# TABLE OF CONTENTS

Table of Contents ....................................................................................................................1
Revision History ..........................................................................................................................3
01 Quality Assurance ................................................................................................................4
 DM-01-01 Analytical Software and Equipment ............................................................4
 DM-01-02 Evidence and Supporting Documentation ..................................................7
 DM-01-03 Case Reviews .............................................................................................8
 DM-01-04 Report Writing Guidelines ...........................................................................9
 DM-01-05 Standard Abbreviations List ......................................................................11
 DM-01-06 Technical Procedure for DM Server Data Storage ...................................19
02 Examination and Recovery Techniques .........................................................................22
 DM-02-01 Physical Evidence Examination ................................................................22
03 Digital Media Analysis ....................................................................................................25
 DM-03-01 Acquisition of Digital Evidence ................................................................25
 DM-03-02 Archiving or Restoring Digital Evidence....................................................28
 DM-03-03 Examination of Digital Evidence ................................................................30
04 Audio/Video/Image Analysis ..........................................................................................32
 DM-04-01 Forensic Video Analysis ...........................................................................32
 DM-04-02 Forensic Audio Analysis ...........................................................................36
 DM-04-03 Forensic Image Analysis ...........................................................................40
05 Internal Department Photographic Support....................................................................43
 DM-05-01 Photographic Overlays .............................................................................43
 DM-05-02 Digital Displays for Court ..........................................................................45
 DM-05-03 Suspect Lineup Eliminations or Enhancements .......................................47
06 Forms .............................................................................................................................48
 Directory of Forms .............................................................................................................48
 Digital Evidence Analysis Inventory ............................................................................48
 Digital Media Inventory .................................................................................................48
 Bios and Written Files ..................................................................................................48
 Chronology of Examination ..........................................................................................48
 Keyword Search ..................................................................................................................48
 Enscripts and Software ....................................................................................................48
 Analog Video Worksheet .................................................................................................48
 Digital Video Worksheet .................................................................................................48

Effective Date: 10/28/2019
Go to Table of Contents
Issued by: System Quality Manager
Printed copy is uncontrolled. Refer to electronic copy for current version.
Audio Worksheet..........................................................................................................48
Mobile Device Worksheet ..........................................................................................48
CF/MF Technical Review Worksheet...........................................................................48
DM-AV Technical Review Worksheet .........................................................................48
Image Worksheet .......................................................................................................48
# REVISION HISTORY

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>Brief Description of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/28/2019</td>
<td>Original Issue</td>
</tr>
<tr>
<td></td>
<td>Previous revision history for individual chapters included in archived documents</td>
</tr>
</tbody>
</table>

Printed copy is uncontrolled. Refer to electronic copy for current version.
01 QUALITY ASSURANCE

DM-01-01 ANALYTICAL SOFTWARE AND EQUIPMENT

1 General Requirements for Analytical Equipment

A. Significant equipment will be validated prior to implementation. Typically, equipment used in Digital/Multimedia analysis provides instructional prompts during use therefore do not require formal instructions unless otherwise indicated in policy. When available, up-to-date externally prepared instruction manuals may be retained for general reference but are not adopted by the laboratory as policy.

B. The Equipment Log (LAB-405), which may be stored digitally, will contain maintenance records for significant equipment.

C. Significant equipment will be maintained and verified in accordance with the prescribed Standard Operating Procedures.

D. The performance check of acquisition equipment will be conducted prior to the acquisition of evidence each day, each case, and each workstation. The process and results will be recorded and retained in the case record. The performance check is conducted by acquiring a piece of media with a known hash value and ensuring the acquired image hash value matches.

E. The performance of significant equipment will be verified after it goes off-site (or out of the DM section) for repair, maintenance, or modification prior to being used again in casework.

F. If significant equipment fails the performance verification or a performance problem is detected and cannot be fixed after general troubleshooting and appropriate corrections, the immediate supervisor must be notified, the equipment must be removed from service, labeled accordingly, and an Equipment Out of Service Incident Form is completed (LAB-410). The completed form is returned to the Quality Assurance Specialist or Quality Manager to initiate the QI process.

G. Repair equipment and conduct a performance verification to ensure equipment is working properly before the returning to service. The Section Supervisor, Technical Leader, and/or Technical Point of Contact may authorize its use on the Equipment Log (LAB-405) and submit a Validation and Verification Form (LAB-408) to the Quality Assurance Specialist or Quality Manager.

2 Significant Equipment

A. When available for use in casework in the laboratory, the following are considered significant equipment and will undergo any necessary maintenance and performance check(s) at least annually:

1. Radio Frequency (RF) Room
2. Ramsey Isolation Boxes (RIB)
3. Hardware wipers
4. Forensic duplicators/physical imagers
5. Hardware write-blockers
6. DM server(s)
7. Forensic Workstation(s) 
8. Audio cassette recorder/player(s) 
9. Micro cassette recorder/player(s) 
10. Audio interface(s) 
11. DVD Recorder(s)/VHS Player(s) 
12. Analog Video Camera(s) 

B. Performance Check Criteria 
1. Radio Frequency (RF) Room – the performance check is successful when the absence of signals to the test mobile device is verified. 
2. Ramsey Isolation Boxes (RIB) – the performance check is successful when the absence of modifications and/or signals to the test mobile device is verified. 
3. Hardware wipers – the performance check is successful when the output of the test media reflects the same content when compared to that of another validated forensic tool. 
4. Forensic duplicators/physical imagers – the performance check is successful when the content and/or hash values match that of the original media. 
5. Hardware write-blockers – the performance check is successful when the absence of modifications to the test media is verified. 
6. DM server(s) – the performance check is successful when there are no critical events or alerts on the Modular Disk Storage Manager Client. 
7. Forensic Workstation(s) – the performance check is successful when the Power-On-Self-Test (POST) completes without error on the forensic workstation. 
8. Audio cassette recorder/player(s) – the performance check is successful when the output of known content is verified. 
9. Micro cassette recorder/player(s) – the performance check is successful when the output of known content is verified. 
10. Audio interface(s) - the performance check is successful when the output of known content is verified. 
11. DVD Recorder(s)/VHS Player(s) - the performance check is successful when the output of known content is verified. 
12. Analog Video Camera(s) - the performance check is successful when the output of known content is verified.

3 General Requirements for Analytical Software 
A. All forensic analysis software will have a user manual or user instructions, in hard copy or digitally accessible, that highlights the function(s) of that version of software. 
B. DM software is categorized into two groups: 
1. The version number indicates whether a software update is major or minor (ex: 7.1 to 7.2 is minor and 7.1 to 8.0 is major); 
2. The version number does not indicate whether the update is major or minor.
C. The majority of DM software falls under the first category and will undergo validation after every major update. Minor updates will not undergo performance verification as the software manufacturer's validation testing is relied upon for non-critical updates. DM software that falls under the second category will be updated only as needed when evidence is not supported by the older version. Whenever updated, the software will undergo validation before use in casework.

D. Forensic analysis software performance will be verified after being moved from the DM section. Wiping software will undergo performance check annually.

E. The performance check of wiping software is successful when another validated forensic software is used to verify that the test media content is wiped.

F. If a performance problem is detected with forensic analysis software, or it fails the performance check, verification, or validation, it will not be used for analysis until it is demonstrated to be functioning properly.

G. Repair the software and perform routine quality control procedures to ensure it is working properly before the software is returned to service.

H. Software updates will be delivered in the following manner:
   1. Directly from manufacturer’s CD/DVD/USB to analysis machines, or
   2. Downloaded from the internet, manually scanned for malware and copied to removable media such as a USB device. Software will then be uploaded to the forensic analysis machine and registration of the product (if needed) will be completed.

4 Security of Analysis Software and Forensic Workstations

4.1 Computer and Mobile Forensic Analysis

Computers used in digital media analysis are stand-alone units not connected to the internet or unsecured network during analysis or when evidence is connected or loaded onto the workstation. Computers used in computer/mobile forensic analysis use proprietary software accessible only through the use of a license or registered dongle which connects to a computer to authenticate the software. Workstations are located in a secure examination area.

4.2 Image Enhancement

Computers used in image enhancement use proprietary software accessible only through the use of a license or registered dongle which connects to a computer to authenticate the software. Workstations are located in a secure examination area.

4.3 Audio/Video Analysis

Computers used in audio/video analysis are stand-alone units not connected to the internet or unsecured network during analysis or when evidence is connected or loaded onto the workstation. Computers used in audio/video analysis use proprietary software accessible only through the use of a license or registered dongle which connects to a computer to authenticate the software. Workstations are located in a secure examination area.
DM-01-02 EVIDENCE AND SUPPORTING DOCUMENTATION

1 Digital Evidence Archives
   A. These are considered to be evidence.
   B. They will be properly marked and sealed when physically stored in the laboratory. Digital evidence archives may also be stored digitally on the secured network server. The retention of digital evidence archives will be documented in the case file and they will be stored in accordance with the Crime Laboratory Service Manual.

2 Digital Report Data
   A. A digital report is not a test report, but are considered to be evidence.
   B. They will be properly marked and sealed when physically stored in the laboratory. Digital report data may also be stored digitally on the secured network server. This data may contain information relevant to an investigation and will be returned to the agency in the form of a digital report.
   C. They will be documented in the case file and stored in accordance with the Crime Laboratory Service Manual.

3 Digital Case File Archive
   A. These data are considered to be work product / electronic case documentation or project files related to the specific forensic software tool used during analysis.
   B. They will be properly marked and retained with the Digital Evidence Archive(s).

4 Restored Digital Image
   A. Prepared on request, these images are considered to be evidence.
   B. They will be properly marked, sealed and transferred when used.
   C. They will be documented in the case file and stored in accordance with Crime Laboratory Service Manual.
DM-01-03 CASE REVIEWS

1 Technical Review

A. Laboratory reports and conclusions must be technically reviewed prior to release. In order to ensure quality, accuracy, and conformance to approved methods and applicable laboratory policies and procedures, it is necessary to conduct thorough technical reviews of case documentation. Technical reviews should consist of the following, at a minimum:

1. Ensure proper technical procedures were followed during testing
2. Ensure data transfers are accurate (example: verify hash values)
3. Verify that sufficient documentation is contained within the case record, including evidence inventory, chain-of-custody, disposition of evidence (as appropriate)
4. Ensure conformance with approved methods and applicable management system documents
5. Ensure that items within the DM specific technical review worksheet (LAB-DM-11 for CF/MF or LAB-DM-12 for A/V) are included in the technical review
6. Ensure test reports contain all required information and are accurate
7. Ensure the technical records support the results, interpretations, opinions, and conclusions in the test report
8. Ensure qualified statements are included where relevant

B. The reviewer(s) must be competent and authorized in the DM sub-discipline to verify compliance with the laboratory’s technical procedures and to ensure that the conclusions are supported by the examination documentation.

C. If an examiner from another laboratory external to DPS is involved in conducting the technical review, the Quality Manager and/or the Section Supervisor will review the technical reviewer’s credentials and ensure that all requirements defined in the Crime Laboratory Service Manual (Review of Laboratory Records) are met before approving their participation in the case review process.

D. Preliminary results may be released to submitting agencies per their request in order to aid in investigation as long as they have been technically reviewed and documented in the case record. A technical review worksheet (LAB-DM-11 for CF/MF or LAB-DM-12 for A/V) is not required when technically reviewing preliminary results as long as the technical review is otherwise documented in the case record.

2 Evidence Re-examination

A. If evidence re-examination is performed, it is conducted by a qualified examiner other than the original analyst.

B. The re-examination results will be documented and maintained in the case record.
DM-01-04 REPORT WRITING GUIDELINES

1 Scope
The specific requirements and recommended statements for reporting examinations performed in Digital/Multimedia are included in this document.

2 Practices
2.1 General

Electronic Elements
A. If notable data are recovered from the evidence submitted, or if enhancements or digital conversions are performed, the data will be duplicated onto appropriate media as a digital report and will be added as evidence into LIMS.

B. In some cases the digital report may contain contraband. In these cases, the digital report will be labeled as containing possible contraband and shall be returned in person.

2.2 Computer and Mobile Reporting Statements
Examples of computer and mobile forensic statements, depending on examination and conclusions:

A. Archived copies of the submitted evidence will be retained by this laboratory; if further analysis is requested, it can be conducted on these archives. If you have any questions or wish to request further analysis, please contact me.

B. A detailed report of this information has been copied to a digital report to be returned with the submitted evidence.

C. Please note that all child pornography images are considered contraband. The digital report that has been included with the evidence may contain contraband material. It cannot be copied or disseminated without the knowledge and permission of the case analyst. Upon adjudication of this case, the digital report shall be destroyed.

D. The recovered data were copied to a digital report to be picked up with the evidence at your earliest convenience. Should you have trouble viewing the contents of the digital report or have any questions, please contact me.

E. Due to the nature of the evidence on the digital report and computer hard drive (or other media), it is the policy of this laboratory that it should be picked up in person. Therefore the evidence you submitted will be retained, please make arrangements to pick it up.

F. The National Center for Missing and Exploited Children (NCMEC) offers a service called the Child Victim Identification Project. NCMEC will attempt to identify known children in any child pornographic images submitted to them. If you would like more information about this service, please contact me.

2.3 Legal Authorization
A. Digital evidence examination is a more intrusive search than a “plain sight” search and it is therefore not acceptable for the Search Warrant to simply give the authority for an officer to seize the computers in a specified location. The wording on the Search Warrant or Consent Form should specifically state that the data which resides on the seized digital media will be forensically examined (recovered and searched) by the TXDPS Crime Laboratory. Templates are available.
B. The laboratory will notify the submitting officer if the information provided on the Search Warrant or Consent to Search form is inadequate for examination of the evidence or if one is not provided at the time of the evidence submission. After this notification, the officer will have 30 days to respond and provide what is needed or the case will be closed without examination. Evidence may be resubmitted to the laboratory for examination after the acceptable search warrant or consent to search form(s) has been obtained.

2.4 Audio, Video, and Image Analysis Reporting Statements

Examples of audio, video, and image forensic statements, depending on examination and conclusions:

A. Video files were extracted from the DVR hard drive. All files from the requested time period were saved and provided in a digital report for your review.

B. The video was trimmed to the time period containing the [subject or object] of interest.

C. Frame by frame images were extracted from each of the videos.

D. From the provided video, [number] of frames were enhanced and saved. These images were written to a digital report for your review and identification.

E. The audio was enhanced in an attempt to clarify the conversation or event.

F. Due to the [limitations in the image/audio quality] limited enhancements could be performed.

3 Limitations

A. Not every situation can be represented by these statements and it may be necessary to modify statements to accurately reflect the results.

B. Technical steps are listed in Worksheet/Chronology.

4 Literature References and Supporting Documentation

The Scientific Working Group on Digital Evidence (SWGDE) Requirements for Report Writing in Digital and Multimedia Forensics, Version 1.0, November 20, 2018
DM-01-05 STANDARD ABBREVIATIONS LIST

1 Scope
This is a listing of abbreviations commonly used by Digital/Multimedia examiners. This list has been generated to assist in the interpretation of case file notes and is not a standardized list of required abbreviations.

2 Abbreviations
▲ Refers to a column sorted a certain direction (by date, file name, etc.)

1:1 Life sized
3GPP 3rd Generation Partnership Project
3G Third Generation
4G Fourth Generation
5G Fifth Generation
ADB Android Debugging Bridge
AD Access Data (manufacturer)
ADJ Adjusted
AE Additional Evidence
APB All-points Bulletin
AFC Apple File Conduit/Connection
ALS Alternate Light Source
AOI Area of Interest
API Application Programming Interface
APFS Apple File System
ASCII American Standard Code for Information Interchange – standard text
AV, A/V Audio/Video
AVI Audio Video Interleave
avg average
AW Alienware (forensic workstation)
BCD Binary Coded Decimal
BGA Ball Grid Array
BIOS Basic Input/Output System (used to refer to PC time/date information)
Bit Binary Digit
bkgd background
BL BlackLight
Blk bal Black balance
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMP</td>
<td>Bitmap</td>
</tr>
<tr>
<td>BN</td>
<td>Bookmark notable data</td>
</tr>
<tr>
<td>CB</td>
<td>Circuit Board</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed Circuit Television</td>
</tr>
<tr>
<td>CD/CD-ROM</td>
<td>Compact Disc</td>
</tr>
<tr>
<td>CDFS</td>
<td>Compact Disc File System</td>
</tr>
<tr>
<td>CDMA</td>
<td>Code-Division Multiple Access</td>
</tr>
<tr>
<td>CF</td>
<td>Computer Forensics</td>
</tr>
<tr>
<td>CHS</td>
<td>Cylinder-Head-Sector</td>
</tr>
<tr>
<td>Chrono</td>
<td>Chronology (LAB-DM-04 worksheet)</td>
</tr>
<tr>
<td>CMOS</td>
<td>Complementary Metal Oxide Semiconductor</td>
</tr>
<tr>
<td>CP</td>
<td>Child Pornography</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>CST</td>
<td>Central Standard Time</td>
</tr>
<tr>
<td>CS6Extended</td>
<td>Creative Suite 6 Extended – Forensic Image Enhancement Software by Adobe Photoshop</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic Redundancy Check</td>
</tr>
<tr>
<td>DAC</td>
<td>Digital Audio Corporation (Quick Enhance plug-in software in Avid for audio enhancement)</td>
</tr>
<tr>
<td>dB</td>
<td>Decibel</td>
</tr>
<tr>
<td>DC</td>
<td>Direct Current</td>
</tr>
<tr>
<td>DD</td>
<td>Low-level copying and conversion of raw data</td>
</tr>
<tr>
<td>DE</td>
<td>Derivative Evidence</td>
</tr>
<tr>
<td>DFU (mode)</td>
<td>Device Firmware Update Mode</td>
</tr>
<tr>
<td>DIMS</td>
<td>Digital Information Image Management System</td>
</tr>
<tr>
<td>DL</td>
<td>Driver License</td>
</tr>
<tr>
<td>DMM</td>
<td>Digital Multi-Meter</td>
</tr>
<tr>
<td>DOC</td>
<td>Document</td>
</tr>
<tr>
<td>DOO</td>
<td>Date of Offense</td>
</tr>
<tr>
<td>DOS</td>
<td>Disk Operating System</td>
</tr>
<tr>
<td>DVD</td>
<td>Digital Versatile Disc, Digital Video Disc</td>
</tr>
<tr>
<td>DVDR or DVD-R</td>
<td>Digital Video Disc Recordable</td>
</tr>
<tr>
<td>DVR</td>
<td>Digital Video Recorder</td>
</tr>
<tr>
<td>EC</td>
<td>Evidence Coordination</td>
</tr>
<tr>
<td>EDGE</td>
<td>Enhanced Data for GSM Evolution</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>EFI</td>
<td>Extensible Firmware Interface</td>
</tr>
<tr>
<td>EMS</td>
<td>Enhanced Messaging Service</td>
</tr>
<tr>
<td>Enl</td>
<td>Enlarge</td>
</tr>
<tr>
<td>Env(#)</td>
<td>Guidance Software’s EnCase (version number)</td>
</tr>
<tr>
<td>EP</td>
<td>Extended Play</td>
</tr>
<tr>
<td>EQ</td>
<td>Equalizer (analog filter equipment for enhancement of audio frequencies)</td>
</tr>
<tr>
<td>ESN</td>
<td>Electronic Serial Number</td>
</tr>
<tr>
<td>Ex / Exh</td>
<td>Exhibit</td>
</tr>
<tr>
<td>exFAT</td>
<td>Extended File Allocation Table</td>
</tr>
<tr>
<td>Exif</td>
<td>Exif data (Exchangeable Image File)</td>
</tr>
<tr>
<td>Exp</td>
<td>Exposure (- under, + over)</td>
</tr>
<tr>
<td>FAT</td>
<td>File Allocation Table</td>
</tr>
<tr>
<td>FCC ID</td>
<td>Federal Communications Commission Identification Number</td>
</tr>
<tr>
<td>Fgrprts, FP</td>
<td>Fingerprint</td>
</tr>
<tr>
<td>Fgrptcard, FPC</td>
<td>Fingerprint Card</td>
</tr>
<tr>
<td>FM</td>
<td>Frequency Modulation</td>
</tr>
<tr>
<td>FTK</td>
<td>Access Data’s Forensic Tool kit</td>
</tr>
<tr>
<td>FVA</td>
<td>Forensic Video Analysis</td>
</tr>
<tr>
<td>FVAU</td>
<td>Forensic Video Analysis Unit</td>
</tr>
<tr>
<td>FW</td>
<td>Fire Wire</td>
</tr>
<tr>
<td>FWS</td>
<td>Forensic Workstation</td>
</tr>
<tr>
<td>GB</td>
<td>Gigabyte</td>
</tr>
<tr>
<td>GMT</td>
<td>Greenwich Mean Time</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile communication</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>GUID</td>
<td>Globally Unique Identifier</td>
</tr>
<tr>
<td>HDD</td>
<td>Hard Disk Drive</td>
</tr>
<tr>
<td>HDTV</td>
<td>High Definition Television</td>
</tr>
<tr>
<td>HFS/HFS+</td>
<td>Hierarchical File System/plus (pertains to MAC OS)</td>
</tr>
<tr>
<td>HiLGT</td>
<td>Highlight</td>
</tr>
<tr>
<td>Ht</td>
<td>Height</td>
</tr>
<tr>
<td>HTML</td>
<td>Hypertext Markup Language</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
</tr>
<tr>
<td>Hware</td>
<td>Hardware</td>
</tr>
<tr>
<td>Hz</td>
<td>Hertz</td>
</tr>
<tr>
<td>IC</td>
<td>Integrated Circuit</td>
</tr>
<tr>
<td>ICCID</td>
<td>Integrated Circuit Card Identifier</td>
</tr>
<tr>
<td>I/O</td>
<td>Input/Output</td>
</tr>
<tr>
<td>IDE</td>
<td>Integrated Drive Electronics</td>
</tr>
<tr>
<td>iDEN</td>
<td>Integrated Digital Enhanced Network</td>
</tr>
<tr>
<td>IE</td>
<td>Windows Internet Explorer</td>
</tr>
<tr>
<td>IEF</td>
<td>Magnet Forensic’s Internet Evidence Finder</td>
</tr>
<tr>
<td>IM</td>
<td>Instant Messaging</td>
</tr>
<tr>
<td>IMEI</td>
<td>International Mobile Equipment Identity</td>
</tr>
<tr>
<td>IMG</td>
<td>Picture, Image</td>
</tr>
<tr>
<td>IMSI</td>
<td>International Mobile Subscriber Identity Number</td>
</tr>
<tr>
<td>Inet</td>
<td>Internet</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IR</td>
<td>Infrared</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>JPG, JPEG</td>
<td>Joint Photographic Experts Group</td>
</tr>
<tr>
<td>JTAG</td>
<td>Joint Test Action Group</td>
</tr>
<tr>
<td>JTrax</td>
<td>Justice Trax LIMS</td>
</tr>
<tr>
<td>KB</td>
<td>Kilobyte</td>
</tr>
<tr>
<td>KFF</td>
<td>Known File Filter (FTK)</td>
</tr>
<tr>
<td>LBA</td>
<td>Logical Block Addressing</td>
</tr>
<tr>
<td>LCD</td>
<td>Liquid Crystal Display Monitor/Television</td>
</tr>
<tr>
<td>LED</td>
<td>Light Emitting Diode</td>
</tr>
<tr>
<td>LEVA</td>
<td>Law Enforcement Video Association (provides Forensic Video Analysis training)</td>
</tr>
<tr>
<td>LinEn</td>
<td>Linux version of the normally DOS based EnCase</td>
</tr>
<tr>
<td>LNK</td>
<td>Link file (.lnk)</td>
</tr>
<tr>
<td>LP</td>
<td>Long Play</td>
</tr>
<tr>
<td>LTE</td>
<td>Long Term Evolution</td>
</tr>
<tr>
<td>MAC</td>
<td>Mac Forensic Workstation</td>
</tr>
<tr>
<td>MB</td>
<td>Megabyte</td>
</tr>
<tr>
<td>MD5</td>
<td>Message-Digest Algorithm</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>MEID</td>
<td>Mobile Equipment Identifier</td>
</tr>
<tr>
<td>MF</td>
<td>Mobile Forensics</td>
</tr>
<tr>
<td>MFT</td>
<td>Master File Table</td>
</tr>
<tr>
<td>Mgray</td>
<td>Middle gray or 18% reflectance</td>
</tr>
<tr>
<td>MHz</td>
<td>Megahertz</td>
</tr>
<tr>
<td>MMS</td>
<td>Multimedia Messaging Service (pertaining to mobile devices)</td>
</tr>
<tr>
<td>MPE+</td>
<td>Access Data’s Mobile Phone Examiner Plus</td>
</tr>
<tr>
<td>MPEG</td>
<td>Moving Picture Experts Group</td>
</tr>
<tr>
<td>Ms</td>
<td>millisecond</td>
</tr>
<tr>
<td>MSISDN</td>
<td>Mobile Station International Subscriber Directory Number</td>
</tr>
<tr>
<td>MTP</td>
<td>Media Transfer Protocol</td>
</tr>
<tr>
<td>mV</td>
<td>millivolt</td>
</tr>
<tr>
<td>NAND</td>
<td>Binary logic gate or storage memory</td>
</tr>
<tr>
<td>NCBI</td>
<td>National Computer Forensics Institute</td>
</tr>
<tr>
<td>NCMEC</td>
<td>National Center for Missing and Exploited Children</td>
</tr>
<tr>
<td>NIC</td>
<td>Network Interface Card</td>
</tr>
<tr>
<td>NN</td>
<td>No notable data</td>
</tr>
<tr>
<td>NOR</td>
<td>Binary logic gate or storage memory</td>
</tr>
<tr>
<td>Nos</td>
<td>Numbers</td>
</tr>
<tr>
<td>NTFS</td>
<td>New Technology File System</td>
</tr>
<tr>
<td>NTSC</td>
<td>National Television System Committee (analog television system that is used in most of North America)</td>
</tr>
<tr>
<td>Olay</td>
<td>Overlay</td>
</tr>
<tr>
<td>OLE</td>
<td>Object Linking and Embedding</td>
</tr>
<tr>
<td>OR</td>
<td>Binary logic gate for logic disjunction</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OTG</td>
<td>On-The-Go cable</td>
</tr>
<tr>
<td>PA</td>
<td>Physical Analyzer</td>
</tr>
<tr>
<td>PB</td>
<td>Petabyte</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PCB</td>
<td>Printed Circuit Board</td>
</tr>
<tr>
<td>PCI</td>
<td>Peripheral Component Interconnect</td>
</tr>
<tr>
<td>PDA</td>
<td>Personal Digital Assistant</td>
</tr>
<tr>
<td>PDF</td>
<td>Portable Document Format</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>Plist</td>
<td>Property list</td>
</tr>
<tr>
<td>POI</td>
<td>Point of Interest (referring to GPS device locations)</td>
</tr>
<tr>
<td>PN, P/N</td>
<td>Part Number</td>
</tr>
<tr>
<td>POST</td>
<td>Power On Self-Test</td>
</tr>
<tr>
<td>Prt</td>
<td>Print</td>
</tr>
<tr>
<td>PRTK</td>
<td>Access Data’s Password Recovery Toolkit</td>
</tr>
<tr>
<td>Pshop</td>
<td>Photoshop</td>
</tr>
<tr>
<td>PT</td>
<td>Performance Test</td>
</tr>
<tr>
<td>PUK</td>
<td>PIN Unlock Key</td>
</tr>
<tr>
<td>PW</td>
<td>Password</td>
</tr>
<tr>
<td>RAID</td>
<td>Redundant Array of Independent Disks</td>
</tr>
<tr>
<td>RAM</td>
<td>Random Access Memory</td>
</tr>
<tr>
<td>RCA</td>
<td>Jack or Plug for carrying a composite signal</td>
</tr>
<tr>
<td>RCFL</td>
<td>Regional Computer Forensic Laboratory</td>
</tr>
<tr>
<td>Reg Rip</td>
<td>Harlan Carvey’s Registry Ripper</td>
</tr>
<tr>
<td>Res</td>
<td>Resolution</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>RIB</td>
<td>Ramsey Isolation Box (for blocking signals to digital devices)</td>
</tr>
<tr>
<td>ROM</td>
<td>Read Only Memory</td>
</tr>
<tr>
<td>SAM</td>
<td>Security Accounts Manager</td>
</tr>
<tr>
<td>SAN</td>
<td>Storage Area Network</td>
</tr>
<tr>
<td>SATA</td>
<td>Serial Advanced Technology Attachment</td>
</tr>
<tr>
<td>SCSI</td>
<td>Small Computer System Interface</td>
</tr>
<tr>
<td>SD</td>
<td>Secure Digital</td>
</tr>
<tr>
<td>SDHC</td>
<td>Secure Digital High Capacity</td>
</tr>
<tr>
<td>SDK</td>
<td>Software Development Kit</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>Shoeprt</td>
<td>Shoeprint</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module</td>
</tr>
<tr>
<td>SIMID</td>
<td>Subscriber Identity Module Identifier</td>
</tr>
<tr>
<td>SMPTE</td>
<td>Society of Motion Picture and Television Engineers</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>SN, S/N</td>
<td>Serial Number</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>SOP</td>
<td>Standard Operating Procedure</td>
</tr>
<tr>
<td>SP</td>
<td>Standard Play</td>
</tr>
<tr>
<td>SRAM</td>
<td>Static Random Access Memory</td>
</tr>
<tr>
<td>SSD</td>
<td>Solid State Drive</td>
</tr>
<tr>
<td>S/T</td>
<td>Service Tag</td>
</tr>
<tr>
<td>SW</td>
<td>Search Warrant</td>
</tr>
<tr>
<td>Sware</td>
<td>Software</td>
</tr>
<tr>
<td>SWGDE</td>
<td>Scientific Working Group on Digital Evidence</td>
</tr>
<tr>
<td>SWGIT</td>
<td>Scientific Working Group on Imaging Technologies</td>
</tr>
<tr>
<td>Sys</td>
<td>System or System file</td>
</tr>
<tr>
<td>TB</td>
<td>Terabyte</td>
</tr>
<tr>
<td>TBC</td>
<td>Time Base Corrector</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol/Internet Protocol</td>
</tr>
<tr>
<td>TFD#, TD, TFI</td>
<td>Tableau Forensic Duplicator, Tableau Duplicator, Tableau Forensic Imager</td>
</tr>
<tr>
<td>TD3</td>
<td></td>
</tr>
<tr>
<td>Tireprts</td>
<td>Tire prints</td>
</tr>
<tr>
<td>Transp</td>
<td>Transparency</td>
</tr>
<tr>
<td>μA</td>
<td>microAmp</td>
</tr>
<tr>
<td>UA</td>
<td>Unallocated Clusters/Space</td>
</tr>
<tr>
<td>UEFI</td>
<td>Unified Extensible Firmware Interface</td>
</tr>
<tr>
<td>UDID</td>
<td>Unique Device Identifier</td>
</tr>
<tr>
<td>UFED PA / PD</td>
<td>Cellebrite’s UFED Physical Analyzer (or Detective)</td>
</tr>
<tr>
<td>UFED</td>
<td>Cellebrite’s UFED</td>
</tr>
<tr>
<td>UICC</td>
<td>Universal Integrated Circuit Card</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunications System</td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterruptible Power Supply</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator or Universal Resource Locator (referencing an Internet resource)</td>
</tr>
<tr>
<td>μS</td>
<td>microsecond</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
<tr>
<td>USIM</td>
<td>UMTS Subscriber Identity Module</td>
</tr>
<tr>
<td>USM</td>
<td>Unsharp mask</td>
</tr>
<tr>
<td>UTC</td>
<td>Coordinated Universal Time</td>
</tr>
<tr>
<td>μV</td>
<td>microvolt</td>
</tr>
<tr>
<td>Veh</td>
<td>Vehicle</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>VHS</td>
<td>Video Home Systems (1/2&quot; video cassette player or tape)</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>VOIP</td>
<td>Voice Over Internet Protocol</td>
</tr>
<tr>
<td>vX</td>
<td>Represents a software version + number (v3.18), can mean any version</td>
</tr>
<tr>
<td>WAP</td>
<td>Wireless Application Protocol</td>
</tr>
<tr>
<td>W bal</td>
<td>White balance</td>
</tr>
<tr>
<td>WiFi</td>
<td>Wireless 802.11 connection</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Access Network</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
<tr>
<td>XWF</td>
<td>X-Ways Forensics</td>
</tr>
</tbody>
</table>
DM-01-06 TECHNICAL PROCEDURE FOR DM SERVER DATA STORAGE

1 Scope
The primary purpose of these procedures is to establish guidelines for the storage of digital forensic images or extractions, or derivative evidence that is copied onto the DM server(s).

2 Related Documents
Archiving or Restoring Digital Evidence (DM-03-02)

3 Policy
A. The DM servers are physically contained in a limited access room. The DM servers are connected to DM forensic workstations through a dedicated internal Virtual Local Area Network (VLAN) that is physically separate from the DPS Texas Law Enforcement (TLE) network. Only systems on this dedicated VLAN can communicate with the DM server(s) and have no public internet access when connecting to the DM server(s). The purpose of this separation is due to the sensitive nature of the evidence or derivative evidence contained on the DM server(s). This data may contain contraband images, sensitive information related to investigations, or files possibly containing viruses.

B. It may be necessary at times to temporarily connect the DM server(s) to the TLE network for the purpose of maintenance and management or support of the server(s). This is done in a supervised and controlled manner by connecting the dedicated network cables configured for the TLE network to the DM server network card(s). In these instances, access is supervised by approved DPS personnel to ensure no unauthorized access to restricted data stored on the DM server(s) occurs. Access to the server is limited to secure username and password. The TLE connection allows a user to remotely conduct management processes such as powering on/off the servers, opening a console, and rebooting the devices. When the DM server(s) are not undergoing maintenance or management, the TLE cables will remain disconnected from the server.

C. Forensic workstations used to acquire, extract, and analyze digital evidence will remain isolated from the internet whenever evidence is connected to or stored on the system. Before workstations are connected to the internet, such as for updates or technical support, the VLAN cable connecting to the DM server(s) must be physically disconnected from the forensic workstation.

D. Copies of forensic images or extractions and derivative evidence may be stored on the DM server(s) as reference material, however there are no requirements for archival or long-term storage on the DM server(s) aside from what is documented in DM-03-02 Archiving or Restoring Digital Evidence. Original evidence should be retained by the submitting agency, as appropriate.

E. Information stored on the DM Server(s) is not a component of the case record.

4 Safety
A. All personnel using electronic equipment should be aware of safety precautions and procedures while using electronic equipment in accordance with laboratory safety policy.

B. Safety equipment includes the use of safety glasses, gloves, dust masks, anti-static mats and clothing as necessary. In some cases, use of fume hood or good ventilation as appropriate.
5 Equipment and Materials

- Forensic Workstation(s)
- DM Server(s)
- TLE
- VLAN cable(s)
- Storage Management software/hardware

6 Standards, Controls, and Calibration

None

7 Procedure

A. Ensure Forensic Workstations have no other external network connections before connecting to the DM server(s).

B. Digital evidence or derivative evidence that is copied to the DM server(s) must be uniquely identified with the associated laboratory case number in the directory name.

C. Evidence and derivative evidence stored on the DM server(s) must have a chain of custody maintained in the Laboratory Information Management System.

D. When applicable, evidence files that are copied to the DM server(s) should undergo a hash verification to ensure the copy is true and accurate. The verification is documented in the case record. If the copy of the evidence files is successfully verified then the original forensic image(s) may be deleted or wiped.

E. DPS.TLE network cables will remain physically unplugged from the DM Server unless the server is undergoing maintenance.

8 Instructions for Use

A. By default, FTK Imager is often set to not detect mapped network drives (such as the DM Server shares). Edit the Windows Registry using these steps (depending on the version of Windows):

1. Click Start and type regedit in the Start programs and files box; press Enter
2. Locate and then right-click the registry subkey: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
3. Point to New, and then click DWORD Value
4. Type EnableLinkedConnections; press Enter
5. Right-click EnableLinkedConnections and click Modify
6. In the Value data box, type 1 and click OK
7. Exit Registry Editor and restart the computer

B. Mapping drives to the workstations can be accomplished in two ways:

1. Copy archiveshares.bat to C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup on the workstation and run the script from this location
The ProgramData directory may be hidden by default. To show hidden files and folders:

a) Type “hidden” in the Start menu search bar;
b) Select Show hidden files and folders under Control Panel;
c) Select Show hidden files, folders, and drives under Folder Options/View

2. Manually create the shares

a) Start → Computer → Map network drive → Select Drive: X → Folder: \10.193.210.54\Archive1 and click Finish

b) Repeat with drives Y and Z for Archive2 and Archive3

C. If unable to map to 10.193.210.54 (HDQPRDDMENAS001) run the script archiveshares-failover.bat to map to the shares hosted from 10.193.210.55 (HDQPRDDMENAS002).

9 Maintenance

The Modular Disk (MD) Storage Manager configures, manages, and monitors the storage array.

A. The MD Storage Manager will give alerts when management of the server is necessary.

B. DM laboratory personnel should regularly monitor the MD Storage Manager and physically check the DM server at least once per week, when possible.

C. DM personnel will document weekly checks in the DM Server #1 Equipment Log.

10 Interpretation

A. The DM server(s) is a mechanical device and is subject to mechanical failure and possible data loss. Original evidence and derivative evidence should be retained by the submitting agency.

B. To prevent contamination of evidence that is stored on the DM server(s), evidence files will labeled, hashed, and stored within separate digital containers whenever possible.

C. Non-evidence data may also be stored on the DM server(s) in a separate digital container.

11 Records

DM Server(s) Equipment Log(s) and Weekly Checks Log
02 EXAMINATION AND RECOVERY TECHNIQUES
DM-02-01 PHYSICAL EVIDENCE EXAMINATION

1 Scope
The primary purpose of these procedures is to establish unifying documentation and standard practices appropriate when performing an initial examination of digital/multimedia evidence.
The procedures presented are intended to be used in conjunction with all applicable laboratory policies, good laboratory practice, and approved scientific methodology.

2 Related Documents
Acquisition of Digital Evidence (DM-03-01)
Archiving or Restoring Digital Evidence (DM-03-02)
Examination of Digital Evidence (DM-03-03)

3 Safety
A. All personnel using electronic equipment should be aware of safety precautions and procedures while using electronic equipment in accordance with laboratory safety policy.
B. Safety equipment includes the use of safety glasses, gloves, dust masks, anti-static mats and clothing as necessary. In some cases, use of fume hood or good ventilation as appropriate.

4 Equipment and Materials
- Envelopes
- Evidence tape
- Markers
- Etching tool
- Plastic bags, paper envelopes, or appropriate evidence containers
- Digital Camera
- Toolkit

5 Standards, Controls, and Calibration
None

6 Precautions
6.1 Contamination
Clean work areas before and between the examination of each evidence item, as appropriate.

6.2 Storage and Handling
Specific care should be taken to avoid physical damage, vibrations, effects of magnetic fields and electrical static and large variations of temperature or humidity.
7 Procedure

7.1 Initial Examination

The initial examination of digital/multimedia evidence is necessary to:

A. Ensure legal search authority prior to examination
B. Identify possible contamination issues
C. Determine if sufficient case information has been provided to conduct a thorough examination
D. Document hardware components, configurations, and settings related to evidence items
E. Determine the appropriate course of action for the collection, preservation and analysis of evidence

The analyst is responsible for the data collection and the preservation of any evidentiary materials that may be on that item.

7.2 Analysis Procedure

1. Locate appropriate search warrant or consent forms. If not present, notify submitting officer that no further analysis will be completed until one is provided. In some cases, evidence is provided by the owner, therefore the requested analysis on the “Laboratory Submission Form” suffices as consent.

2. Retrieve evidence from evidence storage, evidence custodian or another examiner. Verify that the “Laboratory Submission Form” is appropriately completed and a chain of custody maintained. Identify the pertinent forensic requests. Plan the approach to the case.

3. Ensure clean work surface, cover with clean, unused paper when appropriate. Specific care should be taken to avoid physical damage, vibrations, the effects of magnetic fields and electrical static and large variations of temperature or humidity.

4. Document the evidence package and the nature of seals, when appropriate. The case number, item number and examiner initials should be labeled on the packaging. Open the container (avoid breaking previous seals, if possible).

5. Visually inspect the evidence using gloved hands, if necessary.

6. Note whether other items were packaged together with the selected item. Visually examine the evidence and record, as available, the following (documentation may be in the form of inventory photographs which will be stored in the case record.

   a) Condition of the evidence and/or possible contamination or preservation issues

   b) Physical description such as color, size, holes and tears, broken parts, missing parts, or other modifications or defects that make the item appear unusual

   c) Manufacturer’s identification such as make and model, serial numbers, or other marks, as applicable

   d) Any additional evidence items that have been identified and removed from the original evidence item. If feasible, remove hard drive(s) or other storage media devices

   e) Method used to collect other types of evidence
7. Label or tag each item of evidence as appropriate. Include unique case number and examiner initials.

8. Any collected trace evidence may be packaged separately or with the original item, as long as it is uniquely labeled, sealed, initialed and dated. All original exhibits will be re-packaged in the original container, if possible. The evidence is re-sealed in a manner that would allow for the detection of tampering.

### 8 Interpretation

A. Analysts should determine what process will be used to acquire or copy each piece of digital/multimedia evidence based on specifications of the media type, location, and available approved tools and methods.

B. Evaluation of submitted evidence and any necessary documentation will be completed by the forensic analyst at the time of initial examination. This may include, for example, identifying and documenting submitted items of evidence that contain no memory storage (such as Bluetooth adapters, SD card adapters, etc).

C. Proceed to Acquisition of Digital Evidence (DM-03-01) if acquiring or copying digital evidence.

### 9 Records

Laboratory Submission Form (LAB-201)

Digital Multimedia Information Form (LAB-210)

Digital Evidence Analysis Worksheets (LAB-DM-01 through LAB-DM-10, as appropriate)
03 DIGITAL MEDIA ANALYSIS

DM-03-01 ACQUISITION OF DIGITAL EVIDENCE

1 Scope
To assist the analyst in the creation of a forensic digital copy from an item of Digital/Multimedia evidence. This is the secondary step in the Digital/Multimedia (DM) analysis process. This step limits, and in most instances eliminates, the possibility of alteration of the digital evidence.

2 Related Documents
Archiving or Restoring Digital Evidence (DM-03-02)
Examination of Digital Evidence (DM-03-03)

3 Safety
Safety equipment includes the use of safety glasses, gloves, masks, clothing and antistatic mats as necessary. In some cases, use of fume hood or good ventilation as appropriate.

Take precautions for electrical shock.

4 Equipment and Materials
Varies with the method of acquisition used:
- Forensic Workstation
- Tableau device(s)
- Sterile digital media (HDDs, CDs, Floppy disks, SD cards, etc)
- Digital media containing known content with known hash value
- Hardware/software write-blocker
- Crossover network cable
- Controlled boot device (floppy disk, Disc, CD, USB,HDD, etc)
- Appropriate computer/peripheral cables
- Applicable acquisition software
- Applicable wiping software
- Applicable analog media player
- Audio interface

5 Standards, Controls, and Calibration
1. Performance test acquisition software or hardware prior to use on each day, new case, and/or new workstation.
2. Document successful or failed performance test in the case record.

6 Procedure
1. Use sterile digital media to acquire or copy evidence to, when applicable (Note: this does not apply to blank CD/DVDs, which can be used without further preparation). To prepare sterile digital media:
   a) Retrieve forensic analysis target device
   b) Overwrite all disk sectors using validated disk wiping software/hardware
c) Document process in the Forensic Disk Wiping Log
d) Document sterile media identification number or name

2. Document identification information of DM item to be acquired or copied.

3. Conduct performance test of acquisition software/hardware using media with known hash value/content, when applicable.

4. Calculate and document a hash of the original digital media evidence item if possible (many forensic acquisition tools complete this step automatically).

5. Acquire an image of the DM item to sterile media, when applicable, and document the software/hardware type including version number, hardware identification number, and forensic workstation number, when applicable.

6. Calculate and document the hash of the acquired or copied image or file (when copied or moved for the purpose of examination or storage). Compare the hash values of the original evidence and the acquired or copied image or file.

   a) If this value is the same as the hash of the original DM item, the analyst can proceed with the analysis

   b) If this value is different from the hash of the original DM item, the original item should be reacquired or re-copied

   c) If the hash of image or file is different from the original evidence again, and the analyst deems the most likely cause is mechanical failure of the original DM item, document the observations and proceed with the analysis of the first image or file

7. If the difference in the hash is believed to not be caused by mechanical failure of the original item, document the observations and another acquisition or copy should be made.

8. The bit-by-bit acquisition of Solid State Drives (SSDs) may not result in matching hash values due to the volatile nature of SSDs while powered on. This does not mean that the acquisition is not forensically sound. If the hash values do not match during an SSD acquisition, the analyst should document the result and move forward with the examination process.

9. Access and document the BIOS/UEFI time setting information of each submitted computer ensuring no changes are made to any data resident on the computer, when possible. When no notable data are recovered, it is not necessary to document the BIOS/UEFI time setting.

10. When a bit-by-bit acquisition is performed, the evidence should be powered off whenever possible (with the exception of mobile device evidence). At times it may be necessary to boot evidence to obtain a live acquisition (an acquisition of an item while it is powered on), or to conduct a manual examination. This may apply to evidence such as full-disk encrypted computers in which the encryption key or login credentials are provided. If a live acquisition or manual examination of computer evidence (excluding mobile devices) must be performed, the analyst should communicate the possible risks with the submitting agency and proceed only after obtaining authorization from the submitting agency.

11. When analog media is acquired digitally to a forensic workstation, a hash value of the newly created digital file(s) must be generated. This protects the integrity of this
forensic copy. Due to the nature of analog media, subsequent copies will likely calculate different hash values. Therefore, the hash value generated after acquisition serves to protect the integrity solely of the copy created by the examiner.

7 Interpretation

A. Proceed to Archiving or Restoring a Digital Evidence (DM-03-02) or Examination of Digital Evidence (DM-03-03).

B. The analyst will determine that a valid forensic copy was created when the hash value of the copy matches the hash value of the original item unless the original evidence item is volatile or dynamic in nature.

8 Records
Forensic Disk Wiping Log
Chronology of Examination (LAB-DM-04)

9 Literature References and Supporting Documentation
National White Collar Crime Center’s (NW3C) Basic Data Recovery and Analysis (BDRA) USB/file dated 2016
The Scientific Working Group on Digital Evidence (SWGDE) Best Practices for Computer Forensic Acquisitions, Version 1.0, April 25, 2018
DM-03-02 ARCHIVING OR RESTORING DIGITAL EVIDENCE

1 Scope
To assist the analyst in the creation of a digital archive, which may consist of restored data, copied data, converted data, extracted data or restored physically acquired data, when needed. This can ensure the presence of a backup forensic copy in the case of hardware failure or for later reexamination.

2 Related Documents
Acquisition of Digital Evidence (DM-03-01)
Examination of Digital Evidence (DM-03-03)

3 Safety
Safety equipment includes the use of safety glasses, gloves, masks, clothing and antistatic mats as necessary. In some cases, use of fume hood or good ventilation as appropriate.

4 Equipment and Materials
Varies with the method of archiving used:
- Forensic Workstation
- Blank digital media (HDDs, CDs, DVDs, etc)
- DM secure VLAN server
- Appropriate computer/peripheral cables
- Archiving software
- Hashing software

5 Standards, Controls, and Calibration
None

6 Policy
A. Cases related to Capital Murder and Murder must be archived whenever possible. Other case evidence files may be archived with approval from the Technical Point of Contact, Advisory Board Chair, or Section Supervisor. Archives may be destroyed after a period of at least two years following the last released digital forensic report.

B. All digital reports containing notable data will be archived for all cases. Additionally, all evidence that must be returned to the submitting agency prior to analysis must first be archived. These archives can be destroyed following analysis if the offense is not one of the above listed offenses. Exhibits that are NOT examined will not be archived.

C. All digital media deteriorates over time; the archive copy can become corrupt due to aging which can preclude additional examination.

D. A restored image can be created upon request or to assist during an examination.

E. Copies of forensic images or extractions and derivative evidence are considered to be work product. They are uniquely identified and tracked in LIMS, but are not considered evidentiary. This work product is not considered to be a component of the case record.
7 Procedure

1. Copy or restore all evidence files to sterile digital media or location on the secured DM server and document the method used in the case record, as appropriate.

2. Determine the hash value of the archived or restored image and compare it to the hash value of the original evidence item.
   a) If the hash values match, store the archive or restored media.
   b) If the hash values do not match, re-archive or re-restore the digital evidence.
   c) If the hash values do not match after re-archiving or re-restore, determine the hash value of the digital evidence again.
      i. If the hash value of the copy is the same as the original evidence item, re-archive or re-restore the forensic image.
      ii. If the hash value of the copy is different from the original item, reacquire or re-copy from the original DM evidence item, if available.

8 Interpretation

A. Proceed to Examination of Digital Evidence (DM-03-03), when applicable.

B. The analyst will determine that a valid restored image was created when the restored image hash value matches the forensic image hash value.

C. The analyst will determine that a valid archive was created when there are no errors while copying the evidence files, and the hash value of the evidence files matches the hash value of the original DM evidence item.

9 Records

Digital Evidence Analysis Inventory (LAB-DM-01)

10 Literature References and Supporting Documentation


DM-03-03 EXAMINATION OF DIGITAL EVIDENCE

1 Scope

The Examination of Digital Evidence procedure is intended to provide the steps for searching the
digital evidence for data pertaining to the submitted request. If pertinent data is located it will be
included in the report to the submitting official.

2 Related Documents

Acquisition of Digital Evidence (DM-03-01)
Archiving or Restoring Digital Evidence (DM-03-02)

3 Safety

Safety equipment includes the use of safety glasses, gloves, dust masks, anti-static mats and
clothing as necessary. In some cases, use of fume hood or good ventilation as appropriate.

4 Equipment and Materials

- Forensic workstation
- Sterile digital media
- Mobile device data extraction hardware/software
- Forensic analysis software
- Electronic signal isolation device/method
- Commercially available software

5 Standards, Controls, and Calibration

None

6 Procedure

Note: Every case is unique and may require different steps in order to perform analysis. The
following are guidelines only, and it is up to the individual analyst to decide which steps are
required on a case-by-case basis.

1. Examine the forensic copy of the original evidence.
2. Determine the nature of the analysis to be conducted including software to be used, and/or the type of data that may be present on the digital evidence.
   a) Document the software (and its version) used to analyze the copy of the
digital evidence
   b) Document the presence of notable data and examination method used. The
   physical location from which notable data was recovered should be
documented in the case record when appropriate
3. Data that pertains to the investigation will be written to blank digital media.
4. If evidence containing possible contraband is recovered then the evidence file
   should be mounted, if necessary, and scanned for malware, when applicable.
   Document the process and results in the case file. The malware scan can be
   performed before or after analysis.
7 Interpretation

A. Evaluation and interpretation of the case findings will be conducted on a case-by-case basis.

B. Ages of individuals cannot be determined by this analysis from recovered or extracted movies or pictures.

C. The submitting agency will be notified if apparent information pertaining to potential criminal activity beyond the scope of the requested analysis is not included under a consent to search, search warrant, or other request is observed. When appropriate, this information will be technically reviewed by a qualified analyst prior to release.

8 Records

Digital Evidence Analysis Inventory (LAB-DM-01)

9 Literature References and Supporting Documentation


The Scientific Working Group on Digital Evidence (SWGDE) Best Practices for Computer Forensic Examination, Version 1.0, July 11, 2018

04 AUDIO/VIDEO/IMAGE ANALYSIS
DM-04-01 FORENSIC VIDEO ANALYSIS

1 Scope
Video enhancement, clarification, restoration, filtration, and other processing activities that are intended to improve the visual appearance of features in frame(s) of video from a video recording are considered examination tasks. Forensic Video Analysis is the scientific examination, comparison, and/or evaluation of video in legal matters. Various equipment and computerized hardware and software may be used. The appropriate forensic tools will be addressed on a case-by-case basis by the Digital/Multimedia section.

This document contains the procedures for the analysis of video in order to clarify or enhance some or all of the visual information contained within the submitted media. The most typical operations conducted on video or images include, but are not limited to: contrast adjustment, demultiplexing a multiplexed video signal, magnifying an area of interest, frame averaging, sharpening and deinterlacing.

2 Related Documents
Physical Evidence Examination (DM-02-01)
Acquisition of Digital Evidence (DM-03-01)
Forensic Audio Analysis (DM-04-02)
Forensic Image Analysis (DM-04-03)

3 Safety
All personnel using electronic equipment should be aware of safety precautions and procedures while using electronic equipment in accordance with laboratory safety policy. Gloves should be worn to handle any potential biohazard evidence.

4 Equipment and Materials
No reagents. Media requirements dictate the equipment and materials needed. Software is documented on the Approved Software list.

- Forensic Workstation(s)
- Applicable analog video cassette player
- Splicing blocks
- Splicing tape/tabs
- Razor blades/scissors
- Gloves
- Clamps
- Lint free clothes

5 Standards, Controls, and Calibration
None
6 Procedure

Note: Every case is unique and may require different steps in order to perform analysis. The following are guidelines only, and it is up to the individual analyst to decide which steps are required on a case-by-case basis.

A. Prior to Examination.

Consideration should be given to the following before commencing any examination of video evidence:

1. **Examination Priority.** Priority should be given to other forensic examinations (fingerprints analysis, trace evidence analysis, etc.) before any forensic video analysis proceeds. The minimum precautions must be identified and implemented.

2. **Search Authorization.** Proper search warrant or consent to search allowing examination of digital evidence should be verified prior to any forensic video analysis.

3. **Integrity of Evidence.** Video evidence submitted for forensic video analysis should first be reviewed for its integrity. Any deficiency (damage, write protections not in place, etc.) should be documented and resolved before any forensic video analysis proceeds.

4. **Protection of Evidence.** At all times, precautions should be taken to ensure video evidence is protected from external factors (magnetic fields, static electric charges, electrical hazards, etc.) that may cause damage to the media or to the recorded signal contained on the media.

B. All media will be physically examined prior to being inserted into or connected to any device. A visual inspection of the media should be conducted to:

1. Ensure housing or media is intact and not broken, damaged, or dirty

2. If damage is found, take corrective action and document. If media is visibly damaged, the submitting case detective or officer shall be consulted as to whether steps shall be taken to repair the damaged evidence.

3. If necessary, perform basic magnetic tape restoration
   a) **Detangle tape as necessary.**
   b) **If possible, minimize any creases in tape by placing tape between flat, weighted objects.**
   c) **With razor blade and splicing block, remove any portions of tape that are irreparable or might inhibit playback. If segments of the tape are determined to be beyond repair or detrimental to playback, remove and label the segments determined to be irreparable and from where it was removed.**
   d) **Splice restored segments to virgin tape, leader, and hubs, as necessary.**
   e) **Place restored segments in new housings, as necessary.**
   f) **If more damage is noted, further reconstruction may be necessary.**
   g) **Each new cassette will be labeled with appropriate case information and examiners initials**
h) Enable any record-protection device (e.g., punch-out tab, slide record tab, remove record button) on new housings.

4. If tape has residue that may inhibit playback or damage playback equipment, such as soda, oil, plant growth, or sediment, it will not be restored or processed.

C. The examiner shall make every reasonable effort to prevent accidental erasure of media related to criminal investigations.

1. For analog media, “record tabs” shall either be removed from the media or positioned to the “safe” position on the videocassette shell or disk sleeve before any viewing or analysis of the medium is performed.

2. For digital media, write blocking devices or software shall be used when applicable.

D. The best results will be achieved when the media to be examined is the original recording. If it is apparent that the media is a recording of a recording, it will not be analyzed.

E. For analog media, select the appropriate playback device(s) to achieve optimal signal quality.

F. A working copy of the original file will be created and labeled in a manner to recognize such file as a working copy.

1. All subsequent analysis will be conducted on the working copy.

2. If all resources have been exhausted and analysis cannot continue with the working copy, analysis may continue from the original evidence with prior approval of the appropriate chain of command and the submitting officer.

G. To verify that the working copy is a true and accurate representation of the original evidence, a hash verification must be performed for digital evidence.

H. Examine metadata to learn relevant information about the video/image file(s) to be examined. Relevant data includes, but is not limited to:

1. codec,

2. resolution,

3. stream information, and

4. frame rate.

I. If necessary, a video file may be transcoded or converted to a universally playable file format. If the file cannot be transcoded or converted a screen capture utility may be used.

J. The desired video file will be opened in the applicable software program(s) chosen at the examiner’s discretion.

K. Using the selected devices or software, review the submitted video to locate the pertinent segment(s).

L. Whenever possible, techniques that use either no data compression or visually lossless compression should be used.

M. All derived files will utilize the case number and a numbering sequence to identify multiple captures or images.
N. The videofile will be processed as necessary to clarify detail as requested. Any processing steps used in the course of generating the final output video will be recorded, with appropriate values, in the examiner’s case notes and/or software-generated reports.

O. For video clarification, the fewest number of steps as practical shall be used and the examiner shall only use techniques which are documented and can be reproduced.

P. Once enhanced, the file(s) will be saved in a lossless or minimally compressed file format.

Q. If audio analysis is also necessary proceed to Forensic Audio Analysis (DM-04-02).

R. The final video(s) should be saved to appropriate media such as Evidence CD or DVD, USB flash drive or Hard Drive Disk. Regardless of the output media, the examiner must provide a product that accurately represents the visual content of the original evidence.

S. To verify that the derivative and archived evidence are true and accurate representations of the analyzed evidence, a hash verification must be performed for digital evidence.

7 Interpretation

Compare the final product with the original submission to confirm that enhancements have improved the visual appearance in the areas of forensic interest as much as possible.

8 Precautions or Limitations

A. Enhancement capabilities are limited by variables including but not limited to the quality of the original recording, subject to camera distance, light, and motion.

B. Examiners will not identify subjects, objects, or vehicles from surveillance videos.

9 Literature References and Supporting Documentation

Amped FIVE Training Material
DVR Examiner User Guide
LEVA Level I Training Material
LEVA Level II Training Material
DM-04-02 FORENSIC AUDIO ANALYSIS

1 Scope

Audio analysis and/or enhancement ("clarification") is a process that is intended to improve the audible characteristics of a digital or analog signal from a videotape, audiotape (regular or micro cassette), reel-to-reel tape, answering machine, disc, or other media containing audio. Forensic Audio Analysis is the scientific examination, comparison, and/or evaluation of audio in legal matters. Various equipment and computerized hardware and software may be used. The appropriate forensic tools will be addressed on a case-by-case basis by the Digital/Multimedia section.

The processes that may be performed include: media characterization, duplicate/copy, reconstruction/recovery, playback optimization, data extraction, data/signal analysis, enhancement, and format/standard conversions. Audio authentication or voice comparisons are not included.

This document contains the procedures for the analysis of audio in order to clarify or enhance some or all of the audio contained within the submitted media.

The most typical operations conducted on an analog audio media submitted is by duplicating the audio through an audio interface to enhance the overall volume or decrease ambient sounds such as wind noise or other extraneous sounds. Submitted digital audio media should be enhanced and clarified using verified forensic software.

2 Related Documents

Physical Evidence Examination (DM-02-01)
Forensic Video Analysis (DM-04-01)
Forensic Image Analysis (DM-04-03)

3 Safety

All personnel using electronic equipment should be aware of safety precautions and procedures while using electronic equipment in accordance with laboratory safety policy. Gloves should be worn to handle any potential biohazard evidence.

4 Equipment and Materials

No reagents. Media requirements dictate the equipment and materials needed. Software is documented on the Approved Software list.

- Forensic Workstation(s)
- Speakers
- Headphones
- Audio cassette recorder/player
- Micro cassette recorder/player
- Audio interface
- Splicing blocks
- Splicing tape/tabs
- Razor blades/scissors
- Gloves
5 Standards, Controls, and Calibration

None

6 Procedure

A. Prior to Examination.

Consideration should be given to the following before commencing any examination of audio evidence:

1. Examination Priority. Priority should be given to other forensic examinations (fingerprints analysis, trace evidence analysis, etc.) before any forensic video analysis proceeds. The minimum precautions must be identified and implemented.

2. Search Authorization. Proper search warrant or consent to search allowing examination of digital evidence should be verified prior to any forensic video analysis.

3. Integrity of Evidence. Audio evidence submitted for forensic audio analysis should first be reviewed for its integrity. Any deficiency (damage, write protections not in place, etc.) should be documented and resolved before any forensic audio analysis proceeds.

4. Protection of Evidence. At all times, precautions should be taken to ensure audio evidence is protected from external factors (magnetic fields, static electric charges, electrical hazards, etc.) that may cause damage to the media or to the recorded signal contained on the media.

B. All media will be physically examined prior to being inserted into or connected to any device. A visual inspection of the media should be conducted to:

1. Ensure housing or media is intact and not broken, damaged, or dirty

2. If damage is found, take corrective actions and document. If media is visibly damaged, the submitting case detective or officer shall be consulted as to whether steps shall be taken to repair the damaged evidence.

3. If necessary, perform basic magnetic tape restoration
   a) Detangle tape as necessary.
   b) If possible, minimize any creases in tape by placing tape between flat, weighted objects.
   c) With razor blade and splicing block, remove any portions of tape that are irreparable or might inhibit playback. If segments of the tape are determined to be beyond repair or detrimental to playback, remove and label the segments determined to be irreparable and from where it was removed.
   d) Splice restored segments to virgin tape, leader, and hubs, as necessary.
   e) Place restored segments in new housings, as necessary.
   f) If more damage is noted, further reconstruction may be necessary.
g) Each new cassette will be labeled with appropriate case information and examiners initials

h) Enable any record-protection device (e.g., punch-out tab, slide record tab, remove record button) on new housings.

4. If tape has residue that may inhibit playback or damage playback equipment, such as soda, oil, plant growth, or sediment, it will not be restored or processed.

C. The examiner shall make every reasonable effort to prevent accidental erasure of media related to criminal investigations.

1. For analog media, “record tabs” shall either be removed from the media or positioned to the “safe” position on the audio/video cassette shell or disk sleeve before any listening, monitoring, viewing or analysis of the medium is performed.

2. For digital media, write blocking devices or software shall be used when applicable.

D. The best results will be achieved when the media to be examined is the original recording. If it is apparent that the media is a recording of a recording, it will not be analyzed.

E. For analog media, select the appropriate playback device(s) to achieve optimal signal quality.

F. Document the make, model, and settings of the device used to record the submitted video, if possible. These settings may include the recording format and speed.

G. A working copy of the original file will be created and labeled in a manner to recognize such file as a working copy.

1. All subsequent analysis will be conducted on the working copy.

2. If all resources have been exhausted and analysis cannot continue with the working copy, analysis may continue from the original evidence with prior approval of the appropriate chain of command and the submitting officer.

H. To verify that the working copy is a true and accurate representation of the original evidence, a hash verification must be performed for digital evidence.

I. Examine metadata to learn relevant information about the video/image file(s) to be examined. Relevant data includes, but is not limited to:

1. codec,

2. stream information,

3. duration, and

4. bit rate.

J. If necessary, a file may be transcoded or converted to a universally playable file format.

K. The desired file will be opened in the applicable software program(s) chosen at the examiner’s discretion.

L. Using the selected devices and settings, review the submitted audio to locate the pertinent segment(s).

M. All derived files will utilize the case number and a numbering sequence to identify multiple captures or clips.
N. The video/image file will be processed as necessary to clarify detail as requested. Any processing steps used in the course of generating the final output video/image will be recorded, with appropriate values, in the examiner’s case notes and/or software-generated reports.

O. For audio clarification, the fewest number of steps as practical shall be used and the examiner shall only use techniques which are documented and can be reproduced.

P. Once enhanced, the final audio should be output to produce an enhanced copy of the original onto appropriate media.

Q. If video analysis is also requested, proceed to Forensic Video Analysis (DM-04-01) techniques and procedures

R. The file will be saved in the highest quality format to preserve the contents in the best available manner.

S. The final output and saved to appropriate media such as Evidence CD or DVD, USB flash drive or Hard Drive Disk. Regardless of the output media, the examiner must provide a product that accurately represents the audio content of the original evidence.

7 Interpretation

Compare the final copy with the original audio to confirm that enhancements have improved the audio in the areas of forensic interest as much as possible.

8 Precautions or Limitations

Enhancement capabilities are limited by variables including but not limited to the quality of the original recording, subject to recorder distance, wind, and interference.

9 Literature References and Supporting Documentation

Adobe Audition User Guide

iZotope User Guide

DM-04-03 FORENSIC IMAGE ANALYSIS

1 Scope

Image enhancement, clarification, filtration, and other image processing activities that are intended to improve the visual appearance of features in an image are considered examination tasks. Examination is the application of image science expertise to assist in the identification of information from images, the characterization of image features, and the interpretation of image structure. Various equipment and computerized hardware and software may be used. The appropriate forensic tools will be addressed on a case-by-case basis by the Digital/Multimedia section.

This document contains the procedures for the analysis of images in order to clarify or enhance some or all of the visual information contained within the submitted media.

2 Related Documents

Physical Evidence Examination (DM-02-01)
Acquisition of Digital Evidence (DM-03-01)
Forensic Video Analysis (DM-04-01)

3 Safety

Safety equipment includes the use of safety glasses, gloves, masks, clothing and antistatic mats as necessary. In some cases, use of fume hood or good ventilation as appropriate.

4 Equipment and Materials

- Forensic workstation
- Sterile digital media
- Forensic analysis software
- Write-blocking device
- Commercially available software
- Film scanner

5 Standards, Controls, and Calibration

None

6 Procedure

Note: Every case is unique and may require different steps in order to perform analysis. The following are guidelines only, and it is up to the individual analyst to decide which steps are required on a case-by-case basis.

A. Prior to Examination.

Consideration should be given to the following before commencing any examination of video evidence:

1. Examination Priority. Priority should be given to other forensic examinations (fingerprints analysis, trace evidence analysis, etc.) before any forensic video analysis proceeds. The minimum precautions must be identified and implemented.

2. Search Authorization. Proper search warrant or consent to search allowing examination of digital evidence should be verified prior to any forensic video analysis.
3. **Integrity of Evidence.** Video evidence submitted for forensic video analysis should first be reviewed for its integrity. Any deficiency (damage, write protections not in place, etc.) should be documented and resolved before any forensic video analysis proceeds.

4. **Protection of Evidence.** At all times, precautions should be taken to ensure video evidence is protected from external factors (magnetic fields, static electric charges, electrical hazards, etc.) that may cause damage to the media or to the recorded signal contained on the media.

B. All media will be physically examined prior to being inserted into or connected to any device.

C. The best results will be achieved when the media to be examined is the original recording. If it is apparent that the media is a photograph of a photograph, it will not be analyzed.

D. A working copy of the original file will be created and labeled in a manner to recognize such file as a working copy.
   1. All subsequent analysis will be conducted on the working copy.
   2. If all resources have been exhausted and analysis cannot continue with the working copy, analysis may continue from the original evidence with prior approval of the appropriate chain of command and the submitting officer.

E. To verify that the working copy is a true and accurate representation of the original evidence, a hash verification must be performed for digital evidence.

F. The desired image file will be opened in the applicable software program(s) chosen at the examiner’s discretion. The software (and its version) used to analyze the media will be documented.

G. Whenever possible, techniques that use either no data compression or visually lossless compression should be used.

H. All derived files will utilize the case number and a numbering sequence to identify multiple captures or images.

I. The image file will be processed as necessary to clarify detail as requested. Any processing steps used in the course of generating the final output image will be recorded, with appropriate values, in the examiner’s case notes and/or software-generated reports.

J. For image clarification, the fewest number of steps as practical shall be used and the examiner shall only use techniques which are documented and can be reproduced.

K. Once enhanced, the file(s) will be saved in a lossless or minimally compressed file format.

L. If an image is to be used for comparison, it must be calibrated 1:1. These images may be printed 1:1 for use by other analysts or investigators.

M. The final image(s) should be saved to appropriate media such as Evidence CD or DVD, USB flash drive or Hard Drive Disk. Regardless of the output media, the examiner must provide a product that accurately represents the visual content of the original evidence.

N. To verify that the derivative and archived evidence are true and accurate representations of the analyzed evidence, a hash verification must be performed for digital evidence.
7 Limitations

A. Examiners will not identify subjects, objects, or vehicles from surveillance images.

B. For a ruler or scale to be useful in an image, it must be photographed from approximately 90° to minimize distortion. If a great deal of distortion is present, then creating a life-size or 1:1 image is not possible.

8 Literature References and Supporting Documentation

Amped FIVE Training Material

LEVA Level I Training Material

LEVA Level II Training Material


05 INTERNAL DEPARTMENT PHOTOGRAPHIC SUPPORT

DM-05-01 PHOTOGRAPHIC OVERLAYS

1 Scope
Photographic overlays are used to assess the corresponding features from a known image to an unknown image for the purpose of rendering an opinion as to whether the subject or area of interest (AOI) is identical in both images, merely similar, or clearly different. Overlay material is transparent, as is the corresponding image so that if both images are life-size, alignment similarities and dissimilarities are clearly visible.

2 Related Documents
None

3 Safety
Standard laboratory safety precautions.

4 Equipment and Materials
None

5 Standards, Controls, and Calibration
None

6 Procedure
1. If the image is not in a digital format, convert it through the use of a film scanner, a flatbed scanner, or a digital camera.
2. Save the original file and work on a copy of the file.
3. Transform the copies to a similar size for comparison (1:1 if possible) and place them on separate layers in the same canvas using the Grid view for alignment if desired. The top layer will have a percentage of transparency to best view the alignment similarities with the image underneath.
4. Document (if appropriate) the similar or dissimilar alignment features in each image.
5. Save a copy of the new file containing both images. The file can be printed out at life-size (if scales were present) or not to assist the examiner with any forensic comparisons within their discipline.
6. The top layer is printed out on the transparency material at the desired transparency setting. The bottom layer is printed out normally on digital paper with no transparency.

7 Interpretation
A. Check the final printout with the measurement used to scale the image to make sure that it is in fact 1:1 or life-size (if appropriate).
B. If comparisons involve fingerprints, tire prints, shoeprints, jigsaw matches, DNA, tool marks, blood patterns, or any specialized areas within the Crime Lab, return the final image to that section for comparison.
8 Precautions or Limitations

A. Transparency material is currently available in 17” wide rolls, which should cover the width of common evidentiary items such as shoeprints, tire prints, and other impressionary evidence.

B. Angle of view is critical when working with overlays. If the angle of view is different in the AOIs, even if 1:1 scaling is achieved, the overlay probably won’t align to the corresponding area underneath.

C. For a ruler or scale to be useful in an image, it must be photographed from approximately 90° to minimize distortion.

D. If a great deal of distortion is present, then creating a life-size or 1:1 image is not possible.

9 Literature References and Supporting Documentation

Adobe Photoshop User’s Manual


DM-05-02 DIGITAL DISPLAYS FOR COURT

1 Scope
Small or large-format evidentiary displays in all forensic disciplines are included, either mounted or unmounted. Displays can be mounted on mat board or foam core, hinged or unhinged to fold for easier transport, have text, lines, arrows, highlighting, or other desired features added digitally. Features overlaid on top of evidence can have a specified degree of transparency.

2 Related Documents
None

3 Safety
Standard laboratory safety precautions.

4 Equipment and Materials
No reagents. Image requirements dictate the equipment and materials needed, which may include:
- Digital camera
- Scanner
- Forensic workstation
- Printer

5 Standards, Controls, and Calibration
None

6 Procedure
1. If the images are not in a digital format, convert them through the use of a film scanner, a flatbed scanner, or a digital camera.
2. Save the original files and work on copies of the files.
3. Transform the copies to a similar size for comparison and place them side-by-side on the same canvas using the Grid view for alignment if desired.
4. Add the requested digital enhancements.
5. Save a copy of the completed court display.
6. The Court display can be printed out at life-size (if scales were present) or greatly enlarged as requested by the analyst.
Examples:

7 Interpretation

N/A

8 Precautions or Limitations

Analysts should allow sufficient time for the creation of court displays prior to the case going to trial.

9 Literature References and Supporting Documentation

Adobe Photoshop User’s Manual


DM-05-03  SUSPECT LINEUP ELIMINATIONS OR ENHANCEMENTS

1 Scope

Many times investigating officers will have a picture of a suspect that they want to use in a lineup, but it contains other persons or things that need to be removed. In other instances, the officer may have obtained more current information on the suspect and want to reflect those changes in an image that is to be widely distributed.

2 Related Documents

None

3 Safety

Standard laboratory safety precautions.

4 Equipment and Materials

No reagents. Image requirements dictate the equipment and materials needed, which may include:

- Digital camera
- Scanner
- Forensic workstation

5 Procedure

1. If the images are not in a digital format, convert them through the use of a film scanner, a flatbed scanner, or a digital camera.
2. Save the original files and work on copies of the files.
3. Add the requested digital enhancements.
4. Save a copy of the enhanced suspect.

6 Interpretation

Any experienced examiner has the ability to determine whether the resulting image appears to be natural and unaltered so the final person reviewing the images does not know which images in the lineup have been altered.

7 Precautions or Limitations

As the Texas Department of Public Safety is the repository of photographs for Citizen of Texas Driver Licenses, this procedure is a service provided for investigative purposes in other areas of the department and is not tracked in LIMS or considered casework.

8 References

Adobe Photoshop User’s Manual


## 06 FORMS

### DIRECTORY OF FORMS

<table>
<thead>
<tr>
<th>Document Name</th>
<th>FRN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Digital Evidence Analysis Inventory</td>
<td>LAB-DM-01</td>
</tr>
<tr>
<td>2 Digital Media Inventory</td>
<td>LAB-DM-02</td>
</tr>
<tr>
<td>3 Bios and Written Files</td>
<td>LAB-DM-03</td>
</tr>
<tr>
<td>4 Chronology of Examination</td>
<td>LAB-DM-04</td>
</tr>
<tr>
<td>5 Keyword Search</td>
<td>LAB-DM-05</td>
</tr>
<tr>
<td>6 Enscripts and Software</td>
<td>LAB-DM-06</td>
</tr>
<tr>
<td>7 Analog Video Worksheet</td>
<td>LAB-DM-07</td>
</tr>
<tr>
<td>8 Digital Video Worksheet</td>
<td>LAB-DM-08</td>
</tr>
<tr>
<td>9 Audio Worksheet</td>
<td>LAB-DM-09</td>
</tr>
<tr>
<td>10 Mobile Device Worksheet</td>
<td>LAB-DM-10</td>
</tr>
<tr>
<td>11 CF/MF Technical Review Worksheet</td>
<td>LAB-DM-11</td>
</tr>
<tr>
<td>12 DM-AV Technical Review Worksheet</td>
<td>LAB-DM-12</td>
</tr>
<tr>
<td>13 Image Worksheet</td>
<td>LAB-DM-13</td>
</tr>
</tbody>
</table>