SWGDE Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics

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 reader’s responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

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.
3. 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

Intellectual Property:
Unauthorized use of the SWGDE logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

SWGDE Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics

Table of Contents

1. Purpose

The purpose of document is to recommend minimum testing requirements for commonly used forensic tools and procedures. Organizations may exceed these minimums based on operational needs or policies.

Testing is often referred to as validation or verification testing. This document addresses testing to evaluate whether a tool or procedure performs as expected and to understand the limitations of tools.

2. Scope

This document addresses testing of the core tools used to support forensic examinations. Testing may be performed in house or results may be adopted from another competent organization.

This document identifies:

- Categories of tools used by organizations
- Types of testing methodologies that can be used by labs
  - See ***APPENDIX A*** for descriptions of types of testing.
- Frequency of testing
- Test report sources
  - See ***APPENDIX B*** for a list of possible test report sources.
- Documentation of testing results

SWGDE recommends these minimums be met prior to using tools for casework. However, organizations should make the final determination for testing based on operational needs and capabilities.

3. Limitations

This document does not address other types of testing, such as processing speed, ease of use, or whether personnel are adequately trained to use a tool.

4. General Discussion

The purpose of testing is to establish confidence that a tool or procedure performs correctly, thereby reducing the risk of errors. However, given the wide variability of software and hardware versions, it is not possible to ensure that a tool will perform as expected in all situations. Therefore, organizations must balance the confidence gained by the level and frequency of testing with the resources used to perform that testing, including the possibility that additional testing may not find significant errors. This document recommends minimum testing standards that balance the expected benefits of testing with the impact on time and resources. Organizations may have different needs that can change the cost/benefit trade-off.

There are many techniques and strategies for testing forensic tools. Each technique and strategy have different strengths and weaknesses, which must be considered when developing a testing policy.

Organizations should consider using existing tool testing programs that have been designed to simplify the testing process, while ensuring its credibility (e.g., testing plans created by the Computer Forensic Tool Testing [CFTT] project at the National Institute of Standards and Technology [NIST]). CFTT NIST has established a methodology for testing computer forensic software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware. This methodology is used to check that the procedure is suitable for the purpose intended and produces repeatable results.

This document focuses on testing that is most relevant to digital and multimedia organizations.

Testing is not necessarily pass/fail. Some faults may be sufficiently severe that the tool is not appropriate for use, but other faults may only lead to limitations on how the tool is used in certain areas, but not necessarily limit its use in all areas.

There are several sources for the various types of tools. Major sources are commercial, open source, and custom developed. In addition, certain software and hardware may be developed as a forensic tool or it may be developed for other purposes but is useful as a forensic tool. In general, tools developed for a forensics purpose are likely to have documentation relevant for forensics and to have been used in a forensics context, which is likely to have uncovered software faults. Some tools may have little or no documentation but perform a very useful function. Custom-developed software can range from large, enterprise-level tools to small scripts. This document bases its testing baseline recommendations on the function of the tool, not on the tool origin.

5. Categories of Tools and Minimum Recommendations for Testing

Organizations use a mixture of tools and techniques. This section defines different testing requirements based on tool category.

Key determining factors are how the tool or technique is used to interact with evidence or source material, its analysis, and results interpretation. Some tools, such as Adobe Photoshop, can fit in more than one category depending on how they are used.

This section provides recommendations for baseline testing for each category of tool and includes the name and description of the tools and identifies the:

- **Testing type** – The type of testing needed.
- **Frequency** – The frequency of testing.
- **Tester** – Who can do the testing.

5.1 Critical Forensic Tools

Critical forensic tools directly interact with original media or best evidence or can affect integrity (i.e., result in contamination or data modification).

5.1.1 Preservation Tools

Preservation tools prevent changes to evidence or other data.

5.1.1.1 Write Blockers

Write blockers prevent external changes to data on digital media (e.g., hard disks/SSDs, thumb drives, optical discs, DVRs, voice recorders). Write blockers can be hardware or software-based.

- **Testing type**: Write blockers may be checked by attempting to write to the drive and checking if the write command was blocked.
  Write blockers should also be checked to make sure that they do not interfere with reading data. (This can be achieved by testing the write blocker in conjunction with a disk imager.)
- **Frequency**: Before the tool is placed in service, after repair, and after any update or revision is applied. It is recommended that all units be tested.
- **Tester**: Lab. There are automated 3rd party testing tools, e.g., CRU WriteBlocking Validation Utility and CFTT Federated Testing that provide in-depth testing.

5.1.1.2 Radio Isolation

Radio frequency (RF) isolation tools prevent a device (e.g., mobile phone) from connecting to a network to prevent changes to the device.

RF Isolation is used when the device is being transported from the place of seizure to a lab as well as in the lab. There are three primary methods used: shielded containers, placing the device in airplane mode, and SIM cloning.

5.1.1.2.1 Shielded containers

Shielding containers designed to block cell phone signals are difficult to correctly manufacture and maintain and may not be 100% effective due to degrading components. Additionally, while cell phone providers currently operate on multiple bands broadcasting from 700 MHz to 2.3 GHz, close cell tower proximity can make signal interruption difficult. For proper seizure and examination of a cell phone, an examiner must place a phone in airplane mode (if available) as soon as possible, even if a shielded container is used.

- **Testing Type**: Shielded containers must be tested by placing an operational device (e.g., mobile phone) inside the container and seeing if it receives a signal. The device should use a network that is known to be strong in the location where the testing occurs.
- **Frequency**: Before being placed in service, and annually thereafter. High-use items, such as Faraday boxes, should be tested more frequently.
- **Tester:** Lab.

5.1.1.2.2 Airplane Mode

- **Testing type**: Airplane mode is tested empirically by observing if the airplane icon appears, checking that Wi-Fi and Bluetooth are also turned off, and checking that the network strength bars indicate no network connectivity.
- **Frequency**: At time of use.
- **Tester**: Person performing the seizure.

5.1.1.2.3 SIM Cloning

SIM cloning is a process for isolating GSM phones from the cellular network by creating a SIM card without network connectivity.

- **Testing type:** SIM cloning is tested by verifying that the clone contains the proper values for the IMSI and ICCID. This will verify that the GSM phones cannot connect to the network.
- **Frequency**: At time of use.
- **Tester**: Lab.

5.1.2 Acquisition Tools

Acquisition tools are used for the physical or logical collection of data.

5.1.2.1 Disk Imagers

Disk imaging tools perform physical or logical acquisitions of data from digital storage media (e.g., hard disks/SSDs, flash media, network drives).

- **Testing Type:** Testing uses a known dataset test. The test must include the use of write blockers if they are part of the normal lab process for imaging. If the imaging tool includes write blocking, the test must include verification that the media source was unchanged. (If a separate write blocker is used, this verification can happen during write blocker testing.)
    - Testers should be aware of tool limitations (e.g., large sector devices).
    - Testing must verify the imager was able to acquire the entire media or targeted portion of the media (e.g., partitions, directories, files).
    - Testing must include the media types regularly encountered by the lab.
    - Testing should verify the known dataset was acquired correctly or document and understand any anomalies.
    - Testing must document the relevant settings used during the testing.
    - Verification of the test can use either of these methods:
        - Use of a tool capable of doing a bit-by-bit comparison between the original selected data and the acquired data. If the data matches the targeted acquisition was successful.
        - Use of a hashing tool (e.g., MD5, SHA1) and compare the hash value of the original selected data to the hash value of the acquired data.
- **Frequency**: Before the tool is placed in service, after repair, and after any major updates. Many multifunction tools (e.g., Encase) have multiple updates that may not include updating the imager. If the release notes for a minor update say the imager is affected, it must be re-tested.
- **Tester**: Lab, CFTT or other 3rd party organizations can evaluate the same major version. Individual hardware devices may need to be performance-checked by the lab according to organizational policy. Performance checks can test the ability of the device to obtain at least one file from one media type.

5.1.2.2 Mobile Device Imagers

Mobile device imaging tools are used for the extraction of physical or logical data from mobile devices (e.g., phones, tablets, GPS devices).

Testing of mobile device tools presents a challenge not seen in other imaging testing, based on the rapid pace of change for both mobile phones and tools. The goal is to establish that the tool produces expected results – no mobile forensic tools are capable of acquiring all data from all mobile phones. To achieve this, testing should focus on the most common data and phone types. It is not practical to comprehensively test mobile imagers. (Specialized testing can be performed on specific phone models, as needed, based on casework.)

- **Testing type**: Testing mobile device imagers must use a known dataset. However, unlike other digital storage devices, mobile device hardware may change the dataset based on the underlying drive operations, so knowledge about the correctness of the image cannot be based solely on hashing.
  Testing should use known content (e.g., address book, images, videos, messages). The dataset should be representative of common data types that may typically be encountered by the lab. Testing does not need to include all device types and all variations of different operating systems. It is acceptable to use devices seized by the lab as long as the relevant content is documented and private information is not released.
  Known dataset testing should be supplemented with empirical testing. Forensic analysts should be alert to the possibility of incomplete data extraction, other anomalies, and tool limitations.
- **Frequency**: Before the tool is placed in service, after repair (if hardware-based), and after any major update or revision. Mobile device tools change frequently to add support for additional devices, add new functionality, and fix bugs. These changes do not require a re-test unless the added functionality is deemed critical by the organization (based on release notes), or unless otherwise required by organizational policy. For software, it is sufficient to test the software version once; for hardware, testing needs to be performed on each unit.
- **Tester**: Lab, CFTT, or other 3rd party if the same major version.

5.1.2.3 Network Connection and Extraction Applications

Network connection and extraction applications provide a conduit between a forensic workstation and remote resources being acquired. These applications provide native or other enhanced functionality to remote resources. Examples of these applications include F-Response and Nuix.

- **Testing Type**: These tools should be tested using a known dataset. This will provide a baseline capability for the tool.
- **Frequency**: Major releases.
- **Tester**: Lab, 3rd party.

5.1.2.4 Cloud Imagers

There are many types of cloud-based services with different APIs and interfaces. The procedures and tools used to gain access to cloud-based data changes frequently. Additionally, cloud services change often, making stored known data subject to change.

- **Testing type**: Testing should use a combination of known dataset (when practical) and empirical observation. Empirical testing should be done by an experienced analyst.
- **Frequency**: At time of use
- **Tester**: Lab

5.1.2.5 Other Acquisition Tools

There are many other types of acquisition tools including vehicle, drone, or memory tools.

- **Testing type**: In general, these tools should be tested with a known dataset when practical. If a tool is unable to be tested with a known dataset test, then comparison or empirical observation should be used. If empirical observation is the testing procedure, then an experienced analyst should perform this test.
- **Frequency**: In general, major tool versions should be tested.
- **Tester**: Lab, CFTT or other 3rd party if the same major version.

5.1.3 Hashing Tools

Hashing tools use cryptographic hashing algorithms to verify that data is unchanged.

- **Testing type:** Hashing can be tested with either a comparison or a known dataset test. In either case, input should include both binary and text files.
- **Frequency:** When it is placed in service and all major versions. If the hashing software is included in a larger tool, when release notes indicate that the hashing module has changed.
- **Tester:** Lab, CFTT or other 3rd party if the same major version.

5.1.4 Wiping Tools

Wiping tools overwrite existing data to sanitize or prepare storage media.

- **Testing type**: Wipers should be tested with a known pattern on media types used by the laboratory. The following process can be used:
  - Run a wiping tool using a known pattern (e.g., all zeros) against media with known content. A known pattern is preferred over a random pattern in order to verify the media was wiped successfully.
  - Testing must verify that the wipe pattern was applied to the entire targeted portion of the media.
  - View the contents of the wiped media using a hex editor and search for non-zero characters (or the character(s) that should not be present) within the wiped area. If zeros are used, a checksum can verify that the wipe was successful.
- **Frequency**: Before the tool is placed in service, after repair, and after any update or firmware revision. For software, it is sufficient to test the software version once; for hardware, testing needs to be performed on each unit.
- **Tester**: Lab, CFTT or other 3rd party if the same major version.

5.2 Underlying Systems/OS

Many forensic tools run on top of a standard operating system, such as Windows, Mac OS X or Linux. This class includes the hardware, operating systems, peripherals, disk drives, drivers, and firmware. Forensic software uses the underlying technology to accomplish various functions. When a forensic tool is tested, it is important to recognize when it is using the underlying technology of the workstation.

- **Testing type**: Vendor testing is sufficient to use these systems. If a system boots successfully, this is adequate.
- **Frequency**: Not Applicable.
- **Tester**: Vendor.

5.3 Forensic Analysis tools

These are forensic software tools used to find and analyze data. This includes functions such as searching data (e.g., string searching), recovering data (e.g., deleted file recovery) and aggregation and summary (e.g., timeline analysis).

5.3.1 Search tools

Search tools identify files or data that satisfy a given criteria. Examples include: a file with given content (string search); a file with MAC times in a given range; file of a given type (JPG, GIF, DOCX, etc.); or a list of removable attached storage devices.

- **Testing type**: Tools must be tested with either a known dataset or with manual verification of the results. Known dataset testing must include relevant characteristics that will result in an expected outcome when the tool is applied. Examples of characteristics include items that are commonly searched for (e.g., keywords) or searched material (e.g., email or images) and different types of files or media to be searched. The known dataset can include corrupted data or other non-searchable material. This testing will not show the limits of the tool's capabilities but will establish that it can perform the core function. Search parameters to consider include file system type and where to search (e.g., metadata, slack space, compressed files).
- **Frequency**: Before the tool is placed in service and after major update or revision.
- **Tester**: Lab, CFTT or other 3rd party if the same major version.

5.3.2 Recovery tools

Recovery tools are used to recover or reconstruct deleted or corrupted data.

- **Testing Type:** Tools must be tested with a known dataset test. The known dataset must include:
  - For *file carvers* (signature-based) – at least one contiguous file and one fragmented file in unallocated space.
  - For *deleted file recovery* (file system-based) – at least one contiguous file, one fragmented file, and one partially overwritten file that have all been deleted. (See www.cftt.nist.gov for definitions of file carving and deleted file recovery tools.)

  File types and file systems should be representative of work done in the organization. Tools may not be able to correctly recover fragmented files; the testing will show how the tool handles the fragmentation. Recovered data must be verified in an operational context, meaning, the examiner must examine relevant files to see if they are consistent since tools can combine fragments from different files. This testing will not show the limits of the tool's capabilities but will establish that it can perform the core function.
- **Frequency**: Before the tool is placed in service and after major update or revision.
- **Tester**: Lab, CFTT or other 3rd party if the same major version.

5.3.3 Aggregation and Summary

These tools collect data from scattered sources to provide an overall picture of some subset of user or system activity. These tools let an examiner look for patterns of system activity. Typical examples are tools that construct a timeline of selected system events or tools that examine system logs to create graphs of connections (contacts, emails, messages).

- **Testing Type**: These tools must be tested with either a known dataset or by comparison or by manually verifying a subset of the results.
- **Frequency**: Before the tool is placed in service and after major update or revision.
- **Tester**: Lab, CFTT or other 3rd party if the same major version

5.4 Multimedia Tools

This category includes technology used on imagery, audio, and video files. This could include tools for both analog and digital formats.

5.4.1 Viewers/Players:

Many types of viewers are used to display photos, play audio and video or otherwise make data human comprehensible. Note: Tools such as Adobe Photoshop can be both a viewer and an enhancement tool.

- **Testing type**: Empirical testing is sufficient for viewers/players. If the file can be opened and appears to playback properly (e.g., playback speed, aspect ratio that renders objects realistically, and internally consistent timeline), no other testing is required to support using the viewer/player to present multimedia files as evidence. It is acceptable to use multiple players or codecs to find one that can open/view the file correctly. If a file does not playback properly, then comparison or known dataset testing must be used.
  The forensic analyst should be aware that not all viewers can successfully read/ingest all files and that playback may be incomplete or degraded (e.g., dropped frames, jpegs reassembled partially).
  Audio/video playback software may rely on a forensic workstation's operating system, driver architectures, and drivers to deliver a sensory payload (the audio or video). Testing of this software can only be done in the context of the particular installation.
  Known data testing and comparison testing can be used to show player/viewer support for various characteristics of multimedia files. These tests are useful for selecting the best tool and further understanding tool capability. Characteristics include:
  - Video interlacing
  - Pixel aspect ratio
  - Number and types of streams
  - Metadata reporting (e.g., stream and file header discrepancies)
  - Undocumented re-sampling

  If the player/viewer is used to derive measurements (e.g., determining class characteristics such as size or color), then relevant calibrations must be performed.
- **Frequency**: At time of use.
- **Tester**: Lab, vendor.

5.4.2 Multimedia Transcoding

Transcoding is used to preserve files or to allow for further processing that requires a specific format. Screen capturing, which is the process of recording data such as imagery, video sequence, or audio stream from a playback software or device, is a type of transcoding. This is different than making a direct copy of the file.

- **Testing type**: Transcoders can be tested empirically. If the resulting file can be opened and is perceptually transparent (no loss of significant details), no other testing is required. It is acceptable to try multiple transcoders to find one that can create a file that can be opened/viewed without a loss of perceptual transparency. If a file cannot be played/viewed with perceptual transparency, as may occur if one started with a proprietary or unusual format, then known dataset or comparison testing must be used. Known data testing and comparison testing can be used to show transcoder limitations. These tests are useful for selecting the best tool. Characteristics include:
    - Support for needed export formats
    - Preserving original content including metadata and multiple streams
    - Undocumented filters
- **Frequency**: At time of use.
- **Tester**: Lab, vendor.

5.4.3 Imagery/Video/Audio Enhancement

These are tools used to improve the sensory perception of multimedia for the purpose of increased intelligibility, attenuation of noise, and facilitate understanding.

- **Testing type**: Enhancement tools must be tested with a known dataset to determine core operational capabilities. While these tests are not comprehensive, they test the basic functioning of the tool. A lab can add additional capabilities. Capabilities that must be tested with a known dataset (if used by the lab) include:
    - Removal of distortions and noise. Dataset must include a file with the distortions and noises experienced by the lab. Results are evaluated based on tester judgment on the utility of the output and that the tool did not affect a part of the signal that should not have been affected.
    - Enhancement of relevant aural (e.g., speech) or visual element (e.g., faces, fingerprints, license plates). Dataset must include a file with the types of enhancement experienced by the lab. Results are evaluated based on tester judgment on the utility of the output and that the tool did not affect a part of the signal that should not have been affected.

  Tools may be tested to document what changes occur when opening files in that tool when relevant (e.g., to support authenticity determinations).
- **Frequency**: When placed in service and major revisions.
- **Tester**: Lab or 3rd Party. Testing should be confirmed at the lab since enhancement tools are often dependent on the underlying workstation.

5.4.4 Signal Processors and Editors

These tools are used to transform information in an audio, video, or image file by use of filters in order to remove or emphasize a particular component of the signal. They can also be used to measure, count, and display features of the signal. Editors can rearrange, add, or delete sections of a video, audio, or image file. They can also include processing and transcoding functions. These tools need to be tested in order to understand and document what changes occur when opening and processing files with each tool.

- **Testing Type**: If the signal processor and editor are used for edit detection, this must be tested with a known dataset that includes a changed file. The dataset should include file types seen in the lab. Signal analysis must be tested with a known dataset. For other types of signal processing empirical testing is sufficient.
- **Frequency**: When placed in service, major revisions of the tool or underlying workstation, and when a new multimedia format is being captured.
- **Tester:** Lab.

5.4.5 Analog Audio Capture

While most multimedia encountered is processed digitally, there are still cases that use analog media and transmission systems. These tools include playback devices such as video cassette recorders, amps, headphones, speakers, and other analog equipment.

- **Testing type**: Analog audio equipment must be tested empirically before it is used with original evidence.
  It should also be tested using SWGDE Audio Best Practices Section 6.3 (link).
- **Frequency**: When placed in service and, since this equipment may be used infrequently, before capturing evidence.
- **Tester:** Lab.

5.4.6 Analog Video Capture

While most multimedia encountered is processed digitally, there are still cases that use analog media and transmission systems. These tools include playback devices such as video cassette recorders, amps, headphones, speakers, and other analog equipment.

- **Testing type:** Analog video equipment must be tested with a known dataset consisting of an audible tone, frame counter, and color bars. See *SWGIT Section 7, Best Practices for Forensic Video Analysis*.
- **Frequency:** When placed in service and, since this equipment may be used infrequently, before capturing evidence.
- **Tester:** Lab.

5.5 Administrative and Auxiliary tools.

These may be used to manage the investigation, document the investigation, and export relevant material. This includes word processors, case management software and other systems. Applications that are used to open files (e.g., using a financial program or flight simulator program to open files created by that program) are also considered administrative applications.

- **Testing type:** No testing is required beyond vendor testing.

5.6 In-house developed tools.

Tools and techniques developed in house that can influence the results of the examination should be tested by another person or entity competent in the underlying technology. It is not always clear what tools or techniques should be tested. Simple scripts or queries typically do not require this testing. In general, the following situations are indicators of a need for this testing:

- The tool or technique is complex enough that the examiner's notes are not sufficient to recreate the tool or technique
- The code is too large to be included in examiner's notes
- The results cannot be manually verified
- The code is compiled or the source code is not readily available

It is acceptable to have in house testing, but it is recommended that the tester be independent of the developer for more critical tools or situations.

Testing should include using a relevant known dataset (if applicable for the technology being tested). If possible, the tester should use a different dataset than was used to develop the tool.

- **Frequency**: At first use and all tool revisions
- **Tester**: Lab or independent organization

6. Documentation of Testing Results (new header)

Results of lab-based testing should be documented. Testing documentation should include:

- Purpose and scope of testing (identify tool or technique)
- Who performed the testing
- Date
- Testing procedure used or scenarios
- Datasets or other testing material used, including expected results
- Results and a description of anomalies and their significance
- Identified limitations

Documentation of 3rd party testing should refer to the test report. Vendor testing documentation will not generally be available.

7. References

[1] Scientific Working Group on Digital Evidence, "SWGDE Digital & Multimedia Evidence Glossary," 2016. [Online]. https://www.swgde.org/documents

[2] National Institute of Standards and Technology. (2018, February) Computer Forensics Tool Testing Program. [Online]. https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt

[3] *Standard Terminology for Digital and Multimedia Evidence Examination*, ASTM Standard E2916 - 13.

[4] *IEEE Standard for System, Software, and Hardware Verification and Validation*, IEEE Standard 1012-2016.

[5] Joint Committee for Guides in Metrology, "International Vocabulary of Metrology – Basic and General Concepts and Associated Terms (VIM)," BIPM, IEC, IFCC, ILAC, ISO, IUPAC, IUPAP and OIML, 200:2012. [Online]. https://www.bipm.org/en/publications/guides/vim.html

APPENDIX A

Types of Testing

There are several testing strategies that are particularly useful for testing tools and techniques used in labs. These are described below.

1. Testing with a Known Dataset

A known dataset test provides the tool being tested with known input and examines the output to see if it matches or correctly processes the input. Creating known datasets can be difficult depending on the type of test. There needs to be sufficient knowledge of the input to evaluate the output and there needs to be sufficient material in the dataset to create a valuable test.

Datasets may be real world or lab created. While it may appear that real world datasets would produce better testing, this is not necessarily true. Lab created datasets can be targeted at the parameters most important to the functionality being tested. Unless speed is a critical part of a test, real world datasets may not provide any additional confidence in the results.

2. Comparison Testing

A comparison test uses at least two tools in order to determine if both (or all) tools get consistent results.

Comparison testing can also be performed using a known dataset and can be quite valuable to gain confidence in a tool. There are also times when it is infeasible or even impossible to create a known dataset. In this situation, comparison testing may be the best available testing. This testing may not catch as many types of errors as known dataset testing.

3. Empirical Testing

Empirical testing is based on ascertaining whether the tool output is correct by examining the tool’s output or performance. In empirical testing, tool outputs are corroborated with other data, e.g., does the output match expected data type or can it be manually verified. The type of corroboration is based on criteria that are relevant to the type of tool. For example, a password cracker that provides a password which opens a file has shown it is capable of obtaining the expected results.

APPENDIX B

Sources of Test Reports

A significant factor in tool and technique testing is who performs the test. Testing can be performed by the lab, but also by other organizations, notably vendors and 3rd party testers including the NIST Computer Forensics Tool Testing program. Other laboratories also provide test reports. Using test reports from other organizations can be efficient. The NIST Federated Testing program is designed to allow labs to use NIST-developed tests. Labs can also share their test reports, especially if there are significant findings, to benefit the entire forensics community.

1. CFTT Testing including Federated Testing

The Department of Homeland Security Science & Technology Directorate publishes reports from the National Institute of Standards & Technology's (NIST's) Computer Forensic Tool Testing (CFTT) program. NIST has made available testing software that can be used by forensic labs and vendors to test products and will be hosting shared test reports. As of March 23, 2018, Federated Testing is only available for disk imaging, write blocking and mobile device acquisition. Federating Testing will be available for string searching and disk wiping in the near future. New functionalities are being added. See www.cftt.nist.gov.

2. Other 3rd Party Testing

The Department of Defense Cyber Crime Center publishes test reports at dc3.mil. These are available for users from government domains. Other sources of testing can include other labs who share test reports.

3. Vendor Testing

Most vendors test their products prior to release. Commercial and enterprise-level custom forensic tools are often extensively tested for forensic application. Many vendors provide forums to discuss tool anomalies and upgrades made to the tools. There are also forums to discuss general purpose tools used in forensics.

SWGDE Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics
History

Revision	Issue Date	Section	History
1.0 DRAFT	2018-06-14	All	Initial draft created and voted by SWGDE for release as a Draft for Public Comment.
1.0 DRAFT	2018-07-09	--	Formatting and technical edit performed for release as a Draft for Public Comment.
1.0	2018-09-20	--	No changes were made following the Public Comment period. SWGDE voted to publish as an Approved document.
1.0	2018-11-20	--	Formatted and published as Approved version 1.0.