Lab - Using Steghide for Hiding and Extracting Data

Overview

Steghide is a steganography program that is able to hide data in various kinds of images and audio-files. The color- respectively sample-frequencies are not changed thus making the embedding resistant against first-order statistical tests.

The word steganography comes from the Greek name “steganos” (hidden or secret) and “graphy” (writing or drawing) and literally means hidden writing. Steganography uses techniques to communicate information in a way that is hidden.

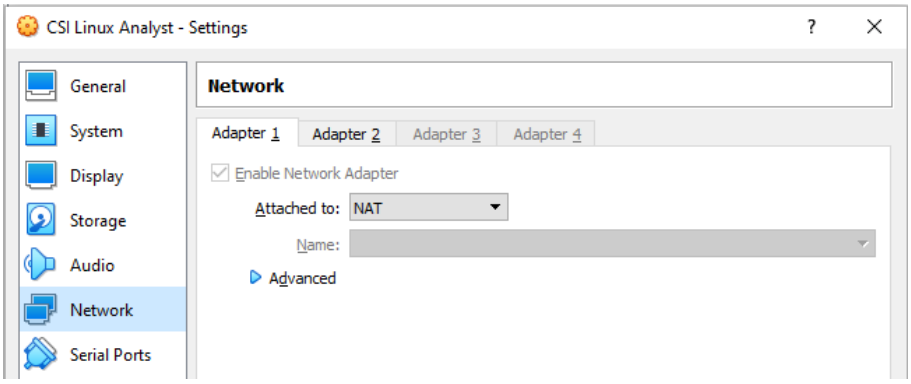
Steganography (the hiding of data in other content types such as images, videos, network traffic etc.) continues to play a role in modern attacks in several forms. Most uses of steganography in malware can be divided into two broad categories: concealing the actual malware contents and concealing the command and control communications (C2) channel.

Lab Requirements

1. Install of CSI Linux Analyst

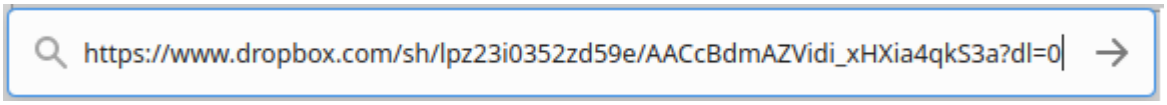
Begin the lab!

Ensure your CSI Linux Analyst has its network adapter configured for NAT for internet access.

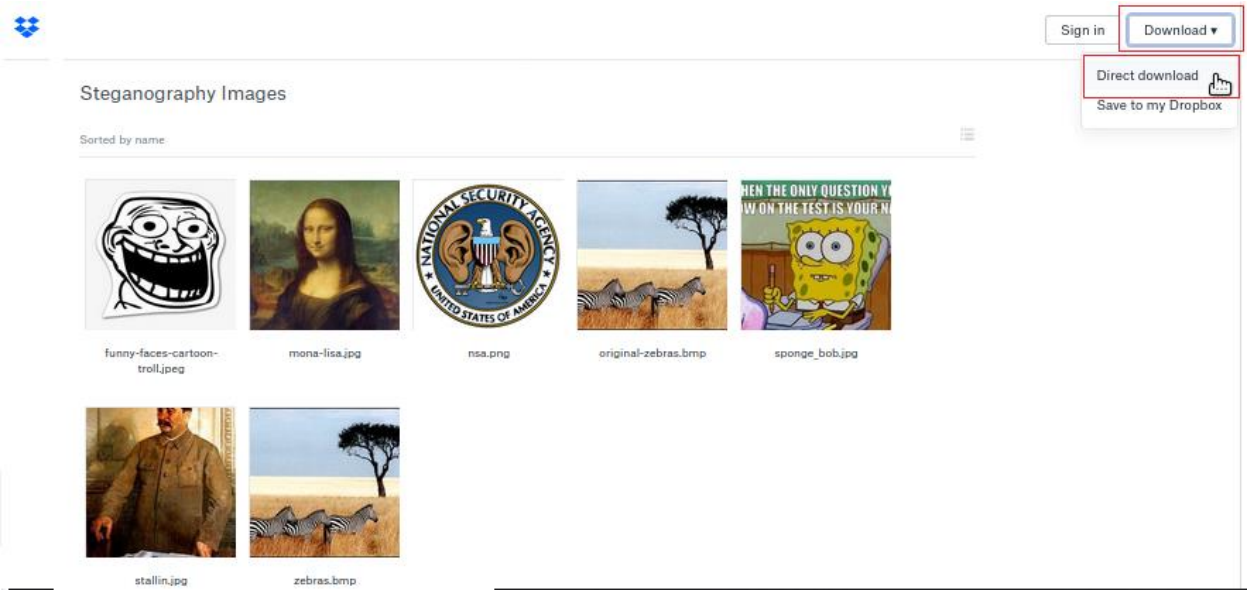


From your CSI Linux Analyst desktop, launch your Firefox browser. Copy and past the following URL into the address bar of your browser.

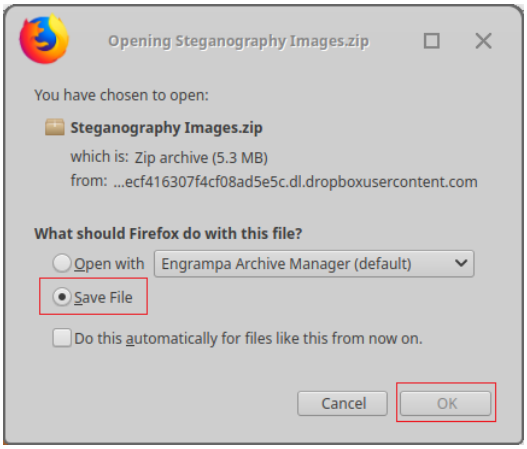
https://www.dropbox.com/sh/lpz23i0352zd59e/AACcBdmAZVidi_xHXia4qkS3a?dl=0



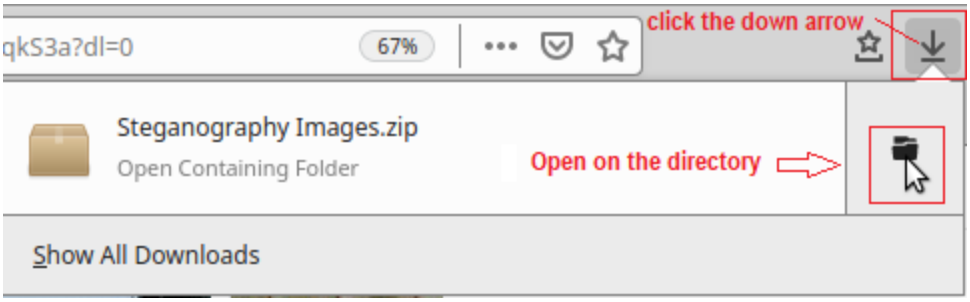
From the Dropbox location, click on the download link in the upper left corner. From the context menu, select Direct download.



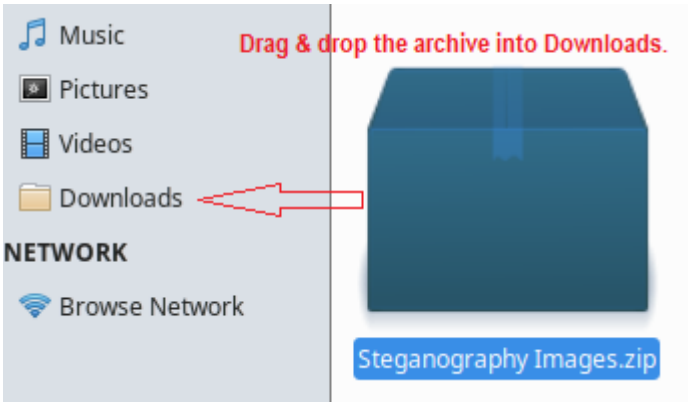
Save the file. The files are saved as a zip archive to your **home/csi** directory.



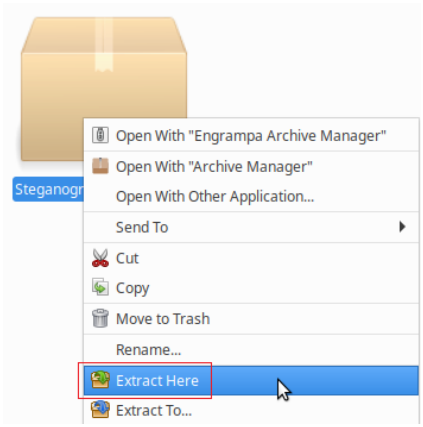
From your browser, open the directory and extract the contents of the zip file.

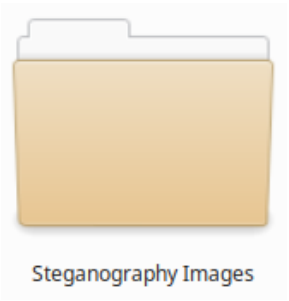


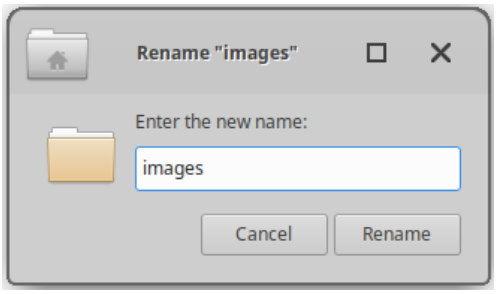
Place and hold your left mouse button on the archive. Drag for the archive over to your downlaod directory. Let go of the left mouse button.



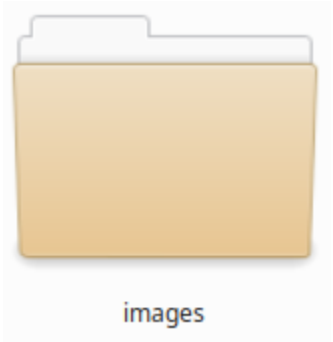
Inside the Download directory, right click on the archive and from the context menu **Extract Here.**







Right click on the extracted directory and rename the extracted directory to just, “images.”



Close out file explorer. Close out any instance of Firefox. Return to the desktop, launch a terminal session.

From the terminal, change directory location to your Downloads directory. Remember, all Linux commands are case sensitive.

At the terminal, type **cd Downloads** hit enter.

```
csi@csi-analyst:~$ cd Downloads
csi@csi-analyst:~/Downloads$
```

At the terminal type **ls** hit enter. The **ls** command lists the contents of the Download directory.

```
csi@csi-analyst:~/Downloads$ ls
 csitools.zip   images  'Steganography Images.zip'
csi@csi-analyst:~/Downloads$
```

At the terminal prompt, type **cd images**

```
csi@csi-analyst:~/Downloads$ cd images
csi@csi-analyst:~/Downloads/images$
```

Again, at the prompt type the **ls** command to see the contents of the images folder.

```
csi@csi-analyst:~/Downloads/images$ ls
funny-faces-cartoon-troll.jpeg  nsa.png             sponge_bob.jpg  zebras.bmp
mona-lisa.jpg                   original-zebras.bmp  stallin.jpg
csi@csi-analyst:~/Downloads/images$
```

This is the directory we will be working out of.

Hide an Image Inside an Image.

In this exercise we will use Steghide to embed the mon-lisa.jpg image into the zebras.bmp image.

At the terminal prompt, type: **`steghide embed -ef mona-lisa.jpg -cf zebras.bmp`**

Hit enter.

Type in a passphrase. This is used to encrypt the file. (remember it!)

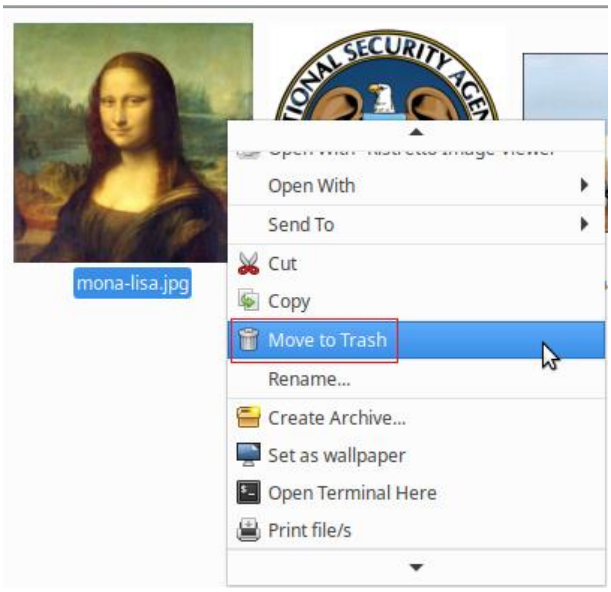
Retype your passphrase. (I used the passphrase, Password123!)

Hit enter.

```
csi@csi-analyst:~/Downloads/images$ ls
funny-faces-cartoon-troll.jpeg  mona-lisa.jpg  nsa.png  original-zebras.bmp  sponge_bob.jpg  stallin.jpg  zebras.bmp
csi@csi-analyst:~/Downloads/images$ steghide embed -ef mona-lisa.jpg -cf zebras.bmp
Enter passphrase:
Re-Enter passphrase:
embedding "mona-lisa.jpg" in "zebras.bmp"... done%
csi@csi-analyst:~/Downloads/images$
```

In after just a few moments, the mona-lisa.jpg image has been embedded in the zebras.bmp image.

From the desktop, open **File System**. Open your **Download** directory, open your **images** directory find and move the **mona-lisa.jpg** image to trash.



Double click to open the zebras.bmp image. The picture opens up using image viewer. Note the file structure, colors, everything about the image looks the same.

Back at your terminal, you're now ready to extract the file we embedded earlier.

At the terminal prompt, type: `steghide extract -sf zebras.bmp -xf mlisa.jpg`

Type in your passphrase. Hit enter.

Data is extracted as mlisa.jpg.

At the prompt, type, ls to see the extracted file is present.

```
csi@csi-analyst:~/Downloads/images$ ls
funny-faces-cartoon-troll.jpeg  nsa.png  original-zebras.bmp  sponge_bob.jpg  stallin.jpg  zebras.bmp
csi@csi-analyst:~/Downloads/images$ steghide extract -sf zebras.bmp -xf mlisa.jpg
Enter passphrase:
wrote extracted data to "mlisa.jpg".
csi@csi-analyst:~/Downloads/images$ ls
funny-faces-cartoon-troll.jpeg  mlisa.jpg  nsa.png  original-zebras.bmp  sponge_bob.jpg  stallin.jpg  zebras.bmp
csi@csi-analyst:~/Downloads/images$
```

From the desktop, open your File System, open your Downloads directory, and finally open your images directory. Find your mlisa.jpg image.

Commands used:

-ef, --embedfile select file to be embedded

-cf, --coverfile select cover-file

-sf, --stegofile select stego file

-xf write the extracted data to <filename>

Summary –

The one huge caveat with using Steghide is the file being embedded into the destination or cover file must be much smaller in size, width and in height. If the payload is too big, steghide will just refuse to complete the operation.