

## Anti-Forensics: The Judicial Arms Race

by Gregory Fordham

Although paper continues to play a role in American Jurisprudence, it has been largely replaced by digital evidence. Just as lawyers and judges have learned to deal with the new medium, so have evil doers.

The expertise of the dark side is not limited to perpetrating wrong but also in hiding it. When paper was king so were shredders, light tables, white-out and various copier manipulations. In the digital age it can be far more sophisticated.

Initially it may have been simple file deletion. Everyone has learned, however, that forensic experts can easily recover deleted files.

File wipers and shredders were the bad guy's answer to deleted file recovery. But these techniques often leave traces of their use even though the data is lost forever. Furthermore, once their use is detected an adverse inference sanction is usually worse than the penalty that the bad guy was facing.

Nonetheless, the frequency of these practices is now almost ubiquitous. Furthermore, as the detection techniques have improved so have the bad guy's disguise, deception, camouflage and other stealth techniques.

For example, since there is no law against file deletion if done before a duty to preserve arises, why not do it in the open. Just turn back the computer clock and make it appear to be from an earlier time.

If the clean up is really complex perhaps a digital forgery is in order. If so, surrender a phony hard drive that has been reconstructed from scratch or with the aid of a prior backup.

If it is a few discrete items that need protection then blend them with the harmless. Changing a file's name and extension is like changing its uniform. So put it in "civilian clothes" and bury it with the rest of the Windows operating system files.

If even greater stealth is needed then completely bury the contraband in another file and hide its existence through a variety of low tech tricks like coloring, sizing, and ordering. Or for something more sophisticated try a least significant bit manipulation.

Of course, all of the above are detectable too. It may require the equivalent of night vision goggles, x-ray equipment or spectrum analysis but they are still detectable despite their cleverness.

Sometimes the more sophisticated techniques are just no match for an observant examiner. A file appending scheme can be detected when content sizes do not seem to match file sizes. Similarly, a nonsensical story can betray a null cipher.

Good and evil have always been at war. Measure and counter measure are the volleys each side makes in search of the other's

weaknesses.

The lesson for lawyers is that there is an undeclared war and it has fostered an arms race of sorts. Therefore, a lawyer's hurdles with digital evidence are not limited to cost saving measures or protecting the smoking gun from legal maneuvering that is designed to keep it hidden.

Indeed there is an ever increasing need to validate the production of digital data. Furthermore, when planning the production request the lawyer must also consider what artifacts and elements should be included in order to facilitate the validation.

In this case both sides use the same weapon—the computer. What differentiates good from evil is how they use the keyboard.

Fortunately, using a computer can be like throwing pebbles in a pond. The destruction may not be undone and the data may not be recoverable. But the ripples on the water and the footprints at the shoreline are detectable nonetheless.

Dealing with these ripples is the next target of the anti-forensic crowd. In recent years they have started developing software to obliterate the ripples without leaving footprints at the shoreline.

Their theory is that detecting a cyber criminal is still a long way from convicting one. Their plan, therefore, is to so badly jumble and deface the remnants and artifacts commonly used by forensic analysts that the evidence is useless.

In light of the proliferation of anti-forensic tools, as well as web sites and conferences teaching these techniques, preservation and perhaps even surprise take on more importance to the lawyer's strategy and discovery plan.

It also means that e-discovery practiced without the aid of computer forensic ninjas is ill-advised. In addition, a raw recruit armed with a rifle does not a warrior make.

§§§

*Gregory Fordham has written extensively on this subject and the Georgia Bar has approved his e-discovery presentation for CLE credit. His papers are available for download from the K&F website, [www.knfcon.com](http://www.knfcon.com). He regularly advises clients on how to structure their e-discovery plans in order to minimize cost and maximize return. He also has served as an expert witness in many state and federal cases involving e-discovery and computer forensics. He is also a contributing writer for the 2007 Construction Law Update which was published earlier this year by Aspen Publishers. His e-mail is [greg@knfcon.com](mailto:greg@knfcon.com)*

