*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 2, Ver. 1 (Mar – Apr. 2015), PP 15-19*
*www.iosrjournals.org*

# A Survey on Mobile Forensic for Android Smartphones

[1]Abdalazim Abdallah Mohammed Alamin, [2]Dr.Amin Babiker A/Nabi Mustafa
*[12],Department of Communications, Faculty of Engineering, Al-Neelain University*
*Khartoum, Sudan*

***Abstract:*** *Mobile forensic is fast becoming an abbreviated term that describes the process of applying digital forensics in mobile phones world. The rapid development in mobile phones industry has led to the emergence of the so-called smart phones which have become nearly the same as computers. Android Smartphones refer to all types of smartphones that use Android operating system. This paper aims to survey the tools and techniques that are used to forensically investigate Android mobile and then provides comparison between the tools according to their roles in the investigation process. Finally, the paper gives recommendation for following the best practices for investigating Android smartphones.*

## I. Introduction

Digital forensics is an interesting fast-paced field that can have a powerful impact on a wide range of situations such as internal corporate investigations, civil litigation, criminal investigations, intelligence gathering, and issues such as national security. As has been defined by National Security Database (NSD), digital forensics is a branch of forensic science including the retrieval and investigation of material found in digital devices, often related to computer crime.[1]

Originally the term was used to exclusively describe the process of forensic investigation of crimes that takes place in computers 'network or the computer has been used as a weapon to conduct the criminal activities, but now the term is widely used to define all types of crimes where any type of digital devices is a subject or an object in the crime scene.[1, 2]

Regardless the type of digital device, the process of forensically investigating such type of devices involves data acquisition which refers to cloning the data from the device to an external source, analysis of the data using analytical tools to classify the data groups and recover information from the data source and finally highlighting the interesting findings that would be potentially evidence for proving the criminal activities.[3]

A digital device could be a computer, a mobile phone, a tablet device or any type of electronic devices.

So now, digital forensics as a science is encompassing many sub-disciplines such as computer forensics, Mobile forensic and network forensic. The scope of this paper is to focus on mobile forensics.

Mobile device forensic, cellular phone forensic or mobile forensics are all synonyms to the same term which refers to the branch of digital forensics that concern with recovering of digital evidence or data from a mobile device under forensically sound conditions.

Mobile forensics, arguably the fastest growing and evolving digital forensics discipline and this is according to the rapid growth in mobile phone industry and it offers significant opportunities as well as many challenges.

One of the most significant break throughs in the development of mobile phone industry is the emergence of what is known today as smartphones.Unlike traditional mobile phones, smart phones are bundled with a complete operating system and many other applications that help users to interact with many data and voice services.

According to (Android forensic), the Android mobile platform has quickly risen from its first phone in October 2008 to the most popular mobile operating system in the world by early 2011.[1]

While the interesting part of Android forensics involves the acquisition and analysis of data from devices, it is important to have a broad understanding of both the platform and the tools that will be used throughout the investigation. A thorough understanding will assist a forensic examiner or security engineer through the successful investigation and analysis of an Android device.

### 1.1 Digital Forensic Investigation Process:-

A forensic Investigation is a process that creates and tests hypotheses to answer questions about an incident that happened. For instance, questions include "what caused the incident to occur", "where did the incident occur", "when did the incident occur", and "who is/are responsible for the incident and what is the evidence to approve the responsibility".[1]

To develop and test hypotheses for digital forensic investigation, a concrete chain of activities or steps need to be followed to ensure the technicality and legality of the investigation. Generally, different digital devices follow a similar forensic investigation process. So the typical process encompasses the following steps:

- **Identification**: identifying the system or the exhibitions that need to be investigated.
- **Data acquisition/ Preservation:** taking an image or cloning the data from the exhibition that belongs to an identified system.
- **Data recovery**: is the process of restoring or pulling out deleted, hidden or actual data from the image file.
- **Forensic analysis:** analyzes the digital artifacts inside the data that has been recovered.
- **Presentation of Evidences**: reporting of evidence found during the analysis face.

The figure below shows the relation between the investigation steps.

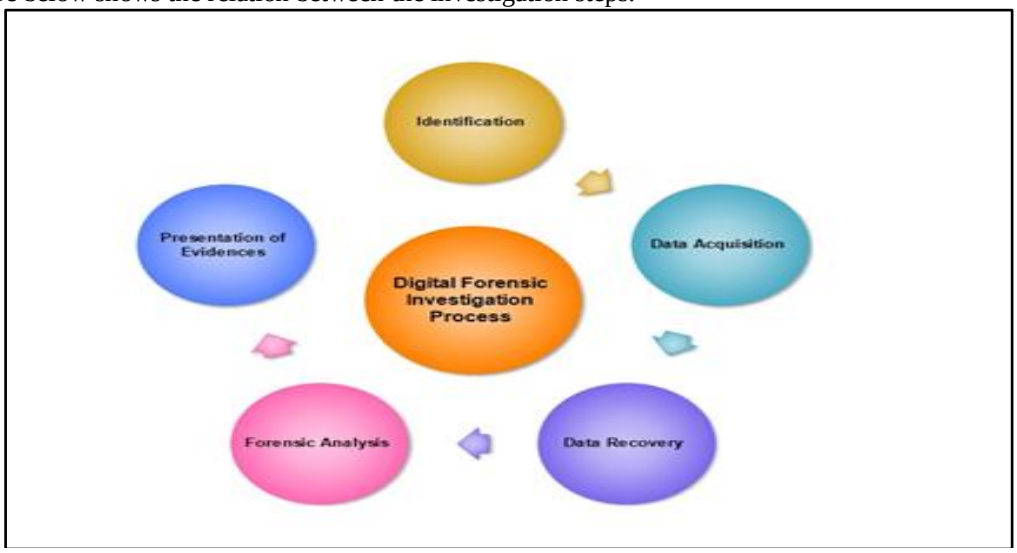


**Figure (1):** Digital Forensic Investigation Process.[1, 3]

For any of the steps above there are variety of tools and techniques that help to accomplish the step. These tools are called digital forensic investigation tools. A generally accepted definition of digital forensic investigation tool is a piece of software or hardware that is used to perform one or more of the above investigation steps.

These tools and techniques are different from one device to another. For example, computer devices have a set of tools that are totally different from smartphone tools. The diversity of forensic investigation tool has come about because of the reason that distinctive computerized or digital device have different hardware and software specifications. Hardware specifications that might differ from one device to another are such as the processor architecture, the type of the main board, type of input/output interfaces and the type of primary storage. Software specifications are such as Operating System (OS), file systems and development environment. Therefore this paper focuses on the digital forensic tools that are specialized on smart phones that are bundled with Android OS.[3]

**1.2 Android Platform and Smartphones:-**

Andre. H defines the Android to refer to an open source mobile device platform that has been developed based on the Linux 2.6 kernel and managed by the Open Handset Alliance, a group of carriers, mobile device and component manufacturers, and software vendors. The history of android as a platform for smartphone has begun in 2008 after the first smartphone was introduced. Since 2008 and up to now, Android had made a remarkable impact on the smartphone market. [1, 4]

Referring to statement in Android.com website, android is the OS that manage more than one billion smartphones and tablets and consequently, this fact makes Android smartphone are one of the most desirable smartphone in the global market. According to International Data Corporation (IDC) which is a premier global provider of market information services and tracks the shipment of smartphone worldwide, the worldwide android smartphone market grew from 60% to reach nearly 85% by the third quarter of 2014. The figure below shows the market share of android smartphone worldwide based on shipment information. [5]

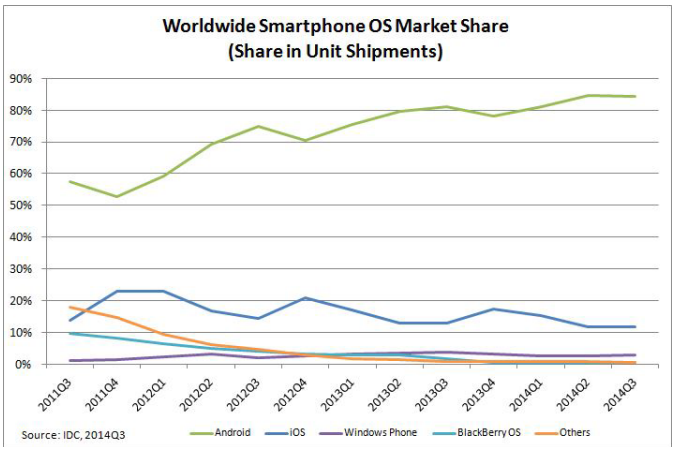


**Figure (2)** smartphone shipment market share based on smartphone's OS [5]

**1.2.1 Android Platform Main Components:**

Following top-down approach, android platform Architecture is divided into three main layers which encompass an applications, middleware and operating system. More breaks down to the architecture, the application contains two components, the middleware also consists of two components and finally the OS layer can be divided into subcomponents. The following is a brief description for the main components of the different layers:

- **Applications**: Some of the major Applications software that are either come with default package of software supported by the Android OS version or installed from android software markets such as Calendar, Maps, Browser, Contact, and Scheduler. Etc.
- **Application framework**: it's a layer below the application and it provides the framework application programing interfaces (API) used by the different running applications.
- **Libraries**: it's a layer below the application framework and provides core features libraries that can be used by the applications. The most important library is libc, the standard C programing library. Additionally, graphic libraries such as openGL and input/output libraries are also important to the applications.
- **Android Runtime**: its main part of the libraries layer and it includes of the Dalvik Virtual Machine (DVM) and Core Libraries. The Core Libraries provide support functionalities of numerous core libraries used in Java programing languages.
- **Linux Kernel:** the Kernel available with Android is 2.6 versions. It contains of a massive list of various drivers used to run different applications. Some of the common drivers available are WiFi, audio, camera, print, video conferencing, etc.[1, 2]

The figure below shows the components of the Android platform.

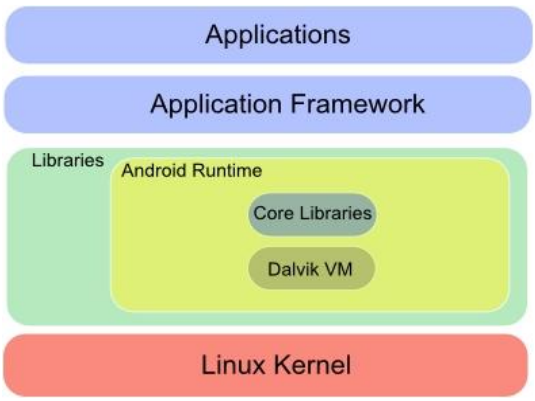


**Figure (3)** Android platform components. [2]

Understanding android architecture and its main components ease the process of investigating smartphones that are bundled with android platform. Of course, nothing worth doing is easy and applying digital forensic for both traditional mobile phones and smartphones have a host of challenges that need to be overcome. Moreover, comprehensive knowledge about the software and hardware architecture of android smartphones helps the digital forensic practitioner to obtain the right tools to perform the steps of the digital investigation,

taking into account that an essential goal of digital forensic is protecting any modification of the target device's data by the practitioner. [1, 3]

## II. Digital Forensic Tools for Android

There are bunch of tools that are dedicated for performing digital investigation for android smartphones. Some of these tools are integrated in a framework with other digital forensic tools that serves other type of smartphones' platforms. The following are the main tools that are used for investigating android smartphones.

**Android Debug Bridge (ABD):** is a multipurpose command line tool that lets you communicate with connected Android-powered device. Throughout a forensics examination the investigator may come across and need to interact with debugging mode of the android platform to pull out some files or to check the value of a certain parameter. The ABD tools are also used by the majority of smartphones' forensic framework as the main subcomponent to communicate with the android platform. The ABD tool can be used to fulfil the data acquisition step. [1, 6]

**Open Source Android Forensics (OSAF):** is an open source unified android forensic that its main focus on investigating malware with in android applications. It follows a standardized process for forensic investigation and a set of best practices for analyzing Android applications OSAF can be used for forensic analysis and presentation of evidences steps [7]

**Andriller:** is a utility with a group of forensic tools for smartphones. Part of these bundled tools are specialized in android forensic. It performs read-only, forensically sound, non-destructive acquisition from Android devices. It has other features, such as powerful Lock screen cracking for Pattern, PIN code, or Password; custom decoders for applications from android smartphones. Beside data acquisition, Andriller can also be used for data recovery, forensic analysis and presentation of evidences steps [8]

**AFLogical:** is an open source extraction tools, available on GitHub that can be used to extract calls, SMS, MMS, MMS parts and contacts from android mobile phones. It creates a directory named with time and date of extraction. It can be used for forensic analysis and presentation of evidences steps. [9]

**WHATSAPP EXTRACT:** is an open source tool for WhatsApp extraction and analysis. It's able to display in an HTML document of all WhatsApp messages extracted from an android phone and iPhone as well. Nowadays, WhatsApp is a wide used instant messaging application. This tool is specialized on forensic analysis and presentation of evidence that could be found on WhatsApp application.[10]

**SKYPE EXTRACTOR:** is an open source tool for extracting skype application data. It can be used to analyze skype application on an android phone. It can extract data such as Account info, contacts info, calls, chats, file transfer, voice mails and deleted and modified messages. This tool is specialized on forensic analysis, data recovery and presentation of evidence that could be found on skype application.[10]

Generally, Android Forensic tools should be able to investigate various types of data in the android smartphone. The following table shows a sample of data that can be extracted.

| | | | | | |
|---|---|---|---|---|---|
| Text messages (SMS/MMS) | Contacts | Call logs | E-mail messages (Gmail, Yahoo, Exchange) | Instant Messenger/Chat | GPS coordinates |
| Photos/Videos | Web history | Search history | Driving directions | Facebook, Twitter, and other social media clients | Files stored on the device |
| Music collections | | Calendar appointments | Financial information | Shopping history | File sharing |

**Tables (1)** sample of extracted data from Android smartphone.

### 2.1 Android Forensic Tools Comparison:

The chart below shows a comparison between the above android forensic tools

| Tools / Features | ABD | Andriller | OSAF | AFLogical | Whatsapp Extract | Skype Extractor |
|---|---|---|---|---|---|---|
| Command lines | √ | | | | | |
| GUI | | √ | √ | √ | √ | √ |
| Android OS | √ | √ | √ | √ | √ | √ |
| Other OS | | √ | | √ | √ | √ |
| Support All Apps | √ | √ | √ | √ | | |
| **Digital Forensic Investigation Process Support** | | | | | | |
| Identification | √ | √ | √ | √ | | |
| Preservation | √ | √ | √ | √ | √ | √ |
| Data Recovery | √ | √ | √ | | √ | √ |
| Forensic Analysis | | √ | √ | √ | √ | √ |
| Presentation | | √ | √ | √ | √ | √ |

**Tables (2)** comparison between android tools

The results obtained from the above table shows that Andriller, OSAF and AFLogical tools covers more steps in the digital forensic investigation process. Other tools are specialized in one step or one task. For instance, WhatsApp Extract and Skype Extract are only specialized on WhatsApp and Skype applications.

## III. Conclusion & Future Work:

No doubt, mobile forensics or digital forensic investigation for mobile devices is the fastest growing and evolving digital forensic discipline. The digital forensic process for any devices is consisted of different steps, starts with the identification, data acquisition, data recovery, forensic analysis and presentation of evidences.

Android as a platform for mobile devices has dominated in the market of smartphone industry. So finding solutions for digitally investigating android smartphone is a critical mission that any digital forensic practitioner should handle. However, knowing the software and hardware architecture of the android smart phone is a crucial step for finding the appropriate tool to perform the digital investigation steps. The spectrum of android forensic investigation is full with many available tools that can handle different steps of the digital investigation process. This paper shows part of the tools that can be used to handle the investigation process and open the door for creating special framework that can follow the standard process of digital forensic for Android smartphones.

## 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