CIS 8630

Business Computer Forensics and Incident Response

Lab Protocol 07: Steganography and Its Detection with JP Hide and Seek and StegDetect

Purpose: Ensure every student understands the hiding of data within images, and is able to make simple image steganographic encodings. Students will also develop first-hand knowledge in techniques for detecting and cracking steganography.

Materials required: (all downloadable files) images_cis8630.zip, jphs05_cis8630.zip, stegdetect04_cis8630.zip, usr.zip

Deliverable: This lab protocol with answers. Be sure your name and team name is on the material delivered.

Preparation

- 1. Logon to your VM machine.
- 2. Onto your desktop, download the four zip files above from
 - a. http://cis.gsu.edu/rbaskerville/cis8630/labs/images_cis8630.zip
 - b. http://cis.gsu.edu/rbaskerville/cis8630/labs/jphs05_cis8630.zip
 - c. http://cis.gsu.edu/rbaskerville/cis8630/labs/stegdetect04_cis8630.zip
 - d. http://cis.gsu.edu/rbaskerville/cis8630/labs/usr.zip
- 3. Make a directory named "stego".

Part One: Hiding data in a JPEG image using JP Hide and Seek

- 1. Unzip the contents of JP Hide and Seek (jphs05_cis8630.zip) into this directory.
- 2. From Windows Explorer, copy the 2009_miss_gsu.jpg file into the stego directory. Double-clicking on the photo to bring it up in the Windows Picture Viewer. This is a clean (no hidden data) photo of the 2009 Miss Georgia State University taken from http://www.gsu.edu/studentevents/miss_gsu.html and should look like the image to right.
- 3. Close the photo viewer.
- 4. From Windows Explorer, right click on the photo and choose "Properties" from the context menu.
 - a. What is the exact size of the file containing this image?



- 5. Examine the PTAC.pdf file that was downloaded with the zip file by double-clicking on the file. This file contains the secret information about the PTA Club members that we plan to hide in the image.
- 6. Run "Jphswin.exe" by double-clicking on the icon. After accepting the license terms, you should see the following screen:

	🧱 JPHS for WIndows - Freeware version BETA test rev 0.5										
Exi	t Open jpeg	Hide	Seek	Save jpeg	Save jpe	g as	Pass phrase	Options	Help	About	
	Input jpeg file										
	Directory Filename										
. Filesize Kb Width pixels Height pixels Approximate max capacity Kb recommended limit Kb											
Hidden file											
Directory Filename											
	Filesize	Кb									
		1.00									
				5	Saved jpe	g file					
	Directory										
	Filename										
	Filesize	Kb									
	No jpeg file h	as beel	n open	ied							

7. Choose "Open jpeg" from the menu and open the JPEG image that was downloaded with the zip file.

Direct	🧱 Select the	input jpeg file		
Filena	Look in: 🚺	stego	• 🛨 🔶	≝
Filesiz	View/			
Appro	10			
÷.	9			10 <u>11</u>
Directi	A			
Filena	2009_mis	s_gsu Lake_Moraine		
Filesiz		P		
	File name:	2009_miss_gsu		Open
		ipeg files (*.jpg *.jpeg)		Cancel

8. JPHS will populate the "input jpeg file" information from the selected file. Notice that it will specify a maximum file size that can be hidden within this image and recommend a limit that will make it less likely that the corruption of the image will be visually detectable. The screen should appear as follows

t	Open jpeg	Hide	Seek	Save jpeg	Save jpeg as	Pass phrase	Options	Help	About	
Input jpeg file										
Directory C\Data\0Svnc\0Proj\Teach\GSU\8630\Lab\Lab07-Stego\Stego										
Filename 2009 miss gsujpg										
riendine coos_mas_gaujpg										
F	Filesize	113 Kb	- V	/idth 320	pixels H	Heiaht 445 i	oixels			
A	Approxima	te max c	apacit:	y 17Kb	o recomm	ended limit	11 Kb			
Lidden file										
	Hidden file									

- 9. Check to see that your data matches the expected values:
 - a. What is the recommended limit to the data file size that can be hidden in this image?
 - b. What is the maximum size for a data file that can be hidden in this image?

10. From Windows Explorer, right click on the secret file, PTAC.pdf, and choose "Properties".a. What is the exact file size of our secret file, PTAC?

- b. Will this image be suitable, in terms of size, for hiding this data?
- 11. Choose "hide" from the menu. You are prompted for a passphrase. This is the passphrase that will be needed to extract the hidden data. Lets choose the word "sentence" as our passphrase. Enter and confirm the passphrase is "sentence". Click "OK".

Input jpeg file Directory C:\Data\0Sync\0Proj\Teach\GSU\8630\Lab\Lab07-Stego\Stego	1
Filename 2009_miss_gsu.jpg	
Filendine 2005_miss_gsu.jpg	
Enter the pass phrase and confirmation	
хихихих	
OK Cancel	
Directory	
Filename	
Filesize	~

3 of 10

12. You will be prompted to select the file containing the information to hide. Choose the file PTAC.pdf that we examined earlier:

it Oper bout	n jpeg Hide Seek Save jpeg Save jpeg as Pass phrase Opt	ions Help
Filena	Look in: 🚺 stego 🔹 🖛 🖭 🕇	
Filesiz Appro Directe Filena Filesiz	PTAC Readme	
Direct Filenan Filesize	Files of type: all files (".")	

- 13. JPHS will report the details of the file to be hidden. Notice that the values reported in JPHS are approximate.
 - a. What is the JPHS reported size of the hidden file PTAC.pdf
 - b. According to JPHS, will this image be suitable, in terms of size, for hiding this data?
- 14. Click on "Save jpeg as". Save the file under the filename "my_2009_miss_gsu.jpg" See below:



15. The JPHS screen will display the details of the three files approximately as below:

	👹 JPHS for WIndows - Freeware version BETA test rev 0.5 📃 🗔 🔀									
Exi	t Open jpeg	Hide	Seek	Save jpeg	Save jpeg as	Pass phrase	Options	Help	About	
	Input jpeg file									
	Directory C:\Data\0Sync\0Proj\Teach\GSU\8630\Lab\Lab07-Stego\Stego									
	Filename 2009_miss_gsu.jpg									
	Filesize 113 Kb Width 320 pixels Height 445 pixels									
	Approxima	te max c	apacity	/ 17 Kł	o recomm	nended limit	11 Kb			
	Hidden file									
	Directory C.\Data\0Sync\0Proj\Teach\GSU\8630\Lab\Lab07-Stego\Stego									
	Filename	PTAC.p	odf							
	Filesize	10 Kb								
					Saved jpeg fil	0				
							-			
	Directory Filename				ach\GSU\863	U\Lab\LabU/-	-Stego\Ste	ego		
			10_mis:	s_ysu.jpy						
	Filesize	92 K.b								
[
	This jpeg file	e has be	en mo	dified and	saved					

- 16. Note the difference in the input and saved JPEG files. From Windows Explorer, right click on the newly created image file and choose "Properties" from the context menu.
 - a. What is the exact size of the file containing this image?
 - b. Is the saved image file larger or smaller than the input image file?
 - c. Does the size of the hidden file determine the size difference between the input and saved image files?

- d. Why?
- 17. From Windows Explorer, double click on one of the two images to view it is the Windows Picture Viewer. Switch between the two images using the blue arrow keys and study the visual differences between the two images:



- a. What differences in these two images are detectable visually?
- 18. Close the viewer. Choose "Exit" from the JPHS menu to close JPHS.

Part Two: Recovering hidden data in a JPEG image using JP Hide and Seek

- 1. As before, run "Jphswin.exe" by double-clicking on the icon and accepting the license terms.
- 2. Choose "Open jpeg" from the menu. Select the file "my_2009_miss_gsu.jpg" (this file contains the hidden data).
- 3. Choose "Seek" from the menu. A passphrase dialog box will open. Enter our passphrase "sentence" into the dialog box passphrase and confirmation text boxes. Click "OK".
- 4. A dialog box will open to allow you to choose a file name and location in which to deposit the recovered information. Enter the file name "my_PTAC.pdf":

Save in: 🔁) Stego	- 🖬 🏪 📼
2009_mis: 2 images_ci 3 jphide.exi 3 jphs 2 jphs 3 jphs05_ci: 3 Jphswin.e	s8630.zip e s8630.zip	☐ jpseek.exe my_2009_miss_gsu.jpg ☐ PTAC.pdf ☐ Readme.txt ☐ stegdetect04_cis8630.zip
File name:	my_PTAC.	pdf Save

- 5. Open my_PTAC.pdf and check that the data contents are the same as the original file. Check the file sizes of the original hidden data file (PTAC.pdf) and the recovered data file (my_PTAC.pdf).
 - a. What is the exact file size of PTAC.pdf?
 - b. What is the exact file size of my_PTAC.pdf?
 - c. Has the steganography changed the hidden data?

Part Three: Detecting hidden data in a JPEG image using StegDetect

- 1. Unzip the rest of the files in images_cis8630.zip into the stego directory. This file contains a number of JPEG images and one text file.
- 2. Unzip stegdetect04_cis8630.zip into the stego directory. StegDetect is a steganography detection and cracking tool that is mainly aimed at unix-based computers, however these files contain a version that runs on windows computers.
- 3. Run the x-windows version of StegDetect by double clicking on xsteg.exe:

👯 xsteg	
File Options	Help
Scan options r jsteg Sensitivity: 1.00 r jphide r outguess r invisible	Stop
Filename	Detection
Message window:	

4. Choose "File" and "Open" from the menu. The "Select File" dialog box will open:

Select File	
Create Dir Delete File	Rename File
C:\Data\0Sync\0Proj\Teach\G	SU\8630\Lab\Lab07-Stego\Stego 🗖
Directories .\ .\ C:\ D:\ E:\ F:\ F:\	Files 2009_miss_gsu.jpg cygwin1.dll gdk-1.3.dll gmodule-1.3.dll gmu-intl.dll gtk-1.3.dll ytk-1.3.dll the files ytk-1.3.dll gnu-intl.
I Selection: C:\Data\OSync\OProj\ [IZ IA Zeach\GSU\8630\Lab\Lab07-Stego\Stego

5. Click "OK" to instruct StegDetect to search all files. The program will display its analysis results for all files. Non-image files in the directory will likely result in error messages:

₫⊼ xsteg	
File Options	Help
Scan options	Stop
Filename	Detection
C:\Data\DSync\DProj\Teach\GSU\8630\Lab\Lab07-Stego\Stego\2009 miss C:\Data\DSync\DProj\Teach\GSU\8630\Lab\Lab07-Stego\Stego\Vmy_2009_r C:\Data\DSync\DProj\Teach\GSU\8630\Lab\Lab07-Stego\Stego\Vrs_gsu.jpg	

a. List below any files that StegDetect suspects of containing hidden data with JP Hide and Seek:

6. Choose "File" and "Exit" from StegDetect.

Part four: Cracking stenographic passwords

- 1. Extract the contents of the usr.zip file directly to your C:\ drive. The .zip file contains a folder named "Usr." Do not modify or change this folder. It contains the required file structure needed for StegBreak for function.
- 2. From StegDetect, three files were shown to have hidden messages: 1) my_2009_miss_gsu.jpg; 2) zebras2.jpg; and lastly, 3) Lake_Moraine.jpg. "Stegbreak.exe," the program we'll use to crack the passwords is a DOS-based program. It will be easier to run if the files with contained messages are in the same folder
- 3. Go to a DOS window by using "CMD" in RUN under the Start menu. Navigate to the stego directory. in which you placed the zip file contents. An example of changing to the dayspace/stego directory is shown below:



3. The command syntax for the stegbreak.exe application can be found in "Stegbreak.pdf" file.

4. Make sure the dictionary used (MedDic.dic) and the rules.ini file are in the same directory as stegbreak.exe. The syntax to run a dictionary attack is:

stegbreak -r rules.ini -f meddic.dic my_2009_miss_gsu.jpg

a) the name following the –r parameter is the "rules.ini" file. It comes with the program but must be in the same directory as stegbreak.

b) the name following the -f parameter is for the name of the dictionary to use. In this case, the dictionary's name is: "MedDict.Dic"...which is found in this same DOS directory as the other files. c) stegbreak defaults to break jphide ... an additional parameter, -t, can be used to crack outguess or jsteg-shell codes. See the stegbreak.pdf file.

d) NB: Avoid cut-and-paste for these commands (some characters may not be recognized by the Unix-based command). Also ensure the command window has administrator privileges (noted in the title bar).

5. The figure below shows the results of breaking the file my_2009_miss_gsu.jpg file. See the password "sentence" delivered in the report.



- 6. What is the password for the hidden message in the file zebras2.jpg?
- 7. What is the content of the hidden message in the files zebras2.jpg

open it?

MRD - [C:\dayspace\stego\Cracked_Zebras] - 🗆 × _ 8 × 😰 File Edit Search View Analysis Extras Window ? 📄 👌 • 🕞 🧔 🥥 💐 📑 16 ANSI hex • 📓 boohoo2 📓 boohoo1 📓 Cracked_Zebras • Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E OF 00000000 \$5 50 44 46 2D 31 2E 34 OD 25 E2 E3 CF D3 OD OA SPDF-1.4. aäïó. 36 20 30 20 6F 62 6A 3C 3C 2F 48 5B 36 33 36 20 31 35 34 5D 2F 4C 69 6E 65 61 72 69 7A 65 64 20 00000010 όΟ οbj<</Η[636] 00000020 154]/Linearized 1/E 8997/L 12952 00000030 31 2F 45 20 38 39 39 37 2F 4C 20 31 32 39 35 32 00000040 2F 4E 20 31 2F 4F 20 39 2F 54 20 31 32 37 38 36 /N 1/O 9/T 12786 3E 3E OD 65 6E 64 6F 62 6A OD 20 20 20 20 20 20 00000050 >>.endobj. 00000060 00000070 .xref..6 17. 00000080 30 30 30 30 30 30 30 30 31 36 20 30 30 30 30 30 0000000016 00000 20 6E OD OA 30 30 30 30 30 30 30 37 39 30 20 30 00000090 n..000000790 0 00000040 30 30 30 30 20 6E OD OA 30 30 30 30 30 30 30 36 0000 n..00000006 00000080 33 36 20 30 30 30 30 30 20 6E OD OA 30 30 30 30 36 00000 n..0000 00000000 30 30 30 38 36 36 20 30 30 30 30 30 20 6E OD OA 000866 00000 n.. 30 30 30 30 30 30 30 30 39 39 33 20 30 30 30 30 30 20 6E 0D 0A 30 30 30 30 30 30 30 30 31 31 33 36 20 30 00000000 0000000993 00000 000000E0 n..0000001136 0 000000F0 30 30 30 30 20 6E OD OA 30 30 30 30 30 30 31 35 0000 n..00000015 Offset: 0 Overwrite

Hint: What type of file is shown below? What extension should you rename the file so that Windows will