Law Practice Today

Search Go

ABA LAW PRACTICE MANAGEMENT SECTION
MARKETING • MANAGEMENT • TECHNOLOGY • FINANCE

Law Practice TODAY

The Dangers of Do-It-Yourself Computer Forensics

By Eric Shirk
November 2007

As Do-It-Yourself or "DIY" becomes a more common practice at law firms, it is becoming more important to evaluate the risks associated with doing certain things yourself. Eric Shirk examines the dangers of using DIY for computer forensics and suggests alternatives that are safer for your firm.

A Do-It-Yourself, or "DIY," trend has permeated the legal industry when it comes to electronic discovery and litigation consulting services. In an effort to reduce costs, law firms and corporations are building internal teams to rely less on outside vendors, with varying degrees of success. However, certain DIY missions in litigation are fraught with peril and should be carefully examined. Such is the case with computer forensics, the discipline of digital evidence gathering and examination, which often culminates in expert testimony in a court of law.

Computer forensics and the collection of digital evidence is a field with its deepest roots originating in law enforcement. Police and government investigators use various tools and techniques to mine digital evidence, tracking down perpetrators in both criminal and civil matters. With the recent explosion of electronically stored information (ESI) and eDiscovery in litigation, computer forensics is much more widespread now, and the demand for skilled professionals has outpaced the supply. Electronic discovery now appears in most cases, as e-mails have become a main form of communication, and electronic financial transactions and money management are commonplace.

Since computer forensics services are frequently needed by legal counsel as well as corporate information technology (IT) departments, consultants have cropped up to fill the need. Truly qualified providers have the training and experience needed, both from a software proficiency and methodology standpoint. However, as with any burgeoning industry, there is a range of quality among consultants and prospective clients need to understand what they are.

Certain corporations and legal teams are considering a do-it-yourself approach to computer forensics in an effort to save money, mostly, and possibly to retain a feeling of control over the situation by keeping the process in-house. In theory, cost and control are the chief perceived benefits of the DIY computer forensics approach, but the dangers can far outweigh the advantages in such a situation.

Dangers of DIY Digital Evidence Collection

Most qualified eDiscovery project managers and certified computer forensics examiners have witnessed many instances where valuable digital evidence was spoliated during collection, either accidentally or intentionally, by newly-assembled teams of DIY digital evidence "experts." When a computer forensics examiner is brought into a matter where a DIY approach has been used, he/she can generally assume that the IT people have taken a "quick peek" at electronic evidence that will play a foundational role in the matter.

Here's a common scenario that comes up with a do-it-yourself collection done by corporate IT. A financial analyst is suspected or confirmed to have committed a white collar crime like insider trading or options backdating – the company decides to terminate the person. The employee is "let go" at 9am, cleans up his desk with a security guard standing by and is escorted to the human resources (HR) department at 9:05am. His/her computer and PDA are sent to the employer's IT department, ideally accompanied by the security guard to safeguard the chain of custody. Then, the company's IT people boot up the employee's computer and begin to fish around in his e-mail and documents, seeking incriminating evidence. Perhaps they then copy all the relevant items to a thumb drive or CD. After all this has taken place, they send the forensics examiner the equipment or set it aside until that examiner arrives.

Sounds harmless enough, right? Wrong. This is a computer forensics consultant's nightmare, which unfortunately happens in the majority of cases. Many of these actions are tantamount to tampering and have probably significantly damaged the examiner's ability to uncover and testify to the truth.

Common Pitfalls of a DIY Approach

When IT guys take a quick peek, they almost always compromise pristine preservation. Law firms may understand this, but unfortunately corporate IT people usually do not. There are major risks involved with the do-it-yourself approach, so consider whether it's worth possibly jeopardizing your potential evidence in the name of the cost and control issues described above.

- **DIY Pitfall #1 - Weak or Nonexistent Chain of Custody**
  IT people and other non-experienced digital evidence professionals are generally not sensitized to maintaining chain of custody for all potential evidence. Chain of custody entails logging all items and tracking their whereabouts from the time they are found or seized up through the trial. The data needs to be preserved and accounted for, every step of the way.

  If "self-collection" or DIY collection has been done, the forensics examiner can immediately expect weakness in preservation of the data. Often the chain of custody is poorly done or simply nonexistent.

- **DIY Pitfall #2 - Spoliation and Tampering**
  Booting up a PC immediately spoliates data and exposes the case to allegations of data tampering. When IT starts up and searches a computer, important file metadata and operating system artifacts are automatically updated. In these circumstances, the client can be subject to allegations of purposeful tampering, but regardless, there is a solid case for unintentional tampering. This creates a "case within a case" – a complication that the legal team will have to fight its way out of, and one that can be costly to the case in terms of time, money, legal sanctions, or all three.

  Spoliation of electronic evidence can have effects ranging from damaging the corporation or firm's reputation, to procedural and/or financial sanctions by a court of law, to default judgments. Consider the IT collection and "quick peek" investigation scenario given above. The incriminating transactions and communications would likely have resided on the financial analyst's computer. The truth lies in the cryptic strings of zeroes and ones that make up the binary code, so if that data has been compromised, the whole case could now be in jeopardy, no matter how deserving the plaintiff may be.

- **DIY Pitfall #3 – Careless Lawyer Mistakes**
  Corporate IT people are not the only ones guilty of carelessness in data collection. The lawyers get into the game here as well. Astonishingly, attorneys sometimes ask users to do their own self-collection. They ask the custodians to decide which e-mails or documents are relevant to forward to them. If you are a white collar criminal, would you knowingly forward incriminating material about yourself to the lawyer? Best practice would dictate that a consistent unbiased collection approach be implemented across all relevant custodians, versus the subjective pick-and-choose method described above.

- **DIY Pitfall #4 – Overlooked Data**
  The DIY approach, whether it's done by an attorney or an IT person, typically overlooks less-than-obvious but still relevant data sources so important evidence can be missed.

Some of these secondary data sources include USB thumb and external drives, personal and department network drives, PDAs and the instant messaging (IM) housed within, as well as back-up CDs and DVDs.

Often in DIY collection there are other critical steps missing, such as photographic documentation. Photographic documentation is a necessary procedure – you are documenting a potential crime scene, after all.

Photographic documentation works as follows: HR will generally notify a forensic examiner in advance of firing someone. The computer forensics examiner will go to the person's desk with the security guard at 9am and be present when the employee cleans out the desk. Then, before anything is touched, photographs are taken of the desk and surrounding papers, documents, and post-its-- including sticky notes bearing all-important passwords-- which will be useful later in the investigation. Serial number labels on the computer, the face of the PC, and the sides of the computer are photographed so that all the USB ports, modems, NIC cards, etc. can be noted. The forensics professional documents every way that data could have gotten in or out of the computer. In doing this careful documentation, the forensic examiner is building a defense to erroneous claims from the other side.

Professional procedures like photographic documentation are incredibly important, especially in smaller matters where a laptop or PC could be the entire crux of the case. If the machine disappears or is altered in such a case, it could trigger crippling sanctions.

- **DIY Pitfall #5 – Inferior Tools, Methods and Training**
  IT staffers often use flawed approaches, like searching in native or Windows applications like Outlook and Adobe. These search methods are often ineffective because they miss important evidence like attachments to e-mails and text within non-searchable PDFs. Frequently, IT people also use tools like Norton Ghost or NT Backup for collection instead of validated forensic tools like EnCase or Forensic Toolkit (FTK). These IT tools are rarely tested and validated for litigation purposes.

  Corporations and law firms must ensure that the people doing the work are properly trained, certified and equipped. Proper training for collection and analysis includes both tool-specific and non-tool certifications.

- **DIY Pitfall #6 – Inherent Bias**
  When looking for an expert witness to testify about authenticity of electronic evidence, clients and counsel need to engage the least possible bias. Expert witness testimony is often disqualifiable if there is even a hint of bias or conflict-of-interest.

  It is a legitimate concern that digital evidence examiners will be not be able to render an

unbiased opinion if they have a vested interest in keeping an employer happy or out of trouble. Internal IT people want to preserve their jobs and their companies, so entrusting them with collecting and analyzing electronic evidence for their own employer's litigation is flawed logic. Hiring an objective, uninterested third party, such as a computer forensics examiner, largely eliminates the chance of inherent bias and conflict of interest, provided that the expert has an impeccable track record in previous litigations.

As mentioned before, expert testimony is a common end-result of a digital forensics examination. Therefore, law firms generally cannot perform this work themselves because of their conflict of interest. Law firms can collect, analyze and cull ESI, but, generally speaking, they don't (and shouldn't) consider doing their own forensic investigations.

Two Realistic Solutions – Hire Experts or Build Out Internal Resources

Basically, corporations and legal teams have two main options when faced with the need for digital evidence collection and examination. One is to hire a reputable computer forensics examiner to handle the collection, preservation and examination of electronic evidence on an as-needed basis.

The other option is to build out the capability internally by hiring a staff of experienced forensics professionals, or by repurposing IT and legal professionals that want to cross over to forensics. If appropriate, the forensics professionals can oversee creation and practices of some of these in-house resources.

Lately, a few corporations have considered doing their own computer forensics investigations, but this is very rare. One of the main deterrents to building an in-house computer forensics capability is cost. To do it right, a corporation would need to spend about $125-$250K to set up a robust computer forensics lab. Add to that the annual cost of training personnel and labor cost for qualified investigators. Most firms and corporations simply don't have enough case volume to justify such expenses.

Some companies that do decide to build versus buy send one or two IT staffers to EnCase training and then claim to have an internal computer forensics resource. Training on one software tool is only scratching the surface of competency. If the volume of litigation is sporadic, or if the resource gets pulled back into his/her legacy IT role, the person's skills quickly become rusty and ineffective. Some companies may opt to have a firm experienced in digital evidence seed their team with experienced forensic examiners and supervise them as necessary, which has proven to be very successful.

To DIY or Not DIY

In the final analysis, your firm or corporation will need to decide what to do in-house and what to outsource to qualified professionals. Preserving reputation is always important. Cutting cost is

always a major priority. However, considering the repercussions of a botched computer forensics collection or investigation is the most important factor of all.

The old adage “you get what you pay for” is certainly true for the majority of situations with computer forensics. Do-it-yourself strategies can work under the right circumstances in collection, but hiring the professionals when necessary, especially for the analysis phase, shows good judgment and smart thinking. Hiring a qualified computer forensics examiner can help you avert disaster and prevent embarrassing or catastrophic situations where the case or your reputation can be damaged or destroyed. If your corporation or legal team is going to do computer forensics yourself, be prepared to navigate dangerous territory and to invest in expert help when you need it.

About the Author

Eric Shirk is a Technical Consultant and Senior Manager with UHY Advisors FLVS, Inc. in the eDiscovery Practice Group. He is a seasoned technologist who holds certifications in computer forensics and has served as an eDiscovery project manager for a global Fortune 10 organization. In addition to his litigation support experience, Eric benefits from having over a decade of experience in the information technology field.