Technical Procedure for Hard Drive Removal

1.0 Purpose - The purpose of this procedure is to remove the hard drives from computers submitted for examination while maintaining the integrity of the evidence.

2.0 Scope - This procedure describes the steps to be taken by personnel of the State Crime Laboratory in removing hard drives from computers which are evidence in forensic computer examinations.

3.0 Definitions

- **BIOS** – Basic Input Output System. A number of machine code routines that are stored in ROM and available for execution at boot.
- **Electrostatic Discharge (ESD)** – an uncontrolled and sudden flow of electrons from one object to another caused by contact between the two objects.

4.0 Equipment, Materials and Reagents

- Computer repair tool kit
- Anti-static bench mat
- Anti-static wrist strap
- Permanent markers
- Camera

5.0 Procedure

5.1 Ensure proper legal authorization.

5.2 Record the system information from the evidence computer.

5.3 In order to avoid damage to the computer and its internal components from electrostatic discharge (ESD), place the computer on an anti-static bench mat, and attach the anti-static strap to the computer.

5.4 If requested by the submitting agency, photograph the condition of the evidence computer prior to opening the case.

5.5 Check for external media connected to the evidence computer. Check for media inside optical drive(s), flash memory slots, and all other external media connections. Remove all external media from the evidence computer and label for identification. Complete labeling as provided in the Laboratory Procedure for Evidence Management.

5.6 The examiner shall attach the anti-static wrist strap prior to opening the case on the computer.

5.7 If requested by the submitting agency, photograph the internal contents of the evidence computer prior to removing the hard drive(s).

5.8 If necessary, mark the cords connecting the hard drive(s) to the evidence computer to facilitate proper reassembly.

5.9 Remove the hard drive(s) from the evidence computer.

5.10 Label the hard drive(s) removed from the evidence computer for identification. Complete labeling as provided in the Laboratory Procedure for Evidence Management.

5.11 Record the drive information (e.g., make, model, serial number, number of sectors, number of heads, and jumper settings).

5.12 With the hard drive(s) removed, boot the evidence computer into the BIOS. If the date and time differ from the actual date and time, record the difference.

5.13 Acquire the hard drive(s) using an acquisition tool from the Approved Software and Hardware List for Computer Forensic Examinations (see Technical Procedure for Evidence Acquisition in Computer Forensic Examinations).

5.14 Reassemble the computer.

5.15 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).

5.16 Calibrations - N/A

5.17 Maintenance – N/A

5.18 Sampling - N/A

5.19 Calculations - N/A

5.20 Uncertainty of Measurement - N/A

6.0 Limitations - Care shall be exercised to guard against ESD, which can damage or destroy the evidence hard drive.

7.0 Safety - N/A

8.0 References

- Myers, Mike. *CompTIA A+ Certification All-in-One Guide Ninth Edition (Exams 220-901 & 220-902)*, New York: McGraw Hill, 2016. Print.
- Scientific Working Group on Digital Evidence. *SWGDE Best Practices for Computer Forensics*, Version 3.1, 2014.
- Scientific Working Group on Digital Evidence. *SWGDE Model Standard Operation Procedures for Computer Forensics*, Version 3.0, 2012.

9.0 Records - N/A

10.0 Attachments - N/A

Revision History		
Effective Date	Version Number	Reason
09/17/2012	1	Original Document
12/07/2012	2	5.10 - reworded for clarity
10/31/2013	3	Added issuing authority to header
11/07/2016	4	5.1 – added statement 5.3 – added to statement 5.5 – edited statement 5.7 – edited statement for clarity 5.10; 5.11 – removed statements 5.11 – added statement 5.13 – added statement to reflect updated procedures Throughout document – changed hard drive to hard drive(s)
07/02/2019	5	Updated header to reflect Digital Evidence Section only; 3.0 - added definition for ESD; 4.0 - added anti-static mat and anti-static wrist strap to equipment; 5.3 – added section regarding ESD and readjusted following section numbers; 5.6 - added anti-static wrist strap; 6.0 - added ESD; 8.0 - removed two previous references and added three new references.