# Camufla archivos detrás de otros archivos

La esteganografía es la técnica del disimulo por excelencia desde tiempos inmemoriales. Su evolución digital se basa en ocultar un determinado archivo dentro de otro aparentemente inofensivo y que, además, puede no tener nada en común con el que se oculta.

## 1: Descarga e inicia OpenPuff

La palabra esteganografía tiene sus raíces etimológicas en la unión de las palabras griegas *Steganos* (cubierto u oculto) y *Grafos* (escritura). Es decir, escritura oculta.

Esta práctica está muy ligada a la criptografía y se basa en ocultar un archivo que quieres enviar a otra persona tras un documento de texto, archivo de imagen o de audio que, aparentemente, nada haría sospechar que en realidad tiene un documento oculto entre sus bits. Para llevar a cabo esa ocultación se utiliza un programa que “corta” el archivo en fragmentos y los camufla entre los bits del archivo huésped. Este software se llama OpenPuff.

OpenPuff será llave que abra y cierre la cerradura que revelará el documento oculto. Por lo tanto, será la pieza clave para realizar el proceso de ocultación.

Puedes descargarlo desde su página web.

OpenPuff es un programa portable. Es decir, que no necesitas instalarlo en tu equipo para que funcione y esa característica es básica para que pase inadvertido ya que podrás ejecutarlo en cualquier ordenador desde una llave USB, ocultar o descifrar un archivo y no dejar rastro.

Al descargar OpenPuff, descargas un archivo comprimido en formato ZIP. Descomprime el archivo descargado y accede a la carpeta que encontrarás en su interior. Allí, busca el ejecutable OpenPuff.exe y haz doble clic sobre él para iniciar la herramienta de cifrado.

## 2: Oculta el archivo secreto

El siguiente paso es cifrar y ocultar el archivo que quieres enviar tras otro que aparentemente no tenga nada que ver.

Haz clic sobre el botón Hide de OpenPuff y se iniciará el cuadro de cifrado y ocultación del archivo. Comienza configurando las claves que permitirán el descifrado del archivo.

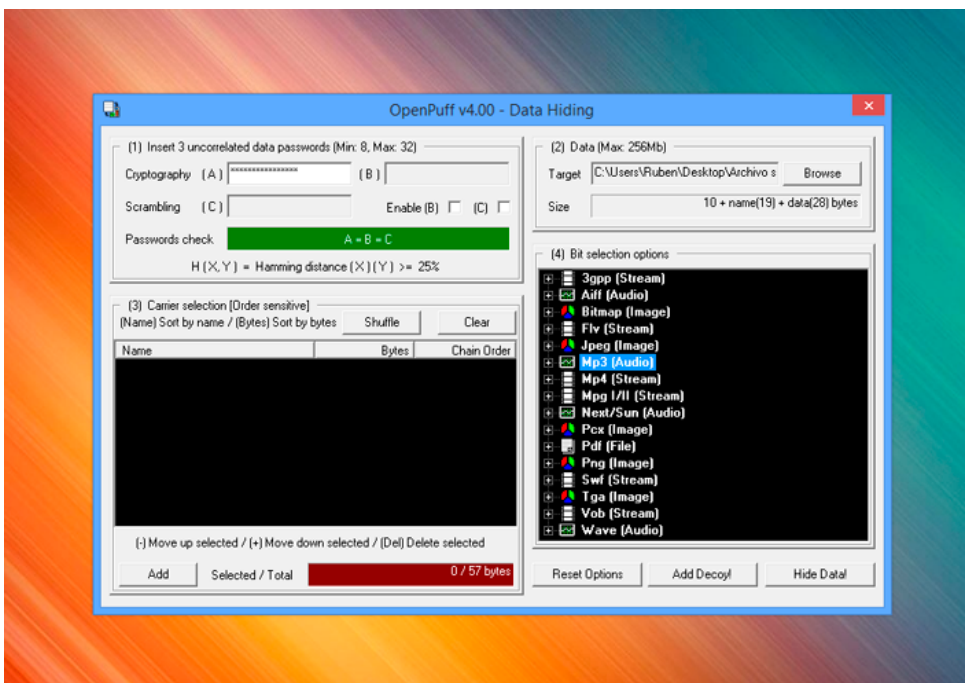
Puedes establecer una combinación de entre una y tres claves para proteger el cifrado del archivo. Si quieres utilizar solo una clave, desmarca las casillas Enable B y C. De ese modo solo se mantendrá activo el cuadro Cryptografy A para que puedas introducir la contraseña en él.

Lógicamente, utilizando las contraseñas B y C añades mayor seguridad al cifrado del documento ya que no sólo deben acertar una contraseña, sino que tienen que hacerlo en tres ocasiones y en el orden correcto.

A continuación, escribe en el cuadro Cryptografy A la contraseña que cifrará y descifrará el archivo. Recuerda esta contraseña ya que será necesaria para su posterior descifrado.

En la barra Passwords check podrás comprobar el nivel de fortaleza de tu contraseña. Si sólo vas a utilizar una contraseña, al menos procura que esta sea mínimamente fuerte. Cuando su fortaleza sea correcta la barra te lo indicará cambiando del rojo al verde.

Ahora, añade el documento que vas a ocultar. Haz clic sobre el botón Browse y selecciona el documento. Nosotros hemos optado por un PDF, pero puede ser de cualquier tipo o formato.




## 3: La tapadera perfecta

Ya has incluido el archivo a ocultar y has establecido la seguridad de su cifrado, ahora es el momento de elegir la tapadera perfecta para que el archivo pase inadvertido.

Haz clic sobre Add y añade el archivo que servirá de anfitrión para ocultar el documento que ya has incluido.

Este archivo debe ser de igual tamaño o superior que el archivo que pretende ocultar y puede ser de texto, de audio, vídeo, etc. OpenPuff permite que el mensaje se oculte repartido en varios archivos anfitriones distintos, cosa que dificultará exponencialmente su descifrado y permitirá ocultar archivos más grandes.

Por el momento, para simplificar el proceso, utiliza solo un archivo anfitrión. Nosotros utilizaremos un archivo mp3.

Para ayudarte a ocultar el archivo, puedes controlar la calidad que tendrá. Si, por ejemplo, estás usando un archivo de audio, puedes modificar su calidad de codificado para así ajustar su tamaño al del archivo a ocultar.

Para ello, en el apartado Selection options, selecciona el tipo de archivo que estás usando y elige una calidad. Cuando el “archivo tapadera” tenga el tamaño adecuado, la barra Select/total cambiará a verde.

A continuación, inicia el proceso de cifrado y fusión de ambos archivos pulsando en Hide Data! y elige una ubicación para el archivo resultante que contendrá ambos archivos.

Al abrir el archivo resultante, en este caso un archivo de audio, se abrirá el reproductor multimedia y lo reproducirá con toda normalidad. Pero creenos, contiene un archivo oculto.

## 4: Descifra el mensaje oculto

Para extraer el documento oculto tras el archivo que has creado en el paso anterior, básicamente debes realizar el mismo proceso a la inversa.

Durante el proceso de ocultación del paso anterior, el archivo oculto se ha fraccionado en partes y se ha mezclado con el archivo anfitrión. El proceso de descifrado consiste en volver a unir a esos fragmentos para volver a formar el archivo original.

La Piedra Rosetta que permite esta reconstrucción será la contraseña que estableciste al cifrarlo.

Inicia OpenPuff y haz clic sobre el botón Unhide para acceder al cuadro de descifrado.

Al igual que hiciste en el paso de cifrado, desmarca las contraseñas que no utilizarás. Estas deben ser idénticas a las utilizadas en el paso de cifrado. Por lo tanto, si usaste solo la contraseña A, desmarca las casillas B y C y escribe la contraseña en Cryptografy A.

A continuación, añade el archivo (o archivos, si usaste varios en el paso anterior) anfitrión que contiene el archivo oculto. Haz clic sobre Add Carriers. Después, haz clic sobre Unhide y elige la ubicación donde se extraerá el archivo oculto.

Tras unos instantes, aparece el nuevo archivo tal y como estaba antes del proceso. El archivo anfitrión no se modifica, por lo que puedes extraer el contenido oculto tantas veces como sea necesario sin que sufra cambio alguno.