Computer Forensic & Investigation

Lab5: Hiding Data

	COURSE: Computer Forensics & Investigation			**MARKS**:
	TOPIC:		**CODE:** BCN3193	
	ASSESSMENT: HOT 1	**NO:** 1	**DURATION:**	

OBJECTIVES:

- Introduction to tools for hiding data using steganography and to tools used for detecting steganography.

INTRODUCTION

- You will practice creating a hidden message using steganography and then attempt to crack someone else's hidden message.

ACTIVITIES:

1. The tools needed for this practical are JPHide and JPSeek and the combined version, JPHS for Windows, the StegDetect suite, some graphical images and numerous dictionaries.

2. JPHide and JPSeek work only on JPEG graphics. You can determine how much data you can hide in an image if you use the Jphswin tool. Try using it on some of the JPEG files in the Graphical Images directory.

3. Using JPHide (from command line), Jphswin, hide some data in any of the JPEG files supplied or in one of your own.

4. To make this practical exercise effective, you should ensure that the password exists in the Combined dictionary provided. (For your information, more dictionary lists are available from http://www.cotse.com/tools/wordlists.htm). Save the new JPEG file in the share directory so someone else in the class can attempt to crack the password and extract the message of this practical.

5. Use StegDetect to determine which JPEG files in the share directory contain steganographic messages. Stegdetect.pdf is a manual for the application. Initially attempt to detect steganography using the default options. You may need to alter the sensitivity option to detect if images contain hidden data.

Questions:

Question 1 Record the initial size of the file, and the size of the steganographically altered file. What does it mean if the file size has altered?

Question 2 View your original file and your altered file. Can you notice any changes in the altered file?

End of Lab5