American Bar Association Young Lawyers Division
The Young Lawyer

thedigitaledge— Computer Forensics
Not Just for "Techies" Anymore

By Jason T. Wright and Scott Wrobel

What is computer forensics?
While many people might conjure a mental image of a crime scene from *CSI* when they hear the word "forensics," forensics is much more than the examination and comparison of fingerprints, DNA, firearms, and other evidence in a criminal investigation. *Merriam Webster* defines "forensic" as "the application of scientific knowledge to legal problems; especially: scientific analysis of physical evidence (as from a crime scene)." Computer forensics is the specialized application of computer investigation and analysis techniques to preserve, identify, extract, document, and interpret electronically stored evidence suitable for presentation in lawsuits. Unlike basic copying of files from the Windows® platform/operating system, a computer forensic acquisition uses industry-standard forensic tools to create a bit-by-bit image of a hard drive or server to preserve all data or evidence. Subsequent forensic analysis of the acquisition can recover "deleted" files, track the history of changes made to files, identify Web sites accessed or transfers of information, and establish timelines with a record of all activity.

How are computer forensics used?
The type of information obtained from a computer forensics acquisition and analysis can be critical in refuting or substantiating statements made in depositions or interviews. For example, during the course of a recent internal investigation, an inconsistency arose regarding the source of breached confidential company information. A forensic acquisition and analysis of the suspect's computer verified the source of the breach based on access logs that were contained on the hard drive, which disproved the suspect's statements provided during an interview. A computer hard drive is one witness that does not lie.

When should I use computer forensics?
When contemplating litigation, during litigation, or when handling internal company investigations, the timing of a computer forensic acquisition is important to the integrity, admissibility, and reliability of the evidence. The sooner digital evidence is acquired the better. Early acquisition of digital evidence decreases the chance of tampering and spoiling the viability and dependability of the media. An act as simple as powering on or off devices (i.e., computer, PDA, or server) can change the state of data and cause certain data to be lost entirely. In the event an acquisition is covert, it is critical to meet with your client's information technology (IT) personnel as soon as possible and understand the IT systems, particularly the backup systems. This meeting is essential as the IT personnel's inside knowledge of the client's systems, architecture, and processes can alert computer forensic professionals to potential problem areas that they may encounter during the forensic acquisition. For example, some IT systems employ auto-delete functions that could potentially erase evidence.

It is equally important that clients, specifically corporations, retain relevant data and other documentation when litigation is reasonably expected (*Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422 (S.D.N.Y. July 20, 2004)). The *Zubulake* court emphasized that when litigation is reasonably expected corporations should issue a litigation hold that directs all employees to preserve documents and data that may be relevant to the litigation. Recently, the court revisited *Zubulake* and discussed parties' preservation obligations by concluding that "[w]hile litigants are not required to execute document productions with absolute precision, at a minimum they must act diligently and search thoroughly at the time they reasonably anticipate litigation." *Pension Comm. of Univ. of Montreal Pension Plan v. Bank of Am. Secs., LLC*, 2010 WL 184312, *24 (S.D.N.Y. Jan. 15, 2010). A corporate litigation hold or preservation memo will go a long way in safeguarding relevant data, electronic or otherwise, in the eyes of courts.

Published in *The Young Lawyer*, Volume 14, Number 9, July 2010.

How much do computer forensics cost?
While computer forensics is a valuable tool, each case must be evaluated separately to determine whether the benefits of a forensic acquisition of electronic data and the subsequent forensic analysis outweigh the costs. First, you must ask the right questions up front in order to determine the appropriate scope of the investigation. Costs can be drastically reduced if you know where to look. By narrowing the investigation to the computers or devices of select persons and/or servers, you can control the costs incurred by computer forensics experts. Good computer forensics experts will work with you to identify the appropriate questions to ask and identify the most potentially beneficial areas of analysis. They also will ensure that you are comfortable with all procedures and are aware of all potential hurdles or roadblocks.

Conclusion
The recovery of electronic data can be vital in obtaining evidence and establishing a fact pattern in lawsuits. But, you must ensure that the recovered data is preserved before a computer user has an opportunity to intentionally or inadvertently destroy or alter it. The need for computer forensics should be determined early in an internal investigation, prior to the discovery phase of litigation, or, at the very latest, during the discovery phase of litigation.

NEXTSTEPS

- *e-Discovery:Current Trends and Cases*. 2008. PC # 1620320. ABA Publishing.
- *Electronic Evidence and Discovery: What Every Lawyer Should Know* Now, Second Edition. 2009. PC # 5450055. Section of Science & Technology Law.
- "Ethical Traps in E-Discovery" (CLE Program Sept. 30, 2010).
    - **Register for the CLE Program at www.abanet.org/cle/smartsoloing/.**

Jason Wright is a manager and Scott Wrobel is a director in the Dispute Advisory & Forensic Services group at Stout Risius Ross, Inc. They can be contacted at jwright@srr.com and swrobel@srr.com.

Published in *The Young Lawyer*, Volume 14, Number 9, July 2010.