D13 Digital Evidence Forensic Education: Computers, Forensics, and the Future

Mark M. Pollitt, MS, Digital Evidence Professional Services, Inc., PO Box 1309, Ellicott City, MD 21041*

After attending this presentation, attendees will learn about the history and present state of digital evidence forensic education and how it may evolve in the future.

This presentation will impact the forensic community and/or humanity by providing factual information about digital forensics to the forensic science community, help to build bridges between traditional forensic science disciplines and digital forensics, and provide a frame of reference for educators from both the computer and forensic science communities. The result will be better service to the general public and the capability to provide critical services in the Information Age.

As defined by the Scientific Working Group on Digital Evidence; digital evidence is information of probative value, stored or transmitted in binary form. The forensic examination of computer hard drives, tapes, and disks have been done for well over a decade. Initially the work was done by criminal investigators in the field and in their offices. With some support from the private sector, organizations and agencies began to develop training programs to teach both the technology and the forensic techniques. In this initial phase, the vast majority of digital forensics was done by people whose education and training was neither forensic science nor computer science.

As the volume and capacity of digital devices grew exponentially, the need for specialized training and education grew. Since digital evidence starts as physical evidence and the goals of a forensic examination are the same for traditional forms of latent evidence as digital evidence, crime laboratories started to develop programs for the examination of digital evidence. Many laboratories began their program by training scientists from traditional disciplines, such as chemists, document examiners, and engineers, in this new field. A new form of forensic laboratory came on the scene; it was the Regional Computer Forensic Laboratory, which focused entirely on the examination of digital evidence.

At the turn of the millennium, computer scientists turned their attention to the problems of computer security and infrastructure protection. It was clear that society's dependence on information, computers, and network communication needed attention. The Federal government established a pair of scholarship and capacity-building programs supported by the National Science Foundation and the National Security Agency, collectively called the Cyber Corps, to increase the quality and quantity of computer scientists that could be employed in the computer security and infrastructure protection. One of the tenants of this new focus on infrastructure protection was that after assets were protected, there needed to be a means to detect adverse activity and then to react to these events. Computer scientists recognized that digital forensics could play a very important role in the detection and reaction phases of infrastructure protection. As a result, traditional computer scientists became interested in digital forensics. One effect of this new attention was that traditional computer scientists began to study forensic science methods and techniques.

In 2003, digital evidence won acceptance as a forensic science with its acceptance as a discipline subject to accreditation by the American Society of Crime Laboratory Directors – Laboratory Accreditation Board. With this acceptance has come rapid adoption of many of the traditional forensic science features, including formal education. This occurred at exactly the same time as computer scientists participating in the Cyber Corps program were becoming interested in forensics.

In early 2003, a group was established, with the support of the FBI Regional Computer Forensics Laboratory Program and the University of Tulsa, which was comprised of faculty from a number of Cyber Corps colleges and universities, forensic science faculty, and digital evidence forensic practitioners from law enforcement and crime laboratories. This group has become known as the Computer Forensic Educators Working Group. In part due to this organization, colleges and universities offering digital forensic courses has grown dramatically and many are beginning to offer certificates and concentrations in digital forensics. Full degrees in digital forensics are not far in the future. It is remarkable that this is occurring at the same time that traditional forensic science educational programs are seeking accreditation.

This presentation will explore how these parallel histories might collide and how the resulting synergy can only benefit the entire forensic science community.

Digital Evidence, Forensic Education, Cyber Corps

 ** Presenting Author*