How a Forensic Collection of Electronic Discovery Can Provide You with the Upper Hand

INTRODUCTION

More and more complex litigation includes electronic discovery as a required component to any matter. As an increasing amount of data is created on a daily basis and stored on a growing number of devices the need for a comprehensive strategy to identify, collect, process and review this data is critical. Long gone are the days of simply requesting custodians hand over relevant emails. In fact such a collection process is sure to open the producing party to spoliation claims and potential sanctions. Here we explore the factors cost, defensibility, comprehensiveness, security, context, efficiency and authenticity to make the case for how forensically collecting and analyzing electronic evidence can provide for lower litigation costs, more defensible productions, better early case assessment, stronger arguments to compel production, and protection against sanctions.

COST

Contrary to the common belief that a forensic collection is always more expensive, it can often result in lower discovery and review costs. By engaging a forensic expert early in the discovery process law firms can reduce discovery costs by:

- Succinctly targeting relevant employee data, date ranges and data repositories. Use of a forensic expert can help to identify where relevant data may reside without the need to schedule expensive downtime of production servers or key employees.

- Collect invaluable computer system and file metadata relevant to the timeline of events. This data may not be available to request at a later time and often provides contextual data surrounding each produced electronic file.

- Recover deleted data that may be germane to the issues at hand. The ability to review this deleted data can often be crucial during the early case assessment phase where attorneys are gauging their client's exposure and how to best respond.

- Maintain electronic discovery in its native format, thereby providing the ability to de-duplicate files, filter, and conduct advanced search techniques to reduce the production set to those files that will ultimately be converted and potentially hosted on a review platform.

- Capture full system snapshots that may be invaluable later in the discovery proceedings. Discovery is often an iterative process that leads to additional discovery requests. These forensic images can be rescanned for the new requests and subsequently produced without the need for another disruptive collection on the original system.

- Easily incorporate additional devices such as tablets and mobile devices for collection and review. More and more information from these devices are being requested as part of e-discovery, but many firms are ill-equipped to handle the collection and subsequent review of the data.

- Prevent e-discovery cost-shifting because the producing party claims that data only resides on media sources such as backup tapes that would involve undue burden or cost to produce. Many times data can be recovered from a forensic image of the storage in question.

- Reduced exposure to spoliation claims and sanctions. Unless the producing party has a technologically enforceable and an auditable process for implementing its litigation hold, then obtaining a forensic image of each custodian's computer can serve to show the producing party's good faith practice at preservation of the data in question.

DEFENSIBLE

Initiating a forensic collection of electronic data for discovery protects clients from improper or incomplete collection of e-discovery data. A forensic collection performed by a forensic expert meets both the Frye and more stringent Daubert standards.

On the other side of the spectrum, when a party chooses to perform its own self-collection using its own employees, that party runs the risk of incomplete collection, spoliation, and added costs. Incomplete

Copyright © 2012, Vertigrate, Inc. All rights reserved.

collection can occur when the employee either deliberately or inadvertently chooses to collect certain information, but not other information. This misstep can occur for many reasons, but it is often because of poor legal or managerial guidance, and/or an insufficient keyword list and related searches.

Since many employees are not familiar with proper collection methodologies nor do all firms have the tools with which to collect data without altering it, many self-collections inherently spoil the data collected. Spoliation occurs whenever the employee interacts with data that he or she has been asked to collect. The simple acts of viewing, opening, forwarding or copying will, at a minimum, alter the underlying metadata of the evidence collected, if not open the producing party to accusations of spoliation or evidence tampering.

In addition to the risks posed by self-collection, there are hidden costs associated with such lay approaches. Without the use of forensic expert, the legal team must manage the task of collecting and tracking each custodian's data set, along with any processing and review of the data. In some cases, parties have had to go back and perform additional collections of the same custodian devices and subsequently review the new collection at the 11th hour. Furthermore, key employee working hours are spent collecting information and/or testifying to authenticity of the information they collected, rather than performing their normal duties.

In both Qualcomm v. Broadcom and Green v. Blitz USA, Inc. self-collections were ultimately found to be deliberately incomplete, and as a result sanctions were entered against each of the producing parties. Subsequently, a collection conducted by a forensic expert will not only yield a more relevant collection, but also one that the courts will view as comprehensive and responsive.

Forensically sound and defensible self-collection tools do exist, but the producing party must carefully weigh the lower initial cost of these tools against the risk that the collection tool may be used improperly and that the employee who ran the self-collection tool may need to testify during the proceeding to authenticate the evidence collected.

COMPREHENSIVE

Early review and production requirements of Federal Rules of Civil Procedure include that all data, even that which is not reasonably accessible be identified. A comprehensive search of electronic data also needs to be performed before the pre-trial conference. Commercially available forensic suites generate a list of all files contained on the data sources collected. This list can be searched and reviewed by law firms to provide a low-cost and rudimentary early case assessment, or the entire data collection can be fed into some of the early case assessment platforms for a more formal review.

It has become regular practice for parties to request metadata along with the files produced. These requests demonstrate the value of metadata as part of the complete document. In Armstrong v. EOP, a hard copy printout or a .tif image (today's digital equivalent of a printout), was determined to not sufficiently satisfy the accuracy of electronically produced files. Forensic collections by definition contain this metadata.

In addition to metadata concerns, both the courts and recognized electronic discovery industry experts such as The Sedona Conference agree that an iterative approach to electronic discovery requests is more responsive than singular searches. Searches based upon an agreed upon list of keywords that may turn out to be either over-inclusive or under-inclusive. By utilizing a forensic expert and collection techniques, data sets can be collected in a single instance. Once collected these sets are available to the producing party to respond to iterative discovery requests without the time and cost associated with additional collection exercises or spoliation concerns because the data was not originally identified or collected.

SECURE

A forensic data collection is by design an inherently sound and auditable data set. They are secure containers that cannot be changed, nor can any of the files contained within them be changed. This characteristic, along with a properly documented chain of custody, protect the producing party against many spoliation claims.

Best practices dictate that not only a computational hash is performed on each file collected, but that second copy

Copyright © 2012, Vertigrate, Inc. All rights reserved.

of the set is also created at the same time. One copy is maintained as the "Best Evidence" copy and the second set is used as the "Working Copy". The best evidence copy is maintained in a secure storage facility, and the working copy is provided to the producing party in order to respond to discovery requests. Should there ever be any concern that the files within the Working Copy were tampered with a review of the Best Evidence copy can quickly clear up any concerns. Any files that are exported for production are logged; all serving to provide the producing party with the ability to respond to iterative production requests while protecting them from spoliation claims.

CONTEXTUAL

Forensic collections not only maintain the file content exactly as it was on the original system, but they also maintain all of the associated metadata with that file and surrounding system events. This additional information can serve to simply provide metadata to the requesting party, or more importantly answer the question "who knew what when".

By examining not only the file's metadata, but also the system events surrounding a file the forensic expert can provide a detailed timeline of what occurred in relation to files in question. This contextual timeline can help during the early case assessment phase for plaintiffs where they can gain greater insight into to both the value and complexity of their case; or for the defense as they gauge their exposure and cost to defend against the plaintiff's claim.

An excellent example of contextual data is the .LNK file, or shortcut file. Shortcut files are regularly created within the Windows operating system for the sake of aiding the normal user in finding a recently opened file. These shortcut files are stored in a number of visible and hidden locations such as Recent Documents, Internet Explorer, Word and unallocated (deleted) space to name a few. These little files are created, and subsequently updated, by default whenever a user opens the file that the shortcut points to. A forensic collection and analysis of shortcut files contained on a user's PC can demonstrate the existence of certain files as well as potentially the method by which they arrived i.e.; email attachment, flash drive, CD/DVD-Rom, local computer, network server or Internet download. While such an analysis is not necessary in all e-discovery related cases, this information can prove to be invaluable when faced with the question of how a file came to be created especially in the case of user's fraudulently back-dating files or intellectual property theft.

EFFICIENT

Forensic experts can help their clients hone in on relevant files more quickly than many other collection and review approaches. Commercial forensic tools utilize the same industry leading search technologies that the e-discovery suites use without the need to pay additional fees for expensive data culling, fuzzy hashing and other add-on service fees that some of the e-discovery suites charge their customers. These same tools also have the ability to use known file filters from the National Institute of Standards and Technology (NIST) that will specifically exclude known file types such as operating system, program and driver files from any type of collection, thereby speeding the review process by allowing the examiner and reviewers to focus on the relevant data. Custom hashes, or file signatures, can also be created so as to flag e-discovery contents for known hot documents without the need for expensive attorney review time.

Because the forensic expert has all of these tools available at the time of collection, they can be employed immediately after the forensic image has been created. Contracting with a forensic expert can speed up the collection, indexing and de-duplication of e-discovery data; thereby reducing both the collection and review time that would otherwise be spent by in-house employees and attorneys on a larger and irrelevant data set.

AUTHENTICITY

A forensic collection inherently includes additional system and file details that can provide attorneys with the ability to prove the authenticity of the evidence being proffered when a fact witness is unavailable or uncooperative. For example, a forensic expert can aid attorneys in demonstrating an exhibit's authenticity by 1) showing that the file was created or modified on a system that is protected by a password or other authentication, 2) showing that the file was accessed

Copyright © 2012, Vertigrate, Inc. All rights reserved.

within a timeframe that the person was known to be on the system (i.e.; via surrounding events), or 3) showing that the file was retrieved from a system that has no indication that others had accessed the system. In both Bone v. State and Ohio v. Huffman, the courts found that the forensic examiner's testimony of best practices and methodologies used to collect, authenticate and analyze the evidence were sufficient to establish the authenticity of the evidence; contrary to the criminal defense claims that the damning evidence seized from the defendant's computer should not be admitted because it could not be authenticated by the defendant.

CONCLUSION

Enlisting a digital forensic expert early on in any e-discovery litigation matter can provide attorneys and their clients with an invaluable asset. As discussed, the forensic expert can help identify the relevant systems from which to collect the electronic evidence and the most efficient and least disruptive way in which to collect it. Once collected the forensic expert's suite of tools can process the evidence by indexing and de-duplicating the data sets while flagging any hot documents or files. This data set can be further examined by the expert to determine timelines, identify deleted or encrypted files, and demonstrate employee behavior that may be critical to both early case assessment and further discovery requests. Finally the forensic expert can assist the legal team in responding to production requests from the other side without the need for additional expensive collections, and provide the review team with a condensed review set of relevant materials from which to build the team's case. These review and production sets can be exported to fit with any of the leading litigation review platforms.

To learn more about forensics and our services, visit us at www.vertigrate.com.

Michael Lombardi is the President and owner of Vertigrate, Inc., a legal technology consulting firm. He holds an MBA from the University of Arizona and is a GIAC Certified Forensic Examiner. He has worked with hundreds of attorneys inside and outside of the courtroom on matters as large as $1.2B.

Copyright © 2012, Vertigrate, Inc. All rights reserved.