Technical Procedure for Generating Results

1.0 Purpose - The purpose of this procedure is to provide guidelines for generating case results.

2.0 Scope - This document applies to State Crime Laboratory personnel who generate results for computer forensic casework.

3.0 Definitions - N/A

4.0 Equipment, Materials and Reagents

- Forensic Tower

5.0 Procedure

5.1 At the completion of an examination, the evidence files must be verified for integrity. This shall be done to ensure that the hash values of the evidence files verify completely. If any changes are made to the evidence files during the examination, the hash values will not verify. The verification of the hash values shall be documented in the case notes. If the hash values do not verify, this shall be reported to the Section Forensic Scientist Manager immediately and this step repeated.

5.2 Make a copy of the pertinent files on a CD or DVD and document the location found (e.g., logical files, deleted files, slack space, and unallocated space). Any CD or DVD that has apparent pornographic images of children copied on it as part of the examination will be labeled to reflect the following: *"This media may contain contraband and is intended for use by law enforcement in an official criminal investigation. Dissemination of this material may result in a criminal violation."*

5.3 A copy of the CDs or DVDs containing files recovered in the case shall be produced and retained in the Laboratory. This copy is for reference only. If further examination is needed in the case, either the original evidence or the forensic image shall be returned to the Laboratory to continue the examination.

5.3.1 When a copy of the work product is made on a CD or DVD for retention in the Laboratory and this media contains possible pornographic images of children, the data on this media shall be password protected to prevent any unauthorized use of these files.

5.3.2 File copy media shall be kept in a locked cabinet and a log shall be kept to indicate the employee who placed the media in the cabinet. Alternatively, file copy media may be secured in the office of the analyst who created the file copy.

5.4 Other examination documentation shall be stored within the Laboratory information and reporting system.

5.5 When practical (not limited by excessive size), copy the forensic image onto a media which shall be returned to the submitting agency along with the original evidence. If further analysis is needed, the media may be returned to the lab. The target hard drive used to make the forensic image may be wiped and reused in further casework examinations.

5.6 A Laboratory Report shall be created in Forensic Advantage (FA).

5.7 When creating a CD or DVD, the session shall be finalized.

5.8 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.

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

5.10 Maintenance – N/A

5.11 Sampling - N/A

5.12 Calculations - N/A

5.13 Uncertainty of Measurement - N/A

6.0 Limitations - Only CD-R, DVD-R or DVD+R disks may be used to copy recovered files and the forensic image. CD-RW or DVD-RW disks shall never be used because the data on the disk may be altered.

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
- Digital/Latent Evidence Section 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
02/01/2013	2	Edited 5.5