Scientific Working Group on
Digital Evidence

SWGDE Best Practices for Computer Forensic Acquisitions

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 Acquisitions

Table of Contents

1. Purpose

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

2. Scope

This document provides basic information on acquisitions of data from computers and their associated storage media. The intended audience is personnel qualified to acquire digital evidence. 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 conduct acquisitions.

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 regarding 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, they should thoroughly document the specifics of the situation and actions taken.

These best practices may not apply in incident response or complex live acquisition scenarios. For guidance with the capture of live systems see *SWGDE Capture of Live Systems* [2].

This document is part of a planned set of best practice guides including *SWGDE Best Practices for Digital Evidence Collection*, *SWGDE Best Practices for Computer Forensic Examination*, *SWGDE Best Practices for Forensic Reporting*, and contains references to said documents not yet published.[1]

4. Preparation

The needs and aims of an investigation must drive the digital forensic process. Preparing for the acquisition of digital evidence includes clear communication between the examiner and investigative team. This communication includes the details of the investigation, the nature and scope of the potential evidence to be acquired, and unique constraints that may impact acquisition. Examiners should consult appropriate legal counsel if clarification on legal authority is needed.

Prior to performing digital acquisition or collection, considerations should be made for the collection and preservation of 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.

[1] References will be updated as planned documents are published.

Examiners should consider the need to collect memory and ancillary data such as metadata, encryption keys, log files, schema information, as well as documentation needed to access and understand the data sought in the context of the investigation, see *SWGDE Best Practices for Digital Evidence Collection* [3]. This information may exist on physical devices, related or paired devices, and remote locations. Examiners should ascertain the appropriate means of acquiring data from identified sources. Examiners should be aware of the limitations of each acquisition method and consider actions to mitigate these limitations if appropriate. Acquisition of devices using novel technologies may require the use of non-traditional acquisition techniques; see *SWGDE Best Practices for the Acquisition of Data from Novel Digital Devices* [4].

Examiners must understand the impact a chosen acquisition technique may have on the source item and minimize adverse effects as much as possible. Where it is not possible to fully prevent alterations to the source item, examiners must document the acquisition process in sufficient detail to account for artifacts of the acquisition process. Where possible, processes used during the acquisition process should be auditable and repeatable.

Examiners should identify appropriate hardware and software tools to conduct the acquisition, ensuring they understand the limitations of the tools. Tools should be validated for use according to organizational policies and procedures (see *SWGDE Recommended Guidelines for Validation Testing* [5] or *NIST Computer Forensics Tool Testing Handbook* [6]). If an examiner is using a native software utility specific to the type of data being acquired (e.g. databases, embedded devices), the examiner must ensure the tool is reliable with respect to the functions of the tool utilized. Examiners must be aware of known issues with their tools and take measures to mitigate any issues.

Prior to the acquisition process, examiners should prepare their destination media if necessary. Sterilization of destination media is not generally required except when needed to satisfy administrative or organizational requirements or when a specific analysis process makes it a prudent practice. For example, examiners may need to sanitize destination media provided to an external recipient to ensure extraneous data is not disclosed. Examiners may also be required to destroy copies of existing data to comply with legal or regulatory requirements. The examiner may need to sanitize the destination media for certain analysis processes such as when media without a file system is cloned for examination (e.g. DVR cloning).

Acquired data should be stored on a trusted platform, either physical media or network storage, configured with appropriate security controls. Data should be acquired to either raw format or a well-documented, widely utilized forensic container. A raw image is a flat, uncompressed image file which necessitate storing metadata and integrity information separately. Forensic container formats can store metadata and integrity information about the acquired data and may support compression of the acquired data. Use of a raw image or widely utilized forensic container format prevents examinations of the acquired data from being dependent on a single tool, vendor, or method of analysis, and helps ensure archived data will be readable well into the future.

5. Considerations

5.1 Location and Environment

Acquisitions should be conducted in a safe and controlled environment with stable electrical power. Access to the work area should be limited to essential personnel. Acquisitions can be performed onsite or offsite. Examiners may need to take extra precautions while performing onsite acquisitions and identify potential environmental conditions that may be out of their control (e.g. power). If unmitigable external factors are likely to interrupt or interfere with the acquisition, examiners should consider prioritizing targeted acquisitions of data, in order of importance to the investigation. This maximizes the likelihood of capturing relevant data prior to any failure or interruption.

5.2 Encryption

Examiners should be aware of encryption technologies at the device, volume, container, and file level. Several options are available to obtain decrypted data. Examiners may need to perform live capture of memory prior to obtaining a disk image to capture possible keys in volatile memory. Examiners may choose to perform a live acquisition of source media to obtain logical images of unencrypted data [2]. Examiners should be aware that some encryption technologies allow saving of recovery keys on local and removable media, in the cloud with a third-party service provider, or via an enterprise management solution. Examiners should also consider whether encryption keys or unencrypted data may be available via non-technical means. These may include asking keyholders for keys, locating keys on written documentation, or compelling disclosure of keys from third parties via legal process. Unencrypted copies of target data may also be available from third party service providers via legal process.

5.3 Boot Loader Restrictions

Some Unified Extensible Firmware Interface (UEFI) implementations contain secure boot loaders that ensure the computer boots an operating system trusted by the computer manufacturer. Secure boot loaders create challenges for examiners attempting to boot alternate operating systems, such as a forensic boot image. Methods to boot an alternate operating system on a computer with a secure boot loader may include disabling boot loader security in the UEFI. Booting to alternate media can require specific key combinations unique to computer manufacturers.

6. Triage

Examiners may need to preview the contents of potential data sources prior to acquisition to reduce the amount of data acquired, avoid acquiring irrelevant information, or comply with restrictions on search authority. Triage typically includes reviewing the attributes and contents of potential data to be acquired, by automated or manual means, to determine its relevance to the investigation. There may be multiple iterations of this process, depending on the complexity of the investigation.

Examiners may decide to acquire a potential data source, in whole or in part, based on the result of the triage process. The focused collection of respondent or relevant data is an acceptable practice; refer to *SWGDE Focused Collection and Examination of Digital Evidence* [7].

Examiners should use forensically sound processes to conduct triage to the extent possible. Examiners should document the triage process in sufficient detail to allow its repetition and account for artifacts created by the triage process.

7. Acquisition Process

The guiding principle for computer forensic acquisitions is to minimize, to the fullest extent possible, changes to the source data. This is usually accomplished by the use of a hardware device, software configuration, or application intended to allow reading data from a storage device without allowing changes (writes) to be made to it.

The examiner should weigh the goals of the anticipated examination against the results of different acquisition methods.

7.1 Types of Acquisitions

7.1.1 Physical – A physical acquisition is a bit stream duplicate of data contained on a device.

7.1.1.1 Hardware or software write blockers should be used when possible to prevent writing to the original evidence.

7.1.1.2 Forensic image(s) should be acquired using hardware or software that is capable of capturing a complete bit stream image of the original media.

7.1.2 Logical – A logical acquisition is the process of acquiring folders and files while utilizing the native file system in which they reside.

7.1.2.1 Hardware or software write blockers should be used when possible to prevent writing to the original evidence.

7.1.2.2 Forensic image(s) should be acquired using hardware or software that is capable of capturing a logical image of the original media.

7.1.3 Targeted Content – Acquiring targeted files or content from a piece of media or device either through a live, physical, or logical acquisition. See *SWGDE Focused Collection and Examination of Digital Evidence* [7].

7.1.3.1 Metadata for targeted files, such as timestamps and permissions, may be lost when the files are copied logically. If the metadata is potentially relevant, the examiner should ensure the metadata is also acquired. This may require imaging targeted files to a container that supports the metadata or separately collecting the metadata. Other artifacts, such as link files and registry keys, may provide additional information about targeted content. Examiners should consider the need to collect these additional files or artifacts.

7.1.3.2 Targeted content could include compound and embedded files.

7.1.4 Forensic Cloning – A forensic clone is the process of creating a bit stream duplicate of data from one storage media to another.

7.1.4.1 If cloning is a requirement for technical reasons (e.g. DVR, Gaming System), it is recommended to acquire the image to a forensic container before cloning.

Any of these acquisition types may be conducted from a live (running) computer system. There are additional considerations for examiners conducting live acquisitions, including:

- Live acquisition tools should execute trusted binaries from controlled media.
- Live acquisition software should execute at the lowest level of privilege needed to ensure all possible data is available for acquisition.

For guidance with the capture of live systems see *SWGDE Capture of Live Systems* [2].

8. Verification and Preview

Verification is the validation of the integrity of the data as acquired. The process of verification does not verify all data is read from the source item. For example, damaged sectors, Host Protected Areas, or Device Configuration Overlays may prevent an acquisition tool from reading those areas.

9. Documentation

Examiners should review acquired data to verify they have acquired the intended items. Examiners should review tool output for indications of failures in the acquisition process and document and resolve those failures as appropriate. Examiners should compute a cryptographic hash value over the acquired data using a NIST-approved Secure Hash Algorithm to facilitate subsequent validation of the acquired data’s integrity.

Examiners should document digital evidence acquisition per organizational policy. The documentation should include a description detailed enough to allow the definitive identification of the item to the exclusion of all others. This information may include:

- Unique identifiers (e.g. make, model, serial number, and asset tag);
- Source of digital evidence (e.g. a description of its location when discovered);
- Unique investigation identifiers (e.g. investigation name, case number);
- Acquisition details (e.g. type of acquisition, imaging tool and version number);
- Hash value(s) of the acquired data;
- Any photographs of the evidence that were taken, either at the time of collection or before the acquisition;
- Acquiring person's name and title;
- Acquisition date;
- Errors encountered during acquisition;
- Any additional documentation as required by the examiner’s organization.

Examiners should document chain of custody as required by organizational policy. When digital evidence is transferred from one person to another, the chain of custody should note at a minimum the following:

- Name of transferring individual;
- Name of receiving individual or facility;
- Date and time of receipt and transfer;
- Purpose of transfer.

Please refer to *SWGDE Best Practices for Evidence Collection* [3] for further collection recommendations.

10. Preservation

After an image is acquired and verified, a working copy should be created and used for examination. Forensic images and related documentation should be retained and maintained consistent with organization policy and applicable law [8].

11. 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". [Online]. https://www.swgde.org/documents

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

[3] Scientific Working Group on Digital Evidence, "SWGDE Best Practices for Digital Evidence Collection," *Public Draft*. [Online]. https://www.swgde.org/documents/draftsForPublicComment

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

[5] Scientific Working Group on Digital Evidence, "SWGDE Recommended Guidelines for Validation Testing,". [Online]. https://www.swgde.org/documents

[6] National Institute of Standards and Technology (NIST), "Computer Forensics Tool Testing Handbook," Computer Forensics Tool Testing Program, August 6 2015. [Online]. https://www.cftt.nist.gov/CFTT-Booklet-08112015.pdf

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

[8] Scientific Working Group on Digital Evidence, "SWGDE Best Practices for Archiving Digital and Multimedia Evidence," *Proposed Document*, TBD.

SWGDE Best Practices for Computer Forensic Acquisitions

History

Revision	Issue Date	Section	History
1.0 DRAFT	2017-08-24	All	Initial draft created and SWGDE voted to release as a Draft for Public Comment.
1.0 DRAFT	2017-09-25	All	Formatted and technical edit performed for release as a Draft for Public Comment.
1.0 DRAFT	2018-01-11	4	Update made in response to public comment. SWGDE voted to publish as an Approved document (Version 1.0).
1.0	2018-04-25	--	Formatted and published as Approved Version 1.0.