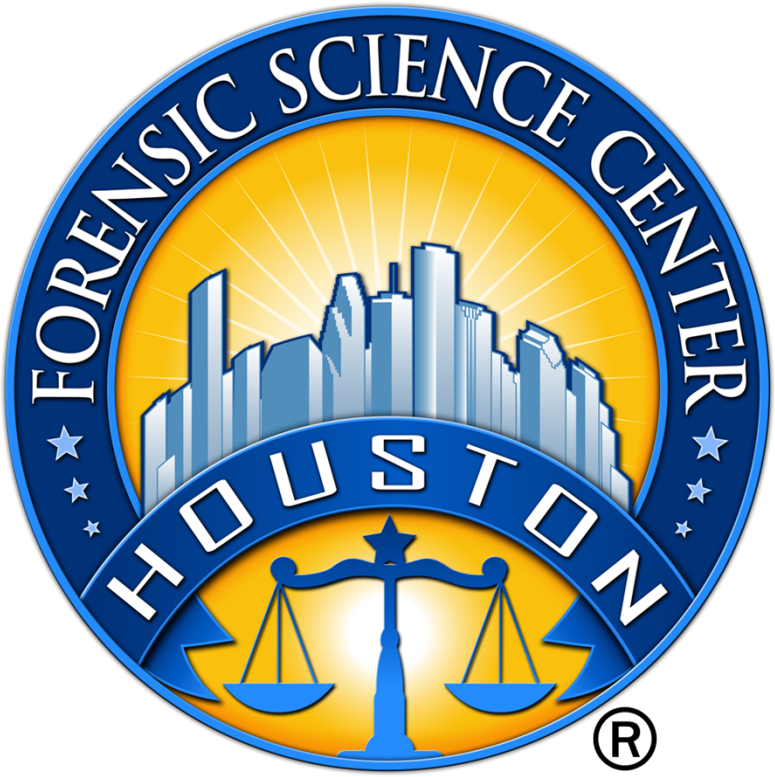

Multimedia Section

Hard Drive Removal Technical Procedure

Digital and Multimedia Evidence Division

1. HARD DRIVE REMOVAL TECHNICAL PROCEDURE

1.1. Purpose

1.1.1. The purpose of this procedure is how to remove the hard drives from devices (i.e. computers and DVRs) submitted for examination while maintaining the integrity of the evidence.

1.2. Scope

1.2.1. This procedure describes the essential steps needed to be taken by analysts in removing hard drives from submitted items of evidence.

1.3. Equipment

1.3.1. Tool kit
1.3.2. Permanent markers
1.3.3. Camera

1.4. Procedure

1.4.1. Photograph the condition of the evidence prior to the forensic examination. Visible damage shall be documented, photographed, and noted in the case record.
1.4.1.1. Analysts should ensure that the camera is securely mounted before photographing evidence.
1.4.2. With the device powered off and power cord and/or battery disconnected, open the case on the device to access the internal drive(s).
1.4.3. Photograph the internal contents of the evidence prior to removing the hard drive(s).
1.4.4. For non-cable acquisitions, disconnect the data and power cords connecting the hard drive to the device.
1.4.5. Remove the hard drive(s) from the device.
1.4.6. With an indelible marker, label the hard drive removed from the device or label the proximal container so it is properly identified. These markings will include the lab case number, evidence item number, and analyst's initials.
1.4.7. Photograph the hard drive to include the identification information.
1.4.8. Record the drive information from the hard drive label in case record. This may be either an automated software report derived from the imaging process, or a manual record. In cases where the hard drive is not accessible (cable acquisition method employed), recording this information may be done during the extraction/imaging process. Drive information may include:

- Make
- Model
- Serial number

- Storage capacity

1.4.9. Where possible or practicable (for computers), reconnect the power source to the computer and boot the evidence computer into the Basic Input Output System (BIOS) with the hard drive removed. If the date and time differ from the actual date and time, record the difference in the case record notes. Document instances where obtaining BIOS information is not feasible.

1.4.10. Record the BIOS information in the case record. BIOS information may include:

- Date and time the BIOS settings were verified
- The key or key sequence invoked to display the BIOS
- BIOS date and time settings
- BIOS manufacturer and version
- Boot sequence settings
- Failure to access the BIOS and reasons why, if applicable

1.4.11. Image the hard drive(s) in accordance with approved procedures for write protection and imaging.

1.4.11.1. For DVR hard drives, imaging may not be necessary as the software can scan the hard drive as is. If the DVR hard drive does need to be imaged, it will be done in accordance with the approved procedures for write protection and imaging.

1.4.12. Reassemble the device.

1.5. Limitations

1.5.1. Care shall be exercised to guard against electrostatic discharges which can damage or destroy the evidence hard drive.

1.5.2. In cases where internal storage consists of flash memory only, drive labels may not exist. This will impact the approach taken to document the storage medium for examination. Traditional methods may not apply and the analyst should do their best to photograph and record the drive component. If the drive is not removable, please refer to the Cable Acquisition Procedure.