Digital Forensics Lab at Dakota State University

iPhones and iPads—iPhones/iPads have the Apple logo on the back (remove the case if necessary)

Android devices—usually have other manufacturer or model markings Ex: Samsung, Motorola, LG, ZTE, etc.

Phone is **OFF**
—
Leave it **OFF**

Phone is **ON**
—
Keep it **ON**

Passcode

Make every effort to identify the passcode (include this on the submission form) - DO NOT try to guess the passcode, there are a limited number of attempts before the phone will be wiped.

Isolation

It is important to isolate the phone from the cellular network to prevent a remote wipe command from being sent to the phone.

DO one of the following:

- Airplane Mode/Bluetooth—swipe down from upper right or up from the bottom—locked phones may require the passcode.
- Faraday Bag—blocks remote wiping or alteration of wireless devices.
- Tin Foil—several layers can isolate the phone if a Faraday Bag is unavailable.
- Paint Can—similar to tin foil, will isolate the device if the above steps are not possible.

Remove the SIM card **ONLY** as a last resort—this can sometimes prevent access to important data.

IMPORTANT: Isolating a powered phone will drain the battery very quickly. Attach the phone to a power pack making sure the phone, power pack and all cables are fully within the enclosure.

Data Storage

Must provide an external hard drive.

Submission Documentation

DSU Digital Evidence Submission Form and Legal Authority

Legal Process

Obtain proper legal authorization prior to submitting to DSU.

Physical Evidence

Check for and process any physical evidence prior to submission to DSU.

Separate Packaging

Each device should be packaged in a separate evidence bag.

DAKOTA STATE UNIVERSITY

madlabs.dsu.edu/digforce
digforce@dsu.edu
605-256-5148

Effective: 04/03/2023