Scientific Working Group on Digital Evidence

SWGDE Best Practices for Computer Forensic Examination

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 Best Practices for Computer Forensic Examination

Table of Contents

1. Purpose

The purpose of this document is to describe the best practices for the forensic examination and analysis of digital evidence from computers and associated storage media. These processes are designed to maintain the integrity of digital evidence. This document is limited to computers and other storage media.

2. Scope

This document provides basic information on the examination and analysis of digital evidence from computers and their associated storage media. The intended audience is personnel qualified to perform examinations on digital evidence acquired from computers and associated storage media. For guidance on recommended training and qualifications, see *SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence* [1]. For the purposes of this document, the term "examiner" refers to those who perform analyses and examinations of digital evidence acquired from computers and associated storage media.

Examination of mobile devices is beyond the scope of this document and is being covered in the draft SWGDE publication, *SWGDE Best Practices for Mobile Device Evidence Collection, Preservation, and Acquisition* [2].

3. Limitations

This document is not intended to be a training manual, nor to replace organizational policy or standard operating procedures, nor should it be construed as legal advice. This document is not all inclusive and does not contain information relative to specific commercial products. This document may not be applicable in all circumstances. When warranted, an examiner may deviate from these best practices and still obtain reliable, defensible results. If examiners encounter situations warranting deviation from best practices or organizational policy, they should thoroughly document the specifics of the situation, actions taken, and results of the deviation.

This document is part of a planned set of best practice guides, *SWGDE Best Practices for Digital Evidence Collection, SWGDE Best Practices for Computer Forensic Acquisitions, SWGDE Best Practices for Computer Forensic Examination*, and *SWGDE Requirements for Report Writing in Digital and Multimedia Forensics* and may contain references to documents not yet published.

4. Preparation

Examiners should review documentation provided by the requestor to determine the processes necessary to complete the examination. Examiners should maintain communication with the requestor and communicate any restrictions, deviations, or limitations that may arise during examination. In addition, examiners should review documentation provided by the requestor to determine whether proper legal authority has been given to perform examination and analysis. Authority may be granular and restrict what examinations may be performed, for example, specifying what search terms may be used. Other legal authorities should be considered (e.g., owner consent, management, or organizational policies). Prior to beginning an examination, appropriate preparations should be made, as described in the following sections.

4.1 Environment

The examination environment should have adequate power, space, and cooling necessary that will not impact the examination and analysis process. Consult the National Institute for Standards and Technology (NIST) Interagency Report, *Forensic Science Laboratories: Handbook for Facility Planning, Design, Construction, and Relocation* [3], for design recommendations. Implement controls and access logs for evidence. Lab procedures should ensure data between cases are not commingled.

4.2 Examination workstation

Examination workstations should provide an isolated, known environment to perform analysis. Forensic tools should be tested and validated prior to use on examinations. Several methods can be used to provide an isolated, known environment. For example:

- Use virtualization technology to encapsulate case data in a working container. A tested, patched, sanitized version of the operating system and forensic tools could be copied and reused for each case.
- Use filesystem and folder organization along with forensic tools to isolate cases.
- Use a known image to revert an examination workstation to a previous state. This may require patching and maintaining the known image for distribution between examiners.
- Use operating system tools to revert an exam workstation to a sanitized state.

4.3 Documentation

Examiners should take contemporaneous notes relevant to their examination. Organizational systems should exist to maintain any notes with their case for later review. Organizations may implement a quality assurance process to review documentation and exam processes.

5. Considerations

Any examination activity should be accompanied by a specific request [4]. Examinations are more likely to produce useful results when they are targeted or guided by dialog with the requestor. Primary consideration for any examination activity should be made to accomplish the parameters of the request. Examiners should endeavor to keep the requestor advised of any additional information that may impact the specifics of the exam request, new leads, conflicting information, or exculpatory information.

Conducting an examination on the original evidence should be avoided if possible. Digital evidence, not written to a forensic container, should be protected with a software or hardware write blocker during examination. Static analysis should be carried out on a copy of the original digital evidence to avoid accidental spoliation or obfuscation [5]. The examiner should ensure the forensic image is archived.

6. Examination

An examination should include a systematic review of the data to determine its relevance to an investigation. During the examination, the following items should be considered where relevant to the request:

- Random access memory (RAM) analysis, active files, operating system (OS) artifacts, registry artifacts, file metadata, compound files, encrypted files, log files, and database files
- Internet browsers, email, social media, and peer-to-peer file sharing
- Deleted files, file slack, partition slack, disk slack, and shadow files
- Disk structures, basic input/output system (BIOS), and boot sequence

Examinations of live systems will require special handling to maintain system integrity and properly capture volatile data, see *SWGDE Capture of Live Systems* [6] for guidance.

7. Analysis

Analysis is the assessment of the information contained within the media. The data learned from the examination is interpreted for probative value and conclusions may be drawn from it. If data is analyzed, findings should be sound and defensible. Any conclusion derived from the data analysis should be written in a report that is concise and complete. Guidance on report writing is being addressed in the draft SWGDE publication, *SWGDE Requirements for Report Writing in Digital and Multimedia Forensics*, [7].

8. References

[1] Scientific Working Group on Digital Evidence and Scientific Working Group on Imaging Technology, "SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence," 2010. [Online]. https://www.swgde.org/documents

[2] Scientific Working Group on Digital Evidence, "SWGDE Best Practices for Mobile Device Evidence Collection, Preservation, and Acquisition," Draft for Public Comment 2018 (Approved Version TBD). [Online]. https://www.swgde.org/documents/draftsForPublicComment

[3] Forensic Science Laboratories Facilities Working Group, "Forensic Science Laboratories: Handbook for Forensic Planning, Design, Construction, and Relocation," NIST Interagency/Internal Report - 7941, June 2013.

[4] Scientific Working Group on Digital Evidence, "SWGDE Focused Collection and Examination of Digital Evidence," 2014. [Online]. https://www.swgde.org/documents

[5] *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*, ISO/IEC 27037:2012.

[6] Scientific Working Group on Digital Evidence, "SWGDE Capture of Live Systems," 2014. [Online]. https://www.swgde.org/documents

[7] Scientific Working Group on Digital Evidence, "SWGDE Requirements for Report Writing in Digital and Multimedia Forensics," Draft for Public Comment 2018 (Approved Version TBD). [Online]. https://www.swgde.org/documents/draftsForPublicComment

History

Revision	Issue Date	Section	History
1.0 DRAFT	2018-01-11	All	Initial draft created and SWGDE voted to release as a Draft for Public Comment.
1.0 DRAFT	2018-04-17	All	Formatted and technical edit performed for release as a Draft for Public Comment.
1.0 DRAFT	2018-06-14	--	No changes. SWGDE voted to publish as an Approved document.
1.0	2018-07-11	--	Minor editorial changes. Formatted and published as Approved version 1.0.