BY KEITH G. CHVAL

Chain of Custody

Recent incidents have shown how important it is for colleges and universities to preserve evidence — including digital evidence — that may be required in a legal investigation.

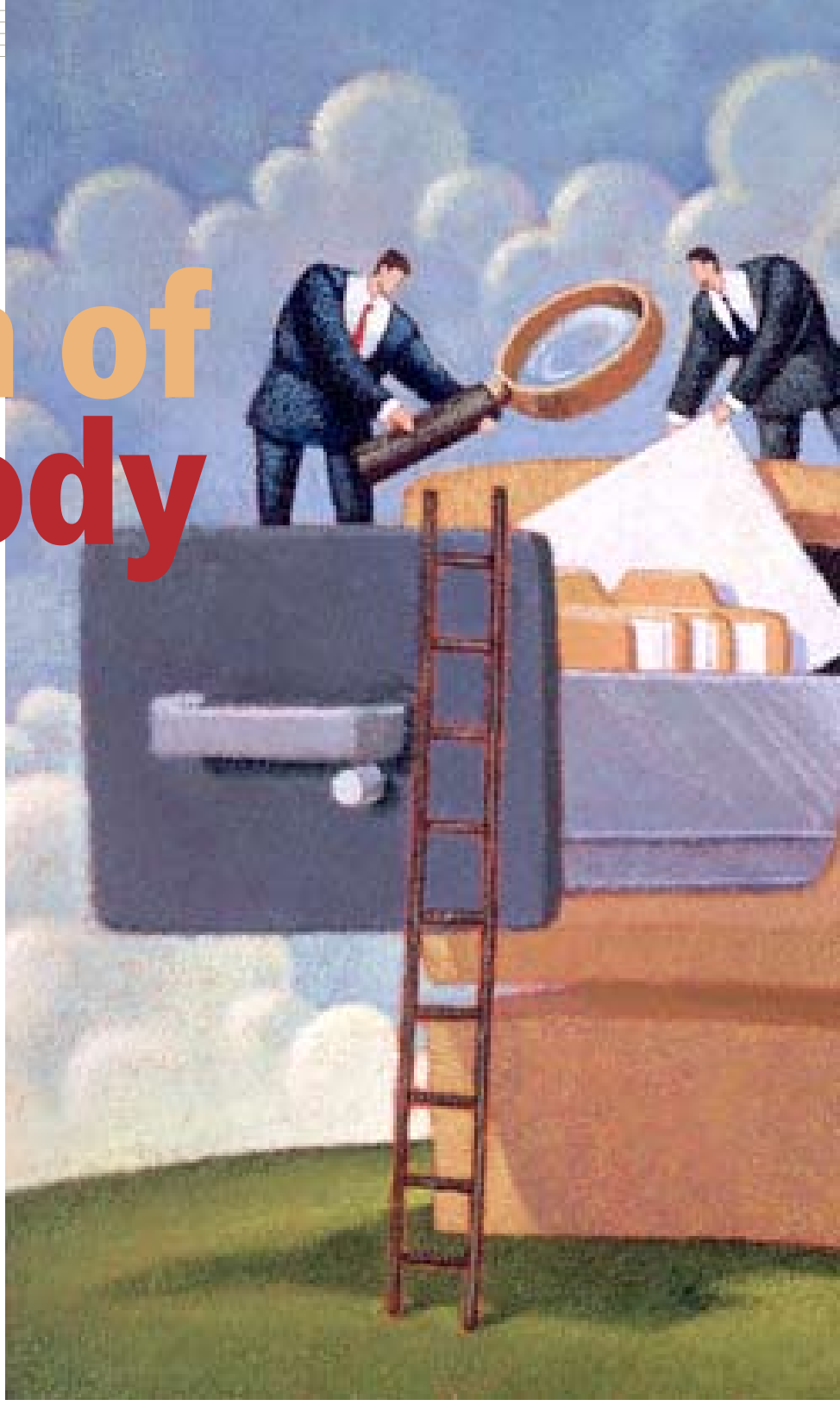


ILLUSTRATION BY LAEL HENDERSON

"Hey Jon, I need the chain of custody."

"The what?"

Your general counsel has just stopped by your office and dropped that bombshell on you as you were drinking your morning cup of coffee.

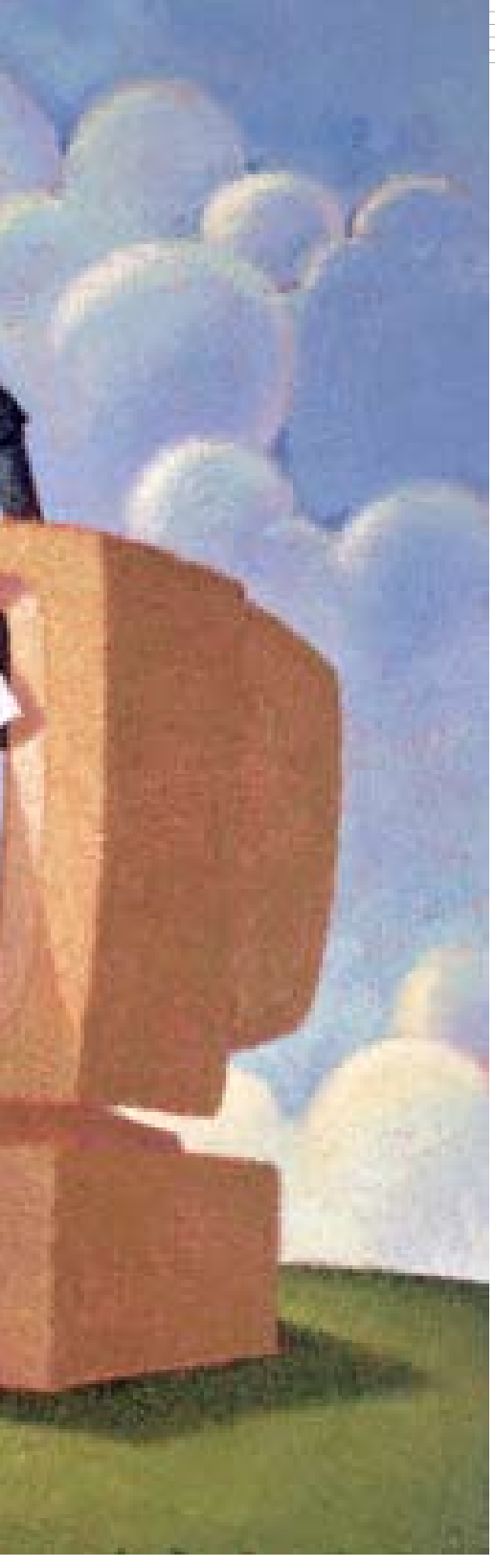
"Remember all those e-mails and other electronic files you gave us in connection with that internal investigation of Smith last summer? Well, the case is going to trial, and we need the chain of custody to prove that Smith really wrote all those things. Without the chain of custody, the judge won't admit any of that information, and we'll get killed at trial."

If "chain of custody" is a new or vague concept to you, you're not alone.

In simplest terms, a proper chain of custody establishes the integrity of a piece of evidence, showing that it wasn't tampered with or otherwise altered since it was first collected.

While chain of custody is a legal term of art — meaning it has a specific meaning in the law and can have legal consequences — it has significant practical implications for IT managers and other professionals.

"Although it plays a critical function in litigation where opposing counsel is challenging the authenticity of evidence — particularly where digital evidence is involved — I've found that there are very few who adequately account for the chain of custody, let alone appreciate its importance," observes Scott Carlson, a partner in the Chicago office of Seyfarth Shaw,



whose practice focuses on electronic evidence and complex litigation.

Where's the Proof?

To illustrate the significance of chain of custody, let's go back to the original anecdote. While the electronic files you were able to produce from Smith's computer proved that he was sharing proprietary information with your competitor, getting those files into evidence at trial is an entirely different matter.

Opposing counsel will challenge the integrity of the files and may claim that the court should not allow that evidence because it was altered, deleted or inserted long after Smith last set foot on your premises. Your attorney is going to need sworn testimony from you, or someone on your staff, to overcome this attack.

Rules of evidence require that a party seeking to admit an item of evidence must first prove that the item is what the party claims it is. In the world of digital evidence, even a modern-day Perry Mason might be left scratching his head.

How do you establish that the critical e-mail you found through your examination of a copy of Smith's hard drive is from the same set of ones and zeroes that existed on his computer when you seized it 18 months ago? It's not as if you could crack open the case on Smith's computer, pull out the hard drive, open it and say, "Aha, I'd recognize those ones and zeroes on that hard drive platter anywhere!"

The chain of custody is the device that the proponent of an item of evidence uses to authenticate that an object is what it purports to be. In this case, it establishes that the e-mail comes from the set of ones and zeroes that were present on Smith's hard drive on the day it was taken into custody.

Collect and Preserve

"Early in my career, we used the chain of custody to show that a particular packet of heroin was the same packet that we seized from a drug dealer, even though one packet of heroin looks like any other packet of heroin," explains Dan Bellich, who retired after 27 years with the FBI to form Protek International, a computer forensics and investigations firm in Clarendon Hills, Ill. "With digital evidence, we use the chain of custody in the same way: to establish that otherwise indistinguishable digital evidence is the same as what was previously seized from a bad guy's hard drive."

The chain of custody provides a road map for the handling of electronic evidence from beginning to end by recording on an evidence log all items that have been collected and tracking in chronological sequence every individual who has had custody of each object. IT managers should work with general counsel to develop and implement a plan for collecting and preserving electronic data in order to maintain a solid chain of custody.

However, before even beginning to collect evidence and create the chain of custody, other potentially valuable evidence needs to be collected at the scene of the crime (in this case, Smith's workspace). Before moving or touching anything there, steps should be taken to record the location and condition of the computer and other items in Smith's workplace. A digital camera and a notepad can be handy tools for capturing evidence such as what was on Smith's computer screen when investigators arrived.

> **"There are going to be times when it's tempting to forgo collecting and maintaining the chain of custody. Don't succumb!"**

Now that the scene has been documented, the process of constructing the chain of custody begins. As each item is carefully collected, it should be marked with a unique identifying number to allow you to locate and track that item. An example in Smith's case might be "06 Smith A 1.1," where 06 refers to the year, Smith is the name of the investigation, A refers to items related to his computer system, the first 1 is the group of peripherals and the

second 1 is the number for the monitor.

The person collecting this item should initial or sign and date the item so that when authenticating it in court, he can explain that he knows this is the monitor he collected from Smith's office because it has the evidence label that includes his handwritten signature and the date it was collected.

The evidence number for all items is recorded on the evidence log, and a record is created of every person who handles that evidence. Those individuals should also be prepared to testify about how they stored the evidence. The record is kept until after the investigation or court proceedings, when the evidence is no longer needed and is not required to be maintained.

The proponent of an item of evidence also must be able to establish that the evidence is in substantially the same condition as it was when it was taken into custody.

"Because digital evidence is more susceptible to intentional or inadvertent alteration or destruction than many forms of evidence, it is critical that a witness be able to offer evidence upon which the judge can conclude that the data is in substantially the same condition as when it was seized," explains Patrick Zeller, a former high-tech prosecutor and litigator who is now assistant general counsel for Guidance Software, a Pasadena, Calif., computer forensics software developer.

Critical areas for establishing this aspect of authenticity include confirming that there are no missing links in the chain of custody; detailing how your storage facility is inaccessible to unauthorized individuals and has proper climate and environment controls; and demonstrating how the tools and processes utilized by your examiner are used in such a way as to not alter any of the data in the course of the examination.

Even with helpful testimony on all these points, you still can't testify, "I saw the ones and zeroes and electromagnetic dust 18 months ago, and what is before us today is in substantially the same condition as it was back then."

However, you do have the next best thing — what's called a hash value. This value is created when a sophisticated algorithm is run against a particular set of data, such as a file, CD or hard drive. The extraordinary unlikelihood of two different data sets generating matching hash values is sufficient to allow a judge to rely on matching hash values as sufficient evidence of authenticity.

By obtaining a hash value as quickly as possible after taking custody of an item of digital evidence and then demonstrating that it matches the hash value of that same evidence at a later date (or a duplicate forensic image that you are working on), you can take the wind out of the sails of any arguments by opposing counsel that the data was changed after you took custody of it.

Chain of Custody Checklist

- Have a plan before an incident occurs. Identify your "go-to" people, whether in-house or outside, while the waters are still calm.
- Do not touch the computer unless you are experienced in digital forensics. Thousands of files are altered simply by turning it on.
- Document the location and condition of everything before touching anything. A digital camera can help.
- Systematically collect items of evidence, marking and recording each item with a unique number.
- Record the date, time, personnel and purpose for every transfer of custody.
- Store evidence in a secured, climate-controlled location, away from other items that might alter or destroy digital evidence.
- Computer forensic examiners should be able to testify that they have validated that their tools and processes do not create alterations to the data.
- Hash values of files and/or media should be created as early as possible.

A Shield and a Sword

Proper evidence handling and chain of custody provide both a shield and a sword for the credibility and persuasiveness of your digital evidence. First, opposing counsel is either going to shy away from this line of attack because a strong chain of custody makes it apparent that you have handled the evidence properly, or they are going to lose credibility with the judge or jury by wasting their time on a pointless matter. Second, the persuasive value of your digital evidence is bolstered, and your credibility is enhanced.

With all the responsibilities placed on busy professionals today, there are going to be times when it's very tempting to forgo collecting and maintaining the chain of custody. Don't succumb!

Take the time to develop and implement your chain of custody and evidence handling protocols. You will be thankful when you're in court and your smoking gun e-mail nails a conviction. ■

Keith G. Chval is a principal with Protek International, a computer forensics, litigation support and investigations firm, and a member of the law firm of Connolly, Ekl & Williams PC, both based in the Chicago suburbs.