B1 Scientific Validation of Digital Forensics Tools: A Case Study

Marcus Rogers, PhD, 401 North Grant Street, West Lafayette, IN 47907; and Philip Craiger, PhD, Daytona State College, Advanced Technology Campus, 1770 Technology Boulevard, Daytona Beach, FL 32117*

After attending this presentation, attendees will: (1) become familiar with the importance of digital forensics tool validation; (2) will be provided an overview of a large-scale study demonstrating digital forensics tool validation process; and, (3) will be presented lessons learned from a validation study.

This presentation will impact the forensic science community by showing how scientific validations of digital forensic tools are important. Anecdotal evidence; however, suggests that the tools do not appear to undergo the same scrutiny as forensic tools in other more established disciplines. Therefore, it is important that examiners (some of whom may not have a good background in computing) understand the tool validation process and how the lack thereof may affect the interpretation of the results.

As with all other forensic disciplines, the results obtained from digital forensics tools must meet basic evidentiary and scientific standards to be allowed as evidence in legal proceedings. In the United States, the requirements for the admissibility of scientific evidence and expert opinion were outlined in the precedent setting U.S. Supreme Court decision *Daubert vs. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579*. The U.S. Supreme Court found that evidence or opinion derived from scientific or technical activities must derive from methods that are proven to be "scientifically valid" to be admissible in a court of law. The term "scientifically valid" suggests that the tools and methods are capable of being proven correct through empirical testing. In the context of digital forensics, this means that the tools and techniques used in the collection and analysis of digital evidence must be validated and proven to meet scientific standards.

The recent case of *State of Florida vs. Casey Anthony* underscores the importance of tool validation. Examiners conducted an initial analysis of the family computer and found that someone had performed an internet search for the keyword "chloroform," and that the same user (apparently) visited a web page — a single time — that contained information on "how to make chloroform." A subsequent analysis with a different tool indicated the same web page had been visited ***84 times*** within a few minutes. Such a discrepancy between tool results clearly indicates a problem with the validity of one, if not both, tools.

This presentation presents an overview of a large-scale digital forensics tool validation study consisting of over 150 validation tests, as well as lessons learned. Funded by the National Institute of Justice, the purpose of the study was to validate several popular digital forensics tool suites with respect to the most commonly employed functions (e.g., keyword search, identifying deleted files, file recovery, hashing, internet history, etc.), across multiple versions of operating systems as well as across multiple file systems. The validation protocol described in the *Scientific Working Group on Digital Evidence's Recommended Guidelines for Validation Testing (Version 1.1)* was used for each validation test. Testing protocols required the creation of multiple source evidence sets for a crossed design (e.g., XP-FAT32; Vista-FAT32, Vista-FAT32, XP-NTFS, Vista-NTFS, 7-NTFS, etc.). Evidence creation scripts were developed and used to create sample evidence for each experimental "cell" (combination of operating system and file system where appropriate).

Although a few anomalies were identified, in general, the results of validation testing suggested that the digital forensic tools were capable of accurately performing the functions tested. Operating system version did not appear to affect accuracy of the tools, nor did file system type (e.g., FAT32 vs. NTFS). One interesting finding was that the user manuals for the tools occasionally did not precisely specify the limitations of a particular function, which could affect the results and consequently an examiner's interpretation of the results. This may be of some consequence if examiners are unfamiliar with the tools, and have little knowledge or experience with validation testing.

Digital Forensics, Tool Validation, Scientific Validation

 ** Presenting Author*