Module B7: Additional 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 and Stegbreaker
3. jpseek

Material:

1. map1.jpg
2. bitmap.bmp

Video Lecture:

1. N/A

Lab Assessment:

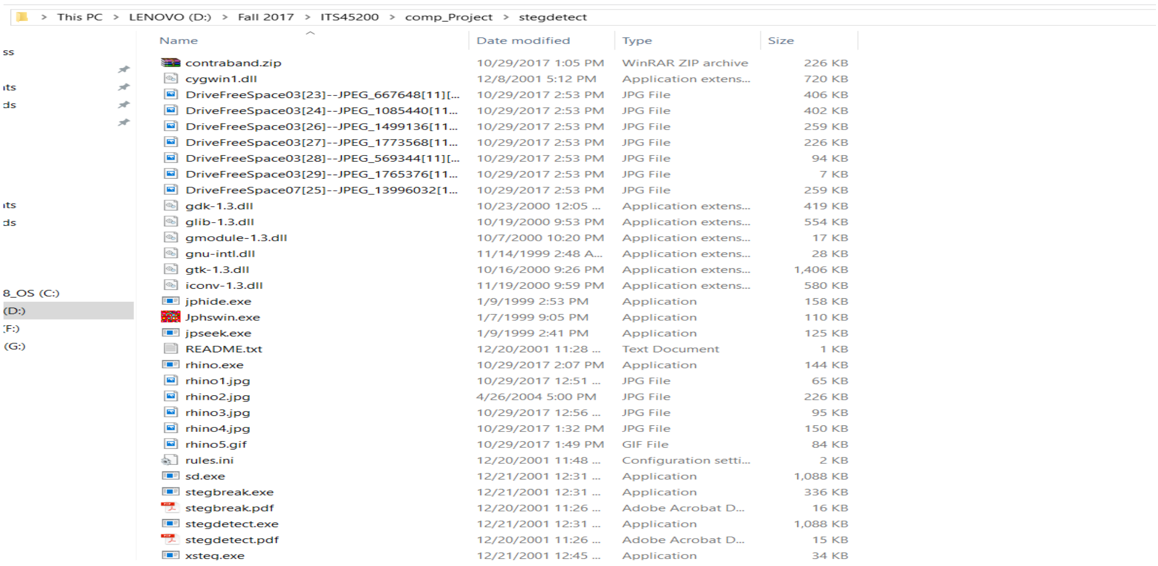
1. B7: Steganography File Recovery Quiz

Acknowledgement:

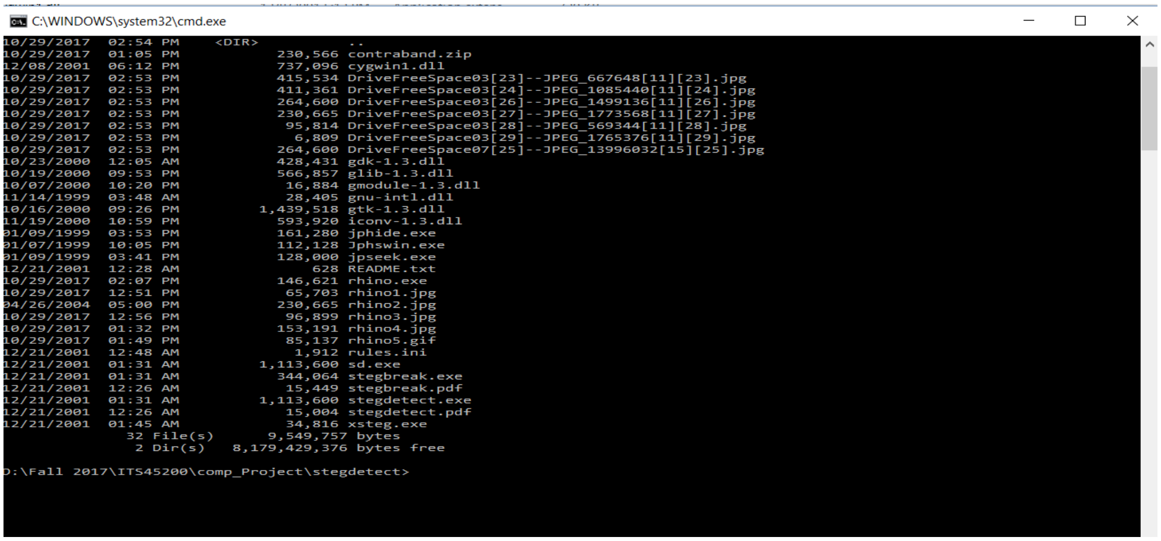
The evidences files are recovered from the disk images and network log traffics from DFRWS 2003 Challenge, https://www.dfrws.org/search

Lab Instructions:

1. Locate the evidences files
2. Copy the evidence file to stegdetect dirctory


This PC > LENOVO (D:) > Fall 2017 > ITS45200 > comp_Project > stegdetect
ss
its
ds
its
ds
8_OS (C:)
(D:)
:F:)
(G:)

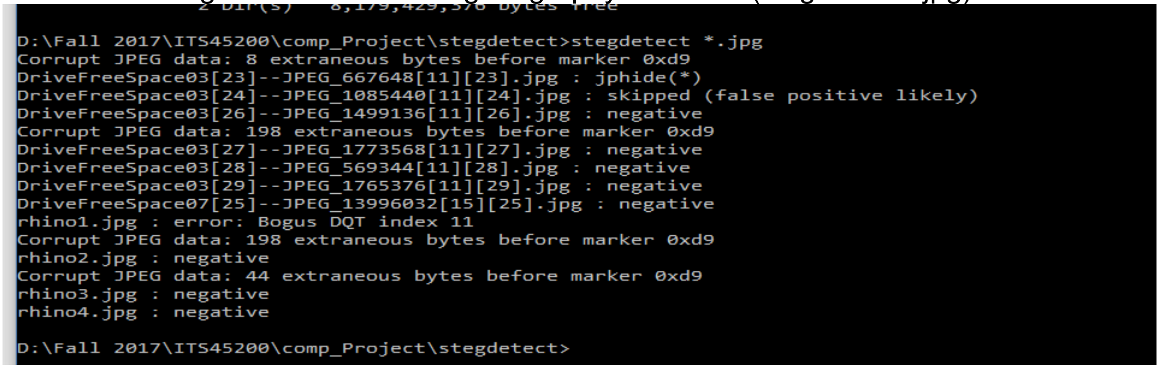
Name	Date modified	Type	Size
contraband.zip	10/29/2017 1:05 PM	WinRAR ZIP archive	226 KB
cygwin1.dll	12/8/2001 5:12 PM	Application extens...	720 KB
DriveFreeSpace03[23]--JPEG_667648[11][...	10/29/2017 2:53 PM	JPG File	406 KB
DriveFreeSpace03[24]--JPEG_1085440[11...	10/29/2017 2:53 PM	JPG File	402 KB
DriveFreeSpace03[26]--JPEG_1499136[11...	10/29/2017 2:53 PM	JPG File	259 KB
DriveFreeSpace03[27]--JPEG_1773568[11...	10/29/2017 2:53 PM	JPG File	226 KB
DriveFreeSpace03[28]--JPEG_569344[11][...	10/29/2017 2:53 PM	JPG File	94 KB
DriveFreeSpace03[29]--JPEG_1765376[11...	10/29/2017 2:53 PM	JPG File	7 KB
DriveFreeSpace07[25]--JPEG_13996032[1...	10/29/2017 2:53 PM	JPG File	259 KB
gdk-1.3.dll	10/23/2000 12:05 ...	Application extens...	419 KB
glib-1.3.dll	10/19/2000 9:53 PM	Application extens...	554 KB
gmodule-1.3.dll	10/7/2000 10:20 PM	Application extens...	17 KB
gnu-intl.dll	11/14/1999 2:48 A...	Application extens...	28 KB
gtk-1.3.dll	10/16/2000 9:26 PM	Application extens...	1,406 KB
iconv-1.3.dll	11/19/2000 9:59 PM	Application extens...	580 KB
jphide.exe	1/9/1999 2:53 PM	Application	158 KB
Jphswin.exe	1/7/1999 9:05 PM	Application	110 KB
jpseek.exe	1/9/1999 2:41 PM	Application	125 KB
README.txt	12/20/2001 11:28 ...	Text Document	1 KB
rhino.exe	10/29/2017 2:07 PM	Application	144 KB
rhino1.jpg	10/29/2017 12:51 ...	JPG File	65 KB
rhino2.jpg	4/26/2004 5:00 PM	JPG File	226 KB
rhino3.jpg	10/29/2017 12:56 ...	JPG File	95 KB
rhino4.jpg	10/29/2017 1:32 PM	JPG File	150 KB
rhino5.gif	10/29/2017 1:49 PM	GIF File	84 KB
rules.ini	12/20/2001 11:48 ...	Configuration setti...	2 KB
sd.exe	12/21/2001 12:31 ...	Application	1,088 KB
stegbreak.exe	12/21/2001 12:31 ...	Application	336 KB
stegbreak.pdf	12/20/2001 11:26 ...	Adobe Acrobat D...	16 KB
stegdetect.exe	12/21/2001 12:31 ...	Application	1,088 KB
stegdetect.pdf	12/20/2001 11:26 ...	Adobe Acrobat D...	15 KB
xsteg.exe	12/21/2001 12:45 ...	Application	34 KB



```
10/29/2017  02:54 PM    <DIR>          ..
10/29/2017  01:05 PM           230,566 contraband.zip
12/08/2001  06:12 PM           737,096 cygwin1.dll
10/29/2017  02:53 PM           415,534 DriveFreeSpace03[23]--JPEG_667648[11][23].jpg
10/29/2017  02:53 PM           411,361 DriveFreeSpace03[24]--JPEG_1085440[11][24].jpg
10/29/2017  02:53 PM           264,600 DriveFreeSpace03[26]--JPEG_1499136[11][26].jpg
10/29/2017  02:53 PM           230,665 DriveFreeSpace03[27]--JPEG_1773568[11][27].jpg
10/29/2017  02:53 PM            95,814 DriveFreeSpace03[28]--JPEG_569344[11][28].jpg
10/29/2017  02:53 PM             6,809 DriveFreeSpace03[29]--JPEG_1765376[11][29].jpg
10/29/2017  02:53 PM           264,600 DriveFreeSpace07[25]--JPEG_13996032[15][25].jpg
10/23/2000  12:05 AM           428,431 gdk-1.3.dll
10/19/2000  09:53 PM           566,857 glib-1.3.dll
10/07/2000  10:20 PM            16,884 gmodule-1.3.dll
11/14/1999  03:48 AM            28,405 gnu-intl.dll
10/16/2000  09:26 PM         1,439,518 gtk-1.3.dll
11/19/2000  10:59 PM           593,920 iconv-1.3.dll
01/09/1999  03:53 PM           161,280 jphide.exe
01/07/1999  10:05 PM           112,128 Jphswin.exe
01/09/1999  03:41 PM           128,000 jpseek.exe
12/21/2001  12:28 AM               628 README.txt
10/29/2017  02:07 PM           146,621 rhino.exe
10/29/2017  12:51 PM            65,703 rhino1.jpg
04/26/2004  05:00 PM           230,665 rhino2.jpg
10/29/2017  12:56 PM            96,899 rhino3.jpg
10/29/2017  01:32 PM           153,191 rhino4.jpg
10/29/2017  01:49 PM            85,137 rhino5.gif
12/21/2001  12:48 AM             1,912 rules.ini
12/21/2001  01:31 AM         1,113,600 sd.exe
12/21/2001  01:31 AM           344,064 stegbreak.exe
12/21/2001  12:26 AM            15,449 stegbreak.pdf
12/21/2001  01:31 AM         1,113,600 stegdetect.exe
12/21/2001  12:26 AM            15,004 stegdetect.pdf
12/21/2001  01:45 AM            34,816 xsteg.exe
              32 File(s)      9,549,757 bytes
               2 Dir(s)   8,179,429,376 bytes free

D:\Fall 2017\ITS45200\comp_Project\stegdetect>
```

3. Run stegdetect to detect steganography host files (stegdetect *.jpg)

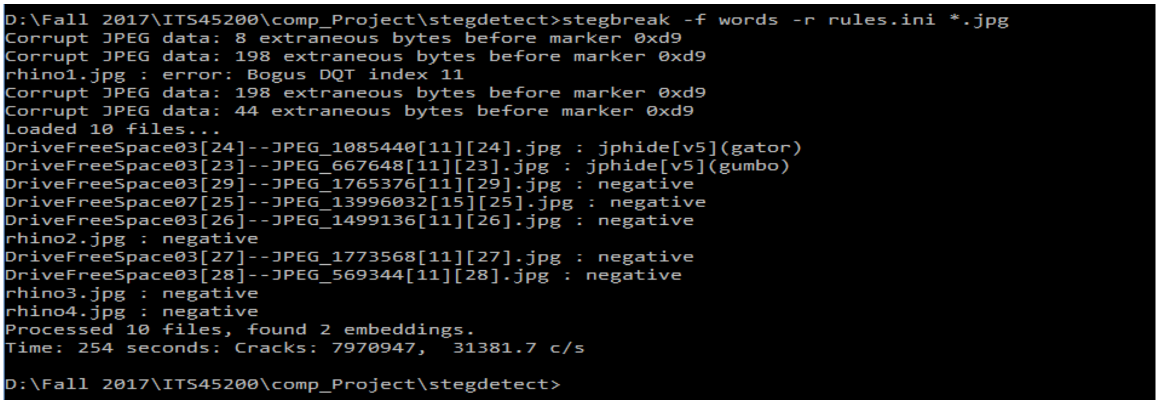


```
               2 Dir(s)   8,179,429,376 bytes free

D:\Fall 2017\ITS45200\comp_Project\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[29]--JPEG_1765376[11][29].jpg : negative
DriveFreeSpace07[25]--JPEG_13996032[15][25].jpg : negative
rhino1.jpg : error: Bogus DQT index 11
Corrupt JPEG data: 198 extraneous bytes before marker 0xd9
rhino2.jpg : negative
Corrupt JPEG data: 44 extraneous bytes before marker 0xd9
rhino3.jpg : negative
rhino4.jpg : negative

D:\Fall 2017\ITS45200\comp_Project\stegdetect>
```

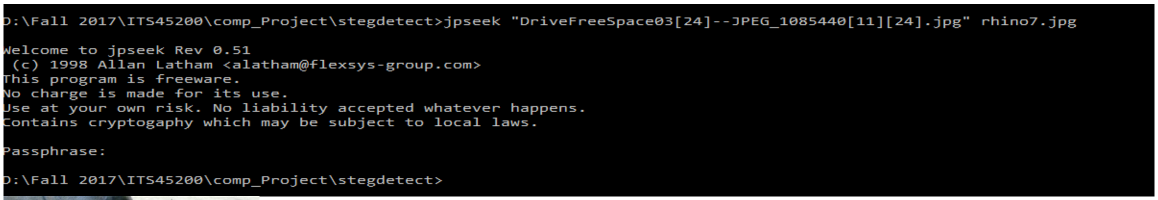
4. Run stegbreaker to recover the passwords used for encryption.



```
D:\Fall 2017\ITS45200\comp_Project\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
rhino1.jpg : error: Bogus DQT index 11
Corrupt JPEG data: 198 extraneous bytes before marker 0xd9
Corrupt JPEG data: 44 extraneous bytes before marker 0xd9
Loaded 10 files...
DriveFreeSpace03[24]--JPEG_1085440[11][24].jpg : jphide[v5](gator)
DriveFreeSpace03[23]--JPEG_667648[11][23].jpg : jphide[v5](gumbo)
DriveFreeSpace03[29]--JPEG_1765376[11][29].jpg : negative
DriveFreeSpace07[25]--JPEG_13996032[15][25].jpg : negative
DriveFreeSpace03[26]--JPEG_1499136[11][26].jpg : negative
rhino2.jpg : negative
DriveFreeSpace03[27]--JPEG_1773568[11][27].jpg : negative
DriveFreeSpace03[28]--JPEG_569344[11][28].jpg : negative
rhino3.jpg : negative
rhino4.jpg : negative
Processed 10 files, found 2 embeddings.
Time: 254 seconds: Cracks: 7970947,  31381.7 c/s

D:\Fall 2017\ITS45200\comp_Project\stegdetect>
```

5. Run jpseek to recover steganography files and supplies with password receoved in step 4.

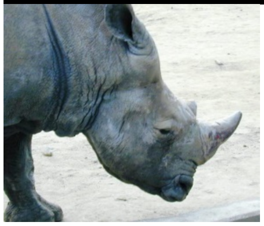


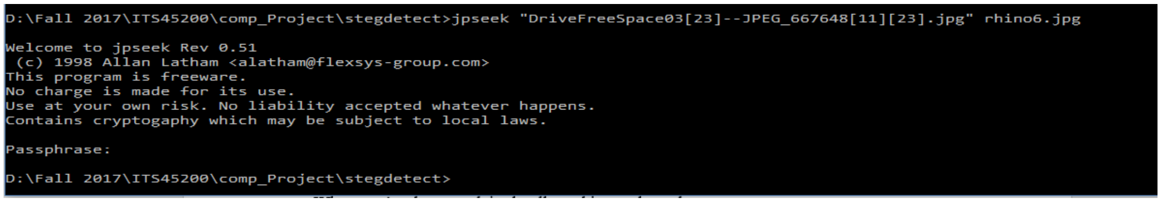
```
D:\Fall 2017\ITS45200\comp_Project\stegdetect>jpseek "DriveFreeSpace03[24]--JPEG_1085440[11][24].jpg" rhino7.jpg

Welcome to jpseek Rev 0.51
 (c) 1998 Allan Latham <alatham@flexsys-group.com>
This program is freeware.
No charge is made for its use.
Use at your own risk. No liability accepted whatever happens.
Contains cryptogaphy which may be subject to local laws.

Passphrase:

D:\Fall 2017\ITS45200\comp_Project\stegdetect>
```





```
D:\Fall 2017\ITS45200\comp_Project\stegdetect>jpseek "DriveFreeSpace03[23]--JPEG_667648[11][23].jpg" rhino6.jpg

Welcome to jpseek Rev 0.51
 (c) 1998 Allan Latham <alatham@flexsys-group.com>
This program is freeware.
No charge is made for its use.
Use at your own risk. No liability accepted whatever happens.
Contains cryptogaphy which may be subject to local laws.

Passphrase:

D:\Fall 2017\ITS45200\comp_Project\stegdetect>
```