

Expert Advice on the Forensic Computer Scientist

The workhorses of the 21st Century are electronic. From the small office to the multinational corporation, “computers” have constantly increasing functionality. They have replaced the legal pad, typewriter, desk calculator, checkbook, drafting table, mailbox, fax machine, camera, slide projector, traditional phone and more. A machine the

size of a suitcase can now electronically house a warehouse full of paper documents. We are inundated with digital data. Our lifestyles constantly create it. Communications that were once relegated to paper or voice, flow efficiently around work and personal environments electronically. This digital data can be used both offensively and defensively in litigation. Enlisting the aid of an expert in forensic computer sciences may yield critical success in discovery in this age when “paper trails” are often a

thing of the past.



By Timothy D. Lange

Information Prospecting: Panning for Gold in a River of Data

Sensitive data lurks in one’s documents, recycle bin, deleted e-mail, and otherwise in hard-drives, old CDs, floppies, back-up tapes, etc. Despite efforts to destroy it, digital evidence can survive. Though savvy techies may attempt to hide data, it can still be found with careful examination. Electronic “paper trails” are often left by users accessing machines and files on them. These digital breadcrumbs can be used in hosts of scenarios, from the identification of participants in a plan or scheme, to attaching supervisory liability for ratification of an act of an employee or agent,

or perhaps tracing the unauthorized access of information to a party thought to have unlawfully disseminated it. Additionally, ordinary document files, whether a draft of a contract or an internal memorandum passed through a review process, are more than they might appear at first blush—metadata included in the document can reveal who made changes, when they were made, what changes were made, who reviewed the document, and perhaps more. Understanding what gold may lie in the riverbed of data available is half the challenge—accessing and locating it lies next.

The E-Discovery Process: Access, Duplicate/Copy and Analyze the Data

Discovery requests seeking electronic data are frequently met with a host of objections. Considerations of privilege, relevancy, and privacy concerns surface. The first hurdle is thus obtaining authorization to access the network or system—which will generally require a carefully crafted preservation order of the Court designed to protect the interests of all parties. Whatever may contain data in question, hard drives, CDs, DVDs, blackberries, text messaging devices, and other storage media (such as back-up media) should be accessed.¹ This access is through a physical interface with that hardware.

Once a physical interface is established with the component having the source data, duplicates, copies and images can be made of the source material. As of November 2005, approximately 150 automated tools existed for helping law enforcement officials investigate computer crimes² and access this data. These tools are not all created equally, and depending on the methods used to find the evidence, a *Daubert* challenge may be successful. The original source needs to be protected from corruption—often with specialized hardware or software for write protection.

Making a duplicate or a copy is not as simple as it sounds. A copy is an accurate reproduction of information contained on an original physical

Tim Lange, a Contributing Club member, is a partner with Benson, Byrne, Risch, Siemens & Lange, LLP in Louisville. He practices primarily personal injury and business law and litigation. He may be reached at (502) 583-8373 or tlange@timlange.com.

item, independent of the electronic storage device (e.g., logical file copy).³ The copy maintains contents, but importantly, attributes may change during the reproduction. A duplicate, on the other hand, is an accurate digital reproduction of all data contained on a digital storage device (e.g., hard drive, CD-ROM, flash memory, floppy disk, Zip, Jaz). The duplicate maintains contents and attributes (e.g., bit stream, bit copy, and sector dump). Again, this expert must ensure that the source is not altered, and that the product made is an accurate digital reproduction of the source data sought. The chain of custody must be protected of these materials as well.

When the source material has been duplicated, the product can be analyzed. Benign files will be excluded (program files, files with obvious titles or content can then be analyzed through string searches, key-words, etc.) and then the material can be scanned for hidden evidence. Files can also be hidden on a hard-drive—perhaps by altering the drive to reflect that it is smaller than it is in reality, or hiding data in the host protected area (HPA) of the computer. Files with hidden data may not copy without error, or may copy with fill data, leaving out the critical, hidden data sought. There are many different products and approaches to locating such material that are well beyond the scope of this primer—any expert engaged should be current with this continually evolving technology.

Other Litigation Functions of This Expert

This expert can also assist with:

- Accessing Password Protected or Encrypted Files. The ability to defeat these protections vary depending on the relative sophistication on both sides of the challenge.
- Deleted File Recovery. Deleted files

can often be recovered. This is the case so long as the deleted file has not been effectively overwritten. Some software products attempt to thoroughly delete files by repeatedly overwriting the space on which they have been saved, though technology continues to improve assisting in identifying and resurrecting this evidence. This may be in “unallocated space” that is unused on the hard drive but was previously occupied by the deleted file, or in “slack space,” which is space in an existing file that can contain remnants of prior files that occupied that space.

- Timeframe and User Activity analysis. Examination of data relative to specific users and times captured electronically can be useful in determining when events occurred on a computer system. This can help in tying usage of the computer to an individual(s) at the time the events occurred—such as may be the case with someone stealing intellectual property or accessing data without authorization.
- Preservation of Evidence. If litigation is imminent, or evidence may otherwise be needed in the future, a forensic computer expert can locate and preserve critical evidence.

As always when engaging an expert, be advised to seek references from fellow KATA members or other counsel having previously worked with the expert. Again, the practical experience of a computer sciences consultant, coupled with whatever certifications and training the expert may present specific to the issues of

the case, should weigh in the selection of the right person for the job. Use KATA’s ListServ to network and discover helpful information about the person under consideration. Request references and background information on any expert with whom you are interested in working. Find out if the expert’s testimony has ever been excluded. Confirm the pertinent schedule of fees and document terms concerning payment and billing before engagement. Clearly convey your case timetables with respect to discovery and trial, and leave ample time for the scheduling and preparation of this expert for his or her discovery and trial depositions. Remember, experts can make or break your case. Choose wisely!

- 1 In some circumstances, it may be appropriate to conduct discovery against the ISP provider of the target party as well.
- 2 From *The Computer Forensics Tools Verification Project*. This project is designed to provide assurance that the tools used in the investigations of computer-related crimes produce valid results. More information can be obtained at www.cftt.nist.gov/project_overview.htm. This is a product of The National Institute of Standards and Technology and supported by the U.S. Department of Justice’s National Institute of Justice.
- 3 Information for this article was gathered from *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, National Institute of Justice, April 2004, <http://www.ncjrs.gov/txtfiles1/nij/199408.txt>

