Disclaimer:

As a condition to the use of this document and the information contained herein, the SWGIT requests notification by e-mail before or contemporaneously 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) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in a formal proceeding, it is requested that SWGIT be notified as to its use and the outcome of the proceeding. Notifications should be sent to: Chair@swgit.org

Redistribution Policy:

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

1. Redistributions of documents, or parts of documents, must retain the SWGIT cover page containing the disclaimer.

2. Neither the name of SWGIT, nor the names of its contributors, may be used to endorse or promote products derived from its documents.

Any reference or quote from a SWGIT document must include the version number (or create date) of the document and mention if the document is in a draft status.

Section 23

Best Practices for the Analysis of Digital Video Recorders

The objective of this document is to provide guidance regarding appropriate practices in the retrieval of video/audio evidence and any associated metadata (referred to in this document as data) from Digital Closed Circuit Television (DCCTV) systems that record to a Digital Video Recorder (DVR). This document specifically addresses DVRs that have been powered down or removed from the scene.

It is strongly recommended to retrieve data at the scene while the DVR is still powered on and operational. For the best practices regarding on-site retrieval methods, see Technical Support Working Group (TSWG) "*Best Practices for the Retrieval of Digital Closed Circuit Television Systems*" [1] and Home Office Scientific Development Branch (now referred to as the Home Office Centre for Applied Science and Technology (CAST)) "*Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems v2.0*" [2].

If determined that data retrieval at the scene is not feasible, practical, or appropriate, the procedures outlined in this document should be followed to maximize the likelihood that the data is preserved and accessible for playback.

DVR analysis may not follow the methodologies from the computer forensics discipline. The key differences between DCCTV retrieval and a computer forensic examination are that the recording device's operational settings may have to be reconfigured to retrieve the video data, the entire system contents may not require a forensic examination, and typically the owner of the DVR is not the subject of the investigation.

This document does not address the examination of hard disk drives (HDDs) submitted without the DVR. In instances where HDDs are submitted without the DVR, every reasonable attempt should be made to obtain the DVR that recorded the data to the HDD. In addition, recovery of data via reverse engineering techniques is not addressed.

This document refers to the internal storage of the DVR as HDD(s), but DVRs may have alternative storage media (e.g. flash media). Some adjustments to the DVR analysis workflow may be required on a case by case basis.

This document is not intended to address Forensic Video Analysis techniques that may be performed after the retrieval of data. For guidance on Forensic Video Analysis, see SWGIT document "*Best Practices for Forensic Video Analysis*". For guidance on Forensic Audio see SWGDE document "*Best Practices for Forensic Audio*".

[1] http://www.tswg.gov/subgroups/isf/electronic-evidence/DCCTV_Web_doc.pdf
[2] http://tna.europarchive.org/20100413151426/http:/scienceandresearch.homeoffice.gov.uk/hosdb/publications/cctv-publications/66-08_Retrieval_of_Video_Ev12835.pdf?view=Binary

BEST PRACTICES

The following are guidelines that describe the SWGIT recommended best practices for DVR analysis.

Evidence Management

Agencies should have documented procedures for the handling, transportation, and storage of evidence. Agencies should have chain of custody procedures in place and should follow these procedures.

At all times precautions should be taken to ensure evidence is protected from external factors that may cause damage to the DVR, media or to the data contained on the media (e.g. magnetic fields, static electrical charges, and electrical hazards).

Quality Control and Quality Assurance

Quality control and quality assurance policies and procedures should be implemented and documented. Technical and administrative peer reviews are integral components of quality control.

Safety

Carry out a risk assessment in order to identify any potential hazards that may arise due to the condition of the DVR, taking account of the following:

Electrical shocks can occur if the device is opened or dismantled.

Electronic devices inappropriately connected may short circuit causing malfunction, loss of data and failure.

Foreign substances may be present on the evidence, it is recommended that protective gloves and eye gear be worn since these substances may carry blood-borne pathogens.

Security

There should be procedures in place to maintain the security of the working data, all notes, and other such analysis related materials to provide the level of security and privacy needed by the organization. For example, archived case related materials should be stored in a manner that limits access. The degree of access will be agency specific.

Infrastructure

Agencies should have sufficient space, equipment and facilities to adequately support the required quality and volume of work.

Work Management

DVR analysis is a labor-intensive process. An upper limit on caseload should be established for every category of tasks.

Documentation

Agencies should establish standards for information included in, and the format for, reporting results.

Training, Competency, and Proficiency

Analysts and/or examiners are encouraged to review SWGIT "*Guidelines and Recommendations for Training in Imaging Technologies in the Criminal Justice System"*, "*SWGIT/SWGDE Guidelines and Recommendations for Training in Digital and Multimedia Evidence*", "*SWGIT/SWGDE Proficiency Test Program Guidelines*", Technical Support Working Group (TSWG) "*Best Practices for the Retrieval of Digital Closed Circuit Television Systems*" [3] and Home Office Scientific Development Branch (now referred to as the Home Office Centre for Applied Science and Technology (CAST)) "*Retrieval of Video Evidence and Production of Working Copies from Digital CCTV Systems v2.0*" [4].

Analysts should have certification in their knowledge domain and associated forensic discipline, when such certification is appropriate and available. Note, however, that the existence of an external professional certification program does not imply that it is necessary, sufficient, or appropriate.

Analysts should demonstrate competency in their discipline prior to being assigned unsupervised case work responsibilities. Analysts should remain proficient through continuing education, training, and peer review of examinations. Agencies should document competency, proficiency and continuing education for each analyst.

The analyst should demonstrate:

- an understanding of the scope of work and how it will be applied in the forensic environment;
- subject matter knowledge and competence;
- working knowledge of DVR recording technology, retrieval methods and evaluation techniques;
- working knowledge of applications and tools utilized in the specific agency;
- working knowledge of SWGIT guidelines for capturing, storing, and processing image/video and audio, including issues relating to topics such as data integrity and compression artifacts;
- understanding of relevant legal precedents;
- knowledge of appropriate case work documentation.

Standard Operation Procedures (SOPs)

There should be Standard Operating Procedures (SOPs) in place for the analysis being performed. These SOPs should be agency specific, reflect the workflow and be general enough to permit flexibility for the required tasks.

[3] *Ibid.*
[4] *Ibid.*

Evidence Marking
Evidence needs to be marked per agency policy. Markings could include labelling with initials, ID number, case number or any other identifying information.

Any identifying information (such as serial numbers) should be documented.
Inappropriate marking or labelling methods may affect playback and could potentially damage the evidence.

Avoid use of markers that contain solvents.

Avoid use of adhesive labels other than on outside solid surfaces.

Chain of Custody
Throughout the entire DVR analysis process, chain of custody must be maintained per agency policy.

Submission Review
A submission form should be completed for every case the examiner receives, regardless of what type of examination or service the requestor is seeking. ***See Appendix A for an example***.

Ensure examiner safety is maintained by determining and documenting whether biohazards such as blood or body fluids are present or other special handling is required.

Determine if other examinations (such as latent print or trace evidence) are required and identify appropriate measures to ensure evidence integrity.

DVR ANALYSIS WORKFLOW

Note: The following workflow should only be performed by trained individuals who are competent and proficient in its proper use and application.

1. Document the physical condition of the evidence (which may include photographs). Physical inspection may include the following:
    - Physical damage
    - Contaminants (e.g. direct, grease)
    - DVR characteristics (e.g. make, model, number of cameras, serial number)
    - DVR output options (e.g. optical drive, USB, network)
    - Existing labels or identifiers
    - When possible, determine if removable media is present in the DVR (e.g. flash media or CD/DVD in the drive).

    Note: If optical media is located, it is appropriate to remove the media, perform a physical inspection and label appropriately. If flash media is located, do not remove the media until research is conducted to determine its contents (e.g. video data, system data).

2. Verify all necessary components, documentation and software are enclosed with the evidence. Examples of these include peripherals, keys, user manuals, passwords, etc.

Multiple levels of access and required passwords may exist, and not all may allow access to export the proprietary data.

Any deficiency should be documented and resolved, if possible, before beginning any forensic analysis (e.g. obtaining required peripheral device or replacement of a damaged power supply). If necessary, contact the submitter and/or other sources to obtain the needed item or information.

3. Prior to continuing analysis, read the user manual and literature. Refer to any additional resources as appropriate. Pay particular attention to potential issues addressed in the manual that may provide additional guidance regarding the course of analysis (e.g. the removal of the HDD may cause the data not to play back in the DVR or a specific brand of HDDs may be required by the DVR).
4. Photograph the DVR and media (such as internal HDDs) in order to document location, connections and physical condition.
5. Mark internal cables and HDDs for identification and proper placement/orientation.
6. Remove the HDD(s) from the DVR using appropriate tools including anti-static protection, as needed.
7. For each HDD, document the make, model, interface, capacity, serial number and jumper settings.
8. Conduct physical inspection of the HDD(s) and label as appropriate.
9. Produce a forensic clone of the HDD(s).
    - It is strongly recommended that forensic clones are produced as opposed to forensic image files.
    - The same make, model and size HDD(s) should be used for the forensic clone(s) when possible.
10. Retain the original HDD(s) as evidence and continue analysis using the forensic clone(s).
11. Properly label the forensic clone(s).
12. Confirm the jumper settings, if present, of the forensic clone(s) are in the same configuration as the original HDD(s).
13. Install the forensic clone(s) in the DVR.
14. Confirm the DVR and external power supply voltage settings are correct.
15. Boot the DVR. Confirm the forensic clone(s) are recognized by the DVR and the data is playable.

    Note: The boot process and/or the HDD menu of the DVR may indicate whether the forensic clone(s) are recognized.

    - If the DVR does not power on or boot successfully, check the following:
        - External power to the DVR is connected properly and the DVR and the forensic clone(s) are receiving power.

- All power switches have been turned on. Some DVRs have multiple power switches.
- Consider using an alternative available power connection, from the motherboard or external source, to the forensic clone; it may have different power requirements than the original.
- Internal cables are secure, operating properly and connected in the correct order (e.g., IDE master/slave configuration). This is predominantly an issue with PC based DVRs which store system files on internal HDD(s).
- DVRs can contain CMOS batteries that if depleted may prevent booting (this can also cause all settings to be lost). Check and replace, if necessary, keeping in mind that important settings can be permanently lost.

- If the DVR boots successfully, but the forensic clone(s) are not recognized, check the following:
  - Make, model and size of the forensic clone(s) are the same as the original HDD(s).
  - Forensic clone(s) are properly installed and connected to the DVR.
  - Cables are secure, operating properly and connected in the correct order (e.g., IDE master/slave configuration).
  - Jumpers are in the correct position, which may differ between the forensic clone(s) and the original HDDs due to brand variances, and may need to be changed to “master” if hard disk write blockers are being used in the chain.
  - Consider using an alternative available power connection, from the motherboard or external source, to the forensic clone; it may have different power requirements than the original.
  - Forensic clone(s) are receiving power and operating properly (e.g. spinning).
- If the forensic clone(s) are recognized by the DVR, but the data is not playable, check the issues addressed above. In addition, the following steps should be considered:
  - Check the DVR for an indication of the amount of recorded footage and/or available storage for recording.
  - Use a hexadecimal editor (e.g. WinHex) to confirm the HDD is not blank.
  - Determine the last time the recorded video was viewed, how the DVR was collected, and whether the DVR has been accessed since collection.
  - Review system documentation and/or contact the manufacturer for guidance.

Note: These issues may reflect the index of the DVR (which associates metadata with recorded footage) has been changed, corrupted, or deleted. The manufacturer may be able to assist with technical knowledge of processes to enable playback. If the index has been deleted, search functions are unlikely to work. Try pressing the play button to attempt to access recent recordings and then rewind to see if video of interest is present.

- If successful results are still not obtained, the DVR may be faulty. Non-evidentiary media (e.g. HDD) should be used to produce test recordings and to verify test recordings play back as expected. If, after testing, the DVR has been determined to be faulty, contact the manufacturer to determine the appropriate course of action. Solutions may include replacement of parts according to manufacturer specifications, or replacement of the DVR with a properly functioning unit.
- If the DVR has been determined, through testing, to be operating properly, the following procedures may be required to retrieve the data. Prior to performing these procedures, the investigator should be informed of the technical challenges and advised of the risks in proceeding.
    - Use of write protection hardware in conjunction with the DVR and original HDD(s) for analysis.
    - Use of the original HDD(s) and DVR without write protection for analysis. Prior to using the original, ensure your forensic clone has not been altered by validating the hash value. If necessary, produce a new forensic clone.

Note: If followed, the DVR analysis workflow described within this document produces successful results in a vast majority of cases. If this process is not successful, consider consulting an individual trained in the interpretation and extraction of data.

16. Conduct an examination of the DVR (logged in as administrator or technical equivalent) in its powered on state.

    Note: Changing the original settings may be necessary to conduct this examination. If settings are changed, document the original configuration and what changes were made.

    Determine the following:

    - System date and time as reported by the DVR and current date and time to establish an approximate offset.

    Note: It is recommended that any previous time and date checks that may have been carried out on the DVR prior to submittal be documented to check for potential anomalies. For example, the clocks on some DVRs do not increment when in a powered off state, or the clock may have reset to a default time after being powered down during seizure.

    - System manufacturer, firmware version, proprietary software name and version.

- Additional user names and passwords.

- Number of cameras capable of being recorded, how many were connected and how many were recording during period of interest.

- Current settings of the DVR to include: motion recording, event recording, frame rate, frame size, compression setting.

- Native and open file format .

17. Conduct an assessment of the DVR to determine the following information:
    - The data for the pertinent date and time was recorded and is present on the DVR.
        - If the data does not appear to be present, verify through all search options listed in the manual that data cannot be located by another search mechanism.
    - Earliest recorded date and time located as well as last date and time recorded.
    - Non-contiguous timeframes (such as missing days) should be identified and documented when appropriate.
    - Pertinent segment(s) of interest and the amount of data to be recovered from the DVR.
    - DVR data recovery options and which one may provide the native file format or otherwise best evidence.

18. By referencing the information gathered during the physical inspection, research and system examination, a protocol should be formulated for the best retrieval method for the recorded data. The specific steps and the order in which they are performed may vary. The procedure may include the following:
    - Internal archival device (e.g. CD/DVD writer, flash media drive).
    - Data transmission connection (e.g. USB, Firewire).
    - Network connection (e.g. Ethernet).
    - Video signal connection (e.g. S-Video, composite).

19. If data collection is determined to be the best method of retrieval, and the amount of data to be collected has been determined, conduct a test download to calculate the amount of media and physical time necessary for the retrieval.

20. Download the native or proprietary data to non-rewritable media. It is recommended to also retrieve an open file format.

21. If the data is downloaded to rewritable media, transfer the data to a non-rewritable media or secure electronic storage as soon as practical.

- Downloaded data not stored on non-rewritable media requires equivalent levels of protection, such as access control and tamper-proof logs.

22. Large amounts of data may be retrieved and placed on one or more hard drives. If the data is not otherwise stored as prescribed above, these hard drives then become evidence.

23. Calculate, verify and document hash values, when applicable.

24. Make sure all required proprietary software and/or codecs are included.
    Verify the native and/or open file format data is accessible on a separate computer.

25. It is recommended to also collect a digital or analog magnetic recording of the data (e.g. Mini-DV)

26. Document data retrieved from the DVR:
    - Date and time ranges for each camera
    - File format(s)
    - Magnetic recording(s)

27. If settings on the DVR were changed during examination, return them to the previous settings, if applicable.

28. If applicable, provide a copy of the proprietary software with playback instructions.

29. Confirm that the DVR operates as expected prior to return.

30. When the system is sent back to the submitter, return the DVR with the forensic clone(s) installed and the original HDDs packaged separately. This is the preferred method, but agency policy regarding the return of evidence should be taken into consideration.

TECHNICAL CONSIDERATIONS

The procedures described within this document are recommended best practices. However, due to the proprietary and often limited functionality of some DVRs, technical consideration should be taken to prevent mechanisms which may result in lost or inaccessible data. These considerations include the following:

- Improper removal of the DVR from the scene or hard drives from the DVR may result in loss of data and/or difficulty in playback of the data
- Disconnecting the HDD from the main board of the DVR may cause the HDD to be permanently disassociated from this device, rendering the data inaccessible by that device.
- Clone copy HDDs may be unrecognizable by the DVR.
- Connecting a HDD write blocker in line with the HDD may result in the HDD being unrecognizable by the DVR.
- Some DVRs are equipped with timed expiry which can result in the data becoming inaccessible by the device.

- Some DVRs go into auto-record mode when switched on, even if no video source is connected. For non PC-based DVRs, consider booting without the HDDs connected, allowing password to be determined without risk of data being overwritten. Once the password has been established it should be possible to disable the recording if auto record mode is engaged. This may involve turning off all or a combination of the following settings: manual, circular, scheduled, event and motion recording. Any changes made to settings should be noted.

Appendix A – Sample Video Submission Form

SUBMISSION OF VIDEO EVIDENCE

Date		Agency Case #		
Submitter Name & Title				
Agency				
Offense		Phone #	Cell #	
Offense Date		Email		
VICTIM (or SUBJECT)		**RACE**	**SEX**	**DOB**
1				
2				
SUSPECT		**RACE**	**SEX**	**DOB**
1				
2				

Brief Details of Case (Attach Report if Necessary)

_____
_____
_____
_____

Examinations Requested

_____
_____
_____
_____

Item(s) Submitted (including seals & packaging)

_____
_____
_____
_____

CCTV System Information

Digital Video Recorder Make, Model, Serial Number _____

Computer Based Stand Alone Networked (Circle One)

Playback software name and version_____

Software provided with evidence YES or NO (Circle One)

System and/or Software Password _____

Included Peripherals/Manuals _____

Retention Time (if known)

_____

System Settings:

Image Quality (i.e. high, medium, low) _____

Frames per second (fps)/pictures per second(pps) _____

Image/Frame recorded size (e.g. 320 x 240) _____

Can it be determined if any cameras are alarm or motion triggered? _____

Number of hard drives, storage capacity of each _____

System firmware version _____

Other available system settings (e.g. event log)_____

Hybrid or Other Equipment Make, Model, Serial Number_____

VHS SVHS Other _____ (Circle One)

What record mode was the system? (Circle One) 2 hour, 6 hour, 12 hour, 24 hour, 48 hour,72 hour, Other _____ Unknown

Multiplexer YES or NO Make and Model _____

Basic Information

Does the recorded date/time accurately represent the time of day? (circle) YES or NO

Date/Time displayed _____

Actual date/time _____

# of Camera/s _____ Active # of cameras _____

Camera make and model _____

Are any cameras infrared-sensitive and if so identify _____

Is audio being recorded? _____# of microphone/s _____

Is a copy of the most current maintenance/service log attached? (circle) YES or NO

Other Information: _____
_____

Scene Contact Information

Scene Address _____

Hours of operation_____

Scene point of contact _____Telephone: _____

CCTV system point of contact _____ Telephone: _____

Location of Equipment at Scene _____

Please provide a sketch of the scene indicating camera/microphone position and placement.

Submitted By _____ **Print Name**_____
Signature