Matthew Austin

Mobile Forensics

Tian Guyan

February 2016

**Assignment 2**

**CIS410/594-01** – Spring Term 2017

**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. The *Seizure* of the mobile device
3. The *Collection* (extraction data from mobile device) that shows that the ESI did not change and is the same when it was collected
4. *Analysis/Examination* by looking into gigabytes of information with automated tools
5. *Presentation* the examiner must present the findings via a written report.
6. What is chain of custody in mobile forensics? ***(5 points)***

The chain of custody document clearly details in chronological order every hand that has been in contact with the piece of evidence, from the seizure to the disposition.

1. What is a Standard Operation Procedure document ***(5 points***)? What is the purpose of SOP? ***(5 points)***

The Standard Operation Procedure is a written document outlining the mission. It covers the person conducting the examination of data and the first responder who are collecting and seizing the devices holding the digital data.

1. Please explain what is a search warrant (***5 points***)? What is an Affidavit? ***(5 points)***

A search warrant is a legal document authorizing a police officer or other officials to enter and search premises. An Affidavit is a written statement confirmed by oath or affirmation that is used as evidence in court.

1. 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)***

The SCOTUS dismissed the evidence because a person's right against unlawful search extends to their digital devices.

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**)

For the same reason stated above SCOTUS dismissed the evidence because a person's right against unlawful search extends to their digital devices. This especially holds true do to the citizen not being a government official and not having a search warrant. This violates the Fourth Amendment the private citizen violates the person's right to their digital device and the private citizen did not have probable cause supported by oath or affirmation.

1. 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)***
2. The device manufacturer
3. The device model
4. The mobile device serial number
5. The color of the device
6. The type of cover for the device
7. The wallpaper visible on the screen or lock screen wallpaper
8. The presence of a camera on the front and/or back
9. The presence of a headphone jack- top,bottom or side
10. Details of any damage to device
11. The size (estimated dimensions) of the device
12. 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)***
13. Put the device in airplane mode
14. Put the device into a signal isolation bag
15. 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)***

Advantages of Turning off the mobile device are:

1. is a quick way to isolate the device
2. protects volatile memory

Disadvantages of Turning off the mobile device are:

1. The is a risk of encountering a protection mechanism when turned on again.
2. if passwords are not collected before, there will still be authentication mechanisms
3. time on device may be set independently
4. Besides the mobile device, what are the other evidences a mobile forensic examiner should collect at the scene? At least five items. **( 5 points)**
5. USB Drive
6. Chargers and USB Cables
7. SD Cards
8. SIM Cards
9. Older Mobile Device accessories
10. Personal Computers
11. 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)**

Yes the employer can legally examine the mobile device without warrant or consent, because The Texas Workforce Commision Policy states “Make it clear to the employee that the employer reserves the right to search and devices, with storage or memory capabilities that they may bring to work and can make copies of any files found therein”

1. 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**)

The purpose of the document is to describe the best practices for the collection of damaged mobile devices (e.g., smartphones, tablets, feature phones).

* 1. What is the scope of this SOP? (**1 point**)

The document provides basic information on the handling of mobile devices damaged by liquid, structural damage, or thermal exposure. The intended audience is first responders and/or others involved in the collection of damaged mobile devices. The document is not intended as a step-by-step guide for conducting data recovery for damaged mobile devices, nor should it be construed as legal advice. The document does not address the forensic processing of recovered devices.

* 1. If a mobile device was previously submerged in liquid, should you remove the battery at the time of collection? (**1 point**)

Yes the battery should be removed (if possible)

* 1. Should you power on the device immediately? Why? (**2 poin**t)

No, applying power may cause additional damage.

1. 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**)

A Smudge Attack is when an attacker attempts to extract information about user input through the inspection of the users smudges.

* 1. In the experiment 1, what is the degree of the best lens angle for pattern retrieval? (**1 points**)

at a 45 degree angle, as well with the best vertical angles: 15, 75, 90 degrees.

* 1. Does simply wiping the smudges on a touch screen with a cloth defeat smudge attack? (**2 point**)

Even though it may slow down the extraction, partial patterns are easily extracted. This can be simulated with a user putting their phone in their pocket.