INTERHACK

Interhack
5 E Long St 9th Fl
Columbus, OH 43215

VOX +1 614 545 HACK
FAX +1 614 545 0076
WEB http://web.interhack.com/

Introduction to Forensic Computing

C. Matthew Curtin, CISSP
Interhack Corporation
cmcurtin@interhack.com

Date: 2008-11-18 17:49:45

Abstract

We have experienced a surge in discussion of “computer forensics,” “cyberforensics,” and “forensic computing” in the past few years. Vendors are offering a wide variety of tools that claim “forensic” capability and a tremendous amount of money is being spent on training people to make them “forensic” qualified.

What exactly do these terms mean and what do practitioners need to know about forensic computing to be effective in the audit and control of information systems?

We address these questions and show how competent and experienced forensic computing expertise can support the legal process and how that differs from the black-and-white world of “slam dunk” cases presented in the popular media.

1 Introduction

"Forensics" is the less-formal term for "forensic science." As an adjective, "forensic" means "for use in legal argumentation." Thus, forensic computing or computer forensics is the use of computer science to answer questions that arise in legal proceedings.

It's important to note that imaging computer media, using cryptographic checksums, and so on are not "forensics" without the legal context.

Of course, "computing" is an extremely broad term; within the realm of forensic computing there are many activities. What exactly an investigator or forensic computer analyst will do depends on the case at hand. Nevertheless, there are a few questions that will arise in every case and that is where the investigation will begin.

Before any legal argument can take place, a set of facts—*what* happened—must be established. Plaintiffs or prosecutors will put forth their allegations; defendants will have an opportunity to counter the allegations. Complaints and responses can be amended, and usually are as proceedings advance. It is not uncommon for each side to have a different set of facts from which the proceedings begin, until there is some agreement between the sides on a subset of facts proffered or until the court accepts some set of facts. In a computing context, this typically means establishing the state of the systems affected.

The next question will often be *who* engaged in whatever action is being debated. Leading to that answer, though, will typically require establishing *how* the action led to the systems getting into the state that they are found.

Investigators do well to remember that it is not their job to argue the case: that's the role of the attorney. Attorneys will develop theories around these fundamental questions that will lead to the conclusion that they want the judicial process to reach. Evidence and testimony will be introduced in order to bring facts before the court. Technical experts may be enlisted to provide opinion about how to interpret certain facts.

Ultimately, a fair judicial process requires that both sides have access to competent legal counsel and that counsel must be supported by competent technical experts.

2 Common Activities

Since the first few questions in the process can be predicted—and indeed there must be some idea about their answers before a suit is filed—there are some common activities that we find in forensic computing.

2.1 Electronic Discovery

By far, the most common issue where law and computer technology overlap is electronic discovery. "Discovery" is a legal process that takes place before trial where someone—usually but not always the opposition—is compelled to produce documentation or facts pertinent to the case.

Traditionally, this has been pretty easy to do for the past few decades. Companies kept most of their records in paper file folders stored in file cabinets. When records came under a discovery order, the firm would simply photocopy all of the pages in a file, review them for privilege, and then send the copies over. Problems with discovery would emerge when people kept their own private files, didn't adhere to the document retention guidelines, and so on. To a large degree, these issues are pretty well understood and have been addressed when it comes to paper files.

The problem is that almost no one keeps all relevant records on paper anymore. What precisely constitutes a "record" is a matter of some debate and is beyond the scope of this discussion, but the important part is that a paralegal can't simply walk over to a file cabinet and start making copies.

How to replace that traditional process with one that will satisfy the requirements of the court without imposing an undue burden on the companies producing the records is a matter being hotly debated in legal circles. Ultimately, either a paralegal or attorney must gain technical training and tools or a technologist with the proper tools must be given the legal process training needed to do the job effectively.

2.2 Data Recovery and Reconstruction

If some of the relevant data have been deleted or the media have been damaged, attorneys will sometimes want to have a technologist reassemble the data. In some cases, this is a very simple matter of reconnecting a name to the data on the filesystem ("undelete"). In other cases, it's a more complicated issue of finding a block or blocks of the filesystem that contain relevant information and putting the pieces back together. Sometimes complete recovery is easily achieved. Other times, no recovery at all is practical.

When the media are physically damaged, data can sometimes be recovered by sending the drive to a clean room facility where the drive case can be opened and special hardware can be used to produce an image of the drive.

2.3 Forensic Analysis

Establishing facts—what data can be found—is a straightforward process. Using readily available forensic tools like The Coroner's Toolkit (TCT), The Sleuth Kit, or EnCase, quite a lot of data can be recovered. When establishing facts, these tools can be very helpful in answering some basic questions of whether something of interest can be found.

After facts have been assembled, however, it might be necessary to enlist a forensic computing consultant to explain to attorneys and the business what the data mean. Such consultants generally work behind the scenes and are not disclosed to opposing counsel. A forensic computing expert is someone who might be called upon to testify about what the data mean and how they should be understood. Such an expert must be so designated by a court and have a pedigree to back up the claim of expertise. Experts are disclosed to opposing counsel and can be grilled by opposing counsel not just on their conclusions but on their qualifications. A training class or certification will not go far in court; while these might help, only someone with years of experience, formal publications, and a long *curriculum vitae* will be admitted as an expert.

3 Limits of Forensic Computing

I'll present three cases from my practice that show some important differences between what happens in real forensic computing and what is shown on television. What these demonstrate is that reality is more murky than fiction and that even if the forensic computing work has been able to establish certain facts, that's only part of a larger puzzle for successful litigation. (Where charges were not filed or minor Defendants were involved, we have eliminated all identifying details.)

3.1 Hands on the Keyboard

"I hope you kissed your kids when you left for work this morning, because you're never going to see them again." So began the email message that came in from a free Web-based email account. Of course the name on the account looked fake and probably was.

After doing some examination of the message headers, we determined that the system that injected the message was actually from the same site as the woman who received the message.

By writing a program to examine the Web browser histories of over 3,000 accounts, we were able to determine which user's account accessed the Web-based email system and sent the message, even finding the proper room and machine.

Police questioned the owner of the account and determined that he didn't know anything about the threat. Additional questioning of the people who were working in the same lab led to the conclusion that the account owner was known for walking away from his terminal without locking it. He was fired for failing to protect his account (in violation of published policy), but no criminal charge was brought forward.

Forensic data analysis correctly identified all of the components of the chain, but without the ability to connect someone's hands to the keyboard, no case could go forward. Had a videocamera been in place, we might have been able to identify a person who was at the machine typing at the time that the message went out and that likely would have led to an entirely different conclusion.

3.2 Specific Intent Required

At the height of the dot-com boom, a company called Pharmatrak was established to provide Web site usage statistics for pharmaceutical companies. In addition to getting detailed reports on their own sites, clients agreed to participate in the program that allowed their highest-level (least-detailed) reports to be shared with the rest of the Pharmatrak client base. Thus, if one client saw that it had one million visitors one month, it would be able to see not only whether that was better or worse than some other period of time, but how that compared with the sites for other companies in the pharmaceutical industry.

The system worked through a combination of technologies such as Web bugs and JavaScript in order to tag the visitor with a unique identifier and to report which page the user was viewing on the pharmaceutical client Web site. Believing this activity to be in violation of the published privacy policies, a number of Plaintiffs sued the pharmaceutical companies and Pharmatrak. We were then retained by Plaintiffs' counsel.

Our analysis of Pharmatrak's data showed that they did, contrary to representations made in the legal proceedings (and to clients before the litigation), collect very detailed information on several hundred people. (We found no evidence whatsoever that Pharmatrak actually used the information, sold it, or even knew that they had it.) After examination of the technology and discussing the mechanism used for the collection, I opined that Pharmatrak's technology was "intercepting" the "content" of a communication that both the pharmaceutical company and the user visiting the Web site believed to be private, explaining the interception mechanism in great detail. The U.S. Court of Appeals for the First Circuit held that this was true and that the system therefore violated the Electronic Communications Privacy Act (ECPA) and remanded the case back to district court to answer the question as to whether the "intent" requirement for ECPA violation had been met. See, In re Pharmatrak Privacy Litigation, 329 F.3d 9 (1st Cir. 2003)

Further analysis was conducted to determine whether Pharmatrak intended to collect such information. I showed that the system, by design, collected all information related to the transaction between Web browser and Web server. Whether this would constitute the kind of intent required by ECPA, however, was ultimately a legal question that had to be argued in light of my finding of fact. Defendants prevailed on that issue and the case was dismissed. See, In re Pharmatrak, Inc. Privacy Litigation, 292 F.Supp.2d 263 (D. Mass. 2003). The standing result of this litigation, however, is a strong ruling in favor of privacy, that even URLs—Web addresses—can contain "protected content" under ECPA.

3.3 Electronic Contraband

In early 2005, a state police computer crimes investigator started to crawl peer-to-peer (P2P) networks looking for contraband and specifically child pornography. That investigation led to the location of a system within the state that was distributing files that the investigator alleged were illegal child pornography. A warrant was obtained and the home with the computer was raided in the early hours of the morning; two computers in the home were confiscated as evidence.

Following the investigation, a prosecutor brought charges against a teenage boy in the household—a second-degree felony, two third-degree felonies, a fourth-degree felony, and a first-degree misdemeanor. The defendant proclaimed innocence and was supported by his father, a doctor of medicine. He quickly hired an attorney and then found me; I was thereafter retained in the case.

Prosecutors said that they had the evidence and that it was clear. They enlisted experts to testify to various details of the case and tried to convince the defense to plea bargain. Because the defendant was being prosecuted in a juvenile process, he would not have a record visible as he would if he were tried as an adult as long as he stayed out of trouble. The defendant voluntarily submitted to various psychological examinations, the results of which conclusively showed that he was not lying about his knowledge of the facts. Father and son discussed the options with their attorney and father did not want the first lesson of his son's adult life to be that it's best to admit guilt wrongly just to get beyond an obstacle.

I led an investigation to find facts and examine the evidence offered by prosecutors. I shared my findings with defense counsel; once prepared with the understanding of the data and the validity of prosecutors' claims, the defense strategy could be solidified and carried out. Finally I prepared an affidavit for the court, part of the process of expert testimony that ultimately leads to the final hearing in front of the judge (juvenile cases are not handled in jury trials). The tools investigators used showed which files were on the system, when they were created, when they were opened, and other details about them. Nevertheless, investigators (incorrectly, in my opinion) interpreted these facts to build their case. I showed how investigators jumped to conclusions and offered other explanations for the facts on which we agreed.

Having seen the defense that they were going to have to face, prosecutors struck a deal that led to all charges being dropped and the young man's record being expunged of all traces of the matter after he submits a paper to the judge describing how P2P networks operate and how users can protect themselves from being unwitting participants in criminal activity online. He is now in his freshman year at a prestigious university.

4 Building Forensic Computing Capability

Legal proceedings are a part of doing business. Your organization can find itself in contention with a regulatory authority over design and implementation of a technical control for HIPAA, GLBA, or Sarbanes-Oxley compliance; others could bring suit against your organization over the impact of your technology (as happened with Pharmatrak); you might even find yourself in a criminal proceeding (perhaps after being maliciously attacked).

Even if your firm isn't directly targeted by litigation, it's very easy for your firm to find itself on the receiving end of subpoenas and discovery orders. If your organization wants to do business with computers, you're going to need to be able to deal with legal proceedings where computer data are involved. How much of that you handle yourself and how much you rely on outsiders will depend on many factors. In any case, this is not a matter for the IT or the Security department to try to tackle alone. Your firm's General Counsel is the top lawyer in the company; that's where discovery orders and other legal proceedings are handled, so it's important to be sure that any capability in this area is done to satisfy the requirements on the business as determined by your counsel.

4.1 Understand How Law Affects Your Business

Law affects the organization in many ways beyond the questions of an attacker breaking in and stealing information. Be sure that you understand how your organization is covered by various Federal, State, and Local law. Be sure that the needs of your General Counsel are well-defined and that you can begin to create the capabilities needed to address their concerns.

4.2 Identify Frequent Needs

As a general rule, it is most cost-effective to handle routine things with internal staff. Thus, companies that are large enough will have their General Counsel and support staff all aboard as permanent full-time employees. Find the things that are the most common issues and look at your existing capabilities. Is this something that you can handle internally? Is it something you can handle with some additional procedure and training being defined? Is it something that you will need to hire additional staff to cover? Might it make more sense for your staff to have a basic procedure for triage to determine when something crosses a certain threshold of likelihood of turning into a legal proceeding?

4.3 Enlist Outside Support

Whether your organization decides not to handle any of the technology for legal argumentation internally or whether it decides to handle it all, be sure that you enlist good forensic computing experts to support you. Even organizations with extensive in-house legal capability enlist outside law firms to support special projects or to provide them specific expertise for issues that require extra attention.

Remember that technical experts and consultants are not attorneys. The issue of *privilege* is extremely important: if you reveal something to a technical expert, that expert might be compelled to reveal that if questioned. Various states have laws about investigative services, often requiring licenses of private investigators. For all of these reasons, it's generally a bad idea for your IT department or Security department to engage outside forensic computing help directly. Though you might find the firm you ultimately use, let your General Counsel decide how the forensic computing firm should be engaged; it might make the most sense for your firm's outside counsel to engage the forensic computing firm to give you the best protection of privileged information.

A few things to look for when you're looking at a forensic computing firm:

1. Who are the people there? How much experience do they have? No matter what their firm's size or history, what matters on the stand is the person testifying.

2. Does the firm perform the basic technical services, or do they also have experience in forensic computing procedure? Can they consult with your attorneys on formulating their cases?

3. Have your outside experts given testimony in real cases? Have they had to defend their work under cross-examination?

4. How have the courts treated their work? Have opposing experts successfully neutralized their fact-finding and analysis? Have their credentials as experts come under fire by opposing counsel, and how did they fare in the eyes of the court?

5. How long has the practice been around? Will the experts have the operational support needed to manage the case load?

6. Does the firm have experience both in supporting cases being brought and defending cases? Or might opposing counsel be able to argue that the "expert" is an activist instead of a technologist?

5 Conclusion

Forensic computing is a broad term that covers the operation and analysis of your computer systems for use in legal proceedings. Working with the law is a part of doing business, so an organization will need to be able to align its legal and IT capabilities to help the organization to achieve its mission. As important as forensic computing is, ultimately it is in support of a legal process whose result will often depend on questions like "intent" or "reasonable doubt" that cannot be answered technically. With competent and experienced support, your counsel can be sure to provide your organization with the best possible representation no matter where it sits in the legal process.

Matthew Curtin, CISSP is the founder of Interhack Corporation, a Columbus-based information security and forensic computing firm, aiding executives and attorneys facing challenges and opportunities involving the management of information. He and his team provide security assessments and incident response drills, as well as services to work with data in legal proceedings. Their work is used to find the right questions to ask and the best answers science can provide. Matt is also a lecturer at The Ohio State University, in the Department of Computer Science and Engineering. He is the author of *Developing Trust: Online Privacy and Security* (Apress, 2001) and *Brute Force: Cracking the Data Encryption Standard* (Copernicus Books, 2005).