Scientific Working Group on Digital Evidence

SWGDE Best Practices for Data Acquisition from Digital Video Recorders

Disclaimer:
As a condition to the use of this document and the information contained therein, the SWGDE 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) in the United States or any Foreign country. 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) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 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 secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

Redistribution Policy:
SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

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

Requests for Modification:
SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for change

Intellectual Property:
Unauthorized use of the SWGDE logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

SWGDE Best Practices for Data Acquisition from Digital Video Recorders

Table of Contents

1. Purpose

The purpose of this document is to provide best practices for acquiring video, audio, and associated data evidence from digital video recorders (DVRs).

These guidelines may also be used to assist agencies when developing standard operating procedures (SOPs) for the acquisition of video and audio evidence from digital video recorders.

2. Scope

This document provides guidance for acquisition of evidence utilizing a DVR's operating system to export the native or proprietary data for use in a criminal investigation and/or prosecution. Consumer-grade DVRs are designed for data to be exported by a user with no training or experience. This document identifies a forensic workflow for acquisition of data from such devices. The purpose of this workflow is to extract best evidence and ensure data integrity.

3. Limitations

The responding individual should have some knowledge of DVRs and a basic understanding of video evidence. This document is not intended to be an exhaustive guide for field personnel that do not have experience acquiring video evidence. Legacy digital outputs are not described in this document; for more information on these options, see *SWGIT Section 24 Best Practices for the Retrieval of Digital Video* [**1**].

This document describes procedures for acquiring data of evidentiary value from consumer-grade DVRs. Methods of retrieval for investigative leads, such as video capture, are not addressed.

This document does not address cloud-based recordings. For more information on cloud-based recordings, see *SWGDE Best Practices for Digital and Multimedia Evidence Video Acquisition from Cloud Storage* [**2**].

This document does not address a computer forensic examination. In rare cases where exporting the data from the device in the field is not practical or feasible, data recovery may require removal of the recording device and the inclusion of a computer forensic examination workflow.

4. Types of Digital Video Recorders

Digital video recorders are primarily found in residential, commercial, or governmental institutions and include these major types:

- Stand-Alone Embedded Digital Video Recorder
- Stand-Alone Network Video Recorder
- Hybrid Digital Recorder
- Dedicated Computer
- Personal Computer
- Server-Based (only accessible by client station)

4.1 Stand-Alone Embedded Digital Video Recorder

Menu-driven device containing a recording system that typically uses a proprietary operating system to convert analog video to digital data and store it.

4.2 Network Video Recorder

Menu-driven device containing a recording system that typically uses a proprietary operating system to accept a digital stream and store it (the conversion from analog to digital occurs on the camera).

NOTE: IP cameras may have the capability of recording multimedia to an SD card on the camera as the primary recording or as a backup.

4.3 Hybrid Digital Recorder

Menu-driven device capable of recording both a network (digital) video stream and/or an analog signal.

4.4 Dedicated Computer

PC-based proprietary system dedicated to recording video.

4.5 Personal Computer

Standard personal computer running video recording software and likely other software.

4.6 Server Based

Network accessed storage (NAS) that may be stored either locally or remotely.

5. DVR Recordings

When acquiring video evidence, the goal is to obtain the highest quality data from the DVR. Most DVRs allow for the export of data. Consideration should be given to the following:

- The evidence from DVRs is perishable and should be acquired as soon as possible.
- The proprietary file format is most likely to provide the best video evidence. This should be the first choice when exporting video and audio evidence.
  - If available, the proprietary player or codec should be downloaded while on scene.
- A secondary export of an open file format may also be obtained, time and safety permitting.

6. Compression

Compression encodes data to reduce the amount of storage used within the DVR. DVRs vary in the amount and type of compression applied to the recordings. Compression settings are usually chosen when the DVR is initially configured. The compression settings should be documented before acquisition. Adjusting the settings during acquisition is not recommended; it will not improve the quality of video that has already been recorded.

- A review of the live monitor may appear to be of better quality than the actual recorded video because compression has not yet occurred.
- For more information, an explanation of compression and issues pertaining to it can be found within *SWGDE Technical Overview of Digital Video Files* [**3**].

7. Legal Considerations

Proper legal authority should be obtained before seizing or acquiring video evidence from a DVR. Refer to organizational policy regarding specific requirements for warrants, consent, or exigent circumstances.

8. Recommended Equipment

The following is a list of equipment that will assist with the acquisition of video and audio evidence from DVRs: (*Note: "**bold**" text indicates priority equipment*.)

- Devices
  - **Portable computer** with:
    - **Administrator rights**
    - **Capability to install proprietary viewers**
    - **No restrictions that would impede the download** (e.g. firewalls, organization software)
    - **USB ports**
    - **Optical media drive** (may be peripheral or built-in)
    - **Network port (RJ45)**
  - Analog capture device
  - Write blocker
  - Scan converter
  - **USB mouse**
  - **Monitor**
  - USB keyboard
- Media
  - Optical disc media (e.g. CDs, DVDs, Blu-ray, etc.)
  - USB flash drives (variety of sizes 1GB and larger)
  - External hard drive

- Cables
  - Composite cable
  - USB extension cable
  - Network cable
  - BNC to RCA adapters
  - VGA to DVI adapter
- Other items
  - **Digital camera**
  - Flashlight
  - Mirror
  - Archival media markers[1]
  - Batteries
  - Power strip and extension cord
  - Gloves
  - Documentation (chain of custody, notes, consent)
  - USB splitter
  - Ladder
  - Phillips and flathead screwdrivers
- Evidence packaging

9. Steps to Take Prior to Acquisition

- Determine the physical location of the recording device. Video may have been captured at remote locations other than the scene of incident. It is preferable to acquire video data directly from the primary recording device rather than through a remote connection or viewing app.
- Obtain legal authority.
- Locate a manual to assist with system information (e.g. passwords, output options) if this information is not known by the system owner/operator.
- Determine whether the relevant video is still on the DVR.
- Locate and view the area of interest.
- Determine how much data needs to be acquired.
- Determine the best method for acquisition.
- Canvass the area for other existing recording devices.
- To prevent tampering, consider isolating the device from any outside network connection (do not disconnect active IP cameras).
- Consider disabling any additional monitors.

[1] Solvent-based permanent ink markers should not be used for labeling optical media discs; use water- or alcohol-based ink markers designed specifically for disc media. For information on how permanent ink markers may affect a disc's data-storing layer, see https://www.tapeonline.com/using-permanent-ink-markers-on-cds-dvds.

10. Steps to Take During Acquisition

Notes should be kept during the acquisition process (see **Appendix A: Sample Audio/Video Field Retrieval Worksheet** at the end of this document for an example). Photographs may also be used in lieu of, or in addition to, written notes.

10.1 Items that should be documented

- Scene contact information:
  - Scene address
  - Scene point of contact and telephone number
- Type of DVR
- Make, model, and serial number of DVR
- DVR password(s) and username(s)
- Number of cameras capable of recording and number of cameras connected
- System time and date and actual time and date
  - NOTE: Do not change the time and date on the DVR system.
  - Calculate if there is a time offset between real time, using a known time reference, such as the Naval Observatory Clock, and the DVR system clock.
  - Applications are available for smart devices that will assist with the offset calculations.

10.2 Additional items that should be documented (if possible)

- Number of microphones capable of recording and number of microphones connected
- Earliest recorded date/time
- Storage capacity
- Whether overwrite is enabled
- System settings:
  - Image quality (i.e. high, medium, low)
  - Frames per second
  - Recorded image/frame size (e.g. 320 x 240)
  - Alarm or motion trigger settings for cameras
  - System firmware version
- System logs
  - Logs may be exported directly or documented through photographs of system display, depending on the system
- Also consider photographing the DVR system, cameras, and connections or sketching camera placement (if necessary).

11. DVR Outputs

Multiple factors, including the amount of evidence to be collected, will determine which output option should be selected from those available.

- DVRs that record in a proprietary file format may use an associated viewer application for playback of output files. You may have to manually select this option to copy the viewer along with video files.
- Some DVR systems limit the amount of data that can be retrieved (downloaded/exported) at a time. This limit may not be specified in the system manual or known to the manufacturer.

11.1 USB Devices

Generally, the DVR's software will have an archive, backup, copy, or export function with which you can offload the data directly to the device attached. If the DVR does not recognize the USB device:

- Formatting the attached USB device using the DVR's operating system may be necessary. Formatting attached devices may be a DVR menu option.
- The USB device's capacity may be too large for the DVR to recognize. Consider trying another USB device of a smaller capacity.
- A broken USB port may also prevent USB devices from being read or recognized by the DVR. Indicator light on USB drive, if present, may help to determine if the port is functional.

11.2 Optical Media Writer

DVRs may have an optical media writer to output recorded data. Generally, the DVR's software will have an archive, backup, copy, or export function with which you can output data directly to the optical media writer. Write-once optical media should be used in preference to rewritable optical media. *NOTE: Some DVRs may only accept a rewritable disc.* If the data is downloaded to rewritable media, transfer the data to non-rewritable media or secure electronic storage as soon as possible. The transfer should be verified according to the methods outlined in *SWGIT Section 13 Best Practices for Maintaining the Integrity of Digital Images and Digital Video* [**4**].

11.3 Network Connection

Many DVRs have network ports. Furthermore, many DVRs have their own proprietary network viewer software that allows for playback and output of the recorded data.

A computer can be connected to the DVR with an ethernet cable to transfer data. Prior to transfer, the network viewer software may need to be installed on the connected computer, although some DVRs will have the viewer available through a web browser. Any setting(s) changed to facilitate connectivity should be made on the destination computer, if possible, rather than on the DVR.

- Network viewers may only allow for viewing the video or the download of an open file format.
- The IP address may be obtained from the DVR menu. Some network viewers are installed on the DVR system for easy access. Otherwise, searching the vendor's website or contacting the vendor directly may be necessary.
- If a network viewer for the system does not exist, a connection may be possible utilizing Windows Explorer, or other web browser, and typing in an appropriate IP address.
- You may need to change security settings on your browser to transfer the data.
- Document the original IP address of the DVR as well as any changes made. Some DVR systems have a limitation on the amount of data that can be transferred.

12. Removal of DVR Unit

In certain circumstances it may be necessary to seize the DVR for submission and/or examination by an analyst. Examples include:

- The amount of video evidence is too large to be downloaded on scene.
- The output ports on the DVR may not be functioning.
- The technician is not able to gain full logical access to the device.
- Officer safety is at risk.
- The DVR may need to be seized to protect the evidence, or if continued access could impact an ongoing investigation.
- Acquisition of data directly from the hard drive is the most appropriate way remaining to obtain relevant data and metadata.
- If the area of interest is not found or believed to be "Deleted" or otherwise inaccessible.
- All other attempts to export data have failed.

If the video is viewable on scene, make a copy of the playback with a recording device (using an analog video recorder or digital recorder) before powering down the DVR. The DVR should be properly powered off before removal, either through system settings or a power switch before

unplugging the machine. Collect all relevant components of the system (e.g. power supply, remote control, manual).

13. Steps to Take After Acquisition and Prior to Leaving Scene

- Complete all the necessary documentation.
  - Initiate a chain of custody for the evidence, per organizational policies.
- Collect all required video data and proprietary playback software/codec(s).
- Verify the acquired video evidence plays back correctly on your portable computer and that the correct dates and times were retrieved.
- The recording system has been returned to its original state (i.e. any changes to the system settings have been restored).
- Any evidence stored on a temporary storage device (e.g. USB drive, rewritable media) should be transferred to a permanent storage device.
- Refer to *SWGDE Best Practices for Maintaining the Integrity of Imagery* [**5**] and local organizational SOPs for guidance on securing and authenticating acquired data.

14. References

[1] Scientific Working Group on Imaging Technology, "Section 24: Best Practices for the Retrieval of Digital Video". [Online]. https://www.swgit.org/documents/Current%20Documents

[2] Scientific Working Group on Digital Evidence, "SWGDE Best Practices for Digital and Multimedia Evidence Video Acquisition from Cloud Storage,". [Online]. https://www.swgde.org/documents

[3] Scientific Working Group on Digital Evidence, "SWGDE Technical Overview of Digital Video Files,". [Online]. https://www.swgde.org/documents

[4] Scientific Working Group on Imaging Technology, "Section 13: Best Practices for Maintaining the Integrity of Digital Images and Digital Video". [Online]. https://www.swgit.org/documents/Current%20Documents

[5] Scientific Working Group on Digital Evidence, "SWGDE Best Practices for Maintaining the Integrity of Imagery,". [Online]. https://www.swgde.org/documents

Appendix A

Appendix A Sample Audio/Video Field Retrieval Worksheet

AUDIO/VIDEO FIELD RETRIEVAL FORM

Incident #: _____ **Offense Type:** _____

Location (Address): _____

Scene Point of Contact: _____

Scene Point of Contact Telephone Number: _____

Date & Time of Offense: _____

Date & Time of Acquisition: _____

Date & Time– Actual: _____ **Date & Time– DVR:** _____

DVR Recording Date & Time Difference to Actual (Time Offset): _____

DVR Type & Manufacturer: _____

DVR Model #: _____ **DVR Serial #:** _____

DVR Username: _____ **DVR Password:** _____

ADDITIONAL INFORMATION (IF AVAILABLE):

Earliest Recorded Date/Time: _____ **Manual for DVR available?** ☐ **Y** ☐ **N**

Storage Capacity: _____ **Overwrite Enabled:** ☐ **Y** ☐ **N** **Firmware Version:** _____

# of Cameras Possible: _____ **# of Cameras Attached to the DVR:** _____ **Cameras Exported:** _____

Camera Resolution: _____ **Camera Frame Rate:** _____ **Logs Present:** ☐ **Y** ☐ **N** **Logs Exported:** ☐ **Y** ☐ **N**

Image Quality: ☐ **High** ☐ **Medium** ☐ **Low** ☐ **Other** _____ **Camera Settings (e.g. alarm or motion triggered):** _____

Starting Date & Time of Selection: _____ **Ending Date & Time of Selection:** _____

Media Backup Format: _____ **Media Copied to: DVD** _____ **CD** _____ **Flash Drive** _____ **Other** _____

Notes:

• Native/proprietary video files should be the highest priority. • Verify video exported on a separate PC prior to leaving scene if possible. • Create a hash value for any video retrieved. • Begin Chain of Custody immediately. • Properly label and protect all electronic evidence. • Do not use ball point pens or stickers on CDs, DVDs, or other disc-based media. • Fill out as much information as you have available on this form. • Retain this form as part of the case file.

SWGDE Best Practices for Data Acquisition from Digital Video Recorders

History

Revision	Issue Date	Section	History
1.0 DRAFT	2017-08-24	All	Initial draft created and SWGDE voted to release as a Draft for Public Comment.
1.0 DRAFT	2017-10-17	All	Formatting and technical edit performed for release as a Draft for Public Comment.
1.0 DRAFT	2018-01-11	12	Minor grammatical changes. Added additional reason to Section 12. SWGDE voted to publish as an Approved document (Version 1.0).
1.0	2018-04-25	--	Formatted and published as Approved Version 1.0.