Chapter 76
Exploring Myths in Digital Forensics:
Separating Science From Ritual

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

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

ABSTRACT

Digital forensic methodology deviates significantly relative to the methods of other forensic sciences for numerous practical reasons, and it has been largely influenced by factors derived from the inception and evolution of this relatively new and rapidly changing field. Digital forensics methodology was developed more by practitioners in its early days rather than by computer scientists. This led to accepted best practices in the field that may not represent the best or, at least, tested, science. This paper explores some of these differences in the practice and evolution between digital and other forensic sciences, and recommends scientific approaches to apply to many digital forensic practice rituals.

1. INTRODUCTION

Although now accepted as a recognized forensic science by the American Academy of Forensic Sciences (AAFS), digital forensics is frequently treated differently than other, more traditional forensic sciences. While it is obvious that characteristics of cyberspace are different from those of physical space, the differences between digital forensics and "real-world" forensics are more subtle; the tools have a different relationship to the materials being examined, the results of the processes are different, and the evolution of the disciplines are different.

This paper will explore some of the ways in which the evolution of digital forensics has occurred that demonstrate the differences between it and forensics in the physical world. Section 2 will describe the basic processes of forensics and how they apply to digital forensics. Section 3 will describe the practice

DOI: 10.4018/978-1-7998-2466-4.ch076

of digital forensics, again focusing on the differences between cyber and physical world forensics. Section 4 discusses the testing of digital evidence and how heretofore "untested" dogmas became industry best practices. Section 5 provides a summary and conclusion.

2. THE PROCESS OF DIGITAL FORENSICS

Due to the manner in which the field of digital forensics evolved, many practices that were developed in the early stages during the 1990s remain in common use today without question. The authors contend that some of these practices have risen to the level of ritual and dogma, and while they might have made sense more than twenty years ago, they have not been studied from a scientific perspective to understand their relevance in today's environment.

One of the foundations of forensic science is Locard's Exchange Principle, which says, in essence, "Every contact leaves a trace" (Petherick, Turvey, Ferguson, 2010). Put another way: if two objects come into contact with one another, some part of each object is left on the other. All of the forensic sciences assume that such contacts and exchanges take place during the commission of a crime.

One common model of the forensics process, which applies equally to digital forensics or "physical" forensics, includes the following six phases (Casey and Schatz, 2011; Palmer, 2001):

1. **Identification:** Surveying a crime scene to determine potential sources of evidence that might have a nexus to the crime;
2. **Preservation:** Maintaining the state of potentially probative items to prevent changes, ensuring evidentiary integrity;
3. **Collection:** Assembling potential evidence in a manner so that the items can be forensically examined on-site (as necessary) or transported to a laboratory facility;
4. **Examination:** Testing each evidentiary item to extract probative information, making it available for analysis. This phase is guided by the legal context of the seizure and scope of the search of the items;
5. **Analysis:** Application of the scientific method, systematic processes, and critical thinking to look at the totality of the evidentiary information to answer the fundamental investigative questions: who, what, where, when, why, and how. This phase includes the analysis of both incriminating and exculpatory evidence;
6. **Reporting:** Document the entire forensics process, particularly explaining how the analysis leads to the conclusions about the crime. The type of investigation – i.e., corporate, civil, or criminal – provides the context for this phase.

2.1. Digital Forensics

Digital forensic practitioners analyze traditional computer systems (e.g., laptops, desktops, and servers), as well as network traffic, mobile devices, and digital media (such as pictures and other images, audio recordings, and videos) (Casey and Schatz, 2011). Locard's Exchange Principle applies in cyberspace as well as it does in physical space. Indeed, it applies so well that there are often hundreds or thousands of contacts that examiners may not be able to detect because of the wealth of devices touched and logs updated as data moves from one place to another on the Internet and other networks.