Data Spoliation – Uncovering the Cover-Up

Maragell, LLC

By: Jeffrey Brenner, NJLPI and Steve Hilary, EnCE, CCE, ACE

Concerned your adversary's client altered a document and deleted the original? Worried your own client deleted key evidence from his computer before turning it over for inspection? Years ago, when a user hit "delete" it didn't always mean "delete" and forensic examiners were quick to amaze litigants with their ability to reclaim the information. With improved hard drive technology and increased operating system security (combined with full disk encryption), today, delete can really mean delete. Or does it? Enter the forensic artifact.

Just as the human brain tells the muscles in the arm to curl, a computer's operating system tells the device what to do when a thumb drive is inserted, how to display a webpage, or when a file is deleted. These types of commands/instructions, among thousands of others, are routinely recorded and stored by the computer's operating system. By studying these items, a forensic examiner can often recreate the user's activities on the computer, including the spoliation of information.

By way of example, a user can remove a file from a computer by simply deleting it. Doing so "sends" the file to the Recycle Bin. This action creates a host of forensic artifacts depending on the (Windows) operating system of the computer (Mac computers have different artifacts). These artifacts can reveal when the file was sent to the Recycle Bin, the original location of the file on the computer, its original size, and the user profile involved.

The file remains in the Recycle Bin until either the user restores the file (either by undoing the deletion or simply dragging it out) or removes it (by deleting the contents of the entire Recycle Bin or selectively deleting the one file). Deleting the deleted file from the Recycle Bin "sends" it to the unallocated/deleted space of the computer. If the drive is an older one, this space may contain the "permanently" deleted data until the data is overwritten by new files created on the computer or until a cleanup process is performed. Until the data is overwritten, keyword searches and forensic file recovery software can be used to locate and/or reclaim the information. If the drive is new (solid state drive or a virtual machine), the file itself is likely unrecoverable.

But what if the custodian were to *wipe* the relevant files from the computer instead of just deleting them? When a person wipes a file using a software program such as Eraser, Window Washer, or PC Cleaner, generally four actions will occur: the software will rename the original file, it will overwrite the original file's data, it may change the timestamps of the original file, and it will delete the original file (not necessarily in this exact sequence).

Many of these transactions can be found in the operating system files even though the file itself has since been destroyed. By extracting and analyzing these operating system files, an examiner can potentially determine the original file's name and location on the hard drive.

If the file cannot be identified, using other forensic artifacts found in the operating system, the examiner may still be able to determine what program was used (assuming the user deleted the wiping program too), when it was installed, and when it was used. The mere use of a wiping program after a litigation hold is in place (or subpoena received) may be enough to impose sanctions even if the original files cannot be identified. And, if that evidence can be coupled with an examination of the user's Internet history showing what searches were conducted (i.e. "how to permanently delete a file") an intentional act can be established.

Another "hiding" place for lost files is the computer's Shadow Copy (sometimes referred to as a "Restore Point"). Depending on the configuration of the operating system, the computer itself may create several Shadow Copies, each one containing a snapshot of the content of the computer at the time. If a file is missing from the computer, by examining this artifact, the examiner may succeed in locating it. The bigger question of why it went missing is a topic for deposition.

Practice Tips: By knowing the original file names and locations of the wiped files, an examiner can potentially restore them from Shadow Copies. In the event no Shadow Copies exist, knowing the wiped file names/folders even existed may provide sufficient evidence to claim spoliation. Finally, analyzing other artifacts on the computer may show when a wiping program was initially used, when it was last run and how many times, and whether the user searched the Internet for tips on how to destroy sensitive files, thereby providing circumstantial evidence of an intentional act.