ARKANSAS STATE CRIME LABORATORY

Digital Evidence Section

Quality Manual

Section Chief:
Jeff Taylor

TABLE OF CONTENTS: **Page**

1.0 Introduction **5**
1.1. Organization and Management Structure 5
1.1.1. Organizational Chart 5
1.1.2. Management
2.0 Personnel Qualifications and Job Descriptions **5**
2.1. Job Descriptions 5
2.1.1. Chief Digital Evidence Analyst 5
2.1.1.1. Working Relationships 6
2.1.1.2. Special Job Dimensions 6
2.1.1.3. Knowledge, Abilities, and Skills 6
2.1.2. Digital Evidence Analyst 6
2.1.2.1. Working Relationships 7
2.1.2.2. Special Job Dimensions 7
2.1.2.3. Knowledge, Abilities, and Skills 7
2.2. Educational Qualifications 7
2.2.1. Chief Digital Evidence Analyst 7
2.2.2. Digital Evidence Analyst 7
2.3. Special Training Requirements 8
2.3.1. Training Prior to Casework 8
2.3.2. Current Literature 8
2.3.3. Training Sessions 8
2.4. Documentation of Training 8
2.5. Meetings 9
3.0 Facilities/Security 9
4.0 Evidence Control 9
4.1. Evidence Accession 9
4.1.1. Chain of Custody 9
4.1.2. Secure Storage 10
4.1.3. Evidence Seals 10
4.1.4. Package Identification 10
4.2. Evidence Handling 10
4.3. Documentation of Evidence and Packaging 11
4.4. Release of Evidence 11
4.5. Release of Information 11
4.6. Disposition 11
4.7. Purging 11
4.8. Destruction 11
4.9. Evidence Assessment 12
4.9.1. Evidence Definitions 12
4.9.2. Evidence Assessment by Supervisor 12

4.10. Policy Statements 12
5.0 Validation 12
6.0 Analytical Procedures 13
6.1. Digital Evidence Recovery 13
6.1.1. Training 13
6.1.2. Evidence Assessment 13
6.1.3. Preparation 13
6.1.3.1. Proper Working Order of Forensic Computer 13
6.1.3.2. Control 13
6.1.4. Procedure 13
6.1.4.1. Hard Drive Examination 13
6.1.4.2. Removable Media Examination 14
6.1.4.3. Laptop Examination 14
6.1.4.4. Handheld Device Examination 15
6.1.5. Verification 16
6.1.6. Quality Assurance/Quality Control 16
6.1.7. Notes/Documentation 16
6.1.8. Assessment of Results 17
6.1.8.1. Reporting 17
6.2. Forensic Video Analysis 17
6.2.1. Training 17
6.2.2. Evidence Assessment 17
6.2.3. Preparation 17
6.2.3.1. Proper Working Order of Forensic Video System 17
6.2.3.2. Control 17
6.2.4. Procedure 18
6.2.4.1. Video Analysis 18
6.2.5. Validation 18
6.2.6. Quality Assurance/Quality Control 18
6.2.6.1. Record Protection 18
6.2.6.2. Essential Equipment 19
6.2.7. Notes/Documentation 19
6.2.8. Assessment of Results 19
6.2.8.1. Reporting 19
7.0 Proficiency Tests 19
7.1. Sources of Testing 20
7.1.1. Manufacturers 20
7.1.2. Other External Providers 20
7.1.3. Internal Testing 20
7.2. Types of Errors and Corrective Action 20
8.0 Court Testimony Review 21
9.0 Case Records 21
9.1. Report Format 21
9.2. Documentation 21

9.3. Technical and Administrative Review 21
9.3.1. Technical Review 22
9.3.2. Administrative Review 22
9.3.3. Types of Errors and Corrective Action 22
10.0 Audits 23
11.0 Complaints 23
12.0 Safety 23

DIGITAL EVIDENCE SECTION

1.0 Introduction

The Digital Evidence section is responsible for analyzing computers, digital storage devices, video and audio evidence for the criminal justice system. This may include systematic retrieval of digital data that may be of evidentiary value, video and audio tape recovery and 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.

1.1 Organization and Management Structure

1.1.1 Organizational Chart:

Governor
Executive Director
Scientific Operations Director
Chief Digital Evidence Analyst
Digital Evidence Analysts

1.1.2 Management

This manual has been approved by the appropriate management authorities and as such is accepted as the routine operating policy of the Digital Evidence Section within the Arkansas State Crime Laboratory.

2.0 Personnel Qualifications and Job Descriptions

2.1 Job Descriptions

2.1.1 Chief Digital Evidence Analyst

- Supervision of a professional staff. Duties include: interviewing, hiring, and training applicants; remediation of procedural issues; review of case files to maintain the quality o f 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.
- Performs related responsibilities as required or assigned.

2.1.1.1 Working Relationships

The Chief Digital Evidence Analyst has regular contact with other laboratory sections, law enforcement officials, attorneys, criminal/civil court personnel, and peers in other states.

2.1.1.2 Special Job Dimensions

Occasional in or out-of-state travel and on-call duty may be required.

2.1.1.3 Knowledge, Abilities, and Skills

- Knowledge of systems and procedures to duplicate, recover, preserve and examine digital evidence.
- Knowledge of hardware and software used in digital evidence examinations.
- Knowledge of laws, regulations, and agency policies governing forensic computer analysis.
- Knowledge of rules of evidence as they apply to the storage, custody, and handling of digital evidence.
- Ability to plan, organize and oversee the work of subordinates.
- Ability to conduct and direct the activities of a digital evidence section.
- Ability to conduct research, prepare and present training on methods of collecting and preserving evidence.

2.1.2 Digital Evidence Analyst

- 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.

2.1.2.1 Working Relationships

The Digital Evidence Analyst has regular contact with other laboratory sections, law enforcement officials, attorneys, criminal/civil court personnel, and peers in other states.

2.1.2.2 Special job Dimensions

Occasional in or out-of-state travel and on-call duty may be required.

2.1.2.3 Knowledge, Abilities, and Skills

- Knowledge of systems and procedures to duplicate, recover, handle/preserve and examine digital evidence.
- Knowledge of hardware and software used in digital evidence examinations.
- Knowledge of laws, regulations, and agency policies governing forensic computer analysis.
- Knowledge of rules of evidence as they apply to the storage, custody, and handling of digital evidence.
- Ability to conduct research, prepare and present training on methods of collecting and preserving evidence.
- Performs related responsibilities as required or assigned.

2.2 Educational Qualifications

2.2.1 Chief Digital Evidence Analyst

- 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 Qualifications Review Committee.

2.2.2 Digital Evidence Analyst

6. 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 Qualifications Review Committee.

2.3 Special Training Requirements

2.3.1 Training Prior to Casework

- The analyst must demonstrate their competence before performing independent casework. This is ensured by requiring the analyst to successfully complete the Digital Evidence Training Manual. This manual must include the following:

    - Working with a qualified analyst in the specific area of analysis to be tested. The duration of this training is dependent upon the type of analysis. The areas of training will be recorded in the individual's training manual. At the completion of this course, the training analyst or supervisor will determine if additional training is needed.
    - Reading and signing off on assigned literature pertaining to the subject matter. This material is assigned by the training analyst or the supervisor.
    - Passing a written competency examination (Tests given during training courses may be substituted).
    - Passing an analytical proficiency test given in the area of analysis to be tested.
    - Participating in at least one moot court (This requirement may be waived if trainee has previous experience as an expert witness or if moot court was performed in another discipline).

2.3.2 Current Literature

- Analysts will be assigned articles on a monthly basis by the supervisor. In addition, pertinent literature will be available for analysts. Analysts are encouraged to maintain knowledge of technology updates and analytical practices by use of internet and periodicals.

2.3.3 Training Sessions

- Each analyst will take part in at least one training session every year. This may include structured in-house training in a scientific discipline to which the analyst is assigned or is being trained.

2.4 Documentation of Training

- Each analyst will be supplied with a binder. All training certificates, college transcripts, proficiency test results, and reviews of testimony will be kept in the binder. It is the responsibility of the individual analyst to keep the binder up to date.

2.5 Meetings

- Section meetings will be held once a month or as often as deemed necessary by the supervisor.

3.0 Facilities/Security

3.1 Arkansas State Crime Laboratory

The Arkansas State Crime Laboratory building has security cameras that observe all points of ingress and egress. Security cameras are located outside the building and on the ground floor of the building. Access from the ground floor to any other floor is controlled by a key-card system that logs the time and date of any entry. Unauthorized personnel must sign in and be accompanied by authorized personnel to proceed to the basement, the second floor or the third floor.

3.2 Digital Evidence Section

The Digital Evidence section is secured by lockable doors. Keys are only issued to analysts within the section and to administration. Each analyst has a set of lockable drawers and cabinets. Keys to these are issued only to the analyst and the section supervisor.

4.0 Evidence Control

4.1 Evidence Accession

The integrity of evidence must be maintained and documented. Several steps are necessary to ensure this integrity. First is a chain of custody system (4.1.1) that tracks the transfer of each package of evidence through accession, analysis, storage and return to the agency. Second is a system of secure storage (4.1.2) that ensures no unauthorized access to evidence. Third is a system of proper evidence seals (4.1.3). Fourth is a system of package identification (4.1.4) that ensures no two items of evidence are mistaken for one another. Through this combination of policies, the integrity of the evidence can be maintained. The identity, location, security and history of each piece of evidence are assured.

4.1.1 Chain of Custody

- A detailed explanation of the chain of custody system can be found in the quality manual of the Evidence Receiving section.
- The Digital Evidence analyst should make the request for evidence items to the Evidence Receiving Section that they wish to obtain. The transfer of these individual pieces of evidence is tracked by the transfer of the package that contains them, which is identified by the barcode associated with the package.

4.1.2 Secure Storage

While in the possession of an analyst, evidence must be controlled at all times. This requires that the evidence be observed or secured. If the analyst is to leave the evidence for an extended period of time, it must be stored in a secure area. A secure area must have access limited to the analyst working the associated case, the supervisor, and administration.

4.1.3 Evidence Seals

Evidence must be in a sealed condition when accepted into the laboratory. It must remain sealed until opened by an analyst. The analyst should, if possible, avoid damaging seals on the evidence made by others. The case file must reflect any opening of the evidence. The analyst must then reseal the package before returning it to the Evidence Receiving section. All seals must be initialed in order to identify who sealed the evidence.

4.1.4 Package Identification

Please see the Arkansas State Crime Laboratory Quality Manual (ASCL-DOC-01) section 4.6 for package identification.

4.2 Evidence Handling

All evidence must be handled in a manner that preserves the integrity and usefulness of the evidence as much as possible. This is discussed more specifically in the sections of the quality manual dealing with the different analytical procedures.

In general, the original condition of the evidence should be maintained as much as possible while performing all necessary analyses. Nondestructive techniques are preferred over destructive techniques, given that the results obtained through each method of analysis are equally valid and useful. Where modification of the evidence is necessary, all modifications performed by the analyst should be noted in the case file. If such modifications are an integral part of a standard method of analysis, a notation of the method of analysis used will suffice.

4.3 Documentation of Evidence and Packaging

General notes must include:

- The case number assigned by the evidence receiving section.
- The initials of the analyst performing the analysis.
- The date the evidence processing was initiated by the analyst.
- The evidence number for each piece of evidence submitted for analysis.
- A detailed description of packaging.
- A description of the contents of each item of evidence.
- Any comments by the analyst concerning the packaging or condition of the evidence or of any variation from routine procedure.

4.4 Release of Evidence

The Digital Evidence Analyst should transport the evidence to the Evidence Receiving Section upon completion of the analysis. Record will be made of the transfer.

4.5 Release of Information

- The release of case information is covered in the Arkansas State Crime Laboratory Quality Manual (ASCL-DOC-01) section 9.2.2.

4.6 Disposition

All evidence will be returned to Central Evidence Receiving after analysis.

4.7 Purging

Case files are scanned or documented into the LIMS system. After administrative review is completed, the paper case files are shredded. The electronic version is considered the official case record.

4.8 Destruction

The Digital Evidence Section does not destroy any original evidence. All evidence is returned to the respective law enforcement agency and all electronic case files are retained permanently.

4.9 Evidence Assessment

4.9.1 Evidence Definitions

- *Digital Evidence:* information of probative value stored or transmitted in digital form.
- *Physical Items:* items in which digital evidence or information may be stored and/or through which digital evidence is transferred.
- *Original Digital Evidence*: physical items and the digital evidence associated with such items at the time of acquisition or seizure.
- *Duplicate Digital Evidence*: an accurate digital reproduction of all digital evidence contained on an original physical item.
- *Forensic Image File*: A bit-by-bit stream accurate reproduction of information contained on an original digital evidence item.

The Arkansas State Crime Laboratory Digital Evidence Section only recognizes original digital evidence as items to be submitted to the court system. Any duplicate digital evidence or forensic image file is considered a working copy and must be securely stored but does not adhere to the same evidence tracking requirements as original digital evidence.

Forensic Image files will be secured on the forensic server and as present on backup media.

4.9.2 Evidence Assessment by Supervisor

The supervisor or his/her designee will evaluate each case to determine:
- What the law enforcement officer wants/needs with regards to each item of evidence.
- If the ASCL is equipped to perform the requested analysis. If not, the supervisor will assist the officer in location of a laboratory that performs said analysis.
- Which analyst(s) will be assigned to the case?

The above may require a conversation with the officer for clarification of the analysis needed. The supervisor may require the assigned analyst to make the assessment and plan a course of action.

4.10 Policy Statements

The Digital Evidence Section reserves the right not to analyze any evidence that is improperly packaged.

5.0 Validation

Validation is covered in the Arkansas State Crime Laboratory Quality Manual (ASCL-DOC-01) section 5.

6.0 Analytical Procedures

6.1 Digital Evidence Recovery

6.1.1 Training

- Training will be conducted by a qualified digital evidence analyst.
- Completion of proficiency, written tests, and moot court. Moot court may be waived if previously completed in another discipline.

6.1.2 Evidence Assessment

- An initial physical examination of the submitted computer system and all associated media should be conducted and documented. Any unusual findings should be documented as well.

6.1.3 Preparation

- All software should be verified and properly licensed for use by the analyst or the Digital Evidence section.

6.1.3.1 Proper Working Order of Forensic Computer

The forensic computer 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 Log Book located in the section.

6.1.3.2 Control

Prior to forensic image creation, a control floppy and/or hard drive must be imaged to ensure that the software or hardware employed in the imaging process does not make alterations or deletions to the digital evidence media.

- A control floppy or hard disk is created by placing multiple files of varying types on it. A MD5 hash is created for the disk and recorded.
- Prior to the imaging of evidence media, this control disk is imaged, the contained files presence verified, the MD5 hash values after imaging are compared to that created prior.
- After successful completion of this process, the result is documented in the case information and the evidence media may then be imaged.

6.1.4 Procedure

6.1.4.1 Hard Drive Examination

- Remove hard disk from the suspect computer tower and document cabling locations.

- Document the storage capacity, make, model, and serial number of the hard disk if available.
- Make an exact bit stream image file of the hard disk using verified software and hardware write blocking tools.
- Place the image file on the forensic server or examination workstation.
- Package and seal the original hard disk 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 or examination worksheet.
- Copy all pertinent "evidence" files to an evidence folder/directory on the forensic server or examination workstation, and make a CD or DVD of evidentiary files and forensic report for the submitting agency/officer.

6.1.4.2 Removable Media Examination

- All removable media associated shall be itemized and labeled properly prior to examination.
- Removable media shall be write-protected if possible prior to examination.
- Make an exact bit stream image file of the removable media using verified software and hardware write blocking tools.
- Place the image file on the forensic server or examination workstation.
- Package and seal the removable media in an envelope 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 examination worksheet.
- Copy all pertinent "evidence" files to an evidence folder/directory on the forensic server or examination workstation, and make a CD or DVD of evidentiary files and forensic report for the submitting agency/officer.

6.1.4.3 Laptop Examination

- Examination via a network cable:
  - The make, model and serial number of the laptop shall be documented prior to examination.
  - A bootable floppy or CD disk shall be placed into the laptop computer and the computer started.

- After the laptop is started, enter the CMOS setup menu by pressing the appropriate set of keys listed on the screen (usually esc, del., F1, or F8). Document the changes made.
- Change the boot sequence value to boot from the inserted disk. Then exit and save the new settings.
- Shut off the laptop computer; attach the network cable to the examination workstation.
- Create an image file of the laptop hard disk using validated software.
- Place the image file on the forensic server or examination workstation.
- Package and seal the laptop computer 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 examination worksheet.
- Copy all pertinent "evidence" files to an evidence folder/directory on the forensic server or examination workstation, and make a CD or DVD of evidentiary files and forensic report for the submitting agency/officer.

- **Examination via 2.5" to 3.5" adapter**

  - Document the storage capacity, make, model, and serial number of the hard disk if available.
  - Make an exact bit stream image file of the hard disk using verified software and hardware write blocking tools.
  - Place the image file on the forensic server or examination workstation.
  - Package and seal the original hard disk 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 or examination worksheet.
  - Copy all pertinent "evidence" files to an evidence folder/directory on the forensic server or examination workstation, and make a CD or DVD of evidentiary files and forensic report for the submitting agency/officer.

6.1.4.4 Handheld Device Examination (Cell Phones and Personal Digital Assistants)

- Document the make, model, and serial number of the device submitted for examination.
- 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. 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 the handheld device with verified software and hardware to an evidence folder/directory on the forensic server or examination workstation, and make a CD or DVD of evidentiary files and forensic report for the submitting agency/officer.

6.1.5 Verification

- All software packages and hardware devices used for the examination of digital evidence should be verified prior to used in the lab to ensure that they properly performs the actions claimed.

6.1.6 Quality Assurance/ Quality Control

- Examination of original digital evidence shall be performed in a forensically sound manner ensuring that data contained on the 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.
- 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.
- A forensic image of all original digital evidence shall be made using verified software utilities.
- 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 duplication process.
- Examination of the evidence shall be in accordance with what the submitting agency has requested. This may include all 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 shall also be examined and the passwords recovered. This process is to ensure that no data that has been intentionally hidden or disguised is overlooked. An exception to this is when there is an overwhelming amount of incriminatory evidence found among the active files. In this case, no other searches are necessary.

6.1.7 Notes/ Documentation

- Full documentation of all procedures performed and software used shall be recorded for every examination and added to the case file.

6.1.8 Assessment of Results

6.1.8.1 Reporting

- A case report shall be generated stating the items and general results.
- A digital html forensic report of the entire case will be generated to detail the evidence and the resulting data recovered during the examination process.
- Following examination, a CD or DVD, containing all the relevant files and digital forensic report will be generated and released to the investigating agency.

6.2 Forensic Video Analysis

6.2.1 Training

- Training will be conducted by a qualified digital evidence analyst.
- Completion of a written knowledge based test, competency test, and moot court. Moot court may be waived if previously completed in another discipline.

6.2.2 Evidence Assessment

- An initial physical examination of the integrity of the submitted video media and all associated media should be conducted and documented. Any deficiency (damage, write protections not in place, etc.) should be documented and resolved before any forensic video analysis proceeds.
- An assessment may be necessary to determine what kinds of enhancement or procedure is needed based on the type of video encountered or what the submitting agency requests.
- Priority should be given to other forensic examinations before any forensic video analysis proceeds.

6.2.3 Preparation

All software should be properly licensed for use by the analyst or the Digital Evidence section.

6.2.3.1 Proper Working Order of Forensic Video System computer

The video system computer 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 Log Book located in the section.

6.2.3.2 Control

A video control tape with standard bars and tone will be acquired prior to evidence VHS tapes to ensure that the system is within operational parameters for video acquisition. The result will be recorded in a logbook maintained for the video enhancement system.

6.2.4 Procedure

6.2.4.1 Video Analysis

a) A: Do a visual inspection of the tape and cassette housing to :
   - Ensure housing is intact
   - Inspect tape for damage (e.g., twisting, separation)
   - If damage is found, take corrective action and document

b) Enable any record-protection device (e.g., punch-out tab, slide record tab, remove record button). Document any alteration made to evidence tape in the case file.
c) If possible, determine if the submitted tape is an original or a copy and document.
d) If possible, determine the make, model, and settings of the device used to record the submitted video and document.
e) Determine the appropriate playback device to achieve optimal signal quality.
f) Using the selected device and settings, review the submitted video to locate the pertinent segments.
g) Determine the appropriate playback setting for processing.
h) A working digital copy of the pertinent segment may be generated.
i) De-interlace video if field based footage.
j) De-multiplex video if needed.
k) The images may be enhanced using a number of processing operations that may include but are not limited to histogram equalization, frame averaging, color correction, sharpening.
l) The final images are output to appropriate media.

6.2.5 Verification

- All software packages and hardware devices used for the examination of video evidence should be verified prior to use in the lab to ensure that they properly performs the actions claimed.

6.2.6 Quality Assurance / Quality Control

6.2.6.1 Record Protection

For the purpose of evidence preservation, upon seizing the video evidence, action should be taken to ensure the evidence is not changed:

- For analog video evidence, the record tab needs to be removed or moved to a saved position.
- For digital video evidence, write protection needs to be employed for the device that contains the video.

6.2.6.2 Essential Equipment

- Analog Video Monitor: A monitor with the ability to view the underscan area of the NTSC analog video signal.
- Video Playback Deck: A real-time S-VHS deck with a built in frame synchronizer or Time Base Corrector (TBC) should be used to playback or digitize video evidence.
- Digital Non-linear Video Editing System: The analysis computer system and digital capture hardware should have the ability to digitize the complete NTSC signal using a uncompressed or lossless compression format, view consecutive images at the field level, and process video without the addition of artifacts.

6.2.7 Notes/ Documentation

- Full documentation of all procedures performed shall be recorded for every examination and added to the case file.

6.2.8 Assessment of Results

6.2.8.1 Reporting

- The resulting product of forensic video analysis may take several forms depending on the needs of the investigating agency.
- An example of storage media used for product archiving may include CD, DVD, analog tape, or hard-copy print.
- Following examination, this storage media containing all the relevant files will be generated and added to the case in JusticeTrax.
- A report is created for the Digital Evidence request in JusticeTrax.

7.0 Proficiency Tests

Proficiency tests are presented to the laboratory and its staff to demonstrate the reliability of the laboratory's 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 laboratory is judged and is an essential requirement in assessing the integrity of this laboratory.

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

7.1 Sources of Testing

7.1.1 Manufacturers

External proficiency tests are provided yearly from DFQS for forensic computer analysis. An internal forensic computer test is available from IACIS that is administered for the use of the CFCE certification renewal.

7.1.2 Other External Providers

Other accredited laboratories may be called upon to devise a proficiency test in a discipline in which no manufacturer supplies one.

7.1.3 Internal Testing

Where an outside source cannot be located or the supervisor deems necessary, a proficiency test will be generated in the laboratory by a qualified analyst in the particular discipline.

7.2 Types of errors and corrective action

Administrative Errors:
Minor errors detected under administrative review of the case file.

- Correct error and take appropriate action to help prevent reoccurrence

Systemic Errors:
Errors such as problems with procedures, equipment, and/or materials

- Review of procedures and instrumentation and take appropriate action to help prevent reoccurrence

Analytical/Interpretative Errors:
Minor errors are those due to a problem, which may affect the quality of work, but is not persistent or serious enough to cause immediate concern for the overall quality of the analyst/examiner's work.

Major errors are those that raise immediate concerns regarding the quality of the analyst/examiner's work.

If there is a discrepancy between the expected results and the experimental results the section chief must notify the quality manager. The section chief and the quality manager must begin an investigation and complete a 'Corrective Action Report'. This form will be maintained in the proficiency case file.

8.0 Court Testimony Review

A review of court testimony for each analyst will be conducted annually by the supervisor or his/her designee. Testimony review is covered in the Arkansas State Crime Laboratory Quality Manual (ASCL-DOC-01) section 10.

9.0 Case Records

9.1 Report Format

Crime Laboratory Letterhead
Details of Evidence Submission
Items Examined
Results of Analysis

9.2 Documentation

The Arkansas State Crime Laboratory Quality Manual (ASCL-DOC-01) section 9.1 covers case file documentation.

9.3 Technical and Administrative Review

All cases will be technically and administratively reviewed. The review process must confirm that electronic versions of all necessary documentation are in the imaging module of the LIMS-plus program.

If a reviewer discovers an error in the case record, the reviewer must document the error on the *Digital Evidence Case Review Form* (see DE-FORM-01) and inform the analyst. If the analyst and the reviewer can not reach consensus, then both the analyst and reviewer must meet with the Section Chief (or designee) for resolution.
All information on the laboratory case review form must be included on the individual sections' case review form. The Section Chief may add more fields if appropriate. Individual

requirements in the laboratory case review form may be removed, if appropriate, with the approval of the Quality Assurance Manager.

9.3.1 Technical Review

The technical review will include a thorough review of analyst bench notes to ensure that the documentation supports the results on the report.

The technical review does not shift the responsibility for the forensic findings to the reviewer, but the reviewer is responsible to ensure that the documentation does reflect adequate basis for the conclusion.

The technical review is to include but not necessarily limited to: bench notes, spectra, graphs, external telephone conversation records, investigative reports, sketches, diagrams and laboratory reports. The documentation must reflect adequate basis for the conclusion.

Routine (no identification or correlation) AFIS and NIBIN searches are not required to be contained in the case file.

9.3.2 Administrative Review

The administrative review of the case file will include review of spelling, grammar, case number, date, and initials on appropriate pages, description of evidence and seals and other appropriate documentation.

9.3.3 Types of Errors and Corrective Action

There are several types of errors, some of which are very minor and do not raise immediate concerns regarding the quality of the analyst/examiner's work product. Others do reflect the quality of the analyst/examiner's work.

Administrative Errors:
Minor errors detected under administrative review of the case file.

Systemic Errors:
Errors such as problems with procedures, equipment, and/or materials

Analytical/Interpretative Errors:
Minor errors are those due to a problem, which may affect the quality of work, but is not persistent or serious enough to cause immediate concern for the overall quality of the analyst/examiner's work.

Major errors are those that raise immediate concerns regarding the quality of the analyst/examiner's work.

If the technical reviewer discovers a problem that raises an immediate concern regarding the overall quality of the analyst/examiner's work, the technical reviewer must promptly notify the Section Chief. The Section Chief, Scientific Operations Director, and the Quality Assurance Manager must determine whether an investigation is warranted. If an investigation is undertaken, the Section Chief must complete a *Corrective Action Request Form* (see ASCL-FORM-08). This form will be maintained in the employee's personnel file.

10.0 Audits

An internal audit of the laboratory will be performed each year (except when an external audit is performed). The Quality Assurance Manager will schedule and coordinate the audit in each section of the laboratory. The audit is then reviewed by the Quality Assurance Manager, Scientific Operations Director and the Executive Director.

Findings will be issued to the appropriate Section Chief. Each Section Chief receiving a finding must either appeal the finding or complete a Corrective Action Report for each finding. These appeals or Corrective Action Reports, along with supporting documentation, must be returned to the Quality Assurance Manager by the assigned deadline. If necessary, the Scientific Operations Director and/or the Quality Assurance Manager will meet with the Section Chief to discuss the findings and their corrective actions.
Annual Accreditation Review Reports will be sent to ASCLD by each laboratory's accreditation anniversary each year by the Executive Director.

11.0 Complaints

Complaints will be handled in compliance with the Arkansas State Crime Laboratory Quality Manual.

12.0 Safety

The laboratory is committed to providing a safe working environment for its employees. The laboratory has a safety manual that must be followed by all employees and guests. Employees not following the safety guidelines as spelled out in the safety manual will be subject to disciplinary action. Guests will be asked to leave or conform to the safety regulations.