

THE MASSACHUSETTS CYBERCRIME INITIATIVE  
RECOMMENDED MINIMUM STANDARDS FOR  
DIGITAL EVIDENCE ANALYSIS

---

VERSION 1  
SEPTEMBER, 2009

**CONTENTS**

**ADMINISTRATION**

1. DEFINITION OF TERMS USED IN THIS MANUAL..... 2

2. MISSION STATEMENT ..... 4

3. SCOPE ..... 5

4. RATIFICATION OF THIS MANUAL ..... 6

5. DEVIATION FROM PROCEDURE ..... 7

**QUALITY CONTROL**

6. DIGITAL EVIDENCE ANALYSIS LABORATORY ..... 8

7. PERSONNEL ..... 11

8. PERSONNEL – TRAINING AND PROFICIENCY..... 13

9. LABORATORY EQUIPMENT TESTING..... 15

10. AUDIT AND REPORTING ..... 16

**STANDARD PROCEDURES FOR DIGITAL EVIDENCE ANALYSIS**

11. CASE PROCEDURE ..... 17

12. EVIDENCE PROCEDURE ..... 20

13. DIGITAL EVIDENCE ANALYSIS PROCEDURE ..... 24

14. REPORT PROCEDURE..... 29

15. CASE REVIEW PROCEDURE ..... 31

## DEFINITIONS OF TERMS USED IN THIS MANUAL

- 1.1 Although many of the definitions below are generally applicable to the field, they are intended for use only in the interpretation of the provisions of this Manual.
- 1.2 *Derivative Evidence* – a term used broadly to identify any data that is extracted, copied, or produced from original evidence. In this context, the term “copied” includes the creation of physical images as well as copying logical files or other data from original evidence. In this context, the term “produced” includes printed items and photographs of screens.
- 1.3 *Digital Evidence Analysis* - the process of identifying, collecting, analyzing, and reporting on the presence and interpretation of data stored on digital media and technical devices. The word *Analysis* is used interchangeably with the word *Examination*.
- 1.4 *Digital Evidence Analyst* – a term defined in Section 7.5 of this Manual.
- 1.5 *Intake Area* – a location designated for the initial receipt of evidence into the laboratory.
- 1.6 *Laboratory* – the physical facility, facility, or areas designated to the Unit to perform digital evidence analysis.
- 1.7 *Laboratory Administration Archive* – the location for the retention and storage of administrative and quality control records identified in this Manual.
- 1.8 *Laboratory Director* – a term defined in Section 7.4 of this Manual.
- 1.9 *Laboratory Equipment* – any technical device or software primarily designated to perform digital evidence analysis. The term Laboratory Equipment is meant to include Digital Forensic Analysis Workstations.
- 1.10 *Mobile Devices* – a term used broadly to identify easily moved and transported technical devices that process, transmit, or store data (including cellular phones, GPS devices, personal digital assistants, smart phones, and similar devices).
- 1.11 *Non-Repeatable Procedure* – a digital evidence analysis procedure that can not be repeated for any reason due to the nature of the evidence. Although not an exhaustive list, there are two illustrative occasions where non-repeatable procedures are most

frequently performed. The first occasion is where the procedure involves the collection or analysis of volatile data (data lost when the power to the device is eliminated). The second occasion is where the procedure is performed on original evidence to which the analyst has limited access, including situations where it will not be taken into laboratory custody for further analysis.

- 1.12 *Original Evidence* – a term used to identify any original technical device or digital media that is part of a digital evidence examination by unit personnel.
- 1.13 *Parent Agency* – the agency, or affiliation of agencies, having ultimate supervisory power over the operations of the unit and laboratory.
- 1.14 *Processing* – a term used to identify the period(s) of time during a digital evidence examination when original evidence is being physically examined or copied.
- 1.15 *Quality Control Documents* – a term used to identify any document (including this Manual) or form used to implement or administer laboratory and unit quality standards.
- 1.16 *Secure Evidence Storage Area* – an area within the laboratory or on the respective agency's physical premises designated for the secure storage of evidence not being processed.
- 1.17 *Unit* – the collective group of individuals formally cleared to perform the specific tasks identified in Section 7 of this Manual.
- 1.18 *Workstation* – a computer system used to perform digital evidence examinations.

## MISSION STATEMENT

- 2.1 Digital evidence analysis is the process of identifying, collecting, analyzing, and reporting on the presence and interpretation of data stored on digital media to prove or support facts in an official, administrative, or legal proceeding.
- 2.2 The mission of the unit is to perform digital evidence analysis.
- 2.3 The unit is committed to conducting examinations in an objective and diligent manner.
- 2.4 The unit is committed to the continued improvement and development of its laboratory, and unit personnel, to maintain the highest standards of competency and proficiency.
- 2.5 The members of the unit are dedicated to the highest standard of integrity.
- 2.6 To accomplish these goals, the unit and laboratory adopt the provisions detailed here (hereinafter collectively referred to as the “Manual”).
- 2.7 The parent agency should dedicate necessary available resources to the laboratory and unit to ensure that digital evidence examinations are conducted in accordance with accepted industry best practices and the provisions of this Manual.

## SCOPE

- 3.1 This Manual details minimum quality control standards for the laboratory and unit.
- 3.2 This Manual details minimum standard operating procedures for digital evidence examinations performed by the unit personnel.
- 3.3 Personnel designated for assignment to the unit must be formally appointed by the respective parent agency and laboratory director.
- 3.4 This Manual sets forth minimum standards for personnel appointed to the unit in the performance of the duties described below.
  - 3.4.1 Conducting digital evidence examinations in the lab or the field.
  - 3.4.2 Performing tasks incident to laboratory operations.
  - 3.4.3 Performing tasks detailed in this Manual.
  - 3.4.4 Assisting other law enforcement agents with the search for and seizure of digital evidence.

## **RATIFICATION OF THIS MANUAL**

- 4.1 This Manual is effective on the date of ratification by the laboratory director and the executive in charge of the agency.
- 4.2 Ratification is official when this Manual is signed by the laboratory director and the executive in charge of the agency.
- 4.3 The version and date of the Manual should be detailed on each page of the Manual.
- 4.4 The Manual should be reviewed on an annual basis in accordance with applicable provisions of Section 10.
- 4.5 The Manual may be amended.
- 4.6 Amendments should be ratified in accordance with Sections 4.1 and 4.2.
- 4.7 The current Manual, including amendments, should be posted in one location in electronic or paper form where it can be easily accessed by all unit personnel.
- 4.8 All unit personnel should be notified that an amendment to the Manual is official and posted.
- 4.9 The notification of the posting of amendments to this Manual should be documented in the laboratory administration archive.

## DEVIATION FROM PROCEDURE

- 5.1 Digital evidence analysis is a dynamic field integrating law and technology. The law, technical requirements, training needs, and best practices relating to digital evidence analysis change frequently.
- 5.2 Deviations from the provisions of this Manual should be avoided to the extent possible but are expected and acceptable when done in accordance with proper procedure.
- 5.3 A deviation from the provisions of this Manual should be documented in the respective case file (if case related) or the laboratory administration archive.
- 5.4 Personnel may deviate from applicable provisions of this Manual where there is a conflict between the respective provision of the Manual and a statute, court decision, or court order.
- 5.5 Whenever possible, a lab supervisor should be notified before and approve of the deviation.
- 5.6 A supervisor may deny a deviation. In the event of a denial, the supervisor should recommend an alternative course of action.
- 5.7 If the supervisor can not be notified of the deviation in advance, the respective personnel should do the following.
  - 5.7.1 Exercise professional discretion in consideration of accepted best practices.
  - 5.7.2 Validate the alternative procedure before use (if applicable).
  - 5.7.3 Document the actions and the reason for the deviation.
  - 5.7.4 Notify a supervisor as soon as possible after the deviation.
- 5.8 A supervisor may take any remedial action necessary to prevent future deviation, including amendment to the Manual.

## **DIGITAL EVIDENCE ANALYSIS LABORATORY**

### 6.1 Physical Standards

- 6.1.1 The laboratory facility should meet parent agency health and safety standards.
- 6.1.2 The laboratory facility should be generally neat and orderly.
- 6.1.3 Access to the laboratory facility should be restricted to authorized personnel.
- 6.1.4 Doors to the facility and/or any secure locations within the facility where original evidence is stored or processed should remain locked at all times.
- 6.1.5 The laboratory facility should have a secure evidence storage area.
- 6.1.6 Access to the secure evidence storage area should be restricted to authorized personnel.
- 6.1.7 Non-unit personnel entering areas where evidence is present should be chaperoned by unit personnel.
- 6.1.8 There should be a log of all persons entering secure evidence storage locations that details the name, date, and time of entry.
- 6.1.9 Logs of secure evidence location access should be retained in the laboratory administration archive.
- 6.1.10 The laboratory facility should have a designated location for the initial intake (hereinafter "Intake Area") and inspection of evidence.
- 6.1.11 The intake area should remain orderly. While in use, the intake area should be designated to one case at one time.
- 6.1.12 Any location in the laboratory facility or other secure evidence storage area where original evidence will be stored or processed should be free from electro-static fields, extreme environmental conditions, and moisture.

6.1.13 The parent agency should determine who has access to the laboratory facility and designated areas within the facility.

## 6.2 Laboratory Equipment

6.2.1 Laboratory equipment should be used for official laboratory purposes.

6.2.2 Laboratory equipment should be properly maintained and upgraded.

6.2.3 Laboratory equipment should be properly acquired, inventoried, and licensed.

6.2.4 Documentation related to the acquisition of lab assets should be retained in the laboratory administration archive.

6.2.5 Manuals, documentation, and other maintenance records relating to laboratory equipment should be stored (in any format) and made readily available to unit personnel.

6.2.6 Laboratory equipment that can no longer produce reliable examination results should be discontinued from use.

6.2.7 Laboratory equipment that is loaned out for use by individuals not assigned to the unit should be inspected to ensure proper working order before next use.

## 6.3 Digital Evidence Analysis Workstations

6.3.1 Hardware and software used to conduct digital evidence analysis should be maintained by authorized unit personnel.

6.3.2 Unit personnel should ensure that digital evidence analysis workstations, including hardware and software, are in proper working order.

6.3.3 Digital evidence analysis workstations should be secured to prevent physical or virtual access to evidence by unauthorized persons.

## 6.4 Laboratory Administration Archive

- 6.4.1 The laboratory director should store documents and records relative to the administration of the laboratory.
- 6.4.2 These records should be saved in a secure location and archived according to department or laboratory policy.
- 6.4.3 These records should include, but are not limited to, documents designated for retention in this Manual.
- 6.4.4 Case files should be maintained and archived in accordance with Section 11.
- 6.4.5 Evidence should be maintained and archived in accordance with Section 12.
- 6.4.6 The laboratory should have a library of educational, training, and instructional resources for use by unit personnel. The library may be in digital format.

## PERSONNEL

- 7.1 Personnel should be formally appointed to the unit.
- 7.2 The unit should have an organizational chart detailing the chain of command.
- 7.3 Unit personnel should not engage in activities that diminish confidence in their professional competence, judgment, integrity, or impartiality.
- 7.4 Laboratory Director (Job Description)
  - 7.4.1 The unit should have a laboratory director appointed by the parent agency's executive authority.
  - 7.4.2 The title for the laboratory director should be determined by the parent agency's executive authority.
  - 7.4.3 The laboratory director should be responsible for any duty described in this Manual.
  - 7.4.4 The laboratory director should be responsible for all operations of the laboratory and the work of unit personnel.
  - 7.4.5 The laboratory director should be a person of integrity and high ethical standards with the education, knowledge, training, and experience to perform competently.
  - 7.4.6 The laboratory director should be responsible for clearing all unit personnel to perform their job duties in accordance with Section 7.7.
  - 7.4.7 The laboratory director's responsibilities should be further defined by the parent agency.
  - 7.4.8 The laboratory director should construe or clarify any provision of this Manual deemed vague or subject to interpretation.
- 7.5 Digital Evidence Analyst (Job Description)

- 7.5.1 A digital evidence analyst may be responsible for any task incident to the examination of technical devices and digital media.
  - 7.5.2 Digital evidence analysts should be responsible for other tasks incident to the operations of the laboratory, at the discretion of a supervisor.
  - 7.5.3 Digital evidence analysts may perform other tasks at the discretion of a supervisor.
  - 7.5.4 A digital evidence analyst should be a person of integrity and high ethical standards with the education, knowledge, training, and experience to perform competently.
- 7.6 Other Tasks
- 7.6.1 The laboratory director may appoint unit personnel to perform other tasks incident to the operation of the laboratory.
  - 7.6.2 Additional official tasks assigned to unit personnel should be documented in a job description.
- 7.7 Laboratory personnel are prohibited from performing any of the below job functions without formal, documented clearance from the laboratory director.
- 7.7.1 Taking part in the identification, collection, seizure, or intake of evidence.
  - 7.7.2 Archiving original evidence.
  - 7.7.3 Collecting, creating, or analyzing derivative evidence.
- 7.8 The laboratory director may authorize or direct unit personnel to perform any other task not detailed above without formal process.

## **PERSONNEL – TRAINING AND PROFICIENCY**

### **8.1 Training File**

- 8.1.1 Unit personnel should have a training file (hereinafter “Training File”) stored in the laboratory administration archive.
- 8.1.2 Unit personnel should keep a current copy of their curriculum vitae in the training file.
- 8.1.3 Other documents detailed within the provisions of this section of the Manual should be retained in the training file.

### **8.2 Personnel and this Manual**

- 8.2.1 All unit personnel should have ready access to the current copy of this Manual.
- 8.2.2 All unit personnel should read and familiarize themselves with the contents of this Manual and all updates and amendments.

### **8.3 Proficiency**

- 8.3.1 Unit personnel should have the requisite combination of knowledge, training, education, and experience to competently perform respective job functions for which they have received clearance.
- 8.3.2 Unit personnel should demonstrate competence through an established laboratory procedure before performing cleared job tasks.
- 8.3.3 Documentation of demonstrated competence should be saved in the training file.

### **8.4 Training and Continuing Education Related to Digital Evidence Analysis**

- 8.4.1 Unit personnel should be trained in the respective job tasks they are cleared to perform.
- 8.4.2 Unit personnel should be trained in report writing.

- 8.4.3 Unit personnel should be trained in the presentation of courtroom testimony. Presence in court during the testimony of other digital forensic analysts should be documented in the training file.
- 8.4.4 Unit personnel should stay current in the field of digital evidence analysis through membership in professional organizations, research, and continuing education and training for the tasks they are cleared to perform.
- 8.4.5 Unit personnel should keep a copy of training/education certificates and agendas/syllabi for courses attended in their training file.
- 8.4.6 Unit personnel should keep a copy of certification and professional organization membership paperwork in their training file.

## LABORATORY EQUIPMENT TESTING

- 9.1 Approval of Write Protection and Evidence Duplication Tools (Hardware and Software) and Techniques
  - 9.1.1 Tools and techniques used to write protect and create derivative evidence from original evidence should be approved for use by the laboratory director.
  - 9.1.2 Tools and techniques used to write protect and create derivative evidence from original evidence should not be used until approved.
  - 9.1.3 The lab director may approve such tools and techniques after testing and validation in accordance with Section 9.3.
  - 9.1.4 The lab director may approve such tools and techniques by adoption of the results of testing performed by another organization or agency.
- 9.2 Tools and techniques used to write protect and create derivative evidence from original evidence should be subject to routine testing and/or performance measures to ensure continued compliance with approval standards.
- 9.3 Procedure for testing and validation of tools and techniques used in the write protection and duplication of original evidence.
  - 9.3.1 Develop a test plan that includes a description of the test; the purpose for the test; what is being tested; the test method; and appropriate controls.
  - 9.3.2 Create and document test conditions, equipment, and software.
  - 9.3.3 Perform test.
  - 9.3.4 Document results.
- 9.4 Software, hardware, and techniques used in the analysis of evidence should be approved for use by the laboratory director after review for consistency with documented manufacturer or developer specifications.

THE MASSACHUSETTS CYBER CRIME INITIATIVE  
RECOMMENDED MINIMUM STANDARDS FOR  
DIGITAL EVIDENCE ANALYSIS

---

- 9.5 Test, calibration, and certification documentation should be retained in the laboratory administration archive.

## **AUDIT AND REPORTING**

- 10.1 The laboratory director should review, or should appoint someone to review, all quality control documents on an annual basis.
- 10.2 The laboratory director should solicit recommendations from unit personnel for changes to quality control documents during the review.
- 10.3 The laboratory director should amend quality control documents as necessary after the review.
- 10.4 Annual Laboratory Review
  - 10.4.1 The laboratory director should conduct an internal evaluation and report on laboratory/unit activity, on a schedule determined by the parent agency.
  - 10.4.2 The evaluation should include a summary of the review of quality control documents, problems and corrective action, volume and type of work, and future recommendations respective to these topics.
- 10.5 Remedial and Corrective Action
  - 10.5.1 The laboratory director may take or institute a process for the institution of remedial or corrective action for violations of the provisions of this Manual.
  - 10.5.2 The laboratory director may take or institute a process for the institution of remedial or corrective action against subordinate personnel for misconduct, negligence, or conduct inconsistent with the professional or ethical standards of the laboratory.
  - 10.5.3 The laboratory director should receive and evaluate complaints relating to laboratory operations or personnel and take appropriate action in accordance with agency or laboratory policy.
  - 10.5.4 The lab director should monitor the progress of personnel subject to corrective or remedial measures.

## **CASE PROCEDURE**

- 11.1 Cases formally accepted by the unit should be entered into a record tracking system.
- 11.2 A copy of the data entered into the record tracking system should be stored in the laboratory administration archive or, alternatively, be readily accessible to unit personnel.
- 11.3 Case Acceptance Procedure
  - 11.3.1 The laboratory director or other agency authority should decide what cases are accepted in the laboratory.
  - 11.3.2 Each accepted case should be documented.
  - 11.3.3 An initial case intake should be documented.
  - 11.3.4 Each accepted case should be given a unique identifying case number at the time of intake.
  - 11.3.5 The laboratory director should assign one unit personnel to be responsible for each accepted case.
  - 11.3.6 The laboratory director should determine the priority to be designated to each respective case.
- 11.4 Case Number
  - 11.4.1 The case number should be recorded on all documentation related to the case.
  - 11.4.2 The case number should be used or referenced in the identification of all original evidence received for examination in the laboratory.
  - 11.4.3 The case number should be used or referenced in the identification of all derivative evidence received for examination in the laboratory.
  - 11.4.4 The case number should be used or referenced in the identification of evidence handled in accordance with the provisions of Section 12 of this Manual.

- 11.5 There may be a hard copy case file and a digital case file maintained for each case.
- 11.6 The contents of the hard copy and digital case file are subject to parent agency and/or laboratory policy.
- 11.7 Unit personnel should sign, initial, or otherwise mark each item in the digital or hard copy case file to identify their respective work product.
- 11.8 Case intake documentation should, at a minimum, clearly include the following information.
  - 11.8.1 The name and identifying/contact information for the person requesting the service.
  - 11.8.2 A detailed explanation of the service requested.
  - 11.8.3 Chain of custody documentation for original evidence prior to receipt in the laboratory.
  - 11.8.4 A detailed description of any media to be examined, including the respective evidence identification numbers and condition upon receipt.
  - 11.8.5 A detailed description of the legal authority for the analysis of the evidence.
- 11.9 Special Issues for Case Intake
  - 11.9.1 Any unit or agency personnel with discretion to accept a case may decline a case for any reason.
  - 11.9.2 Unit personnel should notify the individual making the request for services to the laboratory of the priority designated to the case.
- 11.10 Use of External Service for Component of Examinations
  - 11.10.1 It may become necessary to retain the services of an external organization during an examination.

- 11.10.2 The laboratory director should ensure that the external organization is qualified to perform the requested service.
  - 11.10.3 The laboratory director should ensure that the evidence handling procedures of this Manual are adhered to during the provision of the external service.
  - 11.10.4 The laboratory director should ensure that the appropriate legal authority for the external service is in place.
- 11.11 Case File Disclosure
- 11.11.1 The contents of case files should be considered confidential at all times.
  - 11.11.2 The contents of items in the case file may be reviewed by laboratory and agency personnel.
  - 11.11.3 The contents of the case file, or portions thereof, may be reviewed, copied, or subject to inspection by other persons involved with the respective case, including defense counsel and experts, at the direction of the laboratory director.
- 11.12 Absent court order or contravening agency or laboratory policy, case files should be archived according to agency or laboratory policy.

## **EVIDENCE PROCEDURE**

- 12.1 This procedure applies to the receipt, handling, storage, and archiving of original and derivative evidence by unit personnel.
- 12.2 Procedure for Original Evidence
- 12.2.1 Original evidence received for examination may be delivered to the laboratory by personal delivery.
  - 12.2.2 Original evidence received for examination may be delivered to the laboratory by a tracked, receipt-confirmed, commercial delivery service.
  - 12.2.3 Original evidence may be collected or received for examination by unit personnel in the field.
  - 12.2.4 If packaged, the state of the evidence upon receipt should be documented prior to removing the evidence from the packaging.
  - 12.2.5 The physical state of the evidence should be documented prior to opening or removing any component devices.
  - 12.2.6 The chain-of-custody for evidence should be documented according to agency or laboratory procedure.
  - 12.2.7 Evidence receipts and chain-of-custody documents should be saved according to agency or lab procedure.
  - 12.2.8 Evidence should be analyzed according to the provisions of Section 13.
  - 12.2.9 The transfer of evidence to or from the custody of the laboratory is subject to the approval of the laboratory director.
- 12.3 Procedure for Derivative Evidence
- 12.3.1 Derivative evidence may be stored in digital format with a numbering format that clearly identifies it as relating to the particular case.

12.3.2 Derivative evidence should be segregated virtually or physically from other case data or derivative evidence.

12.3.3 Derivative evidence should be secured from access by unauthorized persons.

#### 12.4 Procedure for Derivative Evidence from a Non-Repeatable Procedure

12.4.1 Derivative evidence from a non-repeatable procedure should be preserved on secure lab media as soon as practicable after the procedure.

12.4.2 A duplicate copy of the derivative evidence from a non-repeatable procedure should be created.

12.4.3 Derivative evidence from the non-repeatable procedure should be stored digitally with a numbering format that clearly identifies it as relating to the particular case.

12.4.4 Derivative evidence from the non-repeatable procedure should be segregated virtually or physically from other case data or derivative evidence.

12.4.5 In the event the computer or device on which the non-repeatable procedure was performed will not be taken into custody for static analysis, the system or device should be documented and photographed before access to the system is lost.

12.4.6 If the derivative evidence from the non-repeatable procedure is preserved under authority of a search warrant, appropriate entries should be made in the search warrant return.

#### 12.5 Evidence Inventory and Identification

12.5.1 Evidence described in Sections 12.2, 12.3, and 12.4 should be clearly labeled with a unique identification number that corresponds to the respective case.

12.5.2 The unique identifying number should be affixed to physical evidence items in a manner designed to be permanent in nature.

12.5.3 All evidence described in Sections 12.2, 12.3, 12.4 should be inventoried in an evidence tracking system.

## 12.6 Storage of Evidence

12.6.1 Evidence should be kept in a secure evidence storage location at all times unless being actively processed.

12.6.2 While being processed, unit personnel must take precautions to secure the evidence.

12.6.3 All evidence, in whatever form, should be secured from temperature extremes, moisture, and electro-static discharge.

12.6.4 Efforts should be made to secure mobile devices, computer systems, and other devices that have network capacity to prevent connection with other devices or networks.

## 12.7 Declination of Evidence

12.7.1 The laboratory may decline to receive evidence for any reason.

12.7.2 The laboratory director should communicate the reason for the declination to the individual attempting the submission.

12.7.3 Nothing should preclude the individual attempting the submission of evidence from submitting the same evidence at a later date.

## 12.8 Return and Archiving of Evidence

12.8.1 Original evidence may be returned to the submitting agency after all necessary analysis procedures are complete.

12.8.2 Archived evidence should be stored according to agency or laboratory policy.

## 12.9 Evidence Confidentiality

12.9.1 Digital evidence analysts often encounter digital evidence, files, and information that are contraband, privileged, or otherwise confidential or sensitive due to their content.

THE MASSACHUSETTS CYBER CRIME INITIATIVE  
RECOMMENDED MINIMUM STANDARDS FOR  
DIGITAL EVIDENCE ANALYSIS

---

- 12.9.2 Data and information from case files and investigations conducted by unit personnel should be considered confidential.
- 12.9.3 Evidence constituting contraband should be clearly marked as contraband.
- 12.9.4 Confidential or sensitive evidence or information should be marked accordingly.
- 12.9.5 The transfer, dissemination, or review of original or derivative evidence, case information, or reports should be conducted in accordance with the provisions of this Manual or at the direction of the laboratory director.

## **DIGITAL EVIDENCE ANALYSIS PROCEDURE**

### **13.1 Legal Authority for Examination**

13.1.1 Each digital evidence examination procedure performed by unit personnel should be legally authorized.

13.1.2 Legal authorization may include a search warrant or an exception to the search warrant requirement.

13.1.3 It is preferred that digital evidence analysis procedures performed pursuant to a consent agreement be memorialized in writing.

13.1.4 The laboratory director and/or prosecutor should review the document providing legal authorization for the digital evidence examination procedure(s) prior to the performance of the respective procedure(s).

13.1.5 After review, the laboratory director should authorize the performance of the digital evidence examination procedure(s) if appropriate.

13.1.6 If the laboratory director does not authorize the digital evidence examination procedure(s) due to a concern related to the legal authorization for the procedure(s), the laboratory director should cause the performance of the respective procedure(s) to cease until the concerns are appropriately addressed and authorization is granted.

13.1.7 The examiner must stop the examination procedure and alert a supervisor if, in the course of an examination, evidence of another crime not under investigation is discovered.

13.1.8 The examiner must stop the examination procedure and alert a supervisor if, in the course of an examination, the legal authority for the examination is withdrawn or changed.

13.2 Digital evidence analysis procedures should be performed within the scope of the terms of the legal authority for the examination.

- 13.3 A copy of legal documents providing authority for the examination procedure(s) should be retained according to agency or laboratory policy.
- 13.4 Securing Evidence in the Field
- 13.4.1 Evidence that may be subject to seizure should be secured from virtual or physical contact by any person not present to assist in the seizure of the evidence.
- 13.4.2 After being initially secured, items of potential evidentiary value should be photographed, videotaped, diagramed, or documented in another fashion before further contact.
- 13.4.3 Technical items that may be seized that are powered off should not be turned on unless they will be subject to a preview examination procedure.
- 13.4.4 Screen displays on powered computer systems and devices should be photographed when practicable.
- 13.4.5 Proper shutdown procedures should be used to secure powered devices.
- 13.4.6 Efforts should be made to secure mobile devices in a manner using hardware, software, or techniques that inhibit the devices' ability to connect to other devices or networks.
- 13.4.7 Pending legal authority, all manuals, documents, cables, peripherals, and other items necessary to complete the digital evidence examination should be secured.
- 13.5 Technical devices should be treated as fragile.
- 13.6 Technical devices should be collected, packaged, transported, and stored in a secure manner where they will not be damaged nor subject to data alteration due to weather extremes, moisture, or other destructive conditions.
- 13.7 A document should clearly detail the following information about evidence seized in the field.
- 13.7.1 A description of the evidence including the power state at the time of seizure.

- 13.7.2 The physical location of the evidence.
- 13.7.3 The individual that identified the evidence.
- 13.7.4 The individual that seized the evidence.
- 13.7.5 The seizure process.
- 13.8 Collection of Derivative Evidence through a Non-Repeatable Procedure
  - 13.8.1 The collection of derivative evidence through a non-repeatable procedure is an acceptable practice.
  - 13.8.2 Procedures performed during collection of derivative evidence through a non-repeatable procedure should be documented.
  - 13.8.3 The examiner should take reasonable precautions to minimize the alteration of data while performing a non-repeatable procedure.
  - 13.8.4 In the event an examiner will collect both the contents of memory and volatile or logical data, memory should be collected first.
- 13.9 Physical Inspection of Evidence
  - 13.9.1 Original evidence should be inspected by the analyst as soon as practicable after the custody of the evidence is transferred to the laboratory.
  - 13.9.2 When taking custody of evidence in the field, the examiner should inspect the evidence before leaving the premises.
  - 13.9.3 When receiving the evidence in the laboratory, the examiner should inspect the evidence, at the time of receipt, in a designated evidence intake area.
  - 13.9.4 The evidence intake area should be kept orderly at all times and reserved for one case at one time.

13.9.5 The examiner should inspect the evidence and document any damage or defect, installed peripherals and devices/drives, unique identifying numbers, and other important information.

13.9.6 The documentation of the physical inspection should be saved according to agency or laboratory policy.

13.9.7 It is preferable for the examiner to assign and affix the unique identifying laboratory evidence number to the evidence at the time of inspection.

#### 13.10 Examination Screening with Case Agent

13.10.1 The examiner should meet with or discuss the examination procedure(s) with the case agent prior to beginning the examination, and request copies of documents necessary to plan the examination.

13.10.2 Documents received from the case agent should be retained according to agency or laboratory policy.

#### 13.11 Examination and Data Reduction

13.11.1 It is acceptable practice to reduce the amount of data to be subject to examination after the inspection process by not imaging and examining every item of original evidence.

13.11.2 Previews of original evidence are an acceptable data reduction practice when performed in accordance with Sections 13.12 and 13.13.

13.11.3 It is acceptable practice to not further examine media or devices that are in a state of disrepair or damage that inhibits the examiner's ability to analyze the media or device.

13.11.4 It is acceptable practice to not further examine media that is previewed and confirmed to be original equipment manufactured.

13.11.5 The laboratory director may determine which evidence items are subject to imaging and analysis.

13.11.6 The decision to not further image or analyze original evidence should not be made until the evidence has been physically inspected.

13.11.7 The decision to not image or analyze original evidence should be documented in accordance with agency or laboratory policy.

#### 13.12 Collecting Derivative Evidence

13.12.1 The examiner should take reasonable precautions to prevent the alteration of data stored on original evidence during processing.

13.12.2 It is preferred in the laboratory setting that examinations be conducted on copies of data derived from original evidence.

13.12.3 When possible, data stored on original evidence should be protected from alteration during processing by use of hardware or software write-block equipment and procedures.

13.12.4 A physical copy of data on original media is preferable to a logical copy.

13.12.5 The integrity of derivative evidence should be verified during the examination and documented according to agency or laboratory policy.

#### 13.13 Analysis of Evidence

13.13.1 The current system or device date and time settings should be documented in comparison to the actual date and time.

13.13.2 Other notable settings from a computer system's BIOS should be documented.

13.13.3 The examiner should analyze derivative or original evidence for items relating to the request for services.

13.13.4 The examiner should analyze original or derivative evidence for the presence of viruses and malware when appropriate.

13.13.5 The examiner should document the location and metadata relating to files or data of interest located on the examined evidence.

THE MASSACHUSETTS CYBER CRIME INITIATIVE  
RECOMMENDED MINIMUM STANDARDS FOR  
DIGITAL EVIDENCE ANALYSIS

---

13.14 Procedures performed in the course of digital evidence examinations should be documented and retained according to agency or laboratory policy.

## REPORT PROCEDURE

- 14.1 A report documenting each digital forensic examination conducted in the laboratory should be prepared for each case, unless the provisions of Section 14.3 apply.
- 14.2 Reports of other activity including assists to other agencies should be prepared upon the orders of the laboratory director or in accordance with agency or laboratory policy.
- 14.3 The examiner does not have to prepare a written report documenting the examination in the following circumstances:
  - 14.3.1 The agency or individual requesting the examination rescinds the request before submission of the evidence.
  - 14.3.2 The case is adjudicated before the examination, or report, is complete.
  - 14.3.3 Other occasions specifically authorized by the laboratory director.
- 14.4 The author of the report must have conducted, participated in, observed, supervised, or technically reviewed the examination.
- 14.5 The author of the report is responsible for the content of the report.
- 14.6 The report and supplemental files may be preserved in digital format.
- 14.7 The report may not be disseminated until the case review procedure described in Section 15 of this Manual is complete.
- 14.8 The report should only be distributed to a law enforcement agency or the agency who has requested the digital forensic examination. The respective agency or individual requesting the examination should assume full responsibility for compliance with discovery obligations.
- 14.9 Report Dissemination
  - 14.9.1 Dissemination of the report or any portion thereof, in any format, should be documented according to agency or laboratory policy.

14.9.2 Dissemination of the report or any portion thereof may be by personal service, delivery service, facsimile, or electronic transmission.

14.9.3 No report nor any portion thereof should be transmitted electronically if it contains information that may be sensitive, pornographic, privileged, or contraband in nature.

#### 14.10 Report Content

14.10.1 Reports should be written in a clear, concise manner and contain sufficient detail for another examiner, competent in the same area of expertise, to make consistent and independent findings.

14.10.2 The report should detail all findings, including negative results, and findings relative to the specific requests made by the person requesting the services of the laboratory.

14.10.3 Changes to the report should be by supplement and not by modification.

14.11 Hard copy reports and/or digital copies of the report and supplemental files that contain contraband, sensitive or confidential information, personal identifying information, or information that may be subject to privilege should be marked accordingly.

#### 14.12 Report Format

14.12.1 Digital forensic examination reports should be in consistent format at the discretion of the laboratory director.

14.12.2 The report should clearly identify the case number and pagination.

14.12.3 The report should be signed by the author.

## **CASE REVIEW PROCEDURE**

- 15.1 Each case should be subject to case review before dissemination of the case report outside the laboratory.
- 15.2 Case review should include the following review procedure.
  - 15.2.1 Administrative review of the case file.
  - 15.2.2 Technical review of the examination.
- 15.3 Technical Review
  - 15.3.1 A person authorized by the laboratory director may conduct the technical review.
  - 15.3.2 The results of the technical review should be documented.
  - 15.3.3 The technical review should include a review of procedure(s) performed during the examination, as well as the output, to assure reliable results.
- 15.4 When the technical review is complete, the case file should be subject to administrative review.
- 15.5 Administrative Review
  - 15.5.1 Any person designated by the laboratory director may perform administrative review.
  - 15.5.2 The reviewer should review the case file and final report to ensure that all paperwork is in order and that the provisions of this Manual have been complied with.
  - 15.5.3 The designated reviewer should document the final completion of the administrative review process in accordance with agency or laboratory policy.