

Mobile Forensics: Guidelines and Challenges in Data Preservation and Acquisition

Shivankar Raghav¹ and Ashish Kumar Saxena²

¹Graduate Student of Computer Science, University at Buffalo, 14260, New York, USA

²Managing Director, AKS Information Technology Services Pvt Ltd, 201301, Uttar Pradesh, India

¹rs228@buffalo.edu, ²ashish@aksitervices.co.in

Abstract— By the beginning of June, 2009, the GSM Association reported that there were over 3.8 billion users of GSM networks in the world [1]. This extraordinary development of mobile communications is a source of new security challenges. Many people use mobile phones in their daily activities, and sometimes, those activities might be criminal in nature. The remarkable advancements in the technology and increase in computing power of these devices over the last few years, has led to an increase of their functionality while keeping the size of such devices small enough to fit in a pocket. The use of mobile phones in criminal activities has led to the need of recovering the data in them. The acquisition of information derived from cellular devices can be used as forensic evidence which has become a prime component of crime scene investigations. In this paper we give a brief introduction to the various stages in mobile forensics and focus on the critical stages of preservation and acquisition of digital evidence from mobile phones to be used as evidence in criminal or civil cases. The paper contains a step by step guide to perform the two critical processes and discusses issues which might come up while performing them.

Keywords— Mobile Forensics, Preservation, Acquisition, Forensic Process

I. INTRODUCTION

The mobile phone has revolutionized communications for nearly every demographic, especially teenagers and young adults, connecting them to the Internet and to each other in South Asia no less than they do in the US or Europe. The use of these phones in criminal activities is therefore increasing by the day.

The Mumbai terrorist attack in November 2008 is one of the many examples of mobiles being used as a terror weapon. The most extraordinary part of this attack was the extent to which the terrorists showed themselves to be part of the mobile phone generation, connected electronically to each other and to their controllers during every phase of the operation, from start to finish. The Mumbai attack is certainly not the first time terrorists have used cell phones, but the way they were used is significant and revealing, as well as unique. In such cases there is a large amount of data that can be extracted from these devices and used as forensic evidence.

Mobile Forensics is defined as the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods [2]. The entire process is broadly divided into five stages: Preservation, Acquisition, Examination, Analysis and Reporting. The *Preservation stage* is the first stage in digital evidence recovery and is the process

of seizing and securing suspect property without altering the contents of data that reside in the devices. *Acquisition* is the process of imaging or otherwise obtaining information from a digital device and its peripheral equipment and media [2]. *Examination and analysis* involves applying tools to uncover digital evidence including that which may be hidden or obscured. Reporting is the process of preparing a detailed summary of all the steps taken and conclusions reached in the investigation of a case [2]. Reporting depends on maintaining a careful record of all actions and observations, describing the results of tests and examinations, and explaining the inferences drawn from the evidence.

Of all the stages in mobile forensics, namely Preservation, Acquisition, Examination, Analysis and Reporting, the first two are considered as the most important stages. Preservation and Acquisition of mobile phones can provide critical evidence and productive leads for follow up investigations. These stages must be performed efficiently and each step taken with caution as the next stages of Examination, Analysis and Reporting entirely depends on how well the first two stages have been performed. Hence the process of retrieval of evidence begins in Preservation and Acquisition.

Mobile forensics is a relatively new field of interest within digital forensics but of late growing rapidly. This field offers many possibilities and has a huge potential but there are many issues before this potential can be realized. There is also a need to formulate a step by step plan for conducting a forensic examination. This paper takes a step in this direction by providing a summary of the steps that need to be followed while performing the stages of Preservation and Acquisition. We have also tried to make investigators aware of certain issues pertaining to data preservation and acquisition. This document can be taken as a starting point for researchers who have been introduced to the field of mobile forensics and require information specific to guidelines and challenges in data preservation & acquisition.

II. PROCESS AND CHALLENGES

In this section we give an outline of the main steps to be followed while carrying out the process of Preservation and Acquisition. A few issues that could be encountered while performing them are listed.

The type of phone generally dictates the procedure to be followed in a forensic investigation. We have basically divided the present day phones into 3 major categories: General Phones (Nokia, Samsung, LG), Blackberry models, Chinese mobile

phones and tried to handle each issue in forensic preservation and acquisition with respect to each of them.

A. Preservation:

Preservation involves the search, recognition, documentation, and collection of electronic-based evidence. In order to use evidence successfully, whether in a court of law or a less formal proceeding, it must be preserved. Failure to preserve evidence in its original state could jeopardize an entire investigation, potentially losing valuable case-related information [2]. This stage is performed by the first responders who first arrive at the scene. Their first task is to secure and cordon off the scene and ensure the security of all individuals. Next, the entire scene is documented using camera/video. This is done to create a permanent record of the scene. The team then determines whether there is a need for any kind of DNA analysis to be conducted. A number of challenges, as mentioned below, can come up during this stage:

- i. Phone found in a liquid.
- ii. Identification of Phones
- iii. On – Off State Challenge
- iv. Isolation

The steps taken to meet these challenges are extremely critical for forensic investigators as a small mistake in performing them can lead to loss of crucial evidence.

Our full paper illustrates the stage of preservation in the form of an informative flowchart and discusses all the challenges mentioned. In this extended abstract a major issue in Preservation is described below:

On - Off State: When a mobile is found at crime scene, it may be in an On or Off state. Depending on the power state and model of the phone, different approaches, as described below, are to be followed:

1) General Phones (Nokia, Samsung, LG):

The USSS (United States Secret Service) document [3] lists a set of rules on whether to turn on or off the device:

- If the device is turned “on” do not turn it “off”.
- Turning the device off may activate the lockout feature.
- If the device is turned “off” leave the device “off”.
- Turning it on could alter evidence on device

2) *Blackberry Devices*: The Blackberry is an always on push messaging device. Information can be pushed through the radio antenna at any point of time. The following are the steps to be followed when a blackberry is found on scene:

- If the Blackberry is “off”, leave it “off”.
- If the Blackberry is “on”, turn the radio “off”.

If the unit is off at the time of acquisition, it should be taken to a shielded location to turn it on and the radio immediately shut down before examination [4].

3) *Chinese Devices*: The Chinese phones pose a big challenge for forensic investigators.

The Chinese manufacturers do not follow any standards and therefore it is unclear how the device will behave in different scenarios. Analysis of a few Chinese phones, like the Sciphone i68 (clone of Iphone), clone of N95, clone of Moto Razr has revealed that in case the battery is removed from the cavity of the phone (for 5-10 minutes), no temporary data such as the date, time and call logs get erased (This could probably be due to some amount of charge left in the phone). However, on keeping the phone off for a considerable period of time erased the call logs and temporary data from the Sciphone i68. Therefore on this current issue, it is best advised to treat the phones as a general phone and to follow the steps given in a).

B. Acquisition:

Performing acquisition at the scene has the advantage that loss of information due to battery depletion, damage, etc. during transportation and storage is avoided [2]. However, it is difficult to perform acquisition at the scene due to the absence of a controlled environment. In a laboratory setting this is readily achievable.

When a mobile is brought to the lab, it is first determined whether the device has been identified. Next, if the device is found to be switched on a different flow is to be followed as compared to a device which is found to be switched off. When a phone is found switched on, the examination is quite straight forward leaving a few minor issues such PIN/Password bypass. However in case a phone is found to be switched off, it is required that the SIM be removed and its acquisition done directly. There are various issues that can come up during acquisition

- i. Selection of Correct Acquisition Tool
- ii. PIN/Password bypass
- iii. Issues with Chinese phones

PIN/Password Protection is one important challenge that is faced by forensic investigators. Common obstructed devices include mobile phones with PIN-enabled identity modules, or with an enabled phone lock setting. A number of ways exist to recover data from obstructed devices. One of the ways is to bypass these devices using a set of codes. For example, a method to bypass the password protection in an Apple Iphone is illustrated in the full version of the paper.

A descriptive flowchart for the process of acquisition has been provided in the final document and the above challenges mentioned have been discussed. A few solutions pertaining to these challenges have also been provided.

REFERENCES

- [1] <http://www.gsmworld.com>
- [2] Wayne Jansen and Rick Ayers, “Guidelines on Cell Phone Forensics”, NIST, May 2007
- [3] USSS. (2006). Best Practices for Seizing Electronic Evidence
- [4] Micheal W Burnette, “Forensic Acquisition of a RIM (Blackberry) Device”, June 2002