CHAPTER 3

Labs and Tools

Information in This Chapter:

- The Role and Organization of Forensic Laboratories
- The Purpose of Policies & Procedures in Forensic Laboratories
- The Role of Quality Assurance in Forensics
- Digital Forensic Hardware and Software
- Accreditation versus Certification

INTRODUCTION

In this chapter we will explore the different types of laboratory setups as well as the hardware and software tools in common use. We'll also take a look at Standard Operating Procedures and Quality Assurance, two critical components of an effective digital forensic lab. Obtaining and maintaining laboratory accreditation, although time-consuming and expensive, greatly improves a lab's performance and the quality of its findings. Examiner certification ensures that the skill of the labs meets a minimum level. At the end of the day, these elements come together to ensure that only valid and reliable results are produced and that justice is served.

FORENSIC LABORATORIES

Forensic labs are scattered throughout the United States and closely follow the jurisdictional lines of law enforcement (local, county, state, and federal) (James & Nordby, 2009). The majority of these facilities are run by a law enforcement agency. The FBI's crime laboratory in Quantico, Virginia, has the distinction of being the largest lab in the world (Saferstein, 2006).

Not all computer forensic examinations are conducted in what would be considered a traditional laboratory setting. Many agencies conduct them locally at their departments if they have the necessary equipment and trained personnel on hand.

The Basics of Digital Forensics. DOI: 10.1016/B978-1-59749-661-2.00003-6

Digital forensics isn't cheap, so not every agency can afford to train and equip their own examiners. One way to meet this ever-growing demand is the **Regional Computer Forensic Laboratory (RCFL)** program started by the FBI. The RCFL program runs sixteen facilities throughout the United States. They provide digital forensic services and training to all levels of law enforcement. Each RCFL is staffed and managed by a partnership of local, state, and federal law enforcement agencies.

The RCFL program is a great success, and making a significant dent in the backlog of digital forensic examinations across the country. During fiscal year 2010, RCFLs nationwide performed 6,564 forensic examinations and processed a whopping 3,086 terabytes of data. To put that in context, the 2010 Annual Report explains it this way; "One single terabyte is equivalent to 1,024 gigabytes or approximately 1,000 copies of the Encyclopedia Britannica." Doing the math, that's about 3,086,000 encyclopedias. The RCFLs process a wide variety of digital devices and media including smartphones, hard drives, GPS (Global Positioning System) units, and flash drives. In 2010, RCFL examiners helped convict rapists, terrorists, and crooked politicians (Federal Bureau of Investigation, 2010).

Virtual Labs

Digital labs don't have to be confined to a single location. Today's technology makes it possible to run a "virtual" lab with the examiners and the central evidence repository located in geographically separate locations. This arrangement has several advantages including cost savings, greater access to more resources (tools and storage for example), access to diverse and greater expertise, and reduction of unnecessary duplication of resources (Craiger).

This virtual arrangement allows for distinct role-based access. For example, full access could be granted to examiners and laboratory management. Prosecutors, investigators, and defense attorneys would have restricted access. This restricted access would limit what those folks could see and what they could do (read only, etc.) (Whitcomb).

There are some considerable concerns with this approach:

1. **Security**—The security of the system must be robust enough to maintain the level of evidence integrity required by the courts. Otherwise there could be catastrophic consequences, such as rendering evidence from multiple cases inadmissible.
2. **Performance**—For this scheme to work, connectivity must be both speedy and reliable. No connection or a slow connection will quickly impact the organization's ability to function.
3. **Cost**—Startup costs in particular are substantial and potentially beyond what many agencies can afford (Whitcomb).

Lab Security

Lab security is always a major concern. Access to the evidence and facilities must be strictly managed. Strict security plays a key role in maintaining the integrity of

the digital evidence that passes through the laboratory. Only authorized, vetted personnel should have access to critical areas such as examination stations and evidence storage. Unauthorized individuals are usually kept out using doors and other physical barriers along with access controls such as keys, swipe cards, and access codes. Digital solutions such as swipe cards and access codes offer an advantage over older methods such as keys. Electronic means provide a ready-made audit trail that can be used in support of the chain of custody. Security is further enhanced with alarm systems and the like.

Unauthorized access isn't the only threat to the evidence. The risk of fire, flooding, and other natural disasters also must be addressed.

The chain of custody continues at the lab, as does the paperwork. In the lab, the evidence must be signed in and out of the evidence storage area for examinations and court. This log must be completed each and every time the evidence is removed or returned to the evidence room or vault. This checkout and check-in process can be done the old-fashioned way with pen and paper or electronically with scanners and bar codes.

Just like in the field, network access to evidence in the lab is also a concern. This is true for both the Internet and the lab's own computers. Best practice tells us that the machine used to perform the examination should not be connected to the Internet. Removing this connection removes that argument that the evidence was somehow compromised by someone or something (malware for example) via the Internet. Virtual labs will need to be able to articulate how the integrity of their evidence is maintained, given the nature of their operation.

Malware (viruses, worms, and the like) could be hiding on any evidence drive brought in for examination. Connecting it in some manner to the internal network poses a major risk to not only the lab's computers but evidence from other cases as well. To mitigate the risk, these drives should be scanned for viruses by at least one antivirus tool prior to examination.

Evidence Storage

When the evidence is not actively being examined, it must be stored in a secure location with limited access. One of the best solutions is a data safe. These safes come in multiple sizes and are specifically designed to protect digital evidence from theft and fire. Some types of digital media are very vulnerable to heat (tape, for example). A data safe is able to keep the media at an acceptable temperature long enough (hopefully) for the fire to be extinguished.

Evidence storage locations must be kept locked at all times when not actively being used. A log or audit trail should also be maintained detailing who entered, when they entered, and what they removed or returned.

Access to evidence storage and other sensitive areas can be controlled by a variety of means including pass codes and key cards. Electronic controls have some distinct advantages over keys. One significant advantage is the ability to log each

and every time an individual accesses a restricted area. This audit trail can be very helpful in monitoring and verifying the chain of custody.

POLICIES AND PROCEDURES

How the lab handles evidence, conducts examinations, keeps records, and secures its facility should not be left to chance or the whims of any one individual. These tasks should be governed by policies and **Standard Operating Procedures (SOPs)**. SOPs are documents that detail, among other things, how common forensic examinations should be performed. The art in writing SOPs lies in finding the right balance between being too narrow or overly broad. If too specific, the SOP will lack the flexibility needed to address any unusual conditions that may arise. In digital forensics, these situations occur far more often than we'd like. If too broad, they can be ineffective in keeping things consistent and ensuring the integrity of the evidence.

There are inherent dangers in not following your organization's policies and SOPs. Odds are that questions on your organization's policies and SOPs will come up during cross-examination should the case go to court.

QUALITY ASSURANCE

In the early 1980s, the Ford Motor Company told us told us that "Quality is Job 1." You may not believe that today in regard to Ford, but it's most assuredly true in regard to forensic science.

Quality assurance (QA) is a bedrock principle that underpins every discipline in forensic science. As such, every lab should have a QA program. Quality assurance is defined as "a well-documented system of protocols used to assure the accuracy and reliability of analytical results" (James & Nordby, 2009). A good QA program will cover a wide array of subjects including peer reviews of reports, evidence handling, case documentation, training of lab personnel, and more (James & Nordby, 2009).

The review process can be divided into two discrete types: a technical review and an administrative review.

- The technical review, conducted by a separate examiner, focuses on the results and conclusions. The central question in a technical review is "Are the results reported by the original examiner supported by the evidence in the case?"
- In contrast, the focus of an administrative review is ensuring that all of the paperwork is present and has been completed correctly.

An examiner's competency must be confirmed and documented on a regular basis. In the forensic community, this is known as proficiency testing. In a proficiency test, examiners must demonstrate their competence with mock evidence. There are four types of proficiency tests:

1. **Open test**—the analyst(s) and technical support personnel are aware they are being tested.

2. **Blind test**—the analyst(s) and technical support personnel are not aware they are being tested.
3. **Internal test**—conducted by the agency itself.
4. **External test**—conducted by an agency independent of the agency being tested. (Scientific Working Groups on Digital Evidence and Imaging Technology, 2011).

These tests may be conducted in-house, with other lab personnel. These results must be documented because at some point, the analyst's skills and abilities may be called into question during a court proceeding. This documentation will be critical should that happen.

The case of Glen Woodall, although concerning DNA, is a powerful example of the need for quality assurance. On July 8, 1997, Glen Woodall was convicted of the brutal sexual assault of two women by a Cabell County, West Virginia, jury. He was summarily sentenced to two life terms with an additional sentence of 203 to 335 years in prison (The DNA Initiative). The arrest and conviction of Woodall brought some much needed closure to both of the victims and peace to the community as a whole. Unfortunately for the victims and community, the relief didn't last long.

The forensic scientist in this case was West Virginia State Police serologist Fred Zain. After an investigation into Zain's work in both West Virginia and Texas, he was charged with perjury and tampering with evidence (Chan, 1994). During the investigation it was found that Woodall was innocent, and that he, too, was a victim. After serving four years in a West Virginia prison, Woodall was released and awarded $1 million from the state for his wrongful imprisonment.

What the panel found was extremely disturbing. They discovered that Zain "fabricated or altered evidence and lied about academic qualifications under oath." That's not all. The panel also found that his supervisors may have been culpable as well, overlooking or hiding complaints about his performance (Chan, 1994).

In 2011, twenty-four years later, the real suspect was arrested and eventually convicted of the crimes of which Woodall was originally found guilty. On April 1, Donald Good was sentenced to over two hundred years in prison (WSAZ, 2011). Cases like this hammer home the need for effective quality assurance programs in all forensic sciences.

Tool Validation

Our tools, be they hardware or software, must function as they are designed. Each and every tool must be validated before it's used on an actual case. A validation process clearly demonstrates that the tool is working properly, is reliable, and yields accurate results. We can't simply accept the manufacturer's word for it; assumptions aren't permitted.

The validation process is another one of those things that has to be committed to paper. To do otherwise will put any evidence found in real jeopardy of being excluded.

Documentation

The importance of complete and accurate documentation can't be overstated. The old saying "if you didn't write it down, it didn't happen" are truly words to live by in this industry. There are different types of documentation and reports used throughout the entire forensic process. These should be spelled out in the labs' or agencies' SOP and policy manuals. Submission forms, chain of custody records, examiner's notes, and the examiner's final report form the crux of the required documentation.

Normally, all the paperwork associated with a specific case is collected into a case file. The case file will contain all of the documentation pertaining to the case, including paperwork generated by the examiner and others. Usually they include case submission forms, requests for assistance, examiners' notes, crime scene reports, case reports, copy of the search authority, chain of custody, and so on (National Institute of Justice, 2004).

FORMS

Preprinted forms are widely used in both the field and the lab. They help guide personnel through the process and ensure that a high level of quality is maintained. Forms ensure all the necessary information is captured in a uniform manner. Typically, forms are used to describe the evidence in detail (make, model, serial number, etc.), document the chain of custody, request an examination, and so on.

EXAMINER NOTES

Examiner's notes cover most, if not all, of the examiner's actions and observations along with corresponding dates. They must be detailed enough to enable another examiner to duplicate the process used during the examination. Things typically recorded here include:

- Discussions with key players including prosecutors and investigators.
- Irregularities found and associated actions taken.
- Operating systems, versions, and patch state.
- Passwords.
- Any changes made to the system by lab personnel and of law enforcement. (National Institute of Justice, 2004)

If you've ever worked in the legal system, then you know that the wheels of justice can turn very, very slowly. This applies to both criminal and civil cases. It can be months or even years before a case ever gets to trial. By the time you have to testify, you may only be able to recall few, if any, facts of the case. The case documentation, and your notes in particular, will prove a great tool to refresh your recollection.

EXAMINER'S FINAL REPORT

The **examiner's final report** is the formal document that is delivered to prosecutors, investigators, opposing counsel, and so on at or near the end of an investigation. These reports typically consist of:

- Identity of the reporting agency.
- The case identification number/submission number.
- Identity of the submitting person and case investigator.
- Dates of receipt and report
- Detailed description of the evidence items submitted including serial numbers, makes, models, and so on.
- Identity of the examiner.
- Description of the steps taken during the examination process.
- Results and conclusions. (National Institute of Justice, 2004)

When drafting the final examiner's report, it's critical to take into account the intended audience, which is primarily laypeople. The lawyers, investigators, judges, and clients will most likely have little to no technical background. All too often these reports are filled with technical jargon and details that only serve to frustrate and confuse the majority of its intended audience. These reports should be comprehensible to a nontechnical audience. Jargon and acronyms should be kept to an absolute minimum.

Two major sections of the examiner's report are the summary and the details of the findings. The summary is a brief description of the results of the examination. The end users of our reports find this feature useful, especially in light of the massive caseload and amount of information they are typically dealing with. The findings included here should be supported and explained in the detailed findings.

The detailed findings provide the substance of the report. They provide the details of the examination, steps taken, results, and so on. Typically you may find details relating to:

- Files directly pertaining to the request.
- Files that support the findings.
- Email, web cache, chat logs, and so on.
- Keyword searches.
- Evidence of ownership of the device. (National Institute of Justice, 2004)

A glossary is a helpful addition to an examiner's report. Anything we can do to help our intended audience wade through any unfamiliar jargon and acronyms is always a good thing. Conveying our findings in a way that can be understood is our responsibility as forensic professionals.

DIGITAL FORENSIC TOOLS

Digital forensic tools make our work much more efficient or even possible. There are tools for specific purposes as well as tools with broader functionality.

They can come in the form of both hardware or software. They can be commercial tools that must be purchased or they can be open source that are freely available. There are advantages and disadvantages to all. Keep in mind, no single tool does everything or does everything exceedingly well. As such, it's a good practice to have multiple tools available. Using multiple tools is also a great way to validate your findings. The same results, with two different tools, significantly increase the reliability of the evidence.

Tool Selection

The digital forensic tool market boasts a large number of products, with more rolling out all the time. How does an examiner know which tools are reliable and which ones are not? How should these tools be validated? The National Institute of Standards and Technology (NIST) and the National Institute of Justice (NIJ) have taken a big step in helping to answer these and other questions.

NIST has launched the Computer Forensic Tool Testing Project (CFTT), which establishes a "methodology for testing computer forensic software tools by development of general tool specifications, test procedures, test criteria, test sets, and test hardware" (National Institute of Standards and Technology).

Let's explore what this looks like. This is an excerpt from the NIST test of a Tableau brand hardware **write blocking device (HWB)**, summarizing some of the test criteria and results:

> "An HWB device shall not transmit a command to a protected storage device that modifies the data on the storage device."
>
> "For all test cases run, the device always blocked any commands that would have changed user or operating system data stored on a protected drive."
>
> "An HWB device shall return the data requested by a read operation."
>
> "For all test cases run, the device always allowed commands to read the protected drive." (National Institute of Justice, 2009)

Each tool, be it hardware or software, must be validated before it is used on casework as well as anytime it is modified or updated. For an example, like other software you're familiar with, our forensic software gets updated on a regular basis. After each update, the tool should be validated again. Validation also proves useful in court, supporting the validity of the tool's results.

Hardware

There are many hardware tools out there designed and built specifically for digital forensics. Some of these tools include cloning devices, cell phone acquisition devices, write blockers, portable storage devices, adapters, cables, and more.

As you might expect, digital forensics is heavily dependent on an assortment of hardware such as PCs, servers, write blockers, cell phone kits, cables, and so on. Figure 3.1 shows a well-equipped digital forensic workstation.

FIGURE 3.1
One of the workstations in the West Virginia State Police Digital Forensics Lab located at the Marshall University Forensic Science Center. (Courtesy of Cpl. Bob Boggs).

Computers are the backbone of any digital forensics lab. So as an examiner you will need the best computer workstation you can afford. Digital forensic exams require quite a bit of computing power. These jobs can tax even the best systems and crush those that don't measure up. A good exam machine has multiple, multi-core processors, as much RAM as you can get (the more the better), and large, fast hard drives. Forensic software manufacturers provide detailed lists of minimum and suggested hardware requirements. Straying below the minimums is done at your own risk. To get a better understanding, let's look at the minimum and recommended system requirements (as of press time) for AccessData's Forensic Tool Kit (FTK).

AccessData's FTK comprises four distinct components and or applications. They are:

1. Oracle Database
2. FTK Client User Interface (UI)
3. Client-side Processing Engine
4. Distributed Processing Engine

The minimums and recommended specifications will vary with each component, but suffice it to say that you can never have too much RAM or computing power. For example, on a machine running the Oracle database, the FTK user interface and the primary processing engine, AccessData recommends the requirements shown in Table 3.1.

Table 3.1 **Basic Recommended Requirement (AccessData Group, LLC, 2011)**

	Minimum	Recommended
Processor	Intel® i7 or AMD equivalent	Intel® i9 Dual Quad Core Xeon, i7 Nehalem or AMD equivalent
RAM	12GB (DDR3) 8GB (DDR2)	12GB (DDR3) 8GB (DDR2)
Operating System	Vista, 2008, Windows 7 (64 bit)	Vista, 2008, Windows 7 (64 bit)

Some components may be installed on separate machines. The minimum and recommended requirements will change depending on which configuration is used.

Examiners frequently sift through massive amounts of data. As such, digital forensics labs need to have the capacity to store voluminous amounts of data. In browsing the PCs for sale on bestbuy.com, the majority of them have between 500 GB and 699 GB of hard drive space. Multiterabyte drives are also available. With numbers like these and caseloads ever increasing, it's easy to see that storage is a major concern.

Digital forensics is no longer a "PC centric" endeavor. Small-scale devices such as cell phones and GPS units are pouring into labs across the country. These devices require different hardware from that used on laptops and desktops. Cellebrite's UFED supports over three thousand phones (Cellebrite Mobile Synchronization LTD). Paraben Corporation, a competitor of Cellebrite, boasts support for more than four thousand phones, PDAs, and GPS units (Paraben Corporation). When dealing with cell phones, having the proper cable is critical. Unlike PCs, mobile devices lack much of the standardization with regard to connectors and cables. Labs need to have a wide selection of cables on hand to cope with the vast array of handsets that walk through the doors. Fortunately, the manufacturers of mobile phone forensic hardware provide many of the required cables.

Several companies make hardware cloning devices. If you recall, a forensic clone is a "bit stream" copy of a particular piece of media such as a hard drive. These tools can really speed up the process, cloning multiple drives at once. They can also provide write protection, hash authentication, drive wiping, an audit trail, and more.

OTHER EQUIPMENT

The hardware and software we discussed earlier are not the only equipment needed. Crime scene kits are very useful outside the lab. These kits are preloaded with all of the supplies an examiner would need in the field to collect digital evidence. Kits contain standard items such as pens, digital camera, forensically

clean storage media, evidence bags, evidence tape, report forms, permanent markers, and the like.

Software

There is a wide array of digital forensic software products on the market today. Some are general tools that serve a variety of functions. Others are more focused, serving a fairly limited purpose. These applications tend to focus on a very specific type of evidence, e-mail or Internet, for example.

When selecting software, a choice needs to be made between going with open source tools or a commercially produced product. There are advantages and disadvantages to both. Factors such as cost, functionality, capabilities, and support are some of the criteria that can be used to make this decision.

ADDITIONAL RESOURCES

Open Source Tools

Cory Altheide and Harlan Carvey's book *Digital Forensics With Open Source Tools* is an excellent reference for those practitioners using these applications.

One of the more popular open source tools is SIFT, or the SANS Investigative Forensic Toolkit. SIFT Workstation is a powerful, free, open source tool. It's built on the Linux Ubuntu operating system. This tool is capable of file carving as well as analyzing file systems, web history, recycle bin, and more. It can also analyze network traffic and volatile memory. It can also generate a timeline, which can be immensely helpful during an investigation. SIFT supports the following file systems:

- Windows (MSDOS, FAT, VFAT, NTFS)
- MAC (HFS)
- Solaris (UFS)
- Linux (EXT2/3/4)

(The SANS Institute)

As for commercial tools, two of the most popular general software tools are Forensic Toolkit (FTK®) from AccessData and EnCase® from Guidance Software. Both are excellent and can make exams easier and more efficient. These applications have "Swiss Army knife"–like capabilities. They perform a multitude of tasks, including:

- Searching
- E-mail analysis
- Sorting
- Reporting
- Password cracking

The search tools in these products are particularly powerful, and give examiners the capability to drill down to precisely the information they are looking for. Here is a quick list of some of the information that can be searched for:

- E-mail addresses
- Names
- Phone numbers
- Keywords
- Web addresses
- File types
- Date ranges

As helpful as these tools can be, they do have some limitations. The reality is that no single tool does it all. For that reason, budget permitting, labs need to have a variety of tools available.

More and more specialty tools are coming on the market. These tools focus on one aspect of digital evidence such as e-mail or web-based evidence. These can bring some additional capabilities to the table that some multipurpose tools don't.

ALERT!

Dependence on the Tools

GUI-based forensic tools can become a crutch. "Push-button" tools can make exams much more efficient, but they don't relieve the examiner of his or her responsibility to understand what's going on beneath the surface. Examiners need to understand not only what the tool is doing, but also how the artifact in question is created to begin with.

Some of the forensic tools that an examiner may use are listed in Table 3.2. Many of these companies offer video tutorials or demonstrations of their products. These can be a great source of additional information. They are typically available from their web site or on YouTube. This is in no way meant as an endorsement of a specific tool. These are only a representative sampling of the many tools that are available.

ACCREDITATION

Accreditation is an endorsement of a crime lab's policies and procedures, the way it does business, if you will (James & Nordby, 2009). **The American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB)** is recognized as a world leader in the accreditation of forensic laboratories. Despite the name, ASCLD/LAB grants accreditation to labs both inside and outside the United States, which it has been doing since 1982 (Barbara).

Table 3.2 Some hardware and software tools that may be found in a digital forensics laboratory

Tool	Use	URL
Forensic Toolkit Access Data Group, LLC	Multipurpose tool (acquisition, verification, searching, reporting, wiping, etc.)	http://accessdata.com
EnCase Guidance Software, Inc.	Multipurpose tool (acquisition, verification, searching, reporting, wiping, etc.)	http://www.guidancesoftware.com
SMART & SMART for Linux ASR Data, Data Acquisition and Analysis, LLC	Multipurpose tool (acquisition, verification, searching, reporting, wiping, etc.)	http://www.asrdata.com/forensic-software/
X-Ways Forensics X-Ways Software Technology AG	Multipurpose tool (acquisition, verification, searching, reporting, wiping, etc.)	http://www.x-ways.net/forensics/
Helix3 Pro e-fense, Inc.	Multipurpose tool (acquisition, verification, searching, reporting, wiping, etc.)	http://www.e-fense.com/products.php
Softblock, Macquisition, Blacklight BlackBag Technologies, Inc.	Multiple Macintosh forensic tools	https://www.blackbagtech.com/forensics.html
Mac Marshall Architecture Technology Corporation	Multiple Macintosh forensic tools	http://www.macmarshal.com/
Raptor Forward Discovery, Inc.	Linux-based acquisition and preview tool	http://www.forwarddiscovery.com/Raptor
Dossier Logicube, Inc.	Hardware acquisition	http://www.logicube.com/
Forensic hardware tools Tableau	Write blockers, bridges, storage, acquisition	http://www.tableau.com/
Wiebetech	Storage, write blockers, etc.	http://www.wiebetech.com/home.php

Based in Garner, North Carolina, ASCLD/LAB has accredited a total of 385 crime laboratories, 17 of those being outside the United States (American Society of Crime Laboratory Directors/Laboratory Accreditation Board).

According to ASCLD/LAB, they have four objectives. They are to:

1. improve the quality of laboratory services provided to the criminal justice system.
2. develop and maintain criteria that may be used by a laboratory to assess its level of performance and to strengthen its operation.

3. provide an independent, impartial, and objective system by which laboratories can benefit from a total operational review.
4. offer to the general public and to users of laboratory services a means of identifying those laboratories that have demonstrated that they meet established standards (American Society of Crime Laboratory Directors/Laboratory Accreditation Board).

Think of ASCLD/LAB as the "Good Housekeeping Seal of Approval" for forensic science. The earning and maintaining an ASCLD/LAB accreditation is no easy chore. It requires an unbelievable amount of time, planning, documentation, and money. Nothing is taken for granted. Every standard met must be backed up with extensive, detailed documentation.

ASCLD/LAB offers two accreditation programs. The first is the legacy program and the second is the international program. The legacy program is the first program instituted by ASCLD/LAB. As you might expect, there are differences between the two programs as well as some common ground. A major difference is the number of criteria that must be met under each program. The international program has considerably more standards to meet than the legacy program. Labs seeking accreditation under the international program are required to fulfill the relevant requirements to demonstrate conformance to the applicable requirements of both the ISO/IEC 17025:1999(E) General Requirements for the Competence of Testing and Calibration Laboratories and the ASCLD/LAB-International Supplemental Requirements for the Accreditation of Forensic Science Testing and Calibration Laboratories.

While accreditation is highly desirable, it's not mandatory. Non-accredited labs can and do successfully process evidence. The reality is that obtaining and maintaining an accredited forensic lab is both a cash and labor-intensive proposition. The kind of staffing and funding commitment required is tough to secure and frankly is not an option for everyone.

THE AMERICAN SOCIETY FOR TESTING AND MATERIALS (ASTM)

In addition to ASCLD/LAB, ASTM International also provides standards for the various disciplines within the forensic sciences, including digital forensics. ASTM International was formerly known as the **American Society for Testing and Materials**. It was founded in 1898 by engineers and chemists of the Pennsylvania Railroad. The standards are developed by subject matter experts that are members of ASTM (ASTM International).

Accreditation versus Certification

These terms may seem interchangeable; however, in the context of a forensic laboratory, they are not. As described earlier, accreditation refers to the laboratory, whereas certification pertains to the individual examiners. Certification normally requires an examiner to pass a written or practical test(s).

The Scientific Working Group on Digital Evidence (SWGDE) issued a paper addressing the certification of digital forensic practitioners. SWGDE asserts that any digital forensic certification must address the following core competencies, at a minimum:

1. Pre-examination procedures and legal issues
2. Media assessment and analysis
3. Data recovery
4. Specific analysis of recovered data
5. Documentation and reporting
6. Presentation of findings (Scientific Working Group on Digital Evidence, 2010)

SUMMARY

The forensic laboratory plays a critical role in our justice system. Well presented forensic evidence can be very, very persuasive to a jury. Many, many cases turn on the forensic evidence itself or the lack thereof. The forensic laboratory therefore plays a pivotal role in the search for justice.

Quality must be a priority in every forensic laboratory and to every forensic professional. Digital forensics is no different. Quality is achieved through the strict adherence to established quality standards as part of an overall quality assurance program. Accreditation of a digital forensics laboratory is one way to ensure conformance to these standards. The recognized world leader in accreditation of forensic labs is ASCLD/LAB. Standards for digital forensics are drafted by the ASTM.

Accreditation and certification are not synonymous. The primary difference is that accreditation pertains to the physical lab where certification applies to the personnel conducting the examinations. Not only should examiners be tested to demonstrate that they are "functioning properly," so to should their tools. Only tools that have been tested and proven reliable should be used when processing a case. This testing procedure is known as validation.

Digital forensic practitioners use both software and hardware tools in their work. No one single tool does everything or does it well. Most labs will have a variety of tools at their disposal to give them the broad capability they need given the wide array of technology they see coming in the door for analysis.

References

About: American Society of Crime Laboratory Directors/Laboratory Accreditation Board. (n.d.). Retrieved June 4, 2011, from: http://www.ascld-lab.org/about_us/aboutoverview.html

AccessData Group, LLC. (2011, February). *Downloads: AccessData.* Retrieved August 24, 2011, from: http://accessdata.com/downloads/media/FTK_3x_System_Specifications_Guide.pdf

American Society of Crime Laboratory Directors/Laboratory Accreditation Board. (n.d.). *Did You Know: American Society of Crime Laboratory Directors/Laboratory Accreditation Board*. Retrieved June 4, 2011, from: http://www.ascld-lab.org/largest_accreditation.html

American Society of Crime Laboratory Directors/Laboratory Accreditation Board. (n.d.). *Objectives: American Society of Crime Laboratory Directors/Laboratory Accreditation Board*. Retrieved June 4, 2011, from: http://www.ascld-lab.org/about_us/objectives.html

Barbara, J. J. (n.d.). *Digital Evidence Accreditation*. Retrieved August 25, 2011, from: http://www.forensicmag.com/article/digital-evidence-accreditation?page=0,3

Barbara, J. J. (n.d.). *Digital Evidence Accreditation: Forensic Magazine*. Retrieved June 4, 2011, from: http://www.forensicmag.com/article/digital-evidence-accreditation

Brunty, J. (2011, March 2). *Validation of Forensic Tools and Software: A Quick Guide for the Digital Forensic Examiner*. Retrieved August 24, 2011, from: http://www.dfinews.com/article/validation-forensic-tools-and-software-quick-guide-digital-forensic-examiner?page=0,2

Carrier, B. B. (2002, October). *Papers: Digital-evidence.org*. Retrieved August 24, 2011, from: http://www.digital-evidence.org/papers/opensrc_legal.pdf

Chan, S. (1994, August 21). *Scores of Convictions Reviewed as Chemist Faces Perjury Accusations*. Retrieved from LATimes.com: http://articles.latimes.com/1994-08-21/news/mn-29449_1_lab-tests-fred-zain-double-murder (Accessed 21.08.94).

Federal Bureau of Investigation. (2010). *Regional Computer Forensics Laboratory Annual Report Fiscal Year 2010*. Washington, DC: U.S. Department of Justice.

James, S., & Nordby, J. J. (2009). *Forensic Science: An Introduction to Scientific and Investigative Techniques, Third Edition*. Boca Raton, FL: CRC Press.

National Institute of Justice. (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*. Washington, DC: U.S. Department of Justice.

National Institute of Justice. (2009). *Test Results for Hardware Write Block Device: T4 Forensic SCSI Bridge (FireWire Interface)*. U.S. Department of Justice, Office of Justice Programs. Washington, DC: National Institute of Justice.

National Institute of Standards and Technology. (n.d.). *Computer Forensics Tool Testing Project Web Site: National Institute of Standards and Technology*. Retrieved June 6, 2011, from: http://www.cftt.nist.gov/index.html

Saferstein, R. (2006). *Criminalistics: An Introduction to Forensic Science (College Edition) (9th ed.)*. Upper Saddle River, NJ: Prentice Hall.

Scientific Working Group on Digital Evidence. (2010, May 15). *Minimum Requirements for Quality Assurance in the Processing of Digital and Multimedia Evidence*. Retrieved August 24, 2011, from: http://www.swgde.org/documents/current-documents/

Whitcomb, C. A. (n.d.). *Virtual Digital Forensics Lab*. Largo, FL: National Center for Forensic Science.

WSAZ. (2011, April 1). *UPDATE: Donald Good Receives Two Life Sentences in Mall Rape Case*. Retrieved from WSAZ.com: http://www.wsaz.com/news/headlines/UPDATE_Judge_OHanlon_Will_Preside_Over_Huntington_Mall_Rape_Case.html (Accessed 17.11.11).