Scientific Working Group on Digital Evidence

SWGDE Standards and Controls Position Paper

Disclaimer:

As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the user's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived for future reference, as needed, in accordance with that organization's policies.

Redistribution Policy:

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.

Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

Requests for Modification:

SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for change

SWGDE Standards and Controls Position Paper

The purpose of this document is to clearly define the SWGDE position on the use of standards and controls in the computer forensics sub-discipline. Recently published articles in Forensic Magazine have generated questions about the need for standards and controls in computer forensics. This paper defines our position that although standards are in use, controls are not applicable in the computer forensics sub-discipline.

Computer forensics differs from many other forensic disciplines with respect to the occurrence of incorrect and false positive results. In some forensic disciplines, a failed examination could wrongly suggest the guilt of an innocent party. For example, a malfunctioning gas chromatograph-mass spectrometer (GCMS) could report a blood alcohol level higher than the true value. In computer forensics; however, false positives are non-existent. If the forensic hardware or software used fails for any reason, the examination will not produce erroneous data. The tools and processes might fail to find existing data, producing a false negative, but they will never find non-existent data.

Because the primary goal of computer forensics examinations is to search for pre-existing data that indicate criminal activity, controls as applied in other forensic disciplines provide no substantive value to the examination process or its outcome. Even if the examiner found all of the known data in a control file, it would not guarantee the success of a subsequent examination. Instead, if the hypothetical goal of an examination was to verify that a file does *not* exist on a piece of media, then a control might need to be created using hardware and software that is identical or very similar to the media in question.

In an effort to meet the perceived accreditation requirement to use appropriate standards and controls, the digital evidence community responded in two ways. First, SWGDE published a position paper in October 2004 describing how hash values are used to ensure data integrity; this paper intended to equate the data integrity process with the use of standards and controls. Second, many digital evidence laboratories adopted a practice of copying and hashing a known file prior to the start of every examination as a control. SWGDE believes these additional efforts taken by the digital evidence community were unnecessary as the use of controls is not applicable because of the nature of computer forensic examinations.

While SWGDE recognizes the importance of ensuring the validity of examination results, we do not believe the application of controls is the means to accomplish this requirement. Validation, data integrity, and performance verification are processes within the computer forensics sub-discipline that are better suited to accomplish this task. Known standards are typically used in validation and performance verification.

Validation (as described in a 2004 SWGDE Document) is a one-time activity based on scientific principles to demonstrate new tools and procedures are suitable for their

intended purpose. Hardware and software are validated prior to their utilization in the laboratory. Data integrity (as described in a 2006 SWGDE White Paper) is performed immediately before and in parallel with every examination. Using these processes, failures are readily identifiable. Performance verification is a periodic quality assurance measure used to ensure equipment continues to operate properly (e.g., a laboratory might have an internal procedure to check their write-blockers at regular intervals).