

Un atacante sabe que muchos tipos diferentes de archivos pueden contener todo tipo de información oculta y que rastrear o encontrar estos archivos puede ser una tarea casi imposible. Por lo tanto, utilizan técnicas taquigráficas para ocultar datos. Esto les permite recuperar mensajes de su base de operaciones y enviar actualizaciones sin que se detecte ningún indicio de actividad maliciosa.

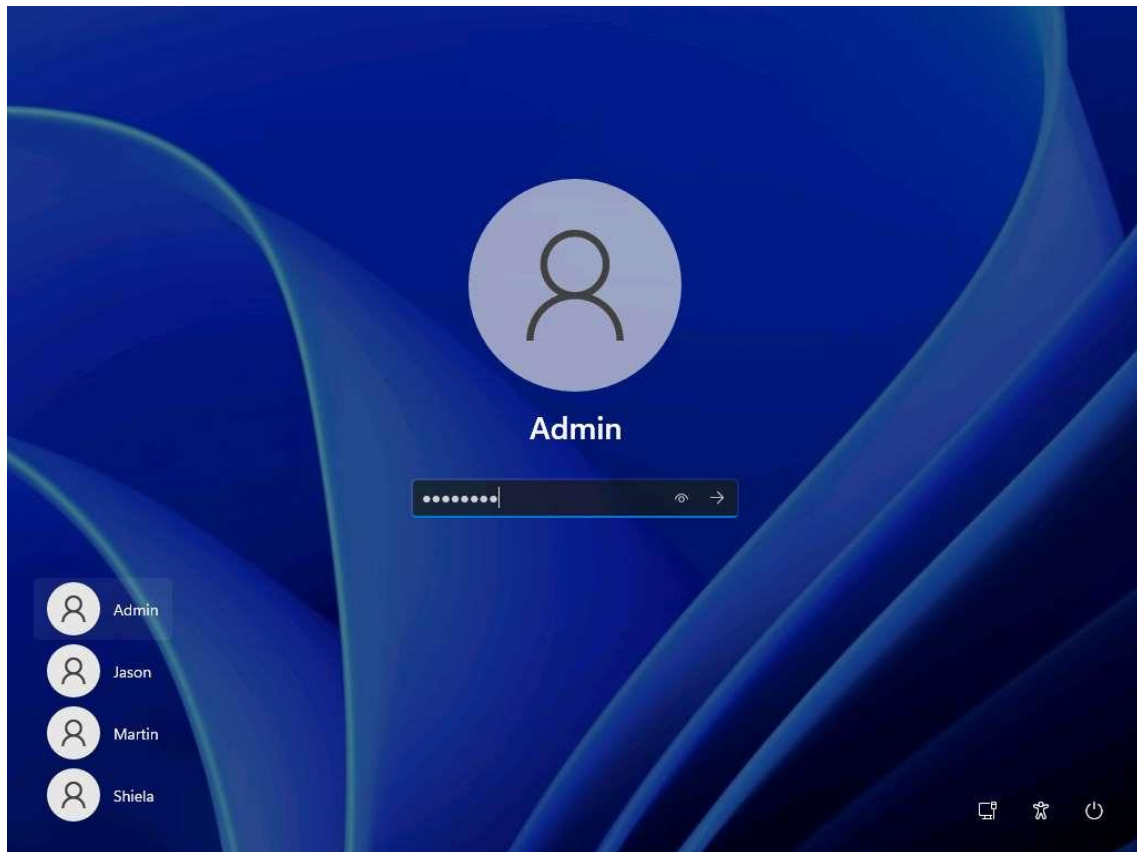
Estos mensajes pueden colocarse a plena vista, y los servidores que suministran estos archivos nunca sabrán que llevan contenido sospechoso. Encontrar estos mensajes es como encontrar la proverbial "aguja" en el pajar de la World Wide Web.

La esteganografía es el arte y la ciencia de escribir mensajes ocultos de tal manera que nadie más que el destinatario previsto sepa de la existencia del mensaje. La esteganografía se clasifica en función del medio utilizado para ocultar el archivo. Un hacker ético profesional o un probador de penetración debe tener un buen conocimiento de varias técnicas de esteganografía.

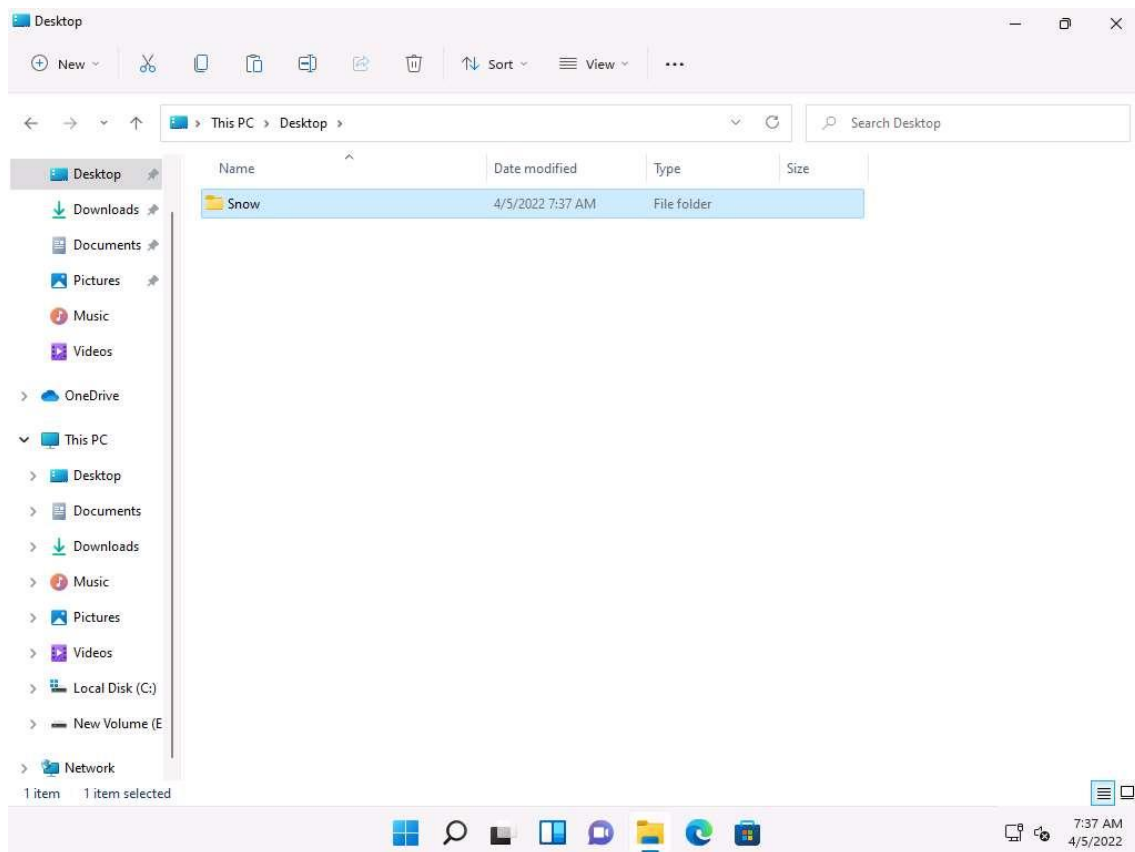
La esteganografía de espacios en blanco se utiliza para ocultar mensajes en texto ASCII añadiendo espacios en blanco al final de las líneas. Como los espacios y los tabuladores no suelen ser visibles en los visualizadores de texto, el mensaje se oculta eficazmente a los observadores casuales. Si se utiliza el cifrado incorporado, el mensaje no puede leerse aunque se detecte. Para realizar la esteganografía de espacios en blanco, se utilizan varias herramientas de esteganografía, como Snow. Snow es un programa que oculta mensajes en archivos de texto añadiendo tabuladores y espacios al final de las líneas, y que extrae los mensajes ocultos de los archivos que los contienen. El usuario oculta los datos en el archivo de texto añadiendo secuencias de hasta siete espacios, intercalados con tabulaciones.

Aquí, vamos a ocultar datos utilizando la herramienta de esteganografía Whitespace Snow.

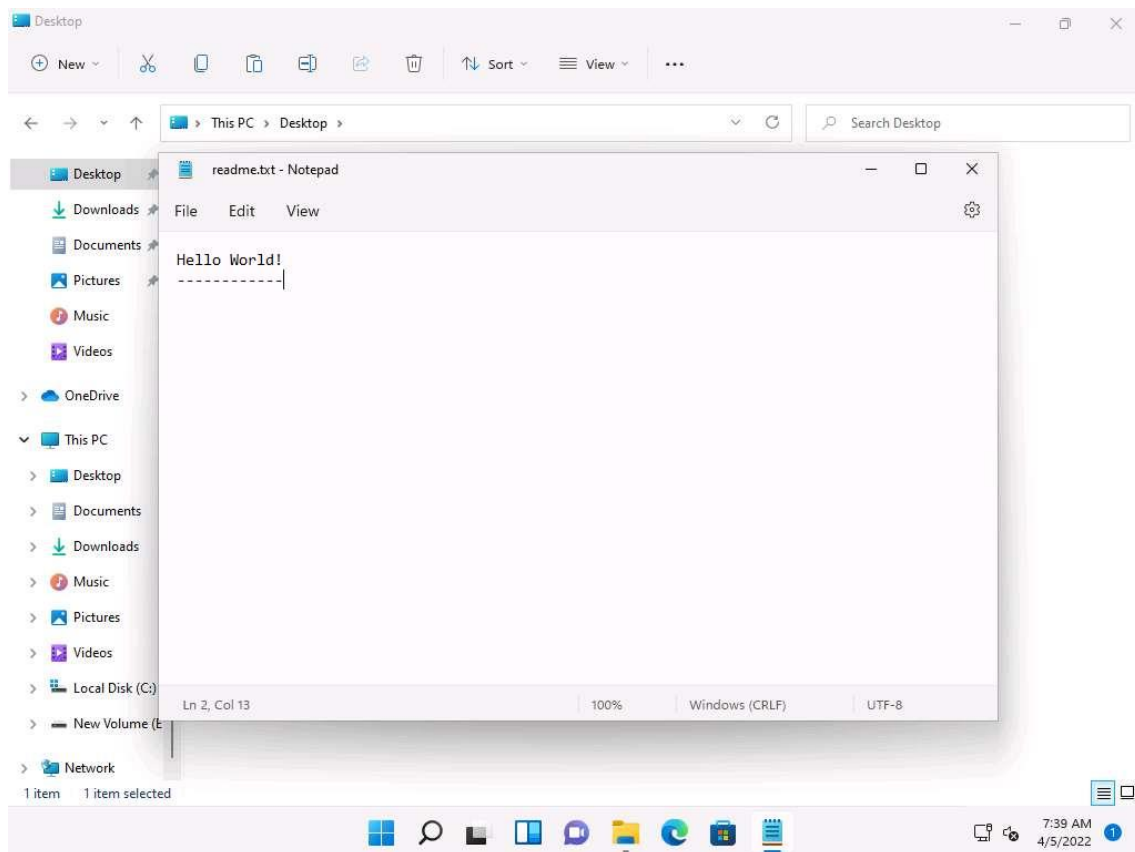
1. Haga clic en **Windows 11** para cambiar a la máquina **Windows 11**.
2. Pulse **Ctrl+Alt+Supr** para activar la máquina, por defecto, el perfil de usuario seleccionado, escriba **la** Contraseña y pulse **Intro** para iniciar sesión.




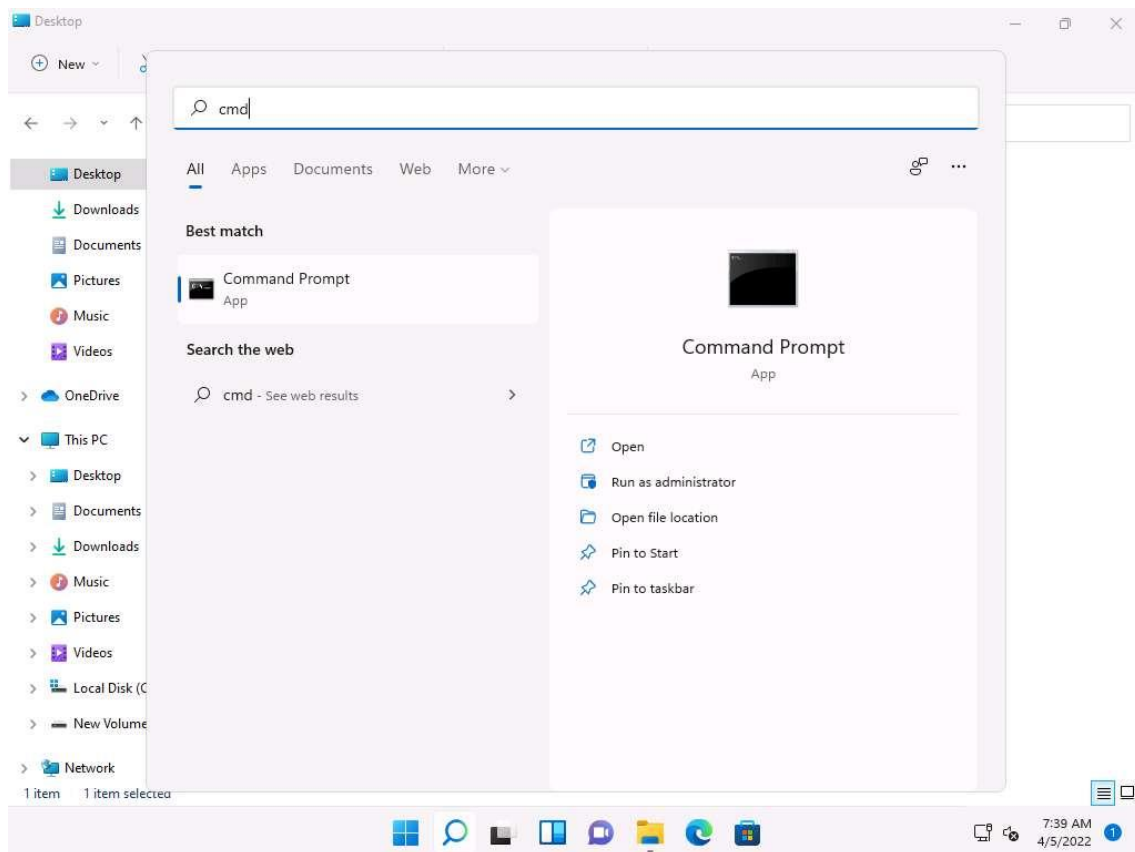
3. Navegue hasta `C:\Tools\Steganography Tools\Whitespace Steganography Tools`, copie la carpeta Snow y péguela en el Escritorio.



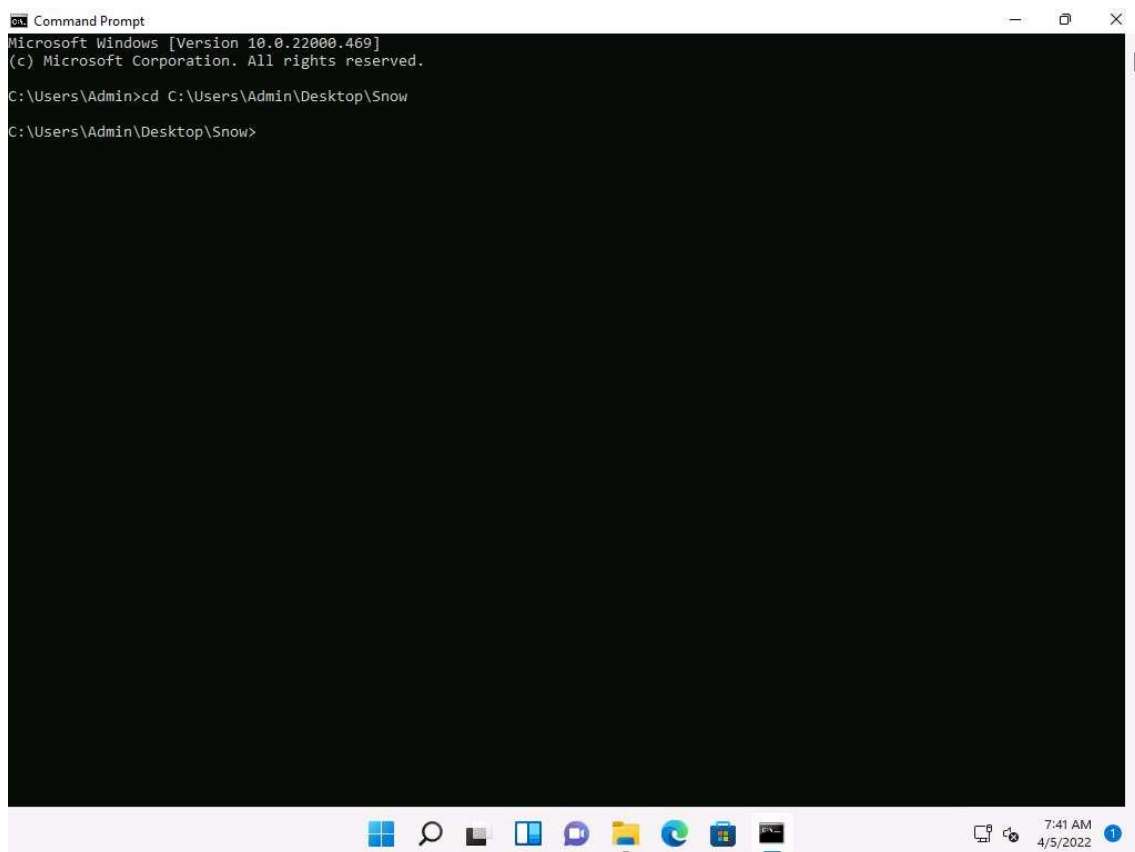
4. Cree un archivo **en el Bloc de notas**, escriba **¡Hola mundo!** y pulse **Intro**; a continuación, mantenga pulsada la tecla **guión** para dibujar una línea discontinua debajo del texto. Guarde el archivo como **readme.txt** en la carpeta donde se encuentra **SNOW.EXE** (**C:\Users\Admin\Desktop\Snow**).



5. Ahora, haga clic en el icono **Buscar** () en el **Escritorio**. Escriba **cmd** en el campo de búsqueda, el **símbolo del sistema** aparece en los resultados, haga clic en **Abrir** para iniciarlo.

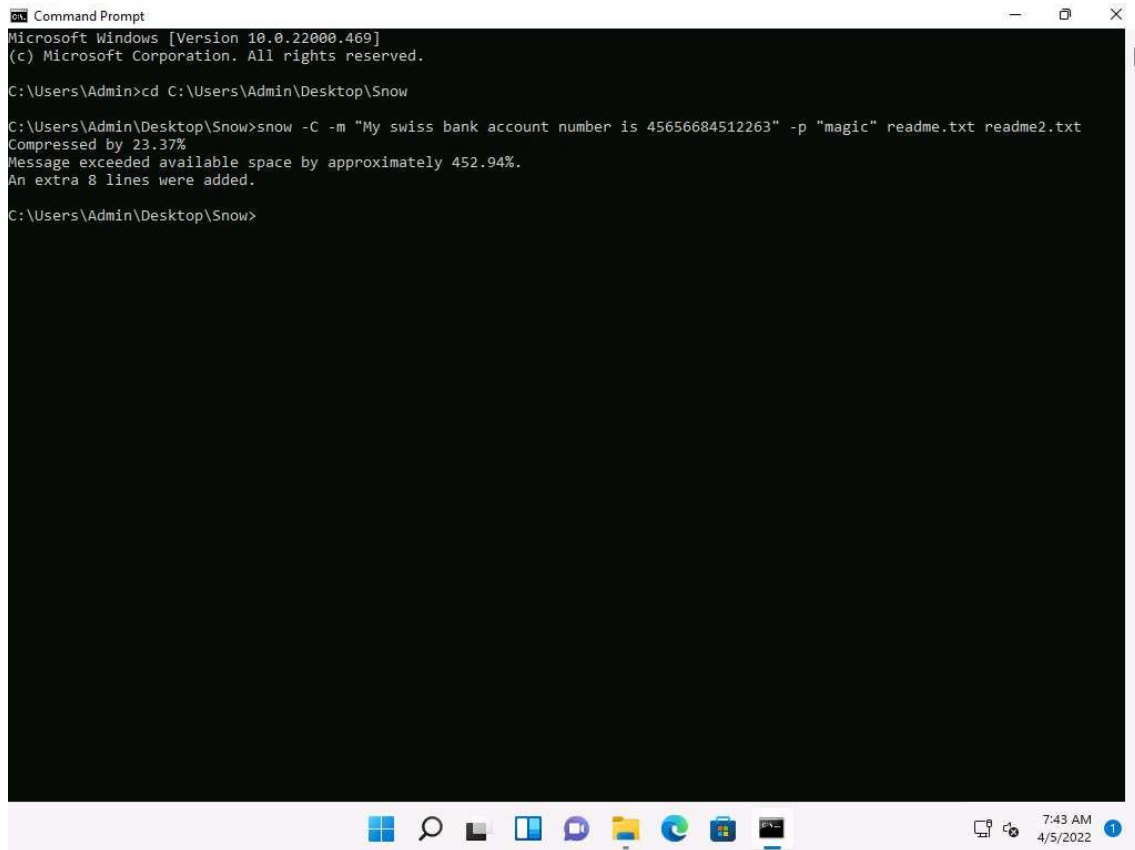


6. En la ventana Símbolo del sistema, escriba `cd C:\Usuarios\Administrador\Desktop\Snow` y pulse Intro.



7. Escribe `snow -C -m "Mi número de cuenta bancaria suiza es 45656684512263" -p "magic" readme.txt readme2.txt` y pulsa Intro.

Nota: (Aquí, **magic** es la contraseña, pero puede escribir la que desee. **readme2.txt** es el nombre del archivo que se creará automáticamente en la misma ubicación).



```
Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>cd C:\Users\Admin\Desktop\Snow

C:\Users\Admin\Desktop\Snow>snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt
Compressed by 23.37%
Message exceeded available space by approximately 452.94%.
An extra 8 lines were added.

C:\Users\Admin\Desktop\Snow>
```

8. Ahora, los datos ("Mi número de cuenta en un banco suizo es 45656684512263") se ocultan dentro del archivo `readme2.txt` con el contenido de `readme.txt`.
9. El archivo `readme2.txt` se ha convertido en una combinación de `readme.txt` + Mi número de cuenta en un banco suizo es 45656684512263.
10. Ahora, escriba **`snow -C -p "magic" readme2.txt`**. Se mostrará el contenido de `readme.txt` (la contraseña es `magic`, que se introdujo al ocultar los datos en el **paso 7**).

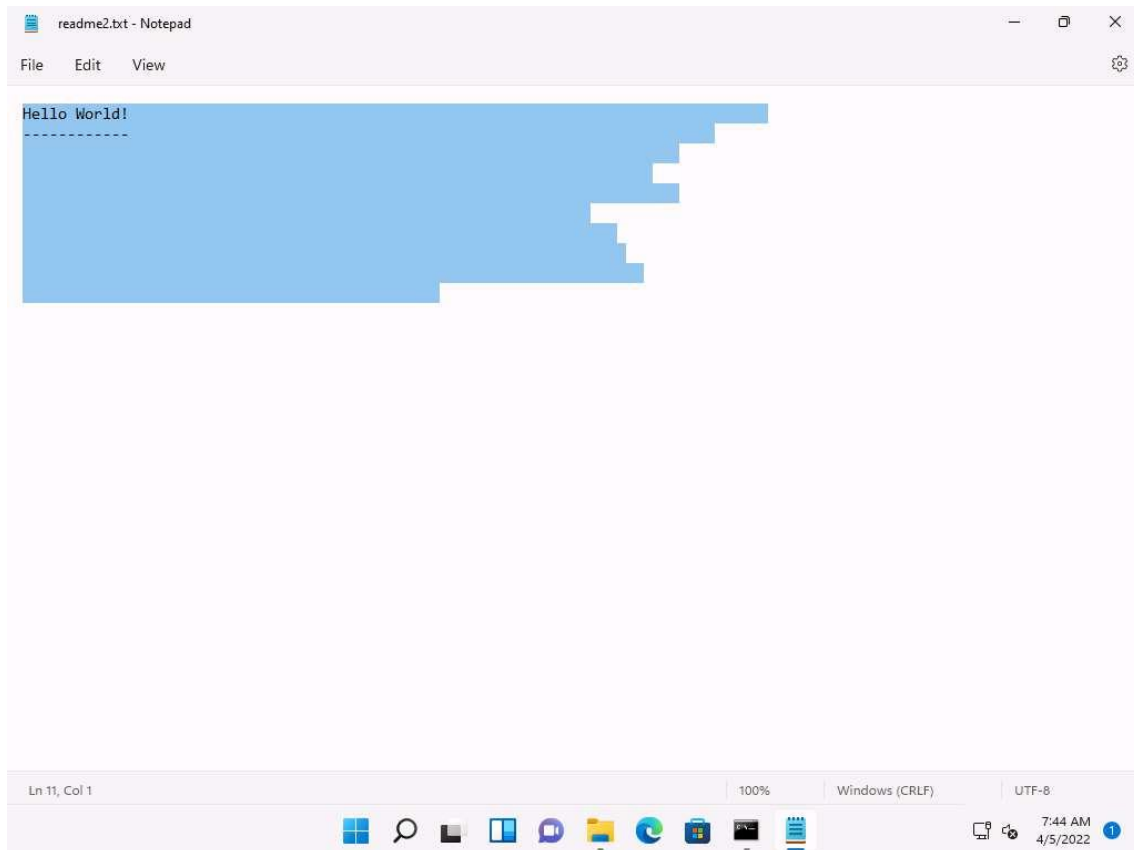
```
Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>cd C:\Users\Admin\Desktop\Snow

C:\Users\Admin\Desktop\Snow>snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt
Compressed by 23.37%
Message exceeded available space by approximately 452.94%.
An extra 8 lines were added.

C:\Users\Admin\Desktop\Snow>snow -C -p "magic" readme2.txt
My swiss bank account number is 45656684512263
C:\Users\Admin\Desktop\Snow>
```

11. Para comprobar el archivo en la GUI, abra el **readme2.txt** en el **Bloc de notas** y vaya a **Editar --> Seleccionar todo**. Verá los datos ocultos dentro de **readme2.txt** en forma de espacios y tabulaciones, como se muestra en la captura de pantalla.



12. Con esto concluye la demostración de cómo ocultar datos utilizando la esteganografía de espacios en blanco.
13. Cierre todas las ventanas abiertas y documente toda la información obtenida.

ESTEGANOGRAFÍA DE IMÁGENES UTILIZANDO OPENSTEGO Y STEGONLINE

Las imágenes son objetos de encubrimiento muy utilizados en esteganografía. En la esteganografía de imágenes, el usuario oculta la información en archivos de imagen de distintos formatos, como .PNG, .JPG o .BMP.


OPENSTEGO

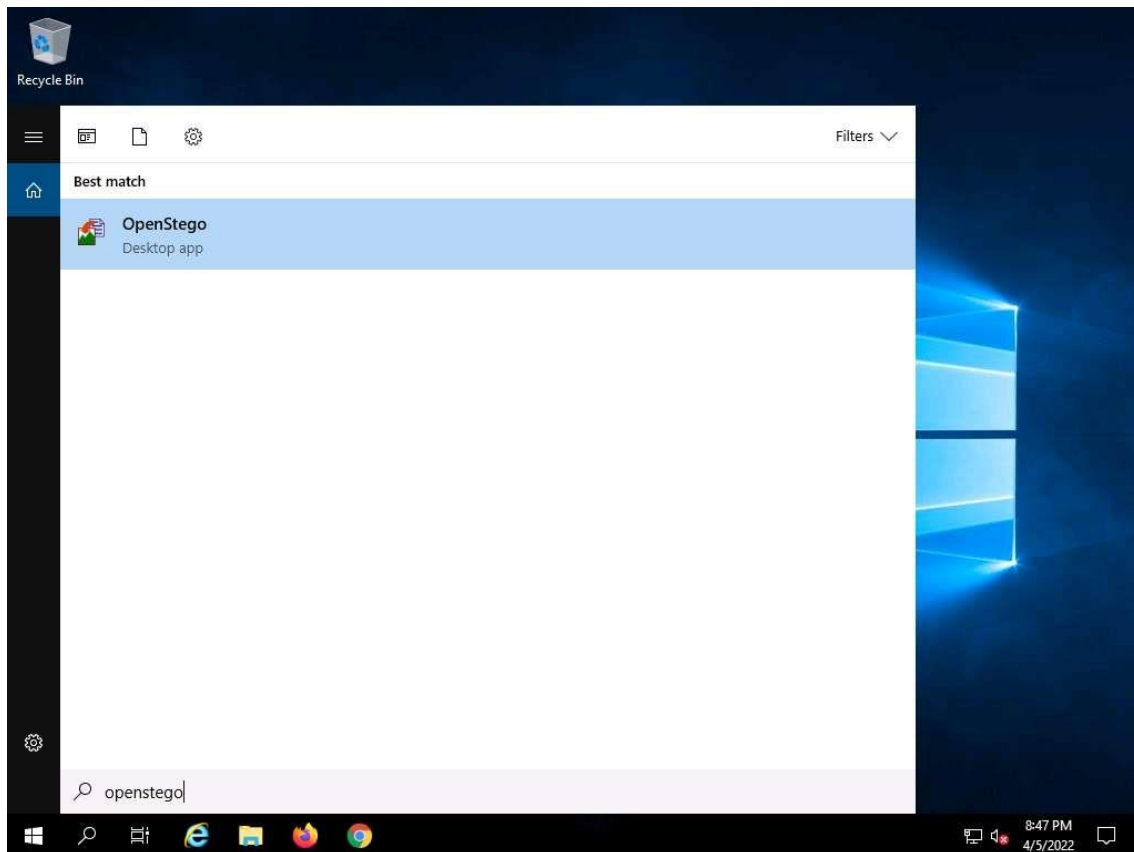
OpenStego es una herramienta de esteganografía de imágenes que oculta datos dentro de las imágenes. Es una aplicación basada en Java que admite el cifrado de datos mediante contraseña para una capa adicional de seguridad. Utiliza el algoritmo DES para el cifrado de datos, junto con el hashing MD5 para obtener la clave DES a partir de la contraseña proporcionada.

STEGONLINE

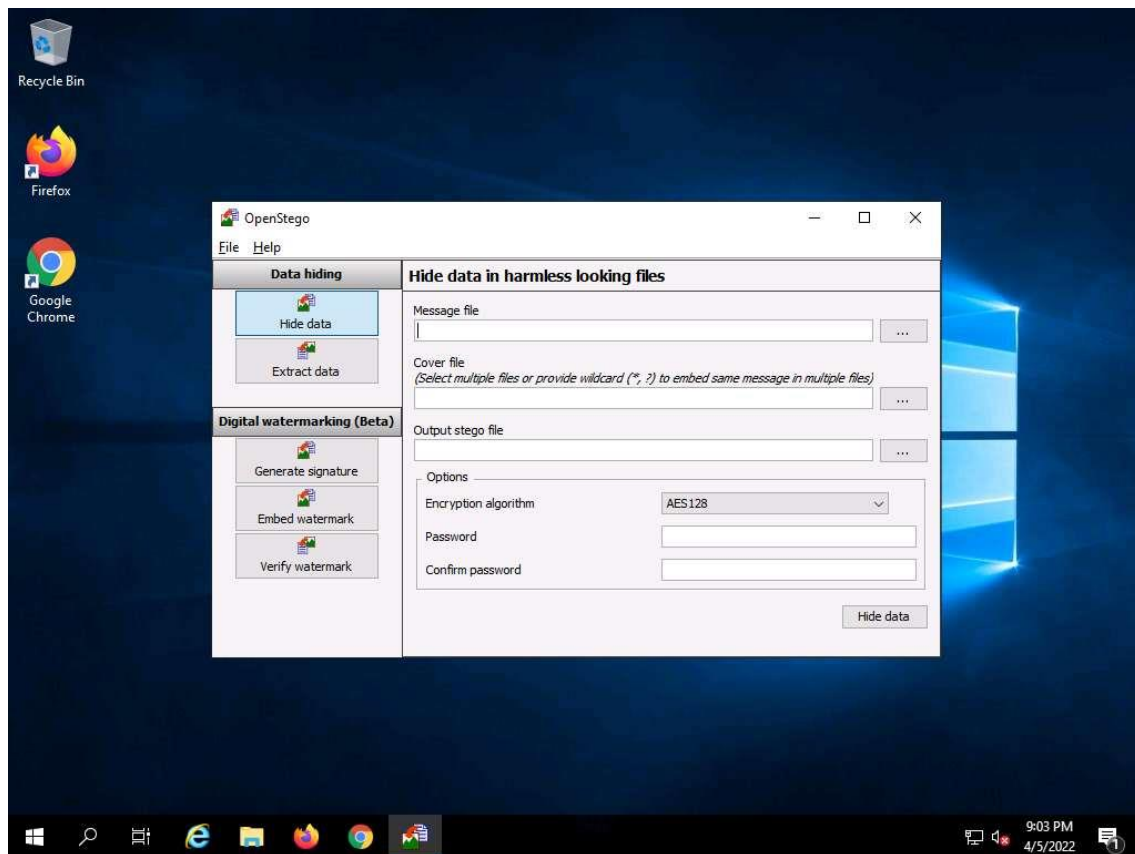
StegOnline es un port de StegSolve basado en web, mejorado y de código abierto. Puede utilizarse para navegar por los 32 planos de bits de la imagen, extraer e incrustar datos mediante técnicas de esteganografía LSB y ocultar imágenes dentro de otros planos de bits de la imagen.

Aquí mostraremos cómo se puede ocultar texto dentro de una imagen utilizando las herramientas OpenStego y StegOnline.

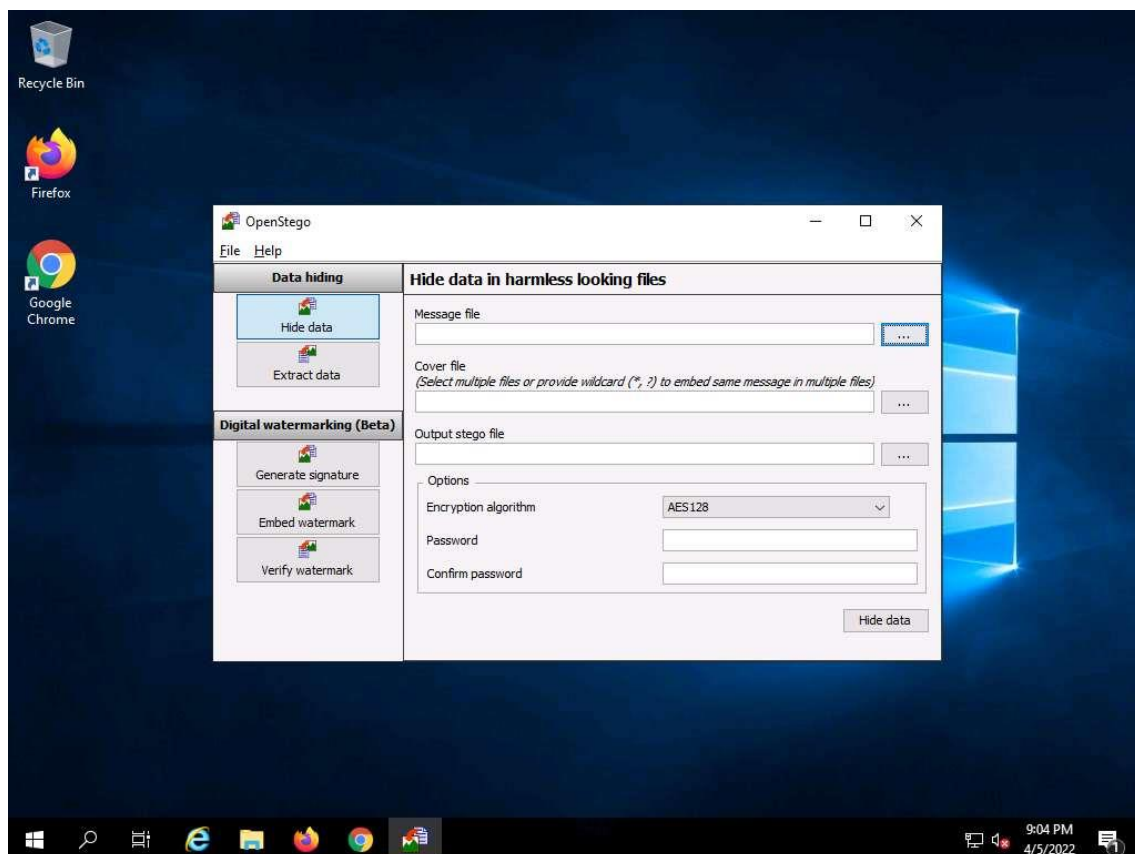
1. Haga clic en Windows Server para cambiar al equipo Windows Server.
2. Haga clic en el icono **Buscar** () en el **Escritorio**. Escriba **openstego** en el campo de búsqueda, **OpenStego** aparecerá en los resultados, haga clic en **OpenStego** para iniciarlo.



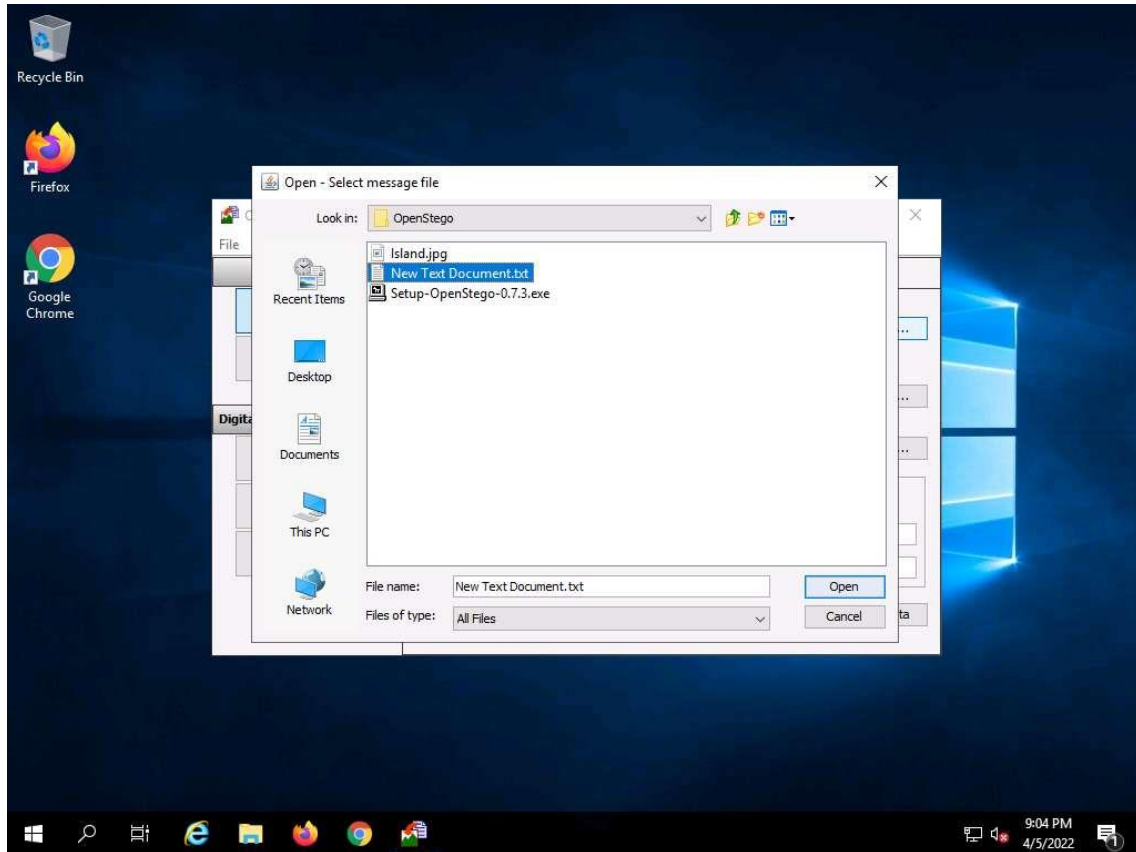
3. Aparecerá la ventana principal de **OpenStego**, como se muestra en la captura de pantalla.



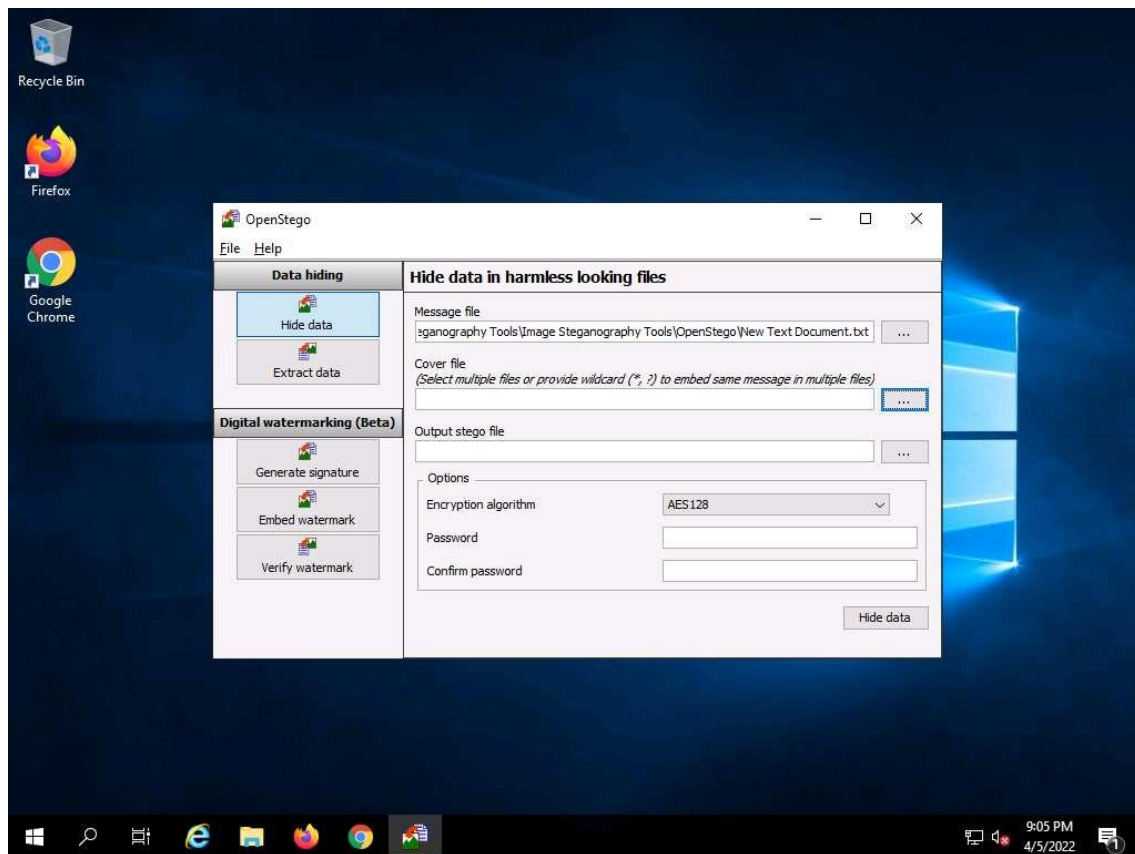
4. Haga clic en el botón de elipsis situado junto a la sección Archivo de mensajes.



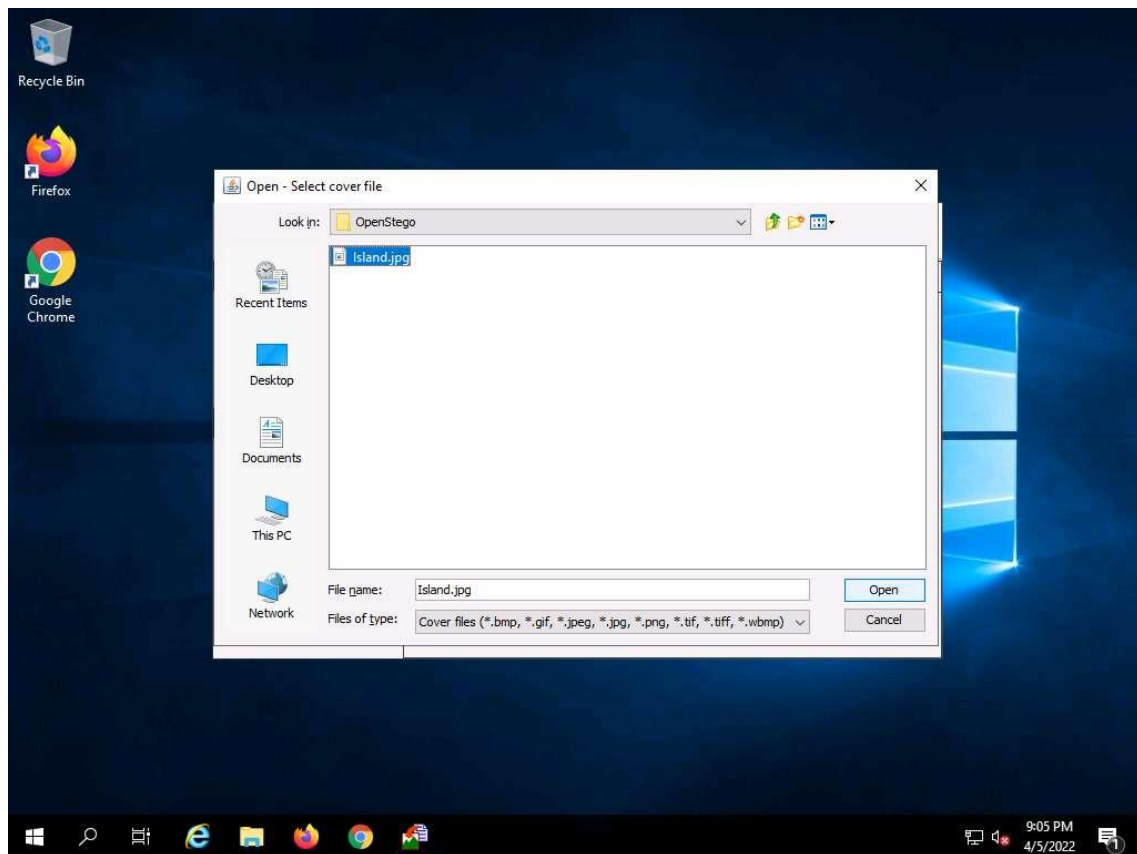
5. Aparecerá la ventana Abrir - Seleccionar archivo de mensaje. Navegue hasta C:\Tools\Steganography Tools\AbrirStego, seleccione Nuevo Documento de Texto.txt, y haga clic en Abrir. Supongamos que el archivo de texto contiene información confidencial, como números de tarjetas de crédito y números PIN.



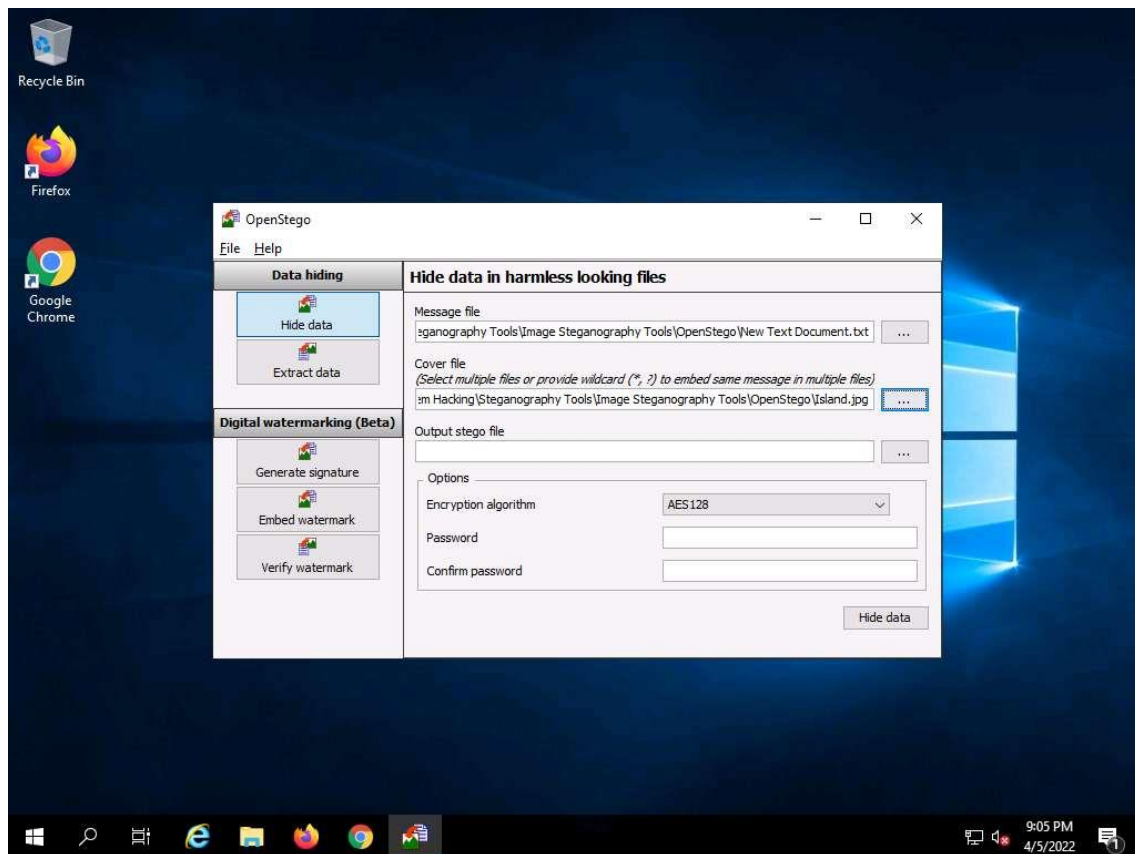
6. La ubicación del archivo seleccionado aparece en el campo **Archivo de mensajes**.
7. Haga clic en el botón **de elipsis** situado junto a **Carátula**.



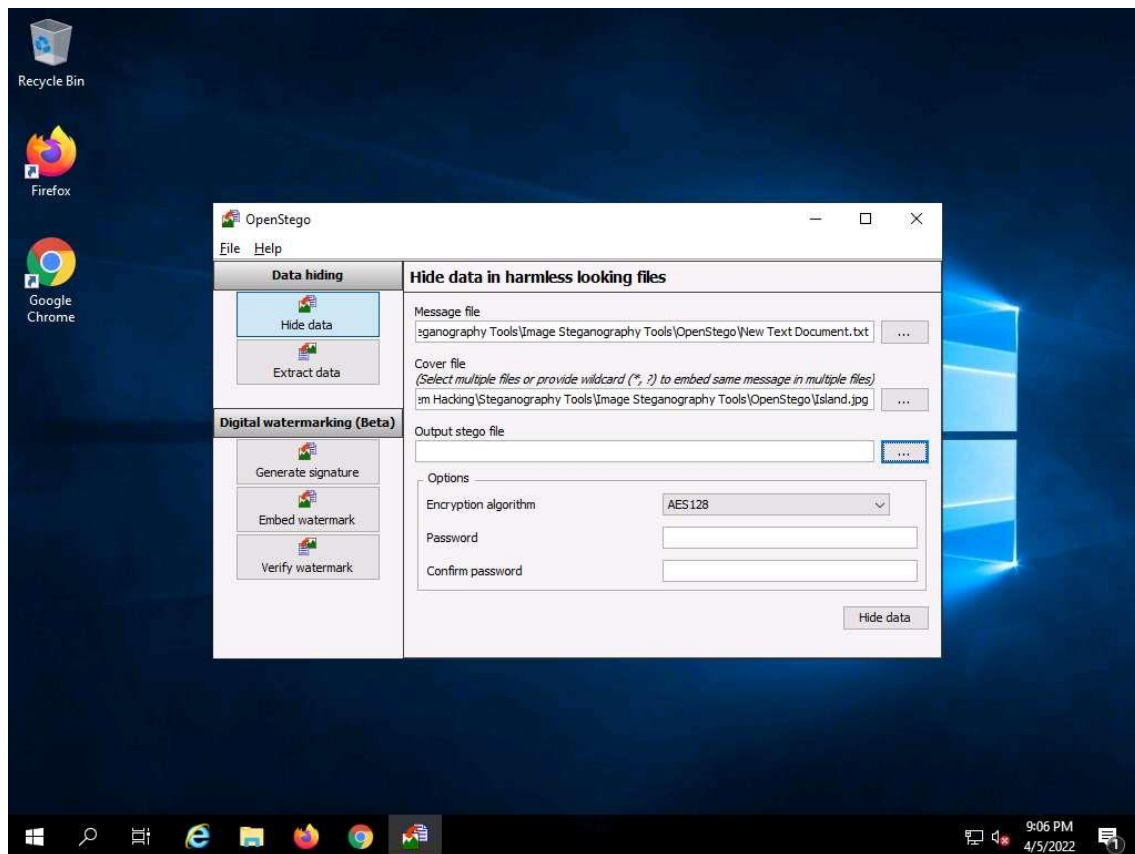
8. Aparecerá la ventana Abrir - Seleccionar Archivo de Portada. Navegue hasta C:\Tools\Steganography Tools\Whitespace Steganography Tools \OpenStego, seleccione Island.jpg, y haga clic en Abrir.



9. Ahora, se cargan tanto el **Archivo de Mensaje** como el **Archivo de Cubierta**. Al realizar esteganografía, el archivo de mensaje se ocultará en el archivo de cubierta designado.

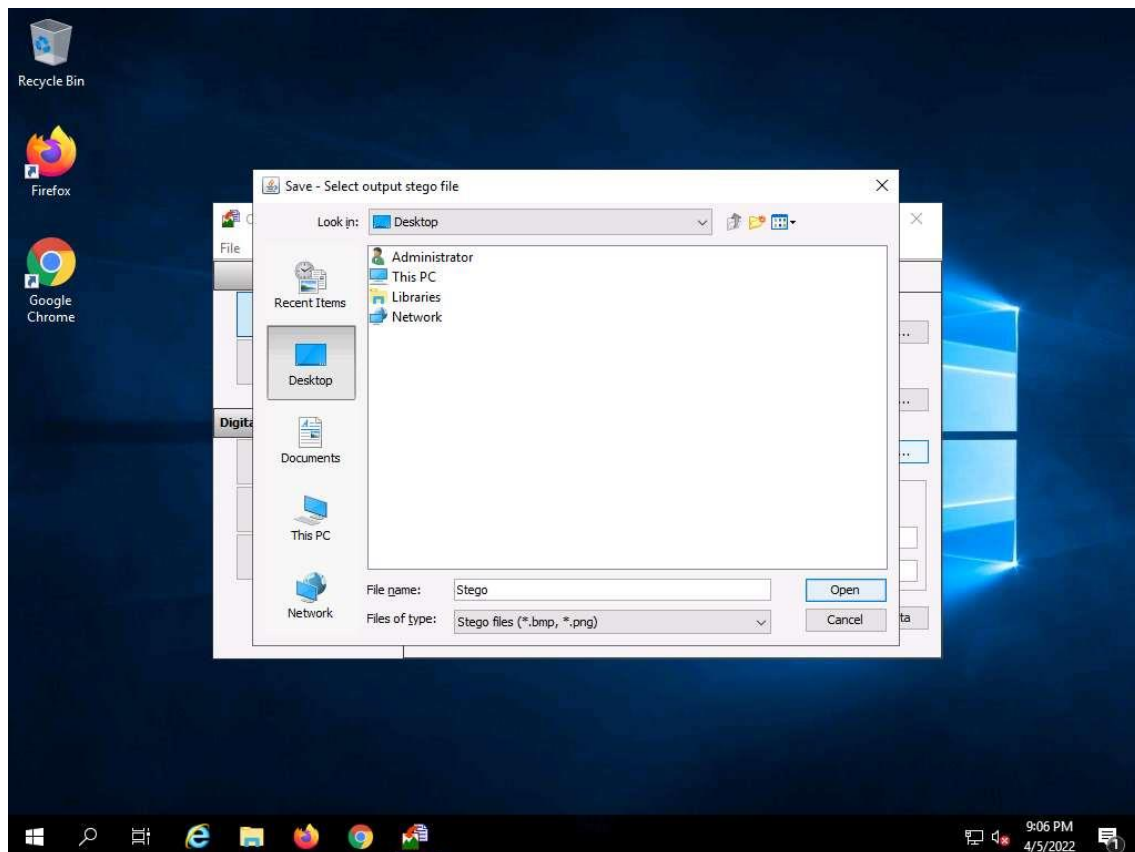


10. Haga clic en el botón **de elipsis** situado junto a **Archivo Stego de salida**.

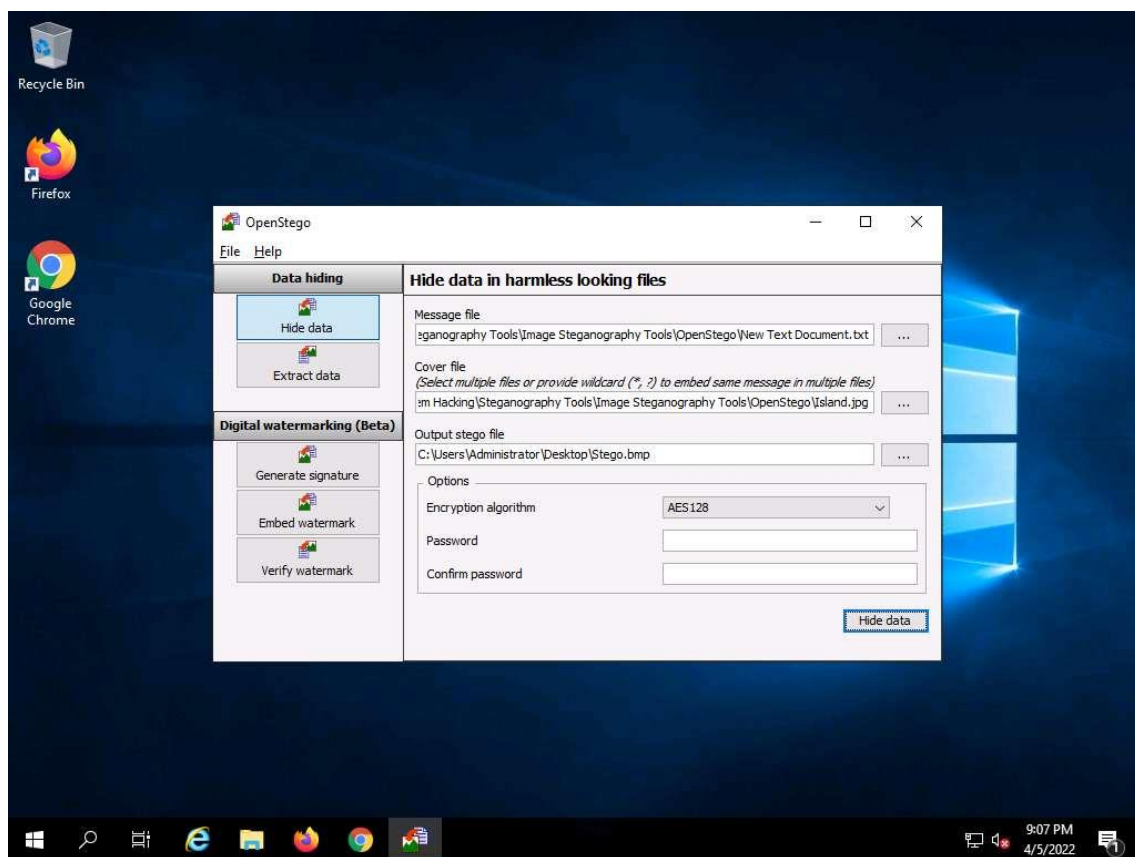


)

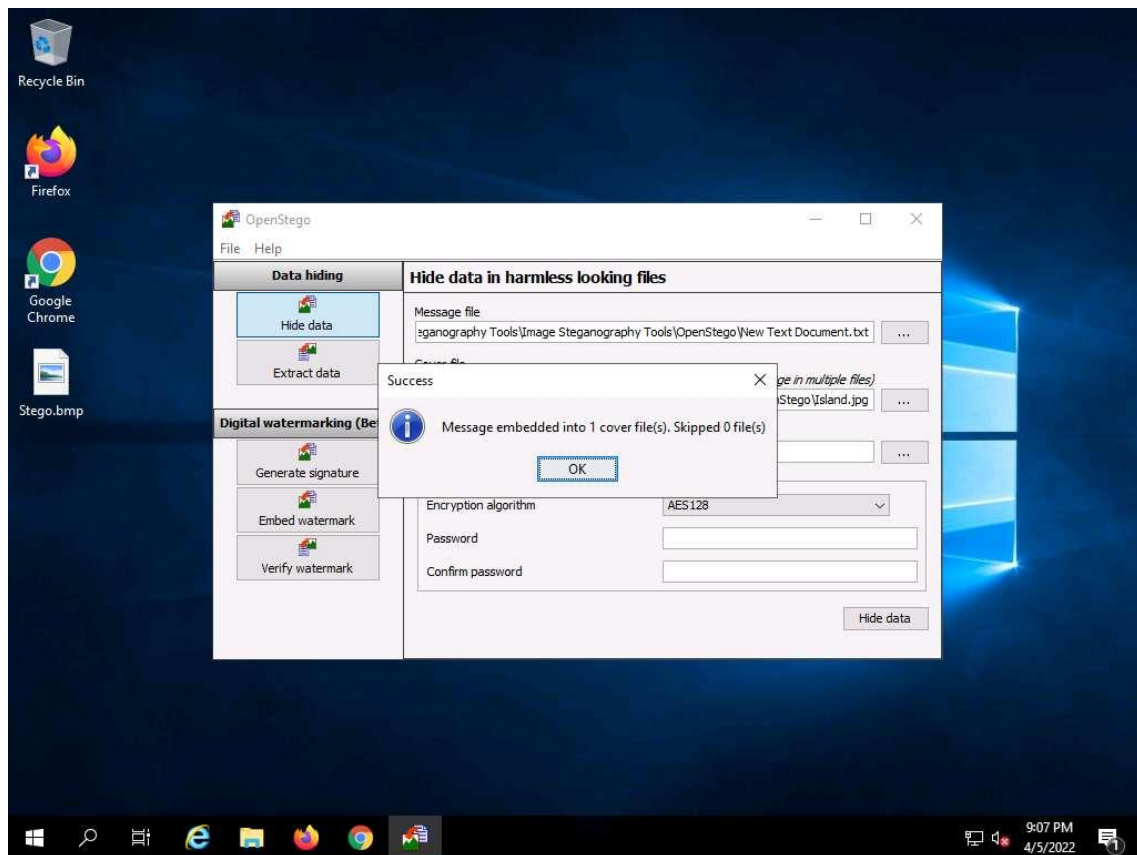
11. Aparecerá la ventana **Guardar - Seleccionar archivo Stego de salida**. Elija la ubicación en la que desea guardar el archivo. En esta tarea, la ubicación elegida es **Escritorio**.
12. Introduzca el nombre del archivo **Stego** y haga clic en **Abrir**.



13. En la ventana **OpenStego**, haga clic en el botón **Ocultar datos**.

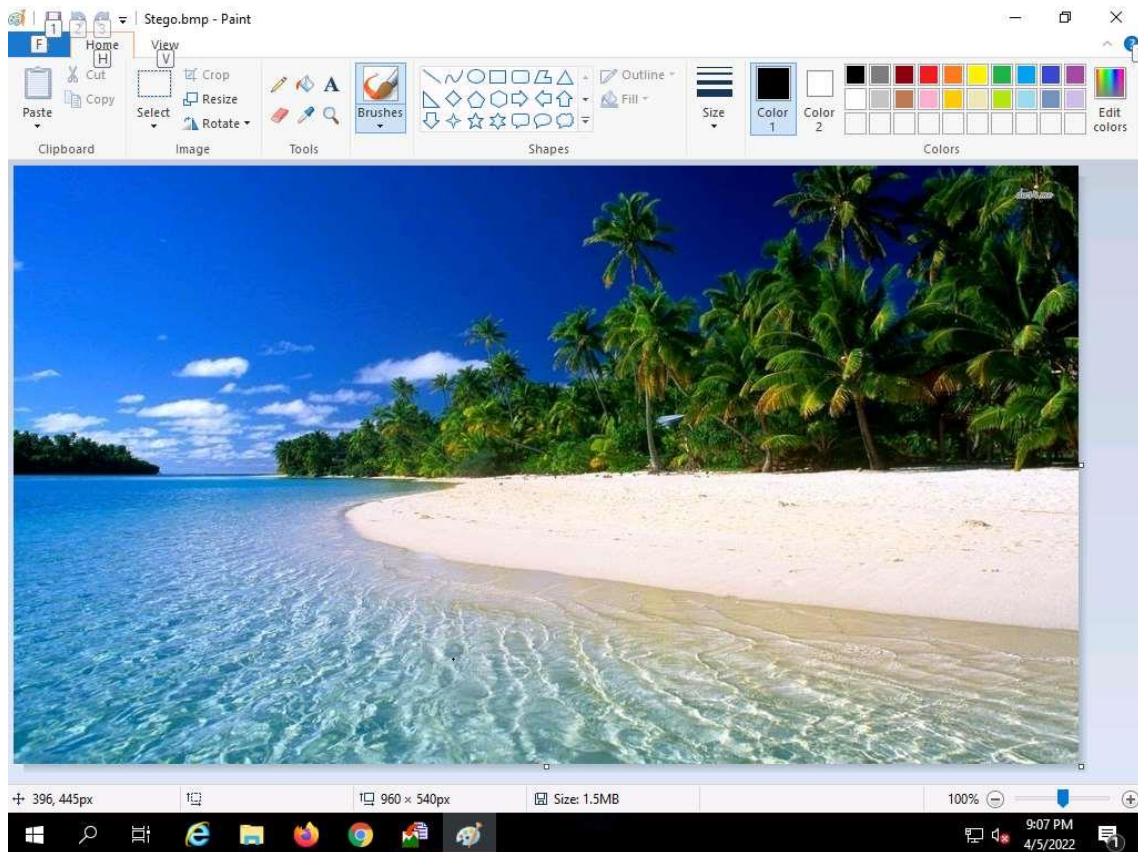


14. Aparecerá una ventana emergente indicando que el mensaje se ha incrustado correctamente; a continuación, haga clic en **Aceptar**.

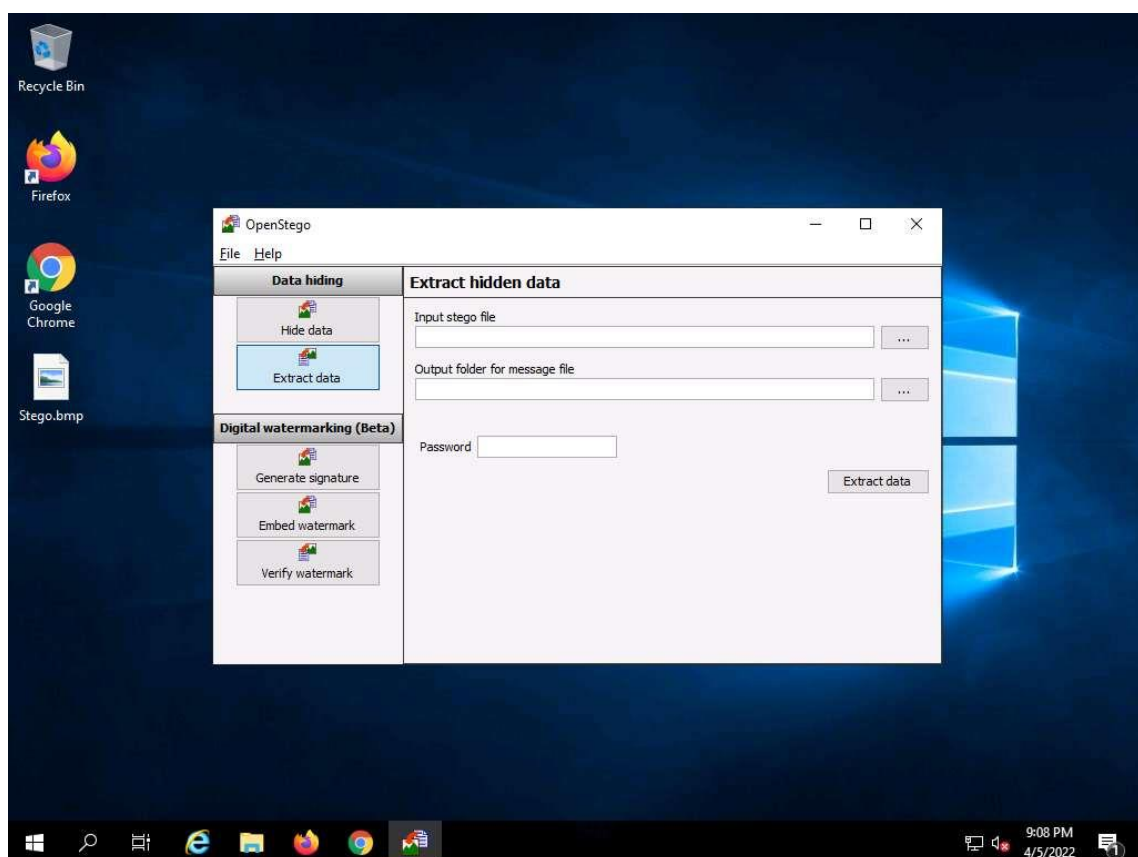


15. Minimice la ventana de **OpenStego**. La imagen que contiene el mensaje secreto aparece en **el Escritorio**. Haga doble clic en el archivo de imagen (**Stego.bmp**) para verlo.

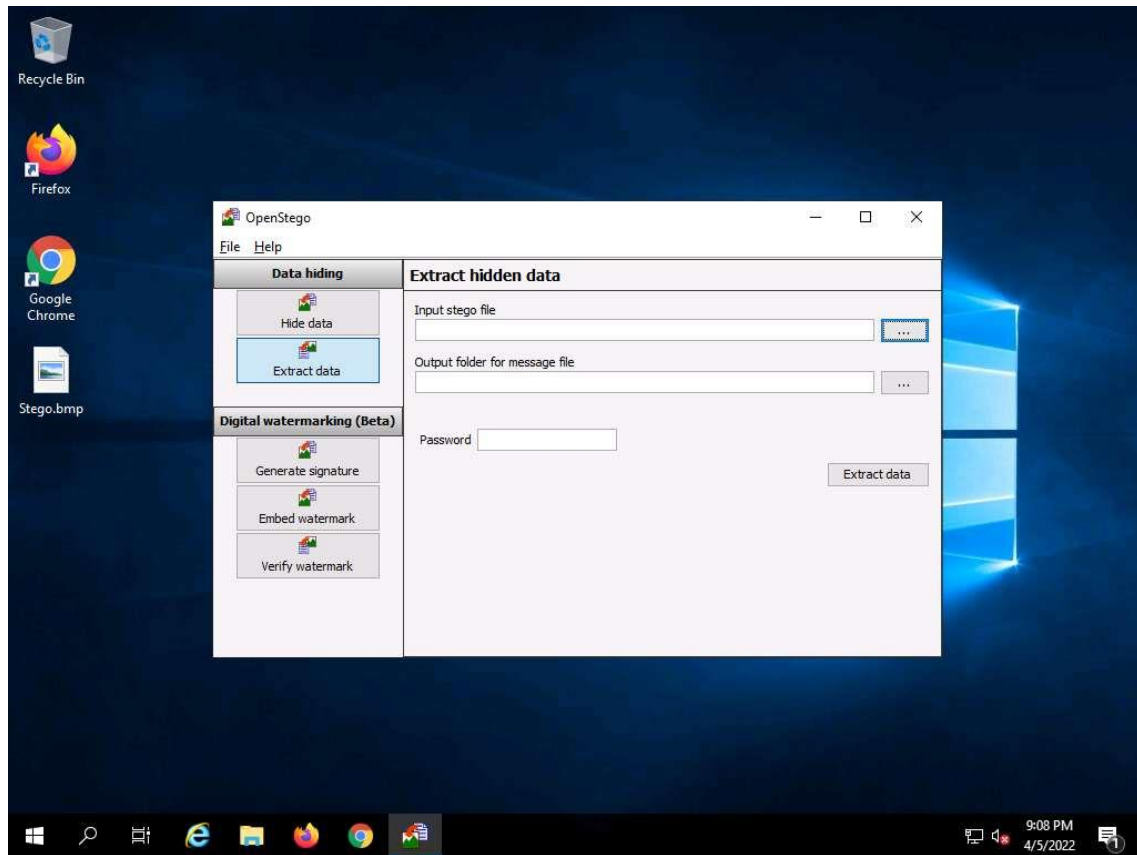
16. Verá la imagen, pero no el contenido del mensaje (archivo de texto) incrustado en ella, como se muestra en la captura de pantalla.



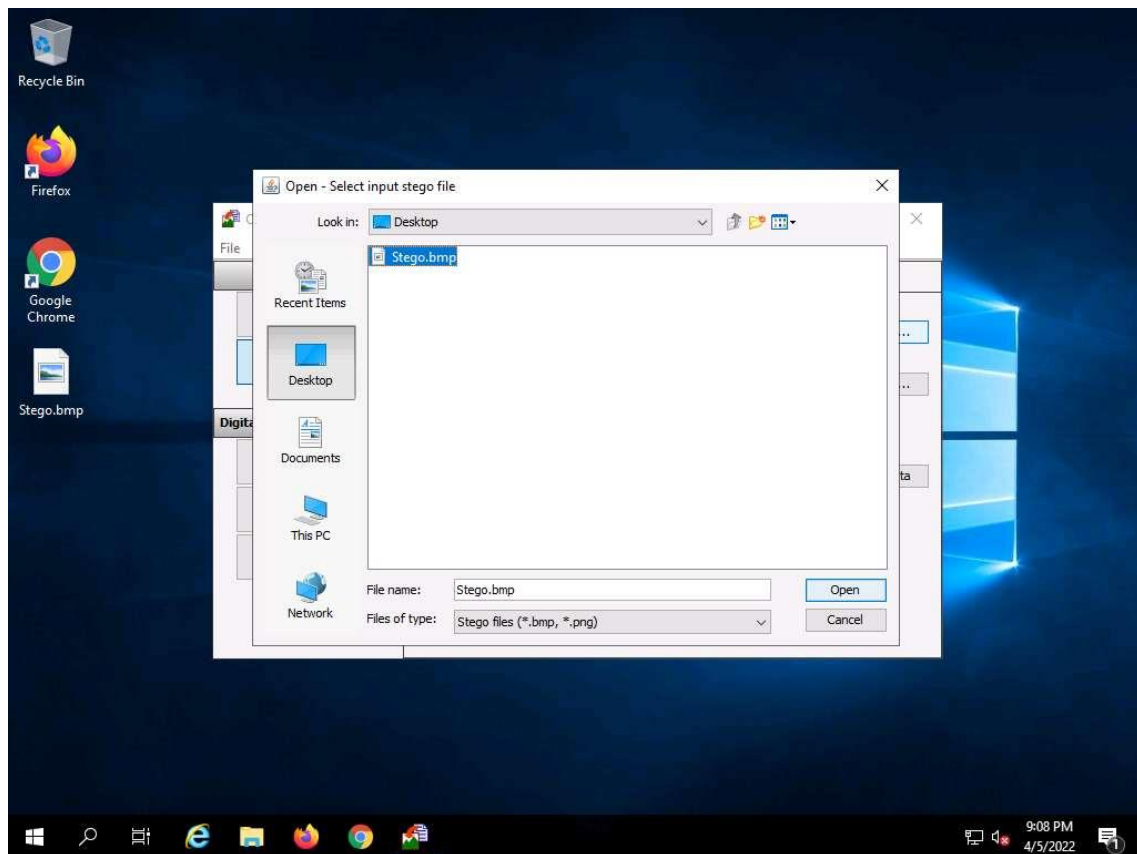
17. Cierre la ventana del visor de **fotos**, cambie a la ventana de **OpenStego** y haga clic en **Extraer datos** en el panel izquierdo.



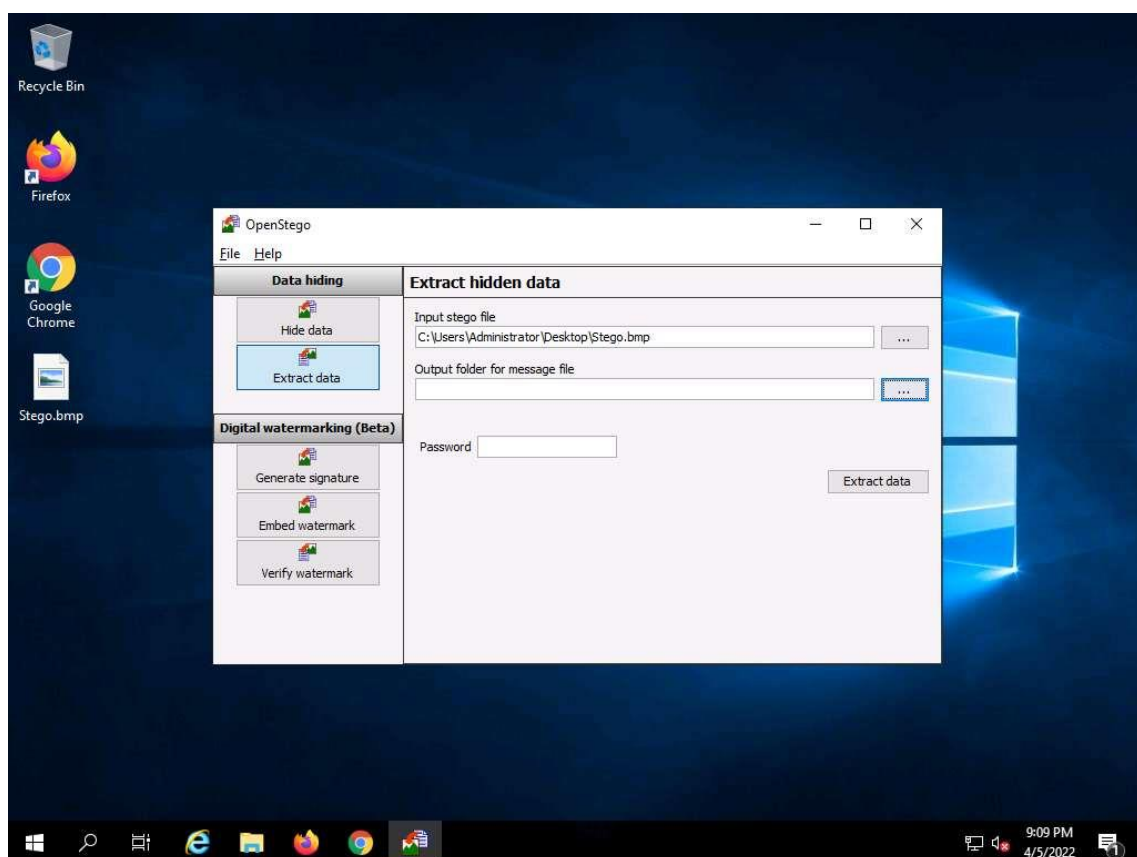
18. Haga clic en el botón **de elipsis** situado junto a **Archivo Stego de entrada**.



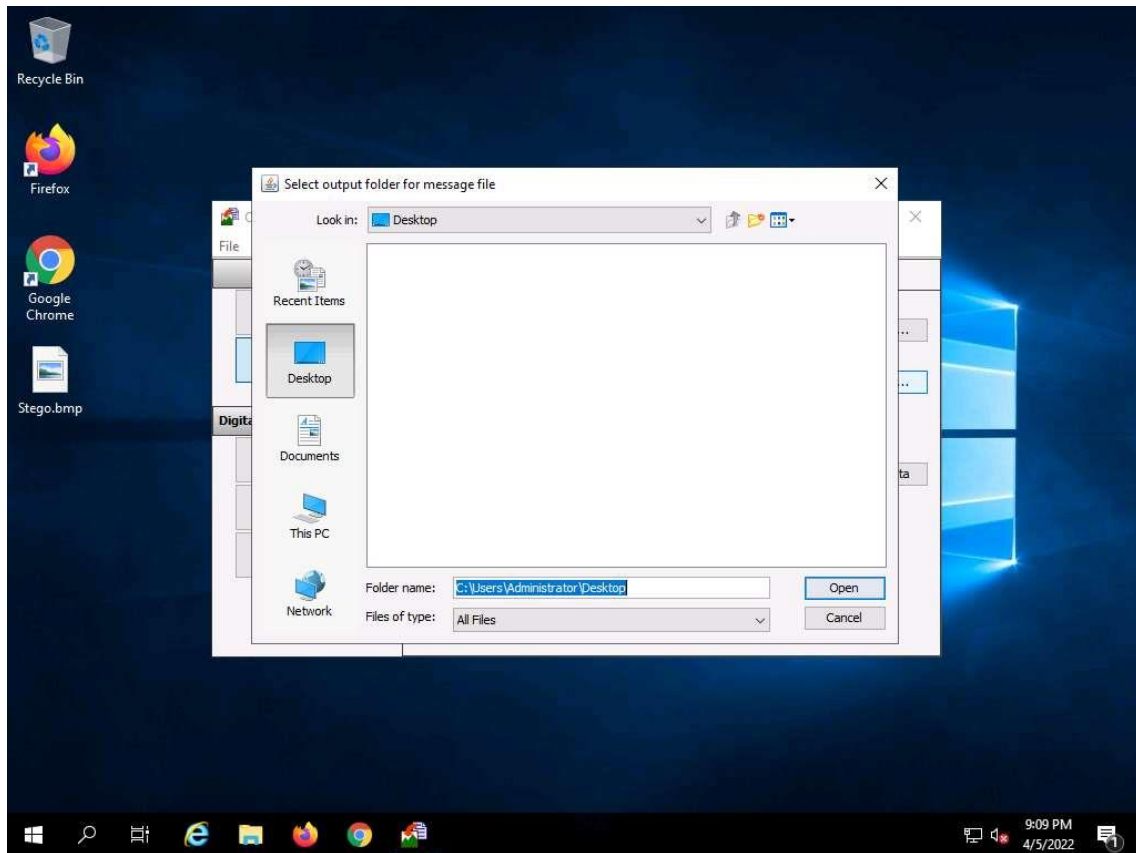
19. Aparecerá la ventana Abrir - Seleccionar archivo Stego de entrada. Desplácese al Escritorio, seleccione Stego.bmp y haga clic en Abrir.



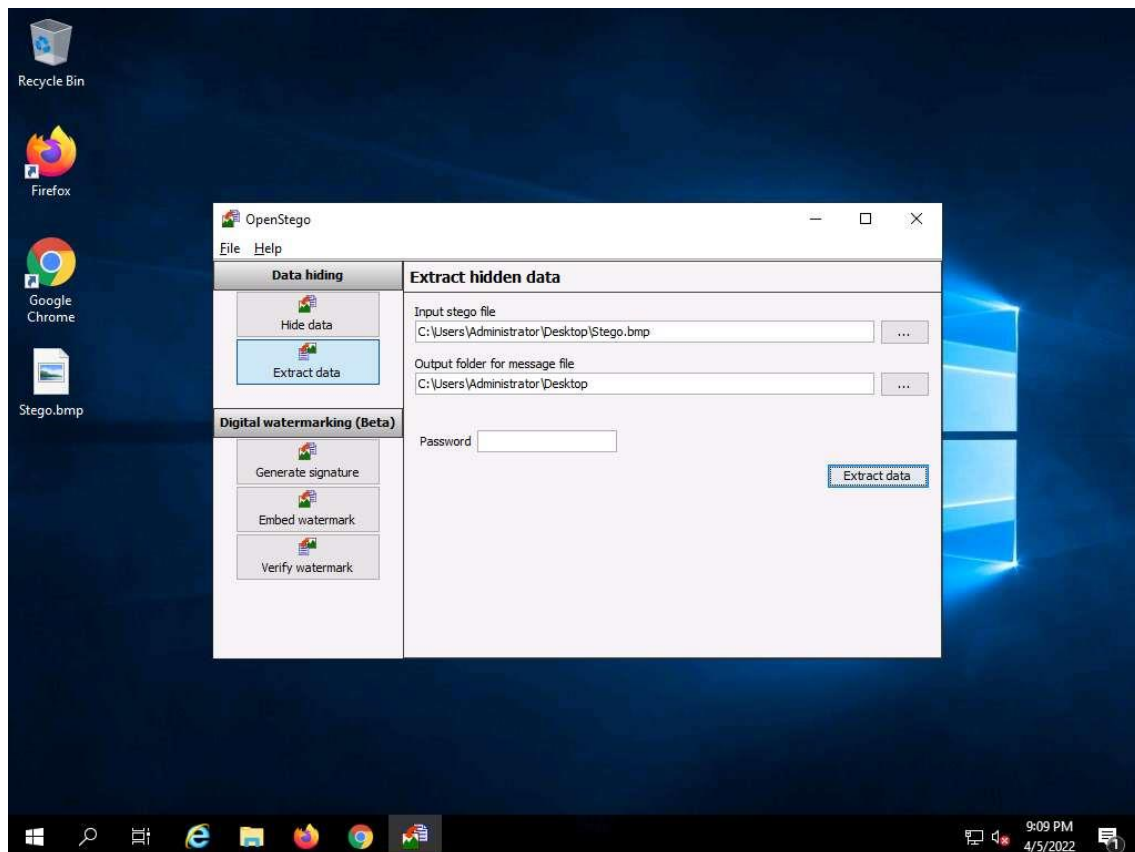
20. Haga clic en el botón de elipsis situado junto a Carpeta de salida para el archivo de mensajes.



21. Aparece la ventana **Seleccionar carpeta de salida para el archivo de mensajes**. Elija una ubicación para guardar el archivo de mensajes (aquí, **Escritorio**) y haga clic en **Abrir**.

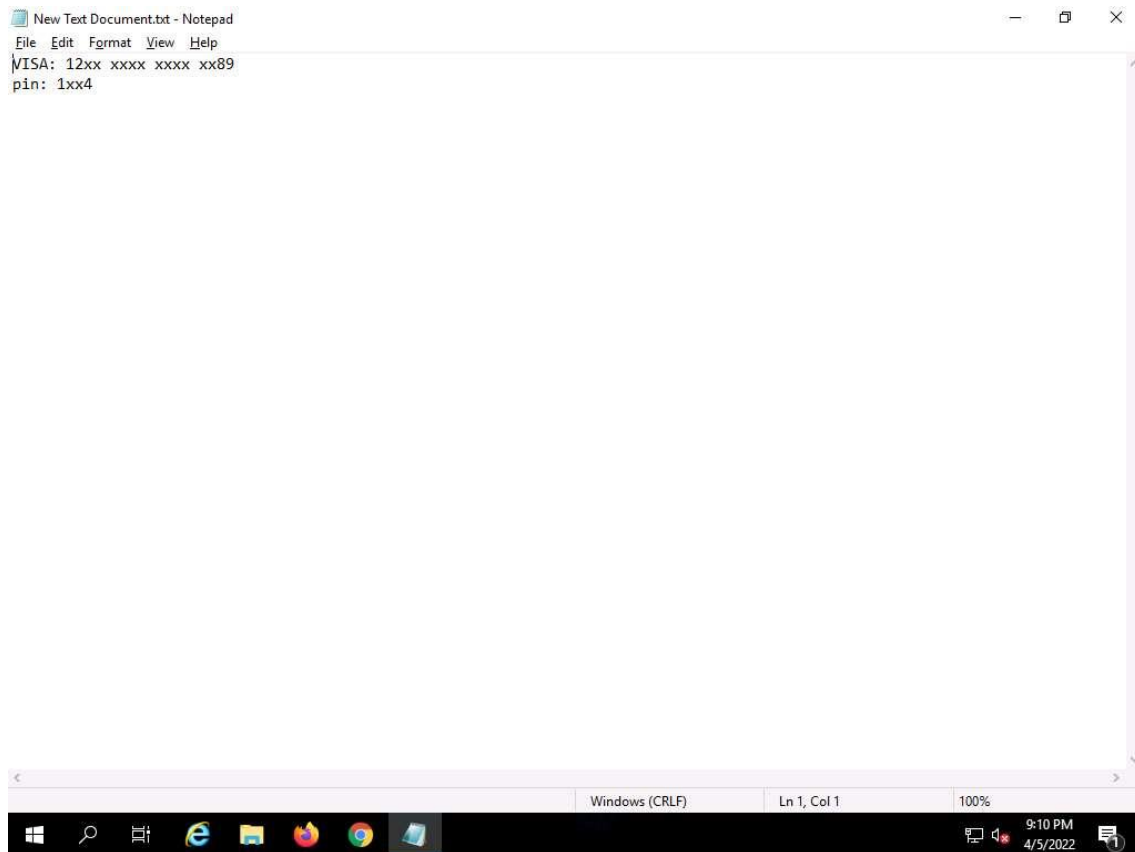


22. En la ventana de **OpenStego**, haga clic en el botón **Extraer datos**. Esto extraerá el archivo de mensajes de la imagen y lo guardará en **el Escritorio**.



23. Aparece la ventana emergente **Éxito**, que indica que el archivo de mensajes se ha extraído correctamente del archivo de portada; a continuación, haga clic en **Aceptar**.
24. El archivo de imagen extraído (**Nuevo Documento de Texto.txt**) se muestra en el **Escritorio**.
25. Cierre la ventana de **OpenStego**, vaya al **Escritorio** y haga doble clic en **Nuevo documento de texto.txt**.
26. El archivo muestra toda la información contenida en el documento de texto, como se muestra en la captura de pantalla.

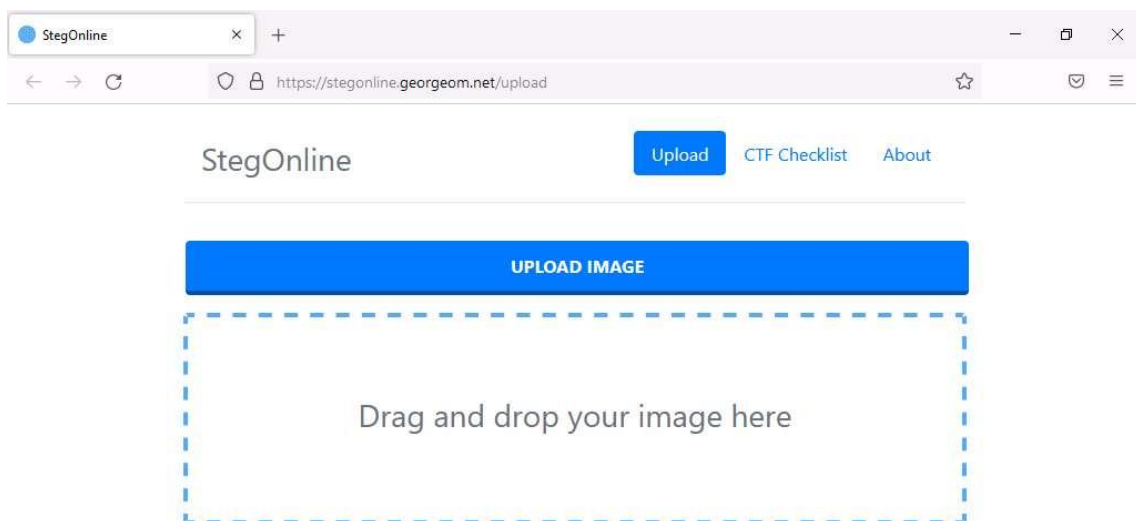
Nota: En tiempo real, un atacante podría buscar imágenes que contengan información oculta y utilizar herramientas de esteganografía para descifrar su información oculta.



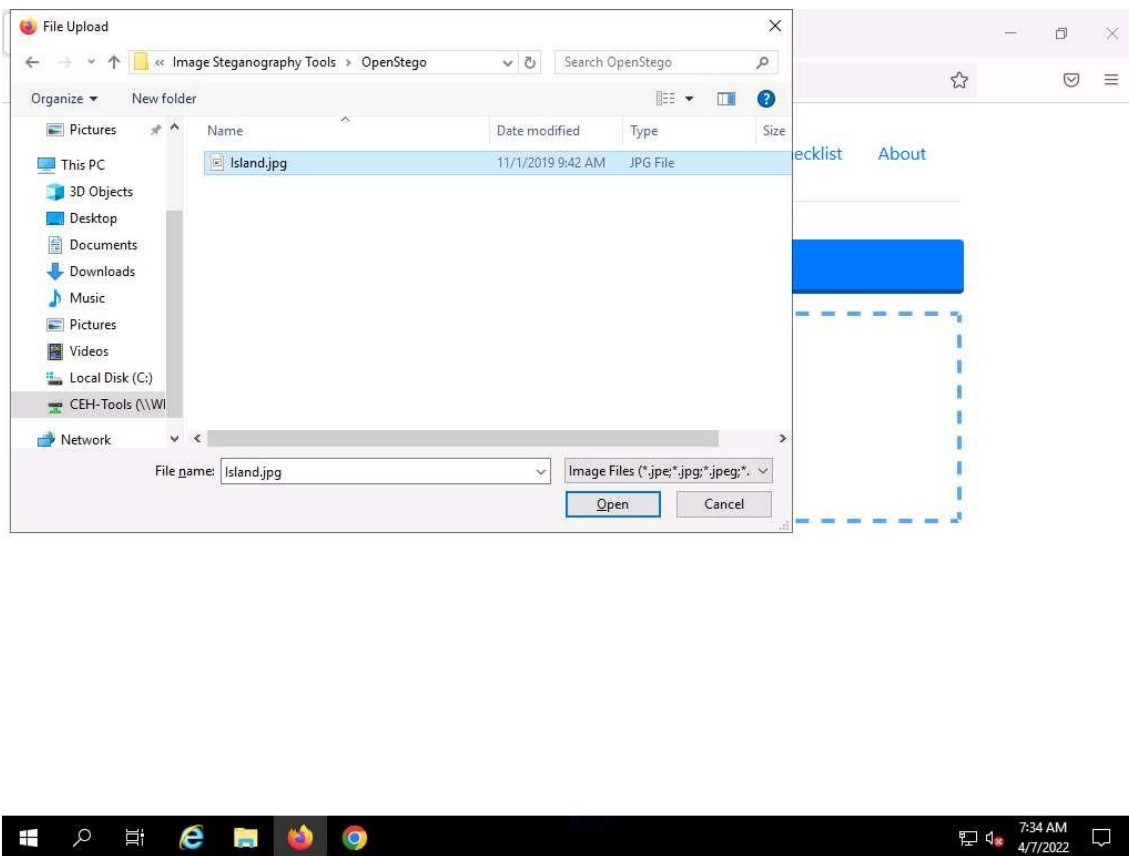
27. Ahora, vamos a realizar la esteganografía de imágenes utilizando la herramienta **StegOnline**.
28. En la máquina **Windows Server**, abra cualquier navegador web (en este caso, **Mozilla Firefox**). En la barra de direcciones coloque el cursor del ratón, escriba **<https://stegonline.georgeom.net/upload>** y pulse **Intro**.



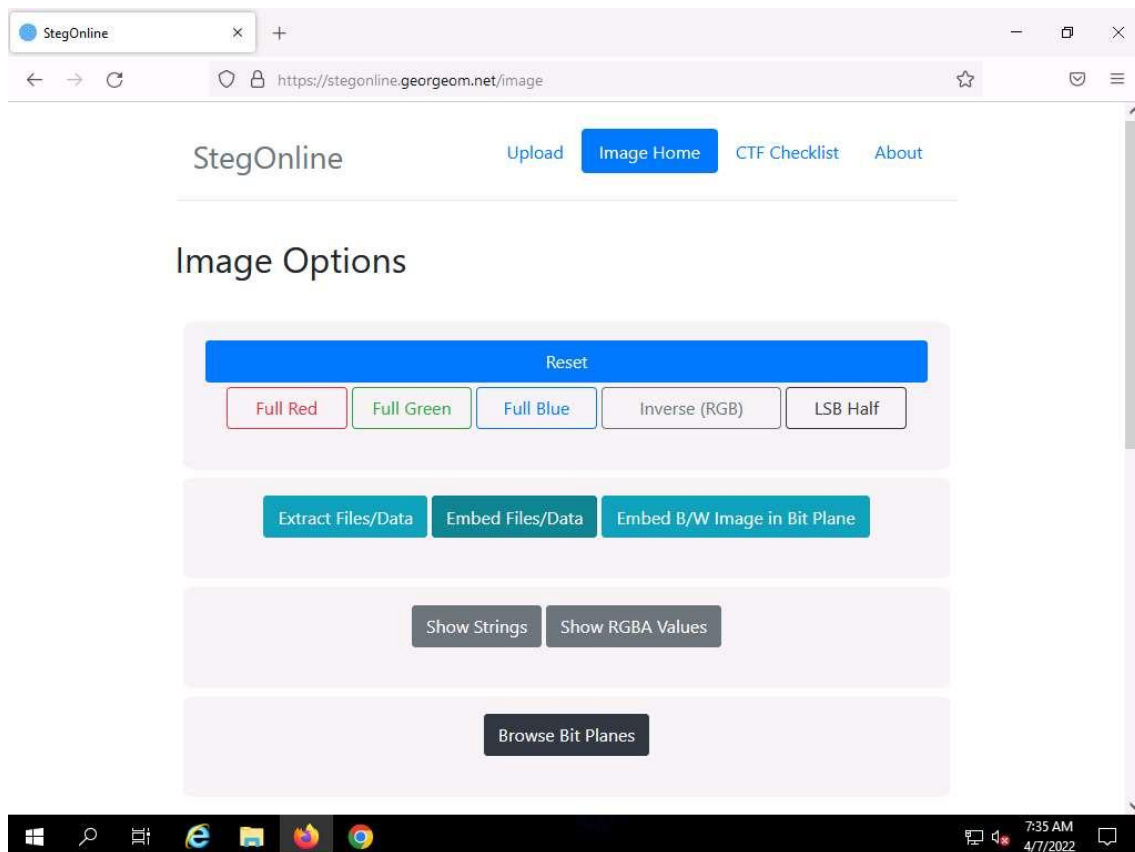
29. Aparece la página web **StegOnline**, haga clic en el botón **CARGAR IMAGEN**.



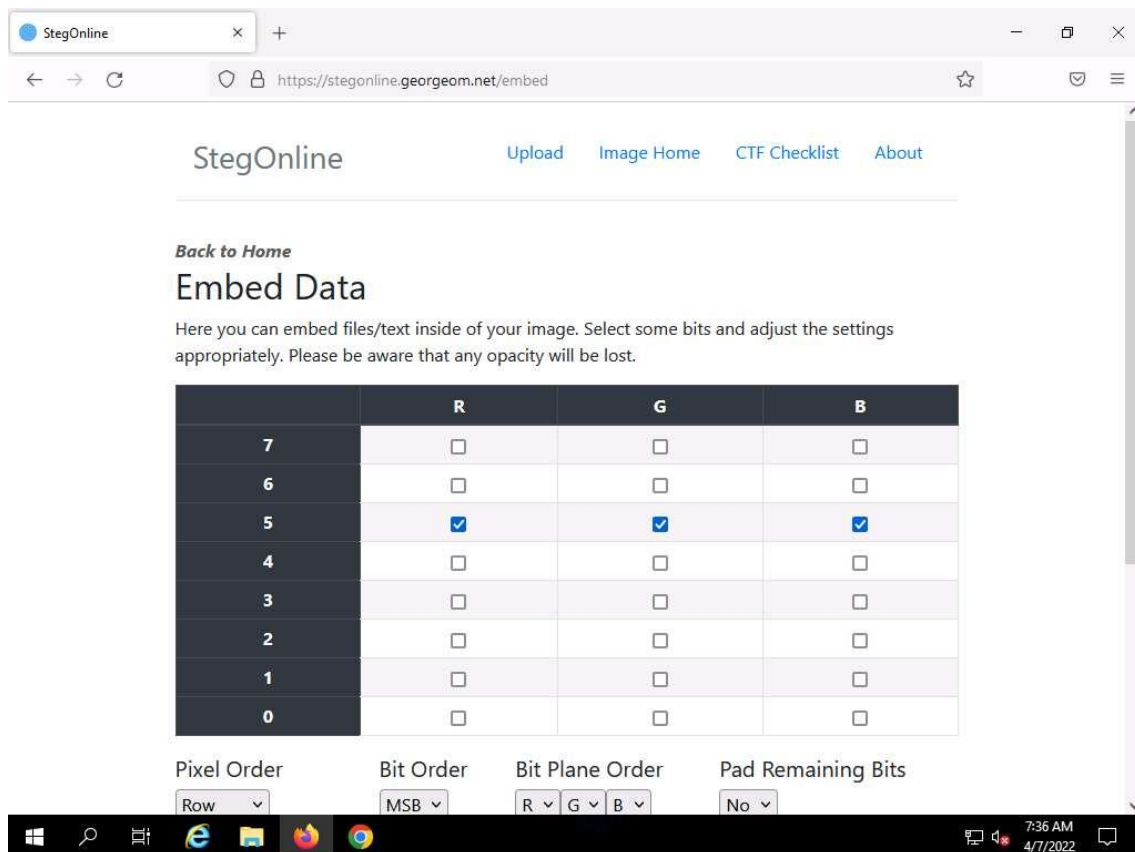
30. En la ventana de Carga de Archivos navegue hasta C:\Tools\Steganography Tools\Whitespace Steganography Tools\OpenStego, seleccione Island.jpg, y haga clic en Abrir.



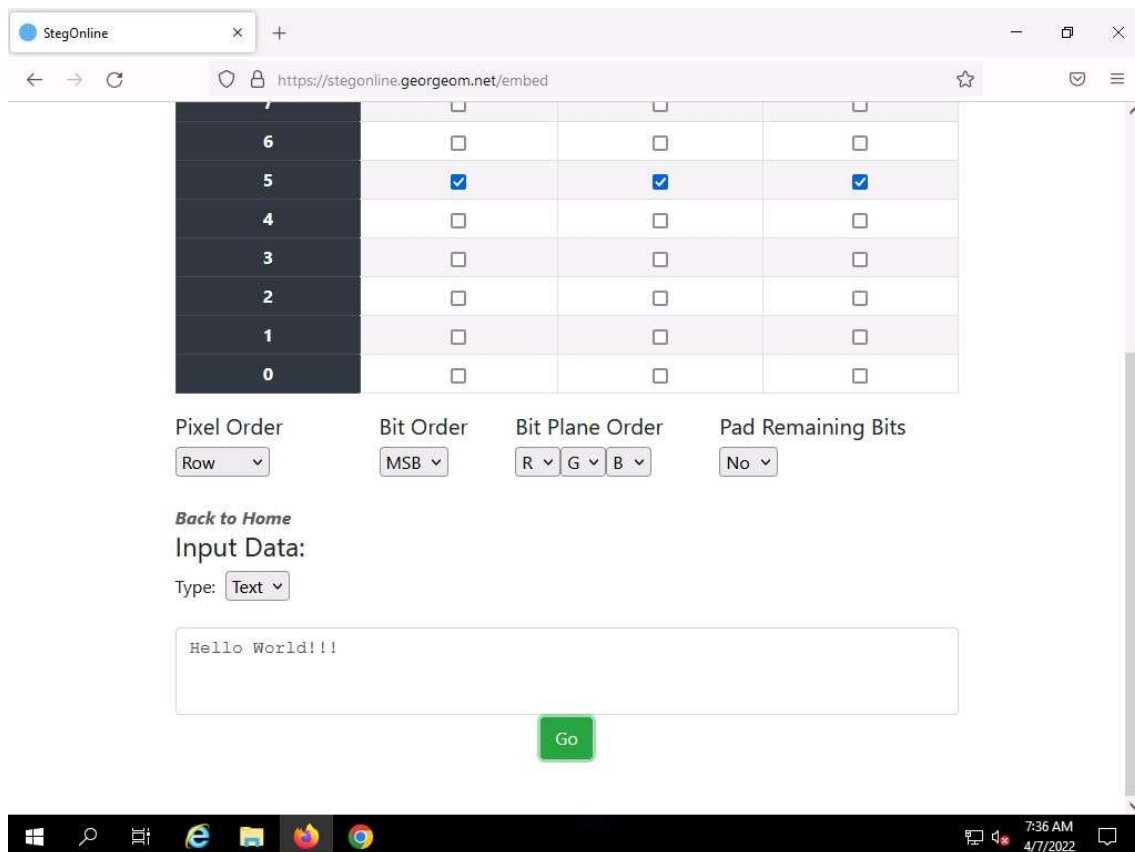
31. En la página Opciones de imagen, haga clic en el botón Incrustar archivos/datos.



32. En la página **Incrustar datos**, marque las casillas de verificación de la fila **5** y de las columnas **R**, **G** y **B**, como se muestra en la captura de pantalla.

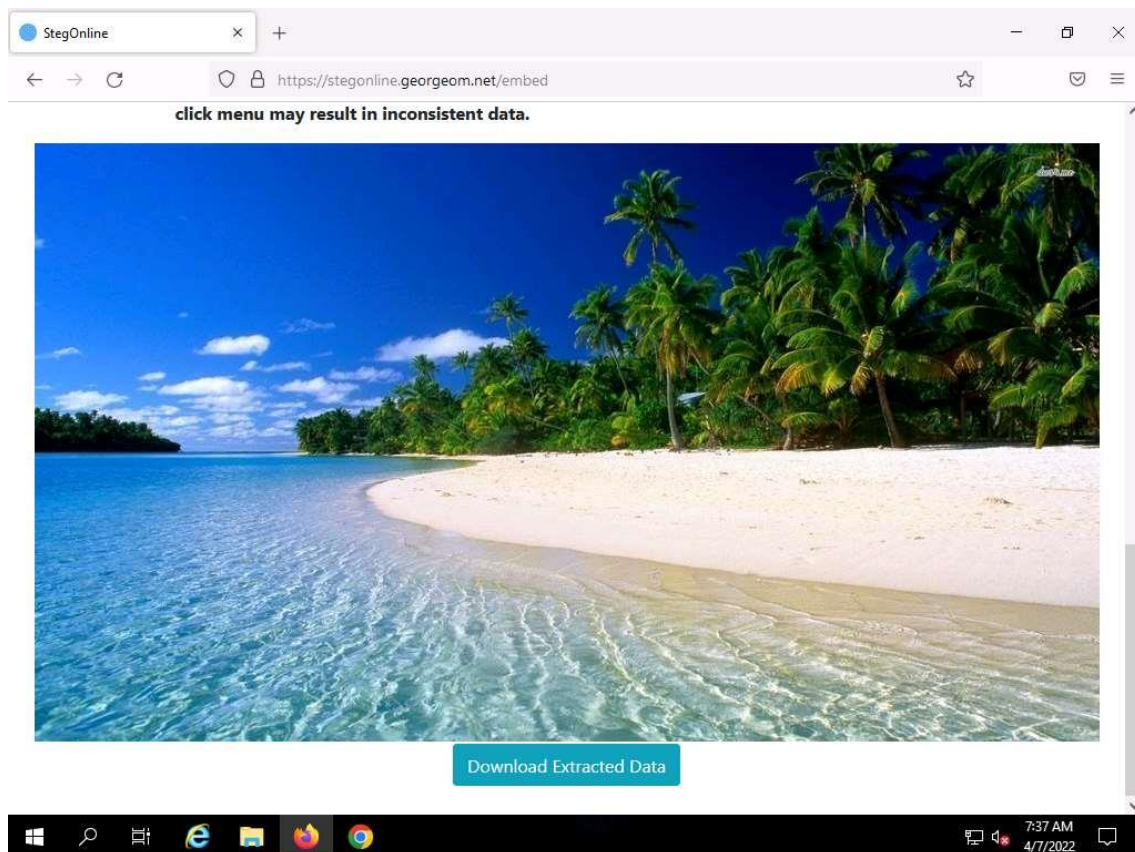


33. Desplácese hasta el campo **Datos de entrada** y asegúrese de que la opción **Texto** está seleccionada en el menú desplegable, escriba **¡Hola Mundo!** y haga clic en **Ir**.

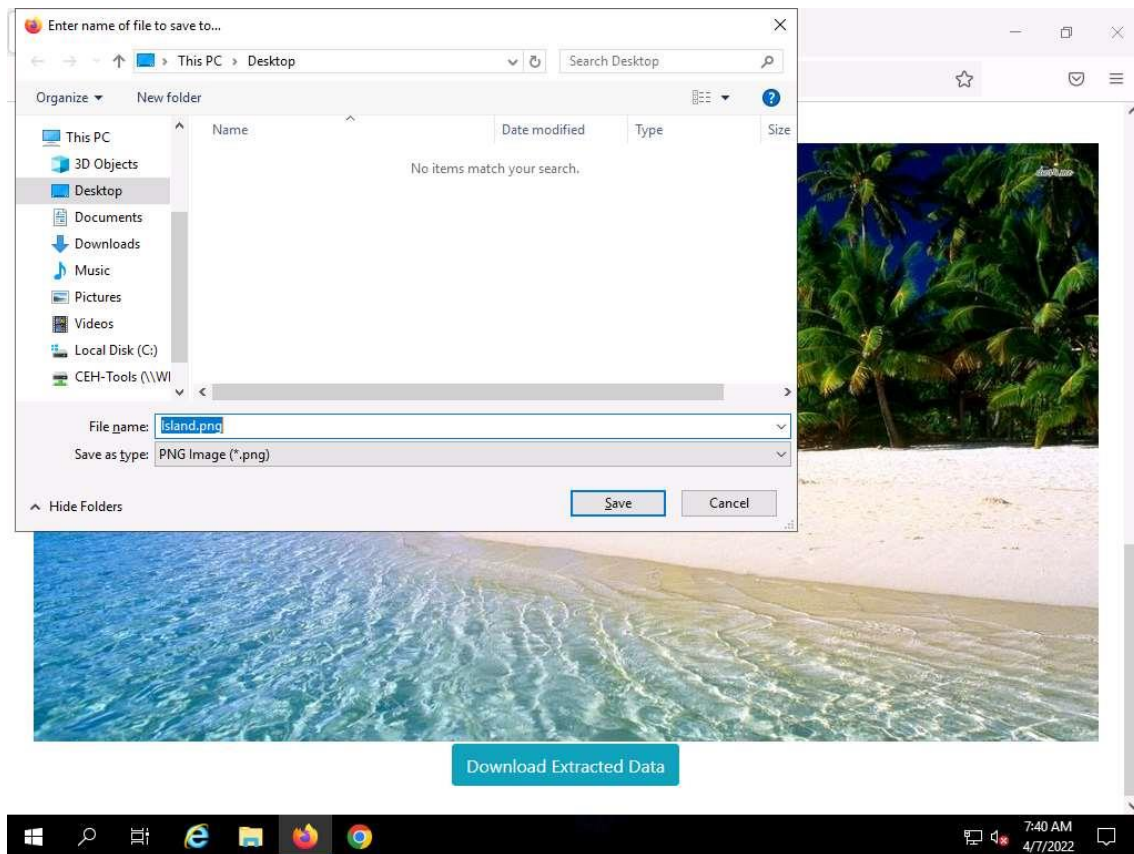


34.Desplácese hacia abajo para ver la imagen en la sección **Salida**, guarde la imagen haciendo clic en el botón **Descargar datos extraídos**.

Nota: Si aparece la ventana emergente **Opening Island.png**, seleccione el botón de opción **Save File** y haga clic en **OK**.

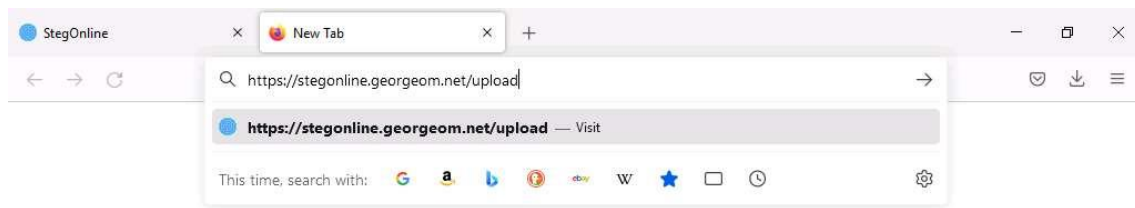


35. En la ventana **Introduzca el nombre del archivo para guardar en...** seleccione la ubicación deseada para guardar la imagen (aquí estamos guardando la imagen en el **Escritorio**) y haga clic en **Guardar**.



36.Hemos conseguido incrustar datos en un archivo de imagen. Ahora, vamos a extraer los datos incrustados.

37.Abra una nueva pestaña en el navegador Firefox, escriba <https://stegonline.georgeom.net/upload> y pulse **Intro**.



38. En la página **StegOnline**, haga clic en el botón **CARGAR IMAGEN** y en la ventana de **carga de archivos** seleccione el archivo **Island.png** del **Escritorio** y haga clic en **Abrir**.

40. En la página **Extraer datos** marque las casillas de verificación de la fila **5** y de las columnas **R**, **G** y **B**, desplácese hacia abajo y haga clic en **Ir**.

Back to Home

Extract Data

Here you can extract data hidden inside of the image. Select some bits and adjust the settings appropriately. The final extracted data is checked against some basic file headers, and so the filetype can be automatically determined.
Please note that Alpha options are only available if the image contains transparency.

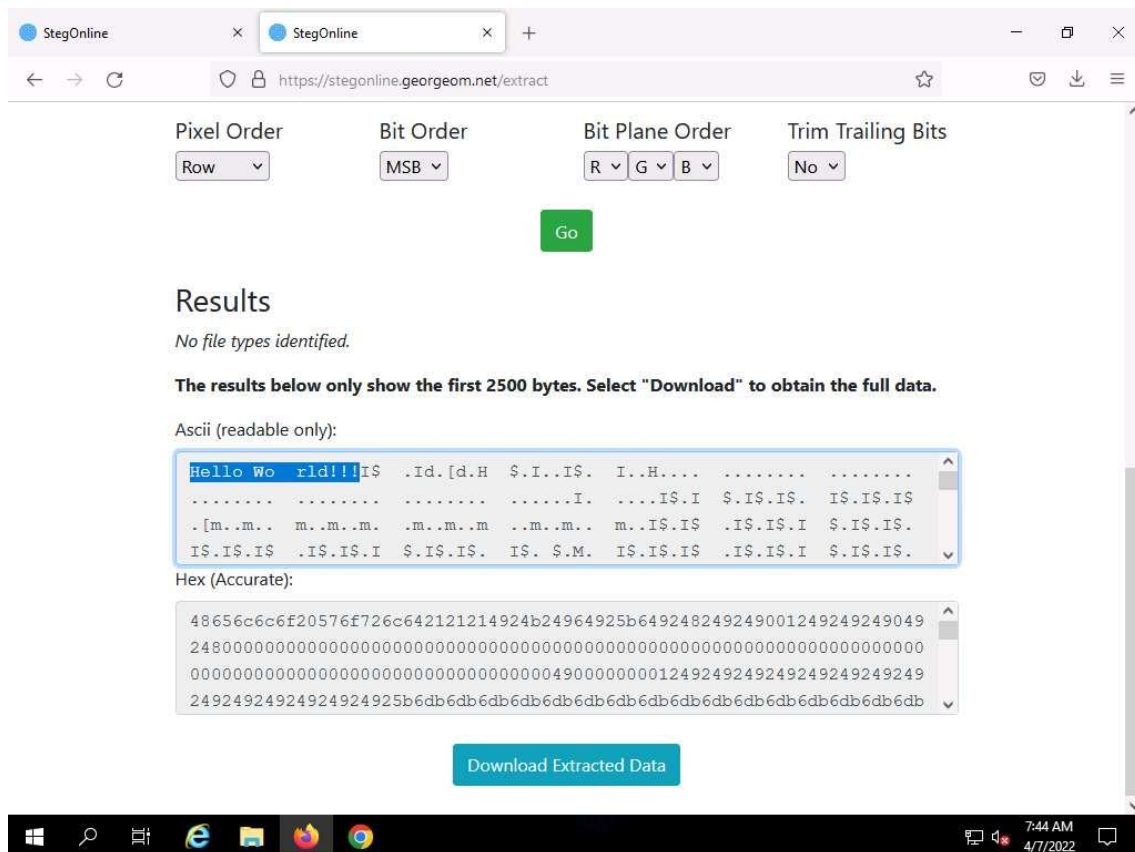
| | R | G | B |
|---|-------------------------------------|-------------------------------------|-------------------------------------|
| 7 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 4 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 1 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 0 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Pixel Order: Bit Order: Bit Plane Order: Trim Trailing Bits:

Go

41. Después de hacer clic en **Ir**, desplácese hacia abajo para ver los datos en la sección **Resultados**.

Nota: También puede descargar los datos extraídos haciendo clic en el botón **Descargar datos extraídos**.



42. Esto concluye la demostración de cómo realizar esteganografía de imágenes utilizando OpenStego y StegOnline.
43. También puede utilizar otras herramientas de esteganografía de imágenes como **QuickStego** (<http://quickcrypto.com>), **SSuite Picxel** (<https://www.ssuitesoft.com>), **CryptaPix** (<https://www.briggsoft.com>) y **gifshuffle** (<http://www.darkside.com.au>) para realizar esteganografía de imágenes en el sistema de destino.
44. Cierre todas las ventanas abiertas y documente toda la información obtenida.