F27 The Need for a Full Specification for Digital Forensic Tool Validation

Nicolas R. Hughes, JD, Harris County Public Defender's Office, Houston, TX 77002-1957*

Learning Overview: After attending this presentation, attendees will better understand the definition and process of validating digital forensic tools.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by demonstrating the need for a fully specified definition of the validation of digital forensic tools.

Digital forensics encompasses the acquisition and analysis of digital data. Digital forensic examiners collect and analyze evidence pertinent to the investigation of traditional crime, cybercrime, or civil matters. Examiners routinely rely on software- and hardware-based tools to analyze otherwise unmanageable amounts of data.

Tool validation is the recognized process for evaluating the accuracy and reliably of an instrument. Validation requires the "provision of objective evidence that a given item fulfils specified requirements, where the specified requirements are adequate for an intended use."[1] The discipline of digital forensics provides a definition of validation that does not fully capture the intent of the formal definition: "[a]n evaluation to determine if a tool, technique or procedure functions correctly and as intended."[2]

In digital forensics, confusion about what "validation" means results in the use of the term to describe a wide range of methodologies. The term may describe manufacturer's internal studies, manual verification of data, and fitness-for-purpose testing conducted by the Computer Forensics Tool Testing Program or laboratories.[3] Non-public or limited manufacturer studies do not provide the empirical data needed to justify reliance upon the tool. Fitness-for-purpose testing and manual verification may demonstrate that a forensic tool operated successfully in one scenario, but typically fails to demonstrate performance over a full range of realistic conditions.

Validating digital forensic tools is inherently difficult. One difficulty is accounting for the number of variables affecting digital investigations. Many tools perform multiple functions—for example, correlating text messages, Global Positioning System (GPS) data, and photo metadata. Tools may accommodate different operating systems, devices, and hardware configurations. Tools and software often receive updates. Each different function, hardware configuration, and version represents a variable that may affect a tool's operation. Additionally, collecting digital forensic reference samples is difficult. The sensitive personal information present on digital devices poses privacy and legal concerns, making it challenging to use real samples.

The discipline should provide a functional, low-level specification of tool validation defining the requirements, reference samples, and methodologies used during tool validation. First, the discipline should enumerate the specifications and requirements for tool validation. These should include the range of conditions expected during analysis, a detailed hierarchy of functionality possible for each forensic process, and any known anomalies expected to affect a given forensic process.[1,4,5] Second, the discipline should curate appropriate validation methods and references samples. The discipline should specify the appropriate use of a validation method, the provenance of reference samples, how to generate synthetic evidence, and should specify how to structure data generated during the study. Finally, the discipline should identify remaining gaps in the assurance methodology. The gaps mark the limitations of present knowledge about forensic tools and should direct future efforts.

Fully specifying the definition of digital forensic tool validation is beneficial. A fully specified definition permits researchers, experts, and developers to make independent, incremental contributions to a common body of assurance methodology. It establishes a common definition of tool validation. Finally, a full specification encourages the generation of public, transparent data used to justify conclusions about tool performance. By fully specifying the definition of tool validation, the discipline strengthens the foundation of digital evidence.

Reference(s):

1. BIPM. *International Vocabulary of Metrology—Basic and General Concepts and Associated Terms (VIM)* 3rd edition. 2008.
2. SWGDE. *SWGDE Recommended Guidelines for Validation Testing.* 2014.
3. NIST. *Computer Forensics Tool Testing Program (CFTT)—Software Quality Group*.
4. Guo Y., Slay J., and Beckett J. Validation and verification of computer forensic software tools-searching function. *Digital Investigation* 6 (2009): S12-S22.
5. Lyle, James R. If error rate is such a simple concept, why don't I have one for my forensic tool yet?" *Digital Investigation* 7 (2010): S135-S139.

Digital Forensics, Tool Validation, Specification

*Presenting Author