Module B6: Steganography File Recovery

Pre-requisite Knowledge and Skills:

1. Understand basic of encryption technology

Learning Objectives

1. Understand the basic of steganography techniques.
2. Be exposed to steganography file un-hide process.

Recommended Running Environment/Tools:

1. Windows OS
2. Stegdetect
3. Invisible secret

Material:

1. map1.jpg
2. bitmap.bmp

Video Lecture:

1. Steganography File Recovery

Lab Assessment:

1. Steganography File Recovery Quiz

Acknowledgement:

The map1.jpg and bitmap.bmp are file recovered from the disk images from DFRWS 2003 Challenge, https://www.dfrws.org/search

Lab Instructions:

Scenario Description

You have two jpeg files, map1.jpg and map2.bmp, and two passwords: *right*, *lefty*. We need to find out whether there is anything different from a regular picture file.

Tasks

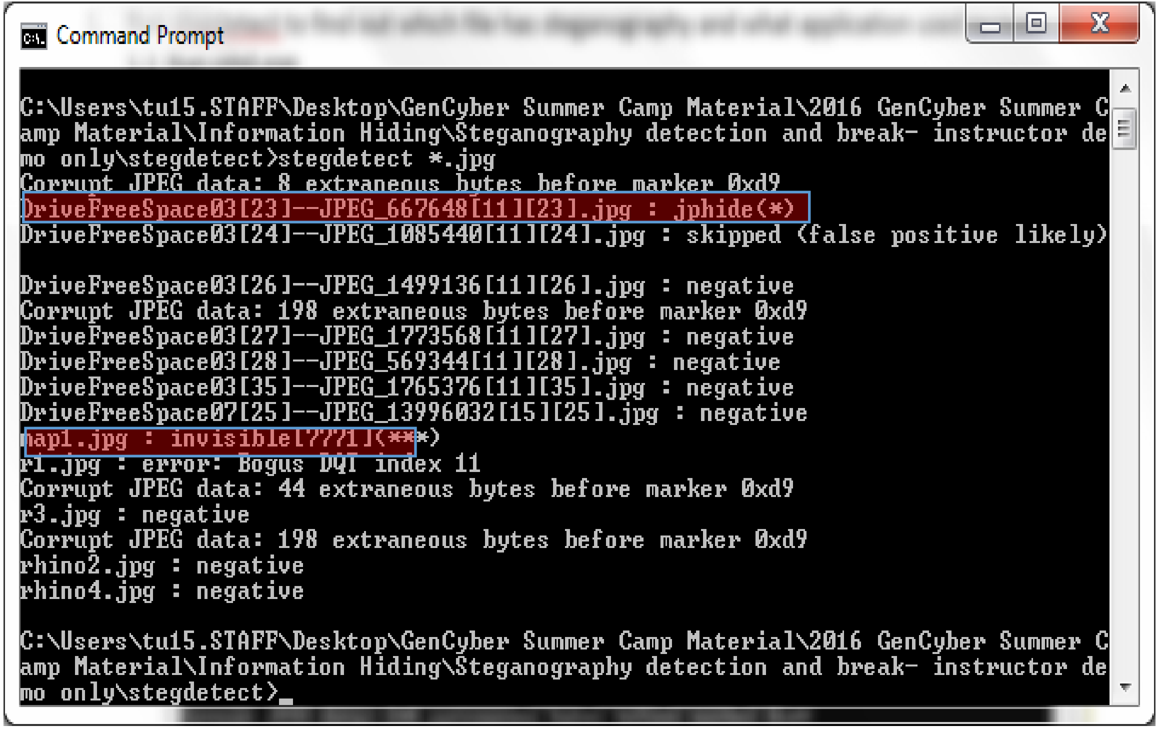
- Detect whether there is anything different from the regular picture fil for e.
- What application has been used to hide data into map1.jpg file
- Recover the following file from map1.jpg file
  - john.doc

Assessment

- Recover a .mov file from the map2.bmp file.

Instructions

1. Run stegdetect to find out which file has steganography and what application used to hide
   a. Run cmd.exe
   b. in command prompt, navigate to the stegdetect folder using cd C:\Users\username\Desktop\ 2016 GenCyber Summer Camp Material\Information Hiding\Steganography detection and break- instructor demo only\stegdetect
   c. run stegdetect : **stegdetect *.jpg** please note what tells about the map1.jpg

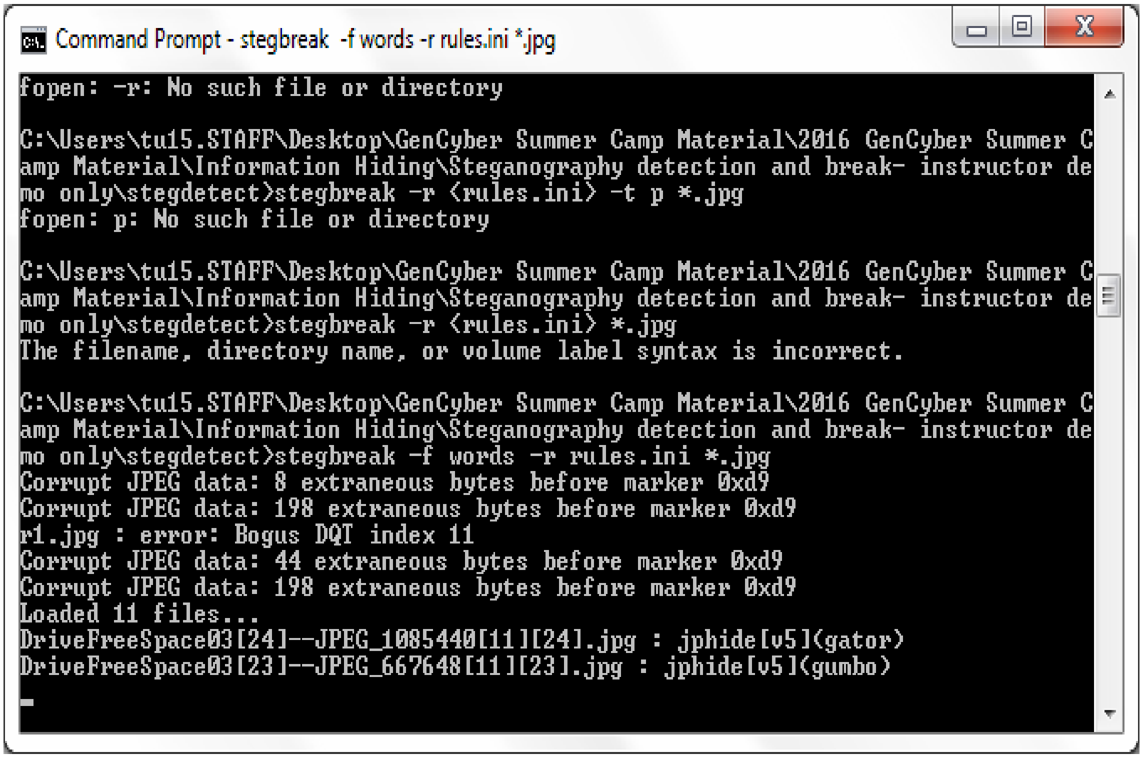


```
C:\Users\tu15.STAFF\Desktop\GenCyber Summer Camp Material\2016 GenCyber Summer C
amp Material\Information Hiding\Steganography detection and break- instructor de
mo only\stegdetect>stegdetect *.jpg
Corrupt JPEG data: 8 extraneous bytes before marker 0xd9
DriveFreeSpace03[23]--JPEG_667648[11][23].jpg : jphide(*)
DriveFreeSpace03[24]--JPEG_1085440[11][24].jpg : skipped (false positive likely)

DriveFreeSpace03[26]--JPEG_1499136[11][26].jpg : negative
Corrupt JPEG data: 198 extraneous bytes before marker 0xd9
DriveFreeSpace03[27]--JPEG_1773568[11][27].jpg : negative
DriveFreeSpace03[28]--JPEG_569344[11][28].jpg : negative
DriveFreeSpace03[35]--JPEG_1765376[11][35].jpg : negative
DriveFreeSpace07[25]--JPEG_13996032[15][25].jpg : negative
map1.jpg : invisible[7771](***)
r1.jpg : error: Bogus DQT index 11
Corrupt JPEG data: 44 extraneous bytes before marker 0xd9
r3.jpg : negative
Corrupt JPEG data: 198 extraneous bytes before marker 0xd9
rhino2.jpg : negative
rhino4.jpg : negative

C:\Users\tu15.STAFF\Desktop\GenCyber Summer Camp Material\2016 GenCyber Summer C
amp Material\Information Hiding\Steganography detection and break- instructor de
mo only\stegdetect>_
```

   d. run stegbreak: stegbreak -f words -r rules.ini *.jpg, **please note**



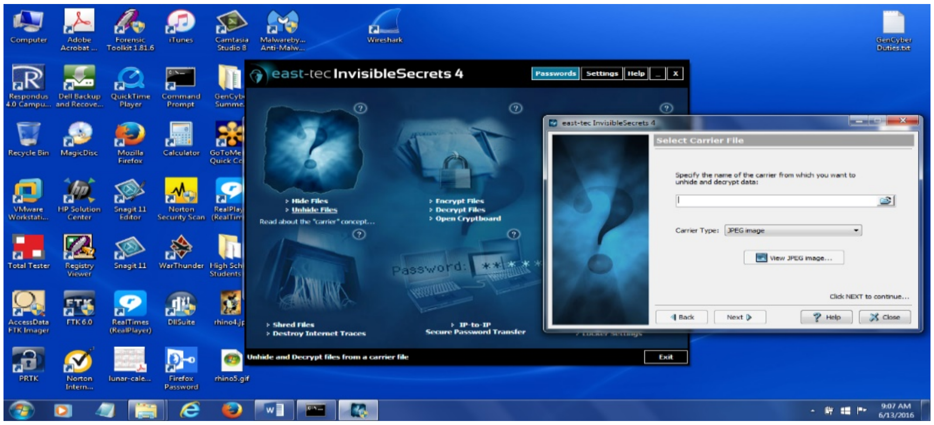
```
fopen: -r: No such file or directory

C:\Users\tu15.STAFF\Desktop\GenCyber Summer Camp Material\2016 GenCyber Summer C
amp Material\Information Hiding\Steganography detection and break- instructor de
mo only\stegdetect>stegbreak -r <rules.ini> -t p *.jpg
fopen: p: No such file or directory

C:\Users\tu15.STAFF\Desktop\GenCyber Summer Camp Material\2016 GenCyber Summer C
amp Material\Information Hiding\Steganography detection and break- instructor de
mo only\stegdetect>stegbreak -r <rules.ini> *.jpg
The filename, directory name, or volume label syntax is incorrect.

C:\Users\tu15.STAFF\Desktop\GenCyber Summer Camp Material\2016 GenCyber Summer C
amp Material\Information Hiding\Steganography detection and break- instructor de
mo only\stegdetect>stegbreak -f words -r rules.ini *.jpg
Corrupt JPEG data: 8 extraneous bytes before marker 0xd9
Corrupt JPEG data: 198 extraneous bytes before marker 0xd9
r1.jpg : error: Bogus DQT index 11
Corrupt JPEG data: 44 extraneous bytes before marker 0xd9
Corrupt JPEG data: 198 extraneous bytes before marker 0xd9
Loaded 11 files...
DriveFreeSpace03[24]--JPEG_1085440[11][24].jpg : jphide[v5](gator)
DriveFreeSpace03[23]--JPEG_667648[11][23].jpg : jphide[v5](gumbo)
_
```

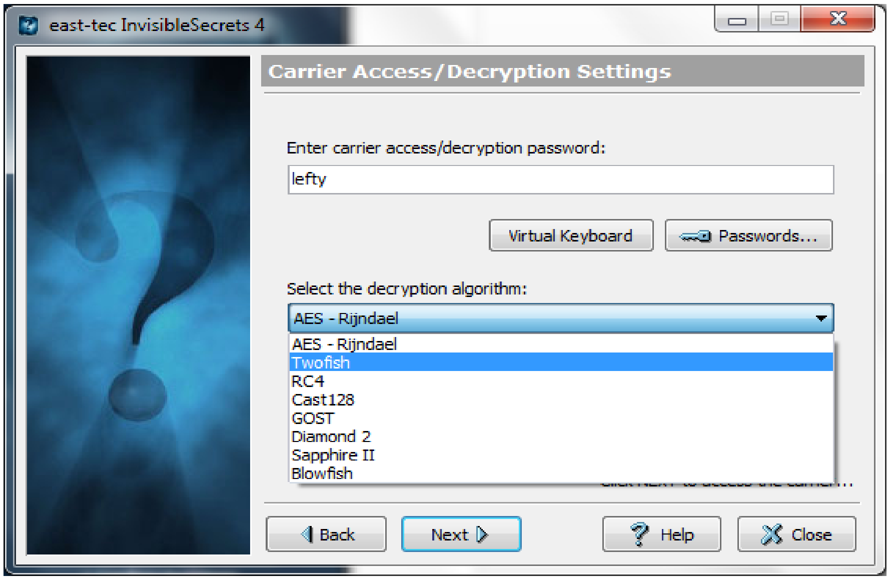
2. run invisible secret and select unhide



Specify the name of the carrier from which you want to unhide and decrypt data:

Carrier Type: JPEG image

3. select map1.jpg and put your password and select twofish as the encryption algorithm



Carrier Access/Decryption Settings

Enter carrier access/decryption password:

lefty

Select the decryption algorithm:

AES - Rijndael

4. you will unhide john.doc, **can you find another file, a music file (password: right)**?