



# INDIANAPOLIS-MARION COUNTY FORENSIC SERVICES AGENCY

*Doctor Dennis J. Nicholas Institute of Forensic Science*

40 SOUTH ALABAMA STREET • INDIANAPOLIS, INDIANA 46204  
PHONE (317) 327-3670 • FAX (317) 327-3607

Michael Medler  
Laboratory Director

## Evidence Submission Guideline #16

### Handling and Submitting Forensic Video Evidence for Investigators

#### Introduction

As video recording devices and Closed Circuit Television (CCTV) systems become a more affordable option in the private and public sectors, there is a corresponding increase in the frequency in which they are encountered in criminal investigations. The ability to obtain detailed information from video evidence has tremendous potential to assist with investigations. Care must be taken to make sure video evidence is accurately processed and presented in court.

New challenges face the Forensic Video Analyst as the Security Industry continues its migration from the decades old analog based technology to a fast changing and diverse digital world. The former standards of magnetic tape, such as VHS, S-VHS, 8mm and others, have given way to literally thousands of competing and proprietary digital video recording systems. These competing digital systems typically share few common characteristics. In the 'old days', any First Responder could recover video evidence from an analog recording device and in most cases, the evidence was easily viewed using a standard VHS player and an accompanying multiplexer. Today, the move to digital requires special skills, knowledge, training and equipment for the recovery and accurate display of even the most basic of digital video evidence.

Analog video technology relies on a common frequency based signal carried at approximately 4.28 MHz (luminance - NTSC) and stored as magnetic information on a videotape. The new Digital Video Recorders (DVRs) convey video images as zeros and ones and can be stored in a myriad of digital storage devices. In order to store large amounts of data into computer hard drives, most DVRs employ lossy compression technology. Compression reduces the amount of data required to represent the original image. The first casualties of lossy compression are image detail and accuracy. It is important for the first responder to acquire the best available evidence.

#### Recovery of Video Evidence

General principles for seizing and maintaining video evidence should be followed by law enforcement agencies. These general principles are:

**1. Rules of Evidence.** The same general rules of evidence should be applied to all video evidence just as it would to any other type of exhibit such as a knife at a homicide or fingerprints at a break-in.

**2. Chain of Custody.** Proper documentation of the chain of custody should be used and preserved to ensure the video evidence can be tendered in court as an exhibit.

**3. Evidence Preservation.** Upon seizing the video evidence, action should be taken to ensure the evidence is not changed:

**a.** For analog video evidence, the record tab needs to be removed or moved to a saved position.

**b.** For digital video evidence, write protection needs to be in place.

**4. Evidence Storage.** A climate-controlled room should be used to store video evidence.

**5. Custodian Responsibility.** Maintaining the evidentiary value of video evidence is the responsibility of the individual who has seized or signed for receipt of the evidence. The individual is responsible for all actions taken in respect to that item until it is formally transferred to another individual.

#### **Recovery of Digital Video Evidence**

No standard currently exists within the visual security industry for the extraction and acquisition of digital video evidence. Operating systems, transmission technologies and component hardware vary from manufacturer to manufacturer. As a result, there is no single 'best process' for connecting to a digital video recorder in order to recover digital evidence. It is important to avoid destructive processes that may change or alter the original data during the acquisition attempt. In most cases, a digital video system will provide a mechanism that will allow recovery of the original data that was recorded to the DVR in the 'first instance'. However, it is important to understand that many DVRs recompress the video images to another format on output. The reasoning often provided for recompression of the visual information is to allow easy viewing in an industry standard digital video file format and viewer, i.e.: Windows Media Viewer, QuickTime, etc. Unfortunately, recompression alters the original data and always removes image detail. It is not recommended to rely on recompressed data for examination if the original data exists and is available for analysis.

#### **Submission of Digital Evidence for Analysis**

Due to the large amount and variety of DVRs available, an investigator should also include the model number of the DVR and the software version of the digital video recorder with their request.

These guidelines were adopted from LEVA Best Practices for the Acquisition of Digital Multimedia Evidence and Guidelines for the Best Practice in the Forensic Analysis of Video Evidence.

Any questions should be directed to the I-MCFSA laboratory at (317) 327-3670.