# *Best Practices for the Acquisition of Digital Multimedia Evidence*

***Sponsored by the Law Enforcement and Emergency Services Video Association (LEVA)***

**Purpose:**

This document is provided to law enforcement agencies and individuals as a Best Practices Guide for the acquisition and initial processing of Digital Multimedia Evidence in preparation for analysis. The information contained in this document is provided as a public service by the Law Enforcement & Emergency Services Video Association (LEVA).

It is recommended that this document be used as a guide. LEVA recommends that law enforcement agencies working with Digital Multimedia Evidence develop specialized expertise and written Standard Operating Procedures in this area.

# TABLE OF CONTENTS

**PURPOSE:** .......... 1

**INTRODUCTION** .......... 3

**DEFINITIONS** .......... 4

*DIGITAL MULTIMEDIA EVIDENCE* .......... 4
*FORENSIC VIDEO ANALYSIS* .......... 4

**STATEMENT OF RESPONSIBILITY** .......... 4

**PART I – FOUNDATION** .......... 4

SOPS .......... 4
ETHICS .......... 5
*Technical Function* .......... 5
*Analytical Function* .......... 5
INTEGRITY VERIFICATION & DATA AUTHENTICATION .......... 6
*Integrity Verification* .......... 6
*Authentication* .......... 6
INTEGRITY VERIFICATION .......... 6
AUTHENTICATION .......... 6

**PART II – PRESERVATION OF DME** .......... 7

UNIQUE CHALLENGES OF DME .......... 8
GAINING PHYSICAL ACCESS .......... 8
INTERCONNECT DEVICES .......... 8

**PART III – EXTRACTION /ACQUISITION OF DME** .......... 10

1. ID THE MODEL AND VERSION NUMBER: .......... 10
2. RESEARCH CODEC: .......... 10
3. DETERMINE THE MOST ACCURATE METHOD OF DATA RECOVERY: .......... 11
4. DATA VERIFICATION USING UNIQUE IDENTIFIER(S) .......... 12
5. VERIFY AND CALIBRATE ASPECT RATIO .......... 13
6. VISUALLY COMPARE ORIGINAL VIDEO TO WORKING COPY .......... 14

**PART IV - CONCLUSION** .......... 15

EDUCATION: .......... 15
*Professional Organizations and Educational Meetings* .......... 16
*Vendor Training* .......... 16
*Seminars* .......... 16
*College Level Courses* .......... 17
RESOURCES .......... 17
*Glossary References* .......... 17
*Books:* .......... 17
*Training Organizations:* .......... 18
*Internet Resources* .......... 18

## Introduction

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. Understanding the effects of compression is critical to accurate interpretation of the video images. It is equally important that the Forensic Video Analyst (FVA) understands how DVR manufacturers "package" their compressed data and how the unique process of compression/decompression (CODEC) may impact the recovery of the video data.

Data, representing video information, often comes wrapped in any one of a number of digital video formats. Many of the these file formats are referred to as an "Open Source" format, that is, many of the commercially available players (i.e., Media Player, Quick Time, VLC Media Player…) can read and play the video data without additional software codes. Some manufactures alter the open source code so it will fit their specific player, thus making the "altered" file format proprietary to the manufacturer's player. Because many DVR systems capture, transmit, store and playback video data in unique ways, a single forensic approach for the acquisition and examination of digital video evidence does not exist.

It may be necessary to research and understand a particular DVRs capture method, transmission, image matrix and CODEC(s) in order to accurately recover and examine the digital video evidence.

This document outlines Best Practices for the acquisition of Digital Multimedia Evidence to assist the FVA to understand some of the technical issues relating to the recovery of video evidence in a digital world. Unlike yesterday's predictable analog video sources, today's DVR systems are unique, incompatible with one another and require different approaches to conduct a forensic video exam. New skills and training are required for the FVA to transition from processing Analog to Digital Video evidence. In a science where standards help to guide analysts through the process of examination, an environment void of standards requires Best Practices.

## Definitions

### *Digital Multimedia Evidence*

Digital Multimedia Evidence (DME) is information of probative value stored or transmitted in binary form including, but not limited to, film, tape, magnetic and optical media, and/or the information contained therein.
NOTE: The term DME used in this document refers specifically to video, audio and the metadata associated with that form of DME. Although audio is often contained within DME sources, this document is not intended to provide a best practice guideline in the area of the Forensic Audio Analysis sub-discipline.

### *Forensic Video Analysis*

Forensic Video Analysis is the scientific examination, comparison and/or evaluation of video in legal matters.

For all other definitions refer to the following:

***Forensic Imaging Multi-media Glossary Covering Computer Evidence Recovery (CER), Forensic Audio (FA), Forensic Photography (FP), Forensic Video (FV):***

http://leva.org/pdf/GlossaryV7.pdf

***SWGDE/SWGIT Digital & Multimedia Evidence Glossary:***

http://theiai.org/guidelines/swgit/swgde/glossary_v2-0.pdf

## Statement of Responsibility

DME is produced using processes of varying quality and reliability and requires interpretation by a qualified Forensic Video Analyst to accurately determine its meaning and representation. It is the responsibility of an investigating agency to ensure a qualified Forensic Video Analyst examines DME in all cases likely to involve criminal charges or Indictments where the identity of an individual or opinion evidence will be offered.

## PART I – Foundation

### SOPs

Standard Operating Procedures (SOPs) establish a foundation for the examination of DME. SOPs are written documents which outline the basic concepts and fundamentals needed for the forensic examination of evidence. This can include, but is not limited to, general concepts, principles, step-by-step instructions, historical data, how to process collected data; and other procedures to insure the quality of the analysis. SOPs should be sufficiently detailed without being so rigid as to not allow for flexibility. SOPs allow for consistency and repeatability in the analytical process. It is strongly recommended that SOPs be tested and validated prior to being used in active casework. There should be a procedure in place to update SOPs and a reporting process if changes in technology dictate that new approaches require a deviation from existing SOPs. It is important that there be technical and administrative approval of all SOPs. SOPs should not be in conflict with departmental or agency policy.

**Ethics**

At all times, a FVA must perform work without influence of bias, free from institutional prejudice, without regard to the potential influences of investigators and prosecutors and should follow accepted scientific methodology and practices, while focusing aggressively on the pursuit of the truth.

**Technical and Analytical Functions**

There are two broad functions involved in the processing of DME. There is a Technical Function and an Analytical Function. Each function requires a different level of education, training and experience.

***Technical Function***

Typically this is a step-by-step process/procedure conducted by a trained individual, which results in a product that may or may not be the final step in the analysis of the DME.

Examples of *Technical Functions* include but are not limited to:

- Copying digital media
- Converting/transcoding digital media from one format to another
- Printing images from digital media
- Archiving data
- Outputting data to an analog or digital medium
- Resizing digital images
- Basic image adjustments
- Time reference adjustments/calibrations

***Analytical Function***

Typically this is a process/procedure requiring additional skills, education, experience and/or training which will result in a product derived from processes, and one which requires a significant amount of judgment and/or an opinion.

Examples of *Analytical Functions* include all *Technical Functions* and also include, but are not limited to the following:

- Comparing and contrasting known objects or persons to questioned objects or persons (Image Comparison, Photographic/Video Comparison)
- Conducting image aspect ratio calibration (establishing height to width relationship of an image)
- Color correction
- Reverse projection
- Photogrammetry
- Motion tracking
- Image stabilization
- DME recovery
- Media alignment (multi-camera synchronization)
- Audio/Video Alignment

- Image analysis
- Peer/Technical review
- Image authentication
- Integrity verification
- Providing opinion evidence

It is important to recognize that it may be appropriate to limit the scope and procedures involved/conducted in a Technical or Analytical Function and to narrow the focus of an examination based on:

- Analysis request
- Existing policy
- Available resources: time, personnel, equipment…

However, in cases involving identification, motion interpretation and opinion evidence, every effort must be made to adhere to scientific methodologies.

**Integrity Verification & Data Authentication**

The terms Integrity Verification and Data Authentication are often interchanged and frequently misunderstood. The Scientific Working Group on Imaging Technology (SWGIT) and the Scientific Working Group on Digital Evidence (SWGDE) define these terms as:

> **Integrity Verification**
>
> The process of confirming that the data presented is complete and unaltered since time of acquisition.
>
> **Authentication**
>
> The process of substantiating that the data is an accurate representation of what it purports to be.

**Integrity Verification**

Integrity Verification seeks to answer the question, has the evidence been changed and/or altered since it was created in the first instance? Changes to data should not necessarily be interpreted as a negative process or an indictment on the reliability of the data. In many cases, digital video evidence must be calibrated, resized, brightened or sharpened. Each process effectively alters the data, but not the data's meaning.

**Authentication**

Authentication seeks to answer the following questions:

- Does the data accurately represent what it purports it to be?
- Is what occurred in front of the camera the same visual information in time and space as that which was recorded on the digital media?
- Can an adequately trained forensic video analyst safely draw conclusions from the resulting data?

By its very nature, digital evidence is ethereal, non tactile and has to be displayed in some manner to be perceived. Record and display processes often result in aspect ratio errors and color errors. Time lapse, motion prediction and compression processes also cause significant challenges to the concept of 'Authentication'. The science of FVA recognizes the frailties of image reproduction in a digital world, and places special emphasis on the necessity of accurate interpretation of the evidence.

**Original v. Copy**

Data representing DME can be easily changed. Changing the data does not necessarily result in a change to the meaning or intent of the data. The mere act of changing the data should not lead one to infer that the data is not authentic or reliable. The process of transcoding digital video from one form to another provides analysts with a working copy of the original, which for many reasons, may be more appropriate for analysis than the original. All efforts should be taken to insure the copy does not reduce or add information that could change the meaning of the original.

Because most DME recovered from digital video recorders has already been compressed by a proprietary CODEC, transcoding may be the only process available to import the data into a forensic analysis system for examination. The original data is often transcoded into another digital form for one of the following reasons:

1. Input into a forensic video analysis system for examination, redaction, alignment, calibration, etc.
2. Provides an alternate method of viewing
3. To remove irrelevant or prejudicial data
4. To archive the data

## PART II – Preservation of DME

In the US, Canada and the United Kingdom, there are different approaches to defining the question of what is an original and what is a copy? However, the underlining principle that the data must be accurate is paramount in each country.

One of the most significant challenges facing Forensic Video Analysts today centers around the task of determining what is the best available evidence for analysis. In most cases, a FVA becomes engaged in an examination long after the evidence has been seized. It is common for a First Responder to acquire DME without regard for either verification or authentication. Often, the word "Original" is boldly written on discs containing data, when in reality the data contained on the disc is a compressed and/or inaccurate copy of the original. This common First Responder practice of obtaining the easiest evidence rather than the best available evidence underscores the premise of this document which is that DME is evidence and trained and skilled experts are required to process it using scientific methodologies.

Where practical, it is always a best practice for an appropriately trained FVA to guide the process of DME acquisition. Where an agency's policy delegates the recovery of evidence to adequately trained specialists, that policy should include the requirement that a FVA be part of the Crime Scene Investigation Team when DME may be involved.

### Unique Challenges of DME

Lack of digital standards in the Visual Security Industry, combined with the wide variety of storage media and connection technologies complicate the recovery process. Some examples of these challenges are:

- Receiving timely notification that DME exists
- Gaining physical access to the equipment storing the DME
- Gaining logical access to the data related to the event in question
- Preventing the overwriting of the relevant data
- Determining if additional expertise is required to access the original data
- Documenting the chain of custody of digital evidence which, by its nature, has no physical form

### Gaining Physical Access

Gaining physical access to digital evidence presents its own host of challenges. Unlike analog videotapes, access to DME is often restricted by various technologies. For instance, the data may be stored off-site in a networked infrastructure or the host operating system may be incompatible with the analyst's tools. In an attempt to make life convenient for law enforcement, manufacturers often provide simplified methods of recovering copies of the DME. Unfortunately, these simplified methods may result in loss of information and could lead to an inaccurate interpretation of the events depicted. Examples of simplified methods may include but are not limited to:

- Direct output to videotape
- Exporting data that results in a format conversion
- Still image export
- Internet transfer/receive options

These changes may adversely affect issues surrounding the reliability of the DME.

In addition, when compared to analog multimedia evidence, which may be overwritten by scheduled rotation of tapes, DME is likely to be overwritten if steps to preserve the evidence are not taken in a timely manner.

### Interconnect Devices

The methods of acquiring DME vary so widely from system to system, that the FVA should be familiar with a variety of connection technologies. Interconnect devices range from USB, IEEE (1394), SCSI, IDE, Parallel and Ethernet to CD's, Discs and even floppy drives. The prevalence of interconnect devices is further complicated when data is stored remotely. Remote storage is common in Network Video Recording technology, where the files are commonly located hundreds and sometimes thousands of miles from the crime scene. Access to remotely stored evidence may be acquired over network cables, phone cables, or through wireless connectivity.

Identifying where the original logical files reside and the best method of connectivity is the first step in acquiring DME. However, prior to taking any steps to secure and acquire DME, legal authority to do so must be established. In all cases where there is a question regarding whether a warrant is required to examine the DME, appropriate legal authorities should be consulted prior to examination. In circumstances where the evidence may be lost or erased before a warrant can be obtained, the data and possibly the entire computer system should be secured. In all cases where a warrant is being sought, examination of the data must not occur before the actual warrant is obtained.

A determination as to whether the relevant data is stored on-site or at a remote location must be made. If the data is stored on-site, the FVA should coordinate with personnel at the storage location to gain access to secured areas, locked containers, or storage devices. If the relevant data is stored off-site, physical access to the storage area may be impractical. If physical access is not practical, the FVA may elect to contact other personnel who can access the DME and make arrangements to preserve the data.

In either case, additional security barriers, such as password protection to the host computer and to the DVR viewer, may need to be overcome in order to access the logical files. Once access to the data is obtained, steps should be taken to ensure no overwriting of relevant data occurs. The capacity of the system may affect the length of time the relevant data is maintained on the storage media before being overwritten. The FVA must take steps to insure the relevant data is protected from the overwriting process. It is considered a poor practice to simply 'pull the power cord' on a DVR, as a sudden loss of power could cause destruction of the evidence. Terminating the power source should be considered a last resort.

After the FVA ensures data is not lost due to overwriting, the FVA may take steps to limit access to the data. This can be accomplished by limiting physical access to the recording/storage device and isolating the recording/storage device from external sources. External sources of access include network cables, phone cables, and wireless communication devices.

If the FVA is unable to accomplish any of the steps mentioned above, the FVA should solicit the assistance of additional resources including but not limited to manufacturer support personnel, network administrators, or a qualified computer forensic examiner.

After preserving the data, the FVA should document all relevant steps taken during the preservation process and then proceed to the acquisition phase.

If data is acquired from the DVR on location and the DVR is to be left at the scene, consideration should be given to the question of “What should be done with the original data which still exists on the DVR?” On the one hand the consequence of erasing the original data on the DVR could result in legal challenges. On the other hand leaving the data on the DVR could provide inappropriate access to the information causing conflicts with the investigation. Under normal use, the DVR will eventually delete the data to make room for new data. The question of whether to erase or not to erase is best left to agency policy, but should be considered in each case. When a FVA determines the data should be erased, justification for that action should be articulated and steps to establish data verification should be taken.

## PART III – Extraction /Acquisition of DME

No standard currently exists within the visual security industry for the extraction and acquisition of DME. 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 for the forensic video analyst 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.

In order to secure the original data and to interpret what the data represents, the FVA should consider the following six steps when acquiring DME.

### 1. ID the Model and Version Number:

Where practicable, the FVA should be able to identify the model number and software version of the digital video recorder that produced the evidence. Authentication and verification rules require a witness to identify the source and reliability of the DME. The FVA may be the most appropriate person to provide that evidence since owner/operators of DVRs rarely are familiar with the technology and since manufacturers are reluctant to offer their engineers for trials. Also, since the FVA is processing and evaluating the evidence produced by the specific DVR, it is imperative that the analyst knows how it operates and can articulate what was done to recover the original data, or at the very least; the FVA must be able to answer the question of how the evidence before the court came to be.

The process of identifying the DVR Model and Version number will likely reveal significant information regarding system and playback specifications. The FVA should determine the manufacturer's recommended viewing resolution. Monitor resolution often dictates how accurately DME will be displayed through the host viewer. If the manufacturer recommends that the data be viewed on a monitor at 800 X 600, it may not play properly on a monitor set up to display at 1024 X 768. In cases where the screen resolution is inconsistent with the recommended settings, the viewing software may not be capable of displaying the data or it may change the height to width aspect of the images.

### 2. Research CODEC:

The lack of standards also impacts the way in which one digital video recorder (DVR) may record an event compared to a DVR of another manufacturer. The methods and types of recording technology typically vary from DVR to DVR model, even those of the same manufacturer. A MPEG compression engine for example, will treat objects recorded from a pan-tilt-zoom camera differently from the way in which a JPEG compressor will treat the same camera view. The MPEG compressor typically will result in a smaller file size, but it will likely also produce motion artifacts. The JPEG video will likely require additional storage space as compared to the MPEG video, but typically the JPEG video clip will provide more image detail. For the FVA, understanding basic CODEC functions is necessary in order to evaluate and interpret digital video images.

**3. Determine the most accurate method of data recovery:**
The absence of standards in the digital multimedia security industry makes it impractical for any one document to specify the best acquisition method for all situations. The best method of data recovery will need to be evaluated on a case by case basis. Generally there are six main categories of acquisition processes. These categories include:

- Using the DME recording system to export multimedia files which can be played back for analysis,
- Using a multimedia capture utility to trans-code the DME into a usable format,
- Copying logical files related to the event from the DME recorder,
- Creating binary images of drives on the DME recording system,
- Seizing the DME recording system, or
- Capturing playback from the DME recording device with an analog recording system.

Exporting DME using the recording device's built in functionality may be the most appropriate method for acquiring data if the FVA can verify the data is exported in its native format and resolution, and the data can be played back accurately for later analysis. This function is often referred to as a backup or archive function. This option may not be available in all DME recording systems, but may be replaced by a function to export a common digital multimedia format. The FVA should be aware that this common multimedia format export function may degrade the image quality making it less desirable than other acquisition methods.

If the DME does not include an appropriate backup/archive function, and the FVA can identify the logical files relevant to the event in question, the FVA may elect to copy these files to an appropriate storage device. The FVA should be careful to determine the correct scope of the event to ensure all relevant files are captured. The FVA should also note there may be multiple types of files necessary to ensure the logical files can be played back for analysis later, including but not limited to:

- Multimedia file
- Index files
- Metadata files (such as those found in point of sale transactions or those that contain the data necessary to reproduce an accurate time/date stamp)

If the logical files can not be identified or if the scope of the recorded event is not clearly defined, it may be necessary to create a binary image of the storage device(s) found on the DME recording system. A binary image is an exact copy of all the binary data, 1's and 0's, which is the video data on the storage device. This process, however, may not allow for the playback of the DME video without the original hardware, as some DVR recorded data is hardware dependent. Creating a binary image may require additional skills and training. In cases where a binary image is required, assistance from a computer forensic examiner should be considered.

Creating a binary image from the DME recording system's storage devices should be conducted when there is a suspicion the data has been tampered with or there is a possibility the stored data contains additional evidence other than the video information. An example of this would be if a personal computer were used by a suspect to conduct financial crimes and the computer doubled as a DVR host CPU. In this instance, the possibility exists that there could be data on the computer relevant to analysis other than a video exam.

Multimedia capture software may be used to transcode the DME data into a usable format which can be analyzed further. It is recommended the capture software be tested prior to being used on evidence.

If all other options fail or are not appropriate, the DME recording system may have to be seized. There may also be instances where in order to protect the data from destruction, the DME recording system should be seized. The question of DVR seizure should be evaluated on a case by case basis and should comply with all legal requirements and departmental SOPs. This is generally less desirable than the previously discussed acquisition option because the DME recording system owner is often a third party to the crime or is the victim of the crime and seizure of the equipment may cause unnecessary hardship. Seizing equipment should be weighed against the benefits gained versus the hardships created by the seizure. If the system is seized, it is recommended the system should be photographed, paying particular attention to the cable connections, before it is disconnected. The system should be properly shut down and any written documentation, such as manuals and operating instructions, seized as well.

Another option for extracting the visual information may include a scan-conversion process that converts the original data into an analog video signal. BNC, S-VIDEO or Composite video outputs usually provide for the easiest acquisition method, however, scan conversion always results in degradation of the image. When visual data is converted to an analog signal within the DVR, the data will be changed from its original digital format (usually a progressive scan environment) to an analog signal (interlaced). Loss occurs when the digital information is scan-converted to an interlaced medium.

DME acquired using an analog process may still provide valuable and reliable evidence for analysis. Cases in which the best evidence of an original digital source exists only in analog form may still be admissible as a duplicate under the definition contained in FRE 1001(4) in the United States. In Canada and in the UK, the weight applied to DME that has been converted to an analog form may be diminished, but if the evidence can be authenticated and is relevant, it will likely be admitted.

### 4. Data verification using unique identifier(s)

Regardless of the method used to acquire information, steps should be taken to ensure the originals and/or any copies of the DME can be verified to ensure it can later be presented as evidence in court. The verification process should establish that the acquired data accurately reflects the original data. Methods of verification include, but are not limited to, visual or aural verification, checksum or hash verifications, and embedded digital signatures.

Visual or aural examination involves ensuring the acquired data provides an accurate representation of the original DME by observing or listening to the acquired data and comparing it to the original data.

Checksum or hash verifications ensure the acquired data was accurately copied. These processes use mathematical algorithms to generate unique identifiers for the original and the copied data. Comparing the unique identifiers of the original data to the unique identifiers of the copied data must result in an exact match and the FVA can be assured the acquired data is exactly the same data as the source.

Digital signatures generally utilize a mathematical algorithm to generate a hash value for the original data which is then encrypted with a private key. Verification of the original data or a copy of the data is accomplished by decrypting the hash value with a public key and comparing it to a contemporaneously calculated hash value for the data. Any minute change to the data will cause the hash comparison to fail. Some DME recording systems embed digital signatures within the DME file or files. These DVR source digital signatures may be used by the FVA to help verify the original data and any subsequent copy of the original data.

### 5. Verify and Calibrate Aspect Ratio

Most video cameras used in a CCTV environment today produce an analog frequency based signal. When the signal is sampled and encoded by a digital video system errors usually occur that cause changes to the height to width relationship of objects and persons captured to the field of view. These errors are often manifested as horizontal stretching of the image in an NTSC signal path and vertical compressing of the image in the PAL environment. To correct this error, the analyst may need to calibrate the aspect ratio of the DME. Calibration is necessary in cases where the analyst provides observations or opinions relating to the comparison of a questioned person or object to a known person or object.

A method for the calibration of DME may include but is not limited to the following steps.

1. Return to the location of the recorded incident and gain control/access to the DVR. Establish a direct signal feed (live feed) from a camera that sends its signal to the original DVR. This should be a direct feed from the camera to a known standard or an analog VHS record deck with both in and out video capabilities. This signal feed will provide the control image for the calibration.

2. Document all relevant information regarding make and model number of the original camera. If the original camera is not available or functioning, a similar camera, with similar lens characteristics can be used in its place. The camera is connected to the DVR, allowing the signal path to pass through the controlled analog or forensic recording device.

3. Fix a SMPTE (Society of Motion Picture and Television Engineers) or equivalent calibration chart at as close to 90 degree angle as is possible in relation to the camera’s lens. The chart should occupy as much of the camera's field of view as possible to allow for proper calibration and alignment. In the event that a standard calibration chart is not available, the camera can be focused on a specific object, such as a building with horizontal and vertical structural lines that can be used as the 'standard'.

4. The signal path should continue through the FVA system or video deck to the original DVR. Both analog and digital recorders should simultaneously record the calibration image.

5. Overlay, or superimpose the calibrated 'standard' image with the DVR still image capture. This process can be done in a number of imaging applications. A filter or function must then be produced that can be applied to the DME in order to calibrate its correct aspect ratio. The FVA must document the horizontal and vertical values used in the alignment. Once the filter/function has been applied correctly to the DME, it is safe to conclude that the aspect ratio of the DME is accurate.

### 6. Visually Compare Original Video to Working Copy

A working copy is a reproduction of information contained in the original data that is subject to further processing. No matter what process is used to acquire the DME, it is important that the FVA visually compares the original data to the recovered images. Not only will this part of the examination help to verify that the best evidence has been extracted, it will offer a means of identifying if any changes have occurred, what effect those changes may have on the analysis; and perhaps it will provide evidence indicating whether additional compression has taken place during the recovery process.

This examination can give indications as to the type of CODEC used in recording the DME and will assist the FVA in offering a reliable interpretation of the data. Some key items to consider during this part of the examination include:

- Artifacts: If an artifact is present when viewing the DME on the DVR, the same artifacts should be present in the copied data if the data is to be considered an original. High contrast areas of the image are locations where artifacts will most likely be manifested and should be examined closely. If the artifacts are different in the extracted files, an explanation should be sought. Some possible explanations may be:

- The DME was transcoded and changed in the extraction process.

- Conflict between software versions (being viewed on a different version than on that which was used to record it).

- Differences in the display viewing technology (i.e.: computer monitor).

- Differences in color settings or sample frequencies can result in the same video having a different appearance when viewed on different computers. Additionally, the software being used to view the video can cause changes to the color information, resolution or aspect ratio of the DME. For example, DME that is viewable using Windows Media Player may have a different aspect ratio and some shifting in color values when viewed using a QuickTime viewer.

  > It should be noted that the presence of artifacts observed in the original that are not observed in the copy provide definitive evidence that changes have occurred. However, the absence of observed changes does not necessarily provide proof of verification.

- Motion: Due to motion prediction errors in many DVR compression systems, there may be instances in which motion may be inaccurately recorded. Where motion prediction errors are present when viewing the original DVR, those same errors should be present in the working copy output for analysis.

In some cases, the only extraction options available may result in the addition or loss of artifacts. The loss or softening of artifacts should not be considered an "improvement" in the image but rather an indication that during the transcoding of the DME, additional compression was applied resulting in the entire image being 'smoothed' or blurred. Changes in artifacts may not render the DME unreliable, but any process that alters the original data should be avoided where possible.

## PART IV - CONCLUSION

Competition within the Digital Video Recording Industry has encouraged diversity of technology and has resulted in the production of many incompatible products, each with its unique method of encoding visual and audio evidence. In an industry constantly in flux and void of standards, it is impossible to list all of the potential ways to process DME. This document is intended to focus the analyst toward critical areas to consider when processing and evaluating DME. Recommendations contained in this document are to be considered General Guidelines. Additional tools, techniques and methodologies, not contained in this document, may be appropriate provided they are based on scientific principles that can be repeated and documented.

### Education:

In order to effectively perform the tasks and duties of a forensic video analyst it is essential that the analyst maintains current knowledge of evolving technologies and must have a self-driven pursuit of further education. The analyst is empowered with the responsibility of acquiring, examining, disclosing, and interpreting evidence that the court can both comprehend and trust. With this responsibility is the need for the analyst to learn about and to become proficient in a number of disciplines. One step on the path to this proficiency is to attend courses specifically geared towards these disciplines.

Examples of recommended courses may include but are not limited to:

- Digital Image Processing
- Forensic Imaging
- Computer Data Processing and Basic Recovery
- Photographic / Video Comparisons
- CCTV Technologies
- Courtroom Testimony
- Law courses related to the forensic disciplines
- Acquisition and Analysis of Digital Multimedia Evidence
- Report Writing
- Presentation of Evidence
- Reverse Projection
- Photogrammetry
- Color Correction
- Multimedia Development and Technologies

There are a number of organizations and schools available to the analyst to obtain appropriate education in the field of Forensic Video Analysis; however, careful evaluation of the course offered should be conducted to ensure that the instructor is credible, has appropriate experience in the field and that the curriculum supports best practices, as outlined in this document. It should be recognized that credible courses usually include a testing mechanism and most often offer hands-on learning environment. One of the methods for evaluating a course is by soliciting the assessment or feedback of prior attendees.

Types of organizations offering training in this science include:

**Professional Organizations and Educational Meetings**
Organizations such as LEVA*, the International Association for Identification (IAI), and the National Technical Investigators Association (NATIA) and others provide regular courses and seminars on forensic video analysis.

**Vendor Training**
Courses and seminars provided by companies that provide digital forensic analysis systems and image processing tools.

**Seminars**
Provided by government agencies, government forensic laboratories, as well as commercial enterprises. Seminars allow analysts to compare and review processing techniques.

**College Level Courses**
Universities, colleges, and technical schools that provide course work in forensic video analysis, video engineering, and image processing.

**Additionally, LEVA provides a Forensic Video Analysis Certification Program that outlines a training plan in forensic video analysis.*

## APPENDIX

### Resources

A myriad of resources are available to assist analysts seeking to improve their understanding of DME. Some resources are aimed specifically at providing technical information on relevant issues. Other resources provide information on general forensic concepts which are equally important.

### Glossary References

Scientific Working Groups on Digital Evidence and Imaging Technology - Digital and Multimedia Evidence Glossary:
http://theiai.org/guidelines/swgit/swgde/glossary_v2-0.pdf

*Forensic Imaging And Multi-media Glossary Covering Computer Evidence Recovery (CER), Forensic Audio (FA), Forensic Photography (FP), And Forensic Video (FV)*
http://leva.org/pdf/GlossaryV7.pdf

### Books:

- CCTV, Second Edition : Networking and Digital Technology -- by Vlado Damjanovski;
- Closed Circuit Television: CCTV Installation, Maintenance and Operation, Second Edition -- by Joe Cieszynski
- CCTV for Security Professionals -- by Alan Matchett
- Video Demystified, Fourth Edition – by Keith Jack
- Today's Video – by Peter Utz
- CCTV Surveillance, Second Edition : Video Practices and Technology -- by Herman Kruegle
- Image and Video Compression for Multimedia Engineering -- Yun Q. Shi
- Computer Imaging: Digital Image Analysis and Processing -- by Scott E Umbaugh

- The Image Processing Handbook, Fourth Edition -- John C. Russ
- Handbook of Image and Video Processing (Communications, Networking and Multimedia) – by Alan C. Bovik
- Image and Video Compression for Multimedia Engineering -- Yun Q. Shi
- Digital Video Compression – by Peter Symes
- How Video Works – by Diana Weynand

**Training Organizations:**

| | |
|---|---|
| Law Enforcement & Emergency Services Video Association | www.leva.org |
| The International Association for Identification | http://theiai.org |
| The International Association of Chiefs of Police | www.iacp.org |
| National Technical Investigators' Association | www.natia.org |
| The American Academy of Forensic Sciences | www.aafs.org |

**Internet Resources**

*Scientific Working Group on Imaging Technology* (SWGIT):
http://theiai.org/guidelines/swgit/index.php

*Scientific Working Group on Digital Evidence* (SWDE):
http://ncfs.org/swgde/index.html

*The International Association of Computer Investigative Specialists* (IASCIS):
http://www.iacis.info/iacisv2/pages/home.php

*National White Collar Crime Center* (NW3C): http://www.nw3c.org

*Regional Computer Forensic Laboratories* (RCFL): http://www.rcfl.gov