



Scientific Working Group on Digital Evidence

Minimum Requirements for Testing Tools Used in Digital and Multimedia Forensics

18-Q-001-2.1

Disclaimer and Conditions Regarding Use of SWGDE Documents

SWGDE documents are developed by a consensus process that involves the best efforts of relevant subject matter experts, organizations, and input from other stakeholders to publish suggested best practices, practical guidance, technical positions, and educational information in the discipline of digital and multimedia forensics and related fields. No warranty or other representation as to SWGDE work product is made or intended.

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 such proceeding. The notification should 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; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in the proceeding please notify SWGDE as to the outcome of the matter. Notifications should be submitted via the SWGDE Notice of Use/Redistribution Form or sent to secretary@swgde.org.

From time to time, SWGDE documents may be revised, updated, or sunsetted. Readers are advised to verify on the SWGDE website (<https://www.swgde.org>) they are utilizing the current version of this document. Prior versions of SWGDE documents are archived and available on the SWGDE website.

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 this SWGDE cover page containing the Disclaimer and Conditions of Use.
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 creation date) of the document and also indicate 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 submitted via the [SWGDE Request for Modification Form](#) or forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of any suggested modification:

- a) Submitter's name
- b) Affiliation (agency/organization)



Scientific Working Group on Digital Evidence

- c) Address
- d) Telephone number and email address
- e) SWGDE 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 suggested modification

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.

This project was supported by Grant # 15PJDP-21-GK-03271-MECP awarded by the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication/program/exhibition are those of the author(s) and do not necessarily reflect those of the Department of Justice.



Scientific Working Group on Digital Evidence

Minimum Requirements for Testing Tools Used in Digital and Multimedia Forensics

Table of Contents

1. Purpose.....	2
2. Scope.....	2
3. Limitations.....	2
4. General Discussion.....	3
5. Categories of Tools and Baseline Recommendations for Testing.....	4
5.1 Critical Forensic Tools	4
5.2 Underlying Systems/OS.....	9
5.3 Forensic Analysis Tools	10
5.4 Multimedia Tools	11
5.5 Administrative and Auxiliary Tools.....	14
5.6 In-house Developed Tools.....	14
6. Documentation of Testing Results.....	14
7. References.....	15
APPENDIX A.....	16
APPENDIX B	17
History.....	18



Scientific Working Group on Digital Evidence

1. Purpose

The purpose of the document is to recommend baseline testing requirements for commonly used forensic tools and procedures. Organizations may exceed these baseline requirements based on how tools are used as well as operational needs and organizational 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 baseline guidelines be conducted 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, software used for interpretive purposes, or whether personnel are adequately trained to use a tool.



Scientific Working Group on Digital Evidence

4. General Discussion

The purpose of testing is to establish confidence that a tool or procedure performs correctly, thereby reducing the risk of errors or misinterpretation of data. 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 assess the risk of not conducting extensive testing and balance the confidence gained by the level and frequency of testing with the resources required 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, risk considerations, or errors that may not be considered to impact the overall output of results.

There are many techniques and strategies for testing forensic tools. Each technique or strategy has different strengths, weaknesses, and risks which must be considered when developing a testing policy. There is inherent risk in any process that may be introduced by human error, process error, or device/software error. The risk level may be associated with frequency of test. The organization must assess their level of risk tolerance based upon the reliability and the outcome of testing history of tools used to support forensic services.

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.

Organizations might consider using existing tool testing programs that have been designed to simplify the testing process, (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.

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.



Scientific Working Group on Digital Evidence

5. Categories of Tools and Baseline Recommendations for Testing

Organizations use a variety of tools and techniques. This section defines different testing requirements and strategies based on the 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 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 should 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 tools.

- **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 software or firmware update or revision is applied.
- **Tester:** Lab. There are automated 3rd party organization testing tools, e.g., CRU WriteBlocking Validation Utility and CFTT Federated Testing that provide in-depth testing.



Scientific Working Group on Digital Evidence

5.1.1.2 Radio Isolation

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

RF Isolation is used when the device is being transported or stored. There are three primary methods used: shielded containers, placing the device in airplane mode, and SIM cloning. Note: Placing a device in airplane mode generally does not disable Bluetooth or Wi-Fi.

5.1.1.2.1 *Shielded Containers/Faraday Cages*

Shielding containers designed to block RF signals are not always 100% effective due to components degrading over time. 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 mobile device, an examiner must place the mobile device 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 a mobile device 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 routinely due to the potential for degradation of the shielding components which may be accelerated due to interaction with the environment. High-use items, such as Faraday boxes, should be tested more frequently.
- **Tester:** Person performing the seizure, analysis, or storage.

5.1.1.2.2 *Subscriber Identity Module (SIM) Cloning*

SIM cloning is a process for isolating Global System for Mobile Communication (GSM) phones from the cellular network by creating a SIM card without network connectivity. Universal Integrated Circuit Card (UICC) is the new generation of SIM card, which contains phone number and account information for mobile devices.

- **Testing type:** SIM cloning is tested by verifying that the clone contains the proper values for the International Mobile Subscriber Identity (IMSI) and Integrated Circuit Card Identification Number (ICCID). This will verify that the GSM phones cannot connect to the network.
- **Frequency:** Prior to first use and after SIM cloning software is updated
- **Tester:** Lab.

5.1.2 Acquisition Tools

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

Minimum Requirements for Testing Tools Used in Digital and Multimedia Forensics

18-Q-001-2.1

Version: 2.1 (March 7, 2024)

This document includes a cover page with the SWGDE disclaimer.

Page 5 of 18



Scientific Working Group on Digital Evidence

5.1.2.1 Disk Imagers

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

- **Testing type:** 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.)
 - ☐ Be aware of tool limitations (e.g., large sector devices).
 - ☐ Verify the imager was able to acquire the entire media or targeted portion of the media (e.g., partitions, directories, files).
 - ☐ Include the media types regularly encountered by the lab.
 - ☐ Verify the known dataset was acquired correctly or document and understand any anomalies.
 - ☐ 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, SHA256) 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. Various tools utilize multiple updates that may not include updating the imager. If the release notes for a minor update say the imager is affected, it should 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.



Scientific Working Group on Digital Evidence

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, social media). The dataset should be representative of common data types that may typically be encountered. Testing does not need to include all device types and all variations of different operating systems. It is acceptable to use seized devices 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 generally considered sufficient to test the major software version releases once; for hardware, testing needs to be performed on each unit.
- **Tester:** Lab, CFTT, or other 3rd party organization 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.

Minimum Requirements for Testing Tools Used in Digital and Multimedia Forensics

18-Q-001-2.1

Version: 2.1 (March 7, 2024)

This document includes a cover page with the SWGDE disclaimer.

Page 7 of 18



Scientific Working Group on Digital Evidence

- **Tester:** Lab, 3rd party organization.

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 RAID, servers, 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 organization 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 between files 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 organization if the same major version.



Scientific Working Group on Digital Evidence

5.1.4 Wiping Tools

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

- **Testing type:** Wiping tools 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 organization if the same major version.

5.2 Underlying Systems/OS

Many forensic tools run on a standard operating system, such as Windows, Mac OS X or Linux. This class of systems 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.



Scientific Working Group on Digital Evidence

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 organization 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 should 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 organization if the same major version.



Scientific Working Group on Digital Evidence

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 organization 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: Image processing tools 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. 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).

The operating system version and workstation configurations may impact the ability to properly playback the file. Known data testing and comparing the output of different tools may 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., use a tool that can look at the binary)
- ☐ Undocumented re-sampling (e.g., interpolation)
- ☐ Decoding artifacts

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.

Minimum Requirements for Testing Tools Used in Digital and Multimedia Forensics

18-Q-001-2.1

Version: 2.1 (March 7, 2024)

This document includes a cover page with the SWGDE disclaimer.

Page 11 of 18



Scientific Working Group on Digital Evidence

5.4.2 Multimedia Transcoding

Transcoding is used to allow for further processing that requires a specific format or to preserve files. 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 from making a direct copy of the file.

- **Testing type:** Transcoders can be tested empirically. (See also Bruehs, WE, Stout, D. Evaluating digital video transcoding for forensic derivative results. J Forensic Sci. 2023; 68: 1036–1048. <https://doi.org/10.1111/1556-4029.15245>). 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. Known data testing and comparing the outputs of multiple tools 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 (if being used by the lab) that must be tested with a known dataset include:
 - ☐ Removal of distortions and noise. Datasets must include a file with the distortions and noises commonly encountered by the lab. Results are subjectively 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 commonly performed 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. *(It should be noted that it is not advisable for the practitioner to provide an interpretation of the enhanced results, i.e., what the characters on the license plate are, or what the speaker said.)*

Tools should 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 organization. Testing should be confirmed at the lab since enhancement tools are often dependent on the underlying workstation.

Minimum Requirements for Testing Tools Used in Digital and Multimedia Forensics

18-Q-001-2.1

Version: 2.1 (March 7, 2024)

This document includes a cover page with the SWGDE disclaimer.

Page 12 of 18



Scientific Working Group on Digital Evidence

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. Non-linear 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. Further information is available in 2022-06-09 SWGDE Best Practices for Forensic Audio (or subsequent versions).
- **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.



Scientific Working Group on Digital Evidence

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.

Testing for large or complex software packages, formal testing with requirements, a test methodology, and published results may be appropriate.

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

6. Documentation of Testing Results

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 organization testing should include a reference to the test report or results. Vendor testing documentation will not generally be available.



Scientific Working Group on Digital Evidence

7. References

- [1] Guidelines for Data Set Development, OSAC, Digital Evidence, Oct22
- [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 (current version).
- [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>



Scientific Working Group on Digital Evidence

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, such as when even independently developed tools have the same underlying problem.

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.



Scientific Working Group on Digital Evidence

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.



Scientific Working Group on Digital Evidence

History

Revision	Issue Date	History
1.0 DRAFT	6/14/2018	Initial draft created and voted by SWGDE for release as a Draft for Public Comment.
1.0 DRAFT	7/9/2018	Formatting and technical edit performed for release as a Draft for Public Comment.
1.0	9/20/2018	No changes were made following the Public Comment period. SWGDE voted to publish as an Approved document.
1.0	11/20/2018	Formatted and published as Approved version 1.0.
2.0 DRAFT	9/21/2023	Completed document update/content revisions and moved forward for SWGDE membership vote to release as a Draft for Public Comment.
2.0 DRAFT	10/15/2023	SWGDE voted to release as a Draft for Public Comment; formatted for release for public comment.
2.1	1/23/2024	Revised document in response to public comments received. Moved forward for SWGDE membership vote to release as a final approved document.
2.1	3/7/2024	Formatted for posting after SWGDE membership voted to release as a Final Publication.