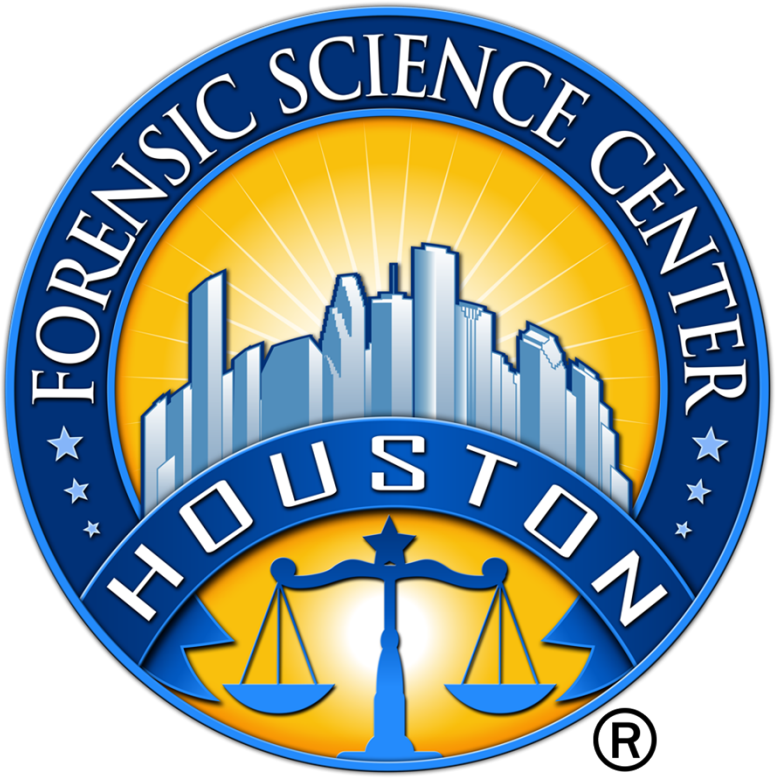

Multimedia Section
Validation and Performance Verification

Digital and Multimedia Evidence Division

1. VALIDATION AND PERFORMANCE VERIFICATION

1.1. Purpose

1.1.1. The purpose of this procedure is to establish guidelines for the validation and/or performance verification of forensic hardware and software.

1.2. Scope

1.2.1. This procedure applies to the forensic tools, hardware, and software used in the Multimedia Section.

1.3. Equipment and Software

1.3.1. Refer to the Multimedia Section's Approved Forensic Software and equipment inventory spreadsheet.

1.4. Overview

1.4.1. The Multimedia Section uses technical procedures, hardware, and software that are widely used in the digital and multimedia evidence discipline. These are known to produce outcomes consistent with the technical services requested by the customer.

1.4.2. The Multimedia Section shall be responsible for determining whether a new method, software, and/or hardware is categorized as a forensic tool.

1.4.3. New forensic tools and methodologies introduced for use in the laboratory that have not been tested by a reputable scientific, law enforcement, or educational organization, laboratory-developed methods, or the use of approved tools outside of their approved scope are to be internally validated prior to being used in evidence testing.

1.4.3.1. This internal validation is documented in the Forensic Software/Hardware Internal Validation Form prior to casework use.

1.4.3.2. The validation required above does not apply in urgent situations as described in the Exigency/Non-Validated Procedures Exception.

1.4.4. Forensic applications to be used by the Multimedia Section that have been tested and validated by reputable scientific, law enforcement, or educational organizations require performance verification. Administrative and interpretative tools do not require validation study nor performance verification.

1.4.4.1. The performance verification will be documented in the Forensic Software/Hardware Internal Validation Form.

1.4.5. Subsequently released sub-versions of previously verified software may be approved for lab use by the section supervisor/lead or manager after a review of the available release

notes. If the released version impacts core forensic services, then it must undergo performance verification before use.

1.4.5.1. An email will be sent to the section when version updates are approved for use on casework. The release notes will be available on the server.

1.4.6. Performance verifications/validations must be successfully performed before the forensic software or hardware are placed in service.

1.5. Equipment and Forensic Software Inventory

1.5.1. Each piece of technical equipment and forensic software is uniquely identified and recorded on the Multimedia Section's Equipment/Software inventory spreadsheet which is maintained by the section supervisor/lead and/or manager. The inventory spreadsheet may include the following:

- Equipment and forensic software licenses, including dongle license numbers where applicable;
- Identity of the item of equipment and/or software (i.e. workstation, write blocker, etc.);
- Manufacturer's name, make, model, and serial number (if known) and/or laboratory inventory number;
- Location (i.e. workstation, computer, laptop, etc.);
- Dates, actions, examiners identity, and results of performance verifications, and the due date of next performance verification (if applicable);
- Applicable software release installations;
- Date taken out of service, if applicable.

1.6. Data Set(s)

1.6.1. A known test data set developed in-house, or obtained from a reputable scientific organization (e.g., NIST) or vendor, is used to facilitate performance verification of certain types of media. The test data set may be the same data set used for conducting test and validation of methods, software, and hardware.

1.6.1.1. Test data sets are not tracked in LIMS and are stored in the DME Vault.

1.6.2. A test data set may include one or multiple of the following types of data for testing computer equipment and software:

- Logical file (document and spreadsheet)
- Folder
- Photo
- Web-based email
- Outlook .pst file
- Deleted files (document, spreadsheet, and photo)

- Deleted folder

1.6.3. A test data set for mobile devices may include one or multiple of the following types of data contained on a physical device or in an image for testing mobile device equipment and software:

- Call log
- Address Book
- Contacts
- Text messages (SMS, MMS)
- Picture(s)
- Video(s)

1.6.4. Test data sets may include one or multiple of the following types of data for audio and video analysis:

- Video file(s)
- Audio file(s)
- DVR

1.6.5. An inventory of the contents of the test data set(s) and associated hash value(s) is retained with the test data set, if applicable.

1.7. Internal Validation/Performance Verification Procedure

1.7.1. Forensic tools, such as software and/or hardware with no externally validated method, will have an internal validation performed.

1.7.1.1. Prior to the implementation of an externally validated standard method, software, and/or hardware, the reliability shall be demonstrated with an appropriate class test data set against its performance characteristics before it's placed into service (performance verification).

1.7.1.2. Both an internal validation and a performance verification will follow this procedure.

1.7.2. An internal validation/performance verification shall consist of the following elements:

- Purpose and/or Scope (a description of the method being tested).
- Methodology (the hardware/software, settings, and test details).
- Test data sets description (used to evaluate the specific function).
- Expected Results
- Results and Conclusions (requirements satisfied or not satisfied, observations, anomalies, concerns, or limitations).

1.7.3. Use the appropriate developed class test data set(s).

1.7.4. If relevant, hash the test data set(s) and compare the recorded values to its original creation value. This will establish that they have not been altered by the methodology.

1.7.5. Record all observations, findings, and recommendations in the Forensic Software/Hardware Internal Validation Form.

1.7.6. Validation/Verification records shall be approved by the section's supervisor/lead or manager, uploaded to Qualtrax, and approved by the Quality Director. These records shall be maintained by the section.

1.7.7. The approved forensic software and appropriate technical procedures must be updated, or a new procedure written, if the method validated has not been used in the laboratory previously.

1.8. Performance Checks

1.8.1. The following hardware must be performance checked annually:

Write Blockers (internal and external)
Faraday enclosures
Tableau TD3
Forensic Workstations

1.8.2. For a performance to pass it must meet one of the following criteria:

1.8.2.1. POST (workstations) - turns on and is operating correctly

1.8.2.2. Extraction (extraction software/hardware) - data was successfully extracted from device

1.8.2.3. Hash (imaging) - hashes for files match appropriately

1.8.2.4. Test (wiping, shielding, write blocking) - device successfully completed proper testing procedure

1.8.3. If hardware should fail, then it must successfully pass a performance check prior to being used on casework.

1.8.4. Performance checks will be documented in the appropriate workflow.

1.9. References

- Validation and Verification of Computer Forensic Software Tools-Searching Function
- Digital Forensics: Validation and Verification in a Dynamic Work Environment
- National Institute of Standards and Technology, Computer Tool Testing Program (www.cftt.nist.gov)
- Scientific Working Group on Digital Evidence (SWGDE), SWGDE Recommended Guidelines for Validation Testing, version 1.1, January 2009. (www.swgde.org)