

Avoiding Common Collection Blunders

By Karl Flusche, Evidence Collection Manager, Fios, Inc.

Electronic discovery is filled with pitfalls and mistakes that can be avoided with proper planning and preparation. One of the biggest areas that can impact both the defensibility and cost of e-discovery is in evidence collection. The effective execution of this phase will have the greatest impact on improving overall e-discovery success, while at the same time lowering associated risks. In other words, if data is harvested and restored in a legally-defensible, forensically-sound manner, then the overall project will have a much better chance of achieving a favorable or expected outcome. Following are some common mistakes that are commonly encountered in the e-discovery world and some advice on how to avoid them in the future.

Blunder #1: On-Site Collection Must Begin Now!

A major law firm was representing a client in a backdating investigation. In facilitating the e-discovery process, the law firm was directing the collection of the evidence with its client. Without consulting with the client's IT department, the law firm insisted having a collection team on-site to gather evidence from 30 custodians, comprising more than 250 gigabytes of data. When the collection team arrived, the client wasn't ready. While some of the custodians were available, the IT department wasn't prepared to have an outside, third-party inside their operations area. The collection team waited a full day before collection could begin and then had to wait for the other custodians to show up the following week. What should have been a two-to three-day collection ended up taking over two weeks and cost five times more than budgeted.

Lessons Learned:

Including IT early on in the planning process will help ensure the legal team, both internally and at the law firm, fully understands what's going to happen on collection day and what preparation needs to take place prior to having the "strangers" come into the facilities to access the computer systems. They will also be able to develop more realistic timeframes and better understand the following:

1. Where are the custodians located, and what's the best time to collect the evidence with minimal disruption to the core business?
2. Does the client's IT staff have both the bandwidth and the technical acumen to collect the evidence in a legally-defensible, forensically-sound manner?
3. Does the client's IT staff have access to the right tools to harvest data correctly?
4. Will the client need third-party training or supervision when harvesting of the data?

Blunder #2: IT is Already on it!

A Fortune 500 company was facing a major class-action law suit involving 100 custodians and more than a terabyte of potentially relevant evidence. In preparation, the IT department had already begun collection using off-the-shelf software and hardware, such as Norton Ghost and Simple-Tech back-up hard drives. An initial testing of 10 custodian's collected drives showed that the hard drives were bad and that the metadata of the evidence was altered. When seeking technical support from the manufacturer, the company learned that the software that came with the hard drives was no longer supported and that the systems were primarily intended for migration, not e-discovery. The IT department had purchased 300 of these hard drive/software combinations with the intention of using them for other pending discovery matters. As a result, the client hired a third-party vendor to re-collect the data from the initial 10 custodians plus all the others. The process added an extra two weeks to the preservation process plus wasted IT time and expense that could have been spent on regular routine business operations.

Lessons Learned:

Most IT departments are tech savvy enough to run an empowered collection on their own with minimum interaction from a third party. However, there are cases where, in order to reduce risk, it may be a good idea to have the IT staff receive training on a particular tool set or have an outside third party provide minimal supervision at the beginning of the collection event. In determining how a collection should be performed and when it should begin, it's important to understand the following:

1. For what type of matter is data being collected, and how much data volume is anticipated?
2. What are the anticipated discovery production dates? How soon does the legal team need the evidence?

Fios

3. Are there any barriers to collecting the evidence?
4. Will data restoration services require any type of forensic analysis? Are deleted files, file fragments, or third-party e-mails an important part of the case?
5. Will data need to be collected from non-traditional systems, as well as workstations, e-mail servers and shared file systems?
6. Will there be any other loose media to be collected (examples: CDs, DVDs, USB flash drives, PDAs, etc.)?

Knowing the answers to these questions in advance of harvesting evidence will save time and expense when responding to discovery and can drastically lower the risk of collecting too little or not enough data.

Blunder #3: Forensic Images are a Must!

A major law firm was representing a Fortune 500 company in a product liability law suit. The law firm insisted on having forensic images, versus forensic copies, taken of all of the hard drives of the 120 custodian's computer systems. Following the collection, the drives were sent to the e-discovery service provider, who when then had to restore all of the files on the collected 120 hard drives into active files so they could be processed and prepared for review. The time and cost for the e-discovery collection and restoration stage doubled.

Lessons Learned:

There's a vast difference in both process and time when creating a bit-by-bit, forensic-image of a hard drive, which is stored in one or more binary container files, versus creating a forensic copy of the live data. Forensic images cannot be immediately loaded and processed into discovery platforms, like Prevail, and must be restored at additional time and expense before any such processing. Forensic copies are immediately loadable and processable and require no further restoration. The only difference in data content between the two is that a forensic image can allow for recovery of deleted files or file fragments. For most large e-discovery matters, creating a forensic copy of live files from potentially relevant repositories will be more than adequate. In order to determine which approach is necessary, one must understand the details of the matter and what level of collection is needed for defensibility. For example:

1. How much extra will it cost for a forensics collection – both in time and money?
2. What does the client hope to accomplish by conducting a full forensics collection versus a creating a forensic copy?
3. Is the recovery of deleted files or partial file fragments needed?
4. Is this a criminal matter or a quasi-regulatory investigation where there's a possibility of impropriety by one of the custodians?
5. Is this an Intellectual Property matter where there's a possibility of theft or abuse?
6. Have company policies been abused or has a contentious situation been created due to an employee departure?
7. Does the full forensics collection need to be done on all custodians or just a few select key targets?

These requirements need to be discussed with the third-party experts prior to collection commencing. And these are all part of the planning that should be done, in partnership, between the law firm, the client, the client's IT department, and the e-discovery services provider.

About the Author:

Karl Flusche has more than 20 years experience in hi-tech investigative operations and large scale electronic evidence discovery projects. As a Certified Fraud Manager (CFE) and the manager of Fios' Electronic Evidence Collection team, Flusche plans and directs all electronic discovery collection and forensic recovery projects for Fios' clients. He holds an M.A. in Business Management from Central Michigan University and a B.S. in Applied Mathematics from the University of Texas. He spent the first 10 years of his career as a special agent with the U.S. Air Force Office of Special Investigations.