



Physical Evidence Bulletin

Digital Evidence Collection – Mobile Devices

Objective The Physical Evidence Bulletin is intended to provide a process to collect and preserve mobile devices and submit them to the Bureau of Forensic Services.

Definition: digital evidence Digital evidence is information of probative value that is stored or transmitted in binary form (i.e. 1's and 0's) that may be involved in: homicides, clandestine laboratories, fraud, child pornography, and/or other crimes.

Definition: mobile device Any digital device designed to be easily transported that may contain digital evidence.

Safety and Other Forensic Evidence Considerations

Safety considerations during collection

- Consider safety first when collecting evidence. Although the collection of physical and digital evidence is important, safety must be the first consideration.
- Evaluate electrical, explosive, flammable, biological, or other hazards before deciding to retrieve the device (e.g. a bloody phone, a cellular phone which may trigger an explosive or a flammable solution)

Fingerprint, Biological/DNA and Trace Evidence

- Examine digital device(s) for possible evidence such as fingerprints, blood, hair, fibers, tissue, etc. that may be relevant to the investigation.
- Do not conduct fingerprint examinations.
Note: Some methods of retrieving fingerprints may damage electrical devices.
- If the preservation of biological evidence is a concern, do not package wet evidence. Digital evidence should be air dried before placing into appropriate containers (i.e. paper).
- It may be appropriate to sub-sample a representative amount of biological/trace evidence to allow for proper preservation steps like drying in lieu of drying out the digital evidence.

Note: The normal degradation of biological stains is accelerated when items are wet and sealed in airtight containers such as a plastic bag or arson can.

Preventing contamination and damage to evidence

- Wear proper protective equipment to prevent contamination (i.e. gloves, face mask, etc.)
 - When articles must be picked up, which may contain latent fingerprints, biological, or trace evidence, they should always be handled as little as possible to limit changing the possible evidence.
-

Collection and Preservation of Digital Evidence

Documentation of digital evidence

- The location and condition of the digital evidence and related evidence at a crime scene should be documented (e.g. sketches, photographs, notes) before recovering and securing.
- Documentation should describe how items were connected.
- Photographs should be used to supplement notes and sketches.
- The date and times of collection of digital evidence should be recorded.

Note: Data can be received and activities occur with digital evidence after the collection. Noting the date and time of receipt may assist in documenting what data may have changed after collection.

Documentation and labeling of packaging

- At minimum the evidence package should include the item number, case number, initials, and date of collection.
 - Package should be sealed, by tape or heat seal, and initialed.
-

Mobile devices submerged in liquids

- If a mobile device was dropped in water or other liquids in an attempt to destroy evidence, store the evidentiary device in the same liquid it was found in.
- Blood or caustic liquids may continue damaging metallic components and may need to be stored in a different liquid (i.e. water).
- If any concerns or special circumstances arise, call the laboratory for further recommendations.

Note: If a battery is found in the device in question, remove the battery from the device yet store in the same liquid it was found in.

Mobile devices submerged in liquids

- Observe whether the mobile device is powered “ON” or “OFF.” DO NOT, under any circumstances, power on the mobile device if the unit is not powered.
- If potential fingerprint, biological, or trace evidence may be present on the device in question, refer to the appropriate physical evidence bulletins for proper evidence handling. It may be appropriate to sub-sample a representative amount of biological/trace evidence to allow for proper preservation steps, like drying.
- Many mobile devices, especially newer models, do not lose data when powered off and some can turn on automatically at a predetermined time. By leaving the unit “OFF” or removing the battery, the following may be prevented: overwriting of deleted data, remote wipe signals from reaching the device, and improper phone handling (e.g. placing calls, sending messages, deleting photos, etc.)

If the mobile device is ...	Then ...
“ON” or powered	<ul style="list-style-type: none"> • Document any data that is transmitted to the device (i.e. incoming calls, text messages, etc.) during seizure, and record all information present on the screen. • Block wireless signals to prevent the device from receiving calls, text messages, etc. <ul style="list-style-type: none"> – Place in “Airplane Mode” and put in evidence package or put in evidence package and place entire package in a Faraday bag or similar material (e.g. arson cans, aluminum foil wrap, etc.).
“OFF” or not powered	<ul style="list-style-type: none"> • If possible, remove the battery from the device. Store the battery in the same container as the device it was removed from. • If the battery cannot be removed, place entire evidence package in a Faraday bag or similar material (e.g. arson cans, aluminum foil wrap, etc.).

Note: If you place a powered “ON” cellular phone in a Faraday bag, the device should be examined as soon as possible because the battery will drain during this period, and will turn off.

“Scrolling” or “browsing” an evidentiary device

- Do not scroll or browse through an evidentiary device, because doing so may alter the device.
- Document any actions that were done on the digital device, if any manipulations were made to it.

Peripherals, SIM cards, memory cards, and passwords

- When seizing mobile devices, look for “peripherals” such as phone related software and manuals, cables, chargers, and search for Subscriber Identity Module (SIM) cards along with flash memory cards (i.e. microSD cards). Peripherals, flash memory cards, and SIM cards may be necessary to conduct a full digital forensic examination.
- Notes or papers with possible passwords or PINs should also be documented and collected.
 - Often, the passwords are not far from the device itself, so keep an eye out for this information.
- Ask subjects in question for passwords or PIN that may be needed for devices and Internet sites in question.

Note: Do not exceed the scope of the search warrant in regards to the case being investigated.

Don’t assume digital evidence was destroyed

- Mobile devices exposed to various conditions can still contain digital evidence.
- If there is doubt call the laboratory for assistance.

Submitting Mobile Device Evidence to the Laboratory

Police reports • Copies of the police and investigative reports in regards to the mobile device should be submitted with the evidence.

Examination requests • The submitting agency should write down the request for examination on the BFS-1 Submittal form or attach a request letter to the BFS-1.
• When possible requests for examination should be more specific than “collect all data,” if, for example, all that is needed are call logs or photos.
• The extraction of data is dependent on the mobile devices and the available tools to extract the information. There are mobile devices which the laboratory cannot acquire data from.

Legal authority to conduct search and the laboratory • The responsibility of legal authority rests with the agency. Requests for service for digital evidence, like other BFS disciplines, are assumed to have the appropriate legal authority.
• Bureau personnel may still need to contact the submitting agency representative to determine the scope of work requested or urgency of the work (e.g. investigative lead, court date, etc.)

For further information and additional resources

The examination of mobile devices is available at the following locations:

Sacramento Criminalistics Laboratory

4949 Broadway Rm. F-147
Sacramento, CA 95820
916-227-3623

Also provides mobile device service to BFS Central Valley, Redding, Chico Laboratories

Fresno Criminalistics Laboratory

5311 North Woodrow
Fresno, CA 93740
559-294-4000

Also provides mobile device service to BFS Freedom Laboratory

Riverside Criminalistics Laboratory

7425 Mission Blvd.
Riverside, CA 92509
951-361-5000

Also provides mobile device service to BFS Santa Barbara Laboratory

Richmond Laboratory

1001 West Cutting Blvd. Ste. 110
Richmond, CA 94804
510-620-3300

Also provides mobile device service to BFS Santa Rosa and Eureka Laboratories

Please contact one of the above laboratories directly, or your regional BFS laboratory, with any further questions that you may have.

For a list of regional laboratories please go to:

https://oag.ca.gov/sites/all/files/agweb/pdfs/bfs/bfs_brochure.pdf or
<http://oag.ca.gov/bfs/>

To locate the most current Physical Evidence Bulletins please go to:

<https://oag.ca.gov/cci/reference#peb>