NOVA IMS Information Management School

MGI

Mestrado em Gestão de Informação
Master Program in Information Management

Toolbox Application to Support and Enhance the Mobile Device Forensics Investigation Process

Breaking Through the Techniques Available

Bruno Miguel Vital Bernardo

Dissertation presented as partial requirement for obtaining the Master's degree in Information Management

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

NOVA Information Management School

Instituto Superior de Estatística e Gestão de Informação

Universidade Nova de Lisboa

TOOLBOX APPLICATION TO SUPPORT AND ENHANCE THE MOBILE DEVICE FORENSICS INVESTIGATION PROCESS – BREAKING THROUGH THE TECHNIQUES AVAILABLE

by

Bruno Miguel Vital Bernardo

Dissertation presented as partial requirement for obtaining the Master's degree in Information Management, with a specialization in Knowledge Management and Business Intelligence

Advisor: Professor Doutor Vitor Manuel Pereira Duarte dos Santos

January 2021

ACKNOWLEDGEMENTS

I would like to express here my full gratitude and appreciation to Professor Dr. Vitor Duarte dos Santos of NOVA IMS, for being so supportive since the day 0 of this master thesis. Together with him, we planned and drew from the beginning the strategy that we would intend to pursue to embrace this very challenging theme and project. Thank you, Professor, for always believing that I was capable of embracing and studying this field and for being always, always available to meet and to help. Likewise, I would like to thank once again to the professor for challenging me to seek to publish this work and to communicate to this science, our project and its insights. I am absolutely pleased and glad that our paths crossed.

I would also like to thank and appreciate all the participants of the focus group meeting, for their availability specially during this pandemic context and for the very important and meaningful insights and guidance. It was very crucial for this work to discuss it with them as their participation was very constructive, allowing for a clear understanding of the reality that this field is currently facing and what are and could be the greatest challenges that it may face. A very special acknowledgement to you.

Likewise, I would also like to thank PwC Portugal, the company that I work for, for the support given.

Lastly, but by no means least, I would also like to thank and dedicate this work to my family, especially to my Parents, to my Grandparents and to my Girlfriend. No feeling can be put into words to express my appreciation, acknowledgement, and thankfulness for believing and betting in me no matter the circumstances, making me feel that I was capable of reaching any high bar that I could dream of and surpass any obstacle that may appear. I also leave here a special thank you and dedication to my Aunt, who was always there whenever I needed and was a crucial and vital help for this work.

ABSTRACT

One of the main topics that is discussed today is how can a person leverage on technology on a positive and secure way in order to enhance their daily life, making it a healthier, more productive, joyful and easier. However, with improvements in technology, comes challenges for which there is not yet a stable and safe way to overcome. One of the greatest challenges that people are faced has to do with their concern on their privacy and on the safeguard of their sensitive information that is stored in any device that one uses. In fact, one of the most used technology is the Mobile, which can take several forms, features, shapes, and many other components. In line manner, cybercrime is growing rapidly, targeting the exploitation and retrieval of information from these gadgets. Even so, with a Mobile, comes several challenges including a rapidly dynamic change in its landscape, an ever-increasing diversity of mobile phones forms, integration of the information on a Mobile into the Cloud and IoT. As such, it's vital to have a stable and safe toolbox that will enable a digital investigator to potentially prevent, detect and solve any issue that may be related to Mobile Device Forensics while solving out various investigations, being it criminal, civil, corporate or any other.

KEYWORDS

Digital Forensics; Digital Archaeology; Mobile Device Forensics; Digital Evidence; Design Science Research

PUBLICATIONS

Before the publication and defense of this Master thesis, one had the opportunity to publish the work developed during the systematic literature review that resulted from the application of the PRISMA methodology. As such, this work was published in 33 pages in the Handbook of Research on Cyber Crime and Information Privacy (2 Volumes) as a book chapter, namely, in the Chapter 14 – Mobile Device Forensics Investigation Process: A Systematic Review, written by the author of this thesis Bruno Bernardo, together with Professor Dr. Vitor Santos, who is the advisor for this thesis and work.

Reference of the book: Cruz-Cunha, M., & Mateus-Coelho, N. R. (2021). Handbook of Research on Cyber Crime and Information Privacy (2 Volumes). IGI Global.

Reference of the chapter: Bernardo, B., & Santos, V. (2021). Mobile Device Forensics Investigation Process: A Systematic Review. In Cruz-Cunha, M., & Mateus-Coelho, N. R. (Ed.), Handbook of Research on Cyber Crime and Information Privacy (pp. 256-288). IGI Global.

INDEX

LIST OF ABBREVIATIONS AND ACRONYMS

IoT Internet of Things

IT Information Technology

OS Operating System

iOS iPhone Operating System

DSR Design Science Research

MSC Mobile Switching Center

HRL Home Location Register

VLR Visitor Location Register

GSM Global System for Mobile Communications

SIM Subscriber Identity Module

SMS Simple Message Services

ICCID Integrated Circuit Chip Identifier

ROM Read-only Memory

RAM Random Access Memory

OS Operating System

ESN Electronic Serial Number

MEID Mobile Equipment Identifier

IMEI International Mobile Equipment Identity

TAC Type Allocation Code

SD Card Secure Digital Card

MMS Multimedia Messaging Services

EEPROM Electronic Erasable Programmable Read Only Memory

UFED Universal Forensics Extraction Devices

USB Universal Serial Bus

1. INTRODUCTION

1.1. BACKGROUND AND PROBLEM IDENTIFICATION

Today, one of the main topics regarding technology, is related to how can a person leverage on these devices on a positive and secure way in order to enhance one's daily life, making it a healthier, more productive and easier one. However, with this comes challenges that concern people's privacy and the safeguard of their sensitive information. In fact, one of the major technologies used is the Mobile Phone, which can take several brands, formats, and features (Klomklin & Lekcharoen, 2016). According to Chernyshev et al. (2017), analysts expect that by 2020, smartphone usage and its network traffic will explain the utmost part of all internet traffic flow.

These devices and its technology are printed in today's society being it fully integrated on the daily routine of most people, from all the ages one can sought (Zhang et al., 2017). It works just like a functional and capable computer system that contains a "treasure trove of data", allowing the user to compile and share documents, multimedia, logs, applications data and performing many other activities with different purposes, while fitting in a pocket (Graves, 2013). Likewise, mobile phones are also being used together with several different applications that can be obtained via downloads from the app store of the mobile phone system operator, being this download of applications growing every year, indicating that the number of users of third-party applications are increasing at the same rate, creating new and different challenges (Ryu et al., 2018).

With mobiles phones come challenges including a rapidly dynamic change in its landscape, an ever-increasing diversity, the integration of its data into the Cloud and into the Internet of Things. In line manner, cybercrime is growing rapidly, targeting the exploitation and retrieval of information from mobiles, thus increasing the importance of Forensics and its branches Digital and Mobile Forensics (Sathe & Dongre, 2018; Omeleze & Venter, 2013).

Henceforth, these data can be used in many purposes, being one of them related to Forensics, which can leverage on a phone's data and information to solve various cases, being potentially the solution to one or playing a crucial role in its result. As such, this dissertation will present the existing tools and techniques that are important for an investigator to be able to prevent, detect and solve any issue that may be related to one's mobile, being it criminal, civil, corporate or any investigation (Jadhav & Joshi, 2016).

Indeed, as a result of the increasing adoption of IT, and the criminal activity that comes along with it, there was the need to introduce the Digital Forensics, which has now evolved into many unique areas from which one can highlight the "Computer Forensics, Network Forensics, Malware forensics, Database Forensics and Mobile Forensics" (Chernyshev et al., 2017: 43). The later one, Mobile Forensics presents itself as a subdiscipline and a branch of Digital Forensics, being it the activity of recuperating digital evidence that resides on a mobile (Omeleze & Venter, 2013).

This field, Mobile Forensics represents one of the most challenging, multipurpose, and heterogeneous field (Chernyshev et al., 2017). In fact, Graves (2013) argues about it as something that there is "no greater challenge to a digital investigator than Mobile Forensics". This is explained by the diversity among mobile devices, its "hardware and software specifics" like the type, the model, supporting OS and other supported features (Chernyshev et al., 2017: 45). What's more, the features can include mobile identifiers, contacts, email, documents, web activity, calendar, calls and messaging registry, photographs, music, video, location information, applications and tools, backups (Chernyshev et al., 2017). In fact, several authors consider that there is no greater challenge for an investigator than the Mobile Forensics, as there is a plethora of data in several, being vital for a digital investigator to acknowledge where to begin locating the data and how to retrieve it (Graves, 2013).

Nonetheless, the Mobile Forensics is being faced with distinct challenges, namely, the lack of tools and standard proven methodologies and documentation that allows one to acknowledge the data that mobiles store, and where to find and retrieve it (Chernyshev et al., 2017). In addition to this, there are challenges originating in the lack of guides available for some models and tools, which seldom provide specific and complete guidance; the higher usage of the IoT and the Cloud, used as an information warehouse and as a service that allows users to exchange and retrieve information; the technology innovation, fast improvements which makes it hard to sustain up-to-date tools; the more robust data protection procedures and a unceasingly shifting corporate attitude (Chernyshev et al., 2017; Omeleze & Venter, 2013).

Accordingly, after acknowledging the limitations that this field has been facing over the years, one can denote a gap that is yet to be clear and explained and that urge the need to be known and potentially implemented. This gap refers to Mobile Forensics as not being able to keep up with the technology advances, the potential that a Mobile has, namely its features and the type of data that it can create, contain, modify, transfer, and store. More so, there is not yet a stable artefact that will allow for a digital investigator to pursuit its activity in a universal, standard, consistent, and stable way, independently of its objective. This artefact could correspond to a tool, a model, a methodology or an informational resource. (Ostrowski et al., 2012). As such this dissertation aims to understand the power and importance that phones can have in Forensics, how phones work, its processes, and its major components. After locating the data, it is relevant to have tools that allow an investigator to retrieve and have access to its content and metadata. Being Mobile Forensics, a complex topic, as there are different devices available, there is not yet a clear definition of the tools to sort the information needed from a mobile and to answer to any issue that an investigator may have.

Additionally, to understand the power that mobiles can have in Forensics, namely in legal cases, one has to understand how these devices work, both focusing on the software and hardware that composes these devices, but also, at the user experience while using a mobile phone (process and components wise), allowing one to get a deeper and more complete understanding on the mobile environment, namely around where the data can be found, as it can be on the mobile or on its SIM/Memory Card.

Furthermore, to obtain a wider knowledge, one should have an overview of the landscape regarding data gathering techniques that will allow a digital investigator to pursue a Mobile Forensics examination process. According to Zhang et al. (2017), one can denote three types of data acquisition from a mobile. The manual methodology embodies the technique of gathering data by interacting with the phone itself connecting to it e.g., via USB, whereas the logical extraction technique involves retrieving data by accessing the file system which contains several data including one that has not been removed by the user or by external interactions. The physical extraction methodology involves the acquisition of data from the physical storage retrieving obliterated data and possibly missing data.

Considering the context described above, this dissertation will acknowledge what are the techniques and methodologies available for Forensics, Digital forensics and Mobile Device forensics and how can a digital investigator leverage on it. As such, one considers that the concept of Digital and Mobile Device Forensics, Digital Archaeology and Digital Evidence are fundamental and key. Consequently, one intends to describe and define them throughout the thesis as to yield a clear and concise definition and overview, analyzing the brief evolution, the key concepts around these terms, the different applications, the challenges, and opportunities that edge around these notions.

Likewise, this comprehensive analysis on the literature available for the topics under research is suitable to inform not only digital investigators, but also people that aspire to be one or that want to retrieve an in-depth acknowledgement on Digital and Mobile Forensics and on the methodologies and applications available to pursuit a digital investigation on devices like the mobile phone. Consequently, the next sections of this work will present the study objectives, the literature review, as well as the methodology and the next steps taken in order to reach the main objective.

1.2. Study Objectives

The main objective of this study is to propose and build a toolbox that will potentially support and improve the Mobile Forensics investigation, allowing investigators to have a fairly stable and up-to-date toolbox that will help in the investigation process, enabling for further improvements in the future. This study also aims at presenting an acknowledgement and a systematic literature review on the topics of Forensics, Digital and Mobile Forensics, which intends to support and increase the awareness and knowledge around these topics. Likewise, it is relevant to acknowledge what are the tools available and how can one leverage on it, aiming to build a toolbox that would potentially have installed the best available software to pursue the Digital Archaeology related to Mobile Forensics. As a result, one defined and elaborated the following primary research question:

*"How to build and use a **toolbox application** to support and enhance **the Mobile Device Forensics investigation process** – breaking through the techniques available".*

This research question, is supported by several sub- research questions described below:

- RQ1: What are the most relevant concepts, challenges, and opportunities around the Forensics field, as well as the different past, present and expected future applications and techniques/methods around it?
- RQ2: What is the maturity level and the relevant context around the Digital Forensics field and on the digital evidence subject?
- RQ3: What are the different existing types and forms of evidence and the cycle and phases of digital evidence collection?
- RQ4: What are the most relevant concepts and notions on the subject of Mobile Device Archaeology and the Mobile Device Forensics field?
- RQ5: What are the different environments and major components that comprehends the mobile devices and are vital to it and to its archaeology?

- RQ6: What is the type of data and information that is and can be generated, created, manipulated, and stored on cell phones and where does these activities are and can be performed?
- RQ7: How are the existing challenges and gaps around Mobile Forensics jeopardizing the Digital Forensics investigations and why is that urging to the need to have more research on this topic?
- RQ8: What are and will potentially be the major challenges and limitations that the Forensics environment is facing are that are reaching its branch and sub-branch Digital and Mobile Device Forensics, respectively.
- RQ9: How can a digital investigator leverage on the existing tools that were studied and aborded when performing a mobile device forensics investigation?

These research questions defined above, ought to create awareness and knowledge on these Forensics fields, addressing several of the issues that an investigator is facing and befalling and that are jeopardizing the Mobile Device Forensics investigation process. These questions can be answered by creating and developing a toolbox that is expected to contain tools and techniques that address several of the issues that an investigator is faced within an examination and to address the lack of knowledge and awareness on the tools and techniques. Likewise, the research questions defined will allow one to retrieve several definitions and perspectives from various literature from different a time frame and epochs that could potentially be extrapolated and leveraged when studying the Mobile Device Forensics topic. To further corroborate this, one has developed sub-objectives, that will support the primary objectives defined to study the research question mentioned above, namely the following:

- Acknowledge and obtain a dense and broad understanding on the Forensics field, its relevant concepts, its origin, history and pertinent evolution throughout time, its major challenges and opportunities and its past, present, and expected future applications and techniques/methods. Hence, allowing for the retrieval of several definitions and perspectives from various literature from different a time frame and epochs that could potentially be extrapolated and leveraged when studying the Mobile Device Forensics topic.

- Acquire a deeper and more extensive knowledge around the relevant context and concepts of the Digital Forensics field and on the digital evidence subject. Thus, understanding what the different existing types and forms of evidence and the cycle and phases of digital evidence collection.

- Understand and obtain a vast and significant notion on the subject of Mobile Device Archaeology and the Mobile Device Forensics field. Therefore, acknowledging:

    - 1) the different environment that comprehends the mobile devices;

    - 2) the major components that are vital in the mobile device and in its archaeology;

    - 3) the type of data and information that is stored on cell phones and how.

    and, performing Benchmark with other fields such as the Computer Forensics, Document Analysis, Digital Evidence, E-mail, and Cloud Forensics.

- Ascertain the existing challenges and gaps that are jeopardizing the mobile devices forensics investigations and that urged the need to have and build a toolbox that would potentially have installed the best available software to pursue an investigation related to Mobile Forensics.
- Assess and determine how mobile phones work while acknowledging what type of data it can generate, create, store, and manipulate and where these activities can be performed.
- Evaluate what were, are and will potentially be the major challenges and limitations that the Forensics environment is facing are that are reaching its branch and sub-branch Digital and Mobile Device Forensics, respectively.
- Assess and acknowledge what are the techniques and tools available for the Forensics investigation process, namely for the Mobile Device Forensics.
- Recognize how can a digital investigator leverage on the existing tools that were studied and aborded when performing a mobile device forensics investigation.

Being this objectives and sub-objectives considered, one ought to answer, understand and study the research question, by levering on topics that are considered to be highly relevant to this dissertation. Given this, one intends to study and explore the literature and notions on Forensics, Digital Forensics, Digital Archaeology and later, Mobile Device Forensics and Digital Evidence, allowing for the acknowledge of pertinent context and concepts around these subjects, that will assist one to perform and achieve a more robust and dense research.

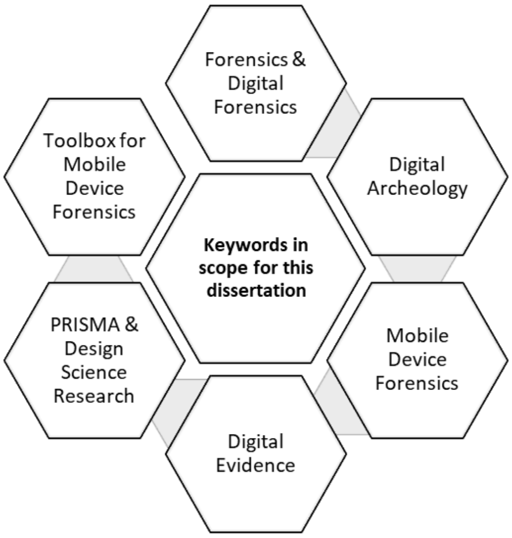

Keywords in scope for this dissertation
Forensics & Digital Forensics
Digital Archeology
Mobile Device Forensics
Digital Evidence
PRISMA & Design Science Research
Toolbox for Mobile Device Forensics

Figure 1 - Keywords relevant and in Scope for this Dissertation

Moreover, in the first part of this dissertation, one will describe in section 2, the importance, and the impact this work may have on the Digital Forensics and its Mobile Forensics field. Besides this, the paper presented follows the afore mentioned structure, designating in section 3, the systematic literature review and in section 4 the methodology that that will be applied to this research as well as the application of this methodology.

2. STUDY RELEVANCE AND IMPORTANCE

With the advances in technology, comes brand new and complex challenges and opportunities that can be exploited in a harmful and unlawful way (Chernyshev et al., 2017). As previously referred, the propagation of mobile phones has led to developments in cybercriminal actions, as they are now an enormous information repository that enables the "creation, transfer and storage" of information. (Chernyshev et al., 2017; Sathe & Dongre, 2018).

According to Jadhav & Joshi (2016), the units of hand-held devices are on the rise rapidly, where one is expecting that in 2019, there will be around 2600 million smartphone users. What's more, the smartphone market was fairly dominated by two OS, Android (Google) and the IOS (Apple) which included a combined market share of 96.7% in the first quarter of 2016. Consequently, the number of opportunities for cybercrimes has increased, due to the amount of critical data stored in a smartphone (Jadhav & Joshi, 2016). For instance, the percentage of cybercrimes involving mobile devices is intensifying distressingly, where in 2015, there was a predictable "loss of 400 billion dollars to global economy due to digital crimes" (Jadhav & Joshi, 2016: 456).

Moreover, the lack of Mobile Forensics tools generated challenges in acknowledging what type of activities and tools are available in an investigation to address all kinds of phones, hardware or software based. For instance, Graves (2013) revisits legal cases where mobile phones were pertinent to the case and its investigator, stating that there is no greater and more complex problem for a digital investigator than Mobile Forensics itself.

This dissertation proposes a different approach to this field by conglomerating and researching for all the information available and aiming at *building and using a toolbox application to support and enhance the Mobile Device Forensics investigation process by breaking through the techniques available.* Hence, enhancing the process allowing it to be effectively and efficiently applied, a process which is ought to be used as a vital foundation of an investigation, namely in "corporate, civil, criminal and military investigations" (Chernyshev et al., 2017).

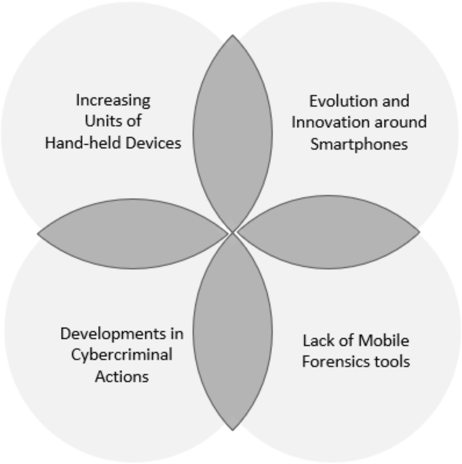

Increasing Units of Hand-held Devices
Evolution and Innovation around Smartphones
Developments in Cybercriminal Actions
Lack of Mobile Forensics tools

Figure 2 - Mobile Device Forensics Challenges

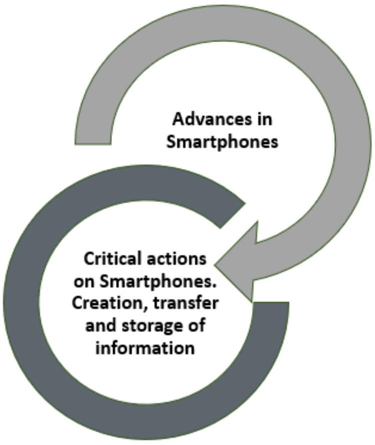

Advances in Smartphones
Critical actions on Smartphones. Creation, transfer and storage of information

Figure 3 - Importance of the Advances in Smartphones

3. LITERATURE REVIEW / THEORETICAL FRAMEKWORK

In the section of the literature Review, one intends to assemble, synthesize, and provide an overview of the disciplines and subdisciplines that are to be addressed in the existing literature and that will potentially support the research that is being performed (Palmatier et al., 2018; Snyder, 2019). By combining and assimilating "findings and perspectives from many empirical findings", one will aim to address the research question defined and uncover subjects in which more extensive research is required, generating added value to the fields under scope of this research, namely the Forensics Science field and its Digital and Mobile Forensics subdisciplines (Snyder, 2019: 333).

Given this, on this section one will explore and acknowledge the different literature available and retrieve the information that one considers to be pertinent and that will corroborate and support this research. This first step was important as to account for the literature and research available and to formulate and design the objective and scope of this literature review (Snyder, 2019). To do so, one has designed and structured this literature review, as a way to conduct a better and more extensive research on the topics that are considered and that were found to be the most relevant ones to be in-scope for the analysis that is being made on this research.

3.1. Literature Review Methodology - PRISMA

Furthermore, on the first part of this section reflects the application of the PRISMA methodology and its process flow diagram as to aid the systematic review on searching the relevant documentation and research on the topic purposed on these sections (David et al., 2015).

The second part presents the acknowledgement and exploration of all the relevant different literature retrieved through the usage of the PRISMA Methodology and through the search of keywords within different databases. This is due to the fact that the topic of Forensics and its branches can contain wide-spread information over different sources with dissimilar levels of importance for this study and so to have a more extensive and focused literature review, one leveraged on the PRISMA Methodology as a way to perform a systematic literature review around these key topics. In fact, nowadays there are countless reputable "open access journals", as well as various online search engines and internet-based university resources, being this number growing each day (Bannister & Janssen, 2019: 1; Smallbone & Quinton, 2011). As such, this allowed one to focus on the potentially most relevant concepts, setting up a path that will support the research process. The structure is flexible, allowing for the inclusion of different topics that may be considered relevant throughout the research process and that will add value to this work, and thus, it is highly pertinent to include them. Consequently, one will conduct, analyze, and write the literature review by focusing on the knowledge and information that are most relevant to the topic (Snyder, 2019).

Likewise, to better acknowledge these topics, one intends to analyze the literature available, which will allow one to leverage on the knowledge and experiences denoted and retrieved from consistent, extensive, and solid bases and sources in order to provide a robust and wide-ranging overview and literature review. Hence, this was an important step as to account for the literature and research available and to formulate and design it (Snyder, 2019).

Furthermore, throughout the initial analysis and contextualization around these referred topics, one noticed that the proliferation of the adoption of IT technologies including innovative devices, tools and all types of services and interactions that it can provide, has led to the urge of numerous and ubiquitous opportunities and challenges that are not exclusive for the Mobile Devices Forensics field, but are also impacting and influencing other various existing and emerging subdisciplines of IT Forensics, like the Cloud Forensics, Computer Forensics, Document and Email Forensics, and many other subareas of the Digital Forensics umbrella.

To perform the systematic review on what is purposed on these sections, one leveraged on the PRISMA methodology and its process flow diagram. The intent of the application of this methodology was to seek and search for the literature in any form that can be relevant and contribute to the results of this research as well as to support the research questions previously described. As such, the systematic review that is presented in this section followed the guidelines and directives of the PRISMA methodology, which stands for the Preferred Reporting Items for Systematics and Meta-Analyses. This methodology represents the collection of a minimum number of articles and/or other types of items for the purpose of the elaboration of systematic reviews and/or meta-analyses (David et al., 2015). As such, one started by considering what were the databases available for these research as well as the ones that are the most suitable for it.

Consequently, the academic resources and literature that were considered during the search around the literature available were from one general academic database that performs a search around several other databases or sites, namely the “NOVA Discovery” database. Other databases such as the “Google Scholar” and the “IEEE Xplore” (a specific database that is focused on research around technology and its environment). The search was performed by leveraging on the application and usage of Boolean logical operators and queries, i.e., AND and OR logical expressions and conditions.

These logical parameters were used and built with the intent of including all the articles and literature that were considered to be the most relevant for this research. As such, in order to identify the publications to be analyzed within the PRISMA methodology (Stage 1 – “Identification”), the following query was written and executed as to search for articles that were published and that contained either in their tittle, resume, abstract or in their full-text or keywords at least (OR logical operator) one of the subsequent terms/expressions: “Mobile Device Forensics”, “Mobile Devices Forensics”, “Mobile Device Forensic”, “Mobile Devices Forensic”, “Mobile Forensics” or “Mobile Forensic”.

As previously referred, the expressions mentioned were used together and linked between, through the application of the Boolean disjunctive logical parameter OR iteration, due to the fact that in the first stage one aimed at retrieving all the publications that would contain the expression of “Mobile Device Forensics” (main topic) or any of its derivations, as the ones written above. This listed query was executed on December 2019 on the “NOVA Discovery” database, using its advanced search engine. Consequently, in this 1st Stage, the number of records retrieved from the “NOVA Discovery” database yielded a total of 1,585 publications, being no other filters applied besides the expressions mentioned above.

Moreover, the next phase is the Screening Stage. In this second Stage, the objective was to apply the criteria chosen for the exclusion of records as to remove those that were not considered as suitable for the systematic literature review under study in this research. As a result, leveraging on the exclusion criterion that were defined, one aim to be able to remove: 1) all the publications that have not been published during the time period in scope for this analysis, namely from 01-01-2013 to 30-11-2019; 2) all the publications that are not written in the English Language; 3) all the articles that are not either in full-text or available for consultation in the database; 4) Articles that are presented duplicated; and, 5) Articles that were considered to be not suitable through the revision and analysis of their Titles and Abstracts (if applicable).

3.2. Results of the Applied Methodology

As previously referred, the systematic review that is presented in this research followed the guidelines and directives of the PRISMA methodology, which served as the basis of the work performed (David et al., 2015). Consequently, the application of the methodology helps one to draw the flowchart that is presented below, which includes the stages that correspond to the phases of the PRISMA method as well as the criteria for identification (Stage 1), exclusion (Screening – Stage 2 - 8), eligibility (Stage 9) and inclusion (Stage 10). As a result of the co-joint application of the Boolean parameters together with the keywords under scope presented in the Methodology section, a total of 1585 articles were retrieved from the initial exploration and search within the "NOVA Discovery" database (Stage 1 – Identification).

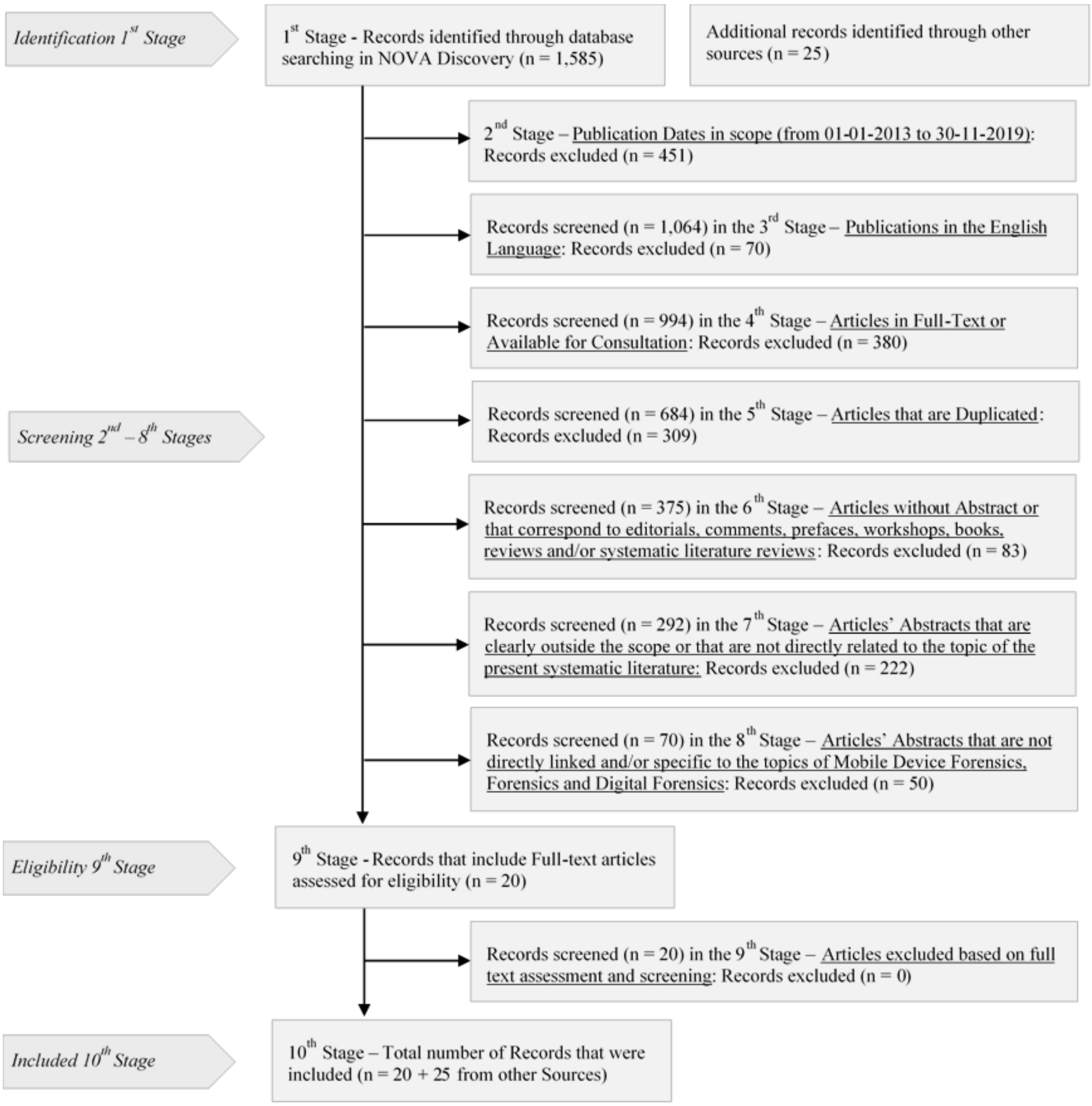

Identification 1st Stage
1st Stage - Records identified through database searching in NOVA Discovery (n = 1,585)
Additional records identified through other sources (n = 25)
2nd Stage – Publication Dates in scope (from 01-01-2013 to 30-11-2019): Records excluded (n = 451)
Records screened (n = 1,064) in the 3rd Stage – Publications in the English Language: Records excluded (n = 70)
Records screened (n = 994) in the 4th Stage – Articles in Full-Text or Available for Consultation: Records excluded (n = 380)
Screening 2nd – 8th Stages
Records screened (n = 684) in the 5th Stage – Articles that are Duplicated: Records excluded (n = 309)
Records screened (n = 375) in the 6th Stage – Articles without Abstract or that correspond to editorials, comments, prefaces, workshops, books, reviews and/or systematic literature reviews: Records excluded (n = 83)
Records screened (n = 292) in the 7th Stage – Articles' Abstracts that are clearly outside the scope or that are not directly related to the topic of the present systematic literature: Records excluded (n = 222)
Records screened (n = 70) in the 8th Stage – Articles' Abstracts that are not directly linked and/or specific to the topics of Mobile Device Forensics, Forensics and Digital Forensics: Records excluded (n = 50)
Eligibility 9th Stage
9th Stage - Records that include Full-text articles assessed for eligibility (n = 20)
Records screened (n = 20) in the 9th Stage – Articles excluded based on full text assessment and screening: Records excluded (n = 0)
Included 10th Stage
10th Stage – Total number of Records that were included (n = 20 + 25 from other Sources)

Figure 4 - PRISMA Methodology Flowchart

After reaching and setting the starting point within the 1585 articles/items, comes the phase of the screening, i.e., filtering out those that fit the exclusion criteria defined, which corresponds to the 2nd up to the 8th Stage of the flowchart presented above. To begin the screening phase, the second stage involved the removal of all the publications and articles that have not been published during the period in scope, namely from the dates of 01-01-2013 until 30-11-2019, leading to the removal of a total of 451 publications from the initial set of items that were published before or after the defined period of dates. Consequently, the 3rd stage corresponded to the screening of 1064 items, where in this stage the objective was to retrieve the publications that were written in the English Language, as such, this stage yielded a total number of 994 items, as 70 articles were removed due to the fact that its language did not correspond to the English one.

Moreover, the 4th stage addressed the 994 items that were retrieved from the previous stage, involving the removal of all the articles that were not available either in full-text or for consultation within the database that supported this analysis. This stage led to the exclusion of 380 items that did match this exclusion criteria, yielding a total of 684 items to be screened within the 5th stage. The 5th Stage aimed at the deletion of the articles that were duplicated, i.e., the same article existing twice or more in the set of 684 items. Within this stage, 309 items were removed as they represented items that were duplicated, appearing more than once in the set, as such, this yielded 375 unique items to be addressed and analyzed within the abstract screen phase which is represented by the stage 6th to 8th of the flowchart.

The Abstract screening phase was performed within stage 6th to 8th, where the focus was on excluding the items that were perceived and considered to be not suitable through the revision and analysis of their Titles and Abstracts (if applicable). As such, the first stage of the Abstract screening, the 6th stage focused on screening the remaining 375 items, excluding those that represented articles without Abstract or that correspond to editorials, comments, prefaces, workshops, books, reviews and/or systematic literature reviews. Consequently, through the analysis of the articles' abstracts (if applicable), there were a total 69 items that did not contain an Abstract, and a total of 14 that represented editorials, comments, prefaces, workshops, books, reviews and/or systematic literature reviews, which summed up to a total of 83 items removed during the 6th stage.

The next stage, the 7th stage, focused on screening the total of items that were not excluded within the previous stage, a total of 292 items. This stage focused on removing the articles that encompassed Abstracts that were clearly outside and/or not directly related to the scope of this systematic literature review. During this screen, one removed a total of 175 items that were clearly outside the objective and scope of this analysis, and a total of 47 articles that were not directly linked to the scope of this research, namely to the topic of the Mobile Device Forensics investigation process. Consequently, this resulted in an exclusion of a total of 222 items within the 7th stage.

The last stage of the Abstract screening phase was the 8th stage, where one analyzed a total of 70 items that were not excluded during the previous stages. At this stage, the main objective was to perform an additional assessment, verification, and validation of the articles' Abstract, excluding those that were not directly linked and/or specific to the topics of Mobile Device Forensics, Forensics and Digital Forensics, as well as to the topics of the digital evidence and applications around the Mobile Device Forensics field. This stage was concluded by removing a total of 50 items from the 70 articles that were yielded by the previous 7th stage.

As a consequence of the screening phase that was performed during the 2nd stage until the 8th, a total of 20 articles were considered to be suitable for full-text assessment that was performed during the 9th stage. At this stage, the 20 articles that were retrieved from the screening phase, were assessed by performing a full-text analysis of its content and its significance to the topic that is being study during this work, leading to the conclusion that all the 20 articles in scope for this stage, were considered as suitable for the present systematic literature review.

Besides this, and during the initial search process, one considered that additional records, namely linked to the topics of Forensics and Digital Forensics, that are the basis of the Mobile Device Forensics, were identified and considered to also be a vital source of information, as such an additional 25 records were identified within other sources and added to the 20 articles identified in the 9th stage.

3.3. Analysis and Discussion on the Literature Review Performed

The discussion focuses on four main topics that will be addressed throughout this research and that one considers to be crucial to provide a solid understanding of the environment and context on the research conducted around these areas. Likewise, these subjects will allow one to be able to acknowledge and reach the objective and subobjectives defined to answer to the research questions.

Moreover, despite Mobile Device Forensics being a fairly recent science that derived from Forensics and posterior from Digital Forensics, there is a scope of research and literature available on these topics which will allow one to leverage on these to study the research questions defined in section 1.2 – Study Objectives.

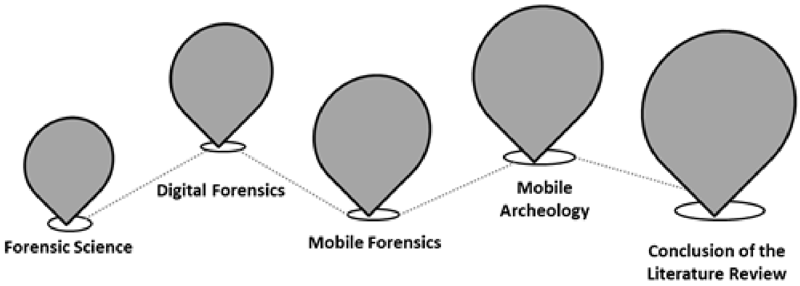


Figure 5 - Flexible Structure and Guidance of the Literature Review

The first part focus on scrutinizing the concept of the Forensics science, presenting the definition of this field, and exploring and analyzing a background synopsis on its progression throughout time, its main core areas of application, its major and more recent opportunities and challenges for organizations and individuals.

Subsequently, in the second part, one will focus on the Digital Forensics subject, understanding its main concept and existing processes and methods as well as its characteristics and available models and systems. In the third part, and after describing and studying these two umbrella subjects, the Forensics science, and the Digital Forensics science, one will introduce and scrutinize the field of Mobile Device Forensics and its components, understanding the main concepts around these areas, as well as the main methodologies, techniques and tools that are used by a digital investigator. As for the fourth part, one will describe the concept of mobile archeology as well as its main concept, strategies, challenges, and tools which are strongly related to the topic of Mobile Forensics.

3.4. The Forensics Science

3.4.1. Concept and Context

As to understand the topic that will be addressed in this research, it is important to acknowledge the concepts that regard its origin and evolution throughout time, namely, the Forensics Science discipline. In fact, there are several definitions in the literature that was under analysis, as a result of the extensive and wide-spread applications and areas of knowledges and interest that this field comprehends, and thus, one can leverage several notions that are as well important to the Digital and Mobile Device Forensics fields. Bell et al (2018) considers Forensics as “the torn between the practice of science”, and “the practices of law”, where the first practice requires one to have empirical proof of the rationality and accurateness of the techniques that are being used, and the second practice represents the techniques and approaches that are accepted grounded on the historic precedent if they have never been subject to experiential authentication (Bell et al, 2018: 4541). For Valdez (2018), Forensics, can be seen as an “emerging field” that comprehends the applications of science together with law to solve different crimes. Consequently, Valdez (2018) refers that different disciplines and subdisciplines have emerged from the Forensics science field, namely, “the digital forensics, forensic accounting, forensic toxicology, forensic odontology, and criminalist. (…) Many other areas of forensic such as forensic psychology and forensic linguistics” (Valdez, 2018: 1).

Strengthening this idea, Arnes (2018) denotes that in Forensics the application and use of science and its techniques have the intent of stablishing “factual answers to legal problems” and that the Forensics science field in its environment can be defined as the use and practice of science to law (Arnes, 2018: 2). The House of Lords (2017) defines the Forensic Science as a “complex” field, as it involves putting together a wide variety of disciplines/fields/areas from science itself, to existing law and regulation, with the aim of applying techniques to “recovery, analysis and interpretation of relevant materials and data” within a forensic examination or during a court case. (House of Lords, 2017: 4).

Furthermore, recent literature considers the Forensic field as the “science of spatial and temporal relationships between people, places and things” that are comprehended within a crime and its scene. This science is hemmed in by the law and its principles and involves matters and combination of matters that no other science disciplines do, as it is a “science of material sourcing” through the use and application of physical and produced materials and processes at its central core (Houck, 2019: 359). In the view of the authors Roux, Ribaux & Crispino (2018), the forensic discipline is considered as a traditional one that corresponds to the “linear application” of science and scientifically methodologies in a legal context, namely for court proceedings (Roux, Ribaux & Crispino, 2018: 608). Earlier these authors (Roux, Crispino & Ribaux, 2012) considered the forensic science as a “serious of scientific disciplines” that are intended to support and aid the criminal justice system, being this science, the practical and technical usage and application of various areas and fields based on the “exploitation of samples” that were retrieved from the crime scene (Roux, Crispino & Ribaux, 2012: 7).

Besides the perspectives described above, Maras & Miranda (2014) described and denoted that the Forensics science represents the discipline that applies “natural, physical and social sciences” to law and its principles (Maras & Miranda, 2014: 1). For Roux, Ribaux & Crispino (2018), this field can also be portrayed and exemplified by the action of examining and exploring the least “likely, fragmented, imperfect, uncontrolled element” in a crime scene (event), being this called the trace. This occasion has to be deciphered, unveiled and grasped to elicit knowledge on this, producing evidence and vital information that can change the course of history regarding a specific event (Roux, Ribaux & Crispino, 2018: 612).

Additionally, after acknowledging and recognizing the different views and perspectives of several authors in different time frames within the topic of Forensics Science, one can highlight that the majority of the concepts that describe the Forensics science, express the idea that Forensics corresponds to a relationship between the application of science together with law to recover, investigate, decode and understand relevant materials and data that could create new knowledge or unveil some knowledge that will ultimately be used in a relevant context, e.g. in a court proceeding. As such, in the figure bellow, one highlighted and segmented the common terms that could be retrieve in the literature analysed and explored which were then used to illustrate and explain the Forensics science concept, namely:

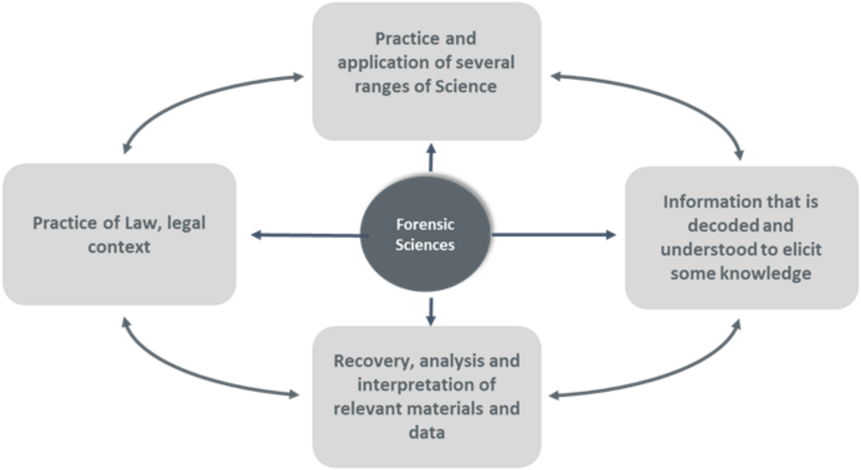

Practice and application of several ranges of Science
Practice of Law, legal context
Forensic Sciences
Information that is decoded and understood to elicit some knowledge
Recovery, analysis and interpretation of relevant materials and data

Figure 6 - Common terms used to describe the Forensics Science concept

3.4.2. Origin and Brief Evolution

After comprehending the various existing definitions around the discipline of the Forensics science, it was considered as relevant to this research, to acknowledge how the term and expression "Forensics" was coined and created, how this field has evolved throughout time, as well as how it has integrated and sustained the technology advances and the emerging fields related to the use of data analysis to evaluate massive amount of different data using different and more complex techniques.

Being this considered and going through the history of the Forensics Science along with the origin of this concept and of this word, one can denote that the word "Forensic" was coined from the Latin word "forensic", which in its essence means, "public to the forum or a public discussion". Later in time, this word gained a modern definition, which can be represented by the expression "relating to, used in, or suitable to a court of law" (Katz and Halámek, 2016: 1)

Consequently, being this definition, the most up to date one, Katz and Halámek (2016) considered that independently of the typology of the science that is being analysed or used, if it is being applied over the purpose of the law itself, it can be considered a Forensic Science. In fact, by analysing the literature available, one can denote that using science and the scientific evidence to solve a crime or an investigation is as old as the courtroom institutions themselves (American Chemical Society, 2017).

Moreover, in its origin the Forensics Science concept was coined and unveiled when the ancient scientist Archimedes, from Greece, was required and requested by the king to investigate and assure whether suspicious activities done by a goldsmith were in fact occurring. These suspicious actions that were raised by the king were whether the goldsmith had swapped silver for gold, while crafting a crown. Leveraging on his knowledge of science, Archimedes turned to water in order to find the solution and the answer for this quest. By using specific weights of the two metals, i.e., silver and gold, he measured and calculated how much litres of water each would displace. Hence, he would be able to provide the king with the answer for his suspicion, while corroborating and supporting this with scientific evidence of the goldsmith's deceit (American Chemical Society, 2017).

Therefore, literature acknowledges that even in ancient times, science was being applied together with law to unveil some sort of inference supported by evidence that were obtained as a result of the usage and application of countless different types of sciences. In fact, Houck (2019) considers that Forensics science is at its essence an "historical science" that is driven by pertinent viewpoints and techniques (Houck, 2019: 359) What's more, the difference from today's reality and the time where Archimedes applied science together with law, is the evolution of the different sciences and the technology advances that impacted each of them, bringing different and more complex challenges that the Forensics field and its subdisciplines have ever faced during its evolution

3.4.3. Existing Investigation Processes and Areas of Applications

Likewise, it is important to understand how Forensics works and what are the type of activities and steps that guide an investigation process. For Arnes (2018), a forensics practitioner needs to be accountable and responsible for associating facts related to the following interrogations: what has happened in that event/crime scene, how did it occur, who has been involved and when did it happened. Henceforth, to do so, the practitioner needs to develop, elaborate, and leverage on scientific techniques and methods and on tools in order to be able to infer on a certain investigation supported by evidence that can be considered "full cast iron certainty" (Arnes, 2018).

Regarding the Forensics activity and the investigation process itself, the House of Lords (2019) presents this process as a four-stage one, that begins with the "trace or wet forensics". At this stage, the forensic specialists conduct and conveys tests in a laboratory to detect some specific evidence, namely objects, retrieved from the crime scene that can be either linked to an action or to an individual; The second stage involves the "interpretation", i.e., the ambiguous inference and outcome from the tests that were pursued in the stage 1. During this step, a Forensics investigator associates inferences made to a certain statistical probability of likelihood of that to occur; The third stage corresponds to the "reconstruction of events", where the knowledge that were retrieved from the acquisition of evidences within the crime scene and the knowledge that were retrieved from the observation and from the testimonial of witnesses are put together by the investigator, who will try to recreate the arrangement of events that took place and that should be similar or equal to the one that is assumed to have happened in reality. The last stage, coined as the "opinion evidence", corresponds to the step where the investigator has to declare what is his/her opinion on the matter based on the analyses that were performed during the three stages and based on the skill, train and experience acquired until that moment (House of Lords, 2019).

In addition to these, Morgan et. al (2018) represented the flow of events that take place while a forensic science is applied to a crime scene to when it arrives to the court itself. These sequences of events start with the crime that was committed, followed by the evidence collection and submission all happen at the crime scene. After pursuing these two activities, the laboratory analysis and evidence interpretation take place, leveraging on the following activities, “eyewitness evidence, intelligence gathering, interview and decision to prosecute”. At the later stage, in the court, is where the presentation of the findings take place, ending with the judicial outcome.

For Houck (2019), the forensics process works according to a four-step process flow, beginning with the “detection”, where the activity of decoding and discovering objects and evidence, “things not seen” and that would remain invisible if it was not the forensics investigator. At this stage, the objective is to unveil and investigate the evidence that may be available and that may contain a meaning to the object discover in its original context. According to the author, Houck (2019), there are two types of meaning, the first is represented as the class level evidence and to discover the source of the material, e.g., “a handgun, a rock, a carpet”. The second type of meaning is embodied by “an added layer” that the criminal action associated to the object or material that was discovered, e.g., “the handgun used to shoot the victim”, and as such, the investigator is classifying the objects, which in the authors’ view is a necessary step of a forensic science. The second step corresponds to the use of multiple disciplines and to the conjunction of their methods. Following this, Houck (2019) refers that the third step should be represented by the recreation of the events that happened “a narrative” that should be the history of that crime. The final stage is characterized by the performance metrics that will be applied to measure and evaluate the result that is being delivered, namely the “accuracy, timeliness and cost” that describe the investigation that is being pursued, as such the Forensics science should convert the physical objects and information obtained from the evidence into knowledge using multiple sciences (Houck, 2019).

In addition, the processes and methods described above can be used and applied in several areas and fields. Consequently, Katz and Halámek (2016: 1), refers that the field of Forensics sciences is composed by “Forensic sciences, including, forensic chemistry, forensic biology, forensic anthropology, forensic medicine, forensic materials science, forensic engineering, computation forensics, and so on (…) forensic botany.” According to these authors, the Forensics encompasses as its most frequent applications the “fingerprints and DNA analyses, both aiming at the identification of crime victims or criminals” (Katz and Halámek, 2016: 1).

However, Katz and Halámek (2016: 1) also refer and state that “Forensics methods go much beyond (…) have been applied for forensic analysis of human or animal hair, fiber, paints and inks, and a variety of human body fluids, as well as for the detection of gunshot residues, controlled substances, explosives and other chemical and biological agents (…). As such this field can be used and applied in and within several disciplines and matters, yielding several opportunities for these field to improve and to be used together with the technology innovation and tools that characterizes the current world. Likewise, for the American Chemical Society (2017), there is also the Wildfire Forensics which leverages and uses similar means to solve mysterious animal deaths or track illegal materials; Environmental forensics cases to track down the source of pollutants or fingerprint nuclear fuels for better security” (American Chemical Society, 2017: 2).

3.4.4. Challenges and Opportunities

The literature that was analyzed and studied regarding the Forensics science seems to reflect and convey that it is crucial for the one who aspire to practice Forensics, independently of the field, to be able to understand what are the challenges that the Forensics science and its related and derived fields are facing, and that are jeopardizing the successful application of its science within an investigation process, preventing the digital investigator to reach insightful and useful conclusions and results.

In fact, the National Academy of Sciences (2009), focused on perceiving and describing what are the major challenges that are impacting the Forensics science field. For instance, accordingly, the main challenges denoted were strongly pointing to the lack of funding, the difficulty and inability in accessing the analytical tools and instruments that would allow one to purse the investigation, the lack of skilled and experienced professionals, the absence of accreditation and supervision as well as the lack of pre-set indicators and measures of the performance within an investigation and the lack of methodology to address the variability and potential bias that the Forensics science may be occurring. The House of Lords (2019) reflects that the major challenges correspond to the availability and ease of use of skills and tools, cybercrime, the magnitude of the investigations that involve forensics can have, and the connection and interface between digital evidence and physical ones. The American Chemical Society (2017), denotes that the one of the major challenges in Forensics and its fields it is the poor assessment and examinations that it involves, i.e. Forensics science seems to be falling short of scientific systematic and accurate requirements and principles and lacking ongoing supervision and evaluation of scientific methods that are to be applied, which should be “held to more rigorous standards” (American Chemical Society, 2017: 2).

Likewise, other literature such as Edmond et al. (2017: 145) refers the “Cognitive Bias” as one of the biggest challenges that a Forensics scientist may be faced. Accordingly, the authors denote that a forensic scientist is faced with the “Cognitive Bias”, meaning that 1) as human beings, people have different perceptions and experience the world in a different manner, people experience the world as the result of “an interpretive process, and depends on our attention, prior beliefs, expectations, experiences and knowledges”; 2) people’s memory is unreliable, as it may change without a person being aware of it, as such, the authors encourage forensics practitioners to leverage on documentation and empirical information, building the bridge to the memory process of “encoding, storage and retrieval”; 3) people’s context and the environment that surrounds a person and includes aspects like “mood, prior experience and peripheral information” may lead the forensic scientist to have an incorrect or a suboptimal decision-making choice; 4) “expertise is domain-task specific”, as one’s expertise is not in a straight line relocated and extrapolated from one task to another; 5) the decision-making process of forensics scientists or any expert is made normally without thinking deliberately, as humans tend to have “limited insight into how we actually made decisions”; 6) the message from a forensics scientist may not be exactly what “lay audiences hear”, in fact, experts tend to have difficulties in communicating, hence audience may retrieve a dissimilar message from that one being transmitted; 7) Edmond et al. (2017) refers that “experience does not necessarily translate into expertise”, meaning that experience in doing a certain task or job does not necessarily mean performance and precision is higher when compared to a person that has less hands-one that task or job; 8) people supervision and review may not be genuinely independent as people make different; 9) confidence seems to be a mediocre prediction of accuracy, especially when it is strengthened; and, 10) people’s feedback is vital to aid the learning process, however, many times it is not available or does not relevant for the scientist to acknowledge (Edmond et al., 2017: 145-150).

Being these challenges considered, it is crucial for the Forensics science to be able to overcome these, being several of those possibly overwhelmed by the need of the increase in studying and exploration of these topics and subjects, including more academic investigation as a way to seek for more rigorous, accurate and precise methodologies, techniques and tools that will be able to provide a digital investigator with a toolkit that will allow the digital investigator to address these challenges.

Furthermore, one acknowledged what are the different applications that Forensics and its subdisciplines can have and to what areas is it applied. According to Maras & Miranda (2014) and Arnes (2018), as any science that is used and applied to law, can be considered a forensic science, there are many branches and subdisciplines e.g., "forensics economics, forensic anthropology, forensic odontology, forensic pathology, forensic toxicology, forensic entomology, forensic psychology, forensic accounting, forensic engineering and computer forensics."

Consequently, recent literature, is exploring how can Big Data and Machine Learning improve its methods by making better and more precise techniques that are expected to generate stronger and supported conclusions. For instance, Lefèvre (2018) presented a paper on how Big data can be applied in forensic science and medicine, noticing and referring that to build a sustainable big data framework for that purpose, it has to contain and follow some actions, namely, to have structure and capabilities to process and analyze information; Training and education on these topics to improve and shape skills; and regulation and ethics.

Accordingly, Big data can provide "an excellent framework that abolishes frontiers between narrower specialties, allowing one to work with standardized tools on evidence (Lefèvre, 2018: 5). Likewise, Margagliotti and Bollé (2019) presented a paper on the topics of "Machine learning & forensic science", referring that "In digital forensics laboratories (…) the quantity of data to analyze has grown continuously in the past years", this is due to the increasing crimes involving technology itself, namely the internet. By doing so, this paper reinforces the need of the use of the machine learning algorithms to support and aid the forensic investigation processes, to handle the forensic problems if digital traces and for instance, classification algorithms are used to identify the origin of paints, using multiple chemical or physical profiles (Margagliotti and Bollé, 2019: 138).

For the American Chemical Society (2017), there are several opportunities regarding the Forensics science, namely in the advances that can impact the scientific techniques and methodology. From disciplines regarding the chemical analyses to topics involving the technology innovation like the Digital and Mobile Forensics. According to this author, even prior to Archimedes and its analyses, historical data seems to suggest that individuals did already attempted to use fingerprints or inks to study documents and its contents.

However, recent literature also shows that Forensics sciences is "at a crossroads", i.e., is at a stage where it is in need of attention namely from the science community (Bell et al., 2018: 4541). Accordingly, the authors states that "As science – and forensic science more specifically – continues to advance, it becomes increasingly absurd to ask or expect lawyers, judges and juries to take sole responsibility for critically evaluating the quality and validity of scientific evidence and testimony" (Bell et al., 2018: 4541).

3.5. The Digital Forensics Science

3.5.1. Concept and Relevant Definitions

After addressing the topic of Forensics science, it is important to acknowledge the origin and evolution of the Digital Forensics concept. As a fact, there are several definitions as a result of the extensive applications and areas of knowledge and interest that this field covers and where it can be applied and leveraged. Valdez (2018) refer that Digital forensics, was previously referred to as Computer Forensics, however nowadays this concept involves and entails testing and analysis of existing electronic devices, which can go from computers, mobile phones to printers and/or other technological machines. According to the author, this science does not intend to prove "someone's innocence or guilty. Rather, its purpose is presenting evidence found through digital forensics" (Valdez, 2018: 1).

Arnes (2018) considers that any forensic activity that is used regarding digital information represents the digital forensics activity rather than a digital investigation which corresponds to an investigation performed in the digital domain. Likewise, Carrier (2003) considers digital forensics has a discipline that has existed since computers and devices had the capacity to store data that could be employed as an evidence. For Du et al. (2017), device forensics is the science that works with files and data in a digital format retrieved from digital devices, that is nowadays urging due to the increasing appearance and innovation of brand-new and innovative technology and due to the inevitable relevance, that digital evidence may have while conducting a criminal investigation, namely those that involve digital resources.

As such, Arnes (2018: 4) regards Digital Forensics as any proved and scientifically generated technique that is applied towards "preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence" that was retrieved from a digital device and that could play an important role in the justice and crime field as well as in unveiling facts related with digital information (Arnes, 2018; Du et al., 2017). Moreover, Aziz et al. (2015), consider that the Digital Forensics science can be thought as a subject within the Information Security field, which the main objective of being able to retrieve, discover, analyse, and conclude on electronic and digital evidence. Denoting this as a process, the authors, referred that it is crucial for the process of the Digital Forensics that these evidence are kept and stored in their original state, while performing any test procedure and validating these evidences in order to reach the reconstruction of a certain event as well as to be able to derive conclusions (Aziz et al., 2015).

Furthermore, it is important to acknowledge an important concept on Digital Forensics, namely the concept of chain of custody, which represents a procedure that tracks the whereabouts of the evidence. This is highly relevant to keep and sustain the truthfulness of the evidence itself, especially if it represents an evidence relevant for a court proceeding, as there is the need to keep and account the evidence guaranteeing that it has not been meddled, ensuring the legal requirements and that the results are acceptable in the court (Valdez, 2018).

According to the author, prior to the any test or analysis of an evidence it is highly relevant to take an image of the evidence, which can be seen as a copy that will embody an "exact replica" of the original one, being this copy authenticated by the comparison of the hash value. This value denotes a "string of characters", which allows the identification of the evidence (Valdez, 2018: 2). This hash value is taken from the original evidence and then corresponded to the one from the copy, if equal the evidence is well-thought-out as not to have been tampered. Valdez (2018) suggests, as a way to prevent any modification, that “write blocks” can be used, which represents and corresponds to “products, software or hardware that are used to capture Forensics images that do not allow for one to write on it” (Valdez, 2018: 2).

3.5.2. Schemes of Evidence Classification

As for the Forensics evidence classification, Maras & Miranda (2014) denotes that there are four schemes of Forensics evidence classification. The physical evidence, where items/physical objects are essential for the case under analysis; The transfer evidence, refers to the one that results from the exchange between two physical items as a result of interaction and contact. Edmond Locard had verbalized this interaction and exchange principle, denoting that when items and surfaces “come into contact, there will be a transference of material from one to another”; The trace evidence, represents the ones like dust, hair, or earth that can be changed without one being aware of it. The pattern evidence represents the one in which its distribution can be inferred to ascertain its method of deposition as compared to evidence undergoing similar phenomena (Maras & Miranda, 2014: 2-3).

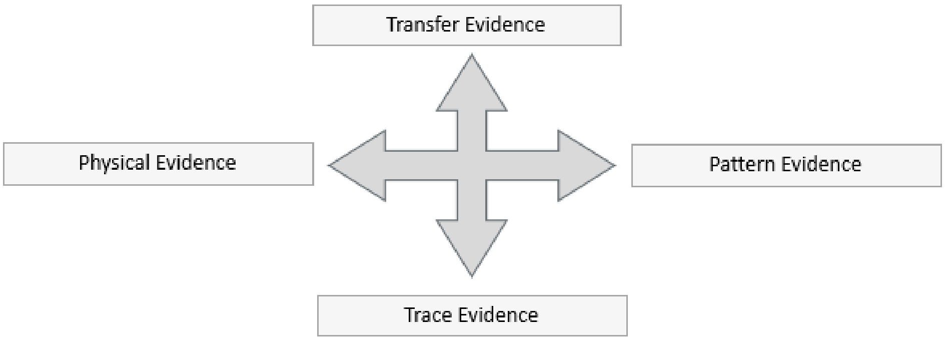


Figure 7 - Four Schemes of Forensics evidence classification

For Carrier (2003), Digital Forensics’ evidence can be classified and grouped within three categories, from which the investigator will try to split and distribute as a way to understand and acknowledge which from the data and later, evidence available belong to each of the three categories. For instance, the first category of digital evidence is the “inculpatory evidence”, which corresponds to evidence that corroborate a given premise/verdict, whereas the second category, “exculpatory evidence”, denotes the one that is used to contradict and refute a given premise/verdict. Lastly, the “evidence of tampering”, represents evidence that are available to the digital investigator, yet these evidences do not corroborate or contradicts a given theory. Nevertheless, this category allows the digital investigator to acknowledge whether the system that is under investigation was manipulated to avoid identification (Carrier, 2003: 2).

3.5.3. The Digital Forensics Process

Sönmez et al. (2017) presented the Digital Forensic Process as one that is triggered by the presence of a new crime that will lead to the emission of a search warrant. Consequently, the next phase posterior to the crime, is to visit and acknowledge the crime scene by protecting it and by photo and video recording as well as the numbering and registration of the evidence. After that, it is required for the evidence to be packed and transferred from the crime scene to a place where there will be more and better tools to test this evidence that were collected. To perform these tests, it is important to determine what is the technique that will be used, to study the image (a replica of the original evidence), to record each step taken as well as the results that were yielded by the analysis.

As a result, the next phase is the formal documentation of the methodology, the study and steps that were taken, and the conclusions that were reached, so that, it can be transformed into a report that is expected to meet the rules for the submission to authorities if necessary.

Moreover, Carrier (2003) considers that the Digital Forensic process is characterized by three main stages, where the main objective is to detect and classify digital evidence that could be a potential resource on an investigation. The stages are the 1) acquisition; 2) analysis; and 3) presentation. At the first stage, the aim is to retrieve all digital data and information that can be extracted, as at this phase the investigator does not own the knowledge necessary to know which data will be applied and used, and so, the objective is to extract as many as possible, including the allocated and unallocated areas of the memory of a device, which is called the image. The next step is the analysis, which reflects the assessment and investigation of the data collected with the intent of identifying potential evidence and patterns so that conclusions can be derived (Carrier, 2003).

Furthermore, the last step of a digital forensic process occurs once the digital investigator is able to extract, analyse, document and present the investigation that was ongoing. As such, the digital investigator has to guarantee that all the analysis and process are admissible, relevant and reliable to be presented in the court. Carrier (2003) refers that for a digital evidence to be acceptable in the court house, the digital investigator has to be able to ensure that 1) tests and analysis having been made to the procedure; 2) during the procedure and its tests, there was a known error rate defined; 3) the procedure has been shared, distributed and subject to peer review; and, 4) the procedure that is being used is widely accepted within the community that involves this science.

Furthermore, the omnipresence of mobile phones in the daily routine of people as well as the utility of its capabilities to improve people’s life and to make it a simpler and more productive one by supporting its users during several different tasks, from financial transactions and leisure activities like multimedia or social networks, to reading, learning, messaging and or contacting with other people (Saleem et al., 2016). Alike, for Su & Xi (2017), the Mobile Phone Forensics science has the main goal of acquiring and collecting relevant data from the mobile devices, parsing it, and providing comprehensive conclusions derived from this data.

3.6. The Mobile Device Forensics Science

3.6.1. Definition, Strategies and Existing Methodologies

As previously referred, the increasing Units of Hand-held devices, i.e., mobile phones, the evolution and innovation around the Smartphones industry, the developments in cybercriminal actions together with the lack of Mobile Forensics tools and accurate and precise methodology, urged to the need that this topic needs to be studied, researched, and thought.

Moreover, as advances in smartphones are leading to the possibility of critical actions to happen and to be performed at real time, namely the creation, transfer and storage of critical and personal information that should be somehow safeguard and at the same time possible to be recovered and retrieved as mobile devices have the capacity to create, manage and store information that can potentially be used as a vital source or information to the resolution to criminal cases (Sathe & Dongre, 2018; Chernyshev et al., 2017; Graves, 2013; Jadhav & Joshi, 2016). Likewise, according to Klomklin & Lekcharoen (2016), about 84% of the world population is expected to own a mobile phone in 2018, which represents an infinite quantity of data and potential vital information to be used e.g. in a crime investigation that according to the authors can be related to several types of cybercrime, from unlawful interception of data, electronic bank fraud, theft of personal and professional information, electronic vandalism and terrorism, electronic corruption and blackmail, money laundering and terrorist financing.

Consequently, as these types of crimes seem to rise in terms of occurrence, it is more than ever relevant to be able to perform a Mobile Device Forensics investigation including the possibility to retrieve and recover data that may have been store, hidden or deleted on a mobile device and that could play a crucial role in the resolution of these case. For instance, Bjornson & Hunter (2016) reflect that traditionally the focus of Digital Forensics shifted from the data that resided in personal computers to the one stored in mobile devices, being the Forensics process similar from one to each other, namely the process of obtaining an exact copy of the mobile phone guaranteeing that modifications are kept away from this copy and that this data can be later turned into information using software-based tools. For Padmanabhan et al. (2016), this field is fairly recent one, and represents an area that is emerging throughout time within the field of digital forensics. Likewise, according to Faheem et al. (2016), the Mobile Forensics science represents one that is part of the digital forensics, as it can be represented as the process of collecting digital evidence using forensic techniques and methods with the help of tools that can make it a more precise and accurate process.

Furthermore, throughout the literature available, several authors considered the Mobile Device Forensics science as one that can be viewed and drawn as a process step investigation procedure. As such, for Ayers et al. (2014), the process step that characterizes the mobile device forensic procedure, can be described as a four-stage process, being these processes structured has to guide and support the digital investigator while performing Mobile Forensics. The first stage is represented by the preservation, which represents the process of retrieving and securely obtain the suspicious mobile devices so that any modification may occur to the device and the data that it contains. For this preservation, the author refers that there are three actions that may prevent changes or modifications from happening as well as any external interactions that may be attempted by outsiders. The first procedure is to turn on the airplane mode of the mobile phone, which will block any connection to the network, Wi-fi and Bluetooth which will prevent communications from happening. The second procedure is shutting down the device, by turning it off, which will alike the first procedure block interactions from happening. Lastly, but not least, the third procedure that can be pursued is to place the mobile device into a shielded box, which will block network and radio communications from outsiders. (Ayers et al., 2014; Faheem et al., 2016; Barmpatsalou et al., 2018).

The second stage of this process is the acquisition phase, where the objective is to retrieve and gather all the data possible from the device and/or any peripheral that is being used together with the device itself. After preserving and acquiring the mobile device and the data/information that could be retrieved from it, it is important to have the right and pertinent tools available for the next stage, the examination, analysis and reporting phases, where at these stages the objective is to analyse and uncover any digital evidence that may be relevant for a given case, such as deleted or hidden data, phone calls and messages logs, pictures, documents any source of information that may be suitable to be presented at the court to corroborate any given case.

Likewise, and according to Sathe & Dongre (2018), when pursuing Mobile Forensics, one should be guided by a step wise process. At this process, the first step is described as the "Identification", where one investigator aims to scrutinize the device physically to understand and acknowledge if the mobile device will potentially be a source of information important and relevant for a criminal investigation. After doing so, the next steps are the "Preservation" and the "Acquisition", which relates to guaranteeing that the mobile phone is inaccessible from outside connections that may jeopardize the data presented within it, where as the "Acquisition" step relates to the activity of obtaining a replica of the device's image. By doing so, the investigator is mitigating the risk that the device may face namely related to the device physical condition and the battery itself.

After isolating the device and acquiring the device digital image, the next step is the "Analysis" and the "Documentation". In the "Analysis" stage, the digital investigator aims at scrutinizing the data that was retrieved from the device and the device itself so that insights and conclusions can be made that will potentially seek to be a relevant part within a criminal investigation, whereas in the "Documentation" step the objective is to formally register every activity that was taken during the investigation, so that all the steps taken to reach the final conclusions and insights are available formally and can be reperformed and audited if necessary. The final step is the "Presentation" which relates to presenting the insights and et conclusions that all the previous steps help reaching (Sathe & Dongre, 2018).

3.6.2. The Evolution of the Mobile Forensics

According to Chernyshev et al. (2017), Mobile Device Forensics is rather a newly subdiscipline of forensics, as in the pre-2007 period, the information that was available on this science, was very outdated, scarce, and poor characterized by the existence of no to limited documentation on it and on the tools that possibly existed. At this time, there were few to no applications or techniques to retrieve digital evidence from a mobile device, and the literature around this topic was focused on understanding how one could retrieve information present on the SIM Card, rather than the mobile phone itself.

Later on, between 2007 until 2010, Chernyshev et al. (2017) denotes that the Mobile Device Forensics area was first presented with guidelines from several institutions and associations, that focused on guaranteeing that a digital investigator has a device data image that would be able to correspond to the original mobile phone state when it was acquired. By doing so, a digital investigator, sidestepped from using and introducing modifications to a device as to meet this requirement defined by the guidelines, resulting in a more challenging data extraction process which yielded less evidence from that one that a digital investigator could retrieve if modifications were introduced.

From 2011 to 2016, Chernyshev et al. (2017) described that during this period, there was a greater need to acquire more digital evidence than before, this is mainly due to the increase in different and innovative technology that the world was being introduced, as such, the mobile device forensics started extending itself to wearables, cloud services and mobile applications, inventing more advanced extractions techniques that would potentially retrieve better and more evidences from this devices.

From this period onwards, the Mobile Devices Forensics science is growing at an enormous rate, following the ongoing advances and diversity in technology that are changing people's life. Likewise, the emergence of brand-new devices and different models are increasing the concern and pressure around phone providers as to increase the security of this devices, which by doing so, makes it harder for a digital investigator to retrieve data and information from these devices. However, despite the Mobile Devices Forensics science being growing at a positive rate, it is not being able to keep up with the even more faster and complex growth around the technology, its evolution and its mobile devices, that seem to evolve and to be better on a daily basis.

3.6.3. Major Challenges in the Field

Regarding, the Digital Forensics branch, the Mobile Device Forensics science, it is likewise relevant to denote the major challenges that this area has faced and is currently facing, namely when data is being extracted from a mobile device. According to Jadhav & Joshi (2016), there are several challenges that this area is facing. One regards the fact that there are several types and models of mobile phones, each with infinite specifications and settings, which result in the need for Mobile Forensics to be elastic and flexible being able to have numerous techniques that will be able to support different types of these devices. Likewise, each mobile phone contains its own built-in characteristics, which may be a potential barrier for a digital investigator when trying to access to this device and extracting information.

Moreover, Jadhav & Joshi (2016) reinforced the idea that there are forensics tools limitations, that may imply that no tool is available that can fit the purpose of accessing and extracting data of a specific phone model. Likewise, as technology evolves, so does the different types of cybercrime, namely malicious applications and files that can contain data that is corrupted due to the occurrence of viruses in the mobile phone. Additionally, Jadhav & Joshi (2016) highlighted that the data that is held on a mobile phone can be dynamic data, i.e., data that may have been modified without the investigators' notice and that may lead to misjudgements and incorrect conclusions, and that there are legal problems associated with a device being used in a e.g., international crime or at a device that belongs to the person but is company owned (Graves 2013; Jadhav & Joshi, 2016).

According to Chernyshev et al. (2017), the principal challenge that characterizes the field of Mobile Forensics, is the lack of documentation and formalization of the techniques that are used and available while pursuing an investigation, which normally consists on several steps that encompass the application of different tools and techniques, as such, and to be admissible in the court as a relevant evidence, the investigator needs to be able to document not only the methodology and techniques used but also, the findings that were achieved being able to present them to corroborate a thesis. Likewise, Omeleze & Venter (2013) highlighted that most of the frameworks and methods that exist and support the Mobile Forensics and other Digital Forensics sciences, lack the testing and procedure analysis before being fully implemented in a Forensics investigation. For Barmpatsalou et al. (2013), the lack of standardization around the Mobile Device Forensics field can be explained by the fast-paced industry of this technology and its changes, which creates greater and greater gaps between the different types and kinds of mobile phones and operating systems available.

In fact, Chernyshev et al. (2017) refer that the applications and tools that are nowadays available for a Mobile Forensics' investigator lack the capability to maintain and generate supporting documentation and log evidence of what was being performed. What's more, there is also a lack of documentation regarding on how to use these tools, what training set, and certifications are needed to be able to use these tools at their fullest, and to be able to acknowledge their capabilities. For instance, there are several tools that have limited to no documentation to support the digital investigator on how to use that specific tool. The same happens to the operating systems that each mobile phone has, due to the fact that some of them have very limited documentation available, especially the least used operating system, building a difficult challenge for the digital investigator to acknowledge where and what to look on these applications (Chernyshev et al., 2017; Omeleze & Venter, 2013).

Furthermore, Chernyshev et al. (2017) highlights that there are more challenges to the Mobile Device Forensics field and that these need to be explored and studied as they are currently jeopardizing the quality and accreditation that is given to a Mobile Device Forensics investigation. As such, the authors refer challenges like the lack of standardized and tested techniques, which are expected or could be used by a digital investigator while pursuing Mobile Forensics. For instance, there are different and divergent techniques that will depend on the mobile phone, the tool that is used, as such the lack of standardization and universal support, makes it less reliable and trusted investigation which may sound dubious in e.g., court. Besides this, the variety of different tools and its imperfections, which characterizes the applications that are available to perform Mobile Device Forensics can also present a challenge that the digital investigator is not accounting for, trusting that the application will work exactly as its value proposition says it will. However, each tool has its own configuration and features that will allow for a more in-depth or high-level analysis that can produce possibly different results and even "contrasting extraction outcomes" and can affected by vulnerabilities and software imperfections and even are possible to be corrupted and hacked.

Moreover, the interface and integration of a person's data on the mobile phone with the cloud services, making it even more difficult for a digital investigator. Cloud services nowadays allow people to perform real-time exchanges of information, both upload and download of unlimited data. Besides, there is little to no support on how to retrieve cloud information using Mobile Device Forensics tools, along with the fact that it is difficult to ensure and establish the ownership of the data that is stored in the cloud (Chernyshev et al., 2017).

In addition, and as previously referred, one of the greatest challenges that a digital investigator faces, is the lack of capability to keep up with the fast-paced environment that characterizes the mobile phone industry and market. Mobile Forensics tools are yet to be capable to sustain the technology evolution and innovation that appears day-to-day which brings complex and unknown challenges for the digital investigator. Along with this, counterfeit and modifications that are performed to the mobile phones can present an additional challenge to which the tools that are available are not able to adjust against these configurations and modifications.

Additionally, the security settings and the antiforensics, also present a relevant challenge for the Mobile Device Forensics field. In fact, as a security measure, many mobile phones manufacturers have the capacity to allow the user to perform the encryption of the user data present on a mobile phone, which is considered as a way to protect this data from outsiders. By doing so, these measures will create and lift a strong barrier that Mobile Forensics tools may not be capable to dig through. Likewise, the antiforensics techniques, which focus on creating methods that will impose Forensics from being able to retrieve data from the device and will eliminate and obfuscate the data that is on the phone (Chernyshev et al., 2017). In addition, as one of the major challenges one can describe the internet of things, as nowadays, people's mobile phone is no longer use just to establish phone calls or to send text messages, mobile phones are widely used together with different IoT, which makes it even harder for a digital investigator to be able to access to a mobile phone's memory and relevant data. Additionally, the emergence of peripheral tools that can be used together with the smartphone, and that require additional tools and methods to be able to acknowledge the information and impact that they have on the mobile phone, like the smartwatch of the fit bands that connect with the smartphone via Bluetooth (Chernyshev et al., 2017).

3.6.4. Major Opportunities in the Field

According to Chernyshev et al. (2017), despite the challenges that were denoted above, there are several opportunities for this field to both evolve and to gain a more importance in the criminal field. As such, according to these authors, one of the major opportunities is derived from the environment that surrounds the mobile device market. For instance, the mobile device market and mobile phones are growing on an ongoing fast-paced rate meaning that new technology and features are explored and delivered every day (Li et al. 2018). In fact, Mumba & Vender (2014) denote that the mobile device landscape belongs to the fastest paced evolving and innovating technologies in the past years, being mobile phones the most used form of communication in the market that is capable of having multiple features that change people's life on a daily basis. Consequently, by focusing on the key architectural and the technological aspects that the mobile phones have, the Mobile Device Forensics field could create and enhance its methodologies and capabilities leveraging on this knowledge to be able to overcome any new features or built-in technology that despite being new, the science will know how to explore it.

Likewise, as the world advances and more and new technologies come out on the market and are available for the users to buy and explore at a cheaper price, so does the integration of the mobile data and its applications with different databases, especially the clouds. As such, as there is neither a harmonized nor a universal and generic data format of the data that is on a mobile phone, the tools and applications that exist on the market will be specific to a certain data type or will be dependent on the level of knowledge and capacity of the digital investigator. Consequently, there is a great gap and need to build and develop a universal and fast extraction and analytics tool that is able to retrieve different types of data, even so, from the cloud, which is nowadays, one of the biggest storage repositories (Chernyshev et al., 2017).

Moreover, it is important that these applications that are developed can focus their analysis and extractions, as mobile phones can have an outrageous amount of data and information, which in the eyes of the digital investigator can be considered as not useful for the analysis. Being able to perform this segmentation, would mean that the applications could extract and analyses the data that is important and do it in an even faster way. Furthermore, it is also important to create more awareness around the Mobile Forensics Tools, bringing more research and important insights that will contribute much for a higher knowledge and better applications but also in a more practical and adequate training resources for a digital investigator (Chernyshev et al., 2017).

3.7. The Mobile Phone's Archaeology and Mobile Forensics Available Applications

3.7.1. Mobile Devices, Its Archaeology and Relevant Concepts

As to understand the field of Mobile Device Forensics in a greater and more in-depth level, it is relevant to understand what are mobile phones and its structure as well as how these devices work, as to acknowledge how and where could a digital investigator apply the available Mobile Forensics tools within an investigation and look to retrieve the mobile's data, any that exists in the mobile's internal and/or external memory, data that was deleted or that is hidden. As such, according to Graves (2013), mobile phones are regarded as "full-duplex" gadgets, where two people can communicate at the same moment, being it different from a half-duplex device (e.g., walkie-talkie) that only allows one person to speak at a time, and that are expected to have an estimate maximum communication distance of about 8 kms. A mobile phone can be used to perform communications across the world, as cellular towers are in place and spread all over the world building up a well-crafted network.

Graves (2013), denotes that communications are prompted by the cell towers, referring that each tower supplies and yield phone carriers with a specific number of frequencies that carriers can use. Mobile phones and cell towers leverage on the usage of a low bandwidth frequencies, allowing it to be reutilized without generating any noise or interference within a nonadjacent cell. Communications are performed following the basis that when the caller makes a mobile phone call, it is picked by the tower that is closest to him/her, and the same will happen to the receiver, as such, the signal is transmitted between the towers and relayed to the target mobile phone. The closer the tower is to the caller, the stronger the signal.

Moreover, important to notice is the Base Transceiver Station concept which corresponds to a radio that interacts and links with the mobile phone, being the Base Station Controller, the manager of the radio equipment and the assignment of the network frequency. Responsible for the switching of the network is the Mobile Switching Center (MSC). This system aims at the management of the communications within the crafted network and interfaces with the public mobile network, and as such, it should be considered to be investigated by a forensics mobile investigator whenever an investigation is taking place. This system contains databases, being them the Home Location Register (HRL) and the Visitor Location Register (VLR), allowing the MSC to process and interact with information that emerges and fluids on the network (Graves, 2013).

According to Graves (2013), the Home Location Register is accountable for the subscriber and service data, whereas the Visitor Location Register is accountable for the cell phones that are outside their service coverage area, i.e., on roaming. These two represent important databases when it comes to mobile phone communication data and can provide information on the subscriber, namely on the address, the service, log of the last locations registered in the network. This information is preserved on the HRL and utilized by the Mobile Switching Center to create detailed call records and route calls and messages.

Moreover, when it comes to the position and location of a mobile phone, it is essential to acknowledge the existence of the Global Positioning System (GPS), which nowadays contains built-in capabilities, allowing it to be tracked, hence permitting the localization of a mobile phone. To locate a phone through the usage of GPS, locating the exact position of a phone in a map, it is necessary that the GPS communicates with three satellites near its position (which is determined by the cell phone's GPS receiver), forming three circles, that will allow one to determine the location of a mobile device, the intersection of these referred circles (Graves, 2013)

Another approach to locating geographically a cell phone is the triangulation or trilateration using cell phone towers, which represents a way of triangulate "in close proximity". For instance, the triangulation between cell towers and its network happens when the first tower begins the calculation of the distance between it and the mobile phone using as a measure the signal strength and reach. After doing so, the second tower measures and calculates the distance from the mobile phone basis on the signal strength alike the first one, and from it one can derive two possible locations where the distances between the first tower and the mobile phone and the distance between the second tower and the mobile phone overlap, reducing down the mobile phone location to two possible points. The third tower will leverage on the signal of the network to track and narrow down the location of the mobile phone to a possible one, and thus locking down the position of the mobile phone.

Moreover, one of the most widely used technology nowadays, is the Global System for Mobile Communications (GSM), which represents a cellular network to which the mobile phones can connect and interact to it by searching for the cellular towers that are in its reach. The GSM involves the usage of the SIM Card Component (Graves, 2013).

Furthermore, importance to notice is the several statuses that the phone can have and what impact this can have on the work of the digital investigator. According to Faheem et al. (2016), the phone status embeds four sub-functions, being the first the screen lock, which if it is enable may require the user to insert a pin-code, login through face id, or fingerprint reader, or through the draw of a pattern that connects dots. These options may represent that the users' phone does not have a lock screen type, which means that the phone will be awake by pressing any key without needing any security type to unlock the phone. The second sub-function is the screen- saver, which can be activated or de-activated by the user's configurations. The third and four functions are represented by the developer option and the flight mode, respectively, being the first an option that allows the user to set more complex parametrizations and settings over the phone, and the second as mentioned before, will block any communication that the phone may attempt. For Faheem et al. (2016), the other functions may involve the emails that are configured on the mobile phone, and the applications that are installed and ready to be used, which include, third party apps (apps installed by the user), disabled and deleted apps. Likewise, functions like reviewing the wi-fi and browser configurations and history are also relevant, as well as the SIM card functions including the calls and messages logs that it registers.

3.7.2. Mobile Phone Features and Diversity

According to Chernyshev et al. (2017), one of the aspects that a digital investigator should invest more time and should acknowledge is the potential features that a mobile phone can have. For instance, according to these authors, a mobile phone can possess features that originate from the device itself, from the carrier that the user has and from the user terminal. As such, the device can have several features like, a Platform, which contains the information that allows one to identify the mobile phone, the network and the local definitions and settings that were defined by the user or that are default settings. Likewise, the device can also contain features like the phonebook list, calls and text messages logs, images and videos and other personal applications that help the user to increase its productivity, like the email, note applications, to do lists, documents, web-browsing history, and calendars. The phone can also store each location that the user was and can be as long as the phone is with the user, with a precise and accurate geographical position. It can also keep information on the usage of each application that the phone has installed, maintain information and data on the social networks' activity, web-browsing or cloud services, as well as information on the networks that the user has used (known networks) or those that are visible to it (Bluetooth devices, Wi-fi networks, mobile data network). Similarly, for Tassone et al. (2013), the data that is extracted from a mobile phone can be use in an investigation, which will include evidence, such as the individual's calls and travel timeline, messages history, calendar and emails content, photos, and emails.

Moreover, one of the most important features that uniquely identifies a Mobile Phone brand is the Operating System that its mobile phone uses to allow the user to interact with the device. As such, these technology diversity around the Operating System of a mobile phone influence widely, the process to retrieve digital evidence from a device. Chernyshev et al. (2017) denotes, that the OS is directly linked to the way the digital investigator proceeds while attempting at extracting mobile device data. Nonetheless, despite the different and various available mobile devices, only a small number of Operating Systems for Mobile Phones are being employed in most smartphones. The most widely used OS in the mobile phone market is the Android, which represents an "open-source Linux-based OS" that belongs to Google, which has a strong share of the mobile phone market and its operating system (Chernyshev et al., 2017). The second most used OS is the iOS, despite having a smaller share when compared to the Android based devices, the Apple iOS, represents a universal OS that runs on all Apple's smartphones.

Both operating systems, present to a digital investigator several challenges that could increase the difficulty in obtaining digital evidence from a mobile phone. For instance, by being an open-source, Linux and Java based OS, there several different variants and an endless number of applications which are subject to a lighter authentication and verification process, being supplied and delivered within non-official channels, increasing the number of occurrences regarding to mobile malware and "rogue apps" which represents counterfeit applications that were introduced to simulate and mimic trusted brands and applications while containing harmful and malicious features (Sathe & Dongre, 2018; Chernyshev et al., 2017). As such, due to this complexity and diversity, a digital investigation usually requires an android smartphone to be unlocked to be able to extract data. Unlike the Android OS, the iOS is rather less complex as it allows for less customization and all applications are only distributed within the official store that is embodied in these devices. However, the iOS present the digital investigators with different challenges from those that one would get from the Android, as the iOS smartphones contain "built-in data protection mechanisms", that are only possible due to high levels of encryptions including the data on the smartphone as well as the backups that are performed.

The mobile phone market also contains smartphones running the Windows Phone OS, the Blackberry and the Symbian which can be encountered during an investigation. Unlike both the Android and the iOS, these two operating systems receive less support and research due to the lower popularity and share on the market. As a result of this, the digital investigator will have less tools available to perform an investigation process if any of these two OS are being used in a mobile phone (Sathe & Dongre, 2018; Chernyshev et al., 2017).

As previously mentioned, the Android operating system contains the biggest market share of the mobile phone's market, which consequently increases the chances for a digital investigator to encounter a mobile device that runs on the Android OS. Likewise, relevant, this operating system is also one of the most open-source one that allows users to program and develop applications that can be used in real time in these smartphones, making it even harder for a digital investigator to be able to retrieve and analyze this OS.

The Android OS was developed by the Open Handset Alliance (OHA), leveraging on the Linux kernel for its core and mounting blocks of this operating system. According to Rao & Chakravarthy (2016), the android OS is characterized by having a Dalvik virtual Machine (VM). This virtual machine allows the mobile phone that is running the android OS to be able to run several applications and processes, however, as this run is processed by a unique id, the applications and processes do not interact with each other, only if special permissions and configurations are assigned to these applications. Important to notice is that android applications come with the .apk file extension, which are store in the internal memory of the mobile device as well as the applications cache, user data and the libraries that support this operating system. The android operation system is consisted in its architecture of four different levels, namely the "applications, application framework, libraries & android environment and Linux Kernel".

Kim et al. (2018) denoted that one of the risks around the Android OS is the fact that a criminal can hide and store information on the system partition, which in order to be accessed the digital investigator will need the device to be rooted, i.e., unlocked (super-privileges). Likewise, one of the ways of crime around mobile phones is when the criminal inserts and injects data that is corrupted in the system partition, which the phone user is unlikely to notice until the crime happens or at the most common cases, the phone user is aware that the phone has been hacked.

Graves (2013) gives the example of several cases where mobile phones were sent into water to destroy evidence. For example, the iPhone has four water indicators on the inside of the phone that turn pink if the device is submerged in water. When an investigator discovers that a phone has been in water, the number one. A method that works is putting the phone in a sandwich bag that has packets of silica gel inside. In all cases it is recommended that the investigator allow the phone to dry for 3 to 5 days.

3.7.3. Data Storage within Mobile Devices

After acknowledging how mobile phone work, communications, and interactions wise, it is relevant to understand how and where the data is stored and what type of data can a mobile phone contain within its components. As previously noted, there is an uncountable amount of information within a mobile phone and its components, e.g., SIM Card or a memory card, as such it is crucial for a digital investigator to understand where to look and trove this information as it can be in any of the several pieces of physical hardware that build the mobile phone and that can contain information (Graves, 2013). As such, the same author denotes than an investigator should seek to retrieve any information about a particular model of a smartphone starting with the phone's manufacturer's web site, where several vital information can be presented as well as a deeper and extensive knowledge of that mobile phone, as every model can contain several specifics that differentiates it from any other mobile phone (Graves, 2013). In fact, Faheem et al. (2016) refers that, there are several sensitive information stored in the SIM Card, in the internal and external memory, which is harder to retrieve with the nowadays' usage of the mobile phone, which will mean that the mobile devices owned nowadays numerous amounts of irrelevant data, which will be mixed with the sensate and critical information that the mobile may have (Faheem et al., 2016).

One of the most important pieces i.e., physical hardware's of a mobile phone is the SIM card, the Subscriber Identity Module, which represents a physical object that has on its memory, important and vital information regarding the cell phone. For instance, the SIM card can contain information on the mobile itself, its user and some other pertinent data that is stored in it. The information and data that the SIM card can contain is the user's mobile phone number, call records log, SMS (Simple Message Services) texts that were sent and received and the contact numbers' list. According to, Omeleze & Venter (2013), the mobile phone is able to have a high storage capacity, storing high volume of data locally, namely on the SIM card, the flash memory and or an SD Card (Secure Digital), being the SIM card built with a processor and an "electronic erasable programmable read only memory" (EEPROM), that is provided with encryption and an encryption key, and that is able to store information and guarantee that the communications are being performed in a secure way. Important to notice, is that the SIM card allows for this information to be transferred to a any other device, if inserted into it, retaining the information mentioned above and passing it to the other mobile phone where it was inserted, thereby transferring most of the phone's data as well as the service of PIN and PUK. A user to access the SIM Card needs to enter a set of digits, named the PIN, that will allow him to access to the information on that SIM Card.

However, if the PIN is typed incorrectly three times, the user will be asked to insert a more complex security authentication, the PUK. If this situation occurs the service carrier provider will inquiry the Integrated Circuit Chip Identifier (ICCID) that is located on the SIM card for verification before it provides the PUK. If the phone's owner inserts and types the PUK 10 times incorrectly, the SIM Card becomes permanently locked. In the case that the mobile phone is a company owned one and managed by it, the mobile phone may be configured to be able to overwrite this rule.

Notwithstanding, these two methods of authentications can be crucial in an information as a digital investigator will most likely need to have a way to access the SIM card and its information, being it possibly already locked on purpose by the criminal activity. Also, the SIM card allows for the encryption of communications, identifying the cell phone to the network. In fact, without one SIM card, a cell phone is only able to call the emergency number of the region where it is. Likewise, nowadays the greatest part of smartphones uses Nano-SIM cards, the smallest version of the SIM Cards. The remaining part of the mobile phones either use Mini-SIM cards or Micro-SIM (Graves, 2013).

Moreover, the SIM Card usually contains 128 KB storage capabilities, however it is not the only storage on a mobile phone. Instead, there is also available other read-only memory (ROM) and RAM, random access memory, where the first represents the storage that holds the operating system (OS) of the device, while the RAM is unstable and volatile (Graves, 2013).

Nonetheless, mobiles can have different characteristics ranging from different types of software and hardware components to different power requirements. Consequently, one of the most powerful and vital sources of information for a digital investigator, is the OS. However, one must pay attention to the fact that phones can seem to have e.g., Android OS, but mobiles can have actually another OS configured to simulate the Android one and as such, the digital investigator will be deceived by this masking of the OS (Graves, 2013).

Omeleze & Venter (2013) highlights that the fast ongoing pace that the mobile phone industry is being characterized has made phone's manufacturers and designers to think on added features that would further develop and improve the interaction that a person has with a mobile phone, as such, several services and applications were introduced, from the Multimedia messaging services (MMS), pictures, photos and videos, to social media applications and games, that are creating the urge for bigger and better flash memory on the mobile phones itself, being this memory nowadays, alike one from a personal computer in terms of storage size. As such, in order to improve and enhance the mobile phone architecture, companies are striving at creating suitable and easy to use mobile phones that can serve any need that the user may be having.

3.7.4. Mobile Device Information

Labelled on a mobile phone, are the SIM and the ICCID described above, nevertheless there are other information on it that could play a useful part in the investigation that is being performed. This information can be related to the electronic serial number (ESN) of a mobile phone or to the mobile equipment identifier (MEID) and the International Mobile Equipment Identity (IMEI). Both the ESN and MEID numbers are unique and specific to the mobile phone itself, and to the network they are inserted. The IMEI number is a hexadecimal number, being specific to GSM mobile phones and could be considered as the Mobile device's "social security number" (Graves, 2013).

According to Graves (2013), in order for a digital investigator to retrieve the information related to the MEID from a mobile phone, one can just type the key "*#06#" on the mobile phone. In the case of the phone being an apple iPhone, a digital investigator could just access to the Settings, General and about. The MEID is a hexadecimal number. Likewise, the IMEI is similar to the MEID as that it will allow for the identification of the mobile device in the network, allowing one to block a mobile phone in case its lost or stolen. The IMEI is printed in the battery compartment of a phone, and is composed by 15 algorisms, which with a different purpose and meaning. The first eight digits pay respect to the Type Allocation Code (TAC), indicating the mobile's model and where it was produced and made. The following six algorisms pay respect to the serial number of the device itself and the last digits is the checksum number. Consequently, as this information is printed and labelled on the mobile phone itself, one individual can remove the labelling, altering it to mimic a different information or to making it imperceptible so that it is impossible for a digital investigation to find the information on it and if this information is found, one cannot interpret it and ensure that it is the correct one. One way to test if the information is correct or not and to retrieve it correctly is by looking at the power cord of the mobile phone itself which is expected to be specific to a certain brand and model.

3.7.5. Storage and Acquisition within Mobile Devices

Regarding the acquisition of information from the mobile phones, the digital investigator attempts to retrieve this information, to do so there is the need to communicate and connect to the mobile during the examination. However, as when a mobile is seized in a search incident to arrest (SITA), if powered, on and connected to the network, there is a possible chance that one can remotely access, alter and even clear the information that is critical and that is residing on this device.

To overcome these challenges, there is available the so called, Faraday Enclosures, whose objective is to keep unwanted signals or interferences away from the mobile phone, i.e., out of an enclosure that where the phone will be in. One derivation of this, is the Faraday's bad, which is a device that prevents radio frequency communication by isolating the mobile phone, containing sealing strips to ensure that the bag is completely isolated, prohibiting any communication from happening. These tools bring one way of communicating to the device, preventing external communication to it, however, one has to consider the risk of during an investigation the bag is opened as to connect any cable or to perform any other activity, and thus, there will be a chance for any external communication to happen (Graves, 2013).

Moreover, it is important for a digital investigator to document every step that he/she takes during an investigation. To do so, Graves (2013) refers the use of screen capture devices, that will allow one investigator to footprint every step that is taken to perform an analysis to a mobile device. Every step and alteration will be recorded and documented guaranteeing that the investigators' work can be audited and reperformed. The author recommends two tools, the first the Paraben's Project-A-Phone and the Eclipse screen capture device. To be able to get a high utility from these tools, it is important that these are used within Faraday's Enclosures, has to guarantee that the work is well documented and the procedures it took to complete it are retrieved precisely. These devices are able to create files, encrypting the files and allowing for annotations that can be directly made on the software that support these devices.

3.7.6. Mobile Phone Data Extraction Levels

Chernyshev et al. (2017) and Ayers et al. (2014), denotes the existence of a five-level data extraction levels that can be performed to a mobile device during a forensics investigation and that can differentiate a tool's capacities. Acknowledging the different level of extraction of data is vital to perform a valid Mobile Forensics investigation, as the one of the major challenges of this process, is to be able to acquire the data exactly as it is stored in the mobile phone, preserving it and being able to retrieve its content, otherwise, this evidence data cannot be used as an evidence in an investigation (Wilson & Chi, 2017).

Following the different levels of data extraction, one can perceive the level 1 of extraction that is called "manual extraction" as being the extraction of the information that is store in the device itself, corresponding to the data that does not require a tool to be extracted and high level of technical complexity. At this level, Bjornson & Hunter (2016), describe the need to perform an exact copy of the memory of the mobile phone, creating the image of it without any modification. For Zhang et al. (2017), the manual extraction, can also be define as an extraction technique that involves direct interaction with the phone itself. Moreover, the Level 2 of extraction is the "logical extraction", which alike the first level, does not require high level of complexity, involving solely the interaction between the user’s computer or terminal to the device itself using e.g., a USB, Wi-fi or the Bluetooth, transferring the data to the user’s computer (Chernyshev et al., 2017; Ayers et al., 2014). Zhang et al. (2017), considers the logical extraction a method of extracting the allocated data, i.e., the one that is not deleted and accessible on the file system itself, being this extraction performed by entering into the device’s file system.

Regarding the level 3 of extraction is represented by the “hex dumping” which reflects a physical extraction which involves one to place the mobile phone into the diagnostic mode using a specific flasher box that will allow the digital investigator to download the flash memory of a mobile phone, which represents a non-volatile memory that can be electronically changed or obliterated (Chernyshev et al., 2017; Ayers et al., 2014). Likewise, at this level of extraction the target is to access to the device’s storage medium, i.e., any type of technology that enables the user to place, maintain and retrieve any electronic data. By doing so, this technique allows the digital investigator to access not only allocated data but also unallocated one, that contain delete or obsoleted data, providing significant amounts of data, that both the level 1 and level 2 extraction would be able to do so (Zhang et al., 2017).

The level 4 of extraction is known as the “Chip-off” extraction which represents the action of retrieving the flash memory chip of a mobile phone, in order to obtain a complete physical image and then retrieve the raw data using specialized tools. The last level of extraction, level 5 represents the “micro read” which involves the need of using an electron microscope to conduct physical observations of logic gates, which corresponds to electronic circuits that contain one or more inputs and only one output. This level requires high level of technical knowledge as there is the need for the digital investigator to translate the observations into readable data (Chernyshev et al., 2017; Ayers et al., 2014).

3.7.7. Mobile Devices Forensics Available Paid and Open-Source Applications

As described above, there are tools and applications available for the digital investigator to support a digital investigation process, however, it is relevant for the digital investigator to understand and acknowledge what are these applications, whether they are free to use or a payment is needed and whether it corresponds to the need and issue that the investigator wants to address during this examination. In the same manner, Chernyshev et al. (2017) refers that there are a high number of tools available for the digital investigator, both paid applications and open-source ones. According to these authors, the advances in mobile technology and the market share that these devices have currently on the technology market, as imposed vendors of mobile forensics tools with new challenges due to the high variety of devices, and the different level of extraction that each need in order for a digital investigator to have access to the data on these applications.

Likewise, the commercial tools available for a digital investigator tend to be expensive, being the price of a tool a factor that reflects the different characteristics of the tool, consequently, the higher the extraction capability of a tool, the higher its price. Additionally, to the acquisition cost of these tools, due to the complexity of the mobile device forensics field, there is the need for a digital investigator to invest on training that is required for one to acknowledge how these tools work and how to take the most out of them. Likewise, paid tools are also an investment which embodies the risk of needing updates to keep up with the fast-paced industry of the mobiles phone, as such, it one tool is most likely to not be able to sustain the fast releases of new mobile phones and new capabilities that the highly active mobile technology landscape embarks (Chernyshev et al., 2017).

Between the paid applications to perform mobile forensics one can highly the Project-A-Phone tool, which includes a high-resolution camera that is able to integrate with the tools that the investigator uses and contains a device that is able to extract data from the device. The NFI memory toolkit represents a tool that is also able to perform data extractions, containing a software that allows for a more low-level way. Nonetheless, there are several free open-source applications that the digital investigation can use while pursuing an investigation, namely, the BitPim tool, which allows the investigator to extract data from "basic feature phones", the LiME, which stands for Linux Memory Extractor, which via debugging bridge between the phone and the application, is able to perform memory retrieval from Android phones.

Likewise, apps like the Autopsy can aid the digital investigator in managing and analyzing digital evidence. According to Chernyshev et al. (2017), the usage of free versus paid tools will depend on the matter that is being under analysis and investigated, however, the authors refer that the same challenges appear for both types, namely, the recover and retrieval of missing and deleted data, the inability to understand and interpret the data stored and the lack of universal support.

Furthermore, regarding the acquisition of data that has been previously deleted, Graves (2013) refers two tools that can be used to perform Image extraction devices due to their physical extraction capabilities, both from Cellebrite, these tools, Universal Forensic Extraction Device (UFED) and the Chinex device. To do so, a phone needs to be connected to these devices, which will then seek to capture all available data from contacts, SMS text messages, videos, pictures, and logs. It can be connected via Bluetooth, infrared, or data cable. It also can replicate and clone SIM cards. Likewise, Rao & Chakravarthy (2016) denote that as for acquisition and examination of mobile data specially, message applications like WhatsApp, the digital investigator may leverage on the usage of UFED (Universal Forensic Extraction Device) and the analysis of the evidence that comes from these using the UFED Physical Analyzer. Likewise, the Cellebrite's UEFD Touch application is able to perform the acquisition of data from a mobile phone in the very different levels of extractions, including the physical one, that refers to the creation of an exact copy of the memory of the mobile phone, supporting also the file system extraction (Bjornson & Hunter, 2016).

Moreover, software that is able to perform the imaging of a mobile phone are very important and relevant for a digital investigation. As such, by acquiring the image of the mobile device, the digital investigation will be able to replicate the mobile device's so that its original state can be preserved and kept away from modifications or any connectivity attempt. To analyze this data, the digital investigator can use the FTK Imager which will allow one to examine the captured images of the partitions, data, cache, and system as well as any applications or data that is held in the device's internal memory, including the text messages, images, video, browser and app history and user account personal information. To use this application at its fullest, the user should root the mobile phone in order to gain access to root user privileges, and then run the Linux command in order to retrieve the image of the mobile phone. The final step is to use the FTK imager for the forensics analysis of this image and for the retrieval of relevant information (Rao & Chakravarthy, 2016).

According to Jadhav & Joshi (2016), FTK Imager will allow the digital investigator to retrieved important information on the mobile phone, namely its IMEI Number and other important information on the device status and on manufacturers information. Likewise, for Shortall & Azhar (2015), FTK Imager is one of the most available tools to perform the imaging of a mobile phone, however, the authors also refer the existence of two more tools that will allow the imaging of a mobile device to be made, namely the EnCase and Linux itself. Moreover, the FTK Imager represents a tool that is free, being one of the most used in the market for the imaging of mobiles, where the EnCase, is also one of the most used, being inclusively used by the police units around Great Britain (Shortall & Azhar, 2015). Software that are able to perform the imaging of a mobile phone are very important to a digital investigator. Given the different types of data extractions that were described previously, Omeleze & Venter (2013) highlighted the fact that for logical acquisition, that is represented by the extraction of data from the logical file allocation memory of a mobile phone, there are some applications available from "the MicroSystematics XRY, EnCaseNeutrino, FTK, Cellebrite Universal forensics extraction devices (UFED) and Paraben Device Seizure".

After extracting the data, it is essential to have a software that will allow one to analyze and visualize it. Graves (2013) refers software like Device Seizure or BlackLight. This software allows for e-mail extraction, data extraction and analysis. According to Faheem et al. (2016), there is available neither paid nor open-source tool that currently can run on the mobile phone itself. The tools that exist required the support of a peripheral, namely the computer. From those available, the authors refer the XRY, UFED, OXYGEN or Paraben's as tools that can be able to analyse and help the digital investigator in visualizing the evidence and deriving any inference.

All of these tools allow the digital investigator to retrieve several information from the mobile phone, including the calls and messages logs, the contact list, emails, Wi-fi networks, activity, history and its configurations, browser activity, installed applications and its cache, device info, such as the phone's model and version, its software version, kernel information, brand manufacturer, IMEI, development option configurations (if its activated or not), flight mode status, battery status, and several configurations that were performed in the device (Faheem et al., 2016). Jadhav & Joshi (2016) suggest that the digital investigator should leverage on tools like the Android SDK, Magnet Axiom, qtADB, FTK Imager and SQLite Forensics. The application qtADB will help the digital investigator to locate where important data is, namely the user data. At this stage, the investigator should be look at the block of the mobile phone that contains the user data, which will represent all the data that is stored in the device's external and/or internal memory and relates to the user and its activity while using the mobile phone.

After locating the user data, the digital investigator can use the Magnet AXIOM, software which allows the investigator to load the image that was created based on the user data and analyse this image, namely the "artefacts" like multimedia, browser and activity history, documents, and personal data. This tool can also be used to document the analysis that is performed by the digital investigator, as well as the documentation of all the log files that show the analysis that the digital investigator has performed. For Jadhav & Joshi (2016), a tool that allows the investigator to examine the browser favourites, history and activity is the SQLite Forensics. This tool allowed Jadhav & Joshi (2016) to retrieve user browser history, namely the websites that the user visited, and examine it.

Furthermore, a big part of the data that a mobile phone creates, transfers and stores, may be store in log files that register, its detailed information as well as the modifications and eliminations that may have occur, as such, Kim et al. (2018) denote that most of the user logs files, both applications and browser related are normally in the SQLite DB format, which makes SQLite Forensics an useful tool whenever a digital investigator is seeking to examine and analyse the user logs, as well as the types of applications that are installed on the phone, the timestamp of each installation of an application. For a digital investigator is highly relevant to acknowledge what were the application installation files used (.apk), in order to retrieve a detailed analysis to understand if this application software was malicious or encrypted (Kim et al., 2018).

Moreover, regarding the acquisition of data from a mobile phone, according to Shortall & Azhar (2015), there is available, however paid, the UFED from Cellebrite application is able to perform physical examination and investigation to the hard drive of a mobile phone on the mobile phone, increasing the chance of the digital investigator being able to find and retrieve deleted data, including data on applications. In fact, UFED represents a physical application which seeks physical data on the hard memory of the mobile phone, which represents a different technique of extracting data, where the digital investigator will look at the physical acquisition of the hard drive and its deleted files rather than seeking and looking at the Operating system to look where the user data is at.

Shortall & Azhar (2015) also denote the Oxygen Forensic Suite as one of the best software for mobile forensics, especially because of its compatibility with different models of mobile phone. This tool differ from many in the mobile device forensics process has it also contain tools for extracting and retrieve information on the messages that the user sends and receive, namely the ones in the instant messaging application, the WhatsApp.

4. METHODOLOGY

4.1. Design Science Research (DSR) Methodology

The methodology that will be used and leveraged throughout this research is the Design Science Research (DSR) methodology for information systems, which can be considered an approach "that seeks to deliver new and innovative artefacts" built and developed from the strength and knowledge of science itself (Baskerville et al., 2018: 140). In line manner, DSR can be split into products (IT artefacts), which will be the case of this dissertation and into Processes (set of activities) (Weber et al., 2012). Likewise, Ostrowski et al. (2012) presents this methodology as a six stages process Model (See Figure 3.1).

- Identify Problem & Motivation
- Define Objective of a Solution
- Design & Development
- Demonstration
- Evaluation
- Communication

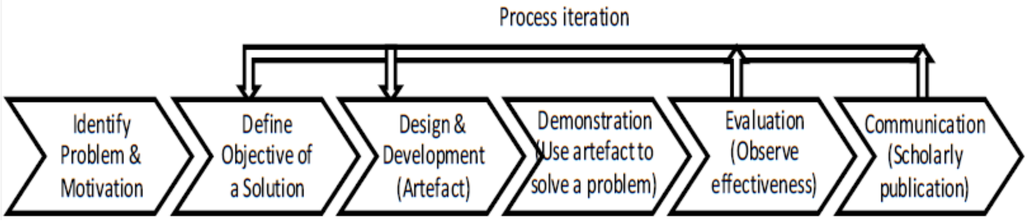

Process iteration
Identify Problem & Motivation
Define Objective of a Solution
Design & Development (Artefact)
Demonstration (Use artefact to solve a problem)
Evaluation (Observe effectiveness)
Communication (Scholarly publication)

Figure 8 - DSR Model. Source: Ostrowski, L., Helfert, M. & Xie, S. (2012)

Moreover, it is relevant to acknowledge how will the proposed methodology be applied in this research. To do such, one will describe how this ought to be used on the research and what potential takeaways can one get.

Step 1 – Problems & Motivations

Similar to Section 1.1, the first stage focuses on finding and describing the pertinent main problems and motivations that characterizes the environment around the topic (Ostrowski et al., 2012; Schorr & Hvam, 2018). Likewise, according to Dresch et al. (2015), it is crucial that the research analyst is able to identify "gaps" that will allow one to investigate possible methods, choosing the one that is most suitable and that will allow one to reach a better and stronger conclusion.

To do so, one researched and investigated on the literature, on scientific journals, papers, national & international news, and conferences that were available as well as other channels that contained information that was considered as pertinent for this research and that contained information on the challenges and the potential applications of forensic science and mobile device forensics.

Throughout literature, one denoted that it is vital for someone that aims to practice any forensic science or that is that is already practicing it, to be able to understand the challenges that characterizes this field and its subdisciplines, that are imposed and that can derive from its activity, namely the following:

- For the National Academy of Sciences (2009), one of the major challenges is the "funding, access to analytical instrumentation, the availability of skilled and well-trained personnel, certification, accreditation and oversight";

- The House of Lords (2019) reflects that the challenges that are and can affect the digital forensics investigation process is its actual use including, "the availability of skills, the global nature of cybercrime, the scale of digital forensic investigations, the interface between digital information and physical information";

- For the American Chemical Society (2017), "science in the courtroom has been riddled with poor analysis (…) many forensic techniques fell short of scientific standards and recommended ongoing evaluations of forensic techniques";

As described above and in the different sections of the literature review, one studied the different challenges that are being imposed to not only the Forensics field, but also to the Digital and Mobile Forensics fields, understanding that the literature available describes several that critical challenges are jeopardizing the accuracy and validity of the Forensics fields and that more research, investment and development need to be pursued in order to be able to sustain the fast-paced technology that embodies the mobile phones which changes at a daily basis.

Step 2 – Objectives & Sub-Objectives

The second phase highlights the importance of defining clearly the objective of the research. This shall be complemented with sub-objectives that will help one, on reaching the main objective. This information is presented in section 1.2. In fact, the second stage goes along with Stage 1 by focusing on the objective and sub-objectives that this research is aiming to achieve and to clarify.

This stage focuses on the important aspect of clearly defining and setting objectives sub-objectives that one will aim to answer as to reach a conclusion on the main research question. As such, these objectives must be linked to the research questions and shall be complemented with sub-objectives that will further support and corroborate the work that is being performed. As such and as previously mentioned in section 1.2., one denoted as the primary objective to:

- Propose and build a toolbox that will potentially support and improve the Mobile Forensics investigation; and,

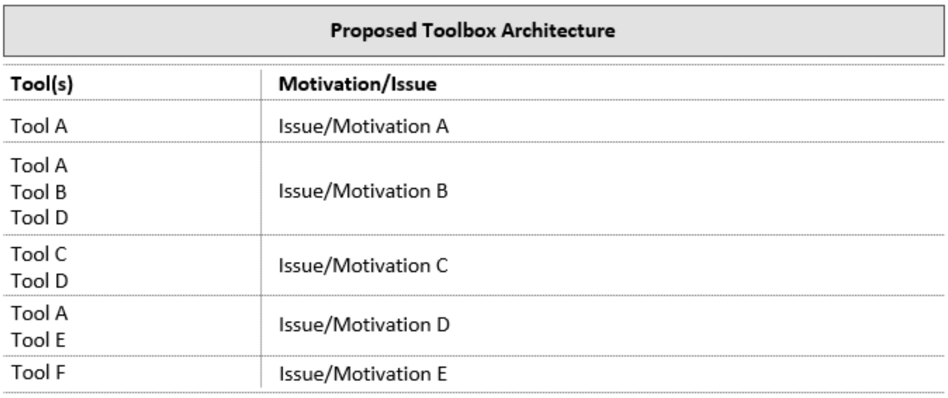
- Acknowledge what are the tools available and how can one leverage on it, aiming to build a toolbox that would potentially have installed the best available software to pursue Mobile Forensics.

Thus, answering to the research question identified of "How to build and use a **toolbox application** to support and enhance the **mobile device forensics investigation process** – breaking through the techniques available".

The research question can be answered by achieving the main 2 objectives defined and well as by achieving the sub-objectives defined previously in section 1.2. that were developed to corroborate, support, and guide the process that will allow one to reach the main objectives.

Step 3 – Building the Artefact

In the third stage, one ought to find the solution to the question under analysis, by building the so-called artefact. To help visualize, one drafted a prototype version of the architecture of the artefact is expected:



Proposed Toolbox Architecture

Tool(s)	Motivation/Issue
Tool A	Issue/Motivation A
Tool A Tool B Tool D	Issue/Motivation B
Tool C Tool D	Issue/Motivation C
Tool A Tool E	Issue/Motivation D
Tool F	Issue/Motivation E

Figure 9 - Artefact Prototype Structure

Throughout the literature review, one noticed that there is a great concern on the digital investigator to acknowledge what are the tools and applications that can be used to perform the Mobile Device Forensics investigation. What's more, the literature review also denotes applications and tools that are open-source, i.e. free to use and those that the user needs to pay in order to be able to have access to it and to apply it during an investigation. As such, the artefact that will be built, will be composed by three different layers of information, that are related to the architecture and process stages/phases studied in the literature available. For instance, in order to build the toolbox and to retrieve and explore the applications and tools that are most suitable for a digital investigator during a Mobile Forensics' examination, one scrutinized the literature available as to seek for the ones that can answer to each phase of the Mobile Device Forensics process.

The different types of features of the tools and applications are presented as a way to allow the digital investigator to acknowledge what are the tools that are available for a Mobile Devices Forensics investigation, both free and/or paid, and dependently on the budget and level of detail and extraction that the digital investigator has and wants to reach, there are three choices from which the digital investigator can choose and opt, which will enlarge its awareness on the existing applications available to the Mobile Forensics science.

Step 4 – Demonstration of the Artefact

Furthermore, in stage four, the demonstration involves putting into practice the artefact by playing the role of the target user (Storey et al., 2017). As such, it will involve a demonstration and description of how a digital investigator can apply and use the proposed toolbox during an investigation.

Step 5 – Evaluation of the Artefact

The fifth stage aims at the evaluation of the Artefact, the Evaluation phase, which Cronholm & Göbel (2016) argue that is the course of witnessing and determining how fine the proposed artefact performs. At this stage, one ought to involve users whose work will be directly improved by this artefact as it can enhance the process independently of the typology of the investigation. As such, one's intent is to have two different focus group, composed by people that work directly or indirectly with the Mobile Devices Forensics science, the Mobile Security and with crime investigation. The focus group is expected to be composed by three questions for the participants.

The first question will seek to understand and acknowledge what the view of each participant on the Toolbox that was purposed, and if it is useful and insightful for the Mobile Device Forensics field. The second and third question have the objective of understanding and retrieving negative critics and reviews as well as positive ones, as a way to improve and enhance the Toolbox and this research. Consequently, by acknowledging the parts of the toolbox where there is more room for improvement or where changes need to be made and by recognizing what are the best and more successful parts of the Toolbox, one will be able to leverage on this knowledge to improve this work and to make it a completer and more insightful one. In addition, users that do not work directly with this tool may also be a vital source of information and input since their criticism and feedback is expected to be clear and less biased than other people that work directly in this field. All the participants will be requested whether one is allowed to transcript some of the main ideas mentioned and described in the focus group and that are important for the analysis and the research as a way to be able to analyse and discuss in a greater detail the most important topics that were discussed and addressed during this group activity.

The evaluation phase was done through the arrangement of a focus group meeting with the main objective of receiving feedback and feedforward from the participants enrolled on what were their impressions, ideas, critics, and recommendations about the proposed artifact and what and how would the participants see it being implemented or recommended to Forensics' practitioners. In the section Focus Group, one explores, the literature behind this methodological approach, as well as the main reasons behind opting for a technique like the focus group one, and how it was structured, including the number of participants, questions, and the moderator role.

Step 6 – Communication of the Results

The sixth stage aims at communicating the results of this research and of the appliance of the artefact. At the Communication stage, the objective is to reach and achieve good communication of this dissertation. As such, this work can be published and presented by Nova IMS as a partial requirement for obtaining the Master's degree in Information Management, as well as, on scientific journals, papers, national & international conferences, and other channels that may be relevant for spreading the content of this work. In fact, before the publication and defense of this Master thesis, one had the opportunity to publish the work performed during the systematic literature review of this Master thesis. As such, this research was published in 33 pages in the Handbook of Research on Cyber Crime and Information Privacy (2 Volumes) as a book chapter, namely, in the Chapter 14 – Mobile Device Forensics Investigation Process: A Systematic Review, written by the author of this thesis Bruno Bernardo, together with Professor Vitor Santos, who is the advisor for this thesis and work.

4.2. Focus Group

As to acknowledge the importance of the framework presented and to validate it and retrieve insightful and valuable inputs from experts on this fields and areas of interest, the study that was considered to fit the best the context under analysis was the Focus Group research methodology, which relies on the evaluation of qualitative data obtained from the engagement of stakeholder's (participants of the focus group), and thus, acknowledge their opinions and assessment of the proposed framework. In fact, Wilson (2016) perceives that this methodology is expected to retrieve and collect a large input of data for the researcher, from the opinions and involvement of a group of people in a short period of time. Likewise, Hartman (2004) observes that in this approach, one's intent is to leverage on the advantage of presenting "structured interviewing techniques" in the dynamic environment that characterizes a group setting (Hartman, 2004: 402).

Accordingly, despite being historically used by researchers, within the study of marketing and market profiling research, this method is nowadays used in an infinite number of different areas, where the "data produced is unique as well" (Wilson, 2016: 44). In the same manner, Kruger et al. (2019) denote that in the past 25 years the usage and application of focus group has increased, given the clear advantage that this technique represents, namely, the fact that group dynamic may potentially generate more insights and inputs for the researcher and that participants in the focus group may support each other while sharing their experience and views. In addition, Hartman (2004) acknowledges that this type of methodology is on a fast-paced rise, being more and more important to many and different fields of interest, as the researchers find it appealing to employ a method that can lead to the creation of knowledge and insights leveraging on a qualitative group dynamic. Moreover, the questions that regard the stakeholders tend to rely on exploring how their perception of a given product, service, artifact and/or topic is, how valuable can it be, how solid and corroborate is the artifact and how do they see and feel about it (Wilson, 2016; Al Qudah et al., 2015). Likewise, Al Qudah et al. (2015), refers that this qualitative methodological approach is expected to produce concrete insights and proposals for the researcher's analysis. In the view of the author, Wilson (2016), focus group usually are structured by the presence of face to face or virtual meeting between the researchers, a focus group moderator (facilitator) and the stakeholders who can be from a more homogeneous area of expertise, or a more heterogeneous one, involving people from different fields and with different lines of expertise. Besides this, the focus group usually intends the later transcription of the main ideas denoted during this activity as for one to be able to perform and analysed the discussion that was conducted, and transcriptions/notes/insights are usually taken in order for further analysis after the focus group meeting (Wilson, 2016). Thus, it is important for the research to concentrate and to acknowledge and leverage on most of the insights and perceptions of the participants, as the focus groups may be used as the "sole source" in what regards data acquisition on a research project (Eaton, 2017: 9).

Important to notice, is the moderator or facilitator role that is crucial to be present in a focus group meeting, as this role is responsible for the coordination, balance and enabling of this meeting. This role should be represented by one that is an aware and that acknowledges the field of the area of the research being perform and should be responsible for guaranteeing that each participant's opinion and view is heard and denoted in the meeting, where there can be several challenges coming from people with different mindsets and personalities (Wilson, 2016). For Al Qudah et al. (2015), the moderator is commonly the researcher who has to maintain a professional attitude towards the meeting and must be in possession of the required "inter-personal" skills to retrieve the most out of the stakeholders and to ensure that the participants converge thoroughly into the topic under analysis and within the research field (Al Qudah et al., 2015: 2). According to Wilson (2016), there can be participants who are dominant speakers (that tend to control a discussion/debate), breathless talkers (who tend to hold a fast-paced speech and that usually persist in presenting their view), quarrelsome talkers (who tend to comprise in arguments with other participants), experts (those that are specialized in the matter under analysis or are practicing that field of expertise) and nervous/shy participants (who tend to be anxious and more cautious to participant, and generally need the moderator to encourage to express themselves).

Furthermore, one's main reason to apply a qualitative methodology approach such as the focus group strategy, was to capitalize on group expertise dynamic to generate and encourage important discussion and brainstorming of ideas and insights as to obtain a wider variety of inputs from different sources. In fact, some authors refer that focus group by encouraging and prompting the group involvement and discussion, tend to generate and gather information that may not be able to be collected from a single participant (Guest et al., 2017; Hartman, 2004). As such, despite acknowledging, the larger amount of time and resources needed to conduct a focus group meeting, which usually takes more time to undertake and to perform that transcription and further analysis (Guest et al., 2017), one beliefs that to pursuit the Design Science Research as a way to validate and communicate the artifact framework presented in this research, the focus group approach is more suitable, as a way to reach and involve a group of experts in this field to discuss and elaborate on their perception, thoughts and feelings on the framework and on the work being performed.

Besides this, Brandl et al. (2018) denote that by providing space and time for stakeholders to provide their input and insight, while allowing for a face-to-face intervention, the focus group methodology tend to boost and increase the number and the quality of the interactions from the participants, as the focus of a focus group is not to generate a consensus between the stakeholders involved, but rather create and collected different perspectives and ideas on a given matter from people with different experiences and views. Given this, and according to Hartman (2004), a focus group should take into considerations some guidelines and assumptions in order for it to achieve its fullest potential. Accordingly, the author refers five different assumptions, being the 1) the research must acknowledge that people represent valuable and insightful sources of information and context; 2) the research must allow for people to debate and discuss, as people are capable and own the ability to be able to express themselves, their beliefs and experience, and thus, should articulate their own insights; 3) the moderator/facilitator of a focus group should be able to encourage and retrieve information and participants' thoughts and perspectives; 4) the researcher must stimulate group dynamics as it can create more valid and consistent information; and, 5) the researcher should leverage on the group activity as it can be potentially a larger and deeper source of information than individual methodologies in particular research' characteristics.

In lines manner, Hartman (2004) suggest that the focus group methodology considers a 6-step approach, being the 1st, the phase where the research must decide the learning objective. The next phase, the 2nd, is where the researcher decides from whom one wants to learn and obtain insightful thoughts and perspectives. The 3rd step suggests that the researcher structures the interview and decides on what type and kind of questions are going to be asked within the group. According to the author, questions are more important the more they are actionable, meaning that the questions' intent is to answer to the researcher’s objectives. Likewise, the author perceives that usually researchers tend to follow the so-called “moderately structured interview structure”, which is represented by mixture of the enclosure of pre-prepared and planned questions and on a later stage, the inclusion of follow-up/probing questions were the intent is to get more concrete and close-ended answers (Hartman, 2004: 404). For instance, according to Eaton (2017), focus group questions should be both open-ended and exploratory, allowing stakeholders to share open-mind inputs without imposing any pressure or conviction, and should not contain jargon expressions and/or complex scientific and technical terminology. Likewise, Djohari & Higham (2020), perceive that the small group context where participants are enrolled in, encourage, and stimulate participants to share experiences that can be trigger by other participants ideas/interventions.

Moreover, at this step, the researcher must also be careful and cautious when picking and deciding the number of participants, as too many stakeholders, may imply and mean that the process of the group dynamic and the collection of inputs may be jeopardized by it (Eaton, 2017; Hartman, 2004). Hence, the usual maximum cap for a focus group tends to be a maximum of 10 participants. What’s more, the 4th step, represents the one where the research must decide whether to be the moderator role or to choose one, to conduct and align the focus group session. Lastly but not least, the 5th step represents the one where the researcher must decide whether to perform the focus group presenting on a given location or virtually, and in the 6th step, the research must focus on having a robust and managed opening of the focus group meeting, where the author suggest that the researcher includes in the agenda, the moderator’s introduction, self-introduction among the researcher and the participants, the discussion of the topic and analysis and on the focus group main objectives and goals (Hartman, 2004).

Similarly, the authors Winlow et al. (2013), denotes that there are key considerations that a research must take into account when and before organizing a focus group meeting. The key considerations are the focus group strategy and size. As previously mentioned, it is highly relevant to choose a number of participants that is not composed by few to many people, rather it should be composed by a number of participants that the research and the moderator (if not the same), feel comfortable and adjusted to the focus group and the matter under analysis. Likewise, the authors suggest that the focus group design is effective and that the participants are well aware of the key topics under research and that the focus meeting follows sequenced questions as to guide the participants throughout the activity, avoid diversions. In addition, the authors perceive that taking into account the focus group management can help the researcher achieving a successful and adding value one. As such, the researcher should consider the importance of the role of the moderator and the group dynamics and interactions. Also, the researcher should take into account the transcription of the main ideas and topics discussed on the focus group as to analyse the insights and the course of the focus group meeting, as to take extensive and transcription notes and leverage on these inputs to their fullest. Given the literature analysed and the adequacy of a focus group technique for this research, one opted to choose participants, that were experts on the matter in the context of this Master’s Thesis, whether more focused on academic research or market appliance of this science. The main reason that sustains this choice, was because of the fact that, as shown in the literature review, there is currently a lack of awareness on this area of expertise, a lack of knowledge and certification, thus, to have people that are somehow experts in this matter, is a great opportunity to validate the framework proposed as well as, retrieve and gather important insights and perspectives from people with different expertise and level of maturity in this matter.

5. FRAMEWORK TO SUPPORT THE MOBILE FORENSICS INVESTIGATION PROCESS

5.1. MOBILE FORENSICS TOOLBOX

After acknowledging and studying extensively the literature regarding the topics of Forensics, Digital Forensics and Mobile Device Forensics and, in a deeper and more conclusive detail, the architecture and archeology of mobile phones, its features and main components, the several and various types of information and storage that it can contain, the different information extraction layers that one can perform during a mobile forensics analysis, and the existing and available paid and open-source applications to perform a mobile forensics analysis, **it was possible to have a crystal clear acknowledgement and prototype on how a Mobile Forensics Toolbox must look like in order to support and enhance the Mobile Forensics Investigation Process.**

Likewise, one studied and analyzed the different existing strategies and methodologies that currently support the mobile device forensics process, its evolution and what are the major challenges and opportunities that are characterizing the environment of not only Mobile Device Forensics but also, Forensics and Digital Forensics. Indeed, it was possible to perceive and retrieve that a Mobile Forensics Toobox, should be defined as a set of different applications and information that aim to improve and enhance the investigation process of a digital investigator, increase the awareness around this topic as well as the knowledge that one will contain. The Mobile Forensics Toolbox should be one that is able to potentially support and improve the Mobile Forensics investigation, allowing digital investigators to have a fairly stable and up-to-date set of tools that can aid them performing different types of procedures within Mobile Forensics. This Toolbox is expected to have installed the best available software to pursue the Digital Archaeology associated to this field, that was retrieved and studied from the extensive literature review performed.

5.2. ASSUMPTIONS

Based on what was studied in the literature review, about Forensics, Digital Forensics and Mobile Device Forensics, it was defined that for a digital investigator to become more aware, conscious, responsive, well-knowledge and smarter on these topics, one should:

- Understand that one of the major technologies used nowadays is the Mobile Phone, which contains several different features and components, such as brands, formats, accessories, as well as, different specifications of hardware and software, models, supported OS and other features (Klomklin & Lekcharoen, 2016; Chernyshev et al., 2017). As a result, Mobile Device Forensics is regarded as one of the most challenging, diverse, and versatile field, being possible the greatest challenge for a Digital Investigator (Graves, 2013; Chernyshev et al., 2017). For instance, according to Chernyshev et al. (2017), it is expected that by 2020, the usage of this technology, namely the smartphones and its network traffic will explain the utmost part of all internet traffic flow.

- Acknowledge the mobile phone, as a fully functional and capable computer system, that is embodied into people's daily routine, and that can contain a "treasure trove of data" allowing people to perform many different activities with various purposes, that may involve documents, pictures, music, messages and calls activity, contacts, mobile identifiers, emails, web activity, multimedia, location information, backups, logs and applications data, while fitting in a pocket (Zhang et al., 2017; Graves, 2013; Chernyshev et al., 2017)

- Comprehend that smartphones are used together with several different accessories like, SIM Cards, Memory Cards, Earphones, Smartwatches and various applications that can be retrieved through a download from the app store of the mobile phone system operator, being this at a rising trend, and consequently more and more third-party applications are being downloaded and used, creating new and different challenges (Ryu et al., 2018).

- Evaluate and understand the impact of the challenges that are characterizing the mobile phones, from the rapid, volatile and dynamic change in its landscape, an ever-increasing diversity of different types, models and features of a mobile phone, the integration of its data into the Cloud and into the Internet of Things, to the increasing adoption of it and the rising risk of cybercrime, targeting the exploitation, corruption and possession of information that can be private, confidential and sensitive (Sathe & Dongre, 2018; Omeleze & Venter, 2013).

- Regard the importance of other sub-branches of Digital Forensics, which has evolved into many different sciences, from Computer Forensics, Malware Forensics, Document Analysis, Digital Evidence, Network Forensics, Database Forensics and many other. Besides this, Valdez (2018) refers that Forensics can be seen as an emerging area, from which several fields have emerged from the digital forensics to forensics accounting, toxicology, odontology, psychology and criminalist, as such and being Mobile Forensics, a subdiscipline of Digital Forensics, it is important for a Digital Investigator to be aware of the best practices and methodologies of other Digital Forensics branches, leveraging on this knowledge and possibly creating synergies and added value to a given investigation (Chernyshev et al., 2017; Omeleze & Venter, 2013).

- Acknowledge that the Mobile Forensics science is being faced with several different challenges, namely, the lack of tools and standard proven formal methods, techniques and documentation, the lack of guidance available regarding the tools and models used to perform an investigation, the higher usage of the IoT and the Cloud to store information and to exchange/retrieve different types of data and information, the rapid technology innovation, implied that tools and methodologies must stay up-to-date and the more robust and limited data protection procedures (Chernyshev et al., 2017; Omeleze & Venter, 2013).

- Comprehend that there is the need to study and perform deeper and extensive research around the topic of Mobile Device Forensics, as there is a clear gap caused by the inexistence of a clear and stable artefact (a tool, a model, a formal documentation and methodology (Ostrowski et al., 2012)) that can allow a digital investigator to perform an examination in a universal, standard and consistent way too allow the investigator to retrieve the pertinent information, and to answer to any issue than may appear while performing the investigation activities.

- Overview that there are different types of data gathering activities and techniques, for a digital investigator pursuing Mobile Forensics. For Zhang et al. (2017), there are three different data acquisition categories from a mobile phone. The first one, the manual methodology embodies the technique of gathering data by interacting with the phone itself. To do so, one can stablish a connection to the phone, via e.g., USB. The second, the logical extraction technique, can be perceived as the retrieving process of data through the access of the file system that contains data that has not been removed by the phone's user. The third, the physical extraction technique regards the acquisition of data from the mobile phone, where the objective is to retrieve data that has been deleted or that is possibly missing.

- Understand that the mobile phones market is one that is composed by two dominated players, Android (Google) and IOS (Apple), which according to Jadhav & Joshi (2016), included a combined market share of 96.7% in the first quarter of 2016. Consequently, it is highly crucial for a digital investigator to have a deep understanding on the foundation's knowledge of these two different operating system, as the potential phone that is being analyzed can most likely be either an Android or a IOS one.

- Acknowledge that forensics is hemmed by the law, science and scientifically methodologies, with the objective of stablishing irrefutable answers and analysis to legal problems, by recovering, scrutinizing, and interpreting relevant materials and data within an examination and during a court case (Houck, 2019; Roux, Ribaux & Crispino, 2018; Arnes, 2018; House of Lords, 2017). Besides, the digital investigator must understand that the investigation process involves science of temporal and spatial aspects, as it can involve people, locations, and materials/objects. (Houck, 2019).

- Understand that independently of the type and source of the science that is being applied within an investigation or examination, if it is being over the intent of the law itself, that is should be considered as a Forensics Science (Katz and Halámek, 2016).

- Needs to be responsible and accountable for the relationships that are stablish between facts and the investigation itself. To do so, the forensics investigator, should be able to answer to the following questions, namely, what kind of event/crime is being examine, where and how did the crime occur, the person(s) involved and when and why it has happened. By doing so, the investigator is able to build an analysis that is sustained and corroborated through the leverage of the science methodologies and methods and on the tools that exist in order to support the inferences made (Arnes, 2018).

- Can consider the forensics activity and examination has a four-stage process. The first stage corresponds the "trace or wet forensics", which should focus on performing analysis and tests over the samples/evidence that were collected from a crime scene and that are likely correlated to it. The second stage corresponds to the interpretation of the analysis performed in stage 1, while using statistical inferences and yielding a statistical probability likelihood to the inferences performed. The third stage is characterized by being the one where the investigator aims at reconstructing the events that should likely emulate the crime that has occur. As for the last stage, the investigator should declare an opinion based on all the previous steps, and on the training, skill and experience acquired until that moment (House of Lords, 2019).

- Regard the following events that should aim and guide a forensics investigation, namely a sequence of events, that should start with the crime/action that was performed and committed, the evidence collection phase and the submission of all materials/objects considered to be important for the examination. Afterwards, the evidence collected should be analyzed leveraging on science, its laboratory analysis and on the investigators' evidence interpretation.

Consequently, and after performing these activities, the investigator should present in the court the findings that resulted from the analysis performed, ending the process as the judicial outcome is declared (Morgan et al., 2018).

- Acknowledge the forensics process can also work as a four-step process flow, that is initiated by the detection phase, where the objective is to decode and discover any object that may be relevant, especially those that would remain invisible or unclear if it were not the forensics specialist investigating. The second step can be overseen as the application of multiple disciplines and methodologies that reside in precise knowledge and science. The next step should be the one where the investigator aims at recreating the story line of the event that has happened. At the final stage, the investigator should assess the performance metrics previously defined, namely, the accuracy, the time, cost of the investigation that was performed and the knowledge that was created by that investigation (Houck, 2019).

- Use and apply, during a forensics investigation, the knowledge retrieved from other disciplines and matters, as by doing so, the forensics investigator is yielding several opportunities for the investigation to be more precise and be improved, as several tools and methodologies can be put together to address any given problem in what regards a forensics investigation (Katz and Halámek, 2016).

- Understand the major challenges that are impacting the field of forensics, namely the lack of 1) financial funds; 2) of qualified and expert professionals; 3) of accessible, available and easy to use techniques and analytical tools to support an investigation; 4) of endorsement and certification; 5) of the implementation of pre-set gauges and measures to assess the performance and the risk involved, such as the implementation of Key Performance Indicators (KPI's) and Key Risk Indicators (KRI's); 6) of rigorous systematic and accurate scientific methodologies and analytical techniques (National Academy of Sciences, 2009; House of Lords, 2019; The American Chemical Society, 2017)

- Consider the need of the increase in studying and exploration of topics regarding the Forensics Sciences, including the pursual of vast and in-depth academic investigations as a way to seek and create more awareness around these sciences as well as to generate more rigorous and precise techniques that can be accessible during an investigation. To do so, the digital investigator should seek to explore how big data and machine learning can be employed as to design and create more robust and precise methodologies and analytical assets, that are expected to generate corroborate and robust conclusions. For instance, Lefèvre (2018) presented that to build a sustainable big data framework for the purpose of Forensics, it has to contain and follow some actions, namely, to have structure and capabilities to process and analyze information; Training and education on these topics to improve and shape skills; and regulation and ethics.

- Perceive the clear definition of the Digital Forensics discipline, which according to the literature studied, can be defined as the forensics activity that entails the analysis and investigation of evidences that reside on electronic devices, i.e. any scientifical technique that is precisely applied towards the preservation, capture, evaluation and interpretation of digital evidence that was obtained from a digital device with the intent of presenting digital evidence found within the investigation rather than prove the innocence or guilt outcome of a given court case. (Valdez, 2018; Arnes, 2018; Du et al., 2017).

- To be acquainted to the concept of chain of custody, which represents the process of tracing the location and state of the evidence that is obtained. Prior to any analysis, it is crucial for the digital investigator to be able to take an image of the evidence, which represents an exact copy/replica of the original one (Valdez, 2018). To authenticate that the copy represents and exact replica of the original one, the digital investigator should invoke the use of hash values comparison. In fact, Valdez (2018), suggest as a way to preserve the evidence and avoid any modification, the usage and application of write blocks to it. This can take the form of a software or hardware that is able to capture a Forensics image of the evidence, enabling the user to write on it.

- Understand the different schemes of evidence classification, which according to Maras & Miranda (2014), can be disclosed into four different groups, namely, the physical evidence, the transfer evidence, the trace evidence, and the pattern evidence.

- Acknowledge what are the main reference steps of the Digital Forensics process. According to Sönmez et al. (2017), the digital investigation process initiates with the presence of a crime, followed by the emission of a search warrant that gives the investigator the right to visit and examine the crime scene as well as protect the evidence and register on a documentation the numbering and the type and description details of the evidence. After doing so, the digital investigator should focus on packing and transferring the given evidence to a safe and secure place that is accessible and suitable for the investigation and the application of techniques. To apply the given tests, the digital investigator should focus on the methodology that is to be applied as well as on the study of the replica, while recording and documenting every step and outcome of the analysis performed. The final stage is the formal documentation of the digital process including the methods applied, the results, the steps taken and the conclusions that were yielded and that can be transformed into a report expected to meet the submission requirements to the authorities if necessary.

- Consider, that for a digital evidence to be suitable in the court, the investigator must ensure the 1) tests and analysis having been made to the procedure; 2) during the procedure and its tests, there was a known error rate defined; 3) the procedure has been shared, distributed and subject to peer review; and 4) the procedure that is being used is widely accepted within the community that involves this science. (Carrier, 2003).

- Perceive, the Mobile Device Forensics field as one that belongs to the area of Digital Forensics, corresponding to the process of retrieving and gathering evidence from a digital source, the mobile device, through the application of tools and techniques to extract this information (Faheem et al. 2016).

- Acknowledge the different methods and techniques available to perform a Mobile Device Forensics investigation, such as the four-stage process method that Ayers et al. (2014) describes. This process is initiated by the preservation phase, followed by the acquisition, examination, and report stage. Likewise, Sathe & Dongre (2018), describe a method focusing on different but similar steps, being the first the identification phase, followed by the preservation, acquisition, analysis, documentation, and presentation stages. As such, both methods are crucial for the creation and the support of the toolbox that will be described in the next section, as the toolbox ought to answer to each step described here and to provide the digital investigator with tools to do so.

- Be aware that the field of the Mobile Device Forensics is growing at an enormous rate, which is trying to keep up to the pace of the ongoing advances and improvements in the technology that supports and changes people's everyday life. As a result, many challenges are characterizing this field, e.g., 1) several different types and models of mobile phones, containing an unlimited number of different specifications and settings that even the user can customize; 2) the forensics tools limitations regarding the different and numerous types and models of mobile phones, the increasing rate of crimes related to the cyber typology, such as through the usage of malicious applications or corrupted files; 3) the lack of documentation, research and formalization of the techniques that are available and used during an investigation process; 4) the lack of testing and standardization of the methods that support and allow for the digital investigation to happen; 5) the limited to no support on the integration of Mobile Phone data into the IOT, namely into the cloud, where it is difficult to establish and ensure the ownership of the data that is being stored there; 6) the emergence of peripheral tools that were built to improve the mobile's functions while working together with it, and allowing for data exchange and storage (Barmpatsalou et al., 2013; Omeleze & Venter, 2013; Jadhav & Joshi, 2016; Chernyshev et al, 2017).

- Consider that there are also several opportunities in this field, namely, the 1) ongoing fast increase and improvements in the technology and its features that characterizes the Mobile Devices Industry; 2) The improvement and focus on more robust and accurate methodologies and techniques, could create several opportunities for this field, digital investigators, and for the on-going academic research; 3) The gap and need to create and develop more accurate, precise, universal and fast extraction tools that allow for the retrieving and analyzing of different types of data from different sources e.g. the mobile device, its peripheral devices and from the cloud; 4) Opportunities for more research and important literature that can support the mobile device investigator, improving the awareness towards the changes and the methodologies available for this process and providing adequate training and literature resources (Mumba & Vender, 2014; Chernyshev et al, 2017; Li et al., 2018).

- Perceive the different features and the diversity of the mobile phones. For instance, a mobile device, contains a platform, where it is possible to identify the mobile phone, a network and local definitions and configurations that are customized by each user to model a specific environment around the mobile phone at the exact image that the user wants the phone to function. Besides this, a mobile can contain data and information like the contact list, calls and messages logs, multimedia, applications, documents, web-browsing history, emails, calendar activity, geographical localization history and positions, social networks activity, travel schedule and historic timeline (Chernyshev et al, 2017; Tassone et al., 2013).

- Comprehend the different operating systems that a mobile phone can have and the impact on the functionality and on the configuration that it can mean and have. As such, despite the numerous operating systems available for a mobile phone, there are a small number of them being currently dominating the mobile market, namely, the Android OS, and the Apple iOS, being the biggest differentiation between this two, the fact that the Android OS is an open-sourced one and as such each present different challenge for a digital investigator. Operating systems like the Windows Phone OS, the Blackberry and the Symbian may also be encountered during an investigation, however, these operating systems will present several challenges to the digital investigator as the receive less support and research due to the fact that they contain a lower popularity and market share within the phone market (Chernyshev et al, 2017; Sathe & Dongre, 2018).

- Understand how mobile phone can store data and where it may be stored. In fact, Faheem et al. (2016), refers that the data may be stored in the internal and external memory of the mobile phone, in the SIM Card and in any other peripheral device that is connected to the phone. For instance, the SIM card holds information and data on the user's mobile phone's number, calls and text messages logs, the contact list and can be transferred to any other device just by connecting the card into other phone. Likewise, the mobile phone is also able and capable of having a high storage capacity, by leveraging on a flash memory or an SD Card, which allows the memory of a phone to be extended with different sizes of capacity. (Omeleze & Venter, 2013).

5.3. TOOLBOX DESIGN/ARCHITECTURE

In the third stage, one ought to find the solution to the question under analysis, by building the so-called artefact. To help visualize, one drafted a prototype version of the architecture of the artefact which is expected and can be seen in the previous sections. Throughout the literature review, one noticed that there is a great concern on the digital investigator to acknowledge what are the tools and applications that can be used to perform the Mobile Device Forensics investigation. What's more, the literature review also denotes applications and tools that are free and open-source, i.e. free to use and the user is able to purpose improvements as well as to develop on it and those that the user needs to pay in order to be able to have access to it and to apply it during an investigation.

As such, the artefact that will be built, will be composed by three different layers of information, that are related to the architecture and process stages/phases studied in the literature available. For instance, in order to build the toolbox and to retrieve and explore the applications and tools that are most suitable for a digital investigator during a Mobile Forensics examination, one scrutinized the literature available as to seek for the ones that can answer to each phase of the Mobile Device Forensics process.

As previously shown, this branch of Forensics, and according to Ayers et al. (2014) can be described as a four-stage process method which is initiated by 1) preservation phase, followed by 2) acquisition, 3) examination, and 4) report. Likewise, Sathe & Dongre (2018), describe a stepwise approach, being the first the 1) identification phase, followed by the, 2) preservation, 3) acquisition, 4) analysis, 5) documentation, and 6) presentation stages. As such, these methods can be put together and support the toolbox creation as well as the software and hardware that can assist the digital investigator. Therefore, as to begin constructing the toolbox, one will segment the different tools analyzed by the different steps/phases of the Mobile Forensics process. Accordingly, and considering the processes described by both Ayers et al. (2014) and Sathe & Dongre (2018), one considered the following phases/steps: 1) Identification & Preservation; 2) Acquisition & Extraction; 3) Analysis & Examination; 4) Documentation & Report.

The reasons and motivations behind one's choice, was due to the fact that the literature analyzed highly emphasize the lack of standardization, documentation and formalization of the techniques available on the field of Mobile Forensics (Chernyshev et al., 2017; Barmpatsalou et al., 2013; Omeleze & Venter, 2013). As such, one's intent is to propose and build a toolbox that will potentially support and improve the Mobile Forensics investigation, and also, to acknowledge the digital investigator to what are the methodologies that exist in the literature and that support the mobile forensics investigation process and to what are the tools available and how can one leverage on it, aiming to build a toolbox that would potentially have installed the best available software to pursue Mobile Forensics. Given this, one decided to put together the literature methodology that support this investigation process as to suggest the standardization of this field within the literature that is available and that there is a lack of acknowledgement.

Given this and in lines manner, the selection of the tools that will compose the toolbox, will also have in consideration the price characteristic of each tool, regarding if the application/device chosen is free for an investigator to use or requires the user to pay a given amount or a license.

The different types of features of the applications and tools that exist to support the mobile forensics field are presented as a way to allow the digital investigator to acknowledge what are the tools that are available for a Mobile Devices Forensics investigation, both free and/or paid, and dependently on the budget and level of detail and extraction that the digital investigator has and wants to reach, there are three choices from which the digital investigator can choose and opt, which will enlarge its awareness on the existing applications available to the Mobile Forensics science.

5.4. Toolbox Strategy and The Supporting Stepwise Approach

As previously mentioned, and as to build one's artifact, i.e., the toolbox, one decided to segment and correspond the existing and analyzed applications and tools to different steps/phases of the Mobile Forensics Investigation Process. Accordingly, and considering the processes described by both Ayers et al. (2014) and Sathe & Dongre (2018), one put together both methods and derive that the following phases/steps should be considered by a digital investigator and should all of them be accurately documented and supported, namely the following phases/steps: 1) Identification & Preservation; 2) Acquisition & Extraction; 3) Analysis & Examination; 4) Documentation & Report.

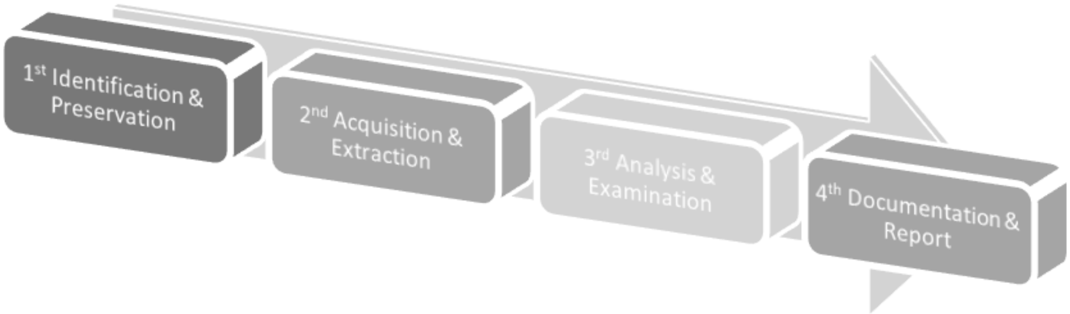

1st Identification & Preservation
2nd Acquisition & Extraction
3rd Analysis & Examination
4th Documentation & Report

Figure 10 – Process Flow developed by the Researcher with the Toolbox Strategy chosen - Based on the two existing mobile forensics methodologies from Ayers et al. (2014) and from Sathe & Dongre (2018)

Likewise, and supported by the literature review supported on the mobile forensics process from both Ayers et al. (2014) and Sathe & Dongre (2018), one will scrutinize and describe each of the steps that one chose for the support and strategy of the toolbox.

As such, in the in the first step, 1st Identification & Preservation, it is highly crucial for the digital investigator to not modify the physical and digital evidence collected, as to prevent from any modifications to occur and that may jeopardize the quality of the investigation and its respective evidence. According to the literature analyzed, the first technique to use when retrieving a mobile phone is to turn on the airplane mode on it, as this mode will prevent and block any communication and connection to the networks available, Wi-fi and Bluetooth. The second technique is to shut down the device, by switching it off, which will similarly to the first technique focus on blocking communications into and out the mobile phone. Lastly, but not least, the third technique is to place the mobile phone into a box that will impede the communication, like the Faraday's box, which represent a shield box that is able to cell block network and radio interactions from the mobile phone to the outside (Ayers et al., 2014; Faheem et al., 2016; Barmpatsalou et al., 2018). As such, the tools and applications chosen for this step should be ones that are able to prevent and protect the evidence both physical (mobile phone, memory chip, SIM card and any other hardware component) and digital (the contents of the hardware afore mentioned). This can be done by blocking and impeding any communication from and into the mobile phone and by creating an exact copy and replica of the mobile phone and its components. Accordingly, Sathe & Dongre (2018) perceive that it is also important at this stage to decide whether the mobile phone and its data (identification) will be pertinent and important for a digital investigation.

The second step, 2º Acquisition and Extraction, where the digital investigator should intent to start the procedures towards the collection and retrieval of a replica of the device's image, which should be an exact copy of the mobile phone and its content and thus, the digital investigator is mitigating two different risks, the risk of someone attempting to communicate with the mobile phone after being retrieved, and the risk of the device's physical conditions and its battery life stamina. As such, the tools and applications chosen for this phases, should be ones that are able to replicate the device image, and/or perform different levels of extraction and acquisitions, as mentioned in the literature review, there are different levels of acquisitions such as the, Manual extraction (acquisition of the data and information that is store in the device itself and that needs no tool), Logical extraction (acquisition of data and information by connecting the device into a computer or a forensics workstation, via USB, Wi-Fi or Bluetooth), Hex dumping extraction (physical acquisition that involves the extraction of data that is residing in a memory card or any type of memory hardware that is a component of the mobile phone), Chip-off extraction (the action of retrieving and extracting the flash memory chip of a mobile phone with a tool that is able to open and deconstruct the mobile phone) and lastly but not least, the micro read extraction (the activity that involves using an electron microscope to conduct physical observations around the logic gates and circuits of a mobile phone) (Chernyshev et al., 2017; Ayers et al., 2014).

The third step, 3º Analysis and Examination, highlights the importance of the digital investigator to be aware and to have access to tools and applications that will allow for further analysis on the data and information collected and retrieved from the 1st and 2º stage. This data can be phonebook numbers, call and messages logs, both text and multimedia, photos, document files, videos, locations track points, emails, browser history and many more, being also data that may have been hidden or deleted (Ayers et al., 2014; Sathe & Dongre, 2018).

Lastly, the final step, the 4th Documentation & Report, is where the digital investigator should focus on document the process that was pursued in all of the phases/steps in the investigation, as well as the evidence that corroborate the process and its conclusions as to be able to have a report that is admissible to a courthouse and that can be a potential vital information for a given case (Ayers et al., 2014; Sathe & Dongre, 2018).

5.5. Toolbox Instantiation and its Structural Design

Given the afore mentioned and given the chosen strategy to support the analysis and choice of the tools and applications that should potentially compose the toolbox, the following applications were analyzed and corresponded to each of the mobile forensics strategy chosen, namely the following 33 applications and tools: Project-A-Phone, NFI Memory toolkit, BitPim Tool, LiME - Linux Memory Extractor, Paladin Forensic Suite and its Autopsy Software, Universal Forensic Extraction Device (UFED) & UFED Chinex device, UFED Physical Analyzer, UFED Touch, AccessData Forensic Toolkit FTK Imager, Guidance Encase, Micro Systemation XRY, EnCase Neutrino, Paraben Device Seizure, BlackLight, Oxygen Forensic Suite Kit, Android SDK (Software Developer Kit), Magnet Axiom, qtADB, SQLite Forensics Toolkit, Fernico ZRT, EDEC Eclipse, Micro Systemation XAMN, iSesamo Phone Opening Tool, Xytronic 988D Solder Rework Station, FEITA Digital inspection station, Circuit Board Holder, FINALMobile Forensics, Susteen Secure View, MOBILedit! Forensic, Andriller, Encase LinEn, Passware Kit Forensic, Elcomsoft iOS Forensic Toolkit.

Through the analysis of the literature available to each of this tools and applications one draw the toolbox architecture having the following attributes for each of the 33 applications analyzed: The step that the tools and applications are most likely to fit in the Process Flow of the Toolbox Supporting Mobile Forensics Investigation Process (1º Identification & Preservation, 2º Acquisition & Extraction, 3º Analysis & Examination, and 4º Documentation & Report), the Free/Paid Feature and the Motivation/Issue/Usage that characterizes each of them. After doing so, one described and analyzed each of the 33 tools and applications, describing for each, the main characteristics, what are they suitable for, some results of tests performed and available on the literature and more information around them. As such one started by describing the first application/tool presented in the toolbox, namely the following:

Project-A-Phone tool - The Project-A-Phone tool can be suitable for an investigation, namely those that require manual examinations or that due to the non-availability of an imaging application or device during an investigation, force the digital investigator to leverage on this tool to perform a manual analysis (Hayes, 2014). This tool, functions as a peripherical one, which includes a high-resolution camera, that allows the user to integrate this tool with others, and thus, creating synergies. Likewise, this tool allows the digital investigator to operate within the mobile phone, by taking screenshots of every step that is pursued and taken during the investigation, creating an instant JPEG, PNG or BMP image files, and automatically yielding sequenced names to each of the images taken (Graves, 2013; Hayes, 2014). What's more, this tool allows for the sequenced organization of all the evidence collected during the investigation process, allowing the user to record audio and video frames during the examination process, as well as letting the user leverage on voice commentary during the process. Due to the size of this device, it allows the user to handle close to any mobile phone in the market, as its equipment allows the tool to adjust to any phone size and measures. Besides this, the tool can be used to document the work pursued as it contains in its characteristics a reporting tool. It is important to notice that this tool requires the mobile phone to be turned on, thus, if not correctly isolated, this tool should not be employed, or be used as a last option, as it makes the mobile phone more vulnerable to outside connections, that can jeopardize the investigation by erasing or hiding the data and its information (Mullen, 2006; Hayes, 2014).

The NFI Memory Toolkit tool - The NFI Memory Toolkit device represents a universal tool designated as the combination and articulation of hardware and software, while allowing the digital investigator to read memory chips and by doing so, retrieving important data, including low-level data extractions and acquisitions. On one hand, the hardware allows this toolkit to connect physically with the memory chip of the mobile device, and on the other hand, the software side allows the tool to undergo the required and necessary queries that the digital investigator needs to access the data inside the memory chip. Likewise, it can perform in damaged and/or password-protected mobile phones, and retrieve several types of data, phone calls registered, the phone book numbers, pictures, multimedia and it may be able to retrieve browser history (Netherlands Forensic Institute, 2011).

The BitPim Tool - The BitPim tool can be regarded as an open source and free tool, that can be used to manage, operate and view the data from a mobile phone, including data from phones that contain basic features. To do so, the tool leverages on the proper connection between the forensic workstation (the station where the forensics investigator is pursuing the investigation process) and the mobile phone device. The data included can be the phone calls and messages logs, multimedia such as video and images, calendar files and contacts (Ayers et al., 2005; Hayes, 2014). Notwithstanding, this tool has not been updated since 2010, which according to Bachler (n.d.), cause many phones to not be recognized by the forensic workstation when connected via USB Port, and thus, the tool is not able to examine the phones.

LiME - Linux Memory Extractor - It is a tool, an open-source and free tool, can be perceived as a technique and tool to retrieve and capture volatile memory from an android phone or any Linux-based one. It works via debugging bridge via USB, between the mobile device and the forensics workstation where the application is, to perform memory retrieval from Android Phones. This tool is thus able to capture a forensic image of the mobile phone. Accordingly, this tool aims to minimize the interaction between the forensics examiner and the kernel (i.e., the central component of an operating system) space processes during the acquisition phase, hence by doing so, it yields captures that are more accurate when it comes to forensics analysis (Heriyanto et al., 2015).

Paladin Forensic Suite and its Autopsy Software - From Sumuri (Paladin's Provider), Paladin represents an open-source toolkit application and suite, which is utilized by the connection of the mobile device to the computer and/or forensics workstation (Sumuri LLC, 2016; Bachler, n.d.). It encompasses a wide variety of open-source tools, like the Autopsy, and many others, which focus on imaging the mobile phone, on recovering and analyzing information from calls and messages to emails, logs and multimedia like photos and videos, while giving the digital investigator several tools present in a user-friendly GUI and that will potentially guide and aid the investigator process. The Autopsy represents an open-source forensics tool, that allows the digital investigator to analyze the imaged create from the mobile device (the step of imaging must be pursued using a different tool), to manage and analyze the digital evidence collected and to document and create a chronological timeline for all the actions that were performed within each phone. This tool is able to perform the manual examination and access raw files retrieved from an android mobile phone. Accordingly, this tool must run on the forensics workstation and is able to retrieve artifacts such as call and text messages logs, multimedia, gps track points and more (Bommisetty et al., 2014).

Universal Forensic Extraction Device (UFED) and UFED Chinex - The Universal Forensic Extraction Device (UFED) represents a commercial device, a separate hardware device, from Cellebrite, that aims at performing image extraction to the mobile devices due to their physical extraction capabilities (Lessard & Kessler, 2010). In order to do so, the digital investigator needs to connect the mobile phone to the UFED device, which will aim at capturing all the available information, from contacts and dials logs, to messages, multimedia, files. This device also supports, Bluetooth and infrared transmission (Lessard & Kessler, 2010; Graves, 2013). This device is also able to perform logical acquisitions, which is represented by the extraction of the data and information present in the logical file allocation memory of a mobile phone (Omeleze & Venter, 2013). Likewise, the device is able to perform physical examination of the mobile phone, increasing the success of reaching and retrieving deleted or missing data from the mobile phone (Shortall & Azhar, 2015). Besides this, the device can also clone SIM cards, and be able to extract information from message applications like the WhatsApp. As such, the UFED can retrieve and gather information from the SIM, even if it is inside the Mobile Phone (Lessard & Kessler, 2010).

Universal Forensic Extraction Device (UFED) Physical Analyzer - The Universal Forensic Extraction Device (UFED) Physical Analyzer represents an analytical platform, from Cellebrite, that aims at performing analyses to the image extracted from a mobile phone. It encloses the analysis of evidence that were retrieved from a mobile Phone, while allowing for both logical and physical analysis through the platform that comes with it, namely the query for words and keywords, shape the data, and create tailored reports on the data so to reach different conclusions and to support the analysis (Bommisetty et al., 2014).

Universal Forensic Extraction Device (UFED) Touch - The Universal Forensic Extraction Device (UFED) Touch, represents a portable compact version from Cellebrite, that can be used in any type of mobile devices investigation, as besides acquiring, and performing different levels of extractions, it allows the user to create an exact copy of the memory of the Mobile Device. Likewise, it also supports the file system extraction. As such, it can acquire levels of extraction such as the physical, the logical and the file system one. In addition, this tool can also capture screenshots of a mobile phone, while yielding the digital investigator with a list of activities that can be performed to conduct several different analyses to the mobile image (Bachler, n.d.). This tool contains an easy to use and analyze GUI (Graphic User Interface), while at the same time It also captures screenshots of the mobile phone. According to Hayes (2014), this tool can be used within the field or in a forensics laboratory/workstation.

AccessData Forensic Toolkit FTK Imager - FTK Imager tool is usually used for physical acquisition, as it can extract the data and information present in the memory chip of a mobile phone, through the connection via USB of the phone to the forensics workstation (Lessard & Kessler, 2010). Besides this, the tool can help the digital investigator in pursuing the physical examination and analysis on different types of data, namely, Contacts book, text, and multimedia messages, call logs, pictures, and multimedia files (Al-Sabaawi & Foo, 2019). Likewise, according to Rao & Chakravarthy (2016), to analyze the different type of data, an investigator can employ the FTK Imager tool, which will allow to analyze the capture images of the partitions, data, cache, and system, including applications' data and the memory chip data. As so, according to the authors to leverage of this applications' full potential, the digital investigator should be capable of rooting the device, as to gain access and privileges as a root user, allowing for deeper and critical access. Accordingly, Jadhav & Joshi (2016) perceive the FTK Imager as a tool that will allow the investigator to gather information such as the IMEI number and other important one on the device status and on the manufacturer's information. In fact, Shortall & Azhar (2015), refer this tool as one of the most available one in the market to perform the imaging of a mobile phone. In addition, the authors, Alhassan et al. (2018), noticed that this tool can not only be able to collect data/evidence that somehow was deleted, such as documents and multimedia files, but also, can gather different data from the mobile's memory, while noticing that the tool was not able to neither spot nor recover any data from the SIM card.

Guidance Encase - The Encase forensic tool focus on acquiring and capturing the digital evidence by imaging the mobile phone through the usage of its disk imaging functions. This tool, which runs under the Windows operating system corresponds to a forensics tool designed for the imaging of mobile phones as well as a provide different and various features to the digital investigator (Byers & Shahmehri, 2009). The Encase tool contains the characteristic, just like the FTK imager, to allow for a client-server remote forensics, in which, an executable is set on the client workstation. According to the author, this may be a useful feature when it comes to remote forensics, where the workstations may be geographically spread, and the digital investigators' team is consolidated in one location (Dykstra, & Sherman, 2012). The authors, Alhassan et al. (2018), noticed that this tool could not collect deleted data from the mobile device.

Micro Systemation XRY - The Micro Systemation XRY can be perceived as a mobile device forensic tool, which was built and formed by Micro Systemation. This tool guides the digital investigator throughout the process and is able and available for logical (extracting information by communicating with the mobile operating system) and physical (retrieving the available raw evidence that are residing in the mobile phone) examination and analysis on mobile phone devices (Hoog, 2011). According to the author, one of the most exclusive characteristics that distinguish this tool, is the fact, that it embodies a device manual which comprises a comprehensive list of the support that is presented for each mobile phone, as well as aids the investigator finding what type and kind of data can be collected and what the application cannot retrieve. Accordingly, the author refers that this application can also offer different options report wise, as the investigator can generate reports in different formats, such as Word, Excel, or PDF, which may include data and evidence regarding the respective analysis. Gajjar & Sharma (2020) denote that this tool, commercial forensics one, provides a fast-paced extraction and acquisition technique, that leverage on the Windows operation system, and that can retrieve and analyse information from mobile phones, such as phonebook, Multimedia and document files, messages as well as calls logs.

Encase Neutrino - According to Hoog (2011), the Encase Neutrino tool was developed to answer the needs of one that needs to forensically retrieve data from a mobile phone and perform analysis, in order to reach a conclusion or to corroborate one. This tool focus on mobile phones with different operating systems, from the IOS, to Android and Windows mobile. Accordingly, the author refers that with this tool the investigator can be able to retrieve, examine and conserve different types of data, from Phone book, text, and multimedia messages, call and emails logs, calendar information, images and videos, and other types of files that may be on the mobile phone. Likewise, the author refers that one of the advantages of Encase Neutrino was its capability to integrate compatibly with any tool from Encase, like the ones analysed in this research, allowing for deeper and integrate analysis. Besides this, this tool can also create and generate reports in formats like the HTML, allowing for the digital investigator to contain all the report in one set page. Notwithstanding, the author tested this tool, and observed that it was not possible to recover deleted text messages, and it was not possible to retrieve the phones and/or multimedia videos that resided in the phone's memory card, just the ones that were sent as a Multimedia Message. Throughout the research, and by analysing the literature available it seems that this tool was discontinued by its manufacturer.

Blacklight - This mobile forensics' tool represents a comprehensive one, and it is seen as a multi-platform, that helps the digital investigator to pursuit the mobile forensics process within the iOS devices, such as the iPhone and iPad, on Android devices and on Windows computers. This tool contains a unique GUI (Graphical user interface), that was designed and built to answer to the needs of forensics examiners, containing capabilities and a friendly and insightful user experience, on all steps of the mobile forensics' investigation process. Likewise, Blacklight is expected to be able to help the investigator in the acquisition phase of the data on the internal memory of a mobile phone, while being also able to aid the examiner in the reporting stage with the generation of the reports, namely custom ones. In fact, this tool is expected to be able to collect data on the equipment and its user (device type, OS version, IMEI), on the book numbers, on calls and messages logs, document files, application data, gps location trackpoints and internet data (Homeland Security, 2016). Likewise, the tool also yields the investigator with the capability to use filter option within large data sets, allow the investigator to apply any filters to quickly seek and retrieve the information that one is looking for, including filter by name, file type and/or attribute.

Paraben Device Seizure - Perceive as a software kit by Paraben's, it aims at allowing the digital investigator to extract, collect, examine, and conclude on the data retrieved from a mobile phone. Likewise, it is a handheld mobile forensics kit that allows for logical and physical data acquisitions, and it is expected to be able to perform the recovery of erased data and full data dumps. Hence, allowing for the analysis and visualization of the data that was acquired and for the bookmarking of the data that is being analysed permitting the investigator to filter within the data by using text strings queries to retrieve and dive in the data that the digital investigator is looking for. According to the author (Hoog, 2011), this software kit is regarded as one that does not modify and alter the digital evidence retrieved in any stage, as it acquires data by connecting the device through an USB data cable to the forensics workstation. Moreover, accordingly the Device Seizure (DS) allows the digital investigator to retrieve and transfer any file to the workstation for further analysis and documentation (Ayers et al., 2005; Hoog, 2011). Besides this, according to Alhassan et al. (2018), this kit is an effective one, which can with high accuracy and effectiveness access to the phone's memory and retrieve important and critical data, even those that were somehow deleted.

Oxygen Forensic Suite Kit - According to Cappa et. Al (2016), the Oxygen Forensic Suite Kit is one of the most noteworthy tools and solutions in the market for the pursual of digital mobile forensics and that establish a connection to the mobile phone via USB. Accordingly, the authors denote that while there is a great rise in the need for mobile forensics tools and capabilities, the high initial price plus maintenance costs are usually some of the characteristics of the commercial mobile forensics' tools. Likewise, Bommisetty et al. (2014), denote that this tool is an advanced one, that allows the digital investigator to recover, retrieve and analyse data from mobile devices, proving logical guidance for different types and models of mobile phones and allowing for a fully computerized acquisition and examination process. Besides this, the tool allows for the integration of images/backups retrieve from a mobile phone using tools like the Cellebrite and XRY, henceforth the digital investigator is able to pursuit analysis on the Oxygen tool. Despite not being able to perform physical and file system extractions, and hence not retrieving a full forensic image, this tool supports logical acquisition and thus, is expected to be able to recover and retrieve data like the book numbers and its photos, calendar details and events, call and messages logs, events logs, pictures, video and audio multimedia, passwords, locations, device and user informational data, emails and its accounts. Even so, it may be able to recover erased data from SQLite databases, thus recovering, erased messages, calls, emails and photos. What's more, the tool contains features, like the filtering of the data using keywords and/or regular expressions, report generation in different formats, like the Word, Excel, PDF and HTML, manual analysis of data, a user-friendly and accessible user interface, and a timeline where it is registered the user's actions and movements organised by data and time (Bommisetty et al., 2014; Asim et al., 2019).

Android SDK (Software Developer Kit) - According to Bommisetty et al. (2014), the Android Software Developer Kit (SDK) corresponds to one tool that aims to allow and guide a user to develop, build, quality test and debug into production applications to be executed and run-on Android operating system phones. Although it does not correspond to a forensics tool but itself, as it involves software libraries, tools and documentations material, it allows the investigator to be provided with valuable and insightful documentation and support that can aid one within an investigation of an Android Device. Hence, the authors, suggest the digital investigator to obtain a deep and good understanding and knowledge of the Android SDK as to understand the particularities of a mobile device and the data on it (Bommisetty et al., 2014).

Magnet Axiom - Magnet Axiom corresponds to a tool which allows to load the imaged that was created based on the user data and analyse that image, and thus, analysing data such as multimedia, browser and activity history, documents, and personal data. This tool can also be applied and employed to document the analysis and the reporting evidence that were under examination and that are vital for the conclusions taken that is performed as well as the documentation of all log files that illustrate the reperformance of the analysis that was performed (Gajjar & Sharma, 2020).

qtADB - Jadhav & Joshi (2016) suggest that the digital investigator should leverage on tools like the Android SDK, Magnet Axiom, qtADB, FTK Imager and SQLite Forensics. The application qtADB will help the digital investigator to locate where important data is, namely the user data. At this stage, the investigator should be look at the block of the mobile phone that contains the user data, which will represent all the data that is stored in the device's external and/or internal memory and relates to the user and its activity while using the mobile phone.

SQLite Forensics Toolkit - As previously mentioned, for Jadhav & Joshi (2016), a tool that allows the digital investigator to perform analysis on the browser favourites, history and activity is the SQLite Forensics. Accordingly, the authors Kim et al. (2018), perceived that a big part of the data and information that is stored in a mobile phone and that it creates, and transfers may be registered in as a log files, which are normally in the SQLite DB format, as such, the SQLite Forensics tool is able to perform analysis on this data, as well as to yield the digital investigator with techniques to quickly filter and search for a given set of data just like in a database. In fact, according to Bommisetty et al. (2014), the SQLite format is a controlled SQL database engine, used by almost every mobile phone including iOS and android devices. This database format is an open source one, that contains multiple tables and views, being portable and accurate at the same time, which is being heavily used by the mobile phones for the purpose of data storage.

Fernico ZRT - Just like the device Project-a-Phone, it consists of a tool that was created with the purpose of photographing the mobile phone's screen, while using a digital camera to do so, and allowing for the documentation of the process that the digital investigator pursues on the analysis (Hayes, 2014). This tool is used for the purpose of performing the manual acquisition of data, which consists of the investigator using the phones screen to get the phone content directly from using the mobile phone, as such, this method, works with every mobile phone and requires not training at all, however, it does not preserve the integrity of the digital evidence in analysis and does not perform the extraction and acquisition of data that is missing or that was erased (Abdulla et al., 2012).

Micro Systemation XAMN - As previously analysed, the XAMN is from Micro Systemation, who is also developed XRY. With XAMN, the company intends to perform link analysis around the mobile phones' forensics investigation, i.e., allowing the digital investigator to leverage on multiple images for different smartphone, while quickly identifying similarities and differences between the phones, including the phones book (Hayes, 2014). Accordingly, this type of analysis may be relevant when try to search and seek what could suspects and victims may have in common. Besides this, the tool contains a calendar and a chronological feature visualization, allowing to link the time and the place where a supposed suspect and/or victim were at that given time (Kim, 2020; Hayes, 2014).

MOBILedit! Forensic - According to Bommisetty et al. (2014), the MOBILedit mobile forensic tool, can be employed by the digital investigator, to visualize, search, find and extract data from a mobile phone namely, the call logs, phone numbers, text and multimedia numbers, document files, calendars and event files, application data, while also, extracting some information on the mobile phone itself, such as the IMEI, and details on the SIM card. In fact, the authors perceived that under some circumstances the tool is capable of extracting deleted data from the mobile phones and backups encryptions. This software yields the investigator capabilities that allow for logical acquisition of data, and by doing so, it allows for examinations and reports on that data, it connects to the mobile phone through infrared, Bluetooth or cable wise. This application identifies critical information of the mobile phone, such as the manufacturer, number of the mobile and IMEI. It can retrieve information like the SIM card phone calls logs and book, last registered numbers dialled, messages, files, multimedia (Alhassan et al., 2018). Moreover, according to Hoog (2011) and Hayes (2014), this tool is able to generate investigation reports in different languages, with preprepared templates, that were developed and designed according to set needs. What's more, this application allows the digital investigator to clone the SIM card and retrieve the information it (Gajjar & Sharma, 2020).

Encase LinEN - From the same manufacturer of the Encase analysed previously, the LinEN software is based on Linux operating system and aims at the disk imaging, i.e., creation of disk images which will then be compatible with the Encase software previously analysed (Byers & Shahmehri, 2009).

Andriller - According to Silveira et al (2020), Andriller represents one of the forensics tools and suites that provide the digital investigator with the capability to acquire and examine data that was extracted from a mobile device. It is designed and focus on the android OS mobile phones working through the connection via USB port from the computer/forensics workstation to the mobile phone, and thus other types of operating systems are not recognized using this tool (Bachler, n.d.). Accordingly, Asim et al. (2019), denote that this forensic tool offers digital investigators tools that allow for the unlock of smartphones, including phones that are Pattern locked, or that contain a Password or a pin combination.

Passware Kit Forensic - The Passware Kit Forensic intents at searching the passwords for iOS and Android mobile phones' backups as well as it is able to acquire Android images, extracting the data from it. It is able to integrate with other software, like the Oxygen Forensic Suite analysed in this thesis (Passware Inc., 2017).

Elcomsoft iOS Forensic Toolkit - According to Hoog (2011), the Elcomsoft iOS Forensic Toolkit, is a commercial application for iOS mobile phones, focusing on being able to perform the physical extraction and acquisition on mobile devices running the iOS operating system, namely, the iPhones and the iPads. Accordingly, this tool is also expected to be able to retrieve critical information on the device and its file system, namely, passwords and encryption keys, and it is supported by both Windows OS and Mac OS (iOS).

Other Relevant tools for the Mobile Forensics Investigation Process - EDEC Eclipse, just like Fernico ZRT and the Project-a-Phone hardware and software kit, represents a tool that allows for the manual extraction of data, where the digital investigator goes through the device's touch screen and/or keypad, and the steps and data are documented in photos taken directly with the EDEC Eclipse device (Attar & Kapale, 2019). As for the technique of Chip-off extraction and acquisition, which intends the data to be directly retrieve from the flash memory of the mobile phone, which is removed through the retrieval of the mobile phone's memory chip directly from the phone. In order to do so, (Attar & Kapale, 2019) suggests tools like the Xytronic 988D Solder Rework Station, iSesamo Phone Opening Tool, FEITA Digital inspection station and Circuit Board Holder. In addition, according to Homeland Security (2020), the Final Mobile Forensics tool, can be used to capture and/or perform analysis and examinations within a mobile phone via logical and/or physical acquisitions of data. This tool can also be applied to identify information and data, like the locations, text and multimedia messages, video, audio, social media, and applications data (Silveira et al., 2020). Likewise, Homeland Security (2016), tested the mobile device acquisition tool, Susteen Secure View provides the digital investigator with the ability to perform logical and physical acquisitions of data for different mobile devices, including the retrieval and collection of phone book, calls and text messages logs, calendar events, applications, and erased data, yielding the digital investigator with a friendly and accessible graphical interface. To sum up the toolbox generated as well as the main features and characteristics of each of the applications and tools analysed, one generated a table containing this information as for the reader to have an overview of the toolbox and its components, namely, the following:

Toolbox Tools and Applications	Process Flow of the Toolbox Supporting Mobile Forensics Process				Free/Paid Feature	Summary of the Motivation/Issue/Usage
	1º Identification & Preservation	2º Acquisition & Extraction	3º Analysis & Examination	4º Documentation & Report		
Project-A-Phone		x		x	Paid	This tool can be suitable for an investigation that require manual examinations or that due to the non-availability of an imaging application or device during an investigation. It functions as a peripherical one, which includes a high-resolution camera, that allows the user to integrate this tool with others. This tool also allows the digital investigator to operate within the mobile phone, by taking screenshots of every step that is pursued and taken during the investigation, automatically yielding sequenced names to each of the images taken, while allowing the user to record audio and video frames during the examination process, as well as letting the user leverage on voice commentary during the process. Due to the size of this device, it allows the user to handle close to any mobile phone in the market.
NFI Memory toolkit		x			Paid	Represents a universal tool designated as the combination and articulation of hardware and software, while allowing the digital investigator to read memory chips. The hardware allows this toolkit to connect physically with the memory chip of the mobile device, and the software side allows the tool to undergo the required and necessary queries that the digital investigator needs to access the data inside the memory chip. It can also perform in damaged and/or password-protected mobile phones.
BitPim Tool		x	x		Free - Open Source	This tool, an open source and free tool, can be used to manage, operate, and view the data from a mobile phone, including data from phones that contain basic features. To do so, the tool leverages on the proper connection between the forensic workstation (the station where the forensics investigator is pursuing the investigation process) and the mobile phone device.
LiME - Linux Memory Extractor		x			Free - Open Source	The LiME, an open-source and free tool is a technique and tool to retrieve and capture volatile memory from an android phone or any Linux-based one. It works via debugging bridge via USB, between the mobile device and the forensics workstation where the application is, to perform memory retrieval from Android Phones. This tool is thus able to capture a forensic image of the mobile phone.

Toolbox Tools and Applications	Process Flow of the Toolbox Supporting Mobile Forensics Process				Free/Paid Feature	Summary of the Motivation/Issue/Usage
	1º Identification & Preservation	2º Acquisition & Extraction	3º Analysis & Examination	4º Documentation & Report		
Paladin Forensic Suite and its Autopsy Software		x	x	x	Free - Open Source	Paladin represents an open-source toolkit application and suite, which is utilized by the connection of the mobile device to the computer and/or forensics workstation. It encompasses a wide variety of open-source tools, like the Autopsy, and many others, which focus on imaging the mobile phone, on recovering and analysing information from calls and messages to emails, logs and multimedia like photos and videos, while giving the digital investigator several tools present in a user-friendly GUI and that will potentially guide and aid the investigator process. The Autopsy, an open-source forensics tool, that allows the digital investigator to analyse the imaged create from the mobile device, and to manage and analyse the digital evidence collected and to document and create a chronological timeline for all the actions that were performed within each phone. This tool is able to perform the manual examination and access raw files retrieved from an android mobile phone.
Universal Forensic Extraction Device (UFED) & UFED Chinex device	x	x			Paid	It represents a commercial device, a separate hardware one, that aims at performing image extraction to the mobile devices due to their physical extraction capabilities. This device also supports, Bluetooth and infrared transmission, and is also able to perform logical acquisitions and physical examination of the mobile phone, increasing the success of reaching and retrieving deleted or missing data from the mobile phone. Besides this, the device can also clone SIM cards, and be able to extract information from message applications like the WhatsApp.
UFED Physical Analyzer			x	x	Paid	It represents an analytical platform, from Cellebrite, that aims at performing analyses to the image extracted from a mobile phone. It encloses the analysis of evidence that were retrieved from a mobile Phone, while allowing for both logical and physical analysis through the platform that comes with it, namely the query for words and keywords, shape the data, and create tailored reports.
UFED Touch	x	x	x		Paid	It represents a portable compact version from Cellebrite, that can be used in any type of mobile devices investigation, as besides acquiring, and performing different levels of extractions, it allows the user to create an exact copy of the memory of the Mobile Device. It also supports the file system extraction, physical and logical ones. This tool can also capture screenshots of a mobile phone, while yielding the digital investigator with a list of activities that can be performed to conduct several different analyses to the mobile image. This tool contains an easy to use and analyse GUI, while at the same time It also captures screenshots of the mobile phone.

Toolbox Tools and Applications	Process Flow of the Toolbox Supporting Mobile Forensics Process				Free/Paid Feature	Summary of the Motivation/Issue/Usage
	1º Identification & Preservation	2º Acquisition & Extraction	3º Analysis & Examination	4º Documentation & Report		
AccessData Forensic Toolkit FTK Imager		x	x		Free	It is usually used for physical acquisition and analysis, as it can extract the data and information present in the memory chip of a mobile phone. An investigator can also employ the FTK Imager tool, which will allow to analyse the capture images of the partitions, data, cache and system, including applications' data and the memory chip data. It can gather information such as the IMEI number and other on the device status and on the manufacturer's information.
Guidance Encase		x	x	x	Paid	The Encase forensic tool focus on acquiring and capturing the digital evidence by imaging the mobile phone through the usage of its disk imaging functions. The tool contains the characteristic, just like the FTK imager, to allow for a client-server remote forensics, in which, an executable is set on the client workstation.
Micro Systemation XRY		x	x	x	Paid	It guides the digital investigator throughout the process and is able and available for logical examination and analysis on mobile phone devices. It embodies a device manual which comprises a comprehensive list of the support that is presented for each mobile phone, as well as aids the investigator finding what type and kind of data can be collected and what the application cannot retrieve. It can also offer different options report wise, which may include data and evidence regarding the respective analysis.
EnCase Neutrino		x	x	x	Paid	This tool focus on mobile phones with different operating systems, from the IOS, to Android and Windows mobile. It can be able to retrieve, examine and conserve different types of data and it is likely to be capable of integrate compatibly with any tool from Encase, like the ones analysed in this research. This tool can also create and generate reports in formats. Throughout the research, and by analysing the literature available it seems that this tool was discontinued by its manufacturer.
BlackLight		x	x	x	Paid	It is a multi-platform, that helps the digital investigator to pursuit the mobile forensics process within the iOS devices, such as the iPhone and iPad, on Android devices and on Windows computers. This tool contains a unique GUI (Graphical user interface). It is expected to be able to help the investigator in the acquisition phase of the data on the internal memory of a mobile phone, while being also able to aid the examiner in the reporting stage with the generation of the reports, namely custom ones. In fact, this tool is expected to be able to collect data on the equipment and its user (device type, OS version, IMEI). The tool also yields the investigator with the capability to use filter option within large data sets, allow the investigator to apply any filters to quickly seek and retrieve the information that one is looking for, including filter by name, file type and/or attribute.

Toolbox Tools and Applications	Process Flow of the Toolbox Supporting Mobile Forensics Process				Free/Paid Feature	Summary of the Motivation/Issue/Usage
	1º Identification & Preservation	2º Acquisition & Extraction	3º Analysis & Examination	4º Documentation & Report		
Paraben Device Seizure	x	x	x		Paid	Perceive as a software kit by Paraben's, it aims at allowing the digital investigator to extract, collect, examine and conclude on the data retrieved from a mobile phone. Likewise, it is a handheld mobile forensics kit that allows for logical and physical data acquisitions, and it is expected to be able to perform the recovery of erased data and full data dumps. Hence, allowing for the analysis and visualization of the data that was acquired and for the bookmarking of the data that is being analysed permitting the investigator to filter within the data by using text strings queries to retrieve and dive in the data that the digital investigator is looking for.
Oxygen Forensic Suite Kit		x	x	x	Paid/Free (Lower/Limited Capabilities)	This kit is an advanced one, that allows the digital investigator to recover, retrieve and analyse data from mobile devices, proving logical guidance for different types and models of mobile phones and allowing for a fully computerized acquisition and examination process. Besides this, the tool allows for the integration of images/backups retrieve from a mobile phone using tools like the Cellebrite and XRY, henceforth the digital investigator is able to pursuit analysis on the Oxygen tool. Despite not being able to perform physical and file system extractions, and hence not retrieving a full forensic image, this tool supports logical acquisition and thus, is expected to be able to recover and retrieve data. What's more, the tool contains features, like the filtering of the data using keywords and/or regular expressions, report generation in different formats, manual analysis of data, a user-friendly and accessible user interface, and a timeline where it is registered the user's actions and movements organised by data and time.
Android SDK (Software Developer Kit)			x		Free	This tool corresponds to one that aims to allow and guide a user to develop, build, quality test and debug into production applications to be executed and run-on Android operating system phones. Although it does not correspond to a forensics tool but itself, as it involves software libraries, tools and documentations material, it allows the investigator to be provided with valuable and insightful documentation and support that can aid one within an investigation of an Android Device.
Magnet Axiom			x	x	Paid	It is a tool which allows to load the imaged that was created based on the user data and analyse that image, and thus, analysing data. This tool can also be applied and employed to document the analysis and the reporting evidence that were under examination and that are vital for the conclusions taken that is performed as well as the documentation of all log files that illustrate the reperformance of the analysis that was performed.

Toolbox Tools and Applications	Process Flow of the Toolbox Supporting Mobile Forensics Process				Free/Paid Feature	Summary of the Motivation/Issue/Usage
	1º Identification & Preservation	2º Acquisition & Extraction	3º Analysis & Examination	4º Documentation & Report		
qtADB	x				Free	The application qtADB will help the digital investigator to locate where important data is, namely the user data. At this stage, the investigator should be look at the block of the mobile phone that contains the user data, which will represent all the data that is stored in the device's external and/or internal memory and relates to the user and its activity while using the mobile phone.
SQLite Forensics Toolkit		x	x		Paid	It is a tool that allows the digital investigator to perform analysis on the browser favourites, history and activity is the SQLite Forensics. The tool is able to perform analysis on this data, as well as to yield the digital investigator with techniques to quickly filter and search for a given set of data just like in a database.
Fernico ZRT	x	x			Paid	Fernico ZRT, just like the device Project-a-Phone, it consists of a tool that was created with the purpose of photographing the mobile phone's screen, while using a digital camera to do so, and allowing for the documentation of the process that the digital investigator pursues on the analysis. This tool is used for the purpose of performing the manual acquisition of data.
Micro Systemation XAMN			x		Paid	This tool intends to perform link analysis around the mobile phones' forensics investigation, i.e., allowing the digital investigator to leverage on multiple images for different smartphone, while quickly identifying similarities and differences between the phones, including the phones book. This type of analysis may be relevant when try to search and seek what could suspects and victims may have in common. Besides this, the tool contains a calendar and a chronological feature visualization, allowing to link the time and the place where a supposed suspect and/or victim were at that given time.
MOBILedit! Forensic		x	x	x	Paid* Free version (MOBILedit Lite)	This tool can be employed by the digital investigator, to visualize, search, find and extract data from a mobile phone, while also, extracting some information on the mobile phone itself, such as the IMEI, and details on the SIM card. It can under some circumstances extract deleted data from the mobile phones and backups encryptions. This software yields the investigator capabilities that allow for logical acquisition of data, and by doing so, it allows for examinations and reports on that data, it connects to the mobile phone through infrared, Bluetooth or cable wise. This application identifies critical information of the mobile phone, such as the manufacturer, number of the mobile and IMEI. It can retrieve information like the SIM card phone calls logs and book, last registered numbers dialled, messages, files, multimedia. This tool is able to generate investigation reports in different languages, with preprepared templates and clone the SIM cards.

Toolbox Tools and Applications	Process Flow of the Toolbox Supporting Mobile Forensics Process				Free/Paid Feature	Summary of the Motivation/Issue/Usage
	1º Identification & Preservation	2º Acquisition & Extraction	3º Analysis & Examination	4º Documentation & Report		
Encase LinEn		x			Paid	From the same manufacturer of the Encase analysed previously, the LinEN software is based on Linux operating system and aims at the disk imaging, i.e., creation of disk images which will then be compatible with the Encase software previously analysed.
Andriller	x	x			Free/Paid - Open Source	This tool represents one of the forensics tools and suites that provide the digital investigator with the capability to acquire and examine data that was extracted from a mobile device. It is designed and focus on the android OS mobile phones working through the connection via USB port from the computer/forensics workstation to the mobile phone, and thus other types of operating systems are not recognized using this tool. Also, this tool offers digital investigators tools that allow for the unlock of smartphones, including phones that are Pattern locked, or that contain a Password or a pin combination.
Passware Kit Forensic	x	x			Paid	The Passware Kit Forensic intents at searching the passwords for iOS and Android mobile phones' backups as well as it is able to acquire Android images, extracting the data from it. It is able to integrate with other software.
Elcomsoft iOS Forensic Toolkit		x	x		Paid	This Toolkit, is a commercial application for iOS mobile phones, focusing on being able to perform the physical extraction and acquisition on mobile devices running the iOS operating system, namely, the iPhones and the iPads. Accordingly, this tool is also expected to be able to retrieve critical information on the device and its file system, namely, passwords and encryption keys, and it is supported by both Windows OS and Mac OS (iOS).
EDEC Eclipse	x				Paid	EDEC Eclipse, just like Fernico ZRT and the Project-a-Phone hardware and software kit, represents a tool that allows for the manual extraction of data, where the digital investigator goes through the device's touch screen and/or keypad, and the steps and data are documented in photos taken directly with the EDEC Eclipse device.
iSesamo Phone Opening Tool		x			Paid	As for the technique of Chip-off extraction and acquisition, which intends the data to be directly retrieve from the flash memory of the mobile phone, which is removed through the retrieval of the mobile phone's memory chip directly from the phone. In order to do so, tools like, the Xytronic 988D Solder Rework Station, iSesamo Phone Opening Tool, FEITA Digital inspection station and Circuit Board Holder, can be employed.
Xytronic 988D Solder Rework Station		x			Paid	
FEITA Digital inspection station		x			Paid	
Circuit Board Holder		x			Paid	

Toolbox Tools and Applications	Process Flow of the Toolbox Supporting Mobile Forensics Process				Free/Paid Feature	Summary of the Motivation/Issue/Usage
	1º Identification & Preservation	2º Acquisition & Extraction	3º Analysis & Examination	4º Documentation & Report		
FINALMobile Forensics		x	x		Paid	This tool can be used to capture and/or perform analysis and examinations within a mobile phone via logical and/or physical acquisitions of data. This tool can also be applied to identify information and data, like the locations, text and multimedia messages, video, audio, social media and applications data.
Susteen Secure View		x	x		Paid	This tool provides the digital investigator with the ability to perform logical and physical acquisitions of data for different mobile devices, including the retrieval and collection of phone book, calls and text messages logs, calendar events, applications, and erased data, yielding the digital investigator with a friendly and accessible graphical interface.

5.6. VALIDATION

In order to pursue this step of the Design Science Research (DSR) methodology, one proceeded with the Validation phase, where the main objective was to retrieve views, thoughts and validations over the Framework and its main features, as well as, the clarification of the impact that the lack of mobile forensics research, knowledge and tools is having/had on the digital investigations, as well as on facing the increasing cybercrime' rates. As a result, this step was brought out by hosting focus group meeting to discuss and validate the framework chosen. Hence, and as previously mentioned in the Methodology section, this meeting held three participants, namely, the following, a person from the area of computer and network science, a person from the area of Mobile Forensics and digital investigations and a person from the information systems auditing, Digital Forensics and cybersecurity fields. As for the moderator role in this focus group, one of the most important and crucial one to have in this type of research methodology, was the Bruno Bernardo (The author researcher that is writing and performing this work). In fact, it was highly crucial to have the moderator role implemented in this focus group, due to the fact that one is performing this work and thus, is aware and acknowledged the fields of the digital forensics and its branch areas, such as Mobile Device Forensics.

Moreover, the focus group meeting was organised on the 21st of December of 2020. In its arranged agenda, the focus group started with an introduction section that included a briefing presentation of the author/researcher of this master thesis, including the academic and professional background and previous experiences. This was followed by a study objectives section, where one demonstrated to all the three participants, Interviewees, the key research question and the two main objectives of this research, the first, proposing and building a toolbox and the second, acknowledging what are the tools available and how can one leverage on it, to pursue the Digital Forensics analysis.

Likewise, one presented to the participants what was the main planned structure of the systematic literature review, which begun with an overview of the Forensics science, followed by the Digital Forensics, Mobile Forensics and the Mobile Archaeology. Besides this, it was also presented to the participants the main topics of this research study as well as the framework that derived from it, as to set the floor for the discussion and to acknowledge every participant of the research. To do so, one performed an overview of the Methodology that was pursued the Design Science Research (DSR), as well as the demonstration of the reached and built artefact, namely the toolbox of applications and tools to support and enhance the Mobile Device Forensics process as well as the methodology that was chosen regarding the Mobile Forensics field. After acknowledging and creating awareness on the framework reached in this thesis, the three participants were presented with the topics of the questions for the Focus Group that was conducted. Moreover, there was a time for a debriefing on the presentation performed and the topics shown, where each participant presented their thoughts and considerations on the importance of this study.

Furthermore, from the focus group meeting conducted to comprehend the framework proposed for the field of mobile forensics as well as the reality of it in the Portugal and Worldwide, important, and crucial contributions and feedbacks were taken into account and integrated in this work, leveraging on them as a major source of input for the validation of the framework presented. As such, and due to the fact that this focus group was very rich in terms of input and knowledge for this research, it was only included on this section the main synthesis including the key ideas/topics of the feedback and inputs retrieved from each of the three participants. Nonetheless, it was perceived as important to incorporate a more detailed transcription of the Focus Group namely, regarding the key/main topics and ideas discussed. As requested from all the three participants, the names of the participants are not disclosed, and the Focus Group meeting flow was anonymized. The four topics of the questions presented were the following:

Focus Group Meeting – Topics of the Questions to the Stakeholders	
Topic 1	Mobile Forensics challenges and the eventual ethical questions and issues that may urge and appear from a person's/digital investigator usage of Mobile Forensics' Tools.
Topic 2	The Utility and contribution of the presented framework for the Mobile Devices Forensics science and for the investigators.
Topic 3	Reflections and insights on what were studied, as well as the relevance, validity, and viability of what was proposed as a framework.
Topic 4	Opinions and feedback containing criticism and suggestions for improvements as well as what in the views of the participants are the future and next steps for this field and research developed on it.

Regarding the initial debriefing and opinions regarding this master thesis, the feedback obtained from I1, was that a toolbox ready to be implemented or utilized comes really handy for a digital investigator in what regards a forensics investigation, and a parallel could be stablished between this field and the computer or any technology that allows user interactivity and storage. Likewise, the Interviewee 2, reflected on the fact that the process may be similar on the mobile phones to the one within the personal computer, which is one type of technology commonly used within any Digital Forensics' investigation. Accordingly, I2 mentioned that both the mobile phones and the computer, a more traditional technology, in what regards the technicalities are similar, as one has a disk with data, and if you have the capabilities to capture that information, the next steps are similar to those that can be performed in any Digital Forensics process. I2 pointed out that a mobile phone is represented by a disk with bites and bytes where in some, the content is encrypted in others is not.

Regarding the Topic 1, with respect to the Mobile Forensics challenges and the eventual ethical questions and issues that may urge within an investigation of these type, the answers were the following: The Interviewee 1 acknowledged that in the Mobile Devices there is the way of functioning, which implies that the digital investigator has access to plenty much everything that is on the phone, accordingly, the I1 refers that with root privileges, the digital investigator has everything, what he/she cannot find is because it does not exist on the phone itself. As a first challenge that the Mobile Forensics field is facing at the moment, the interviewees reflected on the different ethical questions that may urge within an investigation. According to Interviewee 2, within an investigation that is being performed by a company related to a corporative investigation, what usually happens is that there is a lock within the investigation itself, when the digital investigator tries to access corporative information and not personal one.

According to the Interview 1, the challenges that the Mobile Devices Forensics field is currently facing, is the fact that the mobile device's architecture specially the newer ones, were built from the source, within a security environment, which contains as one of the biggest pillars the information' privacy and its security. As such, I1, reflected that the full android architecture was built and sketched based on the types of privileges, bringing special attention to the root privileges and those that were given to each of the different critical activities that can be performed within a mobile phone. Likewise, the I1, mentioned that the architecture of traditional computers has evolved, with the focus of being fully compatible with the different technologies, as such, they are universal and opened. In the case of mobile phones, I1 perceives that they are specific personal objects, which were drawn with the objective to belong to a person and to be personal, and as such they have different purposes as from a personal computer which can be personal but to more than one person.

I1, also reflected that another challenge is the fact that the question of a mobile phone containing personal/professional information is now more relevant than ever, as mobile phones can be a dual-sim one, which may contain data from more than one operator, and allows for the user to have a mode for personal usage and one other for professional usage, raising the difficulty for a digital investigator to be able to split this two worlds of information, personal versus professional, company-wise one. The participant I2, pointed out that the differences between the mobile phones and the traditional computer are emphasized by the capturing process, where in the mobile phones there are distinct characteristics and there is more contamination of what personal wise world and professional world is. In fact, according to I2, nowadays there is the trend for companies to implement the program "bring your own device", where this commodity allows the employees to have their own device both for personal and professional usage, which will increase even more the difficulty in distinguish what is personal from what is company-wise. As such, for I2, if there is the need to separate these two environments, personal from professional, and there is the need to guarantee the traceability of what is captured in the context of Mobile Forensics, then, there should be put into practice the possible implementation of a set of tools at the basis of the operating system of a mobile phone, where the own device should communicate the hash (encryption key) of the image of the mobile phone in a certain time, and where the operator could access this information and potentially share it with a digital investigator under legal requirements.

Likewise, I1 referred that the challenges are enormous. Accordingly, I1 reflected that if the privacy of the data is a concern, and it is, then one possible approach that could be put in place, would be the implementation of a tool or a set of tools within the operating system from the basis, the source of the operating system itself that would come in every mobile phone to guarantee the integrity and completeness of the information. Thus, I1 perceives that this is a possibility in the future for operators and operating system manufacturers to include a set of tools in the architecture of the operating systems.

According to I1, recently, it was implemented the digital wellbeing which caused a great impact to mobile phones users, as it performs and describes to the user some usage information, namely, what applications where used within a specific time frame, how many times were they open, how many clicks and unlocks were done, how much time was spent in each of the applications, as such the user can now have a accurate control over the time and usage of the mobile device. Besides this, I1 pointed out that the budget restrictions that a digital investigator may face, can also impact and influence the investigation process, as an investigator with a wealthy budget reflect can not only, pay for licences that are more expensive and contain more capabilities, as well as can pay for new developments and customization on that tool. Likewise, for I3, there is a challenge that this field is facing regarding the cost of obtaining the digital evidence versus the utility of that evidence, where in an investigation with budget constraints, this is even more relevant.

Moreover, for I2, one of the biggest challenges of any Digital Forensics science is the capability of a digital investigator to guarantee that the data that was captured within the examination was well captured and was not posteriorly manipulated and modified, as to ensure that the hash (encryption key) of the image of the mobile phone when it was received is the same from what was captured. In lines manner, I3 also referred that one of the pillars in any digital forensics' application is that the software that is being used has to have the capabilities to not manipulate and modify the evidence, and at the same time, be compliant with the judicial panorama. For I3, for the challenge of the ethical issues, there should be activities to raise and create awareness around the digital investigators that whenever they are executing and performing a digital investigation or a forensics task, the objective is a mechanical procedure, which implies that the digital investigator should work on resisting to the reading, and to the temptation of reading and sharing the information that is being analysed, as to keep the justice secret as an auditor.

Moreover, for I3 there is nowadays the difficulty binomial as the systems were designed and developed to protect the citizen, the user of the mobile phone, but the systems have to understand that they have to be compliant with the law and the legal requirements, as such, they have to possess mechanisms that should not impose difficulties for the auditor/digital investigator, as such, the systems cannot be designed in a way, that if there is a crime with that device, the authorities responsible cannot performed any capture and analysis of the information that resides on it.

Regarding the Topic 2, focused on the utility and contribution of the presented framework for the Mobile Devices Forensics field and its investigators, the main topics/ideas were the following: As presented in the initial debriefing and opinions regarding this master thesis, the interviewee 2, I2, demonstrated immediately that this toolbox is really useful for a digital investigator as it comes with a ready and handy box of applications and tools that a digital investigator can leverage, in order to solve any issue or to get answers and data. Likewise, this participant also demonstrated that it is relevant to build the parallelism between the Mobile Forensics science and any other that relates to any technology that allows user interactivity and storage, namely the computer.

Moreover, according to the I3, sometimes there is no distinction at all between a forensics analysis performed to a computer from one that was performed on a mobile device, as a mobile phone is a computer with a storage disk that represents a dataset of data. Furthermore, the interviewee I3 referred that the majority of the papers available at the moment in the literature are trying to analyse a given tool and/or application, while perceiving its capabilities and the manner that it can be used in order to reach a certain result. For instance, those papers are not interested in acknowledging what possible impact does the usage of that certain application/tool has or if the results reached or the tool/application employed have any credibility in retrieving the evidence while guarantee it was not modified.

Likewise, I3 points out that the majority of the literature focuses solely on capturing data from a memory of a mobile phone, and no one is seeking for quality/methodological review and criteria that should support and be the basis of a forensics investigation, which is the objective of this research. According to the I3, the work being performed here in this master thesis is more complex and a very difficult process than what is commonly performing in the state of art within this field, as the intent here is more complex and involves more criteria. Thus, I3 highlighted and pointed out that the literature available is not focusing what is being focus here on this thesis, namely, the methodology that is being emphasized here in this work. Besides, I3 also pointed out the fact that the work performed in this research focused also on both older and recent literature and on both free and paid applications/tools. According to I3, the free applications/tools are not used within a judicial investigation, but are usually used in the corporative context, emphasizing that in these field and in the judicial context, the paid applications are those that guarantee the credibility of the investigation as by paying to a company for its application, the investigator is transposing the onus of competence to that organisation.

Regarding the Topic 3, where the intent was to retrieve the reflections and insights on what were studied as well as the relevance and validity of what the toolbox proposed, the inputs were the following: As described in the initial debriefing and opinions regarding this master thesis, the feedback obtained from I1 and I2, was that by having a toolbox with a given set of tools and applications as well as with a methodology supporting these processes, it would be very important for a digital investigator as it come as handy for a digital investigator in what regards a forensics investigation. Also, important was the fact that with this research the author is raising awareness and conscious around the topics of the main challenges that the Mobile Device Forensics science is facing. Furthermore, according to the Interviewee I3, the matrix under analysis should seek to pursuit the process of identifying if the applications and tools that were included in the toolbox regarding the Mobile Forensics, are aligned and compliant with the legal and juridical requirements of a given country, e.g., Portugal and the European Union legal context.

As for I3, the tools and applications that are used in a juridical investigation, should be accepted regarding the point of view of the juridical context of e.g., Portugal and the European Union, in what regards the legal and law requirements. Accordingly, I3 points out that in these types of investigation, not every tool can be employed to extract the data, it has to be accepted in what regards the legal aspects, which I3 refers that the free applications do not usually comply with the legal aspects defined, where the paid applications some do others don't, which limits the options available for the digital investigator. Likewise, the Interviewee I3, also mentioned that there must be a concern for the digital investigator to whether the information that is being retrieved and the process to do so, is compliant with the legal context and requirements. As such, it was not possible to include this information regarding the legal compliance of each application and tool, due to the lack of knowledge and awareness on the legal and law fields from the researcher as well as due to the inexistent available documentation and papers on these matters. According to I3, there is also the need to mark out the ethical questions, which the interviewee referred as being in the Mobile Forensics evidence context or any other proof within a judicial task performed by an element of the authority or a non-element of the authority, is being able to acknowledge what and where the investigator cannot read and share publicly, as such, the investigator should ensure that the task is retrieve the evidence and deliver to the authorities responsible for the analysis procedures. According to I3, these matters are very extensive and thus, one (the author) must decide where to stop with the research on these matters.

Regarding the Topic 4, that involved the opinions and feedback containing any criticism and/or suggestions for improvements, as well as next steps for this field and for the research developed, the feedback was the following: According the I3, as the next steps, the researcher should seek to invest and consult more research and analysis on the legal aspects and the compliance to RGPD guidelines of each of the applications and tools that were included in the toolbox or any other that may be included in the future. For I3, it is highly relevant for this science and its forensics analysis to be aware and to acknowledge whether the application and tool that is being employed is compliant with the legal and law requirements. Likewise, I3 also suggests that it would be interesting to sort the applications from those that guarantee more integrity of the data that was captured (less likely to have been altered and/or erased), to those that guarantee a poor integrity of that data (more likely to have been modified and or deleted). As such, accordingly, the researcher should focus on performing this triage as to perceive which are the applications and tools that guarantee more or less modifications to the evidence, which according to I3, may not be available online and if it is there is little to no support documentation, papers, journals or any mean available to it.

Likewise, I3 also mentioned that it would be interesting for this area and field of research to explore the cost of obtaining the evidence versus the utility of that evidence. For instance, I3 points out that sometimes the cost of a Mobile Devices investigation is not solely the economical cost of investing money but is also the cost related to the investment of time and human resources, and thus, it leads to the comparison between the economical cost of an application vs the time costs. All the three participants I1, I2, I3, reflected in the possibility of the future being the possibility of the operating system itself of a mobile phone contains a tool or a set of tools within it, to allow for a simpler and more accurate and integrated process of retrieving and capturing the data that resides within a mobile phone. This possibility was emphasized specially because the need for a digital investigator to ensure the quality and integrity of the data that is available or that was captured, as well as because of the raising of technology related crimes. Moreover, according to the Interviewee 1, it may be important to consider and bring to the discussion around this field, the topic of the how much expensive can it be for a digital investigator to use a paid application and what level of prices are there in the market.

5.7. Discussion

Within this section one will perform an analysis where the inputs and feedback obtained during the previous stages will be incorporate to reach a conclusive discussion on several different aspects that were raised to the attention during both this research and within the Focus Group Meeting. In fact, aspects such as the relevance of the work and of the toolbox, followed by the validity and viability of the work performed as well as the enhancements that could be pursued in future work related to these matters.

Regarding the relevance and utility of this work, all the three participants agreed on the relevance and criticality of the work being performed within this field. In fact, one of the characteristics of the framework that was highlighted was the fact that it is a set of tools and applications that it is straightly available, up-to-date and convenient for any of the stages that a digital investigator may be in, not only raising knowledge and awareness around the literature available but also, bringing to the table a toolbox that contains the practicalities of the different forensics' tasks and stages.

Likewise, it was considered relevant for the fact that this work is striving to look for criteria of quality and to perform a methodological systematic review as the basis for any Mobile Forensics investigation but also it is looking forward to study the different options that are out there in the market and that may not be acknowledged by the digital investigators. Besides this, it was also highlighted the fact that the work possesses older and recent literature that cover both free and paid applications and tools which allow for the reader to have a very complete overview on these matters.

Regarding the topic of validity and viability, aspects like the different challenges on these field and on the framework were discussed, from the ethical issues that the Mobile Forensics field is facing, namely, the fact that it is very complex and difficult for a digital investigator to be able to separate what is personal from what is profession information within the mobile phone. Likewise, the architecture of a mobile phone was also discussed as these is currently imposing several challenges to the digital investigator as well as to the different applications and tools that are being utilized, as its architecture and operating systems brings complex and secure security and encryption settings.

Other aspects regarding these topics, was the requirements to guarantee the traceability of what is captured in the context of Mobile Forensics, as the digital investigator has to ensure that the different applications and tools that are used, do not alter and manipulate the information that is stored within the device or any of its peripheral components. Likewise, it was reflected the impact that the privacy of data can have within an investigation, where it was highlighted the possible lack of capability of a digital investigator to guarantee that the data that was captured within the examination was well captured and was not posteriorly manipulated and modified, as to ensure that the hash (encryption key) of the image of the mobile phone when it was received is the same from what was captured.

Besides this, the budget restrictions of the different digital investigators may impose limits to the investigation of a forensics examiner as it can limit the choice within the different applications and tools available, where a wealthier budget can reflect in not only, the purchase of more expensive licences and tools which may be more capable and have more features than the less expensive ones, but also, can pay for new developments and customization around those tools. Regarding the improvements that can be performed to the framework as well as the future work to this science, the participants highlighted the fact that one can look for the parallelism that may exist between the Mobile Device Forensics science and any other Digital Forensics Science, namely the Computer science, as it may be possible to leverage on the best practices and existing literature/tools to the Mobile Device Forensics field itself.

Moreover, it was highlighted the need to overview the possibility of the implementation of a given tools and applications at the basis of the operating system of a mobile phone, where the mobile phone would share the hash of its image within a certain time, to its operator which would potentially share this information with a digital investigator under legal requirements. Regarding the ethical awareness, all participants reflected on the need to have activities that would potentially increase the awareness and acknowledgement of all the intervenient within an investigation, as to raise awareness on the topics of resisting to read the information that is being captured and as well as on the temptation of sharing this information with public sources or any other source that is not under the legal flow of that given investigation. Lastly but not least, other feedback and criteria for improvement was the enclosure of more variables regarding the legal and juridical requirements, and thus, acknowledging if the given applications and tools are compliance with the legal requirements as well as with the RGPD Guidelines.

As such, the framework that is described above as well as its methodological standardized basis, was seen by all the participants as very useful and relevance for both the field and its investigators as it focuses on critical aspects. As such, it was understood and acknowledged by the participants that it is very relevant and valid and that it needs to be communicated as to raise awareness and knowledge on this area. Likewise, some adaptations and improvements for future work was suggested, which one considers relevant and was included in the section of next steps and future work, as well as some limitations to the study were denoted in the limitations section.

6. CONCLUSION

To conclude this research, it is important to acknowledge and mention that the objectives and sub-objectives defined were clearly achieved within this work. Based on all these information and deliverables, one expects that both the science of Mobile Device Forensics and any digital investigator will become more aware, concise and smarter on both the existing knowledge around this field but also on the different challenges, opportunities, applications and tools that can boost and aid the digital investigation process. As previously mentioned, before the deliver and defense of this master thesis, one had the opportunity to have its work published as a 33 pages chapter in the Handbook of Research on Cyber Crime and Information Privacy (2 Volumes) as a book chapter, namely, in the Chapter 14 – Mobile Device Forensics Investigation Process: A Systematic Review, written by the author of this thesis Bruno Bernardo, together with Professor Vitor Santos, who is the advisor for this thesis and work.

6.1. SYNTHESIS OF THE RESEARCH

As previously mentioned, the research begun with a systematic literature review over the different fields that were considered relevant for this thesis, namely the Forensics Science, the Digital Forensics Science, Mobile Devices Forensics Science and the Digital Archaeology that characterizes the Mobile Device environment. as performed, a toolbox with application and tools for the support and enhancement of the Mobile Device Forensics was build, and a standard methodology was derived from those existing in the architecture. This supported and helped with the created and derivation of the Framework that was purposed for the field of Mobile Device Forensics. Hence, the Framework had on its composition a set of applications and tools to support and enhance the Mobile Device Forensics as well as a support procedure and standard methodology which was derived from those existing in the literature analysis.

6.2. LIMITATIONS OF THE WORK

As to perceive the actual environment and context around the science of Mobile Forensics as well as around the framework and research performed, it is crucial for one to acknowledge what are the limitations of this research as well as those that this science is facing. As such, it is important to notice that despite the toolbox describing several characteristics and capacities of the applications and tools, tests over mobile phones were not performed of those set of applications due to the high variety of mobile phones, infinite specifications and settings, different operating systems, and components. As Jadhav & Joshi (2016), there are several different models of mobiles, each with infinite specifications and configurations, which result in the need for the field of Mobile Forensics to be a flexible and adapting environment as to be able to have numerous techniques that will be able to support different types of these devices. Likewise, the authors mentioned there are forensics tools limitations, that may imply that no tool is available that can fit the purpose of accessing and extracting data of a specific phone model.

Likewise, one limitation that this research faced was the fact that there is little documentation and research, including papers, journals, testing results around the mobile forensics field as well as the different applications available and testing procedures to it. In fact, according to Chernyshev et al. (2017), the principal challenge that characterizes the field of Mobile Forensics, is the lack of documentation and formalization of the techniques that are used and available while pursuing an investigation. Likewise, Omeleze & Venter (2013) highlighted that most of the frameworks and methods, lack the testing and procedure analysis.

Another limitation of this work was highlighted by the Interviewee I3 in the Focus group present in the Validation Phase of this research and represents the process of identifying if the applications and tools that were included in the toolbox regarding the Mobile Forensics, are aligned and compliant with the legal and juridical requirements of a given country, e.g., Portugal and the European Union legal context. Likewise, the Interviewee I3, also mentioned that there must be a concern for the digital investigator to whether the information that is being retrieved and the process to do so, is compliant with the legal context and requirements. As such, it was not possible to include this information regarding the legal compliance of each application and tool, due to the lack of knowledge and awareness on the legal and law fields from the researcher as well as due to the inexistent available documentation and papers on these matters. What's more, another limitation regards the inexistence of a specific training set and certifications that are needed for a digital investigator and/or a researcher in order to acknowledge what are the guidelines of standards and quality regarding the Mobile Forensics field, thus leading into a complex and difficult to surpass challenge for the digital investigator/researcher to acknowledge the guidelines, where and what to look on the mobile forensics existing applications (Chernyshev et al., 2017; Omeleze & Venter, 2013).

6.3. Next Steps and Future Work

Reflecting on what are the next steps and future work, while having in mind the limitations pointed above and in line on what was concluded and discussed in and after the Focus Group Meeting, it was considered very important to this research the investment in future steps of research on the legal and law aspects and requirements as well as on the compliance to RGPD guidelines of each of the applications and tools that in scope during this master thesis, as to conclude on those that meet the legal aspects and those that do not.

Likewise, one considered important and interesting for the next steps and further research to sort and choose the applications from those that guarantee more integrity and reliability of the data that was acquired, less prompted to manipulations and alterations, to those that jeopardize the integrity of the data as well as the proof. As such, it would be strongly recommended for this field and for the activity of a digital investigator to have access to research that would possibly focus on performing this triage as to acknowledge which are the applications that less jeopardize the integrity of the data. Likewise, it is considered also as relevant to this area, to acknowledge what are the law enforcement most used applications and tools, as to create awareness on the applications and tools that are most commonly used by the authorities.

Likewise, it is considered interesting for this area and field to explore the relationship between the cost of obtaining the evidence and capturing the data versus the utility of that within an investigation within the usage of different application, as to possibly build relationships with certain levels of causality.

In the same manner, the focus group yielded the need for this area and its researchers, should seek to reflect on the possibility of the operating system of a mobile phone itself contain a tool or a set of tools within it, to permit and guarantee the full integrity of the data captured. This is even more important due to the more advanced and recent security settings and the antiforensics, which is described by the fact that mobile phones manufacturers have the capacity to difficult the analysis and the acquisition techniques of a digital investigator.

Furthermore, and lastly but not least, in the future there should be more research within this field as to be able keep up and constantly adjust to this fast-paced environment that characterizes the Mobile industry and the field of Mobile Forensics, as the applications and tools that are available may be more and perform more analysis within the future and must be able to adapt to this ever-changing industry and updates.

BIBLIOGRAPHY

Sathe, S. C., & Dongre, N. M. (2018). Data acquisition techniques in mobile forensics. *Proceedings of the 2nd International Conference on Inventive Systems and Control, ICISC 2018*, 280–286

Chernyshev, M., Zeadally, S., Baig, Z. & Woodward, A. (2017). Mobile Forensics: Advances, Challenges, and Research Opportunities. *IEEE Security & Privacy, Security & Privacy, IEEE, IEEE Secur. Privacy*, (6), 42.

Graves, M.W. (2013). *Digital Archaeology: The Art and Science of Digital Forensics.* Upper Saddle River, NJ: Addison-Wesley, 2013, 600p

Omeleze, S & Venter, H. S. (2013). Testing the harmonised digital forensic investigation process model-using an Android mobile phone. *2013 Information Security for South Africa, Information Security for South Africa,* 1.

Zhang, W., Ma, C., Yu, M., Liu, C. & Wang, Y (2017). N-SVDD: A sensitive message analysis model for mobile forensics. *2017 IEEE Conference on Application, Information and Network Security (AINS), Application, Information and Network Security (AINS), 2017 IEEE Conference On*, 48.

Jadhav, M. & Joshi, K.K. (2016). Forensic investigation procedure for data acquisition and analysis of Firefox OS based mobile devices. *2016 International Conference on Computing, Analytics and Security Trends (CAST), Computing, Analytics and Security Trends (CAST), International Conference On*, 456.

Ostrowski, L., Helfert, M. & Xie, S. (2012). A Conceptual Framework to Construct an Artefact for Meta-Abstract Design Knowledge in Design Science Research. *2012 45th Hawaii International Conference on System Sciences, System Science (HICSS), 2012 45th Hawaii International Conference On*, 4074.

Schorr, F. & Hvam, L. (2018). The Use of Design-science to Define Information Content Requirements for IT Service Catalogs. *2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Industrial Engineering and Engineering Management (IEEM), 2018 IEEE International Conference On*, 497.

Baskerville, R. L., Kaul, M., & Storey, V. C. (2018). Aesthetics in design science research. *EUROPEAN JOURNAL OF INFORMATION SYSTEMS*, *27*(2), 140–153.

Dresch, A., Lacerda, D. P., & Miguel, P. A. C. (2015). A Distinctive Analysis of Case Study, Action Research and Design Science Research. *Revista Brasileira de Gestão De Negócios*, (56), 1116.

Weber, S., Beck, R. & Gregory, R. W. (2012). Combining Design Science and Design Research Perspectives-Findings of Three Prototyping Projects. *2012 45th Hawaii International Conference on System Sciences, System Science (HICSS), 2012 45th Hawaii International Conference On*, 4092.

Storey, M., Engstrom, E., Host, M. Runeson, P. & Bjarnason, E. (2017). Using a Visual Abstract as a Lens for Communicating and Promoting Design Science Research in Software Engineering. *2017 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement*

(ESEM), Empirical Software Engineering and Measurement (ESEM), 2017 ACM/IEEE International Symposium on, ESEM, 181.

Cronholm, S., & Göbel, H. (2016). Evaluation of the Information Systems Research Framework: Empirical Evidence from a Design Science Research Project. *Electronic Journal of Information Systems Evaluation*, *19*(3), 158–168.

Snyder H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research,* 104:333-339.

Palmatier, R. W., Houston, M. B., & Hulland, J. (2018). Review articles: purpose, process, and structure. *JOURNAL OF THE ACADEMY OF MARKETING SCIENCE*, 46(1), 1–5

Bannister, F., & Janssen, M. (2019). The art of scholarly reviewing: Principles and practices. *Government Information Quarterly*, 1–4.

Smallbone, T., & Quinton, S. (2011). A three-stage framework for teaching literature reviews: A new approach. International Journal of Management Education (Oxford Brookes University), 9(4), 1–11.

Bell, S., Sah, S., Albright, T. D., Gates, S. J., Jr., Denton, M. B., & Casadevall, A. (2018). A call for more science in forensic science. *PROCEEDINGS OF THE NATIONAL ACADEMY OF SCIENCES OF THE UNITED STATES OF AMERICA*, 115(18), 4541–4544.

Valdez, B. (2018). Spotlight on a Discipline: Forensics. *International Social Science Review*, Vol. 94 Núm. 2.

House of Lords (2017). Forensic science and the criminal justice system: a blueprint for change. *Science and Technology Select Committee,* 3rd Report of Session 2017–19.

Houck, M. M. (2019). How forensic science works: an architecture for the forensic enterprise. *Australian Journal of Forensic Sciences*, 51(3), 359–368.

Roux, C., Ribaux, O., & CRISPINO, F. (2018). Forensic science 2020 - the end of the crossroads? *Australian Journal of Forensic Sciences*, 50(6), 607–618.

Roux, Claude & Ribaux, Olivier & Crispino, Frank. (2012). From Forensics to Forensic Science. *Current Issues in Criminal Justice*. 24. 7-24.

Maras, Marie-Helen & Miranda, Michelle. (2014). Forensic Science. *Encyclopedia of Law and Economics*, pp.1-6.

Katz, E. and Halámek, J. (2016). Forensic Science – Chemistry, Physics, Biology, and Engineering – Introduction. *In Forensic Science* (eds E. Katz and J. Halámek)

American Chemical Society (2017). Forensic Science: The Promise and Perils of Using Science in the Courtroom

Houck, M. M. (2019). How forensic science works: an architecture for the forensic enterprise. Australian Journal of Forensic Sciences, 51(3), 359–368.

Årnes, A. (2018). Digital Forensics, First Edition. *John Wiley & Sons Ltd*.

House of Lords Science and Technology Select Committee (2019). Forensic Science and the Criminal Justice System: a Blueprint for Change. *3rd Report of session 2017-2019 HL Paper 333.*

Morgan, R. M., Nakhaeizadeh, S., Earwaker, H., Rando, C., Harris, A. F. L., & Dror, I., E. (2018). Interpretation of forensic science evidence at every step of the forensic science process: decision-making under uncertainty*. In R. Wortley, A. Sidebottom, N. T., & G. Laycock (Eds.), Routledge Handbook of Crime Science* (pp. 408-420)

Strengthening Forensic Science in the United States: A Path Forward (2009). *Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council. The National Academies Press*, 352 pages.

Edmond, G, Towler, A, Growns, B, Ribeiro, G, Found, B, White, D, Ballantyne, K, Searston, RA, Thompson, MB, Tangen, JM, Kemp, RI & Martire, K (2017). Thinking forensics: Cognitive science for forensic practitioners. *Science & Justice,* 57(2), 144–154.

Lefevre, T. (2018). Big data in forensic science and medicine. *JOURNAL OF FORENSIC AND LEGAL MEDICINE*, 57, 1–6.

Margagliotti, G., & Bollé, T. (2019). Machine learning & forensic science. *Forensic Science International*, 298, 138–139.

Varol, A., & Sönmez, Y. Ü. (2017). Review of Evidence Collection and Protection Phases in Digital Forensics Process. *International Journal of Information Security Science*, 6(4), 39–46.

Ayers, R., Brothers, S. & Jansen, W. (2014). Guidelines on Mobile Device Forensics. *National Institute of Standards and Technology Special Publication***.** 800-101 Rev. 1**.**

Carrier, B. (2003). "Open Source Digital Forensics Tools - The Legal Argument". *@stake Research Report.* 1-11.

Du, X., Le-Khac, N.-A., & Scanlon, M. (2017). Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service*.*

Bjornson, J., & Hunter, A. (2016). Mobile forensics for cloud data: Practical and legal considerations. *2016 14th Annual Conference on Privacy, Security and Trust (PST), Privacy, Security and Trust (PST), 2016 14th Annual Conference On*, 203–206.

Klomklin, S., & Lekcharoen, S. (2016). A development of mobile phone forensics procedures for law enforcement agencies in Thailand. *ICCSE 2016 - 11th International Conference on Computer Science and Education*, 473–478.

Faheem, M., Le-Khac, N.-A., & Kechadi, T. (2016). Toward a new mobile cloud forensic framework. *2016 Sixth International Conference on Innovative Computing Technology (INTECH), Innovative Computing Technology (INTECH), 2016 Sixth International Conference On*, 736–742.

Rao, V. V., & Chakravarthy, A. S. (2016). Forensic analysis of android mobile devices. *2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE), Recent Advances and Innovations in Engineering (ICRAIE), 2016 International Conference On*, 1–6.

Shortall, A., & Azhar, M. A. H. B. (2015). Forensic Acquisitions of WhatsApp Data on Popular Mobile Platforms. 2015 Sixth International Conference on Emerging Security Technologies (EST), 13.

Kim, D., Lee, Y., & Lee, S. (2018). Mobile forensic reference set (MFReS) and mobile forensic investigation for android devices. Journal of Supercomputing, 74(12), 6618–6632.

Bjornson, J., & Hunter, A. (2016). Mobile forensics for cloud data: Practical and legal considerations. *2016 14th Annual Conference on Privacy, Security and Trust (PST), Privacy, Security and Trust (PST)*, 2016 14th Annual Conference On, 203–206.

Barmpatsalou, K., Cruz, T., Monteiro, E., & Simoes, P. (2018). Current and Future Trends in Mobile Device Forensics: A Survey. *ACM Computing Surveys*, 51(3), 1–31.

S. Li, Q. Sun and X. Xu (2018). Forensic Analysis of Digital Images over Smart Devices and Online Social Networks, *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems*, pp. 1015-1021.

Aziz, N. A., Mokhti, F., & Nozri, M. N. M. (2015). Mobile Device Forensics: Extracting and Analysing Data from an Android-Based Smartphone. *2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec), Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec), 2015 Fourth International Conference on, Cybersec*, 123–128.

Mumba, E. R., & Venter, H. S. (2014). Mobile forensics using the harmonised digital forensic investigation process. 2014 Information Security for South Africa, Information Security for South Africa (ISSA), 2014, 1–10.

Hayes, D. (2014). A Practical Guide to Computer Forensics Investigations. *Pearson Education: London, UK*, 2014.

Mullen, G. (2006). Project-a-Phone Revolutionizes the Art of Presentation. *Telecommunications - Americas Edition*, 40(5), 8.

Netherlands Forensic Institute (2011). The NFI Memory Toolkit II – A universal forensic solution to read memory chips developed by *the Netherlands Forensic Institute*.

Bachler, M. (n.d.). An Analysis of Smartphones Using Open Source Tools versus the Proprietary Tool Cellebrite UFED Touch®, *Marshall University Forensic Science Center.*

Ayers, R., Jansen, W., Cilleros, N., & Daniellou, R. (2005). Cell Phone Forensic Tools: An Overview and Analysis*. National Institute of Standards and Technology (U.S.).*

Heriyanto, A., Valli, C., & Hannay, P. (2015). Comparison of Live Response, Linux Memory Extractor (LiME) and Mem tool for acquiring android’s volatile memory in the malware incident.

Bommisetty, S., Tamma, R. & Mahalik, H. (2014). Practical Mobile Forensics – Community Experience distilled. *Packt Publishing 2014*.

Lessard, J., & Kessler, G. (2010). Android forensics: Simplifying cell phone examinations. *Small Scale Digital Device Forensics Journal 2010,* NO. 1, 1941-6164.

Hoog, A. (2011). Android Forensics - Investigation, Analysis, and Mobile Security for Google Android. *Elsevier*, 2011.

Al-Sabaawi, A. & Foo, E. (2019). A Comparison Study of Android Mobile Forensics for Retrieving Files System. *International Journal of Computer Science and Security (IJCSS)*, 13. 148-166.

Alhassan, J., Oguntoye, R., Misra, S., Adewumi, A., Maskeliunas, R., Damasevicius, R. (2018). Comparative Evaluation of Mobile Forensic Tools. *Advances in Intelligent Systems and Computing.*

Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation, 9(Supplement)*, S90–S98.

Byers, D., & Shahmehri, N. (2009). A systematic evaluation of disk imaging in EnCase ® 6.8 and LinEn 6.1. *Digital Investigation, 6(1)*, 61–70.

Homeland Security – Science and Technology (2016). Test Results for Mobile Device Acquisition Tool – BlackLight v2016.1.

Gajjar, K. & Sharma, P. (2020). Android based Mobile Forensic and Comparison using various Tools. International Research Journal of Engineering and Technology (IRJET). Vol 07.

Cappa, F., Sette, F., Hayes, D., Rosso, F. (2016). How to Deliver Open Sustainable Innovation: An Integrated Approach for a Sustainable Marketable Product. *Sustainability 2016*, 8, 1341

M. Asim, M. Faisal Amjad, W. Iqbal, H. Afzal, H. Abbas and Y. Zhang (2019). AndroKit: A toolkit for forensics analysis of web browsers on android platform, *Future Generation Computer Systems*, vol. 94, pp. 781-794.

Abdulla, K., Jones, A. & Martin, T. (2012). Forensics data acquisition methods for mobile phones. 2012 *International Conference for Internet Technology and Secured Transactions*, ICITST, 265-269.

Kim, A. D., "Digital Forensics Tools Integration" (2020). *Theses and Dissertations*. 3162.

Attar I. & Kapale M. (2019). Conceptual Study of Mobile Forensics. International Journal of Trend in Scientific Research and Development (ijtsrd), 2456-6470, Vol 4, Issue 1, 2019.

Homeland Security – Science and Technology (2020). Final Mobile Forensics Version 2019.07.05 Test Results for Binary Image (JTAG, Chip-Off) Decoding and Analysis Tool: Final Mobile Forensics v2019.07.05.

Silveira, C., Junior, R., Albuquerque, R., Nze, G. Júnior, Orozco, A., Villalba, L. (2020). Methodology for Forensics Data Reconstruction on Mobile Devices with Android Operating System Applying In-System Programming and Combination Firmware. *Applied Sciences*. 10. 4231.

Homeland Security – Science and Technology (2016). Test Results for Mobile Device Acquisition Tool - Secure View v4.1.9.

Wilson, V. (2016). Research Methods: Focus Groups. Evidence Based Library and Information Practice, 11(1 (S)), 44–46.

Al Qudah, D. A., Cristea, A. I., Shi, L., & Alqatawna, J. (2015). Designing an adaptive online advertisement system: A focus group methodology. 2015 10th International Conference on Computer Science & Education (ICCSE), Computer Science & Education (ICCSE), 2015 10th International Conference On, 163–168.

Guest, G., Namey, E., Taylor, J., Eley, N., & McKenna, K. (2017). Comparing focus groups and individual interviews: findings from a randomized study. International Journal of Social Research Methodology, 20(6), 693–708.

Hartman, J. (2004). Using Focus Groups to Conduct Business Communication Research. Journal of Business Communication, 41(4), 402–410.

Eaton, S. E. (2017). Research Assistant Training Manual: Focus Groups. Online Submission.

Djohari, N., & Higham, R. (2020). Peer-led focus groups as "dialogic spaces" for exploring young people's evolving values. Cambridge Journal of Education, 50(5), 657–672.

Brandl, K., Rabadia, S. V., Chang, A., & Mandel, J. (2018). Benefit of focus group discussion beyond online survey in course evaluations by medical students in the United States: A qualitative study. Journal of Educational Evaluation for Health Professions, 15, 25.

Kruger, L. J., Rodgers, R. F., Long, S. J., & Lowy, A. S. (2019). Individual interviews or focus groups? Interview format and women's self-disclosure. International Journal of Social Research Methodology, 22(3), 245–255.

Winlow, H., Simm, D., Marvell, A., & Schaaf, R. (2013). Using Focus Group Research to Support Teaching and Learning. Journal of Geography in Higher Education, 37(2), 292–303.

Sumuri LLC (2016). Quick Start Guide - Paladin Forensic Mode Version 7.00

Passware Inc. (2017). Passware Kit Forensic - The complete encrypted electronic evidence discovery solution.

Sim card sizes standard micro and nano explained Article (2020). Accessed on the 27th Dec 2020. Retrieved from the website: 4g.co.uk/news/sim-card-sizes-standard-micro-and-nano-explained/.

Building a hardware store faraday cage (2018) Article. Accessed on the 27th Dec 2020. Retrieved from the webside: hackaday.com/2018/09/26/building-a-hardware-store-faraday-cage/.

Why a faraday cage? Article. Accessed on the 27th Dec 2020. Retrieved from the website: mysmartsurvival.com/why-a-faraday-cage/.

What is a faraday bag? Article (2018). Accessed on the 27th Dec 2020. Retrieved from the website: faradaybag.com/what-is-a-faraday-bag/.

Technical look phone extraction Article (2019). Accessed on the 27th Dec 2020. Retrieved from the website: privacyinternational.org/long-read/3256/technical-look-phone-extraction

ANNEXES

Annex I – Focus Group meeting transcription (PT) of key/main topics and ideas discussed:

Focus Group Meeting – Topics of the Questions to the Stakeholders	
Topic 1	Mobile Forensics challenges and the eventual ethical questions and issues that may urge and appear from a person's/digital investigator usage of Mobile Forensics' Tools.
Topic 2	The Utility and contribution of the presented framework for the Mobile Devices Forensics science and for the investigators.
Topic 3	Reflections and insights on what were studied, as well as the relevance, validity, and viability of what was proposed as a framework.
Topic 4	Opinions and feedback containing criticism and suggestions for improvements as well as what in the views of the participants are the future and next steps for this field and research developed on it.

In similar manner to what is described in the Validation section of this master thesis, and as requested by all the three participants, the names of the participants are not disclosed, and the Focus Group meeting flow and transcription was anonymized. As such, each participant was attributed with the nomenclature of "I" (Interviewee) plus a given random number from 1 to 3 as to anonymize the insights and contributions given by the stakeholders.

Focus Group meeting synthesis of the transcription (PT) regarding the key/main topics discussed:

I1: Claramente que uma caixa de ferramentas forense dá bastante jeito… em termos de auditoria de redes, segurança de rede, existem pacotes como o backtrack e outros pacotes desses prontinhos exatamente para fazer auditoria.

Moderador: Certo. Aí estamos a falar numa ótica de auditoria de vulnerabilidades.

I1: de redes sim, mas existe esse paralelo, por isso o que tu queres basicamente é uma coisa desse género, mas agora focado nos dispositivos moveis.

Moderador: Exatamente.

I1: A abordagem é a mesma, uma toolbox prontinha a utilizar em que tens os softwares que te resolvem e dão respostas.

Moderador: Exatamente… e dar ao próprio investigador mais do que uma hipótese, ou seja, imaginemos que temos uma equipa de investigadores que não tem um grande orçamento, portanto, temos rúbricas que nos dizem se aquela aplicação é paga ou é grátis, se for por exemplo grátis, mas depois, a versão lite por exemplo é grátis, mas depois tem uma versão paga que contém mais funcionalidades. Portanto, fomos aqui explorar mais opções mais instâncias da própria caixa de ferramentas e eu acho que é essa é uma das grandes mais valias. A metodologia desta nossa análise consiste no modelo PRISMA, fizemos uma revisão sistemática de literatura, onde nos propusemos a analisar toda a literatura existente relevante para o nosso processo… Uma das limitações do estudo claramente que vários autores referem é a questão, de termos muito pouca pesquisa sobre estas áreas, e eu quando falo desta área mais aplicada aos telemóveis, poderia estar a falar noutra qualquer ciência forense digital… O objetivo é olharmos para o produto final, aquilo que temos, que é a caixa de ferramentas…Aquilo que eu me propus com este trabalho, numa vertente foi preparar e contruir esta caixa de ferramentas e para isso estudei… as ciências forenses e as ciências digitais forenses e também a arqueologia dos telemóveis mais especificamente, perceber aqui que componentes fazem parte de um telemóvel, como é que eles funcionam, entrar um bocadinho nas foundations destes tópicos. Por outro lado, outro objetivo foi aumentar aqui o conhecimento nesta área, trazer aqui muito conhecimento, muitos estudos, recolher muita informação para também quem esteja a dar os primeiros passos, independente do nível de maturidade do investigador consegue ter aqui overview bem construído sobre todos estes tópicos. A revisão de literatura… partimos da ciência forense, a mais conhecida, a mais também utilizada e a mais antiga e passamos aqui para a ciência digital e depois para a parte aplicada aos telemóveis, depois fomos aqui para a parte da arqueologia dos telemóveis e fomos aqui estudar também quais é que são não só os grandes desafios desta área, mas também as oportunidades.

I1: Existe um modo de funcionamento dos telemóveis que é o root. Tens tudo, o que tu não conseguires aceder é porque não existe.

Moderador: Uma das grandes limitações… é o facto da capacidade de se conseguir fazer esse root. Para fazer o root é preciso aqui um conjunto de dados, que nem sempre é tão fácil…Alguma quantidade de aplicações requerem que o root esteja feito para conseguirem fazer algum tipo de análise… Apesar de ser um mundo pouco estudado, há muitas aplicações e também há muitas aplicações...que vêm de fornecedores mais conhecidos, mas também… há muitas que são completamente open-source… As propriedades da própria aplicação podem ser por exemplo, uma coisa muito mais limitada…temos aplicações em que o objetivo é simplesmente tirar fotos ao ecrã para efeito de registos e de documentação da auditoria em si aos telemóveis ou numa investigação. Neste caso o objetivo não é de todo retirar dados, mas sim garantir que todos os passos que são dados naquele telemóvel são capturados. Portanto, nós chegamos aqui à nossa metodologia onde estamos a utilizar o Design Science Research… Numa primeira fase identificamos aqui uma série de problemas e motivações, não só da área…de forense aplicada aos telemóveis, mas também de outras áreas forenses. Depois definimos claramente o objetivo…por um lado aumentar o conhecimento nesta área e explorar…o conhecimento que existe nesta área…Por outro lado propor uma caixa de ferramentas que ajude e que melhore este processo de investigação.

I1: Qual é a ordem de grandeza de preços?

Moderador: Do mercado…estas aplicações são todas elas quando pagas, são todas elas muito caras por licença… dependendo muito das capacidades. Para muitos casos onde havia literatura de testes, fomos analisar o que tinha sido feito nesses testes…diante alguns telemóveis, sejam eles androids ou iphones… algumas não há literatura de todo, mesmo com muito pesquisa não conseguimos encontrar. Como estão aqui a ver, esta caixa de ferramentas…tem aqui há volta de 30 e qualquer coisa aplicações…Para cada uma delas foi feito este estudo e foi enquadrado no processo em si, aqui da metodologia… Não sei se têm alguma dúvida…

I2: O que é que tu viste de diferença, digamos desta temática particular com uma temática mais genérica, não aplicável ao mundo dos dispositivos móveis, mas ao mundo do computador pessoal, que é algo que também é muito usado neste tipo de investigações. Que diferenças é que há em termos técnicos, qual é a razão para teres que ter uma especificidade concreta para os dispositivos móveis. Obviamente que há diferenças.

Moderador: é muito comparado esta ciência, com a ciência aplicada aos computadores e à análise de documentos, desde logo é a própria infraestrutura, a própria maneira como o sistema operativo está embutido, como as próprias memorias também estão…organizadas… por exemplo não é possível replicar de todo muitas aplicações que são utilizadas para computadores para telemóveis. Por outro lado…é muito utilizado sinergias, ou seja, aplicações que conseguem analisar a informação de computadores e que depois também conseguem através da conexão do telemóvel via usb com o computador, retirar a informação sobre os telemóveis.

…Há uma componente muito importante…as questões éticas, ou seja, hoje em dia nós temos, eu vi isso muito nos telemóveis, e acho que nos computadores também é muito semelhante, temos telemóveis em que é dado o uso profissional mas também o uso pessoal e portanto fica muito difícil para o investigador conseguir distinguir o que é informação que é… pessoal e que à partida será intransmissível da informação que é corporativa e que pode causar aqui uma série de questões…éticas em termos de concordância, regras.

I2: Corporativa, e tiveres potencialmente a ver informação do tipo pessoal.

Moderador: …Para distinguir o que é que é pessoal e o que é corporativo…é um mundo muito cinzento.

I2: Numa investigação corporativa…o que acontece é…investigar algo no mundo corporativo e não devemos aceder à informação pessoal e por isso temos ali um bloqueio.

Moderador: …vimos na literatura…pesquisas ou investigações feitas no mundo corporativo, em que estão a aceder a um computador ou telemóvel e que tem muita informação pessoal…é um mundo muito difícil e por isso é que eu também trouxe estes tópicos das questões éticos…Aqui… começávamos por abordar as questões éticas…quais é que…são as eventuais questões éticas que podem ocorrer não só da própria ciência forense digital aplicada aos telemóveis mas também desta framework que estamos a apresentar e desta metodologia.

I1: Desafios da ciência forense digital para os telemóveis. A primeira coisa que me ocorre é os telemóveis com arquiteturas novas foram feitas de raiz num ambiente de segurança e por isso, eles vêm a privacidade como um tema forte…dentro da arquitetura… arquitetura android…toda ela foi desenhada na questão dos privilégios, por isso a questão do root…e dos privilégios serem dados um a um em cada uma das atividades… Os computadores tradicionais evoluíram…e por isso houve sempre a preocupação de serem compatíveis. As arquiteturas dos computadores são arquiteturas universais abertas…No caso dos telemóveis foram especificamente, são objetos pessoais…foram desenhados com o intuito de serem pessoais e por isso têm um âmbito diferente… a forma como funcionam como acede…há dois anos a existência dos telefones mais caros de uma perspetiva que separava o pessoal do profissional…as outras referências sobre isso era do género atribuir um telefone da empresa…não ter nada pessoal, por causa da segurança exatamente.

Resumindo… os desafios são enormes. Se pensar que vamos ter uma ferramenta que vem de base, ou um set de ferramentas que vai ter acesso a todo o sistema operativo, eu acho que…devia de fazer parte do sistema operativo provavelmente, para ser tão abrangente…Um investigador com muito dinheiro não só pode pagar as licenças como pode pagar desenvolvimento de ferramenta para o seu fim…Se for a questão da privacidade dos dados, provavelmente eles deveriam de integrar a ferramenta no sistema operativo…Agora apareceu…o bem-estar digital…apareceu agora nos telemóveis com um impacto muito grande…há tanta coisa…quantas vezes esteve em cada aplicação, a olhar, quantas vezes desbloqueou o telefone…informação que antes só estaria…disponível para os operadores, mas agora podemos ter algum controlo sobre isso.

Moderador: …Da experiência mais ao nível corporativo das investigações que são feitas, quer a telemóveis, mas a qualquer tecnologia…quais…são os desafios que são mais frequentes de aparecer e também os mais difíceis de ultrapassar…os próprios desafios são…extrapoláveis para quase todas as áreas de forense digital.

I2: …A separação entre o que é dispositivo movel entre o que é um dispositivo mais tradicional, há diversas diferenças, na perspetiva mais técnica não deixa de ser… tens dados em disco, se tiveres capacidade de aceder a esses dados em disco…o que fazes dai em diante é semelhante. As diferenças são as formas de os capturar, no caso de um dispositivo movel tem características distintas, tens mais contaminação do que é o mundo pessoal e o mundo empresarial nos telemóveis, até porque a tendência cada vez mais as pessoas terem…a empresa tem um bring your own device… aquela comodidade que muita gente utiliza e que depois traz esse desafio de não separação entre o que é o mundo pessoal e o mundo profissional… Depois de capturares os dados, o que tens de aí em diante é exatamente igual ao caso se trate de um pc…um telemóvel são bites e bytes num disco…tens aplicações de natureza distinta…que têm conteúdo encriptado, que não têm encriptado, mas isso também tens…num dispositivo não móvel…Apesar de ter um dispositivo de utilização pessoal e profissional, há uma separação entre o é o contexto profissional e o contexto pessoal. Se de facto isto fosse relevante, separar estes dois mundos e se fosse relevante garantir a rastreabilidade do que é capturado no contexto de ciência forense, o próprio dispositivo deveria dizer, hoje no dia…o hash dos teus dados é este, e isto estava disponível ao operador por exemplo em que num contexto de investigação poderia ser disponibilizado… a ciência subsequente é semelhante…extrair informação dos dados…alguns encriptados e posso ter dificuldades outros não…quero garantir que os dados que foram capturados foram bem capturados e não foram posteriormente manipulados…é um dos desafios… Se isto fosse de facto um valor fundamental, teríamos que embutir mais a montante…o sistema operativo devia permitir dizer…a minha fotografia é esta hash.

I1: …Pensando na perspetiva daquela identidade digital…era mesmo o sistema operativo… que teria e passar para os computadores também para haver a tal identidade…

I3: …Na matriz…incluir uma coluna meet legal aspects…legal proceedings é porque as ferramentas…tem que ser ferramentas que possam ser aceites do ponto de vista do panorama jurídico português/europeu. Não é qualquer ferramenta que pode ser utilizada para extrair os dados, porque se houver um perito da contraparte que vem dizer que aquela ferramenta na extração pode alterar minimamente os dados…seja qualquer coisa…havendo a possibilidade de manipular a prova, aquela ferramenta não pode ser usada, isso limita muito o leque de ferramentas que existem. Nas gratuitas não há, nas que são a pagar… não são ferramentas acessíveis…O aspeto ético…criar a consciência…quando estamos numa tarefa forense…objetivo é um procedimento mecânico… portanto trabalhar na ética é trabalhar na resistência à leitura…não deixar entrar na tentação de partilhar a informação… Manter o segredo de justiça enquanto…auditor...

O Binómio da dificuldade…porque…os sistemas foram desenvolvidos para proteger o cidadão, mas os sistemas também tem que perceber que têm que ser compliance com a lei, tem que possuir mecanismos que não possam dificultar a vida ao auditor, eu não posso usar um determinado nível de encriptação ali porque…a montante…aquele sistema operativo deixa de ser uma arma de defesa…Não pode ser criado de uma forma, a que se cometerem um crime com aquela ferramenta, a autoridade não possa tirar a informação…

O custo de obter a prova versus a utilidade... Três grandes pilares: o software que vou usar tem que ser muito cuidadoso para não alterar a prova, e para isso as autoridades delegam nas forças policiais e delegam nos peritos… Desta metodologia qual dela é que não fere o panorama jurídico.

Moderador: Esse ponto…como uma limitação à própria pesquisa…

I3: Temos que nos enquadrar onde está o aluno…deverá procurar das ferramentas open-source e daquelas que são pagas, mas que tem informação de serem legal compliance…ou por estudos que existam no estado da arte…para perceber que ferramenta é que garante maior integridade dos dados que vai buscar. Deve ordenar por aí, aquelas que garantem à partida maior integridade de dados… Há aplicações que trazem mesmo realmente, já têm inteligência artificial, algumas estão no mercado… Deve – se focar…para fazer uma triagem, quais são as tecnologias de análise forense que garantem menos alteração à prova e aquelas que garantem menos integridade na prova …informação não está simplesmente online e se estiver não vamos encontrar muitos papers a falar sobre ela...Distinguir quais são as mais influenciáveis à prova e menos influenciáveis à prova…

…O inspetor coleta a prova toda. O inspetor de facto faz aqui uma tarefa, monta a história do crime… Ou seja, o perito coleta a prova toda e dá ao inspetor, ou o inspetor com capacidade tecnológica recolhe a prova toda e pega nesta matéria e vai montar uma história…Existe é alguns serviços que empresas providenciam ao mercado de recuperação de informação. E aqui sim é que entram empresas com mais recursos ou com menos recursos… podem capturar mais prova ou menos prova… Não é uma coisa linear… A questão da comparação dos preços é para outro tipo de mercado, por exemplo quando uma empresa por exemplo sofreu de hacking…e tem que olhar para os telefones que estão dentro da empresa…e tem que aferir se alguns daqueles equipamentos esteve envolvido no ataque…e aqui…há formas mais económicas e menos económica de perceber o que é que aconteceu.

Moderador: Para um qualquer investigador, seja ele uma entidade…de autoridade, ou seja, ela por exemplo uma empresa…ter essa visão de…esta aplicação vai – me custar dinheiro ou é gratuita.

I3: …As vezes o custo não é o custo económico é o custo do tempo…essa questão de ter custo por tempo e custo…económico… é matéria para doutoramento também…

…A componente legal…se estamos a fazer auditoria de qualquer coisa temos que cumprir com algum compliance, quanto mais não seja se estamos a falar ao nível civil…Vou analisar o computador…a um determinado nível que não comece a colidir com os direitos que consagram o RGPD…consultar o RGPD, nas questões que, e há guidelines…são os considerando de…que especificam claramente o que é que é dentro do computador de trabalho, a parte pessoal do uso daquele computador e a parte profissional do uso daquele computador…Foca-se na questão da proteção de dados e a questão dos dados do equipamento, do programa que adquire a informação poder ser adequado ao panorama jurídico. E a adequação ao panorama…é o que interfere mais com a prova versus o que interfere menos com a prova, é a utilidade de gastar mais dinheiro para a aquisição de prova e gastar menos dinheiro para a aquisição de prova…binómio de tempo associado a custo.

Moderador: …Juntarmos…várias aplicações que fazem a segunda parte, outras a terceira…temos aqui…um conjunto de…soluções que também fomos identificando…

I3: Obriga a várias questões, obriga ao custo, pouco tempo para ir buscar a matéria porque os casos expiram, há um tempo muito limitado para mover para a fase de instrução…trinómio… preço, menos mexe na prova e que mais ou menos prova consegue coletar…Destas aplicações…procurar informação…que tenha conteúdo em sede de tribunal, ou seja procurar quais são estas aplicações que foram usadas para provar provas em sede jurídica.

Moderador: A última questão…perceber…as vossas reflexões e os próximos passos da pesquisa…

I3: …Balizar aqui a ética…A ética…é aqui em qualquer prova…tarefa jurídica, por um não - elemento da autoridade e por um elemento da autoridade, é saber…aonde é que não pode ler e o que é que não pode estar a ler…como não sabe não se lê, tentasse coletar a prova e entregar… É tão extensa que vai ter que ser o Bruno (autor desta tese) a decidir onde parar, porque se não decidir onde parar, é mais e mais…

I3: …Ás vezes não há uma distinção de como é que faz uma análise forense a um computador e a um telemóvel, porque um telefone é um computador…um disco rígido…um dataset de dados…Muito do que é análise de papers que estão neste momento no estado da arte, temos que perceber que, eles não estão a focar isto que o Bruno (autor desta tese) está a focar, não estão a tentar fazer nenhuma metodologia. Muitos dos papers estão a analisar o que é que são ferramentas que podem fazer com que se consiga chegar a x resultados. Agora, ninguém está preocupado é que impacto é que tem o resultado de determinada ferramenta, ou qual é a credibilidade da ferramenta para não manipular o resultado. E grande parte dos trabalhos, infelizmente, só se focam nisto, eu preciso de tirar coisas da memória de um telemóvel, que ferramentas permitem, ninguém anda aqui a procurar critérios de qualidade, de preço, que é o seu trabalho de questões éticas e é muito mais difícil, porque o seu estado da arte recursivo vai – lhe dizer precisamente isto, há muitas ferramentas que permitem tirar conhecimento, muitas delas desenvolvidas em provas de conceito nessas próprias teses de mestrado, e obviamente não podem ser usadas em sede jurídica…para garantir a integridade da informação.

Moderador: …Tivemos também em conta a data de publicação, tentamos aqui ao máximo…é um mundo que muda muito rapidamente...datas de 2020, 2019… para tentar…tirar uma fotografia do que é mais atual, se é que esse mais atual existe.

I3: …Você fez muito bem, andou ali focado naquelas aplicações as pagas e as gratuitas. As gratuitas não são usadas, as pagas são usadas. As gratuitas não são usadas…é usado no ponto de vista de pen-testing mas no conceito corporativo. No conceito jurídico, é o pago que vai trazer credibilidade, porque ao pagar eu estou a transpor para aquela organização o ónus da competência…

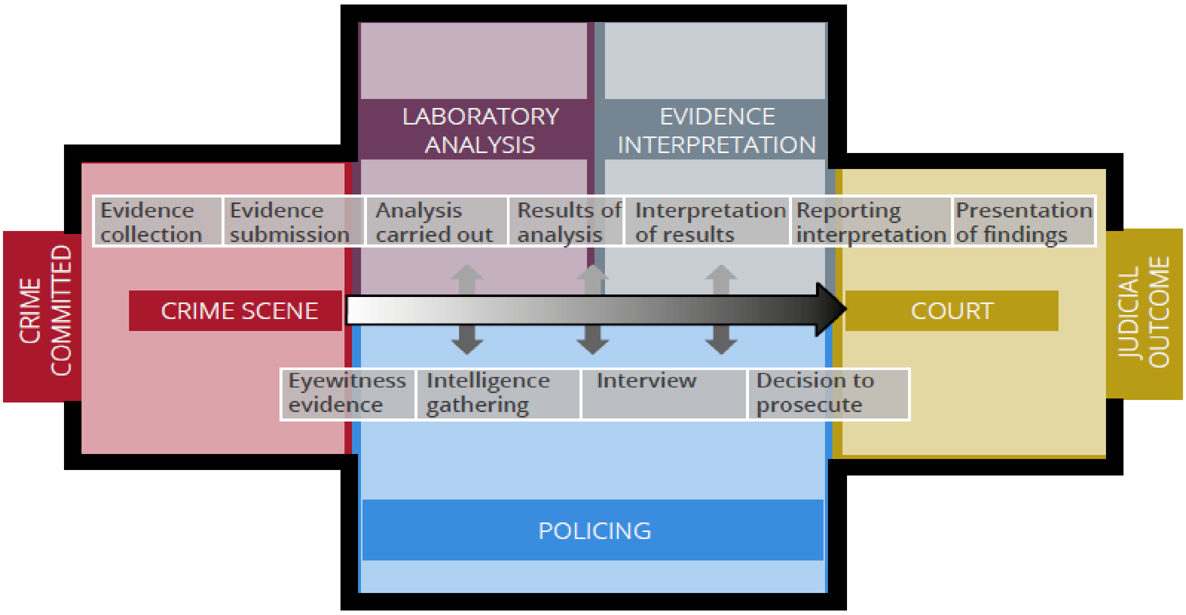
I2: …Na vertente mais profissional e não no mundo jurídico… há um aspeto ético… do facto de não se cruzarem os dois mundos entre o pessoal e profissional. Da perspetiva mais técnica…os próximos passos…na perspetiva mobile e havendo aquela fase a montante e que é distinta do que é o modo mais tradicional de um computador…daí em diante tudo é semelhante. Mas na perspetiva mobile há de facto aqui diferenças…que devem ser…aprofundadas. Quais é que são os mecanismos genéricos que levam a que uma ferramenta que é até é utilizada pelos estados e que não seja utilizada uma ferramenta open-source… com certeza que haverá aqui diferenças técnicas que permitem ter muito mais qualidade que uma ferramenta open-source… Pensando que o forense apesar de tudo não é apenas o mundo criminal, há outros mundos que também são aplicáveis…Em termos de futuro, o caminho não me parece ser que os estados venham a dar…a impor a que os dispositivos móveis tenham a supervisão por parte dos mesmos, dos estados que garanta by default...

I3: …Do ponto de vista jurídico, a lei é…reativa, ou seja, analisa um determinado dataset de atividades dos últimos 6,7 anos e…lança uma lei que nos próximos 7 anos consiga contrapor o que de mal foi feito nos 7 anos para trás. E aqui é que entra a questão do RGPD, é uma lei de facto europeia…com um custo técnico muito elevado para as empresas…é extremamente custoso…a migração dos dados…Nós cá…não temos nenhuma lei que obrigue a que os sistemas operativos tenham em causa o aspeto jurídico…se o crime informático continuar a aumentar… 1000% ao ano…o ano passado foram constituídos arguidos em Portugal, também está na Pordata, 2000 arguidos de crime informático, que conseguiram lesar terceiros…Há um momento em que eu acho que caminhamos para ai, pelo RGPD que saiu, pela obrigação da Google não espiar do ponto de vista de dados pessoais dos utilizadores mas de salvaguardar a proteção no caso de cibercrime dos utilizadores, conforme já se legislou a parte dos dados pessoais, mais tarde ou mais cedo, vai – se legislar o mecanismo que permite ao tribunal salvaguardar os interesses jurídicos das pessoas que estão envolvidas nos crimes. Com tanta tecnologia, tanta marca e tantos sistemas operativos só vão conseguir fazer como fizeram com o RGPD, uma peça legislativa…

I2: … A haver essa abertura… só sendo imposta aos operadores e garantir by default… a capacidade de rastrear essa informação, quando há necessidade disso, num contexto jurídico.

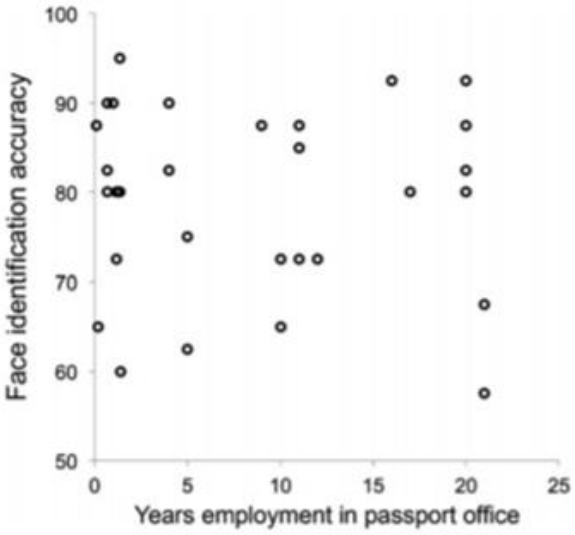
Moderador: Em jeito de conclusão, agradecer os vossos inputs… visões diferentes, pessoas que…tem experiências profissionais diferentes… Gostava de vos pedir se posso utilizar, neste caso, transcrever aquilo que foi dito…de forma anonimizada, transcrever as partes que eu…que de facto podem ser usadas e contribuem aqui…para o nosso trabalho que serão muitas.

At the end of the Focus group meeting, all three participants were asked if one (the author) could transcript the inputs and ideas given in the meeting. As such, both Interviewee 1, 2 and 3 allowed and agreed with the transcription performed above, requiring only the anonymization of their respective names.



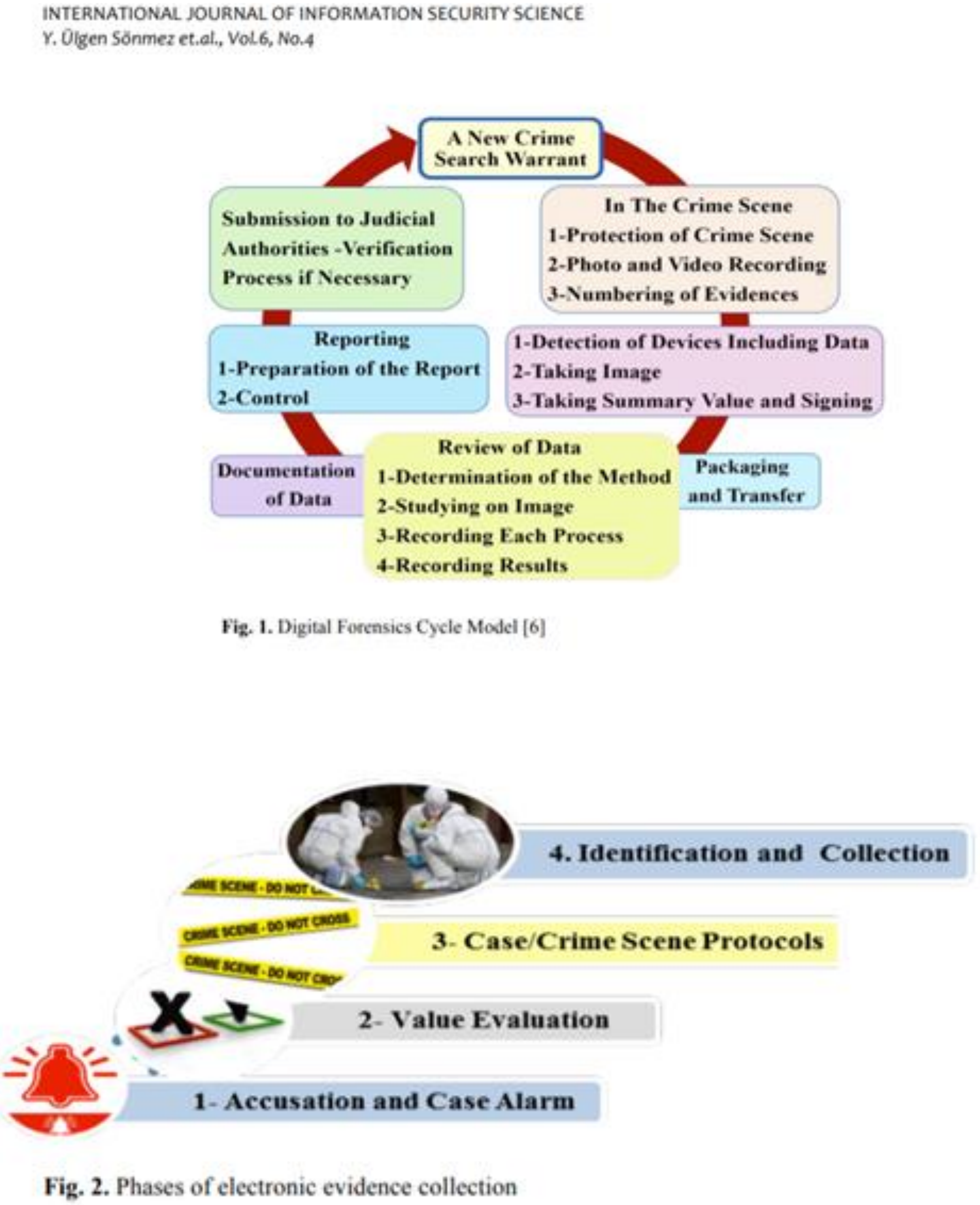
Source: Morgan, R. M., Nakhaeizadeh, S., Earwaker, H., Rando, C., Harris, A. J. L. Dror, I. E., (2018) Interpretation of evidence: Cognitive decision making under uncertainty (at every step of the forensic science process). In R. Wortley, A. Sidebottom, G. Laycock, & N. Tilley (Eds.), Handbook of Crime Science (Abingdon: Routledge, 2016), pp 408–420

Figure 11 - Forensic Science Process retrieved from the source indicated above.



Source: G. Edmond et al. / Science and Justice 57 (2017) 144–154

Figure 12 - Edmont et al. (2017) Comparison between the accuracy levels and the employment years of a worker



INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE
Y. Ülgen Sönmez et.al., Vol.6, No.4

A New Crime Search Warrant
In The Crime Scene
1-Protection of Crime Scene
2-Photo and Video Recording
3-Numbering of Evidences
1-Detection of Devices Including Data
2-Taking Image
3-Taking Summary Value and Signing
Packaging and Transfer
Review of Data
1-Determination of the Method
2-Studying on Image
3-Recording Each Process
4-Recording Results
Documentation of Data
Reporting
1-Preparation of the Report
2-Control
Submission to Judicial Authorities -Verification Process if Necessary

Fig. 1. Digital Forensics Cycle Model [6]

4. Identification and Collection
CRIME SCENE - DO NOT CROSS
3- Case/Crime Scene Protocols
2- Value Evaluation
1- Accusation and Case Alarm

Fig. 2. Phases of electronic evidence collection

Figure 13 - Digital Forensics Process and Cycle – retrieved from the source indicated above.

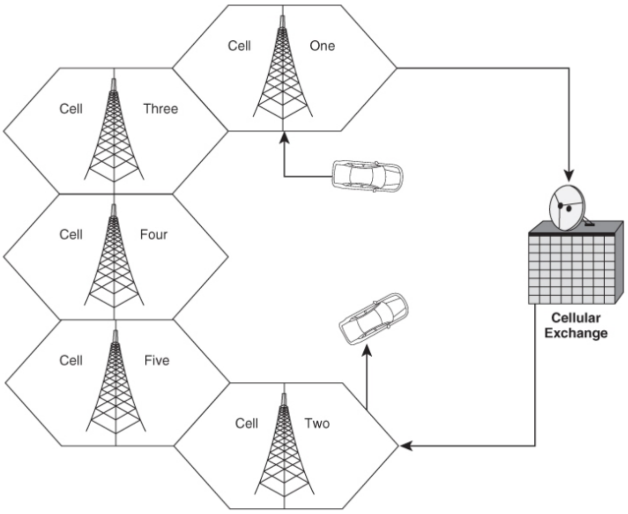


Figure 14.1 Cellular network layout

Figure 14 - Cell Towers - Cellular network layout (Graves, 2013)

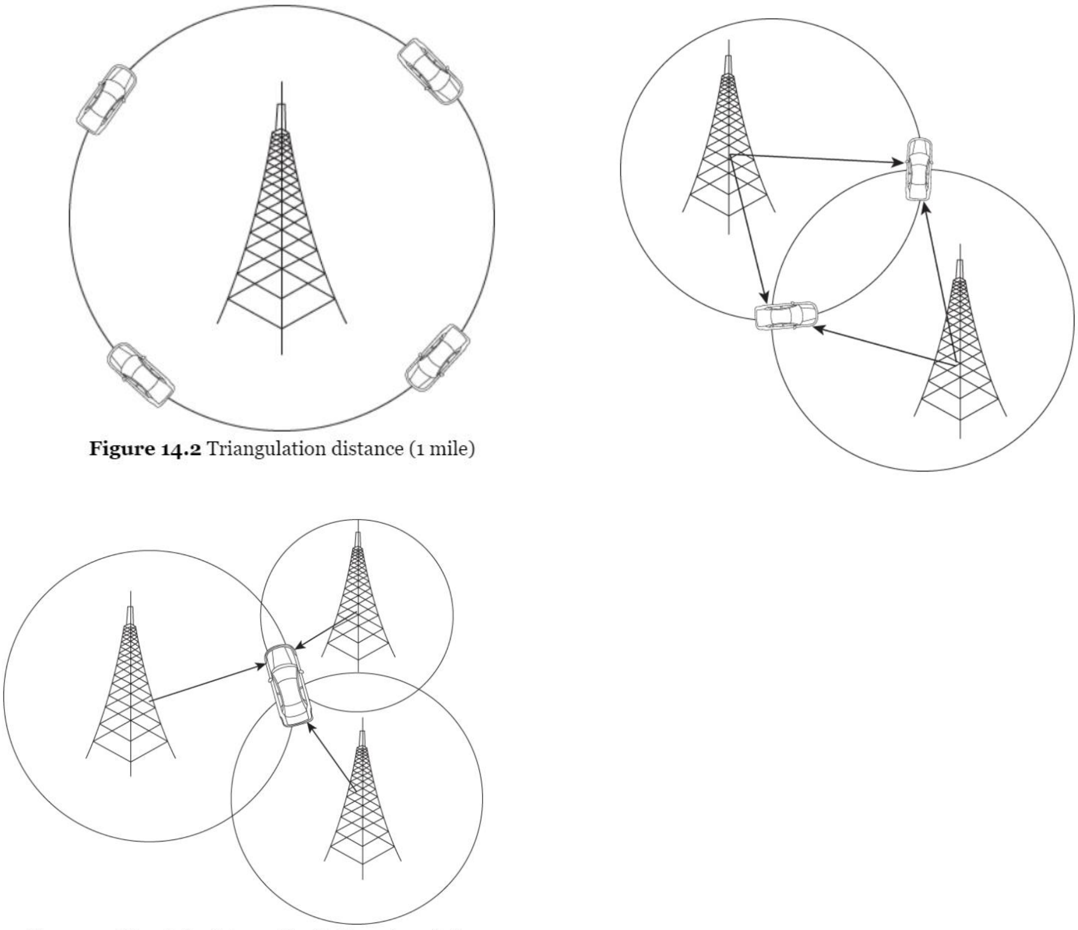


Figure 14.2 Triangulation distance (1 mile)

Figure 14.4 Triangulation distance with a third tower (1.7 miles)

Figure 15 - Triangulation distance - Cell Towers (Graves, 2013)

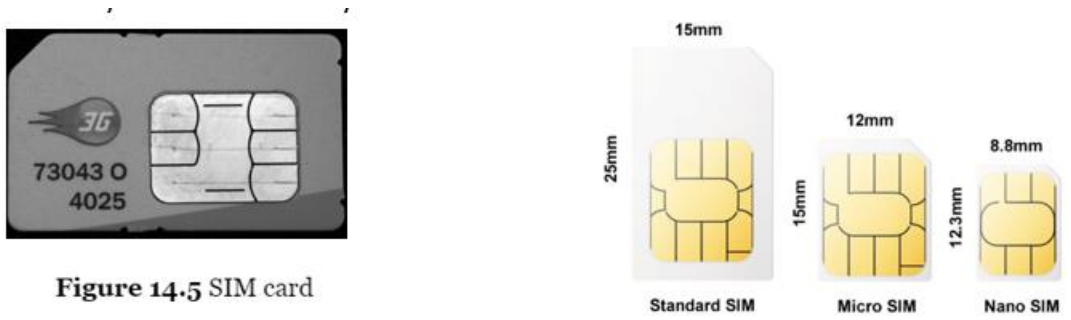


Figure 16 - The SIM Card and its size versions (The first picture from Graves 2013, the second was retrieved from the Website article 4g.co.uk/news/sim-card-sizes-standard-micro-and-nano-explained/)

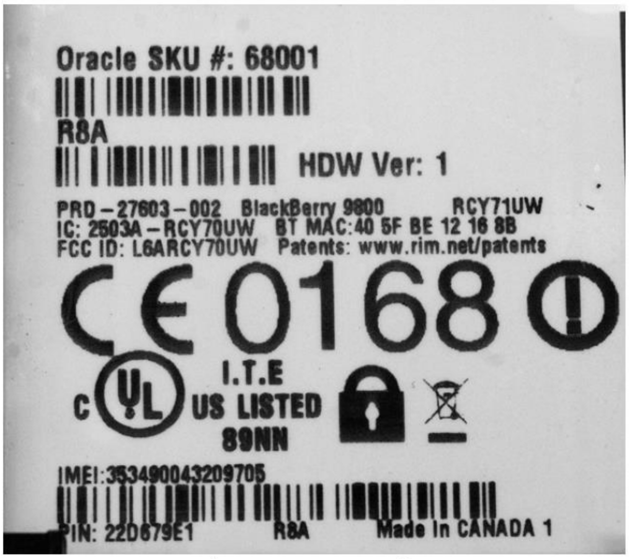

Oracle SKU #: 68001
R8A
HDW Ver: 1
PRD – 27603 – 002 BlackBerry 9800 RCY71UW
IC: 2503A – RCY70UW BT MAC:40 5F BE 12 16 8B
FCC ID: L6ARCY70UW Patents: www.rim.net/patents
CE 0168 ⓘ
c UL I.T.E US LISTED 89NN
IMEI:353490043209705
PIN: 22D679E1 R8A Made In CANADA 1

Figure 14.6 IMEI number

Figure 17 - The information on the IMEI number (Graves, 2013)

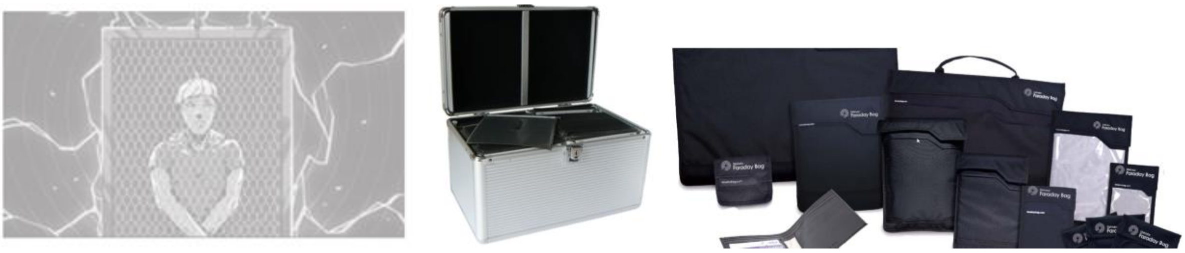


Figure 18 - The Faraday's Enclosure (retrieved from the article hackaday.com/2018/09/26/building-a-hardware-store-faraday-cage/), Box (retrieved from the article mysmartsurvival.com/why-a-faraday-cage/ and Bag (retrieved from faradaybag.com/what-is-a-faraday-bag/), respectively.

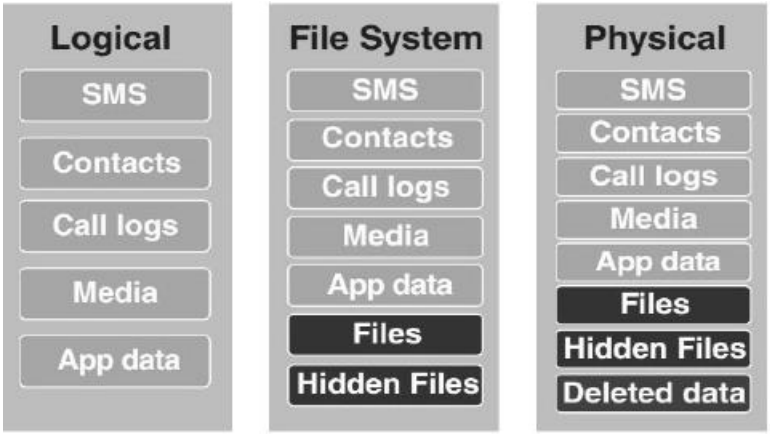


Figure 19 - Types of Phone Extraction (retrieved from the article privacyinternational.org/long-read/3256/technical-look-phone-extraction)