Technical Procedure for Generating Results

1.0 Purpose - The purpose of this procedure is to provide guidelines for generating case results and reporting computer forensic and mobile device evidence analysis results in the State Crime Laboratory.

2.0 Scope - This document applies to State Crime Laboratory personnel who generate results and write reports for computer forensic and mobile device casework.

3.0 Definitions - N/A

4.0 Equipment, Materials and Reagents

- Forensic Tower
- Computer with Forensic Advantage (FA) application

5.0 Procedure

5.1 Pre-Reporting

5.1.1 At the completion of an examination, the forensic image shall be verified for integrity in order to ensure that the forensic image has not changed during the course of the forensic examination. The verification shall be done within the forensic software tool used to conduct the forensic examination. If any changes are made to the forensic image during the examination, it will not verify within the forensic software tool. The verification of the forensic image shall be documented in the case notes. If the forensic image does not verify, this shall be reported to the Section Forensic Scientist Manager immediately and this step repeated.

5.1.2 Transfer the recovered data and the software tool(s) report on to digital media of the appropriate size.

5.2 Reporting

5.2.1 A Laboratory Report shall be created in FA.

5.2.2 Laboratory Reports must contain information specific to the requested examination(s) and must provide the reader with information in a clear and concise manner. Any analysis contained within a report must include an accurate interpretation of the actual results of the examination in a manner approved by the Forensic Scientist Manager or his/her designee.

5.2.3 A narrative-driven reporting method shall be used. In order to establish consistency within laboratory reports with regards to digital forensic examinations, the following items shall be, at a minimum, included within a laboratory report:

- Item(s) examined, including sub-items
- What type of examination was requested (e.g. computer forensics, mobile device, security bypass, etc.)
- Under what authority the exam was performed (e.g. search warrant, consent, etc.)

- Results of the examination, regardless of outcome (e.g. data located, not located, results of virus scans, data encrypted, etc.).
- The methodology used during the examination(s).

Example with positive results:

Item 1 was examined for the presence of possible child pornography pursuant to a search warrant provided by the submitting agency. During the examination, data that may be responsive to the requested examination was located. See the FTK report in Container C1 for specific details about the data recovered during the examination.

Should it become necessary to evaluate the recovered data, the FTK report within Container C1 must be viewed.

Example with negative results:

Item 1 was examined for the presence of possible child pornography pursuant to a search warrant provided by the submitting agency. During the examination, no data was found that appeared to be responsive to the requested search. General system information about the device was documented, and included in the generated FTK report.

5.2.4 The overall process used to identify recovered data or artifacts must be described within the Forensic Scientist's worksheet and is not necessarily needed for the Laboratory Report. The description must be detailed enough so that another digital forensic examiner could replicate the examination if necessary.

5.2.5 Each report detailing the examination of computer or mobile devices shall include the following language in order to satisfy the requirement for methodology documentation:

Item(s) [Item number here] was/were examined utilizing [Insert the name of the forensic tool(s) here].

5.2.6 In instances where suspected child pornography is recovered, a warning statement shall be added to the laboratory report that indicates the presence of contraband.

Example:

The FTK report contained in Container C1 may contain contraband and is intended for use by law enforcement in an official criminal investigation. It is highly recommended that any device used to view the FTK report and the material it contains be disconnected from any network, including the Internet. Dissemination of this material may result in criminal prosecution.

5.2.6 Any additional statements describing the examination results that do not match the criteria above shall be approved by the Forensic Scientist Manager prior to the release of the report.

5.3 **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).

5.4 **Reporting Deviations –** Other result statements may be generated upon approval of the Forensic Scientist Manager

5.5 **Calibrations -** N/A

5.6 **Maintenance –** N/A

5.7 **Sampling -** N/A

5.8 **Calculations -** N/A

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

6.0 **Limitations -** Media of appropriate size may be used to copy recovered files. Media used to copy recovered files 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**

- Technical Procedure for Computer Forensics Performance Verification
- Scientific Working Group on Digital Evidence, *SWGDE Requirements for Report Writing in Digital and Multimedia Forensics*, 2018 November 20, Version 1.0

9.0 **Records –** N/A

10.0 **Attachments -** N/A

Revision History		
Effective Date	Version Number	Reason
12/02/2020	8	5.2.3 – Removed the last paragraph. Corrected header information