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