INFORME DE LABORATORIO 01

INDIRA JOHANA FLÓREZ CÓRDOBA

Estudiante IX

UNIVERSIDAD TECNOLOGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERIA

INGENIERIA DE TELECOMUNICACIONES E INFORMÁTICA

QUIBDÓ – CHOCÓ

2025

INFORME DE LABORATORIO 01

INDIRA JOHANA FLÓREZ CÓRDOBA

Estudiante IX

RAFAEL SANDOVAL MORALES

Docente

UNIVERSIDAD TECNOLOGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERIA

INGENIERIA DE TELECOMUNICACIONES E INFORMÁTICA

QUIBDÓ – CHOCÓ

2025

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

1. INTRODUCCIÓN

El presente informe documenta el proceso de investigación y experimentación en técnicas de ofuscación de archivos y explotación de vulnerabilidades, realizado en un entorno controlado. En la primera fase, se implementó el software Camouflage en Windows XP para ocultar archivos sensibles dentro de archivos comunes como imágenes JPEG, documentos PDF y ejecutables. En la segunda fase, se identificó y explotó la vulnerabilidad BadBlue 2.72, utilizando Kali Linux para obtener acceso remoto no autorizado al sistema Windows XP. Este trabajo tiene como propósito académico fortalecer los conocimientos en seguridad ofensiva y defensiva, específicamente en técnicas de ocultamiento de información y explotación de servicios vulnerables.

2. OBJETIVOS

2.1 Objetivo general

Implementar técnicas de ofuscación de archivos y explotar la vulnerabilidad de BadBlue 2.72.

2.2 Objetivos específicos

- Instalar y configurar el software Camouflage para el ocultamiento de archivos en diferentes formatos.
- Ocultar archivos PDF, documentos Word, archivos de audio e imágenes JPEG.
- Identificar la vulnerabilidad de BadBlue 2.72 mediante escaneo de puertos y servicios.
- Ejecutar el exploit correspondiente para obtener una shell en el sistema Windows XP vulnerable.
- Realizar actividades de post-explotación para enumerar información del sistema comprometido.

3. ALCANCE

El alcance de este informe se limita al entorno académico de laboratorio, utilizando máquinas virtuales con Windows XP y Kali Linux en VirtualBox. Las técnicas de ofuscación se aplicaron únicamente a archivos de prueba, mientras que la explotación de BadBlue se realizó contra una instancia local del servicio. No se incluyen técnicas de evasión de antivirus, persistencia en el sistema comprometido ni explotación de vulnerabilidades adicionales. El informe se centra en demostrar los conceptos fundamentales de ofuscación de archivos y explotación de servicios vulnerables, sin incluir aplicaciones maliciosas en entornos productivos.

4. CAPITULO 1 – OCULTAR FICHEROS EN WINDOWS XP CON CAMOUFLAGE

4.1 Crear carpeta en el escritorio de tu PC físico

Esta imagen muestra el escritorio del sistema operativo anfitrión (el PC físico del usuario), donde se ha creado una nueva carpeta. Esta acción es el paso inicial para preparar los archivos que posteriormente serán ocultados utilizando la herramienta Camouflage dentro de Windows XP. La carpeta servirá como contenedor de los datos que se pretende camuflar.

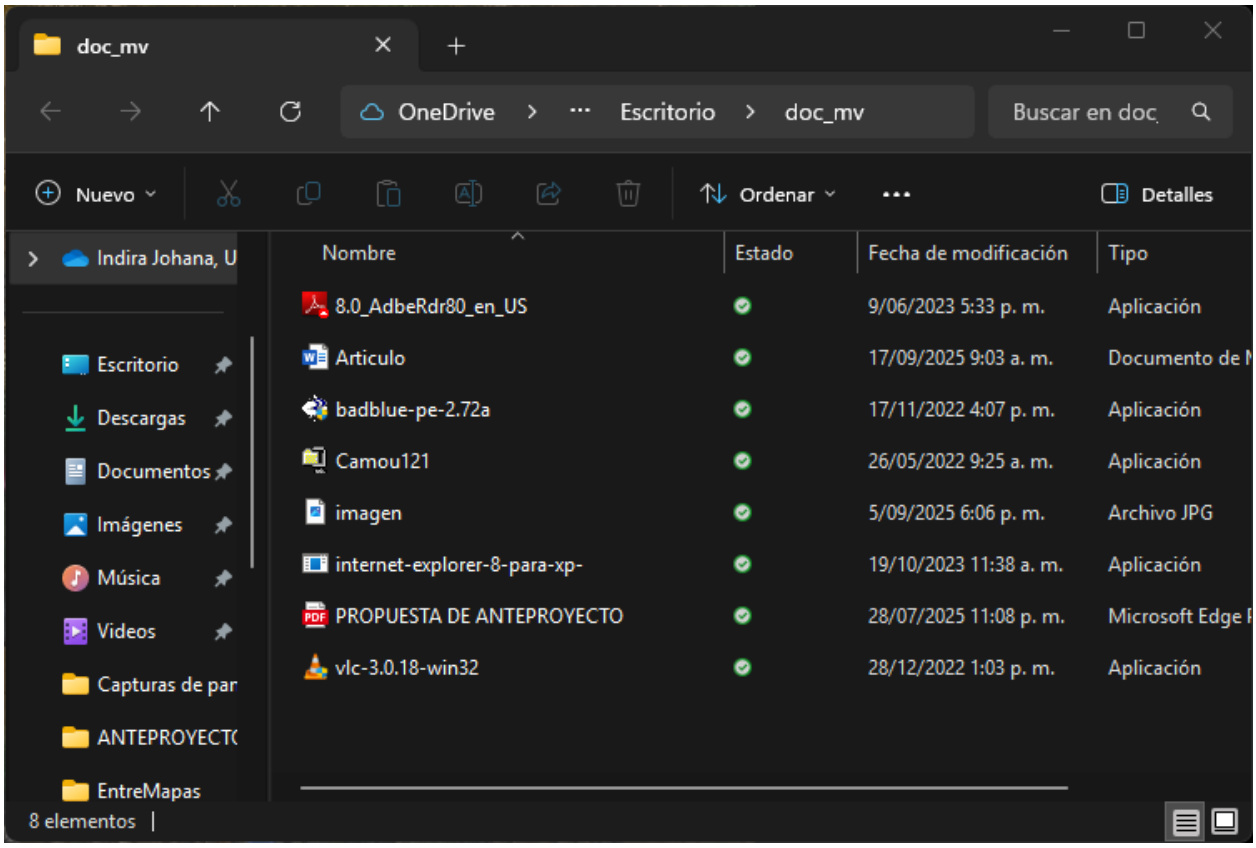

Ilustración 1. Carpeta en el escritorio del PC físico

4.2 Inserción del CD de Complementos para Invitado de VirtualBox

En el menú de **"Dispositivos"** de la máquina virtual Windows XP en VirtualBox, se debe seleccionar la opción **"Insertar imagen de CD de los complementos del Invitado"**, un paso

preliminar para mejorar la integración entre el sistema anfitrión y el virtualizado, facilitando el intercambio de archivos.

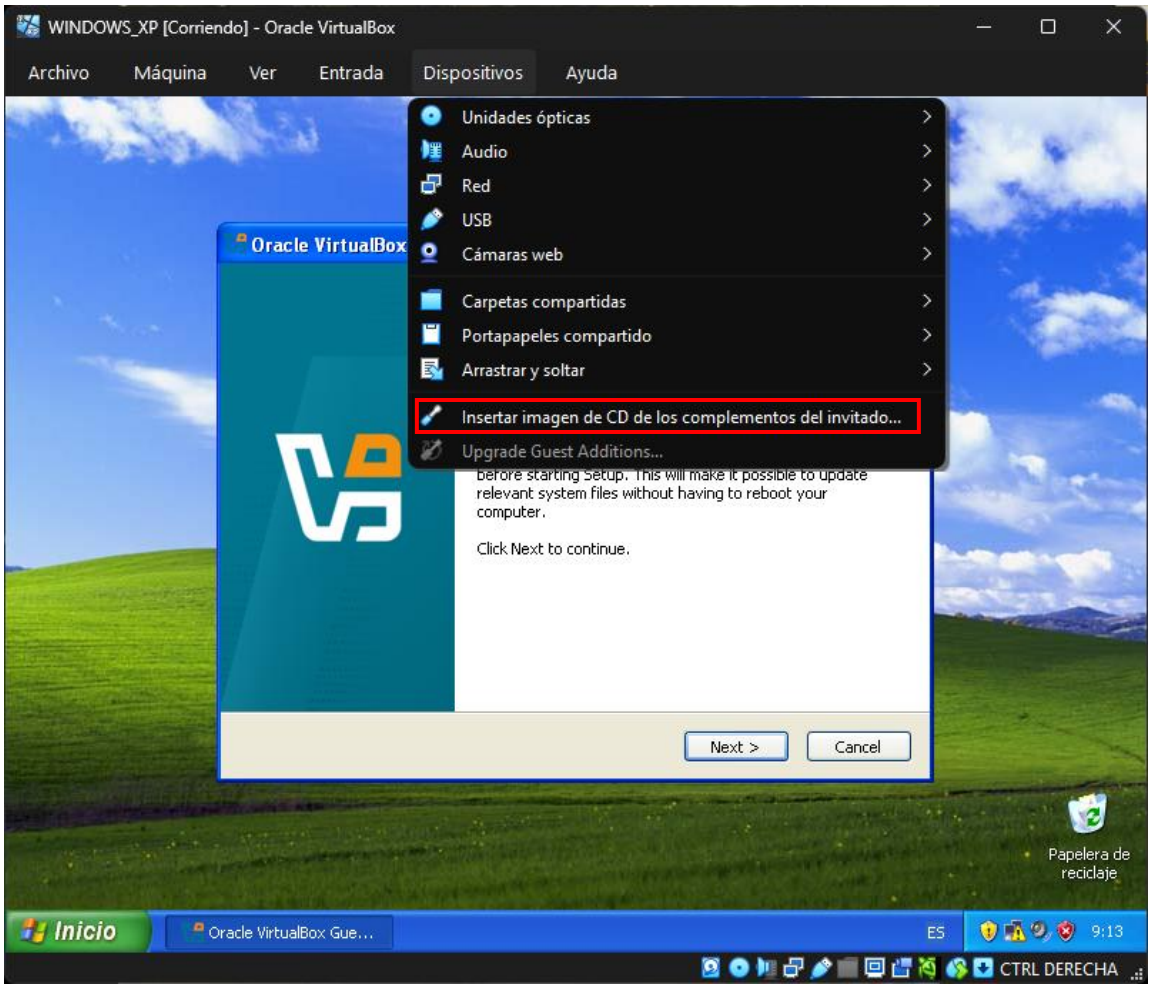

Ilustración 2. Inserción del CD de Complementos para Invitado de VirtualBox

4.3 Elección de la carpeta destino para los Complementos

La ventana muestra la etapa "Elegir ubicación de instalación", donde se confirma la carpeta destino predeterminada para la instalación de los controladores y herramientas esenciales para la integración del sistema.

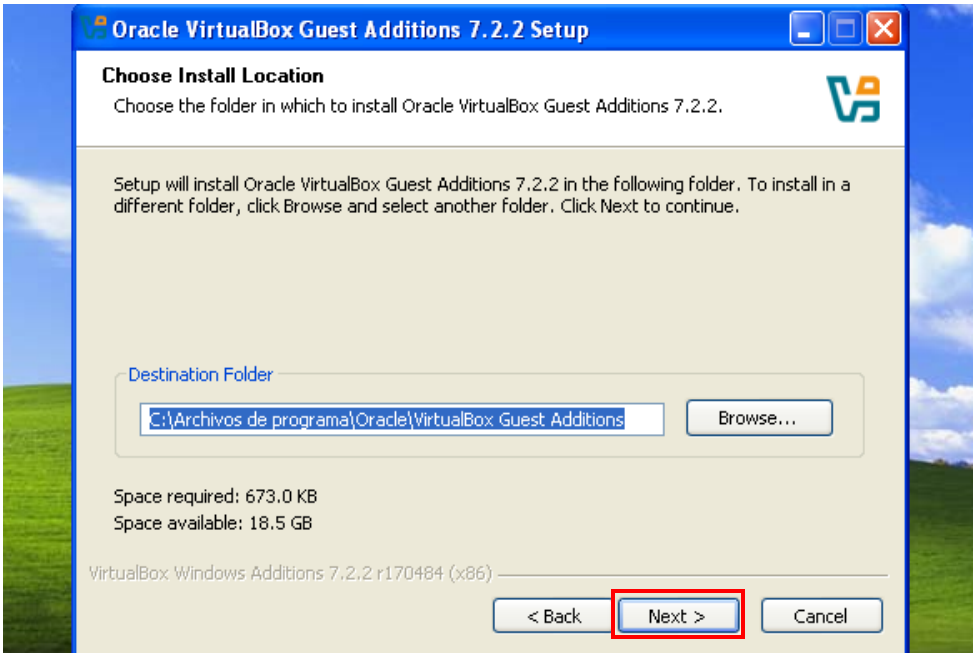

Ilustración 3. Elección de la carpeta destino para los Complementos

Ahora se muestra la etapa "Elegir componentes". Aquí se pueden seleccionar las características a instalar, como las "Entradas en el menú Inicio". Se procede con la instalación estándar, marcando todas las opciones recomendadas.

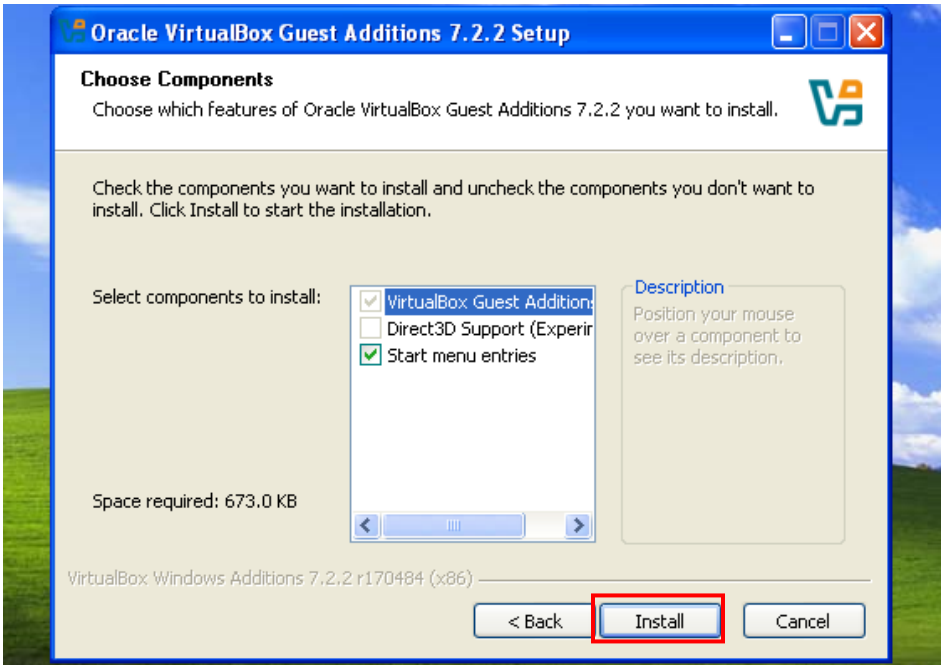

Ilustración 4. Selección de componentes de los Complementos para Invitado

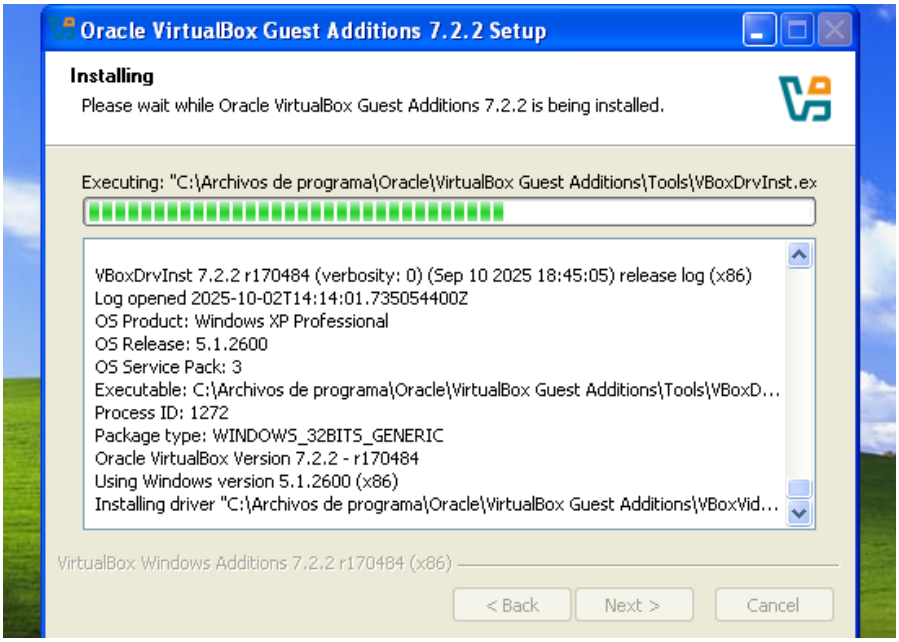

Ilustración 5. Instalación de Guest Additions

Muestra la ventana final de la instalación de los Complementos para Invitado. El sistema solicita reiniciar el equipo para completar la instalación y cargar los nuevos controladores. Seleccionamos la opción **"Reboot now"** para proceder inmediatamente con el reinicio de la máquina virtual Windows XP.

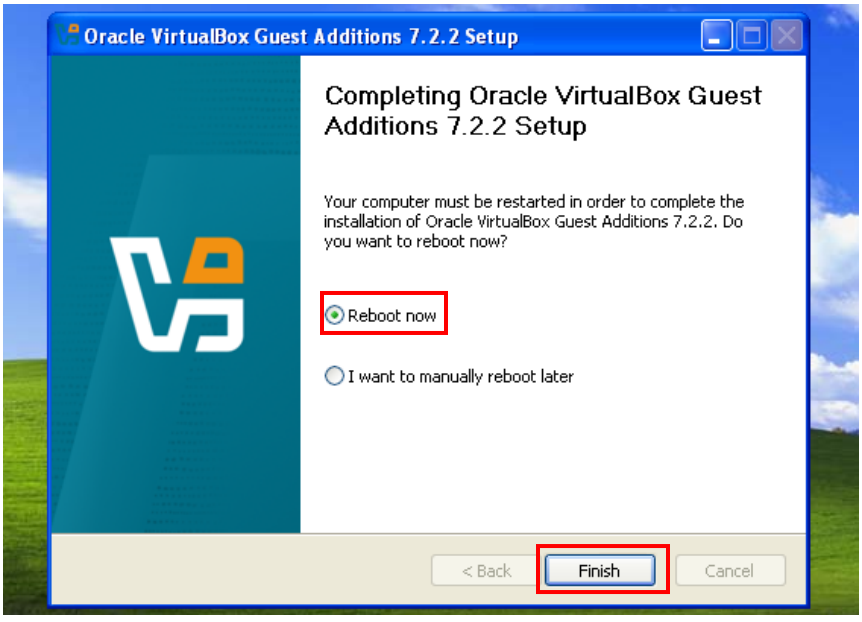

Ilustración 6. Finalización de la instalación y solicitud de reinicio del sistema

4.4 Acceder a Carpetas compartidas para vincular la carpeta del anfitrión

Luego del reinicio accedemos a los archivos del sistema anfitrión desde la máquina virtual. Para ello, seleccionamos **"Dispositivos"** de la ventada de Windows XP, después la opción **"Carpetas compartidas"** y por último en **“Preferencias de carpetas compartidas”.** Este paso es crucial para agregar y compartir la carpeta específica que se creó previamente en el PC anfitrión, permitiendo que Windows XP dentro de la máquina virtual pueda acceder a los archivos y programas almacenados en ella.

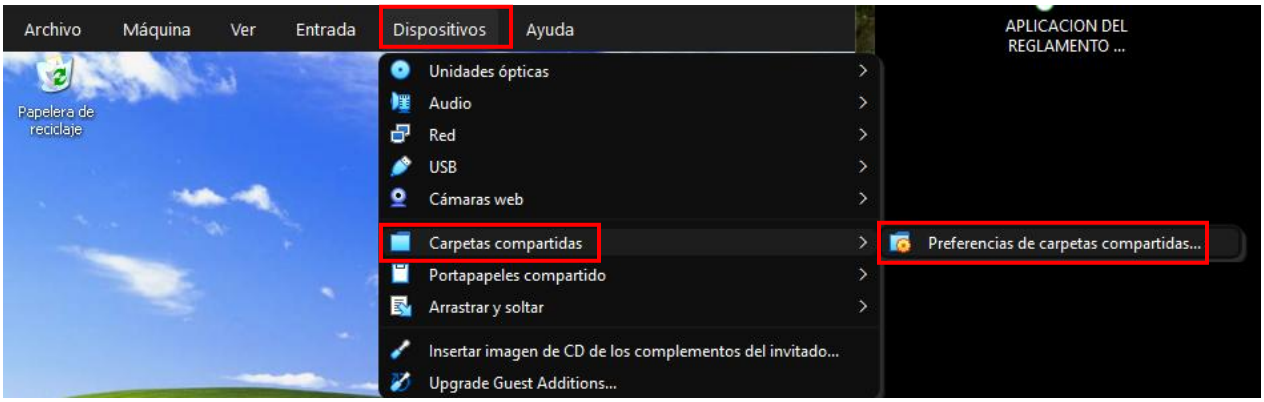

Ilustración 7. Acceso a la configuración de Carpetas Compartidas para vincular la carpeta del anfitrión

Posteriormente le damos clic en el icono que tiene un más.

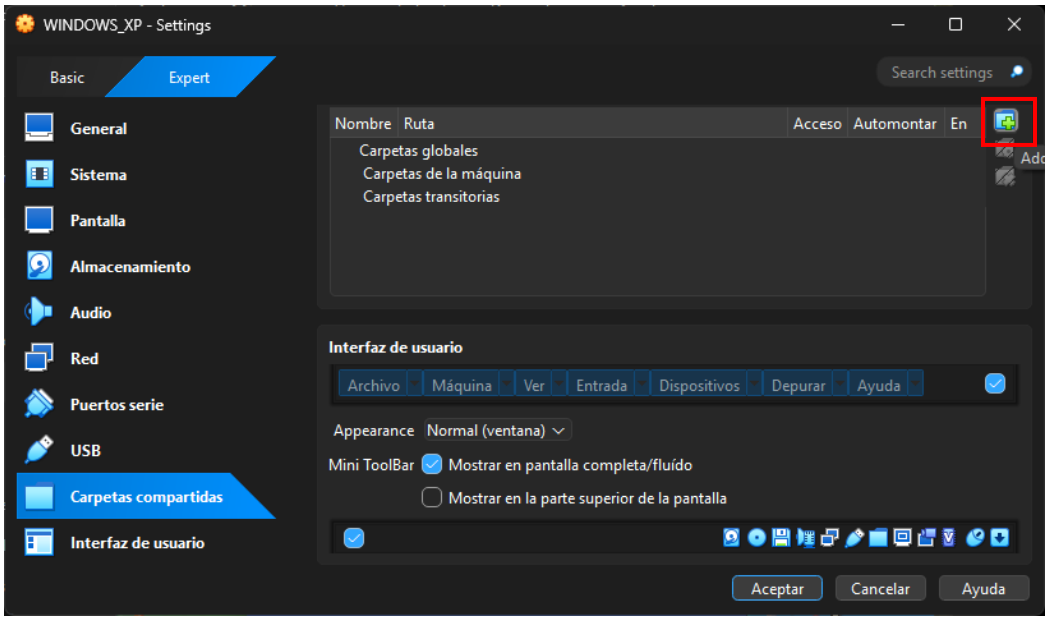

Ilustración 8. Añadir la carpeta del anfitrión

En la nueva ventana seleccionar la carpeta que deseamos compartir.

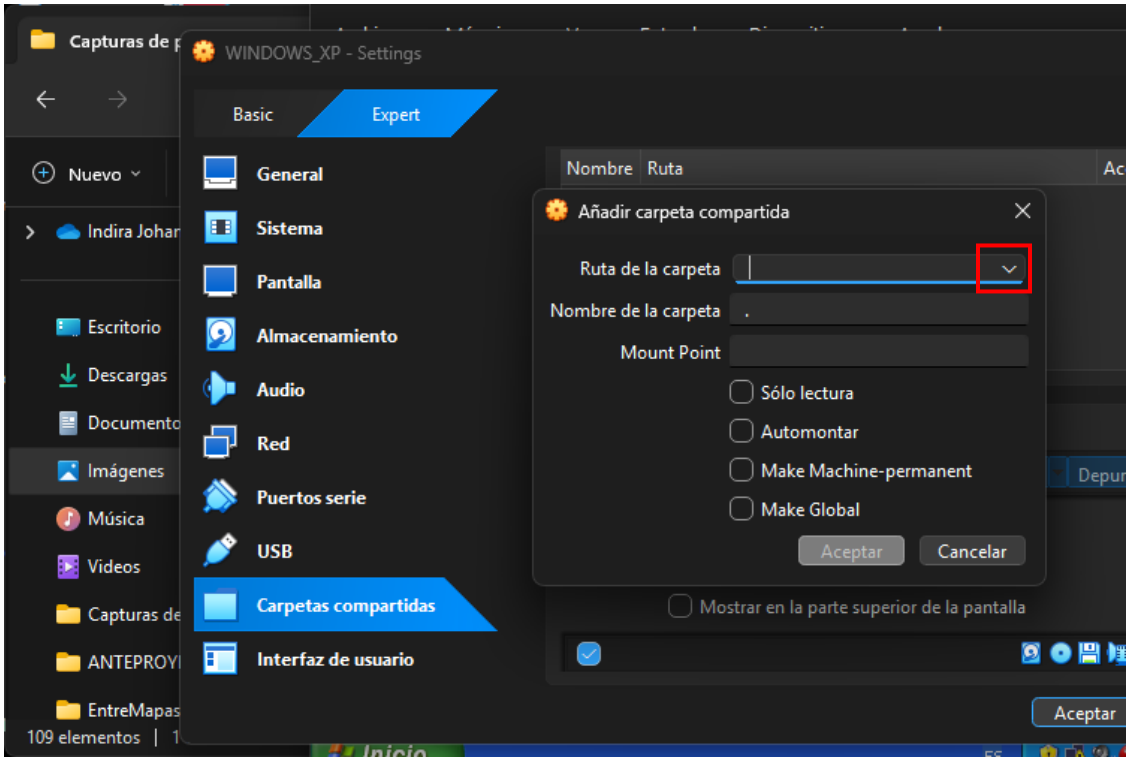

Ilustración 9. Selección de la carpeta del anfitrión para compartir

En este caso, se identifica una carpeta en el Escritorio llamada "doc_mv" que contiene los archivos. También activamos las opciones **“Automontar”** y **“Make Machine-permanent”.**

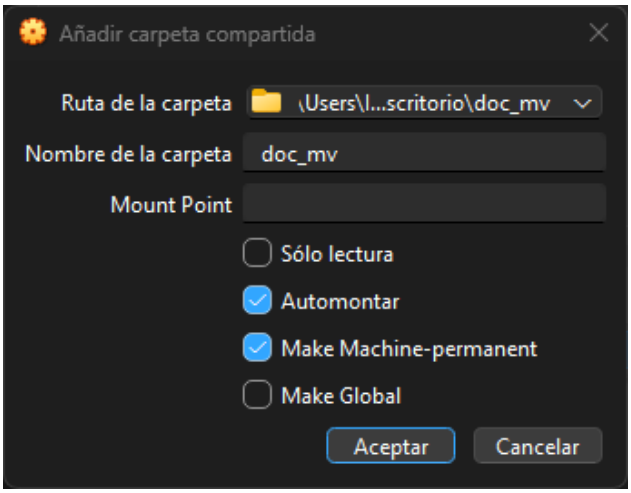

Ilustración 10. Selección de la carpeta del anfitrión para compartir

4.5 Menú Inicio de Windows XP

Hacemos clic en el Menú Inicio de Windows XP y luego en **"Mi PC"** para observar una nueva unidad de red identificada como **"doc_mv en 'VBoxSvr' (Z:)"**, confirmando que el recurso compartido se ha montado correctamente.

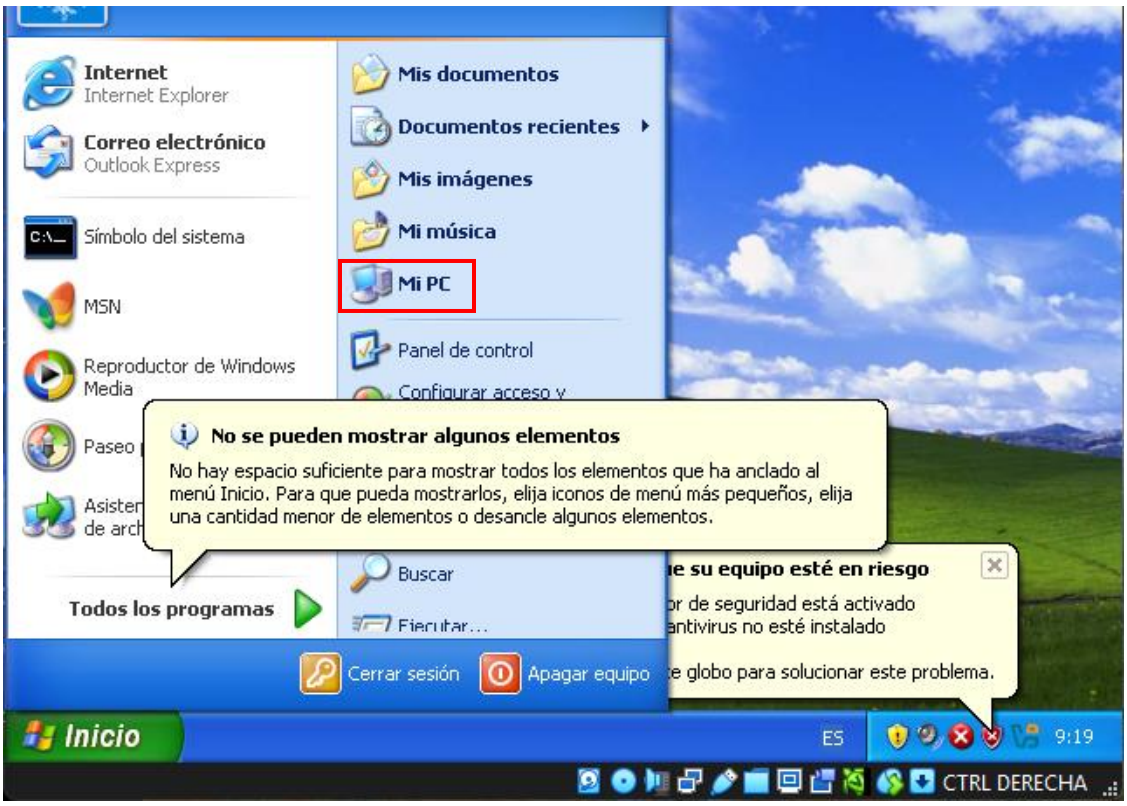

Ilustración 11. Menú Inicio de Windows XP

4.6 Visualización de la unidad de red en Mi PC

Al abrir **"Mi PC"** en Windows XP, se confirma la presencia de la unidad de red **"doc_mv en 'VBoxSvr' (Z:)"** junto a las unidades locales y el CD de VirtualBox Guest Additions. Esto verifica que el sistema reconoce la carpeta compartida.

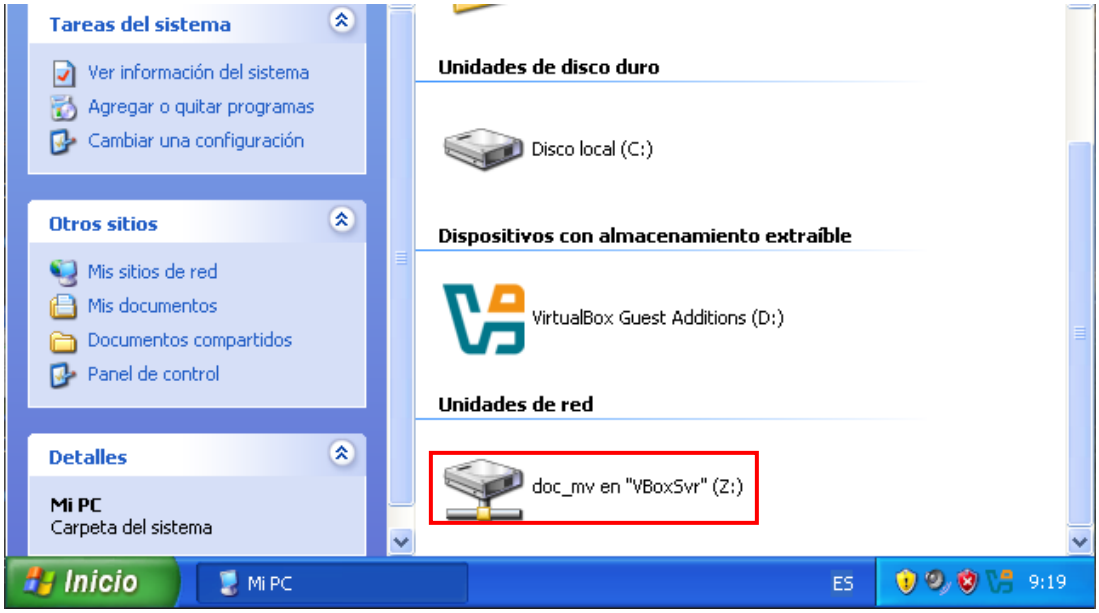

Ilustración 12. Visualización de la unidad de red en Mi PC

Se accede a la unidad Z: (carpeta compartida) y se visualiza su contenido.

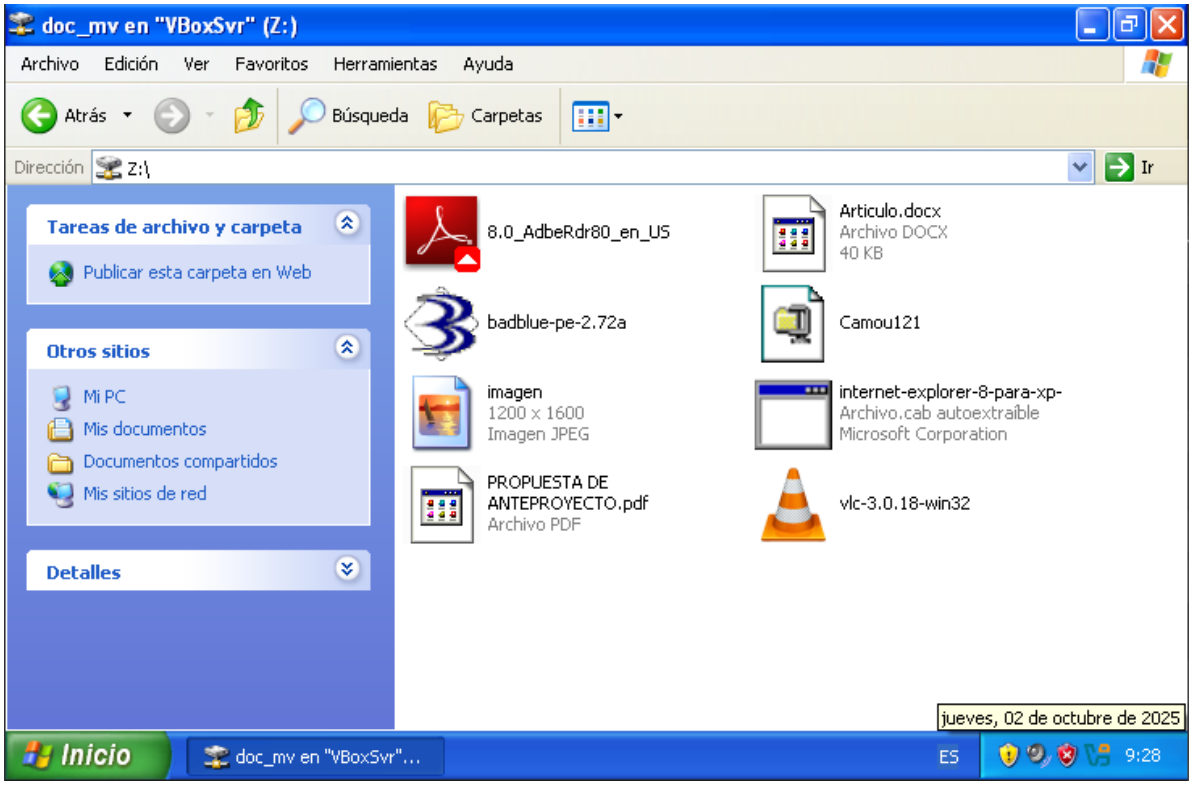

Ilustración 13. Contenido de la carpeta compartida desde la máquina virtual

Hacemos clic derecho sobre uno de los archivos dentro de la carpeta compartida (Z:) y le damos clic en "Copiar".

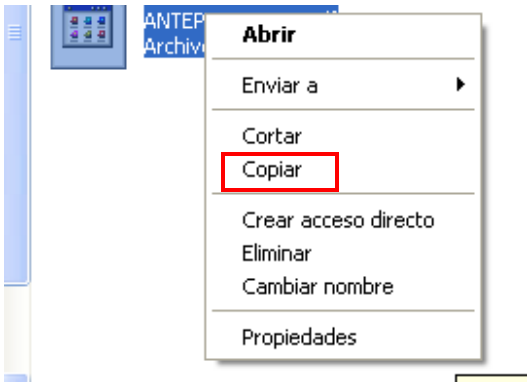

Ilustración 14. Copiar archivos de la carpeta compartida

Luego lo pegamos en el escritorio de Windows XP. (Hacemos eso con todos los archivos que están en la carpeta compartida).

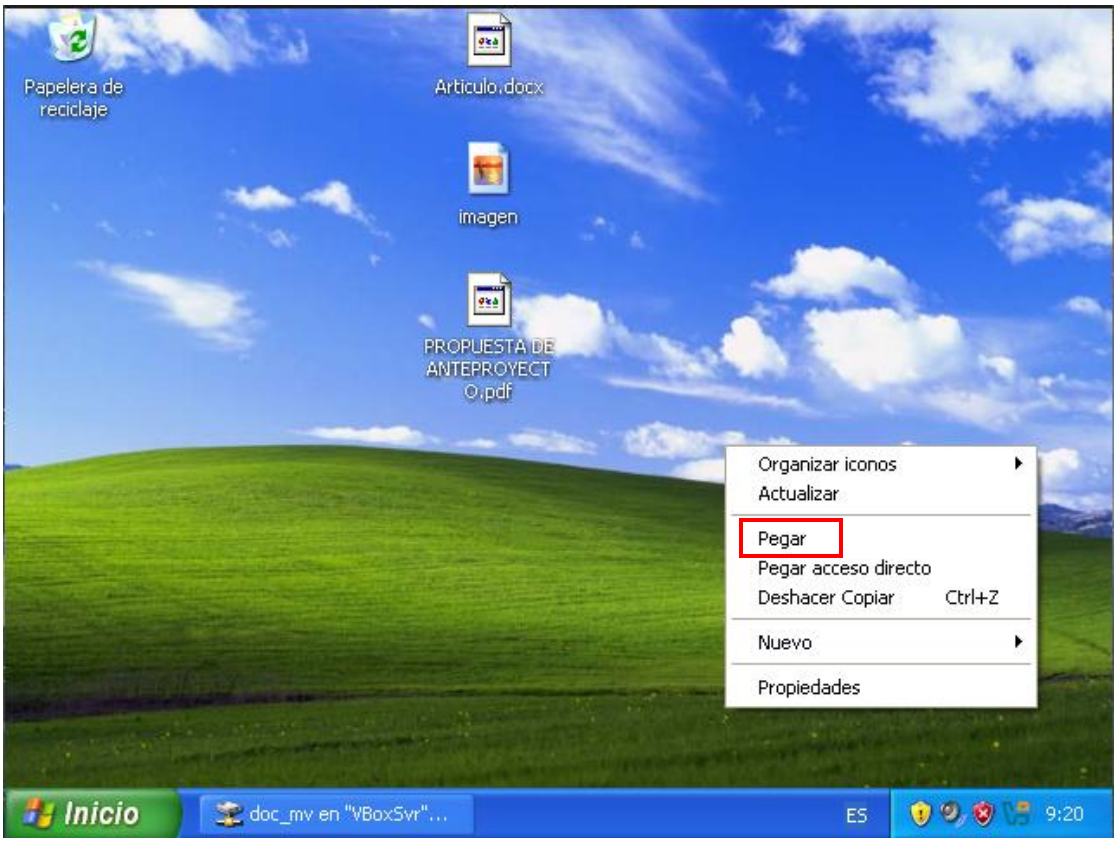

Ilustración 15. Copiar archivos de la carpeta compartida

Otra forma de pegar los archivos al escritorio también es arrastrando los archivos al escritorio con clic sostenido.

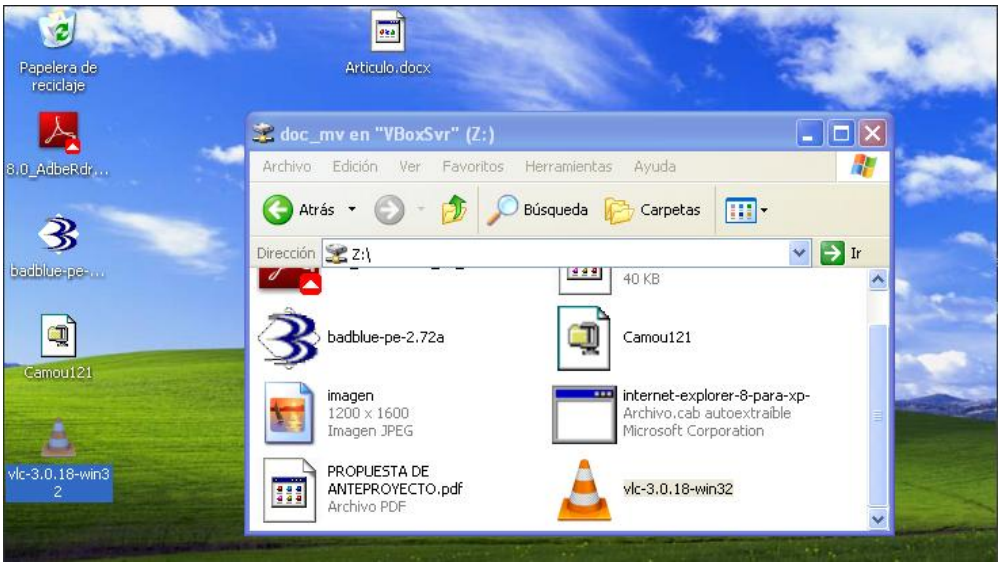

Ilustración 16. Otra forma de copiar archivos de la carpeta compartida

4.7 Instalación de Adobe Reader en Windows XP

Proceso de instalación de Adobe Reader 8 dentro de la máquina virtual, esto es un paso previo para asegurar que se tienen los visualizadores necesarios para los archivos PDF.

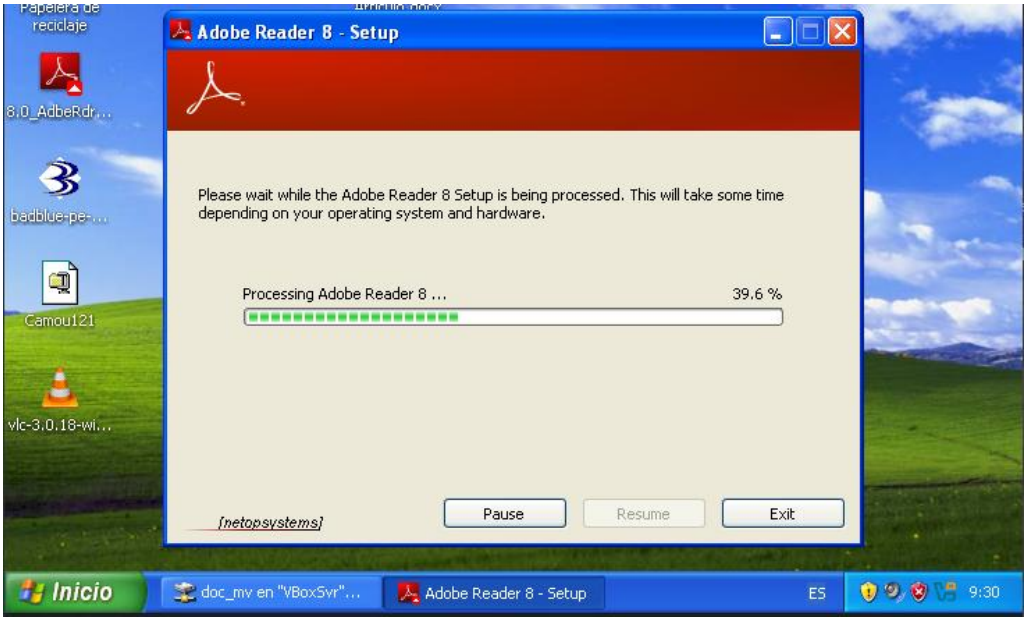

Ilustración 17. Instalación de Adobe Reader en Windows XP

Muestra la ventana el Adobe Reader 8 en el estado "Listo para instalar el programa". Hacemos clic en el botón **"Install"**.

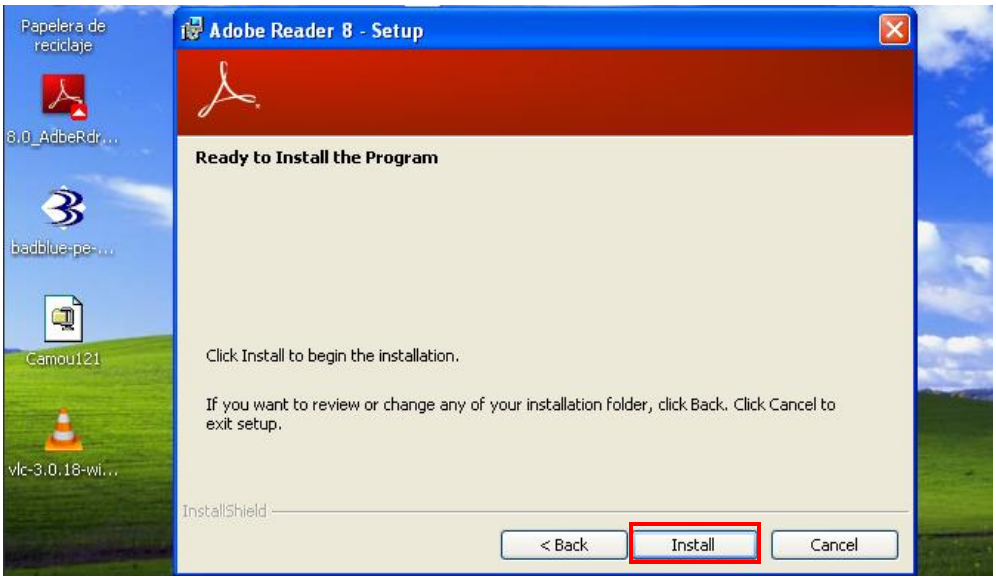

Ilustración 18. Pantalla final de instalación de Adobe Reader 8

4.8 Instalación de BadBlue Personal Edition

Pantalla de bienvenida de la instalación de BadBlue Personal Edition 2.72. Hacemos clic en **"Next"** para proceder con la instalación.

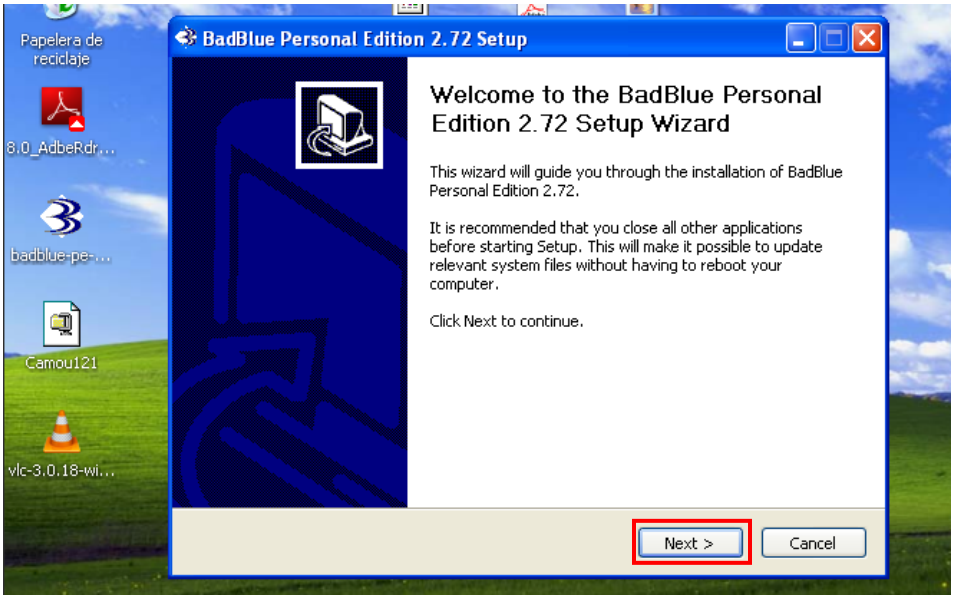

Ilustración 19. Instalación de BadBlue Personal Edition

Progreso de la instalación de BadBlue, donde se extraen archivos PHP y se crean accesos directos en el escritorio y menú de inicio. Al final, se pregunta al usuario si desea que el sitio web se inicie automáticamente al ingresar al sistema y damos clic en **"Sí".**

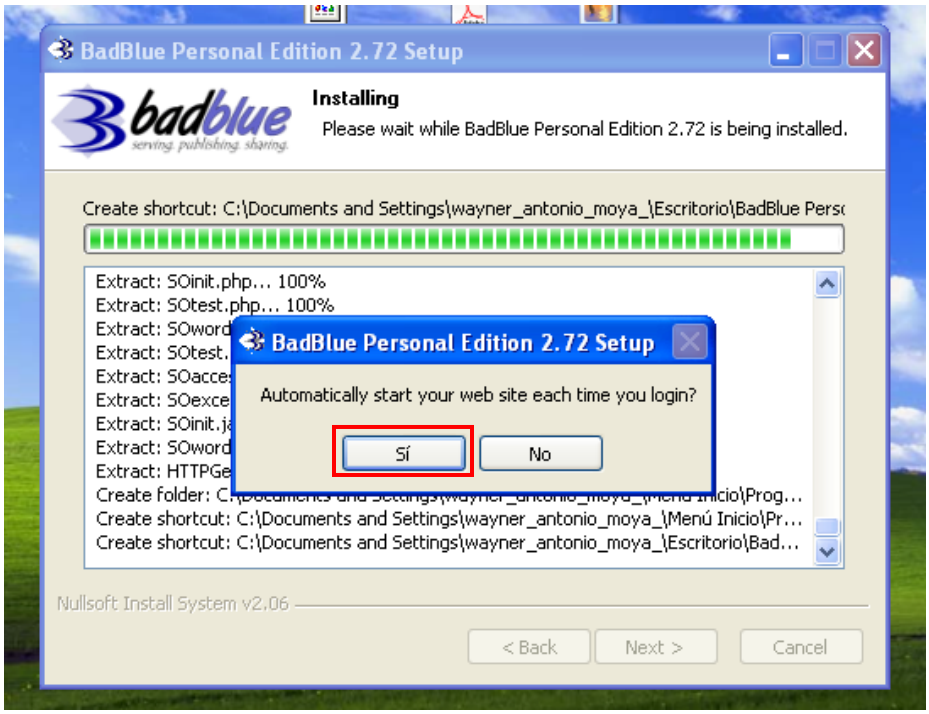

Ilustración 20. Proceso de instalación de BadBlue Personal Edition

4.9 Descompresión del archivo Camou121.exe

Ventana del descompresor WinZip para el archivo Camou121.exe. Hacer clic en Unzip.

Ilustración 21. Descompresión del archivo Camou121.exe

4.10 Pantalla de bienvenida de la instalación de Camouflage

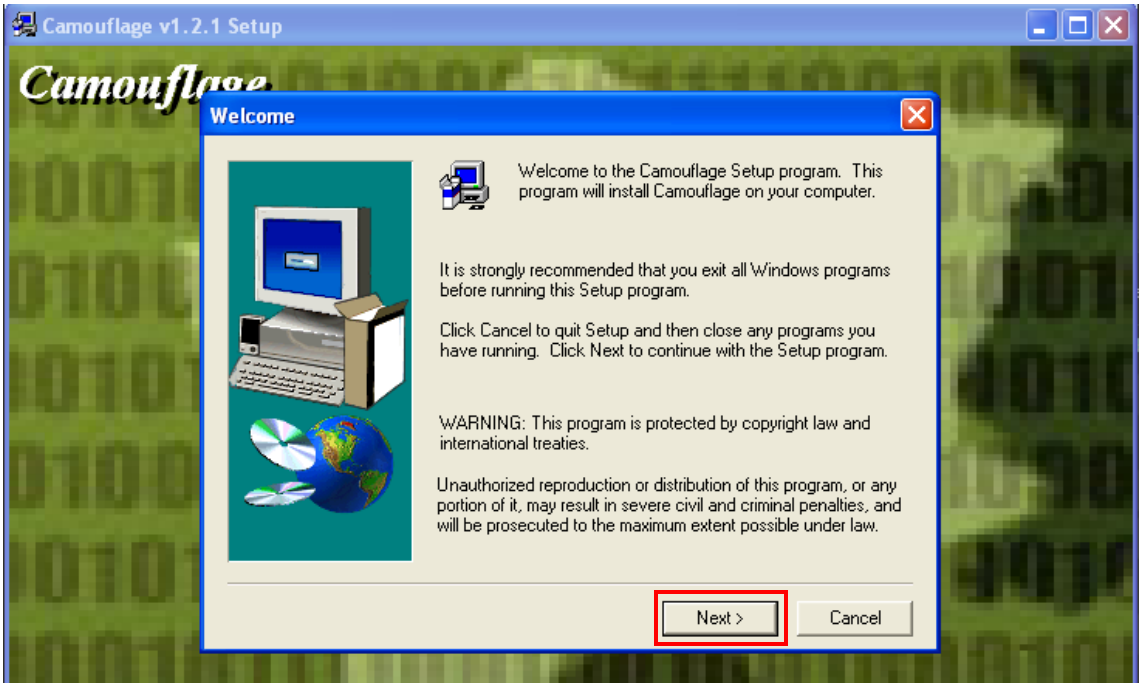

Ilustración 22. Instalación de Camouflage

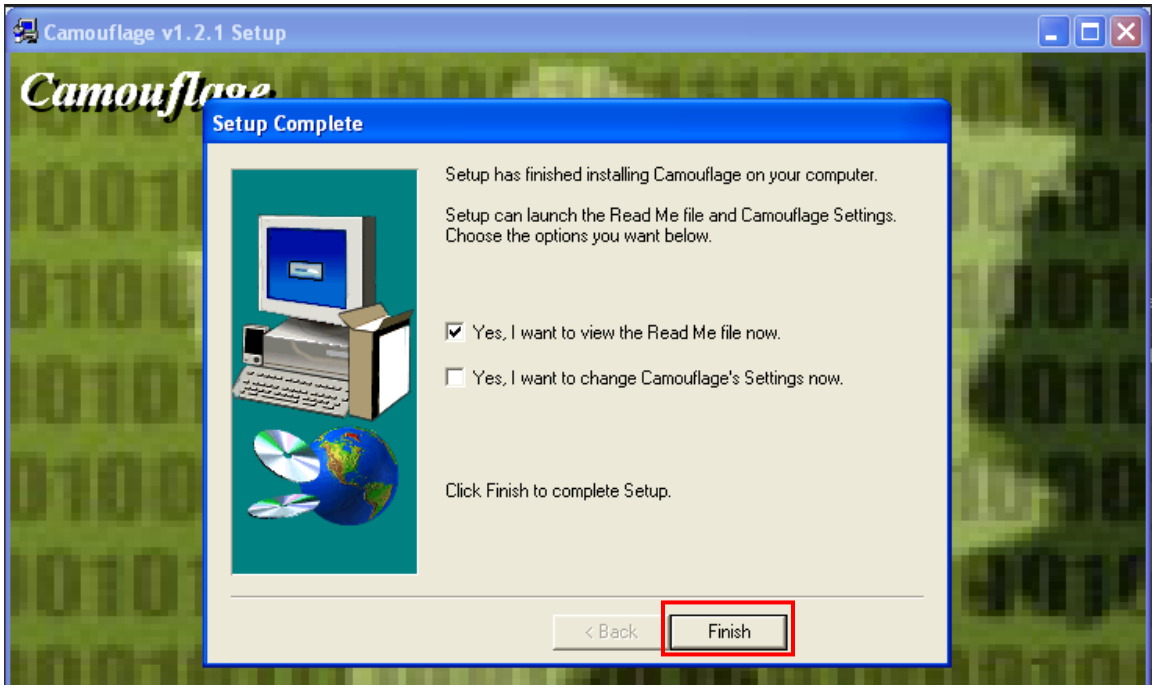

Ilustración 23. Finalización de la instalación de Camouflage

4.11 Instalación de VLC media player

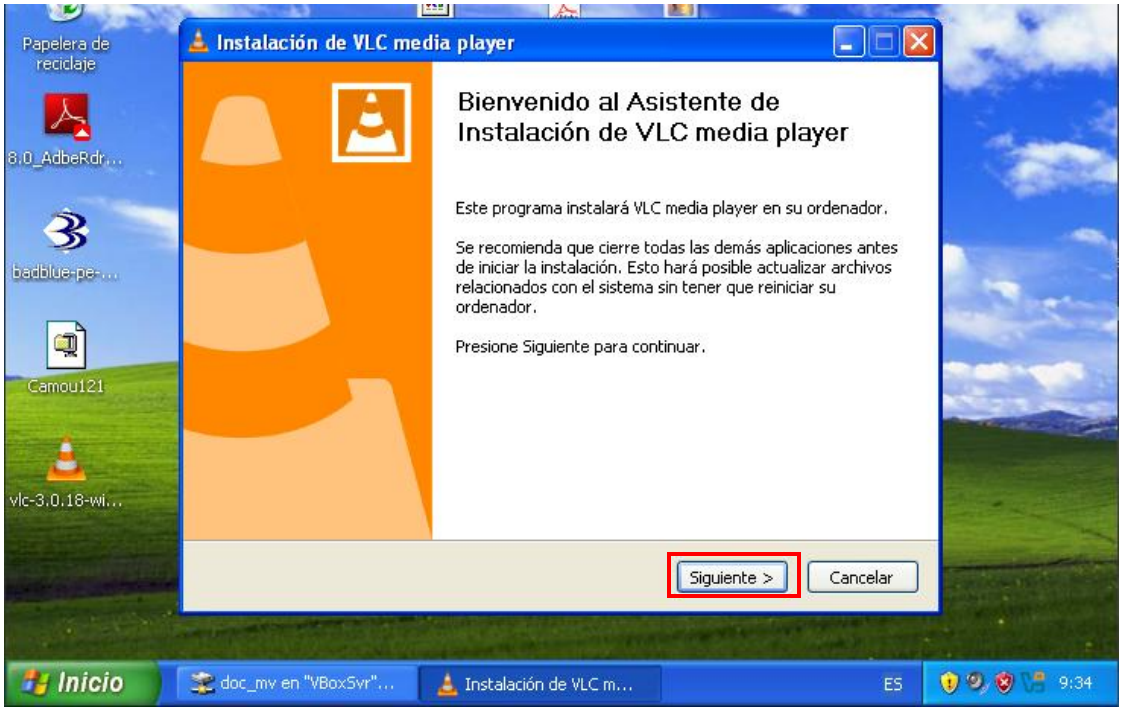

Ilustración 24. Instalación de VLC media player

Ventana donde se puede elegir la ubicación de instalación de VLC media player.

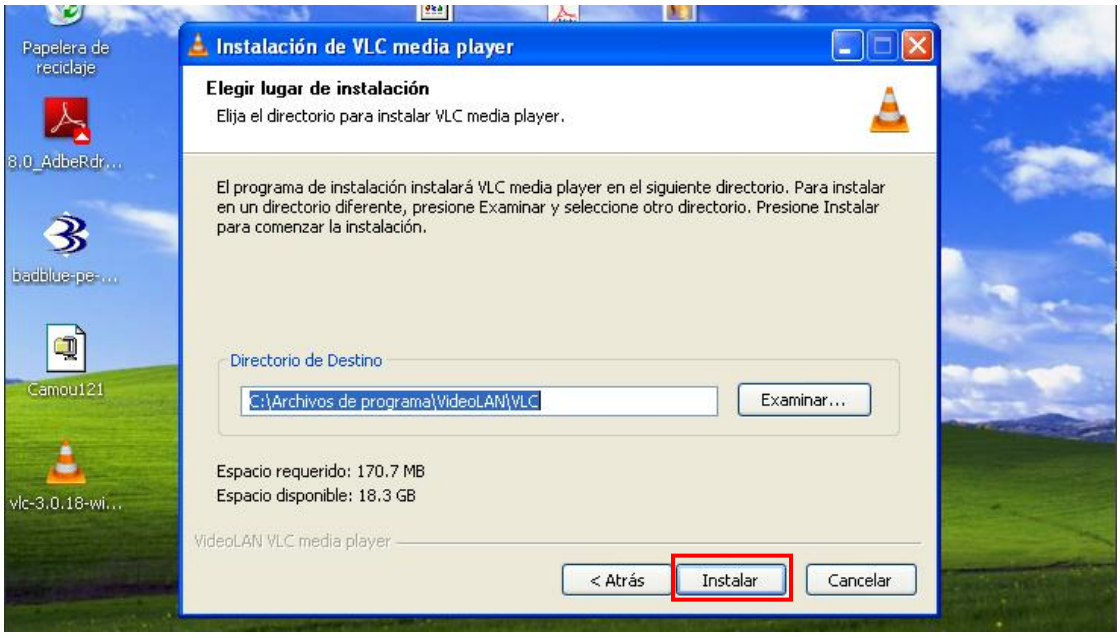

Ilustración 25. Selección de directorio de instalación de VLC

Reproductor VLC media player abierto y funcionando correctamente en el escritorio de Windows XP, confirmando que la instalación fue exitosa.

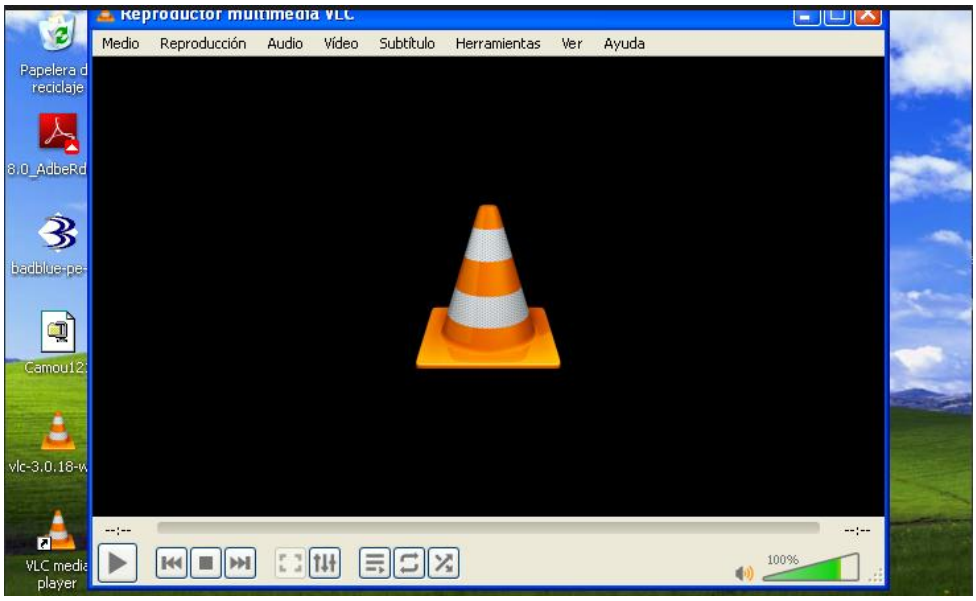

Ilustración 26. VLC media player ejecutándose en Windows XP

4.12 Términos de licencia de Internet Explorer 8

Pantalla de aceptación de los términos de licencia para la instalación de Windows Internet Explorer 8, requisito obligatorio para poder continuar con la instalación del navegador.

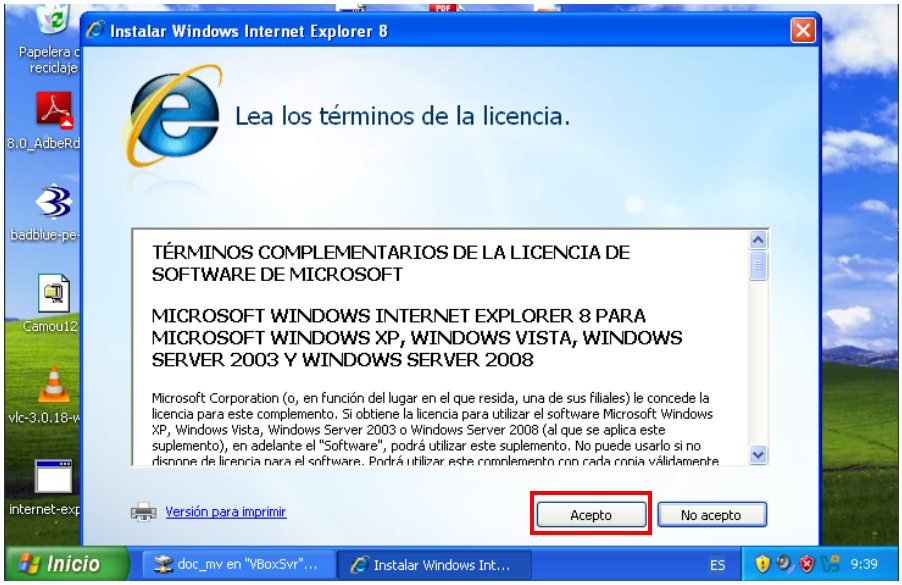

Ilustración 27. Términos de licencia de Internet Explorer 8

4.13 Escritorio con accesos directos de programas instalados

Escritorio de Windows XP con los accesos directos de todos los programas instalados exitosamente: Adobe Reader, BadBlue, Camouflage, VLC media player e Internet Explorer.

Ilustración 28. Escritorio con accesos directos de programas instalados

4.14 Ver propiedades de la imagen

Hacemos clic derecho sobre la imagen y seleccionamos **"propiedades".**

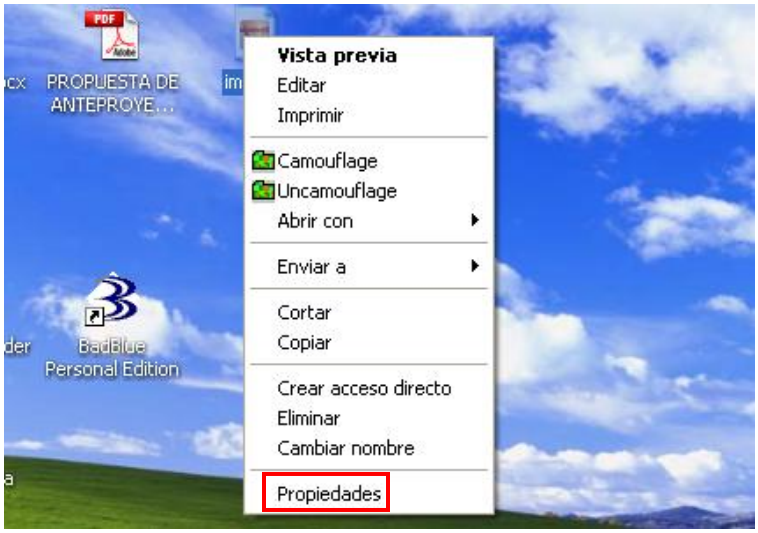

Ilustración 29. Ver propiedades de la imagen

Ventana de propiedades de un archivo JPEG, donde se pueden ver sus detalles, nos fijaremos en su tamaño el cual es de **142KB**.

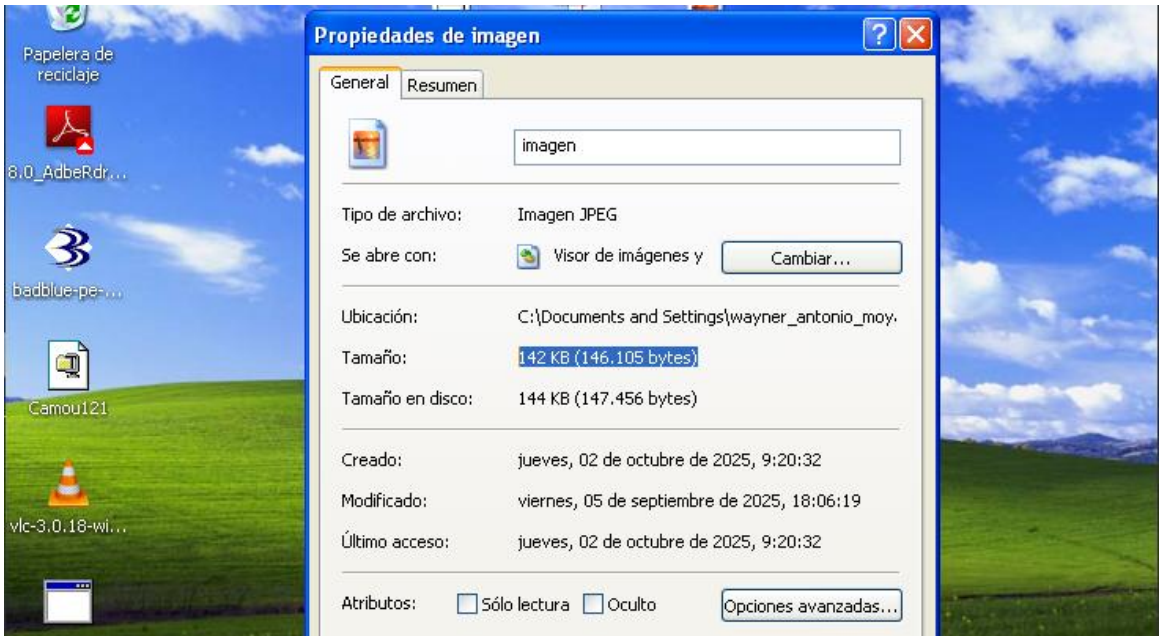

Ilustración 30. Ventana de propiedades del archivo de imagen

4.15 Camuflar archivo PDF en una imagen JPEG

Ahora hacemos clic derecho en el archivo PDF y seleccionamos la opción **"Camouflage"**, para hacer el procedimiento de ocultamiento de archivos.

Ilustración 31. Camuflar un archivo PDF

Ventana de Camouflage mostrando los archivos seleccionados para ser ocultados, en este caso seleccionaremos el archivo **"PROPUESTA DE ANTEPROYECTO.pdf"**.

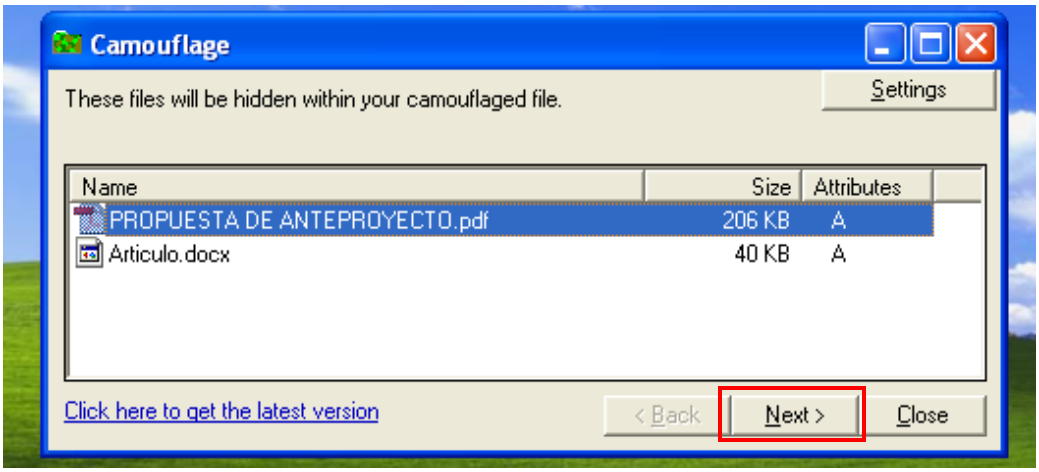

Ilustración 32. Selección del archivo PDF a camuflar

En la nueva ventana seleccionar la imagen que servirá como camuflaje, haciendo que los archivos ocultos parezcan ser este archivo JPEG.

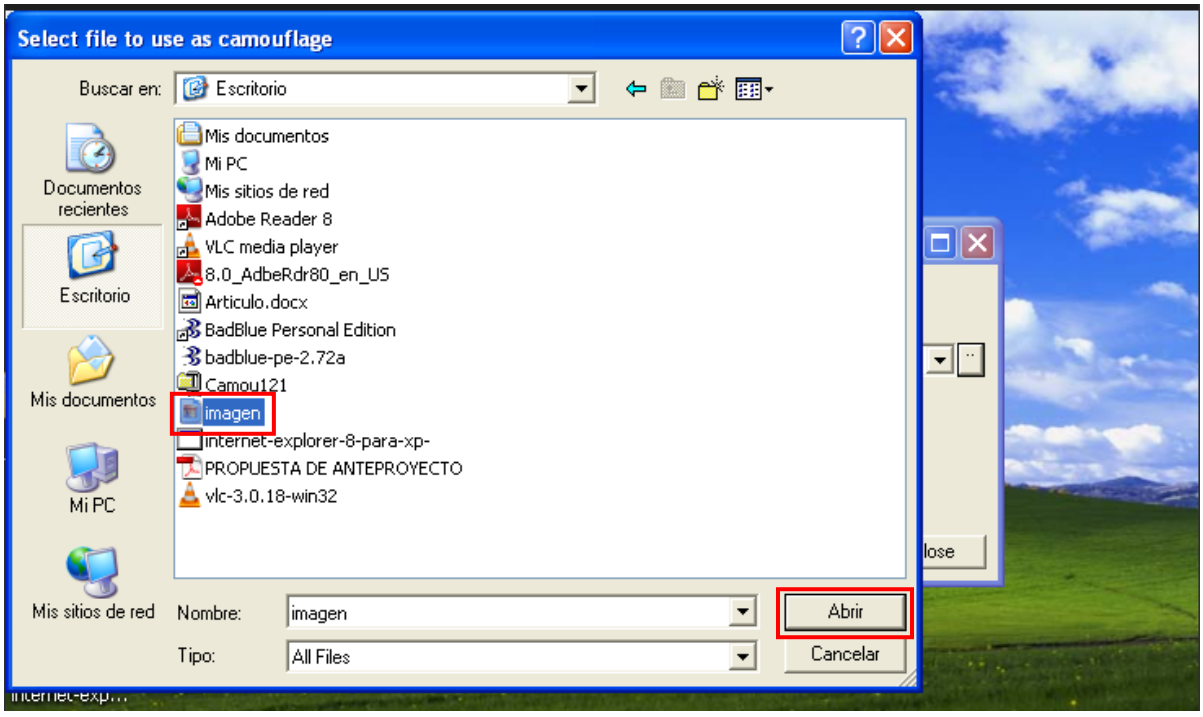

Ilustración 33. Elección del archivo donde se va a camuflar el PDF

Camouflage confirma que se utilizará el archivo "imagen" ubicado en el escritorio.

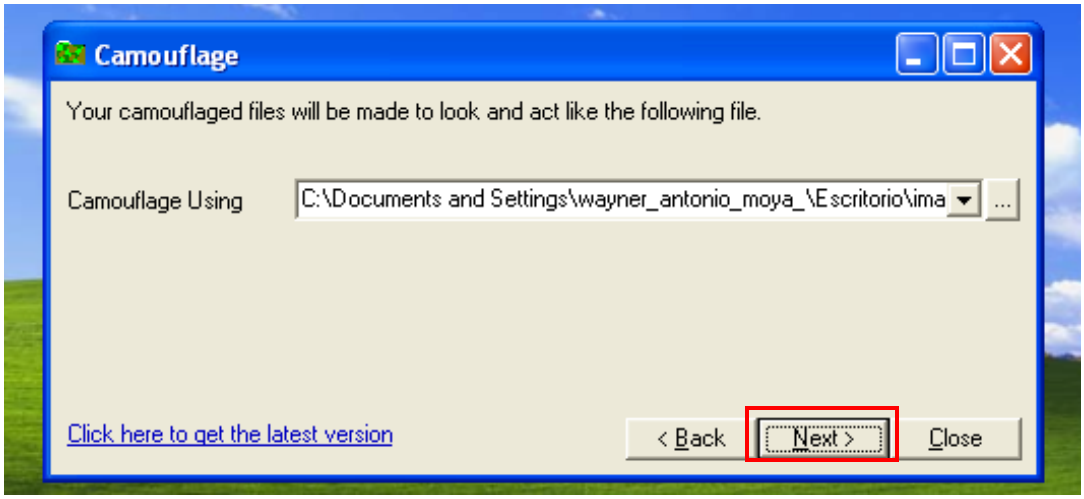

Ilustración 34. Confirmación del archivo de camuflaje

Definir el nombre del archivo camuflado como **"imagen_wpp.jpg"** o el nombre que desees y marca la opción **"Read-only"**.

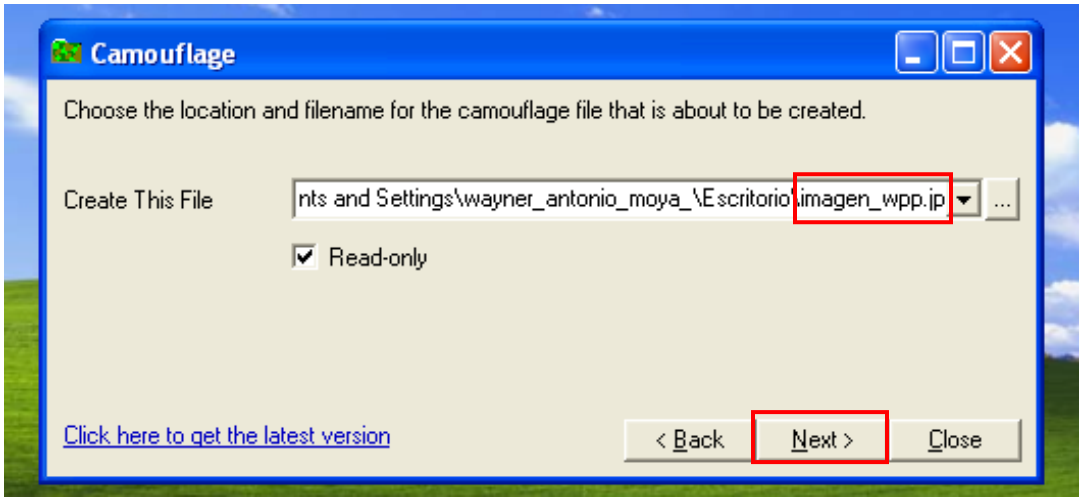

Ilustración 35. Definir nombre del archivo camuflado

Establecer una contraseña que proteja el acceso a el archivo camuflado.

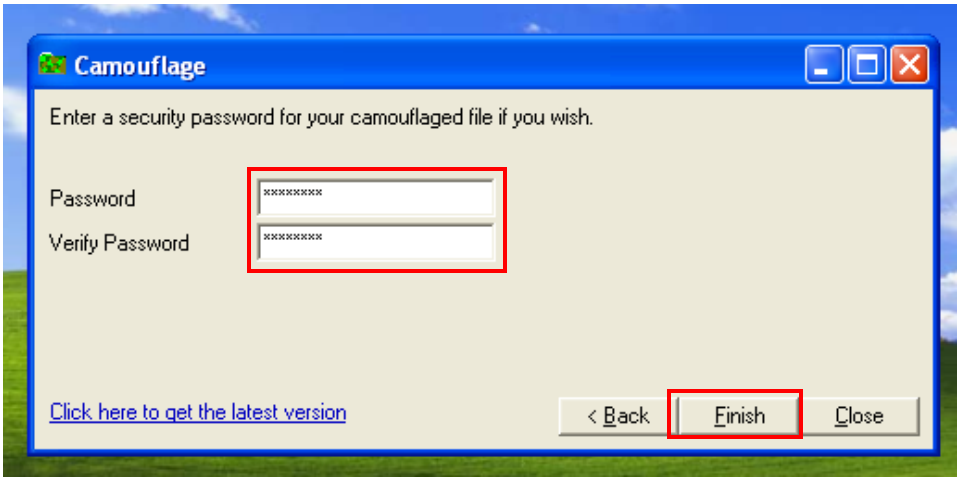

Ilustración 36. Establecimiento de contraseña de seguridad

El escritorio de Windows XP muestra el nuevo archivo **"imagen_wpp"** creado, que visualmente parece una imagen, pero contiene los archivos ocultos.

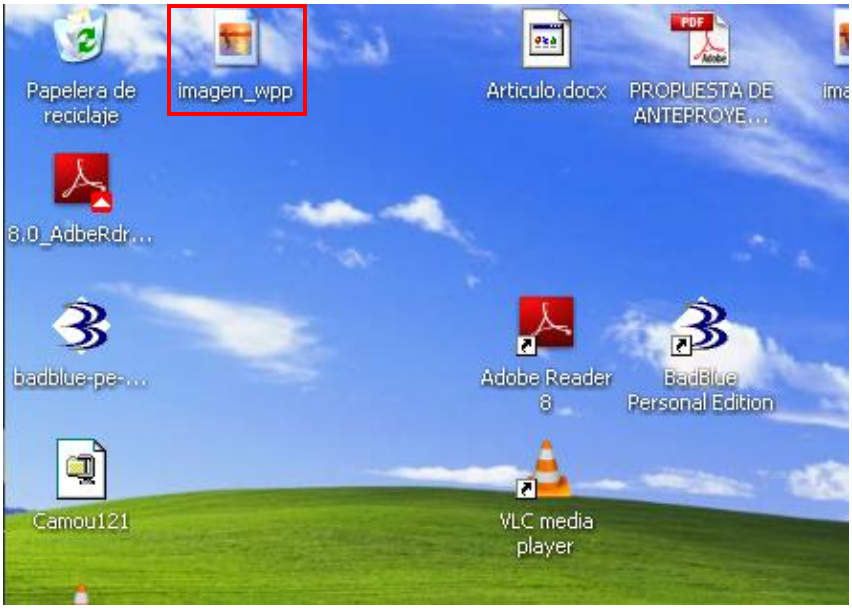

Ilustración 37. Escritorio mostrando el archivo camuflado creado

Abrir el archivo **"imagen_wpp"** con el Visor de imágenes y fax de Windows, mostrando la imagen original seleccionada como camuflaje, demostrando su apariencia normal.

Ilustración 38. Archivo camuflado abierto como imagen

Al hacer clic derecho sobre **"imagen_wpp"**, el menú contextual muestra la opción **"Propiedades"**.

Ilustración 39. Ver las propiedades de la imagen camuflada

Ventana de propiedades de **"imagen_wpp"** mostrando que el archivo tiene de tamaño 389 KB, pesa más que la imagen anterior, ya que contiene el documento oculto.

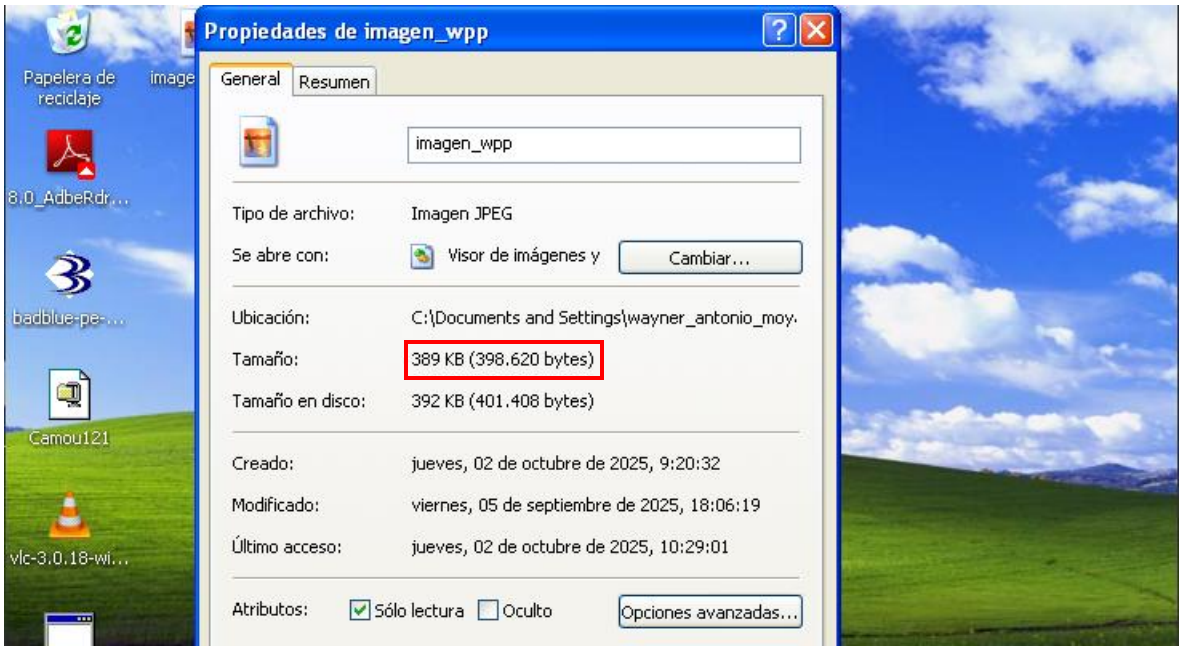

Ilustración 40. Propiedades del archivo camuflado

4.16 Camuflar un archivo de audio de WhatsApp en Adobe Reader

Hacer clic derecho sobre el archivo de audio y seleccionar la opción **"Camouflage"**.

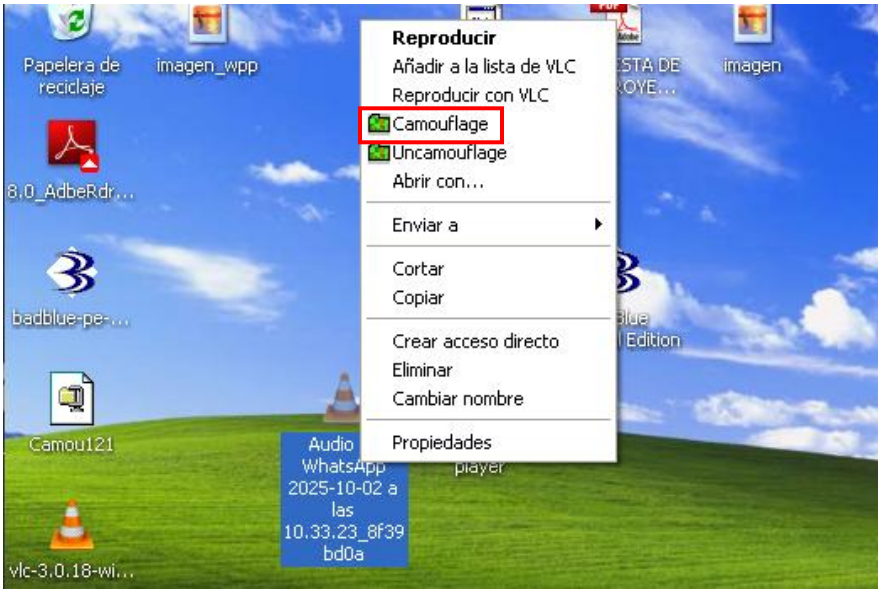

Ilustración 41. Camuflar un archivo de audio

Camouflage muestra que se ha seleccionado el archivo de audio para ser ocultado.

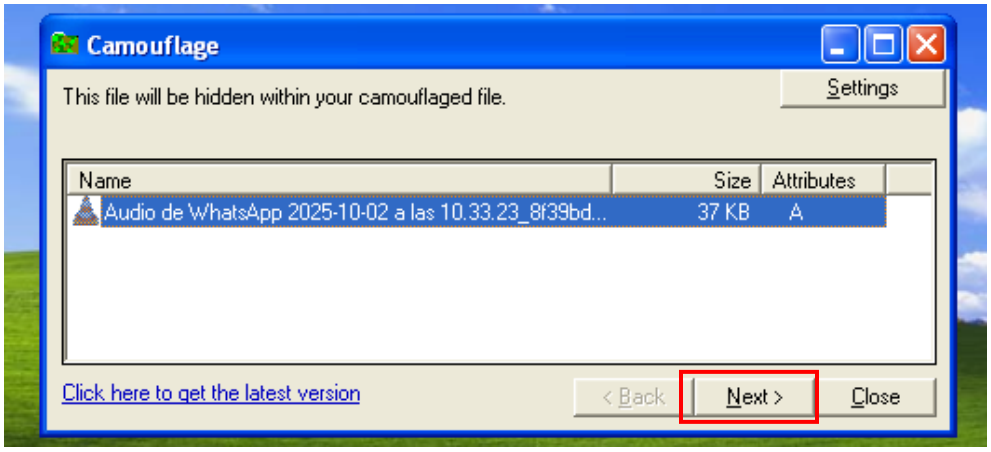

Ilustración 42. Selección del archivo de audio para camuflar

Seleccionar el archivo de Adobe Reader como archivo de camuflaje para el audio de WhatsApp.

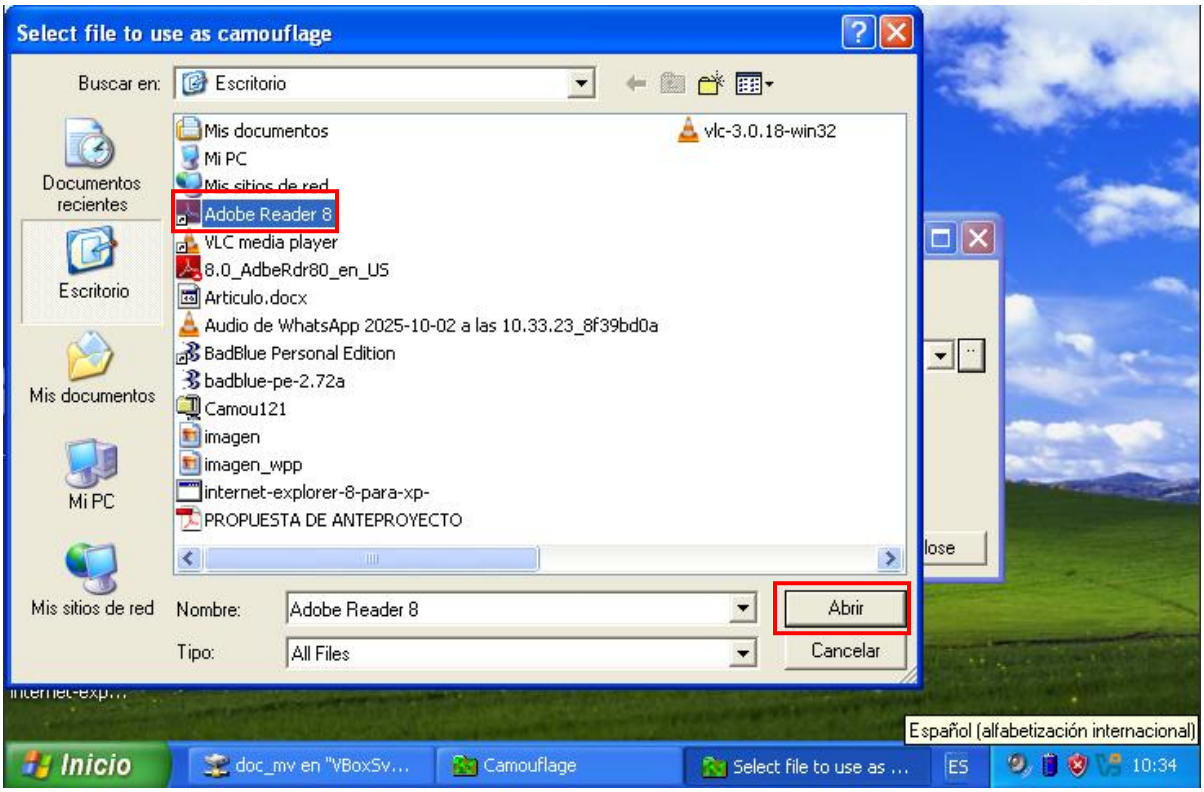

Ilustración 43. Elección del archivo donde se va a camuflar el audio de WhatsApp

Camouflage confirma que utilizará el archivo de Adobe Reader como camuflaje para el archivo de audio.

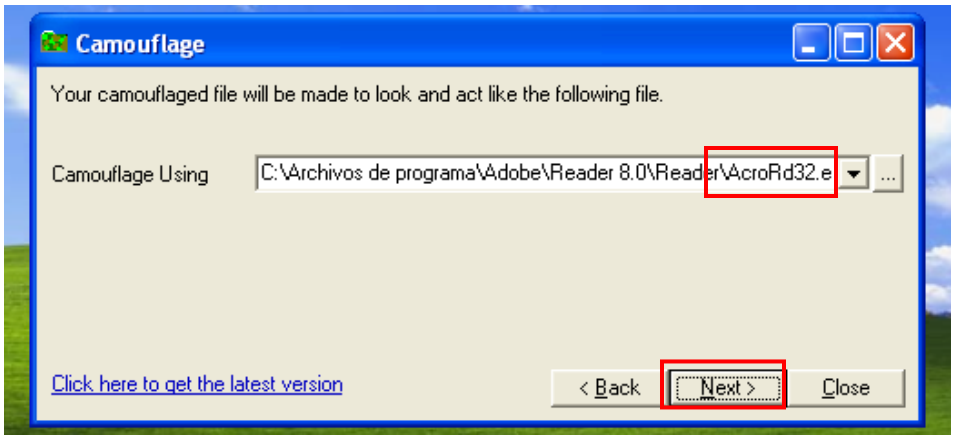

Ilustración 44. Confirmación del uso de Adobe Reader como camuflaje

Se configura una contraseña de seguridad para proteger el archivo camuflado que contiene el audio de WhatsApp.

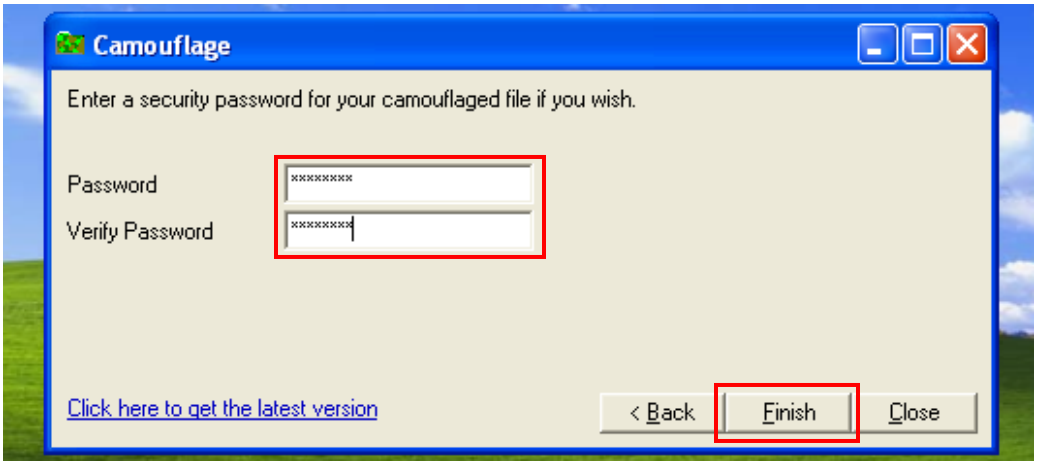

Ilustración 45. Establecimiento de contraseña para camuflar el audio

El escritorio muestra el nuevo archivo **"AcroRd32"** creado, que parece el archivo de Adobe Reader, pero contiene el audio oculto.

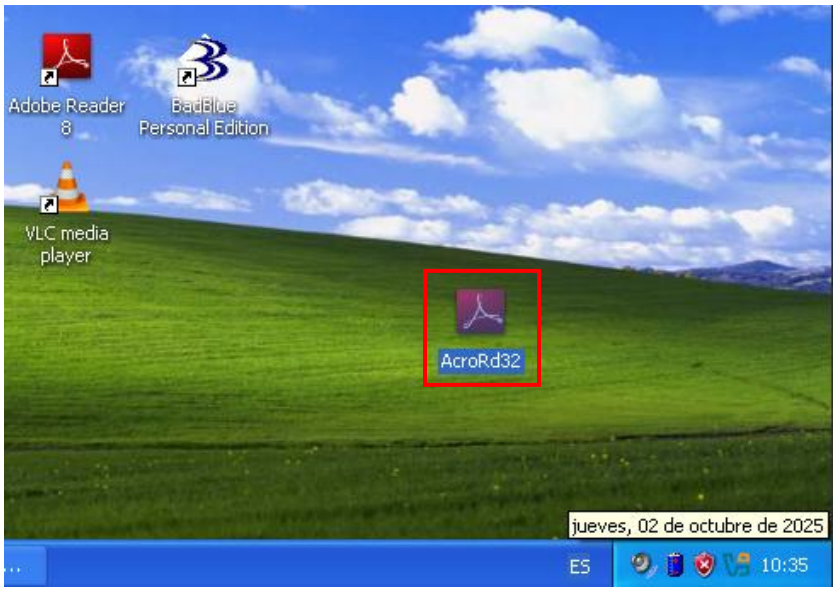

Ilustración 46. Escritorio mostrando el archivo camuflado

4.17 Descamuflar un archivo camuflado

Hacer clic derecho sobre **"AcroRd32"** y seleccionar la opción **“Uncamouflage”**, permitiendo descamuflar el contenido.

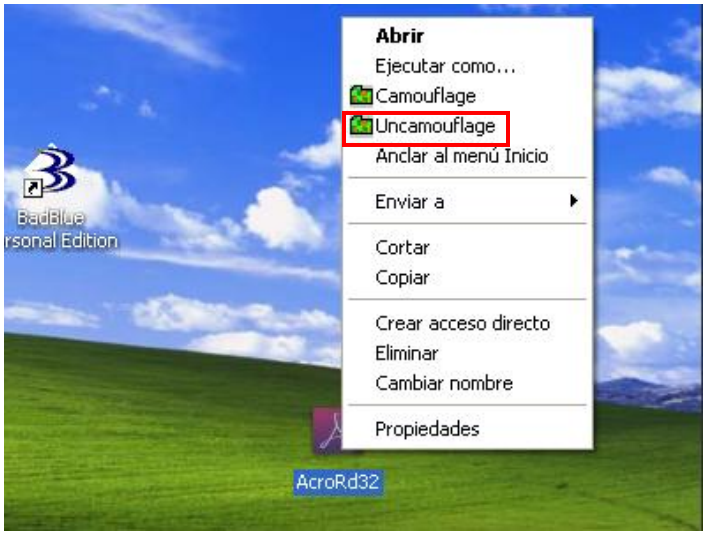

Ilustración 47. Descamuflar archivo camuflado

Ventana de Camouflage solicitando la contraseña para extraer los archivos del archivo camuflado **"AcroRd32".**

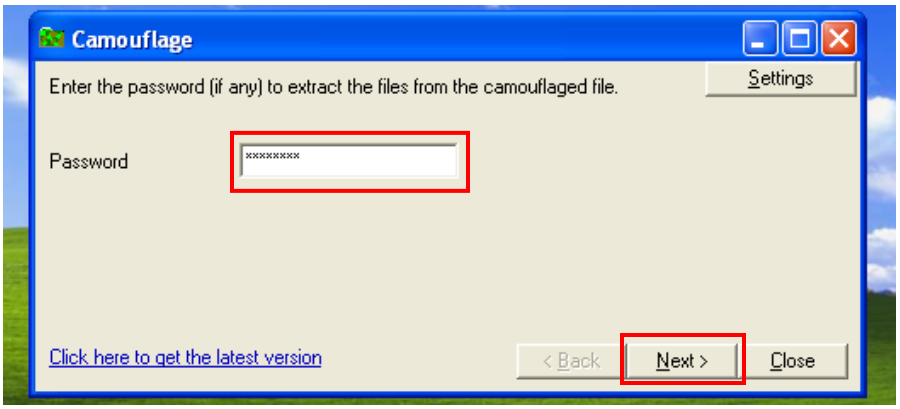

Ilustración 48. Proceso de descamuflaje - ingreso de contraseña

Camouflage muestra los archivos contenidos dentro del archivo camuflado, el propio "**AcroRd32.exe**" y el "**Audio de WhatsApp**".

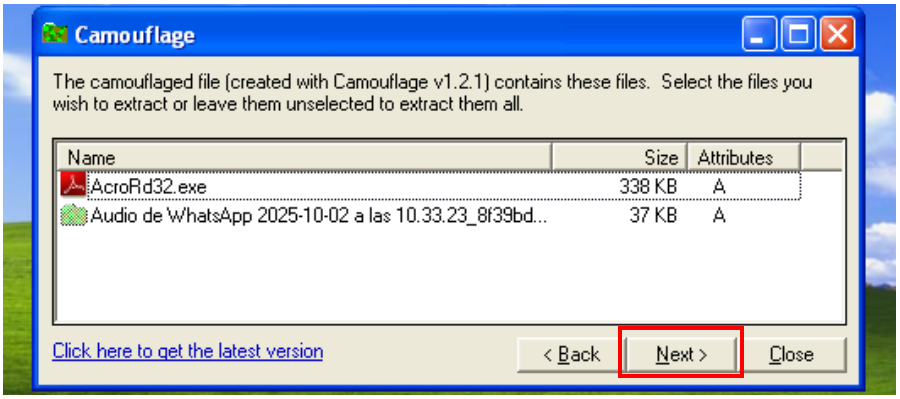

Ilustración 49. Visualización de archivos contenidos en el camuflaje

Seleccionar la carpeta donde se extraerán los archivos ocultos del archivo camuflado.

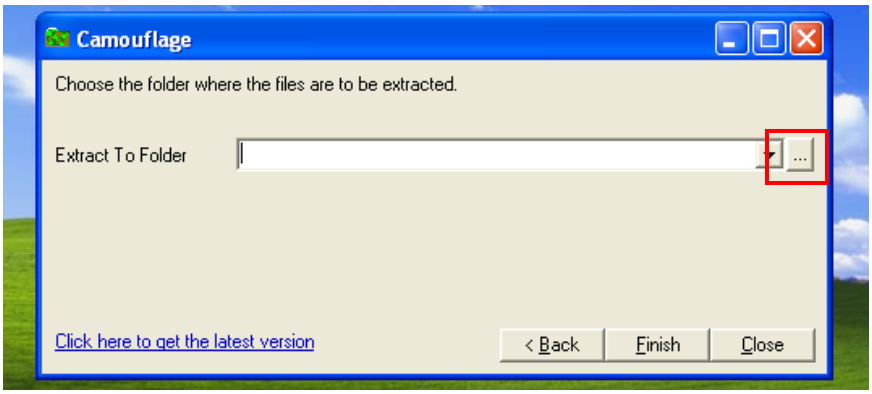

Ilustración 50. Selección de carpeta de extracción

Crear la carpeta **"docs2"** en el escritorio como destino de la extracción haciendo clic derecho y seleccionando la opción **"Carpeta"**.

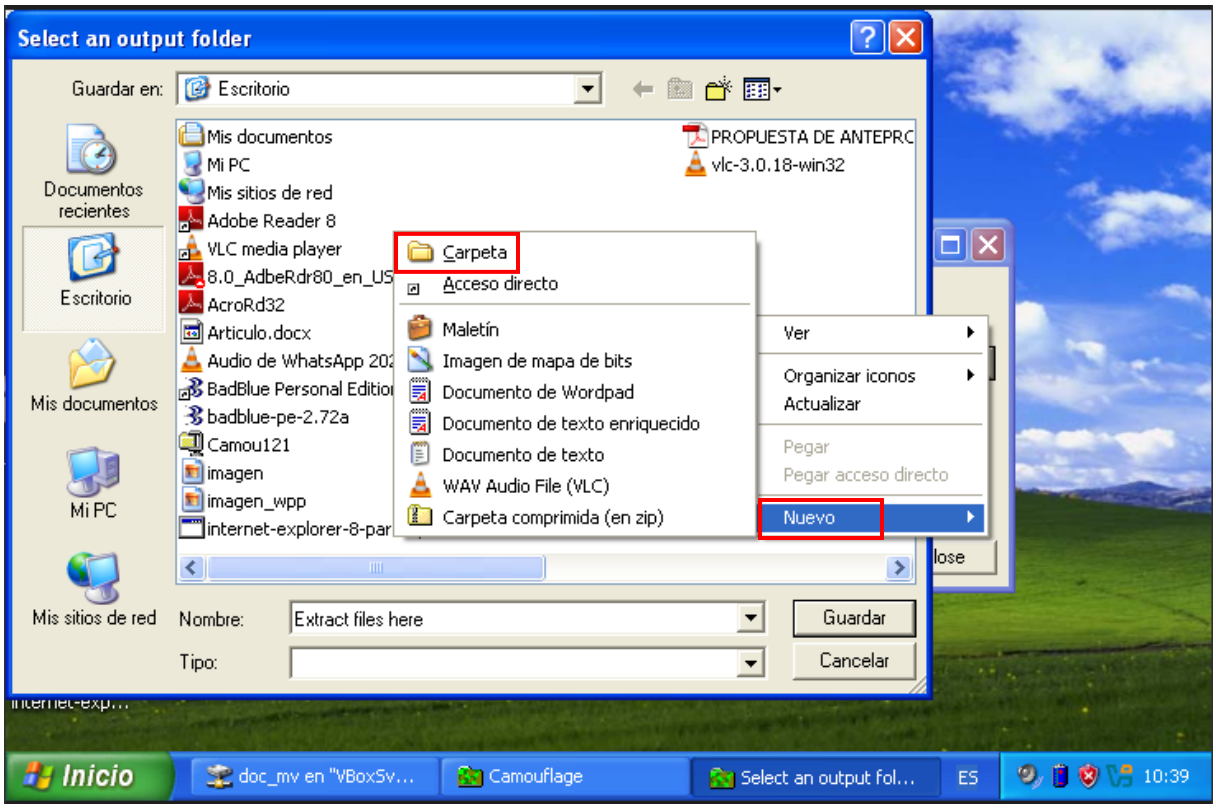

Ilustración 51. Crear carpeta de extracción

Camouflage confirma que los archivos serán extraídos a la carpeta **"docs2"** en el escritorio.

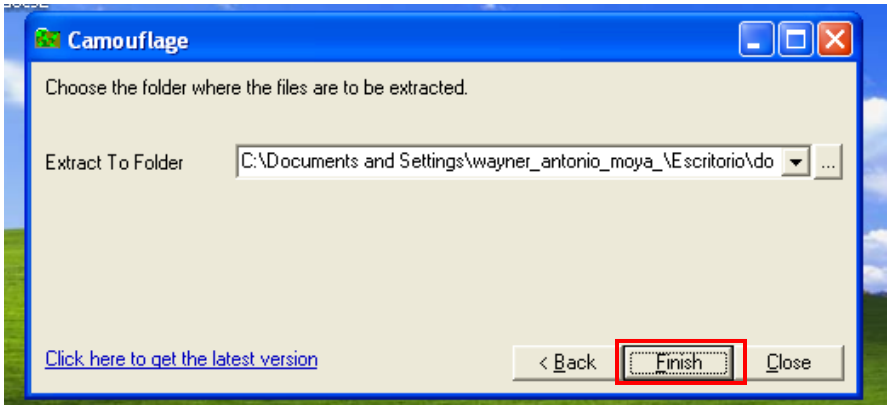

Ilustración 52. Confirmación de la carpeta de extracción

El escritorio muestra la nueva carpeta **"docs2"** creada, que contendrá los archivos extraídos del camuflaje.

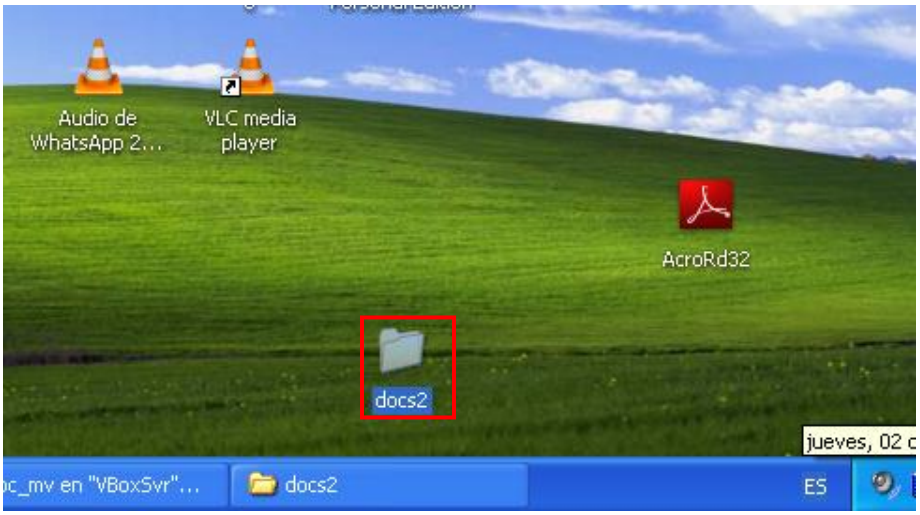

Ilustración 53. Escritorio mostrando la carpeta de extracción

Al abrir la carpeta **"docs2"**, se visualizan ambos archivos extraídos exitosamente, **"AcroRd32.exe"** y el **"Audio de WhatsApp"**, confirmando que el proceso de descamuflaje fue completo y exitoso.

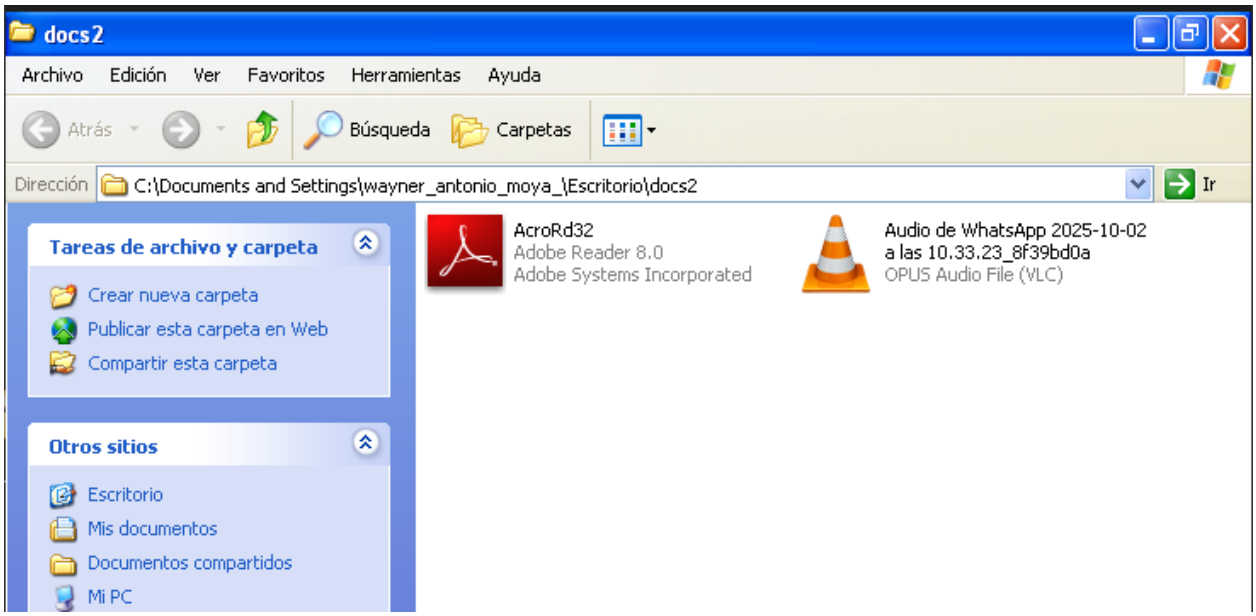

Ilustración 54. Contenido de la carpeta de extracción

4.18 Capacidad de camuflar archivos en un PDF, JPEG, WORD Y EXE

Creamos una carpeta llamada **“ARCHIVOS”** en el PC anfitrión dentro de la carpeta **“doc_mv”** y almacenamos 236 archivos o más.

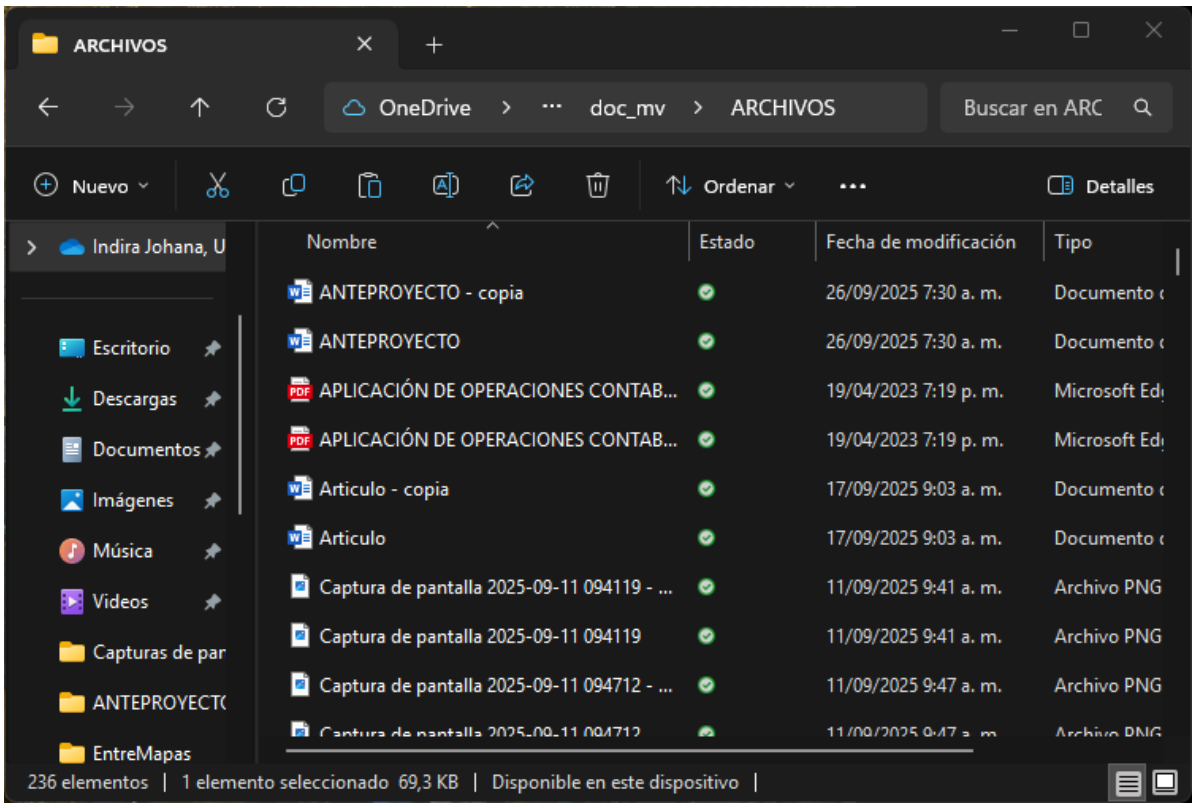

Ilustración 55. Carpeta ARCHIVOS

Nos dirigimos a Windows XP, hacemos clic derecho y seleccionamos **actualizar** para que aparezca la nueva carpeta.

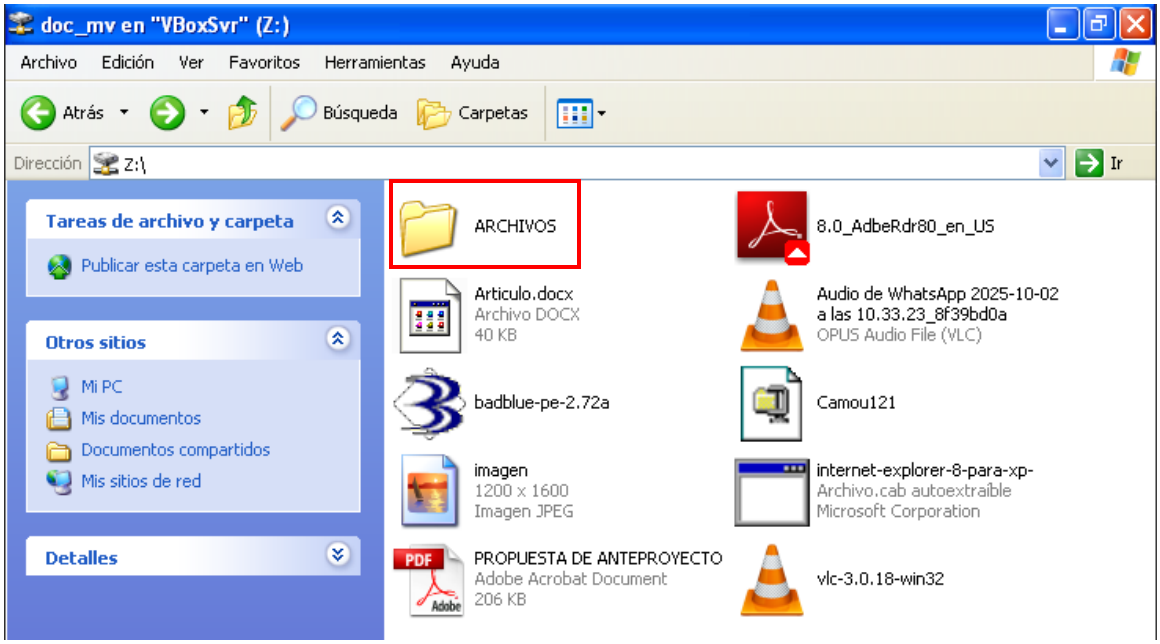

Ilustración 56. Nueva carpeta con archivos en "doc_mv"

Ingresamos a la carpeta “ARCHIVOS” y seleccionamos los archivos que están dentro.

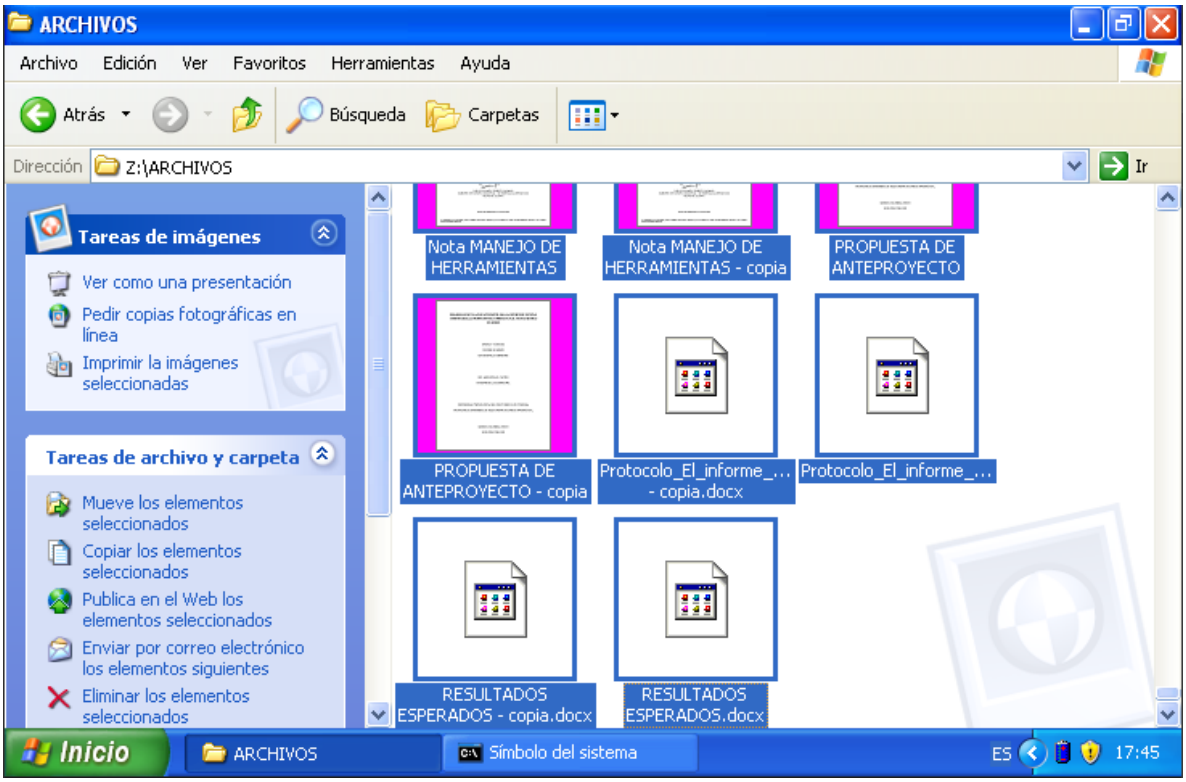

Ilustración 57. Seleccionar archivos de la nueva carpeta

Nota: Camouflage solo permite seleccionar 65 archivos en lote para ser camuflados.

Una vez seleccionados los 65 archivos hacemos clic derecho y seleccionamos la opción **“Camouflage”.**

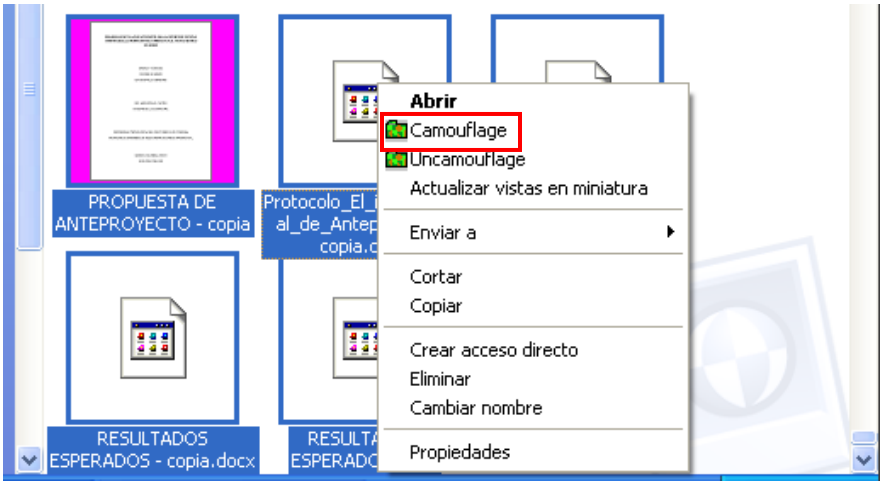

Ilustración 58. Camuflar los archivos de la nueva carpeta

La nueva ventana muestra todos los archivos que hemos seleccionados.

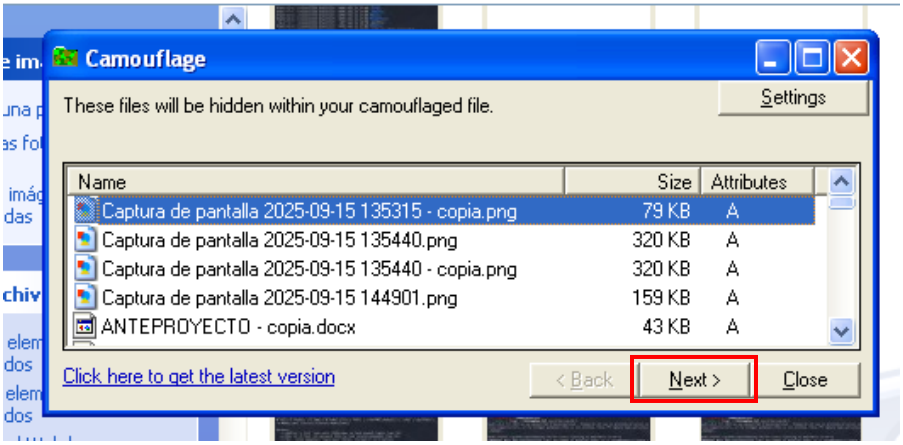

Ilustración 59. Archivos que serán camuflados

Ahora vamos a buscar el archivo en el cual vamos a camuflar los archivos, en este caso será en un documento PDF.

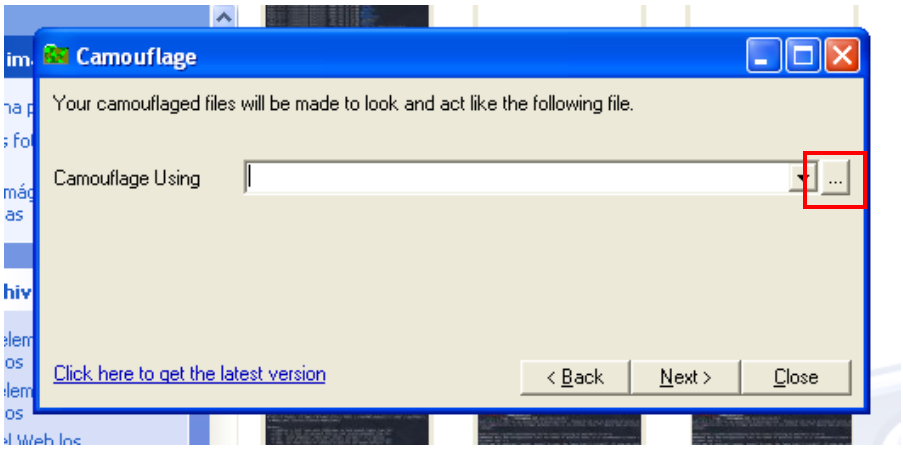

Ilustración 60. Buscar documento donde serán camuflados los archivos

Selección del archivo PDF en el cual se van a camuflar los 65 archivos.

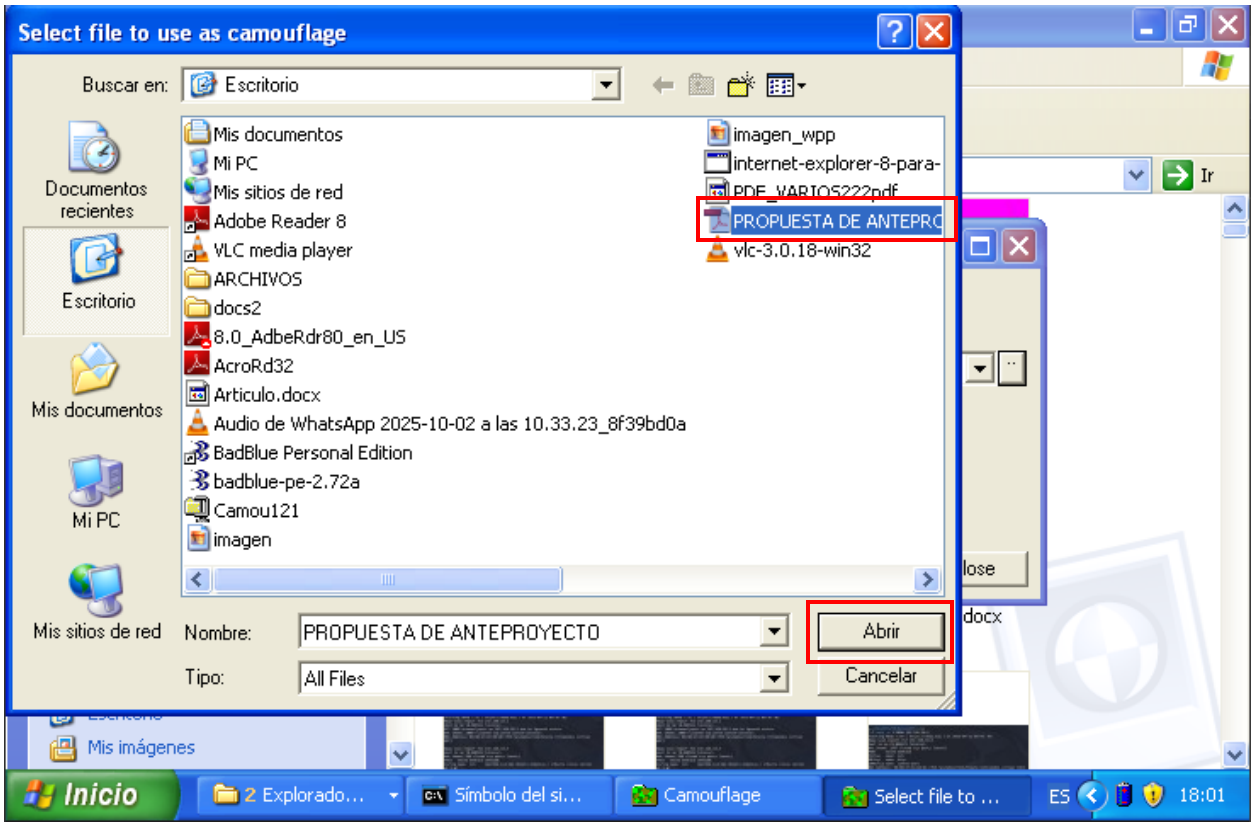

Ilustración 61. Selección del documento PDF

Archivo PDF seleccionado.

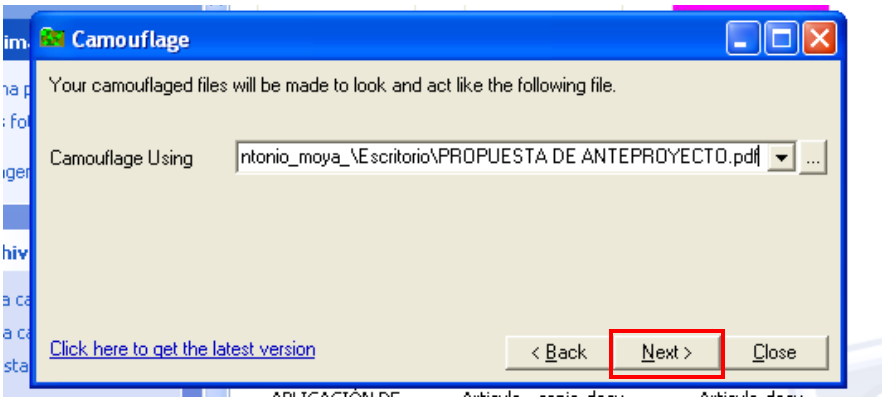

Ilustración 62. Confirmación del archivo PDF seleccionado

Reescribir el nombre del documento PDF.

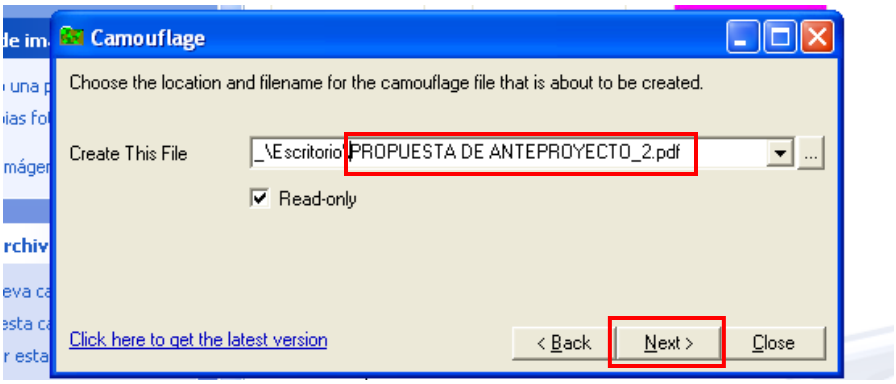

Ilustración 63. Definir nombre del archivo seleccionado

Establecer una contraseña que proteja el acceso a el archivo camuflado.

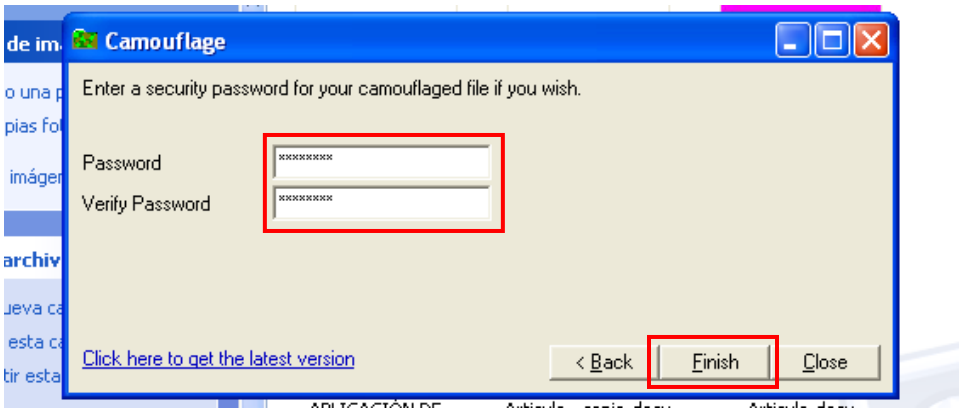

Ilustración 64. Establecer una contraseña que proteja el acceso a el archivo camuflado.

Una vez creado el documento PDF que contiene los archivos camuflados, hacemos clic derecho y seleccionamos la opción **"propiedades"** para ver el tamaño del archivo.

Ilustración 65. Tamaño del documento PDF que contiene los archivos camuflados

También podemos usar la opción **"Uncamouflage"** para observar los documentos que están camuflados dentro del archivo PDF, haciendo clic derecho sobre el archivo.

Ilustración 66. Observar archivos camuflados dentro del PDF

Ventana de Camouflage solicitando la contraseña para extraer los archivos del archivo PDF camuflado.

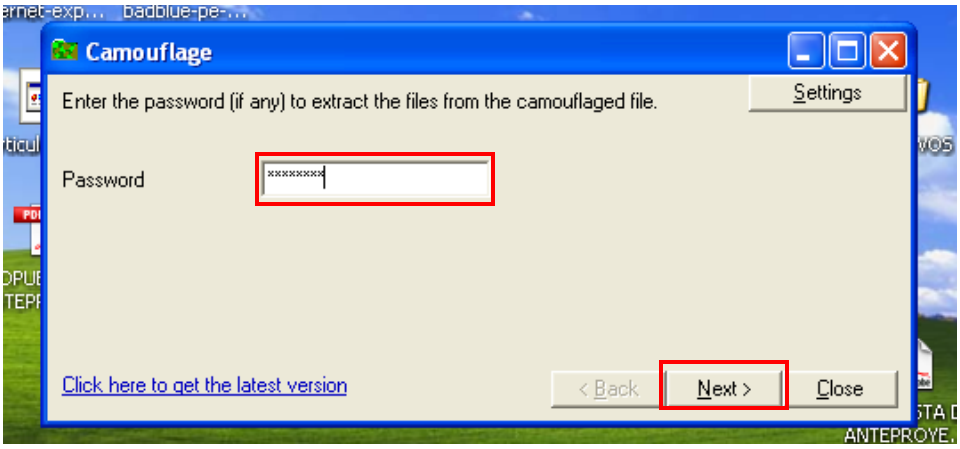

Ilustración 67. Proceso de descamuflaje - ingreso de contraseña

Camouflage muestra los archivos contenidos dentro del archivo PDF camuflado.

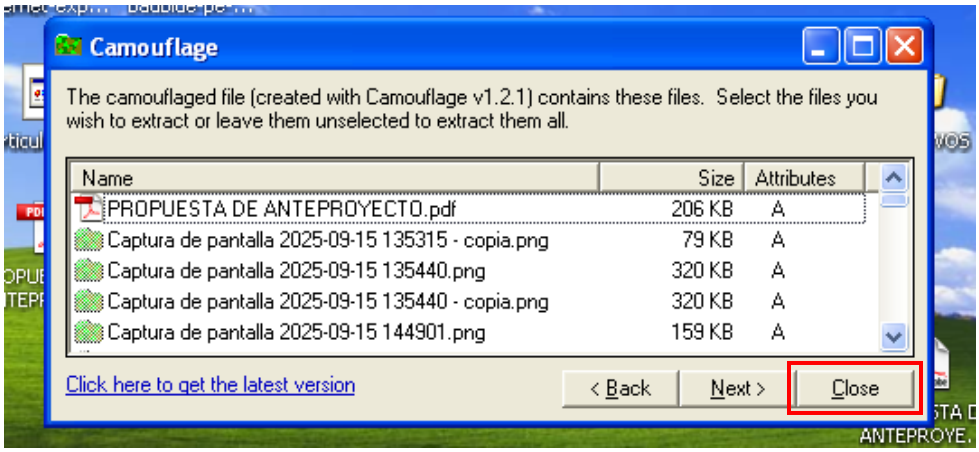

Ilustración 68. Visualización de archivos contenidos en el camuflaje

Ahora vamos a camuflar los 236 archivos que hay en la carpeta **"ARCHIVOS"** en una imagen con formato JPEG**.** Debemos comprimir la carpeta en formato ZIP desde el PC anfitrión, luego vamos a Windows XP y actualizamos la carpeta **"doc_mv"** para que aparezca la carpeta comprimida.

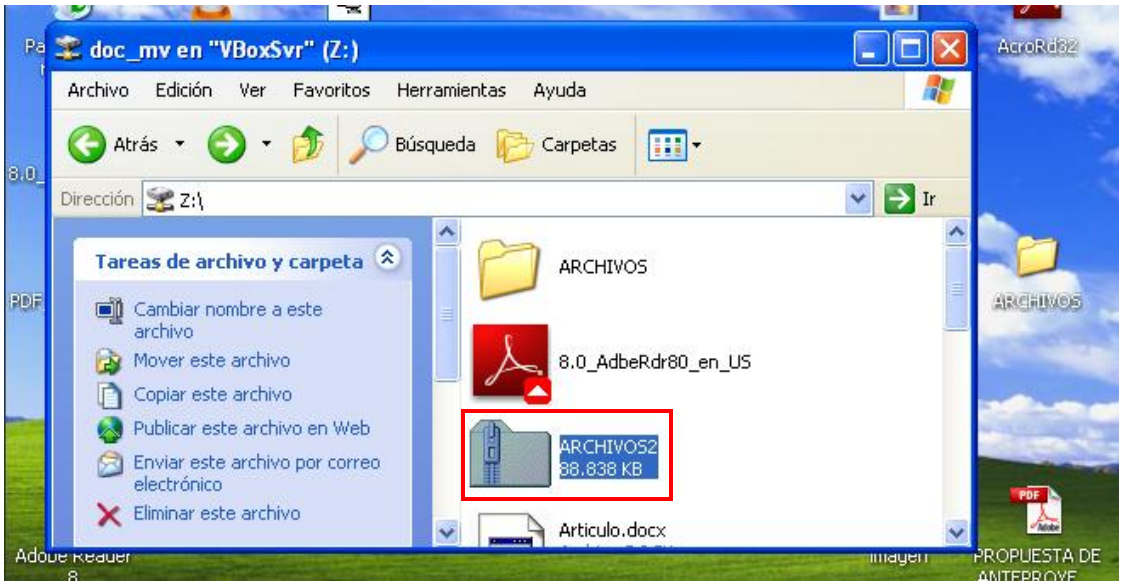

Ilustración 69. Carpeta "ARCHIVOS" comprimida para camuflarla en una imagen JPEG

Nota: Para camuflar una determinada cantidad de archivos y Camouflage no ponga un límite de selección es recomendable tener todos los archivos que se van a camuflar en una carpeta comprimida.

Hacemos clic derecho sobre la carpeta comprimida y seleccionamos la opción **"Camouflage".**

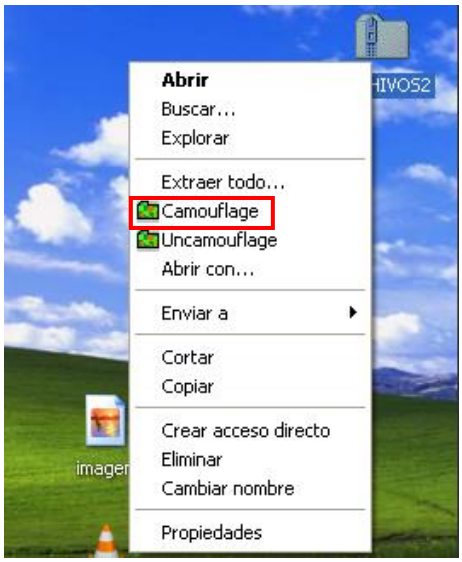

Ilustración 70. Camuflar carpeta comprimida en una imagen JPEG

Camouflage muestra que se ha seleccionado el archivo comprimido.

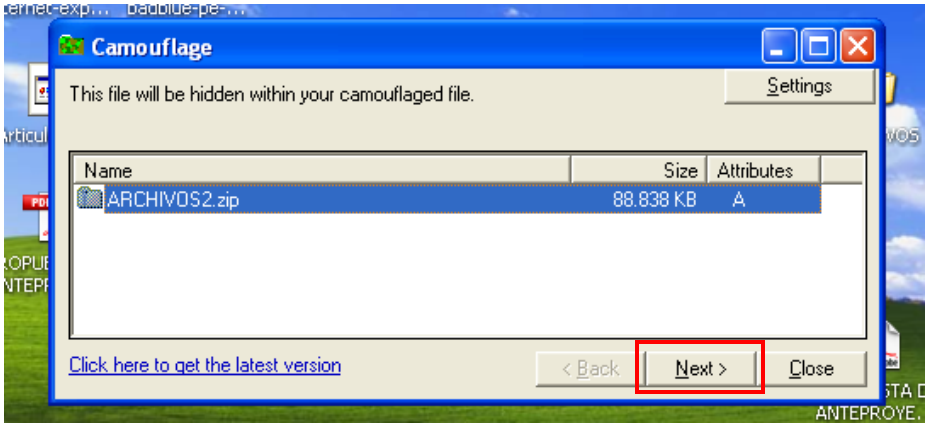

Ilustración 71. Selección del archivo comprimido a camuflar

Seleccionar el archivo de **imagen** como archivo de camuflaje para la carpeta comprimida.

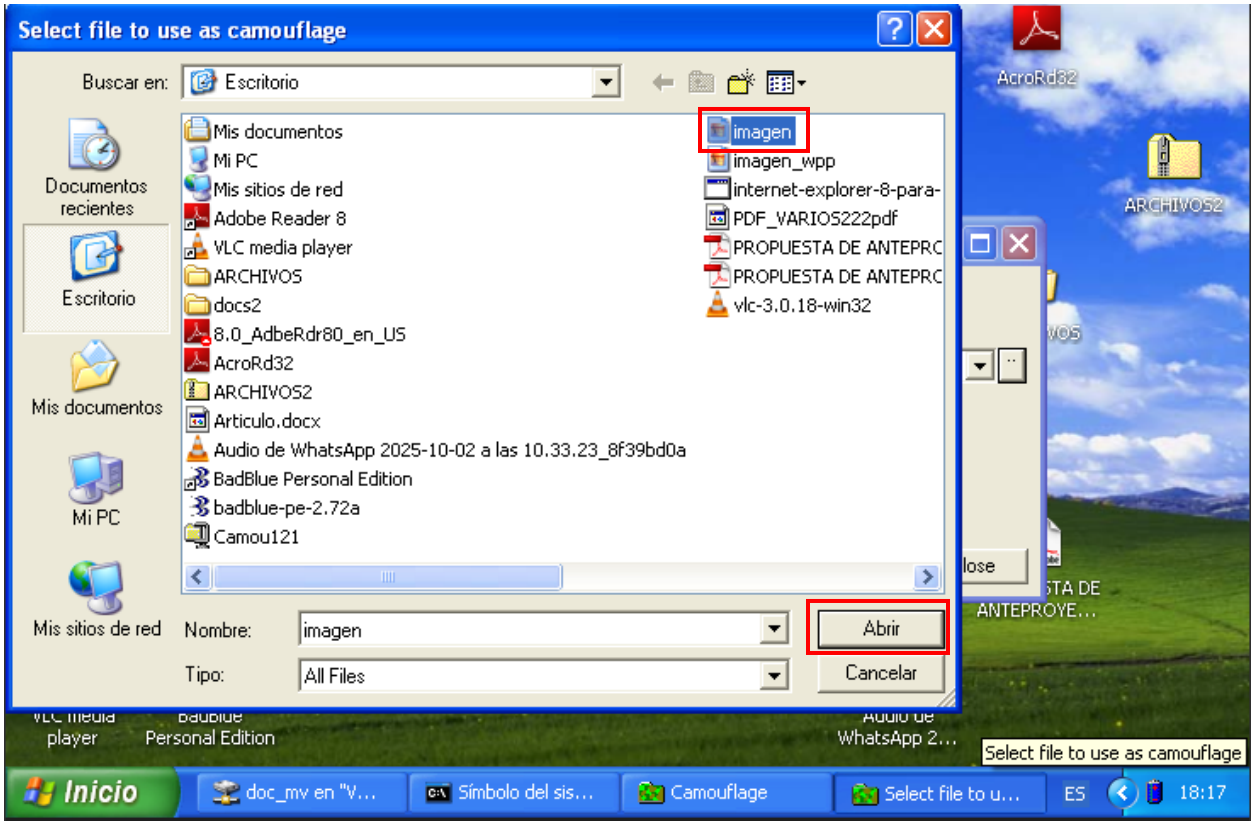

Ilustración 72. Elección del archivo donde se va a camuflar el audio de WhatsApp

Definir el nombre del archivo camuflado como **"imagen22.jpg"** o el nombre que desees.

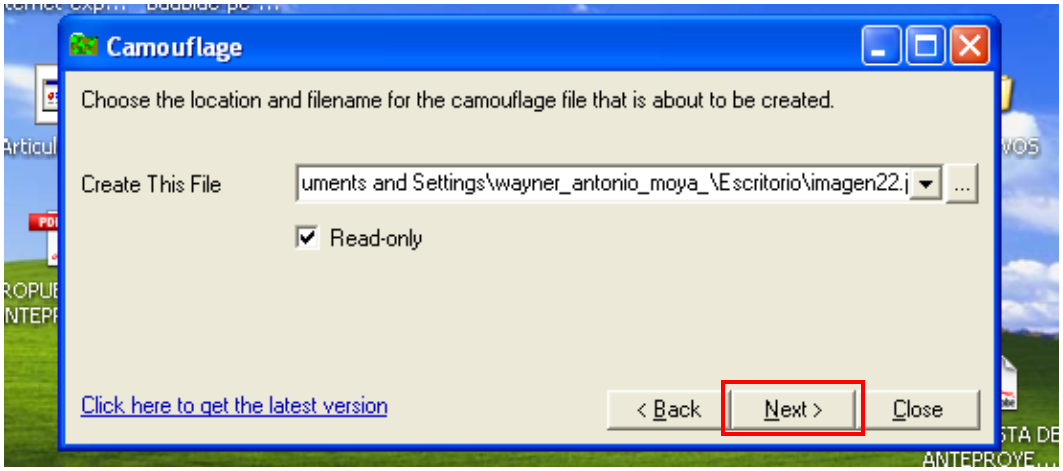

Ilustración 73. Definir nombre del archivo camuflado

Una vez creada la imagen donde se encuentra la carpeta ZIP camuflada, hacemos clic derecho sobre ella y seleccionamos la opción **"propiedades"** para ver el tamaño de la imagen.

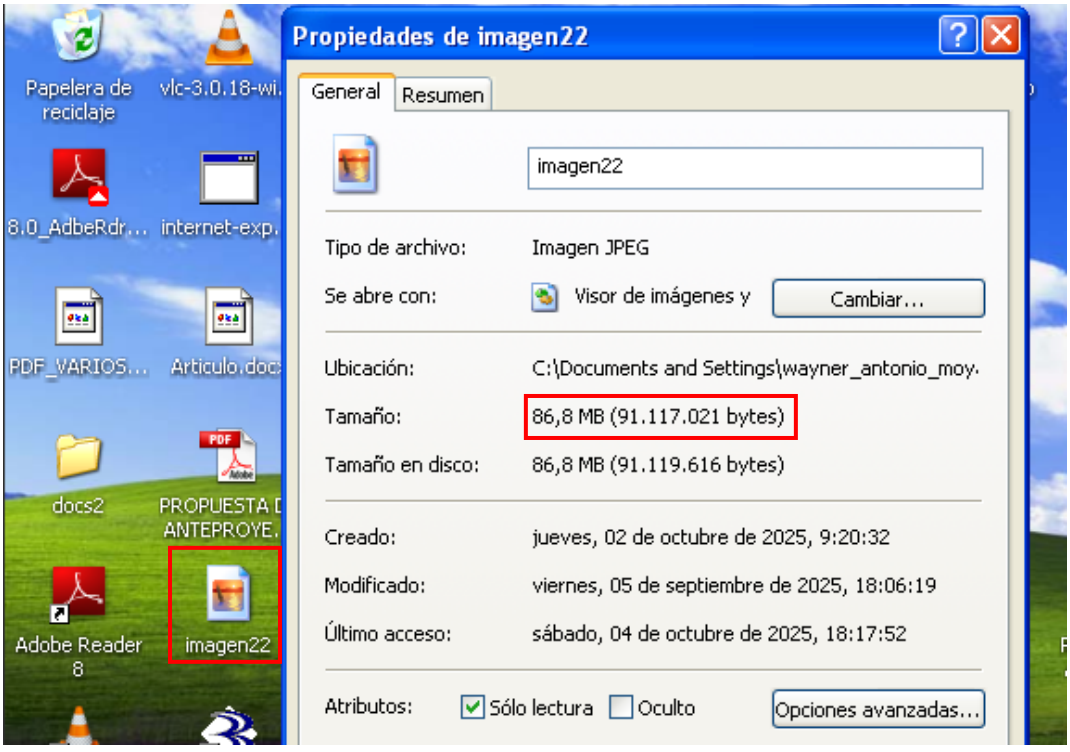

Ilustración 74. Ver propiedades de la imagen22

Ahora vamos a camuflar un archivo que pesa 7.61GB en un documento Word. Hacemos clic derecho sobre el archivo y seleccionamos la opción **"Camouflage".**

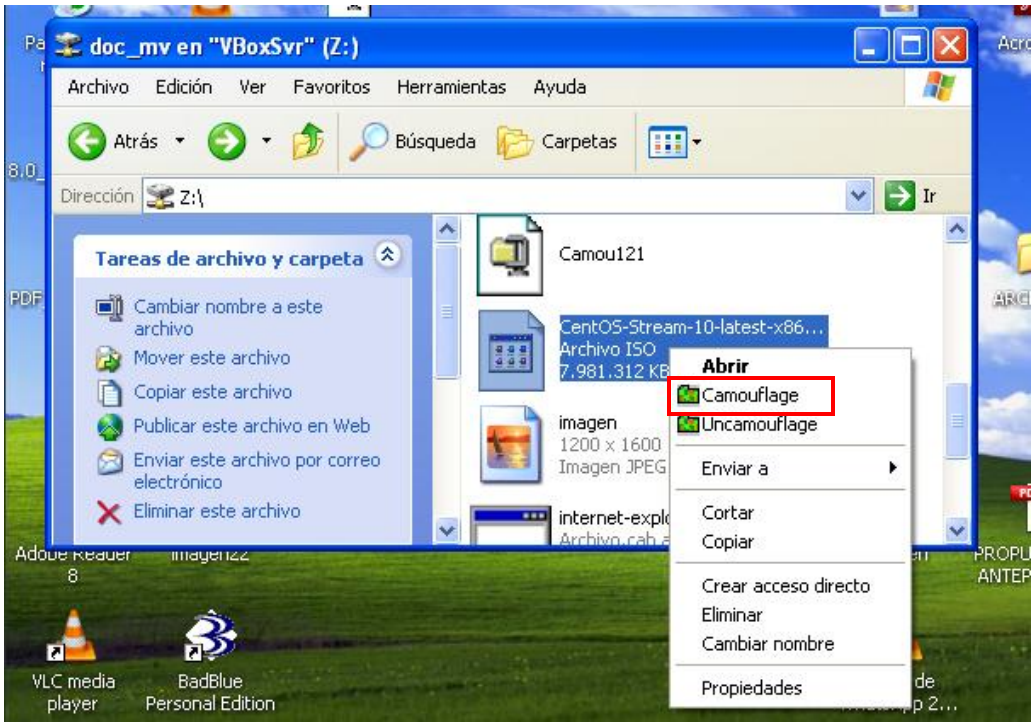

Ilustración 75. Camuflar archivo pesado en un documento Word

Camouflage muestra que se ha seleccionado el archivo que se va a camuflar.

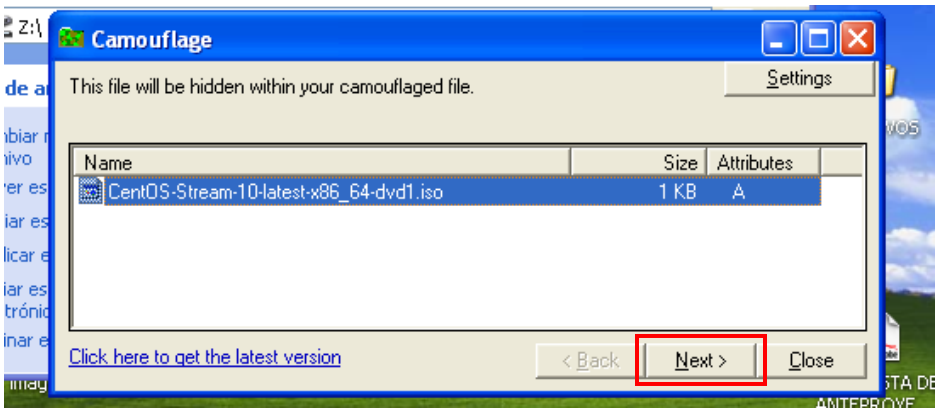

Ilustración 76. Selección del archivo comprimido a camuflar

Seleccionar el archivo de **Articulo.docx** el cual es donde se va a camuflar el archivo que de gran tamaño.

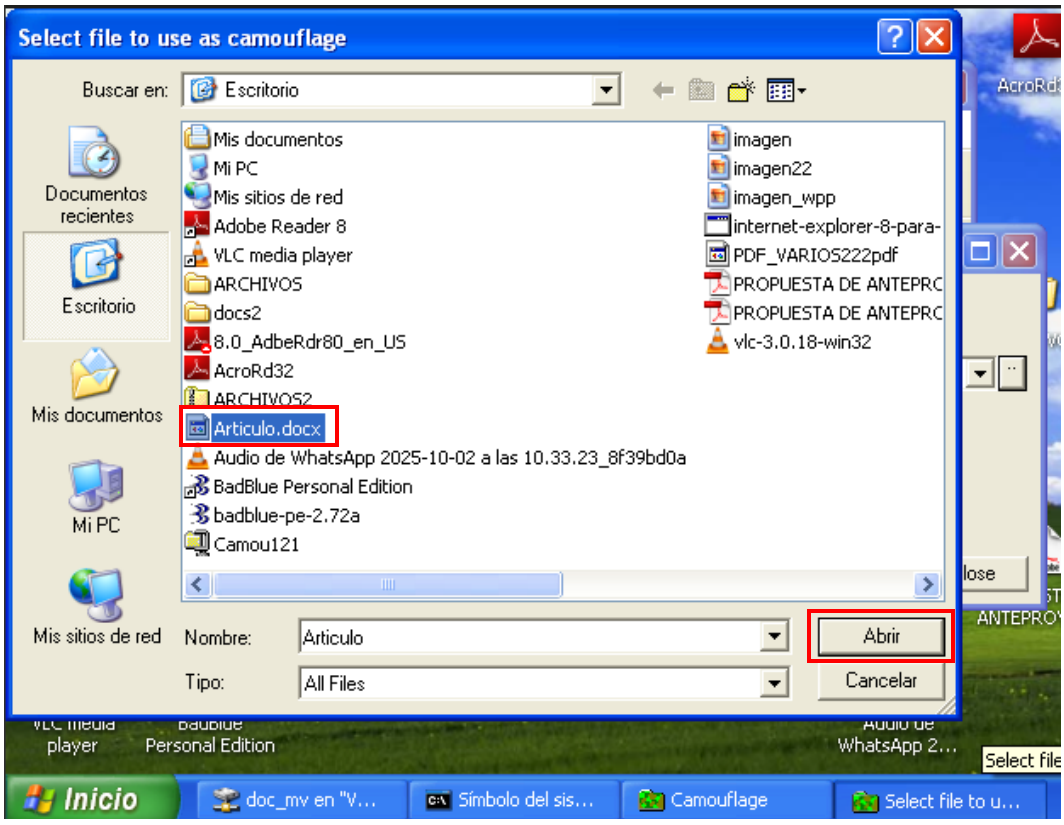

Ilustración 77. Elección del archivo donde se va a camuflar el archivo de gran tamaño

Definir el nombre del archivo camuflado como **"Articulo-copia.docx"** o el nombre que desees.

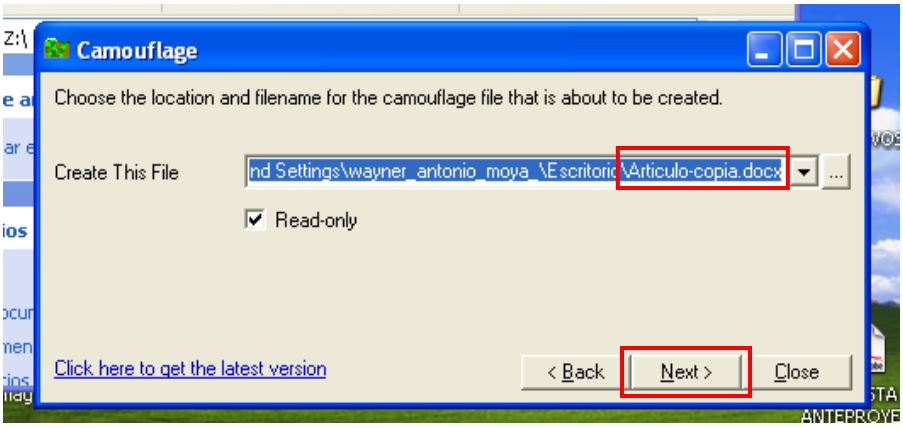

Ilustración 78. Definir nombre del archivo camuflado

Establecer una contraseña que proteja el acceso a el archivo camuflado.

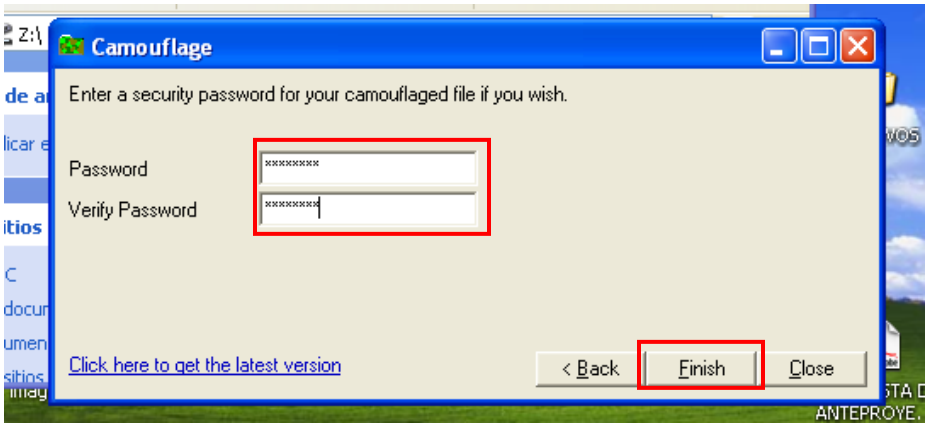

Ilustración 79. Establecer contraseña de protección

El archivo no se pudo camuflar porque solo se puede camuflar 1 archivo si pesa menos de 4 GB, esto también aplica si es en lote (selección de varios archivos) o para una carpeta comprimida en ZIP, la suma de los archivos no puede superar la cantidad de 4 GB.

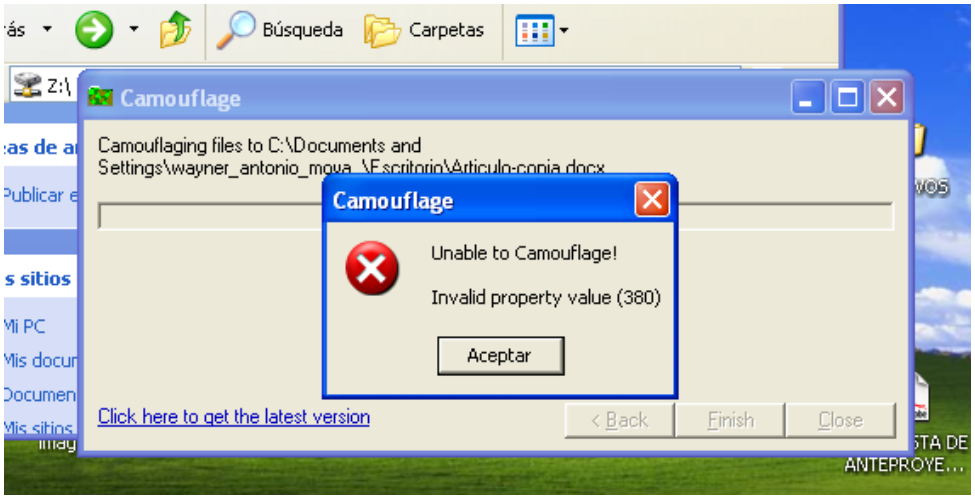

Ilustración 80. Camuflaje no exitoso

5. CAPITULO 2 – EXPLOTACIÓN DE BADBLUE

5.1 Acuerdo de licencia de BadBlue Personal Edition

Ventana de registro y licencia de BadBlue donde se debe ingresar su información personal (nombre completo y correo electrónico) y debe aceptar los términos del acuerdo de licencia antes de poder utilizar el software.

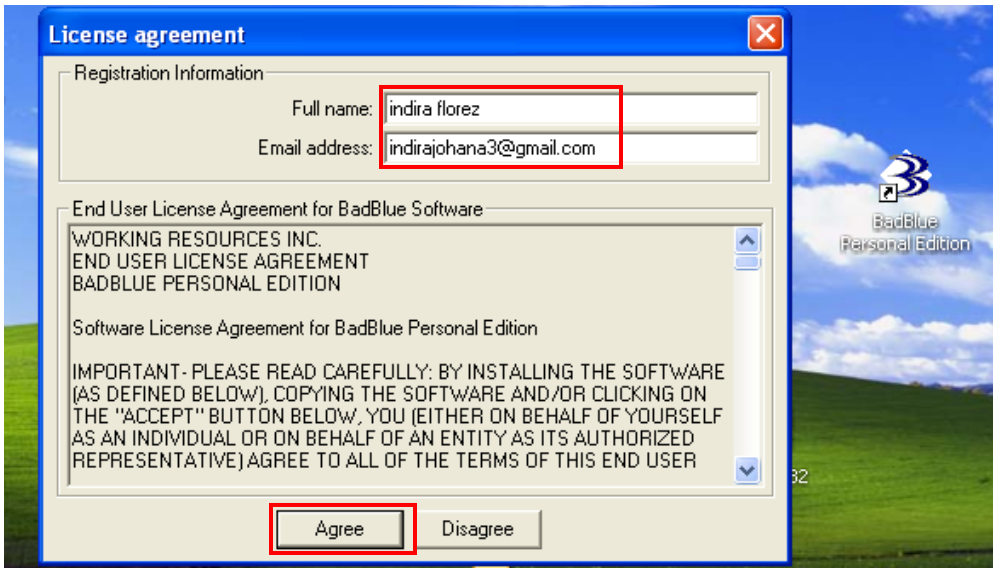

Ilustración 81. Acuerdo de licencia de BadBlue

5.2 Verificación de IP de Windows XP

Captura del símbolo del sistema de Windows XP donde se ejecuta el comando **ipconfig**, mostrando la configuración de red de la máquina virtual. Se identifica la dirección IP **192.168.10.9**, confirmando la conectividad de red necesaria para la explotación.

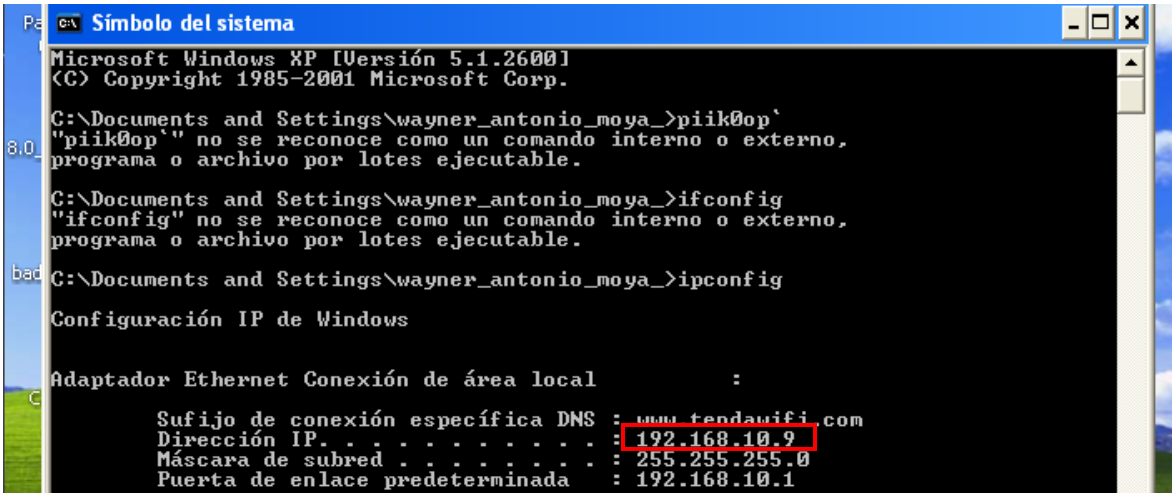

Ilustración 82. Verificación de IP de Windows XP

5.3 Escaneo de red con Nmap desde Kali Linux

En la terminal de Kali Linux ejecutar un escaneo de red con el comando **nmap -sV 192.168.10.0/24**. Los resultados muestran que el host **192.168.10.9 (Windows XP)** tiene varios puertos abiertos, incluyendo el puerto 80 ejecutando **"BadBlue httpd 2.7",** identificando así el servicio vulnerable objetivo.

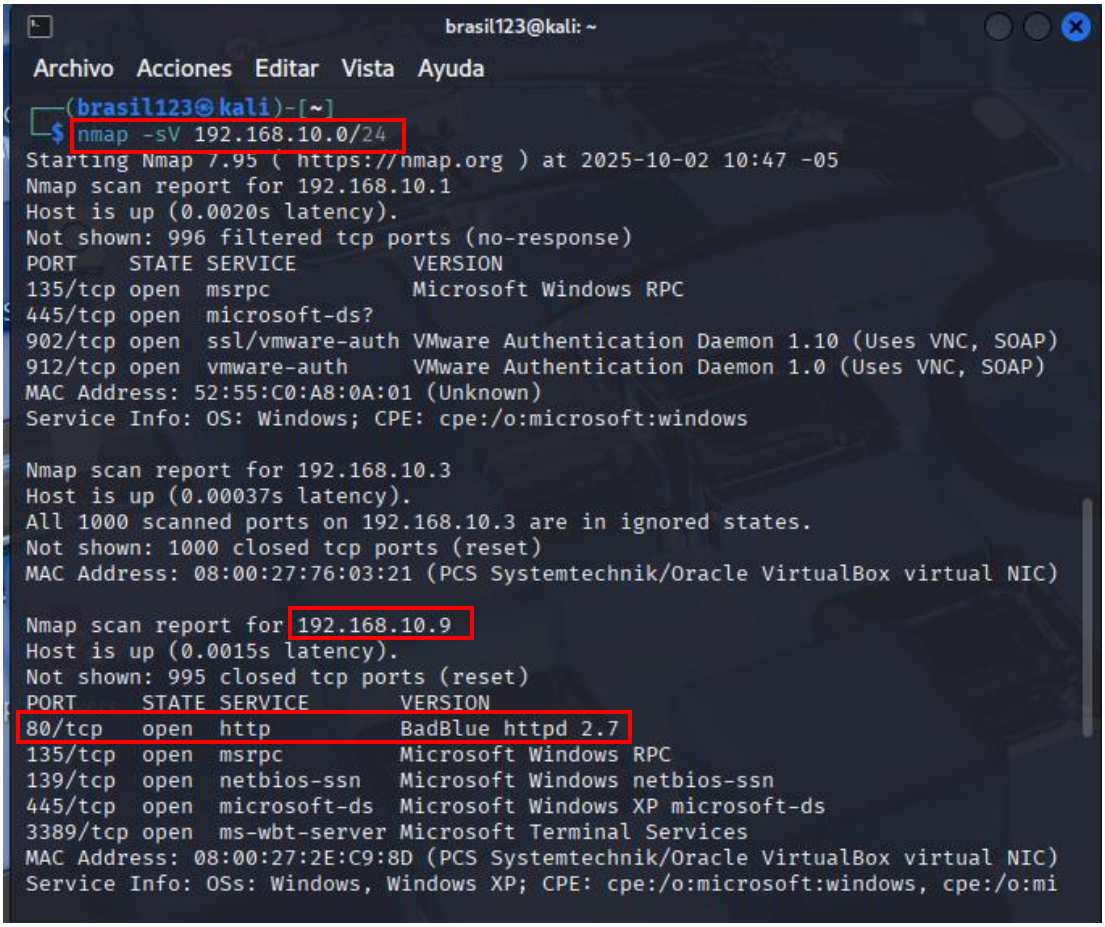

Ilustración 83. Escaneo de red con el comando Nmap

5.4 Acceso a la interfaz web de BadBlue

En el navegador web en Kali Linux accedemos a la interfaz de BadBlue en **http://192.168.10.9**. Se visualiza la página principal del servicio de compartición de archivos BadBlue, confirmando que el servicio está activo y accesible.

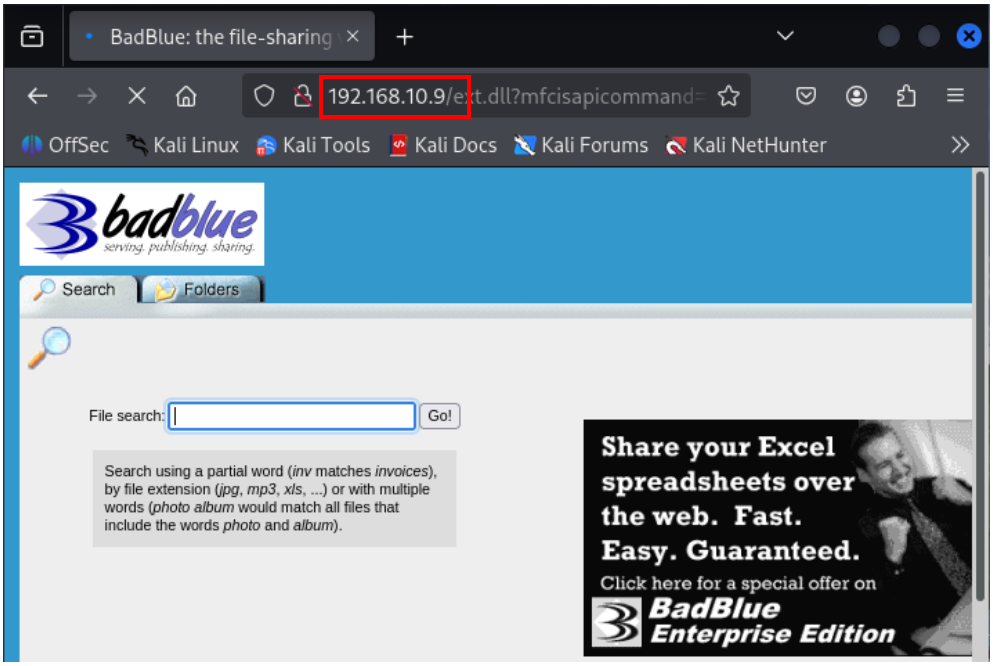

Ilustración 84. Acceso a la interfaz web de BadBlue

5.5 Búsqueda de exploits para BadBlue 2.7

En la terminal de Kali Linux ejecutamos el comando **"searchsploit Badblue 2.7"** para identificar exploits disponibles. Los resultados muestran múltiples vulnerabilidades, incluyendo el exploit que será utilizado.

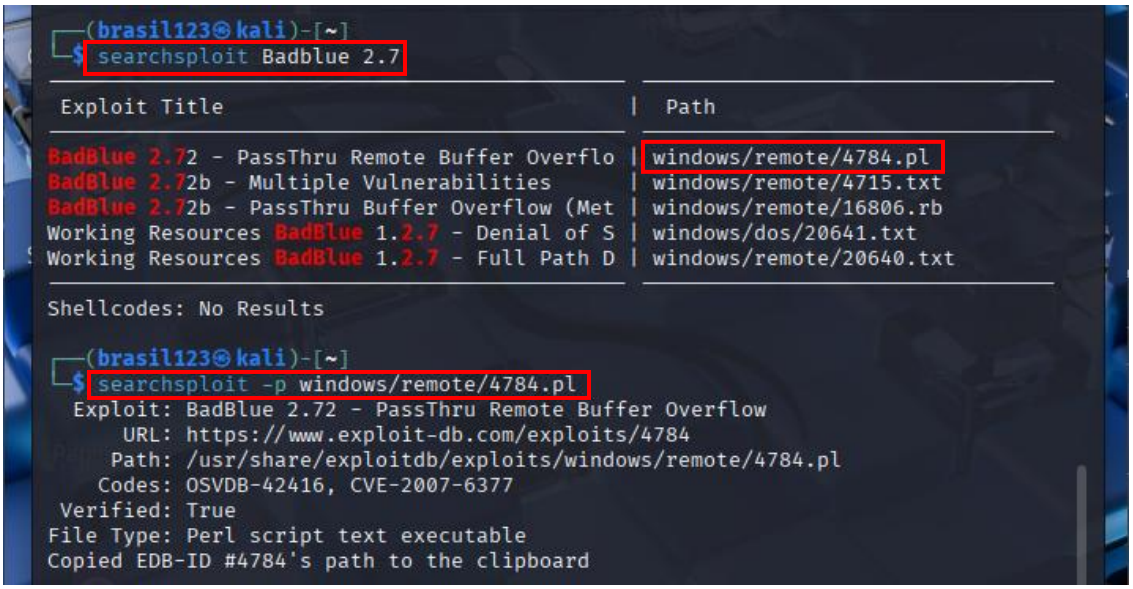

Ilustración 85. Exploit para BadBlue

5.6 Copiar el exploit

Copiar el exploit **4784.pl** desde la base de datos de exploitdb al directorio actual usando **cp /usr/share/exploitdb/exploits/windows/remote/4784.pl .** y luego editarlo con el editor **nano**.

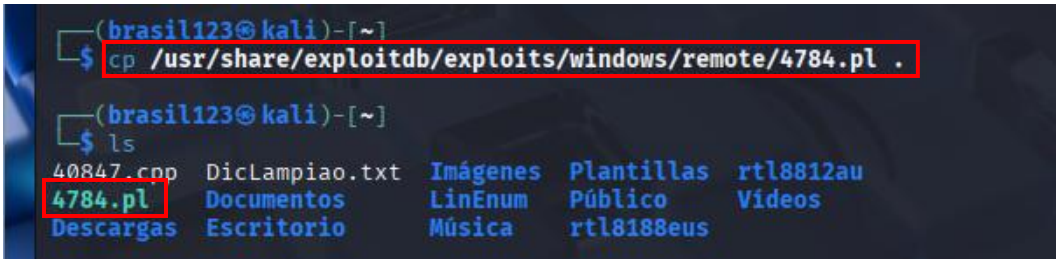

Ilustración 86. Copiar y preparar el exploit para la explotación

5.7 Visualización del código del exploit

Código fuente del exploit usando el comando **cat**.

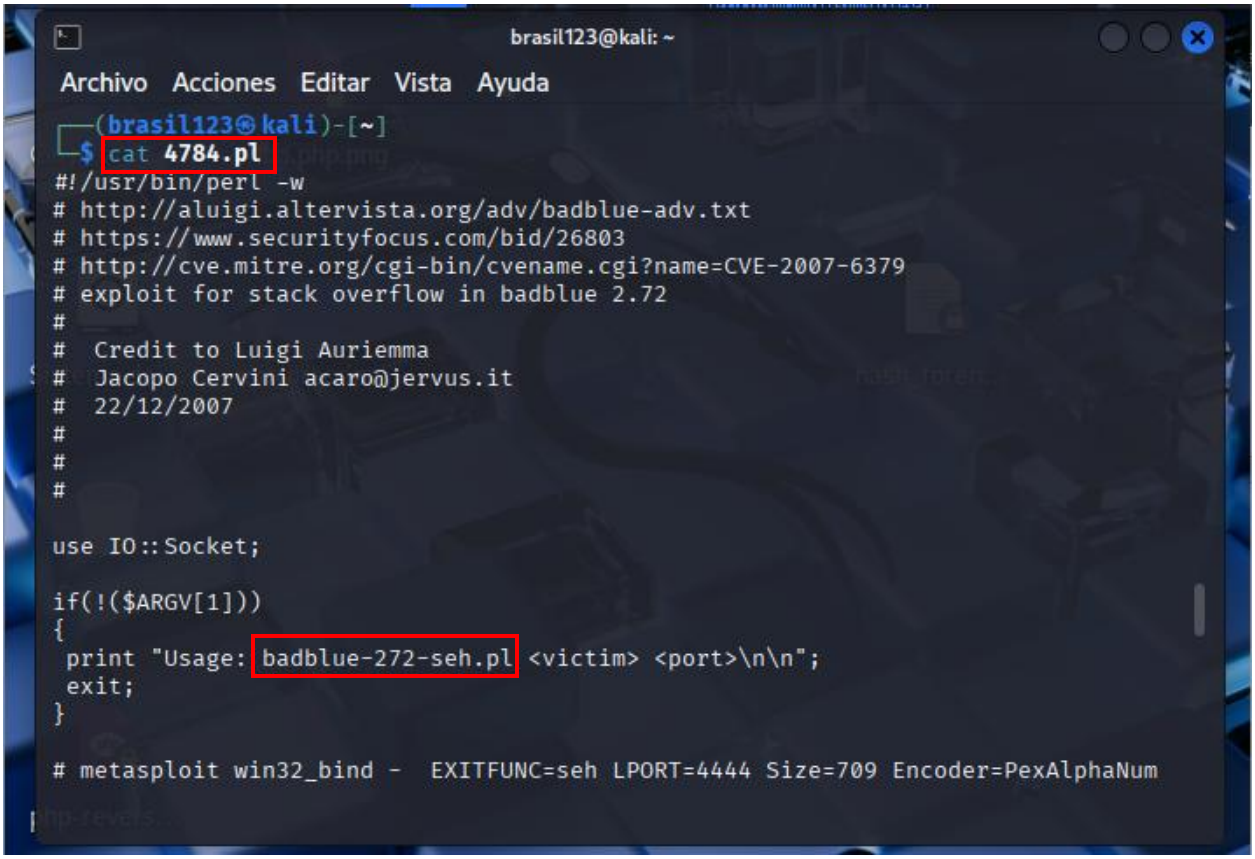

Ilustración 87. Uso del comando cat para ver el código fuente del exploit

5.8 Pegar código fuente del exploit a otro archivo

Luego de visualizar el código fuente del exploit copiamos todo el código y usamos el comando **nano badblue-272-seh.pl** y pegamos el código ahí.

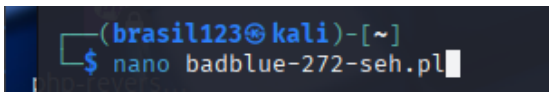

Ilustración 88. Modificación del nombre del archivo exploit

Luego, guardamos con CTRL + O y salimos haciendo CTRL + X.

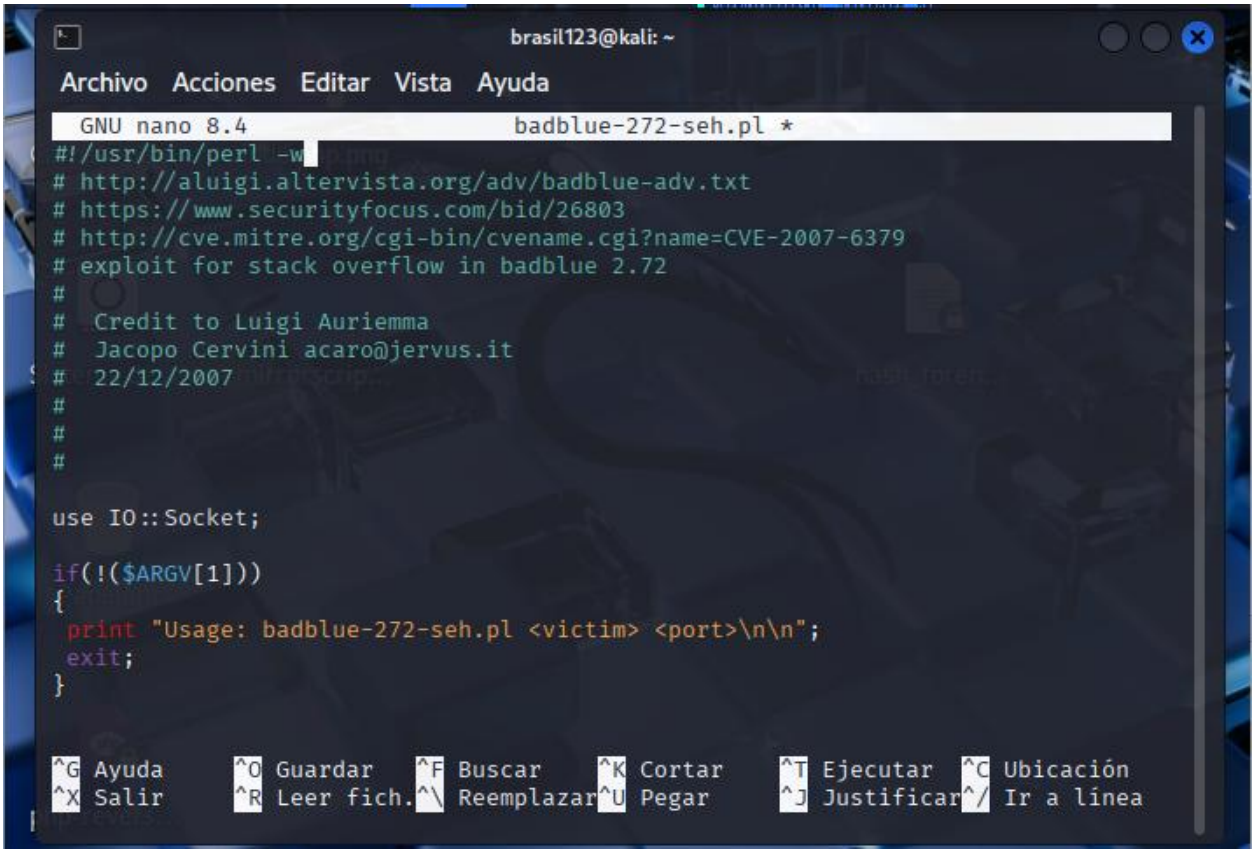

Ilustración 89. Codigo del exploit en el nuevo archivo

5.9 Asignación de permisos de ejecución

Utilizamos el comando **chmod +x badblue-272-seh.pl** para hacer el script ejecutable, seguido de **head -20** para verificar las primeras líneas del código.

Ilustración 90. Asignación de permisos de ejecución

5.10 Ejecución exitosa del exploit

El exploit se ejecuta con **./badblue-272-seh.pl 192.168.10.9 80**, enviando una petición GET maliciosa. Se establece conexión en el puerto 4444 y se obtiene acceso al sistema Windows XP, demostrando la explotación exitosa.

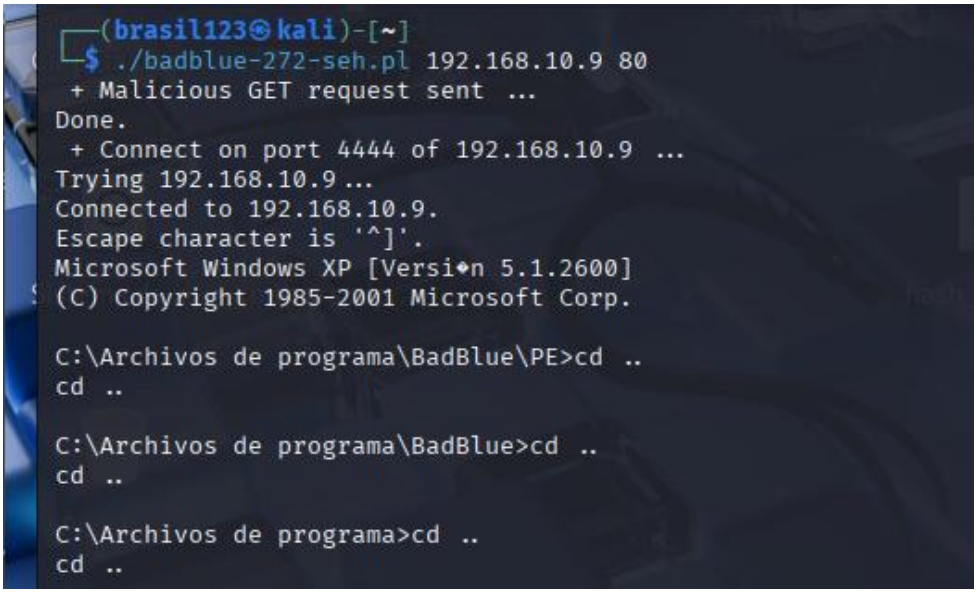

Ilustración 91. Navegación en el sistema comprometido

Comando **systeminfo** ejecutado en la máquina comprometida, mostrando detalles del sistema operativo: Windows XP Professional, confirmando el acceso a información sensible del sistema.

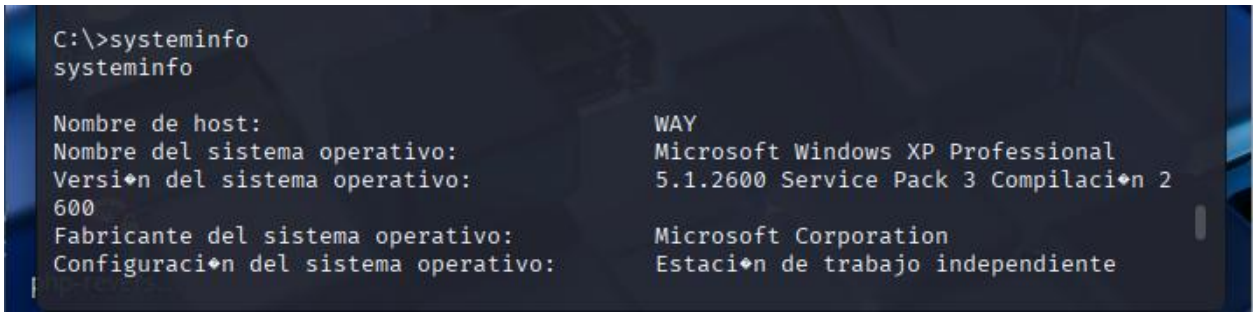

Ilustración 92. Ejecución de systeminfo en el sistema víctima

Comando **net users** mostrando las cuentas de usuario del sistema.

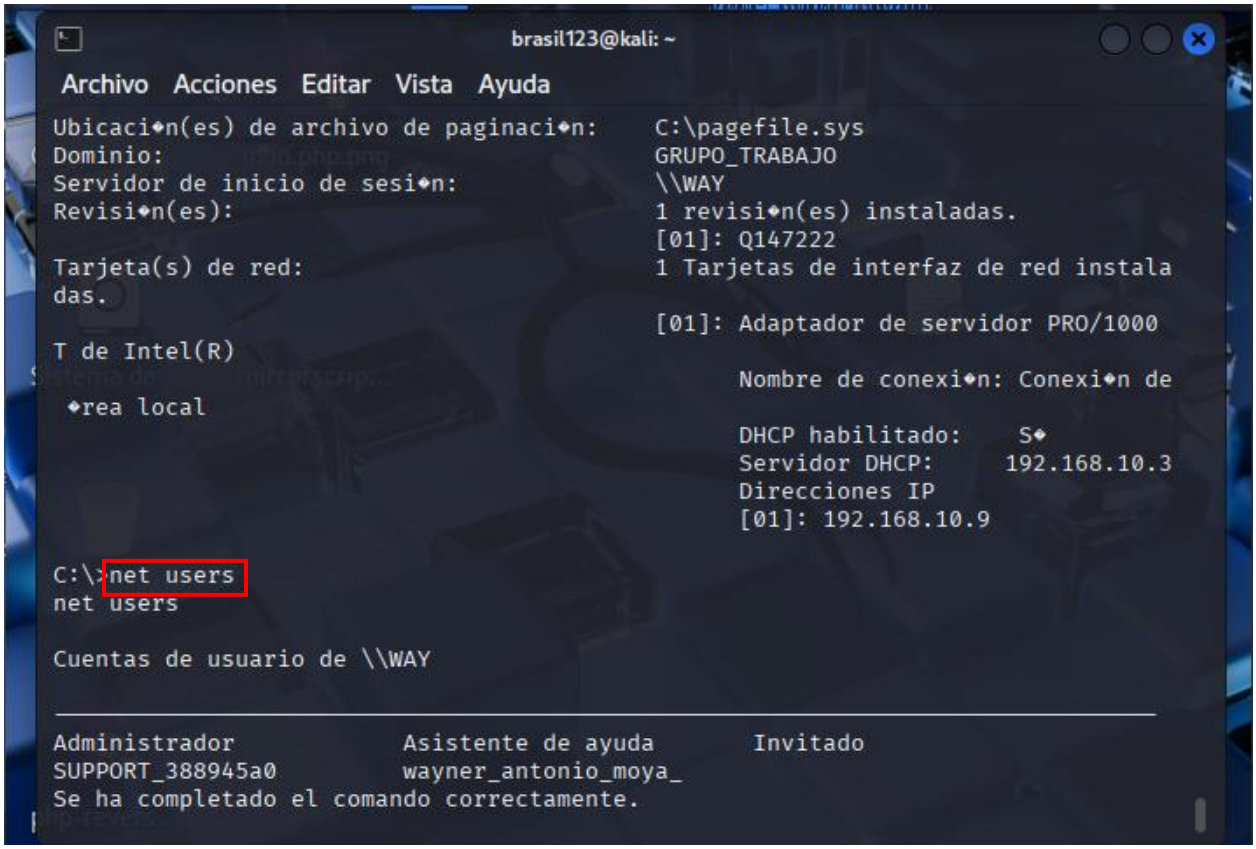

Ilustración 93. Enumeración de usuarios

Comando **tasklist** mostrando todos los procesos activos en el sistema víctima. Se identifica claramente el proceso **"badblue.exe"** con PID 1076, confirmando que el servicio vulnerable sigue ejecutándose mientras se mantiene el acceso.

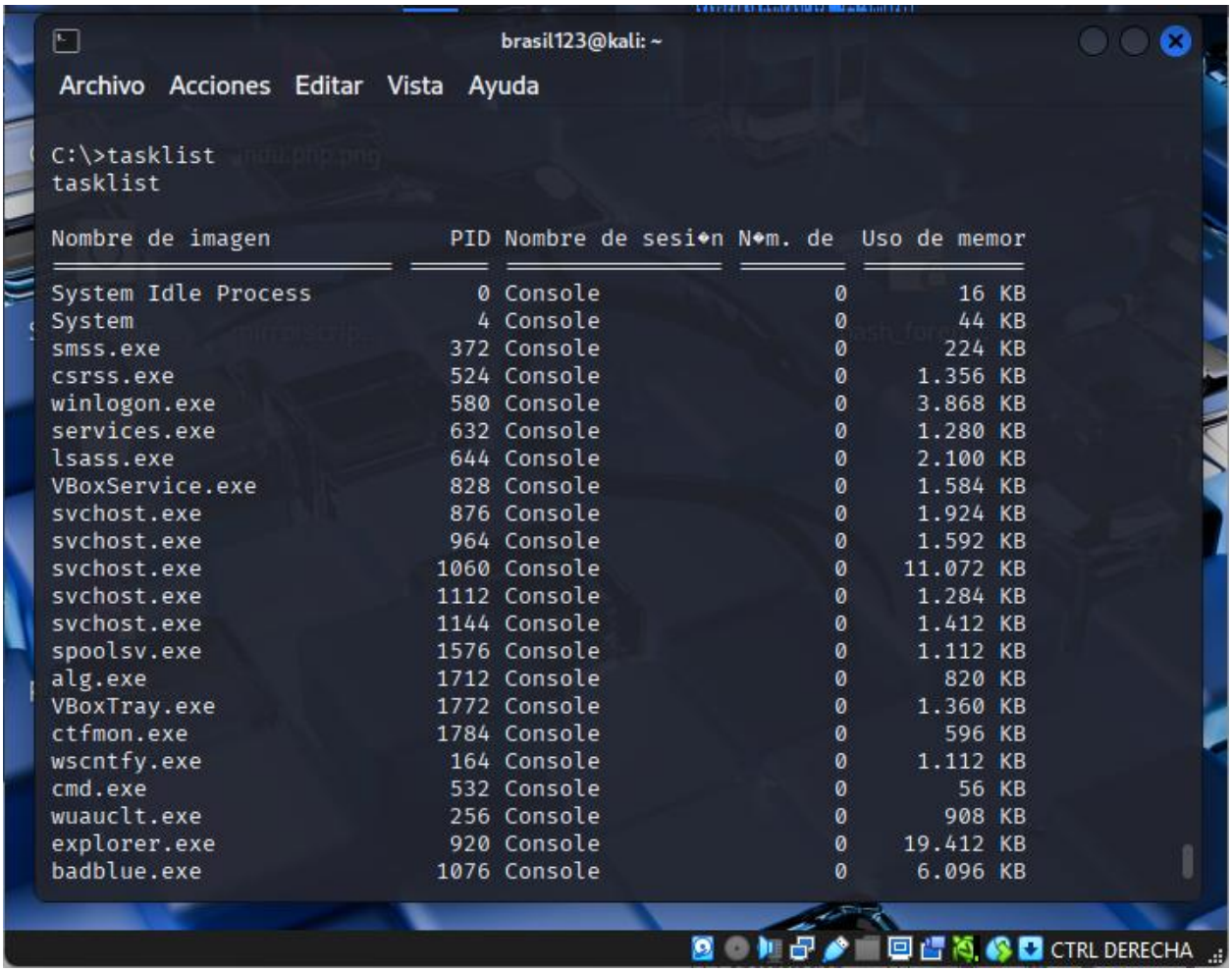

Ilustración 94. Lista de procesos en ejecución

6. CONCLUSIÓN

El laboratorio demostró exitosamente la efectividad de las técnicas de ofuscación de archivos mediante Camouflage, permitiendo ocultar información sensible dentro de archivos comunes sin alterar significativamente su apariencia externa. Se comprobó que es posible camuflar múltiples archivos en formatos JPEG, PDF y ejecutables, aunque con limitaciones en el tamaño máximo de 4 GB por archivo. En la fase de explotación, se confirmó la vulnerabilidad crítica de BadBlue 2.72, obteniendo acceso remoto al sistema Windows XP mediante un exploit de desbordamiento de búfer. La combinación de estas técnicas evidencia la importancia de implementar medidas de seguridad tanto para la protección de información confidencial como para la correcta configuración y actualización de servicios expuestos en red. Este trabajo refuerza los conceptos de seguridad ofensiva y defensiva, proporcionando valiosa experiencia práctica en técnicas relevantes para la auditoría de seguridad informática.

7. BIBLIOGRAFIA

Morales, R. S. (25). *INFORME DE LABORATORIO 01*. Quibdó, Colombia: Universidad Tecnologia del Chocó Diego Luis Córdoba. Recuperado el 9 de 10 de 2025