Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/diin

Digital Investigation

Emerging paper standards in computer forensics

Susan Ballou, Secretary, ASTM E30.12[a,*], *Rhesa G. Gilliland, Co-chair, ASTM E30.12*[b,1]

[a] *National Institute of Standards and Technology (NIST), 100 Bureau Drive, Stop 8102, Gaithersburg, MD 20899-8102, United States*
[b] *Drug Enforcement Administration (DEA), Digital Evidence Laboratory, United States*

ARTICLE INFO

Article history:
Received 3 May 2011
Accepted 3 May 2011

Keywords:
Computer forensics
Paper standards
Standard practice
Education and training
Forensic Digital Image Processing

ABSTRACT

Standards related to computer forensics are being developed to help scientists perform their work effectively. This article describes different types of standards and describes the work of the American Society for Testing and Materials (ASTM) in this area.

Published by Elsevier Ltd.

Standards are utilized by many scientists across the nation and play a major role in accreditation and certification of forensic tools and products, and allow for the validation of results from forensic analyses. It is a role that is bound to expand as new forensic tools and procedures come online, and the courts require assurances that these innovations produce reliable results. Most scientists are aware of the need for standards yet have a limited understanding on the different types of standards that exist.

The types of standards can be split into two major categories; material and paper. The material standard is an artifact that has its properties or composition characterized through rigorous measurement. For example, Standard Reference Material (SRM) 613 is a wafer of glass with certified values of its trace elements. The SRM is used to calibrate equipment or used in a quality assurance program. The other category, paper, is a documentary standard that defines or sets an analysis method or process. Continuing with the glass example used to explain a material standard, a paper standard for glass will be a document that guides the user through a step by step process to determine the trace elements in glass. The standard is vetted through a consensus process resulting in a best practice, such as "Standard Test Method for Determination of Trace Elements in Glass Samples Using Inductively Coupled Plasma Mass Spectrometry (ICP MS)" offered by ASTM E30.

To create a paper standard several options exist and one option is the standards developing organization (SDO), ASTM International. The American Society for Testing and Materials (ASTM) is an example of a voluntary consensus standards organization. The members of ASTM provide the subject matter expertise for the writing and editing of test methods, guides and practices that support their particular discipline. In 2007 the Digital and Multimedia Evidence committee was established under the technical committee, E30 Forensic Science. The Digital and Multimedia Evidence committee, E30.12, has generated two active standards:

* *Corresponding author*. Tel.: +1 301 975 8750; fax: +1 301 948 0978.
E-mail addresses: susan.ballou@nist.gov (S. Ballou), rhesa.g.gilllliland@usdoj.gov (R.G. Gilliland).
[1] Tel.: +1 703 495 6578.
1742-2876/$ – see front matter Published by Elsevier Ltd.
doi:10.1016/j.diin.2011.05.017

- E2678-09 Standard Guide for Education and Training in Computer Forensics
- E2763-10 Standard Practice for Computer Forensics

To achieve standard status, the documents are first reviewed by the E30.12 committee followed by full E30 membership evaluation. These steps constitute a lengthy process with numerous checks and balances but the product ensures a robust, consensus based standard.

The E30.12 committee work products are based on drafts or documents generated from working groups such as The Scientific Working Group on Digital Evidence (SWGDE), The Scientific Working Group on Imaging Technology (SWGIT), or the Facial Identification Scientific Working Group (FISWG). These working groups have diligently culled information from the law enforcement community drafting guides, recommendations or best practices to address identified needs. The working groups achieve standards status for their documents by utilizing the ASTM E30.12 committee, taking advantage of an existing, functional, and globally accepted SDO.

As technology changes, there is a need for new practices and these can be put forward as an independent standard. Subsequently, when the general Standard Practice for Computer Forensics comes up for its review, it can be updated to include the newer standards or adjusted to reference other standards that address specific situations.

ASTM E30.12 is currently working on a new document, Standard Guide for Forensic Digital Image Processing. The next document in development is a terminology standard which will incorporate the SWGIT/SWGDE and the FISWG glossaries.

By selecting ASTM, the working groups in conjunction with E30.12, identify the product category;

- "**Standard Test Method** – defines the way a test is performed.
- **Standard Practice** – defines a sequence of operations that, unlike a test, does not produce a result.
- **Standard Guide** – provides an organized collection of information or series of options that does not recommend a specific course of action."[2]

Through collaborative work between the ASTM Digital and Multimedia Evidence committee and SWGDE, SWGIT, and FISWG, additional standards are on the horizon. The National Academy of Sciences has stated "significant improvements are needed in forensic science…It is clear that change and advancement, both systemic and scientific, are needed in a number of forensic science disciplines-to ensure the reliability of the disciplines, establish enforceable standards, and promote best practices and their consistent application."[3] For the computer and digital evidence community, the generated paper standards have paved the way for improved procedures and processes toward the greater goal of national standardization.

Susan Ballou is the Program Manager for Forensic Science in the Law Enforcement Standards Office at the National Institute of Standards and Technology (NIST). She is the Secretary for the ASTM E30.12 committee.

Rhesa G. Gilliland is the Drug Enforcement Administration (DEA), Digital Evidence Laboratory Director. She is the co-chair of the ASTM E30.12 committee.

[2] http://www.astm.org.

[3] Strengthening Forensic Science in the United States: A Path Forward http://www.nap.edu/catalog/12589.html.