Technical Procedure for DVR Analysis

1.0 Purpose - The purpose of this procedure is to establish a methodology for processing video evidence from a Digital Video Recorder (DVR) device.

2.0 Scope - This procedure describes the steps to be taken by personnel of the State Crime Laboratory in performing an analysis of a Digital Video Recorder (DVR) device.

3.0 Definitions

- **Write Blocker** – A technology in computer forensics equipment that helps to protect the media from inadvertent alteration or deletion.

4.0 Equipment, Materials and Reagents

- Screwdrivers
- Permanent marker
- Forensic Computer or hard drive cloning device
- Target hard drive
- Crossover Ethernet cable
- DVR manufacturer's owner's manual and/or software (if provided or downloadable)

5.0 Procedure

5.1 Remove the hard drive from the DVR unit.

5.2 Connect the hard drive to the forensic computer by means of a write-block device (e.g., internal write block bay, external write block device, etc.).

5.3 Attempt to discern the file storage system for the device.

5.4 **<u>If the hard drive has an easily discernible file system:</u>**

5.4.1 Export the video files from the date and time of interest as determined by the submitting agency.

5.4.2 Proceed with processing the video data in accordance with Digital/Latent Evidence Section Evidence Search Protocol.

5.4.3 Return the original drive to the DVR system upon completion of analysis.

5.5 **<u>If the hard drive does not have an easily discernible file system:</u>**

5.5.1 If possible, a clone of the DVR hard drive shall be made and used in place of the original hard drive. The original hard drive shall be returned to the DVR prior to returning the DVR to the submitting agency.

5.5.2 If a clone is not possible, return the original drive to the DVR system.

5.5.3 Ensure that the DVR is not set to record video by disabling the data overwrite setting in the DVR.

5.5.4 Search for additional means by which to extract the data from the DVR.

5.5.4.1 If the system has an Ethernet connector, make an Ethernet connection between the forensic computer and the DVR device by means of the manufacturer's supplied control software and a crossover Ethernet cable.

5.5.4.2 If the system has a USB connector and a video output, connect a monitor to the DVR and use the manufacturer's means for exporting the data onto the USB device.

5.5.4.3 If there are no output connectors on the device apart from the video monitor connector, attach a monitor to the system and use a camcorder to capture the video data from the attached monitor.

5.6 The manufacturer's website may need to be consulted in order to download appropriate control software and/or owner's manuals for the DVR device.

5.7 **Standards and Controls -** A control disk image with a known hash value is used to ensure the proper functioning of forensic computers used in casework.

5.8 **Calibrations -** The forensic towers used in casework shall be verified each day that they are used to ensure that the computer hardware and software are functioning properly (see the Computer Performance Verification Procedure).

5.9 **Maintenance –** N/A

5.10 **Sampling -** N/A

5.11 **Calculations -** N/A

5.12 **Uncertainty of Measurement -** N/A

6.0 Limitations

6.1 DVR storage of video and subsequent metadata is often proprietary in format making the data virtually inaccessible.

6.2 For some DVRs it is impossible to determine the manufacturer of the device; therefore, the Forensic Scientist will be unable to extract anything from the device without the owner's manual.

7.0 Safety – N/A

8.0 References

- Computer Performance Verification Procedure

9.0 Records - N/A

10.0 Attachments - N/A

Revision History		
Effective Date	Version Number	Reason
09/17/2012	1	Original Document
10/31/2013	2	Added issuing authority to header
01/24/2014	3	Added 5.5.1, 5.5.3; edited 5.5.2