**Assignment 2**

**CIS410/594-01** – Spring Term 2017

**Point Value**: 100 points

**Assignment Due Date**: **02/16/2017**

**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 are the four main phases of mobile forensic examination?The first phase is the seizure of the mobile device. ***(5 points)***
2. What is chain of custody in mobile forensics? ***(5 points)***
3. What is a Standard Operation Procedure document ***(5 points***)? What is the purpose of SOP? ***(5 points)***
4. Please explain what is a search warrant (***5 points***)? What is an Affidavit? ***(5 points)***
5. In the Riley v. California case, a stop for a traffic violation led to Riley’s arrest for a weapons charge. Officers found a mobile phone in the arrestee’s pants pocket. The data was accessed, and a repeated reference to a term known to be associated with a street gang was located on the device. Later, another law enforcement officer examined the device’s contents in more detail and found media (images and videos) that assisted in charging Riley with a shooting. Riley attempted to suppress all the information from the mobile device that it was obtained without a warrant, but he was still convicted. However, the SCOTUS overturned the decision. Why did the SCOTUS dismiss the evidence found in Riley’s mobile phone? ***(10 points)***

1. In *United States v. Grimes (5th Cir. 2001)*, a private citizen searched a computer without consent of the owner and recovered illegal pictures that were later turned over to the police and the illegal pictures are used as evidence against the private citizen. Why are those illegal pictures admissible in court? (**5 points**) Does this violate the Fourth Amendment? (**5 points**)
2. When seizing a mobile phone at the scene, what kind of information about the mobile phone should a mobile forensic examiner document? Please write down at least 10 different types of information about the phone. ***(10 points)***
3. A mobile device can be wiped of data by the owner remotely using the device or manufacturer software. What can you do to prevent the deletion of the data on the mobile device? At least two different methods. ***(10 points)***
4. What are the advantages of turning off the mobile device when seizing it at the scene? ***(5 points)*** What are the disadvantages of turning off the mobile device? ***(5 points)***
5. Besides the mobile device, what are the other evidences a mobile forensic examiner should collect at the scene? At least five items. **( 5 points)**
6. If an employee’s mobile device is owned by his or her employer, can the employer legally examine the mobile device without warrant or consent? Why? **(5 points)**
7. Please read the document named *SWGDE Best Practice for Collection of damaged mobile devices* and answer the following questions:
   1. What is the purpose of this SOP? (**1 point**)
   2. What is the scope of this SOP? (**1 point**)
   3. If a mobile device was previously submerged in liquid, should you remove the battery at the time of collection? (**1 point**) Should you power on the device immediately? Why? (**2 poin**t)
8. Please read the article named *Smudge Attacks on Smartphone Touch Screens* and answer the following questions:
   1. Please explain what is smudge attack in your own words? (**2 points**)
   2. In the experiment 1, what is the degree of the best lens angle for pattern retrieval? (**1 points**)
   3. Does simply wiping the smudges on a touch screen with a cloth defeat smudge attack? (**2 point**)