Scientific Working Group on Digital Evidence

Best Practices for Remote Collection of Digital Evidence from an Endpoint

22-F-003-2.0

The version of this document is in draft form and is being provided for comment by all interested parties for a minimum period of 60 days.

Disclaimer 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 standards, requirements, best practices, guidelines, technical notes, positions, and considerations 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.

SWGDE requests notification by email 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 submitted via the SWGDE Notice of Use/Redistribution Form or sent to secretary@swgde.org.

From time to time, SWGDE documents may be revised, updated, deprecated, 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 Regarding 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 submitted via the SWGDE Request for Modification Form or 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

All images, tables, and figures in SWGDE documents are developed and owned by SWGDE, unless otherwise credited.

Unauthorized use of the SWGDE logo or document content, including images, tables, and figures, 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 Remote Collection of Digital Evidence from an Endpoint

Table of Contents

1. Purpose

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

2. Scope

This document provides basic information on acquisitions of data from remote networked endpoints 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 21-F-001-1.1. Collection of data from cloud sources is addressed in SWGDE 19-F-002-1.0. 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 10-Q-001-1.0.

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, and additional guidance may apply [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 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 ascertain the appropriate means of acquiring data from identified endpoints. Also, examiners should consider the need to collect memory and volatile data such as metadata, encryption keys, log files, and schema information. Proper documentation is needed to access and understand the data sought in the context of the investigation [2].

Implementation will require a tool or method capable of remote collection. Tools and methodology should be secured against attack and interception. A tool that can automatically reconnect and resend data being collected is important, otherwise the collection might be dropped and data would be missed.

Examiners should be aware of the available remote acquisition methods. These methods could fall under one of the following categories:

- Server based (e.g., server connects to the source endpoint to acquire data)
- Endpoint based (e.g., tools that are already part of the operating system used, or tools that are already installed on the endpoint and could be used to acquire data
- Network based (e.g., TAP devices, port mirroring, netflow from routers, etc.),
- Removable media based (e.g., tools could be stored on a removable media and used remotely to acquire data)
- Bring Your Own (BYO), (e.g., in some cases, the examiner might bring their own tools for acquisition)

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 endpoints using novel technologies may require the use of non-traditional acquisition techniques [3].

Examiners must understand the impact a chosen acquisition method may have on the source endpoint and minimize adverse effects as much as possible. Where it is not possible to fully prevent alterations to the source endpoint, 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 [4, 5]. 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 storage destination. Sterilization of the destination is not generally required, especially with cloud storage, except when needed to satisfy administrative or organizational requirements or when a specific analysis process makes it a prudent practice. Acquired data should be stored on a trusted platform, either physical media, cloud storage, 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 [2].

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

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 endpoint.

The acquisition process will require a stable and secure network connection and appropriate access to establish a connection to the source endpoint. 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. Acquiring from locations with low bandwidth capabilities can adversely affect the network and business operations. Also, remote locations may have different data privacy laws that govern the handling/acquisition of digital media.

Additionally, time constraints may be an issue when opting to make a logical versus a physical acquisition, though 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 endpoint is limited or 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. Note- Information Technology personnel are typically not trained in forensic data collections. Proper care should be taken to brief the assisting person(s) on the chain of custody procedures and ensure proper documentation of the evidence movement and actions performed to enable remote collection. 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 endpoint, 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 [6].

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 [2].

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

- If not currently on the source machine/endpoint, 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)/endpoint,
- Establish connectivity to remote tool, Identify data to be collected per order of volatility [1],
- Perform acquisition,
- Verify collected data.

8. Documentation

Examiners should verify that the acquired data includes the intended items by thoroughly reviewing it. 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/endpoint 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. Refer to SWGDE 17-F-002-2.0 for chain of custody documentation information.

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 [3].

10. References

[1] Scientific Working Group on Digital Evidence. *Capture of Live Systems*. SWGDE 07-F-002-2.0. *SWGDE*, 5 Sep. 2014, https://www.swgde.org/wp-content/uploads/2023/11/2014-09-05-SWGDE-Capture-of-Live-Systems-V2-0.pdf

[2] Scientific Working Group on Digital Evidence. *Best Practices for Computer Forensic Acquisitions*. SWGDE 17-F-002-2.0. *SWGDE*, 15 Jun. 2023, https://www.swgde.org/17-f-002/

[3] Scientific Working Group on Digital Evidence. *Best Practices for the Acquisition of Data from Novel Digital Devices*. SWGDE 16-F-003-1.0. *SWDGE*, 21 Feb. 2017, https://www.swgde.org/16-f-003/

[4] Scientific Working Group on Digital Evidence. *Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics*. SWGDE 18-Q-001-2.1. *SWGDE*, 7 Mar. 2024, https://www.swgde.org/18-q-001-2/

[5] National Institute of Standards and Technology (NIST). *Computer Forensics Tool Testing Program (CFTT)*. NIST, Created 8 May 2017, https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt. Accessed 22 Nov. 2024.

[6] Scientific Working Group on Digital Evidence. *Focused Collection and Examination of Digital Evidence*. SWGDE 14-F-003-1.0. *SWGDE*, 5 Sep. 2014, https://www.swgde.org/14-f-003/

11. Additional Resources

- Scientific Working Group on Digital Evidence and Scientific Working Group on Imaging Technology. *Best Practices for Acquiring Online Content*. SWGDE 21-F-001-1.1. *SWGDE*, 15 Mar. 2024, https://www.swgde.org/21-f-001-2/
- Scientific Working Group on Digital Evidence and Scientific Working Group on Imaging Technology. *Best Practices for Digital Evidence Acquisition from Cloud Service Providers*. SWGDE 19-F-002-1.0. *SWGDE*, 17 Sep. 2020, https://www.swgde.org/19-f-002/
- Scientific Working Group on Digital Evidence and Scientific Working Group on Imaging Technology. *Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence*. SWGDE 10-Q-001-1.0. *SWGDE*, 15 May 2010, https://www.swgde.org/10-q-001/

12. 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	9/22/2022	Corrections/edits made, approved for release as Final publication.
2.0 DRAFT	9/19/2024	Updated document content and changed title from *Best Practices for Remote Collection of Digital Evidence from a Networked Computing Environment* to *Best Practices for Remote Collection of Digital Evidence from an Endpoint.* Moved forward for SWGDE vote for release as a Draft for Public Comment.
2.0 DRAFT	11/22/2024	SWGDE voted to approve as Draft for Public Comment. Formatted for release as a Draft for Public Comment.