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 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 Forensics (including Mobile Device Analysis) and Video 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 Forensics and Mobile Device Analysis

Computer Forensics involves the scientific examination, repair (if required), analysis and/or evaluation of electronically stored information contained on a wide variety of data storage devices. These devices include, but are not limited to: computer systems, such as servers, desktops, digital video recorders (DVR), and laptops; mobile devices, such as cellular telephones and tablets; 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) files, records and fragmented 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

The DME section has the capability to acquire logical and physical data from a variety of mobile and digital storage devices. For mobile devices, the available acquisition type is dependent on the make and model 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 Analysis

Forensic Video Analysis involves the scientific examination, repair (if required) and clarification of analog or digital video recordings for the purpose of improving the visual appearance of specific features within the video recording or the overall recording. These recordings can originate from a variety of recording devices including, but not limited to: mobile devices, video cameras and surveillance systems. The clarification of

video recordings 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 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 or may not be reversible.

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). 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. Packing boxes are available from evidence receiving in each laboratory. Only submit the items that you want analyzed.

For submitted computer systems, 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 passwords 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 time an examiner has to conduct research prior to 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:

- Power down the device via its interface and remove the battery; see *Figure 1*. If unable to do either, enable the device's "Airplane Mode" – a setting available on many mobile devices that suspends the device's signal transmitting/receiving functions.

Figure 1

- For applicable mobile devices, it is important to determine if the device (handset) contains a 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 2 – SIM Card

Figure 3 – MicroSD Card

  - Also, if the device is reliant on a SIM card 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

The Virginia Department of Forensic Science recommends mobile devices be packaged at the time of seizure and prior to lab submission as follows:

1. Place in an anti-static bag
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

Figure 4

4. Place in an outer storage bag (container) and seal

Packaging kits may be available from a third party vendor for purchase. For ease, the mobile device may be packaged in an appropriately sized kit at the time of seizure and prior to lab submission.

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 passwords on select devices, this does not always ensure access to the device

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

ITEM – Video Analysis

METHOD – When possible, submitted recordings should be the **ORGINAL** recording.

For digital recordings, submit the recording device containing the recording or the exported recording in the original (native) file format or, if available, an uncompressed and/or lossless file format. If the make and model of the recording device is known, contact the DME section for possible guidance on the best format to submit.

For analog recordings, the write-protect mechanism should be enabled (e.g., removed, moved) in order to prevent the operation of the recording function; *Figures 5* and *6* show example locations.

Figure 5

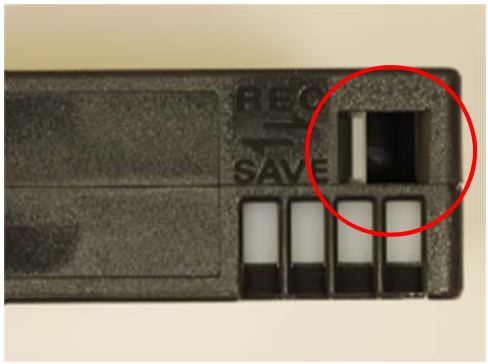

Figure 6

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

For submitted video recordings, 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
- The format (e.g., RAW, native, universal [.avi]) of the recording
- Any specific player 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 area of interest's dialog and the approximate time that the conversation begins and ends.

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

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