Computer Forensics 2

Lab 2 - More on Hiding Information – by Dr Diane Gan

Don't forget to change the folder options so that you can "see" file extensions and system files.
Create a folder on the C drive to save your work C:\ Users\Student*yourname*

1. Merging Files

This exercise combines two files with different file extensions – e.g. .**doc and .xls**

a. Create a Word document, enter some text and save it as the **old version – (97-2003)**

b. Create a Spreadsheet, enter some text and save it as the **old version – (97-2003)**
Close both files

Q1. Record the file sizes for each of your files word doc……

excel spreadsheet……..

c: Using HashMyFiles, generate a MD5 Hash of each of the two files that you are going to combine, by dragging each of them separately into the tool.

MD5 is an algorithm for computing a condensed representation of a message or a data file. The condensed representation is of fixed length and is known as a 'message digest' or 'fingerprint'. The hashing process is a one way function. It is not possible to 'reverse engineer' the original from the MD5 hash.

Or try using the MD5 Hash tool

Q2. What are the two hash values? Copy them out to a notepad (name it hash.txt)

d. Run **Glue** - use the Start menu

e. Browse to your two files using the correct text boxes on Glue and click the **Merge** button.

f. Repeat the Hash step in **c.** on the files again

g. Answer the following questions:-

Q3. Looking at the file size information, which file is "hosting" both files information?

Q4. Using the hashes, can you verify which file has changed and which has not? Y / N

Q5. Which file has changed? ……

h. Try changing the file extension on the file that had changed by renaming the document

Q6. What did you see? ……

2. Steganography - Do not overwrite the original files **in Diane's Uitils**

Make a folder called C:\ Users\Student*yourname***Before**
And another called C:\ Users\Student*yourname***After**
Copy the file from Dianes Utils Exercises\Ex5.2\Couple.bmp and any large jpg from the folder C:\Photos to C:\Users\Student *yourname*\Before

Using OpenPuff

Start by identifying how much free space you have on the C drive – hint use DIR in the command prompt box. (Better to use a USB stick for this)

Q9. How much Free space is there on the C drive? …….……..……...

Create a text file called Secret.txt and save this is in the **Before** folder.

Run **OpenPuff** from the Start menu

Disable the B and C passwords by unchecking the boxes (this speeds up the exercise).
Click on the **Hide** button to open the tool and enter a password (min 8 chars) – use your name.
Note the box goes green when the password is long enough.

Use the large jpg (you could also use an audio, video or even a flash file), which will be the host file, also called the "**carrier**".

Create a secret message using Notepad and save it in the **Before** folder
Click on the **Browse** button in OpenPuff (top right) and browse to your text file.
Click the Add button on the left and select the large jpg file that you copied.

[The Hide! Button should be green at this point – if it is not then you have not picked a big enough carrier file. You can add more than one jpg]

Click Hide! And save your file in the "After" folder or you will get an error message.
Close the window.

Q10. How much Free space is left now? …….……..……...

Compare the two pictures (jpgs) in the Before and After folders

Q11. Can you tell which is the "carrier"? …….……..……..

Go to Unhide and save your extracted secret message in the **After** folder.

Q12. How easily were these files hidden and retrieved? Should we be concerned?

3. **Analyse a Disk using a Hex Editor**

- A hex editor allows you to view disks and files and change/write sectors.
- Start the Hex Editor called **Hexplore** – ICY Hexplorer – go to View Options and change the font to large and select background white to make it easier to read.
- Select **Disk** and **Open Drive** and select your USB or the C drive. You will be asked for a range – 0 to 200,000 should be sufficient.
- You should see the contents of the drive in Hex, with the text version to the right.
- Select **Edit** from the menu bar and in the context menu, select **Find**.
  From Find and the **Text** box type **jpg**
  When asked if you want to search the entire drive select Yes

Q13. Did you find the word "jpg"? …….……..……..

- Try changing the search to FF E0 FF

Q14. What have you just searched for? …….……..……..

Q15. How does this differ from the previous search? …….……..……..

Investigate the other Hex Editors that are available.

4. Evaluating Slack Space

- Scroll down to a sector where there is nothing stored. This is an area where there is all zeros and it is called – **Slack Space**.

- Type in a message about the weather – make sure that you include the word "**weather**".

Q15. Look at the drive using Windows Explorer – can you see anything? ……..……...

- In **Hexplore** go to the start of the drive. In the menu bar, select **Edit | Find**

- View the default settings, notice that searches can be either ASCII or Unicode strings

- In **Value** type **weather** then click **Sector Range** tab – select **Search Entire Disk** – click **OK**

Q16. Did you find the word hidden in slack space? ……..……..……..……....