A TANGLED TRAIL *of* DISCOVERY

JASON KRAUSE

How a special master's sleuth work helped resolve a business dispute

AS A COMPUTER FORENSIC EXAMINER, CRAIG Ball has a speech he likes to give to the owners of the computers he intends to search. In it, he's trying to dissuade them from deleting or destroying files.

"Whatever I find that's not relevant is kept in confidence. But if you're worried someone will see something private, the surest way to make sure someone finds out about your secret or your fetish is to start deleting it," he says. "It's like taking a yellow highlighter to what you don't want me to see."

Ball says he gave a variation of this message more than once—but most forcefully in an April 9, 2005, e-mail—to the defendants in the case of *Key Equipment Finance v. AmeriCap Credit*. But his words appear to have had little effect. In the coming months, he later testified, he found a trail of deleted electronic evidence, and that led to the case's quick conclusion.

Though it was a relatively normal business case that never went to trial, it is a case study in how electronic evidence is recovered and where it is found, as well as in the inherent difficulties in finding, preserving and authenticating electronic data. Traveling around the country seizing computers and analyzing data, Ball assembled enough detail that the case concluded even before it could get out of the discovery phase. Thanks to electronic records stored on employees' desktop computers and elsewhere, little remains secret.

"With information like phone records, credit card records and things like GPS, you can paint a rich, minute-by-minute insight into the life and even the thinking of an individual," Ball says.

THE CASE

IN 2004, KEY EQUIPMENT FINANCE, A LEASING COMPANY based in Cleveland, acquired American Express Business Finance Corp., formerly a business unit of the American Express financial company. In March 2005, unhappy with their new owners, a group of executives from that unit left Key to create AmeriCap Credit, a commercial finance company for construction and commercial vehicles. (The company, which is based in Oak Brook, Ill., changed its name to MeriCap Credit after securing $80 million in financing last April from a private-equity investment firm.)

Their departure might have been a straightforward solution to an unhappy union, except for some electronic documents.

American Express Business Finance, before becoming part of Key, hired a computer forensic expert to investigate whether the departing employees had misappropriated trade secrets. The inspector later testified he had made copies of former employees' hard drives and found reason to believe they had misused company resources: Not only had some workers used their computers to do work for AmeriCap while still on Key's payroll, the investigator said, but some had used a product called R-Wipe & Clean, which he described as "Department of Defense-level technology," to erase files.

Based on this preliminary work, American Express Business Finance filed a motion on Feb. 22, 2005, in U.S. District Court in Houston, seeking to compel AmeriCap to accept arbitration as American Express argued the former employees were required to do by the terms of their employment contracts. Saying AmeriCap employees had used confidential information in violation of this contract, American Express wanted to prevent them from abusing data such as customer and pricing information.

In cases like this, courts are struggling to deal with huge volumes of data and technical issues that were never before considered in trials. Amendments to the Federal Rules of Civil Procedure went into effect in December that address issues tied to e-discovery. But there is also a sense that e-discovery is a buzzword, confusing people as to what's really going on.

"Any attempt to distinguish e-discovery from discovery is fatuous," says Judge Lynn Hughes, who heard the case in Houston in the U.S. District Court for the Southern District of Texas. "Discovery is discovery."

But what digital evidence has done is change the volume and types of evidence a court might hear. That can lead to spiraling costs and protracted battles over what data means. When confronted with the apparent attempts to destroy evidence, Hughes decided to head off such a conflict and brought in a special master, something he says he's done only six times in 10 years.

Hughes thought of Ball, a San Antonio, Texas-based forensic examiner who had worked for the judge's court before. In particular, Ball had worked on a case in which he demonstrated that when one party was on the phone saying he was away from his computer, the man was in all likelihood actually sitting at his computer deleting files.

Hughes issued a March 14, 2005, order that simply read, "Craig D. Ball must conduct a computer forensics analysis of the defendants' home and office computers, including all computers that they may reasonably access."

Hughes concedes it was a broad order but says when he believes one side is not being forthcoming, it's better to be broad. The only problem is, someone forgot to tell Ball about his new job.

On April 6, 2005, Ball got a call from Jones Day attorney Ted Meyer, lead attorney for Key. Meyer told Ball that he had been appointed special master a few weeks before, and that he was to have already started work. It was a surprise, but Ball says when a federal judge

makes such a request, it's hard to say no.

FIRST STEPS

THE FIRST THING A FORENSIC EXAMINER NEEDS IS AN inventory of all the computer equipment a party owns. Then he has to consider which PCs are most likely to have relevant documents. And as the examiner starts copying the data from those PCs, it's also time to look for signs of tampering or misuse.

Ball sees a common, recurring scenario after people receive an order to preserve electronic evidence, and it shows up in the computer activity for the hours and days following the preservation order:

- First an individual starts searching for definitions of legal terms to find out what sort of jeopardy he or she is in.
- The individual then researches how to destroy computer data.
- Then computer or credit card records indicate the individual has purchased or downloaded software to erase computer files.
- Finally, there are often obvious signs that someone has run data-destruction software and, as a result, files are missing.

Ball decided to focus on the "low-hanging fruit," the computers most likely to produce responsive documents. The search began in the Chicago area, where the defendants had servers. On April 24, Ball holed up in an icy colocation facility, or server farm, with rows of computers locked in cages. Server farms are essentially rented homes for computers, refrigerated warehouses where servers are linked to their owners' offices by a network.

Working with two other investigators hired from a computer forensic firm, Ball later testified he found the computers were suspiciously lacking any real business data, even considering they belonged to a startup company. They had the necessary operating systems and software applications, but there was no real data. "It was like they were put in place for a stage set," he says. "The servers were essentially empty."

Ball checked visitors' logs for the facility and found company personnel visits that coincided with the setup of those computers just before his visit. As a new company, AmeriCap could be expected to have new computers and to have recently rented a brand-new colocation space. But what interested Ball was Vetrics, a company formed by a handful of former American Express information technology personnel who were working in Colorado and doing work for AmeriCap. He discovered Vetrics had computers in a server farm there and decided to investigate.

In Chicago, Ball and his team took turns sleeping in the colocation facility. In Englewood, Colo., he worked alone and slept with the computers, trying to collect information as quickly and efficiently as possible. But before Ball left for Colorado, he had filed a report and informed Hughes of his plan, and Hughes issued an unusual order that provided Ball with two federal marshals to assist him. "When Judge Hughes gets mad, he doesn't get loud, he gets quiet—and you'd better listen," says Ball.

On May 24, 2005, Hughes enjoined AmeriCap from destroying documents and chastised the company for violating his initial order. Hughes noted, "AmeriCap has deceitfully responded to narrowly tailored orders for the past three months."

Though AmeriCap officials denied it to him, Ball testified, he suspected the Colorado computers would prove to be the real workhorses for AmeriCap. He and the marshals spent Memorial Day weekend in Colorado visiting server farms and Vetrics employees' homes, downloading and copying computer information.

Though AmeriCap denied any connection to Vetrics, Ball says he found references to Vetrics employees being named as principals, stockholders and officers in AmeriCap. He found information like this by looking in what he calls the "sticky places" in a computer.

Sticky places are the millions and millions of bytes of information that are created on a computer every time it is used. Anytime a file is opened, changes are made, a video is watched or a document is created, the operating system makes copies of these actions and stores them in unused space on a computer. Eventually this information can be overwritten by other files, but more often it remains unaltered.

Ball notes that OLK storage, which is a temporary file created to allow users to open and read e-mail attachments, gave him access to copies of many documents. There were drafts of private placements or other financial spreadsheets, promotional documents, indemnification agreements, business plans and strategic information, he says. Some of these named Vetrics employees as AmeriCap employees, despite company assurances that Vetrics was just a hired information technology firm.

Ball testified he found copies of the court's preservation order on one computer even though the owner claimed ignorance of it. He could even pinpoint the time such documents were opened. And though some

files had been moved or deleted, metadata, or information about the documents, often revealed they were likely to have included proprietary American Express information, Ball testified.

Ball says he also found lots of information had been "deleted," yet he was able to recover much of it. That's because when someone hits the delete key on a PC, the Windows operating system actually leaves alone the ones and zeroes that make up a file. All it does is change information, alerting the system that the disk space containing the "deleted" data can be used by a new file. The original data remains in this unallocated space until the computer gets around to using that space for a new file—and since a modern computer has so much storage space, a lot of information is never overwritten. An experienced forensic examiner can find and reconstruct this deleted information fairly easily. Sometimes, even data that is partially or wholly overwritten can be recovered.

> "PEOPLE GET A FALSE SENSE OF SECURITY. THEN THEY ... DELETE THINGS THAT THEY SHOULD NOT HAVE WRITTEN."
>
> —TED MEYER

Looking for proprietary American Express information, Ball says he found what he called substantial volumes of its customer information, including financing data and schedules of payments in spreadsheets and other document types. But the case came to rely more on the destruction of data than on any evidence actually found.

The most important date in the case was May 24, the day Hughes issued the very strong "do not delete" order to the defendants. Ball later testified he found through his computer examinations that, on the same day as the court order, at 11:37 a.m. MDT, "many thousands of files" were deleted from one computer.

Another computer was so thoroughly worked over, Ball called it "nuked." Using a program called DBAN, a free application for download on the Internet, someone had overwritten every last bit of computer information on one computer so that all that was left was a brain-dead machine, Ball says.

Such a tool is brutally efficient at hiding information, but it is usually a giveaway of an attempt to hide information. Ball also found he could make even a brain-dead computer give up some useful clues.

The PC's owner argued he was just trying to do a thorough job of cleaning out his computer on March 3 before leaving for a new job. But Ball testified he noticed the computer's clock, one of the few things still running, reflected daylight-saving time, which went into effect on April 3. If the employee had wiped the computer on March 3, then the operating system would have been gone and the clock would have never been updated. That seemed to indicate the computer was wiped later than April 3, well after the court had issued its initial preservation order in March.

"On a lobotomized computer there would be no operating system to change the time," Ball notes. "The only way that I could see that could have happened is if the computer were nuked after someone had already changed the setting to account for daylight-saving time."

After imaging about 5 terabytes of data, Ball testified, preliminary exploration revealed proprietary information had been appropriated and data had been destroyed. Other, more tangible forms of evidence also came into play. For example, Ball noticed a BlackBerry stand and charger, but no handheld device.

After the May 24 order, Ball testified, he discovered deletions of thousands of files and more data moved to

A Case Time Line

Feb. 22, 2005—An American Express Business Finance complaint asks for injunctive relief and compelled arbitration, arguing that former employees of Key Equipment Finance, a firm it bought, had used company time and confidential secrets to start and promote a new venture, to be called AmeriCap Credit.

March 3—The U.S. District Court for the Northern District of Illinois orders the case be consolidated in the Southern District of Texas with Judge Lynn Hughes.

March 7—Plaintiffs request a computer forensic examination.

March 14—Hughes appoints Craig Ball special master.

March 15—Hughes issues a preliminary injunction that enjoins the defendant from using Key's proprietary business information.

March 31—Computer forensic examiner Richard Snevel testifies he found evidence defendants may have misused company computers and destroyed documents.

April 21—Hughes orders the defendants to allow Ball to examine computers or have the computers sequestered.

May 18—Key asks for sanctions against AmeriCap employees for destroying documents.

May 24—Hughes issues a more specific order that prohibits defendants from destroying documents, noting AmeriCap has "deceitfully responded to narrowly tailored orders."

June 2—A contempt hearing is held regarding AmeriCap employees' apparent defiance of court orders.

June 9—A settlement is reached as AmeriCap agrees not to use Key's proprietary business information or solicit business from certain Key customers.

storage media from computers. While he cautioned it is impossible to know whose hands were on the computer keyboard or whether most of that data was germane, there were enough files with suspicious names and evidence of tampering. He testified he was even able to trace copies of DBAN software that had been downloaded to disk and apparently distributed among a few key employees.

Computer data is so pernicious that even when an experienced user makes a concerted effort to destroy and alter evidence, all that may happen is that the efforts to conceal are documented. But it is also very difficult to say what the huge volumes of data that are discoverable mean without experienced computer experts involved.

With electronic evidence, a lot of information can be discovered and produced about when documents are created, when computers are booted, and how computers are used. But it is often impossible to know who was actually using a machine.

For example, Ball testified he found evidence a computer was repeatedly booted and moved. He was able to show that someone using different computers had downloaded data-destruction programs. He could see a computer had been turned on and off repeatedly. "That kind of pattern is something that I will sometimes see with individuals who are engaged in some change in the structure of the data on their computer," he told the court. "It could also mean someone just turns off the computer and goes to the bathroom every few minutes."

> "IT'S NOT LIKE PAPER, WHERE YOU PUT IT IN A BOX AND LET IT SIT THERE UNTIL SOMEONE NEEDS IT."
>
> —JULIA NYE

CASE SETTLED

IN THIS CASE, HUGHES CAME ACROSS AS FAIRLY TECH savvy. He hired an experienced forensic examiner to handle discovery (not a crony or old law partner, as is known to happen in courts). And he was willing to ask questions, even ones that might sound stupid, to clarify issues such as whether an expert witness was talking about an e-mail inbox or a regular mailbox.

The combination of evidence of misappropriated information plus the signs of destroyed files and computers wiped clean made for an ugly picture. Still, attorneys say, even though digital evidence is more voluminous, it functions like paper in court. "If we'd have found paper memos, we'd have done the same things," says Jones Day's Meyer. "But we're much more likely to find something on a laptop or e-mail server."

Attorneys say one reason there is so much digital evidence is that it is easy to create, so people have a cavalier attitude toward writing e-mails. "In general, people get a false sense of security," says Meyer. "Then they hit the trash button to delete things that they shouldn't have written."

Meyer says more lawyers and business operators should be trained in what happens in e-discovery. Lawyers should advise clients about what can be discovered from a laptop, desktop, phone or handheld. In addition, clients should be told how to avoid the perception they are hiding or destroying data. Sometimes merely updating a document can be misconstrued as an attempt to conceal. "It's not like paper, where you put it in a box and let it sit there until someone needs it," says Julia Nye, a Jones Day associate who worked with Meyer on the case. "You have to actively preserve and protect digital documents."

Hughes says one reason he hired a forensic expert was that he could see an ugly fight breaking out, and he could see costs getting out of control. Even so, the discovery issues wound up costing well over $100,000. And that's for a case that never got past the early phases of discovery. In the final accounting, AmeriCap paid the cost of discovery.

On June 2, all of Ball's work came to fruition at a contempt hearing with the defendants, their lawyers and the federal marshals listening in. Ball testified at length about his efforts but had to leave early for a speaking engagement. But observers say the defendants looked decidedly uncomfortable and, after a lunch recess, they decided to settle the case. *Key Equipment Finance v. AmeriCap Credit*, No. H-05-0585.

AmeriCap and the attorneys who represented the company for most of the trial didn't respond to repeated requests for comment. But it should be noted that this case is simply a business case that became hung up on some specific problems with spoliation, and Vetrics and AmeriCap never got a trial on the business dispute the case was really about. Instead, the actions of a few employees angered the judge and put the company in a difficult position. So they accepted arbitration.

In the end, Key won an order prohibiting AmeriCap from using specific business or pricing information or from soliciting business from customers on Key lists.

As for the role of digital data in the case, Ball had this to say: "Think of it this way—all the garbage you threw away in the last year was taken to the garage and stored. Some deteriorated, but all the wrappers, correspondence and bills were there.

"We keep such a wealth of information now, the variety of which is greater than ever before." ■

Jason Krause is a legal affairs writer for the ABA Journal. *His e-mail address is krausej@staff.abanet.org.*