SWGDE Collection of Digital and Multimedia Evidence Myths vs Facts

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 Collection of Digital and Multimedia Evidence Myths vs Facts

MYTH: ***"Files that do not have a hash calculated when collected cannot be authenticated."***

FACT: Hashing a file alone is a robust method of confirming file integrity, but digital files without an accompanying hash checksum can be authenticated in other ways. Authentication of a digital file for purposes of digital forensics may be different from authentication required by rules governing admission of evidence in a judicial proceeding.

MYTH: ***"Digital forensic examiners are able to have all available forensic tools on-site to conduct all types of digital forensic analysis."***

FACT: Many forensic analysis processes require advanced tools that are not easily portable. Advanced password cracking tools run on high-powered, large desktop computers or even require a network of large, high-powered computers. Other forensic tools, such as chip-off equipment, are not created to be moved from their permanent location. Additionally, the evidence scene often presents conditions and challenges that are out of the control of personnel. Good scientific techniques, as well as the prudent desire to minimize avoidable negative impact, dictate to eliminate adverse conditions that are in one's control at the scene by moving items to a controlled environment, if possible. This is no different from what happens every day in normal crime scene investigations. Some analyses on evidence that could be done at the scene are conducted at the laboratory to which the evidence is taken.

MYTH: ***"Users cannot edit EXIF or metadata from digital cameras and or images."***

FACT: EXIF and metadata can be deleted or can be edited. Metadata also can drop out altogether during transmission, transfer, or format changes.

MYTH: ***"All data for a company or individual is located at the same physical location as the company or individual."***

FACT: Data accessible from local digital devices may be physically located at another physical location and accessed via the Internet. The local user may not even know where the data is stored. The local IT department may "map" a network location to a local drive letter.

MYTH: ***"All data viewable on a digital device is stored locally on that digital device."***

FACT: Some data accessible on digital devices is stored in "the cloud" and may not be located on the physical device. For example, data seemingly in the Dropbox app on an iPhone is accessible when the device is connected to the Internet. If the device is removed from all data networks, the data is no longer accessible. The files are actually stored in "the cloud" on the Dropbox servers and not on the phone unless the user specifically configures the app to download the data to the physical device.

MYTH: ***"All hard drives can be imaged at the same speed."***

FACT: There are many variables that impact the speed at which a hard drive can be imaged. Some common variables include, the imaging tool used, the speed of the hard drive, presence or absence of bad sectors on the hard drive, and the type of drive connection. Most of these variables cannot be controlled by the examiner. For example, imaging the same 64 GB SATA SSD with one software tool took 36 minutes, a different tool took 33 minutes for the same drive and a hardware imager took 6 minutes.

MYTH: ***"A 'duplicate original' is a myth."***

FACT: If a copy of the original data has the same hash value, that copy can be considered a "duplicate original" and is identical to the original. A hash value can be calculated on a file or any other set of data. A hash value is a mathematical algorithm that generates a hexadecimal output value (alpha-numeric text string). Any change in the data will produce a change in the resulting hash value. Essentially, the hash value of data can be considered the "fingerprint" of the data. Two common hash algorithms currently in use are MD5 and SHA. The use of these algorithms to support "duplicate originals" is described in "Unique File Identification in the NSRL" available at http://www.nsrl.nist.gov/Technical_papers.htm.

MYTH: ***"All data on a computer can be viewed using the 'My Computer' screen."***

FACT: "My Computer" and "File Explorer" are graphical interfaces that are programmed to show normal files on a device. There are several ways around having data displayed in these applications. Folders and files can easily be hidden from the interface by selecting a particular attribute. Additionally, user accounts can be setup conceal any portion of data. While these interfaces also show known file types, unconventional file types or formats will pose problems for a standard interface to display. Locations that are designed for operating system information are programmatically ignored by this type of interface. This occurs, by design, for the standard non-technical user.

MYTH: ***"A digital forensic examiner can conduct a proper and thorough forensic exam only using keyword searches."***

FACT: It is not possible to create, prior to an examination, a comprehensive list of relevant keywords that will identify all relevant digital evidence.

MYTH: ***"Qualifying a witness as an expert in digital forensics means the witness is an expert in computers."***

FACT: The act of endorsing a witness as an expert is a legal designation intended to benefit the trier of fact. There are many facets to the definition of "expert witness." The witness may have little control over the adjective used in conjunction with "expert" and the specific term chosen by a non-technical court officer (e.g., attorney) does not necessarily dictate what that witness knows or is willing to present. Further, the specific terms "digital forensics" or "computer forensics" may imply to the non-technical person that they mean an expertise in all things dealing with computers. However, these terms actually refer to a sub-discipline of digital and multimedia forensics that involves the scientific examination, analysis, and/or evaluation of digital/multimedia evidence in matters of possible legal consequence. (See Federal Rules of Evidence 702 or similar state provisions)

MYTH: ***"It is possible to compile an all-encompassing list of forensic myths."***

FACT: With ever-constant developments in technology and continuous updating of software, it does not seem feasible that a list of forensic myths could ever be deemed all-encompassing and fully current. Layman human sensory perception and intuition about technology as well as purportedly accurate Internet websites frequently bring inaccurate or illusory understandings of what is actually going on in technology, how technology operates, and what is involved in continually evolving digital forensics processes.

MYTH: ***"Forensic analysis involves a digital investigative analyst looking at every file on the digital device."***

FACT: There is no such thing as a "full and complete" forensic analysis. Computers can and often do contain millions of files and databases that contain even more entries. Forensic tools, such as specially written software, are utilized to assist an examiner in finding data that meets criteria or characteristics specified by the examiner. In that process, the software does not display data that does not meet the defined criteria or characteristics.

MYTH: ***"Once a forensic analysis is conducted, every item of significance to a case has been identified."***

FACT: A digital/multimedia evidence examination can be an evolving processes. As investigative values come to light, either directly from the exam or from another source, different items can become relevant and need to be searched, interpreted, extracted, and reported. For example, a physical image is extracted from a seized cell phone pursuant to a search warrant. As requested in the warrant, the examiner reports on all call logs. Later, an investigator identifies contact with a collaborative witness but does not find in the report any further information regarding the witness. An additional warrant is secured if necessary and the examiner is provided the name of the witness and requested to find any other information. The examiner performs searches in unallocated space and recovers fragments of deleted emails from the collaborative witness.

MYTH: ***"There should never be a second analysis conducted because of the potential for conflicting forensics reports."***

FACT: If the first forensic analysis is properly conducted and reported, any subsequent analysis should not ever result in a report that truly contradicts the first report, as far as factual findings are concerned. Opinions, if any, may vary in different reports. It may be that a subsequent examination resulted in finding additional data not found during a prior examination because the information found during the earlier examination seemed to satisfy the requirements of the request at that time. Additionally, the prior examination may have been suspended or terminated prior to completion, pending further request.

MYTH: ***"Because digital images can be manipulated, they should not be admissible."***

FACT: The integrity of digital images can be assured. There are methods that demonstrate digital file integrity including hashing functions, visual verification, digital signatures, written documentation, and checksums/cyclical redundancy checks. Additionally, experts may be capable of determining whether a digital image, film photograph, or film negative has been altered. When evidence is produced suggesting an alteration, experts can be used in an attempt to confirm or refute the assertion.

MYTH: ***"Digitally enhanced images should not be admissible."***

FACT: Digitally enhanced images that reveal features that exist in the image but are not immediately apparent through visual examination have historically been found to be valid and admissible evidence in courtroom proceedings. Case law generally supports the admissibility of digitally enhanced images. It may be required that detailed explanation of the enhancement process first be provided. Frye and Daubert challenges to the use of this technology generally have been resolved in favor of admission of digitally enhanced images. A digital image or film photograph that has been altered or enhanced, which produces an output that does not accurately and fairly depict what was captured, does present admissibility issues. For example, if a blue car is the subject of a photograph and the image is changed to make the car appear red, such an image would certainly be subject to objection absent further explanation. On the other hand, an image that has been enhanced to reveal a fingerprint on a patterned background by removing the background pattern may be admissible because the nature of what the image depicts (a fingerprint) has not been changed. In this respect, it may prove helpful to recall that under rules of evidence an "original" of the data (which is what is created when a digital photograph is captured) is not restricted to the data itself, but "any printout or output readable by sight, shown to reflect the data accurately." [Federal Rule of Evidence 1001(3)]

MYTH: ***"When images are digitally enhanced, they must be reproducible, and these reproductions must be 'bit-for-bit' copies of each other."***

FACT: Digitally-enhanced images must be reproducible; however, when images are enhanced the bit values change. Two persons using the same techniques, producing images visually indistinguishable from each other, will get different bit values. This is an expected and normal occurrence that should not affect the admissibility of the image. Reproducibility is judged by obtaining visually comparable results, not identical bit values.

MYTH: ***"Localized adjustments such as dodge and burn should never be used in the digital enhancement of images."***

FACT: Localized adjustments are appropriate under many circumstances. The dodge and burn technique is one that has its roots in traditional darkroom technology. When the technique is applied appropriately, it can greatly improve the visibility and usefulness of evidence. This processing technique should be documented by the practitioner.

MYTH: ***"Digital enhancement of a fingerprint image can accidentally morph the fingerprint of one person into that of another."***

FACT: When digital image enhancement is performed according to accepted guidelines and standards, it is not possible to change one person's fingerprint into another's. The end result of properly enhancing any image is an increase in the visibility of characteristics of interest within the image. Research completed at Indiana University Purdue University Indianapolis (IUPUI), Mathematical Sciences Department, found that the possibility of such an occurrence to be one in 10 to the 80^{th} power (i.e., 1 followed by 80 zeroes). This number is approximately equal to the number of atoms in the universe.

MYTH: ***"All digital images must be electronically authenticated to be admissible."***

FACT: A digital image, as well as a film photograph, can be authenticated through testimony or other evidence that the image is a fair and accurate representation of what it purports to depict; electronic authentication is not required. Image integrity must not be confused with the requirement to authenticate evidence as a precondition for admissibility in court. Courtroom authentication of an image substantiates that the image is a fair and accurate representation of what it purports to be, whereas integrity verification is the process of confirming that the image presented is complete and unaltered since the time of acquisition. The integrity of digital images can be verified through a number of means, some of which are not electronic.

MYTH: ***"Image files should be left on the camera's removable flash media and the flash media must be available in court as a condition precedent to admissibility of the image."***

FACT: Most removable flash media is designed as temporary storage. Flash media cards that are stored for long periods of time are prone to data corruption that leads to loss of images. Excessive heat or cold, shock, and other improper handling and storage techniques can all put flash media at peril of losing data.

MYTH: ***"Any copy (duplicate) of a digital image made from the camera's media is not an original."***

FACT: When the contents of a camera's media is copied to a hard drive, CD, or DVD by a method that accurately reproduces the data on the camera's media, a duplicate of that data is created. See Federal Rule of Evidence 1001 (4).
Furthermore, "A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original." [Federal Rule of Evidence 1003] This legal result is the same as what has happened digitally; the process of correctly copying the data from the camera's media to another media creates identical data. Copying the data from one media to another is analogous to producing multiple original prints from a negative.

MYTH: ***"Compression of digital images or video is always bad."***

FACT: Compression can be appropriate depending on the intended use of the image or video. Compression should be used with care to avoid material degradation of the image. The use of compression, if over applied, can degrade the quality of the image, but it does not change the subject of the image into a different one.

MYTH: ***"Compressed images, such as those captured in JPEG format, are not suitable for comparative or analytical purposes."***

FACT: It is preferable to capture images that are intended for comparative or analytical purposes using uncompressed formats; however, lossy compressed formats like JPEG may be used if the examiner determines sufficient detail is present in the image for such analysis.

MYTH: ***"All digital images must be treated as evidence and tracked with a chain of custody."***

FACT: Many digital images do not require a chain of custody. Whether a chain of custody is established for a digital file is determined by the reason for which the file has been created or is being maintained and will vary between jurisdictions. For example, seized evidence almost always requires a chain of custody. Images produced or enhanced in a laboratory setting do not always require a chain of custody.

MYTH: ***"All digital imaging equipment must be calibrated to be used in a forensic setting."***

FACT: The requirement for calibration of equipment is determined by individual agencies and manufacturers, based on the type of equipment and their function. The need for calibration generally exists in equipment that performs quantitative or numerical analysis. When required, visual comparison of digital images can suffice as a type of calibration of digital imaging equipment.

MYTH: ***"An expert is required to lay a foundation for any digital images introduced in court."***

FACT: When images that have been subjected to processing to reveal information are being offered in court, a subject matter expert will usually be required to explain the process used. On the other hand, when traditional darkroom type adjustments are applied these are easily understood without the need for an expert. For example, enlarging or brightening an image.

MYTH: ***"Watermarking does not change the original image."***

FACT: Watermarking is a potentially irreversible process of embedding information into a digital signal. It modifies the content of the files and can persist as a part of the file. This process may change the image content as it was originally captured by the camera. Watermarking may occur at the time of recording, at the time the video or images are exported from the system, or during post-processing. Watermarking, as a forensic technique, is not recommended.

MYTH: ***"Images should never have their metadata modified or removed as this will invalidate them for forensic use."***

FACT: While it is best practice to maintain digital image files in an unaltered state from time of capture, separation of image content from metadata may not necessarily invalidate them for forensic use. In the majority of cases, the visual interpretation of an image is not affected by conditions of capture reflected in the metadata. In some cases, the presence of metadata is necessary for the analysis of the image.

MYTH: ***"Digital recordings are always better than analog recordings."***

FACT: The fact that a recording is digital or analog is not a factor for quality. Digital factors include the sample rate and bit depth a recording is made at as well as the compression ratio if compressed while Analog factors include tape speed and equipment calibration. Most important in either case, however, is the microphone placement and proximity of the sound source as well as the environment where the recording is made. If these factors are not addressed or inadequate, any recording, digital or analog, will suffer.

MYTH: ***"Compressed multimedia evidence is the best method of sharing and archiving because of reduced space."***

FACT: Lossy Compression of multimedia is achieved by removing data that cannot be recovered. Therefore, all multimedia evidence should be archived and shared as uncompressed (as reasonable).

MYTH: ***"All audio playback is equal."***

FACT: Built in computer speakers are not designed for optimal playback. The same can be said for earbuds and many headphones. High quality speakers and headphones should be used for audio playback (in the lab and in the courtroom) whenever possible.

MYTH: ***"Cell phone extraction tools accurately get and show everything on a phone."***

FACT: There are multiple steps in the forensic examination of a cell phone. Depending on the functionalities of the particular forensic tool(s) used in an examination, the training and experience of the person conducting the examination, and the scope of legal authority, a physical image or a file system might be extracted, or simply a logical listing of objects (e.g., pictures, SMS messages) could be generated—assuming user pass codes or encryption do not interfere with the process. Once an extraction is complete, most forensic tools will parse, or put into a viewable format, much of the data retrieved from the phone. However, forensic tools rarely parse all data on a phone, and, the person conducting the examination should ensure steps have been taken (possibly including the use of additional forensic tools) to seek out additional user artifacts. It is also the responsibility of the person conducting the examination to be sure validated forensic tools are utilized to accurately extract and interpret data from the cell phone and to validate all findings.

SWGDE Collection of Digital and Multimedia Evidence Myths vs Facts

History

Revision	Issue Date	Section	History
Draft	02/20/2016	All	Initial draft created for internal SWGDE review.
1.0	06/09/2016	--	SWGDE voted to release as a Draft for Public Comment.
1.0	07/20/2016	All	Released as a Draft for Public Comment.
1.0	9/15/2016	Title All	Added “and Multimedia” after “Digital” in the title. Removed myth categories. Added myth "Once a forensic analysis is conducted, every item of significance to a case has been identified" and corresponding explanation. SWGDE voted to publish as an Approved document.
1.0	10/08/2016	All	Formatted and published as Approved version 1.0.
1.1	2017-01-12	Page 5	Added "See Federal Rules of Evidence 702 or similar state provisions" to the end of MYTH “Qualifying a witness as an expert in digital forensics means the witness is an expert in computers” for clarification. SWGDE voted to re-release as an Approved document (Version 1.1).
1.1	2017-02-21	Formatting	Formatted and published as Approved version 1.1.
1.2	2017-06-22	Page 11	Added myth “Cell phone extraction tools accurately get and show everything on a phone." SWGDE voted to publish as Approved.
1.2	2017-07-18	--	Published as Approved version 1.2.