Scientific Working Group on Digital Evidence

Focused Collection and Examination of Digital Evidence

SWGDE 14-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

Focused Collection and Examination of Digital Evidence

Table of Contents

1. Purpose 2
2. Scope 2
3. Limitations 2
4. Considerations 2
   - 4.1 Impartiality and Risk of Exclusion 2
   - 4.2 Training and Experience 3
   - 4.3 Specifics of Investigation 3
   - 4.4 Legal Restrictions / Scope Limitations 3
   - 4.5 Burden of Proof and Investigative Scope 3
   - 4.6 Volume of Data 4
   - 4.7 Operational Constraints in Live Environments 4
   - 4.8 Ownership (custodian) of Devices / Data 4
5. Documentation and Auditability 4
6. References 5
7. Additional Resources 5
8. History 6

1. Purpose

This document aims to guide digital forensics examiners on key considerations for managing the review of extensive data volumes and/or multiple devices.

Due to the continued rapid increase in storage media capacity, it is often impractical or impossible to perform a comprehensive forensic review without prioritizing a targeted subset of the submitted data or devices for analysis. This is not to say that a selective review is recommended or acceptable in all circumstances; however, in consideration of the issues noted below, an examiner must allocate their resources effectively to prioritize data most likely to contain relevant artifacts.

2. Scope

The primary audience for this document is digital forensic practitioners. This document provides considerations for narrowing the scope of a digital evidence collection and examination. The objective of focused data collection and examination is to optimize resource efficiency, including personnel, time, and equipment, while ensuring compliance with legal requirements such as maintaining chain of custody, adhering to privacy regulations, and preserving the admissibility of evidence in court.

3. Limitations

It should be understood this document and the considerations contained herein may not apply in some circumstances. In all cases, examiners are encouraged to consult with the requestor and/or competent legal authority having jurisdiction in their applicable venue.

4. Considerations

The following list of considerations is not intended to be all-inclusive, but should serve as a guide in circumstances where the examiner is considering the focused collection and/or examination of a subset of all data related to the investigation.

4.1 Impartiality and Risk of Exclusion

When conducting a focused or triage-based collection, examiners must remain vigilant to avoid introducing bias into the selection process. A narrowly scoped collection may inadvertently exclude exculpatory evidence—information that could support the innocence of a subject under investigation. Refer to *SWGDE 16-F-002-2.1 Considerations for Required Minimization of Digital Evidence Seizure* [1] for further guidance. To mitigate this risk, examiners should ensure that their methodology is well-documented, repeatable, and defensible. The selection criteria should be based on investigative objectives, not assumptions about guilt. Both inculpatory and exculpatory artifacts must be collected and examined with equal diligence to uphold the principles of fairness, due process, and forensic integrity.

4.2 Training and Experience

Focused collections should begin with clearly defined acquisition and examination objectives. The examiner's expertise significantly shapes the approach to focused data collection. For example, an experienced examiner may quickly recognize patterns in log files or prioritize specific file types, reducing time spent on irrelevant data and improving the quality of the analysis. Training should be ongoing to keep pace with evolving technologies and digital artifacts.

4.3 Specifics of Investigation

Each investigation has unique objectives that should dictate the focus of data collection and examination. For instance, an insider threat investigation may prioritize email correspondence and access logs, while a financial fraud case may focus on accounting records or transaction databases. Understanding the case's goals ensures only the most relevant data or devices (e.g., a suspect's laptop or server) are targeted, aligning the examination with the investigation's needs.

Examiners should maintain clear communication with investigators, legal counsel, and other stakeholders to ensure alignment on scope, expectations, and limitations. Early collaboration helps prevent misunderstandings and ensures that the collection strategy supports the overall investigative goals.

4.4 Legal Restrictions / Scope Limitations

Legal and privacy frameworks, such as General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), or jurisdictional regulations, impose constraints on data collection and examination. Privacy laws may limit access to personal data, requiring examiners to focus only on specific custodians or data types. Additionally, maintaining a proper chain of custody and adhering to court-admissible procedures is critical to ensure evidence validity. For example, an examiner may need to exclude certain data to comply with privacy regulations or limit the scope to court-approved parameters.

4.5 Burden of Proof and Investigative Scope

The standard of proof required in an investigation–whether for legal proceedings or internal policy enforcement–directly influences the scope and depth of data collection and examination. Criminal cases, which require proof "beyond a reasonable doubt", often demand a more exhaustive analysis to ensure all relevant evidence is collected. Civil cases, governed by a "preponderance of evidence" standard, may allow for a more focused approach. In contrast, internal investigations into policy violations may prioritize speed and relevance over legal admissibility, emphasizing actionable insights. Understanding the applicable burden of proof helps practitioners tailor their collection strategy to the context, balancing thoroughness with efficiency

4.6 Volume of Data

The rapid growth in digital storage media capacity, such as multi-terabyte hard drives or cloud repositories, often makes comprehensive collections and/or examinations impractical. To manage this, examiners may prioritize specific file types (e.g., user created documents, emails), time periods, or devices based on relevance. For instance, in a case involving intellectual property theft, an examiner might focus on recently modified documents rather than analyzing an entire server.

Another example is review of surveillance video which is often stored on systems with very high capacities. A specific timeframe understanding may be necessary to only acquire video frames needed.

4.7 Operational Constraints in Live Environments

Practical limitations—such as limited network bandwidth, restricted access to cloud-based data, or the need to maintain uninterrupted business operations—can necessitate a focused and adaptive collection strategy. For instance, in environments where downtime is unacceptable, such as financial transaction servers or Operational Technology (OT) systems in industrial control networks, examiners may need to use remote acquisition tools or schedule collections during maintenance windows. Similarly, in healthcare or emergency response systems, preserving system availability while collecting evidence is critical. These constraints require balancing forensic thoroughness with operational continuity.

4.8 Ownership (custodian) of Devices / Data

The ownership of devices—whether company-issued or personally owned—affects the scope of collection. Legal and privacy considerations require examiners to obtain proper authorization before accessing devices, particularly for employee-owned devices. For example, an investigation may be limited to company-issued laptops to avoid privacy violations, requiring examiners to carefully define the scope based on device ownership.

5. Documentation and Auditability

All decisions made during a focused collection or examination must be thoroughly documented. This includes, but not limited to:

- The rationale for selecting specific data sources or timeframes
- Any constraints (legal, technical, or logistical) that influenced scope
- Tools and methods used
- Any known limitations or exclusions

Proper documentation ensures transparency, supports reproducibility, and provides a defensible record in legal proceedings.

6. References

[1] Scientific Working Group on Digital Evidence. *Considerations for Required Minimization of Digital Evidence Seizure.* SWGDE 16-F-002-2.1. *SWGDE*, 2024, https://www.swgde.org/16-f-002/.

7. Additional Resources

Scientific Working Group on Digital Evidence. *Best Practices for Apple MacOS Forensic Acquisition.* SWGDE 23-F-005-1.0. *SWGDE*, 2023, https://www.swgde.org/23-f-005/.

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

Scientific Working Group on Digital Evidence. *Best Practices for Digital Evidence Acquisition, Preservation, and Analysis from Cloud Service Providers.* SWGDE 23-F-004-1.1. *SWGDE*, 2024, https://www.swgde.org/23-f-004/.

Scientific Working Group on Digital Evidence. *Best Practices for Remote Collection of Digital Evidence from an Endpoint.* SWGDE 22-F-003-2.0. *SWGDE*, 2025, https://www.swgde.org/22-f-003/.

Scientific Working Group on Digital Evidence. *Core Competencies for Digital Forensics*. SWGDE 12-F-006-2.0. *SWGDE*, 2024, https://www.swgde.org/12-f-006/.

8. History

Revision	Issue Date	History
1.0 DRAFT	06/06/2014	Original draft created and voted for release as a Draft for Public Comment.
1.0 DRAFT	06/12/2014	Formatting and technical edit completed for release as a Draft for Public Comment.
1.0 DRAFT	08/28/2014	No changes made; voted to publish as an Approved document.
1.0	09/05/2014	Formatting and technical edit performed for release as an Approved document.
2.0 DRAFT	05/20/2025	Updated Section 4, References, and currently available Additional Resources
2.0 DRAFT	06/29/2025	SWGDE voted to release as a Draft for Public Comment. Formatted for release for public comment.