D20 Digital Evidence as A New Forensic Science Discipline

Carrie M. Whitcomb, MSFS, National Center for Forensic Science,P.O. Box 162367, Orlando, FL*

The goal of this presentation is to inform the audience of courses of action for developing a new forensic science.

In the 1980s, law enforcement began to seize computers and other digital media as potential sources of evidence, just as they had seized business and personal records, letters, diaries, and ledgers previously. Law enforcement used commercially available software "tools" to assist in uncovering latent evidence on hard drives and other electronic storage media. Eventually they began to develop software themselves and vendors began producing forensic software tools. The capacity of computer drives increased and the magnitude of the technology increased. The seized information increased from gigabytes to terabytes, and the work became more complicated. Software was developed that could perform automated searches to elicit specified evidence from large amounts of data.

By the mid- to late 1980s, computers were beginning to show up in forensic laboratories as submissions. In the 1990s, this trend increased and by 1998, the FBI sponsored the formation of the Scientific Working Group for Digital Evidence (SWGDE) in order for the forensic science and investigative communities to develop definitions, best practices, and examination protocols for the collection, preservation, transport, and examination of digital evidence. In 2000, SWGDE approached the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) concerning the possibility of devel- oping an accreditation document for digital evidence. By fall of 2002, this draft document was ready to go before the ASCLD/LAB Delegate Assembly for a vote.

If the accreditation of Digital Evidence Sections in Forensic Laboratories is passed by ASCLD/LAB's Delegate Assembly, the next steps will follow as for all other disciplines: a Proficiency Advisory Committee (PAC) must be formed utilizing experts in the field, and quality assurance programs including competency testing, proficiency testing, and tool validation will follow. Other issues that may follow include:

- Degrees and certificate programs in Digital Evidence areas
- Continuing Education & Training
- Professional Certification
- Professional Journals
- Digital Evidence Sections in Professional Organizations Computer crimes are a growing national and international problem, with the criminal being in one country and the victim in another country. In order to facilitate communication and the exchange of evidence, the law enforcement, forensic science, and legal communities from the various countries must be able to interact through a mechanism that is recognized by all participants. It is the author's opinion that an international consortium for digital evidence should be formed by existing organizations. This consortium could be a focal point for professionals involved in digital evidence collection, examination, investigations, and litigation.

Digital Evidence, New Forensic Science Discipline, Digital Media

 ** Presenting Author*