Matthew Austin

Mobile Forensics

**Assignment 4**

**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)***

***Logical Collection:*** Is the extraction of user data from a mobile device without the collection of a device’s file system. The data is extracted from the mobile device using proprietary protocols and queries, and displayed in the software’s user interface. This is done by using a software tool on an Android device with an Android APK file, but this methods does not return a file system.

***Physical Collection:*** is a bit-by-bit copy of the entire physical store that also includes “deleted” data. This data is a snapshot of the area of the flash memory store that is accessible using specialized tools and methods.

1. What is File System Collection***? (5 points)***

***File System Collection:*** is a step up from Logical Collection because it contains more information which includes the files and folders that the device uses to populate applications, system configurations, and user configurations along with user storage areas.

1. What is Non-invasive physical collection? Please list at least one example. (**5 points**)
   1. ***Invasive Physical Collection:*** this process provides physical acquisition of a phone’s data and requires disassembly of the phone for access to the circuit board.
2. What is invasive physical collection? Please list at least two examples of physical collection? (**5 points**)
   1. ***Non-Invasive Physical Collection:***  a process that provides physical acquisition of a phone’s data without requiring opening the case of the phone, thus the software must communicate with the device to allow for a binary data “dump” of the device.
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:

If the seized mobile device is powered on and unlock (**3 points**)

*Logical Collection*

If the seized mobile device is powered on and lock (**3 points**)

*Non-Invasive Physical Collection*

If the seized mobile device is powered off and requires a password to unlock the phone. **(4 points**)

*Invasive Physical Collection*

1. 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](about:blank). Please answer the following questions:

What is the device name of the iPhone? (**2 point**): Admin’s Phone

What is the last backup date? (**2 point**): 2017-03-02

What is the IMEI of the iPhone? (**2 point**): 013195005428167

What is the model of the iPhone? (**2 point**): iPhone 4S

What is the Apple ID of the iPhone user? (**4 points**): gtian@ramapo.edu

Does this iPhone install the app named Zillow? (**4 points**): Yes

In the address book, there is one person affiliated with Master Card. What is the person’s name and his phone number? (**4 points**):

Jackson Steward (314) 580-6958

Please find out the names/SSID of all the WiFi access points/routers/networks this iPhone has been connected to? (**10 points**):

2014ThanksgivingTurkey, FBUwireless, 2014ThanksgivingTurkey-guest, BW Sherwood Inn & Suites, RH-Wifi, fbutemp, attwifi, FiOS-LSX7D, happyGT2014, Clayton-Recreation-Guest

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**):

The image name is IMG\_0025.JPG.

*Date:* 2017-02-28.

*Location:* Latitude: 38.62833055555 Longitude: -90.35631666666 (1505 Swallow Dr. Brentwood, MO)

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**) In IMG\_0028.JPG “The flag {Message is hidden in the tail}.

1. Please read the article “Exploring Steganography: Seeing the unseen” and answer the following questions:

What is the definition of *Steganography*? **(2 points**)

Steganography is the art of hiding information in ways that prevent the detection of hidden messages. It includes a vast array of secret communications methods that conceal the message’s very existence.

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: (00100111 11101000 11001000)

Resulting pixel 2: (00100110 11001000 11101000)

Resulting pixel 3: (11001000 00100111 11101001)