SWGDE Focused Collection and Examination 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 Focused Collection and Examination of Digital Evidence

Table of Contents

1. Purpose

The purpose of this document is to provide the examiner with considerations to address when dealing with the review of large amounts of data and/or numerous devices.

With the exponential growth of storage media volume, in many situations it has become impractical if not impossible to conduct a forensic review without focusing on a subset of the data or devices submitted 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 wisely apportion their resources to review a selection of the data where the pertinent artifacts are most likely to be found.

2. Scope

This document is targeted toward digital forensic examiners and provides considerations for narrowing the scope of an examination. The goal of a focused examination is to maximize efficiency and utilization of resources, including personnel, time, and equipment.

3. Limitations

It should be understood that 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 targeted collection and/or examination of a subset of all data related to the investigation.

- Training and experience
- Specifics of the investigation
- Time and resources available to conduct the examination
- Legal restrictions / scope limitations
- Burden of proof (for legal cases)
- Volume of media under consideration for review
- Technical limitations
- Logistical constraints (e.g., limited bandwidth, cloud computing, and business continuity)
- Financial restrictions
- Ownership (custodian) of devices

Triage is an ongoing process that may require multiple iterations and refinements in the course of an individual investigation.

5. Artifacts

Given the above considerations relating to the case at-hand, it is acceptable for an examiner to determine which classes or categories of artifacts are appropriate for examination.

For example; an examiner conducting an analysis related to an allegation of harassment via email, may justifiably choose to limit their analysis to artifacts related to email communications.

Additionally, in some cases it may be proper for an examiner to limit their review to specific areas of a device accessible only to a certain user or users (e.g., a given user's profile directory) based on the specifics of the requested examination.

6. Reference Sites and Publications

1. *SWGDE Best Practices for Computer Forensics*, Section: Triage/Preview
   Available: https://www.swgde.org/documents/Current%20Documents
2. NIST Special Publication 800-101 Revision 1: Guidelines on Mobile Device Forensics. Section: On-Site Triage Processing
   Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf
3. Computer Forensics Case Assessment and Triage by Harry Parsonage.
   Available:
   http://computerforensics.parsonage.co.uk/triage/ComputerForensicsCaseAssessmentAndTriageDiscussionPaper.pdf

SWGDE Focused Collection and Examination of Digital Evidence

History

Revision	Issue Date	Section	History
1.0	06/06/2014	All	Original draft created and voted for release as a Draft for Public Comment.
1.0	06/12/2014	All	Formatting and technical edit completed for release as a Draft for Public Comment.
1.0	08/28/2014	None	No changes made; voted to publish as an Approved document.
1.0	09/05/2014	All	Formatting and technical edit performed for release as an Approved document.