Standard Practice for Data Retrieval from Digital CCTV Systems

Video/Imaging Technology & Analysis Subcommittee
Digital/Multimedia Scientific Area Committee
Organization of Scientific Area Committees (OSAC) for Forensic Science

OSAC Proposed Standard

Standard Practice for Data Retrieval from Digital CCTV Systems

Prepared by
Video/Imaging Technology & Analysis Subcommittee
Version: 2.0
June 2020

Disclaimer:

This document has been developed by the Video/Imaging Technology & Analysis Subcommittee of the Organization of Scientific Area Committees (OSAC) for Forensic Science through a consensus process and is *proposed* for further development through a Standard Developing Organization (SDO). This document is being made available so that the forensic science community and interested parties can consider the recommendations of the OSAC pertaining to applicable forensic science practices. The document was developed with input from experts in a broad array of forensic science disciplines as well as scientific research, measurement science, statistics, law, and policy.

This document has not been published by an SDO. Its contents are subject to change during the standards development process. All interested groups or individuals are strongly encouraged to submit comments on this proposed document during the open comment period administered by ASTM International (www.astm.org).

Ballot Rationale: This document is intended to provide procedures and information to aid in for the proper collection of data from DCCTV Digital Video Recorders (DVRs).

Standard Practice for Data Retrieval from Digital CCTV Systems[1]

This standard is issued under the fixed designation X XXXX; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last re-approval. A superscript epsilon (ε) indicates an editorial change since the last revision or re-approval.

1. Scope

1.1 This document provides procedures that ensure playback while maintaining best quality of evidence for the collection of data from Digital Video Recorders (DVRs). It also can aid in the development of Standard Operating Procedures (SOPs).

1.2 This document does not address Forensic Video or Audio Analysis Techniques performed after the retrieval of data.

1.3 No system units are required for this standard practice.

1.4 This standard practice does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety and health practices and determine the applicability of regulatory limitations prior to use.

2. Referenced Documents

2.1 ASTM Standards:[2]

E2916-13 Standard Terminology for Digital and Multimedia Evidence Examination

2.2 TSWG and Federal Bureau of Investigation Material[3]

Best Practices for the Retrieval of Video Evidence from Digital CCTV Systems v1.0 (October 2006)

2.3 Home Office Scientific Development Branch Material:[4]

[1] This Practice/Guide is under the jurisdiction of ASTM Committee *Digital Multimedia Scientific Area Committee* and is the direct responsibility of Subcommittee *Video / Imaging Technology and Analysis*.

Current edition approved XXX. XX, XXXX. Published XX XXXX. DOI: 10.1520/XXXXX-XX.

[2] For referenced ASTM standards, visit the ASTM website, www.astm.org, or contact ASTM Customer Service at service@astm.org. For Annual Book of ASTM Standards volume information, refer to the standard's Document Summary page on the ASTM website.

[3] Available from Combating Terrorism Technical Support Office (CTTSO), http://www.cttso.gov/?q=node/229

[4] Available from Home Office Scientific Development Branch, Sandridge, St. Albans, AL4 9HQ, United Kingdom http://webarchive.nationalarchives.gov.uk/adv_search/

66-08 Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems v.2.0 (August 2008)

2.4 LEVA Material:[5]

2.5 Best Practice for the Acquisition of Digital Multimedia Evidence v.3.0 (April 14, 2010)

2.6 SWGIT/SWGDE Material:[6]

SWGIT Section 24 Best Practices for the Retrieval of Digital Video, v.1.0 (September 27, 2013)

3. Terminology

3.1 *Definitions:*

3.1.1 *aspect ratio, n*—the ratio of the width to the height of a rectangle, such as an image a pixel or an active video frame. **ASTM E2916-13**

3.1.2 *bit stream duplicate, n*—in computer forensics, an exact, bit-for-bit reproduction of all data objects independent of any physical media upon which that data is stored. (Compare copy). **ASTM E2916-13**

3.1.3 *codec, n*—an algorithm to encode and decode digital data, typically to reduce the amount of data for transmission or storage. **ASTM E2916-13**

3.1.3.1 *DISCUSSION*—A codec is not a storage format, but may be required to interpret stored data.

3.1.4 *copy, v*—to reproduce information with some level of accuracy **ASTM E2916-13**

3.1.4.1 *DISCUSSION—Depending on the process used, copying might result in a loss of data (Compare bit stream duplicate).*

3.1.5 *compression, n*—a process to reduce the size of a data file or steam while attempting to retain the original semantic meaning of that data. **ASTM E2916-13**

3.1.6 *data, n*—information in analog or digital form that can be transmitted or processed. **ASTM E2916-13**

[5] Available from Law Enforcement & Emergency Services Video Association (LEVA) International, Inc., 84 Briar Creek Road, Whitesboro, Texas 76273, https://leva.org/

[6] Available from Scientific Working Group on Digital Evidence (SWGDE), https://www.swgde.org/

3.1.7 *digital video recorder, DVR, n*—a stand-alone embedded system or a computer-based system for recording video and, optionally, audio data. **ASTM E2916-13**

3.1.7.1 *DISCUSSION*—For example, a digital video recorder can be a Stand-Alone Embedded Digital Video Recorder, Personal Computer (PC), Network Video Recorder (NVR), etc.

3.1.8 *image set, n*—an accurate and complete reproduction of all data objects, independent of physical media, that are saved as files. **Best Practices for the Retrieval of Video Evidence from Digital CCTV Systems**

3.1.9 *intermediate storage, n*-any media or device on which data is temporarily stored for transfer to permanent or archival storage. **ASTM E2916-13**

3.1.10 *master evidence, n*—the original retrieved data irrespective of media. For example, if the recorded video from the DVR hard drive was downloaded to CD/DVD, that CD/DVD is defined as the master. **Best Practices for the Retrieval of Video Evidence from Digital CCTV Systems**

3.1.11 *metadata, n*—data, frequently embedded within a file, that describes a file or directory**. ASTM E2916-13**

3.1.12 *proprietary file format, n*—any file format that is unique to a specific manufacturer or product. **ASTM E2916-13**

3.1.13 *resolution, n*—in facial identification, image and video analysis, a measure of the limit of an imaging system's capability to distinguish between two separate but adjacent stimuli, such as elements of spatial detail in an image, or similar colors. **ASTM E2916-13**

3.1.14 *work copy, n*—a copy of a recording or data that can be used for subsequent processing and/or analysis. **ASTM E2916-13**

3.1.15 *forensic wipe, n*—in computer forensics, a verifiable procedure for sanitizing a defined area of digital media by overwriting each byte with a known value. **ASTM E2916-13**

4. Summary of Practice

4.1 Recognize and protect Digital CCTV Systems and data.

4.2 Gather information that will assist with further analysis.

4.3 Evaluate the system output options to determine the best and most practical method that will provide the highest quality of evidence.

4.4 Whenever possible, the proprietary file(s) and playback software or codec(s), or both, should be downloaded to a secure electronic storage option to maintain the integrity and quality of the master evidence.

4.4.1 Working copies are to be produced from the master evidence.

5. Significance and Use

5.1 Data retrieval from DVRs may not follow the same methodology as Computer Forensics.

5.2 Due to its evidentiary value, as well as its potential value for intelligence and security matters, it is imperative that data from DVR systems is properly recognized, protected and collected.

5.3 It is highly recommended that the individual retrieving data from CCTV systems should have training and familiarity of these devices prior to retrieving data.

6. Recognizing Digital CCTV Systems and Data

6.1 Digital CCTV systems include three major types:

6.1.1 Stand-Alone Embedded Digital Video Recorder: Menu-driven device containing a recording system that typically uses a Linux based operating system.

6.1.2 Personal Computer (PC): May appear to be a standard computer or may be a proprietary turnkey system with video and audio recording capability.

6.1.3 Network Video Recorder (NVR): Records video and audio from a network connection to a storage device. Data may be recorded or stored at a scene or an off-site location.

6.1.4 These systems may include a built-in multiplexer, transactional data, audio recording capabilities, other peripheral devices, network capabilities, and camera control capabilities. PC-based systems may also contain business or personal data, or both.

6.2 Most DVRs utilize compression to reduce the amount of data storage and transmission requirements.

6.3 The live camera view(s) may appear to be of better quality than the actual recorded video.

6.4 DVR output maybe in a proprietary file format, which usually requires proprietary playback software or a special video or audio codec(s) (or both) from the manufacturer in order to review the files and any metadata (for example, time, date, camera number/name).

6.4.1 The software may automatically copy the proprietary viewer to the output option; however, this specification may need to be manually selected. A correct version should be retrieved from the manufacturer, if the system does not provide a copy. Important: Make sure you download the correct player for the operating system.

6.5 DVRs may allow the data to be downloaded / exported in an "open file format" that can be reviewed in non-proprietary software (for example, AVI in Windows Media Player or MOV in QuickTime). While these formats usually facilitate instant usability, there are several issues including:

6.5.1 The open file format still may be proprietary, which would require additional codec(s) or software.

6.5.2 Open file formats often further compress the video or audio data, or both, which results in a reduction of quality.

6.5.3 Metadata such as time and date information may be lost or modified.

6.5.4 These formats often provide a different resolution or aspect ratio, or both, compared to the proprietary file due in part to the specifications chosen upon export.

7. Protecting DVR Data

7.1 The list of actions below should be followed upon arrival in preparation to acquire all relevant information. This will ensure evidential integrity and the ability to review the data.

7.1.1 Important: Documentation of affirmative permission / consent granted by the owner of the device or a valid search warrant may be necessary (per state law) before beginning any retrieval of evidence from a digital device.

7.1.2 Contemporaneous notes should be kept to provide an audit trail detailing the course of action taken.

7.2 Gain Physical Access

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

7.2.2 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 DVR data and make arrangements to preserve the evidence.

7.3 Gain Logical Access

7.3.1 Usernames 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.

7.3.2 Be aware that the standard user password may provide only limited functionality and an administrator password may be necessary in order to enable data retrieval. Administrative or engineer login access to the DVR usually allows more options for retrieval, including proprietary files.

7.3.3 Determine if a manual is available to assist with system information (for example, passwords, and output options).

7.3.4 A translator may be necessary for those interfaces that use foreign languages.

7.4 Control Access

7.4.1 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. Disconnecting external sources of access such as network cables, phone cables and wireless communication devices should be considered.

7.5 Prevent Loss

7.5.1 Whenever possible, the system should remain recording during the retrieval of the data unless:

7.5.2 Some devices stop recording in order to facilitate the export of data. This may be an unavoidable feature of the system.

7.5.3 There is an immediate risk that important data will be overwritten before it can be retrieved. Steps should be taken to ensure no overwriting of the relevant data occurs until the data has been transferred to the acquisition media. Some systems allow write-protecting a selected video sequence to prevent it from being overwritten before it can be retrieved; however, it should not be assumed that this option will be present.

7.5.4 Attention should be given to pre-scheduled data-purge or over-write settings. This is particularly important if the retrieval cannot be carried out immediately, or needs to be prioritized against other tasks. A maximum time period can then be determined within which the retrieval must be carried out before data is lost.

7.5.4.1 Video systems can be configured for data pruning. "Pruning" reduces the frame count and/or resolution of the recorded video for archiving. This is generally done over a period of time.

7.5.5 This can be accomplished by determining the earliest recorded date. For example, if the earliest recorded date is seven days prior to the incident, it may be seven days before the relevant data is overwritten. However, factors such as motion detection, frequency of alarm triggers (for example, doors opening), recording schedules, etc., could shorten the length of the maximum time period. When the storage device is full, new data overwrites the oldest recorded data in a manner that is not recoverable.

7.5.6 Do not change the time and date on the DVR system as this update may lead to data loss.

7.5.7 Any discrepancy between the system time and real time should be recorded in the notes and accounted for. It is suggested that a reference clock be used, such as the Navy Observatory Master Clock or NIST Telephone Time of Day Service. These services will provide the current time for the local time zone.

7.5.7.1 IP cameras can produce their own on-board time and date that is independent from and may differ with the NVR time and date. Both should be documented.

7.5.8 Determine if a date/time change occurred in-between the time of the incident and the time of acquisition, which would throw off the offset. This will ensure the correct section of data is acquired.

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

7.5.10 When data is deleted by other means (for example, formatting the storage device or restoring factory settings), the space occupied by that data is marked as free for recording. Deleted data in this space may be recoverable for a limited amount of time before being overwritten. However, this is dependent on the formatting process used (for example, Quick Formatting vs. Full Format).

7.5.10.1 It may be necessary to solicit the assistance of additional resources including, but not limited to, manufacturer support personnel, network administrators or a qualified Video or Computer Forensic Examiner.

7.5.11 The venue owner/security system operator may be an option for assistance if appropriate due to the nature of the investigation.

8. Collecting data from DVRs

8.1 Establish that relevant video and audio (if possible) has been recorded by reviewing the recording. Preferably, a person with knowledge of the recording device should operate it during playback, if it is appropriate for them to do so. Care should be taken not to change settings on the DVR.

8.1.1 Refer to the CCTV System Information Form (X1) for an example of what should be documented before the retrieval process. Also, photograph the system if possible. The photographs will provide assistance in returning the system to its original state if any changes are made to facilitate retrieval such as settings or cable connections.

8.2 The following items should be reviewed and documented before the retrieval process:

8.2.1 Scene contact information such as address, hours of operation, scene/DVR point(s) of contact, email and phone number(s).

8.2.2 DVR type (for example, PC-based, Stand-Alone Embedded or NVR).

8.2.3 DVR make/model and serial number.

8.2.4 Device or operating system, user name and password.

8.2.5 Administrative/Engineer user name and password.

8.2.6 Date/Time display and actual date/time.

8.2.6.1 Any discrepancy between the system time and real time.

8.2.7 Number of recording units.

8.2.8 Number of hard drives and storage capacity.

8.2.9 Network Connection.

8.2.10 System firmware version.

8.2.11 Applicable event log(s).

8.2.12 The total number of cameras connected to the DVR and their associated camera numbers/names.

8.2.13 Camera type (for example, alarm/motion triggered or infrared), transmission method; and resolution. Note: a camera may have a local storage option that utilizes removable flash media.

8.2.14 Make(s) and model(s) of camera(s) if known.

8.2.15 System settings to include, but not limited to transmission method, camera resolution, record mode (for example, time lapse recording, for example 2,6,12,24,48,72 hour), image quality (for example, high, medium, low), frames/images per second, recorded image/frame size (for example, 320x240), and audio quality/configurations (for example, mono/stereo, sampling rate).

8.2.16 The total number of microphones/audio inputs connected to the DVR and if the audio is able to be downloaded/exported.

8.2.17 Changes made to the system (for example, overwrite, display settings, etc.) and if photographs were taken.

8.2.18 Hardware export options.

8.2.19 File format export options.

8.2.20 The playback software name and version number if available for export or documented in the user manual.

8.2.21 Passwords associated with playback software.

8.2.22 Prepare a sketch of the camera placement to facilitate the decision making process if time permits and per organization procedures (See X2).

8.3 A determination should be made as to how much and what type of data needs to be retrieved from the DVR. Knowing the timeframe and camera view(s) of interest will aid in this decision.

8.3.1 A listing of all applicable camera numbers/names should be provided by the requestor, which will provide more specific information than a request for “all exterior cameras” or “all cash registers,” for example. This will expedite the retrieval process as well as assist in documenting that all DVR evidence was collected.

8.3.2 Determine if the cameras can be downloaded and played back separately. All the DVR data for the required area of interest should be taken as it was recorded. These cameras should be recorded in isolation, showing one camera full screen and not multi-cameras on a single screen (for example, not 4, 9, and 16 on a single screen).

8.4 Generally, the DVR system software will have an archive, backup, copy, download or export function that will facilitate data retrieval directly to an output option.

8.4.1 It is not recommended that any additional software be installed on the DVR system for example, CD writing software, if it is not present. If it is necessary to install additional software, it is highly recommended to contact the manufacturer prior to installation.

8.4.2 Some DVR systems have a limitation on the amount of data that can be retrieved (downloaded/exported) at a time, typically 1GB, sometimes 2GB. This limit may not be specified in the system manual or known to the manufacturer. It is best to keep file(s) under 1GB, unless it is confirmed that the system is capable of more.

8.5 A downloaded/exported file without the time/date data may provide the highest quality footage. However, a second retrieval of the footage that includes the time/date data should also be recovered to provide this information.

8.5.1 On systems where the time/date stamp can be moved within the frame, ensure that this overlay does not obscure critical events.

8.6 (regardless of the submitted request), all recorded data from all camera views for the requested time should be collected.

8.6.1 It is advisable to collect a non-relevant camera view from the system in the instance that there is an issue with playback. For example, files that do not playback or have readily available software for playback may need manual decoding. It is not a best practice to experiment with decoding options on the actual evidence.

8.7 An evaluation of the output options of the system should help determine the best and most practical method. Collecting the proprietary file(s) should remain the highest priority to ensure image quality and provide the best evidence. Other factors to consider include the amount of media required and the data transfer time. For example:

8.7.1 If the incident is, for example, a 10-minute robbery, the system has a CD writer and the proprietary file(s) fit on a CD, then collection on CD would be the best method.

8.7.2 If the request is, for example, for 24 hours of video and the system has an external USB port, connecting an external USB hard drive may be the best option. This assumes that the system allows for recovery of large amounts of data at one time.

8.7.3 If the request is, for example, for 30 days of video, the best, or only, option may be producing a bit stream duplicate of the hard drive(s) or removing the recording unit, or both, from the scene.

8.8 To enable retrieval from a variety of DVRs that will be encountered, a range of equipment is recommended. See the Recommended Equipment list for more information (X3).

8.9 Performing a test by retrieving a portion of the video will provide guidance about the time and storage requirements for the chosen output option.

8.9.1 If the possibility exists that the data from the DVR retrieval will be used for identification purposes, including but not limited to facial recognition, the collection of aspect ratio calibration data (e.g. sphere method) is recommended.

8.10 When it is impractical or not economically viable to download the requested data and the DVR is too large or complex to be removed, the amount of DVR data to be retrieved should be reevaluated. For example:

8.10.1 It may be possible to reduce the volume of data required by reconsidering the time period of interest or the number of cameras needed.

8.10.2 By reducing the volume of data, it may then be possible to use some of the methods that had previously been rejected.

8.11 The list below is organized with the beginning considered most advisable to the end being the least advisable from a technical and quality of service standpoint.

8.12 CD/DVD Writer

8.12.1 Many DVRs have a built-in or external (USB) CD/DVD writer to retrieve recorded data. In some instances, an external CD/DVD/Blu-ray writer can be connected through a USB/FireWire/SCSI port (see USB/FireWire/SCSI Devices).

8.12.2 Secure electronic storage options should be used (e.g., Write-Once/Read Many (WORM) CD-Rs, DVD-Rs, DVD+Rs, or Blu-ray).

8.12.3 Some DVR systems may only provide an intermediate storage option (e.g., a CD-RW/DVD-RW disc). Any files exported/downloaded to this rewritable medium should be transferred to a secure electronic storage option as soon as possible.

8.12.4 Some drives may only write to a specific brand(s) of media. Consult the DVR or drive user manual to determine which media brand(s) is compatible, or attempt various brands of media if difficulties are encountered.

8.12.5 The system may require that the CD/DVD is formatted, either in the DVR itself or in another computer.

8.12.6 The system may require that the CD/DVD be finalized in the original recording device before the disc can be read in other devices.

8.12.7 The resulting produced WORM media or file(s) on the secure electronic storage is the master evidence.

8.13 Removable Storage Devices

8.13.1 USB ports can be used to connect external storage devices such as flash media (for example, “thumb drives” or flash card options such as CF, SD, MicroSD, xD, etc.,), CD/DVD writers, hard drives, and legacy devices. FireWire/SCSI/eSATA ports may also be present.

8.13.2 Removable storage devices such as flash media and legacy media should be considered intermediate storage.

8.13.3 External hard drives are a good resource when large amounts of data need to be collected.

8.13.4 Establish that the port is a working port for data collection (not a mouse port or system update port), as well as the type of device (format, capacity, and /or brand), with which the port is designed to work.

8.13.5 Some devices may require activation by installing the necessary drivers on the recording system. It is recommended that the manufacturer be contacted before attempting to install any drivers.

8.13.6 Removable storage devices often need to be formatted to a specific capacity and file system recognizable to the DVR.

8.13.7 Some systems that employ flash media drives export files in real time (for example, a 10 - minute file will take 10 - minutes to download/export). This may not be the most appropriate option for the retrieval of a large amount of data.

8.13.8 It may be possible on some PC based systems that utilize a standard Windows Operating System to copy the proprietary file(s) using Windows Explorer.

8.13.8.1 Note: This does not work on all systems as the file(s) retrieved in this manner may require the use of the hardware/software during the retrieval process for subsequent playback. It is strongly recommended to know the system before utilizing this method or to consult the manufacturer to ensure the file(s) copied will be capable of playback.

8.13.9 Some cameras have the option to store data locally on flash media. Check the camera body to identify if there is a removable flash card. If such a card is present, remove the card, and if applicable, use a write blocker to review the footage to assure that it is relevant. If the footage is relevant, transfer the data to a secure electronic storage option to create the master evidence. Warning: with the media card removed, the camera may no longer be recording.

8.14 Network Connection

8.14.1 Many DVR systems have network ports. Furthermore, many have their own proprietary network viewer software, which allows for connectivity and recovery of the proprietary recorded file(s).

8.14.2 If the individual recovering the data has limited experience with computers or networking, it is highly recommended that assistance be obtained prior to retrieving data using this method.

8.14.3 By utilizing the appropriate network cable, computer, and network viewer, a connection to the DVR can be established and the proprietary file(s) downloaded/exported.

8.14.4 The remote or network viewer software is installed on a separate computer/laptop, the IP address of the DVR is most likely configured in the remote viewer software, a connection is established, and the data is downloaded.

8.14.5 Verify that the network viewer will recover the proprietary file(s). For example, some remote viewers only allow for the collection of still images and not the entire proprietary recorded file.

8.14.6 Ensure administrator rights are active on the computer/laptop used for downloading/exporting the file(s). Disable any firewalls and antivirus software.

8.14.6.1 Warning: Disabling firewalls or anti-virus software, or both, can introduce risks such as viruses to the media used for download.

8.14.7 Screen savers should be disabled as they can interfere or disrupt the download/export process.

8.14.7.1 Set the power scheme settings on the computer used for downloading/exporting the file(s) to ‘always on’ with hibernation disabled.

8.14.8 The IP address may be required from the DVR. This usually requires accessing the menu functions of the DVR. Care should be taken not to change other settings on the DVR when doing this.

8.14.9 Some proprietary remote/network viewers are installed on the DVR system for easy access. Otherwise, reviewing manufacturer's information may be necessary.

8.14.10 On some systems, setting up a standard Windows network connection between the computer/laptop and the DVR may be necessary (for example, computer/laptop 192.168.10.1, and the DVR 192.168.10.2).

8.14.10.1 Important: It is best practice to retain the existing IP settings on the DVR and change those on the computer/laptop to match.

8.14.11 If a network viewer for the system does not exist, a connection may be possible utilizing Windows Explorer, a web browser, and typing in an appropriate IP address.

8.14.12 If the IP address was changed on the DVR, make note of the original IP address so that it can be changed back when complete. Changing the IP address may also require rebooting the system.

8.14.13 Some networkable systems may only allow for the video and audio to be streamed out and may not provide proprietary data transfer. Metadata can be lost through streaming.

8.14.14 Ensure network speed is sufficient such that no data is lost and to prevent crashes/timeouts during downloading/exporting.

8.14.15 After completing data retrieval, confirm that the firewall / antivirus software was re-enabled and all system settings are changed back to their prior state.

8.14.16 The computer/laptop or external hard drive(s) that was used to retrieve the DVR file(s) usually is an intermediate medium, and should be transferred to a permanent medium. If the file(s) retrieved are too large, it may be retained as the master evidence.

8.15 Replacing Hard Drives

8.15.1 In some situations, the quickest solution may appear to be removing the original hard drive(s) from the system and replacing them. This option should be considered carefully as there are many factors that come into play.

8.15.1.1 Simply removing a hard drive does not ensure the data contained on that hard drive will play back. Some DVR systems require the actual DVR hardware to playback the video on the drive.

8.15.2 An individual with computer hardware experience should be consulted. Care should be taken to follow appropriate health and safety procedures, particularly with regard to potential exposure to electricity.

8.15.3 Determine if retrieving or replacing the recording device's original hard drive(s), will void an existing warranty on the system, and arrange the proper level of authorization.

8.15.4 A brand new hard drive should be used as a replacement. It is not best practice to reuse old hard drives. See Section 8.16 for more information.

8.15.5 Power down the system prior to removing any hard drive, even if the drive appears to be "hot swappable."

8.15.6 Ensure that all of the system's hard drives are retrieved and location within the system is noted. The system may have a removable drive in a caddy, but also additional internal drive(s).

8.15.7 Document the master/slave drive configuration of all retrieved drive(s).

8.15.8 The DVR may require a specific brand, model and size of hard drive to operate correctly with a replacement. Consult the manufacturer for more information.

8.15.9 The replacement drive(s) may need to be formatted by the DVR before it will recognize and record to it.

8.15.10 Once the replacement drive(s) are installed, restart the system and confirm that recording and playback are operational, as the system may require that vendor specific software/operating system be installed. Failure to install such software can render a system either partially or completely inoperable.

8.15.10.1 Some systems require the original hard drive(s) for proper operation.

8.15.11 If the system is not operational, the DVR unit may have to be retrieved (see Section 8.18), along with the original hard drive(s).

8.15.12 The original removed hard drive(s) are the master evidence.

8.15.13 Inspect the drive(s) using a write blocker and a separate computer/laptop.

8.15.14 The bit stream duplicates are not a discussion for this section and addressed in 8.16.12.

8.16 Drive Duplication

8.16.1 In some situations, drive duplication may be necessary. This option should be considered carefully as there are many factors that come into play.

8.16.1.1 Drive duplication does not ensure playback. Some DVR systems require the original hard drive(s) for playback. The duplicated drive may also need the DVR system in order to playback the media files.

8.16.2 If the individual recovering the data has limited experience with computers or hard drives, an individual with computer hardware experience should be consulted. Care should be taken to follow appropriate health and safety procedures, particularly with regard to potential exposure to electric shock.

8.16.3 A brand new hard drive should be used as a duplicate. It is not best practice to reuse old hard drives.

8.16.4 It is recommended that a bit stream duplicate of the original hard drive(s) is produced, not an image set.

8.16.5 The system should be properly shut down prior to removing any hard drive, even if the drive appears to be "hot swappable."

8.16.6 Some systems require the original hard drive(s) for proper operation. Therefore, if the drive(s) is duplicated, place the duplicated drive back in the system, make sure the system is operational, and retrieve the original drive(s) from the scene. If the system is not operational, the recording device may have to be retrieved, along with the original hard drive(s).

8.16.7 Ensure all the original drives in the system are duplicated as the DVR may have more than one internal drive.

8.16.8 Document the master/slave drive configuration of all duplicated drives.

8.16.9 External playback software may exist to access the data on the duplicate hard drive.

8.16.10 Upon initial inspection, a hard drive duplicated from a system may not appear to contain data when viewed using a standard PC. Many systems utilize proprietary formats or operating systems or both that prevents data from being recognized. If files are not visible upon inspection of a bit stream duplicate, the drive may still contain useful data.

8.16.11 The bit stream duplicate(s) or original drive(s), or both, should be inspected using a write blocker and a separate computer/laptop.

8.16.12 The bit stream duplicates and original drives retrieved from the scene are the master evidence.

8.17 Legacy Output

8.17.1 These output methods include, but are not limited to media such as DDS Tape (Digital Data Storage), Iomega Jaz, Iomega Zip, Floppy, and Magneto Optical. They can be located inside the digital recording unit or as an attached external device. In some circumstances, this

may be the only method available on the DVR system for retrieval of the data. These can typically be connected through the SCSI port.

8.17.2 Legacy Output options, such as the media listed above are intermediate storage.

8.18 Removal of DVR Unit

8.18.1 When the above listed options are either impractical or impossible, then the decision may be made to remove the recording unit itself. This assumes that it is physically possible to do so, and that the removal is justified. For example, where the volume of data required is very large, it may be time efficient to temporarily remove the recorder and perform the retrieval in the lab, rather than on site. Alternatively, there may be no method for extracting the DVR data (for example, CD writer or USB ports), thus it would be necessary to remove the recorder and retain the unit as the master evidence.

8.18.2 Consider the legal implications if the system is removed, such as:

8.18.2.1 Some DVRs are used as both a recording system as well as a business computer.

8.18.2.2 Whether owner consent is necessary and applicable for removing the recording system.

8.18.2.3 Whether the scope of the search warrant encompasses the DVR data and necessary system components.

8.18.2.4 Whether it is necessary or feasible to provide the business with a replacement recording device if their system has been removed.

8.18.2.5 Seize the DVR system if it is an instrument or fruit of the offense.

8.18.3 The recording device should be stopped and the system properly shut down prior to removal.

8.18.4 Ensure all relevant components of the system are collected (for example, power supply, remote control, dongle, manual, cables, and hard drive keys).

8.18.5 Ensure all cables are uniquely identified (for example, camera inputs) to facilitate reinstallation of the system.

8.19 Non-Standard Retrieval Methods

8.19.1 The collection of video/audio signal using non-standard retrieval methods should be a last resort option and conducted if it is the only possible option. For examples, some DVR systems may only have an analog output. For these systems, consider collecting the DVR system as the master evidence. If this is not practical, then the following should be considered:

8.19.2 S-Video/Composite Output

8.19.2.1 Video and audio can only be retrieved in real time and the process should be repeated for each required camera view.

8.19.2.2 When a system has both an S-video and composite output, it is recommended that the S-video output be used.

8.19.2.3 When taking an S-video / composite out into a recording device, it is recommended that the least amount of compression is utilized by the chosen method / device.

8.19.2.4 If audio is also present, it is recommended that uncompressed audio be used by the chosen recording method / device. In the event that uncompressed audio is not an option, the highest quality / bit rate for the available compressed audio format(s) (for example, MP3, WMA, and M4A, etc.,) should be chosen. Audio input levels should be set accordingly, such that the input signal(s) do not overdrive the recorder's circuitry, which would create clipping of the signal and distortion not present in the original recording.

8.19.2.5 Ensure the time/date stamp is displayed on output; this may require checking several signals (for example, composite and S-video).

8.19.2.6 A separate recording without the time/date stamp is recommended, in the event that the position of the time/date stamp obscures desired visual content.

8.19.2.7 It is recommended that the DVR's video output be directly connected to the recording device and a separate output from the recording device be made to a monitor to ensure that the video signal is being received and recorded.

8.19.2.8 If recorded audio is present, the DVR's audio output(s) should be directly connected to the recording device and confirmed as being received and recorded through headphones or loudspeakers.

8.19.2.9 Prior to recording the video data, check and adjust playback speed on the DVR to real time.

8.19.2.10 If multiple audio recordings are present (for example, one for each camera input), select the appropriate audio output on the DVR. Audio outputs should be recorded independently, without mixing two or more channels into a single output, and stereo outputs should not be mixed down to mono.

8.19.2.11 Taking the analog video output from a DVR may produce a different frame size or display aspect ratio, or both, from the original proprietary frame size/display aspect ratio.

8.19.2.12 The recording produced using this process is the master evidence.

8.19.2.13 The recordings produced with and without the date/time stamp are also considered master evidence.

8.20 VGA/DVI/HDMI Output

8.20.1 Some DVR systems have a VGA, DVI (DVI-A/DVI-D) or HDMI output that allows the video data to be displayed on a computer monitor. Devices are available that allow the Digital DVI (DVI-D) and HDMI signals to be directly captured at their resolution, while maintaining the signal's progressive scan format. Alternatively, a scan converter can convert a VGA or DVI signal to a standard video signal, usually analog, which can be recorded to video format and retained as the master evidence.

8.20.2 Either method should be a last resort as the final product may not include all metadata and image/audio quality may be compromised. The latter is especially of concern with scan conversion as it can reduce image quality below that of an S-video/composite output.

8.20.3 Whenever possible, the video should be captured at its native resolution (without scaling).

8.20.4 If recorded audio is present on systems with VGA or DVI outputs, the DVR's audio output(s) should be directly connected to the recording device and confirmed as being received and recorded through headphones or loudspeakers.

9. Verifying and Protecting the Master Evidence

9.1 After retrieval, review the downloaded/exported file(s) on another computer before leaving the scene or at your earliest convenience, to verify that:

9.1.1 The downloaded/exported file(s) play back.

9.1.2 Any associated replay software functions correctly.

9.1.3 The visual characteristics and content of the exported files are consistent with those on the DVR.

9.1.4 The appropriate camera view(s), date(s) and time(s) were retrieved.

9.1.4.1 If multiple files or storage media are retrieved, they should be identified to ensure that the proper order of playback is identifiable.

9.1.5 Once the data is verified, ensure that the DVR has been returned to its original state (for example, any changes to the system settings have been reset), and that the system is operational, preferably in the presence of venue personnel.

9.2 The collected DVR data should be handled as follows.

9.2.1 Initiate a chain of custody for the retrieved data according to Standard Operating Procedures for handling evidence.

9.2.2 Media should be packaged to minimize the likelihood of damage in transit, for example:

9.2.2.1 CDs and DVDs should be kept in individual cases rather than on a spindle.

9.2.2.2 Removable media should be stored in protective packaging.

9.2.2.3 Particular care should be taken to protect hard drives removed from systems when packaged.

9.2.2.4 Keep evidence away from magnets, excessive temperatures and humidity, and otherwise hostile environments.

9.3 Depending upon the data retrieval method chosen, additional steps may be needed to create the master evidence.

9.3.1 Rewritable CD/DVDs, removable storage devices such as external flash cards and "thumb drives," as well as legacy outputs are intermediate storage and should be transferred to a non-rewritable media or secure electronic storage as soon as possible, creating the master evidence.

9.3.2 A forensic wipe should be performed on the intermediate storage media after the master evidence is created.

9.4 Files on non-rewritable media or secure electronic storage will be considered the master evidence.

9.4.1 Master evidence should be handled and packaged according to Standard Operating Procedures.

9.4.2 Working copies may be produced from the master evidence.

10. Keywords

10.1 Data

10.2 Digital Video Recorder (DVR)

10.3 Proprietary File Format

598 10.4 Video

599 10.5 Audio

600

601

APPENDIX

(Non-mandatory Information)

X1. CCTV SYSTEM INFORMATION FORM

CCTV System Information Form

Scene Contact Information:

Scene Address: _____

Hours of Operation: _____

Scene Point of Contact: _____

Email: _____

Phone: _____ Phone: _____

CCTV System Point of Contact: _____

Phone: _____ Phone: _____

Email: _____

Equipment Information:

☐ Digital Video Recorder ☐ Analog Video Recorder

Make/Model: _____

Serial Number: _____

☐ Stand-Alone ☐ Personal Computer ☐ Network Video Recorder ☐ Manual Available

Multiplexor Make/Model: _____

Standard User Name and Password: _____

Administrative/Engineer User Name and Password: _____

Date/Time Display: _____ Actual Date/Time: _____

Date/Time Offset: _____ ☐ Loss Prevention Steps Taken (See Notes)

Other System Information and Settings:

Number of Recording Units: _____ Number of Hard Drives: _____

Storage Capacity: _____

☐ Network Connection (See Notes) IP Address: _____

System Firmware Version: _____ ☐ Applicable Event/Service Log(s) (See Notes)

Total Cameras (See Notes for associated names): _____ Total Active Cameras: _____

☐ Alarm/Motion Triggered (See Notes) ☐ Infrared (See Notes)

Make/Model: _____

Transmission Method: _____ Camera Resolution: _____

Record Mode (Analog) (e.g. 2, 6, 12, 24, 48, 72 hour): _____

Image Quality (Digital): ☐ High ☐ Medium ☐ Low

Image/Frame Size (e.g. 320x240):_____ Frames/Images per Second (FPS / IPS): _____

Total Audio Inputs: _____ Audio Sampling Rate: _____

Location(s) of Microphones: _____

☐ Changes Made to System (See Notes) ☐ Photographs Taken

Export Options (Hardware): _____

File Format Export Options: _____

Playback Software: _____ Version: _____

Playback Software User Name and Password: _____

Media Collected (e.g. tape, CD/DVD, USB Device, etc.): _____

654

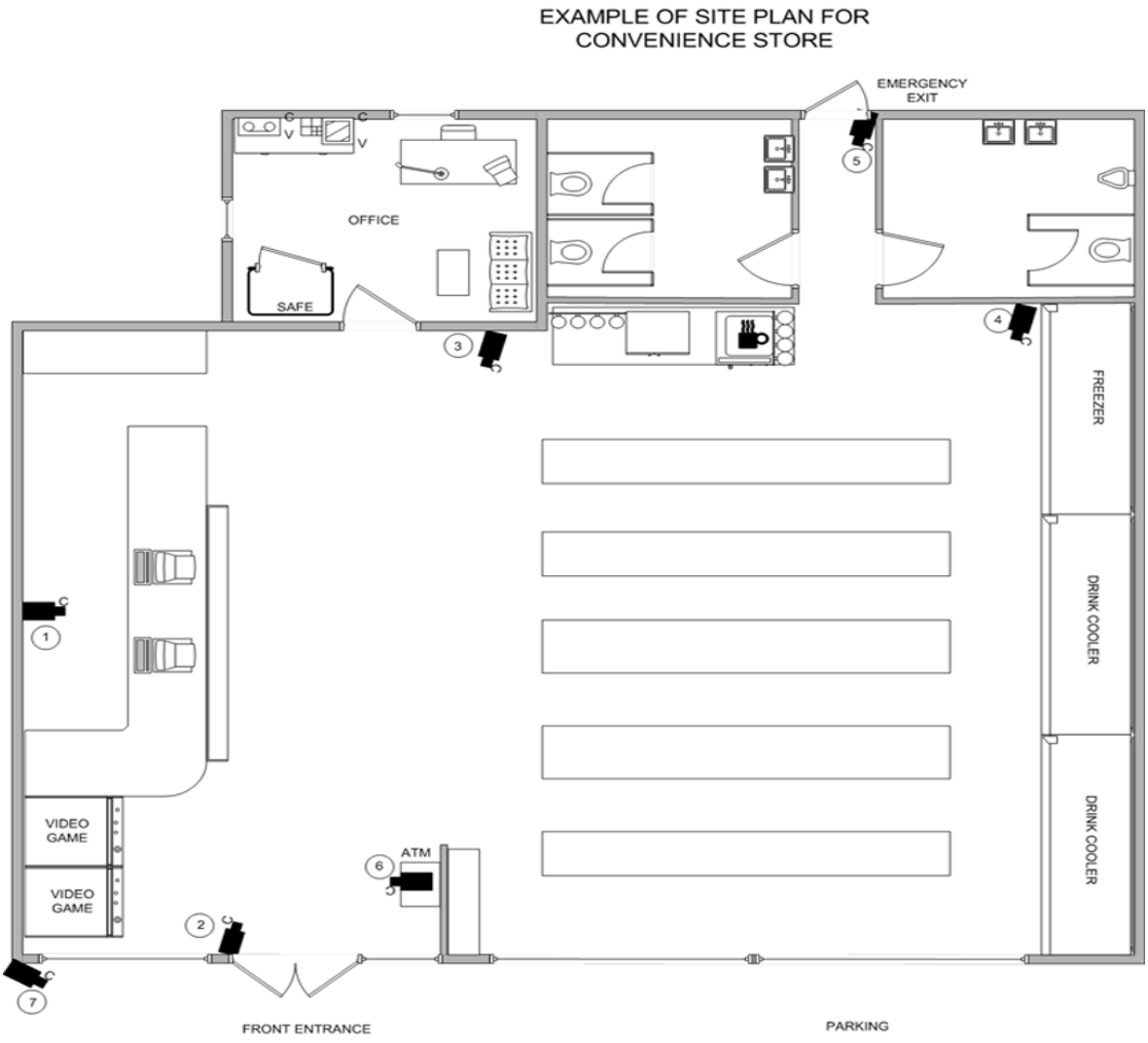
Camera Placement Sketch:

Additional Notes:

APPENDIX

(Non-mandatory Information)

X2. CAMERA PLACEMENT SKETCH



Camera 1: Clerk and check-out area, facing east
Camera 2: Front door entrance, facing north
Camera 3: Outside of office, facing south
Camera 4: Freezer area, facing south
Camera 5: Emergency exit, facing south
Camera 6: Automated teller machine, facing west
Camera 7: Parking lot, facing south-east

APPENDIX

(Non-mandatory Information)

X3. RECOMMENDED EQUIPMENT

The following is a suggested list of equipment that should permit video and audio data retrieval from the most commonly encountered systems:

- Laptop with CD/DVD writable drives, USB ports, network port, eSATA ports, and wireless access. Additionally, the capability for installing proprietary viewers and codecs as well as the ability to change Operating System (OS) settings should be activated. Ensure administrator access is provided, and there are no restrictions that would impede the download (for example, firewalls, and agency software).
- Flash Media Reader (multi-format)
- External CD/DVD Writeable Drive (for example, USB/SCSI/FireWire compatible)
- USB and FireWire Storage Devices in multiple sizes
- IDE, SCSI and SATA Hard Drives in multiple sizes (80, 160, 300 GB for backwards compatibility)
- Four Port Network Switch/Hub
- Internal or USB Floppy Drive
- Write Blockers (USB, IDE, FireWire)
- Blank Media (for example, CD-R, DVD-R, DVD+R, DVD-RAM, CD-RW, DVD-RW, DVD+RW, Blu-ray, flash media, magnetic tapes, etc., in varying sizes)
- Video Monitor (NTSC/PAL)
- Computer Monitor
- Headphones or Loudspeakers
- Device to record video signal
- Scan Converter
- Spherical reference target
- Cables to include, USB, FireWire (iLink, 400, 800), Network (Ethernet Crossover Cable and straight patch cable), S-Video and Composite, as well as RCA to BNC adapters,

Audio (RCA, 3.5 mm Stereo, and 3.5 Mono, attenuator), VGA/DVI-A/DVI-D/DVI-I/HDMI, Power adapters for external devices, and Extension cords / power strips.

- Toolkit containing a still camera with media, flash light, anti-static strap, mirror, assorted screwdrivers, pens, permanent marker (appropriate for marking media), tape (appropriate for marking cables), appropriate forms (for example, chain of custody, notes, and consent forms), evidence packaging (for example, anti-static bags and jewel cases), personal protective gear (for example, gloves and shoe covers).