INTRODUCTION OF TECHNIQUES AND PROCESSES OF MOBILE FORENSIC

Yadav Gupta[1], Ishdeep Singla[2]
[1]M.Tech Student, Department of Information Technology
[2]Assistant Professor, Department of Computer Science and Engineering
Chandigarh University
Mohali, India.

Abstract: ***Today mobile phone devices proliferation is on increase. Mobile phones are used to hold information about the owner and their day to day activities, and sometimes, those activities might be criminal in nature. The use of mobile phones in criminal activities has led to the need of digital forensics. The aim of digital forensics is to recover the potential digital evidence from mobile phones using forensically sound methods so that it can be presented and accepted in court. In this paper, we give a brief introduction to various stages in mobile forensics process and current data acquisition methods and focus on critical stages, preservation and acquisition, of mobile forensics.***

Keywords: ***Mobile Forensics, Preservation, Acquisition, Forensic Process, Digital evidence, Data acquisition, Logical acquisition, Physical acquisition, and Chip-off acquisition.***

I. INTRODUCTION

In the modern era, mobile devices are becoming ubiquitous used by young adults, especially by teenagers for connecting to Internet and to each other. There are 6.8 billion mobile phone users out of 7 billion people worldwide [1][2]. With the advancement of technology, these devices are involved in many day to day activities like the history of the user's behaviour, the user's location information, and lists of frequently views websites in our life. The increasing in use of mobile phones increases criminal activities day by day. The Mumbai terrorist attack is one of the many examples of mobiles being used as criminal activities [3].

Digital forensics of mobile phones is defined as science of recovering digital evidence using forensically sound methods so that it can be presented and accepted in court [4]. The entire process of digital forensics consists of four phases [4]: Preservation, Acquisition, Examination and analysis, and Reporting. In recovery of digital evidence, Preservation phase is the first phase, the forensics investigator must preserve the devices in its original form without altering the contents of data that reside in the devices. In acquisition Phase, forensics investigator acquires data from digital device and its peripheral equipment and media [4]. After that, the forensics investigator starts examining and analyzing the acquired data to uncover digital evidence that may be hidden or obscured. Reporting, the final phase, forensics investigator preparing a detailed summary of all the facts found in previous phase to present to the court or interested entity.

The first two phases, Preservation and Acquisition, of mobile forensics are most important phases can provide critical evidence. An Examination and analysis, and Reporting phase entirely depends on Preservation and Acquisition phases of mobile devices.

In this paper we will focus on the entire process to recover the digital evidence from mobile phones and the current forensics data acquisition methods.

II. PROCESS

In this section, we describe the process of mobile forensic. As mentioned in section 1, the first two phases, Preservation and Acquisition are critical phase and need to be performed with extreme care.

Generally the procedure to be followed in a forensic investigation is dictating from the type of phones. The present day phones are basically divided into three major categories: General Phones (Nokia, Samsung, LG), Blackberry models, Chinese mobile phones [3].

A. PRESERVATION

Preservation is the first and most critical phase of mobile forensic used to confiscating and securing the phone without altering the data contained in the device. Preservation involves the recognition, documentation, search and collection of digital evidence from mobile phone [3]. An entire investigation could endanger without preserve evidence in its original state. First responders who arrive first at scene perform this stage [3]. They first secure the entire scene and documented using camera/video to create permanent record of the scene. After that they inform investigators team to determine whether there is a need for any kind of DNA analysis, to be conducted. While preserve the device certain issues that might arise are mentioned below :

1. On-Off State
2. Isolation
3. Identification of phone
4. Phone found in liquid

These challenges are handling with extreme care as a little mistake jeopardize all process and can lead to loss of potential evidence. The major issue of the Preservation is described below :

1. **On-Off State** Whether to turn the device on or off is the problem that occurs when a phone is found on the crime scene. The device will often be transported in the same state to avoid a shut-down, which would change files [4].These devices are handled with extreme care as the entire process of data acquisition depends on the state of the device found at the crime scene. The possible solutions to this issue for all categories are following :

a) General Phones (Nokia, Samsung, LG)
Whether to turn on or off the device, USSS (United States Secret Service) document [6] lists a set of rules:

1) If the device found on crime scene is turned off leave the device "off", turning the device "on" could alter the content of device.
2) If the device found on crime scene is turned "on" leave the device "on", turning the device "off" may activate the lock of the phone

b) Blackberry phones
In blackberry phones, information can be pushed through the radio antenna at any point of time [3]. If blackberry phones are found on crime scene the following steps are followed:

1) If the device found on crime scene is "off", leave it "off".
2) If the device found on crime scene is "on", turn the radio "off".

c) Chinese Phone
The day to day advancement in Chinese phones becomes a big challenge for forensic investigators. The Chinese companies of mobile phones do not follow any standards [3] and therefore it is difficult to analysis how the device will work with different environments. Reviewing a few Chinese phones revealed that if the battery is removed from phone, no temporary data like call logs, date and time get erased [3]. If the Chinese's phones are keeping off for a considerable period of time it was observed that temporary data will get erased. Therefore treat the Chinese phones as a general phone for investigation, it is best advised on this current issue.

B. ACQUISITION

Acquisition is the process used to acquire the digital evidence from the device that is brought to the lab after proper preservation, documentation, and transportation [3]. Actually acquisition begins on the scene, performing acquisition at the scene has advantages that loss of information due to battery depletion, damage, etc. during storage and transportation is avoided [4]. There are certain issues that might arise are mentioned below :

1. Choosing the correct acquisition tool.
2. PIN/Password Protection.

1. **Choosing the correct acquisition tool**
To acquire the data from device acquisition tools are chosen with extreme care. Firstly tool should be applied on same model of phone found on scene before applying it on original phone. The acquisition tool has the characteristic that its ability to maintain the integrity of extracted data and the device being acquired. This issue is solved by calculating a hash value of the contents of the acquire data and verifying that with the original data on device [4].
2. **PIN/Password Protection**
This is the major issue arise while acquiring the data from mobile phones. Generally PIN-enabled identity modules, or phone lock setting are enabled with the common obstructed devices. The solutions to this issue are described below:

a) General Phones (Nokia, Samsung, LG) and Chinese phones

- **Investigative:** PIN/Password codes can be acquired by interviewing the owner of the device; manually supply commonly used code like 0-0-0-0 for Motorola, 1-2-3-4 for Nokia [3].
- **Software based:** PIN/Password codes can be acquired by using software backdoors which are normally built by manufacturers [3].

b) Blackberry phones
The passwords of Blackberry devices are not stored on devices. The only opportunity for the examiner is to guess 10 times before all the non-OS files get destroy. If the password is not available, then direct-to-hardware solution will be required.

c) Examination and analysis
After acquisition phase, the forensics investigator starts examining and analyzing the acquired data to uncover digital evidence that may be hidden or obscured [3]. The examination of the digital evidence can either be done by hand or with the help of software tools. The investigators use different types of tools for that purpose. Extreme care should be taken while examine and analysis because on particular tool didn't have the right feature [3].

d) Reporting
Reporting, the final phase, forensics investigator preparing a detailed summary of all the facts found in previous phase to present to the court or interested entity. In Reports, the kinds of data extracted and documented, the process used extract data from phone, and any other findings should be documented in a conclusive manner for law enforcement purposes [3]. If the authenticity of the evidence is questioned, the evidence is useless.

III. FORENSICS DATA ACQUISITION METHODS

In this section, we will explain the types of data acquisition methods used for mobile phones. Data acquisition methods

are manual, logical, physical, and chip-off [5].

a) Manual Acquisition

The simple and easy method to acquire data from mobile phones is Manual acquisition [7]. A manual examination of a cell phone typically involves manually retrieves the different areas of information, such as text messages and call history by uses the keypad of mobile phones and taking pictures of data displayed on screen with a camera. To make a truly verifiable manual examination of a cell phone, record the process using a digital video camera running continuously from being to end of the process with no breaks, pause, or edits [8]. The video should begin before the phone is taken out of the secure evidence container and stop after the phone placed back into a secure evidence container. There are number of advantages and disadvantages to use this method.

The advantages of this method are that, it is easy to use; require no training to know how to acquire data from mobile phones. The main advantage of manual examination is it works with all phone models and does not require any driver, software, or cable to perform data acquisition [5]. The disadvantages of this method are that it does not extract deleted and hidden data; not preserve the integrity of the evidence; not work with physically damaged phone and password protected phones. The only data visible to the operating system can be recovered.

The Fernico ZRT tool is used to perform manual examination of cell phones [9]. As shown in Fig. 1, it consists of digital camera to takes photograph of the screen and merges those photos into custom designed report templates. It allows investigators to retrieve data from a mobile device when all other tools would not work.

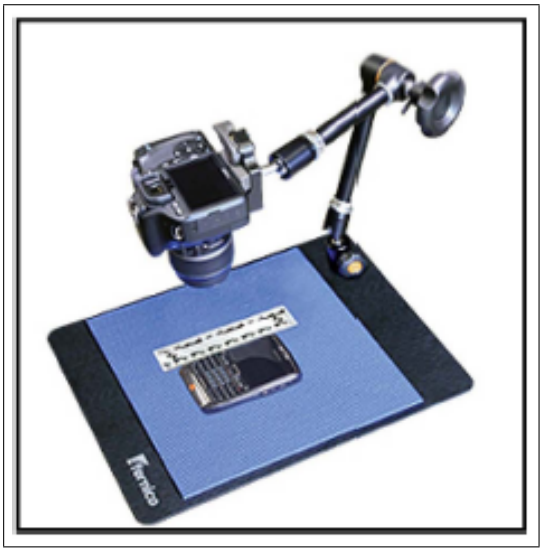

Figure 1: Fernico ZRT [5]

b) Logical Acquisition

Logical acquisition of cell phones are performed by implies a bit-by-bit copy of logical storage objects (e.g., directories and files) that reside in the logical partitions (e.g., a file system partition) of the mobile phone's memory [8]. Logical acquisition using forensics software to acquire data from cell phones and it is not able to recover data from deleted file or located outside of logical partitions, such as unallocated space. Data that can be recovered by using logical acquisition tools are text messages, contact list, and call history, but the images and ringtones are not. Logical acquisition is done by creating a connection between the cell phone and forensics investigator PC using Bluetooth connection, Infrared connection or a cable [9]. The set of AT commands can be used to extract potential evidence from mobile phones [5]. The list of standard AT command and their syntax are available in this reference [10].

There is much forensics software that using AT command to acquire data from mobile phones using logical acquisition such as TULP2G, Oxygen Phone manager, Paraben Cell Seizure [5].

There are number of advantages and disadvantages of logical acquisition. The advantage of logical acquisition has that system data structures are easier for a tool to extract and organize. The disadvantages of logical acquisition are such as the inability to retrieve deleted files; not work with physically damaged phone and password protected phones. When a logical acquisition of cell phones is performed, the phone returned to the custodian to which it belongs.

c) Physical Acquisition

Physical acquisition of cell phones are performed by implies bit-for-bit copying the entire physical memory (e.g. flash memory) of the phone memory chip [5]. Physical acquisition of cell phones method is most similar to the examination of personal computer. Physical acquisition acquires information from the cell phones by direct access to the flash memories. There is a three method to acquire data using physical acquisition [11].

Firstly, flasher tools, that can be used to copies flash memory data by performing lower level data acquisition. Low level data acquisition means independent of operating system [12], it directly acquire data from flasher memory. The flasher tools mostly used for debugging and diagnostics of a mobile phone by manufacturer [11][13][14]. There are several advantages and disadvantages of the flasher box. The advantages of flasher box are such as ability to retrieve deleted and hidden files; working with physically damaged and password protected mobile phones; acquire data from mobile phones that do not have a SIM card [5].

The disadvantages of flasher tool make its usage dangerous rather than useful. The disadvantages of flasher tool are such as the retrieved data has no data structure, make examination and analysis of retrieved data time consuming; not all mobile phones allow full data acquisition of memory chips [13][14].

Secondly, Joint Test Action Group (JTAG), created by a group of European electronics companies, is used to the

testing of small devices [5]. JTAG can acquire data from non-volatile memory and volatile memory [15]. All the data from physical memory can be acquired by connecting all JTAG pin hidden on the PCB with JTAG emulator. However, it is very difficult to search the entire JTAG pin. The JTAG enabled chip has the following pins [5]:

1. TCK (Test Clock)
2. TMS (Test Mode State)
3. TDI (Test Data In)
4. TDO (Test Data Out)
5. TRST (Test Reset

Investigator use JTAG interface to retrieve the content of memory chips and create a complete forensic images of these chips [15]. JTAG interface is shown in Fig. 2.

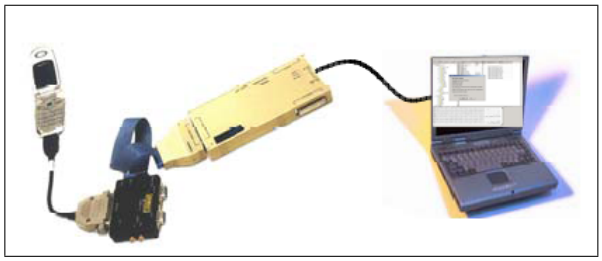

Figure 2: Memory dump using JTAG [24]

There are several advantages and disadvantages of JTAG method.
The advantages of JTAG are such as independent of the mobile phone operating system; create the forensics image of a mobile phone without de-soldering the memory chip [5].

The disadvantages of JTAG are such as it's difficult to find out the entire JTAG pin; not all mobile phones have a JTAG enabled chip; forensics image creating process is slow [5].

Thirdly, we can also acquire data from flasher memory by physically remove a flash memory from a board and read memory content with a memory chip reader. In case, when we cannot use a logical method or a JTAG method, this method is useful to acquire data from mobile phones [15].

d) Chip-off

Chip-off data acquisition method is used to get an image of the internal non-volatile memory [5]. To acquire data from internal non-volatile memory, firstly, de-soldering the non-volatile memory from printed circuit board (PCB). After de-soldering, the non-volatile memory from PCB, cleaning the pins of chip solder that has been left behind from the de-soldering stage. Finally, acquire data from chip by using a chip reader.

To de-soldering flash memory from a PCB, several methods are used depend on the pins out interface of the internal non-volatile memory. Micro Ball Grid Array (BGA) or Thin Small-Outline Package (TSOP) could be used as pins out interface for NAND flash memory [11].

The TSOP pin out chip is shown in Fig. 3.TSOP chips could be de-soldered from PCB by using hot air nozzle or de-soldering iron. The hot air nozzle is shown in Fig. 4.Hot air nozzle is used to de-soldering the TSOP chip from PCB by applying hot air in the edges of TSOP chip.

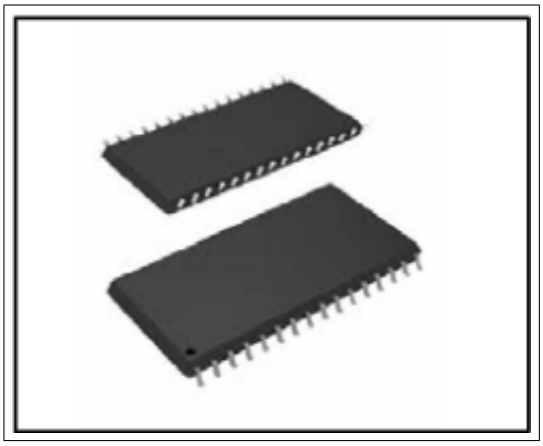

Figure 3: TSOP Chips [5]

Figure 4: Hot air nozzle [5]

The micro Ball Grid Array (BGA) pin out interface is more complicated than the Thin Small-Outline Package (TSOP). The BGA pin out interface is shown in Fig. 5. The BGA chip could be de-soldered by using BGA Rework Station. The BGA Rework Station is shown in Fig. 6. The BGA Rework Station using chip datasheet to applying the acceptable amount of heat in the pins of BGA chip [5].

After de-soldering the chips from PCB, contents of the chips could be read by using memory chip programmer. An example is PB 1600 memory chip programmer.

The chip-off acquisition has several numbers of advantages and disadvantages. The advantages of chip-off acquisition are such as it can work with any type of mobile phone (physically damaged or password protected) and retrieve deleted data. The major advantage of chip-off acquisition is that it preserves the integrity of acquired data. The disadvantage of chip-off

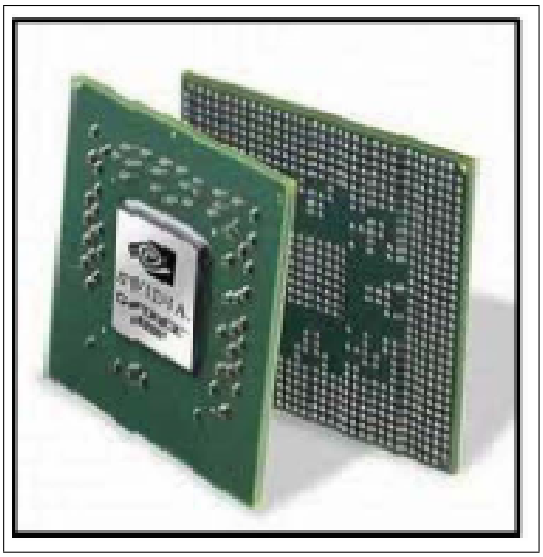

Figure 5: BGA Chips [5]

Figure 6: BGA Rework Station [5]

acquisition is that it can lose some of the evidence, due to the heat of de-soldering the memory may damage the chip. The major disadvantage of chip-off acquisition is that it does not return the mobile phone to its original state that some laws and legislation require.

IV. CONCLUSION

In this, we can provide a summary of the steps that need to be followed while performing the process of mobile forensics and a review of the current data acquisition methods which are manual, logical, physical and chip-off and focus on critical stages, preservation and acquisition, of mobile forensics process. We have also tried to aware the investigator about certain issues pertaining to data preservation and acquisition in mobile forensics and some possible solutions and advantages and disadvantages of each method of data acquisition.

References

[1] Billion mobile-cellular subscriptions. 2013.

[2] Global mobile statistics 2012 Part A: Mobile subscribers; handset market share; mobile operators. pages 918–926, 2012.

[3] S. Raghav and A.K.Saxena. Mobile Forensics: Guidelines and Challenges in Data Preservation and Acquisition. *Proceedings of 2009 IEEE Student Conference on Research and Development (SCOReD 2009)*, pages 16–18, 2009.

[4] W. Jansen and R. Ayers. Guidelines on Cell Phone Forensics. *NIST Special Publication*, page 101, 2007.

[5] Alghafli K.A., Ones A.J and Martin T.A. Forensics Data Acquisition Methods for Mobile Phones. *7th International Conference for Internet Technology and Secured Transactions, ICITST*, 2012.

[6] Wang G, Xu J.J, Chen H.Y and Lu Z.H. Amperometric hydrogen peroxide biosensor with solgel/chitosan network-like film as immobilization matrix. *Biosens, Bioelectron*, pages 335–343, 2003.

[7] Best Practices for seizing Electronic evidence. *USSS*, 2006.

[8] A. Zareen and S. Baig. Mobile Phone Forensics Challenges, Analysis and Tools Classification. *5th Int. Workshop on Systematic Approaches to Digital Forensics Engineering (SADFR)*, pages 47–55, 2010.

[9] Svein Y. Willassen. Forensic analysis of mobile phone internal memory. *Springer*, page 16, 2012.

[10] Brogan K.L and Walt D.R. AT COMMAND SET HILO 3G. *SAGEMCOM*, 2011.

[11] Marcel B., Martien de J, Coert K, Ronald van der K and Mark R. Forensic Data Recovery from Flash Memory. *Small Scale Digital Device Forensics Journal*, (1):1–17, 2007.

[12] K. Jonkers. The forensic use of mobile phone flasher boxes. *Digital Investigation*, (3):168–178, 2010.

[13] M. AI-Zarouni. Introduction to Mobile Phone Flasher Devices and Considerations tor their Use in Mobile Phone Forensics. *5th Australian Digital Forensics*, pages 143–153, 2007.

[14] M. F. Breeuwsma. Forensic imaging of embedded systems using JTAG (boundary-scan). *Digital Investigation*, (1), 2006.

[15] Keonwoo Kim, Dowon Hong, Kyoil Chung and Jae-Cheol Ryou. Data Acquisition from Cell Phone using Logical Approach. *World Academy of Science, Engineering and Technology*, 2007.

