**Matthew Austin**

**Digital Forensics**

**Dr. Tian**

**November 2017**

**Lab 4**

**CIS425** – Fall 2017

**Point Value**: 100 points

**Due Date**: **In class Thursday December 05, 2017**

**Submission Instruction**

Please submit one pdf file, lab4\_notes.pdf, to the instructor in lecture. This lab4\_note includes a detailed notes and the answers to the following questions.

**What you will need: a hosting computer with Linux/Ubuntu OS.**

**Software you may need: Steghide, Steghide-Brute-Force-Tool, base64 decoder, Caesar cipher decoder, python, python-progressbar library.**

**Please download all the following tar file:**

**cis425@mathcswc.fontbonne.edu:~/Lab4.tar**

1. There are five .JPG files and one wordlist.txt file in the TAR file. Each JPEG file contains a secret text message. Please find each secrete message:

The Message in mystery-flag-1.jpg:

* The flag was found using steghide extract -sf mystery-flag-1.jpg -xf flag1.txt. No passphrase was needed.
* The flag is {Denmark}

The Message in mystery-flag-2.jpg:

* The flag was founding using Steghide Brute Force using the wordlist.txt. Information was obtained using password *Thailand2017*.
* The flag is {Thailand}

The Message in mystery-flag-3.jpg:

* The flag was found using [Hex] xxd mystery-flag-3.jpg
* The flag is {Sudan}

The Message in mystery-flag-4.jpg:

* Using xxd mystery-flag-5.jpg and finding the end of the jpg file fd99. Copying the text afterwards and using a brute force Caesar Cipher to decrypt the text (Caesar 7).

- The flag is {Zimbabwe}

The Message in mystery-flag-5.jpg:

* The flag is {Peru}

**Note:** You MUST work on this lab individually. Also, please include a detailed notes.