KERN COUNTY SHERIFF'S OFFICE

1350 Norris Road, Bakersfield, CA 93308
661.391.7500 - www.kernsheriff.org

DONNY YOUNGBLOOD
Sheriff - Coroner - Public Administrator

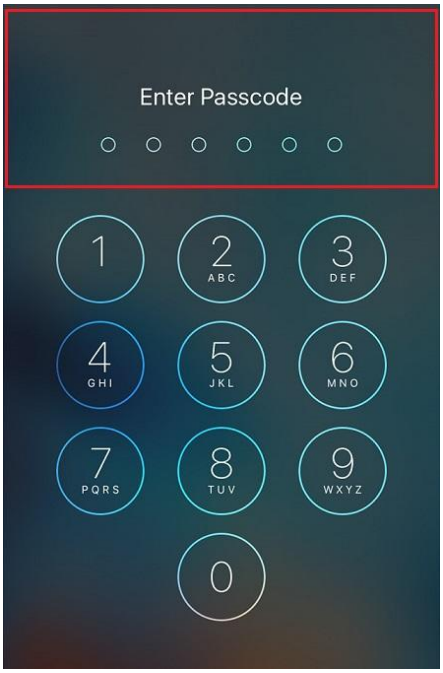
ISSUE: 24-50 ***TRAINING BULLETIN*** ***DATE: December 23, 2024***

Apple iPhone iOS 18.1

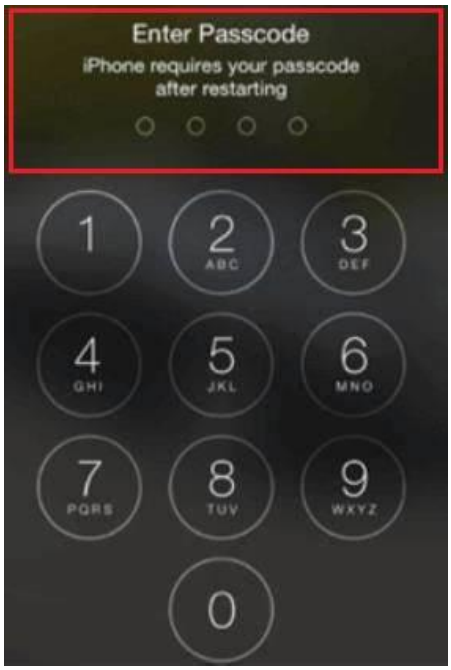
Our training bulletin aims to provide law enforcement and criminal investigation personnel with a comprehensive understanding of Apple's iOS 18.1, released on October 28, 2024. A key feature of this update is the 'inactivity reboot', which automatically reboots the iPhone after 72 hours of inactivity. This feature is a crucial security measure, designed to protect users' personal data in the event of loss or theft.

Following a reboot, an iPhone enters the Before First Unlock (BFU) state, the most secure state an iPhone can be in. In this state, it becomes significantly more challenging, if not impossible, to unlock or extract data stored on an iPhone. It is generally easiest for an iPhone to be unlocked or "cracked" in the After First Unlock (AFU) state, where Law Enforcement can generally utilize forensic tools to extract data from an iPhone.

The 'inactivity reboot' feature is automatic and cannot be turned off by the iPhone user. It applies to all iPhones running iOS 18.1, including older model iPhones that support iOS 18 (iPhone XR and later). To assist anyone seizing an iPhone, we have included two photographs that will help determine which state the iPhone is in.



After First Unlock (AFU)



Before First Unlock (BFU)

Currently, a forensic tool can interrupt the “inactivity reboot” if the deputy or investigator connects the iPhone before the end of the 72-hour idle time. This interruption provides deputies and investigators with more time to obtain the necessary search warrant(s) to extract data from an iPhone. If you're seizing an iPhone running Apple iOS 18.1 or newer and want to seize evidence from it, it's crucial that you bring it to the Crime Scene Investigations (CSI) unit immediately. By doing so, you're ensuring that the necessary forensic tools are utilized to preserve the device.

The following are the current procedures for booking any digital device for physical extraction. These procedures are based on the most up-to-date digital evidence collection and submission practices.

DEVICE

- Do not turn the device off.
- Put the device into Airplane Mode, if possible. Some devices will not allow you to do this without a passcode or pattern.
- Deactivate the Wi-Fi and Bluetooth, if possible.
- Remove the SIM card if you can do so without turning off the device.
- Connect the device to the charging cable to keep the device powered on.
- If an Apple iPhone is possibly running iOS 18.1 or newer, bring the device to a digital forensic analyst as soon as possible to interrupt the “inactivity reboot.”

DIGITAL EVIDENCE SUBMISSION

- A copy of the search warrant with a signed affidavit page or a copy of the signed electronic consent form is required.
- Complete a Digital Evidence Service Request form (Digital Evidence Service Request.xls). Deputies and investigators can locate the form in the Policies & Documents section on SheriffNet.
- Log in to FileOnQ and create an evidence label for each device being submitted for processing.
- Place and plug the device into a digital evidence locker with all necessary paperwork. Digital evidence lockers are currently located in the Crime Scene Investigations building, Metro Patrol Squad Room, and Detective Division.

If you have any additional questions about this training bulletin, please contact the Crime Scene Investigations Unit at CrimeSceneInvestigations@kernsheriff.org.

By acknowledging this training bulletin, you are indicating that you have read the established documents. Acknowledgment of this training bulletin shall be completed by **January 23, 2025.**