# Maintaining Chain of Custody in Digital Video Surveillance

## The Importance of Building a System with Best Practices

**May 2014**

## Contents

## ABSTRACT

When physical evidence is seized during an investigation, it is carefully tracked and stored, maintaining a chain of custody to ensure that the items can be proved to be legitimate when used in court. Digital evidence presents additional challenges, given that it can be copied and modified easily. However, courts still require that a chain of custody be used to prove that the digital evidence is legitimate. This white paper covers the techniques that have emerged to ensure that an unbroken chain of custody can be proved with digital evidence.

## INTRODUCTION

"Chain of custody" is a legal concept based on how evidence seized in an investigation must be handled. Maintaining the proper chain of custody proves that items were not tampered with and are valid as evidence. Every time the item is moved, the move and owner must be logged, from the point of seizure until the da the evidence is presented in court, and even afterwards. Chain of custody with physical evidence is simple. When an item is seized in an investigation, to be valid as evidence, and to ensure it was not tampered with, its every move is logged. This occurs from the point of seizure until the day (and even after) the evidence is presented in court. Depending upon the item, size, etc., the item usually goes into an evidence locker and check-outs are logged meticulously.

*To be admissible in court, electronic data must show an "unbroken chain of custody".*

The advent of digital data has changed the traditional systems of evidentiary control. Digital files can be edited and readily changed. To be admissible in court, electronic data must show an "unbroken chain of custody". In other words, the presenter of the evidence needs to provide ample proof that the data is just now, exactly as it was created, in its entirety, without the possibility that the evidence was altered, deleted in part, tampered with in any other fashion. [1]

Even data files that appear pristine can be questioned and determined to be inadmissible in court, if no precautions have been taken to protect the data. Precautions include:

- What kind of machine/device held the electronic evidence (is a serial number present)?
- Who had access to the machine/device?
- Who owned the machine/device?
- Was the machine/device shared?
- Was information retrieved from a network?
- Was information password protected?
- Who had access to the password-protected information?
- Is the data located at an off-site location?"[2]

[1] Online Law IT Wiki, http://itlaw.wikia.com/wiki/Chain_of_custody

[2] Ibid

## Standards for a Digital Chain of Custody

The essential standards for a physical chain of custody apply to a digital chain of custody, but the possibilities for how the digital evidence has been treated are much broader. Consider the following definition. The online IT Law Wiki defines chain of custody as "a process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred and the purpose for the transfer."[2]

*Any broken link in the chain of custody can be cause for dismissing the evidence, in turn, causing the party to lose its case, regardless of innocence or guilt.*

The answer for "where was the evidence when it was collected" is simple for physical evidence. For digital evidence, the answer is more complex … Consider the following questions:

1. What kind of machine/device held the electronic evidence? (Is a serial number present?)
2. Who had access to the machine/device?
3. Who owned the machine/device?
4. Was the machine/device shared?
5. Was information retrieved from a network?
6. Was information password protected?
7. Who had access to the password-protected information?
8. Is the data located at an off-site location?"[3]

Ensuring that this information is available, or that these questions do not raise doubt as to the validity of the evidence, is a complex process.

The intent of a well-designed video surveillance system is to create video evidence that can be used in any court, in any situation, without question of its quality and authenticity. While there is some legal precedent to allow digital evidence with weak or broken chain of custody, depending upon the case and what is at stake, it is more the norm to classify it as inadmissible. Developing a solution that ensures there is and always will be a strong chain of custody should be the goal.

In order to create a solid chain of custody for digital evidence, the party entering the evidence must provide the following:

- An unbroken, linear timeline, showing the chronological activity of events, including the video that captured the event, how the event was stored digitally, who had access to the data, and what happened to it from the time it was stored to the time of entering the evidence.
- Proof of the controls in place to ensure the video is the same, unaltered digital video file as the day it was stored.

[3] Online Law IT Wiki, http://itlaw.wikia.com/wiki/Chain_of_custody

- Proof that the video itself and the timeline are free of any gaps, periods of time during which the exact custody and location of the evidence cannot be accounted for.

The following quote from Picciotti & Schoenberg describes specifically requirements for a chain of custody with digital evidence. "… a complete chain of custody is not strictly required, it is wise to develop as complete a chain of custody as possible, both to ensure authentication of the evidence and to enhance its credibility. Every transfer of either electronic data or physical data should be documented in Movant's (the party that makes a motion in a case) chain of custody. This would include a record of all copying of data whether it is the hard drive in toto or its electronic transit through the Movant VVS system from Master File to Archival File to Laptop File to Desktop File to Portable File. The chain of custody records must themselves be well maintained to ensure their admission into evidence as business records. Submission of the chain of custody into evidence will generally require testimony from a Movant witness who has knowledge of the chain of custody process."[4]

## Practices that Damage the Digital Chain of Custody

In some cases, usually due to digital storage limits, some organizations will purposefully alter digital data, by reducing the frames per second on the data already stored, erasing data for times with no activity, etc. These practices are not recommended, as doing this eliminates the chain-of-custody. Other solutions exist for solving the data storage problem. The following example expands on this issue:

"In Jenks v. Port Authority, No. 2:06cv 1428, 2008 U.S.Dist. LEXIS 64588 (W.D. Pa. 2008), plaintiff based a claim for false arrest and imprisonment on defendants' reliance on surveillance tapes that contained time gaps. See id. at *1, *8. The surveillance tapes recorded in a "time-lapse" manner at 5 frames per second and were found to have gaps of from five to sixty seconds at various places on the tapes.[1] Id. at *8, *9. Jenks had been arrested and charged with making false statements when he reported that he had been accidentally struck by a scrubbing machine while at work, but the incident was not shown on the surveillance tapes. Id. at 7-8. The Court recognized that Jenks could have been struck by the machine at a time when there was a gap in the tape, and permitted his Section 1983 false arrest claim to go forward."[5]

The risk of a break in the chain of custody is that it poses a question or doubt as to if the evidence is true or if it may have been altered in some way. Typically, courts will require an opposing party to show evidence that alteration of the data or evidence has in fact occurred. However, depending upon the circumstances in the case and motivations, along with access and capability to modify data, giving the

[4] Online Law IT Wiki, http://itlaw.wikia.com/wiki/Chain_of_custody

[5] Picciotti & Schoenberg on Digital Evidence- General Objections to the Introduction of Video Evidence in Court, http://lxtch.com/blog/2013/06/05/picciotti-schoenberg-on-digital-evidence-general-objections-to-the- introduction-of-video-evidence-in-court/

opposing party the ability to present a sufficient question as to the evidence's authenticity opens the door to the court finding the evidence inadmissible.

## The Need for a Digital Chain of Custody

A video surveillance system that cannot ensure that its video evidence has an unbroken chain of custody and is admissible in court is virtually worthless, and the money spent on it is wasted. Failure to meet these standards means a broken chain of custody, and possibly cause for dismissing the evidence. This in turn can cause the party to lose its case, regardless of innocence or guilt.

The best course of action is to implement a system of processes, procedures, and equipment that eliminate the possibility of data alteration and show a clear chain of custody.

## Solution - Automated Digital Video Surveillance Solutions with Chain of Custody

Cost-effective digital video surveillance systems, which incorporate chain of custody best-practices, are now available from Spectra Logic. These automated solutions include disk and digital tape, and ensure that unedited/unaltered, uninterrupted, high-resolution video is stored linearly, with metadata, containing time- stamp and other information about the data, . The video can be stored on disk and on digital tape. Verified copies can be made from the high-resolution digital tape, while always maintaining an original file on tape. Verification can be done against the low-resolution and thumbnail files on disk.

*The best course of action is to implement a system of processes, procedures, and equipment which eliminate the possibility of data alteration and show a clear chain of custody.*

In order to make a change that would be undectable by the Spectra solution, an individual would need not only need access to the video but would need access to three streams of data on two separate mediums, and would need to change the individual times stamps in the data of all three streams. This is virtually impossible to do without detection because of the systems and technology implemented in the Spectra solution. When these are combined with proper processes and procedures to limit personnel access, rock-solid chain of custody is maintained and can be demonstrated in any situation.

See Figure 1.

*The solution allows many layers of fencing/ protection to ensure chain of custody is maintained. The digital tape storage tier also provides additional protection by automatically making a redundant copy of original surveillance video and databases, with time-stamps and other key metadata.*

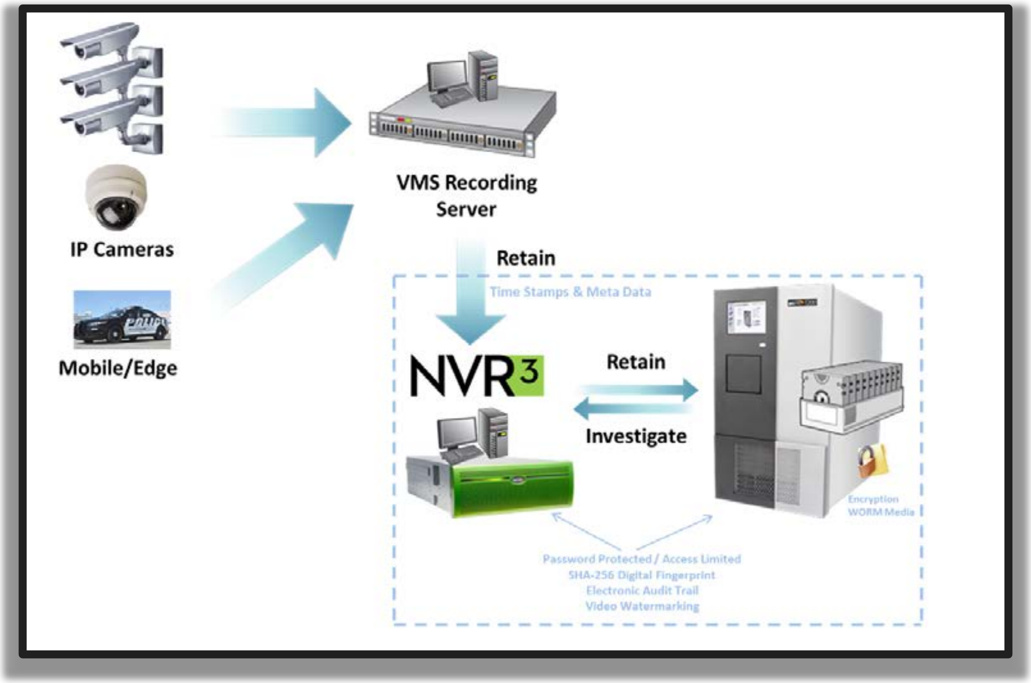

**Figure 1: Spectra video surveillance archive solutions**

The chain of custody is supported with the following:

- Password-protected access
- Storing copies on two different locations (tape and disk)
- Encryption
- Tape removal and load alerts
- Digital fingerprinting
- Video watermark
- Audit trail
- Write Once, Read Many digital tape

## Password-Protected Access

The solutions offer the capability of limiting access, by requiring passwords.

## Dual Media Storage

The video is stored in two forms; the original and the condensed thumbnail version. A user would need to modify both in exactly the same way for the modification to not be noticed.

## Encryption

Encryption can be enabled on the digital tape storage, so even if a tape is removed from the system, it can’t be read or altered.

## Tape Load Alerts

A trigger can be set up to alert the operator when a tape is loaded into the system that has been previously loaded on a tape drive but not in that tape library.

## Digital Fingerprinting

The Spectra solution assigns a digital fingerprint to all the data ingested into the information repository. This is a unique number assigned in a hash algorithm, known as SHA-256. SHA- 256 is a 256-bit algorithm developed by the National Security Agency (NSA) and published by NIST as a U.S. Federal Information Processing Standard. The hash algorithm assigns a unique identification string to every file ingested. If even a single character is changed in a file, the changed file will be given a new, totally different identification string, making it very easy to spot file changes and ensure the data is just as it was originally ingested.

*If even a single character is changed in a file, the changed file will be given a new, totally different identification string, making it very easy to spot file changes and ensure the data is just as it was originally ingested.*

## Video Watermarking

The software in the Spectra solution embeds a constant background image, a watermark, into the copy of the digital video file anytime the original file (or clip of the original file) is being exported or copied to a location outside of the repository. Any time a copy of a video asset is being viewed and the watermark is visible, that indicates the copy was obtained properly. Either a watermark which is present or a copy with a matching digital fingerprint (and no watermark) tells the operator that they are looking at the original, unaltered file/copy.

## Audit Trail

The solution also creates activity logs that provide a security audit trail. The logs track all relevant events, such as file written, file read, file create, file delete, media load, media unload, and media erase. For each event identified, the following information is recorded: the name and IP address of the user who executed the event, the SHA-256 digital fingerprint, the date of the event, and the time the event was logged. Also, a log entry is made every time a file is read, replicated, or migrated. Through these logs, it is easy to verify everything that has happened to a file, from the very minute it was created, to the point it is needed.

## Write Once, Read Many Digital Tape

Write Once,  Read Many (WORM) digital tapes can be only written to one time. Using these tapes ensures with absolute certainty that chain of custody has been maintained and the data is the unaltered original. They can be read  a number of times, any time someone needs to look at the digital data, but they can't be overwritten, or  changed in any way. For applications where there can be no question about the data, WORM digital tape media is the media of choice. It is typically more expensive, as the digital tapes can only be used  once, rather than repurposing tapes, once their retention cycle has been exhausted.

## Conclusion

Maintaining digital chain of custody is essential for any organization creating data that might need to be admissible in court, and this includes video surveillance. Because of all the technology changes to video surveillance and the wide variety of video surveillance technologies, maintain chain of custody is more difficult and complex. With Spectra Logic's video surveillance archive solutions, you can be sure that your video surveillance data is secure, and that chain of custody can be not only preserved but demonstrated.

In addition, while selection of a best-in-class system is important, it is also important to plan for the implementation of processes and procedures to limit accessibility to a handful of key personnel. Being able to present well designed and documented processes and procedures, along with a well-designed system, ensures iron-clad data that can be used for any need that may arise.

When done right, a digital video surveillance system will provide you with peace of mind, knowing that if you ever need the video evidence, it will be there and will have the chain of custody necessary to allow it to be presented in any situation and in any court you might need it. This will allow your organization to triumph in your area of expertise, without worrying about whether your video surveillance data will be there and usable, when you need it most.

*When done right, a digital video surveillance system will provide you with peace of mind, knowing that if you ever need the video evidence, it will be there.*

# Deep Storage Experts

Spectra Logic develops deep storage solutions that solve the problem of long term storage for business and technology professionals dealing with exponential data growth.

Dedicated solely to storage innovation for more than 35 years, Spectra Logic’s uncompromising product and customer focus is proven by the largest information users in multiple vertical markets globally.

Spectra enables affordable, multi-decade data storage and access by creating new methods of managing information in all forms of deep storage—including archive, backup, cold storage, cloud, and private cloud.

For more information, please visit [http://www.spectralogic.com](http://www.spectralogic.com).

SPECTRA

DEEP STORAGE EXPERTS