

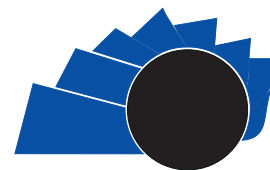


UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Visión Electrónica

Más que un estado sólido

<https://revistas.udistrital.edu.co/index.php/visele/index>



Visión Electrónica

A CURRENT VISION

Forensic analysis with hacking tools on Android devices

Análisis forense con herramientas de hacking en dispositivos Android

Yamir Alexander Arévalo Ortega¹; Sonia Rocio Corredor Vargas²; Gustavo Adolfo Higuera Castro³

INFORMACIÓN DEL ARTÍCULO

Historia del artículo:

Enviado: 14/11/2018

Recibido: 01/12/2018

Aceptado: 27/12/2018

Keywords:

Android operating system

Architecture

Forensic computer science

Hacking tools

Legislation

Mobile forensic analysis



Palabras clave:

Sistema operativo Android

Arquitectura

Informática forense

Herramientas de hacking

Legislación

Análisis forense móvil

ABSTRACT

Currently, the use of mobile terminals is becoming a necessity for a high number of people around the world which has driven the development of devices with Android operating system; In addition to this, the same indiscriminate access to resources of internet and weak local and international regulations on the use, they have become vulnerable to attacks on the network –injection of malware, ransomware–, among many others. Therefore, this article reviews the hacking tools for the forensic investigation of mobile terminals, proposing from the documentary research a forensic information acquisition model to determine tangible and significant evidences as a probative material.

RESUMEN

Actualmente, el uso de los dispositivos móviles se ha convertido en una necesidad para una alta cantidad de personas alrededor del mundo lo cual ha fomentado el incremento de dispositivos equipados con sistema operativo Android; adicionando esto al acceso indiscriminado de los mismos a recursos de internet y ante la débil reglamentación local e internacional sobre este uso, se han hecho vulnerables a los ataques a la red –inyección de malware, ransomware–, entre muchos otros. Por lo anterior, el presente artículo realiza una revisión acerca de las herramientas de hacking para la investigación forense de terminales móviles, proponiendo desde la investigación documental un modelo de adquisición de información forense para determinar evidencias tangibles y significativas como material probatorio.

¹ BSc. In Telecommunications Engineering, Electronics technologist, Universidad Distrital Francisco José de Caldas, Colombia. Member of the research group ROMA, Universidad Distrital Francisco José de Caldas, Colombia. Current position: Junior engineering IM-CE Samsung Electronics, Colombia. E-mail: rma.svc@samsung.com.co ORCID: <https://orcid.org/0000-0001-7300-4617>

² BSc. In telecommunications Engineering, Electronics technologist, Universidad Distrital Francisco José de Caldas, Colombia. Member of the research group ROMA, Universidad Distrital Francisco José de Caldas, Colombia. Current position: Software test analyst functional requirements in Data Tools S.A. E-mail: sonia.corredor@datatools.com.co ORCID: <https://orcid.org/0000-0002-6327-1938>

³ BSc. In Electronic Engineering, Universidad Distrital Francisco José de Caldas, Colombia. Current position: Professor at Universidad Distrital Francisco José de Caldas, Colombia; researcher of the research group ROMA, Universidad Distrital Francisco José de Caldas, Colombia. E-mail: gahiguera@correo.udistrital.edu.co ORCID: <https://orcid.org/0000-0001-9691-789X>

1. Introduction

At present, People from an early age initiate interaction with smartphones, tablets, and other digital devices, making these gadgets an essential part of their daily lives; many—children, adolescents, adults—are addicted to modern digital products. Not figuratively, but literally addicted, [1].

This dependence on mobile devices, especially smartphones, makes them bearers of valuable information, some private and confidential, so the user retains a reasonable expectation that these contents do not transcend to third parties, [2].

The information contained in these devices acquires great importance and value for sensitive data such as access codes or passwords to personal accounts and the registration of mobile banking apps installed in the device [3], thus becoming an attraction for hackers⁴ or criminals that lead to activities like the ransomware⁵, leaving users in position or losing their saved information or paying for its recovery; however, in case of loss or theft, the biggest problem is that sometimes the only way to recover the data is by paying the cybercriminals, and the victims tend to do so, [4].

On the other hand, most of the current mobile phones are running under the Android operating system⁶, [5]; and therefore such system has been ranked as one of the most popular in the mobile device market [6]. To the above, the mistake has been made to think that Android is the only one used in mobile devices; but it is also used in automobiles, cameras, refrigerators, televisions, game consoles, smart watches, smart glass and in many other gadgets⁷ as well, [7]. This massive use is not free of risks and the biggest concern is security. Kaspersky laboratories, says that 99% of malware studies are directed to technological devices with Android-based operating system. Cyber crooks are interested by his popularity and functionality, allowing them to take advantage of the vulnerabilities and economic profit, [8].

It is in the previous sense that, despite the various resources that provide advices on how to keep an Android device safe [9], many users do not know or follow them. From this perspective, there are two fundamental problems in the policies established by

Google Inc. for Android:

- Google does not have a standard of relentless certification applications
- Android provides too domain applications on the functions of the appliance, for this reason the user access requests based needs, [10].

Therefore, it is highly important to keep the Android operating system updated, since it is likely that hackers will attack an earlier version of it because more vulnerabilities have been discovered. More details on these parameters and their justification can be found in, [11].

In addition to the above, it is of this particular case to point out that the handling of smartphones has transcended the realization of basic tasks of voice and text communication, and it tends to the use in the handling of files, emails, and other information oriented to execute some punishable⁸ conduct, [12].

As a result, it is important to identify the tools that help to obtain information from mobile devices that are probative material in a judicial investigation, where the hacking tools serve as support in the application of forensic analysis to computer crime [13], extract the information, identify it, keep it, and interpret it in order that the findings are compelling evidence before the courts, [14].

Consequently, this article makes a documentary investigation of the different hacking tools that contribute to the establishment of an effective method for the authorities in the extraction of computer data seeking to improve the prototypes established by the judicial entities.

The article is structured as shown below: first explained the methodology of research fruit of which establish the categories and subcategories of exploration of information, where a historical account of the problem becomes framed in the past ten years, a technical description of the Android architecture, current legislation Colombian forensic analysis, the fundamental digital forensic analysis, and phases both hacking tools open source as you pay. Finally, presents a proposal that future can be implemented in a laboratory, company or society to make the process of acquiring information in forensics.

⁴ Hacker: Individual expert in the field of computer science, its main purpose is dealing with security systems and be developing continuous techniques to improve the vulnerabilities.

⁵ Ransomware: Activity of the so-called abduction of data in mobile phones.

⁶ Android: Control system on mobile terminals, tablets, clocks and other smart devices with touch screen and screen based on the free Linux software.

⁷ Gadgets: Very small and innovative devices developed to fulfill specific tasks of the manufacturers.

⁸ Punishable: typical, supervising and negligent, conduct that violates a legal right of a person.

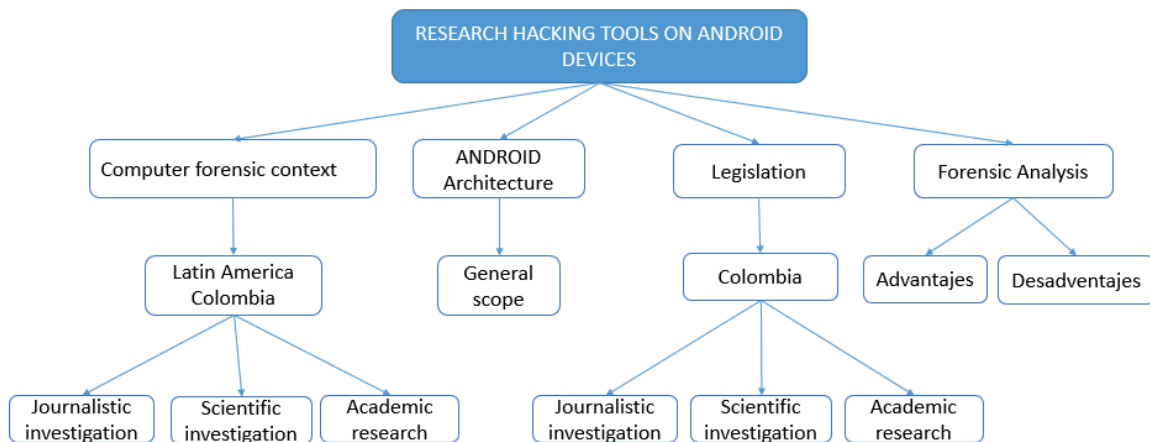
2. Methodology

The architecture of Android devices will be analyzed with the aim of establishing advantages and disadvantages of this system. Likewise, the different regulatory provisions related to data protection in Colombia will be studied, in accordance with the procedures used by judicial experts with the interest of identifying the different hacking tools [15] that serve as support to the authorities and as material academic for the development of future techniques in the application of computer forensics in Android devices.

For the exploratory study, the bibliographic search used the following databases: IEEE Xplore Digital Library, Springer Link, Scopus and SciELO

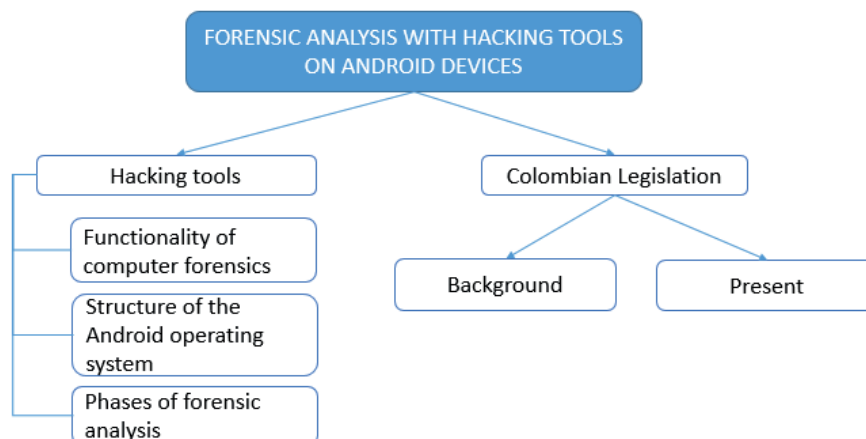
Mexico. The obtained references were determined with the key words used (Mobile forensic analysis, architecture, hacking tools, computer forensics, legislation, Android operating system) that correspond to the categories: “Forensic computer context, Android architecture, Legislation and forensic analysis”; and subcategories: “Hacking Tools and Colombian Legislation” circumscribed in Latin America and Colombia. The endorsement of this methodology was validated by experts from the Autonomous Mobile Robotic Research Group (ROMA) of the Universidad Distrital Francisco José de Caldas. The Method by indices was used for the construction of the revision (vertebrate from a general index) [16], in which the categories and subcategories are established, illustrated in Figures 1 and 2.

Figure 1. Research Hacking tools on Android devices.



Source: own.

Figure 2. Forensic analysis with hacking tools on Android devices.



Source: own

3. Development of the review

3.1. Computer forensics context


In their degree in his thesis Jaramillo D. y Torres M [17] commented that one of the problems facing the country have to do with computer security since it is one of the Nations with more vulnerabilities and cyber-attacks. On the other hand, a study prepared by the Ministry of TIC⁹ at the end of the year 2013 and subsequently published in the first quarter of 2014, indicated that 42% of the subjects had a smart cell phone, the study indicates that 43% of people who use the phone is used periodically downloading Apps from authorized sites [18].

On the other hand, there is no doubt that Latin America is today one of the largest mobile markets in the world. According to estimated eMarketer¹⁰, the number of mobile users has risen to 400 million, compared to 258 million in the United States. According to the report “Digital Future in Focus: Latin America” of comScore¹¹ in 2015, the operating system par excellence is Android.

This represents 83% of users, while iOS just concentrates on 10% and Windows barely represents 4.7%, [19]. In this sense, Deloitte¹² reports that more than half of the people who participated in the survey recorded to have used its intelligent equipment for operations of financial or commercial transactions, registering personal information and sharing information that is assumed is personal, [20].

Now, during the second semester of 2018 the Capacities Center for Cybersecurity of Colombia ‘C4’ was inaugurated, it is possible thanks to the CONPES¹³ 3854 of 2016, which has an infrastructure of more than 5,000 square meters, and which is constituted in the largest complex in Latin America to fight cybercrimes. This research complex, is located in the town of Puente Aranda in Bogotá (Colombia), it has a strategic component in equipment and forensic equipment that integrates specialized technology for the reception, projection and management of cyber incidents and ensure cybersecurity in the country through prevention, forensic cyber investigation, and strategic relationship, [21], Figure 3 and Table 1.

Figure 3. Main organizations of Digital Forensic Analysis in Colombia [17].

	DIGITAL ENTER	ADALID CORP	POLITICAL CYBERNETIC CENTER	ASOTO GROUP
YEARS OF SERVICE	21 years	10 years	14 years	20 years
ESPECIALIZATION	Leader in Professional data recovery	Specialists in new technologies	Investigation and prevention of cyber crimes	Data recovery
SERVICES	<ul style="list-style-type: none"> Data recovery Back up on site or remote Digital Forensic Analysis Total and permanent file deletion Computer expertise Recycling of media 	<ul style="list-style-type: none"> Laboratory service Technical and legal advice ISO 27001 Business Fraud Investigation Protection of brands and People on the Internet Ethical Hacking 	<ul style="list-style-type: none"> CAI Virtual Forensic Computer Lab Investigation on cases of Cybercrime and Cybersecurity 	<ul style="list-style-type: none"> Digital Forensic Laboratory Computer Security Data recovery Chain of custody for Forensic cases

⁹ TIC: It refers to the information technologies and communications.

¹⁰ eMarketer: It is a subsidiary of market research with 93% ownership that provides information and trends related to digital marketing, media and commerce.

¹¹ comScore: It is a society of marketing research on the Internet that facilitates marketing data and services to many of the companies on the Web sites.

¹² Deloitte: It prepares research and studies related to the behavior of the main industries in the local and global scope.

¹³ CONPES: National economic and Social Policy Council was created by law 19 of 1958.

Table 1. History of computer forensics [22].

HISTORICAL SUMMARY OF FORENSIC COMPUTING UNTIL 2013	
In 1984: In 1984 FBI creates "Magnetic Media Program"	In 1993: The first International Conference on Digital Evidence is held.
In 1992: The Book: "a forensic methodology for countering computer crime", by P. A. Collier y B. J. Spaul is coined the term "computer forensics".	In 1995: It was created the International Organization of Digital Evidence (IOCE).
In 1997: In December, the G8 countries in Moscow declared that "law enforcement officials must be trained and equipped to deal with high-tech crimes."	In 1998: It was created the International Association of Computer Investigative Specialists (IACIS) that will certify professionals from government agencies in Certified Forensic Computer Examiner (CFCE), it is one of the most prestigious certifications in the forensic field.
In 1999: The total work of the FBI in forensic computer science is superior to 2000 cases through the analysis of 17 terabytes of data.	In 2000: The first regional Forensic Computing Laboratory of the FBI is created.
In 2003: The total work of the FBI in computer forensic cases exceeds 6500, through the analysis of 782 terabytes of data.	

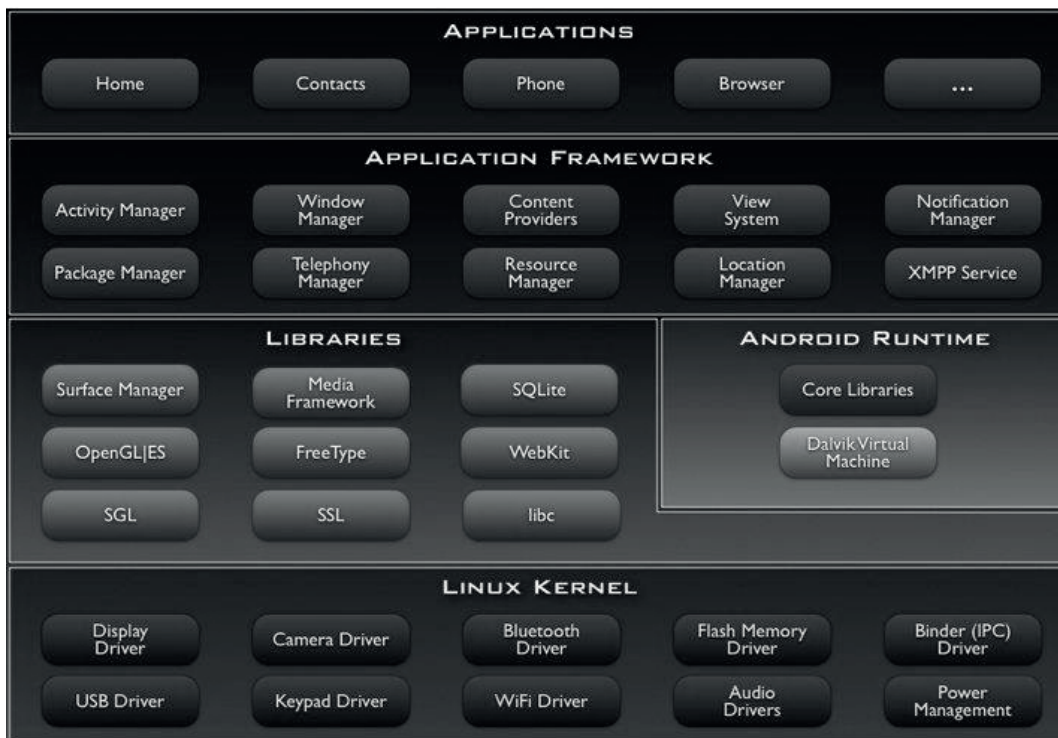
It is to say, the protection of information has been worked from all areas (legal, technical and organizational), as well as in all its dimensions (confidentiality, integrity and confidentiality); that is why the demand for professional experts in computer forensics is considerably growing. Subsequently, and according to the security division of Computerworld University, the tendency of customers today is to look for experienced professionals with highly technical knowledge and who can provide quick and real solutions in complex situations [23]. The digital expertise is the key in the courts around the world, as well as in many companies where there is a huge

interest in investigating the multiple computer attacks to which they are subjected or the cases of industrial espionage that affect their creations. All this implies that the experts of digital analysis are increasingly demanded.

3.2. Android Architecture

Android is built on an architecture formed by 4 different layers, but related among them, each layer uses services from the previous layers and offers its own to the upper layers. Figure 4 shows a global view by layers of the architecture used by Android, [24].

Figure 4. Architecture Android [25].



3.2.1. Description of the Android architecture

Applications: Here the content, both the implied default Android as the beneficiary go installing then all Apps use the API¹⁴, [26].

Application Framework¹⁵: The main idea is to improve any type of application developed. Any App that is believed to the Android OS [27], whether they are native, third companies or designed by Google, or even the customer create or manufacture, using the own set of API (application programming interface) and the identical “framework”, represented by that level.

Libraries: Developed using C/C++, these libraries form the core of Android enabling you to deliver all their capacities, [28].

Android runtime: Form the main libraries, which are bookshops [29], the Dalvik virtual machine with lots of Java classes, allowing stakeholders to perform several tasks in the same circumstances of time.

Linux Kernel: It is the heart of the Android operating system. In this layer the mandatory [30] controls so that any mechanism at the level of hardware to function. Whenever a Developer includes a new hardware module, the first thing you should do is to mount control libraries inherently this incorporated in the own Android Linux kernel.

Root User: Table 2 is a description of the advantages and disadvantages of being a user root [31] since devices from their manufacturing for safety reasons bring invalidated access.

4. Analysis of legislation in Colombia against forensic analysis

In the study of hacking tools, appears the concept of cybercrime, which has timidly approached by

Colombian legislation compared with the provisions in Regulation tabled this phenomenon at the international level, Therefore, prior to exposing the traceability of known and the computer forensics-related legislation, it is necessary to quote the scholar H. W. Torres, who developed the concept of computer crime in the universal contour by defining: “All punishable conduct¹⁶ in which the active subject uses a method or technique of a computer nature in its execution that has as a means or instrument integral elements of a computer or telematics system or legal interests protected by the right to privacy, intellectual property and software to which without being recognized by our legislator, it is accepted by international writers as Computer Infringement “, [32].

In this content, the procedure implemented by the competent jurisdiction in Colombia clarifies that for research forensic computer terminals mobile “smartphone”, are equals roughly exploring the collected information that contains messages, passwords, data, images, among others, technique that relies on a backup to extract or retrieve information located in the memory of the appliance.

Accordingly, the Colombian authorities have determined some protocols for the collection of information that serve as probative evidence in an investigation with legislative authorization, which allows to access to the information contained in smartphone mobile devices is permitted, provided such action is carried out within a judicial procedure, considering that such proof is required, in addition to reasonable and proportional, for establishing the liability of suspect or accused presenting the obtaining of such information for the evaluation of the judge’s control in the presence of the possible guilty and his defense lawyer, in respect of the constitutional right to due process.

Table 2. Advantages and disadvantages of being a Root user.

Advantages root user	Disadvantages root user
*It is gained full control over the device, both the actions to be performed and access to the entire file system (which by default is blocked for normal users). * Installation of applications that make use of typical root functionalities. * Install an operating system ROM different from the one that came from the factory with the device	* Unprotect the system, allowing that any malware applications to also access to those privileged actions and violate the security of the mobile.

Source: own.

14 API (Application programming interfaces): Allows you to create specific programs based on the set of functions or commands.
 15 Framework: It is a hierarchical and technical placement that indicates the types of software that can be developed or should be developed, so your interrelations between the layers.
 16 Punishable: Conduct that needs to be sanctioned.

Table 3. Colombian Regulations.

Law 527	Law 1273	Law 1453	Document CONPES 3701	Law 1564	Law 1581	Budapest Agreement	Decret 032	Decret 1078	Document CONPES 3854	Legal Ruling 5111
1999	2009	2011	2011	2012	2012	2013	2013	2015	2016	2017

Source: own.

As it can be seen in Table 3, in Colombia the issue of legislation since 1999 has been addressed with Law 527 “By means of which the access and use of data messages is defined and regulated (...)” [33]; One of the pillars of the Law is in the data messages, establishing the criterion to evaluate a data message probatively. Subsequently, Law 1273 of 2009 created new criminal types related to computer crimes and the protection of information and data with prison terms up to 120 months and fines up to 1,500 legal monthly minimum wages, [34].

But it is not until mid-2011 that in Colombia there is the line and orientation of the macro policy given by the CONPES (National Council of economic and social policy)–CONPES document 3701, relating the policy guidelines for cybersecurity and cyberdefense. The general objective of Document CONPES 3701 was “(i) to implement appropriate instances to prevent, coordinate, attend, control, generate recommendations and regulate incidents or cyber emergencies to face the threats and risks that threaten cybersecurity and national cyberdefense; (ii) provide specialized training in information security and expand the lines of research in cyberdefense and cybersecurity; and (iii) strengthen legislation on cybersecurity and cyberdefense, international cooperation and advance Colombia’s accession to the different international instruments on this issue.” [35].

In 2013, through the Ministry of Foreign Affairs, the country formally requested accession to the European Convention on cybercrime, it

was also known as the Budapest Convention. This agreement establishes the principles of an international agreement on cybersecurity and the sanction of cybercrimes. The same year in which the National Digital Commission and State Information Commission is created, whose object “will be the coordination and superior orientation of the execution of public functions and services related to the management of public information, the use of technology infrastructure information for interaction with citizens and the effective use of information in the Colombian State, issuing the guiding features of the Colombian Cyber Emergency Response Group of the Ministry of National Defense and advising the National Government on policies for the technology sector of information and communications, in accordance with the definition that the Law makes of them.” [36].

A new document “CONPES 3854–National digital security policy” was generated in mid-2016, whose objective was to “Strengthen the capacities of the multiple stakeholders to identify, manage, treat and mitigate digital security risks in their socio-economic activities in the digital environment.” [37].

Currently, in Resolution No. 5111 of 2017 of the Commission for the Regulation of Communications–CRC “By which the Regime for the Protection of the Rights of Users of Communications Services is established (...)” [38], the rights and obligations of users of communications services, as well as the obligations of operators to use appropriate technological tools to prevent fraud within their

networks and the duty to make periodic controls regarding the effectiveness of these mechanisms”. In this sense, the national authorities count on the collaboration of telephone and internet operators in Colombia, who are the largest distributors of mobile devices operating in the national territory with an Android system, these operators provide preliminary information to the authorities, for the identification of the users and the equipment that are placed in custody, in which the forensic analysis is developed.

4.1. Forensic analysis on mobile devices with Android operating system.

It is usually divided into five phases that help to maintain a structured study, facilitating the verifiability, the reproducibility of the analysis, these are: Preservation, acquisition, analysis, documentation and report, [39].

Presented 3 different techniques to extract evidence, [40] with advantages and disadvantages which can be seen in Table 4.

To access the evidence in a device must be account must be enabled USB debugging and if the

terminal has locked the screen must be any evasive maneuver from the computer point of view [45].

4.1.1. What can be obtained from forensic analysis?

Contacts calendar, call log, calendar-tasks, sent-received SMS, video-images, email, Internet cache, Java application artifacts, acquisition phases of mobile devices, preserving connection data, acquisition of SIM card, acquisition of internal memory (physical or logical) and finally acquisition of other digital media, [46]. The forensic process is divided into 5 stages, which are detailed in Figure 5 below.

4.1.2. Hacking tools that support forensic analysis on mobile devices with Android operating system

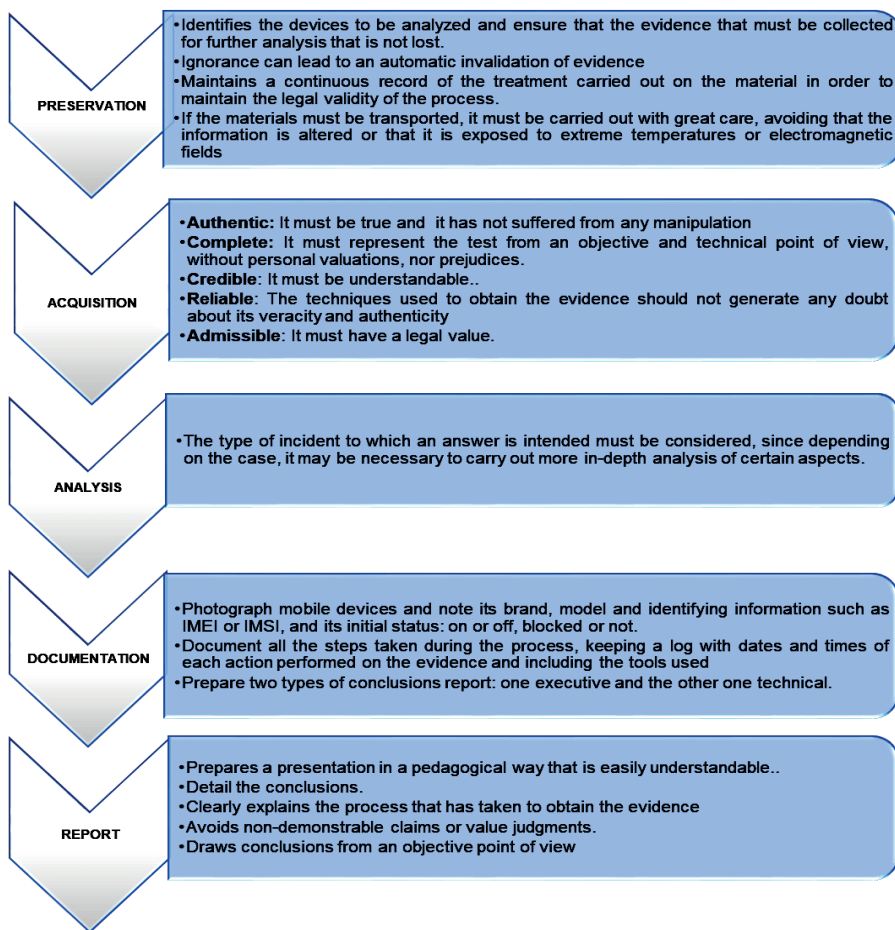
Main payment instruments have the advantage of evading defenses own operating system and follow the instructions for use, however, their disadvantage is the cost and does not guarantee full access. Below is a brief description of some tools both payment and free use.

Table 4. Advantages and Disadvantages extraction methods.

Methods	Advantages	Disadvantages
Physical acquisition [41]: It consists of making an identical replica of the original, so that all the potential evidence is preserved.	It is possible to search for deleted items and blocks that have not been marked as used.	Its complexity with respect to other methods and the time it takes to complete it
Logical Acquisition [42]: It consists of making a copy of the objects stored in the device. For this, the mechanisms implemented natively by the manufacturer are used, that is, those that are used in a habitual way to synchronize the terminal with a computer	* It is easy to get and, normally, does not require specialized hardware. * In some cases, it can be done from another device (that is, it can be tested), so the APIs of the analyzed device are not used.	* It does not copy deleted files or information that has been hidden in the file system. * It depends on the access permissions to the different files of the system.
Acquisition of the filesystem [43]: It allows obtaining all files visible through the file system, which does not include deleted files or hidden partitions	*It takes advantage of the mechanisms integrated in the operating system to perform the copying of files, Android Device Bridge (ADB [44]) in the case of Android * Recover certain information deleted	* It does not include deleted files or hidden partitions

Source: own.

Figure 5. Fundamental phases of digital forensics.



Source: own.

4.1.3. Open source

Synthesized in Table 5:

Table 5. Free hacking tools for the user.

Tool	Description
AFLogical OSE-Open source Android Forensics app and framework	It is an application in APK format that must be previously installed on the Android terminal. Once the process is finished, it allows extracting varied information to the SD card (call register, list of contacts and installed applications, text messages and multimedia) and then it must be recovered either by connecting the card to an external device or by means of the ADB, [47].
Android Pattern Lock Cracker	It is a small tool that breaks the blocking pattern on Android devices, [48].
FTK Imager Lite	It is a tool for obtaining images and previewing data used to acquire data (evidence) in a forensic manner by creating copies of data without making changes in the original evidence, [49].
LIME- Linux Memory Extractor	LiMe is a memory extractor of the Loadable Kernel Module (LKM) that allows the acquisition of volatile memory from Android devices. Tool that allows complete memory captures on Android devices, [50].
Android Data Extractor Lite (ADEL)	It is a tool developed in Python that allows obtaining a forensic flowchart from the databases of the mobile device. To be able to perform the process, it is necessary that the mobile device is rooted or have a custom recovery installed, [51].
WhatsApp Xtract	A simple tool that allows to display WhatsApp chats on the desktop computer, [52].
Skype Xtractor	ILeer and extract information from user data files of Skype's Internet telephony software. referring to contacts, chats, calls, files transferred and messages deleted, among others, [53].

Source: own.

4.1.4. Payment

Synthesized in Table 6:

Table 6. Paid hacking tools for the user.

Tool	Description
Cellebrite Touch 2	It is a comprehensive mobile forensic science solution that allows law enforcement, military, and intelligence agencies to extract test data with solid forensics, [54].
Encase Forensics	EnCase® Forensic is a powerful research platform that collects digital data, performs analysis, reports on discoveries and preserves them in a valid format for legal purposes and validated by the courts, [55].
Oxygen Forensic Suite	Among its features: Find passwords for backups and encrypted images; omit screen lock on popular devices with Android operating system; Acquire history of locations and media files of drones; extracts data from clouds: iCloud, Google, Microsoft, among others; offers import and analysis of call data records, [56].
MOBILedit! Forensic	It allows you to extract all the data from a phone with just a few clicks. This includes deleted data, call history, contacts, text messages, multimedia messages, photos, videos, recordings, calendar items, reminders, notes, data files, passwords and data from applications such as Skype, Dropbox, Evernote, Facebook, WhatsApp, Viber, Signal, WeChat and many others, [57].

Source: own.

5. Proposed alternative

This process is based on the proposed exploratory and analytical research that emerges from the technique of documentary analysis as an input to the analytical process. The development methodology of the document will be the Deming PHVA cycle (Plan, Do, Verify, Act) [58], since it has a process-based approach in order to make it easier to identify, plan, implement and improve the processes and procedures that must be followed and take it into account to achieve the goal.

To carry out this proposal, the Manual of Procedures of the Chain of Custody System is considered, which was published in 2004 by the Office of the Attorney General of the Nation [59];

however, it is important to highlight that this manual focuses only on the physical evidence not in the digital evidence, is for this reason that raised diagram of forensic analysis of Figure 6 as a method of analysis to be used by the expert computer where you can appreciate 4 stages that are implemented by the same actor in this case is the analyst, identified stages are:

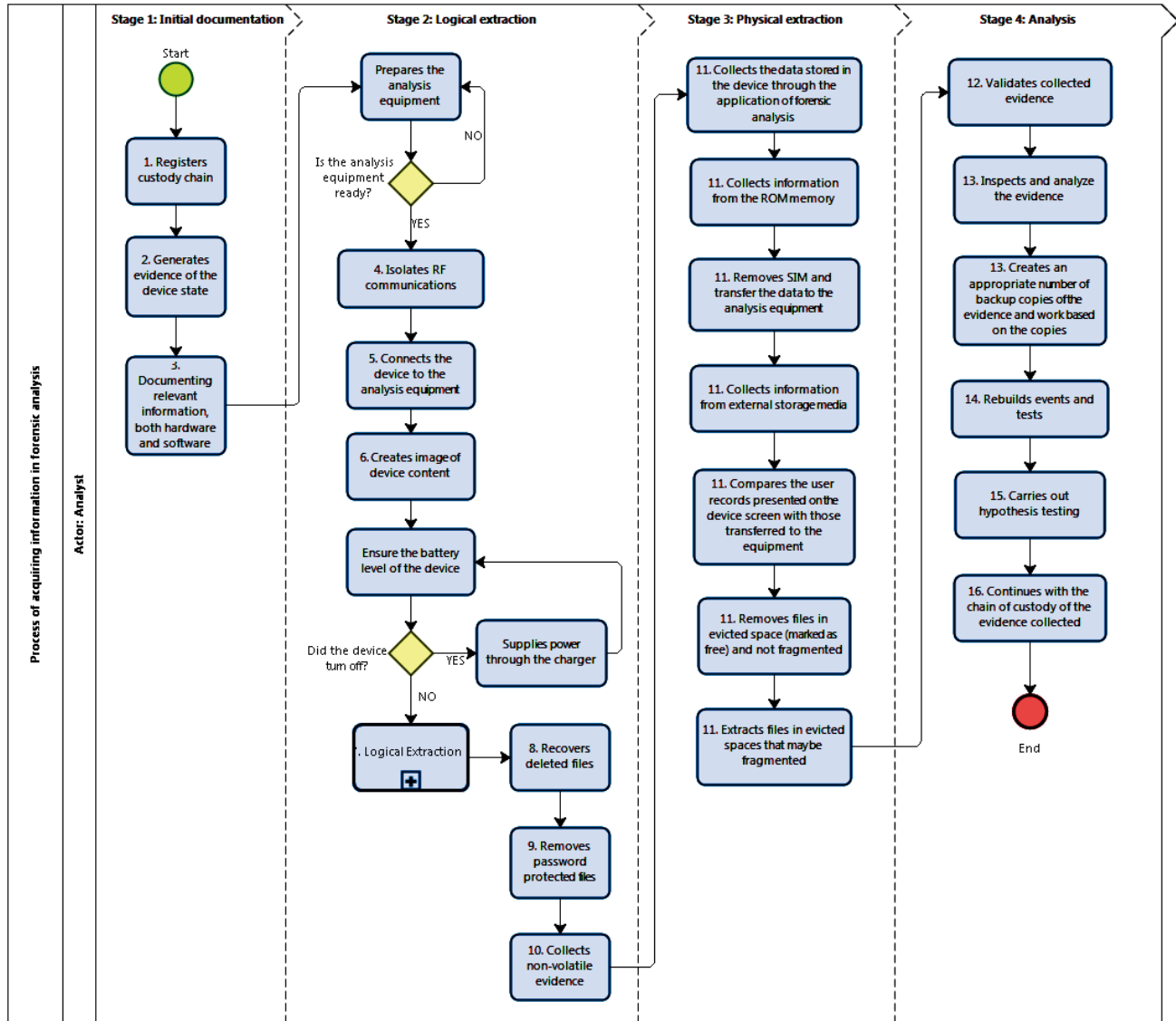
Stage 1: Initial documentation.

Stage 2: Logical extraction.

Stage 3: Physical extraction.

Stage 4: Analysis.

Figure 6. Process of acquiring information in forensic analysis.



Source: own.

Table 7. Stages of the process of acquiring information in forensic analysis.

N°	Stages	Activity	Description
1	1	Registry custody chain	Diligence in a chain custody document
2	1	Photographs Registration	The photographic record of the current state in which the mobile terminal is received and is made.
3	1	Document manufacturer and operating system information.	At a primordial level, standard forensic tools should be able to recover active data.
4	2	Isolate communications	It is recommended to submit the terminal to an RF communications isolation equipment
5	2	Connect the device to the PC	The device must be connected to the computer in charge of the analysis, using a data cable or other means accepted by the device.
6	2	Creating image of the content of the device	The forensic analyst must immediately create an image of the content of the memory by using the appropriate tools.
7	2	Extraction of information to examine	The forensic analyst must examine and classify the information by file type.
8	2	Recovery of deleted files.	Most of the operating systems do not delete the information at the moment in which a user requests the deletion of a certain file. But, in some way, they register the space occupied by that file. Analysts must use the available tools to allow recovery of deleted data.
9	2	Removing protected files with passwords	The forensic analyst must have the ability to open protected files with passwords or compressed or encrypted files.
10	2	Recovery of non-volatile evidence	Through applications, collect user data stored on the device.
11	3	Physical Extraction- ROM Memory-SIM- External storage media	Physical extraction involves searching for information directly in the data space, omitting all types of file system structure. With which the metadata is ignored and different techniques are applied on the pure content of the block in the storage device..
12	4	Validate collected evidence-Inspection and analysis of evidence	This involves the identification of relationships between the set of files linked to a particular activity and the verification of installed applications, among others.
13	4	Inspection and analysis of the evidence	The forensic analyst must inspect the content of the evidence and the extraction of the information, which is critical to prove the case. Before proceeding with the inspection of the evidence, an appropriate number of evidence backup copies should be created.
14	4	Reconstruction of Events and Test	The analyst initiates this phase with a collection of objects along with their roles and characteristics and will end up with a collection of disordered or partially ordered events that may have occurred.
15	4	Hypothesis testing	D After the events have been sequenced, the hypothesis regarding the incident can be validated. The final theory must be supported by the evidence and must offer a justification. Any confidence value that has been assigned during the reconstruction of events must be taken into account when evaluating the hypothesis.
16	4	Continue the chain of custody	The forensic analyst must perform due process, which is to have available the information to deliver the analyzed evidence in order to continue the chain of custody.

Source: own.

6. Conclusions

- Statistically in the present article, a 2% of theoretical sources taken from science and technology bibliography were identified, 39% of internet sources in the definition of technical concepts of Android architecture and a remaining 59% taken from essays, journals and academic articles for the identification of methods in the extraction of information as part of forensic analysis and hacking tools.
- As stated in this article, it is obvious that the Android operating system is the most currently embedded in mobile devices, where security problems have been found, given that the detected vulnerability allows certain Play Store applications to execute administrator commands, approving both the automatic installation of malware like access to the rest of

the system, putting in danger the information contained in the terminal as images, videos, music or documents.

- The Colombian legislative branch has made progress in the promulgation of a legal framework related to computer forensics (Law 527 of 1999, Document CONPES 3701 of 2011, Resolution 5111 of 2017). It establishes some mechanisms for the protection of digital information of users within the Colombian constitutional framework. Likewise, this framework generates tools for the authorities in search of establishing a forensic protocol that serves to advance an analysis of the devices and extract relevant information from them that provides evidentiary elements to punish the citizens who make use of them to carry out criminal behavior.

- It is considered important that a computer forensic expert must possess specialized technical knowledge, in order to obtain favorable results that can be presented as digital evidence in a judicial investigation, through the use of hacking tools.
- Colombian authorities and academic institutions must be constantly updating the technological advances developed by the international community, in order to strengthen the knowledge of its team of researchers, experts and other collaborators; to adopt new procedures in the obtaining of probative means that facilitate the judicial exercise and the decision making by the judges of the republic.
- The forensic investigation of Android mobile devices is a field of recent development in Colombia, in which the availability of technical knowledge and analysis tools are in inverse proportion to the interest generated by national authorities in the face of high demand of purchase by users; This is due to the vertiginous trade of smartphones, tablets, media players and even smart appliances. Therefore, the developers of this system will have greater interest in the expansion of these devices towards the conquest of the markets, rather than in the protection of the information handled by users.
- Based on the proposed alternative, this process can be applied or implemented to bring evidence in a satisfactory and forceful way before a court as evidentiary support, or also to any company or society that requests to solve an internal problem of computer security.

References

- [1] G. Tupper, “¿Por qué nos obsesionan las pantallas?”, 2017. [Online]. Available at: <https://www.eltiempo.com/tecnosfera/dispositivos/crece-la-adiccion-a-los-dispositivos-moviles-104940>
- [2] W. Fernández León, “La recuperación judicial de información almacenada en celulares”, 2017. [Online]. Available at: <https://www.ambitojuridico.com/noticias/columnista-impreso/penal/la-recuperacion-judicial-de-informacion-almacenada-en-celulares>
- [3] D. Jáuregui Sarmiento, “El uso de apps móviles bancarias crece más de 50% al año”, 2017. [Online]. Available at: <https://www.larepublica.co/finanzas/el-uso-de-apps-moviles-bancarias-crece-mas-de-50-al-ano-2489011>
- [4] J. M. Sánchez, “El secuestro de datos en los «smartphones» sigue aumentando”, 2016. [Online]. Available at: https://www.abc.es/tecnologia/redes/abci-secuestro-datos-smartphones-201607011330_noticia.html
- [5] S. Fernández, “Las impresionantes cifras del mercado mundial de móviles: sistemas, líneas y fabricantes”, 2017. [Online]. Available at: <https://www.xatakamovil.com/mercado/las-impresionantes-cifras-del-mercado-mundial-de-moviles-sistemas-lineas-y-fabricantes>
- [6] A. Moscaritolo, “El 99.6% del mercado móvil le pertenece a Android y iOS”, 2017. [Online]. Available at: <https://latam.pcmag.com/sistemas-operativos-moviles/18490/news/el-996-del-mercado-movil-le-pertenece-a-android-y-ios>
- [7] A. Gupta, “Learning Pentesting for Android Devices”, Packt Publishing Ltd, 2014.
- [8] Kaspersky Lab, “CIO América Latina: Increíble: El 99% del malware móvil está dirigido al sistema operativo Android”, 2012. [Online]. Available at: https://latam.kaspersky.com/about/press-releases/2012_cio-america-latina-increible-el-99-del-malware-movil-esta-dirigido-al-sistema-operativo-android
- [9] I. Khokhlov and L. Reznik, “Android system security evaluation”, 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2018. <https://doi.org/10.1109/CCNC.2018.8319325>
- [10] Symantec, “Symantec Analysis of Apple’s iOS and Google’s Android Platform Cites Improved Security over PCs, but Major Gaps Remain”, 2011. [Online]. Available at: https://www.symantec.com/about/newsroom/press-releases/2011/symantec_0627_02
- [11] I. Khokhlov and L. Reznik, “Data security evaluation for mobile android devices”, 20th Conference of Open Innovations Association (FRUCT), 2017. <https://doi.org/10.23919/FRUCT.2017.8071306>

- [12] Fiscalía General de la Nación, “Manual de Procedimientos de la Fiscalía en el Sistema Penal Acusatorio”, 2009. [Online]. Available at: <https://www.fiscalia.gov.co/colombia/wp-content/uploads/2012/03/spoa.pdf>
- [13] P. J. Arnedo Blanco, “Herramientas de análisis forense y su aplicabilidad en la investigación de delitos informáticos”, thesis MSc., Universidad Internacional de La Rioja, España, 2014.
- [14] Organización de los Estados Americanos, “Habilidades de Análisis Forense Informático”. [Online]. Available at: http://www.oas.org/juridico/english/cyb_mex_forense.pdf
- [15] K. A. Zaabi, “Android device hacking tricks and countermeasures”, IEEE International Conference on Cybercrime and Computer Forensic (ICCCF), 2016, pp. 1-10. <https://doi.org/10.1109/ICCCF.2016.7740441>
- [16] O. Londoño Palacio, L. Maldonado Granados and L. Calderón Villafañez, “Guía para construir estados del arte”, 2016. [Online]. Available at: <http://iconk.org/docs/guiaea.pdf>
- [17] D. A. Jaramillo, M. L. Torres, “Estado del análisis forense digital en Colombia”, thesis, Universidad Militar Nueva Granada, 2016.
- [18] MinTIC, “77% de las personas de estrato uno en Colombia accede a internet”, 2014. [Online]. Available at: <https://www.mintic.gov.co/portal/604/w3-article-6048.html>
- [19] Headway, “América Latina: 5 datos sobre el boom del mercado móvil”, 2015. [Online]. Available at: <http://www.headwaydigital.com/read-news-blog/32-Amrica-Latina-5-datos-sobre-el-boom-del-mercado-mvil.html>
- [20] A. M. Cataño and I. Caro, “Colombianos cada vez más conectados por medio de dispositivos móviles inteligentes: ¿Bendición o maldición?”, 2018. [Online]. Available at: <https://www2.deloitte.com/co/es/pages/about-deloitte/articles/comunicado-de-prensa-encuesta-anual-de-consumo-movil.html>
- [21] Policía Nacional de Colombia. “Policía Nacional inaugura el Centro de Capacidades para la Ciberseguridad de Colombia ‘C4’”, 2018. [Online]. Available at: <https://www.policia.gov.co/noticia/policia-nacional-inaugura-centro-capacidades-ciberseguridad-colombia-c4>
- [22] K. Córdoba. “Historia de la Informática Forense”, 2014. [Online]. Available at: <http://informaticaforensekarolcordoba.blogspot.com/2014/11/historia-de-la-informatica-forense.html>
- [23] Computerworld University, “La demanda de profesionales expertos en análisis forense informático está en crecimiento”, 2015. [Online]. Available at: <http://www.computerworlduniversity.es/actualidad/la-demanda-de-profesionales-expertos-en-analisis-forense-informatico-esta-en-crecimiento>
- [24] W. Hu, D. Han, A. Hindle and K. Wong, “The build dependency perspective of Android’s concrete architecture”, 9th IEEE Working Conference on Mining Software Repositories (MSR), 2012, pp. 128-131. <https://doi.org/10.1109/MSR.2012.6224270>
- [25] J. M. Fuentes, A. Pierra, A. Fírvida, H. Pérez, A. López and L. D. Sierra, “Android para escritorio”, *Revista Cubana de Ciencias Informáticas*, vol. 10, 2016, pp. 82-93.
- [26] G. Bavota, M. Linares-Vásquez, C. E. Bernal-Cárdenas, M. D. Penta, R. Oliveto and D. Poshyvanyk, “The Impact of API Change and Fault-Proneness on the User Ratings of Android Apps”, *IEEE Transactions on Software Engineering*, vol. 41, no. 4, 2015, pp. 384-407. <https://doi.org/10.1109/TSE.2014.2367027>
- [27] R. F. Heriniaina, “CoSINcheck to protect users from installing potentially harmful Android applications”, Third International Conference on Mobile and Secure Services (MobiSecServ), 2017, pp. 1-5. <https://doi.org/10.1109/MOBISECSERV.2017.7886564>
- [28] P. Kaur and S. Sharma, “Google Android a mobile platform: A review”, Recent Advances in Engineering and Computational Sciences (RAECS), 2014. <https://doi.org/10.1109/RAECS.2014.6799598>
- [29] Y. Zhang, J. Dai, X. Zhang, S. Huang, Z. Yang, M. Yang and H. Chen, “Detecting third-party libraries in Android applications with high precision and recall”, IEEE 25th International

- Conference on Software Analysis, Evolution and Reengineering (SANER), 2018, pp. 141-152. <https://doi.org/10.1109/SANER.2018.8330204>
- [30] P. Yuan, Y. Guo, X. Chen and H. Mei, "Device-Specific Linux Kernel Optimization for Android Smartphones", 6th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2018, pp. 65-72. <https://doi.org/10.1109/MobileCloud.2018.00018>
- [31] W. You, B. Liang, W. Shi, S. Zhu, P. Wang, S. Xie and X. Zhang, "Reference Hijacking: Patching, Protecting and Analyzing on Unmodified and Non-rooted Android Devices", IEEE/ACM 38th International Conference on Software Engineering (ICSE), 2016, pp. 959-970. <https://doi.org/10.1145/2884781.2884863>
- [32] H. W. Torres, "Derecho informático", Ediciones Jurídicas Gustavo Ibañez Ltda, 2018.
- [33] Mintic, "Ley 527 de 1999", 1999. [Online]. Available at: <https://www.mintic.gov.co/portal/604/w3-article-3679.html>
- [34] A. Canedo Estrada, "La informática forense y los delitos informáticos", *Revista Pensamiento Americano*, no. 4, 2010, pp. 81-88
- [35] Mintic, "Documento Conpes 3701", 2011. [Online]. Available at: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf
- [36] República de Colombia, "Decreto 0032 de 2013", 2013. [Online]. Available at: <http://wsp.presidencia.gov.co/Normativa/Decretos/2013/Documents/ENERO/14/DECRETO%2032%20DEL%2014%20DE%20ENERO%20DE%202013.pdf>
- [37] Departamento Nacional de Planeación, "Documento Conpes 3854", 2016. [Online]. Available at: <https://colaboracion.dnp.gov.co/CDT/Conpes/Economicos/3854.pdf>
- [38] Comisión de regulación de Comunicaciones, "Resolución CRC 5111 de 2017", 2017. [Online]. Available at: <https://www.crcm.gov.co/resoluciones/00005111.pdf>
- [39] L. Paus, "5 fases fundamentales del análisis forense digital", 2015. [Online]. Available at: <https://www.welivesecurity.com/la-es/2015/04/15/5-fases-analisis-forense-digital/>
- [40] A. Martínez, "Herramientas para realizar análisis forenses a dispositivos móviles", 2016. [Online]. Available at: <https://www.certs.es/blog/herramientas-forense-moviles>
- [41] S. C. Sathe and N. M. Dongre, "Data acquisition techniques in mobile forensics", 2nd International Conference on Inventive Systems and Control (ICISC), 2018, pp. 280-286. <https://doi.org/10.1109/ICISC.2018.8399079>
- [42] N. Y. P. Lukito, F. A. Yulianto and E. Jaded, "Comparison of data acquisition technique using logical extraction method on Unrooted Android Device", 4th International Conference on Information and Communication Technology (ICoICT), 2016, pp. 1-6. <https://doi.org/10.1109/ICoICT.2016.7571934>
- [43] Z. Wang, R. Murmuria and A. Stavrou, "Implementing and Optimizing an Encryption Filesystem on Android", IEEE 13th International Conference on Mobile Data Management, 2012, pp. 52-62. <https://doi.org/10.1109/MDM.2012.31>
- [44] S. M. Muzammal and M. Ali Shah, "ScreenStealer: Addressing Screenshot attacks on Android devices", 22nd International Conference on Automation and Computing (ICAC), 2016, pp. 336-341. <https://doi.org/10.1109/IConAC.2016.7604942>
- [45] J. García, "Adquisición forense de dispositivos Android", 2015. [Online]. Available at: <https://myslide.es/technology/que-esconde-tu-telefono-adquisicion-forense-de-dispositivos-android.html>
- [46] G. D. Presman, "Introducción al Análisis Forense de Dispositivos Móviles", 2010. [Online]. Available at: http://www.presman.com.ar/admin/archivospublicaciones/archivos/Analisis%20forense%20de%20celulares_20100721064941.pdf
- [47] V. Šimić, "Open source Android forensics tools", 2014. [Online]. Available at: <https://sgros-students.blogspot.com/2014/03/open-source-android-forensics-tools.html>
- [48] A. Martínez, "Herramientas para realizar análisis forenses a dispositivos móviles", 2016,

- [Online]. Available at: <https://www.certs.es/blog/herramientas-forense-moviles>
- [49] AccessData, “FTK® Imager Lite 3.1.1”. [Online]. Available at: <https://marketing.accessdata.com/ftkimagerlite3.1.1>
- [50] Darknet, “LiME – Linux Memory Extractor”, 2015. [Online]. Available at: <https://www.darknet.org.uk/2015/10/lime-linux-memory-extractor/>
- [51] Informático Forense Madrid, “Herramientas para análisis forenses a dispositivos móviles”, 2018. [Online]. Available at: <http://informatico-forense-madrid.es/herramientas-analisis-forense-moviles>
- [52] A. Latorre, “WhatsApp Xtract y WhatsApp Sniffer: explotando los fallos de seguridad de WhatsApp”, 2012. [Online]. Available at: <https://elandroidelibre.elespanol.com/2012/05/descubre-el-otro-uso-de-whatsapp-con-whatsapp-xtract-y-whatsapp-sniffer.html>
- [53] Simple Carver Suite Features, “Skype Extractor”, 2006. [Online]. Available at: <http://www.simplecarver.com/tool.php?toolname=Skype%20Extractor>
- [54] P. Tikvah, “Cellebrite presenta la plataforma UFED Touch2”, 2016. [Online]. Available at: <https://www.cellebrite.com/es/press/cellebrite-presenta-la-plataforma-ufed-touch2/>
- [55] Ondata, “Encase forensic software: características y funciones”. [Online]. Available at: https://www.ondata.es/recuperar/encase_forensic.htm
- [56] Oxygen forensic, Advanced software to extract data from multiple sources”. [Online]. Available at: <https://www.oxygen-forensic.com/en/>.
- [57] MOBILedit, “Forensic Express”, 2018. [Online]. Available at: <https://www.mobiledit.com/forensic-solutions/>
- [58] L. E. Larrota, J. M. Martínez and V. F. Orjuela, “Diseño de una guía para la auditoría de análisis forense en dispositivos móviles basados en tecnología Android para legislación colombiana”, thesis, Universidad Católica de Colombia, 2014.
- [59] Corte Constitucional de Colombia, “Sentencia C-186/08”, 2008. [Online]. Available at: <http://www.corteconstitucional.gov.co/relatoria/2008/C-186-08.htm>