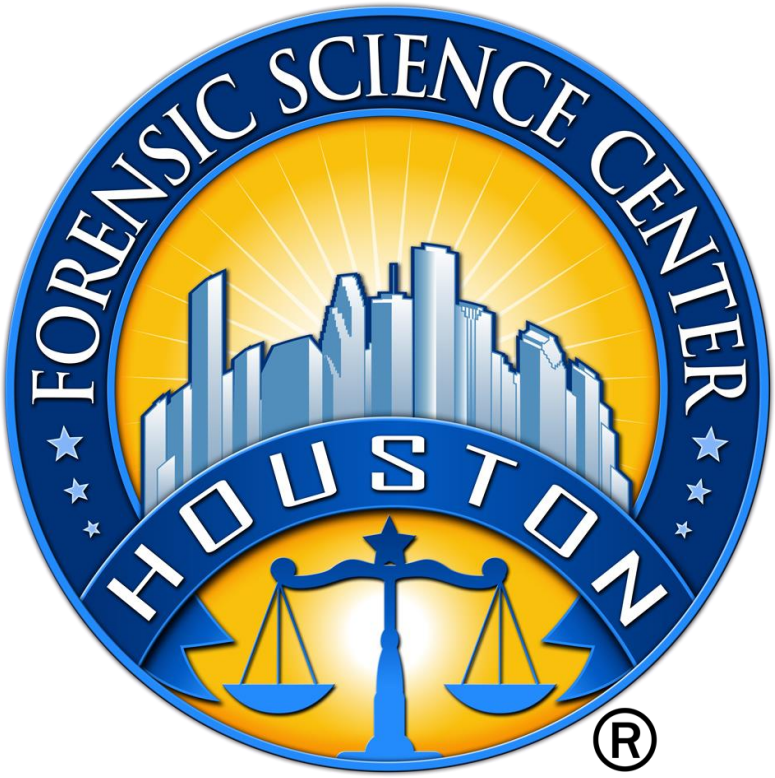

Digital Forensics

Physical and Logical Imaging Technical Procedure

Crime Scene/Digital and Multimedia Division

11. Physical and Logical Imaging Technical Procedure

11.1. Purpose

11.1.1. The purpose of this procedure is to avoid damage and alterations to original evidence when creating forensic copies of digital media.

11.2. Scope

11.2.1. This procedure applies to Digital Forensic Laboratory examiners tasked with capturing or recovering data from physical and logical digital media devices such as a hard drives or external media.

11.3. Equipment

- Forensic workstation
- Approved write protection hardware or software
- Forensic disk duplicator, if applicable
- Target forensic media

11.4. Overview

11.4.1. The original source media is best evidence. Forensic examiners conduct their forensic examinations utilizing forensic copies of the source media to safeguard and preserve original evidence from deleterious change. Verification of the forensic image is accomplished by hashing the image files during the imaging phase and post processing, if applicable, using a hash algorithm and/or cyclical redundancy checks (CRC) to ensure the forensically copied data matches the original data. Upon completion of the examination, the original evidence is returned to the customer and any forensic images are then deleted from examination machines to prepare for the next examination.

11.4.2. Whenever possible, original digital media should be imaged and the data analysis should be conducted on the image rather than the original device. The original media is imaged to a separate device, such as a hard drive, which is used to temporarily store the image.

11.4.3. If the number of devices are such that the total storage volume of exceeds the capacity of the storage capabilities on the forensic examination machine, the forensic images can be copied to the F-SAN or a NAS device. Should the original media be copied to or directly imaged to a Forensic SAN or NAS, the image shall be uniquely identified and stored within a uniquely identified folder. Upon completion of the forensic examination, the forensic working copies shall be deleted.

11.5. Physical Imaging Procedure

11.5.1. Connect the forensic target drive.

11.5.2. Use an approved hardware write blocking device, such as Weibetech or Digital Intelligence Write Blockers.

11.5.3. Attach the media to be imaged to a write blocking device, if applicable, noting that certain workstations are equipped with built in write blockers. A software write blocker such as FastBlock SE may also be utilized.

11.5.4. Power on or enable the write-blocking device.

11.5.5. Begin the imaging process.

11.5.6. At the conclusion of the imaging process, verify the image integrity using a hash algorithm. For FTK Imager and EnCase, this is an integrated and automated function. Save the output summary bookmark into the software forensic data report. Copy that log to the case record.

11.5.7. Power down equipment and remove the media. Secure the original device by re-installing it into the computer or other housing, if applicable.

11.5.8. The following information should be documented in the case record:

- Date and time the imaging was initiated.
- Hardware and software (include version) used to create the image.
- Unique identifier for the forensically wiped media used to store the image.
- The hash values verifying the image integrity, when applicable.
- Automated logs, if possible.
- Record if the imaging fails.

11.6. Logical Imaging Procedure

11.6.1. Connect the forensic target drive.

11.6.2. If a network acquisition is being employed to capture network-stored data, the forensic workstation will connect to the network and the forensic software will be directed by the examiner to the network storage location of the evidence data to be retrieved.

11.6.3. Launch the approved forensic imaging software to capture the logical data.

11.6.4. Direct the software to the file, folder, mounted volume, or attached network drive to be acquired.

11.6.5. Begin the imaging process, being sure to choose the option to hash the source during acquisition (if not enabled by default).

11.6.6. At the conclusion of the imaging process, verify the image integrity using a hash algorithm. For the DFL-approved software and devices, this is an integrated and automated function.

11.6.7. Unmount and detach the target drive and secure it as described.

11.6.8. The following information should be documented in the case record:

- Date and time the imaging was initiated.
- Hardware and software (include version) used to create the image.

- Unique identifier for the forensic image folder used to store the logical files or logical images.
- The hash values verifying the image integrity, when applicable.
- Automated logs, if enabled, that document success or process failures.

11.7. Quality Control Checks

11.7.1. The forensic computer used in casework shall be performance verified (POST check) annually to ensure that the forensic computer is functioning properly. The procedure for this verification process can be found in the Validation and Performance Verification Procedure.

11.8. Limitations

- Attempts to image damaged media may not be successful. Files and or file fragments may be the only information recoverable.
- Improperly invoked commands or incorrect connection of the source media may result in destruction of data or deleterious change.
- Forensic imaging may or may not capture data in a Host Protected Area or Dynamic Disk Overlay/Dynamic Configuration. This is dependent upon the write blocker being used and its capabilities or settings.
- The use of virtualized forensic processing may require different procedures than those set out herein.
- This procedure does not apply to cellular devices in general, but does apply to the devices' internal storage media (SD) cards when so equipped.
- Unallocated clusters, deleted files and folders, file slack, volume slack, alternate data streams, and other data areas that are normally acquired with physical imaging are not obtained using logical acquisitions.

11.9. References

- Technical Manual – Procedure for Write Protection
- Access Data FTK Imager User Manual
- Guidance Software EnCase User Guide
- Weibetech and Digital Intelligence Write Blocker User Guides
- Tableau User Manual