



# Best Practices for the Acquisition of Digital Multimedia Evidence

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

## **Disclaimer:**

As a condition to the use of this document and the information contained therein, the LEVA requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings). Such notification shall include:

- 1) The formal name of the proceeding, including docket number or similar identifier;
- 2) The name and location of the body conducting the hearing or proceeding;
- 3) The subsequent to the use of this document in a formal proceeding please notify LEVA as to its use and outcome; and
- 4) The name, mailing address (if available) and contact information of the party offering or moving the document into evidence.

Notifications should be sent to [documentation@leva.org](mailto:documentation@leva.org). It is the user's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived for future reference, as needed, in accordance with that agency's policies.

## **Redistribution Policy:**

LEVA grants permission for redistribution and use of all publicly posted documents provided that the following conditions are met:

- 1) Redistributions of documents or parts of documents must retain the LEVA cover page containing the disclaimer.
- 2) Neither the name of LEVA nor the names of contributors may be used to endorse or promote products derived from its documents.
- 3) Any reference or quote from a LEVA document must include the version number (or create date) of the document and mention if the document is in a draft status.

*LEVA Best Practices for the Acquisition of Digital Multimedia Evidence  
Version 3.0 (April 14, 2010)*

**Purpose:**

This document is provided to law enforcement agencies and individuals as a Best Practices Guide for the acquisition of Digital Multimedia Evidence. 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: .....	2
EXECUTIVE SUMMARY .....	4
DEFINITIONS .....	5
<i>MULTIMEDIA EVIDENCE</i> .....	5
<i>FORENSIC VIDEO ANALYSIS</i> .....	5
<i>INTEGRITY VERIFICATION</i> .....	5
<i>AUTHENTICATION</i> .....	5
INTRODUCTION .....	5
PART I – PRESERVATION OF DME .....	6
<i>GAINING PHYSICAL ACCESS</i> .....	6
<i>GAINING LOGICAL ACCESS</i> .....	6
<i>CONTROLLING ACCESS</i> .....	6
<i>PREVENTING LOSS</i> .....	6
PART II – ACQUISITION OF DME .....	6
<i>DOCUMENT SYSTEM INFORMATION</i> .....	7
<i>DETERMINE THE MOST ACCURATE METHOD OF DATA RECOVERY:</i> .....	7
<i>TRANSFER ALL CODECS AND REQUIRED VIEWER FILES</i> .....	8
<i>TRANSFER ALL RELEVANT MEDIA FILES</i> .....	8
<i>VERIFY THAT TRANSFERRED MEDIA FILES ARE PLAYABLE ON A SEPARATE COMPUTER</i> .....	8
<i>VERIFY THAT ALL RELEVANT MEDIA WAS TRANSFERRED AND THAT IT IS A FAIR REPRESENTATION OF     WHAT WAS ON THE RECORDING SYSTEM</i> .....	8
PART III – ADDITIONAL CONSIDERATIONS .....	8

## **Executive Summary**

The proliferation of digital video recording systems (DVRs) in our society presents significant challenges to law enforcement when attempting to obtain visual evidence of a crime. Proprietary digital recording technology and a lack of interoperable standards in the CCTV Industry, means that no single Standard Operating Procedure or process can be referenced for the acquisition of all Digital Multimedia Evidence (DME).

First Responders, Digital Evidence Specialists, Forensic Video Analysts and Technicians require specialized equipment, skills, knowledge and training to ensure that DME is protected and that Best Evidence is recovered and preserved.

Data that is commonly exported from DVR systems are often wrapped in any one of a number of digital video containers or players. Many of the players are referred to as "Open Source" and allow easy viewing of the data in most computer systems. However, 'Open Source' players and containers, such as those identified by file extensions with *.WMV*, *.AVI*, *.AFS*, etc., often indicate that the visual quality of the evidence has been reduced from its original form.

The goal of this document is to guide the investigator through Best Practices to ensure that best evidence is the target of DME acquisition and that the integrity of the original data is maintained.

## Definitions<sup>1</sup>

### ***Multimedia Evidence***

Analog or digital media, including, but not limited to, film, tape, magnetic and optical media, and/or the information contained therein.

NOTE: The term Digital Multimedia Evidence (DME) used in this document refers specifically to multimedia evidence in a digital form.

### ***Forensic Video Analysis***

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

### ***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.

## Introduction

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. It is best practice for appropriately trained personnel to guide the process of DME acquisition to ensure that the relevant data is complete and unaltered.

This document addresses issues relating to the preservation and acquisition of DME. All steps taken during the preservation and acquisition processes should be documented. Additionally, all laws and departmental policies pertaining to search and seizure of evidence should be adhered to during the acquisition of DME.

In all cases where there is a question regarding whether a warrant is required to seize DME, appropriate legal authorities should be consulted.

---

<sup>1</sup> SWGDE and SWGIT Digital & Multimedia Evidence Glossary, Version: 2.3 (May 22, 2009)

## **PART I – Preservation of DME**

DME preservation should consider the following:

- Gaining physical access
- Gaining logical access
- Controlling access
- Preventing loss

### **Gaining Physical Access**

If the data is stored on-site, coordinate with personnel at the storage location to gain access to secured areas, locked containers, or storage devices.

Access to remotely stored evidence may be acquired over network cables, phone cables, or through wireless connectivity. It may be necessary to contact other personnel who can access the DME and make arrangements to preserve the data.

### **Gaining Logical Access**

Username and passwords may be required to gain logical access to the data on the system. Local network information, such as IP addresses, may also be required.

### **Controlling Access**

Controlling access to the system can be accomplished by limiting physical access to the recording/storage device and by isolating the recording/storage device from external sources. External sources of access include network cables, phone cables, and wireless communication devices.

### **Preventing Loss**

Steps should be taken to ensure no overwriting of the relevant data occurs until the data has been transferred to the acquisition media. Attention should be given to pre-scheduled data-purge and/or over-write settings.

It may be necessary to solicit the assistance of additional resources including, but not limited to, manufacturer support personnel, network administrators, or a qualified computer forensic examiner.

A sudden loss of power could cause destruction of the evidence. Terminating the power source should be considered a last resort.

## **PART II – Acquisition of DME**

**Acquisition of DME** should consider the following:

- Document system information
- Determine the most accurate method of data recovery
- Transfer all codecs and required viewer files from the DVR
- Transfer all relevant media files from the DVR
- Verify that transferred media files are playable on a separate computer
- Verify that all relevant media was transferred and that it is a fair representation of what was on the DVR

### **1. Document System Information**

Documentation should include the following:

- DVR make and model,
- Serial number(s),
- software version number(s),
- relevant usernames and passwords
- date & time off-set (calibrated to real time referencing an accurate time source; eg: CAD),
- number of operating cameras,
- any other relevant information.

### **2. 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. Exporting in multiple formats may be advantageous. In addition to acquiring the native video files, a transcoded copy (eg: *.avi*) may provide an interoperable format for ease of use by investigators. Note: Transcoded copies are often of lesser quality than the native file format.

There are a number of acquisition methods, which include:

- Using the DVR software to export the native file format
- Copying the originally recorded files related to the event from the DVR
- Using a screen capture utility to record the DME in a usable format
- Use the DVR to export transcoded media files
- Creating binary images of drives on the DVR
- Seizing the DVR
- Capturing playback from the DVR with an analog recording system.

### **3. Transfer all codecs and required viewer files**

If the media requires a proprietary player or a specific codec in order to be played, transfer the player and/or codec with the media.

### **4. Transfer all relevant media files**

Determine which files are related to the incident, including all media and metadata files.

### **5. Verify that transferred media files are playable on a separate computer**

Load media files, proprietary players and/or codecs onto the computer used for acquisition and verify the media files are viewable.

### **6. Verify that all relevant media was transferred and that it is a fair representation of what was on the recording system**

Compare exported video to the original system to verify that the images transferred onto the computer used for the acquisition appear the same.

## **PART III – ADDITIONAL CONSIDERATIONS**

It may be necessary to seize the DVR. Consideration should be given to the impact on the DVR owner balanced with the needs of the investigation and data protection.

The acquired data is evidence and proper procedures should be followed, including chain of custody, integrity verification, evidence protection and storage of the digital media.

All personnel involved in the acquisition of DME should obtain adequate training.

Agencies involved in the analysis of DME should ensure their examiners develop specialized skills and knowledge in the area of DME Processing.