ARKANSAS STATE CRIME LABORATORY

DIGITAL EVIDENCE QUALITY MANUAL

DIRECTOR:

KERMIT B. CHANNELL, II

CONTENTS

1 SCOPE

This manual follows the requirements specified by ANSI-ASQ National Accreditation Board (ANAB), which is based on the ISO/IEC 17025:2017 standards and the 2017 ANAB ISO/IEC 17025:2017 — Forensic Science Testing and Calibration Laboratories Accreditation Requirements (AR 3125).

The manual follows the outline of the *ASCL Quality Manual (ASCL DOC 01)*.

The *Digital Evidence Quality Manual* is written specifically for the analysts working in the Digital Evidence Section and performing analysis in computer forensics.

1.1 INTERNATIONAL STANDARD: GENERAL REQUIREMENTS

See *ASCL DOC-01 Quality Manual*.

1.2 INTERNATIONAL STANDARD: SCOPE

See *ASCL DOC-01 Quality Manual*.

2 NORMATIVE REFERENCES

This section follows references from the *ASCL DOC-01 Quality Manual* and all other references listed in this manual are located in the Digital Evidence section or on the Digital Evidence S: drive.

3 TERMS AND DEFINITIONS

Terms and definitions are located in the *ASCL Quality Manual (ASCL-DOC-01)*.

4 GENERAL REQUIREMENTS

See *ASCL DOC-01 Quality Manual.*

5 STRUCTURAL REQUIREMENTS

5.1 ESTABLISHMENT

See *ASCL DOC-01 Quality Manual.*

5.2 MANAGEMENT

The Arkansas State Crime Laboratory is managed by the Director, who has overall responsibility for the laboratory.

For 5.2.1 – 5.2.8 See *ASCL-DOC-01 Quality Manual*.

5.2.9 DIGITAL EVIDENCE STAFF

5.2.9.1 CHIEF DIGITAL EVIDENCE ANALYST

QUALIFICATIONS

The formal education equivalent of a bachelor's degree with science courses; plus three years experience in a scientific laboratory. Other job-related education and/or experience may be substituted for all or part of these basic requirements upon approval of the Scientific Operations Director.

AUTHORITIES & RESPONSIBILITIES

- Supervision of a professional staff. Duties include: interviewing, hiring, and training applicants; remediation of procedural issues; review of case files to maintain the quality of the work product within the section.
- Manages the digital evidence section by assigning cases and ensuring that cases are worked within a reasonable timeframe, ordering equipment and supplies, preparing short and long-range plans, and participating in the development of section and agency budget.
- Performs evidence examination by reviewing submission reports received from law enforcement agencies and analyzing evidence for possible recovery of data.
- Maintains a complete chain of custody of evidence, documents evidence while performing tests, and writes detailed reports of final analysis and results including inventory of evidence examined. Submits reports to appropriate investigative agencies.
- Presents testimony in court as an expert witness, interprets results of forensic examinations, and explains methods used.
- Attends conferences and training to keep abreast of new technology and forensic methods.
- Ensures compliance with the ANAB accreditation standards.

- Has the overall responsibility for the technical operations and the provisions of the resources needed to ensure the required quality of laboratory operations.
- Performs related responsibilities as required or assigned.

5.2.9.2 DIGITAL EVIDENCE ANALYST

QUALIFICATION

The formal education equivalent of a bachelor's degree with science courses; plus three years' experience in a scientific laboratory. Other job-related education and/or experience may be substituted for all or part of these basic requirements upon approval of the Chief Digital Evidence Analyst.

AUTHORITIES & RESPONSIBILITIES

- Performs evidence examination by reviewing submission reports received from law enforcement agencies and analyzing evidence for possible recovery of data.
- Maintains a complete chain of custody of evidence, documents evidence while performing tests, and writes detailed reports of final analysis and results including inventory of evidence examined. Submits reports to appropriate investigative agencies.
- Presents testimony in court as an expert witness, interprets results of forensic examinations, and explains methods used.
- Attends conferences and training to keep abreast of new technology and forensic methods.
- Performs related responsibilities as required or assigned.

5.2.9.3 SECTION QUALITY MANAGER

- Reviews section documents and forms and updates as needed. Verifies that everyone is using the current versions.
- Ensures section logs (e.g. Computer Maintenance Log) are up to date.
- Performs verifications of newly released software versions to check for proper functionality.

5.2.9.4 SECTION SAFETY MANAGER

- Conducts monthly safety inspections and ensuring that proper practices and procedures are being followed within the section.
- Maintains records of any safety incidents within the section.
- Works with the Arkansas State Police Head Quarters Building Services Manager to seek ways to improve the safety program.

Each subordinate shall be accountable to only one immediate supervisor for each category of testing.

The analyst appointed by the Chief Digital Evidence Analyst or the analyst present in the section with the highest seniority will serve as a deputy for key management personnel when the Chief

Digital Evidence Analyst will be absent for three days or longer. All affected personnel shall be notified

All employees will be notified of their responsibilities and expectations concerning the objective of the ASCL quality system. Feedback on actual job performance will be conveyed in annual performance evaluations.

The Chief Digital Evidence Analyst will have meetings as needed to convey information to section staff.

5.3 SCOPE OF LABORATORY ACTIVITIES

The Digital Evidence section is responsible for analyzing computers and digital storage devices for the criminal justice system. This may include systematic retrieval of digital data that may be of evidentiary value, as well as, provide technical support to law enforcement agencies. Upon request, analysts provide law enforcement agencies with technical assistance during crime scene operations. This analysis is performed in a chain-of-custody environment using validated and appropriate procedures in order to ensure the most accurate and relevant analytical results.

For additional information see *ASCL DOC-01 Quality Manual.*

5.4 NORMATIVE DOCUMENTS

See *ASCL DOC-01 Quality Manual.*

5.5 LABORATORY OPERATIONS

See *ASCL DOC-01 Quality Manual.*

5.6 QUALITY MANAGEMENT

See *ASCL DOC-01 Quality Manual.*

5.7 MANAGEMENT SYSTEM COMMUNICATION AND INTEGRITY

See *ASCL DOC-01 Quality Manual.*

6 RESOURCE REQUIREMENTS

6.1 GENERAL

See *ASCL DOC-01 Quality Manual.*

6.2 PERSONNEL

6.2.1 GENERAL

See *ASCL DOC-01 Quality Manual.*

6.2.2 COMPETENCE REQUIREMENTS

See *ASCL-DOC-01 Quality Manual*.

6.2.2.1 ANALYST/EXAMINER EDUCATIONAL REQUIREMENTS

See *ASCL-DOC-01 Quality Manual*.

6.2.2.2 TRAINING PROGRAM

The Chief Digital Evidence Analyst shall ensure the competence of all who operate equipment, perform tests, evaluate results, and sign test reports in the Digital Evidence Section. The Chief Digital Evidence Analyst is to supervise personnel in training, or assign a qualified Digital Evidence Analyst.

Various topics will be covered throughout the training including: new employee orientation, evidence handling, computer forensics training, laboratory analysis, report writing, and legal issues. As each topic is completed, it will be signed and dated by the trainee and trainer. Once the training program is completed, a case release form will be signed and dated by the supervisor, trainer, and trainee. Also, a statement of competency shall be documented by the Chief Digital Evidence Analyst and maintained in Qualtrax. More detail of the training program is outlined in ASCL Digital Evidence Section Training Manual (DE-DOC-02).

6.2.2.2.1 MOOT COURT

The training program shall include training in the presentation of evidence in court. Moot court may be waived if previously completed in another category of testing

6.2.3 COMPETENCE OF STAFF

See *ASCL-DOC-01 Quality Manual* and *DE-DOC-02 Training Manual*.

6.2.4 DUTIES, RESPONSIBILITIES, AND AUTHORITIES

See job descriptions in section 5.2 of this manual.

6.2.5 PERSONNEL REQUIREMENTS

See *ASCL-DOC-01 Quality Manual*.

6.2.6 AUTHORIZATIONS

See *ASCL-DOC-01 Quality Manual*.

6.3 FACILITIES AND ENVIRONMENTAL CONDITIONS

6.3.1 GENERAL

See *ASCL-DOC-01 Quality Manual*.

6.3.2 DOCUMENTATION

See *ASCL-DOC-01 Quality Manual*.

6.3.3 MONITORING RECORDS

See *ASCL-DOC-01 Quality Manual*.

6.3.4 CONTROL OF FACILITIES

See *ASCL-DOC-01 Quality Manual*.

6.3.4.1 ACCESS

The Digital Evidence section consists of rooms that are either locked by a key or require a security fob for entry. Distribution of keys and security fobs are limited to those authorized by the ASCL Director. Physical door keys and security fobs are distributed by the Regulatory and Building Operations Services division of the ASP. Analysts in the section are assigned keys to doors, storage cabinets, etc. A key log is kept in the section tracking the location of each key. There is key box located in the Chief Digital Evidence Analyst's office. The Chief Digital Evidence Analyst has possession of the key to the key box. A log must be kept when keys are added or removed from the section key box.

See *ASCL-DOC-01 Quality Manual* for additional access information.

6.3.4.2 PREVENTION OF ADVERSE INFLUENCES

Analyst shall take reasonable precautions to protect the evidence from loss, cross-transfer, contamination and/or deleterious change.

6.3.4.3 SEPARATION

See *ASCL-DOC-01 Quality Manual*.

6.3.5 EXTERNAL ACTIVITIES

See *ASCL-DOC-01 Quality Manual*.

6.4 EQUIPMENT

6.4.1 ACCESS

The Digital Evidence Section has adequate equipment to perform all necessary testing. Access to the Digital Forensic equipment is restricted by the criteria in section 6.3.4.1 of this manual.

6.4.2 OUTSIDE EQUIPMENT

See *ASCL-DOC-01 Quality Manual*.

6.4.3 PROPER FUNCTIONING

Instruments used in the Digital Evidence section for the testing of evidence are Processing and Imaging Computers, as well as, a Grayshift Graykey, used in the acquisition of Apple cell phones/smartphones/tablets.

Instrumentation/Equipment Training

Only individuals who have been trained in the proper use of the instrumentation/ equipment are authorized to use it. New employees shall be trained on the appropriate instrumentation/equipment during their training program. When new instrumentation/equipment requires a validation, appropriate personnel will be trained. Up-to-date instructions on the use and maintenance of the instrument/equipment shall be readily available for use.

Instrument/Equipment Identification

Each instrument will be uniquely identified with a sticker which states the name of the instrument.

Handling and Maintenance of Instrument/Equipment

All instrumentation/equipment will be maintained in a clean, orderly, and safe condition. Laboratory equipment and instrumentation shall be handled responsibly to ensure optimal

performance and to avoid contamination and premature wear and damage. It is the Chief Digital Evidence Analyst responsibility to ensure that proper planning and care is taken when equipment or instrumentation is initially located or subsequently moved. Due care shall be taken if equipment or instrumentation is to be shipped to a manufacturer or vendor for calibration or maintenance to minimize the possibility of damage in transit. Equipment that is infrequently used shall be stored (covered, powered-down, etc.) per the manufacturer's recommendations. Preventative maintenance steps are taken by the Chief Digital Evidence Analyst and Digital Evidence Analysts to ensure optimum performance from the equipment, this includes but not limited to performing a Windows update on each computer. When this action is taken, it is documented in the Computer Maintenance Log for the computer it was performed on. Other actions may be performed as needed.

Outside Maintenance

A performance verification shall be performed on instrumentation and equipment that has gone outside of the direct control of the laboratory (e.g., for repair or preventive maintenance) to ensure that its calibration status is satisfactory before being returned to service. Calibration or maintenance records will reflect that the equipment was functioning properly prior to being returned to service.

6.4.4 PERFORMANCE VERIFICATION

Processing and imaging computers should be maintained and in proper working order. This may be accomplished by a successful power on self-test (POST) and successful loading of the operating system (OS). See section 6.4.10 in this manual for additional information.

6.4.5 FITNESS FOR SERVICE

See *ASCL-DOC-01 Quality Manual*.

6.4.6 CALIBRATION REQUIREMENT

See *ASCL-DOC-01 Quality Manual*.

6.4.7 CALIBRATION PROGRAM

See *ASCL-DOC-01 Quality Manual*.

6.4.8 LABELLING

See *ASCL-DOC-01 Quality Manual*.

6.4.9 OUT OF SERVICE

If an instrument/equipment is not working properly or potential problems are observed, it is the duty of the analyst to immediately take the appropriate steps to repair/correct the problem or

inform the appropriate individual of the problem. Any problem and the action to correct the problem must be logged in the instrument/equipment's log. Instrumentation/Equipment that is not working properly must be clearly marked as being 'OUT OF SERVICE' in order to prevent inadvertent use of the equipment. The instrument/equipment will not be used in casework until appropriate calibration or verification is performed. When it has been determined that instrumentation/equipment was not working properly, the Chief Digital Evidence Analyst shall take into consideration the effect the problem may have had on previous tests.

6.4.10 INTERMEDIATE CHECKS

Processing and imaging computers should be maintained and in proper working order. This may be accomplished by a successful power on self-test (POST) and successful loading of the operating system (OS). This operation should be completed each month and the results placed in the Computer Maintenance Log. There is a separate log for each processing and imaging computer.

6.4.11 CORRECTION FACTORS

See *ASCL-DOC-01 Quality Manual*.

6.4.12 EQUIPMENT ADJUSTMENT

See *ASCL-DOC-01 Quality Manual*.

6.4.13 EQUIPMENT RECORDS

Records are located in the Maintenance Logs folder on the Digital Evidence server. These logs contain such information as identity of equipment, location, manufacturer, model, serial number, asset number, install date, and software information. Information that is recorded in the records includes date of maintenance item, initials of who performed the maintenance, and remarks about the maintenance performed.

6.5 METROLOGICAL TRACEABILITY

See *ASCL-DOC-01 Quality Manual*.

6.6 EXTERNALLY-PROVIDED PRODUCTS AND SERVICES

See *ASCL-DOC-01 Quality Manual*.

7 PROCESS REQUIREMENTS

7.1 REVIEW OF REQUESTS, TENDERS, AND CONTRACTS

See *ASCL-DOC-01 Quality Manual*.

7.2 SELECTION, VERIFICATION, AND VALIDATION OF METHODS

7.2.1 SELECTION AND VERIFICATION OF METHODS

See *ASCL-DOC-01 Quality Manual*. Digital Evidence test methods are listed in Section 9 of this manual.

7.2.2 VALIDATION OF METHODS

See *ASCL-DOC-01 Quality Manual*.

7.3 SAMPLING

See *ASCL-DOC-01 Quality Manual*. Digital Evidence test methods are listed in Section 9 of this manual.

7.4 HANDLING OF TEST ITEMS

7.4.1 GENERAL

The Digital Evidence Section will receive, secure, analyze and document evidence submitted by duly authorized agencies. The Digital Evidence Section will process evidence in a timely manner consistent with the need for quality services, preservation of the chain-of-custody and protection of the integrity of the evidence. It is a system-wide priority to ensure that the necessary precautions are taken to maintain the integrity of the evidence, including proper collection and preservation techniques.

The Evidence Receiving Quality Manual (ER-DOC-01) contains policies and procedures for the transportation, receipt, handling, protection, storage, retention, maintenance, control and disposition of test items, including all provisions necessary to protect the integrity of the test item.

7.4.1.1 HANDLING PROCEDURE

7.4.1.1.1 STORAGE

Cabinets are provided in the Digital Evidence Section for the storage of evidence. These cabinets are secured by key lock and are located in an environment that prevents the deterioration, loss, and damage of the evidence.

Evidence in the process of examination may be left unattended for limited periods of time, but must be in a secure limited access area. If the analyst needs to be away for a longer period of time, the evidence shall be secured in a short-term storage location, whenever practical. If this is not possible, the analyst shall take reasonable precautions to protect the evidence from loss, cross-transfer, contamination and/or deleterious change.

7.4.1.1.2 PACKAGING AND SEALING

PACKAGING

Evidence submitted for testing in the Digital Evidence section must be properly packaged, labeled and sealed to prevent contamination, loss or deleterious change. If there is any packaging deficiency noted at the time of receipt, it must be corrected, preferably by the submitting customer. If the customer is not available or it is not expedient to call the customer back to correct the deficiency, an evidence technician may take steps to correct the problem (i.e. provide a remedial seal). However, if the deficiency is serious enough to bring into question the integrity or identity of the test item, the Chief Digital Evidence Analyst and customer agency must be contacted to resolve the issue before the evidence is analyzed.

If a packaging deficiency is not apparent until the case is checked out by an analyst, the analyst may correct the deficiency. If there is any concern that the packaging deficiency has affected the integrity or identity of the test item, the Chief Digital Evidence Analyst and the customer agency shall be advised and consulted with for further instructions.

If the analyst discovers an inconsistency between the stated and actual contents of a package or the suitability of an evidence item for testing, the analyst shall make all attempts to contact the customer and document the discussion on an Agency Contact Form (ASCL-FORM-06) prior to issuing a report. For minor inconsistencies, the analyst shall use their judgment on whether to contact the customer, but must make a note of the discrepancy in the case file.

All remedial actions taken to correct packaging or evidence deficiencies shall be noted in the case record (e.g. submission form or analyst's notes).

SEALING

Evidence will be sealed in a manner in which the contents cannot readily escape and in such a manner that opening the container would result in obvious damage or alteration to the container or

its tape seal. All evidence must bear a proper seal which shall include the initials or other identification of the person sealing the evidence across the seal.

When the container is opened, the original seal shall be left intact, whenever practical, and a new opening made. When the analysis or examination is completed, the new opening shall be sealed, as outlined in these procedures; thus the original container seals will be intact and all seals will be clearly marked.

If reusing the original container is impractical, a new evidence container may be used. It shall also be marked and sealed according to the above procedures and the original evidence packaging shall be kept inside the second evidence container. If the original packaging cannot be kept, there must be complete documentation along with a picture of original packaging retained in the case record. Documentation of the change in packaging along with description must be documented in the case record for future reference.

7.4.1.1.3 CHIAN OF CUSTODY

See *ASCL-DOC-01 Quality Manual*.

7.4.1.1.4 CUSTOMER NOTIFICATION

See *ASCL-DOC-01 Quality Manual*.

7.4.2 ITEM IDENTIFICATION

A unique case number is assigned to every case when evidence is initially received by the laboratory. Each exterior container is labeled with a unique barcode. Agency evidence numbers will be used to identify the evidence whenever practical.

If uniquely-identified items must be subdivided, then appropriate subitem identifiers will be assigned and each subitem will be labeled with its identifier. This allows for the tracking of each subitem and the identification of its origin.

All evidence will be marked or identified with the laboratory case number (e.g. YYYY000000), if practical, to ensure that it is identifiable and traceable to the corresponding case. Otherwise, the proximal container must be marked or identified with the laboratory case number.

7.4.2.1 EXTENT

All items received by the ASCL will be identified as detailed in § 7.4.2 when possible.

7.4.3 DEVIATIONS

See *ASCL-DOC-01 Quality Manual*.

7.4.4 ENVIRONMENTAL CONDITIONS

See *ASCL-DOC-01 Quality Manual*.

7.5 TECHNICAL RECORDS

7.5.1 GENERAL

See *ASCL-DOC-01Quality Manual*.

7.5.1.1 TECHNICAL RECORD RETENTION

See *ASCL-DOC-01Quality Manual*.

7.5.1.2 ABBREVIATIONS

Abbreviations may be used in examination records. An abbreviation legend is accessible to all analysts in the Digital Evidence Section, located on the Digital Evidence Drive.

7.5.1.3 TECHNICAL RECORD SUFFICIENCY

Technical records to support a report shall be such that, in the absence of the analyst, another competent reviewer could evaluate what was done and interpret the data. The *DE-FORM-02_04 Case Documentation* form shall be filled out in accordance to section 9 of this manual and uploaded into the appropriate folder in the LIMS system.

7.5.1.4 TECHNICAL RECORD PERMANENCY

See *ASCL-DOC-01Quality Manual*.

7.5.1.5 REJECTION

See *ASCL-DOC-01Quality Manual*.

7.5.1.6 CALIBRATION DATA

See *ASCL-DOC-01Quality Manual*.

7.5.2 AMENDMENTS TO TECHNICAL RECORDS

See *ASCL-DOC-01Quality Manual*.

7.6 EVALUATION OF MEASUREMENT UNCERTAINTY

The Digital Forensic Section does not provide any results that require a measurement of uncertainty.

7.7 ENSURING THE VALIDITY OF RESULTS

7.7.1 GENERAL

The Digital Evidence Section maintains a quality manual containing quality control procedures designed to monitor and ensure the validity of test results. Quality control data will be recorded in a way to allow trends to be detected and, whenever practical, statistical techniques will be used to review the data. The records shall be retained to show that all appropriate quality control measures have been taken and are acceptable.

The following is a list of quality control measures used by the Digital Evidence Section:

- Functional checks of measuring and testing equipment
- Technical and administrative review of reported results
- Competency testing of analysts before beginning casework
- Testimony monitoring (for testifying analysts)
- Where applicable, the use of positive controls
- Review of all calculations and data transfers (e.g., cut and paste from a source to a destination) for accuracy, including that the correct information was transferred, by someone other than the examiner (e.g., the technical reviewer)

7.7.1.1 VERIFICATION

The Digital Evidence Section does not perform verification of independent examinations.

7.7.1.2 CASE REVIEW

See *ASCL-DOC-01 Quality Manual* and *DE-FORM-01 Case Review Form*.

7.7.1.2.1 TECHNICAL REVIEW

See *ASCL-DOC-01 Quality Manual.*

7.7.1.2.2 TESTIMONY REVIEW

A testimony review of all testifying personnel from the Digital Evidence Section will be conducted in accordance with the policies outlines in § 7.7.1.2.3 of the ASCL-DOC-01 Quality Manual.

Testimony of testifying personnel from the Digital Evidence Section will be conducted, at a minimum, once per accreditation cycle.

The first testimony of testifying personnel will be reviewed.

7.7.2 INTERLABORATORY COMPARISONS

See *ASCL-DOC-01 Quality Manual.*

7.7.2.1 EXTERNAL PROFICIENCY TESTING

For each location and calendar year, the ASCL participates in at least one external proficiency test for each discipline in which accredited services are provided. The providers of these tests are authorized to release the test results to ANAB.

7.7.3 MONITORING ACTIVITY ANALYSIS

See *ASCL-DOC-01 Quality Manual.*

7.7.4 INDIVIDUAL PROFICIENCY TESTING

Each analyst and technical support personnel engaged in testing activities, verifications, case review, or the authorization of results shall successfully complete at least one internal or external proficiency test per calendar year in each discipline in which they perform that work.

The areas of proficiency testing for the Digital Evidence discipline include:

- Computer Forensics
- Mobile Devices

The Digital Evidence discipline will successfully complete at least one external proficiency test annually. ANAB approved test providers shall be used where available. If there is not an ANAB approved test provider available, the ASCL will locate and use another source of an external test in the discipline.

7.7.5 PROFICIENCY TESTING REQUIREMENTS

Proficiency tests are presented to the Digital Evidence Section to demonstrate the reliability of the section analytical methods as well as the interpretive capability of the analyst. Participation in the proficiency test program is the primary means by which the quality performance of this section is judged and is an essential requirement in assessing the integrity of this section.

All analysts/examiners performing and reporting independent casework will participate in the proficiency-testing program. Each analyst/examiner must perform one (1) proficiency test per calendar year using the same analytical methods and techniques as are used for comparable casework. A minimum of one (1) external proficiency test must be completed annually in each discipline from an ANAB approved provider if available. If an approved provider is unavailable, an external proficiency test must be obtained from another source.

In addition, each examiner must be proficiency tested (internal or external) at least once, during each four-year accreditation cycle, in each category of testing in which the examiner performs casework. Questions on a proficiency test which do not fall within the normal scope of testing do not require a response. The reason for not responding will be documented in the case record, and the technical reviewer will include a review of this decision in their evaluation of the responses. The decision to not respond to a question will be made in consultation with the Quality Assurance Manager to help ensure conformance with accreditation requirements.

The following proficiency testing information will be stored in a Qualtrax workflow that can be accessed through Qualtrax reports:

- Individual's name
- Unique ASCL case number
- External proficiency identifier, if applicable
- Proficiency provider
- Date proficiency case file assigned
- Date test completed

All internal and external proficiency tests will have a case file generated in JusticeTrax. All administration and examination documentation will be in the assigned electronic case file. This electronic version is considered the official proficiency case record. In addition, the following will be maintained in the case file:

- How the samples were obtained or created (after testing is complete and results have been received)
- Proficiency test results from the provider
- Corrective Action Request Qualtrax workflow report, when applicable

The Chief Digital Evidence Analyst is responsible for comparing the analytical results to the expected results, determining if the analytical results are acceptable, and for reviewing these results with the analyst.

The Chief Digital Evidence Analyst is responsible for comparing the analytical results to the expected results, determining if the analytical results are acceptable, and for reviewing these results with the analyst.

The following criteria shall be used for evaluating proficiency test results:

- All tests are graded as satisfactory or unsatisfactory.
  - A satisfactory grade is attained when the experimental results match the expected results.
- If there is a discrepancy between the expected results and the experimental results, the Chief Digital Evidence Analyst must notify the Quality Assurance Manager.
- Minor discrepancies may be deemed satisfactory based on the following factors with approval of the QA Manager:
  - Discipline interpretation guidelines
  - Consensus results

If the results are deemed to be unsatisfactory, the Chief Digital Evidence Analyst must initiate a Corrective Action Request in Qualtrax.

7.7.6 PROFICIENCY TEST SCHEDULE

Each individual engaged in testing activities (both analysts and technical support personnel) shall be proficiency tested annually in each discipline in which they perform testing.

Each analyst and technical support personnel engaged in testing activities shall be proficiency tested in each area of testing appearing on the ASCL's Scope of Accreditation at least once during each accreditation cycle.

See *ASCL-DOC-01 Quality Manual*.

7.7.7 PROFICIENCY TEST SOURCING

See *ASCL-DOC-01 Quality Manual*.

7.7.8 PROFICIENCY TEST RECORDS

See *ASCL-DOC-01 Quality Manual*.

7.8 REPORTING OF RESULTS

See *ASCL-DOC-01 Quality Manual*.

REPORT CD

In addition to the report created in JusticeTrax, a Forensic Report CD (or DVD) may be generated detailing information about the evidence and findings that are of interest to a case. This Forensic Report CD/DVD is considered evidence and is returned to the submitting agency.

7.9 COMPLAINTS

See *ASCL-DOC-01Quality Manual*.

7.10 NONCONFORMING WORK

See *ASCL-DOC-01Quality Manual*.

7.11 CONTROL OF DATA AND INFORMATION MANAGEMENT

See *ASCL-DOC-01Quality Manual*.

8 MANAGEMENT SYSTEM REQUIREMENTS

See *ASCL-DOC-01 Quality Manual*.

9 TEST METHODS

9.1 GENERAL

This section provides standard procedures for tests and examinations performed by the Digital Evidence Analysts. All software packages and hardware devices used for the examination of evidence should be verified prior to use in casework to ensure that they perform the actions claimed.

Examination of computer evidence that contains hard drive or other digital storage media shall be performed in a forensically sound manner ensuring that data contained on submitted original digital evidence is not altered. For this reason, the original digital evidence shall only be used to make a forensic image and not for the analysis procedure. Some exceptional cases may require alterations to be made on the original media to be used during an examination. These situations will be fully documented and a justification provided.

Examination of mobile devices (i.e. cell phones, tablets, etc.) may require changes to the data due to the particular nature of the technology. In addition, alterations to the device settings may be necessary in order to complete a forensic acquisition.

Prior to and following any actions performed on the original media, a MD5 hash value will be generated to ensure that no file artifacts or inadvertent writes to or from the original media occurred. Examination shall be performed on the forensic image rather than the original digital evidence to ensure the integrity and authenticity of the evidence. The original evidence and the forensic image will be hashed and compared to ensure the copy exactly matches the original and that no alterations were made during the imaging process.

Examination of the evidence shall be in accordance with what the submitting agency has requested. This may include the examination of active files, hidden files, deleted files, data contained in unallocated areas, and data contained in slack areas. Data that has been password protected and encrypted may also be examined and the passwords recovered. This process is to ensure that no data that has been intentionally hidden or disguised is overlooked.

9.1.1 SELECTION OF METHODS

The Digital Evidence Section shall use test methods that meet the needs of the customer and are appropriate for the tests undertaken. Standard Methods, Laboratory Developed Methods or Non-Standard Methods may be utilized in casework after the appropriate validation and/or performance verifications have been performed as described in this section. The most current version of the method must be documented and readily available to the analyst for reference unless it is not appropriate or possible to do so.

9.1.2 STANDARD METHODS

Standard Methods are methods published in international, regional or national standards or by reputable technical organizations, or in relevant scientific texts or journals, or as specified by the manufacturer of the equipment. Before utilizing a Standard Method in casework, a performance verification must be performed to ensure the reliability of the method. Records of the performance verification shall be retained in the appropriate discipline. Standard methods do not need to be supplemented or rewritten as internal procedures if these standards are written in a way that they can be used as published. However, it may be necessary to provide additional documentation for optional steps in the method or additional details to ensure consistent application.

9.1.3 LABORATORY-DEVELOPED METHODS

Laboratory-Developed Methods are modifications of standard methods for a specific laboratory purpose. Laboratory-Developed Methods must be validated and a performance verification completed prior to use in casework.

9.1.4 NON-STANDARD METHODS

Non-Standard Methods are methods or procedures that are developed to meet a forensic need not covered by Standard Methods. Non-standard methods must be appropriate and contain a clear specification as to the intended use of the method. These methods must be validated and a performance verification completed prior to use in casework.

9.1.5 DIGITAL EVIDENCE DATA

- Computer software is documented in sufficient detail and suitably validated/verified.
- Digital Evidence data is secured. This is accomplished by storing the data on a Windows domain server that is isolated from the lab wide domain server. Digital Evidence Analysts are issued password protected user accounts to access the server.
- Computers and equipment are maintained to ensure proper functioning and are provided with environmental and operating conditions necessary to maintain the integrity of the data.
- Case evidence forensic images, documentation, reports, and exported data are stored on the domain server until archived or approved for removal by the Digital Evidence Section Chief.

9.1.6 CONTROLS

Prior to a computer forensic examination, a control device comparable to a device being worked must be acquired to ensure proper working order of the write-protection hardware or software used on a case. Examples of devices include IDE hard drive, SATA hard drive, and USB thumb drives. These control devices contain known data and known MD5 hash values. The examiner must ensure that no alterations or deletions occurred during the process of acquiring the control device. After successful completion of this process, notes are made in case documentation and the evidence may then be examined.

9.1.7 VERIFICATIONS

Prior to being used in casework, software and write protect devices must be verified. This verification should include checks that the tool will provide expected results or that the tool maintains the integrity of the evidence. Software tool verification should be completed on each new whole number version upgrade. If the tool meets the test requirements, the tool will be approved and authorized for casework by the Chief Digital Evidence Analyst or designee.

9.2 HARD DRIVE EXAMINATION

- Remove hard drive from the computer tower or notebook and document information about the computer. Documentation must include case number, examiner name/initials, page number, and date.
- Document the make, model, serial number, and storage capacity of the hard drive if available.
- Image a control hard drive of same type as evidence drive. Verify the MD5 hash value is correct
- Create an exact bit stream image file from evidence drive using verified software and hardware write blocking tools, and place on forensic server
- Package and seal the original hard drive in an envelope and place in original container with computer
- When the storage media cannot be removed from the computer (e.g., notebook computers), it may be necessary to boot the computer with a USB drive or disc, bypassing the installed media. This should be accomplished by verified software designed for this procedure. This process will be fully documented.
- Examine the forensic image. This may involve recovering folders, performing signature analysis, data carving, etc.
- Document hash verifications, bookmarks, operating system versions, and drive specifications. This documentation may be on the resulting forensic report media and/or on DE-FORM-02_04 Case Documentation
- Copy all pertinent information of evidentiary interest to an evidence folder/directory on the forensic server, and make a CD or DVD of evidentiary files and forensic report for the submitting agency/officer

9.3 REMOVABLE MEDIA EXAMINATION

- All removable media should be documented prior to examination. Documentation must include case number, examiner name/initials, page number, and date.
- A control of same type of removable media should be acquired prior to examination of evidence
- Removable media shall be write-protected if possible prior to examination
- Create an exact bit stream image file of the removable media using verified software and hardware write blocking tools, and place on forensic server
- Package and seal the removable media and place in original container

- Examine the forensic image. This may involve recovering folders, performing signature analysis, data carving, etc.
- Document hash verifications, bookmarks, operating system versions, and drive specifications. This documentation may be on the resulting forensic report media or on DE-FORM-02_04 Case Documentation
- Copy all pertinent information of evidentiary interest to an evidence folder/directory on the forensic server, and make a CD or DVD of evidentiary files and forensic report for the submitting agency/officer

9.4 HANDHELD DEVICE EXAMINATION (CELL PHONES, SMARTPHONES, TABLETS, AND PERSONAL DIGITAL ASSISTANTS)

- Document make, model, IMEI/ESN/MEID number of the device submitted for examination. Documentation must include case number, examiner name/initials, page number, and date. DE-FORM-02_04 Case Documentation is provided for documentation.
- Determine the best possible method for retrieval of the data stored on the handheld device.
- Ensure network isolation for data integrity by employing a faraday box or removing SIM Card.
- Place acquired data on forensic server
- Document hash verifications and pertinent device information. This documentation may be on the resulting forensic report media or examination worksheet
- Copy all pertinent data from handheld device with verified software and hardware to an evidence folder/directory on the forensic server or examination workstation, and make CD or DVD of evidentiary files and forensic report for the submitting agency/officer