



Setting up an electronic evidence forensics laboratory

Hank Wolfe

Associate Professor,
Computer Forensics &
Security,
Information Science Dept.,
Otago School of Business,
University of Otago,
Corner of Clyde & Union
Streets, PO Box 56,
Dunedin, New Zealand
Tel: +64 3 479-8141
Fax: +64 3 479-8311
Email: hwolfe@infoscience.otago.ac.nz

In our last column we took a look at being an expert witness and giving forensic evidence testimony. An added word of cautionary advice for private practitioners: CHARGE A LOT for expert testimony! If you are involved in a high-profile case that drags on and on and you must testify as an expert witness repeatedly at the whim and caprice of the various attorneys, it could disrupt your private practice and cause potential loss of current and future earnings. Your current case load could be seriously delayed and your credibility for future work may also be damaged. The previous discussion, by nature, was very general, however each jurisdiction has a formal set of directives and guidelines specifically to assist expert witnesses so you must also refer to these for more details.

The following discussion will be focused on setting up an electronic evidence forensics laboratory and the various parts that make up a professional facility. The many parts also include the portable forensics kit(s), which includes documentation forms, evidence bags, tags, labels, etc, as well as portable hardware and associated software for undertaking an evidentiary acquisition on site. Not all such activities may be performed in the lab, but the mobile forensics toolkit must be fully compatible and in sync with the laboratory acquisition equipment and software at all times.

There may be accreditation for such laboratories, depending on the jurisdiction. For example, in the US one such accreditation may be sought from the American Society of Crime Laboratory Directors. If accreditation is possible in your jurisdiction, it may be advisable to explore the criteria for achieving it. While there may be differing views as to the value of accreditation, it is my opinion that having it is one more stone in the

foundation of credibility, and therefore it should be viewed in a positive light.

The parts

There are several parts that make up a forensics laboratory. Firstly, there is the physical facility itself. This will be the home base for secure storage of evidentiary materials, for the analysis of captured data, for the operation of cloned systems, for the production of final evidence reports, and for the physical premises where the forensics professional will perform most of their duties and work. So, it is a secure storage facility, an office, an operational laboratory, and a production facility all rolled into one.

It should also have a separate interview facility or office where interviews and/or collaborative investigative procedures can be carried out without disturbing any ongoing technical or forensic work. Normally an investigating officer or attorney with an in-depth knowledge of the case will have queries that can be answered more effectively in collaboration with the forensic investigator. The forensics professional will, in real-time, perform specific analysis and/or search actions to find the answer to questions posed by the investigating officer or attorney.

Physical requirements

Physical floor space will be dictated by the size of the group that will occupy it. The space should be in a secure location or contain appropriate measures that will stop unauthorized access to the premises. It should have an adjacent and secure walk-in lock-up vault that can keep intruders from gaining access to its contents as well as protect the contents from fire/heat, smoke, water, and electromagnetic emanations (and should generally not be near radio equipment). The

seized equipment, as well as official certified evidentiary copies of seized data, will be stored in this vault and, with the appropriate enforced sign-out/in procedures, it will serve to maintain the chain of evidence. Therefore, access to the vault and its contents should be logged and monitored at all times.

There also needs to be adequate lockable storage space for various specialized equipment that will, over the course of investigations, be acquired and used for other investigations. This space must also accommodate consumables like CDs, DVDs, removable hard drives of various capacities, paper, toner cartridges, etc.

Hardware requirements

A number of computers is required, including a network server with large storage capacity (preferably configured for the standard removable hard drives). This server will be used to manage, document and administer cases, store various software tools, and manage one-off specialist hardware. The hardware that must be managed will include, for example, devices like Rimage CD production units, CopyPro floppy disk readers, printers, etc. The evidentiary copy of seized data is usually written to CD or DVD and, because of the large capacity of current hard drives, this can be a time-consuming process. The Rimage, and other units like it, make it possible to create, number and label the media unattended, producing as many as 50 CD/DVDs without intervention. Capturing the contents of floppy disks is even more time consuming, and devices like the CopyPro can acquire as many as 50 floppy disks without intervention. The capabilities of these types of devices may vary from model to model; the two mentioned above are merely examples with specific capacities.

There should also be separate Internet connection(s). (NEVER connected to the forensics server). The Internet will be useful for finding and sharing forensics information and

techniques and for communicating with other forensics professionals. Staying abreast of developments in this field is a vital part of staying viable in the forensics arena. The Internet provides one source to help accomplish this need.

There should be a number of workstations that connect to the internal network. This number will depend on how many forensics people are employed. The workstations will enable them to work on individual cases simultaneously and have access to the shared devices and resources.

Portable acquisition computers (the kit) will be required. Ideally, each should be configured identically with the standard forensics suite of tools and removable hard drives (the same standard hard drives as above) of various capacities. Each kit should have a robust carrying case that can accommodate extra hard drives, an array of associated connection plugs and converters, and a hard drive write blocker such as FastBlock. The forensic kits will be used for on-site acquisition and/or seizure. It is usually preferable for acquisition to be undertaken in the controlled conditions of the laboratory, however there are circumstances where that is not practical and an evidentiary acquisition must be undertaken on site (for example, when dealing with an Internet service provider). These kits must also have an assortment of forms, labels, tags, pens, tape, evidence bags, an electronic camera, a GPSS, etc, all of which are vital to the process of seizure and acquisition.

There will be an ongoing need to obtain devices, media, cables, converters, and specialized media readers of various types, both for experimental purposes and for the acquisition of evidence from media other than hard drives or floppies (for example, SIMs, flash memory of various description, iButtons, etc).

The hardware and physical premises constitute the largest outlay of funds. This, however, is an ongoing process and funds must be allocated

Henry B. Wolfe

Henry B. Wolfe has a long computing career spanning more than 43 years. He currently specializes in cryptographic problems where related to forensic investigation, general computer security, surveillance, and electronic forensics teaching these topics to law enforcement (both in New Zealand and internationally) as well as at the graduate level in the University of Otago located in Dunedin, New Zealand, where he is an associate professor.

regularly for the purchase of new hardware as it finds its way into the public arena.

Software requirements

The standard forensics software packages, such as EnCase, Forensics Tool Kit, Password Recovery Tool Kit, etc, are expensive products. It is worth noting that some require dongles to work and that these must be managed. In most cases the capabilities of the software tool outweigh the nuisance and inconvenience of the required dongle. These products tend to be upgraded annually and, in each case, funds must be allocated for the upgrades. However, the software tools that are used comprise a far wider range than just those cited above. Many are freeware and many are not. No single tool performs the entire job of forensics acquisition, analysis and reporting, so we tend to use the right tool for the right task. Therefore, the forensics software tool library will be extensive and will probably continue to grow. Having the right tool may make the difference between capturing relevant evidence and not being able to do so — a case may be won or lost as a result.

In addition, of course, the standard operational software will be required. This includes LAN software, operating systems, administrative software, graphics software, etc. These too will need to be upgraded occasionally, so funds must be allocated for this ongoing process too.

While the continued cost of software acquisition and upgrades is smaller than that of hardware, it still constitutes a significant portion of any forensic laboratory budget and must not be overlooked. The physical price of operating a forensics laboratory is not insignificant.

Procedural requirements

Methods and procedures are an important part of operating a successful forensics laboratory.

The main issues that can and usually are attacked when evidence is presented in a court of law are credentials and methodology. Therefore, close attention must be paid to strictly following and documenting the methodology formally adopted by the lab in the acquisition, analysis and reporting processes. Moreover, it is equally important to have a formal procedure that documents the handling and control of evidence in order to be able to document the 'chain of evidence'. These are the two main issues that are unique to a forensics laboratory. There are other procedures and policies that should be in place and enforced, but they are the standards like Internet usage, email rules, back-up regimes, etc.

Summary

All of these parts, facility, hardware, software and procedures still rely on the skills, dedication and professionalism of the people involved. The commitment and dedication required of these people mean that esprit de corps and morale is vital to any such operation. This comes from leadership by example and good management — a topic for another forum.

This column concludes this series of articles about electronic forensics. We hope that you have found the series to be useful and illuminating. It has deliberately been broad in its scope and content and intended as an introductory briefing on electronic forensics. You may find a more detailed discussion in our soon-to-be published book (*Practitioner's Guide to Electronic Forensic Evidence Gathering*). Remember, if you have questions or comments (critical, complimentary or helpful), please contact us.