Summary

17025 is the standard for which forensic labs must be accredited in order to be considered legally defensible. In order to establish a new digital forensics lab that meets the requirements of ISO/IEC 17025, the following steps must be taken:

Physical Layout: A diagram of the physical layout of the lab should be created, including the evidence storage area for up to 20 cases, 2 analysis computers, and physical security measures such as key-card access, security cameras, and secure storage for evidence. The diagram should also include the location of other essential equipment, such as a printer and backup storage.

Equipment Inventory: A list of all the equipment needed to run the lab should be created, including both hardware and software. The list should include a minimum of 2 analysis computers, backup storage, a printer, and any specialized software required for forensic analysis. The list should also include any additional hardware or software required for accreditation.

Lab Accreditation Plan: A plan for accreditation should be created, including a timeline for achieving accreditation, a budget for the process, and a list of the accreditation bodies that the lab intends to apply to. The plan should also include a process for maintaining accreditation once it is achieved.

Lab Maintenance Plan: A maintenance plan for the lab should be created, including regular equipment maintenance, software upgrades, and regular testing to ensure that the lab remains in compliance with ISO/IEC 17025. The plan should also include a process for regularly reviewing and updating the lab's policies and procedures.

Staffing: A staffing plan should be created, including job descriptions for a lab manager and a technician. The lab manager should have a strong background in digital forensics and experience running a forensic lab, while the technician should have a strong technical background and experience in forensic analysis. The plan should also include a process for hiring and training additional staff as the lab grows.

Accreditation Plan

To begin an accreditation for a digital forensic lab for International Standard ISO/IEC 17025:2005 a lab must apply for “General Requirements for the Competence of Testing and Calibration Laboratories” and provide evidence of ownership of this document prior to applying for accreditation. This plan will use the ANB and ISO 17025:2005 standards for accreditation. The lab will be accredited by the American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB). Accreditation will

ensure that the lab meets established standards and guidelines for conducting digital forensics. The accreditation process will include regular assessments, periodic audits, and ongoing training for lab staff.

The following steps will be used to start the accreditation process:

For initial laboratories only, the following steps must be taken to start the accreditation process:

1. Complete the indicated sections of the site assessment checklist and submit the checklist along with other required documents to ANAB.
2. Contact the ANSI-ASQ National Accreditation Board (ANAB) website for information on accreditation fees and to request a quote.
3. Prepare the laboratory to meet the requirements of ISO/IEC 17025:2005, including:
    - Implementing a quality management system (QMS)
    - Providing evidence of ownership of the ISO/IEC 17025:2005 standard
    - Ensuring the lab has the necessary personnel, equipment, facilities, and processes to perform digital forensic examinations.
4. Submit a formal application for accreditation to ANAB, which will include a detailed assessment of the laboratory's QMS and the laboratory's ability to meet the requirements of ISO/IEC 17025:2005.
5. Prepare for an on-site assessment, during which the ANAB assessor will evaluate the laboratory's operations, processes, and procedures to ensure they meet the requirements of ISO/IEC 17025:2005.
6. Once the laboratory has been deemed to meet the requirements of ISO/IEC 17025:2005, ANAB will issue the laboratory with an accreditation certificate.
7. Maintain the accreditation status by demonstrating continuous compliance with the requirements of ISO/IEC 17025:2005 and participating in periodic reassessments.

Completion of indicated sections of the site assessment checklist and submission of the completed checklist to the ANAB. The site assessment checklist includes evaluation of the laboratory's physical location, infrastructure, and staff training. The laboratory must provide proof of ownership of ISO/IEC 17025:2005 and demonstrate that the laboratory has the necessary policies, procedures, and practices in place to meet the requirements of the standard. The laboratory must also provide evidence of its quality management system, including its policies and procedures, and demonstrate that the system is being implemented and followed consistently.

Once the laboratory has completed the site assessment checklist, it will be reviewed by the ANAB. If the laboratory meets the requirements, a site assessment will be scheduled. During the site assessment, the ANAB assessor will verify the information provided in the site assessment checklist, observe the laboratory's practices and procedures, and interview laboratory staff. The assessor will then provide a report to the ANAB, and the ANAB will decide on accreditation.

The laboratory must maintain its accreditation by regularly reviewing and updating its policies, procedures, and practices and by participating in periodic surveillance assessments by the ANAB. The laboratory must also maintain the necessary documentation, including test and calibration results, records of staff training, and quality management system records.

In conclusion, the accreditation process for a digital forensics' lab requires a commitment to meeting the requirements of ISO/IEC 17025:2005 and participation in the site assessment and periodic surveillance assessments by the ANAB. This process will help ensure the laboratory provides accurate and reliable results and maintains the highest level of competence and quality in its operations.

Contact the ANSI-ASQ National Accreditation Board (ANAB) website for information on accreditation fees at http://www.anab.org/lab-related-accreditation/request-for-quote

d) Forensic service providers who have already begun preparing for accreditation under the previously released accreditation requirements must continue to use the 2017 ANAB accreditation requirements, even if their accreditation process has not been completed. The laboratory must provide evidence of their commitment to quality by having a quality manual and a quality management system in place that meets the requirements of ISO/IEC 17025:2017. The quality manual should detail the laboratory's procedures and processes, including the control of documents, management of records, and management of nonconforming work. The laboratory must also have a quality management system that includes a system for continuous improvement and assessment of the laboratory's performance.

2. List of Approved Accreditation Organizations in the US:

1. The ANSI-ASQ National Accreditation Board (ANAB)
2. American Association for Laboratory Accreditation (A2LA)
3. The Forensic Quality Services (FQS)
4. The American Society of Crime Laboratory Directors/ Laboratory Accreditation Board (ASCLD/LAB)
5. The Accreditation Commission for Forensics Laboratories (ACFL)
6. The International Association of Forensic Sciences (IAFS)
7. The American Society of Crime Laboratory Directors (ASCLD)
8. The National Accreditation Board for Testing and Calibration Laboratories (NABL)
9. The Performance Review Institute (PRI)

These are some of the main organizations in the US that are approved for accreditation in digital forensics labs.

3. The laboratory must be familiar with and comply with all relevant ISO/IEC 17025:2005. The table below serves as a sample for the ISO checklist for an accreditation application. The necessary steps for accreditation are listed:

Policy Topic	Attachment Number	Submission Examples Required	ISO Reference	Initial	Reaccreditation	FoT Addition
ISO/IEC 17025	6A.1	Completion of the general information section which includes details such as the name of the laboratory, address, contact information, and scope of accreditation. Listing of the quality management system (QMS) policies and procedures used by the laboratory. Description of the laboratory's infrastructure including physical facilities, equipment, and storage for evidence. Proof of the laboratory's competence through staff training, experience, and qualification. Evidence of the laboratory's impartiality, confidentiality, and security policies. Evidence of the laboratory's ability to perform traceable calibrations and maintain the necessary records. Evidence of the laboratory's ability to follow established methods, procedures, and guidelines.	All			
Site Assessment Checklist	6A.2	Cover Letter: A cover letter introducing the laboratory, its purpose for seeking accreditation, and requesting for a site assessment. Application Form: A completed application form providing details of the laboratory such as name, location, and contact information. Proof of Ownership: A proof of ownership of the ISO/IEC 17025:2005 standard, either a physical copy or an electronic copy. Site Assessment Checklist Attachment 6A.2: A completed Site Assessment Checklist attachment number 6A.2 providing information on the laboratory's physical location, facilities, and available resources.	All			

		Technical Capabilities: Detailed information on the laboratory's technical capabilities and the scope of accreditation requested. Laboratory Quality Manual: A copy of the laboratory's quality manual, which outlines the laboratory's policies, procedures, and quality control measures. Staff Qualifications: Details on the laboratory staff, including their qualifications, training, and experience. Equipment List: A list of equipment used by the laboratory, including their make, model, and calibration status. Calibration and Maintenance Records: Records of calibrations and maintenance performed on equipment used by the laboratory. Previous Accreditation Records: If applicable, records of previous accreditation from other organizations, including any non-conformities or corrective actions taken. Additional Supporting Documents: Any additional documents or information that the laboratory wishes to provide in support of its accreditation application.				
Organization Chart	6A.3	The laboratory has a clear and effective structure in place that supports its work and enables it to meet the requirements of ISO/IEC 17025:2005. It should also show that personnel have been assigned specific roles and responsibilities and have the necessary authorities to perform their duties effectively.	ISO 4.1.5.e			
Document Control	6A.4	The laboratory must have a documented procedure in place that outlines the process of document control, including the creation, review, approval, distribution, and archiving of documents. This procedure must be reviewed and updated periodically to ensure its effectiveness.	ISO 4.3.1			
Document Control	6A.5	Identification of documents required by the quality management system and by ISO/IEC 17025:2005, including determination of the necessary frequency of review and revision. Documentation control process, including the review and approval of documents prior to issue and updating them when changes occur.	ISO 4.3.2.1			

		Ensuring that relevant documents are available at the points where they are needed. Ensuring the documents remain legible and readily identifiable. Ensuring that changes to documents are identified and that the current version is available at all locations where it is needed. Providing evidence of the implementation and maintenance of the document control process. Archiving of obsolete documents.				
Corrective Action	6A.6	Description of the nonconformity or deviation: This should include a clear and concise explanation of what went wrong and why it was deemed a nonconformity or deviation. Root cause analysis: An investigation should be conducted to determine the root cause of the nonconformity or deviation. This should include a clear and concise explanation of the underlying issue and why it occurred. Corrective action plan: A plan should be developed to address the nonconformity or deviation. This plan should include a description of the actions that will be taken to correct the issue, who will be responsible for implementing the actions, and a timeline for completion. Evidence of implementation: Documentation should be provided that demonstrates the corrective actions were implemented as planned. This could include photographs, process documentation, or other relevant materials. Results of the corrective action: The results of the corrective action should be documented, including any follow-up assessments to verify that the nonconformity or deviation has been effectively addressed.	ISO 4.9.1, 4.11.1, 2A.4.11.1			

Preventive Action	6A.7	Identification of non-conformances: All non-conformances identified during the internal audit or external assessment must be	ISO 4.12.2			

		documented and reported to the laboratory management. Analysis of non-conformances: The laboratory management must analyze the cause of the non-conformances and determine if it is a systematic issue that needs to be addressed. Implementation of preventive action: The laboratory management must develop a preventive action plan to address the root cause of the non-conformances and prevent it from happening again. Monitoring the effectiveness of preventive action: The laboratory management must monitor the effectiveness of the preventive action plan and take necessary actions to ensure its success. Documentation of preventive action: The preventive action plan, its implementation, and its effectiveness must be documented and maintained in the laboratory's quality manual.				
Internal Audit	6A.8	The internal audit team will review the procedures, records and other relevant documents to ensure that they comply with the requirements of ISO/IEC 17025:2005. The internal audit team will conduct a review of the laboratory's processes and practices to determine if they are in compliance with the requirements of ISO/IEC 17025:2005. The team will assess the effectiveness of the laboratory's quality management system by evaluating its implementation and maintenance. The internal audit team will observe and assess the laboratory's testing and calibration processes to determine their compliance with the requirements of ISO/IEC 17025:2005. The team will review the laboratory's corrective action and preventive action	ISO 4.14.3 2A.4.14.1			

		processes to determine their effectiveness and efficiency. The internal audit team will submit a report to the laboratory management that summarizes their findings, recommendations and observations. The laboratory management will review the internal audit report and take appropriate action to address any findings or recommendations. The laboratory will maintain a record of the internal audit and its results to demonstrate its commitment to continuous improvement and adherence to the requirements of ISO/IEC 17025:2005.				
Management Review	6A.9	Review of the lab's objectives: The management should assess the lab's objectives and how well they align with the organization's goals and mission. Assessment of the lab's performance: The management should evaluate the lab's performance, including its test results, customer feedback, and internal audits. Review of resources: The management should review the lab's resources, including equipment, personnel, and budget, to ensure they are sufficient to meet the lab's objectives. Discussion of any changes: The management should discuss any changes in the lab's environment, including changes in regulations, customer requirements, and advancements in technology, and determine how they will impact the lab's objectives. Identification of opportunities for improvement: Based on the review, the management should identify opportunities for improvement and determine what actions need to be taken to address them.	ISO 4.15.2			

		Final decision: The management should make a final decision on the lab's direction and priorities, and establish a plan of action to achieve its objectives.				
QA Reports	6A.10	A summary of the laboratory's performance over the past year, including data on internal audits, customer complaints, and other measures of quality. A description of any corrective or preventive actions taken by the laboratory in response to any issues identified through their internal quality control processes. A plan for continuous improvement, detailing the laboratory's goals for the coming year and the steps they will take to achieve those goals. Data on the laboratory's calibration and maintenance records, including information on the frequency and results of calibrations and any issues identified through routine checks.	2A.4.15.2			
Facilities	6A.11	Laboratory Floor Plan	2A.5.3			
Test Methods	6A.12	The scope of the method, including the purpose and the type of test or calibration being performed Equipment and materials required Procedure to be followed, including step-by-step instructions, calculations, and any relevant notes or comments Validation of the method, including any relevant data or results that demonstrate the validity of the method Any relevant quality control procedures that ensure the accuracy and reliability of the results	ISO 5.4.1			
Traceability	6A.13	This includes a system for tracking the chain of custody of evidence from the time it is collected to the time it is analyzed and reported on. This could include documentation of the person who collected the evidence, the date and time it was	ISO 5.6			

		collected, and any transfers of custody that take place during the analysis process. The lab would need to demonstrate that it has a robust and secure system for tracking this information, which is in line with the requirements of ISO 5.6. Additionally, the lab should be able to demonstrate the traceability of its measurement results, including the use of calibrated instruments and reference materials, as well as the accuracy and reliability of the data generated. This documentation would be a key part of the accreditation submission, and would be reviewed as part of the assessment process to ensure that the laboratory is meeting the requirements of ISO/IEC 17025:2005.				
Uncertainty of Measurement	6A.14	The lab will establish a measurement uncertainty budget for each test method used in the lab, following the guidance provided in ISO 5.10.3.1c. The lab will conduct periodic assessments of measurement performance to validate the accuracy and precision of the measurement results. The lab will maintain a log of all measurements taken in the lab, including the measurement uncertainty budget, and the results of periodic assessments of measurement performance. The lab will provide training to all personnel on the importance of accurate and precise measurement and on the proper techniques for conducting measurement. The lab will regularly review the measurement uncertainty budget to ensure that it remains up-to-date and accurate. The lab will provide a report to the accreditation body, demonstrating compliance with the ISO 5.4.6 requirement for uncertainty of measurement, including the measurement uncertainty budget, results of periodic assessments of measurement	ISO 5.4.6, 5.10.3.1c			

		performance, and the log of all measurements taken in the lab.				

Final Report	6A.15	Overview of the digital forensics lab: A brief description of the lab, including its purpose, size, location, and services offered. ISO/IEC 17025:2005 compliance: A statement confirming that the lab complies with all relevant ISO/IEC 17025:2005 requirements, including the assessment and evaluation of the lab's technical competence. Assessment findings: A summary of the results of the site assessment, including any areas of non-compliance and any recommended corrective actions. Quality management system: A description of the lab's quality management system, including the policies, procedures, and protocols in place to ensure consistent and reliable results. Staff training and development: A description of the training and development opportunities offered to staff, including any relevant certifications and qualifications. Equipment and facilities: A description of the lab's equipment and facilities, including any investments made to improve the lab's capabilities. Accreditation status: A statement confirming the lab's accreditation status, including any relevant accreditation numbers and the name of the accreditation body. Future plans: A description of the lab's future plans, including any planned expansions or upgrades, and any goals for the next three years.	2A.5.10			

		Appendices: Any additional documents, such as the site assessment checklist, the internal audit reports, or the management review reports, should be included as appendices.				
Proficiency Testing	6A.16	A description of the proficiency testing program used by the laboratory, including the type of tests performed and the frequency of participation. A summary of the laboratory's results from its most recent proficiency testing event, including the type of test performed, the date of the event, and the results obtained by the laboratory. Documentation of the laboratory's analysis and interpretation of its proficiency testing results, including any corrective actions taken as a result of low scores or other issues. A statement from the laboratory's management indicating its commitment to participation in proficiency testing and its understanding of the importance of proficiency testing in ensuring the quality of its work. Supporting documents, such as proficiency testing certificates or reports from the proficiency testing provider, to demonstrate the laboratory's participation in and results from proficiency testing.	Module 6			

Forensic Laboratory Floor Plan

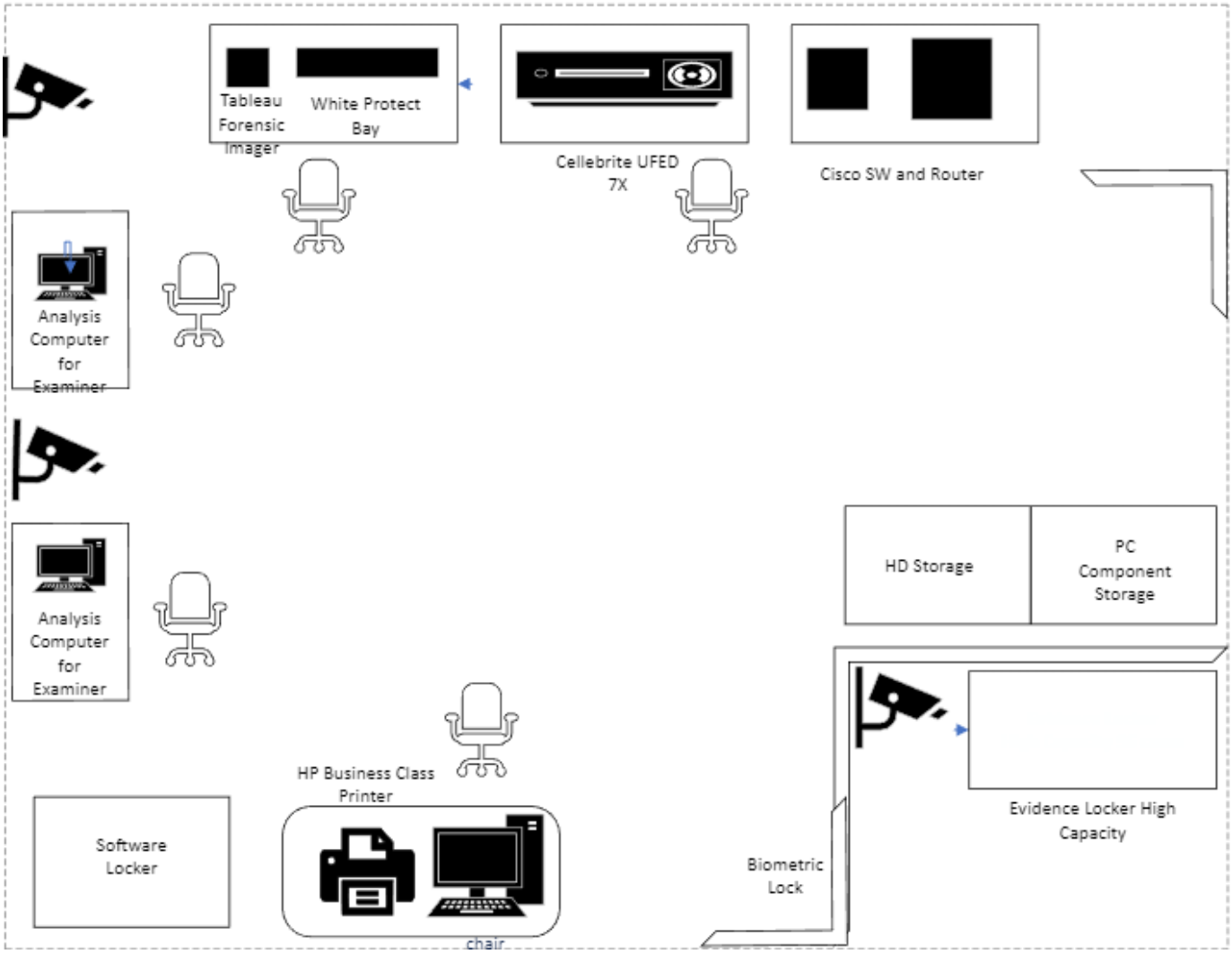
Tableau Forensic Imager
White Protect Bay
Cellebrite UFED 7X
Cisco SW and Router
Analysis Computer for Examiner
Analysis Computer for Examiner
HD Storage
PC Component Storage
HP Business Class Printer
Software Locker
Evidence Locker High Capacity
Biometric Lock
chair

Inventory

Hardware

Computer Chairs (5)

PC Power Cables

20 IDE Cables

20 SATA Cables

Secure Storage Room

Cisco 3560 Switch

20 CAT 6E cables

Fluke Network Cable Tester

Spectrum Analyzer

PC Components (Adapters, Cables, etc.)

Digital Forensic Workstations (2)

Hard Drive Duplicator (1)

Hard Drive Sanitizer (1)

Mobile Device Forensic Extraction Tool (1)

CD/DVD Drive (1)

External Hard Drive Enclosures (5)

Uninterruptible Power Supply (UPS) (1)

Fireproof and Waterproof Safe (1)

Security Cameras (3)

Access Control System (1)

Software

Kali Linux

Helix Pro

Forensic Analysis Software (EnCase, FTK)

Disk Imaging Software (DD, FTK Imager)

Mobile Device Analysis Software (Oxygen Forensic Suite, Cellebrite UFED)

Hash Verification Software (md5sum, HashVerifier)

File System Analysis Software (Autopsy, X-Ways Forensics)

Encryption and Decryption Software (VeraCrypt, AxCrypt)

Virtual Machine Software (VirtualBox, VMware Workstation)

Network Analysis Software (Wireshark, NetWitness Investigator)

Data Recovery Software (Recuva, R-Studio)

Maintenance Plan

1. Calibration Requirements: All hardware and software used in the lab must be calibrated on a regular basis to ensure accuracy and reliability. The frequency of calibration will depend on the specific equipment and usage patterns. It is recommended to calibrate all equipment at least once a year.
2. Maintenance Requirements: Regular maintenance is essential for ensuring that all hardware and software are functioning correctly and efficiently. Maintenance activities should be performed at least once a year and should include:

    - Updating firmware and software
    - Cleaning equipment (e.g. dusting, wiping down surfaces)
    - Replacing consumable items (e.g. batteries, air filters)
    - Checking and replacing worn or damaged parts
    - Testing and verifying that all equipment is functioning properly

3. Documentation: It is important to keep a detailed record of all maintenance activities, including the date, equipment, and any issues or repairs made. This documentation can be used to track trends, identify potential problems early on, and support any future legal proceedings.

4. Quality Control: The lab should have a quality control process in place to verify the accuracy and reliability of all equipment used in the analysis process. This process should include regular checks of the equipment against known data, as well as conducting tests and comparisons with other equipment.

5. Training: Regular training should be provided to all lab staff to ensure that they are aware of the maintenance requirements, procedures, and best practices for the lab.

6. Emergency Preparedness: A plan should be in place for responding to emergencies or unexpected equipment failures. This plan should include backup equipment, procedures for preserving evidence, and communication protocols with relevant stakeholders.

By implementing these practices, the lab can ensure the accuracy and reliability of the equipment and the integrity of the data being analyzed.

Definitions

The following terms shall have the designated meanings:

DFS: Department of Forensic Sciences - Refers to the department within the police organization that is responsible for conducting digital forensics investigations.

DOM: Department of Mathematics - Refers to the department within the police organization that is responsible for providing mathematical support for the DFS.

EVID: Evidence - Refers to any physical or digital artifact that is collected as part of a digital forensics investigation.

EVID-STOR: Evidence Storage - Refers to the secure storage area designated for storing digital evidence collected during investigations.

DF-LAB: Digital Forensics Lab - Refers to the laboratory facility within the DFS that is dedicated to conducting digital forensics investigations.

DF-ANALYSIS: Digital Forensics Analysis - Refers to the process of conducting digital forensics investigations, including the examination and analysis of digital evidence.

DF-TECH: Digital Forensics Technician - Refers to the individual who is responsible for conducting digital forensics investigations.

DF-EQUIP: Digital Forensics Equipment - Refers to the hardware and software used by the DFS for conducting digital forensics investigations.

DF-PROC: Digital Forensics Procedures - Refers to the established protocols and guidelines that the DFS follows for conducting digital forensics investigations.

SEC-MEAS: Security Measures - Refers to the physical and digital security measures implemented to protect the DF-LAB and the digital evidence stored within.

Scope

These practices apply to casework units of the FSL with instrumentation and equipment that have an effect on the validity of forensic examinations.

Roles/Responsibilities

Laboratory Manager:

- Oversee the day-to-day operations of the DF-LAB
- Ensure that the DF-LAB is in compliance with all relevant regulations and standards
- Develop and implement policies and procedures related to digital forensics investigations
- Manage the DF-TECHs and provide training and support as needed
- Ensure the proper maintenance of DF-EQUIP
- Act as the primary point of contact between the DFS and other departments within the police organization

Quality Assurance Liaison:

- Oversee the quality control processes within the DF-LAB

- Develop and implement quality assurance protocols for digital forensics investigations
- Ensure that all DF-TECHs are following established DF-PROC
- Monitor and report on the performance of DF-EQUIP
- Act as the primary point of contact between the DFS and external accreditation organizations

Digital Forensics Technician:

- Conduct digital forensics investigations in accordance with established DF-PROC
- Collect and analyze digital evidence
- Prepare reports and provide expert testimony in court as needed
- Maintain and update DF-EQUIP as required
- Participate in continuing education and training to stay up-to-date with the latest advancements in digital forensics

Evidence Storage Manager:

- Manage the secure storage of digital evidence (EVID-STOR)
- Ensure that all digital evidence is stored in accordance with established protocols
- Conduct periodic audits of the EVID-STOR to ensure the security and integrity of digital evidence
- Maintain accurate records of all digital evidence stored within the EVID-STOR
- Act as the primary point of contact between the DFS and other departments for accessing stored digital evidence.

Maintenance Practices

Calibration of Equipment:

- The Laboratory Manager, Quality Assurance Liaison, or designee will ensure that all DF-EQUIP is calibrated on a regular basis in accordance with the manufacturer's specifications.
- A record of all calibrations will be maintained and include the date, equipment type and identifier, and the results of the calibration.
- Any discrepancies found during calibration will be documented and addressed immediately.

Software Maintenance:

- The Laboratory Manager, Quality Assurance Liaison, or designee will ensure that all DF-EQUIP software is kept up-to-date and patched as needed.
- A record of all software installations, updates, and patches will be maintained.
- Any issues with software will be reported immediately to the Laboratory Manager, Quality Assurance Liaison, or designee.

Equipment Cleaning:

- All DF-EQUIP will be cleaned on a regular basis in accordance with the manufacturer's specifications.
- A record of all cleanings will be maintained and include the date, equipment type and identifier, and a description of the cleaning performed.

Preventive Maintenance:

- The Laboratory Manager, Quality Assurance Liaison, or designee will ensure that all DF-EQUIP is subjected to preventive maintenance on a regular basis in accordance with the manufacturer's specifications.
- A record of all preventive maintenance will be maintained and include the date, equipment type and identifier, and a description of the preventive maintenance performed.

Equipment Replacements:

- The Laboratory Manager, Quality Assurance Liaison, or designee will ensure that any DF-EQUIP that is beyond repair or no longer serviceable is replaced in a timely manner.
- A record of all equipment replacements will be maintained and include the date, equipment type and identifier, and a description of the replacement.

Calibration Procedures

Instruments and/or equipment requiring calibration will have documented procedures for performing calibrations.

Calibration procedures will include, at a minimum, the following:

1. Schedule and frequency of calibration, which will be based on manufacturer's recommendations, industry standards, and the level of precision required for the specific instrument or equipment.
2. Procedure for performing the calibration, which will be followed in accordance with the manufacturer's instructions and industry standards.
3. Documentation of calibration results, including date of calibration, who performed the calibration, and results of any tests performed during the calibration.
4. Equipment that is found to be out of calibration will be immediately removed from service and repaired or replaced as needed.
5. Regular review and revision of calibration procedures will be performed to ensure that they remain current and effective in maintaining the accuracy and reliability of the instruments and equipment.

The Laboratory Manager, Quality Assurance Liaison, or designee will be responsible for overseeing the calibration process and ensuring that all procedures are followed in a consistent and effective manner. This will include regular monitoring of the calibration records and taking corrective action as necessary.

Reference Standards, Certified Reference Materials and Reference Materials

Where practicable, reference standard traceable to SI units (International System of Units) or certified reference materials will be used to perform calibrations and verify the accuracy of instruments and equipment.

Reference standards, certified reference materials, and reference materials will be:

1. Kept in a secure location and protected from damage or contamination.
2. Regularly checked for accuracy and stability and replaced as necessary.
3. Documented, including information on the source, date of purchase, date of last verification, and any other relevant information.
4. Used in accordance with the manufacturer's instructions and industry standards.
5. Properly stored and maintained to ensure their continued accuracy and stability.

The Laboratory Manager, Quality Assurance Liaison, or designee will be responsible for ensuring that reference standards, certified reference materials, and reference materials are used and maintained in accordance with these procedures. This will include regular monitoring of their accuracy and stability and taking corrective action as necessary.

Calibration Interval

The calibration interval will be documented for each instrument requiring calibration. Manufacturers' operating instructions or industry standards will be used to determine the appropriate calibration interval. In general, the calibration interval will be based on the stability and accuracy of the instrument and the frequency of use. For instruments used in critical applications or for which stability is an issue, the calibration interval may be shorter. For instruments that are used infrequently, the calibration interval may be longer. The Laboratory Manager, Quality Assurance Liaison, or designee will be responsible for ensuring that instruments and equipment are calibrated at the appropriate intervals. This will include scheduling calibrations in advance, documenting the results of calibrations, and taking corrective action as necessary.

Maintenance

Instruments and equipment will be properly maintained. The Laboratory Manager or designee will ensure that a preventive maintenance plan is established and followed for each instrument and equipment in the lab. This plan will include:

- Cleaning of equipment and instruments as needed.
- Periodic inspection and testing of equipment to ensure it is in good working order.
- Updating of software and firmware as needed.
- Replacing of worn or damaged parts.
- Verifying the accuracy and performance of instruments after maintenance is performed.
- Designating a trained and qualified technician to perform the preventive maintenance activities.

- Ensuring that all maintenance activities are performed in a manner that does not compromise the integrity of the evidence.
- Having backup equipment and instruments available in the event that a primary piece of equipment is undergoing maintenance.
- Keeping a log of all maintenance activities, including the date of the activity, the technician who performed it, and a description of the work performed.
- Keeping all maintenance records and logs secure and protected to ensure their confidentiality and integrity.
- Regularly reviewing the preventive maintenance plan and updating it as needed to ensure that it continues to meet the needs of the lab.
- Conducting regular performance assessments of all equipment and instruments to ensure that they are functioning correctly and accurately.
- Keeping up-to-date with the latest maintenance practices and technology in the field of digital forensics to ensure that the lab is operating at its best.

The Laboratory Manager, Quality Assurance Liaison, or designee will ensure that the preventive maintenance plan is documented and that maintenance activities are recorded in the instrument and equipment log. Any deviations from the preventive maintenance plan will also be documented and investigated.

Preventive Maintenance

Preventive maintenance will be performed according to a regular, predetermined schedule, based on the manufacturer's recommendations and industry standards. The preventive maintenance schedule will include tasks such as cleaning, checking software and hardware updates, and inspection of physical components for signs of wear or damage. The Laboratory Manager or designee will ensure that all preventive maintenance tasks are documented, including the date of completion, the person who performed the maintenance, and any issues or recommendations noted during the maintenance process.

Instruments and equipment will also be periodically inspected to ensure they are functioning properly, and any necessary repairs or replacements will be made in a timely manner. The Laboratory Manager or designee will ensure that all repair or replacement activities are documented, including the date of completion, the person who performed the maintenance, and the nature of the repair or replacement.

To ensure that the lab is able to function properly, the Laboratory Manager or designee will establish a preventive maintenance program that includes regular check-ups, replacement of worn or broken components, and updates to hardware and software. The program will be reviewed regularly to ensure that it is working effectively and that it meets the needs of the lab.

Corrective Maintenance

When an instrument cannot be properly calibrated, fails to meet the performance characteristics established for the Corrective Maintenance procedures will be implemented in the event of an instrument or equipment failure. The Laboratory Manager or designee will ensure that the necessary steps are taken to identify the cause of the failure and to repair the instrument or equipment in accordance with the manufacturer's specifications. This may include troubleshooting and repair procedures, replacement of parts, and/or replacement of the entire instrument. A written record of the corrective maintenance performed, including the date, nature of the problem, and the solution, will be maintained and kept on file in the lab. Additionally, any instrument or equipment that has been subject to corrective maintenance will be re-evaluated and tested to verify that it meets its original performance specifications before being returned to service.

Performance Checks

In instances where calibration is not required or appropriate, performance checks should be carried out at regular intervals to ensure that the instruments and equipment continue to meet established performance characteristics. The Laboratory Manager or designee will ensure that performance checks are performed and documented. The frequency of these checks will be determined by the type of instrument, its use, and the results of previous performance checks. The results of these performance checks will be recorded and analyzed to identify any trends or potential issues that may require further investigation or corrective action. If the results of a performance check indicate that an instrument or equipment has failed to meet established performance standards, corrective action will be taken to address the issue.

Malfunctioning Equipment

Equipment that has been subjected to overloading or mishandling, gives suspect results, or has been shown to be malfunctioning in any way must be immediately removed from service and repaired or replaced as necessary. The Laboratory Manager, Quality Assurance Liaison, or designee will ensure that the equipment is either repaired or replaced, and then tested and verified for proper performance before being placed back into service. A record of all maintenance, repairs, and replacement activities will be kept and made readily available for inspection and review.

Equipment Security

Test and calibration equipment, including both hardware and software, shall be safeguarded from adjustments, damage, theft, or unauthorized use. Physical security measures such as locks, security cameras, and alarm systems will be implemented to protect the equipment. Additionally, all software and hardware will be regularly backed up and stored in secure locations. Access to the equipment and laboratory will be restricted to authorized personnel only and monitored using a secure login system. The laboratory manager or designee will regularly conduct security audits to ensure that all security protocols are being followed.

Bibliography

American Academy of Forensic Sciences. (2018). Digital Evidence in Criminal Investigations. Journal of Forensic Sciences, 63(6), 1532-1540.

Digital Forensics Research Workshop. (2019). Best Practices in Digital Forensics. Springer International Publishing.

International Association of Computer Security Professionals. (2021). Guidelines for Digital Forensics Investigations. IACSP Press.

National Institute of Standards and Technology. (2017). Computer Forensic Tool Testing (CFTT) Project. NIST Special Publication, 1800-20.

National White Collar Crime Center. (2019). Digital Forensics for Criminal Investigations. NW3C Research Report, RR-19-03.

Oster, M. (2020). The Digital Forensics Handbook. CRC Press.

Palma, R., & Acosta, A. (2022). Computer Forensics: Techniques, Tools and Issues. Springer International Publishing.