ORANGE COUNTY
SHERIFF'S DEPARTMENT

Training Bulletin

Computer Forensics Detail – Evidentiary Mobile Device Booking Procedures

Background

As mobile devices (i.e. cell phones & tablets) have become a fundamental part of our lives, most investigations now involve searching and seizing such devices for evidentiary purposes. Due to stronger security measures, there are new challenges to successfully extract and examine data from these devices. The most pressing challenge deals with the encryption of data. Most devices are encrypted and secured with a passcode, swipe pattern, or other security measure. To decrypt the data, bypassing or obtaining the passcode is vitally important. Forensic software utilized by the Computer Forensics Detail (CFD) can assist in bypassing some of these security measures without a known passcode, however, the success rate, speed at which this can be done, and the amount of data that can be obtained depends on the powered on/off state of the device when it arrives at the lab.

Solution

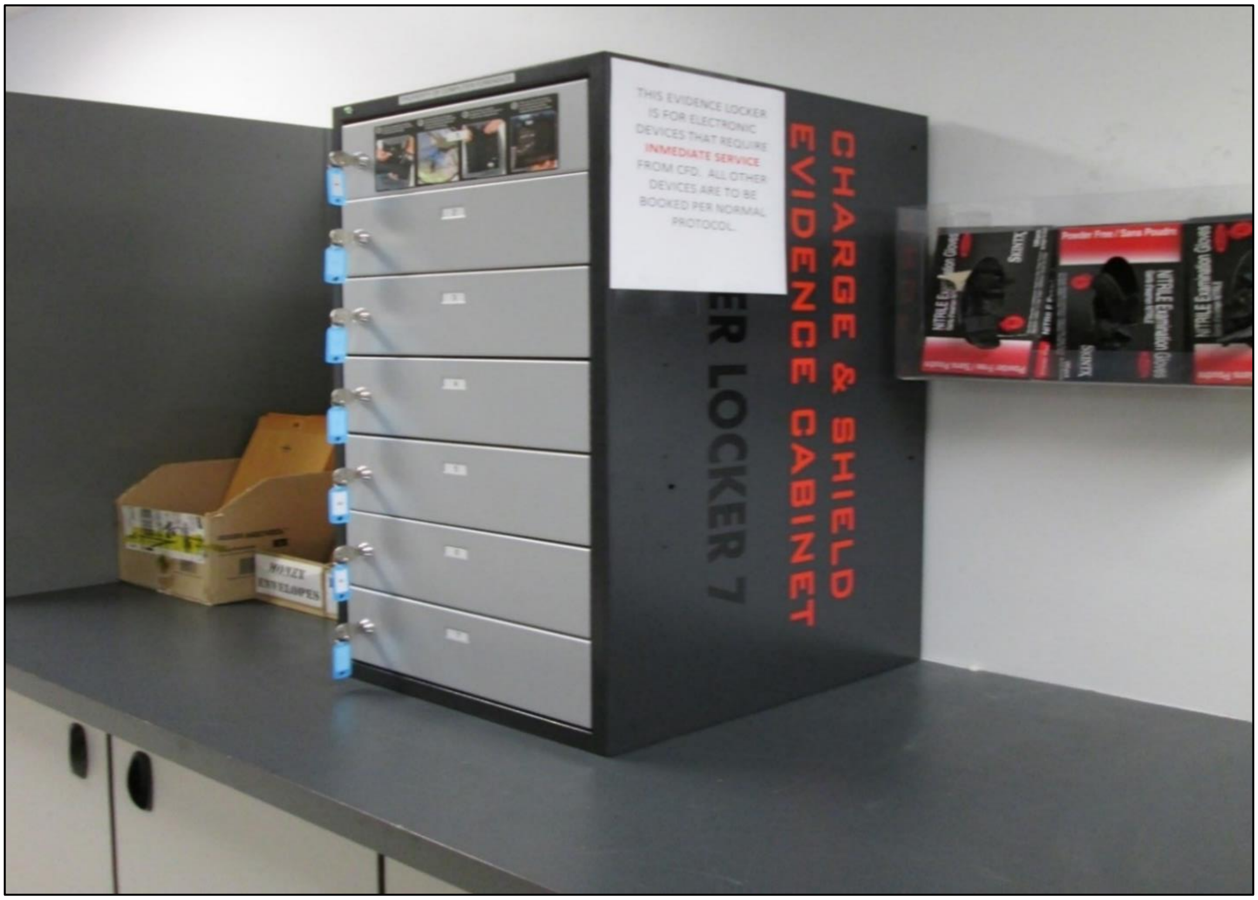
The Department has recently deployed a cell phone locker at the Brad Gates Building Property/Evidence Booking Station to accommodate devices with unknown passcodes, so they can be connected to power while the proper legal search authority is being sought (search warrant, consent, PRCS or probation terms). Only devices suspected of containing evidentiary data to support an investigation should be considered for examination. **Only devices with unknown passcodes should be placed into the cell phone locker.** All other devices should be isolated from their networks (Airplane mode enabled, WiFi & Bluetooth turned off), powered down, and booked into a regular Property/Evidence locker. Personnel should document each step that is taken prior to booking a device in their police report, as any manipulation will alter metadata.

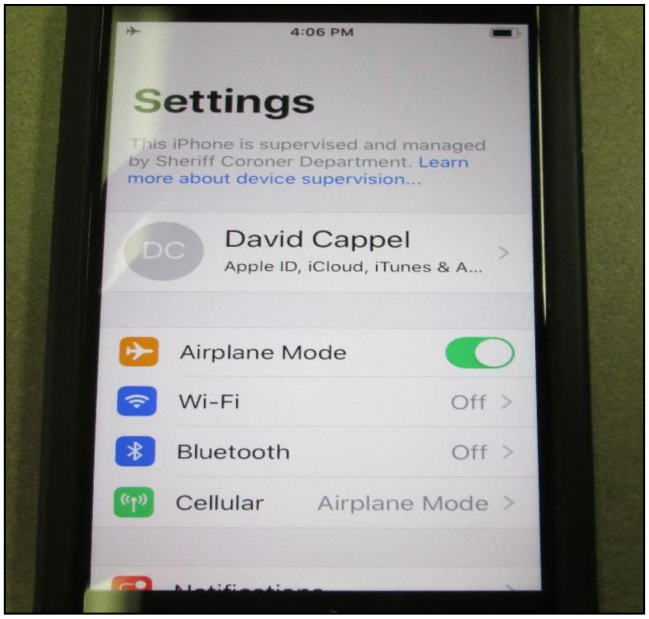
PROCEDURES FOR BOOKING & SUBMITTING A DEVICE FOR FORENSIC EXAMINATION:

- Isolate device from network by placing it into Airplane Mode with Wi-Fi & Bluetooth turned off.
- Enter the item into the P.E.A.B.I.T.S (Remedy) System.
- Place device into manila envelope with the charging port accessible; write initials, PIN and date on outside of envelope; staple evidence tag to manila envelope; write initials & PIN in lower left hand corner of tag. **DO NOT** seal manila envelope or affix barcode sticker to envelope.
- Open available locker bay of Blocker Locker 7 cell phone locker (only at Brad Gates location).
- Place envelope with the device into the black nylon faraday bag.
- Connect the device to power cable (outside zippered pouch has assorted cables for each brand of device).
- Place Remedy barcode sticker in the larger windowed sleeve on outside of faraday bag.
- Seal faraday bag; place it back into locker; close & lock the door, drop key into lockbox on left side.
- Complete Digital Media Examination Request form found in the Document Center (keyword: “computer”).
- Email completed form to: computerforensics@ocsheriff.gov, along with proper search authority.

(See the following illustrated instructions for further details)

ONLY EVIDENTIARY PHONES WITH UNKNOWN PASSCODES SHOULD BE BOOKED INTO THIS LOCKER


THIS EVIDENCE LOCKER IS FOR ELECTRONIC DEVICES THAT REQUIRE IMMEDIATE SERVICE FROM CFD. ALL OTHER DEVICES ARE TO BE BOOKED PER NORMAL PROTOCOL.
CHARGE & SHIELD
EVIDENCE CABINET
ER LOCKER 7


4:06 PM

Settings

This iPhone is supervised and managed by Sheriff Coroner Department. Learn more about device supervision...

DC David Cappel
Apple ID, iCloud, iTunes & A...

Airplane Mode ●

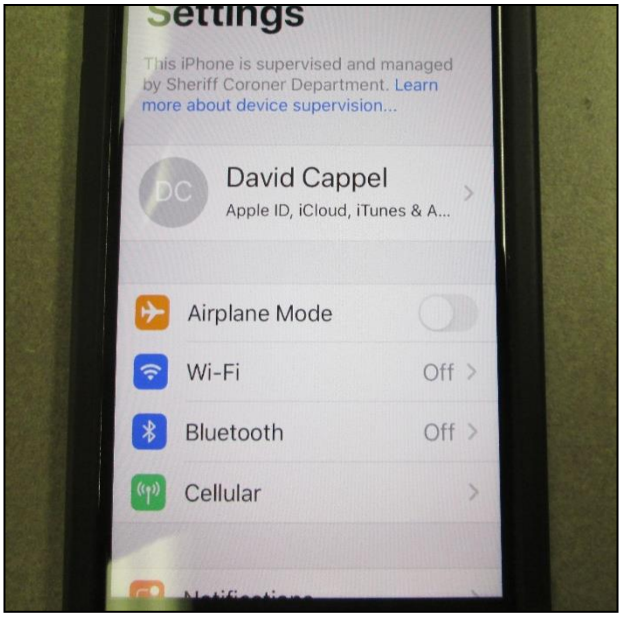
Wi-Fi Off >

Bluetooth Off >

Cellular Airplane Mode >

Notifications

Enable airplane mode


Settings

This iPhone is supervised and managed by Sheriff Coroner Department. Learn more about device supervision...

DC David Cappel
Apple ID, iCloud, iTunes & A...

Airplane Mode ○

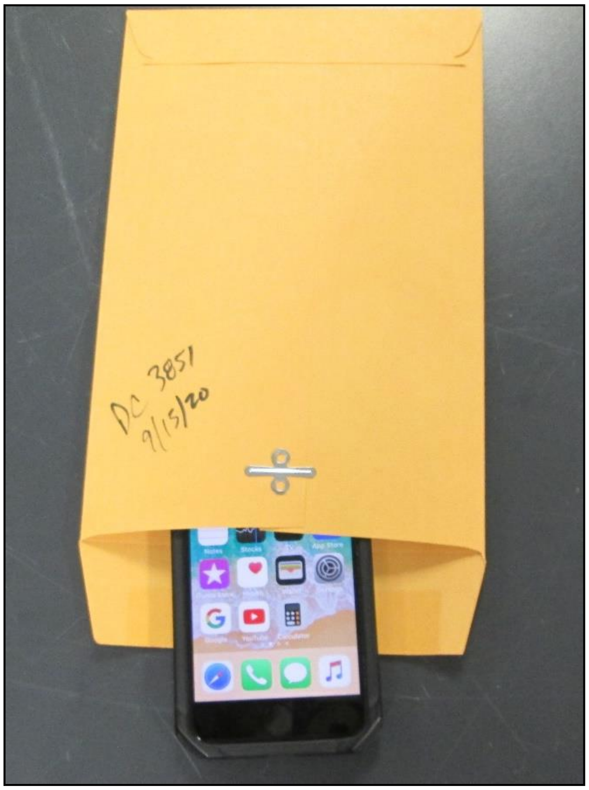
Wi-Fi Off >

Bluetooth Off >

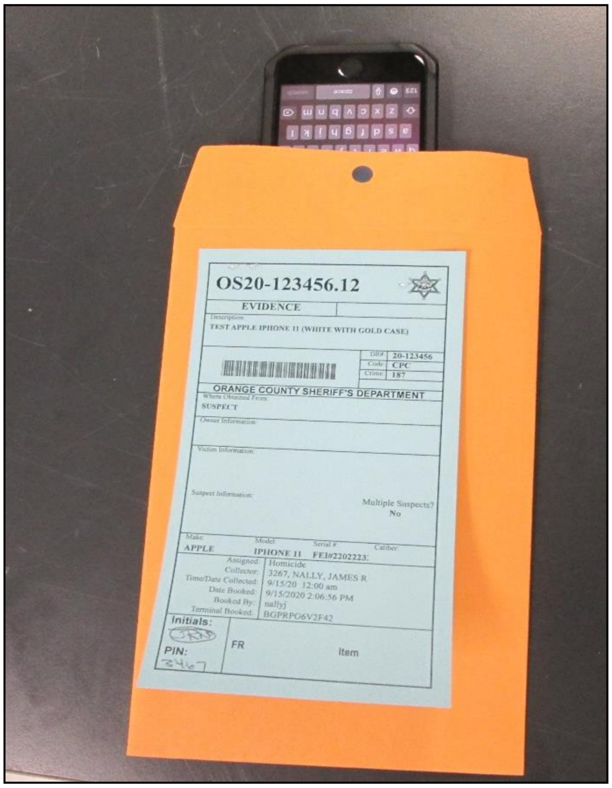
Cellular >

Notifications

Ensure Wi-Fi and Bluetooth are off



Initial, pin and date unsealed envelope



OS20-123456.12

EVIDENCE

Description:
TEST APPLE IPHONE 11 (WHITE WITH GOLD CASE)

DR#: 20-123456
Code: CPC
Crime: 187

ORANGE COUNTY SHERIFF'S DEPARTMENT

Where Obtained From:
SUSPECT

Owner Information:

Victim Information:

Suspect Information:

Multiple Suspects?
No

Make: APPLE
Model: IPHONE 11
Serial #: FEI#2202223:
Caliber:

Assigned: Homicide
Collector: 3267, NALLY, JAMES R
Time/Date Collected: 9/15/20 12:00 am
Date Booked: 9/15/2020 2:06:56 PM
Booked By: nallyj
Terminal Booked: BGPRPO6V2F42

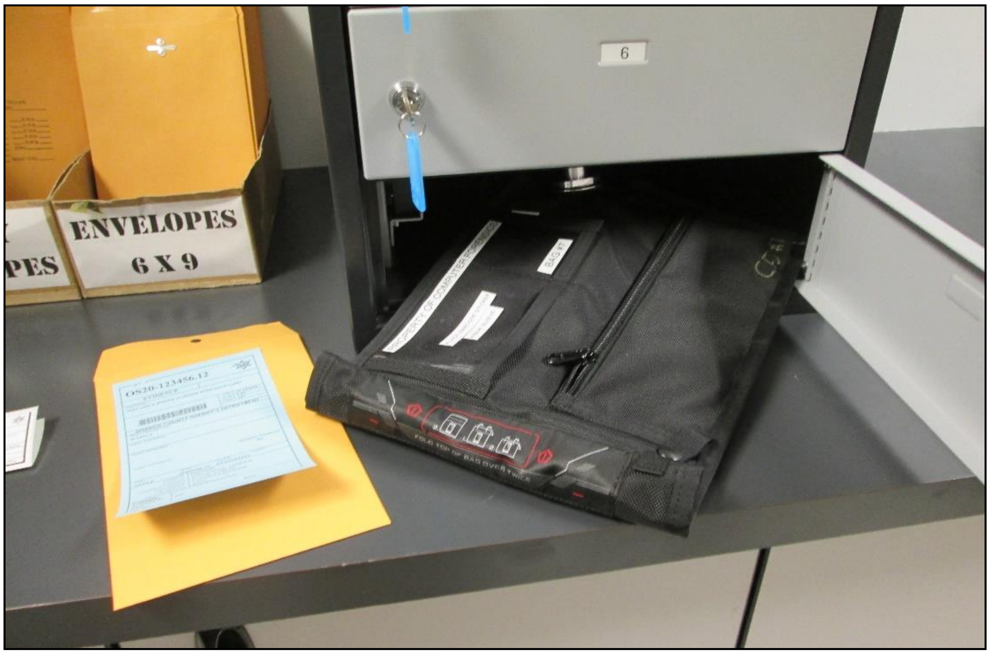
Initials: JRN

PIN: 3467

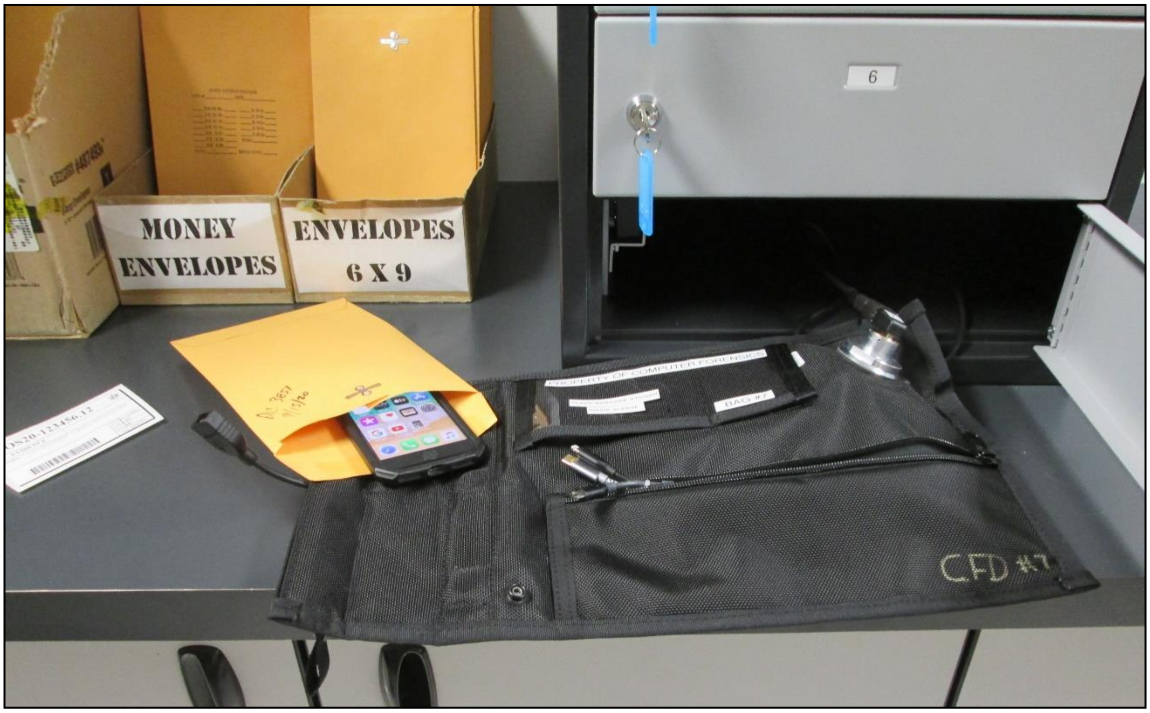
FR

Item

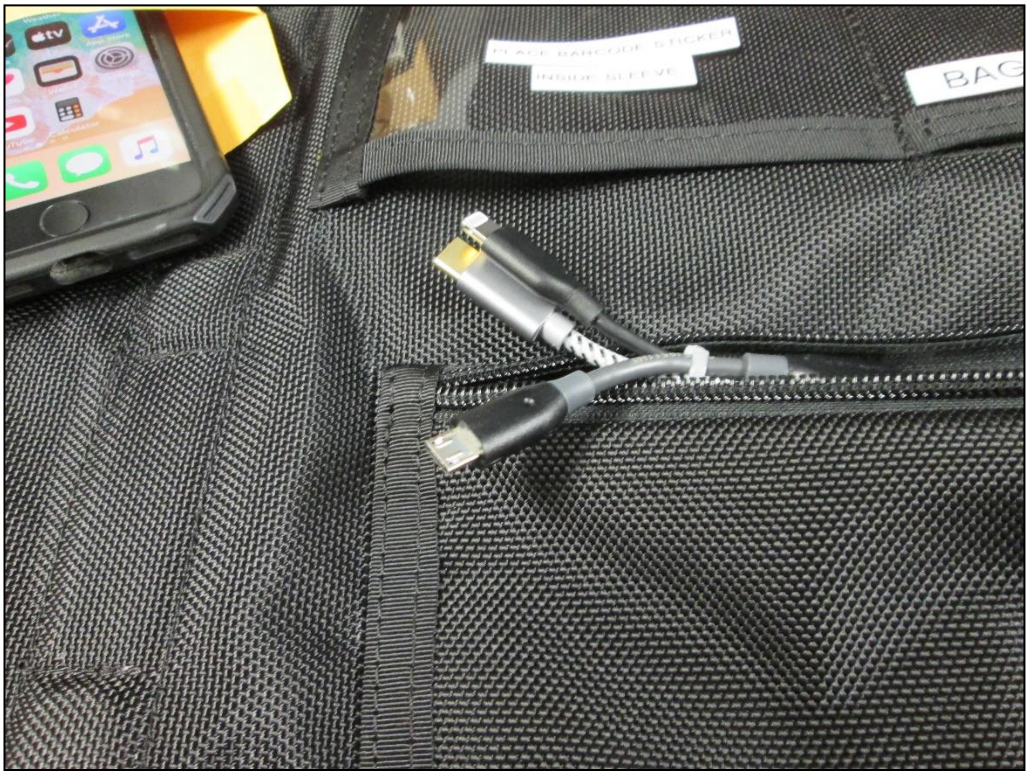
Staple evidence tag on outside of envelope



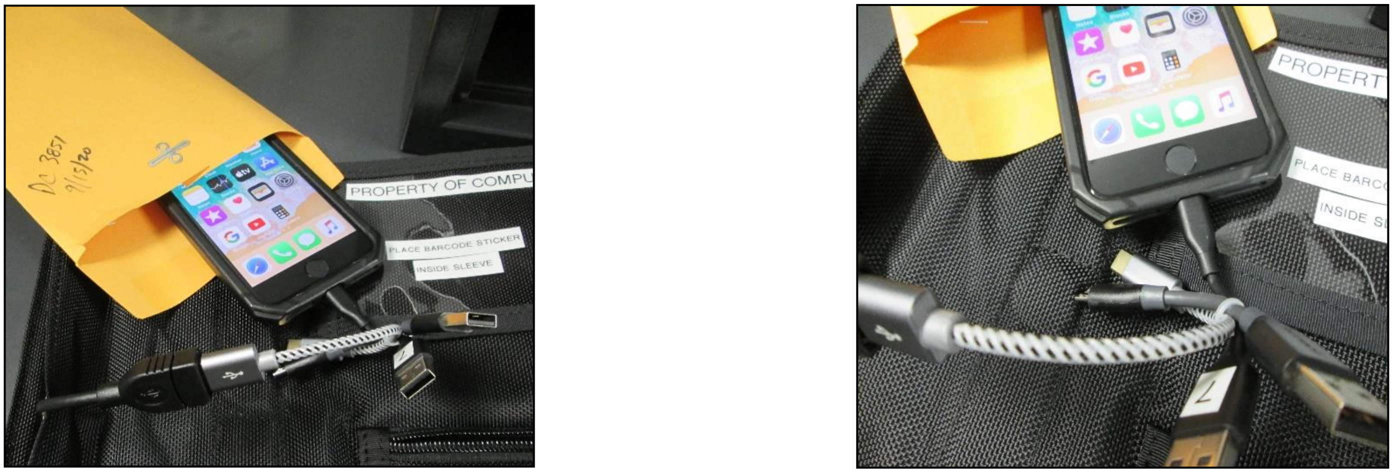
Open locker bay and remove Faraday Bag



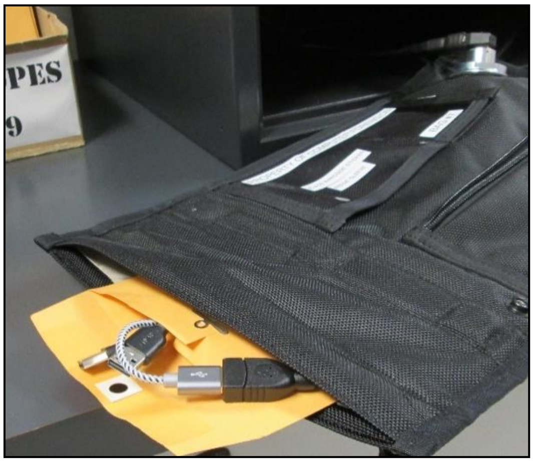
Place device in unsealed envelope



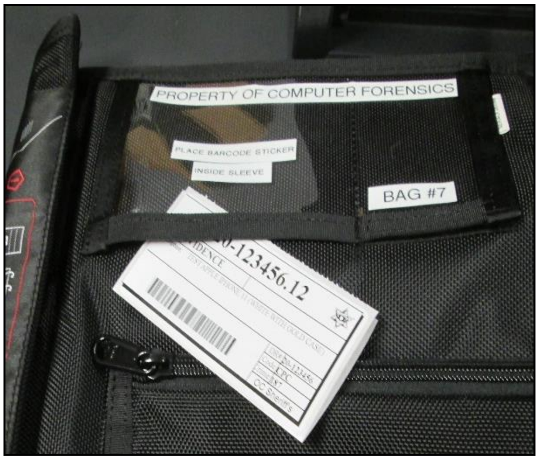
Select appropriate charging cable from zippered pouch on outside of Faraday Bag



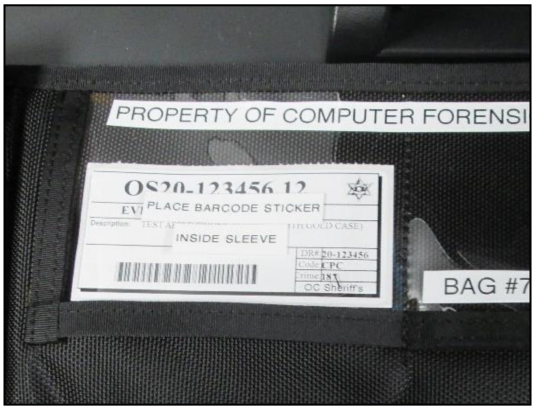
Plug charging cable into device charging port



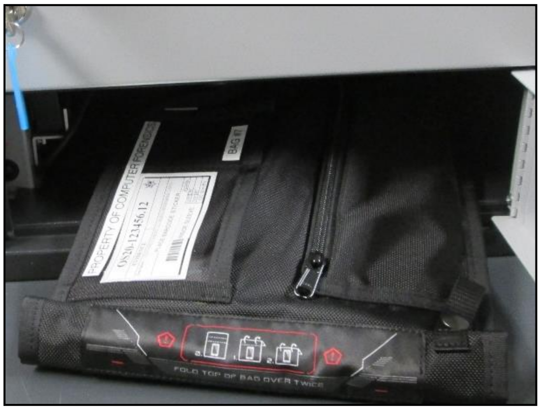
Connect power cable from inside of Faraday Bag to device charging cable



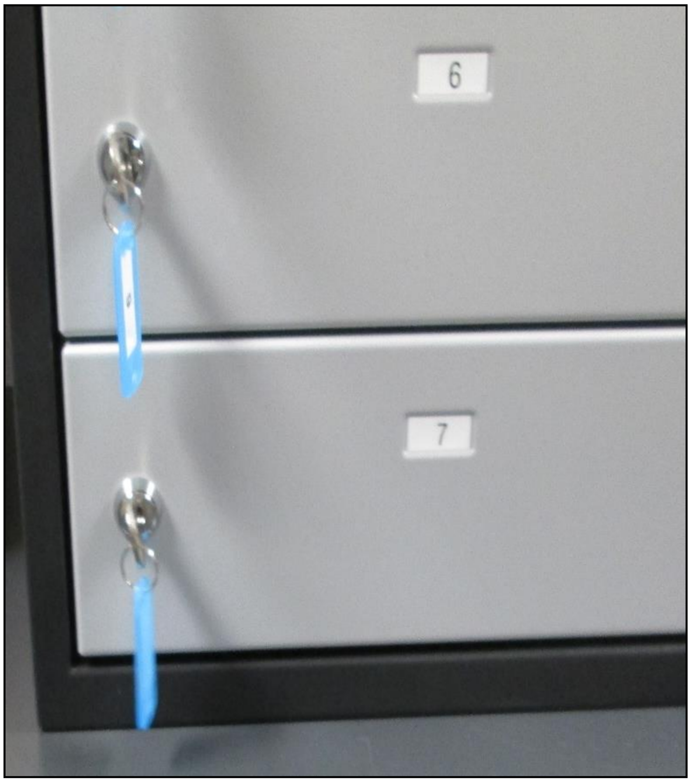
Leave barcode sticker on attached paper



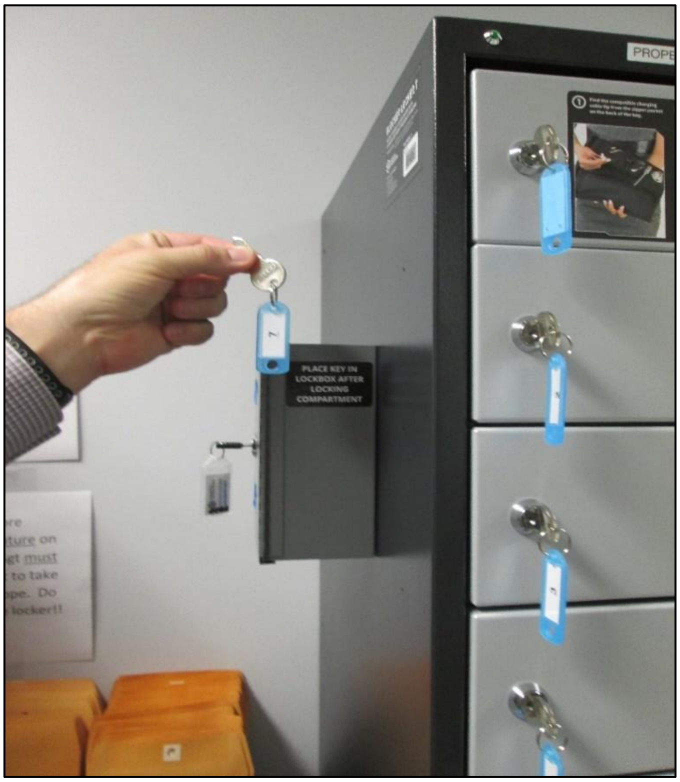
Place evidence barcode sticker into windowed sleeve on Faraday Bag



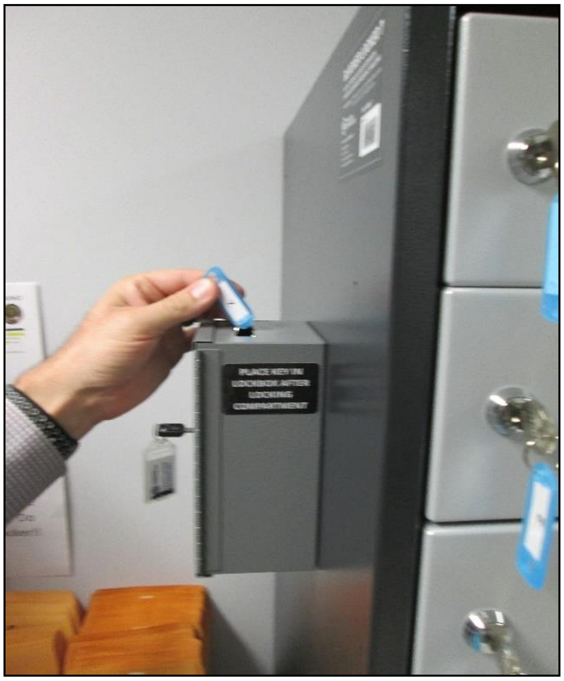
Seal Faraday Bag and put back into locker bay



Close and lock door



Remove key from locker door



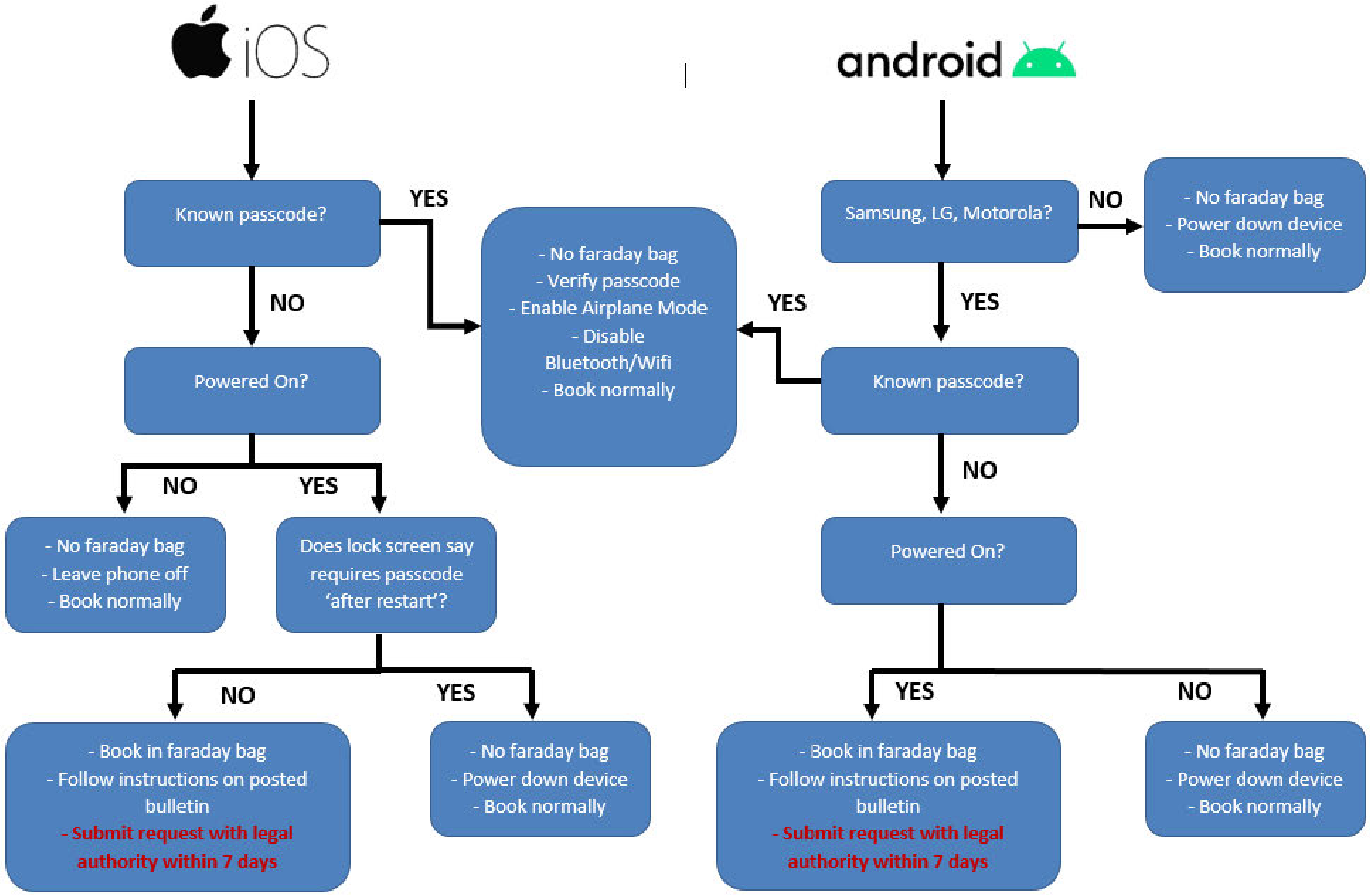
Drop key into lockbox on outside of locker

After booking device:

- **Seek proper search authority (i.e., search warrant, consent, PCRS/ probation terms**
- **Complete Digital Media Examination Request form**
- **Email completed form and proper search authority to: computerforensics@ocsheriff.gov**

BOOKING CELL PHONES / TABLETS

****ONLY BOOK IN A FARADAY BAG IF YOU'LL SUBMIT AN EXAMINATION REQUEST, WITH LEGAL AUTHORITY, WITHIN 7 DAYS****



OCSD Computer Forensics Detail Contact Information:

Sergeant [redacted]
Investigators [redacted]

Email computerforensics@ocsheriff.gov

After Hours Call-outs:

Contact the Department Commander [redacted]