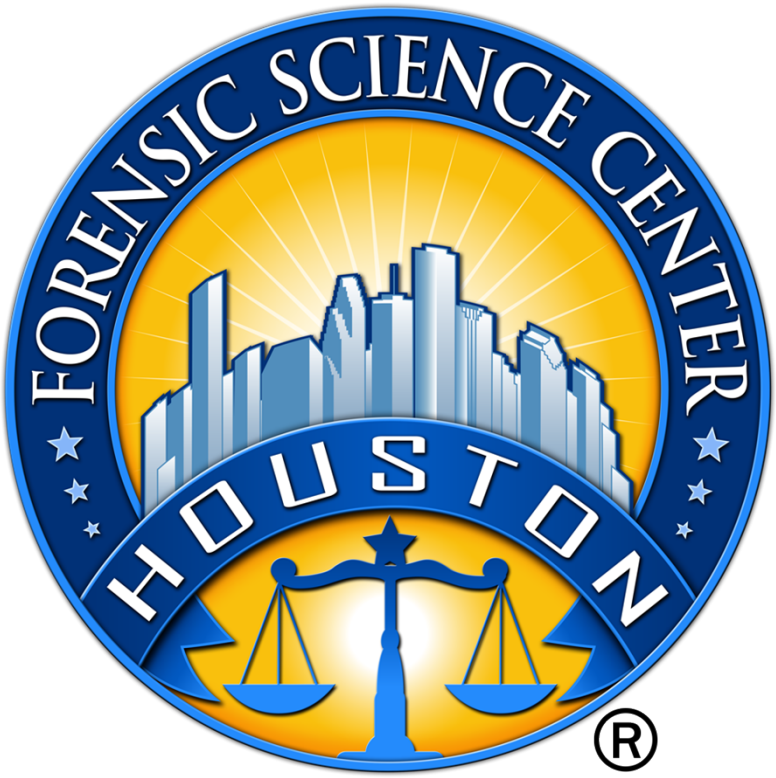

Digital Forensics
Evidence Handling

Crime Scene/Digital and Multimedia Division

2. Digital Forensic Laboratory Evidence Handling

2.1. Purpose

To establish guidelines for the receipt, tracking, protection, marking, handling, and return of evidence in the Digital Forensic Laboratory.

2.2. Scope

This procedure applies to all Digital Forensic Laboratory employees and administrative personnel who receive, handle, or process evidence.

2.3. Submission of Evidence

2.3.1. Examination requests are most commonly submitted via the Laboratory Information Management System (LIMS) for HPD-controlled evidence. HPD stakeholders, in consultation with the DFL, may also submit their evidence directly to the lab for examination. For non-HPD stakeholders, evidence is submitted via the HFSC Client Services/Case Management Division (CS/CM) utilizing their evidence submission guidelines.

2.3.2. Evidence is generally couriered by HFSC personnel to the DFL from the HPD Property Division, or from CS/CM.

2.3.3. At the DFL, submitted items shall be visually examined for damage prior to analysis at the time the evidence is unpackaged. Evidence should be photographed prior to examination and notations of damage recorded in the case record.

2.3.4. Peripheral equipment not designed to store digital data (e.g. monitors and keyboards) will not be accepted unless those items are unique and are required to facilitate the examination.

2.3.5. Receipt of evidence from the customer will be documented at the time of transfer either electronically or on paper as part of the chain of custody.

2.3.6. Digital Forensic Laboratory personnel receiving evidence shall ensure the items are properly labeled and sealed.

2.3.6.1. If an existing seal is observed to be broken at the time of submission, the item should be rejected.

2.3.7. DFL personnel shall confirm search authority for the device to be examined, when not explicitly stated in the request, by confirming with the requestor or a representative via phone or email communication and document this communication in the case record. When the search warrant is provided as an item of evidence, the examiner shall review the search authority listed to ensure relevance and document this review in the case record.

2.4. Receiving Evidence

2.4.1. It is the responsibility of the examiner to maintain the integrity of the evidence at all times while in his/her custody. Evidence must be protected from loss, cross-transfer, contamination and/or deleterious change.

2.4.2. Evidence shall be sealed properly. Examiners will check the evidence container to ensure that proper seal(s) are in place whenever evidence is received. A proper seal is one in which there is no possibility that the contents of a container can be removed, altered or a substitution made without the seal being obviously disturbed.

2.4.2.1. NOTE: Some items of evidence may be too large to seal inside a container. However, every effort will be made to secure and store the item with its appropriate identifiers to ensure items are not confused with submitted evidence from other cases. For example, computers, at a minimum, should have evidence tape applied to the cover opening of the computer chassis. The intake technician should apply his or her initials and date of receipt on the evidence tape.

2.4.3. Receipt of evidence will be documented at the time of transfer electronically or on paper as part of the chain of custody.

2.4.4. Cases that contain items that could represent a possible biohazard require special handling. While working with possible biohazards, proper precautions, such as wearing gloves and cleaning with a diluted bleach solution may be needed. Contaminated items shall be sanitized as best as is practical and labeled to the effect that a potential biohazard may exist prior to placing into the evidence vault if received in an unsealed container. Likewise, contaminated items should be sanitized prior to being introduced into the examiners workstation area.

2.4.5. Evidence items contained within a case will be labeled. This also includes media device(s) containing the extracted data from the original physical evidence or digital evidence data source (e.g. evidence CD/DVD created for the customer).

2.4.5.1. Some items of evidence may be too small to be marked or labeled with unique identifiers directly on the item. If so, it shall be marked on its proximal container.

2.4.5.2. For groups of like evidence such as CD's/DVDs, the groups of items may be labeled with one unique identifier as long as the items of evidence are securely packaged and sealed together.

2.5. Evidence Security

The Digital Forensic Laboratory personnel will ensure that evidence integrity is not compromised. Access to evidence within the Digital Forensic Laboratory is controlled. The Digital Forensic Laboratory operational area is controlled with restricted access. Access to the restricted area is only available through key cards issued by HFSC. Visitors will be escorted into the evidence facility only by a member

of the Digital Forensic Laboratory or administrative staff with proper keycard access. Access controls allow examiners to process and examine evidence while maintaining the integrity of the evidence.

Most digital evidence examinations can be conducted at the examiner's desk. Any area where there is evidence being actively worked or where evidence is kept to permit ready access for examination is considered to be an operational area. The short term evidence storage room and the server room are located in, and considered an operational area.

2.6. Return of Evidence to the Customer

2.6.1. All items and sub-items within a case will be packaged to protect from loss, cross-transfer, and/or deleterious change. Whenever possible, evidence will be packaged in the same condition and/or containers as it was received.

2.6.2. Outer evidence containers will be sealed according to the Quality Manual handling of evidence procedures.

2.6.3. The return of evidence will be documented at the time of transfer either electronically or on paper as part of the chain of custody.

2.6.4. Evidence artifacts extracted from the source media provided to the customer, generally on CD/DVD, will be assigned an item number. The CD/DVD or other media shall be labeled on the media or on its sealed container with the case identifying information and have its own chain of custody.

2.6.5. Upon completion of the forensic examination, original media evidence along with the controlled exported evidence exhibits will be either directly released to the customer or couriered via CS/CM. Proper chain of custody documentation will be completed.