DIGITAL FORENSIC BYTE-SIZED TIPS

2023 MOBILE SERIES | PART 1

Mobile Device Response

Mobile devices will likely appear in every search or major incident we encounter. In today's letter, we'll discuss mobile device response steps that should be considered when encountering a mobile device on-scene.

Locate and identify the mobile device
Locate the evidentiary mobile device. Notate the manufacturer and any unique identifiers (IMEI, MEID, Serial Number, etc.)

Determine if the mobile device is on or off
Keep a turned-on mobile device powered on and on a charger.
If a mobile device is off, leave it off.

Take steps to protect the evidence from wireless connection
If phone settings are accessible - enable airplane mode and disable Wi-Fi, Location, and Bluetooth.
If settings are inaccessible, eject the SIM card from the SIM card tray or slot.

Identify if there is a passcode/password
Collect passcodes or passwords on-scene, if possible. Ask persons on-scene or keep an eye out for sticky notes or paper with potential codes or passwords written down.

Know your resources
Review the NDCAC Best Practices for Collection/Seizure of Mobile Devices for Law Enforcement brochure.

DIGITAL FORENSIC BYTE-SIZED TIPS

2023 MOBILE SERIES | PART 2

Transporting Mobile Devices

When transporting evidentiary cellular mobile devices, you will want to consider the best way of packaging the mobile device to both transport and protect/preserve the evidence.

FARADAY BAGS VS. TINFOIL

Having Faraday Bags in your search kit is highly recommended. Keeping your evidentiary mobile device in a new Faraday Bag (with no holes or wear) will protect your mobile devices from interacting with Wi-Fi, Bluetooth, or Cellular Signals.

FARADAY BAG
MIC85, CC BY-SA 4.0, VIA WIKIMEDIA COMMONS

Tin foil is the classic way of protecting a phone from radio signals. But with stronger radio signals, tin foil has become less effective. But in a pinch, using heavy duty foil to wrap around the evidentiary device 4-5 times can help preserve the phone from radio signals.

POWER BANK
OBTAINED FROM CANVA PRO

USB POWER BANKS

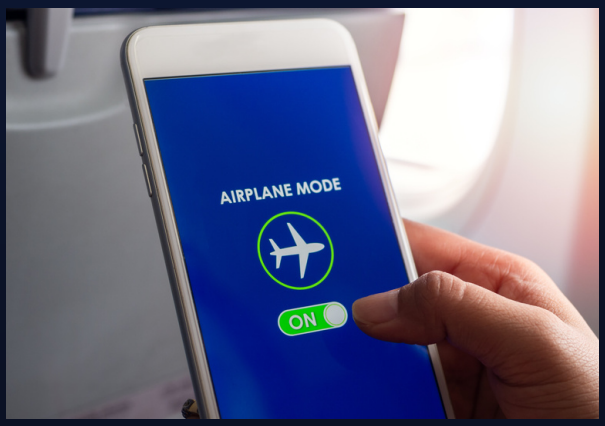
If you collect a phone that is in a powered-on state at the scene, do your best to keep that phone powered on. Keeping USB power banks in your on-scene kit with a variety of common mobile power connectors (USB-C, Lighting, USB Micro-B). You can connect your evidentiary phone to the power bank and insert it into your Faraday Bag to keep your phone powered on during transport.

DIGITAL FORENSIC BYTE-SIZED TIPS

2023 MOBILE SERIES | PART 3

Airplane Mode

In today's letter, we'll be discussing what airplane mode is and why it may be important to use in the digital forensic field.



AIRPLANE MODE

Airplane mode is a term coined for a mode that disables radio-related connectivity for mobile devices. Other names include offline, standby, and flight mode. Airplane mode is essentially a shortcut for disabling a series of settings in one swipe. Airplane mode disables the following:

CELLULAR

Airplane mode disables connection to cellular networks. Features like data-usage, calling, and SMS/MMS texting will be disabled.

WI-FI

Airplane mode may disable connection to wireless networks.

BLUETOOTH AND NEAR FIELD COMMUNICATIONS (NFC)

Bluetooth and NFC are both functions that allow connection and the communication of data over short distances. Airplane mode disables these functions.

FORENSIC SIGNIFICANCE

Isolating evidentiary devices protects potential evidence from outside interference. Isolating evidence from wireless networks by using tools, like Airplane mode, **could prevent your evidence from being wiped or altered.**

DIGITAL FORENSIC BYTE -SIZED TIPS

2023 MOBILE SERIES | PART 4

Before and After First Unlock

In this week's letter, we will explain why it is so important to do your best to keep an evidentiary mobile devices powered-on and charged after seizing them,

When encountering a mobile device, it can be in one of two states:

BEFORE FIRST UNLOCK (BFU)

A state a device enters after being powered on but has not been unlocked. In this state the device's data is encrypted and using forensic tools would require a brute force attack that can take months to years.

AFTER FIRST UNLOCK (AFU)

A state a device enters after being unlocked at some point since being turned on. If it has maintained power since the first unlock, it will remain in the AFU state and the device's data is decrypted. The probability of getting a successful extraction is greater.

CONSIDERATIONS

The vast majority of phones being carried around by people are in the AFU state. However, the large majority of evidentiary phones are in the BFU state, as they have been powered down and stored. When seizing a mobile device that's AFU make sure to **keep it powered on and connect it to a charger as soon as possible**. If the battery dies, or if it is powered off, we lose the advantage of AFU.

DIGITAL FORENSIC BYTE -SIZED TIPS

2023 MOBILE SERIES | PART 5

SIM and SD Cards

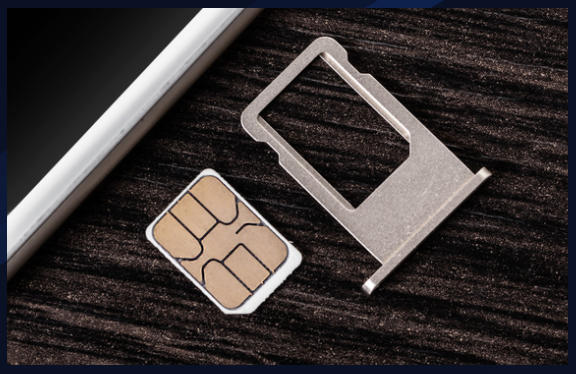
In mobile devices, you'll likely see two different types of cards inside. In this week's letter, we'll learn about accessing the two types of cards and their differences.

ACCESSING THE SIM/SD CARD

To reach the SD and/or SIM card, a paperclip may be needed to insert and push out the SIM card tray. The SIM card may be beneath the battery on phones with removable back panels. **Do not power off a phone to remove the SIM or SD card** before consulting a forensic examiner.

SUBSCRIBER IDENTITY MODULE (SIM) CARD

The SIM card identifies and authorizes a device to use a cellular network. **Removing the SIM card will isolate the device from the cellular network.** The SIM card contains data like a phone number and user identity. On older mobile phones, the SIM card my contain contact lists and text messages. The SIM card will have a 19-20 numeric serial number and may have the manufacturer's company logo printed on the front.



SIM CARD AND TRAY
OBTAINED FROM CANVA PRO

SECURE DIGITAL (SD) CARD

An SD Card contains digital storage for the cellphone. An SD card **may contain graphics, videos, files, or application data.** The front of the SD card may have manufacturer name, storage size, and a serial number printed on.

SD CARD IN PHONE SLOT
OBTAINED FROM CANVA PRO

DIGITAL FORENSIC BYTE -SIZED TIPS

2023 MOBILE SERIES | PART 6

Mobile Phones and Liquid

It is not uncommon to be fishing evidentiary phones out of lakes, rivers, oceans, or even toilets. In this week's letter, we'll provide the best practices for mobiles phones exposed or submerged in water or other liquids.

SPLASHES, SPILLS, AND MINIMAL EXPOSURE

If you encounter a mobile phone that has only been minimally exposed to liquid (splashed, spilled on, etc.) then remove the phone from any liquid source and wipe the phone down. If the phone is powered off, do not power on the phone. Most new mobile phones have splash and water resistance but are not fully water proof. **Never put the phone in rice**. It will not absorb the water potentially inside the phone and introduces dust and other bacteria that may cause additional damage to internal compoennts.

SPILLED WATER ON PHONE
OBTAINED FROM CANVA PRO

SUBMERGED IN LIQUID

If the mobile phone is fully submerged in liquid, then you will want to keep the mobile phone submerged in the same liquid. Arson cans or capsules can be used to collect the device in the liquid. Once a device is removed from liquid, oxidation begins and may damage internal components beyond repair. **Immediately bring the mobile phone to a digital examiner trained in cleaning and handling liquid-submerged phones.**

SUBMERGED PHONE IN OCEAN WATER
OBTAINED FROM CANVA PRO