B2 Standardization of Digital Forensic ResearchTechniques

Carey R. Murphey, PhD, White Oak Labs, 5121 Valerie Street, Bellaire, TX 77401*

After attending this presentation, attendees will have increased insight into the challenges regarding standardization of emerging techniques and protocols in the field of digital forensics and will be better able to evaluate various ways in which the research community might have greater impact on standard operating procedures used by labs or investigators.

This presentation will impact the forensic science community by identifying, clarifying, and analyzing issues observed in the process of translating published techniques into adopted standard operating procedures in digital forensics.

This presentation explores the challenges of taking a technique from peer-review and publication to use in standard operating procedures by labs and investigators. Also discussed are the various constraints related to the age of the field, vendor support, and the standardization and certifications processes that are intended, in part, to directly support widespread adoption of good practices.

A case study involving forensic examination of Windows® logs is used for illustrative purposes. Despite the combination of a peer- reviewed, published protocol and a freely available software tool that facilitates implementation of the protocol, the recommended approach appears to have had quite limited adoption in the form of standard operating procedures. This was unexpected and indicates additional requirements that appear to significantly impact adoption of good practices in digital forensic labs. Peer-review, freely available tools, and even standardization of good practices might have enhanced impact on adopted standard operating procedures if additional requirements of digital forensics labs are met.

Ultimately this presentation addresses the question, what can one do to encourage regional digital forensic labs or individual investigators to adopt peer-reviewed techniques for digital forensics? Peer-review of a protocol may be valuable support for satisfying *Daubert* challenges, but it is only one of a number of requirements that labs may face in order to adopt a protocol into its standard operating procedures. Many digital forensic labs have a strong reliance on commercial software tools, such that availability of a tool that supports the protocol is an important consideration for incorporating the protocol into standard operating procedures. In some ways, this may be inherent to digital forensics due to rapidly emerging information technology and aspects of commercial software tool development. Software tools can help satisfy requirements for reliability, reproducibility or uniform accuracy. In this opinion, even the combination of peer-review of a protocol together with a freely available software tool may still have quite limited impact. This can be seen in the contrast between the reliance on commercial tools in many labs compared with the more limited adoption of open source tools. Some labs may be reluctant to codify a standard procedure without associated commercial vendor support. This suggests that peer-review, tools, and even standardization efforts may have a significantly enhanced impact if additional requirements are met.

Digital Forensics, Standard Operating Procedures, Requirements