Technical Procedure for Computer Forensics Performance Verification

1.0 Purpose – The purpose of this procedure is to ensure that forensic computers and forensic tools utilized in casework are functioning properly prior to beginning an examination.

2.0 Scope - This procedure describes the steps to be taken prior to beginning a computer forensic examination by personnel of the State Crime Laboratory to determine that forensic computers and forensic tools are in proper working order.

3.0 Definitions

- **Control Media –** A standard piece of media with a known hash value.
- **Hash Value –** An alphanumeric value that uniquely represents a set of data.
- **Power-On Self Test (POST) –** A series of diagnostic tests that are performed when a computer powers on and determines proper functioning of the hardware components.
- **Forensic Tool** – Forensic software tool or standalone hardware device utilized to conduct acquisitions in casework.
- **System Image –** Backup of the system drive that contains a clean install of the operating system (OS).

4.0 Equipment, Materials and Reagents

- Forensic Computer
- Approved Forensic Software Tool or Hardware Device
- Control Media

5.0 Procedure

5.1 The Computer Forensics Performance Verification Procedure shall be used prior to beginning a computer forensic examination.

5.2 The forensic computers used in casework shall be restored to a clean system image before beginning a new case. The Forensic Scientist shall ensure that the computer restored and completed its POST successfully (see the Technical Procedure for System Image Restoration).

5.2.1 Forensic tools for acquisition that are standalone hardware devices do not need to be restored between cases; however, a Control Media shall be acquired prior to acquiring evidence items.

5.3 The forensic computer or forensic tool shall successfully complete its POST without errors. If the POST reports an error, then the forensic computer or forensic tool shall not be used in casework until the error has been corrected and POST completes successfully.

5.4 The Control Media with a known hash shall be acquired prior to acquiring an item of evidence in a case. The Control Media shall be acquired each day that items of evidence are acquired and for each forensic software tool or hardware device being utilized. If more than one item of evidence is acquired in the same day with the same tool, then it is only necessary to acquire the Control Media before the first item.

5.5 The acquisition hash value of the Control Media must match the known hash value for the acquisition tool to be functioning properly. If the hash values do not match, then the forensic computer or forensic tool shall not be used in casework until the source of the error in the hash values has been determined and corrected.

5.6 The Forensic Scientist shall ensure that the acquisition hash value matches the known hash value for the Control Media. If the hash values match, then the acquisition tool is functioning properly on the forensic computer or forensic tool.

5.7 A notation shall be made in the log within the FA system for the applicable forensic computer or tool. In addition, a notation shall be made in the Forensic Scientist's case notes.

5.8 **Standards and Controls -** All forensic computers and forensic tools shall be functioning properly before beginning a computer forensic examination. Control media with a known hash value is used to ensure the proper functioning of acquisition tools for forensic computers and forensic tools.

5.9 **Calibrations –** N/A

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 – N/A

7.0 Safety – N/A

8.0 References

- Technical Procedure for System Image Restoration
- Scientific Working Group on Digital Evidence Model Standard Operating Procedures for Computer Forensics

9.0 Records - N/A

10.0 Attachments - N/A

Revision History		
Effective Date	Version Number	Reason
09/17/2012	1	Original Document
10/31/2013	2	Added issuing authority to header
08/29/2014	3	Added control thumb drive to 5.1, 5.4, and 6.1 Removed sentence regarding 3.5" floppy disk imaged in Windows or DOS from 5.1
11/07/2016	4	Throughout document: changed procedure from daily occurrence to prior to beginning a computer forensic examination; changed control disk to control media; removed references to tower and VM and changed to forensic computers and forensic tools 3.0 – removed definition for VM and added new definitions 4.0 – added to equipment list 5.1 – changed and moved to 5.2; added new statements for 5.1 to include system restoration and POST 5.2 – changed statement to Control media; changed MD5 hash to hash value 5.4 – edited Standard and Control to reflect updated procedure 6.0 – Incorporated into section 5.0 8.0 – updated References