# 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** |

# DIGITAL & MULTIMEDIA EVIDENCE SECTION

## OVERVIEW

The Virginia Department of Forensic Science's (DFS) Digital & Multimedia Evidence (DME) Section encompasses the preservation, processing and analysis of evidence in an analog or digital format. The section is divided into the sub-disciplines of Computer Analysis (including Mobile Device Analysis) and Video Analysis (including Image Analysis).

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

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

## CAPABILITIES AND SERVICES

Due to the amount of time these types of examinations can require to complete, it is essential that evidence be submitted in a timely manner. Please allow for adequate lead and completion times.

### Computer and Mobile Device Analysis

Computer and Mobile Device Analysis involves the scientific examination, repair (if required), analysis and/or evaluation of electronically stored information contained on a wide variety of electronic devices. These devices include, but are not limited to: computer systems, such as servers, desktops, digital/network video recorders (D/NVR), and laptops; mobile devices, such as cellular telephones and tablets; and digital storage devices, such as hard disk drives, solid-state drives, flash memory, and optical discs.

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

- Existing and previously-existing (deleted) data
  - Electronic communications, such as email, chat, and text / multimedia messages
  - User activity or usage patterns, such as web-browser (Internet) activity, call logs, and application usage/activity
  - Multimedia files, such as pictures, audio and video recordings

The DME section has the capability to acquire logical and physical data from a variety of devices. The available acquisition type is dependent on the make, model, and functional 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).

### Video and Image Analysis

Video and Image Analysis involves the scientific examination, repair (if required) and clarification of analog or digital video recordings, or still images for the purpose of improving

the visual appearance of specific features within the video recording or image or the overall recording or image. These can originate from a variety of devices including, but not limited to: mobile devices, video cameras, and DVRs and NVRs; and their clarification can lead to the identification of persons of interest or other pertinent information, such as a timeline of events.

Especially in the case of analog recordings, it is imperative that the media **NOT** be repeatedly accessed or played back and that it be submitted as soon as possible for analysis – severe damage or loss of data can occur that may be irreversible. However, prior to submission, the recording should be queued to a timeframe immediately preceding the area in interest.

## COLLECTION GUIDELINES

**The packaging container used to submit items of evidence should be large enough to accommodate the return of derivative evidence sources and examination results media, such as print, flash memory, hard-disk drive or optical disc (e.g., CD, DVD, Blu-Ray Disc).**

Evidence descriptions should be listed on the Request for Laboratory Examination (RFLE) form. The requested information being sought (i.e., Area of Interest [AoI]) and any other additional information should be indicated on the DME Submission Supplement form available on the DME webpage:

http://www.dfs.virginia.gov/wp-content/uploads/2015/07/242-F108-DME-Submission-Supplement.pdf

**ITEM** – Computer or Digital Storage Devices

**METHOD** – Evidence should be in a rigid container and should be protected from extreme temperature and strong magnetic sources. Do not apply adhesive labels to optical media. Only submit the items that you want analyzed.

Please include the following:

- The area(s) of interest to be identified / recovered
- Any power cables / adapters
- Any required passwords
  - 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

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

The results, unless otherwise requested, will be provided on digital storage media.

**ITEM** – Mobile Devices

**METHOD** – 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. This can be accomplished in one of the following ways:

- Enable the device's "Airplane Mode" – a setting available on many mobile devices that suspends the device's signal transmitting/receiving functions
- Determine if any security measures (e.g. PIN, password, pattern-lock, encryption) are enabled
- Power down the device via its interface and, if applicable, remove the battery; see *Figure 1*
  - Depending on enabled security measures, this process may prevent future access to the device
- For applicable mobile devices, it is important to determine if the device (handset) contains a Universal Integrated Circuit Card (UICC) (aka Subscriber Identity Module [SIM] card) 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 1**


**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 bag (e.g. paper envelope)
2. Wrap in aluminum foil (5 times with heavy duty or 10 times with standard thickness)
    a. This step can be skipped if the device's battery has been removed or “Airplane Mode” has been enabled
3. Place in a >3 mil thick shielded enclosure (e.g., "Faraday" bag; see *Figure 4*)
    a. This step can be skipped if the device's battery has been removed or “Airplane Mode” has been enabled
4. Place in an outer storage bag (container) and seal
    a. If applicable, label that the battery has been removed or “Airplane Mode” has been enabled

**Figure 4**

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

For submitted mobile devices, please include the following:

- The area(s) of interest to be identified / recovered
- Any power cables / adapters
- Any required passwords
    - 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

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

The results, unless otherwise requested, will be provided on digital storage media.

**ITEM** – Video and Image Analysis

**METHOD** – 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. If time permits, also export the recording into an open file format, such as an *AVI*.

For analog recordings, 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 locations.


**Figure 5**

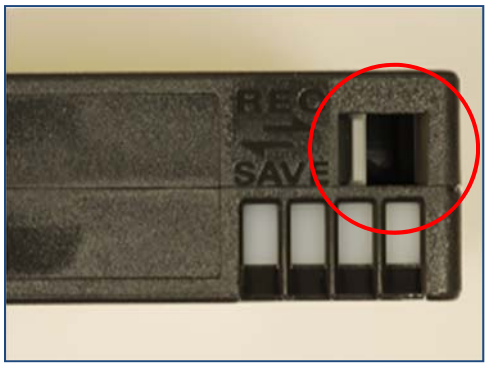


**Figure 6**

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

Please include the following:

- The area(s) of interest to be clarified
- Any power cables /adapters /manuals
- Any required passwords
- Any damage present
- 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 date/time and current date/time
- The format (e.g., native, open) of the recording
- Any specific player and/or codec required to play the recording

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 a brief description of the activity occurring within the area of interest and the approximate time that the activity begins and ends.

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

The results, unless otherwise requested, will be provided on digital storage media.