

# Computer Forensics Today

*Kelly J. (KJ) Kuchta*

**W**hen people hear the word “forensics,” it often generates a mental image of the movie series with Jack Klugman as a medical examiner named Quincy. The fact is that there are as many as 25 separate forensic disciplines. They run from forensic accounting to forensic medicine and forensic pathology. The word *forensics* literally means “a science that deals with the relation and application of a particular field.” Computer forensics is the science that is concerned with the relation and application of computers and legal issues. The proliferation of the computer in society today has pushed the computer forensics discipline to the forefront of business.

Computer forensics has recently made its presence felt in the business community. Litigation such as the recent antitrust cases including Microsoft and others has made companies realize that the risk associated with computer networks is substantially greater than they first realized. Information is captured in vivid details, and many of these details are things that some would prefer never to be known.

This, however, is also a two-edged sword, given that these details can be useful when captured for demonstrating what happened during certain events. The computer forensic professional is a cross between technician, programmer, and investigator — a curiosity-oriented person who likes determining why and how past events have occurred.

The value that computer forensics delivers is applicable in a number of situations in business. First and foremost, computer forensics tools and methodology are instrumental during a computer incident, whether it be the identification of an intruder on an organization’s network or gaining insight into events such as theft of intellectual property or criminal matters.

The legal community is not far behind businesses in realizing the value of computer forensics. Computer forensics is used to uncover the proverbial “smoking gun” and to organize voluminous amounts of data. E-mail has proved to be an inviting target, because people often say things in e-mail without realizing that their words stay around for a long time. Discovery

---

*K. J. KUCHTA is a senior manager for Ernst & Young’s National Information Systems Assurance & Advisory Services in the area of Computer Forensics. He is a Certified Protection Professional (CPP) and a Certified Fraud Examiner (CFE) with over 13 years of experience in investigating frauds in the areas of banking, financial services, and insurance. He has conducted or managed in excess of 65,000 investigations in his career, many of them involving computers.*

*Not only is technology changing, but so are the users, who have become more sophisticated in their ability to cover their tracks.*

motions in the past asked for paper. What is found on paper today? Not much; the really juicy stuff is in e-mail and files that have been modified. Attorneys now routinely ask for electronic copies of e-mail systems. (The value of this request is explained subsequently in this article.)

Because they understand the implications of e-mail and altered files, computer forensic professionals are asked to help address these issues. They occur by making process improvement changes that reduce the risk of incidental release of unwanted information and capture information that would be useful to an investigation. These situations have brought computer forensics from its past to its present position today.

#### **BACKGROUND OF COMPUTER FORENSICS**

The roots of computer forensics can be traced back to the law enforcement and military communities who were faced with investigating incidents and crimes on computers. An effort was made to understand how the computer worked and whether there were opportunities to exploit its configuration. Significantly, this initiative was born out of the fact that computers were being used to commit crimes more and more. Advances in technology are still driving new forensics tools and methodology. Both private companies and government security agencies are striving to perfect computer forensics tools. Technology that can read layers of data on a hard drive that has been written over many times is just one example. Of course, new operating systems and applications require computer forensics professionals to be on top of their game in understanding new products.

Many of the subject matter experts today were part of the development of yes-

teryear and they agree that things are moving at a much faster rate today than during previous periods. Not only is technology changing, but so are the users, who have become more sophisticated in their ability to cover their tracks. Software and advice on how to defeat computer forensics contain a mixture of fact and fiction. Because of this, computer forensic professionals worth their salt will always test applications and techniques to confirm results.

Training courses for computer forensics professionals have typically been limited to law enforcement agencies. This is changing, because a number of companies are offering computer forensics training along with their forensic tools. The tool sets can be as basic as batch files in DOS or a MS-Windows application. The interest shown by the business community has helped make the market for forensic training and tools lucrative and results in a wider range of choices in computer forensics tools. Unfortunately, these choices are not limitless. A certain amount of research is needed to determine the tools that are right for each situation. Just as all computer equipment is not created equal, not all forensic applications are created equally.

#### **WHAT IS COMPUTER FORENSICS?**

Many readers may already have some idea of what computer forensics is. The main objectives of computer forensics professionals are to preserve, collect, and analyze evidence found on computers in order to determine the facts in question. They must also provide credible and reliable expert testimony in court if necessary. Although this sounds very straightforward, it is no small task. The discussion now addresses the different aspects of this challenge. Readers should keep in mind that this is a high-level discussion and overview. A computer forensics examination

covers a lot of ground so, keeping written documentation that is informative, organized, and accurate is paramount to the success of the case.

### **Legal**

The legal level is the most stringent level that any forensic examination will have to endure. It is important to understand the legal concepts that will impact the ultimate outcome. The object is to preserve, collect, and analyze evidence that might be used in civil or criminal court. A good computer forensics professional will work as if the case might go to the highest level, criminal court. The reason for this is that the burden of proof is greatest in this arena. In criminal court, the case must be proved “beyond a reasonable doubt,” whereas civil court requires only a “preponderance of evidence.” In essence, criminal court requires proving things with a 99 percent degree of certainty, and civil court requires proving things with 51 percent degree of certainty. If work is prepared to the standard of 51 percent it is almost impossible to later present the same work product with the higher degree of certainty. When computer forensics professionals start working, it is unclear what burden of proof will be required, so they must use the standard for the highest level to keep all options open.

A brief discussion of preservation and admissibility is appropriate here. The courts have given four guidelines that should be addressed in order to introduce computer evidence. Computer records are considered admissible if they are

- produced during the regular course of business
- authentic
- meet the best-evidence rule
- show a chain of custody

All of these standards give the defense a chance to challenge the evidence on the grounds that the guidelines were not followed and the evidence is therefore inadmissible.

The forensic professionals will need to establish that these standards have been met. The courts will accept computer records that have been produced by the business and are thought to be trusted documents. This guideline suggests that the record was made “at or near the time by, or from information transmitted by, a person with knowledge.” This was primarily driven out of the “hearsay rule.” The courts would rather trust business records that a company uses to conduct its business rather than a hearsay account of the evidence. The computer forensics professional needs to demonstrate that the records are authentic and do not contain hearsay statements. This might include using an algorithm to generate a nonduplicable hash on the original evidence. The hash would be modified if the evidence were altered. The hash can later be reviewed to determine whether corruption has occurred.

The court requires that the best evidence be used in court. This means that original evidence is best. However, exceptions are allowed — for example, if the original evidence would be destroyed or altered by using the original evidence, then the next best record is acceptable. As a rule, a computer forensics professional will make a copy of the original evidence, because using the original might alter or destroy evidence.

Finally, the computer forensics professional must be able to demonstrate that the evidence has maintained its integrity through a “chain of custody.” This chain of custody must show that from the time that the evidence was gathered to its present state, it was under the direct control of the appropriate professionals. The computer forensic professional must secure the evidence to prevent intentional and unintentional alteration of the evidence.

### **Technical**

Now that the objective has been determined, the discussion focuses on meeting the legal requirements with technology.

*As a rule, a computer forensics professional will make a copy of the original evidence, because using the original might alter or destroy evidence.*

*If the objective is to recover evidence that is believed to be deleted, then the physical copy works best.*

For this discussion, it is assumed the evidence was found in a desktop computer. Files that are saved to a hard drive are allocated space and cataloged in the directory of the computer. Deleting files merely removes the file from the directory list but leaves the file intact on the hard drive until it is written over. By knowing how the operating system works, the computer forensics professional can capture information that was thought to be vanished or nonexistent.

Most operating systems are configured to start writing to various log and application files when initiated. Shortly after the operating system is launched on the hard drive of the computer, it will change a large number of files, including log and temp files. The measure of authenticity will seriously be in question by allowing the operating system to boot to the hard drive. The remedy is to boot the computer from a controlled situation (e.g., a boot disk). Any application or executable that writes to the hard drive must to be eliminated. Now that the evidence has been preserved, it must be accessed.

The computer forensics professional will make an image or copy of the drive. There are two options as to what will be imaged — logical or physical drives. It depends on what the objective is, but a logical copy will work well if the investigator is trying to organize information and believes that the information has not been altered. If the objective is to recover evidence that is believed to be deleted, then the physical copy works best. The physical image will capture all data found on the drive including deleted files, temp files, and slack space.

There are three options for creating an image of a drive: use the parallel port, insert a SCSI card, or image drive to drive.

1. Using the parallel port is slow and unstable and is nonobtrusive to the target computer. In situations in which the

computer owner does not consent to having someone touch his or her computer, this option may be best; it averts the claim that the investigator somehow destroyed the computer.

2. SCSI provides speed and accuracy but requires the computer forensics professional to insert the card and change the connections on the bus.
3. Imaging drive to drive is fast, efficient, and very effective when the investigator can pop out a hard drive and insert it on a forensic computer's bus. This also allows the use of write blocking function on the hard drive that contains evidence. The low cost of hard drives makes this an appealing alternative.

Having secured the evidence, it is time to determine facts.

### **Investigation**

The tool set of a computer forensic professional should include indexing software, key word search utilities, general computer utilities such as disk edit or disk probe, data acquisition applications, and even password cracking software. The list is much more detailed, but the picture is clear. The objective is to use tools that give access to the data below the file level. Most tools will let the investigator view the data in a hexadecimal format. Computer forensics professionals generally acquire a larger tool set the longer they have been practicing forensics.

The issue in question dictates the next steps to be taken. If the aim is simply to organize the data from a logical image, then indexing software can be used to sort the information and provide output of files on the image. This is often used in litigation situations in which a lot of data must be reviewed for content. A search of the suspected image for key words can point to files that are of interest and help target efforts.

The physical image is what really provides treasure troves of information. It is possible to collect deleted files, temp files, and information found in slack space. The objective determines where one would start. Obviously, if pornography is a concern, the focus would be on gif, jpg, and other image files. Intellectual property issues would call for reviewing the files in question to determine whether trace evidence is still present or they have been modified in anyway. The real test of a computer forensics professional, however, is placing a particular person at the keyboard at a particular time.

Different operating systems and applications offer unique challenges and sometimes different tools and techniques. Constant development and review are need to ensure that adequate tools are available for each operating system and application that might be encountered.

#### **Human Relations**

This brief section is included to make the point that the output of all of this effort is still communication and human interaction. Not only should computer forensics professionals have an excellent grasp of the legal and technical issue of forensics, but they must be able to convey the concept to individuals do not have this same knowledge level. Often, they need to explain the concepts to a judge, a jury, a general counsel, a CEO, or another non-technical person. Without the ability to convey the basic principles to a nontechnical person, technical acumen does not really matter.

#### **BUSINESSES TODAY**

Interest within the business community in computer forensics is being driven by the CIO and the General Counsel. CIOs are most interested in their incident response capabilities. The computer forensics professionals are asked both to help build the incident response plan and to conduct the actual response. The incident response

issues include theft of information and physical assets, sabotage, business interruptions, and harassment. General counsels are most interested in responding to or creating a discovery motion that asks for electronic information. The discovery motion basically acts as a demand order sanctioned by the court to provide information or data that is applicable to a legal issue. Record retention of e-mail is often a common area of concern as well. Backup tapes with e-mail records dating back five years serve no business purpose but often provide the “smoking gun” to opposing counsel. Understanding how records can be retrieved is instrumental in reducing the risk from unwanted discovery.

#### **FOOD FOR THOUGHT**

Following the high-level overview of computer forensics, the discussion now turns to the issues that will shape the profession in the future. Windows 2000 is one of these issues. A majority of the forensic tools in use were designed work with FAT 16 and 32 file structures, not the NTFS structure found in Windows NT and Windows 2000. The next year will be very revealing as to the direction computer forensics will take five to ten years from now. Changes to both technology and technology providers will cause growing pains for the profession.

More and more corporations are realizing they have a significant amount to lose in this network computing environment. Some will be diligent about evaluating the risk and make changes to prepare for the inevitable day when an event will cause them to focus on computer-based evidence. Others will merrily go on their way until the issue jumps up and grabs them by the throat. The overall situation resembles the opening scene from the sitcom “Quincy,” where most students pass out at the first glimpse of the dead body and only a few remain standing. Managers must decide what will be their company’s reaction? ■