Technical Procedure for Macintosh Native Examination

1.0 Purpose - The purpose of this procedure is to examine data methodically from a device running the Apple Macintosh OS X or iOS operating systems by means of a forensic examination platform running the Apple OS X operating system.

2.0 Scope - This procedure applies to all personnel of the State Crime Laboratory who examine data from devices running the Apple Macintosh OS X or iOS operating systems submitted to the Laboratory as evidence.

3.0 Definitions

- **OSX** – The OS Ten (X) operating system for Apple computers, originally built off of the BSD UNIX kernel, which has been ported to work on Intel processors.
- **iOS** – The operating system for Apple devices (iPods, iPads, iPod Touches, iPhones, etc.).
- **Finder** – An application in the Apple OS X operating system that allows access to the files and folders on a given computer (similar to Windows Explorer on the Windows platform).
- **File Vault** - An application on versions of OS X that allow the user to encrypt the contents of their Home folder. File Vault uses AES-128 encryption.
- **Home Folder** – A folder in the Apple OS X directory structure in which all user data for a given user account is stored.
- **Shadow File** – A mounted file that is attached to, but not part of, a locked forensic image file. The mounted shadow file can then be indexed by Spotlight to find relevant data.
- **Spotlight** – An application in the Apple OS X operating system that indexes the contents of files and allows for subsequent searching of the index.
- **iTunes** - An application in the Apple OS X operating system that is used to “sync” and transfer data to and from devices running the iOS operating system.

4.0 Equipment, Materials and Reagents

- Macintosh laptop or desktop, running the OS X operating system, specifically designated for use in Mac forensics analysis
- Prepared target drive containing a RAW/DD image of the suspect device (if the device is a computer running OS X or an iPod that was connected to a USB write-blocker during imaging)
- External drive enclosure for the prepared target drive (if used) and appropriate cables

5.0 Procedure

5.1 If the suspect device is a computer running the Mac OSX Operating System:

5.1.1 Attach the external hard drive enclosure containing the target drive to the examination Mac laptop or desktop.

5.1.2 In Finder, locate the forensic image file of the suspect system on the target drive. Be careful not to mount the forensic image file before it has been locked (see limitations section below). Right-click or press ‘Command + I’ to open the “Get Info” dialog box in Finder. Select the “locked” radio button to lock the forensic image into read-only mode.

5.1.3 Mount the locked forensic image by double-clicking on the forensic image file.

5.1.4 If File Vault is enabled:

5.1.4.1 Create dictionaries for use in the decryption process.

5.1.4.2 Utilize the created dictionaries in concerted decryption attacks against the File Vaulted directory(s) using password cracking applications.

5.1.4.3 If the decryption efforts are successful, copy the File Vaulted Home directory to the target drive and decrypt it. Then, mount the unlocked Home directory for further examination.

5.1.5 Create a shadow file for the locked forensic image file. Mount the shadow file and index it for use in Spotlight.

5.1.6 Create a new user account for use in examining the suspect data. Enable “fast user switching” in the process.

5.1.7 Copy all relevant user data from the locked forensic image into the newly created forensic examination user account.

5.1.8 Log into the newly created forensic examination user account.

5.1.9 Utilize the native OS X applications on the forensic examination machine to examine the data in the newly created forensic examination user account.

5.1.10 Using the native OS X applications, create report artifacts by means of the built-in ‘print to PDF’ and screenshot capabilities.

5.2 If the suspect device is running the Mac iOS Operating System:

5.2.1 Create a new user account for use in examining the suspect data. Enable “fast user switching” in the process.

5.2.2 Using the newly created forensic examination user account, open the iTunes application. Set the option to prevent automatic syncing with the computer by selecting: iTunes → Preferences → and check the “Prevent iPods, iPhones, and iPads from syncing automatically” option.

5.2.3 Connect the device to the examination computer (see limitations section below).

5.2.4 Take a screenshot of the Summary tab of the iTunes application to record information concerning the device.

5.2.5 Right-click on the root of the device’s entry (on the left side of the screen) and select “Back-Up” from the menu. This will copy the contents of the device (see limitations section below) to the directory ~/Library/Application Support/MobileSync/Backup/(GUID for the device).

5.2.6 Upon successful completion of the backup process, remove the device from the examination computer.

5.2.7 Examine the contents of the device's backup files for data of relevance.

5.3 Standards and Controls - N/A

5.4 Calibrations - The Macintosh laptop or desktop used in casework shall be validated each day that it is used to ensure that the computer hardware and software are functioning properly. The procedure for this validation process can be found in the Digital/Latent Evidence Section Computer Performance Verification Procedure.

5.5 Maintenance – N/A

5.6 Sampling - N/A

5.7 Calculations - N/A

5.8 Uncertainty of Measurement - N/A

6.0 Limitations

6.1 Great care must be taken when selecting the forensic image file during the locking process. Double-clicking on a forensic image file before the file has been locked will mount the image file read-write in the operating system and will change data on the forensic image file.

6.2 The Apple OS X operating system has options to securely delete files, rendering them impossible to recover. Furthermore, due to the optimization routines on OS X file systems, it is possible that previously deleted files might not be recoverable because they have been overwritten by other data.

6.3 File Vault utilizes an AES-128 encryption scheme and is therefore virtually impossible to decrypt by means of brute-force.

6.4 Some iPhones are password protected and cannot be backed up to any account except the one under which it was registered. Furthermore, most iPhones are set to erase all of its data if the incorrect password is entered more than ten times.

6.5 Any iPhone (beyond version 2) can be remotely wiped by the user. Measures must be taken to prevent the iPhone from receiving RF signals whenever powered on.

6.6 A sync of an iPhone may, or may not, give the examiner access to voicemails and emails. A sync of an iPhone will not provide a copy of unallocated space for examination.

6.7 Due to the ease with which an iPod can be modified during the syncing process, it is recommended that any iPod be connected to a forensic USB bridge device before being connected to a computer.

7.0 Safety – N/A

8.0 References

- Procedure for Computer Performance Verification

- Mac OS X, iPod, and iPhone Forensic Analysis (Syngress Press, ISBN: 978-1-59749-297-3)

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