Chapter 36
Disconnects of Specialized Mobile Digital Forensics within the Generalized Field of Digital Forensic Science

Gregory H. Carlton
California State Polytechnic University, Pomona, USA

Gary C. Kessler
Embry-Riddle Aeronautical University, Daytona Beach, USA

ABSTRACT

The study and practice of forensic science comprises many distinct areas that range from behavioral to biological to physical and to digital matters, and in each area forensic science is utilized to obtain evidence that will be admissible within the legal framework. This article focuses on inconsistencies within the accepted methodology of digital forensics when comparing the current best practices of mobile digital devices and traditional computer devices. Here the authors raise the awareness of this disconnect in methodology, and they posit that some specific tasks within the traditional best practices of digital forensic science are artifacts of ritual rather than based on scientific requirements.

INTRODUCTION

Within the legal environment, United States courts have ruled that digital data is a form of scientific evidence, and as such, the scientific approach of forensics is necessary to acquire, analyze, and report on evidence derived from digital devices.

Digital forensics, a field of forensic science, addresses the data acquisition, data analysis, and reporting aspects concerned with digital devices (i.e. computer workstations, notebook computers, computer servers, smart phones, tablets, digital cameras, GPS devices, etc.) in order to utilize data from these devices as evidence in legal matters. Traditionally, digital forensics evolved from the field of computer

DOI: 10.4018/978-1-7998-2466-4.ch036

forensics, where the focus was on obtaining evidence from computer workstations and servers. As technology evolved, mobile digital devices became prevalent and perhaps even ubiquitous today.

Along with the rise in usage of these mobile devices is the rise in the necessity to obtain evidence from them for use in litigation, and in order to obtain this evidence from the data within these mobile devices, forensic examiners often are required to utilize specialized methods. Frequently, the specialized methods necessary to obtain and analyze data from these mobile devices include tasks that are prohibited within the traditional methodology of digital forensics best practices.

TRADITIONAL DIGITAL FORENSIC METHODOLOGY

Traditional digital forensics methodology evolved from the need to scientifically gather evidence from computer workstations. The best practice establishes the preferred method to acquire evidence is to obtain a static bit-stream image from the suspect's physical device and store this image onto a logical file within the forensic examiner's workstation.

Being static, rather than dynamic, requires that the suspect's workstation is powered off prior the data acquisition process. Typically, after a suspect's workstation is powered off, the physical storage media are removed, connected to a physical write-blocking device (Kessler & Carlton, 2014), which is then connected to the forensic examiner's workstation, and the bit-stream image(s) are acquired (Forensic Focus, 2016).

The reasoning for the necessity of the static data acquisition is to ensure that the process is repeatable, which seems scientific. The argument here is that another forensic examiner can repeat the best practice of a static data acquisition and obtain the same result, whereas, had a dynamic data acquisition taken place (i.e., the suspect's workstation is still powered on and running), then data would change throughout the data acquisition process, making it impossible to duplicate the exact results.

In performing a static data acquisition, best practice methodology establishes that the sources of the bit-stream images are the physical devices of a suspect's media, not the logical volume(s) contained within the physical devices (Henry, 2016). The rationale here is that by acquiring a bit-stream image from the physical device, one would obtain all of the data on the physical device, including active files (i.e., allocated clusters), file slack, unallocated clusters, and unused space. On the other hand, if the source of the bit-stream image would be from a logical volume, then only active files would be included in the image, and then only the portions of the allocated clusters from the beginning of each file until the end of each logical file, thus omitting file slack. Likewise, unallocated clusters and unused space would not be included within the bit-stream image.

This all-inclusive approach of obtaining an image from the physical device is deemed necessary, as data might exist in unused space if previously a deleted volume had existed within those sectors. Also, much valuable data might be collected from unallocated clusters or file slack.

MOBILE DIGITAL FORENSIC METHODOLOGY

Before Mobile digital forensic methodology evolved from the traditional digital forensic methodology; however, it quickly became apparent that many of the canons of traditional digital forensic methodology simple do not work with contemporary digital devices. The courts initially admitted evidence from these