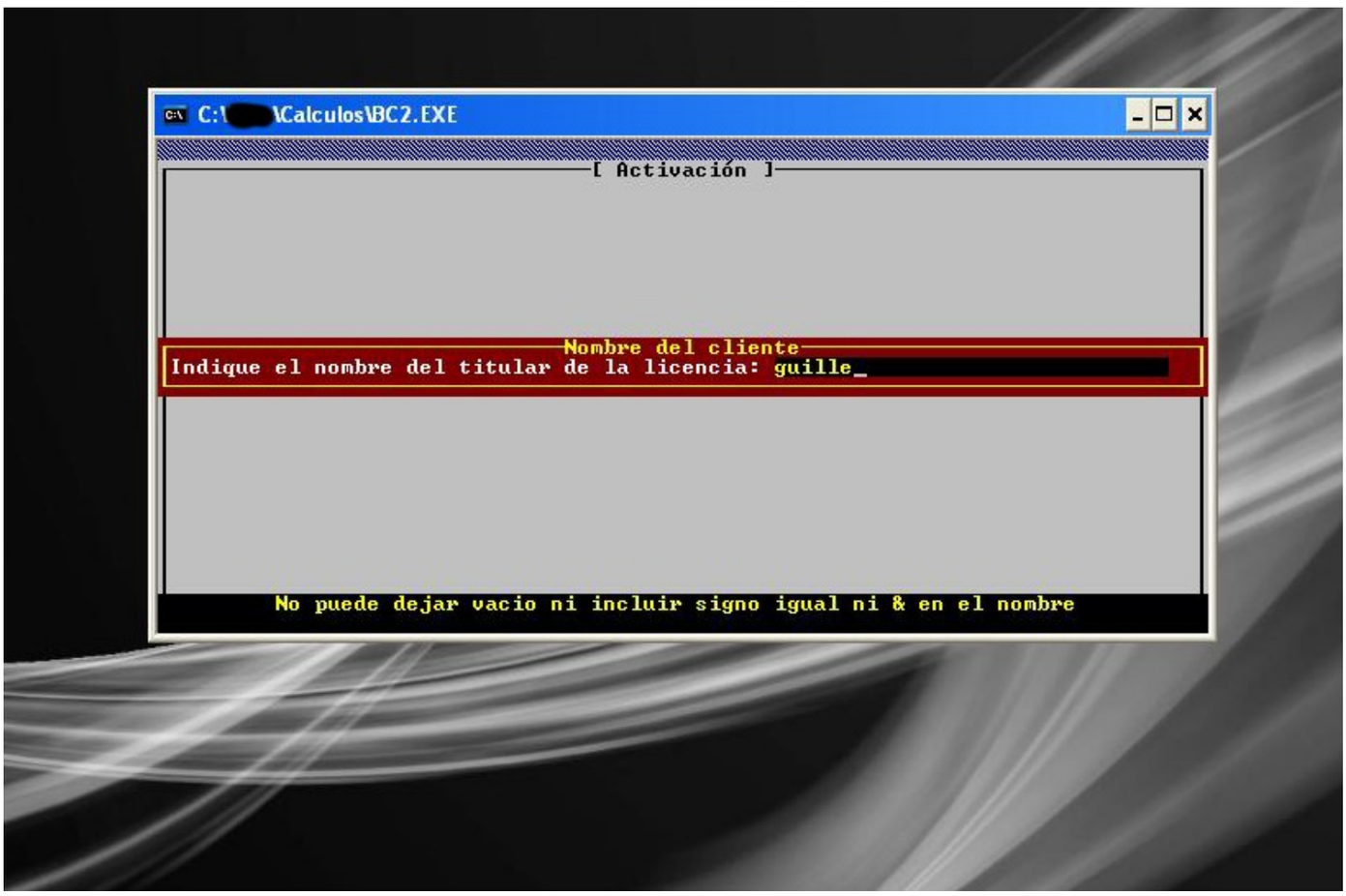
Me tome el atrevimiento de hacer un logo de cracks latinos je je!.

Cabe aclarar que **no** voy a mencionar el nombre del programa utilizado, ya que el mismo es de uso comercial, y utilizo un sistema de censura en el tutorial…no apto para menores de 18 años.. je je!!.

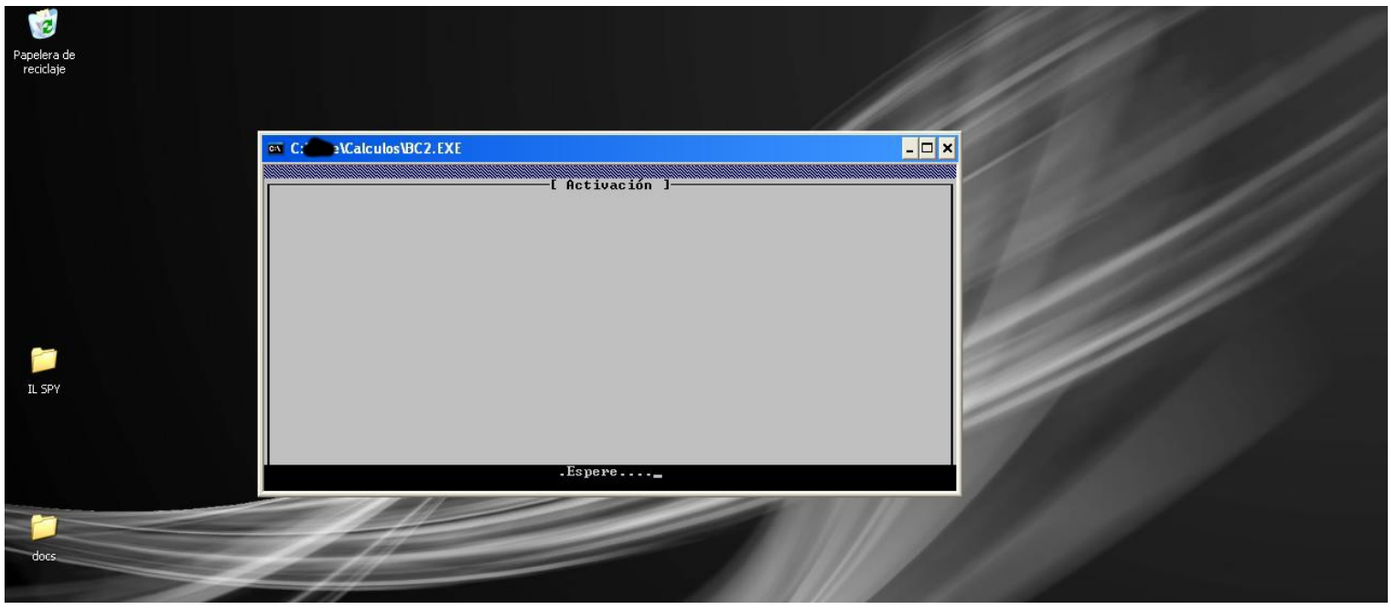
Quien necesite el programa puede mandarme un mensaje privado y me pondré en contacto.

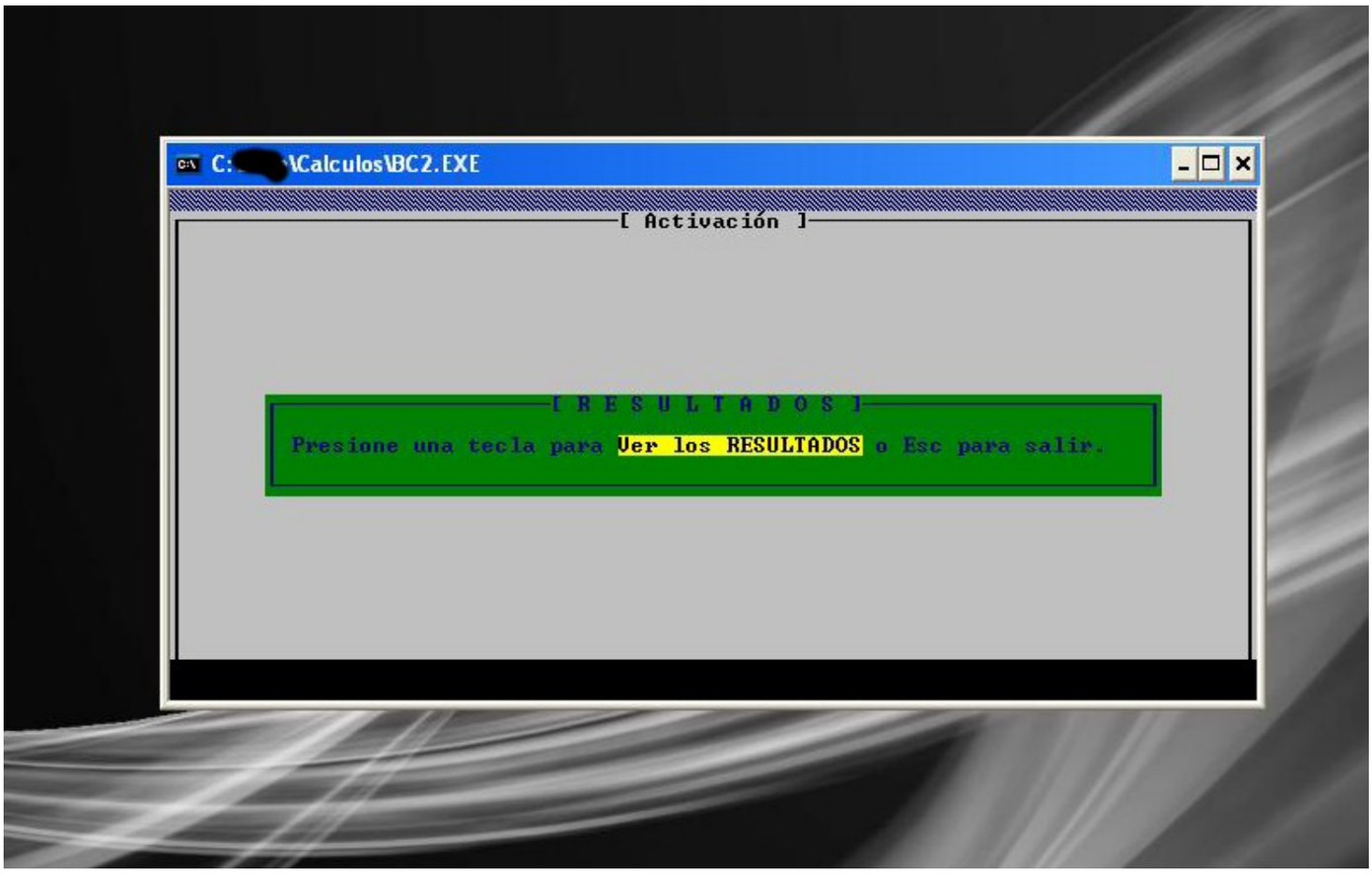
EMPEZAMOS:

Este programa casi finalizando la instalación nos va a presentar la siguiente pantalla en donde nos invita a colocar nuestro nombre de usuario, a lo cual accedemos a realizarlo:

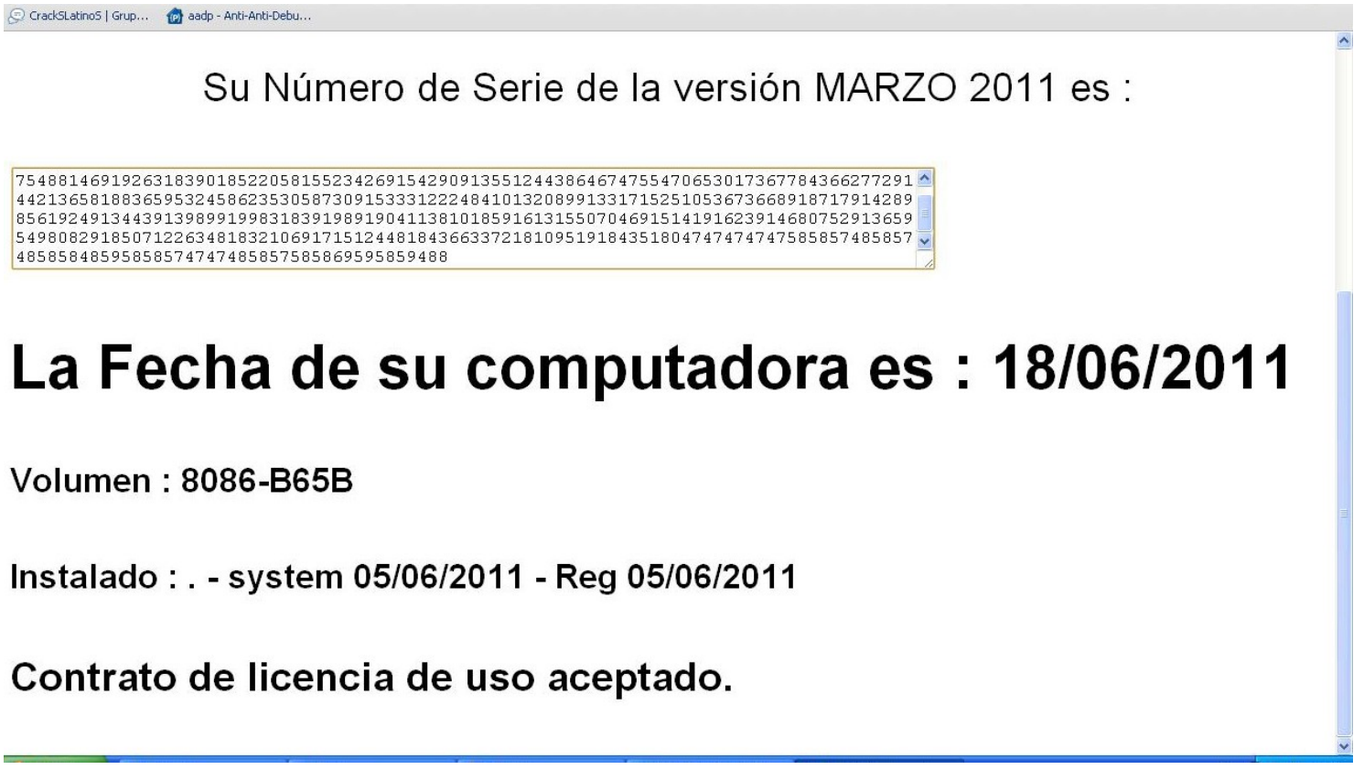


Es de destacar que el proceso de instalación y de activación no se hace a través de un programa de 32 bits, sino de 16 bits (D.O.S) como se puede ver en las imágenes

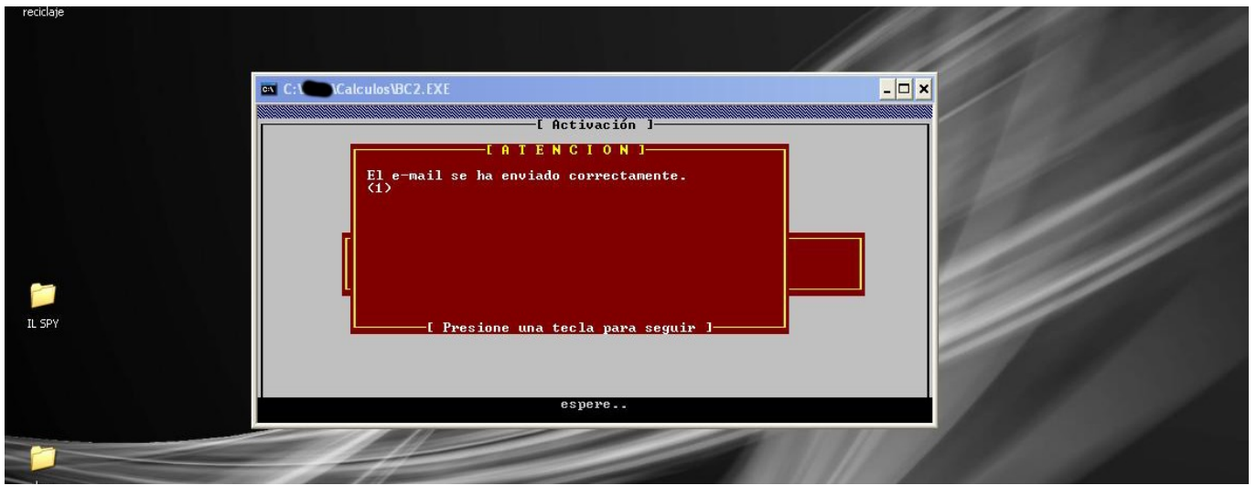




Presionamos la tecla “Enter” como nos indica, y se nos va a abrir una ventana de nuestro navegador web como se puede apreciar en la figura siguiente.



Luego se nos presenta

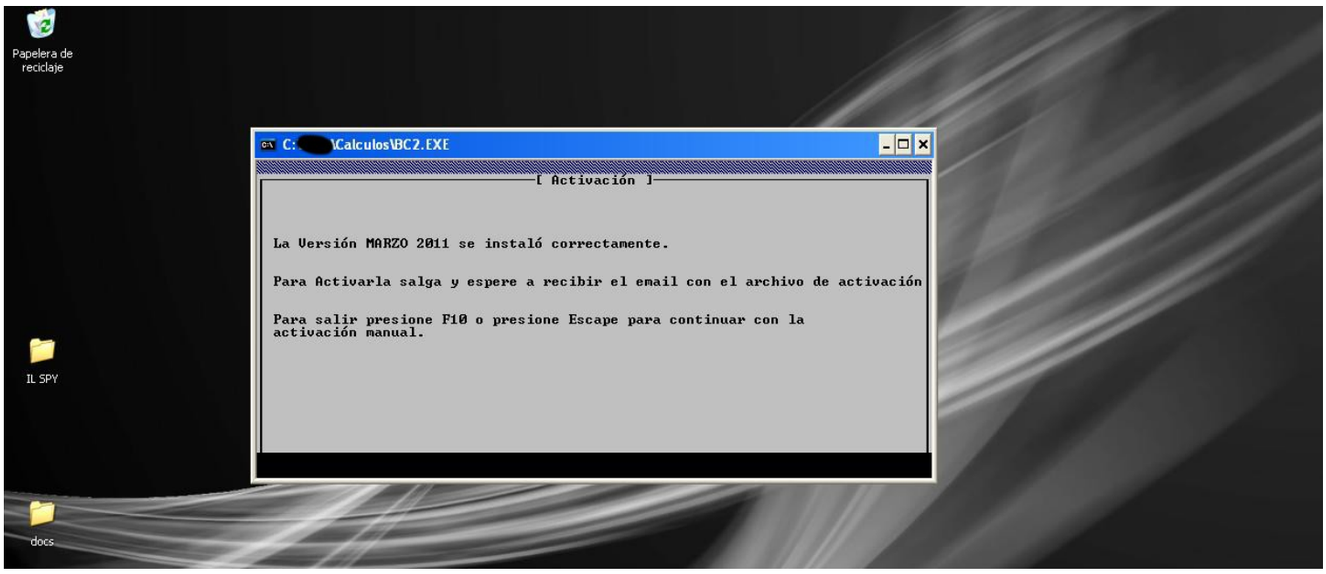


Aquí quiero aclara que la activación del programa se realiza lógicamente previo pago de una suma de dinero, luego le mandan al usuario vía mail un correo con un archivo “activador” que debe ser ejecutado para que active el programa previa modificación de la hora del reloj de tu computadora.

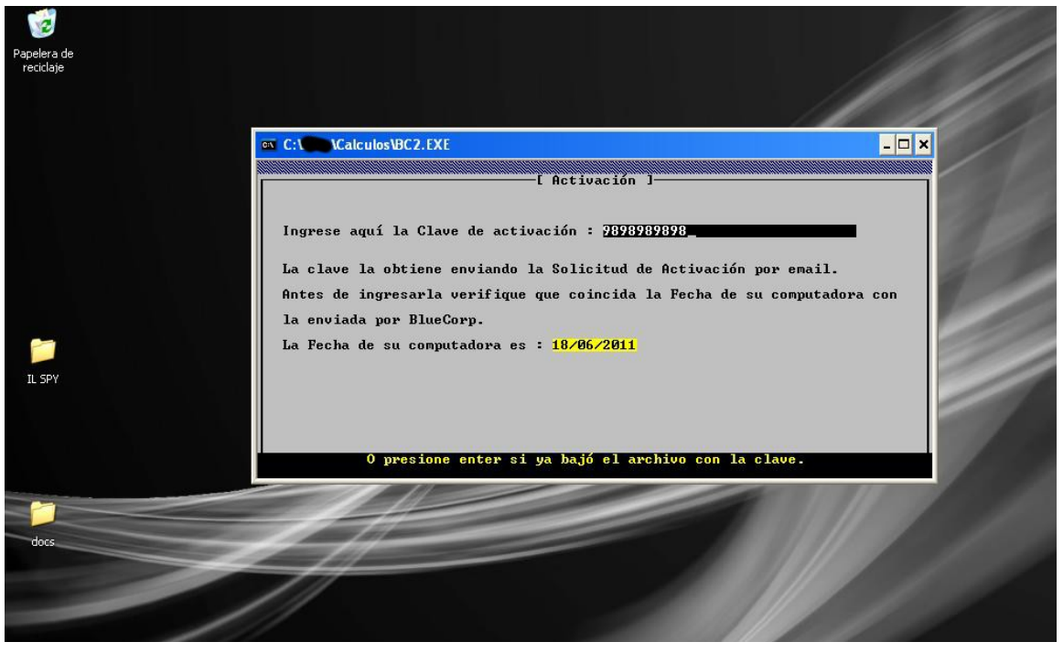
Es decir que cambias primero la fecha de tu computadora a la que apareció en la imagen de más arriba, y luego ejecutás el .exe que te mandan por correo, una vez que se finaliza recién ahí volvés a la fecha correcta de tu Pc. (para mí y que quede entre nosotros… je je! peor no se les puede haber ocurrido…!!).

Quédensen tranquilos que nosotros no lo vamos a hacer.

Luego aparece:



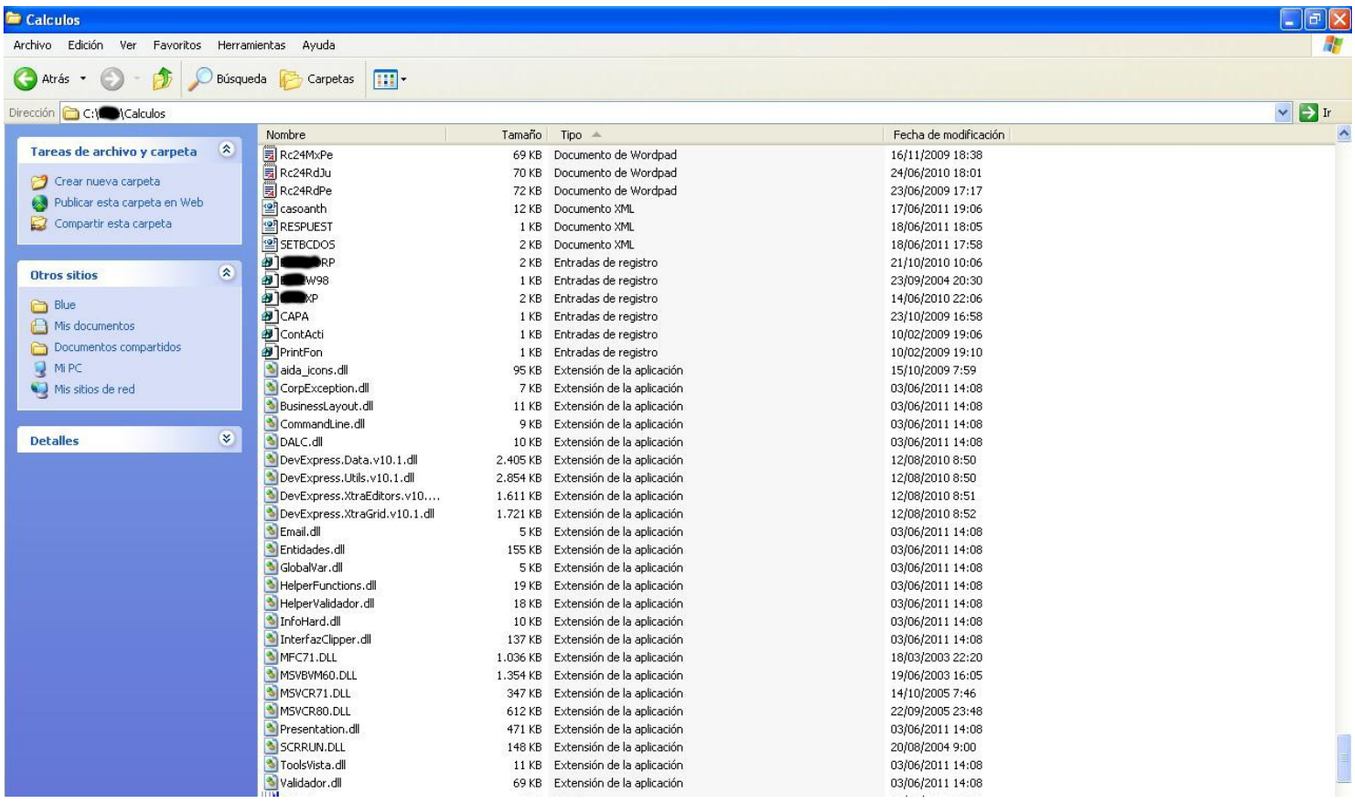
Presionamos escape y ponemos un serial cualquiera.. nota: solo admite numéricos, porque si ponemos alguna letra no lo ingresa.



Una vez que ingresamos el serial, no nos aparece ningún tipo de mensaje y se cierra esta pantalla, pero obviamente que es incorrecto.

Hecho todo esto vamos a la carpeta donde se instalo este bicho… que no es ni más ni menos que en la raíz de nuestro disco rígido ya que no nos permitió elegir donde hacerlo.

Si la exploramos vamos a ver entre toda la lista de archivos las siguientes dll



Como verán hay una dll que se llama validador.. pero no valida el programa, sino un calculo que ingresa el usuario dentro del programa.

También en esta carpeta vamos a ver que hay varios archivos .exe que no son de 32 bits sino que se utilizan para la instalación del programa.

Buscamos el ejecutable principal y lo pasamos por el RDG a ver que nos dice.

Hacemos clic en donde está en rojo para un análisis más profundo para ver que nos informa..

También no nos dice nada.. pero que “interactúa” con dll.. Nota: intenté hacer la captura de pantalla.. pero no salió.. solo sale igual que la presentada arriba. Pero podemos ver que hacer interop con dlls nativas.

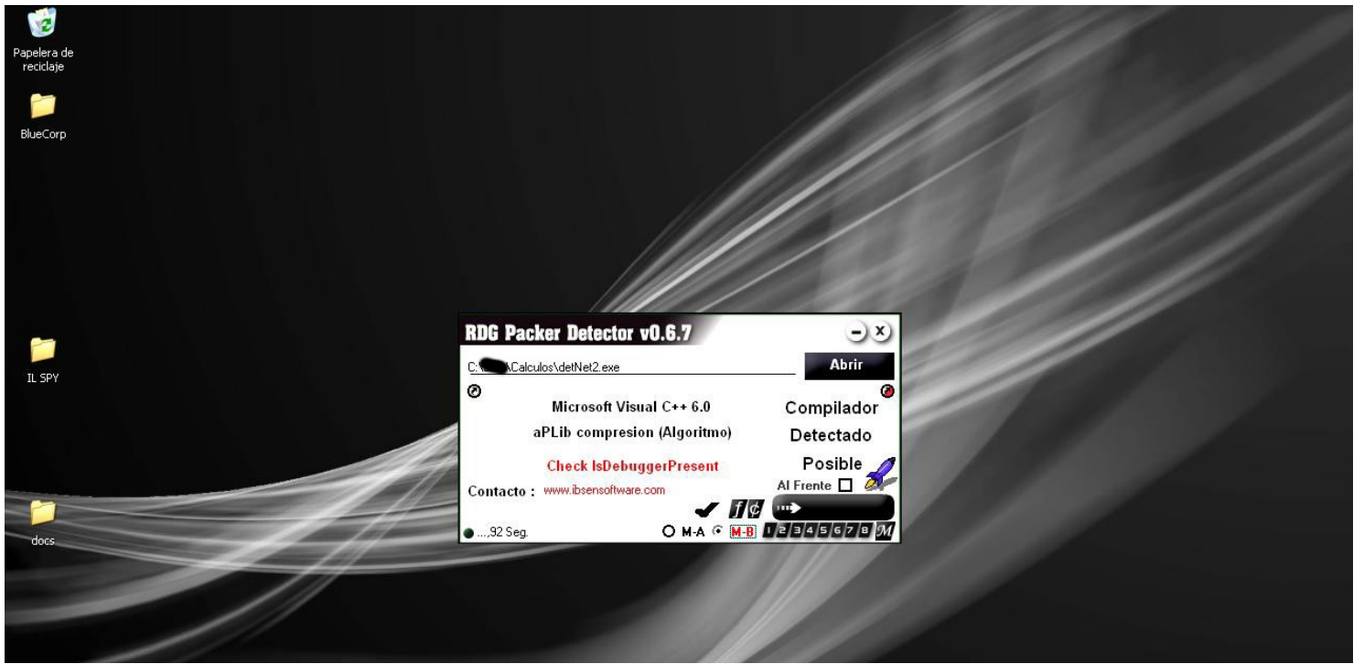
Investigué un poco y encontré lo siguiente:

"El espacio de nombres System.Runtime.InteropServices proporciona una gran variedad de miembros que admiten la interoperabilidad COM y los servicios de invocación de plataforma. Si no está familiarizado con estos servicios, vea Interoperar con código no administrado.

Los miembros de este espacio de nombres proporcionan varias categorías de funcionalidad.

Los atributos controlan el comportamiento del cálculo de referencias, como el modo de organizar las estructuras o el modo de representar las cadenas. Entre los atributos más importantes se encuentran el atributo DllImportAttribute, que se utiliza para definir los métodos de invocación de plataforma que se utilizan para obtener acceso a las API no administradas, y el atributo MarshalAsAttribute, que se utiliza para especificar la forma de calcular las referencias de los datos entre la memoria administrada y no administrada."

Como veo en las dll del directorio una sospechosa (dedNet2.dll) que me llama mi atención, también la paso por el detector, quiero aclarar que digo que llama mi atención porque como la activación se realiza por medio de internet.. quizás tenga algo que ver.. total no viene mal y la analizo igual:

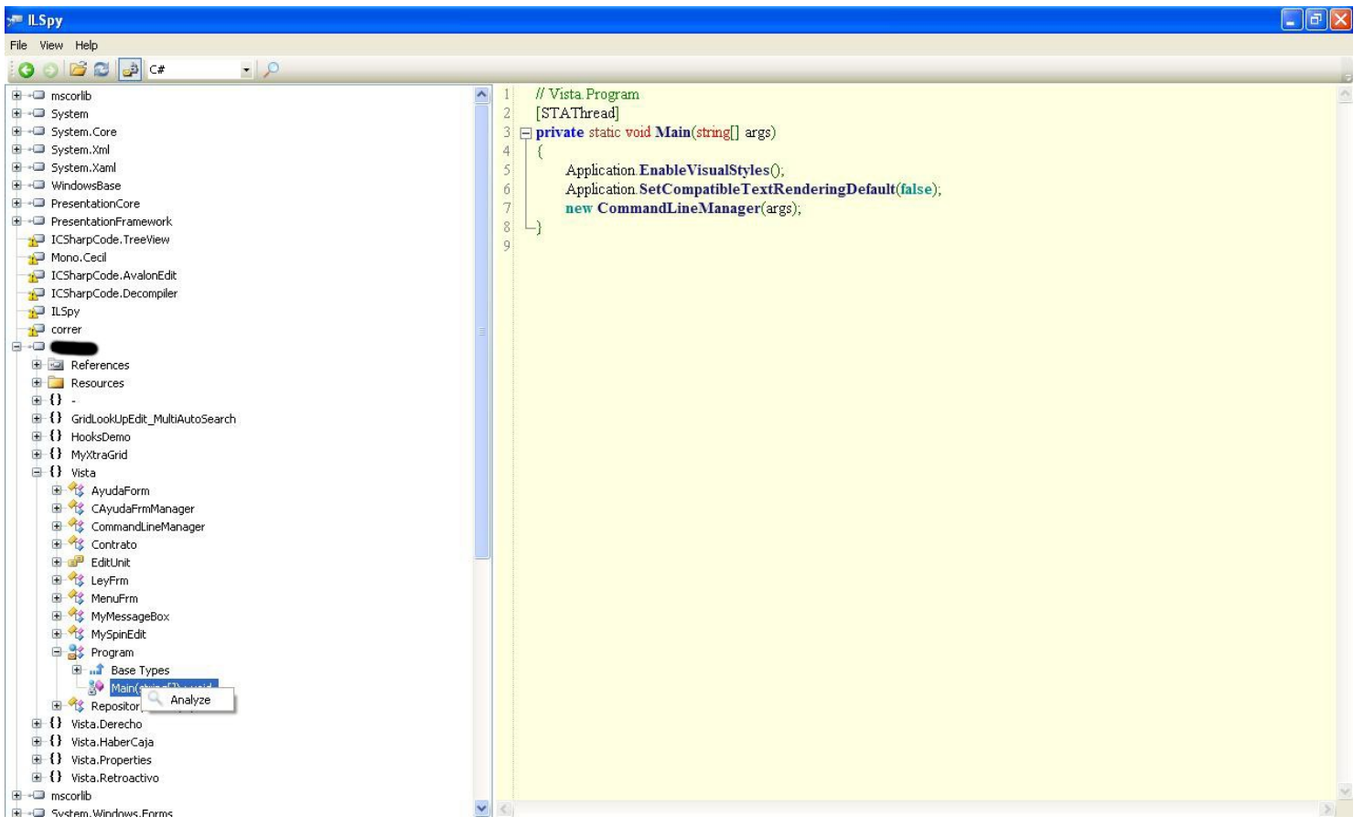


Como podemos apreciar tiene una protección antidebugger. Quiero contarles que entré en la duda, y me preguntaba: ¿Que me conviene... atacar el activador o el principal?

Nota: * El principal cuando se ejecuta aparece una ventana mensaje donde dice que el programa no está activado y botón aceptar y se cierra.

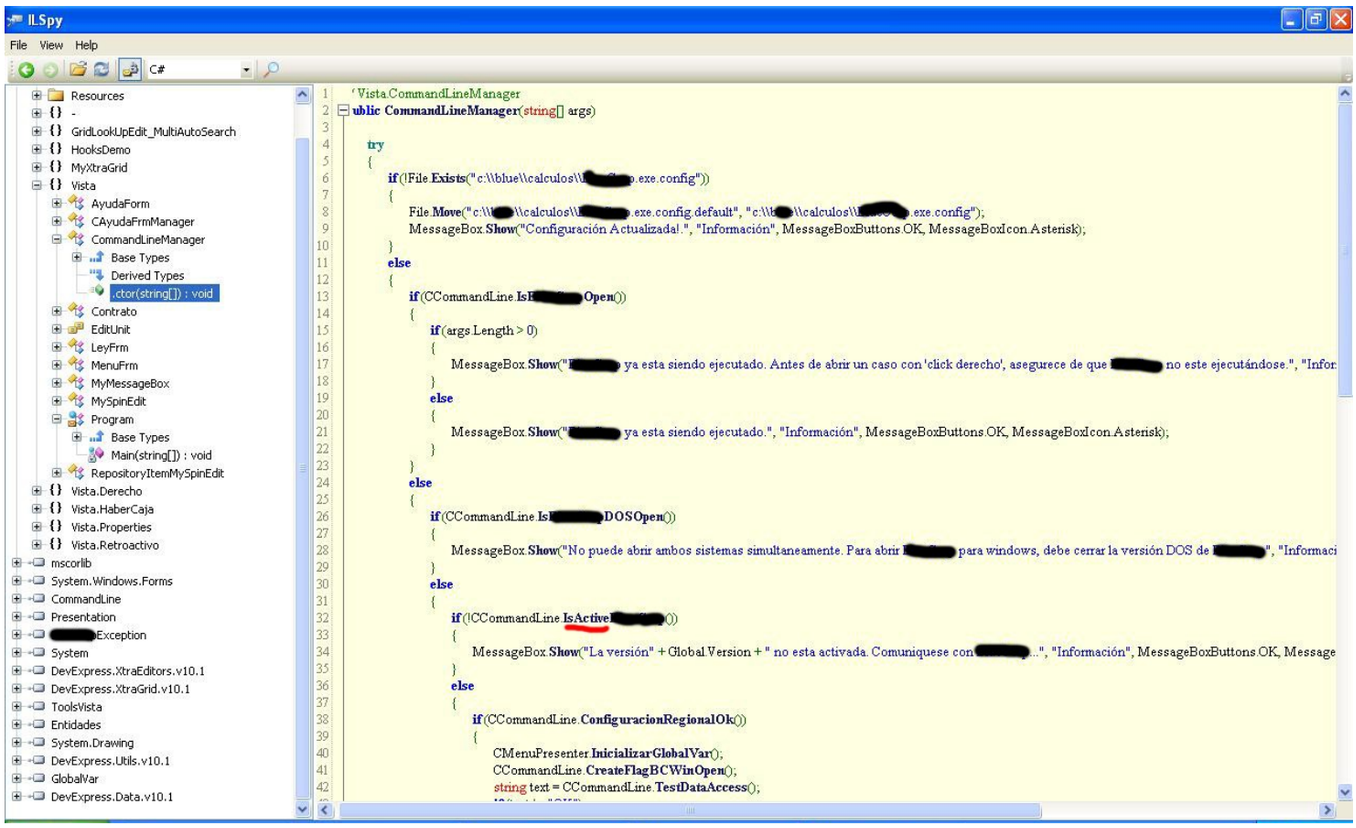
Así que me puse a experimentar con varios debuggeadores.. como el Olly, Ida, Calimero.. y cuando el programa detecta que hay debugger, cambia su comportamiento “modificándose” y obligándonos a reinstalarlo de nuevo, ya que si lo ejecutamos.. muestra un mensaje que hay 2 versiones del mismo ejecutándose (por más que esté todo cerrado).

Pero lo más fácil y que nos conviene es que . como es un net el principal, abrimos el IL Spy o el Reflector, cargamos nuestro ejecutable principal (el único de 32 bits que hay) y vemos lo siguiente:



Como podemos ver el código no está ofuscado ni tampoco empaquetado,, ni nada por el estilo.

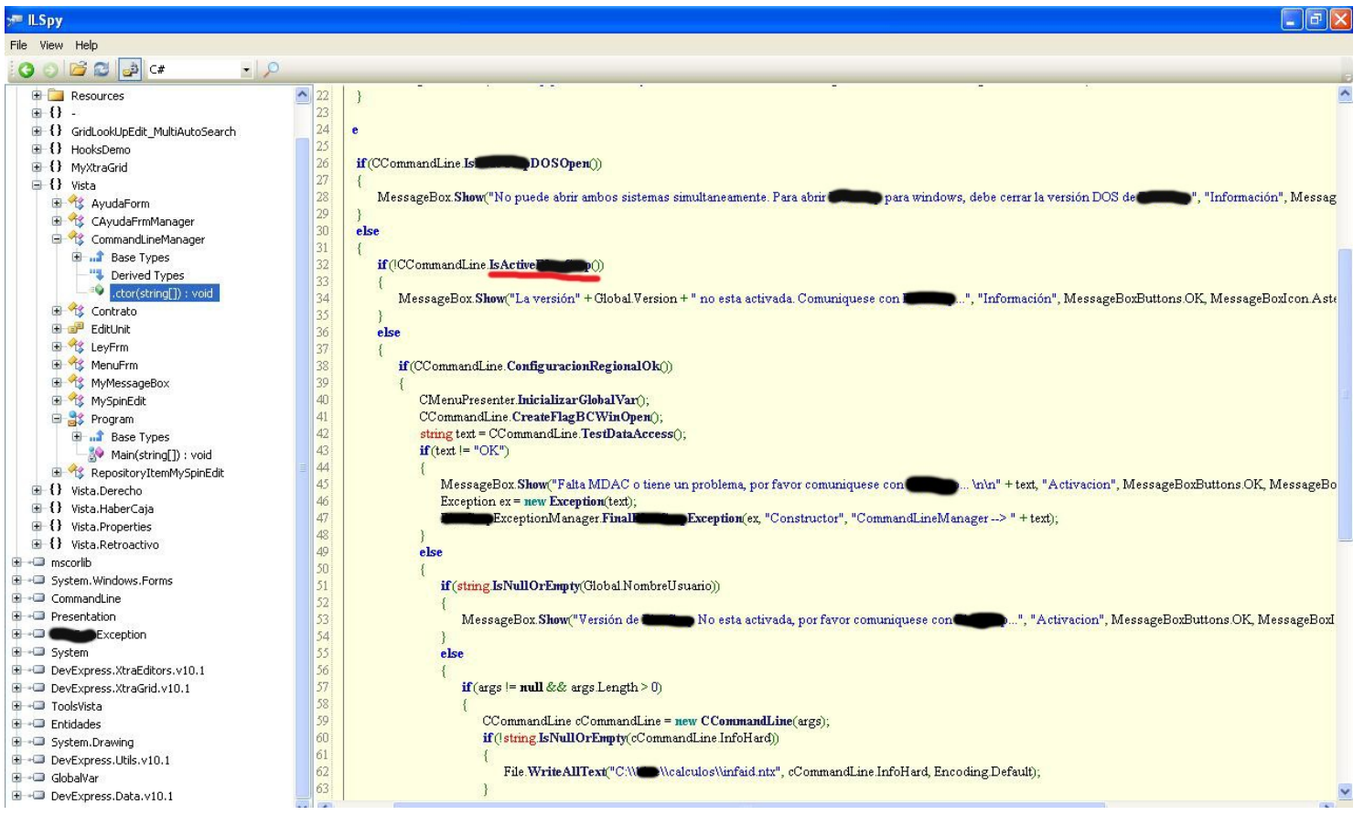
Así que nos dirigimos a analizar el Main del programa principal. Vemos como en la imagen de arriba aparece una clase que se llama CommandLineMannager, así que seguimos este hilo para ver hasta dónde nos conduce.



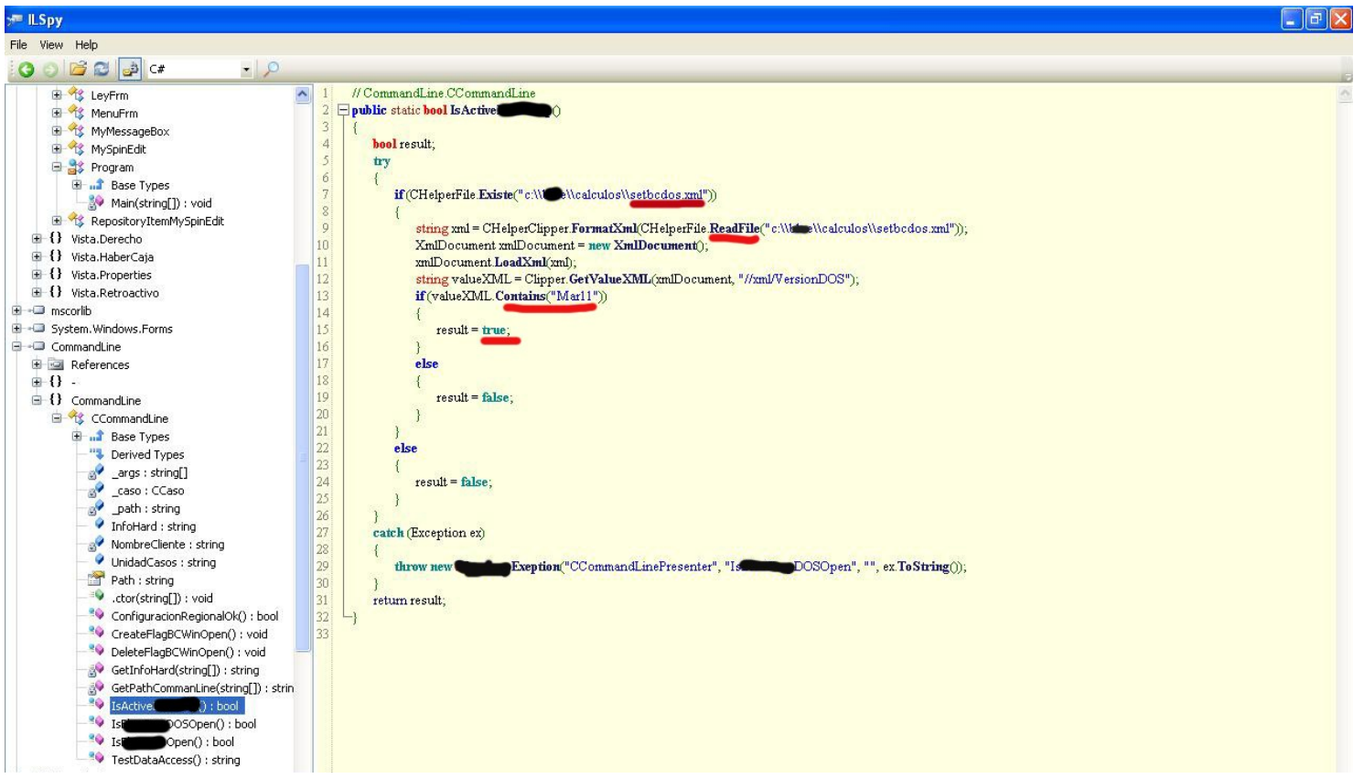
Bueno.. primero quiere volver a pedir perdón por tanta censura pero en mi país se está poniendo fea la cuestión por violación de derechos intelectuales.. así que no me queda otra.. pero lo único que aparece detrás de esa censura negra es el nombre del programa (nada interesante).

Volviendo a los nuestro vemos que hay una llamada a un método muy interesante… "IsActiveXX()".. seguido del mensaje de Bad Boy. (este es el "messageBox" que nos aparece al intentar ejecutar el programa sin la activación correspondiente). Así que la clave para que nos registre es esté método devuelva siempre "true"

Así que vamos derecho para allá.. parece que vamos por buen camino!.



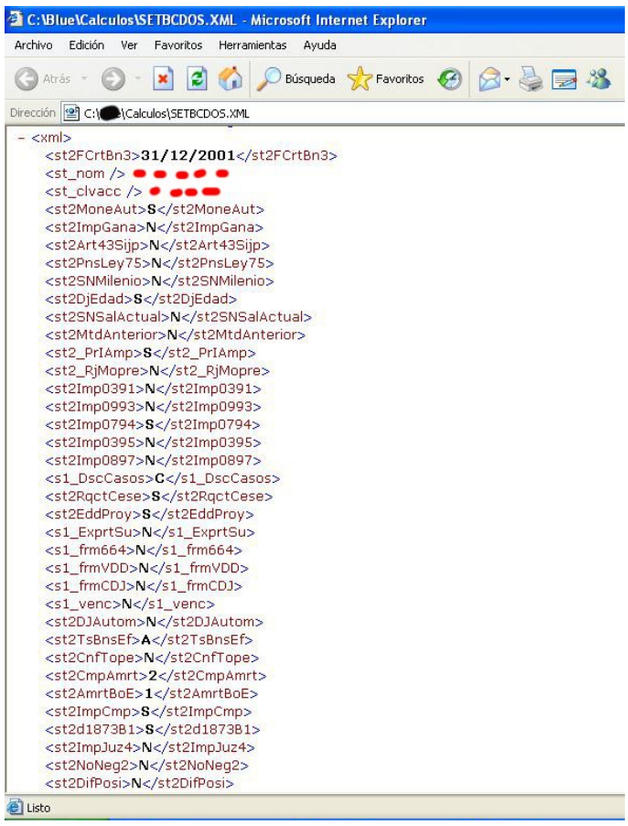
Ahora entramos en el método IsActiveXX() para ver de qué se trata

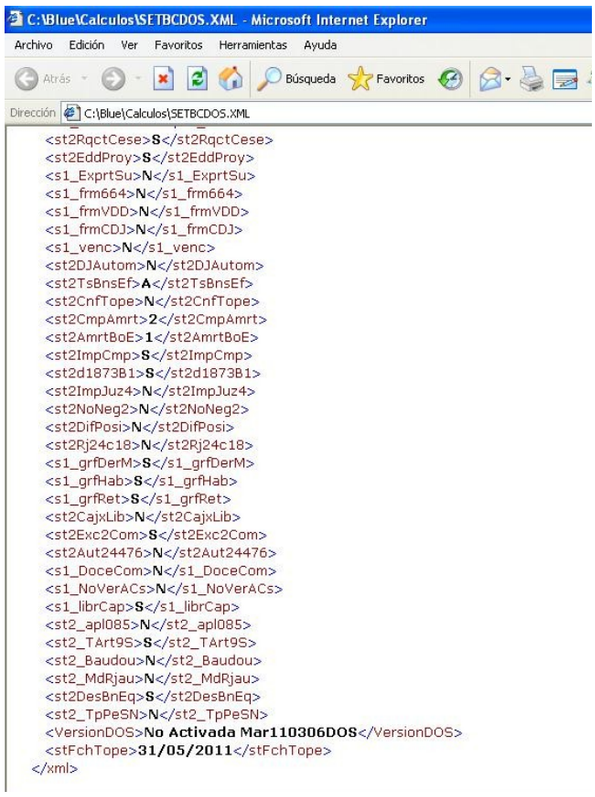


Ahí vemos donde esta subrayado en rojo en la imagen que el programa antes de iniciarse verifica si existe un archivo .xml, si este no existe entonces devuelve falso, en cambio si existe lo va a leer su contenido y si este contiene la cadena Mar11 devuelve true.

Es decir que la activación del programa se basa en ese archivo xml, en donde verifica el nombre de usuario, si esta activado o no activado y demás variables necesarias para la ejecución del programa.

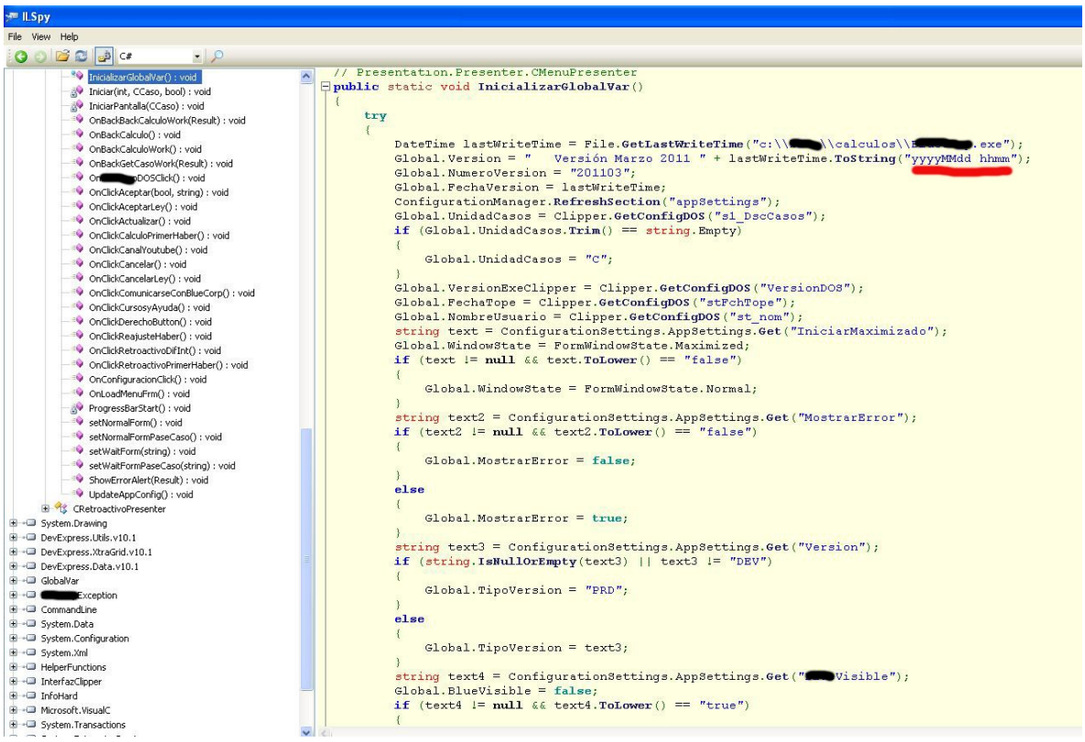
Entonces vayamos a analizar el contenido del archivo xml en cuestión





Vemos que ahí donde marqué en rojo deja un espacio en blanco donde claramente se puede distinguir que está haciendo referencia al nombre de usuario (st_nom) y abajo la fecha de activación. También llegando al final del xml vemos que claramente dice “No Activada”

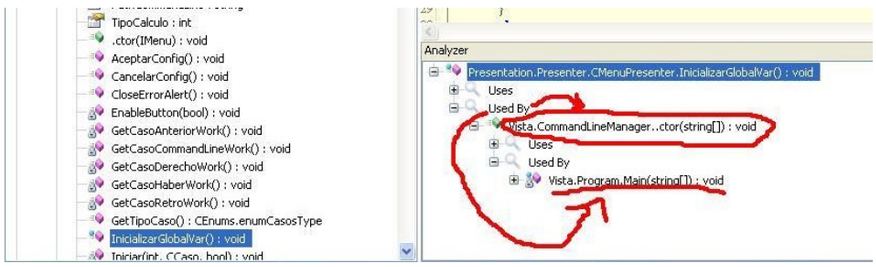
Si recordamos más arriba en la imágenes podíamos ver que en el constructor de la clase CommandLineManager había una llamada a InicializarGlobalVar



Vemos que en el formato de la fecha es año, mes, día y hora con minutos.

Si recordamos, más arriba habíamos visto que en el método IsActiveXX(), una de las condiciones para que devuelva verdadero es que la variable GlobalNombreUsuario no tiene que tener una cadena nula o vacía.

Y si seguimos el hilo a este proceso con el IL Spy vemos



Que según entiendo este método es usado por el constructor de la clase CommandLineManager, que a su vez es utilizado por el Main del Programa.

Entonces en conclusión no haría falta modificar el .exe, sino que solamente sería suficiente con modificar el contenido del archivo xml (el que hacíamos referencia anteriormente)

Para hacerlo basta con cualquier editor de xml o incluso en mi caso utilicé el bloc de notas de Windows.

Solo basta con que este archivo tenga un nombre de usuario para que el programa se inicie, no obstante ello, preferí completar no solo el campo nombre, sino también el segundo campo que hacía referencia a la fecha de activación y en las últimas líneas cambiar la cadena “No activada” por “Activada”.. Solo porque me pareció que quedaba más prolijo .

El resultado nos queda así:


```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xml>
<st2FCrtBn3>31/12/2001</st2FCrtBn3>
<st_nom>Solid Snake</st_nom>
<st_clvacc>2011 20110616 1912        </st_clvacc>
<st2MoneAut>S</st2MoneAut>
<st2ImpGana>N</st2ImpGana>
<st2Art43Sijp>N</st2Art43Sijp>
<st2PnsLey75>N</st2PnsLey75>
<st2SNMilenio>N</st2SNMilenio>
<st2DjEdad>S</st2DjEdad>
<st2SNSalActual>N</st2SNSalActual>
<st2MtdAnterior>N</st2MtdAnterior>
<st2_PrlAmp>S</st2_PrlAmp>
<st2_RjMopre>N</st2_RjMopre>
<st2Imp0391>N</st2Imp0391>
<st2Imp0993>N</st2Imp0993>
<st2Imp0794>S</st2Imp0794>
<st2Imp0395>N</st2Imp0395>
<st2Imp0897>N</st2Imp0897>
<s1_DscCasos>C</s1_DscCasos>
<st2RqctCese>S</st2RqctCese>
<st2EddProy>S</st2EddProy>
<s1_ExprtSu>N</s1_ExprtSu>
<s1_frm664>N</s1_frm664>
<s1_frmVDD>N</s1_frmVDD>
<s1_frmCDJ>N</s1_frmCDJ>
<s1_venc>N</s1_venc>
<st2DJAutom>N</st2DJAutom>
<st2TsBnsEf>A</st2TsBnsEf>
<st2CnfTope>N</st2CnfTope>
<st2CmpAmrt>2</st2CmpAmrt>
<st2AmrtBoE>1</st2AmrtBoE>
<st2ImpCmp>S</st2ImpCmp>
<st2d1873B1>S</st2d1873B1>
<st2ImpJuz4>N</st2ImpJuz4>
<st2NoNeg2>N</st2NoNeg2>
<st2DifPosi>N</st2DifPosi>
<st2Rj24c18>N</st2Rj24c18>
<s1_grfDerM>S</s1_grfDerM>
```

<s1_grfHab>S</s1_grfHab>

<s1_grfRet>S</s1_grfRet>

<st2CajxLib>N</st2CajxLib>

<st2Exc2Com>S</st2Exc2Com>

<st2Aut24476>N</st2Aut24476>

<s1_DoceCom>N</s1_DoceCom>

<s1_NoVerACs>N</s1_NoVerACs>

<s1_librCap>S</s1_librCap>

<st2_apl085>N</st2_apl085>

<st2_TArt9S>S</st2_TArt9S>

<st2_Baudou>N</st2_Baudou>

<st2_MdRjau>N</st2_MdRjau>

<st2DesBnEq>S</st2DesBnEq>

<st2_TpPeSN>N</st2_TpPeSN>

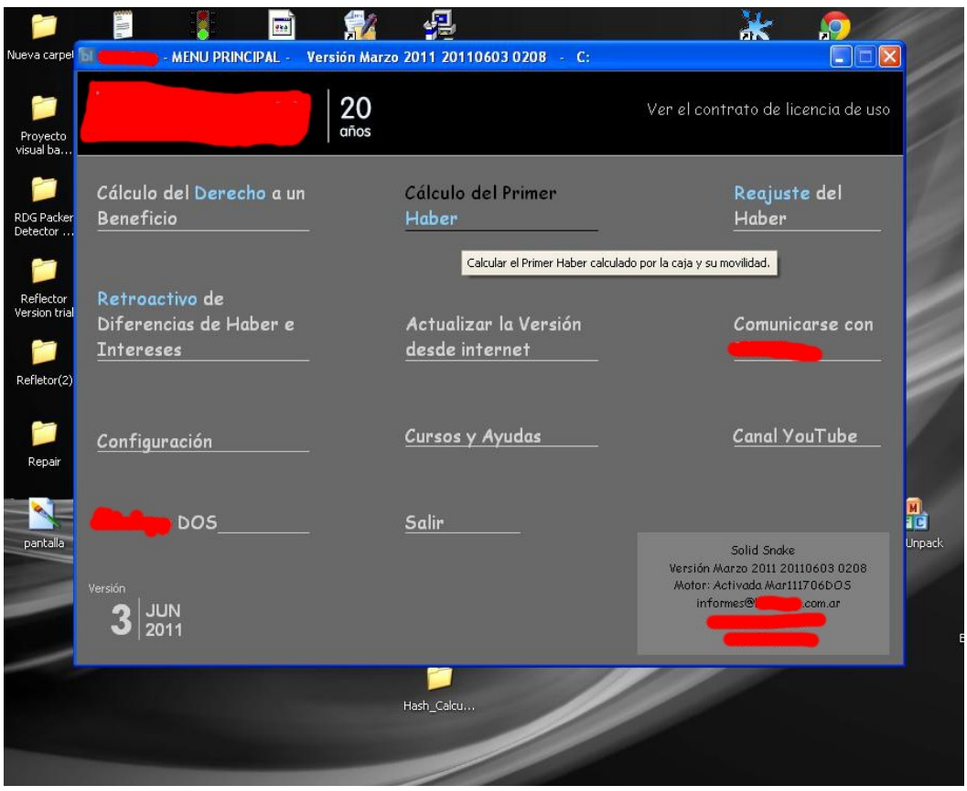
<VersionDOS>Activada Mar111606DOS</VersionDOS>

<stFchTope>31/07/2012</stFchTope>

</xml>

Guardamos las modificaciones

Ahora ejecutamos el archivo principal del programa y vemos que esta 100% funcional y registrado a nombre de Solid Snake (je je…como verán me gusta la saga Metal Gear Solid)



En rojo solo está tapando el nombre del programa

Conclusión

Para que el programa solo basta con que el campo nombre de usuario del xml no esté en blanco.

Según palabras de mi gran maestro trompetin17evony "…los que tengan 64 bits, NO les fun por que usa el driver
MIcrosoft Jet oledb 4.0, deben modificar el CorFlag para que sea IL Only + 32Bit Required"

Finalizando

Perdonen por los errores que seguramente cometí en este tutorial, ojalá que se haya entendido..ya que no soy muy bueno explicando… además espero que este tute le pueda servir a alguien!.

Quiero agradecer nuevamente a todos los crackers que comparten sus conocimientos con los demás, también a Ricardo Narvaja quien siempre me ayuda desinteresadamente cuando tengo alguna duda y nuevamente Muchísimas Gracias a trompetin17evony. Y Gracias!! a CracksLatinos por este espacio!!. Saludos a todos y hasta la próxima!!