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

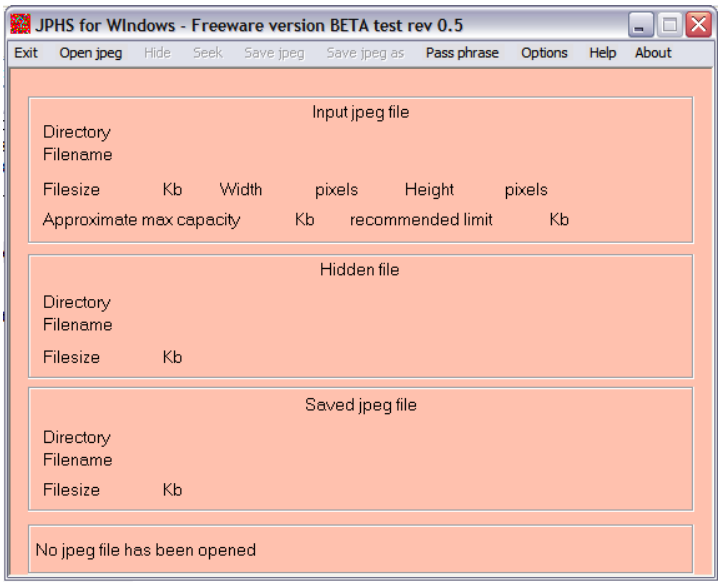
3. Make a directory named "stego".

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

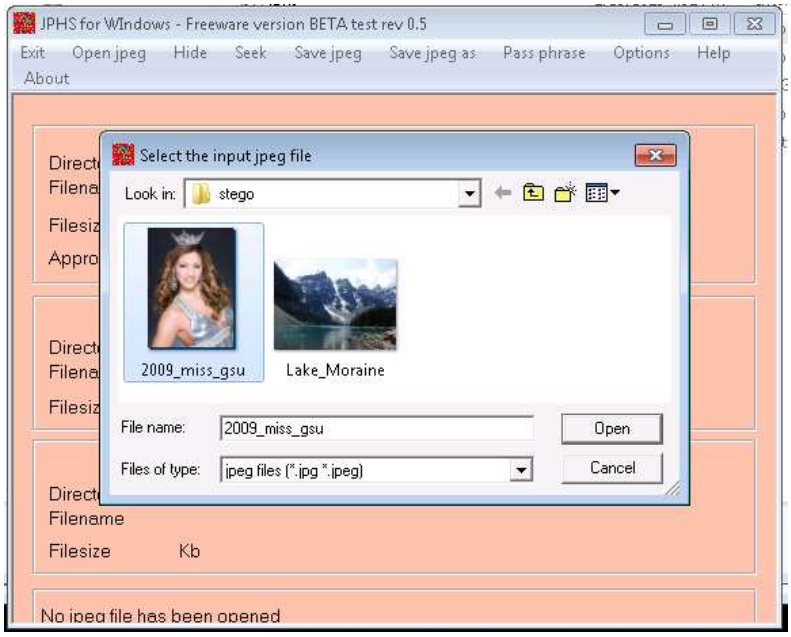
1. Unzip the contents of JP Hide and Seek (jphs05_cis8630.zip) into this directory.
2. From Windows Explorer, copy the 2009_miss_gsu.jpg file into the stego directory. Double-clicking on the photo to bring it up in the Windows Picture Viewer. This is a clean (no hidden data) photo of the 2009 Miss Georgia 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?

_____

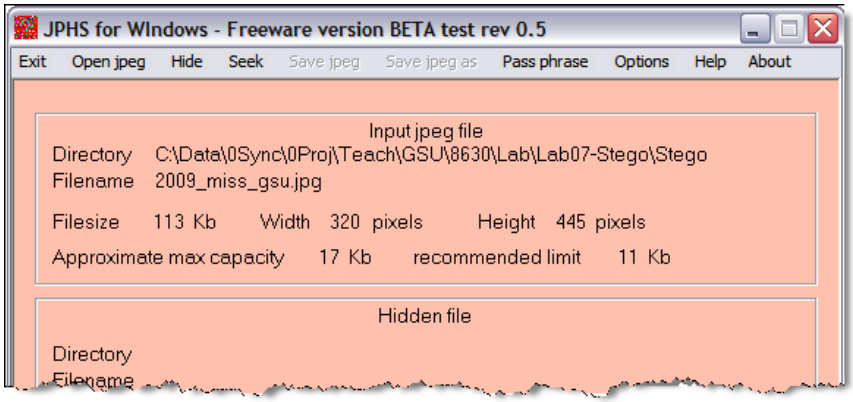
5. Examine the PTAC.pdf file that was downloaded with the zip file by double-clicking on the file. This file contains the secret information about the PTA Club members that we plan to hide in the image.
6. Run "Jphswin.exe" by double-clicking on the icon. After accepting the license terms, you should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




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




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




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?

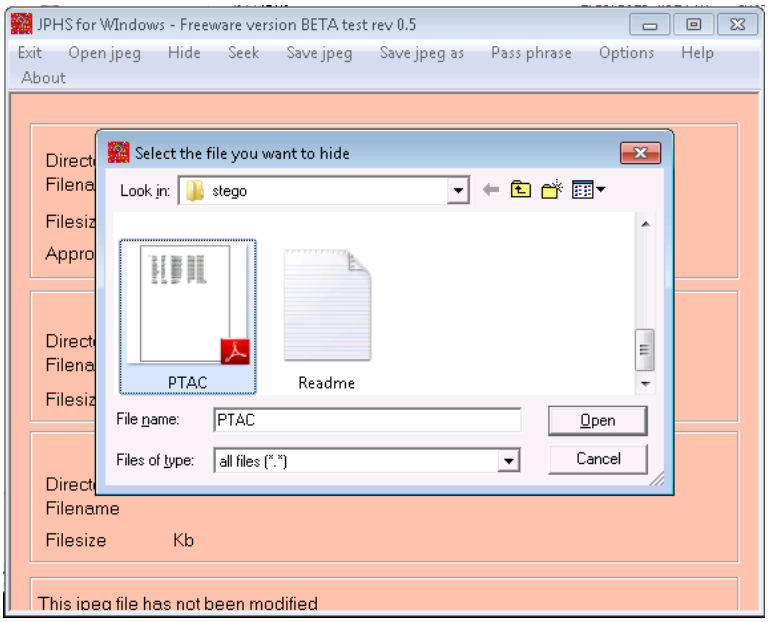
       _____

    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".

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



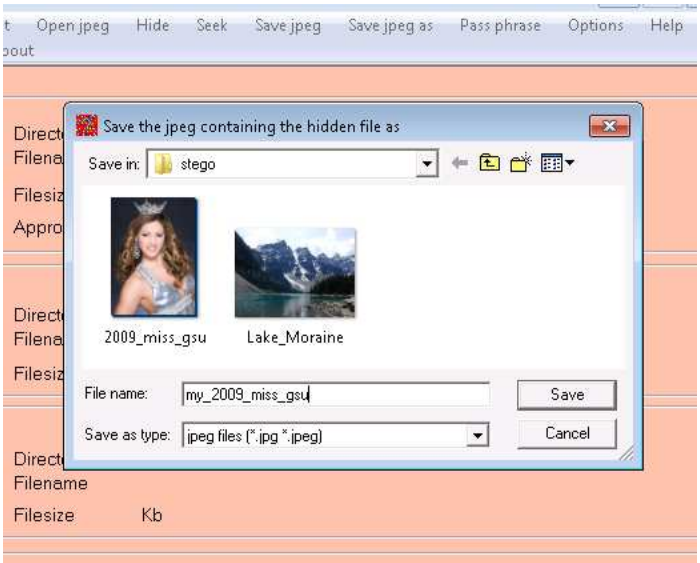

13. JPHS will report the details of the file to be hidden. Notice that the values reported in JPHS are approximate.
    a. What is the JPHS reported size of the hidden file PTAC.pdf

    _____

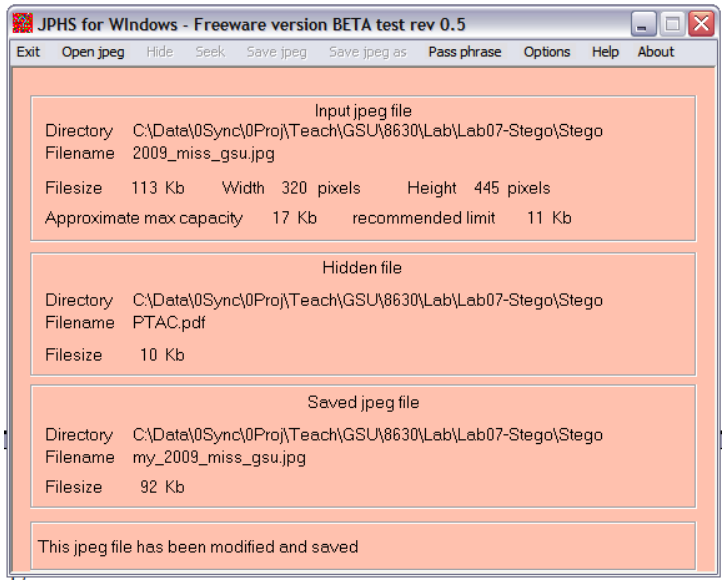
    b. According to JPHS, will this image be suitable, in terms of size, for hiding this data?

    _____

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:




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? _____

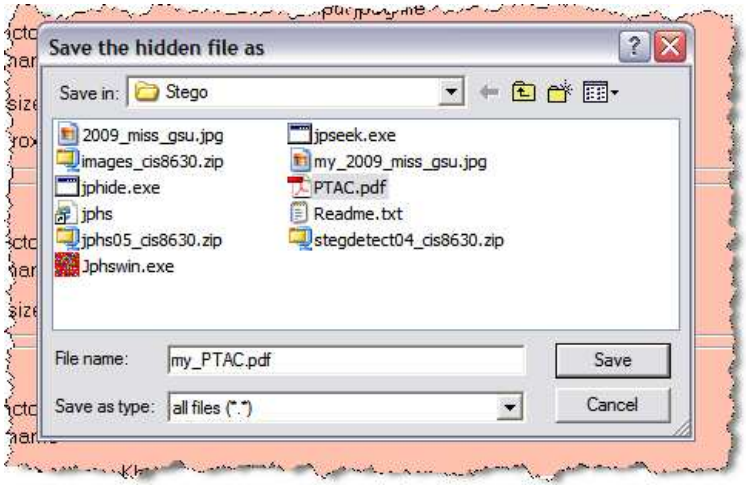
17. From Windows Explorer, double click on one of the two images to view it is the Windows Picture Viewer. Switch between the two images using the blue arrow keys and study the visual differences between the two images:


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":




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?

    _____

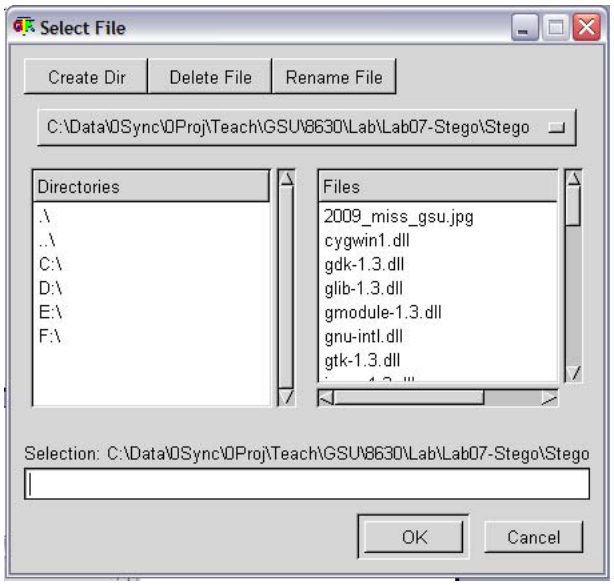
    c. Has the steganography changed the hidden data?

    _____

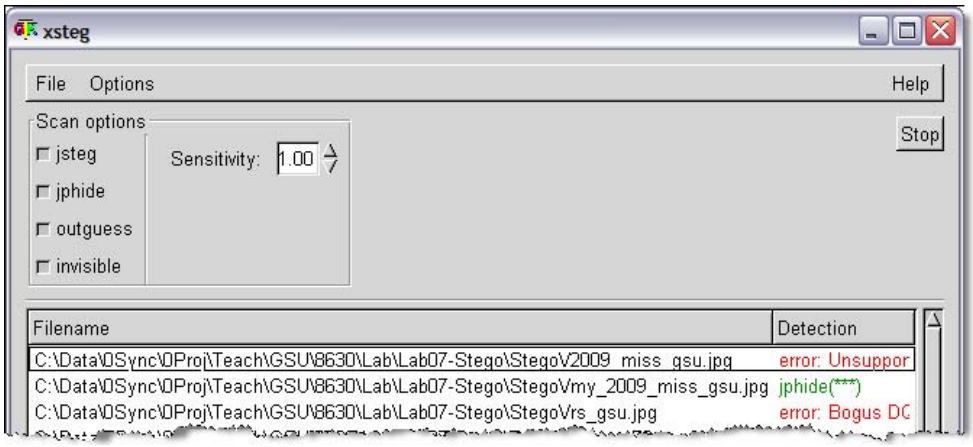
**Part Three: Detecting hidden data in a JPEG image using StegDetect**

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:


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




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:




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

_____

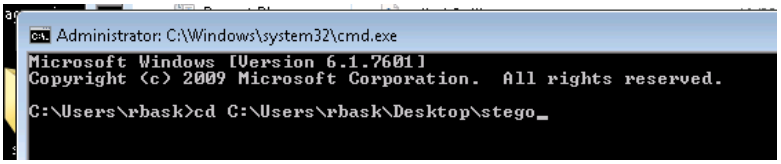
_____

_____

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:



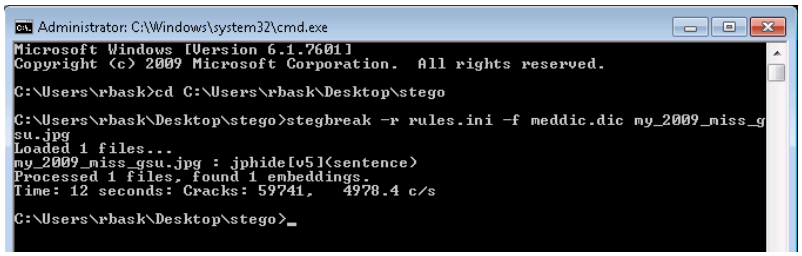

3. The command syntax for the stegbreak.exe application can be found in "Stegbreak.pdf" file.

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

_____

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