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. The steps of examination may be omitted or worked in different sequential order based on the device and the scientist's training and experience.

3.0 Definitions

- **Write Blocker** – A technology in computer forensics that protects media from inadvertent alteration or deletion.

4.0 Equipment, Materials and Reagents

- Screwdrivers
- Permanent marker
- Forensic Duplicator
- Video Analysis Equipment
- Target hard drive
- DVR manufacturer's owner's manual and/or software (if provided or downloadable)
- External hard drive dock
- Write-Blocker
- DVR Examiner

5.0 Procedure

5.1 Remove the hard drive from the DVR unit.

5.2 Using a write blocker, preview the DVR's hard drive to determine if DVR Examiner supports the DVR's file system.

5.3 Connect the hard drive to the forensic duplicator.

5.4 Clone or create a DD forensic image.

5.5 Verify the DVR date and time, and calculate the time difference between DVR time and actual time.

5.5.1 Using DVR Examiner Software

5.5.1.1 Place and connect the hard disk drive containing the clone/forensic image into an external hard drive dock.

5.5.1.2 Connect the external hard drive dock to the video analysis equipment.

5.5.1.3 Using the DVR Examiner software, select and detect the appropriate hard disk drive.

5.5.1.3.1 If it is suspected that video footage has been deleted, ensure the "Scan for inaccessible data" box is checked.

5.5.1.4 Select the requested cameras, clips, and timestamps to be exported.

5.5.1.4.1 When exporting the video clips, export and save the generated DVR Examiner report.

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

5.6.1 A clone of the original DVR hard shall be installed in the DVR. Any video that is to be exported, shall be exported from the clone hard drive.

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

5.6.3 Ensure that the DVR is not set to record video by disabling the data overwrite in the DVR settings menu.

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

5.6.4.1 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.

5.6.4.2 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.

5.7 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.

5.8 **Standards and Controls -** All forensic computers and forensic tools shall be functioning properly prior to beginning a computer forensic examination (see Technical Procedure for Computer Forensics Performance Verification).

5.9 **Calibrations -** N/A

5.10 **Maintenance –** N/A

5.11 **Sampling -** N/A

5.12 **Calculations -** N/A

5.13 **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 video from the device without the owner's manual.

7.0 Safety – N/A

8.0 References

- Technical Procedure for Computer Forensics Performance Verification

9.0 Records - N/A

10.0 Attachments - N/A

Revision History		
Effective Date	Version Number	Reason
12/02/2020	6	Deleted 5.4 and 5.5. removed Crossover Ethernet cable, added Forensic Duplicator changed for clarity: 5.6.2