Technical Procedure for DOS Hard Drive Imaging

1.0 Purpose - The purpose of this procedure is to use the Microsoft DOS operating system to create a forensic image of evidence hard drives without altering the data on the hard drive.

2.0 Scope - This procedure describes the steps to be taken by personnel of the State Crime Laboratory in using the Microsoft DOS operating system to image hard drives which are evidence in computer forensic examinations.

3.0 Definitions

- **Evidence drive** – Hard drives submitted as evidence.
- **Forensic boot disk** – Computer disk containing the MS DOS operating system and a forensic imaging program which is used to boot a computer without altering the data on evidence hard drives.
- **MD5 hash** – A 128-bit value that uniquely describes the contents of a file. This is a standard hash value used in computer forensics.
- **SAN** – Networked array of hard drives used as a digital evidence repository.
- **Case Folder** – A folder, designated by case number and located on the SAN, for use in a specific investigation.

4.0 Equipment, Materials and Reagents

- Forensic Tower or Portable Forensic Workstation
- Prepared Target drive
- Approved software for forensic imaging
- Forensic boot disk

5.0 Procedure

5.1 Insert the evidence drive and the Target drive into the forensic computer.

5.2 Boot the forensic computer into DOS using a forensic boot disk.

5.3 Use an approved hashing program to obtain the MD5 hash value of the evidence drive before imaging.

5.4 Image the evidence hard drive using an approved imaging tool and following the imaging procedures in the product manual.

5.5 If imaging in EnCase:

5.5.1 Ensure that the evidence drive is locked and unlock the Target drive.

5.5.2 EnCase presents an option to compress the file. Compression may be used in order to require fewer CDs or DVDs to store the forensic image at the completion of the analysis.

5.5.3 When presented a MD5 hash option, choose YES. EnCase uses this hash to verify that the Target drive is an exact forensic image of the evidence hard drive.

5.5.4 EnCase offers the ability to password protect the forensic image. Do not password-protect the forensic image.

5.5.5 The Maximum Desired Evidence File Size should be set to 640 Mb if the forensic image is to be saved to CDs. Larger file sizes may be used if the image files will be written to DVDs.

5.5.6 In rare cases, EnCase is unable to create a forensic image of the evidence drive. In this case, other approved imaging programs shall be used (see 3.1 in Digital/Latent Evidence Section Approved Software for Forensic Computer Examinations).

5.5.7 After verifying that the forensic image has been successfully completed, remove the subject's hard drive from the forensic computer.

5.6 When SAN is available for use, transfer forensic image file(s) from Target drive to Case Folder on SAN drive.

5.7 EnCase is the primary imaging tool used by the State Crime Laboratory. Situations may occur when other tools need to be used. Based on training and experience, another imaging tool from the approved list may be used.

5.8 When working with the hard drive from a laptop computer, the smaller laptop hard drive can be imaged by using the adapter to connect it to the standard IDE connector. The same imaging procedures are used.

5.9 If possible the acquisition shall be performed using Windows. Imaging in Windows is much faster than imaging in DOS.

5.10 Using compression in EnCase has no damaging effects on evidence. The files created are two to three times smaller than uncompressed files; however, creating compressed images may take five times longer than creating uncompressed images.

5.11 There may be instances when the evidence hard drive cannot be successfully imaged. In the event that a forensic image cannot be made of the evidence hard drive due to either hardware or software problems, all approved methods of imaging the drive shall be exhausted and the attempts to image the hard drive shall be documented before any examination on the original evidence hard drive.

5.12 Standards and Controls - A control disk image with a known hash value is used to ensure the proper functioning of forensic computers used in casework.

5.13 Calibrations - The forensic towers used in casework shall be verified each day that they are used to ensure that the computer hardware and software are functioning properly (see the Computer Performance Verification Procedure).

5.14 Maintenance – N/A

5.15 Sampling - N/A

5.16 Calculations - N/A

5.17 Uncertainty of Measurement - N/A

6.0 Limitations

6.1 Write protection used in the forensic imaging of hard drives can be either hardware or software write protection. The DOS imaging procedure shall be used to image a hard drive when hardware to write protect the hard drive is not used.

6.2 While the evidence drive is in the computer and the hard drive is not write protected, the computer shall not be booted into Windows. Booting into Windows can change files on the evidence drive.

6.3 Locking the evidence hard drive ensures that the Target drive cannot be accidentally copied onto the subject hard drive. Ensure that the subject hard drive is locked.

6.4 When using imaging software other than EnCase, care must be taken to ensure that the evidence data is not destroyed by copying the Target drive onto the Evidence drive.

6.5 Making a forensic image of the subject's hard drive is not the same as making a copy of the subject's hard drive. When a hard drive is copied, only the logical files are written to the Target drive. When a forensic image of a drive is created, all of the information on the suspect hard drive is written to the Target drive (including slack space, unallocated space, and deleted files).

7.0 Safety - N/A

8.0 References

- EnCase Forensic User Manual
- EnCase Intermediate Analysis and Reporting Course Guide
- EnCase Advanced Computer Forensics Course Guide
- Forensic Toolkit User Guide
- Forensic Boot Camp Training Manual
- Computer Performance Verification Procedure

9.0 Records - N/A

10.0 Attachments - N/A

Revision History

Effective Date	Version Number	Reason
09/17/2012	1	Original Document