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

Refer to the Digital Evidence Dictionary

4.0 Equipment, Materials and Reagents

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

5.0 Procedure

5.1 If the portable device is on when submitted to the laboratory, place the device in the isolation box to disable network connections and if necessary remove the SIM card. If the portable device is off when submitted into the laboratory, 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).

5.1.1 If the SIM card is unable to be removed prior to powering on the device or the settings are unable to be enabled/disabled, the device needs to be isolated from any networks either in an isolation box or bag. Network isolation of the mobile device shall be maintained until the Wi-Fi, Bluetooth, and cellular radios have been disabled or examination is complete.

5.2 Inspect the evidence for physical damage. If damage is present, it must be documented in the analyst's case notes.

5.3 Label the evidence using permanent marker or an evidence label in accordance with the Laboratory Procedure for Evidence Management. Avoid placing identifying marks on removable labels present on the evidence.

5.4 Information specific to the evidence (e.g., type/size of media, manufacturer, labels, and status of any write protection feature) must be documented in case notes.

5.5 The technician and/or assigned forensic scientist shall photograph the front and back of the device and put the pictures in the case notes.

5.6 Determine if the device was submitted with a SIM card or other removable media such as a micro SD card. Based on the tool being used the SIM card and removable media may be left in the phone or physically taken out of the device prior to beginning the examination.

5.6.1 SIM Cards

5.6.1.1 Prior to SIM Card extraction a control media shall be examined

5.6.1.2 Conduct an extraction of the SIM card with a supported mobile device tool and 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 PUK is present, this shall be documented in the case notes.

5.6.1.3 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, if possible.

5.6.2 SD Cards and other removable media

5.6.2.1 Prior to evidence media examination the write-blocker shall be tested using the WiebeTech WriteBlocking Validation Utility and a control media with known hash value shall be examined.

5.6.2.1.1. Connect the control media to the forensic tower through the use of a write-blocker.

5.6.2.1.2. Use the forensic software tool to obtain an initial hash value of the control media.

5.6.2.1.3. If the known hash value and the initial hash values match, then the forensic software tool is verified for use.

5.6.2.2 Insert the SD card into the forensic tower using a SD card adapter.

5.6.2.3 Use a forensic software tool to obtain an initial hash value of the SD card.

5.6.2.4 Use a forensic software tool to obtain an extraction of the SD card and onto the target drive.

5.6.2.5 Use a forensic software tool to obtain a post hash value of the SD card.

5.6.2.6 Verify that the extraction completed successfully and that the initial hash value for the SD card matches the post hash of the SD card.

5.6.3 For purposes of reporting, SIM cards and SD/microSD cards shall be considered part of the mobile device and not 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 and/or a physical description.

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

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 Determine the best extraction supported by the approved forensic software tools for the mobile device. 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.

5.9 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 bypass data cables may be used to provide power.

5.10 Wipe the target drive with an approved data wiping utility prior to data extraction. A transfer drive may be used instead of a target drive without wiping.

5.11 Extract mobile device data onto a target or transfer 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.

5.11.1 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.

5.12 Transfer the extraction from the transfer media to a forensic tower for processing. Once the extractions are transferred to the forensic tower, the extractions need to be processed using the proper mobile device tool. Reports shall be created for the data extractions using an approved mobile device tool.

5.12.1 If data extraction is performed using GrayKey and Cellebrite is used to process the extraction, a GrayKey Report, a device information report (Cellebrite Device Information Report), and a Cellebrite reader report (portable case) shall be generated and included in the Laboratory Case File and evidence media.

5.12.2 If data extraction and processing is performed using Cellebrite, a device information report (Cellebrite Device Information Report) and a Cellebrite reader report (portable case) shall be generated and included in the Laboratory Case File and evidence media.

5.12.3 If data extraction is performed using GrayKey and Axiom is used to process the extraction, a GrayKey Report shall be generated and included in the Laboratory Case File and evidence media, and an Axiom Portable Case shall be generated and included in evidence media.

5.12.4 If data extraction and processing is performed using Axiom, an Axiom Portable Case shall be generated and included evidence media.

5.13 When the extraction(s) are complete, the device shall be powered off and any removable media shall be returned to the submitting agency, separated from the device.

5.13.1 If one Digital Evidence section member performs a data extraction on a mobile device and the device is transferred to another Digital Evidence section member for analysis, a verification of the extracted data shall be performed and documented in the examiner's notes. A verification review shall be completed in the Forensic Advantage system.

5.14 All reports and extractions shall be copied to digital media and returned to the submitting agency at the completion of the examination. For SIM card only extractions, only the device information report is required. This report may be transmitted to the submitting agency through Forensic Advantage.

5.15 Results of Examination – A narrative-driven reporting method shall be used. In order to establish consistency within laboratory reports with regard to digital forensic examinations, the following items shall be, at a minimum, included within a laboratory report:

- The methodology used during the examination
- Item(s) examined and any removeable media present
- What type of examination was requested (e.g. mobile device, security bypass, etc.)
- Under what authority the exam was performed (e.g. search warrant, consent, no expectation of privacy, etc.)
- Type of extraction(s) obtained
- If a passcode was identified and the result of the passcode
- Reports generated during the examination

The following are examples for report wording. The examples may be modified based on the case circumstances.

5.15.1 Methodology

5.15.1.1 The following methodologies were used in the examination of this case: visual examination, mobile device extractions, and processing.

5.15.2 Cell Phone Extraction: Examination of (Item number) found it was protected by a (type of password). The passcode was identified as (passcode). (Item number) contained a SIM Card.

5.15.3 Extraction Statements:

5.15.3.1 Physical Extraction: (Item number) was extracted, processed, and user reports were generated. A physical extraction and SIM card extraction were obtained.

5.15.3.2 Full File System Extraction: (Item number) was extracted, processed, and user reports were generated. A full file system extraction and SIM card extraction were obtained.

5.15.3.3 Partial File System: (Item number) was extracted, processed, and user reports were generated. A partial extraction and SIM card extraction were obtained. Currently, only a partial extraction is available for this device. Should vendor support for another extraction become available or the submitting agency obtains the passcode and further analysis be required, the submitting agency may resubmit Item _ .

5.15.3.4 No support: A data extraction was attempted, and these attempts were unsuccessful. Currently, there is no forensic tool support for this device at the Laboratory; however, the tools are constantly being updated by the vendors as new devices and updated operating systems are released. Should vendor support become available and further analysis be required, this item may be resubmitted.

5.15.4 (Container number) was created and contains the following: (list reports created below in bullet formatting)

5.15.5 Contraband results

5.15.5.1 The Cellebrite report contained in Container (number) may contain contraband and is intended for use by law enforcement in an official criminal investigation. It is highly recommended that any device used to view the Cellebrite report and the material it contains be disconnected from any network, including the Internet. Dissemination of this material may result in criminal prosecution.

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.

6.2 Hash values are required to be created throughout the examination process in accordance to Appendix A.

6.2.1 If an AXIOM or Cellebrite UFED 4PC Advanced Logical extraction is obtained, hashing is not required.

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.

12.1.1.1 If the phone is powered off or in the Before First Unlock state and not supported by forensic tools, the phone will be returned.

12.1.1.2 If the phone is powered on and in the After First Unlock state, the submitting agency will be contacted to notify them about the tool support status and the phone will be retained for 30 days to see if supports becomes available. If after 30 days support is still not available, the submitting agency will be contacted to determine how to proceed with the examination.

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 bypass 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 should be consistent.

13.0 Safety

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 Mobile Device Evidence Collection & Preservation Handling and Acquisition,* 2020, Version 1.2.
- Scientific Working Group on Digital Evidence, *SWGDE Best Practices for Collection of Damaged Mobile Devices,* 2016, Version 1.1
- Scientific Working Group on Digital Evidence, *SWGDE Best Practice for Mobile Device Forensic Analysis*, 2020, Version 1.0
- Scientific Working Group on Digital Evidence, *SWGDE Digital & Multimedia Evidence Glossary*, 2016, Version 3.0.
- Scientific Working Group on Digital Evidence, *SWGDE Best Practices for Digital Evidence Collection,* 2018, Version 1.0
- Scientific Working Group on Digital Evidence, *SWGDE Focused Collection and Examination of Digital Evidence,* 2014, Version 1.0
- Scientific Working Group on Digital Evidence, *SWGDE Core Competencies for Mobile Phone Forensics,* 2013, Version 1.0
- Laboratory Procedure for Evidence Management
- Laboratory Procedure for the Physical Inspection of Digital Evidence
- Laboratory Procedure for Obtaining Evidentiary Standards
- National Institute of Standards and Technology, *Guidelines on Mobile Device Forensics*, 2014, Revision 800-101 (Rev. 1).

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 –

Appendix A**– Required Hash Values**

Revision History		
Effective Date	Version Number	Reason
08/02/2024	7	5.0 - Moved information to maintain a better workflow 5.1.1 – Updated language 5.5 – Updated location of photographs 5.6.1.2 – Update language 5.6.2.2 – Update language 5.6.2.3 – Update language 5.6.2.4 – Update language 5.6.2.5 – Update language 5.12 – Update language 5.12.1 – Update report names 5.12.2 – update report names 5.16 – update results of examinations and examples 14 – Updated references

Appendix A – Required Hash Values

Mobile Device:
Extraction Hash
Verification Hash, if more than one employee is involved in the extraction
Post-examination Extraction Hash

SD Card:
Pre-extraction Hash of SD Card
Post-extraction Hash of SD Card
Extraction Hash
Verification Hash, if more than one employee is involved in the extraction
Post-examination Extraction Hash

Secure Folder:
Extraction Hash
Verification Hash, if more than one employee is involved in the extraction
Post-examination Extraction Hash