A. Purpose:

To outline the steps taken to retrieve and analyze data stored in cloud storage. Evidence may be submitted with a cell phone analysis request or other request that applies to devices that use cloud storage for backup. The internal memory of these devices will be extracted, as well as onboard memory card(s) /SIM card(s). The extraction(s) will be parsed using approved software program(s). Searches and other in-depth analyses will be conducted on the parsed data including the data related to information stored in cloud storage. A laboratory report of the analysis results will be produced to provide to the requesting agency.

B. Responsibility:

Forensic Examiners or analysts assigned to the Computer Crimes Forensic Unit

C. Definitions/Abbreviations:

Refer to CC SOP-26 - Definitions and Abbreviations.

D. Procedure:

1. The technique used for the examination of cell phones or other mobile devices should be determined by, but not limited to, the examiner's training knowledge and experience.

2. Current acceptable techniques for data extraction and analysis include:
    a. Using the Cellebrite UFED Touch Unit, UFED 4PC or comparable approved software to extract data contained on the cell phone or mobile device and using the UFED Physical Analyzer software to parse and analyze data recovered from the device by following the manufacturer's protocol, as well as, the examiner's training and experience.

    b. Using the Cellebrite UFED Cloud Analyzer software to extract the data from cloud storage accounts that were identified and parsed out by the UFED Physical Analyzer software. An Account Package folder containing the storage account credentials is produced.

3. Once the cloud storage account information is recovered through the use of the UFED Physical Analyzer software, the Account Package folder can be copied to an external hard drive which will then be connected to a computer with Internet access and the UFED Cloud Analyzer software installed on it. If the examiner is using their forensic

system, access to the Unit's intranet should be disabled before enabling Internet access. For guidance, refer to CC SOP-19 (QC Protocol – Forensic Computer).

If the credentials are provided in a different manner, this information can be entered and used for the recovery of cloud storage account information.

4. Following the software import procedures, the Account Package data will be imported into the UFED Cloud Analyzer software and relevant case information will be input into the software.

5. A recovery of the data contained in the cloud storage accounts will be conducted and the extracted data will be saved to the external hard drive. Using the software a UFDR report will be generated for this data to be later analyzed by the examiner using the UFED Physical Analyzer software.

6. A report and attachment data of the results will be produced following the laboratory reporting protocol (Refer to CC SOP-09-Laboratory Report Protocol).

References:

Cellebrite UFED Touch, UFED4PC, and UFED Cloud Analyzer software user manual or training documentation.

CC-SOP-18: Cell phone analysis protocol

Note:

UFED Cloud Analyzer usage for probation and parole cases:

The UFED Cloud Analyzer software will be used on an as needed basis for probation and parole cases based on the examiner's training and experience along with the examination of information that was recovered by the UFED Physical Analyzer software. If another agency becomes involved in the case, refer to the next paragraph for guidance.

UFED Cloud Analyzer usage for non-probation/parole cases:

If a search and seizure warrant is not provided that refers to cloud data, the examiner should refer this case to Case Management to seek guidance from the submitting agency or the State's Attorney/U.S. Attorney's Office on whether analysis may proceed.