SWGDE Comments on Forced Minimization Requirements for the Seizure of Digital Evidence

Disclaimer:
As a condition to the use of this document and the information contained therein, 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 any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall 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; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

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 the SWGDE cover page containing the disclaimer.
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 create date) of the document and mention 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 the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) 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 change

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.

SWGDE Comments on Forced Minimization Requirements for the Seizure of Digital Evidence

Table of Contents

1. Background

There is a growing tendency to restrict the amount or types of digital information, or data, that can be seized during the execution of legally-authorized operations, such as search warrant executions. Those limiting decisions are typically being made by the investigative or legal parties during the search authorization phase, thereby impacting the scope of the search. In the same vein, limitations have also been placed on the subsequent analysis of legally seized digital information. This is a disturbing trend as it can have a negative impact on the investigation and cause, not only a loss of both inculpatory and exculpatory information, but worse, could result in the misinterpretation of information that causes detrimental consequences.

This trend seems to be a reflection by the courts of a growing concern that digital evidence examinations are becoming a "general" (i.e., unreasonable) search. General searches are not permitted under the Constitution. Specificity and particularity of what is being searched and searched for must be articulated in an affidavit and search warrant. The problem with electronically stored information is that it is not necessarily stored contiguously in one location, nor in an easily read or understood format, nor is the valuable descriptive information such as date and time values (known as metadata), or user attribution data, co-located with the actual information of relevance (the particular item authorized for seizure). All of this information together is what must be analyzed, and therefore seized, in order to produce the best possible version of investigative information.

To further complicate matters, there are so many variants in today's digital world as to how information is stored on any specific device or system that the process of pre-limiting data capture (such as seizure, imaging, or copying) is nearly impossible, if at all, without resulting in a loss of probative information. It is doubtful that the court would attempt to impose a restriction prohibiting the collection of only the subject's DNA that was inherited from his father or grandmother. It is the loss of such probative information that is concerning and possibly detrimental to the admissibility of the information. Attempts at minimization have a significant potential to exclude relevant in-scope (i.e., inculpatory) and possibly exculpatory information from collection, analysis, and judicial review. For this reason, (among the many historically discussed and documented reasons such as time, ease, access to tools, etc.[1]) the necessity to seize entire data storage devices and media is most likely necessary. Furthermore, whether data can or cannot be parsed adequately in order to perform minimization procedures at any time **must** be performed by someone that is technically knowledgeable and trained to do so.

Only when the necessary data is seized, imaged, or copied, can it be analyzed thoroughly to make a determination as to whether it fulfills the specificity and particularity required by the legal authorization. It is only during full analysis of all component parts of a specifically stored piece of information that a proper review of compliance can be attained, and the authorized

[1] See the U.S. Dept. of Justice "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations", January 2015 3rd Edition - with specific reference to Chapter 2.C.3

probative data can be made available to the investigative and judicial processes. The forensic analysis in this sense works much like a "taint team" would, e.g., prosecutors/agents not otherwise assigned to the case reviewing and excluding material not germane to the investigation/scope of the search authorization. During a digital analysis, the forensic examiner does the parsing from a non-biased perspective, but with full understanding of how the information fulfills the scope requirements.

Some examples of pre-decisional minimization instructions that have been discussed but can be practically impossible to execute include:

- Only active information can be seized; deleted data must be excluded.
- Digital acquisitions are restricted to data falling within a specified timeframe.
- Only files located with a specific user's "profile" can be copied.
- Only certain data can be imaged from digital media.

Many attempts at pre-minimization decisions are often in error, and most are probably due to a lack of sufficient understanding of the technical limitations, steps, and considerations in the digital forensic process. Technical issues aside, attempts such as these at pre-minimization can have a significant potential to exclude relevant in-scope information from collection, analysis, and judicial review. One example of the detriment that can be caused by such a decision is:

- The probable cause in a particular case relates to the viewing, downloading, and sharing of graphic images that are sexually exploitative of children within a certain date range. If a court limits a forensic examination to only those dates, and to only such graphic images, an examiner would not be able to analyze relevant and important (if not critical) 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 other *res gestae* evidence.

2. Technical Issues with the Limitations Relevant to DE

When an examiner conducts an acquisition of electronically stored information, the preferred best practice is a 'physical' acquisition where all stored data on a device is acquired irrespective of logical arrangement or organization. This method captures not only data in active "allocated" files, but also recovers (often valuable) deleted information. While subsequent analysis can be limited to a given date range or specific set of directories, unless the court intends to abandon the ability to recover deleted files, which may later be determined to be in-scope, a full physical image must first be acquired.

2.1 Deleted Data Example – Pictures

If unallocated space is not specifically collected during an acquisition or an examiner is limited to a logical file copy, an examiner will 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, it is common that there is no metadata associated with the reconstituted

picture. While the examiner can testify to the contents of the file that, 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 stamps can often not be completed, even post-acquisition.

2.2 Cell Phone Example – Extraction

In regard to a cell phone, in lieu of a physical image an examiner may be able to acquire a logical copy of the device's objects, e.g. call logs, but in doing so, will not be able to (in most cases) recover deleted information. Additionally, the examiner has no method to acquire data from a cell phone according to a specified time/date range, logically or physically.

2.3 Cell Phone Digital Artifact Example – SMS Messages

Mobile device forensic tools simply do not allow an examiner to acquire SMS/MMS messages based on specified time/date ranges. Additionally, in order to search for messages that may have been deleted, depending on the type of phone, an examiner either needs a physical image (feature phone) or at a minimum, a full copy of the database that holds the messages (smart phone, but still will potentially miss items no longer of record). Once the acquisition(s) is (are) completed, an examiner will need to add the entire image, or database, into software to then sort and exclude items out of the specified date/time range. Additionally, while the message content may be recovered, other items, such as time/date stamps and sender/receiver numbers, may not be able to be recovered, thus eliminating the ability to filter/view only specific times/dates.

2.4 Anti-Forensics Techniques

Savvy users often employ techniques to confound or limit an examiner's ability to discover and analyze relevant information. Many of these methods involve the manipulation of file system time and date information. Timestomping, or directly changing these values, is one such method that is used to change the date-time stamp of in an-scope file, to appear out-of-scope.

Additionally, any file can be (even innocuously) placed into a (possibly encrypted) container or archive with a much newer date/time stamp, which obscures its contents. Without acquiring and subsequently analyzing all files, the examiner has no way to discover these containers and determine the relevancy of their contents.

2.5 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. This restriction is based upon an incorrect belief that users of a multi-user operating system are effectively confined to their assigned areas of the storage device. In truth, breaking out of a designated profile to store information on other areas of the disk, including those reserved for other users, can be a trivial exercise for a savvy user.

Unallocated storage space, which would contain deleted files, is not assigned to specific users. Therefore, information written by one user to a file that is subsequently deleted can be

incorporated into another user's storage space when that space is later allocated to store the second user's files.

Additionally, there is a considerable amount of valuable data related to the targeted user, as well as records of user activity, backup files, and other relevant artifacts, stored by the operating system in locations not accessible to users of the system. Lastly, aside from the file itself, there are numerous digital artifacts throughout the drive, many outside the directories under the user's profile that relate to the file in question. These additional digital artifacts identify interactions with the file 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 additional digital artifacts, the context of a user's knowledge, interaction, and possibly even intent, some of which may be exculpatory, may be unavailable. Without a full physical acquisition, these files are unavailable to the examiner.

3. Appropriate Limited Acquisitions

There are situations where an on-scene, focused collection of data specified by certain criteria, such as date range or logical container, is appropriate, e.g., recovering data from a third-party server in a data center. In this situation, the examiner may have no choice but to conduct a collection of the storage device on scene from a live system and if necessary, only collect files within a specified date/time range or from specified directories. It should be noted that there are digital artifacts that may provide context to a file in question that do not have a date or time associated with the digital artifact. Collecting only files that fall within a range of date/times will miss these digital artifacts.

4. Recommendation

Time and date sorting as well as user attribution is an analysis function and, in many cases, only feasible after the acquisition (logical or physical) is completed. If a court deems it necessary to limit an examiner's analysis to a specified date range, this restriction is more appropriately applied post-acquisition so as not to exclude potentially valuable in-scope or exculpatory information from analysis and judicial review. Unlike traditional paper files and filing cabinets, the targeted file cannot be separated from the container (filing cabinet) during a search. The nature of digital evidence is a structure of 1's and 0's that are not as easily separated and require the entire container to be seized for proper digital investigation.

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 taint teams, privilege reviews, and special masters, that ensure both the privacy of uninvolved parties, and the thorough execution of lawful seizures and searches. While the judicial remedy of suppression is also available to a court when a constitutional or, if prescribed by law, statutory violation has occurred, there may be other adverse consequences an examiner or the prosecution may face in a case. Timely consultation with competent legal counsel may be advisable.

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 time/date stamps, 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.

SWGDE Comments on Forced Minimization Requirements for the Seizure of Digital Evidence

History

Revision	Issue Date	Section	History
Draft	5/27/2016	All	Initial draft created for SWGDE internal review.
1.0	06/09/2016	--	SWGDE voted to release as a Draft for Public Comment.
1.0	06/23/2016	All	Formatted/edited and posted as a Draft for Public Comment.
1.0	09/15/2016	--	No changes made. SWGDE voted to publish as an Approved document.
1.0	10/08/2016	All	Formatted and edited to publish as an Approved document.