Matthew Austin

Mobile Forensics

**Assignment 3**

**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)***

The UICC is a mobile smart card that is used in mobile terminals in cellular networks. While only being a few kilobytes, the UICC provides security and integrity to personal data. It is an advanced version of a SIM card. It is comprised of a computer/microprocessor, its own data storage and software, and can connect to the internet with its own Internet Protocol.

1. 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)***

ICCID stands for (Integrated Circuit Card Identifier)

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

***ICCID:*** 9868 3203 0012 0010 12

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

They are important because it can help the examiner determine the phone calls sent/received, contacts, sms details, customer database, call detail records, and HLR.

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**) Yes.

1. What is IMSI (**5 points**)? Why is this IMSI important to mobile forensics (**5 points**)?

International Mobile Subscriber Identity which a is the unique number that identifies the subscriber on the cellular network. It is important to mobile forensics because this number is used to find a subscriber across the network and deliver calls, data, and other transactional information.

1. 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**): 460
   2. Network Carrier name (**4 points**): 011
   3. MISID – Mobile Station ID (**2 points**): 361608170
2. 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:*** 1392
   2. ***1010 1000 0010 1001:*** 10829
   3. ***1345:*** 0001 0011 0100 0101
   4. ***5963:*** 0101 1001 0110 0011
3. Please explain what is PIN1, PIN2, and PUK in SIM card (**10 points**)

The PIN1 code is used to prevent others from gaining unauthorized access to your mobile phone handset. The PIN2 code is a four- to eight-digit password that you enter when using or requesting user certificates or performing tasks such as resetting total call charges. PUK is used to unlock a PIN1 or PIN2 for which PIN Lock has been activated after the wrong PIN code is entered three times in a row.

1. 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**): 1-732-640-7329
   2. The voice mail # (**1 point**): 1-805-637-7243
   3. Check Balance # (**1 point**): #225#
   4. Check Text usage # (**1 point**): #674#
   5. Forbidden PLMNs (**1 point**): FFFFFFFFFFF (None, I assume)
2. What is the benefits of using multiple forensics tools in a mobile forensics investigation? Please write at least 2 benefits. (**5 points**)
3. one software solution will not provide all the tools necessary to process: Every type of device, OS, and different types of stored data
4. No one tool can process and analyze all mobile devices.
5. 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**)
6. Created an image (baseline) of device M using MPE+.
7. Created a hash list of the files using FTK.
8. Using UFED Touch (the software to be validated) and the same device M, conducted a full extraction of the device.
9. Compared the files obtained from the collection by UFED Touch to the hashes obtained in step 2 in FTK
10. Analyzed any files that were different as identified by the hash.

1. 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**)?

Open source tools disclose all of their procedures through source code and allow one to verify that the tool is indeed following the published process and not publishing only the minimum required. In addition, open source tools should publish the procedural details in a language other than just source code. They satisfy those requirements by showing all other procedures and code for the community to look over and fix.

* 1. What is the goal of digital forensics in an investigation (**2 points**)?

The goal of digital forensic analysis is to identify digital evidence for an investigation. An investigation typically uses both physical and digital evidence with the scientific method to draw conclusions.

* 1. What is “Daubert Test” (**2 points**)? How does open source digital forensic tools satisfy the “test”? (**2 points**)
     1. Testing: Can and has the procedure been tested?
     2. Error Rate: Is there a known error rate of the procedure? - Publication: Has the procedure been published and subject to peer review?
     3. Acceptance: Is the procedure generally accepted in the relevant scientific community?
     4. Open Source digital tools satisfy the “test” because Open source tools document the procedures they use by providing the source code, thus allowing the community to accept or reject them.