Technical Procedure for Evidence Acquisition in Computer Forensic Examinations

1.0 Purpose - This procedure establishes the process to acquire digital media evidence.

2.0 Scope - This procedure applies to the personnel of the State Crime Laboratory for use in acquiring digital media evidence submitted for a Computer Forensic examination.

3.0 Definitions

- **Forensic Image** – An exact copy of the original evidence.
- **Target drive** – Digital media that stores forensic images and other case related data.
- **Hash value** – An alphanumeric value that uniquely represents a set of data.
- **Control Media** – A standard piece of media with a known hash value.
- **Write-Blocker** – A read-only software or hardware device that protects the integrity of the original evidence by not allowing any writes or alterations to occur during the acquisition process.
- **BIOS** – Basic Input Output System. A number of machine code routines that are stored in ROM and available for execution at boot.

4.0 Equipment, Materials and Reagents

- Approved forensic software tool or hardware device for acquisition
- Forensic computer
- Write-Blocker
- Target drive
- Control media

5.0 Procedure

5.1 The Forensic Scientist shall determine the appropriate method of acquisition for the submitted evidence. Hard drives shall always be removed when possible (see Technical Procedure for Hard Drive Removal). If a method of acquisition does not complete successfully due to software or hardware issues, then all approved methods shall be exhausted before documenting that the evidence could not be acquired. All approved acquisition methods shall be exhausted and documented before conducting an examination on an evidence drive.

5.2 In the event that submitted evidence may have internal or external damage, the Forensic Scientist may utilize discretion in acquiring the evidence before obtaining the initial hash value. This is to prevent the evidence from becoming inoperable before acquiring an exact copy.

5.3 For acquisition methods that require access to the BIOS or Target Disk Mode, the Forensic Scientist may check the settings in BIOS or bootable devices prior to connecting the target drive or acquisition tool. This is to accommodate for the varying types of evidence that may have more than one hard drive. While accessing the BIOS, remove all hard drives from the boot order if possible when using forensic boot media.

6.0 Acquisition Procedure using Forensic Software on a Windows Operating System

6.1 Connect target drive to the forensic computer.

6.2 The Control Media shall be acquired before acquiring evidence (see Technical Procedure for Computer Performance Verification).

6.3 Connect evidence to the forensic computer through the use of a write-blocker.

6.4 Use forensic software tool to obtain an initial hash value for the evidence.

6.5 Use forensic software tool to acquire the evidence onto the target drive.

6.6 Verify that the acquisition completed successfully and that the initial hash value for the evidence matches the acquisition hash value for the forensic image.

7.0 Acquisition Procedure using a Standalone Hardware Device

6.1 Connect target drive to the destination drive connection on the hardware device.

6.2 The Control Media shall be acquired before acquiring evidence (see Technical Procedure for Computer Performance Verification).

6.3 Connect evidence to the appropriate write-block connection on the hardware device.

6.4 Use the hardware device to obtain an initial hash value for the evidence.

6.5 Use the hardware device to acquire the evidence onto the target drive.

6.6 Verify that the acquisition completed successfully and that the initial hash value for the evidence matches the acquisition hash value for the forensic image.

8.0 Acquisition Procedure using Forensic Boot Media for an Apple Macintosh Computer

8.1 Use this procedure only if the evidence computer has hard drive(s) that are non-removable. This procedure shall only be used on Intel-based Macintosh (Mac) computers.

8.2 Ensure that any external media has been removed from the computer. External media shall be acquired separately.

8.3 Ensure that the computer has a power source and is connected to any peripherals as needed.

8.4 Insert or connect the boot media into the Mac computer while powered off.

8.5 Connect target drive to the Mac computer.

8.6 Power on the Mac while holding down the OPTION key. If presented with a lock icon, then a firmware password exists on the Mac. Do not proceed with this acquisition method if the Mac has a firmware password. If no firmware password exists, then it is permissible to proceed with acquisition. The available bootable devices will appear on the screen.

8.7 Select the boot media. Be aware that the boot media may be listed as a “Windows” disk as this is the default naming convention for non-Mac media. Be aware that some Mac computers have a Windows partition.

8.8 Obtain an initial hash value of the evidence Mac.

8.9 Acquire the evidence Mac onto the target drive.

8.10 Verify that the acquisition completed successfully and that the initial hash value for the evidence matches the acquisition hash value for the forensic image.

8.11 Power off the Mac by holding down the power button and disconnect the target drive and boot media. Some boot media have a shutdown option that may also be used.

9.0 Acquisition Procedure using Target Disk Mode for an Apple Macintosh Computer

9.1 Use this procedure only if the evidence computer has hard drive(s) that are non-removable. When a Macintosh (Mac) computer is placed in Target Disk Mode, it is a read-write mode; therefore, the Forensic Scientist shall utilize a hardware write-blocker for acquisition. If the Mac computer has more than one hard drive, then utilize the Acquisition Procedure using Forensic Boot Media for an Apple Macintosh Computer.

9.2 Ensure that any external media has been removed from the computer. External media shall be acquired separately.

9.3 Ensure that the computer has a power source and is connected to any peripherals as needed.

9.4 Connect target drive to forensic computer. If utilizing a standalone hardware device, then connect target drive to the destination connection of the device.

9.5 Power on the Mac while holding down the OPTION key. If presented with a lock icon, then a firmware password exists on the Mac. Do not proceed with this acquisition method if the Mac has a firmware password. If no firmware password exists, then it is permissible to proceed with acquisition. Turn off the system by holding down the power button.

9.6 Power on the Mac by holding down the “T” key to enter Target Disk Mode.

9.7 When the Target Disk Mode symbol appears on the screen, connect the evidence Mac to a hardware write-blocker attached to the forensic computer. If utilizing a standalone hardware device, then connect the evidence Mac to the write-block connection of the device.

9.8 Obtain an initial hash value of the evidence Mac.

9.9 Acquire the evidence Mac onto the target drive.

9.10 Verify that the acquisition completed successfully and that the initial hash value for the evidence matches the acquisition hash value for the forensic image.

9.11 Disconnect the Mac and power off by holding down the power button.

10.0 Acquisition Procedure using Forensic Boot Media for Computers with BIOS

10.1 Use this procedure only if the evidence computer has hard drive(s) that are non-removable and the proper key(s) for accessing the BIOS can be obtained.

10.2 Determine the required key(s) to access the BIOS through manufacturer documentation, reference materials, testing, etc. If unable to determine how to access the BIOS, do not continue with acquisition through this method.

10.3 Research the specifications for the model computer and determine if it is possible to boot the computer from external media. If it is possible to boot the computer with external media, then determine what type of boot media will be required (CD, USB, etc.).

10.4 Ensure that any external media has been removed from the computer. External media shall be acquired separately.

10.5 Ensure that the computer has a power source and is connected to any peripherals as needed.

10.6 Insert or connect the boot media into the evidence computer.

10.7 Connect the target drive to the evidence computer.

10.8 Power on the evidence computer while holding down the key(s) to access the BIOS. The Forensic Scientist shall be prepared to remove the power source immediately in the event that the evidence computer may have bypassed the BIOS.

10.9 Set the boot sequence or boot order to boot from the forensic boot media.

10.10 Use the forensic boot media to obtain an initial hash value for the evidence.

10.11 Use the forensic boot media to acquire the evidence onto the target drive.

10.12 Verify that the acquisition completed successfully and that the initial hash value for the evidence matches the acquisition hash value for the forensic image.

10.13 Power off the evidence computer. Disconnect the target drive and forensic boot media.

11.0 Acquisition Procedure for Optical Media

11.1 Connect target drive to the forensic computer.

11.2 The Control Media shall be acquired before acquiring evidence (see Technical Procedure for Computer Performance Verification).

11.3 Insert optical media evidence into a read-only optical drive.

11.4 Use forensic software tool to obtain an initial hash value for the evidence.

11.5 Use forensic software tool to acquire the evidence onto the target drive.

11.6 Verify that the acquisition completed successfully and that the initial hash value for the evidence matches the acquisition hash value for the forensic image.

11.7 Optical media may be previewed at the discretion of the Forensic Scientist.

12.0 Acquisition Procedure for Digital Cameras

12.1 Memory cards shall be removed from the digital camera and acquired separately.

12.2 Connect target drive to forensic computer or forensic hardware device.

12.3 The Control Media shall be acquired before acquiring evidence (see Technical Procedure for Computer Performance Verification).

12.4 Connect evidence to the forensic computer through the use of a write-blocker or through forensic hardware device.

12.5 Use forensic software tool or hardware device to obtain an initial hash value for the evidence.

12.6 Use forensic software tool or hardware device to acquire the evidence onto the target drive.

12.7 Verify that the acquisition completed successfully and that the initial hash value for the evidence matches the acquisition hash value for the forensic image.

12.8 Determine if the digital camera has internal memory storage. If an adapter cable for the digital camera is available, then the internal memory of the camera shall also be examined.

13.0 Procedure for Cloning Digital Evidence

13.1 Determine the sector count for the evidence that will be cloned.

13.2 Select a target drive with the same sector geometry as the evidence if possible. The target drive must be of equal or larger size.

13.3 Connect target drive to the destination drive connection on the hardware device.

13.4 Connect evidence to the appropriate write-block connection on the hardware device.

13.5 Use the hardware device to obtain an initial hash value for the evidence.

13.6 Use the hardware device to clone the evidence onto the target drive.

13.7 Verify that the cloning procedure completed successfully. Disconnect the evidence and target drive (clone) from the hardware device.

13.8 Use a forensic software tool or hardware device to obtain a hash value for the target drive (clone). Ensure that the target drive (clone) is connected to the forensic computer or forensic hardware device through the use of a write-blocker. Verify that the hash value of the target drive (clone) matches the initial hash value for the evidence. For drives with different sector geometry, the target drive (clone) hash value will not match the evidence hash value due to different amount of sectors. In order to verify that the data is an exact copy on a drive with different sector geometry, a software tool such as EnCase will need to be used to obtain a hash value for the data copied to the target drive (clone). Determine the exact amount of sectors for the evidence and enter that sector count into the software tool to obtain a hash value for the exact amount of sectors on the target drive (clone). If the hash value for the data on the target drive (clone) matches the hash value for the original evidence, then the data on the target drive (clone) is verified to be identical.

14.0 Procedure for Restoring a Forensic Image

14.1 Determine the sector count for the forensic image that will be restored.

14.2 Select a target drive with the same sector geometry as the forensic image if possible. The target drive must be of equal or larger size.

14.3 Connect target drive to the forensic computer.

14.4 Add the forensic image to be restored into forensic software.

14.5 Restore the forensic image onto the target drive.

14.6 Remove the target drive (restore) immediately after completion to prevent any changes from occurring to the drive.

14.7 Verify that the restore completed successfully. If the forensic software did not conduct an automatic verification of the hash values, then manually obtain the hash values to verify the restore completed successfully. Connect the target drive (restore) to the forensic computer through the use of a write-blocker. Use forensic software to obtain a hash value for the target drive (restore). Verify that the hash value for the target drive (restore) matches the hash value for the forensic image. For drives with different sector geometry, the target drive (restore) hash value will not match the forensic image hash value due to different amount of sectors. In order to verify that the data is an exact copy on a drive with different sector geometry, a software tool such as EnCase will need to be used to obtain a hash value for the data restored to the target drive (restore). Determine the exact amount of sectors for the forensic image and enter that sector count into the software tool to obtain a hash value for the exact amount of sectors on the target drive (restore). If the hash value for the data on the target drive (restore) matches the hash value for the forensic image, then the data on the target drive (restore) is verified to be identical.

15.0 Standards and Controls

15.1 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).

16.0 Calibrations – N/A

17.0 Maintenance – N/A

18.0 Sampling – N/A

19.0 Calculations – N/A

20.0 Uncertainty of Measurement – N/A

21.0 Limitations

21.1 Due to the technology of Solid State Drives, the initial hash may not always match the acquisition hash for the forensic image. This shall be documented in the case notes.

21.2 When a PDA is submitted for analysis, great care shall be taken to ensure that the batteries do not fully discharge. The volatile memory in a PDA may be lost when the batteries fully discharge. New batteries shall be placed in PDAs for examination. PDAs with rechargeable batteries shall be charged if a charger is available.

21.3 It is not possible to acquire the Control Media in some of the methods listed in this procedure.

22.0 Safety – N/A

23.0 References

- Scientific Working Group on Digital Evidence Model Standard Operating Procedures for Computer Forensics
- Technical Procedure for Computer Forensics Performance Verification
- Technical Procedure for Hard Drive Removal

24.0 Records – N/A

25.0 Attachments – N/A

Revision History

Effective Date	Version Number	Reason
11/07/2016	1	Original Document

All copies of this document are uncontrolled when printed.