Business Horizons (2016) **59**, 593—604

Available online at www.sciencedirect.com

ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

www.elsevier.com/locate/bushor

A multidisciplinary digital forensic investigation process model

Raymond Lutui

Auckland University of Technology, 55 Wellesley Street East, Auckland 1142, New Zealand

KEYWORDS
Forensic investigation models;
Smart devices;
Mobile forensics;
Network forensics;
Cloud forensics

Abstract Worldwide usage of mobile smart devices has increased dramatically over the past two decades. The popularity of these devices has grown as a result of their increased processing power, storage capacity, and memory; they can now hold enormous amounts of both personal and private business data. In addition to the consideration of mobile devices, the scope of any forensic investigation has also grown to include cloud environments. Previously, we proposed a working model that can improve the effectiveness and efficiency of an investigation in a multidisciplinary environment. The study presented herein, however, evaluates a straw man model derived from current practice models to identify the required improvements. The study also proposes a new improved process model known as a multidisciplinary digital forensic investigation process model.

1. The current state of digital forensics

The term 'digital forensics' originated as a synonym for computer forensics, but later expanded to encompass forensic examination of all digital technologies. Reith, Carr, and Gunsch (2002, p. 2) define *computer forensics* as "the collection of techniques and tools used to find evidence in a computer." The same authors, however, explain *digital forensics* as a broader concept to include (p. 2):

> The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operation.

Digital forensics can be broken down into categories, including computer forensics and mobile forensics. *Mobile forensics* is used to deal with forensic investigation of crimes that involve mobile smart devices, such as smartphones and tablets. Types of data that can be retrieved from these smart devices

E-mail address: raymond.lutui@aut.ac.nz

0007-6813/$ — see front matter
http://dx.doi.org/10.1016/j.bushor.2016.08.001

include call logs, text messages, and contact lists (Da-Yu, Shiuh-Jeng, Sharma, & Huang, 2009; Mellars, 2004).

Due to the omnipresent nature of mobile smart devices, they play a substantial role in digital crime. Regardless of their differences, they all carry precious information that can be vital to an investigation (Mohtasebi & Dehghantanha, 2013). To obtain data from a mobile device for forensic analysis, the investigator needs the help of a tool—and often more than one. Due to the differences in terms of technologies employed, investigators will have to engage different methods and tools depending on the devices involved (Albano, Castiglione, Cattaneo, & de Santis, 2011). The most challenging part is data acquisition, especially when it comes to acquiring data from volatile memory (Dezfouli et al., 2012). As described in the NIST Special Publication 800-101, *mobile device forensics* is the art of employing science to extract digital evidence from a mobile device under forensically compliant conditions while employing accepted techniques (Jansen & Ayers, 2007).

1.1. Digital forensics: Existing standards and guidelines

Digital data on mobile devices has three known properties: it is easy to copy, easy to modify, and difficult to acquire (Lin, Han-Chieh, & Shih-Hao, 2011; Yadav, Ahmad, & Shekhar, 2011). Therefore, prior to acquiring data from a mobile smart device, extra precautions must be taken and standard procedures and base practices must be followed carefully. This process is purposely implemented in order to preserve the integrity of the data or change the state of the device (Jansen & Ayers, 2007). Figure 1 shows the relationship of various fields of digital forensics.

As illustrated, there are four main areas: computer forensics, network forensics, cloud forensics, and mobile forensics (Lin et al., 2011). Regardless of the relevant area, the first step in every investigation is identification. To satisfy the identification phase, data will be extracted from the target device. However, the four areas of digital forensics require different techniques with regard to data acquisitions.

Extracting data from mobile smart devices is different from obtaining data from a computer. In the case of a computer, the hard disk can be isolated. For that reason, the forensic investigator will only work with a clone and not the actual data. However, extracting data from a smartphone's internal memory is more challenging (Fang et al., 2012; Jansen & Ayers, 2007). The most important component of this practice is to preserve the integrity of potential evidence. Certain principles and standards must be met so the findings can be admissible in a court of law (Jansen & Ayers, 2007). Therefore, there is a need to maintain the integrity and credibility of digital evidence. Reputable organizations, such as the ACPO in the United Kingdom and NIST in the United States, have made efforts to develop guidelines to help investigators.

In the NIST Special Publication 800-101, Wayne Jansen and Rick Ayers (2007) explained the purpose of their guidelines is divided into two parts. The guidelines are designed to help organizations properly navigate evolving policies and procedures for dealing with mobile phones. Also, the guidelines aim to prepare digital forensic experts for dealing with

Figure 1. Various fields of digital forensics