Form	Deviation Request Form
Title	DRF Technical Procedure for DVR Analysis - updated
Laboratory Location	Raleigh Lab
Discipline/Section	Digital Evidence
A. Requested deviation applies to:	Technical Procedure for DVR Analysis
B. Requested deviation:	Add-5.1.1—If the DVR has more than one hard drive, a sub-item entry for each hard drive will be created within Forensic Advantage. Replace all instances of DVR Examiner with Magnet Witness.
C. Necessity for the deviation:	Update the procedure if more than one hard drive is found in a DVR. DVR Examiner has been discontinued by the vendor and replaced with Magnet Witness for DVR examinations.
D: Technical Review and Authorization	
Technical Authorization	Yes - Authorized
Technical Authorizer	☐ Trevillian, Jim
Duration	1 year / next procedure revision
E: Quality Assurance Authorization	
Acceptable within general QA guidelines and good laboratory practice?	Yes
Significant negative impact to Crime Laboratory Quality System?	No
QA Authorization	Yes - Authorized
QA Authorizer	☐ Suggs, Timothy
Effective Date:	2/7/2025

Version: 3.0
Created at 2/3/2025 7:14 AM by ☐ Hunt, Sterling
Last modified at 2/3/2025 12:42 PM by ☐ Suggs, Timothy

Close

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 - See Digital Evidence Dictionary

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 Prior to evidence media examination, the write-blocker shall be tested using the WiebeTech WriteBlocking Validation Utility and a control media with known hash value shall be examined.

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

5.4 Connect the hard drive to the Tableau Forensic Bridge.

5.5 Clone or create a DD forensic image.

5.6 Verify the DVR date and time and calculate the time difference between DVR time and actual time.

5.6.1 Using DVR Examiner Software

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

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

5.6.1.2.1 Ensure the "Scan for inaccessible data" box is checked, click on the video property box and select save.

5.6.1.2.2 Document the highlighted supported features on the DVR worksheet.

5.6.1.3 Export the DVR Examiner Clip List.

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

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

5.7 If DVR Examiner does not support the file system:

5.7.1 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.

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

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

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

5.7.4.1 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.

5.7.4.2 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.

5.8 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.

5.9 Results of Examination – Results shall include the total number of videos exported and the resulting reports that were generated. The following is an example for report wording. The example may be modified based on the case circumstances.

5.9.1 (Item number) contained a DVR, which was hashed and imaged using Forensic Toolkit Imager. The DVR was examined, and the requested videos were exported to a (media used) using DVR Examiner. Resulting in a total of (number) video files being returned in Container (number). A DVR Examiner Clip List Report and a DVR Examiner Export List Report are being returned in Container (number).

5.10 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).

5.11 Calibrations - N/A

5.12 Maintenance – N/A

5.13 Sampling - N/A

5.14 Calculations - N/A

5.15 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
08/02/2024	7	3.0 - added reference and removed definition 5.2 – added 5.4, 5.6.1 and subsections – updated 5.7 – added DVR Examiner 5.9 - added