**Assignment 3**

**CIS410/594-01** – Spring Term 2017

**Point Value**: 100 points

**Assignment Due Date**: **03/02/2017**

**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. What is Universal Integrated Circuit Card (***5 points***)? What does a UICC comprise? Hint: it comprises a CPU and other hardware. ***(5 points)***
2. What is ICCID (**5 points**)? A mobile forensics examiner use a SIM card reader and found the following ICCID, please write down the ICCID in decimal format so that a layman can understand it? ***(5 points)***

***98 68 32 03 00 12 00 00 10 12***

***ICCID:***

1. Today’s UICC/SIM card contains little information because of its limited size compare to the amount of data a typical smart phone uses. However, why is it still important for a mobile forensics examiner to analyze an UICC/SIM card? ***(5 points***)?

1. The Ki (Ciphering Key) is the individual subscriber authentication key. It is a 128-bit number that is paired with an IMSI when the SIM card is created. The Ki is stored on both the SIM card and at the Authentication Center (AuC). Can a forensic examiner find the value of Ki by using forensics software? (**5 points**)
2. What is IMSI (**5 points**)? Why is this IMSI important to mobile forensics (**5 points**)?
3. A mobile forensics examiner found a SIM card and used a SIM card reader to find the IMSI value, please answer the following questions based on the IMSI value: 460011361608170
   1. Country name (**4 points**):
   2. Network Carrier name (**4 points**):
   3. MISID – Mobile Station ID (**2 points**):
4. In Binary Coded Decimal, each number is represented by a 4-bit binary code. Please write down the decimal number of the first two BCD numbers (a and b) and the BCD numbers of the 2 decimal numbers (c and d) : ***(*10 points*)***
   1. ***0001 0011 1001 0010:***
   2. ***1010 1000 0010 1001:***
   3. ***1345:***
   4. ***5963:***

1. Please explain what is PIN1, PIN2, and PUK in SIM card (**10 points**)
2. Please download the file *Phonebook.phn* from Blackboard and read the content of the file using SIMple. Please find the following information from the *Phonebook.phn* file and describe the steps you take to find those value:
   1. The phone user’s own dialing # (**1 point**):
   2. The voice mail # (**1 point**):
   3. Check Balance # (**1 point**):
   4. Check Text usage # (**1 point**):
   5. Forbidden PLMNs (**1 point**):
3. What is the benefits of using multiple forensics tools in a mobile forensics investigation? Please write at least 2 benefits. (**5 points**)
4. As a mobile forensics examiner, you just purchased a new forensics software. Please explain the procedure of validating the new forensics software. Please list the steps as 1, 2, 3, 4, and so on. (**10 points**)
5. Please read the article named *Open Source Forensics Tools* and answer the following questions:
   1. What are the legal requirements of digital forensics tools (**2 points**)? How do open source tools satisfy those requirements (**2 points**)?
   2. What is the goal of digital forensics in an investigation (**2 points**)?
   3. What is “Daubert Test” (**2 points**)? How does open source digital forensic tools satisfy the “test”? (**2 points**)