Scientific Working Group on Digital Evidence

Best Practices for Personnel Presenting Digital Evidence in Legal Proceedings

23-Q-001-1.1

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)
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

Best Practices for Personnel Presenting Digital Evidence in Legal Proceedings

Table of Contents

1. Purpose

The purpose of this document is to describe best practices for the key knowledge, skills, and abilities investigators/digital forensic examiners need to present digital evidence in legal proceedings.

2. Scope

This document is a companion paper to 'Introduction to Testimony in Digital and Multimedia Forensics 22-Q-001-1.1' intended to expand on key topics, provide additional guidance, considerations, highlights key skills, knowledge, and preparation required to provide expert testimony in legal proceedings.

3. Limitations and Considerations

This document was prepared with the resources available at the time of publication. This document should not be construed as legal advice from an attorney.

4. General Considerations

The credibility of the investigator / digital forensic examiner must focus on the goals of truthfully establishing credibility, avoiding the fundamental problems of compromised scientific validity, mitigating risk of biases and error when an examiner exceeds the scope of their training and expertise or has been exposed to external pressures or considerations.

5. Legal, Ethical, & Character Considerations

A. Digital Forensics Defined

Digital forensics is the field of forensic science that is concerned with the collection, examination, analysis, and reporting of electronic data for use in criminal, civil, and administrative proceedings while preserving the integrity of the information and maintaining a strict chain of custody for the data.

The use of electronic data in legal proceedings rests with the premise that the process used to obtain the electronic data is designed to minimize alteration of data structures and is otherwise reproducible.

B. The Forensic Process

As set forth in *Digital Investigation Techniques: A NIST Scientific Foundation Review*, NIST IR 8354, there is no single technique that can be called "Digital Forensics." There are hundreds if not thousands of individual techniques that might be employed in a digital forensic examination. NISTIR 8354 finds that, overall, digital evidence examination rests on a firm foundation based in computer science. Electronic data extracted from a digital device should be admissible in court, provided the process comports with the Rules of Evidence within the respective jurisdiction where the testimony is sought.

C. Rules of Evidence

"Rules of Evidence" refers to the applicable set of procedural requirements for the introduction of evidence at a legal proceeding. Rules can vary considerably by jurisdiction (i.e. federal or state), type of proceeding (criminal, civil, administrative, grand jury or trial, jury or bench trial, as examples), type of evidence (physical, documentary, testimonial, demonstrative, etc.) and manner of introduction.

The Federal Rules of Evidence (1975, "FRE") codify the evidence law that applies in United States federal courts. Many states have adopted the FRE or a variation thereof as the rules in their jurisdiction; others have their own rules which are completely different from the FRE. Generally, for evidence to be admissible, a proper "foundation" must be laid by the offering party. A judge must be satisfied that the required foundation has been laid before issuing a ruling on the admissibility of a piece of evidence.

Federal Rule of Evidence 702 requires the following of expert testimony:

1. the proffered witness must be an expert, as qualified by specialized knowledge, skill, training, experience or education;
2. the expert must testify to scientific, technical or specialized knowledge; and
3. the expert's testimony must assist the trier of fact.

The overriding consideration with regard to these three factors is that expert testimony should be admitted if it will assist the trier of fact. In *General Electric Co. v. Joiner*, 522 U.S. 136 (1997), the Supreme Court clarified *Daubert*, holding that an appellate court may still review a trial court's decision to admit or exclude expert testimony. The standard of review for this inquiry is the "abuse of discretion" standard.

Witnesses should consult with the attorney calling them to determine which rules of evidence apply in the jurisdiction where they will testify, and how those rules could affect the questions being asked of them, or how evidence will be introduced in the proceeding. For further information relating to expert witnesses, see *SWGDE Introduction to Testimony in Digital and Multimedia Forensics*.

D. Applicability of the *Daubert* or *Frye* Standards

Courts use two standards for the admissibility of expert testimony, both of which are grounded in legal precedent. First, there is the *Frye* Standard, which is still in place in some jurisdictions, but has been largely replaced by the *Daubert* Standard. *Daubert* has been extended to cover technical experts through what is known as the *Kumho Tire* case. As to the admissibility of expert testimony, each court is empowered with discretion to allow any testimony under Federal Rule of Evidence 702. If an investigator / forensic

examiner will be qualified as an expert witness, trial judges may rule on the admissibility of their testimony, in part or in whole, based upon the "Daubert" or "Frye" standards.

The older *Frye* standard, espoused in *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923), requires that the forensic methods employed and related expert testimony about it be "generally accepted within the relevant scientific community."

The *Frye* standard was used at the federal level until 1993 when the United States Supreme Court effectively overruled *Frye* in *Daubert v. Merrill Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).

Daubert held that the *Frye* standard was incompatible with Rule 702 of the Federal Rules of Evidence, which generally requires that expert testimony be (1) relevant and (2) reliable in order to be admissible. *Daubert* has more specific "illustrative factors" to be used by courts in determining the admissibility of scientific evidence and testimony: (1) whether the technique or theory in question can be and has been tested, (2) whether it has been subjected to peer review and publication, (3) its known or potential error rate, (4) the existence and maintenance of standards controlling its operation, and (5) whether it is generally accepted within the relevant scientific community. With some variations, most states have adopted the *Daubert* standard, with a minority of states continuing to use the older *Frye* standard.

The *Kumho Tire* case extends *Daubert* by allowing flexibility in the *Daubert* factors for testimony that may not fit within a traditional scientific discipline but otherwise encompass technical knowledge. In so holding, the Supreme Court, however, noted that the trial court would retain its "gatekeeping" function in assessing whether such testimony, based on technical knowledge, is sufficiently reliable such that it can be admitted at trial.[1]

The burden to establish either standard is on the party offering the expert testimony to satisfy *Daubert* or *Frye* by a preponderance of the evidence. Witnesses that will be qualified as experts should consult with the attorney calling them to determine which

[1] The Kumho Tire case came from Kumho Tire, Co. v. Carmichael, 526 U.S. 137 (1999). In the Kumho Tire case, attorneys for Carmichael called upon a tire failure analyst named Donald Carlson Jr. to determine if a fatal accident was caused by treatment of the tire beyond manufacturer specifications, or a manufacturing defect in said tire. The defense challenged this expert's testimony under the existing Daubert standard, as it could not meet those four criteria. Initially the trial court agreed. The Supreme Court, however, held that Daubert should be applied flexibly and that other factors could argue in favor of admissibility; and the trial court ultimately should serve as a "gatekeeper" to permit testimony that is sufficiently reliable within a particular scientific field or trade while excluding testimony that is based on non-reliable knowledge or experience. It is this extension that forms the basis of the admissibility of expert testimony which does not fall directly under a specific academic degree, accreditation, or certification.

standard applies in the jurisdiction where they will testify, and how the standard could affect the questions being asked of them.

Challenges to this admission can be the basis for appeal under review of an abuse of this discretion. The basis for this review was established in *General Electric Co. v. Joiner*, 522 U.S. 136 (1997).

E. Ethics

A digital forensics examiner must maintain integrity and remain objective when examining the data regardless of how it may impact the case for the party that has engaged them. A practitioner must also maintain confidentiality, not only of the engaging party but also to the data's custodian as the practitioner may encounter and observe sensitive information that falls outside of the scope of the investigation. A digital forensic examiner's competence, behavior, and due care is a representation not only of the individual but can be a reflection on the industry as a whole.

F. Character Considerations

An expert witness's mental, moral, political, and criminal history may be investigated and made public during the course of legal proceedings. Potential experts should consider their public stance, politics, arrest record, criminal background, and social media that may include behaviors of the witness. While professional history, training, and certification are used to recognize a witness in a litigation as an expert, an expert's character is often the vector of attack to have an expert, their findings or testimony disqualified.

In criminal cases, prior findings of incredibility or administrative discipline by an examiner called to testify also may require disclosure under *Giglio v. United States*, 405 U.S. 150 (1972).

G. Professional History

A practitioner's experience will be reviewed by the court when being considered for qualification as an expert witness. Often encapsulated in Curriculum Vitae or resume, the practitioner should be able to document their education, work history, training, certifications, professional organization affiliations, and any additional supporting qualifiers that demonstrate their specialized skills, experience, and expertise relevant to the subject matter.

Certain jurisdictions require a practitioner to disclose their professional history for a set period of time as well as a complete statement of their opinion, and any bases relied upon

thereto, prior to the testimony. Practitioners are encouraged to consult with legal counsel to become aware of the appropriate rules in their respective jurisdictions.

6. Courtroom Presentation

A. Neutrality

The digital forensic examiner enjoys an important position within the criminal, civil, and administrative justice system. Rather than advocating for a particular party, the digital forensic examiner must employ the use of best practices in maintaining the integrity of evidence during its collection, examination; and report only what the data represents in a clear and cogent manner after a thorough review and analysis of forensic evidence and any corroborating material. The examiner also should be mindful of any bias, unconscious or known, throughout the digital forensic process.

Even if paid by a party, the findings of a digital forensic examiner should be presented in an unbiased way, without omission, distortion or misrepresentation of any facts stemming from the forensic examination. Doing otherwise tarnishes not only the examiner, but also the field of forensic science.

B. Area of Expertise

The field of digital forensics encompasses a large universe of disciplines. It may be unreasonable for a practitioner to have sufficiently in-depth knowledge, education, experience and training to be a subject matter expert in multiple disciplines.

It is important to recognize that digital evidence is a dynamic landscape. Technology, software, tools, and methodologies are in constant change. It is important that practitioners keep current with methodologies and technologies, as well as their limitations. This can be achieved through continued education, training, participation in professional organization, knowledge transfer from affiliates, and research.

A digital forensic examiner should anticipate being confronted with fundamental concepts, scholarly articles, and learned treatises on their area of expertise. The failure to maintain sufficient continuing education could result in the expert being impeached on their lack of knowledge in their area of expertise, and otherwise impair future standing as an expert. See Federal Rule of Evidence 803(18)(permitting the use of scholarly articles and learned treatises for impeachment of expert witnesses and assisting a trier of fact in understanding technical subject matter).

C. Limitations

It is important to recognize which sub-disciplines will be covered in a particular matter and if that content exceeds your current knowledge and comfort level. A forensic examiner therefore should recognize both the limitations of their knowledge in digital forensics as well as whether the question being asked falls into the area of their expertise.

For instance, an examiner with education, training, or experience only in the area of the forensic examination of desktop / laptop forensics, should refrain from answering questions involving the examination of mobile devices; and explain to the party posing the question and the court that s/he is not qualified to answer such a question. The same concept is true if asked about the forensic examination of servers in a network intrusion case where the expert examined a desktop/laptop computer and found certain event logs erased and/or altered. Any gaps in the examiner's testimony should be addressed by the calling of an additional witness, if necessary.

A digital forensic expert should be mindful of limitations in order to provide clear testimony without overextending him or herself into an area where they have little expertise, ultimately undermining their credibility.

D. Brevity and Relevance

For testimony to be useful and understandable, a forensic examiner should keep responses as concise and to the point as possible. Examiners should provide only as much detail as necessary to answer the question being asked truthfully, correctly, and completely, without providing details that are irrelevant to the question but could impact the case. The examiner should focus on the details necessary to support the conclusions drawn through the analysis.

E. Clarity

When testifying in an administrative or judicial proceeding, the investigator and/or digital forensic examiner should strive to explain findings in its layperson's terms, providing the trier of fact the opportunity to review any relevant forensic artifacts.

To provide the trier of fact this opportunity, the investigator and/or digital forensic examiner may need to provide a desktop or laptop computer with sufficient Random Access Memory (RAM) and sufficient hard drive space to accommodate such a review.

The investigator and/or digital forensic examiner should consult with legal counsel and/or the court prior to providing their testimony to accommodate these concerns.

Refer to *Introduction to Testimony in Digital and Multimedia Forensics 22-Q-001-1.1.*

7. Competencies / Qualification for Investigators / Examiners

Prior to testimony, a court will need to ascertain that an investigator and/or digital forensic expert has specialized knowledge that will help the trier of fact to understand the evidence or to determine a fact in issue. While no particular education or certification is necessarily required to provide expert testimony, a court will weigh the educational background, certification (industry-level or vendor-agnostic), training, and experience of an investigator and/or digital forensic examiner to determine whether the testimony will assist the trier of fact in coming to a conclusion.

To attain the requisite background to be qualified as an expert, the investigator and/or digital forensic examiner should consider the following:

A. Quality Management System

Digital forensic units often institute formal quality management systems. Quality management systems help the unit accomplish consistency of operations as well as the delivery of reliable and repeatable results in a timely manner. Quality management systems often incorporate training, initial competence, and ongoing proficiency programs. They may include technical, quality, or administrative review procedures for forensic reports and output. A formal quality management system, in and of itself does not necessarily demonstrate that an examiner has the requisite background to provide expert testimony. However, the training and continuing education programs offered by some quality management systems may offer valuable evidence of the examiner's proficiency performing tasks or procedures they will be called on to testify about, or provide expert opinions interpreting findings.

B. Certification

Certification is an action or process of attaining competency in a certain area or field through a prescribed curriculum of study. This curriculum may encompass attendance at certain classes as well as a requisite amount of experience. It may also require passage of written and practical examinations. A certification typically is evidenced by a physical and/or virtual document. Depending on the rigor of the process, a certification can bolster standing if the certification is recognized in the field and particularly if it is relevant to the subject matter.

C. Training and Continuing Education

Training is the development of skills and/or knowledge in a certain area or field through a variety of adult learning techniques to ensure proficiency or mastery of knowledge given prescribed conditions of performance and to a defined standard. It is important that training prescribe learning outcomes and objectives as well as what training content is

necessary to enable such outcome. Performance must be measured for each learning objective in terms of knowledge and application where appropriate. Training takes many forms such as in person traditional structured classes, online live training as well as self paced material, on-the-job training, mentorship, and review of case work. Regardless of training format the principles above should be applied to enable measurement of learning and retention of desired content, performance and resulting proficiency of the student. Training and proficiency may be evidenced through a variety of physical and/or virtual methods.

The field of digital forensics changes quickly, and examiners should be engaged with the digital forensics community to maintain awareness of new trends, challenges, and issues.

D. Publication

Peer-reviewed publications can provide support in meeting the *Daubert* criteria. It should be noted, the *Daubert* standard applies specifically to theories and techniques, while the *Kumho Tire* extension applies to the expert. Consequently, even if the publication does not apply directly to the theory or technique to which the expert attests, it may speak to their personal skill or experience in the field, and thus can assist with satisfying the *Kumho Tire* extension as well.

E. Experience

Experience is the process of obtaining skills and/or knowledge through direct observation or participation in a certain field amassed over time. An investigator and/or digital forensic examiner should maintain a record of the events/experiences encountered during their career that can be verified through documentation and third party testimony. These events/experiences may include, but are not limited to: 1. number of digital devices identified, preserved, examined, and analyzed; 2. types/nature of case; 3. outcome of examination; and 4. amount of times called to provide testimony in an administrative, civil, or criminal proceeding.

These records may assist the examiner in providing required information in certain jurisdictions which require a practitioner to disclose their professional history for a minimum of a set period of time prior to the testimony.

The complexity of investigations as well as testimony can vary from basic preservation and reporting, to in depth analysis, sometimes incorporating a hypothesis, a theory, testing, and validation. A practitioner should have the necessary supporting experience with the subject matter and methods being used to withstand scrutiny.

Investigators and digital forensic examiners should be mindful of these considerations if testimony may be required in their field of expertise.

8. References

[1] Introduction to Testimony in Digital and Multimedia Forensics 22-Q-001-1.1

[2] SWGDE Glossary. Available at: https://www.swgde.org/glossary.

[3] Digital Investigation Techniques: A NIST Scientific Foundation Review, NISTIR 8354 available at: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8354.pdf.

[4] Federal Rules of Evidence 701 et. seq.

[5] Frye v. United States, 293 F. 1013 (D.C. Cir. 1923).

[6] Daubert v. Merrell Dow Pharmaceuticals, 113 S.Ct. 2786 (1993).

[7] Federal Rule of Evidence 803(18).

[8] Federal Rule of Criminal Procedure 16

[9] Refer to Document 2 / Training and Standards (Pending)

History

Revision	Issue Date	History
1.0 DRAFT	6/12/2023	Initial draft created.
1.0 DRAFT	9/21/2023	Moved forward for SWGDE membership vote to release as a Draft for Public Comment.
1.0	10/15/2023	SWGDE voted to release as a Draft for Public Comment; formatted for release for public comment.
1.1	1/23/2024	Revised document in response to public comments received. Moved forward for SWGDE membership vote to release as a final approved document.
1.1	3/7/2024	Formatted for posting after SWGDE membership voted to release as a Final Publication.