SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

FOR585: Advanced Smartphone Forensics

MOST RELEVANT EVIDENCE PER GIGABYTE!

DFIR_SmartPhone_v2.3_7-17

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

FOR500
Windows Forensics (Formerly FOR408)
GCFE

FOR518
Mac Forensics

FOR526
Memory Forensics In-Depth

FOR585
Advanced Smartphone Forensics GASF

OPERATING SYSTEM & DEVICE IN-DEPTH

INCIDENT RESPONSE & THREAT HUNTING

FOR508
Advanced IR and Threat Hunting
GCFA

FOR572
Advanced Network Forensics and Analysis GNFA

FOR578
Cyber Threat Intelligence

FOR610
REM: Malware Analysis
GREM

SEC504
Hacker Tools, Techniques, Exploits, and Incident Handling GCIH

@sansforensics
sansforensics
dfir.to/DFIRCast
dfir.to/gplus-sansforensics
dfir.to/MAIL-LIST

MOST RELEVANT EVIDENCE PER GIGABYTE!

Smartphone Acquisition Guide

A Device On & Unlocked

1. Isolate device from the network if possible
   - Disable WiFi and Hotspots
   - Airplane mode
   - SIM ID cloning
2. Take the necessary steps to ensure physical device access is possible
   - Remove passcode
   - Enable USB debugging
   - Enable "Stay Awake" option
   - Disable timed screen lock features
3. Physical Acquisitions
   - Acquire supporting media
   - SIM card(s)
   - Media cards
   - Check associated media for device backups
4. Logical acquisitions*
   - Logical/file system acquisitions
   - Device backups

*Turning the phone off at this stage could invoke device passcode.

B Device On & Locked

iOS

1. These devices can be physically acquired even if passcode is set with use of custom boot loaders
   - iPhone 2G/3G/3GS/4
   - iPod touch 1/2/3/4G
   - iPad 1st Generation
2. Physical acquisition is not possible on 64-bit and the non-jailbroken devices if the passcode is set and unknown
   - iPhone 4s-latest
   - iPod touch 5G-latest
   - iPad 2-latest
3. Acquire supporting media
   - SIM card
4. Check associated computers and media for device backups
   - Check paired computers for lockdown.plist file
   - Check for iTunes and iCloud backup files

Android

1. Physical access MAY require that USB debugging mode is enabled. Forensic tools will use custom bootloaders to bypass the passcode if applicable
2. Acquire supporting media
   - SIM card(s)
   - Media card(s)
3. Check associated computers and media for device backups
   - Computers and media cards

BlackBerry

1. All acquisition methods, including physical acquisition, require passcode
2. Acquire supporting media
   - SIM card(s)
   - Media cards
3. Check associated computers and media for device backups
   - .bbb and .ipd files
   - Check media card for info.mkf file and, if present, attempt to get password using Elcomsoft Phone Password Breaker

Nokia OS

1. Physical acquisition will bypass passcode in most cases
2. If device is locked, attempt Nokia default passcode of 12345
3. Acquire supporting media
   - SIM card(s)
   - Media cards — will often contain backup of key user data (email, SMS, contacts, calendars)
4. Check associated computers and media for device backups
   - Nokia PC Suite

Windows

1. Attempt physical acquisition to bypass passcode
2. Acquire supporting media
   - SIM card
   - Media cards

Knock-Off

1. Physical acquisition will most often bypass passcode
2. Acquire supporting media
   - SIM cards
   - Media card(s)

Device Is Off

1. Attempt physical acquisition while turned off →
2. Turn on and go to step 1 of A or B

JTAG or CHIP-OFF

JTAG | BOTH | CHIP-OFF

JTAG

- The phone must be returned to a fully functional state
- Less expensive acquisition option

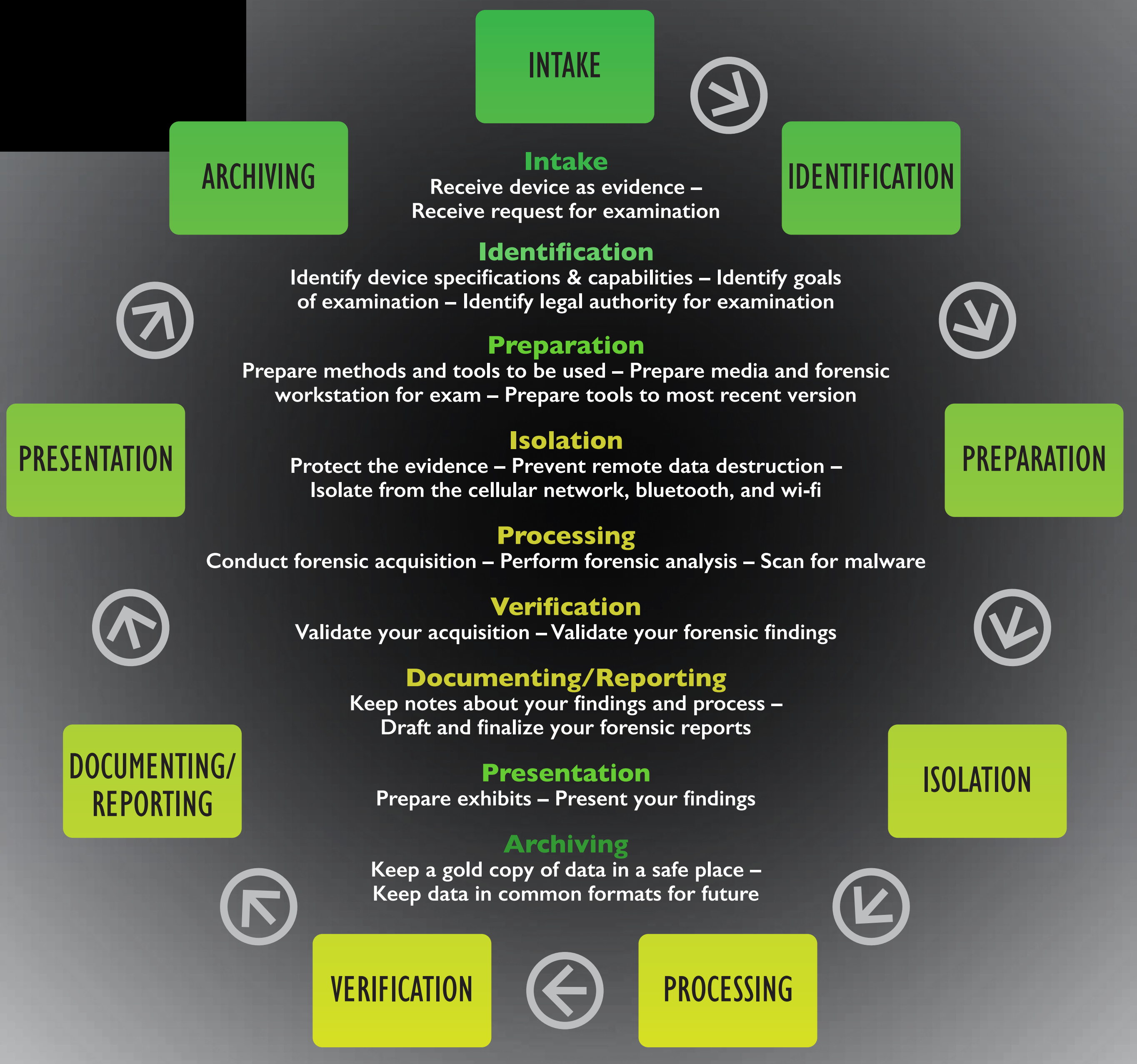
Both

- Device model is unsupported by traditional methods
- USB ports damaged or inaccessible
- Only partial support exists (file system or logical)

CHIP-OFF

- The device has sustained extensive damage
- JTAG ports have been disabled by manufacturer
- When exact state of flash memory must be preserved

Nine Elements of Mobile Forensic Process



Intake
Receive device as evidence – Receive request for examination

Identification
Identify device specifications & capabilities – Identify goals of examination – Identify legal authority for examination

Preparation
Prepare methods and tools to be used – Prepare media and forensic workstation for exam – Prepare tools to most recent version

Isolation
Protect the evidence – Prevent remote data destruction – Isolate from the cellular network, bluetooth, and wi-fi

Processing
Conduct forensic acquisition – Perform forensic analysis – Scan for malware

Verification
Validate your acquisition – Validate your forensic findings

Documenting/Reporting
Keep notes about your findings and process – Draft and finalize your forensic reports

Presentation
Prepare exhibits – Present your findings

Archiving
Keep a gold copy of data in a safe place – Keep data in common formats for future

Acquisition Methods

LOGICAL

- Includes active information from logically stored data
- Is supported for most devices by most tools
- Easy reporting
- May not provide access to a complete set of raw files

FILE SYSTEM

- Includes active files and folders from file system
- May contain remnants of deleted items
- Is supported for most devices by most tools
- May require the passcode if set

PHYSICAL

- Includes active and deleted data
- Not all deleted data are parsed
- Provides complete access to files on the devices
- Not supported for all devices
- Requires advanced decoding and examination

MANUAL

- Examiner scrolls through device to document contents
- Photographs or video of displayed data
- Supported for all devices unless physically damaged
- Simple reporting, but time-consuming

Encoding vs. Encryption

ENCODING SCHEMES	
ASCII	Unicode
UTF-8	Base64

ENCRYPTION ALGORITHMS	
AES	Blowfish
Twofish	Serpent

Definition of Encoding

1. To convert (as a body of information) from one system of communication into another, especially to convert (a message) into code
2. To change (information) into a set of letters, numbers, or symbols that can be read by a computer

Definition of Encryption

1. To change (information) from one form to another, especially to hide its meaning

Mobile Malware and Spyware

Common Signs and Symptoms

- Android devices are most at risk for mobile malware infection
- Poor battery life
- Dropped calls and call disruptions
- Unusually large phone bills
- Data plan spikes
- Device performance problems
- Unexpected device behaviors
  - Unplanned reboots
  - Apps that close or open on their own
  - Unexplained settings changes
- Unexplained application errors
- High-risk user behavior
  - Risky downloads, browsing or link-clicking
- Spyware: Device was out of owner's control
  - Spyware installation requires possession of the device

Potential Infection Vectors

- Official app stores
  - Legitimate apps with increased or unneeded permissions
- Third-party app store repositories
  - Copycat paid apps for "free"
- Androids with outdated OS versions
- Jailbroken iPhones
- Unlocked Windows phones
- Malicious websites
  - Direct "drive-by" download malware installation
- "Smishing"
  - Direct victim targeting through email, SMS, and MMS

Types of Mobile Malware

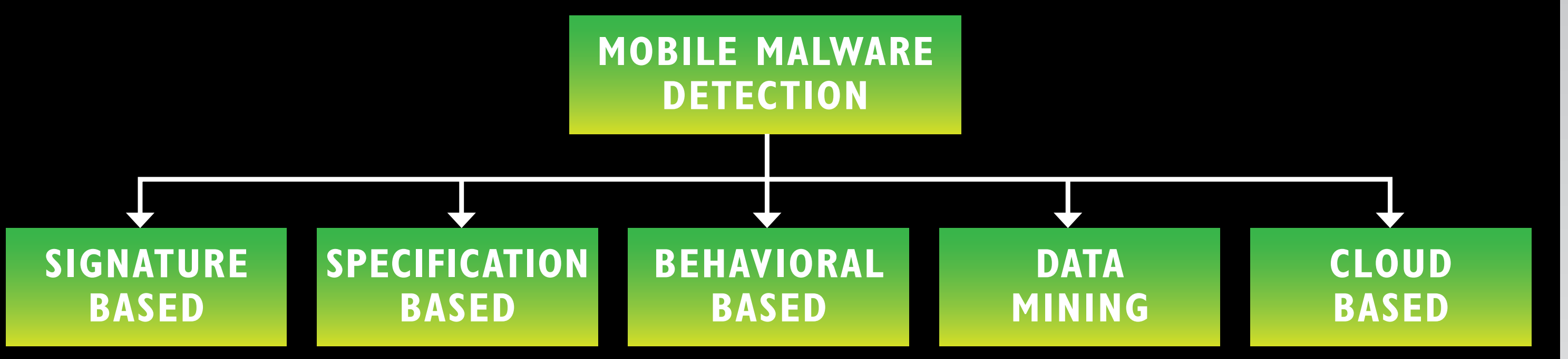
- Malware
  - Backdoor
  - Trojan
  - Worm
- Potentially unwanted applications
  - Adware
  - Trackware
  - Spyware
- Three most common types:
  - SMS trojans
  - Fake install apps
  - Trojan spys

Mobile Malware Examination Tips

- Scan for malware with forensic tools
- Scan for malware with anti-virus software
  - Export file system extraction and scan
- Manually check installed applications for suspicious .apk files
  - Downloaded .apk files may be found in the Root\App, Data\App, or Download directories
  - Most .apk files will be legitimate applications
  - Individual suspicious .apk files can be examined further using static or dynamic methods
- Check download folder(s) for suspicious files
- Check browser history for visits to suspicious sites
- Check for links from SMS, MMS, and email
- Examine activity on phone around the suspected time of infection
- Research any error messages or notifications that might give you clues about infection

Detection

- Finding malware
  ijcset.com/docs/IJCSET13-04-04-094.pdf



Online Mobile Malware Sandboxes

- Upload suspicious .apk files to the Internet for online sandbox analysis:*
  - http://www.apk-analyzer.net
  - http://mobilesandbox.org
  - https://anubis.iseclab.org
  - https://code.google.com/p/droidbox

*Depending upon your location in the world, these sites may or may not be blocked.

Local Static Malware Analysis

- Tools installed on local machine for mobile malware analysis:
  - Android SDK
  - Dex2Jar
  - Dexter
  - JD-GUI
- Virtual machine environments for mobile malware analysis:
  - Santoku

Mobile Malware Prevention

- Installation of mobile malware antivirus apps can assist users in preventing and detecting infection. Some mobile malware antivirus providers include:

- Avast	- AVG
- BitDefender	- Kaspersky
- Lookout	- Sophos
- TrendMicro	- Symantec (Norton)
- TrustGo	

DFIR Smartphone Forensics

MOST RELEVANT EVIDENCE PER GIGABYTE!

SANS FOR585: ADVANCED SMARTPHONE FORENSICS
Course Authors

twitter.com/sansforensics

Heather Mahalik
hmahalik@gmail.com
@heathermahalik

Domenica Crognale
domenica.crognale@gmail.com
@domenicacrognal

Cindy Murphy
cindymurphy2412@gmail.com
@cindymurph

Common Smartphone Evidence Locations

IOS DEVICES

DATABASE	DESCRIPTION
Library/CallHistory/call_history.db Library/CallHistoryDB/CallHistory.storedata	Call logs Call record ((iOS 8 – iOS 10)
Library/AddressBook/AddressBook.sqlitedb	Contacts
Library/AddressBook/AddressBookImages.sqlitedb	Contact images
Library/SMS/sms.db	SMS messages
Library/SMS/Attachments/*	MMS file
Library/Calendar/Calendar.sqlitedb	Calendar
Library/Notes/notes.sqlite	Notes
Library/Safari/*	Safari activity
Library/Accounts/Accounts3.sqlite	Account information
Library/BullitenBoard/ClearedSections.plist	Logs of cleared notifications
Media/PhotoData/Photos.sqlite	Metadata about multimedia files
Library/TCC/TCC.db	Application permissions
Library/Databases/DataUsage.sqlite	Application information and usage details
Library/ADDataStore.sqlite	iOS unlock data repository (Refer to mac4n6.com)
Library/CoreDuet/coreduetd.db	unlock data repository (Refer to mac4n6.com)

PLIST	DESCRIPTION
com.apple.commcenter.plist	Device phone number, network carrier, ICCIDs, and IMSIs
com.apple.accountsettings.plist	Email accounts pushed to device
com.apple.Maps.plist	Last latitude and longitude, map search history
Library/Maps/Bookmarks.plist com.apple.Maps/Maps com.apple.Maps/Maps	Maps bookmarks History.mapsdata (iOS 7) GeoHistory.mapsdata (OS 8 – iOS 10)
SystemConfiguration/com.apple.wifi.plist	WiFi
SystemConfiguration/preferences.plist	WiFi and more
Library/Preferences/com.apple.mobilenotes.plist	Notes
Library/SpringBoard/IconState.plist	Homescreen icon layout
Library/ConfigurationProfiles/UserSettings.plist	User-created restrictions
Library/Preferences/com.apple.springboard.plist	User-created restrictions
Library/Preferences/com.apple.WebFoundation.plist	Safari activity
Library/Preferences/com.apple.MobileSMS.plist	SMS, iMessage and FaceTime
Library/Preferences/com.apple.madrid.plist	SMS, iMessage and FaceTime
Library/DataAccess/AccountInformation.plist	Email sync data
Library/DataAccess/iCloud-'iCloud email account name'/.mboxCache.plist	iCloud email account information
Library/DataAccess/iCloud-'iCloud email account name'/.OfflineCache/'number'	iClould offline cache

BLACKBERRY OS 10

4g LTE

APPLICATION FILES	CONFIGURATION AND SETTINGS FILES		SYSTEM OR USER-GENERATED DATA FILES		
.bar (BlackBerry)	.dat (Android)	.config (BlackBerry)	.db	.sqlite	.jpeg
.apk (Android)	.conf (BlackBerry)	.pem (certificates)	.db-shm	.txt	.txt
.dex (Android)	.xml (Android)		.db-wal	.jpg	.doc, .xls, .ppt, etc.

PATH	EVIDENTIARY DATA	FILE TYPE
File system/settings/pps/services/phone/private/lines/vchat	BB device PIN	N/A
File system/settings/pps/services/bluetooth/network/status	Bluetooth address	N/A
File system/settings/pps/system/bookmarks	Browser bookmarks	N/A
File system/app/sys.browser.'unique device id'/appdata/data/webviews/cache	Cached web objects	N/A
File system/app/sys.browser.'unique device id'/appdata/data/webviews/database/	Cached web objects	N/A
File system/settings/accounts/1000/sysdata/pim/db/1-pim	Calendars	.db
File system/settings/accounts/1000/sysdata/pim/db/8-pim	Call Logs	.db
File system/system/app/sys.browser.'unique device id'/appdata/data/chrome/	Chrome browser artifacts	.db
File system/settings/accounts/1000/sysdata/search/	Complete app listing (including enterprise apps)	.db
File system/system/app/sys.browser.'unique device id'/appdata/data/webviews/localstorage	Default browser artifacts	.db
File system/settings/accounts/1000/sysdata/pim/db/20-pim File system/settings/accounts/1000/sysdata/pim/db/2-pim	Device contacts	.db
File system/settings/pps/services/phone/private/lines/cellular	Device phone number	N/A
File system/settings/pps/services/phone/private/lines/cellular	Last dialed number	N/A
File system/settings/accounts/1000/sysdata/pim/db/5-pim	Linking database	.db
File system/settings/var/places/Places_backup.txt	Location services	.txt
File system/settings/accounts/1000/_startup_data/sysdata/text_messaging/attachments/	Message attachments	Mutli-media files
File system/settings/accounts/1000/sysdata/pim/db/18-pim	Notes	.db
File system/media/documents/	Office documents (Docs To Go)	.xls, .doc, .ppt
File system/settings/pps/services/pim/accounts/settings/	Per app basis – account settings	N/A
File system/settings/var/etc/netsecure/wpa_pps.conf	Saved wireless access points	N/A
File system/settings/pps/services/geolocation/rimlocp/scan_status	Scanned locations	N/A
File System/settings/var/db/text_messaging/messages	SMS and MMS	.db
File system/app/sys.android/'Android application name'	Third-party Android applications	N/A
File system/app/'third-party app name'	Third-party BlackBerry and Android applications	.db, sqlite, .xml, .conf, .dat, etc.
File system/media/camera/	User-created photos	.jpg
File system/settings/pps/services/phone/private/lines/celluar	Voicemail number	N/A
File system/settings/var/etc/netsecure/vpn/	VPN client	.conf
File system/system/app/sys.browser.'unique device id'/appdata/data/webviews/database	Webmail	.db
File system/settings/var/etc/netsecure/ wpa_pps_protected.conf	Wireless passwords	N/A

BlackBerry

FOR585: Advanced Smartphone Forensics

A smartphone lands on your desk and you are tasked with determining if the user was at a specific location at a specific date and time. You rely on your forensic tools to dump and parse the data. The tools show location information tying the device to the place of interest. Are you ready to prove the user was at that location? Do you know how to take this further to place the subject at the location of interest at that specific date and time? Tread carefully, because the user may not have done what the tools are showing!

Mobile devices are often a key factor in criminal cases, intrusions, IP theft, security threats, and more. Understanding how to leverage the data from the device in a correct manner can make or break your case and your future as an expert. FOR585: Advanced Smartphone Forensics will teach you those skills.

YOUR TEXTS AND APPS CAN AND WILL BE USED AGAINST YOU!

WINDOWS PHONE 8/10

PATH	
Users/WPCOMMSERVICES/APPDATA/Local/Unistore/Store.vol	SMS Contacts
Users/WPCOMMSERVICES/APPDATA/Local/UserData/Phone	Call history
Users/DefApps/APPDATA/INTERNETEXPLORER/NetCache/	Internet browsing history
Users/PublicPictures/CameraRoll/ (WP_YYYYMMDD_###.jpg)	Pictures taken with the device Videos taken with the device
Users/PublicPictures/SavedPictures/	Pictures saved to the device from other sources (Facebook, etc.)
Users/WPCOMMSERVICES/APPDATA/Temp/RequestManager/Cache	Cached images from message attachments
SharedData/Comms/Messaging/Temp/MMS	File attachments from incoming and outgoing mms messages
SharedData/Comms/Unistore/Data (in various subfolders)	MMS attachments MMS formatting information MMS message content
SharedData/Input/neutral/	ihds.dat – user input word list (unique words) livehads.dat – form history

ANDROID

3G

PARTITION	FILE	TABLE	DESCRIPTION
Data	Root/Property/persist.sys.timezone	*	Timezone
Data	Root/Property/netpolicy.xml	*	Timezone
Data	com.android.providers.contacts/databases/contacts2.db com.android.providers.contacts/ databases/calllog.db com.sec.android.provider.logsprovider/databases/*.db	calls calls logs	Call logs Call logs (OS 7) Call logs and more!
Data	com.android.providers.contacts/ databases/contacts2.db	accounts	Login info
Data	com.android.providers.contacts/ databases/contacts2.db	contacts and raw contacts	Contacts
Data	com.android.providers.telephony/ databases/mmssms.db	sms and part	SMS/MMS
Data	com.google.android.gms/databases/herreva	-	Wireless network and MAC addresses
Media	/0/DCIM/Camera	-	EXIF data with location info
Data	"Application Folder"	Application Data Files*	
Data	/dalvik-cache	.dex files (Application related)	
Data	/system/packages.xml /system/packages.list /system/netpolicy.xml	Application permissions	
Data	/system/packages.list	Application metadata	
Data	/system/usagestats/0/<various directories>/*.xml	Application Usage	
Data	/system/batterystats.bin /system/batterystats-daily.xml /system/batterystats-checkin.bin	Application Usage (may be difficult to parse)	
Data	/com.sec.android.app.launcher/databases/launcher.db /com.android.providers.downloads/databases/downloads.db	Application artifacts (even after deleted)	
Data	/system/dmappmgr.db	Application Usage	