Date: 04 /01 /2025

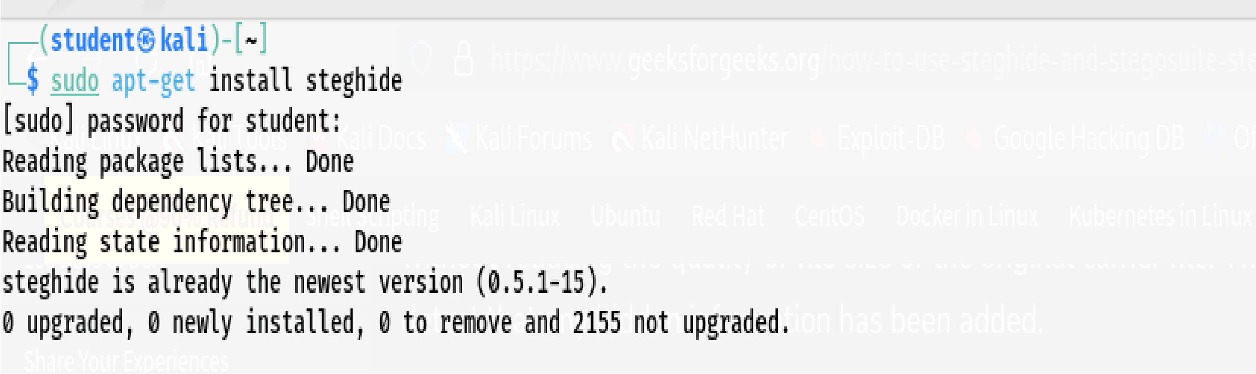
Lab Practical #_4:

Perform steganography and DOS attack.

Step 1:- **Steghide : Installation & Usage**

Steghide is a free and open source steganography program that allows you to hide secret files or messages within audio, image, and video files. It works right from the command line interface in Kali Linux. The key advantage of Steghide is that it can embed data without reducing the quality or file size of the original carrier file. This makes it difficult to detect that any hidden information has been added.
To use Steghide, you first need to install it in Kali Linux. You can do this easily by typing the following command :

```
sudo apt-get install steghide
```

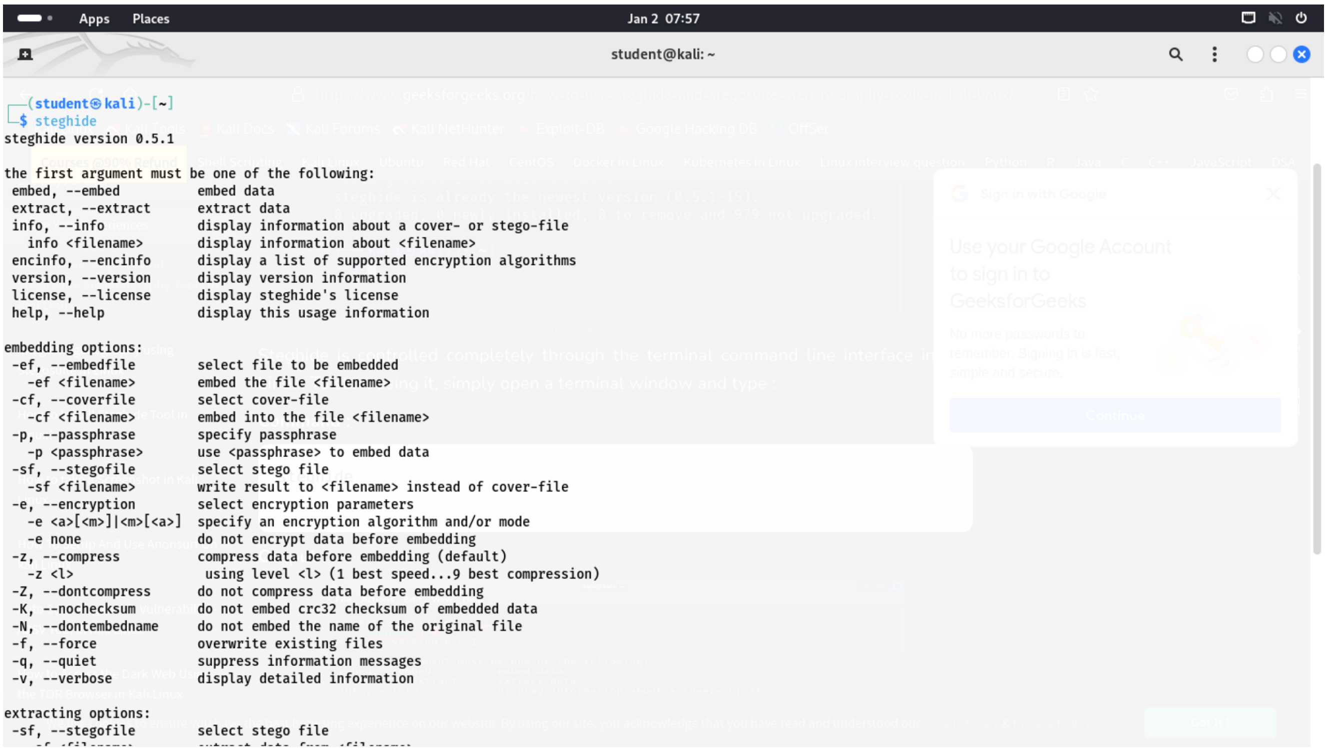


```
┌──(student㉿kali)-[~]
└─$ sudo apt-get install steghide
[sudo] password for student:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
steghide is already the newest version (0.5.1-15).
0 upgraded, 0 newly installed, 0 to remove and 2155 not upgraded.
```

Date: 04 /01 /2025

Step:-2 Steghide is controlled completely through the terminal command line interface in Kali Linux. To start using it, simply open a terminal window and type :

Steghide

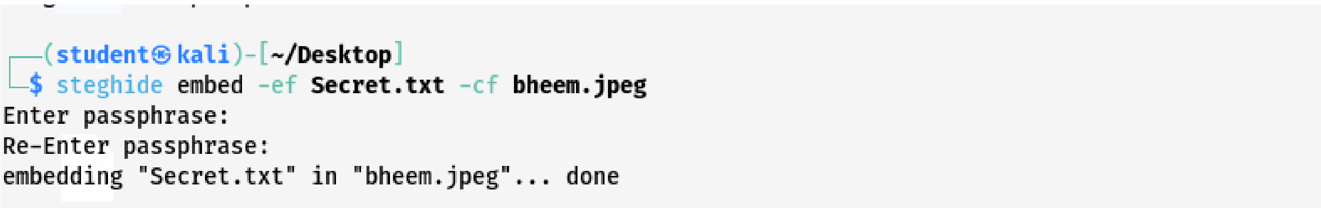


```
┌──(student㉿kali)-[~]
└─$ steghide
steghide version 0.5.1

the first argument must be one of the following:
 embed, --embed          embed data
 extract, --extract      extract data
 info, --info            display information about a cover- or stego-file
   info <filename>       display information about <filename>
 encinfo, --encinfo      display a list of supported encryption algorithms
 version, --version      display version information
 license, --license      display steghide's license
 help, --help            display this usage information

embedding options:
 -ef, --embedfile        select file to be embedded
   -ef <filename>        embed the file <filename>
 -cf, --coverfile        select cover-file
   -cf <filename>        embed into the file <filename>
 -p, --passphrase        specify passphrase
   -p <passphrase>       use <passphrase> to embed data
 -sf, --stegofile        select stego file
   -sf <filename>        write result to <filename> instead of cover-file
 -e, --encryption        select encryption parameters
   -e <a>[<m>]|<m>[<a>]  specify an encryption algorithm and/or mode
   -e none               do not encrypt data before embedding
 -z, --compress          compress data before embedding (default)
   -z <l>                 using level <l> (1 best speed...9 best compression)
 -Z, --dontcompress      do not compress data before embedding
 -K, --nochecksum        do not embed crc32 checksum of embedded data
 -N, --dontembedname     do not embed the name of the original file
 -f, --force             overwrite existing files
 -q, --quiet             suppress information messages
 -v, --verbose           display detailed information

extracting options:
 -sf, --stegofile        select stego file
   -sf <filename>        extract data from <filename>
```

Date: 04 /01 /2025

Step:-3 Create a text file called " secret.txt " and add some simple secret message text to it. Save it in your working directory. Also place the image file you want to use to hide the data, like " gfg.jpg ", in the same folder. Open a terminal window and use the " steghide embed " command to embed " secret.txt " into " bheem.jpg ".

```
steghide embed -ef Secret.txt -cf bheem.jpeg
```



```
┌──(student㉿kali)-[~/Desktop]
└─$ steghide embed -ef Secret.txt -cf bheem.jpeg
Enter passphrase:
Re-Enter passphrase:
embedding "Secret.txt" in "bheem.jpeg"... done
```

It will ask you to create a password. Choose a strong password and enter it. This will be needed to extract the hidden data later. Steghide will embed "secret.txt" inside "kevinmitnick.jpg" using the password encryption.

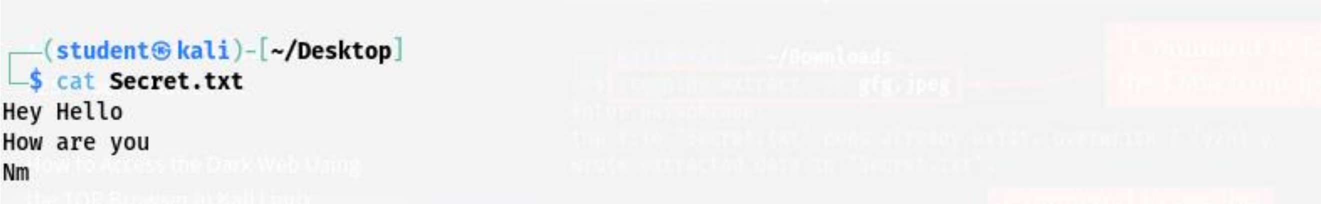
Now the image file contains the secret data entirely hidden within it. You can safely share or store the image file like normal. When ready, use the following below command with the password to retrieve the embedded " Secret.txt " file.

Date: 04 /01 /2025

Step:-4 Command to Extract the Data from jpg file

```
steghide extract -sf bheem.jpeg
```

```
cat Secret.txt
```

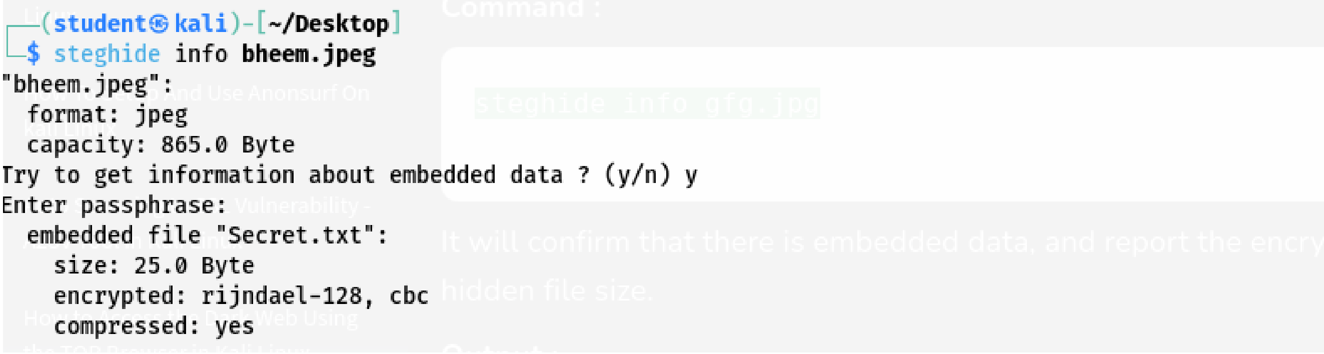


```
┌──(student㉿kali)-[~/Desktop]
└─$ cat Secret.txt
Hey Hello
How are you
Nm
```

Date: 04 /01 /2025

Step:-5 It will confirm that there is embedded data, and report the encryption algorithm and hidden file size below is the command:

```
steghide info gfg.jpg
```



```
┌──(student㉿kali)-[~/Desktop]
└─$ steghide info bheem.jpeg
"bheem.jpeg":
  format: jpeg
  capacity: 865.0 Byte
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "Secret.txt":
    size: 25.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

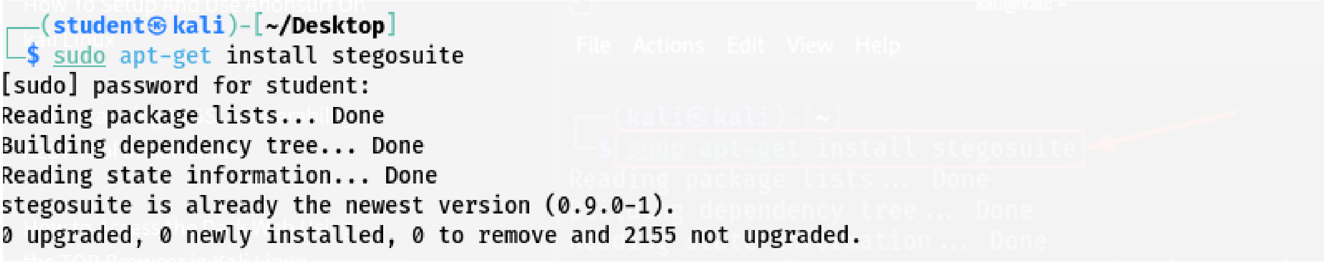
Date: 04 /01 /2025

Step:-6 StegoSuite : Installation & Usage

StegoSuite is another free steganography tool included in Kali Linux. The main difference from Steghide is that StegoSuite provides a graphical interface, making it more user-friendly.

To install StegoSuite, open a terminal and type :

```
sudo apt-get install stegosuite
```

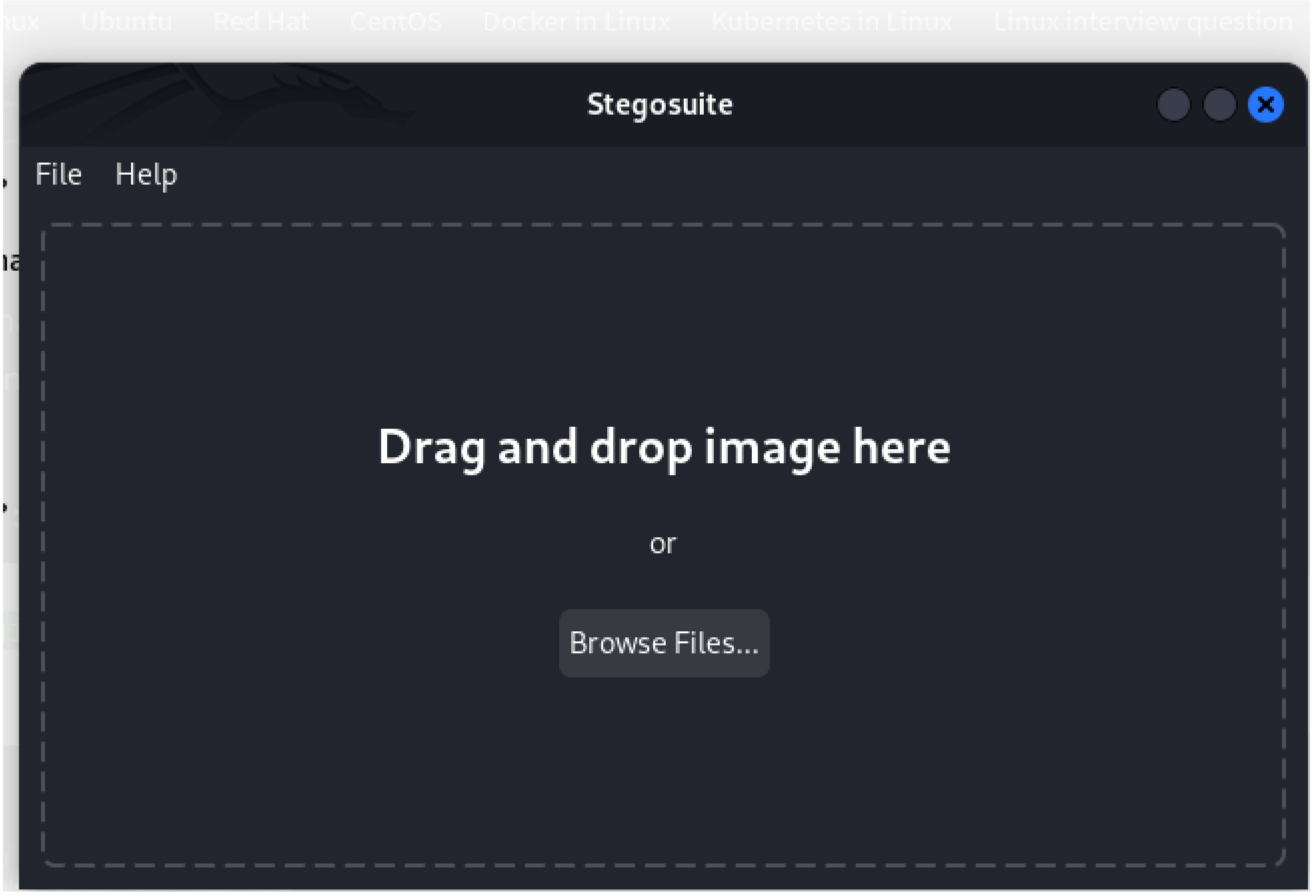


```
┌──(student㉿kali)-[~/Desktop]
└─$ sudo apt-get install stegosuite
[sudo] password for student:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
stegosuite is already the newest version (0.9.0-1).
0 upgraded, 0 newly installed, 0 to remove and 2155 not upgraded.
```

Date: 04 /01 /2025

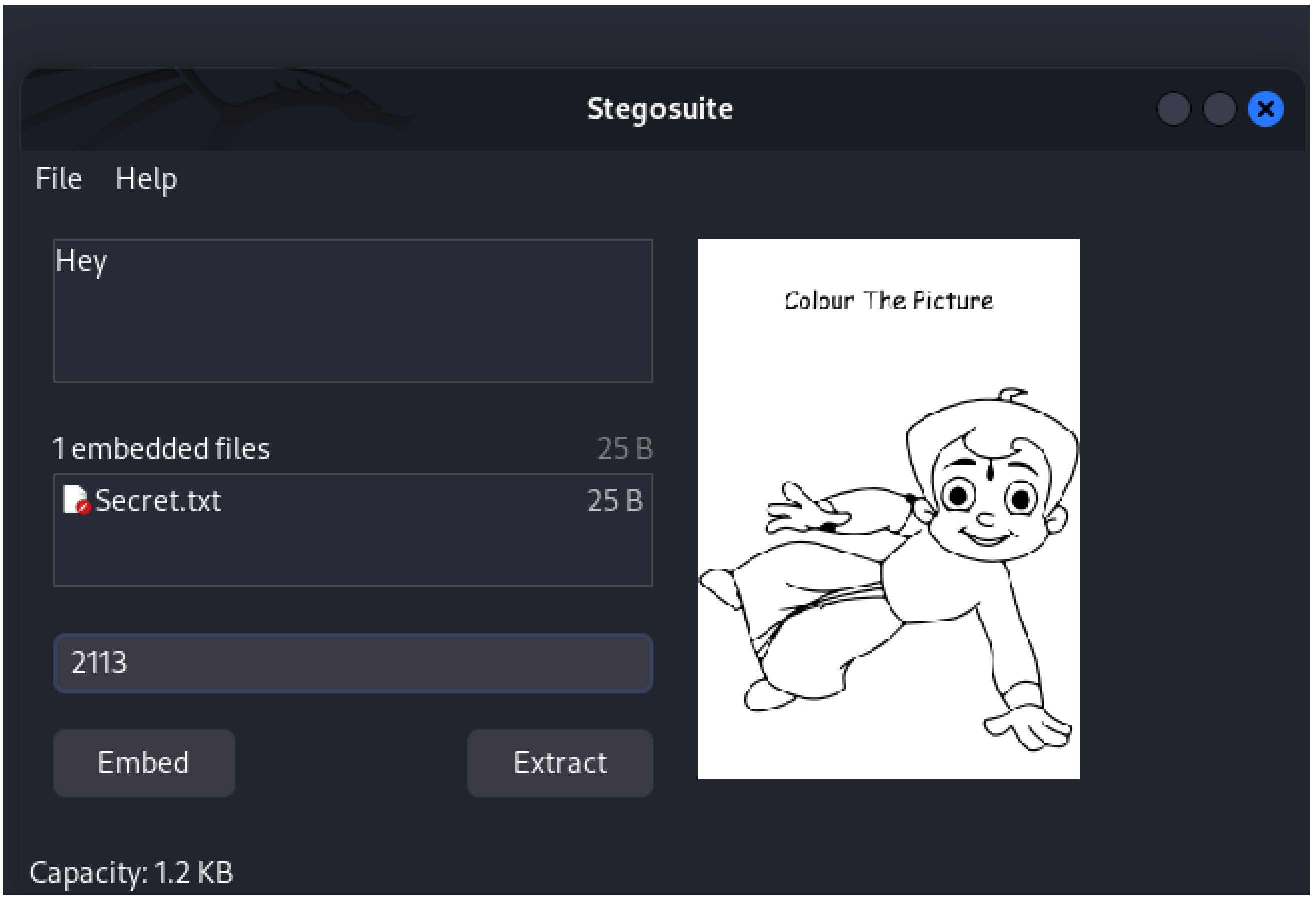
Step:-7 Once you have installed the StegoSuite package in Kali Linux, you can easily start using the program. Now you just need to type the following command to Launch the StegoSuite Tool.

```
stegosuite gui
```



Date: 04 /01 /2025

Step:-8 After Selecting the Image file Enter the secret text Message or Just Drag and Drop the " Secret.txt " file. Then Set the Password to Encrypt the Image file and Click on Embed. Follow the Steps as Shown in the Below GIF file.



Hey

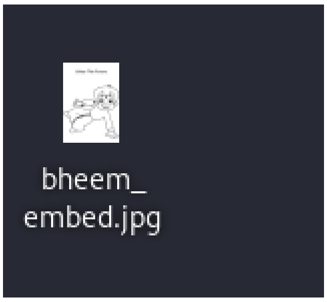
1 embedded files 25 B

Secret.txt 25 B

2113

Capacity: 1.2 KB

Step:-9 After that you will see this New file created on the Desktop name " gfg_embed.png " this file include our hidden file in it.



Now the image file contains the secret data entirely hidden within it You can safely share or store the image file like normal. Whenever you want to see the Hidden Text file just use " stegosuite gui " Command and Select the New File that created onto our Desktop and Just type the Password and hit the Extract Button.