

LEGAL TECH

The Legal Strategy of Computer Forensics

By Tino Kyprianou

As technology advances by leaps and bounds, digital devices are now an integral part of our lives. Every day we use cell phones, laptops, iPads, iPods, GPS systems — the list is endless. A large part of our activities and transactions are captured on these devices or on a network server somewhere. So what happens when an individual or organization is accused of wrongdoing or winds up in a legal dispute? For the legal process to be thorough, comprehensive and equitable, electronic evidence inevitably becomes a part of the discovery process.

So what's an attorney to do? The technologies involved are so numerous, complex and ever evolving, the existence or location of the evidence is not so obvious, the client is not knowledgeable of the consequences of using technology and the adversary is more resourceful and well-versed in the complexities of digital devices and e-discovery.

Based on my experience as a computer forensics examiner, below are some areas where collaboration between an attorney and an examiner proved to be invaluable.

Do you trust your adversary to provide you with all the electronic evi-

dence relevant to the case? In the normal course of litigation, attorneys exchange documents that are relevant to the case. However, how can an attorney be sure that all relevant documents have been produced? Can you leave it to the opposing attorney to search deep and wide for the existence of relevant documents? How would you know if documents exist but are left out because the opposing attorney is not technologically savvy to guide his client to produce all available evidence, including those in digital devices? In several of our cases, fragments of deleted files found on a computer after a forensic analysis proved to be pivotal to a case and the parties quickly settled in order to avoid further embarrassment. In other cases, having examined the opposing side's computers, we produced thousands of relevant e-mails that caused them to settle to avoid a time-consuming and expensive review process.

Your adversary has a court order to produce your client's computer — do you know what's in it? It's fairly common that a law enforcement agency or your adversary is successful in getting a court order to examine your client's computers or other electronic devices. It would be prudent, therefore, for an attorney to anticipate the possibility of a court order

and pre-emptively find out what's on the digital devices so she can have all the information at her disposal to intelligently determine the best legal strategy for her client.

Is there a chance that your client forgot to tell you about files she deleted? It's often possible for clients to forget details of their actions that happened two or three years ago. You ask all the relevant questions and you are confident that all facts are known to you. During discovery, the other side asks for a forensic examination of your client's hard drive. You confidently agree, knowing that there is nothing incriminating to your client. The opposing side, having examined the computer, finds that some files containing important evidence have been deleted. Your client could have been genuine in her forgetfulness but can you take the chance? It would therefore be prudent to review the hard drive before it's turned over or, having examined it, decide not to produce it without a court order.

Do you have all the devices that might contain discoverable data? Attorneys are not always up to date with new technologies nor are they fully cognizant of how companies and individuals store or back up electronically stored information; after all, they are not technologists but law practitioners. The labyrinth of compliance issues covering different industries can also complicate matters even further. Data now can reside not only on PCs, laptops, flash drives,

Kyprianou is president of Axiana LLC in Morristown (www.axiana.com), which specializes in computer forensics and e-discovery. He is a certified examiner and a member of the International Society of Forensic Computer Examiners and the Association of Certified Fraud Examiners.

cellphones, corporate networks/servers and back-up tapes but also on GPSs, the cloud, social networking sites, virtual machines, ISP providers, cameras, iPads, iPods, smartphones, digital copiers, swipe cards and more. A computer forensics consultant will act as the attorney's own technologist in identifying where digital data may reside and take the necessary steps to recover it or advise in sending the opposing attorney a request for documents from specific devices.

Discovery and document production don't always reveal all the evidence — you might need to explore deeper. Discovery and production of documents deal with documents that are available for production. Sometimes, however, more important are the actions of the computer user; what he did and didn't do. Artifacts found in the computer's registry, applications logs, Internet browsing, recently accessed files, software used, unallocated space, just to name a few, can be extremely important to a case. A computer forensics expert can analyze all these important system files to find if and when a USB device was plugged in, files copied to external devices, the user's log on/off times, the system's last shutdown, whether the system's date and time have been manipulated, the user's Internet usage, hidden and encrypted files and much more. Furthermore, what attorneys don't know can handicap and hinder them in getting the best results for their clients. In many of our cases, col-

laboration between an attorney and a computer consultant resulted in refocusing a case to areas not previously considered, and subsequent computer examinations uncovered information that completely changed the outcome of a case.

Protect the integrity of the evidence and maintain proper and defensible chain of custody. The protection of the integrity of the evidence and a defensible chain of custody are of paramount importance to every case. This necessitates proper training and experience. IT employees, computer technicians and computer shops by and large are not trained to properly handle evidence or follow methodologies in the collection of evidence that can withstand legal challenge. The attorney's responsibility is to ensure that the evidence is adequately protected, all evidence collection protocols have been followed and no spoliation or evidence tampering has occurred.

Design an effective keyword search and defensible search methodology. In my experience, keyword selection and design is one of the least understood areas. Attorneys understand what a keyword is but unfortunately not much thought is given to the possible effects on e-discovery. In order to be thorough and all-encompassing, an attorney will use as many keywords as possible in different combinations and variations. Poorly designed keyword searches, however, can result in hundreds of thousands or even millions of worthless hits that are very costly and time consuming to sort through.

One must also consider whether the search will include the free space of the computer, the handling of non-searchable documents (fax images, zip archives, etc.) and generally the search methodology to be followed. These can become a point of contention between attorneys and, absent an agreement, can result in legal challenges.

Engage an expert witness. A computer forensics consultant, by virtue of his knowledge, training and experience, might be called to testify in court. It would therefore be advantageous for the attorney to retain the services of a competent computer forensics expert who will not only uncover the relevant electronic evidence, but who also has the ability to write comprehensive, intelligible reports on his findings and defend and explain those findings in court.

File effective court certifications. In many cases, an attorney is required to file a certification to compel a computer inspection in response to the other party's refusal to produce electronically stored information. The knowledge and expertise of a computer forensics consultant will be helpful in drafting a meaningful and defensible certification, thus increasing the chances of success. Working closely with the attorney, the consultant will offer guidance and advice as to the best way to approach the unique technical challenges of each case, while at the same time presenting all the relevant facts with sufficient clarity to help the judge make an informed decision. ■