Technical Procedure for Windows Imaging

1.0 Purpose - The purpose of this procedure is to use a Microsoft Windows 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 imaging hard drives submitted as evidence, using the Microsoft Windows operating system.

3.0 Definitions

- **Evidence drive** – Hard drives submitted as evidence.
- **MD5 hash** – A 128-bit value that uniquely describes the contents of a file. This is the standard hash value used in computer forensics.
- **Forensic drive** – Hard drive containing the operating system and all the forensic software that will be used in the examination.
- **Clone** - The process of performing a sector-by-sector copy operation from the suspect drive to the destination drive. The number of sectors copied is determined by the size of the suspect drive.

4.0 Equipment, Materials and Reagents

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

5.0 Procedure

5.1 Attach the evidence drive to the forensic computer using a read only hardware device.

5.2 Insert the forensic drive and Target drive in the forensic computer and boot into Windows.

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

5.4 Generate a forensic image of the evidence drive and save it to the Target drive using an approved imaging software program in Windows, following the imaging procedures in the product manual.

5.5 If using EnCase:

5.5.1 Image the evidence drive by choosing the Acquire button on the tool bar.

5.5.2 On the Options screen, enter the case information that the program requests. This information will be used by the program in preparing the EnCase report.

5.5.3 Check the box for Generate image hash. EnCase uses this hash to verify that the Target drive contains an exact forensic image of the evidence drive.

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

5.5.5 In rare cases, EnCase is unable to create a forensic image of the subject hard drive. In this case, make a clone of the subject hard drive onto the target drive using other approved imaging software such as SnapBack, or an approved hardware device such as the VOOM HardCopy II.

5.5.6 While the subject hard drive is attached to the read only device, additional programs that require access to the physical disk may be run (e.g., anti-virus software or Net Analysis).

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

5.6 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.

5.7 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.

5.8 In most situations, the Windows acquisition is preferable if the hardware allows it. Imaging in Windows is much faster than imaging in DOS.

5.9 The Computer Forensics Unit is equipped with forensic towers having a read only Firewire connection. Hard drives which are connected through validated read-only devices are write protected and may be imaged in the Windows environment.

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

5.11 In instances where the virus scan takes an excessive amount of time to complete, it is permissible to copy all of the logical files out to the Target hard drive and run the scan on these files.

5.12 Virus definitions on anti-virus software shall be updated regularly.

5.13 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.

5.14 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).

5.15 Maintenance – N/A

5.16 Sampling – N/A

5.17 Calculations – N/A

5.18 Uncertainty of Measurement – N/A

6.0 Limitations

6.1 The DOS imaging procedure must be used to image a hard drive when hardware to write protect the hard drive is not used.

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

6.3 Using compression in EnCase has no damaging effects on the evidence. These files created are smaller than uncompressed files; however, creating compressed images may take longer than creating uncompressed images.

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
10/31/2013	2	Added issuing authority to header