Technical Procedure for Cable Acquisition

1.0 Purpose - The purpose of this procedure is to image evidence drives installed in the evidence computers in a situation where the hard drive is difficult or impossible to remove. This procedure provides for imaging these computers without making changes to the data on the evidence drive.

2.0 Scope - This procedure describes the steps to be taken by personnel of the State Crime Laboratory in imaging computers using a null-modem parallel (laplink) cable or network crossover cable.

3.0 Definitions

- **Target Drive** – Drive to which information from the evidence drive is being written
- **Evidence Drive** - Hard drives submitted as evidence.
- **EnCase boot floppy** - A 3 ½ inch computer disk containing the MS DOS operating system and a copy of the EnCase forensic imaging program which is used to boot a computer without altering the data on evidence hard drives.
- **Server mode** – DOS mode into which the evidence computer is put to enable it to send data to a forensic computer in a forensically safe manner for imaging.
- **Client mode** - DOS mode into which the forensic computer is put to enable it to receive data from an evidence computer in a forensically safe manner for imaging.
- **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
- EnCase boot floppy

5.0 Procedure

5.1 Set up the evidence computer in server mode by booting into DOS using an EnCase boot floppy.

5.2 Connect the evidence computer and forensic computer using a network crossover cable between the network interface cards or connect the laplink cable from the parallel port of the evidence computer to the parallel port of the forensic computer (running through the dongle if a parallel port dongle is used).

5.3 Once the evidence computer has booted, run EnCase in DOS.

5.4 The evidence computer will display hard drive information on the screen and you will note that the evidence drive is locked.

5.5 Choose “server mode” from the choices at the bottom of the screen.

5.6 A window will be displayed showing “Server Mode” and the message “waiting to connect.”

5.7 Install the Target drive into the forensic computer.

5.8 Set up the forensic computer in client mode by booting the forensic computer into DOS using an EnCase forensic boot disk and running EnCase.

5.9 Ensure that the screen of the forensic computer shows "client mode" in the title bar.

5.10 The information on the screen will be from the evidence computer.

5.11 The evidence drive can now be acquired by following the steps in the **Computer DOS Hard Drive Imaging Procedure**.

5.12 Prior to imaging the hard drive, use an approved hashing program to obtain the MD5 hash value of the evidence drive before imaging.

5.13 When acquisition has started, the server (evidence) computer window will show that a connection has been established and the data being transferred.

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

5.15 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.

5.16 In order to use a network crossover cable, the evidence computer must be equipped with a network interface card and the forensic boot disk must contain the DOS drivers for that network interface card. Otherwise, the parallel cable shall be used.

5.17 This is a very slow method of data acquisition. Using a network crossover cable is a faster method of imaging a hard drive than using a parallel cable. A hard drive greater than 20 GB in size may take several days to acquire using a parallel cable.

5.18 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.

5.19 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. The procedure for this verification process can be found in the Computer Performance Verification Procedure.

5.20 Maintenance – N/A

5.21 Sampling – N/A

5.22 Calculations – N/A

5.23 Uncertainty of Measurement – N/A

6.0 Limitations

6.1 Always set up the evidence computer in server mode first.

6.2 If possible, check the evidence computer prior to booting to ensure that the boot order is to the floppy drive first. Also, disable any power saving features in the BIOS.

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
- 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