[Issue,1(1):29July,2013]

ISSN: 2321-8134

IJFEAT

INTERNATIONAL JOURNAL FOR ENGINEERING APPLICATIONS AND TECHNOLOGY

Mobile Forensics – A Literarure Review

Namrata R. Agrawal[*1], Sapna S. Panjwani[2], Ashish K. Sharma[3], Sangita S. Sharma

[*1]*Asst. Prof., Manoharbhai Patel Institute of Engineering and Technology (MIET), Gondia, Maharashtra, India,*

tonamrataagrawal@gmail.com

[2]*Asst. Prof., Manoharbhai Patel Institute of Engineering and Technology (MIET), Gondia, Maharashtra, India,*
sapna.ss95@gmail.com

[3]*Asst. Prof., Manoharbhai Patel Institute of Engineering and Technology (MIET), Gondia, Maharashtra, India,*
ash5000@rediffmail.com

[4]*Asst. Prof., Manoharbhai Patel Institute of Engineering and Technology (MIET), Gondia, Maharashtra, India,*
sangitaasharma1975@gmail.com

Abstract

Mobile forensics is the buzzword in the present era of "the Information Age". With mobile phones now transformed into Smartphone's, are ubiquitously used of late. Over the years, there has been an exponential rise in the use of mobile phones. But at the same time, there has been considerable rise in the use of mobile phones in committing crime. The newer mobile phones are equipped with numerous functionalities and thus contain the wealth of information which can be acquired from them. These mobile phones contain nuggets of data which could act as potential evidence in crime investigation. Thus, the mobile phones have become goldmines for forensic investigators. Albeit a lot of work has been done in this area but still it acts as a fertile area for new researchers. Moreover, there is a dearth of suitable and well-organized literature material so as to assist the researchers and practitioners in this area. Thus, this paper aims to create a data bank to facilitate the referencing needs of researchers and practitioners. To this end, this paper presents the literature review pertaining to this topic. The literature review is based on the data collected from various research papers, tools and web sources that will strongly assist in easy referencing.

Index Terms: *Mobile forensics.*

1. INTRODUCTION

The digital forensic field is very vast. It includes operating system forensics, network forensics, web forensics, mobile forensics etc. The need for mobile forensics arises from increasing number of mobile crimes that are committed annually. Mobile forensics is used to bring the justice, those responsible for crime using smart phones. The rapid technological advancements and increasing popularity of mobile devices pose great challenges for investigators and law enforcement officials all over the world (Yadav, 2011). The continued growth of the mobile device market, the possibility of their use in criminal activity will only continue to increase. The mobile device market provides many manufactures and models causing a strong diversity. Due to such features and facilities, people will more depend on application such as SMS, MMS, Internet Access, Online Transactions etc. There are many tools and techniques available to identify and investigate the crimes done with the help of mobiles or computers. So, it becomes difficult for a professional investigator to choose the proper forensics tools for seizing

ISSN: 2321-8134

internal data from mobile devices. Such mobile device also provides a good source of evidence for forensic investigators to prove or disprove the commitment of crimes of victims. (Daware and Thakare, 2012) Forensic Science is the use of forensic techniques and values to provide evidence to legal or related investigations Mobile phone forensic analysis is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods. The phone no longer simply connects us vocally with another, instead it stores our activities, dates, private numbers, experiences – written, visual or audio-visual; and it allows access to the internet where we send private and public messages. We no longer laugh, cry and love face to face; instead, all is recorded on our 'Smartphone'. As we transfer our experiences from the active, interpersonal world, to the digital; nothing remains private. Whispered conversations, clandestine notes, and mental images are transferred and recorded by phone instead. Although it may defy the ICT novice, deletion has never really meant deletion. Forensic investigators commonly start with phone numbers dialed, answered, received or missed; stored phone numbers of people whom the mobile phone user may know and text messages sent, received or deleted (Punja, 2008). Mobile phone capabilities increase in performance, storage capacity and multimedia functionality turning phones into data reservoirs that can hold a broad range of personal information. From an investigative perspective, digital evidence recovered from a cell phone can provide a wealth of information about the user, and each technical advance in capabilities offers greater opportunity for recovery of additional information .Mobile phone forensics is a challenge as there is yet no de facto mobile phone operating system, Mobile phone forensic analysis involves either manual or automatic extraction of data to be carried out by the mobile phone forensic examiners. Automatic extraction is used when the device is compatible with one or more pieces of forensic software and manual extraction is necessary when no compatible software is present. Automatic reading of a SIM Card is used when the mobile phone is supported by one or more pieces of forensic software. A manual verification is then required to confirm the extracted data is complete and correct. Manual reading of SIM card is used when the mobile phone is not supported by any forensic software, or the support offered is limited to such a degree that very little data is capable of being extracted. This method of analysis requires a forensics examiner to manually traverse a handset and digitally record each of the screens. This will include the recording of audio and videos in a format playable by the OIC. All images taken will be produced as a paper based report. Forensic analysis of a mobile device using either manual or automatic techniques can produce some or all of the following data: Make and model of the mobile handset; Mobile Station International Subscriber Directory Number (MSISDN) (Kevin, Andrew, Stephen and Cassidy, 2010). Albeit a lot of work has been done in this area but still it acts as a fertile area for new researchers. This paper aims to create a data bank to facilitate the referencing needs of researchers and practitioners in this area. To this end, this paper presents the literature review pertaining to this topic. The literature review is based on the data collected from various research papers, tools and web sources that will strongly assist in easy referencing

2. LITERATURE REVIEW

Digital forensic is an important part of computer investigation to recovering of data. Recent technological advances in mobile phones and the development of smart phones have led to increased use and dependence on the mobile phones. The explosion of its use has led to problems such as fraud, criminal use and identity theft which have led to the need for mobile phone forensic analysis. It has been a widely used area over the years and still it leaves a lot to be researched. (Al-Zarouni, 2007) has discussed mobile phone flasher devices and considerations for their use in mobile phone forensics. (Baggili, Richar and Rogers, 2007) has discussed a database

ISSN: 2321-8134

driven approach that could be used to store data about the mobile phone evidence acquisition testing process. This data can then be used to calculate tool error rates, which can be published and used to validate or invalidate the mobile phone acquisition tools. (Ahmed, Dharaskar) have highlighted the nature of some of the newer pieces of information that can become potential evidence on mobile phones and some of the emerging technologies and their potential impact on mobile phone based evidence and also cover some of the inherent differences between mobile phone forensics and computer forensics, some of the weaknesses of mobile forensic toolkits and procedures and shows the need for more in depth examination of mobile phone evidence.(Thing , Kian-Yon and Chang, 2010) have proposed an automated system to perform a live memory forensic analysis for mobile phones an investigated the dynamic behavior of the mobile phone's volatile memory, and the analysis is useful in real-time evidence acquisition analysis of communication based applications.(Adelstein, 2003) have created a Platform (MFP) for performing remote network forensics. With it, investigators can gather evidence on a remote running system, maintain a copy of the original evidence (protected by a cryptographic hash), and run various analyses on the data to determine the next steps in the investigation, how the MPF supports a small set of analysis tools that illustrate the potential of the MFP. In particular, he created 3 sample logfile analysis tools. They detect if the data in a log file has been tampered, and also served to define how the analysis tools fit into the overall MFP framework. (Mutawa, Baggili and Marrington , 2012) focuses on conducting forensic analyses on three widely used social networking applications on smart phones: Facebook, Twitter, and MySpace. The tests were conducted on three popular smartphones: BlackBerrys, iPhones, and Android phones. The tests consisted of installing the social networking applications on each device, conducting common user activities through each application, acquiring a forensically sound logical image of each device, and performing manual forensic analysis on each acquired logical image. The forensic analyses were aimed at determining whether activities conducted through these applications were stored on the device's internal memory. (Kubi, Shahzad and Oliver) have created Some Tools for Extracting e-Evidence from Mobile Devices and also evaluated UFED Physical Pro 1.1.3.8 and XRY 5.0 following "Smartphone Tool Specifications Standard" developed by NIST, in order to start developing a framework for evaluating and referencing the "goodness" of the mobile forensic tools.(Kevin, Andrew, Stephen and Cassidy,2010) has explained how recent technological advances in mobile phones and the development of smart phones has led to increased use and dependence on the mobile phone and discusses mobile phone forensic analysis, what it means, who avails of it and the software tools used.(Jansen, Ayers R, 2006) have provided forensic software tools for cell phone subscriber identity module. (Thakur, Chourasia and Singh, 2012) aims at acquiring and analyzing data in the cellular phone, which is similar to computer forensics and explains the basics of the GSM system. Evidence items that can be obtained from the Mobile Equipment, the SIM and the core network are explored. (Zareen and Dr Shamim Baig, may 2010) has documented mobile phone forensics challenges, analysis and tools classification 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.(Shivankar and Saxena,2009) given a brief introduction to the various stages in mobile forensics and focus on the critical stages of preservation and acquisition of digital evidence from mobile phones to be used as evidence in criminal or civil cases with a step by step guide to perform the two critical processes and discusses issues which might come up while performing them.(Willassen) has presented two different methods of physical imaging of mobile phone memory units. The methods are applied to several popular modern mobile phones, and it is shown that the methods can

ISSN: 2321-8134

be utilized in practice to recover important evidence such as deleted text messages. (Paul McCarthy, 2005) provided an overview of the methods commonly used to acquire data from mobile phones in a forensic manner and discussed limitations and issues inherent in software based data acquisition, as is the legal admissibility of information acquired using these methods. By doing so, the need to verify the methods currently in use is highlighted.(Maynard Yates II) have given a comprehensive perspective of each popular digital forensic tool and offer an inside view for investigators to choose their free sources or commercial tools. (Bhadsavle and Wang, 2009) research in creating a baseline for testing forensic tools. This research was accomplished by populating test data onto a cell phone (either manually or with an Identity Module Programmer) and then various tools effectiveness will be determined by the percentage of that test data retrieved. (Danker ,Ayers and Mislan, June2009) has focused on hashing techniques for mobile device forensics and research has been conducted on the hash values calculated for mobile device data objects.(Akkaladevi, Keesara and Luo) presented an overview of forensic tools and discuss the challenges involved in the design of forensic tools with the steps needed to develop better toolkits in the digital forensic world. (Fiorillo, 2009) has introduced flash memory forensics with a special focus on completeness of evidence acquired from mobile phones and the particular nature of non-volatile memories present in nowadays mobile phones; how they really work and which challenges they pose to forensic investigators along with an advanced test in which some brand new flash memories have been used to hide data in man-made bad blocks: the aim is to verify if forensic software tools are able to acquire data fromsuch blocks, and to evaluate the possibility to hide data at analysts eyes. (Jansen, Delaitre, Moenner , 2008) has highlighted overcoming impediments to cell phone forensics. (Ramabhadran) has described the various processes involved in the forensic investigation of Windows mobile devices in the form of a twelve-stage model.(Daware and Thakare, 2012) have given an overview of digital forensic process and tools and also the comparison between computer and mobile forensics. Each popular digital forensic tool and offer an inside view for investigators to choose their free sources or commercial tools. Also they have focused on the area and applications of digital forensics. (NIST, 2007) has described cell phone forensic tools: an overview and analysis update. (Paul McCarthy, 2005) in his thesis give an overview on forensic analysis of mobile phones. (Wayne Jansen, Rick Ayers, 2006) has presented forensic software tools for cell phone subscriber identity modules. (Simon and Slay, 2009) gave a solid foundation by explaining enhancement of forensic computing investigations through memory forensic techniques. (Bhadsavle and Wang, 2008) validating tools for cell phone forensics. (Al Zarouni, 2006) has discuss about mobile handset forensic evidence is a challenge for law enforcement.

CONCLUSION

Today mobile phones have become an essential commodity for everyone. With the advent of Smartphone's, there has been a considerable rise in the use of mobile phones. However, the explosion of its use has led to problems such as fraud, criminal use and identity theft which have led to the need for mobile phone forensic analysis. Mobile phones act as a significant resource for forensic analysis which in turn will help the examiner in crime investigation. Mobile forensics is used to extract potential evidences from the mobiles involved in criminal activity. Even though a lot of work have been done in this area but still it acts as a fertile area for new researchers. Thus, this paper makes an attempt to present the literature review in an organized manner covering various aspects of mobile forensic analysis. The literature review is based on the data collected from various publications, books, tools and web sources. It has been realized from the study that even though the field has been researched a lot so far, but still it acts as a fruitful area for new researchers as it is very vast. It is

ISSN: 2321-8134

anticipated that this paper will facilitate the reference needs of researchers and practitioners and hence will encourage research in this area.

REFERENCES

[1]. Baggili I, Richard M and Rogers M. "Mobile Phone Forensics Tool Testing: A Database Driven Approach" Issues in *International Journal of Digital Evidence* Fall 2007, Volume 6, No. 2 p.

[2]. Yadav S. "Analysis of Digital Forensic and Investigation". *VSRD-IJCSIT*, Vol. 1 (3), 2011, 171-178p.

[3]. Ahmed R and Dharaskar RV, "Mobile Forensics: an Overview, Tools, Future trends and Challenges from Law Enforcement perspective".

[4]. Ahmed R and Dharaskar RV. "Mobile Forensics: the roadblocks ahead, proposed solutions using Protocol Filtering and SIM programming". *International Journal of Computer Science and Applications* Vol. 2, No. 2p, November / December 2009.

[5]. Vrizlynn L. L. Thing , Kian-Yong Ng and Ee-Chien Chang , "Live memory forensics of mobile phones" digital investigation (2 0 1 0) S 7 4 eS82 .

[6]. Adelstein F. " MFP: The Mobile Forensic Platform" . *International Journal of Digital Evidence* Spring 2003, Volume 2, No 1p.

[7]. Al Mutawa, Baggili I, and Marrington A. "Forensic analysis of social networking applications on mobile devices" . *Digital Investigation* 9 (2012) S24–S33.

[8]. Kubi A , Shahzad S and Oliver P. " Evaluation of Some Tools for Extracting e-Evidence from Mobile Devices" .

[9]. Kevin C, Andrew R, Stephen P and Sean C. "Mobile Phone Forensic Analysis". *International Journal of Digital Crime and Forensics*, Vol. 2, No. 2 p, April-May 2010.

[10]. Thakur R, Chourasia K and Singh B. "Cellular Phone Forensics" . *International Journal of Scientific and Research Publications*, Volume 2, NO.8, August 2012.

[11]. Amjad Z and Dr Shamim B. "Mobile Phone Forensics Challenges ,Analysis and Tools Classification". *International Workshop on Systematic Approaches to Digital Forensic Engineering*, May 2010, 47-55p.

[12]. Shivankar R and Saxena A. "Mobile Forensics: Guidelines and Challenges in Data Preservation and Acquisition". *Student Conference on Research and Development* , 16-18 Nov. 2009, UPM Serdang, Malaysia.

[13]. Willassen S. "Forensic analysis of mobile phone internal memory".

[14]. Paul McCarthy. "Forensic Analysis of Mobile Phones" . *A thesis submitted for the Bachelor of Computer and Information Science (Honours) Degree* 2005.

[15]. Maynard Y. "Practical Investigations of Digital Forensics Tools for Mobile Devices".

[16]. Bhadsavle N and Ju An Wang. "Validating Tools for Cell Phone Forensics" . *ASEE Southeast Section Conference* 2009.

[17]. Shira D, Rick A and Mislan P. "Hashing Techniques for Mobile Device Forensics" . *Small scale digital device forensics journal*, VOL. 3, NO. 1, JUNE 2009

[18]. Somasheker A, Himabindu K and Xin L. "Efficient Forensic Tools For Handheld Devices: A Comprehensive Perspective".

[19]. Salvatore F. "Theory and practice of flash memory mobile forensics". *7th Australian Digital Forensics Conference.*

[20]. Ramabhadran A. "Forensic Investigation Process Model For Windows Mobile Devices ".

[21]. Daware S and Thakare V. "Mobile Forensics: Overview of Digital Forensic, Computer Forensics Vs Mobile Forensics and Tools". *Published by Foundation of Computer Science, New York,USA.* May 2012 32-35p.

[22]. NIST 2007, "Cell Phone Forensic Tools: An Overview and Analysis Update", March 2007.

[23]. Paul McCarthy. "Forensic Analysis of Mobile Phones" , *BS CIS Thesis, University of South*

ISSN: 2321-8134

Australia, School of Computer and Information Science, Mawson Lakes, October 2005.

[24]. Wayne Jansen, Rick Ayers. "Forensic Software Tools for Cell Phone Subscriber Identity Modules", *Conference on Digital Forensics, Association of Digital Forensics, Security, and Law (ADFSL)*, April 2006.

[25]. Al-Zarouni M. "Introduction to mobile phone flasher devices and considerations for their use in mobile phone forensics".*5th Australian digital forensics conference* December 2007.

[26]. Jansen W, Ayers R. "Forensic software tools for cell phone subscriber identity modules". *Conference on Digital Forensics, Association of Digital Forensics, Security, and Law (ADFSL*); April 2006.

[27]. Jansen W, Delaitre A, Moenner L . " Overcoming impediments to cell phone forensics".*41st Hawaii International Conference on system sciences* ; 2008.

[28]. Simon M, Slay J. "Enhancement of forensic computing investigations through memory forensic techniques". *International Conference on availability, reliability and security*, 2009,p. 995e1000.

[29]. Bhadsavle N, Wang JA. "Validating tools for cell phone forensics". *Southern Polytechnic State University* .2008. Technical Report.CISE-CSE-08-05

[30]. Al Zarouni M. "Mobile handset forensic evidence: a challenge for law enforcement". 4th *Australian Digital Forensics Conference;* 2006. Perth, Australia.