Midterm - Police Digital (Computer) Forensic Lab Accreditation

Helen Bramow, MA

Cybersecurity Department, Old Dominion University

CYSE 407: Digital Forensics

Prof. Bryan Bechard

April 21, 2024

Midterm - Police Digital (Computer) Forensic Lab Accreditation

Introduction/Background

This lab is for supporting a medium size police department and must be accredited. ANAB/ANSI is the National Accreditation Board for forensics labs. It is only for digital forensics investigation to investigate crimes. The International Organization of Standards ISO/IEC 17025:20017 Forensic Accreditation is the most current international regulation for labs with testing and calibration; it is the ISO main standard for digital forensics labs. It is from the American National Standards Institute's National Accreditation Board (ANAB) and this is the 2017 update, as the prior one was from 2005. ("ISO/IEC 17025:2017")

Accreditation/certification is necessary to prove accuracy and further provides assurance of the work because this is an industry standard, and it is not only national, but it is an international standard. As per this reference, this particular certification standard is for all labs, not just digital forensic labs (DFLs). Therefore, there are some additional and necessary standards for DFLs, like: the analysts must be proficient, and chain of custody. (S. Taylor, 2021, p. 1)

Accreditation/Certification Requirements

Under this accreditation there are five general requirements as follows:

- **General –** includes confidentiality and impartiality.
- **Structural –** both organizational and lab responsibilities, lab legality.
- **Resource –** equipment, lab environment, contractors and personnel.
- **Process –** stakeholders, reporting results, methods, exhibits, complaints, data control and nonconforming works. 17025 standards assure the accuracy of digital forensics work.
- **Management System –** internal audits, risk management, corrective actions and management review. (S. Taylor, 2021, p. 2)

DFL Requirements (Taylor added)

Supplemental requirements of DFL, in addition to those above-mentioned 5 general requirements were listed above in the previous paragraph. It is necessary to show both:

- a chain of custody and
- the proficiency of analysts in DFL. (S. Taylor, 2021)

Accreditation Plan

To become an accredited police digital forensic lab and to meet ANAB ISO/IEC 17025:2017 standards, first an application for lab calibration and testing must be filed. ISO 17025:2017 is also used as the guide for lab setup so that it can pass accreditation that verifies that the lab produces quality work in the nature of digital media forensics. (See available Guide below.) Both the lab procedures and policies and the calibration of equipment must be able to product quality results regarding the evidence. The application is at the end of this document, form FA 3068 - Forensic Service Provide Accreditation for Accreditation. A request for a quote will need to be done also. After application, ANAB will schedule an on-site visit to ensure compliance. Accreditation requires that the lab has a management system documenting all policies, procedures and objectives. (Alcock, 2018) The responsibility for this will be the lab manager as stated below. Accreditation also assists with analysts in court being questioned because they are more confident and there are less errors. (S. Taylor, 2021)

The steps for review are as follows:

- request a quote; Request a Quote
- application;
- review documents;
- assess accreditation;
- action to correct (corrective action), then another visit (follow-up);
- decision is made on accreditation; and
- after surveillance, then reassessment is done. Steps for Accreditation

ANAB ISO - resourses - to download: the accreditation manual, MA 3033 and FA 3068.
Guide ISO 17025-2017 - testing and calibration is outlined on p. 22.

Methodology - 8 Phases

There are 8 phases to accreditation to be successful. "Practical Guidance for Digital Forensic Laboratory Accreditation - A Case Study" (S. Taylor, 2021)

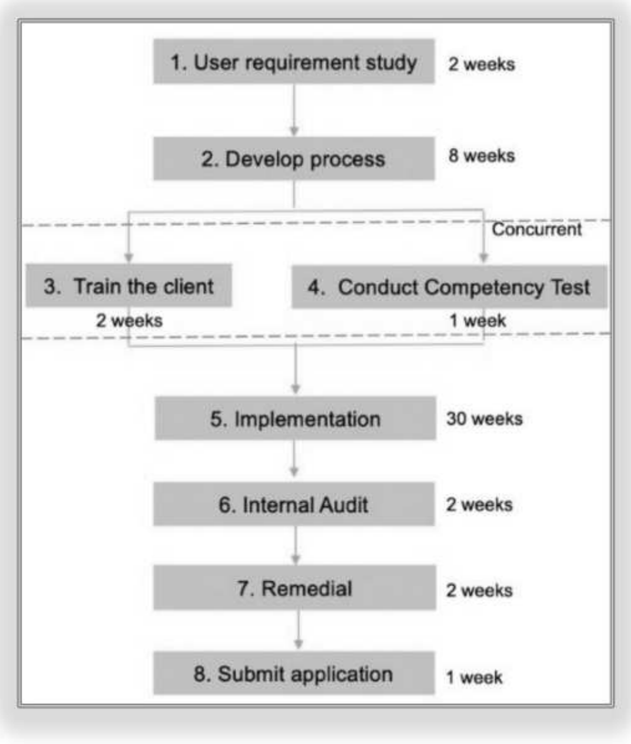


Figure 1 - https://www.oic-cert.org/en/journal/pdf/3/1/B5%201-6%20%20Paper%201%20Practical%20Guideline%20for%20Digital%20Forensics%20Laboratory%20Accreditation%20(with%20author).pdf

Methodology (Cont'd.) - Guideline - 8 Phases to Accreditation (2 months - 3 years)

1. **Conduct user requirement study**. This phase is aimed at the gaps between current lab procedures and the ISO requirements. This phase should take about 2 weeks.
2. **Develop written forensic process**. Analysts give input on writing: manuals, forms, technical procedures, and policies. The goal is to create a 'short process flow' using analysts' input. This phase should take about 8 weeks.
3. **Analysts training session**. This phase should take 2 weeks. (Conducted during the Competency Test.)
4. **Competency Test** (Supplemental). After this phase is analyst will be assigned cases. This phase should take about 1 week.
5. **Implementation of the process**. The analyst alone must implement the forensic plan. There must be records kept for the Accreditation Body assessment. This phase should take about 30 weeks.
6. **Internal audit with 3 auditors**. This audit ensures that ISO procedures are being followed. This phase should take 1 week, but together with the report it takes about 3 weeks.
7. **Remedial phase**. This phase is dependent on the above phase #6, the internal audit findings. The auditing issues must be resolved. This phase takes about 2 weeks.
8. **Application submitted**. The internal audit report and the written process must both be submitted along with the form. Afterwards then ANAB will send over 2 auditors to observe implementation. * It is this author's opinion on this study, S. Taylor, that accreditation can be secured in about 2 months with the correct coaching. (S. Taylor, 2021)

This study took only 2 months; however, it could take longer up to 3 years. According to S. Taylor, ISO training is available and it is recommended especially for management levels. Secondly, it was noted that there must be actual cases to work on. Also, there needs to be a schedule and a plan, and it needs to be followed. (S. Taylor, 2021)

Calibration Plan

Calibration on all equipment must be done to ensure it is working properly at all times, and produces accurate results for the submitted evidence in digital forensics. The lab manager, under the scope of 'quality review' will outline the policy and procedure for calibration; track all logs on calibration and verify when equipment is calibrated, and when it needs to then be recalibrated. The manager will also keep track of all the vendors used for repair when necessary, as well as the calibration and repair logs. The log will detail the specifics of all equipment, as well as the origination date, any repair dates, and estimated replacement dates. (B. Nelson, 2019) The manager is also responsible for the documentation of: any errors and failures, as well as the above-mentioned events, ensuring lab management has an effective management and reporting system to ensure accuracy. (Alcock, 2018)

ISO 17025:2017 is international meaning that labs everywhere hold this accreditation. That is important because they also will share agreements with other lab accreditation bodies internationally as well. That means the scope of it is global, and the results are accurate and trusted worldwide then. There are 'key elements' that are considered satisfied by this accreditation and they are same with other accreditation labs under other accreditation bodies. Those 'key elements' are things like: identifying the unique calibration, the results, the date, and any specifics about the device. "Measurements are essential for regulatory compliance and product integrity." (Hatchard, 2024) As stated above, the lab manager is responsible for tracking the key elements that ensure lab accuracy. Also, this same work is done around the world everywhere and labs here in the U.S. sometimes work with labs outside the country on cases.

Lab Specifics

•	Lab Accreditation Plan	3 years
•	Lab Maintenance Plan	Weekly, and then yearly
•	Evidence Storage	20 cases
•	Analysis Computers	4
•	Equipment: Software & Hardware min.	20
	Job Descriptions	
	Manager	
	Lab Technician	
•	Sensitive Materials Handling Company (B. Nelson, 2019, p. 75)	
•		
	Manager	
	Lab Technician	

Inventory

Forensic Tools – Hardware

Secure Storage Room	
Evidence Kits	
1st Time on Scene	
Labels, Gloves	
Bags & Faraday Bags	
Trash cans	4 - 2 square, 2 round (classified materials)
2 regular trash square	
2 sensitive materials (B. Nelson, 2019, p. 75)	
Lab Coats	4
Protective Glasses	4
Voltage Meter	2
Digital Camera	2
USB adapters and drives	5
hard drives, assorted	
antistatic strap	5
IDE cables, USB cables,	5 each
SATA cards and cables (B. Nelson, 2019, p. 81)	
ID creator for security badges	
Anti-static pad	10
Computers -	
Evidence Storage	1

Analysis	
Monitors	6
Keyboards	6
Printer/Scanner	1
Document Shredder	1
Table	2 - 1 in evidence room, 1 main room
Chairs	2 - 2 in evidence room
Workstation/Desks	5
Chairs	7 - main room
Bookshelves	3 - 1 in evidence room, 2 main room
Workstations - 1 each	4
Conference Area	2
Projector	1
Security System -	
Cameras outside CCTV	4 - both outer doors, parking lot, behind building
Cameras inside CCTV	5 - entry door, other door, evidence door, inside evidence room, hallway/main work area
Secured Door Locks -	3
Evidence Storage	
Front Door	
Other Door	
Wireless Monitor	2
No Windows in Lab	

Tools for Mobile devices and other devices -

1. pliers,
2. tweezers,
3. flashlight
4. screwdriver set, and
5. tool to remove SIM card.

Software -
Maintain minimum of 2 licenses for each software package.

Software - Operating Systems (OS) –

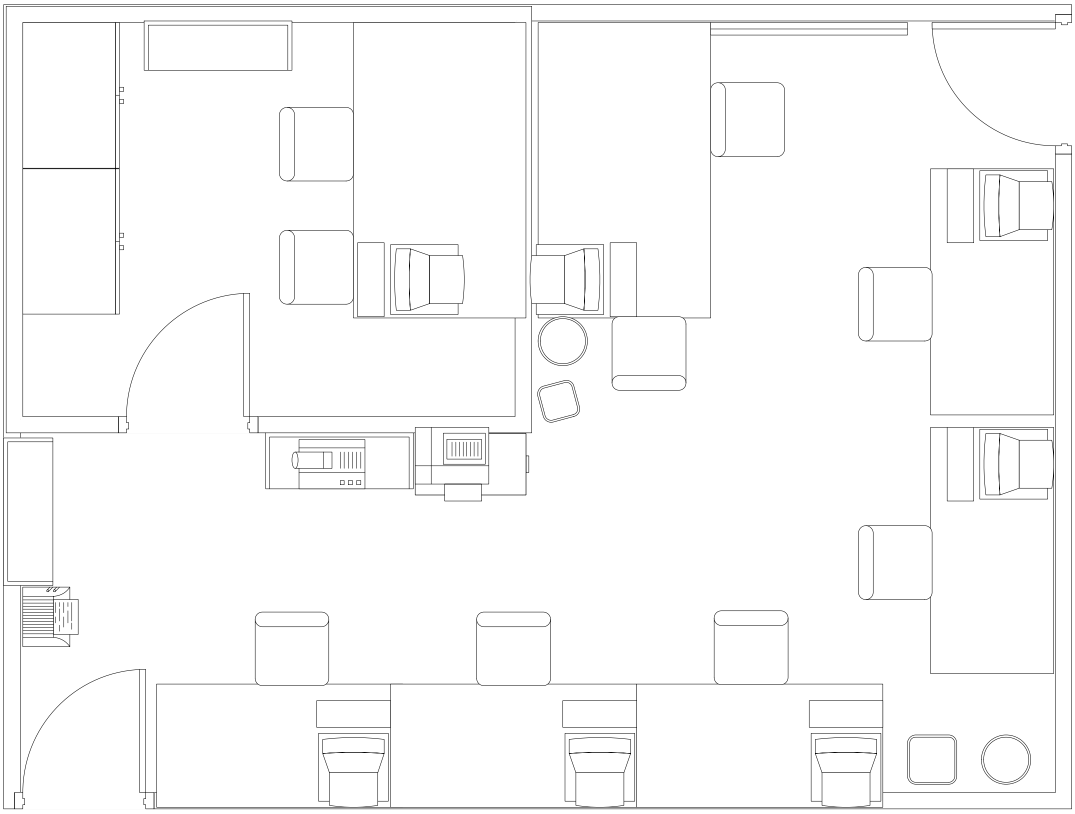
Windows
Linux
Apple MAC
Legacy OS, many different copies w/ licenses (B. Nelson, 2019, pp. 80 - 81)

Software - Forensic Tools –

6. Autopsy – The Sleuth Kit
7. ProDiscover
8. Dream Screens USB SIM Card Reader - Multi-Media SD, w/SIM editing, Adapters (Micro, Nano, and SIM) and Text Recovery Software
9. FTK Imager

10. Volatility – RAM memory
11. Registry Recon – Windows OS registry
12. Wireshark
13. Caine – Linux (Poston, "7 best computer forensics tools", 2021) (free)
14. Xray Forensics – Windows, can run off a USB
15. EnCase
16. Mandiant Redline
17. Bulk Extractor – Linux, MAC, Windows (Poston, "Computer forensics tools.", 2021)
18. X-ways
19. Magnet Axiom
20. SANS Sift Workstation (free) - Ubuntu Linux tools; incident response; CLI; supports Linux and Windows
21. Velociraptor (free) - incident reporting (Scruthy, 2024)
22. Write Blocker
23. accounting - Quickbooks, or Peachtree

Lab Diagram – (Visio)



Security

Surveillance Cameras

- Cameras - CCTV, digital cameras record 24/7 -
  - inside (5) and outside (4) the facility; and
  - including inside evidence storage room.
- Intruder alerts are sent directly to the police station.
- Fire alert is sent to both the police station and the fire station.
- Far Infared and night vision, audio recording

Surveillance cameras recordings are kept on the server and backed up daily.

Wireless Security Monitors

Three monitors: front door; evidence storage room; and the other door. Wireless monitors allow wireless, keyless entry with a code and/or key card. Both the Technician and Lab Manager have key cards and code.

Secure Storage Room for Evidence

Small, locked room with secure (locked) cabinet and/or secured (locked) file cabinet inside. Outside is a security monitor with a password to unlock only available to technicians and lab manager. All visitors must log in with the: date and time in/out recorded as per every entry. Passwords are changed every 6 months unless an employee leaves or there is a new hire. However, the whole lab must be secure similar to an evidence locker, to work in. (B. Nelson, 2019)

Visitors

Anyone who is not an employee of the lab is a visitor and all visitors must be escorted and logged in. Visitor logs are to be kept up-to-date. Cleaning crews, repairmen, or anyone visiting for any reason is a visitor. They should each be given a visitor badge also. (B. Nelson, 2019, p. 76)

Maintenance Plan

Disaster and Recovery Plan

Backup all workstations weekly so they can be restored in the event of a loss. They should be accessible and a copy should be safely stored in another location. Then, any lab configuration changes must also be recorded. This included any updating of software. (B. Nelson, 2019, pp. 81 - 82) Policies and procedures must document the disaster and recovery plan and be kept updated so in the event there is an issue the procedure will work to restore all systems without data loss or evidence loss/compromise. The lab manager is responsible for the policies and procedures and for updating them. (B. Nelson, 2019, p. 65)

Cleaning

Cleaning Service nightly weekly includes vacuuming, remove trash and dust. Cleaning crew must be escorted around the facility. Dust contributes to static electricity so cleaning is essential to the lab consistency and accuracy. (B. Nelson, 2019, p. 75) Annual maintenance must also be done. (B. Nelson, 2019, p. 87)

Equipment Checks

Equipment checks are carried out by the Forensic Examiners - the hardware and software must be checked and continually monitored to ensure they are working properly. Any repairs will be completed as soon as possible. (B. Nelson, 2019, p. 88) Examiners will report to the lab management any discrepancies immediately, so that faulty equipment can be either repaired or replaced.

Risk Management and Audits

Upgrading any equipment is part of both risk management and audits that are done monthly. Most equipment may only last about 18 months up to 3 years and will need replaced. There should be a schedule every 12 months which equipment needs replaced and lists the exact components of it. (B. Nelson, 2019, p. 82) Replacement value can then be estimated also. Risk management internal audits are required, added to 17025 in the Nov. 2017 update. Risks must be assessed to mitigate any issues, as far as damages and costs in litigation. Confidentiality requirements are part of risk management. Personnel training and competence are also part of risk management to mitigate any liability or damages. (Alcock, 2018)

In-house Audits

Audits should be done routinely to ensure policies and procedures are being followed and if they need updated also. Both the evidence storage lockers section and the lab area must be audited. At least 1 time every month the lab, the ceilings, floors, etc. need to be audited, as well as the doors, whether they shut right or not. There could be something new that went unnoticed. Locks need to be inspected, ensure logs are being used for visitors and evidence lockers are closed still. If there is evidence still in process when the day's over needs to be returned to the evidence storage locker. (B. Nelson, 2019, p. 77) Make sure there is an evidence log and it is up-to-date, meaning any time it is opened it needs to be logged. (B. Nelson, 2019, p. 75)

Job Descriptions - Lab Management and Examiner

Lab Manager -

The lab manager has certain general responsibilities -

- sets up policies/procedures for the lab to manage cases;
- sets up policy for maintenance and calibration of equipment;
- assists in group decision making process;
- takes on financial responsibilities for the lab;
- ensure ethical standard of staff;
- plans for the software and hardware updates necessary;
- promotes quality in lab processes;
- designs outline for: steps to follow once case arrives; how to log in evidence; visitor guidelines; and report filing.
- production schedules

- manages the examiner's case loads, determines how many they can handle and when reports are filed; and
- monitors policies to ensure safety. (B. Nelson, 2019, p. 65)

Digital Forensics Lab Lead Engineer - Digital Forensics Lab Lead Engineer - Indeed.com - Washington D.C. [from an actual job posting -- hybrid, full-time work]

Job Description - Maintain, build and operate a forensic network (digital and standalone unit) that supports the nation. Responsible for moderizing: network, computers, software and servers. Work as a team in monitoring resources and ensure that architecture and software is compatible.

Qualifications - BS in: cybersecurity, IT or digital forensics. 5 years experience in analysis of digital forensics with lead roles. Experience with: Windows OS, configure backups, CISCO networks, Nuix Investigate, Graykey, Penlink, Passware, Magnet Axiom, Cellebrite and ADF Triange. Candidate also needs to have experience at: refreshing system lifecycle, documenting system design and developing standard operating procedures.

Technician (Examiner/Analyst) -

Examiners/analysts should have at least 2 years experience in their field as well as specific training and certification specific to digital forensics. They should have some IT certifications, minimum CompTIA A+, but also CompTIA Security and CompTIA Networking also. A BS in CS or Digital Forensics is also required. They will need to continue their education every year. Training standards and competence are essential parts of accreditation for staff. (Alcock, 2018)

Digital Forensics Analyst I Job Posting - Digital Forensic Analyst I - Indeed.com CGS, LLC Houston TX [from an actual job posting -- hybrid, full-time work]

Job Description - Applicant must be willing to travel for on-site work, but work in the forensics lab usually. Motivated, team centered, works well with others, have fluent experience and knowledge in forensics. Be willing to work in a fast paced environment with tight deadlines, and under pressure. Assist in redefining processes and procedures for the lab office. Know the evidence rules, follow the 'chain of custody' and produce quality work. Other IT functions may also be part of the job.

Qualifications - BS degree in: CS/Engineering and/or Digital Forensics. 1.5 years forensics experience, including: acquisition of evidence on different devices, and able to complete advanced forensic analysis (intermediate level). Candidate should have experience with the following forensic tools: Encase, FTK Imager, Oxygen, X1 Social Discovery, Mac Quisition, Cellebrite and Logicube Falcon.

Skills - Candidate should understand: encryption, and file systems for Windows and/or MACs and mobile devices. Should also have some experience in preservation of evidence on various devices: laptops, mobile phones, servers, Cloud, and social media and be able to do it in a manner that is most appropriate for forensic work. Candidate should possess effective communication, tactful both in verbal and in written format. Detail oriented, good organization skills, ability/willingness to work extra hours, possess valid passport, willing to travel on short notice. Candidate should have the ability to document work according to industry standards. Train other employees when necessary. Possess good troubleshooting tactics, and solve problems (complex) very quickly.

Technical Skills - understand/know/possess the following:

- EDRM - electronic discovery reference model;
- 1 industry standard like: CCE, EnCe, GCFE, CCO, CCPA, CCME and/or CCFE.;
- support applications for litigation: Nuix, LAW PreDiscovery, Concordance, and or Relativity;
- data manipulation/scripting from different platforms using exported structured data, in creating client reports;
- scripting in BAT (PowerShell), Active Directory (Windows) and copy tools like Robo/Rich; and
- have experience with: coding and/or programming, database (Access, SQL, HTML,VB) languages.

Lab Floor Plan

- Workstations
- Working space around workstations - 10 x 15, about 150 square feet of space.
- Exits - 2. (B. Nelson, 2019, p. 78)

References

"ISO/IEC 17025:2017". (n.d.). Retrieved Apr. 5, 2024, from https://www.iso.org/: https://www.iso.org/standard/66912.html

Alcock, T. (2018, Apr. 20). *"Changes to Forensic Laboratory Accreditation Requirements ISO IEC 17025."*. Retrieved Apr. 14, 2024, from https://www.forensicfocus.com/: https://www.forensicfocus.com/legal/changes-to-forensic-laboratory-accreditation-requirements-iso-iec-17025/

B. Nelson, A. P. (2019). *"Guide to Computer Forensics and Investigations, Sixth Edition".* Boston: Cengage.

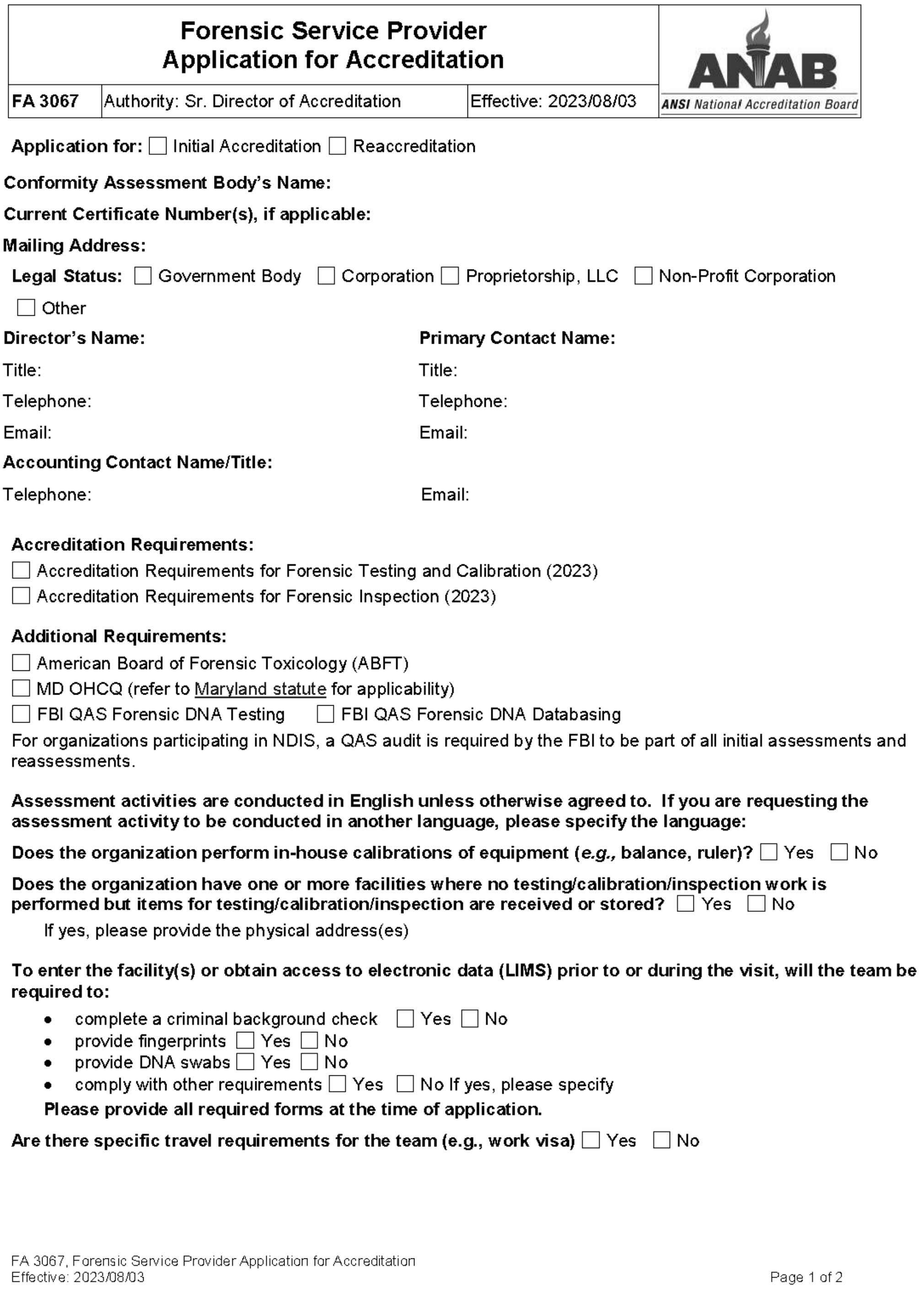
Hatchard, L. (2024, Mar. 8). *"Understand ISO 17025 Calibrations and why They are Important to You"*. Retrieved Apr. 16, 2024, from https://www.ellab.com/: https://www.ellab.com/blog/understand-iso-17025-calibrations-and-why-they-are-important-to-you/

Poston, H. (2021, Jan. 6). *"7 best computer forensics tools"*. Retrieved Feb. 25, 2024, from https://resources.infosecinstitute.com/: https://resources.infosecinstitute.com/topics/digital-forensics/7-best-computer-forensics-tools/

Poston, H. (2021, Jan. 8). *"Computer forensics tools."*. Retrieved Feb. 25, 2024, from https://resources.infosecinstitute.com/: https://resources.infosecinstitute.com/topics/digital-forensics/computer-forensics-tools/

S. Taylor, A. M. (2021, Apr.). "Practical Guideline for Digital Forensics Laboratory Accreditation – A Case Study". *OIC-CERT Journal of Cyber Security, 3*(1), 1-6. Retrieved Apr. 6, 2024, from https://www.oic-cert.org/en/journal/pdf/3/1/B5%201-6%20%20Paper%201%20Practical%20Guideline%20for%20Digital%20Forensics%20Laboratory%20Accreditation%20(with%20author).pdf

Scruthy. (2024, Apr. 2). *"Best-digital-forensics-software"*. Retrieved Apr. 14, 2024, from https://www.softwaretestinghelp.com/: https://www.softwaretestinghelp.com/best-digital-forensics-software/



Forensic Service Provider Application for Accreditation

FA 3067	Authority: Sr. Director of Accreditation	Effective: 2023/08/03	ANAB ANSI National Accreditation Board

Application for: □ Initial Accreditation □ Reaccreditation

Conformity Assessment Body's Name:

Current Certificate Number(s), if applicable:

Mailing Address:

Legal Status: □ Government Body □ Corporation □ Proprietorship, LLC □ Non-Profit Corporation

□ Other

Director's Name: **Primary Contact Name:**

Title: Title:

Telephone: Telephone:

Email: Email:

Accounting Contact Name/Title:

Telephone: Email:

Accreditation Requirements:

□ Accreditation Requirements for Forensic Testing and Calibration (2023)

□ Accreditation Requirements for Forensic Inspection (2023)

Additional Requirements:

□ American Board of Forensic Toxicology (ABFT)

□ MD OHCQ (refer to Maryland statute for applicability)

□ FBI QAS Forensic DNA Testing □ FBI QAS Forensic DNA Databasing

For organizations participating in NDIS, a QAS audit is required by the FBI to be part of all initial assessments and reassessments.

Assessment activities are conducted in English unless otherwise agreed to. If you are requesting the assessment activity to be conducted in another language, please specify the language:

Does the organization perform in-house calibrations of equipment (*e.g.,* balance, ruler)? □ Yes □ No

Does the organization have one or more facilities where no testing/calibration/inspection work is performed but items for testing/calibration/inspection are received or stored? □ Yes □ No

If yes, please provide the physical address(es)

To enter the facility(s) or obtain access to electronic data (LIMS) prior to or during the visit, will the team be required to:

- complete a criminal background check □ Yes □ No
- provide fingerprints □ Yes □ No
- provide DNA swabs □ Yes □ No
- comply with other requirements □ Yes □ No If yes, please specify

Please provide all required forms at the time of application.

Are there specific travel requirements for the team (e.g., work visa) □ Yes □ No

Please provide the number of personnel authorized to perform work accredited by ANAB or for which accreditation by ANAB is being sought:

Testing/Calibration authorized personnel:

Inspection authorized personnel:

Has the organization ever been accredited to ISO/IEC 17025 by an accreditation body other than ANAB?

□ Yes □ No Name of accreditation body:

Has your accreditation been suspended or withdrawn in the past? □ Yes □ No

Has the organization ever been accredited to ISO/IEC 17020 by an accreditation body other than ANAB?

□ Yes □ No Name of accreditation body:

Has your accreditation been suspended or withdrawn in the past? □ Yes □ No

Complete a Forensic Draft Scope of Accreditation for each location.

ANAB's accreditation services are governed by and subject to the AG 1008 Terms and Conditions for Accreditation, which are incorporated by reference here and available here.

Name (printed)

Signature

Date

Submit questions and the completed application to QualityMatters@anab.org