

-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
```



```
(kali@kali)-[~]$ sudo apt-get install steghide
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  icu-devtools libbabel20230802 libbnn3 libflac12t64 libfuse3-3 libgeos3.13.0 libglapi-mesa libcub-dev libjxl0.10 liblbfgsb0 libopenh264-7 libpoppler145 libpython3.12-minimal libpython3.12-stdlib libpython3.
  python3-setproctitle python3.12-tk ruby-zeitwerk strongswan
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libbcrpt4 libbhash2
Suggested packages:
  libbcrpt-dev mcrpt
The following NEW packages will be installed:
  libbcrpt4 libbhash2 steghide
0 upgraded, 3 newly installed, 0 to remove and 261 not upgraded.
Need to get 309 kB of archives.
After this operation, 907 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:2 http://kali.download/kali kali-rolling/main amd64 libbhash2 amd64 0.9.9-10 [92.4 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 steghide amd64 0.5.1-15 [144 kB]
Get:1 http://mirror.freemove.org/kali kali-rolling/main amd64 libbcrpt4 amd64 2.5.8-8 [72.2 kB]
Fetched 309 kB in 2s (128 kB/s)
Selecting previously unselected package libbcrpt4:amd64.
(Reading database ... 433687 files and directories currently installed.)
Preparing to unpack .../libbcrpt4_2.5.8-8_amd64.deb ...
Unpacking libbcrpt4:amd64 (2.5.8-8) ...
Selecting previously unselected package libbhash2:amd64.
Preparing to unpack .../libbhash2_0.9.9-10_amd64.deb ...
Unpacking libbhash2:amd64 (0.9.9-10) ...
Selecting previously unselected package steghide.
Preparing to unpack .../steghide_0.5.1-15_amd64.deb ...
Unpacking steghide (0.5.1-15) ...
Setting up libbhash2:amd64 (0.9.9-10) ...
Setting up libbcrpt4:amd64 (2.5.8-8) ...
Setting up steghide (0.5.1-15) ...
Processing triggers for libc-bin (2.41-6) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2025.2.0) ...
```

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
```



```
(kali@kali)-[~/Desktop]
$ steghide embed -cf car.jpeg -ef Secret.txt
Enter passphrase:
Re-Enter passphrase:
embedding "Secret.txt" in "car.jpeg" ... done
```

- 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
```



```
(kali@kali)-[~/Desktop]
$ steghide info car.jpeg
"car.jpeg":
  format: jpeg
  capacity: 443.0 Byte
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "Secret.txt":
    size: 94.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

- 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.jpeg
```



```
(kali@kali)-[~/Desktop]
$ file car.jpeg
car.jpeg: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 299x168, components 3
```

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

Example:

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



```
(kali@kali)-[~/Desktop/StegExpose]
$ file /home/kali/Desktop/car.jpeg
/home/kali/Desktop/car.jpeg: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 299x168, components 3
```

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
```



```
(kali@kali)-[~/Desktop]
$ xxd car.jpeg | head
00000000: ffd8 ffe0 0010 4a46 4946 0001 0100 0001 .....JFIF.....
00000010: 0001 0000 ffd9 0043 0009 0607 100f 0d0f .....C.....
00000020: 0f0f 100f 1010 100f 0f0f 0d0f 0f10 0f10 .....
00000030: 0f0d 0f15 1516 1615 1615 1518 1d28 2018 .....( .
00000040: 1a25 1d15 1521 312d 2629 2b31 2e2e 171f .%...!1-6)+1...
00000050: 3338 332d 3728 2d2e 2dff db00 4301 0a0a 383-7(-.-...C...
00000060: 0a0e 0d0e 1710 101a 2b1d 1d1d 2d2d 2d2b .....+...--+
00000070: 2d2d 2d2d 2d2d 2b2b 2d2d 2b2d 2d2b 2d2d .....++--+--+
00000080: 2d2d 2b2d 2d2d 2d2d 2d2b 2d2d 2d2d 2d2b --+-----+--+
00000090: 2d2b 2d2d 2d2d 2d2d 2b2d 2d2b 2d2d ffc0 -+-----+--+..
```

- 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
```



```
(kali㉿kali)-[~/Desktop]  
$ binwalk car.jpeg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01

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

Example:

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



```
(kali㉿kali)-[~/Desktop]  
$ binwalk /home/kali/Desktop/car.jpeg
```

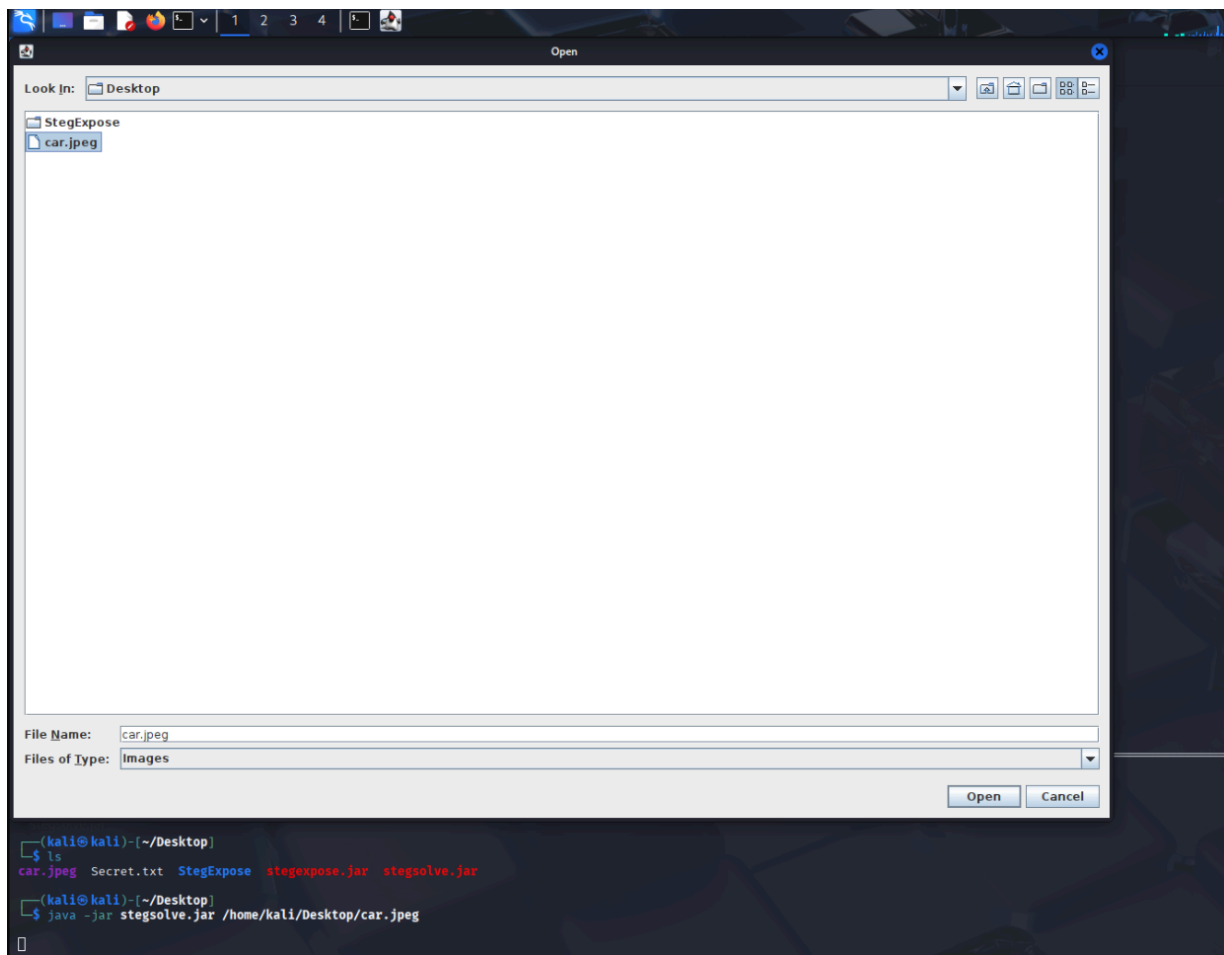
DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01

- 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
```



```
(kali@kali)-[~/Desktop]  
$ steghide extract -sf /home/kali/Desktop/car.jpeg  
Enter passphrase:  
the file "Secret.txt" does already exist. overwrite ? (y/n) y  
wrote extracted data to "Secret.txt".
```

- 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.