C15 Exploring Myths in Digital Forensics

Gary C. Kessler, PhD, Embry-Riddle Aeronautical University, 600 S Clyde Morris Boulevard, COAS 128.06, Daytona Beach, FL 32114; and Gregory H. Carlton, PhD, Cal Poly Pomona, Computer Information Systems Dept, 3801 W Temple Avenue, Pomona, CA 91768*

The goals of this presentation are to explain the evolution of digital forensics as a practice and to explore the historical rationale of some of the “myths” leading to the “best practices” in digital forensics and why many may no longer be relevant given today’s technologies.

After attending this presentation, attendees will have a better perspective of applying admissibility tests to digital evidence.

Digital forensics — née *computer forensics* — is one of the newer forensic science sections in the American Academy of Forensic Sciences (AAFS), having been established in 2008. After attending this presentation, attendees will understand some of the fundamental differences between digital forensics and the more traditional forensic sciences. Among these differences is the historical way in which digital forensics has evolved as a science and a field of practice. Appreciation of these differences may contribute to the conversation surrounding the current work of the National Institute of Justice and the National Institute of Standards and Technology as they try to codify a definition of the science of digital forensics.

Unlike the traditional forensic sciences, digital forensics investigations and methodologies were originally developed 30 years ago by computer-savvy users and practitioners rather than by the computer science community. The development of computer forensics as a discipline and field of study was very ad hoc in the 1980s and 1990s; indeed, there were very few computer forensics examiners who were not in the law enforcement community during that era. Furthermore, computer forensics courses and curricula in higher education were practically non-existent 15 years ago.

The acceleration of change in computer technology over the last 25 years has resulted not only in changing digital forensics hardware and software tools and methodologies, but also in big changes in the very technology that holds the evidence, ranging from floppy disks and hard drives to smartphones and solid-state memory devices. Many of the “best practices” of the 1990s are actually irrelevant with today’s technologies, yet are still taught in training and education programs today. Decisions based upon the adherence to the myths might cause investigators or prosecutors to not introduce probative evidence at trial, falsely believing that such evidence would not withstand a challenge in court; alternatively, a challenge might be successfully mounted due to a lack of understanding of true best practices.

This study will introduce several of the long-held computer forensics myths and discuss their place in the modern practice of digital forensic science.

Digital Forensics, Best Practices, Evidence