ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 4, April 2016

Forensic Simplified Methodology for Android Data Extraction

Santos MRP, Alves TF, Neto RPC

Bachelor of Computer Science from Teresina, Brazil.

ABSTRACT: The use of Android Smartphone and the wide range of services available in hardware and software make these devices a valuable repository information and data. Data acquisition approaches in mobile devices needs interactions with the smartphone, unlike computational extraction. In mobile approaches, is necessary install applications and use others tools to proceed with the forensics analysis. With the real big number of information that these devices contain, it's important create a one-way form to collect the information, so, it is a big challenger for computers forensics collect and purchase the files and information of the owner of the device, or only proof his involvement to characterization of an crime. This paper objective to propose a one-way form to analyze in legitimate and authorized Android devices, applying forensics techniques with adhesions of the features in the Android Platform.

KEYWORDS: Android. Smartphone, Forensics.

I. INTRODUCTION

The smartphones are combinations of two classes of devices: cell and personal assistance. The first smartphones were released by BlackBerry in 2002, who for few years dominated the market, together with Nokia, since the release of IPhone by Apple [1- 3].

Unlike traditional phones, the smartphones can connect to the internet through mobile broadband (3G, 4G) or wi-fi, enabling a large number of shares and resources. The smartphones Androids is the most popular for final users, one reason for this is that they are more completely, due theses platform be target exclusively for mobile devices [4].

There are varied Operational systems in market, like Firefox OS, Windows Phone, IOS, etc. In this paper, we treat only Android devices. This operational system were purchased by Google in 2005, when they decides to participate o this kind of market, the system is Open source and it's based in Linux [5].

II. ANDROID SMARTPHONE LAYERS

In now we present the layers of android devices, we can see in the figure below the division in layers, we will present all of them.

In the lower layer, we have the kernel, which is responsible for provide a hardware abstraction layer that provides the access to excenciais resources, like file system, the memory management, etc. [6].

In the libraries layers we have a collection of subprograms used for applications development, they have vital information and data that provides a smooth operations to apps and others programs. We can consider some libraries present in that layer like, SQLite, Web kit, etc. [6,7].

In the Framework application layer, we have the standard structure of applications [8.9].

Finally, we have the application layer; this is the layer that the applications are run. In this layer we have a basic set of applications, like browser, music player, video, etc.

III. DIFFICULTIES OF ANDROID EXTRACTION DEVICES DATA AND INFORMATION

According to NIST (National Institutes of Standards and Technology), the forensic analysis may pass by four process: device seizure, acquisition, test and report [10].

Other difficult is about the use of rooms that allows modification in the original system format, making actions more difficult.

Other challenger is about the use of passwords and encryption to protect the data, it's easy extract data form a device without encrypt or password, since with a password simple, but in the others case is extremely difficult.

The apps used for one kind of device may not work in other, in others words, apps used for forensics IPhone may not work in Android.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 4, April 2016

Others issues is about the lack reporting, evidence corrupting, the capability of cloud data be seized, etc. [12, 13].

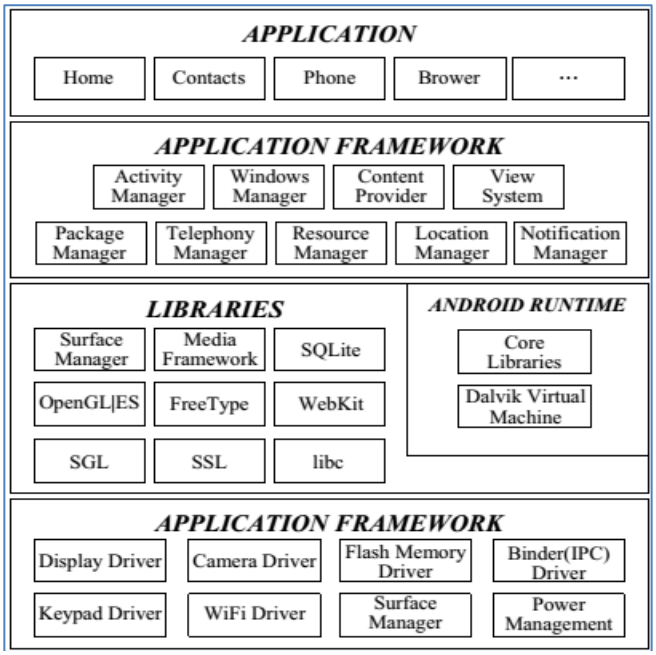

Figure 1: Android Smartphones layers. Google. Inc.

IV. PROPOSE MODEL FOR DATA EXTRACTION

Now we have the method that describes the process to perform forensic analysis in smartphone with Android. The focus of the process is based in collect information like video, messages, audio, etc. Due to large amount of possible target for actions.

We try to propose and standardize the forensics process model, considering the actions and research environment. Our model will be focus in only three process subdivision that will be presented in next figure.

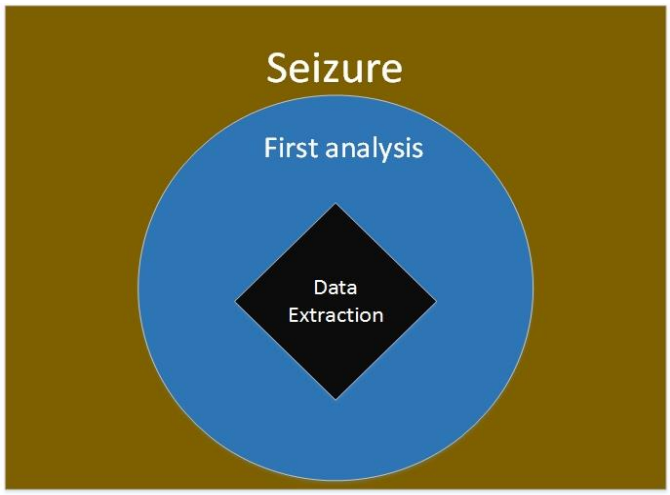

Figure 2: Hierarchy of the proposed mode.

In this hierarchy model is very cleaner to understand that we have a unidirectional model, that should occur by following the steps, first the seizure, second the first analysis and finally the data extraction.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 4, April 2016

Will be consider only the activities associated with the figure, and any one of them have some typical characteristics, we can highlight the following characteristics:
Seizure – the seizure process proposed have to occur with the presence of a professional expert witnesses, for a righteous bust. In this activity, we consider that occur on of the most important activities, once the seizure must occur within the law of the country.
First analysis – the first data extraction only can be carried out with the presence of an expert, and this activities only consider surface analysis, and if it's possible, interview with the suspect.
Data extraction – this is the focus of our proposed model, since after the seizure and the first analysis, we had the data extraction process with an expert forensics laboratory.

A. Seizure:

The first process in our model proposed is the seizure of the device, in this process we consider that the forensics has already seized the device, and will proceed as showing in the figure bellow.

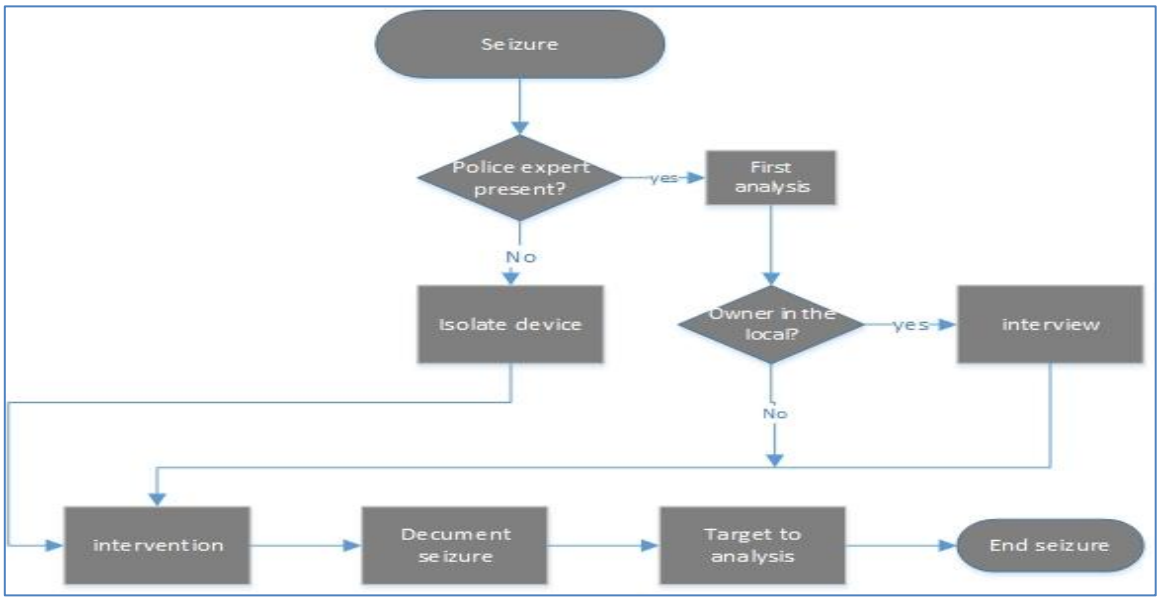

Figure 3: seizure proposed by the model.

It is possible to observe that we consider the presence of a professional expert in forensics in the local, if a cap or other prison officer, the firs process in only held the seizure of the phone isolate the device for intervention and before this document the seizure for conclude de seizure. If the forensics in present in the scene of the seizure of phone, he will proceed an interview with the possible criminal.

B. First analysis:

In the next figure, will be present the propose model for first analysis in the phone, this step must be help before the phone seized, and only consider superficial analysis in the device sized.
In this proposed step must consider the presence of forensics expert, with the phone in hand he will proceed to initial extraction, if it's possible extract initial data, the forensics will make the appraisal report and end this, if the initial extract don't solve the initial request, he must diversify the test as much as possible.

C. Data extraction:

In this step we consider that the device is in lab for forensics activity, and will be held all process possible to collect the data in seized phone.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 4, April 2016

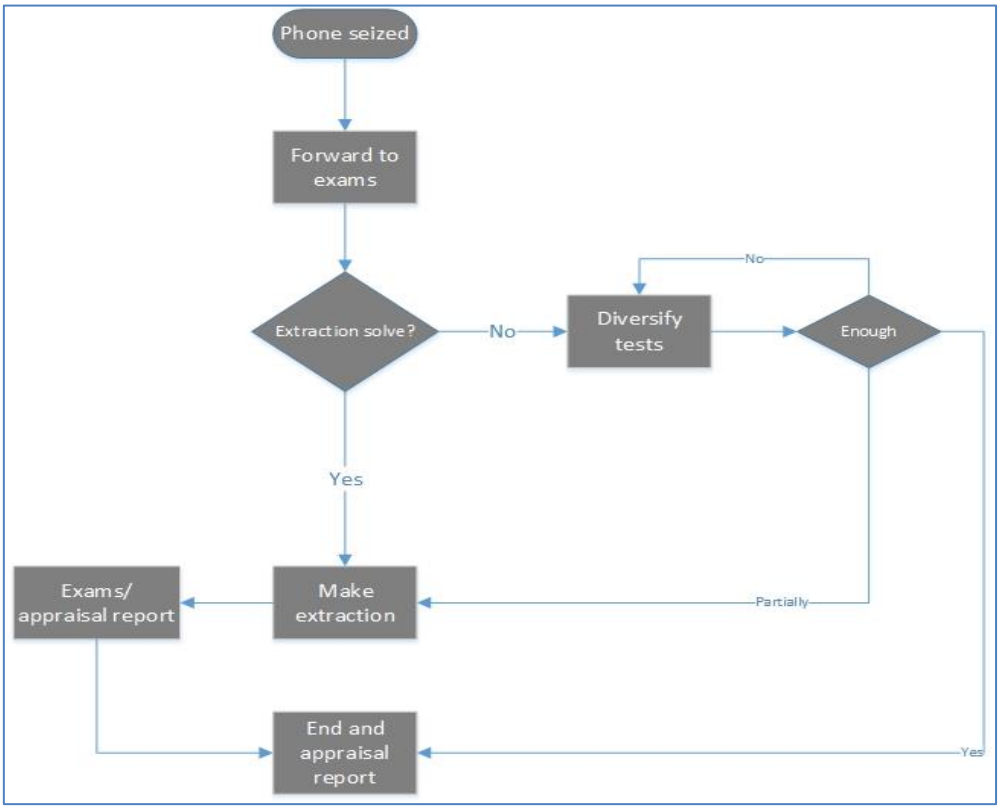

Figure 4: Proposed model for first analysis.

The first step in this process is collecting the documentation of all previous activities, to an initial understanding. Before this, it's important verify if the device is the right on, after this, will be held all analysis possible.
Making the forensics analysis in the memory card, if the phone have one, if not, will start in the phone. Its important consider if the phone contains root, or if has password, this things can make the process a bit difficult, or even prevent the forensics analysis.
After all process, is needed checks the data collect, and after that, documentation the process and finalize the analysis.

V. RELATED WORKS

About forensics analysis, we have the master thesis of André Morum, intituled "Proposta de metodo de analise pericial em smartphones com sistema operacional android" that formed the basis for the proposal [10]. For security. To the area of security, the following article was verified form Santos and Raimundo intitule identifying vulnerabilities in cloud computing using penetration test that was used for theoretical fundaments in security standard [11]. Another model proposed for android extraction is in the paper intitule A study if user integrity during acquisition of Android devices [13].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 4, April 2016

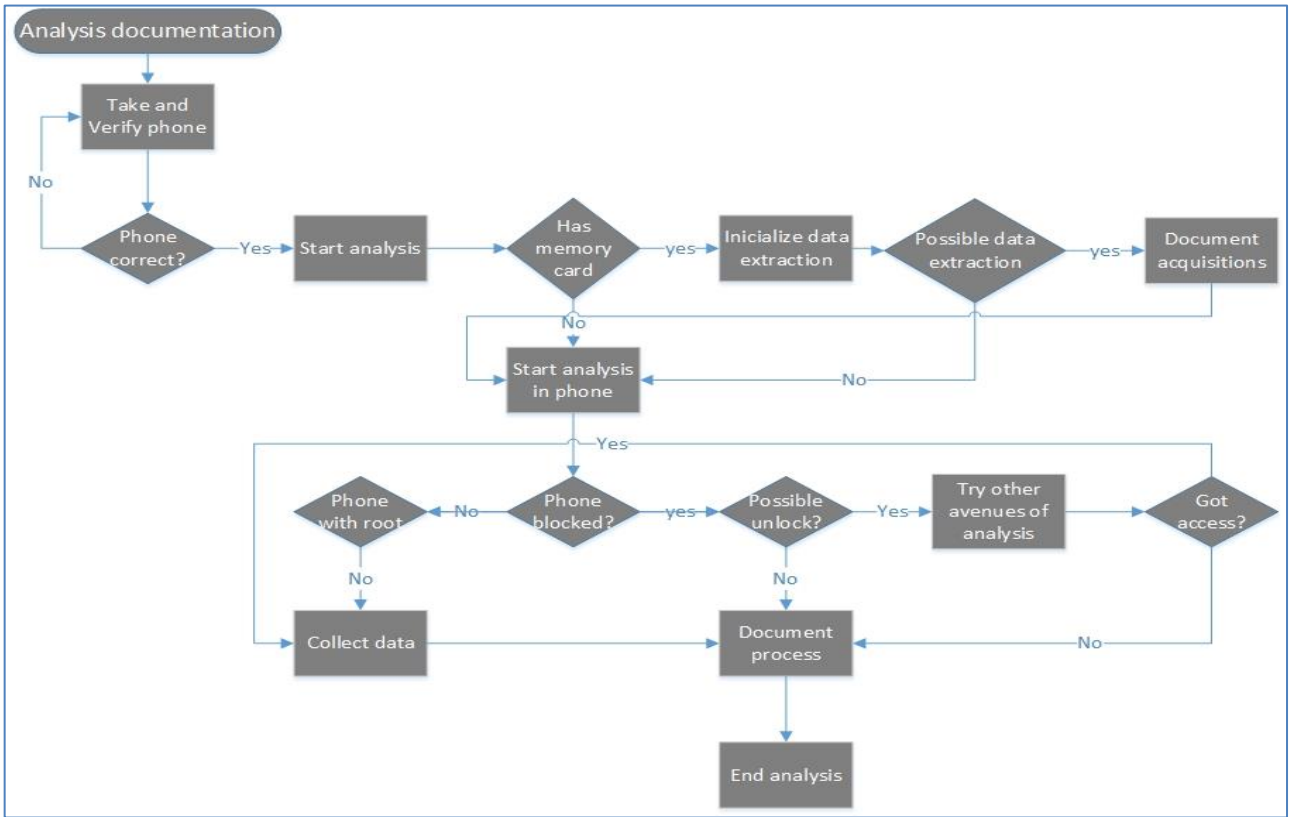

Figure 5: Simplified model for initial data extraction.

VI. TEST PERFORM

The data acquisition is a very important moment, once for the device be analyzed, it is necessary an expert forensics to make the procedure, and it's very important for the expert have a good know about the Android platform.

To perform the method presented in android devices, and protect the data integrity, bringing the Android device to the original state when finish the data extraction, it's important prepare a custom recovery image, one way to compare the data image with the original is using the CRC (cyclical redundancy checksum).

The data can be collect in the card and in the phone. It's recommended collect and save all data collected. All the proposed process has to the documented, describing all information as possible, like if the data was collect by a forensics tools or by copy image.

All experiment can be tested using forensics tools, Now Secure Forensics, that provide access to root exploit, screen lock bypass tools, Data parsing, deleted data recovering, and many others resources. Other forensics tools that ca be held to perform the process present in this paper is UFED, that can disable default locks/PIN/passs world, physical extraction and de-codification, etc.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 4, April 2016

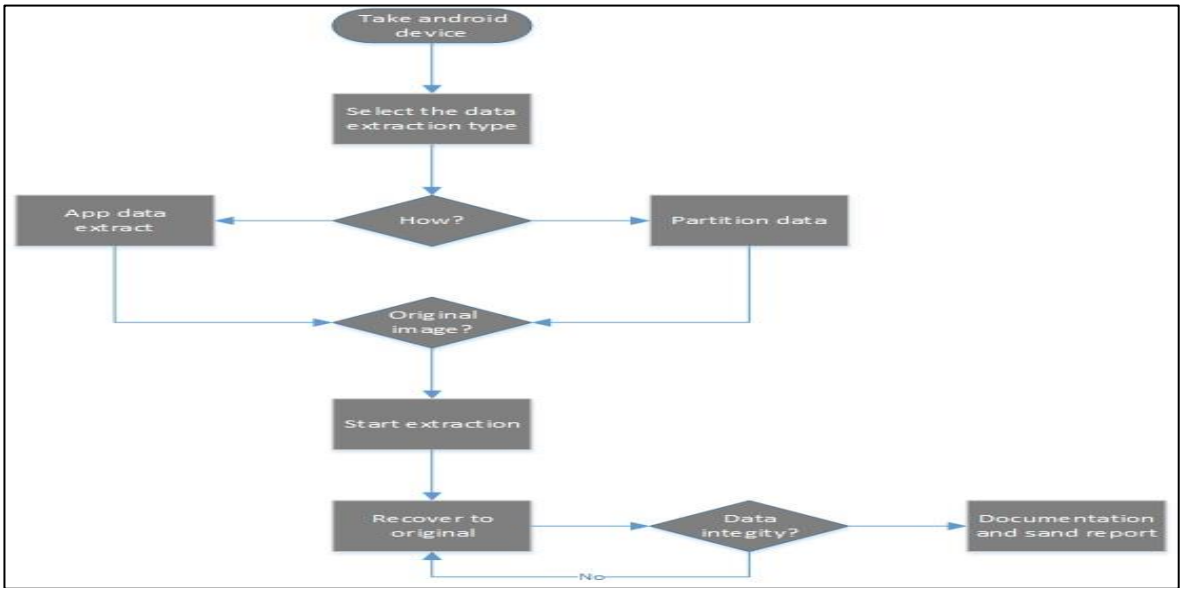

Figure 6: Simplified model perform the test.

This diagram is based in the possible use of data extraction in android devices, like app data extraction or partition data. To collect image from the device and start the extraction.

VIII. CLONCUSION

This kind of process must held by a forensics analysis, acting respectfully and following the pattern of the country. This propose presents a simplified form and useful, considering the steps present in this paper.

At the end of this process, is possible to perform a forensics analysis with more agility, and following safety rules, considering, in superficial form, all possible scene that can occur in a seizure and analysis.

The diagram can be use in decision and to perform forensics test in android devices. This way, was presented a clean and easy way to proceed with tests, using technics and efficient ways applied to Android.

REFERENCES

1. Simão AML. Proposta de método para análise pericial em SMARTPHONE com sistema operacional Android. Dissertação UNB, 2011.
2. Campbell A, Choudhury T. From Smart to Cognitive Phones. Smartphones, roy want. 2012.
3. Song,Hee-Chan, Analysis of the global smartphone market and the strategies of its major players.Hanyang University.
4. IBGE, PNAD 2013. Rio de Janeiro, 2014.
5. Wink GL. Desenvolvimento de Soluções de Dispositivos Móveis na Área da Saúde. Porto Alegre, 2012.
6. Silv ES. Inteligência coletiva sob controle? A hegemonia do Google e seu domínio, apropriação e mediação da informação. João pessoa, 2014.
7. Mendonça VRL. Bittar TJ, Dias MS. Um estudo dos Sistemas Operacionais Android e iOS para o desenvolvimento de aplicativos, Instituto de Ciências Matemáticas e de Computação Universidade de São Paulo, 2012.
8. http://developer.android.com/guide/basics/what-is-android.html
9. Fayada M. Schmidt D, Johnson R. Bilding apllication frameworks: object-oriented foudantions of framework desing. john wiley & sons, 1999.
10. Simão, AML. Proposta de metodo de analise pericial em smartphones com sistema operacional android. UNB, 2011.
11. Matias RPS, Raimundo PCN, Indentifying vulnerabilities in cloud computing using penetration test. J Comput Eng Inf Technol, 2015, 4:2
12. Marjie, t. Britz. Computer forensics and cyber-crime: an introduction. Professor of Criminal Justice Clemson University3 ed. 2013
13. Son M, Lee Y, et al. A study if user integrity during acquisition of Android devicesDigital investigation. Elsevier, 2013.

BIOGRAPHY

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 4, April 2016

Matias Romario Pinheiro dos Santos, Bachelor in computer science at ESTÁCIO | CEUT (Centro de Ensino Unificado de Teresina), Master Student at UFC (Universidade Federal do Ceará) and it is one of the participants LARA group (laboratory automation and robotics applied) and Nupaccthe.

Taisa Alves Ferreira Bachelor in computer science at ESTÁCIO CEUT (Centro de Eniso Unificado de Teresina), Master student at UFPI (Universidade Federal do Piaui). Is one of the participants NUPACCTHE Nupaccthe (Núcleo de Pesquisas Avançadas em Ciência da Computação de Teresina).
taisa.tyla@gmail.com

Raimundo Pereira da Cunha Neto, has a degree in Bachelor of Computer Science For the State University of Piauí (2003) , Specialization in Specialization in Security For College St. Augustine (2005) and a Masters in Electrical Engineering from the University Federal do Maranhão (2011) .