Procedure 12.26	Eugene Police Department
EFFECTIVE DATE 5-18-18	

Cellebrite Kiosk

12.26.1 PURPOSE AND SCOPE

The Cellebrite Kiosk located in the Property Crimes Unit work area is available for all trained and certified staff to use for cellphone extractions for investigative information and evidence. A list of the staff members who are authorized to operate the system is available in multiple locations of the kiosk cubicle. The Forensic Evidence Unit (FEU) should be consulted for all questions and assistance in using the kiosk. All evidence will be handled in accordance with established policies and procedures.

12.26.2 EXTRACTION DEFINITIONS

a. Logical – Is limited to what is present on the phone, not hidden or deleted content and not any photos from third party applications. Retrievable data: *SMS, Contacts, Call Logs, Media, App data.*

b. File System – This is similar to logical extractions but copies a file system which could include some hidden and deleted information. Retrievable data: *SMS, Contacts, Call Logs, Media, App data, Files, Hidden files.*

c. Physical – This extraction is the most comprehensive and detailed. The extraction accesses both allocated and unallocated space in the phone's physical memory. This can include GPS locations, web history, data on images, wi-fi networks and other system data. Retrievable data: *SMS, Contacts, Call Logs, Media, App data, Files, Hidden files, Deleted data.*

12.26.3 EXTRACTION TYPES

a. **iPhones** – The password for iPhone 5S and newer must be known for processing to be completed Processing should be possible on most iPhones older than the 5S. Two options are available because physical extractions cannot be completed using the Kiosk. If desired, this work can be performed by the FEU. Processing should be conducted in this order:

1. File System extraction
2. Logical extraction

b. **Android** - Three options are available. Extractions may also be performed on locked phones by following the prompts. Processing should be conducted in this order:

1. Physical extraction – (*This type can only be read and processed at FEU*.)
2. File System extraction
3. Logical extraction

12.26.4 KIOSK OPERATION

a. All SD and SIM memory cards (if present) should be removed from the phone and processed first using the designated ports on the kiosk. Follow the prompts related to these specific extractions.

b. Remove the case on the phone to find the correct model number of the phone. This number may be under the battery on an Android or Google phone.

c. Attach the cellphone and follow the prompts on the kiosk for the correct cables, phone model and extraction types available for that phone.

12.26.5 SAVING EXTRACTIONS

a. All evidence extractions and kiosk photos (if taken) must be saved in the designated "Large Digital Evidence" folder (LDE UPLOAD) on Server A04. (Please refer to the handling instructions posted in the kiosk work area)

b. The Evidence Control Unit (ECU) must be notified of the upload via e-mail.

c. The completed Kiosk Processing Worksheet (Appendix A, and located at the kiosk) should be saved with case notes. A second copy of the Logical extraction can be saved to a thumb drive for use by the staff person conducting the extraction.

12.26.6 CELLPHONE HANDLING

a. When processing a cellphone it must be rendered safe and secure. This is recommended even for processing at the kiosk but is an absolute necessity for processing at FEU.

1. Access the phone with a passcode if available. Document the passcode.
2. Place the phone in "AIRPLANE" mode.
3. Set screen to NEVER lock.
    a. For iPhones follow these steps:
    Settings > Display and Brightness > Auto-Lock (set to NEVER)
    b. For Android phones follow these steps:
    Menu > Settings > Lock screen & Security > Screen lock type > Pin or Fingerprints > Enter current pin # > Lock type select "NONE"
    c. Do <u>not</u> power off!

b. If being submitted for FEU processing:

1. Transport in a faraday bag or wrap the phone in 5 complete layers of tinfoil.

2. Submit to ECU in cabinets designated with faraday bags equipped with charging cables (Please refer to the Evidence Packaging Manual).

12.26.7 FORENSIC EVIDENCE UNIT PROCESSING

a. Only cellphones with possible evidence of criminal activity should be sent to FEU for processing.

b. Apple devices, GPS units and Blackberry devices are best processed at FEU with Physical Analyzer software. The software at FEU is required to perform Physical Extractions (recoveries) on iPhones and to read the physical extraction data from Android phones. FEU's processing includes the data organization and searching.

12.26.8 iPHONE WITHOUT A PASSWORD

a. There are limited options remaining if the password is unknown or unavailable for accessing an Apple device and the device is not supported by Cellebrite. The following are three remaining options:

1. Collect the computer (with any passwords to access them) in which the phone is commonly synced to iTunes. Playlist files that are generated when a phone is synced to iTunes can be used in Cellebrite as the encryption key bypass to unlock the device.

2. A chip-off process may be performed when all other options have been exhausted. A chip-off process includes removing the storage chip from the phone, and installing it into an accessible phone in order to view the chip contents.

   Use of this option will destroy the device. This process is currently being referred to an outside agency. Contact FEU for information.

3. Send to Cellebrite for an extraction. EPD is allotted one free extraction per year so this option is reserved for critical cases. The Investigation Division Lieutenant must determine if this case reaches the level necessary to approve sending the phone to Cellebrite.

Chris Skinner
Chief of Police