Technical Procedure for Apple Macintosh Preview

1.0 Purpose - The purpose of this procedure is to use the HELIX Linux operating system to preview evidence hard drives without altering the data on the hard drive.

2.0 Scope - This procedure describes the steps to be taken by personnel of the State Crime Laboratory to use the HELIX Linux operating system to preview computers running the Apple Macintosh operating system.

3.0 Definitions

- **FireWire Target Mode** – FireWire Target Mode allows an Apple Macintosh system to act as if the entire computer were an external FireWire hard drive for another system. This mode works at the firmware level before the operating system is engaged and booted. It is entered by holding down the "T" key on the Apple Macintosh system during the boot process.
- **HELIX** – HELIX is a Linux operating system variant that was specially constructed for forensic examination of live systems due to the fact that all media on the system is placed in read-only mode.
- **fstab** – fstab is a configuration file that contains information for all of the partitions and storage devices in a Linux-based computer including how and where the partitions and storage devices should be mounted.
- **HFS** - Hierarchical File System (HFS) is a file system developed by Apple for use in computers running the Apple Macintosh OS. HFS is also referred to as Apple Macintosh OS Standard. HFS+ - HFS Plus or HFS+ is a file system developed by Apple to replace their Hierarchical File System (HFS) as the primary file system used in Apple Macintosh computers (or other systems running Apple Macintosh OS). HFS Plus is an improved version of HFS, supporting much larger files (block addresses are 32-bit length instead of 16-bit) and using Unicode for naming the file items. HFS Plus also uses a full 32-bit allocation mapping table, rather than HFS's 16 bits. HFS Plus is also referred to as Apple Macintosh OS Extended.

4.0 Equipment, Materials and Reagents

- Forensic Tower
- FireWire (IEEE 1394) cable
- HELIX CD
- Prepared Target drive (as needed)

5.0 Procedure

5.1 With both systems powered off, connect the forensic tower to the Apple Macintosh using a FireWire cable.

5.2 Insert a power cable to any Apple MacBook or other Apple Macintosh laptop to be previewed. Do not allow a laptop to run on battery power during a preview or acquisition if the appropriate AC power cord is available.

5.3 Boot the Apple Macintosh and place in FireWire Target Mode by pressing the "T" key until a screen with a FireWire logo appears.

5.4 Boot the forensic tower into the HELIX environment.

5.5 When the HELIX environment has fully loaded, open a terminal session.

5.6 Navigate to the /etc directory.

5.7 Edit the fstab file. Navigate to the entry in the fstab file that corresponds to the HFS partition on the Apple Macintosh's hard drive and change the partition type from "hfs" to "hfsplus."

5.8 If there is a need to copy data off the Apple Macintosh during the preview, the Target drive must be mounted as read/write in the fstab file by changing the "ro" characteristic (Read-Only) to "rw" (Read-Write).

5.9 Close the terminal session.

5.10 On the HELIX desktop, click once on the Apple Macintosh hard drive icon to mount the drive. Repeat this process for the Target drive (if used) to mount the Target drive.

5.11 Preview the Apple Macintosh system using the tools of choice.

5.12 At the completion of the preview, power down the Apple Macintosh and disconnect the FireWire cable between the two systems.

5.13 The changes to the fstab file allow the HELIX environment to read the file system on newer Apple Macintosh systems while remaining in a read-only state.

5.14 Boot the Apple Macintosh into FireWire Target mode as this mode engages at the firmware level before the operating system is booted. To enter FireWire Target Mode, boot the Apple Macintosh and hold down the "T" key until a screen with a floating FireWire logo appears.

5.15 **Standards and Controls -** A control disk image with a known hash value is used to ensure the proper functioning of forensic computers used in casework.

5.16 **Calibrations -** The forensic towers used in casework shall be validated each day that they are 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.

5.17 **Maintenance –** N/A

5.18 **Sampling -** N/A

5.19 **Calculations -** N/A

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

6.0 Limitations

6.1 **NEVER** use a Microsoft Windows operating system to preview or image an Apple Macintosh system FireWire connection. Microsoft operating systems "touch" drives during the boot sequence. Furthermore, FireWire connections cannot be write-protected so there is no way to prevent writes to the Apple Macintosh system when mounted to a Windows OS.

6.2 If you are using another Apple Macintosh as the examination platform, turn off Disk Arbitration to ensure there are no inadvertent writes to the suspect Apple Macintosh system.

7.0 Safety – N/A

8.0 References

- Procedure for Computer Performance Verification

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