Technical Procedure for Cellular Telephone Deleted Data Extraction

1.0 Purpose – The purpose of this procedure is to extract deleted data from cellular telephones compatible with the Cellebrite UFED Physical Analyzer or XRY.

2.0 Scope - This procedure describes the steps to be taken by personnel of the State Crime Laboratory in extracting data from various types of cellular telephones which may be submitted.

3.0 Definitions

- **Cellebrite** – A universal forensic extraction device for cellular telephones.
- **XRY** – Forensic extraction software for cellular telephones.
- **SAN** – Networked array of hard drives used as a digital evidence repository.
- **Case Folder** – A folder designated by case number and located on the SAN, for use in a specific investigation.
- **UFED Physical Analyzer** – A software product created by Cellebrite for the extraction of deleted content from cellular telephones.

4.0 Equipment, Materials and Reagents

- Cellebrite unit with catalog of cellular telephone adapter cables
- XRY software with catalog of cellular telephone adapter cables
- Thumb drive
- Online SAN drive
- Forensics computer with UFED Physical Analyzer installed

5.0 Procedure

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

5.2 Place the telephone into airplane mode (if supported).

5.3 Cellebrite Instructions

5.3.1 Follow the instructions in Chapter 3 (Performing Data Extraction) of the UFED Physical Analyzer 2.0 user manual.

5.3.2 Once the data has been extracted by the Physical Analyzer, click “Open in Physical Analyzer.”

5.3.3 Once the preprocessing component is completed, you will be able to view deleted content from the cellular phone through the Physical Analyzer program.

5.3.4 A report shall be generated using the instructions in Chapter 5.6 (Generating Reports) of the UFED Physical Analyzer 2.0 user manual.

5.4 XRY Instructions

5.4.1 Follow the instructions in Getting Started: Starting a New Extraction of the XRY User Manual for data extraction

5.4.2 Once the data has been extracted by XRY, click "Finish."

5.4.3 Once the preprocessing component is completed, you will be able to view deleted content from the cellular phone through XRY.

5.4.4 A report shall be generated using the instructions in the Export portion of the XRY user manual.

5.5 The thumb drive should then be used to transfer the report from the forensic computer to the case folder located on the SAN storage drive.

5.6 Standards and Controls – N/A

5.7 Calibrations - There is no calibration required due to the variability of cellular telephone models on the market and the lack of a universal standard for performance verification.

5.8 Maintenance – N/A

5.9 Sampling – N/A

5.10 Calculations – N/A

5.11 Uncertainty of Measurement – N/A

6.0 Limitations - A cellular telephone should be powered off when submitted for analysis. During processing it is necessary to power on the telephone; the device should not be allowed to connect to its cellular network. Allowing the telephone to receive a signal from the cellular network can result in a change in the data contained on the internal memory of the telephone.

7.0 Safety – N/A

8.0 References

- UFED Physical Analyzer 2.0 user manual
- XRY User Manual

9.0 Records – N/A

10.0 Attachments – N/A

Revision History		
Effective Date	Version Number	Reason
09/17/2012	1	Original Document
05/03/2013	2	1.0-Change to reflect that XRY is included 3.0- Added XRY to the definitions 4.0-Added XRY to the Equipment list 5.3-Moved all Cellebrite instructions from 5.4 and 5.5 and placed them under 5.3 5.4-Created a new 5.4 in order to explain how to use XRY to find and extract deleted content 5.5-Moved information for Cellebrite to 5.3 8.0-Added XRY User Manual to the References list