



Standard Guide for Establishing Confidence in Digital Forensic Results by Error Mitigation Analysis¹

This standard is issued under the fixed designation E3016; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ϵ) indicates an editorial change since the last revision or reapproval.

^ε¹ NOTE—Editorial changes were made throughout in September 2016.

1. Scope

1.1 This guide provides a process for recognizing and describing both errors and limitations associated with tools used to support digital forensics. This is accomplished by explaining how the concepts of errors and error rates should be addressed in digital forensics. It is important for practitioners and stakeholders to understand that digital forensic techniques and tools have known limitations, but those limitations have differences from errors and error rates in other forensic disciplines. This guide proposes that confidence in digital forensic results is best achieved by using an error mitigation analysis approach that focuses on recognizing potential sources of error and then applying techniques used to mitigating them, including trained and competent personnel using tested and validated methods and practices.

2. Referenced Documents

2.1 ISO Standard:²

ISO/IEC 17025 General Requirements for the Competence of Testing and Measurement Laboratories

2.2 SWGDE Standards:³

SWGDE Model Quality Assurance Manual for Digital Evidence

SWGDE Standards and Controls Position Paper

SWGDE/SWGIT Proficiency Test Program Guidelines

SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence

3. Significance and Use

3.1 Digital forensics is a complex field that is heavily reliant on algorithms that are embedded in automated tools and used to process evidence. Weaknesses or errors in these algorithms,

tools, and processes can potentially lead to incorrect findings. Indeed, errors have occurred in a variety of contexts, demonstrating the need for more scientific rigor in digital forensics. This guide proposes a disciplined approach to mitigating potential errors in evidence processing to reduce the risk of inaccuracies, oversights, or misinterpretations in digital forensics. This approach provides a scientific basis for confidence in digital forensic results.

3.2 Error rates are used across the sciences to explain the amount of uncertainty or the limitation of a given result. The goal is to explain to the reader (or receiver of the result) the confidence the provider of the result has that it is correct. Many forensic disciplines use error rates as a part of how they communicate their results. Similarly, digital forensics needs to communicate how and why there is confidence in the results. Because of intrinsic difference between the biological and chemical sciences and computer science, it is necessary to go beyond error rates. One difference between chemistry and computer science is that digital technology is constantly changing and individuals put their computers to unique uses, making it infeasible to develop a representative sample to use for error rate calculations. Furthermore, a digital forensic method may work well in one environment but fail completely in a different environment.

3.3 This document provides a disciplined and structured approach for addressing and explaining potential errors and error rates associated with the use of digital forensic tools/processes in any given environment. This approach to establishing confidence in digital forensic results addresses *Daubert* considerations.

4. Background

4.1 Digital forensic practitioners are confident in the ability of their methods and tools to produce reliable conclusions; however, they often struggle to establish their confidence on a scientific basis. Some forensic disciplines use an error rate to describe the chance of false positives, false negatives, or otherwise inaccurate results when determining whether two samples actually come from the same source. But in digital forensics, there are fundamental differences in the nature of

¹ This guide is under the jurisdiction of ASTM Committee E30 on Forensic Sciences and is the direct responsibility of Subcommittee E30.12 on Digital and Multimedia Evidence.

Current edition approved May 1, 2015. Published June 2015. DOI: 10.1520/E3016-15E01.

² Available from American National Standards Institute (ANSI), 25 W. 43rd St., 4th Floor, New York, NY 10036, <http://www.ansi.org>.

³ Available from the Scientific Working Group on Digital Evidence (SWGDE), <https://www.swgde.org>.