

Learning the Computer Forensic Way

Kelly J. (KJ) Kuchta, CFE, CPP

The last article was part of the series on building a computer forensics program by identifying what tools a computer forensic professional might use. Of course, having the best tools does not guarantee success or even equate to proficiency. To get to that point, a computer forensics professional needs to have good tools and proper training on how to maximize their use.

How do you find a good computer forensics training program? Well, it is easy if you know where and what to look for. Three years ago your choices would have been very small. Fortunately, today is different because you have a number of choices. You should, however, identify your needs and select the best training program for your particular purpose. This article is going to discuss the different types of training programs available, what will work best for your particular needs, what the components of a computer forensic program include, and who is offering these types of programs.

For the purposes of this article, I am going to discuss computer forensic training programs for desktop computing. Throughout the industry this is generally considered the basics because it is where computer forensics got started. It also provides the fundamentals that advanced or network forensics are based on. The entire content of the rest of this article will focus on the basics of desktop forensics. The advanced forensic training components will be covered in future articles.

There are at least four different kinds of training programs in the area of computer forensics. Some have been around for years. Others are offered to people of similar affiliation and others are in their infancy. Be aware that all training programs are not created equal nor are their objectives the same. The types of computer forensic training programs you are likely to find are for law enforcement only, vendor specific, computer forensic overview, and the hands-on practitioner's computer forensic training.

K.J. KUCHTA is the national director for METASeS Computer Forensic and Litigation Support Service practices in Phoenix, AZ. 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.

I like to think of a computer forensics professional as having three different types of skill sets in one person: part help desk, programmer, and finally, investigator.

TYPES OF TRAINING PROGRAMS

Law Enforcement Only Training

As the label implies, these programs are limited to law enforcement officers. They are very similar to the last type of program we will discuss in this section, i.e., the hands-on practitioners computer forensic class. The most prominent training organization in this area is the International Association of Computer Investigation Specialist (IACIS). Generally speaking, their course is the benchmark against which all other courses are measured.

Other law enforcement agencies both on national and local levels offer courses on a more sporadic basis. These classes not only cover the technical aspects of computer forensics but also are heavy in criminal law issues. A majority of their focus is on investigating child pornography, Internet crimes, and drug cases. Because of this, the methodology taught is very rigid in order to meet the criminal standard of *beyond a reasonable doubt* burden of proof. The criminal standard can be easily applied in the civil arena. Using the civil standard of the burden of proof called *a preponderance of evidence*, however, does not lend itself to be used in a criminal court. I always like to use the higher standard as it can be used in both the criminal and civil environments.

If you are one of the fortunate ones who get an opportunity to go to these training courses, go! The military and law enforcement communities are where computer forensics first got its start. There are good courses in the private sector; however, the wealth of experience that can be gained by attending the law enforcement only courses is phenomenal.

Vendor Specific Training

These courses are offered by vendors who have computer forensic tools for sale. These types of courses are generally very good about covering the features that make their tools powerful. For obvious reasons, they do not like to cover the weaknesses or inadequacies of their product. If you were going to use a particular tool a majority of the time, I would highly recommend using a vendor's training program. The vendor should know how to use its tools better than most users, though that is not always the case. Another benefit of attending the vendor's training classes is that you get a chance to develop a rapport with a trainer who is also an agent of the vendor.

These individuals can be extremely helpful by resolving any challenges you might face as well as soliciting your feedback on future product enhancements. As a point of clarification, vendor-specific courses are composed of a large amount of hands-on training, which should not be confused with the hands-on practitioner's training courses given by service providers.

What you do not get, however, is a training course that covers all of the forensic principles, methodology, and procedures used by a forensic professional along with an overview of other potential products. These items give the forensic professional a broad base of knowledge and understanding as to what is happening behind the surface. Being knowledgeable about all of the aspects of computer forensics is what makes the professional an expert or journeyman.

If you recall, I discussed this topic in the last article of this series. Many of the professionals see those who know just how to point and click on one par-

ticular product as a liability to the profession and call them "wannabees." These wannabees cannot explain what is happening in the background of the application and often consider its operation as somewhere along the lines of magic. Most argue that point-and-click applications are not inherently bad, but their use can let the professional become dull and uninformed, thus giving point-and-click applications the appearance of performing magic. My word of caution is to take advantage of vendor training but do not let it be your only source of training.

Computer Forensic Overview Training

These types of training classes will go heavy on the academic theory of computer forensics. There are a number of these courses offered to the private sector mostly by professional organizations and associations. They can be very useful to managers of information security departments by giving them an overview of the capabilities of computer forensics. Attendees at these courses will generally not receive any hands-on training of computer forensics tools.

You should not expect to attend one of these courses and become a computer forensic expert. These courses are usually two to three days in duration, which is really only enough time to summarize the theory and not practice technique. I also find that these courses are good for people considering participating in the forensic area and other individuals who might have to work with computer forensic professionals. I would include computer emergency response teams (CERT) in this category. Some service providers will actually bring this type of training program to the client and its CERT.

Practitioner Hands-On Training

These training courses are geared toward the computer forensic practi-

tioner. The duration of most of these courses is five days. Expect to get a detailed lesson plan on the computer forensics methodology, principle, and process. These types of training classes may have upwards of 50 percent hands-on exercises. If you aspire to be a professional who can roll up your sleeves and perform computer forensic tasks, these types of programs are for you.

Your training courses may even require you to be A+ certified or require that you read a substantial amount of information prior to attending the course. You may be required to demonstrate an understanding of MS-DOS, understand how computers work, and have an appetite for technical information.

I like to think of a computer forensics professional as having three different types of skill sets in one person: part help desk, programmer, and finally, investigator. The most important characteristic as an investigator is to have a natural curiosity in wanting to understand why something happened the way it turned out.

IDENTIFYING YOUR NEEDS

Before selecting a training course, which may or may not meet your expectations, consider the role that you will have during the process where computer forensics is in use and what objectives you have. Ask questions such as: Are you managing a computer forensics unit or actually performing the actual tasks? If you have dedicated resources available to perform the tasks, are they using a specific forensic tool for a majority of their work? If you manage a forensic unit or individual, are these persons experienced computer forensic professionals?

By answering these questions, you can begin to select the best training program for your needs. You should also determine what objectives you and your organization are trying to

meet. Because you must be a sworn law enforcement officer to attend the law enforcement training courses, I will not discuss using this option except to say if you want hands-on training and get a chance to attend a law enforcement only course — do.

If your organization is going to make a serious investment in bringing a computer forensic capability in-house, you need to understand the basics to manage it properly. As a manager of the unit, you should attend the computer forensic overview courses to understand the general process and requirements needed to build a first class computer forensic unit. If you are someone who will be expected to perform the actual examination, you should consider either the practitioner's or vendor-specific training courses.

If your organization is considering using a service provider to perform your computer forensic service work, I would highly recommend attending the computer forensic overview courses. It is very important to understand what you are managing. A number of service providers in the computer forensic area prefer to have clients who are in the dark about what they do out of fear that the client might not need their service anymore. While there is a small grain of truth to this, I prefer to have a client that is knowledgeable about the process and can be specific about objectives. Having a good understanding might intimidate some service providers, but it is the best way for the client to receive the maximum value for the money. It helps the client take a more active role in the process that others are providing.

On a final note on this topic, if you have the training resources, I recommend that any new person who is interested in computer forensics start with the practitioner's training, rather than the vendor-specific courses.

Most practitioner training courses will give you some general training about the forensic tools they use. Chances are that these tools are the same ones that your vendor-specific training programs offer. This can and should be followed up by the vendor-specific courses. I like this format because you have a general foundation to build your knowledge on and then you know where you need instruction. Most people I talk to who follow this progression of courses find that it provides a much more enriching experience. If you cannot attend both, you are best served by taking the practitioner's course because the broader base of knowledge prepares you for more a diverse set of circumstances.

COMPONENTS OF COMPUTER FORENSIC TRAINING PROGRAMS

As I mentioned, all computer forensic courses are not created equal. I am not going to cover what component should be in the law enforcement only and vendor-specific training courses because the content and components are dictated by such things as legal issues or the capabilities of the specific forensic tool. I do want to cover the components of the computer forensic overview and practitioner's training courses.

The major differences between the two courses will be in the area of receiving hands-on experience and the depth and time devoted to covering the course material. As you can imagine, academic theory is often very different from real world experiences. My previous article talked about packing a bag for Murphy and the impact of Murphy's law on computer forensics. This is truly where the rubber meets the road. Experience can and does overcome a vast majority of these problems.

I see a number of so-called computer forensic practitioners who can talk the talk but the minute they need to walk, they fall. Practice using your

tools, understanding your methodologies, and following your procedures. This is the only sure way of becoming experienced in this discipline. Make sure that you understand the differences and do not get caught in a trap of overpromising and underdelivering.

What should you be looking for in a computer forensic overview or practitioners training program? There are eight areas that I look for in computer forensic training programs. They are:

1. Introduction to computer forensics
2. Computer hardware
3. Operating systems and files structures
4. Preserving digital evidence
5. Making forensic grade images
6. Examination Techniques
7. Legal Issues
8. Networking Basics

In the introduction to computer forensics section, I expect to see an overview of the components in the rest of the training course so that the attendees have a general idea of what they are going to learn, what tasks they can reasonably be expected to perform, and what is not going to be covered. This section should include the history of computer forensics, methodology to be employed, why it is done this way, and finally, a glimpse at the future and the problems you are likely to encounter.

The computer hardware section should require the trainees to understand why the computer works the way it does. You should be able to identify each component of the computer, what it does, and how it works with the other components. Troubleshooting is also high on this list because sometimes the professional inherits a computer that is on its deathbed, or the examination requires the professional to disassemble the computer. You will need to return the computer to the condition in which it

was found, so this is a crucial area of your training. This section should also cover the drivers needed to use the computer, disk structure, and the Power on Self Test, or P.O.S.T., process.

The file structure of operating systems is also a very important section because it will help the practitioner understand how information is saved to the hard disk and how it is used in computer forensics. I like to see the following operating systems covered: MS-DOS, Windows 9X, Windows NT, and Windows 2000. This can also be expanded to cover Linux and Macintosh operating systems. The issue with covering these two operating systems is that they are diverse (especially Macintosh) enough to require additional time and different tools. Most training courses do not cover these because of the lack of time in the training course and these operating systems are not yet commonly found in the field. This section should also address deleted files, file slack, swap files, temporary files, and any other operating system's specific file structure issues.

The preserving digital evidence section should teach the trainee about collecting electronic evidence without tampering with it. A key component of computer forensics is that the evidence is never altered by our methodology or process. In order to prevent this from happening, the target hard drive must not be allowed to be written to. Depending on the procedure used, it might include using a boot disk or even placing the hard disk on the bus of a forensic computer as the slave drive. This section will be one that you will want to pay close attention to.

The section on making a forensic grade image will give the attendees the information they need to complete the last step of electronic evidence collection. You should expect to see

what happens during the imaging process, why it needs to be completed that way and some common problems that might be encountered. It should also introduce and demonstrate the different tools that are used to image electronic media. Some of these tools are software or hardware based. The process should also cover the differences and issues associated with taking the image in a controlled environment such as a lab or in the field. I would also like to see the issue of hard disk sanitation addressed along with the other topics associated with this issue. With the knowledge of computer forensics, the professional should not be ignorant about contamination of information from one case to another. This subject should address this issue.

The next section on examination techniques should cover the tools used to conduct a forensic examination and techniques used to maximize their usage. This should include how to search for specific information, capture and convert information to a usable format, record and document the forensic process used for reporting, and even how to crack passwords. Because these courses are not vendor specific, I would expect to get an overview of a number of tools in a best of breed format. Part of this section should at the very least give the attendees a good overview of the forensics tools demonstrated in the course. This provides you with a chance to use each tool before making a decision about buying one versus the other.

No training course should be considered complete without addressing the legal issues that impact computer forensics and technology in particular. Look for information about the difference between criminal versus civil law, privacy issues, attorney-client privilege, spoliation of evidence, what is expected of an expert

witness, law enforcement liaison and Title 3 issues or, more specifically, wiretap violations. These are all things that a computer forensic professional should know and understand in order to stay on the right side of things.

The final area that I recommend receiving training in is networks. With the push into distributed computing and away from individual computers, it becomes paramount for the computer forensic professional to keep updated on the knowledge of networks. I would look for an IP review, introduction to protocols, forensics in a distribute system and network, or advanced forensics. The important point here is that if you decide to get into the computer forensic area, you should be prepared to be constantly pushed by both man and technology.

For those of you who will take practitioner's training courses, look for goal-based training in which hands-on exercises build on one another. The final exercise should make you put it all together just as if it were a real-life computer forensic experience. Prepare to be challenged in these types of courses so that the training will stick with you. Any instructors who cannot develop training courses that will not make you use what you have learned will doom you and your company to wasting a large amount of time and money.

FINDING YOUR COMPUTER FORENSICS ZEN MASTER

Now that you know what to look for, where do you find it? I have put together a list of potential resources that offer training courses that might fit your needs. The organizations I have listed below are believed to be reputable, but I would strongly recommend that you ask for references, especially if it is an organization that you are not personally familiar with. I will break the organizations out just

as I discussed them above. Some of the organizations offer different types of training and have even tried to make the course a hybrid of two or more areas. By the same token, they may have a different type of course for each area.

- Law enforcement only
 - International Association of Computer Investigative Specialist (IACIS): <http://www.cops.org>
- Vendor specific
 - Vogon Data Recovery and Forensic Computing: <http://www.vogon.co.uk/fc-o2.htm>
 - Mares and Company, LLC: http://www.dmares.com/maresware/TRAINING/training_basic.htm
 - Guidance Software Inc: <http://www.guidancesoftware.com/training/fst.htm>
 - AccessData Corporation: <http://www.accessdata.com/training.htm>
- Computer forensic overview
 - SANS: <http://www.sans.org/newlook/home.htm>
 - Computer Security Institute (CSI): <http://www.gocsi.com>
 - METASes: <http://www.metases.com>
- Practitioner's training
 - Computer Security Institute (CSI): <http://www.gocsi.com>

- High Tech Crime Network (HTCN): <http://www.cftco.com>
- CyberEvidence, Inc: <http://www.cybercrime.com/services.htm>
- Fiderus Institute: <http://www.fiderus.com/resources/press/training.asp>
- METASes: <http://www.metases.com>
- High Technology Crime Investigation Association (HTCIA) — Note these training classes are presented in a piecemeal approach. <http://htcia.org/>

The following are some important questions to ask when considering subscribing to a computer forensic training program:

- Is the course offered only at the host site or can it be brought to a client site?
- Is the software included in the price or do you only get freeware or a demo copy?
- Is there a limit to the size of the class?
- How many instructors will be teaching the class?

Feel free to ask as many questions as you must to determine whether the course is for you. After all, if your questions cannot or will not be answered prior to the class, what makes you think your questions will be answered during the training? ■