**AIM:**

Perform Steganography using steghide

**REQUIREMENTS:**

Steghide

Kali Linux

Word for documentation

**IMAGE FILE:**

Valley.jpg

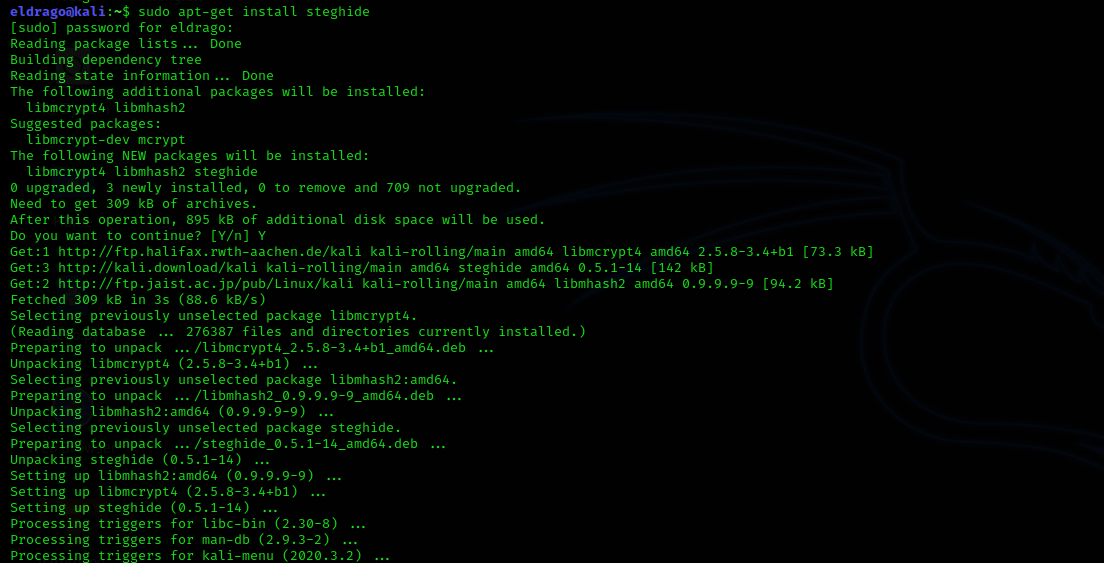


**Steghide**:

* It is a steganography program that is able to hide data in various kinds of image- and audio-files. The colour- respectively sample-frequencies are not changed thus making the embedding resistant against first-order statis-tical tests.
* Features include the compression of the embedded data, encryption of the embedded data and automatic integrity checking using a checksum.
* The JPEG, BMP, WAV and AU file formats are supported for use as cover file.
* There are no restrictions on the format of the secret data

**Installation:**

* Just type in command **sudo apt-get install steghide**



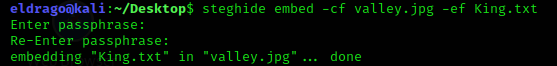
* help, --help Display a help screen. No arguments required.



* To embed the text in the image using steghide, we need to enter our text in a file



* When data is entered to file embed the text in the image.jpg.
* Run this command **steghide embed -cf valley.jpg -ef King.txt**.
* It will ask for passphrase, enter it and enter it again.
* We should use the embed command if we want to embed secret data in a cover file.
* It has arguments:
* -ef, --embedfile filename
* Specify the file that will be embedded (the file that contains the secret message).
* Note that steghide embeds the original file name in the stego file.
* When extracting data (see below) the default behaviour is to save the embedded file into the current directory under its original name.
* If this is omitted or filename is -, steghide will read the secret data from standard input.
* -cf, --cover file filename
* Specify the cover file that will be used to embed data.
* The cover file must be in one of the following formats: AU, BMP, JPEG or WAV.
* If this argument is omitted or filename is -, steghide will read the cover file from standard input.



* The text in image has been embed.
* Now let’s extract that embed test from image.
* We need to run this command steghide extract -sf image.jpg.
* It will ask for passphrase enter it. The data is been extracted to file.
* If you have received a file that contains a message that has been embedded with steghide, use the extract command to extract it.
* The following argument: -sf, --stegofile filename specify the stego file (the file that contains embedded data).
* If this argument is omitted or filename is -, steghide will read a stego file from standard input.

