StegHide:

Steghide is a steganography program capable of hiding data in a variety of image and audio files. The color and sample frequencies aren't changed sequentially, making the embedding resistant against first-order statistical tests.

Features:

- Embedded data compression
- Support for JPEG, BMP, WAV, and AU files
- Embedded data encryption
- Decryption via password
- Uses various algorithms for encryption
- Embedding of a checksum to verify the integrity of extracted data

Installation:

- sudo apt-get install steghide -y

Find a picture:

Steghide supports JPEG and BMP image file types. Once you have an image, make sure that it is available.

Your secret text file is ready:

sudo nano steg.txt

You can check to see if the text file is created and the contents by running the following command.

cat steg.txt

Embedding data in the image:

To achieve this, Run the following command to embed “luv.txt” in an image named “steg.jpeg”.

steghide embed -ef steg.txt -cf steg.jpeg

Where

- ***Steghide*** *– Program Name*
- ***Embed*** *– this is the command*
- ***-cf*** *– This flag is for the cover file (the file used to embed the data)*
- ***filename*** *– this is the name of the cover file*
- ***-ef*** *– This flag is for the embed file (the file that will be embedded)*
- ***Filename*** *– This is the name of the embedded file*

Extraction of Data From Image Via Steghide:

steghide extract -sf steg.jpeg

Password Protect Files:

This command is different in that it specifies a password in the command itself, therefore, we do not need to specify it separately.

steghide embed -ef steg.txt -cf steg.jpeg -p 1234

sudo steghide extract -sf luv.jgeg -p 1012

Retrieve Information of Embedded File:

If we have an image in which the data is suspected to be hidden and if so, what algorithm is used to encrypt the data in the file? Then we will use the following command:

steghide info steg.jpeg

Verbose Mode

steghide embed -v -ef steg.txt -cf steg.jpeg