SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition

Disclaimer:

As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall 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; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

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 the SWGDE cover page containing the disclaimer.
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 create date) of the document and mention 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 forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) 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)

ARCHIVED

h) Basis for change

Intellectual Property:

Unauthorized use of the SWGDE logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate 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 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.

ARCHIVED

SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition

Table of Contents

1. Purpose and Scope 4
2. Disclaimer 4
3. Considerations 4
4. Evidence Collection & Preservation 6
4.1 Preparation 6
4.2 Documentation 6
4.2.1 Documenting the Scene 6
4.3 Evidence Preservation Process for First Responders 6
4.3.1 iOS Preservation Process and Flowchart 7
4.3.2 Android Preservation Process and Flowchart 8
4.4 Peripherals 10
5. Evidence Handling 10
5.1 Damage 10
5.2 Traditional Forensics 10
5.3 Access 11
5.3.1 Smart Locks 11
5.3.1.1 Device Powered On and Locked 11
5.3.1.2 Device Powered On and Unlocked 12
5.3.1.3 Mobile Device Management (MDM) 12
5.3.1.4 Physical Encryption 12
5.3.1.5 Backup Encryption 12
5.4 Network Isolation 13
6. Evidence Acquisition 13
6.1 Equipment Preparation 13
6.2 Device Identification 13
6.3 Extraction Methods 14
6.3.1 Extraction of Mobile Device Storage 14
6.3.2 Removable Media 15
6.3.3 GSM Mobile Device Considerations 15

ARCHIVED

6.3.4 iOS Device Considerations 15
6.3.5 Android Device Considerations 15
6.3.6 Other Mobile Device Data Sources 16
6.3.7 Synchronization 16
6.3.8 Cloud Based Services for Mobile Devices 16
6.3.9 Archive 17
7. References 17

ARCHIVED

1. Purpose and Scope

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

This document provides best practices for the collection, preservation, and acquisition of evidence from mobile devices. The collection and preservation of data from mobile devices is performed in the field, as well as the lab. Increasingly, field personnel are also performing acquisitions. This document provides best practices for the three functions that are likely to be needed by field personnel. The intended audience is personnel qualified to collect, preserve, or acquire digital evidence. For guidance on recommended training and qualifications, see *SWGDE/SWGIT 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 proprietary interfaces, sometimes making it difficult to extract digital evidence. Version specific expertise may be necessary to attain access, and may alter workflows listed below.

Examples encountered are as follows:

- **Incoming and Outgoing Signals** – Attempts should be made to block incoming and outgoing signals of a mobile device. A common method includes Radio Frequency (RF) blocking containers (e.g., Faraday bag or room). RF signal blocking containers may not

always be successful. They may drain the battery and failure may result in data alteration. Refer to section ***5.4 Network Isolation*** for additional information.

- **Cables** – Data cables can be unique to a particular device and forensic tool.
- **Destruction of Data** – There are methods to destroy data locally and remotely on a mobile device. This is why the device must be isolated from all networks (e.g., carrier, WiFi, Bluetooth) as soon as possible. Examiners should be cognizant that a mobile operating system may have automated processes which will destroy data on power-on, or after a specific duration of time, and choose an extraction method or schedule that addresses these concerns where applicable.
- **Drivers** – Conflicts may occur due to existing operating system drivers, proprietary drivers, driver version inconsistencies, and vendor specific drivers. Ability to find proper drivers may be difficult. Drivers may be included with a forensic tool or downloaded from a website. Drivers may compete for control for the same resource if more than one forensic product is installed on the analysis machine.
- **Dynamic Nature of the Data** – Data on active (powered-on) mobile devices is constantly changing. There are no write-blocking methods for mobile devices.
- **Encryption** – Data may be stored in an encrypted state preventing access or analysis.
- **Equipment** – Equipment used during examinations may not be the most recent version due to a variety of reasons, such as purchasing / budgeting delays or verification requirements of hardware, firmware, or software.
- **Field analysis** – Triaging mobile devices is not considered a full examination. However, if a triage is performed, the device should be protected and isolated from all networks.
- **Inconsistent Industry Standards** – Manufacturers and carriers may use proprietary methods to store data (e.g., closed operating systems, proprietary data connections).
- **Loss of Power** – Many mobile devices may lose data or initiate additional security measures once powered off.
- **Passwords** – Authentication mechanisms can restrict access to a device and its data. Traditional password cracking methods can lead to permanent inaccessibility or destruction of data.
- **Removable Media Cards** – Processing media cards while still inside the device poses risks (e.g., not obtaining all data including the deleted data, altering date/time stamps).
- **Identity Module e.g., USIM, CSIM, RUIM Cards** – 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.
- **Training** – The individual collecting, examining, and analyzing a mobile device should be trained to preserve and maintain data integrity.
- **Unallocated Data / Deleted Data** – Mobile device forensic tools may support only a logical acquisition of data that may limit the amount of data that can be recovered.

ARCHIVED

4. Evidence Collection & Preservation

4.1 Preparation

Determine the necessary equipment to take to the scene. Ensure there is legal authority to collect the evidence to be acquired.

4.2 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, presence of a passcode, presence of a passcode), examiner interactions with the device, and physical characteristics of each device (e.g., damage, identifying information such as the make, model, serial number, and any identifying marks, and connections).

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

4.2.1 Documenting the Scene

- Accurately identify and account for evidence. Non-electronic materials such as invoices, manuals, and packaging material may yield useful information about the capabilities of the device, its network, associated account, manufacturer, model, and unique identifiers (e.g., IMEI, MEID, ESN, MAC address), including unlock codes. Photographing the scene in conjunction with documenting the state of each digital device encountered may be helpful in the investigation.

- Photograph relevant digital devices and peripherals (e.g., cables, power connectors, removable media, and connected items) as a part of thorough scene documentation. Avoid touching or contaminating the mobile device when photographing it and the environment where found. If the device's display is in a viewable state, any changes should be photographed and documented until the device is powered-off or in an unresponsive state.

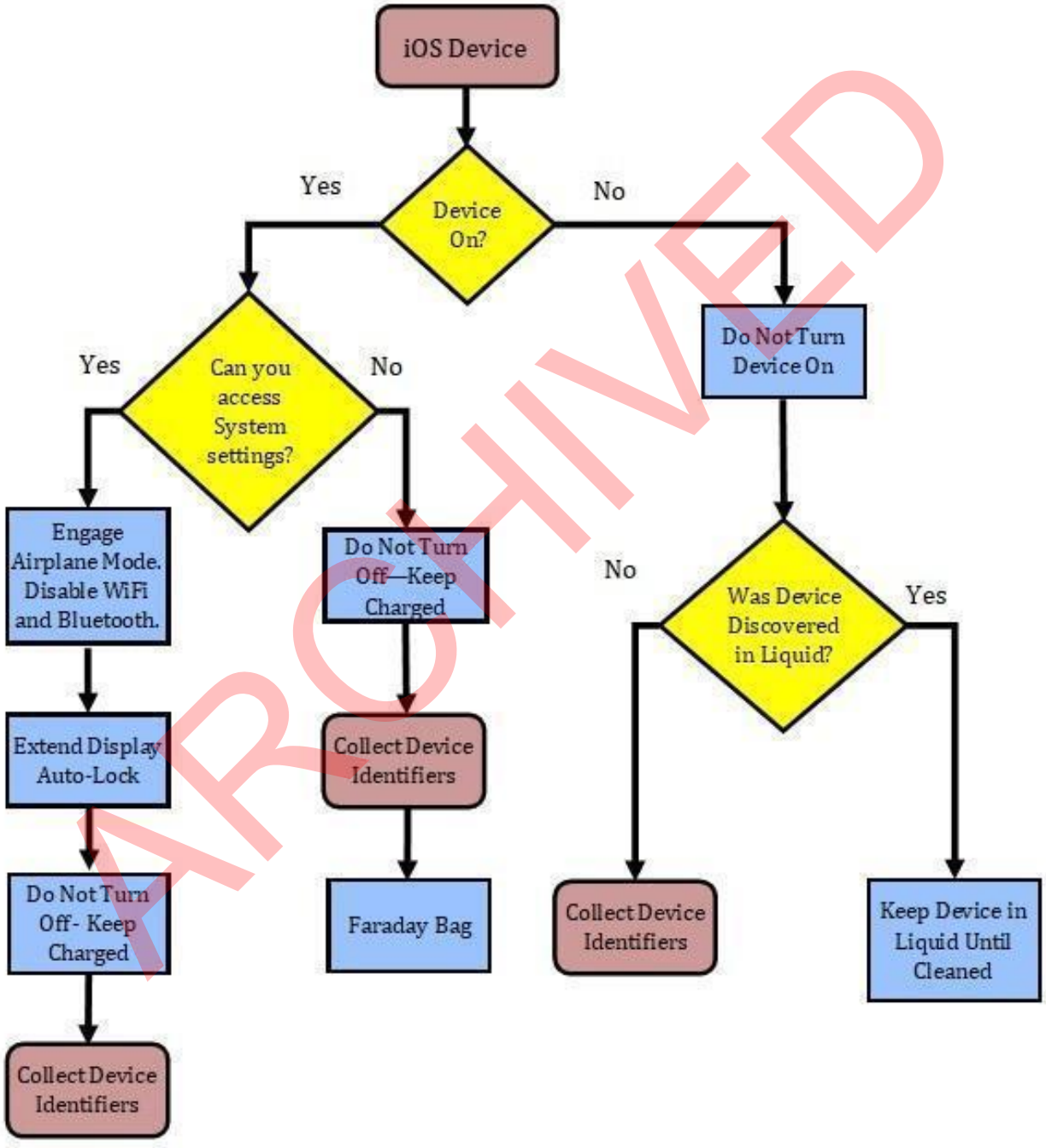
4.3 Evidence Preservation Process for First Responders

The following flow charts provide a basic overview of the best practices for preserving evidence when seizing particular types of mobile devices and is not meant to be all encompassing. Circumstances may warrant deviation from the procedures outlined herein. Subjects should not be permitted to handle a device or be provided access to evidence unless deemed necessary to facilitate access to the device (e.g., subject applies biometric identifiers or enters a passcode).

ARCHIVED

4.3.1 iOS Preservation Process and Flowchart

iOS is a mobile operating system created and developed by Apple exclusively for its mobile hardware, including the iPhone, iPad, and iPod Touch. The following flowchart details steps that should be taken to preserve digital evidence on an iOS device.



ARCHIVED

The flow chart above is not all-inclusive for all versions of iOS. Version specific expertise may be necessary in order to obtain access and may alter the foregoing workflow. If the device is powered on, it may contain volatile data, including encryption keys, and should not be turned off. A power source should be connected as soon as possible to prevent the device from powering down. Be sure to seize the charging cable to keep power to the device. It may be possible to adjust the Display Auto-Lock feature to extend the length of time before Auto-Lock is enabled. If the device is unlocked, the examiner should take steps to prevent its locking, such as disabling the lock code or repeatedly interacting with the touch-screen.

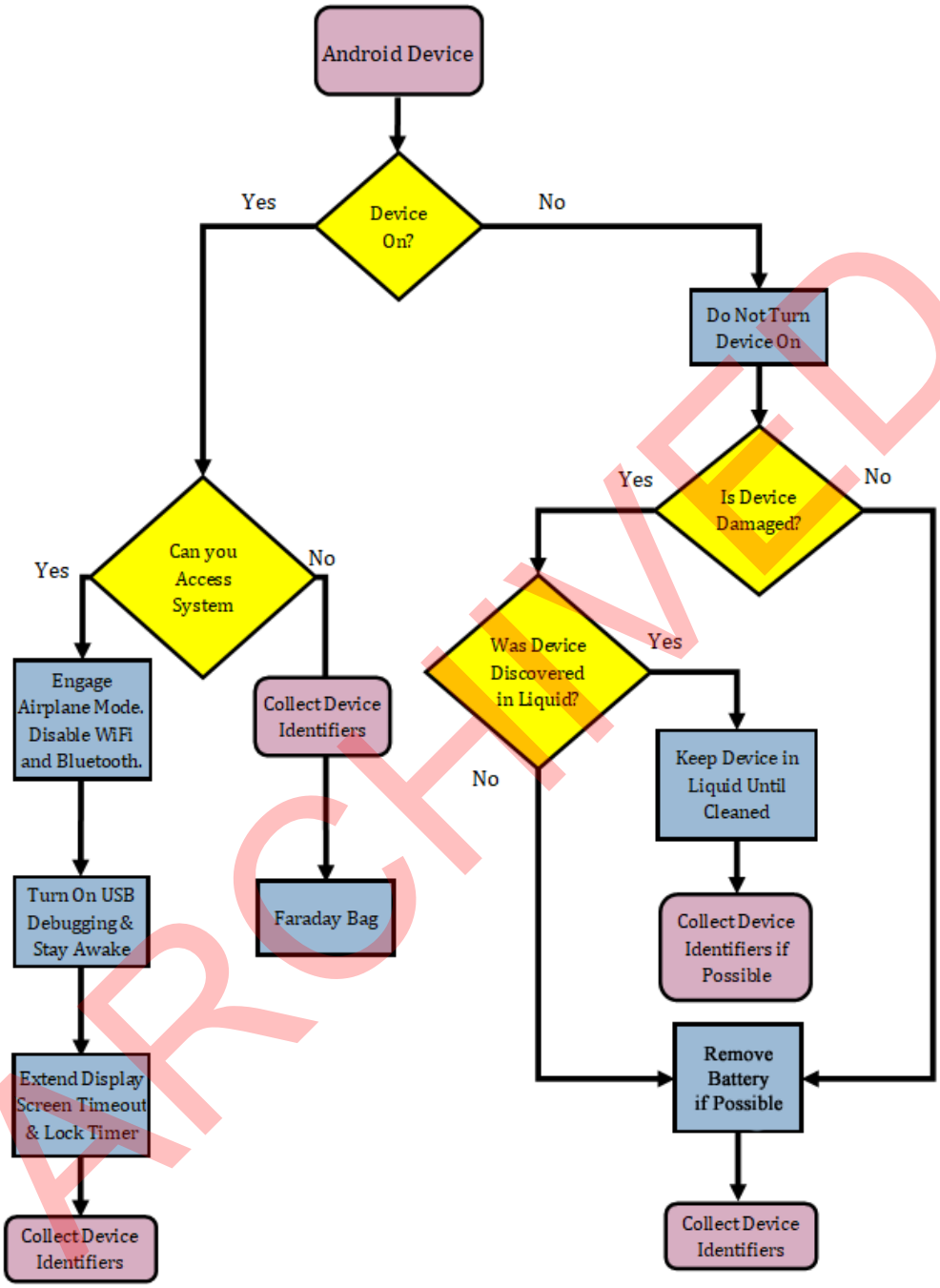
Place the device in "Airplane Mode" (by swiping up from the bottom and selecting airplane mode) and verify that WiFi and Bluetooth are off. If the device cannot be placed in "Airplane Mode," put it in a Faraday bag to prevent network interaction from potentially altering data on the device. Mobile devices blocked from connecting to a network will boost power output while trying to obtain a signal. This will drain a device's battery at an accelerated rate. If it is necessary to keep the device powered on, connect it to an external power source such as a portable battery pack. Both the mobile device and the charging source should be placed inside the Faraday bag. If the charging source is not placed in the Faraday bag, the cable can act as an antenna and the device may be able to connect to the network.

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.

4.3.2 Android Preservation Process and Flowchart

Android is a Linux-based mobile operating system developed by Google and has the largest install base of any mobile operating system. Android is available in many different versions and, unlike iOS, is offered on devices manufactured by numerous companies. The following flowchart details steps that should be taken to preserve digital evidence on an Android device.

ARCHIVED



ARCHIVED

The flow chart above is not all-inclusive for all versions of Android. Version specific expertise may be necessary in order to attain access; and may alter the foregoing workflow. If the device is powered on, it may contain volatile data, including encryption keys, and should not be turned off. A power source should be connected as soon as possible to avoid the device powering down. Be sure to seize the charging cable to keep power to the device. If the device is unlocked, the

examiner should take steps to prevent its locking such as disabling the lock code or repeatedly interacting with the touch-screen. It may be possible to adjust the Display Screen Timeout feature to extend the length of time before Auto-Lock is enabled.

Place the device in "Airplane Mode" (by swiping down from the top and selecting airplane mode) and verify that WiFi and Bluetooth are off. In order to give the best chance of accessing the evidence at a later date, enable USB debugging, if possible.

If the device cannot be placed in "Airplane Mode", put it in a Faraday bag to prevent network interaction from potentially altering data on the device. Mobile devices blocked from connecting to a network will boost power output while trying to obtain a signal. This will drain a device's battery at an accelerated rate. If it is necessary to keep the device powered on, connect it to an external power source such as a portable battery pack. Both the mobile device and the charging source should be placed inside the Faraday bag. If the charging source is not placed in the Faraday bag, the cable can act as an antenna and the device may be able to connect to the network.

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.

4.4 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, Internet of Things (IoT) devices).

5. Evidence Handling

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

5.1 Damage

Foreign substances on or in, or other damage to a mobile device may complicate, but not necessarily prevent the recovery of data. Repairing damaged components on a mobile device and restoring the device to working order for examination and analysis may be possible. Given the potential for the spread of blood-borne pathogens or electric shock due to a contaminated or damaged device, suitable precautions must be used to protect the health and safety of the examiner and the integrity of the device during seizure and subsequent data recovery. Personnel should adhere to agency-specific procedures and follow the guidance provided in *SWGDE Best Practices for Collection of Damaged Mobile Devices*. Any damage or other related device condition should be documented and shared with any subsequent evidence custodian or examiner.

5.2 Traditional Forensics

Traditional forensic processes, such as fingerprints or DNA testing, may need to be conducted in order to establish a link between a mobile device and its owner or user. If the device is not handled properly during preservation and collection, physical evidence can be contaminated and

ARCHIVED

rendered useless. As such, handle all potentially evidentiary items with 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 completed before digital forensic processes.

5.3 Access

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

5.3.1 Smart Locks

Advanced security features are natively available on some Android device models or can be installed 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 lock and unlock when a device detects it is "on-body" of the custodian or owner that originally unlocked the device. If a device is unlocked by the owner, as long as the phone senses it is still in possession of the owner it will stay unlocked. If the phone detects that it has been removed from the owner's custody (e.g. set down on a table) then the phone may lock. If the owner boards a vehicle or train, the phone may not lock for up to five to ten minutes. If the owner boards a plane, the phone may never lock. This should be considered when seizing or recovering a phone from someone's person.

- **Trusted Places:** This feature is designed to lock and unlock when the device detects it enters (unlocks) and leaves (locks) 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 phone detects that it leaves the location, it will automatically lock. This should be considered when seizing or recovering a phone before leaving the scene.

- **Trusted Devices:** This feature is designed to lock and unlock when a device is connected to another trusted Bluetooth device. For example, a user can set their watch as a trusted device. So when a phone is paired with a trusted device, it can be configured to remain unlocked and when this connection is severed, the device is locked again. This should be considered when seizing or recovering a device that is connected to Bluetooth.

5.3.1.1 Device Powered On and Locked

Consideration should be given when "guessing" the passcode. A user may enable their phone to erase its content after a select number of failed attempts. Although there are solutions that will brute-force a passcode, this method may take years to recover the passcode.

ARCHIVED

If a device is locked, consideration should be given to searching for a "backup" stored on a computer, external media, or in an 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.

5.3.1.2 Device Powered On and Unlocked

When a locked device is recovered in an unlocked state, the phone should be collected on-site as soon as possible. Ultimately, keep the phone awake using the least invasive method such as manually interacting with the screen, altering the auto-lock settings, or using an automated process that does not change a device's data. 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.

5.3.1.3 Mobile Device Management (MDM)

Some organizations may choose to restrict access on mobile devices issued to their employees. Using Mobile Device Management, an organization's system administrator can restrict many features of the device from a user. A common example includes blocking the phone's USB port access, which might make the acquisition of the device impossible. If the device is locked with MDM, examiners may need to seek assistance from the system administrator to extract data.

5.3.1.4 Physical Encryption

Physical, or full-disk encryption, encrypts the entire memory chip. This encryption can be enabled natively by the manufacturer, or if capable, enabled by the end user. Some physical encryption features require authentication prior to the booting process; whereas, others automatically decrypt all reads before returning it to the calling process but are stored on the chip in an encrypted state.

5.3.1.5 Backup Encryption

Encryption can be enabled on iOS device backups using the backup feature of Mac OS Finder, iCloud, and iTunes applications. The passwords for encrypted iOS backups stored on Windows or MacOS computers are defined by the user at the time of backing up an iOS device. This preference is persistent and will encrypt all future backups of that device until turned off. An unlocked device can be successfully acquired with backup encryption enabled but the password is required to access the data in a decrypted state. Tools exist to decrypt iOS devices and iOS backups using brute force or dictionary attacks. Additionally, tools exist with the capability to retrieve iOS backups from the Apple iCloud environment using the Apple iCloud username and password or the binary authentication token created by iCloud Control Panel and stored on a MacOS or Windows computer. To obtain data from a user's iCloud account, see *SWGDE Best Practices for Digital Evidence Acquisition from Cloud Service Providers*.

ARCHIVED

5.4 Network Isolation

Disconnect mobile devices from their networks to ensure data is not remotely modified or destroyed. Mobile devices typically have a reset capability that clears all user content, resetting device memory to the original factory condition. Because this may be performed in person or remotely, immediate precautions (e.g., separate the device from its user, network isolation) are necessary to ensure evidence is not modified or destroyed.

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, WiFi, 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, or utilizing a Cellular Network Isolation Card (CNIC) for GSM phones.

Powering off the device to isolate it from the network poses the risk of engaging authentication mechanisms (e.g., passwords, PINs) or enabling enhanced security features, potentially rendering data inaccessible.

6. Evidence Acquisition

6.1 Equipment Preparation

"Equipment" in this section refers to the hardware and software 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.[1]
- NIST provides test reports illustrating the capabilities and limitations of specific mobile device tools. See http://www.cftt.nist.gov/ for more information [1].

6.2 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 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 iPhones.

ARCHIVED

[1] The validation process is discussed in the documents titled "*SWGDE Recommended Guidelines for Validation Testing*" and "*SWGDE Requirements for Testing Tools Used in Digital & Multimedia Forensics*" available at https://www.swgde.org/documents.

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.

6.3 Extraction Methods

The level of extraction and analysis required depends on the request and the specifics of the investigation. Each acquisition level of mobile forensics has its own corresponding skill set, tool set, and risk. The levels are:

- **Manual** – A process that involves the manual operation of the keypad and handset display to document data present in the device's memory.
- **Logical** – A process that extracts individual files or objects.
- **File System** - A process that extracts files from a file system and may include data marked for deletion.
- **Physical (Non-Invasive)** – A process that provides physical acquisition of a device's data without requiring opening the case of the device.
- **Physical (Invasive)** – A process that provides physical acquisition of a device's data requiring disassembly of the device providing access to the circuit board.
    - **JTAG (Joint Test Action Group)** - A process that involves the disassembling of a device and connecting to test access ports.
    - **ISP (In-System Programming)** - A process that involves the disassembling of a device and connecting to memory chip pinouts.
    - **Chip-Off** – A destructive process that involves the removal and reading of a memory chip to conduct analysis.

Mobile device acquisition tools may offer multiple acquisition levels (often depending on the tool vendor) and tool capabilities may vary according to device type, manufacturer, and model. 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.

6.3.1 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. Because these techniques may leave behind digital artifacts, the examiner should document the use of these methods.

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 confirm 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.

ARCHIVED

6.3.2 Removable Media

Mobile devices may contain removable media. Mobile device forensic tools will often perform acquisitions for these types of removable media. If a mobile device is powered on, the removable media should remain in the device during extraction. If a mobile device is powered off, acquire the removable media separately from the device. If the live device is required to interpret data on the removable media, a separate acquisition may be considered once the removable media has been returned to the device.

6.3.3 GSM Mobile Device Considerations

For mobile devices requiring a UICC/SIM, examiners must acquire and examine both the device and the UICC/SIM(s).

If the device is powered off, the examiner should process the UICC/SIM first, before powering on the device or acquiring the device storage. If the mobile device is powered on, a joint extraction of the device and UICC/SIM should be completed before removing the UICC/SIM. Because a direct extraction may recover deleted messages not accessible via the device, the UICC/SIM should also be subsequently removed from the mobile device and inserted into an appropriate reader for a direct extraction.

If the device stores messages on the UICC/SIM, a joint extraction of the device and UICC/SIM may change the message status from “Unread” to “Read” during the extraction process. Where the message status matters to the investigation, examiners should perform separate and independent extractions (i.e. acquiring the UICC/SIM directly before acquiring the contents of the device).

6.3.4 iOS Device Considerations

Prior to iOS 11, a logical extraction of an iOS device could be performed on an unlocked device. Apple has instituted a new pairing procedure that requires the use of a device’s passcode in order to establish a trust relationship between the device and the computer; a logical extraction is possible only when the passcode is entered.

Many commercial acquisition tools perform an iTunes backup of the device; if a device user has enabled encrypted backups, the examiner will require the backup password to complete the acquisition or decrypt the acquired data.

If prompted, examiners should enable encryption for iTunes backups when conducting an extraction. Data tied to the keychain.plist file cannot be extracted without encryption enabled for the backup.

6.3.5 Android Device Considerations

Most of the access methods for locked Android devices rely on USB debugging mode being active on the device to begin the forensic data extraction process. Tool functionality exists that can enable this mode on some locked Android devices.

ARCHIVED

Obtaining data from locked Android devices may also be possible using JTAG[2] or chip-off[3] methods; however, acquiring data via this method on a device that uses full disk encryption will yield encrypted data.

6.3.6 Other Mobile Device Data Sources

In addition to data present directly on a mobile device and its associated external storage (e.g., its UICC/SIM or associated removable media), examiners should be aware of other data sources that may contain data relevant to the examined device.

Three primary examples are: data located on systems with which a mobile device is administered or synced, other devices such as smartwatches or tablets, and cloud-based mobile device services.

6.3.7 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.

6.3.8 Cloud Based Services for Mobile Devices

Cloud based services have augmented the capabilities of mobile devices in a number of ways. One of the most noticeable augmentations allows a mobile device to store and access data beyond its internal device storage limitation. Additionally, cloud services give mobile device users the ability to access the same piece of data across multiple platforms or devices. As it may not be readily apparent whether specific data is stored on the device or in the cloud, examiners should always consider the potential of cloud-based data as a vital component of their mobile device examination.

Various tools currently available provide the examiner the ability to connect directly to cloud storage and acquire the data. Cloud acquisitions present unique legal considerations, as the search may be deemed to occur outside the issuing jurisdiction. See *SWGDE Best Practices for Digital Evidence Acquisition from Cloud Service Providers*.

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. The enterprise's mobile device administrator may be able to assist examiners in gaining access to, or information about, the device being examined. Where an MDM solution manages a device, MDM policies may limit an examiner's access to

ARCHIVED

[2] Additional information about JTAG for mobile devices can be found in the document "*SWGDE Best Practices for Examining Mobile Phones Using JTAG*," available at https://www.swgde.org/documents.

[3] Additional information about Chip-Off for mobile devices can be found in the document "*SWGDE Best Practices for Chip-Off*," available at https://www.swgde.org/documents.

data on the device. Attempts to remove MDM policies may engage tamper protections, resulting in loss of data on the device.

6.3.9 Archive

Acquisition case files should be hashed and archived according to organizational policy and applicable laws. These case files may contain device acquisitions using a proprietary image format. Examiners should ensure these acquisitions are in a format that is accessible in the future.

7. References

[1] National Institute of Standards and Technology (NIST) (2018, February) Computer Forensics Tool Testing Program (CFTT), https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt.

ARCHIVED

SWGDE Best Practices for Mobile Device Evidence Collection & Preservation, Handling, and Acquisition

History

Revision	Issue Date	Section	History
1.0 DRAFT	2018-06-14	All	Initial draft created and voted by SWGDE for release as a Draft for Public Comment.
1.0 DRAFT	2018-07-30	All	Formatting and technical edit performed for release as a Draft for Public Comment.
1.1 DRAFT	2018-09-20	All	Content updates/edits to most sections following initial Public Comment period. Voted by SWGDE for re-release as a Draft for Public Comment.
1.1 DRAFT	2018-11-20	--	Formatted and posted as Draft for Public Comment.
1.1	2019-06-06	4.3.2	Minor edits were made following the Public Comment period. SWGDE voted to publish as an Approved document.
1.1	2019-07-16	--	Formatted and published as Approved version 1.0.
1.2	2020-01-15	5	Content update/edits to section. Voted by SWGDE for re-release as Draft for Public Comment.
1.2	2020-19-17		Voted for release as final publication
1.2	2025-10-17	ALL	Added ARCHIVED watermark.

ARCHIVED