Scientific Working Group on Digital Evidence

SWGDE Best Practices for Computer Forensics

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 user's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived for future reference, as needed, in accordance with that organization's policies.

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.

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

PURPOSE

The purpose of this document is to describe the best practices for computer forensics. This document is not all inclusive and does not contain information relative to specific operating systems or forensic tools. If you are not a computer forensic specialist, you should consult with one before proceeding. If you are dealing with technology outside your area of expertise, consult with an appropriate specialist.

1.0 Seizing Evidence

General guidelines concerning the seizing of evidence are provided as follows:

- Consult with the investigating officer to determine the necessary equipment to take to the scene.
- Review the legal authority to seize the evidence, ensuring any restrictions are noted. If necessary during the execution of the seizure, obtain additional authority for evidence outside the scope of the search.
- When it is impractical to remove the evidence from the scene, the evidence items should be copied or imaged according to local procedures.
- All suspects, witnesses, and by-standers should be removed from the proximity of digital evidence, ensuring that the above individuals are not in possession of potential evidence.
- Solicit information from potential suspects, witnesses, LAN administrators, etc. to ascertain knowledge of the system to be seized (e.g., password(s), operating system(s), screen name, email address.
- Scene should be searched systematically and thoroughly for evidence.

Searchers should be able to recognize the different types of evidence.

1.1 Evidence Handling

If the computer is turned off, ***do not*** turn on the computer.

A computer forensic specialist should be consulted when available.

- Before powering down a computer, consider the potential of encryption software being installed on the computer or as part of the operating system. If present, appropriate forensic methods should be utilized to capture the encrypted data before the computer is powered down.
- Assess the power need for devices with volatile memory and follow agency policy for the handling of those devices.
- Document the condition of the evidence.
    - Take legible photographs (screen, computer front and back, and area around the computer to be seized) and/or make a sketch of the computer connections and surrounding area.
- Appropriately document the connection of the external components.
- Note and document any pre-existing damage to the evidence.

1.1.1. Stand-alone computer (non-networked)

- Disconnect all power sources by unplugging from the back of the computer. Also, remove batteries from laptops.
- Place evidence tape over the power plug connector on the back of the computer.

1.1.2. Networked computer

- Workstations: remove the power connector from the back of the computer
- Place evidence tape over the power plug connector on the back of the computer.

Note: Any network computer can be used for file sharing and those systems should follow normal shut down procedures.

1.2 Servers

- A determination should be made as to the extent of data that should be seized.
- Capture volatile data if necessary.
- If shutdown is necessary, use the appropriate commands.

Warning: Pulling the plug could severely damage the system; disrupt legitimate business; and/or create officer and department liability.

- Each piece of evidence should be protected from change and a chain-of-custody maintained as determined by agency policy. Appropriate packaging of evidence can include any of the following:
    - Plastic/paper bags or sleeves.
    - Computer case sealed with evidence tape over case access points and power connector.
    - Devices with volatile memory should be packaged appropriately to allow for power to be maintained to the device.
- Specific care should be taken with the transportation of digital evidence material, to avoid physical damage, vibration, and the effects of magnetic fields, electrical static, and large variations of temperature and humidity.

2.0 Equipment Preparation

"Equipment" in this section refers to the non-evidentiary hardware and software the examiner utilizes to conduct the forensic imaging or analysis of the evidence.

- Equipment must be monitored and documented to ensure proper performance is maintained.
- Only suitable and properly operating equipment shall be employed.
- The manufacturer's operation manual and other relevant documentation for each piece of equipment should be accessible.
- Analysis/Imaging software should be validated prior to use as discussed in the "*SWGDE Recommended Guidelines for Validation Testing*."

3.0 Forensic Imaging

- Examiner should be trained as discussed in the "*SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence*."
- Document the current condition of evidence.
- Precautions should be taken to prevent exposure to evidence that may be contaminated with dangerous substances or hazardous materials.
    - All items submitted for forensic examination should be examined for the integrity of their packaging. Any deficiency in the packaging, which may compromise the received value of the examination, should be documented. Consideration should be given if the deficiency in packaging warrants the refusal to conduct the examination. Any exceptions between the inventory and the actual evidence by the examiner should be documented.
- Hardware or software write blockers are to be used to prevent the evidence from being modified.
- Methods of acquiring evidence should be forensically sound and verifiable.
- Forensic image(s) should be captured using hardware/software that is capable of capturing a "bit stream" image of the original media.
- Digital Evidence submitted for examination should be maintained in such a way that the integrity of the data is preserved. Additional information on data integrity can be located in the following White Paper "*SWGDE Data Integrity within Computer Forensics".*
- Properly prepared media should be used when making forensic copies to insure no commingling of data from different cases.
- Forensic image(s) should be archived to media and maintained consistent with departmental policy and applicable laws.

4.0 Forensic Analysis/Examination

- Examiner should be trained as discussed in the "*SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence*."
- Examiner should review documentation provided by the requestor to determine the processes necessary to complete the examination and ascertain legal authority to perform the requested examination. Examples of such authority include: consent to search by owner, search warrant, or other legal authority.
- Consideration should be given to the following before commencing any examination:
    - The urgency and priority of the requestor's need for information
    - The other types of forensic examination, which may need to be carried out on the evidentiary item.
    - Which items offer the best choice of target data in terms of evidentiary value.
- An examination strategy should be agreed upon and documented between the requestor and examiner.
- Conducting an examination on the original evidence media should be avoided if possible. Examinations should be conducted on forensic copies or via forensic image files.
- Appropriate controls and standards should be used during the examination procedure.
- Examination of the media should be completed logically and systematically consistent with the agency's SOPs.

4.1 Forensic Analysis/Examination of Non-Traditional Computer Technologies

With the rapid development of technologies such as cell phones, PDA's, iPod's, DVR systems, and gaming systems, etc., traditional forensic techniques and procedures may not be appropriate nor effective in the processing of this type of data.

All attempts should be made to utilize accepted best practices and procedures when processing electronic digital devices in a non-traditional format. If these techniques are ineffective and/or not appropriate for the analysis of this type of data, alternate procedures may be used. All non-traditional techniques, if possible and feasible should be tested and/or validated prior to the application on the original media. All steps of the methodology utilized should be documented.

5.0 Documentation

Evidence handling documentation should include:

- copy of legal authority,
- chain of custody,
- the initial count of evidence to be examined,
- information regarding the packaging and condition of the evidence upon receipt by the examiner,
- a description of the evidence, and
- communications regarding the case.

Examination documentation should:

- be case specific, and contain sufficient details to allow another forensic examiner, competent in the same area of expertise, to be able to identify what has been done and to access the findings independently.

Documentation should be preserved according to the examiner's agency policy.

6.0 Reports

- Examination reports should meet the requirements of the examiner's agency.
- Reports issued by the examiner should address the requestor's needs.
- The report is to provide the reader with all the relevant information in a clear and concise, manner.

7.0 Review

- The examiner's agency should have a written policy establishing the protocols for technical/peer and administrative review.

The examiner's agency should have a written policy to determine the course of action if an examiner and reviewer fail to reach agreement.

Revision	Issue Date	Section	History
1.0	11/15/04	All	**Original Release**
2.0	4/12/06	All	Added Section 4.1 Forensic Analysis/Examination Of Non-Traditional Computer Technologies. Added additional bullet under Section 3.0 Forensic Imaging.
2.1	7/19/06	All	Clarified Section 1.1 Evidence Handling. Added "and a chain-of-custody maintained".