IOSR Journal of Engineering (IOSRJEN)
e-ISSN: 2250-3021, **p**-ISSN: 2278-8719
Vol. 3, Issue 8 (August. 2013), ||V1|| PP 23-29

Mobile Forensics Opportunities and Challenges in Data Preservation

Mojtaba Dashti[1], Leyla Roohi[2], Rezza Moieni[3]
University Teknology Malaysia (UTM) Malaysia [1]Mdkseyyed3, [2]Rleyla3, [3]*Mrezza3*

Abstract: - Mobile cellular telephone subscriptions are subscriptions to a public mobile telephone service using cellular technology, which provide access to the public switched telephone network [1]. Nowadays, mobile phone handhelds are everywhere and are used for various applications. Convergence of media provides a great opportunity for mobile users. Yet, there has been a growing rate of challenges according to mobile systems. The advancement in mobile computing systems in one hand and reducing the size of handhelds in the other hand are the main reasons of widely usage of mobiles. Meanwhile, the criminal use of mobile phones has led the need of recovering their data [2]. The derived data from mobiles can be used in forensics according to terms and conditions. In this paper various challenges in mobile forensic is reviewed with a focus on mobile models and categories. Then a fundamental vision on data acquisition and mobile data preservation is presented. In this paper a step by step data collection and preservation is identified.

Keywords: - *mobile, forensics, preservation, acquisition*

I. INTRODUCTION

There are few researches about mobile forensics [11][12] evolution in consumer electronics has caused an incredible growth in the size of mobile digital data. Most mobile phones these days have a built-in camera and are able to record, store, play and forward picture, audio, and video data [13]. Some others are utilized with radio and/or other multimedia applications. All these applications need a memory to process and store and retrieve data. A lot of this data is related to human behavior and might become subject of a forensic investigation [13].

There are a large variety of memories in mobile phones. Currently, flash memories are the most dominant non-volatile solid-state storage technology in consumer electronic products. An increasing number of embedded systems use high level file systems comparable to the file systems used on personal computers. Current forensic tools for testing of mobile phones or PDAs or any other embedded systems usually perform logical data acquisition [13] by which it is not possible to recover all data from a storage medium most of the time. For example deleted files are recoverable, but sometimes also other data which is not directly relevant from a user side, cannot be acquired and potentially interesting information might be missed. For this reason data acquisition is wanted at the lowest layer where evidence can be expected. For hard disk based storage media it is very common to copy all bytes from the original storage device. The same procedure is desired for embedded systems with solid-state storage media well [13]. in the following section, structure of mobile devices is described in order to clarify the fundamentals of storage and retrieval of data.

II. STRUCTURE OF MOBILE DEVICES[16]

The mobile system consists of four main elements; SIM card, Memory, Mobile network and mobile equipment. In this section these elements are described. For the sake of this article, the use of mobile devices is not referring to thumb drives, USB drives, memory sticks portable flash drives, or portable externally enclosed hard drives. Mobile devices specifically refer to Cellular (or Mobile) Phones, Portable Digital/Data Assistants (PDA's), and Smart Phones. Bear in mind that some of the older model PDAs's, such as the initial Palm and BlackBerry series devices do not have radio (cellular) capability and are simply used to store personal information (contacts, calendars, memos, to-do lists, etc.).

Mobile Devices can be categorized as:

1) *Cellular Phones*
a) *Code Division Multiple Access (CDMA) - Typically handset only*
b) *Global Systems Mobile (GSM) - Handset and SIM*
c) *Integrated Digital Enhanced Network (iDEN) - Handset and SIM*
2) *Portable Digital/Data Assistants (PDA's)*
a) *Palm Pilots (Palm OS),*
b) *Pocket PC's (Windows CE, Windows Mobile),*
c) *BlackBerry's (RIM OS) that contain no radio (cellular) capability.*

d) *Others (Linux, Newton,)*

3) *Smart Phones - hybrid between 1 and 2, which have radio capability.*

Making a video or audio call is no more main function of mobile phones. Nowadays smartphones are the main players of this area. [16]. smartphones encompass the features of cell phones (radio capability) and the ability to store data as well as surfing the web and/or send text messages (SMS) and/or multimedia messages, (MMS). Checking emails, instant message (IM), downloading/uploading content to and from the Internet, take pictures as well as video. In fact, a mobile device can do what a computer system can do, just on a smaller scale. In this way, many forensic threats or crimes can be committed using mobile phones [16]. However special characteristics of mobile phone need special forensic tools to acquire preserve and investigate data in a mobile.

Table 1,2 have listed some common tools.

Details of digital data is examined carefully by forensic experts usually by a computer. After that, the forensic experts conduct tests, examine and analyze the data according to each case using specifically tailored tools with design specifications. Some of the tools are battery powered and use volatile memory susceptible to the loss of data. Although, recently forensic experts recover and capture deleted information using portable devices when conducting examinations such as e-mail addresses, user's text messages, user's profile, and user's contact list, date of modification, pictures and telephone numbers. Furthermore, different devices such as; memory card, Personal Digital Assistant (PDA), digital Audio player, camera, Global Positioning Systems (GPS), laptops and other systems and devices were usually found at any crime scene. By measuring up correspond to moveable PC, and their extracted features are of great benefit to digital investigators. [14]. To effectively obtain some benefits of the forensic investigations, organizations should formulate clear forensic policy statements which define the roles and responsibilities of their internal and external workforce, their reporting relationships, quality verifications of measures, recording and handling of sensitive information, legal compliances, management support, policy reviews, and endorse forensic activities [11].

III. ACQUISITION OF MOBILE DATA

The word 'forensics', when used in conjunction with computers, is normally thought of as the analysis of a computer system for the purpose of achieving a prosecution in relation to a criminal act conducted using the computer system [17]. Rather the software applications developed and deployed on the mobile device acts more like 'spyware', which allows the employer to check mobile devices which they own but are used by an employee in carrying out the duties of their employment. Therefore, the employer may simply wish to maintain an ability to check mobile devices for illegal content. Illegal content may include downloaded Internet images or confidential files that an employee should not have access to.

Many tools are developed for mobile forensic so far. Two main categories are memory forensic tools and SIM forensic tools. Table I lists mobile devices analysis tools while table II depicts SIM cart forensic tools.

TABLE I. Mobile Device Forensic Tools [16]

Tools Name	Tools Link
Aceso (Radio Tactics, Ltd.)	http://radio-tactics.com/
Athena (Radio Tactics, Ltd.)	http://radio-tactics.com/
BitPIM	http://www.bitpim.org/
CellDEK (Logicube)	http://www.logicubeforensics.com/products/hd duplication/celldek.asp
CellDEK TEK (Logicube)	http://www.logicubeforensics.com/products/hd duplication/celldek-tek.asp
Device Seizure (Paraben)	http://www.paraben-forensics.com/handheld forensics.html
MOBILedit! Forensic	http://www.mobiledit.com/forensic/
Neutrino (Guidance Software)	http://www.guidancesoftware.com/products/neutrino.aspx
Oxygen Forensic Suite	http://www.oxygensoftware.com/en/products/forensic/
PhoneBase2 (Envisage)	http://www.envisagesystems.co.uk/html/phonebase.html
Secure View for Forensics (Susteen)	http://www.mobileforensics.com
TULP2G (NFI)	http://tulp2g.sourceforge.net
UFED (Cellebrite)	http://www.cellebrite.com/cellebrite-for-forensics-law-enforcement.html
XRY (MicroSystemation)	http://www.msab.com/en/

TABLE II. SIM Card Forensic Tools[16]

Tools Name	Tools Link
ForensicSIM	http://www.radio-tactics.com/forensic sim.htm
SIMCon	http://www.simcon.no
SIMIS	http://www.3gforensics.co.uk/simis.htm
SIMSeizure	http://www.paraben-forensics.com/handheld forensics.html
USIMdetective	http://www.quantaq.com/usimdetective.htm

IV. PRESERVATION AND ACQUISITION PROCESS AND CHALLENGES

In this part we speculate the Preservation and Acquisition process. As above mentioned Preservation and Acquisition are one of main steps in mobile forensics and need to be implemented with great care. The process in forensics study is typically identified by type of phone. We have classified the existing phones into 3 main classes: Typical mobile phones (Nokia, Samsung, and LG), Blackberry models, Chinese mobile phones and attempted to describe forensic problems of each category according to preservation and acquisition.

B. Preservation

Preservation includes the search, identification, documentation, and capturing of electronic-based evidence. For a successful use of evidence, no matter where it is used, it ought to be preserved. Not good preserving of evidence in its original could put in the whole investigation to a dangerous situation due to losing precious case-related information. This step is done by the first responders who first arrive at the scene. Securing the scene and to make sure of the security and safety of all individuals is their initial job. Afterwards, the whole scene is recorded using camera/video. This is executed in order to have a permanent record of the scene. Then, the investigator team indicates if or not they need to conduct any DNA analysis. The procedure in the following of above mentioned process is shown on table III. Several specific issues might be arisen while following the procedure. These issues have been tackled one by one as challenges and references from the flowchart. Some possible issues are as following:

TABLE III. : Actions After Cellphone Is Founded In Crime Scene

Step	Action	Next Step
1	Secure the scene Protect the integrity of electronic devices Formulate a search plan	2
2	Evaluate the scene and search for all electronic devices Document the entire scene by creating a permanent record of the scene	3
3	Is there a need for other forensic analysis (DNA etc)	If yes 4 If no 5
4	Contact medical forensic team	5
5	Has the phone been found in a liquid?	If yes 6 If no 9
6	Remove the battery	7
7	Is the liquid caustic?	If no 8 If yes 12
8	Store the phone (excluding battery) in a re-closable glass basket filled with the same fluid as in which it has been found	12
9	If possible try and identify the model and make of the phone (challenge 3)	10
10	Is the phone switched on? (challenge 1)	If yes 11 If no 12
11	Take all measures to not interrupt the power supply and isolate the phone from radio signals (challenge 2)	12
12	Secure the phone with all accessories	13
14	Follow investigative techniques to know as much about the electronic device as possible(PIN, model etc)	14
15	Follow strict procedures for documentation packaging transportation and storage given in [2]	16
16	Acquisition	end

Challenge1: On-Off State

One of the main challenges occurs when a mobile phone is found at a crime scene. The problem of finding a phone in a crime scene and the decision on turning it on or off is very challenging these days. There may be a situation in which the power of mobile is going to be off. Moreover changing the on/off situation may cause a change in the RAM data of the mobile.

It has to be noted that such devices must be handled appropriately as the whole procedure of data acquisition relies on the way of handling them. Feasible solutions to the above issue can be described as following:

1) General phones (Nokia, Samsung, LG): **A set of rules provides by USSS (United States Secret Service):**

- 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.

It is strongly needed to isolate the phone from any radio signals in case of the phone is kept on. This reason for this action is to preserve the phone information such as SMS messages from distorting. This problem is discussed in detail in challenge 2.

2) Blackberry devices

Such devices are a permanent on push messaging device. Information can be pushed via radio signals at any time. If the device is kept on and demands for a passkey, its battery has to be removed and placed in a preserved bag from radio signals. If the device is off, it has to be taken in a safe and secured location. Afterwards, it must be turned off [2].

3) Chinese Devices

The Chinese devices cause great concerns in the field of forensics investigations. The Chinese phone production companies do not execute any standards and thus it is quite difficult to predict the phone behavior in different situations. It can be inferred from the analysis of some Chinese phones such as, Sciphone i68 (clone of iPhone), clone of N95, clone of Moto Razr that if the battery is removed from the device, all temporary data is kept [2]. But, if turning it off continues for a long time, the temporary data are removed from the phone of Sciphone i68. Hence, for this issue, it is better to behave them like general phones and follow the procedure when facing General Phones.

Challenge2: Isolation

In case of the device is kept on, it is needed to isolated from radio signals. This is done for preventing any distorting actions on inside data. The following are actions that vastly done in order to isolate the mobile device:

1) *Use a shielded work area:* Shielding the whole area might be very costly but effective action to investigate safely. A "Faraday tent" is a cheap way to isolate the whole investigation area which lets portability as well.

2) *Use a shielded container:* A portable shielded container can let the conducting of investigation safely at the time that the phone is located inside of container.

Keeping the phone on, while radio isolated causes deteriorating the battery life because of the increased power consumption since it attempt continuously for connecting to a network. The solely solution is to have as much as possible cables in hand.

Challenge 3: Identification of the phone

One of the most important stages is identification of a phone. Not identifying the phone properly makes any forensic investigation (using toolkit, cables identification in order to charge the battery etc.) totally impossible.

1) General phones (Nokia, Samsung, LG) and Blackberry models:

If the phone is kept on the information on device's display might help to indicate the phone type. For instance, the manufactures or service provider's name may appear on display. Some other things that might help in identification of a device involves: manufacturer's logos, serial numbers, the cradle and power adaptor. [8] is one example of web sites which contain different mobile phone databases that can be used for identification of a specific phone based on characteristics and attributes.

2) Chinese phones:

It is quite impossible and difficult to identify a Chinese mobile phone without removing the battery since they are just clones of current mobile phones and thus they do not carry any labels or manufacturer's names on them. It is perilous for a forensics investigator with the latest knowledge of mobile phones who face with such situation.

Several highlighted clues that might help the investigator to identify if or not a phone is a Chinese clone are as follows:

- It is possible that a clone does not have any manufacturer's or service provider's logo
- The thickness/weight and other appearance features might be different from the original one
- The IMEI number is possibly invalid when the battery is removed

The following are some advices on how to recover the name/hardware and software of a Chinese phone:

- The mobile phone is generally similar to one of the existing phones in the market and can be figure out by looking up on the Internet and searching by typing: 'ABC clone' for example to identify the hardware and software
- Removing the battery and then appearing the IMEI number, however it is needed to placed back the battery immediately and switch the phone to the previous state, unless there is danger of altering the state of the phone

C. Acquisition

This process commences when the device is arrived on the lab after appropriate preservation, and transportation. Some of the acquisition stages can be started at the scene with considering that time is a crucial factor in forensics investigation. Table IV portraits the flowchart of acquisition process. A great care ought to be taken when choosing a proper tool to ensure its acceptability and consistency. The tool which is supposed to choose has to be applied to a same model of phone prior to applying to the original phone. Forensics experts should also be equipped with the sufficient latest training information of the tools and procedures.

TABLE IV. Acquisition process

Step	Action	Next Step
1	Phone received	2
2	Has the phone been identified?	If no 3 If yes 4
3	Identify the phone	4
4	Is the phone switched on? (challenge 1)	If yes 5 If no 9
5	Take all measures to not interrupt the power supply (investigator should have common cables) and isolate the phone from radio signals (challenge 2)	6
6	Look up the phone capabilities and download manual	7
7	Select the phone and forensic tool and plan the examination and analysis (challenge 4)	8
8	Test both the tool on an identical phone before using it on the same phone	14
9	First try and remove the SIM card without taking the battery out. If it is not possible to do so remove the SIM and put the battery back on immediately	10
10	Clone the SIM using existing tools	11
11	Read the PIN/PUK status using a forensic tool	12
12	Contact provider to get the PUK/find a way to gain access using a backdoor (challenge 5)	13
13	Examine the SIM using a forensic tool (challenge 4)	14
14	Examine and analyze (challenge 6)	end

Challenge 4: choosing the correct acquisition tools

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 forensics tool's features are its capability of marinating and keeping the original data source in mobile phones and extracting them as well. The first issue is handled by preventing the devices from any request for distorting the data inside the phones. The second one is tackled by calculating a cryptographic hash of the contents of the evidence files built and validating that this value remains unchanged throughout the lifetime of those files.

Challenge 5: PIN/Password protection

General blocked devices involve mobile phones with PIN-enabled identity modules or a phone with enabled lock setting.

1) *General phones (Nokia, Samsung, LG) and Chinese phones.* There are several ways to retrieve data from blocked mobile phones. They are classified into three categories.

- Investigative: Interviewing the device owners that manually provide common used input (1-2-3-4 for Nokia mobile phones and 0-0-0-0 for Motorola devices), disable feasible insecure settings.
- Software-based: Attain access using software which are typically created by predictors and manufactures.

These software backdoors are typically accessible on web-based sources or via contacting with manufactures and service providers, use of alike (U) SIMS: SIM's can be cloned and the alike software backdoor (duplicate) can be used to test different methods of forensic investigation with no deteriorating the original SIM.

Some websites like [10] supply their Chinese mobile phone's owners by offering them the unlocking and other secret codes. There are other forums and websites that facilitate the process of bypassing unlock codes for specific types of mobile phones. For instance, there is the password for iPhone in order to being bypassed and thus all its inside information can be accessed.

2) Blackberry phones:

The best action to do is to get the password in case the RIM is password protected. The RIM password is not kept inside the device, it is only identifiable by comparison the original password and the password entered by the user. The investigator can try his/her chance to guess that for only 10 times before the file system wipe is activated for protecting the data. In case the file system wipe is activated by the device all non-OS files will be destroyed. There is no software up to now that able to bypass the password protection system of mobile phone devices. In case of not having the password the only solution would be direct-to-hardware.

Challenge 6: Miscellaneous issues

- The status of read and unread messages is a popular forensic issue. Various outcomes are resulted through various ways and tools. When an unread SMS message is read indirectly from a (U) SIM is read make the phone operating system to alter the SMS message status in response and vice versa, if it is read directly by a tool, thus no changes in the SMS message would happen.
- Encryption and some other techniques can be applied to change the inside data. The examiner has to be familiar with and have the required tools and know how to response in face of such phenomenon.
- Malicious code: It is possible that the mobile phone contains malicious software such as virus or Trojan. No matter through a wired or wireless connector, such software may try to expand into other mobile phones and other devices.

V. CONCLUSION

In this article, various challenges in the field of mobile forensic are introduced in terms of preservation and acquisition of data. The introduced challenges categorized to different mobile phones like smartphones, normal phones and Chinese ones. Also a recommendation on data preservation of forensic data in mobiles is presented.

REFERENCES

[1] International Telecommunication Union, World Telecommunication/ICT Development Report and database, and World Bank estimates
[2] Shivankar Raghav and Ashish Kumar Saxena, "Guide lines and challenges in Data preservation and Acquisition" , 2009
[3] USSS. (2006). Best Practices for seizing Electronic Evidence
[4] Michael W Burnette, "Forensic Acquisition of a RIM (Blackberry) Device", June 2002.
[5] Wayne Jansen and Rick Ayers, " Cellphone Forensic Tools", NIST, May 2007
[6] Sue Wilkinson, "ACPO Guide for Computer Based Evidence", 2007

[7] Shafik Punja, "Blackberry Forensics – Mobile Forensics World Conference", 2009
[8] GSM Arena, www.gsmarena.com, Phones, www.phonescoop.com
[9] Numbering planes, http://namehangkorpa.wordpress.com, 07(acc)
[10] Iphone Pass Code workaround, http://mobileforensics.files.wordpress.com
[11] Wayne Jansen and Rick Ayers, "Guide lines on Cell Phone Forensics NIST, May 2007
[12] Breeuwsma, M. et al, Forensic Data Recovery from Flash Memory, Small Scale Digital Device Forensics Journal, Vol. 1 , No. 1, June 2007, pp1-17,
[13] Breeuwsma, M., Jongh, M. De, Klaver, C., Knijff, R. Van Der, & Roeloffs, M. (2007). Forensic Data Recovery from Flash Memory, 1(1).
[14] Tomlinson, Hugh(2010). "Assassins Had Mahmoud Al- Mabhouh in Sight as Soon as He Got to Dubai." Times, 17 Feb. 2010. Retrieved 10 May 2011. site: http://www.timesonline.co.uk/tol/news/world/middle_east/article702 9669.ece.
[15] Breeuwsma, M., Jongh, M. De, Klaver, C., Knijff, R. Van Der, & Roeloffs, M. (2007). Forensic Data Recovery from Flash Memory, 1(1).
[16] Punja, S. G., & Mislan, R. P. (2008). Mobile Device Analysis, 2(1), 1–16.
[16] Punja, S. G., & Mislan, R. P. (2008). Mobile Device Analysis, 2(1), 1–16.
[17] Irwin, D., & Hunt, R. (2009). Forensic information acquisition in mobile networks. *2009 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, 163–168. doi:10.1109/PACRIM.2009.5291378