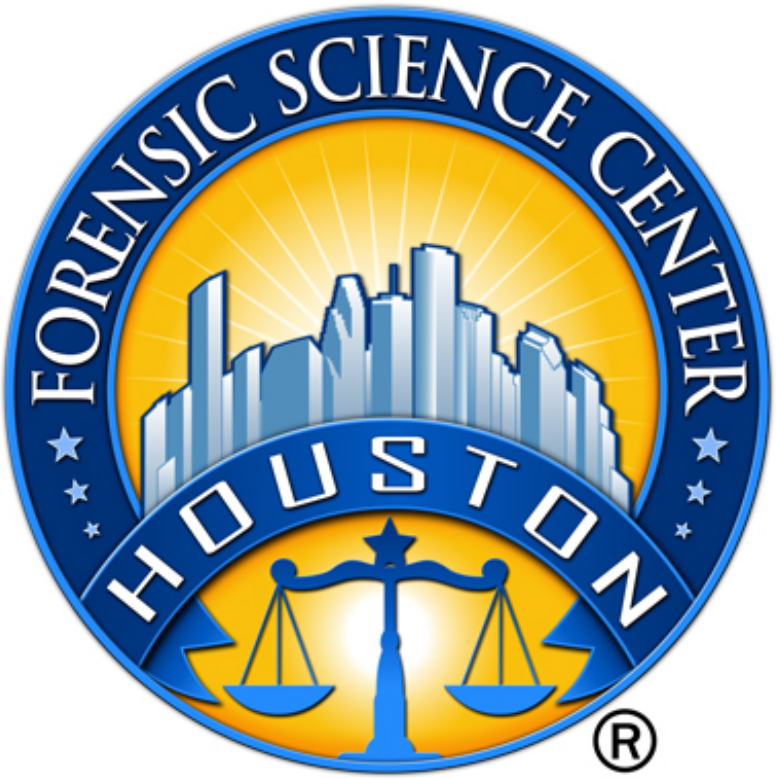

Multimedia Section
Administrative/Quality

Digital and Multimedia Evidence Division

1. Administrative/Quality

1.1. Overview

1.1.1. The Multimedia Section is responsible for the analysis of audio/video and digital evidence. The analysts are responsible for extracting, analyzing, and/or enhancing the evidence once formal requests are made by laboratory customers. Analysts may be required to testify in local, state, and federal courts concerning the procedures followed to extract, preserve, analyze, duplicate, enhance, and repair multimedia evidence.

1.2. Limitations

1.2.1. It is widely acknowledged in the forensic multimedia scientific communities that data storage and systems used to create, store, and manage data varies. Variables include types of hardware, software, software versions, and sometimes alternate use of hardware and software from its original intent. Analysts apply their education, training, skills, knowledge, abilities, and experience to formulate a plan to analyze data and media by employing the most thorough and accurate methods defined by the section's standard operating procedures (SOPs); and use the best applicable scientific practices of the digital and multimedia evidence discipline.

1.3. Safety

1.3.1. Analysts must be aware of their personal safety when handling biohazard evidence and when called to a scene. If an analyst suspects a biohazard is present on media or other devices at a scene or in the laboratory, measures will be taken to ensure their personal safety, such as wearing personal protective equipment like gloves, masks, etc.

1.3.2. Gloves must be worn when handling any item that is thought to contain a biohazard. If media or other devices contain a biohazard, proper PPE shall be worn and the HFSC Health and Safety Manual will be followed.

1.3.2.1 Gloves should be worn when opening submitted items in case of a biohazard. Once the item has been sanitized or no biohazard is observed, gloves can be removed for examination.

1.3.3. Analysts should be aware that electronic devices are powered by electricity and measures should be taken to avoid shock.

1.3.4. If disassembly of a device is required during analysis, analysts will be cautious of sharp edges.

1.3.5. Injuries should be reported to a supervisor/lead or manager immediately to receive appropriate medical attention.

1.4. Security

1.4.1. The Multimedia Section's general work area is secured by locked doors controlled with key card access. Assigned evidence is stored at the analyst's desk, in a designated work area, or in the evidence storage room (DME Vault), all of which is inside the secured section general work area.

1.4.2. Evidence in the process of examination is stored at the analyst's desk or a designated work area. At no time will evidence be left in an unsecured or uncontrolled work area. If an analyst leaves for an extended period of time (greater than five minutes), they must make sure that the evidence is secured in a work area or in the presence of section personnel.

1.4.3. Upon completion of analysis and/or reviews, evidence items will be packaged, sealed, and stored in the DME Vault until the evidence and derivatives are returned to the customer.

1.5. Equipment/Maintenance

1.5.1. Equipment must be maintained to ensure proper performance. Only suitable and properly operating equipment shall be used for casework. Equipment not functioning properly will be labeled and taken out of service.

1.5.2. Equipment not frequently used will be performance checked prior to use on casework. Infrequently used equipment will be labeled as out of service equipment until used. Performance checks are documented in Qualtrax.

1.5.3. The section maintains an inventory list of laboratory equipment and software (including number of licenses and version numbers) internally.

1.5.4. Analog equipment is performance checked prior to use and noted in the case record.

1.5.5. Digital cameras are used for documentation purposes only and are not performance checked but are cleaned as needed.

1.5.6. Forensic software that is infrequently used will be performance checked prior to use if the software is not used in a given year. Infrequently used software is identified by the section supervisor/lead or manager and is listed on the Infrequently Used Software list. The frequency of the use of software is determined based on technical review data and by staff feedback. Performance checks will be documented in the case record.

1.5.6.1. If a software on the list is performance checked, then it will be taken off the list until not in use again.

1.6. Integrity Verification

1.6.1. Digital and multimedia evidence submitted for examination **must** be maintained in such a way that the integrity of the data is preserved and proven to be 'reliable' for court testimony.

1.6.2. Integrity verification can be accomplished digitally (i.e. hashing) and/or visually as to content and quality.

1.6.3. Write-blockers can also be used for evidence such as USB drives, hard drives, etc. to prevent modification (addition, deletion, or alteration) of media content.

1.6.4. If the submitted media has a mechanism designed to preserve the recording (safety-record tabs, jumper, software setting, etc.), document its state upon receipt. If not already engaged, activate the mechanism and document that fact. If there is a clear reason not to engage the write protection (e.g., to preserve fingerprints), document that it was not engaged and the reason.

1.7. Evidence Handling

1.7.1. **Submission of Items for Examination:**

1.7.1.1. The analyst, in conjunction with the requestor/submitter, will ensure that the most appropriate format of the evidence is submitted.
1.7.1.1.1. For DFL requests in LIMS, section personnel must confirm search authority for the device to be examined, when not explicitly stated in the request, by confirming with the requestor/submitter via phone or email and document this communication in the case record. When the search warrant is provided as an item of evidence, the analyst shall review the search authority listed to ensure relevance and document this review in the case record.
1.7.1.1.2. If the requestor/submitter does not respond to communication regarding the necessary search authority within 5 business days then that request will be closed, and the requestor/submitter will be notified via email. No report will be issued.
1.7.1.2. Evidence to be analyzed by the section will be directly delivered to the section by the Client Services & Case Management team. In expeditious circumstances, evidence can be delivered in-person by the customer after being tagged in the HPD property room, if possible.
1.7.1.3. All submitted evidence must have a LIMS record. A unique forensic case number will be automatically assigned by LIMS when the case is created.
1.7.1.4. Submitted items should be photographed/scanned prior to examination. In the event damage is identified/discovered by the analyst, photographs/scans must be taken of the specific damage and documented in the case record.
1.7.1.5. Any derivative/child item(s) and/or the proximal container must be labeled with the forensic case number, item number, and analyst initials. If the item is too small then it must be marked with the analyst's initials, if possible, and/or the proximal container will be labeled.
1.7.1.6. Peripheral equipment that does not store data (i.e. monitors, VCRs, audio players) will not be examined unless those items are unique and are required to facilitate the examination.
1.7.1.7. Evidence that is not in an analyst's custody must be secured in the DME Vault or a designated work area. Be sure that internal transfers are reflected in LIMS.
1.7.1.7.1. All evidence in the DME Vault must be packaged and sealed in accordance with the HFSC Quality Manual. Analysts must date and initial all seals placed by the analyst. It is recommended that the date and initials appear between the actual seals and containers (i.e. bag or wrapping). The forensic case number and item number will be labeled on the packaging or other label (i.e. HPD property room tag).
1.7.1.7.2. For evidence submitted from the property room, the forensic case number will be written, or a barcode affixed to the packaging. Seals will remain as submitted from the property room unless the seal is broken or damaged.
1.7.1.7.3. DVRs, computers, monitors, or any other larger item(s) will be delivered to the DME Vault as is from the property room. The condition of the item will be documented in the test report. Analysts will provide a seal

over the power source (or somewhere comparable) upon return to the property room.

1.7.1.8. Evidence does not need to be sealed while it is in the analyst's custody or in a designated work area.

1.7.1.8.1. If an analyst does not work on a case for an extended period of time (over 30 days), the evidence must be secured in the DME Vault until analysis can be completed. Evidence items running the brute force client are considered actively being worked on.

1.7.1.8.2. Evidence items that are running the brute force client in an attempt to obtain the passcode can be stored in a designated work area. The evidence will stay in the designated work area until a passcode is obtained, or the evidence is requested to be returned. Items will be labeled with the FCN, item number, and analyst initials.

1.7.1.9. If a case is received where a biohazard is suspected, the appropriate safety precautions must be followed. See the Houston Forensic Science Center (HFSC) Health and Safety Manual for more detailed information.

1.7.1.10. Direct media duplication is not treated or documented as a forensic process and may not be in LIMS. Direct copies will be labeled as such when stored in the DME Vault awaiting pickup.

1.7.1.11. In instances where a video is requested to be transferred from a cell phone (in the presence of the submitting agency), the transfer process will be documented in the case record. No forensic software is used in this process. The resulting CD/DVD will be documented in LIMS and case notes. If the cell phone needs to be submitted, a DFL request will be made in LIMS.

1.7.1.12. Archive items (i.e. laboratory copies) will be stored on the Archive shelf in the evidence storage room and are not treated as evidentiary items.

1.7.1.13. In some instances, a link provided via email is the only way to access the evidence that is requested. No management approval is needed in these circumstances.

1.7.1.13.1. The evidence that is downloaded/extracted from the link will be put onto a medium (i.e. USB, DVD, etc.) and that will become the item of evidence entered into LIMS. The download/extraction will be documented in the case record along with documentation of the link provided.

1.7.2. **Scene Response:**

1.7.2.1. Multimedia Section analysts respond to scenes to retrieve video for customers (refer to Scene Response SOP for procedures at scenes). These are commonly referred to as call outs.

1.7.2.2. A request form will be filled out for every scene that an analyst responds to. If one request form is used for multiple locations, then that form must be scanned/uploaded into each LIMS assignment. This does not apply to search warrant previews or other on-site forensic previews.

1.7.2.3. If video is retrieved from the scene, the files will be put onto a disc or USB drive and given to the investigator/requesting agency at the scene and documentation

of this will be in the case record. This will be the original evidence and will be retained by the requesting agency.

1.7.2.3.1. If additional analysis is requested, the requesting agency will need to submit the original evidence to the HPD property room and make a request using HFSC's portal. In expeditious circumstances, evidence can be delivered in-person by the customer after being tagged in the HPD property room, if possible.

1.7.2.3.2. If video is retrieved at the scene by someone other than the analyst, the analyst will document in the case record who exported the video and the video will be given to the requesting agency at the scene.

1.7.2.3.3. It is the Multimedia Section's policy that derivative evidence will not be retained by the analyst. If evidence does need to be retained, the analyst must obtain prior written approval from the section supervisor/lead or manager.

1.7.2.4. If no video is retrieved at the scene, a request form will still be filled out and a report will be issued.

1.7.3. **Returning Evidence:**

1.7.3.1. Upon completion of casework (including technical and administrative reviews), evidence must be packaged and/or sealed properly.

1.7.3.2. Outer evidence containers will be sealed, and the seal properly labeled with the analyst's initials and date before being returned.

1.7.3.3. The originally submitted item(s) along with hardcopies, CD's, DVD's, USBs, and other items produced at the request of the submitter will be kept in the DME Vault until released to an authorized individual or storage location.

1.8. Documentation

1.8.1. The analyst will document observations while performing casework with handwritten or typed notes. The case record must contain a thorough description of submitted items, notation of any repairs made, analyst's notes/observations, photographs, and hardware and software used for casework (to include version number of software). The case record/file is stored electronically in LIMS.

1.8.1.1. If observations are documented electronically, then those original observations in their entirety are copied and pasted directly into LIMS and will serve as the report. If any corrections or edits are made, then that original report is saved prior to editing and attached to the case record.

1.8.1.2. When a case record is printed, all documentation must be marked with the analyst's initials, forensic case number, and page number.

1.8.1.3. Case records can also be maintained on an archive disc that is retained in the section, if needed.

1.8.1.4. Discrepancies with the submission information must be documented in the case record.

1.8.2. Technical note taking must be kept throughout the examination process to document how items were handled, procedures taken to extract evidence, and methods performed in order to achieve results. These are considered the analyst's original observations.

1.8.2.1. The notes must be detailed enough to allow a comparably trained analyst to repeat the process and arrive at the same result.

1.8.3. The analyst is responsible for writing a report that provides the reader with all the relevant information in a clear and concise manner.

1.8.4. If a case requires a deviation from normal operating procedures, the proposed deviation must be presented in detail to the section supervisor/lead, section manager, or division director. The section supervisor/lead, section manager, or division director will approve or disapprove the proposed deviation. The deviation and the approval must be documented in the case record (refer to HFSC's Quality Manual section 7.2.1.7).

1.8.5. It is sometimes necessary to modify a report after it has been issued. This may be necessary to correct an error in the report, to document additional analysis conducted, or for various other reasons.

1.8.5.1. If it becomes necessary to amend a signed report, the new report will be identified as amended and will contain a reference to the original report that it is replacing. The amended report must state why the amended report was issued. The original report must be maintained within the case record.

1.8.6. The analyst must ensure that all communications (telephonically, email, text, etc.) with investigators/attorneys are documented in LIMS (i.e. in case notes or the "Comm Log" section in LIMS).

1.9. Technical and Administrative Reviews

1.9.1. All case records (including derivatives) will be technically reviewed by an analyst authorized to perform technical reviews and who is not the author of the report. This review will be documented in LIMS.

1.9.2. All case files will be administratively reviewed by an individual other than the author of the report and the technical reviewer prior to the issuance of the final report. This review will be documented in LIMS.

1.9.2.1. For call out/scene response requests, the technical and administrative review can be completed by the same analyst but not the analyst who responded to the call out.

1.9.3. In the event derivative data (an "investigative copy") needs to be released to the customer because of expeditious circumstances, the analyst must inform the customer that a report cannot be issued until administrative and technical reviews are completed.

1.9.4. If there are conflicts during a technical review where the case analyst and the technical reviewer cannot agree on the way a case was handled or how a case is being reported, the conflict shall be brought to the section supervisor/lead, section manager, or division director for a determination/resolution. These types of conflicts must be tracked by the section supervisor/lead or manager in efforts to monitor trends and ensure quality.

1.10. Data Storage and Retention Policy

1.10.1. All work product (including any intermediary files) that will be reviewed by the technical reviewer can be stored on the section's designated server.

1.10.2. Once both the technical and administrative reviews have been completed, the case files on the server may be deleted.

1.10.2.1. Files will be deleted from the server after approximately 30 days unless approved for a longer duration by the section supervisor/lead or manager.

1.10.2.2. All original photographs taken of evidence items will be permanently stored on the server in a designated area and organized under the FCN or ACN. These will not be deleted.

1.10.3. There will be instances where the work product cannot be stored on the server for review:

1.10.3.1. Size of the data is too large to be stored (i.e., DVR dumps).

1.10.3.2. No analysis could be done.

1.10.3.3. Technical difficulties with the network and/or server (this can include server failure).

1.10.4. All derivative evidence created by an analyst will have an assigned item number in LIMS and will be properly packaged and sealed.

1.10.4.1. These derivative items will be returned to the submitting agency. Both the original and derivative evidence will be retained by the submitting agency.