**Assignment 4**

**CIS410/594-01** – Spring Term 2017

**Point Value**: 100 points

**Assignment Due Date**: **03/30/2017**

**Submission Instruction**

Please submit a hardcopy of your assignment solution to your instructor in class on the due date and also submit it (word or pdf document) on BB by 11:59pm on the due date.

**Description**

1. There are two main different types of mobile evidence collection: logical collection and physical collection. Please explain what is logical collection***? (5 points)*** What is physical collection? ***(5 points)*** What is the major difference? ***(5 points)***
2. What is File System Collection***? (5 points)***

1. What is Non-invasive physical collection? Please list at least one example. (**5 points**)
2. What is invasive physical collection? Please list a least two examples of physical collection? (**5 points**)
3. There are logical collection, non-invasive physical collection, and invasive physical collection. Please indicate the order of the three types of collections an examiner should use in each scenario:
   1. If the seized mobile device is powered on and unlock (**3 points**)
   2. If the seized mobile device is powered on and lock (**3 points**)
   3. If the seized mobile device is powered off and requires a password to unlock the phone. **(4 points**)
4. Please use santoku virtual machine and the iPhoneBackupAnalyzer2 tool to analyze the iPhone Backup file that you are supposed to download from [tim@mathcswc.fontbonne.edu:~/iPhoneBackup2](mailto:tim@mathcswc.fontbonne.edu:~/iPhoneBackup2). Please answer the following questions:
   1. What is the device name of the iPhone? (**2 point**)
   2. What is the last backup date? (**2 point**)
   3. What is the IMEI of the iPhone? (**2 point**)
   4. What is the model of the iPhone? (**2 point**)
   5. What is the Apple ID of the iPhone user? (**4 points**)
   6. Does this iPhone install the app named Zillow? (**4 points**)
   7. In the address book, there is one person affiliated with Master Card. What is the person’s name and his phone number? (**4 points**)
   8. Please find out the names/SSID of all the WiFi access points/routers/networks this iPhone has been connected to? (**10 points**)
   9. Please find an image file that displays the text “COMPUTER SCIENCE”, what is the location and the date when this image is taken? (**5 points**)
   10. As an FBI agent, you know that the suspect is a fan of hiding information in image files. Please find the flag(s) embedded in one or more image file(s) stored in the “/CameraRollDomain/Media/DCIM/100AP..” folder? (**15 points**)
5. Please read the article “Exploring Steganography: Seeing the unseen” and answer the following questions:
   1. What is the definition of *Steganography*? **(2 points**)
   2. Based on the article, what is the resulting 3 pixels of embedding the letter ‘I’ into a 24-bit image (every pixel is 3 bytes) file with *Least Significant Bit* *Insertion* method. The 3 pixel you are going to use is (**8 points)**:

Pixel 1: (00100111 11101001 11001000)

Pixel 2: (00100111 11001000 11101001)

Pixel 3: (11001000 00100111 11101001)

Resulting pixel 1: ( )

Resulting pixel 2: ( )

Resulting pixel 3: ( )