Designation: E2763 – 10

Standard Practice for Computer Forensics[1]

This standard is issued under the fixed designation E2763; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This practice describes techniques and procedures for computer forensics within the context of a criminal investigation.

1.1.1 This practice can be applicable to civil litigation.

1.2 This practice describes seizing possible evidence, proper evidence handling, digital imaging, forensic analysis/examination, evidence-handling documentation, and reporting.

1.3 This practice is not all inclusive and does not contain information relative to specific operating systems or forensic tools.

1.4 The values stated in SI units are to be regarded as standard. No other units of measurement are included in this standard.

1.5 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety and health practices and determine the applicability of regulatory limitations prior to use.*

2. Referenced Documents

2.1 *ASTM Standards:*[2]

E2678 Guide for Education and Training in Computer Forensics

2.2 *SWGDE Standards:*[3]

Recommended Guidelines for Validation Testing

3. Significance and Use

3.1 The purpose of this practice is to describe techniques and procedures for computer forensics in regard to evidence handling, computers, digital imaging, and forensic analysis and examination.

3.2 The examiner should be trained in accordance with Guide E2678.

3.3 Individuals not trained in proper digital evidence procedures should consult with an appropriate specialist before proceeding.

3.4 When dealing with technology outside your area of expertise, consult with an appropriate specialist before proceeding.

4. Seizing Evidence

4.1 General guidelines concerning the seizing of evidence are:

4.1.1 Consult with the investigator or responsible party to determine the necessary equipment to take to the scene.

4.1.2 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.

4.1.3 When it is impractical to remove the evidence from the scene, the evidence items shall be copied or imaged according to organizational policy.

4.1.4 All suspects, witnesses, and bystanders shall be removed from the proximity of digital evidence to ensure the integrity of potential evidence.

4.1.5 Solicit information from potential suspects, witnesses, system administrators, and so forth, to ascertain knowledge of the systems to be seized (for example, password(s), operating system(s), screen names, remote access users, and E-mail addresses).

4.1.6 The scene shall be searched systematically and thoroughly for evidence. Searchers shall be trained to recognize the different types of evidence. Check for additional media that may be attached to the computer system.

5. Evidence Handling

5.1 Document the scene, which can include: taking clear, detailed photographs (of the computer screen, of the front and back of the computer, and of the area around the computer to be seized) and making a sketch/notation of the computer connections and surrounding area, or both.

5.2 If the computer is turned off, **DO NOT** turn on the computer.

---

[1] This practice is under the jurisdiction of ASTM Committee E30 on Forensic Sciences and is the direct responsibility of Subcommittee E30.12 on Digital and Multimedia Evidence.

Current edition approved Aug. 15, 2010. Published September 2010. DOI: 10.1520/E2763-10.

[2] For referenced ASTM standards, visit the ASTM website, www.astm.org, or contact ASTM Customer Service at service@astm.org. For *Annual Book of ASTM Standards* volume information, refer to the standard's Document Summary page on the ASTM website.

[3] Available from Scientific Working Group on Digital Evidence (SWGDE), http://www.swgde.org/documents.

5.2.1 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 used to capture the unencrypted data and any volatile data that would be lost if the computer is powered down.

5.2.2 Be aware that storage devices may not be physically connected and a proper search for wireless devices must be conducted.

5.2.3 Assess the power needs for devices with volatile memory and follow organizational policy for the handling of those devices.

5.2.4 Document the condition of the evidence, including any preexisting damage.

5.2.5 Appropriately document the connection of the external components.

5.3 *Stand-Alone Computer (Non-Networked):*

5.3.1 Disconnect all power sources by unplugging from the back of the computer. Also, remove batteries from laptops.

5.3.2 Place evidence tape over the power plug connector on the back of the computer.

5.4 *Networked Computer:*

5.4.1 *Workstations*—Remove the power connector from the back of the computer.

5.4.2 Place evidence tape over the power plug connector on the back of the computer.

NOTE 1—Any network computer can be used for file sharing and those systems should follow normal shutdown procedures.

5.5 *Servers:*

5.5.1 Determine whether the network connection should be disconnected after consulting with an individual trained in proper digital evidence procedures.

5.5.2 A determination shall be made as to the extent of data that should be seized.

5.5.3 Capture volatile data if necessary.

5.5.4 If shutdown is necessary, use the appropriate commands. (**Warning—**Pulling the plug could severely damage the system, disrupt legitimate business, or create officer and department liability, or combinations thereof.)

5.6 Each piece of evidence shall be protected from change and a chain of custody maintained as determined by organizational policy. Appropriate packaging of evidence can include any of the following:

5.6.1 Plastic/paper bags or sleeves;

5.6.2 Computer case sealed with evidence tape over case access points and power connector;

5.6.3 Some devices may require power to maintain the volatile memory and should be packaged appropriately; and

5.6.4 Specific care shall be taken with the transportation of digital evidence material to avoid physical damage, vibration, and the effects of magnetic fields, static electricity, and large variations of temperature and humidity.

6. Equipment Preparation

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

6.1.1 Equipment shall be monitored and documented to ensure proper performance is maintained.

6.1.2 Only suitable and properly operating equipment shall be used.

6.1.3 The manufacturer's operation manual and other relevant documentation for each piece of equipment shall be accessible.

6.1.4 Analysis/imaging software shall be validated before use as discussed in the SWGDE Recommended Guidelines for Validation Testing.

7. Forensic Imaging

7.1 Document the current condition of evidence.

7.2 Take precautions to prevent exposure to evidence that may be contaminated with dangerous substances or hazardous materials.

7.2.1 All items submitted for forensic examination shall be examined for the integrity of their packaging. Any deficiency in the packaging, which may compromise the received value of the examination, shall be documented. Consideration shall be given if the deficiency in packaging warrants the refusal to conduct the examination. Any exceptions between the inventory and the actual evidence discovered by the examiner shall be documented.

7.3 Hardware or software write blockers should be used to prevent the evidence from being modified.

7.4 Methods of acquiring evidence should be forensically sound and verifiable.

7.5 Forensic image(s) should be captured using hardware/software that is capable of capturing a "bit stream" image of the original media.

7.6 Digital evidence submitted for examination shall be maintained in such a way that the integrity of the data is preserved, for example, use a hashing function.

7.7 Properly prepared media shall be used when making forensic copies to ensure no commingling of data from different sources.

7.8 Forensic image(s) shall be archived to media and maintained consistent with departmental policy and applicable laws.

8. Forensic Analysis/Examination

8.1 The examiner shall 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.

8.2 Before commencing any examination, consider:

8.2.1 The urgency and priority of the requestor's need for information and the time conditions contained in the search authorization;

8.2.2 The other types of forensic examination that might need to be carried out on the evidentiary item; and

8.2.3 Which items offer the best choice of target data in terms of evidentiary value.

8.3 The requestor and the examiner should identify the scope and purpose of the examination.

8.4 Conducting an examination on the original evidence media should be avoided. Examinations should be conducted on forensic copies or via forensic image files.

8.5 Use appropriate controls and standards during the examination procedure.

8.6 Conduct the examination of the media in a manner consistent with the laboratory's standard operating procedures (SOPs).

8.7 *Forensic Analysis/Examination of Nontraditional Computer Technologies:*

8.7.1 With the rapid development of technologies such as cell phones, smart phones, personal digital assistants (PDAs), portable digital audio players, digital video recorder (DVR) systems, gaming systems, and so forth, traditional digital forensic techniques and procedures may not be appropriate nor effective in the processing of this type of data.

8.7.2 All attempts shall be made to use accepted practices and procedures when processing electronic digital devices with a nontraditional format. If these techniques are ineffective or not appropriate for the analysis of this type of data or both, alternate procedures may be used. All nontraditional techniques, if possible and feasible, shall be tested or validated or both before the application on the evidentiary media. All steps of the methodology used shall be documented.

9. Documentation

9.1 Evidence-handling documentation shall include:

9.1.1 Copy of legal authority,

9.1.2 Chain of custody,

9.1.3 Initial count of evidence items to be examined,

9.1.4 Information regarding the packaging and condition of the evidence upon receipt by the examiner,

9.1.5 Description of the evidence, and

9.1.6 Communications regarding the case.

9.2 Examination documentation shall 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 access the findings independently.

9.3 Documentation shall be preserved according to the examiner's organizational policy.

10. Report

10.1 Examination reports shall meet the requirements of the examiner's organization.

10.2 Reports issued by the examiner shall address the requestor's needs.

10.3 The report is to provide the reader with all the relevant information in a clear and concise manner.

11. Review

11.1 The examiner's organization shall have a written policy establishing the protocols for technical/peer and administrative review.

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

12. Keywords

12.1 computer data; computer forensic analysis; computer forensics; computers; evidence; software; volatile memory