

Notice of Violation of IEEE Publication Principles

"Mobile Phone Forensics: Challenges, Analysis and Tools Classification"

by Amjad Zareen, Shamim Baig

in the Proceedings of the 2010 International Workshop on Systematic Approaches to Digital Forensic Engineering, May 2010, pp. 47-55

After careful and considered review of the content and authorship of this paper by a duly constituted expert committee, this paper has been found to be in violation of IEEE's Publication Principles.

This paper contains significant portions of original text from the paper cited below. The original text was copied without attribution (including appropriate references to the original author(s) and/or paper title) and without permission.

Due to the nature of this violation, reasonable effort should be made to remove all past references to this paper, and future references should be made to the following article:

"Cell Phone and GPS Forensic Tool Classification System"

by Sam Brothers

in a presentation to Digital Forensics,

http://www.mobileforensicsworld.org/2009/presentations/MFW2009_BROTHERS_CellPhoneandGPSForensicToolClassificationSystem.pdf, May 2009

Mobile Phone Forensics Challenges, Analysis and Tools Classification

Amjad Zareen

Centre for Advance Studies in Engineering
Islamabad, Pakistan
amjad.zareen@yahoo.com,

Dr Shamim Baig

Centre for Advance Studies in Engineering
Islamabad, Pakistan
msbaig@case.edu.pk

Abstract— 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. Digital forensic specialists will require specialized tools for forensics examination of mobile phones for proper recovery and speedy analysis of data present on mobile phones. Based on the various extraction methods different levels of analysis can be logically grouped for evidence acquisition from mobile phones. Based on these levels (Manual, Logical, Hex-Dump, Chip-Off and Micro Read) a pyramid of forensic tools available in international market can be sketched. Scope of this paper is to excavate into challenges associated while carrying forensic analysis of mobile phones, elaborate various analysis techniques and depict a pyramid of forensic techniques and tools.

Keywords— Analysis, Evidence, Forensics, Messages, Mobile, Pyramid, SIM, Tools

I. INTRODUCTION

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. Mobile phones have the similar potential of holding evidence as any other digital media can. Phenomena of recovering deleted information from mobile phone is similar as it can be done for a hard drive [1]. 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. Non-forensic tools are less effective while the forensic tools provide widely varying results. A forensic examiner must be clear about what is acquired and how it is to be acquired.

II. EVIDENCE ITEMS AVAILABLE IN MOBILE PHONES

Mobile phones contain various evidence items which can be of interest for a Forensics Examiner. Sources of evidence in a Mobile phone may include: Subscriber Identity Module (SIM), Mobile Phone Internal Memory, Memory Cards and Network Service Providers. External memories for Mobile Phones may include SIM, SD, MMC, CF cards, and the Memory Stick. Memory cards are increasingly common in new handsets and exist in different physical “form factors” (e.g. MMC, microSD, MemoryStick Duo). These cards can have large storage (32GB cards are available) and usually PC-compatible FAT file system is adopted. Contents of these cards may include pictures, movies, MP3 or any file at all. The SIM and memory cards need a card reader to make a forensic copy. These must be carefully analyzed, as it is possible to recover (deleted) data like contacts or text messages. Significant amount of deleted data can be recovered from memory cards while using established computer forensic techniques and tools (like Encase, FTK etc) meant for Computer Forensics. This method involves normal data recovery procedures while considering Memory Card as an external storage media and their File System as FAT. Logical tools can recover live data from memory cards within handsets. But the phone never provides deleted files during a logical acquisition. Memory card needs to be accessed directly to retrieve deleted data. When a file is deleted from a FAT partition: the file’s directory entry is changed to show that the file is no longer needed and first character of filename is replaced with a ‘marker’. The file data itself is left unchanged which means that deleted files can be found (by reading directory entries). Large volumes of information are also available with Network Service Providers (Mobile Phone Operators). Additional items of evidence can also be found from these Network Operators which may include: Call Data Records CDRs, Messages Information, and Subscriber Information (including Name, Address, Number, National Identity etc). Law enforcement agencies at times also rely on application software to deal with large amount of data available with Network Operators. These software offer features like: finding criminal by backtracking mobile numbers from IMEI, graphical reports on usage and connection patterns of a particular target phone etc. Analysis of call data records and the corresponding tower-antenna pairs can also provide useful

TABLE- I
POSSIBLE EVIDENCE ITEMS ON MOBILE PHONE

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

information as evidence in a criminal trial. This type of analysis can only allow the investigator to be able to state that the call was placed from an area and not a single address or small geographical area. This information is suited to eliminate alibi locations [12]. Possible evidence items that can be found from modern day mobile phone while carrying forensic examination include those mentioned in the Table-I.

III. CHALLENGES ASSOCIATED WITH MOBILE PHONE FORENSICS

A. Mobile phone forensics is challenging field due to fast changes in technology. Several models of mobile phones exist in the world today. Manufacturers lack standardized methods of storing data. Most of the mobile phones use closed operating systems and has proprietary interfaces. To meet this challenge there is always a need for development of new forensics tools and techniques.

B. Signals of mobile phone need to be blocked while carrying forensics analysis. Blocking RF signals quickly drains the battery. This can be minimized while carrying forensics analysis of mobile phones in properly shielded labs. Shielding methods for lab include such as EMI/EMC protection.

C. Large variety of data cables exist for mobile phones. Identification and collection of cables required for forensics analysis of mobile phones is challenging task. Small databases for defining mobile phone models and their associated cables with tags can help a great deal.

D. 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.

E. Conflicts can occur due to different operating system, vendor and version specific device drivers. It is therefore recommended to have separate machines for each type of forensic software. However to economize resources Virtual Machine environments can be created.

F. Data on active mobile phone tends to change constantly due to lack of conventional write-blocking mechanism. Analysis must be done on a phone that is powered ON but it is ideal that the phone does not receive any calls, text messages, or other communications. Shielded labs can address this issue.

G. Most of the international trainings available in the field are vendor specific. There is need of for neutral and standard trainings.

H. Status of unopened emails and messages will change after reading them. Care must be taken while recoding such type of evidence.

J. 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.

K. Authentication mechanisms can confine access to data. Finding of Personal Identification Number (PIN), Phone Unlock Key (PUK), and handset and memory card passwords can become difficult at times.

L. Now days there are various methods available to remotely destroy or change data on a mobile phone. Such happening can be avoided in shielded lab environments while carrying forensic investigations. Care must also be taken to protect mobile phones while carrying them to labs.

- M. Data from mobile phone internal memory is restricted without the use of SIM card. Inserting another SIM can cause the loss of mobile phone data.
- N. Many commercial mobile phone forensic tools only provide logical acquisition of data. Deleted data can only be recovered using physical acquisition.
- O. Introduction of Mobile Number Portability (MNP) can result into improper identification of subscriber. Mobile Phone network operators may be consulted for proper identification.
- P. IMEI changing for few mobile handsets is possible with the use flashing tools like Universal Flasher UFS-3. This can result improper identification of phones. These illegal activities shall be banned.

IV. LEVELS OF ANALYSIS FOR DATA ACQUISITION FROM MOBILE PHONES

Methods for data acquisition from mobile phones mainly depend upon the condition, model, time and nature of the case. There is currently no standard method for analyzing mobile phone internal memory. Results obtained after forensic examination of mobile phones are different for different manufacturers. Each forensics extraction product does well in some areas and not so well in other areas. It is therefore recommended for forensic examiner to not focus on low hanging fruit. Methods that are currently used in the field of mobile phone forensics focus on extracting information by utilizing a cable, infrared or Bluetooth connection to the phone, and then extracting information by using the AT-command set which has been specified for communication with serial modems as per GSM specifications [8]. To aid investigators with information extraction, several software packages exist to perform this process. Cell-Seizure, TULP and Oxygen Phone Manager are examples of such software packages [9] [10] [11]. For complete Mobile Phone Forensic examination we need both Logical and Physical extractions. Logical extraction methods are quick, easy to use, reliable, 100% forensically secure and extract "all" data including contacts, calls, calendar, SMS, photos etc. While Physical extraction can create a "complete" memory image, extracts even deleted data (including system and network provider information like previous IMSI etc) , can retrieve data from devices where no SIM is present, bypass (and retrieve) handset security codes and is also useful for memory card analysis. The extracted data while carrying Physical extraction is in raw Hex-format and decoding of binary data is required. Using both logical and physical extractions give the investigators a better view. Physical tools can successfully be used to enable phones for logical extraction. Decoding of Physical data is hard as there are no standards in mobile phones. Based on the various extraction methods different levels of analysis can be logically made for evidence acquisition from mobile phones as shown in Figure-1.



Figure-1: Levels of Analysis

Manual Acquisition involves reviewing phone documentation and browsing manually using the keypad and display of mobile phone to document data present in the mobile phone. It is fast method, works on almost every phone, no cables are required and it is easy to use. However, it will not get all data, prone to errors, time consuming and will not recover deleted files.

Logical Acquisition involves access to the user files while connecting data cable to the handset and extracting data using AT commands using various software tools. It is a fast and easy to use method, supports foreign language, lot of information/research is available and reporting features are also available. However this method writes data to handset require lot of cables and does not provide access to deleted data.

Hex Dump Analysis involves physical acquisition of a mobile phone's file system. This type of extraction involves either a cable connection and specific software or removing chips from circuit board and "dumping" contents. Data is obtained in a "raw" form which requires interpretation. This method provides access to deleted data from mobile's internal memory (that has not been overwritten) and help extracting data hidden from handset menus. This is the fastest growing part in the Cell Phone Forensic Tools. Limitations of hex-dumping include: data conversion requirements, inconsistent report formats, came out of the hacker community, difficult to use, require custom cables, source code not available and restricted to specific manufacturers.

Chip-Off method involves the removal of a memory chip from mobile phone and read in either second phone or EEPROM reader to conduct forensic analysis. It is an expensive method and extracts ALL data from mobile phone memory. This gives better picture of what is going on holistically in the mobile phone. Data is not contiguous which is hard to interpret and convert.

Micro Read is a process that involves the use of a high-power microscope to provide a physical view of the electronic circuitry of mobile phone memory. This method can be used while acquiring data from physically damaged memory chips. This is an expensive method. It extracts and verify all data from mobile phone memory and is most forensically sound [12].

It is important for forensic examiner to try out more forensically sound levels before attempting lower levels of analysis. Methods mentioned at the top of pyramid in Figure-1 are more forensically sound, more technical, require more time for analysis, more expensive and require more training.

V. TOOLS CATEGORIZATION BASED ON LEVELS OF MOBILE PHONE FORENSICS ANALYSIS

The core objective of any Mobile Phone Forensic tool is to extract digital evidence. In addition, these tools also support examination and reporting functions. It is important for any forensic tool to preserve the integrity of acquired and extracted data. This is achieved by blocking and eliminating write requests to the device containing the data and calculating hashes of the evidence files. Mobile Phone Forensic tools can be placed in various levels as shown in Figure-2 corresponding to the levels of analysis (Figure-1).

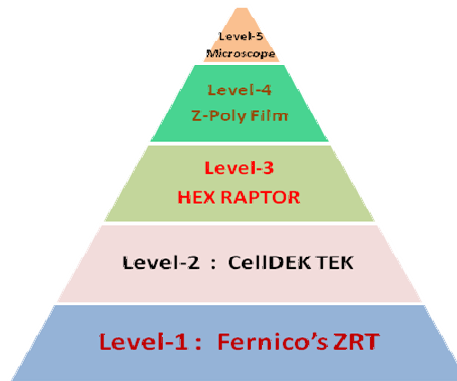


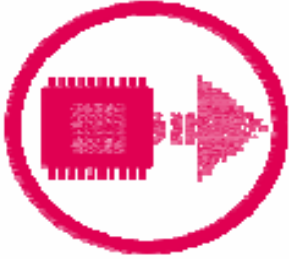
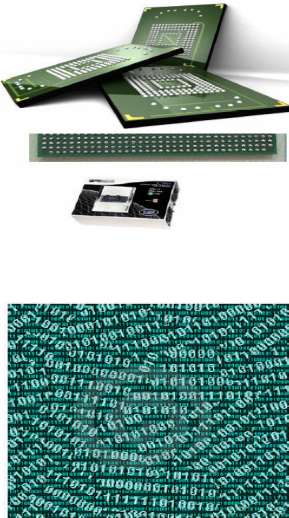



Figure-2: Tools Levels

Different tools / methods (with few distinctive features) used in the field of mobile phone forensics corresponding to each level of analysis corresponding Figure-2 are listed in Table-2.

TABLE-2
LEVELS AND TOOLS FOR MOBILE PHONE FORENSICS

Level-1	ZRT (Fernico)
Features: <ul style="list-style-type: none"> ▪ Rugged ▪ Works for every phone ▪ Also useful for other small pieces of evidence ▪ Includes microphone ▪ Shoots video ▪ Sometimes the only way ▪ Easiest for Jury to Understand 	
Level-2	CellDek TEK (Logicube)
Features: <ul style="list-style-type: none"> ▪ Cable Management ▪ Portable ▪ Includes Optional Laptop ▪ Instinctive Interface ▪ Report Creation ▪ Supports SIM Card Acquisition and Imaging ▪ iPhone Support ▪ Case Management ▪ Supports around 650 Phones 	

Level-3	HEX RAPTOR (FTS)
<p>Features:</p> <ul style="list-style-type: none"> ▪ Extract SIM card serial and IMSI up to last 8 SIM cards ▪ Finds handset security code ▪ Deleted data from mobile memory also possible ▪ XML Reporting Feature 	
Level-4	Chip Off
<p>Features:</p> <ul style="list-style-type: none"> ▪ Removing the Chip using Summit 1100 BGA Rework System ▪ Mounting the Chip using Fuji Poly W-Series Elastomeric Connectors ▪ Re-Balling (Depends on Luck!) ▪ Reading the Chip using BP Microsystems 1710 ▪ Translation of data ▪ Very costly and delicate and time consuming 	
Level-5	Electronic Microscope
<p>Features:</p> <ul style="list-style-type: none"> ▪ Use chemical process to remove top layer of chip ▪ Use microscope to read gates manually ▪ Translate binary to Hex ▪ Translate hex to Data ▪ Very costly and time consuming 	

VI. SUMMARY OF FINDINGS

- A. Significant amount of deleted data can be found from memory card (if available in handset) using traditional computer forensic tools.
- B. A mobile forensic tool namely HEX-RAPTOR by FTS (Forensic Telecommunication Services - UK) can analyze the dump of mobile phone memory which is locked using security code. Mobile phone security code can be read using this product [5].
- C. In some cases HEX-RAPTOR also recovers IMSI or SIM Serial Numbers of up to eight previously used SIM cards in mobile phone. This is unique feature and can give leading information to solve criminal cases.
- D. It is good to have variety of tools from different vendors and at different levels (Figure-2) in order to achieve maximum results from forensic examination.
- E. Rapidly introduced mobile phone models by different manufactures pose increased challenges and require introduction of new forensic tools and updates to existing solutions at the same pace.
- F. Forensic examination of mobile phones must start from forensically sound levels before attempting lower levels of analysis. Levels mentioned at the top of pyramid in Figure-1 are considered more forensically sound, more technical, require more time for analysis, more expensive and require more training.
- G. Application software with features like: backtracking mobile numbers from IMEI, graphical reporting on usage and connection patterns etc; can be of great help while dealing with huge amounts of data available with mobile phone operators and law enforcement agencies.

VII. CONCLUSION

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, however, beneficial for law enforcement, in the collection and preservation of valuable evidence. Levels of mobile phone forensic analysis include Manual, Logical, Hex-Dump, and Chip-Off and Micro Read. Based on these levels, mobile phone forensic tools can be categorized to form a pyramid (Figure-2). Levels and tools mentioned at the top of the pyramid are considered forensically sound, more technical, more expensive, require more time for analysis and require more training. Usage of higher levels of investigation not only requires very high degree of knowledge and competency from the forensic investigators but also demand a great deal of preparation, carefulness and a large amount of research and testing before the actual examination. In future mobile phones seem to be heading towards junction with other digital devices like MP3 players, GPS devices, Laptops, Personal Digital Assistants (PDA) and Digital Cameras. Thus more data will be available on such devices for forensic extraction. Variety of tools from different vendors and expertise on various levels of extraction will help forensic investigators a great deal to extract all possible evidentiary items available on these devices.

REFERENCES

[1]. Forensic analysis of mobile phone internal memory

Svein Y. Willassen

Norwegian University of Science and Technology

[2]. S. Willassen, Forensics and the GSM mobile telephone system,

International Journal on Digital Evidence 2003:2:1

[3]. Guidelines on Cell Phone Forensics

NIST Draft Special Publication 800-101

[4]. ACPO - Good Practice Guide for Computer Based Electronic Evidence

[5]. FTS - Forensic Telecommunication Services

<http://www.ForensicTS.com>

[6]. Mobile Phone Forensics Articles

<http://www.e-evidence.info/cellarticles.html>

[7]. RF Isolation

<http://mobileforensics.files.wordpress.com/2007/03/rfisolation.pdf>

[8] 3G Partnership Project, ETSI TS 300.642 – AT command set for GSM mobile equipment, Version 5.6.1, Oct 1998.

[9] Paraben Cell Seizure, Software Package, Available at:

<http://www.paraben.com/>

[10] Oxygen Phone Manager, Software Package, Available at:

<http://www.oxygensoftware.com/>

[11] TULP2G, Open Source Project, Available: <http://sourceforge.net/projects/tulp2g/>

[12] Provider Side Cell Phone Forensics

Terrence P. O'Connor

SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL, VOL. 3, NO. 1, JUNE 2009 ISSN# 1941-6164

[12] Design Principles for Tamper-Resistant Smartcard Processors”

<http://www.cl.cam.ac.uk/~mgk25/sc99-tamper.pdf>