Scientific Working Group on Digital Evidence

Best Practices for Computer Forensic Acquisitions

17-F-002-2.0

Disclaimer and Conditions Regarding Use of SWGDE Documents

SWGDE documents are developed by a consensus process that involves the best efforts of relevant subject matter experts, organizations, and input from other stakeholders to publish suggested best practices, practical guidance, technical positions, and educational information in the discipline of digital and multimedia forensics and related fields. No warranty or other representation as to SWGDE work product is made or intended.

As a condition to the use of this document (and the information contained herein) in any judicial, administrative, legislative, or other adjudicatory proceeding in the United States or elsewhere, 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 such proceeding. The notification should 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; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in the proceeding please notify SWGDE as to the outcome of the matter. Notifications should be sent to secretary@swgde.org.

From time to time, SWGDE documents may be revised, updated, or sunsetted. Readers are advised to verify on the SWGDE website (https://www.swgde.org) they are utilizing the current version of this document. Prior versions of SWGDE documents are archived and available on the SWGDE website.

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 this SWGDE cover page containing the Disclaimer and Conditions of Use.
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 creation date) of the document and also indicate 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 any suggested modification:

a) Submitter's name

b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) SWGDE 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 suggested modification

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.

Scientific Working Group on Digital Evidence

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 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 or the acquisition of complex disk arrays or hybrid storage devices.

This document is part of a planned set of best practice guides including *SWGDE Best Practices for Digital Evidence Collection* [1], *SWGDE Best Practices for Computer Forensic Examination* [2], and *SWGDE Requirements for Report Writing in Digital and Multimedia Forensics* [3].

4. Preparation and Considerations

The needs and aims of an investigation must drive the digital forensic process, including acquisition. Clear communication between the examiner and stakeholders is paramount in preparing for the seizure, acquisition, and analysis of digital evidence. This communication can include 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 of legal authority is needed.

Consideration should be given to the relative volatility of both digital and traditional evidence artifacts (e.g., fingerprint, DNA, trace). The order of collection, acquisition, and analysis of each should be planned to mitigate destruction of the others.

Precautions should be taken to prevent exposure to evidence that may be contaminated with dangerous substances or hazardous materials.

Examiners should consider the need to collect volatile and ancillary data such as metadata, encryption keys, log files, and 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* [1]. 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. Non-traditional techniques may be required for the acquisition of data from devices using novel technologies; 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 Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics* [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 should ensure the tool is reliable with respect to the functions of the tool utilized. Examiners should be aware of known issues with their tools and take measures to mitigate them.

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 sterilize 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 sterilize 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 necessitates storing metadata and integrity information separately. Forensic container formats can also store metadata and integrity information about 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.

4.1. 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 in the field or laboratory. Examiners may need to take extra precautions while performing acquisitions in the field to identify potential 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.

4.2. Encryption

Examiners should be aware of encryption technologies at the device, volume, container, and file level. Several options are available to obtain decrypted data. To obtain encryption keys, examiners may need to capture memory prior to obtaining a disk image, and attempt to decrypt later. Examiners may choose to perform a live acquisition of source media to obtain logical images of decrypted data. 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.

4.3. Hardware Specifics

Examiners should, when possible, become familiar with the specific configurations and nuances of hardware that is to be acquired. Examiners may encounter computer systems which do not allow the removal of the internal storage device based on the storage being fixed to the motherboard. Furthermore, examiners may encounter systems having a TPM (Trusted Platform Module) which binds the internal storage device data to the computer in which it is installed. This may require a review of the manufacturer's documentation of the specific hardware and/or an Internet search for technical specifications of the specific make and model of the device.

5. 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 data, or comply with restrictions on search scope. 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; *see Targeted Collection*, below.

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 to account for artifacts created by the triage process.

6. 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 the source media (i.e., write-blocking).

The examiner should weigh the goals of the anticipated examination against the advantages and disadvantages of different acquisition methods.

7. Types of Acquisitions

7.1. Physical

A physical acquisition is a bitstream duplicate of data contained on a device including slack space potentially containing deleted data.

- Hardware or software write-blockers should be used when possible to prevent writing to the original evidence.
- Forensic images should be acquired using hardware or software that is capable of capturing a complete bitstream image of the original media.

7.2. Logical

A logical acquisition is the process of acquiring structured data, such as folders and files, typically by utilizing the native file system in which they reside.

- Hardware or software write-blockers should be used when possible to prevent writing to the original evidence.
- Forensic images should be acquired using hardware or software that is capable of capturing a logical image of the original media.

7.3. Live Acquisition

A live acquisition is a physical or logical acquisition of data or files from a running system, typically by using that system's raw device access or file system.

7.4.1 Live Acquisitions Considerations

- Live triage or acquisition may be the only opportunity to obtain data from an encrypted system. Detailed documentation should be kept of all actions taken. Additional considerations for examiners conducting live acquisitions include:
    - Live acquisition tools should execute trusted binaries from controlled media.
    - Systems may require administrative/elevated account permissions for successful acquisition. However, live acquisition software should execute at the least level of privilege needed to acquire all sought data.
    - System and file dates and times may change as a result of live access.
    - Processes may conflict and create system instability.
    - Live acquisition may be susceptible to smear.

- Live Acquisition may include:
    - Physical or logical acquisition of storage
    - Acquisition of volatile system data such as system environmental variables, processes, and network connections
    - System Memory
    - Application memory

- Order of Volatility - The potential volatility and the effect of the collection on the computer system requires consideration for the order in which the data is collected. This order may change based upon the computer system. The examiner must understand the needs of the specific situation and prioritize the collection of volatile data accordingly.
    - The generally recommended order of volatility is:
        - Running processes
        - Network connections
        - RAM (on some systems RAM collection may cause instability and therefore should be conducted last)
        - System settings
        - Encryption keys (e.g., Bitlocker)
        - Application (e.g., web browser, cryptocurrency wallets) artifacts
        - Storage media

7.4.2 Live Memory

- Live memory acquisition methods copy data in system memory (i.e., RAM). Generally, memory acquisition methods require administrator or privileged access for the system. The time required to extract all data from a system may contribute to the condition known as “smear”, where data is modified by the running system during the acquisition process creating inconsistencies in the acquired data. For additional information regarding memory acquisition see *SWGDE Best Practices for Digital Evidence Collection* [1].

- Running applications can be targeted for acquisition of their process memory. Malware and other applications such as anonymous browsers which may not be accessible after device shutdown.
- Cryptocurrency wallets and keystores may be open and accessible in a running program. Legal preparation should be made concerning the acquisition of cryptocurrency wallets, which may be necessary to acquire while a system is running.
- Encrypted communication, such as PGP (Pretty Good Privacy), requires keys to decrypt and may require exporting while the system is live. PGP provides cryptographic privacy and authentication for data communication.

7.4.3 Live File/File System Acquisition

- A live file/file system acquisition permits the examiner to acquire data which may not be accessible once the system has been shut down. This data can include mounted encryption containers, network storage, and databases. It is recommended the following should be conducted while the system is live:
  - As full disk encryption may prevent access to data after shutdown, the file system should be acquired.
  - Encryption keys such as Bitlocker keys should be exported.
  - Unsaved open files should be collected.

7.4. Forensic Boot Media Acquisition

Booting a subject computer to a specially configured forensic operating system utilizing the subject hardware to access storage media without removing it from the system.

7.4.1 Boot Loader Restrictions

- Booting from forensic distribution media (e.g., Windows FE, Paladin) provides an examiner the ability to image the storage media of the subject computer from a controlled boot environment utilizing the subject hardware. Recent changes in hardware and software architecture have affected the viability of this option.
- 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 bootloader may include disabling boot loader security in the UEFI. Booting to alternate media can require specific key combinations unique to computer manufacturers.
- UEFI implementation on a subject computer may create challenges to forensic acquisition, including:
  - UEFI restriction against booting from media not native to the subject computer preventing the use of forensic boot environments.

- Full disk encryption in conjunction with a TPM, which binds data from the storage device to the computer in which it is installed. Physical removal of storage media is not recommended.
- SecureBoot is a feature of UEFI 2.2 requiring the operating system that is attempting to load to have a valid certificate. The UEFI firmware will then validate this certificate against a database of known signatures that are loaded into firmware by the OEM at the time of manufacture. The OEM can and may update a list of revoked certificates with firmware updates in the future. Prior to allowing the loading of any boot code, the signature must be validated against this database and if none is found the system will not boot from the device presented. As of the time of this writing there are two signed Linux kernels (Ubuntu 12.10, Redhat Fedora 18) in existence but none of the forensically sound distributions have adopted one yet, but Microsoft supports SecureBoot for: Windows 8, 8.1, 10, 11 and Server 2012, 2012 R2, 2016, 2019, 2022.

7.4.2 Workarounds

- UEFI and its related technologies are inconsistently implemented by hardware and software vendors. Hardware vendors may build in varying degrees of UEFI support on a model-by-model basis. They may also include setup menus enabling UEFI features to be turned off, with the intention of allowing access, or even boot access, to non-UEFI boot media. The terminology for these options may vary, but can include “Compatibility Support Mode (CSM)” or “legacy mode”. The result is that it may be possible, in some cases, to turn off UEFI-based external boot restrictions while maintaining access to the subject device’s original boot media.
- Changing SecureBoot settings on Bitlocker enabled systems may result in the loss of stored encryption keys and require the Bitlocker recovery key to decrypt the data. If the recovery key is not available, the data may be irrecoverably lost.
- Should it not be possible to disable UEFI boot restrictions, the following workarounds may be possible:
  - Note: Examine the subject device for TPM presence prior to media removal.
  - Remove the internal storage device and image it externally (physical acquisition).
  - Image the media while the OS is running (logical acquisition).
  - Boot to a UEFI compatible boot environment such as Windows PE or Windows To Go

7.5. Targeted Collection

Acquiring selected files or content through a live, physical, or logical acquisition.

Targeted collection may be indicated for the review of large amounts of data, numerous devices, or limited-scope search authority. Considering the issues below, a selective collection may not be applicable, recommended, or acceptable in all circumstances.

- Training and experience

- Specifics of the investigation
- Time and resources available to conduct the acquisition or examination
- Legal restrictions / scope limitations
- Burden of proof (for legal cases)
- Volume of media under consideration for review
- Technical limitations
- Logistical constraints (e.g., limited bandwidth, cloud computing, and business continuity)
- Financial restrictions
- Ownership (custodian) of devices

An examiner may determine which classes or categories of artifacts are appropriate for collection. For example, an examiner conducting an analysis related to an allegation of harassment via email, may justifiably choose to limit their analysis to artifacts related to email communications.

It may be proper for an examiner to limit their review to specific areas of a device accessible only to a certain user or users (e.g., a given user's profile directory) based on the specifics of the requested examination.

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.

Targeted content could include compound and embedded files.

7.6. Forensic Cloning

A forensic clone is the process of creating a non-containerized bitstream duplicate of data from one storage media to another.

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. Media to which data is to be cloned should be sterilized prior to use.

8. Verification and Preview

Verification is the validation of the integrity of the acquired data by comparing the hash of the acquired data to the hash of the acquisition stream or source data. The process of verification might not verify all data as read from the subject media. 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 the acquisition of the intended items, review output logs or error logs for indications of failures in the acquisition process, and document (and resolve if possible) those failures as appropriate. Examiners should compute cryptographic hash values over the acquired data using a NIST-approved hash algorithm to facilitate subsequent validation of the acquired data's integrity.

Examiners should document digital evidence acquisitions per organizational policy. The documentation should include a description detailed enough to allow the definitive identification of the items 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 and time (including time zone);
- 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:

- Unique identification of the item
- 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 Digital Evidence Collection* [1] 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 [7].

11. References

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

[2] Scientific Working Group on Digital Evidence, “SWGDE Best Practices for Computer Forensic Examination”. [Online]. https://www.swgde.org/documents.

[3] Scientific Working Group on Digital Evidence, “SWGDE Requirements for Report Writing in Digital and Multimedia Forensics”. [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". [Online]. https://www.swgde.org/documents

[5] Scientific Working Group on Digital Evidence, "SWGDE Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics,". [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 Best Practices for Archiving Digital and Multimedia Evidence". [Online]. https://www.swgde.org/documents.

12. Additional Resources

“Booting UEFI imaged media with/without GPT using VMWare”. [Online]. http://justaskweg.com/?p=1093.

“Forensic Analysis of GPT disks and GUID partition tables”. [Online]. http://www.digitalforensics.ch/nikkel09.pdf.

Infosec Institute, “UEFI and the TPM: Building a foundation for platform trust”. [Online]. http://resources.infosecinstitute.com/uefi-and-tpm/.

Microsoft, “Boot Windows PE in UEFI or legacy BIOS mode”. [Online]. http://technet.microsoft.com/en-us/library/dn293283.aspx.

Microsoft, “Install Windows PE to Run from a Drive (Flat Boot or Non-RAM)”. [Online]. http://technet.microsoft.com/en-us/library/hh825045.aspx.

Microsoft, “UEFI Firmware”. [Online]. http://technet.microsoft.com/en-US/library/hh824898.aspx.

"UEFI and secure boot in depth". [Online]. http://www.zdnet.com/uefi-and-secure-boot-in-depth-7000012138/.

History

Revision	Issue Date	History
1.0 DRAFT	8/24/2017	Initial draft created and SWGDE voted to release as a Draft for Public Comment.
1.0 DRAFT	9/25/2017	Formatted and technical edit performed for release as a Draft for Public Comment.
1.0 DRAFT	1/11/2018	Update made in response to public comment. SWGDE voted to publish as an Approved document (Version 1.0).
1.0	4/25/2018	Formatted and published as Approved Version 1.0.
2.0 DRAFT	9/21/2022	Update draft and inclusion of content from documents SWGDE Capture of Live Systems and SWGDE UEFI and its Effect on Digital Forensics Imaging.
2.0 DRAFT	1/12/2023	Submitted for SWGDE vote to release as a Draft for Public Comment.
2.0	3/31/2023	SWGDE voted to release as a Draft for Public Comment; formatted for release for public comment.
2.0	6/15/2023	Minor revisions made, submitted to SWGDE to vote to release as a Final Approved Document.
2.0	7/12/2023	SWGDE voted to publish as a Final Approved Document (Version 2.0). Formatted for release as a Final Approved Document.