README

-Detecting-steganography-with-tools-like-StegExpose-analyzing-file-signatures

AIM:

To detect hidden data using steganography detection tools like StegExpose and analyze file signatures for authenticity and manipulation.

DESIGN STEPS:

Step 1:

Install StegExpose or use the JAR version to detect steganography in image files.

Step 2:

Run StegExpose on a directory of suspected image files using the command:

Step 3:

Analyze file signatures using tools like file, binwalk, or xxd to check for inconsistencies or embedded content.

PROGRAM:

StegExpose and File Signature Analysis Commands

PROCEDURE:

1.Install and Set Up StegExpose

- a) Download the StegExpose .jar file from the official repository.
- b) Ensure Java Runtime Environment (JRE) is installed.
- c) Run the tool on an image or a folder of images:\
- d) The output will list detection scores and a "suspect" verdict if steganography is found.

2.Scan Individual Files

- a) Run StegExpose on a single image:
- b) The tool uses statistical analysis methods like RS analysis, Sample Pair
- c) analysis, and Chi-square attack to detect hidden content.

3.Analyze File Signatures

- a) Use Linux commands to verify the file's true format:
- b) Every file type has a magic number (e.g., JPEG files start with FFD8).
- c) Comparing the actual signature with the file extension helps identify mismatches or embedded file tricks.

4. Cross-Check File Behavior

- a) Rename the file (e.g., mv suspicious.jpg suspicious.zip) and try extracting it:
- b) Sometimes, files are disguised (e.g., a ZIP file hidden as a JPG), and this trick helps uncover such embedded archives.

5.Optional: Use Other Tools

- a) Tools like binwalk, stegsolve, or zsteg can be used for deeper analysis, especially for PNG files or binary dumps.

OUTPUT:

1.Install and Verify Steghide Tool

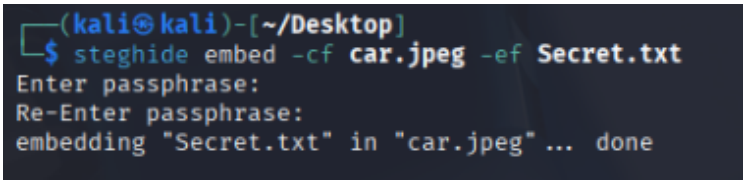
```
sudo apt update
sudo apt install steghide
```

2.Embed the Secret Message into the Image

- If you are in the directory of the suspected image use the following command:

  Example:

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



- Else mention the folder path you want to check using the following command :

  Example:

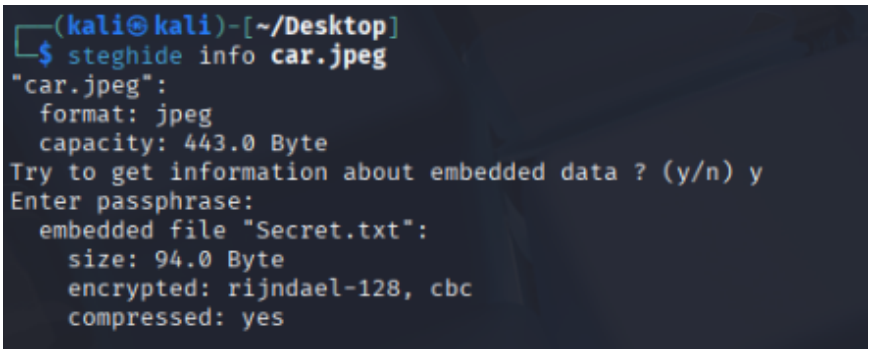
```
steghide embed -cf /home/kali/Desktop/car.jpeg -ef /home/kali/Desktop/Secre
```

3.Retrieve Information About the Embedded Data

- If you are in the directory of the suspected image use the following command:

  Example:

```
steghide info car.jpeg
```



- Else mention the folder path you want to check using the following command :

  Example:

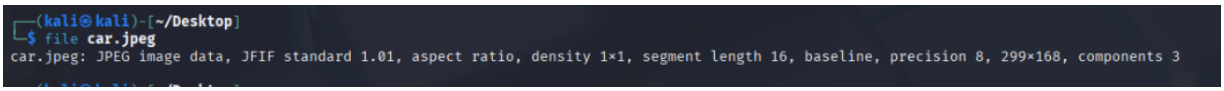
```
steghide info /home/kali/Desktop/car.jpeg
```

4.Analyze File Signature

- If you are in the directory of the suspected image use the following command:

Example:

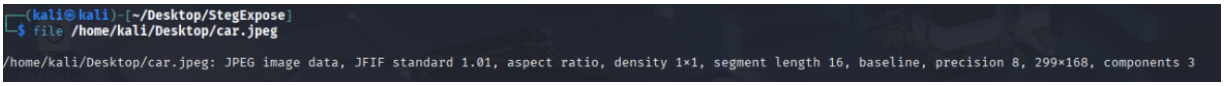
```
file car.jepg
```



- Else mention the folder path you want to check using the following command :

  Example:

```
file /home/kali/Desktop/car.jpeg
```

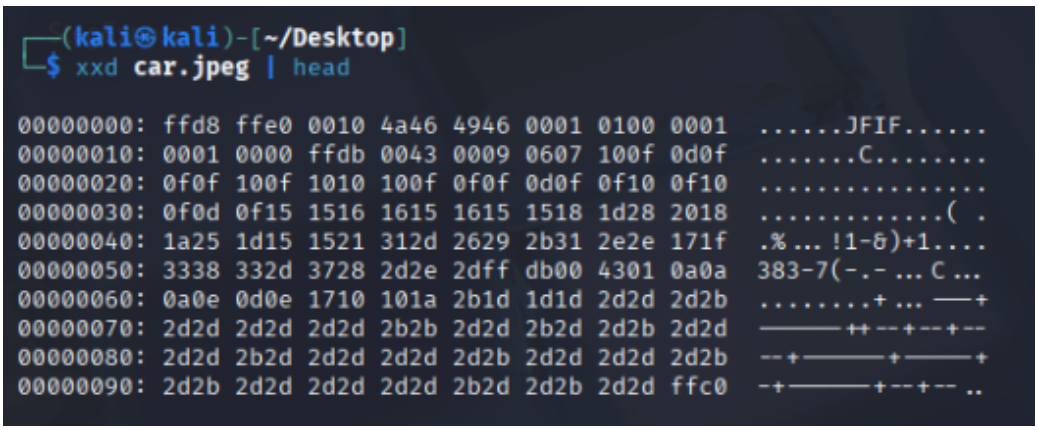


5.Analyze Hex Dump of File

- If you are in the directory of the suspected image use the following command:

  Example:

```
xxd car.jpeg | head
```



- Else mention the folder path you want to check using the following command :

  Example:

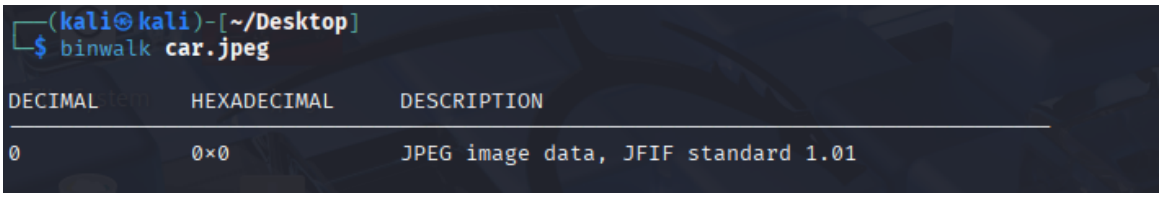
```
xxd /home/kali/Desktop/car.jpeg | head
```

6.Optional: Use Other Tools Like Binwalk And Stegsolve:

- **Binwalk:**
  - If you are in the directory of the suspected image use the following command:

Example:

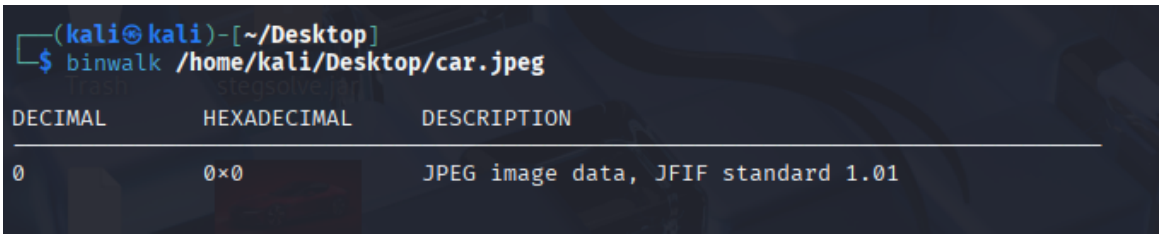
```
binwalk car.jpeg
```



- Else mention the folder path you want to check using the following command :

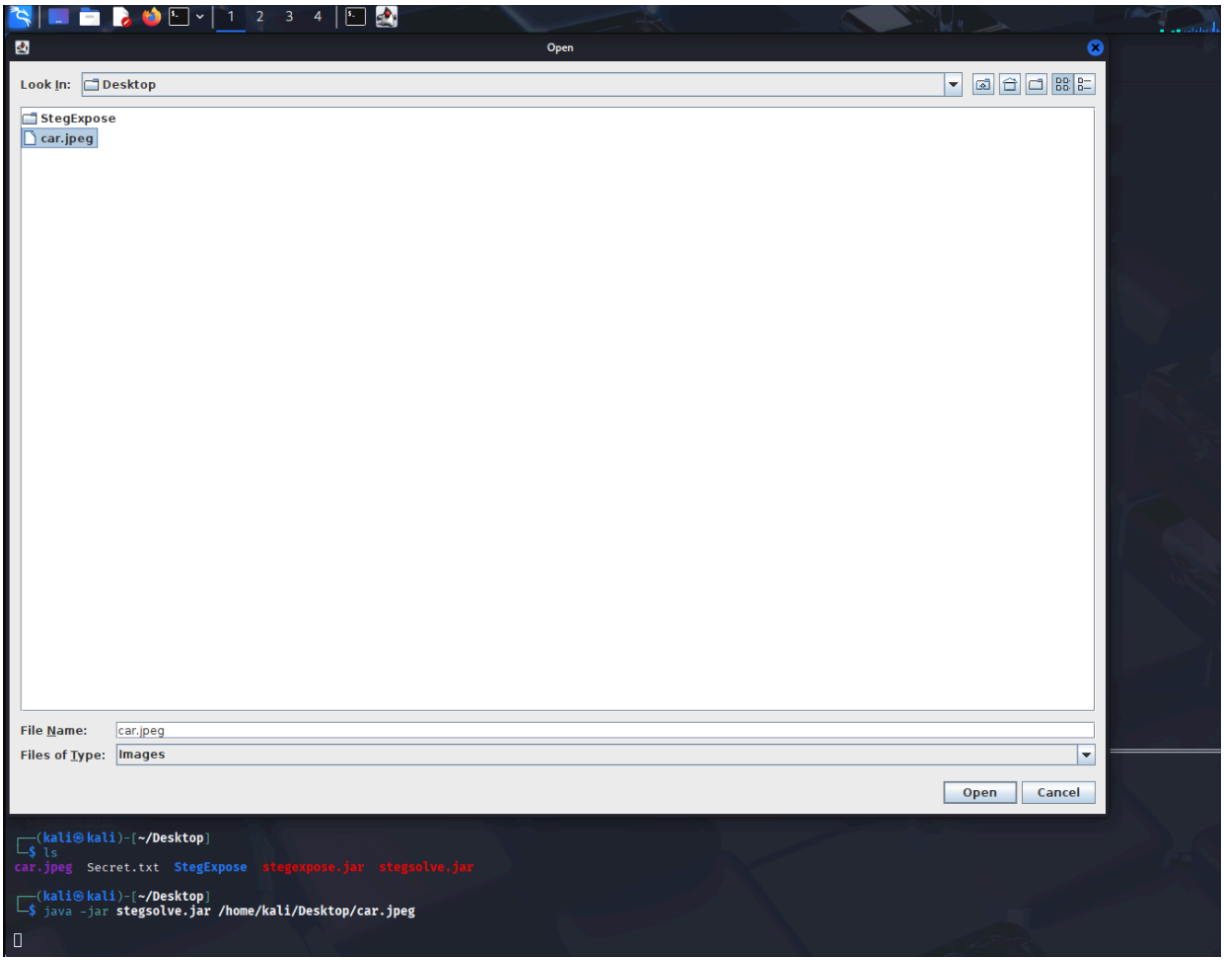
  Example:

```
binwalk /home/kali/Desktop/car.jpeg
```



- **Stegsolve:**
  - Command:

```
java -jar stegsolver.jar /home/kali/Desktop/car.jpeg
```

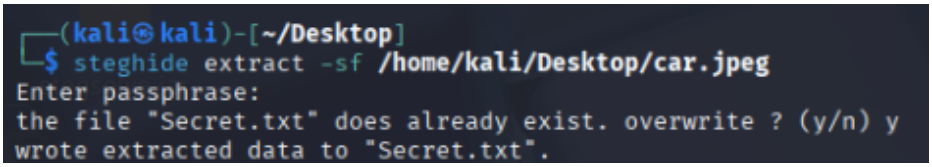


7.Extract the Hidden Secret from Image

- If you are in the directory of the suspected image use the following command:

  Example:

```
steghide extract -sf car.jpeg
```



- Else mention the folder path you want to check using the following command :

  Example:

```
steghide extract -sf /home/kali/Desktop/car.jpeg
```

RESULT:

Hidden data was successfully detected and file signatures were analyzed for irregularities.