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 (forensic image) 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 digital media and document the location found (e.g., logical files, deleted files, slack space, and unallocated space). Any media 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 file copy of the digital media 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 File copy media shall be kept secured in the digital evidence vault or 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 Standards and Controls - All forensic computers and forensic tools shall be functioning properly prior to beginning a computer forensic examination (see Technical Procedure for Computer Forensics Performance Verification).

5.8 Calibrations - N/A

5.9 Maintenance – N/A

5.10 Sampling - N/A

5.11 Calculations - N/A

5.12 Uncertainty of Measurement - N/A

6.0 Limitations - Media of appropriate size may be used to copy recovered files and forensic image(s). Media used to copy recovered files and forensic images shall be burned to read-only discs or the media shall be set to read-only permissions when possible.

7.0 Safety - N/A

8.0 References

- EnCase Intermediate Analysis and Reporting Course Guide
- EnCase Advanced Computer Forensics Course Guide
- Technical Procedure for Computer Forensics Performance Verification

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
10/31/2013	3	Added issuing authority to header
10/19/2015	4	6.0 – Added Blu-Ray media
11/07/2016	5	5.1 – edited for clarity 5.2 – edited statement to include all media types 5.3 – edited statement for clarity and to include all media types 5.3.1 – removed statement 5.3.2 – edited statement for clarity 5.7 – removed statement 5.8 – updated Standards and Controls to reflect updated procedure 5.9 – removed statement 6.0 – edited statement to include all media types 8.0 – updated references