Technical Procedure for Mobile Device Extraction

1.0 Purpose –This procedure establishes a systematic process for data extraction from mobile devices.

2.0 Scope - This procedure describes the steps to be taken by personnel of the State Crime Laboratory in extracting data from mobile devices.

3.0 Definitions

- **Target drive** – A sterile piece of media used to store forensic image(s) and case related data.
- **Isolation** – Method to ensure that the device cannot connect to a network during examination.
- **SIM card** – The Subscriber Identity Module card used in some devices that allows the device to connect to a carrier network (AT&T, Verizon, Sprint, etc.). SIM cards may contain identifying information and other data.
- **SIM card Adapter** – A device used to connect the various types of SIM cards (micro or nano) to the forensic tool for extraction.
- **Micro SD card** – The micro SD (Secure Digital) card found in some devices that may contain user data.
- **Physical extraction** – A method of extraction that includes a bit-by-bit image of the flash memory of a device that contains system and user data to include deleted data, hidden data, and unallocated space.
- **File System extraction** – A method of extraction that includes the file system and user data of the device and may contain deleted data from databases in the file system.
- **Logical extraction** – A method of extraction that includes user data available through the device's Application Program Interface but does not include deleted data or unallocated space.
- **PIN** – The Personal Identification Number that may be enabled on devices or SIM cards to provide security for the device. If a PIN is enabled, the user will need to enter a PIN to unlock the device.
- **PUK** – The Personal Unlock Key is a code needed to unlock a SIM card after unsuccessful PIN attempts. A PUK code is generally only available from the network provider.
- **Passcode** – A password code set by the user to prevent access to the device that involves entering the passcode to unlock the device.
- **Pattern lock** – A type of security lock set by the user to prevent access to the device that involves drawing a pattern to unlock the device.
- **Fingerprint lock** – A type of security lock set by the user to prevent access to the device that involves scanning a fingerprint to unlock the device.

4.0 Equipment, Materials and Reagents

- Approved mobile device tools for data extraction (software or hardware)
- Forensic computer
- Target drive
- Set of cables and connectors
- Isolation equipment
- SIM card adapter

5.0 Procedure

5.1 Wipe the target drive with an approved data wiping utility prior to data extraction.

5.2 Ensure legal authorization.

5.3 Determine if a Physical, File System, or Logical extraction of the mobile device is supported by approved mobile device tools. Refer to the support documentation for each tool to determine support for individual devices. The level of extraction will depend on the support for the device.

5.4 Determine if the device contains a SIM card or removable media such as a micro SD card. All SIM cards and removable media shall be physically taken out of the device if possible prior to beginning the examination.

5.5 Conduct an extraction of the SIM card with a supported mobile device tool. For micro SIM cards or nano SIM cards, use a SIM card adapter. Determine if the SIM card is locked with a PIN or requires a PUK code. If a PIN was given at evidence submission, use the PIN to unlock the SIM. Do not attempt to unlock a SIM card without a known PIN or PUK code.

5.6 Use a mobile device tool to clone the SIM card onto an access SIM card. Insert the clone SIM card into the mobile device. In the event that a SIM card cannot be cloned, then it is permissible to conduct an extraction with the original SIM card in the device. This shall be documented in the case notes. If conducting an extraction with the original SIM card, do not insert the original SIM card back into the device until the device has been properly isolated.

5.6.1 To ensure proper isolation once powered on, place the device into airplane mode or flight mode if possible. Disable Wi-Fi and Bluetooth connections if necessary. Network isolation of the mobile device shall be maintained.

5.7 Conduct an acquisition of the removable media using an approved software or hardware tool (see Technical Procedure for Evidence Acquisition in Computer Forensic Examinations) before returning it to the mobile device. After acquisition is complete, insert the removable media back into the mobile device.

5.8 Determine if the device is locked (PIN, passcode, pattern lock, fingerprint lock, etc.) and whether or not approved mobile device tools support a password bypass. If a passcode was given at evidence submission, use the passcode to unlock the device. Do not attempt to unlock a mobile device without a known passcode as some devices can be set to lock or wipe after too many attempts.

5.9 Extract mobile device data onto a target drive using an approved mobile device tool. Refer to the mobile device tool support documentation for the appropriate procedural steps, cable connections, and settings for the device. Document the methods used to extract data from the device.

5.10 Ensure that the device maintains power during the extraction process. If no battery was submitted with the device or the battery does not function properly, then power-up data cables may be used to provide power.

5.11 When the extraction(s) are complete, the device shall be powered off and the battery removed if possible to prevent the device from inadvertently powering on after examination.

5.12 Create a report for the data extraction in an approved mobile device tool.

5.13 Copy the report to digital media to return to the submitting agency.

5.14 Copy the report to digital media to be retained in the Laboratory. This copy is for reference only.

5.15 If practical, copy the forensic images (extractions) onto digital media to be returned to the submitting agency along with the original evidence.

6.0 Standards and Controls

6.1 Use of Control Media does not apply to mobile device extractions due to the fact that mobile devices are powered on for extraction.

7.0 Calibrations – N/A

8.0 Maintenance – N/A

9.0 Sampling – N/A

10.0 Calculations – N/A

11.0 Uncertainty of Measurement – N/A

12.0 Limitations

12.1 Mobile devices present unique challenges due to numerous models of devices, proprietary software, rapid changes in technology, passcodes, and encryption. Not all mobile devices are supported by forensic tools. In the event that the mobile device is not supported by forensic tools, a Forensic Scientist may conduct a manual examination of the device. This shall be documented in the case notes. Isolation shall be maintained.

12.2 Mobile devices are powered on for extraction. A mobile device shall never be allowed to connect to a carrier network or Wi-Fi signal. Not utilizing proper isolation may result in the alteration of evidence or may allow a remote wipe signal to reach the device.

12.3 Some extractions may require the Forensic Scientist to utilize Bluetooth to obtain an extraction from the device. In the event that the forensic tool requires a Bluetooth extraction, it is permissible to pair the mobile device with the forensic tool through a Bluetooth connection.

12.4 Some extractions may require removable media to be inserted into the device if the removable media slot is empty. In the event that the forensic tool requires removable media, it is permissible to insert forensic media (wiped and formatted) into the device for extraction.

12.5 In the event that the mobile device has internal or external damage, the Forensic Scientist may determine the appropriate procedure for examination based on training and experience. If the battery appears to be damaged or swollen, use power-up cables instead of the battery.

12.6 Always proceed with caution when attempting passcodes on a mobile device. Some devices are set to lock or wipe after a set number of failed attempts. It is also unknown how many passcode attempts may have already taken place before the device was submitted to the Laboratory.

12.7 Mobile devices should be handled with caution. If possible, place the device into isolation before removing a protective case to prevent inadvertently powering on the device. Be aware of buttons on the side of the case that may power on the device or access a camera.

13.0 Safety – N/A

14.0 References

- Scientific Working Group on Digital Evidence Best Practices for Mobile Phone Forensics
- National Institute of Standards and Technology Guidelines on Mobile Device Forensics
- Cellebrite UFED User Manual
- XRY User Manual

15.0 Records – N/A

16.0 Attachments – N/A

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