Handbook of Research on Cyber Crime and Information Privacy

Maria Manuela Cruz-Cunha
Polytechnic Institute of Cávado and Ave, Portugal

Nuno Ricardo Mateus-Coelho
Polytechnic Institute of Management and Technology, Portugal

Volume I

IGI Global
PUBLISHER of TIMELY KNOWLEDGE

A volume in the Advances in Information Security and Privacy (AISP) Book Series

Published in the United States of America by
IGI Global
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Names: Cruz-Cunha, Maria Manuela, 1964- editor. | Mateus-Coelho, Nuno Ricardo, 1981- editor.
Title: Handbook of research on cyber crime and information privacy / Maria Manuela Cruz-Cunha and Nuno Ricardo Mateus-Coelho, editors.
Description: Hershey, PA : Information Science Reference, [2021] | Includes bibliographical references and index. | Summary: "This book contains research on cyber-crime activities and approaches, developments, and practical examples of cyberspace security, personal and global privacy, information assurance, information protection, and ICT Law"-- Provided by publisher.
Identifiers: LCCN 2020014003 (print) | LCCN 2020014004 (ebook) | ISBN 9781799857280 (hardcover) | ISBN 9781799857297 (ebook)
Subjects: LCSH: Computer crimes. | Computer security. | Privacy, Right of.
Classification: LCC HV6773 .H3745 2021 (print) | LCC HV6773 (ebook) | DDC 364.16/8--dc23
LC record available at https://lccn.loc.gov/2020014003
LC ebook record available at https://lccn.loc.gov/2020014004

This book is published in the IGI Global book series Advances in Information Security and Privacy (AISP) (ISSN: pending; eISSN: pending)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 14
Mobile Device Forensics Investigation Process: A Systematic Review

Bruno Bernardo
Nova Information Management School, NOVA University Lisbon, Portugal

Vitor Santos
https://orcid.org/0000-0002-4223-7079
Nova Information Management School, NOVA University Lisbon, Portugal

ABSTRACT

One of the main topics that is discussed today is how can a person leverage technology in a positive and secure way in order to enhance their lives. However, with improvements in technology comes challenges; the concern that people have over their privacy and the safeguard of sensitive information being the greatest. In fact, one of the most used technologies is the mobile, which can take different forms, features, and shapes and create, store, delete, and transfer various types of data that can be evidence for the forensics fields. As such, this chapter proposes a different approach to this field by conglomerating and researching for all the information available and aiming at building a comprehensive systematic literature review on the topics of forensics, digital and mobile device forensics using the PRISMA methodology, with the intent of supporting and enhancing the mobile device forensics investigation process and allowing for a more robust and up-to-date knowledge base by breaking through the techniques available.

1. INTRODUCTION

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 is the Mobile, which can take several brands, formats and features (Klomklin & Lekcharoen, 2016). These devices are printed in

DOI: 10.4018/978-1-7998-5728-0.ch014

the daily routine of most people, from all the ages one can sought (Zhang et al., 2017). It works just like a functional computer system that contains a "treasure trove of date", allowing the user to compile and share documents, multimedia, logs, applications data, 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 to solve cases, being potentially the solution to one. As such, this chapter 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).

Nonetheless, the Mobile Forensics is being faced with challenges, namely, the lack of tools and of standard proven methodologies that permit the authors to acknowledge the data that mobiles store, and where to find and retrieve it (Chernyshev et al., 2017). Even so, this chapter 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's 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.

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). Therefore, this chapter 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, the authors consider that the concept of Digital and Mobile Device Forensics, Digital Archaeology and Digital Evidence are fundamental for this chapter. Consequently, the authors intend to describe and define them throughout this chapter 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 this 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.

2. METHODOLOGY

The main objective of this study is to present an acknowledgement and a study on the topics of Forensics, Digital and Mobile Forensic which will potentially support and improve the awareness and knowledge

around these topics, allowing investigators to have a fairly stable and up-to-date knowledge that will help in the investigation process, enabling for further improvements in the future. Likewise, it is relevant to acknowledge what are the tools available and how can one leverage on it, to pursue the Digital Archaeology related to Mobile Forensics. As a result, the authors defined and elaborated the following research question:

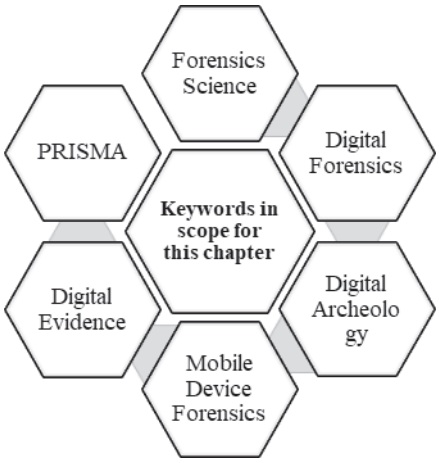
- RQ1: What are the most relevant concepts, challenges and opportunities around the Forensics field, as well as the different past, present and expected future applications and techniques/methods around it?
- RQ2: What is the maturity level and the relevant context around the Digital Forensics field 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?

Being these research questions considered, the authors ought to answer, understand, study and explore the literature and notions on Forensics, Digital Forensics, Digital Archaeology, Mobile Device Forensics and Digital Evidence, allowing for the acknowledge of pertinent context and concepts around these subjects, that will assist the authors to perform and achieve a more robust and dense research.

These research questions defined above, ought to create awareness and knowledge on these Forensics fields and as well to address several of the issues that an investigator is facing and befalling and that are jeopardizing the mobile device forensics investigation process, many caused by the lack of knowledge and awareness on the tools and techniques available for an investigator. Likewise, the research questions defined will allow the authors 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.

Moreover, the paper presented follows the afore mentioned structure: Results of the Applied Methodology and the Analysis, Discussion and Conclusion. As such, the first part of the paper 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 chapter (David et al., 2015).

Figure 1. Keywords relevant and in scope for this chapter



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 widespread information over different sources with dissimilar levels of importance for this study. As such, this allows the authors 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, to better acknowledge these topics, the authors intends to analyze the literature available, which will allow the authors 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, the authors 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.

Furthermore, in order to perform the systematic review on that is purposed on these chapter, the authors 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 chapter 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, the authors 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 analysed 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".

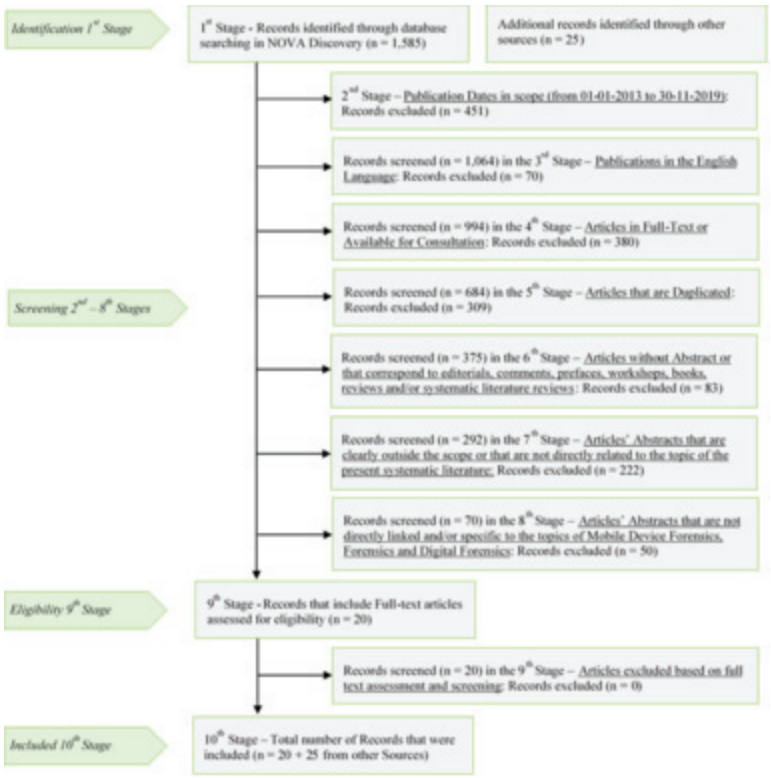
As previously referred, the expressions mentioned were used together and linked between through the application of the Boolean disjunctive logical parameter OR iteration, due to the fact that in the first stage the authors aimed at retrieving all the publications that would contain the expression of "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, the authors 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).

Results of the Applied Methodology

As previously referred, the systematic review that is presented in this chapter 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 help the authors 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).

Figure 2. 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, the authors 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 the authors 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 of 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, the authors 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.

Analysis, Discussion and Conclusion

The discussion focuses on four main topics that will be addressed throughout this research and that the authors 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 the authors to be able to acknowledge and reach the objective and subobjectives defined to answer to the research questions.

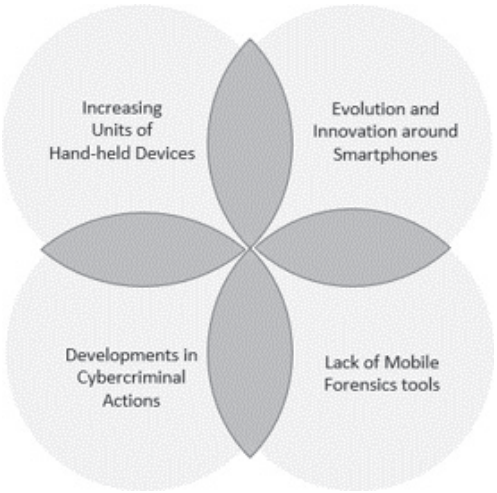
Therefore, the first part focus on scrutinizing the concept of the Forensics science, presenting the definition of this field and exploring and analyzing a background synopsis on its progression throughout time, its main core areas of application, its major and more recent opportunities and challenges for organizations and individuals. Subsequently, in the second part, the authors 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, the authors will introduce and scrutinize the field of Mobile Device Forensics and its components, understanding the main concepts around these area, as well as the main methodologies, techniques and tools that are used by a digital investigator. As for the fourth part, the authors will describe the concept of mobile archaeology as well as its main concept, strategies, challenges and tools which are strongly related to the topic of Mobile Forensics.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 (Sathe & Dongre, 2018; Chernyshev et al., 2017).

According to Jadhav & Joshi (2016), the units of hand-held devices are on the rise rapidly, where it is expected 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 chapter proposes a different approach to this field by conglomerating and researching for all the information available and aiming at building a systematic literature review with the intent of supporting and enhancing the Mobile Device Forensics investigation process by breaking through the techniques available. Hence, allowing the process to be effectively and efficiently applied, a process which is ought

Figure 3. Mobile Device Forensics Challenges



to be used as a vital foundation of an investigation, namely in "corporate, civil, criminal and military investigations" (Chernyshev et al., 2017).

The Forensics Science

As to understand the topic that will be addressed here, 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, as a result of the wide-spread applications and areas of knowledges that this field comprehends, and thus, the authors 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).

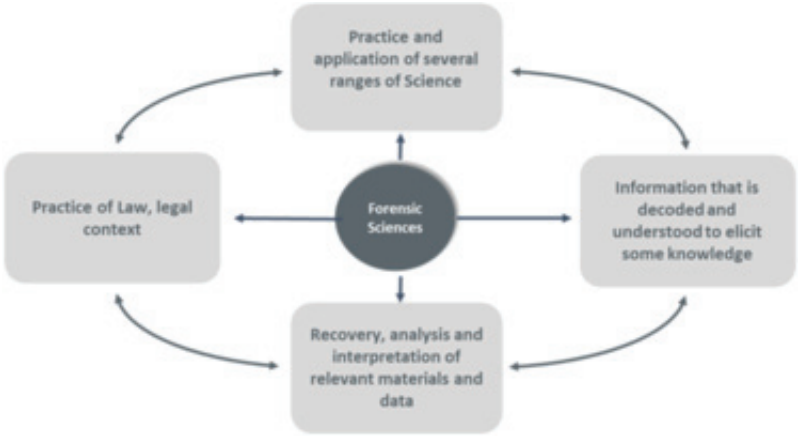
Furthermore, recent literature considers the Forensic field as the "science of spatial and temporal relationships between people, places and things" that are comprehended within a crime and its scene. This science is hemmed in by the law and its principles and involves matters and combination of matters that no other science disciplines does, 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 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 perspectives of several authors in different time frames, the authors can highlight that the majority of these concepts, 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, the authors highlighted and segmented the common terms that could be retrieve in the literature analyzed and explored which were then used to illustrate and explain the Forensics science concept, namely:

Figure 4. Common terms used to describe the Forensics Science concept



Moreover, it was important 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.

As such, the authors 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, the authors 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 liters 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 evidences 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

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 evidences that can be considered "full cast iron certainty" (Arnes, 2018).

Regarding the Forensics activity, 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 conducts 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 evidences, "things not seen" and that would remain invisible if it wasn't 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), 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) 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).

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, the authors 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 can Big data 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 this 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, 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).

The Digital Forensics Science

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, analyze and conclude on electronic and digital evidence. Denoting that it is crucial for the process of the Digital Forensics that these evidences are kept 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). According to Valdez (2018), 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).

Likewise, as for the 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 5. Four schemes of forensics evidence classification

For Carrier (2003), Digital Forensics' evidences 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 evidences 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 evidences 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).

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 evidences. After that, it is required for the evidences to be packed and transferred from the crime scene to a place where there will be more and better tools to test this evidences that were collected. To perform these tests, it is important to determine what is the technique that will be used, to study the image, to record each step taken and its results.

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 evidences 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, analyze, 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.

The Mobile Device Forensics Science

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 type 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 be 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, 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 analyze 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 is 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).

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 these science, was very outdated, scarce and poor characterized by the existence of no to limited documentation on these science 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 could one 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.

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 of mobiles, 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 misjudgments 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 this field, 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 phones has, due to the fact that some of them have very limited documentation available, specially 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, present also 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 are 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).

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 these 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 word advances and more and new technologies come out on the market and are available for the users to buy and explore at a more cheaper price, so does the integration of the mobile data and its applications with different databases, specially the clouds. As such, as there is neither an harmonized nor an 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).

The Mobile Phone's Archaeology and Mobile Forensics Available Applications

Furthermore, it is relevant to understand what are the 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. 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 amount 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.

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 are 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.

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 evidences, 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 machines 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.

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 amount 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 these 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.

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.

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. This 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.

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).

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 needs in order for a digital investigator to have access to the data on this 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 has the ability to replicated 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 evidences 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 tool 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 exists 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 evidences 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.

REFERENCES

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

Årnes, A. (2018). *Digital Forensics* (1st ed.). John Wiley & Sons Ltd.

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

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.

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. doi:10.1145/3177847

Barmpatsalou, K., Damopoulos, D., Kambourakis, G., & Katos, V. (2013). A critical review of 7 years of Mobile Device Forensics. *Digital Investigation*, *10*(4), 323–349. doi:10.1016/j.diin.2013.10.003

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. doi:10.1073/pnas.1712161115 PMID:29650539

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.

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

Chernyshev, M., Zeadally, S., Baig, Z., & Woodward, A. (2017). Mobile Forensics: Advances, Challenges, and Research Opportunities. *IEEE Security and Privacy*, *15*(6), 42–51. doi:10.1109/MSP.2017.4251107

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

Edmond, G., Towler, A., Growns, B., Ribeiro, G., Found, B., White, D., Ballantyne, K., Searston, R. A., Thompson, M. B., Tangen, J. M., Kemp, R. I., & Martire, K. (2017). Thinking forensics: Cognitive science for forensic practitioners. *Science & Justice*, *57*(2), 144–154. doi:10.1016/j.scijus.2016.11.005 PMID:28284440

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. 10.1109/INTECH.2016.7845142

Graves, M. W. (2013). *Digital Archaeology: The Art and Science of Digital Forensics*. Addison-Wesley.

Houck, M. M. (2019). How forensic science works: An architecture for the forensic enterprise. *The Australian Journal of Forensic Sciences*, *51*(3), 359–368. doi:10.1080/00450618.2017.1375396

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.

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.

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. 10.1109/CAST.2016.7915012

Katz, E., & Halámek, J. (2016). Forensic Science – Chemistry, Physics, Biology, and Engineering – Introduction. In E. Katz & J. Halámek (Eds.), *Forensic Science*. doi:10.1002/9783527693535.ch1

Kim, D., Lee, Y., & Lee, S. (2018). Mobile forensic reference set (MFReS) and mobile forensic investigation for android devices. *The Journal of Supercomputing*, *74*(12), 6618–6632. doi:10.100711227-017-2205-5

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.

Lefèvre, T. (2018). Big data in forensic science and medicine. *Journal of Forensic and Legal Medicine*, *57*, 1–6. doi:10.1016/j.jflm.2017.08.001 PMID:29801942

Li, S., Sun, Q., & Xu, X. (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*, 1015-1021.

Maras & Miranda. (2014). Forensic Science. *Encyclopedia of Law and Economics*.

Margagliotti, G., & Bollé, T. (2019). Machine learning & forensic science. *Forensic Science International*, *298*, 138–139. doi:10.1016/j.forsciint.2019.02.045 PMID:30903948

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 Routledge Handbook of Crime Science. Academic Press.

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*, *2014*, 1–10.

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.

Padmanabhan, R., Lobo, K., Ghelani, M., Sujan, D., & Shirole, M. (2016). Comparative analysis of commercial and open source mobile device forensic tools. *2016 Ninth International Conference on Contemporary Computing (IC3), Contemporary Computing (IC3), 2016 Ninth International Conference On*, 1–6. 10.1109/IC3.2016.7880238

PRISMA-P Group. (2015). Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015: Elaboration and explanation. *BMJ (Clinical Research Ed.)*, 349. PMID:25555855

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.

Roux, C., Ribaux, O., & Crispino, F. (2012). From Forensics to Forensic Science. *Current Issues in Criminal Justice*, *24*(1), 7–24. doi:10.1080/10345329.2012.12035941

Roux, C., Ribaux, O., & Crispino, F. (2018). Forensic science 2020 - the end of the crossroads? *The Australian Journal of Forensic Sciences*, *50*(6), 607–618. doi:10.1080/00450618.2018.1485738

Ryu, J. H., Kim, N. Y., Kwon, B. W., Suk, S. K., Park, J. H., & Park, J. H. (2018). Analysis of a third-party application for mobile forensic investigation. *Journal of Information Processing Systems*, *14*(3), 680–693.

Saleem, S., Popov, O., & Baggili, I. (2016). A method and a case study for the selection of the best available tool for mobile device forensics using decision analysis. *Digital Investigation*, *16*(Supplement), S55–S64. doi:10.1016/j.diin.2016.01.008

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 10.1109/ICISC.2018.8399079

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. 10.1109/EST.2015.16

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. doi:10.1016/j.jbusres.2019.07.039

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.

Su, Q., & Xi, B. (n.d.). Key technologies for mobile phone forensics and application. *Proceedings - 2017 2nd International Conference on Multimedia and Image Processing, ICMIP 2017, 2017–January*, 335–340. 10.1109/ICMIP.2017.15

Tassone, C., & Martini, B., Kim-Kwang, R. C., & Slay, J. (2013). Mobile device forensics: A snapshot. *Trends and Issues in Crime and Criminal Justice*, *460*, 1.

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

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.

Wilson, R., & Chi, H. (2017). A case study for mobile device forensics tools. *Proceedings of the South-East Conference*, 154–157. 10.1145/3077286.3077564

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. 10.1109/AINS.2017.8270423