REGIONAL COMPUTER FORENSICS LABORATORY

RCFL

CONTINUING EDUCATION SERIES

An ongoing training initiative that provides law enforcement and first responders with the latest information they must know about digital evidence.

To access the Series online, visit www.rcfl.gov.

CONTINUING EDUCATION SERIES

5 STEPS

1 ASSESS THE SITUATION.

When handling mobile phones, there are good reasons for leaving the device on or powering it off:

Leave the phone on when you want to:

- Handle a password protected/encrypted device—if searching for time-sensitive evidence, document actions taken using a camera or video recorder when possible.
- Monitor incoming information—find a charger or method to keep the device powered on.
- Block signals—place device in "Airplane Mode" or seal in a Faraday bag and process the phone within 24 hours because the battery will drain and turn the phone off.

Power the phone off when you want to:

- Preserve evidence
- Safeguard the evidence—seal the phone in an evidence bag and submit it for examination.

2 DON'T BROWSE.

Scrolling through a suspect's mobile phone may alter evidence, and preserving evidence is key. If an investigator must search for time-sensitive evidence, document action(s) taken, what was previewed, and evidence located. Photograph or videotape the evidence as it appears on the device if possible.

3 LOOK FOR PERIPHERALS & SIM CARDS.

When seizing mobile devices, look for "peripherals" such as cables and chargers, and search for Subscriber Identity Module (SIM) cards along with flash memory cards. (Smart Phones commonly save data to SDs or other flash cards.) These items are helpful during a full digital forensics examination.

4 FIND PASSWORDS.

Users can apply a password to protect their privacy. Depending on the device, it may be possible to bypass the password; however, this process typically takes time. Search for written passwords where the device was found.

5 DON'T ASSUME DIGITAL EVIDENCE WAS DESTROYED.

Mobile devices, including phones that have been in fires, water, inside a sewer system, encased in concrete, broken, bloody, or old, can still contain digital evidence. Seize the device and submit to a certified digital forensics Examiner for a full examination.

Access the RCFL Program's Continuing Education Series online by logging onto:

WWW.RCFL.GOV