VIRGINIA DEPARTMENT OF FORENSIC SCIENCE

EVIDENCE HANDLING & LABORATORY CAPABILITIES GUIDE

DIGITAL & MULTIMEDIA EVIDENCE

Contact Information

If you have any questions concerning the Digital & Multimedia Evidence examination capabilities or evidence handling procedures, please call the Training Section or the Digital & Multimedia Evidence Section Supervisor listed below.

Please note that the Digital & Multimedia Evidence Section is located at the Central Laboratory in Richmond.

Section Contact	**Phone Number**
Jesse Lindmar	**(804) 588-4128**

OVERVIEW

The Virginia Department of Forensic Science's (DFS) Digital & Multimedia Evidence (DME) Section provides examination services that encompass the preservation, repair, acquisition, processing/identification, analysis/verification, clarification, and reporting of information stored in an analog or digital format. The section is divided into the sub-disciplines of Computer Device Analysis, Mobile Device Analysis, and Video & Image Analysis.

Additional information regarding DME services, capabilities and collection guidelines is available on the DME webpage:

https://www.dfs.virginia.gov/laboratory-forensic-services/digital-multimedia-evidence/

CAPABILITIES AND SERVICES

Due to the amount of time DME examinations may take, it is imperative that the evidence be submitted in a timely manner and with sufficient details relating to the request. Please advise DME of any scheduled court dates or continuances, and significant changes in the investigation that may affect DME's prioritization of the examination.

Computer and Mobile Device Analysis

Computer and Mobile Device Analysis involve the scientific examination of electronically stored information originating from a wide variety of devices. These devices include, but are not limited to, computer devices, such as servers (dedicated and cloud), desktops, laptops, game systems, magnetic card skimmers, and the "Internet of Things" (IoT); mobile devices, such as cellular telephones, tablets, and GPS navigation devices; and digital storage devices, such as hard disk drives, flash memory, and optical discs.

Analysis of these types of devices can result in the identification and recovery of a wide variety of information including, but not limited to:

- Existing and previously-existing (deleted) data
- Data decryption, and security measure (e.g., passcode, pattern lock) identification or circumvention
- Electronic communications such as email, chat, text/multimedia messages, call logs and contacts
- Multimedia files such as pictures, audio recordings and video recordings
- Documents and spreadsheets
- User activity or usage patterns, such as web-browser (Internet) activity, location information, device or application usage, file activity, timeline of events, as well as activity attribution

The DME section has the capability to acquire decrypted physical and logical data from a variety of devices. The available acquisition method is dependent on the make, model, functionality and security state of the device, which will also determine the ability to bypass any security measures that are in use. Furthermore, acquired data can be made available to other DME sub-disciplines for further analyses (e.g., video clarification) or returned as a result for the submitting agency to analyze themselves.

Video & Image Analysis

Video & Image Analysis involves the scientific examination of analog or digital video recordings, and print or digital still images. These recordings and still images can originate from a variety of devices including, but not limited to, cellular telephones, hand-held video cameras, body-worn cameras, security/surveillance systems, dashboard cameras, home videos or digital cameras.

Analysis of video recordings or still images can result in, but is not limited to:

- Existing and previously-existing (deleted) recordings and still images
- Confirmation of correct visual display (e.g., aspect ratio, playback speed, etc.)
- Clarification (enhancement) of specific details of a person or object

A variety of clarification techniques are available, including, but not limited to:

- Image deblurring
- Magnification (aka Zoom)
- Frame Averaging
- Reduction in playback speed
- Demultiplexing
- Redaction of sensitive information or material

COLLECTION GUIDELINES

Evidence descriptions should be listed on the Request for Laboratory Examination (RFLE). The Area of Interest (AOI) (i.e., requested information and/or time frame) being sought and any other additional information should be indicated on the DME Submission Supplement form.

ITEM – Computer or Digital Storage Devices

PROCESS – Evidence should be in a rigid container and should be protected from extreme temperature and strong magnetic sources. Only submit the items that you want analyzed.

Please include the following information on the DME Submission Supplement form:

- The area(s) of interest to be identified/recovered
- Any removable storage devices
- Any power cables/adapters/manuals
- Any required passcodes
    - Although the laboratory has the capability to bypass security measures on select devices, this does not always ensure access to the area(s) of interest
- Any damage present
- Any access to or modifications made
- Authorization to utilize potentially destructive processes

Providing this information will limit the amount of research an examiner has to conduct prior to beginning analysis.

Unless otherwise directed, a date/time filter may be applied to parsed data encompassing a time frame beginning (at most) six (6) months prior to the offense date listed on the RFLE, and ending with the most recent date/time of activity identified within the parsed data.

For cases in which the request is broad (e.g., all data on a device, all communications) the results identified from automated processes will be returned to the requesting submitter as soon as completed. No manual analyses will be performed. Additional information related to the request, that would require such manual analyses to produce a result, will be documented on the Certificate of Analysis. After a review of the automated results, if the submitting agency determines additional data is required, the agency may resubmit the original and/or derivative evidence ("evidence sources") for an expedited, supplemental examination.

The examination results and evidence sources, unless otherwise requested, will be provided via electronic file transfer and/or on digital storage media (e.g., optical disc, USB flash drive, hard disk drive).

ITEM – Mobile Devices

PROCESS – It is of the utmost importance to isolate the device from its associated communication networks, thus preventing the transmission and destruction of data on the device, as well as maintaining the device in its most vulnerable security state. This can be accomplished in one of the following ways:

- If the device is seized powered on:
  - Enable the device's "Airplane Mode" – a setting available on many mobile devices that suspends the device's signal transmitting/receiving functions
    - Disable any other communication settings (e.g., Wi-Fi, Bluetooth, etc.) that are not automatically disabled by enabling Airplane Mode
    - If present, remove the Universal Integrated Circuit Card (UICC) (aka Subscriber Identity Module [SIM] card) from a device that is powered on
  - Determine if any security measures (e.g., Secure Startup, PIN, password, pattern-lock, encryption) are enabled
    - Secured Apple and Android devices with an unknown passcode require specific handling in order to maximize the amount of data available for extraction and the speed of passcode identification. The following evidence handling guidelines should be followed:
      1. Ensure the device stays powered on and is sufficiently charged – DO NOT ALLOW THE DEVICE TO POWER OFF OR REBOOT

2. Shield the device from communication networks by putting the device into Airplane Mode, removing its UICC, and/or placing it in a shielded enclosure
3. Submit the device to the Central laboratory as soon as possible

- For non-Apple and non-Android devices, power down the device via its interface or by long-pressing its power button and, if applicable, remove its battery; see *Figure 1*
  - Depending on enabled security measures, this process may prevent future access to the device

Figure 1 – Battery Removal

- If the device is seized powered off:
  - If applicable, remove its battery and UICC
- For applicable mobile devices, it is important to determine if the device (handset) contains a UICC or flash memory card such as a micro Secure Digital (microSD) card
  - Either card can be located internally, typically under the battery, or externally along the side of the device; *Figures 2* and *3* show example locations
  - These storage devices should be indicated on the RFLE as additional items of evidence, typically as sub-items to the handset

Figure 2 – UICC

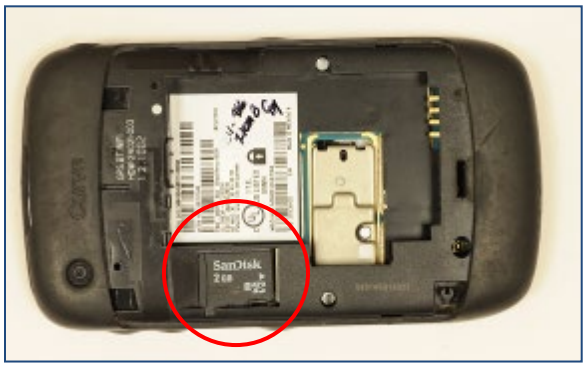

Figure 3 – MicroSD Card

  - Also, if the device is reliant on a UICC to authenticate the device to a service provider's network(s), removal may be an additional shielding measure
- Package the item at the time of seizure to provide a multi-layer approach for static dissipation and effective shielding

  DFS recommends mobile devices be packaged at the time of seizure and prior to lab submission as follows:

  1. Place in an anti-static container (e.g., paper envelope)
  2. Place in a >3 mil thick shielded enclosure (e.g., "Faraday" bag; see *Figure 4*) or wrap in aluminum foil (5 times with heavy duty or 10 times with standard thickness)

Figure 4 – Faraday Bag

   a. This step can be skipped if the device's battery has been removed, or Airplane Mode has been enabled (confirming cellular/data and Wi-Fi are disabled) and/or the UICC removed

3. Place in an outer storage bag (container) and seal
   a. If applicable, label that the battery has been removed, or that Airplane Mode has been enabled (confirming cellular/data and Wi-Fi are disabled) and/or the UICC removed

Packaging kits may be available from a third party vendor for purchase

Please include the following information on the DME Submission Supplement form:

- The area(s) of interest to be identified/recovered
- Any removable storage devices
- Any power cables/adapters
- Any required passcodes
  - Although the laboratory has the capability to bypass security measures on select devices, this does not always ensure access to the device
- Any damage present
- Any access to or modifications made
- Authorization to utilize potentially destructive processes (e.g., advanced automated data acquisition equipment, "chip-off", etc.)

Providing this information will limit the amount of research an examiner has to conduct prior to beginning analysis.

Unless otherwise directed, a date/time filter may be applied to parsed data encompassing a time frame beginning (at most) six (6) months prior to the offense date listed on the RFLE, and ending with the most recent date/time of activity identified within the parsed data.

For cases in which the request is broad (e.g., all data on a device, all communications) the results identified from automated processes will be returned to the requesting submitter as soon as completed. No manual analyses will be performed. Additional information related to the request, that would require such manual analyses to produce a result, will be documented on the Certificate of Analysis. After a review of the automated results, if the submitting agency determines additional data is required, the agency may resubmit the original and/or derivative evidence ("evidence sources") for an expedited, supplemental examination.

The results, unless otherwise requested, will be provided via electronic file transfer and/or on digital storage media (e.g., optical disc, USB flash drive, hard disk drive).

ITEM – Video and Image Analysis

PROCESS – When possible, submitted recordings/images should be the **ORIGINAL** recording/image.

For digital recordings, submit the recording device containing the original recording, or the exported recording in its original (native) file format with, if available, its proprietary player and the exported recording in an open file format, such as an *AVI*.

DFS can only analyze recordings stored on local devices or copies of acquired recordings on storage devices that are submitted to the Department. For recordings stored on a separate offsite backup network or cloud storage location, consultation with your legal counsel will be necessary to determine the appropriate course of action.

Provide a copy of the acquired recording on a storage device (e.g., optical disc, USB flash drive); optical disc (e.g., CD, DVD, BD) is preferable.

For analog recording submissions, it is imperative that the videocassette **NOT** be repeatedly played back or left on "pause", as severe irreversible damage can occur. However, prior to submission, the recording may be queued to a timeframe immediately preceding the area in interest. Additionally, the write-protect mechanism should be enabled (e.g., removed, opened) in order to prevent the operation of the recording function. *Figures 5* and *6* show example mechanisms.

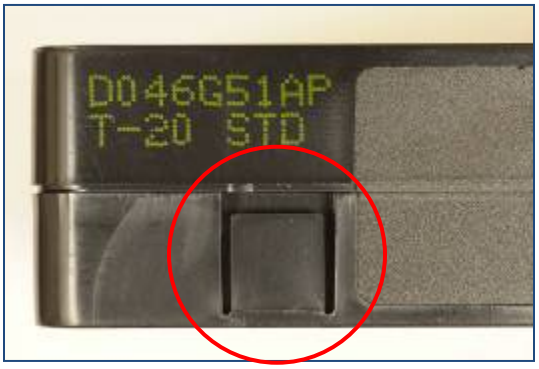

Figure 5 – Write-Protect Tab

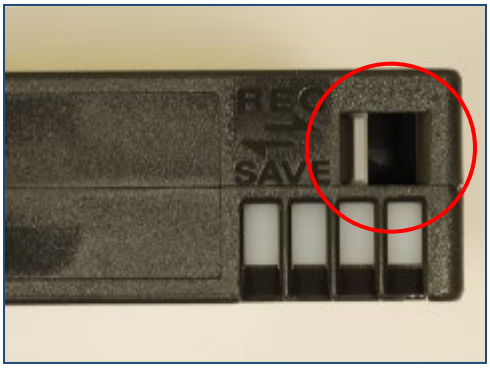

Figure 6 – Write-Protect Sliding Tab

Evidence should be packaged in a rigid container and should be protected from extreme temperature and strong magnetic sources.

Please include the following information on the DME Submission Supplement form:

- If submitting a recording:
  - The area(s) of interest to be identified, recovered, and/or clarified
    - If the camera system is utilizing Infrared Radiation (IR), light and dark, and patterns and prints may appear differently than they would under normal camera operation
  - The make and model of the recording device that made the recording
    - System settings and parameters (e.g., frame rate, resolution, image quality, network connectivity)
    - Displayed system date/time vs. current date/time
  - The format (e.g., native, open) of the recording
  - Include any specific player and/or codec required to play the recording
- If submitting a recording device:
  - The area(s) of interest to be identified, recovered, and/or clarified
  - Any removable storage devices
  - Any power cables/adapters/manuals

- Any required passcodes
  - Although the laboratory has the capability to bypass security measures on select devices, this does not always ensure access to the data
- Any damage or biohazards present
- Any access to or modifications made
- Authorization to utilize potentially destructive processes

If clarification is not required on the entire recording, the particular area of interest to be clarified should be specifically indicated. This can be done by providing the approximate time that the activity begins and ends and/or a brief description of the activity occurring within the area of interest. Providing this information will limit the amount of research an examiner has to conduct prior to beginning analysis.

The results, unless otherwise requested, will be provided via electronic file transfer and/or on digital storage media (e.g., optical disc, USB flash drive, hard disk drive).