What Does a Child Pornography Case Tell You About Computer Evidence?

By Christopher B. Hopkins

It may surprise you that a child pornography case from Illinois may change how you handle computer evidence in your cases and how you maintain computers in your home. In *United States v. Seiver*, Seventh Circuit Judge Richard Posner held that police had sufficient probable cause to search a home computer even though the alleged crime (uploading pornographic images) had occurred seven months before. The opinion, which unfortunately reads like a "how to" manual for those who want to hide illicit computer activity, explains the massive amount of information on a PC which reveals (a) what websites were visited, (b) what images have been viewed on the computer, and (c) what files may exist even after deletion. In fact, this "hidden" information is so easy to recover that such evidence could be obtained in non-forensic discovery or a by parent interested in the internet escapades of a teenager.

In the *Seiver* case, the defendant downloaded a pornographic video which a 13-year old girl had created. Defendant Seiver extracted still images from the video, uploaded them to a file sharing website, and then sent a message via Facebook to the girl's stepmother. The authorities traced the Internet Protocol (IP) address to Seiver's computer, obtained a search warrant, and arrested him (to bring this closer to home, one news story reported that Seiver had allegedly contacted minors in Florida).

The *Seiver* decision distinguishes itself from other computer crime cases since Judge Posner's decision explains that, even if the defendant had deleted the incriminating files, there was sufficient probable cause for a search warrant, months after the fact, since "modern computer technology and the usual behavior of its users" lead to lingering data long after files are deleted or websites were visited. In short, the normal use of a computer will preserve a website log, images viewed, and files even if they were viewed momentarily or even deleted.

According to Judge Posner, "…it appears that few consumers of child pornography… understand well enough how their computer's file system works…" First, regardless of which internet browser is used (e.g., Internet Explorer, Chrome), the name of every website visited is saved in a text file called "index.dat." This surprisingly small file exists right now on every computer you own and may report every website visited since the machine was purchased. There is, of course, an operational purpose for this log (which is generally hidden from plain view on the C: drive) but, in the forensic context, it also provides a harvestable web history. Apparently even sites visited using the "incognito" or "private browsing" functions are recorded. You can view the index.dat file on your computer using free software like Index.dat Viewer, Index.dat Analyzer, or Index.dat Scanner. Likewise, you can erase the Index.dat file using free software such as CCleaner however the file will begin anew the next time the browser opens a website. Keep in mind, however, the spoliation and ethical risks associated with deleting files (see the $522,000 sanction for the lawyer who instructed his client to delete Facebook photos, bit.ly/QvMz7h).

Second, both Mac and Windows machines preserve images from webpages in temporary internet files (or "cache"). In short, every picture which has appeared in a computer's browser is saved, at least temporarily, in the cache. For operational purposes, this speeds up your browsing experience; for forensic purposes, the cache may be a trove of information about a user's viewing habits. Do a Google search for "view temporary internet files" to determine how to inspect those files. Both Explorer and Chrome can be set to delete temporary files upon closure. CCleaner will clean out the cache.

Third, are deleted files (such as a "cleaned" internet browser cache) really erased? As Judge Posner explains, "… the file hasn't left the computer. The trash folder is a waste-paper basket; it has no drainage pipe to the outside. [The file] is still there and normally is recoverable by computer experts until it's overwritten…" In the *Seiver* case, as an example, the court held that seven months was not too long for there to still be probable cause that deleted evidence might still exist. Judge Posner noted that the operating system, the size of the hard drive, and how often new files are saved will accelerate the normal speed of overwriting deleted data. Moreover, "a deleted file is not overwritten all at once, it may be possible to reconstruct it from bits of data composing it (called 'slack data') which are still retrievable because they have not yet been overwritten even if the overwriting has begun." To this end, consumer-level programs such as Recuva will permit a user to view deleted files; meanwhile, once again, CCleaner is the application of choice to "wipe" unused portions of the hard drive (Mac OS X has a "secure empty trash" option built in).

Judge Posner's opinion concludes with the notion that "despite the availability of software for obliterating or concealing incriminating computer files, the use of such software is surprisingly rare." To that end, he determined that seven months was too short to conclude that probable cause of finding a data trail had evaporated; moreover, he advised savvy law enforcement officers that the search warrant affidavit should apprise the magistrate that deleted files are recoverable. This advisement is likewise warranted for lawyers, judges, and parents.

Christopher B. Hopkins is a shareholder at Akerman Senterfitt. Send an email, without indecorous attachments, to christopher.hopkins@akerman.com.