Volume 6, Issue 2, February 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Comprehensive Analysis of Smartphone Forensics & Data Acquisitions

S Kumar Reddy Mallidi
Student (M.Tech), Dept of CSE
MVGR College of Engineering,
Andhra Pradesh, India

Parimala Palli
Assistant Professor, Dept of CSE
MVGR College of Engineering,
Andhra Pradesh, India

Abstract*−*Now a day's usages of smart mobile devices are growing vastly. This made them involved in many crimes and other incidents. Computer forensic investigators are in need of forensic tools specially designed for these smart phones for examination and recovery of the data presented inside the memory of the mobile devices. Mobile forensic tools divided into different levels based on the different acquisition methods performed on them. These levels are manual, logical, physical, Chip-Off, and Micro Read [1]. This paper discusses the two acquisition methods i.e. logical and physical acquisitions with the help of forensic tools that are available in the market and compares the results of these acquisition methods for three different smart phones that are used at feverish pace by consumers in the mobile market.

Keywords* − *Computer forensics, mobile forensics, smart phones, acquisition.

I. INTRODUCTION

According gartner report of 2013 on the usage of smart phones worldwide, statistics state that sales of smart phones according based on operating system Android occupies a share of 78.4%, iOS takes 15.6%, while other OS like Microsoft, Blackberry and others take 3.2%, 1.9% and 0.9% respectively [2].

Mobile phone forensics is the science of recovering digital evidence under forensically sound conditions. A forensic investigator can find evidence of interest in mobile phone storage locations such as Subscriber Identity Module (SIM), internal memory of mobile, external memory card and network service provider [3].

One of the deep-laid challenges presented to mobile forensic researchers in designing mobile forensics tool is maintaining capability in an environment of rapid development of technology. Smart mobile devices, for example, are can say as a combination of traditional mobiles and PDA devices, these smart phones more resemble personal computer rather than they do phones. Because of this they become particularly interesting for forensic examination as they contain voluble data that could make a forensic examination specialist interesting. Any way the methods used to extract the evidence from smart phones are somewhat different when compared with the extraction methods used for computer hard disk [4]. Smart mobile phones use different operating system, which are having their own file systems and file formats which are quite different when compared with traditional computers. And the methods they use to communicate were completely different. So extracting information from these devices creates unexceptional problems for investigators. So it is impossible to examine a smart phone with basic computer forensic tools, they requires unique tools specially designed for the mobile devices and having knowledge of the way these devices store data, the way these devices communicate and the possible evidence that present in them.

In previous days attackers and hackers used to invade servers and PCs presented in organizations without any purpose, just to have fun. Later they used to attack to destroy the important data of the organization with purposes like destroying competing organization. Later on they attacked to steal data from a PC or server, or to do their work. Due to increased use of these handheld devices, now the problem of hacking spread to these devices. Now a day's these devises were attacked by hackers, or used by hackers to hack other mobiles or computers. So there is a need of forensic tools for these devices along with having them for computers.

The rate of growth in the digital forensic tools available for mobile devices is very less compared to the growth of mobile technology. There exist two important factors to be considered in using mobile forensic tools, the device's state at the time of acquisition and radio isolation. An examiner can do static acquisition on a general computer after disconnecting it from the power source due to the data presented in non-volatile memory and it's also saves the current state of the computer. But this is not possible in mobile devices because the major evidence presents in volatile memory only, which can't be recovered once the device was switched off. And the other factors that makes only live acquisition possible in case of mobile devices was the locks or passwords that activated once the device was restarted. Another problem was the evolution of operating systems in mobile devices are fast, and different operating systems where presented which makes deployment of mobile forensic tools very difficult [5].

In this paper analyses the capabilities of the forensic tools accessible to examiners practicing in the area of mobile forensics, three mobile forensic tools which are known popularly were used to collect the data by performing both physical and logical acquisition.This paper explains how different mobile forensic collection and examination tools worked, how the data can be extracted from the smart phones using these tools.

II. EVIDENCE DATA PRESENT IN SMART PHONES

Multifarious data items are present in smart phones which can be used as evidence in many cases, which is of interest for a forensics practitioner or investigator. In a smart phone there was different evidence items were present, which include: SIM, phone's internal memory, external memory and data presented with network service providers. External memories in smart phone may include SIM memory and memory cards. Memory cards are available in many physical forms (e.g.: micro SD, MMC cards etc.). The storage capacity of current available cards is from 256 MB to 32 GB. File system adopted in these cards is FAT file system. The memory cards and SIM cards need memory card and SIM card readers to generate a forensic disk copy of these. Memory of these cards is non-volatile and if carefully examined we may extract deleted data also. The data items present in SIM are contacts, text messages, and call entries, data present in memory cards include images, videos, audios and different types of files. We can use normal computer forensic procedures and tools (like Prodiscover, Encase, Access data FTK etc) meant for Computer Forensics for examining these cards because they use FAT file system which was used by computers in floppy disks, pen drives etc. During logical acquisition we can recover live data from these memory cards within handsets. But we can't extract deleted data. We have to access memory card to extract deleted data by doing static acquisition. When a file is deleted in FAT file system, the file's directory entry in FAT table is changed and the memory provided for the file was available for new file. The previous file data itself is left unchanged until it is over written by other, which means we can acquire that deleted files from the cards.

We can collect huge information from network service providers. The evidence items that can be collected from service provider includes previous records, those may not be available in mobile devices. The data items that can be found from these service providers include call records, messages and Subscriber Information like name, address, IMEI number etc. Law enforcement officers use these data to find criminals with the help of application software that provide features like tracing back the mobile numbers using IMEI numbers. From the interpretation of call records and the corresponding antenna-tower pairs can also provide information which can be used as evidence in a criminal trial to verify alibi location of suspect [6].

III. LEVELS OF ANALYSIS METHODS

Methods used for data extraction from mobile devices phones depend mainly on the conditions like model, time, nature of the case and resources available.Methods used to extracting information from smart phones focuses on connecting the device to PC using cable, Bluetooth or infrared. After that data will be carved from the device's memory by using different ways. To support examiners for acquire information verity of tools available [7].

Based on the acquisition methods the analysis techniques are characterized in to different levels as shown in figure 1 [1].

Manual acquisition means viewing phone records and manually flipping through the display and keypad of mobile device to gather information available in the mobile device.

Logical acquisition means obtaining the user files by connecting phone and PC using data cable or Bluetooth and acquiring information using forensic tools available. It is a fast, easy and reliable method. And majority tools support many languages and features like reporting also available.

Physical acquisition also known as Hex-dump analysis involves static acquisition of a mobile device's file system. In this type of acquisition analysis is done by either connecting the mobile device using cable or removing cards from device and extracting data by copying total file system. Data obtained by this method is in raw format and must be converted to binary format which was done by the software tool we use.

Chip-Off method involves the analysis of memory by removal of a chip from mobile device and analyzing by either using identical phone or EEprom reader. This method extracts all data from mobile phone memory but expensive.

Micro Read is a method that involves the process of using a high-power electronic microscope to provide physical view of the gates inside the electronic chips of mobile device. This method can extract data from physically damaged chips also but is very expensive.

For complete forensic examination of a mobile device we need to extract the deleted data also, so to do that both logical acquisition and physical acquisition are needed.

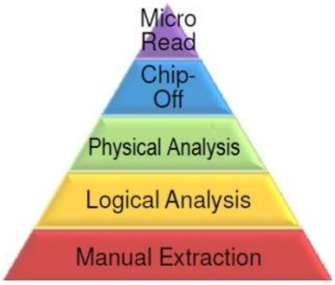

Fig . 1. Levels of analysis

Logical acquisition is fast, easy, reliable and forensically secure and extract all data from a smart phone like call logs, contacts, messages, calendar entries, videos, images etc. where as we can create complete image of the memory using physical acquisition. By using this we can extract even deleted data and even the SIM is not present, which is not possible using logical acquisition. We can bypass and extract passwords present in the device and also useful for external memory card examination. So in this paper used both physical and logical acquisitions

While there is availability of numerous smart phones, this paper studies the three main operating systems in which two are dominating in the market, namely Apple iOS, Android (Samsung galaxy S2). The third was Android (Micromax using Chinese MTK chipset) (see Table I). The main reason to select a Chinese mobile for study is according to recent information these Chinese mobiles are widely using in many crimes.

And the study was done using three of the popular mobile forensic tools that can do both physical and logical acquisitions. These tools are widely used by forensic investigators and practitioners globally. The three tools selected were mentioned as Tool-A, Tool-B and Tool-C (the names of these tools has not been mentioned to avoid being seen as supporting commercial interests, however details can be provided upon request).

IV. EXAMINATION BENCH SETUP

Smart mobile devices

The three phones selected for this study, based upon the popularity of their operating systems—Apple iPhone 4, Samsung galaxy S2 and Micromax canvas 2 (see Table I). At the time analysis their operating systems were not very latest versions, the main reason for this was mobile forensic tools take some time to certified as efficient tool for analyzing latest versions of operating systems and so, it was considered wise to use smart phones with older operating systems that will be supported with the selected mobile forensics tools.

TABLE I. SPECIFICATIONS OF SMART PHONES

Mobile device	**iPhone 4 16GB Black GSM**	**Samsung galaxy S2**	**Micromax canvas 2**
Manufacturer	Apple	Samsung Electronics	Micromax
Operating system	iOS 5.1	Android 4.0.3 (Ice Cream Sandwich)	Android 4.0.3 (Ice Cream Sandwich)
RAM	512MB	1GB	512MB
Internal memory	16GB	16GB	2GB
External memory card	None	microSD (4GB)	microSD (4GB)
Chipset	Apple A4	Qualcomm S3-APQ8060 Snapdragon	MTK MT6577
CPU	1 GHz Cortex-A8	Dual-core 1.2 GHz Scorpion	Dual-core 1 GHz Cortex-A9

To guarantee the results of this study was satisfying and as similar as possible to real world examination. Prior to the study of these selected phones they were used by real users, which makes it valuable when comparing it with only setting upthe phones with experimental data, as it allowed detection of anomalies within high range of data that would otherwise will not be detected.

Personal computer environment

All forensic tools used to study need a PC for examining or analyzing the reports. To make sure that no errors or conflicts were present in the results of the tools, all three forensic tools were installed on three individual PCs of identical configuration that can supported by three selected forensic tools. The configurations of the computers used in this examination are as follows:

CPU: Intel® Core i3-4005U 2.4GHz
RAM: 4GB
OS: Windows 7 Professional SP1 32bit
GPU: NVIDIA GeForce GT 240M 512MB
HDD: 500GB @ 7200rpm

V. TOOL-ANALYSIS

The three selected mobile forensic tools Tool-A, Tool-B and Tool-C. All three tools are able to perform logical and physical acquisitions on all three selected smart phones. Logical acquisition means the ability to copy the logical storage objects of the smart phone (e.g. contacts, call logs and files etc. [8]). Logical acquisition on all three smart phones is done by using manufacturer's interface with the help of data cable, which is generally used for synchronizing the phone with a PC. This acquisition method usually doesn't extract any deleted data because in this acquisition copying or extraction is done file-by-file not bit-by-bit. Physical acquisition means the ability to do copy of the whole physical storage bit-by-bit, which enables the forensic tools to extract deleted data which wasn't over written [8]. However, this analysis needs direct access to the smart phone's file system. Then only the tool was able to extract the deleted information from the memory using procedures such as carving. In this method particular file headers types of interest are searched and extracted. Carving is a generally used procedure in computer forensics to filter a huge data set [9].

Before starting the forensic examination it is needed to define the types of data items that are to be collected from physical and logical acquisitions, and can be presented as evidences. By reviewing each forensic tool's output data types available, a common set of data types has been selected. The selected data types are contacts, call logs, messages (SMS and MMS), E-mails, calendar events, bookmarks, browsing history, images, videos and audios. The entries of these data types were extracted and reported. From the examination a variation is noted in between the results of the three mobile forensic tools.

VI. EXPERIMENTAL FINDINGS

The number of entries extracted by using the three selected mobile forensic tools from the three mobile devices was showed in the tables 2-7. The figures in parentheses represent the number of deleted items.

Contacts

The reports of contact entries shows variations between the three forensic tools in case of Android devices (Samsung and Micromax), the entries that reported are combined entries of data from multiple origins (see Table II). The iPhone results are similar for all three tools. In physical extraction Tool-A and Tool-B produced similar results for both iPhone and Samsung, and extracted deleted entries also. But physical extraction of Micromax phone was not supported because the tools are not yet upgraded to access MTK chipset used in majority Chinese mobiles.

The huge differences in the Android acquired results are due to the multiple data origins for contacts which includes records of Facebook and Google accounts. The tools handled these entries in different ways. Some were merged by some tools and some were not able to extract.

Call history

During logical acquisition all three tools were successfully acquired call history entries from all three mobile devices (Table III). The data reported entries were similar in all cases. Physical acquisition also produced almost similar results for both Tool-A and Tool-B and deleted also extracted. Tool-B reported duplicate entries also which are eliminated by Tool-A (Table III).

Messages (SMS/MMS)

During the logical acquisition the Android's SMS/MMS message entries were extracted successfully, and were similar for all three tools. The iPhone entries showed a variation in the entries. Further investigation finds out that this was due to the huge and various types of messages in the device. Tool-A and Tool-C shows similar results where as Tool-B shows less number of entries, because Tool-B's capacity is limited to 30,000 non-file records in logical mode.

Unexpectedly during logical acquisition Tool-A recovered 2,316 deleted messages from the iPhone. This is because the SQLITE database in iPhone keeps the deleted messages until a cleaning process is run. This is known as garbage process which was normally run on demand or when a database is ideal for performance reasons.

During physical acquisition both Tool-A and Tool-B acquired same results and extracted 2,136 deleted messages in case of iPhone, where as 356 deleted entries in case of Samsung galaxy (Table IV).

TABLE II. CONTACTS ACQUISITION REPORT

Mobile Device	**Logical Acquisition**			**Physical Acquisition**		
	Tool A	***Tool B***	***Tool C***	***Tool A***	***Tool B***	***Tool C***
Apple iphone	75	77	75	122(27)	137(27)	Not Supported
Samsung Galaxy S2	256	192	156	273(17)	298(17)	
Micromax canvas 2	193	126	93	Not Supported		

TABLE III. CALL HISTORY ACQUISITION REPORT

Mobile Device	**Logical Acquisition**			**Physical Acquisition**		
	Tool A	***Tool B***	***Tool C***	***Tool A***	***Tool B***	***Tool C***
Apple iphone	98	98	98	73(6)	73(1)	Not Supported
Samsung Galaxy S2	133	133	133	0	0	
Micromax canvas 2	65	65	65	Not Supported		

TABLE IV. MESSAGES (SMS/MMS) ACQUISITION REPORT

Mobile Device	**Logical Acquisition**			**Physical Acquisition**		
	Tool A	***Tool B***	***Tool C***	***Tool A***	***Tool B***	***Tool C***
Apple iphone	42,326(2,316)	30,000	42,326	42,326(2,316)	42,326(2,316)	Not Supported
Samsung Galaxy S2	2,043	2,043	2,043	2,043(356)	2,043(356)	
Micromax canvas 2	356	356	356	Not Supported		

TABLE V. E-MAIL ACQUISITION REPORT

Mobile Device	**Logical Acquisition**			**Physical Acquisition**		
	Tool A	***Tool B***	***Tool C***	***Tool A***	***Tool B***	***Tool C***
Apple iphone	289	Not Supported	Not Supported	289(39)	289(7)	Not Supported
Samsung Galaxy S2	114			114(15)	114(13)	
Micromax canvas 2	165			Not Supported		

Email

Email data acquisition was not supported by Tool-B and Tool-C on the three smart phones being tested. For both logical acquisition and physical acquisitions, only Tool-A was able to extract emails from all three phones. This was because Tool-B and Tool-C unable to perform jailbreak or root the devices. A jailbreak is a process that bypasses software security to allow privileged code to execute on the device without any approval from the manufacturer[10], and was not used and neither was a root (a process that permits forensic software to bypass standard security restrictions and gain 'root' privileges [11])on any devices by Tool-B and Tool-C as part of this study.

Physical acquisitions performed better than logical acquisition. Tool B was able to extract email entries (undeleted and deleted) from two of the devices tested iPhone and Samsung.

Calendar entries

Calendar entries were successfully recovered and reported by all three selected tools. There exists a small variation between the tools, Tool-A reported more entries in both physical and logical acquisitions. For example Tool-A done logical acquisition on Samsung, this extracted Facebook calendar entries also (Table VI). This indicates that all Facebook calendar entries were not been included in Tool-B and Tool-C's acquisition reports. Compared to Tool-B, Tool A was able to extract more deleted calendar entries from both iPhone and Samsung as part of its physical acquisition.

Bookmarks & Web history

Bookmark and web history entries extracted by all three tools during logical acquisition were similar. In case of Micromax there is a small variation that is Tool-C extracted 5 cache history entries also (see Table VI indicated with *). But during physical extraction Tool-A is able to extract more entries while extracting web history. This is because during physical acquisition Tool-A was able to extract entries from YouTube application also. During physical extraction both Tool-A and Tool-B gave similar reports (Table VI).

Media files

During logical acquisition Tool-B and Tool-C reported similar results in case of media files which includes images, videos and audio. But Tool-A was able to extract more number of files compared to other, because Tool-A extracts media files by comparing the file headers with known file headers which enables it to extract unknown file formats also. This feature was not available in Tool-B and Tool-C.

In case of physical acquisition more number of media files was reported than logical acquisition because during logical acquisition physical access to external memory was not possible. Tool-A was able to extract more deleted files than Tool-B, for example in case of Samsung Tool-A reported 1,564 images where Tool-B was able to extract only 968 images.

Physical acquisition

Physical acquisition was well supported by Tool-A and Tool-B for both iPhone and Samsung mobiles, where as Tool-c was unable to do physical acquisition for any of the selected devices. And in case of Micromax physical extraction was not supported by any of the tools because the tools are not yet designed to support mobile devices using the Chinese MTK chipset. Due to this physical acquisition of Micromax canvas 2 was not possible since it was using MTK chipset.

TABLE VI. CALENDAR, BOOKMARKS AND WEB HISTORY ACQUISITION RESULTS

Data Item	**Mobile Device**	**Logical Acquisition**			**Physical Acquisition**		
		Tool A	***Tool B***	***Tool C***	***Tool A***	***Tool B***	***Tool C***
CALENDAR ENTRIES	Apple iphone	17	9	9	17(7)	9(4)	Not Supported
	Samsung Galaxy S2	103	89	89	103(15)	89(10)	
	Micromax canvas 2	14	7	7	Not Supported		
BOOK MARKS	Apple iphone	22	22	22	22	22	Not Supported
	Samsung Galaxy S2	14	14	14	14	14	
	Micromax canvas 2	2	2	2	Not Supported		
WEB HISTORY	Apple iphone	15	15	15	40	15	Not Supported
	Samsung Galaxy S2	198	198	198	245(34)	238(28)	
	Micromax canvas 2	1	1	6*	Not Supported		

TABLE VII. MEDIA FILES ACQUISITION REPORT

Data Item	**Mobile Device**	**Logical Acquisition**			**Physical Acquisition**		
		Tool A	***Tool B***	***Tool C***	***Tool A***	***Tool B***	***Tool C***
IMAGES	Apple iphone	1,328	870	870	1,883(28)	1,265(14)	Not Supported
	Samsung Galaxy S2	2,578	2,146	2,146	9,935(1,564)	8,482(968)	
	Micromax canvas 2	468	468	468	Not Supported		
VIDEOS	Apple iphone	23	23	23	38	38	Not Supported
	Samsung Galaxy S2	11	8	8	22(14)	22(10)	
	Micromax canvas 2	3	3	3	Not Supported		
AUDIOS	Apple iphone	0	0	0	(23)	(19)	Not Supported
	Samsung Galaxy S2	200	46	46	78	78	
	Micromax canvas 2	31	31	31	Not Supported		

VII. CONCLUSION

The aim of this study was to gain knowledge and to understand how data can be extracted from smart phones using both logical and physical acquisition methods. And to understand the capabilities of three popular and well known mobile forensic tools in examining and acquiring data from smart phones which were using latest operating systems that were the dominating in the world wide market. By comparing the finding it was concluded that one must not depend entirely on single mobile forensic tool to acquire and to present all potential evidence from a smart phone.

From this study, new and advanced features as well as limitations of mobile forensic tools were found. One of the more advanced features some tools provided included extracting deleted messages from a logical acquisition, identifying and extracting unknown files that are files having non-standard extension by comparing their header formats, extracting data from multiple sources and collection of web history beyond the browser. Limitations of some tools are like unable to extract emails from some devices during logical acquisition which is due to the need to 'root' a phone, some tools extract duplicate entries also, some tools can't perform physical acquisitions and physical acquisition on mobiles featured with MTK chipset was not supported by any of the tool. These limitations are not handled successfully and it was assumed that majority of these limitations will be over come as the mobile forensic tools updated and upgraded. Because of the number of different smart phones emerging into the market, it is impossible that every mobile forensic tool will have the ability to examine all smart phones as demonstrated in this paper.

It should be considered that when using these tools for analyzing smart phones that uses OS designed by different vendors, examination results may vary (e.g. Android). Vendors generally customize their implementation of the OS regularly, which may result in storing the information in various locations when compared to standard OS.

To extract the maximum data successfully from a smart phone, forensic examiners and investigators need be aware new and advanced features and limitations of the tools available and particularly tool they are using. This will make them to wisely select their tool of interest in a case where heavy workloads are present and where timeliness is critical. It is better to perform examination with multiple tools so each and every data item will be extracted.

REFERENCE

[1] "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.

[2] Janessa Rivera Gartner & Rob van der Meulen Gartner 2014, http://www.gartner.com/newsroom/id/2665715.

[3] McKemmish R 2008. When is digital evidence forensically sound. *Advances in Digital Forensics* IV(285): 3–15.

[4] Jansen WA, Delaitre A & Moenner L 2008. Overcoming impediments to cell phone forensics, in *Proceedings of the 41st Annual Hawaii International Conference on System Sciences*: 7–10 January 2008: 483–483

[5] Mobile device forensics: A snapshot by Christopher Tassone, Ben Martini, Kim-Kwang Raymond Choo and Jill Slay, Trends & issues in crime and criminal justice, No. 460, Aug 2013.

[6] Provider Side Cell Phone Forensics, Terrence P. O’Connor, Small scale digital device forensics, VOL. 3, NO.1, JUNE 2009 ISSN# 1941-6164.

[7] 3G Partnership Project, ETSI TS 300.642 – AT command set for GSM mobile equipment, Version 5.6.1, Oct 1998.

[8] Grispos G, Storer T & Glisson W 2011. A comparison of forensic evidence recovery techniques for a windows mobile smart phone. *Digital Investigation* 8(1): 23–36.

[9] DFRWS 2006. *DFRWS 2006 forensics challenge overview*. http://www.dfrws.org/2006/challenge/.

[10] Obaidli HA, Iqbal A & Iqbal B 2012. A novel method of iDevice (iPhone, iPad, iPod) forensics without jailbreaking, in *Proceedings of 2012 International Conference on Innovations in Information Technology* (IIT): 18–20 March 2012: 238–243

[11] Christin N, Vidas T & Zhang C 2011. Toward a general collection methodology for android devices. *Digital Investigation* 8(Supplement): S14–S24