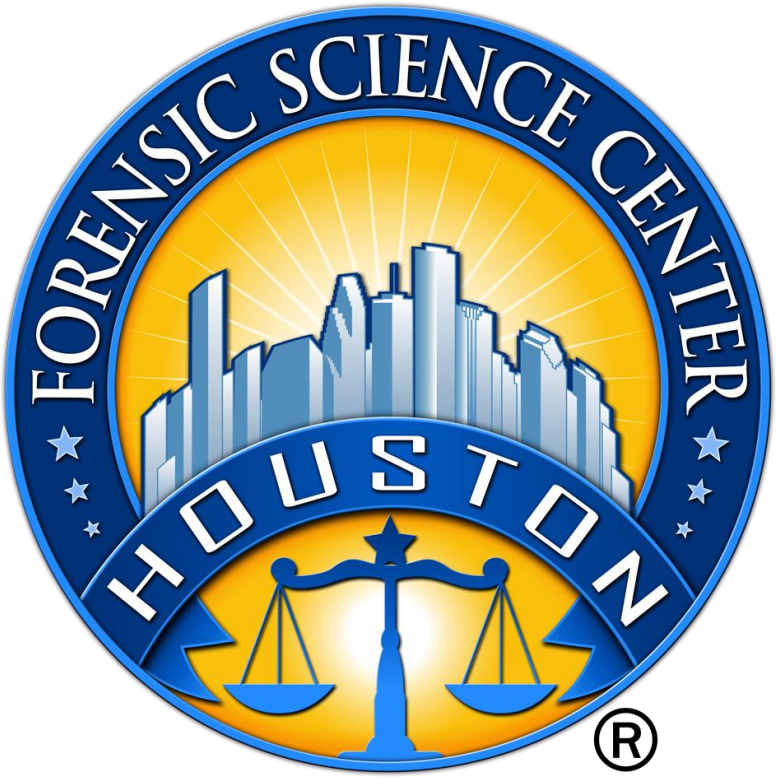

Digital Forensics

Definitions and Abbreviations

Crime Scene/Digital and Multimedia Division

14. DEFINITIONS AND ABBREVIATIONS

14.1. Purpose

14.1.1. This procedure contains definitions and abbreviations used in the Digital Forensic Laboratory.

14.2. Scope

14.2.1. These abbreviations are used for all Digital Forensic Technical procedures.

14.3. Definitions and Abbreviations

- **Administrative Software** – Software used for administrative purposes, such as writing reports. The Laboratory Information Management System (LIMS) and MS Word are examples of administrative software.
- **BIOS** – Basic Input Output System. Program that manages computer system startup and data flow between the computer operating system and attached devices such as keyboard, mouse, and printer. The BIOS stores system and configuration settings for a computer including date, time, boot sequence, chipset information, attached hardware, and onboard interrupt handlers.
- **Digital Media** – Any storage device that holds digital data.
- **EnCase boot**– CD/DVD or USB Drive
- **Forensic Software** – Software capable of physical device imaging, media wiping, or data extraction from portable and embedded devices.
- **F-SAN** – Storage device attached to the DFL internal server.
- **Hash Values:**
    - **MD5** – Message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hexadecimal value commonly used to verify data integrity. Hash functions are commonly used to guard against malicious changes to protected data in a wide variety of software, Internet, and security applications, including digital signatures and other forms of authentication
    - **SHA-1** – Secure Hash Algorithm is another cryptographic hash function. Its result is usually expressed as a 160 bit (20-byte) hexadecimal number. This algorithm was developed by the NSA.
- **Interpretive Software** – Software capable of reading file structure and intelligibly interpreting the file into a logical presentation. Many are capable of both forensic imaging and presentation

of the content. The presentation of content is considered interpretive (a document file will appear with legible results, etc.) Non-forensic software, such as media players, MS Word, etc., are also considered interpretive when representing data.

- **Logical Image** – A capture of all, or a targeted subset, of the active data on a logical partition of a hard drive. This active (or visible) data is what one would find if you were to browse through the drive with My Computer on Windows or with the Finder on a Mac. A logical image doesn't include deleted files, file fragments, and deleted or clear space from a drive partition.
- **Performance Verification** – The DFL internal confirmation that an externally validated tool, technique, or procedure performs as expected.
- **Physical image** – An exact copy/bit stream image of the source media that is inclusive of logical files, along with deleted content, file fragments, and other content that may not be apparent to the casual user. Thus, physical imaging is the preferred method for data acquisition.
- **Portable Electronic Device** – Device such as a tablet, GPS unit, cellphone, etc., meant to be portable and stores digital data.
- **Quality Control Checks** – The periodic confirmation of the reliability of the equipment, software, and/or hardware such as towers and virtual machine.
- **Ramsey Faraday Enclosure** – Device that shields its contents from cellular, Bluetooth, and WiFi signals.
- **Target Drive** – Destination drive to store data transferred from submitted evidence drives.
- **Validation** – A performance confirmation of a tool, technique, or procedure through examination and the provision of objective evidence that it functions correctly and as intended.
- **Wipe** – The act of completely erasing digital data from media.