SWGDE Best Practices for Digital Evidence Collection

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 Digital Evidence Collection

Table of Contents

1. Purpose

The purpose of this document is to describe the best practices for the collection of items that may contain digital evidence. 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 collection of items that may contain digital evidence. For the purposes of this document, "collector" refers to any personnel designated and trained to collect digital evidence. For guidance on recommended training and qualifications, see *SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence* [1].

Collection of digital evidence from 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, a collector may deviate from these best practices and still obtain reliable, defensible results. If collectors encounter situations warranting deviation from best practices, they should thoroughly document the specifics of the situation and actions taken.

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, SWGDE Requirements for Report Writing in Digital and Multimedia Forensics*, and may contain references to documents not yet published.

4. Preparation

Preparing for the collection of digital evidence includes clear communication between the collector and investigative team. This communication includes the details of the investigation, the nature and scope of the potential evidence, and any unique constraints which could impact acquisition. Collectors should review the legal authority authorizing the search to determine what items may be collected.

The possibility of anti-forensics techniques (e.g., destructive or explosive devices and wiping technology) and encryption should be considered. Appropriate safety measures should always be paramount in planning, along with adherence to organizational policies and procedures.

5. Considerations

Prior to collecting digital evidence, consider collecting and preserving traditional forensic evidence (e.g., fingerprint, DNA, trace). Precautions should be taken to prevent exposure to evidence that may be contaminated with dangerous substances or hazardous materials.

Considerations should be taken to isolate the scene's network traffic to prevent outside connectivity.

6. Search

Remove all non-essential personnel from the proximity of the digital evidence, if possible.

Consider dividing the scene into manageable sections (e.g., rooms) and documenting using photographs and sketches; label the scene in an identifiable manner.

Collectors should recognize devices that may store data and information about the items containing the data (e.g., notes containing usernames, passwords, operating systems documentation, encryption recovery keys, and network credentials). See **7. Documentation** below for more information on the documenting the evidence location.

It is important to determine the computer system's or digital media's operational state. For example, a computer in standby mode may appear to be powered down, but it is not and should be handled as a running system. If a computer is powered off, do not turn on the computer.

Observe the system for any potential destructive activity. If destructive activity is occurring, pull the power plug from behind the desktop computer, or in the case of a laptop, pull the power cord and, if possible, remove the battery. If a destructive activity is found, stop the activity and document all actions taken. If applicable, isolate the computer system from any network connectivity.

Consider the capture of random access memory (RAM) and other volatile data from the operating system, see *SWGDE Capture of Live Systems* for detailed information [3].

Where permitted, the search should be comprehensive. This could include external storage media, which may be connected via network, disguised storage, and other non-standard media. If any of the following situations are encountered, collections specialists should consider consulting more experienced personnel:

- Live systems with file or disk encryption
- Running systems displaying documents or other files of interest
- Running systems acting as virtual machine hosts
- Enterprise class storage systems such as Storage Area Networks (SANs)
- Non-standard or novel devices, (e.g., home automation, media streaming devices)

(See *SWGDE Capture of Live Systems*, *SWGDE Best Practices for Mobile Device Evidence Preservation and Acquisition*, and *SWGDE Best Practices for the Acquisition of Data from Novel Digital Devices* for more information [3] [2] [4].)

As soon as practical, store and secure evidence to prevent loss, contamination, or deleterious change.

7. Documentation

Document the collection of devices in accordance with organizational guidelines and procedures. At a minimum, this documentation should include a chain of custody and evidence inventory.

Documentation may include a written description or photographs of the collection location, the device state (e.g., powered on/off, open files), and physical characteristics (e.g., damage, identifying marks, serial numbers, connections).

The chain of custody documentation should be contemporaneous to the collection and include a description or unique identifier for the evidence, the date and time of receipt, and reflect all transfers. The record should easily identify each person (e.g., name and signature) taking possession of an item.

Evidence inventories should contain a listing of the items collected and may be used for search warrant returns, report writing, or other reasons.

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

[4] Scientific Working Group on Digital Evidence, "SWGDE Best Practices for the Acquisition of Data from Novel Digital Devices," 2017. [Online]. https://www.swgde.org/documents

SWGDE Best Practices for Digital Evidence Collection

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	None	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.