SWGDE Requirements for Report Writing in Digital and Multimedia Forensics

Disclaimer:
As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

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

Redistribution Policy:
SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

Requests for Modification:
SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for change

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

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

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

SWGDE Requirements for Report Writing in Digital and Multimedia Forensics

Table of Contents

1. Purpose 4
2. Scope 4
3. Limitations 4
4. General Discussion 5
5. Minimum Requirements 5
   5.1 General information 5
   5.2 Request 6
   5.3 Submitted or collected items 6
   5.4 Results, details of examination, and supporting data 6
   5.5 Opinions and Conclusions, if included 6
   5.6 Disposition 6
   5.7 Report authorization 6
6. Amendments to Examination Reports 7
7. References 7

1. Purpose

The purpose of this document is to define the minimum required elements of an examination report used to document a forensic examination of digital and multimedia evidence.

2. Scope

This document is intended for any persons preparing reports to document the processes and/or results of a forensic examination of digital and multimedia evidence. This document may not be all inclusive and there may be additional reporting (e.g., expert witness disclosure requirements), which is not considered within the scope of this document. This document does not address writing examination notes on which the report is based.[1]

3. Limitations

The required elements for an examination report discussed below are not necessarily all inclusive, but are the minimum expected elements of an examination report. This information does not take into account organizational policies, nor requirements mandated by accreditation bodies.

[1] AR3125 7.5.1.3 requires technical records to be sufficiently detailed such that another reviewer possessing the relevant knowledge, skills, and abilities could evaluate what was done and interpret the data.

4. General Discussion

Digital and multimedia evidence, as well as the tools, techniques, and methodologies used in an examination, are subject to challenge in a court of law or other formal proceedings. Proper documentation is essential in providing individuals the ability to reproduce the forensic process and the results.

Reporting is the process of preparing a summary of steps taken during the examination of digital media. A thorough examination report is written using documentation collected by the examiner, including photographs, drawings, case-notes, tool-generated content, etc. Many forensic tools come with built-in reporting functionality that is specific to that tool's actions and results, but does not typically document the full scope of the examination. Tool reports may be considered supporting documentation to the examination report or referenced as an appendix.

It is the responsibility of the examiner to produce the examination report, which should contain all the following:

- Report title (e.g., examination report, amended report)
- Case identifier and requester
- Clearly stated purpose of the examination
- Description of the processes and results of tests and examinations with supporting data, as needed (e.g., automated tool reports, screen captures and other exhibits)
- Explanation of conclusions/opinions drawn from the data, if appropriate
- Disposition of evidence
- Report authorization

5. Minimum Requirements

The following defines the elements to include in an examination report but does not define any specific format. Formatting and layout options are up to the examiner, or they may be defined by organizational policies or jurisdictional court rules.

5.1 General information

5.1.1 A title similar to "Report of Examination," to provide an immediate and accurate identification of the information being provided

5.1.2 Name and address of the examining organization/laboratory

5.1.3 Case identifier and page accountability (page number and total number of pages)

5.1.4 Date of report (date of final signed version)

5.1.5 Acronyms and abbreviations defined at first use, if not in the common vernacular of the general public

5.2 Request

5.2.1 Date of request

5.2.2 Requestor name and organization

5.2.3 Details, purpose, and scope of the request

5.2.4 Authority for request (e.g., consent, search warrant, contract, etc.)

5.3 Submitted or collected items

5.3.1 Date items submitted or collected

5.3.2 Method of delivery/collection

5.3.3 Submitter information (e.g., name and organization), if applicable

5.3.4 Information to uniquely identify each item submitted or collected for examination, such as make, model, serial number, marking, hash value or some other means to adequately identify the item (whether examined or not), typically provided in a listed format

5.4 Results, details of examination, and supporting data

The examination report must describe the results of the request in terms that are clear and unambiguous such that a layperson can understand. The examination report must adequately describe the overview of the processes performed. The results of all processes must also include descriptions of data that were recovered, extracted, and provided. If applicable, deviations from SOPs must be disclosed.

Many organizations separate the results from the details and supporting data. Based on organizational policy or legal requirements, the report and case notes may be combined.

Any examination results or analysis provided by a subcontractor must be identified.

5.5 Opinions and Conclusions, if included

If opinions and/or conclusions are included in the examination report, then the report should document the opinion and its basis.

5.6 Disposition

The examination report must include a description of the disposition of original and derivative works (e.g., destroyed, returned, or retained).

5.7 Report authorization

The examination report must include the name of the report authorizer and signature (e.g., handwritten, digital, or electronic signature).

6. Amendments to Examination Reports

After the release of a final report, if an examination report requires amendment, a new report must be released with edits identified and explained. The amended report must reference the original report.

7. References

[1] Rick Ayers, Sam Brothers, and Wayne Jansen, "Guidelines on Mobile Device Forensics," *NIST Special Publication 800-101*, pp. Section 6.3, pages 52 through 54, May 2014. [Online]. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

[2] *Standard Practice for Computer Forensics*, ASTM Standard E2763 - 10.

[3] *Standard Practice for Reporting Opinions of Scientific or Technical Experts*, ASTM Standard E620 - 11.

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

[5] *Conformity assessment – Requirements for the operation of various types of bodies performing inspection*, ISO/IEC 17020:2012.

[6] *General requirements for the competence of testing and measurement laboratories*, ISO/IEC 17025:2017.

[7] Rule 26. Duty to Disclose; General Provisions Governing Discovery, Federal Rules of Civil Procedure Title V Disclosures And Discovery. 2011. [Online]. Available: https://www.gpo.gov/fdsys/pkg/USCODE-2011-title28/html/USCODE-2011-title28-app-federalru-dup1-rule26.htm

[8] National Commission on Forensic Science, "Recommendation to the Attorney General: Documentation, Case Record, and Report Contents," September 13, 2016. [Online]. https://www.justice.gov/archives/ncfs/page/file/905536/download

[9] Scientific Working Group on Digital Evidence, "SWGDE Best Practices for Computer Forensics," 2014. [Online]. https://www.swgde.org/documents

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

[11] Scientific Working Group on Digital Evidence, "SWGDE Framework of a Quality Management System for Digital and Multimedia Evidence Forensic Science Service Providers," 2017. [Online]. https://www.swgde.org/documents

[12] Scientific Working Group on Digital Evidence, "SWGDE Model QAM for Digital Evidence Laboratories," 2012. [Online]. https://www.swgde.org/documents

[13] Scientific Working Group on Digital Evidence, "SWGDE Model SOP for Computer Forensics," 2012. [Online]. https://www.swgde.org/documents

SWGDE Requirements for Report Writing in Digital and Multimedia Forensics

History

Revision	Issue Date	Section	History
1.0 DRAFT	2018-06-14	All	Initial draft created and SWGDE voted to release as a Draft for Public Comment.
1.0 DRAFT	2018-07-09	All	Formatted and technical edit performed for release as a Draft for Public Comment.
1.0	2018-09-20	4; 5.4	Minor changes made in response to public comments. SWGDE voted to publish as an Approved document.
1.0	2018-11-20	--	Formatted and published as Approved version 1.0.