Part A: S-Tools

S-tools is a steganography tool used to hide messages inside of BMP, GIF and WAV files on Windows systems. The file in which the data is hidden is called the *carrier file.* Depending on the options that you choose, the output file that contains the hidden data may have different properties than the original file.

Use the provided Lab Assignment 5 .ppt file to submit captures / Snips for submission. Please insert a text box on the relevant slide for your answers to embedded questions (??) as you move through the Lab Assignment.

Open the Win7 VMware image. In the c:\security folder, find the **stego** folder. This folder contains several steganography programs like s-tools4, setgdectec-04.zip, and Invisible Secrets. Start S-Tools by double-clicking the **s-tools.exe** executable (located in the **s-tools4** folder).

1. Select **File → Properties** to view the compression ratio for the file that is being hidden. The higher the compression the longer it will take to hide the file, however larger files can be hidden with higher compression. Select **OK** to accept the default compression
2. On the root of c: drive create a folder named **Ex5 (this is the same as Assignment 5).**
3. From the **c:\security\stego** folder copy the **Lab1.bmp** file to the **Ex5** folder. Drag the **Lab1.bmp** file onto the S-Tools window.
4. Use Notepad to create a document with a short text message. Save this file in the **Ex5** folder with the name ***yourfirstname*.txt**. Now drag this file on top of the **Lab1.bmp** image in the S-Tools window. At the passphrase prompt, enter **info6001** as the passphrase and confirm.
5. S-Tools supports a number of encryption algorithms, including IDEA, DES, 3DES, and MDC. Click the down arrow to view the options. Accept the default of IDEA and click **OK.**
6. The newly created .bmp file with the hidden encrypted text now appears in the S-Tools interface with the name **hidden data**. Can you see any difference from the original .bmp file?? *Answer text box on Slide* 1.
7. Right-click on the hidden data window and select **Properties**. Notice the dimensions of the file as well as the memory usage.
8. Now right-click the original .bmp and select **Properties.**

   Is the information the same or different?? *Answer in text box on Slide 1.*
9. Right-click on the hidden data window and select **Save as** and enter ***yourFOLusername*.bmp** as the file name and save to the **c:\Ex5** folder. **Exit** out of S-Tools. (File – Exit)
10. In the **Ex5** folder select the **Lab1.bmp** and ***yourFOLusername*.bmp** files and display the properties of both files. What is the size of both files?? *Answer in text box on Slide 1.*
    Can you tell that a text file has been hidden in the .bmp file?? *Answer in text box on Slide 1.*

    1. ***Take a capture or Snip of the properties of both .bmp files in the Ex5 Submission file.***

11. Restart S-Tools and drag the ***yourFOLusername*.bmp** file onto the S-Tools window.
    Right-click and select **Reveal**. You are now prompted for the passphrase to reveal any hidden data. Enter and confirm the passphrase that you set in step 4 and click **OK**.

    2. ***Take a screen capture for the Ex5 Submission file showing the revealed archive***

Part B - Invisible Secrets

Invisible Secrets has a wider range of carrier file types and more options than S-Tools provides. Files can be hidden within the following file types: JPEG, BMP, HTML and WAV.

Copy the file plane.jpg from the c:\security folder to the c:\Ex5 folder

From the **c:\security\stego\invisible secrets** folder double-clicks **etinvisiblesecrets-install.exe** to start the installation program

Accept the default installation steps. After the installation, Invisible Secrets launches the purchase order window. Click **Continue Trial** to start the program.

1. From the **Invisible Secrets 4** menu select **Hide Files**
2. When the **Select the files you want to hide in the carrier w**indow opens select **New Message** button.
3. Enter **Ex5 Stego** as the subject and click OK – OK *(Do not save the file after encryption*)
4. When Word Pad opens enter your full name and ***your***FOLusername as the text. Select **Save** and close Word Pad
5. Click **Next** to specify the carrier file that will be used to hide your message
6. In the **Select Carrier File** windows use the browser folder button to locate the **plane.jpg** file in the **C:\security** folder and click **Open - Next**
7. In the **Encryption Settings** windows enter **ism18** as the encryption password (this is the encryption key). The trial version only allows short 5 character passwords
8. In the Select the encryption algorithm box, click the down arrow to see the available encryption algorithm**.**

3. Take a screen capture of the encryption options for the Ex5 Submission file.

9. Select **AES** as the algorithm to be used Click **Next**
10. In the **Target File Settings** windows enter **yourfirstname2** as the file name and save in the **c:\Ex5** folder
11. Click **Hide** to encrypt the file **Ex5 Stego.rtf** and hide the file inside the **yourfirstname2.jpg** file
12. Click **Next – Finish** to complete the process.
13. In the **c:\Ex5** folder double click on both the plane.jpg and **yourfirstname2.jpg**.
    Can you tell that a text file has been hidden inside the picture?*?* Check
    the size of both files*??*

Exit Invisible Secrets

Invisible Secrets allows a number of steps performed on the newly created file.

1. To reveal the information in the **yourfirstname2.jpg** file, start Invisible Secrets. Click the **Continue Trial** button
2. Select **Unhide Files**
3. Navigate and select the **yourfirstname2.jpg** file and click **Next**
4. Enter the passphrase selected and click **Next**
5. The Unhide/Decrypt Data window lists the original text file, Ex5 Stego.rtf In the Select the destination folder navigate to c:\Ex5 folder Click **Unhide - Finish** to extract the file.
6. After the process is finished **Exit Invisible Secrets**.
7. In the c:\Ex5 folder double clicks on Ex5 Stego.rtf to view the text file content

4. Take a screen capture of the file content for the Ex5 Submission file

Close word Pad

Part C – Xsteg/Stegdetect

Xsteg/Stegdetect is a tool used to determine if there is information hidden in a particular file through the use of stegonagraphic techniques. Xsteg is the graphical interface to StegDetect.

To run the program, open a command prompt.
Change to the **C:\security\stego\stegdetect-0.4\stegdetect** directory, at the prompt type **xsteg** to start the program. By default, the program will detect hidden files created by 4 programs listed under Scan Options

1. Select **File → Open**
   In the left panel double click on **C:\** and next double click on **Security**
   In the right panel select a jpg file that was not used in this lab (Frigate or I am Canadian)
   Scan the file
   A negative result shows no hidden message is present

2. Change to the Ex5 folder and select the **yourfirstname2.jpg** file
   Scan the file
   Xsteg will detect if a message has been hidden inside the .jpeg file and what program was used to hide the message

   The message window details the options that were used during the test.

5. Take a screen capture of the scan output for the Ex5 Submission file

Advanced Encryption Standard AES

Open a command prompt and move to the **c:\security\AES** folder

Open Notepad.exe
Enter your name, student number and FOL username as text in this file
Save as ***yourFOLname.txt*** in the **c:\security\AES** folder

Encrypt the text file

The aescrypt.exe program must be run from the command line

The encryption key will be info6001

To encrypt a file c:\security\AES> **aescrypt.exe -e -p info6001 *FOLname*.txt**

The encrypted file has **.aes** extension

Delete the ***yourFOLname.txt***

To decrypt the file c:\security\AES> **aescrypt -d -p info6001 *FOLname*.txt.aes**

View the c:\security\aes folder and see that the ***yourFOLname.txt*** has been recreated

6. Place the encrypted file with your FOLname as an embedded object for the Ex5 Submission file

Please deposit your single .pptx answer file. File name format = <your_FOLID>_A5_23W.pptx

e.g. "b_patel12345_A5_23W.pptx"