International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET218321

A Forensic Evidence Recovery from Android Device Applications

Axay Patel[1], Dr. Priyanka Sharma[2], Prof. Dharti Dholariya[2]

[1]Student, School of Information Technology and Cyber Security, Rashriya Raksha University, Lavad, Gandhinagar, Gujarat, India

[2]School of Information Technology, Artificial Intelligence, and Cyber Security, Rashtriya Raksha University, Gandhinagar, Gujarat, India

Article Info
Volume 8, Issue 3
Page Number : 135-140

Publication Issue :
May-June-2021

Article History
Accepted : 12 May 2021
Published: 22 May 2021

ABSTRACT

In a computerized world, indeed unlawful conduct and/or violations may be named as advanced. This world is expanding. Getting to be versatile, where the fundamental computation and communication substances are Little Scale Computerized Gadgets (SSDDs) such as standard versatile phones, individual computerized collaborators, smartphones, and tablets. The ought to recoup information, which might refer to illegal and unethical exercises gave rise to the teaching of portable forensics, which has ended up a fundamental portion of computerized forensics. The literature relevant to Smartphone forensics, as explored in this paper, focuses on the architecture of Smartphone operating systems. It also addresses the digital evidence of Smartphone applications. in this paper undertakes practical experiments to identified sources for evidence that can later be used in the judiciary system. In this research, I'll use open-source Tools that can recover deleted data from the application.

Keywords : Mobile forensics, cell phone evidence, mobile phone forensic tool-kits, digital device forensics, and e-Evidence

I. INTRODUCTION

Mobile forensics may be a modern sort of gathering digital evidence where the data is recovered from a mobile phone. It depends on prove extraction from the internal memory of a versatile phone when there's the capability to access information. Portable phone advances have seen rapid development in later a long time. Different computer program apparatuses are available to recover and analyse smartphone information. Each tool has a set of points of interest and limitations.

A. THE HEADWAY OF CELL PHONES

Phones improve the methodology progression of adaptable exchanges advancement. They are not from a certain point of view used for the clarification of prompting and calling, they have various applications. Mobile phones are before long utilized for examining the Web and exploring through maps, similarly as, for photography, videography, and different other use cases. There is a progress in coordinate organization that goes indistinguishably with the movement of PDAs. Far off correspondences like Far away Nearby Region Associations (WLANs) have made to ended up speedier and all the more consistent. Cell

correspondences like the fourth Time (4G) and fifth Period (5G) Adaptable Constructions are by and large available and offers information speeds in a few Mbps.

B. ARCHITECTURE OF SMARTPHONE WORKING SYSTEMS

A handful number of smartphones working frameworks exists in the market today. Android architecture on the other hand consists of five layers, applications layer, the application framework, libraries, Android run time and the Linux kernel. The applications layer is written in Java. Applications are usually developed by third party companies and later ported to the device. On the other hand, each set of application programming interfaces available (API) that contains some of the capabilities are interesting, such as those that provide the interface with the file system.

C. SMARTPHONE FORENSICS

Cell phones have been able to be fundamental to our consistently lives. Cell phones are as of now used as an adaptable office or amusement centre, joining fundamental requirements for speaking with friends and family members. Their capacity limit and getting ready abilities are to be contrasted with low-end PCs. Cell phones had the chance to be defenceless against the equivalent and more critical weaknesses as PCs. The data in cell phones like pictures, documents, messages, accounts and short messages (SMS) can be distantly gotten to if the gadget is related to the Internet. This reality poses a significant test for crime scene investigation specialists. There are numerous applications that can run on a cell phone and more are fostered every day. Considering the arrangement of cell phone sellers, convenient applications and coordinating shows, the errand of logical examination on versatile telephones is truly difficult. When managing portable contraptions, for example, cell phones, there are three districts where data is taken care of: the SIM card, which essentially contains contact information and writings; the gadget memory, which stores the customer made data like MMS, instant messages, photographs, media...etc., and furthermore contains the telephones working framework and settings; and, the gadget memory which to stores advantageous application programming, for example, "Whats Application" and the reasonable logs. There are additionally adaptable limit memory contraptions, for example, Miniature SD cards again store tremendous measures of information. Cell phones that have adaptable applications, for example, "Whats Application" store data inside the actual application on the particular gadget.

II. RELATED WORK

Husein et al. 2009 [16] studied and reported the forensic analysis of three different instant messaging applications (IMs): AIM, Yahoo! Messenger and Google Talk, (both client based and web-based versions) showing that various useful artefacts related to IMs can be recovered from the iPhone, including username, password, buddy list, last log-in time, and conversation timestamp as well as conversation details. A forensic examination of Instant Messaging on smartphones such as the iPhone pose a new challenge for investigators as well as researchers due to the uniqueness of the file system.

Anglano was able to reconstruct the list of contact sand the chronology of messages that had been exchanged by users. The correlation of the contents of the chat database with the information stored in the log files allows the investigator to determine which messages have been deleted, when these messages were exchanged, and the users that exchanged them [17]. But the usage of any hash function is not performed in this paper.

Mahajan et al. 2013 [18] directed measurable information investigation of two broadly utilized IMs on Android telephones: Whats Attach Viber. The

tests and investigation were performed determined to figure out what information and data can be found on the gadget's interior memory for moment couriers for example talk informing logs and history, send and got pictures or video documents, and so forth Yet, this paper doesn't cover the insights regarding the discovered follows and proof as it is restricted to ordinary talk situation as it were. Removing information from cell phones is testing. Dissimilar to PCs that have predetermined number of major working framework merchants, there are endless producers of cell phones and cell phones with their own restrictive innovation and arrangements. Simultaneously, there are cell phone crime scene investigation apparatuses accessible, for example, U took care of from Praise, the Katana Criminology instrument Lamp, Dark light Legal sciences Programming, Paraben's Gadget Seizure and Miniature Systematization's XRY. As featured by PC Legal sciences Educator, Darren Hayes from Payes College, these instruments are not complete enough in the specific make and model of Google Android, Apple iOS gadget or other cell phone models they can deal with. The way that Android makers divided its working framework presents a troublesome factor. On the Apple iOS, its security demonstrating is compelling to such an extent that bypassing the PIN is a test for computerized criminology specialists.

In this paper, I directed Android criminology. By reliably utilizing forensically solid principles, I directed acquisitions and examination. This paper portrays the extricating of information on POCO X2 cell phone that chips away at Android 11 working framework and Samsung System J7 dependent on Android 10.

III. METHODOLOGY

A. COMPUTER FORENSIC PROCESS MODEL

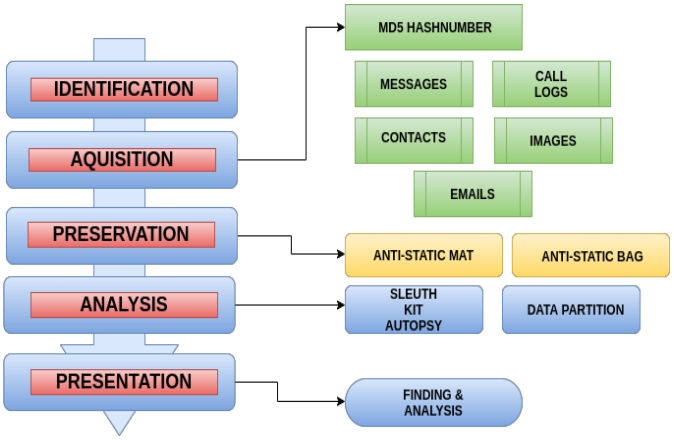

Figure 1 : PC Legal Cycle Model

A norm and widespread advanced crime scene investigation measure should be applied in all computerized criminology practices as portrayed on the left half of Figure 1. It comprises of recognizing the potential confirmations identified with the case being researched. The proof can be workers, PCs, cell phones, pen drives, cameras or printed copy records, among others. When distinguished, the examiners will gain the things in a measurable way with its appropriate techniques. Imaging or making duplicates of the first thing is an unquestionable requirement. The things procured should be kept and safeguarded in a legitimate and secure stockpiling with proper logs on chain of authority. Examination of the proof will be made utilizing the fundamental crime scene investigation devices. Consequences of the examination should be archived as a feature of the report to be introduced to the law implementation or proprietor of the examination. The correct side of Figure 1 shows the utilization of potential instruments and things identified with the securing, protection, examination and show stages in an advanced legal science generally speaking interaction.

In this paper, the extraction of proof for investigation is talked about. We expect that different period of the advanced criminology are taken consideration in like

manner. We are utilizing Investigator Unit Post-mortem examination as our information extraction and examination device. Detective Pack Examination is one of the broadly utilized legal sciences device that permits us to effectively investigations hard drives and PDAs. When a proof material (for this situation the PDAs), has been obtained, extraction of information can be made. Significantly, preceding that, imaging or replicating of the undiscovered telephone memory should be led. The accompanying sub-areas will examine the means taken in removing the conceivable proof dwelling on the obtained cell phone.

B. TECHNIQUES

Decide the Mounting Points of the Information Parcel

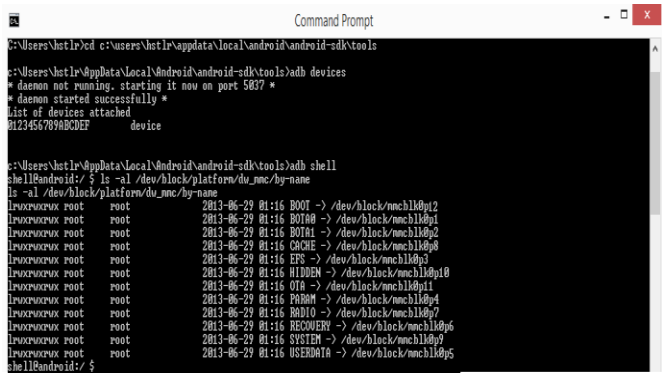

Figure 2 : Distinguishing the Mounting Focuses in the phone

To picture the information parcel, we need to distinguish the mounting points of each segment in the telephone. For this situation, the way or mounting focuses for information segment (USERDATA) is/dev/block/mmcblk0p5 as in Figure 2.

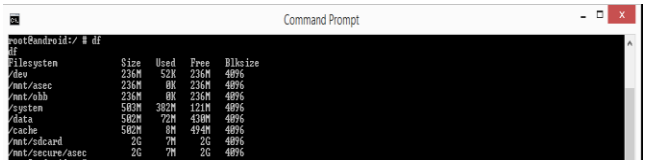

Figure 3 : Accessible Circle Space of Document Framework Mounted

Every one of the important advances and orders were at first not known. A ton of references and experimentation were made. We alluded for appropriate procedures and techniques for these exercises from assets in [4], [6], [7], [8] and [10].

IV. DISCOVERIES AND EXAMINATION

Coming up next are data that can be removed and finishing advanced legitimate sciences on PDAs that are in different stage and restrictive is for sure a test for legal sciences ace. Information bothering Android based telephones can be eliminated utilizing the privilege mechanical gatherings and measures. It is essential to get a handle on the telephone plan, working designs, PC quantifiable cycle and coherent mechanical congregations before do the information extraction and recuperation of reports. Information from the Contact Once-finished, Call Logs, Schedule, Picture, Messages, SMS and GPS Track-point are figured out some approach to be taken out. Related information can be singled out and broke down for the law execution to relate these confirmations to the case. Such electronic confirmations would then have the choice to be brought to the court. The information extraction for various android cell phones changes dependent on their engineering models and their maker restrictive plan. Unreliably related for the examination. This incorporate content messages of SMS, substance of email and its connection, contact list, related picture and significant occasions from the schedule. Despite the fact that this is a model case, we accept our technique can be applied for genuine cases.

Directory Listing
Call Logs
Table | Thumbnail

Source File	From Phone Number	Start Date/Time	End Date/Time	Direction	Name	Data Source	To Phone Number
contacts2.db	0175153563	2015-04-20 14:34:04 SGT	2015-04-20 14:34:04 SGT	Missed	Faih	fypdata2.dd	
contacts2.db		2015-04-16 06:01:40 SGT	2015-04-16 06:01:40 SGT	Outgoing	nadhar	fypdata2.dd	0145348676
contacts2.db	0145348676	2015-04-14 13:05:14 SGT	2015-04-14 13:06:15 SGT	Incoming	014 534 8676	fypdata2.dd	
contacts2.db		2015-04-12 21:25:05 SGT	2015-04-12 21:25:05 SGT	Outgoing	nadhar	fypdata2.dd	0145348676
contacts2.db		2015-04-12 21:24:55 SGT	2015-04-12 21:24:55 SGT	Outgoing	nadhar	fypdata2.dd	0145348676
contacts2.db	0172583290	2015-04-12 20:16:32 SGT	2015-04-12 20:16:40 SGT	Incoming		fypdata2.dd	
contacts2.db	0179653217	2015-04-12 19:52:35 SGT	2015-04-12 19:52:35 SGT	Missed	Joros	fypdata2.dd	
contacts2.db		2015-04-12 17:01:47 SGT	2015-04-12 17:01:47 SGT	Outgoing	adeep	fypdata2.dd	+60175153563
contacts2.db		2015-04-12 16:56:08 SGT	2015-04-12 16:56:08 SGT	Outgoing	nadhar	fypdata2.dd	0145348676
contacts2.db	0177151691	2015-04-12 16:53:09 SGT	2015-04-12 16:53:09 SGT	Missed		fypdata2.dd	
contacts2.db	0133317291	2015-04-12 16:48:44 SGT	2015-04-12 16:48:44 SGT	Missed		fypdata2.dd	
contacts2.db	0142758890	2015-04-12 16:46:29 SGT	2015-04-12 16:46:29 SGT	Missed		fypdata2.dd	
contacts2.db	0148429123	2015-04-12 16:43:30 SGT	2015-04-12 16:43:30 SGT	Missed		fypdata2.dd	
contacts2.db	0176520290	2015-04-12 16:32:22 SGT	2015-04-12 16:32:22 SGT	Missed		fypdata2.dd	

Figure 4 : Findings for Call Logs

Correspondences between the suspects through call can likewise be separated from the call logs of the telephone proprietor as in Figure 4.

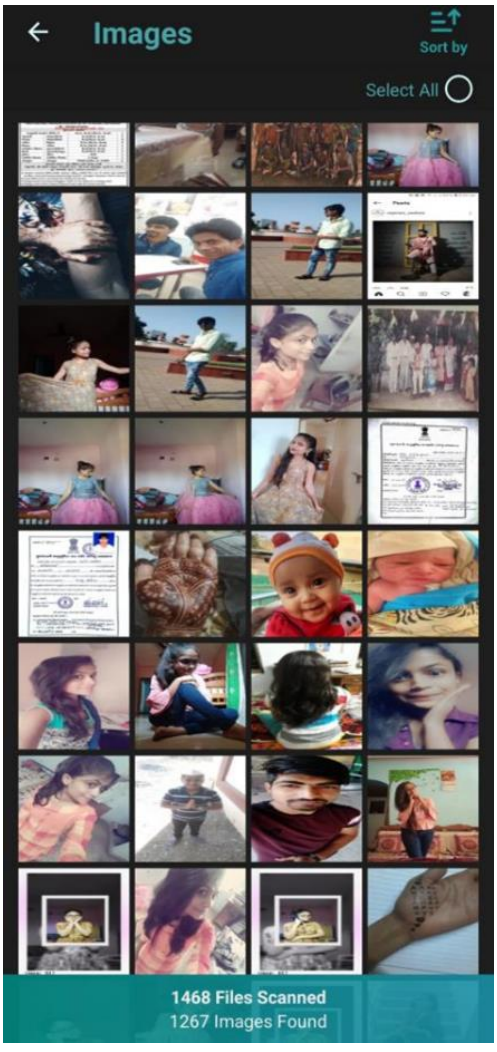

Figure 4 : Discoveries for Pictures Recovered

A picture tells 1,000 words. In any examination, pictures may prompt valuable phase of the examinations.

V. CONCLUSION

Finishing advanced legitimate sciences on PDAs that are in different stage and restrictive is for sure a test for legal sciences ace. Information bothering Android based telephones can be eliminated utilizing the privilege mechanical gatherings and measures. It is essential to get a handle on the telephone plan, working designs, PC quantifiable cycle and coherent mechanical congregations before do the information extraction and recuperation of reports. Information from the Contact Once-finished, Call Logs, Schedule, Picture, Messages, SMS and GPS Track-point are figured out some approach to be taken out. Related information can be singled out and broke down for the law execution to relate these confirmations to the case. Such electronic confirmations would then have the choice to be brought to the court. The information extraction for various android cell phones changes dependent on their engineering models and their maker restrictive plan.

VI. REFERENCES

[1]. Hawthorne EK, Shumba RK. Teaching Digital Forensics and Cyber Investigations Online: Our Experiences. European Scientific Journal Sept 2014; Special (2): 255-261

[2]. http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk

[3]. Forensic Magazine Website, “An Introduction to Android Forensics”., Retrieved on 5 May 2015 from http://www.forensicmag.com/articles/2010/04/introduction-android-forensics

[4]. Muhammad Faheem, N-A. Le-Khac, Tahar Kechadi, “Smartphone Forensic Analysis: A Case Study for Obtaining Root Access of an Android

Samsung S3 Device and Analyse the Image without an Expensive Commercial Tool", Journal of Information Security, 2014.

[5]. Martin, A., "Mobile Device Forensic", SANS Forensics White paper, Retrieved on 10 April, 2015 from http://digital-forensics.sans.org/community/papers/gcfa/mobile-device-forensics_3553

[6]. Jeff Lessard, Gary C. Kessler, "Android Forensics: Simplifying Cell Phone Examinations", Scale Digital Evidence Forensics Journal Vol.4, September 2010.

[7]. http://digital-forensics.sans.org/community/downloads

[8]. Android Developers Website. Retrieved on 14 April 2015 from http://developer.android.com/index.html

[9]. Azhar, M.H.B. and Barton, T.E.A. (2017) 'Forensic analysis of secure ephemeral messaging applications on android platforms', in International Conference on Global Security, Safety, and Sustainability, January, pp.27–41, Springer, Cham.

[10]. The Sleuth Kit, Retrieved on 5 March 2015 from http://www.sleuthkit.org/sleuthkit/,

[11]. Hawthorne EK, Shumba RK. Teaching Digital Forensics and Cyber Investigations Online: Our Experiences. European Scientific Journal Sept 2014; Special (2): 255-261

[12]. https://www.guidancesoftware.com/products/Pages/encase- forensic/overview.aspx?cmpid=nav

[13]. http://www.securityisfun.net/2014/06/booting-up-evidence-e01-image-using.html

[14]. Choo, K.R. (2013) 'Cloud and mobile forensics: own cloud as a case study', Digital Investigation, Vol. 10, No. 4, pp.287–299.

[15]. Tassone, C.F., Martini, B. and Choo, K.K.R. (2017) 'Visualizing digital forensic datasets: a proof of concept', Journal of Forensic Sciences, Vol. 62, No. 5, pp.1197–1204.

[16]. Mohammad Iftekhar Husain and Ramalingam Sridhar. I forensics: forensic analysis of instant messaging on smartphones. In Digital forensics and cyber-crime, pages 9–18. Springer, 2009.

[17]. Cosimo Anglano. Forensic analysis of WhatsApp messenger on android smartphones. Digital Investigation, 11(3):201 – 213, 2014. Special Issue: Embedded Forensics.

[18]. Aditya Mahajan, MS Dahiya, and HP Sanghvi. Forensic analysis of instant messenger applications on android devices. arXiv preprint arXiv:1304.4915, 2013.

Cite this Article

Axay Patel, Dr. Priyanka Sharma, Prof. Dharti Dholariya, "A Forensic Evidence Recovery from Android Device Applications", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 8 Issue 3, pp. 135-140, May-June 2021. Available at doi : https://doi.org/10.32628/IJSRSET218321

Journal URL : https://ijsrset.com/IJSRSET218321