SWGDE Best Practices for Computer 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 Best Practices for Computer Forensics

Table of Contents

1. Purpose

The purpose of this document is to describe the best practices for collecting, acquiring, analyzing and documenting the data found in computer forensic examinations.

2. Scope

This document provides basic information on the logical and physical acquisition of computers and their associated storage media. The intended audience is examiners in a lab setting and personnel who collect digital evidence in the field.

This document is not intended to be used as a step-by-step guide for conducting a proper forensic examination when dealing with computers nor should it be construed as legal advice.

3. Limitations

This document does not cover all digital devices that may contain electronically stored information (e.g., mobile phones, game systems and GPS devices).

This document only discusses those devices currently available at the time of writing. Emerging technologies will be addressed in future revisions.

Many organizations do not have examiners that can be available for all collections of digital evidence. Triaging and previewing techniques should only be conducted by properly trained personnel. There may be times when triaging and previewing a computer are not feasible.

Acquisitions and limitations related to cloud computing are outside the scope of this document.

4. Evidence Collection

General guidelines concerning the collection of digital evidence are provided as follows:

- Consult with the investigator to determine the details of the case and potential evidence to be collected.
- Determine the necessary equipment to take to the scene.
- Review the legal authority to collect the evidence, ensuring any restrictions are noted. If necessary during the collection, obtain additional authority for evidence outside the original scope.
- Occasionally, there may be a need to conduct traditional forensic processes on media (e.g., DNA and latent prints). These are case dependent and should be discussed with the investigator to determine the need for such processing as well as the order in which the processes should be performed.
- When evidence from the scene cannot be removed, it should be copied or imaged on-site.
- All individuals not involved in the collection process should be removed from the proximity of digital evidence.
- Individuals who may have relevant information (e.g., user names, passwords, operating systems and network credentials) should be identified and interviewed.
- The scene should be searched systematically and thoroughly. Searchers should be able to recognize different types of devices that may contain digital evidence (e.g., novelty USB drives, servers and wireless storage devices).
- The possibility of anti-forensics techniques (e.g., destructive devices and wiping software) should be considered.

5. Evidence Handling

- Document the condition of the evidence.
    - Photograph (screen, computer front and back, and area around the computer to be seized) and/or make a sketch of the computer connections and surrounding area.
    - Determine if the computer is in stand-by mode and follow procedures as if it was powered on.
- Document the external component connections.

6. Evidence Triage/Preview

- Evidence triage may not be appropriate for all situations.
- Evidence preview may miss items of evidentiary value.
- Time and date stamps may be affected by the evidence triage/preview process on live systems.
- An evidence preview/triage shall not take the place of a complete exam.

6.1 Powered-On Systems

The examiner should:

- Examine the computer for any running processes. If it is observed running a destructive process, the examiner should stop the process and document any actions taken.
- Capture RAM and other volatile data from the operating system – see *SWGDE Capture of Live Systems*.
- Determine if any of the running processes are related to cloud or off-site storage. When encountered, the examiner should coordinate with the appropriate legal authority to ensure the scope covers the off-site acquisition.
- Document and hibernate any running virtual machines.
- Consider the potential of encryption software installed on the computer or as part of the operating system. If present, appropriate forensic methods should be utilized to capture the unencrypted data before the computer is powered off.
- Save any opened files to trusted media.
- Evaluate the impact of pulling the plug vs. shutting the computer down. This is typically dependent upon the operating system and file system encountered.
- Isolate the computer from any network connectivity.
- Use a triage tool to preview data.

6.2 Powered Off Systems

If the computer is powered off, ***do not*** turn on the computer.

- Only personnel trained to preview/triage computers should power on the computer and preview/triage data.
- Disconnect all physical network connectivity.
- Consider the possibility of Wake on Wireless LAN (WoWLAN) and BIOS timed booting sequences.
- Verify the computer system for compatibility with triage tools and software.
- Identify and document evidence, if applicable.
- Export evidence to trusted media.

6.3 Loose media

- When possible, use write blocking devices to collect and document evidence.

6.4 Computers

- Disconnect all power sources by unplugging from the back of the computer.
- Laptop batteries should be removed.

6.5 Servers

- Determine whether to get logical files, logical images, or physical images.
- If possible, consideration should be given to the collection of backup tapes and their associated drives, , as the tapes may contain additional evidence.
- Unless the situation warrants it, capturing volatile data may not be necessary.

Warning: Pulling the plug on a server may severely damage the system, disrupt legitimate business and/or create organizational liability.

7. Evidence Packaging /Transport

- Each piece of evidence should be protected from damage or alteration, labeled and a chain-of-custody maintained as determined by organizational policy.
- Specific care should be taken with the transportation of digital evidence to avoid physical damage, vibration and the effects of magnetic fields, electrical static and large variations of temperature and/or humidity.

8. Equipment Preparation

Equipment refers to the non-evidentiary hardware and software the examiner utilizes to conduct the forensic imaging or analysis of evidence.

- The examiner should ensure that the equipment is adequate for the task and in proper working condition. The condition of the equipment should be documented.
- Hardware and software must be configured to prevent cross contamination.
- The manufacturer's operation manual and other relevant documentation for each piece of equipment should be available if needed.
- Analysis/Imaging software should be validated prior to its use as discussed in *SWGDE Recommended Guidelines for Validation Testing*.

9. Acquisition

- Examiners should be trained as discussed in *SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence*.
- Precautions should be taken to prevent exposure to evidence that may be contaminated with dangerous substances or hazardous materials.
- All items submitted for forensic examination should be inspected for their physical integrity.
- Methods of acquiring evidence should be forensically sound and verifiable; method deviations shall be documented.
- Digital evidence submitted for examination should be maintained in such a way that the integrity of the data is preserved. Additional information on data integrity is discussed in *SWGDE Data Integrity within Computer Forensics*.
- Forensic image(s) should be archived to trusted media and maintained consistent with organization policy and applicable laws.
- Any errors encountered during acquisition should be documented.
- Steps should be taken to ensure the integrity of the data acquired; this may include one or more of the following:
    - Hash values (e.g., MD5, SHA-1 and SHA-256)
    - Stored on read-only media (e.g., CD-R and DVD-R)
    - Sealed in tamper-evident packaging

9.1 Acquisition Types

- Physical
  - Hardware or software write blockers should be used when possible to prevent writing to the original evidence.
  - Forensic image(s) should be acquired using hardware or software that is capable of capturing a bit stream image of the original media.
- Logical
  - Hardware or software write blockers should be used when possible to prevent writing to the original evidence.
  - Forensic image(s) should be acquired using hardware or software that is capable of capturing a "sparse" or logical image of the original media.
- Live
  - Live data should be acquired using hardware or software that is capable of capturing a "sparse" or logical image of the original media.
  - Live acquisition software should be run from trusted media to prevent unnecessary changes to the live system.
  - Live acquisition software should be run at the highest level of privilege available to ensure all possible data is available for acquisition.
  - Additional information on live acquisitions is discussed in *SWGDE Capture of Live Systems*.
- Targeted File(s)
  - Targeted file(s) should be acquired using hardware or software that is capable of capturing a "sparse" or logical image of the original media.
  - Examiners should request whether associated artifacts are to be collected relating to the targeted file(s) (e.g., LNK files, Jump lists and associated registry keys).

10. Forensic Analysis/Examination

- Examiners should be trained as discussed in *SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence*.
- Examiners should review documentation provided by the requestor to determine the processes necessary to complete the examination.
- Examiners should review the legal authority (e.g., consent to search by owner, search warrant or other legal authority).
- Conducting an examination on the original evidence media should be avoided if possible. Examinations should be conducted on forensic copies or images.
- Appropriate controls and standards should be used during the examination procedure.
- Examination of the media should be completed logically and systematically consistent with organizational policy.

11. Documentation

Documentation should include all required information and be preserved according to the examiner's organizational policy.

11.1 Acquisition Documentation

Acquisition documentation should include:

- Examiner's name.
- Acquisition date.
- Acquisition details (e.g., type of acquisition, imaging tool and version number).
- Physical condition of the evidence and unique identifiers (e.g., serial number, description, make and model).
- Original and verification hash values.
- Photographs and/or sketches.
- Any additional documentation as required by the examiner's organization.

11.2 Examination Documentation

Examination documentation should be case specific and contain sufficient details to allow another forensic examiner, competent in the same area of expertise, to identify what was done and to replicate the findings independently.

11.3 Evidence Handling Documentation

Evidence handling documentation should include:

- Copy of legal authority (e.g., search warrant, consent to search and administrative).
- Information regarding the packaging and condition of the evidence upon receipt by the examiner.
- A description of the evidence.
- Communications related to the case.

12. Report of Finding

- Information should be presented in a format that may be read and understood by non-technical individuals.
- Examiners should be able to explain all information contained within the report.
- Should include any relevant information contained within the acquisition and/or evidence handling documentation.
- Reports issued by the examiner should address the requestor's needs and
    - Document the scope and/or purpose of the examination.
    - Give a detailed description of the media examined (e.g., hard disk, optical media or flash drive).
    - Include any supplemental reports related to the examination.
    - Provide the examiner's name and date of exam.
    - Be reviewed according to organizational policy.

13. Review

The examiner's organization should have policies for technical, peer and administrative reviews.

14. References

The following SWGDE documents are referenced in this document:

- SWGDE Capture of Live Systems
- SWGDE Data Integrity within Computer Forensics
- SWGDE Recommended Guidelines for Validation Testing
- SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence

Access the most current version of these documents at www.swgde.org.

SWGDE Best Practices for Computer Forensics

History

Revision	Issue Date	Section	History
1.0	11/15/2004	All	Original Release
2.0	04/12/2006	All	Added Section 4.1 Forensic Analysis/Examination Of Non-Traditional Computer Technologies. Added additional bullet under Section 3.0 Forensic Imaging.
2.1	07/19/2006	All	Clarified Section 1.1 Evidence Handling. Added "and a chain-of-custody maintained."
3.0	01/17/2013	All	Major revisions and updates for all sections.
3.0	02/11/2013	All	Edit/format for publishing as Public Draft.
3.0	09/14/2013	Disclaimer	No document changes. Formatted for publishing as Approved Document.
3.1	06/06/2014	Section 2	Changed "investigation" to "examination." Voted to release as a Draft for Public Comment.
3.1	06/12/2014	Disclaimer/ All	Formatted for publishing as a Draft for Public Comment.
3.1	08/28/2014	None	No changes made; voted to publish as an Approved document.
3.1	09/05/2014	All	Section 3 (Definitions) removed from document and added to Glossary. Formatting and technical edit performed for release as an Approved document.