SWGDE Best Practices for Mobile Device Forensic Analysis

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)
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.

SWGDE Best Practices for Mobile Device Forensic Analysis

Table of Contents

1. Purpose

The purpose of this document is to provide best practices for the analysis of data derived from mobile devices following a forensic acquisition. The intended audience is personnel tasked with analyzing data from mobile devices.

2. Scope

This document addresses artifacts commonly available for review with forensic software, identifies the differences in how mobile operating systems store key artifacts, and discusses advanced techniques for the analysis of data not parsed by forensic software.

This document is the second part of a planned set of best practice guides which includes *SWGDE Best Practices for Mobile Device Evidence Collection and Preservation, Handling, and Acquisition*, *SWGDE Best Practices for Mobile Device Forensic Analysis* (this document), *and SWGDE Requirements for Report Writing in Digital and Multimedia Forensics.* For guidance on recommended training and qualifications, see *SWGDE/SWGIT Guidelines & Recommendations for Training in Digital & Multimedia Evidence*.

3. Disclaimers

This document is not a step-by-step guide for conducting forensic analysis of mobile devices, nor is it intended to provide legal advice.

Mobile device forensic analysis can recover location data which is distinct from data derived from call detail records (CDRs) produced by cellular network providers. Inconsistencies between these two data sources, such as timestamp information and content, are expected and understandable because data is recorded and stored differently.

If confirmation of examiner-reported device locations is required, the examiner can obtain and verify locations via provider Call Detail Records (CDRs). Note: obtaining historical location detail records from a provider typically requires obtaining an additional legal order. For further information regarding historical cell site analysis, see *SWGDE Recommendations for Cell Site Analysis.*

4. Preparations

Examiners should review documentation provided by the requestor to determine the processes necessary to complete the analysis while staying within the scope of the investigation. Examiners should maintain communication with the requestor and communicate any restrictions, deviations, or limitations that may arise during analysis. In addition, examiners should review documentation provided by the requestor to determine whether proper legal authority has been given to perform the analysis. Authority may be granular and restrict analysis; for example, specifying what search terms or date ranges may be used. Other legal authorities should be considered (e.g., owner consent, management, or organizational policies).

Logical acquisitions of mobile device data may result in the limited recovery of application and user data. This can be supplemented by a manual analysis of relevant artifacts through the interface of the device (e.g., the photographic documentation of third-party message applications that are unsupported by forensic tools).

Physical acquisitions will result in a richer set of collected data and provide the examiner with the opportunity to prioritize the analysis of relevant artifacts.

For additional information on the aforementioned types of acquisitions, see *SWGDE Best Practices for Mobile Device Evidence Collection and Preservation, Handling, and Acquisition*.

5. Considerations

Data recovered during the analysis process can frequently help establish ownership, possession, and use of the device. Unique device identifiers recovered during the analysis process, such as the IMEI, MEID, IMSI, and ICCID number, can be used in conjunction with records obtained from network service providers to supplement the investigation and validate the results from the analysis.

A mobile device's date and time can be obtained by the cellular network or manually set by the user. This can be an important piece of information to an investigation and the examiner should be mindful that the device's date and time values could differ from the actual date and time (e.g., the time zone the device was actually in, as opposed to how the device was manually set up). Any differences should be noted and appropriate adjustments should be made to reflect accurate information.

Enhanced 911 (E911) is a technology mandated by the U.S. Federal Communications Commission (FCC) enabling mobile devices to process 911 calls and to provide the geographic location of the handset. Additionally, users of GSM and other UICC/SIM dependent devices may also establish cellular voice communication by dialing 911 without the presence of a SIM card.

In situations where 911 is dialed on a mobile device, regardless of the service status, the location information may be recorded by the device. This location information may be an estimated latitude and longitude of the device with a specified degree of accuracy, a specific latitude and longitude of the cellular system antenna, and cell-site and sector the device was connected. The network service provider may record this information, thus CDRs can be of interest to an investigator for validation purposes. Outgoing 911 calls may or may not be logged in the memory of the mobile device or UICC/SIM. For cell site analysis, see *SWGDE Recommendations for Cell Site Analysis.*

6. Artifacts of Value

Mobile device manufacturers generally provide specification information regarding the features and capabilities of a device. Exact specifications of a device may vary based on the following: iterative changes made during the manufacturing process, the era in which the device was manufactured, operating system updates, firmware version, modifications, and

applications installed on the device. The potential evidence to be analyzed on a device may include the following items:

- Subscriber and equipment identifiers
- Various user accounts
- UICC / SIM Card (Universal Integrated Circuit Card/Subscriber Identity Module Card)
- External media storage
- Date/time, language, and other settings
- Phonebook/Contact information
- Calendar information
- Text messages / SMS (Short Message Service)
- Multimedia messages / MMS (Multimedia Messaging Service)
- Instant messages
- Call logs
- Email
- Photos and included metadata such as EXIF (Exchangeable Image File Format)
- Videos and included metadata such as XMP (Extensible Metadata Platform)
- Audio and voicemail recordings
- Web browsing activities
- Electronic documents
- SQL Databases
- Network and WiFi information
- Bluetooth devices and connections
- Social media-accounts-related data
- Applications-related data
- Health data
- Location data
- Saved passwords, encryption keys, or any other authentication or access mechanisms
- VoIP applications
- Third Party Communication application data

7. Forensic Tool Analysis

Once the device has been acquired, an examiner may take the following steps: parsing and searching the data, identifying and marking key evidence, and organizing the artifacts to be included in a final report.

Each forensic tool has varying capabilities and there may be times when utilizing multiple tools is necessary to meet the needs of the examiner. For example, one tool may not be able to decipher or parse all available data at the time of analysis; however, a second tool may have the capability to interpret data that the first was unable to parse. Additional data may be parsed and available to the examiner by reprocessing the device as forensic tools are updated.

The capabilities of a forensic tool, the specific operating system present, and the type of device being examined will determine what types of artifacts can be recovered, identified, and

included in a final report. The search capabilities of a tool can play a significant role in the discovery of information used for the documentation of relevant artifacts. For example, some tools capable of searching for textual evidence can identify and categorize files based on file extension, where others use a file signature database. The latter feature is preferable since it lessens the possibility of missing data because of an inconsistent file name extension (e.g., eliminating a text file where an extension was changed to that of a graphics or image file). Similarly, the ability of a tool to recover images automatically into a common graphics library for analysis is useful.

Some tools may only have a search capability that matches specific input text strings while other more advanced tools allow for more intelligent search capabilities, allowing for generalized regular expression patterns (grep) type searches, including wildcard matches, searches based on types of encoding (e.g., 7bit PDU) filtering of files by extension, and directory and batch scripts that search for specific types of content (e.g., email addresses, URLs). The greater the tool's capabilities, the more the forensic examiner benefits from experience and knowledge of the tool.

8. Validation of Data Results

Items that may be of evidentiary value and deemed admissible in court cases should be validated. Results from a forensic tool can be validated in several ways. One method is to compare sample results and spot-checking across multiple tools on the extracted data. Another method is to manually examine data where it resides within the device extraction. Some tools indicate where automatically-parsed content is stored, making it easier for the examiner to verify the data is presented or decoded properly. Another reliable method to validate analysis results is to compare the parsed content with content that is actually viewable on the subject device. This also assists in the identification of unsupported application parsing.

If multiple tools provide the same results, the examiner can articulate with a higher level of certainty that the results are accurate and reproducible. If the results do not match across multiple tools, with manual parsing, or with what is viewable on the subject device, then the examiner is responsible for properly addressing the contradictions. Steps should be made to identify the tool's limitations and what can be done to properly present the data. Validation issues must be addressed and documented. For tool validation, see *SWGDE Recommended Guidelines for Validation Testing.*

9. Evidentiary Considerations

9.1. Timeline analysis

A timeline is a chronological listing of events or actions occurring on a device that may be of interest to an investigator. It should be noted, timeline events generated by a tool may not be a complete listing of all the events that occurred on a device. Timelines are considered a snapshot of the information derived from parsed data only.

9.2. Data hiding applications

Mobile applications do exist to hide user content. These applications are specifically designed to mask the contents within and can appear like traditional applications installed on the device by default (e.g., *Calculator+*).

9.3. Logical Encryption

Logical, or file-based, encryption encodes selective data in a file system. This type of encryption can be enabled using features included in the operating system or can be enabled using third-party applications. Additionally, individual applications may deploy encryption on a per-file or per-directory basis. Because file-based encryption can be independently enabled on specific files and within applications, this data may not be automatically recognized by common mobile forensic tools. Forensic analysis software may include functionality to decrypt select application data through the utilization of a passcode or password.

However, it should be noted that some applications advertise the ability to encrypt user content, but they do not actually perform any encryption. To an examiner, the data may be unreadable at face value, and look encrypted, when the data is simply encoded. Many false encryption claims made by application developers are actually encoded with Base 64 encoding. Mobile forensic tools may allow an examiner to manually decode the content properly.

9.4. Malware Detection

Malicious software may exist on a mobile device which can be designed to obtain user credentials and information, promote advertisements and phishing links, remote access, collect ransom, and solicit unwanted network traffic. Forensic tools are not always equipped with antivirus and anti-malware to automatically detect malicious applets on a device. If the tools do have such capability, they do not typically run against an extraction without examiner interaction. If the examiner's tools do not have antivirus/anti-malware capability, the examiner may need to manually detect malware through the use of common anti-virus software applications as well as signature, specification and behavioral-based analysis.

10. Mobile Operating Systems

Mobile device operating systems, much like desktop operating systems, bridge software and hardware and determine the functions and features available on each phone. The operating system of a phone can be proprietary to specific device manufacturers or open-source. Mobile operating systems include the following:

- Android: open-source software currently maintained and developed by Google available for a range of devices. Derivatives of Android exist that are not maintained by Google (e.g., Fire OS, OmniRom, MIUI).
- iOS: proprietary software developed by Apple available solely on Apple devices.
- Linux: though Android's kernel uses the Linux kernel, specific Linux derivatives exist that target mobile devices. As of writing, no Linux release currently has a notable mobile device market share (e.g., PureOS, Ubuntu Touch).

- Windows Mobile: proprietary software developed by Microsoft. Microsoft has listed the latest version, Windows 10 Mobile, as EOL and has announced no future mobile OS development intentions. [1]
- Other: operating systems developed by manufacturers.

According to the International Data Corporation (IDC), Android and iOS mobile operating systems compose the vast majority of the world market share. [2] For that reason, this document will focus on the analysis of those two systems.

10.1. Android Analysis

Android devices are manufactured by a number of companies, including Samsung, LG, Google, HTC, Sony, and Motorola. The large quantity of Android device manufacturers results in a wider variation in mobile device handsets, features, characteristics, internal storage structure, and forensic analysis tool support.

The version of Android operating system can have a meaningful impact on the location of important evidentiary artifacts within the device's file system and internal storage. Examiners should be cognizant of the variance in operating system versions that they may encounter during analyses of Android devices.

10.1.1. Cloud Account

Android strongly suggests users register and sync the device to a Google account. This feature, if logged in, syncs personal information, settings, and allows access to Google services including Drive, Maps, Photos, Calendar, and others. Identifying the cloud account(s) on an Android device can reveal the owner of the device and additional evidence sources.

10.1.2. Google Play

Google Play, formerly known as Android Market, is the default application for downloading applications. However, Android users are not confined to Google Play as a source for applications. Users may access the third-party application market or they may install an application offline. Enterprises can distribute internal applications as well through Mobile Device Management (MDM) systems. For this reason, there is a possibility that Android devices may have more applications not supported by forensic tools.

Forensic software may not support automated parsing of third-party application data due to the proliferation of such applications. A manual review of the device's catalog of installed applications can assist an examiner with identifying unparsed application data. This catalog is typically parsed and made available for review by forensic software, but a manual analysis of the packages.xml file within the device's system partition can assist with the identification of installed applications. The list of installed Android applications should be reviewed in order to assist with identifying sources of potentially relevant information, such as communications from third-party applications. Moreover, it may be beneficial to reach out to the application provider to obtain subscriber account information and other records of activity associated with the application.

There are two primary backup methods for Android devices: cloud-based and manual. There are many cloud-based backup services including Google, manufacturer-specific backup options such as “Samsung Cloud,” or a multitude of available third-party backup applications. Manual backups can also exist on a PC or other devices. Identifying and securing cloud or manual backups can potentially yield additional stored data not resident on the device. Cloud backup data can also assist with validating data contained within a device.

10.2. iOS Analysis

Apple’s proprietary operating system on their mobile devices is called iOS. This operating system platform is generally met with major updates every year and is incrementally updated throughout the year with minor changes. The version of iOS will be relevant during analysis of the device. For example, iOS 10.3 changed the file system from HFS+ to APFS, thus changing the location of certain files.

Although there may be artifacts similar in name and function as the Android mobile operating system, there will be useful evidentiary artifacts only found in iOS. If a forensic tool does not fully support parsing the artifacts located within iOS, it is recommended that an analysis be performed using a Mac in lieu of missing important file system artifacts.

10.2.1. Cloud Account

iOS devices allow and encourage users to register and sync the device to an iCloud account using an Apple ID. This feature, if logged in, syncs personal information, settings, and allows access to Apple services including iMessage, FaceTime, iCloud, App Store, Find My, Music, and others. Identifying the cloud account(s) on an iOS device can reveal the owner of the device and additional evidence sources.

Due to this syncing of Apple devices, artifacts located on an iOS device may have originated from other devices using the same Apple ID account. Although this frequent syncing of devices may offer a seamless experience for the user, care must be taken to ensure which device is associated with the artifact in question. For example, forensics tools used on iOS devices may not differentiate Safari internet history (history.db) by the device used to access the websites in question.

10.2.2. Apple Services

iOS devices are equipped with applications and features proprietary to Apple that allow a user to store data on Apple’s servers and communicate with other Apple IDs through the Internet. These services include, but are not limited to, iCloud, iMessage and FaceTime.

10.2.3. iMessage

iMessage is an Internet-based messaging service that allows users to send and receive text messages, chats, and MMS between two or more Apple devices. iMessage data may reside on the mobile device, additional devices synced by an Apple ID, and iCloud accounts. iMessages are routed through Apple’s servers, therefore carrier records will not reflect the

communications. A user can disable the iMessage feature on the device. If iMessaging capabilities are enabled, poor connectivity can still result in the transmission of a message with another Apple device through standard carrier wireless service. In this case, the message would be routed as a general SMS /MMS, and it would appear in a carrier's records.

10.2.4. FaceTime

FaceTime is an Internet-based call service that allows users to video call between two or more Apple devices. Like iMessages, FaceTime records may reside on the mobile device, devices synced by an Apple ID, and an iCloud account. FaceTime calls are routed through Apple's servers, therefore carriers will not possess stored records of the communications.

10.2.5. App Store

By default, Apple restricts the installation of unsigned third-party apps and only allows approved apps through the App Store. To install an application, the user is required to sign into an Apple account and authorize the installation of the app. This installation is recorded within the Apple ID and the iOS as a "purchase" date. The presence of apps which are unavailable in the App Store may indicate the device is "Jailbroken" or the application in question is sideloaded; thus, providing insight into the user's technical abilities.

10.2.6. iOS Time Format

iOS devices utilize UNIX Epoch and CF Absolute Time formats to record dates and times. The UNIX Epoch format represents the number of seconds elapsed since January 1, 1970 and will be represented as a 4-byte (32 bit) value. The CF Absolute Time format represents the number of seconds elapsed since January 1, 2001 and will also be represented as a 4-byte (32 bit) value. For example, the CF Absolute time integer 219216022 can be decoded as Thursday, 13 December 2007 05:20:22 UTC.

11. External Media Analysis

Many mobile devices allow flash media (e.g., MicroSD, M2 cards) to be installed in the mobile device to supplement the internal storage. This type of media can significantly increase the storage capacity of a device up to hundreds of gigabytes of data. Flash media cards can be removed for imaging and analysis outside the mobile device. If the removable media is encrypted, it's data may need to be extracted while mounted in the mobile device. The acquired external media should then be analyzed in conjunction with the device.

UICC card extractions should be analyzed to identify carrier information and locally stored user generated data.

12. Artifact Analysis

Automated tools that parse device data may not always fully interpret or process all relevant user data. One of the first analysis steps an examiner should take is to see what applications were parsed by the automated tool. If an application of value was not parsed, an examiner may need to manually parse files to locate relevant data. Some forensic tools provide scripting interfaces to allow examiners to extend the automated processing of artifacts.

A primary difference between mobile device forensics and computer forensics is the volatility that exists in the mobile device's memory and data storage. This is highlighted in two automatic functions that are engineered into mobile devices: wear leveling and garbage collection. These functions are essentially writing, organizing, defragmenting, and cleaning data within a mobile device in pursuit of streamlining the device's functionality. Furthermore, these functions have both advantages and disadvantages for examiners alike. Wear leveling may be advantageous to an examiner because it can allow for a greater chance to recover deleted artifacts. However, garbage collection may make deleted data unrecoverable. Garbage collection and wear leveling are randomized, and are virtually impossible for examiners to predict. As such, the recovery of deleted artifacts, while still possible, may seem random.

Due to the constant volatility that exists in mobile devices, multiple extractions from the same device will result in non-matching hashes. However, this does not mean hashing is obsolete. An examiner should still hash an extraction to ensure the content does not change during analysis. Additionally, the hashing of individual files may assist in identifying and excluding certain files based on their digital fingerprint (e.g., ransomware).

12.1. Applications

Applications installed from stores such as Google Play and App Store are assigned a unique identifier following the reverse domain naming convention of *com.developer.appname* and a corresponding system directory is created on the host device. Default iOS applications such as Camera, Calendar, Music, etc., can be identified by the application ID *com.apple.appname*. Applications can locally store settings, configuration information, and user data on the device. Cross-platform applications - applications written for multiple operating systems - may store artifacts in different data structures or locations. Examiners should be aware applications can also store substantive user data on third-party cloud storage which is not always available to examiners through a forensic acquisition of the device. To obtain data from Internet based applications, see *SWGDE Best Practices for Digital Evidence Acquisition from Cloud Service Providers*.

12.2. Databases

Mobile device operating systems and software applications often store application data and configuration settings within databases. SQLite databases are one of the most widely used database engines on mobile devices and will likely contain the most data of evidentiary value to the examiner. SQLite databases are a stand-alone, lightweight, cross-platform, serverless database engine. They may have a file extension of .sqlite, .db, and possibly no file extension at all. SQLite databases can contain user data relating to SMS, MMS, call logs, contacts, calendars, user notes, installed applications, and browser history. Database files may contain deleted content that is not viewable on the device.

The analysis of these databases vary based on either the examiner's toolset or manual parsing abilities. The tools available to the examiner, however, may have parsing limitations. This is a result of the enormous amount of applications released into the marketplace every day, the

application container featuring the data is encrypted, or because of version upgrades that change the application program interface (API) of a supported legacy system.

If the aforementioned tool limitations exist, then manually parsing or exporting the database from a mobile device image may be necessary. Most tools will provide the examiner with the capability to export the targeted database for manual analysis. However, if manually examining a database file, an examiner needs to be aware of associated sqlite journal or log files that may be present. These files may contain data changed by the user or OS that is not present in the main database file. SQLite -journal files function as a backup up of the main database. With SQLite version 3.7.0, associated -journal files changed to Write Ahead Log (-wal) files. The -wal file may contain data not yet committed to the main database.

After carving or exporting a database, manual analysis is generally completed using either open source programs or commercial programs that organize the data into individualized tables. From there, concentrating on relevant tables and reviewing the information within is the key to finding targeted data.

12.3. XML Files

Android devices typically store valuable system-related information within .xml files. These configuration files can contain saved settings and application usage information

12.4. Plists

Plist files are configuration files featured within Apple's operating systems to store system and user-defined settings and logging. Similar to Windows' registry files, Plist artifacts may contain data ranging from encryption keys to credit card numbers to location data.

13. Manual Analysis

Whether or not a device is supported by the forensic tools available to the examiner, a manual preview of the device should be completed, if possible. This option should be used as a final step. Manual analysis will not provide any deleted data and may not uncover data hidden by the user. Manual analysis also comes with a risk of changing attributes or evidence on the device. For example, accessing the gallery to view photos may change the last accessed time of the photos. Similarly, manually reviewing text messages may change the status of the messages from read to unread. As previously indicated, however, such analysis is helpful to validate findings and look for artifacts unsupported by the examiner's tool set.

To conduct a manual analysis, the examiner should use a digital camera or video recorder to properly document the artifacts on the target device. Pictures or videos should be taken of the requested artifacts and ensure clear focus of the screen. During the analysis, the examiner must document all settings changed and applications that were accessed on the device.

If the device was not powered off since being obtained from the owner, the examiner should focus on any running applications, notifications, open internet browser windows, time/date, and any encryption that may be enabled if the device is powered off.

14. References

[1] Microsoft, KB4522812, Windows 10 Mobile EOL note, https://support.microsoft.com/en-au/help/4522812/windows-10-update-kb4522812
[2] Chau, M., & Reith, R. (2019, October 25). Smartphone Market Share - OS. Retrieved January 13, 2020, from https://www.idc.com/promo/smartphone-market-share.

SWGDE Best Practices for Mobile Device Forensic Analysis

History

Revision	Issue Date	Section	History
1.0 DRAFT	2020-01-16	All	Initial draft created and voted by SWGDE for release as a Draft for Public Comment.
1.0	2020-09-17		Voted for release as final publication