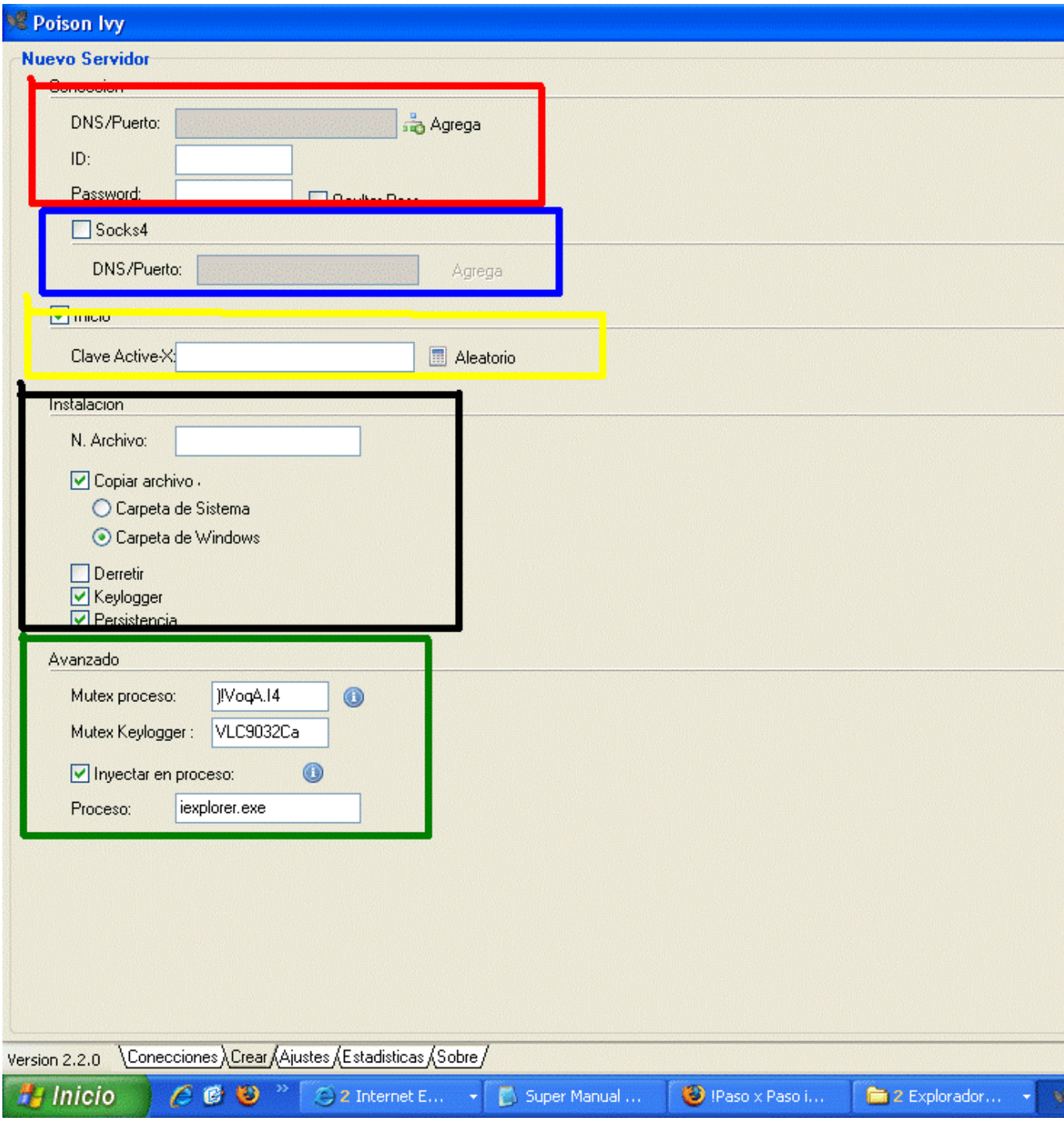
Cuando hayamos descargado el troyano recomiendo descomprimirlo a una carpeta nueva vacía ya que el troyano viene comprimido en zip. Para esta labor necesitamos desactivar nuestro antivirus. Cualquier error que diga: No tiene los permisos necesarios es referente al antivirus no hay discusión.

***Comenzamos Al abrir por primera ocasión el troyano nos aparecerá la ventana de aceptar el contrato de uso le damos a accept, a continuación nos aparecerá la ventana del poison ivy, si tienes el antivirus activo no podrás hacer la labor, así que importantisimo que desactives el antivirus y descomprimas el troyano en una carpeta nueva para abrirlo desde ahí, esta parte trata de la configuración así que anda a la pestaña crear, a continuación nos aparecerá la siguiente ventana.

⚠ This image has been resized. Click this bar to view the full image. The original image is sized 1024x76



PANEL CONEXIÓN

***DNS/Puerto: En este panel se configura a que host/direccion ip/dominio se conectara el server que mandaras por ejemplo, tu ip o dominio no-ip. El puerto sera el que usara el troyano para conectarse es importante que elijas un puerto recomendado para la conexión yo digo que el predeterminado 3460 es bueno, pero también puedes usar el 80 o el 8181 que también considero buenos,Si pones una = la tendrás que poner en el panel de configuración del troyano para que conecte. Te recomiendo siempre probar la conexión antes.

***ID: Es el nombre predeterminado que tendrá vuestra Posible Control al conectarse,

por ejemplo si escribes prueba, cuando se conecte a tu troyano tendrá el nombre prueba que posteriormente podrás cambiar.

- Ocultar pass: activado esta casilla la password que pongas se expresara en asteriscos (***)

PANEL SOCKS 4

Este panel no es imprescindible ni importante en ningún aspecto, es uno especialmente diseñado para los que utilizan conexión mediante proxys que son programas que toman dominios de cualquier lugar del planeta para cubrir tu ip. Si lo activas debes estar seguro del dominio y puerto configurados en tu proxy, en lo personal recomiendo no activarla, y a los que no usen y no tengan el mínimo conocimiento de lo que es = dejarla desactivada siempre.

***Socks 4: Activando la casilla activaras las correspondient es configuracione s del panel

***DNS/PUERTO: colocamos el puerto y del dominio previamente configurados en el servidor proxy.

***PASSWORD: Es el password de la conexión no es nada importante ni necesario, es como para privacidad. Si pones una = la tendrás que poner en el panel de configuración del troyano para que conecte.

PANEL START UP

Este panel pequeño configura las opciones startup, osea las opciones de arranque del server , la verdad que es fácil esta parte.

***INICIO: Al activar esta casilla entonces estarías activando el sistema de creación de clave en el registro para que el troyano inicie con windows.

***Clave Activex: crea una clave en el registro de la Posible Control para que inicie con windows, pon Aleatorio y creara una clave cualquiera.

PANEL INSTALACIÓN

Estas son las opciones de la instalación del server en la pc de la Posible Control.

***NOMBRE DE ARCHIVO: Cuando la Posible Control ejecute el troyano el troyano solo se instalara en una carpeta de la pc Posible Control (específicamente la que elegiste) , en esta opción deberás poner el nombre que quieres que tenga el server cuando se instale , deberá terminar en la extensión .exe por ejemplo: prueba.exe,

***COPIAR ARCHIVO A: Activando la casilla correspondient e activas las demás para su configuración

-CARPETA DEL SISTEMA: activando esta casilla configuras que el server se instalara en la carpeta system32 de la Posible Control , por si las dudas esta carpeta se encuentra en Disco Local/WINDOWS/Sytem32.

-CARPETA DE WINDOWS: activando esta casilla configuras que el server se instalara en la carpeta de WINDOWS.

***DERRETIR: Activando esta casilla el server se borrara automáticamente cuando lo ejecuten pero si se instalara.

***KEYLOGGER: Activando esta casilla activaras las opciones y el guardado del keylogger, recomiendo activarla siempre.

***PERSISTENCIA: Activando esta casilla el server sera muy difícil de eliminarlo (el instalado), incluso hasta para los antivirus, tirara un mensaje de error siempre de : El archivo no puede ser borrado ya que esta siendo usado por otro programa. Lo que hace muy difícil su eliminación.

PANEL AVANZADO

aquí en este panel las opciones avanzadas del server.

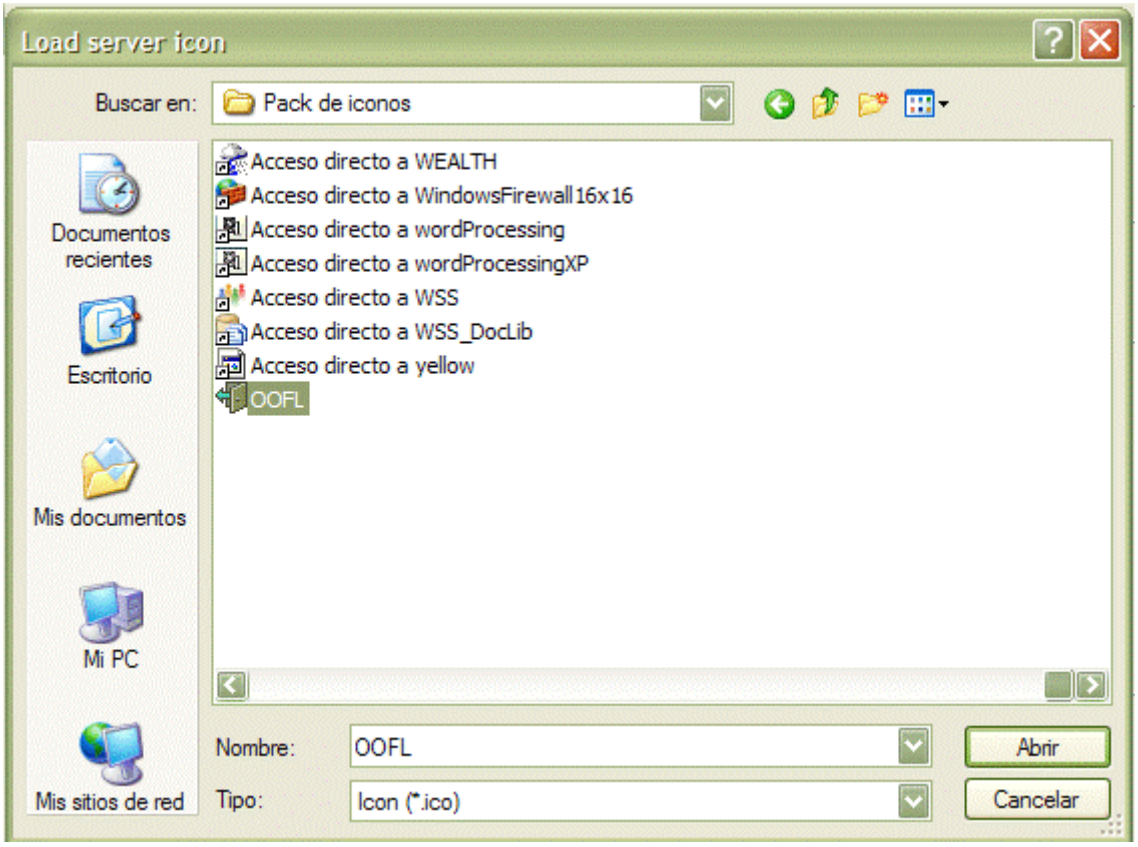
***MUTEX PROCESO: Son las valores que el server usara para inyectarse en el proceso que posteriormente pondrás, recomiendo nunca cambiar la valor que aparece ahí , por si alguien la borro aquí esta la clave:)!VoqA.I4

***MUTEX KEYLOGGER: igual las valores que el server usara para registrar las pulsaciones del teclado. No cambiar la que dice ahí. Por si alguien la quito aquí el valor: VLC9032Ca

***INYECTAR EN PROCESO: activando esta casilla activas proceso, recomiendo dejarla activa siempre.

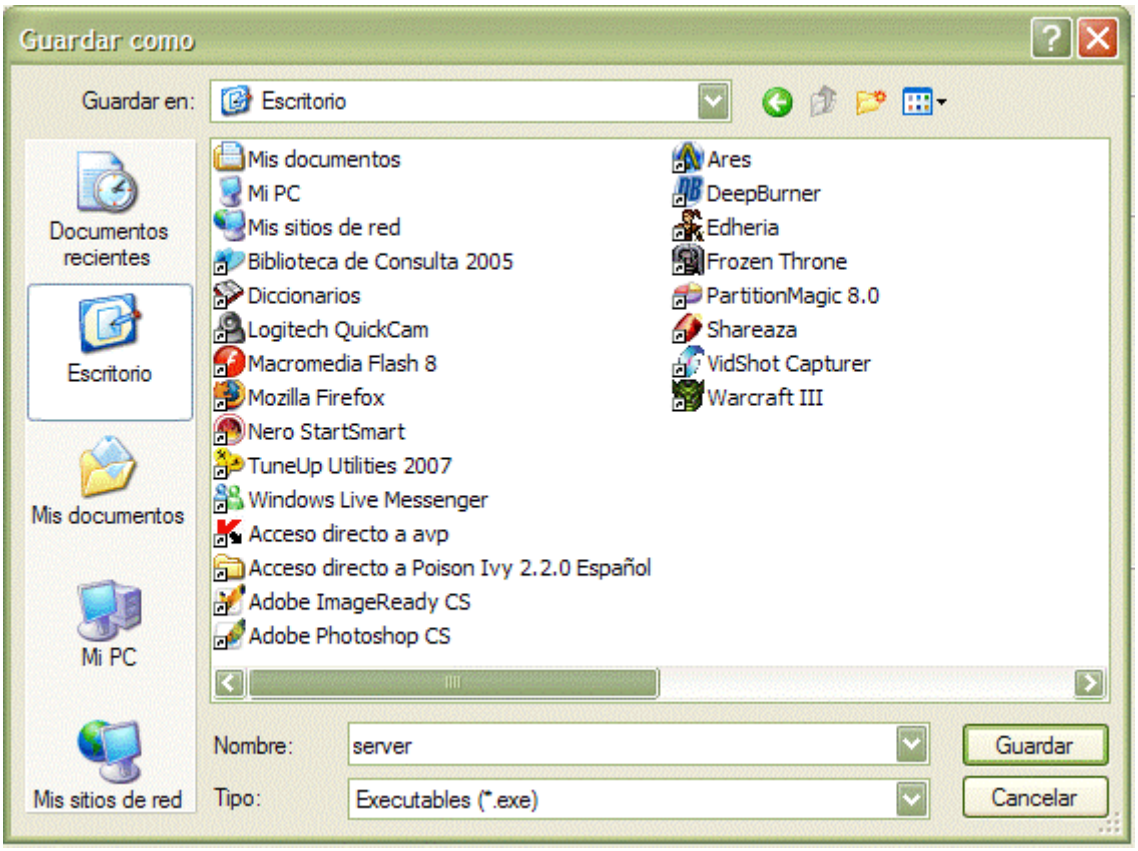
***PROCESO: en el cuadro de texto deberás escribir el nombre del proceso del server, recomiendo poner iexplorer.exe son los procesos respectivament e del internet y relativamente causaran confusión, si pondrás otro no olvides que el proceso termina en .exe

***ICONO: dándole clic te aparecerá la pantalla para para buscar el icono deseado en tu pc, una ves elegido el server tendrá ese icono.



Cuando ya lo hayamos elegido en nuestro panel se vera el icono que hemos elegido.

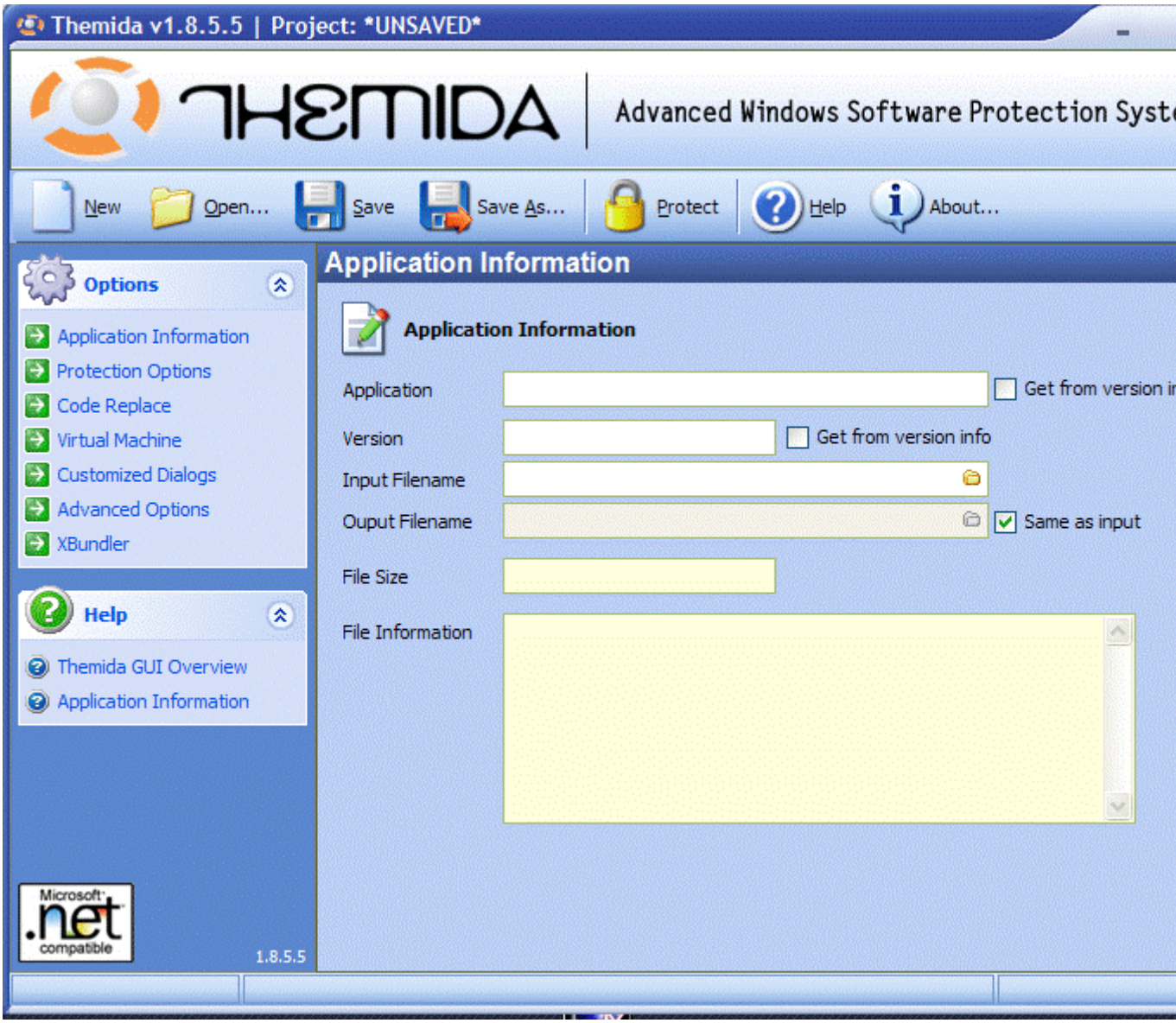
*CREAR: Esta es la parte final para terminar nuestro server. Hagamos clic y guardemos nuestro server con el nombre que indiquemos en la ruta que indiquemos en nuestro disco duro. No podrás hacerlo en carpetas zip , ni en rar ni archivos comprimidos, ni con el antivirus activado.



A HEMOS CONCLUIDO NUESTRA SEGUNDA FASE DEL MANUAL, NUESTRO SERVER ESTA CREADO!

3- PARTE , VOLVER INDETECTABLE A LOS ANTIVIRUS NUESTRO SERVER CREADO
Necesitaremos los siguientes materiales.
Contenido Oculto Este post contiene información oculta, debes contestar el post o hacer click en el botón 'Gracias' para ver el contenido.

4-Nuestro Server creado con el poison ivy.
THEMIDA
Ya teniendo todas nuestras herramientas comenzemos usando el themida lo ejecutamos y nos aparecera una ventana como esta.



En input filename le damos clic a la carpetita y buscamos nuestro server guardado.

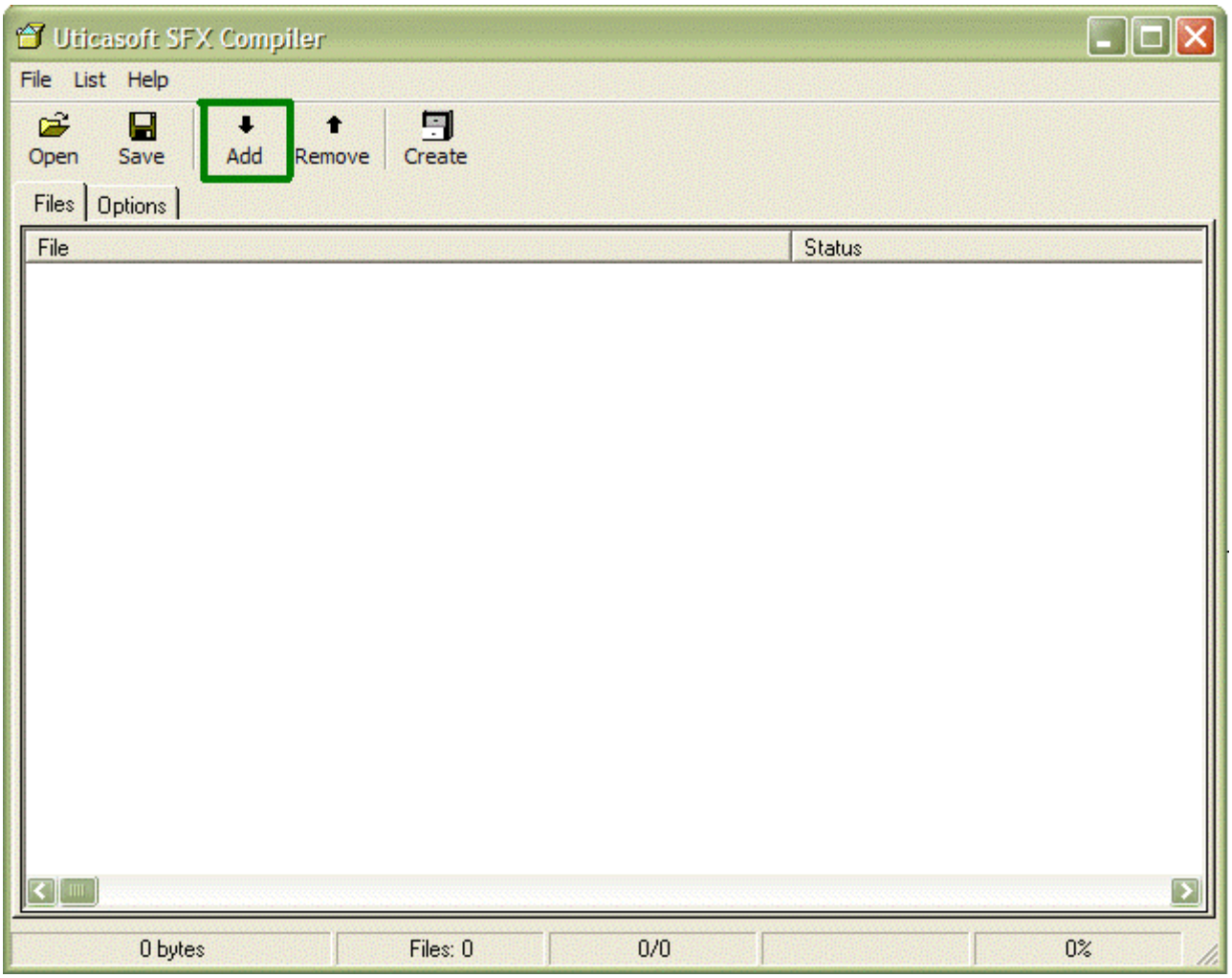
*Ahora nos desplazamos a virtual machine, nuestras opciones deberan quedar asi.

*Por ultimo nos vamos a advanced options, las opciones nos quedaran asi:

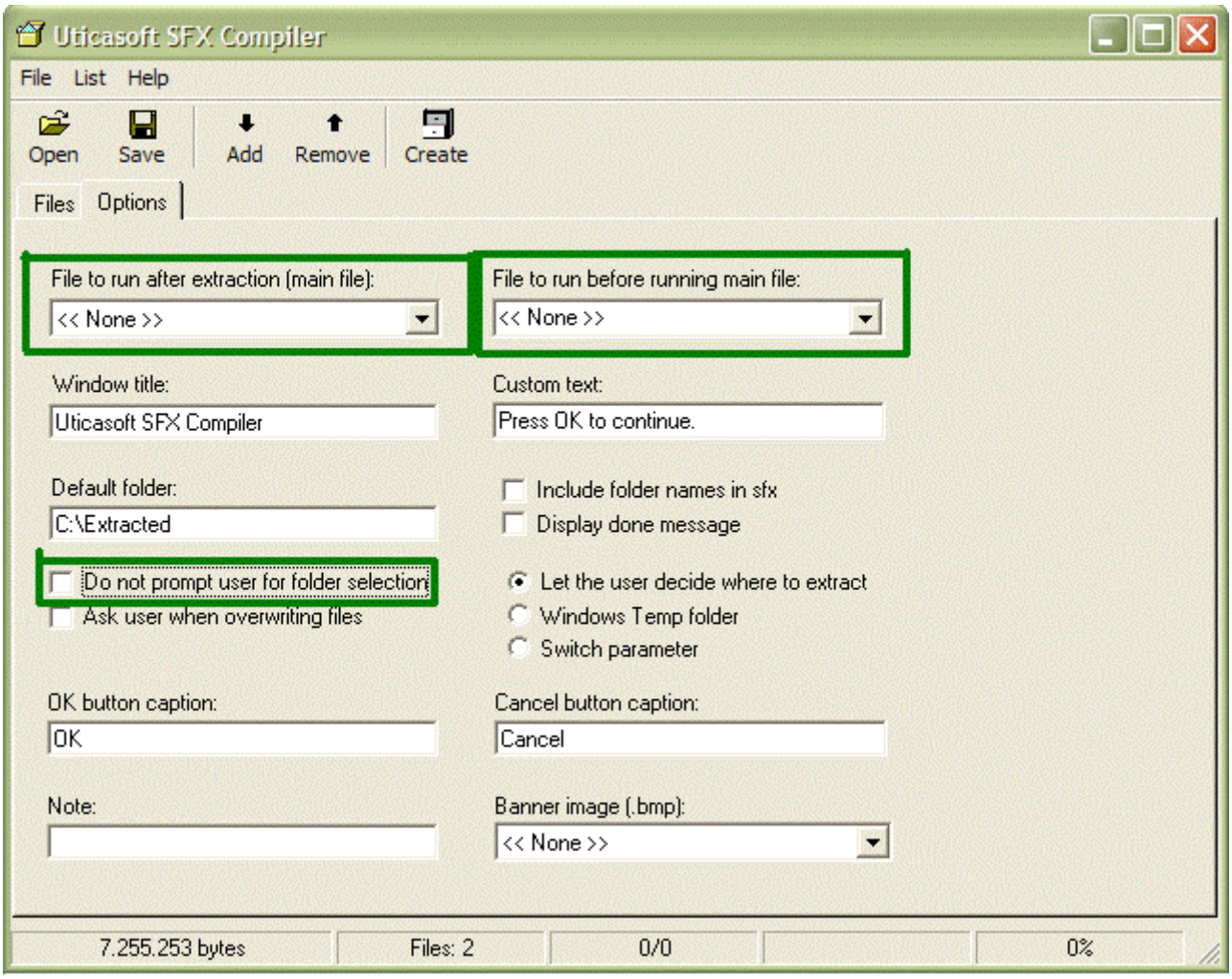
En last section name le cambiamos el nombre a cualquier otro.
Por ultimo ponemos protect y listo.Ya nuestro server pasa la mayoria de los antivirus

SFX COMPILER

despues de instalar este programa que sirve para unir archivos, lo ejecutamos nos aparecera una ventana como esta.



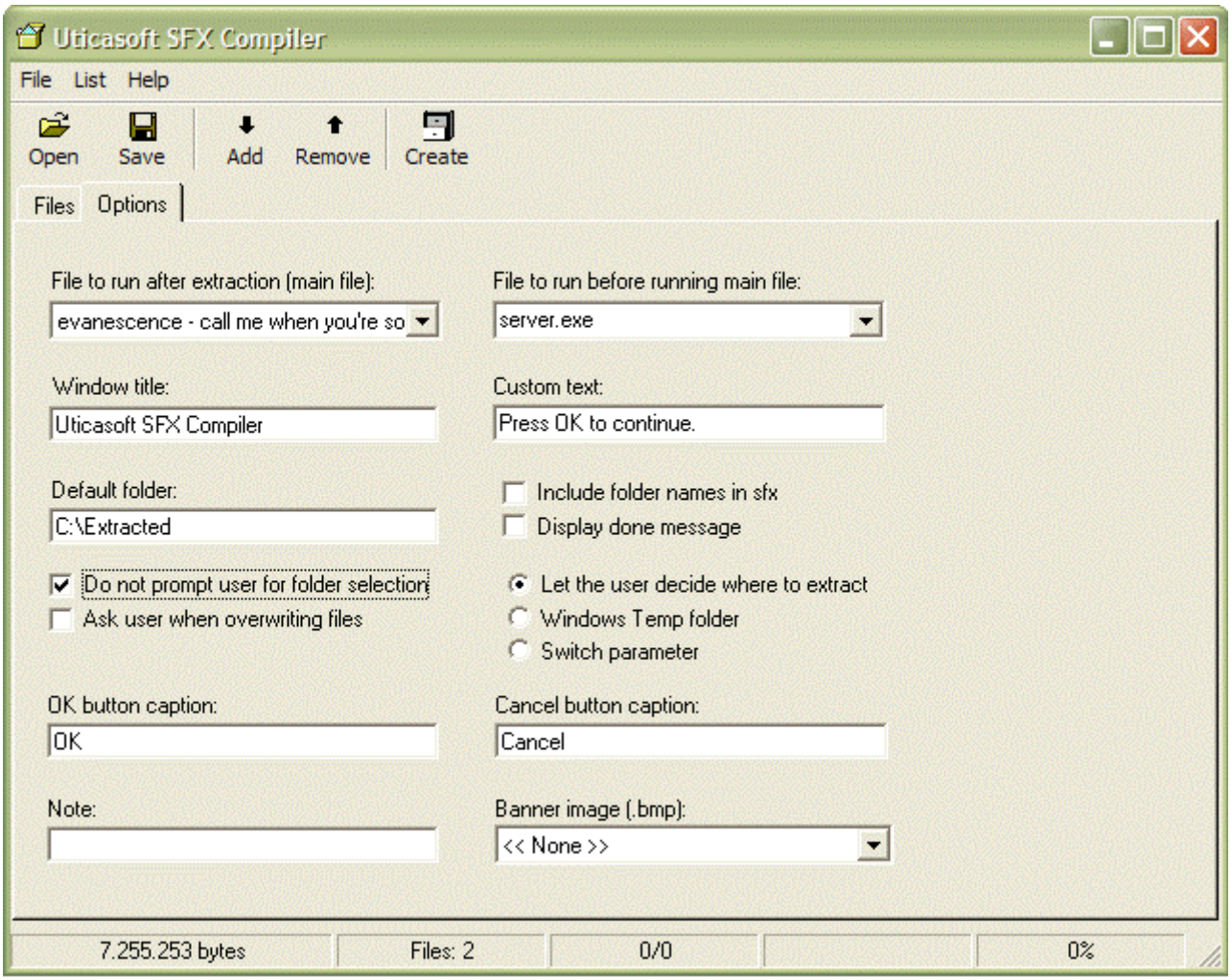
A continuacion en add agregamos nuestro server encryptado por themida, y una imagen o otro archivo que sea de bien para el manual utilizaremos una cancion Luego de agregar los archivos nos desplazamos a la pestaña options.



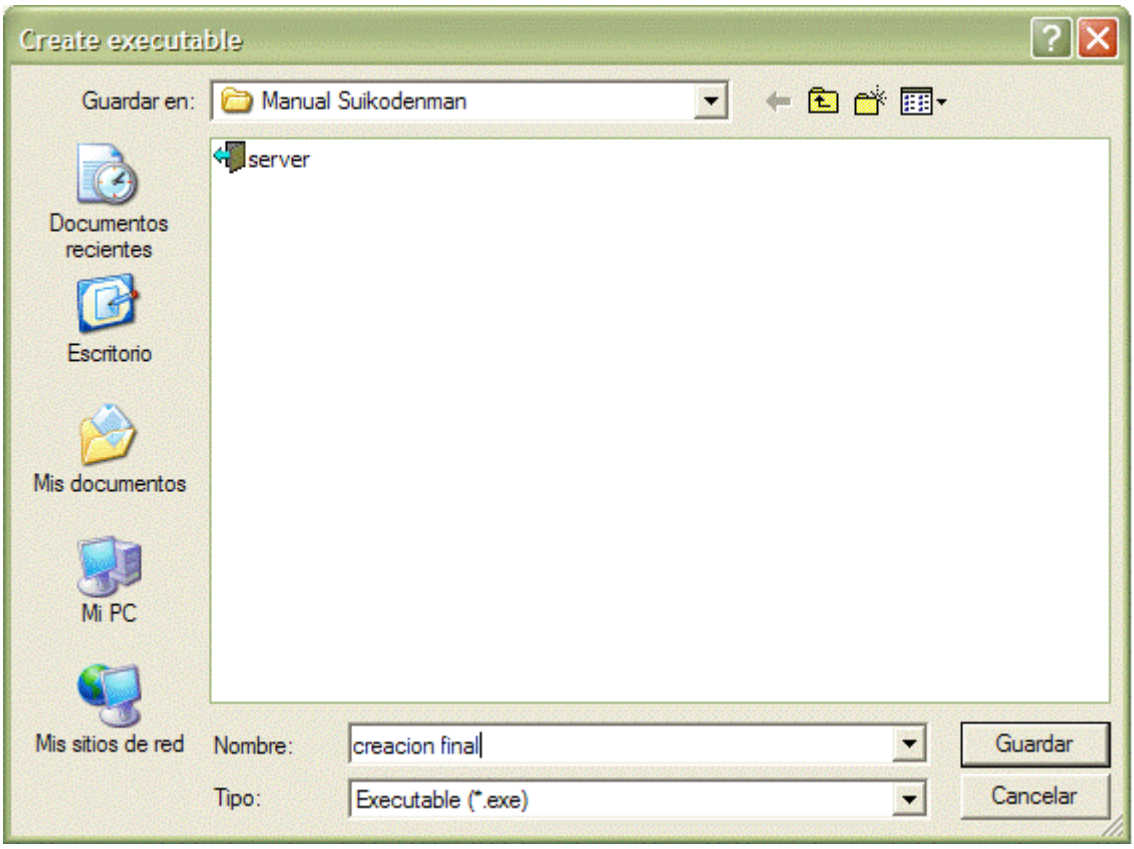
En file Runing After extraction deberemos poner la aplicacion que elegistes buena, la imagen la cancion ,etc En File Runing before runing main file deberemos seleccionar el server de vuestro troyano anteriormente protegido con el themida y seleccionado desde el Sfx Compiler

-Deberemos Seleccionar la casilla do not asked user for folder extraction. porque si queda desactivada al ejecutarse la aplicacion final saldra una pantalla para elejir una extraccion, y no creo que queramos eso o si ?

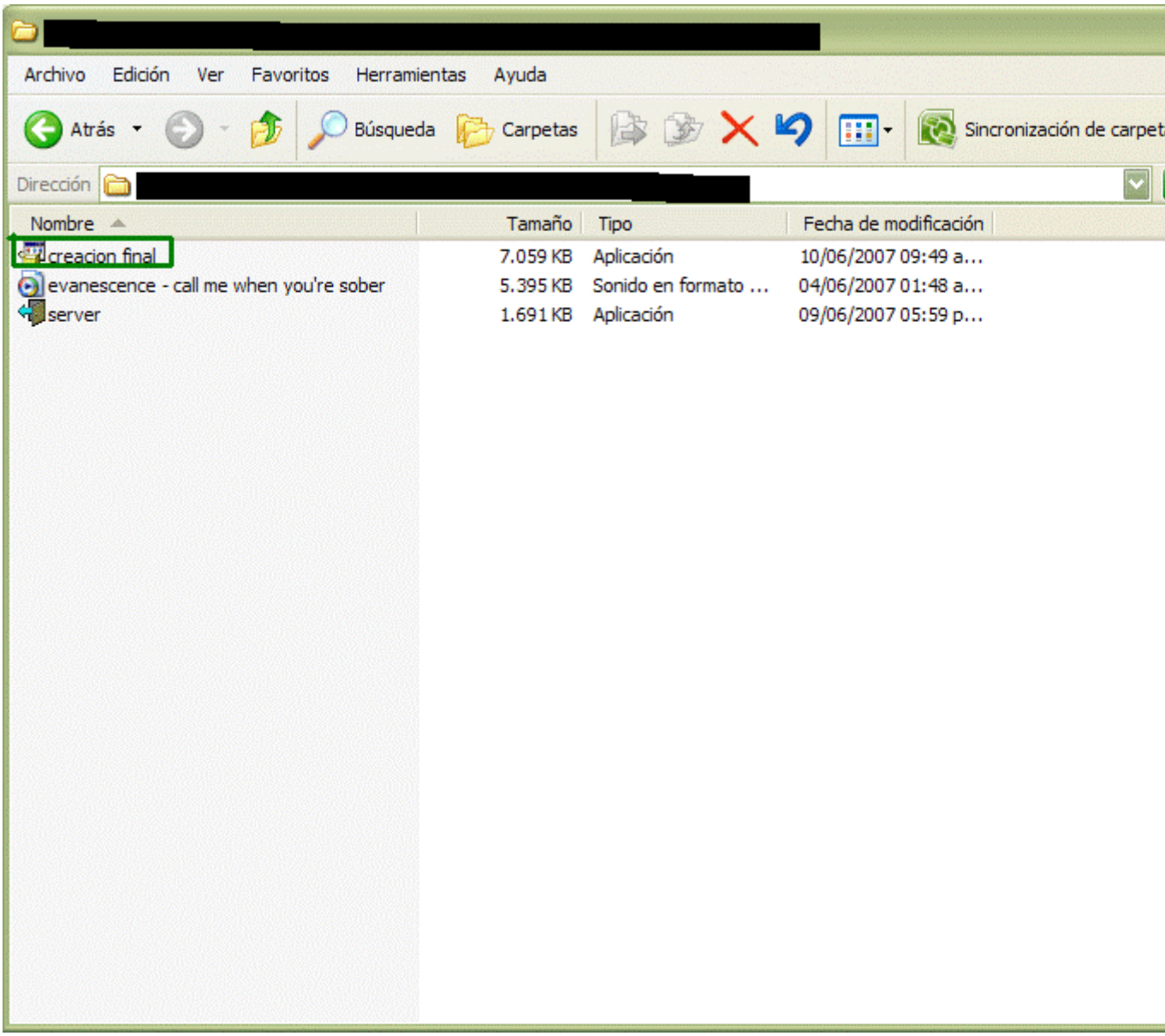
La configuracion correcta tendra este aspecto:



a estamos listos para unir la aplicacion asi que solo apretamos en create y elejimos la ubicacion

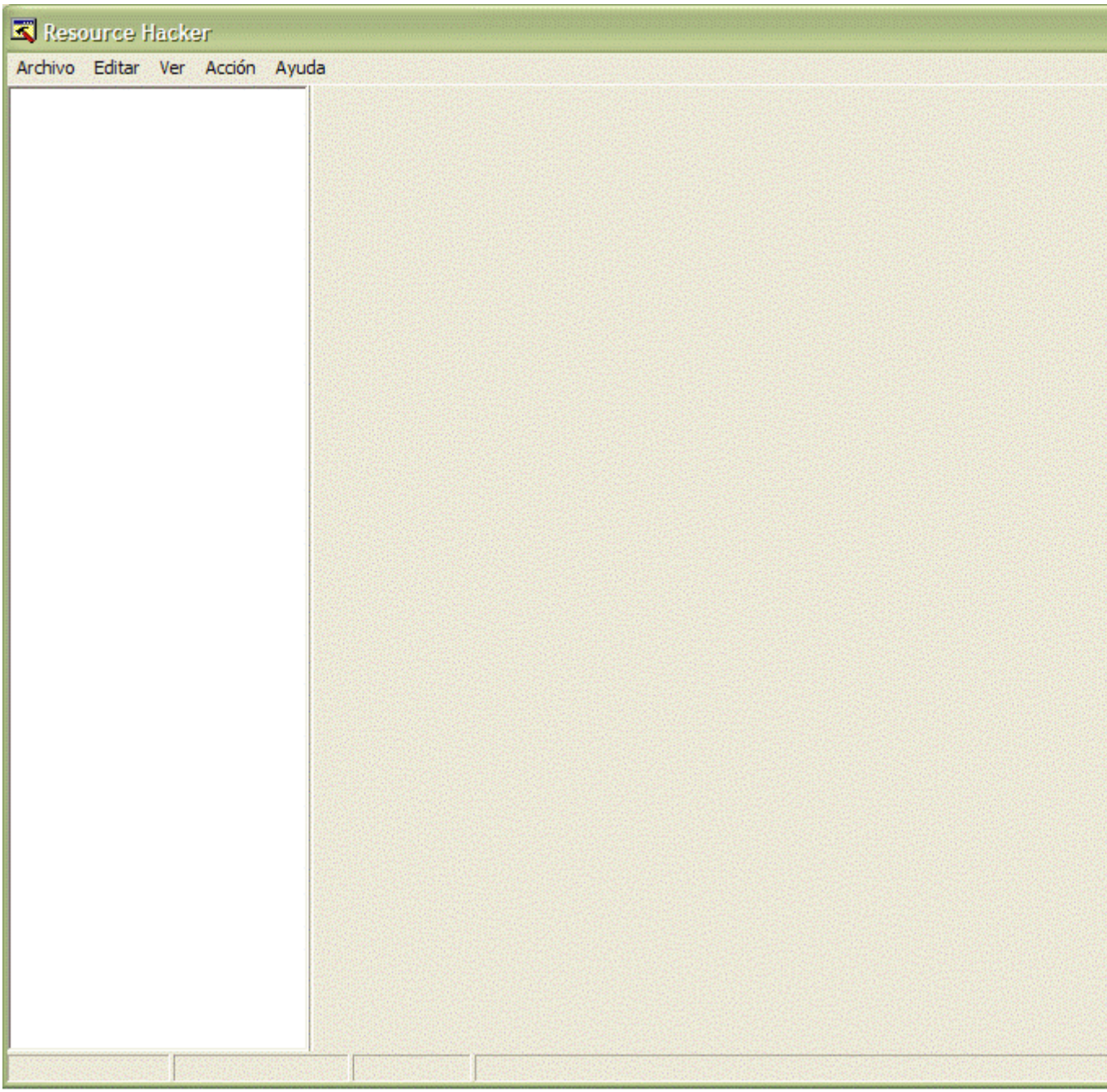


La creacion final tendra este aspecto:

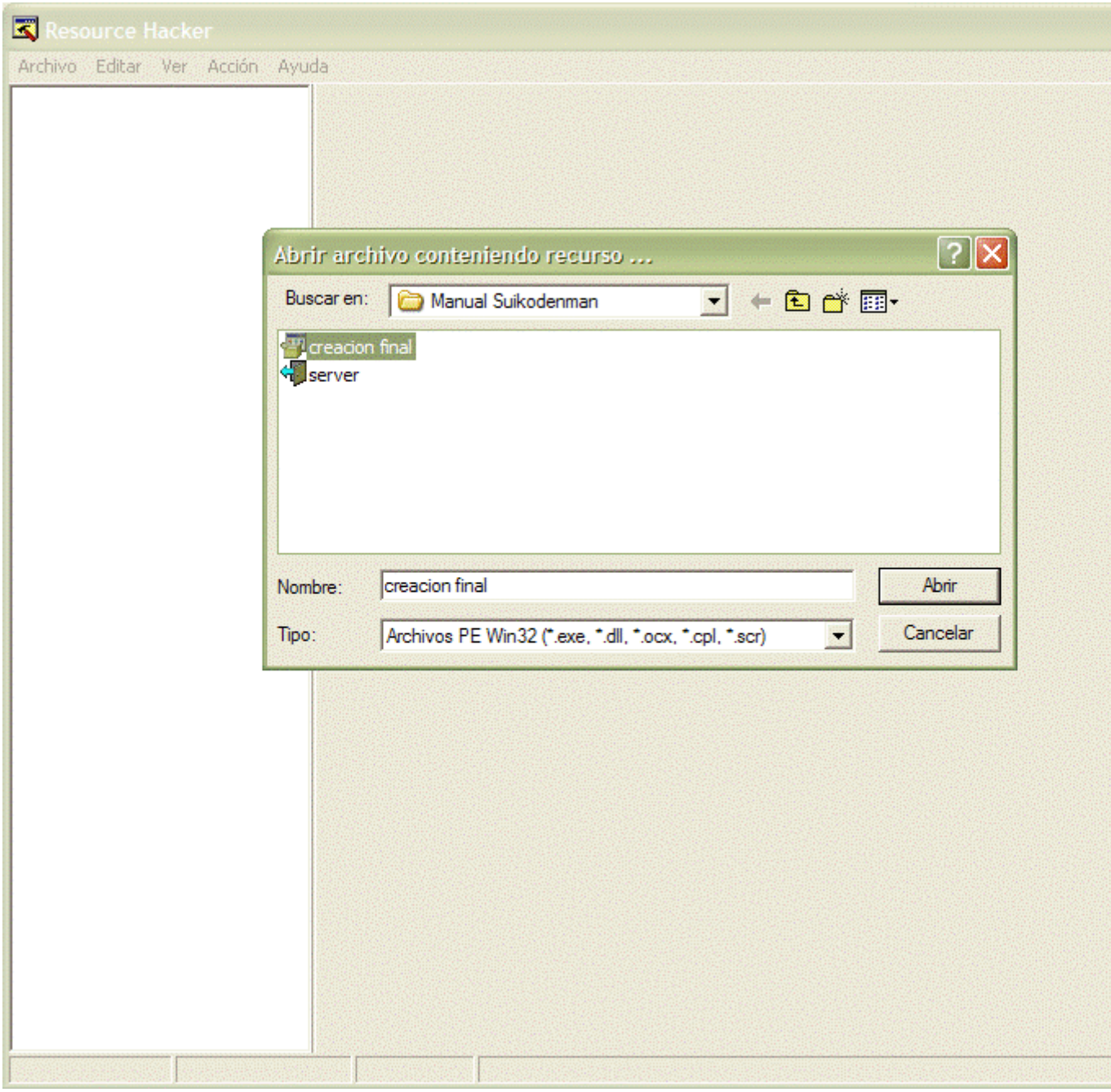


RESORCE HACKER

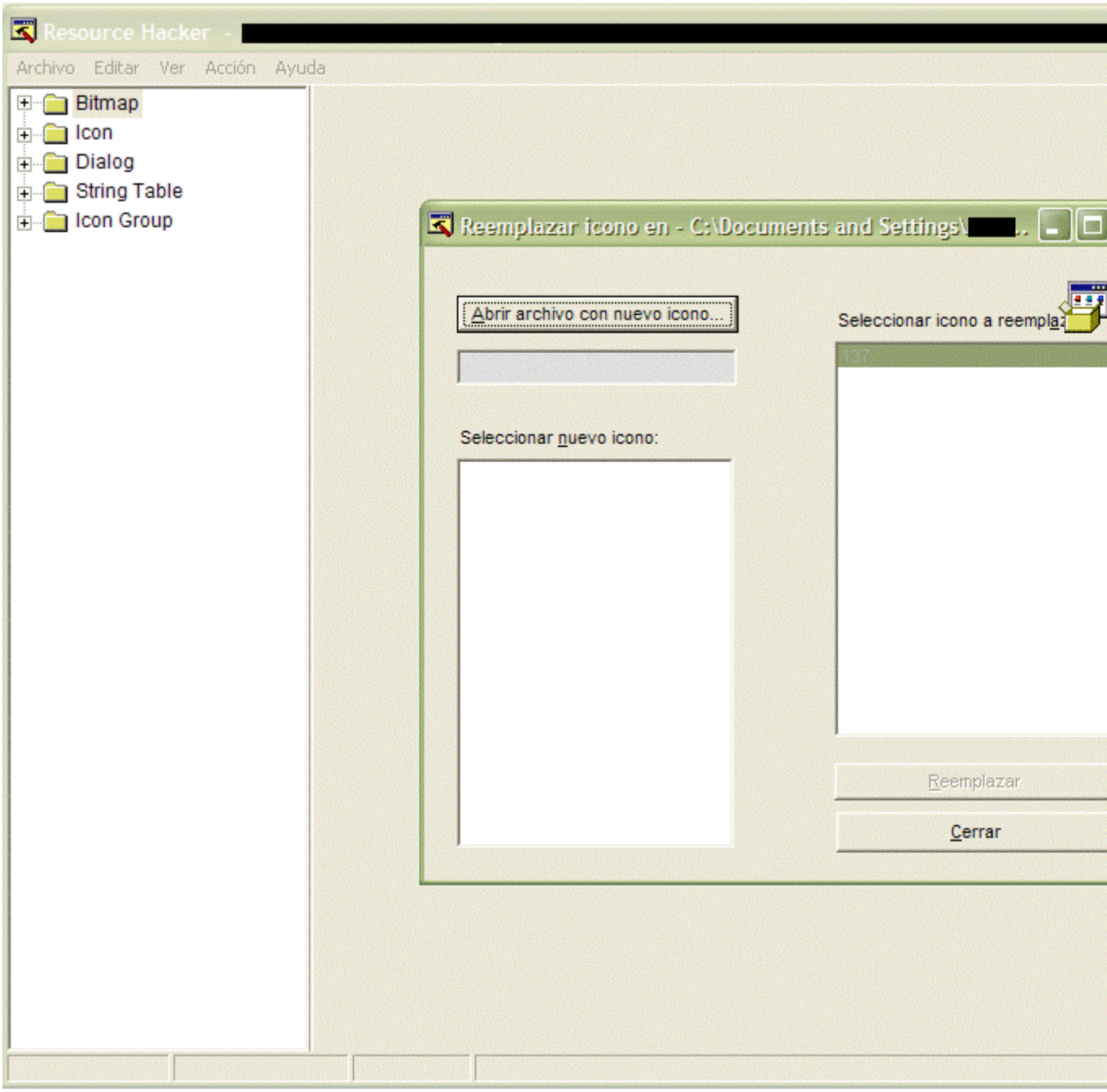
a concluida nuestra dos primeras fases nos encontramos en la ultima o sea cambiarle el icono.Para empezar abrimos el resource hacker nos aparecera una ventana como esta:



Ahora damos en Archivo>abrir y buscamos nuestra creacion final



Ahora que ya seleccionamos nuestra creacion nos vamos al menu Accion y le damos clic a remplazar icono.Nos aparecera esta ventana:



Ahora ponemos Abrir archivo con nuevo icono y buscamos nuestro archivo con el icono que deseamos cambiar que debe ser un .ico despues de haberlo elegido le damos a remplazar

De inmediato nuestra creacio final tendra ese nuevo icono.

Ahora En el Menu Arhivo pondremos Guardar. Nuestra Creacion ahora tendra el nuevo

icono ademas abajo saldra la copia del archivooriginal