Scientific Working Group on Digital Evidence

Considerations for Required Minimization of Digital Evidence Seizure

16-F-002-2.1

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

Considerations for Required Minimization of Digital Evidence Seizure

Table of Contents

1. Summary

To reduce excessive intrusion into privacy, the scope of court ordered searches of digital devices is often limited by the issuing court. In most cases, implementing these limitations is only feasible after the acquisition (or extraction) of data is completed. If a court finds it necessary to limit analysis to a specified date range or other selected data, this restriction is appropriately applied post-acquisition to avoid excluding potentially valuable in-scope information from analysis and judicial review.

2. Background

There is a growing tendency for courts to impose restrictions on the seizure of data from electronic devices, most notably mobile devices and computers, during the execution of judicially-ordered searches, such as those pursuant to a search warrant. These limiting decisions are typically made during the search authorization phase and impact the scope of the search. Limitations to the subsequent analysis of legally seized digital information are also becoming common. These limitations can have a negative impact on an investigation by causing the loss of relevant inculpatory and exculpatory information, and misinterpretation of the seized information. This document aims to describe the technological and evidentiary consequences of imposing such limitations.

This trend follows a growing concern that, as daily life becomes more dependent on technology, digital evidence examinations become more intrusive into "vast quantities of personal information." Courts are applying greater specificity and particularity requirements to protect privacy and avoid constitutionally prohibited over-broad searches and seizures.

Traditional notions of specificity and particularity often do not translate well to digital evidence and can create technical challenges to limiting the search and seizure of electronically stored information. Issues applicable to acquiring data from one type of electronic device, such as mobile phones, may not apply to other devices like computers. Relevant electronically stored information is not necessarily stored contiguously in one location, nor in an easily read or understood format. Relevant and valuable descriptive information such as metadata (e.g., date and time values), and other user attribution data, is often stored in different 'locations' on a device, separate and apart from the particular data sought. Seizure and review of all of this information is necessary for accurate analysis.

To further complicate matters, there are many ways in which information is stored on specific devices or systems. Attempts at minimization have a significant potential to exclude relevant inculpatory and exculpatory information. For this reason, (among the many historically discussed and documented reasons such as time, ease, access to tools, etc.), the necessity of acquiring the full contents of data storage devices and their media, when possible, is significant.

For the reasons discussed in detail below, it is the position of SWGDE that the technical complexities involved in extraction of data from digital devices demand that, when required, minimization measures are best conducted after the initial acquisition.

See U.S. Dept. of Justice's "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," January 2015 3rd Edition—with specific reference to Chapter 2.C.3.

3. Technical Issues Related to Limitations Imposed on Digital Evidence Acquisitions

Forensic examinations of electronic devices generally involve two primary stages: 1) acquisition of data from a device; and 2) analysis of the acquired data.

In most cases, best practice for acquiring electronically stored information is to perform the most complete type of acquisition available. While not always possible, a physical acquisition is the preferred and most complete method. A physical extraction acquires all stored data irrespective of logical arrangement or organization of the information, including data in allocated, unallocated, and recovered locations. Different combinations of acquisition methods and architecture will have differing potentials for recovered data.

For many devices, a selective extraction where only particular types of data, or data from a selected time period, are acquired is not possible. When required, it is within the second stage of examination (the analysis of the acquired data) where minimization such as category or date range limitations, should be implemented.

Once all available data has been acquired from a device, it can then be analyzed and filtered to include only in-scope data. Because accurate filtering often requires repetitive, multi-step analysis, preservation of the full body of the extracted data allows for re-filtering for relevant in-scope data without needing to re-acquire the device.

Decisions regarding minimization in the acquisition stage must be made with sufficient understanding of the technical limitations and necessary steps, and in consideration of the consequences to the forensic process, including the significant potential for exclusion of relevant in-scope information.

3.1 Compound Files

Commonly occurring on all computing systems (including mobile devices), compound files are files that contain other files. Compound files can create complications for filtering data. Compressed archives, email files, embedded documents, and others can contain categories of files different from that of the container or that have different dates. For example, a Zip archive created on an out-of-scope date could contain files with creation or modification dates that would make them in-scope, and vice versa. Word documents and PDFs can contain embedded pictures of relevance to an investigation that would be excluded by a cursory "image files only" filter. Email account storage files and email messages themselves can contain in-scope files or content, regardless of the date of the message, or the creation date of the archive. Encrypted file containers can hold entire file systems containing both in and out-of-scope data. The file system timestamps on database files only reflect the creation, modification, or access times for the database itself, not the individual records within.

Effective and accurate filtering of compound files requires appropriate analysis to ensure the filtering criteria are properly applied to the contained data. No tool or process can conduct this type of filtering prior to or during acquisition.

3.2 Acquiring Only a Targeted Profile

Search and seizure restrictions ordered to limit the scope of an examination to files found only within a specific user's "profile" (directories reserved by the operating system for that user) are problematic and can limit effective analysis of indicia of ownership. It is a common misconception that users of a multi-user operating system are effectively confined to their assigned areas of the storage media. In truth, breaking out of a designated profile to store information on other areas of the disk, including those reserved for other users, is a trivial exercise for a savvy user.

Additionally, there is a considerable amount of valuable data related to the subject user, including records of user activity, backup files, and other relevant artifacts, stored by the operating system in locations not accessible to users of the system. There are numerous artifacts throughout the drive, many outside the directories under the user's profile, that relate to the files under the subject users' control. These artifacts identify interactions with files in question including if the file had been opened, edited, modified, moved and several other factors that may be significant in determining the context of a user's knowledge of a file. Without the examination of these artifacts, the context of a user's knowledge, interaction, and possibly even intent, may be unavailable. Without a full system acquisition, these files are unavailable to the examiner.

3.3 Anti-Forensics Techniques

Savvy users often employ techniques to confound or limit an examiner's ability to discover and analyze relevant information. File timestamps are trivially easy to manipulate. Manipulation of file timestamps is a common method of hiding suspect files or making in-scope files appear out-of-scope. File timestamps should not be relied upon as the sole method for determining a file's relevance in a search. For these reasons, imposing date and time limitations on the data to be analyzed should be done, if at all, with these issues in mind.

Many computing systems use file extensions to identify types of files. Extensions such as .jpg, .gif, and .png identify the files as pictures. A user can easily change this extension (it is only part of the filename) and the operating system will no longer properly identify the filetype. In Windows, a portable network graphic (e.g., photo.png) file renamed to photo.txt will not display as an image. Users can use this "aliasing" technique to hide files. Analysis is required after acquisition to determine the true filetype prior to filtering.

4. Examples

- Multiple conversations between two individuals were reflected in the text message contents of an individual's device. A "date range" limitation encompassing only the day of the offense was imposed on the data that could be obtained from the device at issue. However, the device user's act of deleting relevant messages that occurred on that date

had removed the timestamps on these now deleted, but still recoverable messages. As a result, the imposition of a "date range" limitation on the data that could be analyzed excluded this probative evidence from the investigation.

- The probable cause in a particular case related to the viewing, downloading, and sharing of graphic images that were sexually exploitative of children within a certain date range. The court limited the forensic examination to only those dates and to only these graphic images. These limitations prevented the examiner from analyzing relevant and important contextual information such as user profiles, system clock information, other identifying system information such as network card MAC address and IP logs, information about other users of the computer, evidence of other downloading or sharing, communications regarding downloading or sharing, or relevant "other act" evidence. In short, the ability to determine when and who accessed and/or viewed, downloaded or shared the graphic images is greatly diminished by imposition of the date range. As a consequence, information that could have identified other victims was not discovered.
- If unallocated space is not specifically collected during an acquisition or an examiner is limited to a logical file copy (i.e., it only includes individual files or objects), an examiner may not be able to recover deleted, and potentially in-scope, pictures. Additionally, when pictures are 'carved' (recovered) from unallocated space in a mobile phone acquisition where either no encryption or Full Disk Encryption was present, it is common that there is no metadata associated with the reconstituted picture. While the examiner can testify to the contents of the recovered file, when assembled and viewed in appropriate software looks like a picture, the file system metadata, which could include times and dates originally saved with that picture may not be recovered. Consequently, filtering by date/time is often impossible, even post-acquisition.
- There are artifacts that may provide context to a file in question that do not have a timestamp associated with the artifact or the date/time for the artifact may be out of scope. Collecting only files that fall within a range of date/times will miss these records, which could impact the understanding of the in-scope data. This could occur where a recoverable deleted screenshot contains images of messaging conversations between the device user and another individual. Another example is internet history or download history records stored in files with created and modified dates that don't reflect the date of the records they contain. Imposing a date limitation in this case would cause relevant information to be improperly excluded.

5. Recommendations

Filtering and sorting in order to impose limitations on the search and seizure of digital evidence is an analysis function and, in most cases, only feasible after the acquisition is completed. If a court deems it necessary to limit an examiner's analysis to a specified date range or some other

limitation, this restriction is more appropriately applied post-acquisition so as not to exclude potentially valuable in-scope information from analysis and judicial review. Unlike traditional paper files and filing cabinets, targeted files cannot always be separated from their container (filing cabinet) during a search.

If the court's concerns for minimization are sufficient to justify restrictions of the types described above, there are established methods that may better achieve these goals such as filter teams, privilege reviews, and special masters, that ensure both the privacy of uninvolved parties, and the thorough execution of lawful seizures and searches.

A forensic examiner and case investigator should discuss the types of information (e.g., email, browsing history, chat logs, temporary internet files, connection logs, system information, user profile(s)) and attributes of that information (e.g., associated timestamps, metadata) that may reasonably be expected to contain information relevant to a specific investigation. These discussions should assist the drafter of the search warrant affidavit and search warrant or other legal search authorization in describing what needs to be searched for and why there is probable cause to believe that information, if it exists, may be found as described, and what, if any, technical limitations come into play during the forensic examination (e.g., automated tools).

The active participation and consultation of a digital forensics examiner prior to the drafting of search authorization document e.g., an affidavit and search warrant, may have a significant beneficial impact on the end result, as up-front education of case investigators, judges, and prosecutors regarding the unique considerations that need to be accounted for in the forensic examination of digital evidence. The desired result should be that whatever the scope of authority granted by a court in approving a search authorization, that it is not unfairly limited due to a lack of understanding or misunderstanding of technical matters by the reviewing judge.

6. History

Revision	Issue Date	History
1.0 DRAFT	5/27/2016	Initial draft created for SWGDE internal review.
1.0 DRAFT	6/9/2016	SWGDE voted to release as Draft for Public Comment.
1.0 DRAFT	6/23/2016	Formatted/edited and posted as a Draft for Public Comment.
1.0 DRAFT	9/15/2016	No changes made. SWGDE voted to publish as an Approved document.
1.0	10/8/2016	Formatted and edited to publish as an Approved document.
2.0 DRAFT	9/21/2023	Updated and forwarded to SWGDE membership for vote to release as a Draft for Public Comment.
2.0 DRAFT	10/13/2023	SWGDE voted to release as a Draft for Public Comment; formatted for release for public comment.
2.1 DRAFT	5/14/2024	Non-substantive change made to the second paragraph of section 3, as well as grammatical and punctuation corrections throughout the document. Moved forward for SWGDE membership vote to release as a Final Approved Document.
2.1	8/5/2024	SWGDE voted to release as a Final Approved Document. Formatted for release as Final Approved Document.