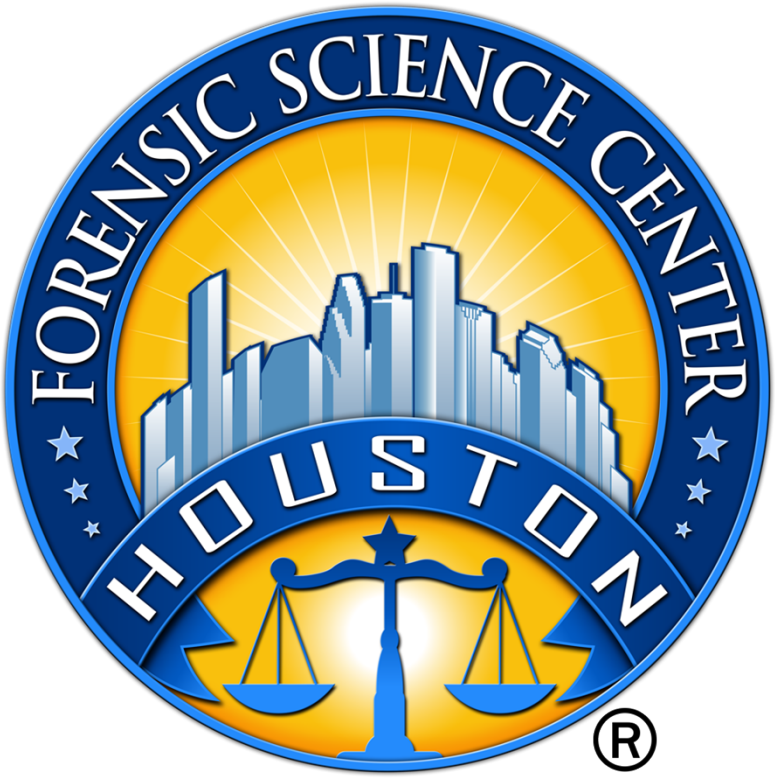


# Digital Forensics
# Section Guidelines

Crime Scene/Digital and Multimedia Division

# 1. Digital Forensic Laboratory Section Guidelines

## 1.1. Purpose

The procedures in this manual apply to examiners of the Digital Forensic Laboratory (DFL) when providing forensic services to customers. It is recognized that the digital data collection, recovery, and analysis field changes frequently therefore preventing the establishment of a rigid set of procedures to cover each and every case. This requires examiners to use their ingenuity, training, and experience to meet the requirements of the customers. These procedures establish the baseline for reliable technical services and are not intended to limit examiner's ingenuity when providing services to meet the customer's requirements.

When a technical procedure is dependent upon the use of a particular type of software and/or hardware, the step-by-step instructions on how to use the software/equipment or perform the analysis will not be included within the procedure. If vendor instructions are not sufficiently detailed, then additional instructions will be included in written procedures. User manuals will be available online, on the DFL internal server, or located in the proximity of forensic equipment.
There may be instances in which time-sensitive investigations/ threat to life situations require immediate processing and/or analysis of submitted evidence. For these instances, refer to the Exigency Procedure Section.

## 1.2. Responsibilities

**Technical Supervisor**

The Digital Forensics Laboratory is supervised by the Technical Supervisor for this section. His/her responsibilities include, but are not limited, to administrative, supervisory, and the operational functions of the DFL section. The technical supervisor responsibilities may include:

- Ensuring that new personnel are trained to the section's and quality standards.
- Conducting annual performance reviews of DFL personnel.
- Performing Administrative/Technical reviews of case records submitted by DFL personnel.
- Conducting Courtroom testimony evaluations.
- Serving as Training Liaison between the section, HFSC and personnel.
- Administering competency and proficiency tests to DFL personnel.
- Maintaining DFL personnel training file.
- Ensuring hardware, software and equipment are in proper working conditions.
- Ensuring that all quality standards are met as required for the section.
- Approving validation studies on hardware and software used for forensic casework.
- Recommending software and hardware to be implemented in the laboratory.

In the absence of the Technical Supervisor, another member of the DFL may be appointed to serve as a designee.

**Digital Examiner**

A Digital Forensic Examiner is a staff member who is authorized to examine digital evidence in assigned case work. Contingent on training and authorization, the duties of an examiner may include the following:

- Perform extraction and recovery of digital data from electronic devices.
- Write impartial test reports with details pertaining to their extraction and/or recovery of digital data.
- Perform technical reviews of case records submitted by DFL personnel. The reviewer is qualified through technical experience to conduct these reviews.
- Perform administrative reviews of case records submitted by DFL personnel.
- Respond to on-scene incident call outs and assist customers in identifying devices that may contain evidence.
- Provide expert testimony in court.
- Provide training and mentor guidance to new personnel.
- Ensure hardware, software and equipment is in proper working conditions.
- Validate and/or performance-check software and hardware to be used for forensic casework.

### 1.3. Digital Forensic Analysis Limitations

Digital data storage methodologies and systems vary. Variables include hardware, software and software operating systems, software release versions, and sometimes alternative use of hardware and software from original intent. Examiners apply their education, training, and experience to analyze data; and to use best scientific practices in that regard.

### 1.4. Safety

Examiners should be aware of their personal safety when handling test items.

Digital devices are powered by electricity. Devices should be disconnected from power sources when disconnecting and/or removing internal components (e.g., hard drives).

The internal components of digital devices, particularly desktop computers, are tightly configured with the potential for encountering sharp metal edges. Examiners should exercise caution when maneuvering inside devices. Gloves are an acceptable safeguard. Injuries should be reported to the section manager and the Health and Safety Specialist.

If biohazard substances are present on evidence, measures will be taken to sanitize and decontaminate the media as best as possible. While wearing rubber or latex gloves, use a bleach-solution sanitizing wipe(s) to remove visible biological materials present on the device. It is a good practice to sanitize all

devices when unpackaging them and prior to ungloved handling to prevent contamination. When using bleach-wipes, care should be exercised to prevent cleaning solution from seeping into and possibly damaging electronic components. Please refer to the HFSC safety manual for further information for utilizing cleaning solutions.