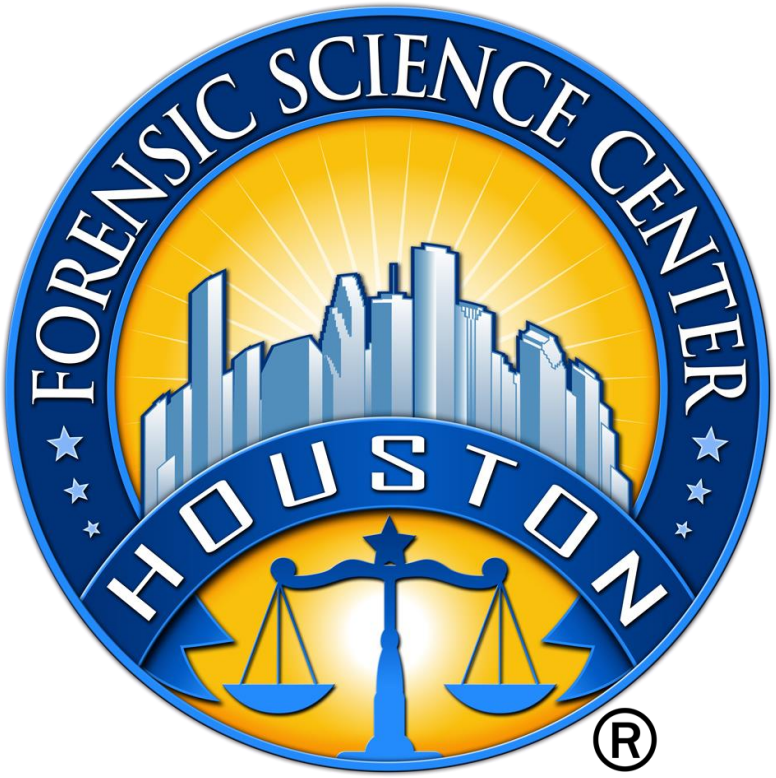


# Digital Forensics

# Validation and Performance Verification

Crime Scene/Digital and Multimedia Division

## 5. VALIDATION AND PERFORMANCE VERIFICATION

### 5.1. Purpose

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

### 5.2. Scope

5.2.1. This procedure applies to the forensic tools, hardware, and software used in the Digital Forensic Laboratory Section.

### 5.3. Equipment and Software

5.3.1. Refer to Approved Forensic Software and Hardware list for Forensic Digital Examination Section.

### 5.4. Overview

5.4.1. The Digital Forensic Laboratory uses technical procedures, hardware, and software that are widely used in the digital forensic discipline. These are known to produce outcomes consistent with the technical services requested by the customer.

5.4.2. The Digital Forensic Laboratory shall be responsible for determining whether a new method, software, and/or hardware is categorized as a forensic tool.

5.4.3. 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. This internal validation study is documented in the DFL Forensic Software/Hardware Internal Validation Form prior to casework use. After successful testing and documentation, each examiner desiring to utilize the new method or tool is required to conduct a performance check before placing it into service.

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

5.4.4. Forensic applications to be used by the Digital Forensic Laboratory that have been tested and validated by reputable scientific, law enforcement, or educational organizations require performance verification. These performance verifications will be tracked in the equipment spreadsheet where such software/hardware will be labeled as a forensic tool. Administrative and interpretative tools do not require validation study nor performance verification. Subsequently released sub-versions of previously verified software may be approved for lab use by the section's management after a review of the

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

5.4.4.1. The performance verifications for sub-versioning described above does not apply to mobile device forensic software.

5.4.5. Both Internal Validations and Performance Verifications are performed on the individual forensic functionality of the software/hardware rather than treating the software as a single entity. The validation and performance verification of specific functions allow the software/hardware in use to be partially utilized for active examinations rather than having to undergo validation of each individual functionality component. Equipment used for administrative or interpretative purposes, as well as equipment solely designed to decrypt data and/or identify, remove, or bypass security measures, does not require validation.

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

**5.5. Equipment and Forensic Software Inventory**

5.5.1. Each piece of technical equipment and forensic software is uniquely identified and recorded on the DFL Equipment/Software inventory spreadsheet which is maintained by the section's management. 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 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;
- Firmware updates;
- Hardware maintenance carried out and dates, as well as upgrades;
- Damage, malfunction, modification or repair to the equipment; and
- Date taken out of service if applicable.

**5.6. Data Set(s)**

5.6.1. 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 digital devices or components. The test data set may be the same data set used for conducting test and validation of methods, software, and hardware.

5.6.2. 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

5.6.3. 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)

5.6.4. A test data set(s) is maintained and controlled in LIMS as a tool for performance verification. 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.

**5.7. Internal Validation Procedure**

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

5.7.2. An internal validation study should consist of the following elements:

- Purpose and Scope (a description of the method being tested).
- Requirements (equipment specific function being validated).
- Methodology (the hardware/software, settings and test details).
- Test data sets description (used to evaluate the specific function).
- Expected Results
- Usage requirements (tool usage conditions required to compensate for any identified limitations).
- Results and Conclusions (requirements satisfied or not satisfied, observations, anomalies, concerns, or limitations).

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

5.7.4. 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.

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

5.7.6. Validation records shall be approved by the Section's management or technical designee and the Quality Director. These records shall be maintained by the Section's management.

5.7.7. The Approved Forensic Software and Hardware for Forensic Digital Examination Section and appropriate technical procedures should be updated or a new procedure written if the method validated has not been used in the laboratory previously.

**5.8. Performance Verification**

5.8.1. 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.

5.8.2. Class data sets are tracked in LIMS and their chain of custody is updated prior to and after the performance verification testing.

5.8.3. A report documenting the performance verification shall be completed and tracked in LIMS.

5.8.3.1. This report shall be technically reviewed by a qualified examiner or supervisor who verifies the correct method of performance verification was utilized and the results were properly documented in LIMS and DFL Software/Equipment inventory spreadsheet.

5.8.3.2. This report shall be administratively reviewed by an examiner or supervisor who verifies the report format and content are correct.

5.8.4. Performance verification testing using internal test data shall be tracked in the DFL Software/Equipment inventory spreadsheet for each item tested.

5.8.5. At a minimum, any procedure taken directly from reference sources shall be demonstrated and documented to be effective when performed by the Digital Forensic Laboratory Examiners.

5.8.6. The Approved Software for Forensic Digital Examination Section and appropriate technical procedures shall be updated if new forensic software and hardware is added to the section.

**5.9. Forensic Workstations and Laptops Performance Verification – No Integrated Write Protection**

5.9.1. The laboratory establishes the performance of forensic workstations and laptops (with or without integrated write protection) in several ways. First, when forensic workstations are used with associated forensic software or other data collection techniques, those methods are validated, verified, or adopted from reputable scientific organizations. When a laboratory method is developed in-house or approved methods are used for an alternate purpose, a validation or verification of the results is conducted. The forensic image and files contained within that/those images are hashed for verification to establish the integrity of the evidence output. These factors and activities establish the accurate performance of computers (workstations) used to support technical services.[1]

5.9.2. For standard forensic workstations and laptops without integrated write protection devices, a successful Power On - System Test (POST) will meet the requirement for performance verification. This performance verification requirement applies to workstations used to process physical devices (physical evidence – computers, peripheral devices, video, or mobile devices). This section does not apply to administrative computers.

**5.10. Forensic Workstations Performance Verification with Integrated Write Protection**

5.10.1. For forensic workstations with integrated write protection devices installed, a successful Power On System Test (POST) meets the requirement for performance verification. Additionally, each internal write protection device must be performance verified to include installed forensic imaging software. This performance verification requirement applies to workstations used to process physical devices (physical evidence – computers, peripheral devices, video, or mobile devices). Performance verification is required for each individual write protection unit installed in the forensic workstation to ensure that the units function as intended.

5.10.2. It is understood that there is no standard forensic software build common to each forensic computer used by examiners in the lab due to operating system and forensic license copyright restrictions

5.10.3. The integrated write protection units of a forensic workstation are performance verified annually.

**5.11. Write Protection Devices Performance Verification Procedure**

- The following steps are followed to verify performance of write protection devices:

[1] Laboratory management has incorporated by reference the Scientific Working Group for Digital Evidence "SWGDE Standards and Controls Position Paper," Version 1.0 issued January 30, 2008.

5.11.1. The controlled data set will be restored to a wiped digital device. The restored data volume will be hashed along with the logical files and compared with the stored hash values for the associated logical files on the controlled data set. Note: The volume hash values from the source will not match the destination volume hash value as a result of the restore process due to differing drive geometry, make, model and manufacturer of each device. The restore function in EnCase will verify a hash value after replication over the identical number of sectors that are being examined. If a separate MD5 hash is run on the target media, the hash values will only match if it computes the value over the exact number of sectors included from the source drive. However, the logical files resulting from this process should always match.

5.11.2. The write protection device will be connected to the restored digital device and to the workstation in accordance with the manufacturer's instructions.

5.11.3. Each device will be powered on.

5.11.4. An attempt will be made to read the data on the digital device attached to the write blocker.

5.11.5. An attempt will be made to delete a file from the digital device attached to the write blocker.

5.11.6. An attempt will be made to save a known data file (write attempt) to the digital device attached to the write blocker.

5.11.7. At the conclusion of these steps (1-6), the data on the original digital device will be hashed and the resulting hash will be compared with the controlled test data hash value to verify no data has been altered.

5.11.8. Successful performance verification will be documented in the equipment's spreadsheet.

5.11.9. Unsuccessful performance verification will be documented in the equipment's spreadsheet. Section management will be promptly notified when a write protection device fails.

### 5.12. Imaging Devices Performance Verification Procedure

- The following steps are followed to verify performance of imaging devices:

5.12.1. The controlled data set will be loaded onto a wiped digital device. The data will be hashed and compared with the stored hash for the controlled data set.

5.12.2. The imaging device will be connected to the loaded digital device. A wiped target device will be used to capture the image.

5.12.3. Each device will be powered on.

5.12.4. An attempt will be made to image the test data set to the target device following the manufacturer's instructions for imaging and hashing. The resulting hash will be noted.

5.12.5. At the conclusion of these steps, the data on the test digital device will be hashed and the resulting hash will be compared with the controlled data set hash value and the image hash to confirm there are matches between all three indicating data on the test device has not been altered and the image was successful.

5.12.6. Successful performance verification will be documented in the equipment's performance verification spreadsheet maintained by the section's management.

5.12.7. Unsuccessful performance verification will be documented in the equipment's spreadsheet. Section management will be promptly notified when a write protection device fails.

**5.13. Wiping Devices Performance Verification Procedure**

- The following steps are followed to verify performance of wiping devices:

5.13.1. A destination hard drive will be used.

5.13.2. The wiping device will be connected to the media device containing the data and to the workstation in accordance with the manufacturer's instructions.

5.13.3. Each device will be powered on. The manufacturer's instructions will be followed for configuring the wiping device.

5.13.4. An attempt will be made to wipe the data from the digital device using the wiping device.

5.13.5. At the conclusion of the wiping process, the wiped device will be examined with a hex editor or forensic software to visually observe the data has been wiped using "00" or other hex value specified by the examiner.

5.13.6. Each step will be documented. A comparative hash value is unnecessary, since the before and after values will not match if the wiping process was successful. The success of the wiping function will be documented in the DFL Equipment/Software inventory spreadsheet.

5.13.7. Section management will be promptly notified when a wiping device fails.

**5.14. Performance Verification of Forensic Software**

5.14.1. Due to ubiquitous acceptance within the forensic community, the full features and functionality of forensic software applications will not undergo complete performance verification. Software applications which will not be fully tested include, but are not limited to, EnCase and Forensic Toolkit (FTK). However, each of these tools will be performance verified for:

- Physical imaging
- Wiping media (EnCase only)

5.14.2. Tools which are considered interpretive or administrative (e.g., Windows OS, Microsoft Office Suite, Adobe Reader, etc.) will not undergo performance verification.

**5.15. Performance Verification of Physical Imaging Software**

- The following procedures are used to verify performance of physical imaging software:

5.15.1. The controlled data set will be loaded onto a wiped digital device. The data on the digital device will be hashed and compared with the stored hash for the controlled data set.

5.15.2. The digital device to be imaged will be connected to a forensic workstation with an approved write blocker. A second digital device, or a partition on a workstation or forensic storage area network, will be designated as the target drive for the creation of an image of the digital device.

5.15.3. Each device will be powered on and the forensic software that is to be used to image the data on the digital device with the copy of the controlled data set to the target drive or partition will be launched. Imaging software will be configured to hash the imaged data.

5.15.4. An attempt will be made to image the data on the digital device and record the hash value of the image created to the target drive or partition.

5.15.5. At the conclusion of these steps, the data on the target drive will be hashed again and the resulting hash will be compared with the original test data hash value and the image hash to confirm matches. If the hashes match, indicating no data has been altered, the performance of the imaging software is considered verified.

5.15.6. Successful performance verification will be documented in the DFL Equipment/Software inventory spreadsheet.

5.15.7. Unsuccessful performance verification will also be documented in the DFL Equipment/Software inventory spreadsheet. Section management will be promptly notified when a write protection device fails. The equipment will not be used on casework until verification is successful.

**5.16. Performance Verification of Wiping Software**

- The following procedures are used to verify performance of wiping software:

5.16.1. A drive that needs to be sanitized/wiped shall be identified and used for this process.

5.16.2. The digital device to be wiped will be connected to the workstation.

5.16.3. Each device will be powered on. Configuration of the software to wipe the digital device is performed.

5.16.4. An attempt will be made to wipe the data from the digital device using the software.

5.16.5. At the conclusion of the wiping process, the digital device will be examined with a hex editor or forensic software to visually observe that all data has been wiped.

5.16.6. Successful performance verification will be documented in the DFL Equipment/Software inventory spreadsheet.

5.16.7. Unsuccessful performance verification will be documented in the DFL Equipment/Software inventory spreadsheet. Section management will be promptly notified when a write protection device fails.

**5.17. Performance Verification of Mobile Device Extraction Software**

- The following procedures are used to verify performance of mobile device extraction software:

5.17.1. The mobile device (data set) to be imaged or extracted will be connected to a forensic workstation with the appropriate connector cable. A second digital device, or a partition on a workstation or forensic storage area network, will be designated as the target drive for the creation of an image or extraction of the mobile device.

5.17.2. The device will be powered on and the forensic software that is to be used to capture the data on the mobile device with the copy of the controlled data set to the target drive or partition will be launched.

5.17.3. An attempt will be made to image or extract the data on the mobile device.

5.17.4. At the conclusion of these steps, the data on the target drive will be compared with the original test data for confirmation. If the data on the target drive matches the original, the performance of the extraction software is considered verified.

5.17.5. Successful performance verification will be documented in the DFL Equipment/Software inventory spreadsheet.

5.17.6. Unsuccessful performance verification will also be documented in the DFL Equipment/Software inventory spreadsheet.

5.17.7. Section management will be promptly notified when a write protection device fails. The equipment will not be used on casework until verification is successful.

**5.18. Performance Verification of Mobile Device Extraction Hardware**

- The following procedures are used to verify performance of mobile device extraction hardware:

5.18.1. The mobile device (data set) to be imaged or extracted will be connected to the extraction device with the appropriate connector cable. A second digital device, or a partition on a workstation or forensic storage area network, will be designated as the target drive for the creation of an image or extraction of the mobile device.

5.18.2. The device will be powered on and the extraction hardware that is to be used to capture the data on the mobile device with the copy of the controlled data set to the target drive or partition will be powered on.

5.18.3. An attempt will be made to image or extract the data on the mobile device.

5.18.4. At the conclusion of these steps, the data on the target drive will be compared with the original test data for confirmation. If the data on the target drive matches the original, the performance of the extraction hardware is considered verified.

5.18.5. Successful performance verification will be documented in the DFL Equipment/Software inventory spreadsheet.

5.18.6. Unsuccessful performance verification will also be documented in the DFL Equipment/Software inventory spreadsheet. Section management will be promptly notified when a write protection device fails. The equipment will not be used on casework until verification is successful.

**5.19. 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)