Articles + Publications | May 24, 2024

Following the Trail of Lost or Destroyed ESI with Forensic Imaging

For The Defense

WRITTEN BY

Toyja E. Kelley | Noah J. Mason

Locke Lord Washington, D.C., Partner **Toyja Kelley** and Atlanta Associate **Noah Mason** co-authored an article published in For The Defense discussing tactics that litigants use to hide or destroy electronically stored information (ESI). In the article, Kelley and Mason address how attorneys can detect tampered ESI with the help of forensic experts, citing examples of cases where courts have looked at such behaviors to determine whether forensic imaging is warranted. The authors explain, “One of the best ways to determine whether and to what extent ESI [has] been accessed or destroyed is to obtain a forensic image.” Kelley and Mason further note, “The best practice is to have imaging performed by an objective third party who can establish a chain of custody and thwart accusations of spoliation.”

“With the expansion of file sharing and cloud services, it is even more difficult to track and detect all of the devices and locations where relevant files may be stored. This will require even more diligence on the part of counsel when the opponent delays providing ESI, reports a device has been destroyed, or resists an inspection,” Kelley and Mason emphasize.

Read the full For The Defense article (subscription may be required) or view the article below.

When there is potentially crucial evidence on a computer or device once controlled by the opposing party, an ex-employee plaintiff, or someone suspected to have stolen trade secrets we want to track it down as soon as possible. For anything done on a computer there will be a trail of data that can be traced. That information can reveal what files were on the device, when those files were downloaded or transferred, and how they were used. But what do we do when the trail goes cold or comes to a dead end? Even when a user attempts to cover their tracks by deleting or overwriting files there is often a traces of data left behind that can provide valuable information the deleted information or even allow for the recovery a file.

This article discusses tactics litigants used to hide or destroy electronically stored information (“ESI”), how attorneys can detect it with forensic experts, and how courts have looked at such behaviors to determine whether suspicious behavior warrants forensic imaging. It is not an exhaustive study of these topics –as tactics change as rapidly as technology and features on the newest device. But we will look at recent cases to provide insights into the issues, expose common tactics, and show how counsel uncover suspicious activity despite efforts to hide it.

A forensic expert can be hired to track and assess whether a file has been erased or modified as well as how and when a file was last accessed. However, forensic examination may only be available after the party seeking examination can show unauthorized access to data or some other improper conduct. As a result, defense counsel

must have both the technical and legal skills to uncover and address attempts at spoliation. *See* SHANNON BROWN, ESQ., MA, JD, PEEKING INSIDE THE BLACK BOX: A PRELIMINARY SURVEY OF TECHNOLOGY ASSISTED REVIEW (TAR) AND PREDICTIVE CODING ALGORITHMS FOR EDISCOVERY, 21 Suffolk J. Trial & App. Advoc. 221, 223 (2016). In order to properly supervise technology vendors as required by the Model Rules of Professional Conduct, we must be informed users of forensic imaging technology and exhibit more than an uncritical reliance on these experts in our cases. *Id*.

Analyzing ESI through Forensic Imaging

We can use depositions and written discovery to get information about the location of discoverable information and evidence of possible spoliation, but those are not the only means available to you. As one district court reasoned, "witnesses who destroy relevant evidence may also testify falsely." *See Otogenetics v. Omega Biosciences*, No. 1:15-CV-2697-SCJ, 2016 U.S. Dist. LEXIS 202816, at *13 (N.D. Ga. Mar. 14, 2016). One of the best ways to determine whether and to what extent ESI been accessed or destroyed is to obtain a forensic image.

Forensic imaging enables experts to take a snapshot of a hard drive or registry of a device and track access, files, as well as determine whether external devices were connected that could transfer files to other computers. *See generally Krumwiede v. Brighton Assocs.*, LLC, No. 05 C 3003, 2006 U.S. Dist. LEXIS 31669, at *11 (N.D. Ill. May 8, 2006). Prior to extraction or analysis of any data on a device, an exact copy of the original storage media on subject device is taken called a "ghost image" or "mirror image." To create a true forensic image all parts of the device or media must be copied at the hard drive level. *See What is Forensic Hard Drive Imaging*, FORENSICON, ***https://www.forensicon.com/resources/articles/what-is-forensic-hard-drive-imaging***. (last updated August 15, 2023). It is a highly detailed process and there are multiple methods and tools trained professionals use to create forensic image. *Id*. The process allows an expert to examine files on a device with minimal impact. *Id*. It can often reveal metadata describing when a file was created, where it was stored, when it was last accessed and whether devices capable of transferring, overwriting, or storing file data were connected to a device. *See generally, Krumwiede*, 2006 U.S. Dist. LEXIS 31669, at *11. The best practice is to have imaging performed by an objective third party who can establish a chain of custody and thwart accusations of spoliation,

Forensic imaging is regularly used in civil litigation to aid discovery. *John B. v. Goetz*, 531 F.3d 448, 459 (6th Cir. 2008). A party may choose on its own to preserve information through forensic imaging, and district courts have, for various reasons, compelled the forensic imaging and production of opposing parties' computers. *Id* at 459. Many federal courts "have assumed that the provisions of Rule 34(a) concerning inspection, copying, and testing of tangible objects are sufficient to authorize a court to order reproduction of an entire hard drive using the 'mirror image' method." *See List Indus. v. Umina*, No. 3:18-cv-199, 2019 U.S. Dist. LEXIS 73481, at *9 (S.D. Ohio May 1, 2019). Even still, some federal courts have noted that forensic imaging is an expensive and burdensome process that often requires the production of privileged information, which can unnecessarily add to the expense and complexity of the case. *Diepenhorst v. City of Battle Creek*, Case No. 1:05-cv-734, 2006 U.S. Dist. LEXIS 48551, *10-11 (W.D. Mich. June 30, 2006). The Advisory Committee Notes narrow the scope of Rule 34(a) stating:

Inspection or testing of certain types of electronically stored information or of a responding party's electronic information system may raise issues of confidentiality or privacy. The addition of testing and sampling to Rule 34(a) with regard to documents and electronically stored information is not meant to create a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances. Courts should guard against undue intrusiveness resulting from inspecting or testing such systems.

Advisory Committee Notes to Fed. R. Civ. P. 34. For instance, in a recent Appeals Court of Maryland decision guided by federal court protocols, the court weighed a non-party's privacy rights against the discovery needs of that case. *St. Frances Acad. v. Gilman Sch., Inc.*, No. 1390, 2022 Md. App. LEXIS 203, at *19 (App. Mar. 21, 2022). The court upheld the lower court's decision in fashioning a discovery order granting in-part, Gilman's (represented by Locke Lord counsel) demand for forensic imaging of a cell phone. Id. at *8. In that decision court noted that Gilman through its counsel, suggested a procedure that tailored search criteria to limit intrusiveness and protected the privacy of information on the device. Id. at * 9. The proposed procedure made sure "no human looks at [the data] until [counsel for the device's owner] gets an opportunity to go through it" and counsel for the cell phone's owner would be the first person to review data before it is disclosed to Gilman's counsel. *Id*.

Compelling a Forensic Image Requires More than Suspicion of Misconduct

Courts have been cautious in requiring the mirror imaging of computers where the request is extremely broad in nature and the connection between the computers and the claims in the lawsuit are vague or unsubstantiated. *John B.*, 531 F.3d at 459- 460. "Mere skepticism that an opposing party has not produced all relevant information is not sufficient to warrant drastic electronic discovery measures." *Id*. As such, "even if acceptable as a means to preserve electronic evidence, compelled forensic imaging is not appropriate in all cases." *Id*. However, in cases involving trade secrets and electronic evidence courts have been more willing to grant permission to take a forensic image of devices that may contain electronic data directly related to the alleged violation. *See IHS Glob. Ltd. v. Trade Data Monitor LLC*, No. 2:18-cv-01025-DCN, 2019 U.S. Dist. LEXIS 220327, at *9 (D.S.C. Dec. 23, 2019).

Courts are continuing to develop a standard for when digital forensics can be used to aid discovery. SEE JEY E. GRENIG & WILLIAM C. GLEISNER, III, EDISCOVERY & DIGITAL EVIDENCE, §11:8, (November 2022). Generally, courts will look to the facts of the case and nexus between the device and claims in the suit to determine whether a forensic image is proportional to the needs of the case. *See IHS Glob. Ltd. v. Trade Data Monitor LLC*, No. 2:18-cv01025-DCN, 2019 U.S. Dist. LEXIS 220327, at *9 (D.S.C. Dec. 23, 2019). In evaluating whether to order or allow a forensic image some courts may consider "whether the responding party has withheld requested information, whether the responding party is unable or unwilling to search for the requested information, and the extent to which the responding party has complied with discovery requests." *Bennett v. Martin*, 928 N.E.2d 763, 774 (Ohio App. 10 Dist., 2009) (citing *Diepenhorst* 2006 U.S. Dist. LEXIS 48551, *10-11).. When a requesting party demonstrates…the responding party's failure to produce requested information, the scales tip in favor of compelling forensic imaging. *See id.*

The justification for forensic imaging goes beyond just reviewing the documents or files contained on a device but can also offer valuable insights in whether files had been impermissibly copied, saved, manipulated or used. *See Ameriwood Indus.*, Inc.*, v. Liberman*, 2006 U.S. Dist LEXIS 93380, at *3 (E.D. Mo. Dec. 27, 2006). Particularly, in cases where a party allegedly used the computer itself to commit the wrong that is the subject of the lawsuit, items on the hard drive are discoverable. Most notably when it comes to an investigation of spoliation, a forensic examination of an image can reveal whether a party made any efforts to delete files or "scrub" the devices at issue. For example, in *IHS Glob. Ltd. v. Trade Data Monitor, LLC* the court granted a forensic inspection when the plaintiff alleged a defendant misused proprietary information while working for them and sought a forensic examination of a laptop to determine when and how the defendant used documents which had already been produced. See *IHS Glob. Ltd.*, 2019 U.S. Dist. LEXIS 220327, at *9. Similarly, in *List Indus. v. Umina*, the court ruled that a forensic image be produced after the defendant unilaterally imaged the hard drive and refused to

produce the image to the plaintiff. No. 3:18-CV-199, 2019 WL 1933970, at *5 (S.D. Ohio May 1, 2019). As such, counsel seeking a forensic image of a device where one has not already been ordered are tasked with showing ESI was improperly withheld, deleted, or misused often without the benefit of access to the device that may contain insights on what information had been available.

Under the federal spoliation standard, there must be proof of the existence of discoverable information showing that evidence once existed when it has been intentionally removed can be incredibly challenging, and without it there is no claim for spoliation. *See Marshall v. Dentfirst*, P.C., 313 F.R.D. 691, 694 (N.D.Ga., 2016) (citations omitted). Thus, as it pertains to ESI counsel must be able to prove the existence of discoverable information on a device before they can seek additional discovery about spoliation. Forensic imaging is one way to prove information may have once existed on a device, but the facts must warrant such an investigation..

File Shredding Can be Hard to Detect

Depending on the method and level of sophistication of attempts to destroy data, a digital forensic expert may be able to detect whether an application had been used. However in some cases they may not be able to determine the full extent to which files were destroyed or altered, because a program has been used to wipe the registry of a computer. *See generally*, *NITV Fed. Servs., LLC v. Dektor Corp.*, No. 18-80994-CIV, 2019 WL 7899730, at *4 (S.D. Fla. Sept. 20, 2019). There are also programs that overwrite deleted files on the hard drive or attempt to find deleted files ensuring they could not be recovered by a neutral vendor or opposing expert. *Id*. There are also ways to "brick" a laptop by encrypting it without providing a way to access the laptop without their password, or "zero fill" a hard drive –a method of formatting a hard drive whereby the formatter wipes the contents by overwriting them with zeros. *NITV*, 2019 WL 7899730, at *17. These applications go by many names, such as, CCleaner, Defraggler, WinUndelete, and the most appropriately named, File Shredder. *See generally id*. at *17.

In one of the more egregious cases, *Taylor v. Mitre Corp.*, the plaintiff used CCleaner to delete files from a computer that he used for work prior to destroying it with a sledge hammer. No. 1:11-CV01247 LO/IDD, 2012 WL 5473715, at *3 (E.D. Va. Sept. 10, 2012), report and recommendation adopted, No. 1:11-CV-1247, 2012 WL 5473573 (E.D. Va. Nov. 8, 2012). However before destroying and disposing of the computer he backed up the files on it to another laptop. *Id*. The court ordered Plaintiff to submit the second computer to inspection pursuant to Federal Rule of Civil Procedure 34. *See id*. at *3. The investigation revealed that Plaintiff downloaded the aptly named "Evidence Eliminator" on his laptop three days after the court ordered him to submit the computer to inspection. *Id*. Evidence Eliminator's website described the software as one that "deep cleans your computer of 'sensitive material,' leaving you with a clean PC, a clean conscience and instant peace of mind" and that "eliminates all evidence from your PC and has proven to defeat forensic software that cost a lot more than Evidence Eliminator." *Id*. Files deleted by Evidence Eliminator could not be recovered, and Plaintiff also ran CCleaner during the litigation overwriting another 16,000 files. *See id*. at *4. Although the court ultimately ordered sanctions for spoliation, the effort was so thorough that it was impossible to determine how many files plaintiff deleted or the relevancy of those files. *Id*.

In *Experience Hendrix, LLC v. Pitsicalis*, Plaintiff's forensic expert found that after the suit had been filed defendants ran programs called "Advanced Mac Cleaner," "CleanMyMac," programs that have a "shred" function, rendering a file unrecoverable by overwriting it. No. 17 CIV. 1927 (PAE), 2018 WL 6191039, at *4 (S.D.N.Y. Nov. 28, 2018). In response, the defendants claimed the programs were used to free up space on their hard drives. *See id*. Subsequently, the court ordered spoliation sanctions, noting that by installing the shredding

software on the devices in the face of an order to produce and an ESI protocol, defendants intentionally caused destruction of evidence. *Id*. at *10. This case demonstrates that while an ESI protocol may not prevent attempts to destroy ESI, but it can provide a basis to pursue spoliation.

Many of the applications used to destroy evidence have legitimate functions in clearing hard drives to improve performance. The legitimate uses make it even more difficult to show that information was lost due to an "affirmative act" intended to destroy evidence rather than routine maintenance.

In another case it took a "smoking gun" witness to show spoliation where the suspicious behavior left few traces of actual destruction of ESI. In *NITV Fed. Servs.*, *LLC v. Dektor Corp.*, NITV's digital forensic expert's review of Herring's hard drives showed that on the day after he canceled his deposition. Herring, a defendant, downloaded a program called File Shredder, a "free desktop application for shredding unwanted files beyond recovery.". 2019 WL 7899730, at *4 (S.D. Fla. Sept. 20, 2019). The digital forensic expert could not determine whether and to what extent files were destroyed. *See id*. Without evidence that files had ever been on the device, the court may have viewed this activity as suspicious but not rising to the level of spoliation, as Herring testified that he had an unexpected hard drive crash due to a virus prior to when litigation began. However, defendant's own IT consultant, a former employee, testified that Herring asked him about file deletion software, revealing a plan to intentionally shred relevant ESI on the hard drive and a scheme mislead plaintiff. *See id*. at *8. Having found that Herring violated the agreed-upon forensic protocol the court ordered the sanction of default under Rule 37(e). *See id*. at *9.

What We Can Do to Stay on the Trail

The discovery process relies heavily on the responding party to search records and produce the requested data in good faith. Courts generally handle ESI discovery the same way they handle other discovery, relying on the responding party to produce in accordance with the rules, rather than allowing unfettered access to a party's data. With the expansion of file sharing and cloud services, it is even more difficult to track and detect all of the devices and locations where relevant files may be stored. This will require even more diligence on the part of counsel when the opponent delays providing ESI, reports a device has been destroyed, or resists an inspection.

Based on the sample of cases discussed herein, there are things counsel can do to stay ahead of these issues. In a case involving ESI counsel should:

- Investigate and seek discovery about all devices and locations that that may contain relevant data.
- Create a timeline of events and a list of individuals that controlled or had access to the devices.
- Issue a specific directive about avoiding the use of hard drive cleaning applications in preservation letters.
- Review local rules, standing orders, and prior case law in the jurisdiction for any policy or standard used by the court to evaluate when a forensic image can be ordered.
- Confer with opposing counsel to request an independent forensic review or protocol for imaging as soon as is practicable and suggest that opposing counsel collect any devices, while agreed-upon examination forensic examination protocol and is pending.
- Finally, once it appears that the responding party failed to comply with their discovery obligations such that data cannot be recovered, counsel should consider requesting the court to order a forensic image of devices that may contain relevant data to determine whether the efforts have been made to make files unreadable or unrecoverable.

Republished with permission from For The Defense.

RELATED INDUSTRIES + PRACTICES

- Litigation + Trial