# Chapter 16
# The Need for Digital Evidence Standardisation

**Marthie Grobler**
*Council for Scientific and Industrial Research, South Africa & University of Johannesburg, South Africa*

## ABSTRACT

*Continuous developments in forensic processes and tools have aided in elevating the positioning of digital forensics within the legal system. The equally continuous developments in technology and electronic advances, however, are making it more difficult to match forensic processes and tools with the advanced technology. Therefore, it is necessary to create and maintain internationally accepted standards to control the use and application of digital forensic processes. This article addresses this need and touches on the motivation for such internationally recognised standards on digital evidence. It also looks at current work in and progress towards the establishment of digital evidence related documents addressing all phases of the digital forensic process.*

## INTRODUCTION

Digital forensics is a promising discipline that allows for many interdisciplinary professions within the larger computer security domain: ranging from businesses and corporations, the legal domain, military and national defence, intelligence communities, academics and technical domains. It deals with the application of scientific knowledge for collecting, analysing, and presenting legal evidence, and focuses mainly on the discovery and preservation of digital evidence for proof of and eventual prosecution of criminal activity (Taylor, Endicott-Popovsky, & Frincke, 2007).

Whereas digital forensics used to be a specific tradecraft practiced only by selected specialists, it has now grown into a global industry and a key aspect of many investigations. This is largely due to the emergence of digital evidence not only featuring in computer specific criminal cases such as hacking and malware attacks, but becoming a more common element in almost any type of crime. For example, digital evidence are a fundamental part of many corporate communication structures (i.e., email communication, calendar entries, instant messages and voice messages) and are therefore inherently considered as evidence in any criminal activities within the corporate domain.

DOI: 10.4018/978-1-4666-4006-1.ch016

In addition, digital evidence has also been used in criminal investigations involving murder and kidnapping (Chizoba, 2005; Taub, 2006; Taylor et al., 2007), and can thus be extended to any domain thinkable. This rapid growth and omnipresence of digital evidence enforces the need for regulated and standardised digital forensics.

Continuous developments in forensic processes and tools have assisted in the promotion and positioning of digital forensics within the legal system. However, at the same time continuous developments in technology and electronic advances are making it more difficult to match forensic processes and tools with the advanced technology. *"In a time of growing scrutiny of the digital forensic profession, and of forensic sciences in general, practitioners need to unite to develop accepted practice and ethics standards across all sectors of the industry"* (Kroll Ontrack Onpoint, 2011). This results in a general lack of widely accepted models and frameworks (Taylor et al., 2007). Although a lot of work has been done towards standardising this process, it has not yet been finalised. Therefore, it becomes very important that internationally developed and accepted standards are put in place to ensure the consistent application of digital forensics across the globe.

## THE SCOPE OF DIGITAL EVIDENCE

According to Garfinkle (2010), the Golden Age of digital forensics was the period from 1999 to 2007. Digital forensics was deemed as a mystical mechanism that could enable specialists to recover lost and deleted files and emails, find hidden information and give law enforcers insight into criminals' minds at a push of a button. It was during this period that the emergence of the so-called CSI (Crime Scene Investigation) effect became widespread, mystifying many people with fancy gadgets and technical abilities that allowed digital evidence to be extracted in the process of fighting digital crime.

Traditionally, best practices for digital forensics was prevalent for doing investigations on machines running Microsoft Windows, searching for file formats such as Microsoft Office documents, JPEG, AVI, and WMV. Investigations were mostly restricted to a single, non-virtual computer system, and storage devices came with standard interfaces and were generally small enough to image during a single working day. Generally, best practices were accepted as the norm for digital forensics during this Golden Age. However, technological advances, changes in general business processes, and the modern tendency for over reliance on the Internet have changed the digital forensics playing field.

Nowadays, the world is increasingly dependent on computers and technology for communications, transactions, commerce and entertainment. During a typical business day employees email documentation, access information on organisational servers and store data via the cloud. Many people own smart phones, tablets and iPads that enable the sending of emails, SMSes and instant messages from a single device. The playing field is now not a single computer system anymore, but a virtualised environment with non-conformist file types, a variety of customised storage devices and non-standard interfaces, as well as terabytes of storing space. Yarrow (2011) suggested that in 2010 alone, 1.9 billion emailers sent 107 trillion emails, averaging on 294 billion emails sent on a single day. 255 million websites were in existence at the end of 2010, with 25 billion tweets sent, and 36 billion photos uploaded to Facebook in 2010. In addition, it is suggested that by the end of 2010, the mobile phone penetration in South Africa was close to 98% (Rao, 2011).

All these developments and the increased digital inclination of many people make the dispersion of digital evidence across the Internet common. As a result, it is inevitable that sensitive business information is more exposed and vulnerable to misuse by technology-adept individuals, both on a local and international scale. This necessitates