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. The steps of examination may be omitted or worked in different sequential order based on the device and the scientist's training and experience.

3.0 Definitions

- **Target drive** – A sterile piece of media used to store forensic image(s) and case related data.
- **Mobile Device** – devices that are not desktop or laptop computers, to include, but not limited to, mobile phones, tablets, digital cameras, Global Positioning System (GPS) units, and unmanned aerial vehicles (drones).
- **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 biometric security mechanism set by the user to prevent access to the device that involves scanning a fingerprint to unlock the device.
- **Chip-Off Extraction–** A method of data extraction which involves the removal a flash memory chip from the printed circuit board (PCB) of a device and directly reading the binary data from the flash memory chip. This type of data extraction is considered destructive as the device will be permanently inoperable after the memory chip is removed from the PCB.
- **JTAG Extraction–** A method of data extraction which involves using a Joint Testing Action Group (JTAG) boundary scan technique to retrieve data from a flash memory chip. This type of data extraction is considered to be non-destructive.

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
- BGA Rework Station
- Riff Box

5.0 Procedure

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

5.2 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.

5.2.1 If it is determined that a chip-off or JTAG extraction is necessary, refer to the *XRY Advanced Acquisition Training Workbook* for guidance.

5.2.2 Since the chip-off extraction procedure is destructive in nature, written approval shall be obtained from the submitting agency prior to performing the procedure. The approval must include an acknowledgement by the submitting agency's investigating agent and the agent's supervisor of their understanding of the destructive nature of the chip-off extraction process and an indemnification agreement. Any consent collected under this requirement must be documented in FA, to include uploading any copy of consent collected to the FA object repository.

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

5.3.1 For purposes of reporting, SIM cards and SD/microSD cards shall be considered part of the mobile device; they should not be considered a separate item or sub-item. In order to identify a SIM card in the examination worksheet, the Integrated Circuit Card Identifier (ICCID) number or other identifiers must be used. SD/microSD cards must be identified in an examination worksheet using any available external identifiers or a physical description.

5.3.2 When generating results, SIM and SD/microSD cards must be documented separately from the mobile device in the Laboratory Report.

5.4 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.

If a SIM card is necessary for mobile device operability, 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.

5.5 To ensure proper isolation once powered on, place the device into approved isolation equipment (e.g. a Ramsey Box) prior to powering on the mobile device, and then place the mobile device into airplane mode or flight mode, if possible. Disable Wi-Fi and Bluetooth radios (unless a Bluetooth connection is necessary for an extraction). Network isolation of the mobile device shall be maintained until the Wi-Fi, Bluetooth, and cellular radios have been disabled.

5.6 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.

5.7 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. If the passcode is unknown and the approved mobile device tools support a password bypass attack, attempt to bypass the passcode.

5.8 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.

5.8.1 It may be necessary to use multiple mobile device tools on the same mobile device in order to get a holistic view of the data residing on the device and any removable storage media it may contain. In those instances, the examiner shall document which additional tools were used.

5.9 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.

5.10 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.

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

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

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.

12.1.1 Due to not all mobile devices being supported by forensic tools (no brute force support), the scientist shall return any extracted data; however, if forensic tool support becomes available or the submitting agency obtains the passcode, the mobile device may be resubmitted for further analysis.

12.1.2 If brute force attack is supported, after approximately nine (9) months of attempts, the scientist shall determine if further access attempts are warranted. If the scientist determines no further attempts are warranted, the extracted data shall be returned to the submitting agency.

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.

12.8 Due to the solid state storage in mobile devices, hashes of mobile device storage will typically not be consistent due to file system and medium optimization (i.e. garbage collection and wear-leveling), thus making it impractical to hash mobile devices during the examination. Hash values for removable media may be consistent, but removable media does contain the same optimization features seen in mobile device which can cause hash value variation.

13.0 Safety

13.1 Infrared (IR) light can cause permanent damage to the human eye. Since the chip-off extraction process uses an IR heater to dislodge a flash memory chip from a PCB, protective goggles must be worn at all times when the IR heat emitter is in operation.

13.2 Soldering irons and soldering material become extremely hot during use. Since the chip-off extraction process uses a soldering iron and soldering material, both the iron and material must not be touched while in use and given sufficient time to cool after use prior to touching.

14.0 References

- Scientific Working Group on Digital Evidence, *SWGDE Best Practices for Mobile Phone Forensics*, 2013, Version 2.0.
- Scientific Working Group on Digital Evidence, *SWGDE Best Practices for Chip-Off*, 2016, Version 1.0.
- Scientific Working Group on Digital Evidence, *SWGDE Best Practices for Examining Mobile Phones using JTAG*, 2015, Version 1.0.
- National Institute of Standards and Technology, *Guidelines on Mobile Device Forensics*, 2014, Revision 800-101 (Rev. 1).
- Micro Systemation AB, *XRY Advanced Acquisition Training Workbook*, 2017.

15.0 Records – A report generated by the mobile device examination tool containing device identification must be included in the case record object repository.

16.0 Attachments – N/A

Revision History		
Effective Date	Version Number	Reason
12/02/2020	5	2.0 – Updated scope 12.1.1 and 12.1.2 – Added sub-sections Corrected header information 15.0 - Added record for case file