Designation: E3016 – 18

An American National Standard

Standard Guide for Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis[1]

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.

1. Scope

1.1 This guide provides a process for recognizing and describing both errors and limitations associated with tools, techniques, and methods used to support digital and multimedia evidence forensics. This is accomplished by explaining how the concepts of errors and error rates should be addressed in digital and multimedia evidence forensics. It is important for practitioners and stakeholders to understand that digital and multimedia evidence 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 and multimedia evidence 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 mitigate them, including trained and competent personnel using tested and validated methods and practices. Sources of error not directly related to tool usage are beyond the scope of this guide.

1.2 *This international standard was developed in accordance with internationally recognized principles on standardization established in the Decision on Principles for the Development of International Standards, Guides and Recommendations issued by the World Trade Organization Technical Barriers to Trade (TBT) Committee.*

2. Referenced Documents

2.1 *ISO Standard:*[2]

ISO/IEC 17025 General Requirements for the Competence of Testing and Calibration 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 and multimedia evidence 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 and multimedia evidence 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 and multimedia evidence forensics. This approach provides a scientific basis for confidence in digital and multimedia evidence forensic results.

3.2 Error rates are used across the sciences to characterize the likelihood that a given result is correct. 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 and multimedia evidence 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 and multimedia evidence forensic method may work well in one environment but fail completely in a different environment.

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

[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 June 1, 2018. Published June 2018. Originally approved in 2015. Last previous edition approved as E3016 – 15$^{\varepsilon 1}$.DOI: 10.1520/E3016-18.

[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 (SWDGE), https://www.swgde.org.

4. Background

4.1 Digital and multimedia evidence 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 and multimedia evidence forensics, there are fundamental differences in the nature of many processes that can make trying to use statistical error rates inappropriate or misleading.

4.2 The key point to keep in mind is the difference between random errors and systematic errors. Random errors are characterized by error rates because they are based in natural processes and the inability to perfectly measure them. Systematic errors, in contrast, are caused by many different factors. In computer software, for example, an imperfect implementation can produce an incorrect result when a particular condition, usually unknown, is met. Digital forensics – being based on computer science – is far more prone to systematic than random errors.

4.3 Digital and multimedia forensics includes multiple tasks which, in turn, use multiple types of automated tools.

4.4 For each digital and multimedia evidence forensic tool,, there is an underlying algorithm (how the task should be done) and an implementation of the algorithm (how the task is done in software by a tool). There can be different errors and error rates with both the algorithm and the implementation. For example, hash algorithms used to determine if two files are identical have an inherent false positive rate, but the rate is so small as to be essentially zero.

4.5 Once an algorithm is implemented in software, in addition to the inherent error rate of the algorithm, the implementation may introduce systematic errors that are not statistical in nature. Software errors manifest when some condition is present either in the data or in the execution environment. It is often misleading to try to characterize software errors in a statistical manner since such errors are not the result of variations in measurement or sampling. For example, the hashing software could be poorly written and may produce the same hash every time an input file starts with the symbol "$".

4.6 The primary types of errors found in digital and multimedia evidence forensic tool implementations are:

4.6.1 *Incompleteness*—All the relevant information has not been acquired or found by the tool. For example, an acquisition might be incomplete or not all relevant artifacts identified from a search.

4.6.2 *Inaccuracy*—The tool does not report accurate information. Specifically, the tool should not report things that are not there, should not group together unrelated items, and should not alter data in a way that changes the meaning. Assessment of accuracy in digital and multimedia evidence forensic tool implementations can be categorized as follows:

4.6.2.1 *Existence*—Are all reported artifacts reported as present actually present? For example, a faulty tool might add data that was not present in the original.

4.6.2.2 *Alteration*—Does a forensic tool alter data in a way that changes its meaning, such as updating an existing date-time stamp (for example, associated with a file or e-mail message) to the current date.

4.6.2.3 *Association*—Do all items associated together actually belong together? A faulty tool might incorrectly associate information pertaining to one item with a different, unrelated item. For instance, a tool might parse a web browser history file and incorrectly report that a web search on "how to murder your wife" was executed 75 times when in fact it was only executed once while "history of Rome" (the next item in the history file) was executed 75 times, erroneously associating the count for the second search with the first search.

4.6.2.4 *Corruption*—Does the forensic tool detect and compensate for missing and corrupted data? Missing or corrupt data can arise from many sources, such as bad sectors encountered during acquisition or incomplete deleted file recovery or file carving. For example, a missing piece of data from an incomplete carving of the above web history file could also produce the same incorrect association.

4.6.3 *Misinterpretation*—The results have been incorrectly understood. Misunderstandings of what certain information means can result from a lack of understanding of the underlying data or from ambiguities in the way digital and multimedia evidence forensic tools present information.

4.7 The basic strategy to develop confidence in the digital and multimedia evidence forensic results is to identify likely sources of error and mitigate them. This is done by applying tool testing and sound quality control measures as described in this guide including:

4.7.1 *Tool Testing:*

4.7.1.1 Determine applicable scenarios that have been considered in tool testing.

4.7.1.2 Assess known tool anomalies and how they apply to the current case.

4.7.1.3 Find untested scenarios that introduce uncertainty in tool results.

4.7.2 *Sound Quality Control Procedures:*

4.7.2.1 Tool performance verification.

4.7.2.2 Personnel training, certification and regular proficiency testing.

4.7.2.3 Written procedures in accordance with applicable organizational quality assurance procedures.

4.7.2.4 Examinations should be documented utilizing applicable organizational quality procedures.

4.7.2.5 Document deviations/exceptions from standard operating procedures.

4.7.2.6 Laboratory accreditation.

4.7.2.7 Technical/peer review.

4.7.2.8 Technical and management oversight.

4.7.2.9 Use multiple tools and methods.

4.7.2.10 Maintain awareness of past and current problems.

4.7.2.11 Reasonableness and consistency of results for the case context.

4.8 A more formalized approach to handling potential sources of error in digital and multimedia evidence forensic processes is needed in order to address considerations such as those in *Daubert*.

4.9 The error mitigation analysis process involves recognizing sources of potential error, taking steps to mitigate any errors, and employing a quality assurance approach of continuous human oversight and improvement. Rather than focusing only on error rates, this more comprehensive approach takes into account all of the careful measures that can be taken to ensure that digital and multimedia evidence forensics processes produce reliable results. When error rates can be calculated, they can and should be included in the overall error mitigation analysis.

5. Procedures

5.1 Mitigating errors in a digital forensics process begins by answering the following questions:

5.1.1 Are the techniques (for example, hashing algorithms or string searching) used to process the evidence valid science?

5.1.2 Are the implementations of the techniques (for example, software or hardware tools) correct and appropriate for the environment where they are used?

5.1.3 Are the results of the tools interpreted correctly?

5.2 Considering each of these questions is critical to understanding errors in digital and multimedia evidence forensics. The next three sections explain the types of error associated with each question. In the first section, *Techniques* (5.3), the basic concept of error rates is addressed along with a discussion of how error rates depend on a stable population. The second section, *Implementation of Techniques in Tools* (5.4), addresses systematic errors and how tool testing is used to find these errors. The third section, *Tool Usage and Interpreting Results* (5.5), summarizes how practitioners use the results of digital and multimedia evidence forensic tools. This overall approach to handling errors in digital and multimedia evidence forensics helps address *Daubert* considerations.

5.3 *Techniques*—In computer science, the techniques that are the basis for digital processing includes copying bits and the use of algorithms to search and manipulate data (for example, recover files). These techniques can sometimes be characterized with an error rate.

5.3.1 *Error Rates*—An error rate has an explicit purpose – to show how strong the technique is and what its limitations are. There are many factors that can influence an error rate including uncertainties associated with physical measurements, algorithm weaknesses, statistical probabilities, and human error.

NOTE 1—*Systematic and Random Errors:* Error rates for many procedures can be treated statistically, however not all types of experimental uncertainty can be assessed by statistical analysis based on repeated measurements. For this reason, uncertainties are classified into two groups: the random uncertainties, which can be treated statistically, and the systematic uncertainties, which cannot.[4] The uncertainty of the results from software tools used in digital and multimedia evidence forensics is similar to the problems of measurement in that there may be both a random component (often from the underlying algorithm) and a systematic component (usually coming from the implementation).

5.3.1.1 Error rates are one of the factors described in *Daubert* to ascertain the quality of the science in expert testimony.[5] The underlying computer techniques are comparable to the type of science that is described in *Daubert*. Are the underlying techniques sound science or junk science? Are they used appropriately? In computer science, the types of techniques used are different from DNA analysis or trace chemical analysis. In those sciences, the technique or method is often used to establish an association between samples. These techniques require a measurement of the properties of the samples. Both the measurements of the samples and the associations have random errors and are well described by error rates.

5.3.1.2 Differences between digital and multimedia evidence and other forensic disciplines change how digital and multimedia evidence forensics uses error rates. There are error rates associated with some digital and multimedia evidence forensic techniques. For example, there are false positive rates for cryptographic hashing; however, the rate is so small as to be essentially zero. Similarly, many algorithms such as copying bits also have an error rate that is essentially zero. See Appendix X1, X1.2 and X1.3, for a discussion of error rates associated with hashing and copying.

5.3.2 *Error Rates and Populations*—There are other major differences between digital and multimedia evidence forensics and natural sciences-based forensic disciplines. In biology and chemistry-based disciplines, the natural components of a sample remain fairly static (for example, blood, hair, cocaine). Basic biology and chemistry do not change (although new drugs are developed and new means of processing are created). In contrast, information technology changes constantly. New types of drives (for example, solid-state drives) and applications (for example, Facebook) may radically differ from previous ones. There are a virtually unlimited number of combinations of hardware, firmware, and software.

5.3.2.1 The rapid and significant changes in information technology lead to another significant difference. Error rates, as with other areas of statistics, require a "population." One of the key features of a statistical population is that it is stable, that is, the essential elements of the composition remain constant. This allows predictions to be made. Since IT changes quickly and unpredictably, it is often infeasible to statistically describe a population in a usable way because, while the description may reflect an average over the entire population, it may not be useful for individual situations. See Note 2 for an example of this.

NOTE 2—*Deleted File Recovery Example:* File fragmentation is significant to the performance of deleted file recovery algorithms. In general, the more fragmented the files, the harder it is to recover the original files. For conventional (magnetic) hard drives, the amount of fragmentation was governed by the size of the hard drive (which change rapidly as bigger drives are brought to market) and usage patterns (which change rapidly such as storing large amount of multimedia files or using new applications). The resulting complexity itself meant that it was very difficult to

[4] Taylor, John R., *An Introduction to Error Analysis: The Study of Uncertainties in Physical Measurements*, University Science Books, Sausalito, CA, 1997, p. 93.

[5] Daubert v. Merrell Dow Pharmaceuticals (92-102), 509 U.S. 579, 1993.

determine what performance could be expected for a given drive type or user. This then changed completely when solid state drives (SSDs) were introduced and became popular. They no longer optimize performance by keeping files contiguous, rather moving files to prolong storage cell life. Additionally, the drive may "clean" deleted material. These kinds of paradigm shifts in IT are common and sometimes have unknown effects on forensic tools.

5.3.2.2 In examining these two differences – *(1)* the virtually infinite number of combinations, and *(2)* the rapid pace of change – it can be seen that error rates for digital and multimedia evidence forensics are different from other forensic disciplines. It is apparent that the error rate for many techniques being close to zero would imply that the topic of errors is of no concern to the digital and multimedia evidence forensics profession; this is clearly not the case. Similarly, it is not useful to say that potential sources of error cannot be addressed because of the lack of a meaningful population.

5.3.2.3 In order to understand error meaningfully, it is necessary to look at digital and multimedia evidence forensic tools. The tools implement a variety of computer science techniques and are "where the rubber hits the road" in digital and multimedia evidence forensics. Errors in tools and their use can have a much more significant negative impact on a digital and multimedia evidence forensic process. The next section discusses these types of errors.

5.4 *Implementation of Techniques in Tools*—The kinds of errors that occur in tools are systematic errors, not the random errors generally associated with measurements. See Note 1 for an explanation of random and systematic errors. Digital and multimedia evidence forensic tools (for example, software, hardware, and firmware) are implementations of techniques. Tools are known to contain bugs of varying impact. Bugs are triggered by specific conditions and result in an incorrect output. For example, a tool may have a bug that causes it to underreport the size of a hard drive leading to a partial acquisition.

5.4.1 Because software bugs are logic flaws, the tool will produce the same result if given the same inputs. (In some rare cases, it may be that not all inputs are known or reproducible, in which case the program output can vary from run to run.) The output is not random, even though it is wrong. These are the systematic errors. The appendix has digital and multimedia evidence forensics-based examples showing the difference between the error rate of a technique and systematic errors of tool.

5.4.2 In order to address systematic errors in tools, one must draw on computer science and software engineering. Software engineering provides methods for testing software to ascertain if it does what it is supposed to do. *Software testing and validation is the primary method for mitigating the risk of errors in tools.* Software testing can never prove that a tool is always functioning correctly; however, good testing can lead to confidence that the tool is unlikely to fail within the situations for which it has been tested.

5.4.3 There is another situation – primarily within forensic imaging of hard drives – that may cause tools to give different, but acceptable, results when processing the same drive. While imaging a hard drive, tools may not be able to read bad sectors on a drive. Tools may skip varying amounts of readable sectors that surround the bad sector for performance reasons. The resulting forensic images of a given drive made by different tools can be different and will have different hash values. Neither the tools' differing strategies for imaging a hard drive with bad sectors, nor the resulting images that differ are errors. They are, instead, the result of basic limitations with reading failing hardware.

5.4.4 When searching for something, such as a keyword or type of file, it is possible that the tool will find things that are not relevant (false positive) or fail to find things that are (false negative). These are not errors in the colloquial sense of a mistake, but are a method to describe the limitations of the tool. Digital and multimedia evidence forensic tools are designed to report only information that actually exists on the original drive, and not to report anything that does not exist. One of the goals of tool testing is to verify that this holds true.

5.5 *Tool Usage and Interpreting Results*—Even when a technique is properly implemented in a tool, the tool can be used improperly, leading to errors. Furthermore, misinterpretation of what certain information means can result from a lack of understanding of the underlying data or from ambiguities in the way digital and multimedia evidence forensic tools present information.

5.5.1 Another significant consideration related to the interpretation of results is assessing the quality of data that was reconstructed from deleted material or recovered in an unusual manner. Such data may be incomplete, may mix data from multiple original sources, or have other problems. Technical/peer review and use of a second method are often needed to address the limitations of reconstruction and recovery.

5.5.2 The errors associated with the improper tool usage, misinterpretation of results, and human factors errors are beyond the scope of this guide. They can best be addressed by sound management practices including training, proficiency testing, peer review, and best practices. Additional information is available in the SWGDE-SWGIT Guidelines and Recommendations for Training and the SWGDE Model Quality Assurance Manual for Digital Evidence Laboratories, Sections 5.2 and 5.9.

6. Error Mitigation Techniques

6.1 The field of digital and multimedia evidence forensics requires an approach to error analysis that goes beyond error rates, and addresses the broader scope of errors that are relevant to digital and multimedia evidence forensics. Digital and multimedia evidence forensics is best served by a framework that guides practitioners to state the sources of potential errors and how they were mitigated in a disciplined manner. This guide presents an error mitigation analysis process that addresses each discrete digital and multimedia evidence forensic task/process in order to accomplish this. The analysis must be flexible enough to address the wide range of evidence types and sources. Mitigation techniques will not be able to address every potential situation and the resulting error mitigation analysis should clearly state this.

6.1.1 An error mitigation analysis must address the potential sources of error for each major process and document the mitigation strategies that were employed. A list of common

mitigation strategies is described below. Three approaches for applying these as part of an Error Mitigation Analysis Report are included in Section 8. Many of these activities are discussed in ISO/IEC 17025, General Requirements for the Competence of Testing and Calibration Laboratories. Effective implementation of these activities will reduce the risk of errors.

6.2 *Tool Testing*—Tool Testing focuses on how the tool performs in situations that it was designed to handle. Evaluation of a tool is usually conducted by testing it against known data to provide confidence that a given tool is working as expected. If a tool is used in other situations, additional testing or verification will be needed. Testing has been demonstrated in computer science to be an effective method for revealing errors in tools. Testing provides confidence in multiple situations by eliminating known sources of systematic error.

6.2.1 The primary limitation of testing is that no amount of testing can prove that the tool is functioning correctly in all instances of its use. Even if all tests produce the expected results, a new test scenario may reveal unexpected results. In practice, the more testing of diverse test scenarios, the more confidence you have that the software works correctly.

6.2.2 Another limitation of testing is that each version of a tool could have flaws that are unique to that version operating in a particular environment. As new operating systems, hardware, software, and protocols evolve and new applications emerge, tools are updated to address these new developments in IT. Tool testing is further challenged by the large number of variables related to the tool and environment in which it is used.

6.2.3 These issues relate directly to the discussion of populations (see 5.3.2) and deciding how much testing is enough is an active area of research in computer science. The amount of testing often depends on the application of the software. For example, safety control systems for nuclear power stations are tested more rigorously than other non-life critical systems. Tools and functions that address the integrity of the evidence need to be tested more rigorously than functions that can be verified by alternative methods, including manual inspection.

6.3 *Performance Verification*—Performance verification refers to checking a specific tool in the environment in which it is used to ensure it can perform its given function. This is not a repetition of the in-depth tool testing already performed, but rather a quick check that the hardware has not failed, that a piece of software can interact with the environment in which it is run, or that new copies of tools that have been received are working. This may consist of running a subset of the tests from in-depth tool testing. See also SWGDE Standards and Controls Position Paper.

6.4 *Training*—Training in forensic processes in general and in the specific tool used mitigates the risk that the tool is used incorrectly. In accordance with SWGDE-SWGIT Guidelines and Recommendations for Training, forensic practitioners should be trained on the tools they are using. Formal training can include classes. Informal training can include review of tool documentation and on the job training. See also SWGDE/SWGIT Proficiency Test Program Guidelines.

6.5 *Written Procedures*—Having written procedures mitigates risk by documenting the correct procedures so forensic practitioners can more easily follow them. Procedures can be updated to keep current with industry best practices, and to state the limitations of specific tools and in what situations they are unsuitable for use.

6.6 *Documentation*—Documentation mitigates errors by allowing for review of work performed and for supporting reproducibility. A forensic practitioner's work must be reviewable in a meaningful way, including repetition of the process to assess the reliability of the results. Following written procedures and documenting significant outcomes should cover the majority of a practitioner's work. It is also important to retain and review audit/error logs of digital and multimedia evidence forensic tools in order to assess whether they functioned properly or encountered problems. Thorough documentation is especially critical for situations not fully covered by standard operating procedures. When such exceptions occur, detailing the situation and how it was handled is essential for error mitigation analysis.

6.7 *Oversight*—Technical and management oversight of digital and multimedia evidence forensic processes mitigates errors by ensuring that practitioners are trained in the tools they are using, that tools are tested, that documentation is produced and that procedures are followed.

6.8 *Technical/Peer Review*—Technical/peer review mitigates error by having another qualified forensic practitioner look for errors or anomalies in digital and multimedia evidence forensic results. This is especially important if there are novel techniques used or outcomes or findings are outside of expected results.

6.9 *Use of Second Method*—The use of a second method by the forensic practitioner mitigates errors by verifying results. Common second methods include:

6.9.1 After acquiring a forensic image of a hard drive with a tested hard drive imager and write blocker, forensic practitioner uses cryptographic hashes to verify that evidence is unchanged.

6.9.2 Manual review of reconstructed files, such as from deleted file recovery or file carving.

6.9.3 Manual review of files identified by a hash as being part of a contraband collection.

6.9.4 Use of multiple tools such as virus scanners, which while providing similar functionality, work differently.

6.9.5 *Use of Multiple Tests*—Since most digital and multimedia evidence forensic processes are non-destructive, it is possible to repeat most forensic processes as many times as necessary without "using up" the evidence. The forensic practitioner can use multiple techniques or repeat specific processes (including peer review) on copies of the evidence because the copies can be verified to be identical to the original.

6.10 *Awareness of Past and Current Problems*—Digital and multimedia evidence forensics is a rapidly moving field. Forensic practitioners can mitigate errors by staying current with problems discovered in their laboratory and elsewhere. There are several sources including vendor blogs, conferences,

listservs, forums, professional publications, and peer reviewed journals. Before relying on a particular source, forensic practitioners should carefully consider the reliability of the information and, when feasible, verify the problem for themselves.

6.11 *Error Rates*—The use of error rates can mitigate errors by showing the limits of a technique. Many digital and multimedia evidence forensics techniques, such as copying and cryptographic hashing, have very small error rates.

6.11.1 Other techniques, such as file recovery, have error rates that are dependent on multiple conditions present on the media, which are often unique to that piece of media. Therefore, it is not advisable to state an error rate for such techniques as it not likely to be relevant. There are cases where an error rate can be determined but techniques require a method to establish a baseline and may only be able to be applied in specific circumstances.[6] Error mitigation for these situations must employ other techniques, such as use of a tested tool (that reveals the tools limitations) or use of a second method.

6.12 *Context/Consistency of Data Analysis*—Context/Consistency Analysis mitigates error by checking that recovered or identified material makes sense. Does the data make sense in context? Is it in the expected format? For example, the tool purports to recover a JPEG file that further examination reveals is actually a PDF file.

6.13 *Other*—This is not an all-inclusive list of error mitigation strategies. Forensic practitioners should document and explain other strategies they employed.

7. Summary

7.1 Many processes in digital and multimedia evidence forensics have fundamental differences from those in other forensic disciples that make them unsuitable for error rate evaluations. As a result, relying solely on error rates is insufficient and potentially misleading as a method to address the quality of the science when applying *Daubert*-type factors to digital forensics. In general, assessing the reliability of scientific testimony goes beyond error rates to include whether results are the product of sound scientific method, whether empirical testing was performed, and whether standards and controls concerning the process have been established and maintained. Therefore, when applying *Daubert*-type factors to digital and multimedia evidence forensics, it is necessary to go beyond merely stating an error rate – it is necessary to perform a comprehensive error mitigation analysis that addresses potential sources of error and how they have been mitigated. Mitigation techniques will not be able to address every potential situation and the resulting error mitigation analysis should clearly state this.

7.2 Digital and multimedia evidence forensics is best served by a framework that guides practitioners to state the sources of potential errors and how they were mitigated in a disciplined manner. This guide provides a disciplined and structured approach to recognizing and compensating for potential sources of error in evidence processing. This error mitigation analysis process involves recognizing sources of potential error, taking steps to mitigate any errors, and employing a quality assurance approach of continuous human oversight and improvement. This more comprehensive process for addressing error is more constructive to establishing the scientific rigor and quality of digital and multimedia evidence forensic results than merely seeking out an error rate.

7.3 In the face of ever changing technology, digital forensic practitioners can provide reliable results by continuing to apply and develop best practices that provide guidance for how to perform forensic processes across disparate technology landscapes. Best practices may include implementing an array of error mitigation strategies such as those listed above, the foundation of which includes competent personnel implementing tested and validated tools and procedures, and employing a quality assurance approach of continuous human oversight and improvement.

8. Report

8.1 The following are three examples for what an error mitigation report might look like, each quite different from one another. The purpose is to provide sample language and sample structures for the reports. The first is quite comprehensive and shows the full breadth of applying the error mitigation strategies. The second example addresses a more specific situation and has a more focused error mitigation report. The third is focused on addressing the use of a new technique within a forensic process.

8.2 It is expected that the reader will select from the examples to create a template that works well within their laboratory and is appropriate for the type of forensic process performed. The goal is to document and communicate the steps taken to reduce errors and expose areas where there is still a significant source of error. For example, the use of a non-tested tool should be obvious from an error mitigation report and would require additional explanation for why untested tools were used.

8.3 *Example Report One*—The case involves intellectual property theft and includes web-based e-mail and cell phone analysis.

[6] For an example of an error rate for a specific situation see: Garfinkel, S. L., et al., "An Automated Solution for the Multiuser Carved Data Ascription Problem," *IEEE Transactions on Information Forensics and Security*, Vol 5, No. 4, December 2010. Available online: http://simson.net/clips/academic/2010.TFIS.Ascription.pdf, 11 June 2014.