Scientific Working Group on Digital Evidence

SWGDE Best Practices for Remote Collection of Digital Evidence from a Networked Computing Environment

22-F-003-1.0

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

SWGDE Best Practices for Remote Collection of Digital Evidence from a Networked Computing Environment

Table of Contents

SWGDE Best Practices for Remote Collection of Digital Evidence from a Networked Computing Environment

1. Purpose

The purpose of this document is to describe the best practices for the forensic acquisition of digital evidence from remote networked devices. These processes are designed to maintain the integrity of digital evidence.

2. Scope

This document provides basic information on acquisitions of data from remote networked devices and will not include remote collection of mobile devices, online content from social media and web pages, or acquisition from cloud sources Collection of online sources such as web pages is addressed in SWGDE Best Practices for Acquiring Online Content v1.0. Collection. Collection of data from cloud sources is addressed in SWGDE Best Practices for Digital Evidence Acquisition from Cloud Service Providers v1.0 The examiner should be proficient with tools, techniques, and practices for forensic remote acquisition. 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].

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

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 the 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 must have the legal authority to collect data and forensically examine the collected data. If clarification on legal authority is needed, the examiner should consult with the appropriate legal counsel.

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]. Examiners should ascertain the appropriate means of acquiring data from identified networked sources. Examiners should be aware of the limitations of each acquisition method and consider actions to mitigate these limitations if appropriate. Consideration should be given to methods and limitation variables as they relate to various operating systems. 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 devices and minimize adverse effects as much as possible. Where it is not possible to fully prevent alterations to the source device, 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 website [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.
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.
Acquired data should be stored on a trusted platform, either physical media or network storage, configured with appropriate security controls. Secure and auditable cloud storage allows for more efficient forensic collection as the examiner can publish data directly to the cloud storage. See SWGDE Best Practices for Computer Forensic Acquisitions for additional information [8].

Obtain appropriate permissions and access on the remote endpoint, and/or intermediate endpoint, if required. This becomes more difficult with attempting cross-domain connections.

The acquisition process will require a stable and secure connection and appropriate network access. Consideration should be given to network speed acquisition capabilities as it relates to mission needs, scope, business closure times, infrastructure downtime, etc. Depending on the size of the data set being acquired this can be a huge limitation to remote collections.

Implementation will require a tool or method capable of remote collection. Tools and methodology should be secured against attack and intercept.

5. Considerations

On many networks, IP addresses are assigned dynamically and can change over time. Though IP addresses should be documented, they should not be relied upon for a host identification. Computer hostname, MAC address, or other immutable identifiers should be used when available. Also, coordination with the investigator or requester to ensure identifiers are known, such as user profile names and unique folder names may assist in properly identifying the remote connected device.

The acquisition process will require a stable and secure network connection and appropriate access to establish a connection to the source machine/device. Consideration should be given to network acquisition speed capabilities as it relates to mission needs, scope, business operating hours, infrastructure downtime, etc. Depending on the size of the dataset being acquired, inadequate network throughput may severely impact remote collections.

Additionally, time constraints may be an issue when opting to make a logical versus a physical acquisition. It is recommended to make the most comprehensive acquisition that meets the scope of the investigation.

The examiner may ship a pre-configured computer system preloaded with forensic collection applications, if network connectivity to the source machine/device is limited or if the system cannot be transported. The examiner may remotely connect to the pre-configured system and direct the end-user to attach data storage media to the system for collection.

Coordinate with the appropriate Information Technology personnel of the organization which has custody of the data to be collected. The following information would be beneficial to assist in the collection of data:

- Administrative access (network shares, servers, log locations, firewall information, etc.)
- A network map to have an understanding of infrastructure and applicable acquisition targets.

- Data retention
- Disaster recovery or backup plans

6. Triage

Examiners may need to preview the contents of potential data sources prior to acquisition. Previews may help 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 to determine its relevance to the investigation. There may be multiple iterations of triage, depending on the complexity of the investigation.

Examiners may decide to acquire a potential device, in whole or in part, based on the result of the triage process. This may depend on the scope, size of media, or time available. The focused collection of data based on an investigation or legal request 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 by utilizing validated forensic collection applications and processes. Data should be acquired in raw format or a well-documented, widely supported forensic container [3].

The following should serve as best practices for acquiring data from a remote source machine/device:

- If not currently on the source machine/device, the forensic application's servlet or agent (if used) is placed in an obscure location on the internal media so as to not interfere with the user data intended to be collected. Native operating system utilities may have to be used to establish a connection.
- Establish connectivity to remote (source) machine/device
- Establish connectivity to remote tool, if applicable
- Identify data to be collected per order of volatility [2]
- Perform acquisition
- Validate collected data

8. 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. The documentation should include a description detailed enough to allow the definitive identification of the source machine/device to the exclusion of all others. This information may include:

- Unique identifiers (e.g. make, model, serial number, and asset tag);
- Unique investigation identifiers (e.g. investigation name, case number);
- Acquisition details (e.g. type of acquisition, collection tool and version number);
- Hash value(s) of the acquired data;
- Any screen captures 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 the chain of custody of the acquired data in a format suitable for retrieval. Chain of custody documentation is addressed in SWGDE Best Practices for Computer Forensic Acquisitions v1.0.

9. Preservation

After digital evidence is collected and verified, a working copy can be created per organization policy and used for the examination. Collected digital evidence and related documentation should be retained and maintained consistent with organization policy and applicable law [8].

10. Reference Sites and Publications

[1] Scientific Working Group on Digital Evidence and Scientific Working Group on Imaging Technology, "SWGDE Minimum Requirements for Quality Assurance in the Processing of Digital and 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 Computer Forensic Acquisitions." [Online]. https://www.swgde.org/documents/published

[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/published

[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/published

[6] National Institute of Standards and Technology (NIST), Computer Forensics Tool Testing website[Online]. https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt

[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 Computer Forensic Acquisitions". [Online]. https://www.swgde.org/documents

History

Revision	Issue Date	History
1.0 DRAFT	6/9/2022	Initial draft created
1.0 DRAFT	7/15/2022	Voted for release as a Draft for Public Comment.
1.0 DRAFT	9/22/2022	Corrections/edits made, proposed for release as Final Publication