# FROM DVR TO DISCOVERY:

## *Best Practices When Dealing with Digital Video Evidence*

**John Swanson** and **Jack Nevins** S-E-A

It's become common practice in the litigation of claims to ensure the proper handling of physical evidence — retaining an expert to retrieve and store it, track the chain of custody, and avoid spoliation. Digital video evidence, however, is not always given the same consideration. Despite how prevalent video evidence has become - and how critical it can be to a claim - it is often improperly retained, mishandled, or otherwise corrupted. At times, these oversights have the potential to take a smoking gun and turn it into a landmine. Fortunately, implementing a few best practices to preserve the integrity of digital video evidence will enable the right expert to make use of a video, even if circumstances aren't ideal.

### ACQUISITION & HANDLING

With the amendment to the Federal Rules of Evidence (FRE) addressing electronically stored information (ESI) such as digital video evidence, consideration must be given to the preservation of potentially relevant evidence when litigation is reasonably anticipated. Acting proactively is paramount, as electronic data is both transient and highly susceptible to alteration, modification, deletion, or permanent loss. Failure to preserve relevant ESI can negatively impact litigation outcomes and lead to adverse court rulings. One surprisingly common oversight is leaving a digital video recorder (DVR) system powered on, thereby overwriting older footage through cyclic recording, silently erasing critical data.

The process of collecting, preserving, and preparing electronic evidence for admissibility is addressed in FRE 901(a) and 902(13)–(14), which concern provenance and authentication. Digital forensic experts are uniquely qualified to collect evidence in a manner that satisfies these rules. Industry best practices include:

- Use of forensic write-blocking hardware/software to prevent alteration of source data.
- Automated logs, notes, and photographs documenting all expert actions.
- Use of digital hashing algorithms to ensure integrity at each stage of collection and handling.

A hash algorithm is a computational tool designed to process a file or collection of data (input) and produce a fixed-length hash value unique to the input. A change in the calculated hash value signals a potential integrity issue. The goal is to preserve all relevant data in a forensically sound manner while maintaining the original source unaltered. Done correctly, such evidence withstands scrutiny and is admissible in court.

### TRANSFER & STORAGE

Once collected, the evidence must be stored securely for the duration of the claim and litigation process, which may span years. Best practices call for:

- Multiple encrypted copies stored across different mediums (e.g., encrypted hard drives, secure network storage, flash media).
- Redundancy to guard against loss from hardware failure or corruption.

When production of evidence is re-

quired by court order, response to discovery requests, or provision to other experts, digitally identical copies can be readily reproduced. These copies are validated by recalculating and matching hash values to confirm their fidelity. Any such production, be it in whole or in part, should include proper chain of custody documentation to ensure full traceability and court compliance.

## "NATIVE FORMAT" DIGITAL FILES

It is critical to understand the vast differences between forensic data preservation versus a more crude data copy process. A forensic data image is a digitally identical, bit-for-bit replica of the source data validated against the original. A data copy produced through non-forensic processes will likely alter the source data and produce a non-identical copy that cannot be validated to the original. If we again consider the DVR appliance, these systems permit a user to produce selected video data by accessing a live system and navigating an administrative menu to produce "data exports." Typically, the exported data is produced in a different form than the data that resides on the internal storage media. The term "native format" refers to the data form as it resides on the internal storage media. Any non-native format produced during a live export process will result in a compressed or degraded format, which not only violates forensic best evidence-preservation processes but also results in an inferior file quality, which may impact future analysis of the video data. Further, non-forensic copy processes are likely to remove or alter critical metadata, such as file creation date and time, frame rate, original file format, original camera make and model, geo-coordinate data and much more.

To apply any form of validation of video evidence, forensic best practices must be followed from the outset. Without the ability to calculate a hash value of a forensic image of a DVR storage drive or a subset of native files preserved forensically, the provenance and veracity of the data cannot be verified and is therefore open to attack under FRE provisions.

## VIDEO/IMAGE ENHANCEMENT

With digital video evidence in hand, the next step is to make use of the video itself – the actual imagery. While properly acquired and handled video evidence provides the best possible data for review and analysis of that imagery, that doesn't mean that the data captured is clear and obvious. Often, digital video evidence is low resolution, grainy, blurry, washed out, or otherwise not an ideal view of the subject or incident. Worse, not all digital evidence is handled properly, resulting in over-compressed video with reduced quality, screen recordings of video instead of the native file, or worst of all, yet all too common, video of the video — handheld cellphone video of the video evidence playing on a screen.

In any case, most digital video evidence will benefit from forensic video enhancement. The goal of a forensic video enhancement is to improve the visual clarity of the data that exists within the file, such as improving legibility of specific features or actions. The keyword here is "forensic," because this can often be misconstrued as modifying or altering the evidence. Though it technically has been modified, in that it's no longer an exact copy of the original, the important distinction is that forensic enhancement is a clarification that is tracked and quantified, not an arbitrary alteration. Properly conducted enhancement does not substantively alter the imagery and is not the same as "doctoring" a video. Rather, it uses validated tools and methods to apply a series of mathematical equations to adjust the numerical values represented by the individual pixels that comprise the overall digital image. These equations, often applied in the form of "filters," serve purposes like improving brightness and contrast, reducing blur, enlarging or magnifying details, stabilizing shaky video, and reducing or removing distortion.

## A BIT ABOUT COMPRESSION

Furthermore, as with analyzing the make-up of a digital file and its metadata, additional analysis of the pixel information is often conducted at the enhancement stage. Most notably, the video compression. Simply put, video compression is how all the numerical values contained within a digital file, the 1s and 0s that are translated into images, are optimized to reduce file size while maintaining a certain fidelity based on the compression parameters. Most video evidence is captured and stored with some form of compression before anyone even accesses the file, and any time a video is clipped, cropped, trimmed, or transferred, there is the potential for that compressed data to be re-compressed, resulting in a less reliable video. That's not to say video compression inherently makes a video less reliable or less accurate. Even highly compressed videos can still contain accurate, reliable information. Still, it's useful to understand how a video has been compressed to address whether it's a significant factor in a given case.

In fact, understanding video compression and ensuring the use of validated tools are further reasons to engage qualified forensic experts, even for basic video editing. Gone are the days when you could recruit a friend or family member to help trim a video because they're "good with computers," or they "took a digital media class last semester." With the prevalence of digital video, the industry's understanding of this evidence is becoming more and more sophisticated, which means it is facing greater and greater scrutiny. Questions about whether a specific detail is seen on an I-Frame or P-Frame, the level of quantization, or the method of interpolation in an enlarged image may cast doubt on the validity of perfectly good evidence. A qualified forensic expert can address these topics and help ensure that video evidence holds up to this line of questioning.

## CONCLUSION

Digital video evidence can be a powerful asset or a liability, depending on how it is handled. From initial acquisition and forensic preservation to secure storage, analysis, and enhancement, each step must be executed with attention to accuracy and according to established processes to ensure admissibility and reliability. Courts expect digital evidence to meet the same rigorous standards as physical evidence. Failure to do so can jeopardize success and welcome a less-than-desirable outcome. By engaging qualified digital forensics professionals and adhering to industry best practices, insurance and legal professionals can avoid the risk of sanctions and adverse rulings and ultimately strengthen the integrity of their claims or defenses.

*John Swanson is discipline lead, imaging sciences for S-E-A. He specializes in creating demonstrative evidence and other visuals using a variety of 3D, video, photo, and graphics techniques; forensic video and photo analysis; and scientific 3D modeling and animation, aided by over a decade of experience in the field of 3D laser scanning and digital preservation of evidence.*

*Jack Nevins is practice lead, digital forensics for S-E-A. He advises clients on the identification, proper collection, and analysis of all forms of electronically stored information. From automated water slides to cloud-based storage systems, he has over 25 years of diverse experience within the litigation and insurance areas.*