ARKANSAS STATE CRIME LABORATORY

Digital Evidence Section Quality Manual

COPY

Table of Contents

1 Scope 3
4 Management Requirements 4
4.1 Organization 4
4.2 Management System 7
4.3 Document Control 7
4.4 Review of Requests, Tenders, and Contracts 9
4.5 Subcontracting of Tests and Calibrations 9
4.6 Purchasing Services and Supplies 9
4.7 Service to the Customer 9
4.8 Complaints 10
4.9 Control of Nonconforming Testing 10
4.10 Improvement 10
4.11 Corrective Action 10
4.12 Preventative Action 10
4.13 Control of Records 10
5 Technical Requirements 13
5.1 General 13
5.2 Personnel 13
5.3 Accommodation and Environmental Conditions 15
5.4 Test Methods 15
5.5 Equipment 24
5.6 Measurement Traceability 26
5.7 Sampling 26
5.8 Handling of Test Items 27
5.9 Assuring the Quality of Test Results 29
5.10 Reporting the Results 32

COPY

1 Scope

This manual follows the requirements specified by the Association of Crime Laboratory Directors/Lab Accreditation Board (ASCLD/LAB) International Program which utilizes the ISO/IEC 17025-2005 standards and the 2011 ASCLD/LAB International Supplemental Requirements.

The Digital Evidence Section Quality Manual is written for the analysis of:

- Computer Forensics
- Video Analysis

COPY

4 Management Requirements

4.1 Organization

Personnel Qualifications, Authorities, and Responsibilities
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

1. 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.
2. 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.
3. Performs evidence examination by reviewing submission reports received from law enforcement agencies and analyzing evidence for possible recovery of data.
4. 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.
5. Presents testimony in court as an expert witness, interprets results of forensic examinations, and explains methods used.
6. Attends conferences and training to keep abreast of new technology and forensic methods.
7. Ensures compliance with the ASCLD/LAB accreditation standards.
8. Has the overall responsibility for the technical operations and the provisions of the resources needed to ensure the required quality of laboratory operations.
9. Performs related responsibilities as required or assigned.

COPY

Digital Evidence Analyst

Qualification

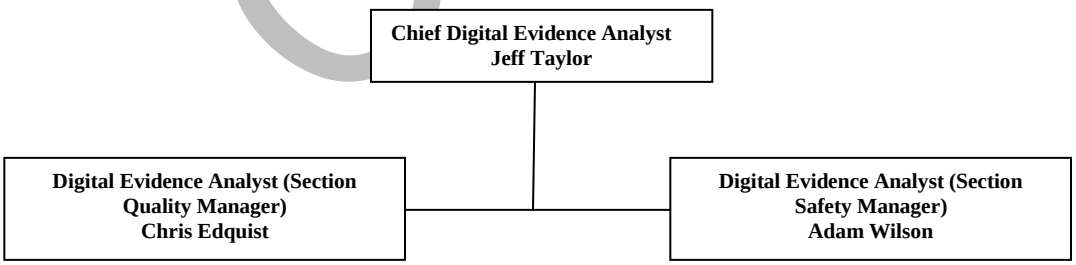
The formal education equivalent of a bachelor's degree with science courses; plus three years' experience in a scientific laboratory. Other job related education and/or experience may be substituted for all or part of these basic requirements upon approval of the Chief Digital Evidence Analyst.

Authorities & Responsibilities

1. Performs evidence examination by reviewing submission reports received from law enforcement agencies and analyzing evidence for possible recovery of data.
2. 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.
3. Presents testimony in court as an expert witness, interprets results of forensic examinations, and explains methods used.
4. Attends conferences and training to keep abreast of new technology and forensic methods.
5. Performs related responsibilities as required or assigned.

COPY

Digital Evidence Organization Chart



Section Quality Manager

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

Section Safety Manager

1. Conducts monthly safety inspections and ensuring that proper practices and procedures are being followed within the section.
2. Maintains records of any safety incidents within the section.
3. Works with the lab wide Health and Safety Manager to seek ways to improve the safety program.

Other Responsibilities

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 Section will have meetings as needed to convey information to subordinates

COPY

4.2 Management System

Digital Evidence Quality Manual

The Digital Evidence Quality Manual (DE-DOC-01) is a compilation of policies and procedures for use in the Digital Evidence section. The quality manual is readily available on Qualtrax. Digital Evidence personnel are responsible for familiarizing themselves with and utilizing these policies and procedures. The quality manual is reviewed annually by the Section Chief and Section Quality Manager and updated as needed to reflect changing organizational, technical and procedural information. This review is documented in Qualtrax.

Deviations

Unforeseen circumstances may arise which require immediate deviations from the policies and procedures of this manual. In such situations, the request for exceptions to policy will be submitted in writing to the Section Chief, or designee, of the laboratory. The request must include an adequate description of the circumstances requiring the action, a statement of the proposed alternative policy and procedure, and the intended duration of the exception. The Section Chief will maintain documentation of the approved policy exception.

COPY

Mission Statement

The Digital Evidence section is responsible for analyzing computers, digital storage devices, and, video evidence for the criminal justice system. This may include systematic retrieval of digital data that may be of evidentiary value, and video enhancement as well as technical support to law enforcement agencies. 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.

Supporting Manuals

ASCL Digital Evidence Section Training Manual (DE-DOC-02) contains a uniform training program for newly hired Digital Evidence Analysts. This document is available on Qualtrax and available to all Digital Evidence Analysts.

4.3 Document Control

Controlled Document Preparation

Documents generated in the Digital Evidence section should be prepared by personnel with adequate knowledge in the subject. The document must include enough detail and

specificity to ensure that the activity conforms to quality specifications and/or expectations.

Controlled Document Review and Approval
Documents generated in the Digital Evidence Section must be reviewed and approved by the QA Manager and Digital Evidence Section Chief. The Digital Evidence Quality Manual will be reviewed and approved by the QA Manager, Chief Digital Evidence Analyst, Scientific Operations Director and Executive Director.

Document Availability
Documents must be available at all locations where operations essential to the effective functioning of the laboratory are performed

Individuals may print hardcopies of internal documents as needed for personal use; however, these copies are unofficial.

Archiving Controlled Documents
Employees will destroy outdated documents upon receiving updated documents. It is the employee's responsibility to verify that they are using the current revision of any document.

Document Changes
Revised documents are subject to the same review, approval, documentation and issuance requirements of the original document as stated above.

When a controlled document is revised, the editor of the document must detail in Qualtrax the changes made. The Document Compare feature in Qualtrax allows the user of the document to see any deletions, additions, and changes to the document.

Steps for Revising a Controlled Document

The Preparer of the document is responsible for:

- Preparing the document in the proper format.
- Addressing or resolving comments from reviewers.

The Section Chief is responsible for:

COPY

- Ensuring that Quality and Training Manual reviews are completed annually.
- Reviewing and approving all discipline specific controlled documents.
- Ensuring that the documents are scientifically suitable for issue.

4.4 Review of Requests, Tenders, and Contracts

Prior to performing analysis in a case, the submission sheet is reviewed to ascertain the type of analysis requested.

By completing and submitting the submission sheet, the agency requesting analysis relinquishes all decisions regarding analytical processing and choice of methods to the ASCL.

Deviations

When an agency requesting analysis agrees to the contract (e.g. ASCL Submission sheet), the agency agrees that the ASCL may make deviations as deemed necessary. The agency will be notified (e.g. iResults, phone call, email, etc.) if a request is cancelled, resulting in no analysis being performed.

Amendments

If the contract needs to be amended after work has begun, all affected personnel shall be notified.

COPY

4.5 Subcontracting of Tests and Calibrations

Refer to ASCL Quality Manual (ASCL-DOC-01)

4.6 Purchasing Services and Supplies

When purchasing items that require certain specifications in order to correctly perform testing, these items and their specifications will be detailed in Qualtrax as a workflow.

4.7 Service to the Customer

Refer to ASCL Quality Manual (ASCL-DOC-01)

4.8 Complaints

Any staff member receiving a complaint should notify their supervisor. The complaint shall be documented and given to the supervisor. The supervisor shall forward the complaint to the Scientific Operations Director who will investigate the situation and notify top management when necessary. When the concern takes on the nature of a complaint about the laboratory's activities or deficiencies in the quality system, the Chief Digital Evidence Analyst will investigate the situation and forward all the information to the QA Manager.

4.9 Control of Nonconforming Testing

All employees and supervisory personnel must be vigilant for any indication of nonconforming tests and work. For Level 1 and Level 2 Non-Conformities the Section Chief and QA Manager will be notified immediately for consultation and to evaluate the significance of the nonconforming testing or work. For further explanation regarding nonconforming testing, see the lab wide quality manual (ASCL-DOC-01)

4.10 Improvement

Suggestions for ways to improve the quality of the Digital Evidence Section are encouraged. (Examples: procedures, policies, technical improvements)

4.11 Corrective Action

Refer to ASCL Quality Manual (ASCL-DOC-01)

4.12 Preventative Action

Refer to ASCL Quality Manual (ASCL-DOC-01)

4.13 Control of Records

Historical non-electronic case files for the Digital Evidence Section are located in a storage cabinet in the Digital Evidence Section.

Discipline quality records such as trainings records, proficiency tests, etc. will be stored in a location designated by the Section Chief and accessible to employees in the section.

Security and Protection of Records

COPY

Digital data pertaining to case examination will be transferred and stored on the forensic server located in the section server room. The server room is equipped with an independent air conditioning system to maintain appropriate temperature. The server room is limited by physical access to section analysts and others as needed by laboratory administration or the section chief. In addition, the server computers are limited by Windows Server user authentication. The server containing the case data makes use of a RAID5 disk array to reduce the risk of data loss. Periodic archival of data storage is accomplished by tape devices (DLT, SDLT, LTO). Upon archival, a spreadsheet is created and stored on the section drive that contains the case numbers on each labeled tape. The subsequent created tape is labeled and placed in a locked cabinet in the section server room.

Data Recording

Dates should be recorded throughout the records to indicate when the work was performed, but a minimum, the starting and ending dates must be recorded. A starting date is recorded at the beginning of examination when the evidence is being documented. An ending date is recorded when the final report is Draft completed. Any corrections will be made by an initialed, single strikeout (so that what is stricken can still be read) by the person making the change. Correction fluid or correction tape may not be used.

Examination and Administrative Records

Examination records are any records generated by the analyst/examiner for a case file (e.g. notes, worksheets, photographs, spectra, printouts, charts and other data). Examination records that are essential for the evaluation and interpretation of the data must be stored in the appropriate folder within the 'Request' folder in the LIMS case file.

The unique Arkansas State Crime Laboratory (ASCL) case number (YYYY-00000) (handwritten or electronically generated) and the analyst's handwritten initials or secure electronic equivalent of initials or signature must be on all examination records in the case file.

All other records contained in the case file will be considered administrative records and will be stored in the 'Case Images' folder in the LIMS case file.

The unique Arkansas State Crime Laboratory (ASCL) case number (YYYY-00000) (handwritten or electronically generated) must be on all administrative records in the case file.

COPY

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

COPY

5 Technical Requirements

5.1 General

Controls
Prior to forensic examination, a control device for the type of case being worked must be acquired to ensure proper working order of hardware or software used in a case. Examples of devices include IDE hard drive, SATA hard drive, GSM cell phone, SIM card, and CDMA cell phone. 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.

5.2 Personnel

Training Program
The Digital Evidence Section Chief shall ensure the competence of all who operate equipment, perform tests, evaluate results, and sign test reports in the Digital Evidence Section. The Section Chief 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, forensic video 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 Section Chief and maintained in the Employee History Binder. More detail of the training program is outlined in *ASCL Digital Evidence Section Training Manual* (DE-DOC-02).

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

Additional Training
Training shall include the application of ethical practices in forensic sciences, a general knowledge of forensic science, and applicable criminal and civil law procedures.

COPY

Job Descriptions
Current job descriptions for personnel involved with testing shall be maintained in their Employee History Binder.

Authorization Documentation
The Digital Evidence Section Chief shall authorize personnel to perform sampling, testing, issuing of reports, and operating particular types of equipment. This authorization documentation shall be part of the competency documentation (see above) and shall be dated and signed by the Digital Evidence Section Chief and maintained in the Employee's History Binder. Each Employee's History Binder shall also contain a curriculum vitae or resume that includes educational and professional qualifications, training, skills and experience. The individual's Training Binder will contain all completed training records.

Technical Personnel Qualifications
Analysts working in the Digital Evidence discipline shall possess a baccalaureate degree with science courses.

Competency Testing
All analysts and technical support personnel that generate analytical results, regardless of academic qualifications or past work experience shall satisfactorily complete a competency test (examination of sufficient unknown samples and taking a written/oral test) in each category of testing in which they intend to perform casework. Satisfactorily completing a competency test means achieving the intended results. Failure to achieve the intended results would require review or retraining until testing achieves the intended results.

COPY

Competency Testing Requirements
For laboratory personnel whose job responsibility includes report writing, a competency test shall include, at a minimum:

- Examination of sufficient unknown samples to cover the anticipated spectrum of assigned duties and evaluate the individual's ability to perform proper testing methods;
- A written report to demonstrate the individual's ability to properly convey results and/or conclusions and the significance of those results/conclusions;
- A written or oral examination to assess the individual's knowledge of the discipline, category of testing, or task being performed; and
- Moot court to demonstrate the individuals' ability to properly convey and present results of evidence in court.

Moot Court may be waived for employees receiving training in additional categories of testing within the same discipline.

Literature

Digital Evidence maintains and provides access to literature resources such as books, articles, and journals on topics relevant to Digital Evidence. Analysts will be assigned a literature review. After completion of review, a log book shall be updated to reflect the article reviewed, initials of reviewer, and date reviewed.

5.3 Accommodation and Environmental Conditions

Access/Security

The Digital Evidence section consists of rooms that are either locked by a key or require a security fob for entry. Security fobs are issued to authorized personnel in order to access these area(s). An *Access Area Approval Form* (ASCL-FORM-10) must be completed prior to giving security fob access to an individual. Analysts in the section are assigned keys to doors, storage cabinets, etc. A key log is kept in the section tracking location of each key. There is key box located in the Section Chief's office. The Section Chief 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

5.4 Test Methods

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.

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. Identify type of hard drive (ex. SATA, IDE)
- Image a control hard drive of same type as evidence drive. Verify the MD5 hash value is correct

COPY

- 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
- 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

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

Examination of original digital evidence 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.

COPY

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.

COPY

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.
- Acquire control phone of same type (GSM/CDMA)
- Determine the best possible method for retrieval of the data stored on the handheld device.
- If possible, acquire the device prior to removal of the battery or 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

Video Analysis (Analog)

- *DE-FORM-07 Forensic Video Examination Worksheet* is available on Qualtrax to document the package description, evidence description, controls, evidence details, operations performed/settings and examiner remarks. *DE-FORM-08 Forensic Video Item Description Worksheet* is available on Qualtrax to document the item's description. The requirements detailed below will be documented on these forms, where appropriate and necessary.
- Document information about the evidence media. Documentation must include case number, examiner name/initials, page number, and date.
- Perform a visual inspection of the tape and housing to ensure housing is intact and that there is no damage. If damage is found, take corrective action and document
- Enable any record-protection device (e.g. punch-out tab, slide record tab, remove record button). Document any alteration make to evidence media.
- If possible, determine if the submitted evidence media is an original or a copy and document. If submitted evidence media is a copy, attempt to obtain the original evidence media.
- If possible, determine the make, model, and settings of the device used to record the submitted evidence media and document
- Determine the appropriate playback device to achieve optimal video quality
- Capture video from a control VHS tape containing SMPTE color bars to verify capture software is functioning correctly.
- Ensure the resulting captured video represent original media by performing a visual inspection and that the output settings fall within acceptable ranges.
- A working digital copy of the pertinent segment(s) is generated, and a visual inspection is performed to ensure working copy accurately represents original evidence media.
- Document that the control was performed and that the expected results were acquired. Then proceed with examination of evidence media.
- Determine video settings of evidence including, but not limited to, frame rate and pixel dimensions (e.g. 320 x 240)
- Review the submitted evidence media to locate pertinent segments.
- Determine the appropriate playback settings for processing
- Obtain MD5 hash values for each digital working copy file.
- De-interlace video if field based footage
- De-multiplex video if needed
- If necessary, still images from video may be generated
- The images may be enhanced using a number of processing operations that may include, but are not limited to histogram equalization, frame averaging, color correcting, and sharpening. Document settings used in these operations.

COPY

- Verify and document MD5 hash value match of working copies from forensic computer workstation to server before archival.
- The final images are output to appropriate media.

Digital Video Recorder (DVR) Evidence Retrieval

- *DE-FORM-07 Forensic Video Examination Worksheet* is available on Qualtrax to document the package description, evidence description, controls, evidence details, operations performed/settings and examiner remarks. *DE-FORM-08 Forensic Video Item Description Worksheet* is available on Qualtrax to document the item's description. The requirements detailed below will be documented on these forms, where appropriate and necessary.
- Document information about the evidence device. Documentation must include case number, examiner name/initials, page number, and date.
- Remove the hard drive(s) from the DVR using appropriate tools.
- Document the hard drive make, model, capacity, serial number, and jumper settings.
- 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 for return to agency
- Determine the best method to retrieve the data for video enhancement. This may include extracting digital video files to the forensic video workstation or restoration of hard drive image files to another similar hard drive (forensic hard drive clone)
- If a clone drive is produced, install in the DVR and power on.
- Document any changes made to DVR settings needed for examination.
- Document DVR system date/time and compare to actual date/time to establish an approximate offset.
- Document any current settings of the DVR as well as date/time ranges for each camera if possible.
- Collect data from DVR using options that may provide the native file format or best evidence format.
- If video is to be captured through analog channels with Avid Video Capture software tool, first capture video from a control VHS tape containing SMPTE color bars to verify capture software is functioning correctly.
- Ensure the resulting captured video represent original media by performing a visual inspection and that the output settings fall within acceptable ranges.

COPY

- Connect DVR to video breakout box with the best available connection (BNC, S-Video, RCA). Document this connection option.
- A working digital copy of the pertinent segment(s) is generated, and a visual inspection is performed to ensure working copy accurately represents original evidence media.
- Document that the control was performed and that the expected results were acquired. Then proceed with examination of evidence media.
- If video is able to be digitally exported from DVR, transfer recovered media to forensic workstation. Calculate, verify, and document MD5 hash values for copy to forensic workstation and then subsequent copy to forensic server for archival.
- If digital files are recovered from hard drive image files, calculate, verify and document MD5 hash values for copy to video enhancement workstation and then subsequent copy to forensic server for archival.

COPY

Video Analysis (Digital)

- *DE-FORM-07 Forensic Video Examination Worksheet* is available on Qualtrax to document the package description, evidence description, controls, evidence details, operations performed/settings and examiner remarks. *DE-FORM-08 Forensic Video Item Description Worksheet* is available on Qualtrax to document the item's description. The requirements detailed below will be documented on these forms, where appropriate and necessary.
- Document information about the evidence media. Documentation must include case number, examiner name/initials, page number, and date.
- If possible, determine if the submitted evidence media is an original or a copy and document. If submitted evidence media is a copy, attempt to obtain the original evidence media.
- If possible, determine the make, model, and settings of the device used to record the submitted evidence media and document.
- Perform a virus scan(s) on digital video file(s) that are submitted as evidence.
- Obtain MD5 hash values for each file, copy over evidence file(s) to the forensic workstation, then hash resulting master working copy(ies) to verify a bit-for-bit match was copied. All subsequent working copies should be generated from the master working copy. Document that the hash values match.
- Prior to examination of evidence media capture video from a control digital video file with Camtasia (or other capturing software) to verify capture software is functioning correctly.
- Ensure the resulting captured video file represents original media by performing a visual inspection and that the proper settings were maintained such as aspect ratio and frame rate.
- Document that the control was performed and that the expected results were acquired. Then proceed with examination of evidence media.
- Determine video settings of evidence including, but not limited to, frame rate and pixel dimensions (e.g. 320 x 240).
- Determine the appropriate playback settings for processing; if possible, capture video from the native file format using the proprietary video player.
- A working digital copy of the pertinent segment(s) is generated, and a visual inspection is performed to ensure working copy accurately represents original evidence media and that settings such as frame rate and aspect ratio are maintained.
- Using the selected device and settings, review the submitted evidence media to locate pertinent segments.
- De-interlace video if field based footage
- De-multiplex video if needed

COPY

- Processes applied to working copy(ies) should be documented in the order in which there were applied to ensure integrity and the reproducibility of the results.
- If necessary, still images from video may be generated
- The images may be enhanced using a number of processing operations that may include, but are not limited to histogram equalization, frame averaging, color correcting, and sharpening. Document settings used in these operations.
- The final images are output to appropriate media.
- Verify and document MD5 hash value match of original evidence and working copies from forensic computer workstation to server before archival.

Deviation

If it becomes necessary to make a deviation from a documented method and/or procedure, it must be technically justified and authorized by the Digital Evidence Section Chief. The deviation will be documented in the case record. The Section Chief will keep a log of method/procedure deviations.

Selection of Methods

The Digital Evidence Section shall use test methods that meet the needs of the customer (refer to Section 4.7 *Service to the Customer* in the ASCL Quality Manual (ASCL-DOC-01)) 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.

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.

Laboratory-Developed Methods

COPY

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.

COPY

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.

Validation of Methods
Refer to ASCL Quality Manual (ASCL-DOC-01)

Control of Data
When a case has been 'draft completed', the individual has ensured that they have checked all calculations and data transfers for accuracy and that the calculations conform to written procedures. By completing the technical review, the technical reviewer is confirming that they have checked the calculation(s) and data transfers for accuracy.

Digital Evidence Data
When computers or automated equipment are used for the acquisition, processing, recording, reporting, storage, or retrieval of evidence, Digital Evidence ensures that

a. Computer software is documented in sufficient detail and suitably validated/verified.

b. 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.

c. 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.

5.5 Equipment

Instruments used in the Digital Evidence section for the testing of evidence are Processing and Imaging Computers, a Universal Forensic Extraction Device (UFED),

COPY

used in the processing of cell phones/smartphones/tablets, and a Forensic Video Computer System, used in the processing of video evidence.

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). This operation should be completed each week and the results placed in the Computer Maintenance Log. There is a separate log for each processing and imaging computer. For the UFED, verify it powers up correctly, and that it displays date and time and proper serial number of device. For the Forensic Video Computer System, verify the computer successfully passes the POST test and the breakout box loads properly.

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, and this training will be documented and kept in each individual's Employee History Binder. Up-to-date instructions on the use and maintenance of the instrument/equipment shall be readily available for use.

Instrument/Equipment Identification

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

Instrument/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 include date of maintenance item, initials of who performed the maintenance, and remarks about the maintenance performed.

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 Section Chief's 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

COPY

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 Digital Evidence Section Chief 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.

Instrumentation/Equipment 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 Section Chief shall take into consideration the effect the problem may have had on previous tests.

COPY

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.

5.6 Measurement Traceability

Refer to ASCL Quality Manual (ASCL-DOC-01)

5.7 Sampling

Refer to Section 5.4 of this manual for techniques utilized for each method.

5.8 Handling of Test Items

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.

Evidence Retention

Once the processing of evidence is complete as outlined in section 5.4 of this manual, the original evidence is packaged back up in its original container, sealed, and submitted back to the Evidence Receiving section of the lab.

Sub-Items

Items which are subdivided in the laboratory shall be tracked through the documented chain of custody to the same extent that original items are tracked.

Evidence 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

COPY

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.

Test Item Identification

A unique case number is assigned to every case when evidence is initially received by ASCL. Each exterior container must have its unique barcode label affixed to it. Agency evidence numbers will be used to identify the evidence whenever practical.

If testing requires that uniquely identified items be subdivided within the laboratory, appropriate sub-item identifiers shall be assigned and the item(s) labeled by the analyst so that the sub-item may be easily tracked and identified as having originated from a particular item.

Suitability of Test Items

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 Digital Evidence Section Chief 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 Digital Evidence Section Chief 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).

COPY

Safeguarding the Integrity of Evidence
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.

Unattended 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 all analysts are out on lunch break, the doors in the section must be shut and locked. 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.

Evidence Marking
All evidence will be marked or identified with the laboratory case number (e.g. YYYY-000000), 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.

5.9 Assuring the Quality of Test Results

Proficiency Testing
Proficiency tests are presented to the Digital Evidence Section to demonstrate the reliability of the sections 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 ASCLD/LAB approved provider if available. If an approved provider is unavailable, an external proficiency test must be obtained from another source.

COPY

In addition, each examiner must be proficiency tested (internal or external) at least once, during each five-year accreditation cycle, in each category of testing in which the examiner performs casework.

Each Section Chief or designee shall maintain a log of proficiency testing in the individual's Employee History Binder. This log shall contain the following:

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

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 Form (ASCL-FORM-08), when applicable

Each Section Chief 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.

Each Section Chief 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 Section Chief must notify the Quality Assurance Manager.

COPY

- 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 Section Chief must initiate a Corrective Action Request in Qualtrax.

Proficiency Record Retention
Proficiency testing records will be retained for at least 15 years.

Case Review
All cases will be technically and administratively reviewed prior to the release of the report. The review process must confirm that electronic versions of all necessary documentation are in the imaging module of LIMS. The review process will be documented on the *Digital Evidence Case Review Form (DE-FORM-01)*.

If a reviewer discovers an error in the case record, the reviewer must document the error on the *ASCL Digital Evidence Case Review Form (DE-FORM-01)* and inform the analyst. If the analyst and the reviewer cannot reach consensus, then both the analyst and reviewer must meet with the Section Chief (or designee) for resolution.
All non-conforming work identified during review will be handled according to Section 4.11 *Corrective Action.*

Technical Review
Refer to ASCL Quality Manual (ASCL-DOC-01)

Administrative Review
Refer to ASCL Quality Manual (ASCL-DOC-01)

Testimony Review
Refer to ASCL Quality Manual (ASCL-DOC-01)

Testimony Record Retention
Records of testimony monitoring will be retained for at least 15 years.

COPY

5.10 Reporting the Results

General

When analytical conclusions and/or opinions are made on evidence submitted for analysis, a 'Report of Laboratory Analysis' will be issued to the investigating agency. The results shall be reported accurately, clearly, unambiguously and objectively. Each analyst/examiner will proofread and sign their reports ensuring the report is accurate and error-free. LIMS allows the analyst to sign their reports electronically.

Laboratory Report Exceptions

A laboratory report is not required when a case is adjudicated or the customer cancels the request before the work or report is completed.

Reports

The laboratory report will contain, at a minimum, the following information except where an alternate location is named.

a) The title, 'Report of Laboratory Analysis.'
b) The name Arkansas State Crime Laboratory and the address of the laboratory that performed the test.
c) Unique ASCL Case # (YYYY-000000) and page number x of x on each page of the report.
d) Investigator's name, investigator's agency and the address of agency.
e) The tests performed will be documented in the analytical notes.
f) Unambiguous identification and description of the item(s). The description may include the general condition of the item (i.e. wet, glass broken, etc.). A more detailed description of the condition of the item, if applicable, will be in the analytical notes.
g) The date the items were received by the laboratory will be documented on the *Evidence Submission Form* (ASCL-FORM-12/_WD). The date(s) of testing will be documented in the examination record.
h) When sampling is used, the report will be clear that the results are based on a sampling plan. Details about the sampling plan must be clearly documented in the examination record.
i) The results of testing and, where appropriate, the units of measurement.
j) The name, title and electronic signature of the analyst.
k) The following statement will appear on all reports, "The results stated above relate only to the items tested."
l) The following statement will appear on all reports, "This is only an official ASCL report when reproduced in full."

COPY

Opinions and Interpretations
The following statement will appear on all laboratory reports, "The following represents the interpretations/opinions of the undersigned analyst."

Electronic Transmission of Results
The analyst's signature on the laboratory report is electronically secure and may only be affixed with scanning of an analyst's barcode and the use of a PIN number. After the case has been administratively reviewed, the document becomes a static PDF file.

Reports are normally disseminated to the customer through JusticeTrax iResults. Facsimile or email may be used to transmit results to the customer, but the employee must follow Arkansas State Statute 12-12-312 and the policy on *Confidentiality of Records* (ASCL-DOC-01 Section 4.13.1.3).

Report Format
ASCL reports are generated using the LIMS and will be formatted in a manner to accommodate the types of tests conducted and to minimize the possibility for misunderstanding or misuse. Section Chiefs should ensure that discipline report designs are optimized for the clear presentation of test results.

Supplemental and Amended Reports
Refer to ASCL Quality Manual (ASCL-DOC-01)

Report CD
A Forensic Report CD (or DVD) may be generated detailing information about the evidence and findings that are of interest to a case.

COPY