A. Purpose:

To outline the steps taken to analyze cell phones. A Cell phone analysis request means that the internal memory of the device will be extracted, as well as onboard memory card(s)s /SIM card(s). The extraction(s) will be parsed using a software program(s). Searches and other in depth analyses will be conducted on the parsed data. A laboratory report of the analysis results is produced and provided to the requesting agency.

B. Responsibility:

Forensic Examiners

C. Definitions/Abbreviations:

Refer to CC SOP-26 - Definitions and Abbreviations.

D. Procedure:

1. The technique used for the examination of cell phones should be determined by, but not limited to, the examiners training knowledge and experience.
2. Current acceptable techniques for data extraction and analysis include:
   a. Using the CelleBrite UFED Touch Unit or UFED 4PC software to extract data contained on the cell phone and using the UFED Physical Analyzer software to parse and analyze data contained on the cell phone by following the manufacturer's protocol, as well as, the examiner's training and experience;
   b. Using Oxygen Forensic Suite software to extract data contained on the cell phone by following the manufacturer's protocol, as well as, the examiner's training and experience;
   c. Manually scrolling through the cell phone and recording relevant information pertaining to the request for analysis.
   d. Graykey can used for extraction of data from iPhone devices.
3. Every effort should be taken to ensure that the cell phone is protected from receiving an external signal. For example, using the Ramsey Shielded Test Enclosure.
4. If a different method is used to analyze the cell phone, thoroughly document it in the Cell Phone Worksheet\Notes (QR-CC-16) and all other appropriate records. In addition, bring this method to the Technical Lead and/or the Unit Supervisor's attention for further review.
5. If a passcode locked Apple device has been submitted for analysis refer to CC SOP-50 and CC SOP-53.
6. If a custom passcode or pattern locked device has been submitted for analysis and current methods cannot bypass or determine the code, submit a Cell Phone Passcode Needed Notification Letter (QR-CC-51) to the submitting agency. If the passcode cannot be provided within 5 business days, the evidence should be returned to the agency with a report stating the analysis could not be conducted.

References:

1. CelleBrite UFED Touch user manual or training documentation.

2. Oxygen Forensic Suite user manual or training documentation.