The objective is to prevent unauthorized access, which could lead to questions about the chain of custody of the evidence.

Building a Computer Forensics Laboratory

Kelly J. (KJ) Kuchta CFE, CPP

This is the first article in a five-part series on computer forensics considering five aspects of a computer forensics program. This series will include: "Building A Forensic Laboratory," "Creating Your Forensic Tool Box," "Training Your Forensics Team," "Understanding Forensics Methodology," and "Conducting Forensic Investigations."

If your organization has decided to build a computer forensics capability in-house or is even considering the possibility, do you know what kind of physical resources are needed to carry out this task? If you have no direct experience in establishing a computer forensic laboratory, the answers might surprise you. This article walks through some of the things you should consider. The size of your laboratory will have a bearing on the cost of this process, as will the geographic location of your laboratory, type of forensic work you will perform, and objective. This article addresses the initial cost and implementation effort, but there are continual costs and requirements that need to be considered in maintaining a laboratory. New technology will require constant vigilance in keeping your investment sharp.

There are five key areas to consider in building a forensic laboratory for your organization. They include:

- ☐ 1. Facilities
- ☐ 2. Configuration
- ☐ 3. Equipment
- ☐ 4. Software
- ☐ 5. Reference materials

This article addresses each area, pointing out important considerations that should be taken into account when building a computer forensic laboratory.

K.J. KUCHTA CFE, CPP, is the National Director for METASeS SecuritE-RESPONSE Services, based in Phoenix, Arizona. He is an active member of the High Technology Crime Investigation Association (HTCIA), Association of Certified Fraud Examiners (ACFE), Computer Security Institute (CSI), International Association of Financial Crime Investigators Association (IAFCI), and the American Society of Industrial Security (ASIS). He currently serves as the Chair on the ASIS Standing Council of Information Technology Security.

FACILITIES

Let's first tackle the facilities as they relate to creating a secured environment. Our objective is to prevent unauthorized access, which could lead to questions about the chain of custody of our evidence. The environment we are trying to create is every bit as sterile and controlled as a medical laboratory (though it may not be as clean). In some ways it is just as important because the information coming from the lab will be used to decide liability or possibly the guilty or innocence of a person or corporation. That is a pretty high standard to hold the digital evidence your team will be working on. But it is necessary in order to present evidence to a court of law in the United States. It can be even more stringent in other countries. If this standard is not met, allegations of tampering, sloppy practices, or unreliable use of equipment can taint your hard work. What you are protecting is the equipment and evidence that is to be used in a court of law. This is generally the first attack that the opposing counsel will take. Think about it, if they get the evidence thrown out of court, the case wilts and you or your corporation could end up with yolk on your face.

To meet the objectives listed above, I highly recommend that the laboratory be constructed in an area that has a low volume of traffic. Limit access by only allowing those individuals working in the laboratory to enter. The access control system should be of good quality to prevent unauthorized access. To prevent unauthorized access, it is recommended that there be no windows that open in the lab. It is a good idea to have only one entrance into the laboratory, which allows for easier control of the facility.

Remove all false ceilings. I have personally observed a "secured facility" that was as easy to penetrate as popping the ceiling tile out and climbing over the wall. The same could be said for raised floors that are so common in data centers. If working on an important piece of work, be prepared for opposing counsel to want to review your facility and nit-pick your security. It is much better to think of it now than to lose the case and spend the money later.

CONFIGURATION

Once the facility has been secured, we can design the room configuration to maximize our efforts. Let's talk a little about the furniture and furnishing that a laboratory should have. The list might include:

☐ *Desktops*, with plenty of room to disassemble a computer on
☐ *Bookcases for your library*, to include reference material and software
☐ *Evidence safe or locker*, large enough to store media such as hard drives, tapes, CD-ROMs, etc.
☐ *LAN and server stations*, to establish network or launch multiple jobs
☐ *Storage shelves*, for equipment not in use

I recommend setting up the desktops in a clustered setting to improve communication and allow for easier interaction between forensic professionals. This configuration lends itself to establishing a forensic network if you chose. Should you choose to build a forensic network, keep in mind any network security issues that might compromise your data. In general, it is a good idea to construct your forensic network as a "stand-alone" network. Doing this will help keep the network security issues to a minimum. If you choose to build a network, I would highly recommend establishing a backup process for the electronic data. Do not forget to make sure that you have adequate power supplies for all of the equipment you will have. I recommend having at least four (4) electrical outlets for each workstation/person. That would include workstation, monitor, maybe an external drive like DLT or DAT, and printer

I have personally observed a "secured facility" that was as easy to penetrate as popping the ceiling tile out and climbing over the wall.

or other device. You can never have too many; so plan accordingly.

The safe should be secure and offer protection from fire. This provides a good preservation net should a catastrophe occur at the facility. If your laboratory is used extensively, you will probably have various pieces of hardware in the evidence locker on an irregular basis. It will be a tremendous advantage to have this equipment close and under the security of the laboratory. You might also find some law enforcement agencies that have a much tighter control on evidence and have an "evidence room" in a different location. The philosophy is to allow very limited time with the evidence so that it removes the possibility of tampering with the information.

EQUIPMENT

How you equip your laboratory will depend on a number of things, such as the types of operating systems you will use, size of storage capacity, tape media used, and even what type of forensic analysis might be carried out. I have listed some of the items you should consider and will later address the specifics of some of the key components. The list might include:

☐ 1. *forensic towers* with large CPU, large RAM, and multiple ports for hard drives, CD-ROM writer
☐ 2. *monitor*
☐ 3. *UPS (uninterrupted power supply)* to protect your hardware and evidence
☐ 4. *printer*
☐ 5. *server* if you are planning to establish a forensics network in the laboratory
☐ 6. *external SCSI jazz drive* for saving forensic evidence or images
☐ 7. *variety of SCSI cards* compatibility between hard drives makes these a necessity
☐ 8. *extra hard drives* for saving forensic evidence or images
☐ 9. *tape drives* that should match the type of media you are likely to encounter or need to fulfill your backup process (i.e., DAT, exabyte, DLT, etc.)
☐ 10. *blank tapes* for saving forensic evidence
☐ 11. *mobile computer* to take into the field (see forensic tower specifications and try to come as close as possible to performance)
☐ 12. *disk duplicator*, a forensic hardware device that will make an exact copy of a hard drive to another hard drive
☐ 13. *digital camera* for establishing the condition of evidence or a situation
☐ 14. *computer toolkit* (you may need to get your hands dirty and pop off the case of the computer.)
☐ 15. *hub* for the office and field because you might have a need to set up a network
☐ 16. *various cables, SCSI adapters, screws, jumpers, etc.*

Some items will need to be purchased for each forensic practitioner and others can be shared. I do not include the individual personal computer, which should be used to write correspondence, reports, or even check e-mail.

Most organizations want to use the same computer to complete forensic examinations and for individual use. There are a number of reasons why I do not recommend it, but I will give you just three. First, while running resource intensive forensic programs, the use of the computer for other purposes (dependent on type of use) will steal cycles from the CPU and degrade performance of the application. Second, individuals almost certainly want to check e-mail and use the Internet to research topics, which inevitably means Internet network connectivity and network security issues. Finally, in an effort to keep the hard drive sterile, you will want to keep

unrelated information away from your case information.

There are several choices for your forensic tower. Of course, there is the processor speed. It is your choice; however, the time needed to complete a job will correspond to your CPU and RAM. A slow processor can lead to ineffective use of the time spent on accomplishing a task. Depending on the money you want to spend, you might want to consider a dual processor. There is a tremendous amount of flexibility with a dual processor, including using it as a desktop workstation and server.

You will also want to consider purchasing a forensic tower with the ability to add data ports. I prefer using Data Port Vs because they allow you to easily insert a different drive into the tower without removing the case. You can use one data port as the primary drive. By having a different operating system loaded on its own hard drive, you can easily interchange the operating system by interchanging the hard drive. Add another data port (secondary) for hard drives with forensic evidence and you can interchange between cases and operating systems in short order.

There are a number of choices in mobile computers for your forensic fieldwork. The obvious prerequisite is having sufficient processor speed and RAM. Your three most important considerations are the size of unit, hard drive space, and data ports or interfaces. Because you may have to lug the computer with you on a plane, size and weight matter. I have used or seen a number of mobile labs that remind me of a large lunchbox. They have a hard exterior case with one side pulling apart and turning into a keyboard. The monitor is built into the box and, while it is not the highest quality monitor, it is definitely good enough to get the job done. They are lightweight and easily fit into the overhead space on most airlines. I prefer having a large hard drive in the 60 to 80 gigabyte size, which allows for storing multiple images. You will also want to have the flexibility of having data ports, or a data interface as mentioned above, so that you will not need to pull the case off the computer.

SOFTWARE

The next article in this series will cover this topic in greater detail. However, I want to break down the type of software in which you will want to invest. It is important to understand what is needed and the functionality each product offers. The software can be broken down into:

- ☐ 1. imaging
- ☐ 2. analysis
- ☐ 3. conversion
- ☐ 4. viewing
- ☐ 5. monitoring
- ☐ 6. security utilities
- ☐ 7. Over-the-counter software

Let me offer some definitions and describe the functionality to help get a better feel for each product. The next article in this series will address the specific product's functionality, price and user friendliness.

Imaging

An important part of computer forensics is the acquisition and preservation of the evidence. To complete this process, you will need an application that makes an exact copy of the data, or lack of data, in each sector of the targeted hard drive. This will need to be accomplished without changing any of the data. This process is called "making an image" or producing a "mirror image." The image can then be searched for items of interest or restored to another hard drive. The restored image can replace the original drive in the computer and search without the concern of altering the original data.

The software should also include an audit feature to help determine if you have an exact copy. Most software uses a hash-like MD5 to create an

An important part of computer forensics is the acquisition and preservation of the evidence. To complete this process you will need an application that makes an exact copy of the data, or lack of data, in each sector of the targeted hard drive.

algorithm of the evidence. If one bit of evidence is changed, the hash will create a different algorithm. The forensic professional can then compare the original evidence hash to the hash of the evidence copy to determine if they match. If they do not match, you have a problem with your copy and will need to take another image. You need an exact match to ensure that your image is accurate. Matching hashes gives you a very large mathematical probability that your copy is accurate. Depending on the particular hash, the odds can be in the billions- or even trillions-to-one that a match will occur without having an exact match.

Some imaging software can adapt to multiple operating systems, while some are designed for specific operating systems. There are also hardware solutions that image drives and will be addressed in a subsequent article. You will need to do your homework and determine the operating systems with which you will be working.

Analysis

The analysis functionality can mean a variety of things. It can mean conducting document, application, or word searches; file comparisons; matching data from a known document to an unknown document; reviewing deleted data; or comparing source code. I have not found a single piece of software that is able to handle all of these tasks. Some are packaged to provide many of these functionalities and you really need to understand what they are as well as your objectives.

Most applications are operating system specific so you really need to study the operating systems you will be working with the most and the functionality you desire. Because the value of computer forensics is becoming more apparent, there are more products being produced almost on a monthly basis. There are also many talented individuals who write programs to perform specific functions. My one word of caution is that any tool or application that is used should be thoroughly tested and validated before using it on an examination of importance. To use an unproven tool is asking for trouble under cross-examination.

Conversion

During many forensic examinations, I have come across data that cannot be easily analyzed unless it is converted to some other form. This can happen for a number of reasons. Information that was saved with an older version of an application or an application that is no longer available is a good example. In other cases, the data is in a native application that does not lend itself for a particular purpose. I experience this issue when I need to produce e-mail for a particular client that does not have the specific e-mail application. An option I can choose is to convert the e-mail into a different format that the client can view. A second option would be to print every e-mail (this can get ugly!) Even a third option would be to help the client install the e-mail application; however you then would have tech support and user training issues. You can probably think of others but the point is to try to find a clean solution.

Viewing

If your particular examination requires viewing a large number of graphic files or a wide variety of types of files, you will want to acquire a viewer. A graphical viewer can be an excellent way to view 20 or so pictures at a time. Most desktops with Internet connectivity have a large number .jpg and .gif files on them. If you have the task of finding a specific .gif or .jpg file, searching them individually might require a significant amount of time. A document viewer is also a must if you intend to review many different types of files. It can also handle different versions of an application.

Another feature that can be powerful is if you are printing copies of the document, the full path of the document can be printed on the document itself. This is both useful in documenting where the file was found and organizing the data.

Monitoring

Occasionally, the event is still ongoing as you are conducting your examination. You may have the need to collect and review data on a near-real-time basis. There are a number of different tools at your disposal to accomplish this, but you must understand what each will do for you, as well as the implications to your examination. Keystroke capture programs have their place in your toolbox but will require you to place the application on the target computer.

Keystroke capture programs provide the ability to record the activity of the computer that is targeted. The results are saved to a file on the target computer and are either retrieved or e-mailed to you for analysis. If you have valuable evidence on a target computer, placing your application on it may be cause for an allegation that you tampered with the evidence. During such situations, I like to obtain a forensic image of the target computer before using an application like this.

Other monitoring applications that you might consider function like a sniffer. Using these applications on a network provides you with the ability to get near-real-time data on the users or to change your focus to different users when appropriate. Because you are observing network traffic, the risk of modifying or altering the target computer's data is significantly reduced. The shortcoming is that you will not be able to observe the computer activity that is confined to the desktop. Using applications like these requires a good deal of forethought before using them to understand the benefits and disadvantages of their use.

Security Utilities

This is kind of a grab-bag for a forensic professional. You might find everything from password crackers, to encryption, erase utilities, hash sets, and comparison applications. These applications can and do vary by the type of engagement on which you are working. Sometimes, you will need to crack a password-protected file to review the information; thus you want to have the best password crackers possible. Many forensic professionals encrypt their work to protect the case details. This seems like a good idea until the examiner has left his or her position; or worse, the password is forgotten. Don this idea; do yourself a favor and make a conscious decision that is best for you with a contingency plan.

You will probably collect images on a large drive on your desktop or mobile computer. If you do, do not forget that you will need to clean the drive of all previous data as a safety precaution. There are a number of erase utilities that should do the trick. Hash sets can be useful if you are looking for rogue programs and have a good set of hashes from these programs. Comparison applications find their place when comparing the data on different tapes or media. With some DLT tapes in the range of 80 gigabytes, you can use the applications to identify files that have and have not changed between recordings.

Over-the-Counter

If you are going to encounter several different operating systems or applications, it is a good idea to accumulate new and old software — in particular, old software. I have spent many hours trying to find older versions of software that are no longer produced or supported by the manufacturer. This typically happens with mergers, acquisitions, and bankruptcies. Consultants typically are called into various situations and encounter all sorts of software. You might be asked to restore e-mail tapes that are five or

One of the most important resources for your laboratory is to have a good library.

more years old. This task will require restoring the tapes to a rebuilt server with the exact same software and operation system, including the correct version and service packs.

I make a point of saving older versions of software in a library that I might need in the future. If you are going to start your own library, consider saving operating systems, backup software, e-mail, word processing and any proprietary applications. The same may hold true for older equipment. Tape drives, floppy drives, and other storage devices are a few examples of the equipment you might want to save.

REFERENCE MATERIALS

One of the most important resources for your laboratory is to have a good library. The software you collected above will help fill out your library very nicely. You will, however, want to have a good source of reference material at your fingertips when you need answers. You can supplement it in any way that you would like. I would like to suggest a number of books to get you started, including:

☐ *A+ Certification,* Jean Andrews, ISBN 1-57610-241-6
☐ *Upgrading and Repairing PCs,* Scott Mueller, ISBN 0-7897-1903-7
☐ *High Technology Crime*, Kenneth S. Rosenblatt, ISBN 0-9648171-0-1
☐ *Investigating Computer Related Crime*, Peter Stephenson, ISBN 0-8493-2218-9
☐ *Digital Evidence and Computer Crime*, Eoghan Casey, 0-12-162885-X
☐ *Electronic Evidence*, Alan M. Gahtan, ISBN 0-459-27070-2

It probably goes without saying, but try to get the most current edition available as technology changes quickly and the best references are the most current. You should also supplement your library with technical references of the most common applications you will encounter. I also like to include in my library various periodicals covering forensics and computer investigations.

SUMMARY

I hope the information provided in this article gives you a good idea of the type of things that you need to consider when building a computer forensic laboratory. If you anticipate that your work will be very generic, you will probably be able to get by with the minimal amount of equipment and resources. My experience has shown me that you should plan on allotting anywhere from $20,000 to $35,000 in facilities and equipment cost per forensics personnel you hire.

From an ongoing perspective, you should also recognize that you will need to update your equipment, software, and library to include the newest technology. If you are conducting forensics for a particular organization, you will need to understand any technology changes that the organization has embraced. That means migrating to Windows ME or changing e-mail to some other application. Even a change from one operating system on your network to another might cause you to change equipment or even get new training. Thinking ahead helps keep your headaches to a manageable level. To build and keep a top-notch computer forensics laboratory, you will be required to invest time, patience, and money. Good Luck! ■