# ESI Spoliation is as easy as 1-2-3

If you think spoliation of electronic evidence is only caused by careless lawyers, think again. It only takes a click of a mouse, or the insertion of a USB device for you to destroy what could be the most important fact in your client's case. Case law considers even negligent destruction a basis for a spoliation claim. See Sampson v. City of Cambridge, Md., 251 F.R.D. 172, 179 (D. Md. 2008). Couple that with recently amended FRCP 37(e) which provides a federal court with a means to sanction a party for its failure to take reasonable steps to preserve relevant electronic evidence, and you have cause for many a sleepless night.


## MARAGELL Corporate Investigations

**Contact:** Jeffrey Brenner, Esq., NJLPI

**Address:** 2 Coleman Ave, Suite 201, Cherry Hill, NJ 08034

**Phone:** 856.429.0325 x223

**Fax:** 856.429.0539

**Email:** jbrenner@maragell.com

**Website:** www.maragell.com


In a case involving stolen computer files, the dates and times when those files were copied off a device, and the date and time they were copied onto another (or when they were last accessed or viewed) can mean the difference between inculpation and exculpation.

### Consider these fact patterns:

1. "My client may have emailed those confidential documents to herself, but she saved them on her computer only because she was told she might need to work at home to get the project done. She never looked at them again." Upon a forensic examination of the laptop, the "last accessed" dates for all the company documents she saved to her computer match the date she met with the attorney. Why? Because the attorney wanted to review them before responding to the prior employer's demand notice/lawsuit. Counsel's ability to credibly argue her client never looked at the files after she saved them years ago just got harder.

2. Same case, but instead of files on a laptop, the files are on a thumb drive. "My client may have copied them onto a thumb drive, but she swears she never copied them elsewhere." Upon a forensic examination of the thumb drive, all the "last accessed" dates were changed to the date the client met with the attorney. Why? Because the attorney inserted the thumb drive into her computer and copied them to the server to review them before producing them to the other side. Counsel's ability to credibly argue her client never copied them elsewhere just got harder.

3. Same case, but instead of saving files to a personal laptop, the client deleted her personal files from the company laptop. "My client only deleted her pictures and personal documents prior to returning the company-issued laptop to HR." Upon a forensic examination of the laptop, it is determined that on three separate days leading up to the employee's departure, a file wiping program was used to permanently destroy a host of files—all that was left was a pattern of 1's and 0's over wide sections of the hard drive. Counsel's ability to credibly argue her client didn't take any company records before destroying "only her personal files" just got harder because it cannot be determined what files were deleted.

**Practice Points:** Preservation of metadata can be achieved through the use of free write-blocking software that can be installed on a computer (http://dsicovery.com/software), as well as by changing the USB settings on the computer. Doing so will enable the user to freely examine data on the devices without the risk of changing "last accessed" dates and other metadata fields that could prove useful. Metadata can also be preserved through the use of forensic imaging hardware and software tools (which require specialized training), and can be targeted to specific files at issue, or the entire hard drive. In the light of Rule of Professional Conduct 1.1, Competence, and the ease in which data can be lost, altered, and destroyed, it is incumbent upon counsel to rely upon forensic specialists for guidance whenever electronic evidence is involved.