IDEA GROUP PUBLISHING **ITB13038**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This paper appears in the publication, *Digital Crim and Forensic Science in Cyberspace*
edited by Panagiotis Kanellis, Evangelos Kiountouzis, Nicholas Kolokotronis, and Drakoulis Martakos

Chapter V

Validation of Digital Forensics Tools

Philip Craiger, University of Central Florida, USA

Jeff Swauger, University of Central Florida, USA

Chris Marberry, University of Central Florida, USA

Connie Hendricks, University of Central Florida, USA

Abstract

An important result of the U.S. Supreme Courts Daubert decision is that the digital forensic tools must be validated if the results of examinations using those tools are to be introduced in court. With this audience in mind, our chapter describes important concepts in forensic tool validation along with alternative just-in-time tool validation method that may prove useful for those who do not have the capability of conducting extensive, in-depth forensic tool validation efforts. The audience for this chapter is the law enforcement agent and industry practitioner who does not have a solid theoretical background—from training or experience—in software validation, and who is typically time-constrained in the scope of their validation efforts.

Introduction

As with all other forensic disciplines, digital forensic techniques and 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 (1993). The U.S. Supreme Court found that evidence or opinion derived from scientific or technical activities must come 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 techniques 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.

Traditional software validation testing is performed as a routine part of any software development effort. Software validation has been well studied, and the basic tenets of a successful validation approach have been codified in numerous standards accepted by such international bodies as the IEEE. There are significant references and standards covering the role of validation testing during software development, as illustrated in the references to this chapter.

There is often some confusion between the terms validation and verification as applied to software testing. The definitions provided in "General Principles of Software Validation; Final Guidance for Industry and FDA Staff" (http://www.fda.gov/cdrh/comp/guidance/938.html):

- **Software verification** provides objective evidence that the design outputs of a particular phase of the software development life cycle meet all of the specified requirements for that phase. Software verification looks for consistency, completeness, and correctness of the software and its supporting documentation, as it is being developed, and provides support for a subsequent conclusion that software is validated. Software testing is one of many verification activities intended to confirm that software development output meets its input requirements. Other verification activities include various static and dynamic analyses, code and document inspections, walkthroughs, and other techniques.
- **Software validation** is a part of the design validation for a finished device…considers software validation to be 'confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through software can be consistently fulfilled.' In practice, software validation activities may occur both during, as well as at the end of the software development life cycle to ensure that all requirements have been fulfilled. …the validation of software typically includes evidence that all software requirements have been implemented correctly and completely and are traceable to system requirements. A conclusion that software is validated is highly dependent upon comprehensive software testing, inspections, analyses, and other verification tasks performed at each stage of the software development life cycle.