Urge for Novel and Secure Software Framework for Extraction and Decoding of Mobile Artifacts

Mr. Bhushan M. Manjre[1], Dr. Krishan Kumar Goyal [2]

Department of Information Technology, Tulsiramji Gaikwad College of Engineering and Technology, Nagpur.[1]

Dean, Faculty of Computer Application, RBSMTC, Agra.[2]

bhushan.manjre@gmail.com[1], kkgoyal@gmail.com[2]

Abstract

Mobile Forensics is now days, increasingly becoming more challenging as it is the field of science that is continuously evolving with respect to the rapidly developing technologies and techniques for the extraction of the mobile data and its decoding. Majority of the crimes are getting committed digitally and especially the criminals are preferring mobile handsets than a laptop or desktop machines, leaving the footprints behind which could be evidence against them. The mobile handsets along with their software applications are getting more advanced and sophisticated mainly due to advances in Cloud computing where clouds are used to store data, Anti-forensics where efforts are made to defeat forensic procedures and Encryption which is used to secure the data during transit. But when compared with the pace of development in mobile hardware and software, the forensic tools and techniques are growing very slowly. Hence the contemporary forensic tools and methodologies are becoming increasingly obsolete and hence urges for the advanced forensic tools, methods which could comply with the need of today's mobile forensics. Hence, this work presents a detailed survey of the contemporary challenges faced by the forensic experts with the current forensic tools and its methodologies and also the need, scope and opportunities associated with the novel and secure software framework that can address the majority of issues occurring while extraction and decoding of mobile artifacts.

Keywords: *Mobile Forensics, Cloud computing, Anti-forensics, Encryption, Mobile Artifacts.*

1. Introduction

Today is the Era of Information Technology where the new technologies arrive day by day and the existing technologies evolve continuously to provide ubiquitous environment to the human being to carry out not only the personal but also the business tasks in skyrocket speed. The major role in this revolution is being played by the mobile phones or smart phones. Mainly the mobile phones are advancing with respect to their operating systems, the firmware, their hardware components too where there is competition among the device manufactures to give phenomenal features to their users with less cost especially with Android mobile phones. Number of detected malicious installation packages on mobile devices worldwide from 4th quarter 2015 to 2nd quarter 2021 in Fig.1:

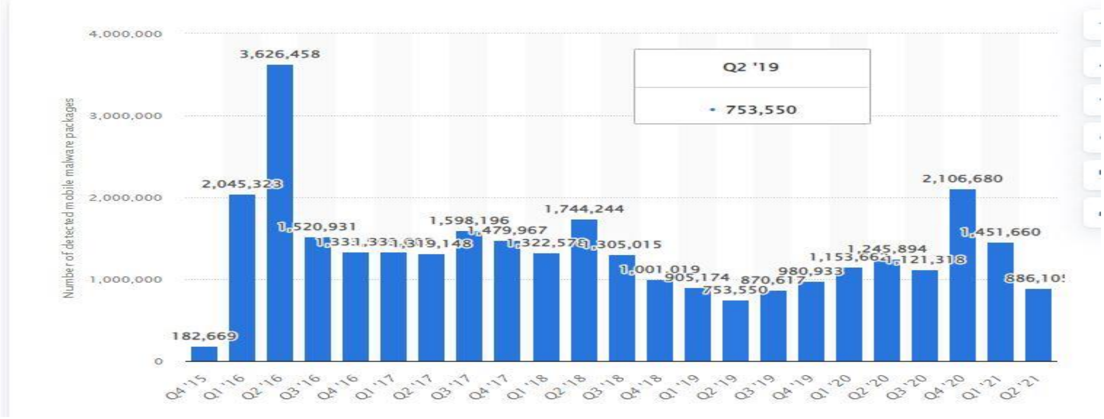

Fig.1: Number of detected malicious installation packages on mobile devices worldwide from 4th quarter 2015 to 2nd quarter 2021
Source: Statista.com

Today variety of tasks a Smartphone can perform like not only dialing call and receiving the same but also doing text message, email, sending audio, video, pdf and almost all type of multimedia. It also stores the most sensitive personal and financial information of the users. Android developers are adding variety of utility applications day by day for managing personal and business tasks. Smartphones vendors dream to make it as replacement for the computers by embedding variety of hardware and software components in it. This lures the hackers and the malware developers also to exploit the vulnerabilities in the smartphones and to commit the cybercrimes. Even as the number of mobile handhelds used by world is increasing day by day, the number of stolen phones and the infected one by the malwares is also growing too. Here the stream of Mobile Forensics comes into a prominent role as the countermeasure to identify the attacks launched on the smartphones and to detect the criminals committing cybercrime. But with different blends of hardware and softwares, network and communication protocols, no single tool can be used as universal tool for carrying out the mobile forensic investigations for all smartphones. With the inappropriate expertise in MDF tools, forensic field knowledge, and practice of handling cases, a forensics investigator may commit serious mistakes that could destroy important data [7]. This paper will present challenges in mobile forensics with respect to the available tools, their merits and demerits and will highlight the urge for the novel and secure software framework to create the mobile forensic tool for the extraction and decoding of mobile artifacts.

2. Challenges in mobile forensics

Hardware differences

There is huge variety of mobile handhelds available in the market which is of different models and are by global manufacturers. When it comes to carry out Mobile Forensics, the experts are flooded with variety of handsets with different softwares, operating systems, hardwares. The challenge increases due to the very short span of evolution of higher models of the same handhelds. So the forensic expert not only critically needs to update themselves on new MDF but also on new handsets.

Mobile operating systems

Majority of the PCs are found to be with Windows OS. But that's not the case with smartphones. The various operating systems of mobile handheld are HP's webOS, Apple's iOS, RIM for Blackberry, Google's Android and Nokia's Symbian OS. This pool of operating systems and their continued evolutions to higher versions makes the Mobile Forensic a tedious task for the forensic experts.

Mobile platform security features

The modern smartphones come with different built in technical security features. Their main purpose is to secure the users privacy and data. Even though these are proved to be useful for the users but it imposes new challenges for the data acquisition and the examination process. The deep encryption from hardware layer to software layer requires to be broken to absorb the data out of modern smartphones.

Lack of resources

As the number of smartphones with different hardware configuration are flooding the market, hence the accessories such as power chargers, data connectivity USB cables and the batteries which are required during the Mobile Forensics also need to be maintained by the Forensic experts for the successful forensic procedures.

Preventing data modification

The alteration or the modification of the data stored in the smartphones should be strictly prohibited for the Forensics procedures. But as the data in the smartphone tends to modify as the handset is merely switched ON, avoiding the data alteration is almost impossible. Background processes like calendar, clock still continue to run even if the phone is switched off, the similar application will cause the change in the integrity of the data with sudden state change.

Anti-forensic techniques

Many anti-forensic techniques, such as data hiding, data forgery, data obfuscation, and secure wiping, make the process of investigations on digital media more challenging.

Dynamic nature of evidence

It is an easy task to change or modify the digital evidence or proof, either intentionally or unintentionally. Simply, accessing an application on the smartphone might modify the data stored by that application on the device to be investigated.

Accidental reset

Everything on the Mobile phones can be reset. Mistakenly Resetting the device or even accidentally, while investigation may result in the damage of data.

Alteration of Device

If the suspect tries to modify or upgrade the manufacture's operating system, or moving, renaming application files, may lead to the complete alteration of the mobile handheld.

Passcode Recovery

Now days, all the smartphones come with the in-built passcode mechanism to unlock them. The forensic expert requires the access of the passcode protected smartphone but that too without the loss of data which is challenging task. Even though bypassing techniques for the screen lock come to rescue, but these techniques are not compatible with all smartphones.

Communication Shielding

There are numerous technologies with the help of which the smartphones communicate with outer world like cellular networks, Bluetooth, Wi-Fi, Infrared. It is important to immediately seize the device as further communication by it may modify the data possessed by mobile handheld.

Lack of availability of tools

The wide range of Smartphone with different firmwares, softwares and hardware are present in the market. For all these handhelds, no single universal forensic tool is available. Hence the approach of combination of tools needs to be followed but choosing the appropriate tool for a particular handheld is always a challenge.

Malicious programs

Often the Smartphone might be infected with some malicious software or malware, such as a virus or a Trojan. These malicious softwares may result into serious damage or loss to the crucial data in the phone and may result into destruction of digital evidence.

Legal Limitations

No geographical boundaries do exist for the crimes committed through mobile devices. But when it comes to handle multijurisdictional issues, the awareness regarding the nature of crime and the regional legislations is mandatory for the forensic experts.

3. Related Work

Very less work has been done towards creating the software frameworks for the mobile forensic tools. In [1], the authors mainly taken into consideration the terrorist network and the criminal network and tried to address the issue by the combination of Hadoop technology amalgamated with the renowned EnCase MF software so that massive Big Forensic data could be extracted more efficiently and effectively. The resultant framework model proves to be much efficient in extraction and decoding of Big Forensic Data. By combining the NodeXL, digital forensics and the technologies of Hadoop, the authors formulated and proposed Big Forensic Data framework. Figure 2 depicts variety of input files from the EnCase, the MDF tool. These files are inputted to Hadoop framework for the forensic processing. The data obtained from this process is then inputted to NodeXL by which the social network graph can be designed. This graph is then used to identify terrorist network or organized/unorganized crime networks. [1]

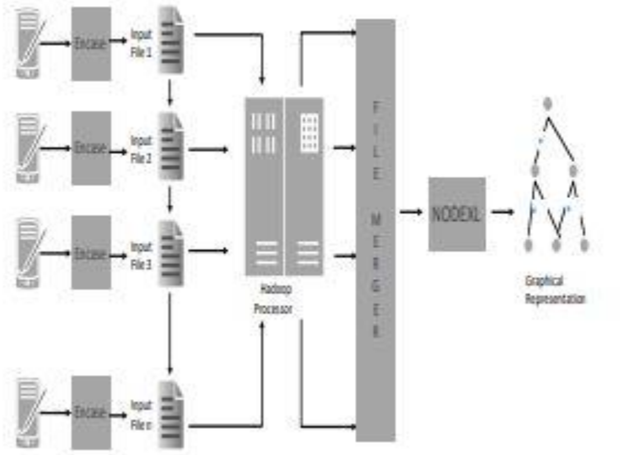

Fig.2: SYSTEM ARCHITECTURE

In [2] the authors have proposed a Harmonized Mobile Forensic Investigation Process Model (HMFIPM) for MF field. Here the DSR i.e Design Science Research is utilized to frame the HMFIPM. DSR is mainly used to give solution to unsolved problem or to give the improved, efficient and effective solution to any problem which has been solved earlier. In the problem domain, if the knowledge growth is to be achieved, the model needs to be developed with DSR methodology. To frame the HMFIPM, the main four phases have been adapted as shown in Fig.3.

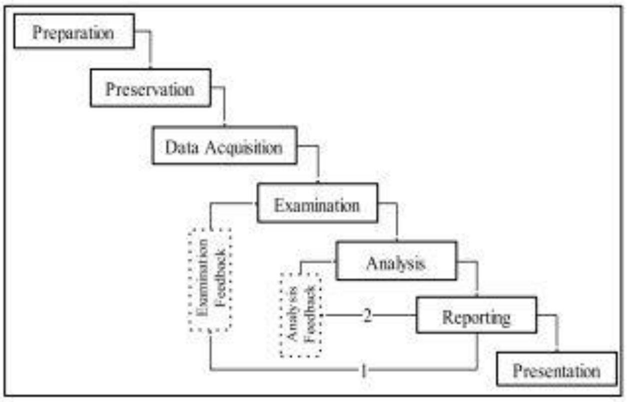

Fig.3: Harmonized Mobile Forensic Investigation Process Model (HMFIPM)

In [3], the authors proposed seven tier framework and each tier represents a layer, responsible for its specific functionality. As shown in fig. 4, the tier 1 layer performs the preparation and strategy making process. The tier 2 layer does detect the scene of crime happened. The tier 3 layer seizes the digital evidence and also takes care to preserve it safely. The tier 4 layer is responsible for data extraction and acquisition. The tier 5 layer functions as examiner and analyzer of the extracted evidence data. The tier 6 layer contains the reporting tool and performs the documentation which stands as evidence. The tier 7 layer will be closing the case.

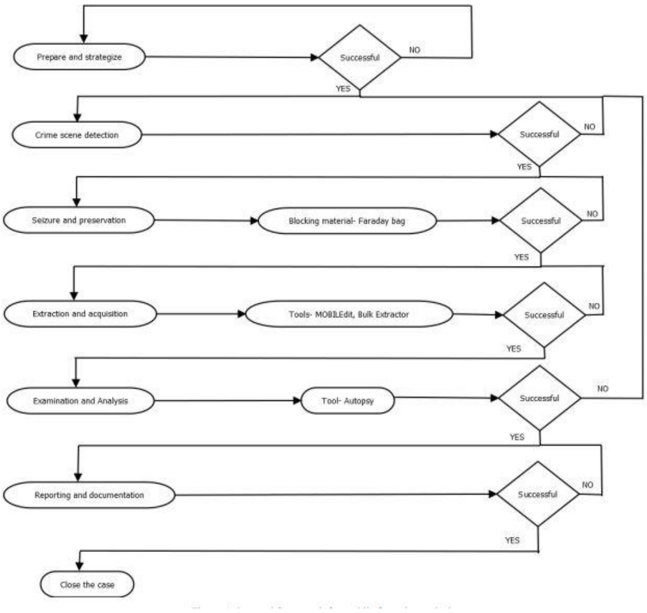

Fig.4: Seven Layered Framework for MF Analysis

In [4], for the purpose of MF, the MOS testing framework is proposed by authors. The framework has been developed for the evaluation of the variety of mobile forensic tools in terms of anti-forensics and the platform support offered by them. For a particular case and for the platform specific profiles, it assures the quality of performance of the peculiar mobile forensic tool. The proposed framework extends the test plan from NIST (National Institute of Standards and Technology) by including assertions and test actions to cover anti-forensics as well. In [5], the authors state that Even though the local acquisition methods are quite useful but they majority times, tend to be non-supportive for specific target mobile handheld. Maximum smartphones support data acquisition on remote basis but that scenario demands further resources specifically when compared to the local methods. Also the complete integrity of the extracted data cannot be guaranteed by local as well as remote methods. So using the combination of local and remote methods can come to rescue so that the above issue could be addressed. Hence the gathering of data as soon as possible once the crime is committed, is possible by the forensic experts in urgent cases. In [6], the TULP2G forensic software framework was proposed by the authors aiming at the detailed examination of the electronic devices by the forensic analyst. Even though this tool does not fully automate the forensic analysis, but proves to be efficient when it comes to minimize human errors and to accelerate the pace of forensic investigators. The proposed framework only defines the workflow for the forensic examination and provides abstract design of the modules to the software developers in the form of plug-ins. These modules i.e plug-ins contain the modus operandi of the actual investigation process. It imbibes the general developers “learn once apply everywhere” strategy. The drawback of the proposed framework is that one needs to put initial efforts to get used to the process workflow. The beauty of the framework lies in simplicity for the software developers to add specific handheld functionality without worrying about the graphical user interface and to avoid the redundancy in coding. The authors feel that their approach will inspire the developers to create fully automated forensic software tool.

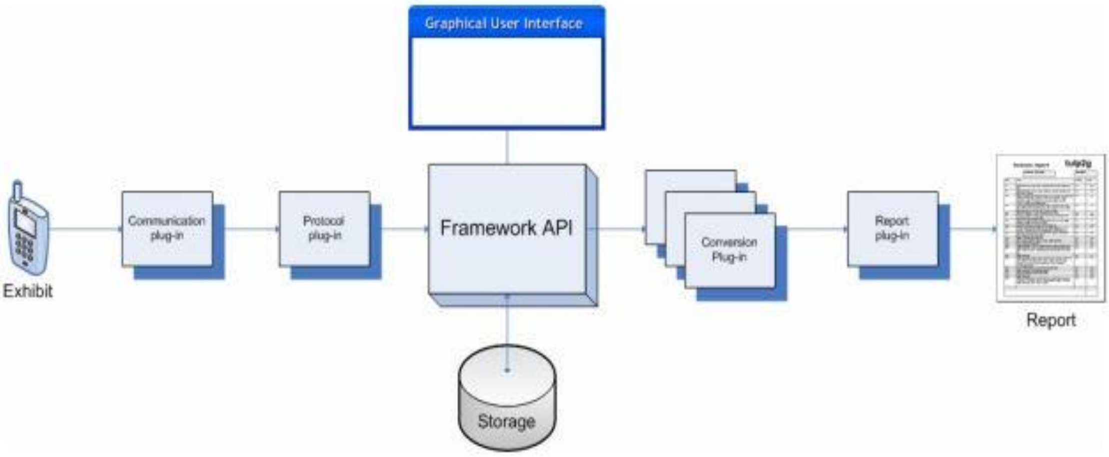

Fig.5: TULP2G Framework Architecture.

4. Conclusion

In today’s era, the world is facing challenges mainly due to Crimes and Terrorism. Both the challenges are empowered by the digital revolution in the mobile smartphones. Technologically the smartphones are skyrocketing and here comes the need of Mobile Forensics with the help of which, crucial evidences for criminal investigations can be gathered. When we speak about the efficiency of any latest mobile forensic tools like MOBILedit, Autopsy, Oxygen Forensic Suite, Encase Forensics, FTK Imager Lite, their efficiency is limited against large pool of variety of mobile handsets as the smartphones tend to differ in operating system, hardware, firmware, in-built security features, communication protocols etc. If at all, the utility of these tools needs to be improved for supporting more devices, then some new functionalities needs to be added in them so that the single tool could be versatile for almost all mobile forensic cases. Various crucial changes in the software development life cycle of these mobile forensic tools is the solution towards the creation of universal mobile forensic tool. In the above paper, we put focus on various challenges in the mobile forensics which are mainly due to lack of sophisticated, universal and versatile mobile forensic tool. Hence there is dogmatic need to not only create the novel and secure software framework but also to implement the same to output such a MF tool that will address majority of the problems faced by mobile forensic experts today.

References

[1] Sachdev, Hitesh; wimmer, hayden; Chen, Lei; and Rebman, Carl (2018) "A New Framework for Securing, Extracting and Analyzing Big Forensic Data," Journal of Digital Forensics, Security and Law: Vol. 13, Article 6.

[2] ARAFAT AL-DHAQM 1,2, (Member, IEEE), SHUKOR ABD RAZAK 1 , (Member, IEEE), RICHARD ADEYEMI IKUESAN 3 , (Member, IEEE), VICTOR R. KEBANDE 4 , AND KAMRAN SIDDIQUE 5 , (Member, IEEE) (2020) "A Review of Mobile Forensic Investigation Process Models", IEEE Access.

[3] Mayuri Goel, Vimal Kumar," Layered Framework for Mobile Forensics Analysis", 2 nd INTERNATIONAL CONFERENCE ON ADVANCED COMPUTING AND SOFTWARE ENGINEERING (ICACSE-2019)

[4] Maxwell Anobah, Shahzad Saleem and Oliver Popov, "TESTING FRAMEWORK FOR MOBILE DEVICE FORENSICS TOOLS", Journal of Digital Forensics, Security and Law, Vol. 9(2) 2014

[5] S. H. Mohtasebi and A. Dehghantanha," Towards a Unified Forensic Investigation Framework of Smartphones", International Journal of Computer Theory and Engineering, Vol. 5, No. 2, April 2013

[6] Jeroen van den Bos and Ronald van der Knijff, "TULP2G – An Open Source Forensic Software Framework for Acquiring and Decoding Data Stored in Electronic Devices", International Journal of Digital Evidence, Fall 2005, Volume 4, Issue 2

[7] Ashcroft, John, Deborah. J.Daniels, and Sarah V. Hart, "Forensic examination of digital evidence: A guide for law enforcement Department of Justice. 2004 U.S , https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

[8] Oluwafemi Osho, Sefiyat Oyiza Ohida, "Comparative Evaluation of Mobile Forensic Tools", I.J. Information Technology and Computer Science, 2016, 01, 74-83

[9] Nihar Ranjan Roy, Anshul Kanchan Khanna, Leesha Aneja, "Android Phone Forensic: Tools and Techniques", International Conference on Computing, Communication and Automation (ICCCA2016)

[10] Sundar Krishnan, Bing Zhou, Min Kyung An, "Smartphone Forensic Challenges", International Journal of Computer Science and Security (IJCSS), Volume (13) : Issue (5) : 2019

[11] Claudinei Morin da Silveira, Rafael T. de Sousa Jr, Robson de Oliveira Albuquerque, Georges D. Amvame Nze, Gildásio Antonio de Oliveira Júnior, Ana Lucila Sandoval Orozco, Luis Javier García Villalba, "Methodology for Forensics Data Reconstruction on Mobile Devices with Android Operating System Applying In-System Programming and Combination Firmware", Appl. Sci. 2020, 10, 4231; doi:10.3390/app10124231

[12] Riadi, R. Umar, and A. Firdonsyah, ''Identification of digital evidence on Android's blackberry messenger using NIST mobile forensic method,'' Int. J. Comput. Sci. Inf. Secur., vol. 15, no. 5, pp. 155–160, 2017.

[13] A. Goel, A. Tyagi, and A. Agarwal, ''Smartphone forensic investigation process model,'' Int. J. Comput. Sci. Secur., vol. 6, no. 5, pp. 322–341

[14] Rodney Wilson , Hongmei Chi."A Case Study for Mobile Device Forensics Tools", ACM SE 17, Apr 13-14 2017, Kennesaw, GA, USA ACM 978-1-4503-1203-5/12/03

[15] Kumari, N., & Mohapatra, A. K. (2016, March). An insight into digital forensics branches and tools. In International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 2016 (pp. 243-250). IEEE.

[16] Mumba, E. R., & Venter, H. S. (2014, August). Mobile forensics using the harmonised digital forensic investigation process. In Information Security for South Africa (ISSA), 2014(pp. 1-10). IEEE.

[17] Aziz, N. A., Mokhti, F., & Nozri, M. N. M. (2015, October). Mobile Device Forensics: Extracting and Analysing Data from an Android-Based Smartphone. In Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec), 2015 (pp. 123-128). IEEE

[18] Padmanabhan, R., Lobo, K., Ghelani, M., Sujan, D., & Shirole, M. (2016, August). Comparative analysis of commercial and open source mobile device forensic tools. In Ninth International Conference on Contemporary Computing (IC3), 2016 (pp. 1-6). IEEE.

[19] Roy, N. R., Khanna, A. K., & Aneja, L. (2016, April). Android phone forensic: tools and techniques. In International Conference on Computing, Communication and Automation (ICCCA), 2016 (pp. 605-610). IEEE.

[20] National Institute of Standards and Technology (NIST). (2013). Computer Forensics Tool Testing Program: Mobile Devices. Retrieved May 05, 2014, from http://www.cftt.nist.gov/mobile_devices.html

[21] A. Distefano and G. Me. (2008, August). An overall assessment of mobile internal acquisition tool. DFRWS. Digital Forensic Research Workshop Baltimore, MD. [Online]. Available: www.dfrws.org/2008/proceedings/p121-distefano.pdf

[22] Hariani, Imam Riadi, "Detection Of Cyberbullying On Social Media Using Data Mining Techniques", International Journal of Computer Science and Information Security (IJCSIS),Vol. 15, No. 3, March 2017.

[23]Andriller, "Andriller – Android Forensic Tool", Available at http://www.andriller.com, accessed on November 15, 2016

[24] Faiz Albanna, Imam Riadi, "Forensic Analysis of Frozen Hard Drive Using Static Forensics Method", International Journal of Computer Science and Information Security (IJCSIS), Vol. 15, No. 1, January 2017.

[25] Nuril Anwar, Imam Riadi, and Ahmad Luthfi, "Forensic SIM Card Cloning Using Authentication Algorithm", International Journal of Electronics and Information Engineering, Vol.4, No.2, PP.71-81, June 2016 (DOI: 10.6636/IJEIE.201606.4(2).03), 2016