



Chain of Custody

How the Phoenix RSM™ video lifecycle management solution provides proper video surveillance Chain of Custody capabilities

A Brief Introduction to Chain of Custody

Chain of Custody legal definition: The order of places where, and the persons with whom, physical evidence was located from the time it was collected to its submission at trial.

—Webster’s New World Law Dictionary

Chain of Custody is a familiar concept in criminal law, but until recent years it was foreign to civil litigators. In the criminal law arena, police would seize evidence, seal it in a plastic bag, label it, and sign it in to a locked evidence room. If the evidence was taken out by anyone for any purpose (for example, for laboratory examination or testing) that withdrawal would be noted on the log, as would its return. The next removal from the room would likely not be until its presentation at the trial itself.

Historically, evidentiary chain of custody was rarely an issue in civil litigation. With the advent of the digital age, however, it has become a major issue because the actual nature of evidence in civil litigation has undergone a radical transformation—from tangible paper to intangible electronic data.

Regarding the importance of chain of custody, before a physical object connected with the commission of a crime may be admitted in evidence, there must be a showing that the object is in substantially the same condition as when the crime was committed (Gallego v. United States of America, 276 F.2d 914 9th Cir. 1960 citing United States v. S. B. Penick & C., 2 Cir., 136 F.2d 413, 415 (2d Cir. 1943)). Chain of custody testimony would include documentation on how the evidential data was gathered, transported, analyzed, and preserved for production.

This information is important to assist in the authentication of electronic data since it can be easily altered if proper precautions are not taken. Gallego affirms that proper chain of custody is valid when there is “...no likelihood of intermeddlers tampering with it.” It is also much more complicated to handle electronic data as evidence than it is to sign in tangible narcotics confiscated

at the time of arrest and sign them out again at the time of trial. Because of this, electronic discovery is a multi-stage process and custody is an issue at every one of those stages.

Stages of Electronic Discovery

The generally accepted stages of the electronic discovery process are:

1. identification (determining the scope, breadth and depth of “electronically stored information” (ESI) needed)
2. preservation, (maintaining the integrity of the ESI) collection, (gathering ESI from various sources)
3. analysis (determining relevant summary information)
4. presentation as evidence during trial (effectively presenting the ESI at depositions, hearings, and trial)

The requirements for maintaining the chain of custody applies to all stages of the electronic discovery process, and because the discovery process has so many steps, the chain of custody can be very long and convoluted.

The “Amended Federal Rules” require the preservation and disclosure of ESI. The admissibility of ESI will hinge, in part, on laying a proper foundation for the electronic evidence. Often, the chain of custody for digital information involves 1) describing the methodology used, 2) logging all subsequent transactions with this ESI, and 3) the actual chain of custody of the ESI itself during and after the retrieval process. The foundation for admissibility of ESI may be attacked by objecting to any prong of the process.

In short, “You have to explain what this evidence is, where it came from and where it went, and there can’t be a gap,” explains Dana Lesemann, vice president and deputy general counsel of Stroz Friedberg, a consultancy that specializes in computer forensics and investigations.

As you will see, SoleraTec’s Phoenix RSM properly logs and maintains the Chain of Custody that will assist in the admission of electronically stored information as evidence within a legal setting. Phoenix does this in three distinct ways: digital fingerprinting, video watermarking, and audit trails.

Digital Fingerprinting

Phoenix RSM automatically assigns a digital fingerprint to all data ingested into the Phoenix Information Repository.

A digital fingerprint is a unique number assigned to each file using a mathematical equation using information about the file itself. The result is a numerical value that is completely unique to the file assigned, which cannot be duplicated should the file be changed in any manner. In the computer industry, this value is known as a “hash algorithm.”

Phoenix RSM utilizes the standard SHA-256 hash method of assigning a digital fingerprint to each ingested or captured digital file. SHA stands for “Secure Hash Algorithm” SHA-256 is similar to the more widely known MD5 hash and is part of the SHA-2 family of algorithms. MD5 is a 128-bit algorithm, SHA-1 is a 160-bit algorithm, whereas SHA-256 is a 256-bit algorithm. The SHA hash functions are a set of cryptographic mathematical functions which convert a large, possibly variable-sized, amount of data into a small datum, usually a single integer set as an index. The SHA-256 hash was designed by the National Security Agency (NSA) and published by NIST as a U.S. Federal Information Processing Standard. SHA-256 is patented under US patent 6829355. The United States has released the patent under the Fair Use allowance.

What is a hash value and how is it utilized?

A hash value is a digital fingerprint. It is applied to a file and recorded. The hash value will change if even one bit of data in a file is changed or altered. Digital files can be externally validated to a properly generated SHA-256 hash with independent third-party hash key generators. Simply upload a file to one of these external validating systems and the appropriate SHA-256 hash key will be displayed. Compare that key to the Phoenix RSM digital fingerprint to insure authenticity. If the hash is the same, the file has not been changed in any way.

The digital fingerprint within Phoenix RSM is stored with its corresponding data file and is checked at every stage of management or access. If the data has been altered intentionally or through hardware/software failure, the system will flag the inconsistency.

Video Watermarking

In order to indicate that a copy of the original high-resolution file is being reviewed, Phoenix RSM will embed a constant background image—a watermark—into the copy of the digital video file anytime the original file—or a segment (“clip”) of the original file—is being exported or copied to a location outside of the Phoenix Information Repository. Thus, whenever you are viewing a video asset and this watermark is visible, you can rest assured that you are looking at a properly obtained copy of the original

video asset. Conversely, when there is no watermark and the digital fingerprint matches, you are able to ascertain that you are looking at the original file.

Audit Trail

Phoenix RSM provides a security audit trail through activity logs. These activity logs include the following events: file read, file write, file create, file delete, media load, media unload, and media erase. For these events, the following information is recorded: name and IP of the user who executed the event and the date and time the event was executed. Logs will also contain the SHA-256 digital fingerprint. As every Phoenix Vault is queried for the specific file in question (as it may have been migrated or replicated throughout the Phoenix federated Information Repository), a log entry is made each time a file is read, accessed, replicated, or migrated.

A model of this logging process that many users have experienced is the online FedEx or UPS tracking systems. When a shipper uses one of these services, the shipper sends the recipient an e-mail with a tracking number. By inputting the tracking number on the FedEx or UPS websites, the recipient can track the shipping progress of the package across the country or across the world. These tracking systems are updated with all key progress information usually within minutes or a few hours of the event. In a similar fashion, every step of the interaction with the ESI is logged for review and to verify admissibility in court.

SoleraTec’s Phoenix RSM solution properly protects and manages evidentiary assets so that they will hold up in court. To prove chain of custody, you will need to document the details of how the evidentiary file was handled every step of the way.

Confirmation and Production of Chain Integrity

Production of electronic documents is usually a two step process. The first step is discovery, and the second step is the legal review. The discovery component is conducted using an e-discovery search tool, such as Phoenix RSM, to identify all documents that match a set of criteria commonly associated with the documents required for review.

The e-discovery tools built into Phoenix RSM make it easy to generate a simple search query that will locate all documents with a common element, (such as a case number or camera id). Phoenix RSM’s unique “criteria stacking interface” can also be used to build highly complex, multiple component search queries that can produce relevant search results to a few documents that share multiple, unique criteria.

The review process of the documents discovered is usually conducted by a smaller subset of personnel with higher security privileges, as the documents being reviewed are normally sensitive and private in nature. Again, Phoenix’s standard e-discovery tools easily accommodate this necessity.

After a legal review is completed and the reviewing party has chosen which electronic documents to produce to the opposition, it is time to regenerate the hash algorithms to verify that what is being produced is identical to what was first collected. It is essential that incoming evidence generates these hash-value keys on the incoming evidence well before handling it in any other manner. Phoenix RSM automatically generates these hash-value keys on ingest or video capture. This is a crucial action in preparation for the next stage.

Once the forensic copy of the relevant video segment has been obtained, it can be burned onto a CD or DVD for submission to the court or legal counsel. This CD or DVD should be placed into a sealed envelope with the digital fingerprint, date, and reviewing personnel information.

Again, the process as mentioned above would be completed by utilizing a third party file validation service (and you can download a third-party hash generator for file validation at <http://www.softpedia.com/get/System/File-Management/Easy-Hash.shtml>).

Presentation at Trial

In the eyes of the court, it is accepted that a carefully protected clone of a digital asset is as good as the original digital asset. The first clone of a digital asset that investigators take has become known by a number of monikers such as “best evidence,” “forensic copy,” and “file clone.” For the purposes of this document, we will refer to this clone as the “forensic copy.” Best Practices demand that, at this point, an additional copy—or working copy—should be made, either from the original or from the forensic copy, and all further processing, review, and analysis be performed on this working copy. The forensic copy should then be secured in such a fashion as to avoid any alteration, damage, or spoliation. All further logging of custody will be done with respect to the forensic copy of the ESI.

The court will therefore accept the foundation for the forensic copy and approve its admissibility. This type of forensic acquisition has been effectively employed for years and has resulted in a forensically defensible chain of custody.

A forced purge (or destruction) of the data at end of the court case may also be required. Phoenix RSM is designed to purge selected files or group of files from its repository through a manual or automated process.



www.SoleraTec.com • Tel: (760) 743-7200 • Email: Info@SoleraTec.com
SoleraTec Headquarters: 2430 Auto Park Way, Suite 205, Escondido, CA 92029

© 2010 SoleraTec LLC All rights reserved. SoleraTec, SoleraTec logo, Phoenix logo, are trademarks of SoleraTec LLC. All other third party brands, products, service names, trademarks, registered service marks are the property of and used to identify the products or services of their respective owners. All specifications are subject to change without notice.

In Review

SoleraTec’s Phoenix RSM is a professional video lifecycle management solution that performs digital fingerprinting, video watermarking, and audit trail functions automatically. By simply utilizing the Phoenix RSM’s core technology, robust Chain of Custody is handled automatically for the end-user. Using the following three steps, any user can ensure they have a proper Chain of Custody system:

Step 1: Review the Digital Fingerprint

Utilizing Phoenix’s digital fingerprinting functionality, you can rest assured that the file you have is an exact clone of the file that was originally ingested.

Step 2: Review the Video Watermark

With video watermarking, you can be certain that you are viewing a properly obtained “forensic copy” of the originally file. And when you do not see the video watermark, you know that need to validate the digital fingerprint, which will indicate whether you are looking at the original file.

Step 3: Review Phoenix Vault activity logs to show Chain of Custody

With Phoenix RSM logging all file read, file write, and file create activity, the log files present a documented history of the overall chain of custody that can highlight the digital fingerprint and video watermarking activities as well as any migrate actions the file may have encountered while under Phoenix RSM management.

Summary

By utilizing the three-step approach to a proper chain of custody, as outlined in this paper, any and all ESI that is collected can be considered for admissibility into a court of law.

The above steps, which are comprised by the built-in functionality of the Phoenix RSM video lifecycle management solution, support a “Best Practice” scenario to meet ideal chain of custody requirements.

About SoleraTec

SoleraTec is a leading developer of archive, storage, asset and video lifecycle management software for corporate customers. SoleraTec leverages a heritage of nearly a decade and a half to deliver a level of quality, sophistication, and technological advancement that has established it as one of the premier data protection solution providers in the industry. SoleraTec works through OEM, dealer, and integrator relationships to deliver complete data protection solutions. The company was established in 1997 by a team of industry veterans with experience deploying data protection, HSM, and storage lifecycle management solutions to some of the largest companies around the world.