Survey on Mobile Phone Forensics: Guidelines and Challenges in Data Preservation and Acquisition

Vinod Patil
Abha Gaikwad-Patil College of Engg, Mohgaon, Nagpur

Sulabha V. Patil
Tulshiramji Gaikwad-Patil College of Engg & Technology, Mohgaon, Nagpur.

ABSTRACT
Now a day billions of 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 [1]. The acquisition of information derived from cellular devices can be used as forensic evidence which has become a prime component of crime scene investigations [1]. Here I 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.

Keywords
Mobile Forensics, Preservation, Acquisition, Examination, Analysis and Reporting Preservation, Acquisition, Forensic Process, Analysis, Evidence, Pyramid, SIM, Tools, Forensics, Messages, Mobile.

1. INTRODUCTION
Mobile phones and other handheld devices are everywhere now a day. Cell phones and cellular devices can be involved in a crime or other incident. 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 phone forensic includes the methods that show how evidences are taken from mobile phones. It is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods. It includes analysis of both SIM and Phone Memory [3]. Mobile phones have the similar potential of holding evidence as any other digital media can. A phenomena of recovering deleted information from mobile phone is similar as it can be done for a hard drive [3]. Like any other digital media, evidence items contained in mobile phones are fragile and can easily be deleted or can be overwritten. Main aim for carrying research in the field of mobile phone forensics is to extract useful information from these devices and present it as evidence in court of law. One must be well prepared before trying to examine data on a mobile phone device. Mobile device forensics requires knowledge of the technology and knowing the tools and their limitations of processes is must. Using multiple tools and verifying the results manually can help.

Mobile Forensics Process 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 interferences 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.

2. REVIEW
The digital forensic community faces a constant challenge to stay abreast of the latest technologies that may be used to expose relevant clues in an investigation. Mobile phones are commonplace in today's society, used by many individuals for both personal and professional purposes. Mobile phone forensics is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods. Cell phones vary in design and are continually undergoing change as existing technologies improve and new technologies are introduced. When a cell phone is encountered during an investigation, many questions arise: What should be done about maintaining power? How should the phone be handled? How should valuable or potentially relevant data contained on the device be examined? The key to answering these questions is an understanding of the hardware and software characteristics of cell phones.

3. PROCESS

3.1 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 determined whether there is need for any kind of DNA analysis to be conducted. A series of steps need to be followed after this as shown in Fig. 1. There are certain issues that can arise while following some of the steps. These issues have been handled separately as notes and references from the flowchart have been linked to each of them. Some of the issues that might arise are provided in the notes below:

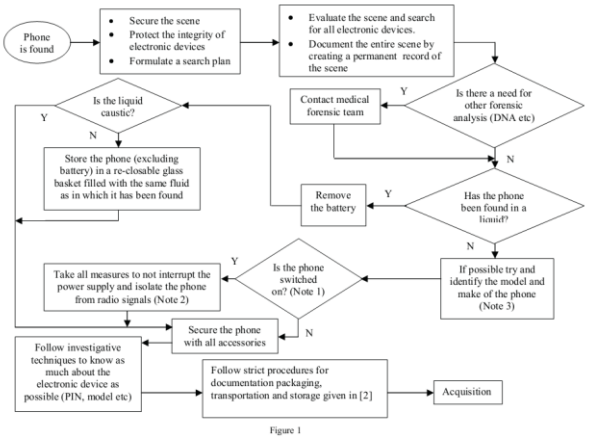

Fig 1: A Series of Steps need to be followed

Note 1: On-Off state

The problem that occurs when a phone is found on a crime scene is whether to turn the device on or off. It is absolutely imperative that these devices are handled properly as the entire process of data acquisition depends on the state of the phone at the crime scene and the way the device is handled. The following are the possible solutions to this issue for each category:

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.

If the phone is kept on, it is required that the phone be isolated from radio signals. This is done to ensure new traffic, such as SMS messages, from overwriting/modifying existing data. This issue is discussed in Note 2.

Note 2: Isolation

If the phone is kept on, it is required that the phone be isolated from radio signals. This is done to ensure new traffic, such as SMS messages, from overwriting/modifying existing data. The following are the techniques widely followed for isolating the mobile device:

1) Use a shielded work area: Shielding an entire work area can be an expensive but effective way to conduct examinations safely in a fixed location. A "Faraday tent" is an inexpensive way to shield an entire work area that also allows portability.
2) Use a shielded container - A portable shielded container can allow examinations to be conducted safely once the phone is situated inside.

Keeping the phone on, but radio isolated, hastens battery life due to increased power consumption as it tries unsuccessfully to connect to a network, raising its signal strength to the maximum.

Note 3: Identification of the phone

Identification of a phone is one of important steps in forensic acquisition since without proper identification, forensic examination using a toolkit, identification of cables for charging the battery and connecting the cable to the computer cannot to perform.

1) General Phones (Nokia, Samsung, LG) models
If the phone is powered on, the information appearing on the display can sometimes help identify the type of phone. For example, the manufacturer's or service provider's name may appear on the display, or the screen layout may indicate the family of operating system used. Other clues that allow identification of a device include such things as manufacturer logos, serial numbers, the cradle, and power adapter. Various Web sites contain databases of phones that can be queried based its specifications and features.

3.2 Acquisition

The process of acquisition begins when the device is brought to the tab after proper preservation, and transportation. Some of the steps in acquisition can actually begin on the scene as time is always of the essence in forensics. The flowchart for acquisition is given in figure 2.

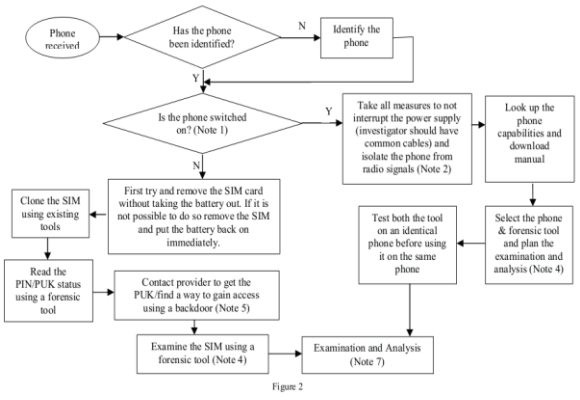

Fig 2: The flowchart for acquisition

Note 4: Choosing the correct acquisition tool

Care should be taken when first choosing a tool to ensure its acceptability and consistency. The tool should be applied on a phone of the same model before using it on the original phone. Forensic specialists should also receive adequate up-to-date training in the tools and procedures to employ. The most important characteristic of a forensic tool is its ability to maintain the integrity of the original data source being acquired and also that of the extracted data. The first problem is tackled by blocking or otherwise eliminated write requests to the device containing the data. The second is done by calculating a cryptographic hash of the contents of the

evidence files created and recurrently verifying that this value remains unchanged throughout the lifetime of those files [2].

Note 5: PIN/Password Protection

Common obstructed devices include mobile phones with PIN-enabled identity modules, or with an enables phone lock setting.

1) General Phones (Nokia, Samsung, LG) phones:
A number of ways exist to recover data from obstructed devices. They fall into three classes:

- Investigate: asking / interviewing the owner of the device, manually supply commonly used input (1-2-3-4 for Nokia 0-0-0-0-0 for Motorola), exploit possible insecure settings.
- Software-based: gain access using software backdoors which are normally built by manufacturers. These backdoors are normally available on the internet or available by contacting manufacturer, use of duplicate (U) SIMS: SIM's can be cloned and the duplicate can be used to try out various methods of forensic investigation without damaging the original SIM.

Note 7: Miscellaneous Issues

- A well-known forensic issue that arises is the status of read and unread messages. Different tools show different results. Reading an unread SMS message from a (U) SIM indirectly through the handset causes the operating system of the phone to change the status accordingly. Had the (U) SIM been read directly by a tool, no change in status would occur.
- Encryption and other techniques might be used to alter the data. The investigator should have the tools and expertise to overcome such circumstances.
- Malicious code: The device may contain malicious software like a virus or a Trojan. Such malicious program may attempt to spread over other devices either over a wired or wireless interface.

3.3 Forensic Acquisition Of Sim Cards:

When conducting forensic examinations of GSM/UMTS mobile devices, it is also important to inspect the contents of associated SIM cards. In some cases, there might be multiple SIM cards that an individual uses in different countries or for different purposes. Some devices function with dual SIM cards. In addition, the storage capacity and utilization of USIM cards is increasing and may contain substantial amounts of relevant information. Furthermore, when a user deletes items from a SIM card, some devices will leave remnants of deleted data on the card like SMS messages [4]. The hierarchical storage structure of a SIM card is relatively straightforward, and the content of each file is defined in the GSM Technical Specification (GSM 11.11). There is one master file that contains references to all other files on the SIM card. There are many tools for extracting data from SIM cards, including TULP2G (http:// tulp2g.sourceforge.net/), developed by the Netherlands Forensic Institute and made freely available. To use TULP2G to acquire data from a SIM card, first open the SIM Investigation profile, select the Investigation tab, and Run the SIM plug-in to extract data from card. The types of information that may be available on a SIM card are listed in below table. This includes the location area identifier (LAI), which is stored in EFLOCI (7F20:6F7E), providing the country, network, and location area identifier. Each time a mobile device moves to a new area, the LAI information is updated on the SIM card. Location information may also be available when the GPRS mobile data service is used. The EFLOCIGPRS (7F20:6F53) contains GPRS Routing Area Information similar to the LAI information as shown in figure 3 using Paraben's Device Seizure software.

Description	Location
SMS	7F10:6F3C
MSISDN	7F10:6F40
Last Dialed Numbers (LDN)	7F10:6F44
Abbreviated Dial Numbers (ADN)	7F10:6F3A
IMSI	7F20:6F07
LOCI	7F20:6F7E
LOCIGPRS	7F20:6F53

Table 1: Selection of Information that can be Stored on SIM Cards

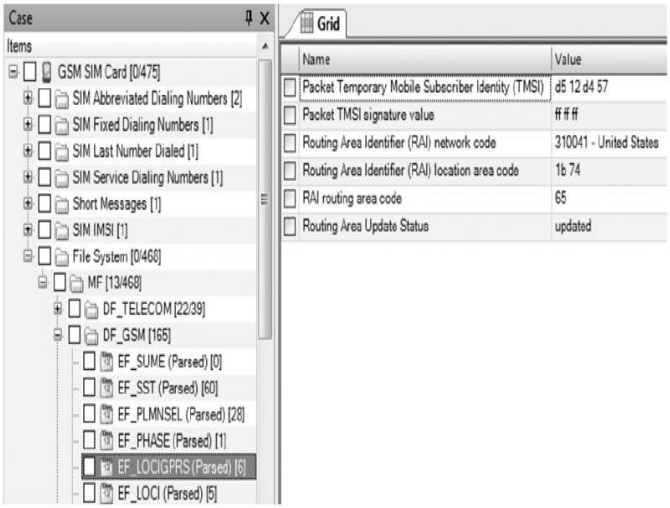

Figure 3. Information extracted from a SIM card using Paraben Device Seizure.

4. EVIDENCE ITEMS AVAILABLE IN MOBILE PHONES

Possible evidence items that can be found from modern day mobile phone while carrying forensic examination include those mentioned in the Table 2.

Evidence Items	Source
Name of Service Provider	Printed on back of SIM
Unique Id Number	-"-
Location Area Identity (LAI)	Stored inside SIM
Integrated Circuit Card Identifier (ICCID)	Stored inside SIM and corresponds to the number printed on SIM
International Mobile Subscriber Identity (IMSI)	Stored inside SIM and it is unique id for every subscriber
Text Messages Data (SMS)	Stored on SIM as well as on handset
Contacts	-"-
Call Logs	-"-
International Mobile Equipment Identity (IMEI)	Stored as well as printed on Mobile
Multimedia Messages	Mobile phone memory
Images/Sound/Videos	-"-
WAP/Browser History/Emails	-"-
Calendar Items / Notes	-"-
Information of Previous SIMs	Few mobile phones also hold information of previously used SIM cards
MSISDN(Mobile Subscriber Integrated Services Digital Network) / Telephone Number	At times available in SIM memory. Few network operators give facility to dial some code for finding it

Table 2: Possible evidence items on mobile phone

5. CHALLENGES ASSOCIATED WITH MOBILE PHONE FORENSICS

- Use new forensics tools and techniques due to fast changes in technology.
- Signals of mobile phone need to be blocked while carrying forensics analysis.
- Identification and collection of cables required for forensics analysis of mobile phones is challenging task.
- Most of the commercially available forensic tools do not provide solutions to deal with physically damaged mobile phones. Forensic examiners must be trained and equipped to handle such situations.
- Mobile phones may lose data or ask for security measures on next restart once shut down. Owner of the mobile phone (if available) may be asked about security codes.

6. CONCLUSION

There is immense scope in the area of mobile forensics as it is relatively a new field. We have provided a summary of the steps that need to be followed while performing the stages the first two stages. We have also tried to make investigators aware of certain issues pertaining to data preservation and acquisition in mobile forensics and discussed a few possible solutions. Like any other digital forensic investigation, it is vital to recover all possible evidence from a mobile phone device in a forensically sound manner. Due to the variety of different handheld device models, firmware releases, service providers, etc., forensic examination of cellular phones can be a challenging process. The examination of cellular phones and handheld devices is beneficial for law enforcement, in the collection and preservation of valuable evidence.

7. REFERENCES

[1] Shivankar Raghav and Ashish Kumar Saxena, Nov. 2009 "Mobile Forensics: Guidelines and Challenges in Data Preservation and Acquisition".

[2] Wayne Jansen and Rick Ayers, "Guidelines on Cell Forensics", NIST, May 2007.

[3] Amjad Zareen and Dr. Shamim Baig, August 2010 "Mobile Phone Forensics: Challenges, Analysis and Tools Classification".

[4] Eoghan Casey and Benjamin Turnbull, "Digital Evidence on Mobile Devices".

[5] Wayne Jansen and Ricy Ayers, "Cell Phone Forensic Tools", NIST, May 2007.

[6] Sue Wilkinson,"ACPO Guide for Computer Based Evidence", 2007.