Digital/Latent Evidence Section
Technical Procedure for Removable/External Media Imaging to SAN

1.0 Purpose - The purpose of this procedure is to image various types of removable media (e.g., floppy disks, CDs, DVDs, MP3 players, Zip disks, Jazz disks, LS120 disks, digital cameras and flash memory cards) without making changes to the data on the media.

2.0 Scope - This procedure describes the steps to be taken by personnel of the State Crime Laboratory in imaging various types of removable media which may be submitted.

3.0 Definitions

- **SAN** – Networked array of hard drives used as a digital evidence repository.

4.0 Equipment, Materials and Reagents

- Forensic Tower or Portable Forensic Workstation
- Online SAN drive

5.0 Procedure

5.1 If possible, write protect any removable media.

5.2 If using EnCase for the examination, the removable media shall be added to the case and imaged to the SAN drive.

5.3 If the media can be write protected and keyword searches are not needed on the media, preview the original media without making a forensic image first.

5.4 If working with evidence CD-R or CD-RW disks, read them in read only CD drives. This will prevent changes from being made to the evidence. The Sony CD-R/DVD-R drive installed on the Computer Forensic Unit's forensic towers has been validated to ensure that changes will not be made to evidence media.

5.5 Hard drives shall only be imaged in DOS if write protection hardware is not in use. Likewise, removable media which can be write protected shall be imaged in the Windows based EnCase program.

5.6 When batch imaging floppy disks, EnCase chooses the disk capacity of the first floppy imaged as the capacity of all floppies in the batch. If a double density disk is imaged first, EnCase will not see all of the data on any high density disks which are imaged later in the batch.

5.7 EnCase has problems reading the format used by some computers to write to CD-RW disks. If a CD-RW is imaged or previewed in EnCase and shows no data on the disk, the disk shall be examined in Windows Explorer. If there is data on the disk and EnCase does not recognize it, Windows Explorer will read it. If a disk is found that contains data but is not recognized by EnCase, this disk shall be examined with CD/DVD Inspector or another approved imaging program. If the data is still not viewable, the data on the disk must be copied to a CD-R disk for use in EnCase. This method will only capture the Logical files on the CD-RW and not the deleted files or slack space.

5.8 Media Specific Notes

5.8.1 **Floppy Disks -** High density and double density floppy disks shall be batched and imaged separately

5.8.2 **CDs -** When using EnCase to image CD-RW disks, care shall be taken to ensure that EnCase can read the data on the disk (see **5.7**).

5.8.3 **Zip Disks -** Zip disks cannot be write protected and shall be imaged in DOS or imaged using hardware or software write protection.

5.8.4 **PDAs -** For PDA examination, a docking cradle made for the particular make and model of PDA is required. When the PDA is attached to the forensic tower using the cradle, EnCase sees the PDA as a piece of removable media. The data contained on the PDA can then be acquired by EnCase in the same method as with any other type of removable media.

5.8.5 **Digital Cameras -** For examination of digital cameras, the flash memory cards shall be removed from the camera. A flash media card reader is used to read the data on the media. EnCase sees the flash media as a piece of removable media. The data contained on the flash media card can then be acquired by EnCase in the same method as with any other type of removable media. If an adapter cable is available, the internal memory of the camera shall also be examined using approved forensic software.

5.9 **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.

5.10 **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).

5.11 **Maintenance –** N/A

5.12 **Sampling -** N/A

5.13 **Calculations -** N/A

5.14 **Uncertainty of Measurement -** N/A

6.0 **Limitations -** When a PDA is submitted to the Laboratory for analysis, great care shall be taken to ensure that the batteries do not fully discharge. The volatile memory in a PDA can be lost when the batteries completely discharge. PDAs which use AA or AAA batteries shall have new batteries placed into the PDA. PDAs with rechargeable batteries shall be charged if the charger is submitted. If these things cannot be done to ensure the safety of the evidence on the PDA, the evidence shall be imaged and then worked at the appropriate time.

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
12/7/2012	2	5.8.2 **-** changed (See **5.8**) to (See **5.7**)