Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 44 No. 8
August 2023

Mobile Forensic for Android Smart phone

[1] Aslam. J. Karjagi, [2] S. A. Quadri, [3] Rafeeda. A. Karjagi, [4] Niyaz Ahamad. Herkal, [5] Mr. Sayed Khalid. Kazi, [6]Mr. Azharuddin. Inamdar

[1] Assistant Professor, [2]Professor, [3]Assistant Professor, [4]Student, [5]Student, [6]Student
[1]Department of CSE, Secab Institute of Engineering and Technology College, Bijapur 586 101, Karnataka, India
[2]Department of CSE, Secab Institute of Engineering and Technology College, Bijapur 586 101, Karnataka, India
[3]Department of MCA, Secab Institute of Engineering and Technology College, Bijapur 586 101, Karnataka, India
[4]Department of CSE, Secab Institute of Engineering and Technology College, Bijapur 586 101, Karnataka, India
[5]Department of CSE, Secab Institute of Engineering and Technology College, Bijapur 586 101, Karnataka, India
[6]Department of CSE, Secab Institute of Engineering and Technology College, Bijapur 586 101, Karnataka, India

Abstract

Mobile forensics is an fast paced field in the electronic market. The end product of this development are the smart-phones which are no less than the computers. The objective of the following paper is to better comprehend various tools and techniques used in the process of mobile forensics in android phones. The proposed paper also makes an comparison between the tools and techniques depending upon their participation or role in the process of investigation, ultimately recommending appropriate tools and techniques or practices for the process of investigation for android phones.

Introduction:

Mobile forensics is an entrancing field that can effectively influence a wide extent of conditions, for instance, internal corporate assessments, national security, criminal assessments, information amassing, and issues and open security. Open Security Database (NSD) describes progressed criminology as a piece of lawful science recollecting and assessment of data found in mobile phones.

In the initial stage the term was used to exclusively represent the pattern of quantifiable assessment of infringement that occurs in digital devices or the devices that has been used as a weapon to lead the violations, however at this point the term is comprehensively used to describe a wide scope of bad behaviors where mobile phones are involved. [1,2]

The procedure of investigating forensically for such sort of devices incorporates data acquisition, which suggests data extraction from one device to an outer device, assessment of the data utilizing forensics tools to categorize into various data-groups furthermore, recoup data from the source(data) and concluding with depicting the intriguing revelations that could be the conceivable proof for exhibiting the condemnable acts.[3]

A computerized gadget may be categorized as a PC, a smart-phone, a hand-held device or may be any electronic gadget. Digital examination or forensics is a science that has many sub-instructs, for instance, PC criminology, Mobile forensics and network forensics. The objective of the proposed paper is to focus on Mobile forensics.

Cell phone legal, wireless crime scene investigation, mobile device forensics is a comparable term which deals with recuperating of modernized proof or content from a PDA or mobile phones under forensically suitable conditions.

Mobile forensics is the quickest and progressive modernized field of study. One of the most important aspect in the progression of PDA industry is the ascent of what is alluded to today as cell phones. Not at all like feature phones, smart phones or cell phones are bundled with an all out working structure and various applications that help customers to render services of various data and voice.
According to the Android forensics it is said that the Android versatile stage has quickly rose from its first telephone in October 2008 to the most renowned portable working structure by mid 2011.[1]

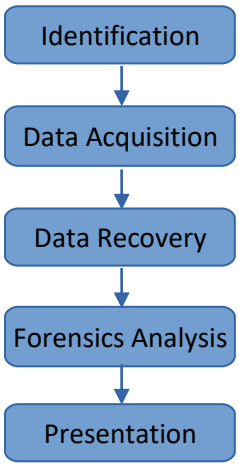
The fascinating fact of Android legal sciences or forensics is that it obtains and examines the acquired information from the mobile devices, it is imperative to have a wide comprehension of the tools and the platform. Both will be used through out the assessment. An escalated apprehension will support a lawful reviewer or safety(security) engineer towards the effective assessment and examination of an Android device.

1.1 Brief of Investigation Cycle of Digital Forensic :-

A forensic Investigation of a scene is a cycle involving, making and testing of hypotheses to deliver on demands for a scene that has happened. For example, questions join "what caused the scene to occur", "where did the event occur", "when did the scene occur", and "who is/are obligated for the scene and what is the confirmation to underwrite the responsibility".[1]
A sequence of activities or courses must be followed to affirm the particular and genuineness of the evaluation to make & test theories for forensics examination. The normal cycle incorporates following steps:

•**Identification**: reorganization of the framework or the presentations that should be explored.
•**Data procurement/Preservation**: fetching a image or making clone of the information from the presentation that has a place with the framework.
•**Data recuperation**: It is defined as reestablishing or extracting deleted, hided or actual information from the image record.
•**Forensic examination**: breaks down the advanced items from the information which is being acquired from the scene.
Introduction of Evidences: While examination is performed, evidences are determined and announced . The illustration underneath displays the connection among the examination steps.

Figure (1): Investigation Process of Digital Forensic



For any of the strategies above there are various tools and procedures that help to achieve the development. Such types of procedures are called as digital forensic investigation tool.. The significance of of the discussed tool is to accomplish various steps involved in digital forensic process as referred in fig 1.
The tools and procedures discussed above vary from device to device. For instance , tools used for computer devices are different from tools used for smart-phones. The major reason for diversification lies in difference in hardware detailing such as processor architecture, I/o interfaces and software detailing such as type of operating system being used and files systems. Thusly the proposed paper bases on the genuine forensics tools that are explicit on PDAs and are packaged with Android OS.[3]

1.2 Android Platform and Smartphones:-

Andre. H depicts the Android to imply an open source remote stage that has been made

dependent upon the Linux 2.6 part and controlled by the Open Handset Confederation, a party of transporters, PDA and piece creators, and programming sellers. The chronicled foundation of android as a stage for remote has started in 2008 after the primary telephone was presented. From the year 2008 and up till now, Android note commendably influenced the cell phone market. [1, 4]

Ingratiating decree in Android.com site, says that android is such an operating system that regulate multi-billion PDAs and tablets and thusly, making Android smart-phone the most enchanting PDA in the general market. As per International Data Corporation (IDC) which is a boss overall supplier of market data and do the tracking of the consignment of wireless around the world, the overall android cell phone market has reach about 85% from 60% continually since most recent couple of years. The figure underneath shows the bit of the pie of android wireless generally subject to shipment information.

Year	2018(%)	2019(%)	2020(%)	2021(%)
IOS	14.9	13.9	14.6	14.0
Android	85.1	86.1	85.4	86.0
Others	0.0	0.0	0.0	0.0
Aggregate	**100**	**100**	**100**	**100**

Figure (2) consignment market share based on smart-phone‟s OS [5]

1.2.1 Android Platform Main Components:

Pursuing top-down strategy, android stage design/Architecture is separated in three basic layers that join an applications, middle-ware and working structure. While isolates to the designing, their are two sections in the application, the middle-ware moreover includes two portions, ultimately the Operating System layer can be categorized into smaller components. Coming up next is a compact portrayal towards the essential fragments of the various layers:

•**Applications**: Many of the important Applications programming that either accompany default programming is upheld by the Android Operating System or introduced from android programming marketplace for example, Calendar, Maps, Browser, Contact, and Scheduler. And so on.

•**Application system:** This layer can be located beneath the application and it gives the artifact of application programming interfaces (API) utilized by diverse executable applications.

•**Libraries**: This layer can be located underneath the application structure and supports major attributes or aspects that may be utilized by the applications. The libc library which is the standard C programming library is considered to be the most significant . Moreover, realistic libraries, for example, openGL and info/yield libraries are additionally critical to the applications.

•**Android Runtime**: This runtime is the fundamental aspect of the libraries layer and it incorporates the Dalvik Virtual Machine (DVM) and Core Libraries. The Core Libraries offer utilities of various center libraries utilized in Java programming dialects.

•**Linux Kernel**: the Kernel accessible with Android is 2.6 adaptations. Linux kernel comprises of different drivers required to operate various applications. A portion of the regular drivers accessible are WiFi, sound, camera, print etc. [1, 2]

The illustration underneath represents the parts of the various stages of Android platform.

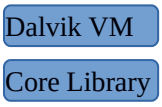


Figure (3) Components of Android Architecture. [2]

Knowing android planning and its standard parts energize the course towards exploring smart-phones that are bundled with android stage. Obviously, a practitioner will have to face lots of challenges due to proliferation of various types of smart-phones. Moreover, complete information about the architecture and working of android cell phones enables the forensics practitioner to pick the best tool suitable for the investigation. [1, 3]

I. Discussion of different tools used for digital forensic on Android smart-phones

Many types of devices are available which are submitted for performing advanced appraisal for android smart-phones. Herewith we discuss following standard tools utilized for exploring android smart-phones.

Android Debug Bridge (ADB): It is a useful request line tool that facilitate to interact with related android controlled devices. It does that through a logical appraisal the pro may run over and need to connect with exploring technique for the android stage to pull out specific records or to find the assessment of a particular limit. The ABD instruments are furthermore used by the most of PDAs' quantifiable structure as the principal subcomponent to talk with the android stage. The ABD contraption can be utilized to fulfill the data acquiring stages. [1, 6]

Open Source Android Forensics (OSAF): It is an open source brought together with android forensic and its guideline revolve around looking at malware inside the android applications. It is required to follow a standardized cycle for quantifiable assessment and some practices for separating Android applications OSAF that can be utilized for forensic examination and presentation of evidence progresses [7]

Andriller: It is an tool which consists of assemblies of forensic tools for mobile phones. Some segment of this packaged tool are functional in android forensic. It has various features, for instance, astounding Lock screen parting for Pattern, PIN code, or Password; custom decoders for applications from android mobile phones. Close to data obtainment, Andriller can be utilized for data recovery, forensic assessment and presentation of presentable evidences.[8]

AFogical: It is an open source extraction device, which may be utilized to **eliminate** calls, SMS, MMS, MMS parts and contacts from android smart-phones. It makes a record titled with time and date of extraction. It might be utilized for quantifiable examination and presentation of evidence methods. [9]

WHATSAPP EXTRACT: It is an freely available tool that can be used for extraction & examination of whatsapp application. It can show in a HTML record of all WhatsApp messages eliminated from an android phone and iPhone as well. Presently, WhatsApp is a broadly used messaging application. The Whatsapp extract is specific on lawful assessment and presentation of evidence that could be recovered on WhatsApp application.[10]

SKYPE EXTRACTOR: It is an freely available tool/device for isolating skype application's data. In general skype extractor may be utilized for analysis of skype application on an android phone. Also used to eliminate data, for instance, Account information, contacts information, calls, talks, record move, telephone messages and deleted and altered messages. This mechanical assembly is explicit on quantifiable assessment, data recovery and presentation of verification that could be found on skype application.[10]

For the most part, Android Forensic devices ought to have the option to examine different kinds of information in the android cell phone. The accompanying table demonstration an example of information that can be removed.

Tables (1) illustration of selected data from smart-phones of Android OS.

Contacts	**Text messages**	**Instant Messenger/Chat**	**Location**	**Call logs**	**E-mail messages**
Music collection	**Search History**	**Search History**	**Driving Directions**	**Social Media**	**Files stored on the smart-phone**
File sharing	**Financial Information**				

2.1 Comparison of Android forensic tools:

The table beneath demonstrate a comparability study of the above discussed android forensic softwares/tools

Tables 2: comparability between android forensic softwares/tools

Tools	**ABD**	**Andriller**	**OSAF**	**AFLogical**	**Whatsapp Extract**	**Skype Extractor**
Command lines	■					
Attributes		■	■	■	■	■
Android OS	■	■	■	■	■	■
Other OS		■	■	■	■	■
Assist all types	■	■	■	■		
Digital Forensics Investigation Process Support						
Identification	■	■	■	■		
Preservation	■	■	■	■	■	■
Data Recovery	■	■	■	■	■	■
Forensic Analysis		■	■	■	■	■
Presentation		■	■	■	■	■

The outcomes represented in above table demonstrates that Andriller, OSAF and AFLogical are covering more strolls in the genuine legal evaluation measure. Their are techniques which are exclusive to specific application. For example, WhatsApp Extract and Skype Extract are just explicit on WhatsApp and Skype applications.

I. Conclusion & Future Work:

Mobile forensics for the cell phones is the fastest progressive field . The serious legitimate cycle for any contraption or

techniques involved different advances, commencement with the distinctive evidence, data acquiring, data recovery, logical assessment and presentation of affirmations.

Android as a platform for PDAs has overwhelmed in the marketplace of remote industry. So discovering solutions for investigating android smart-phone is a captious concern for any forensics examiner. In order to identify suitable tool to carry out the digital investigation on android smart-phones, prior knowledge of hardware and software architecture is critical. The android investigation process consist of various tools for managing several phases of investigation process. The proposed paper shows part of the tool that can be utilized in handling an investigating process and open the entry for making exceptional structure or a relevant framework which can follow the standard procedure of digital investigation.

References

[1] A. Hoog, Android Forensics: Investigation, Analysis and Mobile Security for Google Android: Syngress, 2011.
[2] L. ı. N. Claudio Maia, Lu´ıs Miguel Pinho. (2014, Evaluating Android OS for Embedded Real-Time Systems. Cyber Forensics.
[3] E. H. S. Brian D. Carrier. 02/02/2015). An Event-Based Digital Forensic Investigation Framework. Available: http://www.digital-evidence.org/papers/dfrws_event.pdf
[4] Android.com. (2014). History of Android. Available: http://www.android.com/history/
[5] idc.com. Smartphones Market share, Q3 2014. Available: http://www.idc.com/prodserv/smartphone-os-market-share.jsp
[6] Developer. android, Android Debug Bridge
[7] http://osaf-community.org/. (2015). OSAF Open-Source Android Forensics. Available: http://osaf-community.org/wiki/tiki- index.php
[8] Andriller.com. (2015). Andriller. Available: https://andriller.com/
[9] viaforensic.com. (2014). Android forensics. Available: https://github.com/viaforensics/android-forensics
[10] O. S. T. f. M. F.-. SANS.(2013. Available: https://digital-forensics.sans.org/summit-archives/Prague_Summit/Open_Source_Tools_for_Mobile_Forensics_Mattia_Eppifani.pdf