Scientific Working Group on Digital Evidence

Best Practices for Mobile Devices Evidence Collection & Preservation Handling and Acquisition

18-F-003-2.0

The version of this document is in draft form and is being provided for comment by all interested parties for a minimum period of 60 days.

Disclaimer Regarding Use of SWGDE Documents

SWGDE documents are developed by a consensus process that involves the best efforts of relevant subject matter experts, organizations, and input from other stakeholders to publish standards, requirements, best practices, guidelines, technical notes, positions, and considerations in the discipline of digital and multimedia forensics and related fields. No warranty or other representation as to SWGDE work product is made or intended.

SWGDE requests notification by email before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in such proceeding. The notification should include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in the proceeding please notify SWGDE as to the outcome of the matter. Notifications should be submitted via the SWGDE Notice of Use/Redistribution Form or sent to secretary@swgde.org.

From time to time, SWGDE documents may be revised, updated, deprecated, or sunsetted. Readers are advised to verify on the SWGDE website (https://www.swgde.org) they are utilizing the current version of this document. Prior versions of SWGDE documents are archived and available on the SWGDE website.

Redistribution Policy

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain this SWGDE cover page containing the Disclaimer Regarding Use.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or creation date) of the document and also indicate if the document is in a draft status.

Requests for Modification

SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be submitted via the SWGDE Request for Modification

Form or forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of any suggested modification:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) SWGDE Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for suggested modification

Intellectual Property

All images, tables, and figures in SWGDE documents are developed and owned by SWGDE, unless otherwise credited.

Unauthorized use of the SWGDE logo or document content, including images, tables, and figures, without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

Scientific Working Group on Digital Evidence

Best Practices for Mobile Devices Evidence Collection & Preservation Handling and Acquisition

Table of Contents

1. Purpose and Scope

Mobile devices, smartphones, and tablets are portable devices that have an embedded system architecture, processing capability, on-board memory, storage, and may have telephony capabilities.

This document provides best practices for the collection & preservation, handling, and acquisition of evidence from mobile devices. The collection and preservation of data from mobile devices is performed in the lab, as well as in the field, e.g., for consent or exigent circumstances. This document provides best practices for the functions that may be utilized by field personnel. The intended audience is personnel qualified to collect & preserve, handle, or acquire digital evidence. These processes are designed to maintain the integrity of digital evidence. For guidance on recommended training and qualifications, see *SWGDE 10-Q-002-3.0 Guidelines & Recommendations for Training in Digital & Multimedia Evidence*.

The techniques and methods featured in this document are designed to maintain the integrity of the evidence while maximizing the data recovered.

2. Disclaimer

This document is not to be used as a step-by-step guide for executing a proper forensic investigation when dealing with mobile devices, nor construed as legal advice.

3. Considerations

Mobile devices present a unique forensic challenge due to rapid changes in technology. There are numerous makes and models of mobile devices in use today. Many of these devices use closed source operating systems and/or proprietary interfaces, sometimes making it difficult to extract digital evidence. The operating systems also come in various iterations and may require different methods of extraction for acquiring the data. An additional consideration is the same operating system can be altered for specific vendors. Operating system version and tool-specific expertise may be necessary to attain access and may alter the workflows listed below.

The considerations are organized alphabetically, not in order of operations for mobile device evidence collection & preservation, handling, and acquisition.

Examples include the following:

- **Anti-Forensics/Dead-Man Switches**: Be advised that mobile operating systems and applications may have automated features that could lead to unrecoverable data under certain conditions, such as after a set period, a brute-force attempt, or when a USB connection is made. Examiners should employ extraction methodologies that address these concerns where applicable.
- **Cables**: Data cables can be unique to a particular device and forensic tool. Cables are available in both data/sync and charging-only capabilities. In some instances, specialized cables may be used to place a device into an alternative mode to facilitate acquisitions. It's important to use high-quality/certified cables for data acquisition, as cables

manufactured to a low standard may not provide a sufficient signal that facilitates a proper connection (i.e., handshake) between devices and may cause damage.

- **Data Retention Periods**: A multitude of artifacts are only retained for a specified period of time. Delays in acquisition may lead to the inability to retrieve data that is temporal in its period of storage. Turning off the device or using network isolation may not preserve the temporal data.
- **Drivers**: Drivers may be included with a forensic tool or downloaded from various sources. Conflicts may occur due to existing operating system drivers, proprietary drivers, driver version inconsistencies, and vendor-specific drivers.
- **Dynamic Nature of the Data**: Data from powered-on mobile devices is constantly changing. Power cycles on mobile devices will affect volatile data. Limit extraneous device handling to avoid data overwrites.
- **Encryption**: Data may be stored in an encrypted state (e.g., full-disk or file-based), possibly preventing access or analysis without the use of more advanced forensic methods.
- **Equipment**: Following validation, the latest tested version of forensic equipment and software should be used. The use of multiple forensic tools may be necessary to maximize results or corroborate findings.
- **External Power Source**: To prevent a device from powering down due to battery exhaustion or rebooting, it is recommended to connect the device to a consistent power supply whenever practical. Air transport may prohibit battery connection to a mobile device for safety reasons.
- **Extraction of Mobile Device Storage**: Examiners pursuing an extraction of a mobile device's storage may have to use processes that will leave digital artifacts. It may be necessary to install a bootloader or software client, gain root access to the device's operating system, or accept wireless connections to extract data from the device. These techniques may leave behind digital artifacts, necessitating contemporaneous notes. A single tool may not extract or present all data contained in a mobile device. Manually reviewing the contents of a mobile device or using a second forensic tool can corroborate the results or provide additional data not recovered during the initial extraction. Hash values from multiple extractions of the same device may not match due to the dynamic nature of storage media on mobile devices.
- **Inconsistent Industry Standards**: Manufacturers and carriers may use proprietary methods to store data (e.g., closed operating systems, proprietary data connections).
- **Integrated Circuit Cards, aka Subscriber Identity Modules**: On feature phones, lack of or removal of an identity module may prevent the examiner from accessing data stored

on the internal memory of a handset. Inserting an identity module from another device may cause loss of data.

- **Loss of Power**: Many mobile devices may lose data or initiate additional security measures once powered off or restarted, which could prevent data acquisition.
- **Mobile Device Management**: Mobile Device Management configurations may prevent acquisition of a device. Prior to making configuration changes, the examiner should confirm that any changes will not result in complete data loss or factory reset of the device.
- **Network Isolation**: To reduce the potential of remote wipes or receipt of additional data, place the mobile device in a Radio Frequency (RF) blocking container such as a Faraday bag, box, or room, or use another signal-blocking method to reduce or prevent network connectivity.
- **Passwords/Passcodes**: Authentication mechanisms can restrict access to a device and its data. Of importance, in some instances, there are a limited number of attempts for wrong passwords/passcodes. Incorrect passwords/passcodes could lead to unrecoverable data or exfiltration of information about the attempt. Older mobile devices may be of aid in obtaining passwords for a current device.
- **Peripherals**: Search all areas of the scene to identify related items. Paired or linked devices may provide valuable information in addition to the mobile device (e.g., computers, smartwatches, tablets, security key hardware, Internet of Things (IoT) devices).
- **Phone Number Portability**: A phone number, also referred to as a Mobile Station International Subscriber Directory Number (MSISDN), may not be permanently tied to a specific wireless provider and can be transferred between devices either by Subscriber Identity Module (SIM) card or electronic SIM (eSIM).
- **Removable Media**: Mobile devices may contain removable media, and forensic tools will often perform acquisitions of this data. Removable media may be adoptable (encrypted with the device) or portable (able to be moved from device to device and accessed). Adoptable storage should be read through the device and portable storage may be read from an external reader or via the mobile device. It is recommended to image portable storage externally from the device via a write blocker to acquire a physical image.
- **Synchronization**: Data related to a mobile device can often be found on a computer, smartwatch, tablet, or other associated device due to synchronization or sharing of information through a backup process or cloud service account. Likewise, data from a computer or other devices that have been synchronized may also be found on the mobile

device. Due to this information exchange, it may be possible to link a particular mobile device to a particular system or device with which it was connected.

- **Training**: The individual collecting, examining, and analyzing a mobile device should be trained to preserve and maintain data integrity. Refer to S*WGDE 12-F-003-1.0 Core Competencies for Mobile Phone Forensics*.
- **USB Restricted Mode (USB RM)**: Some devices utilize a setting that limits a device's USB port to work only as a charging port in certain circumstances.
- **Virtual Network**: Isolated virtual networks and virtual machines may be necessary for certain cases (e.g., malware, CSAM) to prevent spillage or contamination.
- **Write Blocking**: Since mobile forensics acquisitions require communication with the device, there are no write-blocking methods available for mobile devices themselves, whereas write-blocking is sometimes applicable to portable storage media.

4. Evidence Collection & Preservation

4.1 Documentation

Document the collection of devices in accordance with organizational guidelines and procedures. Documentation may include a written description or photographs of the collection location, the device state (e.g., powered on/off, locked/unlocked), pin code/password (if known), the time displayed on the device, network connections, external physical characteristics of the device, and/or examiner interactions with the device. External physical characteristics include identifying information such as the make, model, serial number, damage, and/or any identifying marks. Documentation should include all changes made by interacting with the mobile device and settings.

The chain of custody documentation shall be contemporaneous and include a description of item(s), unique identifier(s), and the date/time of receipt or transfers. The record shall fully identify each person (e.g., name, title, signature) taking possession of an item.

4.1.1 Device Identification

A forensic acquisition begins with the identification of the mobile device. The type of device generally dictates the tools and techniques to be used to extract data.

The manufacturer's label, sometimes printed on the casing or found within the battery cavity, often lists the make and model number of the mobile device and other identifiers including the Federal Communications Commission Identification Number (FCC ID) and equipment identifiers (i.e., International Mobile Equipment Identity (IMEI), Mobile Equipment Identifier (MEID), and the Electronic Serial Number (ESN)). Certain device components may contain additional identifying information, such as the IMEI microprint on the SIM card tray of some Apple devices.

If the mobile device is powered on, the information appearing on the display may aid in its identification. For example, the manufacturer or service provider's name may appear on the

display, or the screen layout may indicate the operating system in use. This information is often used to identify a device's chipset which may dictate acquisition methodology.

4.1.2 Legal Authority

Ensure there is proper legal authority to collect and/or examine the evidence to be acquired. Proper legal authority includes a signed search warrant from a court of competent jurisdiction, court order, engagement letter, consent, corporate policy, and/or it has been established that privacy rights associated with the device no longer exist. See *SWGDE 16-F-002-2.0 Considerations for Required Minimization of Digital Evidence Seizure*.

4.1.3 Documenting the Scene

Initial documentation should begin with photographs and/or video of the overall scene to capture the environment in which the device was discovered. Capture close-ups of the physical condition of the device. Take special care in not disturbing the device unless necessary. Evidence markers are recommended to associate the device with the corresponding documentation.

Search, seize, and examine non-electronic materials such as device boxes, packaging materials, SIM card frames, and manuals which can contain information related to the device's unique identifiers. Notebooks and papers found within the vicinity of the device can also contain information related to usernames and passwords.

4.1.4 Evidence Handling

Improper handling of a mobile device during preservation and collection may cause loss of data. The following information is provided to ensure the best chances for recovery.

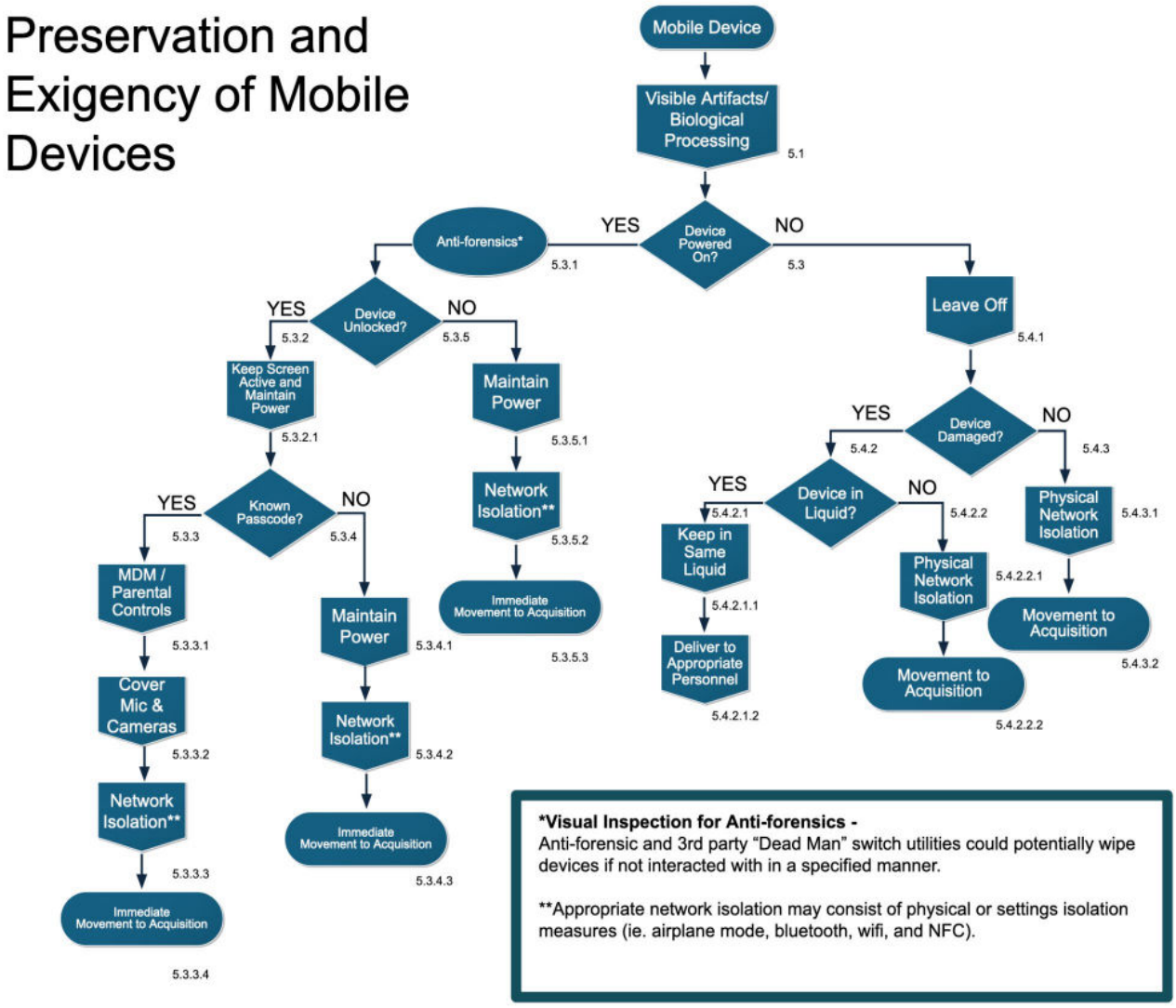
4.1.5 Traditional Forensic Processes

Traditional forensic processes, such as fingerprints or DNA testing, may need to be conducted. If the device is not handled properly during preservation and collection, evidence can be contaminated and rendered useless. As such, handle all potentially evidentiary items with appropriate personal protective equipment (e.g., gloves) and submit to an appropriate lab as the situation dictates. Traditional forensic processes (e.g., DNA, latent prints) on a mobile device should be considered. Time sensitive needs of digital evidence preservation should be balanced with potential requirements to complete traditional forensics processes before digital forensic processes. Applicable agency-specific procedures should be followed.

5. Preservation and Exigency of Mobile Devices

The following flow chart provides a basic overview of the best practices for preserving evidence when seizing mobile devices and is not meant to be all-encompassing. This workflow does not preclude organizational standard operating procedures or deviations when extenuating circumstances exist.

To prevent unnecessary altering of data on the device, only manually access the device when needed to facilitate access, to view evidentiary artifacts prior to the acquisition, or where immediate action is required.



5.1 Visible Artifacts/Biological Processing

Photograph relevant devices and peripherals (e.g., cables, power connectors, removable media, and connected items) as part of a thorough scene documentation. Avoid touching or contaminating the mobile device(s) when photographing. If the device's display is in a viewable state, photograph and document its original state, and any further changes. It is important to ensure that the state of the device is maintained and that photography/documentation efforts do not inadvertently change the state of a device, such as locking or removing the power source. Include any smear mark patterns that may be used to obtain passcode Include any smear mark patterns that may be used to obtain passcode.

Consider the potential presence of physical evidence (e.g., biological, trace, latent prints, contaminants). Work in conjunction with other forensic disciplines to determine appropriate processing procedures for the device.

5.2 Equipment Preparation

"Equipment" in this section refers to the hardware the examiner utilizes to conduct data extraction and analysis of the evidence. Equipment and software applications should be tested and validated prior to being used in casework.

See *SWGDE 18-Q-001-2.0 Minimum Requirements for Testing Tools Used in Digital and Multimedia Forensics*.

5.3 Device - ON

It is critical to follow the recommended steps to prevent degradation or loss of data from devices that are on.

It is important to be aware of an inactivity timer which may cause a reboot. A reboot occurs when data is at rest after a predetermined amount of time, potentially moving a device from an AFU state into a BFU state. Once the device has rebooted, it is returned to its most secure state, making some data unrecoverable.

5.3.1 Anti-Forensics

Visual cues to the existence of anti-forensic utilities may include but are not limited to, a red "X" in the taskbar or notification messages on the lock screen.

Features can be enabled on a device via third-party applications that can lock and unlock a device beyond traditional locking mechanisms (e.g., timing locks and device locking buttons).

- **On-Body Detection**: This feature is designed to keep a device unlocked when it detects it is "on-body". If a device is unlocked as long as the phone senses, it is still held or being carried it will stay unlocked. If the device detects that it is no longer being held or carried (e.g., set down on a table) then the device may lock.
- **Trusted Places**: This feature is designed to keep a device unlocked when it detects it is at a trusted location. This is most commonly determined by location services and wireless internet networks. A user, for example, may set their home as a "Trusted Place" allowing their device to remain unlocked while within the proximity of their home. When the mobile device detects that it leaves the location, it will automatically lock. This should be considered when seizing or recovering a mobile device before leaving the possible trusted location.
- **Trusted Peripheral Devices**: This feature is designed to lock and unlock when a device is in a specified proximity to a trusted peripheral device. For example, a user can configure a mobile device to lock and unlock based on the proximity of a trusted smart watch.

5.3.2 Device Unlocked – YES

There are unique considerations for unlocked devices in order to facilitate the most complete acquisition.

5.3.2.1 Keep Screen Active and Maintain Power

It is pertinent to maintain both power on and an active screen for an unlocked device in order to maximize availability of data. Consider disabling or extending the screen lock setting to the longest period possible and connect the device to a consistent power source. Maintaining an active screen may require constant interaction from either an external source (e.g., mouse jiggler) or human interaction.

5.3.3 Device Unlocked – YES – Known Passcode

When a passcode for an unlocked device is known, there is a necessity to ensure device state is maintained.

5.3.3.1 MDM/Parental Controls

Often in an enterprise environment, a central server or control system (e.g., a Mobile Device Management (MDM)) may be used to administer and configure mobile devices and obtain access to data from controlled mobile devices.

Some organizations may choose to restrict access on mobile devices or parts of mobile devices issued to their members. Using an MDM, an organization's system administrator can restrict many features of the device from a user, such as blocking the phone's USB port access, which might make the acquisition of the device impossible. If the device is locked within an MDM, examiners may need to seek assistance from the system administrator to extract data. Prior to requesting MDM configuration changes, examiners should confirm that any configuration changes will not result in complete data loss or factory reset of the device.

Similar restrictions can be applied with a variety of Parental Control applications and system settings. If device acquisition is being prevented, and the examiner has ruled out the presence of MDM configurations on the device, the examiner should review for system settings or Parental Controls applications that are preventing access.

5.3.3.2 Cover Microphone and Cameras

Be cognizant that the microphone and camera could be turned on when an incorrect passcode is entered resulting in exfiltration of information about the attempt. Use either a microphone blocking plug or take precautions that are available to prevent audio collection. Cover all cameras including front and rear facing.

5.3.3.3 Network Isolation

It is necessary to isolate mobile devices from networks to ensure data is not remotely modified or destroyed. Remote wiping capabilities exist that could remove data. Network isolation also prohibits receipt of additional data.

Historically, examiners isolated a mobile device from network connectivity by placing the device in "airplane mode." The airplane mode feature in newer versions of mobile operating systems may not disable Bluetooth, Bluetooth Low Energy (BLE), Wi-Fi, and other wireless protocols—or may only disconnect them temporarily. Examiners should manually confirm network connectivity has been disabled or consider alternate means of isolation, including placing the device in an RF shielded enclosure.

Be aware that RF shielding containers are not always fully effective at shielding all signals. Faraday shielding (physical shielding) can drain the device's battery as it may force the device to continuously search for signals, using more power in the process. While power should be maintained via an external power source, it is pertinent that the power source does not breach the RF shield. For example, a cable should not go from the mobile device inside of the Faraday enclosure to an external power source.

Remember that even a momentary exposure to networks can be destructive to data. When transferring from one Faraday space to another, ensure that the device never breaks RF shielding. When using a Faraday room, be cognizant of opening doors. If a Faraday vestibule exists, ensure only one door is open at a time. Regularly test these RF shielding containers to confirm their effectiveness. Refer to Katz's *A Field Test of Mobile Phone Shielding Devices.*

5.3.3.4 Immediate Movement to Acquisition

Immediacy in movement to acquisition is considered critical in order to preserve artifacts that become unrecoverable over time.

5.3.4 Device Unlocked – YES – Unknown Passcode

When the passcode is unknown, there are still steps that can be taken to acquire data in many circumstances depending on the make/model/operating system on the mobile device and the tools available to the examiner at the time.

5.3.4.1 Maintain Power

Connect the mobile device to a consistent external power source. It is important that power be maintained such that the device does not reboot resulting in less data availability.

5.3.4.2 Network Isolation

See 5.3.3.3.

5.3.4.3 Immediate Movement to Acquisition

See 5.3.3.4.

5.3.5 Device Unlocked – NO

Frequently, devices are encountered in a locked state. These locks can be password-based, pattern-based, GPS-based, or biometric in nature (e.g., fingerprint scanner or face unlock). Devices restrict access to user data while in a locked state differently depending on the device.

5.3.5.1 Maintain Power

See 5.3.4.1.

5.3.5.2 Network Isolation

See 5.3.3.3.

5.3.5.3 Immediate Movement to Acquisition

See 5.3.3.4.

5.4 Device – OFF

When a device is received in the OFF state, recovery may still be possible, but the device will need continued assessment to determine the most appropriate steps.

5.4.1 Leave Off

When a mobile device is recovered in an off state, it is essential to leave it powered off. Do not apply power. Additional power cycles may affect data availability. Some devices power on automatically when connected to a power source.

5.4.2 Device Damaged - YES

If a device is received in a damaged condition, please refer to *SWGDE 14-F-004-1.1 Best Practices for Collection of Damaged Mobile Device*.

Applying power may cause additional damage and the device should not be connected to any power source (i.e., battery or power adapter). Physical damage is not always indicative of device inoperability or the impossibility of data recovery. The type of damage (if known) should always be documented and communicated to the examiner. The need to conduct additional forensic processes on mobile devices (e.g., DNA, latent (prints)) should be discussed before any cleaning efforts. Discussions with lab personnel will help determine the order in which those processes should be performed.

5.4.2.1 Device in Liquid - YES

Devices previously submerged, but no longer in liquid, should be submitted to mobile forensics trained personnel for immediate processing.

When collecting liquid damaged devices, a key objective is to get the device before a properly trained examiner as soon as possible. If a mobile device was previously submerged in liquid, the battery should be removed at the time of collection (if possible). Attempts to power on the device may result in additional damage. Individuals collecting damaged devices should notify the lab of any known liquid damage or exposure at the time of laboratory submission.

5.4.2.1.1 Keep in Same Liquid

Devices discovered submerged in liquid should be collected in a watertight container with sufficient liquid to submerge the device. The device should remain immersed in the same liquid (e.g., pond water) until the time of the examination. The device should then be transported to the

lab for processing as soon as possible. Devices found submerged in flammable, caustic, or bio-hazardous liquids require remediation on-scene before transporting them to the lab.

5.4.2.1.2 Deliver to Appropriate Personnel

Liquid-damaged devices should be transported to the lab as soon as possible.

5.4.2.2 Device in Liquid – NO

If the device is not in liquid, care should still be taken in processing the mobile device.

5.4.2.2.1 Physical Network Isolation

See 5.3.3.3 Network Isolation Settings based network isolation may not be feasible for damaged devices. Utilize physical network isolation methods.

5.4.2.2.2 Movement to Acquisition

See 5.3.3.4.

5.4.3 Device Damaged – NO

A mobile device that is off and has no signs of physical damage still requires specific collection and preservation steps.

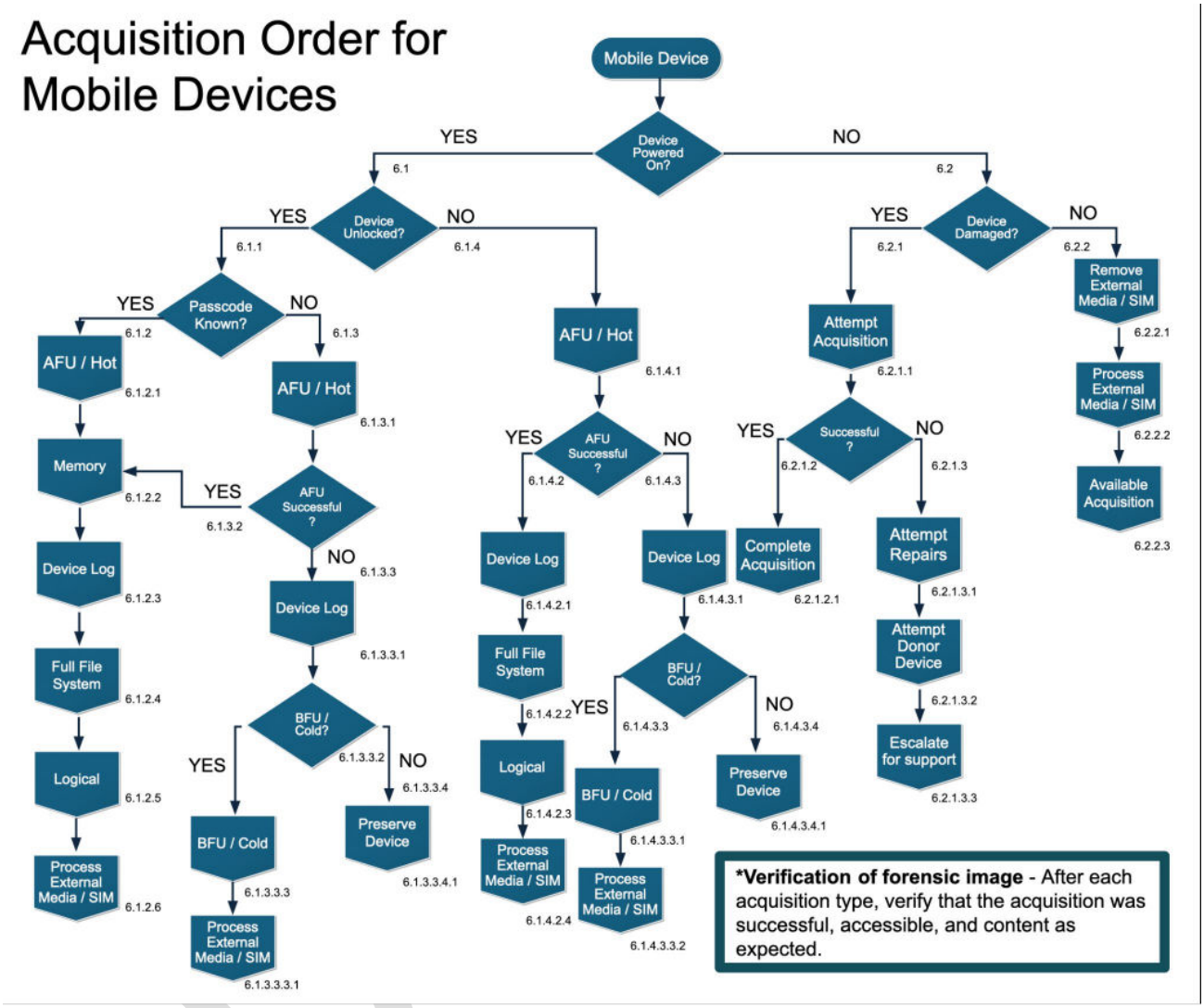
5.4.3.1 Physical Network Isolation

See 5.3.3.3. Network Isolation Settings based network isolation may not be feasible for damaged devices. Utilize physical network isolation methods.

5.4.3.2 Movement to Acquisition

See 5.3.3.4.

6. Acquisition Order for Mobile Devices



The flow chart above is not all-inclusive for all mobile devices/versions. Device/version specific expertise may be necessary in order to obtain access and may alter the foregoing workflow.

The types of extraction and analysis required depend on the request and the specifics of the investigation. Each mobile forensics acquisition method has its own corresponding skill set, tool set, and complexities. The methods described below are organized alphabetically, not in order of operations. Please refer to the "Acquisition Order for Mobile Devices" flowchart to determine the acquisition order based on the state of the device.

- **Device Logs**: A process of extracting available device, system, and crash logs (e.g., Sysdiagnose, unified logging, live system logs, and other crash reports) for analysis. As some of these logs are intended for operating system diagnostics, they are often available

in alternate device states and can be created even when the operating system is not user-accessible.

- **File System**: A process that requests the active files and folders from the file system. This acquisition can contain remnants of deleted data and non-user data. File System acquisitions include:
    - **After First Unlock (AFU/Hot)**: A collection of available data from a powered-on device that has been unlocked at least once since the last operating system boot.
    - **Before First Unlock (BFU/Cold)**: A collection of available data from a powered-on, locked device that has not been unlocked since the last operating system boot. This extraction contains a limited dataset when compared to AFU, Full File System, or Logical extractions.
    - **Full File System (FFS)**: A complete collection of all available active files and folders.
    - **Partial File System**: A partial collection of active files and folders from the file system. Partial File System extractions include, but are not limited to, AFU and BFU.
- **Logical**: A process that requests file data from the operating system, which then interprets and returns the resultant data. Various techniques query the operating system in order to extract the data. These techniques can include, but are not limited to, backup utilities, application agents, and manual interaction. Manual interaction involves direct interaction with the device display to photograph/video/document data accessible via the user interface.
- **Physical**: A process that extracts data via a direct connection to the device storage area. This includes Boot Loader, Chip-Off, In-system Programming (ISP), and Joint Test Action Group (JTAG) acquisitions. The resultant data from a device that utilizes File-Based Encryption (FBE) or Full-Disk Encryption (FDE) will be encrypted. At the time of publication, methodologies do not allow for decryption of FBE data. The ability to decrypt FDE data varies.
    - **Boot Loader**: Code that executes in a runtime environment prior to operating system initialization. Physical acquisitions using this method replace the existing code.
    - **Chip-Off**: A destructive process that involves the removal and reading of a memory chip to conduct analysis. Please refer to the *SWGDE 15-F-002-1.0 Best Practices for Chip-Off* document for more information.
    - **In-System Programming (ISP)**: A process to read data from an embedded Multi-Media Card (eMMC) chip. This process involves the disassembling of a device and connecting to appropriate locations on the Printed Circuit Boards

(PCB) that trace back to the eMMC without removing the eMMC from the PCB. When a pinout is unknown, a test device should be used to determine the pinouts, as the process is destructive to the device. ISP is not applicable if the card storage is set to "Adoptable" as the data will be encrypted.

- **Joint Test Action Group (JTAG)**: The Joint Test Action Group is an association that authors PCB testing via the *IEEE 1149.1-2013 Standard Test Access Port and Boundary Scan Architecture* [1]. In physical acquisitions, data is acquired via connection to these defined test access ports. This method involves disassembling a device and connecting to JTAG defined locations on the PCB.

- **File-Based Encryption (FBE)**: In the context of mobile forensics, FBE refers to a method of protecting files on storage media by using unique encryption keys per file.
- **Full-Disk Encryption (FDE)**: In the context of mobile forensics, FDE refers to a method of protecting a specific storage area using a single encryption key.[1]

6.1 Device – ON

The first step in determining the acquisition order is to determine if the device is on or off. Next check to see if the device is unlocked.

6.1.1 Device Unlocked – YES

If the device is unlocked, next determine if the passcode is known.

6.1.2 Device Unlocked – YES – Known Passcode

If a password for the device is recovered, the password should be tested by using methods other than locking the phone. An example of this is manually interfacing with a device's passcode settings, which will generally require a passcode entry.

6.1.2.1 AFU (Hot)

When the device is unlocked with a known passcode, first create an AFU extraction if available methodology exists for make/model device.

6.1.2.2 Memory

If memory analysis is considered to be critical to a case, ensure steps are taken to prevent bit rot which may have a detrimental effect on the analysis of the dump. Bit rot is a type of data corruption and if it has occurred on the device during the extraction then the extraction will not be suitable to use for analysis. There are ways to minimize bit rot, such as freezing the handset

[1] Note: Mobile device acquisition tools may offer multiple acquisition methods (often depending on the tool vendor) and tool capabilities may vary according to device manufacturer, model, operating system, software, and/or network provider. As a result, the examiner may need to employ tools from multiple vendors and run acquisitions at multiple levels in order to maximize the volume of recovered data.

before dumping the RAM, it is not recommended to leave a device in the freezer for longer than 25 minutes. Bit rot can be detected by looking at an extraction with a hex viewer. Bit rot causes an unusual number of bits in a byte to be set, so an extraction with more bits set over the course of a page at the beginning, in the middle and at the end would indicate that an extraction may be corrupted. See "Section 2.2: The Cold Boot Attack" and "On the Practicability of Cold Boot Attacks."

6.1.2.3 Device Log

Trigger and/or collect appropriate device logs. Some device logs, such as Sysdiagnose, will be available in a full file system extraction. Some logs may need to be extracted separately.

6.1.2.4 Full File System

Next attempt a full file system acquisition for the mobile device.

6.1.2.5 Logical

There are multiple ways to obtain a logical acquisition providing varying amounts of data collection. Logical collections also include backups which may be available on peripheral devices. Backups may be password protected and/or encrypted. If possible, obtain passwords for backup encryption as they are often different from device passwords.

It is recommended that manual acquisition be utilized as a last resort as means of digital acquisition. If manual acquisition is conducted, it is recommended to do such with video recording of the acquisition as the device is manually manipulated.

Ensure that the logical acquisition includes any external media being read through the device allowing for an acquisition to ensure data is available from both adoptable and portable media.

It is important to consider not only methods that require interaction with the mobile device itself, but also those logical extractions from cloud sources. See *SWGDE 19-F-002-1.0 Best Practices for Digital Evidence Acquisition from Cloud Service Providers*.

6.1.2.6 Process External Media/SIM

When possible, process external media outside of the mobile device, even if the storage area was acquired from within the mobile device. This allows for a physical acquisition of storage media as opposed to limiting to a file system acquisition. Acquisition of adoptable storage may be futile due to device-based encryption.

6.1.3 Device Unlocked – YES – Unknown Passcode

Data acquisition may be possible of an unlocked device even when a passcode is unknown.

6.1.3.1 AFU (Hot)

When the device is unlocked with an unknown passcode, first create an AFU extraction if available methodology exists for make/model device.

6.1.3.2 AFU Successful – YES

If AFU extraction is successful continue with steps from 6.1.2.2 through 6.1.2.6.

6.1.3.3 AFU Successful – NO

Even when an AFU extraction is unsuccessful there may be other methods of obtaining data

6.1.3.3.1 Device Log

See 6.1.2.3.

6.1.3.3.2 BFU (Cold)

When the device is unlocked with an unknown passcode, and an AFU extraction is unsuccessful, consider if your situation necessitates placing the device into a cold state. In some situations, exigency may require any data available be obtained, in other situations it may be more prudent to wait until a methodology for a more complete extraction becomes available. **Choosing to place a device in BFU mode may reduce future data availability**. Memory acquisitions may be an option, but also require the device to be rebooted. A memory acquisition may include a password allowing for other acquisitions. If it is decided to wait, continue to maintain the device in a powered-on state and prevent reboot via any means available.

6.1.3.3.3 BFU (Cold) Successful – YES

In some cases, it will be determined to place the device in a BFU state to obtain a limited BFU extraction.

6.1.3.3.3.1 Process External Media/SIM

See 6.1.2.6.

6.1.3.3.4 BFU (Cold) Successful – NO

Sometimes a BFU extraction is not available.

6.1.3.3.4.1 Preserve Device

The device should be preserved in the event acquisition capabilities for the device become available at a later time.

6.1.4 Device Unlocked – NO

In the event that a device is powered on and locked, there may be options for data acquisition.

Consideration should be given when making attempts at an unknown passcode. A mobile device may be configured to erase its contents after a select number of failed passcode/password attempts. It is important to annotate password attempts.

In some cases, biometrics may be used to unlock a device. However, biometric unlocks may be limited in time availability and still may require passcode to perform an acquisition.

Existing solutions may provide bypass or brute force options. However, brute force options may in some situations require excessive timeframes (e.g., years) to complete.

Consideration should be given to searching for a backup stored on a peripheral device, or in a cloud-based iCloud account. A backup stored on a computer may contain a pairing record (lockdown file) between the computer and the phone which could be used to gain access to a locked device. These pairing records do expire over time and may reset after a device has been rebooted; thus, requiring a passcode in order to be unlocked.

6.1.4.1 AFU (Hot)

When the device is locked and the passcode is unknown, first attempt an AFU extraction if available methodology exists for the device.

6.1.4.2 AFU Successful - YES

If AFU extraction is successful, continue with steps from 6.1.4.2.1 through 6.1.4.2.4

6.1.4.2.1 Device Log

See 6.1.2.3.

6.1.4.2.2 Full File System

If a password was recovered from an AFU acquisition, proceed with a Full File System acquisition. See 6.1.2.4.

6.1.4.2.3 Logical

If a password was recovered from an AFU acquisition, proceed with a logical acquisition. See 6.1.2.5.

6.1.4.2.4 Process External Media/SIM

See 6.1.2.6.

6.1.4.3 AFU Successful – NO

If the AFU extraction is not successful, continue with Device Log extraction.

6.1.4.3.1 Device Log

See 6.1.2.3.

6.1.4.3.2 BFU (Cold)

When the device is locked and an AFU extraction is unsuccessful, consider if your situation necessitates placing the device into a cold state. In some situations, exigency may require any data available be obtained, in other situations it may be more prudent to wait until a methodology for a more complete extraction becomes available. **Choosing to place a device in BFU mode may reduce future data availability**. Memory acquisitions may be an option, but also require the device to be rebooted. A memory acquisition may include a password allowing for other

acquisitions. If it is decided to wait, continue to maintain the device in a powered-on state and prevent reboot via any means available.

6.1.4.3.3 BFU (Cold) Successful – YES

See 6.1.3.3.3.

6.1.4.3.3.1 Process External Media/SIM

See 6.1.2.6.

6.1.4.3.4 BFU (Cold) Successful – NO

See 6.1.3.3.4.

6.1.4.3.4.1 Preserve Device

See 6.1.3.3.4.1.

6.2 Device – OFF

If the device is off, leave it off. Collect identifying data about the device, such as model number, carrier and unique identifiers that are visible.

6.2.1 Device Damaged – YES

Despite damage to a device, acquisitions may be possible via tooling or advanced methods.

6.2.1.1 Attempt Acquisition

Damaged devices present a unique situation and such methods available will vary. Follow best practices for damaged devices. See *SWGDE 14-F-004-1.1 Best Practices for Collection of Damaged Mobile Devices*.

6.2.1.2 Acquisition Successful – YES

Sometimes a damaged device can be acquired via normal means.

6.2.1.2.1 Complete Acquisition

Attempt to obtain the most comprehensive acquisition(s) available.

6.2.1.3 Acquisition Successful – NO

Sometimes damaged devices cannot be acquired via normal means. At this time, work with trained personnel on further steps 6.2.1.3.1–6.2.1.3.3.

6.2.1.3.1 Attempt Repairs

Skilled and trained personnel should attempt repairs. It is important to note that irreparable damage could occur from attempting a repair.

6.2.1.3.2 Attempt Donor Device

In some instances, it is valuable to find an equivalent device to facilitate repair.

6.2.1.3.3 Escalate for Support

In some instances, repair requirements may exceed capabilities, equipment, and training of organization personnel and may require escalation to specialized facilities.

6.2.2 Device Damaged – NO

Devices are at times received in an off state without damage.

6.2.2.1 Remove External Media/SIM

With a device in an off state, it is recommended to remove external media prior to processing.

6.2.2.2 Process External Media/SIM

See 6.1.2.6.

6.2.2.3 Perform Available Acquisition

Reinstall removed external media and/or SIM. Then perform the most comprehensive acquisition(s) available.

7. References

[1] Institute of Electrical and Electronics Engineers (IEEE). *Standard Test Access Port and Boundary Scan Architecture.* IEEE 1149.1-2013. *IEEE Explore,* May 2013, https://ieeexplore.ieee.org/document/6515989.

8. Additional Resources

- Gruhn, Michael, and Tilo Müller. "On the Practicability of Cold Boot Attacks." *Fredrich-Alexander-Universität Erlangen-Nürnberg*, Germany. *CyberSiDE Mirrors*, 2013, https://cyberside.net.ee/docs/fares_coldboot.pdf. Accessed 15 Jan. 2025.
- Katz, Eric. *A Field Test of Mobile Phone Shielding Devices*. 2010. Purdue University, MA thesis. *Purdue e-Pubs*, https://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1033&context=techmasters.
- Müller, Tilo, et al. "Section 2.2: The Cold Boot Attack." *Frost: Forensic Recovery of Scrambled Telephones*. Department of Computer Science, Friedrich-Alexander University of Erlangen-Nuremberg, 2012, https://faui1-files.cs.fau.de/filepool/projects/frost/frost.pdf. Accessed 15 Jan. 2025.
- National Institute of Standards and Technology (NIST). *Computer Forensics Tool Testing Program (CFTT).* Software Quality Group, *NIST,* 2018, https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt. Accessed 15 Jan. 2025.

- Scientific Working Group on Digital Evidence (SWGDE). *Best Practices for Chip-off*. SWGDE 15-F-002-1.0. *SWGDE*, 2015, https://www.swgde.org/15-f-002/.
- Scientific Working Group on Digital Evidence (SWGDE). *Best Practices for Collection of Damaged Mobile Devices*. SWGDE 14-F-004-1.1. *SWGDE*, 2014, https://www.swgde.org/14-f-004/.
- Scientific Working Group on Digital Evidence (SWGDE). *Best Practices for Digital Evidence Acquisition from Cloud Service Providers*. SWGDE 19-F-002-1.0. *SWGDE*, 2019, https://www.swgde.org/19-f-002-archive/.
- Scientific Working Group on Digital Evidence (SWGDE). *Best Practices for Examining Mobile Phones Using Joint Test Action Group (JTAG).* SWGDE 15-F-001-1.0. *SWGDE*, 2015, https://www.swgde.org/15-f-001/.
- Scientific Working Group on Digital Evidence (SWGDE). *Considerations for Required Minimization of Digital Evidence Seizure*. SWGDE 16-F-002-2.1. *SWGDE*, 2016, https://www.swgde.org/16-f-002/.
- Scientific Working Group on Digital Evidence (SWGDE). *Core Competencies for Mobile Phone Forensics.* SWGDE 12-F-003-1.0. *SWGDE*, 2012, https://www.swgde.org/12-f-003/.
- Scientific Working Group on Digital Evidence (SWGDE). *Guidelines & Recommendations for Training in Digital & Multimedia Evidence*. SWGDE 10-Q-002-3.0. *SWGDE*, 2010, https://www.swgde.org/10-q-002/.
- Scientific Working Group on Digital Evidence (SWGDE). *Minimum Requirements for Testing Tools Used in Digital and Multimedia Forensics.* SWGDE 18-Q-001-2.0. *SWGDE*, 2018, https://www.swgde.org/18-q-001-2/.

9. History

Revision	Issue Date	History
1.0 DRAFT	6/14/2018	Initial draft created and SWGDE voted to approve as Draft for Public Comment.
1.0 DRAFT	7/30/2018	Formatted for release as a Draft for Public Comment.
1.1 DRAFT	9/20/2018	Content updates and edits to most sections following initial Public Comment period. SWGDE voted to approve as a Draft for Public Comment.
1.1 DRAFT	11/20/2018	Formatted for release as a Draft for Public Comment.
1.1	6/6/2019	Minor edits were made to section 4.3.2 following the Public Comment period. SWGDE voted to approve as a Final Approved Document.
1.1	7/16/2019	Formatted for release as a Final Approved Document.
1.2 DRAFT	1/15/2020	Content update to section 5. SWGDE voted to approve as a Draft for Public Comment. Formatted for release as a Draft for Public Comment.
1.2 DRAFT	9/17/2020	No comments received. SWGDE voted to approve as a Final Approved Document. Formatted for release as a Final Approved Document.
2.0 DRAFT	1/16/2024	Major revisions made to the document.
2.0 DRAFT	1/15/2025	SWGDE voted to approve as a Draft for Public Comment.
2.0 DRAFT	2/7/2025	Formatted for release as a Draft for Public Comment.